

**Huawei Qiankun**

# **Security CloudService**

<b>Issue</b>	01
<b>Date</b>	2024-01-02



**Copyright © Huawei Technologies Co., Ltd. 2024. All rights reserved.**

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

## **Trademarks and Permissions**



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

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

## **Notice**

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

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

# Security Declaration

## Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

# Contents

<b>1 Qiankun Shield and Firewall Onboarding.....</b>	<b>1</b>
1.1 Onboarding USG6000E Series Firewalls .....	1
1.1.1 Scenario Description.....	1
1.1.2 Hardware Description.....	1
1.1.3 Connecting Cables.....	3
1.1.4 Logging in to the Web UI.....	5
1.1.5 Checking and Upgrading the Version.....	7
1.1.6 Configuring the Device Network.....	9
1.1.7 Loading the Cloud Service Component Package.....	14
1.1.8 Configuring Interconnection Between the Firewall and Cloud Platform .....	15
1.1.9 Checking the Interconnection Result.....	20
1.1.10 Setting Service Parameters (Border Protection and Response Service).....	22
1.2 FAQ.....	23
1.2.1 How Do I Configure Security Policies Required by Border Protection and Response Service (USG6000E Firewalls)?.....	23
<b>2 Border Protection and Response.....</b>	<b>31</b>
2.1 Service Overview.....	31
2.1.1 What Is the Border Protection and Response Service?.....	31
2.1.2 Functions.....	33
2.1.3 Product Highlights.....	35
2.1.4 Application Scenarios.....	35
2.2 Purchase Guide.....	39
2.2.1 Activating the Commercial Service.....	39
2.2.1.1 Activating the Service Using a Tenant Account.....	39
2.2.1.1.1 Registering a Huawei Qiankun Account.....	39
2.2.1.1.2 Activating the Service Package.....	39
2.2.1.2 Activating the Service Using an MSP Account.....	41
2.2.1.2.1 Registering a Tenant Account by MSP.....	41
2.2.1.2.2 MSP-Entrusted Management.....	43
2.2.1.2.3 Activating the Service Package.....	45
2.3 Device Provisioning Guide.....	47
2.3.1 Configuring Device Onboarding.....	47
2.3.2 Configuring Device Security Zones.....	47

2.3.3 Creating Global Whitelists.....	50
2.3.4 Blacklist and Whitelist Authorization.....	51
2.3.5 Subscribing to Alarms and Reports.....	51
2.3.6 Checking Threat Events.....	53
2.4 User Guide.....	53
2.4.1 Checking the Cyber Security Status.....	53
2.4.1.1 Checking the Security Protection Dashboard.....	53
2.4.1.2 Checking the Homepage of the Border Protection and Response Service.....	57
2.4.2 Quick Configuration.....	59
2.4.3 Handling Threat Events.....	60
2.4.3.1 Event Overview.....	60
2.4.3.2 External Attack Sources.....	62
2.4.3.3 Compromised Hosts.....	66
2.4.3.4 Malicious Files.....	70
2.4.4 Managing Blocklists and Allowlists.....	72
2.4.4.1 Clearing IP Address Blacklists from a Specified Device with One Click.....	72
2.4.4.2 Manually Creating an IP Address Blacklist or Whitelist.....	73
2.4.4.3 Checking IP Address Blacklists and Whitelists Fast.....	76
2.4.4.4 Manually Creating a Domain Name Blacklist.....	78
2.4.4.5 Checking Domain Name Blacklists Fast.....	79
2.4.5 Checking Security Reports.....	80
2.4.6 IP Address Security Zone Management.....	82
2.4.6.1 Monitoring the Security Zone Status.....	82
2.4.6.2 Configuring a Global Whitelist.....	83
2.4.6.3 Configuring Untrusted Intranet Addresses.....	85
2.4.6.4 Configuring Device Security Zones.....	87
2.4.7 Authorization Management.....	89
2.4.7.1 Blacklist and Whitelist Authorization.....	89
2.4.8 Configuring the Automatic Threat Blocking Duration.....	90
2.4.9 Configuring Custom Signature Authorization.....	91
2.4.10 Configuring Metadata Detection and Protection Rules.....	92
2.4.11 Tenant Service Management by an MSP.....	94
2.4.11.1 Introduction to Tenant Service Management by an MSP.....	94
2.4.11.2 Introduction to the MSP homepage.....	94
2.4.11.3 Performing Operations on Managed Services.....	94
2.4.12 More Operations.....	101
2.4.12.1 Basic Tenant Operations.....	102
2.4.12.2 Basic MSP Operations.....	103

# 1 Qiankun Shield and Firewall Onboarding

---

[1.1 Onboarding USG6000E Series Firewalls](#)

[1.2 FAQ](#)

## 1.1 Onboarding USG6000E Series Firewalls

### 1.1.1 Scenario Description

This document describes how to bring a firewall online and how to configure the Border Protection and Response Service.

**Table 1-1** Matching firewall models

Service	Firewall Model
Border Protection and Response Service	USG6530E/USG6585E

### 1.1.2 Hardware Description

#### NOTE

This section uses the USG6585E as an example. Other models are slightly different from the USG6585E. For details, see "Installation > Hardware Guide > Hardware Overview" in the [HUAWEI USG6000E Product Documentation](#).

Figure 1-1 Appearance and auxiliary materials of the USG6585E

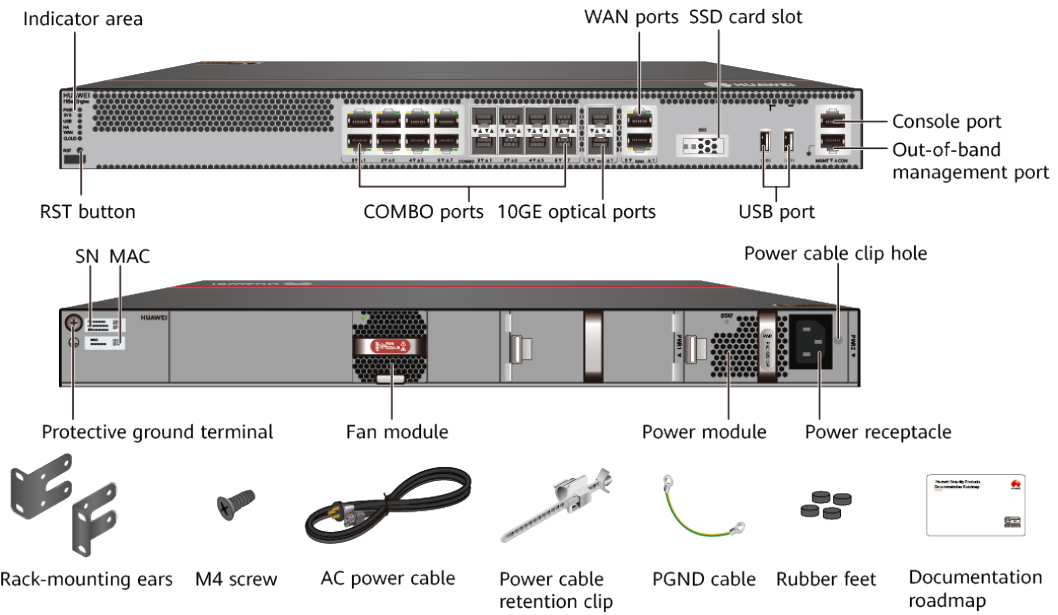


Table 1-2 USG6585E service port description

Port Name	Description
Combo ports (0–7)	<ul style="list-style-type: none"><li>The electrical port and its corresponding optical port are multiplexed. They cannot both work. (For example, when an optical port is activated, the corresponding electrical port is automatically disabled.)</li><li>Electrical and optical ports share the same interface view and are numbered from GigabitEthernet0/0/0 to GigabitEthernet0/0/7.</li><li>By default, a combo port works as the electrical port. You can run the <b>combo enable { copper   fiber }</b> command to configure a combo port to work as an electrical port or optical port as required.</li></ul>
WAN ports (0 and 1)	The ports are numbered as WAN0/0/0 and WAN0/0/1.
10GE optical ports (0 and 1)	The ports are numbered as XGigabitEthernet0/0/0 and XGigabitEthernet0/0/1.
MGMT port	Management interface of the device. The port is MEth0/0/0 and its default IP address is 192.168.0.1.

Table 1-3 USG6585E indicator description

Silkscre en	Name	Color	Status	Description
PWR	Power indicator	Green	Steady on	The power module is working properly.
		-	Steady off	The power module is faulty or the device is not powered on.
SYS	SYS indicator	Green	Steady on	The system is being powered on or restarted.
		Green	Blinks once every 2 seconds (0.5 Hz)	The system is running properly.
		Green	Blinks four times every second (4 Hz)	The system is starting.
		Red	Steady on	A system fault occurs.
		-	Steady off	The system is not running.

1.1.3 Connecting Cables

Connecting Ethernet Cables

Figure 1-2 Connecting Ethernet cables for the USG6585E

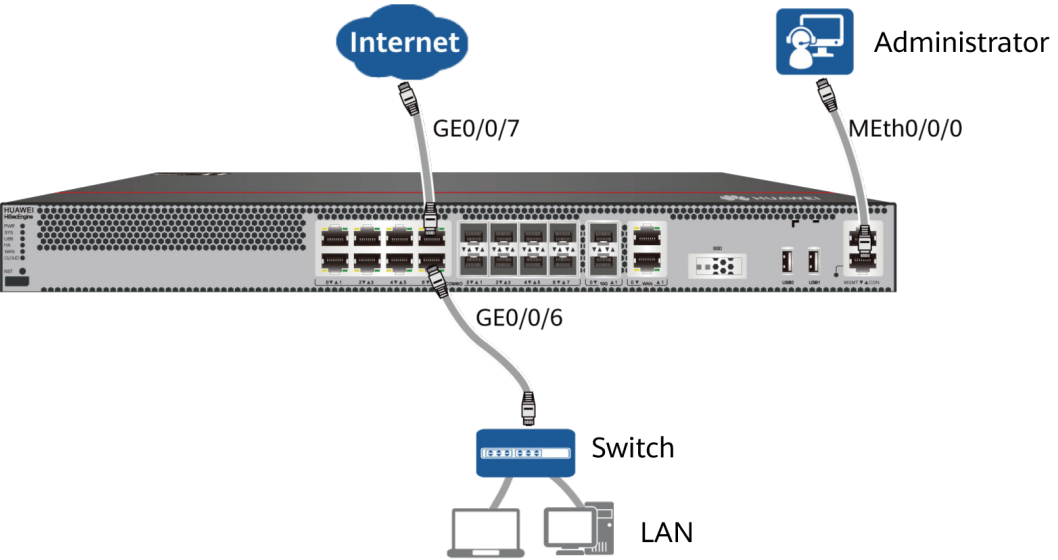
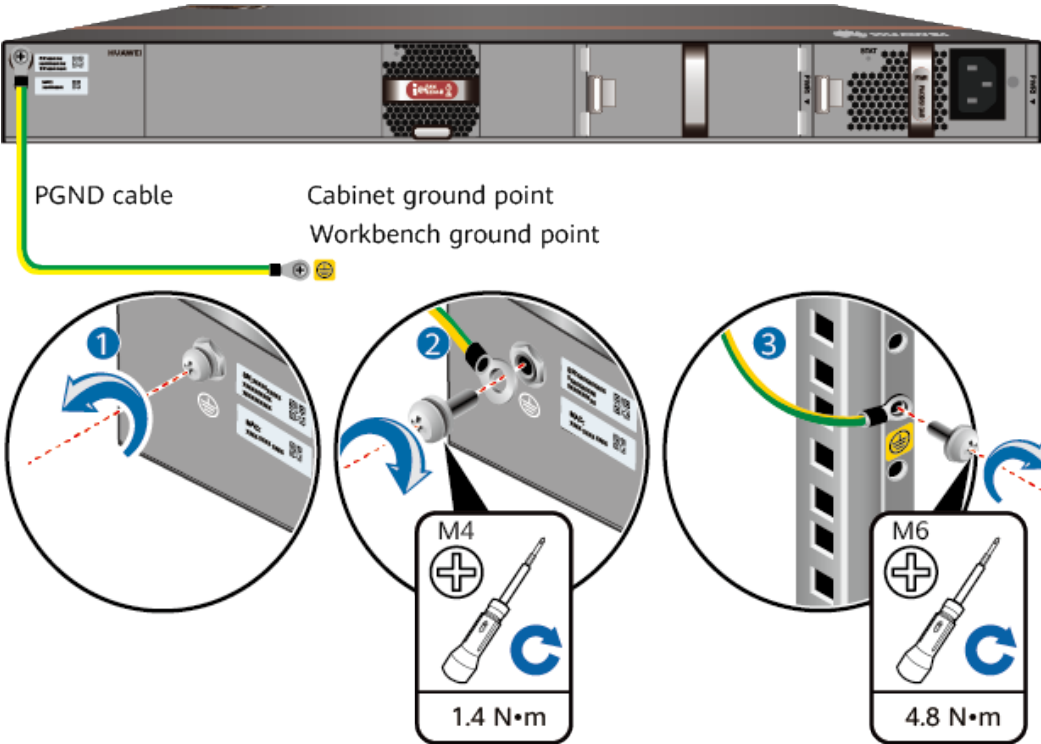


Table 1-4 Interface description

Interface Silkscreen	Interface Number	Description
6	GE0/0/6	Downlink service interface, which is a Layer 3 interface and connects to the LAN switch. Here, GE0/0/6 is used as an example.
7	GE0/0/7	Uplink service interface, which is a Layer 3 interface and connects to the Internet. Here, GE0/0/7 is used as an example.
MGMT	MEth0/0/0	Management interface of the device. This interface connects to the management PC and is used for service configurations on the device web UI. The default IP address of the interface is 192.168.0.1.

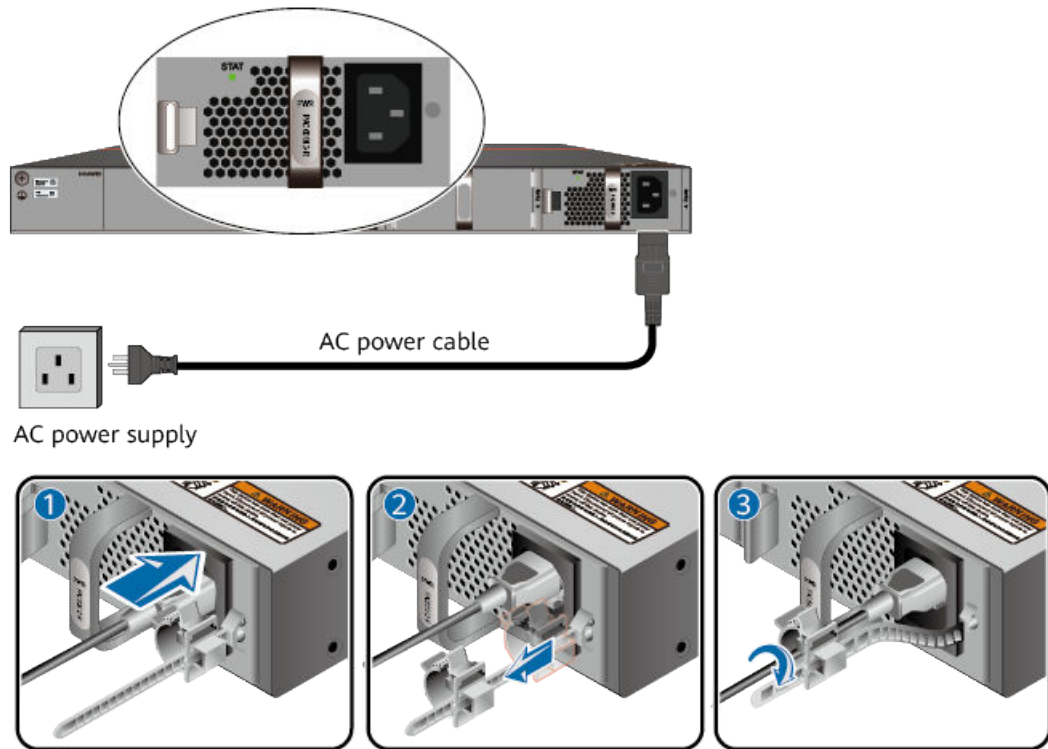
Connecting a PGND Cable

Figure 1-3 Connecting a PGND cable



## Connecting a Power Cable and Buckle

Figure 1-4 Connecting a power cable and buckle



### 1.1.4 Logging in to the Web UI

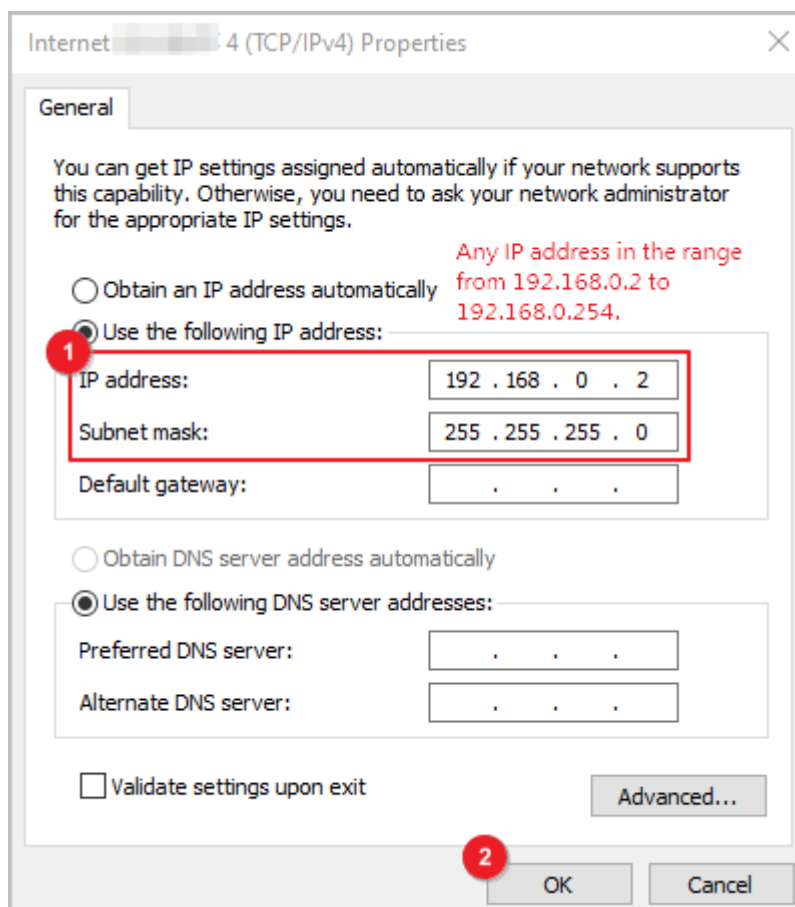
#### Procedure

1. Configure an IP address for the network interface on the management PC so that the PC can communicate with the management interface (default IP address: 192.168.0.1/24) on the device. The following steps assume that the PC is running Windows 10.
  - a. Click **Start** and then **Control Panel**.
  - b. Choose **Network and Internet** > **Network and Sharing Center**. In the navigation pane on the left, click **Change adapter settings**.
  - c. Right-click the network adapter to be configured and choose **Properties** from the shortcut menu. Double-click **Internet Protocol Version 4 (TCP/IPv4)** and configure the IP address shown in [Figure 1-5](#).

#### NOTICE

If the PC has multiple network adapters and you cannot determine which network adapter is used, you are advised to remove and install the network cable and observe the status of each network adapter to determine the network adapter to be configured.

**Figure 1-5** Configuring an IP address



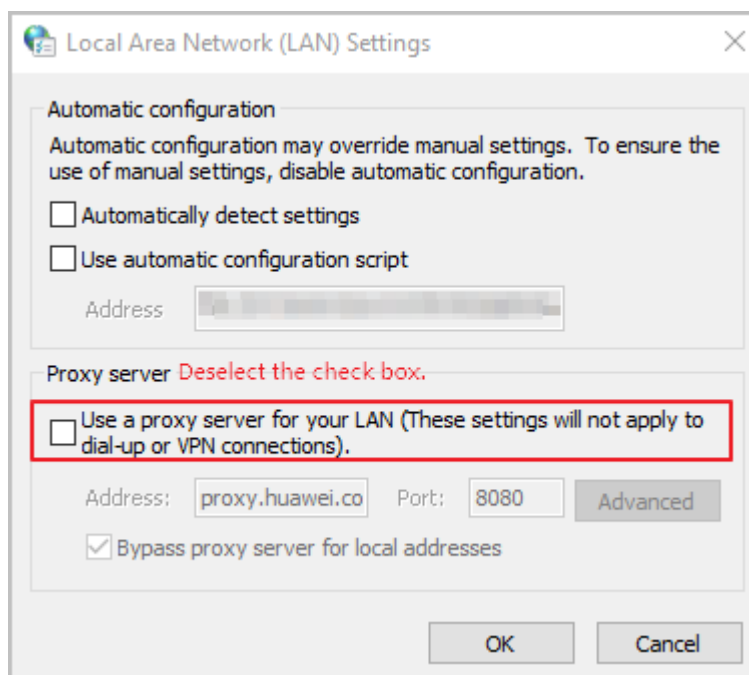
2. Disable the network connection proxy.

If the network connection proxy is set, you may fail to log in to the web UI of the device. Therefore, you are advised to cancel the setting.

- a. Go back to **Control Panel** and click **Internet Options**.
- b. On the **Connections** tab page, click **LAN settings** in the **Local Area Network (LAN) settings** area.

Check whether a proxy server is set. If so, deselect the proxy server.

**Figure 1-6** Setting a proxy



3. Open a browser (Google Chrome is recommended) and access the standard configuration page at <https://192.168.0.1:8443>.
4. Before you log in for the first time, you need to register an administrator account. Complete the registration as prompted.
5. After the registration is complete, the login page is displayed. Use the registered administrator account to log in.

## 1.1.5 Checking and Upgrading the Version

### Context

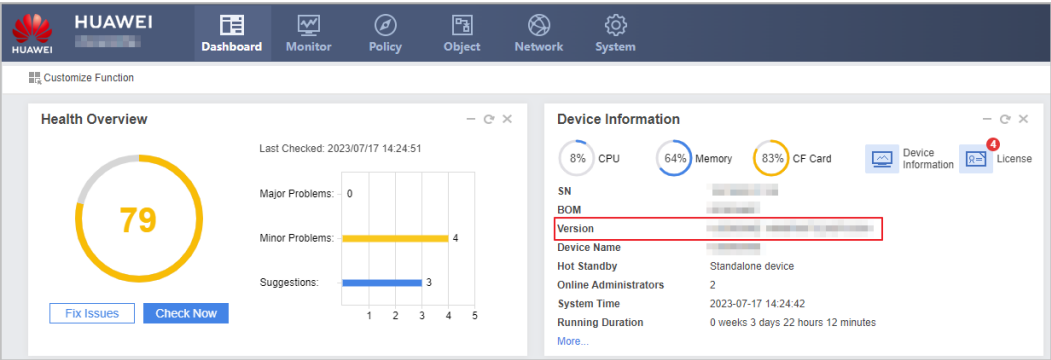
Before using this service, upgrade its version to a supported one. For details about the supported versions, see section "[Configuring Device Onboarding](#)" in the *Deployment Guide* of Border Protection and Response Service.

### Procedure

1. Log in to the standard page at <https://192.168.0.1:8443>.
2. Choose **Dashboard** > **Device Information** to view the information about the running software version.

If the version is not a recommended or supported version, upgrade it.

Figure 1-7 Device information



3.
- (Optional) Log in to [Huawei enterprise technical support website](#), select the corresponding model and recommended version, and download the software package. If you do not have an account, register one as prompted.

Figure 1-8 Downloading a software package

<input type="checkbox"/> Software Name	Size	Publication Date	Downloads	Download software	Manual Verification Signature File	Automatic Verification Signature File
<input checked="" type="checkbox"/> USG65E_V600R007C20 bin	202.30MB	2022-08-31	445	<a href="#">Download</a>	pgp	cms
<input type="checkbox"/> [blurred software name]	69.63KB	2022-08-31	91	<a href="#">Download</a>	pgp	cms

Download

Comment

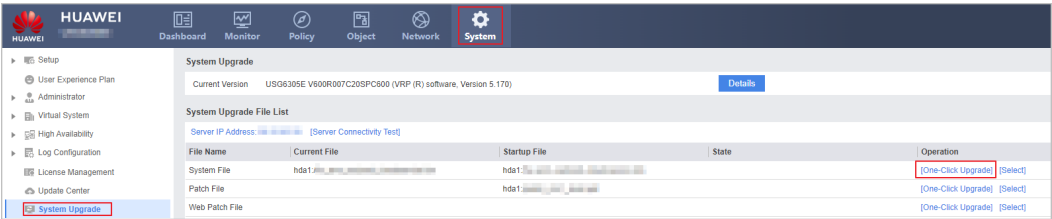
4.
- (Optional) Perform one-click upgrade.

NOTE

This section describes only the key steps for **One-Click Upgrade**. For more upgrade methods and precautions, see [HUAWEI USG6000E V600R007C20 Upgrade Guide](#).

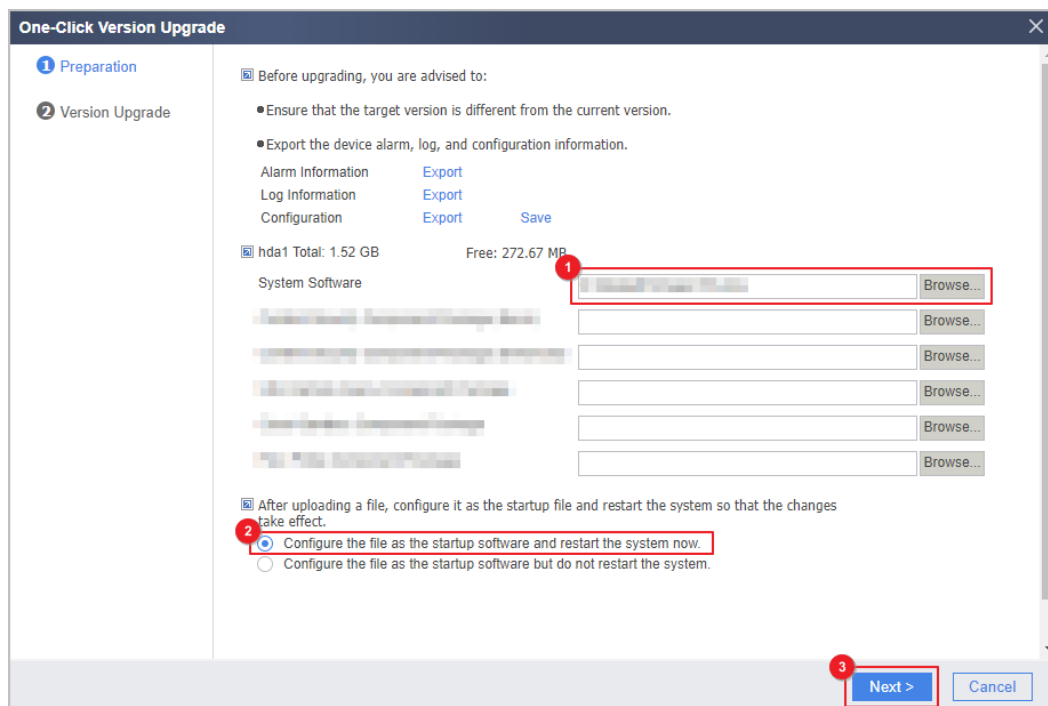
- a.
- Choose **System > System Update**, and click **One-Click Upgrade** corresponding to **System File**.

Figure 1-9 System upgrade



- b.
- On the page that is displayed, perform the operations shown in the following figure.

**Figure 1-10** One-click upgrade



- c. Click **Next** to start the upgrade.

**NOTE**

The upgrade takes 10 to 15 minutes. After the upgrade succeeds, the device automatically restarts.

- d. Verify the configuration.

After the device is started, log in to the web UI, choose **System > System Update**, and view information about the running system version in **System File**.

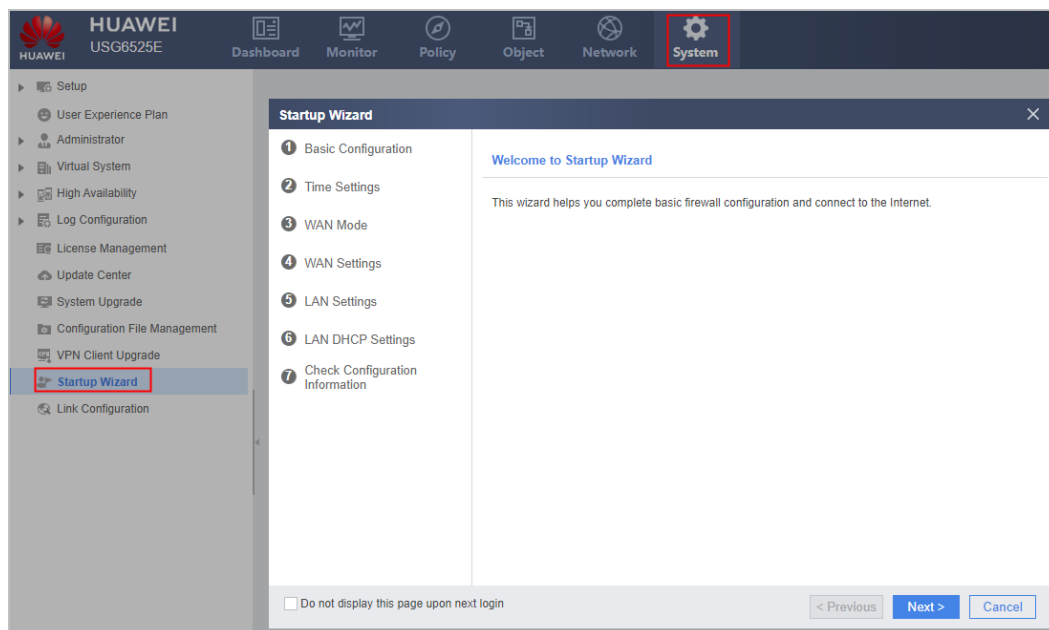
If the running version is the recommended one, the upgrade is successful.

