Configuration Guide
RG-SNC_2.33_EN_Build20161108

Copyright Statement

Exemption Statement

This document is provided “as is”. The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Obtaining Technical Assistance

- Ruijie Networks Website: http://www.ruijienetworks.com/
- Service Email: service_rj@ruijienetworks.com
- Technical Support: http://www.ruijienetworks.com/service.aspx
- Technical Support Hotline: +86-4008-111-000

Chapter 1 Homepage

The TOP N information of the system is shown on the homepage, which includes the following: TOP N of device performance indexes, TOP 8 of alarm statistics and faulty devices, TOP 10 of realtime alarms.

TOP N of device performance index can be displayed with 5, 10, 15, 20, or 25. The initial value is 5.

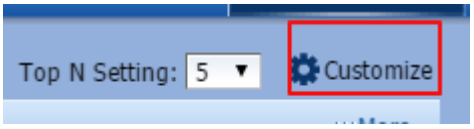
Figure 1.1. Homepage - TOP N

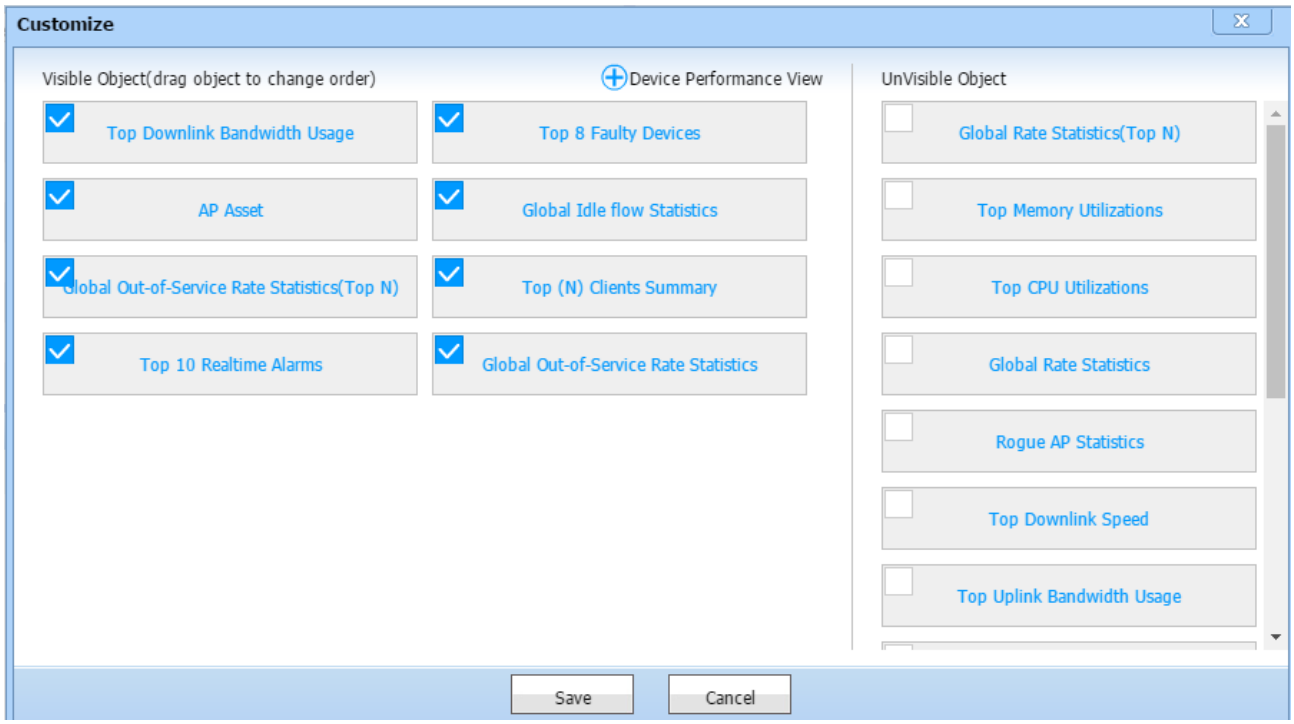
Setting of TOP N of device performance indexes

Figure 1.2. Homepage TOP N setting 1

Figure 1.3. Homepage TOP N setting 2

Click **Customize**. The **Customize** page appears. You can select the metrics to be displayed and drag the metrics to change their order. The items in the **Device Performance View** are displayed on the home page.





- Device performance index includes CPU utilization, memory utilization, bandwidth receiving utilization, bandwidth sending utilization. The utilization is displayed using color pillar and the height of pillar is in proportion to the utilization value. Three colors are used: Green means the device performance index threshold is not reached. For example:
- Orange means level 1 device performance index threshold is reached. For example:
- Red means level 2 device performance index threshold is reached. For example:
- If only level 1 index threshold is configured, it will show only green or orange.
- Each TOP N device group of performance index is sorted according to the utilization value.
- Alarm statistics is classified based on alarm level and shown with histogram. The alarm level can be distinguished from color. For alarm level, please refer to Example
- TOP 8 of faulty devices shows the devices which generate normal level above alarm and the alarm has not been acknowledged yet in the system. The devices are displayed based on the generation time of the alarm.
- TOP 10 of realtime alarms show the alarms which are above normal level and are not acknowledged yet in the system. The newly generated 10 alarms are displayed and sorted based on the alarm level.

Chapter 2 Device Management

This module enables you to add, delete, modify and view devices, interfaces and relevant parameters.

- Device Info Management
- Device Operation
- Modify Device Information in Batch
- Batch Synchronization of Device Information
- Device Interface Management
- Device Parameter Management
- Terminal Management
- Batch Synchronization of Device Information
- Modify Device Information in Batch

2.1. Device Info Management

This module describes addition, deletion, modification and search operations of devices and devices info, and user friendly display.

- Global Device Search
- Add Device
- Device Autodiscovery
- Device Group Management
- Import Device Group Tree
- Export Device Group Tree
- SNMP and Telnet Templates Batch Modification
- Search Device
- Delete Device
- View Device Info
- View Device MIB Info
- Sync Device Info

2.1.1. Add Device

The device can be managed only after it is added to the system. Manual adding is one of the methods the system provides to add devices, and it is used to add a device with an unknown IP address to the system.

Operation Steps

1) Go to **Device** page, and click **Add Device** to enter the **Add Device** page, as shown below:

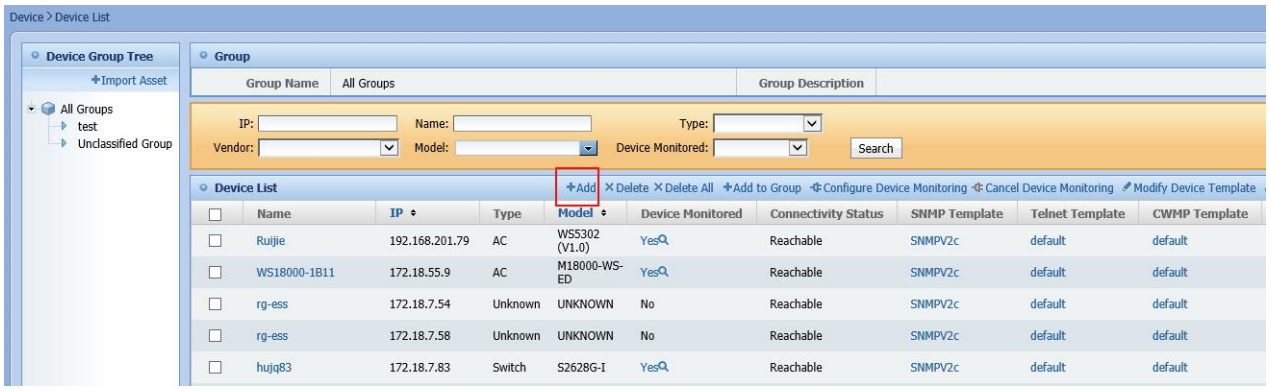


Figure 2.1-2.2. To enter Add Device page

Fill in the information on **Add Device** page, and then click **Add** to add device information, as shown below:

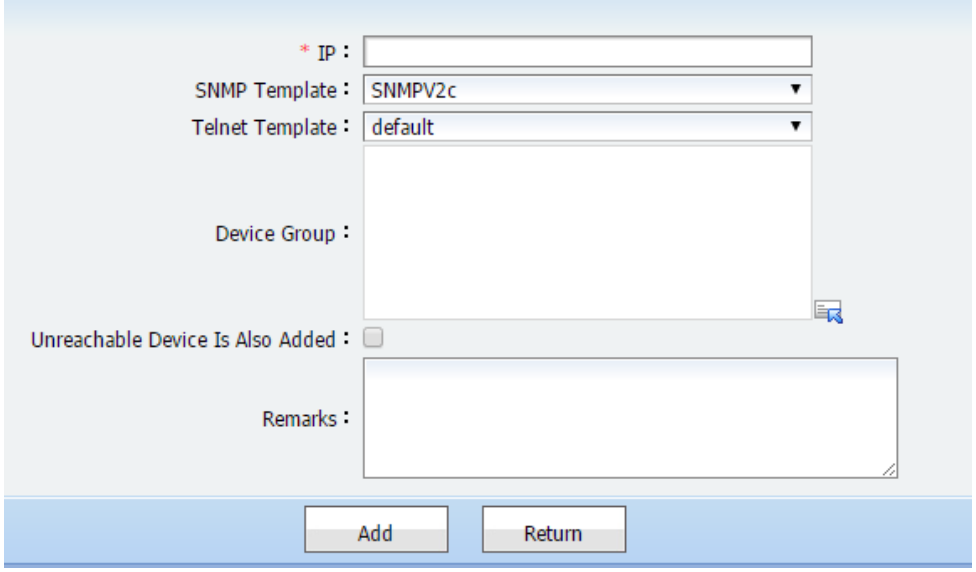


Figure 2.3. Add Device page

Clicking **Return** on **Add Device** page will bring system back to **Device** page without saving any change.

Note

The device IP address must not be null and must be valid.

Note

When adding devices, use the selected SNMP template to obtain MIB info of devices. If the parameters in the SNMP template do not match those of a device, the device can be successfully added, but the MIB info cannot be obtained.

Note

If "**Non-connective Device Is Also Added**" is checked, a device which cannot be reached by Ping command can also be added. Otherwise, it cannot be added.

2.1.2. Device Autodiscovery

The device can be managed only after it is added to the system. Device Autodiscovery is one of the methods the system provides to add devices. It scans the network segment specified by users to discover a manageable device and then add it to the system. If no network segment is specified, the devices in the whole network are scanned.

Operation Steps

1) Go to **Device** page, and then click **Device Autodiscovery** to enter **Device Autodiscovery** page, as shown below:

Figure 2.4. Enter Device Autodiscovery page

On **Device Autodiscovery** page, input the seed IP address, start IP address and end IP address for topology discovery, choose one or multiple SNMP templates, and then click **Autodiscovery** to start autodiscovery, as shown below:

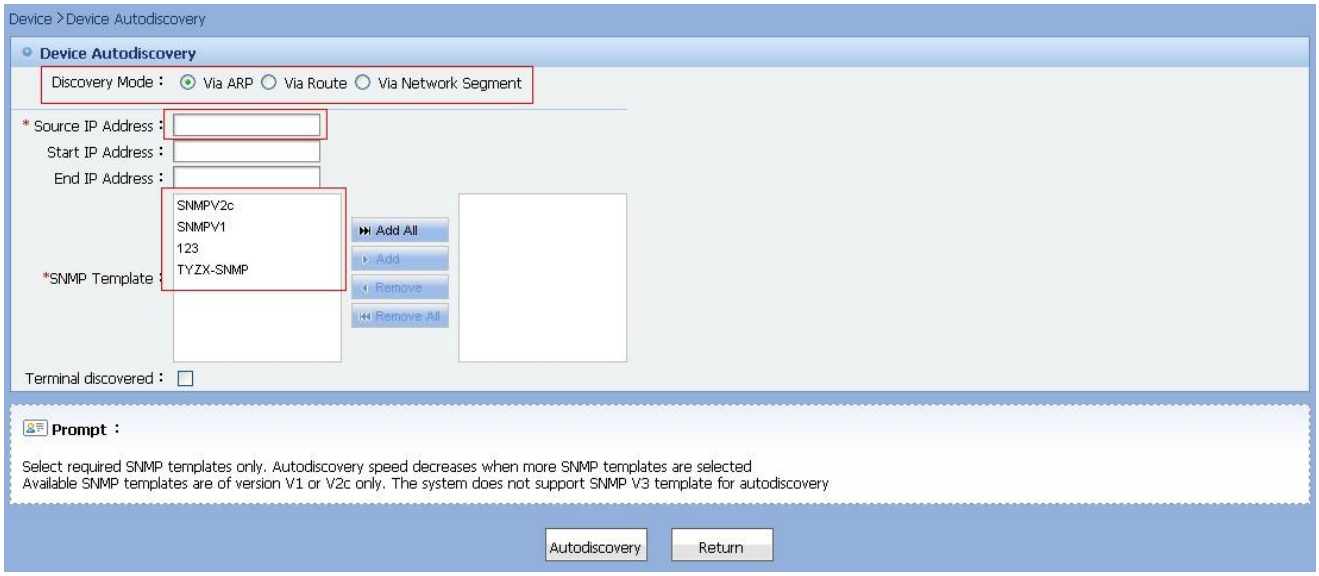
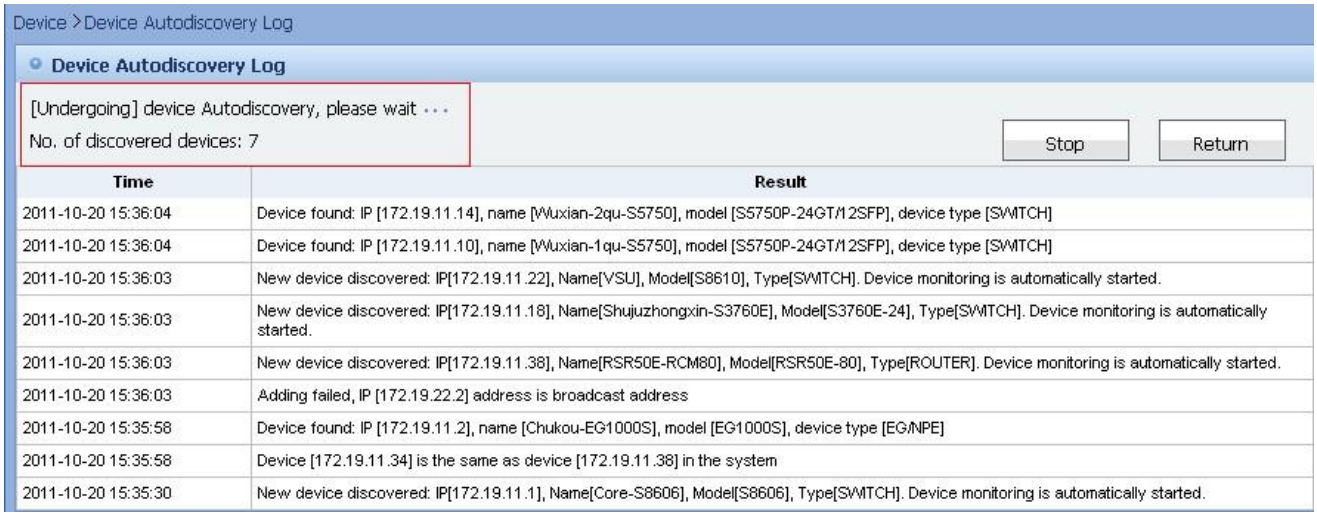


Figure 2.5. Device Autodiscovery page

The system will switch to **Device Autodiscovery Log** page after autodiscovery is started. Autodiscovery progress, info of found devices and error messages will be shown dynamically on this page as follows:



Time	Result
2011-10-20 15:36:04	Device found: IP [172.19.11.14], name [Wuxian-2qu-S5750], model [S5750P-24GT/12SFP], device type [SWITCH]
2011-10-20 15:36:04	Device found: IP [172.19.11.10], name [Wuxian-1qu-S5750], model [S5750P-24GT/12SFP], device type [SWITCH]
2011-10-20 15:36:03	New device discovered: IP[172.19.11.22], Name[VSU], Model[S8610], Type[SWITCH]. Device monitoring is automatically started.
2011-10-20 15:36:03	New device discovered: IP[172.19.11.18], Name[Shujuzhongxin-S3760E], Model[S3760E-24], Type[SWITCH]. Device monitoring is automatically started.
2011-10-20 15:36:03	New device discovered: IP[172.19.11.38], Name[RSR50E-RCM80], Model[RSR50E-80], Type[ROUTER]. Device monitoring is automatically started.
2011-10-20 15:36:03	Adding failed, IP [172.19.22.2] address is broadcast address
2011-10-20 15:35:58	Device found: IP [172.19.11.2], name [Chukou-EG1000S], model [EG1000S], device type [EG/NPE]
2011-10-20 15:35:58	Device [172.19.11.34] is the same as device [172.19.11.38] in the system
2011-10-20 15:35:30	New device discovered: IP[172.19.11.1], Name[Core-S8606], Model[S8606], Type[SWITCH]. Device monitoring is automatically started.

Figure 2.6. Device Autodiscovery page

Click **Stop** on **Device Autodiscovery Log** page to switch the system to **STOPPING** status. Autodiscovery will be stopped in several seconds.

Note IpRouteTable and IpAddrTable in SNMP are used in autodiscovery.

Note The seed IP address must not be empty. The input must be a legal L3 device IP address.

Note The start IP address must NOT be greater than the seed IP address. For example, 192.168.1.1 is less than 192.168.1.3. The end IP address must NOT be less than the seed IP address.

Note In autodiscovery, device MIB info will be read if the SNMP access parameter of a device matches that in the SNMP template. Otherwise, the MIB info won't be read.

Note Please select necessary SNMP templates only. The more SNMP templates you select, the slower the autodiscovery speed is.

Note Only SNMP template version V1 and V2c are available. Autodiscovery with SNMP template version V3 is not supported.

2.1.3. Device Group Management

Through Device Group Management, devices can be classified to different groups and easily managed.

Go to **Device** page, click **Import Asset** icon to enter **Group Management** page, as shown below:

Figure 2.7. Device Group Management page

2.1.4. SNMP and Telnet Templates Batch Modification

On the **Device**, you can modify SNMP and Telnet templates in batch.

Operation Steps

1) Go to **Device** page, select devices on which SNMP and Telnet templates need to be modified (or do Search Device operation). Then click **Edit SNMP Template** or **Edit TELNET Template**, and the system will prompt the dialog box for SNMP or Telnet modification, as shown below:

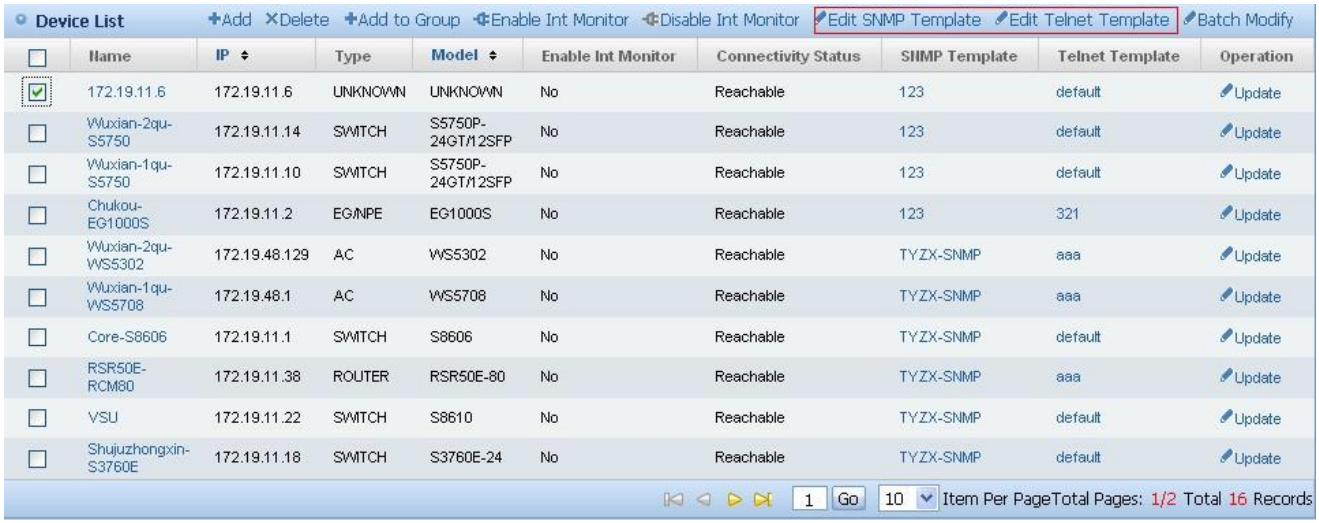


Figure 2.8. **Edit SNMP Template** and **Edit TELNET Template** Buttons

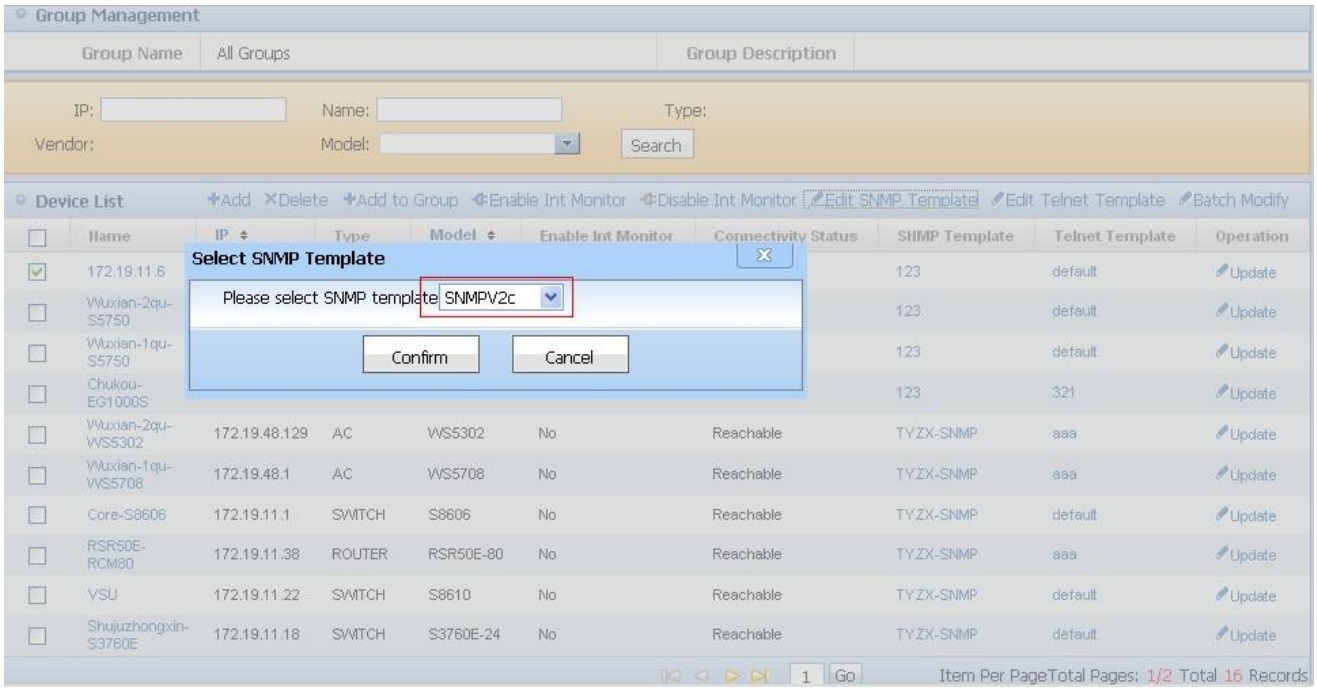


Figure 2.9. Modify SNMP Template

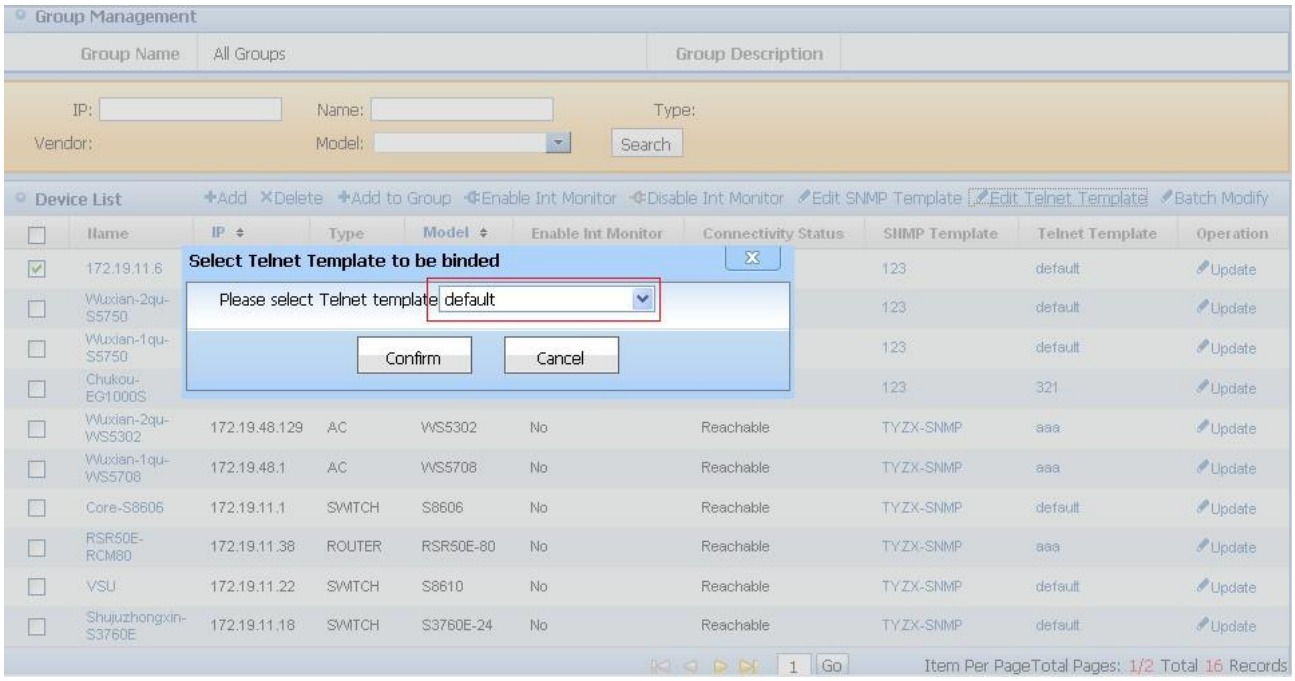


Figure 2.10. Modify Telnet Template

Note

When searching for a device IP address, the system will do fuzzy search to IP addresses of all devices IP tables. For example, if device A whose IP address is 192.168.1.172 and device B whose IP address is 192.168.2.10 are in the system, and IP 192.168.3.172 is in IP table of device B, then both device A and device B will be found if the keyword is “172”.

2.1.5. Search Device

On the **Device** page, you can search devices of the system by device IP, name, type, manufacturer and model.

Operation Steps

1) Go to **Device** page, input device IP address, name, type, manufacturer and model, and then click **Search**. The system will list the devices which match the search conditions, as shown below:

Figure 2.11. Search Device

Go to **Device** page, and click **device IP address** or **model** column header to order the column, as shown below:

Figure 2.12. Order Device

Note

When searching a device IP address, the system will do fuzzy search to IP addresses of all devices IP tables. For example, if device A whose IP is 192.168.1.172 and device B whose IP is 192.168.2.10 are in the system, and IP 192.168.3.172 is in IP table of device B, then both device A and device B will be found if the keyword is “172”.

Note

Order device supports no order(double arrow), ascend order(down arrow) and descend order(up arrow). The order is to all devices in the list, not just devices on the current page.

2.1.6. Delete Device

Batch devices deletion can be done on **Device** homepage.

Operation Steps

1) Go to **Device** page, select devices in device list, and then click **Delete**. The system will prompt you to confirm the deletion. Click **OK** to do the deletion, as shown below:

Figure 2.13. Delete Device

2.1.7. View Device Details

Device info can be viewed on Device Detail page.

Operation Steps

1) Go to **Device** page, and click **Device Name** link in device list to enter **Device Detail** page of the device, as shown below:

Name	IP	Type	Model	Enable Int Monitor	Connectivity Status	SNMP Template	Telnet Template	Operation
172.19.11.6	172.19.11.6	UNKNOWN	UNKNOWN	No	Reachable	123	default	Update
Wuxian-2qu-S5750	172.19.11.14	SWITCH	S5750P-24GT/12SFP	No	Reachable	123	default	Update
Wuxian-1qu-S5750	172.19.11.10	SWITCH	S5750P-24GT/12SFP	No	Reachable	123	default	Update
Chukou-EG1000S	172.19.11.2	EG/NPE	EG1000S	No	Reachable	123	321	Update
Wuxian-2qu-WS5302	172.19.48.129	AC	WS5302	No	Reachable	TYZX-SNMP	aaa	Update
Wuxian-1qu-WS5708	172.19.48.1	AC	WS5708	No	Reachable	TYZX-SNMP	aaa	Update
Core-S8606	172.19.11.1	SWITCH	S8606	No	Reachable	TYZX-SNMP	default	Update
RSR50E-RCM80	172.19.11.38	ROUTER	RSR50E-80	No	Reachable	TYZX-SNMP	aaa	Update
VSU	172.19.11.22	SWITCH	S8610	No	Reachable	TYZX-SNMP	default	Update
Shujuzhongxin-S3760E	172.19.11.18	SWITCH	S3760E-24	No	Reachable	TYZX-SNMP	default	Update

Figure 2.14. Search Device

On **Device Detail** page, there is device info tab group. The default tab is device basic info, as shown below:

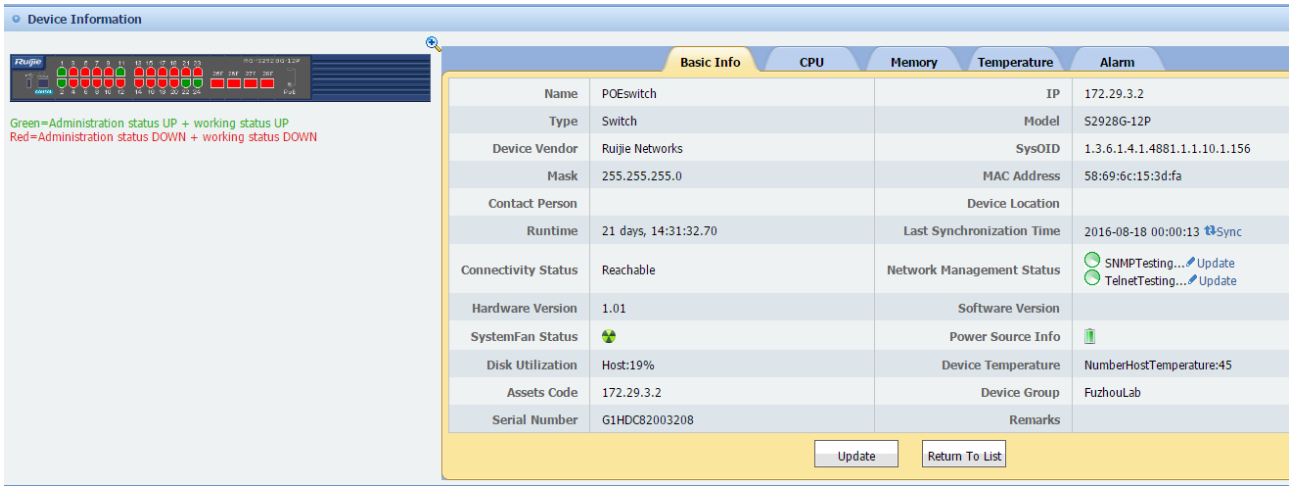


Figure 2.15. Device Info - Basic Info

The system will do device SNMP and Telnet connectivity test when Device Detail page is shown. The test is conducted through ajax, so that operations on the page will not be affected. “Detecting, please wait” prompt will be shown when the test is running. Connectivity info will be shown after the test is complete, as shown below:

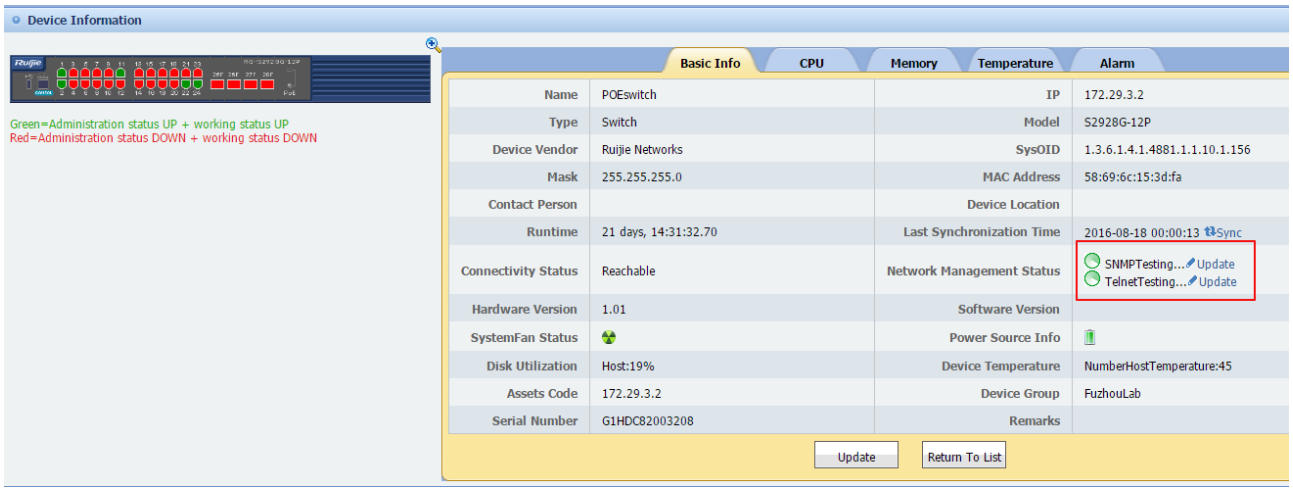


Figure 2.16. SNMP and Telnet Connectivity Test - Detecting

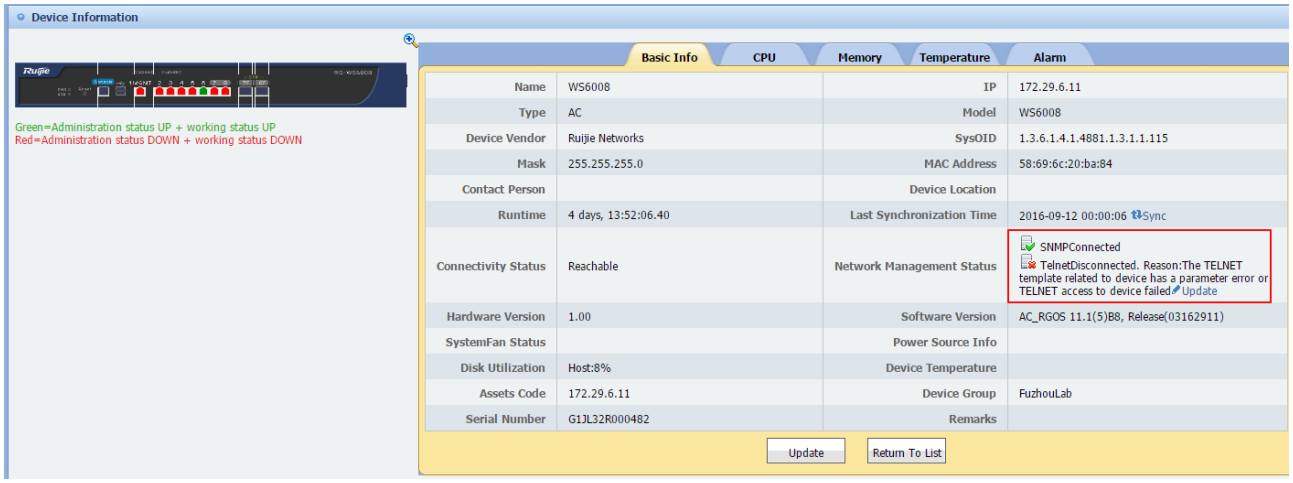


Figure 2.17. SNMP and Telnet Connectivity Test - Detection Complete

2.1.8. Update Device Info

This function enables you to edit the device information.

Operation Steps

1. On **Device List**, click **Update** to enter **Modify Device Information** page, as shown below:

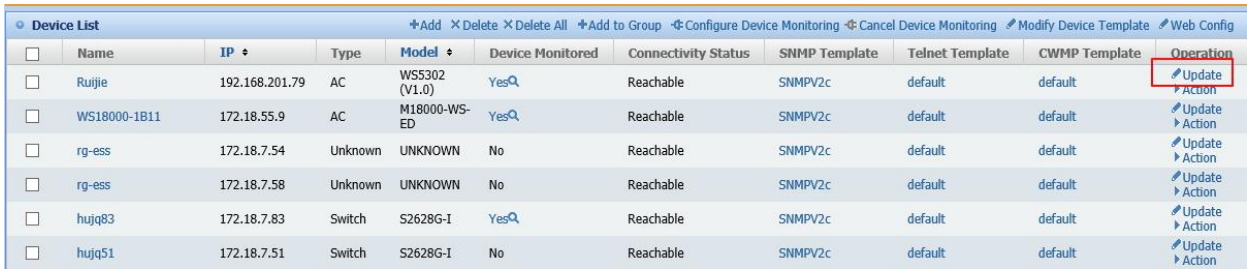


Figure 2.18. Modify Device Information

2. You can also go to the specified device details page, click **Update** to enter **Modify Device Information** page, as shown below:

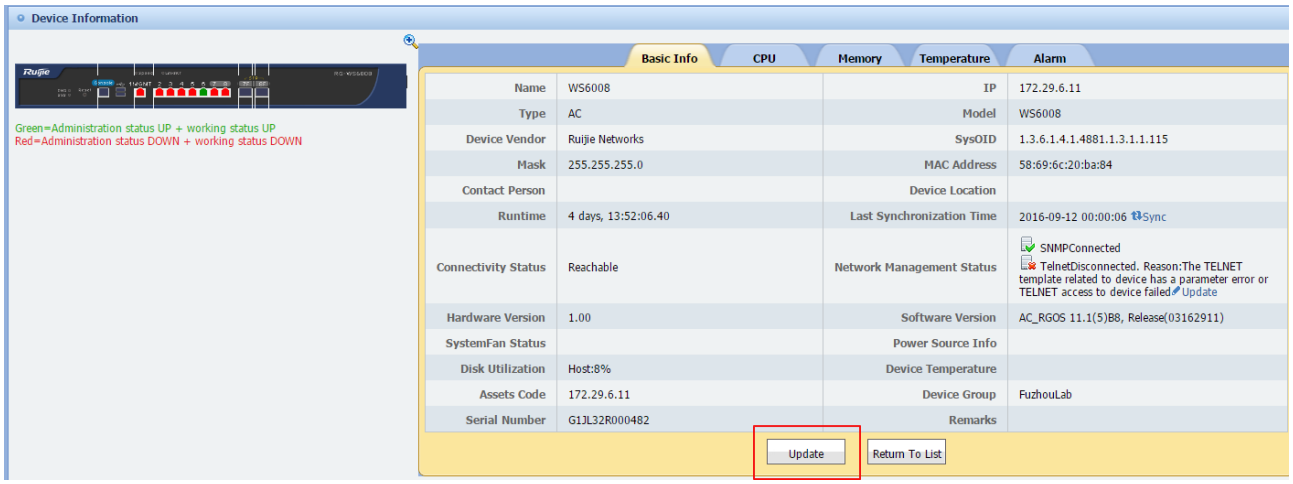


Figure 2.19. Device Details

3. On the **Modify Device Information** page, you can edit the device name, IP address, management IP address, SNMP template, Telnet template, CWMP template, contact person, device location, device group and remarks. If the device has multiple IP addresses, management IP address must be one of them.

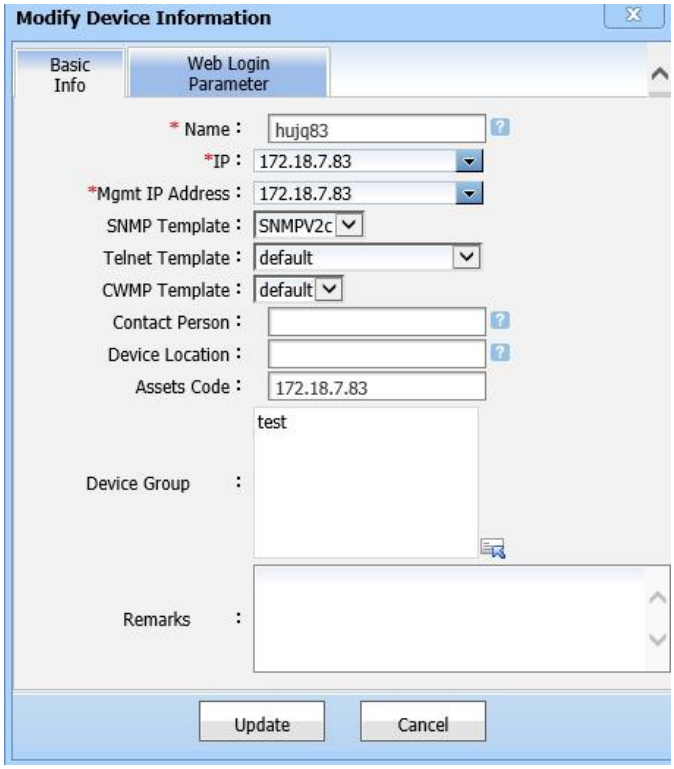


Figure 2.20. Modify Device Information

2.1.9. View Device Info

This function enables you to view the device information such as IP address table, ARP table, routing table and interface table.

- IP Address Table
- ARP Table
- Routing Table
- Interface Table
- MAC Forwarding Table

2.1.9.1. IP Address Table

Operation Steps

In **Device List**, click the specified device to enter **Device Details.** On the left **Navigation Bar**, **go to Device**>**Device Information**>**IP Table** to view the **IP Table** page, as shown below:

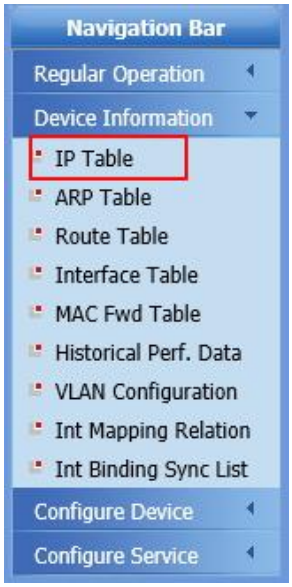


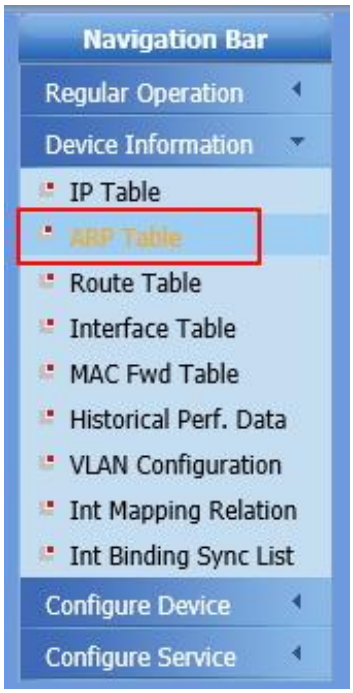
Figure 2.21. IP Address Table page

2.1.9.2. ARP Table

In the system, you can easily view the ARP table of device MIB info.

Operation Steps

In **Device List**, click the specified device to enter **Device Details.** On the left **Navigation Bar**, **go to Device**>**Device Information**>**ARP Table** to view the **ARP Table** page, as shown below:



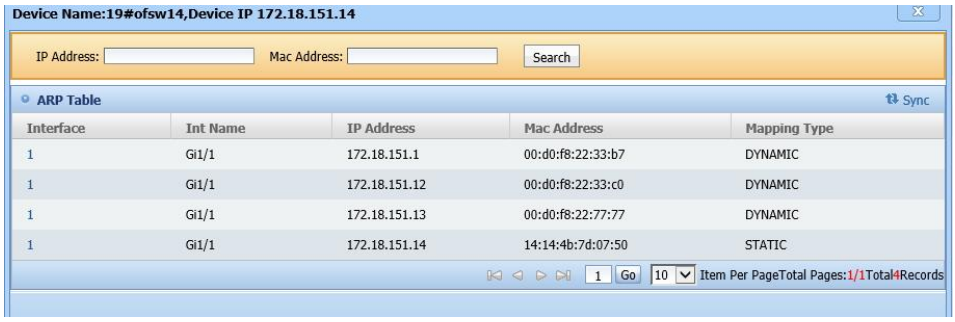
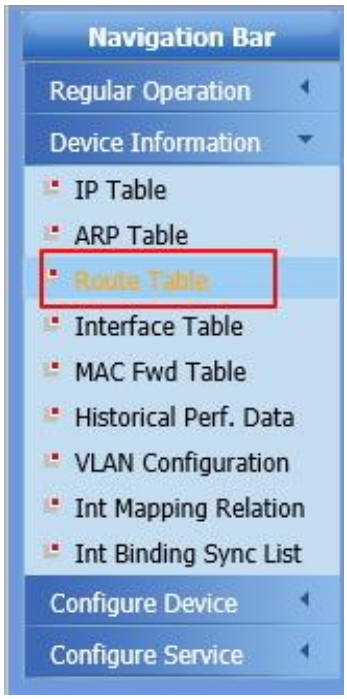


Figure 2.22-2.23. ARP Table page

2.1.9.3. Routing Table

Operation Steps

In **Device List**, click the specified device to enter **Device Details.** On the left **Navigation Bar**, **go to Device**>**Device Information**>**Route Table** to view the **Route Table** page, as shown below:



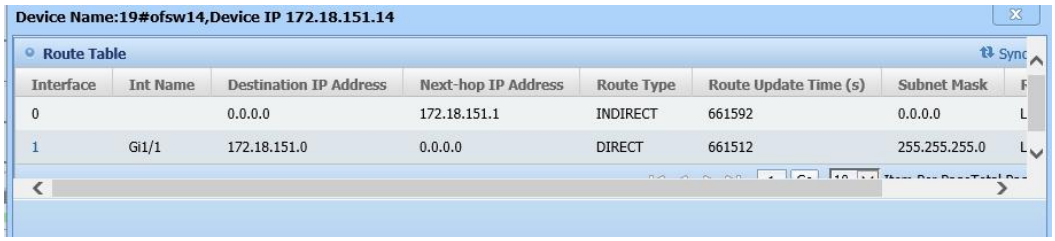
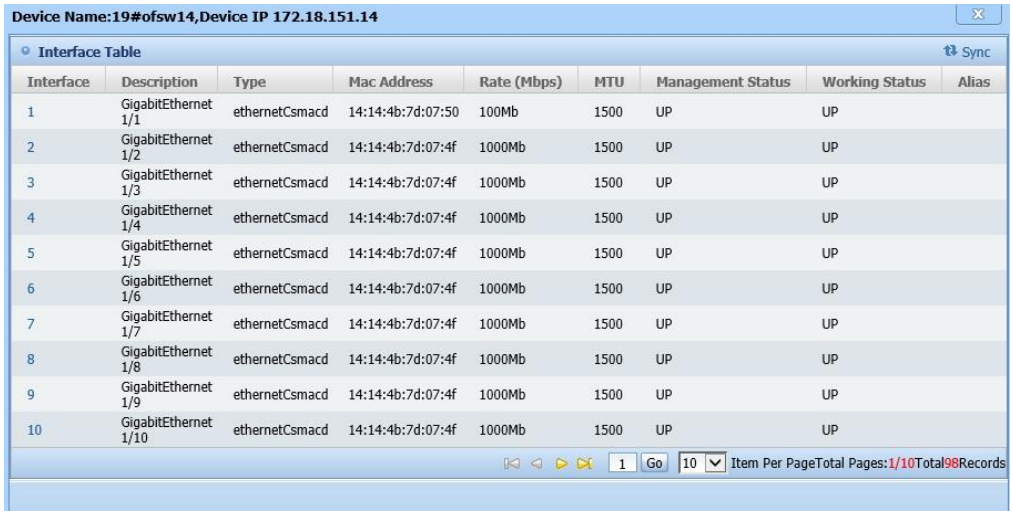


Figure 2.24-2.25. Route Table page

2.1.9.4. Interface Table

Operation Steps

In **Device List**, click the specified device to enter **Device Details.** On the left **Navigation Bar**, **go to Device**>**Device Information**>**Interface Table** to view the **Interface Table** page, as shown below:



Device Name:19#ofsw14,Device IP 172.18.151.14

Interface Table

Sync

Interface	Description	Type	Mac Address	Rate (Mbps)	MTU	Management Status	Working Status	Alias
1	GigabitEthernet 1/1	ethernetCsmacd	14:14:4b:7d:07:50	100Mb	1500	UP	UP	
2	GigabitEthernet 1/2	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
3	GigabitEthernet 1/3	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
4	GigabitEthernet 1/4	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
5	GigabitEthernet 1/5	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
6	GigabitEthernet 1/6	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
7	GigabitEthernet 1/7	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
8	GigabitEthernet 1/8	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
9	GigabitEthernet 1/9	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	
10	GigabitEthernet 1/10	ethernetCsmacd	14:14:4b:7d:07:4f	1000Mb	1500	UP	UP	

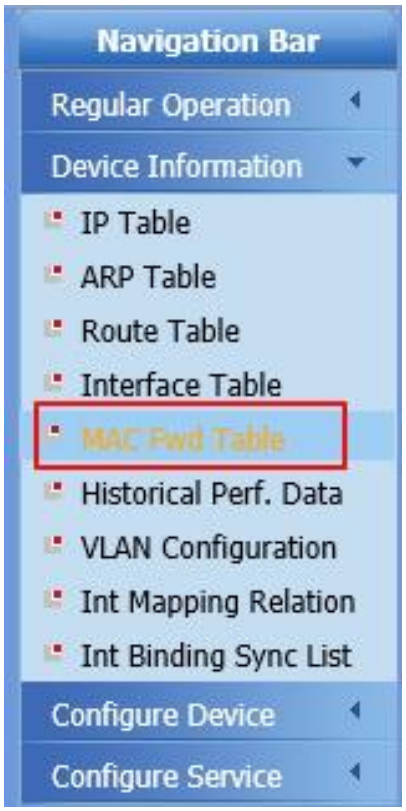
1 Go 10 Item Per PageTotal Pages:1/10Total98Records

Figure 2.26-2.27. Interface Table Page

2.1.9.5. MAC Forwarding Table

Operation Steps

In **Device List**, click the specified device to enter **Device Details.** On the left **Navigation Bar**, **go to Device**>**Device Information**>**MAC Fwd Table** to view the **MAC Fwd Table** page, as shown below:



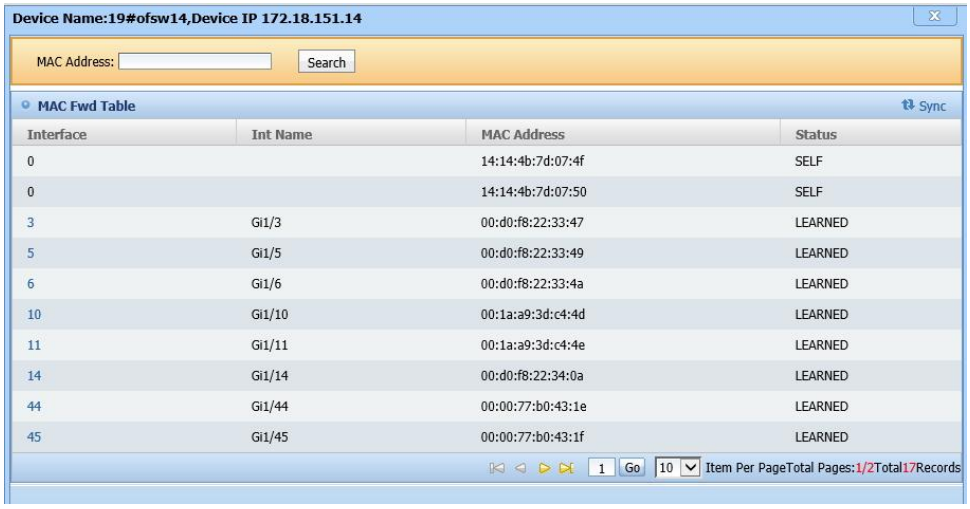


Figure 2.28-2.29. MAC Forwarding Table page

Note Most of the data is from entries of ipAddrTable (IP address table), ipNetToMediaTable (ARP table), ipRouteTable (routing table), and ifTable(interface table) of RFC 1213.

Note Besides, the interface name of interface detail is from entry ifName of ifXTable (interface extension table) of RFC 2233.

Note If SNMP template is correct while ARP table and routing table are empty, please perform sync.

2.1.10. Sync Device Info

The system will sync some device info, including system group, IP address table and interface table in device MIB, when Device Detail page is visited. But, sync operations are needed to sync ARP address table and routing table in device MIB.

Operation Steps

1) The system will do Sync when ARP address table, routing table and MAC forwarding table are visited for the first time, as shown below:

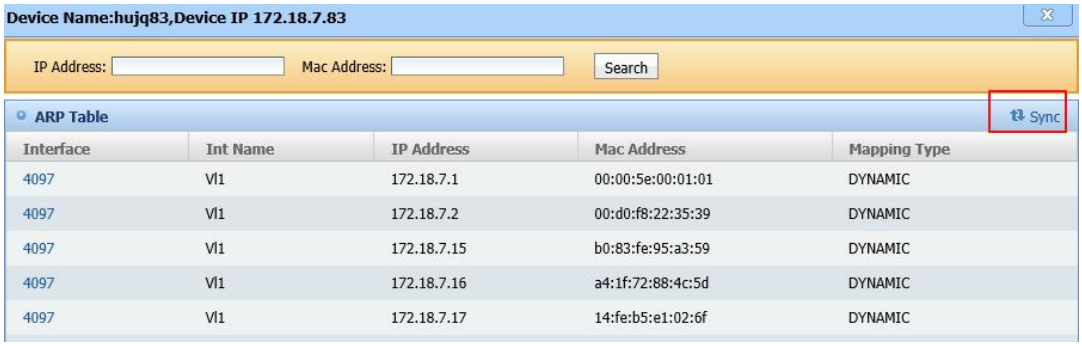


Figure 2.30. Sync View

Go to **Device Detail** page, click **Sync** link, the system will prompt dialog indicating the sync is ongoing. After it is done, **Device Detail** page will be refreshed, as shown below:

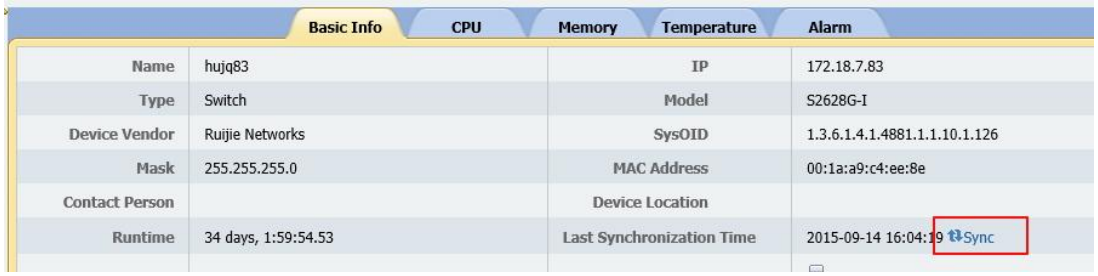


Figure 2.31. Sync Link

Note: Correct MIB info can be synchronized only when SNMP is in reachable state.

Note: The system retrieves interface table, routing table and other data when doing sync. It takes longer time when using SNMP V3 template. So we recommend you to use SNMP V2c template.

2.2. Device Operation

This module describes basic operations on devices.

- Telnet Operation
- Ping Operation
- Traceroute Operation
- Switch to Device Web Management Page
- Network Inspector

2.2.1. Telnet Operation

On **Device Detail** page, Telnet operation can be performed to the device.

Operation Steps

1) Go to **Device Detail** page, and click **Telnet** link. The system will display the Telnet command prompt box for the operating system (just like what you do by running Telnet via command line), as shown below:

Figure 2.32. Telnet Link

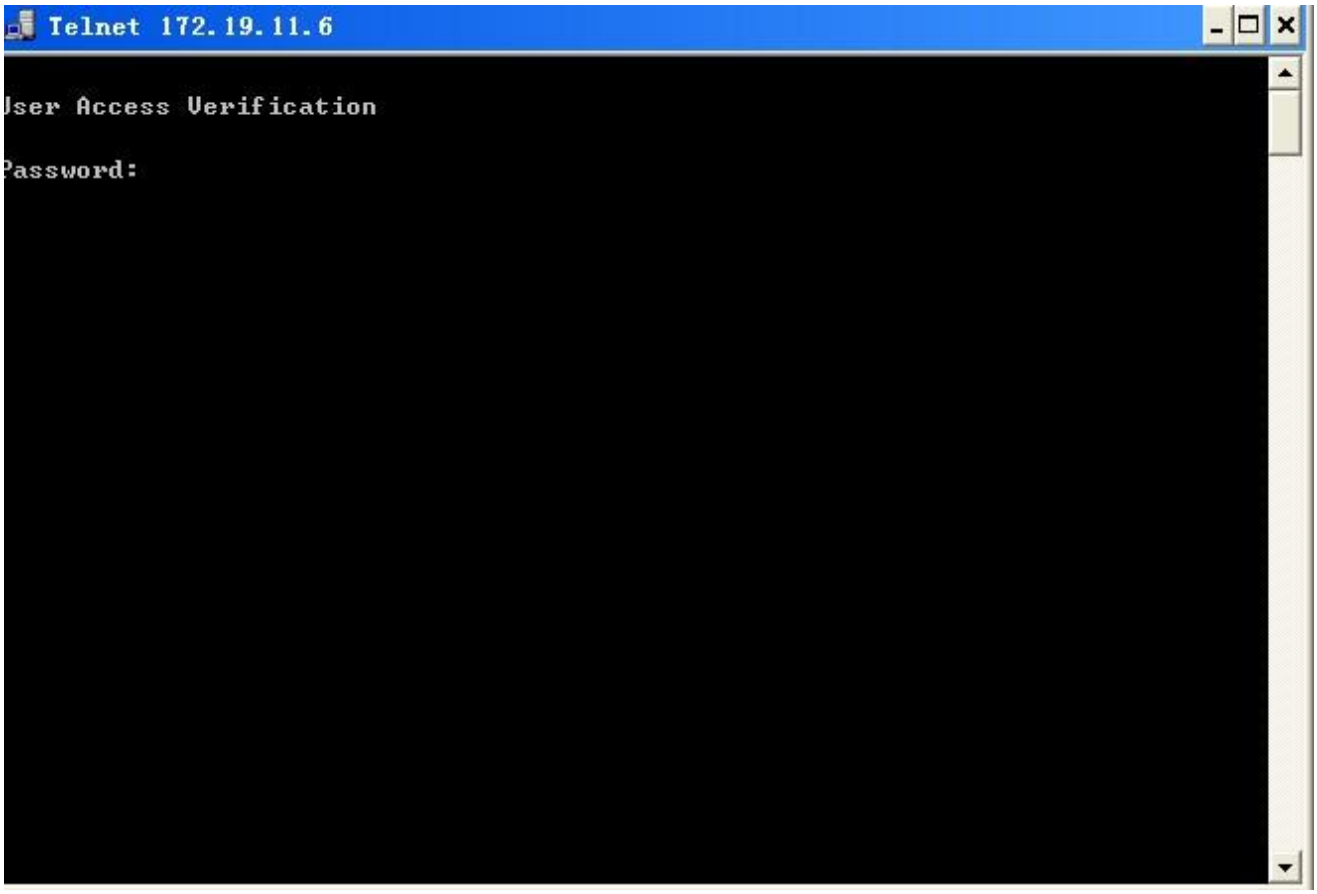


Figure 2.33. Telnet Command Prompt

Note

Because of the default policy of IE7.0, Telnet to the device might fail in IE 7.0. In this case, you can click the prompt icon beside the Telnet link on the page and modify Registry according to the steps in the pop-up box to Telnet to the device again.

2.2.2. Ping Operation

On **Device Detail** Info page, ping operation can be performed to the device.

Operation Steps

1) Go to **Device Detail** page, click **Ping** link. The system will prompt an info box to show the result. You can close the box by clicking close button at the upper right corner, as shown below:

Figure 2.34. Ping Link

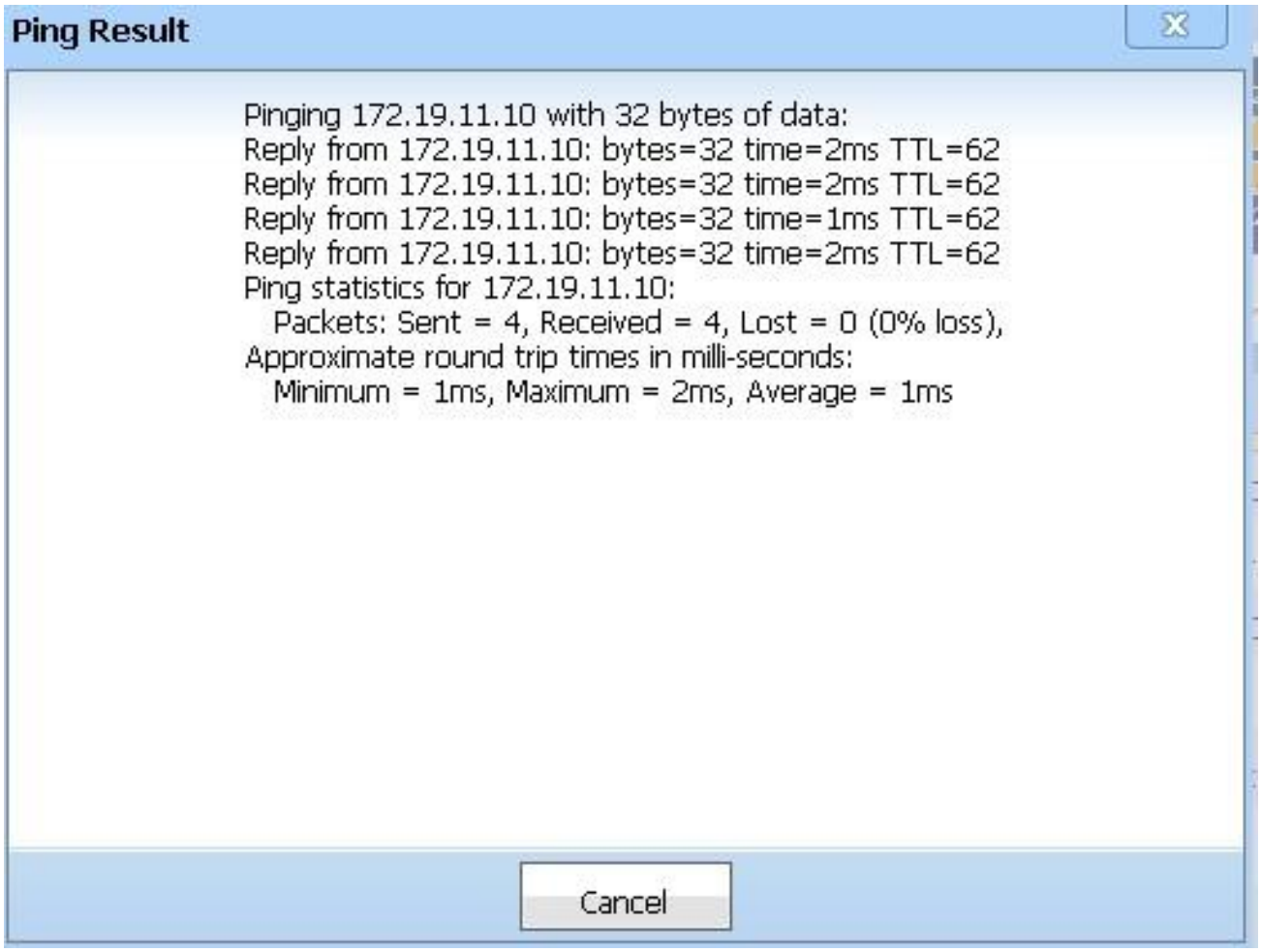


Figure 2.35. Ping Result Info Box

Note

The Ping command is run from the server, not your client machine. That is, the result is that of pinging from the server to the device.

2.2.3. Traceroute Operation

On **Device Detail** page, traceroute operation can be performed to the device.

