

**Huawei-Qiankun-Connector
V600R023C10**

Huawei Qiankun Connector Feature Package Usage Guide (USG6000F)

Issue 02
Date 2024-04-17



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.

Huawei Technologies Co., Ltd.

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

Website: <https://www.huawei.com>

Email: support@huawei.com

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

1 About This Document..... 1

2 Feature Package Installation Guide..... 6

2.1 Precautions for Installing a Feature Package..... 6

2.2 Installation Preparations..... 7

2.2.1 Preparing a Feature Package..... 7

2.2.2 Checking the Running System Software Version..... 7

2.2.3 Checking the Remaining Storage Space..... 8

2.3 Installation Procedure..... 9

2.3.1 Uploading or Downloading a Feature Package to a Device..... 9

2.3.1.1 Device Functioning as an FTP Server..... 9

2.3.1.2 Device Functioning as an FTP Client..... 11

2.3.1.3 Device Functioning as an SFTP Client..... 12

2.3.2 Installing a Feature Package..... 14

2.3.3 Verifying Feature Package Installation..... 14

2.4 Upgrading a Feature Package..... 15

2.5 Uninstalling a Feature Package..... 15

3 Cloud Service Usage Guide..... 17

3.1 Cloud Service Connection Configuration..... 17

3.1.1 Cloud Service Connection..... 17

3.1.2 Cloud Service Connection Principles..... 18

3.1.3 Configuration Precautions for Cloud Service Interconnection..... 19

3.1.4 Default Settings for Cloud Service Connection..... 20

3.1.5 Connecting the Device to Cloud Service..... 21

3.1.6 Example for Connecting the Device to Cloud Service..... 25

3.2 Huawei Qiankun Access Wizard (Public Cloud Scenario)..... 31

3.3 Huawei Qiankun Access Wizard (OP Scenario)..... 42

3.4 Cloud Service Configuration Commands..... 53

3.4.1 cloud-bwl access-key secret-access-key..... 53

3.4.2 cloud-bwl ca-certificate..... 54

3.4.3 cloud-bwl interval..... 55

3.4.4 cloud-bwl server..... 56

3.4.5 cloud-service ca-certificate..... 58

3.4.6 cloud-service enable.....	59
3.4.7 cloud-service host.....	60
3.4.8 cloud-service local-certificate.....	62
3.4.9 cloud-service logic-id.....	63
3.4.10 threat-protection cloud-authorization enable.....	64
3.5 Cloud Service Diagnostic Commands.....	66
3.5.1 display cloud-bwl.....	66
3.5.2 display log statistic type seccloud-log.....	69
3.5.3 reset log statistic type seccloud-log.....	71
3.6 Personal Data Description of Huawei Qiankun Connector.....	72

1 About This Document

Overview

This document describes how to use the cloud service feature, including installing the cloud service feature package, configuring the cloud service feature, and querying reference information, such as commands and logs.

By default, system software does not support cloud service. To use the cloud service function, install the cloud service feature package first.

The following table lists the product versions related to this document.

Product Name	Version
The USG6000F series have the following models: • USG6500F – USG6510F-D – USG6530F-D – USG6555F – USG6585F • USG6600F – USG6615F	V600R023C10

Content Conventions

The purchased products, services and features are stipulated by the contract made between Huawei Technologies Co., Ltd. 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.

Personal Data Declaration

Some personal data (such as MAC or IP addresses of terminals) may be obtained or used during operation or fault location of your purchased products, services, or features. Huawei does not independently collect or store user communication information. You are responsible for complying with applicable laws and regulations when enabling related functions used to collect or store user communication information. During user communication information usage and storage, proper measures must be taken to protect user communication information.

Disclaimer

In response to Customer's explicit request, Huawei makes commercially reasonable efforts to provide the cloud service feature (Feature):

Customer and its authorized parties shall, as required by applicable laws and regulations, provide the users, governmental bodies, and any other third parties with necessary information, and obtain and maintain all necessary consents, licenses, and authorizations, when using and maintaining Features. Applicable laws and regulations, user agreements, terms of use, privacy policy or statement, any other lawful agreements (Agreements), and publicly or targeted statements (Statements) shall not be violated. Huawei provides Features to Customer as per Customer's warrants to Huawei that Customer will use and maintain Features as permitted by applicable laws and regulations, Agreements and Statements. Huawei will not bear any legal obligations or liabilities, including but not limited to, claims, liabilities, obligations, costs, expenses, penalties, injunctions, and judgments that are not caused by Huawei's misconduct when Customer and its authorized parties are using and maintaining Features.

In the event that any governmental body adopts laws and regulations, or Customer signs agreements with third parties or makes statements, which materially affect the legitimacy of Features wholly or partially, or the provision of Features, Huawei reserves its right to, at its sole discretion, terminate the provision of Features without any liability to the extent permitted by law.

Symbol Conventions

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

Symbol	Description
	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Symbol	Description
	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Command Conventions

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

Convention	Description
Boldface	The keywords of a command line are in boldface .
<i>Italic</i>	Command arguments are in <i>italics</i> .
[]	Items (keywords or arguments) in brackets [] are optional.
{ x y ... }	Optional items are grouped in braces and separated by vertical bars. One item is selected.
[x y ...]	Optional items are grouped in brackets and separated by vertical bars. One item is selected or no item is selected.
{ x y ... } *	Optional items are grouped in braces and separated by vertical bars. A minimum of one item or a maximum of all items can be selected.
[x y ...] *	Optional items are grouped in brackets and separated by vertical bars. Several items or no item can be selected.
&<1-n>	The parameter before the & sign can be repeated 1 to n times.
#	A line starting with the # sign is comments.

GUI Conventions

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

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in boldface . For example, click OK .
>	Multi-level menus are in boldface and separated by the ">" signs. For example, choose File > Create > Folder .

MAC Address and Public IP Address Usage Declaration

For purposes of introducing features and giving configuration examples, the MAC addresses and public IP addresses of real devices are used in the product documentation. Unless otherwise specified, these addressees are used as examples only.

The IP addresses, URLs, and email addresses involved in open-source software comply with industry practices and open-source software usage specifications.

To implement functions and features, the device uses the public addresses listed below.

Table 1-1 Public address list

Public Address	Remarks
mgt.seccloud.huawei.com	Domain name of the controller, which is used by devices to proactively register with the controller and go online.
mgt.ctsgw.damddos.com	
cmcc.device.qiankun-saas.huawei.com	
unicom.secosou.qiankun-saas.huawei.com	
rd.seccloud.huawei.com	Domain name of the cloud service host, which is used to receive security logs and forensic data.
cmcc.dgs.qiankun-saas.huawei.com	

Default API Account

Default Account	Default Password	Applications
huawei	None	Huawei Qiankun Security Cloud Service uses this account to manage the device through NETCONF.

Default Account	Default Password	Applications
yundi	None	Huawei Qiankun Security Cloud Service uses this account to manage the device through NETCONF.

Update History

Updates between document issues are cumulative. Therefore, the latest document issue contains all updates made in previous issues.

2 Feature Package Installation Guide

This document describes the precautions, preparations, and procedure for feature package installation as well as the procedure for feature package uninstallation.

2.1 Precautions for Installing a Feature Package

2.2 Installation Preparations

2.3 Installation Procedure

2.4 Upgrading a Feature Package

2.5 Uninstalling a Feature Package

2.1 Precautions for Installing a Feature Package

Before installing a feature package, read the following precautions carefully:

- The system software package does not contain the functions in a feature package. Details are described in this document.
- For the USG6000F, a feature package must be uploaded or downloaded to the **flash:/** directory of the device.
- The version of a feature package must match that of the system software. Otherwise, the feature package cannot be successfully loaded.
- You are advised to install a feature package according to the following scenario-specific procedures.

Table 2-1 Scenario-specific procedures for feature package installation

Scenario	Installation Procedure
Install a feature package without upgrading the device or after the device is upgraded.	1. Upload or download a feature package to a device. 2. Configure the feature package to take effect immediately.

Scenario	Installation Procedure
Install a feature package and upgrade the device.	1. Upload or download a feature package to a device. 2. Configure the feature package to take effect at the next startup. 3. Upgrade the device.

- In hot standby scenarios, you need to install a feature package on both the active and standby devices.

2.2 Installation Preparations

2.2.1 Preparing a Feature Package

Procedure

- Step 1

Log in to <https://support.huawei.com/enterprise> to download the desired feature package according to [Table 2-2](#).

Table 2-2 Basic information about feature packages

Applicable Product	Feature Package Name	Applicable Software Version
• USG6510F-D • USG6530F-D • USG6555F • USG6585F • USG6615F	Huawei-Qiankun-Connector_V600R023C10 SPC100.ccx	V600R023C10

----End

2.2.2 Checking the Running System Software Version

Procedure

- Step 1

Check the running system software version of the device.

```
<HUAWEI> display version
Huawei Versatile Routing Platform Software
VRP (R) software, Version 8.20.0.1 (USG V600R023C10)
.....
```

- Step 2

Check whether a feature package has been installed on the device.

```
<HUAWEI> display startup
MainBoard:
Configured startup system software:      flash:/***.cc
Startup system software:                  flash:/***.cc
```

```
Next startup system software:      flash:/***.cc
Startup saved-configuration file:   flash:/vrpcfg.zip
Next startup saved-configuration file: flash:/vrpcfg.zip
Startup paf file:                  default
Next startup paf file:             default
Startup patch package:             NULL
Next startup patch package:        NULL
Startup feature software:        NULL    //The current device does not have any feature package
successfully loaded.
Next startup feature software:    NULL    //The current device does not have any feature package
to be loaded at the next startup.
```

----End

2.2.3 Checking the Remaining Storage Space

Context

The remaining storage space of a device must be larger than the size of the feature package to be uploaded or downloaded to the device.

Procedure

Step 1 Check the remaining storage space of the device.

Run the **dir** command in the user view to check the remaining storage space of the device.

```
<HUAWEI> dir
Directory of flash:/

Idx Attr   Size(Byte) Date      Time      FileName
 0 dr-x     - Dec 01 2020 15:06:06  $_checkpoint
 1 dr-x     - Dec 29 2020 04:03:11  $_install_mod
.....

2,388,152 KB total (2,113,828 KB free)
```

Step 2 (Optional) Delete unnecessary files.

If the remaining storage space of the device is less than the size of the feature package to be uploaded or downloaded to the device, delete unnecessary files.

NOTE

Before deleting a system software package (.cc), configuration file (.cfg, .zip, or .dat), license file (.dat or .zip), or patch file (.pat), ensure that it is no longer required.

- A file deleted using the **delete filename** command is placed into the recycle bin but still occupies space in the flash memory. To permanently delete files from the recycle bin, run the **reset recycle-bin** command, and the deleted files cannot be restored.
- A file deleted using the **delete /unreserved filename** command is permanently deleted without being placed into the recycle bin. This command is equivalent to running the **delete filename** command first and then the **reset recycle-bin** command.

Permanently delete the unnecessary file **test.txt** from the device.

```
<HUAWEI> delete /unreserved flash:/test.txt
```

----End

2.3 Installation Procedure

You are advised to install a feature package according to the following scenario-specific procedures.

Table 2-3 Scenario-specific procedures for feature package installation

Scenario	Installation Procedure
Install a feature package without upgrading the device or after the device is upgraded.	1. Upload or download a feature package to a device. 2. Configure the feature package to take effect immediately.
Install a feature package and upgrade the device.	1. Upload or download a feature package to a device. 2. Configure the feature package to take effect at the next startup. 3. Upgrade the device.

2.3.1 Uploading or Downloading a Feature Package to a Device

You can use one of the following methods to upload or download a feature package to a device.

2.3.1.1 Device Functioning as an FTP Server

Pre-configuration Tasks

Before using FTP to perform file operations, you have completed the following tasks:

- Ensure that there are reachable routes between a PC and the device.
- Ensure that the PC supports FTP client software.

In the following example, the device functions as an FTP server. The FTP username is **ftpuser**, the password is **YsHsjx_202206**, the device IP address is **10.1.1.1/24**, the PC IP address is **10.1.1.2/24**, and the FTP working directory is **flash:/**. You can change the settings according to the live-network plan.

NOTE

The FTP protocol has security risks. You are advised to use SFTP for file operations.

Procedure

Step 1 Configure a device as an FTP server.

Start the FTP service on the device, and set the FTP username to **ftpuser** and password to **YsHsjx_202206**.

```
<HUAWEI> system-view
[HUAWEI] ftp server enable
[HUAWEI] aaa
[HUAWEI-aaa] local-user ftpuser password irreversible-cipher YsHsjx_202206
[HUAWEI-aaa] local-user ftpuser service-type ftp
[HUAWEI-aaa] local-user ftpuser privilege level 3
Warning: This operation may affect online users, are you sure to change the user privilege level ? [Y/N]:Y
[HUAWEI-aaa] local-user ftpuser ftp-directory flash:/
[HUAWEI-aaa] return
```

NOTE

The user privilege level must be set to 3 so that the FTP connection can be successfully established.

Step 2 Access the FTP server from a PC.

NOTE

This example assumes that the PC runs a Windows operating system.

Save the feature package to be uploaded to a specified directory (for example, **D:**). Choose **Start > Run**. Enter **cmd** and press **Enter**. Enter **ftp 10.1.1.1**. Then enter the username and password as prompted, and press **Enter**. Set the file transfer mode to **binary**.

```
C:\Documents and Settings\Administrator>ftp 10.1.1.1
Connected to 10.1.1.1.
220 FTP service ready.
User(10.1.1.2:(none)): ftpuser //Enter the FTP username.
331 Password required for ftpuser.
Password: //Enter the FTP password.
230 User logged in.
ftp> binary //Set the file transfer mode to binary.
200 Type set to I.
```

Step 3 Upload the feature package from the PC to the device.

Run the **put local-filename [remote-filename]** command to upload the feature package from the PC to the **flash:/** directory of the device. After the feature package is uploaded, run the **bye** command to terminate the FTP connection.

```
ftp> put D:\Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
200 Port command okay.
150 Opening BINARY mode data connection for /Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
226 Transfer complete.
ftp> bye
221 Server closing.
```

Step 4 Check the operation result on the device.

Run the **dir** command on the device to check whether the feature package is uploaded to the specified directory.

```
<HUAWEI> dir
Directory of flash:/

Idx Attr  Size(Byte) Date    Time      FileName
39  -rw-   364,100  Mar 30 2021 10:57:34 Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
.....
```

----End

2.3.1.2 Device Functioning as an FTP Client

Pre-configuration Tasks

Before using FTP to perform file operations, you have completed the following tasks:

- Ensure that there are reachable routes between a PC and the device.
- Ensure that the FTP server program is installed on the PC.