## 1.1.6 Configuring the Device Network

### Procedure

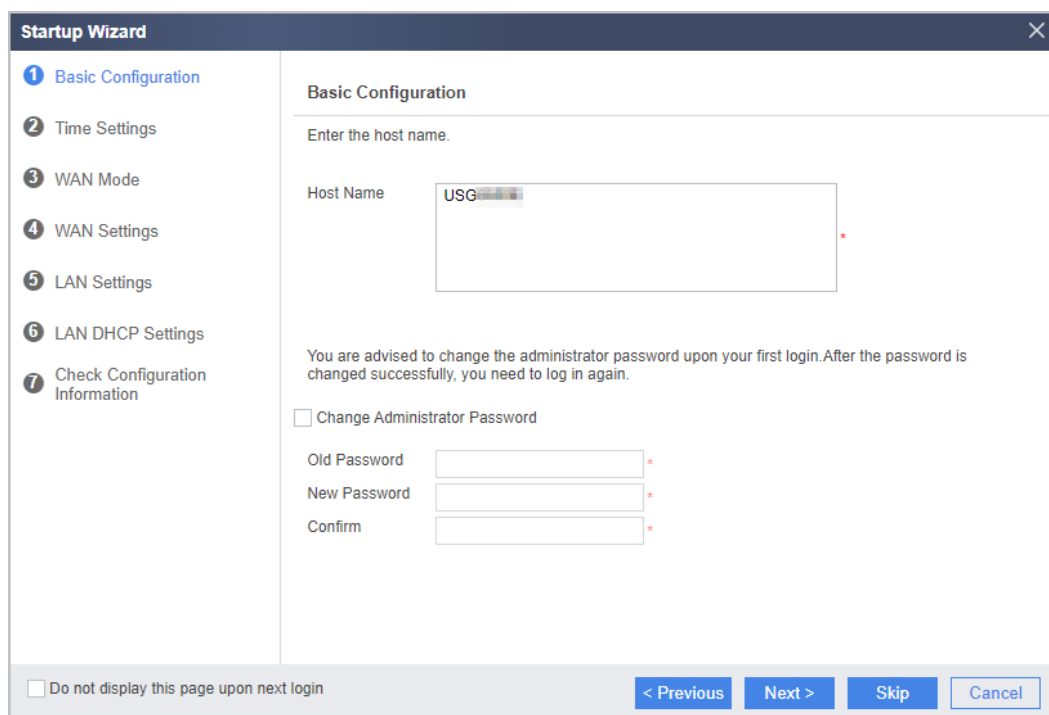
1. Choose **System > Startup Wizard**, and click **Next**.

**Figure 1-11** Startup wizard

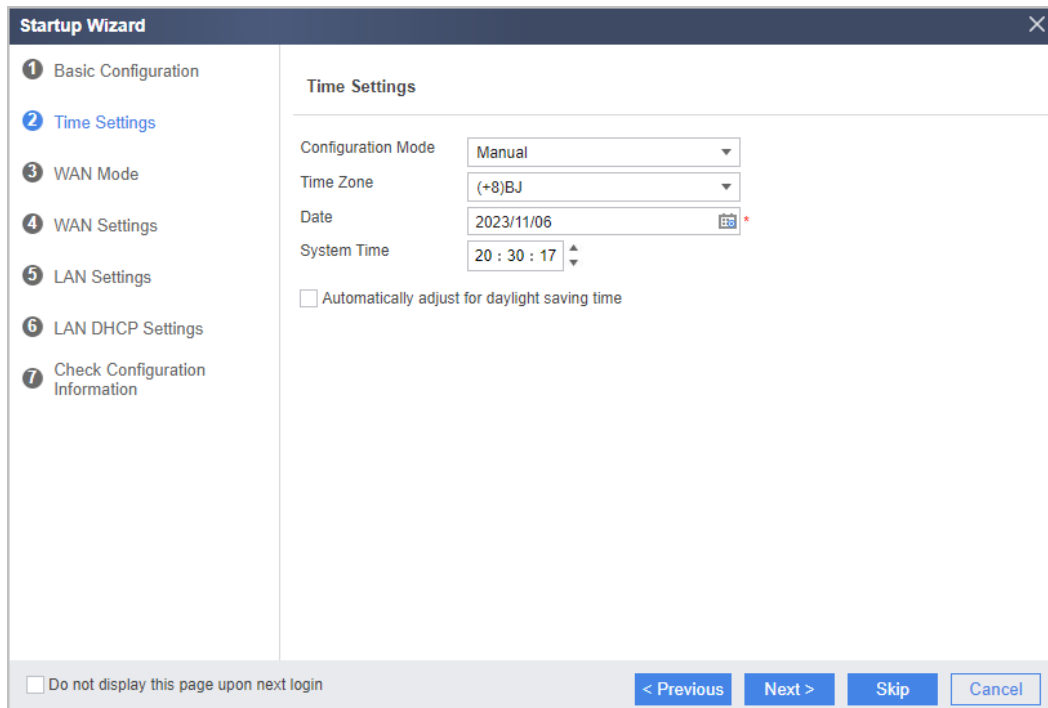


2. Configure basic information as shown in the following figure and click **Next**.

**Figure 1-12** Configuring basic information

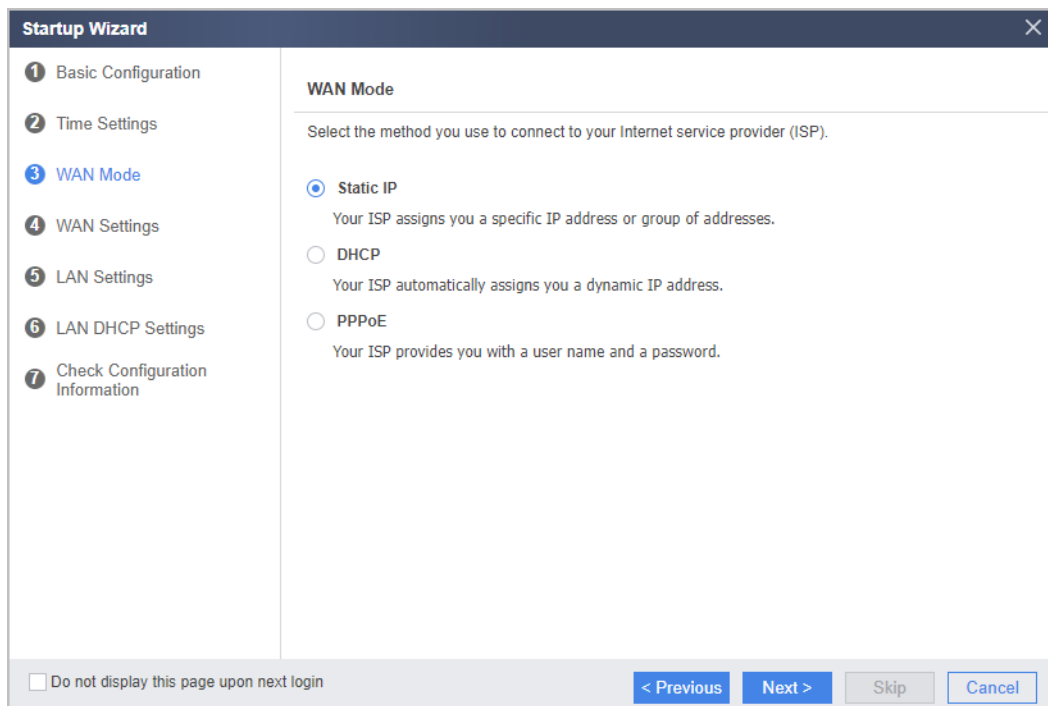


3. Set the system time as shown in the following figure and click **Next**.

**Figure 1-13** Configuring the system time

The screenshot shows the 'Startup Wizard' window with the 'Time Settings' tab selected. On the left, a list of steps includes 'Basic Configuration', 'Time Settings' (highlighted), 'WAN Mode', 'WAN Settings', 'LAN Settings', 'LAN DHCP Settings', and 'Check Configuration Information'. The main area is titled 'Time Settings' and contains the following fields: 'Configuration Mode' set to 'Manual', 'Time Zone' set to '(+8)BJ', 'Date' set to '2023/11/06' with a calendar icon, and 'System Time' set to '20 : 30 : 17' with up/down arrows. There is an unchecked checkbox for 'Automatically adjust for daylight saving time'. At the bottom, there is a checkbox 'Do not display this page upon next login' and four buttons: '< Previous', 'Next >', 'Skip', and 'Cancel'.

4. Select an Internet access mode. Most private lines access the Internet by using a configured public IP address, and therefore the static IP mode is used as an example here. Click **Next**.

**Figure 1-14** Selecting an Internet access mode

The screenshot shows the 'Startup Wizard' window with the 'WAN Mode' tab selected. On the left, the list of steps is the same as in Figure 1-13, but 'WAN Mode' is highlighted. The main area is titled 'WAN Mode' and contains the text 'Select the method you use to connect to your Internet service provider (ISP)'. There are three radio button options: 'Static IP' (selected), 'DHCP', and 'PPPoE'. Below each option is a brief description: 'Your ISP assigns you a specific IP address or group of addresses.' for Static IP, 'Your ISP automatically assigns you a dynamic IP address.' for DHCP, and 'Your ISP provides you with a user name and a password.' for PPPoE. At the bottom, there is a checkbox 'Do not display this page upon next login' and four buttons: '< Previous', 'Next >', 'Skip', and 'Cancel'.

5. Set Internet interface parameters and click **Next**.

**Figure 1-15** Configuring Internet access

The screenshot shows the 'Startup Wizard' window with the 'WAN Settings -- Static IP' tab selected. The left sidebar lists steps 1 through 7, with '4 WAN Settings' highlighted. The main area contains instructions to set parameters for internet access and a list of fields: Interface (GE0/0/7), IP Address (1.1.1.1), Subnet Mask (255.255.255.0), Default Gateway (1.1.1.10), Primary DNS Server (8.8.8.8), and Secondary DNS Server. A red box highlights the Interface, IP Address, Subnet Mask, and Default Gateway fields. A red note on the right says 'Set these parameters based on service requirements'. At the bottom, there is a checkbox 'Do not display this page upon next login' and buttons for '< Previous', 'Next >', 'Skip', and 'Cancel'.

6. Set LAN interface parameters and click **Next**.

**Figure 1-16** Configuring LAN interfaces

The screenshot shows the 'Startup Wizard' window with the 'LAN Settings' tab selected. The left sidebar lists steps 1 through 7, with '5 LAN Settings' highlighted. The main area contains instructions to enter LAN interface information and a list of fields: Interface (GE0/0/6), IP Address (10.0.0.1), and Subnet Mask (255.255.255.0). A red box highlights the Interface, IP Address, and Subnet Mask fields. A red note on the right says 'Set these parameters based on service requirements'. At the bottom, there is a checkbox 'Do not display this page upon next login' and buttons for '< Previous', 'Next >', 'Skip', and 'Cancel'.

7. Enable the DHCP service on the LAN so that the firewall can dynamically allocate IP addresses to intranet PCs.

**Figure 1-17** Enabling the DHCP service on the LAN

8. Verify configurations and click **Apply**.

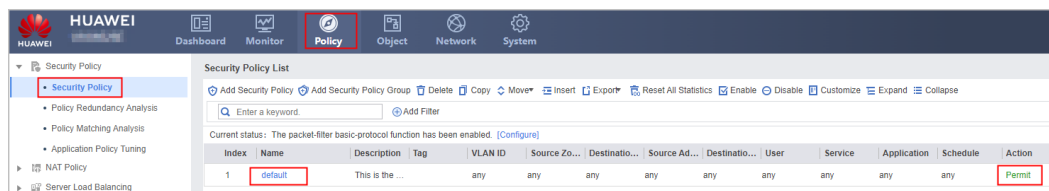
**Figure 1-18** Verifying configurations

9. Choose **Policy > Security Policy > Security Policy** and check whether the action of the **default** security policy is **Permit**.

If not, click the policy name **default** to access the page for modifying the security policy and change the action to **Permit**.

 **NOTE**

You are not advised to create other security policies because the cloud may fail to automatically deliver the created security policies.

**Figure 1-19** Security policy

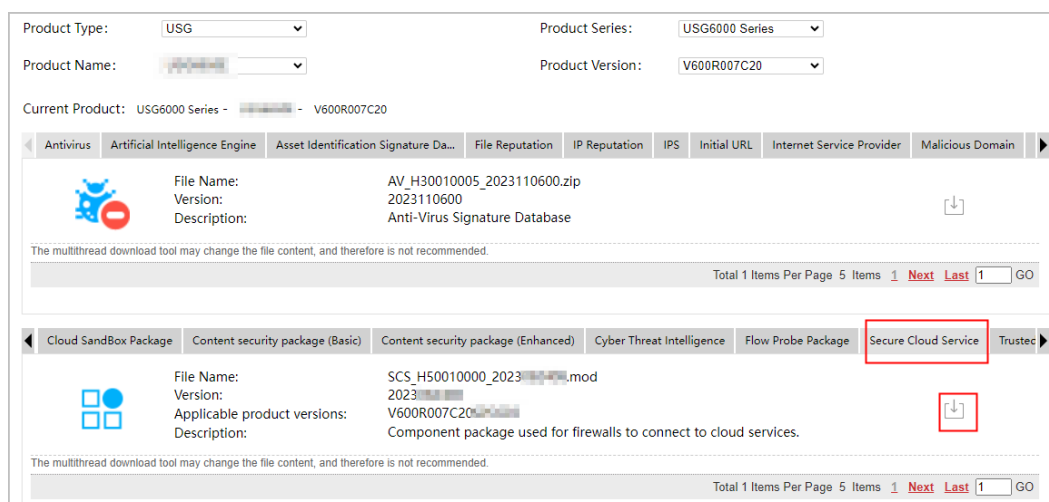
## 1.1.7 Loading the Cloud Service Component Package

### Procedure

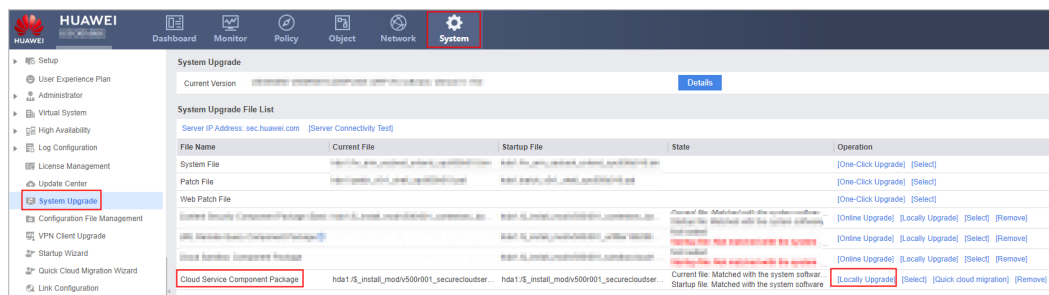
1. Access Huawei security platform (domain name: [isecurity.huawei.com](https://isecurity.huawei.com)). Choose **Signature Update** > **Signature Update**. Select the desired product and version.
2. Download the security cloud service component package.

 **NOTE**

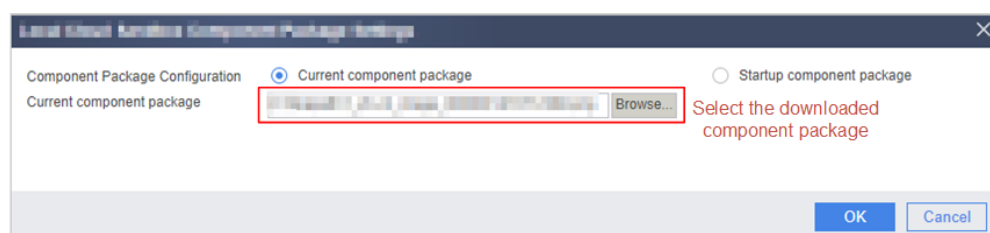
The system software version must match the component package version. Otherwise, the component package cannot be successfully loaded.

**Figure 1-20** Downloading the security cloud service component package

3. Access the standard configuration page at <https://192.168.0.1:8443>, choose **System** > **System Update**, and click **Locally Upgrade**, as shown in the following figure.

**Figure 1-21** Upgrading the component package

4. Select the downloaded component package and click **OK**.

**Figure 1-22** Uploading the component package

## 1.1.8 Configuring Interconnection Between the Firewall and Cloud Platform

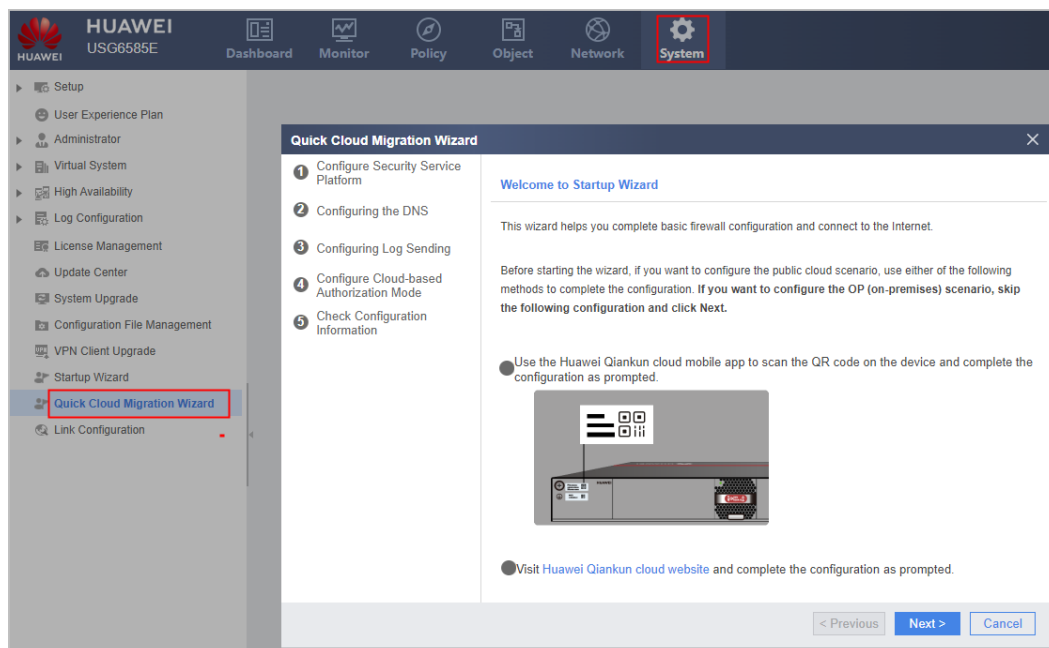
### Prerequisites

- The device can access the Internet.
- The cloud service component package has been loaded.
- You have purchased cloud services.

### Procedure

1. Access the standard configuration page at <https://192.168.0.1:8443> and choose **System > Quick Cloud Migration Wizard**. On the page that is displayed, click **Next**.

**Figure 1-23** Quick cloud migration wizard

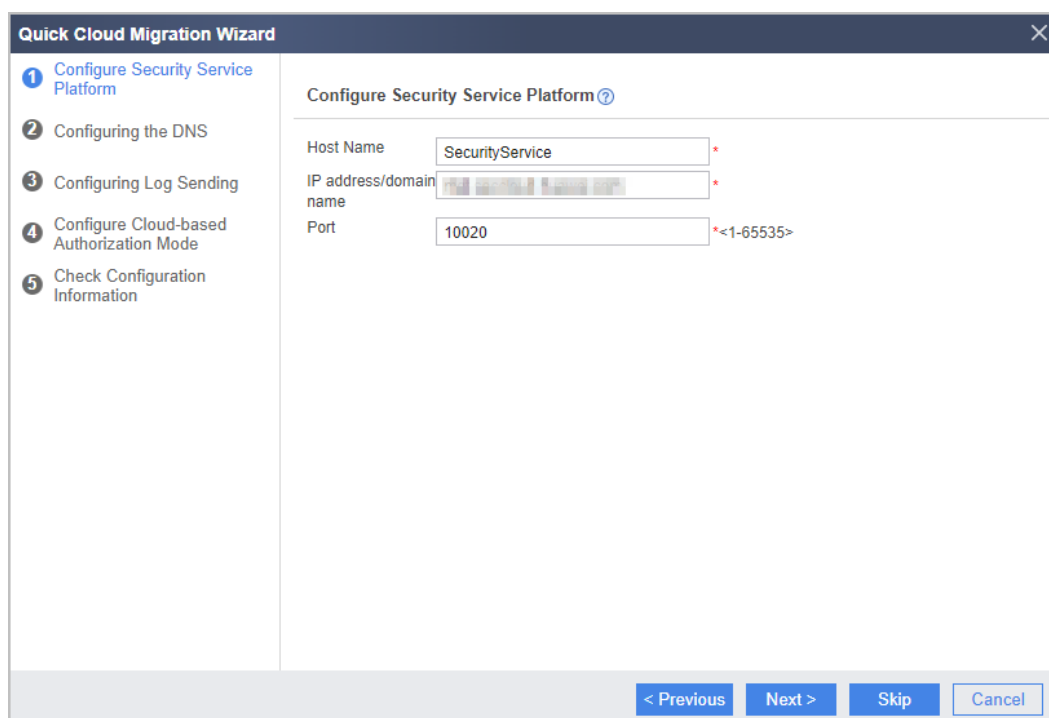


2. Configure the security service platform as shown in the following figure and click **Next**.

**NOTE**

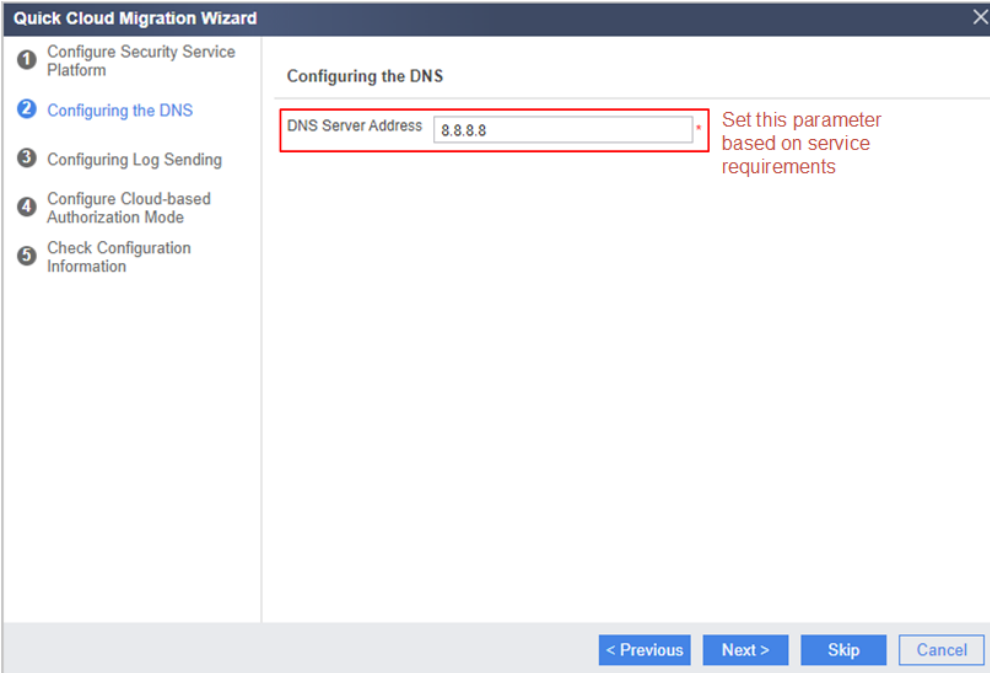
**IP address/domain name** indicates the address or domain name used by the device to send registration requests to the security service platform. Set this parameter based on the actual address or domain name of the target site.

**Figure 1-24** Configuring the security service platform



3. Configure the DNS server address and click **Next**.

**Figure 1-25** Configuring a DNS server



Quick Cloud Migration Wizard

1 Configure Security Service Platform

2 Configuring the DNS

3 Configuring Log Sending

4 Configure Cloud-based Authorization Mode

5 Check Configuration Information

Configuring the DNS

DNS Server Address 8.8.8.8

Set this parameter based on service requirements

< Previous Next > Skip Cancel

4. Configure log sending as shown in the following figure and click **Next**.

**NOTE**

**Cloud service host IP address/domain name** indicates the address or domain name used by the device to send logs to the cloud. Set this parameter based on the actual address or domain name of the target site.

**Figure 1-26** Configuring log sending

The screenshot shows the 'Quick Cloud Migration Wizard' window. On the left, a list of steps is shown: 1. Configure Security Service Platform, 2. Configuring the DNS, 3. Configuring Log Sending (highlighted in blue), 4. Configure Cloud-based Authorization Mode, and 5. Check Configuration Information. The main area is titled 'Configuring Log Sending' and contains the following settings: 'Cloud service PCAP enabling' with a toggle switch turned on, 'Enabling Cloud Service Traffic Report' with a toggle switch turned on, 'Cloud service host IP address/domain name' with a text input field containing a placeholder, and 'Cloud service CA certificate' with a dropdown menu showing 'default\_ca.cer'. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Skip', and 'Cancel'.

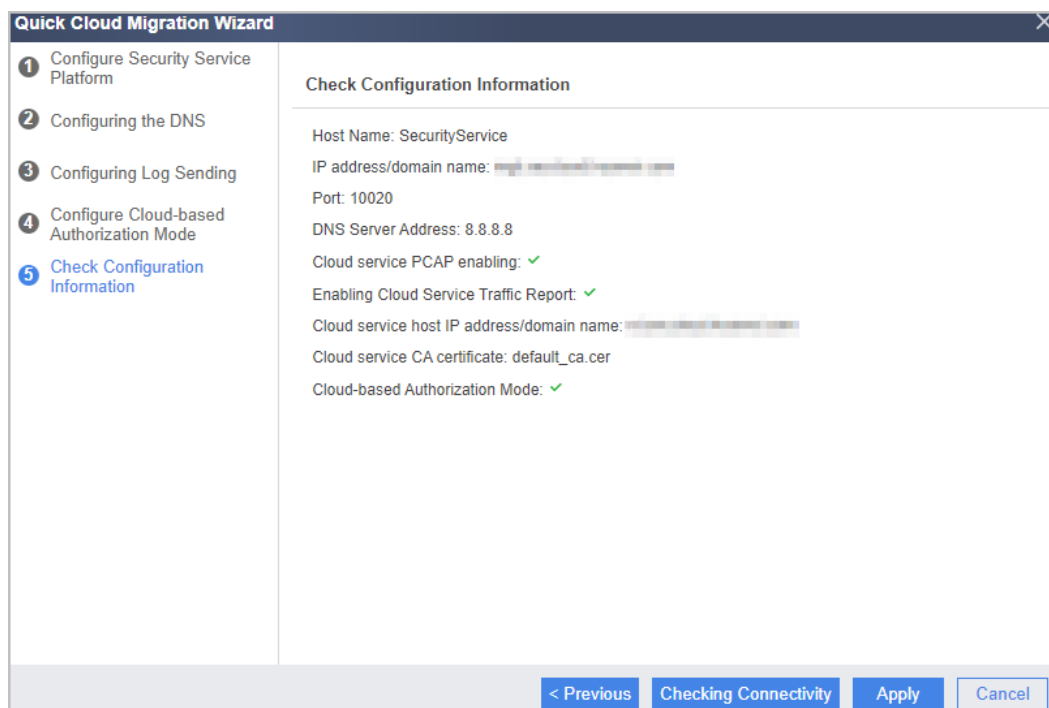
5. Enable the cloud-based authorization mode and click **Next**.

**Figure 1-27** Enabling the cloud-based authorization mode

The screenshot shows the 'Quick Cloud Migration Wizard' window. On the left, a list of steps is shown: 1. Configure Security Service Platform, 2. Configuring the DNS, 3. Configuring Log Sending, 4. Configure Cloud-based Authorization Mode (highlighted in blue), and 5. Check Configuration Information. The main area is titled 'Configure Cloud-based Authorization Mode' and contains the following setting: 'Cloud-based Authorization Mode' with a toggle switch turned on. At the bottom right, there are four buttons: '< Previous', 'Next >', 'Skip', and 'Cancel'.

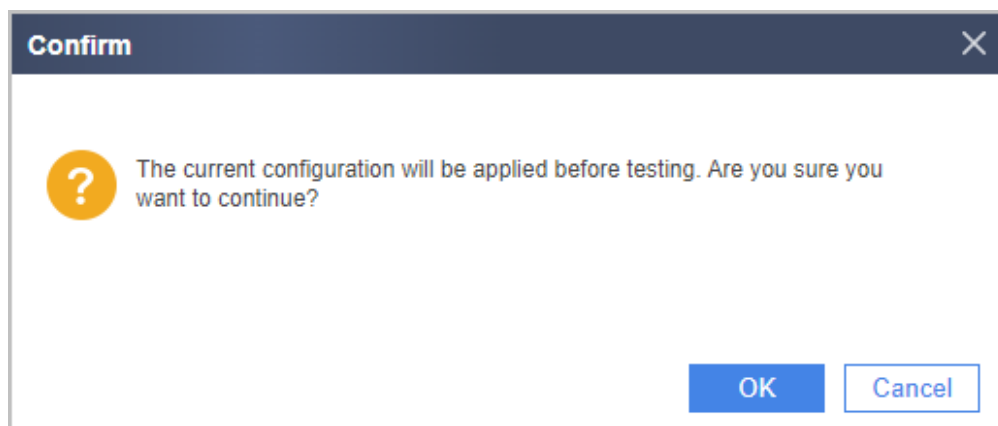
6. Verify configurations and click **Checking Connectivity**.