Operation Steps

1) Go to **Device Detail** page, and click **Route Trace** link. The system will display info box to show the result of traceroute on the device. Click **Close** in the upper right corner to close the dialog box, as shown below:

Figure 2.36. Traceroute Link

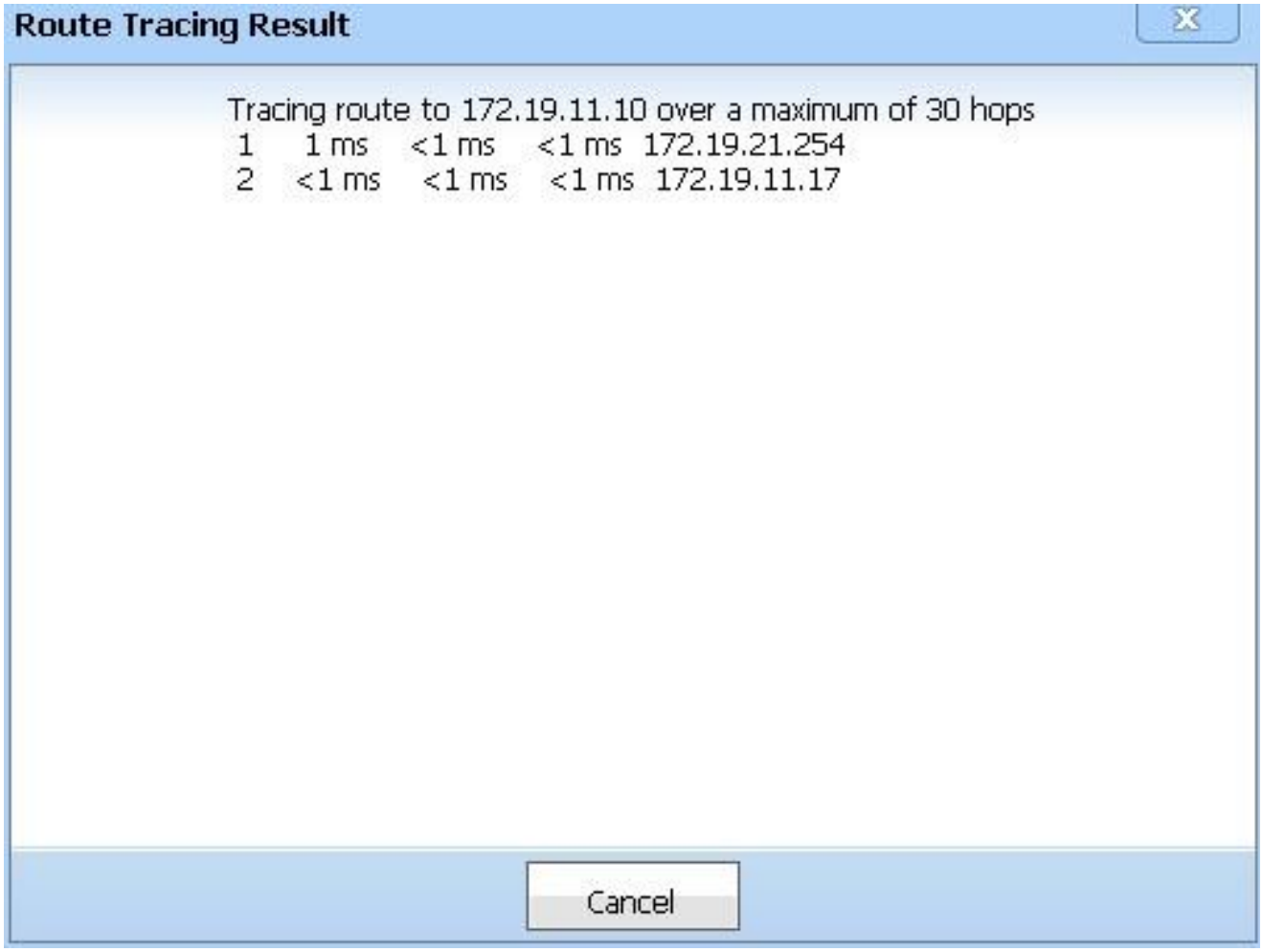


Figure 2.37. Traceroute Result Info Box

Note

Traceroute operation is performed from the server on which the system is running, not your client. That is, the result is that of traceroute from the server to the device.

2.2.4. Switch to Device Web Management Page

You can switch to **Device Web Management** page from **Device Detail** page.

Operation Steps

1) Go to **Device Detail** Info page, and click **Web** link. Then, **Device Web Management** page will be displayed, as shown below:

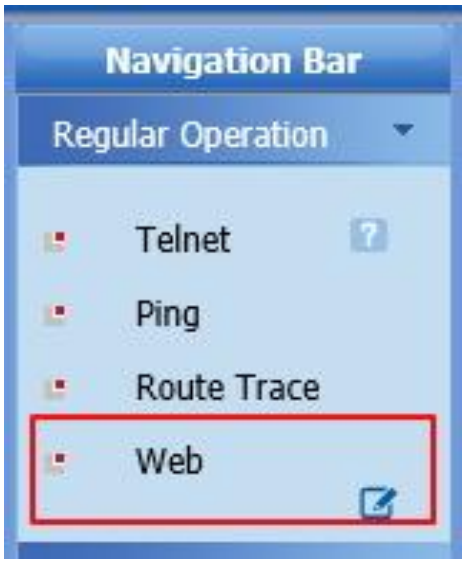


Figure 2.38. Device Web Management link

Note

Device Web Management page is accessible only when Web Management service is running on the device.

2.2.5. Network Inspector

The purpose of Network Inspector is to conduct Ping, SNMP and Telnet tests on a server to devices. Connectivity test result is passed if a device can be connected by any of the three methods. Connectivity test result is failed if a device can NOT be connected by any of the three methods. In the system, periodical connectivity test plan and real-time manual connectivity test are both available. Connectivity test result will be generated as a test report for download.

- Auto Connectivity Test
- Connectivity Test
- Test Report Download

2.2.5.1. Auto Connectivity Test

In the system, periodical auto connectivity test can be scheduled to do connectivity test on devices. Connectivity test result will be generated as a test report for download.

Operation Steps

1) Go to any page of Device; click **Network Inspector** link in the navigation bar on the left to enter **Network Inspector** page. Then click **Periodical Test** to enter **Periodical Connectivity Test** page, as shown below:

Figure 2.39. Select **Network Inspector**

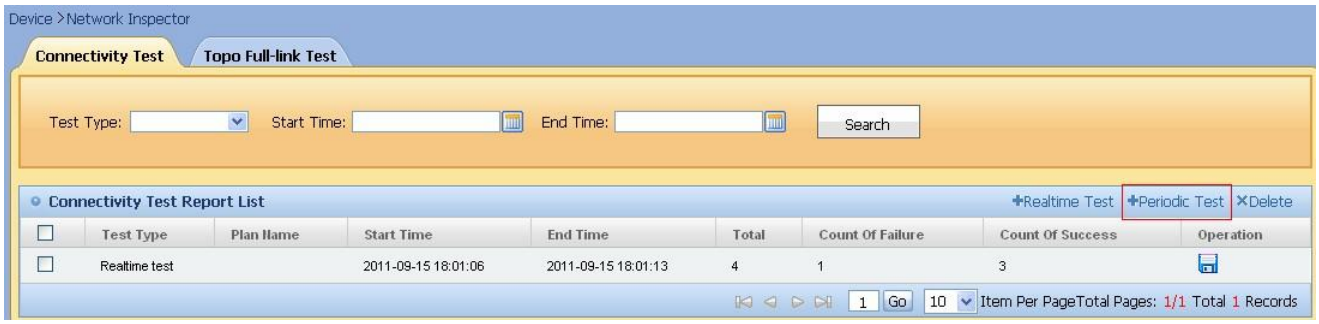


Figure 2.40. Select **Periodical Test** operation

- Add or Modify Auto Connectivity Test
- Enable or Disable Auto Connectivity Test
- Delete Auto Connectivity Test

3.2.5.1.1. Add or Modify Auto Connectivity Test

Auto connectivity test can be added or modified on Auto Connectivity Test page. The Operation Steps for connectivity test addition and modification are basically the same.

Operation Steps

1) Go to **Periodical Connectivity Test Plan** page, and click **Add** to enter **Add Plan** page; or click **Modify** to enter **Modify Plan** page, as shown below:

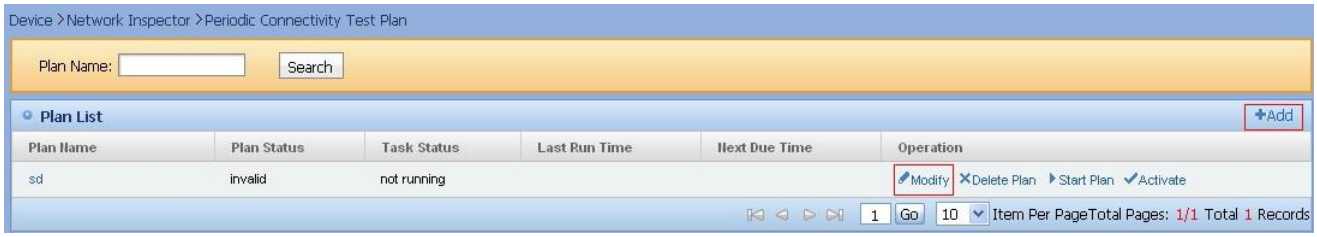


Figure 2.41. Enter Add or Modify Periodical Connectivity Test Plan page

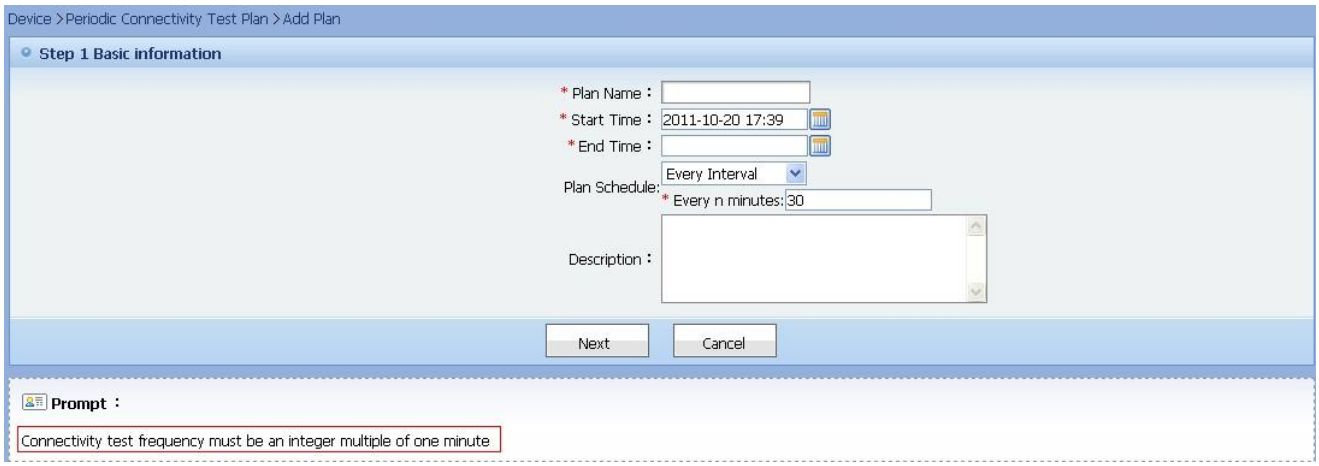


Figure 2.42. Step 1 of Add Plan (same as Modify Plan): Basic Info

2) Click **Next** on Add Plan - Basic Info page to enter Step 2 - **Select Device** page. On this page, you need to select devices on which connectivity test will be done in the plan. **Selected Devices List** is first shown on this page. Click **Select Device** to select devices in the prompted device list and add them to the **Selected Devices List**. Then click **Finish** to finish plan addition, as shown below:
3) Click **Previous** to go back to step 1 of Add Plan. Click **Finish** to finish plan addition.

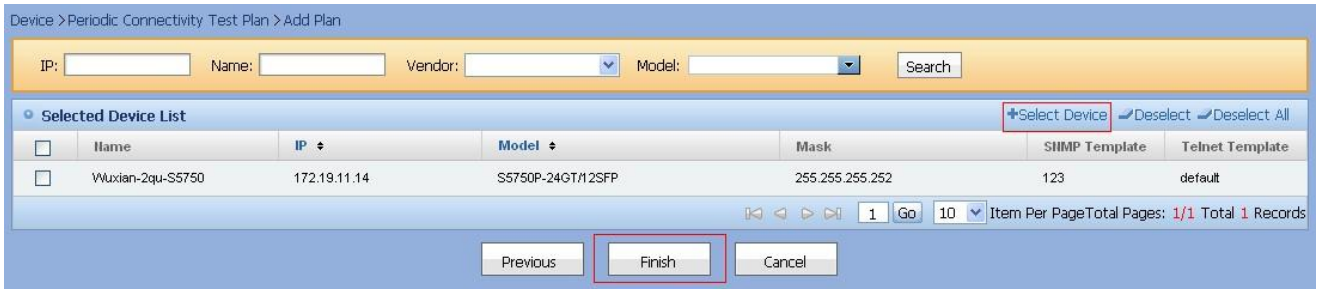


Figure 2.43. Step 1 of Add Plan: Select Device

Note

Frequency of connectivity tests must be an integer multiple of 1 minute.

Note

The status of newly added periodical connectivity test plan is “Disabled”. To change it to “Enabled”, see **Enable or Disable Auto Connectivity Test**.

3.2.5.1.2. Enable or Disable Auto Connectivity Test

The default status of newly added periodical connectivity test plan is “Disabled”. You can do “Enable” operation to enable it. (Only the enabled plan will run according to the set parameters.)

An enabled plan can be disabled by “Disable” operation.

Operation Steps

1) A “Disabled” plan can be enabled by clicking **Activate** in the operation column, as shown below:

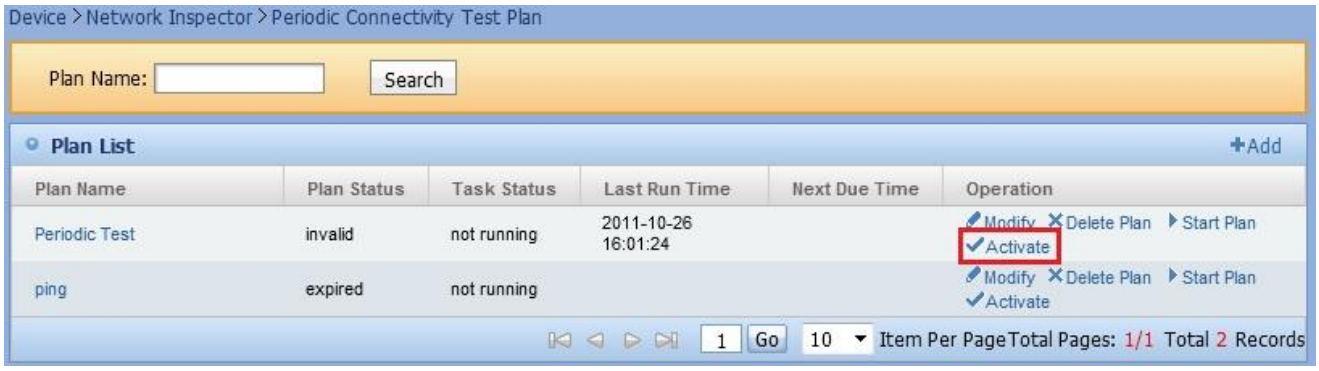


Figure 2.44. Enable Plan

An “Enabled” plan can be disabled by clicking **Disable** in the operation column, as shown below:

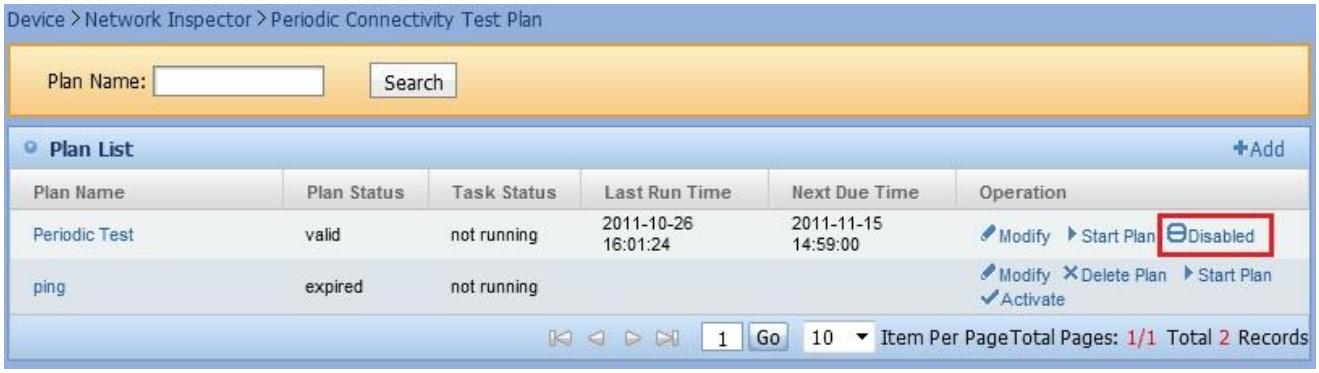


Figure 2.45. Disable Plan

3.2.5.1.3. Delete Auto Connectivity Test

Plans can be deleted in the plan list.

Operation Steps

1) Click **Delete Plan** in operation column of plan list, as shown below. The system prompts you to confirm the deletion. Click **OK** to finish the deletion.

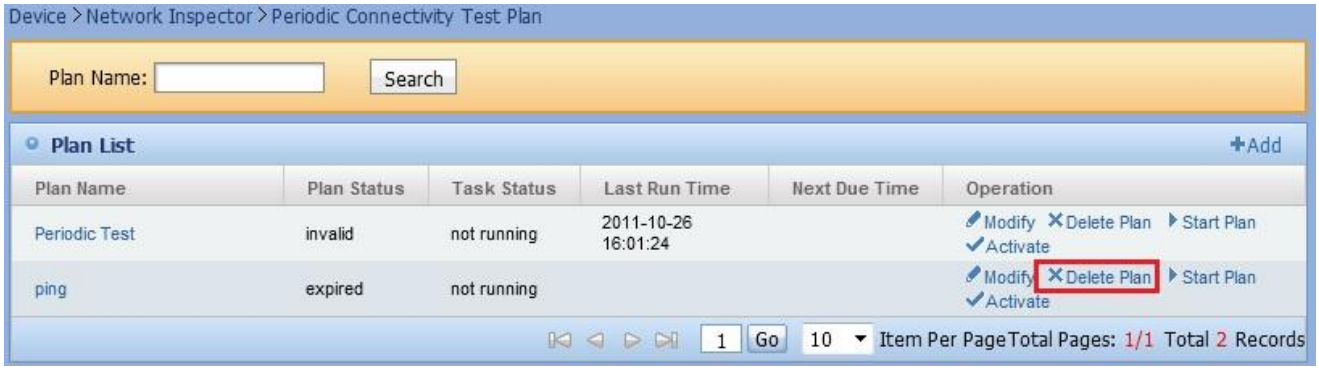


Figure 2.46. Delete Plan

Note

A plan can be deleted only when its status is “Disabled”. If its status is “Enabled”, please do “Disable Plan” (see **Enable or Disable Auto Connectivity Test** before deleting it.

2.2.5.2. Connectivity Test

In the system, manual connectivity test can be done to know real-time connection status of devices. Connectivity test result will be generated as a test report for download.

Operation Steps

1) Go to **Device** page, and click **Network Inspector** to enter **Network Inspector** page; click **Realtime Test** to enter **Realtime Connectivity Test** page, as shown below:

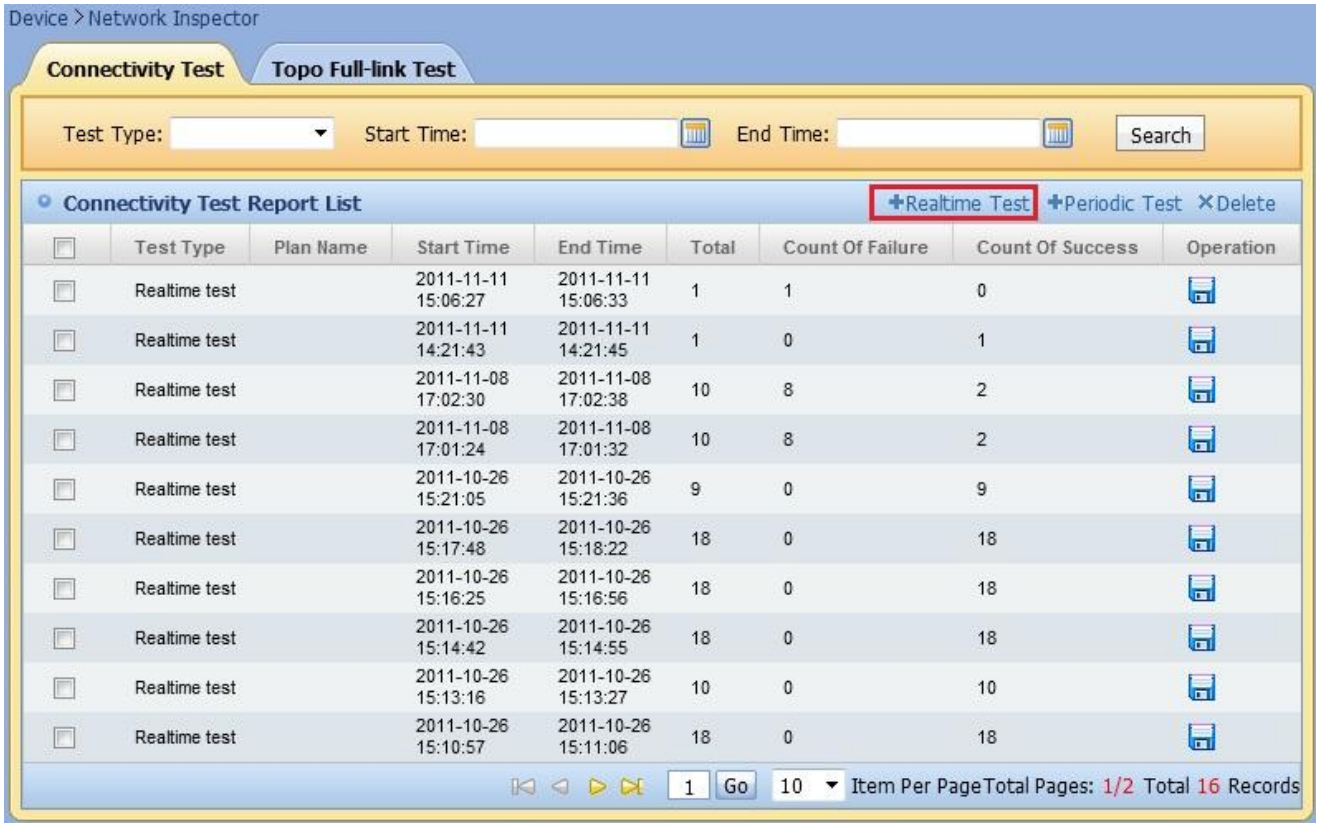


Figure 2.47. Enter Connectivity Test page

On **Connectivity Test** page, you can choose to conduct connectivity test on all devices by selecting **All Devices** for all devices. Select **Select Manually**, and then click **Select Device** to select devices if you want to conduct connectivity test on some devices, as shown below:

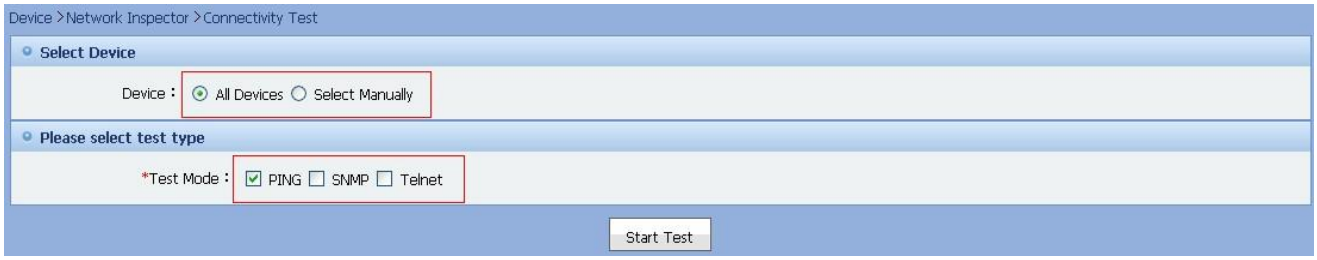


Figure 2.48. Connectivity Test Device Choose page - All Devices

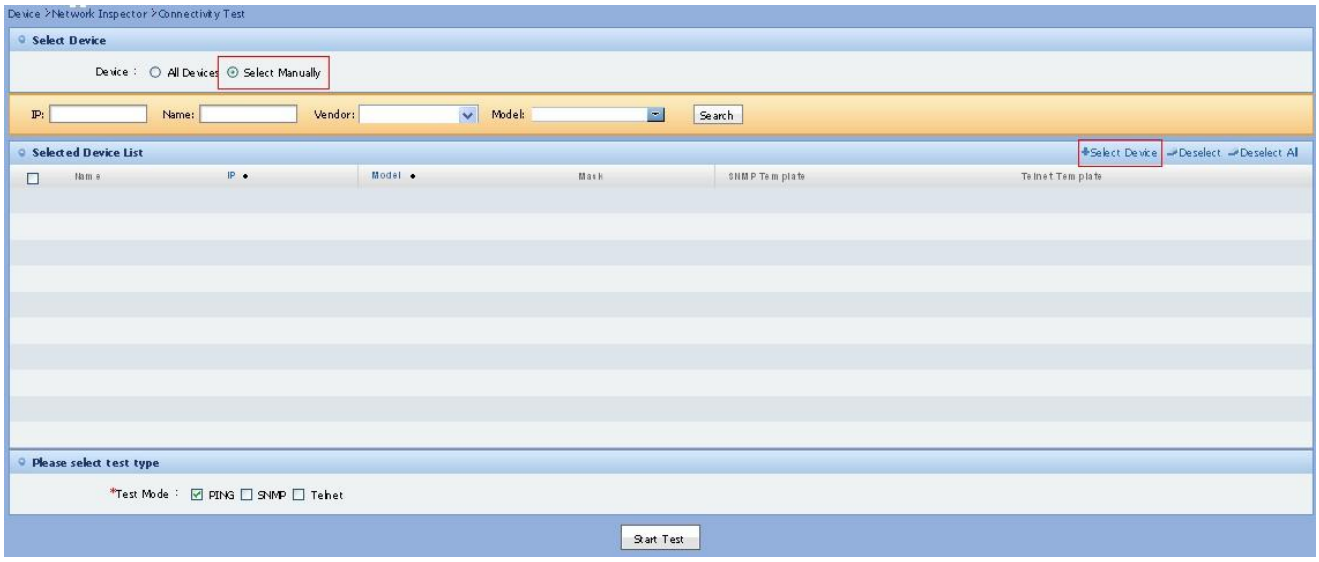


Figure 2.49. Connectivity Test Device Choose page - Choose Devices

The system will switch to Realtime Connectivity Test Log page after **Start Test** button is clicked.

On Realtime Connectivity Test Log page, test progress and results are shown dynamically. If a device is unreachable, it will be highlighted in red in the log.

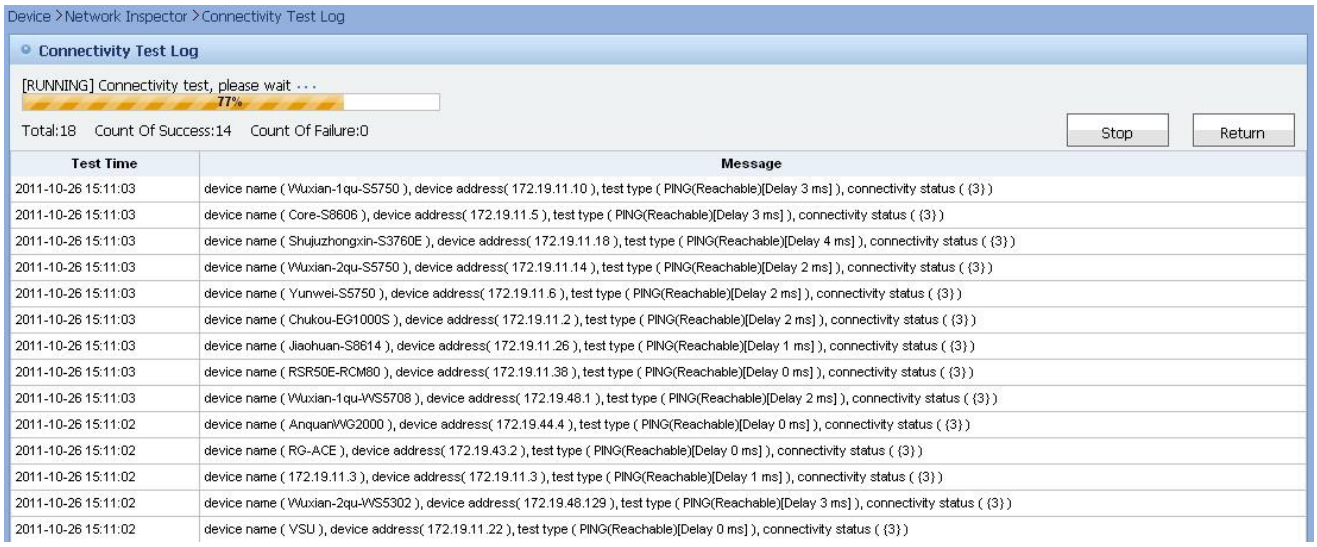


Figure 2.50. Realtime Connectivity Test Log page

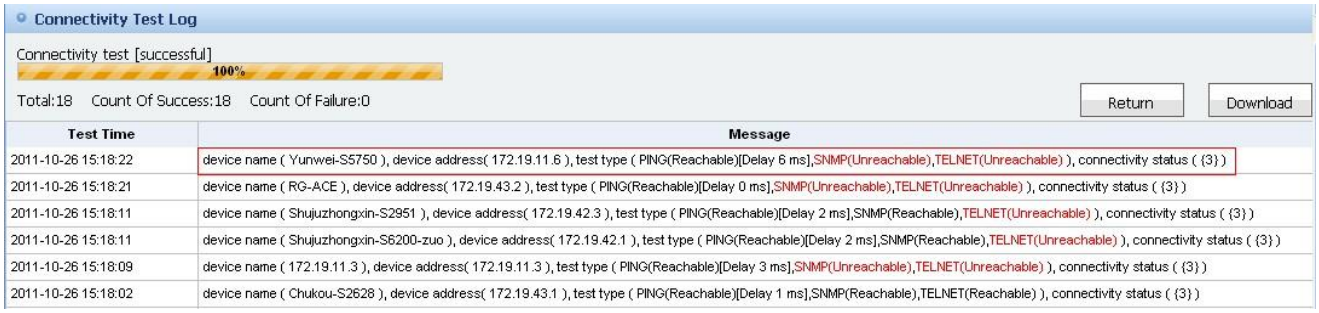


Figure 2.51. Realtime Connectivity Test Log page - Unreachable devices highlighted

Note

If the connectivity test is not conducted to all devices, at least one device should be selected. Otherwise, connectivity test cannot be run.

2.2.5.3. Test Report Download

After automatic periodical connectivity test or manual real-time connectivity test is done, the test result will be generated as a test report for download.

1) Go to **Device** page, and click **Download** button after the connectivity test is done to download the test report, as shown below:

Figure 2.52. Connectivity Test Result page

On **Connectivity Test Report Download** page, you can search for test reports according to test type (real-time or automatic periodical) and/or start/end time. The Save File dialog box will be prompted after you click **Download** in action column of the targeted report. Then you can save the report by clicking **Save**, as shown below:

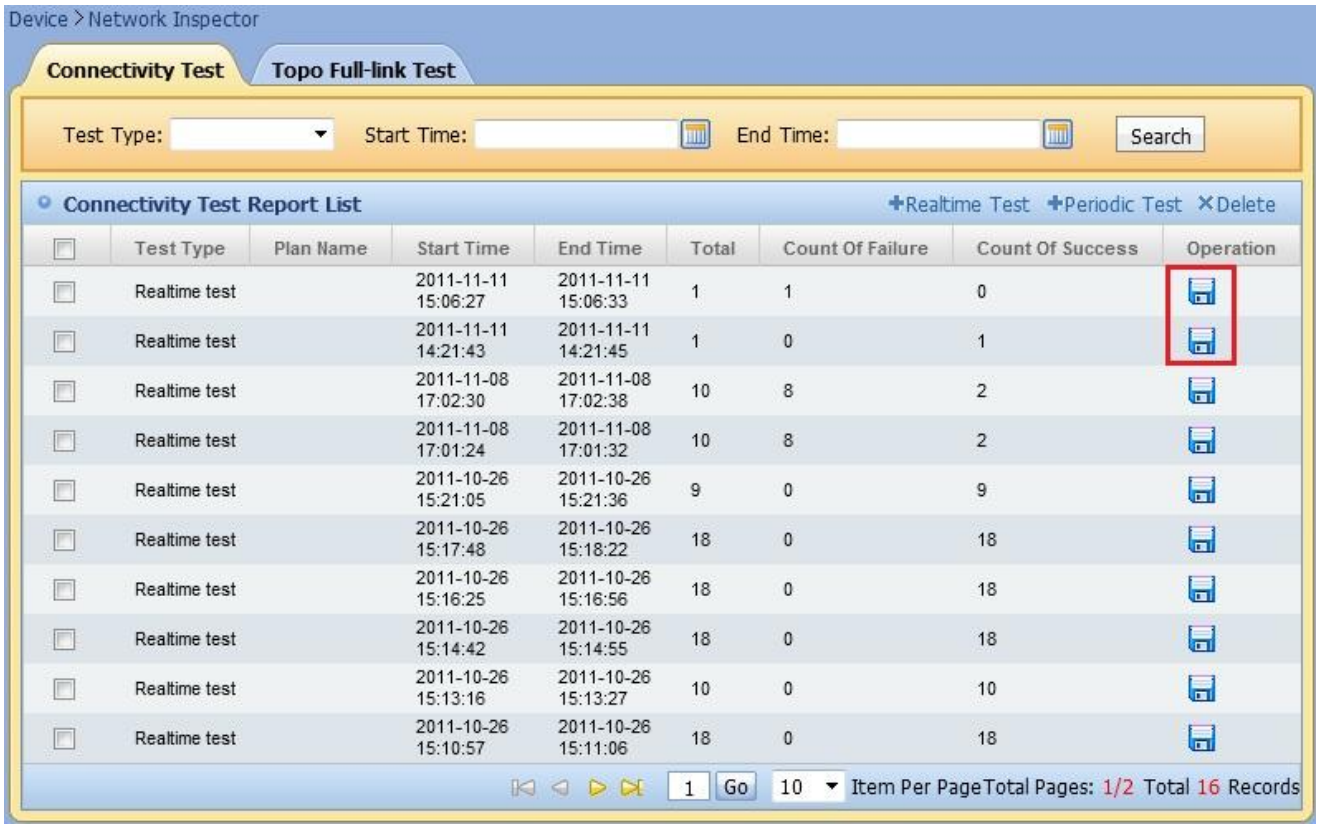


Figure 2.53. Connectivity Test Report Download page

2.3. Device Interface Management

This module describes device interface info user-friendly display, device interface basic operations and basic parameters modification.

- View Device Interface Panel
- View Interface Detail
- Enable or Disable Interface
- Enable or Disable PoE
- Set Interface Parameters
- Set Interface to Be Monitored or Not Monitored

2.3.1. View Device Interface Panel

Through this functionality, users can view the status of all interfaces on device panel intuitively.

1) On **Device Detail** page, device interface panel is shown automatically. Device interface status is indicated by colors. GREEN = Work Status UP;; RED = Work Status DOWN. When the mouse is on an interface icon, the basic info of the interface will be shown at a floating layer. The system will switch to detailed info page of the interface if it is clicked, as shown below:

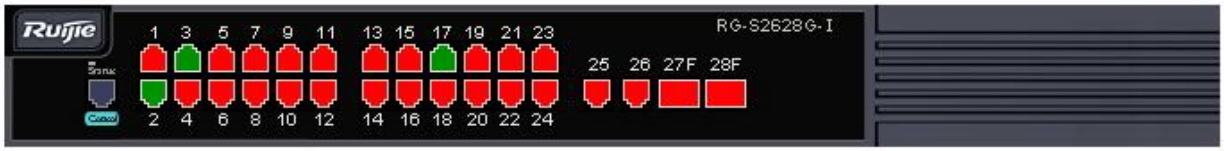


Figure 2.54. Real Device Panel

Logical panel will be shown as follows if the device model is not recognized in the system, or the real device panel is not available in the system yet:

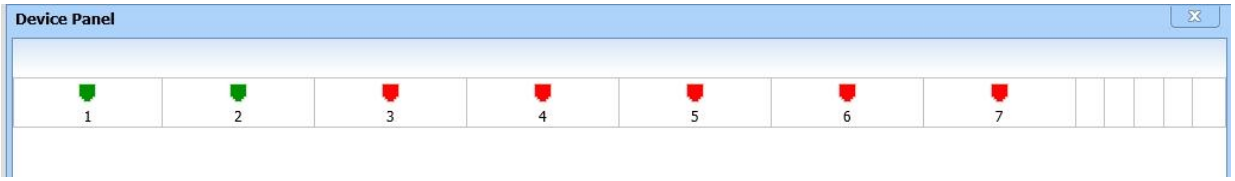


Figure 2.55. Logical Panel

2.3.2. View Interface Detail

Click the specified interface icon to enter the Detailed Interface Information page. (See **View Device Interface Panel**), then you can view the basic interface information and modify the interface settings.

Operation Steps

1) Click the specified interface icon to enter the Detailed Interface Information page

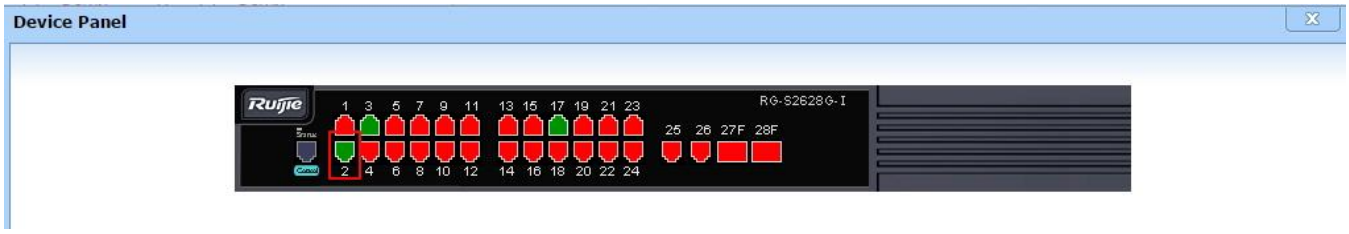


Figure 2.56. Device Interface Icon

Figure 2.57. Detailed Interface Information

You can perform the following operations on the Detailed interface Information page.

- Enable or Disable Interface
- Enable or Disable PoE
- Set Interface Parameters
- Set Interface to Be Monitored or Not Monitored

2.3.3. Enable or Disable Interface

Interface enable or disable operations can be performed on devices on device panel of Device Detail page and Device Interface Detail page.

Operation Steps on Device Detail page

1) Go to **Device Detail** page, and right-click an interface on device panel. Click **Enable interface** to enable the interface if it is disabled or **Disable interface** to disable the interface if it is enabled. The **Device Detail** page will be refreshed afterwards, as shown below:

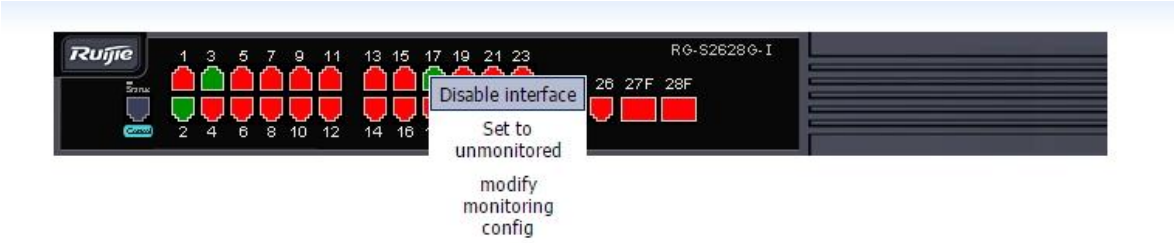


Figure 2.58. Disable the Interface

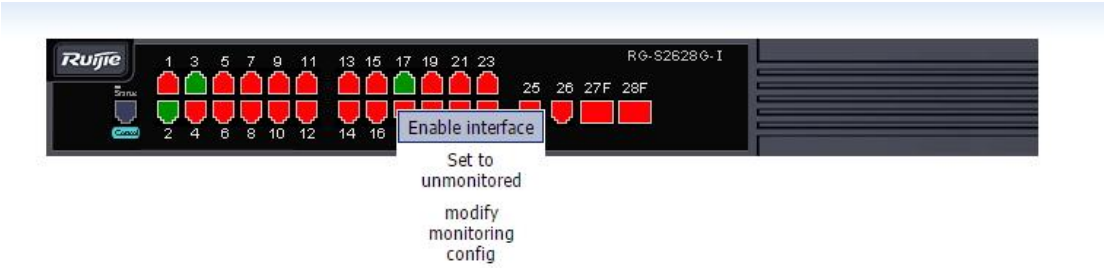


Figure 2.59. Enable the Interface

Operation Steps on Device Interface Detail page

1) Go to **Device Interface Detail** page. Click **Open Port** to enable the interface if it is disabled or **Close Port** to disable the interface if it is enabled. The **Device Interface Detail** page will be refreshed afterwards, as shown below:

Figure 2.60. Enable the Interface

Figure 2.61. Disable the Interface

Note

The function is implemented through SNMP (read and write rfc1213 interface mib). If it fails, please check if SNMP read and write permission is correctly configured in the SNMP template.

Note

Only one of “Open Port” and “Close Port” link will be available at the same time.

2.3.4. Enable or Disable PoE

This function describes how to enable and disable PoE on the Device Detail and Detailed Interface Information pages .

Operation Steps on the Device Detail Page

1) Go to the **Device Detail** page, and right-click an interface on device panel. Click **Enable PoE** to enable PoE for the interface if the interface PoE status is disabled (or click **Disable PoE** to disable PoE for the interface if the interface PoE status is enabled). The **Device Detail** page will be refreshed afterwards, as shown below:

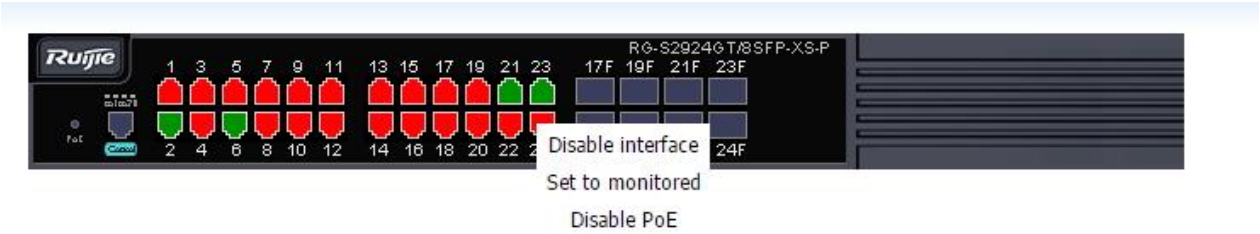


Figure 2.62. Disable PoE

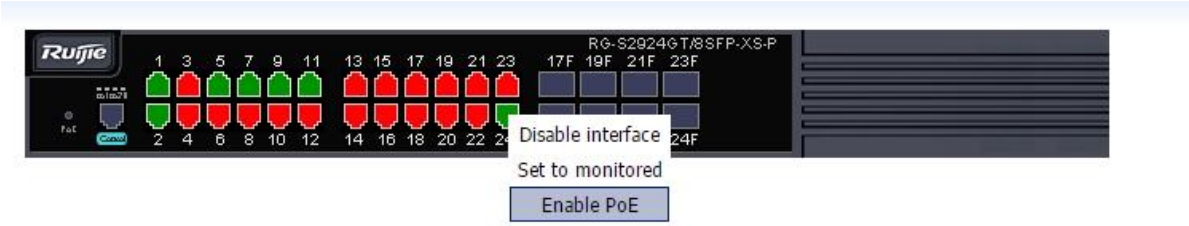


Figure 2.63. Enable PoE

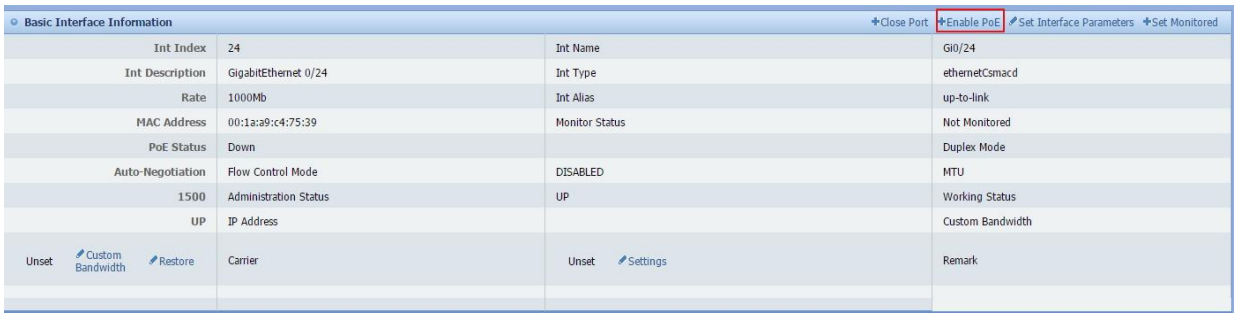
Operation Steps on the Detailed Interface Information Page

1) Go to the Detailed Interface Information page, and click **Enable PoE** to enable PoE for the interface if the interface PoE status is disabled (or click **Disable PoE** to disable PoE for the interface if the interface PoE status is enabled). The Detailed Interface Information page will be refreshed afterwards, as shown below:

Basic Interface Information | Close Port | Disable PoE | Set Interface Parameters | Set Monitored

Int Index	23	Int Name	Gi0/23
Int Description	GigabitEthernet 0/23	Int Type	ethernetCsmacd
Rate	1000Mb	Int Alias	
MAC Address	00:1a:a9:c4:75:39	Monitor Status	Not Monitored
PoE Status	Up		Duplex Mode
Auto-Negotiation	Flow Control Mode	DISABLED	MTU
1500	Administration Status	UP	Working Status
DOWN	IP Address		Custom Bandwidth
Unset Custom Bandwidth Restore	Carrier	Unset Settings	Remark

Figure 2.64. Disable PoE



Basic Interface Information | Close Port | Enable PoE | Set Interface Parameters | Set Monitored

Int Index	24	Int Name	Gi0/24
Int Description	GigabitEthernet 0/24	Int Type	ethernetCsmacd
Rate	1000Mb	Int Alias	up-to-link
MAC Address	00:1a:a9:c4:75:39	Monitor Status	Not Monitored
PoE Status	Down		Duplex Mode
Auto-Negotiation	Flow Control Mode	DISABLED	MTU
1500	Administration Status	UP	Working Status
UP	IP Address		Custom Bandwidth
Unset Custom Bandwidth Restore	Carrier	Unset Settings	Remark

Figure 2.65. Enable PoE

Note

This function is implemented through SNMP (Read-write POWER-ETHERNET-MIB pethPsePortTable mib). If it fails, please check whether the read-write permission is correctly configured in the SNMP template.

2.3.5. Set Interface Parameters

In the system, basic interface parameters can be set on individual interface: duplex mode, rate, flow control mode.

Operation Steps

1) Go to **Detailed Interface Information** page, and click **Set Interface Parameters** link to switch to **Set Interface Parameters** page, as shown below:

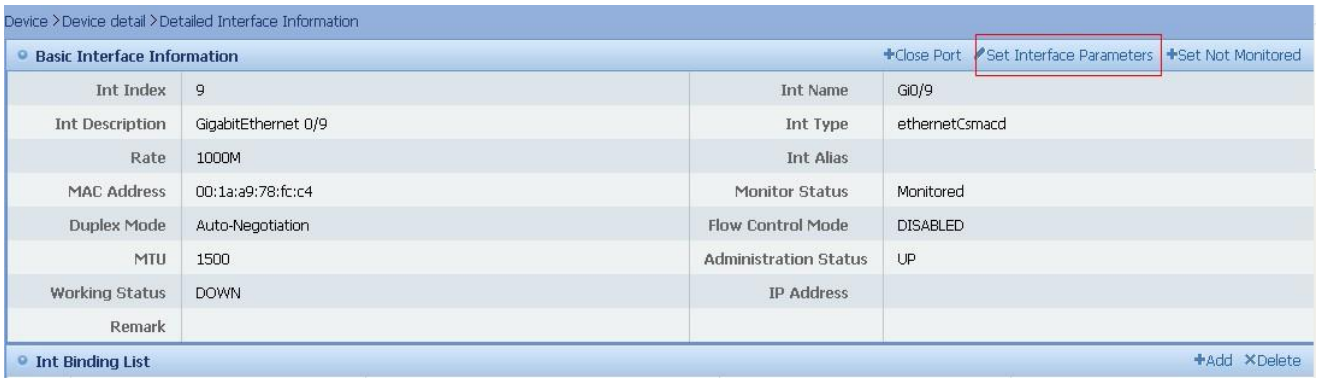


Figure 2.66. Set Interface Parameters link

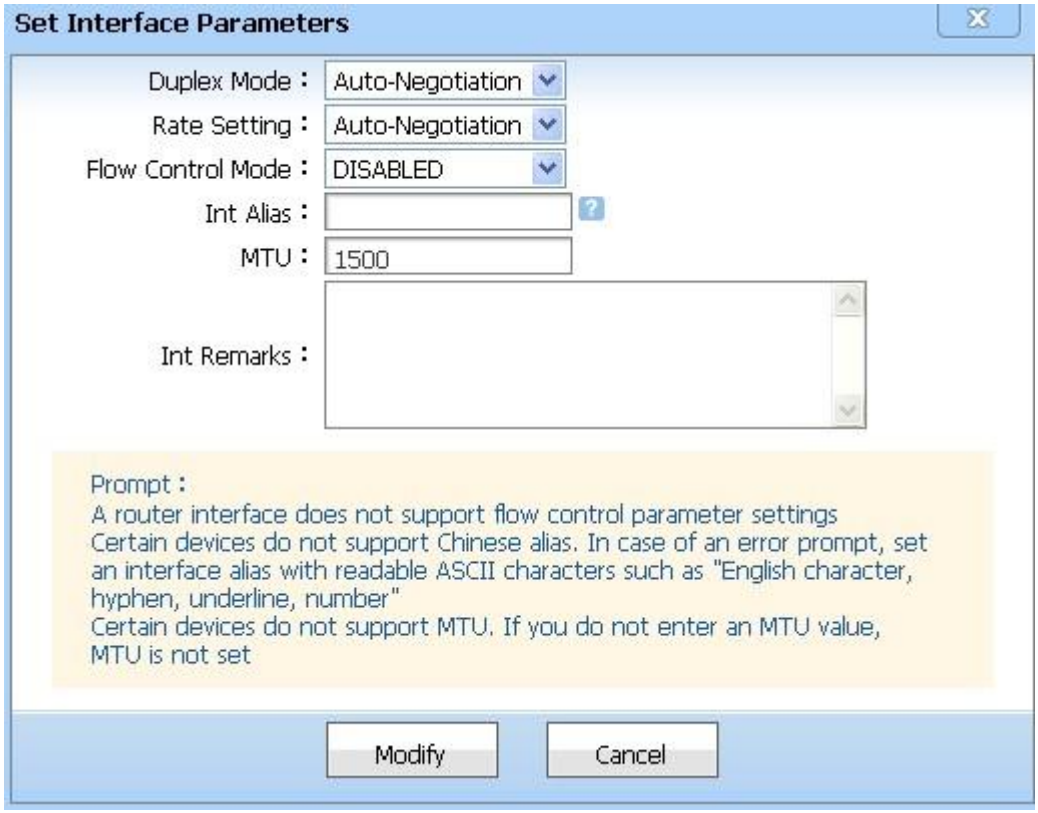


Figure 2.67. Set Interface Parameters page

2) On **Set Interface Parameters** page, you can choose values of duplex mode, rate and flow control mode from the drop-down boxes. Then, click **Modify**, and the system will prompt successful modification.

Note

If the chosen value is not supported by the device, the setting will fail. For example, the setting will fail if the rate is set to be 10Gbps while the supported max rate of the interface is 100Mbps.

Note

Interface notes can be set in the system even when device is not connected, as interface notes are not synced to the device.

2.3.6. Set Interface to Be Monitored or Not Monitored

Interfaces can be set to be “Monitored” or “Not Monitored”. When an interface is in “Not Monitored” state, the system will ignore its Trap events and will not collect its performance info. When an interface is in “Monitored” state, the system will handle its Trap events (probably upgrade them to alarms). The system will also collect performance info of the interface if the device of the interface has been added to performance monitoring (see **Monitored device management**).

In the system, you can do “Set Interface to Be Monitored or Not Monitored” operation to a single interface or to interfaces in batches.

Operation Steps of Single Interface Setting - Device Detail page

1) Go to **Device Detail** page, and right-click an interface on device panel. Click **Set to monitored** or **Set to unmonitored** menu based on the fact that the interface is in Not Monitored state or Monitored state. The system will monitor or not monitor the interface, and **Device Detail** page will be refreshed, as shown below:

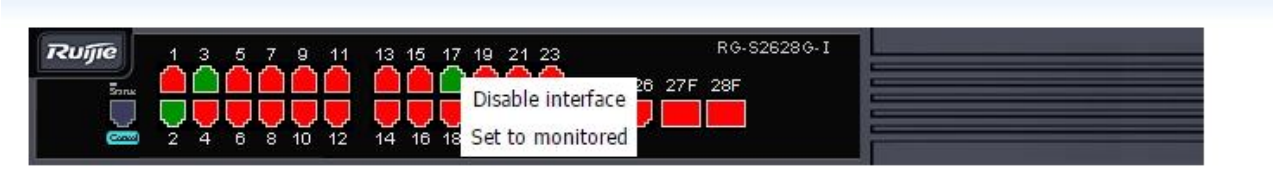


Figure 2.68. Set to Be Monitored

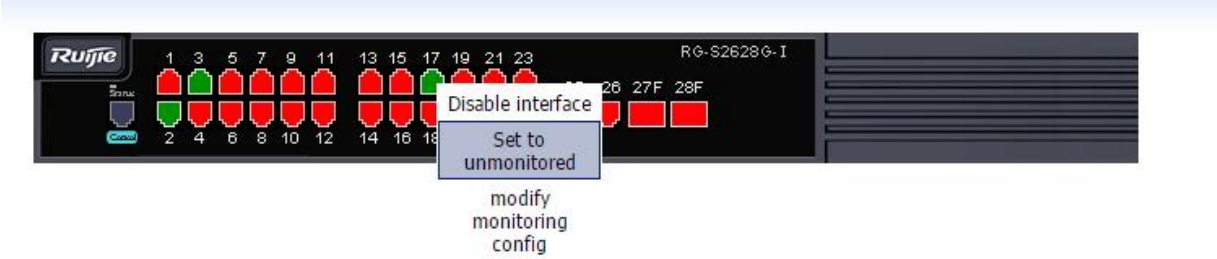


Figure 2.69. Set to Be Not Monitored

Operation Steps of Single Interface Setting - Device Interface Detail page

1) Go to **Detailed Interface Information** page, and click **Set Monitored** or **Set Not Monitored** link based on the fact that the interface is in Not Monitored state or Monitored state. The system will monitor or not monitor the interface, and **Device Detail** page will be refreshed, as shown below:

Figure 2.70. Set to Be Monitored link

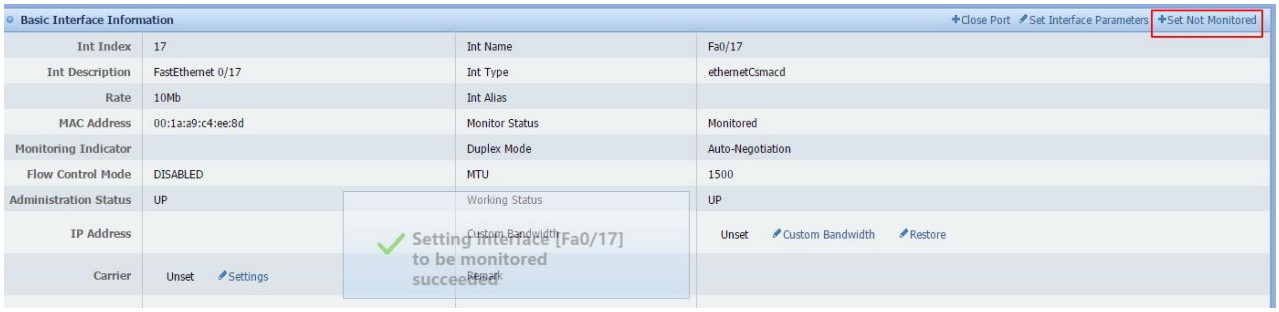


Figure 2.71. Set to Be Not Monitored link

Operation Steps of Interfaces Batch Setting

1) On **Device Detail** page, go to **Configure Device** > **Int Batch Setting**. The system will switch to **Interface Batch Setting** page. On this page, choose interfaces in batches, and then click **Set Monitored** or **Set Not Monitored** to set the states of chosen interfaces. Click **Return** to go back to **Device Detail** page, as shown below:

Figure 2.72. Device Interfaces Batch Setting link

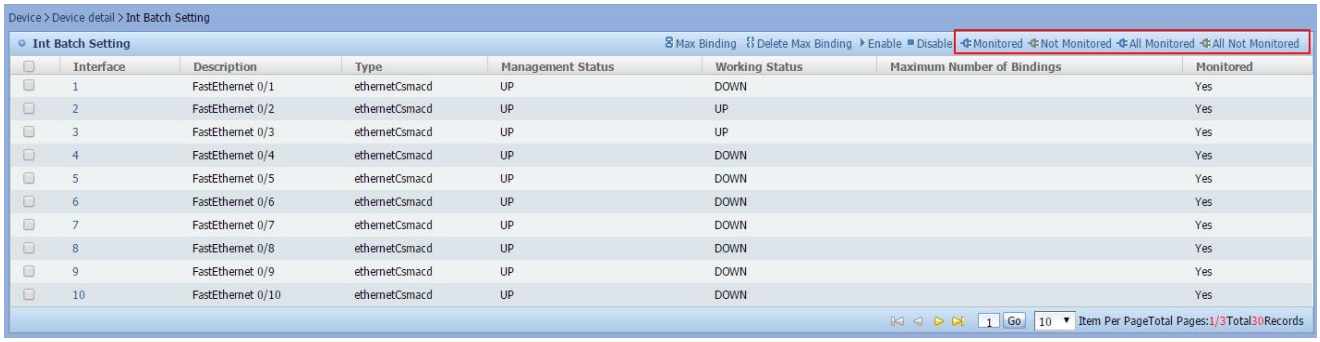


Figure 2.73. Device Interfaces Batch Setting page

Note

Only one of “Set Monitored” and “Set Not Monitored” links is shown on Interface Detail page at the same time.

2.4. Device Parameter Management

This module describes functionalities about SNMP and Telnet templates.

- SNMP Template Configuration
- Telnet Template Configuration

2.4.1. SNMP Template Configuration

In networks with high security level, different SNMP parameters are used for devices in different areas. Normally several devices are set to be in one group and one set of parameters are used in the group. When network management software is used to do SNMP operations on these devices, its parameters must be consistent with those configured on the devices. To deal with this case, the system uses templates to associate devices and parameters. Thus, setting parameters on every device is avoided.

Operation Steps

1) On **Device**, click **Template Management**, and then click **SNMP Template** tab.

Figure 2.74-2.75. Template Configuration

Add SNMP Template

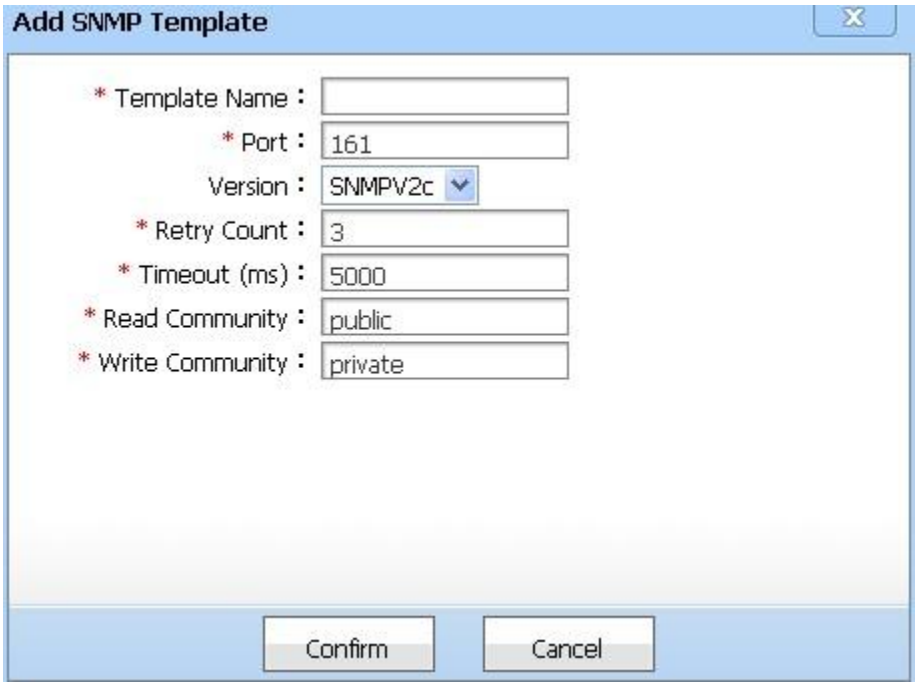


Figure 2.76. Add V2c Template

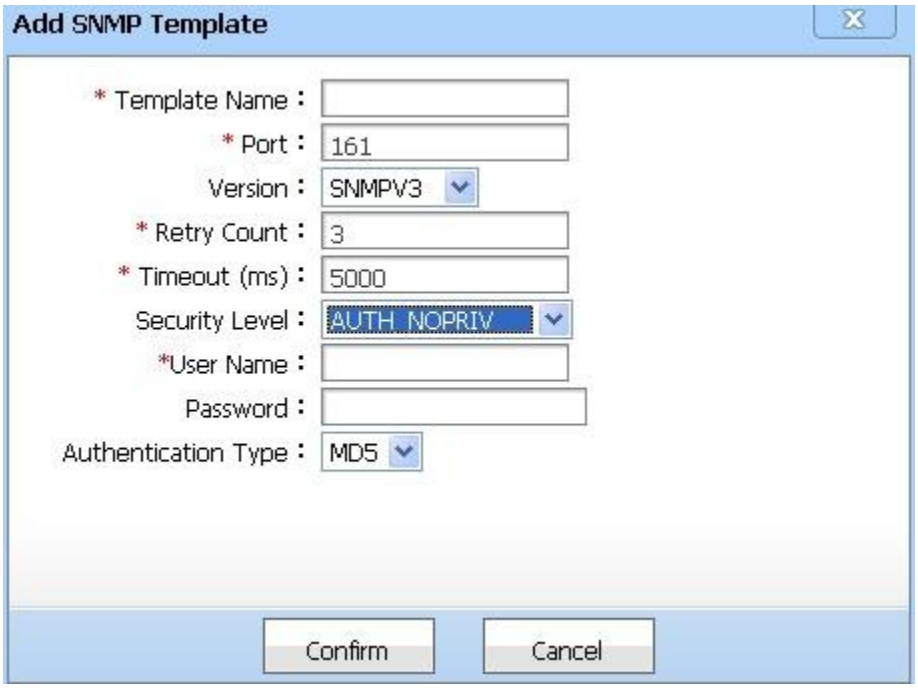


Figure 2.77. Add V3 Template

Admin can delete SNMP templates. The system comes with 3 SNMP templates. Admin can view and modify these templates, but cannot delete them.

Super administrator can associate devices with SNMP template. One device can only be associated with one SNMP template. If the associated template of a device is deleted, the device will be associated with the default template. SNMP operations on device use the parameters defined in its associated SNMP template.

Figure 2.78. Associate SNMP Template with Devices

By default, the system uses SNMPv2c template that comes with the system as default template. Super administrator can set other templates come with the system, i.e. SNMPv1 template and SNMPv3 template, to be default template. There can only be one default template at a time.