In the following example, the device functions as an FTP client and the PC functions as an FTP server. The FTP username is **ftpuser**, the password is **YsHsjx_202206**, the PC IP address is **10.1.1.1/24**, and the device IP address is **10.1.1.2/24**. You can change the settings according to the live-network plan.

NOTE

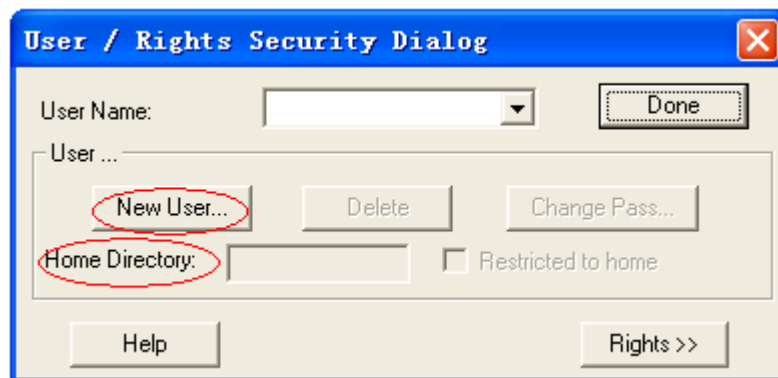
The FTP protocol has security risks. You are advised to use SFTP for file operations.

Procedure

Step 1 Configure a PC as an FTP server.

Run the FTP server program (for example, wftpd32) on the PC. Choose **Security > Users/rights**.

Figure 2-1 Configuring an FTP server



Click **New User** in the displayed dialog box, and set the username to **ftpuser** and password to **YsHsjx_202206**. Set **Home Directory** to the FTP working directory on the PC. In this example, the FTP working directory is **D:\ftp**. Click **Done** to close the dialog box. Do not exit the FTP server program when the feature package is being downloaded.

Step 2 Log in to the FTP server from the device.

```
<HUAWEI> ftp 10.1.1.1
Trying try 10.1.1.1 ...
Press CTRL + K to abort
Connected to try 10.1.1.1.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(ftp 10.1.1.1:(none)):ftpuser //Enter the FTP username.
331 Give me your password, please
Enter password: //Enter the FTP password.
230 Logged in successfully
```

```
[ftp] binary //Set the file transfer mode to binary.  
200 Type set to I.
```

Step 3 Download the feature package.

Run the **get** *local-filename* [*remote-filename*] command on the device to download the feature package from the FTP server (PC). After the feature package is downloaded, run the **bye** command to terminate the FTP connection.

```
[ftp] get Huawei-Qiankun-Connector_V600R023C10SPC100.ccx  
500 Unidentified command SIZE Huawei-Qiankun-Connector_V600R023C10SPC100.ccx  
200 PORT command okay  
..  
226 Transfer finished successfully.
```

Step 4 Check the operation result on the device.

Run the **dir** command on the device to check whether the feature package is downloaded to the specified directory.

```
<HUAWEI> dir  
Directory of flash:/  
  
Idx Attr   Size(Byte) Date      Time      FileName  
39  -rw-    364,100  Mar 30 2021 10:57:34 Huawei-Qiankun-Connector_V600R023C10SPC100.ccx  
.....  
  
----End
```

2.3.1.3 Device Functioning as an SFTP Client

Pre-configuration Tasks

Before using SFTP to perform file operations, you have completed the following tasks:

- Ensure that there are reachable routes between a PC and the device.
- Ensure that the SFTP server program is installed on the PC.

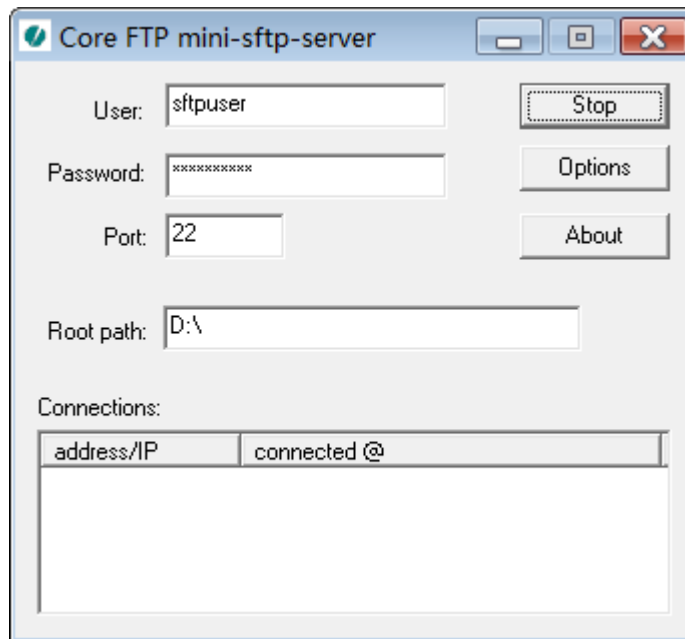
In the following example, the device functions as an SFTP client and the PC functions as an SFTP server. The SFTP username is **sftpuser**, the password is **YsHsjx_202206**, the device IP address is **10.1.1.2/24**, and the PC IP address is **10.1.1.1/24**. You can change the settings according to the live-network plan.

Procedure

Step 1 Configure a PC as an SFTP server.

Run the SFTP server program (for example, Core FTP mini-sftp-server) on the PC.

Figure 2-2 Configuring an SFTP server



In the displayed dialog box, set **User** to **sftpuser** and **Password** to **YsHsjx_202206**. Set **Root path** to the SFTP working directory on the PC. In this example, the SFTP working directory is **D:**. Do not exit the SFTP server program when the feature package is being downloaded.

Step 2 Log in to the SFTP server from the device.

```
<HUAWEI> system-view
[HUAWEI] ssh client first-time enable

[HUAWEI] sftp 10.1.1.1
Trying 10.1.1.1 ...
Press CTRL+K to abort
Connected to 10.1.1.1 ...
The server is not authenticated. Continue to access it? [Y/N]: y
Save the server's public key? [Y/N]: n

Please input the username: sftpuser //Enter the SFTP username.
Enter password: //Enter the SFTP password.
sftp-client>
```

Step 3 Download the feature package.

Run the **get local-filename [remote-filename]** command on the device to download the feature package from the SFTP server (PC). After the feature package is downloaded, run the **quit** command to terminate the SFTP connection.

```
sftp-client> get Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
Remote file: / Huawei-Qiankun-Connector_V600R023C10SPC100.ccx ---> Local file: Huawei-Qiankun-
Connector_V600R023C10SPC100.ccx
Downloading the file. Please wait.../
Downloading file successfully ended.
File download is completed in 1 seconds.
sftp-client> quit
```

Step 4 Check the operation result on the device.

Run the **dir** command on the device to check whether the feature package is downloaded to the specified directory.

```
<HUAWEI> dir
Directory of flash:/

Idx Attr   Size(Byte) Date      Time      FileName
39  -rw-    364,100  Mar 30 2021 10:57:34 Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
.....
```

----End

2.3.2 Installing a Feature Package

Feature packages can be installed using different methods. Select a method according to [2.1 Precautions for Installing a Feature Package](#).

- Configure the feature package to take effect immediately.
<HUAWEI> **install feature-software Huawei-Qiankun-Connector_V600R023C10SPC100.ccx**
- If an independent feature software package has been loaded to a device and the basic software package needs to be replaced, perform the following operations to specify an independent feature software package that takes effect at the next startup.

- a. Delete the current independent feature software package that takes effect at the next startup.

```
<HUAWEI> reset feature-software next-startup feature-file
```

NOTE

An independent feature software package is one that can be displayed in the **Next startup feature software** field of the **display startup** command output.

After the **reset feature-software next-startup** command is executed, the feature software package will not be installed upon the next startup. If a feature is not integrated in the next-startup basic software package, the feature configuration will be deleted during a startup. To prevent configuration loss, specify a feature software package that matches the next-startup basic software package before you restart the device. If a feature is integrated into the next-startup basic software package, it is automatically installed.

- b. Specify a next-startup basic software package.

```
<HUAWEI> startup system-software name
```

- c. (Optional) Specify a feature software package that matches the next-startup basic software package.

```
<HUAWEI> startup feature-software Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
```

2.3.3 Verifying Feature Package Installation

Run the **display startup** command to check whether the feature package is successfully installed.

```
<HUAWEI> display startup
MainBoard:
Configured startup system software:    flash:/***.cc
Startup system software:               flash:/***.cc
Next startup system software:          flash:/***.cc
Startup saved-configuration file:      flash:/vrpcfg.zip
Next startup saved-configuration file: flash:/vrpcfg.zip
Startup paf file:                      default
Next startup paf file:                 default
Startup patch package:                 NULL
Next startup patch package:            NULL
Startup feature software:           flash:/Huawei-Qiankun-Connector_V600R023C10SPC100.ccx //
Feature package that is successfully loaded to the current device
Next startup feature software:      flash:/Huawei-Qiankun-Connector_V600R023C10SPC100.ccx //
Feature package to be loaded at the next startup of the current device
```

If the feature package fails to be installed, no information about the feature package is displayed in the preceding command output.

2.4 Upgrading a Feature Package

Context

If a feature package has been installed and needs to be upgraded, you can perform a feature package upgrade.

Procedure

Step 1 Upgrade a feature package.

- Upgrading a feature package
<HUAWEI> **upgrade feature-software** Huawei-Qiankun-Connector_V600R023C10SPC100.ccx

If the specified feature package is of an earlier version, you can roll back the feature package.

Step 2 After upgrading a feature package, you can run the **display startup** command to check whether the operation is successful.

- Checking whether a feature package is successfully upgraded.

```
<HUAWEI> display startup
MainBoard:
Configured startup system software:    flash:/***.cc
Startup system software:               flash:/***.cc
Next startup system software:          flash:/***.cc
Startup saved-configuration file:      flash:/vrpcfg.zip
Next startup saved-configuration file: flash:/vrpcfg.zip
Startup paf file:                      default
Next startup paf file:                 default
Startup patch package:                 NULL
Next startup patch package:            NULL
Startup feature software:             flash:/Huawei-Qiankun-
Connector_V600R023C10SPC100.ccx //Feature package that is successfully loaded to the current
device
Next startup feature software:         flash:/Huawei-Qiankun-
Connector_V600R023C10SPC100.ccx //Feature package to be loaded at the next startup of the
current device
```

----End

2.5 Uninstalling a Feature Package

Context

If the functions provided by a feature package are no longer required, you can uninstall the feature package.

NOTE

After a feature package is uninstalled, the feature configuration will be deleted. Exercise caution when uninstalling a feature package.

Procedure

Step 1 Uninstall a feature package.

- Uninstalling a feature package
<HUAWEI> **uninstall feature-software** Huawei-Qiankun-Connector_V600R023C10SPC100.ccx

Step 2 After uninstalling a feature package, you can run the **display startup** command to check whether the operation is successful.

- Checking whether a feature package is successfully uninstalled

<HUAWEI> **display startup**

MainBoard:

```
Configured startup system software:    flash:/***.cc
Startup system software:                flash:/***.cc
Next startup system software:          flash:/***.cc
Startup saved-configuration file:      flash:/vrpcfg.zip
Next startup saved-configuration file:  flash:/vrpcfg.zip
Startup paf file:                      default
Next startup paf file:                 default
Startup patch package:                 NULL
Next startup patch package:            NULL
Startup feature software:           NULL //The current device does not have any feature package
successfully loaded.
Next startup feature software:      NULL //The current device does not have any feature
package to be loaded at the next startup.
```

----End

3 Cloud Service Usage Guide

- [3.1 Cloud Service Connection Configuration](#)
- [3.2 Huawei Qiankun Access Wizard \(Public Cloud Scenario\)](#)
- [3.3 Huawei Qiankun Access Wizard \(OP Scenario\)](#)
- [3.4 Cloud Service Configuration Commands](#)
- [3.5 Cloud Service Diagnostic Commands](#)
- [3.6 Personal Data Description of Huawei Qiankun Connector](#)

3.1 Cloud Service Connection Configuration

NOTE

In actual deployment, the onboarding process varies according to the networking scenario. For details about the end-to-end configuration process, see [Huawei Qiankun Product Documentation](#).

3.1.1 Cloud Service Connection

Definition

Cloud Service connection, a function of the Huawei Qiankun Security CloudService solution, works by connecting the device—the border protection node of the enterprise network—to the Huawei Qiankun Security CloudService platform deployed on Huawei Cloud. In this way, attacks and threats on the enterprise network can be analyzed in real time and protection policies can be automatically delivered to the device.

Purpose

The Huawei Qiankun Security CloudService solution is designed to address the enduring issues facing legacy network security solutions—for instance, weak protection and challenging security O&M. Connecting to the Huawei Qiankun Security CloudService platform, the device periodically collects information such as security logs and forensic data and reports the information to the platform. Then

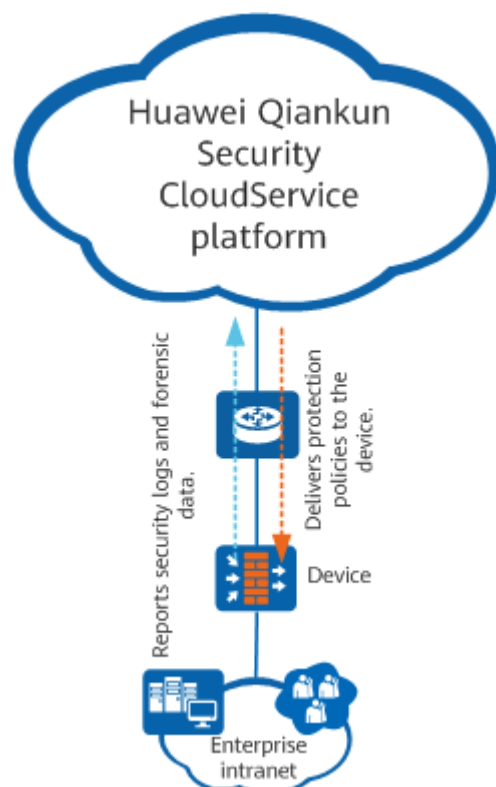
the platform analyzes the security of the information in real time, automatically delivers protection policies to the device based on the analysis results, and periodically sends data and reports to enterprise administrators via email or SMS.