**Figure 1-28** Checking connectivity

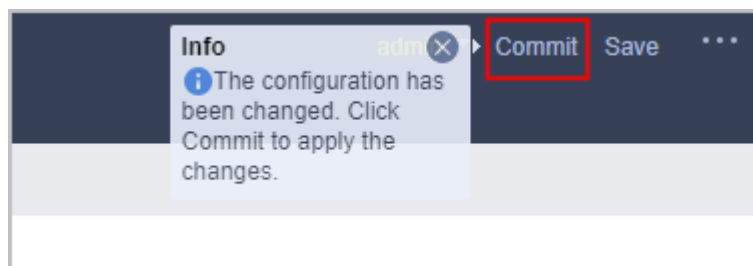


7. In the displayed dialog box, click **OK** to continue the connectivity test.

**Figure 1-29** Configuration delivery prompt



8. In the displayed dialog box, click **OK**.
9. Wait for 1 to 2 minutes and click **Checking Connectivity** again. If the following information is displayed, the connectivity test is successful. Click **OK** and then **Finish**.
10. Click **Commit** at the upper right corner of the page and commit the configuration as prompted.

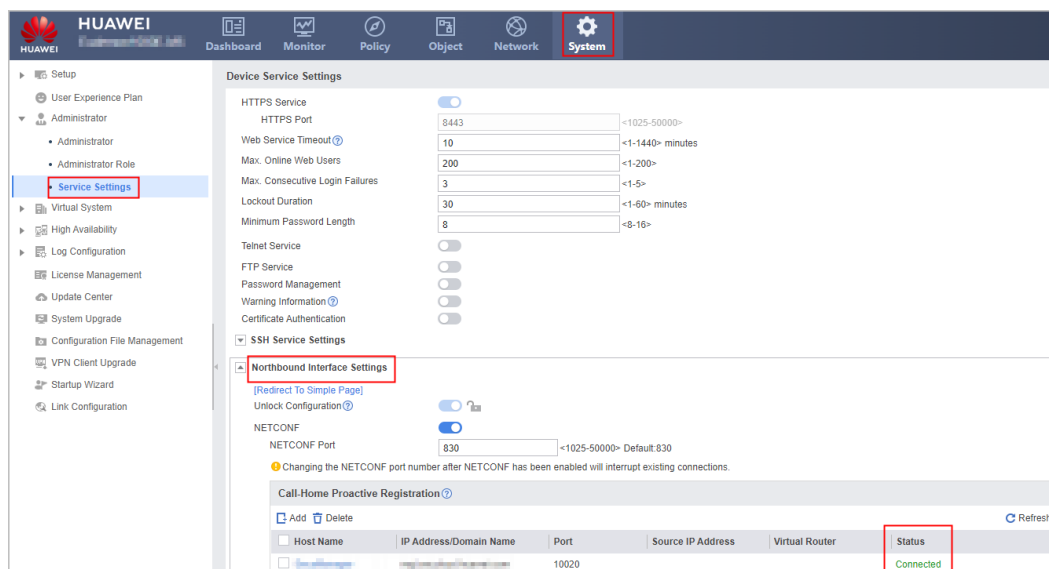
**Figure 1-30** Committing the configuration

## 1.1.9 Checking the Interconnection Result

### Procedure

1. Access the standard configuration page at <https://192.168.0.1:8443>.
2. Choose **System** > **Administrator** > **Service Settings**. In the **Northbound Interface Settings** area, view the northbound connection status.

If **Status** is **Connected**, the interconnection is successful. If the interconnection fails, see [Troubleshooting](#).

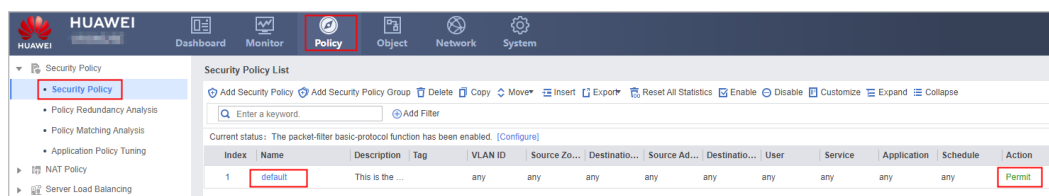
**Figure 1-31** Checking the connection status

### Troubleshooting

If the Qiankun Shield device fails to go online, perform the following steps:

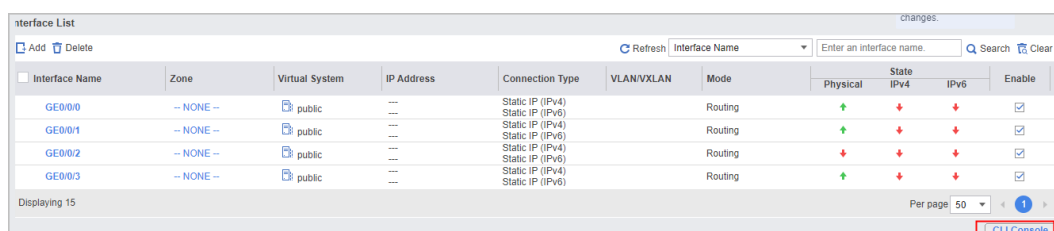
1. Check whether the action of the **default** security policy is **Permit**. If not, change the action to **Permit**.

Figure 1-32 Security policy



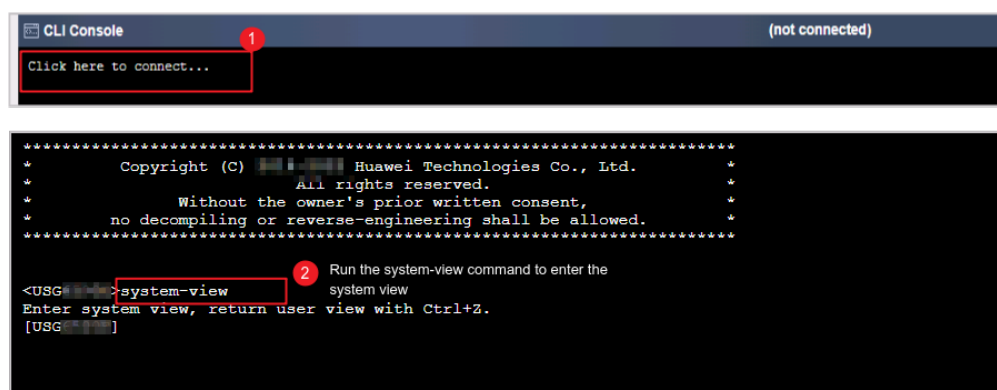
- In the lower right corner of any page, click **CLI Console**.

Figure 1-33 Security policy



- Perform the operations shown in the following figures to enter the system view.

Figure 1-34 Entering the system view



- Run the **ping** command to check whether the communication between the device and the gateway on the customer network is normal.  
**ping 10.1.1.254** //Use the actual gateway IP address instead of 10.1.1.254.  
If the gateway IP address cannot be pinged, check the network cable connection.
- Run the **ping** command to check whether the DNS server on the customer network properly resolves the IP address of the device.  
**ping mgt.seccloud.huawei.com** //Assume that the domain name used by the device to send registration requests to the security service platform is mgt.seccloud.huawei.com. Use the actual domain name of the target site during your operations.  
If the ping operation fails, run the **ping IP address of the DNS server** command to check whether the network communication between the device and the DNS server is normal.
- Run the **telnet** command to check whether the interface on the device for registering with the public network platform works properly.

**telnet mgt.seccloud.huawei.com 10020** Assume that the domain name used by the device to send registration requests to the security service platform is mgt.seccloud.huawei.com. Use the actual domain name of the target site during your operations.

If the command output contains SSH certificate exchange information, the interface works properly. If the interface is faulty, check whether port access restrictions are configured on the customer's security device.

## 1.1.10 Setting Service Parameters (Border Protection and Response Service)

### Context

You also need to set service parameters to ensure the normal running of the Border Protection and Response Service.

### Procedure

- Log in to the standard page at <https://192.168.0.1:8443/>.
- Verify that the security policies have been successfully delivered to the device.

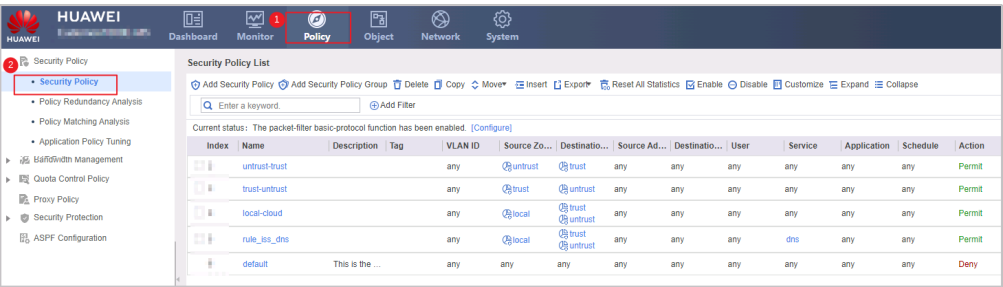
After the device is onboarded, the cloud platform deploys a related service package, which takes about 2 minutes. After the package is successfully deployed, security policies are automatically delivered to the device.

**Figure 1-35** shows the page after the security policies are delivered to the device. There are five security policies. The action of the **default** security policy is automatically changed to **Deny**.

#### NOTE

- If only **default** and **rule\_iss\_dns** security policies or only the **default** security policy exists on the device, the cloud platform automatically delivers other security policies to the device.
- If other security policies exist on the device, the cloud platform does not automatically deliver any security policy to the device. You need to configure required security policies on the device by referring to [1.2.1 How Do I Configure Security Policies Required by Border Protection and Response Service \(USG6000E Firewalls\)?](#) in the *FAQ*.

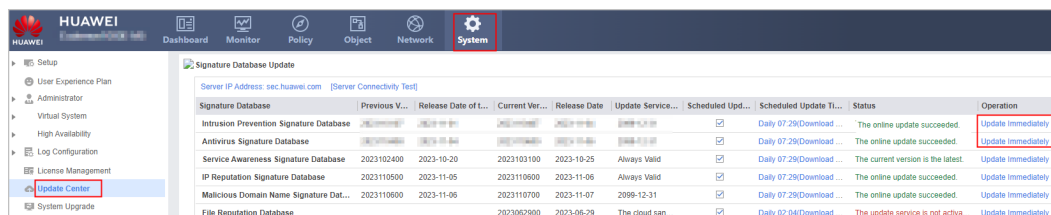
Figure 1-35 Security policy



Index	Name	Description	Tag	VLAN ID	Source Zone	Destination Zone	Source Address	Destination Address	User	Service	Application	Schedule	Action
1	untrust-trust			any	untrust	trust	any	any	any	any	any	any	Permit
2	trust-untrust			any	trust	untrust	any	any	any	any	any	any	Permit
3	local-cloud			any	local	trust	any	any	any	any	any	any	Permit
4	rule_iss_dns			any	local	trust	any	any	any	dns	any	any	Permit
5	default	This is the ...		any	any	untrust	any	any	any	any	any	any	Deny

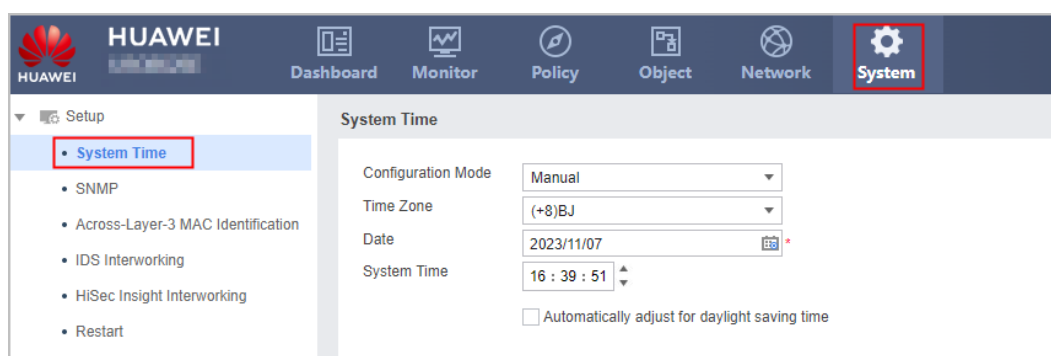
- Choose **System** > **Update Center** to check whether the online update of the IPS signature database and antivirus signature database is successful. The update takes about 10 minutes. If the update fails, click **Update Immediately**.

Figure 1-36 Update center



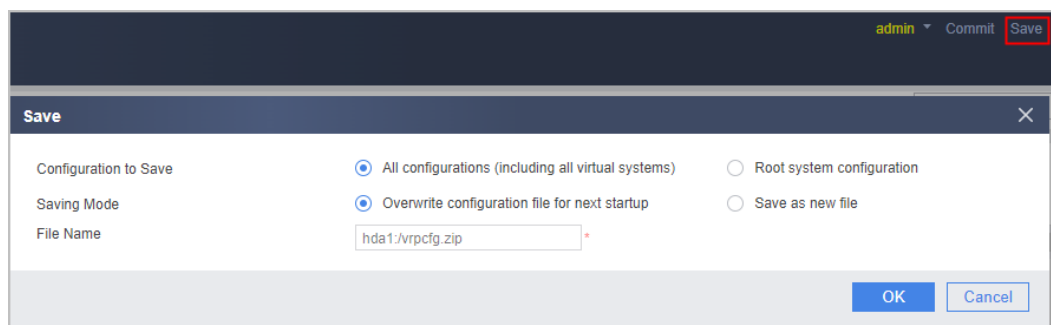
4. Choose **System** > **Setup** > **System Time** to check whether the device system time is consistent with the current time. If not, adjust the device system time to ensure that the cloud can accurately master the occurrence time of threat events.

Figure 1-37 System time



5. Click **Save** in the upper right corner. On the page that is displayed, click **OK** to save the configuration to prevent configuration loss after the device restarts.

Figure 1-38 Saving configurations



## 1.2 FAQ

### 1.2.1 How Do I Configure Security Policies Required by Border Protection and Response Service (USG6000E Firewalls)?

Perform the following steps:

1. Create the antivirus profile **AV\_default** and the IPS profile **IPS\_default**. Reference the created profiles when **configuring security policies required by services**.

- a. Choose **Object > Security Profiles > Antivirus**, create the antivirus profile **AV\_default** as shown in the following figure, and click **OK**.

**Figure 1-39** Creating an antivirus profile

**Add Antivirus Profile**

Name: AV\_default

Description:

Attack Evidence Collection: ☐ After detecting a virus, the system obtains packets containing the virus. You can view the packet payload in the corresponding log.

Protocol	File Transfer Protocol		Mail Transfer Protocol			File Sharing Protocol	
	HTTP	FTP	SMTP	POP3	IMAP ?	NFS ?	SMB ?
Upload	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Download	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Action	Block	Block	Alert	Alert	Alert	Alert	Block

**Application Exception List**

Select an application.

Name	Action
No data	

**Virus Exception List**

Enter a virus ID.

ID	Name
No data	

The system detects services at the application layer. If the services of an entered or selected application are transmitted through one of the specified protocols, the detection of that application is

The viruses in the virus exception list are not restricted by antivirus rules. To obtain virus IDs, refer to relevant logs.

- b. If the following prompt is displayed, select the check box as shown in the following figure, and click **OK**.

**Figure 1-40** Confirm

**Confirm**

2. This function may compromise the system performance. Exercise caution when you use this function.

3. The attack evidence information may occupy a large amount of system space. Ensure that the log storage device has sufficient space.

4. You are advised to disable this function after attack evidence collection is complete.

☒ I agree and am fully aware of possible risks.

- c. Choose **Object > Security Profile > Intrusion Prevention** and create the intrusion prevention profile **IPS\_default** as shown in the following figure.

**Figure 1-41** Creating an intrusion prevention profile

**Add Intrusion Prevention Profile**

Name:  \*

Description:

Attack Evidence Collection: ☒ This function collects packets containing a threat signature when a network threat is detected. The payloads of these packets can be viewed in the logs. You can use the attack evidence collection function if necessary.

Associated Detection: ☒ Associated detection detects brute force attacks. If IP address translation has been performed on traffic passing through the device, disable this function to prevent false positives.

Domain Name Checking: ☒ [\[Exceptions\]](#)

Action:

**Signature Filter List** | Signature Exception List | Protocol Anomaly Detection

☒ Add ☐ Delete ☐ View Results ☐ Move

Name	Target	Severity	OS	Applicat...	Protocol	Category	Action	Edit
No data								

OK Cancel

- d. Click **Add**, configure a signature filter for **IPS\_default** as shown in the following figure, and click **OK**.

**Figure 1-42** Configuring a signature filter

**Add Signature Filter**

Signature filtering can quickly obtain multiple required signatures. Signatures are filtered by attribute, such as object, severity, and protocol. If no filtering attributes are specified, all signatures are displayed.

Name:

Target: ☒ Server ☒ Client

Severity: ☒ High ☒ Medium ☒ Low ☐ Informational

OS: ☒ Windows ☒ Unix-like ☒ Android ☒ iOS ☒ Other

Application:

Protocol: ☒ all

Category: ☒ all

Action: ☒ Default ☐ Alert ☐ Block

- e. If the following prompt is displayed, select the check box as shown in the following figure, and click **OK**.

**Figure 1-43** Confirm

**Confirm**

2. This function may compromise the system performance. Exercise caution when you use this function.

3. The attack evidence information may occupy a large amount of system space. Ensure that the log storage device has sufficient space.

4. You are advised to disable this function after attack evidence collection is complete.

☒ I agree and am fully aware of possible risks.

- f. Click **Commit** in the upper right corner of the page to submit the security profiles for activation. The security profiles take effect only after being activated.

2. Configure security policies required by services.
  - a. Choose **Policy > Security Policy > Security Policy**, click **Add Security Policy**, and configure the security policies **untrust-trust**, **trust-untrust**, **local-cloud**, and **rule\_iss\_dns** in that sequence.
  - b. Configure the security policy **untrust-trust**. Set the source security zone to **untrust**, destination security zone to **trust**, antivirus profile to **AV\_default**, intrusion prevention profile to **IPS\_default**, and action to **Permit**.

**Figure 1-44** Configuring a security policy named untrust-trust

The screenshot shows the 'Add Security Policy' configuration window. The window has a sidebar on the left with sections: General Settings, Source and Destination, User and Service, Action, and Content Security. The main area contains the following fields:

Section	Field	Value	Notes
General Settings	Name	untrust-trust	
	Description		
	Policy Group	-- NONE --	
	Tag	Select or enter a tag.	
Source and Destination	Source Zone	untrust	[Multiple]
	Destination Zone	trust	[Multiple]
	Source Address/Region	Select or enter an address.	
	Destination Address/Region	Select or enter an address.	
	VLAN ID	Enter a VLAN ID.	<1-4094>
User and Service	User	Select or enter a user name.	[Multiple]
	Access Mode	Select an access mode.	
	Device	Select or enter a device.	
	Service	Select or enter a service.	
	Application	Select or enter an application.	[Multiple]
	URL Category	Select or enter a url category.	[Multiple]
Action	Schedule	Select a time range.	
	Action	<input checked="" type="radio"/> Permit <input type="radio"/> Deny	
Content Security	Antivirus	AV_default	[Configure]
	Intrusion Prevention	IPS_default	[Configure]
	URL Filtering	-- NONE --	[Configure]
	File Blocking	-- NONE --	[Configure]
	Data Filtering	-- NONE --	[Configure]
	Application Behavior Control	-- NONE --	[Configure]
	Cloud Access Security Awareness	-- NONE --	[Configure]
	Email Filtering	-- NONE --	[Configure]
	APT Defense	-- NONE --	[Configure]

- c. Configure the security policy **trust-untrust**. Set the source security zone to **trust**, destination security zone to **untrust**, antivirus profile to **AV\_default**, intrusion prevention profile to **IPS\_default**, and action to **Permit**.

Figure 1-45 Configuring a security policy named trust-untrust

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination?

General Settings

Name

trust-untrust

Description

Policy Group

-- NONE --

Tag

Select or enter a tag.

Source and Destination

Source Zone

trust

Destination Zone

untrust

Source Address/Region?

Select or enter an address.

Destination Address/Region?

Select or enter an address.

VLAN ID

Enter a VLAN ID.

<1-4094>

User and Service

User?

Select or enter a user name.

Access Mode?

Select an access mode.

Device?

Select or enter a device.

Service?

Select or enter a service.

Application

Select or enter an application.

URL Category

Select or enter a url category.

Schedule

Select a time range.

Action

Action

Permit

Deny

Content Security

Antivirus

AV\_default

Intrusion Prevention

IPS\_default

URL Filtering

-- NONE --

File Blocking

-- NONE --

Data Filtering

-- NONE --

Application Behavior Control

-- NONE --

Cloud Access Security Awareness

-- NONE --

- d. Configure the security policy **local-cloud**. Set the source security zone to **local**, destination security zones to **trust** and **untrust**, service to **any**, and action to **Permit**.

Figure 1-46 Configuring security policy named local-cloud

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [\[Select Template\]](#) [Switch Source and Destination?](#)

General Settings

Name

local-cloud

Description

Policy Group

-- NONE --

Tag

Select or enter a tag.

Source and Destination

Source Zone

local

Destination Zone

untrust,trust

Source Address/Region

Select or enter an address.

Destination Address/Region

Select or enter an address.

VLAN ID

Enter a VLAN ID.

User and Service

User

Select or enter a user name.

Access Mode

Select an access mode.

Device

Select or enter a device.

Service

any

Application

Select or enter an application.

URL Category

Select or enter a url category.

Schedule

Select a time range.

Action

Action

Permit

Deny

Content Security

Antivirus

-- NONE --

Intrusion Prevention

-- NONE --

URL Filtering

-- NONE --

File Blocking

-- NONE --

Data Filtering

-- NONE --

Application Behavior Control

-- NONE --

Cloud Access Security Awareness

-- NONE --

Email Filtering

-- NONE --

APT Defense

-- NONE --

- e. Configure the security policy **rule\_iss\_dns**. Set the source security zone to **local**, destination security zones to **trust** and **untrust**, service to **dns**, and action to **Permit**.

Figure 1-47 Configuring a security policy named rule\_iss\_dns

Add Security Policy

Note: You can use a policy template to quickly define the required policy. [Select Template] Switch Source and Destination?

General Settings

Name

rule\_iss\_dns

Description

Policy Group

-- NONE --

Tag

Select or enter a tag.

Source and Destination

Source Zone

local

Destination Zone

trust,untrust

Source Address/Region?

Select or enter an address.

Destination Address/Region?

Select or enter an address.

VLAN ID

Enter a VLAN ID.

<1-4094>

User and Service

User?

Select or enter a user name.

Access Mode?

Select an access mode.

Device?

Select or enter a device.

Service?

dns

Application

Select or enter an application.

URL Category

Select or enter a url category.

Schedule

Select a time range.

Action

Action

Permit

Deny

Content Security

Antivirus

-- NONE --

Intrusion Prevention

-- NONE --

URL Filtering

-- NONE --

File Blocking

-- NONE --

Data Filtering

-- NONE --

Application Behavior Control

-- NONE --

Cloud Access Security

-- NONE --

# 2 Border Protection and Response

---

[2.1 Service Overview](#)

[2.2 Purchase Guide](#)

[2.3 Device Provisioning Guide](#)

[2.4 User Guide](#)

## 2.1 Service Overview

### 2.1.1 What Is the Border Protection and Response Service?

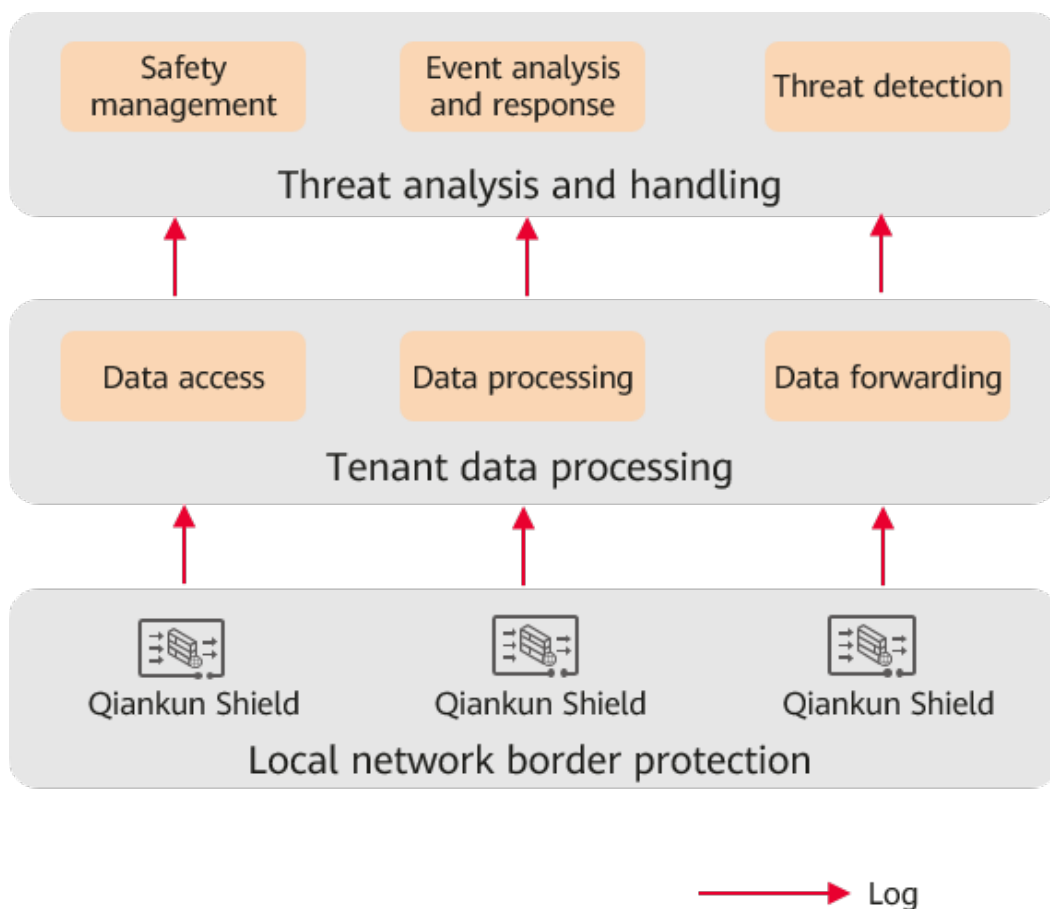
The Border Protection and Response Service uses Qiankun Shield devices to provide border protection for tenants' local networks. It also performs intelligent analysis and handling based on logs provided by Qiankun Shield devices, ensuring the enterprise intranet security. Huawei Qiankun integrates detection models, such as alarm-based automatic confirmation and threat analysis, to intelligently identify potential threats on tenants' local networks and automatically handle these threats. In this way, tenants can benefit from simplified local O&M and improved security protection.

#### Logical Architecture

As shown in [Figure 2-1](#), the Border Protection and Response Service is implemented in three stages.

- **Local network border protection:** Qiankun Shield devices deployed at the tenant network border ensure the security of the local network border with functions such as intrusion prevention, antivirus, and DNS filtering.
- **Tenant data processing:** The data access center of Huawei Qiankun processes logs from Qiankun Shield devices and persistently stores service data.
- **Threat analysis and handling:** After obtaining service data, the threat analysis and handling center of Huawei Qiankun completes automatic analysis and security response through threat detection, event analysis and response, and security management. [Figure 2-2](#) shows the analysis procedure.

**Figure 2-1** Logical architecture



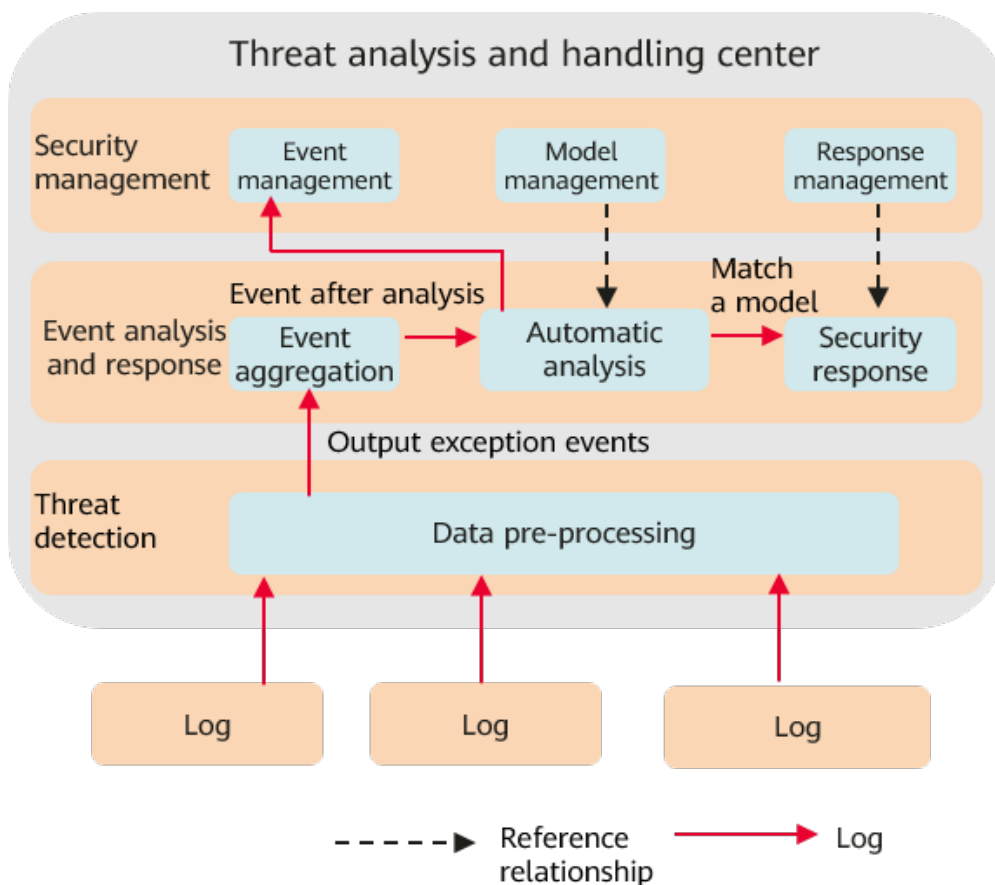
## Threat Analysis and Handling

As shown in [Figure 2-2](#), after obtaining service data, the threat analysis and handling center completes automatic analysis and security response through threat detection, event analysis and response, and security management.

