Datacom Network Open Programmability V100R020C00

User Guide

Issue	02
Date	2020-12-30

HUAWEI

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: https://www.huawei.com

Email: support@huawei.com

Contents

1 Overview

After a function package is compiled locally, you can import it to the NCE open programmability system (OPS) for online commissioning and use, implementing device management, device configuration delivery, and service configuration delivery.

The OPS is applied in the following scenarios:

- Managing and configuring a device

  The OPS automatically generates the device configuration page based on the device YANG model (compiling and loading an SND package) for you to manage and configure a device.
- Configuring network services across devices

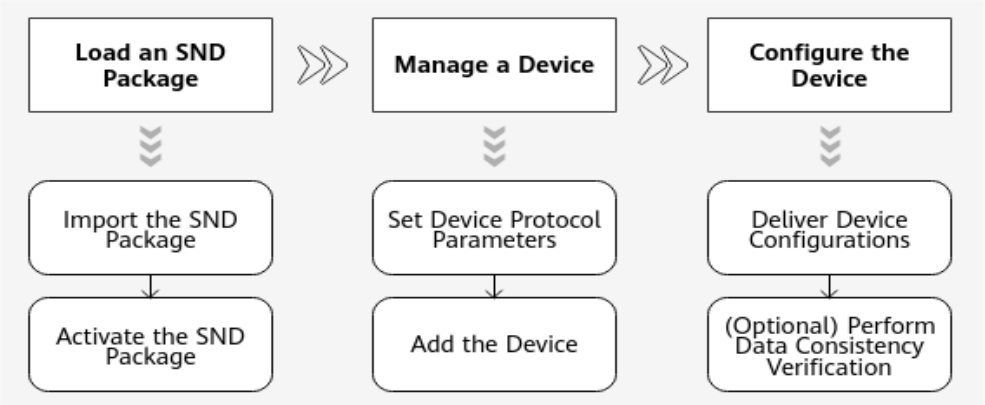
  The OPS automatically generates the service configuration page based on the service YANG model (compiling and loading an SSP package) for you to deliver service configurations to devices.
- Verifying data consistency between a device and the OPS

  You can verify data consistency between a device and the OPS. If the data is inconsistent, you can perform data consistency comparison, synchronization, and verification.

2 Operation Procedure

You can develop a function package (such as an SND or SSP package) based on site requirements by referring to the development guide and then configure devices and services by referring to the following process.

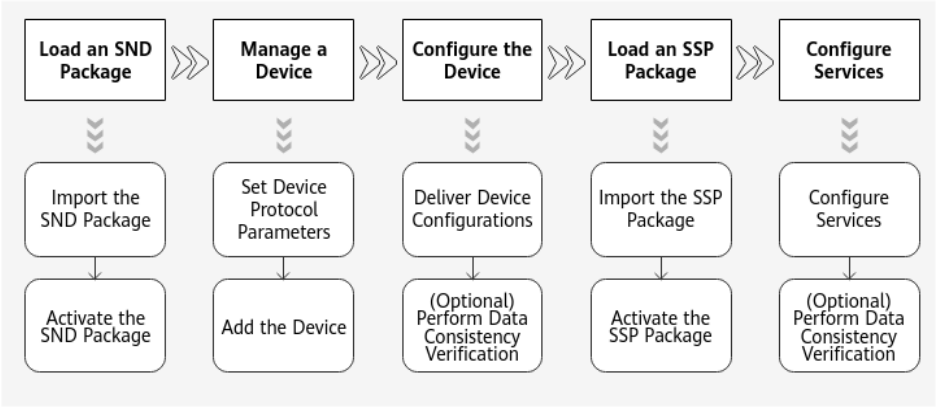
Figure 2-1 Process of managing and configuring a device



1. Load an SND package:
   a. Import the compiled SND package to the system.
   b. Activate the SND package.
2. Manage a device:
   a. Set protocol parameters, including the user name and password.
   b. Add a device. After the device is added, the controller automatically initiates a connection to the device.
3. Configure the device using either of the following methods:
   - Method 1: After all device data is collected, synchronize data based on data on NCE and the device based on the NCE or device data.
   - Method 2: Configure the device on the device configuration page.

   If the configuration data in the system is modified by a third party or is lost after a device restarts unexpectedly, the configuration data in the system will be inconsistent with that on the device. In this case, you can perform data consistency verification on the device.

Figure 2-2 Process of configuring network services across devices



If a device is not managed, manage the device by referring to the preceding flowchart and then configure services. If the device has been managed, you do not need to perform the first three steps.

1. Load an SND package:
   a. Import the compiled SND package to the system.
   b. Activate the SND package.
2. Manage a device:
   a. Set protocol parameters, including the user name and password.
   b. Add a device. After the device is added, the controller automatically initiates a connection to the device.
3. Configure the device using either of the following methods:
   a. Method 1: After all device data is collected, synchronize data based on data on NCE and the device based on the NCE or device data.
   b. Method 2: Configure the device on the device configuration page.
4. Load an SSP package:
   a. Import the compiled SSP package to the system.
   b. Activate the SSP package.
5. Configure services.

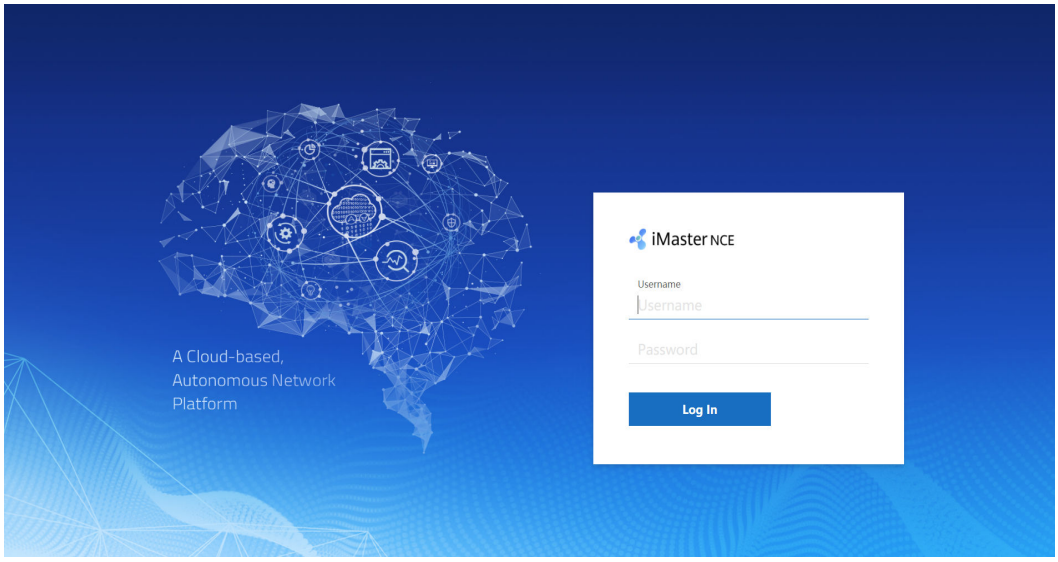
3 System Login

The open programmability system (OPS) provides two deployment modes: One is that the system is integrated into iMaster NCE-IP and released as an app (service open programmability). The app is deployed with iMaster NCE-IP. The other one is that the system is released as an independent software package. The open programmability mini software package is installed independently. This section describes how to log in to the system using a browser.

Logging In to the OPS App

Step 1 Log in to the NCE O&M plane. Access the O&M plane at **https://***IP address of the O&M plane*:**31943**. Enter the user name and password and click **Log In**.

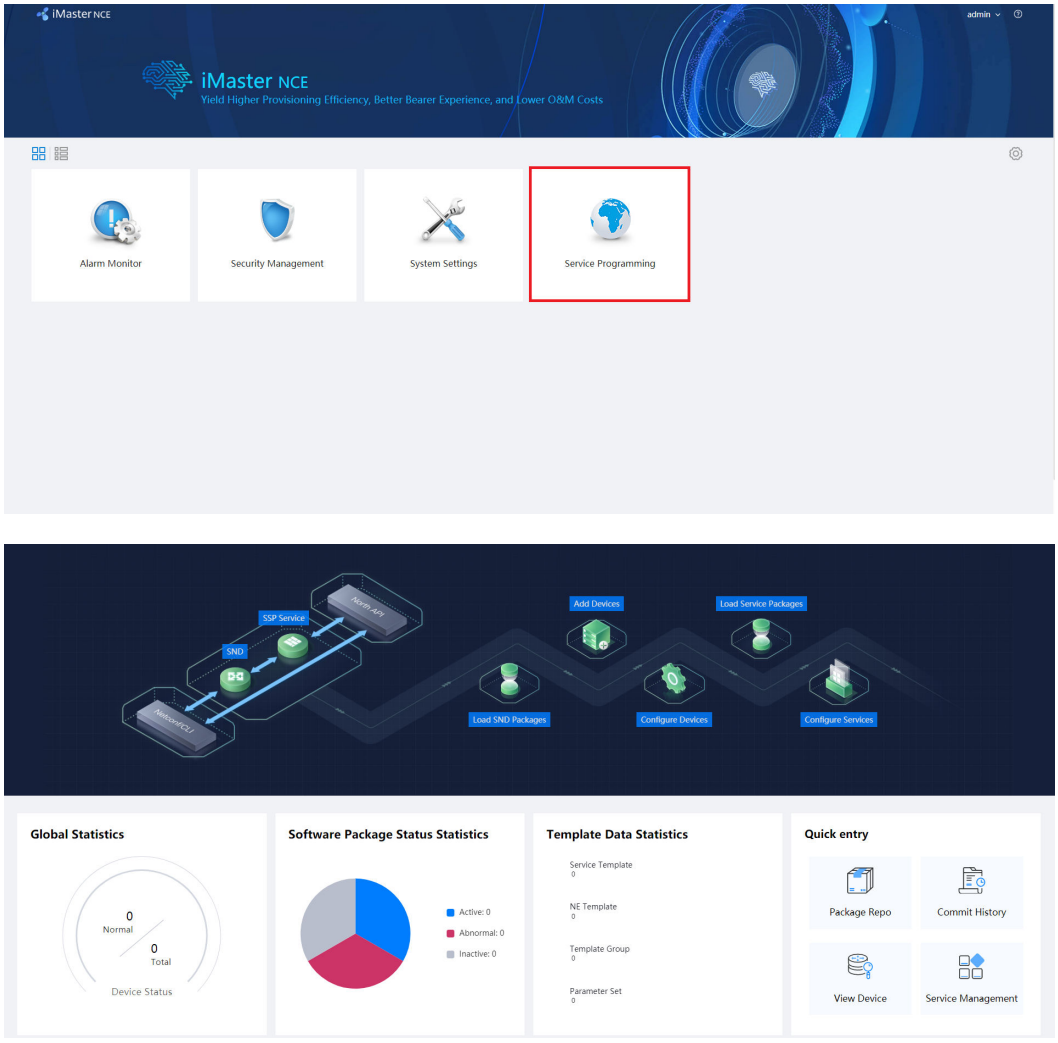
Figure 3-1 Logging in to the NCE O&M plane



NOTE

- You need to change the password upon the first login. Keep the new password properly. To improve system security, you are advised to periodically change the password to prevent security risks such as brute force cracking.
- The IP address of the O&M plane is the client login IP address configured on the Common_Service node. If the Common_Service node is deployed in a cluster, the IP address is set to the floating IP address of the cluster. If the Common_Service node is deployed in single-node mode, the IP address is the client login IP address of the node.

Step 2 After logging in to the system, click **Service Programming** on the homepage to access the OPS.



Step 3 On the home page, click the corresponding shortcut entry or click any shortcut entry based on the actual application scenario to access the main menu.

----End

Logging In to the open programmability Mini System

Step 1 Log in to the developer community and download the open programmability mini software package (**AOCmini_V100R020C00.zip**) on the resource download tab page.

Step 2 Decompress **AOCmini_V100R020C00.zip** and double-click **start.bat** to start the AOC mini service. The window is displayed.

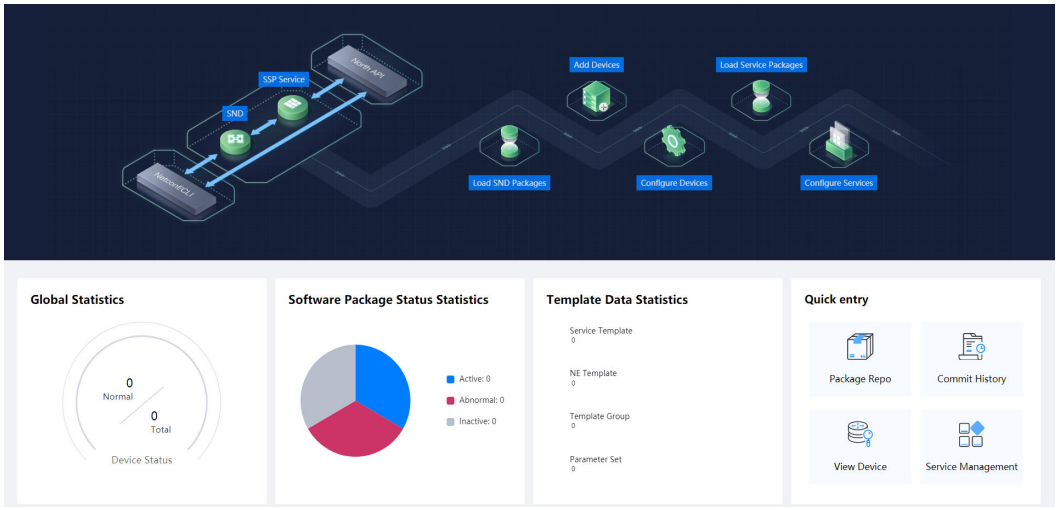
```
C:\Users\swx944510\Desktop\AOCmini\envs\Product-AOCService\controller>..\..\..\rtsp\tomcat\bin
\catalina.bat start
Using CATALINA_BASE:   "C:\Users\swx944510\Desktop\AOCmini/envs/Product-AOCService/"
Using CATALINA_HOME:   "C:\Users\swx944510\Desktop\AOCmini/rtsp/tomcat"
Using CATALINA_TMPDIR: "C:\Users\swx944510\Desktop\AOCmini/envs/Product-AOCService/\temp"
Using JRE_HOME:        "C:\Users\swx944510\Desktop\AOCmini/rtsp/jdk/"
Using CLASSPATH:       "C:\Users\swx944510\Desktop\AOCmini/rtsp/tomcat\bin\bootstrap.jar;C:\Users
\swx944510\Desktop\AOCmini/rtsp/tomcat\bin\tomcat-juli.jar"

========================================
AOCmini is starting, please wait a moment.
```

Step 3 Wait for about three minutes until the system is started.

```
2020-09-10 16:10:28 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:33 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:39 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:43 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:48 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:53 Console message: AOCmini is starting, progress: 95.70%
2020-09-10 16:10:58 Console message: AOCmini is starting, progress: 97.68%
2020-09-10 16:11:03 Console message: AOCmini is starting, progress: 97.68%
2020-09-10 16:11:08 Console message: AOCmini is starting, progress: 97.68%
2020-09-10 16:11:13 Console message: AOCmini started successfully, please visit https://127.0.0.1:32018/
aocwebsite/ in browser.
```

Step 4 Log in to the AOC mini system at https://127.0.0.1:32018/aocwebsite.

Figure 3-2 Home page of the AOC mini system



Step 5 On the home page, click the corresponding shortcut entry or click any shortcut entry based on the actual application scenario to access the main menu.

----End

4 Package Repository Management

Package repository management includes repository management, package management, public key management, and task management.

Repository management is used to create, modify, and delete repositories where software packages are stored. Package management is used to import, deploy, update, and delete software packages. Public key management is used to upload and delete public keys. Task management is used to check software package tasks.

4.1 Repository Management

Scenario Description

A repository stores software packages. Before creating or importing a software package, you must create a repository. You can create repositories of different types or authentication modes as required.

Procedure

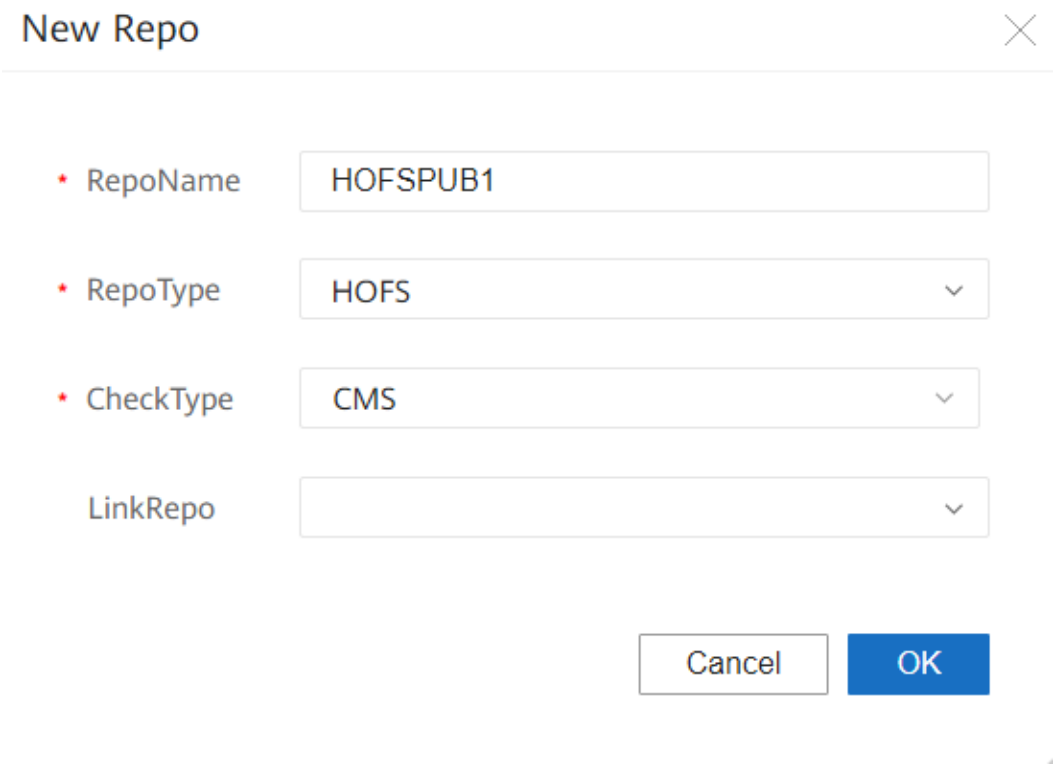
Step 1 Choose **Package Repo** from the main menu.

Step 2 Choose **Repo** from the navigation pane, and click **New Repo** in the upper right corner of the page. In the **New Repo** dialog box that is displayed, set required parameters.

Table 4-1 Key parameters

Parameter	Description
RepoType	FS: Packages are stored in the disk of the node where the package repository management service is deployed, delivering low reliability. HOFS: Packages are stored in the HOFS file system, implementing high reliability. If you have high requirements on package reliability, HOFS is strongly recommended.
CheckType	SHA256: Integrity verification is performed only on packages stored in the repository. ASC: Signature verification is performed on packages stored in the repository to ensure that the packages are not tampered with. CMS: Signature verification is performed on packages stored in the repository to ensure that the packages are not tampered with. **NOTE** The security level of SHA256, ASC, and CMS increases in ascending order. To ensure secure storage of packages in the repository, you are advised to select **ASC** or **CMS**. If two or more authentication modes are selected, the system performs authentication based on the selected authentication modes in sequence when you upload a package. As long as one authentication mode is passed, the package can be successfully uploaded to the repository.

Figure 4-1 Creating a repository



----End

Follow-up Procedure

If **CheckType** is set to **ASC** or **CMS**, you need to import the public key for signature verification. The public key is used to verify the signature of each package managed by the repository. Otherwise, signature verification cannot be performed.

Related Operations

You can perform the following operations as required:

- To modify a repository, click **Modify** in the **Operation** column of the repository to be modified. You can modify the repository name and authentication mode.
- To delete a repository, click **Delete** in the **Operation** column of the repository to be deleted.

4.2 Package Management

4.2.1 Creating a Software Package

Scenario Description

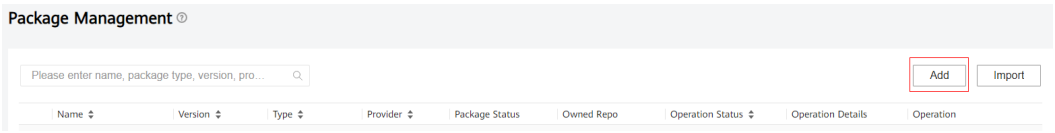
When a software package is created, the default software template directory and sample code are generated for you to develop the software package.

Procedure

Step 1 Choose **Package Repo** from the main menu.

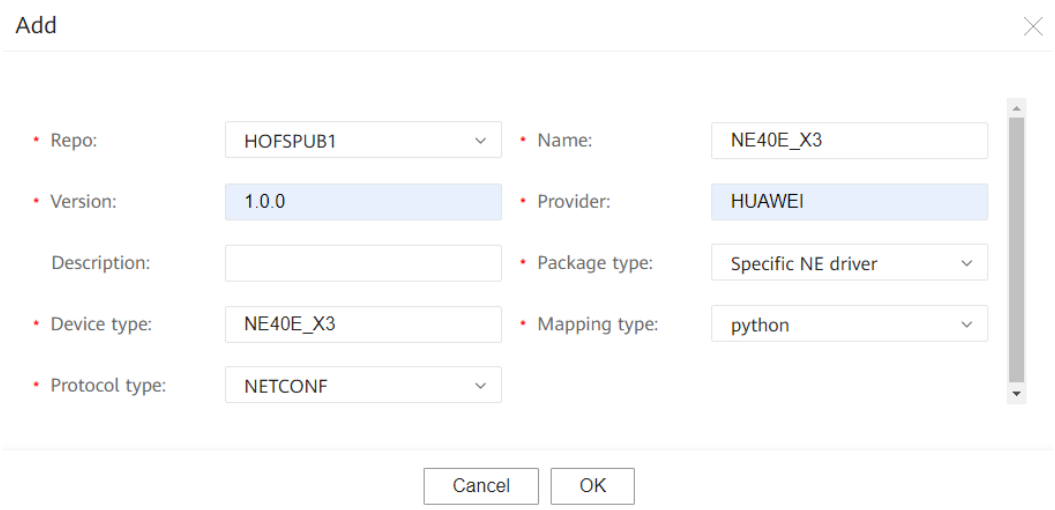
Step 2 Choose **Package Management** from the navigation pane, and click **Add** in the upper right corner of the page.

Figure 4-2 Creating a software package



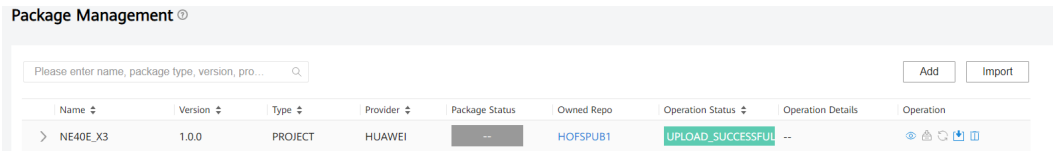
Step 3 In the **Add** dialog box that is displayed, set mandatory parameters, such as **Name**, **Version**, **Provider**, and **Package type**. The name and version uniquely identify a software package. The provider refers to the provider of a software package.

Figure 4-3 Parameters for creating a software package



Step 4 After the software package is created, you can view the new software package on the **Package Management** page.

Figure 4-4 Exporting a software package



----End

Follow-up Procedure

You need to export the new software package locally for programming. After the development is complete, import the software package to the system.

Related Operations

- To view a software package, click in the **Operation** column.
- To uninstall a software package, click in the **Operation** column.
- To delete a software package, click in the **Operation** column.
- To export a software package, click in the **Operation** column.

4.2.2 Importing a Software Package

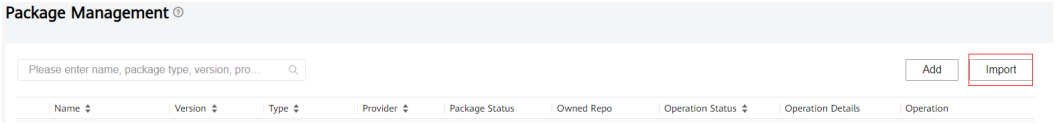
Scenario Description

You can import a software package that has been programmed or obtained from other developers to the system. The imported software package can be used only after being deployed as required.

Procedure

Step 1 Choose **Package Repo** from the main menu. Then choose **Package Management** from the navigation pane, and click **Import** on the displayed page.

Figure 4-5 Importing a software package



Step 2 In the **Import** dialog box that is displayed, select the software package to be imported.

Figure 4-6 Dialog box for selecting the software package to be imported

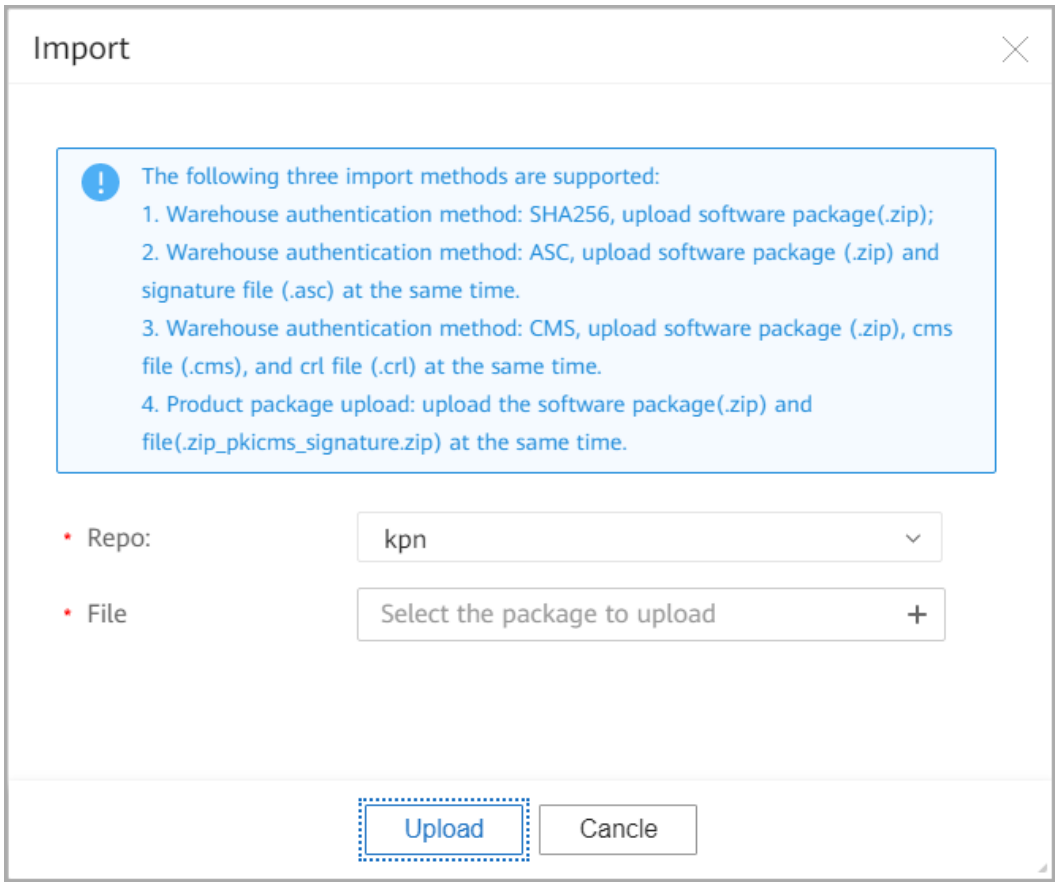
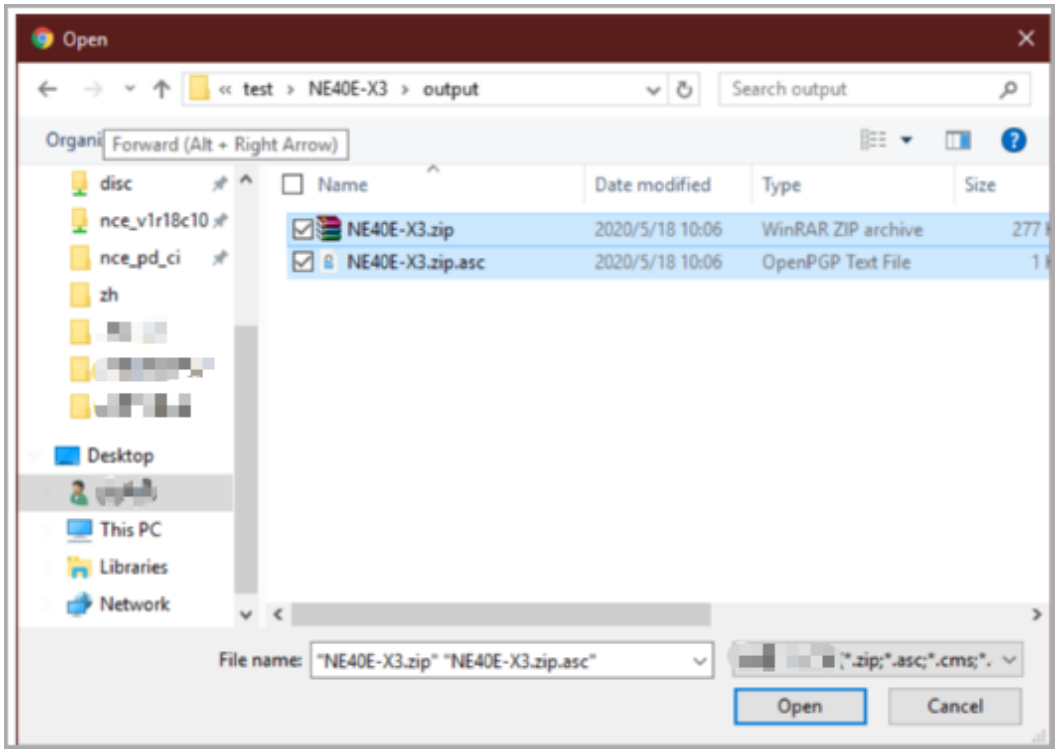
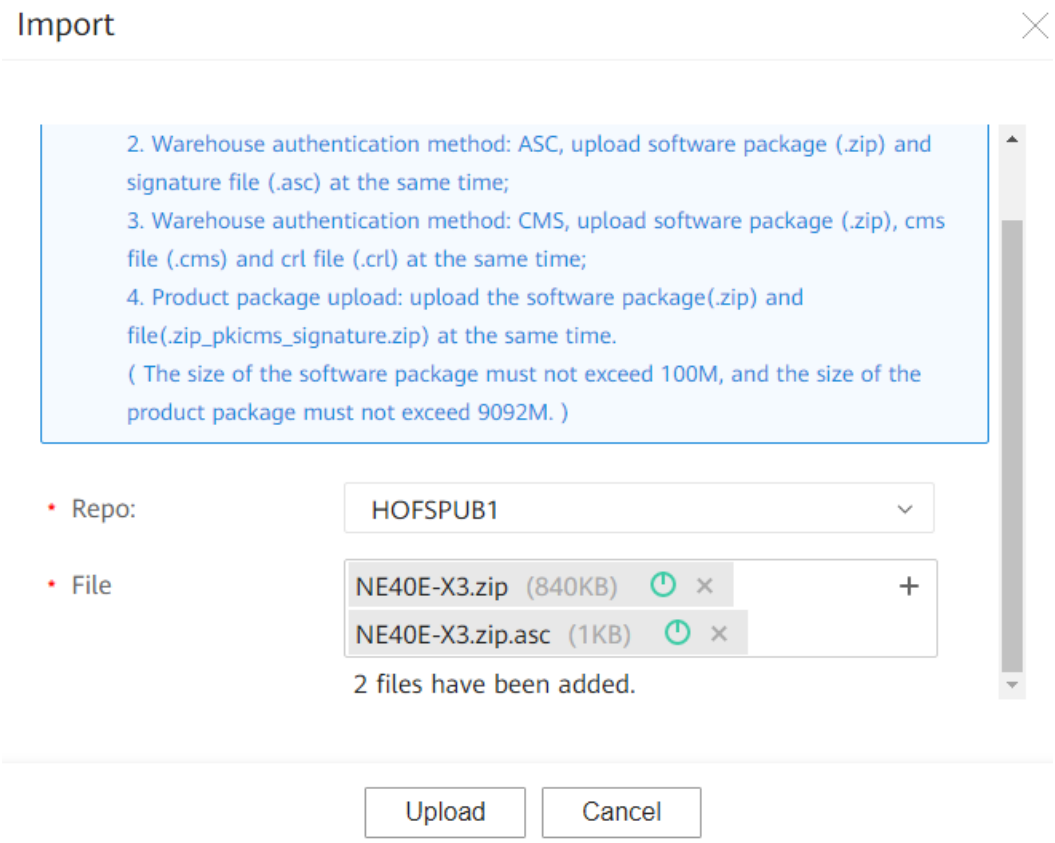


Figure 4-7 Selecting the software package and signature file to be imported



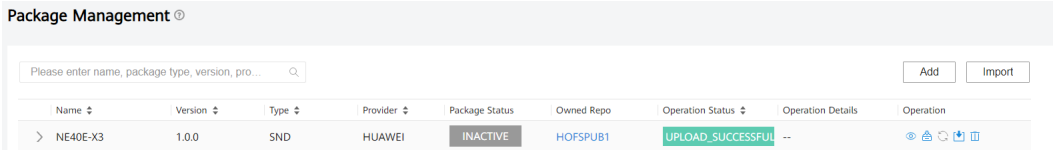
Step 3 Click **Upload**.