Figure 2.79. Set Default Template

Note Communication process using SNMP V3 is relatively slower than those using V2c or V1.

Note The configuration of SNMP V3 protocol must match that on devices. Otherwise, the system can neither access devices through SNMP V3 protocol, or receive or handle Trap info from devices correctly.

Note The following CLI command allows SNMP V3 administrator to set and view management parameters of node MIB-2(1.3.6.1.2.1) by using username v3user in authentication+encryption mode. Authentication mode is MD5, and authentication password is MD5-Auth. It uses DES Encryption, and encryption key is DES-Priv. At the same time, sending Trap messages with SNMP V3 format to 192.168.65.199 is allowed. The user to send Trap messages is v3 user. Trap messages are sent in authentication+encryption mode. Authentication mode is MD5, and authentication password is MD5-Auth. It uses DES Encryption, and encryption key is DES-Priv.

```
Ruijie#config
Ruijie(config)# snmp-server view v3userview 1.3.6.1.2.1
Ruijie(config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
Ruijie(config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56 des-priv
Ruijie(config)#snmp-server host 192.168.65.199 traps version 3 priv v3user
Ruijie(config)#end
Ruijie#write
```

2.4.2. Telnet Template Configuration

In networks with high security level, different Telnet connection parameters are used for devices in different areas. Normally several devices are set to be in one group and one set of parameters are used in the group. When network management software is used to do Telnet operations on these devices, its parameters must be consistent with those configured on the devices. To deal with this case, the system uses templates to associate devices and parameters. Thus, setting parameters on every device is avoided.

Out-of-band management indicates that a device only can be connected by serial port at the first time it is used. After configuration, network devices can be connected and managed by Telnet virtual terminal. Command lines can be used in both ways. The Telnet management mode here only indicates Telnet virtual terminal mode.

Operation Steps

1) On **Device**, click **Template Management**, and then click **Telnet Template** tab.

Figure 2.80. Telnet Template

The system comes with a Telnet template. Users can view and modify this template, but cannot delete it. Super administrator can add, delete, modify and view self-defined Telnet templates.
Administrator can add self-defined Telnet template.

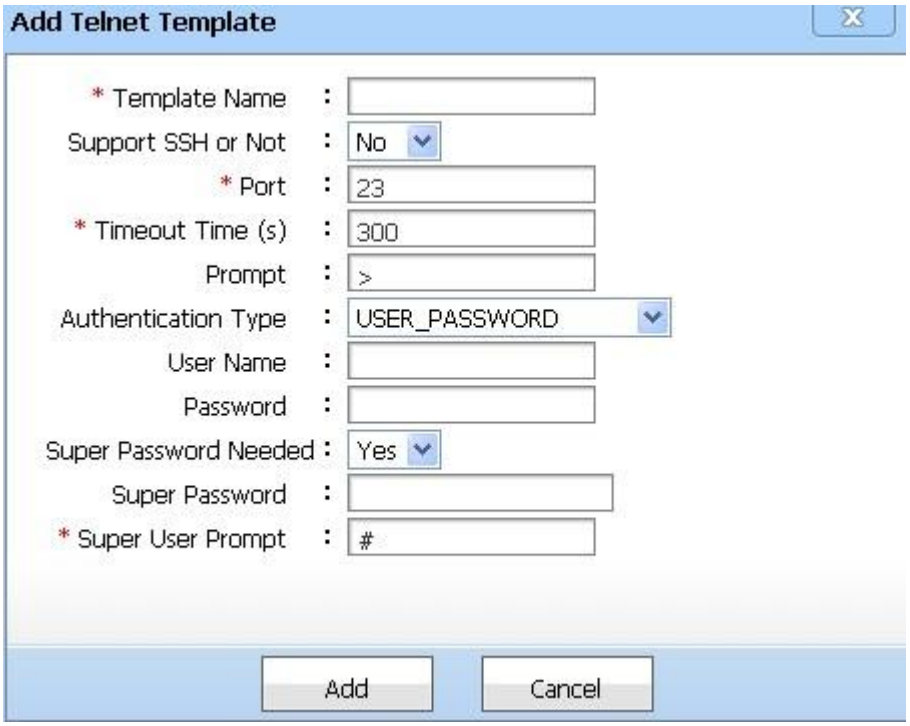


Figure 2.81-2.82. Add Telnet Template

SSH access is supported in Telnet template. After selecting SSH support, please select SSH version (V1 or V2) and port number (default 22). There are three authentication modes: 1. password only; 2. username and password; 3. no username or password, with Telnet prompt displayed directly.

1. Password Only

Figure 2.83. ONLY_PASSWORD

2. Username and Password

Figure 2.84. USER_PASSWORD

3. No username or password, with Telnet prompt displayed directly

Figure 2.85. NOUSER_NOPASSWORD

Administrator can modify Telnet templates, and delete self-defined Telnet template.
Super administrator can associate devices with Telnet template. Each device can be associated with one TELNET template only. If the associated template of a device is deleted, the device will be associated with Telnet template coming with the system.

Figure 2.86. Associate Telnet Template

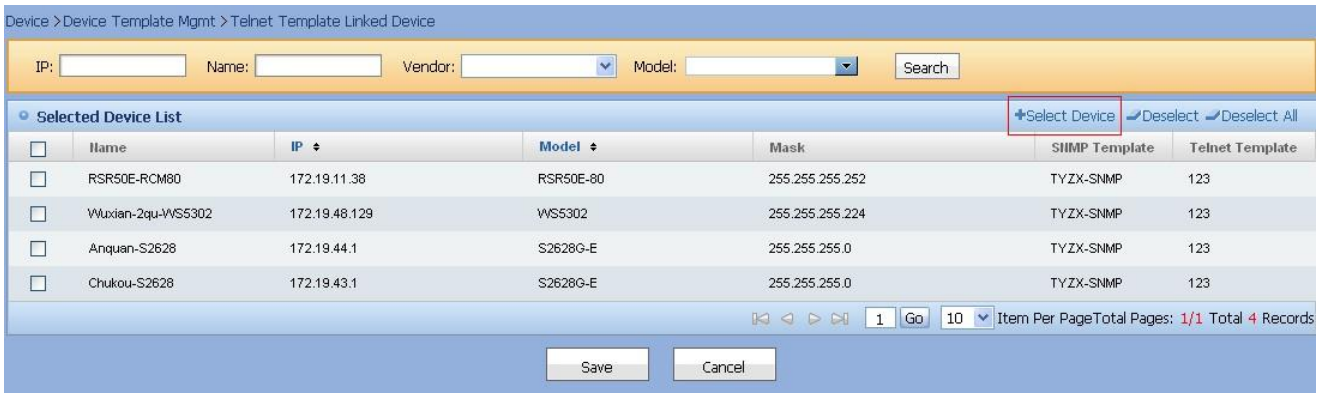


Figure 2.87. Associate Telnet Template - Associate Device List

Note When operations (e.g. software distribution, upload, config) are performed by Telnet protocol, the parameters in the device-associated Telnet template will be used. But they will not be used when these operations are performed by logging in to the device by Telnet commands directly.

Note The system does not support operating devices through SSH.

Note Telnet CLI mode is required for operations such as device config backup, device software distribution, VLAN config, IP/MAC/port binding, interface traffic control, duplex, and rate setting.

Note The execution time of the time-consuming device software distribution operation may be longer than 5 minutes. Please set proper timeout according to devices.

Note Before using SSH2, please set the maximum number of Telnet terminals to be greater than 10. For Ruijie devices, input line vty 0 20 in config mode.

2.5. Terminal Management

This module includes terminal info addition, deletion, modification and search, binding and unbinding to switch port, and IP/MAC abnormity detection.

- View Terminal Info
- Add Terminal
- Modify Terminal Info
- Delete Terminal
- Import or Export Terminal Info
- Terminal Binding/Unbinding
- IP/MAC Collision Detection
- Subnet Usage Statistics

2.5.1. View Terminal Info

By Viewing terminal info, users can know PC, host, wireless STA and their online info of the system. The info includes IP, MAC, computer name, uplink device IP, device interface, contact and remarks.

Operation Steps

1) On **Device** page, click **Terminal List** on the left menu.

Figure 2.88. Enter Terminal Management page

Choose a terminal info column to view terminal name, type, source, IP, MAC, uplink device IP, binding status, online user, and online time, as shown below:

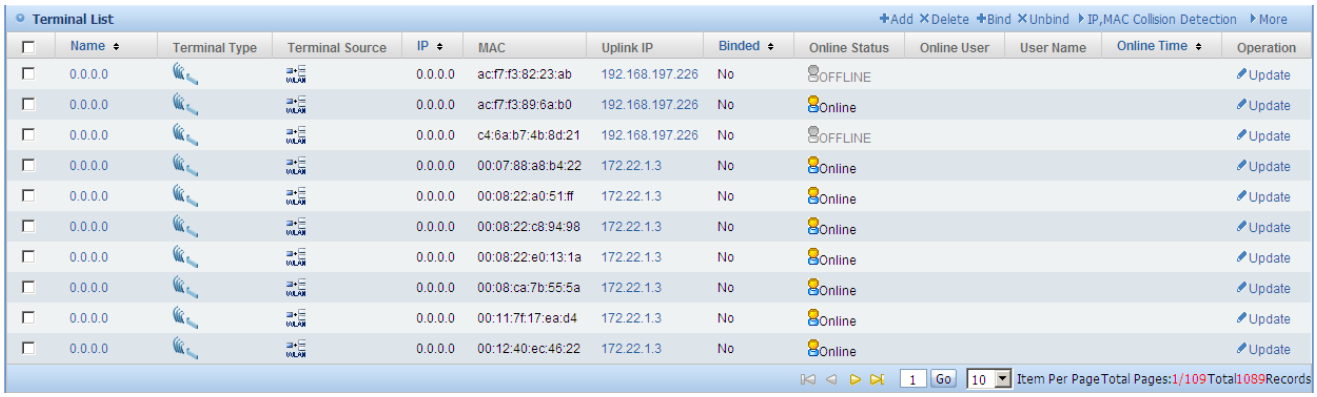


Figure 2.89. View Terminal Info List page

Click terminal name link to view terminal detail, as shown below:

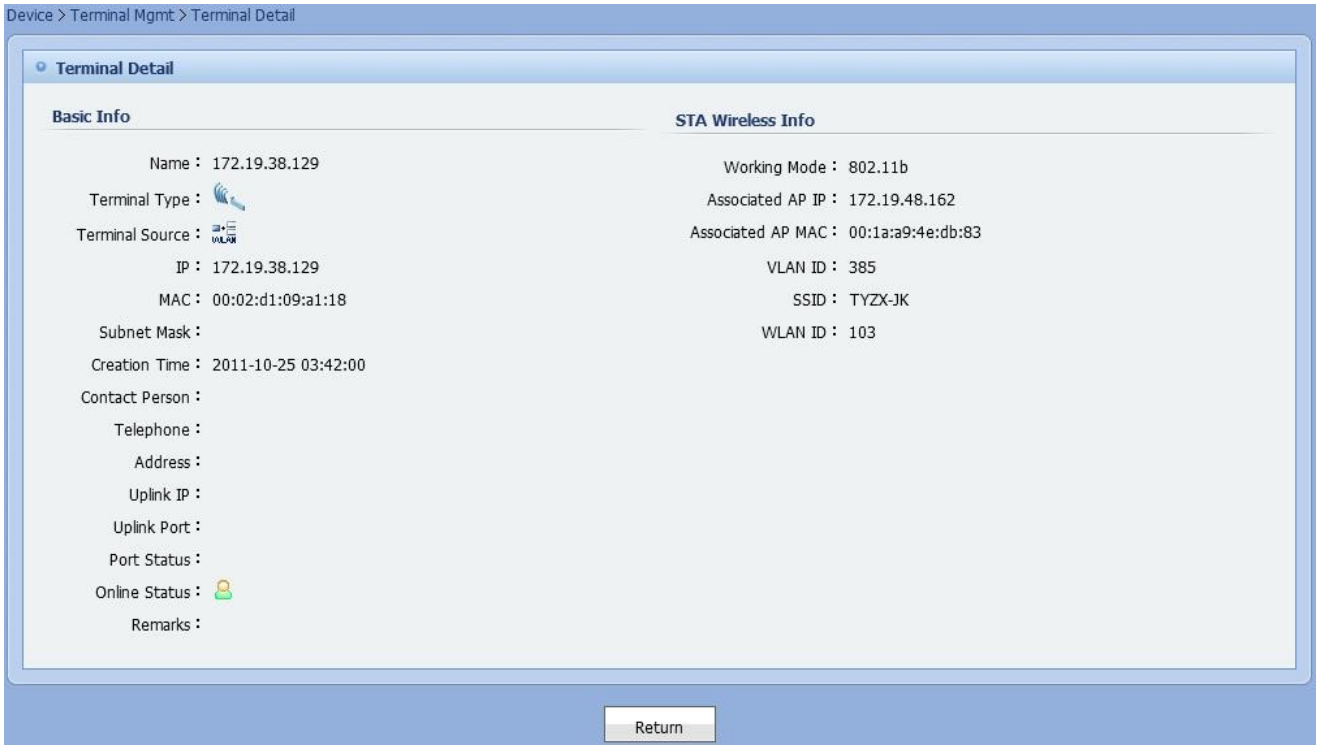


Figure 2.90. View Terminal Info page

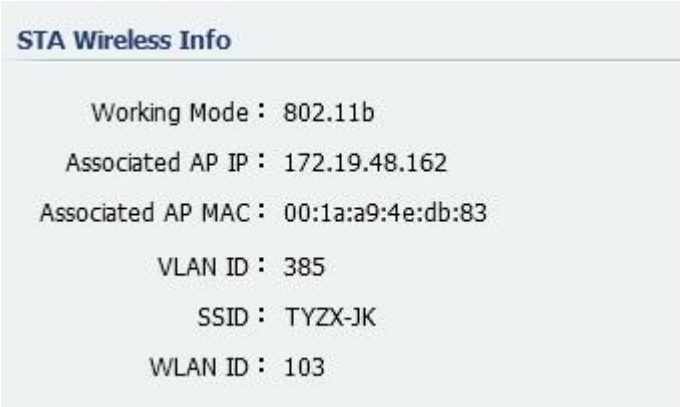


Figure 2.91. View Terminal Info page - STA Info

Figure 2.92. View Terminal Info page - Host Port Detection

Figure 2.93. View Terminal Info page - Terminal Operation

On **View Terminal** page, click **Return** to go back to **Terminal List** page.

2.5.2. Add Terminal

Users can add terminals manually.

Operation Steps

1) On **Terminal Info List** page, click **Add** to enter Add Terminal page.
On **Add Terminal** page, input terminal info, and then click **Add** to save terminal info, as shown below:

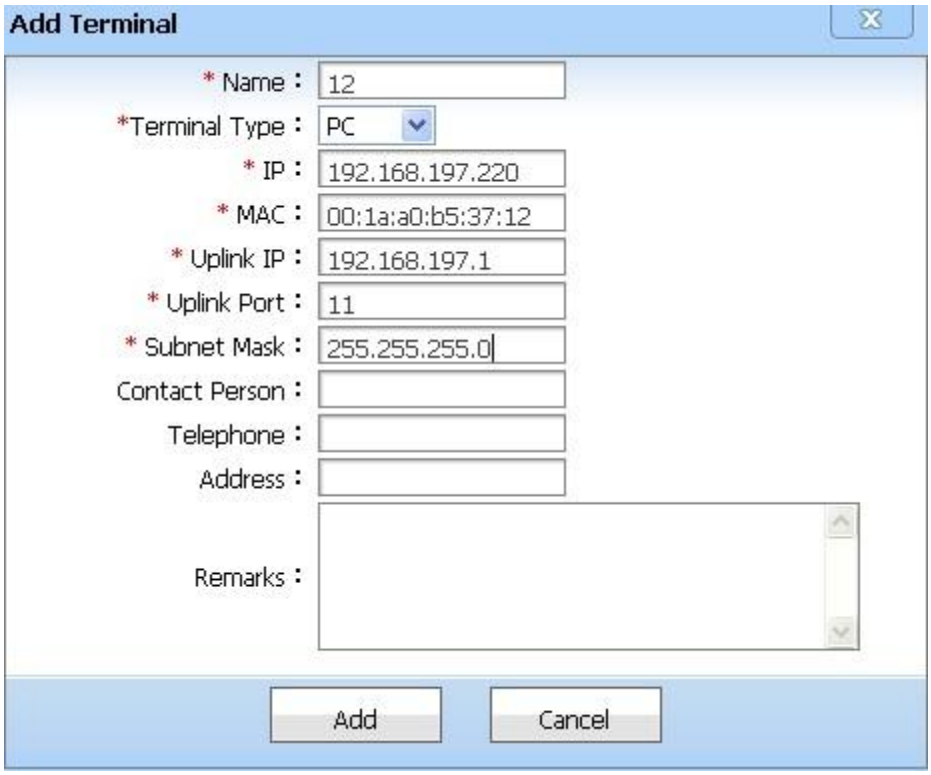


Figure 2.94. Add Terminal Info page

On **Add Terminal** page, and click **Cancel** to return to **Terminal List** page. In this case, the system saves no information.

Note

Please go to **Network Topology** module to discover Layer 2 devices via Layer 2 topology discovery before adding terminals.

Note

Adding a terminal manually is necessary only when a terminal is not discovered by Layer 2 topology discovery. Terminals whose IP or MAC already exist in the system cannot be added manually.

Note

To add a terminal, the subnet to which the terminal belongs, uplink device IP address and interface must be input.

2.5.3. Modify Terminal Info

Users can modify the name, contact, position, remarks and other info of terminals.

Operation Steps

1) On terminal info list page, click **Update** icon.

On **Modify Terminal** page, input necessary info, and click **Update** to save, as shown below:

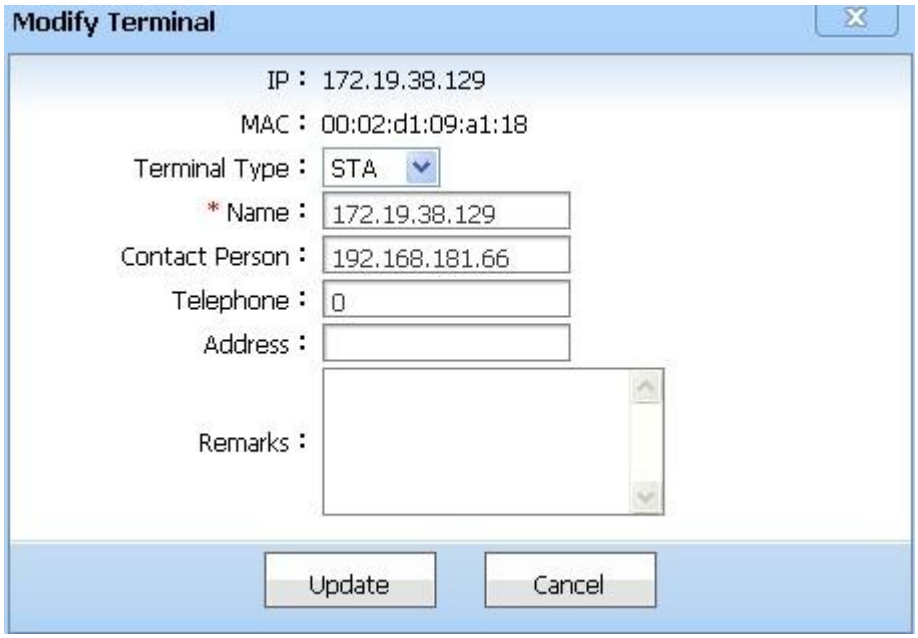


Figure 2.95. Modify Terminal Info page

2.5.4. Delete Terminal

Users can manually delete terminal info.

Operation Steps

1) On **Terminal List** page, choose terminals, and then click **Delete**.

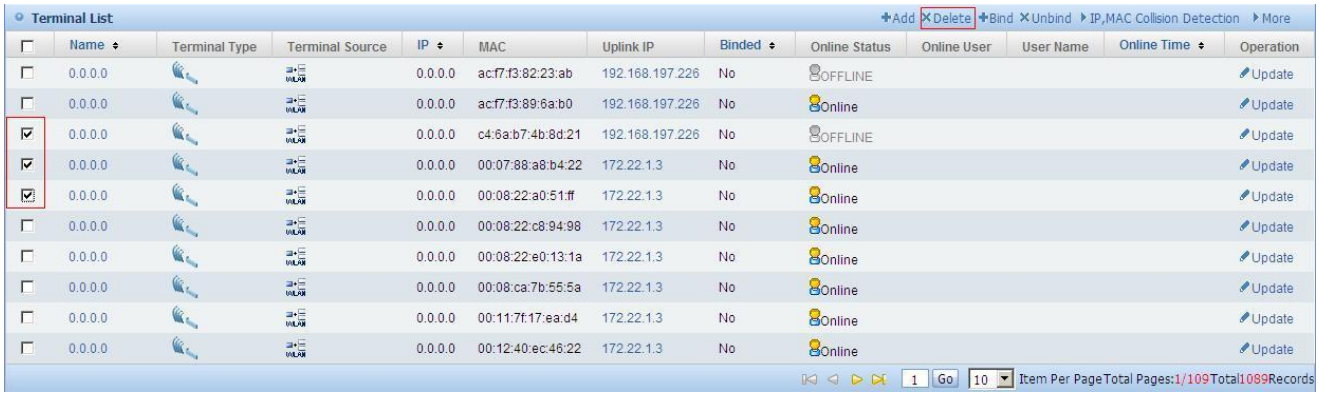


Figure 2.96. Choose Delete Terminal page

The system will display the confirmation box. Click **Confirm** to confirm the deletion.
The system will return to terminal info list page after the deletion is confirmed.

Note Corresponding Layer 2 topology terminal node will be deleted after terminal deletion.

2.5.5. Import or Export Terminal Info

Users can import terminals complying with rules based on terminal import template. Terminal info can be exported into EXCEL files.

Operation Steps

1) On **Terminal List** page, click **Import**.

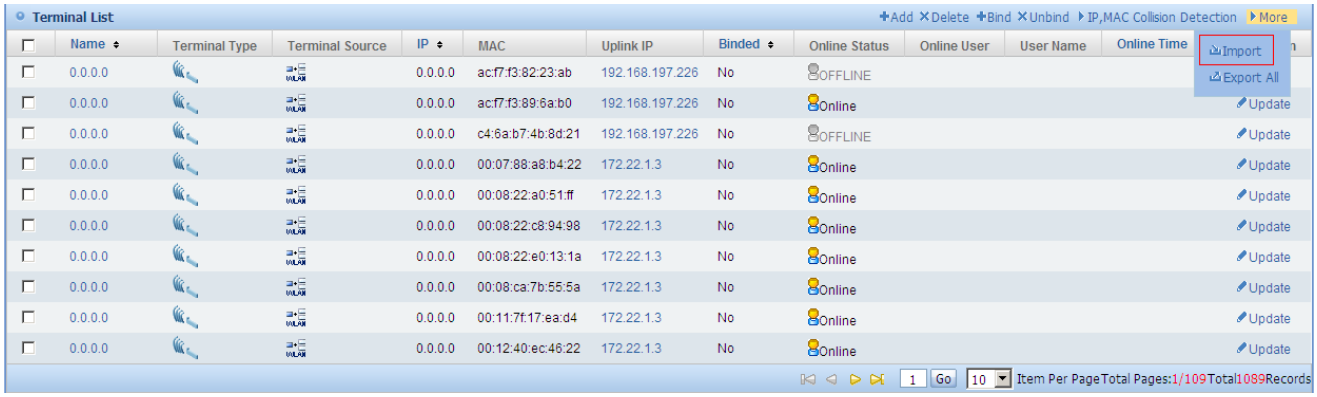


Figure 2.97. Enter Terminal Import page

The system will switch to **Terminal Import** page. Click **Select Imported File** to choose EXCEL file to import, and then click **Upload** button to make the system do terminal import.

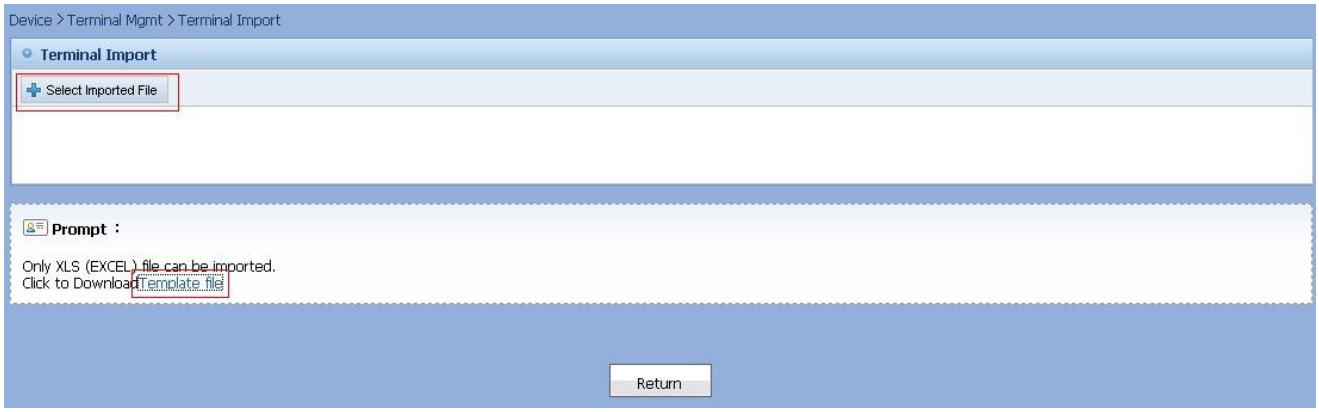


Figure 2.98. Terminal Import page

The system will switch to **Terminal Import Log** page to show the importing status.

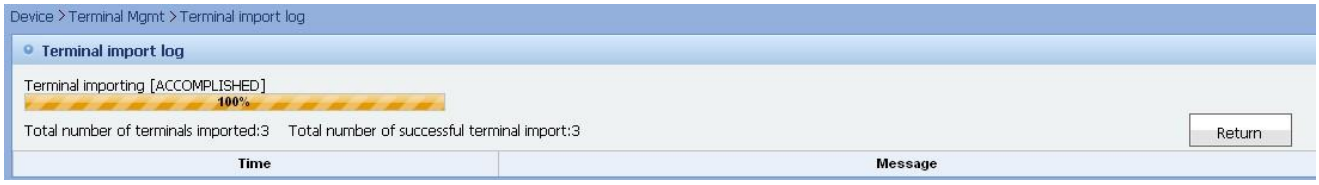


Figure 2.99. Terminal Import Log page

On **Terminal List** page, click **Export**.

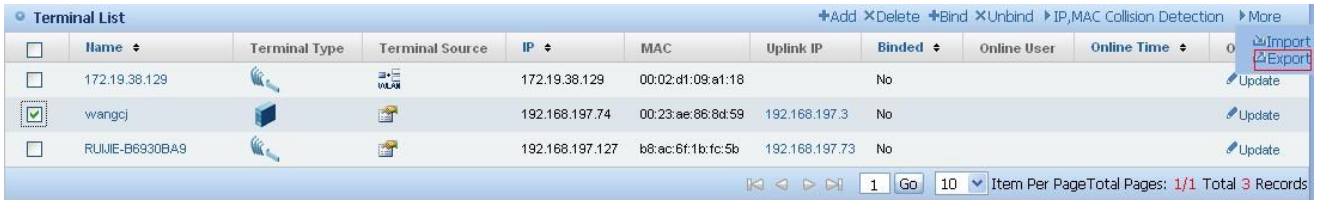


Figure 2.100. Choose Export Terminals page

File Download dialog box will be displayed. Click **Save**.
The system will display Save File dialog box. Input file name, and then click **Save**.

2.5.6. Terminal Binding/Unbinding

In the system, terminals can be bound to their uplink device interfaces (IP-MAC binding). This will put a restriction on MAC and IP allowed to visit the interface of the device. Thus, the interface can only be accessed by network elements consistent with the IP-MAC binding.

Operation Steps

1) On **Terminal List** page, choose terminals to be bound, and then click **Bind**.

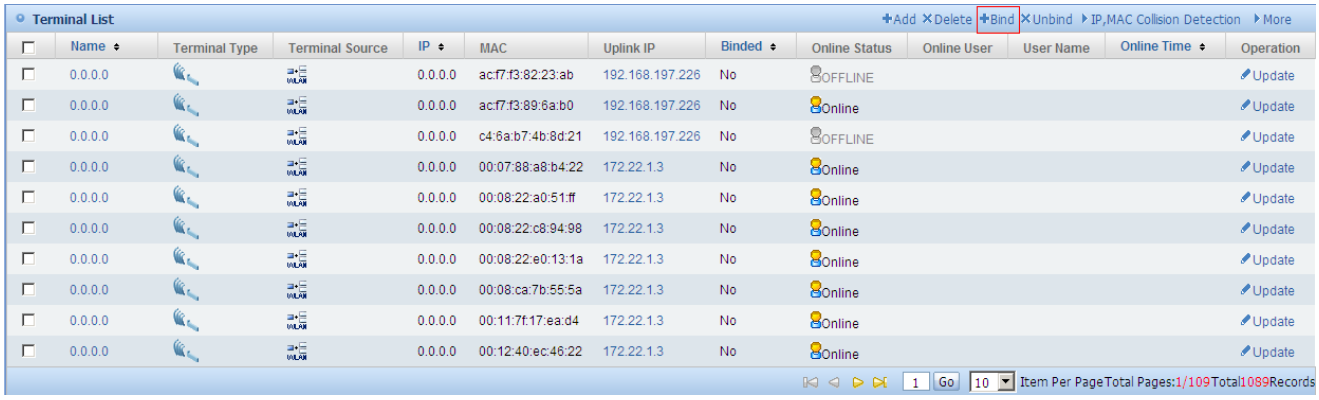


Figure 2.101. Bind Terminal page

If binding is successful, binding success message will be shown and binding column in the list will be marked with Yes. If binding fails, the failure cause will be shown.
On **Terminal List** page, choose terminals to be unbound, and then click **Unbind**.

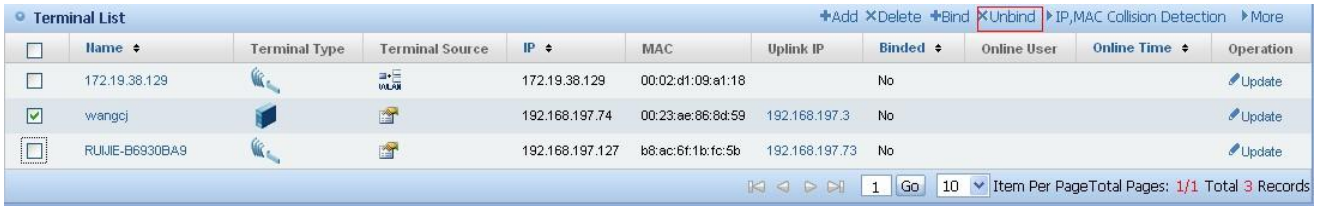


Figure 2.102. Unbind Terminal page

If unbinding is successful, unbinding success message will be shown and binding column in the list will be marked with No. If unbinding fails, the failure cause will be shown.

Note: Only terminals with uplink devices and interfaces should be chosen to do binding. Otherwise, binding will fail.

Note: Bound terminals must be selected before doing unbinding. Otherwise, unbinding will fail.

2.5.7. IP/MAC Collision Detection

IP/MAC Collision Detection is to check if there is single IP address mapped to multiple MAC addresses or single MAC address mapped to multiple IP addresses in the system. If yes, it indicates that there is wrong setting or ARP attack in the system.

Operation Steps

1) On **Terminal List** page, click **MAC-to-IPs** to do single MAC mapped to multiple IP detection.

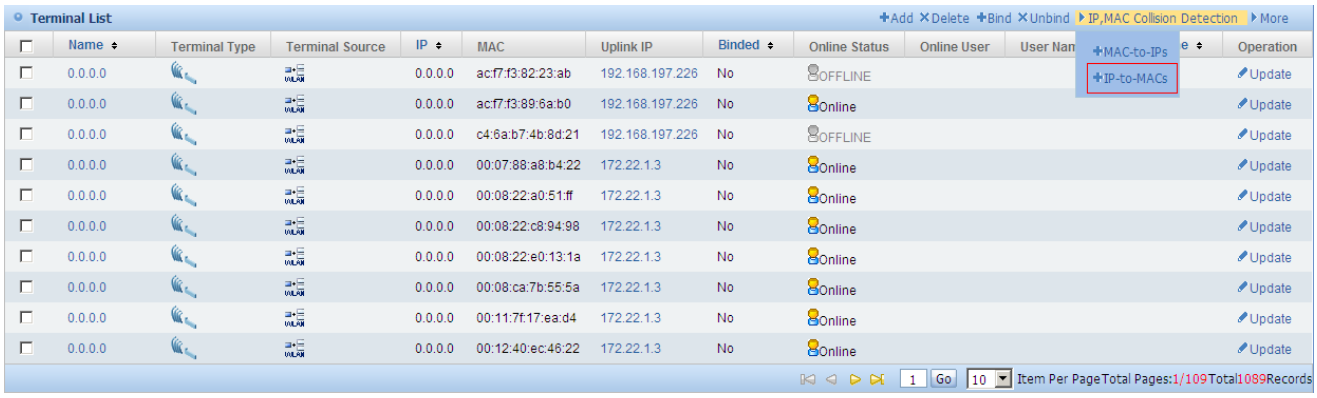


Figure 2.103. IP Collision Detection page

The system shows detection result. If there is no collision, no data will be shown. Otherwise, the abnormal PC info will be shown.

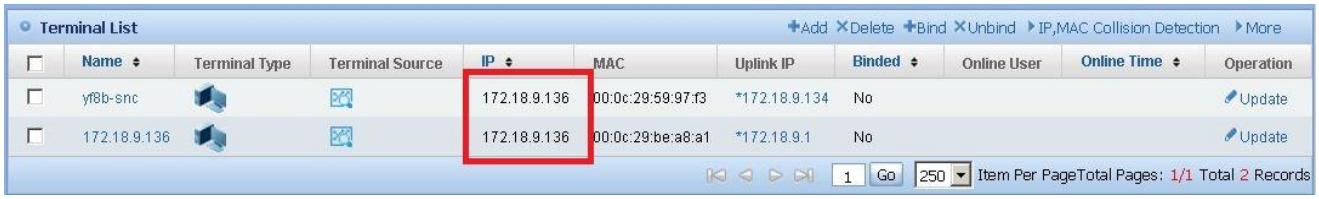


Figure 2.104. IP Collision Detection Result page

On **Terminal List** page, click **IP-to-MACs** to do single IP mapped to multiple MAC detection.

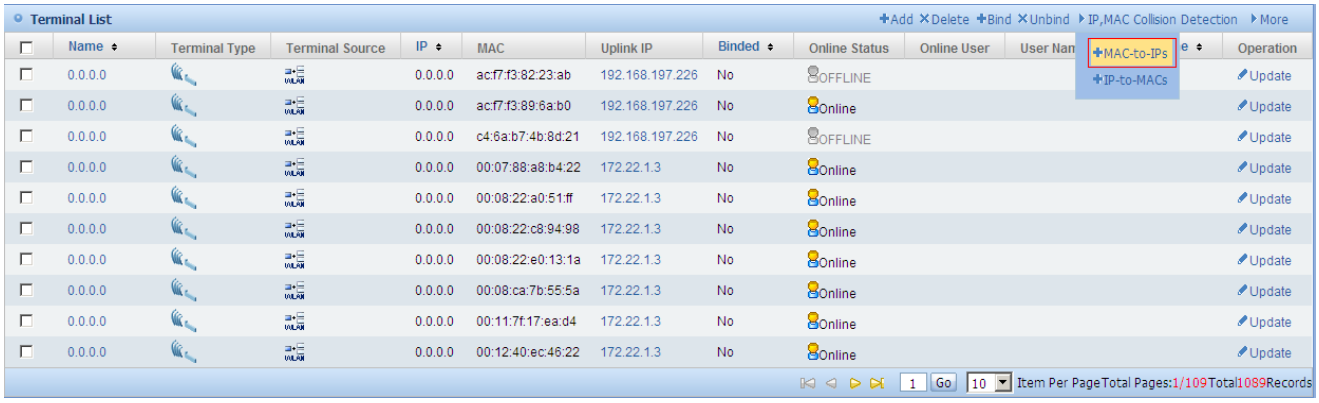


Figure 2.105. MAC Collision Detection page

The system shows detection result. If there is no collision, no data will be shown. Otherwise, the abnormal PC info will be shown.

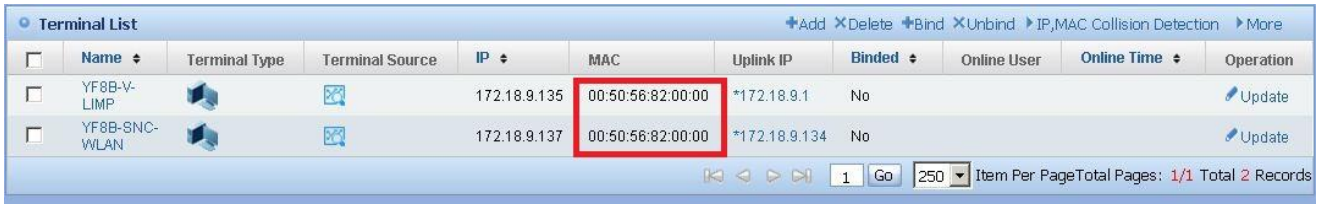


Figure 2.106. MAC Collision Detection Result page

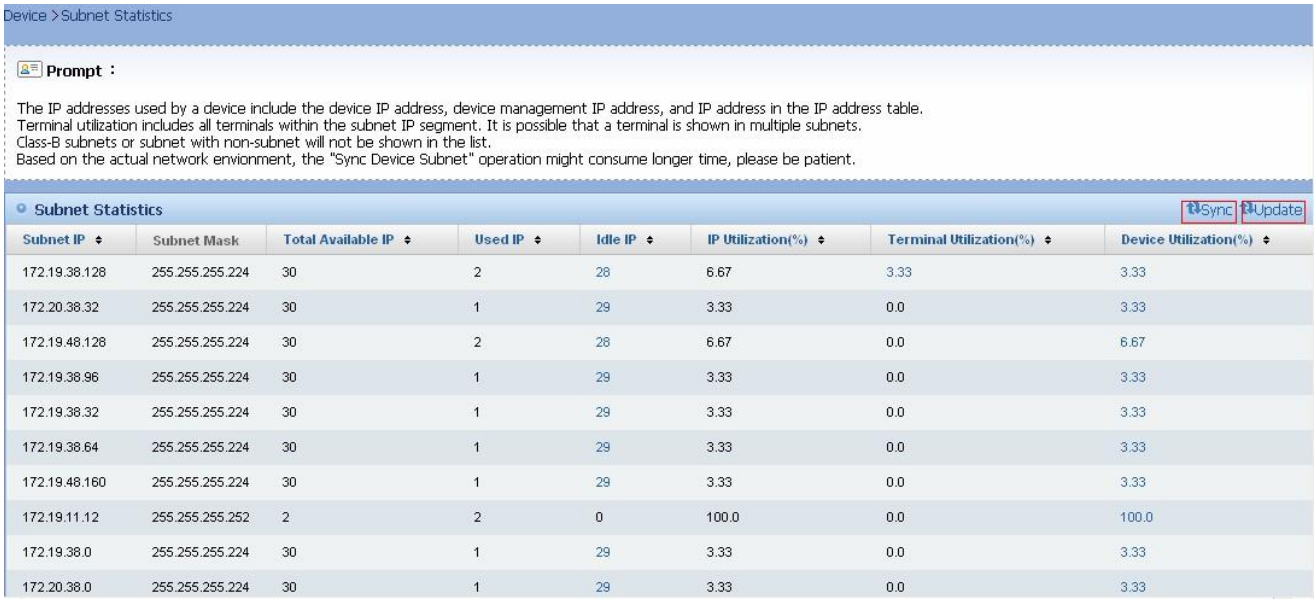
Note IP/MAC collision detection is only performed on devices discovered by topology discovery.

2.5.8. Subnet Usage Statistics

Subnet Usage Statistics is to do statistics on the IP usage of a subnet. Users can view occupation of devices and terminals IP addresses in the subnet, as well as existing available IP addresses.

Operation Steps

1) Click **Subnet Statistics** in system management to enter **Subnet Statistics** page.



Subnet IP	Subnet Mask	Total Available IP	Used IP	Idle IP	IP Utilization(%)	Terminal Utilization(%)	Device Utilization(%)
172.19.38.128	255.255.255.224	30	2	28	6.67	3.33	3.33
172.20.38.32	255.255.255.224	30	1	29	3.33	0.0	3.33
172.19.48.128	255.255.255.224	30	2	28	6.67	0.0	6.67
172.19.38.96	255.255.255.224	30	1	29	3.33	0.0	3.33
172.19.38.32	255.255.255.224	30	1	29	3.33	0.0	3.33
172.19.38.64	255.255.255.224	30	1	29	3.33	0.0	3.33
172.19.48.160	255.255.255.224	30	1	29	3.33	0.0	3.33
172.19.11.12	255.255.255.252	2	2	0	100.0	0.0	100.0
172.19.38.0	255.255.255.224	30	1	29	3.33	0.0	3.33
172.20.38.0	255.255.255.224	30	1	29	3.33	0.0	3.33

Figure 2.107. Subnet Usage Statistics Report

Note

1. Please do **Sync** device subnet when using this function for the first time. It might take a long time, please be patient.

Note

If there is no data in subnet statistics, please click **Update** to get the latest data.

Note

If you want to check the latest data, please click **Update**.

Note

Subnet data in the list comes from subnet management. If subnet data is wrong, please click **Refresh** to get the latest data.

On **Subnet Statistics** page, choose **Idle IP**, and click available IP number to enter available IP list.

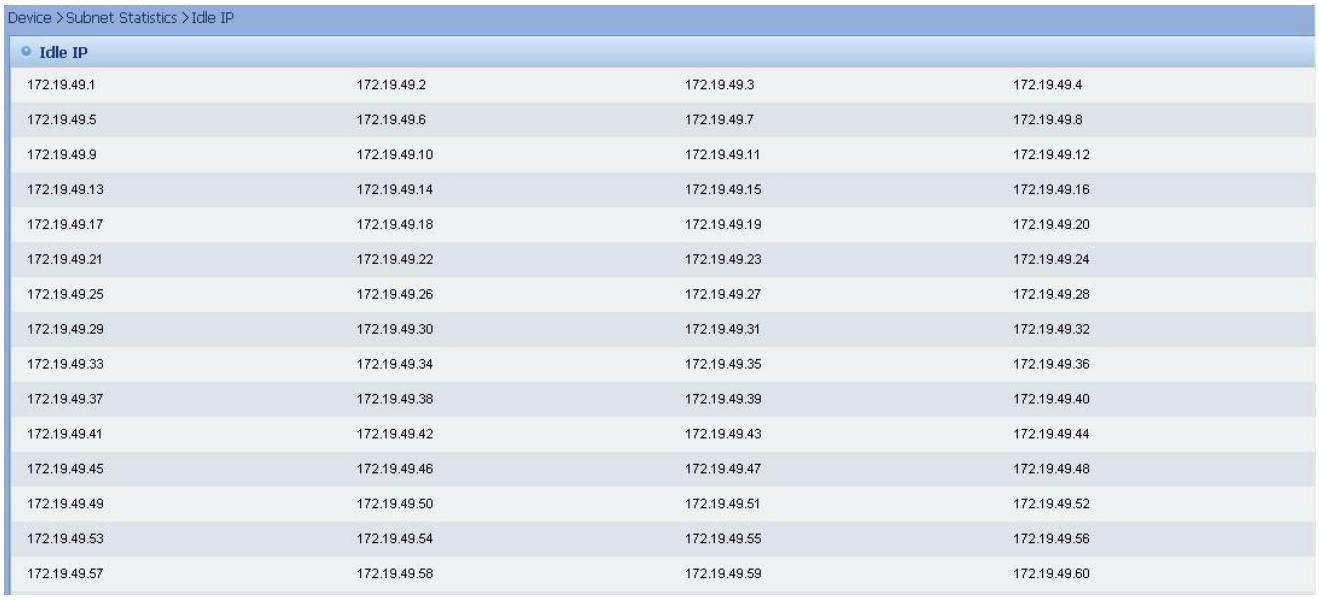


Figure 2.108. Available IP List

On **Subnet Statistics** page, choose **Terminal Utilization**, and click the usage value to enter terminal list.

Figure 2.109. Associated Terminal

On **Subnet Statistics** page, choose **Device Utilization**, and click the usage value to enter device list.

Figure 2.110. Associated Device

Note IP used by device includes device IP, device management IP and IP in IP address table.

Note Terminal usage includes all terminals in subnet IP segment. So it is possible that a terminal appears in multiple subnets.

Note Class B subnets are not shown in the list, nor subnets with 0 subnet.

2.6. Batch Synchronization of Device Information

Major Functions

- Realtime Synchronization of Device Information
- Automatic device synchronization

2.6.1. Realtime Synchronization of Device Information

Operation Steps

1) On batch synchronization of device information page, click **Realtime Device Synchronization** to enter realtime device information synchronization page. As shown below:

Figure 2.111. Realtime Device Information Synchronization

On realtime device information synchronization page, you can select **All Devices** to synchronize information of all the devices in the system, or select **Select Manually** to decide the alarm type of non-major version and the devices you want to Synchronize. As shown below:

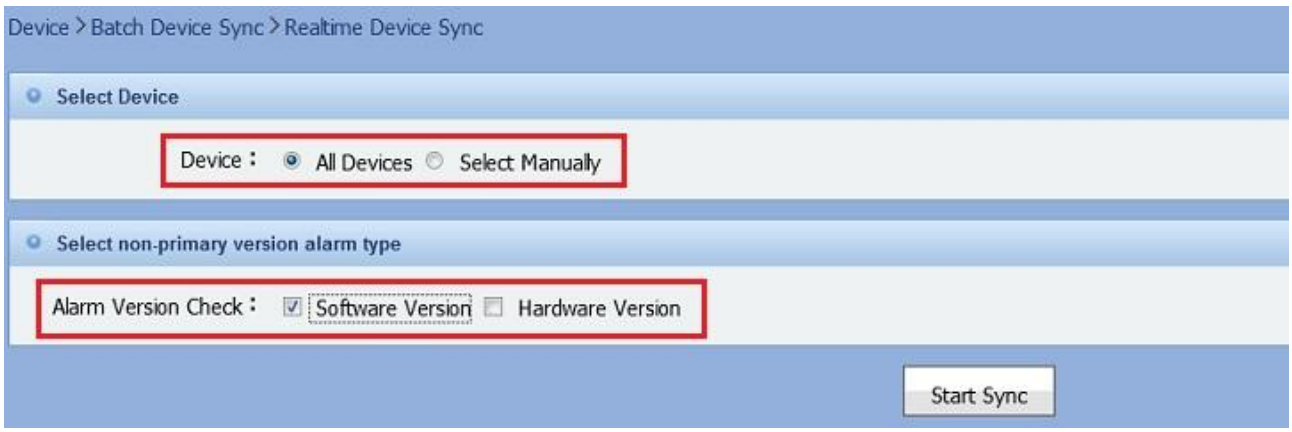


Figure 2.112. Realtime Device Information Synchronization (Select Manually)

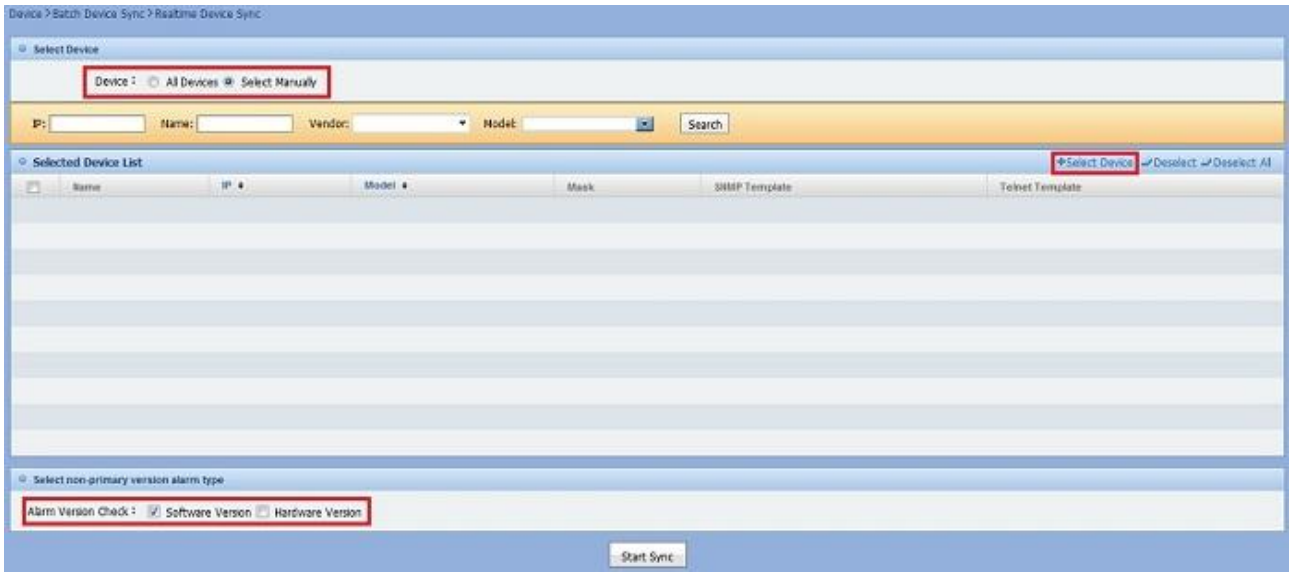


Figure 2.113. Realtime Device Information Synchronization (All Devices)

Click **Start Synchronization**, you can see the batch synchronization log. As shown below:

Figure 2.114. Device information synchronization is in progress

2.6.2. Automatic Device Synchronization

Major Functions

- Add a Synchronization Plan
- Modify Synchronization Plan
- Query Synchronization Plan
- Activate or disable a synchronization plan
- View Plan Detail

2.6.2.1. Add a Synchronization Plan

Operation Steps

1) On **Batch Device Sync** page, click **Add Sync Plan**, the following is shown:

Figure 2.115. Synchronization Plan Addition List

Figure 2.116. Add Synchronization Plan

In **Add Plan** page, click **Next t**o enter **Select Device** page to add plan for device sync in batches. On **Select Device** page, please select the devices which will be synchronized in the plan. The Selected Devices list will be shown firstly, after clicking **Select Device**, a pop-up page will show the device list from which you can select devices for adding to selected devices list. Click **Previous** to return to the first step of adding synchronization plan. Click **Finish** to finish the plan addition. As shown below:

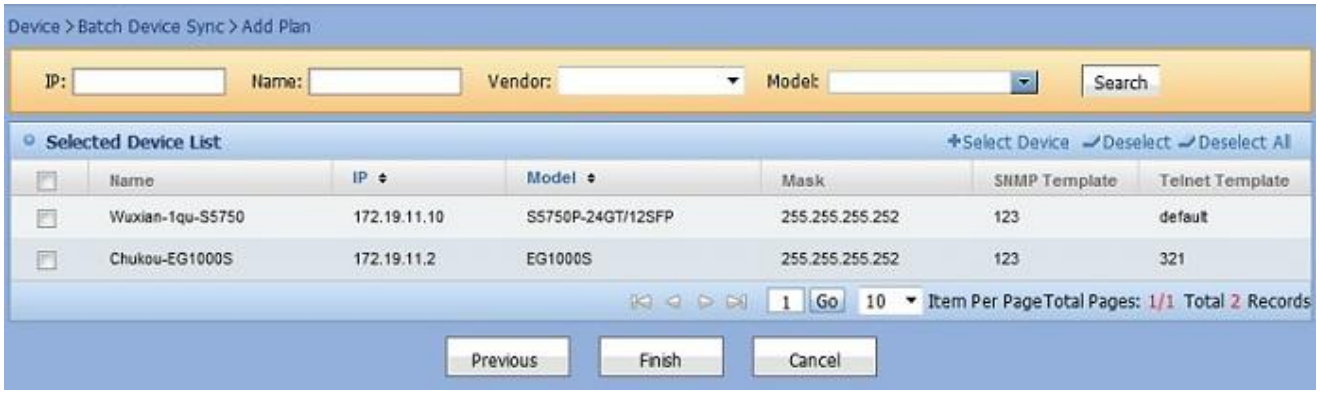


Figure 2.117. Device List

2.6.2.2. Modify Synchronization Plan

Operation Steps

1) On batch synchronization of device information page, click the plan name to enter the plan detail page. As shown below:

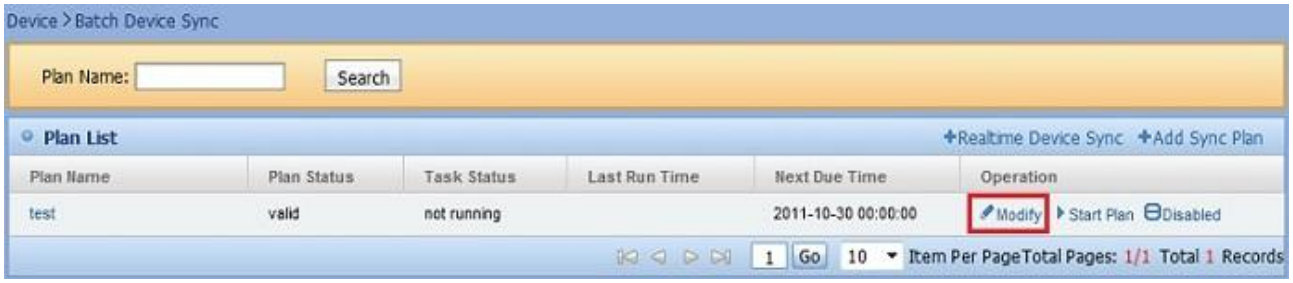


Figure 2.118. Synchronization Plan List

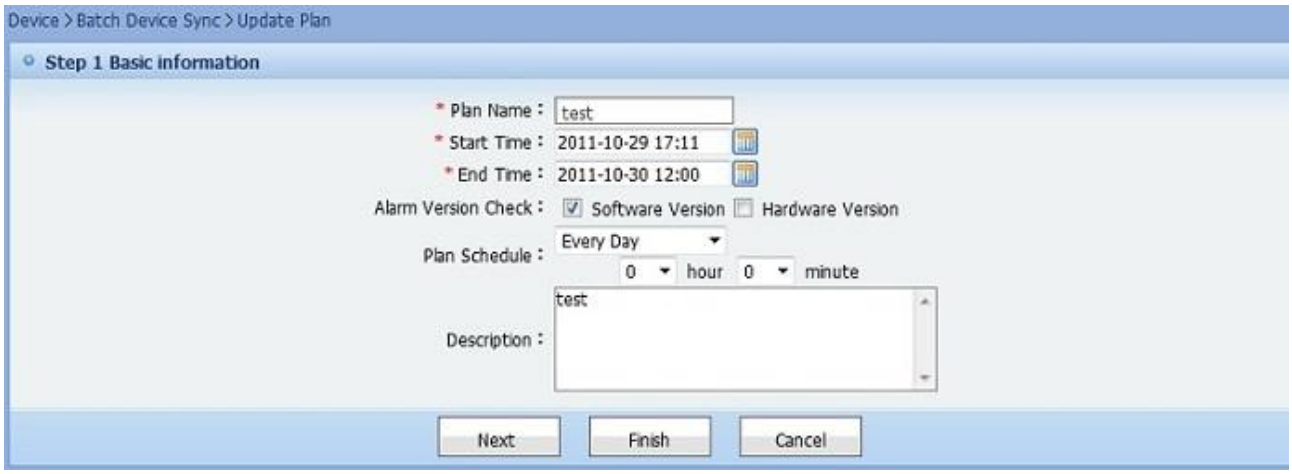


Figure 2.119. Synchronization Plan Modification Page

2.6.2.3. Query Synchronization Plan

Operation Steps

1) On **Batch Device Sync** page, enter the “Plan Name” and click **Search** to query synchronization plan. As shown below:

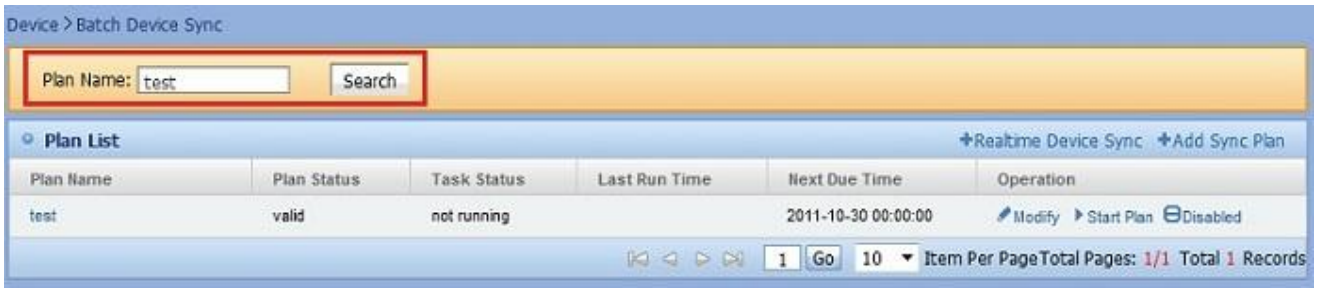


Figure 2.120. Query Synchronization Plan

2.6.2.4. Activate or Disable a Synchronization Plan

After you add a synchronization plan, the synchronization plan is in “invalid” state. You can click **Activate** to activate the synchronization plan. Only an activated plan can run according to the configured parameters. When a plan is activated, you can execute the disable operation to disable the plan.

Operation Steps

1) When an plan is in “invalid” state, you can click the **Activate** to activate the plan. As shown below:

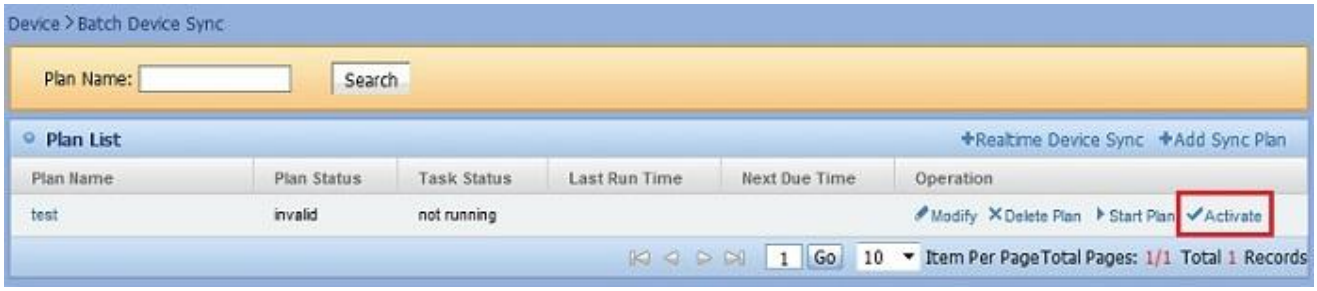


Figure 2.121. Activate a Plan

When the plan is in “Valid” state, you can click **Disable** to disable the plan. As shown below:

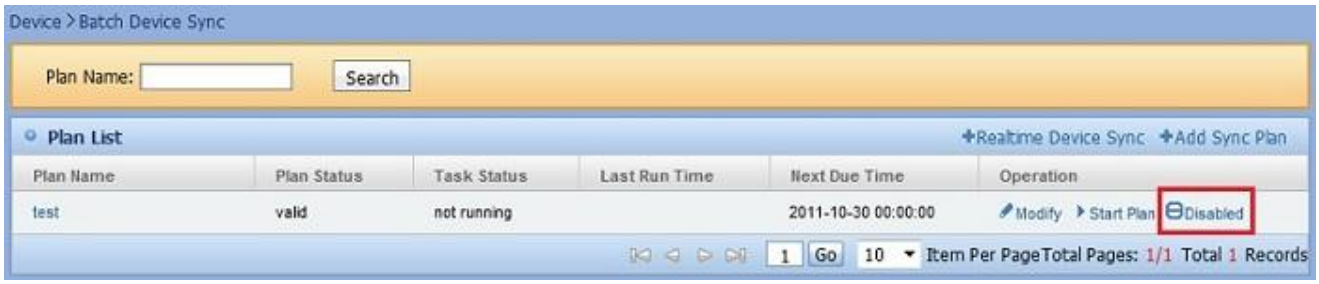


Figure 2.122. Disable a Plan

2.6.2.5. View Plan Detail

Operation Steps

1) On **Batch Device Sync** page, click the plan name to enter the **Plan Detail** page. As shown below:

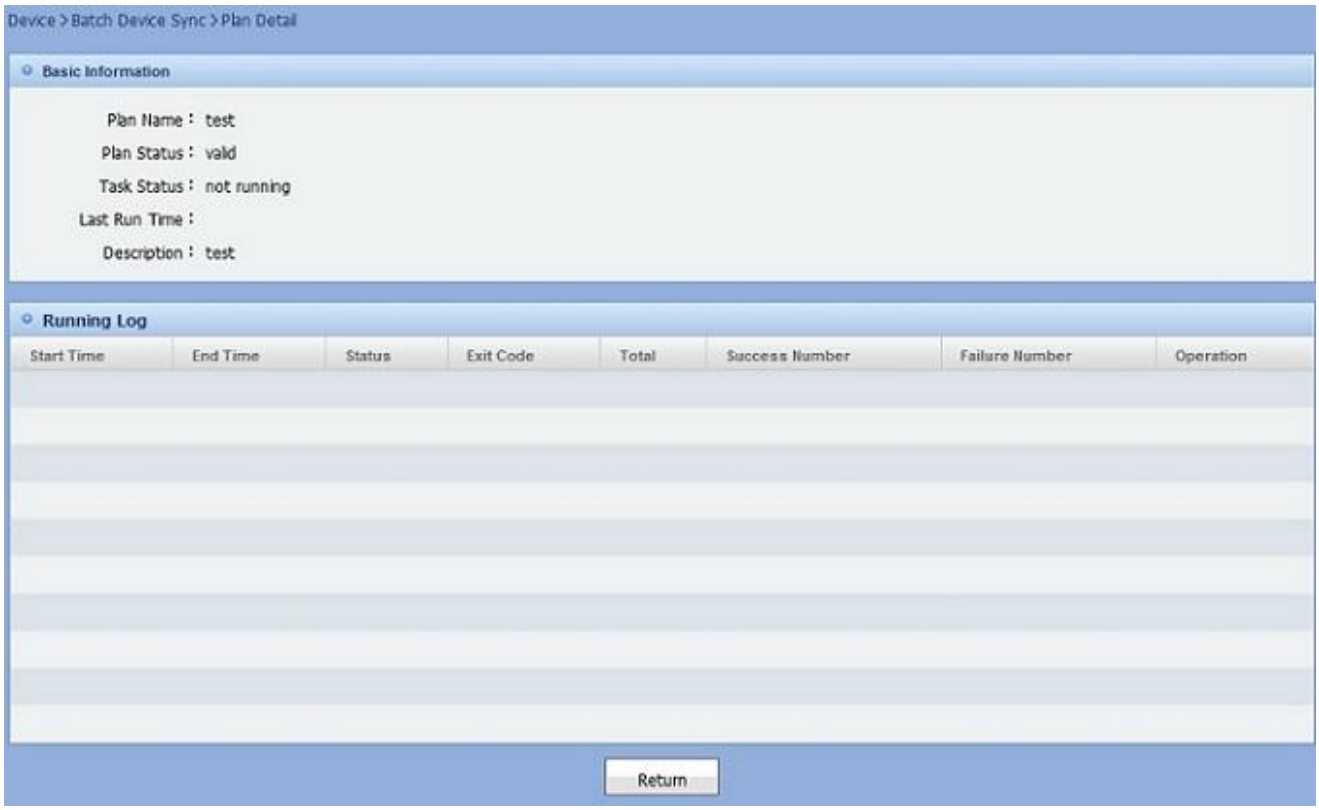


Figure 2.123. View Plan Detail Page

Chapter 3 Topology Management

Topology management provides an intuitive way to manage networks and devices. Devices are shown as nodes in topology view. Connections among devices, aka topology relation, are shown as links in topology view. Based on connection type, the links are shown in Layer 3 topology view, route topology view or Layer 2 topology view respectively. You can perform network monitoring and maintenance by monitoring alarm and traffic of devices and links, as well as other convenient operations on devices.

- Major Functions

3.1. Major Functions

The following are the major functionality modules of topology view.