- **Threat detection:** preprocesses the format and fields of the obtained logs and then outputs abnormal events.
- **Event analysis and response:** performs aggregation analysis, automatic analysis, and security response on output abnormal events, in that order. Output abnormal events are aggregated and analyzed based on the corresponding aggregation policy. Then, the aggregated events are automatically analyzed and determined based on the automatic analysis model. The security response automatically responds to the events that match the analysis model. Based on automatic analysis, security experts further analyze and handle the analyzed events (including matched and unmatched events).
- **Security management:** provides security experts of Huawei Qiankun with visualized event portals, manual event handling capabilities, routine management capabilities, and security response management capabilities. Security experts can check events after automatic analysis through event management, configure and adjust automatic analysis models in a timely

manner through model management, and perform routine maintenance of blacklists and whitelists through response management.

**Figure 2-2** Threat analysis and handling



## 2.1.2 Functions

### Local Network Border Protection

Qiankun Shield devices are deployed at the tenant network border to ensure local security with technologies such as intrusion prevention, antivirus, and DNS filtering. After tenants subscribe to the Border Protection and Response Service, Qiankun Shield devices can:

- Perform intrusion prevention detection on traffic to comprehensively defend against various intrusion behaviors.
- Perform antivirus on traffic to effectively prevent data damage, permission change, and system breakdown caused by virus files.
- Perform DNS filtering on traffic to comprehensively control domain name access.

### Tenant Data Security Processing

- Data authorization: After being authorized by users, local Qiankun Shield devices send data only within the authorization scope.

- Encrypted transmission: Local Qiankun Shield devices transmit logs to the cloud service platform through Hypertext Transfer Protocol Secure (HTTPS) or Transport Layer Security (TLS).
- Encrypted storage: Data is encrypted using the encryption component of the Huawei key management center (KMC), and then stored on Huawei Qiankun.
- Handling principle: Data is used only for threat analysis and tracing by operation experts of the cloud service platform.
- Information isolation: Each user receives analysis reports and SMS messages through their own service account. Information is only sent to relevant users.

## Automatic Analysis

Huawei Qiankun can analyze and determine threat events based on analysis models and handle the events based on the determination results. Drawing on the strengths of automatic analysis capabilities and security experts of Huawei Qiankun, tenants can benefit from simplified local O&M and enhanced protection efficiency.

After automatic analysis, the following handling methods are available:

- If an event matches the false positive model, the event status changes to false positive.
- If an event matches an alarm-based automatic confirmation model or a threat analysis model, automatic analysis will request the security response to perform the corresponding processing.
- Security experts can refer to the automatic analysis results to further analyze and handle the events.

## Security Response

Security response is a closed-loop response to security events. It includes two security response actions: delivering blacklists and sending alarms. Tenants can leverage the security response capabilities of Huawei Qiankun to significantly improve the efficiency of closed-loop responses to security events.

Security response provides the two security response actions in the following scenarios:

- For events that can be automatically handled after automatic analysis, the automatic analysis requests security response to deliver a blacklist or send an alarm.
- For events that need to be handled by security experts after automatic analysis, security experts can manually deliver a blacklist or send an alarm through the event management menu on the portal.
- A tenant delivers a blacklist on the tenant portal.

## Precise Analysis by Security Experts

Security experts of Huawei Qiankun integrate security capabilities to quickly and accurately identify sophisticated threats.

- Security capabilities of Huawei Qiankun are continuously enhanced by consolidating live-network confrontation experience into Huawei Qiankun.

- Latest vulnerability analysis and intelligent signature production of Huawei Qiankun help quickly cope with new threats.
- Security experts analyze each discovered security alarm in a unified manner and use various security capabilities of Huawei Qiankun to resolve the latest threats.

## 2.1.3 Product Highlights

### Cross-Service Association

The detection results can be dumped to Object Storage Service (OBS) to meet compliance requirements, and synchronized to the Situation Awareness (SA) service for visualized operations.

### Accurate Threat Identification

Based on intelligent analysis models such as false positive model, alarm-based automatic confirmation model, and threat analysis model, as well as Huawei Qiankun security experts' experience on the live network, the service performs correlation analysis on the data to quickly and accurately discover threats.

### Automatic Threat Response

Threat events are automatically handled after being detected using security response actions: delivering blacklists and sending alarms. Users are then notified through SMS messages and emails. This improves the efficiency of closed-loop responses to threat events.

## 2.1.4 Application Scenarios

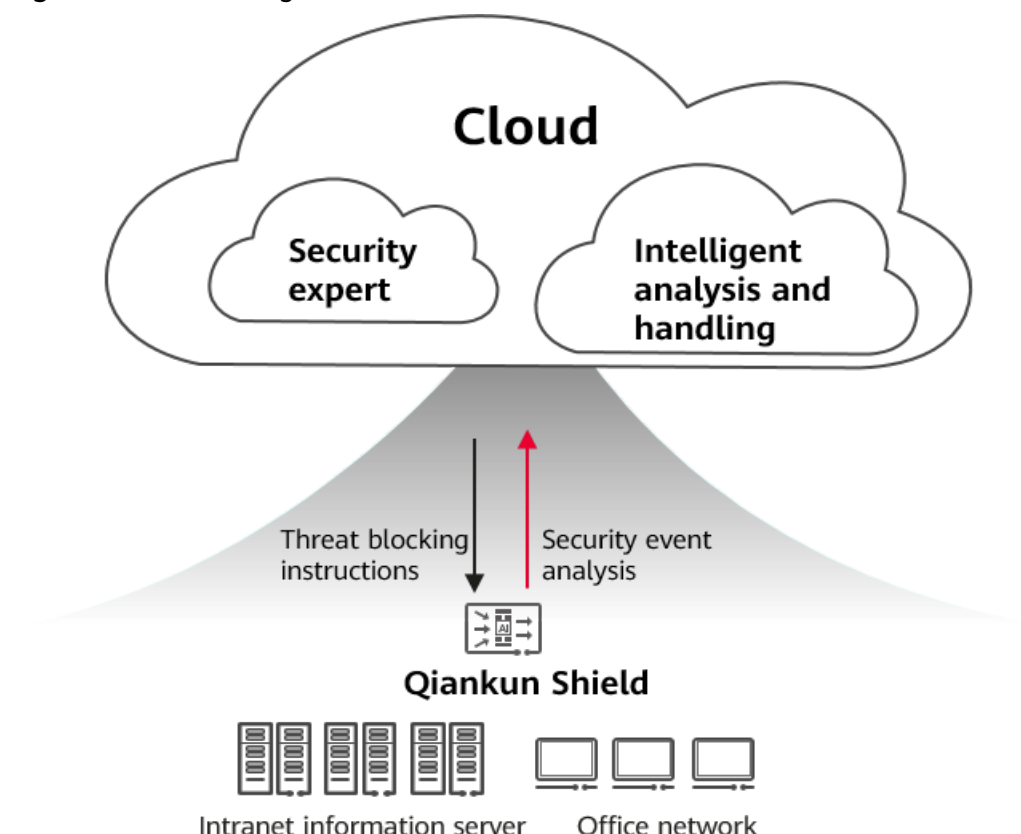
### Internet Egress of SMEs

Typically, small and medium-sized enterprises (SMEs) have very small or no security budgets. They often have no dedicated network security owners, and cannot afford on-site services. Even if basic security devices are purchased, results are poor as there is a lack of professional security O&M personnel. For these reasons, SMEs tend to have almost no security protection. Even a common virus may compromise the entire information system of an SME. With network attacks increasingly prevalent, routine service operations are often severely affected. This has made network security construction vital for SMEs.

Main security construction requirements of SMEs:

- There is no workforce for security O&M. This deters SMEs from purchasing multiple types of security devices.
- The security budget is very limited, and on-site services are unaffordable. SMEs prefer to outsource the network security construction to obtain basic security capabilities. In this way, the internal network can communicate with the external network without affecting routine service operations.

**Figure 2-3** Internet egress of SMEs



Functions implemented by the Border Protection and Response Service:

- Only one Qiankun Shield device needs to be deployed at the egress of the enterprise network. Huawei Qiankun automatically delivers intrusion prevention and antivirus capabilities to the Qiankun Shield devices to effectively block external network threats and prevent virus-infected files from spreading. In addition, the internal and external networks can communicate with each other without affecting routine service operations.
- With only minimal investment, SMEs can purchase cloud service security capabilities, obtain security expert services and intelligent threat handling capabilities, and outsource network security construction to Huawei Qiankun, greatly reducing local O&M workload.

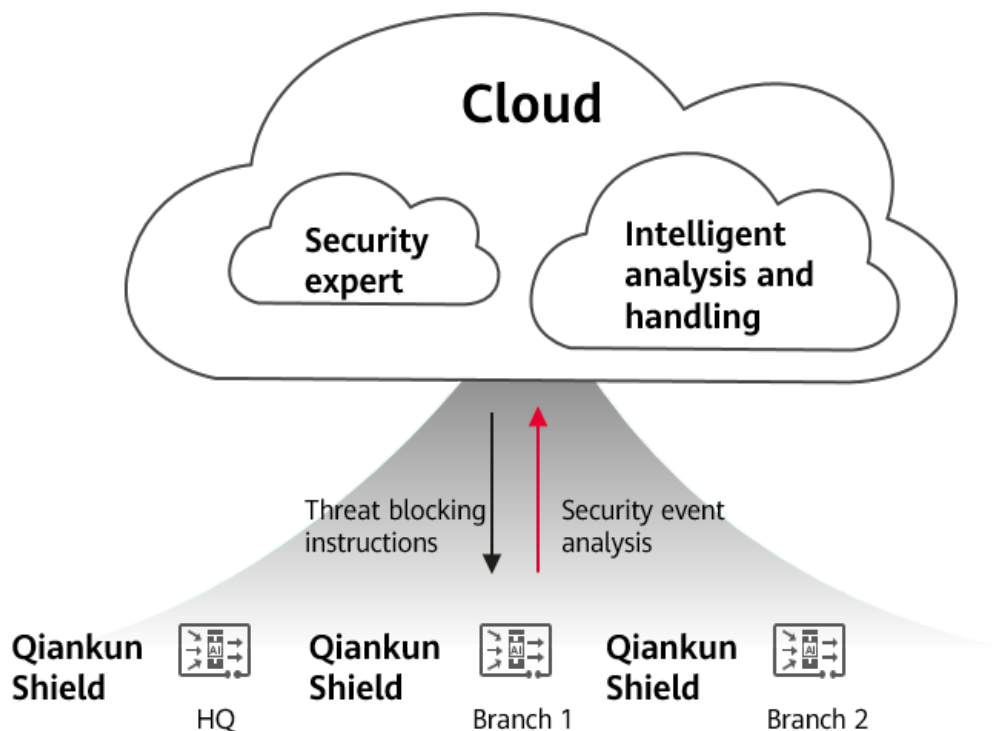
## Multi-branch Interconnection of Large Enterprises

Large enterprises usually provide services across a country, with branches distributed in multiple regions. These branches frequently communicate with each other. Typically, such enterprises have small-scale network security departments at the headquarters. These security departments mainly depend on security vendors or integrators for security construction, and purchase on-site services from vendors or service providers. Due to limited capabilities of on-site service personnel, lack of dedicated security O&M personnel in branches, and frequent transmission of Internet data between branches, the overall security posture of such enterprises is poor and they are vulnerable to all kinds of attacks; even those launched by common hackers.

Main security construction requirements of large enterprises:

- Simplified local O&M: Due to limited budgets for security O&M, security O&M personnel cannot be dispatched to each branch and on-site services cannot be purchased for each branch. Even if on-site services are purchased, robust security cannot be achieved due to limited capabilities of on-site service personnel.
- Unified protection: The solution covers all branch networks and analyzes security events of the entire enterprise. It also responds to threats in a unified manner and blocks threats in time. In addition, the headquarters can be informed of the security posture of each branch in a timely manner.

**Figure 2-4** Multi-branch interconnection of large enterprises



Functions implemented by the Border Protection and Response Service:

- The intelligent analysis and handling capabilities of Huawei Qiankun improve automatic O&M efficiency and automatically block threats. Security experts of Huawei Qiankun provide 24/7 online services to resolve complex network security issues and simplify local O&M.
- One Qiankun Shield device is deployed at the Internet border of each branch to act as the security protection node. The device works with security services of Huawei Qiankun to implement unified protection for all branch networks.
- Based on the overall analysis of security events through Huawei Qiankun, the system automatically responds to and blocks threats in a timely manner, and sends security alarms to the security administrators at the headquarters by email. The security administrators can then respond to emergencies and deal with serious host compromise events. The security administrators at the headquarters use the weekly and monthly reports provided by the global

security service to get an understanding of the overall network security posture and the network security status of the entire enterprise.

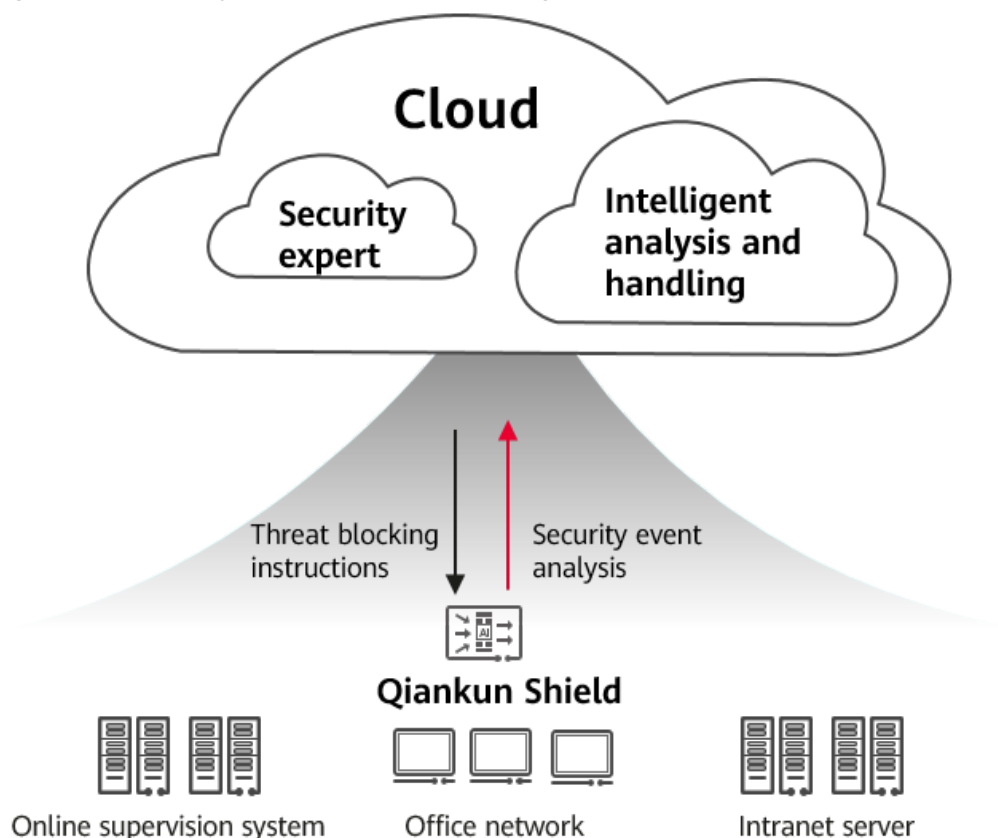
## Security Construction and Management for Some Industries

In industries such as government, healthcare, and education, upper-level administrative departments place stringent network security requirements on subordinates. However, subordinates are unable to implement comprehensive network security construction due to tight security budgets and sub-par technical capabilities. What is worse, the upper-level departments cannot effectively manage whether the network security requirements are met. They also lack a means of urging subordinates to swiftly rectify the items that fail to meet the requirements.

Main security construction requirements of such departments:

- Subordinates meet the network security requirements of upper-level departments, in spite of limited budgets.
- The upper-level departments can effectively manage the subordinates and urge them to swiftly rectify items that do not meet the requirements.

**Figure 2-5** Security construction and management for some industries



Functions implemented by the Border Protection and Response Service:

- With only minimal investment, customers can purchase cloud service security capabilities and obtain security expert services and intelligent handling capabilities.

- Huawei Qiankun is used to analyze and respond to threat events in a unified manner, and block them in time. On top of this, security experts of Huawei Qiankun help solve difficult problems, making up for insufficient technical capabilities of subordinates.
- When sending security alarms and email reports to subordinates, Huawei Qiankun also sends global security detection reports to upper-level departments to comprehensively display the security posture of subordinates and whether security events are handled in a timely manner, implementing effective and timely management of subordinates.

## 2.2 Purchase Guide

### 2.2.1 Activating the Commercial Service

#### 2.2.1.1 Activating the Service Using a Tenant Account

##### 2.2.1.1.1 Registering a Huawei Qiankun Account

###### NOTE

- Huawei Qiankun can be used on the Huawei Qiankun console. Before login, you need to register a Huawei Qiankun account.
- If you have a tenant account created by Huawei Qiankun managed service provider (MSP), skip this section.

**Step 1** Access the Huawei Qiankun console.

**Step 2** Click **Sign Up** on the login page.

Register an account as prompted.

----End

##### 2.2.1.1.2 Activating the Service Package

###### Context

After purchasing the cloud service license offline, you need to activate the offline order on Huawei Qiankun. [Table 2-1](#) lists the device models that can work in conjunction with this service.

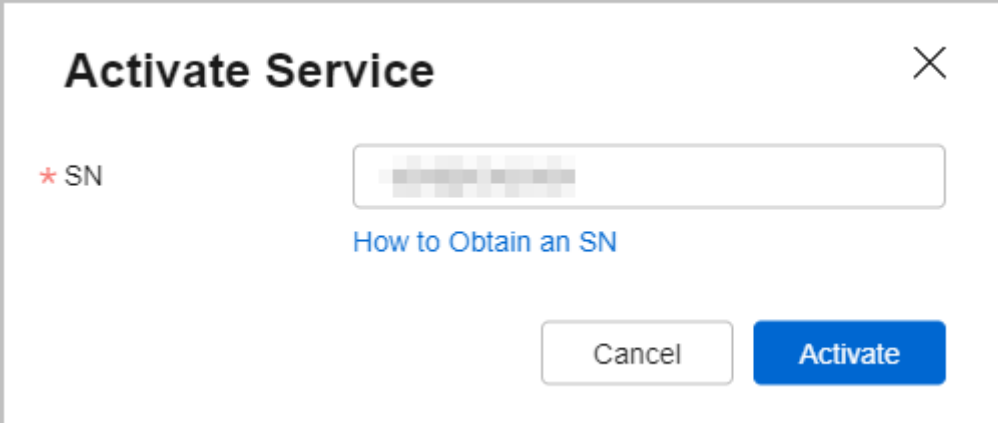
**Table 2-1** Device models

Device Model	Activation Mode
USG6530E/USG6585E	For details, see <a href="#">Procedure</a> .

## Procedure

1. Log in to the Huawei Qiankun console using a tenant account.
2. Click **Orders** in the menu bar, and then click the **My Packages** tab.
3. Click **Activate Service**, and then select **Activate by SN**. On the **Activate Service** page, enter the device SN and click **Activate**.

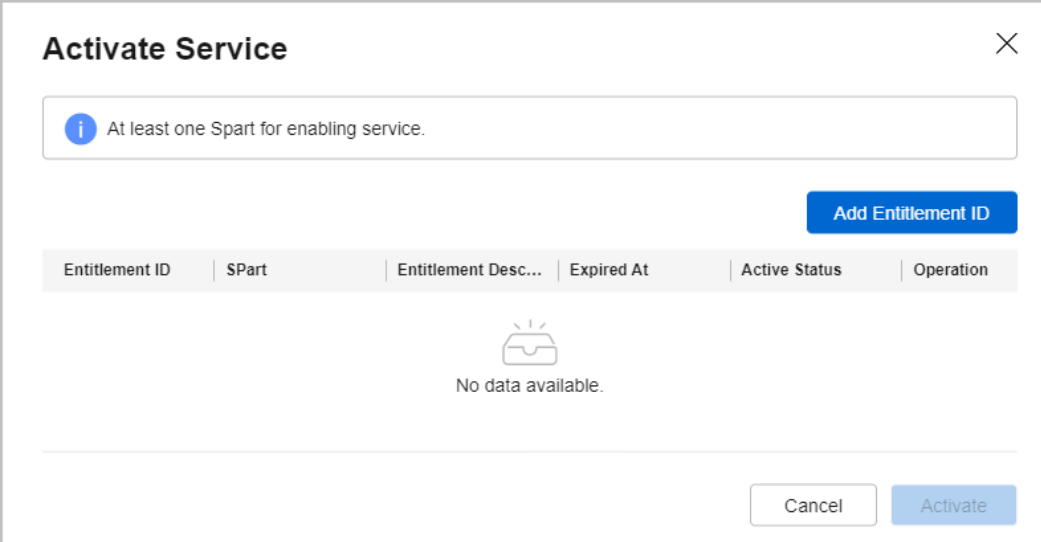
Figure 2-6 Entering an SN



The screenshot shows a modal window titled "Activate Service" with a close button (X) in the top right corner. Inside the window, there is a label "★ SN" followed by a text input field containing a blurred device serial number. Below the input field is a blue link that says "How to Obtain an SN". At the bottom right of the window are two buttons: a light gray "Cancel" button and a blue "Activate" button.

4. (Optional) On the **Activate Service** page, click **Add Entitlement ID**.  
If Huawei engineers have activated the license in the ESDP system, the activated entitlement ID is displayed on this page. In this case, skip this step.

Figure 2-7 Activate Service

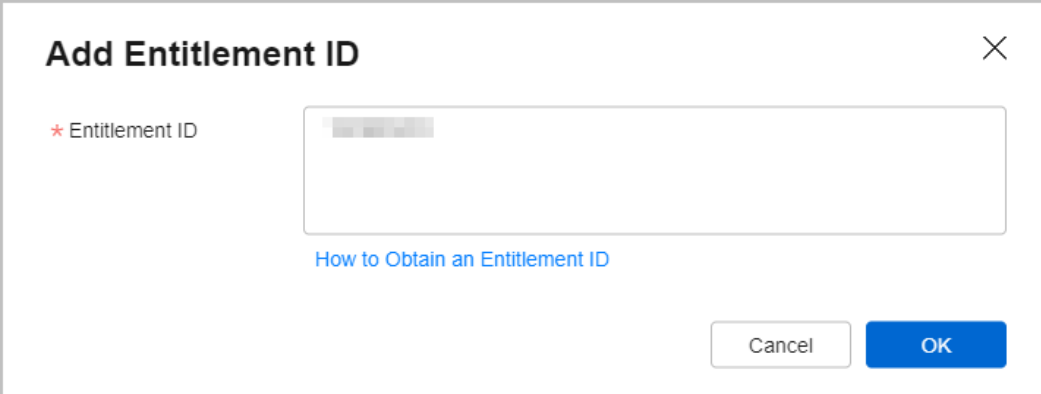


The screenshot shows the "Activate Service" modal window. At the top, there is an information icon (i) and a message: "At least one SPart for enabling service." Below this message is a blue button labeled "Add Entitlement ID". Underneath the button is a table with the following headers: "Entitlement ID", "SPart", "Entitlement Desc...", "Expired At", "Active Status", and "Operation". The table body is empty, and below it is a message "No data available." with a small icon of a document with a checkmark. At the bottom right of the window are "Cancel" and "Activate" buttons.

5. On the **Add Entitlement ID** page, enter the entitlement IDs as prompted and click **OK**.  
If Huawei engineers have activated the license in the ESDP system, skip this step.  
If the license is not activated, you need to add entitlement IDs. Entitlement IDs related to the Border Protection and Response Service include the standard edition entitlement ID, professional edition entitlement ID,

automatic threat blocking entitlement ID, and threat protection database update entitlement ID. Set this parameter based on the actual entitlement ID.

**Figure 2-8** Add Entitlement ID

A dialog box titled "Add Entitlement ID" with a close button (X) in the top right corner. It contains a label "Entitlement ID" with a red asterisk, followed by a text input field. Below the input field is a blue link "How to Obtain an Entitlement ID". At the bottom right are "Cancel" and "OK" buttons.

**Add Entitlement ID**

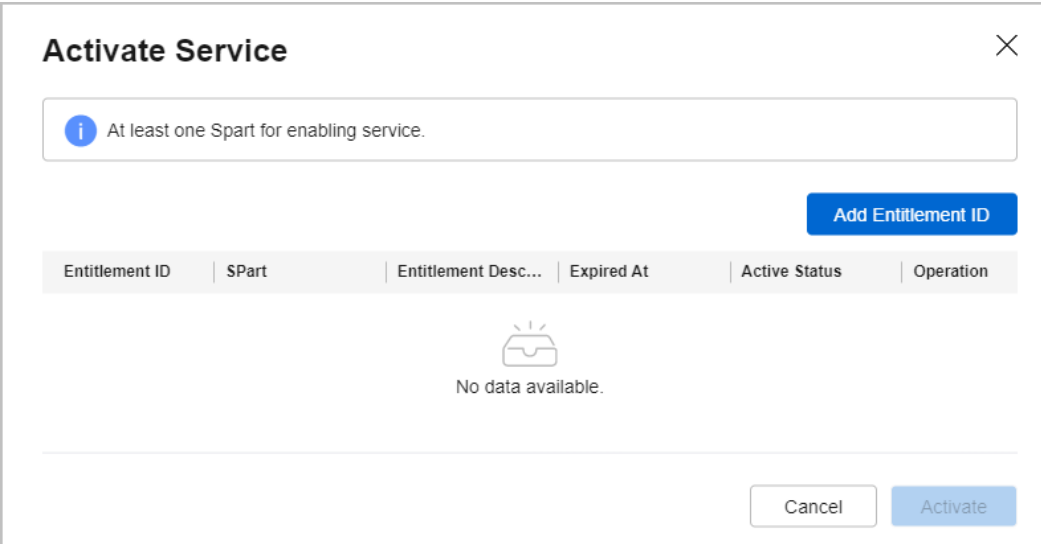
\* Entitlement ID

How to Obtain an Entitlement ID

Cancel OK

6. On the **Activate Service** page, click **Activate**.

**Figure 2-9** Activate Service

A dialog box titled "Activate Service" with a close button (X) in the top right corner. It contains an information icon and the text "At least one SPart for enabling service." Below this is a blue button "Add Entitlement ID". Underneath is a table header with columns: "Entitlement ID", "SPart", "Entitlement Desc...", "Expired At", "Active Status", and "Operation". Below the header is a message "No data available." with a folder icon. At the bottom right are "Cancel" and "Activate" buttons.

**Activate Service**

At least one SPart for enabling service.

Add Entitlement ID

Entitlement ID	SPart	Entitlement Desc...	Expired At	Active Status	Operation
No data available.					

Cancel Activate

7. After the service is activated, choose **Resources Center > Device Management > Devices** in the menu bar. On the page that is displayed, you can see that the device is in unregistered state.

## 2.2.1.2 Activating the Service Using an MSP Account

### 2.2.1.2.1 Registering a Tenant Account by MSP

#### Procedure

- Step 1** Log in to the Huawei Qiankun console using an MSP account.
- Step 2** Click **Tenants** in the upper right corner of the console. The **Managed Tenants** page is displayed.

**Step 3** 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 2-10** 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 all 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. Set tenant administrator information and click **Finish**.

**Figure 2-11** Configuring self-created tenant administrator information

The screenshot shows the 'Create Tenant' interface. At the top, there are two steps: '1 Tenant Info' and '2 Tenant Admin Info'. The 'Tenant Admin Info' section is active. It contains the following fields:

- \* Tenant Admin Name:** A text input field with the value 'user\_admin'.
- \* Password Mode:** Two radio buttons. 'Password Authentication' is selected, and 'SMS Authentication' is unselected.
- \* Password:** A password input field with masked characters '.....' and a toggle icon.
- \* Confirm Password:** A password input field with masked characters '.....' and a toggle icon.
- Phone Number:** A dropdown menu showing 'China +86' and a text input field with the placeholder 'Enter a phone number.'
- Email Address:** A text input field with the placeholder 'Enter an email address.'
- Description:** A large text area for additional information.

----End

## 2.2.1.2.2 MSP-Entrusted Management

### Context

You can entrust your services to a desired MSP to reduce the OPEX of your enterprise.

### Procedure

- Step 1** Log in to the Huawei Qiankun console using a tenant account.
- Step 2** Click your account in the upper right corner, and choose **Agencies**.
- Step 3** Click **Create** and set parameters based on the **Agency parameters**.