3.1.2 Cloud Service Connection Principles

The Huawei Qiankun Security CloudService solution is designed to address the enduring issues facing legacy network security solutions—for instance, weak protection and challenging security O&M. The solution adopts an innovative cloud-edge integration architecture, comprising the cloud protection node at the network boundary of the enterprise and the Huawei Qiankun Security CloudService platform deployed on Huawei Cloud.

This solution offers cloud-based security services to enterprises through Firewall-as-a-Service (FWaaS) by connecting the device with the Huawei Qiankun Security CloudService platform. The device periodically collects information such as security logs and forensic data related to targeted attacks and threat events from both the enterprise intranet and Internet, and transmits the information to the platform. Then the platform analyzes the security of the information in real time, automatically delivers protection policies to the device based on the analysis results, and periodically sends data and reports to enterprise administrators via email or SMS.

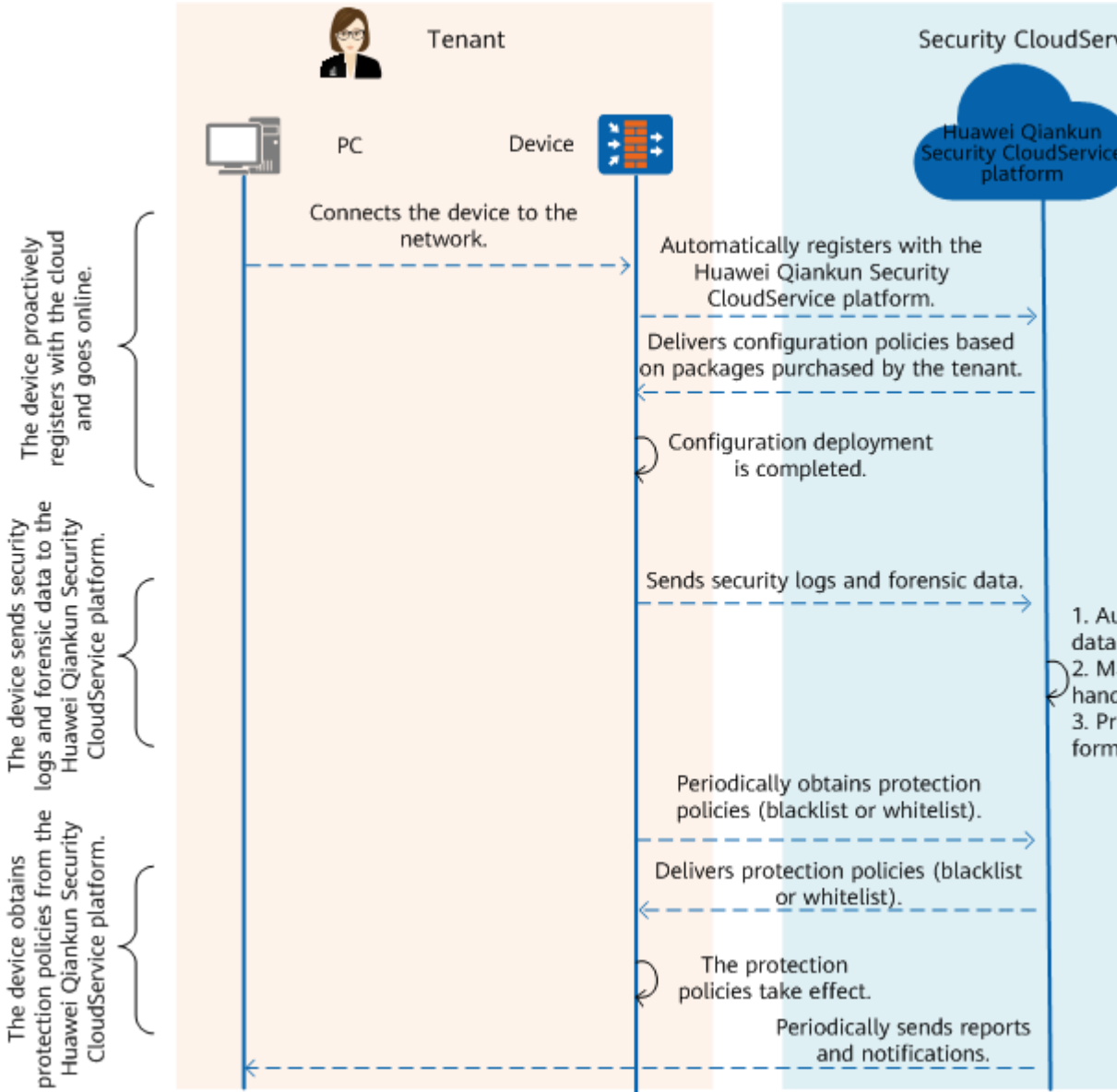
Figure 3-1 Device role in the Huawei Qiankun Security CloudService solution



In the Huawei Qiankun Security CloudService solution, the device serves as the cloud protection node and interworks with multiple service components on the cloud to complete key security actions, such as onboarding, sending security logs and forensic data, and obtaining the blacklist and whitelist. **Figure 3-2** illustrates

the service interaction process between the device and the Huawei Qiankun Security CloudService platform.

Figure 3-2 Service interaction between the device and the Huawei Qiankun Security CloudService platform



3.1.3 Configuration Precautions for Cloud Service Interconnection

Licensing Requirements

Cloud Service Connection is not under license control. Cloud service functions require purchasing a license to use them.

Hardware Requirements

Table 3-1 Hardware requirements

Series	Models
USG6500F	USG6510F-D/USG6530F-D/USG6555F/USG6585F
USG6600F	USG6615F

Feature Requirements

Table 3-2 Feature requirements

Feature Requirements	Series	Models
Maximum size of attack evidence collection packets for a single session. The maximum size of attack forensics packets for a single session is 100 KB.	USG6500F USG6600F	USG6510F-D/ USG6530F-D/ USG6555F/ USG6585F USG6615F
To use the log interconnection function of the security cloud service, you need to load the cloud service feature package. Otherwise, the function is unavailable.	USG6500F USG6600F	USG6510F-D/ USG6530F-D/ USG6555F/ USG6585F USG6615F

3.1.4 Default Settings for Cloud Service Connection

Table 3-3 lists the default settings for cloud service connection.

Table 3-3 Default settings for cloud service connection

Parameter	Default Settings
Cloud-based authorization mode	Disabled
Domain name or IP address of the cloud service host	The default domain name is mgt.seccloud.huawei.com .

Parameter	Default Settings
Sending security logs and forensic data	The default domain name used by the cloud service host to receive security logs and forensic data is rd.seccloud.huawei.com .
Obtaining the blacklist or whitelist from the cloud service host	Not configured
Sending traffic reports	Disabled

3.1.5 Connecting the Device to Cloud Service

Prerequisites

By default, devices cannot connect to Cloud Service. Before configuring Cloud Service connection parameters, log in to the Huawei technical support website, search for the corresponding product and version in the software download area, and download **Huawei-Qiankun-Connector_V600R023C10SPC100.ccx**. For details about how to install the feature package, see "Upgrade Maintenance Configuration" in CLI Configuration Guide > System Management Configuration.

Context

Log in to the web UI, choose **System > Startup Wizard**, and perform configurations. For details, see "Huawei Qiankun Access Wizard" in Web Configuration Guide > System. You can also run the following commands to perform configurations.

Procedure

Step 1 Enter the system view.

```
system-view
```

Step 2 Enable the cloud-based authorization mode.

```
threat-protection cloud-authorization enable
```

To connect the device to Cloud Service, enable the cloud-based authorization mode first.

After the cloud-based authorization mode is enabled on the device, the update service (IPS signature database update and antivirus signature database update) and URL remote query are controlled by the cloud. After the license expires, you need to renew the license on the cloud. Other function control items and resource control items are still controlled by the local license. The following describes some items for your reference:

- **IPS:** The IPS signature database can only be updated online, which is controlled by the cloud.
- **Antivirus:** The antivirus signature database can only be updated online, which is controlled by the cloud.

- URL filtering: Remote URL query is controlled by the cloud. Wait about one hour after the cloud-based authorization mode is enabled. After that, the device can successfully connect to the remote URL query server.

After the cloud-based authorization mode is disabled, the update service and remote URL query are controlled by the local license. The signature database can be updated locally or online.

Step 3 Configure the device to proactively register with the Huawei Qiankun Security CloudService platform in callhome mode.

1. Enter the NETCONF user interface view.

```
netconf
```

2. Set the NETCONF session model to YANG.

```
work-mode yang
```

3. Create a callhome template and enter the callhome template view.

```
callhome callhome-name
```

4. Create a NETCONF connection instance and enter the NETCONF connection instance view.

```
endpoint endpoint-name
```

5. Configure the IP address and TCP port number of the device management component of the Huawei Qiankun Security CloudService platform that establishes a NETCONF connection with the device.

```
peer-ip ip-address port port-number  
quit  
quit  
quit
```

Step 4 Configure the device to verify the CA certificate and local certificate of the Security CloudService host.

```
cloud-service ca-certificate ca-certificate-filename  
cloud-service local-certificate certificate-name
```

By default, the Huawei CA certificate **default_ca.cer** and local certificate **default_local.cer** are predefined on the device. To use the predefined certificates, run the **pki import-certificate default_ca realm default** and **pki import-certificate default_local realm default** command to import the certificates to the device memory, and then run the **cloud-service ca-certificate** and **cloud-service local-certificate** command.

To replace the certificate of the Security CloudService host, contact the administrator of Security CloudService. After the certificate is replaced, the Huawei Qiankun Security CloudService platform will notify the administrator via the Huawei Qiankun CloudService APP to update the corresponding certificate on the device.

To achieve this, upload a new certificate, import it into the device memory, and run the **cloud-service ca-certificate** command to replace the certificate.

In the case of a local certificate, upload the certificate and a key pair file, import them to the device memory, and then run the **cloud-service local-certificate** command to replace the certificate.

Step 5 Configure the device to send security logs and forensic data to Security CloudService.

With the intrusion prevention (such as attack forensics) and antivirus functions, the device can send security logs such as IPS threat logs and antivirus logs and attack forensic data (threat packets) to Security CloudService.

1. Configure the domain name or IP address of the Security CloudService host.

```
cloud-service host { domain domain-name | ip ip-address }
```

Only one host can be configured for the device. The new configuration overwrites the historical configuration.

2. Enable the function of sending domain name information in IPS threat logs.

```
cloud-service domain enable
```

3. Enable the function of sending attack forensic data.

```
cloud-service pcap enable
```

To view statistics about logs and forensic data sent to Security CloudService, run the **display log statistic type seccloud-log** command in the diagnostic view.

Step 6 Configure the device to send traffic reports to Security CloudService.

The device sends traffic reports to Security CloudService by email so that tenants can grasp the current network's traffic characteristics and bandwidth usage.

```
cloud-service traffic-report enable
```

To view statistics about traffic reports sent to Security CloudService, run the **display log statistic type seccloud-log** command in the diagnostic view.

Step 7 Configure the device to obtain the IP address blacklist or whitelist from Security CloudService.

1. Configure the domain name, IP address, or port number of the blacklist or whitelist server of Security CloudService.

```
cloud-bwl server { hostname host-name | ip ipv4-address | port port }
```

2. Configure an access key to securely connect to the blacklist or whitelist server of Security CloudService for authentication.

```
cloud-bwl { access-key access-key-id | secret-access-key secret-access-key }
```

3. Configure the CA certificate used by the device to communicate with the blacklist or whitelist server of Security CloudService.

```
cloud-bwl ca-certificate ca-certificate-name
```

The device obtains the blacklist or whitelist from its connected blacklist or whitelist server of Security CloudService through an HTTPS channel. Therefore, you need to specify the CA certificate for verifying the device's connectivity to the server. Otherwise, the blacklist or whitelist cannot be obtained.

Before running this command, apply for a certificate and upload it to the device. Then run the **pki import-certificate** command to import the certificate.

To view the blacklist or whitelist and obtaining status records acquired from Security CloudService, run the **display cloud-bwl { list | record }** command in the diagnostic view.

Step 8 Configure the device to obtain the domain name blacklist or whitelist from Security CloudService.

The device uses the threat information source function to periodically obtain the domain name blacklist or whitelist from Security CloudService through the HTTPS channel for domain name detection.

1. Enter the security telemetry view.
security-telemetry
2. Create a threat information source.
threat feed name *name*
3. Configure Security CloudService connection parameters in the threat information source.

Operation	Command	Description
Configure the Security CloudService URI for the device to request data.	uri <i>uri</i>	You need to obtain the URL from Security CloudService. The URL must start with https://.
Configure a local certificate.	local-certificate <i>certificate-name</i>	The local certificate is used by Security CloudService to verify the device identity. Before using the certificate, upload it to the device and run the following command to import the certificate to the memory: pki import-certificate local filename <i>local-certificate-name</i>
Configure a CA certificate.	ca-certificate <i>ca-certificate-file</i>	The CA certificate is used by the device to verify the Security CloudService identity. Before using the certificate, upload it to the device and run the following command to import the certificate to the memory: pki import-certificate ca filename <i>ca-certificate-name</i>
Configure a Security CloudService access ID.	access-id <i>access-id</i>	It is obtained from Security CloudService.
Configure a Security CloudService access key.	access-key <i>access-key</i>	It is obtained from Security CloudService.

Operation	Command	Description
Configure an interval for requesting data.	refresh interval <i>interval</i>	The device obtains data at the interval specified by <i>interval</i> .

4. Enable the threat information source.

```
status enable
```

After the configuration is complete, run the **display security-telemetry threat feed statistic** command to check the connection status between the device and Security CloudService and related statistics. Run the **display security-telemetry domain-reputation { blacklist | whitelist }** command to check the domain name blacklist or whitelist obtained by the device.

Step 9 Configure the device to send system logs to Security CloudService.

1. Enter the system view.

```
system-view
```

2. Configure the IP address, port number, VPN, and rate limit for the device to receive system logs.

```
sec-log server source { ipv4 ipv4_address | ipv6 ipv6_address } port port_number [ vpn-instance vpn-instance-name ] [ car car-value ]
```

3. Enter the security telemetry view.

```
security-telemetry
```

4. Configure the types of data to be collected.

```
collect syslog
```

If you run this command multiple times, all configurations take effect.

5. Create a destination to receive data, and specify the CA certificate that verifies the received data as well as the IP address, port number, or VPN information of the destination system.

```
destination-group destination-name  
ca-certificate ca-certificate-file  
ipv4-address ipv4-address [ port port ] [ vpn-instance vpn-name ]
```

6. Create a sensor group to specify the types of data to be collected and reported to the destination system.

```
sensor-group sensor-name  
select syslog
```

If you run the **select syslog** command multiple times, all configurations take effect.