- Topology Discovery
- Edit Topology View
- Topology View Management
- Key Path Detect
- Alarm Monitoring
- VSU Topology
- Other Operations

3.1.1. Topology Discovery

There are three types of topology views in the system. They are:

1) Layer 2 Topology View

Aka, “Physical Topology View”. The topology view we generally indicate is Layer 2 topology view. The system offers the most operations to Layer 2 topology. And most topology operations can be performed in views of Layer 2 topology view.

Physical topology view is the “Layer 2 Topology” of whole network view. But unless the network scale is small, e.g. less than 200 network elements, physical topology view is not used a lot. The more common practice is to use custom views or group views. See **Topology View Management**.

The topology discovery we are talking about is mainly referred to “**Layer 2 Network Topology Discovery**” (aka, “Physical Network Topology Discovery”). It is used to figure out the physical links between network elements, so that all the network devices could be connected in Layer 2 topology view, as well as whole network topology, sub-network topology and custom topology. Hence the actual connections in the network is shown.

Layer 3 Topology View

Aka, “Logical Topology View”. It is mainly used to demonstrate relations between Layer 3 devices and sub-network(i.e. network segment). In Layer 3 topology view, you can navigate to Layer 2 topology view of any sub-network by double clicking the sub-net icon.

No separate topology discovery is needed to find Layer 3 topology relations. After finishes adding devices or auto device scan, system will analyze the relation of the devices and sub-net, then add it to Layer 3 topology view.

Route Topology View

Route topology view is used to demonstrate route relations among Layer 3 devices (i.e. Layer 3 switches and routers) in the system. Accordingly, route topology discovery is used to find route relations among Layer 3 devices.

Layer 2 Network Topology Discovery

In topology view, you can perform real-time topology discovery, or set topology discovery to run periodically and incrementally.

Real-time topology discovery has an option: “Complete device L2 switching info before discovery”, as shown below. We recommend you to check this option before running topology discovery if there are less than 200 devices in your network. If your network has more than 200 devices, you should not select this option in the first time of topology discovery. But if the discovery result does not meet your expectation (e.g. some links are missing), you can select the option and perform

Layer 2 topology discovery. Stage “Complete device L2 switching info” of the option makes topology discovery results more stable and accurate. But, it also makes topology discovery slow, that is, about 5 to 10 minutes for every 100 devices.

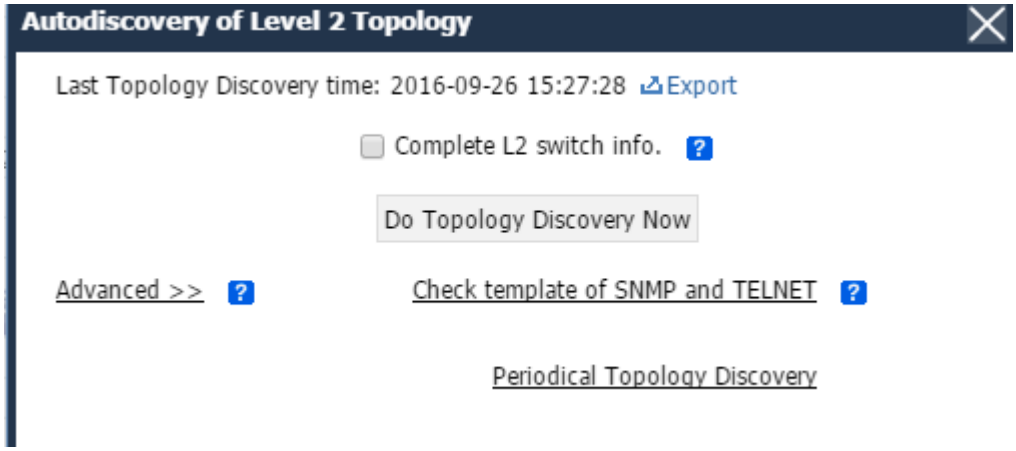


Figure 3.9. Real-time Topology Discovery

Besides, “Complete device L2 switching info” requires Telnet to devices. So, to get correct topology discovery result, please make sure that Telnet templates of devices are correctly configured.

You can also set topology discovery to run regularly, aka, periodical topology discovery. You can set the interval (in days) of the discovery, and the time to run the discovery.

In periodical topology discovery, “Complete device L2 switching info before discovery” is mandatory.

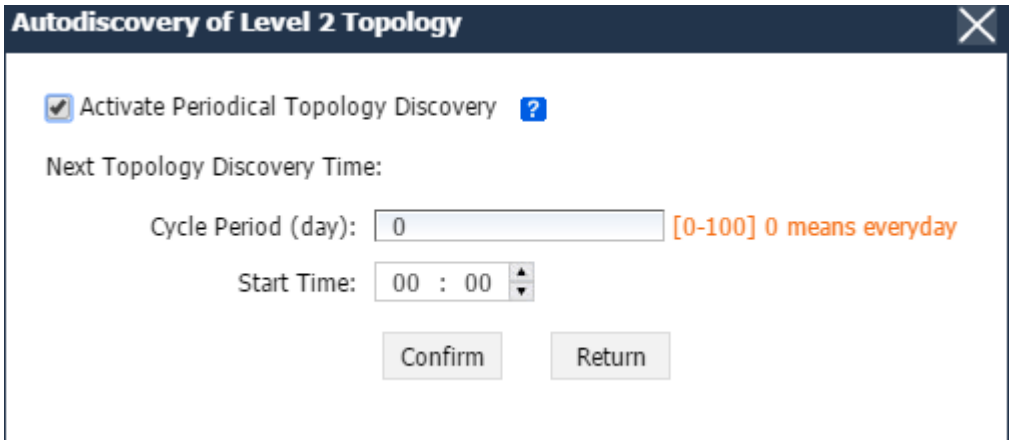


Figure 3.10. Periodical Topology Discovery

3.1.2. Edit Topology View

Admin can enter edit mode of topology view by clicking **Enter Edit Mode** in toolbar. Edit toolbar has the following functionalities:

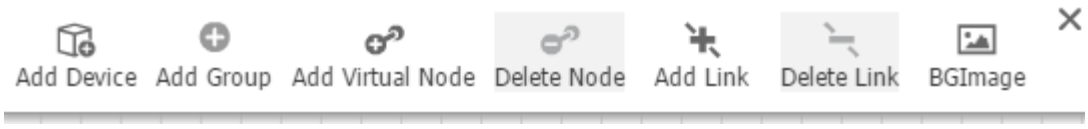


Figure 3.11. Edit Toolbar

1) **Add device**: Admin can add devices to topology view, just as adding device functionality in **Device**.
Add Group: Admin can add groups to topology view.
Add virtual node: Admin can add virtual nodes to topology view. Virtual nodes can be buildings and Internet clouds.
Delete nodes: Admin can delete one or more nodes from the system through mouse selection or CTRL clicking.
Add link: Admin can add a link from one node in the topology view to another one. Linearity (single solid line, single dotted link, double solid line, double dotted line), uplink node interface and downlink node interface can be defined.
Delete link: Admin can delete a link after choosing it by mouse clicking.
BGImage: Admin can change background image.

3.1.3. Topology View Management

Topology View Management provides the most intuitive ways to manage topology views in the network. Devices and connections among devices, aka topology relations, are shown in topology view as nodes and links. Based on connection type, topology relations are organized in Layer 3 topology view, route topology and level 2 topology. You can monitor and maintain the network through monitoring alarm and traffic info of devices and links, as well as other operations on devices. You can set a default topology.

- Layer 2 Topology
- Layer 3 Topology
- Route Topology

3.1.3.1. Layer 2 Topology

Layer 2 topology: admin can view link layer topology among devices and PCs. It demonstrates actual physical connections.

1) Global topology: admin can view link layer topology among devices and PCs. It demonstrates actual physical connections.

Topology view operations supported in global network topology view are: add device, add virtual node, delete node, add link, delete link, L2 topology discovery, path topology and topology view permissions setting. For details, see **Edit Topology View**.

Subnet topology: it is subview of Layer 2 topology. Admin can choose a subnet to view topology view of its devices.

Topology view operations supported in subnet topology are: add device, add virtual node, delete node, add link, delete link, L2 topology discovery, path topology and topology view permissions setting. For details, see **Edit Topology View**.

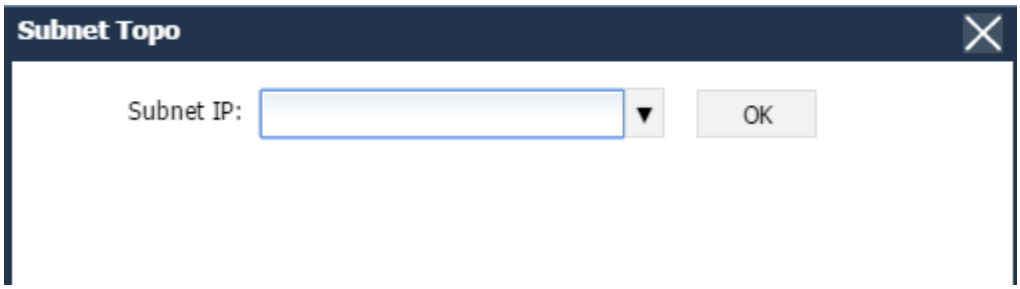


Figure 3.14. Choose Subnet Topology

Custom topology: admin can add customized views to Layer 2 topology if needed. In the system, users can define custom view with the following steps: input custom view name, select devices or input IP range to filter devices, and save. Then the newly created view will be shown in custom view automatically. Addition, modification, deletion operations can be performed on this newly created view or its sub-view. Devices in the view can also be added or removed.

Topology view operations supported in subnet topology are: add device, add virtual node, connect virtual node to sub-view, add node to the view, remove node from the view, delete node, add link, delete link, L2 topology discovery, path topology and topology view permissions setting. For details, see **Custom Topology**.

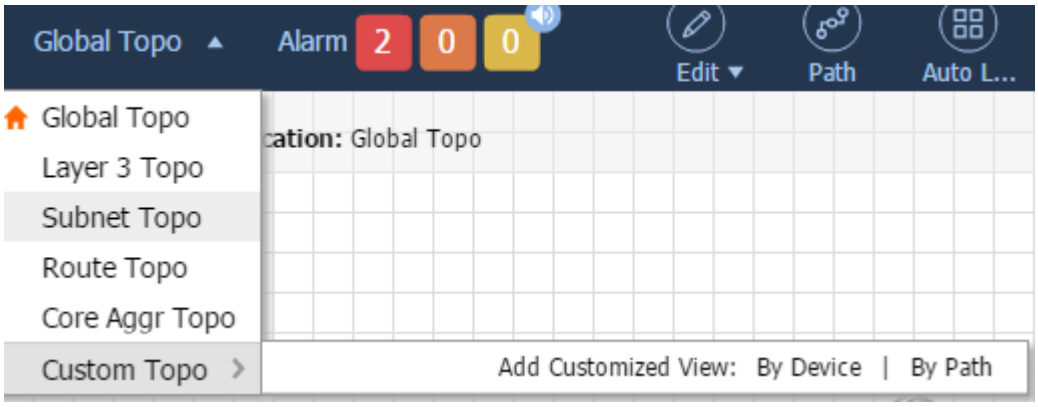


Figure 3.15. Custom Topology

Custom Topology

Custom Topology: It is a type of Layer 2 topology view. Admin can define custom topologies for different devices in Layer 2 topology view, and view the link layer topology between devices and PCs, which reflects the actual physical links.

Path Topology: shows the link topology of whole-network source devices and destination devices. For details, see **Path Topology**.

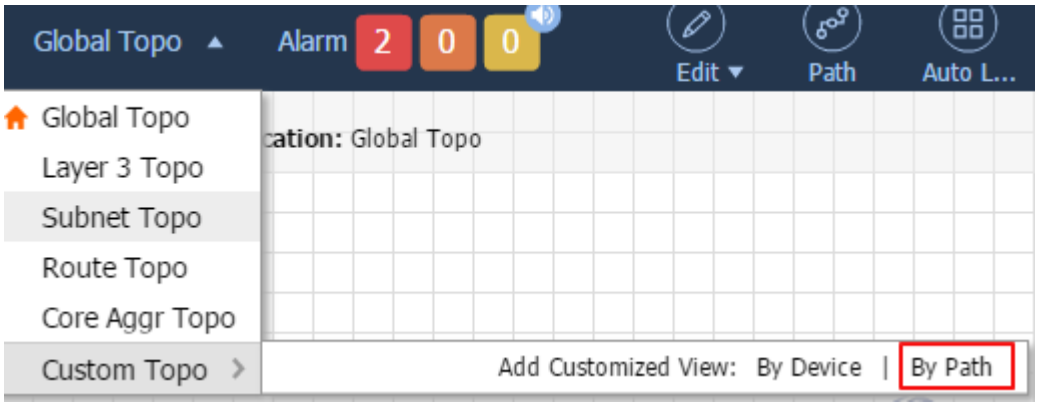
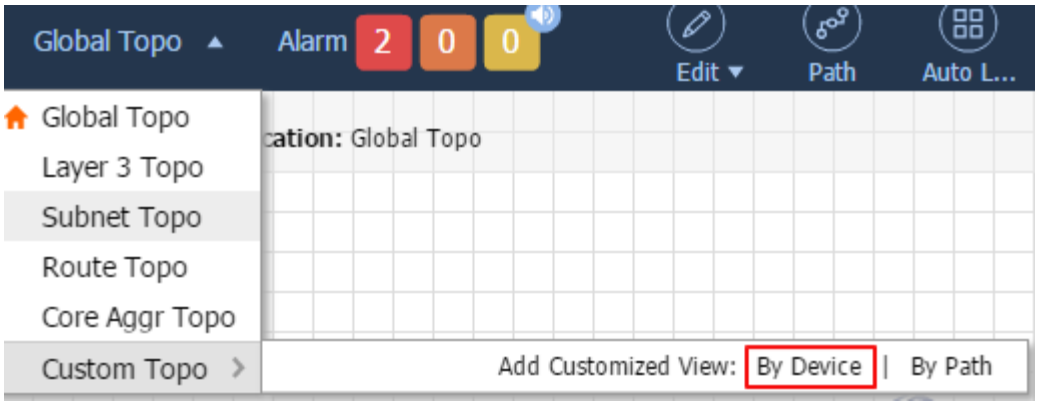


Figure 3.17. Path Topology

- Other Custom View: Admin can create self-defined topology view as needed.

Edit Custom Topology: The system shows custom topology view list when admin clicks **Custom Topology**. Admin can edit custom view by clicking **Enter Edit Mode** on the menu bar.

1) Add custom view: Admin can select a custom topology view to add sub-view to it. After sub-view is added, the sub-view will be automatically created under selected custom view. This is not supported in **Core Aggregation Topology** or **Group Topology**.



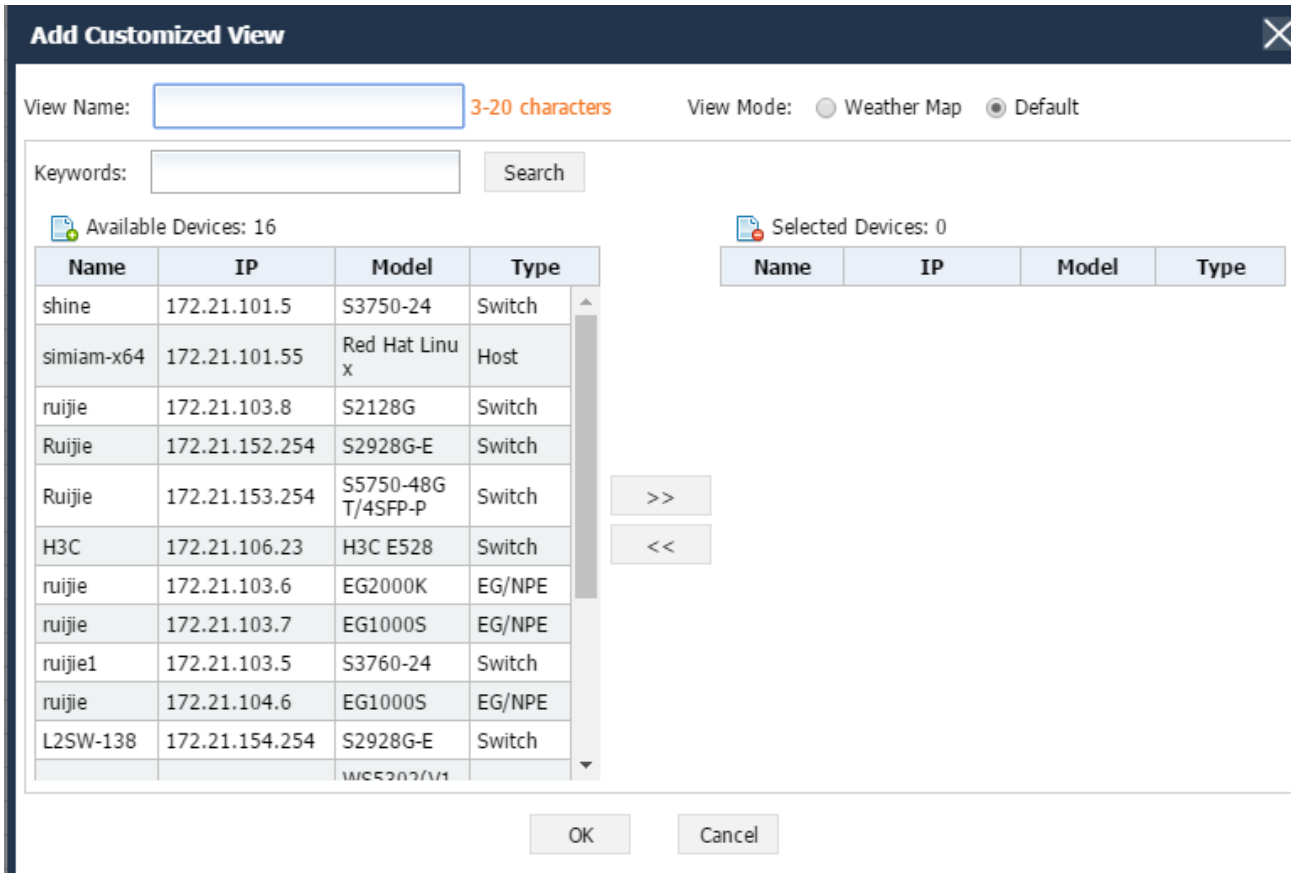


Figure 3.18. Input view name, and click Add to add custom view.

Modify custom view: Admin can modify a custom topology view after selecting it. This is not supported in **Core Aggregation Topology** or **Group Topology**.

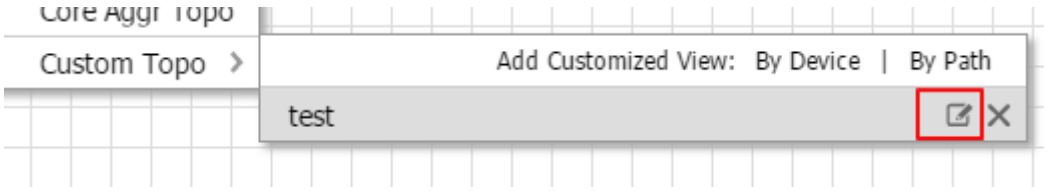


Figure 3.19. View name modification and view devices addition and removal can be performed in “Modify custom view”.

Delete custom view: Admin can delete a custom topology view after selecting it. This is not supported in **Core Aggregation Topology** or **Group Topology**.

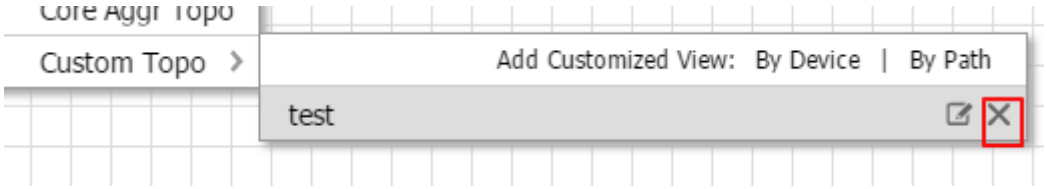


Figure 3.20. Delete Custom View

View Operations in Edit Toolbar: After admin clicks to enter edit mode, edit toolbar will be shown. Then admin can perform operations on devices and links in the view. For details, see **Edit Topology View**.

3.1.3.2. Layer 3 Topology

Layer 3 topology: shows the access relations among whole network Layer 3 devices and segments. Admin can double-click a segment to view its Layer 2 topology (link layer topology).

- Admin can click **Layer 3 Topo** link to view Layer 3 topo

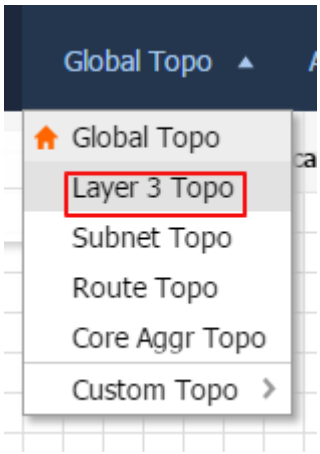


Figure 3.21. View Layer 3 Topo

3.1.3.3. Route Topology

Route Topology: shows the route relations among Layer 3 devices (e.g. Layer 3 switches, routers and etc) in the system.

- Admin can click **Route Topo** to view route topo.

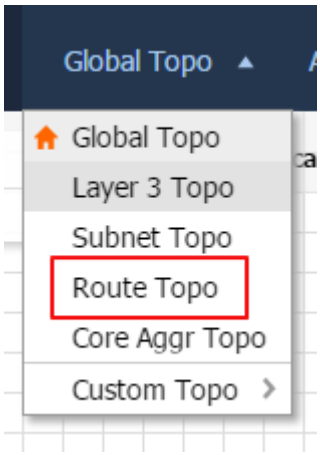


Figure 3.22. View Route Topo

3.1.4. Key Path Detect

Admin can go to key path detect panel by clicking **Key Path Detect** on menu bar.

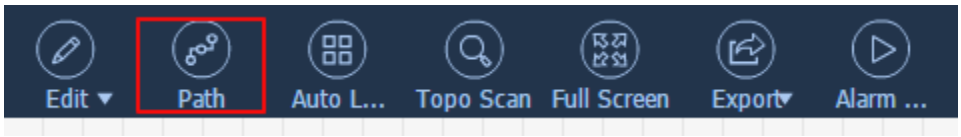


Figure 3.26. Perform Key Path Test

There are two key path detect ways:

- Real-time key path detect.

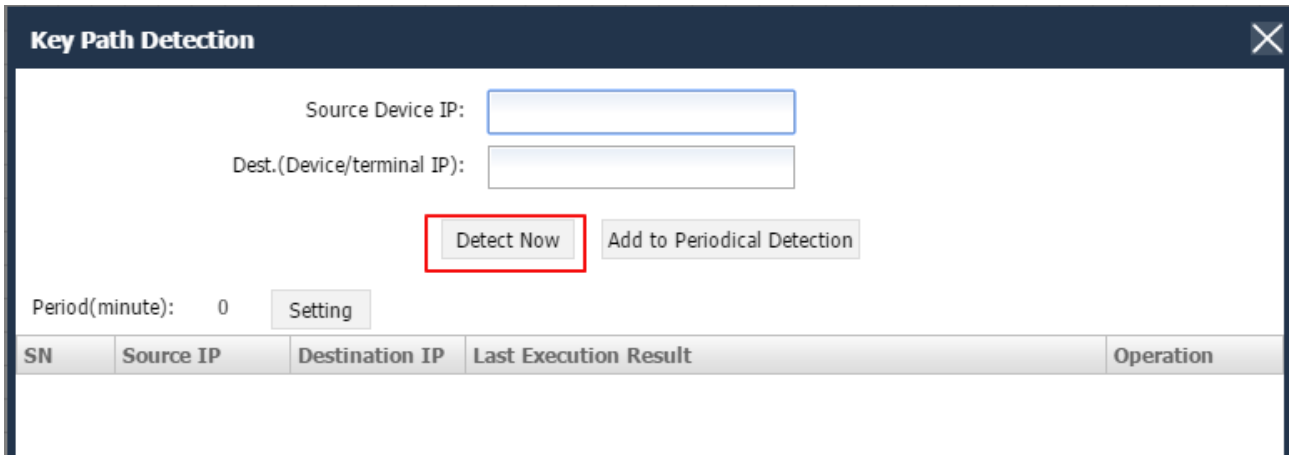


Figure 3.27. Real-time Test

Admin can input source (device name or IP) and destination (device name or IP), and click **Detect Now** to test the path from source to destination. The system will display the result of ping command (reachable/unreachable), and return Traceroute info. If not reachable, an alarm with ping result and traceroute info will be generated.

- Periodical key path detect.

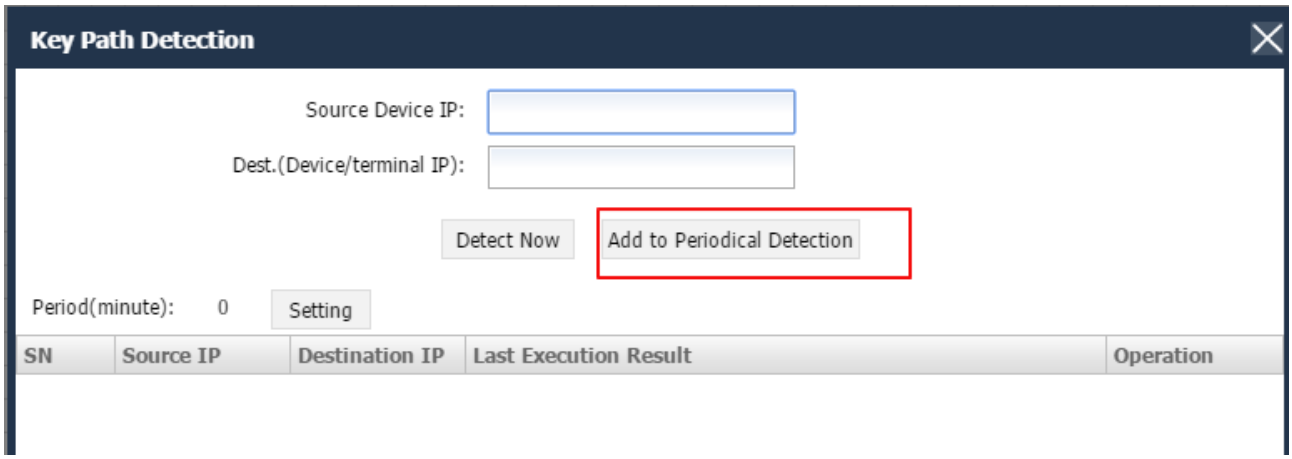


Figure 3.28. Add to Periodical Detection

1) Admin can input source (device name or IP) and destination (device name or IP), and click **Add to Periodical Detection** to add source IP and destination IP to periodical test list.

Admin can set periodical execution time, which should be between 5 and 999 minutes. After it is set, the system will show next execution time. When it is in the execution time, the system will perform ping and traceroute operations on source IP and destination IP in the periodical detection list. Alarms will be generated automatically if ping fails.

Admin can perform detection on source and destination IP in periodical detection list by clicking **Detect Now** in the operation column. Its effect is the same as that of real-time key path detect.

3.1.5. Alarm Monitoring

This function enables you to monitor alarm messages in real time and get a marquee display of these messages on the topology.

Operation Steps

1) Click **Alarm Monitoring** on the top menu, and the alarm monitoring window is displayed to provide a marquee display of real-time alarm messages.

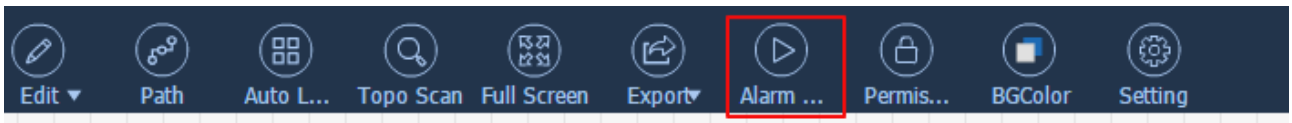


Figure 3.29. Enabling Alarm Monitoring

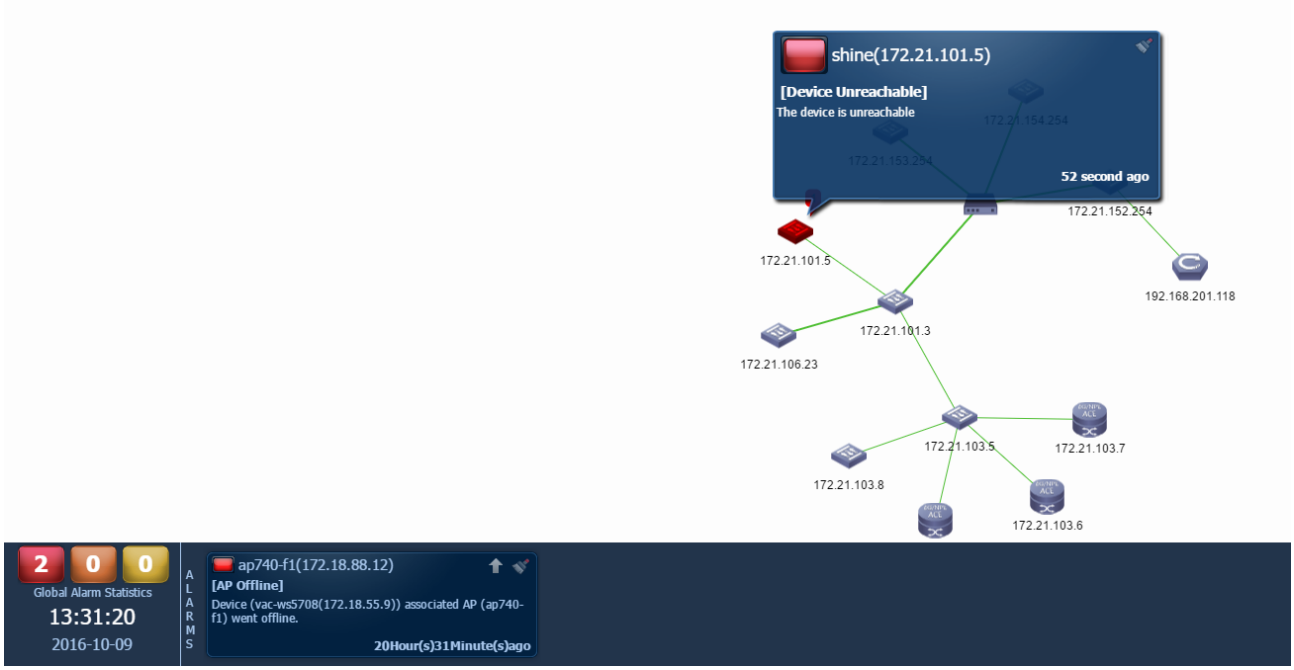


Figure 3.30. Alarm Monitoring Window

Click **Pause** or the space bar to stop the marquee display of alarm messages.

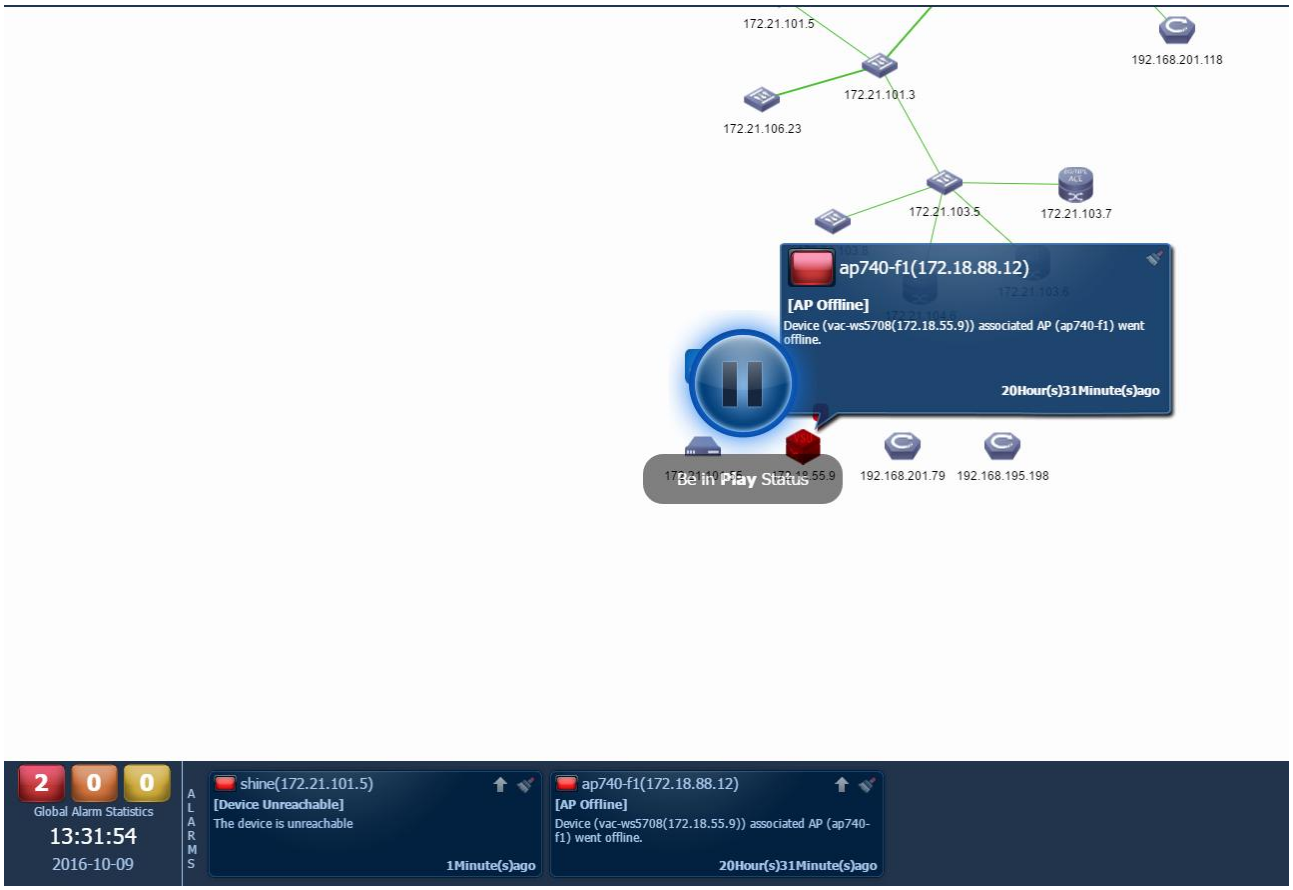


Figure 3.31. Stopping Marquee Display

Click **Restore** or the space bar to restore the marquee display of alarm messages.

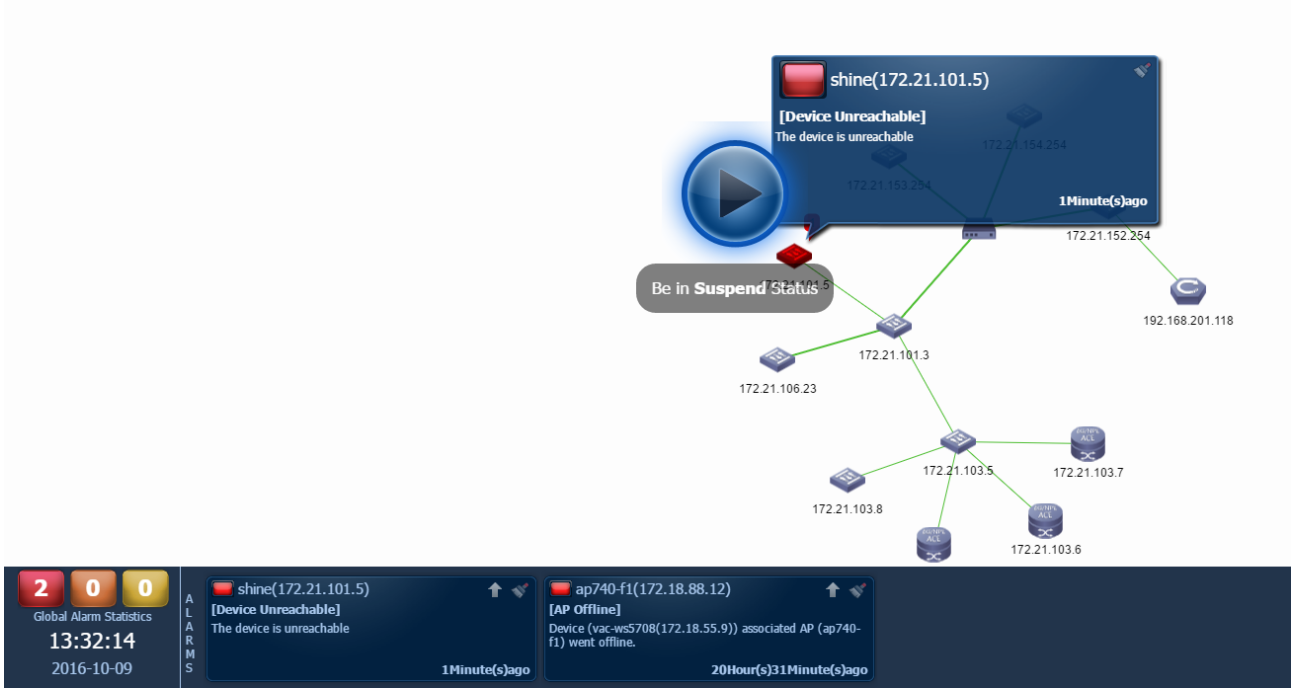


Figure 3.32. Restoring Marquee Display

Click **Exit** to exit the page and disable alarm monitoring.

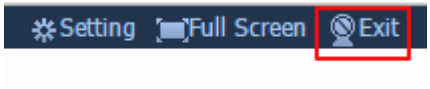


Figure 3.33. Disabling Alarm Monitoring

Click **Setting** to modify the parameters in the Alarm Monitoring Parameter Settings window displayed.

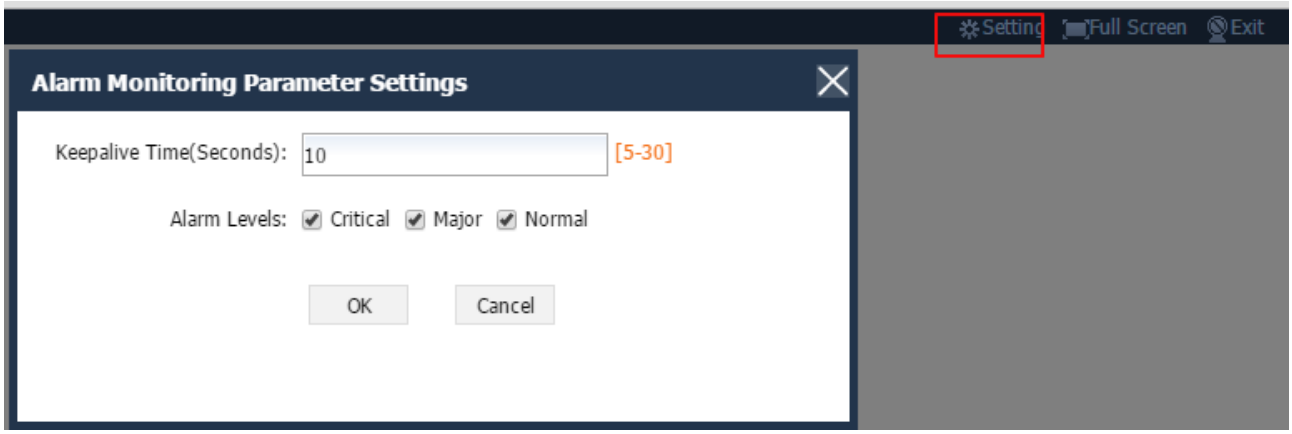


Figure 3.34. Modifying Alarm Monitoring Settings

Click **Clear Alarm** at the upper right corner of the alarm message to clear the message.

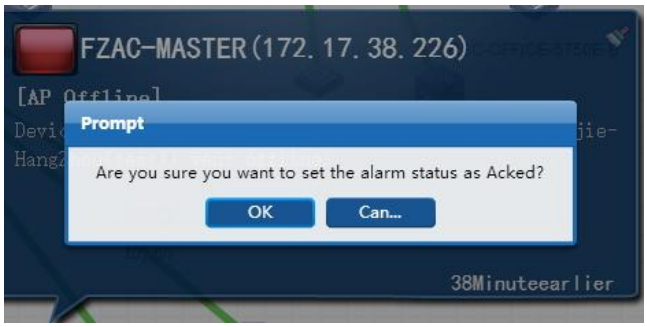


Figure 3.35. Clearing Alarm

Click **Locate Alarm** at the upper right corner of the alarm message to locate the alarm in the topology.

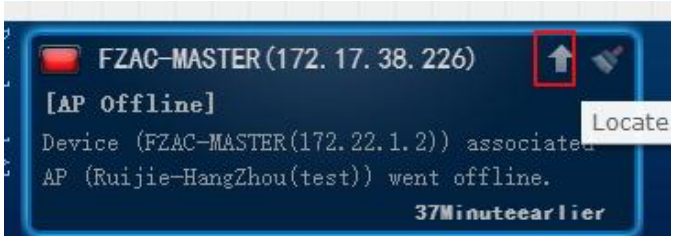


Figure 3.36. Locating Alarm

3.1.6. VSU Topology

This function enables you to view VSU topology.

Operation Steps

1) Find the VSU device.

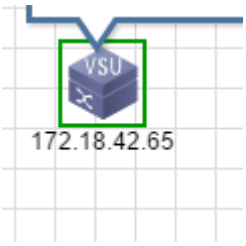


Figure 3.37. VSU Device Icon

Click **Unfold Inner Topology** at the right upper corner on the VSU panel.

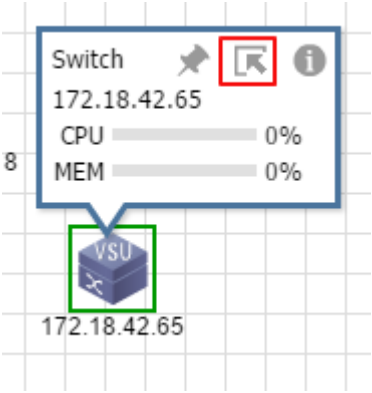


Figure 3.38. Unfolding VSU Topology

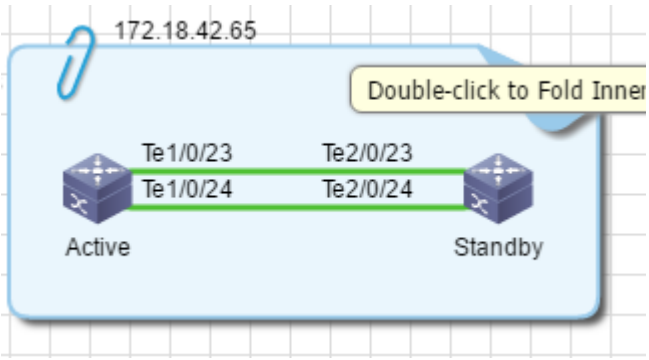


Figure 3.39. Unfolded VSU Topology

3.1.7. Other Operations

1) Topology View Permission

This function enables the admin to set topology view permissions.

Go to **Topology View Permissions Setting**. Select a **Role Name** from the dropdown list, and then select the topology views allowed.

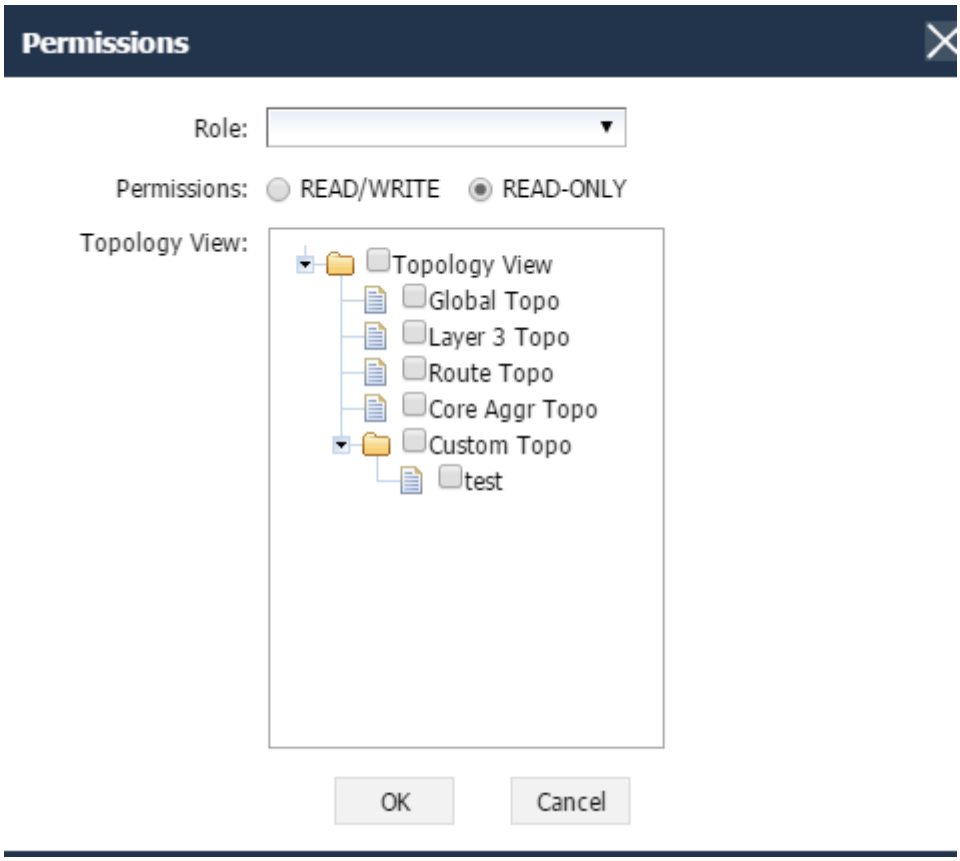
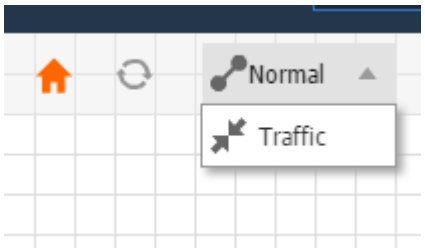
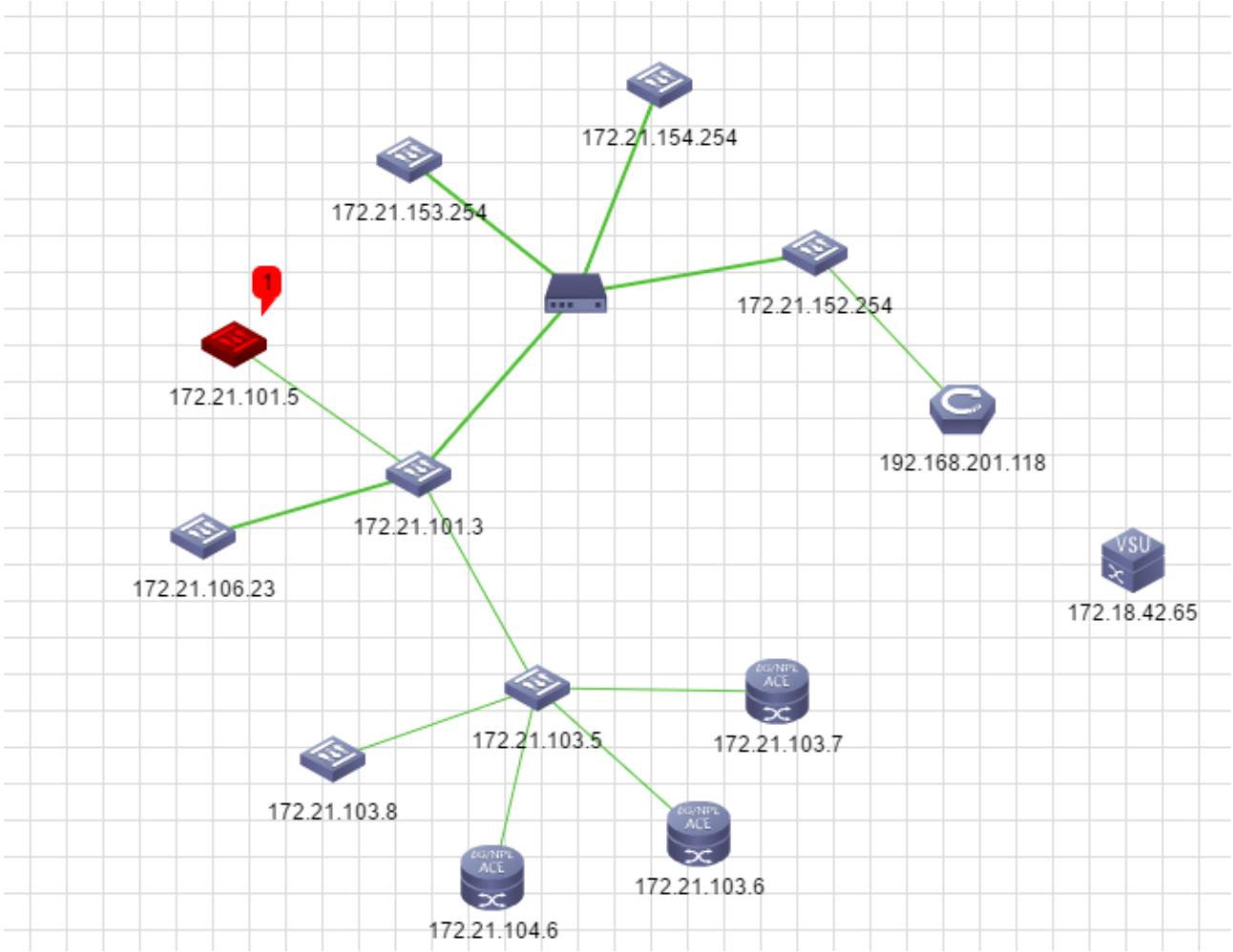


Figure 3.40. Topology View Permission Settings

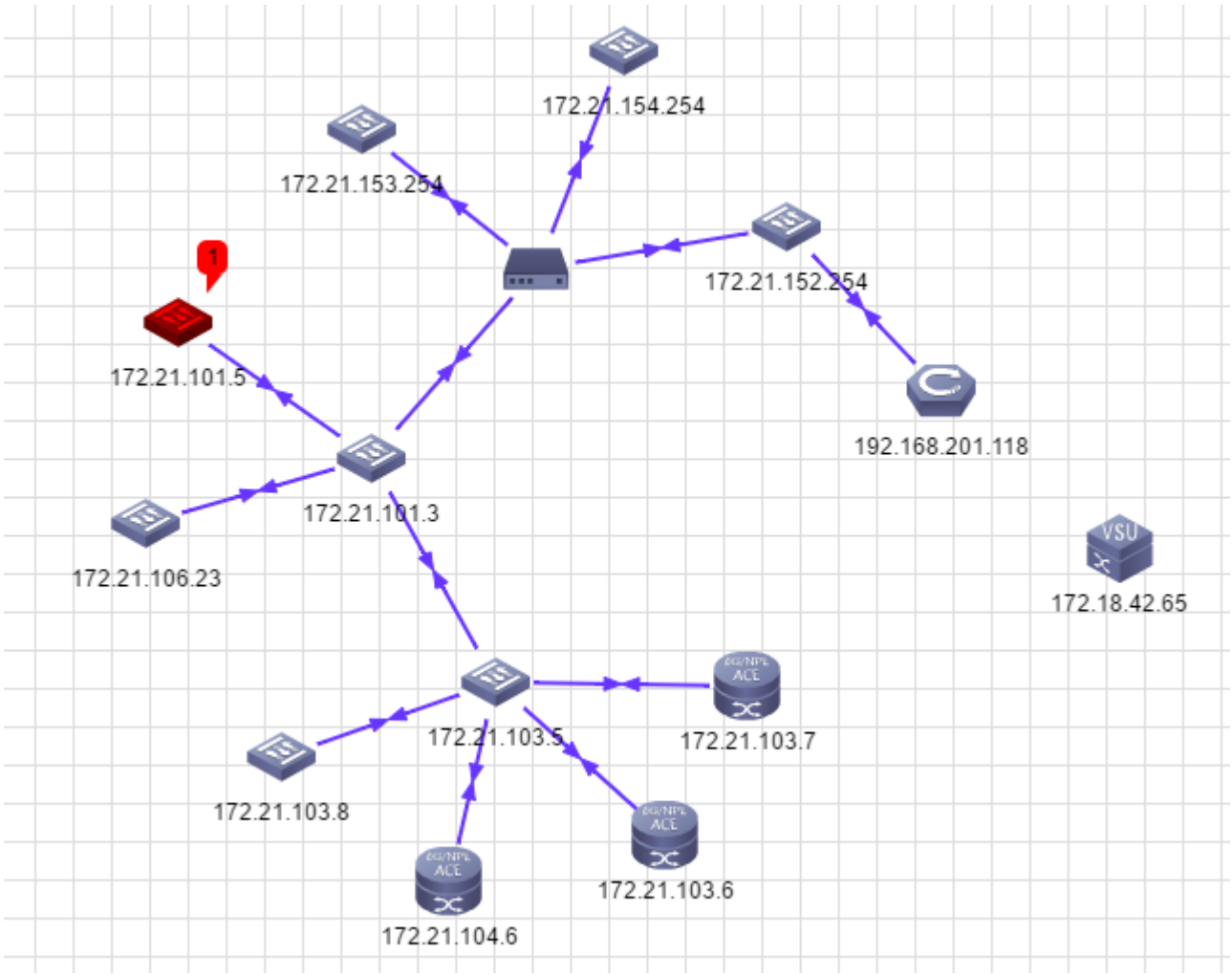
2) Mode View



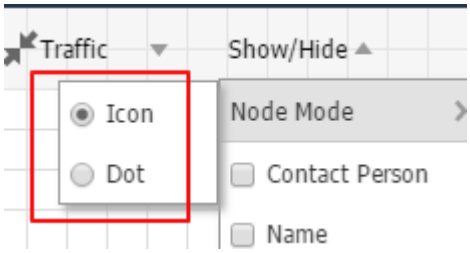
You can switch the topology to the **Normal** view. Bandwidth is indicted by the link width.



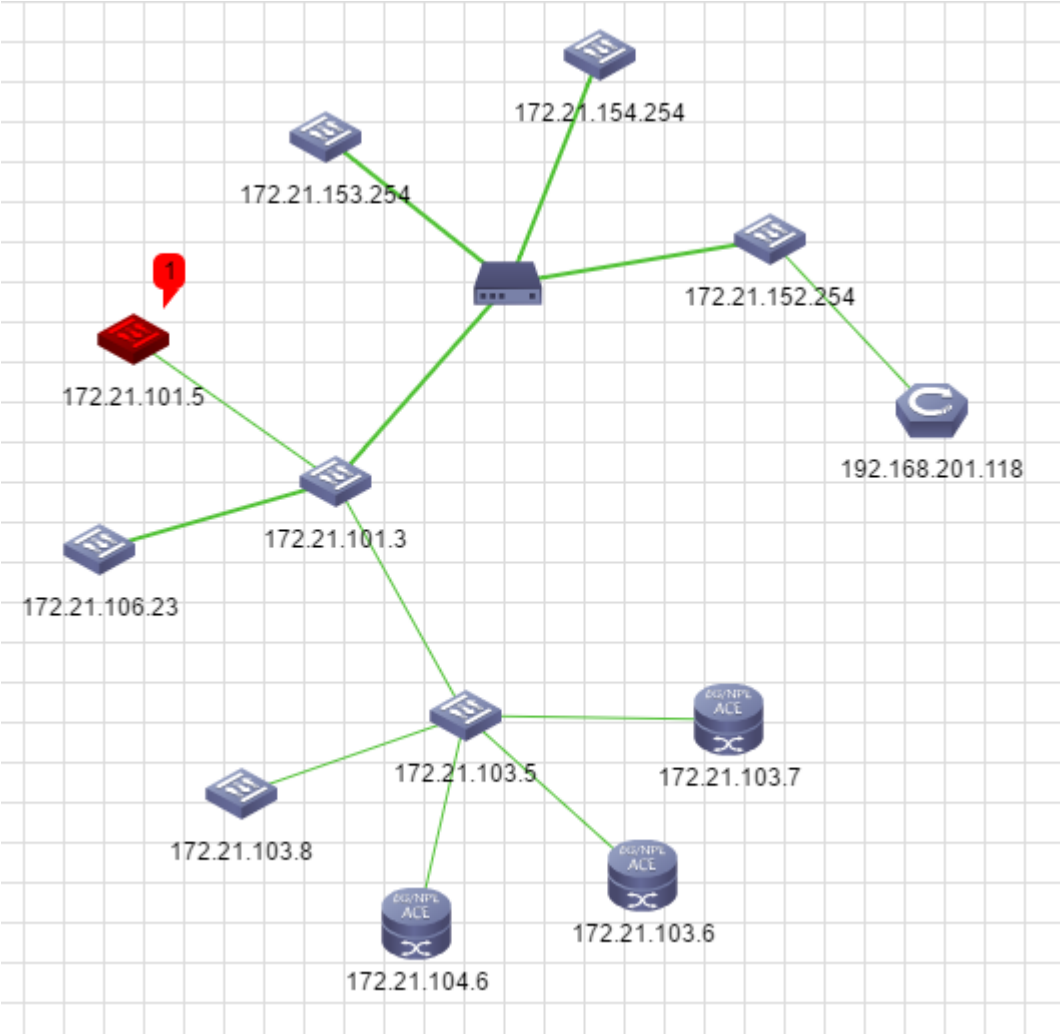
You can switch the topology to the **Traffic** view. Bandwidth usage is indicated by the link color.



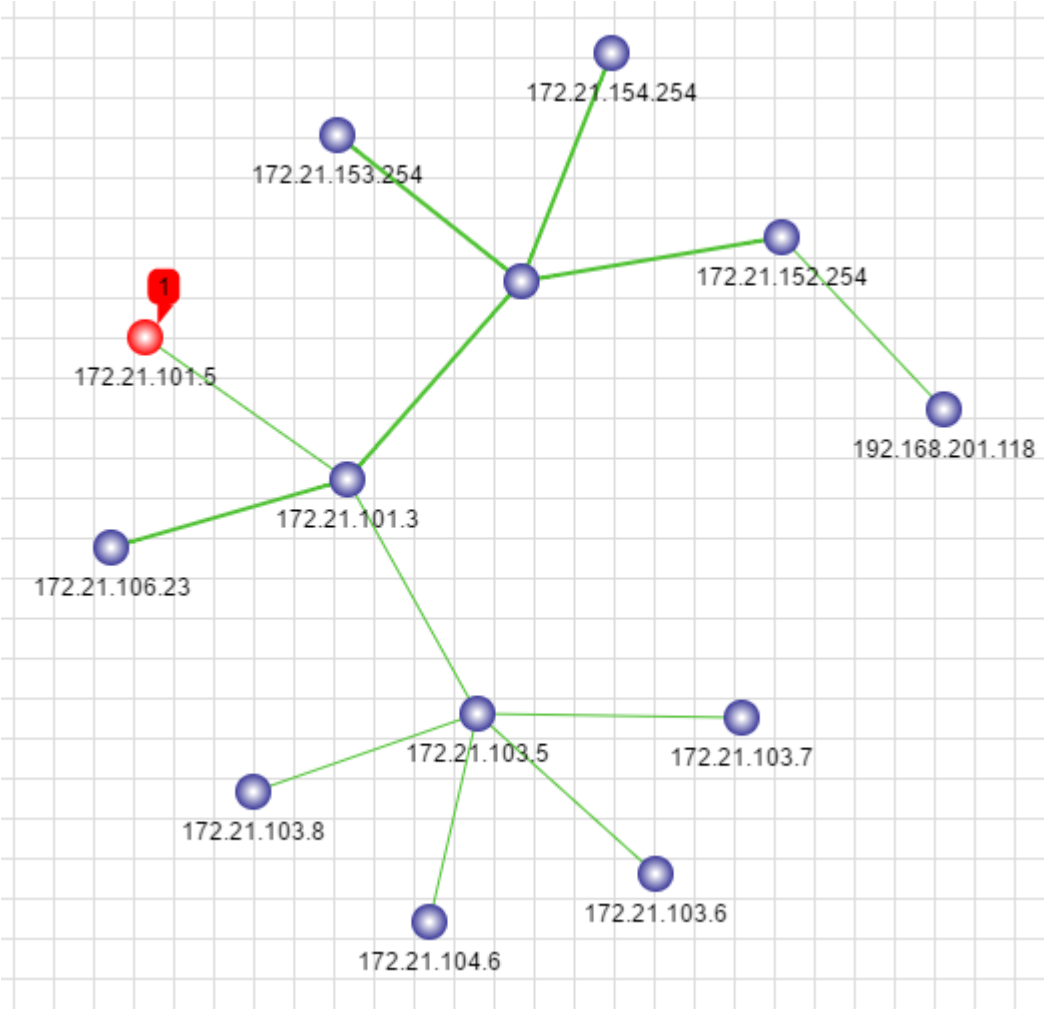
3) Node Mode



You can display the node as an icon.

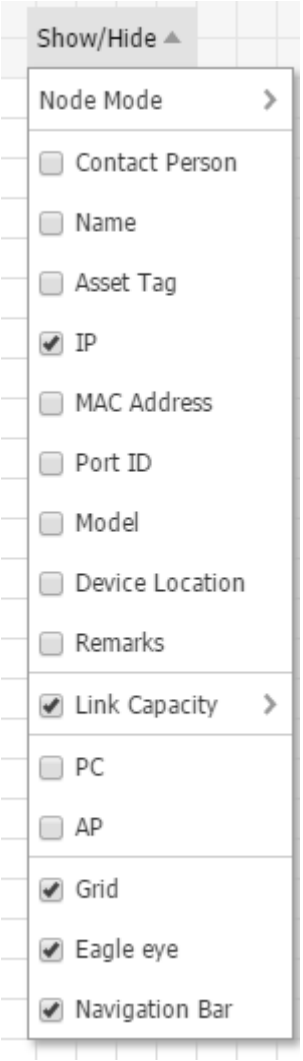


You can display the node as a dot.



4) Display Content

This function enables you to custom the display content, including device information, Link Capacity, PC, AP, Grid, Eagle Eye, and Navigation Bar.



5) Custom Icons

This function enables you to set custom icons.

Double click the node. The **Detailed Device Info and Operation** page appears. Click **Modify Device Icon**

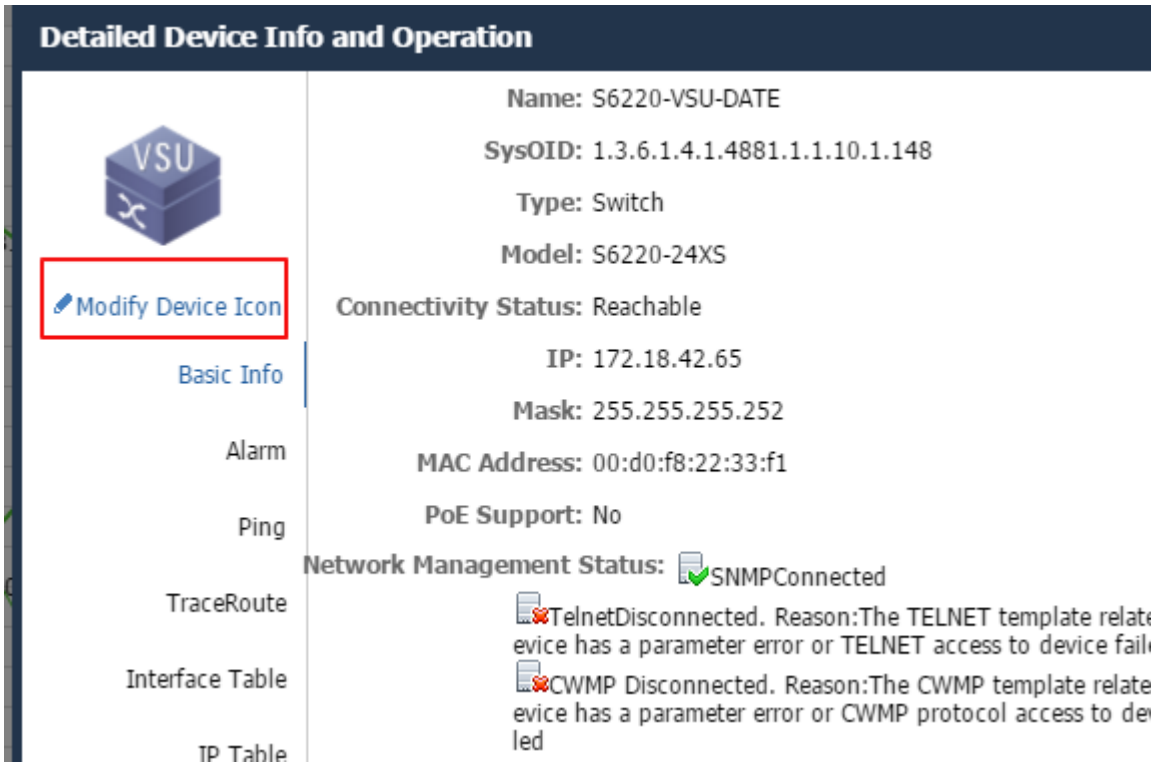


Figure 3.42. Clicking Change Icon

Chapter 4 Advanced

As for network management, do you often encounter the following problems:

- Now there are more than a dozen devices on hand to be upgraded with software , what should I do?
- Device configuration has been modified, and I want to restore now. But there is no backup?
- This interface can only be used by certain people, that interface is used by another person. It's terrible, how to manage so much interfaces?
- Want to see the IP, MAC, PORT mapping information about device interface, but need input a bunch of commands as well!
- Features of Network management software are numerous, but a lot of things cannot be done for configuration.