Figure 2-12 MSP-entrusted page

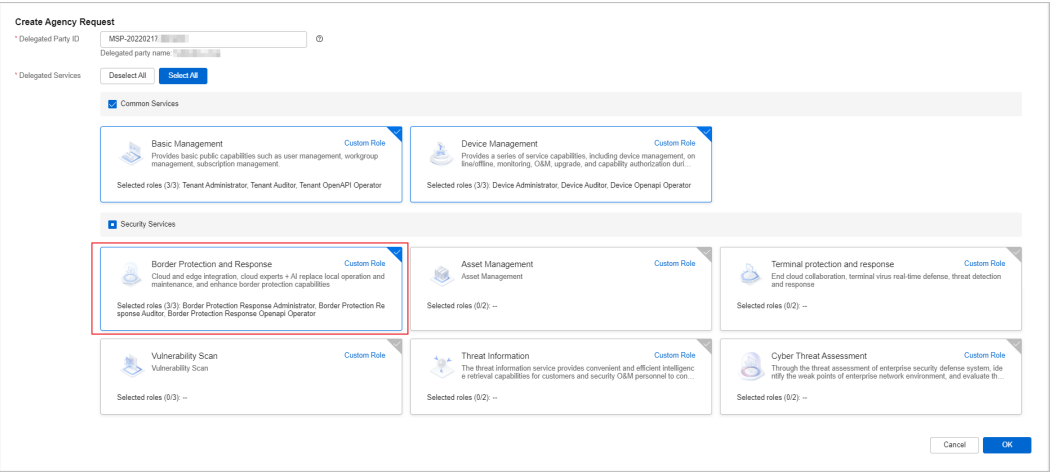


Table 2-2 Agency parameters

Parameter	Description
Delegated Party ID	<ul style="list-style-type: none"><li>• If the current tenant account is created by an MSP, the MSP ID is displayed automatically by default.</li><li>• If the current tenant account is self-registered, obtain the unique ID (unique ID on the right of the MSP account page) from the delegated MSP.</li></ul>
Delegated Services	<p>List of services and the corresponding execution permissions that can be entrusted to the MSP.</p> <ul style="list-style-type: none"><li>• When <b>Border Protection Response Administrator</b> is selected, the MSP has operation permissions on services.</li><li>• When <b>Border Protection Response Auditor</b> is selected, the MSP has only the permission to check services.</li><li>• When <b>Border Protection Response Open api Operator</b> is selected, the MSP has the permission to use the API service.</li></ul> <p>By default, all roles are selected. You can click <b>Custom Role</b> on the service card to select the delegated roles.</p>
Agency Expiration Time	Agency expiration time, after which the agency automatically ends.
Description	Agency description which will be displayed in the approval process of the MSP.

Step 4 Click **OK**.

Step 5 In the **Confirm Agency Information** dialog box, read the risks, select **I have read and agree to Agency Authorization Agreement and understand the risks of performing this operation**, and click **OK**.

After the MSP approves the agency request, an agency relationship is established between the tenant and MSP.

----End

### 2.2.1.2.3 Activating the Service Package

#### Context

After purchasing the cloud service license offline, you need to activate the offline order on Huawei Qiankun. [Table 2-3](#) lists the device models that can work in conjunction with this service.

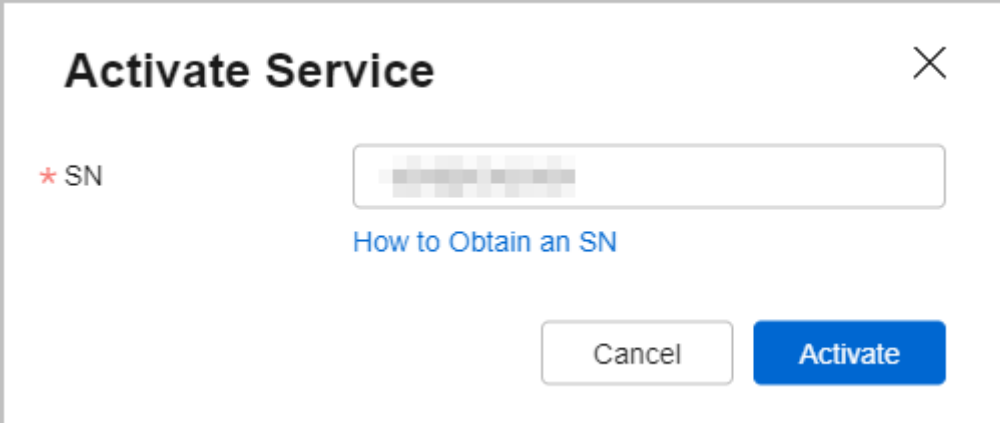
**Table 2-3** Device models

Device Model	Activation Mode
USG6530E/USG6585E	For details, see <a href="#">Procedure</a> .

#### Procedure

1. Log in to the Huawei Qiankun console using a tenant account.
2. Click **Orders** in the menu bar, and then click the **My Packages** tab.
3. Click **Activate Service**, and then select **Activate by SN**. On the **Activate Service** page, enter the device SN and click **Activate**.

**Figure 2-13** Entering an SN



4. (Optional) On the **Activate Service** page, click **Add Entitlement ID**.  
If Huawei engineers have activated the license in the ESDP system, the activated entitlement ID is displayed on this page. In this case, skip this step.

**Figure 2-14** Activate Service

**Activate Service**

At least one SPart for enabling service.

Add Entitlement ID

Entitlement ID	SPart	Entitlement Desc...	Expired At	Active Status	Operation
No data available.					

Cancel Activate

- On the **Add Entitlement ID** page, enter the entitlement IDs as prompted and click **OK**.

If Huawei engineers have activated the license in the ESDP system, skip this step.

If the license is not activated, you need to add entitlement IDs. Entitlement IDs related to the Border Protection and Response Service include the standard edition entitlement ID, professional edition entitlement ID, automatic threat blocking entitlement ID, and threat protection database update entitlement ID. Set this parameter based on the actual entitlement ID.

**Figure 2-15** Add Entitlement ID

**Add Entitlement ID**

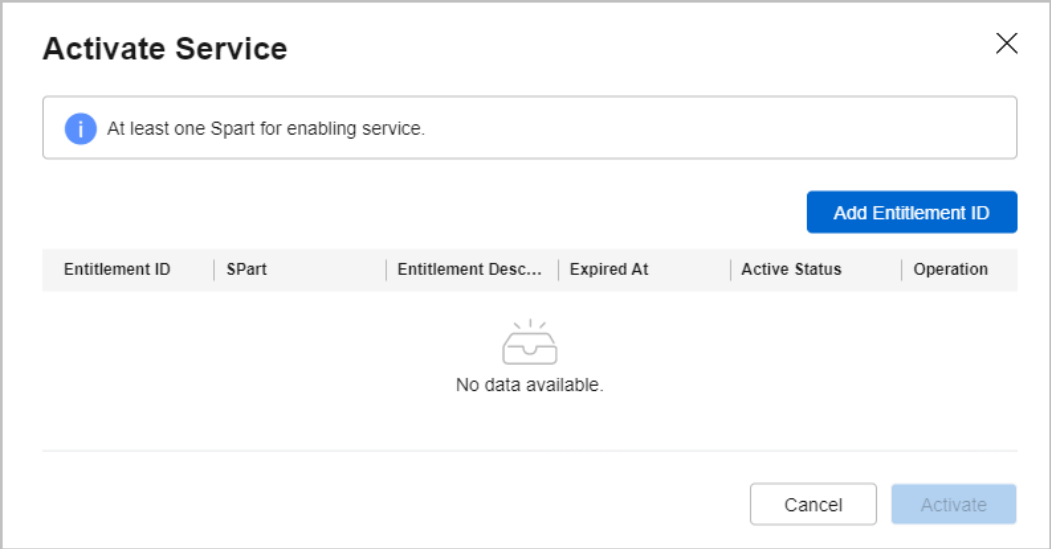
★ Entitlement ID

How to Obtain an Entitlement ID

Cancel OK

- On the **Activate Service** page, click **Activate**.

Figure 2-16 Activate Service



7. After the service is activated, choose **Resources Center > Device Management > Devices** in the menu bar. On the page that is displayed, you can see that the device is in unregistered state.

2.3 Device Provisioning Guide

2.3.1 Configuring Device Onboarding

The border protection and response service can be used only after required devices are deployed on the customer side. [Table 2-4](#) lists the Qiankun Shield models that can work in conjunction with this service.

Table 2-4 Device Model

Device Model	Supported Version	Onboarding Guide
USG6530E/USG6585E	V600R007C20SPC605 and later	<a href="#">Onboarding the USG6000E Series Firewalls</a>

2.3.2 Configuring Device Security Zones

Context

Huawei Qiankun needs to identify the security zones to which the attack source and destination belong for threat event analysis.

Huawei Qiankun provides the following types of security zones:

- User-trusted Zone:** It is a security zone trusted by users. It usually refers to users' internal networks. Huawei Qiankun does not block the **threat traffic** initiated from this zone.

- **Mixed Zone:** It is a special security zone between **User-trusted Zone** and **User-untrusted Zone** in terms of trust level. Huawei Qiankun does not block the **threat traffic** initiated from this zone.
- **User-untrusted Zone:** It is a security zone not trusted by users. It usually defines insecure networks such as the Internet. Huawei Qiankun automatically blocks the **threat traffic** initiated from this zone.

## Procedure


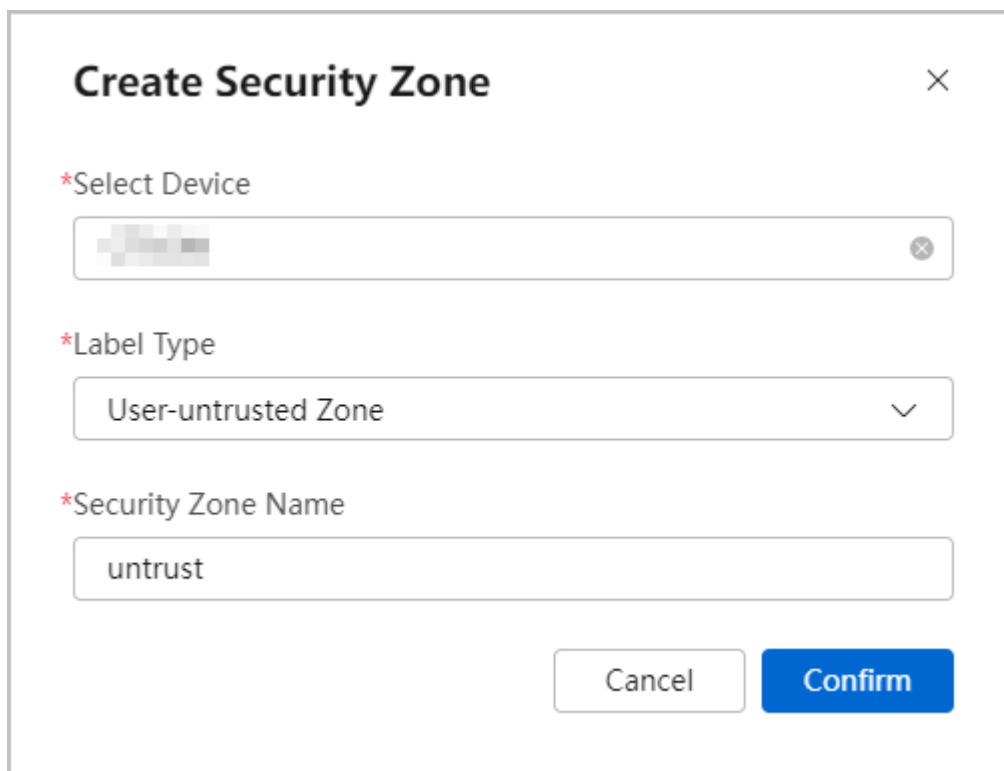
- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Choose **Services** > **IP Security Zone**.
- Step 3** Click **Create** in the **Device Security Zone** area, and add the untrust zone to **User-untrusted Zone**.

Figure 2-17 Creating a security zone



The image shows a 'Create Security Zone' dialog box with a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk:

- \*Select Device:** A text input field with a blurred placeholder and a clear button (X) on the right.
- \*Label Type:** A dropdown menu currently showing 'User-untrusted Zone' with a downward arrow on the right.
- \*Security Zone Name:** A text input field containing the text 'untrust'.

At the bottom right, there are two buttons: a 'Cancel' button and a blue 'Confirm' button.

- Step 4** (Optional) Add the **trust** zone to **User-trusted Zone**. By default, the **trust** zone has been added to **User-trusted Zone** on Huawei Qiankun. If the **trust** zone is deleted, perform this step to add it.

Figure 2-18 Creating a security zone

Create Security Zone

\*Select Device

\*Label Type

User-trusted Zone

\*Security Zone Name

trust

Cancel

Confirm

After the security zones are added, the following page is displayed.

Figure 2-19 Device security zones

User-trusted Zone(1)  
trust

Mixed Zone

User-untrusted Zone(1)  
untrust


----End

## 2.3.3 Creating Global Whitelists

### Context


You can add IP addresses of all intranet assets and address segments that provide external services to the global whitelists to prevent blacklists containing the preceding IP addresses from being delivered by Huawei Qiankun automatically and by Huawei Qiankun security service personnel.

### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Choose **Services > IP Security Zone**.
- Step 3** Create global whitelists from **Global Address Management > Global Whitelist**.

**Figure 2-20** Creating a global whitelist

### Create Global Allowlist ×

 The global allowlist of a tenant takes effect for all devices of the tenant. IP addresses matching global allowlist entries will not be automatically blocked by the blacklist. You can set multiple network segments to protect your assets.

\*Name

Remarks

\*IP Address/Range ?

10.1.1.1-10.2.2.2  
10.3.3.3

Entered 2 / 200

Cancel

Confirm


----End

## 2.3.4 Blacklist and Whitelist Authorization

### Context

Huawei Qiankun needs to be authorized before delivering blacklists to your devices.

### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
  - Step 2** Choose **Services** > **Authorization**.
  - Step 3** Perform operations as prompted.
- End

## 2.3.5 Subscribing to Alarms and Reports

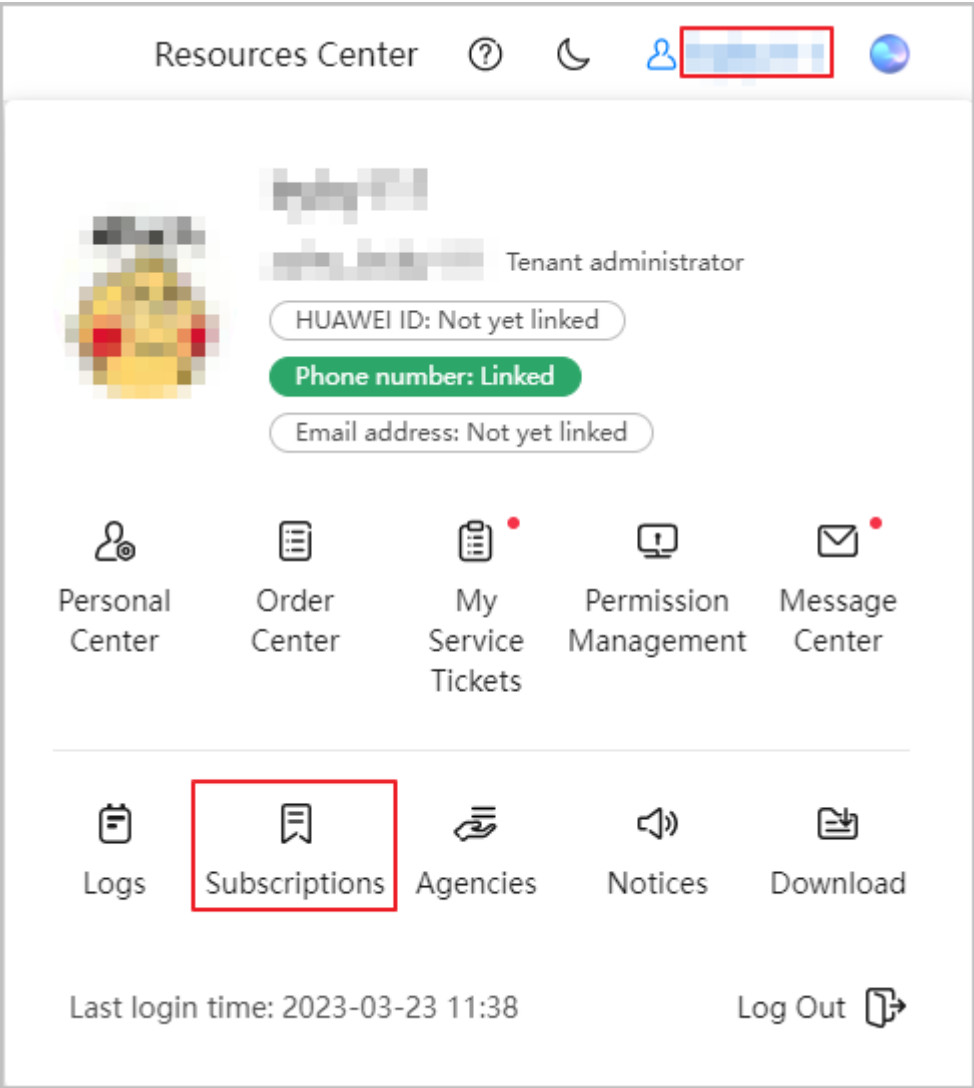
### Context

After the subscription, Huawei Qiankun sends alarms and security reports to you via SMS or email.

### Procedure

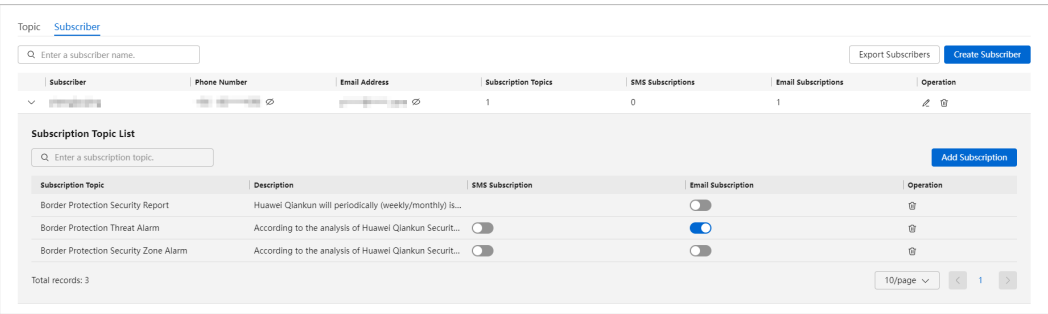
- Step 1** Log in to the Huawei Qiankun console, click the account in the upper right corner, and then click **Subscriptions**.

Figure 2-21 Subscription



Step 2 Add subscriptions as prompted on the **By Subscriber** page.


Figure 2-22 Adding subscriptions by subscriber



----End

## 2.3.6 Checking Threat Events

### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Click **Threat Events** in the menu bar. Threat events on Huawei Qiankun are displayed, indicating that Huawei Qiankun can properly receive threat logs from devices.
- Step 3** Then, you can handle these events on the Huawei Qiankun console. For details, see section "Handling Threat Events" in the *User Guide*.

----End

## 2.4 User Guide

### 2.4.1 Checking the Cyber Security Status

#### 2.4.1.1 Checking the Security Protection Dashboard

##### Context

The security protection dashboard displays three parts: security identification and detection, security response and recovery, and latest events. The three parts include top 5 compromise types, top 5 threat types, threat events, system health status, average threat detection duration, threat blocking rate, detected attack types, threat IP blocking trend, and latest events.

The security protection dashboard provides differentiated functional modules based on the Border Protection and Response Service package type. The basic function module is applicable to users who have activated any package. The function module marked with the professional edition tag is applicable only to users who have activated the professional edition package. For details about the function modules and corresponding packages, see [Table 2-5](#).

Figure 2-23 Security protection dashboard






## Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose **Dashboard > Security Protection Dashboard**.

### NOTE

If only security-related services of Huawei Qiankun are purchased and activated, the security protection screen is displayed by default.

**Step 2** (Optional) Configure the security protection screen.

- Click  to set the refresh interval. After the function of refreshing the dashboard periodically is enabled, the account on the page stays in the logged-in state and will not be automatically logged out even upon session timeout.
- Click  to view the dashboard in full screen.
- Click the  button to customize the dashboard name and select the modules to be displayed.

**Table 2-5** Description of modules on the security protection dashboard

Appli cable Pack age	Module	Description
Stand ard, Stand ard + auto matic blocki ng, and Profe ssion al	Security Health Status	Displays the security health score, which is calculated based on the security issues detected by security services in real time and certain scoring rules.
	Incident	Displays the numbers of handled and total external attack sources, compromised hosts, and malicious files.
	Top 5 Threat Detection Types	Displays top 5 threat event types by quantity.
	Top 5 Compromise Types	Displays top 5 causes leading to compromised hosts by quantity.
	Security Events	Displays the number of security events of each type. <ul style="list-style-type: none"> <li>– <b>Original Alarms:</b> Huawei Qiankun identifies original events based on threat logs provided by Qiankun Shield devices.</li> <li>– <b>Alert:</b> Huawei Qiankun aggregates original events into alarm events after automatic model-based analysis and manual handling by security operations experts.</li> <li>– <b>Incident:</b> After further intelligent analysis, Huawei Qiankun classifies alarm events into three types: external attack sources, compromised hosts, and malicious files.</li> </ul>
	Attack Map	Dynamically displays the source-to-destination attack direction and region distribution of the latest threat events.
	Latest Events	Displays threat event information in reverse chronological order.
	Threat IP Blocking Trend	Displays the trend of the number of blocked attack source IP addresses in the last 30 days.
	Detected Attack Types	Displays top 5 detected attack types by quantity.
	Avg Threat Detection Duration	Displays the average time taken by Huawei Qiankun to detect threat events based on the logs reported by Qiankun Shield devices.

Appli cable Pack age	Module	Description
	Threat Blocking Rate	Displays information about threat event blocking. <ul style="list-style-type: none"><li>– <b>Attack flow + source blocking</b>: displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies and blacklisted by Huawei Qiankun.</li><li>– <b>Attack flow blocking</b>: displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies.</li><li>– <b>Attack source blocking</b>: displays the number of threat events to which Huawei Qiankun has delivered blacklists.</li><li>– <b>Other events</b>: displays the number of threat events that have not been handled.</li></ul>
Professional	Top 5 File Attack Types	Displays top 5 malicious file types by file type (such as .exe and .zip).
	Top 5 Hosts by Number of Malicious Files	Displays top 5 host IP addresses with the largest number of malicious files.
	Top 5 Attack Source Geo-locations	Displays top 5 countries or regions by the number of attack sources.
	Threat Event Severity Distribution	Displays the distribution of threat events of different severity levels in a pie chart.
	Threat Type Trend	Displays the quantity trend of external attack sources, compromised hosts, and malicious files in the last 30 days.
	Threat Type Handling Status	Displays the handling status of external attack sources, compromised hosts, and malicious files (unhandled, blocked, ignored, or manually handled).

----End

2.4.1.2 Checking the Homepage of the Border Protection and Response Service

Context

On the home page of Border Protection and Response Service, you can view the overall running status of the service, including **Real-time protection by local devices**, **Cloud-based analysis and intelligent identification**, and **Risk traceability and in-depth cleaning**. It also displays statistics such as **TOP Detected Attack Type**, **Threat Blocking Rate**, **Threat Event Trends in 30 Days**, and **Blacklist Trends in 30 Days**.

Procedure


- Step 1
- Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2
- Check the homepage of the Border Protection and Response Service.

Figure 2-24 Homepage of the Border Protection and Response Service

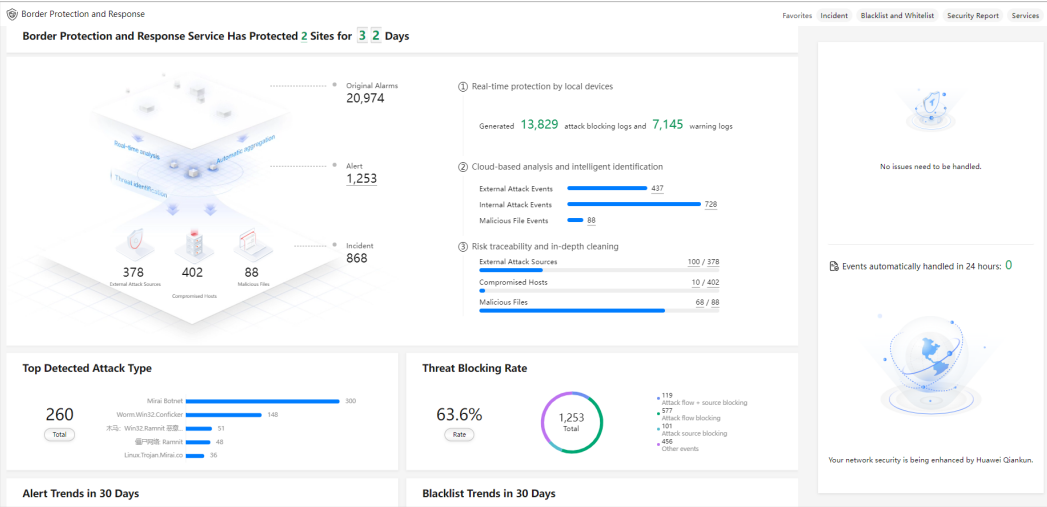


Table 2-6 Introduction to the homepage of the Border Protection and Response Service

Section	Module	Description
Service value presentation	Border Protection and Response Service Has Protected X Sites for X Days	Displays the number of sites, number of days for which the service has been used, and converted labor efficiency. You can click the site number to view the site list.

Section	Module	Description
	Overview	<p>Displays the overall overview of security events.</p> <ul style="list-style-type: none"> <li>• <b>Original Alarms:</b> Huawei Qiankun identifies original events based on threat logs provided by Qiankun Shield devices.</li> <li>• <b>Alert:</b> Huawei Qiankun aggregates original events into alarm events after automatic model-based analysis and manual handling by security operations experts. You can click the event number to view the list of alarm events.</li> <li>• <b>Incident:</b> After further intelligent analysis, Huawei Qiankun identifies threat events and classifies them into three types: external attack sources, compromised hosts, and malicious files.</li> </ul>
	TOP Detected Attack Type	Displays top 5 detected attack types by quantity.
	Threat Blocking Rate	<p>Displays information about threat event blocking.</p> <ul style="list-style-type: none"> <li>• <b>Attack flow + source blocking:</b> displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies and blacklisted by Huawei Qiankun.</li> <li>• <b>Attack flow blocking:</b> displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies.</li> <li>• <b>Attack source blocking:</b> displays the number of threat events to which Huawei Qiankun has delivered blacklists.</li> <li>• <b>Other events:</b> displays the number of threat events that have not been handled.</li> </ul>
	Alert Trends in 30 days	Displays the trend of the number of alarm events in the last 30 days.
	Blacklist Trends in 30 days	Displays the trend of the number of delivered blacklists in the last 30 days.
Smart Assistant	Health status evaluation	Provides a quick entry for handling threat events by site.
	Event Handling	<p>Huawei Qiankun automatically processes exception events to ensure normal service running.</p> <p>Displays the number and overview of exception events in the last 24 hours.</p>

----End

## 2.4.2 Quick Configuration

### Context

To use the Border Protection and Response Service properly, you need to add multiple configurations on Huawei Qiankun in addition to onboarding devices. To simplify the deployment process and reduce learning costs, the Border Protection and Response Service provides quick configuration guidance. You can complete the configuration on the corresponding page as prompted.


### Procedure

When you log in to Huawei Qiankun for the first time, the Border Protection and Response Service automatically displays the initial configuration page. You need to complete the following configuration items:

- IP address security zone management: You can configure global whitelists and untrusted intranet addresses. For details, see [2.4.6 IP Address Security Zone Management](#).
- Authorization management: Huawei Qiankun can automatically deliver blacklists to devices of a tenant only after the tenant is authorized, ensuring networking security. For details, see [2.4.7 Authorization Management](#).
- More configurations
  - Automatic threat blocking configuration: You can customize the blocking duration for the blacklists automatically delivered by Huawei Qiankun. For details, see [2.4.8 Configuring the Automatic Threat Blocking Duration](#).
  - User-defined signature configuration: You can determine whether to enable the user-defined IPS signature function. security operations experts of Huawei Qiankun can deliver user-defined signatures to devices only after authorization. User-defined signatures can be flexibly processed based on customer services to improve threat defense capabilities. User-defined signatures are verified, configured, and delivered by security operations experts of security operations experts in a unified manner. Do not directly configure user-defined signatures on the device to avoid conflicts with signatures delivered by Huawei Qiankun.  
security operations experts can deliver IPS user-defined signatures after multi-user evaluation in emergencies. IPS user-defined signatures can be used as network patches to block generated attacks. Users can use IPS user-defined signatures to block private or customized traffic.  
To use this function, toggle on **Custom Signature Authorization**. For details, see [2.4.9 Configuring Custom Signature Authorization](#).
  - Subscription setting: The Border Protection and Response Service can notify you of emergency events via SMSs and emails, and periodically send weekly and monthly security reports to your mailbox. You can enable the related function through subscription. For details, see .

You are advised to complete the initial configuration according to the recommended steps to obtain better service experience. If you choose to skip the

initial configuration temporarily and want to continue the configuration later, click **Get Start** in the menu bar to start the initial configuration.

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

**Step 2** Complete the initial configuration as prompted.

 **NOTE**

After the initial configuration is complete, you can click **Services** in the menu bar to start the service configuration process.

----End

## 2.4.3 Handling Threat Events

### 2.4.3.1 Event Overview

#### Context

After identifying alarm events, Huawei Qiankun performs further intelligent handling, identifies threat events, and classifies them into three types: external attack sources, compromised hosts, and malicious files.

By default, data of the last 30 days is displayed on the threat event page. Tenants can select a period in the upper right corner to view data. When a tenant clicks **More**, data of the last three months is displayed.

 **NOTE**

Service data of tenants will be retained for a maximum of three months.


Threat events in some special scenarios are labeled with different tags.

- The threat event of a successful attack is labeled with **Successful Attack** in the **Event Name** column.
- Threat events detected by devices that are onboarded in bypass mode are labeled with **Bypass** in the **Attack Status** column. A device working in bypass mode cannot block traffic.

You can view threat events by event type or site. The two modes display the same threat events in different ways. Unless otherwise specified, the following sections describe external attack sources, compromised hosts, and malicious files by event type.

High-level tenant accounts have the permission to check and handle their own and lower-level tenant accounts' threat events.

#### Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

**Step 2** Click **Threat Events** in the menu bar.

Step 3 Check threat events by event type or site.

- By event type: Click **By Event Type**.  
When you view threat events by event type, the threat event page displays four modules: **Event Overview**, **External Attack Sources**, **Compromised Hosts**, and **Malicious Files**.