7. Create a subscription task, associate it with the destination group and sensor group, and specify the local certificate. Use a local certificate to identify the device whose data is sent to a destination system.

```
subscription subscription-name  
destination-group destination-name  
sensor-group sensor-name  
local-certificate certificate-name
```

----End

3.1.6 Example for Connecting the Device to Cloud Service

Networking Requirements

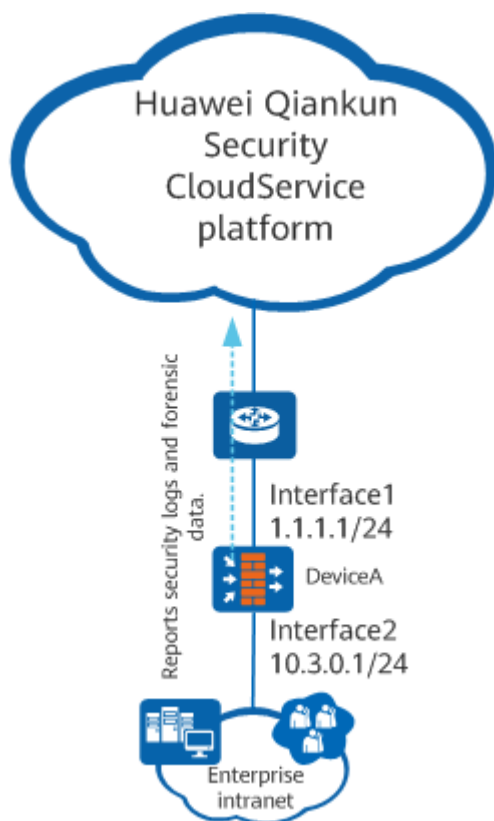
In [Figure 3-3](#), an enterprise has deployed DeviceA as a security gateway at the intranet border to allow Intranet users to access the web server on the Internet.

Connecting to the Huawei Qiankun Security CloudService platform, DeviceA periodically sends security logs to the platform. Then the platform analyzes the security of the logs in real time, automatically delivers protection policies to the device based on the analysis results, and periodically sends data and reports to enterprise administrators via email or SMS.

Figure 3-3 Connection between the device and Huawei Qiankun Security CloudService platform

NOTE

Interface1 and interface2 stand for 10GE1/0/1 and 10GE1/0/2, respectively.



Configuration Roadmap

1. Configure the device to access the Internet using a static IPv4 address.
2. Create a security policy.
3. Configure the Cloud Service connection parameters.

NOTE

This example describes only the configuration on the local device. For the configuration on Security CloudService, contact the administrator.

Procedure

1. Configure the device to access the Internet using a static IPv4 address. For details, see "CLI: Example for Accessing the Internet Using a Static IPv4 Address" in Typical Configuration Examples > Accessing the Internet Using One Interface.

2. Configure IPS and antivirus profiles.

```
[DeviceA] profile type ips name IPS_default  
[DeviceA-profile-ips-IPS_default] collect-attack-evidence enable  
[DeviceA-profile-ips-IPS_default] signature-set name default  
[DeviceA-profile-ips-IPS_default-default] os unix-like windows android ios other  
[DeviceA-profile-ips-IPS_default-default] target both  
[DeviceA-profile-ips-IPS_default-default] severity low medium high  
[DeviceA-profile-ips-IPS_default-default] protocol all  
[DeviceA-profile-ips-IPS_default-default] category all  
[DeviceA-profile-ips-IPS_default-default] quit  
[DeviceA-profile-ips-IPS_default] quit  
[DeviceA] profile type av name AV_default  
[DeviceA-profile-av-AV_default] collect-attack-evidence enable  
[DeviceA-profile-av-AV_default] quit
```

3. Create security policy **local_cloud** to allow the device to send security logs to Security CloudService.

```
[DeviceA] security-policy  
[DeviceA-policy-security] rule name local_cloud  
[DeviceA-policy-security-rule-local_cloud] source-zone local  
[DeviceA-policy-security-rule-local_cloud] destination-zone untrust  
[DeviceA-policy-security-rule-local_cloud] destination-zone trust  
[DeviceA-policy-security-rule-local_cloud] policy logging  
[DeviceA-policy-security-rule-local_cloud] action permit  
[DeviceA-policy-security-rule-local_cloud] quit  
[DeviceA-policy-security] quit
```

4. Create security policy **rule_iss_dns** to connect the device to the DNS server.

```
[DeviceA] security-policy  
[DeviceA-policy-security] rule name rule_iss_dns  
[DeviceA-policy-security-rule-rule_iss_dns] source-zone local  
[DeviceA-policy-security-rule-rule_iss_dns] destination-zone trust  
[DeviceA-policy-security-rule-rule_iss_dns] destination-zone untrust  
[DeviceA-policy-security-rule-rule_iss_dns] service dns  
[DeviceA-policy-security-rule-rule_iss_dns] policy logging  
[DeviceA-policy-security-rule-rule_iss_dns] action permit  
[DeviceA-policy-security-rule-rule_iss_dns] quit  
[DeviceA-policy-security] quit
```

5. Create security policy **trust_untrust** to protect intranet users from threats when they access the Internet.

```
[DeviceA] security-policy  
[DeviceA-policy-security] rule name trust_untrust  
[DeviceA-policy-security-rule-trust_untrust] source-zone trust  
[DeviceA-policy-security-rule-trust_untrust] destination-zone untrust  
[DeviceA-policy-security-rule-trust_untrust] policy logging  
[DeviceA-policy-security-rule-trust_untrust] profile AV_default  
[DeviceA-policy-security-rule-trust_untrust] profile IPS_default  
[DeviceA-policy-security-rule-trust_untrust] action permit  
[DeviceA-policy-security-rule-trust_untrust] quit  
[DeviceA-policy-security] quit
```

6. Create security policy **untrust_trust** to protect extranet users from threats when they access the intranet.

```
[DeviceA] security-policy  
[DeviceA-policy-security] rule name untrust_trust  
[DeviceA-policy-security-rule-untrust_trust] source-zone untrust  
[DeviceA-policy-security-rule-untrust_trust] destination-zone trust  
[DeviceA-policy-security-rule-untrust_trust] policy logging  
[DeviceA-policy-security-rule-untrust_trust] profile AV_default  
[DeviceA-policy-security-rule-untrust_trust] profile IPS_default  
[DeviceA-policy-security-rule-untrust_trust] action permit  
[DeviceA-policy-security-rule-untrust_trust] quit  
[DeviceA-policy-security] quit
```

7. Create a PKI domain.

```
[DeviceA] pki realm cloud-bwls  
[DeviceA] pki realm cloud_hupo  
[DeviceA] pki realm default
```

8. Configure the SSH user and SSH server.

```
[DeviceA] ssh user huawei
[DeviceA] ssh user huawei authentication-type x509v3-rsa
[DeviceA] ssh user huawei assign pki default
[DeviceA] ssh user huawei service-type netconf
[DeviceA] ssh authorization-type default root
[DeviceA] ssh server publickey x509v3-ssh-rsa
[DeviceA] ssh server assign pki default
[DeviceA] ssh client publickey x509v3-ssh-rsa rsa_sha2_256 rsa_sha2_512
```

9. Configure an SSL policy for the gRPC client.

```
[DeviceA] ssl policy default
[DeviceA-ssl-policy-default] quit
[DeviceA] grpc
[DeviceA-grpc] grpc client
[DeviceA-grpc-client] ssl-policy default
[DeviceA-grpc-client] quit
```

10. Configure the device to proactively register with the Huawei Security CloudService platform in callhome mode. **peer** is the domain name of the device management component in the platform and needs to be obtained from the administrator.

```
[DeviceA] netconf
[DeviceA-netconf] work-mode yang
[DeviceA-netconf] callhome cloud-service
[DeviceA-netconf-callhome-cloud-service] endpoint cloud-service
[DeviceA-netconf-callhome-cloud-service-endpoint-cloud-service] peer mgt.seccloud.huawei.com
port 10020
[DeviceA-netconf-callhome-cloud-service-endpoint-cloud-service] quit
[DeviceA-netconf-callhome-cloud-service] quit
[DeviceA-netconf] quit
[DeviceA] quit
```

11. Install the Huawei Qiankun connector feature package.

To configure Security CloudService connection parameters, install the Huawei Qiankun connector feature package first.

Log in to Huawei technical support website, search for the corresponding product and version in the software download area, download the **Huawei-Qiankun-Connector_V600R023C10SPC100.ccx** Huawei Qiankun connector feature package, and upload it to the device.

```
<DeviceA> install feature-software Huawei-Qiankun-Connector_V600R023C10SPC100.ccx
Info: Operating, please wait for a moment....done.
Info: Succeeded in installing the feature.
```

12. Enable the cloud-based authorization mode.

```
<DeviceA> system-view
[DeviceA] threat-protection cloud-authorization enable
```

13. Configure the device to verify the CA certificate or local certificate of the Security CloudService host.

```
[DeviceA] cloud-service ca-certificate default_ca.cer
[DeviceA] cloud-service local-certificate default_local.cer
```

By default, the Huawei CA certificate **default_ca.cer** and local certificate **default_local.cer** are predefined on the device. To replace the certificate of the Security CloudService host, contact the administrator of Security CloudService. After the certificate is replaced, the Huawei Security CloudService platform will notify the administrator via the Huawei Qiankun CloudService APP to update the corresponding certificate on the device. To achieve this, upload a new certificate, run the **pki import-certificate** command to import the certificate, and then run the preceding commands to replace the certificate.

14. Enable the function of sending traffic reports.

```
[DeviceA] cloud-service traffic-report enable
```

15. Set the domain name used by the Security CloudService host to receive security logs and forensic data to **rd.seccloud.huawei.com**, and enable the function of sending attack forensic data externally. The address for collecting logs of Security CloudService can be obtained from the administrator of the Huawei Qiankun Security CloudService platform.
[DeviceA] **cloud-service host domain rd.seccloud.huawei.com**
[DeviceA] **cloud-service pcap enable**
16. Configure the blacklist or whitelist function.
[DeviceA] **firewall blacklist enable**
[DeviceA] **firewall whitelist enable**
17. Configure the domain name of the Security CloudService blacklist or whitelist server. Use the default port number for the device to obtain the blacklist or whitelist from Security CloudService.
[DeviceA] **cloud-bwl server hostname www.hostname.com**
18. Configure an access key to securely connect to the blacklist or whitelist server of Security CloudService for authentication.
[DeviceA] **cloud-bwl access-key KtUEj8ySfi4qvAdgZ7XzoBRilnZ5AcJqfW70ciOL**
[DeviceA] **cloud-bwl secret-access-key 2950055747b74d0db848e87d3761fd77**
19. Configure the CA certificate used by the device to communicate with the blacklist or whitelist server of Security CloudService.
[DeviceA] **cloud-bwl ca-certificate huawei_ca.cer**

NOTE

- The device obtains the blacklist or whitelist from its connected blacklist or whitelist server of Security CloudService through an HTTPS channel. Therefore, you need to specify the CA certificate for verifying the device's connectivity to the server. Otherwise, the blacklist or whitelist cannot be obtained.
- Before running this command, apply for a certificate and upload it to the device. Then run the **pki import-certificate huawei_ca.cer** command to import the certificate.

Verification

- Run the **display log statistic type seccloud-log** command in the diagnostic view to check statistics about logs sent to the server of Security CloudService.
- Run the **display cloud-bwl list** command in the diagnostic view to check the blacklist and whitelist obtained from Security CloudService.

Configuration Scripts

```
#
sysname DeviceA
#
profile type ips name IPS_default
collect-attack-evidence enable
signature-set name default
os unix-like windows android ios other
target both
severity low medium high
protocol all
category all
profile type av name AV_default
collect-attack-evidence enable
#
security-policy
rule name untrust_trust
source-zone untrust
destination-zone trust
policy logging
```

```

profile av AV_default
profile ips IPS_default
action permit
rule name trust_untrust
source-zone trust
destination-zone untrust
policy logging
profile av AV_default
profile ips IPS_default
action permit
rule name local_cloud
source-zone local
destination-zone trust
destination-zone untrust
policy logging
action permit
rule name rule_iss_dns
source-zone local
destination-zone trust
destination-zone untrust
service dns
policy logging
action permit
#
ssh user huawei
ssh user huawei authentication-type x509v3-rsa
ssh user huawei assign pki default
ssh user huawei service-type snetconf
ssh authorization-type default root
ssh server publickey x509v3-ssh-rsa
ssh server assign pki default
ssh client publickey x509v3-ssh-rsa rsa_sha2_256 rsa_sha2_512
#
ssl policy default
grpc
grpc client
  ssl-policy default
#
pki realm cloud-bwls
pki realm cloud_hupo
pki realm default
#
firewall blacklist enable
firewall whitelist enable
#
netconf
callhome cloud-service
  endpoint cloud-service
  peer-ip 2.2.2.2 port 10020
work-mode yang
#
threat-protection cloud-authorization enable
#
cloud-service traffic-report enable
cloud-service host ip 3.3.3.3
cloud-service pcap enable
#
cloud-bwl server hostname www.hostname.com
cloud-bwl access-key %+%######!!!!$!!!!*!!!!iyYB~@1nn{C)H&f{FWM3(-T*Q]V9DDXtkKL\|Z7d:Tx0}lq/K!!!!!!%+%#
cloud-bwl secret-access-key %+%######!!!!$!!!!
*4c93*19Bd.<JoooSOtl"LKLq""1Ob{Hgw4#B8;AoN6}QTHiN*)@[_(\U%+%#
cloud-bwl ca-certificate huawei ca.cer

```

3.2 Huawei Qiankun Access Wizard (Public Cloud Scenario)

Context

To address issues such as inadequate protection and challenging security O&M associated with traditional network security solutions, Huawei launches Huawei Qiankun Security CloudService. Huawei Qiankun Security CloudService adopts an innovative cloud-edge integration architecture, and comprises the security cloud service platform deployed on Huawei Cloud and the cloud protection node deployed at the enterprise network edge.

In the Huawei Qiankun Security CloudService Solution, the cloud service platform collaborates with devices to provide cloud-based security services in firewall-as-a-service mode. Devices regularly gather security logs and forensic data related to targeted attacks and threat events from both the enterprise intranet and Internet. This information is then transmitted to the cloud service platform. The platform then uses the big data platform to perform real-time security analysis on the logs and data, automatically delivers protection policies to the devices based on the analysis results, and periodically sends the protection data and reports to enterprise administrators through emails or SMS messages for data and report display.