The service module of the RG-SNC is to provide solutions with special design for the above problems.

Numerous equipment upgrades do not take up your rest time now!

It can be done by **Device Software Management** function. The backup and upgrade of device software can be executed definitely in the time off duty (or network load is lower). It will be done automatically, no impact on the normal operational of network.

Regular backup of device configuration. The network management system achieves intelligent management!

By **Configuration Backup And Restore** function, regular backup, restoration of device configuration can be done. User can even define the baseline version of the device configuration , and system will alert automatically for the change of device configuration .

Binding management for a large number of interfaces, the network management system can help you to achieve!

By **Interface Binding Management** function, user can synchronize interface information which was bound to the devices, and operate the interface binding information easily as well.

Device interface IP, MAC, PORT mapping information, just at a glance!

By **Interface Mapping Management** function, the mapping information of interface is very easy to check. If the mapping information of interface was changed, and how to do? Do not worry, there is regular synchronization function.

Powerful business configuration function!

By **Business Configuration** function, complex business configuration commands are implemented. Periodically change the device password periodically switch SNMP functions, service configuration can help you to do (of course, you'd better not to do so , or else you have to manually synchronize modified information of TELNET module .)

Business configuration module, powerful enough? Do not worry, here provide more.

By **STP Configuration Management** function, it's very convenient to manage interface STP configuration parameters, restore the default configuration and set STP priority of device.

By **Interface Control Plan** function, user can close or open a specific port according to the planning cycle. Of course, plan can be configured manually.

By the way, before you start using them, see **Use guidelines**.

4.1. Use Guidelines

1) Checking SNMP and TELNET template configuration for device

It is required that system devices are configured with the correct SNMP and TELNET templates (which is the precondition to ensure the normal operation of the SNC system).

As in the service module, you can carry out recovery, restoration and other operations on device configuration, so there is a proposal in service module : SNMP configuration for the device, TELNET passwords and other operations should have a unified plan. Otherwise, the SNC system does not work after device configuration is restored.

The Application of TFTP

When backing up device software, issuing device software, backing up device configuration, use the TFTP protocol to transfer files. There is embedded TFTP server in RG-SNC system. During system installation, TFTP configuration has been configured already. Usually, re-configuration is not required.

Service Directory Structure

In the directory navigation of system, user can find “**Advanced**” module easily. “**Advanced**” module has three sub-item: “**Device And Software**”, “**Business**” and “**Device Interface**”.

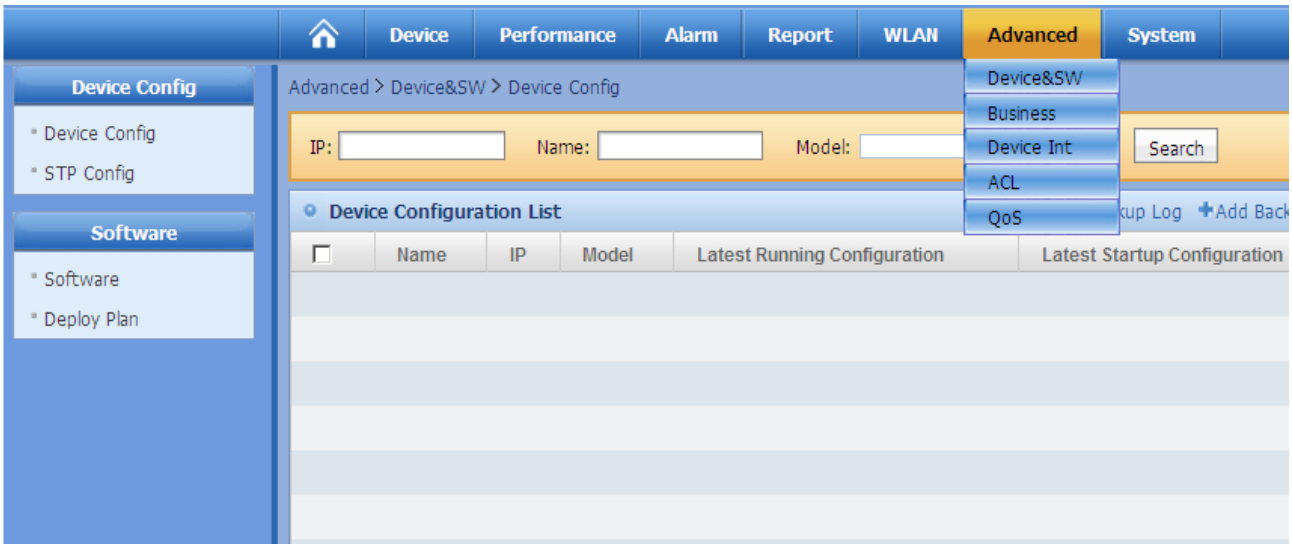


Figure 4.1. Service Directory

”Device And Software” includes backup and restoring of device configuration; STP configuration management; management and deployment function for device software.

”Business” includes the business configuration function for device.

”Device Interface” includes the following functions: binding of device interface, switch plan and mapping management.

4.2. Device Software Management

Brief Introduction

As for the controllable Network Management device, the deployment of device software happens frequently. The operation of backing up and recovering device software is introduced below.

Backup of Device Software

There are two ways to import device software into our system.

1) Go to **Advanced > Device and Software menu**, click **Software Management**. Select **Upload File**.
Select one device to be backed up in **Device**, enter interface Detail Information. Click **Software Backup** in the left operation navigator bar to backup software from device.

These two kind of backup operation is relatively simple, will not go into the details here.

Figure 4.2. Interface “Upload File”

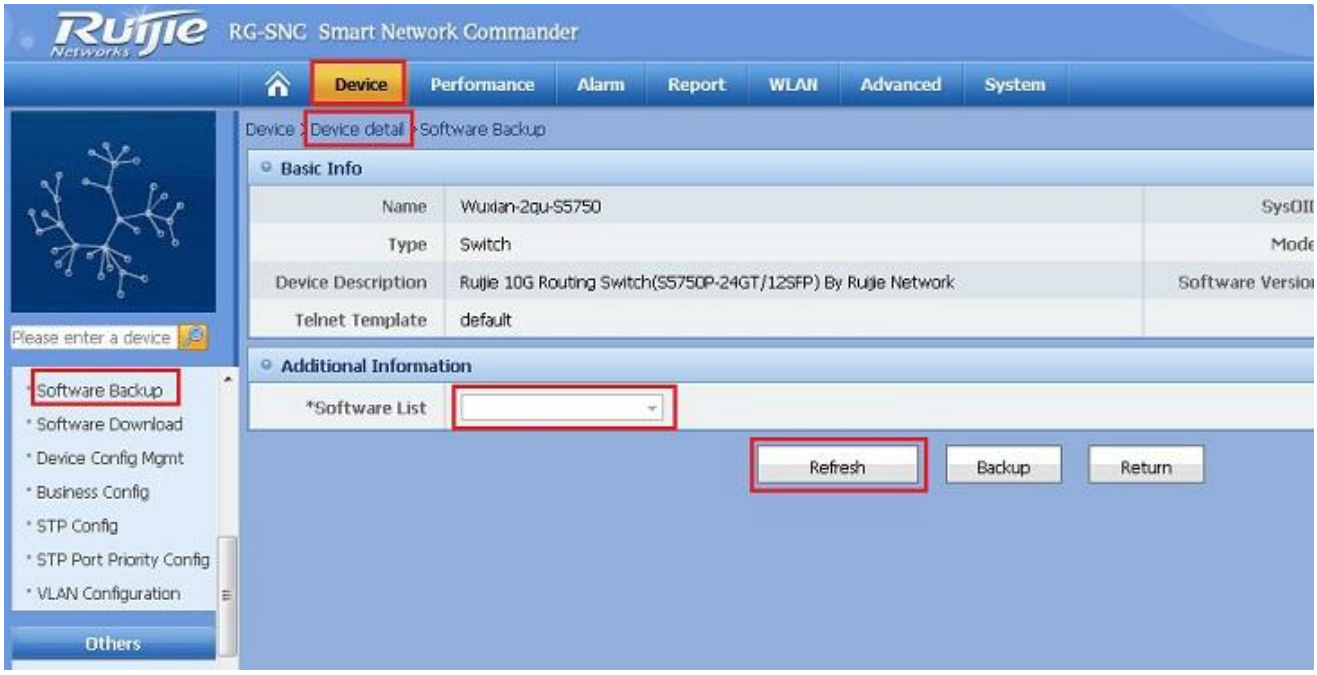
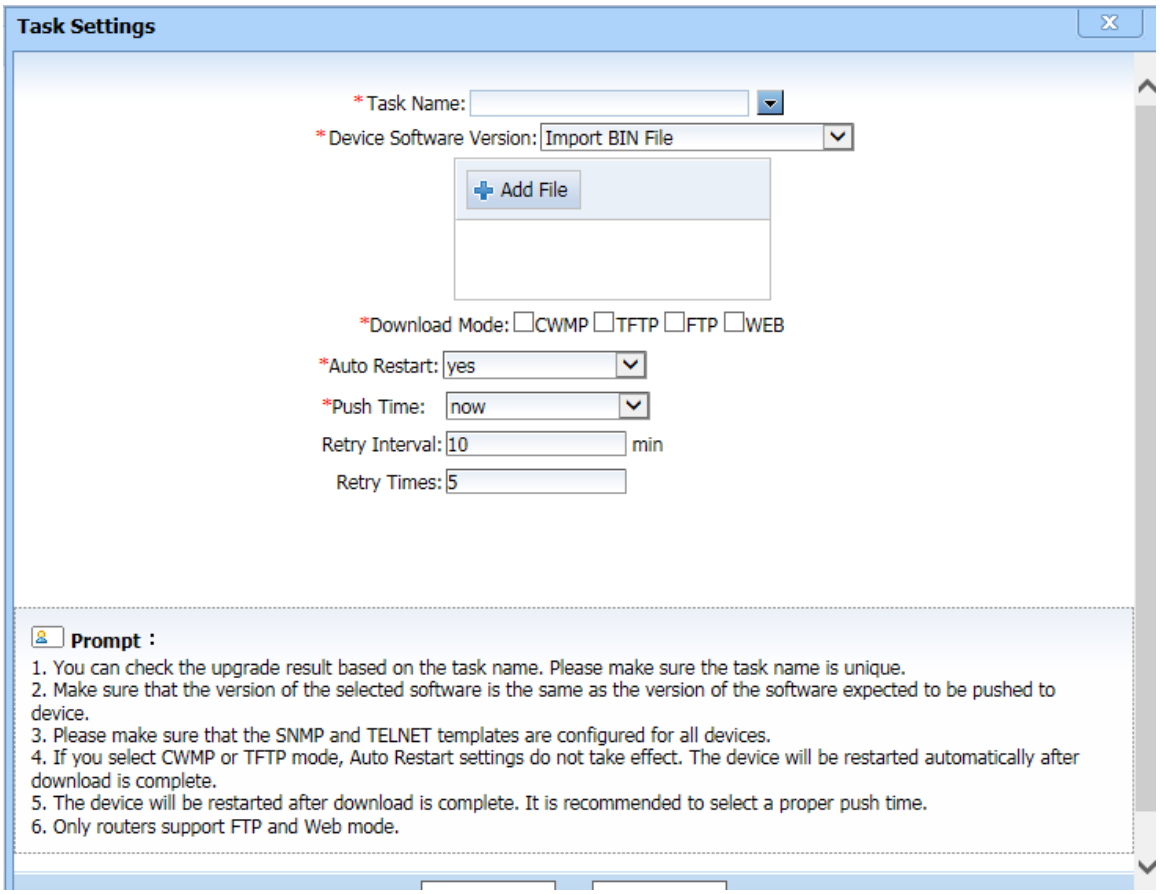


Figure 4.3. Interface “Software Backup”

Software Push

Choose **Advanced** > **Software Push**. The **Software Management** > **Push Management** page appears. Select the target device, click **Push Software** and enter parameters.

Note Only routers support FTP and Web mode.



4.3. Configuration Backup And Restore

Basic concept

- Running Configuration

That is, display configuration information by the **show run** command in the device.

- Startup Configuration

Config.text file in the root directory in the device. System will back up the file via TFTP.

- Baseline

The system allows you to set a particular backup of the running configuration as the baseline version. After setting the baseline version, system will compare the running configuration and startup configuration synced up everytime with the baseline version. If inconsistent information is found, the system will generate alarms automatically.

Brief Introduction

In “**Device Configuration Management**” module, user can capture system configuration (Running Config) or start up configuration (Startup Config) of device immediately or periodically, configuration captured will be stored in the network management server in the form of file. User can view the contents of the file. User can also define a baseline version of the configuration of device and the system will automatically give reminder when device configuration changes.

User can go to **Advanced > Device and Software**” , then enter **Device and Software**; select **Device Config** in the left navigation, enter the **Device Configuration Management**. Its main function is shown in the figure:

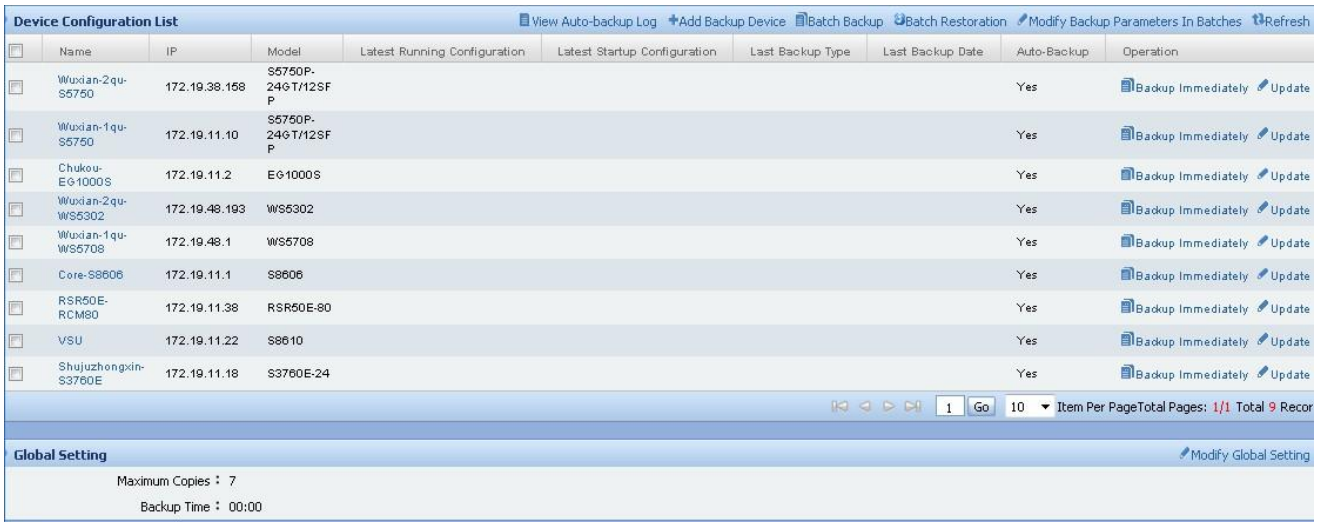


Figure 4.8. Device Configuration List

Device configuration backup and restore mainly involves: **Backup Device Configuration**, **View Device Configuration And Set Baseline**, **Restore Device Configuration**. Other operations are simple and briefly described as follows:

In the **Device Configuration Management** page, click **Refresh** in the area of **Device Configuration List**, then reload backed up configuration information:

As for “Global Setting”, in the global settings, you can view the number of device configuration copies in current system, and keep copies, and the time point of backing up device configuration automatically in current system. Click **Modify Global Setting**, this item could be edited. If user want to check the status of automatic backup in system, user can click **View Auto-Backup Log** in the area of **Device Configuration List**.

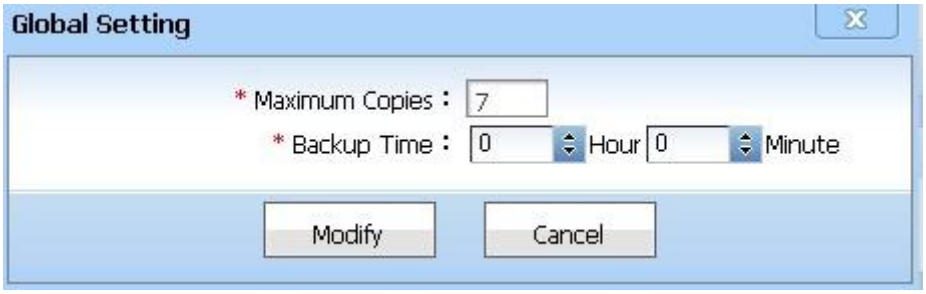


Figure 4.9. Modify Global Setting

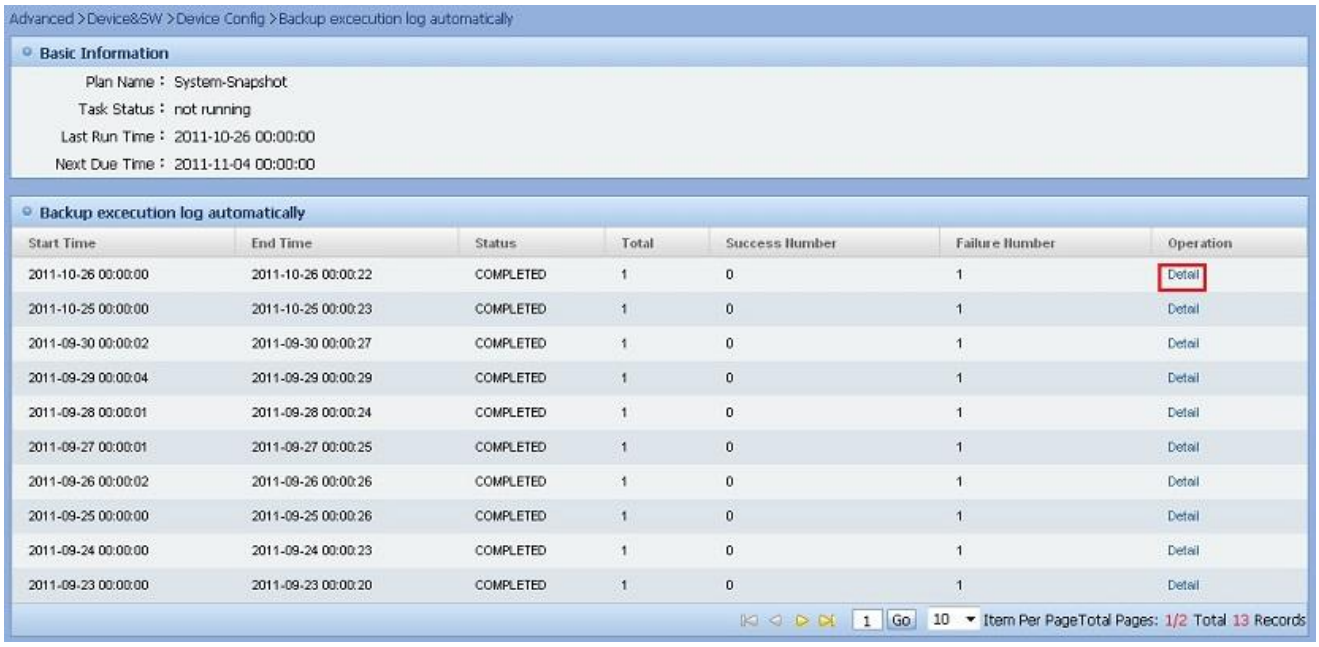


Figure 4.10. View Auto-Backed up Log

Best Practices

Same rules should be set for the TELNET and SNMP configuration of network device. Otherwise, the operation such as restoring configuration, prevents the network management system from accessing your device.

It's enough to backup only important devices automatically. In addition, it's better to arrange the automatic backup after midnight, in order to prevent backing up of devices from impacting the network .

4.3.1. Backup Device Configuration

Operation Steps

Backup device configuration mainly includes the following:

- **Backup Configuration for Single Device**

For backup operation of device configuration, from **Device Configuration** in a single device, click **Backup Device Configuration immediately**. Users can easily navigate to **Device Configuration** page in single-device through two ways.

1) On the **Device Configuration** page, search for the specified device, click the corresponding device name in **Device Configuration List**. (Go to **Advanced > Device And Software** menu and enter **Device And Software** module; select in the left navigation bar to enter **Device Configuration**.)

On the detail Information page of corresponding device, click **Device Configuration Management** connection in the left navigation bar. (In the "device" module, search for the specified device, click the corresponding device name in "**Device List**", you can enter "Detail Information" of corresponding device)

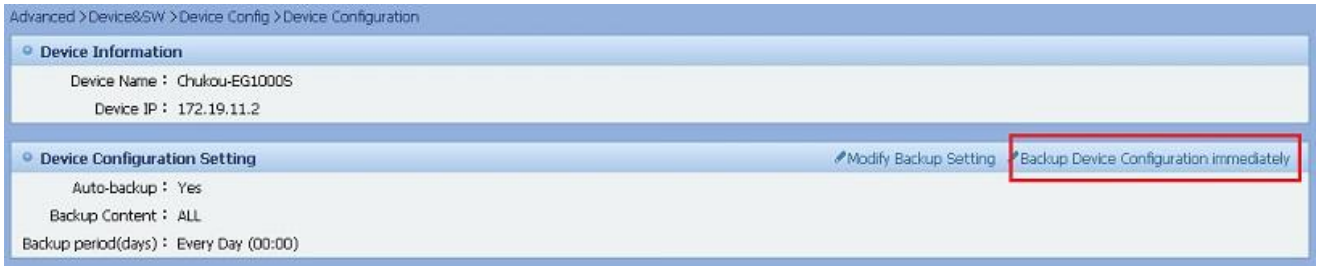


Figure 4.11. Configuration Management For Single Device

- **Batch Backup of Device Configuration**

On the **Device Configuration** page, select the devices to be batch backed up in **Device Configuration List**, click **Batch Backup**. (Go to **Advanced > Device And Software** menu and enter **Device And Software** module ; select **Device Configuration** in the left navigation bar to enter **Device Configuration Management**.)

Figure 4.12. Batch Backup Operation in “Device Configuration Management”

■ **Automatic Configuration Backup**

1) On the **Device Config** page, click **Add Backup Device**, enter “Non-Auto-Back Device List”. (Go to **Advanced > Device and Software** menu and enter **Device And Software**; select **Device Configuration** in the left navigation bar to enter **Device Config**.)

On the **Non-Auto-Back Device List**, select the device to be backed up automatically, click **Enable Auto-backup**”. On the A**dd Backup Device** page, set content for backup and execution cycles here.

After adding operation is completed, if modification is required. select the device you want to modify and click the **Modify Backup Parameters In Batches** on the **Device Config** page to update corresponding backup contents and implementation of appropriate backup cycle.

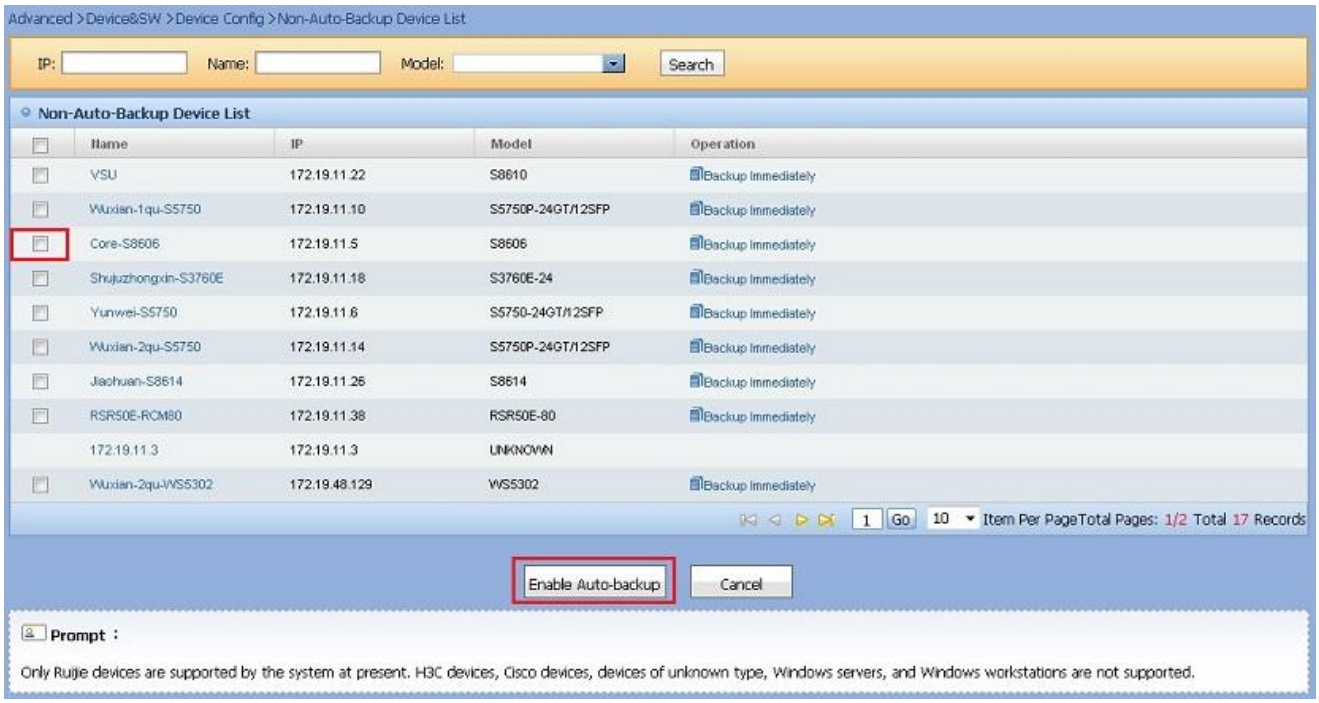


Figure 4.13. Interface “Non-Auto-Back Device List”

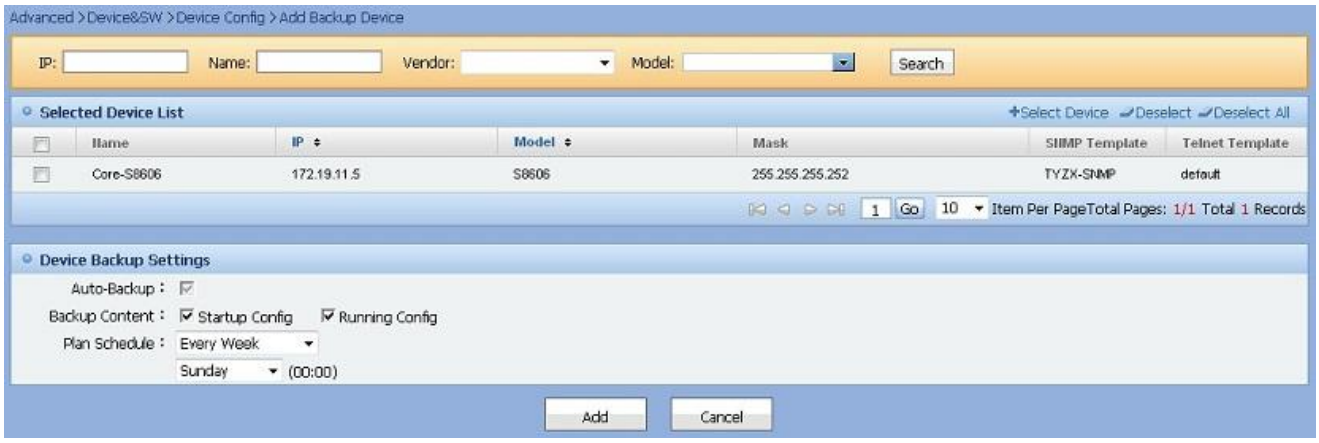


Figure 4.14. Page “Add Backup Device”

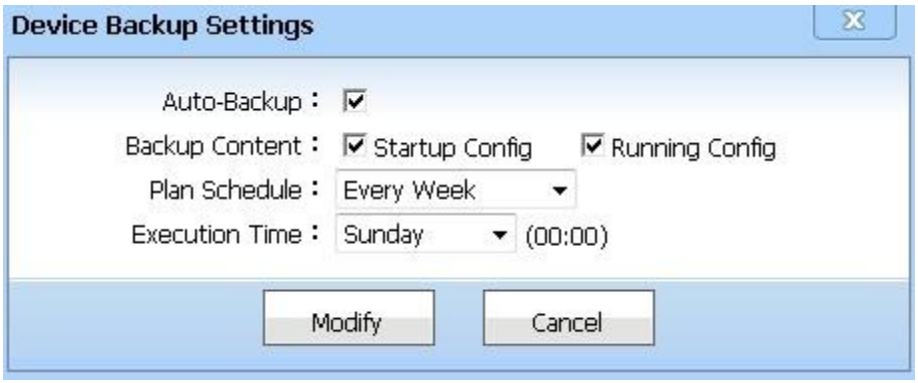


Figure 4.15. Window “Device Backup Settings”

Best Practices

It’s enough to backup only important devices automatically. That is: the device has a backup version or it’s automatic backup device. User can look for other devices, execute the backup operation on the **Non-Auto-Back Device List** page .

4.3.2. View Device Configuration And Set Baseline

View Device Configuration

The following takes the viewing the latest “Running Configuration” of device “192.168.197.144” as an example. the Specific instructions are as below:

- On the **Device Config** page, search for “192.168.197.144” in “Device IP:”. Click **Latest Running Configuration** or **Latest Startup Configuration** to view the latest “Running Configuration” or “Startup Configuration”.(Go to **Advanced > Device And Software** menu and enter Device And Software; select **Device Configuration** in the left navigation bar to enter **Device Config**.
- On the **Device Config** page, search for “192.168.197.144” in “Device IP:”. Click the corresponding device name, enter Configuration Management page for single device (Go to **Advanced -> Device and software** menu and enter **Device And Software** module; select Device Configuration in the left navigation bar to enter **Device Config**.

Of course, on the **Configuration Detail** page for corresponding device, click **Device Configuration Management** in the left navigation bar. (In module “**Device**”, after querying specified equipment, click on corresponding device name in “Device list “, you can enter the “Configuration Detail” of corresponding device.)

Figure 4.16. Configuration Detail page

Baseline Settings For Device Configuration

On the **Configuration Management** page for single device, click **Set to Baseline** of corresponding “Running Configuration” in the “Device Configuration List” . There are two ways for user to navigate to interface “Configuration Management” for single device easily.

- On **Device Config** page, search for specified devices, click the corresponding device name in “Single Device Configuration List”. (Go to **Advanced > Device and Software** menu and enter **Device And Software**; choose **Device Configuration** in the left navigation bar to enter **Device Config**.)
- On the **Configuration Detail** page of corresponding device, click the **Device Configuration** in the left operating navigation bar. (In module “Device”, search specified devices, click on the corresponding device name in “Device List”, you can enter “Detail Information” of corresponding device.)
- On the **Device Configuration Details** page of Running Configuration, click **Set to Baseline**.

Comparison of Device Configuration

Comparison of Device Configuration, is to compare the similarities and differences between the two configuration files, and use highlight format to show the difference between them. System supports two different modes of comparison. One: Comparison for backed up files; Two: before restoration, compare restoration file and “Running Configuration” of current device. Here, We only taking “Comparison for backed up files” for example, such as comparing backup configuration in device “192.168.197.144”.

1) Step 1: On **Device Configuration**, search for “192.168.197.144” by “Device IP:”, click the corresponding device name, enter **Device Configuration** for single device. (Go to **Advanced > Device And Software** menu and enter **Device And Software** module; select **Device Configuration** in the left navigation bar to enter **Device Config**.)

Of course, you can click **Device Config** in the left navigation bar on **Detail Information** of corresponding device. (In module “Device”, search specified devices, click the corresponding device name in “Device List”, you can enter “Detail Information” of corresponding device.)

Step 2: On **Single Device Configuration List**, select two backup “Startup Configuration” in “Single Device Configuration List”, click **Compare** to enter **Compare Device Configuration** page.
Step 3: On **Compare Device Configuration**, you can check the two configuration files by selecting display method of “Difference Line” or “Location Line”.

Figure 4.17. Single Device Configuration List

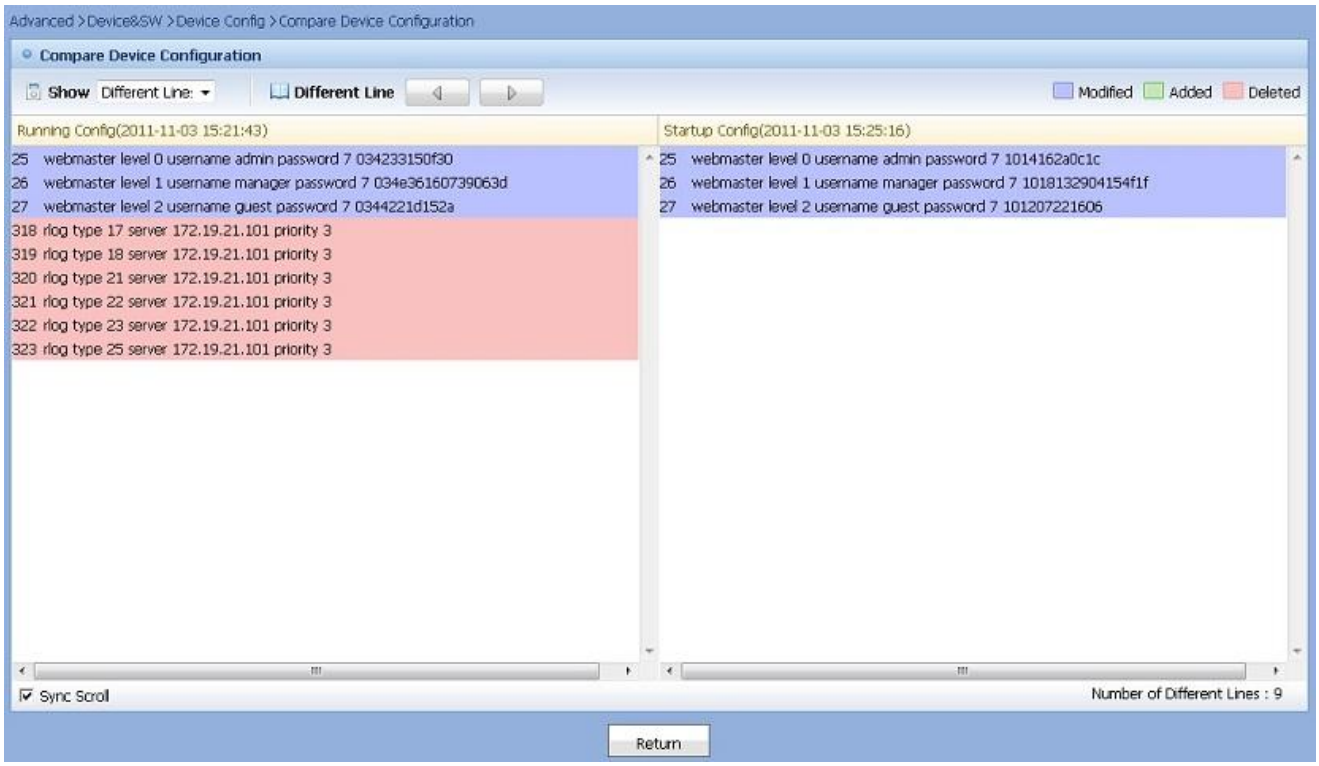


Figure 4.18. Compare Device Configuration

4.3.3. Restore Device Configuration

Restore operation of Device Configuration mainly involves the following:

Restore Single Device Configuration

- Methods one: Click **Restore** on the **Device Config** page. For details, refer to **View Device Configuration And Set Baseline**.
- Method two: On **Configuration Management** of single device, execute operation “Restore” for configuration file on **Single Device Configuration List**. User can be navigated to the **Configuration Management** page of single device easily by two means. On the **Device Config** page, search specified devices, click the corresponding device name in “Device Configuration List”. (Go to **Advanced> Device and Software** menu and enter the **Device And Software** module, choose **Device Configuration** in the left navigation bar to enter **Device Config** page.). On the Detail Information page of corresponding device, click **Device Configuration** in the left operating navigation bar. (In module “Device”, search specified devices, click the corresponding device name in “Device List”, you can enter “Detail Information” of corresponding device.)

Batch Device Restore Configuration

1) Step 1: Select devices to be restored on the **Device Config** page, click **Batch Restoration** to batch restore device configuration.

Step 2: Select backup configuration file to be restored on the **Device Config** page. Note: the default option for target configuration file is baseline.
Step 3: Click **Restore**.

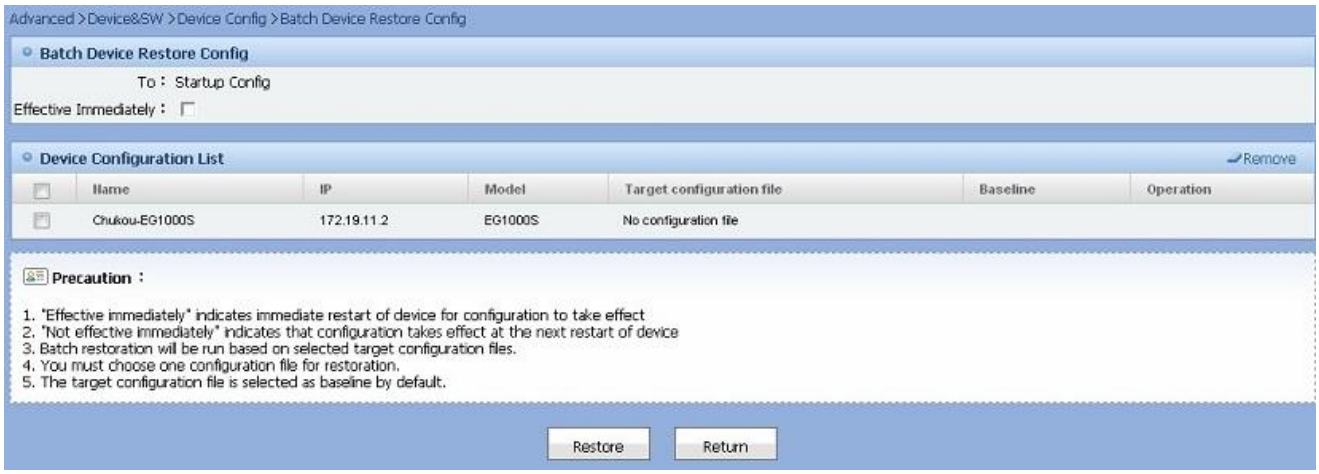


Figure 4.19. Batch Device Restore Configuration

Best Practices

On the **Batch Device Restore Configuration** page, if there is an unconfirmed restored version, user can click **View Difference**.

Only display important devices on the **Batch Device Restore Configuration** page. That is, the device including the backup version or device automatically backed up.

4.4. Business Configuration

Basic Concept

- Configuration Commands

CLI command, that is, operation command deployed after logging in to the device. As for the specific command help, you can view configuration manuals such as “RG - * * series switches configuration manual”.

- Configuration Template

The configuration command set which meets specific business operation, mainly used to facilitate selection of many configuration command operation during business configuration.

- Business Plan

Configuration commands are deployed to the device by system with customization of business configuration plan. System sends configuration commands to the device according to execution schedule within configuration plan. Manual plan can be used as well. When finishing the configuration of plan, user can click **Start Plan** to start.

Brief Introduction

”Business” module is located in the sub-menu of “Advanced” - >”Business”. “Business” is a process to simulate how the user configure device with the CLI command. The steps show how to use “Business” with the configuration of the following commands as example:

```
Ruijie#config
Ruijie(config)# snmp-server view v3userview 1.3.6.1.2.1
Ruijie(config)# snmp-server group v3usergroup v3 priv read v3userview write v3userview
Ruijie(config)# snmp-server user v3user v3usergroup v3 auth md5 md5-auth priv des56 des-priv
Ruijie(config)#snmp-server host 192.168.65.199 traps version 3 priv v3user
Ruijie(config)#end
Ruijie#write
```

Note

CLI configuration above allows SNMP V3 managers to view and configure management variable under node MIB-2 (1.3.6.1.2.1) by using the mode of authentication plus encryption with the user name v3user. The authentication mode is MD5, with password of MD5-Auth, and the encryption mode is DES with the encryption key of DES-Priv. It allows SNMP V3 managers to send trap to 192.168.65.199 with SNMP V3 format by using the mode of authentication plus encryption with the user name v3user. The authentication

mode is MD5, with password of MD5-Auth, and the encryption mode is DES with the encryption key of DES-Priv.

In the “Configuration Command List”, configure the following commands respectively (For the specific configuration process, refer to **Config Command**):

1) config command content: config
snmp-server_view command content: snmp-server view #{ viewName} #{ oidTree}
snmp-server_group command content: snmp-server group #{ groupName} #{ version} #{ auth} #{ opt} #{ viewName}
snmp-server_user command content: snmp-server user #{ userName} #{ groupName} #{ version} #{ auth} #{ encrypted} #{ authPassword} #{ priv} #{ des56} #{ privPassword}
snmp-server_host command content: snmp-server host #{ hostAddr} traps #{ vrf} #{ vrfname} version #{ version} #{ auth} #{ community} #{ udpport} #{ portnum}
end command content: end
write command content: write

On the **Configuration Command Template** page, create template (For the specific configuration process. refer to **Config Template**):

1) snmp-server Template Command: config, snmp-server_view, snmp-server_group, snmp-server_user, snmp-server_host, end, write

On the **Business Plan** page, new manual plan snmp-server. (For the specific configuration process. refer to **Business Plan**.
As for the execution results of task plan, could be shown in the execution log. Refer to **Execution Log For Business Configuration**.

Best Practices

Generally, configuration template includes: config, configuration of corresponding business configuration, end, write and other operations. If you follow the principle to meet specific business operations, it will be more convenient

4.4.1. Config Command

Basic Concept

- Command Parameters

Related Parameters in CLI Command

- Failure Signs

Information output by system if command fails

- Success Signs

Information output by system if command succeeds

Operation Method

The following describes how to add configuration command by taking “snmp-server” as an example. As for deleting configuration command, due to relatively simple; as for modifying the configuration command, due to similar with adding configuration command, will not go into the details here.

Prepare in advance: User must understand the role and format of the command at first before configuring snmp-server host command . The following is relevant specification in “RG-S8600 Series Switch Command Reference Manual V10.2 (3)”:

To specify the SNMP host (NMS) sending trap message, run the configuration command “snmp-server host” in the system view. The “No” form of this command will cancel the specified SNMP host.

snmp-server host host-addr traps [vrf vrfname] [version { 1 | 2c | 3 [auth | noauth | priv]] community-string [udp-port port-num][notification-type]

1) Step 1: On the **Advanced > Business** submenu, click **Config Command List** in the left navigation bar, then enter the **Config Command List** page .

Step 2: On the **Config Command List**, click **Add Command** to enter **Command Definition** page.
Step 3: Considering there are many parameters needed for the command, click label **Parameters** to add command parameters in advance.

Step 4: Click **Add** and input the following items in the pop-up **Parameters** dialog box, in turn: “Name” is “hostAddr”, “Default” is “empty” and “Optional” to “No “, then click **Finish**.
Step 5: Repeat Step 4, and add in order of “Vrf”, “vrfname”, “version_f”, “Version”, “auth”, “community”, “udpPort”, “portNum”, “notificationType”.
Step 6: Switch to label **Details**. Click **Edit Command** within “Command Content”, then show dialog **Edit Command**.
Step 7: In dialog box **Edit Command**, enter “snmp-server host”, click **Insert Text**. Select **hostAddr** in Available Parameters, click **Insert Parameters**. Then insert text “traps”, insert parameters “vrf”, “vrfname”, “version_f”, “version”, “auth”, “community”, “udpPort”, “portNum”, “notificationType”. When input is complete, click **Update** to close dialog box **Edit Command**.
Step 8: On the **Command Definition** page, if there is “Error” signs or special “Success” signs, click corresponding **Edit Command** to input related content.
Step 9: On the **Command Definition** page, input “Name” with “snmp-server_host”, select “Compatibility” with “Rui Jie”, click **Finish**. The adding process ends.

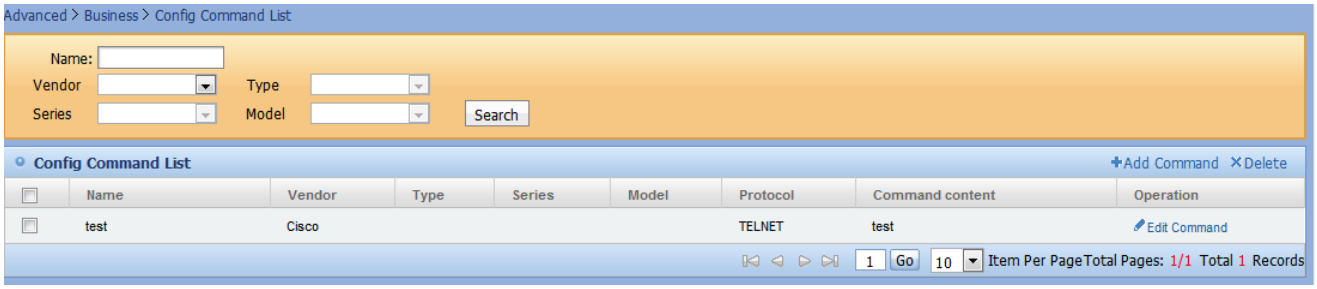


Figure 4.20. Config Command List

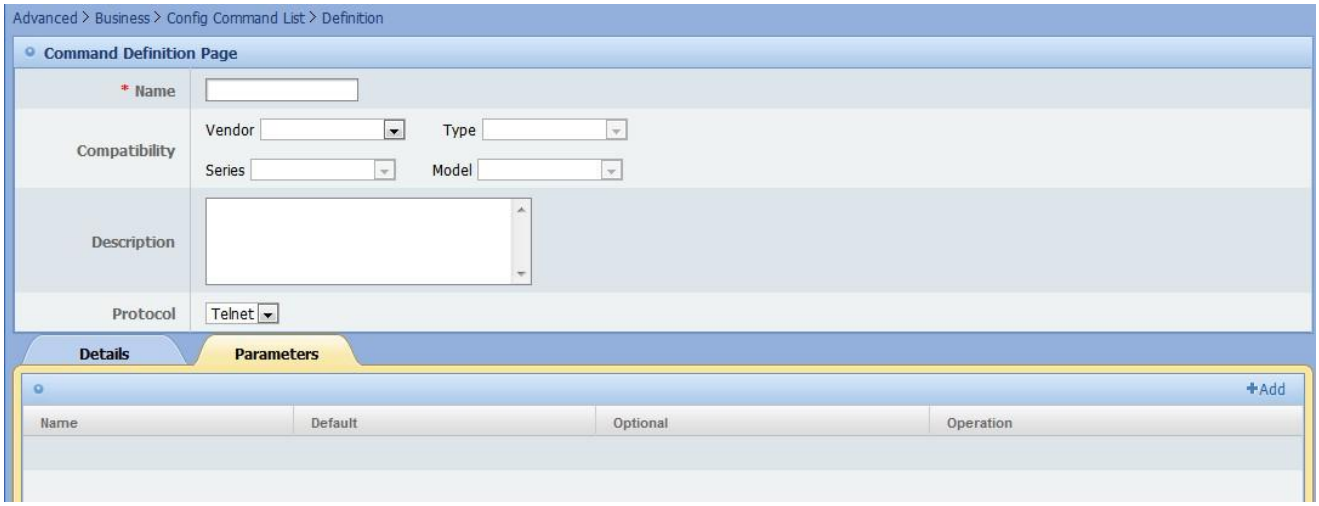


Figure 4.21. Command Definition

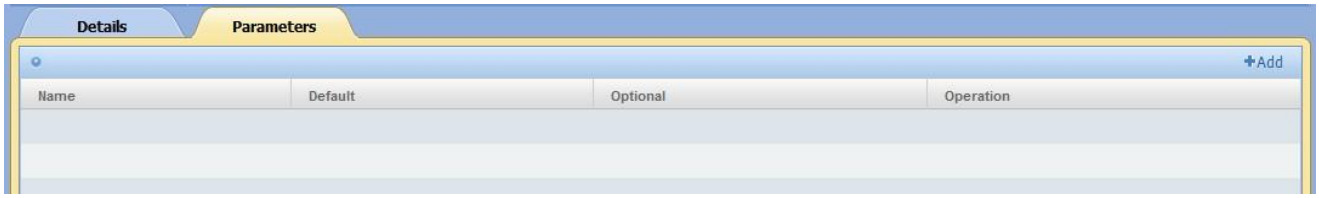


Figure 4.22. Add Parameters

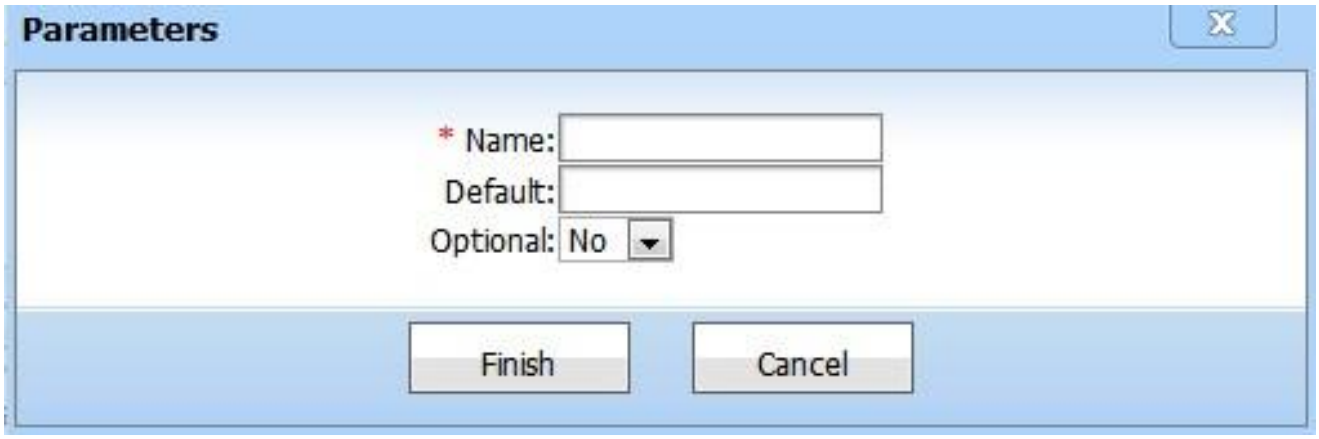


Figure 4.23. Parameters setting page

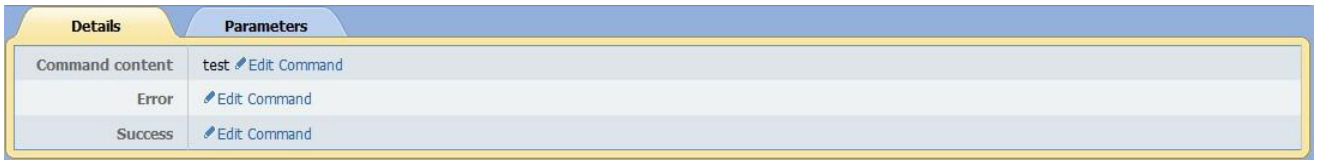


Figure 4.24. Command Details

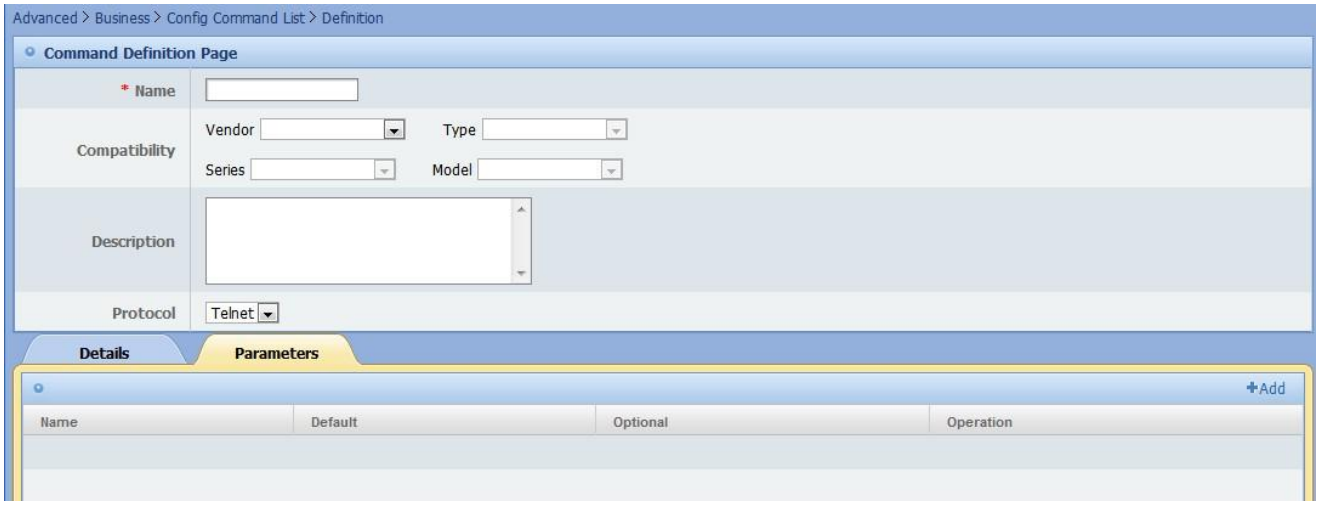


Figure 4.25. Command Definition page

4.4.2. Config Template

Basic Concept

The following describes how to configure a Template by taking “snmp-server” as an example. As for deleting a template, due to relatively simple ; As for updating a template, due to similar with adding Configuration Template, will not go into the details here.

Preparation in Advance : The following configuration commands already exist in system .(As for how to add “Configuration Command”, refer to Config Command):

- Content of Command config: config
- Content of Command snmp-server_view: snmp-server view #{ viewName} #{ oidTree}
- Content of Command snmp-server_group: snmp-server group #{ groupName} #{ version} #{ auth} #{ opt} #{ viewName}
- Content of Command snmp-server_user: snmp-server user #{ userName} #{ groupName} #{ version} #{ auth} #{ encrypted} #{ authPassword} #{ priv} #{ des56} #{ privPassword}

- Content of Command snmp-server_host: snmp-server host #{ hostAddr} traps #{ vrf} #{ vrfname} version #{ version} #{ auth} #{ community} #{ udpport} #{ portnum}
- Content of Command end: end
- Content of Command write: write

1) Step 1: Go to **Advanced > Business** submenu, click Template List in the left navigation bar, then enter the **Template List** page.

Step 2: On the **Template List** page, click **Add Template** and go to the **Template Definition** page.
Step 3: On the **Command** tab, click **Add Command**, then pop-up the **Select Command** dialog box.
Step 4: On the **Select Command** dialog box, search “Config”, “snmp-server_view”, “snmp-server_group”, “snmp-server_user”, “snmp-server_host”, “end” and “write”. Then add it.
Step 5: On the **Select Command** dialog box, adjust the order of commands by clicking the operation button in the **Operation** column. To make the order: “config”, “snmp-server_view”, “snmp-server_group”, “snmp-server_user”, “snmp-server_host”, “end”, “write”
Step 6: On the **Template Definition Page**, fill in “Template Name” as the “snmp-server”. Then the configuration template is added.

Additional features: Sometimes, in order to implement more features for the same template, or, to avoid configuring the same template, user can use “Parameter” and “Rule”. Setting “snmp-server_host” only when input parameters “needTrap” is “true” will be taken as an example below.

1) Step 1: Click **Add** on the **Parameter** tab, fill in “Name” with: “needTrap” in the pop-up “Parameter” dialogue framework,.

Step 2: On the **Rules** tab, click **Edit** on the pop-up “Edit Rule” dialogue framework.
Step 3: Click **Add Step** on the **Edit** rule framework for dialogue.
Step 4: On the **Edit Rule** dialog box, choose **Command** and click **Insert Command** in line **Template Command**.
Step 5: On the **Edit Rule** dialog box, click **Add End Step**.
Step 6: Repeat from step 3 to step 5, followed by the “Add Step” “snmp-server_group”, “snmp-server_user”.
Step 7: Click **Add Step** on dialog box **Edit** rule.
Step 8: On the **Edit** rule dialog box, select “needTrap”, “equal” one by one in line “If statement”, then input “true”, click **If Stat**.
Step 9: On the **Edit** rule dialog box, select “snmp-server_host” in the line “Template Command” , click **Insert Command**.
Step 10: On the **Edit** rule dialog box, click **End Stat**.
Step 11: On the **Edit** rule dialog box, click **Add End Step**.
Step 12: Repeat step 3 to step 5, followed by the “Add Step”, “Insert Command”, “Add End Step”.
Step 13: On the **Edit** rule dialogue box, click **Update** to finish editing the rule.

Figure 4.26. Config Template List

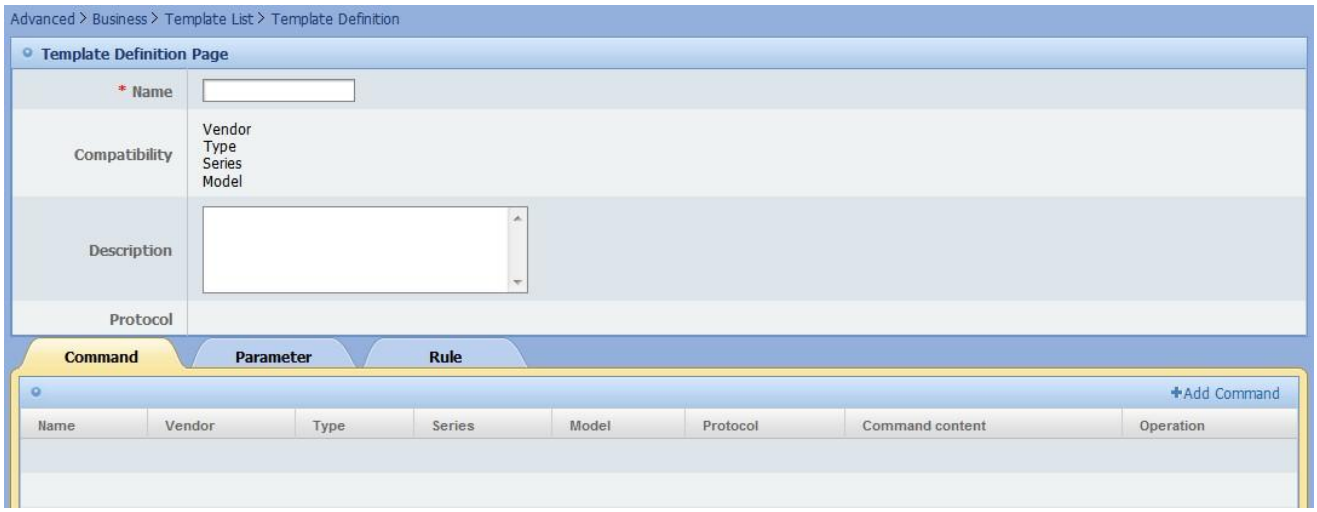


Figure 4.27. Template Definition Page

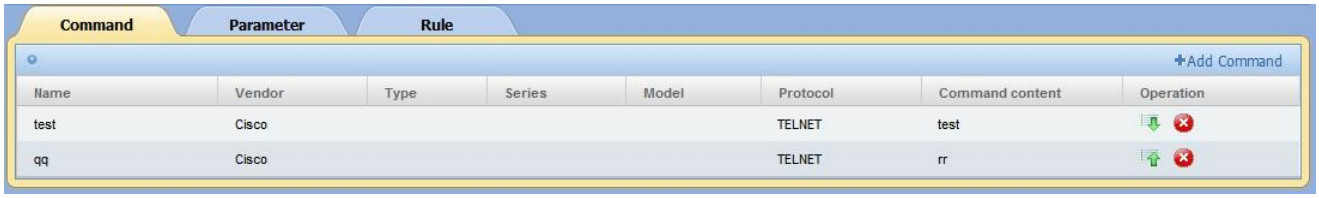


Figure 4.28. Template Command Page

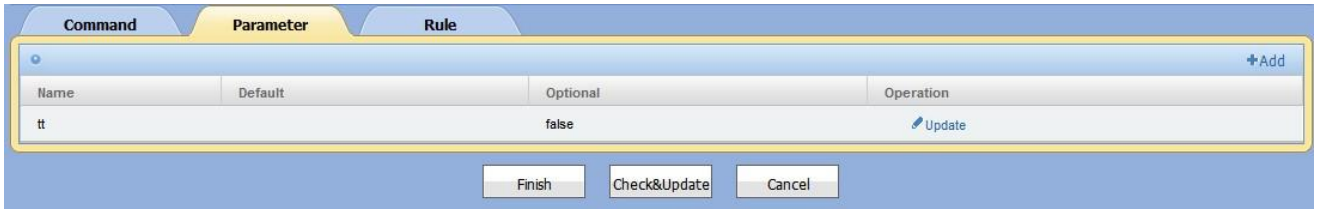


Figure 4.29. Template Parameter Page

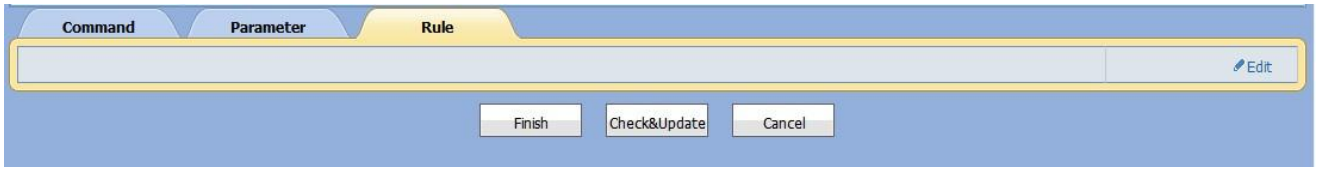


Figure 4.30. Rule Content Page

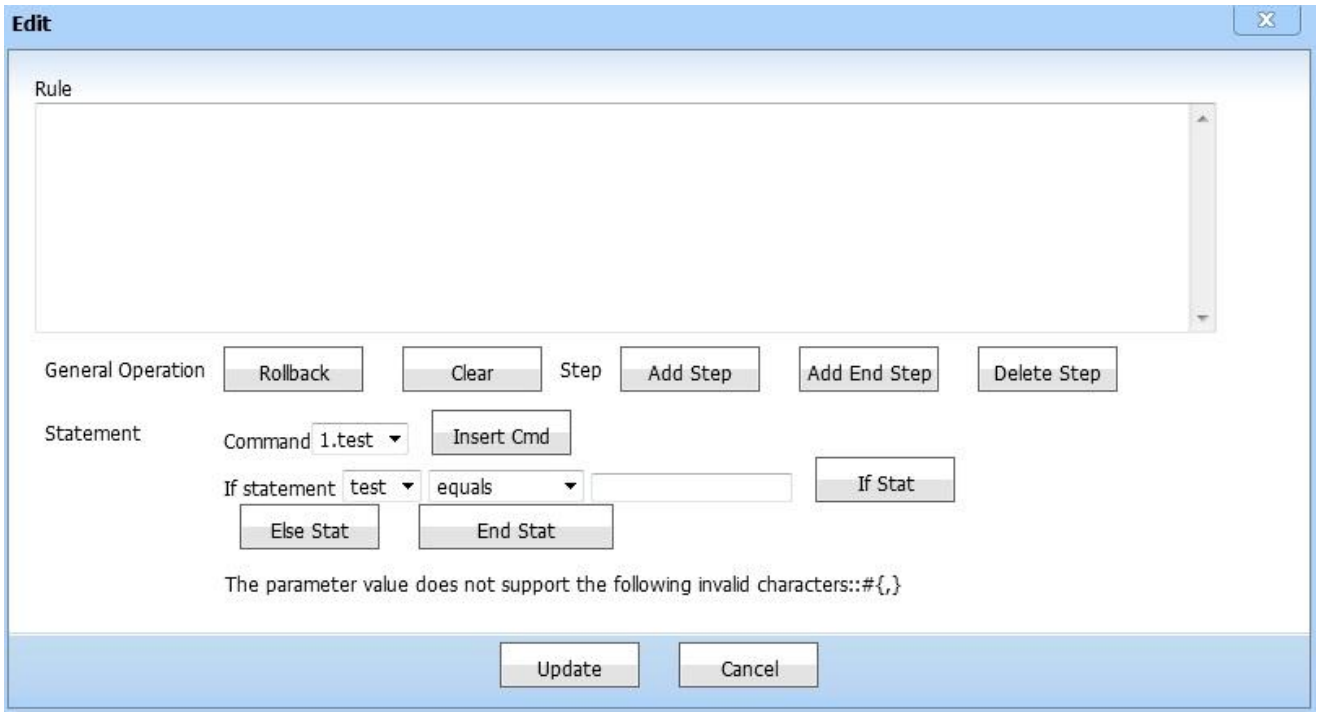


Figure 4.31. Edit Rule Page

Best Practice

Once rule content is configured, the system will only support the operation steps in rule content.