Figure 2-25 Checking threat events by event type

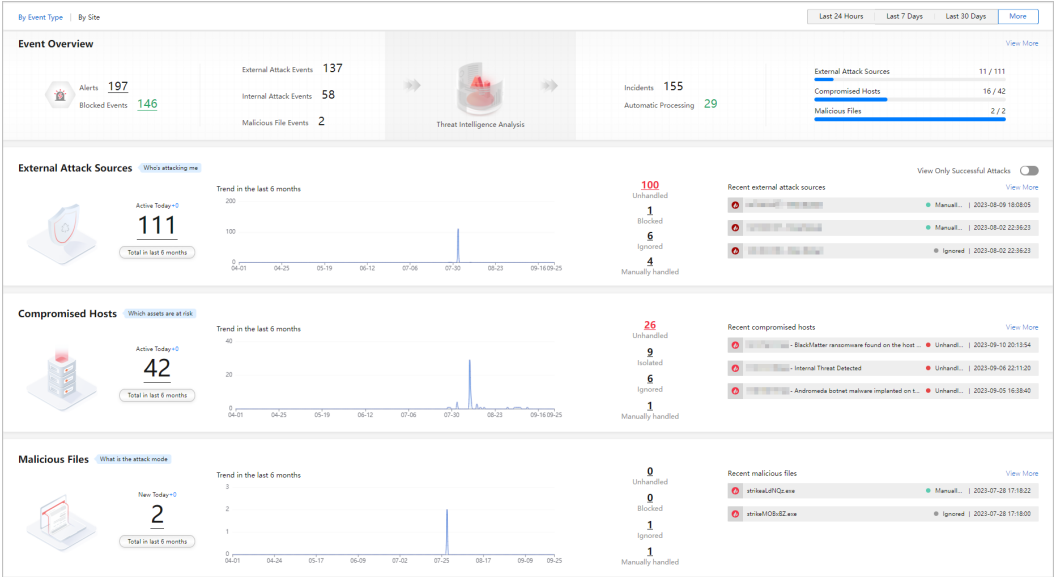


Table 2-7 Checking threat events by event type

Module	Description
Event Overview	<p>Displays information about threat events.</p> <ul style="list-style-type: none"><li>On the left of the card: Click the corresponding number to view all alarm events and alarm events that have been automatically blocked.</li><li>On the right of the card: The blue lines indicate the threat events that have been handled automatically or manually, and the gray lines indicate the threat events that have not been handled. You can move the cursor to the lines to view details data.</li></ul> <p>You can <b>View More</b> to go to the alarm event details page.</p>
External Attack Sources	<p>Displays information about external attack sources. You can click <b>View More</b> to view details of external attack sources.</p>
Compromised Hosts	<p>Displays information about compromised hosts. You can click <b>View More</b> to view the details of compromised hosts.</p>
Malicious Files	<p>Displays information about malicious files. You can click <b>View More</b> to view the details of malicious files.</p>

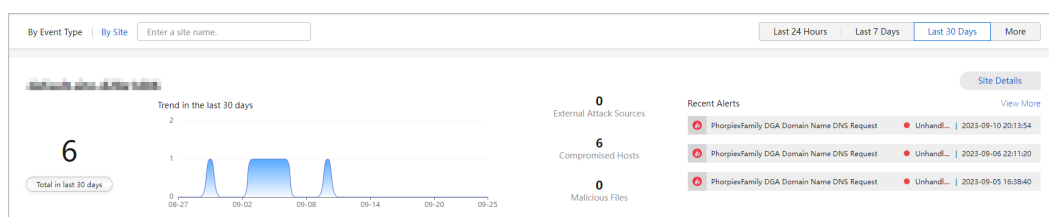
- By site: Click **By Site**.

When you click **By Site** to check threat events, the threat event page displays threat events at each site. You can click **Site Details** corresponding to a site to view the site model.

A site is a collection of devices located in the same administrative domain, either physically or logically. Network quality and security evaluation is performed on a per-site basis, achieving unified device monitoring and management.

Huawei Qiankun aggregates threat logs reported by the Qiankun Shield devices that do not belong to any site into alarm events. The alarm events will be included in the unknown site.

**Figure 2-26** Checking threat events by site



-----End

## 2.4.3.2 External Attack Sources

### Prerequisites

**2.4.7.1 Blacklist and Whitelist Authorization** has been completed.

### Context

Huawei Qiankun determines whether a threat event is an external attack source based on the following rules:

- If a host in a user-untrusted zone or mixed zone launches attacks, the IP address of the host is not in the global whitelist or in the default private network segment, the threat event is an external attack source.  
For details about the user-untrusted zone and mixed zone, see [2.4.6.4 Configuring Device Security Zones](#). For details about the global whitelist, see [2.4.6.2 Configuring a Global Whitelist](#). The default private network segments are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.555, and 192.168.0.0 to 192.168.255.255.
- If an intranet IP address in the user-untrusted zone or mixed zone initiates attacks and the IP address is an untrusted private IP address, the threat event is an external attack source. For details about the untrusted intranet IP address, see [2.4.6.3 Configuring Untrusted Intranet Addresses](#).

Huawei Qiankun can handle an external attack source event in the following ways:

- Huawei Qiankun intelligently analyzes the event, delivers an IP address blacklist, and sets the handling status of the event to **Blocked**.


- Huawei Qiankun intelligently analyzes the event and cannot deliver an IP address blacklist. security operations experts then conduct a further analysis and manually deliver an IP address blacklist. In this case, the handling status of the event is displayed as **Blocked**.
- If both intelligent analysis of Huawei Qiankun and security operations experts cannot handle the event based on existing information or the handling policy fails to be delivered, the handling status of the event is displayed as **Unhandled**.

Tenants need to manually handle such events by employing measures such as blocking attack sources and marking their status (**Manually handled** or **Ignored**).

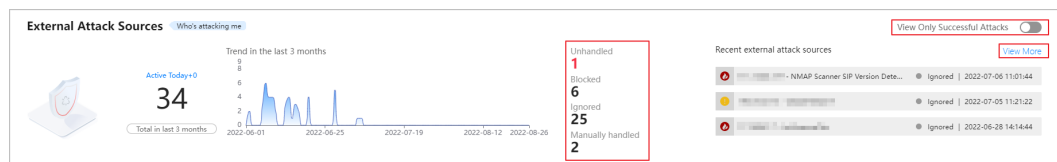
Huawei Qiankun can automatically deliver IP address blacklists only when the following versions are activated:

- Border Protection and Response Service Standard and automatic blocking
- Border Protection and Response Service Professional
- Border Protection and Response Service Advanced
- Border Protection and Response Service Trial

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Threat Events** in the menu bar.
- Step 3** Check the overview of external attack sources, and click a number or **View More** to view details.

**Figure 2-27** Overview of external attack sources



- Step 4** Handle the external attack sources

- Block attack sources.

If an IP address is an external attack source address, click **Block Attack Source** in the operation column to deliver the IP address blacklist.

After receiving the IP address blacklist from Huawei Qiankun, the Qiankun Shield devices block traffic sent by and to the blacklisted IP address.

### NOTE

Devices can work in hot standby mode. If two devices are onboarded and bound to work in hot standby mode but the active device cannot work properly, the standby device will take over services from the active device. When you block external attack sources on the **By Event** tab page, the IP address blacklist is delivered to both the devices working in hot standby mode, and you can see two records in the **Historical IP Blacklist**.

Figure 2-28 Blocking attack sources

**Block Attack Sources** [X]

Attack Source List: Total Records: 1


Attack Source IP ↑↓	Name of Delivered Device

Block Duration

☐ Permanent ☒ 2 Days 0 Hours 2 Minutes

☒ You are about to block the external attack source. After this operation is performed, all access requests from the attack source IP address will be blocked within the validity period. Are you sure you...

Cancel **Confirm**

If the handling status of the external attack source is marked , the external attack source is unblocked.

- Mark the event status.
  - Manually handled  
Tenants manually handle external attack source events, for example, searching for the target hosts based on the source and destination addresses of the events, and scanning for and removing viruses from the target hosts. Then, they can mark the event status as **Manually handled**.
  - Ignored  
If an event does not need to be handled or is a false positive, set the event status to **Ignored** in the operation column.

#### NOTE

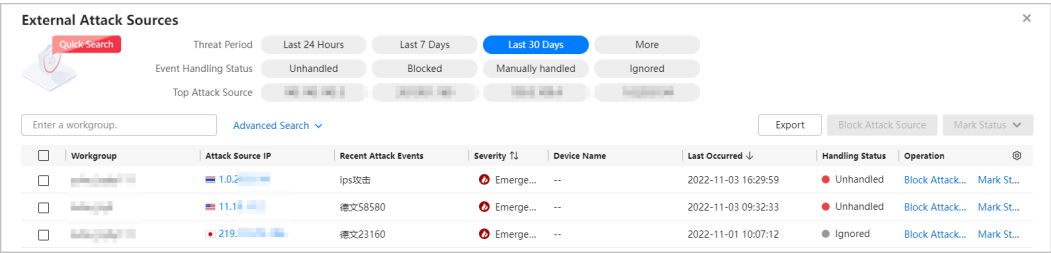
If you do not know how to handle the problem or the problem persists after you handle it, contact the corresponding Managed Security Service Provider (MSSP) or channel partner.

----End

## Follow-up Procedure

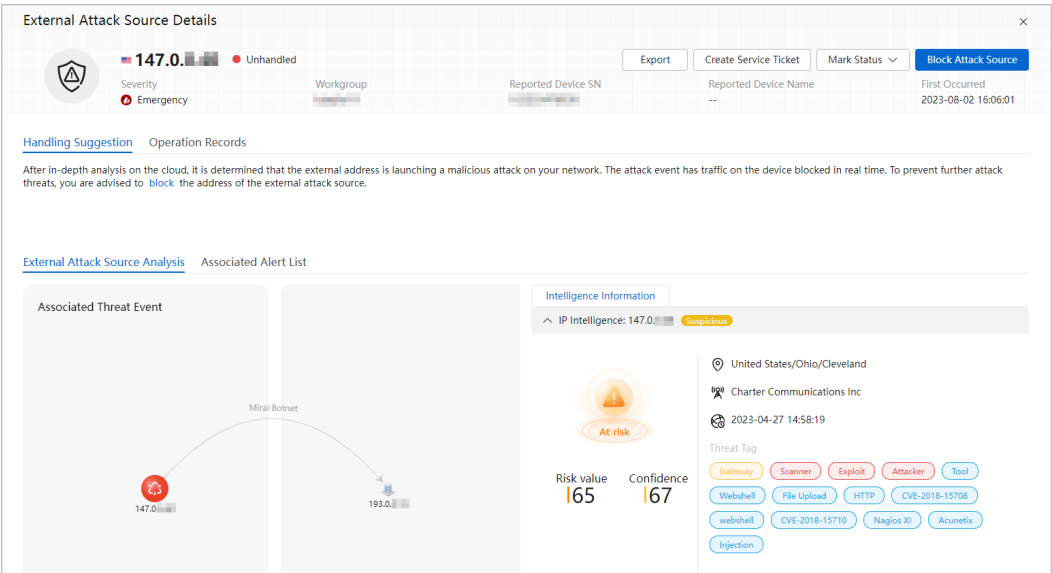
- On the **External Attack Sources** page, a national flag is displayed before each IP address in the **Attack Source IP** column. You can move the mouse cursor over a flag to view the country name, and click an IP address to check details about the external attack source.  
You can set search criteria in **Advanced Search** and click **Export** to export the list of external attack sources that meet the search criteria to an Excel file. Alternatively, you can select the target external attack sources and click **Export** to export the list of selected external attack sources.

Figure 2-29 List of external attack sources



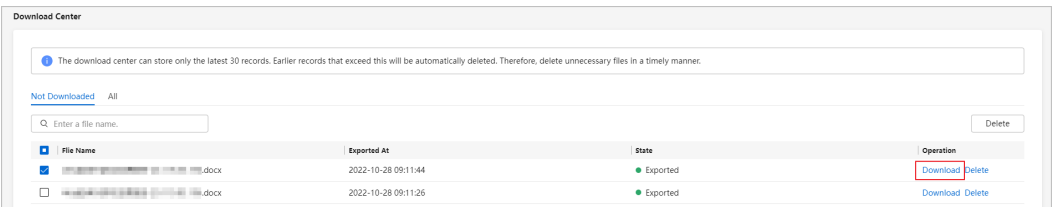
- The external attack source details page displays information such as handling suggestions, handling records, external attack source analysis, and associated alarm event list.
  - You can click **Export** to export details about a specific external attack source to a Word file.

Figure 2-30 Details page of an external attack source



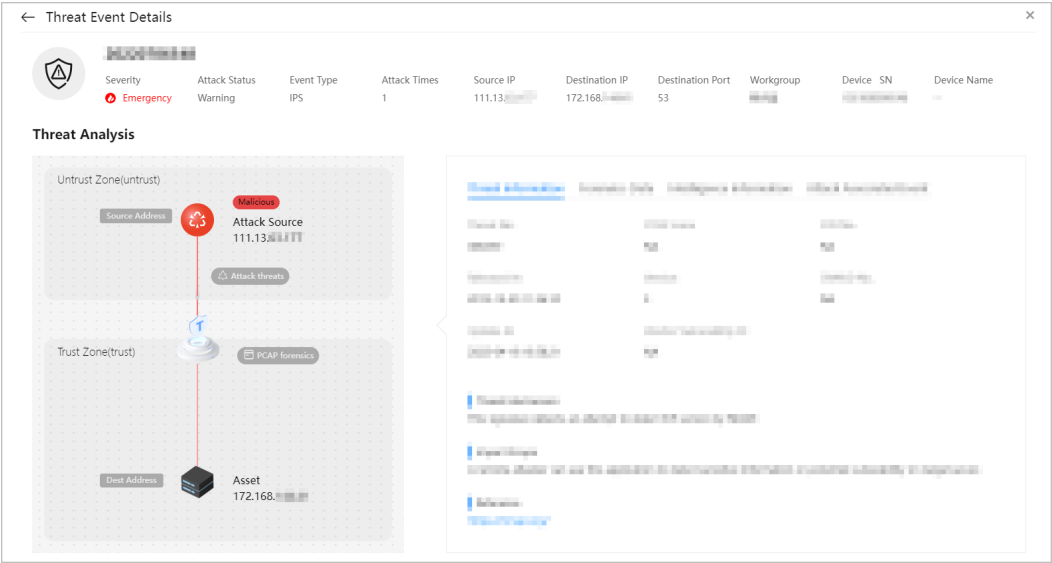
After the export is complete, click your account in the upper right corner and click **Download** to download the corresponding file.

Figure 2-31 Download Center



- You can click an event name in the **Associated Threat Event List** area on the **External Attack Source Details** page to check details about the event.

Figure 2-32 Threat Event Details page



NOTE

The **External Attack Source Details** page may contain public IP addresses, helping you learn about threat events. The service does not proactively initiate connections to these public IP addresses.

2.4.3.3 Compromised Hosts

Prerequisites

2.4.7.1 Blacklist and Whitelist Authorization has been completed.

Context

Huawei Qiankun determines whether a threat event is a compromised host based on the following rules:

1. If a host in the user-trusted zone initiates attacks, the host is considered as a compromised host. For details about the user-trusted zone, see 2.4.6.4 Configuring Device Security Zones.
2. If a host whose IP address is in the global whitelist initiates attacks, the host is considered as a compromised host. For details about the global whitelist, see 2.4.6.2 Configuring a Global Whitelist.
3. If a host whose IP address is an untrusted intranet IP address initiates attacks, the host is not considered as a compromised host. For details about the untrusted intranet IP address, see 2.4.6.3 Configuring Untrusted Intranet Addresses.
4. If a host whose IP address belongs to the default private network segment initiates attacks, the host is considered as a compromised host. The default private network segments are 10.0.0.0 to 10.255.255.255, 172.16.0.0 to 172.31.255.555, and 192.168.0.0 to 192.168.255.255.

Based on the compromise types, security operations experts can classify compromised hosts into the following types: **Ransomware, Mining, Worm, C&C,**

**Vulnerability Attack**, and **Insecure Configurations**. Those whose compromise types are not identified are classified into **Other**.


For a compromised host, Huawei Qiankun sends an SMS or email alarm to the tenant and sets the status of the compromised host to **Unhandled**. Tenants need to handle the threat event by isolating the compromised host or marking the event status (manually handled or ignored).

In addition, for the compromised hosts detected after malicious domain name detection events are analyzed, Huawei Qiankun sends SMS and email alarms to tenants and automatically delivers the domain name blacklist. Users' access to the domain names in the blacklist will be blocked.

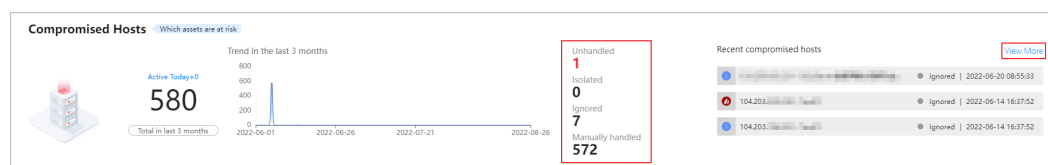
USG6603F-C and USG6000F support the delivery of the domain name blacklists since V600R023C10. USG6000E-C and USG6000E can automatically deliver domain name blacklists only when the following version is activated:

- Border Protection and Response Service Standard and automatic blocking
- Border Protection and Response Service Trial
- Border Protection and Response Service Advanced

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Threat Events** in the menu bar.
- Step 3** Check the overview of compromised hosts, and click a number or **View More** to view details.

**Figure 2-33** Overview of compromised hosts



- Step 4** Handle compromised hosts.
- Isolate a compromised host.
- If no service is running on a compromised host or services will not be affected after the compromised host is isolated, click **Isolate Host** in the **Operation** column to deliver the IP address blacklist.
- After receiving the IP address blacklist from Huawei Qiankun, the Qiankun Shield devices block traffic sent by and to the blacklisted IP address.

### NOTE

Devices can work in hot standby mode. If two devices are onboarded and bound to work in hot standby mode but the active device cannot work properly, the standby device will take over services from the active device. When you isolate a host on the **By Event** tab page, the IP address blacklist is delivered to both the devices working in hot standby mode, and you can see two records in the **Historical IP Blacklist**.

**Figure 2-34** Isolating a host

**Isolate Host** [X]

Host List: Total Records: 1


Compromised Host IP ↑↓	Name of Delivered Device
65.126. [REDACTED]	[REDACTED]

Block Duration

1 ☐ Permanent ☒ 2 Days 0 Hours 2 Minutes

2 ☒ You are about to isolate the compromised host. After this operation is performed, the external access traffic of the host will be blocked by the Qiankun Shield device to prevent malicious remote access...

3

If the handling status of the compromised host is marked , the host isolation is cancelled.

- Mark the event status.
  - Manually handled  
A tenant manually handles compromised hosts, for example, scanning for and removing viruses on the compromised host. After confirming that the host has no security risk, the tenant can mark the compromised host status as **Manually handled** in the **Operation** column.
  - Ignored  
If an event does not need to be handled or is a false positive, set the compromised host to **Ignored** in the operation column.

#### NOTE

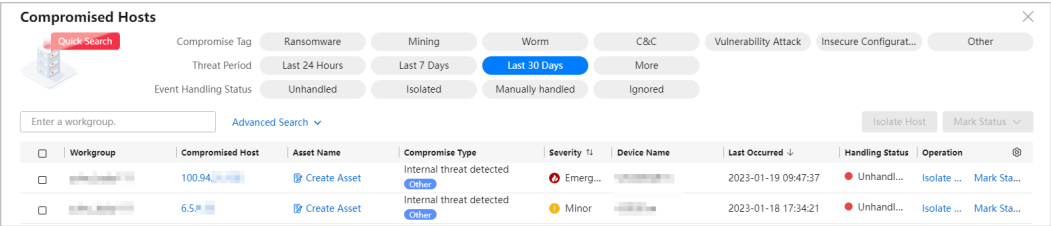
- The handling suggestion may contain the link of a reference manual for you to handle the threat event.
- If you do not know how to handle the problem or the problem persists after you handle it, contact the corresponding Managed Security Service Provider (MSSP) or channel partner.

----End

## Follow-up Procedure

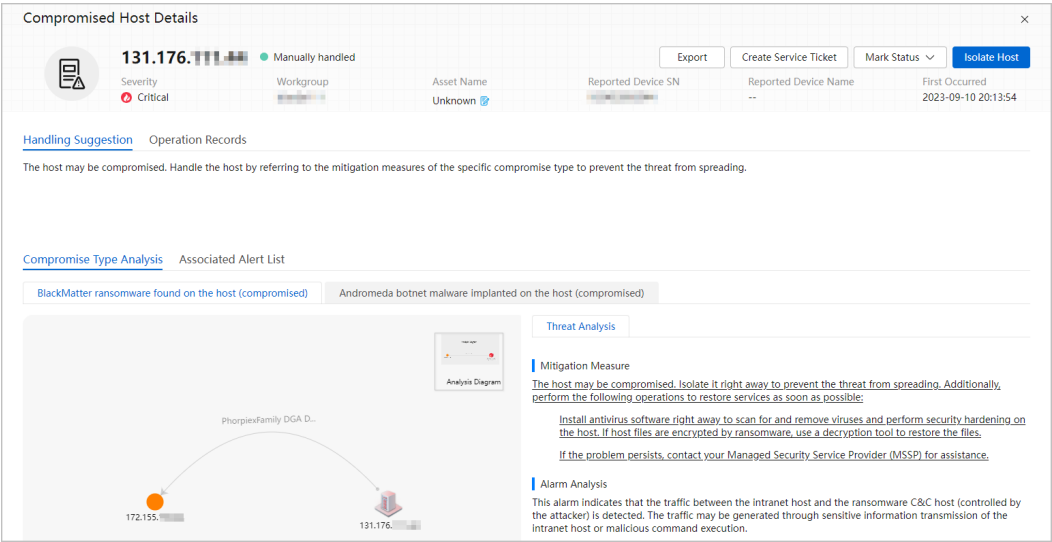
- On the **Compromised Hosts** page, you can click the IP address of a compromised host to view details about the compromised host.

Figure 2-35 Compromised host list



- The compromised host details page displays information such as handling suggestions, handling records, compromise type analysis, and associated alarm event list.
  - You can click **Export** to export details about a compromised host to a Word file.

Figure 2-36 Compromised Host details page



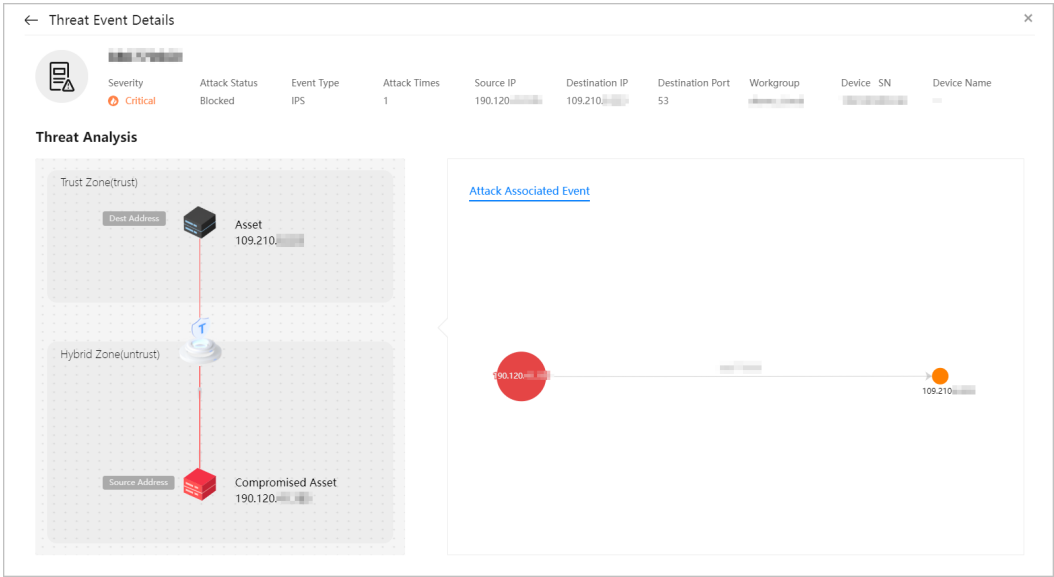
After the export is complete, click your account in the upper right corner and click **Download** to download the corresponding file.

Figure 2-37 Download center



- You can click an event name in the associated threat event list on the details page of compromised hosts to check details about the event.

Figure 2-38 Threat event details



**NOTE**

The details page of compromised hosts may contain public IP addresses, which are used only to display event information to help you learn about threat events. The service does not proactively initiate connections to these public IP addresses.

2.4.3.4 Malicious Files

Context

Huawei Qiankun determines the detection type of a threat event based on logs provided by the device. If the detection type is AV/CDE, the threat event is identified as a malicious file event.

If the malicious file is blocked when the device detects it, the status of the malicious file event is **Blocked**. If the malicious file is not blocked when the device detects it, the status of the malicious file event is **Unhandled**.

For malicious files that are in **Blocked** or **Unhandled** state, Huawei Qiankun can send SMS and email alarms to notify tenants or deliver an IP address blacklist.

Tenants need to handle the malicious files in **Unhandled** state and mark them as **Manually handled** or **Ignored**.

Procedure


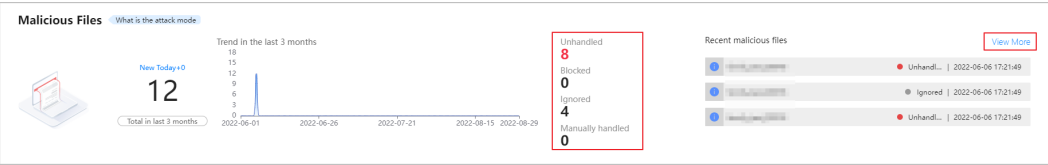
- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Threat Events** in the menu bar.
- Step 3** Check the overview of malicious files, and click a number or **View More** to view details.

Figure 2-39 Overview of malicious files



Step 4 Mark the status of unhandled malicious files.

- Manually handled  
Tenants manually handle specific events, for example, searching for and clearing malicious files based on the source and destination addresses of events, and file names.  
After confirming that malicious files have been cleared from hosts, mark the events as **Manually handled** in the **Operation** column.
- Ignored  
If the events are false positives or do not need to be handled, mark the events as **Ignored** in the **Operation** column.

NOTE

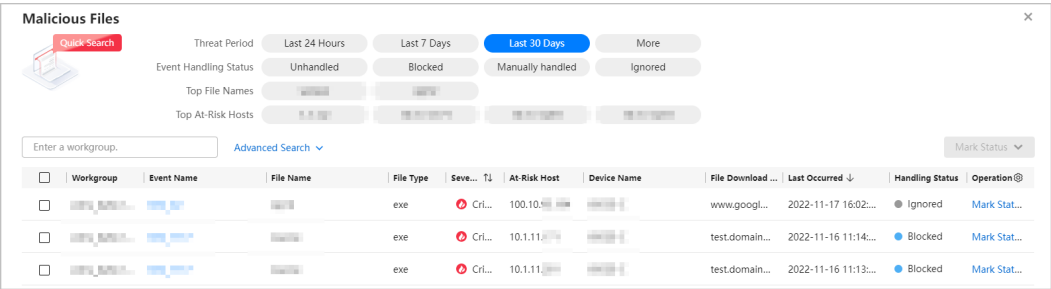
If you do not know how to handle the problem or the problem persists after you handle it, contact the corresponding Managed Security Service Provider (MSSP) or channel partner.

----End

Follow-up Procedure

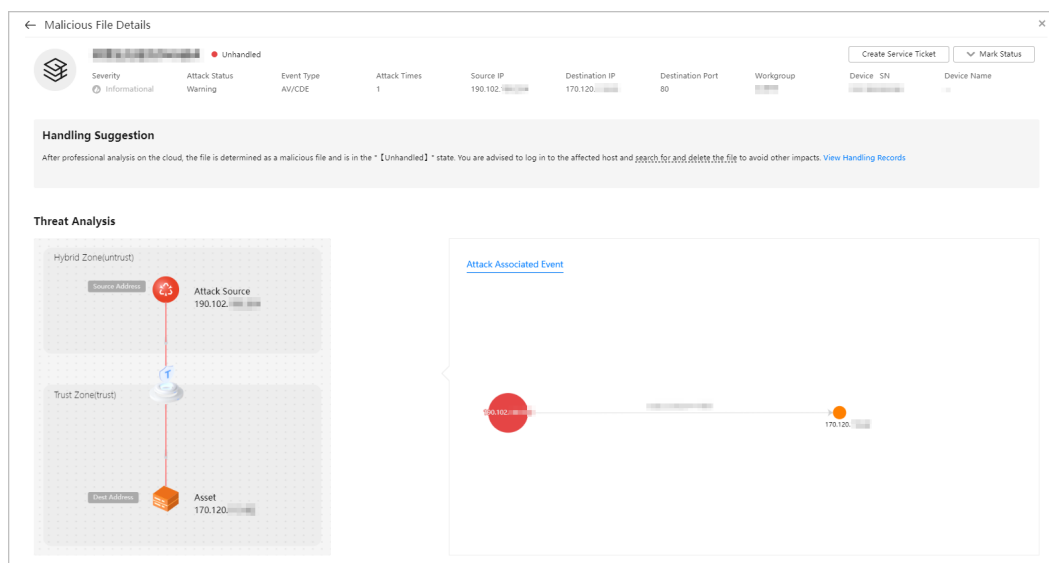
- On the **Malicious Files** page, you can click an event name to view details of the malicious file event.

Figure 2-40 Malicious Files page



- The **Malicious File Details** page contains **Handling Suggestions**, **Operation Records**, and **Threat Analysis**.

Figure 2-41 Malicious File Details page



#### NOTE

On the **Malicious File Details** page, the event names and malicious file information may contain public IP addresses, helping you learn about threat events. The service does not proactively initiate connections to these public IP addresses.

## 2.4.4 Managing Blocklists and Allowlists

### 2.4.4.1 Clearing IP Address Blacklists from a Specified Device with One Click

#### Context


If a service exception occurs on a device to which IP address blacklists have been delivered, you can clear all the IP address blacklists from the device with simply one click to ensure quick service recovery.