NOTE

Only the USG6615F, USG6510F-D, USG6530F-D, USG6585F, and USG6555F support this configuration.

NOTE

- Only level-3 administrators (system administrators) can view and configure the Huawei Qiankun access wizard.
- Huawei Qiankun Security CloudService depends on the Huawei Qiankun Connector feature package. Therefore, install the Huawei Qiankun Connector feature package first. Obtain the Huawei Qiankun Connector feature package from Huawei support website. For details about how to install the feature package, see Configuring the Feature Package.

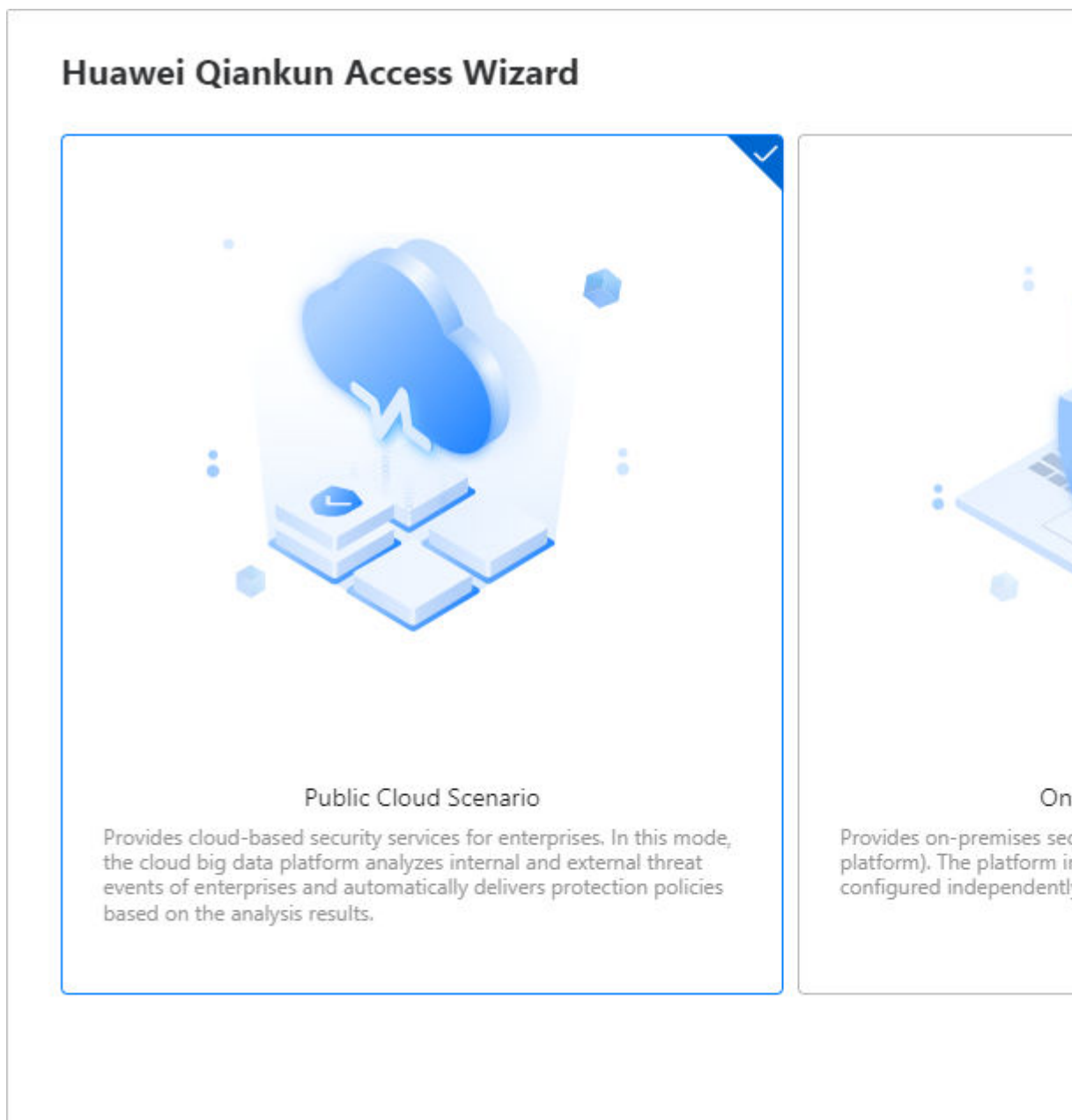
Procedure

Step 1 Choose **System > Huawei Qiankun Access Wizard**. The wizard page is displayed.

Alternatively, choose **System > System Upgrade** and click **Huawei Qiankun Access Wizard** in the **Huawei Qiankun Connector Package** operation list to access the wizard page.

Step 2 Select **Public Cloud Scenario**.

Click **Next** to access the **Preparation** page.

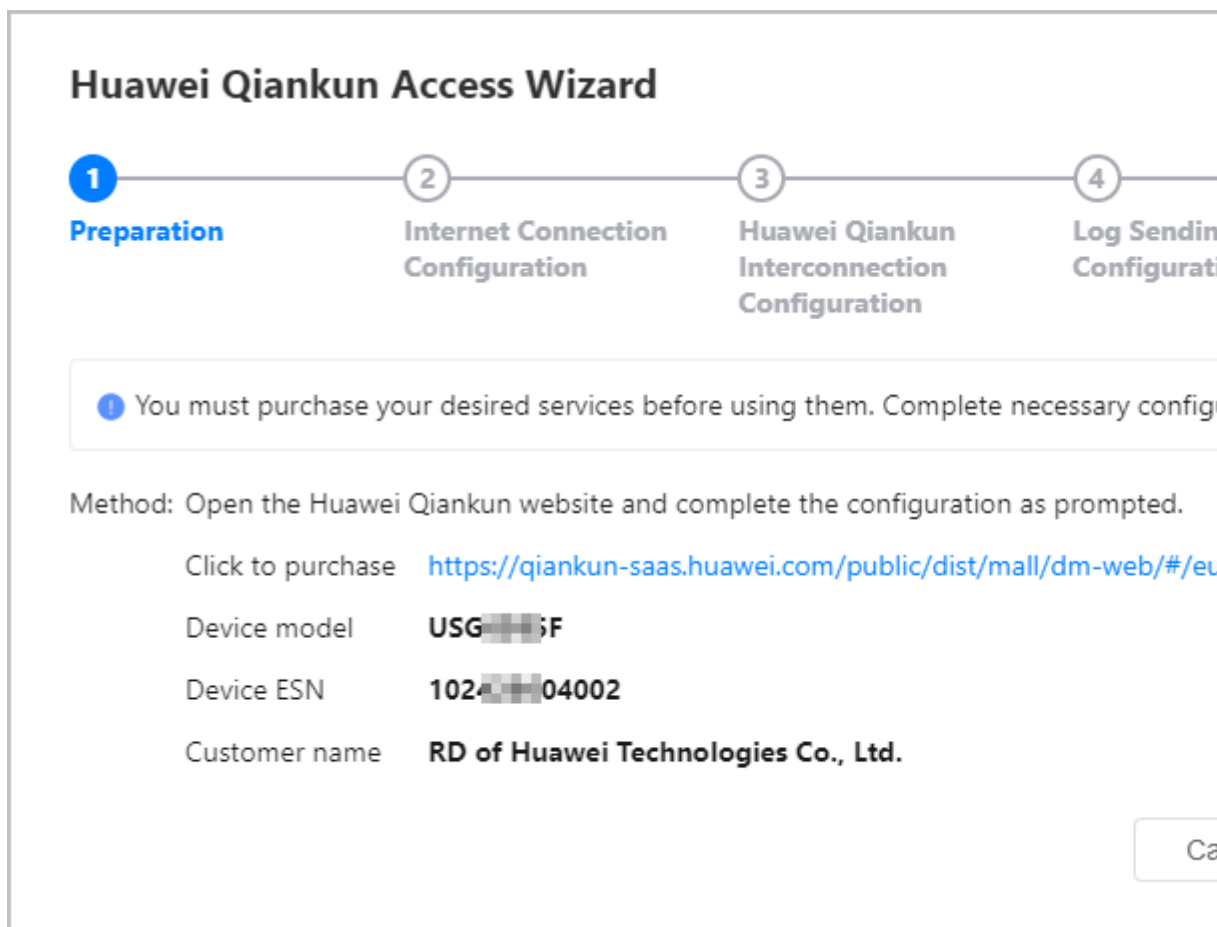


Step 3 Learn about Huawei Qiankun Security CloudService and purchase the service.

Huawei Qiankun Security CloudService is a payment item. To use the service, purchase it as prompted and configure Huawei Qiankun website as prompted.

The device model, device ESN, and customer name are displayed on the page. Such information facilitates the purchase of Huawei Qiankun licenses.

Click **Next** to access the **Internet Connection Configuration** page.



Step 4 Configure the device to connect to the Internet.

- If the device has been connected to the Internet, skip this step.
- If the device is not connected to the Internet, set related parameters. Click **Next**. The **Huawei Qiankun Interconnection Configuration** page is displayed.

Huawei Qiankun Access Wizard

1

2

3

4

Preparation

Internet Connection Configuration

Huawei Qiankun Interconnection Configuration

Log Sending Configuration

1. If the Internet connection has been configured, click Skip to go to the next step.

2. You need to configure a security policy for Internet connection. Click [Add Security Policy](#) to add a security policy.

*

Internet Access Interface

10GigabitEthernet1

Internet Access Mode

Static IP

DHCP

PPPoE

*

IP/Mask

1.1.1.1/255.255.255.0

*

Default Gateway

1.1.1.0

*

DNS1

2.2.2.2

DNS2

DNS3

Cancel

Previous

Parameter	Description
Internet Access Interface	Interface connected to the network.

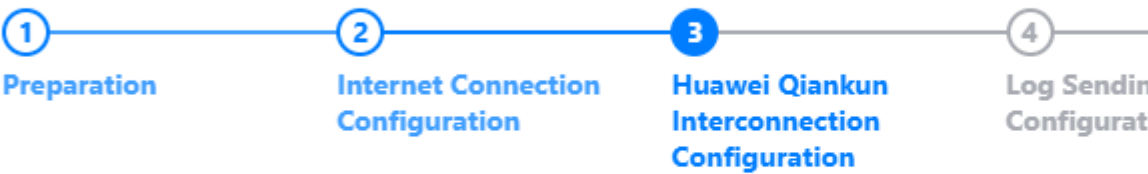
Parameter	Description
Internet Access Mode	Internet access mode. The Internet access mode is selected based on the actual network conditions. If Static IP is selected, you need to manually configure the IPv4 address, default gateway, and DNS information. Static IP: If you obtain a fixed IP address or an IP address range from a network service provider, select this access mode. DHCP: If you automatically obtain IP addresses from a network service provider, select this access mode. PPPoE: If the device functions as a PPPoE client, use this connection type. NOTE If the Internet access mode is set to PPPoE, a dialer interface is created or an existing dialer interface is associated by default. • If a dialer interface exists under the corresponding Internet access interface, the foremost dialer interface is selected by default. For details about the query sequence when multiple dialer interfaces exist under a physical interface, see <i>Configuring the Dialer Interface</i>. • If the corresponding Internet access interface does not have a dialer interface, create a dialer interface.
IP/Mask	IP address: specifies the public IP address of the interface. The IP address cannot conflict with the IP addresses of other interfaces on the device or other devices on the network. Subnet mask: specifies the subnet mask of the IP address.
Default Gateway	Default gateway address of the interface. NOTE The default gateway address cannot be a broadcast address or network address.
DNS Server	IP address of the DNS server. You can add multiple DNS servers. A maximum of three DNS servers can be added. When the first DNS server fails, the second one works, and so on. To ensure DNS service reliability, you are advised to configure multiple DNS servers.

Parameter	Description
User Name	User name for CHAP or PAP authentication sent by the PPPoE client. The value cannot contain any question mark (?), cannot contain only double quotation marks (""), and cannot contain double quotation marks (""), and spaces at the same time. The user name and password must be both configured. If no user name or password is configured on an interface, all users are not authenticated by default. This parameter can be configured when Internet Access Mode is set to PPPoE.
Password	Password for CHAP or PAP authentication sent by the PPPoE client. The value cannot contain any space or question mark (?), and cannot contain only asterisks (*) or double quotation marks (""). The user name and password must be both configured. If no user name or password is configured on an interface, all users are not authenticated by default. This parameter can be configured when Internet Access Mode is set to PPPoE.
IP Address Obtaining Mode	Mode in which the interface obtains an IPv4 address. • Auto • Specify This parameter can be configured when Internet Access Mode is set to PPPoE.
Service Name	PPPoE service name. The value is a string of 1 to 128 case-sensitive characters without any space, asterisk (*), question mark (?), or quotation mark ("). When multiple PPPoE sessions are configured on an interface, you are advised to configure a service name to establish a session with the PPPoE server that provides the specified service. This parameter can be configured when Internet Access Mode is set to PPPoE.
MTU of PPP negotiation	Maximum MTU for PPP negotiation during PPPoE session establishment. The value is an integer in the range of 64 to 2000. By default, the maximum MTU for PPP negotiation during PPPoE session establishment is 1500 bytes. This parameter can be configured when Internet Access Mode is set to PPPoE.

Parameter	Description
Add Security Policy You need to configure security policies to allow mutual access between the device and DNS server and between the device and cloud service. Therefore, perform the following configurations:	
Allowing the device to access the DNS server	Source Zone: local Destination Zone: trust, untrust Source IP Address/Region: any Destination IP Address/Region: any Service: dns Content Security: - Action: Permit
Allowing the device to access the cloud service	Source Zone: local Destination Zone: untrust Source IP Address/Region: any Destination IP Address/Region: any Service: https Content Security: - Action: Permit

Step 5 Set the parameters for the interconnection between the device and Huawei Qiankun Security CloudService.

Huawei Qiankun Access Wizard



- !

1. Check the connectivity. You can proceed to the next step only after confirming that th

2. If the configuration changes during connectivity check, the existing NETCONF Call-Ho

cleared and a new instance is created.

* Destination Domain
Name / Destination IP
Address ?

Contact the cloud platform administrator to obtain the IP address or domain

* Port

10020

Connection Status

✔

 Connection successful

Check Connectivity

Ca

Parameter	Description
Destination Domain Name/Destination IP Address	IP address/domain name and TCP port number of the cloud service management component. The default domain name is mgt.seccloud.huawei.com.
Port	The port number is in the range of 1 to 65535. The default port number is 10020. The IP address/domain name and TCP port number of the cloud service management component can be obtained from the cloud platform administrator.