4.4.3. Business Plan

Basic Concept

- **Automatic Plan**

The plan is run automatically by the background. Users can customize the period and valid time of running. Note: Automatic Plan needs to be actived before running.

- **Manual Plan**

The plans need to be started by user. Of course, the automatic plan, in the case of being activated, can also be started manually.

Operation Method

The following describes how to add business configuration Plan by taking “snmp-server” as an example. As for deleting business configuration Plan, due to relatively simple; as for updating the business configuration plan, due to similar with adding business configuration Plan, we will not go into the details here.

Preparation in Advance: The following “Configuration Template” already exists in system. (As for how to add “Configuration Template”, refer to **Config Template**):

- Template Command of config: config
- Template Command of snmp-server: snmp-server_view, snmp-server_group, snmp-server_user, snmp-server_host
- Template Command of end: end
- Template Command of write: write

1) Step 1: Go to **Advanced > Business** submenu, click **Business Plan** in the left navigation bar , then enter the **Business Plan** page.

Step 2: On the Business Plan page, click **Add** to start **Add Plan**.
Step 3: Click **Select Template** on the **Add Plan** page. Select “snmp-server” in pop-up window **Select Template**, then click **Select**.
Step 4: Click **Next**, then go to the **Template Parameter Setting** page. User can input corresponding configuration parameters here. (As here are more parameters, will not describe them in detail. See the following screenshot for Configuration Template Parameter) .
Step 5: Click **Next** and enter **Preview** to check whether the inputted corresponding parameters have problem or not.

Step 6: Click **Next**, select the device to be deployed with command. Click **Select Device**. Search and select the corresponding device: “192.168.197.144”, “192.168.197.190” in the pop-up dialog box **Available devices list to be selected**. Click **Add**.
Step 7: Click **Next** and enter the **Plan Setting** page. Fill in the “Plan Name” as the “snmp-server”, “Plan Type” as “Automatic Plan”, “Start Time” as “2010 - 08-12 11:10”, “End Time” as “2010-08-19 12:00”, “Plan Schedule” as “12:00 Daily”.
Step 8: Click **Finish** to return to the **Business Plan** page, then **Activate** the Plan. So far, the plan addition is complete.

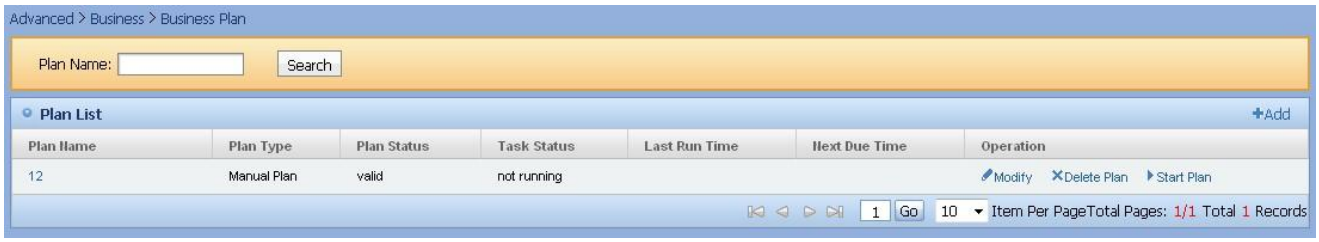


Figure 4.32. Business Plan

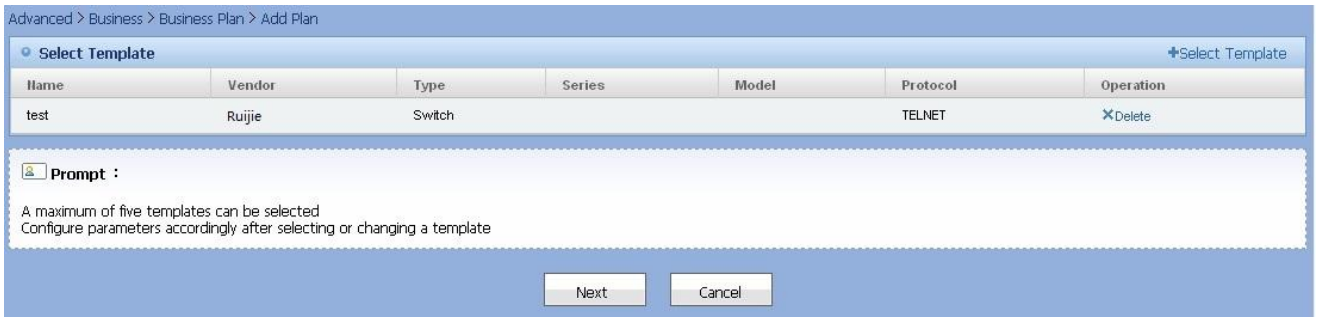


Figure 4.33. Select Configuration Template

Figure 4.34. Template Parameter Setting

Figure 4.35. Preview

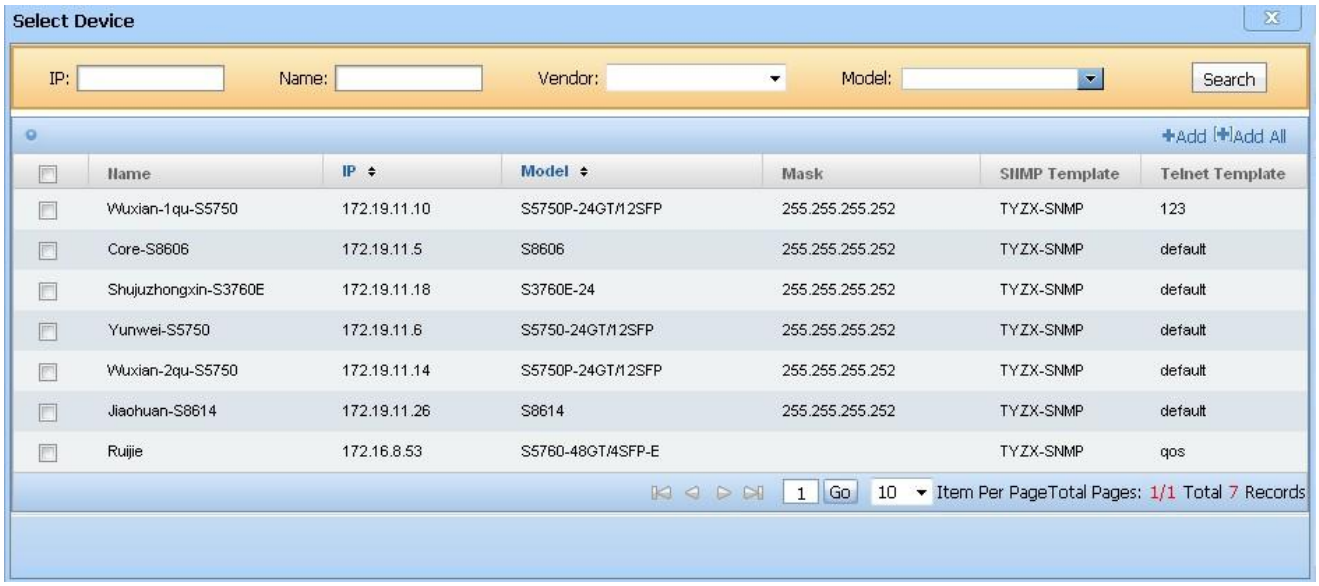


Figure 4.36. Select Device

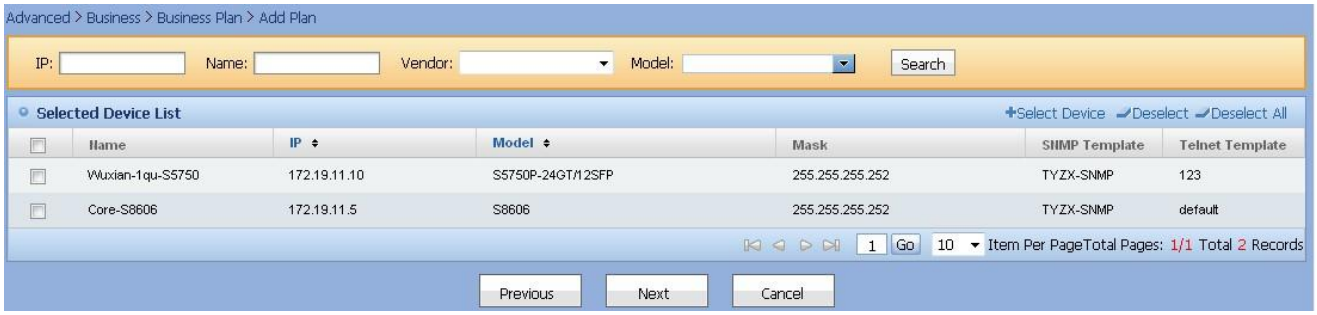


Figure 4.37. Selected Device List

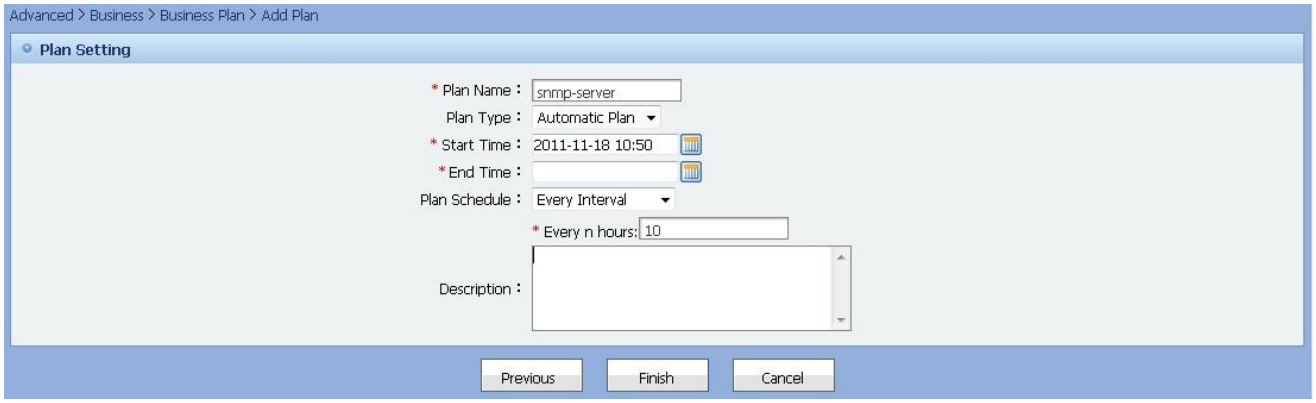


Figure 4.38. Plan Setting

4.4.4. Execution Log For Business Configuration

The following describes how to check the execution log for Business Configuration and how to “Re-execute” the abnormal task by taking “snmp-server” as an example.

Check the Running of the Plan

Advance preparation: Business plan “snmp-server” already exists in system. It has been activated and is running. For specific plan configuration, refer to **Business Plan**.

■ **Method One:**

1) Step 1: Go to **Advanced > Business** submenu, click **Business Plan** in the left navigation bar, then enter the **Business Plan** page .

Step 2: Search “snmp-server” on the **Business Plan** page. If “snmp-server” is found, click corresponding program name in the Plan List to enter the **Plan Detail** page.

Step 3: Select the last action on the **Plan Detail** page ,click **Detail** to check the running conditions of plan.

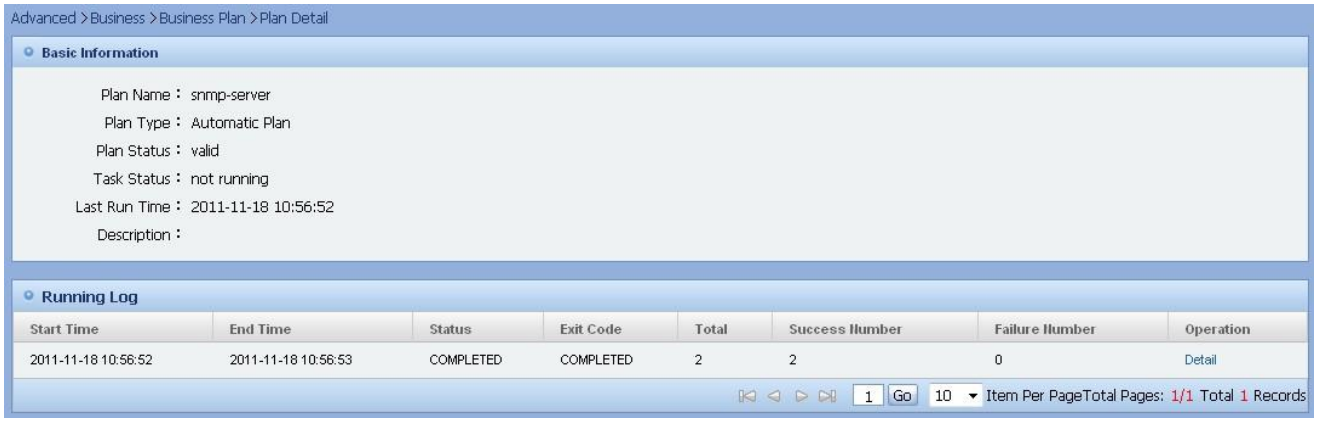


Figure 4.39. Plan Details

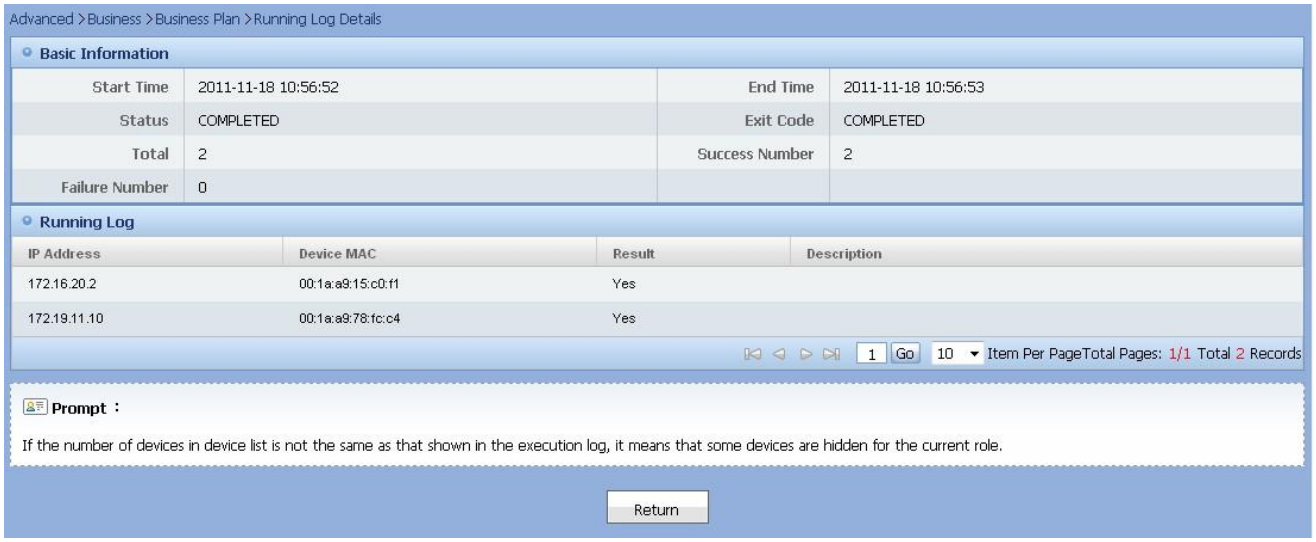


Figure 4.40. Running Log Details

■ **Method Two:**

1) Step 1: Go to **Advanced > Business** submenu, click **Execution Log** in the left navigation bar, then enter the **Execution Log** page .

Step 2: Search “Template” with “snmp-server” on the **Execution Log** page.

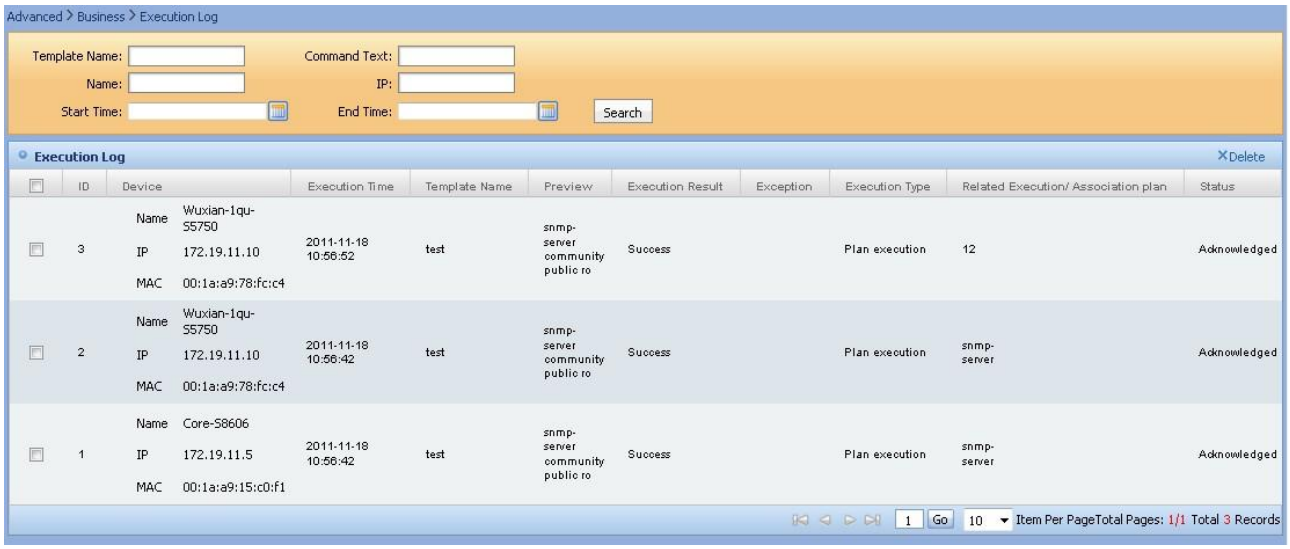


Figure 4.41. Execution Log

”Re-execute” Exceptional Task

In the example above, we found execution fails in the device with IP “192.168.51.251”, the following describes how to “Re-execute” the task.

1) Step 1: Go to **Advanced > Business** submenu, click **Unacked Exception Log** in the left navigation bar, then enter the **Unacked Exception Log** page .

Step 2: Search for IP address “192.168.51.251” on the **Unacked Exception Log** page.

Step 3: Click **Re-execute** of the found result on the **Unacked Exception Log** page.

Figure 4.42. Unacked Exception Log

4.5. STP Configuration Management

Brief Introduction

The STP Configuration Management includes: “Port Priority Configuration” and “STP Parameter Configuration”. “Batch STP Parameter Configuration” can be done here.

We will introduce how to set the “Port Priority Configuration” of “port 1” on device “192.168.197.164” to “128”, and how to update the “STP Parameter Configuration” for this device. As for “Batch STP Parameter Configuration”, due to similar with the operation to single device, will not go into the details here.

Port Priority Configuration

1) Step 1: Go to **Advanced > Device and Software** menu, click **STP Configuration** in the left navigation bar, then enter the **STP Config** page .

Step 2: Search for “192.168.197.164” on the **STP Config** page, click **Priority Setting** to enter the **Port Priority Config** page.

Note

On the **Details** page for the corresponding device, click **Port Priority Config** in the left navigation bar. It works also. (In the “Device” module, search the specified device and click the corresponding device name in the “Device List”, go to “Details” of corresponding device.)

Step 3: On the **Port Priority Config** page, select “Port 1” in the area “Device Interface List” , select “Port Priority” as “128” in the area “STP Port Priority Configuration”, click **Confirm**.

Figure 4.43. STP Configuration page

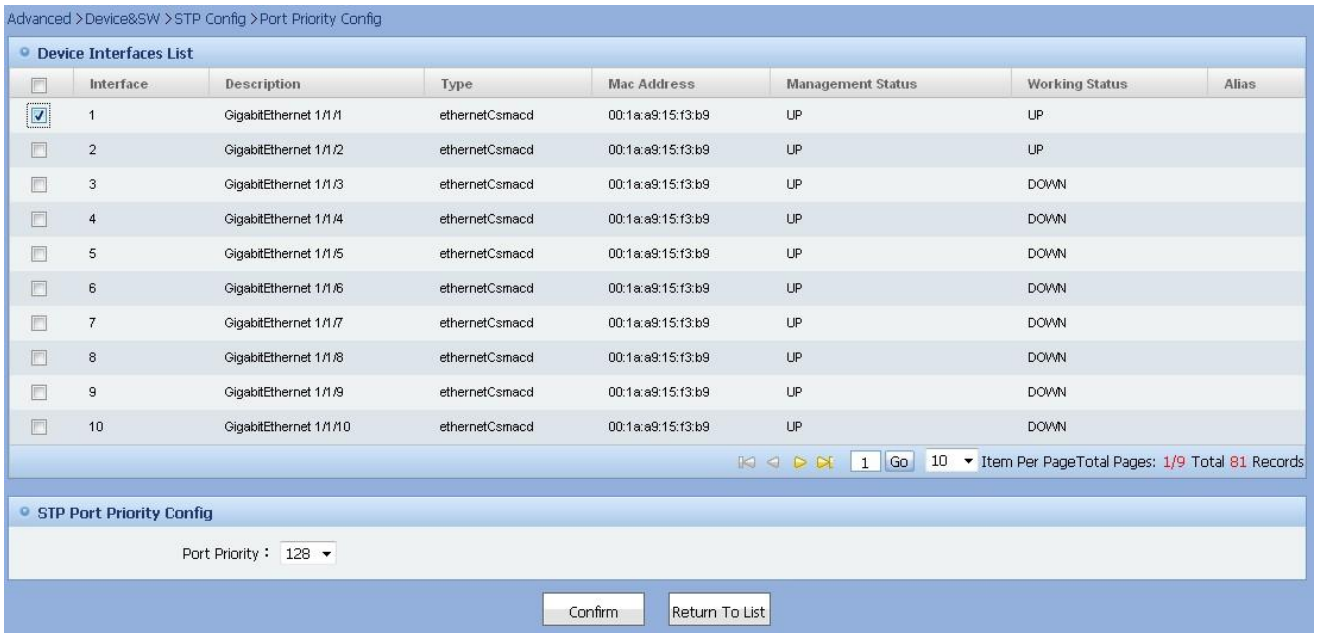


Figure 4.44. Port Priority Configuration

STP Parameter Configuration

1) Step 1: Go to **Advanced > Device and Software** menu, click **STP Configuration** in the left navigation bar, then enter the **STP Config** page .

Step 2: Search for “192.168.197.164” on the **STP Config** page, click **Parameter Setting** to enter the **STP Config** page.
Step 3: On the **STP Config** page, suggest user do “Sync” operation before updating corresponding configuration. Of course, “Default” can be done as well to restore the configuration recommended by system.

Additional Description: Batch STP Parameter Configuration could be used in “Step2”. As process is similar, it will not be illustrated repeatly.

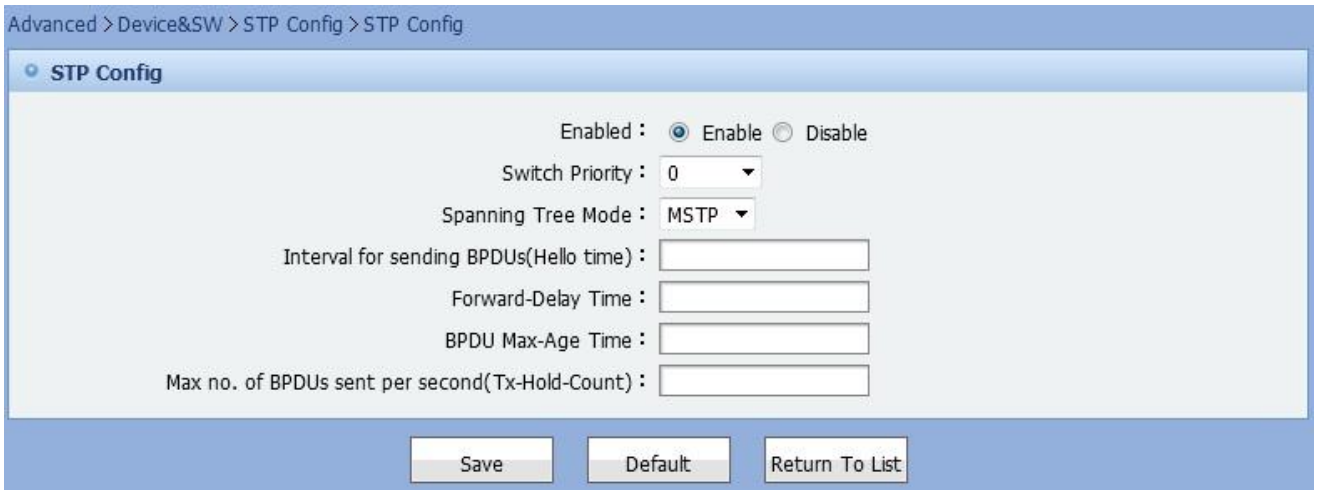


Figure 4.45. STP Parameter Configuration

4.6. Interface Binding Management

Basic Concept

- **Layer 2 MAC, PORT**

Binding MAC and PORT on the device.

- **Layer 3 IP, MAC, and PORT**

IP, MAC, PORT binding operation on the device. Provided that the MAC in device forwarding list, can find the IP of PC

Brief Introduction

Interface binding management mainly aims to manage the function of the device interface to binding accessed MAC, that is, import, export, add, delete function for Device Interface Binding.

The following introduce in detail, how to synchronize interface binding data of “192.168.197.164”, as well as, how to add to bind “port 1” of this device to “00:25:64: c5: cd: 60”. As for the import, export, delete function of equipment interface binding , the interface is more clearly. Not repeat this instructions .

- **View Device Interface Binding**

1) Step 1: Click **Devices** menu on the **Device List** page, search for “192.168.197.164”, enter the device details page. Step 2: On the **Device detail** page, click **Int Binding Sync List**” on the left navigation bar, enter the **Int Binding Sync List** page, you can view the corresponding interface binding information.

Note

User can also search for “192.168.197.164” on the **Int Binding Sync List** page, to view the corresponding interface binding information.

Figure 4.46. Interface Bindings Sync List

- **Synchronization of device interface binding**

1) Step 1: Go to **Advanced > Device Int** menu, click **Int Binding Sync** on the left the navigation bar, enter the **Int Binding Sync** page.

Step 2: Click **Select Device**, search for “192.168.197.164” in the pop-up dialogue **Select Device**, select the appropriate device, click **Add**.
Step 3: Click **Start** and enter the **Device Interface Binding Synchronization Log**, waiting for the finish of “Synchronization” here. So far, the synchronization ends.

Note

Additional instructions: “Int Binding Syn” is mainly batch synchronization of the device. As for Interface Synchronization for a single device, in the interface “Details” of corresponding device, user can click **Int Binding Sync List** on the left navigation bar, then enter the **Int Binding Sync List**. User can also click **Sync** here. (i.e. search specified equipment in the “Device “module, click on corresponding device name in the “device List”, user can enter the **Details** page of corresponding device.). This relatively simple process will not be described in detail.

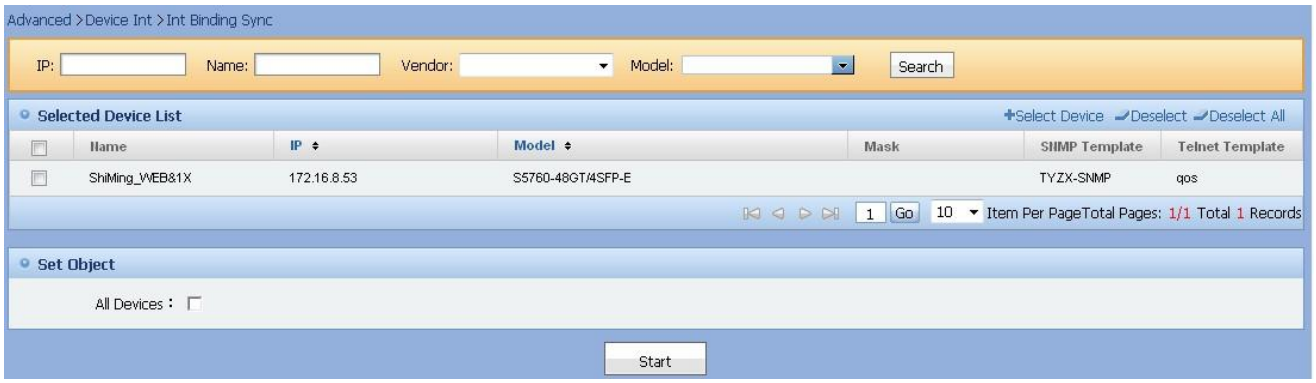


Figure 4.47. Interface Binding Synchronization

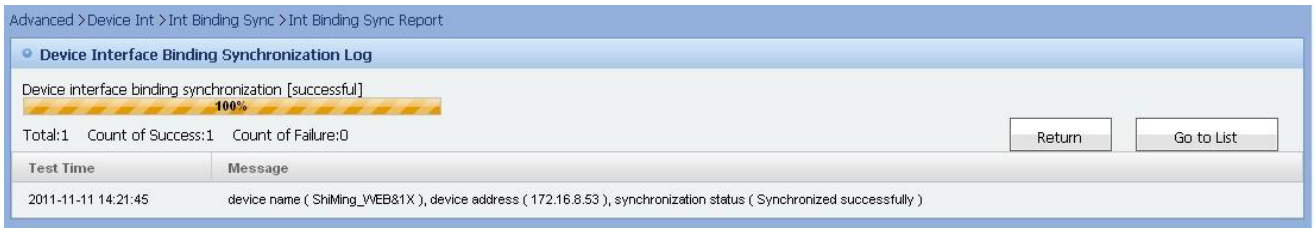


Figure 4.48. “Device Interface Binding Synchronization Log

■ **Add Interface Binding For Device**

1) Step 1: Go to **Advanced > Device Int**, click **Int Binding Mgmt** on the left navigation bar, enter the **Int Binding Mgmt** page.

Step 2: Click **Add** and enter the **Add Int Binding** page .
Step 3: On the **Add Int Binding** page, user can click **Wizard Settings** in the “IP” and enter the **Device List** page. Then search for “192.168.197.164” here, click **Next** and enter the **Interface Select** page. Select “port 1” here, click **Finish** and return the **Add Int Binding** page.

Note

Additional Description: This step can also be equivalent to filling “IP” with “192.168.197.164”, “interface” with “1”.

Step 4: Fill in “00:25:64:c5:cd:60” in the “Binded MAC” on the **Add Int Binding** page . Of course, You can also select the MAC address in **Wizard Setting**
Step 5: On the **Add Int Binding** page, click Add to complete the operation.

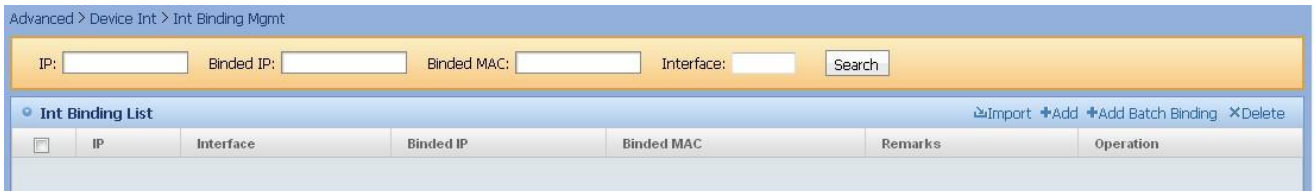


Figure 4.49. Interface Binding Management

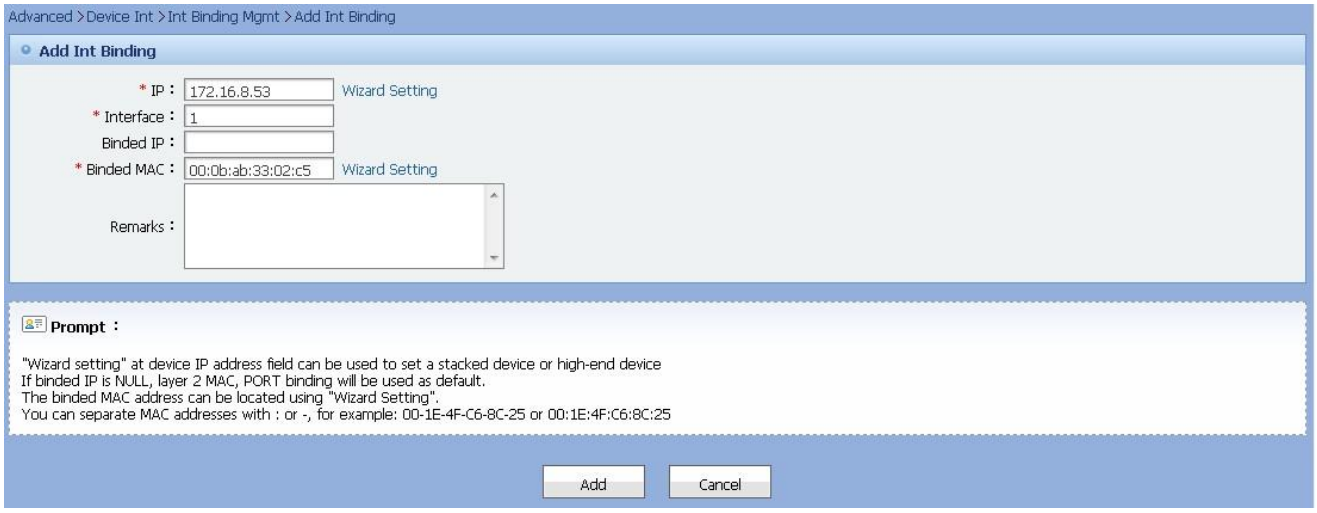


Figure 4.50. Add Interface Binding

4.7. Interface Mapping Management

Brief Introduction

Operations for interface mapping relation of the device mainly include synchronizing device mapping information and viewing the device's interface map information. Two modes can be used: 1. Manual synchronization. 2. Periodical synchronization.

The following example show how to synchronize interface mapping information for "192.168.197.164" manually, and how to synchronize interface mapping information for "192.168.197.164" once every 24 hours.

■ **Synchronize Device Interface Mapping Relation Manually**

1) Step 1: Click **Device** menu on the **Device List**, search for "192.168.197.164", enter the "Details" of Device.

Step 2: On the "Details" of Device, click **Int Binding Sync List** on the left navigation bar, enter the **Int Binding Sync List**.

Step 3: On the **Int Binding Sync List** page, click **Sync** to synchronize the interface Mapping relation in device.

Figure 4.51. Interface Binding Sync List

■ **Synchronize Device Interface Mapping Relation Periodically**

1) Step 1: Go to **Advanced > Device Int** menu, click **Int Mapping Plan** in the left navigation bar, enter the **Int Mapping Plan**.

Step 2: Click **Select Device** on the **Int Mapping Plan** page. Search for "192.168.197.164" in the pop-up dialogue box **Select Device**, select the corresponding device, click **Add**.

Step 3: Click the **Int Mapping Plan** page, enter Plan Schedule: Every n hours" to "24" in the "Parameter Configuration", click **Edit** to end the configuration.

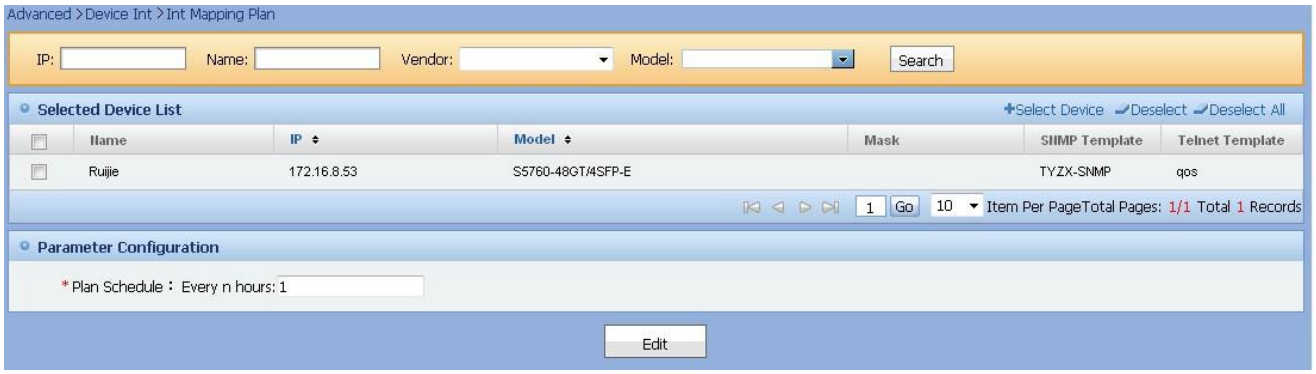


Figure 4.52. Interface Mapping Plan

■ **Viewing Device Interface Mapping Relation**

1) Step 1: Go to **Advanced > Device Int** menu, click **Interface Mapping List** on the left navigation bar, enter the **Interface Mapping List** page.

Step 2: Search for "192.168.197.164" on the **Interface Mapping List** page, to view the corresponding interface mapping information.

Note

On the interface "Details" of Device, User can also click **Interface Binding Sync List** in the left navigation bar, enter the **Interface Binding Sync List** page .

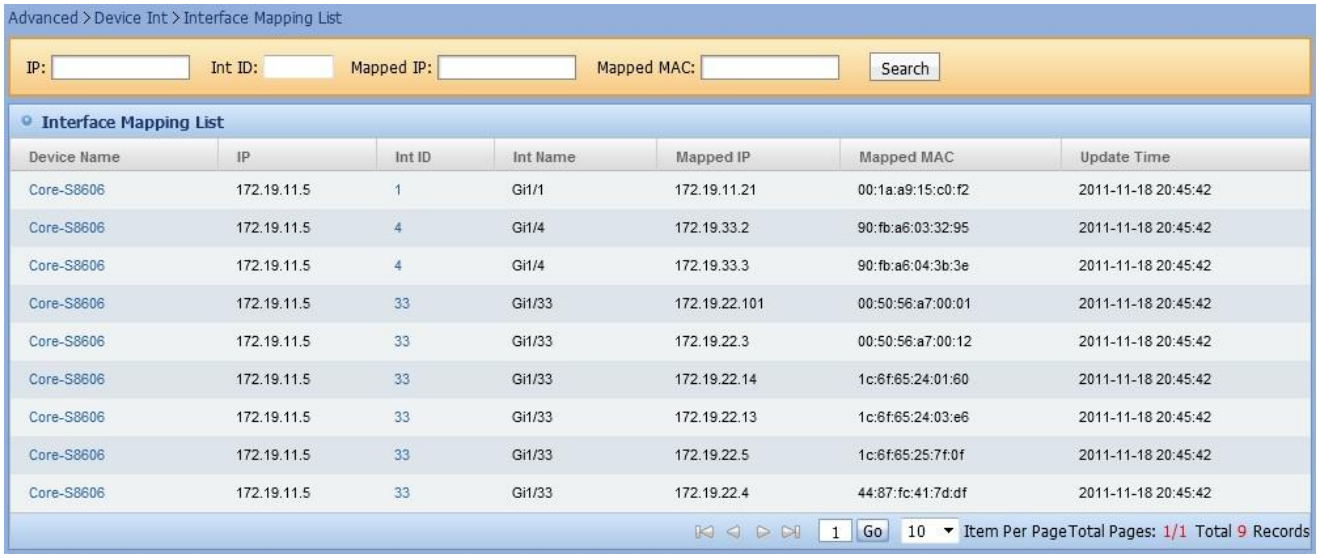


Figure 4.53. Interface Mapping List

4.8. Interface Control Plan

Basic Concept

■ **Automatic Plan**

The plans that run automatically in the background of system. User can customize the cycle period and valid period of the execution. Note: Auto plan needs to be activated before running.

■ **Manual Plan**

The plans that need to be started by user. Of course, the auto plan, in the case of activation, can also be started manually.

Brief Introduction

User can add some interface control plans to regularly execute the switch operation on the device interface in the system.

The following example shows how to configure a plan, from “2010-08-16 00:00” to “2010-08-20 23:59”, to close “Port 1” of “192.168.197.164” on “18” daily. As for deleting interface control plan, due to relatively simple; As for updating the interface control plan, due to similar with adding interface control plan, will not go into the details here.

1) Step 1: Go to **Advanced > Device Int** menu, click **IntControl Plan** in the left navigation bar, enter the **Int Control Plan** page.

Step 2: Click **Add** on the **Int Control Plan** page, and start operation **Add Plan**, enter the **Basic Information** page.
Step 3: Input the plan which “Plan Name” is “dev_down”, “Plan Type” is “Auto Plan”, “Start Time” is “2010-08-16 00:00”, “End Time” is “2010-08-20 23:59”, “Plan Schedule” is “18” daily. Then click **Next**, enter the **Selected Device List** page.
Step 4: Click **Select Device** on the **Selected Device List**. Search for “192.168.197.164” in the pop-up dialogue box **Select Device**, select the device, then click **Next**, enter **Configure Interface Control Parameters**.
Step 5: Click icon “Port 1” to “off” on **Configure Interface Control Parameters**”, then click **Finish**.
Step 6: Return to **Interface Control Plan**, do not forget to **Active** the plan added a moment ago. So far, adding plan is completed.
After that: As for the running status of the plan, user can search “dev_down” on **Business Plan**, click corresponding “Plan Name”, enter the “Plan Name” to check the running status of the plan.

Figure 4.54. Interface Control Plan

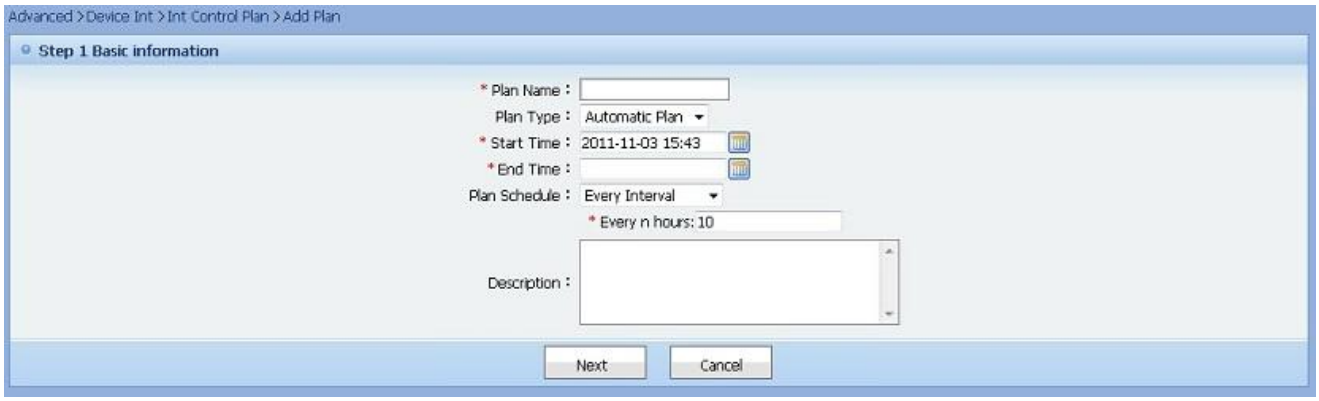


Figure 4.55. Basic Information

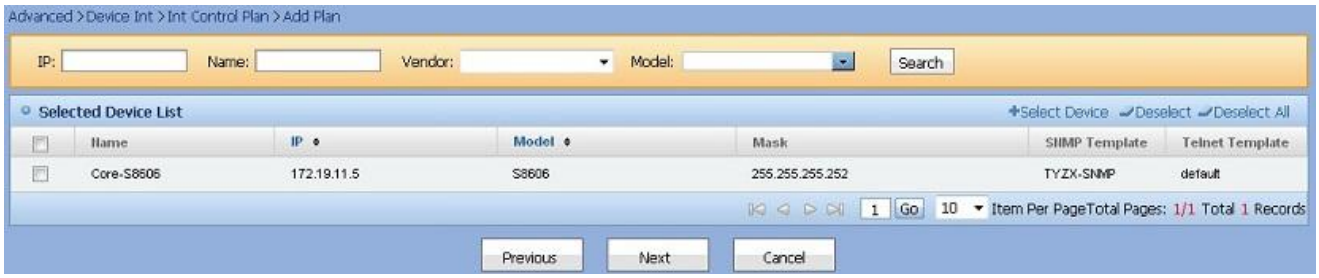


Figure 4.56. Selected Device List

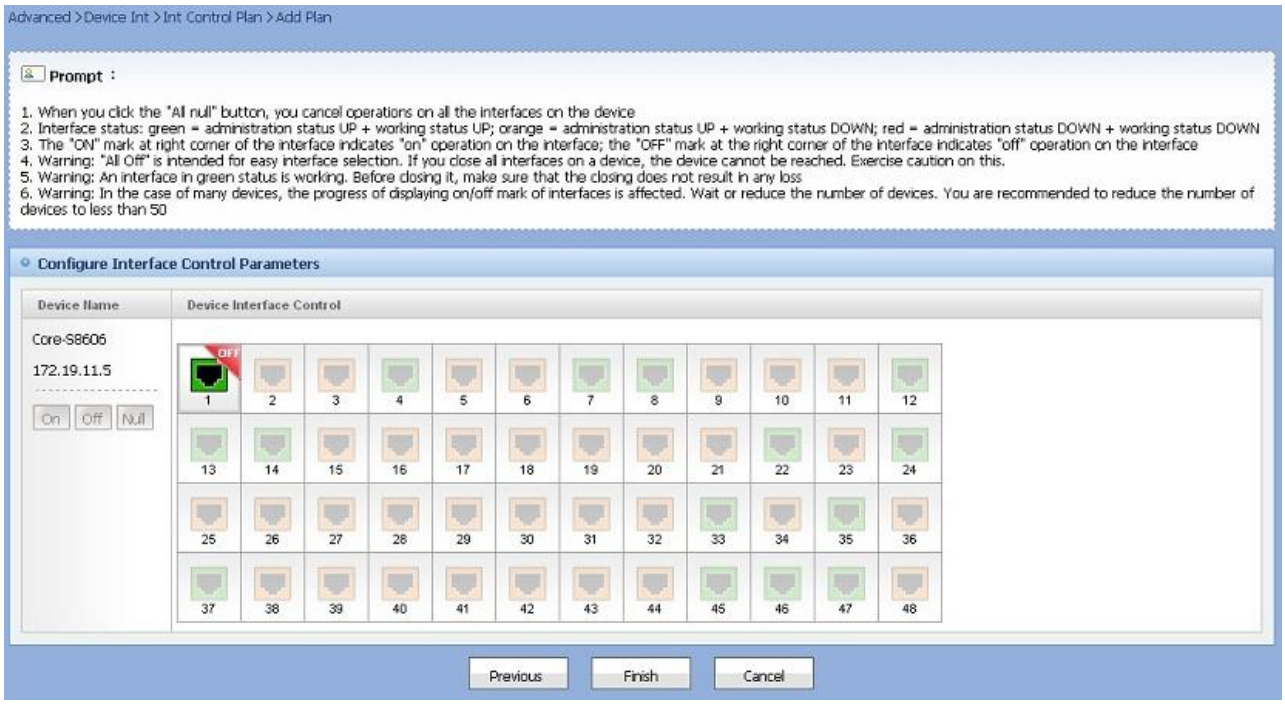


Figure 4.57. Configure Interface Control Parameters

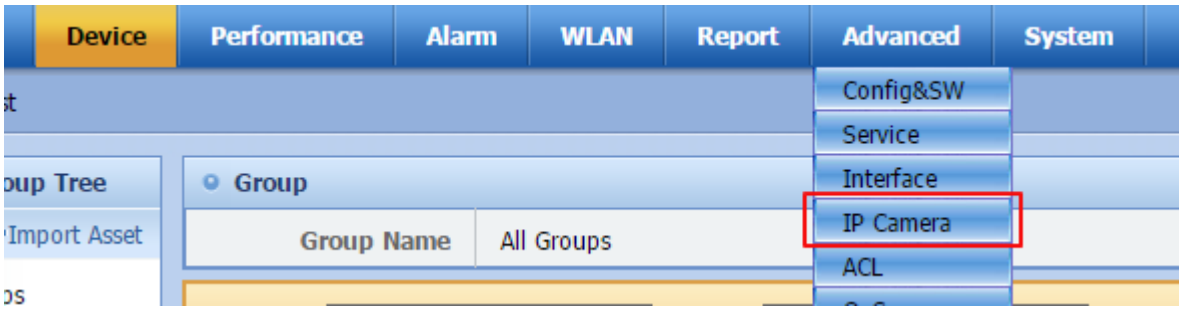
Figure 4.58. Plan Details

4.9. IP Camera

4.9.1. Add IP Camera

Operation Steps

1) Go to **Advanced** > **IP Camera**, click **Add** on the **Device List** page, as shown below:



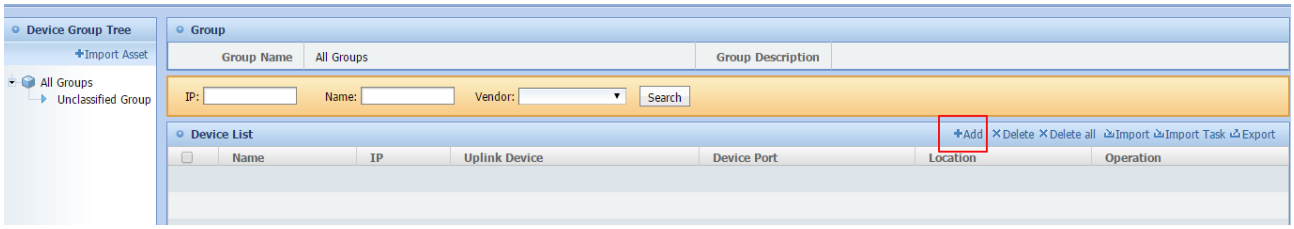


Figure 5.59.Adding IP Camera

2) Fill in the IP camera information, click **Add**, as shown below:

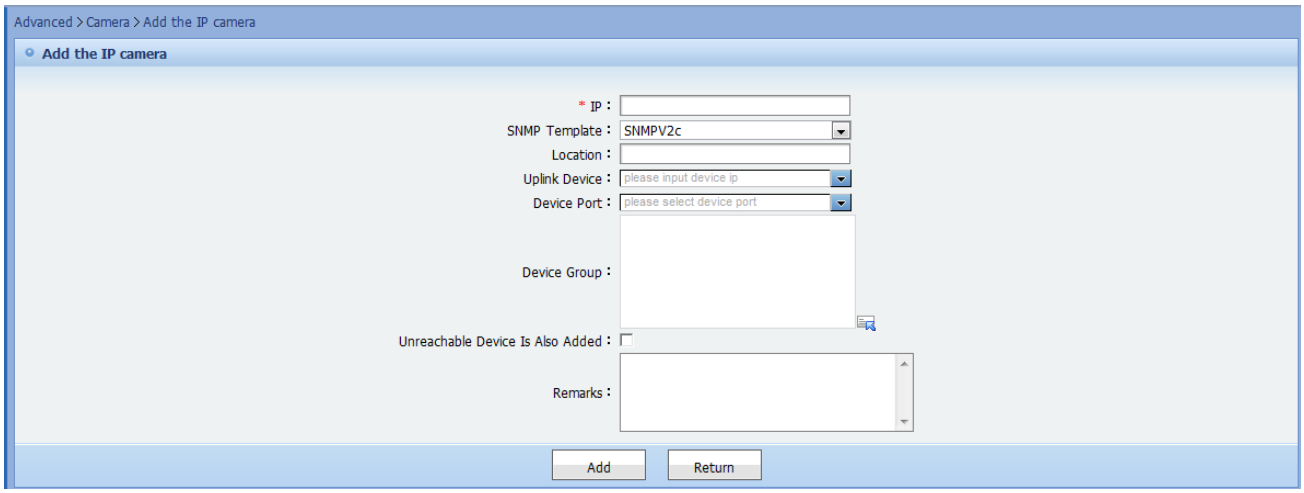


Figure 5.60 Filling in IP Camera Info

Caution The device IP address must be valid.

Caution The SNMP template is used to obtain device MIB. If the parameters in the SNMP template do not match those of the device, the device can be added, but the MIB info cannot be obtained.

Caution If you want to specify an uplink device for the IP Camera, select a device from the **Uplink Device** dropdown box. The uplink device can be only: SWITCH, EG/NPE and ROUTER.

Caution Once an uplink device is selected, the **Device Port** dropdown list will display all ports of this device.

Caution

If **Unreachable Device is Also Added** is checked, the device that fails to ping can be also added. Otherwise, it cannot be added.

4.9.2. Delete IP Camera

Operation Steps

1) Go to **Advanced** > **IP Camera** > **Device List**, select an IP camera, click **Delete**, as shown below:

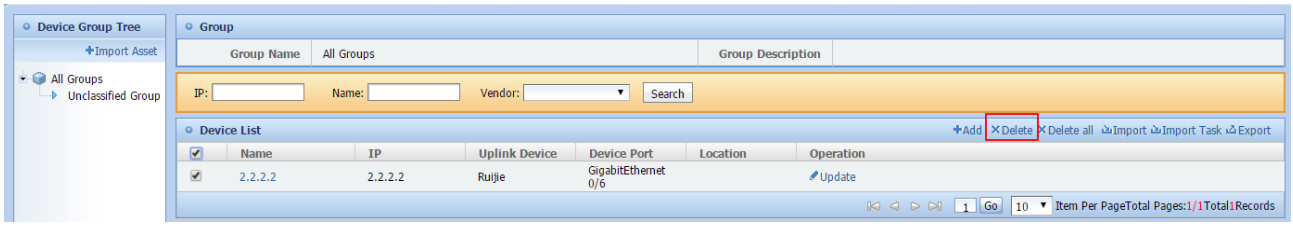


Figure 5.61. Deleting IP Camera

2) Click **Delete all**, to delete all IP cameras in the list.

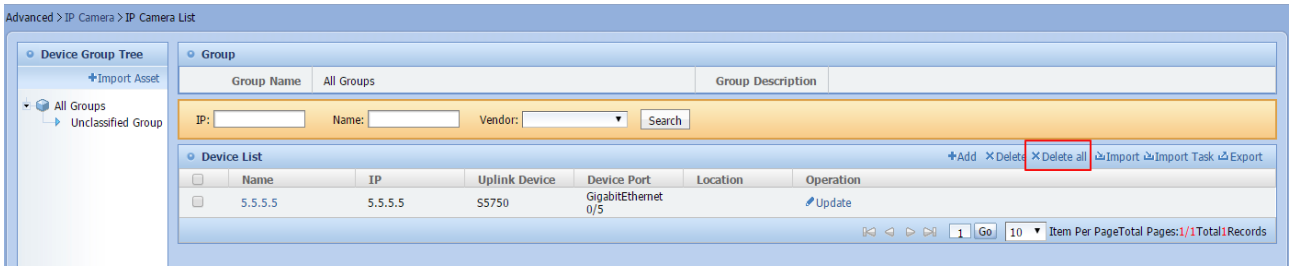


Figure 5.62. Deleting All IP Cameras

4.9.3. Modify IP Camera

Operation Steps

1) Go to **Advanced** > **IP Camera** > **Device List**, select an IP camera, click **Update**, as shown below:

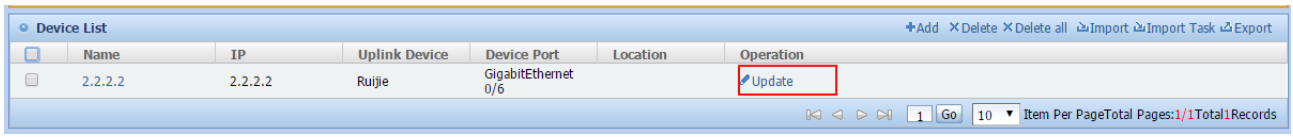


Figure 5.63. Modifying IP Camera Info

2. Edit the IP camera information, and click **Update**.

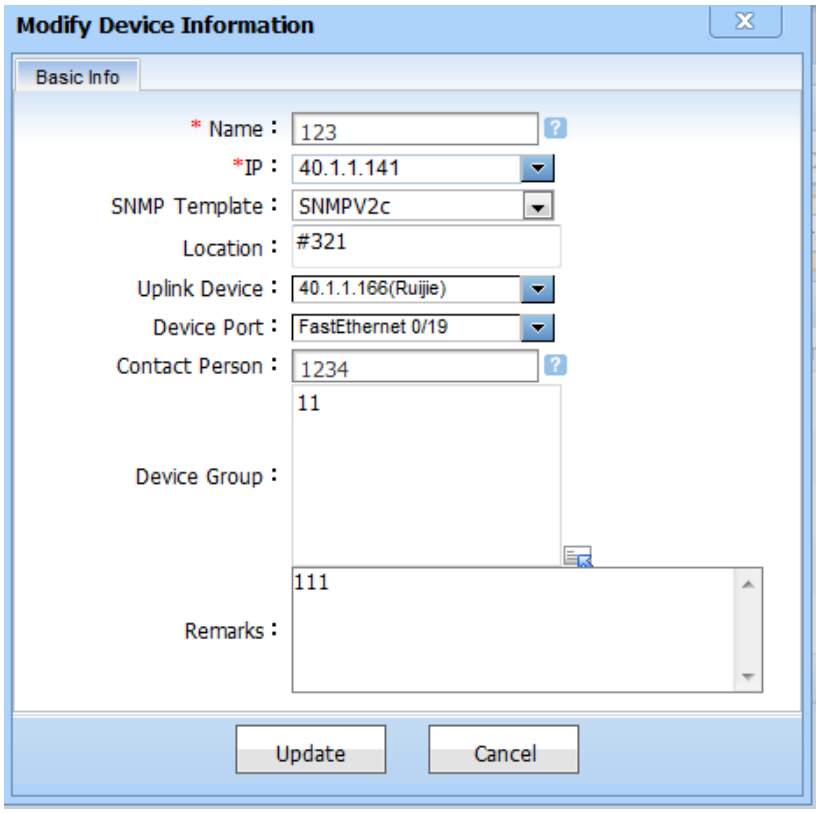


Figure 5.64. Modifying IP Camera Info

4.9.4. Query IP Camera

This function enables you to query the IP camera by the criteria such as camera IP, name, vendor.

Operation Steps

Enter the query criteria (camera IP, name or vendor), click **Search**, as shown below:

Figure 5.65. Querying IP Camera

4.9.5. Display IP Camera

Operation Steps

1) Click an IP camera name to enter the details page, as shown below:

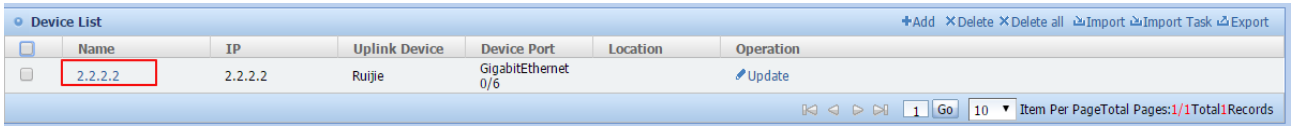


Figure 5.67. Device List

2. On the **Camera detail** page, the camera information is displayed, as shown below:

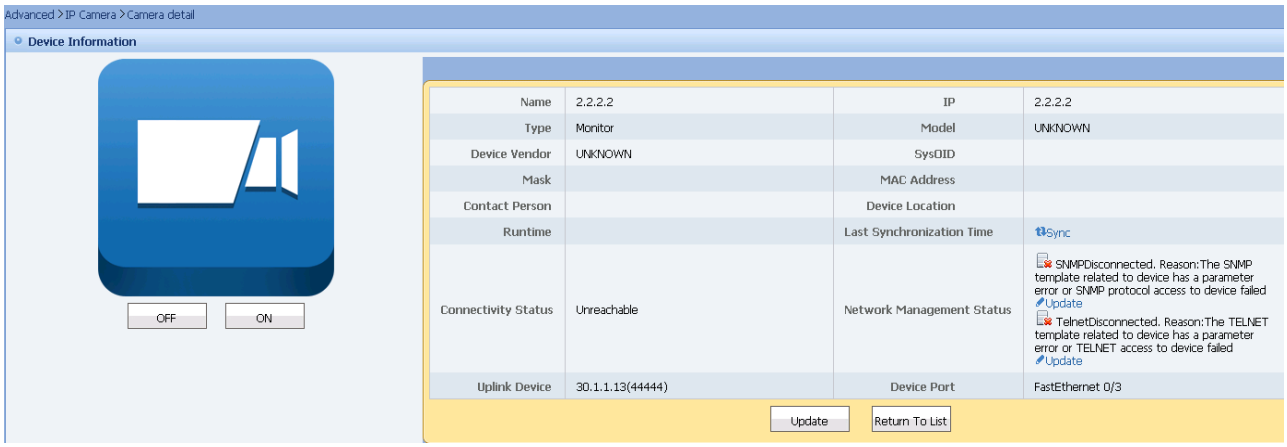


Figure 5.68. IP Camera Details

3. Click **ON** or **OFF** to enable or disable the IP camera.

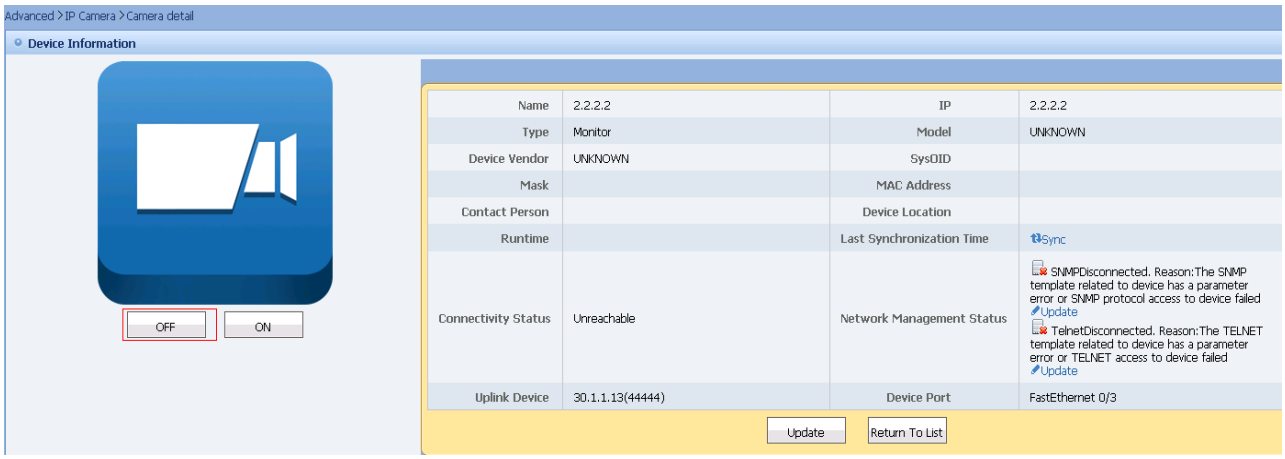


Figure 5.69. Enabling IP Camera

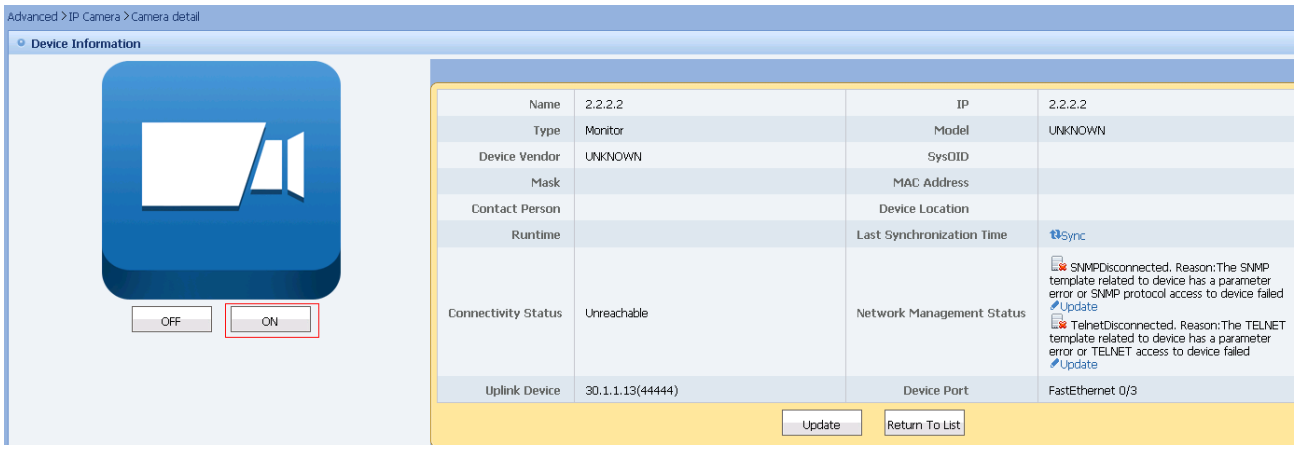


Figure 5.70. Disabling IP Camera

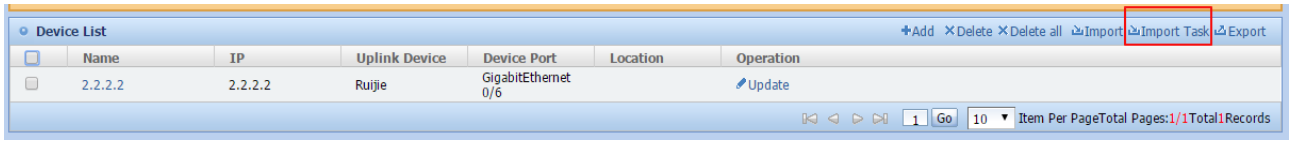
4.9.6. Import IP Camera

This function enables you to add the IP camera in batch by **Import** or **Import Task**.