Figure 4-8 Uploading a software package



After the software package is imported, you can view the imported software package on the **Package Management** page.

Figure 4-9 Successfully importing a software package



----End

Follow-up Procedure

You need to deploy the software package after being imported to ensure that software package functions take effect in the system.

Related Operations

- To view a software package, click in the **Operation** column.
- To uninstall a software package, click in the **Operation** column.
- To delete a software package, click in the **Operation** column.

- To export a software package, click in the **Operation** column.
- To deploy a software package, click in the **Operation** column.

4.2.3 Deploying a Software Package

Prerequisites

The software package has been successfully uploaded or uninstalled, and all dependent software packages have been successfully deployed.

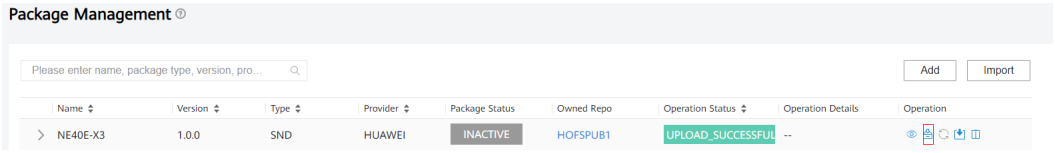
Scenario Description

You need to deploy a software package to make it take effect in the system.

Procedure

Step 1 Choose **Package Repo** from the main menu. Then choose **Package Management** from the navigation pane. On the **Package Management** page, click in the **Operation** column to deploy the software package.

Figure 4-10 Installing a software package



Step 2 Wait for a few minutes until the software package is deployed.

When a software package is deployed, the system loads the corresponding code, script, and model in the package, and generates database entries based on the model.

Table 4-2 Status change after deployment

Deployment Status	Package Status	Operation Status	Description
DEPLOY_SUCCESS	ACTIVE	DEPLOY_SUCCESS	The software package is successfully deployed.
DEPLOY_FAILURE	INACTIVE	UPLOAD_SUCCESS (same as the operation status before you click)	As long as the software package fails to be deployed, the system performs a rollback and the rollback succeeds. For details about the deployment failure cause, see operation details.

Deployment Status	Package Status	Operation Status	Description
	ABNORMAL	DEPLOY_FAILURE	• As long as the software package fails to be deployed, the system performs a rollback and the rollback fails. For details about the deployment failure cause, see operation details. • If the status of a software package is abnormal, click to enable the system to automatically restore the software package to the inactive state.

----End

Related Operations

- To update a software package:

  Click in the **Operation** column to update the software package to the target version.

  NOTE

  Before updating the software package, ensure that the original software package is successfully activated and deployed. When the software package is updated, the system automatically uninstalls the original software package and deploys the new software package (that is, the software package of the target version).

  Table 4-3 Status change after update

Update Status	Package Status	Operation Status	Description
UPDATE_SUCCESS	Software package of the target version: **ACTIVE** Original software package: **INACTIVE**	Software package of the target version: **DEPLOY_SUCCESS** Original software package: **UNINSTALL_SUCCESS**	The software package is successfully updated. **NOTE** When an SSP package is updated and some YANG model objects of the original package are deleted, the system automatically deletes data of the deleted objects during the update. Therefore, exercise caution when you perform this operation.

Update Status	Package Status	Operation Status	Description
UNINSTALL_FAILURE	Software package of the target version: **INACTIVE** Original software package: **ACTIVE**	Software package of the target version: **UPLOAD_SUCCESS** Original software package: **DEPLOY_SUCCESS**	As long as the software package fails to be updated, the system performs a rollback and the rollback succeeds. For details about the update failure cause, see operation details.
	Software package of the target version: **ABNORMAL** Original software package: **ABNORMAL**	Software package of the target version: **DEPLOY_FAILURE** Original software package: **UNINSTALL_FAILURE**	As long as the software package fails to be updated, the system performs a rollback and the rollback fails. For details about the uninstallation failure cause, see operation details.

- To uninstall a software package, click in the **Operation** column.

Table 4-4 Status change after uninstallation

Uninstallation Status	Package Status	Operation Status	Description
UNINSTALL_SUCCESS	INACTIVE	UNINSTALL_SUCCESS	The software package is successfully uninstalled.
UNINSTALL_FAILURE	ACTIVE	DEPLOY_SUCCESS	As long as the software package fails to be uninstalled, the system performs a rollback and the rollback succeeds. For details about the uninstallation failure cause, see operation details.

Uninstallation Status	Package Status	Operation Status	Description
	ABNORMAL	UNINSTALL_FAILURE	As long as the software package fails to be uninstalled, the system performs a rollback and the rollback fails. For details about the uninstallation failure cause, see operation details.

- To delete a software package, click in the **Operation** column.
- To export a software package, click in the **Operation** column.

4.2.4 Viewing Software Packages

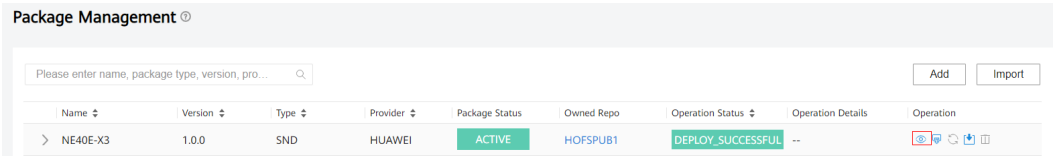
Scenario Description

You can view the software packages that exist in the system on the page.

Procedure

Step 1 Choose **Package Repo** from the main menu. Then choose **Package Management** from the navigation pane, and click on the displayed page.

Figure 4-11 Software package view



Step 2 In the file view displayed on the **check** page, click a file. The file content then is displayed on the right area.

Figure 4-12 Software package file view

----End

4.3 Public Key Management

4.3.1 Uploading a Public Key

Scenario Description

If a package signed using a private key is uploaded to the repository, you need to use the public key to verify the signature of the package so as to ensure that the package is not tampered with. In this case, you need to import the corresponding public key before uploading the package.

NOTE

A private key supports only the RSA algorithm, and the private key length must be in the range from 3072 to 4096.

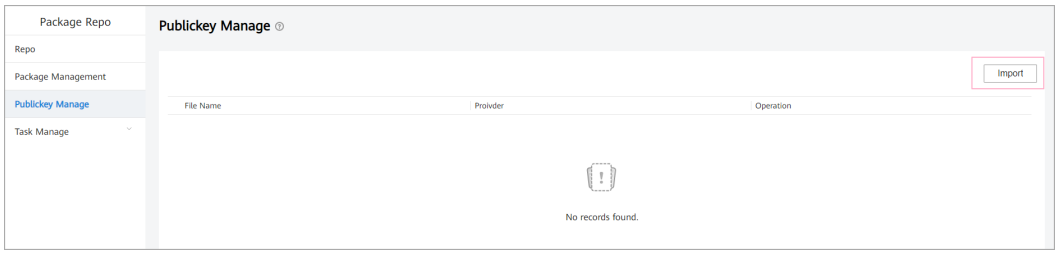
Context

Keys are generated in pairs, including a public key and a private key. The private key is used to sign packages, and the public key is used to verify signatures. If the signature passes the verification, the package is not tampered with.

Procedure

Step 1 Choose **Package Repo** from the main menu. Choose **Publickey Manage** from the navigation pane, and click **Import** on the displayed page.

Figure 4-13 Importing a public key



Step 2 In the **Import** dialog box that is displayed, set **Provider** to the software package provider, and select the public key file.

Figure 4-14 Entering the public key provider

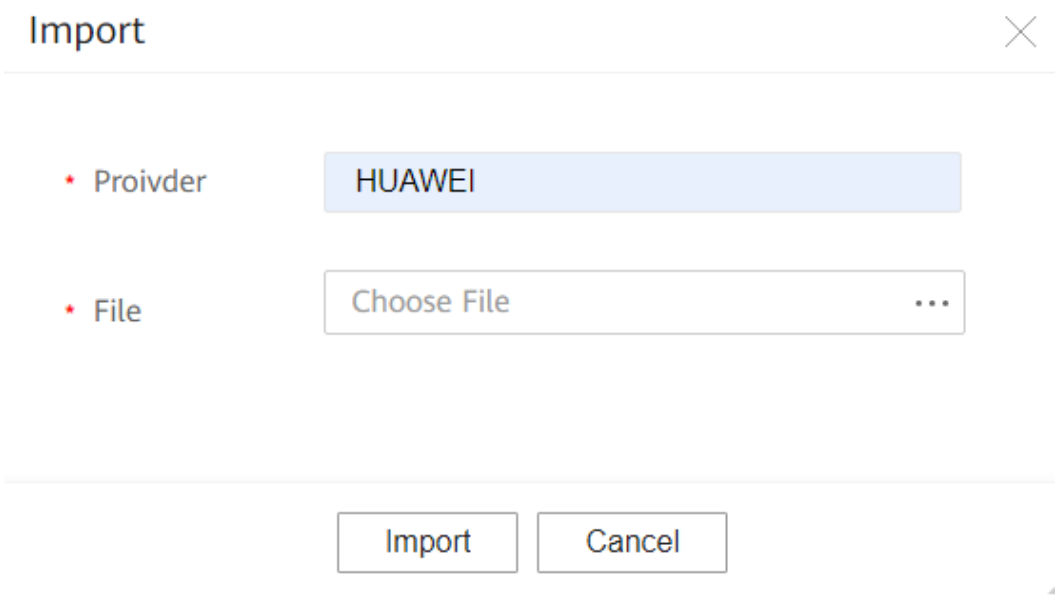
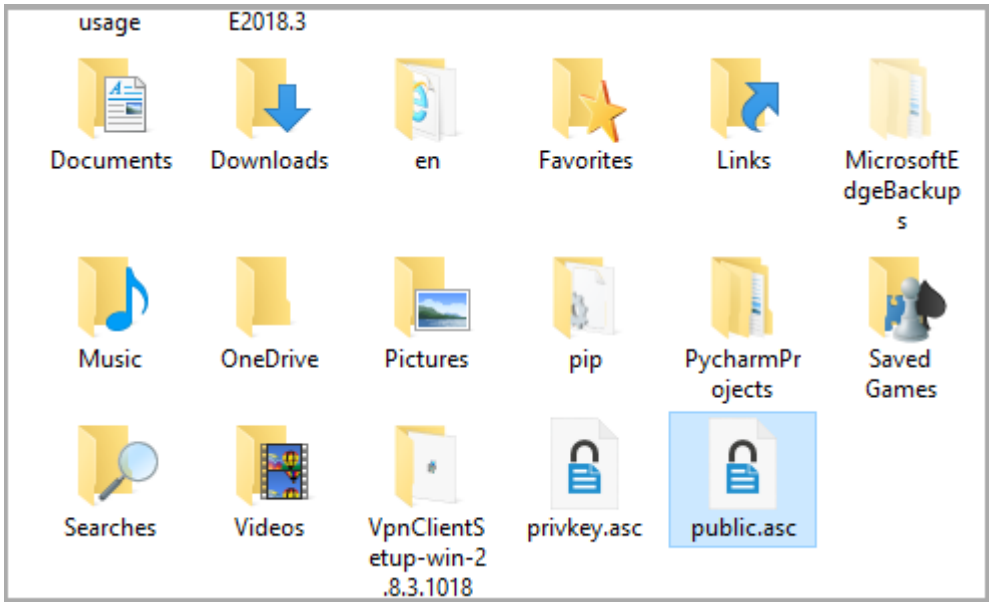
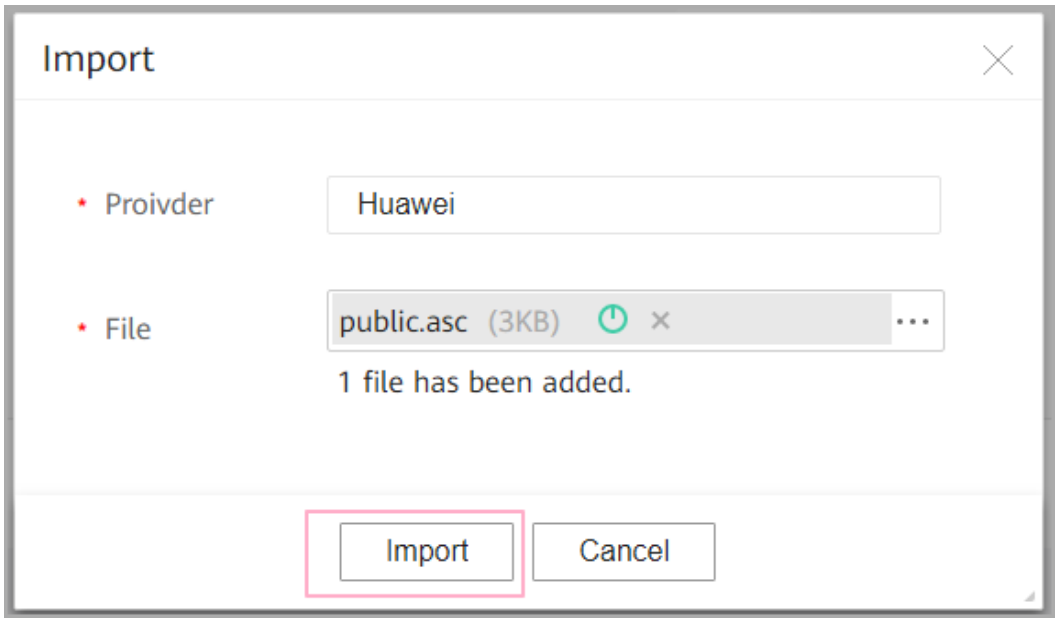


Figure 4-15 Selecting the public key file



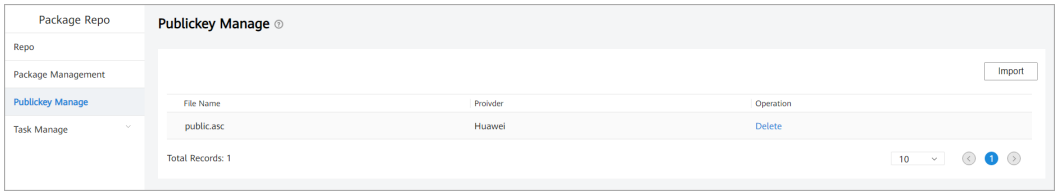
Step 3 Click **Import**.

Figure 4-16 Importing a public key



Step 4 After the public key is imported, you can view it on the **Publickey Manage** page.

Figure 4-17 Successfully importing a public key



----End

Related Operations

To delete a public key, click **Delete** in the **Operation** column.

4.4 Task Management

4.4.1 Managing Software Packages

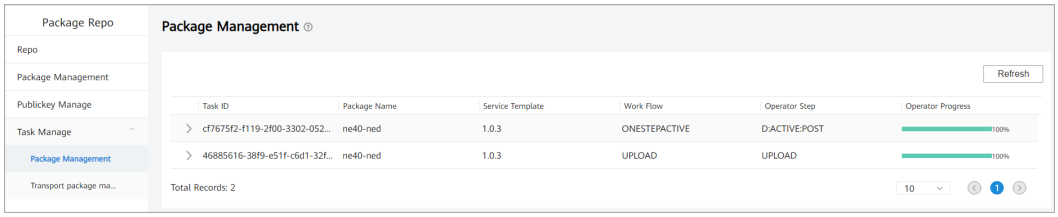
Scenario Description

You can view the progress of each software package task on the page.

Procedure

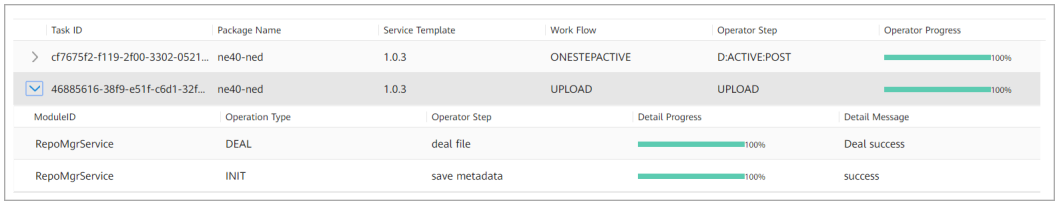
Step 1 Choose **Package Repo** from the main menu. Then choose **Task Manage** > **Package Management** from the navigation pane.

Figure 4-18 Software package view



Step 2 Click the collapse icon on the left of the software package to be viewed to expand the software package task details.

Figure 4-19 Expanding details about a software package task



----End

4.4.2 Managing Transport Packages

A transport package is a collection of product software packages. You can manage software packages in batches.

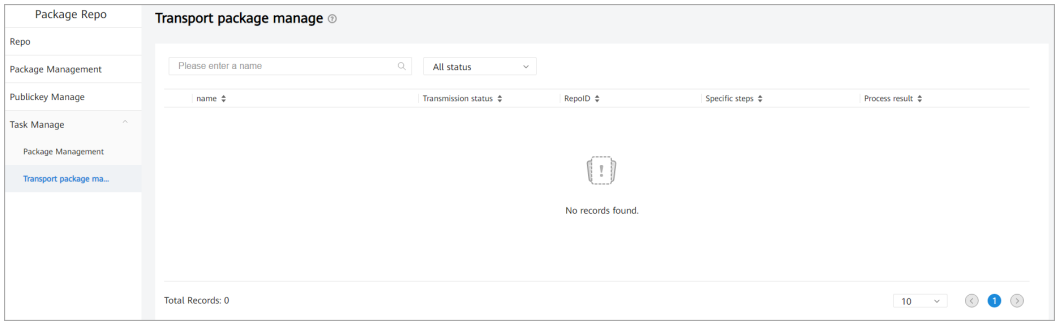
Scenario Description

You can view the progress of each transport package task on the page.

Procedure

Step 1 Choose **Package Repo** from the main menu. Then choose **Task Manage** > **Transport package manage** from the navigation pane.

Figure 4-20 Transport package view



Step 2 Click the collapse icon on the left of the transport package to be viewed to expand the transport package task details.

----End

5 Device Management

5.1 Adding a Device

Prerequisites

- Protocol parameters have been configured on a device.
- The network between the device and NCE is normal.

Scenario Description

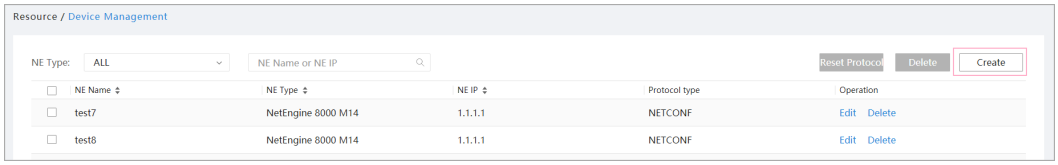
Device adding indicates that a device is added to NCE for management. You can perform subsequent service operations on the device only after the device is managed by NCE.

After a device is added, NCE automatically establishes a NETCONF connection with the device. If the connection is normal, the device status is online. If the device is disconnected, NCE will attempt to establish a connection with the device again.

Procedure

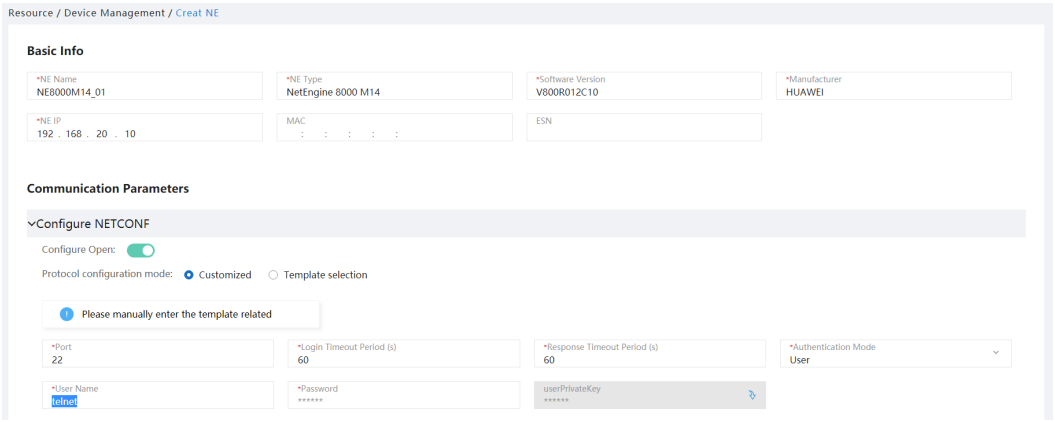
Step 1 Choose **Resource** > **Device Management** from the main menu. On the **Device Management** page, choose **Create** > **Create**.

Figure 5-1 Creating an NE



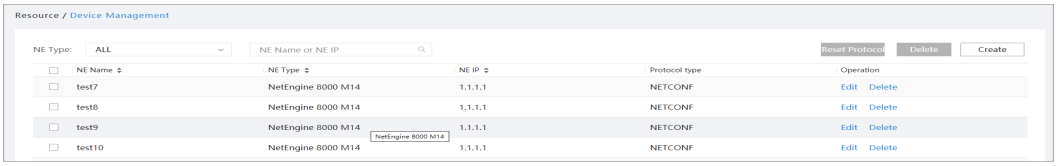
Step 2 On the displayed **Create NE** page, set mandatory parameters such as **NE Name** and **NE IP**, and set communication parameters such as NETCONF and SNMP. You can click **Customized** or **Template selection** to configure communication parameters.

Figure 5-2 Communication parameters



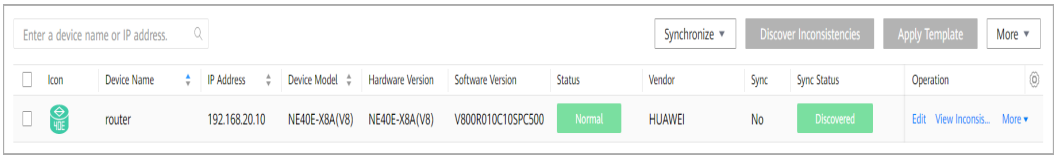
Step 3 After the device is added, you can view the new device on the **Device Management** page.

Figure 5-3 Viewing device information



Step 4 After the protocol connection is established, the device status changes to normal, indicating that the device is successfully managed by NCE. Choose **Device Configuration** > **Device Configuration** from the main menu. to view the device status.

Figure 5-4 Device status



----End

Related Operations

- To edit a device, choose **Resource** > **Device Management**, and click **Edit** in the **Operation** column corresponding to a device.
- To delete a device, choose **Resource** > **Device Management**, and click **Delete** in the **Operation** column corresponding to a device.

5.2 Importing a Device

Prerequisites

- Protocol parameters have been configured on a device.
- The network between the device and NCE is normal.

Scenario Description

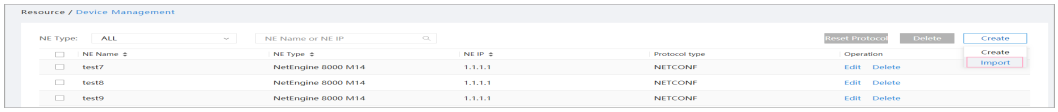
Device import indicates that a device is imported to NCE for management. You can perform subsequent service operations on the device only after the device is managed by NCE.

After a device is imported, NCE automatically establishes a NETCONF connection with the device. If the connection is normal, the device status is online. If the device is disconnected, NCE will attempt to establish a connection with the device again.

Procedure

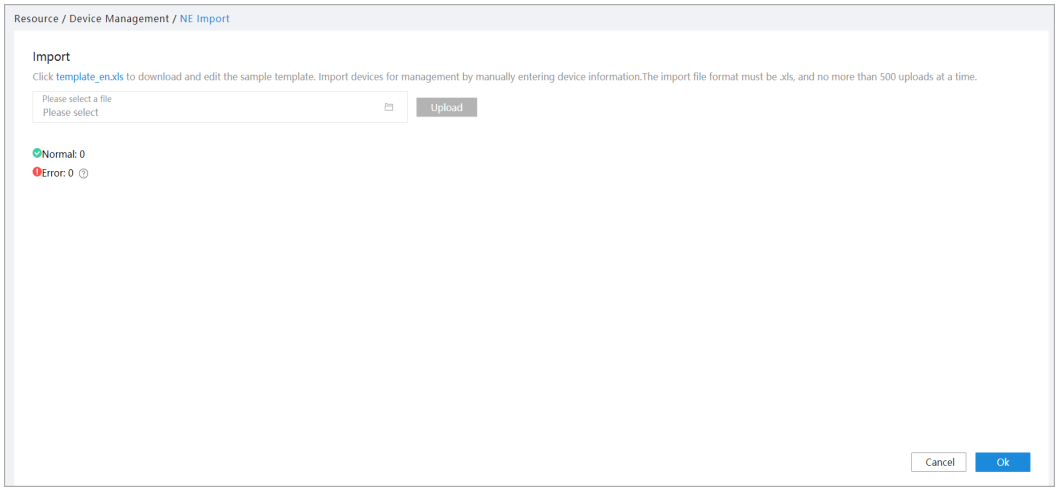
Step 1 Choose **Resource** > **Device Management** from the main menu. On the **Device Management** page, choose **Create** > **Import**.

Figure 5-5 Import



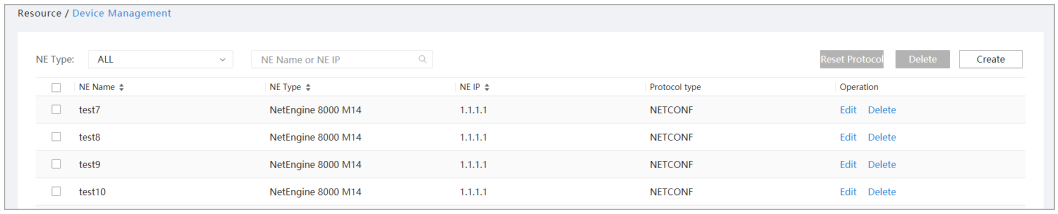
Step 2 On the displayed **NE Import** page, select the template file to be imported and click **Upload**.

Figure 5-6 Importing a template file



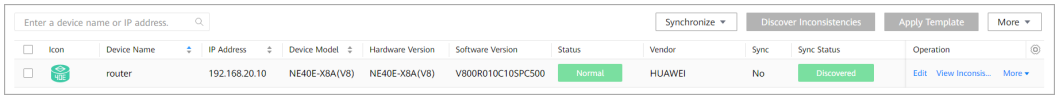
Step 3 After the template file is imported, you can view the new device on the **Device Management** page.

Figure 5-7 Checking the device



Step 4 After the protocol connection is established, the device status changes to normal, indicating that the device is successfully managed by NCE. Choose **Device Configuration** > **Device Configuration** from the main menu. to view the device status.

Figure 5-8 Device status



----End

5.3 Configuring Device Parameter Templates

Scenario Description

Parameter management refers to configuring NETCONF, SNMP, Telnet, and STelnet parameter templates on NCE. When adding a device, you can select the corresponding template.

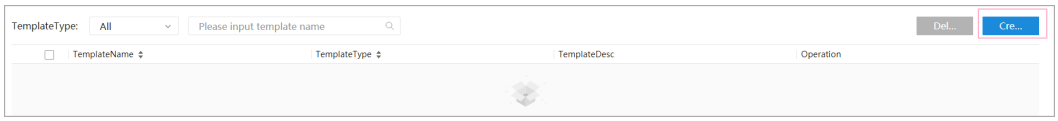
NOTE

The device parameter management function is provided in the development state. This function is unavailable in the official version.

Procedure

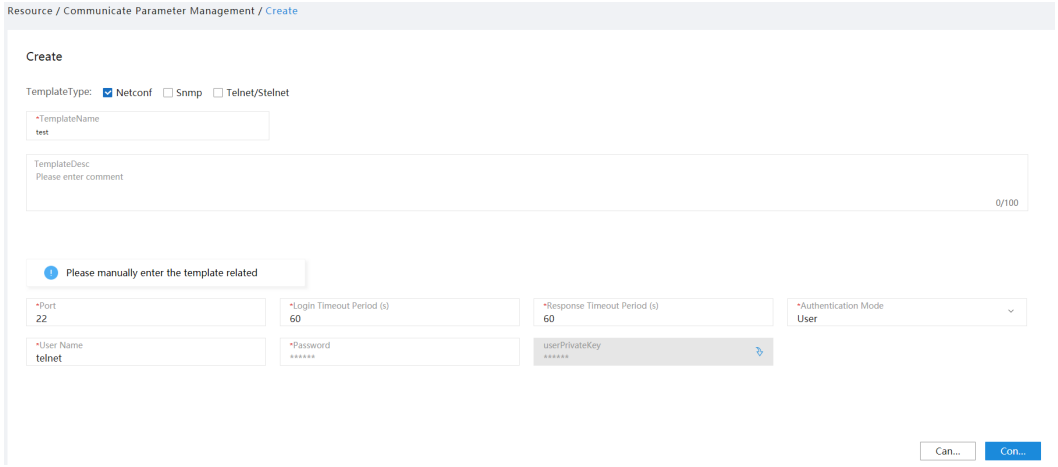
Step 1 Choose **Resource** > **Device Communication Param Templates** from the main menu. On the **Device Communication Param Templates** page, click **Create**.

Figure 5-9 Parameter management



Step 2 On the displayed page, select a template type, configure template information, and click **Confirm**.

Figure 5-10 Template information



Step 3 After the template is created, you can view the new template on the **Device Communication Param Templates** page.

Figure 5-11 Viewing the created template

----End

Related Operations

- To edit device parameters, choose **Resource** > **Device Communication Param Templates**, and click **Edit** in the **Operation** column of a template.
- To delete device parameters, choose **Resource** > **Device Communication Param Templates**, and click **Delete** in the **Operation** column of a template.

5.4 Configuring SNMP

To enable the controller to receive device alarms, you need to set SNMP parameters.

Context

The controller uses SNMP to receive alarms and discover devices and topologies.

If alarm triggering conditions are met, the forwarders send SNMP trap messages to notify the controller of forwarder events, so that network administrators can handle these events in a timely manner.

Prerequisites

Forwarders have been added to the controller.