Parameter	Description
Connection Status	After interworking with Huawei Qiankun, click Check Connectivity to check whether the connection between the device and Huawei Qiankun is normal. If so, click Next to access the Log Sending Configuration page. If not, return to the previous step to configure the Internet connection. NOTE When you click Check Connectivity, the system automatically delivers the configuration for interworking with Huawei Qiankun. Then click OK. If the configuration changes during connectivity check, the existing NETCONF Call-Home connection instance configuration is cleared and a new instance is created.

Step 6 Configure the device to send security logs, forensic data, and reports to Huawei Qiankun Security CloudService.

Huawei Qiankun Access Wizard

1

Preparation

2

Internet Connection Configuration

3

Huawei Qiankun Interconnection Configuration

4

Log Sending Configuration

The content security function needs to be configured for the log sending function.

* Destination Domain Name/Destination IP Address

Contact the cloud platform administrator to obtain the IP address or domain

Ca

Parameter	Description
Destination Domain Name/Destination IP Address	Domain name/IP address used by Huawei Qiankun Security CloudService host to receive security logs and forensic data. The default domain name is rd.seccloud.huawei.com. The address for collecting logs of Huawei Qiankun Security CloudService can be obtained from the cloud platform administrator.

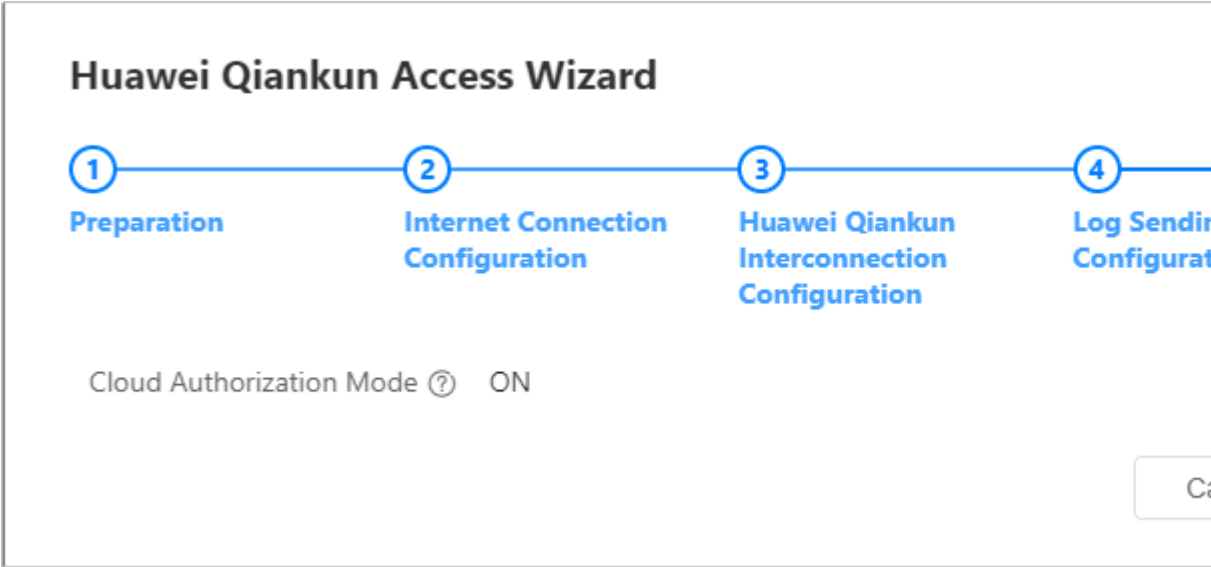
Step 7 Configure the cloud authorization mode.

By default, the cloud authorization mode is enabled. It cannot be disabled.

After the cloud authorization mode is enabled, the update service items are controlled by the cloud and no longer support local upgrade.

 NOTE

- The update service items include intrusion prevention, antivirus, and remote URL query.
- Except the update service items, function service items and resource service items are controlled by the local license file and are irrelevant to the authorization mode.



- After the cloud authorization mode is enabled, the status of the license resources for the update services in **License Management** is **Cloud-based Authorization**. If a license resource item is about to expire, renew it on the cloud in a timely manner.
- After the cloud authorization mode is enabled, the **Update Service Validity Period** status of the signature database update service items in **Update Center** is **Cloud-based Authorization**, and the signature databases are automatically updated on the cloud.

Step 8 Click **Finish** to complete the Huawei Qiankun access configuration.

----End

Follow-up Procedure

1.

After the access wizard is configured, choose **Policy > Security Policy**. Set the action of the **default** security policy to **Permit** to ensure that the current services of users are not affected and the device can go online successfully.
2.

After the device goes online, configure a security policy to allow LAN users to access the Internet. The detailed configurations are as follows:

N o.	Descrip tion	Sour ce Secu rity Zone	Desti natio n Secu rity Zone	Sour ce IP Addr ess	Desti natio n IP Addr ess	Servi ce	Content Security	Actio n
1	Protect intranet users from threats when they access the Internet .	trust	untru st	any	any	any	• Antivirus: default • Intrusion preventio n: Create a template and enable attack forensic.	Perm it
2	Protect Internet users from threats when they access the intranet.	untru st	trust	any	any	any	• Antivirus: default • Intrusion preventio n: Create a template and enable attack forensic.	Perm it
3	Deny all the traffic that does not match the precedi ng security policies.	any	any	any	any	any	-	Deny

3.3 Huawei Qiankun Access Wizard (OP Scenario)

Context

The OP scenario provides on-premises security services (one customer, one platform). The platform interconnection address needs to be configured independently.

 NOTE

Only the USG6615F, USG6510F-D, USG6530F-D, USG6585F, and USG6555F support this configuration.

 NOTE

- Only level-3 administrators (system administrators) can view and configure the Huawei Qiankun access wizard.
- Huawei Qiankun Security CloudService depends on Huawei Qiankun Connector Package. Therefore, install Huawei Qiankun Connector Package first. Obtain the Huawei Qiankun Connector feature package from Huawei support website. For details about how to install the feature package, see Configuring the Feature Package.

Procedure

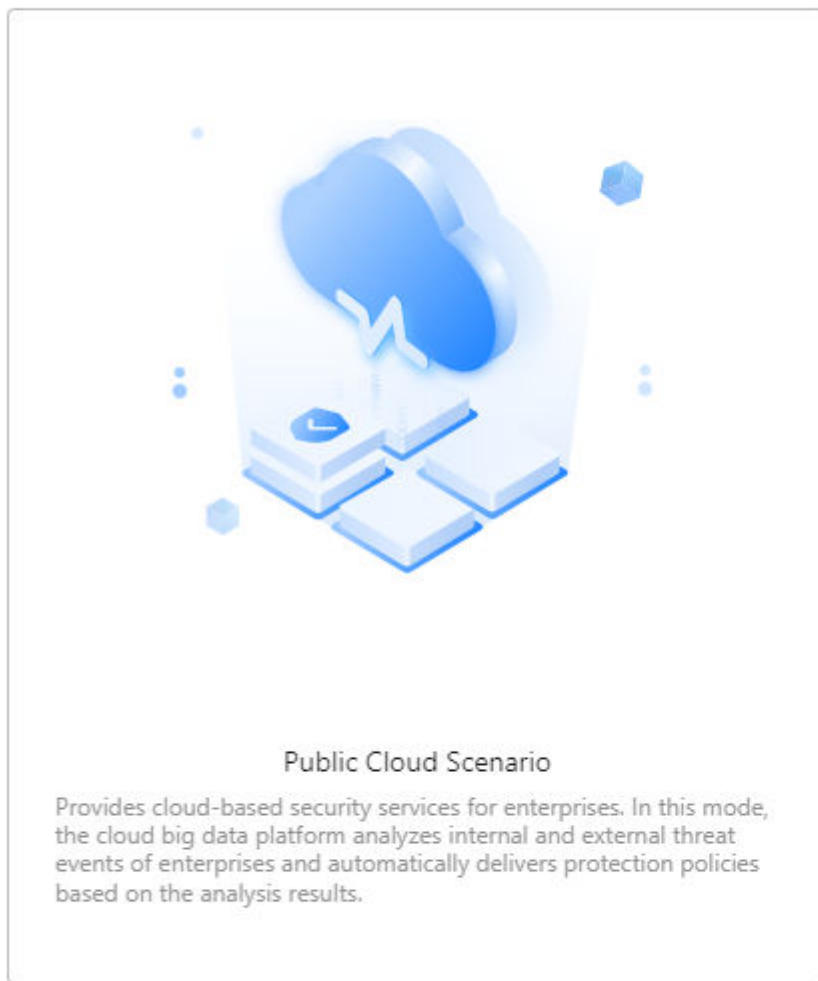
Step 1 Choose **System > Huawei Qiankun Access Wizard**. The wizard page is displayed.

Alternatively, choose **System > System Upgrade** and tap **Huawei Qiankun Access Wizard** in the **Operation** column of **Huawei Qiankun Connector Package** to access the wizard page.

Step 2 Select **On-Premises Scenario**.

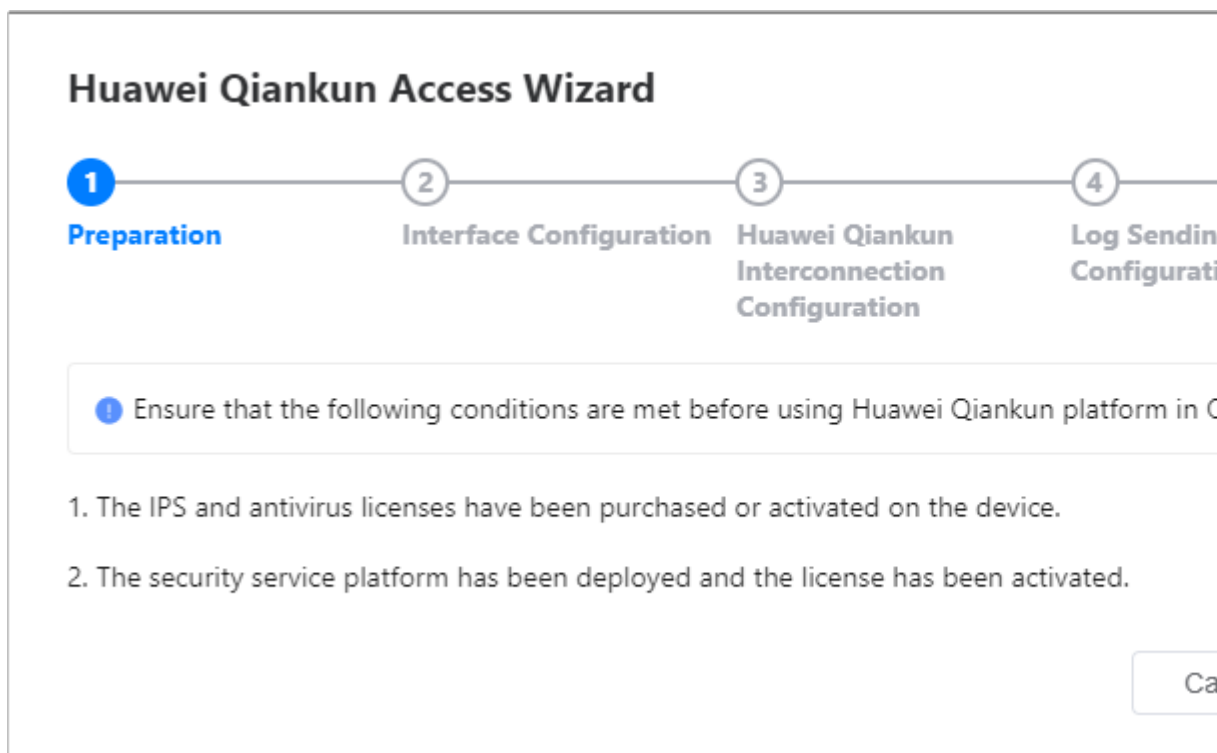
Click **Next** to access the **Preparation** page.

Huawei Qiankun Access Wizard



Step 3 Follow the wizard to purchase related services, and then follow the instructions to complete the configurations of the Huawei Qiankun website.

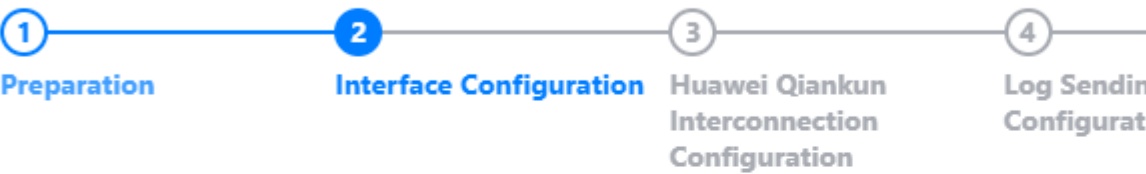
Click **Next** to access the **Interface Configuration** page.\



Step 4 Configure the device to connect to the Internet.

- If the device has been connected to the Internet, skip this step.
- If the device is not connected to the Internet, set parameters. Click **Next**. The **Huawei Qiankun Interconnection Configuration** page is displayed.

Huawei Qiankun Access Wizard



- !

1. This interface is used to connect to the OP.

2. You need to configure a security policy for Internet connection. Click [Add Security Po](#)

* Interface

10GE/0

Connection Mode

☒ Static IP ?

☐ DHCP ?

☐ PPPoE ?

* IP/Mask

1.1.1.1/255.255.255.0

* Default Gateway

1.1.1.0

DNS1 ?

2.2.2.2

DNS2

DNS3

Cancel

Pre

Parameter	Description
Interface	Interface connected to the OP.

Parameter	Description
Connection Mode	Internet access mode. The Internet access mode is selected based on the actual network conditions. If Static IP is selected, you need to manually configure the IPv4 address, default gateway, and DNS information. Static IP: If you obtain a fixed IP address or an IP address range from a network service provider, select this access mode. DHCP: If you automatically obtain IP addresses from a network service provider, select this access mode. PPPoE: If the device functions as a PPPoE client, use this connection type. NOTE If the Internet access mode is set to PPPoE, a dialer interface is created or an existing dialer interface is associated by default. • If a dialer interface exists under the corresponding Internet access interface, the foremost dialer interface is selected by default. For details about the query sequence when multiple dialer interfaces exist under a physical interface, see <i>Configuring the Dialer Interface</i>. • If the corresponding Internet access interface does not have a dialer interface, create a dialer interface.
IP/Mask	IP address: specifies the public IP address of the interface. The IP address cannot conflict with the IP addresses of other interfaces on the device or other devices on the network. Subnet mask: specifies the subnet mask of the IP address.
Default Gateway	Default gateway address of the interface. NOTE The default gateway address cannot be a broadcast address or network address.
DNS Server	IP address of the DNS server. You can add multiple DNS servers. A maximum of three DNS servers can be added. When the first DNS server fails, the second one works, and so on. To ensure DNS service reliability, you are advised to configure multiple DNS servers.