#### CAUTION

If you clear all IP address blacklists from specified Qiankun Shield devices with one click, the Qiankun Shield devices will no longer have protection capabilities and the enterprise network may be attacked. Exercise caution when performing this operation.

High-level tenant accounts have the permission to delete their own and lower-level tenant accounts' IP address blacklists.

#### Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

- Step 2** Click **Blacklist and Whitelist** in the menu bar.
- Step 3** Choose **Device IP Blacklist > IP Address Blacklist** and click **Clear Device Blacklist**.
- Step 4** Clear blacklists from specified devices.

**Figure 2-42** Clearing blacklists from specified devices

**Clear Device Blacklist** [X]

Q Enter a device name or SN.

	Device Name	Device SN	Tenant Name
<input checked="" type="radio"/>	1CC8DA16	102452856542	bianjie111

Total records: 6

10/page [v] [ < ] 1 [ > ]

☒ You will clear all blacklist policies on the selected device. Are you sure you want to clear them ?

[ Cancel ] [ Confirm ]

----End

## 2.4.4.2 Manually Creating an IP Address Blacklist or Whitelist

### Context

- An IP address blacklist is used to block threats and attacks. After local devices receive IP address blacklists from Huawei Qiankun, they discard the packets with IP addresses matching the IP address blacklists.

For different threat events, IP address blacklists can be delivered in the following modes:

- External attack sources: IP address blacklists can be delivered by Huawei Qiankun automatically, security operations experts, and tenants who click **Block Attack Source**.
- Compromised hosts: After you click **Isolate Host**, an IP address blacklist is delivered.

In addition, you can manually deliver IP address blacklists to specified devices based on the actual network environment or service requirements, improving the flexibility of security protection.

- IP address whitelists can be delivered by Huawei Qiankun to devices to permit packets with IP addresses matching the whitelists.


High-level tenant accounts have the permission to create and modify their own and lower-level tenant accounts' IP blacklists and whitelists.

 **NOTE**

When users manually deliver blacklists and whitelists and their number exceeds the upper limit of devices, the system displays a message indicating that the delivery fails.

When Huawei Qiankun automatically delivers blacklists and the number of device blacklists exceeds the upper limit, Huawei Qiankun deletes the earliest-delivered blacklists to ensure successful delivery. If the remaining blacklists are manually delivered by users, Huawei Qiankun fails to deliver the blacklists automatically.

## Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.

**Step 2** Click **Blacklist and Whitelist** in the menu bar.

**Step 3** Create an IP address blacklist. The procedure for creating an IP address whitelist is similar.

Choose **Device IP Blacklist > IP Address Blacklist** and click **Create**.

### Create Blacklist

Class D IP addresses 224.0.0.0 to 239.255.255.255 cannot be delivered.

\*Select Device

Optional (4)

Q Enter a device name.

Device ...

Device ...

Workg...

1

☒

☒

☐

☐

Total records: 4

< 1/1 >

Selected (0)

Q Enter a device name.

Device ...

Device ...

Workg...

2

>

<

No records found.

Total records: 0

3

\*Source/Destination

☒ Source ☐ Destination

\*IP Address

10.10.10.10

\*Protocol

ANY

\*Port

ANY

Block Duration

☐ Permanent ☒ 2 Days 0 Hours 0 Minutes

☒ You are about to create a blacklist policy on the selected devices. After the policy is complete, the devices will block all access to the IP address. Are you sure you want to create it ?

Cancel

4 Confirm

Parameter	Description
Select Device	Devices to which an IP address blacklist is to be delivered.
Source/Destination	Source or destination IP address. The source and destination IP addresses can be delivered at the same time.
IP Address	IP address of packets to be blacklisted or permitted. The IP address blacklists containing class D reserved addresses (224.0.0.0–239.255.255.255) cannot be delivered.
Protocol	IP protocol, which can be set to <b>ANY</b> , <b>TCP</b> , <b>UDP</b> , or <b>ICMP</b> .

Parameter	Description
Port	The value <b>ANY</b> indicates all ports.
Block Duration	Validity period of an IP address blacklist.

**Step 4** Click **Confirm** to deliver the IP address blacklist to specified devices.

----End

### 2.4.4.3 Checking IP Address Blacklists and Whitelists Fast

#### Context

IP address blacklist and whitelist management is an important part of border protection. Compared with traditional sophisticated security detection methods, IP address blacklists and whitelists can directly and effectively block malicious attacks, reducing system resource consumption and loads on Qiankun Shield devices.

IP address blacklists and whitelists are mainly delivered in the following situations:


- Huawei Qiankun automatically delivers IP address blacklists after analyzing threat events.
- After processing the threat event, security operations experts determine that it is an attack and deliver an IP address blacklist.
- Tenants manually create and deliver IP address blacklists and whitelists on the console.

IP address blacklists and whitelists can be in the following states:

- **Effective:** IP address blacklists and whitelists stored on Huawei Qiankun have been successfully delivered to the Qiankun Shield devices and have taken effect.
- **Deploying:** IP address blacklists and whitelists stored on Huawei Qiankun have not been delivered to the Qiankun Shield devices.
- **Failed:** The delivery command has been issued but IP address blacklists and whitelists fail to be delivered.


High-level tenant accounts have the permission to check their own and lower-level tenant accounts' IP blacklists and whitelists.

#### Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

**Step 2** Click **Blacklist and Whitelist** in the menu bar.

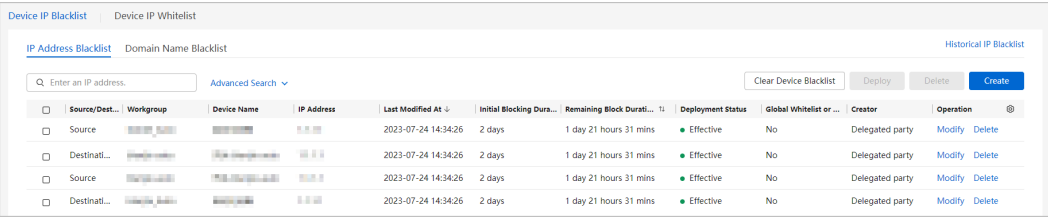
**Step 3** Check IP address blacklists on devices.

Choose **Device IP Blacklist > IP Address Blacklist**. You can click  in the **Last Modified At** column to view the records in chronological or reverse chronological order.

 **NOTE**

After Huawei Qiankun delivers the IP address blacklist to block IP addresses, the device periodically obtains the IP address blacklist from Huawei Qiankun. The generation time of the IP address blacklist on the two sides may be different. Therefore, the remaining blocking duration of the IP address blacklist displayed on the two sides may be different. Use the remaining blocking duration on Huawei Qiankun.

**Figure 2-44** Checking IP address blacklists on devices



Source/Dest...	Workgroup	Device Name	IP Address	Last Modified At	Initial Blocking Duration	Remaining Block Duration	Deployment Status	Global Whitelist or ...	Creator	Operation
Source				2023-07-24 14:34:26	2 days	1 day 21 hours 31 mins	Effective	No	Delegated party	Modify Delete
Destinati...				2023-07-24 14:34:26	2 days	1 day 21 hours 31 mins	Effective	No	Delegated party	Modify Delete
Source				2023-07-24 14:34:26	2 days	1 day 21 hours 31 mins	Effective	No	Delegated party	Modify Delete
Destinati...				2023-07-24 14:34:26	2 days	1 day 21 hours 31 mins	Effective	No	Delegated party	Modify Delete

**Table 2-8** Key parameters of the IP address blacklist

Parameter	Description
Global Whitelist or Not	If a source or destination IP address is in the global whitelist, a blacklist containing the IP address cannot be delivered by Huawei Qiankun automatically or by its security operations experts. The IP address blacklist can only be manually created and delivered by tenants and MSPs.
Creator	<ul style="list-style-type: none"><li>● <b>Tenant:</b> A tenant manually delivers an IP address blacklist on Huawei Qiankun.</li><li>● <b>Delegated party:</b> An MSP manually delivers an IP address blacklist on Huawei Qiankun.</li><li>● <b>System:</b> An IP address blacklist is delivered by Huawei Qiankun automatically or by security operations experts.</li><li>● <b>Third-party interface:</b> Carriers deliver an IP address blacklist.</li></ul>

----End

**Follow-up Procedure**

- Check historical IP address blacklists.  
A historical IP address blacklist refers to an IP address blacklist that has taken effect but has been deleted or expired. You can choose **Blacklist and Whitelist > Device IP Blacklist > IP Address Blacklist > Historical IP Blacklist** to check historical IP address blacklists.
- Modify an IP address blacklist or whitelist.  
Select an IP address blacklist or whitelist and click **Modify** in the **Operation** column to reconfigure the IP address blacklist or whitelist.

- Delete an IP address blacklist or whitelist.  
Select an IP address blacklist or whitelist and click **Delete** in the **Operation** column to delete the IP address blacklist or whitelist.

#### 2.4.4.4 Manually Creating a Domain Name Blacklist


##### Context

Huawei Qiankun delivers domain name blacklists to devices to block access from internal assets to specified domain names.

Typically, Huawei Qiankun automatically delivers domain name blacklists to devices after performing intelligent analysis on threat events. In addition, you can manually deliver domain name blacklists to a specified device based on the actual network environment or service requirements, improving the flexibility of security protection.

High-level tenant accounts have the permission to create, modify, and delete their own and lower-level tenant accounts' domain name blacklists.

##### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Blacklist and Whitelist** in the menu bar.
- Step 3** Choose **Device IP Blacklist > Domain Name Blacklist**, click **Create**, and set parameters.


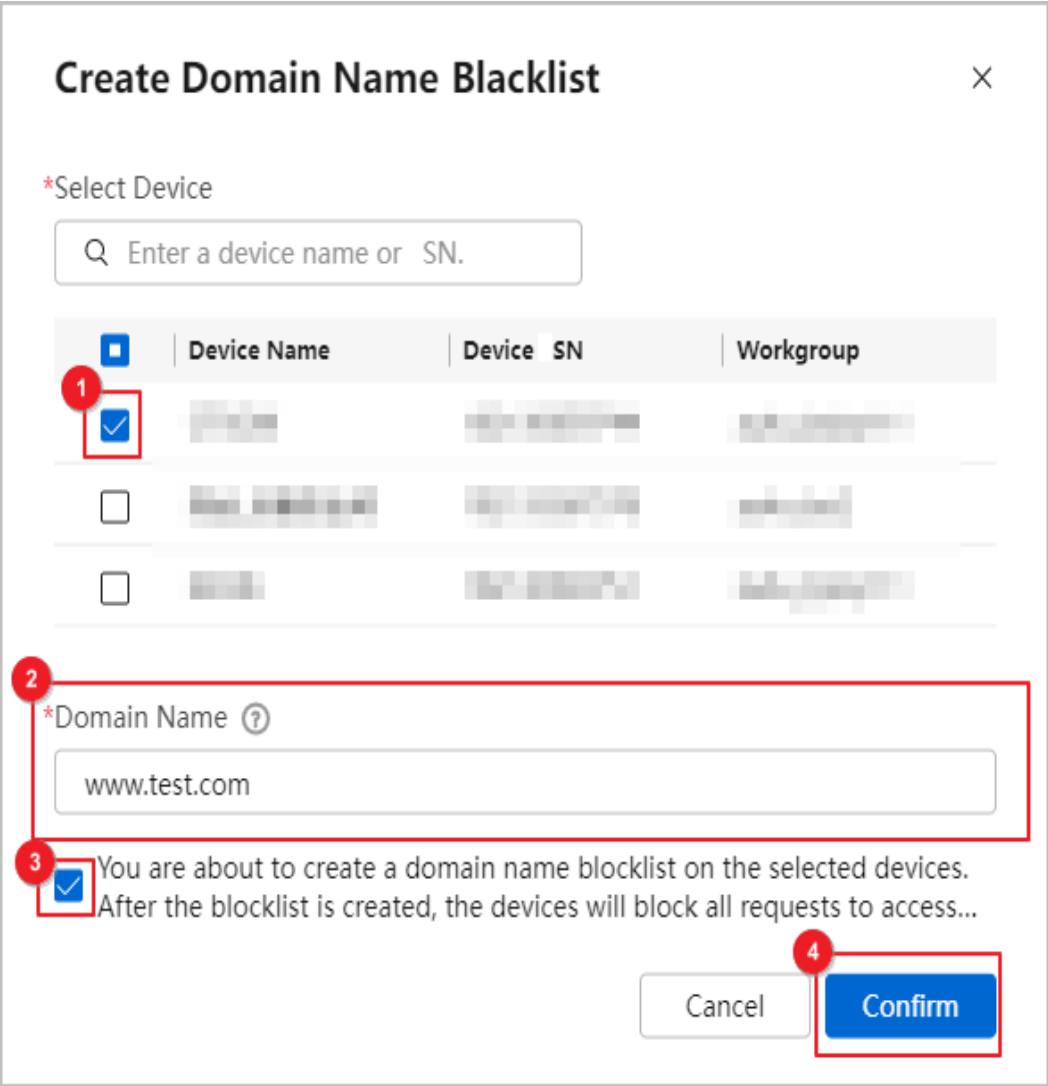
Domain names support regular expression match. For details about the rules, move the mouse cursor over the  icon next to **Domain Name**.

Figure 2-45 Creating a domain name blacklist



**Step 4** Click **Confirm** to deliver the domain name blacklist to specified devices.

**NOTE**

Domain name blacklists are not immediately delivered to the DNS filtering profiles of the devices. Instead, Huawei Qiankun delivers domain name blacklists at an interval of 1 minute. By default, domain name blacklists are permanently valid.

----End

2.4.4.5 Checking Domain Name Blacklists Fast

Context

Domain name blacklist management plays an important role in border protection. Associating security policies with DNS filtering profiles can effectively prevent internal assets from repeatedly accessing malicious domain names.

Domain name blacklists are mainly delivered in the following situations:


- Huawei Qiankun automatically delivers domain name blacklists after performing an intelligent analysis on threat events.
- Tenants manually create and deliver domain name blacklists on the console.

Domain name blacklists can be in the following states:

- **Effective:** Domain name blacklists stored on Huawei Qiankun have been successfully delivered to the Qiankun Shield devices, and have taken effect.
- **Deploying:** Domain name blacklists stored on Huawei Qiankun have not been delivered to the Qiankun Shield devices.
- **Failed:** The delivery command has been issued but domain name blacklists fail to be delivered.

High-level tenant accounts have the permission to check their own and lower-level tenant accounts' domain name blacklists.

## Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

**Step 2** Click **Blacklist and Whitelist** in the menu bar.

**Step 3** Choose **Device IP Blacklist** > **Domain Name Blacklist**, and view domain name blacklists.

----End

## Follow-up Procedure

Deleting a domain name blacklist: Select a domain name blacklist and click **Delete** in the **Operation** column to delete the domain name blacklist.

## 2.4.5 Checking Security Reports

### Prerequisites

You have bound an email address through the subscription management. For details, see section "[Subscription Management](#)" in *Tenant Operation Guide*.

### Context


Huawei Qiankun provides the function of checking security reports to help tenants learn about the trend of network security status in a certain period.

Tenants can view security reports on the security report page. Huawei Qiankun generates security reports of the last week or month on Monday or the first day of each month. After subscribing to the border protection security report on the **Account** > **Subscription** page, tenants can link email addresses to their accounts to receive weekly or monthly security reports.

Currently, common reports and customized reports are supported. Huawei Qiankun retains the reports of the last three calendar months (including the current month) only.

- Common reports: They are classified into weekly reports and monthly reports. Top-level tenants can check individual reports of each tenant in the current workgroup and summary reports of all tenants. None-top-level tenants can only check individual reports.
- Customized reports: security operations experts or MSPs can configure the periodic report generation. The customized reports cannot be subscribed to. They can be pushed only by security operations experts or MSPs.

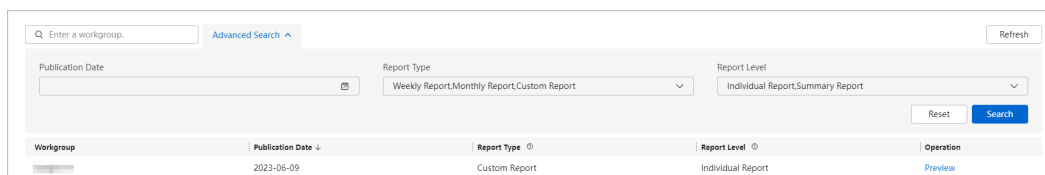
## Procedure

**Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.

**Step 2** Click **Security Reports** in the menu bar.

**Step 3** Select a report and click **Preview**.

**Figure 2-46** Security report list



**Step 4** Check security reports.

**Table 2-9** Introduction to security reports

Module	Description
Cyber Security Report Overview	Displays statistics about original alarms, threat events, and specific risks.
Threat Events	<p>Threat events are real security attack events automatically identified by the system based on original security alarms and automatic analysis technologies such as association analysis, expert models, and artificial intelligence.</p> <p>This module displays information, including the trend of threat events, threat types, destination addresses, details, as well as statistics on severity and response status.</p>
Special Risk   External Attack Source	<p>External attack sources are the addresses of external attackers identified by the system after automatic analysis and determination of threat events. Handling external attack sources promptly can reduce external intrusion threats.</p> <p>This module displays the quantity trend, attack source locations, attack types, details, as well as statistics on severity and threat status.</p>

Module	Description
Special Risk   Compromised Host	<p>Compromised hosts are internal risky asset addresses identified by the system after automatic analysis and determination of threat events. The compromised hosts include the following types: mining, remote control, ransomware, and internal attack threats.</p> <p>This module displays the trend of compromised hosts, malicious actions, compromised types, details, as well as statistics on severity and threat status.</p>
Special Risk   Malicious File	<p>Malicious files are malicious program files identified by the system after automatic analysis and determination of threat events. The files include Trojan horses, worms, mining, ransomware, and advertisements. The system automatically detects and blocks high-risk malicious files.</p> <p>This module displays the quantity trend, file types, risky hosts, details as well as statistics on severity and threat status.</p>

----End

## Follow-up Procedure

- You can click **Export to PDF** on the preview pages of security reports to download the security reports in the PDF format to the local PC.
- After learning about the trend of security status, you can handle the issues by referring to [Handling Threat Events](#).

### NOTE

If you do not know how to handle the problem or the problem persists after you handle it, contact the corresponding Managed Security Service Provider (MSSP) or channel partner.

## 2.4.6 IP Address Security Zone Management

### 2.4.6.1 Monitoring the Security Zone Status


#### Context

The Qiankun Shield device's odd-numbered ports (in the untrust zone) are used to connect to upstream devices, and even-numbered ports (in the trust zone) are used to connect to downstream LAN devices. If the upstream and downstream connections are incorrect, threat event notification and display on Huawei Qiankun will be affected.

Huawei Qiankun determines the probability of reverse connection of the uplink and downlink interfaces on the Qiankun Shield devices based on the IPS and CDE events aggregated in the last 24 hours. For example, if the probability of the CDE event is 100%, it indicates that the uplink and downlink interfaces on the Qiankun Shield devices are 100% connected in reverse.

Huawei Qiankun provides the checking result to the security operations experts who determine whether the interfaces are connected in reverse based on the IPS and CDE events. If so, a message is displayed on this page, indicating that the device security zones are connected in reverse.

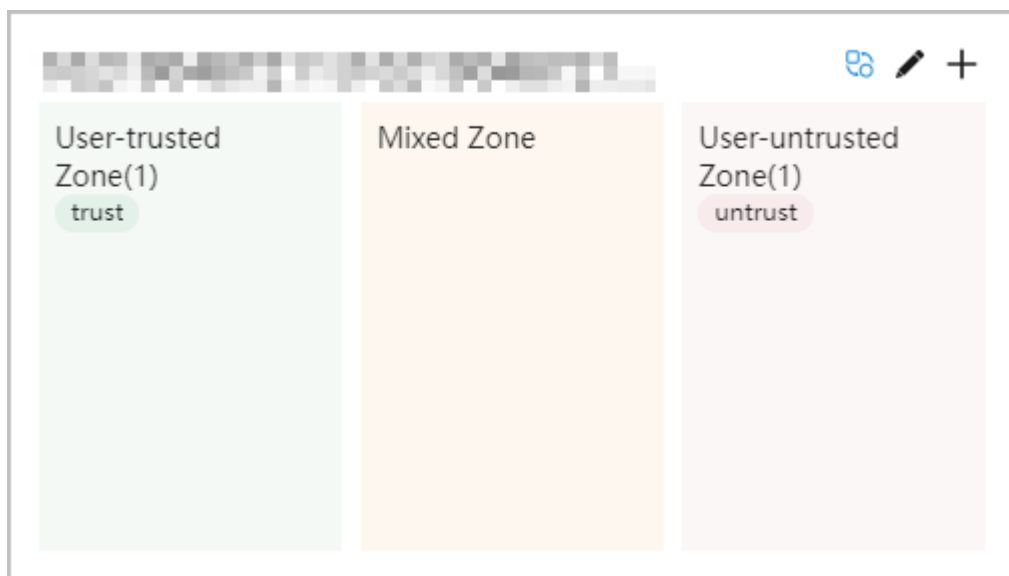
## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Click **Services** in the menu bar, and choose **IP Security Zone** from the navigation tree.
- Step 3** Check the device card in the **Device Security Zone** area.

### NOTE

If tenants see a message indicating that ports in the device security zones are reversely connected, it indicates the cables are incorrectly connected to the Qiankun Shield devices. In this case, tenants need to exchange the uplink and downlink interface connection on the local Qiankun Shield devices.

**Figure 2-47** Device security zones reversely connected



----End

## 2.4.6.2 Configuring a Global Whitelist


### Context

If the services running on some assets are of critical importance or some assets are free from security risks after confirmation, you can add the IP addresses of these assets to the global whitelist to prevent these IP addresses from being blacklisted.


After the IP address of an asset is added to the global whitelist, an IP address blacklist containing the IP address cannot be delivered to the Qiankun Shield

devices by Huawei Qiankun automatically or by its security operations experts. When a tenant delivers an IP address blacklist containing the IP address through blocking attack sources, isolating hosts, or configuring an IP address blacklist policy on Huawei Qiankun, Huawei Qiankun prompts the tenant whether to continue the delivery. The tenant determines whether to continue the delivery based on the requirements.

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Services** in the menu bar, and choose **IP Security Zone** from the navigation tree.
- Step 3** Create global whitelists from **Global Address Management > Global Whitelist**.

### NOTE

- To check the input rules of **IP Address/Range**, move the mouse cursor on the  icon.
- The name of a global whitelist can be customized. You can flexibly set multiple global whitelists (a maximum of 20 global whitelists can be created for a single zone) based on service requirements. However, the network segments in multiple global whitelists cannot overlap.
- You are advised to configure a global whitelist when the device is deployed in off-path mode to help the system identify threat events.

**Figure 2-48** Creating a global whitelist

**Create Global Whitelist** ×

! The global allowlist of a tenant takes effect for all devices of the tenant. IP addresses matching global allowlist entries will not be automatically blocked by the blocklist. You can set multiple network segments to protect your assets.

\*Name

Remarks


\*IP Address/Range ?   
10.3.3.3

Entered 2 / 200

Cancel Confirm

----End

### Follow-up Procedure


- You can click the global whitelists in the **Global Address Management** to modify the existing configuration.
- You can click the  icon next to the global whitelists in the **Global Address Management** to delete the existing configuration.

### 2.4.6.3 Configuring Untrusted Intranet Addresses


#### Context

The intranet addresses that are highly risky can be added to **Untrusted Intranet IP Address**. If Huawei Qiankun detects a risky intranet address, Huawei Qiankun matches the intranet address against those in **Untrusted Intranet IP Address**. If the intranet address is not found in **Untrusted Intranet IP Address**, Huawei Qiankun does not deliver the IP address as a blacklisted IP address to the device.

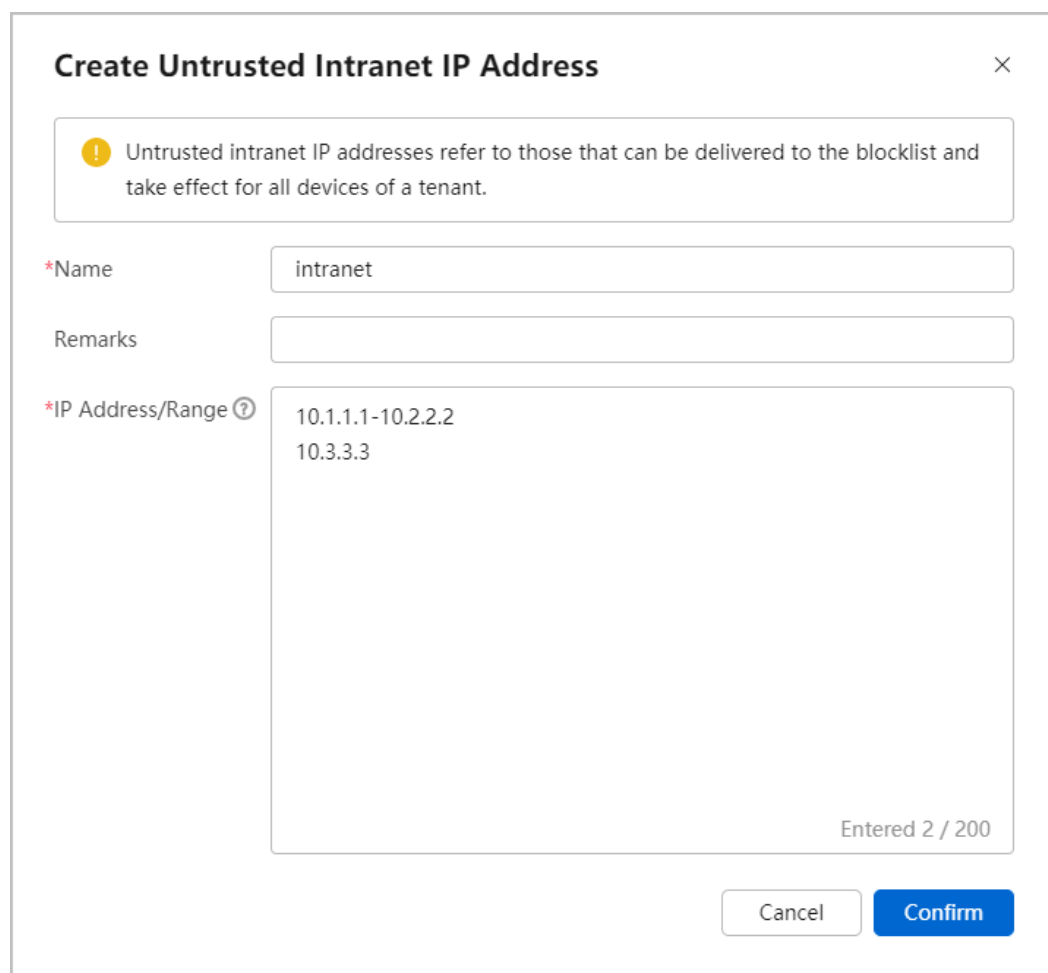
## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Click **Services** in the menu bar, and choose **IP Security Zone** from the navigation tree.
- Step 3** Configure untrusted intranet IP addresses from **Global Address Management** > **Untrusted Intranet IP Address**.


### NOTE

- To check the input rules of **IP Address/Range**, move the mouse cursor on the  icon.
- The name of an untrusted intranet IP address can be customized. You can flexibly set multiple untrusted intranet IP addresses based on service requirements (a maximum of 20 untrusted intranet IP addresses can be created for a single zone).

**Figure 2-49** Creating untrusted intranet IP addresses




**Create Untrusted Intranet IP Address** ×

 Untrusted intranet IP addresses refer to those that can be delivered to the blocklist and take effect for all devices of a tenant.

\*Name


Remarks

\*IP Address/Range    
10.3.3.3

Entered 2 / 200

----End

## Follow-up Procedure

- You can click untrusted intranet IP addresses in the **Global Address Management** to modify the existing configuration.
- You can click the  icon next to untrusted intranet IP addresses in the **Global Address Management** to delete the existing configuration.

### 2.4.6.4 Configuring Device Security Zones

#### Context


Huawei Qiankun needs to identify the security zones to which the attack source and destination belong for threat event analysis.

Huawei Qiankun provides the following types of security zones:

- **User-trusted Zone:** It is a security zone trusted by users. It usually refers to users' internal networks. Huawei Qiankun does not block **threat traffic** initiated from this zone.
- **Mixed Zone:** It is a special security zone between **User-trusted Zone** and **User-untrusted Zone** in terms of trust level. Huawei Qiankun does not block the **threat traffic** initiated from this zone.
- **User-untrusted Zone:** It is a security zone not trusted by users. It usually defines insecure networks such as the Internet. Huawei Qiankun automatically blocks the **threat traffic** initiated from this zone.