Procedure

NOTICE

The SNMP protocol does not support data consistency verification. Therefore, once the SNMP configuration is delivered, it cannot be modified on the device. Otherwise, the data between NCE and the device is inconsistent.

Step 1 Choose **Resource** > **SNMP Configuration** from the main menu. On the displayed page, set **Trap Service** and **SNMPv3 Security Parameters**.

Step 2 **Trap Service** allows the controller to transparently transmit trap messages received from forwarders to the trap server. You can determine whether to enable this function.

Set parameters and click **Apply**.

Figure 5-12 Trap service

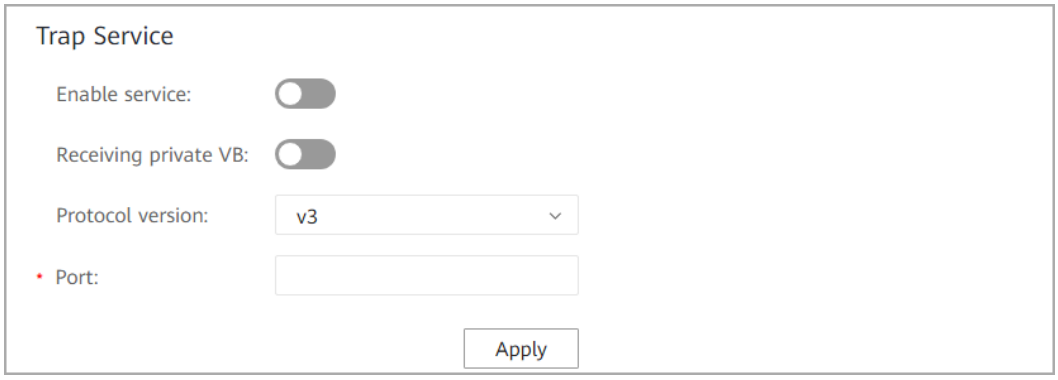


Table 5-1 Trap service parameters

Parameter	Description
Receiving private VB	Whether the controller receives trap messages that carry extended private VBs.
Protocol version	SNMPv3 and SNMPv2c are supported. SNMPv2c has security risks. To improve security, SNMPv3 is recommended.
Port	Port used by the controller to send and receive information.

Step 3 By configuring parameters in the **SNMPv3 Security Parameters** area, the controller can perform authentication and encryption on trap messages received from forwarders before transmitting them.

In the **SNMPv3 Security Parameters** area, click **Create**. In the **Create** dialog box that is displayed, set required parameters and click **OK**.

Figure 5-13 Create

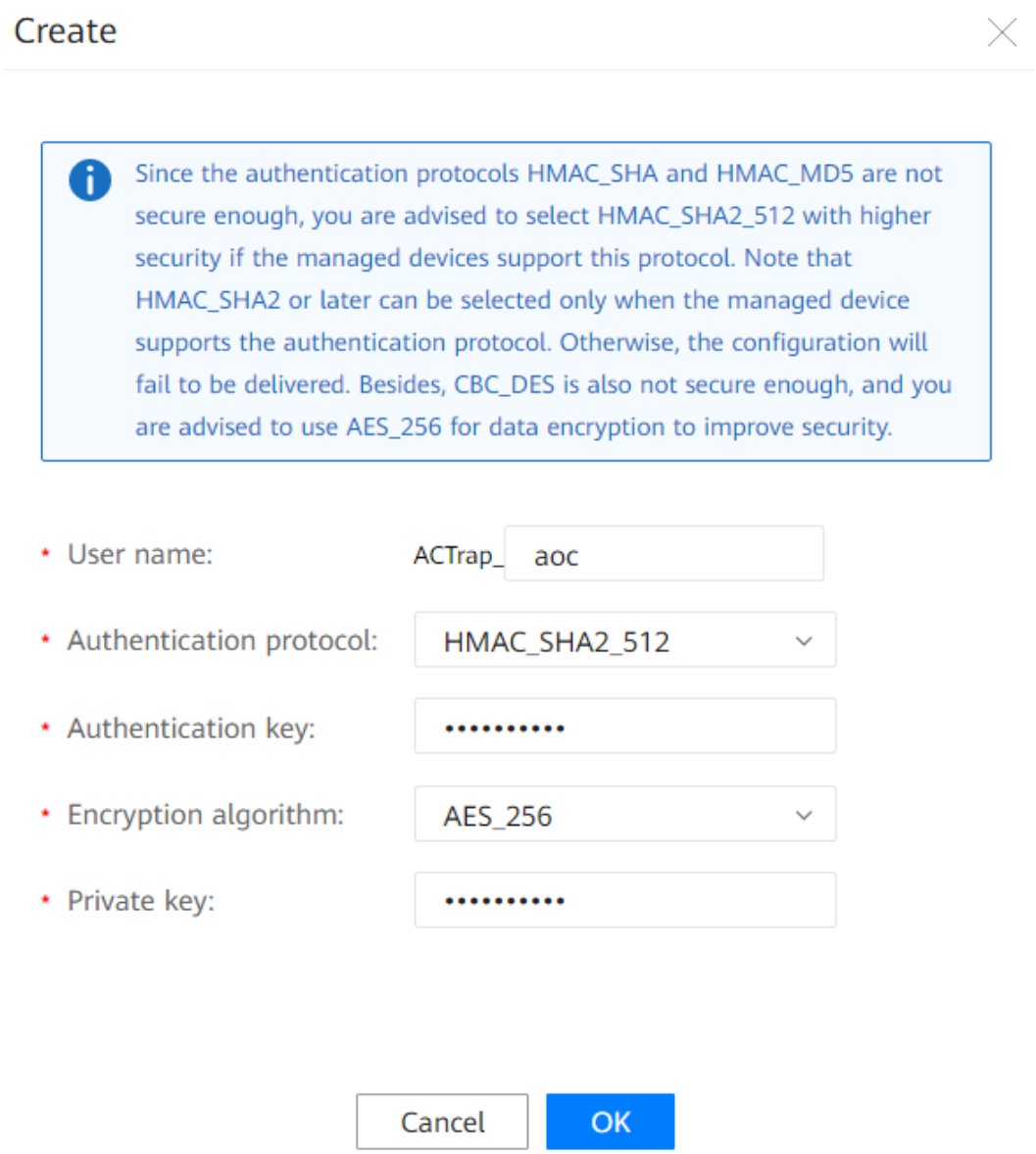


Table 5-2 SNMPv3 security parameters

Parameter	Description
User name	The prefix has a fixed value of **ACTrap**, and the suffix is user-defined. The user name prefixed with **ACTrap** is used only for Agile Controller and cannot be configured using commands.
Authentication protocol	Authentication protocol, which can be SHA, MD5, SHA2_256, SHA2_384, or SHA2_512. You are advised to use SHA2_512 for higher security.
Authentication key	Authentication key.

Parameter	Description
Encryption algorithm	Encryption algorithm, which can be AES_128, AES_256, or CBC_DES. This parameter is optional, but it is recommended that you use AES_256 for higher security.
Private key	Private key for encryption.

----End

5.5 Configuring an SSH Client

To interconnect with a device that supports only the weak encryption algorithm, you need to configure an SSH client and enable risk encryption algorithms.

Context

SSH provides powerful encryption and authentication functions. A public key is generated by the SSH server and bound to the SSH client. The SSH client checks the validity of the public key bound to the SSH server to ensure protocol transmission security and protect devices against attacks such as IP address spoofing and simple password interception. Currently, SSH2.0 is supported.

Prerequisites

The southbound protocols NETCONF and CLI have been configured on a device, and the SSH function has been enabled.

Procedure

Step 1 Choose **Resource** > **SSH Client Configuration** from the main menu.

Step 2 On the **SSH Client Configuration** page, select the **NETCONF** or **CLI** tab to check binding information between all managed SSH servers and RSA or DSA public keys.

Figure 5-14 NETCONF

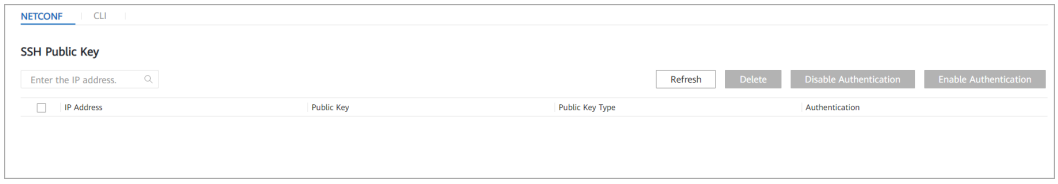
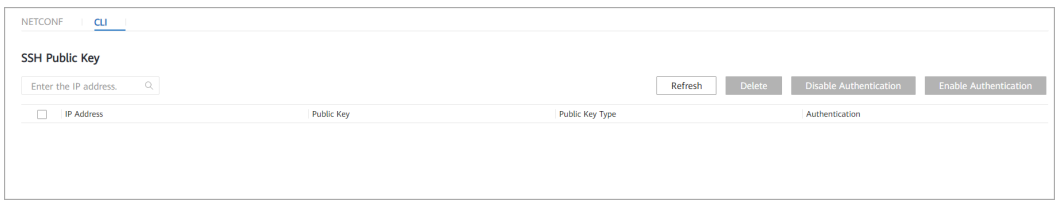


Figure 5-15 CLI



Step 3 (Optional) Enable risk encryption algorithms. Risk encryption algorithms have poor security and are disabled by default. You are not advised to enable risk encryption algorithms.

To enable this function, set **Enable risk encryption algorithms**. In the displayed **Warning** dialog box, click **OK**.

----End

Parameter Description

Table 5-3 Parameters for configuring an SSH client

Parameter	Description
IP Address	IP address of the SSH server.
Public Key	Public key generated by the SSH server. The public key is bound to the SSH client so that the SSH client can authenticate the server.
Public Key Type	Currently, two types of public keys are supported: • RSA: Uses the public key for encryption and private key for decryption. • DSA: Uses the digital signature and authentication to ensure security. The private key is used to sign the files or messages. The SSH client uses the public key to authenticate the signature. The security verification process of DSA is faster than that of RSA.
Authentication	The authentication function is disabled by default. To ensure data transmission security, you are advised to enable this function. • ON • OFF

Follow-up Procedure

You are advised to periodically delete the invalid public key information from the SFTP server. If the peer public key is incorrect, you can click **Delete** to manually delete the SSH public key.

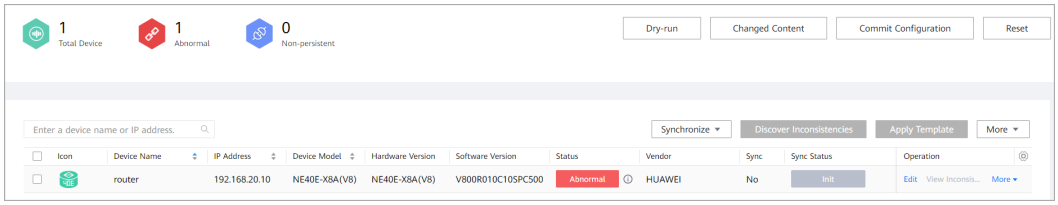
6 Device Configuration

6.1 Configuring a Device on the Web UI

Procedure

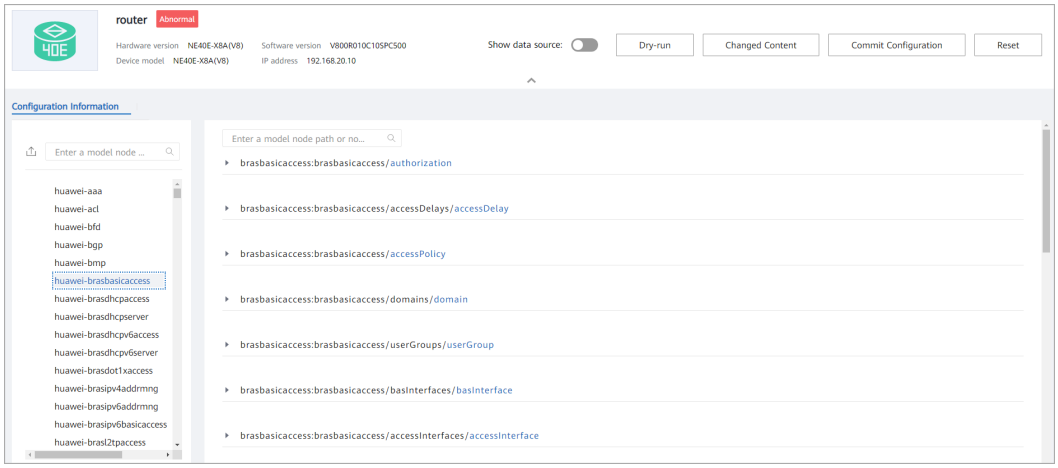
Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu. On the **Device Configuration** page, click **Edit** in the **Operation** column of a device to be configured.

Figure 6-1 Accessing the device configuration page



Step 2 On the page that is displayed, select the required model.

Figure 6-2 Selecting a model

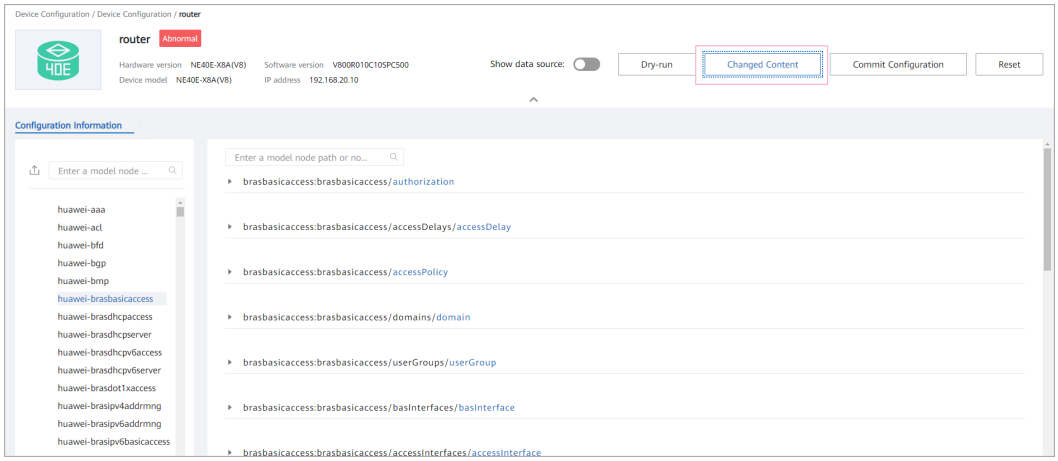


Step 3 Edit the selected model.

Step 4 Click **Dry-run**.

Step 5 Click **Changed Content**.

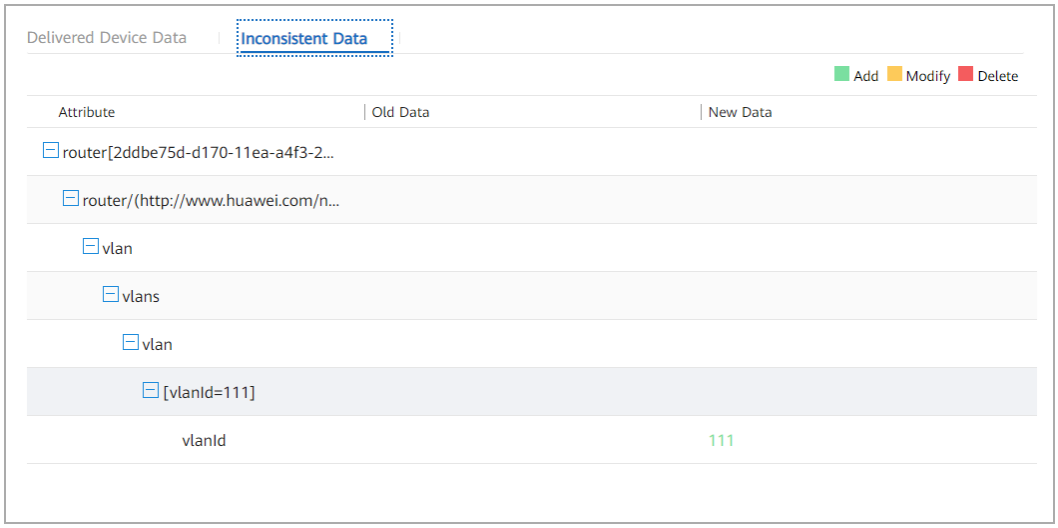
Figure 6-3 Viewing the changed content



Step 6 In the dialog box that is displayed, view the protocol packets delivered to the device.

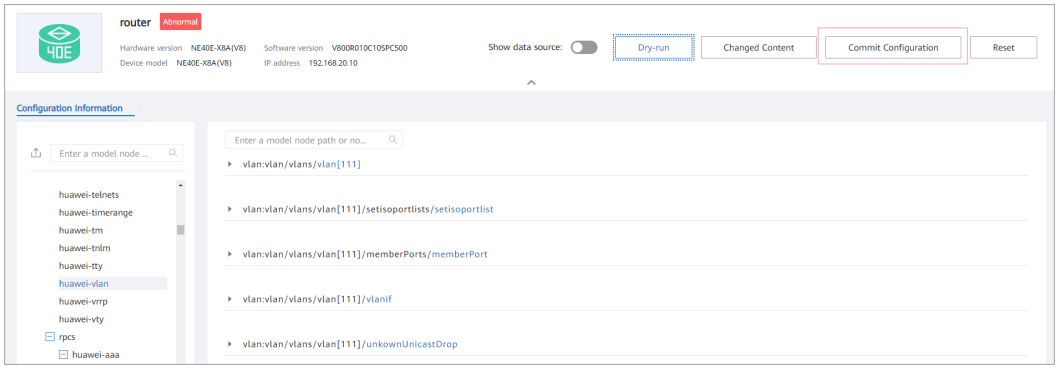
Figure 6-4 Previewing device data to be delivered

Figure 6-5 Previewing inconsistent data



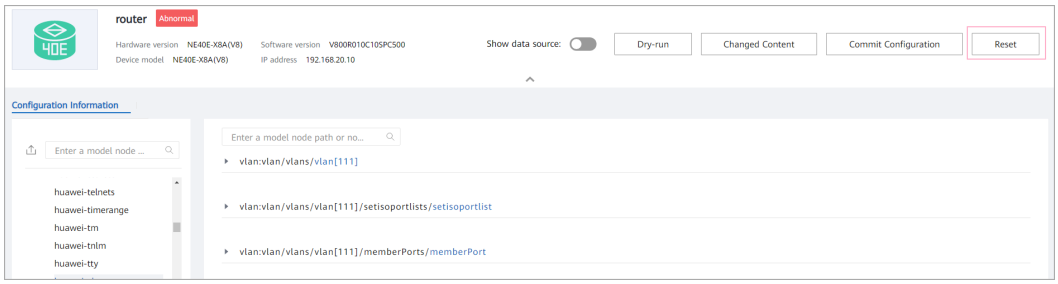
Step 7 If the result meets expectations, click **Commit Configuration**.

Figure 6-6 Committing the configuration



Step 8 If the result does not meet expectations or reconfiguration is required, click **Reset**.

Figure 6-7 Resetting data



NOTE

- After a user opens a web page, the foreground applies for a transaction ID from the background. If the user does not edit the page for a long time, the background will age the transaction ID. The default validity period of a transaction ID is 5 days. If the third-party package used for editing the configuration is forcibly uninstalled, the background clears the transaction ID that is being used. If the user continues to use the old transaction ID to edit the configuration, a dialog box is displayed, indicating that the local transaction ID has expired. In this case, click **OK** and then click **Reset** to edit the configuration again.
- If multiple users modify the same data at the same time, a transaction conflict may occur. In this case, click **OK** and then click **Reset** to edit the configuration again.

  Specifications of transaction conflicts

  – In the following scenarios, no conflict will occur:
    1. Multiple users modify irrelevant data nodes at the same time.
    2. User 1 and user 2 perform operations at the same time. Node A functions as a container or list node. User 1 deletes Node A, and user 2 adds Subnode B under Node A. User 1 commits the configuration first, then user 2 commits the configuration of adding Subnode B without refreshing the page. In this scenario, no conflict will occur, and Node A and Subnode B are retained.
  – In the following scenarios, a conflict will occur:
    1. Multiple users modify the same leaf node at the same time, and commit the configurations in sequence.
    2. User 1 and user 2 perform operations at the same time. Node A functions as a container or list node, and contains Node B that functions as a leaf or leaflist node. User 1 deletes Node A, and user 2 modifies or deletes Node B. User 1 commits the configuration first, and then user 2 directly commits the configuration without refreshing the page.

----End

6.2 Configuring a Device Using the Northbound CLI

Step 1 Choose **CLI** from the main menu. The CLI is displayed.

```
Welcome to NCE CLI
[NCE]>
```

Step 2 **Optional:** Run a command to enter the device view.

```
[NCE]> nes ne ?
[ipi-zba900-r-bn-01]
[NCE]> nes ne ipi-zba900-r-bn-01
[nes:nes/ne[ipi-zba900-r-bn-01]]>
```

Step 3 Edit device features.


```
[nes:nes/ne[ipi-zba900-r-bn-01]]> sys
syslog  system
[nes:nes/ne[ipi-zba900-r-bn-01]]> system
systemInfo  fileCollectTaskInfos
[nes:nes/ne[ipi-zba900-r-bn-01]]> system systemInfo
sysName sysContact  sysLocation sysDesc sysObjectId sysGmtTime  sysUpTime  sysService  platformName
[nes:nes/ne[ipi-zba900-r-bn-01]]> system systemInfo sysName Huawei1
[nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]>
```

Step 4 Conduct a dry-run on the device features.

```
[nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]> dry-run
[OK]
```

Step 5 Preview the configuration of device features.

```
[nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]> display dry-run preview
### ipi-zba900-r-bn-01  ###
<system xmlns="https://www.huawei.com/netconf/vrp/huawei-system">
<systemInfo>
<sysName>Huawei1</sysName>
</systemInfo>
</system>
[nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]>
```

- If the displayed result in **Step 5** meets expectations, commit the configuration.
  ```
  [nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]> commit
  ```
- To delete the configuration, reset the configuration.
  ```
  [nes:nes/ne[ipi-zba900-r-bn-01]/huawei-system/system:system/systemInfo]> return
  [NCE]> reset
  ```

----End

6.3 Verifying Device Data Consistency

Prerequisites

A southbound device has been imported to NCE, and the network connection between the southbound device and NCE is working properly.

Scenario Description

- Configuration comparison

  If the southbound device is configured offline or data is lost after it restarts unexpectedly, the configurations of the southbound device and NCE will be inconsistent.

  To learn the differences between the NE configurations on NCE and running configurations on southbound devices, click **Discover Inconsistencies**.
- If the NE configurations on NCE and running configurations on forwarders are inconsistent:
  - If forwarder configurations are considered correct, select **Synchronize from Device** to synchronize inconsistent configurations from forwarders to NCE.
  - If NE configurations on NCE are considered correct, select **Synchronize to Device** to synchronize inconsistent configurations from NCE to forwarders.

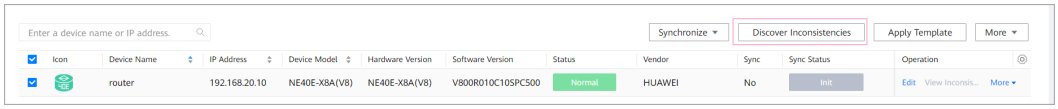
  In normal cases, the NE configurations on NCE and forwarder configurations must be consistent.

6.3.1 Comparing Configurations

Procedure

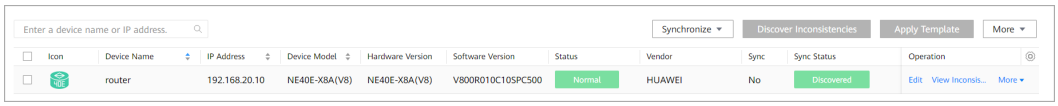
Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu. On the **Device Configuration** page that is displayed, select a southbound device and click **Discover Inconsistencies**.

Figure 6-8 Triggering inconsistency discovery



Step 2 After inconsistency discovery is complete, the value of **Sync Status** changes to **Discovered**. Click **View Inconsistencies** in the **Operation** column to access the inconsistency display page and view the inconsistent configurations.

Figure 6-9 Inconsistency discovery completed



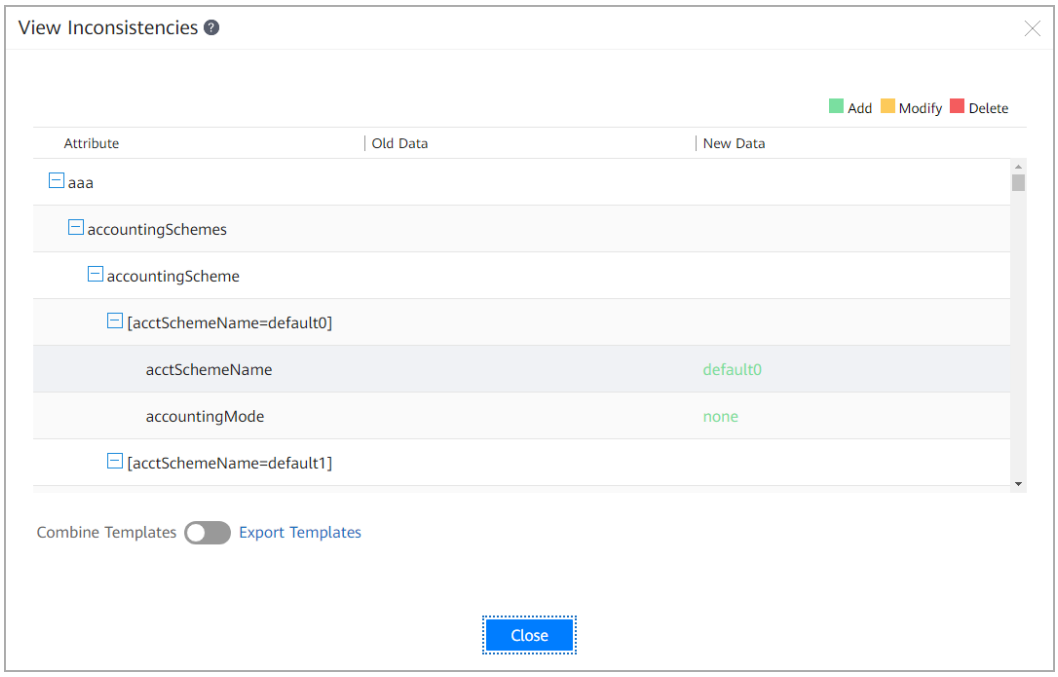
NOTE

The value of **Sync** indicates whether the forwarder and NCE configurations are consistent.

If the value is **No**, the forwarder and NCE configurations may be inconsistent, and the actual result depends on the SND implementation. To determine whether the configurations are consistent, use the inconsistency discovery function.

Step 3 On the inconsistency display page, the data in the **Old Data** column indicates the NCE data, and the data in the **New Data** column indicates the forwarder data.

Figure 6-10 Inconsistency display page



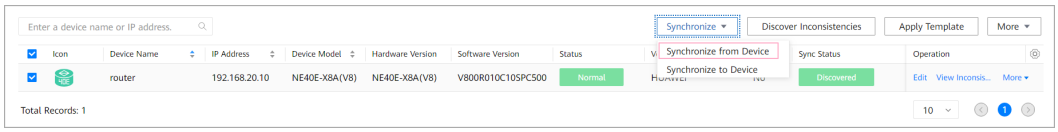
----End

6.3.2 Synchronizing Data from a Device

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu. On the **Device Configuration** page that is displayed, select a southbound device, click **Synchronize**, and select **Synchronize from Device**.

Figure 6-11 Triggering synchronization



Step 2 After data is successfully synchronized, the value of **Sync Status** changes to **Synchronized**. Click **View Inconsistencies** in the **Operation** column to access the inconsistency display page and view the inconsistent configurations between NCE and the forwarder before the synchronization.

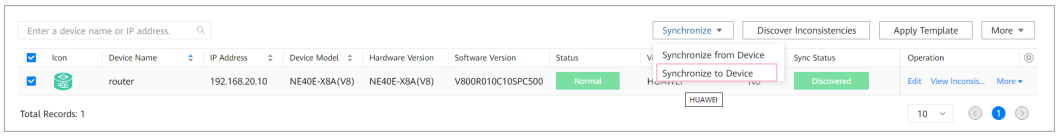
----End

6.3.3 Data Consistency Verification

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu. On the **Device Configuration** page that is displayed, select a southbound device, click **Synchronize**, and select **Synchronize to Device**.

Figure 6-12 Triggering data consistency verification



Step 2 After data consistency verification is complete, the value of **Sync Status** changes to **Reconciled**. Click **View Inconsistencies** in the **Operation** column to access the inconsistency display page and view the inconsistent configurations between NCE and the forwarder before the data consistency verification.

----End

6.3.4 Saving Southbound Device Configurations

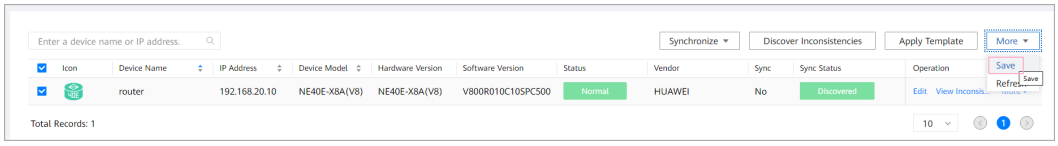
Context

After NCE delivers configurations (including data consistency verification) to a southbound device, the southbound device needs to periodically save the configurations to prevent configuration loss caused by device restarts. Theoretically, devices should automatically save the configurations. However, some devices cannot automatically save configurations. To prevent this problem, NCE provides the function of manually saving southbound device configurations.

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu. Select a southbound device, click **More**, and select **Save**.

Figure 6-13 Triggering the saving of southbound device configurations



Step 2 View the saving result. After southbound device configurations are saved successfully, the saving result is **Success**.

----End

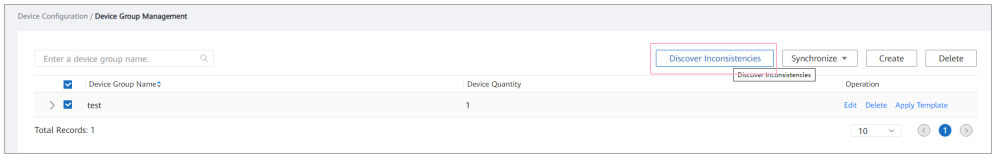
6.3.5 Managing Device Group Data Consistency

Procedure

Step 1 Choose **Device Configuration** > **Device Group Management** from the main menu. Then select a device group.

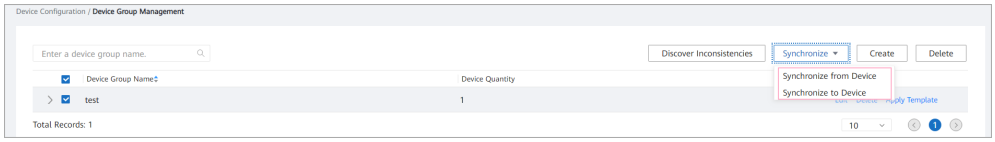
- Click **Discover Inconsistencies** to trigger inconsistency discovery for the device group.

Figure 6-14 Triggering inconsistency discovery for a device group



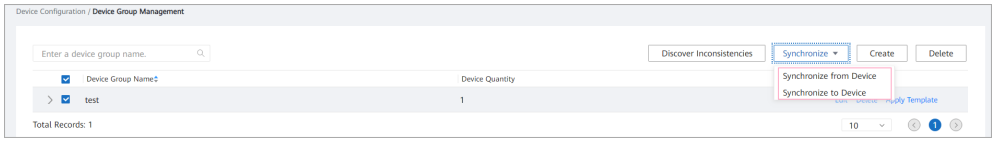
- Click **Synchronize** and select **Synchronize from Device** to trigger synchronization for the device group.