Parameter	Description
User Name	User name for CHAP or PAP authentication sent by the PPPoE client. The value cannot contain any question mark (?), cannot contain only double quotation marks (""), and cannot contain double quotation marks (""') and spaces at the same time. The user name and password must be both configured. If no user name or password is configured on an interface, all users are not authenticated by default. This parameter can be configured when Connection Mode is set to PPPoE.
Password	Password for CHAP or PAP authentication sent by the PPPoE client. The value cannot contain any space or question mark (?), and cannot contain only asterisks (*) or double quotation marks (""). The user name and password must be both configured. If no user name or password is configured on an interface, all users are not authenticated by default. This parameter can be configured when Connection Mode is set to PPPoE.
IP Address Obtaining Mode	Mode in which the interface obtains an IPv4 address. • Auto • Specify This parameter can be configured when Connection Mode is set to PPPoE.
Service Name	PPPoE service name. The value is a string of 1 to 128 case-sensitive characters without any space, asterisk (*), question mark (?), or quotation mark ("). When multiple PPPoE sessions are configured on an interface, you are advised to configure a service name to establish a session with the PPPoE server that provides the specified service. This parameter can be configured when Connection Mode is set to PPPoE.
MTU of PPP negotiation	Maximum MTU for PPP negotiation during PPPoE session establishment. The value is an integer in the range of 64 to 2000. By default, the maximum MTU for PPP negotiation during PPPoE session establishment is 1500 bytes. This parameter can be configured when Connection Mode is set to PPPoE.

Parameter	Description
Add Security Policy You need to configure security policies to allow mutual access between the device and DNS server and between the device and cloud service. Therefore, perform the following configurations:	
Allowing the device to access the DNS server	Source Zone: local Destination Zone: trust, untrust Source IP Address/Region: any Destination IP Address/Region: any Service: dns Content Security: - Action: Permit
Allowing the device to access Huawei Qiankun Security CloudService	Source Zone: local Destination Zone: untrust Source IP Address/Region: any Destination IP Address/Region: any Service: https Content Security: - Action: Permit

Step 5 Set parameters for connecting the device to Huawei Qiankun Security CloudService.

Huawei Qiankun Access Wizard

1

2

3

4

PreparationInterface ConfigurationHuawei Qiankun Interconnection ConfigurationLog Sending Configuration

1

1. Check the connectivity. You can proceed to the next step only after confirming that the
2. If the configuration changes during connectivity check, the existing NETCONF Call-Home
cleared and a new instance is created.

* Destination Domain Name / Destination IP Address

10.1.1.77

* Port

10020

Connection Status

✓

Connection successful

Check Connectivity

C

Parameter	Description
Destination Domain Name/Destination IP Address	IP address/domain name and TCP port number of the cloud service management component. The port number ranges from 1 to 65535.
Port	Obtain the IP address/domain name and TCP port number of the cloud service management component from the cloud platform administrator.

Parameter	Description
Connection Status	After interworking with Huawei Qiankun, click Check Connectivity to check whether the connection between the device and Huawei Qiankun is normal. If so, click Next to access the Log Sending Configuration page. If not, return to the previous step to configure the Internet connection. NOTE When you click Check Connectivity, the system automatically delivers the configuration for interworking with Huawei Qiankun. Please confirm. If the configuration changes during connectivity check, the existing NETCONF Call-Home connection instance configuration is cleared and a new instance is created.

Step 6 Configure the device to send security logs, forensic data, and reports to Huawei Qiankun Security CloudService.

Huawei Qiankun Access Wizard

1

2

3

4

Preparation

Interface Configuration

Huawei Qiankun Interconnection Configuration

Log Sending Configuration

The content security function needs to be configured for the log sending function.

* Destination Domain Name/Destination IP Address

10.10.10.10

Threat Log ?

ON

* Destination Port

30201

Attack Forensics ?

Traffic Report ?

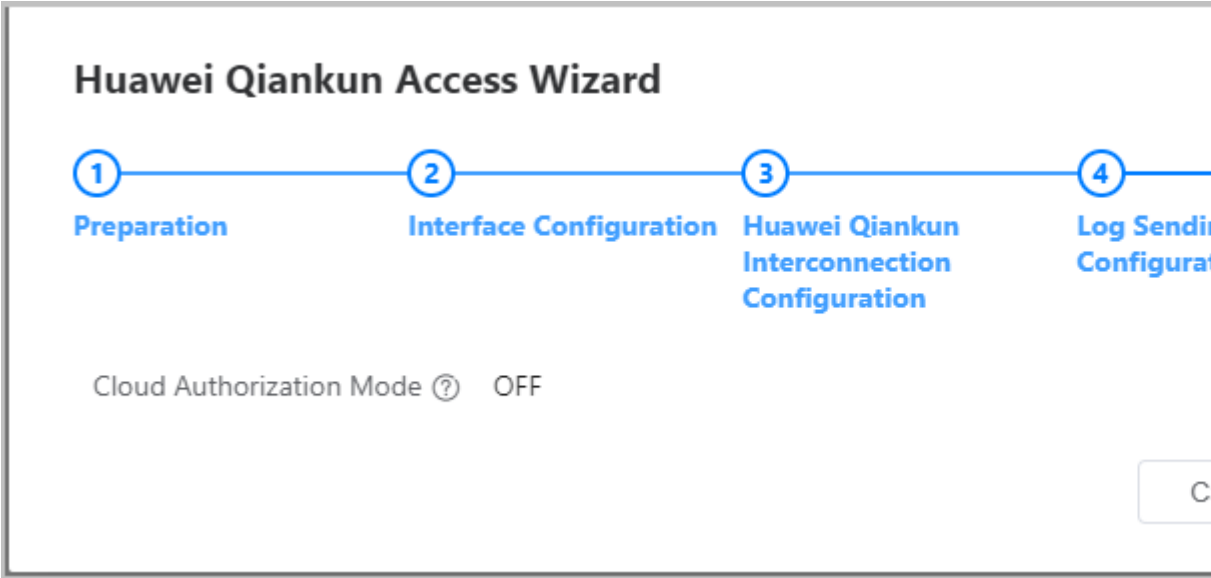
Cancel

Pre

Parameter	Description
Destination Domain Name/Destination IP Address	Domain name/IP address used by Huawei Qiankun Security CloudService host to receive security logs and forensic data. The address for collecting logs of Huawei Qiankun Security CloudService can be obtained from the cloud platform administrator.
Threat Log	Enabled by default and cannot be disabled.
Attack Forensics	Disabled by default and can be modified. The attack forensic data is malware data packets or threat data packets.
Traffic Report	Disabled by default and can be modified. The device sends traffic reports to Huawei Qiankun by email so that tenants can gain insight into the current network's traffic characteristics and bandwidth utilization.

Step 7 Configure the cloud authorization mode.

In the OP scenario, disable the cloud authorization mode. By default, this mode is disabled.



Step 8 Click **Finish** to complete the Huawei Qiankun access configuration.

----End

Follow-up Procedure

1. After the access wizard is configured, choose **Policy > Security Policy**. Set the action of the **default** security policy to **Permit** to ensure that the current services of users are not affected and the device can go online successfully.
2. After the device goes online, configure a security policy to allow LAN users to access the Internet. The detailed configurations are as follows:

N o.	Descrip tion	Sour ce Secu rity Zone	Desti natio n Secu rity Zone	Sour ce IP Addr ess	Desti natio n IP Addr ess	Servi ce	Content Security	Actio n
1	Protect intranet users from threats when they access the Internet.	trust	untrust	any	any	any	- Antivirus: default - Intrusion prevention: Create a template and enable the attack forensic function.	Permit
2	Protect Internet users from threats when they access the intranet.	untrust	trust	any	any	any	- Antivirus: default - Intrusion prevention: Create a template and enable the attack forensic function.	Permit
3	Deny all the traffic that does not match the preceding security policies.	any	any	any	any	any	-	Deny

3.4 Cloud Service Configuration Commands

3.4.1 cloud-bwl access-key secret-access-key

Function

The **cloud-bwl access-key secret-access-key** command configures the access key for interconnecting with the cloud service blacklist and whitelist server.

The **undo cloud-bwl** command deletes the access key for interconnecting with the blacklist and whitelist server of a cloud service.

By default, this function is not configured.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-bwl { **access-key** *access-key-id* | **secret-access-key** *secret-access-key* }
undo cloud-bwl { **access-key** | **secret-access-key** }

Parameters

Parameter	Description	Value
access-key <i>access-key-id</i>	Specifies the access key ID provided by the cloud service.	The value is a string of 1 to 64 case-sensitive characters and 128 to 188 case-sensitive characters, spaces not supported. If spaces are used, the string must be enclosed in double quotation marks (" ").
secret-access-key <i>secret-access-key</i>	Specifies the access key provided by the cloud service.	The value is a string of 1 to 64 case-sensitive characters and 128 to 188 case-sensitive characters, spaces not supported. If spaces are used, the string must be enclosed in double quotation marks (" ").

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

Obtain the access key ID and access key from the cloud service administrator.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the access key for connecting to the blacklist and whitelist server of a cloud  
service to KtUEj8ySfi4qvAdgZ7XzoBRilnZ5AcJqfW70ciOL.  
<HUAWEI> system-view  
[HUAWEI] cloud-bwl access-key KtUEj8ySfi4qvAdgZ7XzoBRilnZ5AcJqfW70ciOL
```

3.4.2 cloud-bwl ca-certificate

Function

The **cloud-bwl ca-certificate** command configures the CA certificate used by a device to communicate with a cloud server when the cloud server delivers a blacklist or whitelist to the device.

The **undo cloud-bwl ca-certificate** command cancels the specified CA certificate.

By default, this function is not configured.

NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-bwl ca-certificate *ca-certificate-name*

undo cloud-bwl ca-certificate

Parameters

Parameter	Description	Value
ca-certificate <i>ca-certificate-name</i>	Specifies the name of the CA certificate.	The value is a string of 1 to 64 case-sensitive characters. It cannot contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When a cloud server interconnects with a device to deliver the blacklist and whitelist to the device, you need to specify a CA certificate to verify the connection between the cloud server and the device. Otherwise, the blacklist and whitelist cannot be delivered.

Prerequisites

Before running this command, apply for a certificate, upload the CA certificate to the device storage, and import the certificate to the memory. For details, see the **pki import-certificate** command.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

Specify huawei_ca.cer as the CA certificate used for communication between the device and the cloud server that delivers the blacklist and whitelist.

```
<HUAWEI> system-view  
[HUAWEI] cloud-bwl ca-certificate huawei_ca.cer
```

3.4.3 cloud-bwl interval

Function

The **cloud-bwl interval** command sets the interval for incrementally downloading the cloud service blacklist and whitelist.

The **undo cloud-bwl interval** command cancels the configuration.

By default, if the interval for incrementally downloading the cloud service blacklist and whitelist is not specified, the default value 30s is used.

NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-bwl interval *interval*

undo cloud-bwl interval

Parameters

Parameter	Description	Value
interval <i>interval</i>	Specifies the interval for incrementally downloading the cloud service blacklist and whitelist.	The value is an integer that ranges from 10 to 300, in seconds.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

To change the interval for incrementally downloading the cloud service blacklist and whitelist, run the cloud-bwl interval command.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the interval for incrementally downloading the cloud service blacklist and
whitelist to 60s.
<HUAWEI> system-view
[HUAWEI] cloud-bwl interval 60
```

3.4.4 cloud-bwl server

Function

The **cloud-bwl server** command configures the domain name, IP address, or port number of the cloud service blacklist or whitelist server.

The **undo cloud-bwl server** command cancels the configuration.

By default, the domain name or IP address of the cloud service blacklist or whitelist server is not specified, and the default port is 443.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

```
cloud-bwl server { hostname host-name | ip ipv4-address | port port }  
undo cloud-bwl server { hostname | ip | port }
```

Parameters

Parameter	Description	Value
hostname <i>host-name</i>	Specifies the domain name of the cloud service blacklist and whitelist server.	The value is a string of 1 to 253 case-sensitive characters, spaces not supported. If spaces are used, the string must be enclosed in double quotation marks (" ").
ip <i>ipv4-address</i>	Specifies the IP address of the cloud service blacklist and whitelist server.	The value is in dotted decimal notation.
port <i>port</i>	Specifies the port of the cloud service blacklist and whitelist server.	The value is an integer ranging from 1 to 65535.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

The device obtains the blacklist and whitelist from the cloud service blacklist and whitelist server and delivers the configuration to implement unattended automatic protection on the tenant side.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the domain name of the cloud service blacklist and whitelist server to  
www.hostname.com, IP address to 1.1.1.1, and port number to 443.  
<HUAWEI> system-view  
[HUAWEI] cloud-bwl server hostname www.hostname.com  
[HUAWEI] cloud-bwl server ip 1.1.1.1  
[HUAWEI] cloud-bwl server port 443
```

3.4.5 cloud-service ca-certificate

Function

The **cloud-service ca-certificate** command configures the CA certificate used for interconnecting with a cloud server.

The **undo cloud-service ca-certificate** command cancels the configuration.

By default, this function is not configured.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-service ca-certificate *ca-certificate-file*

undo cloud-service ca-certificate

Parameters

Parameter	Description	Value
ca-certificate <i>ca-certificate-file</i>	Specifies the name of a certificate.	The value is a string of 1 to 64 case-sensitive characters, and cannot contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device is used in the cloud service solution, run this command to configure the CA certificate used for interconnecting with the cloud service host. Huawei CA certificate default_ca.cer has been preconfigured on the device by

default. You can run the cloud-service ca-certificate default_ca.cer command to directly use the certificate.

If the certificate of the cloud service host has been replaced, the corresponding certificate needs to be replaced on the device side. You need to upload the certificate, run the **pki import-certificate** command to import the CA certificate, and then run this command to replace the CA certificate.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the CA certificate used for interconnecting with the cloud server to default_ca.cer.
```

```
<HUAWEI> system-view  
[HUAWEI] cloud-service ca-certificate default_ca.cer
```

3.4.6 cloud-service enable

Function

The **cloud-service enable** command enables the function of sending attack forensics and traffic reports and domain name logs of ECSs.