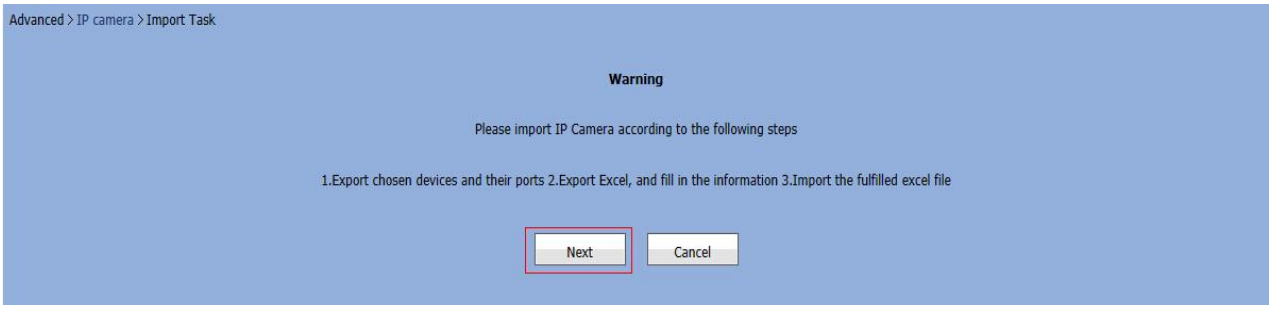
You can click **Import** to import the IP cameras through the file filled with the camera information. If the camera information is unfilled, the **Import Task** function will guide you to perform camera import.

Operation Steps

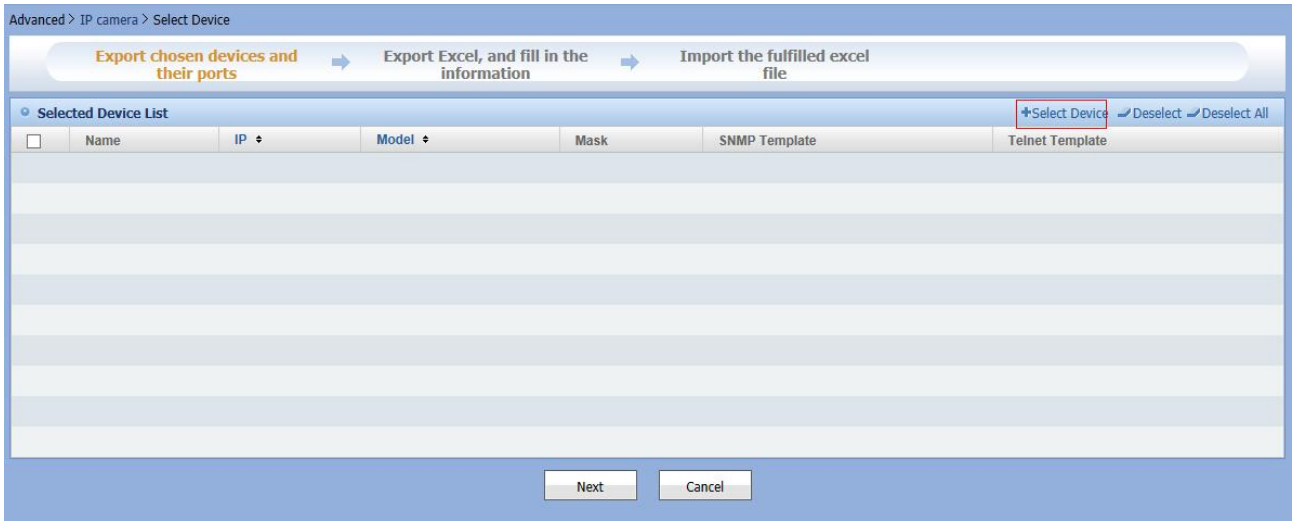
1) Click **Import Task**, and follow the steps for device import.

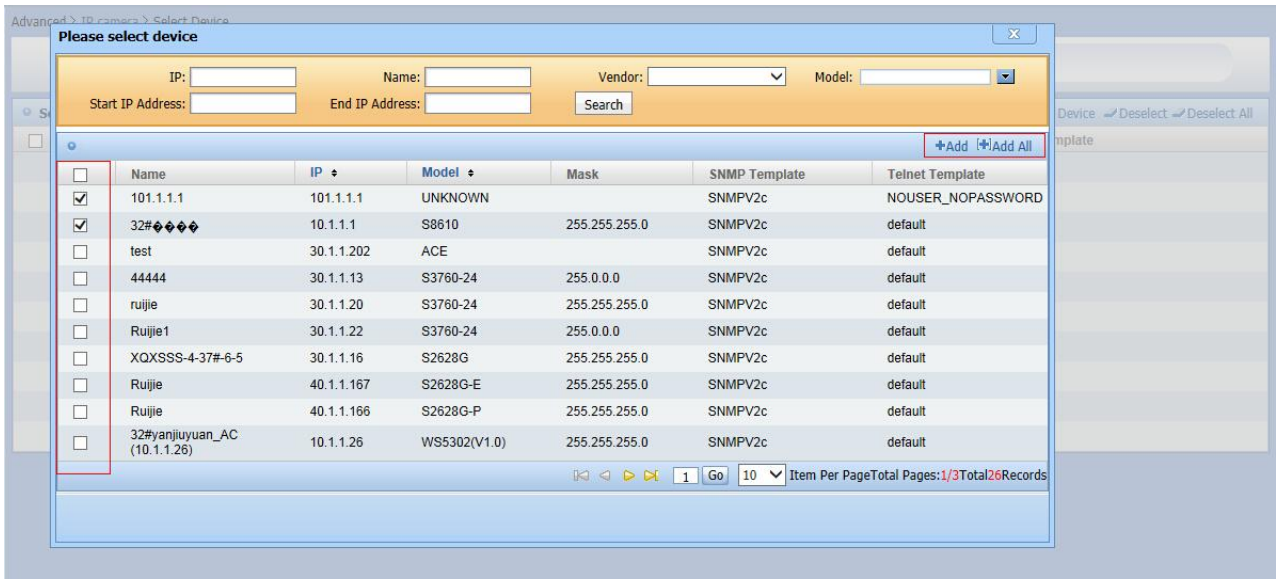


2) Click **Next**.

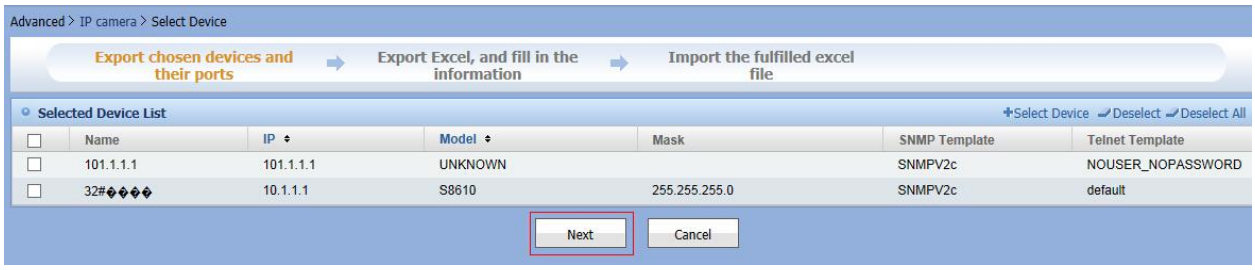


3) Click **Select Device** to select the uplink device, as shown below:

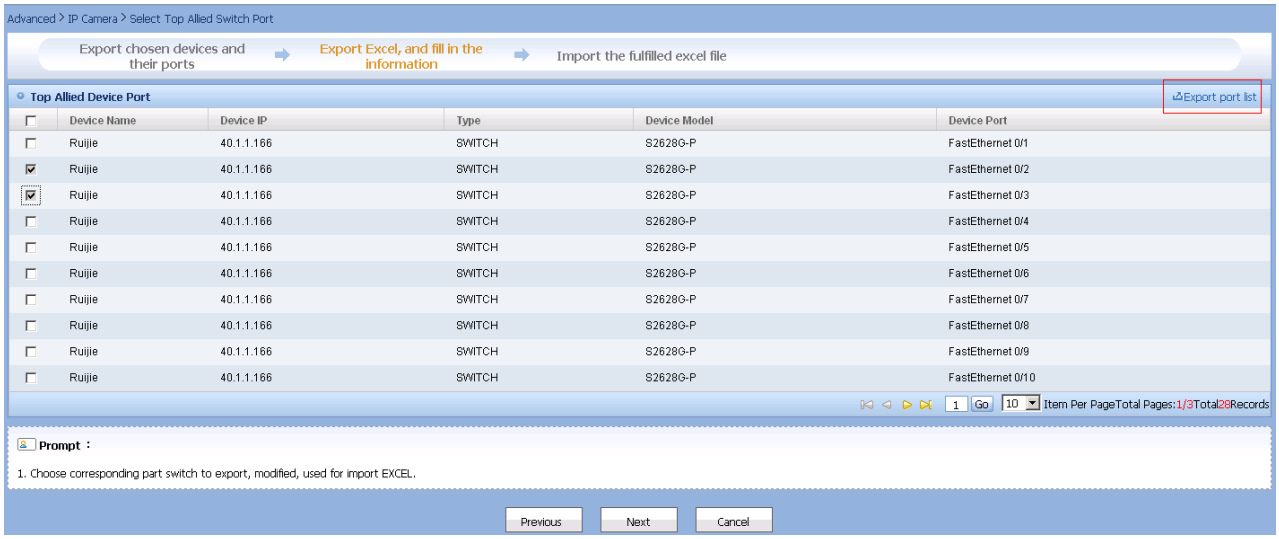




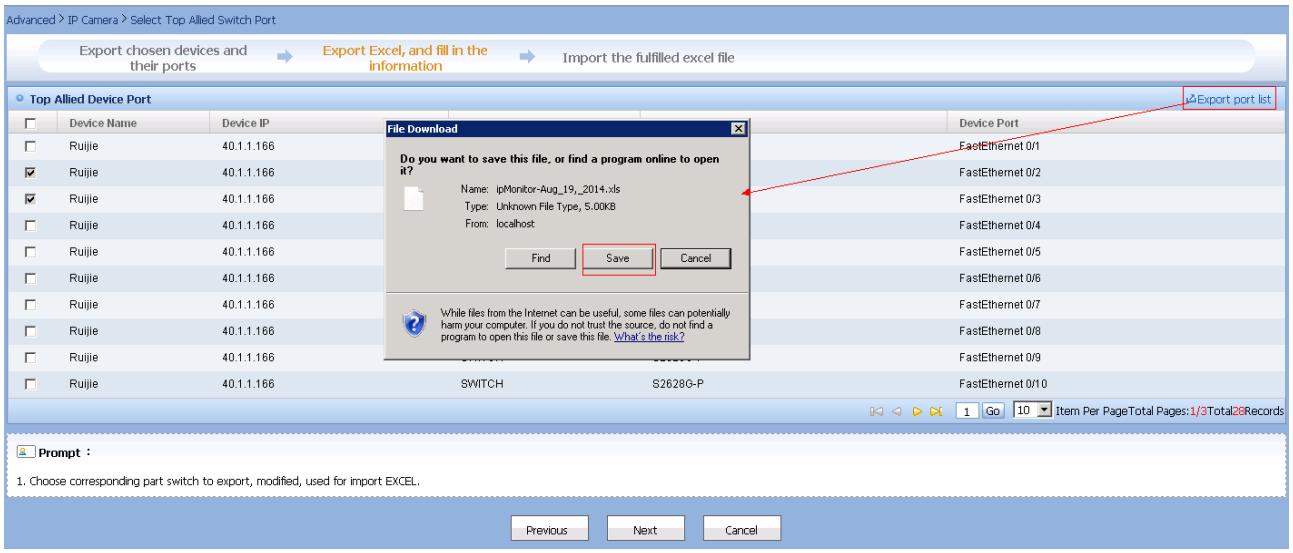
4) Click **Next**.



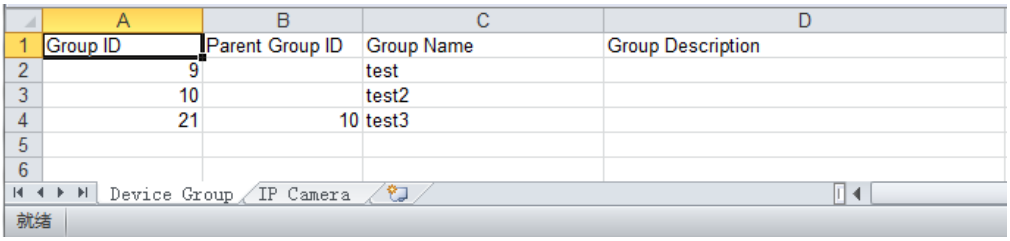
5) Select the port for IP camera connection.



6) Click **Save** to save the generated device import file.



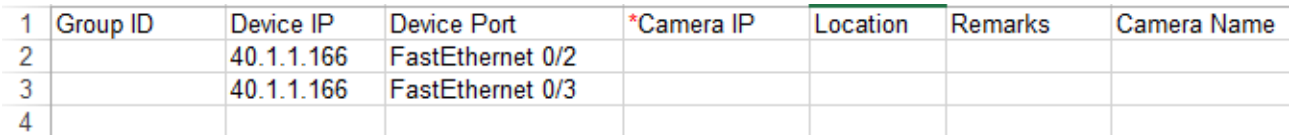
The generated excel file has two tabs: **Device Group** tab and **IP Camera** tab. You can fill in related information as needed, as shown below:



	A	B	C	D
1	Group ID	Parent Group ID	Group Name	Group Description
2	9		test	
3	10		test2	
4	21	10	test3	
5				
6				

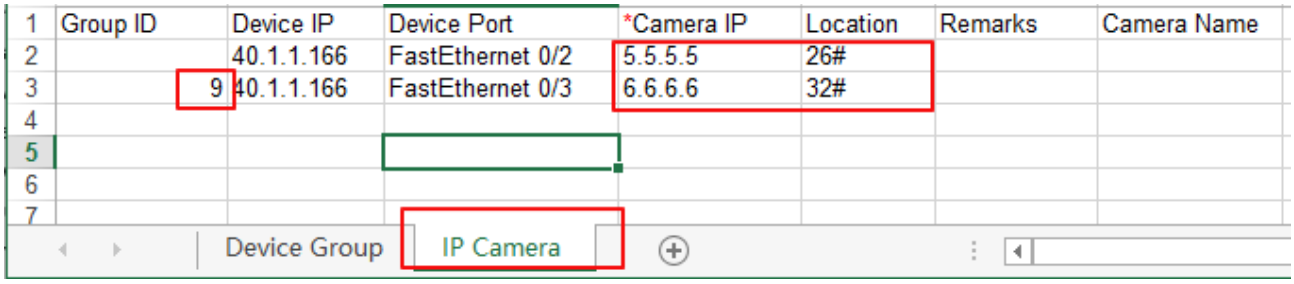
Device Group | IP Camera

就绪



	Group ID	Device IP	Device Port	*Camera IP	Location	Remarks	Camera Name
2		40.1.1.166	FastEthernet 0/2				
3		40.1.1.166	FastEthernet 0/3				
4							

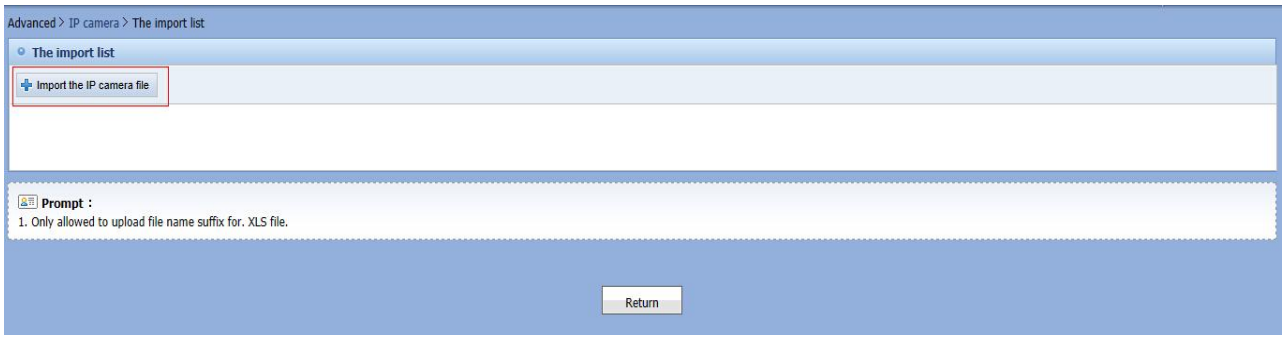
7) Fill in the IP camera information, such as IP address, location, remarks and Group ID.



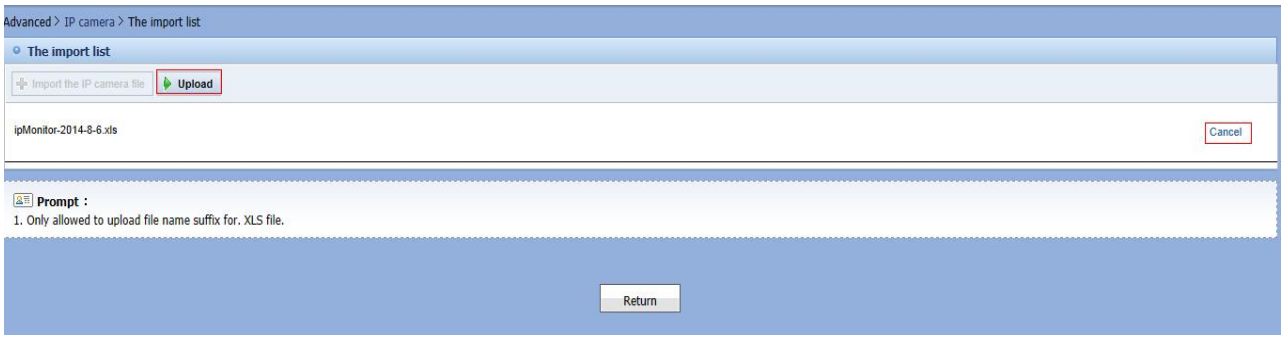
	Group ID	Device IP	Device Port	*Camera IP	Location	Remarks	Camera Name
2		40.1.1.166	FastEthernet 0/2	5.5.5.5	26#		
3	9	40.1.1.166	FastEthernet 0/3	6.6.6.6	32#		
4							
5							
6							
7							

Device Group | IP Camera

8) Click **Import the IP camera file** to import the edited excel file.



9) Click **Upload**, as shown below:

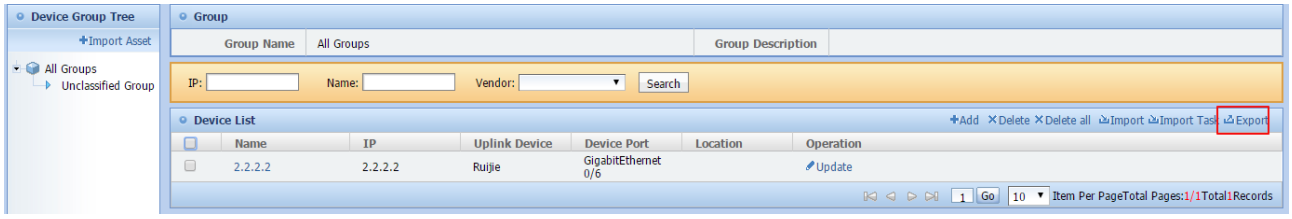


The import log is shown below:

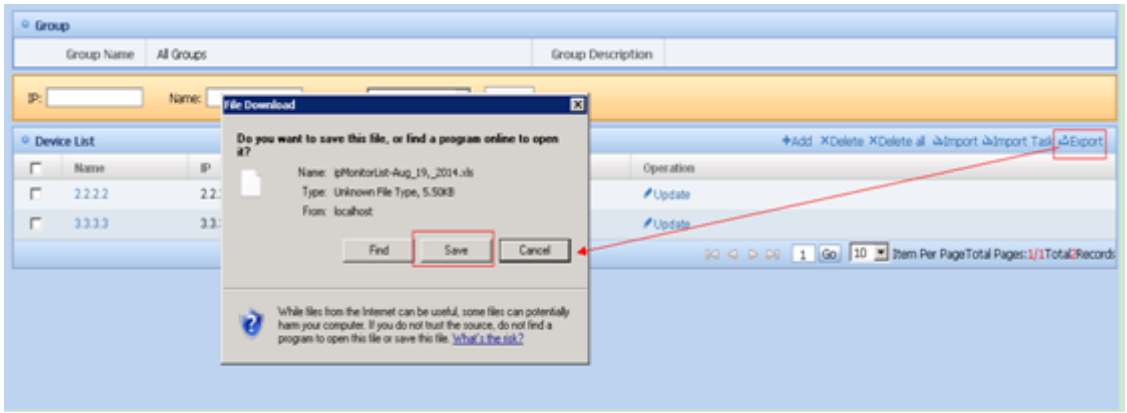
4.9.7. Export IP Camera

Operation Steps

1) Go to **Advanced** > **IP Camera** > **Device List**, click **Export**, as shown below:



2) Click **Save** on the pop-up dialog box to save the export file, as shown below:


Group
Group Name
All Groups
Group Description
IP:
Name:
Device List
Add
Delete
Delete all
Import
Import Task
Export
Name
IP
Operation
2.2.2.2
3.3.3.3
Update
Update
Item Per Page
Total Pages:
Total Records:
File Download
Do you want to save this file, or find a program online to open it?
Name: ipMonitorList-Aug_19,_2014.xls
Type: Unknown File Type, 5.50KB
From: localhost
Find
Save
Cancel
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not find a program to open this file or save this file. What's the risk?

Chapter 5 Performance Management

The performance management provides user to monitor the device, set the KPI threshold value, enable monitor for interface, view realtime performance line chart, query performance history data and export data to a report file.

Function list

- KPI for device
- Global performance threshold value management
- Query for performance history
- Monitored device management
- View the performance curve in real time
- Query and export for performance history data
- Single device monitoring
- Multiple device monitoring

5.1. KPI for Device

KPI for a device include the following:

- CPU Utilization(%)
- Memory Utilization(%)
- Interface receiving rate(M bytes/s)
- Interface sending rate(M bytes/s)
- Interface receiving usage(%)
- Interface sending usage(%)
- Interface receiving discard rate(M packets/s)
- Interface sending discard rate(M packets/s)
- Interface receiving error rate(M packets/s)
- Interface sending error rate(M packets/s)
- Interface receiving unicast rate(M packets/s)
- Interface sending unicast rate(M packets/s)
- Interface receiving broadcast rate(M packets/s)
- Temperature(°C)
- Disk usage(%)
- Interface CRC error rate(%)

For a KPI that is not included in the monitor list, the system provide a shortcut to add it into the monitor list; for a KPI that is included in the monitor list, you can not only view the performance data for today, but also query the data for last 7 and 30 days and even change the threshold value.

For those thresholds like CPU consumption and memory consumption that can be applied to multiple devices, the result for today will mark the data for different devices in different colors. If there exists warnings for a KPI, the system will mark the range with the two level threshold values, that is yellow line for level 1 and red line for level 2.

Note Data of CPU consumption and memory consumption comes from a private MIB implementation, other interface data comes from RFC1213 ifTable (RFC2233 ifXTable).

5.2. Global Performance Threshold Management

With this function, you can view and set the global threshold value for a KPI, or restore the value to its initial value.

View and set the global threshold value for KPI

If the system finds a KPI value exceed the threshold, a warning alert with corresponding level will be emit. By default, the system will not enable global threshold value for any KPI and you must use **Add monitor to device** to apply the global

threshold. However, if a device threshold value for a KPI is applied on the device, the global threshold value for that KPI will not applied on the device.

There are two levels of threshold value in the system. By default, level 1 threshold is enabled and you can configure the system whether to enable the level 2 threshold. If the collected data is between level 1 and level 2, a level 1 warning is emit; if the data exceed level 2 threshold, a level 2 warning is emit.

In the “Global performance indicator threshold list” page, you can view the global threshold for every KPI of any kind.

1) Go to the **Performance** menu and select [Global Performance Threshold] menu item, the system will go into the management page where you can view the threshold and warning level for each KPI.

Select any KPI in the “**Global performance indicator threshold list**” and click **Set**, as shown by the screenshot below:

Performance > View Global Performance Indicator Thresholds

Global Performance Indicator Threshold List — Default

Indicator Name	Description	L1 Threshold	L2 Threshold	L3 Threshold	Threshold Setting
CPU Utilization (%)	CPU Utilization	85	90	95	Set
Memory Utilization(%)	Memory Utilization	85	90	95	Set
Interface Receiving Rate (Mbits/s)	Interface Receiving Rate	300	500	700	Set
Interface Sending Rate (Mbits/s)	Interface Sending Rate	300	500	700	Set
Interface Receiving Utilization (%)	Interface Receiving Utilization	85	90	95	Set
Interface Sending Utilization (%)	Interface Sending Utilization	85	90	95	Set
Interface Receiving Discard Rate(Mpackets/s)	Discard Rate of Receiving Packets	1	4	5	Set
Interface Sending Discard Rate(Mpackets/s)	Discard Rate of Sending Packets	1	4	5	Set
Interface Receiving Error Rate(Mpackets/s)	Error Rate of Receiving Packets	1	4	5	Set
Interface Sending Error Rate(Mpackets/s)	Error Rate of Sending Packets	1	4	5	Set
Interface Receiving Unicast Rate(Mpackets/s)	Rate of Receiving Unicast Packets	1	4	5	Set
Interface Sending Unicast Rate(Mpackets/s)	Rate of Sending Unicast Packets	1	4	5	Set
Interface Receiving Broadcast Rate(Mpackets/s)	Rate of Receiving Broadcast Packets	1	4	5	Set
Interface Sending Broadcast Rate(Mpackets/s)	Rate of Sending Broadcast Packets	1	4	5	Set
Temperature(degrees Celsius)	Temperature	55	65	75	Set
Disk Utilization(%)	Disk Utilization	85	90	95	Set
CRC Error Rate(%)	CRC Error Rate	10	25	50	Set

Figure 5.1. Global threshold list

In the page for threshold modification, select any item you need to modify, as shown by the screenshot below:

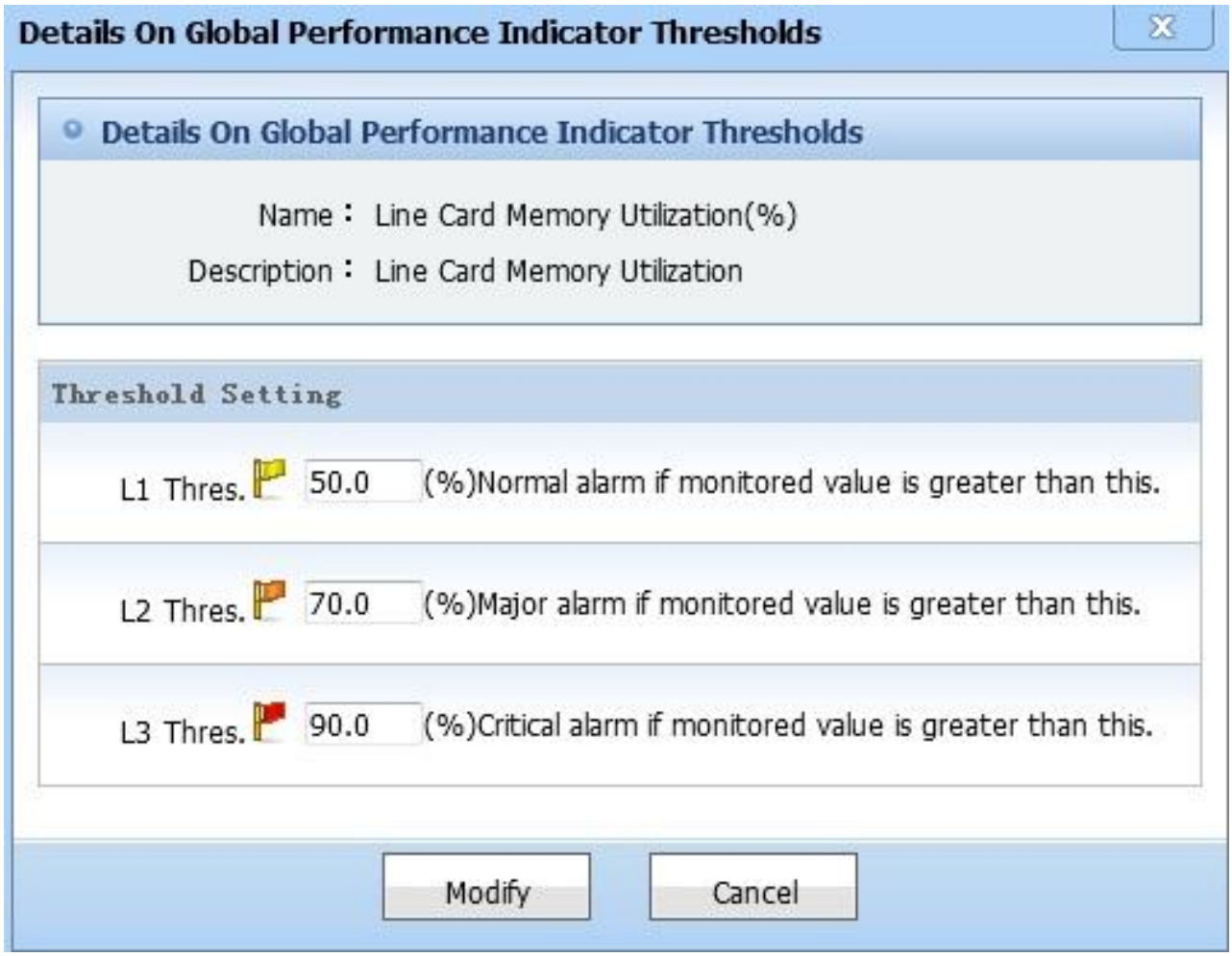


Figure 5.2. The page to modify global threshold

Note

Level 1 threshold must not be greater than level 2 threshold and level 1 warning must not be greater than level 2 warning.

Click **Modify** and commit the change, the system will return to the global threshold list. As shown by the screenshot below:

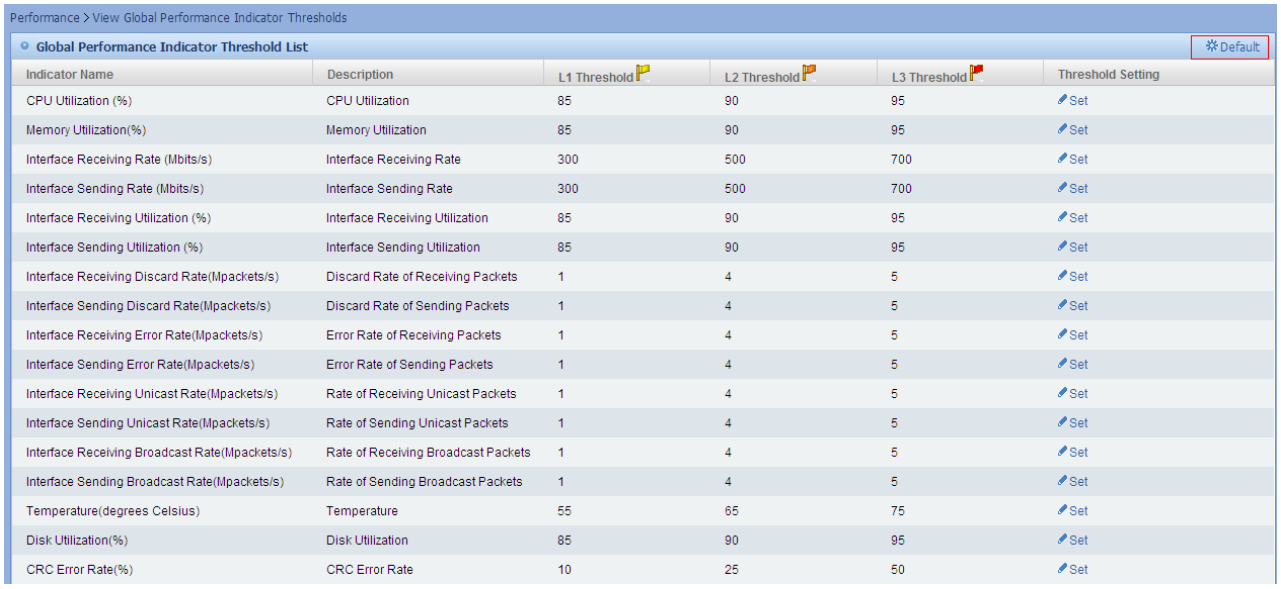
Indicator Name	Description	L1 Threshold	L2 Threshold	L3 Threshold	Threshold Setting
CPU Utilization (%)	CPU Utilization	85	90	95	Set
Memory Utilization(%)	Memory Utilization	85	90	95	Set
Interface Receiving Rate (Mbits/s)	Interface Receiving Rate	300	500	700	Set
Interface Sending Rate (Mbits/s)	Interface Sending Rate	300	500	700	Set
Interface Receiving Utilization (%)	Interface Receiving Utilization	85	90	95	Set
Interface Sending Utilization (%)	In		90	95	Set
Interface Receiving Discard Rate(Mpackets/s)	D		4	5	Set
Interface Sending Discard Rate(Mpackets/s)	D		4	5	Set
Interface Receiving Error Rate(Mpackets/s)	E		4	5	Set
Interface Sending Error Rate(Mpackets/s)	Error Rate of Sending Packets	1	4	5	Set
Interface Receiving Unicast Rate(Mpackets/s)	Rate of Receiving Unicast Packets	1	4	5	Set
Interface Sending Unicast Rate(Mpackets/s)	Rate of Sending Unicast Packets	1	4	5	Set
Interface Receiving Broadcast Rate(Mpackets/s)	Rate of Receiving Broadcast Packets	1	4	5	Set
Interface Sending Broadcast Rate(Mpackets/s)	Rate of Sending Broadcast Packets	1	4	5	Set
Temperature(degrees Celsius)	Temperature	55	65	75	Set
Disk Utilization(%)	Disk Utilization	85	90	95	Set
CRC Error Rate(%)	CRC Error Rate	10	25	50	Set

Figure 5.3. Global Threshold List

Restore the threshold to its initial value

1) Go to the **Performance** menu and select [Global Performance Threshold] menu item, the system will go into the management page.

Click **Default**, as shown by the screenshot below:



Indicator Name	Description	L1 Threshold	L2 Threshold	L3 Threshold	Threshold Setting
CPU Utilization (%)	CPU Utilization	85	90	95	Set
Memory Utilization(%)	Memory Utilization	85	90	95	Set
Interface Receiving Rate (Mbits/s)	Interface Receiving Rate	300	500	700	Set
Interface Sending Rate (Mbits/s)	Interface Sending Rate	300	500	700	Set
Interface Receiving Utilization (%)	Interface Receiving Utilization	85	90	95	Set
Interface Sending Utilization (%)	Interface Sending Utilization	85	90	95	Set
Interface Receiving Discard Rate(Mpackets/s)	Discard Rate of Receiving Packets	1	4	5	Set
Interface Sending Discard Rate(Mpackets/s)	Discard Rate of Sending Packets	1	4	5	Set
Interface Receiving Error Rate(Mpackets/s)	Error Rate of Receiving Packets	1	4	5	Set
Interface Sending Error Rate(Mpackets/s)	Error Rate of Sending Packets	1	4	5	Set
Interface Receiving Unicast Rate(Mpackets/s)	Rate of Receiving Unicast Packets	1	4	5	Set
Interface Sending Unicast Rate(Mpackets/s)	Rate of Sending Unicast Packets	1	4	5	Set
Interface Receiving Broadcast Rate(Mpackets/s)	Rate of Receiving Broadcast Packets	1	4	5	Set
Interface Sending Broadcast Rate(Mpackets/s)	Rate of Sending Broadcast Packets	1	4	5	Set
Temperature(degrees Celsius)	Temperature	55	65	75	Set
Disk Utilization(%)	Disk Utilization	85	90	95	Set
CRC Error Rate(%)	CRC Error Rate	10	25	50	Set

Figure 5.4. Restore the Initial Value

5.3. Query for Performance History

You can customize the query to fetch the KPI for one or more devices at the same time, and export the result to an EXECLE file.

Operation Steps

1) Enter the **Performance Mgmt** menu, select **History Perf Query** navigation tab on the left and the system will go to the page.

Figure 5.5. History Performance Query

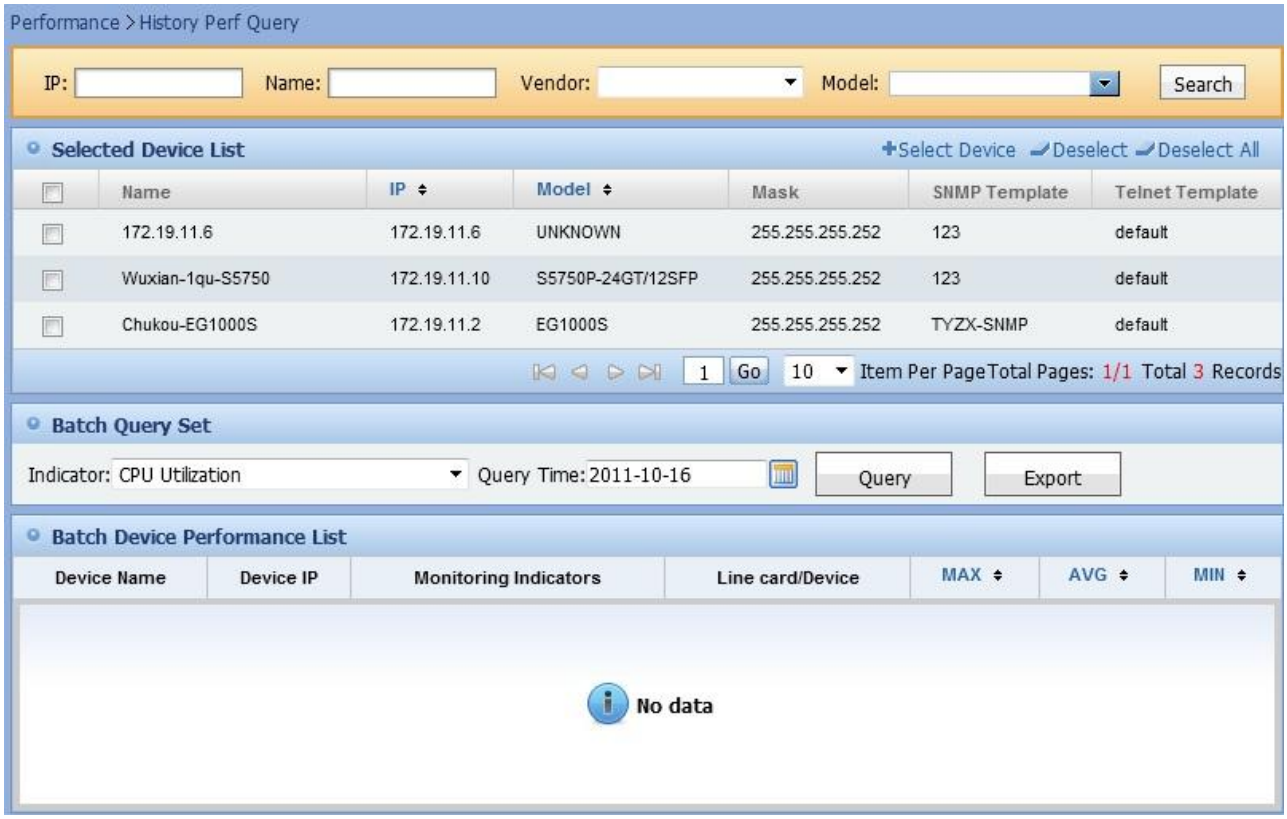


Figure 5.6. Browse the performance history list

You can click **Select device** to select one or more devices.

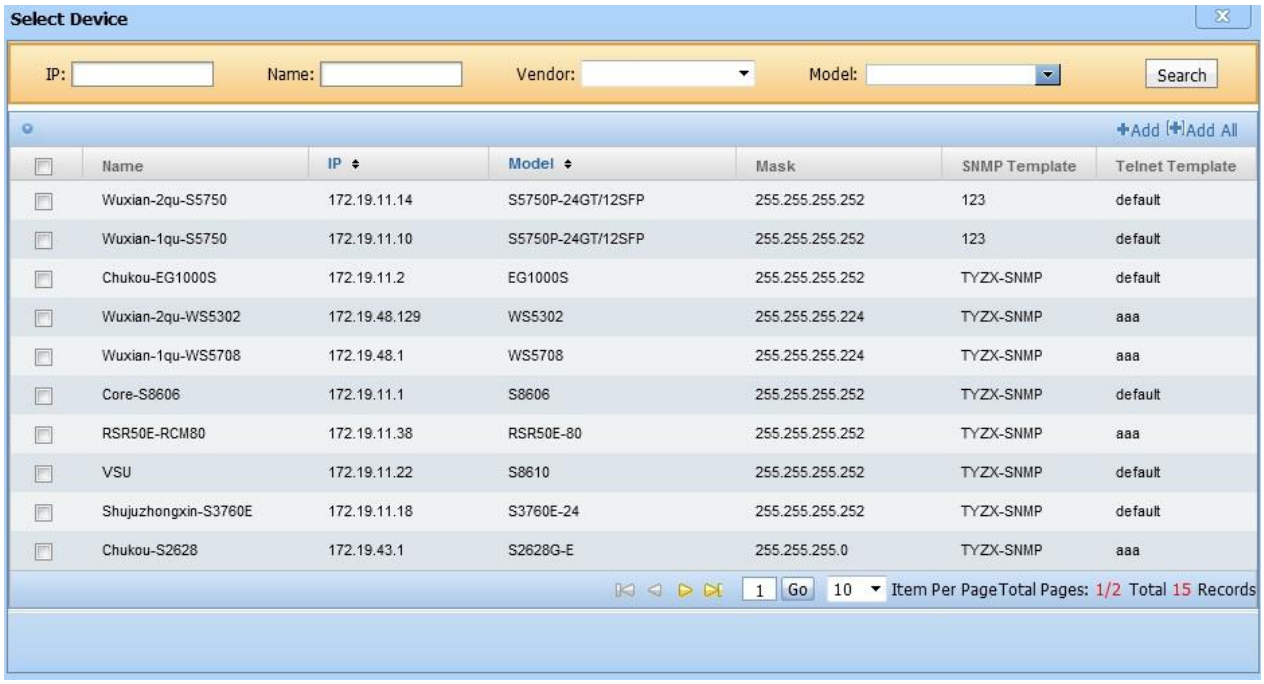


Figure 5.7. Select One or More Devices

You can query the data about the selected devices, KPI and query time.

Figure 5.8. Batch Query

Note You can export the query result into an EXCEL file.

Note You can click **max value**, **avg value** or **min value** to sort the results.

5.4. Monitored Device Management

With monitored device management, you can view the devices in the monitoring list, add devices for monitoring, set threshold for the device, or remove the device from the monitoring list.

Function list

- Query monitored device
- Add monitored devices
- Delete monitored device
- Modify monitoring indicator

- View details of monitored devices

5.4.1. Query Monitored Device

Query monitored devices with customized condition.

You can query monitored devices by IP, name or the device model name, as shown by the screenshot below:

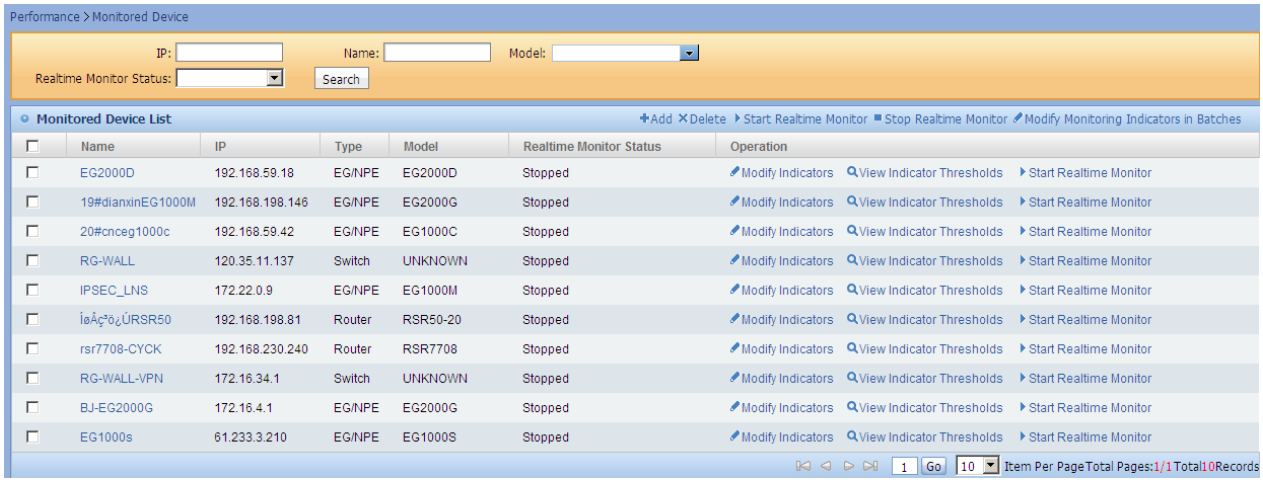


Figure 5.9. Query Monitored Device

5.4.2. Add Monitored Devices

Add one or more devices for performance monitoring.

1) Enter the **Performance** menu and select **Monitored Device** menu item.

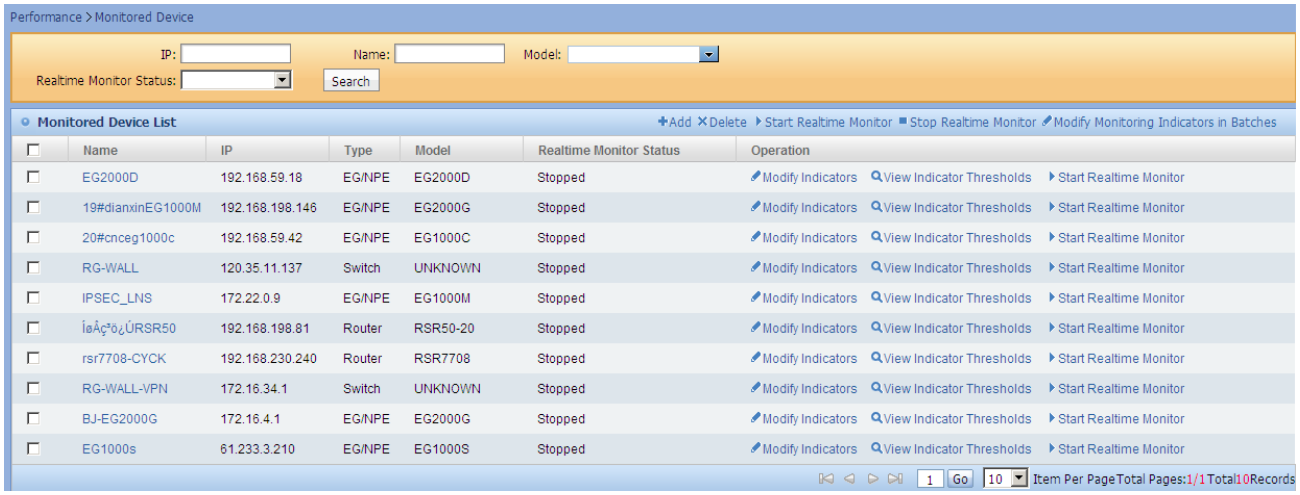


Figure 5.10. Query Monitored Device page

Click **Add** to start the wizard to add monitored devices, as shown by the screenshot below:

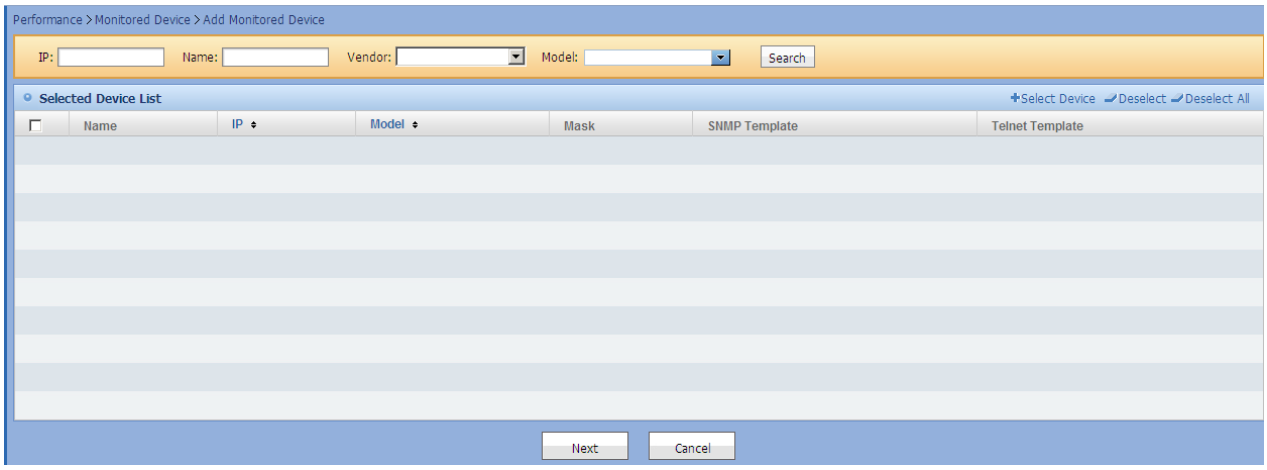


Figure 5.11. Step 1 of the wizard

In this step, click **Select Device** to enter the **Select Device** page, as shown by the screenshot below:

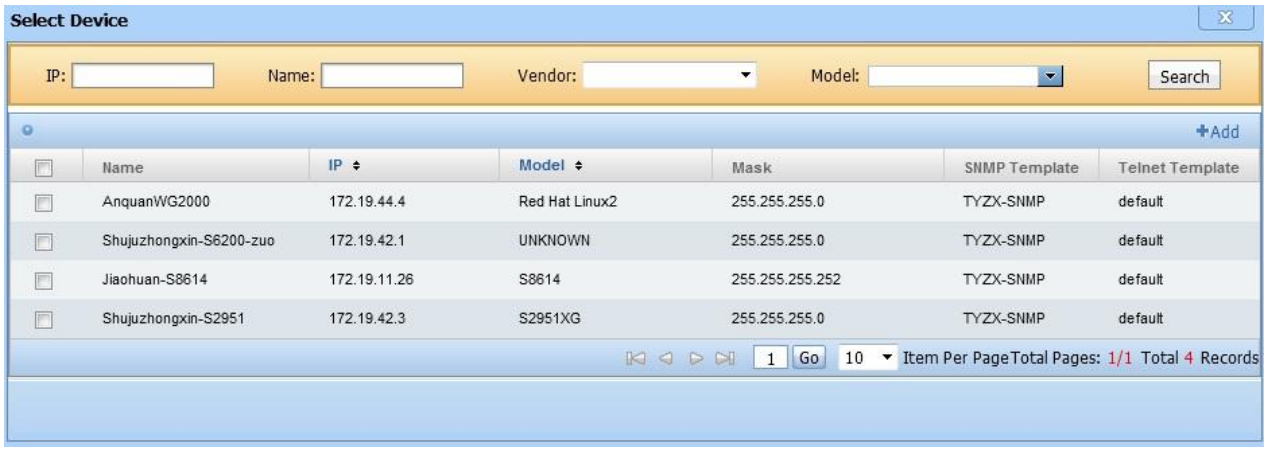


Figure 5.12. Add monitored device -> Select devices page

On the **Select Device** page, tick any checkbox for the device to monitor and then click **Add** or **Add All**, as shown by the screenshot below:

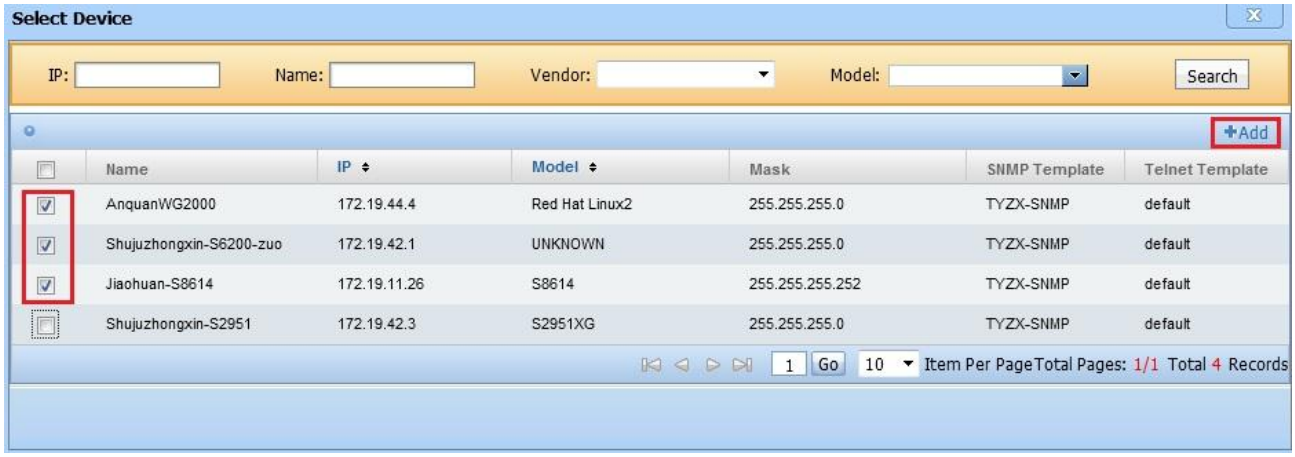


Figure 5.13. Add monitored device -> Select devices page -> Select Device

Once devices are selected, return to the **Add Monitored Device** page, as shown by the screenshot below:

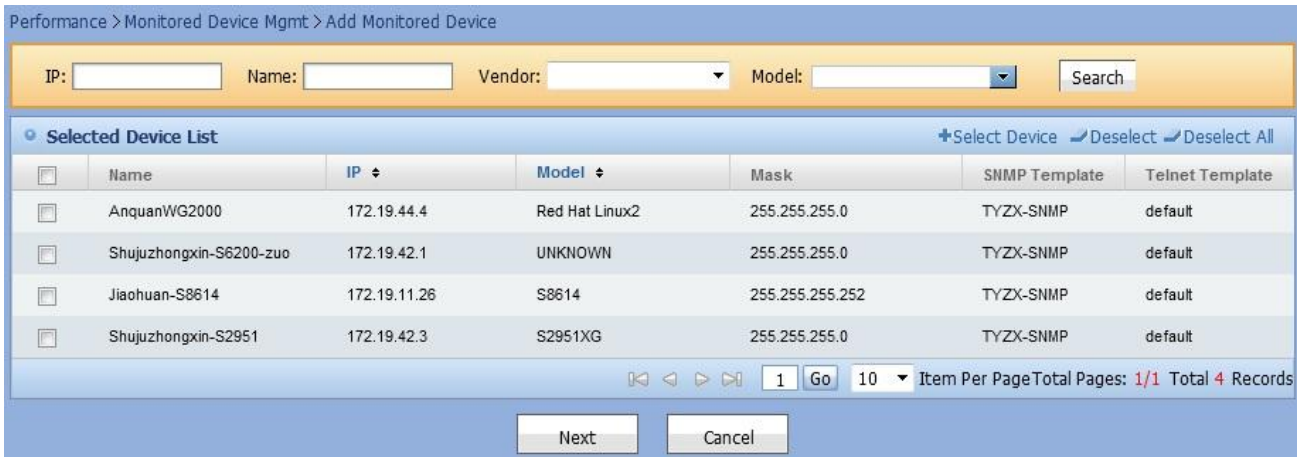


Figure 5.14. Step 1 for adding monitored device

Note If you want to remove the selected devices, click **Deselect** or **Deselect All** to remove devices.

Click **Next** to enter the step 2 of the wizard, as shown by the screenshot below:

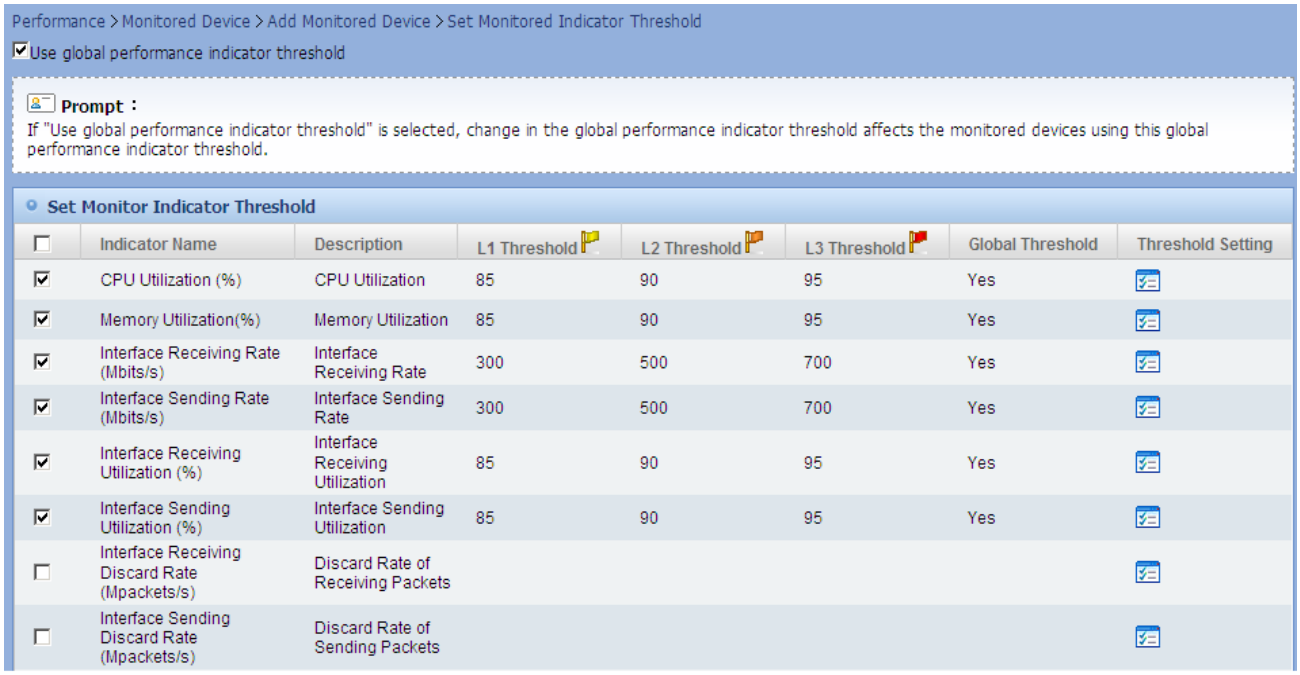


Figure 5.15. Add monitored device -> set threshold value

Note You can enable warning for any KPI just by selecting it in this page, that is, if the KPI is not selected, only the data is collected but no warning will be emit for it. Notice: to enable KIP for interfaces, you have also configure the “switch on/off for monitoring”(default to off), please refer to **Device interface detail information** page for more information.

Click **Finish** to complete the wizard and return to monitored device query page, as shown by the screenshot below:

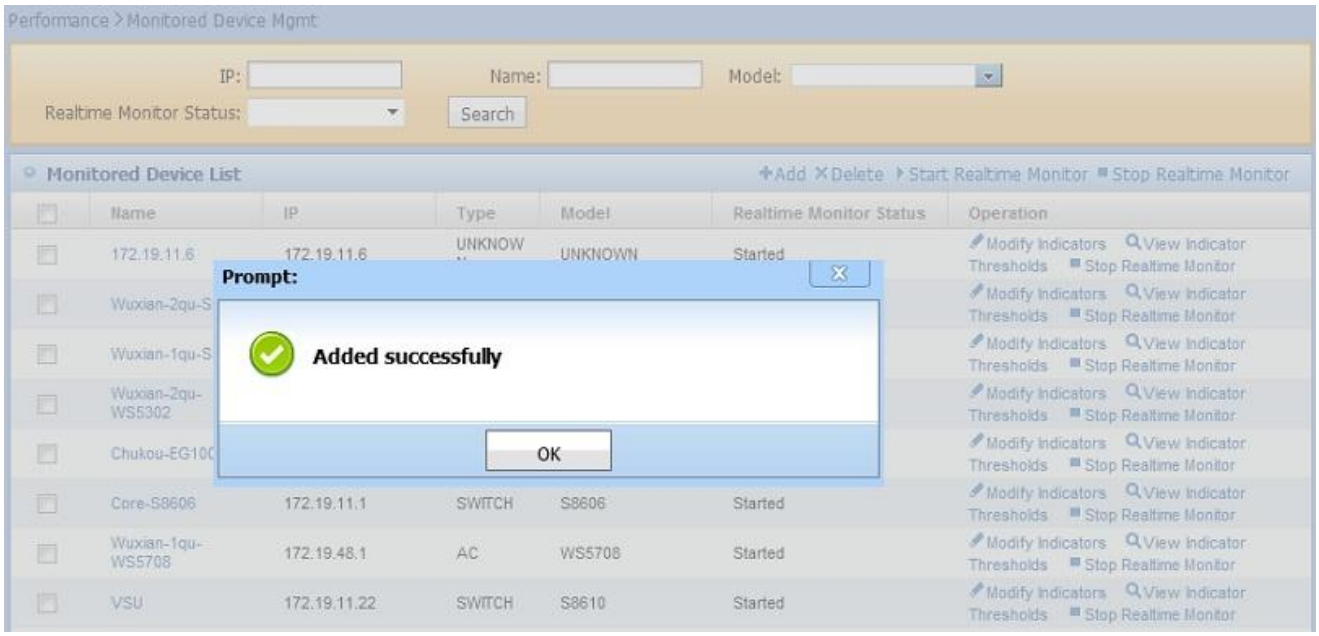


Figure 5.16. Add monitored device successfully

5.4.3. Delete Monitored Device

Enter the **Performance** menu and select **Monitored Device** menu item. Select the monitored device entry and click **Delete**, as shown by the screenshot below:

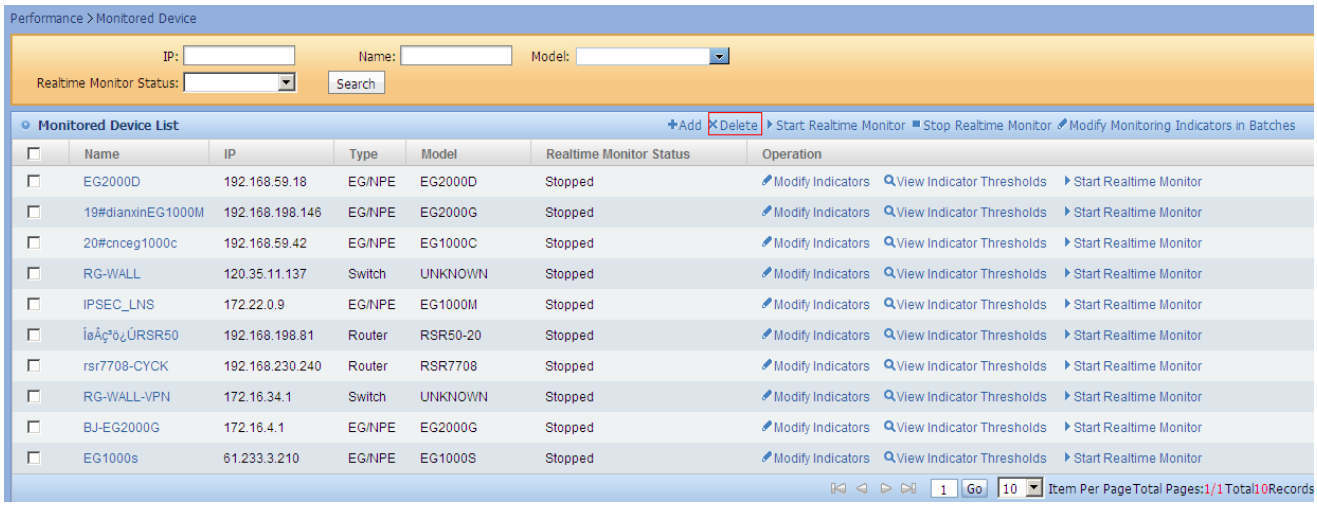


Figure 5.17. Delete monitored device

5.4.4. Modify Monitoring Indicator

1) Enter the **Performance** menu and select **Monitored Device** menu item.