Figure 6-15 Triggering synchronization for a device group



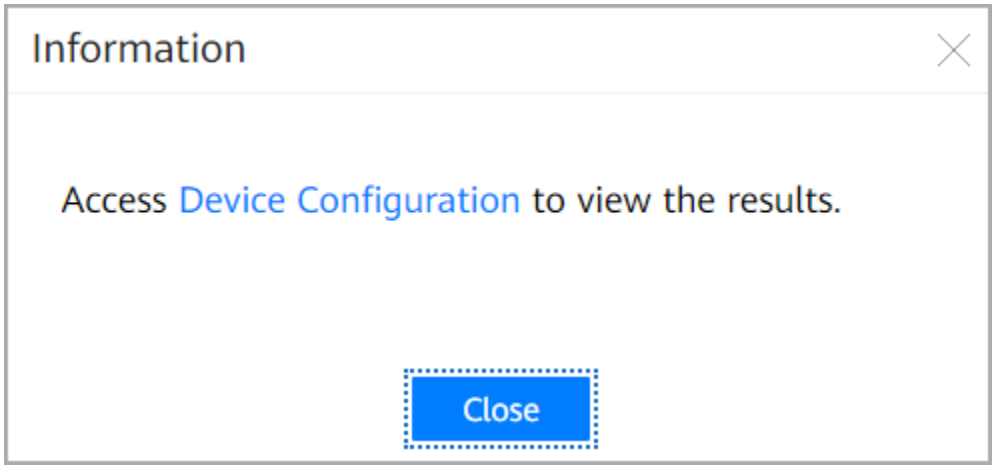
- Click **Synchronize** and select **Synchronize to Device** to trigger data consistency verification for the device group.

Figure 6-16 Triggering data consistency verification for a device group



Step 2 After inconsistency discovery, synchronization, or data consistency verification is triggered for a device group, the **Information** dialog box is displayed. Click the hyperlink in the dialog box to access the **Device Configuration** page and view the operating status of specific devices.

Figure 6-17 Dialog box that contains the hyperlink for accessing the **Device Configuration** page



----End

6.3.6 Managing Configuration Records

Context

NCE provides the configuration record function. You can view device configuration records on the **Device View** and **Record View** pages. In addition, you can view the configuration records delivered to southbound devices after service instances are decomposed.

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration History** from the main menu.

The **Device Configuration History** page displays configuration records by device or record sequence.

Figure 6-18 Device view

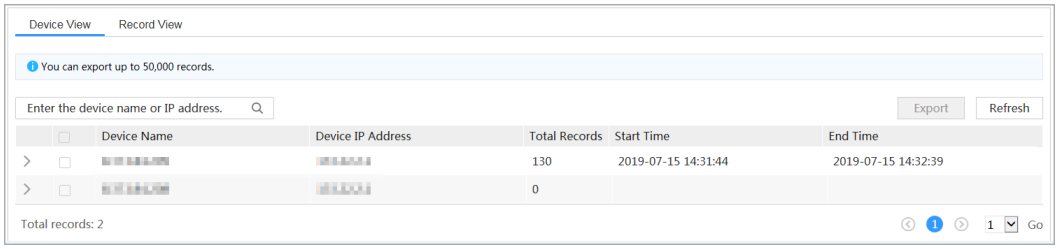
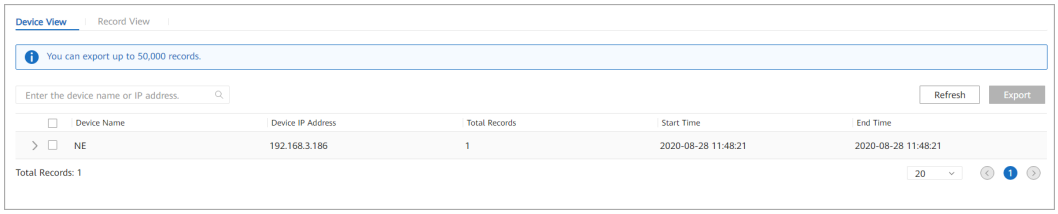
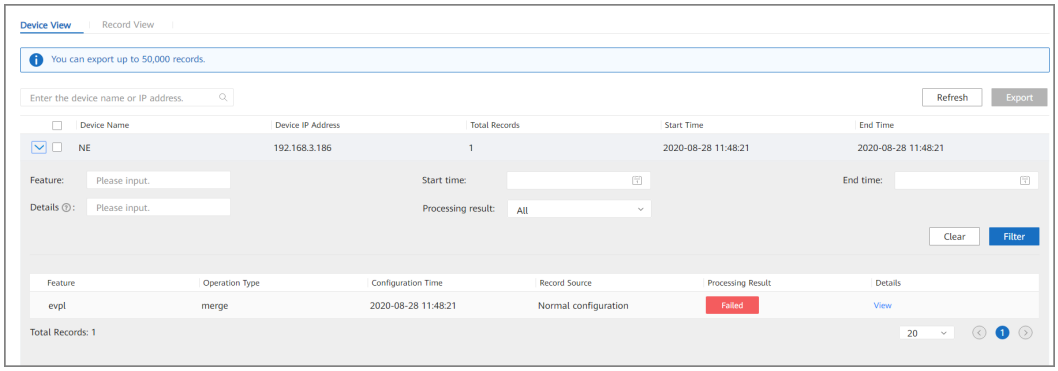


Figure 6-19 Record view



Step 2 In the device view, click > to view the configuration record details. Click **View** in the **Details** column to view the configuration data delivered by NCE to southbound devices.

Figure 6-20 Configuration record details in the device view



NOTE

If too many records exist, filter them by **Feature**, **Details**, **Start time**, **End time**, and **Processing result**.

Table 6-1 Configuration record parameters

Parameter	Description
Device Name	Name of a southbound device.
Device IP Address	IP address of a southbound device.
Total Records	Number of configuration records delivered by NCE to a southbound device.
Start Time	Start time of configuration delivery.
End Time	End time of configuration delivery.
Feature	Name of a feature.
Operation Type	Operation type of delivered packets.
Configuration Time	Configuration time of a feature.
Record Source	There are two record sources: • Normal configuration • Rollback configuration
Processing Result	There are two processing results: • Succeed • Failed
Details	Check the configuration data delivered by NCE to a southbound device.

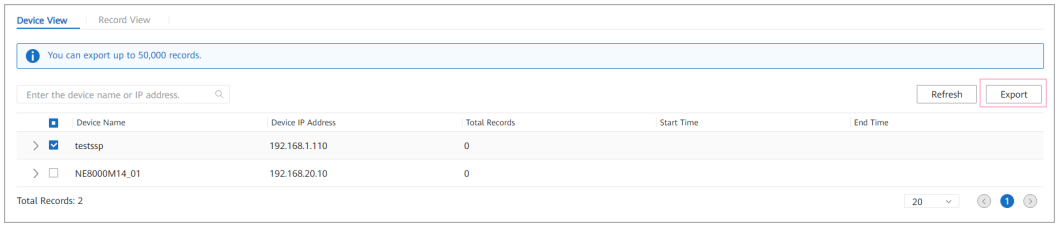
Step 3 Compared with the device view, the record view has two more fields: **Transaction ID** and **Service Instance**.

Table 6-2 Fields specific to the record view

Parameter	Description
Transaction ID	Transaction ID used when NCE delivers configurations to a southbound device. This field is empty when configurations are delivered in non-transaction mode.
Service Instance	Service instance path configured for a southbound device.

Step 4 In the device view, select a southbound device and click **Export** to export the southbound device configuration records of the selected device. After the records have been exported, the exported records are automatically downloaded.

Figure 6-21 Export operation in the device view



Step 5 In the record view, select configuration records, and click **Export**. In the dialog box that is displayed, click **Export all data** or **Export selected data** to export specific device configuration records. After the records have been exported, the exported records are automatically downloaded.

Figure 6-22 Export operation in the record view

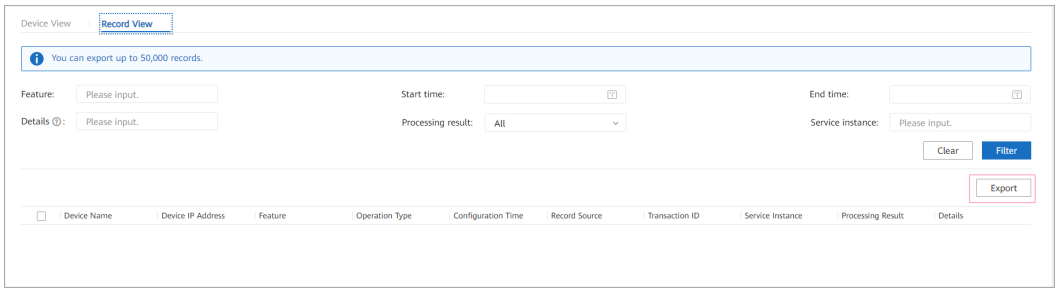
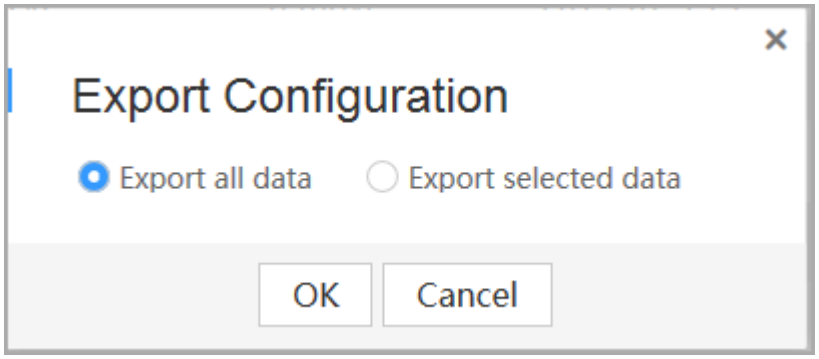


Figure 6-23 Options for exporting configuration records



----End

6.4 Device Group Management

Scenario Description

Before applying a template or template group to multiple devices, add these devices to the same device group. A device group may contain multiple devices and device groups.

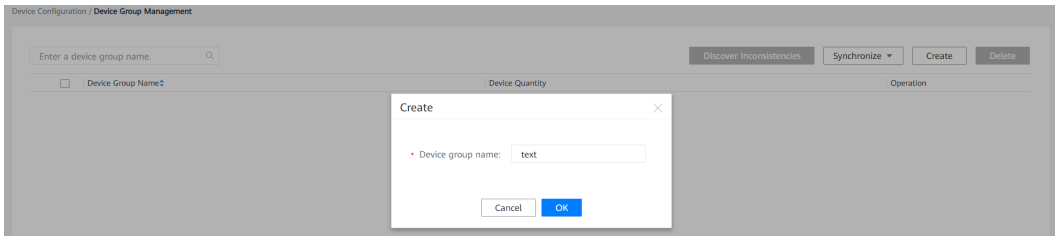
6.4.1 Creating a Device Group

Procedure

Step 1 Choose **Device Configuration** > **Device Group Management** from the main menu.

Step 2 On the **Device Group Management** page that is displayed, click **Create**. In the dialog box that is displayed, enter the device group name and click **OK**.

Figure 6-24 Creating a device group



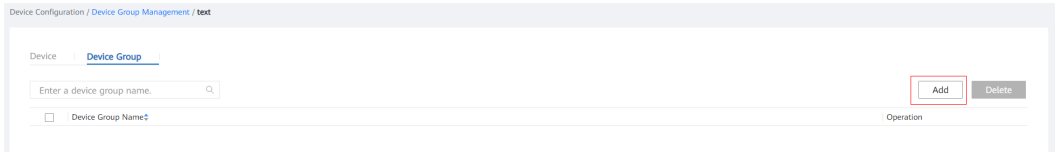
Step 3 In the displayed list, add a sub device group or device.

NOTE

- On the **Device** tab page, click **Add** to add a device.
- On the **Device Group** tab page, click **Add** to add a sub device group.

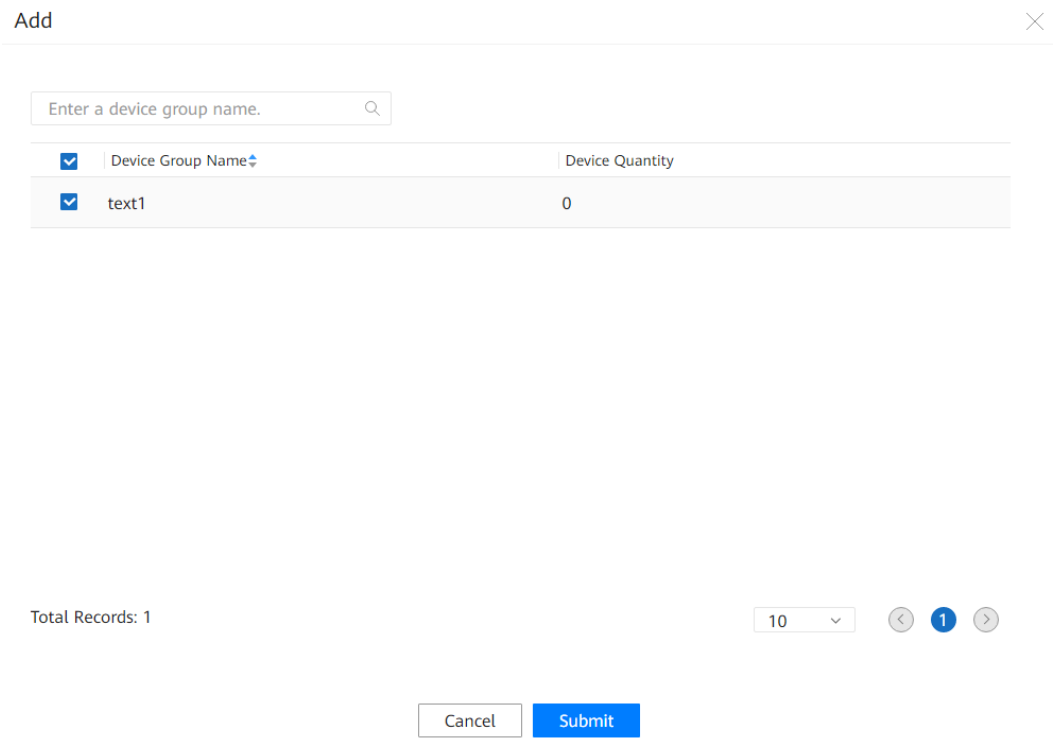
The following example adds a sub device group.

Figure 6-25 Adding a sub device group



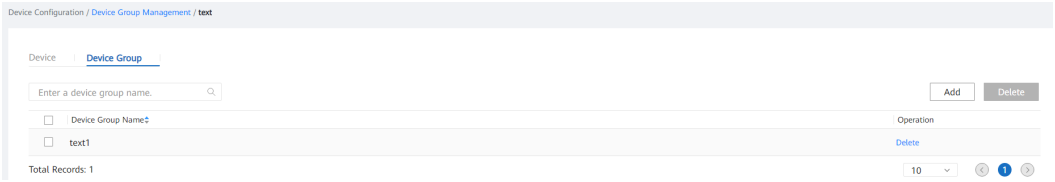
Step 4 In the displayed list, select the device or device group to be added and click **Submit**.

Figure 6-26 Selecting a sub device group



Step 5 On the **Device Group** tab page, you can view the added sub device group.

Figure 6-27 Viewing the added sub device group



Step 6 Click **Device Group Management** in the upper left corner to return to the **Device Group Management** page and view the created device group.

----End

Related Operations

- To edit a device group, choose **Device Configuration** > **Device Group Management**. On the page that is displayed, click **Edit** in the **Operation** column.
- To delete a device group, choose **Device Configuration** > **Device Group Management**. On the page that is displayed, click **Delete** in the **Operation** column.

6.5 Applying a Template

Scenario Description

To orchestrate and deliver configurations to devices or networks in batches, you can select devices or device groups or access the **Application Template** page from the **Service Management** page to orchestrate configuration templates and deliver configurations.

6.5.1 Applying a Template to a Device

Prerequisites

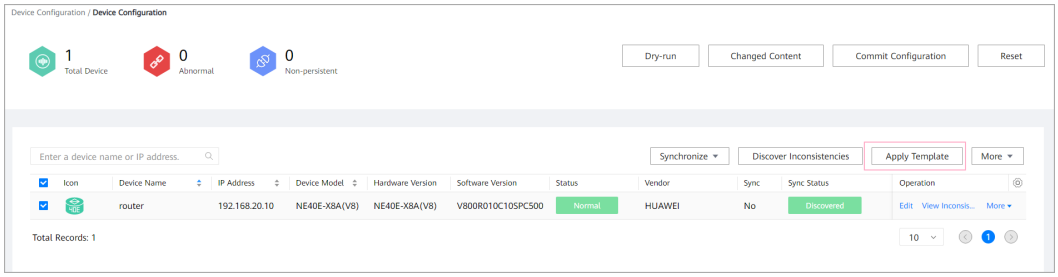
- Interconnection between NCE and the device is normal.
- A template has been created according to **8.1.3 Creating an NE Template**.
- (Optional) The parameter set required by the template has been created according to **8.4.1 Creating a Parameter Set**.

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu.

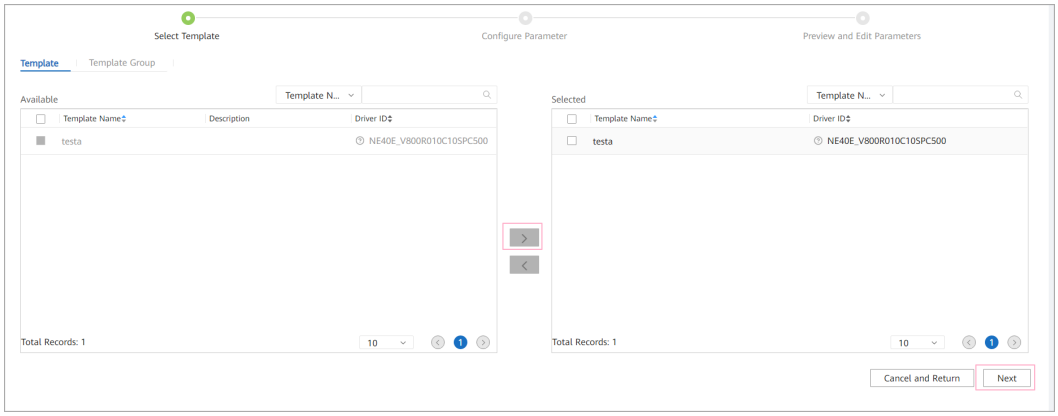
Step 2 On the **Device Configuration** page that is displayed, select a device and click **Apply Template**. Alternatively, click **More** in the **Operation** column of the device, and select **Apply Template**.

Figure 6-28 Accessing the **Apply Template** page from the **Device Configuration** page



Step 3 On the **Template** tab page, select a template in the available template area, click >, and click **Next**. Alternatively, click the **Template Group** tab, and select a template group in the available template group area. Then click > and click **Next**.

Figure 6-29 Adding a template

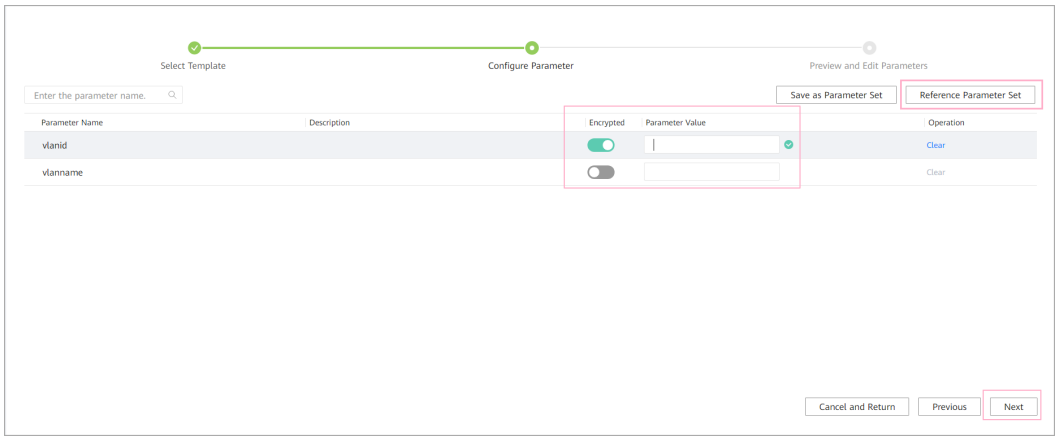


Step 4 On the **Configure Parameter** page that is displayed, modify parameter values and click **Next**.

You can modify the parameters as follows:

- Click **Reference Parameter Set** to reference the parameter content in a parameter set.
- Enable the **Encrypted** function if a parameter needs to be displayed in ciphertext on the GUI.
- Directly enter the parameter value.

Figure 6-30 Configuring parameters



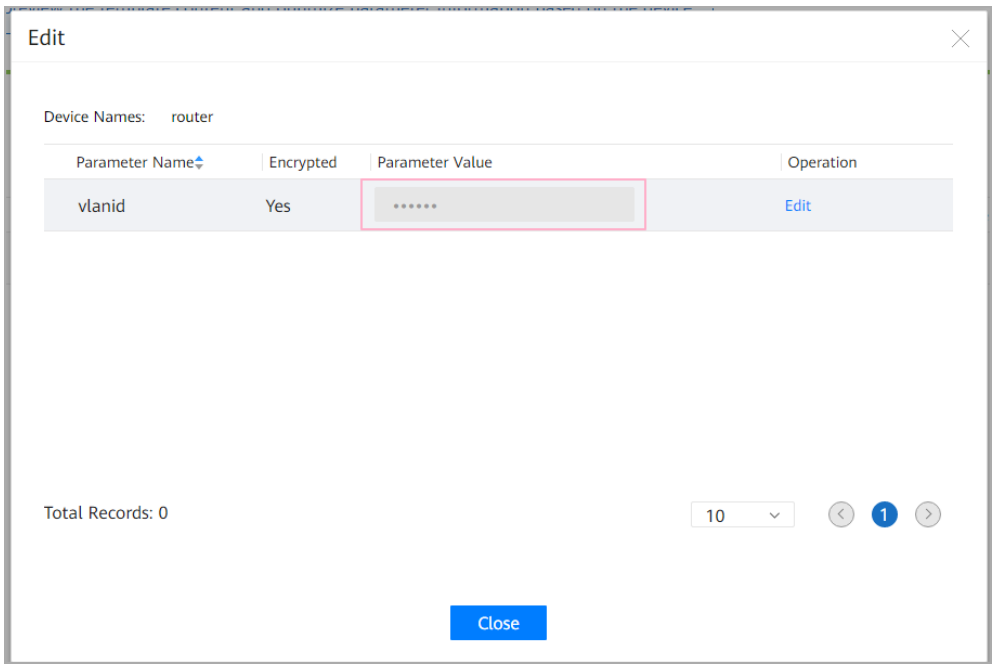
Step 5 Preview and edit parameters.

1. On the **Preview and Edit Parameters** page that is displayed, click **View** in the **Operation** column of a device.
2. View the template content in the preview dialog box that is displayed.

Figure 6-31 Viewing the template content

3. Click **Edit** in the **Operation** column of a device.
4. In the edit dialog box that is displayed, click **Edit** to modify a parameter value. After completing the modification, click **Save**.

Figure 6-32 Setting parameters



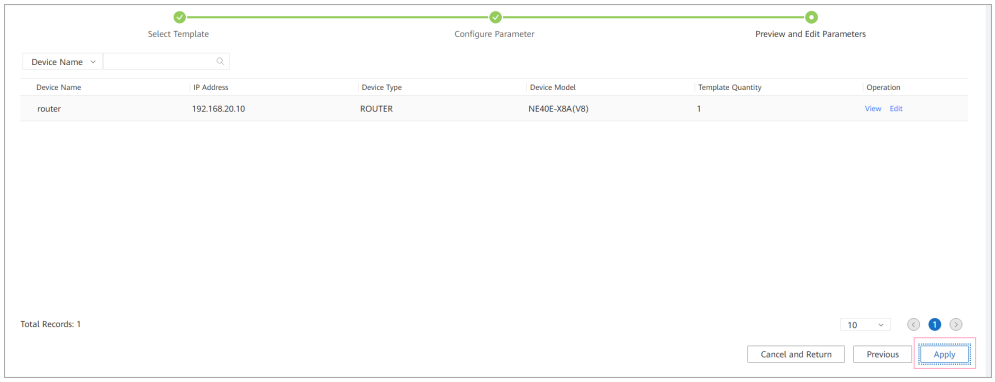
Step 6 Deliver a template.

NOTE

- To commit the configuration to the cache of NCE and deliver the configuration to the device, click **Submit and deliver**.
- To commit the configuration to NCE only, click **Submit**.

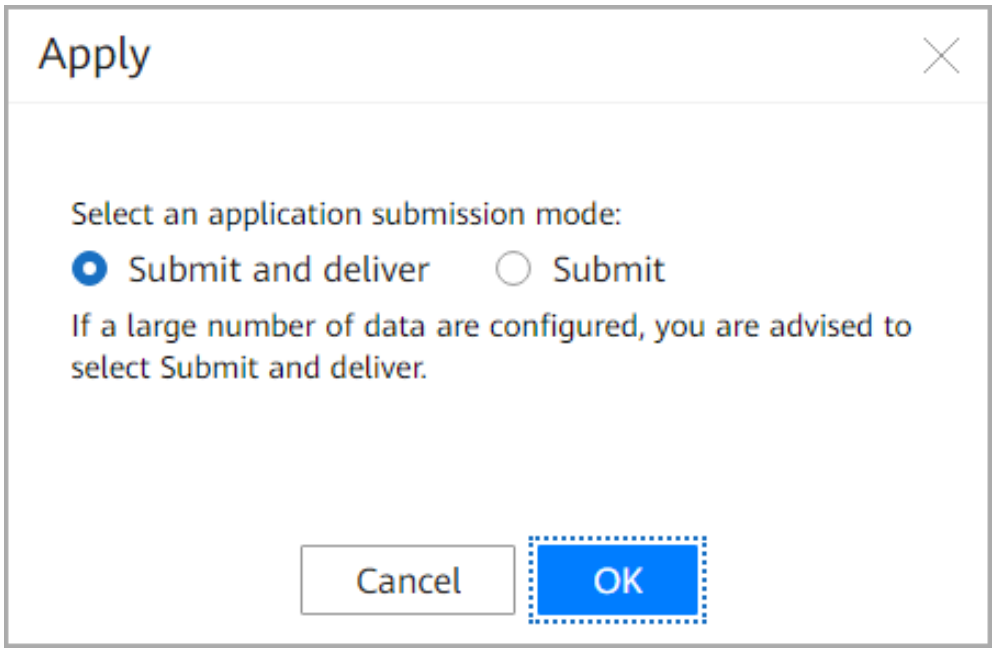
1. Click **Apply**.

Figure 6-33 Applying a template



2. In the dialog box that is displayed, click **Submit and deliver** and click **OK**.

Figure 6-34 Apply dialog box



----End

6.5.2 Applying a Template to a Device Group

Procedure

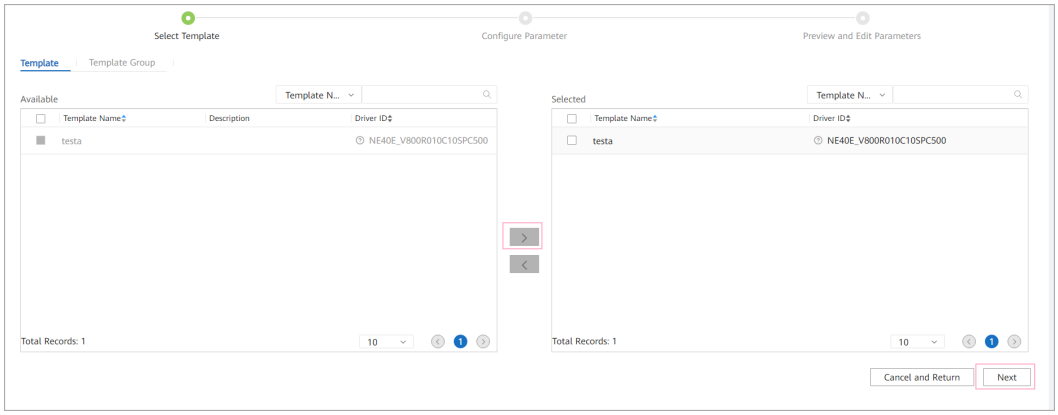
Step 1 Choose **Device Configuration** > **Device Group Management** from the main menu.

Step 2 On the **Device Group Management** page that is displayed, click **Apply Template** in the **Operation** column of a device group.

Figure 6-35 Accessing the **Apply Template** page from the **Device Group Management** page

Step 3 On the **Template** tab page, select a template in the available template area, click >, and click **Next**. Alternatively, click the **Template Group** tab, and select a template group in the available template group area. Then click > and click **Next**.

Figure 6-36 Adding a template

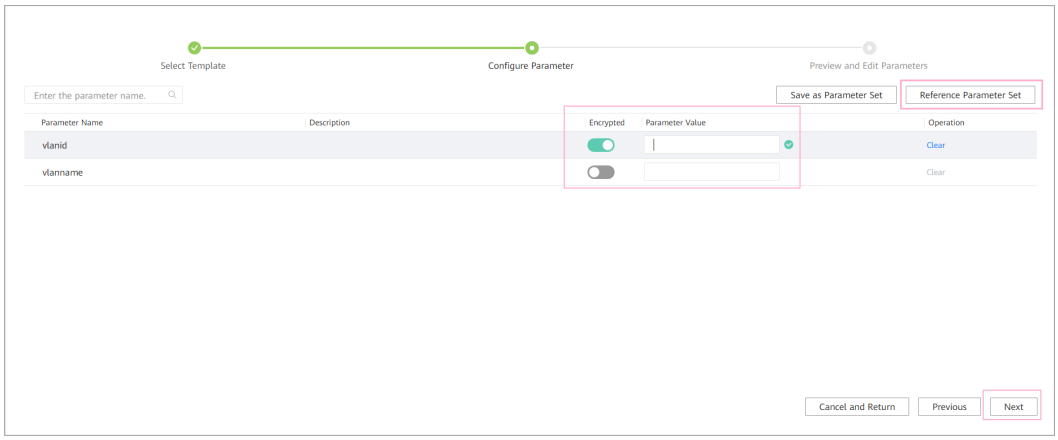


Step 4 On the **Configure Parameter** page that is displayed, modify parameter values and click **Next**.

You can modify the parameters as follows:

- Click **Reference Parameter Set** to reference the parameter content in a parameter set.
- Enable the **Encrypted** function if a parameter needs to be displayed in ciphertext on the GUI.
- Directly enter the parameter value.

Figure 6-37 Configuring parameters



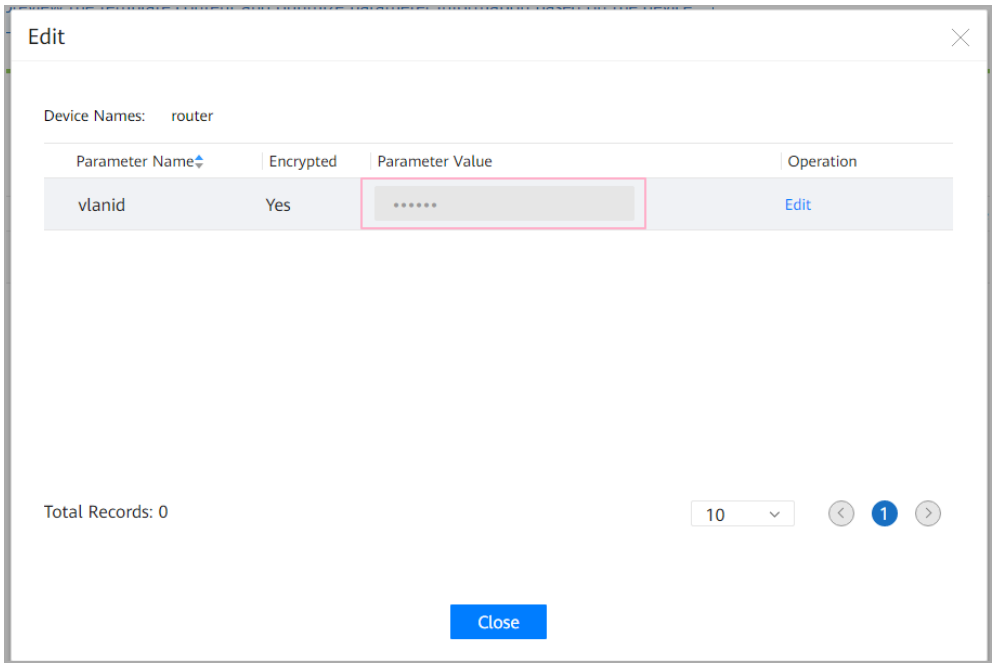
Step 5 Preview and edit parameters.