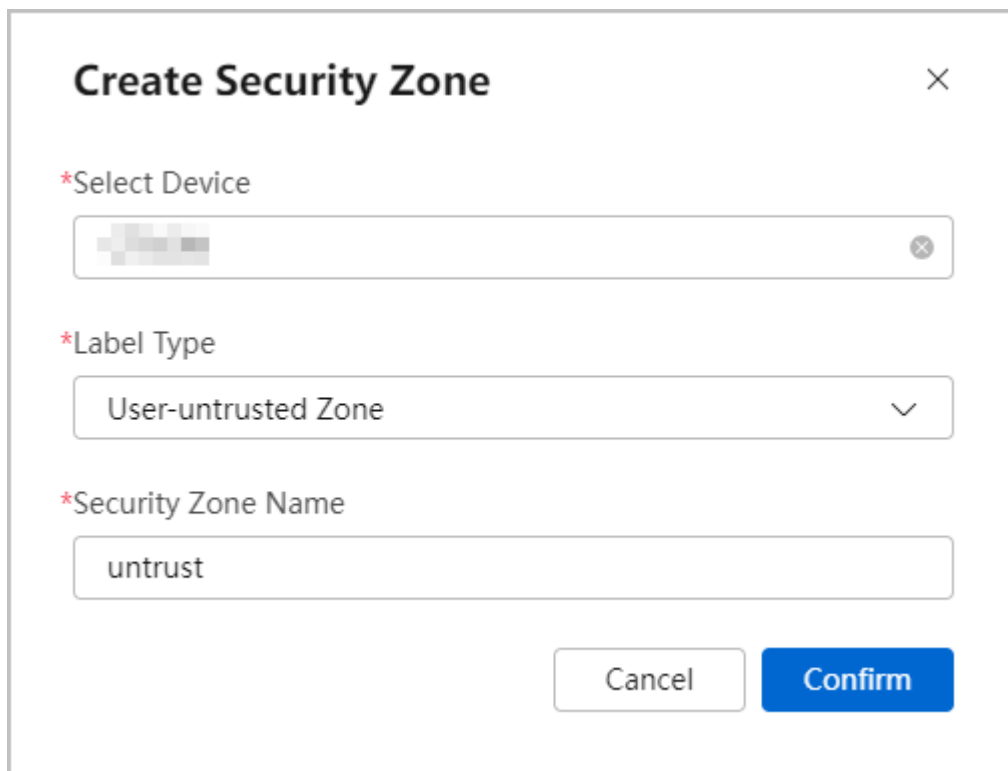
By default, Huawei Qiankun adds the trust zone and DMZ to **User-trusted Zone**, and the untrust zone to **Mixed Zone**. In addition, Huawei Qiankun adds other zones to the corresponding security zones (except **User-untrusted Zone**) based on threat events.

#### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Click **Services** in the menu bar, and choose **IP Security Zone** from the navigation tree.
- Step 3 Optional:** Click **Create** in the **Device Security Zone** area to add the corresponding security zones, for example untrust zone, to **User-untrusted Zone**.

If you want Huawei Qiankun to deliver the IP address blacklists containing the IP addresses of threat events, add the corresponding security zone to **User-untrusted Zone**.


**Figure 2-50** Creating a security zone



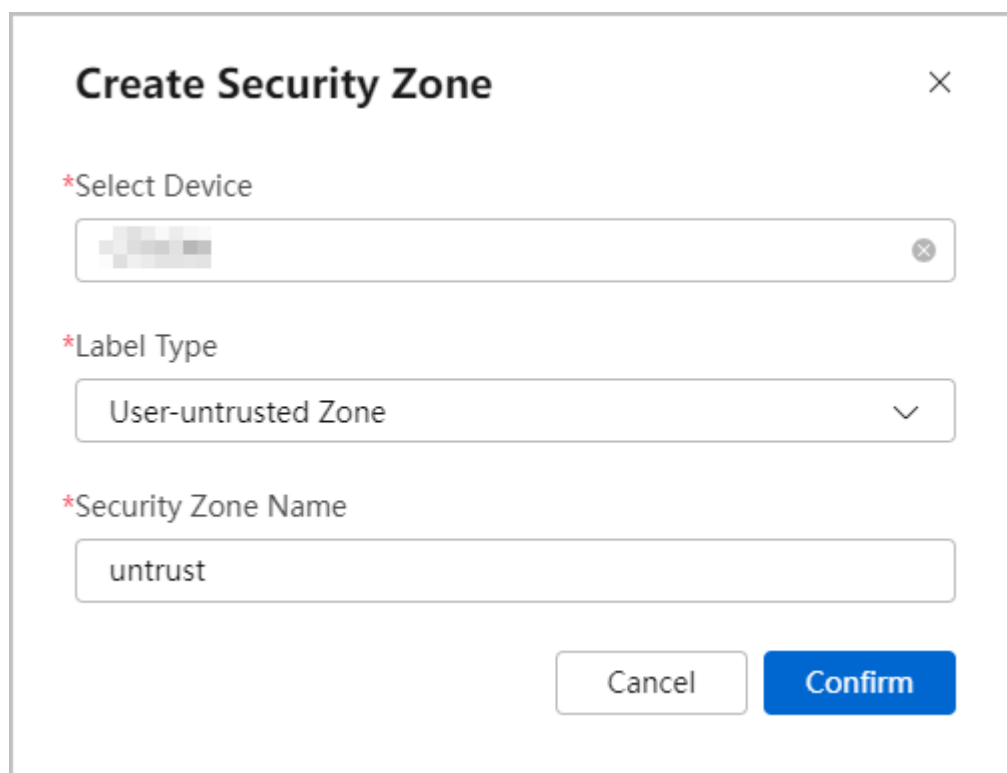
The image shows a 'Create Security Zone' dialog box with a close button (X) in the top right corner. It contains three required fields, each marked with a red asterisk:

- \*Select Device:** A text input field with a blurred placeholder and a clear button (X) on the right.
- \*Label Type:** A dropdown menu currently showing 'User-untrusted Zone' with a downward arrow on the right.
- \*Security Zone Name:** A text input field containing the text 'untrust'.

At the bottom right of the dialog are two buttons: a 'Cancel' button and a blue 'Confirm' button.

**Step 4 Optional:** Click  in the upper right corner of the device card, and drag security zones to different zones.

You can drag security zones to different zones based on requirements to help Huawei Qiankun determine threat events.

**Figure 2-51** Setting zone labels

**Create Security Zone**

\*Select Device

\*Label Type

User-untrusted Zone

\*Security Zone Name

untrust

Cancel Confirm

**Step 5** Click **Save** in the upper right corner of the device card to save the configurations.

----End

## 2.4.7 Authorization Management

### 2.4.7.1 Blacklist and Whitelist Authorization

#### Prerequisites

Perform the following steps to configure the address security domains. Then, perform blacklist and whitelist authorization so that Huawei Qiankun can correctly deliver the IP blacklists.

1. **Configuring Device Security Zones.**

Huawei Qiankun delivers an IP address blacklist for a threat event only when the threat event is initiated from **User-untrusted Zone**. Therefore, you need to add the corresponding security zone to **User-untrusted Zone**.

2. **Configuring a Global Whitelist.**

After the configuration, Huawei Qiankun cannot deliver an IP address in the global whitelist as a blacklisted IP address to the Qiankun Shield Device. This ensures that IP address blacklists can be delivered properly by Huawei Qiankun.

3. **Configuring Untrusted Intranet Addresses.**

After the configuration, Huawei Qiankun matches IP addresses in the IP address blacklist against those in **Untrusted Intranet IP Address**. If the IP

addresses are not found in **Untrusted Intranet IP Address**, Huawei Qiankun does not deliver the IP addresses as blacklisted IP addresses to the device.


## Context

Huawei Qiankun uses the automatic analysis model to analyze the logs provided by the device, and automatically delivers the IP address blacklist and domain name blacklist based on the analysis result. Huawei Qiankun can automatically deliver the IP address blacklist and domain name blacklist to a tenant's devices only after the tenant authorizes blacklist management.

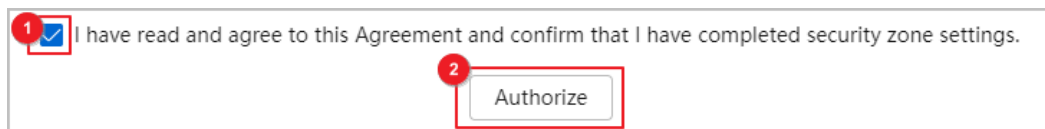
The default validity period of the blacklists automatically delivered by Huawei Qiankun is two days.

Currently, only top-level tenants have the permission to authorize blacklist and whitelist management.

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Click **Services** in the menu bar, and choose **Authorization > Blacklist and Whitelist Agreement**.
- Step 3** Perform authorization after verifying that the IP address security zone management is completed.

**Figure 2-52** Blacklist and whitelist authorization



----End

## Follow-up Procedure

After the function is authorized, you can perform the following operations:


- [Managing Blacklists and Whitelists](#).
- You can click **Cancel Authorization** or **Authorize** again at any time as required.

## 2.4.8 Configuring the Automatic Threat Blocking Duration

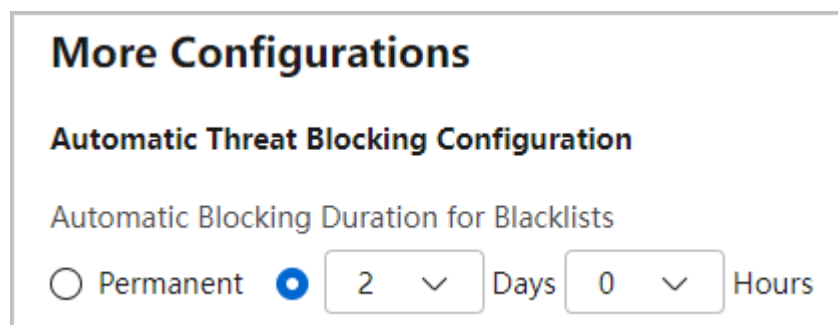
### Context

You can customize the blocking duration for the blacklists automatically delivered by Huawei Qiankun.

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Choose **Services > More Configurations**.
- Step 3** Configure the blocking duration.

**Figure 2-53** Automatic threat blocking configuration



----End


## 2.4.9 Configuring Custom Signature Authorization

### Context

Security operations expert can configure custom signatures as required and deliver the custom signatures to the device. The device then performs the actions preset in the custom signatures on traffic.

You need to enable custom signature authorization. After this function is enabled, Security operations expert can deliver custom signatures to a tenant's devices.

## Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services > Border Protection and Response**.
- Step 2** Choose **Services > More Configurations**.
- Step 3** Enable custom signature authorization.

**Figure 2-54** Custom signature authorization



----End

## 2.4.10 Configuring Metadata Detection and Protection Rules

### Prerequisites

- The metadata detection and function applies only to the USG6603F-C and USG6606F-C.
- The metadata detection function is supported only by the Border Protection and Response Service professional edition package.

### Context


Metadata is generated by extracting session and protocol information from original traffic. Huawei Qiankun can intelligently detect metadata to effectively defend against web attacks (including information disclosure, credential theft, injection detection, and DoS) and external connections in which malicious domain names are requested through the DNS protocol.

For important intranet assets, you can configure metadata detection and protection rules as required. Huawei Qiankun receives metadata based on the configured protected network segment and performs threat analysis based on the metadata to better protect important intranet assets.

According to whether protected network segments are configured, actions are taken as follows:

- For devices configured with protected network segments, collect the following data:
  - Metadata using HTTP and whose destination IP address is in the protected network segment.
  - Metadata using DNS and whose source IP address is in the protected network segment.
- Metadata is not collected for devices that are not configured with protected network segments.

### Procedure

- Step 1** Log in to the Huawei Qiankun console, and choose  > **My Services** > **Border Protection and Response**.
- Step 2** Choose **Services** > **Metadata Detection and Protection Rules** in the menu bar.
- Step 3** Click **Create** and create a metadata detection and protection rule as prompted.

**Figure 2-55** Creating a metadata detection and protection rule

Add Metadata Detection and Protection Rule

\*Select Device

USG6603F-C

\*Protected Network Segment ?

2.3

2.3

2 / 20

Cancel

Confirm

**Table 2-10** Key parameters

Parameter	Description
Select Device	Enter the device SN or device name for fuzzy search and select the device.
Protected Network Segment	<ul style="list-style-type: none"> <li>One protected network segment or range can be configured in each line.</li> <li>Lines are separated by carriage returns.</li> <li>The total number of protected IP addresses cannot exceed 65536.</li> <li>Only IPv4 addresses are supported.</li> </ul> For example: 127.0.0.1 127.0.0.1/24 127.0.0.2-127.0.0.10

----End

**Follow-up Procedure**

- After creating a metadata detection and protection rule, you can perform the following operations:
- Modify: Click **Modify** in the **Operation** column to modify an existing metadata detection and protection rule. You can only modify the protected network segment but cannot specify another device.
  - Delete: Click **Delete** in the **Operation** column to delete an existing metadata detection and protection rule.

## 2.4.11 Tenant Service Management by an MSP

### 2.4.11.1 Introduction to Tenant Service Management by an MSP

Managed service providers (MSPs) are organizations that provide network deployment, management, security detection, security protection, and O&M for tenants. Generally, MSPs have professional service management and maintenance capabilities.

After purchasing Huawei Qiankun, a tenant can entrust the management role to a professional MSP if the tenant is not equipped with comprehensive network construction, service management, and security O&M capabilities, to reduce the investment of manpower and capital of the enterprise. After tenants entrust services to MSPs, the MSPs perform routine management and periodic inspection on the services, handle exceptions and issues found during service running, and provide risk assessment and event handling suggestions.

A tenant account can establish agency relationships with multiple MSP accounts, and an MSP account can manage services of multiple tenant accounts.

Two modes of tenant service management by an MSP are available:

- Tenant-based management: An MSP directly accesses the tenant page on behalf of a tenant to perform operations.
- Service-based management: An MSP manages all tenants using a single service and implements operations.

The Border Protection and Response Service supports tenant service management by **Tenants** or **Services**.

### 2.4.11.2 Introduction to the MSP homepage

For details about the MSP home page, see section "[Introduction to the MSP Home Page](#)" in the *MSP Operation Guide*.

### 2.4.11.3 Performing Operations on Managed Services

#### Prerequisites

Tenants have entrusted MSPs to manage the Border Protection and Response Service. For details, see "[MSP-based Management](#)" in the *Common Tenant Operations*.

#### Context

The management operations by an MSP vary according to managed services. This section only describes the management operations by an MSP on the Border Protection and Response Service. For details about other common basic operations, such as personalized settings, rights- and domain-based management, tenant creation, service ticket creation, and log viewing, see [2.4.12.2 Basic MSP Operations](#).


The Border Protection and Response Service supports service management by **Tenants** or **Services**. Unless otherwise specified, the following part introduces service management by **Tenants**.

## Searching for and Following Tenants

**Step 1** Log in to the Huawei Qiankun console using an MSP account and click **Tenants** in the menu bar.

**Step 2** Perform related operations in the tenant list on the left.

- Search for a tenant.

Enter a tenant name in the search box and click the  icon on the left or press Enter.

- Check tenant information

Click the target tenant. The corresponding user information, such as the name, mobile number, and email address, is displayed on the right of the tenant list.


- Follow

Click **Follow** next to tenant names in the list and asterisks (\*) are displayed. If you do not need to follow the tenant names, click **Unfollow**.

- Add labels

Click **Add Label**. The label details are displayed below the tenant name in the list. To delete a label, click **x** next to the label.

- Filtering tenants

Click  in the upper right corner of the tenant list to filter tenants by label.

----End

## Entering and Exiting MSP-based Management

**Step 1** Log in to the Huawei Qiankun console using an MSP account and click **Tenants** in the menu bar.

**Step 2** Select a tenant to be managed in the tenant list on the left.

**Step 3** Enter and exit MSP-based management.

- Enter the management

Click **Enter Management View**. The MSP directly accesses the tenant page on behalf of a managed tenant. The management operations by an MSP are the same as the operations by a tenant.

- Exit the management

After the service management by an MSP is completed, click **Exit Management View** on the console home page. The MSP account page is displayed.

Figure 2-56 Exiting the management



----End

## Handling Threat Events

This section introduces MSP management by service.

- Step 1** Log in to the Huawei Qiankun console using an MSP account and click **Services** in the menu bar.
- Step 2** (Optional) Filter tenants by tenant name or label in the **Tenant List** area.
- Step 3** Click **View Details** on the right of the service card or tenant list.
- Step 4** Click **Threat Events** in the menu bar to handle threat events.

For details, see [Handling Threat Events](#).

----End

## Delivering IP Blacklists and Whitelists

This section introduces MSP management by service.

- Step 1** Log in to the Huawei Qiankun console using an MSP account and choose **Services > Border Protection and Response** in the menu bar.
- Step 2** (Optional) Filter tenants by tenant name or label in the **Tenant List** area.
- Step 3** Click **View Details** on the right of the service card or tenant list.
- Step 4** Click **Blacklist and Whitelist** in the menu bar.
- Step 5** The following describes how to deliver IP address blacklists in batches.

Choose **Device IP Blacklist > IP Address Blacklist**, click **Create**, set parameters, and deliver the IP address blacklists to devices of tenants in batches.

A maximum of 50 IP addresses separated by carriage return characters can be added at a time.

If the delivery is successful, the number of IP address blacklists that are successfully delivered is displayed. If the delivery fails, the detailed information about the IP address blacklists that fail to be delivered is displayed.

**Figure 2-57** Delivering IP address blacklists in batches

Create Blacklist

Class D IP addresses 224.0.0.0 to 239.255.255.255 cannot be delivered.

Select Device

Optional (4)

Enter a device name.

	Device Na...	Device SN	Workgroup
<input checked="" type="checkbox"/>			
<input checked="" type="checkbox"/>			
<input type="checkbox"/>			
<input type="checkbox"/>			

Total records: 4

1/1

Selected (0)

Enter a device name.

No records found.

Total records: 0

Source/Destination ☒ Source ☒ Destination

IP Address

1.1.1.1  
2.2.2.2  
3.3.3.3

3 / 50

Protocol

ANY

Port

ANY

Block Duration ☐ Permanent ☒ 2 Days 0 Hours 0 Minutes

☒ You are about to create a blacklist policy on the selected devices. After the policy is complete, the devices will block all access to the IP address. Are you sure you want to create it?


Cancel Confirm

----End

## Delivering Domain Name Blacklists

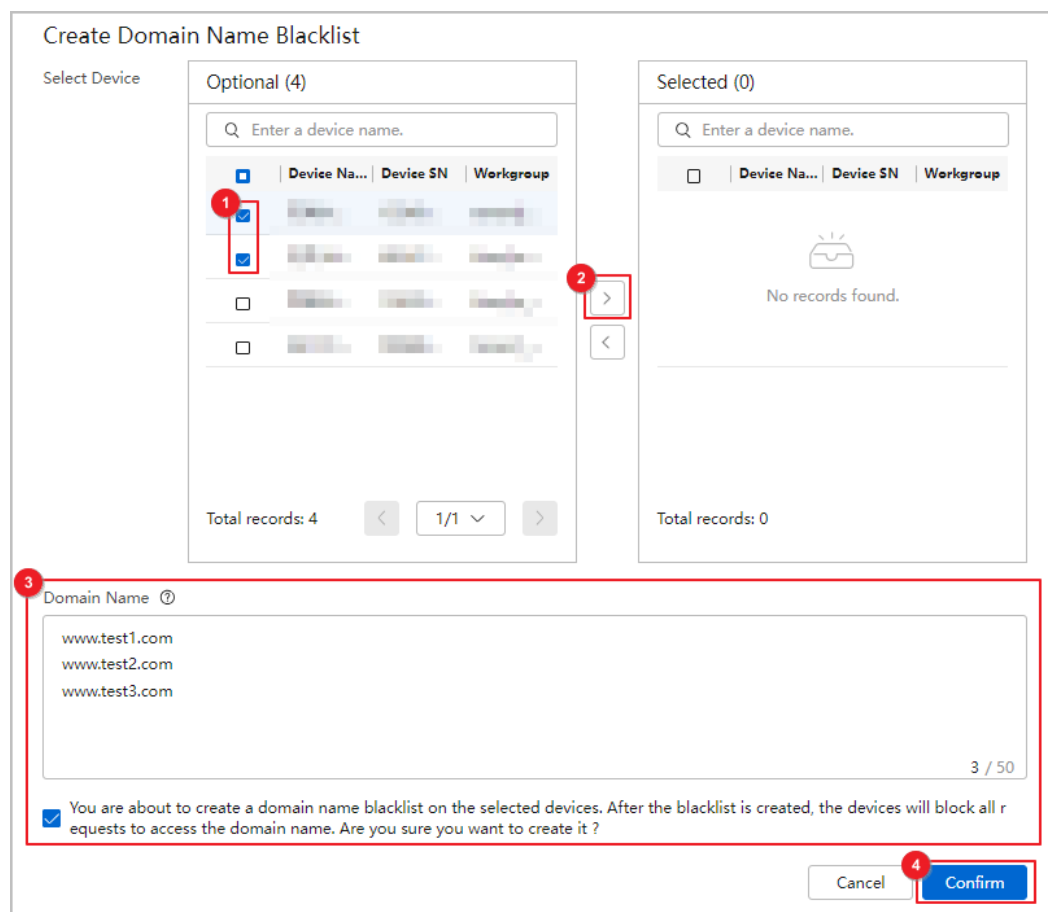
This section introduces MSP management by service.

- Step 1** Log in to the Huawei Qiankun console using an MSP account and choose **Services > Border Protection and Response** in the menu bar.
- Step 2** (Optional) Filter tenants by tenant name or label in the **Tenant List** area.
- Step 3** Click **View Details** on the right of the service card or tenant list.
- Step 4** Click **Blacklist and Whitelist** in the menu bar.
- Step 5** Choose **Device IP Blacklist > Domain Name Blacklist**, click **Create**, set parameters, and deliver the domain name blacklists to devices of tenants in batches.

A maximum of 50 domain names separated by carriage return characters can be added at a time. Domain names support regular expression matching. For details about the rules, move the mouse cursor over the  icon.


If the delivery is successful, the number of domain name blacklists that are successfully delivered is displayed. If the delivery fails, the detailed information about the domain name blacklists that fail to be delivered is displayed.

**Figure 2-58** Delivering domain name blacklists in batches



----End

## Checking Security Reports

- Step 1** Log in to the Huawei Qiankun console using an MSP account and click **Tenants** in the menu bar.
- Step 2** Select a tenant to be managed in the tenant list on the left.
- Step 3** Click **Enter Management View**. Then choose  > **My Services** > **Border Protection and Response**.
- Step 4** Click **Security Reports** in the menu bar to check the security reports.

For details, see [2.4.5 Checking Security Reports](#).

----End

## Creating a Custom Report

MSPs can specify a period to generate custom reports and push the reports to managed tenants. The MSP can use this function only during service management by **Services**.

- Step 1** Log in to the Huawei Qiankun console using an MSP account and choose **Services** > **Border Protection and Response** in the menu bar.
- Step 2** (Optional) Filter tenants by tenant name or label in the **Tenant List** area.
- Step 3** Click **View Details** on the right of the service card or tenant list.
- Step 4** Choose **Security Reports**, click the **Custom Report** tab, and click **Create**.
- Step 5** Set related parameters. Confirm and push the reports.

Figure 2-59 Customizing reports

**Confirm** [X]

\*Report Level... ☒ Individual Report

1 Time Range 2022-11-02 19:00 ~ 2022-11-03 19:00 [Calendar Icon]

\*Select Tenant

<input type="checkbox"/>	Tenant Name	Workgroup	Operation
2 <input checked="" type="checkbox"/>	[Redacted]	[Redacted]	Preview

3 [Cancel] [Confirm]

-----End

## Checking the Security Protection Dashboard

The MSP security protection dashboard displays data related to security events of all managed tenants.


- Step 1** Log in to the Huawei Qiankun console using an MSP account and click **Dashboard** in the menu bar.
- Step 2** **Optional:** Click  in the upper left corner of the page, filter tenants by label, and customize related data to be displayed.
- Step 3** Check the MSP security protection dashboard.

Figure 2-60 MSP security protection dashboard

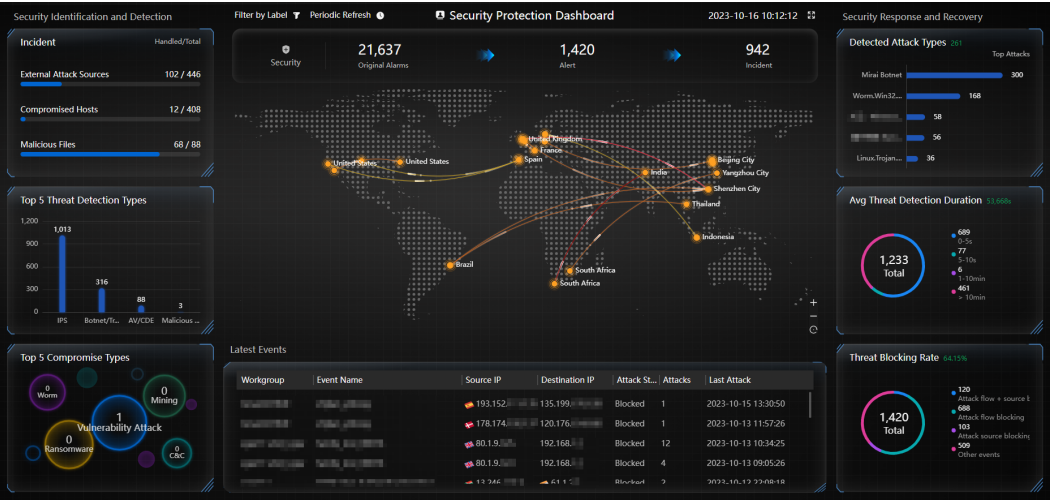


Table 2-11 Description of modules on the MSP security protection dashboard

Module	Description
Incident	Displays the numbers of handled and total external attack sources, compromised hosts, and malicious files.
Top 5 Threat Detection Types	Displays top 5 threat event types by quantity.
Top 5 Compromise Types	Displays top 5 causes leading to compromised hosts by quantity.
Security Events	Displays the number of security events of each type. <ul style="list-style-type: none"><li>● <b>Original Alarms:</b> Huawei Qiankun identifies original events based on threat logs provided by Qiankun Shield devices.</li><li>● <b>Alert:</b> Huawei Qiankun aggregates original events into alarm events after automatic model-based analysis and manual handling by security operations experts.</li><li>● <b>Incident:</b> After further intelligent analysis, Huawei Qiankun classifies alarm events into three types: external attack sources, compromised hosts, and malicious files.</li></ul>
Attack Map	Dynamically displays the source-to-destination attack direction and region distribution of the latest threat events.
Latest Events	Displays threat event information in reverse chronological order.
Detected Attack Types	Displays top 5 detected attack types by quantity.

Module	Description
Avg Threat Detection Duration	Displays the average time taken by Huawei Qiankun to detect threat events based on the logs reported by Qiankun Shield devices.
Threat Blocking Rate	<p>Displays information about threat event blocking.</p> <ul style="list-style-type: none"><li>• <b>Attack flow + source blocking:</b> displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies and blacklisted by Huawei Qiankun.</li><li>• <b>Attack flow blocking:</b> displays the number of threat events detected and blocked by Qiankun Shield devices based on security protection policies.</li><li>• <b>Attack source blocking:</b> displays the number of threat events to which Huawei Qiankun has delivered blacklists.</li><li>• <b>Other events:</b> displays the number of threat events that have not been handled.</li></ul>

----End

## Exporting the compromised Host Report

The MSP can use this function only during service management by **Services**.

- Step 1** Log in to the Huawei Qiankun console using an MSP account and choose **Services** > **Border Protection and Response** in the menu bar.
- Step 2** (Optional) Filter tenants by tenant name or label in the **Tenant List** area.
- Step 3** Click **View Details** on the right of the service card or tenant list.
- Step 4** Click **Threat Events** in the menu bar. Click **View More** in the upper right corner of the **Compromised Hosts** area.
- Step 5** Click **Export** and export the analysis report as prompted.

----End

## 2.4.12 More Operations

## 2.4.12.1 Basic Tenant Operations

**Table 2-12** Basic tenant operations

Operation	Scenario	Entry Point	Reference
Entrusting services to an MSP	You can entrust your services to an MSP for routine O&M by creating an agency request.	Click your account in the upper right corner of the console, and click <b>Agencies</b> .	<a href="#">Agency Management</a>
Creating a service ticket	When using a service, you can create service tickets if you encounter any problems. After receiving your service tickets, Huawei engineers will quickly analyze, locate, and resolve the problems.	Click your account in the upper right corner of the console, and click <b>Service Tickets</b> .	<a href="#">Service Ticket Management</a>
Creating a user	Huawei Qiankun supports rights- and domain-based management. You can create workgroups based on your organization structure and create users in the workgroups.	Click your account in the upper right corner of the console, and click <b>Permission Management</b> .	<a href="#">Creating a User</a>
Managing subscriptions	Huawei Qiankun allows you to subscribe to diverse service topics to quickly learn about the service running status, security reports, and alarms.	Click your account in the upper right corner of the console, and click <b>Subscriptions</b> .	<a href="#">Subscription Management</a>
Viewing logs	Logs include operation logs and security logs. You can view logs as required.	Click your account in the upper right corner of the console, and click <b>Logs</b> .	<a href="#">Viewing Logs</a>

## 2.4.12.2 Basic MSP Operations

Table 2-13 Basic MSP operations

Operation	Scenario	Entry Point	Reference
Logging in to the console	To use a service, you need to use an MSP account to log in to the console.	Visit Huawei Qiankun Marketplace and click <b>Log In</b> in the upper right corner for login.	<a href="#">Account Registration and Login to the Console</a>
Managing your personal information	You can customize your account information, including the username, password, email address, and profile picture.	Click your account in the upper right corner of the console, and click <b>Personal Center</b> .	<a href="#">Personal Center</a>
Managing MSP accounts	Rights- and domain-based management is supported. You can create workgroups based on your organization structure and create MSP accounts in the workgroups.	Click your account in the upper right corner of the console, and click <b>Permission Management</b> .	<a href="#">Account Management</a>
Managing tenants	You can create, query, modify, and export tenant information.	Click <b>Tenants</b> in the menu bar of the console.	<a href="#">Tenant Management</a>
Creating a service ticket	When using a service, you can create service tickets if you encounter any problems. After receiving your service tickets, Huawei Qiankun engineers will quickly analyze, locate, and resolve the problems.	Click your account in the upper right corner of the console, and click <b>Service Tickets</b> .	<a href="#">Service Ticket Management</a>
Viewing logs	Logs include operation logs and security logs.	Click your account in the upper right corner of the console, and click <b>Logs</b> .	<a href="#">Viewing Logs</a>

Operati on	Scenario	Entry Point	Reference
Viewing notices	You can check notices to learn about the latest service news, such as product notices, security notices, and upgrade notices.	Click your account in the upper right corner of the console, and click <b>Notices</b> .	<a href="#">Viewing Notices</a>