The **undo cloud-service enable** command disables the function of sending attack forensics and traffic reports and domain name logs of ECSs.

By default, this function is disabled.

NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-service { pcap | traffic-report | domain } enable

undo cloud-service { pcap | traffic-report | domain } enable

Parameters

Parameter	Description	Value
pcap	Indicates the packet capture function.	-
traffic-report	Indicates the traffic log report function.	-

Parameter	Description	Value
domain	Indicates domain name logs.	-

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In the cloud service solution scenario, you can run this command to enable or disable the function of sending attack forensics, traffic reports, and domain name logs.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Enable the function of sending attack forensics.
<HUAWEI> system-view
[HUAWEI] cloud-service pcap enable

# Enable the function of sending traffic reports of ECSs.
<HUAWEI> system-view
[HUAWEI] cloud-service traffic-report enable

# Enable the function of sending domain name logs of ECSs.
<HUAWEI> system-view
[HUAWEI] cloud-service domain enable
```

3.4.7 cloud-service host

Function

The **cloud-service host** command configures the domain name and IP address of the interconnected cloud service host and the port for the cloud service host to receive attack evidence collection data, threat logs, and traffic reports.

The **undo cloud-service host** command cancels the configuration of the interconnected cloud service host.

By default, this function is not configured. If only the domain name or IP address of the cloud service host is configured and no port is configured, the cloud service host uses port 30201 to receive threat logs, port 30202 to receive attack evidence collection data, and port 30203 to receive traffic reports.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

```
cloud-service host domain domain-name  
cloud-service host ip ip-address  
cloud-service host { threat-log-port threat-log-port-value | pcap-port pcap-port-value | traffic-report-port traffic-report-port-value } *  
undo cloud-service host
```

Parameters

Parameter	Description	Value
ip <i>ip-address</i>	Specifies an IP address.	The value is in dotted decimal notation.
threat-log-port <i>threat-log-port-value</i>	Specifies the port for the cloud service host to receive threat logs.	The value is an integer ranging from 1024 to 65535. The default value is 30201.
pcap-port <i>pcap-port-value</i>	Specifies the port for the cloud service host to receive attack evidence collection data.	The value is an integer ranging from 1024 to 65535. The default value is 30202.
traffic-report-port <i>traffic-report-port-value</i>	Specifies the port for the cloud service host to receive traffic reports.	The value is an integer ranging from 1024 to 65535. The default value is 30203.
domain <i>domain-name</i>	Specifies a domain name.	The value is a string of 1 to 64 case-insensitive characters, spaces not supported. If spaces are used, the string must be enclosed in double quotation marks (" ").

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

In cloud service scenarios, this command configures the cloud service host before the cloud service host can receive data.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the port for the cloud service host to receive traffic reports to 55555.  
<HUAWEI> system-view  
[HUAWEI] cloud-service host traffic-report-port 55555  
  
# Set the domain name of the cloud service host to rd.seccloud.huawei.com.  
<HUAWEI> system-view  
[HUAWEI] cloud-service host domain rd.seccloud.huawei.com
```

3.4.8 cloud-service local-certificate

Function

The **cloud-service local-certificate** command configures the local certificate used for interconnecting with a cloud server.

The **undo cloud-service local-certificate** command cancels the configuration.

By default, this function is not configured.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

```
cloud-service local-certificate certificate-name  
undo cloud-service local-certificate
```

Parameters

Parameter	Description	Value
local-certificate <i>certificate-name</i>	Specifies the name of a certificate.	The value is a string of 1 to 64 case-sensitive characters, and cannot contain spaces.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device is used in the cloud service solution, run this command to configure the local certificate for interconnecting with the cloud service host. The Huawei local certificate default_local.cer has been preconfigured on the device by default. You can run the cloud-service ca-certificate default_local..cer command to directly use the certificate.

If the certificate of the cloud service host has been replaced, the corresponding certificate needs to be replaced on the device side. You need to upload the certificate, run the **pki import-certificate** command to import the certificate, and then run this command to replace the certificate.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the local certificate used for interconnecting with the cloud server to  
default_local.cer.  
<HUAWEI> system-view  
[HUAWEI] cloud-service local-certificate default_local.cer
```

3.4.9 cloud-service logic-id

Function

The **cloud-service logic-id** command configures a logical ID.

The **undo cloud-service logic-id** command cancels the configuration.

By default, the logical ID is not configured.

NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

cloud-service logic-id *logic-id-value*

undo cloud-service logic-id

Parameters

Parameter	Description	Value
<i>logic-id-value</i>	Specifies a logical ID.	The value is a numeric string of 16 digits.

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

When the device is used in the e-Surfing security cloud solution, you can run this command to configure a logical ID related to an order. The e-Surfing security brain can determine the cloud service capabilities of the device based on the logical ID.

If the logical ID is not configured or incorrectly configured, the callhome connected to the SecoManager is disconnected.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Set the logical ID to 1234567891011121.  
<HUAWEI> system-view  
[HUAWEI] cloud-service logic-id 1234567891011121
```

3.4.10 threat-protection cloud-authorization enable

Function

The **threat-protection cloud-authorization enable** command enables cloud-based authorization.

The **undo threat-protection cloud-authorization enable** command disables cloud-based authorization.

By default, cloud-based authorization is disabled.

Format

threat-protection cloud-authorization enable

undo threat-protection cloud-authorization enable

Parameters

None

Views

System view

Default Level

2: Configuration level

Usage Guidelines

Usage Scenario

This command applies only to cloud service interconnection. Before enabling the cloud authorization mode, ensure that the device supports cloud service interconnection and has the Huawei Qiankun connector feature package installed.

If the device is connected to a cloud service, enable the cloud authorization mode.

After the cloud authorization mode is enabled, the update services (intrusion prevention signature database update and antivirus signature database update) and remote URL query are controlled by the cloud instead of the local license. After the license expires, you need to renew the license on the cloud and update the signature database online. Other function control items and resource control items are still controlled by the local license. Control details are as follows:

- The intrusion prevention function is available. The intrusion prevention signature database update is controlled by the cloud, and only online update is supported.
- The antivirus function is available. The antivirus signature database update is controlled by the cloud, and only online update is supported.
- The URL filtering function is available, and remote URL query is controlled by the cloud.

After the cloud authorization mode is disabled, the update service and remote URL query are controlled by the local license. The signature database can be updated locally or online.

Precautions

If the Huawei Qiankun connector feature package is not loaded, the cloud authorization mode cannot be enabled. However, disabling the cloud authorization mode is not controlled by the feature package.

After the cloud authorization mode is enabled, you need to wait for about 1 hour before connecting to the remote URL query server.

Example

```
# Enable the cloud authorization mode.  
<HUAWEI> system-view  
[HUAWEI] threat-protection cloud-authorization enable
```

3.5 Cloud Service Diagnostic Commands

3.5.1 display cloud-bwl

Function

The **display cloud-bwl list** command displays the blacklist and whitelist obtained from the cloud platform.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

```
display cloud-bwl { list | record }
```

Parameters

Parameter	Description	Value
list	Blacklist and whitelist records delivered by the cloud service.	-
record	Displays the status records of the blacklist and whitelist obtained by the device from the cloud platform.	-

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

To view the blacklist and whitelist obtained from the cloud platform, run the display cloud-bwl { list | record } command.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

 NOTE

The actual command output varies according to the device. The command output here is only an example.

Display the blacklist and whitelist status obtained from the cloud service management platform.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose] display cloud-bwl record
Time                Type                Result ADD( OK | FAIL|REPLACE|TTL_OVER| OLD ) DEL( OK | FAIL|NOT_FIND|
ID_DIF) CHECK_DEL
-----
2021-08-19 10:23:38  download full  Success  2  0  0  0  0  0  0  0  0  0  0
```

Display the blacklist and whitelist obtained from the cloud service management platform.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose] display cloud-bwl list
Type|Direction      IP|Protocol|Port      LifeTime(mins)|LeftTime(mins)|HitTimes|ErrorCode|ID
-----
WHITE|dst            1.1.1.1 | 0 | 0      8554 | 0 | 0 | 0 | 6e63d148-8d1f-4735-
b67c-457847727890
total : 1
```

Table 3-4 Description of the **display cloud-bwl** command output

Item	Description
Time	Time when the device obtains the blacklist and whitelist from the cloud service.
Type	In the display cloud-bwl list command output, Type indicates the entry type. • BLACK: blacklist. • WHITE: whitelist. In the display cloud-bwl record command output, Type indicates the download type of the blacklist or whitelist. • download full: full download. • download inc: incremental download.
Result	Obtains the status. • Success. • Fail.

Item	Description
OK	Number of blacklists and whitelists that are successfully downloaded or deleted.
OLD	Number of aged blacklists and whitelists.
CHECK_DEL	Number of entries deleted after verification.
total	Total number of entries.
Direction	Type of a blacklist or whitelist. - src: indicates the source address type. - dst: indicates the destination address type.
IP	IP address.
Port	Port ID.
Protocol	Protocol type.
LifeTime	Lifetime.
LeftTime	Remaining validity period.
HitTimes	Number of times the entry is matched.
ErrorCode	Error code.
ID	Blacklist or whitelist ID.
ADD	Blacklist and whitelist to be added.
DEL	Blacklist and whitelist to be deleted.
FAIL	Number of blacklists and whitelists that fail to be downloaded or deleted.
REPLACE	Number of replaced blacklists and whitelists.
TTL_OVER	Number of timeout blacklists and whitelists.
NOT_FIND	Number of entries that are deleted from the cloud but cannot be found on the local device during full download.
ID_DIF	Number of entries with different IDs but the same key value.

3.5.2 display log statistic type seccloud-log

Function

The **display log statistic type seccloud-log** command displays statistics about logs sent from the data plane to the cloud server.

 NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

display log statistic type seccloud-log [**slot** *slot-id* **cpu** *cpu-id*]

Parameters

Parameter	Description	Value
slot <i>slot-id</i>	Specifies the slot ID.	The value is an integer, and the value range depends on the device configuration.
cpu <i>cpu-id</i>	Specifies the CPU ID.	The value is an integer, and the value range depends on the device configuration.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Through the **display log statistic type seccloud-log** command, you can view the log statistics sent to the cloud server.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

 NOTE

The actual command output varies according to the device. The command output here is only an example.

Display statistics about logs sent from the data plane to the cloud server.

```
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose] display log statistic type seccloud-log
2021-05-19 12:12:53.211
Log and Packet Capture Statistics:
-----
                ips      av      bwt      pcap      domain
normal          :
received (fragments) num :
abnormal num      :
complete pcap
num              :
no memory discard :
save complete num :
exceed the limit discard :
https send ok num :
https send exceptions num :
https connect err num :
ssl-cer-file err num :
esn err num      :
callhome err num :
-----

Traffic-Report Statistics:
-----
                intf      src-ip      app
normal          :
received (fragments) num :
abnormal num      :
Complete pcap
num              :
no memory discard :
save complete num :
exceed the limit discard :
https send ok num :
https send exceptions num :
https connect err num :
https authen err num :
ssl-cer-file err num :
esn err num      :
callhome err num :
```

Table 3-5 Description of the **display log statistic type seccloud-log** command output

Item	Description
Log and Packet Capture Statistics	Log and packet capture statistics.
ips	IPS type log statistics.
av	AV type log statistics.
bwt	Botnet, Trojan horse, and worm log statistics.
pcap	Pcap log statistics.
domain	Statistics on domain name filtering logs.
normal	Normally inserted message.
received (fragments) num	Number of messages received.

Item	Description
abnormal num	Number of abnormal messages.
complete pcap num	The number of complete packet capture files.
no memory discard	Out of memory drop message.
save complete num	Number of stored complete messages.
exceed the limit discard	Discard message after overrun.
https send ok num	Number of successful sending of HTTPS.
https send exceptions num	The number of HTTPS sending exceptions.
https connect err num	Number of HTTPS connection failures.
https authen err num	Number of HTTPS authentication failures.
ssl-cer-file err num	Number of SSL certificate key verification failures.
esn err num	Number of ESN acquisition failures.
callhome err num	Number of callhome failures.
Traffic-Report Statistics	Traffic report statistics.
intf	Interface statistics.
src-ip	Source IP statistics.
app	Application information statistics.

3.5.3 reset log statistic type seccloud-log

Function

The **reset log statistic type seccloud-log** command is used to clear the log statistics count sent from the data plane to the cloud server.

NOTE

This command is supported only on the USG6510F-D, USG6530F-D, USG6555F, USG6585F and USG6615F.

Format

reset log statistic type seccloud-log [*slot slot-id* *cpu cpu-id*]

Parameters

Parameter	Description	Value
slot <i>slot-id</i>	Specifies the slot ID.	The value is an integer, and the value range depends on the device configuration.
cpu <i>cpu-id</i>	Specifies the CPU ID.	The value is an integer, and the value range depends on the device configuration.

Views

Diagnostic view

Default Level

3: Management level

Usage Guidelines

Usage Scenario

Run the **reset log statistic type seccloud-log** command to clear the statistics of logs sent from the data plane to the cloud server.

Precautions

This command is supported only when the Huawei Qiankun connector feature package is loaded.

Example

```
# Clear the log statistics count sent to the cloud server by the data plane.
<HUAWEI> system-view
[HUAWEI] diagnose
[HUAWEI-diagnose] reset log statistic type seccloud-log
```

3.6 Personal Data Description of Huawei Qiankun Connector

Precautions

To make sure that all functions provided by the product can be used, perform operations according to the instructions in the product documentation. According to local laws and regulations in different countries, carriers have different requirements on privacy protection. The privacy data list may not cover all the information to be contained in the privacy statement required by laws and regulations of your country.

Usage Scenario	Collected Personal Data	Collection Source and Method	Purpose and Security Protection Measure	Data Retention Period and Policy	Deletion Measure	Data Export Method (Such as Interfaces and Commands) Implementation Scheme (Anonymization or Pseudonymization)	Personal Data Export Guide
Attack forensics	Data packet	After a threat is detected, the device sends the packets matching the attack features to the Huawei Qiankun cloud service platform or HiSec Insight. The device itself does not retain the data.	Used for attack analysis and forensics. The device does not retain data and transmits the data to the Qiankun service platform or HiSec Insight through encrypted channels.	The device does not retain data.	The device does not retain data.	The device does not retain data.	The device does not retain data.