1. On the **Preview and Edit Parameters** page that is displayed, click **View** in the **Operation** column of a device.
2. View the template content in the preview dialog box that is displayed.

Figure 6-38 Viewing the template content

3. Click **Edit** in the **Operation** column of a device.
4. In the edit dialog box that is displayed, click **Edit** to modify a parameter value. After completing the modification, click **Save**.

Figure 6-39 Setting parameters



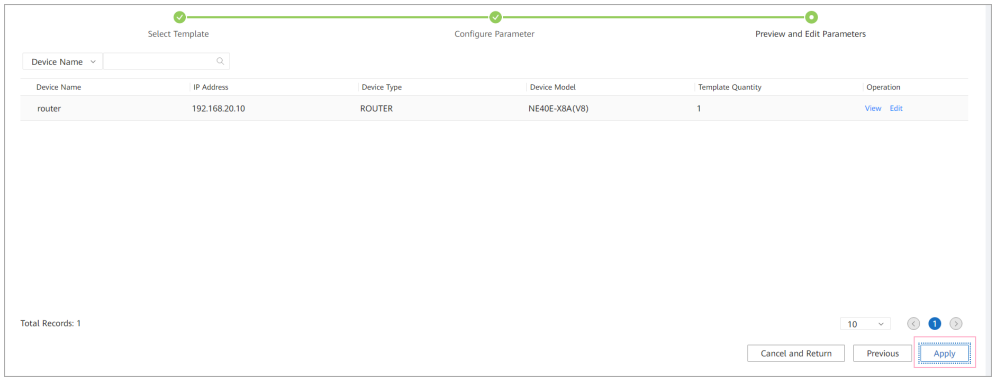
Step 6 Deliver a template.

NOTE

- To commit the configuration to the cache of NCE and deliver the configuration to the device, click **Submit and deliver**.
- To commit the configuration to NCE only, click **Submit**.

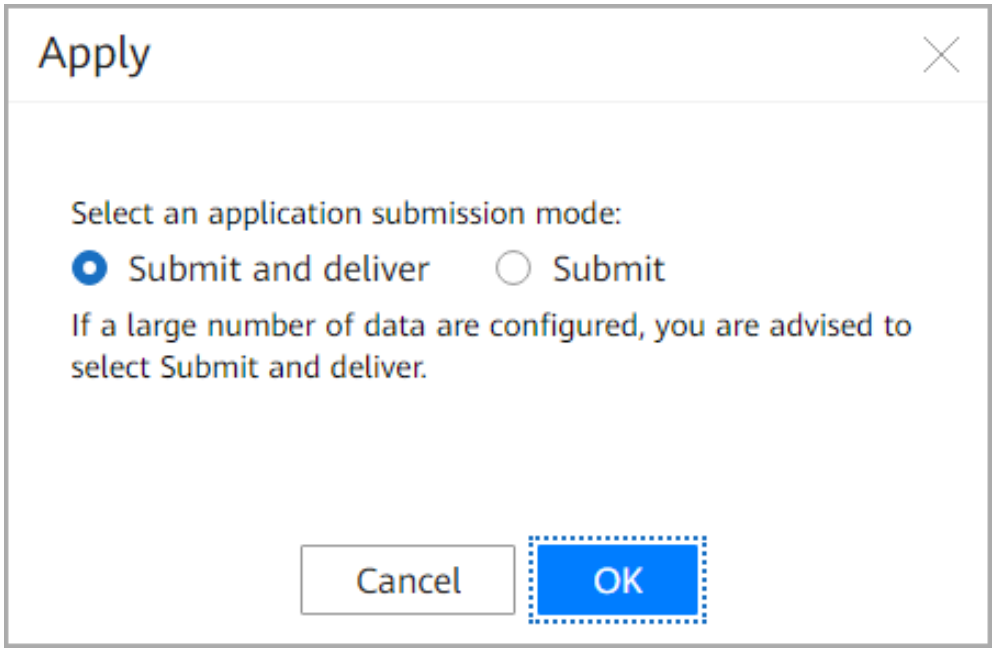
1. Click **Apply**.

Figure 6-40 Applying a template



2. In the dialog box that is displayed, click **Submit and deliver** and click **OK**.

Figure 6-41 Apply dialog box



----End

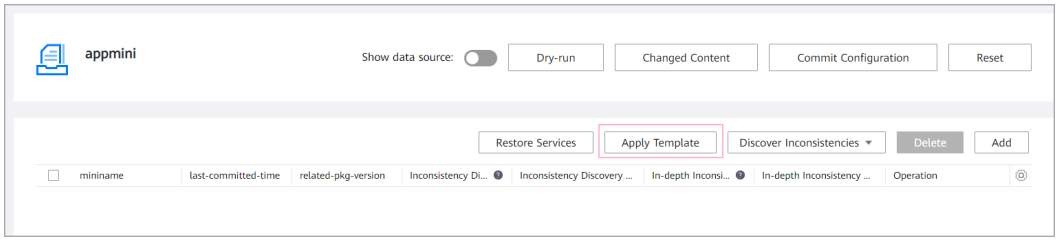
6.5.3 Applying a Template to a Network-Level Service

Procedure

Step 1 Choose **Service Management** from the main menu. The **Service Management** page is displayed.

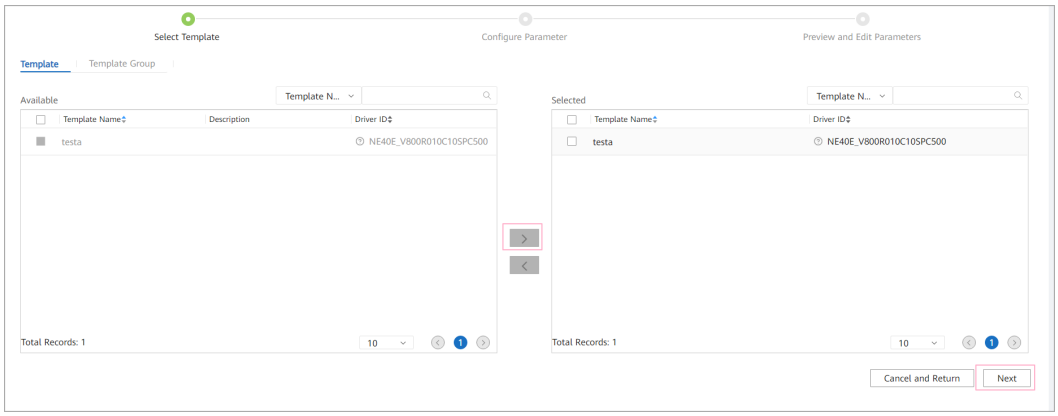
Step 2 On the **Service Management** page that is displayed, click **Apply Template** to access the **Apply Template** page.

Figure 6-42 Accessing the **Apply Template** page from the **Service Management** page



Step 3 On the **Template** tab page, select a template in the available template area, click >, and click **Next**. Alternatively, click the **Template Group** tab, and select a template group in the available template group area. Then click > and click **Next**.

Figure 6-43 Adding a template

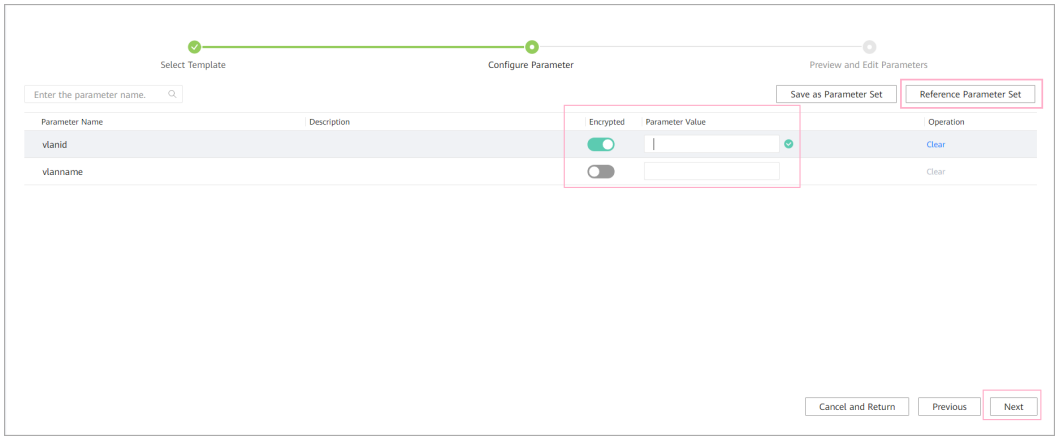


Step 4 On the **Configure Parameter** page that is displayed, modify parameter values and click **Next**.

You can modify the parameters as follows:

- Click **Reference Parameter Set** to reference the parameter content in a parameter set.
- Enable the **Encrypted** function if a parameter needs to be displayed in ciphertext on the GUI.
- Directly enter the parameter value.

Figure 6-44 Configuring parameters



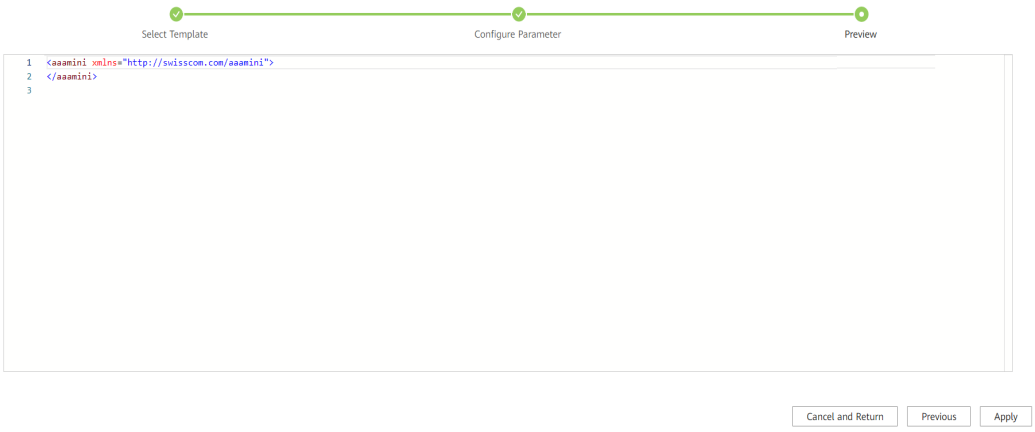
Step 5 Preview the template.

Figure 6-45 Viewing the template content

```
1  <aaamini xmlns="http://swisscom.com/aaamini">
2    <username>12345</username>
3  </aaamini>
4
```

Step 6 Click **Apply** to deliver the template.

Figure 6-46 Applying a template



----End

7 Service Configuration

This chapter describes how to configure services on multiple devices using the service management function. You can configure services on the service management page or using commands.

Prerequisites

- Devices are online.
- Service packages have been activated.

Scenario Description

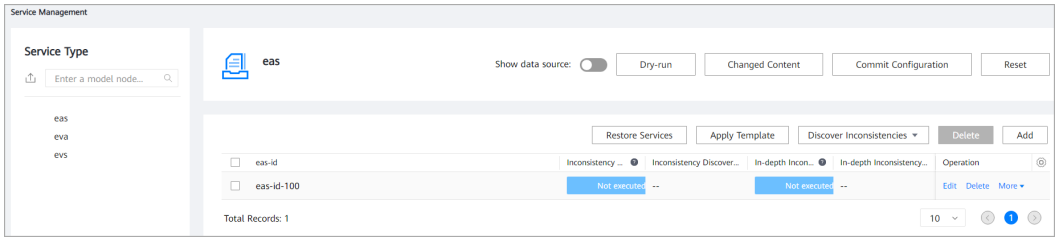
This scenario applies if you need to perform end-to-end service configurations across devices on NCE.

7.1 Configuring Services on the Web UI

Procedure

Step 1 Choose **Service Management** from the main menu. On the **Service Management** page that is displayed, click the required service model.

Figure 7-1 Selecting a service model



NOTE

The service type information in the left pane of the **Service Management** page derives from the instances defined in the service package.

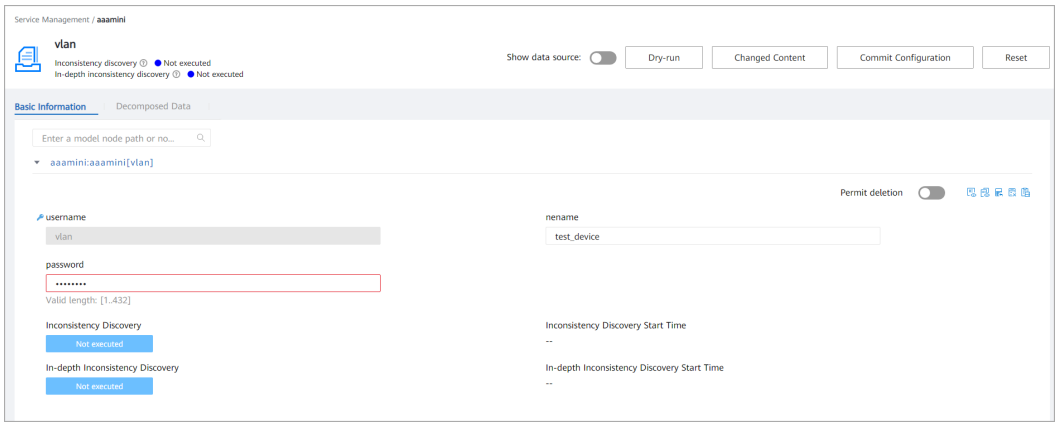
Step 2 Click **Edit** to edit the model data.

Click to recompute the data of a service instance that is not modified.

NOTE

After a service instance is updated, it is decomposed and recomputed. The decomposed data is updated to the latest based on the current computing result and corresponds to the current configuration of the service instance.

Figure 7-2 Recomputing data



NOTE

On the **Service Management** page, you can trigger recomputing of a service instance that is not modified. When this function is used, the service instance is recomputed and converted to logic codes for delivery.

When a service instance is modified, the internal code logic is invoked to recompute and deliver configurations. Therefore, you can update or create a service instance to deliver modified configurations to devices.

In some scenarios, the service instance is not updated, but the internal code logic needs to be invoked to recompute and deliver service configurations. For example:

1. If the service processing code changes while the service instance configurations do not change, the configurations need to be recomputed and delivered again.
2. If the device configuration is modified in other modes, for example, through the CLI or synchronization on NCE, the service instance needs to be deployed again to overwrite the synchronized data.

Click to undeploy a service instance.

NOTE

On the **Service Management** page, you can trigger undeployment of a service instance. When this function is used, the service instance deletes decomposed NE configurations.

If services of devices are affected after decomposed NE configurations are deleted by the service instance and the original network configurations needs to be retained, roll back the NE configurations and wait for the configurations to be delivered again. (Recomputing must be triggered before configuration redelivery.)

Step 3 Click **Changed Content** to view service data changes.

Figure 7-3 Clicking **Changed Content**

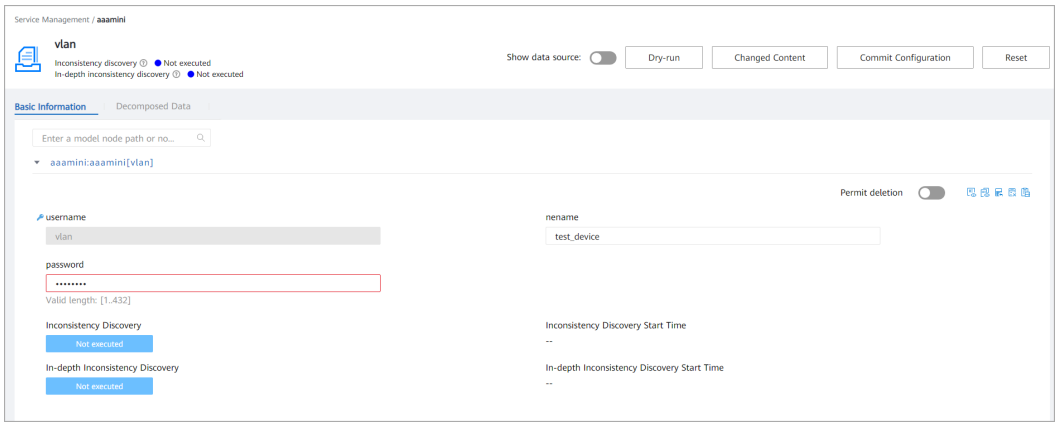
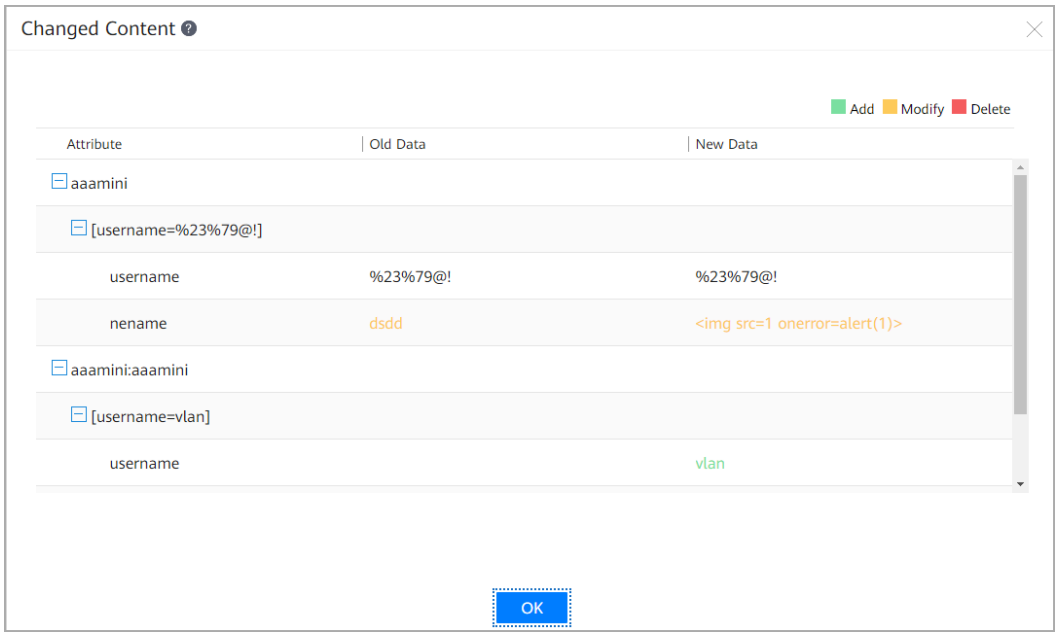
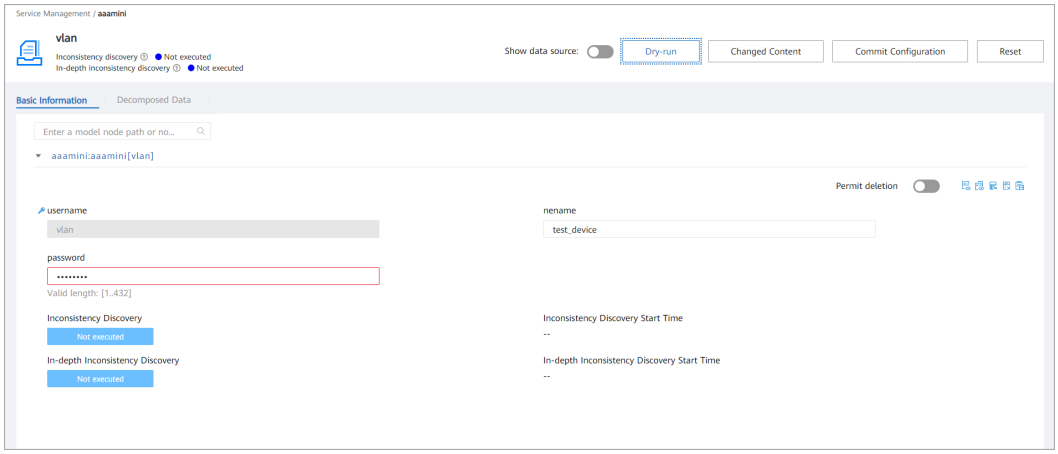


Figure 7-4 Viewing service data changes



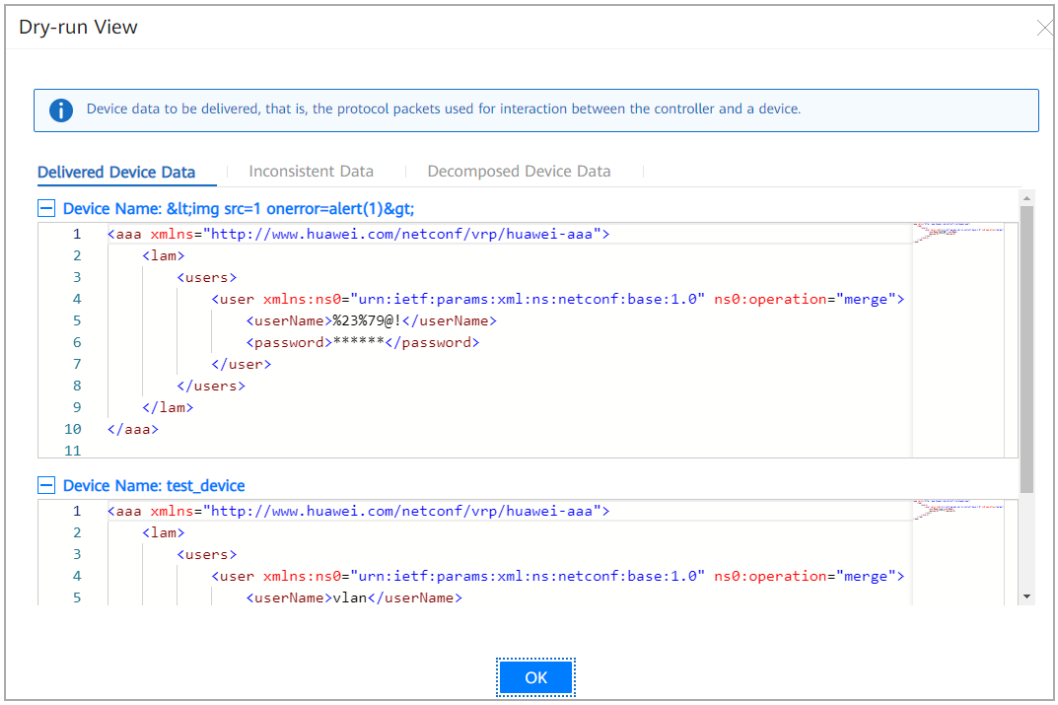
Step 4 Click **Dry-run** to check whether the configuration is correct.

Figure 7-5 Clicking **Dry-run**



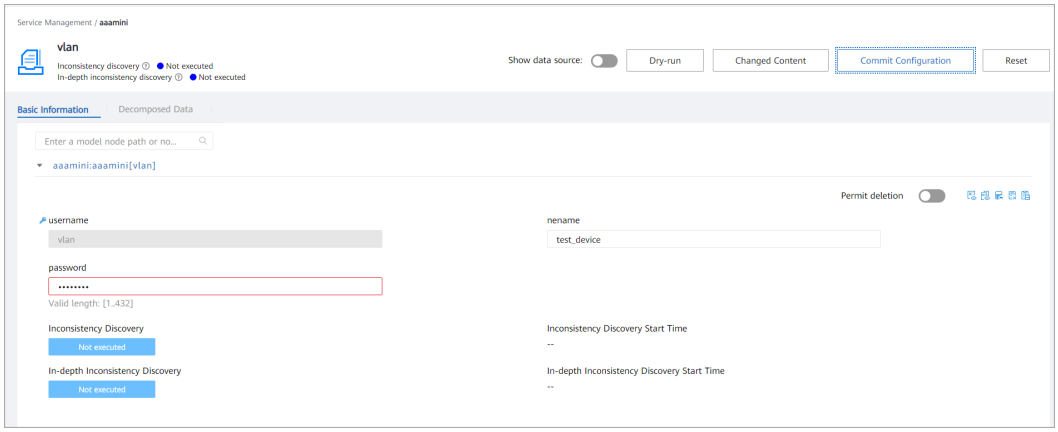
Step 5 After the dry run is complete, the **Dry-run View** page is displayed. You can view device data to be delivered and inconsistent data.

Figure 7-6 Viewing device data to be delivered on the **Dry-run View** page



Step 6 If the result displayed on the **Dry-run View** page meets expectations, click **Commit Configuration**.

Figure 7-7 Committing the configuration



NOTE

When the current configuration is delivered, the following conflicts are checked:

1. **Multi-terminal operation conflict**

   Before delivering configurations, NCE checks whether the operation configurations of multiple terminals conflict with each other. Assume that the same service instance service 1 (x=1, y=2) is configured for both terminal 1 and terminal 2. The service instance is then edited, submitted, and updated to service 1 (x=2, y=2) for terminal 1, while terminal 2 performs operations based on the original service 1 (x=1, y=2). In this case, the system displays a message indicating a conflict when terminal 2 submits data.

   Current solution: Roll back to the previous configuration and perform configuration again.

2. **Device configuration conflict**

   Before delivering device configurations, NCE checks whether the device data is inconsistent with the NCE data. If so, a message is displayed indicating that a configuration conflict may occur. A conflict message is displayed in the following scenarios:

   1. When NCE manages a device for the first time and does not synchronize the device data, data is not synchronized between NCE and the device.
   2. NCE saves the sequence IDs of device configuration changes. (The IDs can be obtained from the device or calculated on NCE based on the total value of device configuration verification times.) Before redelivering configurations, NCE obtains the sequence IDs again. If an ID change is detected, NCE considers that a configuration change occurs.
   3. When a device is disconnected from NCE during configuration delivery, NCE rolls back the configurations. If the device is offline for a long time, the NCE data is inconsistent with the device data.

   Current solution:

   1. Commit the device configurations forcibly. In this case, NCE does not check conflicts.
   2. Synchronize data with the device, then edit and commit the configurations again.

3. **Service configuration conflict**

   Before delivering service configurations, NCE checks whether the configurations delivered to a device conflict with each other. Assume that both service 1 and service 2 deliver the description configurations of VLAN 2 to device 1. In this case, NCE checks whether the two configurations are the same. If not, the system displays a message indicating that a configuration conflict occurs.

   Current solution:

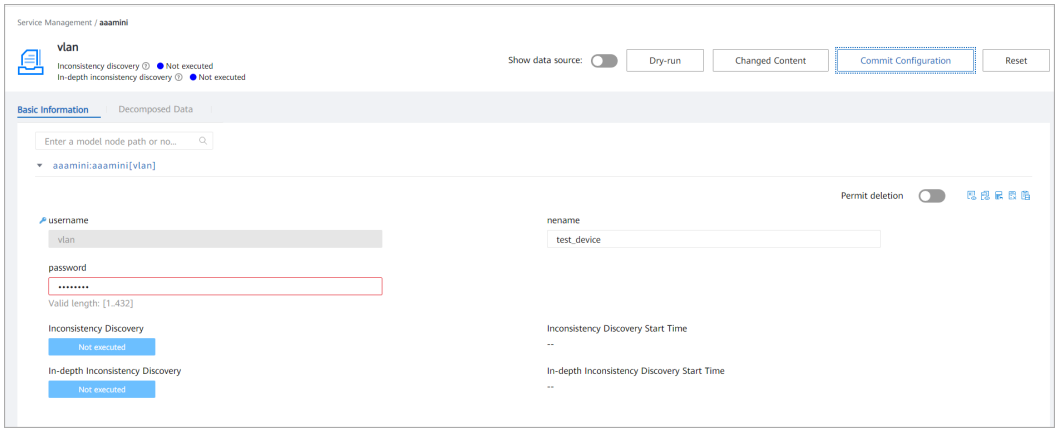
   1. Commit the service configurations forcibly. In this case, NCE does not check conflicts.
   2. Delete the previous service configurations and attributes related to the service configurations to avoid conflicts with the current service configurations.

No networking mode

When configurations are delivered through NCE, the configurations will be written to the NCE database and delivered to devices. When configurations are delivered in no networking mode, the configurations will only be written to the NCE database without being delivered to devices.

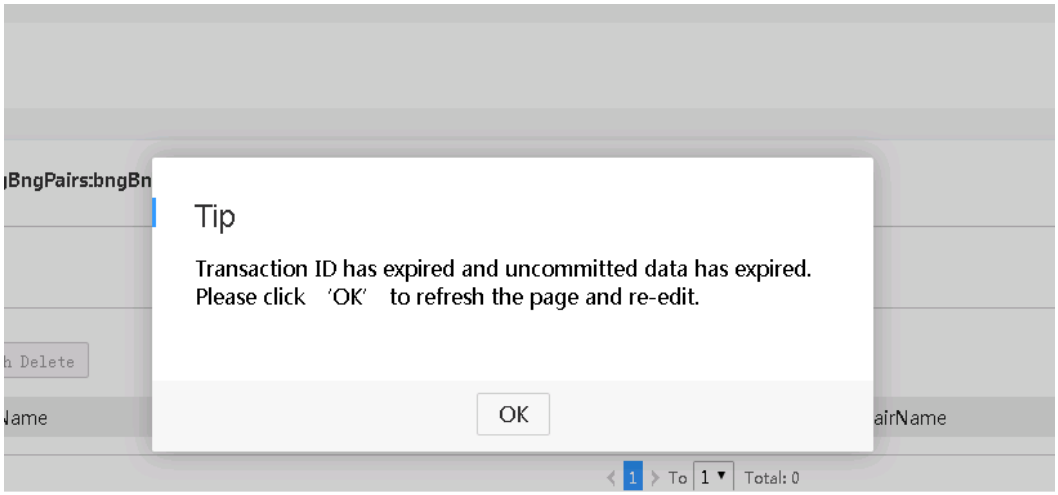
Step 7 If the result displayed on the **Dry-run View** page does not meet expectations or you need to reset the configuration, click **Reset**.

Figure 7-8 Resetting the configuration



Step 8 If the configuration is not edited for a long time or the third-party package is forcibly deleted, the system displays a message indicating that the transaction has expired when you perform operations on the GUI. In this case, click **OK** in the displayed **Tip** dialog box to refresh the page and edit the configuration again.

Figure 7-9 Message indicating that the transaction has expired



NOTE

After a user opens a web page, the foreground applies for a transaction ID from the background. If the user does not edit the page for a long time, the background will age the transaction ID. The default validity period of a transaction ID is 5 days. If the third-party package used when the user edits the configuration is forcibly uninstalled, the background clears the transaction ID that is being used.

If the user continues to use the old transaction ID to edit the configuration, a dialog box is displayed, indicating that the local transaction ID has expired.

----End

7.2 Configuring Services Using the Northbound CLI

Step 1 Choose **CLI** from the main menu. The CLI is displayed.

```
Welcome to NCE CLI
[NCE]>
```

Step 2 **Optional:** Run the command to enter the service view.

```
[NCE]> applications
[app:applications]>
```

Step 3 Edit the service.

```
[app:applications]> hbng hbng_ins
[app:applications/hbng:hbng[hbng_ins]]> core_id 4033
[app:applications/hbng:hbng[hbng_ins]]> pool_soo ZBB
[app:applications/hbng:hbng[hbng_ins]/hbng:pool_soo[ZBB]]> soo 501
[app:applications/hbng:hbng[hbng_ins]/hbng:pool_soo[ZBB]]> quit
[app:applications/hbng:hbng[hbng_ins]]>
```

Step 4 Conduct a dry run for the service configuration.

```
[app:applications/hbng:hbng[hbng_ins]]> dry-run
[OK]
```

Step 5 Preview the configuration.

```
[app:applications/hbng:hbng[hbng_ins]]> display dry-run preview
### ipi-zba900-r-bn-01  ###
<system xmlns="https://www.huawei.com/netconf/vrp/huawei-system">
<systemInfo>
<sysName>Huawei1</sysName>
</systemInfo>
</system>
[app:applications/hbng:hbng[hbng_ins]]>
```

- If the displayed result meets expectations, commit the configuration.
  ```
  [NCE]>commit
  ```
- To delete the configuration, reset the configuration.
  ```
  [NCE]> reset
  ```

----End

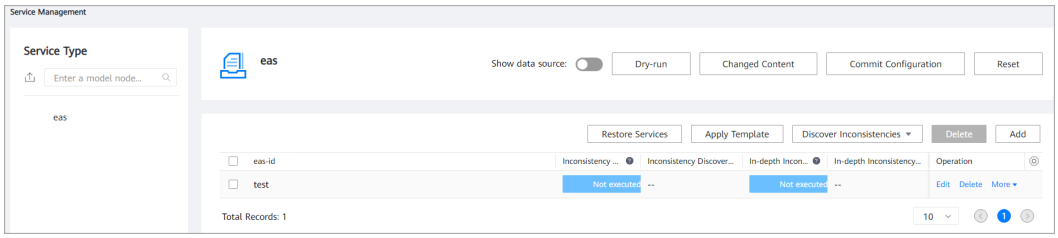
7.3 Verifying Service Data Consistency

7.3.1 Performing Service Inconsistency Discovery

Procedure

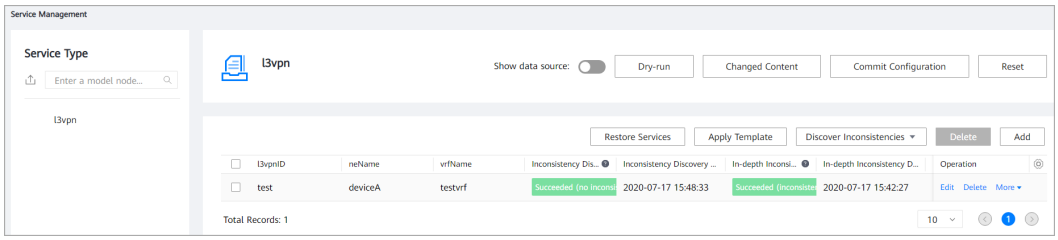
Step 1 Choose **Service Management** from the main menu. On the **Service management** page that is displayed, select a service instance. Then click **Discover Inconsistencies** and select **Discover Inconsistencies**.

Figure 7-10 Triggering inconsistency discovery



Step 2 After service inconsistency discovery is complete, the value of **Inconsistency Discovery Status** changes to **Succeeded (inconsistencies found)**.

Figure 7-11 Inconsistency discovery completed



Step 3 The southbound device list is displayed on the left of the service inconsistency display page.

Select a service instance, click **More**, and select **View Inconsistencies**. The detailed inconsistent data is displayed on the right of the service inconsistency display page. The data in the **Old Data** column indicates the southbound device configurations saved in the NCE database and the data in the **New Data** column indicates the southbound device configurations generated after service instances are recomputed.

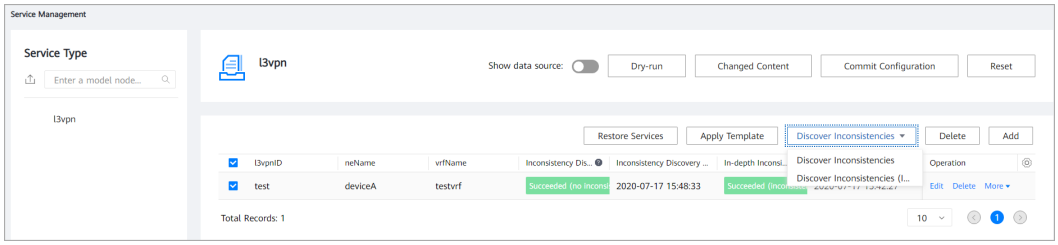
----End

7.3.2 Performing In-Depth Service Inconsistency Discovery

Procedure

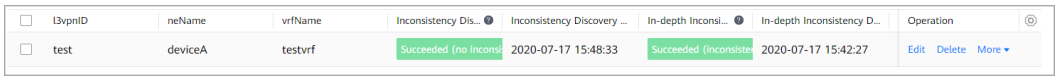
Step 1 Choose **Service Management** from the main menu. On the **Service management** page that is displayed, select a service instance. Then click **Discover Inconsistencies** and select **Discover Inconsistencies (In-depth)**.

Figure 7-12 Triggering in-depth inconsistency discovery



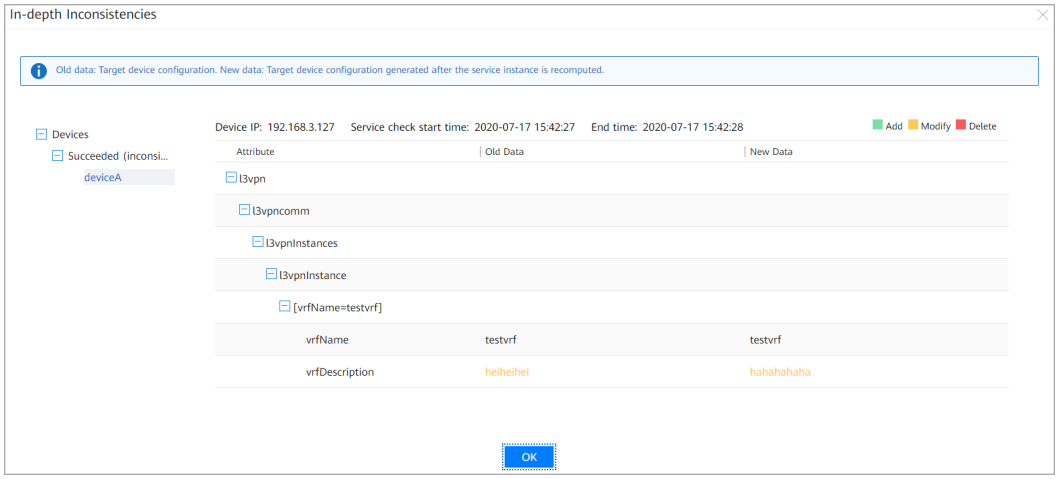
Step 2 After service inconsistency discovery is complete, the value of **In-depth Inconsistency Discovery Status** changes to **Succeeded (inconsistencies found)**.

Figure 7-13 In-depth inconsistency discovery completed



Step 3 Choose **Service Management** from the main menu. On the **Service Management** page that is displayed, click **More** and select **View In-depth Inconsistencies**. The southbound device list is displayed in the left pane of the in-depth service inconsistency display page.

Figure 7-14 In-depth inconsistency display page



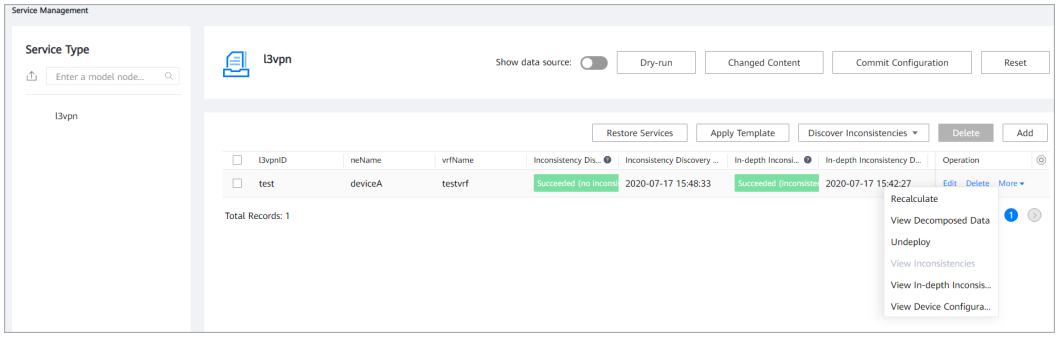
----End

7.3.3 Checking Southbound Configuration Records of Service Instances

Procedure

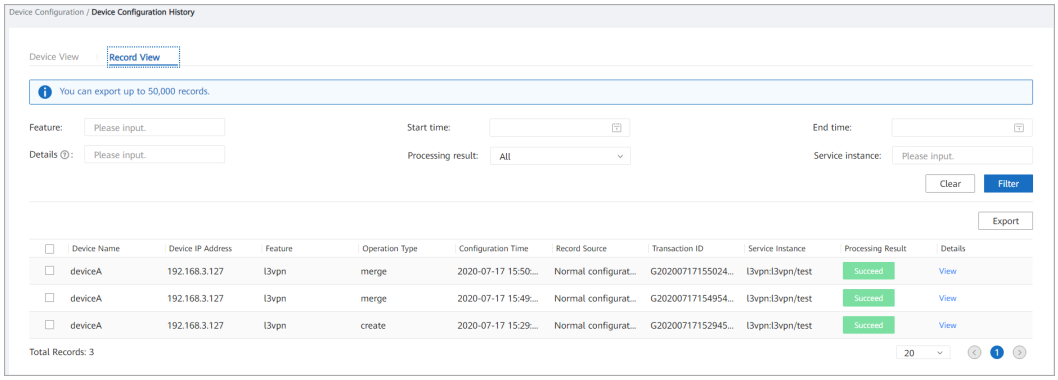
Step 1 Choose **Service Management** from the main menu. On the **Service Management** page that is displayed, click **More** and select **View Device Configuration History**. The **Record View** tab page is displayed.

Figure 7-15 Accessing the record view



Step 2 On the **Record View** tab page, the configuration records of the service instance are automatically filtered and displayed.

Figure 7-16 Device configuration record management page



----End

8 Template Management

Scenario Description

Template management allows you to manage NE templates and service templates. To deliver configurations, select a template from available templates and orchestrate as well as deliver the template.

8.1 Managing NE Templates

Scenario Description

You can use the NE template management function to manage device-level templates.

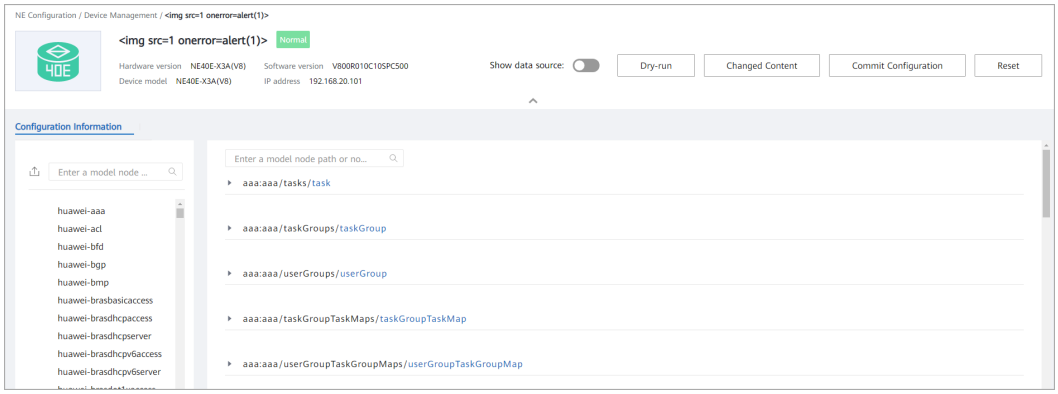
8.1.1 Exporting an NE Template Based on a YANG File

Procedure

Step 1 Choose **Device Configuration** > **Device Configuration** from the main menu.

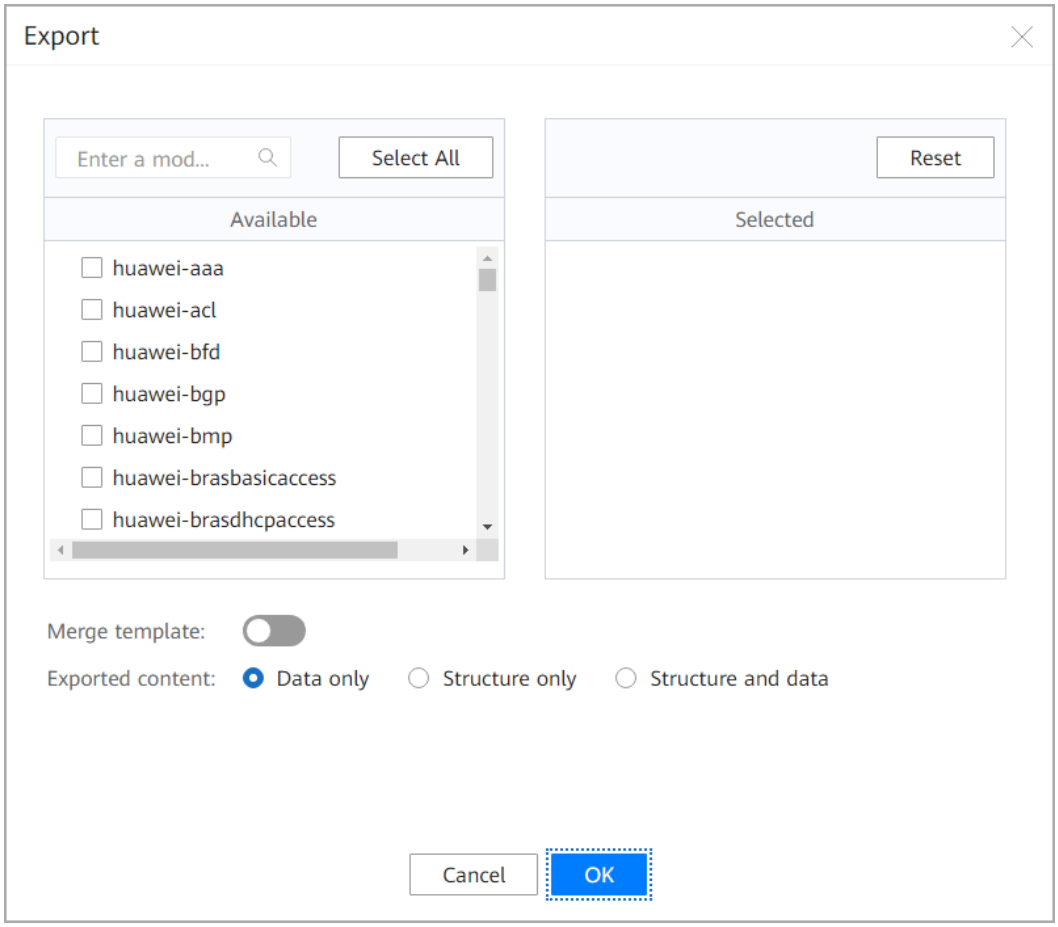
Step 2 On the **Device Configuration** page that is displayed, click **Edit** in the **Operation** column of a device to access the **Configuration Information** page.

Figure 8-1 Editing device information



Step 3 On the **Configuration Information** page that is displayed, click  in the upper left corner.

Figure 8-2 Exporting the YANG file



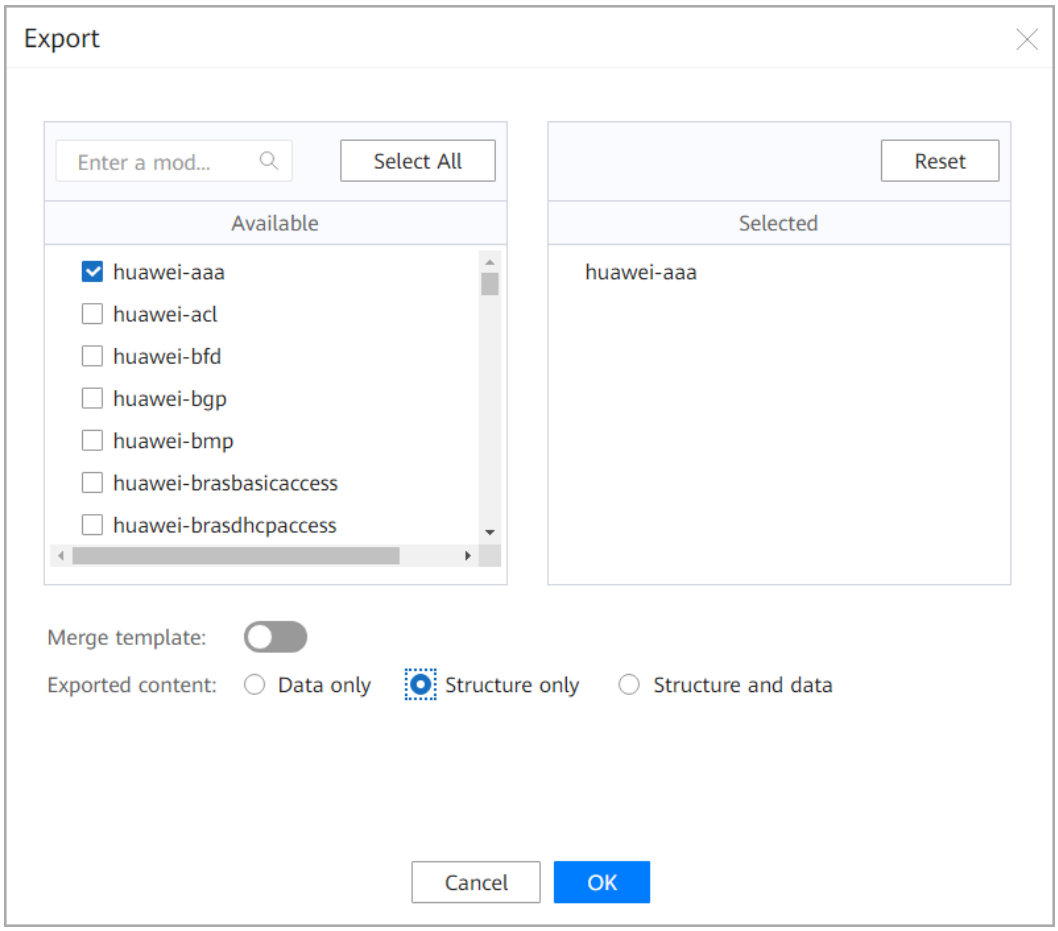
Step 4 In the **Export** dialog box that is displayed, select the YANG file to be exported as a template, set **Merge template** and **Exported content**, and click **OK**.

NOTE

- You can enable **Merge template** to merge the template content generated by multiple YANG files.
- Three modes are available for exporting a template: **Data only**, **Structure only**, and **Structure and data**.

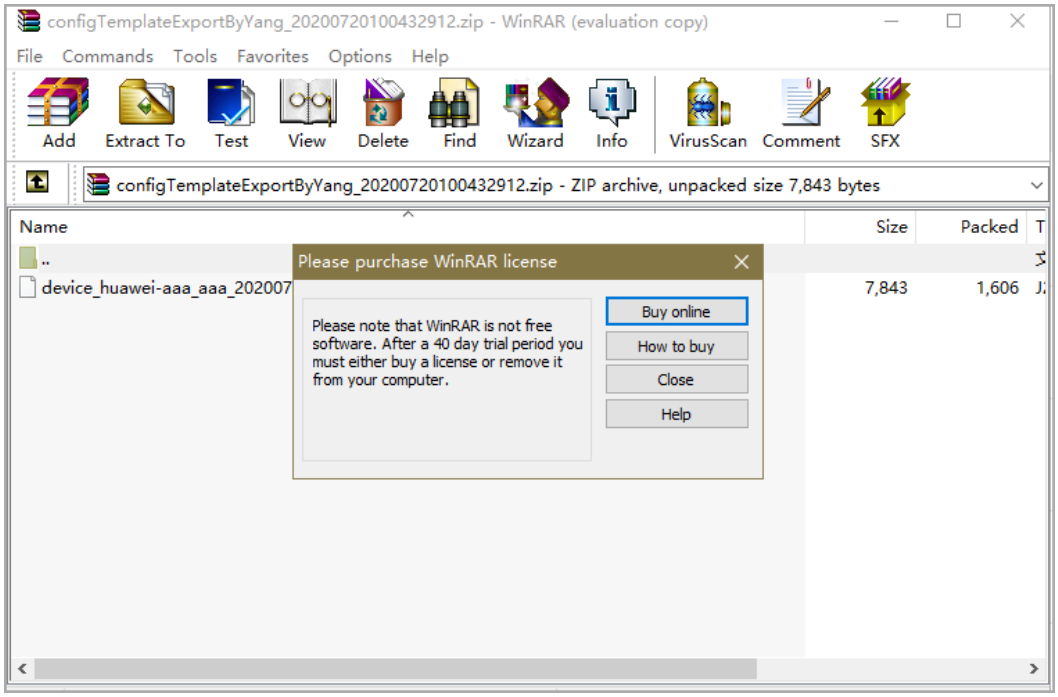
The following example exports a template in **Structure only** mode.

Figure 8-3 Selecting files



Step 5 In the displayed window, you can view the exported template.

Figure 8-4 Exported template



----End

8.1.2 Importing an NE Template

Prerequisites

An NE template has been successfully exported according to **8.1.1 Exporting an NE Template Based on a YANG File**.

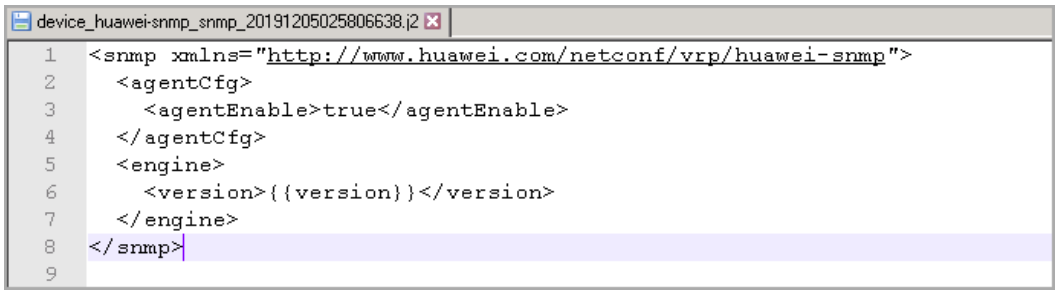
Procedure

Step 1 Edit the template exported based on a YANG file. The following example describes the SNMP configuration. Delete the unnecessary objects and define the objects that require parameter transfer as parameters.

NOTE

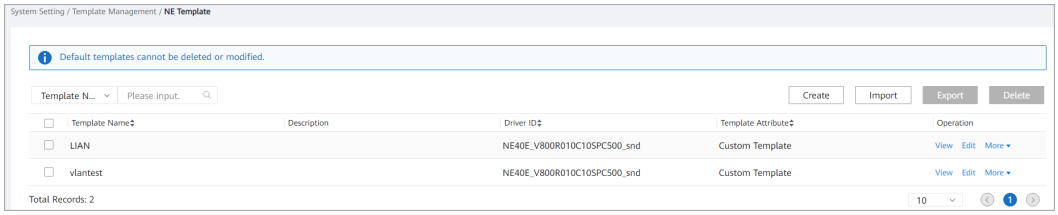
The defined parameter name must be enclosed in {{}}.

Figure 8-5 Edited template



Step 2 Choose **System Setting** > **Template Management** > **NE Template** from the main menu. On the **NE Template** page that is displayed, click **Import**.

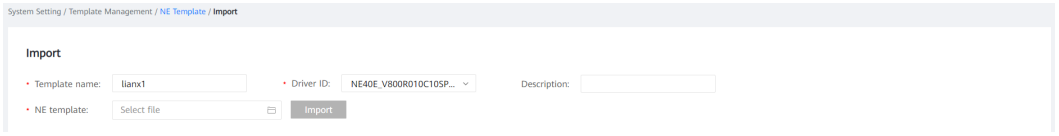
Figure 8-6 NE template import page



Step 3 In the displayed dialog box, set the template name and import a template file.

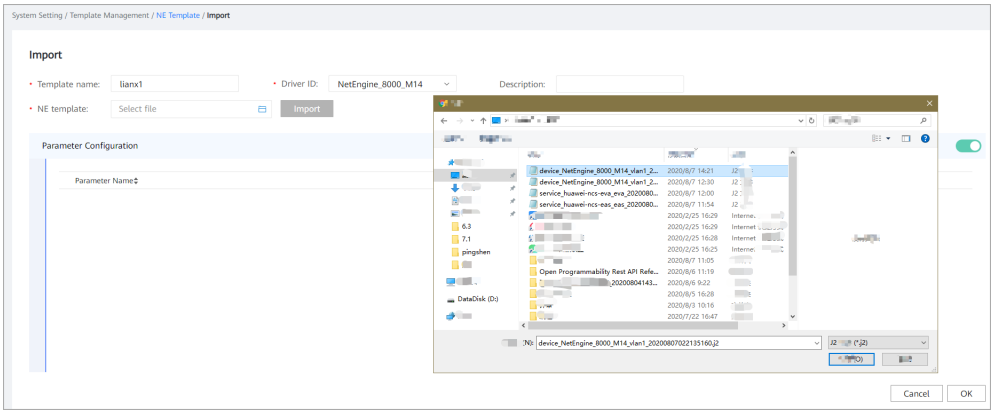
1. Set **Template name**, **Driver ID**, **Description**, and **NE template**.

   Figure 8-7 Setting **Template name**, **Driver ID**, **Description**, and **NE template**

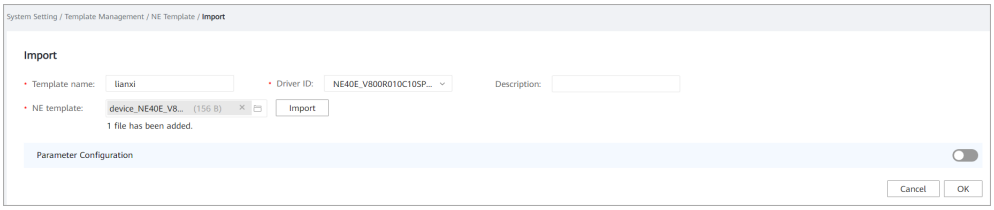
2. Click , select the edited template, and click **Open**.

   Figure 8-8 Selecting a file

3. Click **Import**.

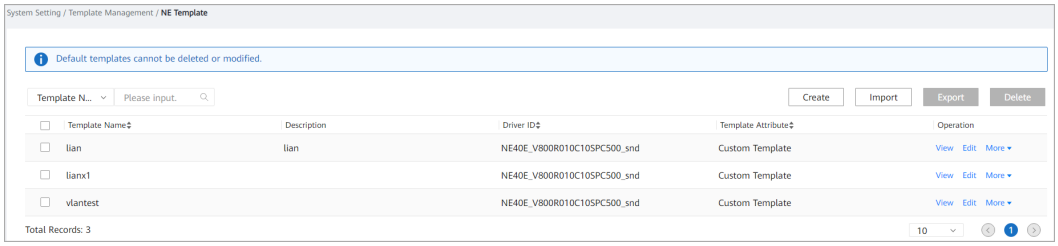
   Figure 8-9 Uploading an NE template

4. Click **OK** after the template is imported.

Step 4 View the template list. The imported template is displayed in the template list.

Figure 8-10 Viewing the imported template



----End

8.1.3 Creating an NE Template

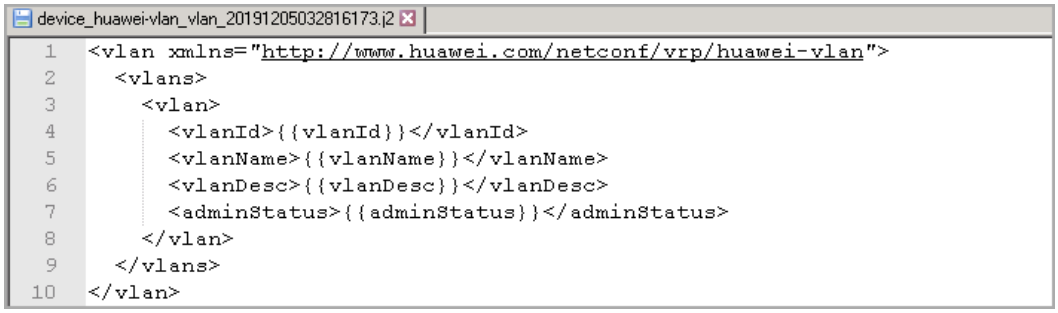
Procedure

Step 1 Edit the template content. The following example describes the VLAN configuration. Define the objects that require parameter transfer as parameters.

NOTE

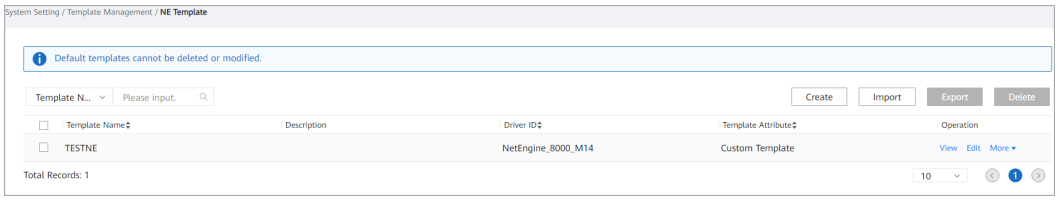
The defined parameter name must be enclosed in {{}}.

Figure 8-11 Edited template



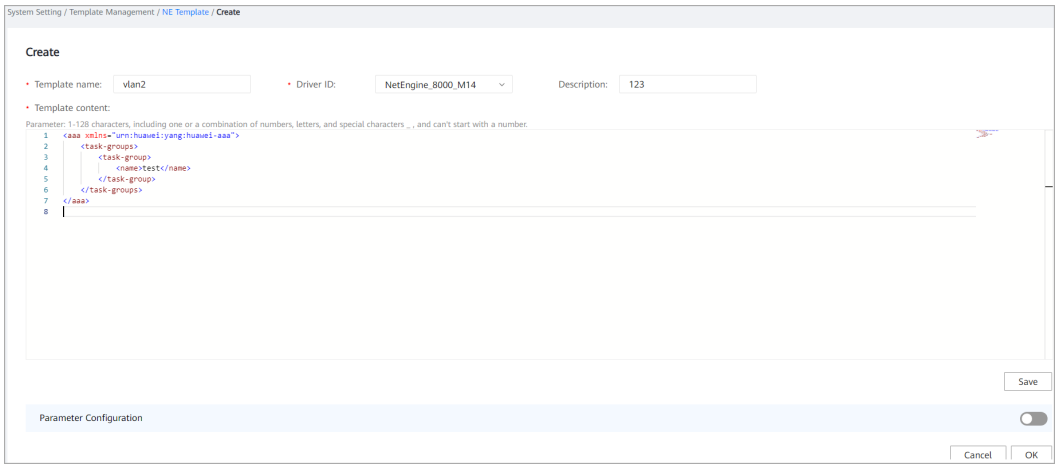
Step 2 Choose **System Setting** > **Template Management** > **NE Template** from the main menu.

Figure 8-12 Creating an NE Template



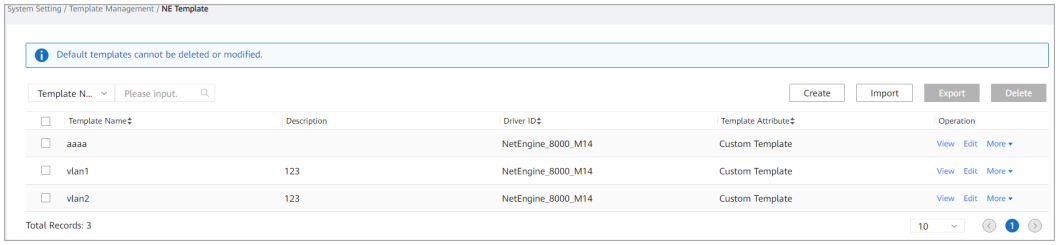
Step 3 Click **Create**. In the displayed dialog box, set **Template name**, **Description**, **Driver ID** and **Template content**, and click **OK**.

Figure 8-13 Editing an NE template



Step 4 View the template list. The created template is displayed in the template list.

Figure 8-14 Viewing the created template



----End

8.1.4 Deleting an NE Template

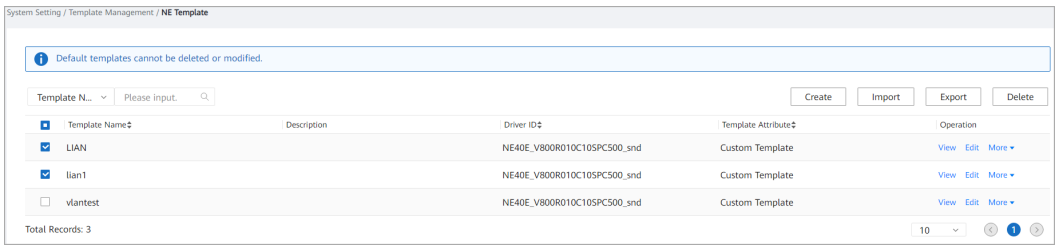
Procedure

NOTE

- To delete a single template, click **More** in the **Operation** column and select **Delete**.
- To delete templates in batches, select them and click **Delete**.

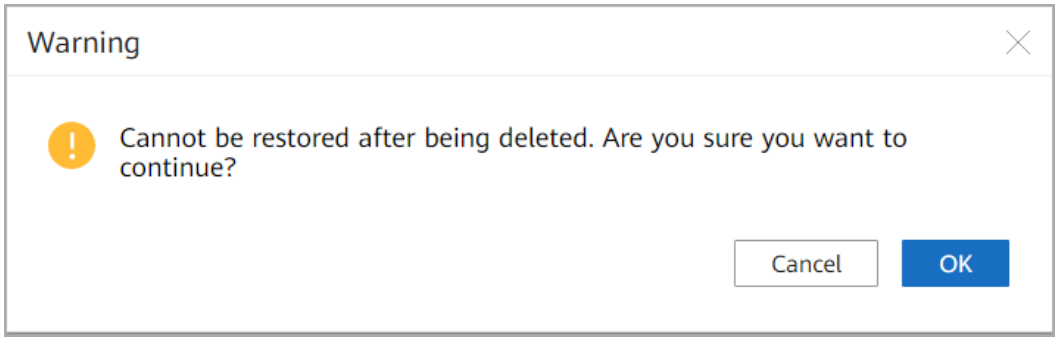
Step 1 Choose **System Setting** > **Template Management** > **NE Template** from the main menu. On the **NE Template** page that is displayed, select the templates to be deleted and click **Delete**.

Figure 8-15 Deleting NE templates in batches



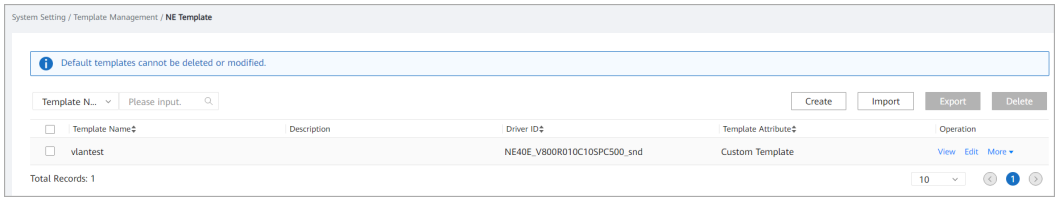
Step 2 In the displayed dialog box, click **OK**.

Figure 8-16 Warning message displayed after the deletion of templates



Step 3 View the template list. The templates have been deleted.

Figure 8-17 Successful template deletion



----End

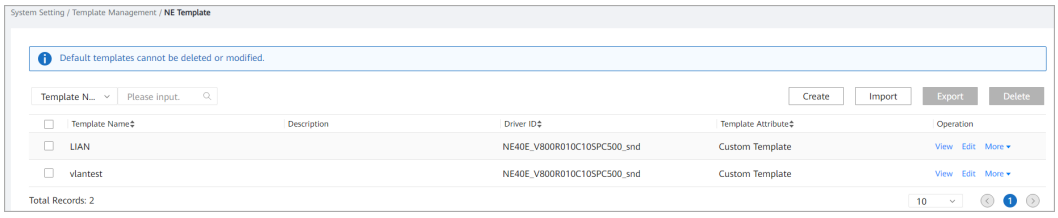
8.1.5 Exporting an NE Template

Procedure

Step 1 Choose **System Setting** > **Template Management** > **NE Template** from the main menu.

Step 2 On the **NE Template** page that is displayed, select the template to be exported and click **Export**.

Figure 8-18 Exporting an NE template



----End

8.2 Managing Service Templates

Scenario Description

You can use the service template management function to manage network-level templates.

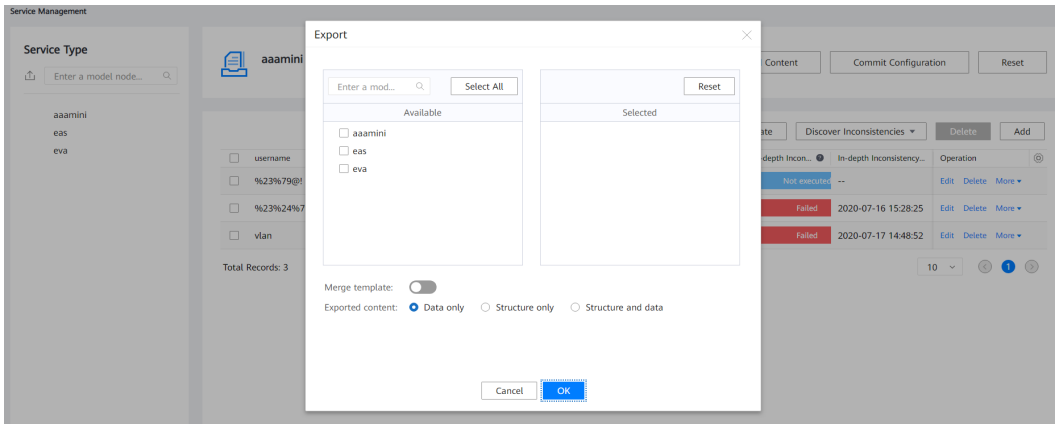
8.2.1 Exporting a Service Template Based on a YANG File

Procedure

Step 1 Choose **Service Management** from the main menu. The **Service Management** page is displayed.

Step 2 On the **Service Management** page that is displayed, click  and select the YANG file to be exported as a template.

Figure 8-19 Service Management page



Step 3 In the **Export** dialog box that is displayed, set **Merge template** and **Exported content**, and click **OK**.

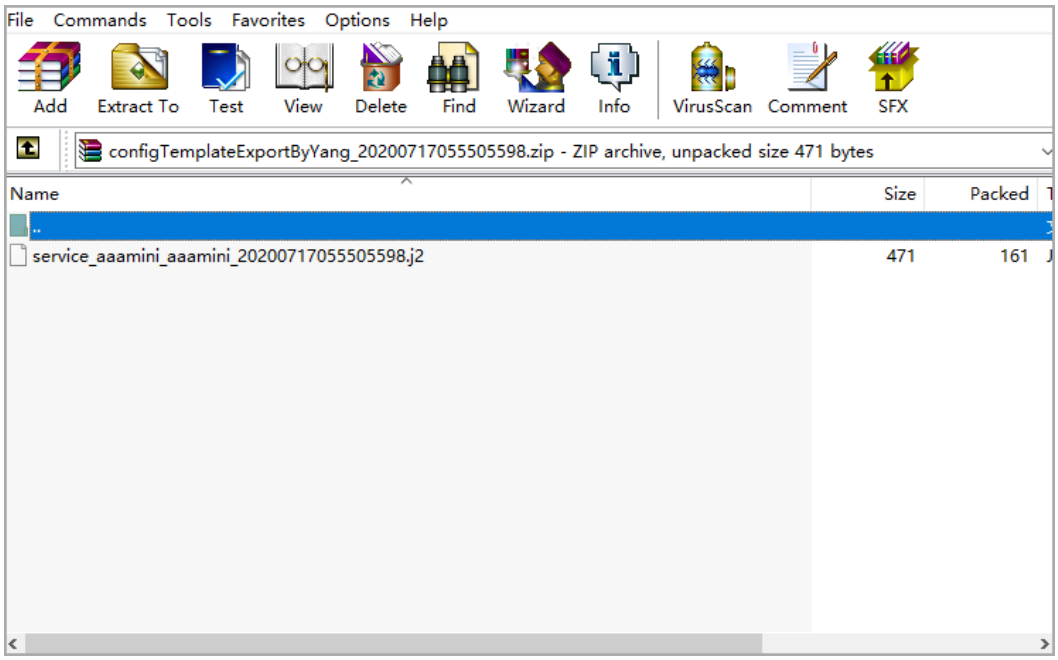
NOTE

- You can enable **Merge template** to merge the template content generated by multiple YANG files.
- Three modes are available for exporting a template: **Data only**, **Structure only**, and **Structure and data**.

The following example exports a template in **Structure only** mode.

Step 4 In the displayed window, you can view the exported template.

Figure 8-20 Exported template



----End

8.2.2 Importing a Service Template

Prerequisites

A service template has been exported according to **8.2.1 Exporting a Service Template Based on a YANG File**.

Procedure

Step 1 Edit the template exported based on a YANG file. The following example describes the VLAN mapping configuration. Delete the unnecessary objects and define the objects that require parameter transfer as parameters.

NOTE

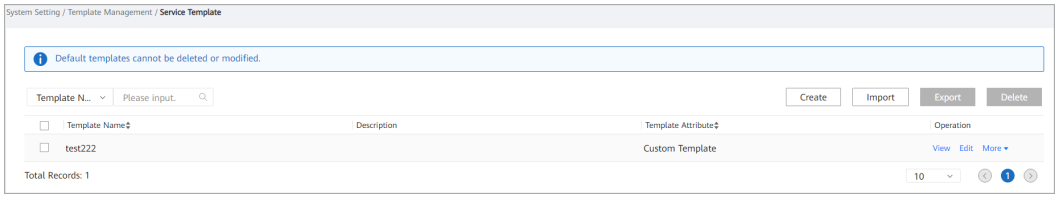
The defined parameter name must be enclosed in {{}}.

Figure 8-21 Edited template

```
<vlan_mapping xmlns="http://example.com/vlan_mapping">
  <pe_id>{{pe_id}}</pe_id>
  <trunk_id>{{trunk_id}}</trunk_id>
  <mapping_id>{{mapping_id}}</mapping_id>
</vlan_mapping>
```

Step 2 Choose **System Setting** > **Template Management** > **Service Template** from the main menu. On the **Service Template** page that is displayed, click **Import**.

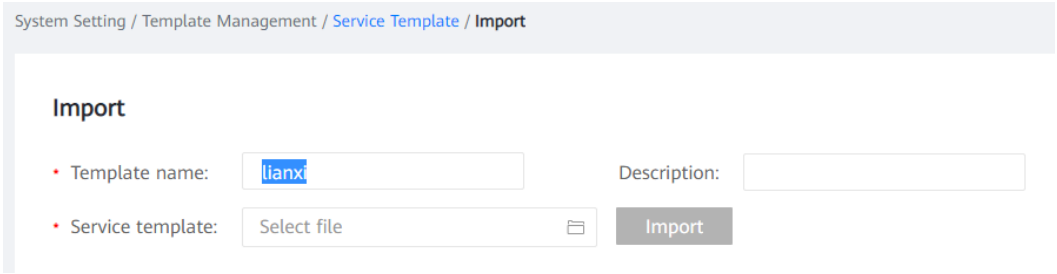
Figure 8-22 Clicking **Import**



Step 3 In the displayed dialog box, set the template name and import a template file.

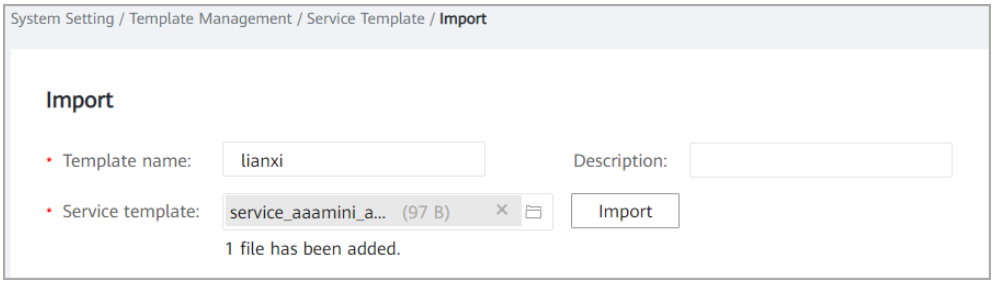
1. Set **Template name**, **Description**, and **Service template**.

   Figure 8-23 Setting **Template name**, **Description**, and **Service template**

2. Click , select the edited template, and click **Import**.

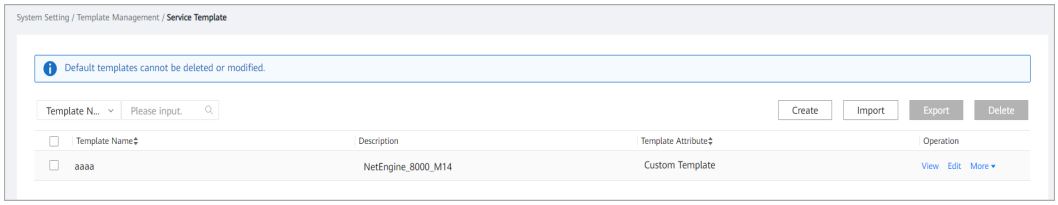
   Figure 8-24 Importing a service template

3. Click **OK** after the template is imported.

Step 4 View the template list. The imported template is displayed in the template list.

Figure 8-25 Viewing the imported service template



----End

8.2.3 Creating a Service Template

Procedure

Step 1 Edit the template content. The following example describes the configuration of bngVrfsPairs. Define the objects that require parameter transfer as parameters.

NOTE

The defined parameter name must be enclosed in {{}}.

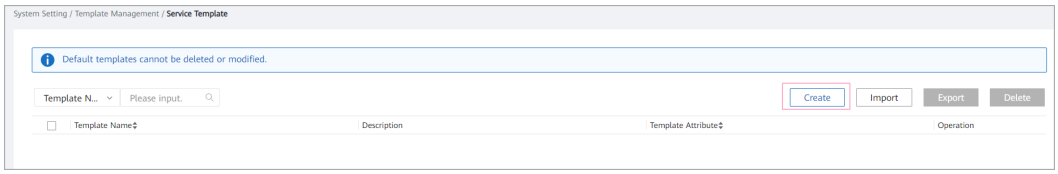
Figure 8-26 Edited template

```
<bngVrfsPairs xmlns="http://swisscom.com/bngVrfsPairs">
  <bngVrfsPairsName>{{bngVrfsPairsName}}</bngVrfsPairsName>
  <bngServiceName>{{bngServiceName}}</bngServiceName>
  <pairName>{{pairName}}</pairName>
</bngVrfsPairs>
```

Step 2 Choose **System Setting** > **Template Management** > **Service Template** from the main menu.

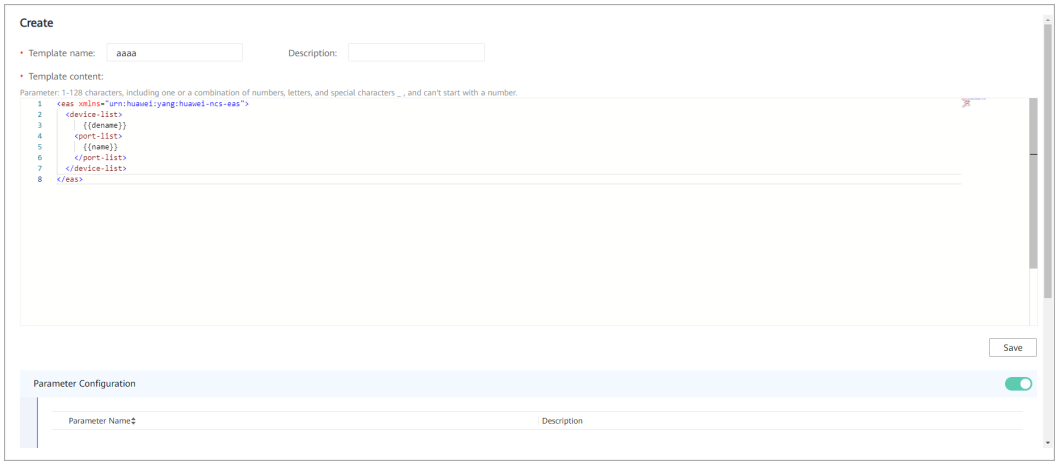
Step 3 On the **Service Template** page that is displayed, click **Create**.

Figure 8-27 Creating a template



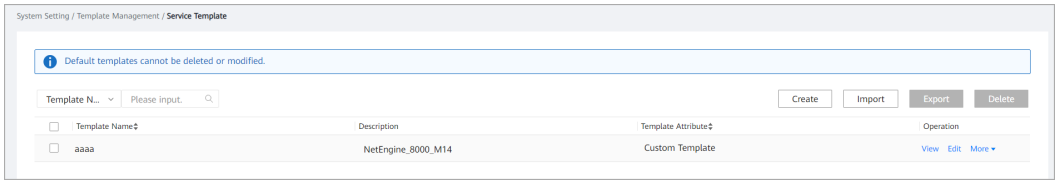
Step 4 In the displayed dialog box, set **Template name**, **Description**, and **Template content**, and click **OK**.

Figure 8-28 Editing a template



Step 5 View the template list. The created template is displayed in the template list.

Figure 8-29 Viewing the created template



----End

8.2.4 Deleting a Service Template

Procedure

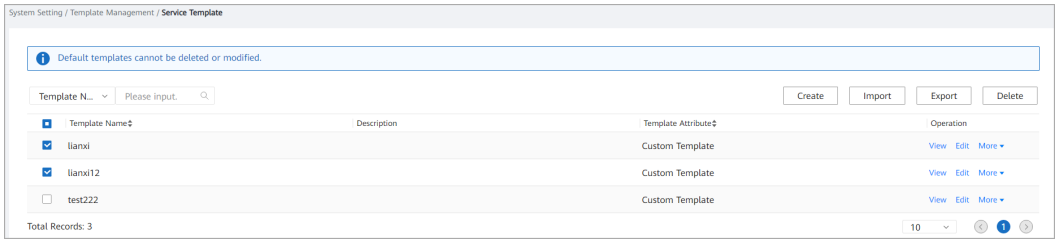
NOTE

- To delete a template, click **More** in the **Operation** column, and click **Delete**.
- To delete templates in batches, select them and click **Delete**.

Step 1 Choose **System Setting** > **Template Management** > **Service Template** from the main menu.

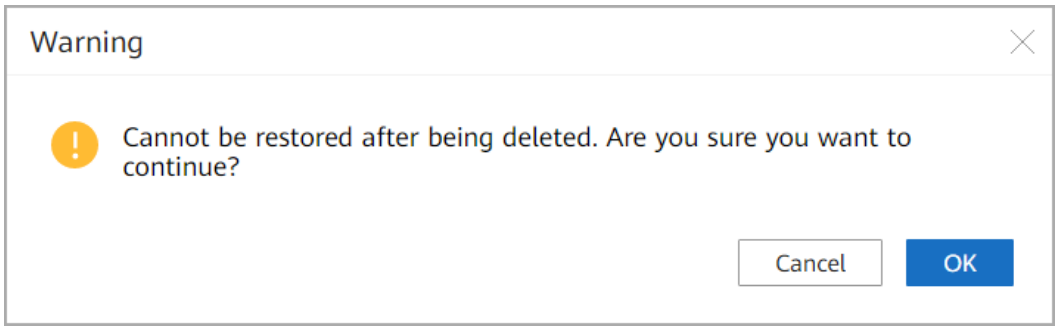
Step 2 On the **Service Template** page that is displayed, select the templates to be deleted and click **Delete**.

Figure 8-30 Deleting service templates in batches



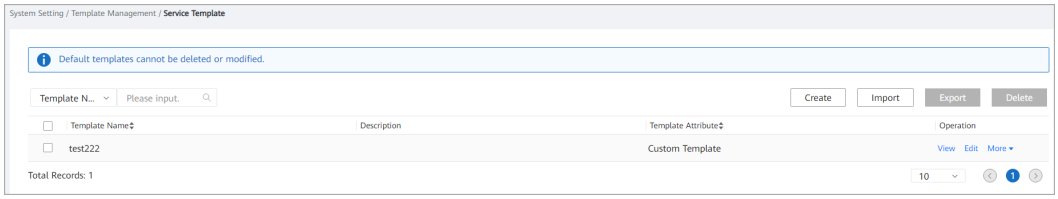
Step 3 In the displayed dialog box, click **OK**.

Figure 8-31 Warning message displayed after the deletion of templates



Step 4 View the template list. The templates have been deleted.

Figure 8-32 Successful template deletion



----End

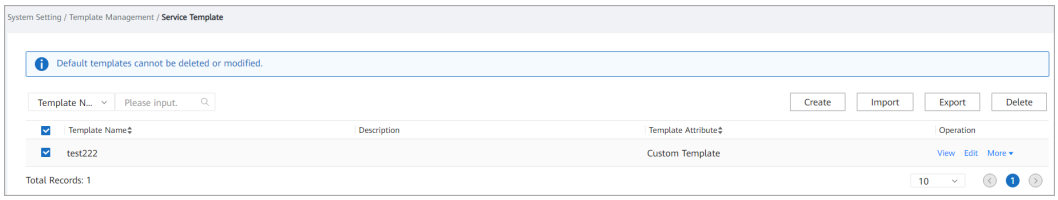
8.2.5 Exporting a Service Template

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Service Template** from the main menu.

Step 2 On the **Service Template** page that is displayed, select the template to be exported and click **Export**.

Figure 8-33 Exporting a service template



----End

8.3 Managing Template Groups

Scenario Description

A template group is a collection of service configurations. You can use template groups for preliminary service orchestration.

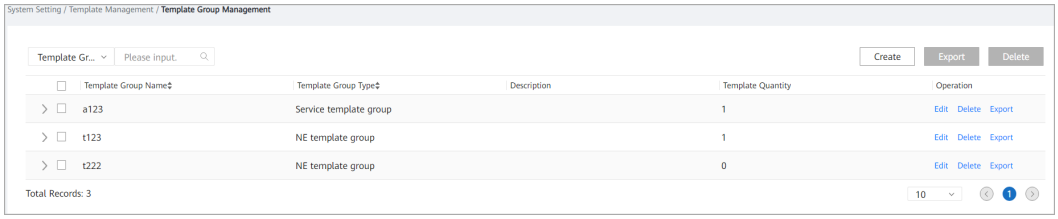
8.3.1 Creating a Template Group

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Template Group Management** from the main menu.

Step 2 On the **Template Group Management** page that is displayed, click **Create**.

Figure 8-34 Template Group Management page

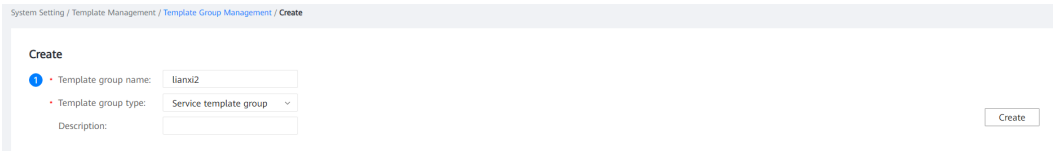


NOTE

There are two types of template groups: NE template group and service template group. The following example describes how to create a service template group.

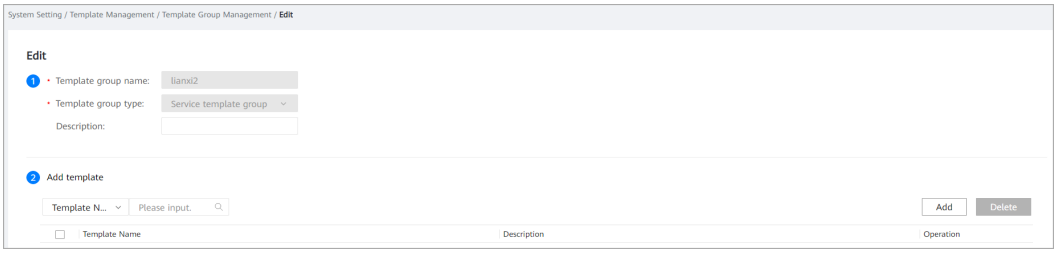
Step 3 On the **Create** page that is displayed, set **Template group name**, **Template group type**, and **Description**, and click **Create**.

Figure 8-35 Creating a template group



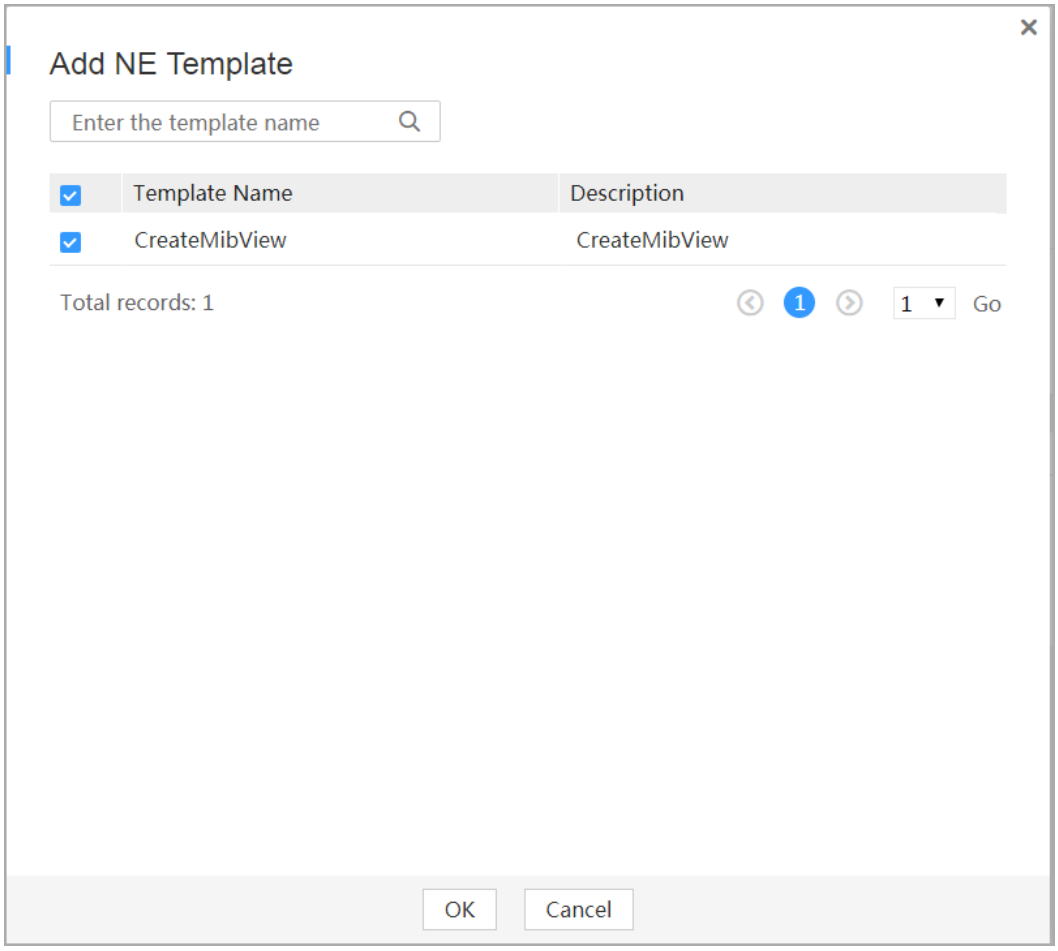
Step 4 Under **Add template**, click **Add**.

Figure 8-36 Adding a template



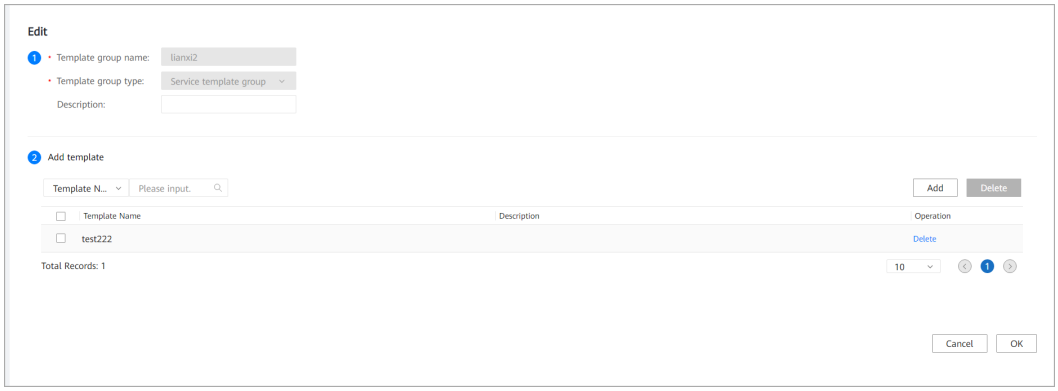
Step 5 Under **Add template**, select the template to be added and click **OK**.

Figure 8-37 Adding a service template



Step 6 Under **Add template**, you can view the added template.

Figure 8-38 Viewing the added template



Step 7 Click **OK** to return to the **Template Group Management** page and view the created template group.

----End

8.3.2 Deleting a Template Group

Procedure

NOTE

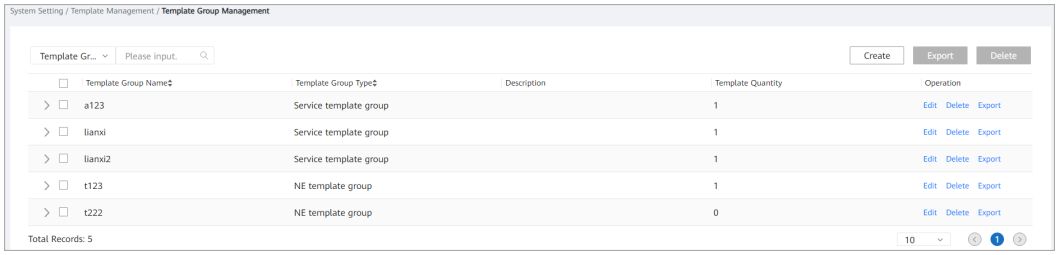
- To delete a template group, click **Delete** in the **Operation** column.
- To delete template groups in batches, select them and click **Delete**.

The following example deletes template groups in batches.

Step 1 Choose **System Setting** > **Template Management** > **Template Group Management** from the main menu. The **Template Group Management** page is displayed.

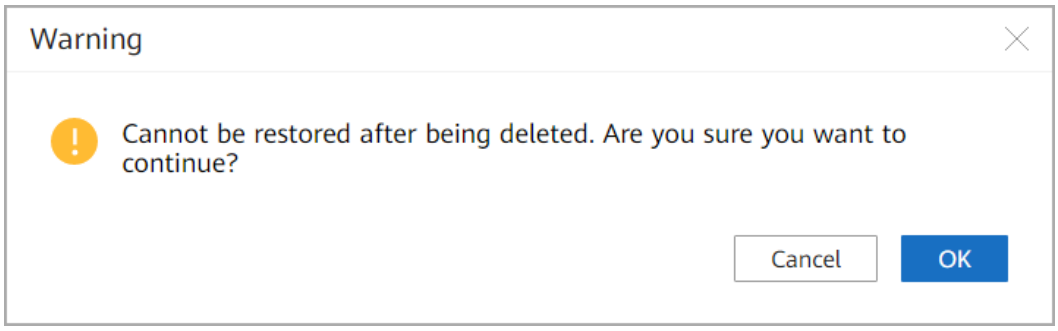
Step 2 On the **Template Group Management** page that is displayed, select the template groups to be deleted and click **Delete**.

Figure 8-39 Deleting template groups



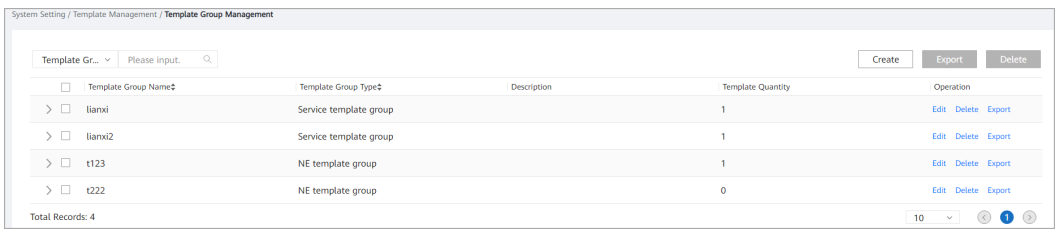
Step 3 In the displayed dialog box, click **OK**.

Figure 8-40 Warning message displayed after the deletion of template groups



Step 4 View the template group list. The template groups have been deleted.

Figure 8-41 Successful deletion of template groups



----End

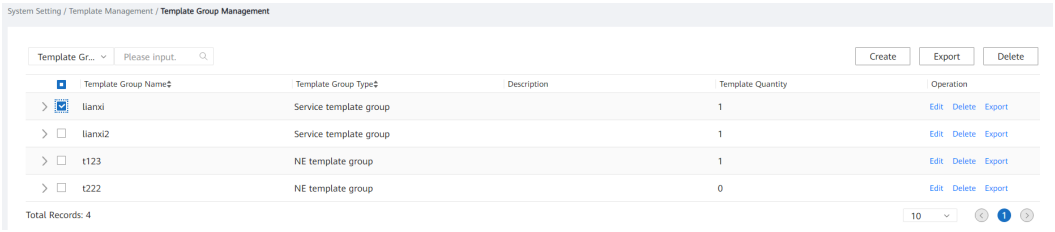
8.3.3 Exporting a Template Group

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Template Group Management** from the main menu.

Step 2 On the **Template Group Management** page that is displayed, select the template group to be exported and click **Export**.

Figure 8-42 Exporting a template group



----End

8.4 Managing Parameter Sets

Scenario Description

You can use the parameter set management function to manage parameters defined in templates. You can preconfigure parameter sets and directly select a template and the corresponding parameter set for delivery.

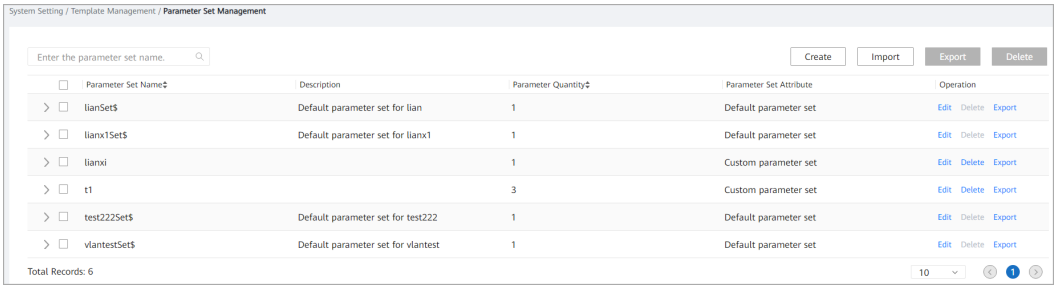
8.4.1 Creating a Parameter Set

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Parameter Set Management** from the main menu.

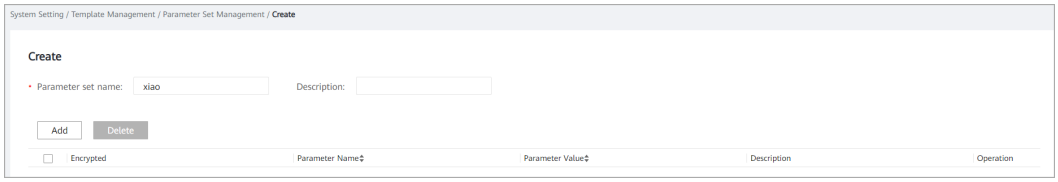
Step 2 On the **Parameter Set Management** page that is displayed, click **Create**.

Figure 8-43 Creating a parameter set



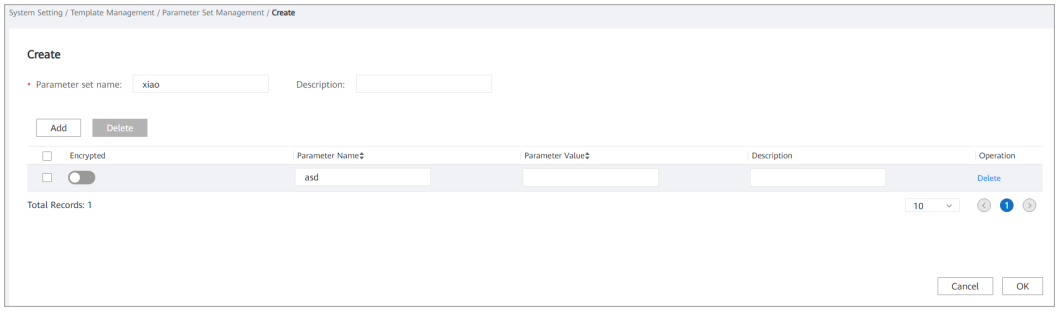
Step 3 On the **Create** page that is displayed, set **Parameter set name** and click **Add**.

Figure 8-44 Setting **Parameter set name**



Step 4 In the displayed list, set the parameters and click **OK**. On the **Parameter Set Management** page that is displayed, you can view the created parameter set.

Figure 8-45 Setting parameters



----End

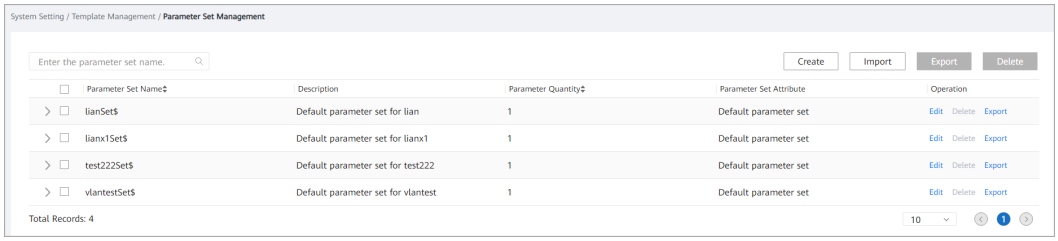
8.4.2 Importing a Parameter Set

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Parameter Set Management** from the main menu.

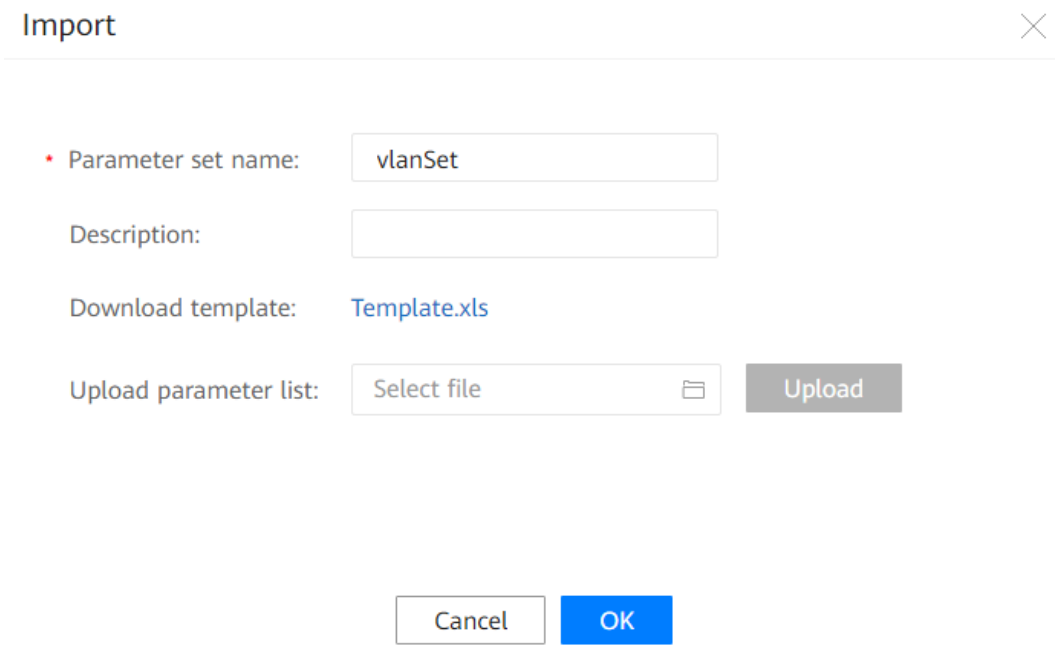
Step 2 On the **Parameter Set Management** page that is displayed, click **Import**.

Figure 8-46 Parameter Set Management page



Step 3 In the **Import** dialog box that is displayed, set **Parameter set name**.

Figure 8-47 Setting **Parameter set name**



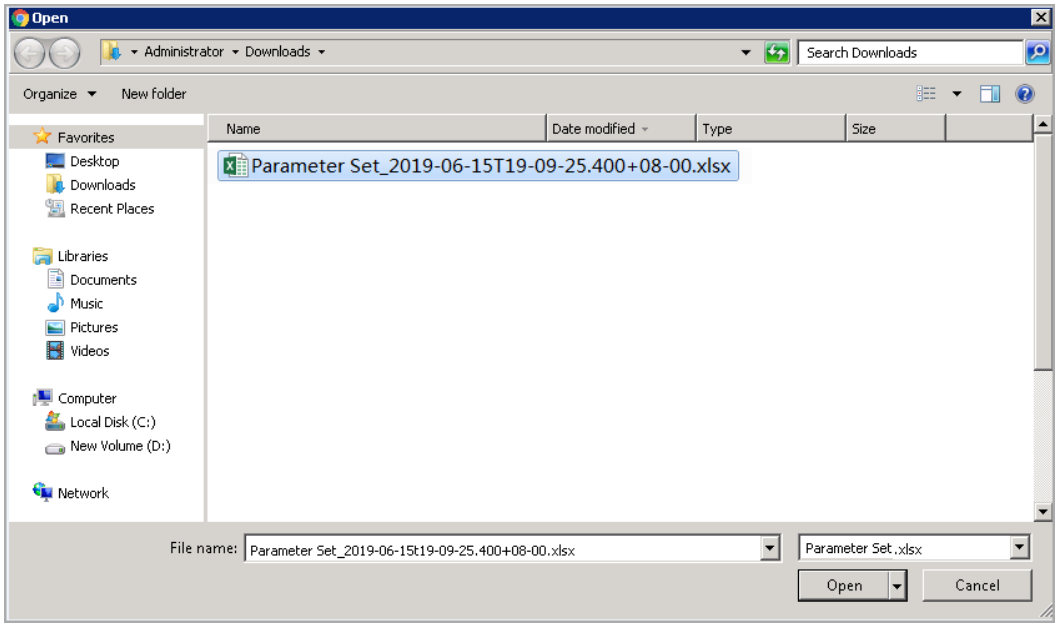
NOTE

Two file sources are available for setting **Upload parameter list**:

1. In the **Import** dialog box, download the parameter template, then edit and save it as a new parameter template.
2. Use the parameter template exported in **8.4.4 Exporting a Parameter Set**.

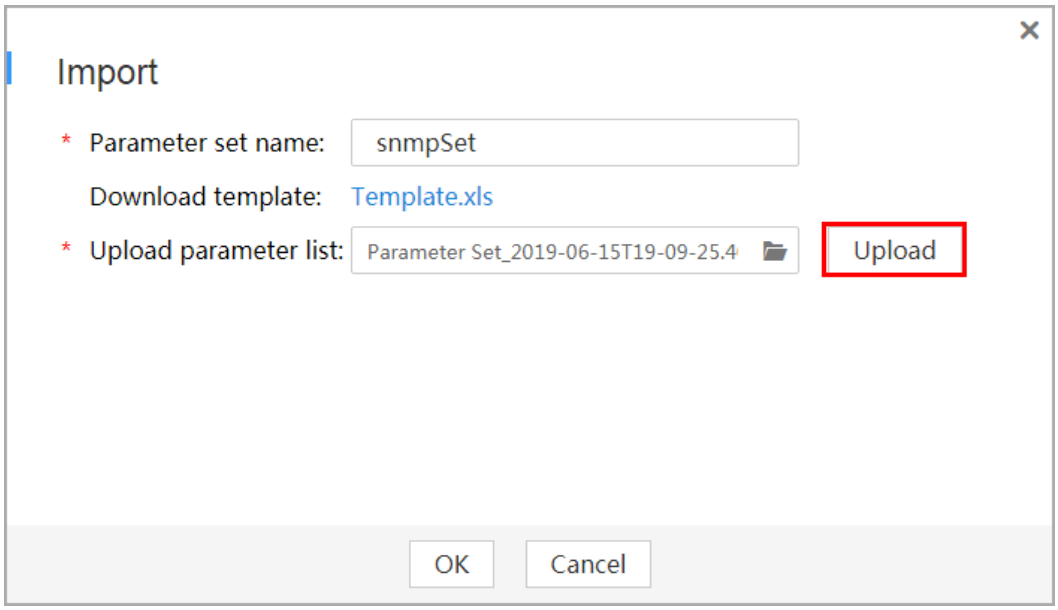
Step 4 Click and select the edited template.

Figure 8-48 Selecting a file



Step 5 Click **Upload**. Then click **OK** after the template is uploaded.

Figure 8-49 Uploading a parameter set



----End

8.4.3 Deleting a Parameter Set

Procedure

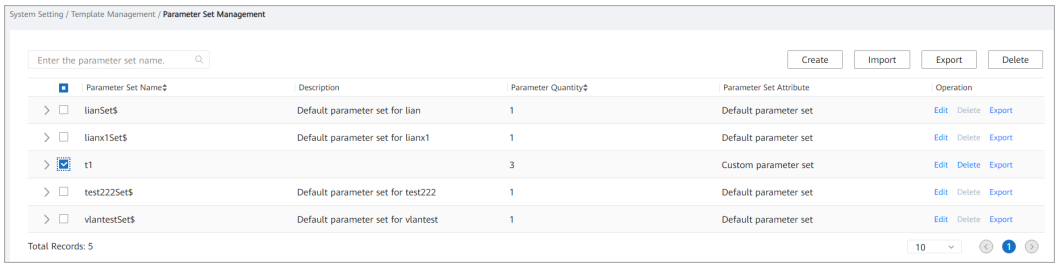
NOTE

- To delete a parameter set, click **Delete** in the **Operation** column.
- To delete parameter sets in batches, select them and click **Delete**.

The following example deletes parameter sets in batches.

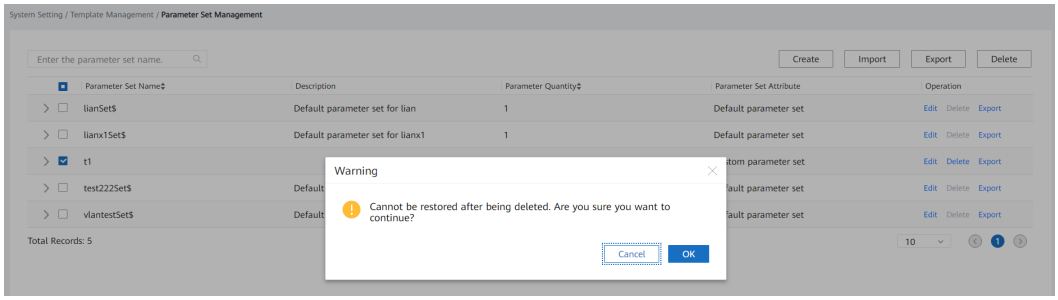
Step 1 Choose **System Setting** > **Template Management** > **Parameter Set Management** from the main menu.

Figure 8-50 Parameter Set Management page



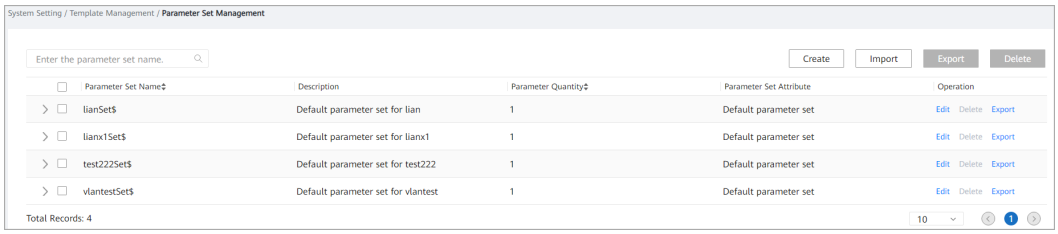
Step 2 In the displayed dialog box, click **OK**.

Figure 8-51 Warning message displayed after the deletion of parameter sets



Step 3 View the parameter set list. The parameter sets have been deleted.

Figure 8-52 Successful deletion of parameter sets



----End

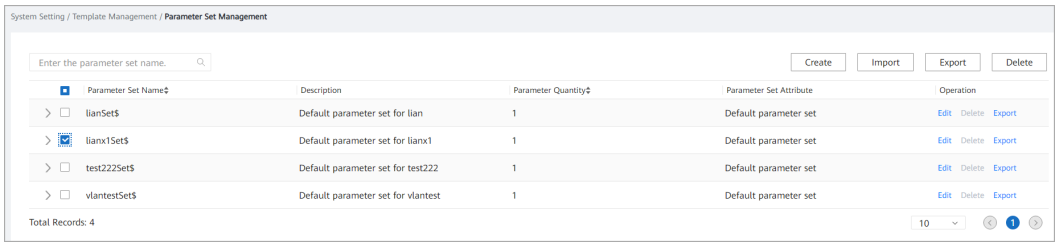
8.4.4 Exporting a Parameter Set

Procedure

Step 1 Choose **System Setting** > **Template Management** > **Parameter Set Management** from the main menu.

Step 2 On the **Parameter Set Management** page that is displayed, select the parameter set to be exported and click **Export**.

Figure 8-53 Exporting a parameter set



----End

9 Configuration Management

The **Commit History** page records the commitment history of service management, NE management, CLI, and consistency management during synchronization based on forwarder data. On this page, you can view historical commitment records and roll back specific commitment points.

9.1 Task Management

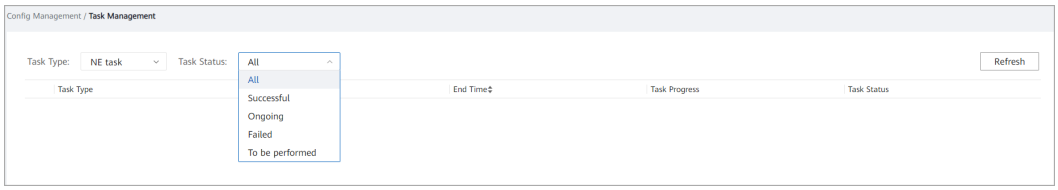
Scenario Description

Task management allows you to view the execution progress and result of a configuration task. Currently, only NE configuration tasks can be viewed.

Procedure

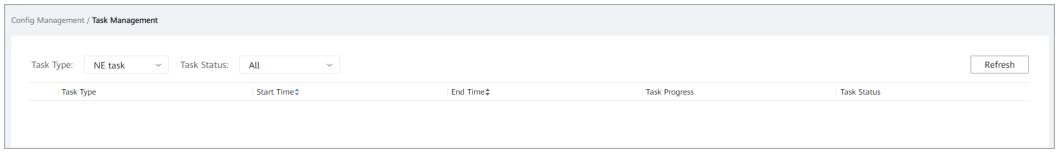
Step 1 Choose **Config Management** > **Task Management** from the main menu. On the **Task Management** page that is displayed, filter and view tasks by task status.

Figure 9-1 Filtering tasks by task status



Step 2 View the task status and execution result based on the filtering result.

Figure 9-2 Task details display



NOTE

Tasks that have been completed for more than half an hour are periodically cleared and are not displayed on the page.

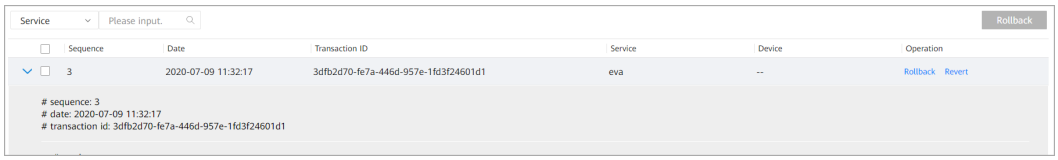
----End

9.2 Commit History

The **Commit History** page records the commitment history of service management, NE management, CLI, and consistency management during synchronization based on forwarder data. On this page, you can view historical commitment records and roll back specific commitment points.

Step 1 Choose **Config Management** > **Commit History** from the main menu. On the **Commit History** page, commitment records are displayed in order of time. You can click > on the left to view the detailed configurations.

Figure 9-3 Viewing the committed information



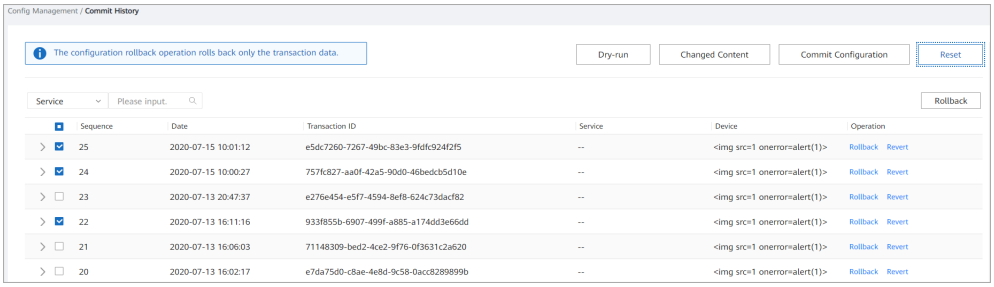
NOTE

The OPS framework tunes the committed information to facilitate storage and computation.

Step 2 Roll back specific commitment points. The following rollback methods are available:

- Roll back a single commitment point: Click **Rollback** in the **Operation** column. Then click **OK**.
- Roll back all configurations between the current time and a specified commitment point: Click **Revert** in the **Operation** column. Then click **OK**.
- Roll back multiple commitment points: Select commitment points, click **Rollback**, and click **OK**.

Figure 9-4 Selecting multiple commitment points for rollback



NOTE

1. You are advised to check whether the configurations meet expectations before performing a rollback.
2. When a single commitment point is rolled back, only this specific point will be rolled back if its configuration is not associated with that of the next commitment point. Otherwise, the next commitment point is also rolled back.

   For example:

   Commitment point 1: An instance (instance 1) is delivered.

   Commitment point 2: An attribute of instance 1 is delivered.

   When commitment point 1 is rolled back, commitment point 2 is also rolled back.

----End

10 CLI

This chapter describes the CLIs provided by the OPS and provides examples to facilitate user operations.

10.1 General Guidelines

1. Entering a question mark (?): Display the help information. A question mark (?) can be entered following other commands, such as preset executable commands (including **clear**, **dry-run**, **reset**, and **display**) and node names (such as **applications** and **bngBngPairs**) in the current view, or entered separately.

```
[NCE]> applications ?
bngBngPairs
bngSystemNes
isp
ispPairs
bngRoutingPairs
bngAaaPairs
hbng
```



```
bngVrfPairs
[NCE]>
```

2. Completing a command: After entering a correct prefix character, you can press **Tab** to complete the character string. If there are multiple strings with the same prefix, all the strings are displayed.
3. Command output: The information enclosed in square brackets ([]) is the prompt information, and the directly displayed strings are configurable.

```
[app:applications]> hbng abc
[app:applications/hbng:hbng[abc]]> domains
[Valid length:[1..64] description:Name of a domain, it is not case sensitive.]
[app:applications/hbng:hbng[abc]]>
```

NOTE

A maximum of 3,500 lines can be displayed on the CLI.

10.2 applications

Run the **applications** command to enter the service view.

```
Welcome to NCE CLI
[NCE]> applications
[app:applications]> ?
bngBngPairs
bngSystemNes
isp
ispPairs
bngRoutingPairs
bngAaaPairs
hbng
bngVrfPairs
clear
commit
display
dry-run
quit
return
undo
[app:applications]>
```

10.3 commit

```
Welcome to NCE CLI
[NCE]> applications
[app:applications]> hbng abc
[app:applications/hbng:hbng[abc]]> commit
[OK]
[app:applications]>
```

Run the **commit** command to deliver configurations. This command cannot be used to set parameters.

10.4 display Commands

Run the **display** commands to query information.

10.4.1 display this

Run the **display this** command to query data in the RDB and CDB. In this example, **"domainName":"bbb"** is the data in the CDB, as shown in the following figure.

```
[app:applications/hbng:hbng[hbng_ins]]> display this
{
  "hbng":
  [
    {
      "bng_service_name":"hbng_ins",
      "domains":
      [
        {
          "domainName":"aaa"
        },
        {
          "domainName":"bbb"
        }
      ]
    }
  ]
}
[app:applications/hbng:hbng[hbng_ins]]>
```

10.4.2 display this-configuration

Run the **display this-configuration** command to query data in the RDB. (In this example, the data **"domainName":"bbb"** in the CDB is not displayed.)

```
[app:applications/hbng:hbng[hbng_ins]]> display this-configuration
{
  "hbng":
  [
    {
      "bng_service_name":"hbng_ins",
      "domains":
      [
        {
          "domainName":"aaa"
        }
      ]
    }
  ]
}
[app:applications/hbng:hbng[hbng_ins]]>
```

10.4.3 display inconsistency-discovery

Run the **display inconsistency-discovery** command to query NE configuration inconsistencies (in the NE view). Before running this command, you need to run the command for comparing NE configuration inconsistencies described in **10.6.2 nes inconsistency-discovery [A] [B]...**.

```
[nes:nes/ne[ipi-zba900-r-bn-04]]> display inconsistency-discovery
### huawei-rsa ###
 rsa
  + rsaLocalKeys
    + rsaLocalKey
      + keySize: 2048
  + rsaPeerKeys
    + rsaPeerKey
      + [keyName=******]
        + keyName:******
```



```
        + encodeInType:DER
        + keyCode:
3082010A028DFADF5F4A65DSFADFADCVDFG055465ADSF5ASDF456A4DF5A4DF54AS65DF41FD231AD5F46
ADF5A1DF2
     + rsaGlobalCfg
       + maxKeyPair:20
### ietf-interfaces ###
      ......
```

10.4.4 display dry-run preview

Run the **display dry-run preview** command to query configuration comparison information. This command provides the same function as the **Delivered Device Data** tab page in the dry-run view on the GUI. You need to run the **dry-run** command before running this command.

```
Welcome to NCE CLI
[NCE]> nes ne ipi-zba900-r-bn-04
[nes:nes/ne[ipi-zba900-r-bn-04]]> system systemInfo sysName abc
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]> dry-run
[OK]
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]> display dry-run preview
### ipi-zba900-r-bn-04 ###
  <system xmlns="http://www.huawei.com/netconf/vrp/huawei-system">
    <systemInfo>
      <sysName>abc</sysName>
    </systemInfo>
  </system>
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]>
```

10.4.5 display dry-run compare

Run the **display dry-run compare** command to query the comparison result. This command provides the same function as the **Inconsistent Data** tab page in the dry-run view on the GUI. You need to run the **dry-run** command before running this command.

```
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]> display dry-run compare
### ipi-zba900-r-bn-04/(http://www.huawei.com/netconf/vrp/huawei-system)system ###
  system
    systemInfo
      +sysName: abc
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]>
```

10.5 dry-run

Run the **dry-run** command to perform comparison. The preview and comparison commands in **10.4.4 display dry-run preview** and **10.4.5 display dry-run compare** can be executed only after the **dry-run** command is executed successfully.

```
Welcome to NCE CLI
[NCE]> nes ne ipi-zba900-r-bn-04
[nes:nes/ne[ipi-zba900-r-bn-04]]> system systemInfo sysName abc
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]> dry-run
[OK]
[nes:nes/ne[ipi-zba900-r-bn-04]/huawei-system/system:system/systemInfo]>
```

10.6 nes Commands

Run the **nes** command to enter the NE management view.

10.6.1 nes ne [xxx]

Run the **nes ne** *[xxx]* command to enter the view of a single NE. *[xxx]* indicates the NE name.

```
[NCE]> nes ne ?
[ipi-zba900-r-bn-04 ipi-zba900-r-bn-17]
[NCE]> nes ne ipi-zba900-r-bn-04
[nes:nes/ne[ipi-zba900-r-bn-04]]>
```

10.6.2 nes inconsistency-discovery [A] [B]...

Run the **nes inconsistency-discovery** *[A] [B]...* command to compare NE configuration inconsistencies. *[A] [B]...* indicates the NE names. One or more NE names can be entered.

```
[NCE]> nes inconsistency-discovery ipi-zba900-r-bn-04
[OK]
[NCE]>
```

10.6.3 nes sync-to *[A] [B]...*

Run the **nes sync-to** *[A] [B]...* command to synchronize data from the NMS to NEs. *[A] [B]...* indicates the NE names. One or more NE names can be entered.

10.6.4 nes sync-from *[A] [B]...*

Run the **nes sync-from** *[A] [B]...* command to synchronize data from NEs to the NMS. *[A] [B]...* indicates the NE names. One or more NE names can be entered.

10.7 quit

Run the **quit** command to return to the upper-level view.

```
[NCE]> applications hbng abc domains bbb
[app:applications/hbng:hbng[abc]/domains[bbb]]> quit
[app:applications/hbng:hbng[abc]]>
```

10.8 reset

Run the **reset** command to reset configured data. This command must be executed in the top-level view. After this command is executed, the transaction IDs are deleted on the CLI side.

```
[app:applications/hbng:hbng[abc]]> return
[NCE]> reset
[OK]
[NCE]>
```

10.9 return

Run the **return** command to return to the top-level view.

```
[app:applications/hbng:hbng[abc]/environment[bbb]/vrfs[abc]]> return
[NCE]>
```


10.10 clear Command

Run the **clear** command to clear all contents on the screen. This function is the same as the **clear** command on Linux.

10.11 undo

This command is used to perform a deletion operation, for example, deleting a list, leaf list, leaf, or presence container node.

```
[app:applications]> display this
{
  "applications":
  {
    "hbng:hbng":
    [
      {
        "bng_service_name":"hbng1"
      },
      {
        "bng_service_name":"abc"
      }
    ]
  }
}
[app:applications]> undo hbng abc
[app:applications]> display this
{
  "applications":
  {
    "hbng:hbng":
    [
      {
        "bng_service_name":"hbng1"
      }
    ]
  }
}
[app:applications]>
```

10.12 rpc Command

The **rpc** command can be executed when the YANG file of a service or NE contains an RPC structure.

10.13 recompute

Run the **recompute** command based on the **hbng** service point to perform recomputing. For details about the application scenarios of recomputing, see **Figure 7-2**.

The recomputing function can be used only on the points under the **applications** level.

```
[app:applications]> hbng hbng1
[app:applications/hbng:hbng[hbng1]]> recompute
[OK]
[app:applications/hbng:hbng[hbng1]]>
```