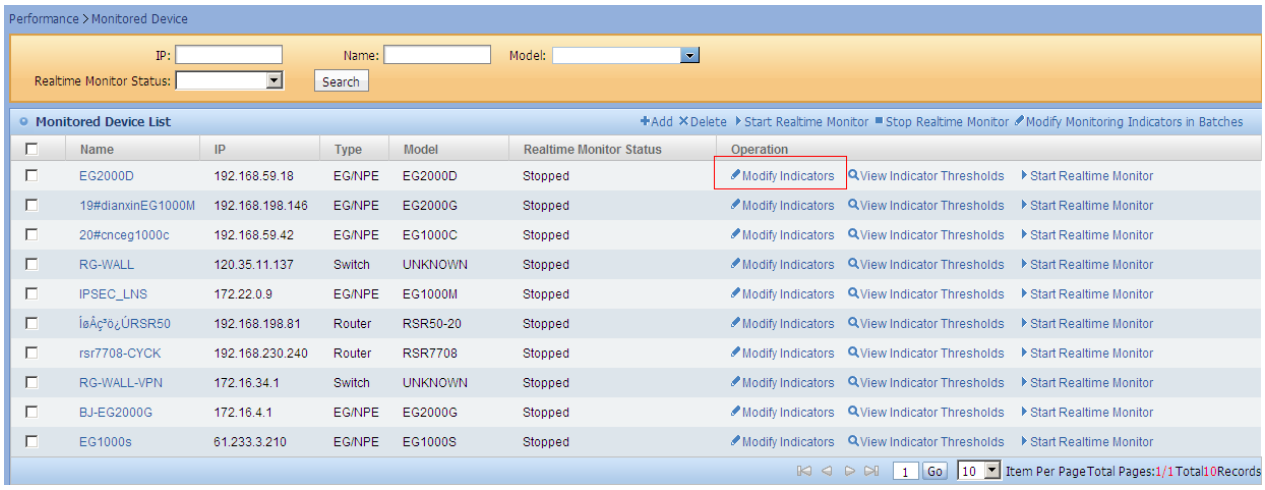


Figure 5.18. Monitored Device Management page

Select a monitored device entry and click the modify link under the operation column, the system will enter the page where you can modify the threshold value for the KPI. As shown by the screenshot below:

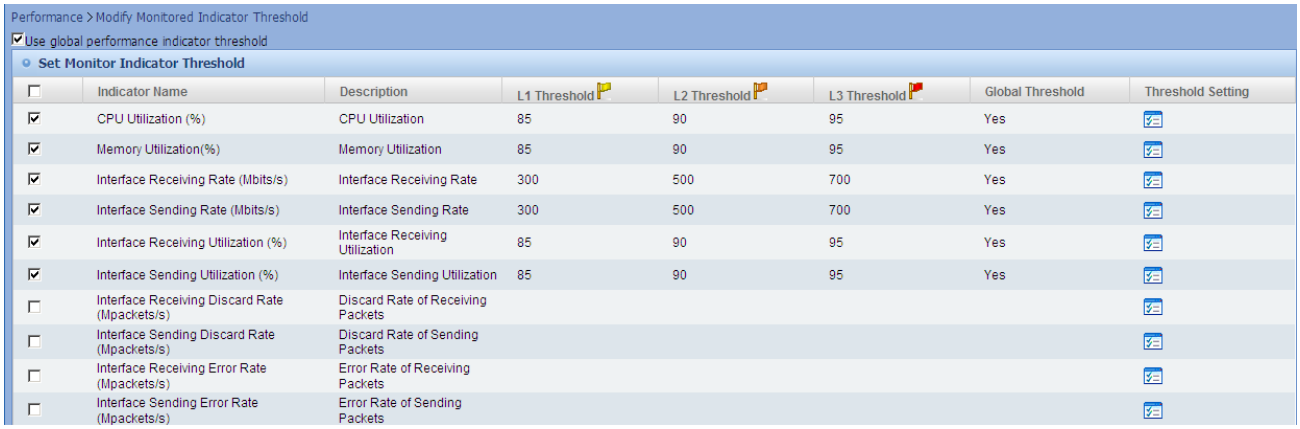


Figure 5.19. Set monitor indicator threshold page

Note

You can enable warning for any KPI just by selecting it in this page, that is, if the KPI is not selected, only the data is collected but no warning will be emit for it. Notice: to enable KIP for interfaces, you have also configure the “switch on/off for monitoring”(default to off), please refer to **Device interface detail information** page for more information.

On the monitor indicator threshold setting page, select all the KPIs that need to be modifies and click **Modify** to commit the new threshold value that you input, then the system will return to the query page. As shown by the screenshot below:

Figure 5.20. Modify monitoring indicator page

5.4.5. View Monitored Device Details

On the monitored device page, click the view indicator threshold link and the system will go into the detail information page, as shown by the screenshot below:

Performance > View Global Performance Indicator Thresholds

Global Performance Indicator Threshold List

Default

Indicator Name	Description	L1 Threshold	L2 Threshold	L3 Threshold	Threshold Setting
CPU Utilization (%)	CPU Utilization	85	90	95	Set
Memory Utilization(%)	Memory Utilization	85	90	95	Set
Interface Receiving Rate (Mbits/s)	Interface Receiving Rate	300	500	700	Set
Interface Sending Rate (Mbits/s)	Interface Sending Rate	300	500	700	Set
Interface Receiving Utilization (%)	Interface Receiving Utilization	85	90	95	Set
Interface Sending Utilization (%)	Interface Sending Utilization	85	90	95	Set
Interface Receiving Discard Rate(Mpackets/s)	Discard Rate of Receiving Packets	1	4	5	Set
Interface Sending Discard Rate(Mpackets/s)	Discard Rate of Sending Packets	1	4	5	Set
Interface Receiving Error Rate(Mpackets/s)	Error Rate of Receiving Packets	1	4	5	Set
Interface Sending Error Rate(Mpackets/s)	Error Rate of Sending Packets	1	4	5	Set
Interface Receiving Unicast Rate(Mpackets/s)	Rate of Receiving Unicast Packets	1	4	5	Set
Interface Sending Unicast Rate(Mpackets/s)	Rate of Sending Unicast Packets	1	4	5	Set

Figure 5.21. View indicator threshold devices

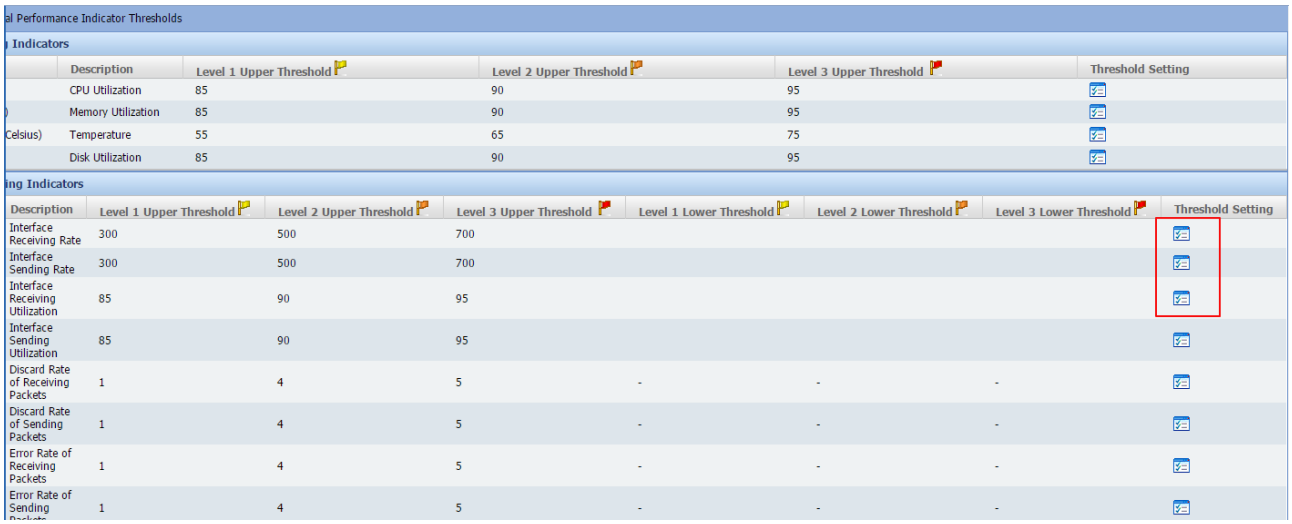
5.4.6. Enable Low Thresholds

Low threshold can be configured only for the following indicators: Interface Receiving Rate, Interface Sending Rate, Interface Receiving Utilization, Interface Sending Utilization.

Operation Steps

1. Go to **Performance** > **Global Perf Thresholds**.

2. Click **Threshold Setting** of a specified indicator to set global low thresholds.

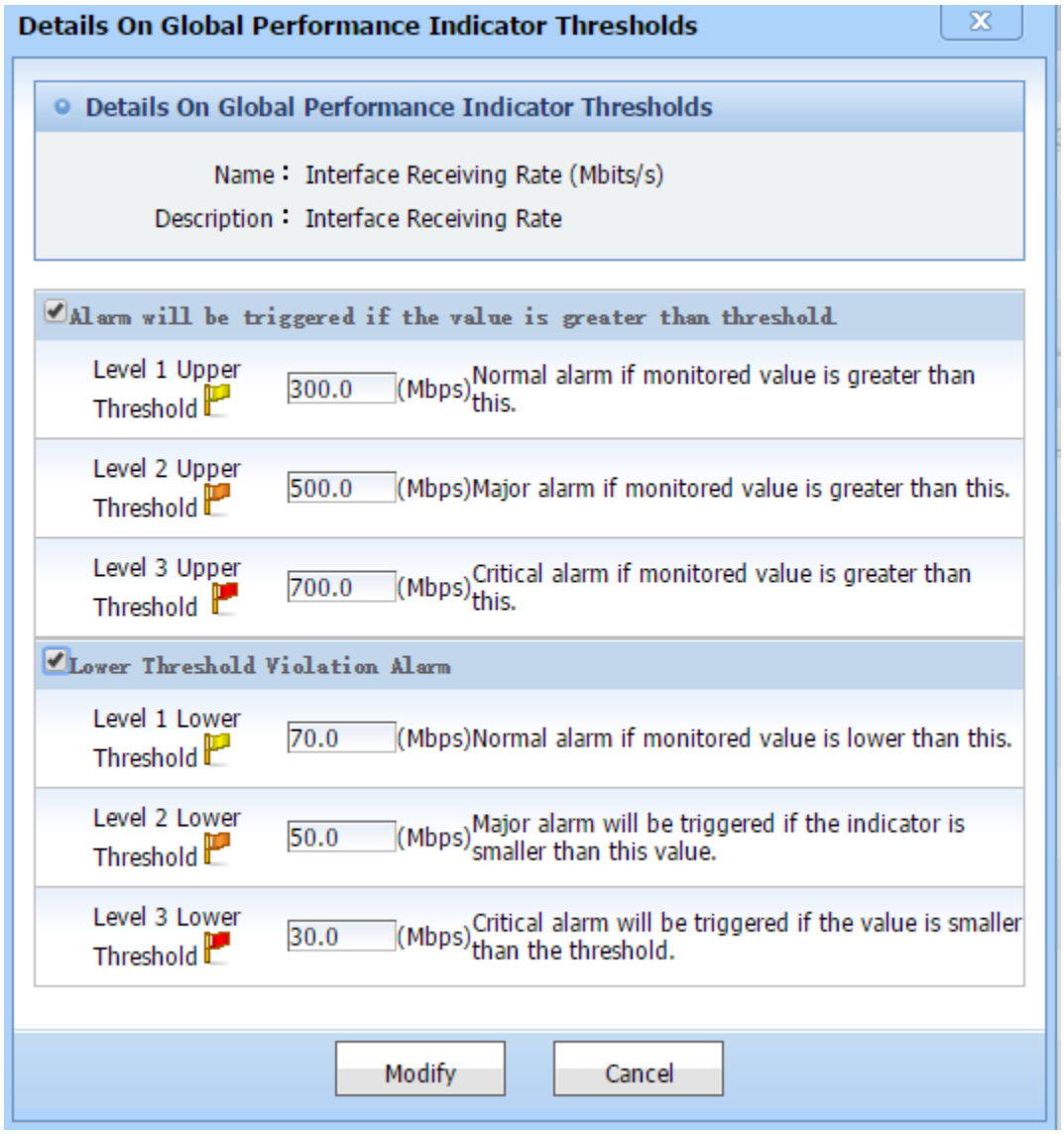


al Performance Indicator Thresholds

	Description	Level 1 Upper Threshold	Level 2 Upper Threshold	Level 3 Upper Threshold	Threshold Setting
	CPU Utilization	85	90	95	
)	Memory Utilization	85	90	95	
Celsius)	Temperature	55	65	75	
	Disk Utilization	85	90	95	

ng Indicators

Description	Level 1 Upper Threshold	Level 2 Upper Threshold	Level 3 Upper Threshold	Level 1 Lower Threshold	Level 2 Lower Threshold	Level 3 Lower Threshold	Threshold Setting
Interface Receiving Rate	300	500	700				
Interface Sending Rate	300	500	700				
Interface Receiving Utilization	85	90	95				
Interface Sending Utilization	85	90	95				
Discard Rate of Receiving Packets	1	4	5	-	-	-	
Discard Rate of Sending Packets	1	4	5	-	-	-	
Error Rate of Receiving Packets	1	4	5	-	-	-	
Error Rate of Sending	1	4	5	-	-	-	



5.5. View the Performance Curve in Real Time

Once the device is under monitor, you can view the realtime KPI line chart in device detail page or interface detail page.

Main curves

- View the performance curves of CPU and memory in real time
- View the performance curves of CPU and memory on high-end and stacked devices in real time
- View the performance curves for each index of interfaces in real time

5.5.1. View the Performance Curves of CPU and Memory in Real Time

1) Select **Device** tab to open device management page.

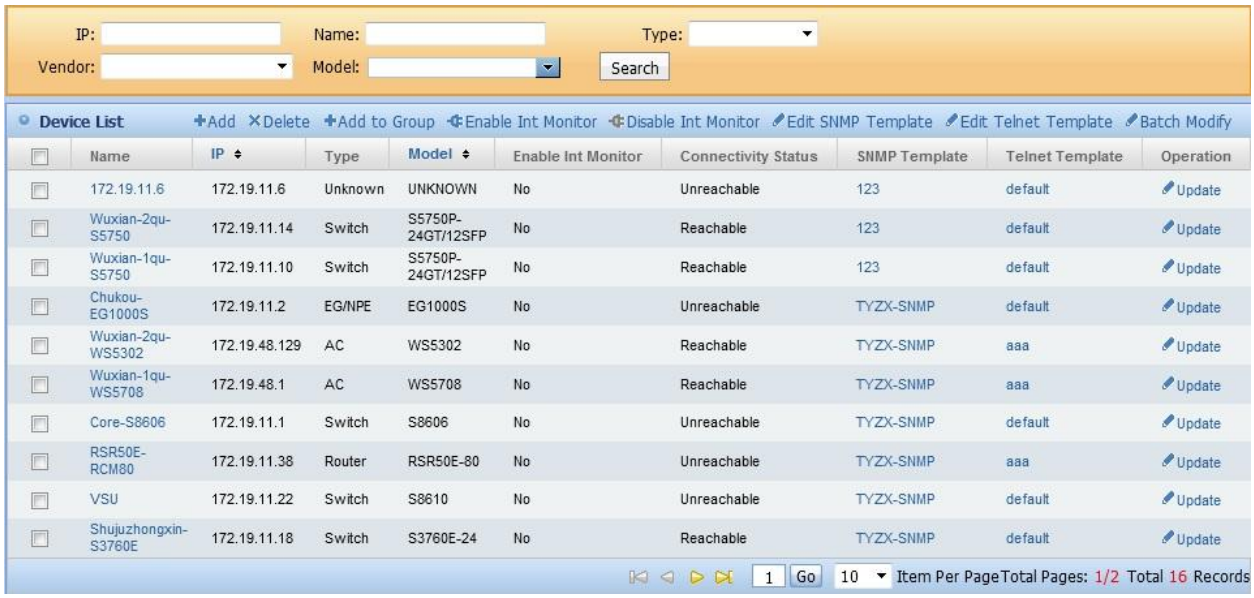


Figure 5.22. Device management page

Select a device entry, click the “device name” link to open the device detail page, as shown by the screenshot below:

Device > Device detail

Device Panel

Green=Administration status UP + working status UP Orange=Administration status UP + working status DOWN Red=Administration status DOWN + working status DOWN

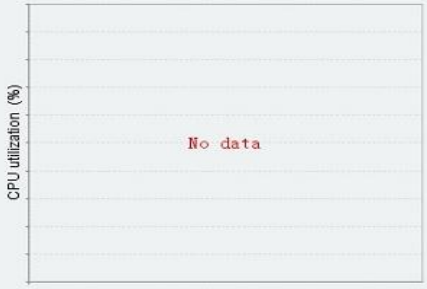
Basic Info | Other Info | IP Table | ARP Table | Route Table | Interface Table | MAC Fwd Table

Name	Wuxian-2qu-S5750	IP	172.19.11.14
Type	Switch	Model	S5750P-24GT/12SFP
Hardware Version	1.6	Software Version	RGOS 10.3(4b3), Release(65758)
Runtime	20 days, 4:12:47.81	Last Synchronization Time	2011-10-28 14:31:45
Connectivity Status	Reachable	SNMP Connectivity Status	Connected
Telnet Connectivity Status	Connected	SystemFan Status	
Power Source Info		Disk Utilization	
Device Temperature			

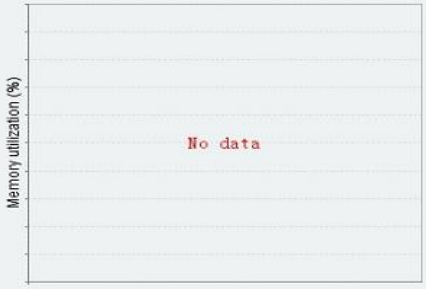
Update

Select Line Card

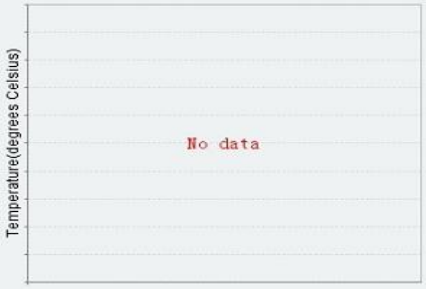
Realtime CPU Utilization Curve



Realtime Memory Curve



Realtime Temperature curve



Latest 10 Alarms

Alarm Category	Level	Event	Description	Last Alarm Time
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-31 14:58:01
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-28 18:03:51
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-27 15:25:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-27 14:35:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 11:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 10:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 08:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 07:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 04:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 03:55:00

Return To List

Figure 5.23. View the performance curves of CPU and memory in real time in the “device detail” page

5.5.2. View the Performance Curves of CPU and Memory on High-end and Stacked Devices in Real Time

1) Select **Device** tab to open device management page.

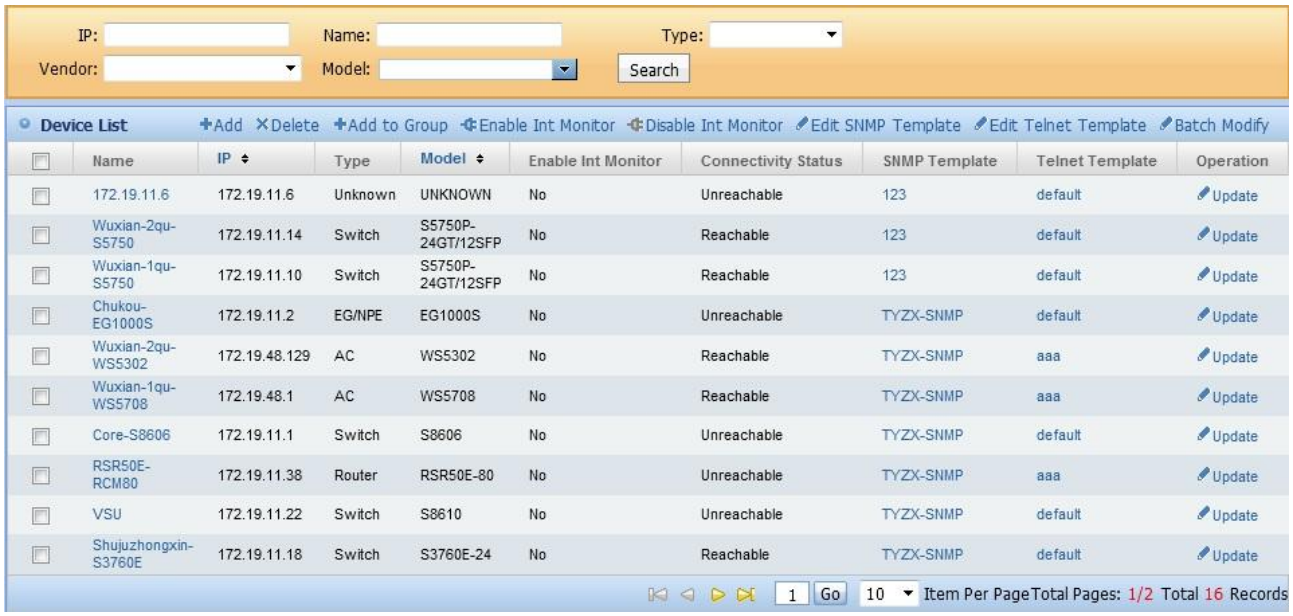


Figure 5.24. Device management page

Select a high-end or stacked device entry, click the “device name” link to open the device detail page, as shown by the screenshot below:

Device > Device detail

Device Panel

Green=Administration status UP + working status UP Orange=Administration status UP + working status DOWN Red=Administration status DOWN + working status DOWN

Basic Info | Other Info | IP Table | ARP Table | Route Table | Interface Table | MAC Fwd Table

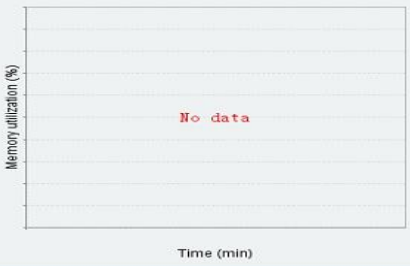
Name	RSR50E-RCM80	IP	172.19.11.38
Type	Router	Model	RSR50E-80
Hardware Version	1.02	Software Version	RGOS 10.4(2b2) Release(85900)
Runtime	0:05:26.74	Last Synchronization Time	2011-10-26 17:18:10
Connectivity Status	Reachable	SNMP Connectivity Status	Connected
Telnet Connectivity Status	Connected	SystemFan Status	Number1SystemFan Status:NORMAL Number2SystemFan Status:NORMAL Number3SystemFan Status:NORMAL Number4SystemFan Status:NORMAL Number5SystemFan Status:NORMAL Number6SystemFan Status:NORMAL
Power Source Info	Number1=Power Source Status:NORMAL Number2=Power Source Status:POWER OFF Number3=Power Source Status:NO EXIST	Disk Utilization	
Device Temperature	NumberHostTemperature:35		

Update

Select Line Card

Realtime CPU Utilization Curve

Realtime Memory Curve



Realtime Temperature curve

Latest 10 Alarms

Alarm Category	Level	Event	Description	Last Alarm Time
Device		Temperature exceeding threshold	The Host temperature of device whose name is [RSR50E-RCM80] and IP is [172.19.11.38] reached 35 degree Celsius, exceeded threshold Frist Level value 30.	2011-10-31 15:18:01
Device		Cold start	Device Cold Restarted	2011-10-31 15:15:35
Device		Link Up	The linking status of Device 172.19.11.38 Port Gi0/3 is UP.	2011-10-31 15:15:33
Device		Device unreachable event	Device Un-connectable	2011-10-31 10:31:48
Device		Temperature exceeding threshold	The Host temperature of device whose name is [RSR50E-RCM80] and IP is [172.19.11.38] reached 38 degree Celsius, exceeded threshold Frist Level value 30.	2011-10-28 16:33:53
Device		SNMP authentication failure	SNMP request containing wrong community received .	2011-10-28 13:17:11
Device		Cold start	Device Cold Restarted	2011-10-28 08:38:43
Device		Cold start	Device Cold Restarted	2011-10-27 11:52:51
Device		Device unreachable event	Device Un-connectable	2011-10-26 17:18:10
Device		Device unreachable event	Device Un-connectable	2011-10-22 04:02:39

Return To List

Figure 5.25. View the performance curves of CPU and memory on high-end and stacked devices in real time

5.5.3. View the Performance Curves for Each Index of Interfaces in Real Time

1) Select **Device** tab to open device management page.

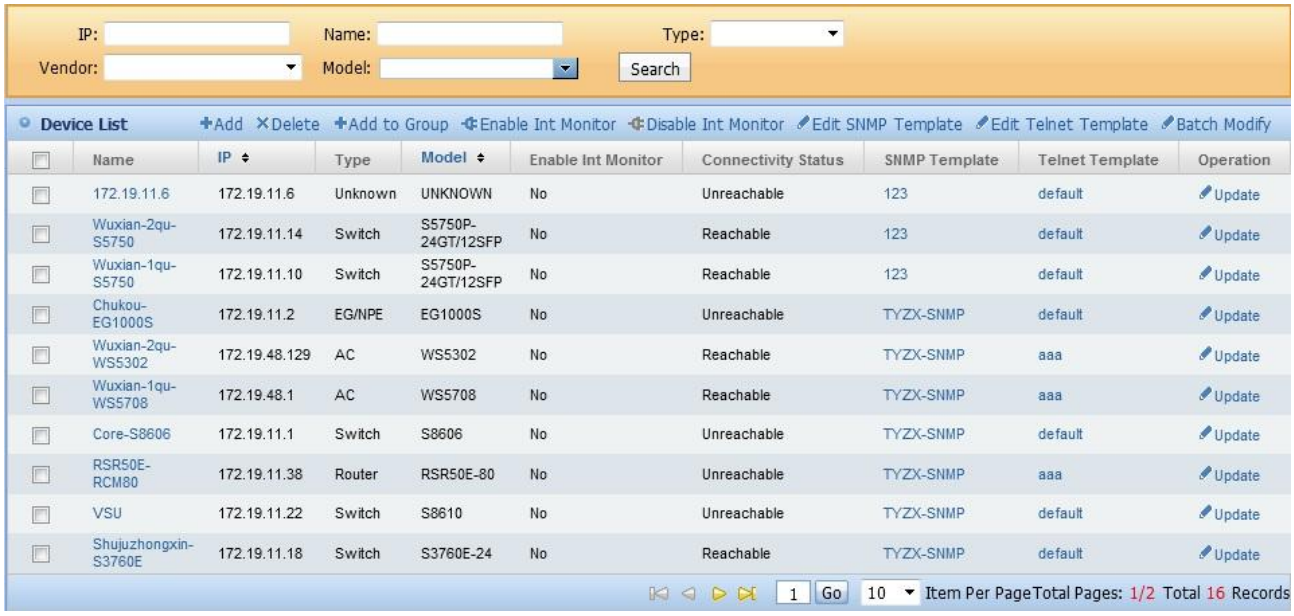


Figure 5.26. Device management page

Select a device entry, click the “device name” link to open the device detail page, as shown by the screenshot below:

Device > Device detail

Device Panel

Green=Administration status UP + working status UP Orange=Administration status UP + working status DOWN Red=Administration status DOWN + working status DOWN

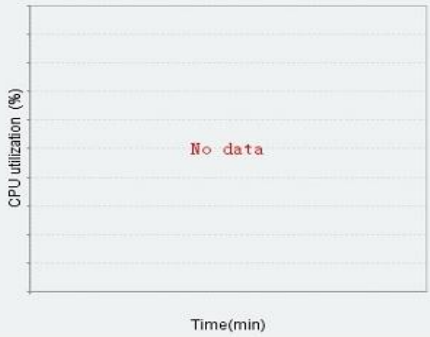
Basic Info | Other Info | IP Table | ARP Table | Route Table | Interface Table | MAC Fwd Table

Name	Wuxian-2qu-S5750	IP	172.19.11.14
Type	Switch	Model	S5750P-24GT/12SFP
Hardware Version	1.6	Software Version	RGOS 10.3(4b3), Release(65758)
Runtime	20 days, 4:12:47.81	Last Synchronization Time	2011-10-28 14:31:45
Connectivity Status	Reachable	SNMP Connectivity Status	Connected
Telnet Connectivity Status	Connected	SystemFan Status	
Power Source Info		Disk Utilization	
Device Temperature			

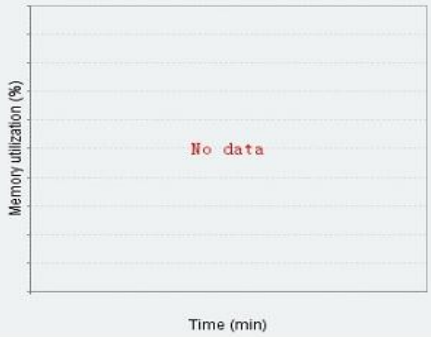
Update

Select Line Card

Realtime CPU Utilization Curve



Realtime Memory Curve



Realtime Temperature curve

Latest 10 Alarms

Alarm Category	Level	Event	Description	Last Alarm Time
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-31 14:58:01
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-28 18:03:51
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-27 15:25:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 63, exceeding threshold Frist Level value 50%	2011-10-27 14:35:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 11:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 10:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 08:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 07:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 04:55:00
Performance		Memory threshold exceeded	Usage of memory Host in device whose name is [Wuxian-2qu-S5750] and IP is [172.19.11.14] reached 56, exceeding threshold Frist Level value 50%	2011-10-27 03:55:00

Return To List

Figure 5.27. Device detail page

Click an interface link to open the interface detail page, as shown by the screenshot below:

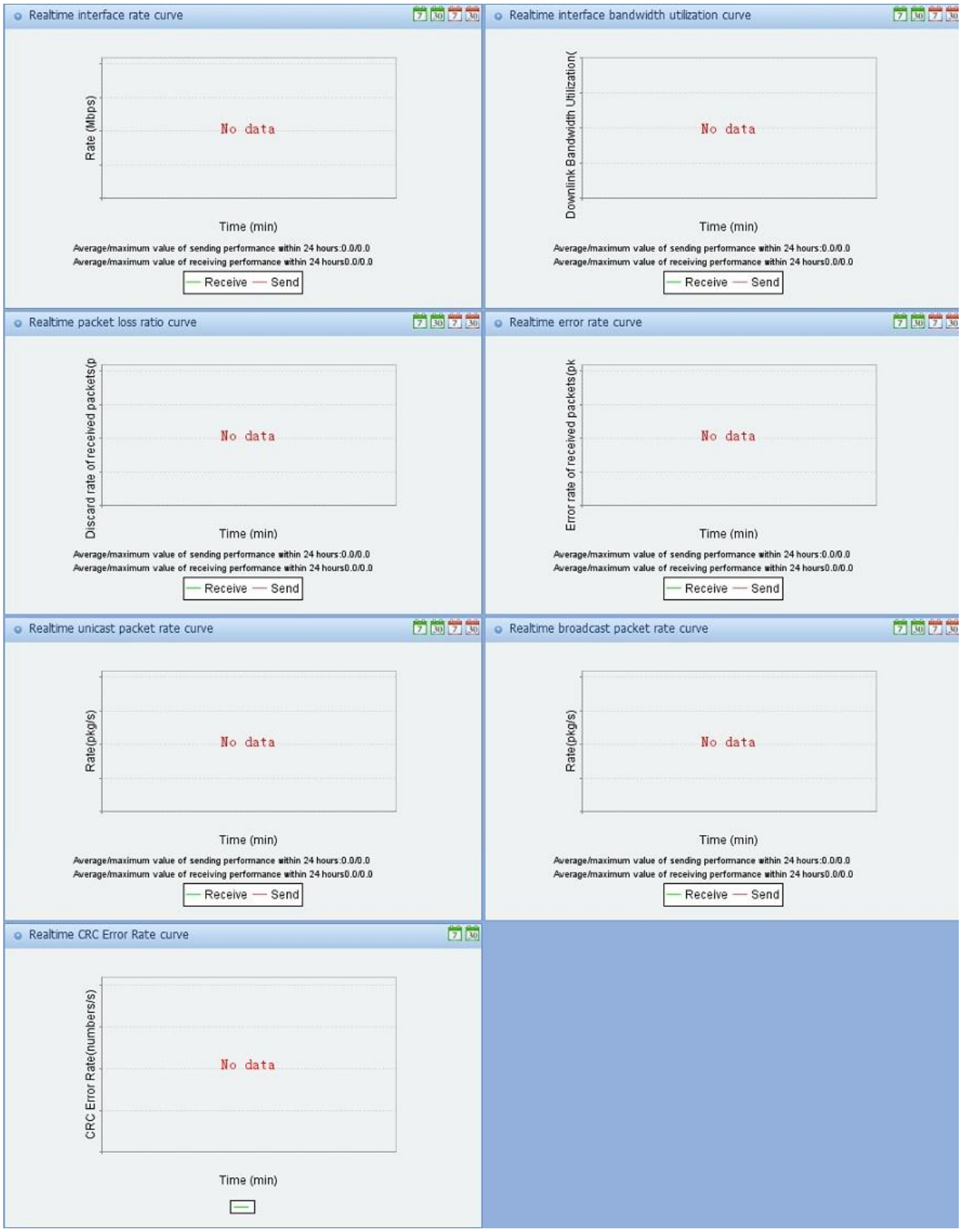


Figure 5.28. Interface detail page - realtime performance line chart

5.6. Query and Export for Performance History Data

You can query performance history data and export the result to a file.

- Query and export performance history data
- Query and export the performance history data of high-end or stacked devices

5.6.1. Query and Export Performance History Data

1) Select **Device** tab and open the device management page.

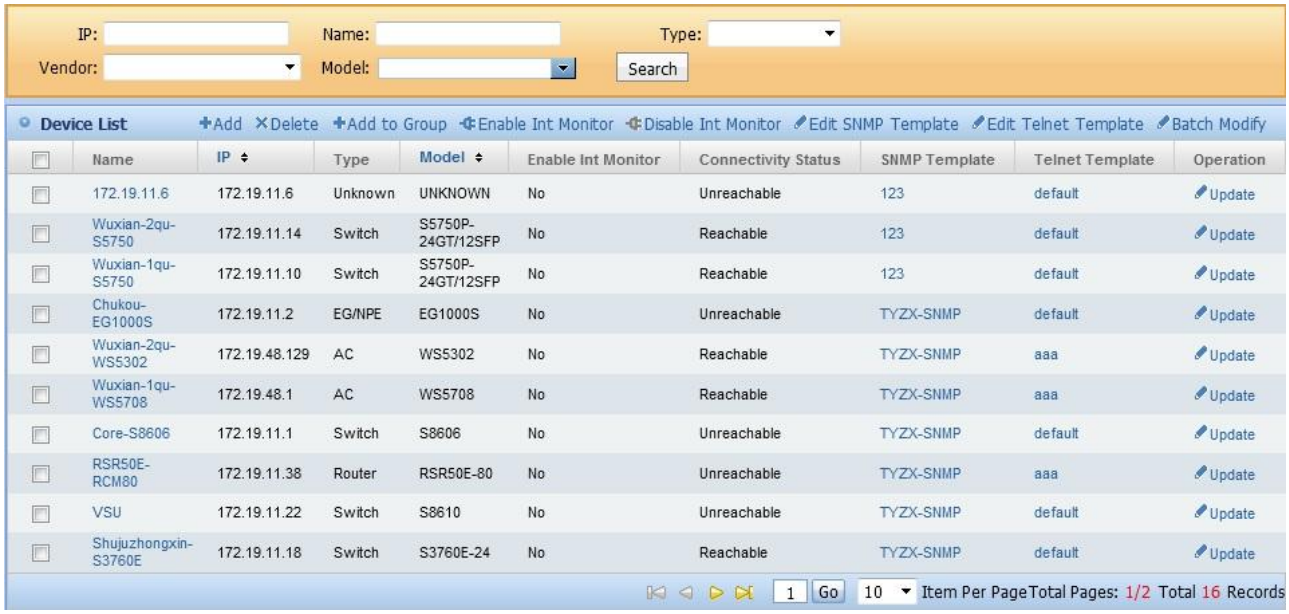


Figure 5.29. Device management page

Select a device entry, click the “device name” link to open the device detail page, as shown by the screenshot below:

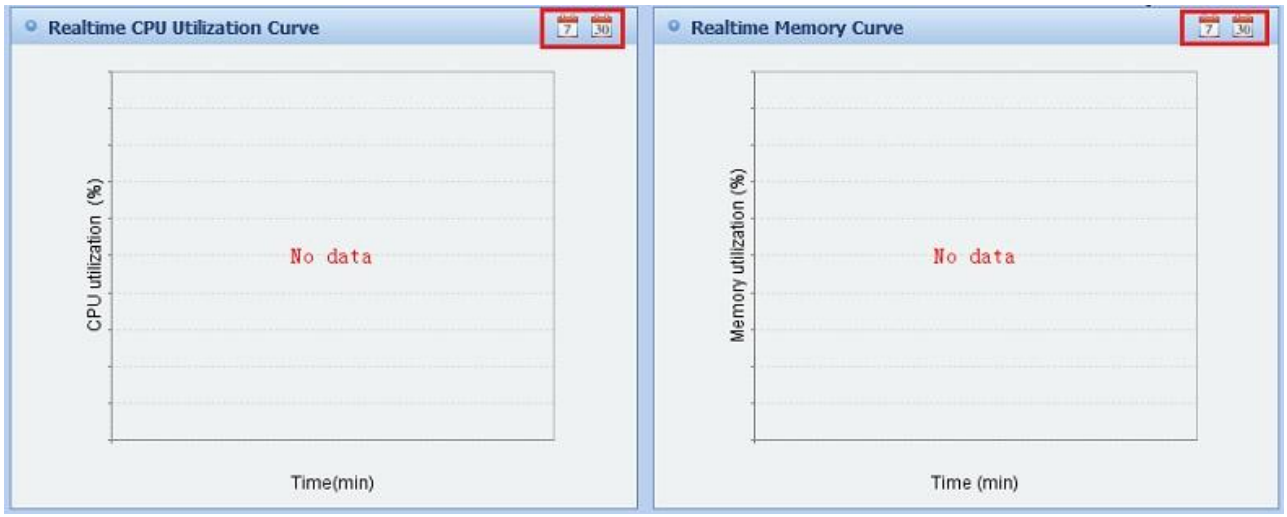


Figure 5.30. Device detail page

For KPI like CPU/Memory, you will enter the page to query and export performance history data by clicking the “7”/”30” icon on the top right of the line chart, as shown by the screenshot below:

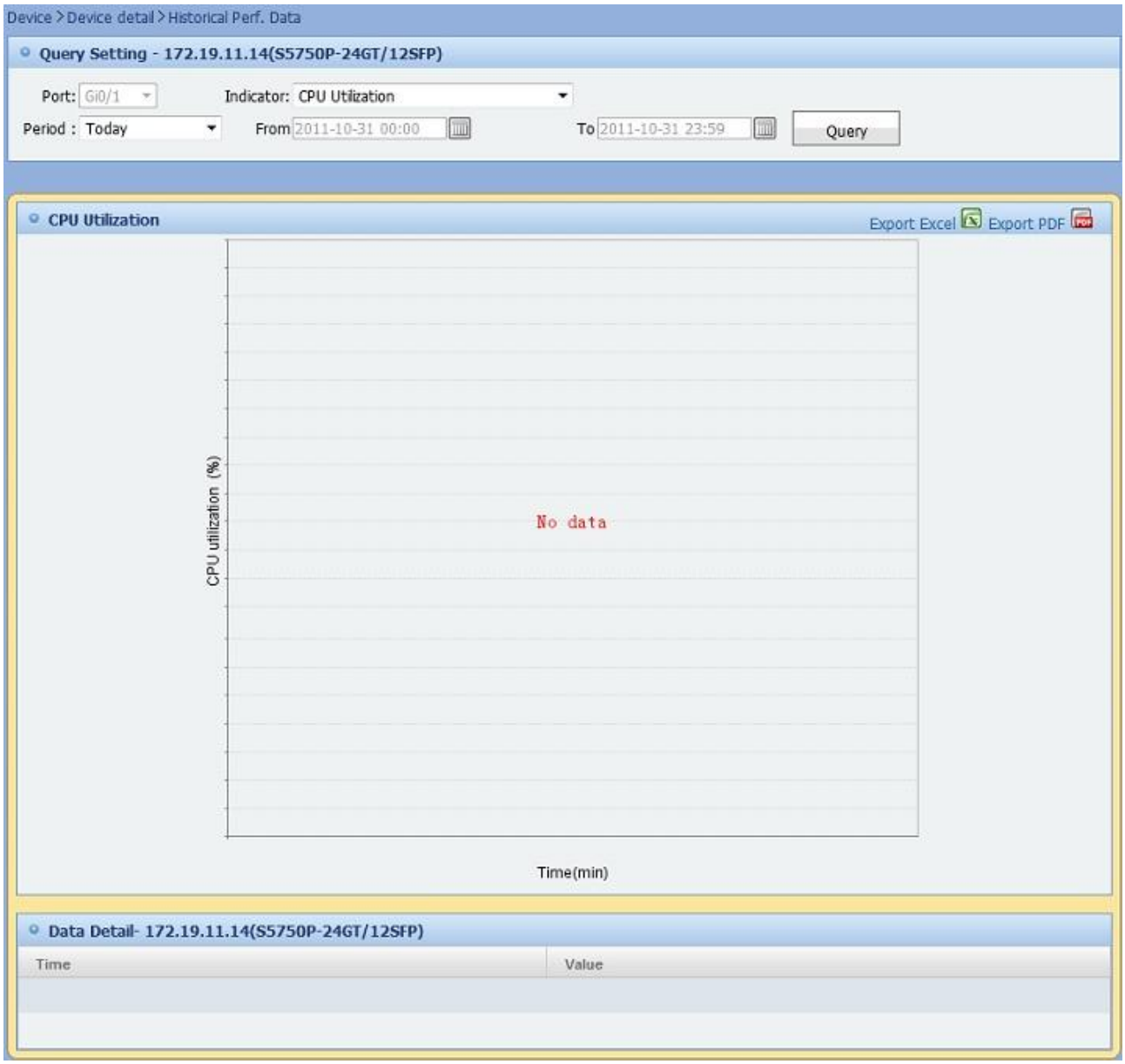


Figure 5.31. Device detail page

On the query and export page, select the KPIs you are interested in with a time range, the system will generate a line chart report for you, as shown by the screenshot below:

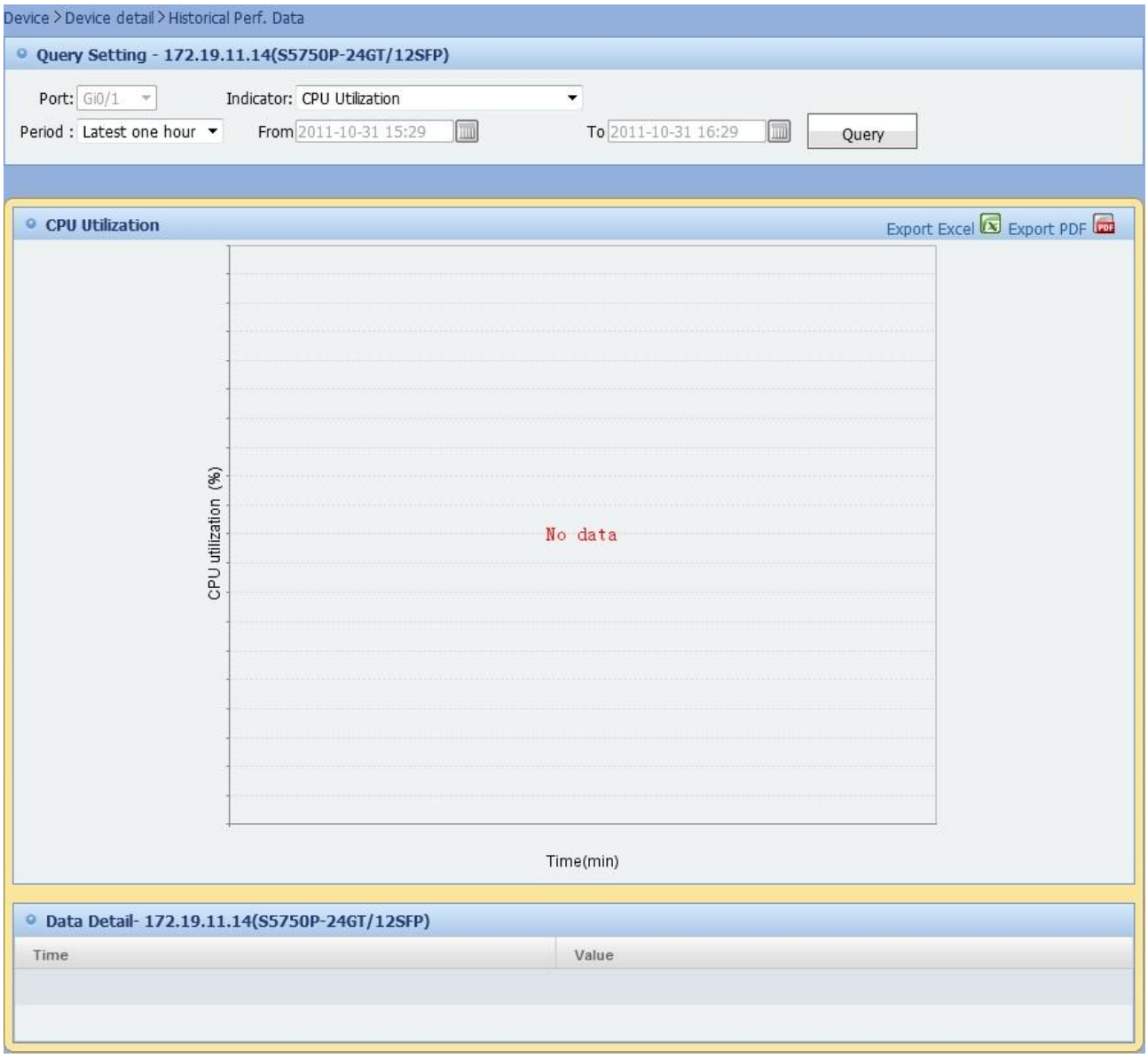


Figure 5.32. Query performance history data

Note The system has defined the following time ranges :Latest one hour: the system will fetch the performance history from one hour earlier to the current time and the history data is precise to minute.

-
- Today : the system will fetch today's performance history from 0:00 to current and the history data is precise to minute.
- Latest 7 days: the system will query performance history from 7 days ago to yesterday(excluding today) and the history data is precise to hour, including Max, Min and AVG value.
- Latest 30 days: the system will query performance history from 30 days ago to yesterday(excluding today) and the history data is precise to hour, including Max, Min and AVG value.
- Customize time: the system will query performance history within the specified time range(no earlier than 180 days ago) and the history data is precise to day, including Max, Min and AVG value.

Note Only with the customize time option can you set the time slot and the time is precise to day.

On the device detail page, you will enter the page to query and export performance history data by clicking the "7"/"30" icon on the top right of the line chart for the KPI, as shown by the screenshot below:

Figure 5.33. Query performance history data

5.6.2. Query and Export the Performance History Data of High-end or Stacked Devices

1) Select "**Device**" tab and open the device management page.

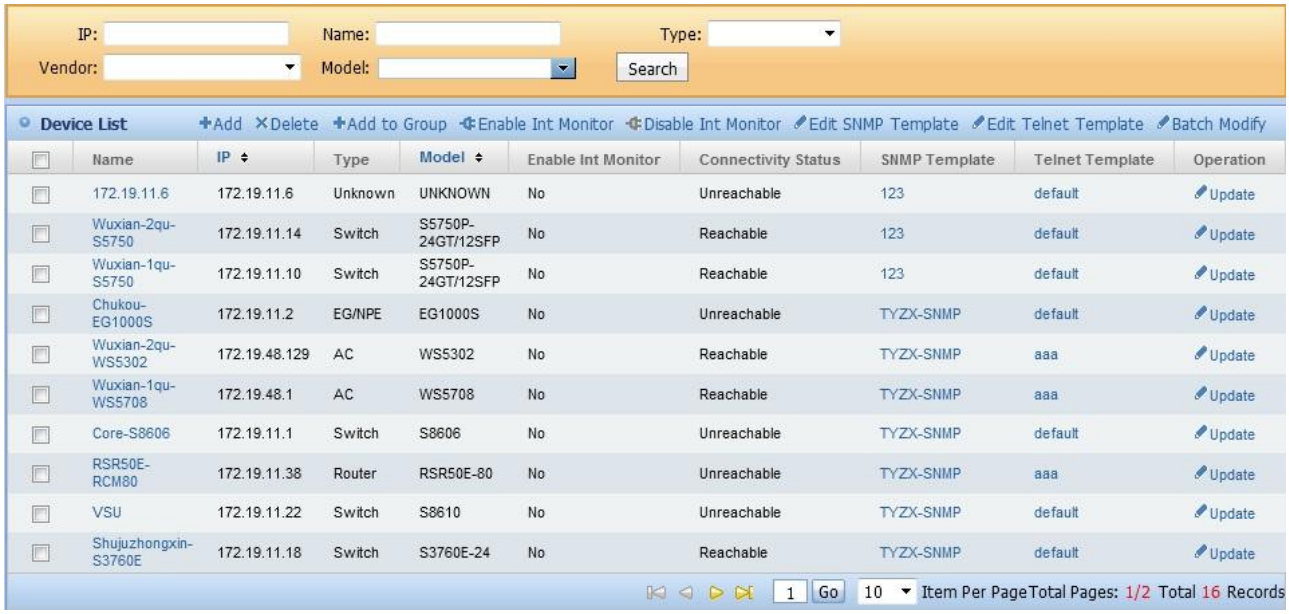


Figure 5.34. Device management page

Select a high-end or stacked device entry, click the "device name" link to open the device detail page, as shown by the screenshot below:

Device > Device detail

Device Panel

Green=Administration status UP + working status UP Orange=Administration status UP + working status DOWN Red=Administration status DOWN + working status DOWN

Basic Info | Other Info | IP Table | ARP Table | Route Table | Interface Table | MAC Fwd Table

Name	RSR50E-RCM80	IP	172.19.11.38
Type	Router	Model	RSR50E-80
Hardware Version	1.02	Software Version	RGOS 10.4(2b2) Release(85900)
Runtime	0:05:26.74	Last Synchronization Time	2011-10-26 17:18:10
Connectivity Status	Reachable	SNMP Connectivity Status	Connected
Telnet Connectivity Status	Connected	SystemFan Status	Number1SystemFan Status:NORMAL Number2SystemFan Status:NORMAL Number3SystemFan Status:NORMAL Number4SystemFan Status:NORMAL Number5SystemFan Status:NORMAL Number6SystemFan Status:NORMAL
Power Source Info	Number1=Power Source Status:NORMAL Number2=Power Source Status:POWER OFF Number3=Power Source Status:NO EXIST	Disk Utilization	
Device Temperature	NumberHostTemperature:35		

Update

Select Line Card

Realtime CPU Utilization Curve

Realtime Memory Curve

Realtime Temperature curve

Latest 10 Alarms

Alarm Category	Level	Event	Description	Last Alarm Time
Device		Temperature exceeding threshold	The Host temperature of device whose name is [RSR50E-RCM80] and IP is [172.19.11.38] reached 35 degree Celsius, exceeded threshold Frist Level value 30.	2011-10-31 15:18:01
Device		Cold start	Device Cold Restarted	2011-10-31 15:15:35
Device		Link Up	The linking status of Device 172.19.11.38 Port Gi0/3 is UP.	2011-10-31 15:15:33
Device		Device unreachable event	Device Un-connectable	2011-10-31 10:31:48
Device		Temperature exceeding threshold	The Host temperature of device whose name is [RSR50E-RCM80] and IP is [172.19.11.38] reached 38 degree Celsius, exceeded threshold Frist Level value 30.	2011-10-28 16:33:53
Device		SNMP authentication failure	SNMP request containing wrong community received .	2011-10-28 13:17:11
Device		Cold start	Device Cold Restarted	2011-10-28 08:38:43
Device		Cold start	Device Cold Restarted	2011-10-27 11:52:51
Device		Device unreachable event	Device Un-connectable	2011-10-26 17:18:10
Device		Device unreachable event	Device Un-connectable	2011-10-22 04:02:39

Return To List

Figure 5.35. Device detail page

For KPI like CPU/Memory, you will enter the page to query and export performance history data by clicking the “7”/”30” icon on the top right of the line chart, as shown by the screenshot below:

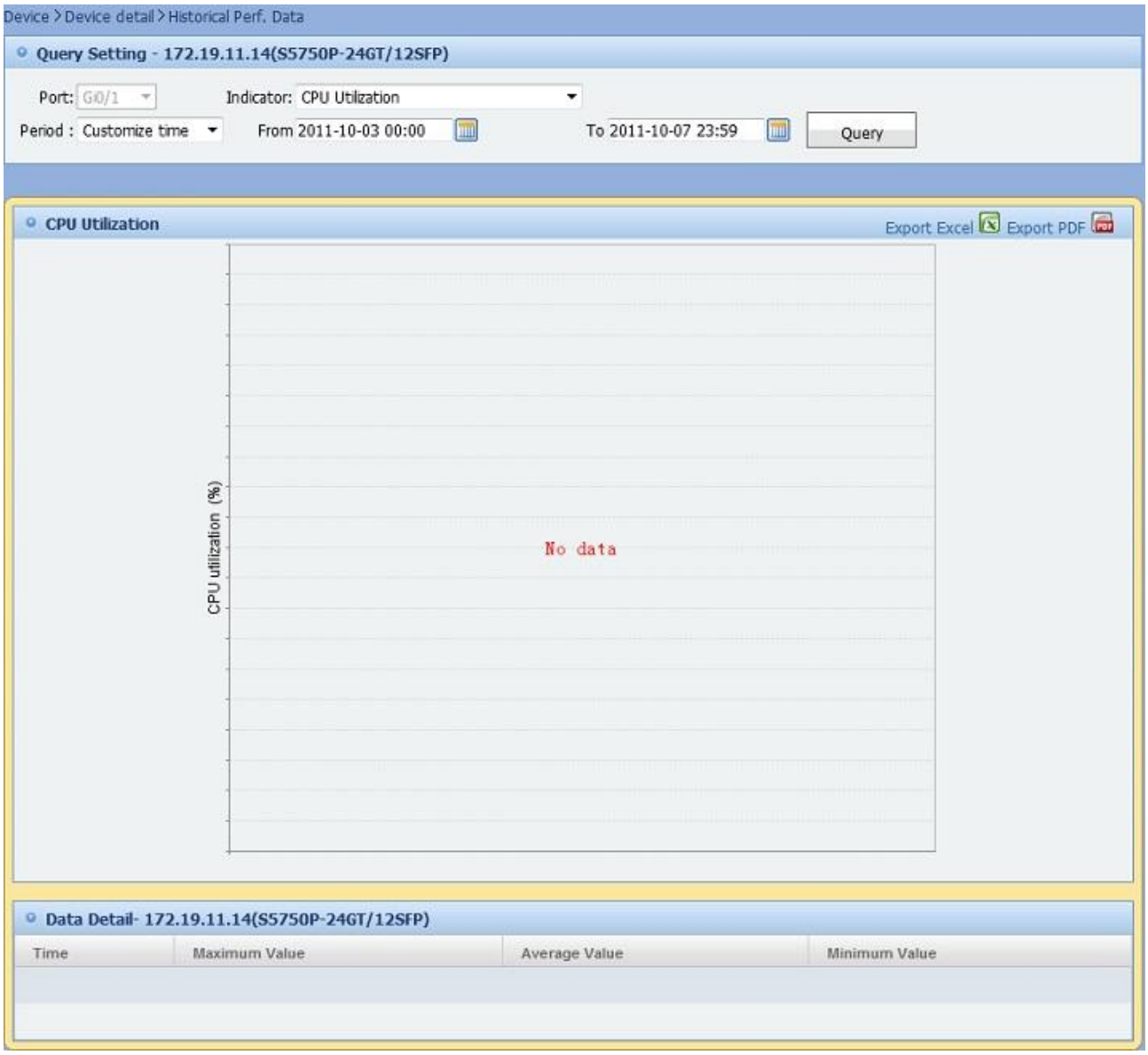


Figure 5.36. Device detail page

On the query and export page, select the KPIs you are interested in with a time range, the system will generate a line chart report for you, as shown by the screenshot below:

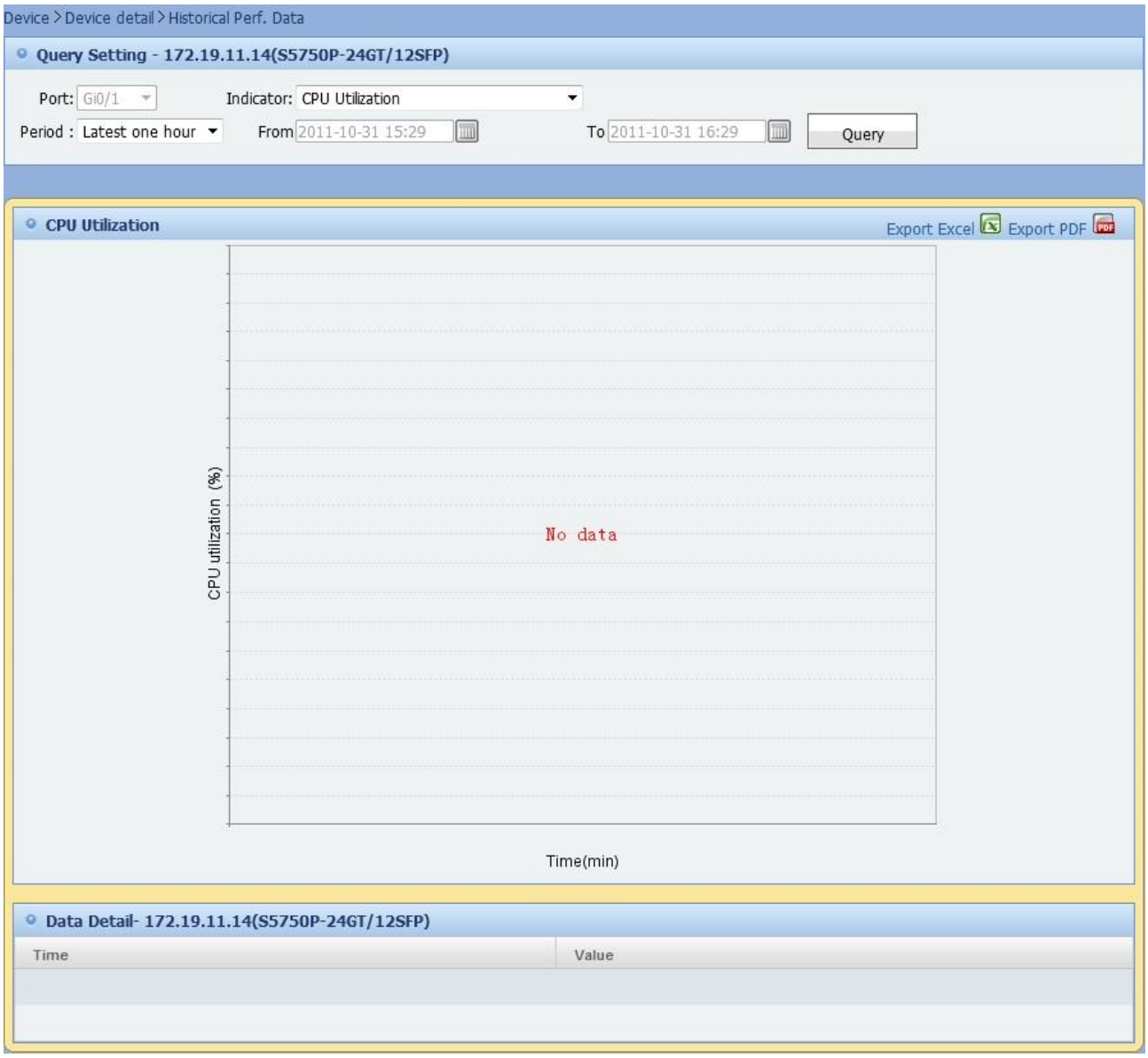


Figure 5.37. Query performance history data

Note The system has defined the following time ranges :Latest one hour: the system will fetch the performance history from one hour earlier to the current time and the history data is precise to minute.

- Today : the system will fetch today's performance history from 0:00 to current and the history data is precise to minute.
- Latest 7 days: the system will query performance history from 7 days ago to yesterday(excluding today) and the history data is precise to hour, including Max, Min and AVG value.
- Latest 30 days: the system will query performance history from 30 days ago to yesterday(excluding today) and the history data is precise to hour, including Max, Min and AVG value.
- Customize time: the system will query performance history within the specified time range(no earlier than 180 days ago) and the history data is precise to day, including Max, Min and AVG value.

Note Only with the customize time option can you set the time slot and the time is precise to day.

On the device detail page, you will enter the page to query and export performance history data by clicking the "7"/"30" icon on the top right of the line chart for the KPI, as shown by the screenshot below:

Figure 5.38. Query performance history data

5.7. Single Device Monitoring

In this page, you can monitor the performance for one device and its interfaces.

1) On the **Performance Mgmt** page, select **Single-device View** item to open the monitor page.

Figure 5.39. Single device monitoring page

On the realtime monitoring page, move the mouse to the line on the chart, a tip will prompt with the collection time and value at that point.

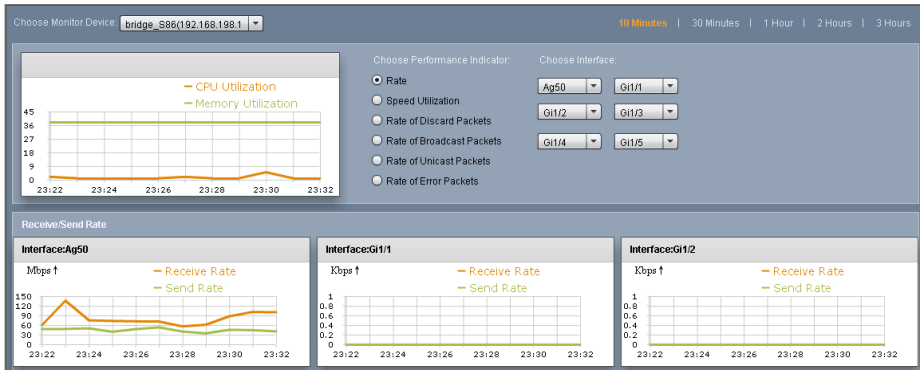


Figure 5.40. Single device monitoring page

In the single device monitoring page, you can do the following:

- Select a device to monitor: Select the IP of a device from the dropdown list on the top left of the page to select a device to monitor, and then the system will refresh right away.
- Select the monitoring time range: Select the time range from the dropdown list on the top right of the page. The default time range is 10 minutes (data collected from 10 minutes ago to now).
- Select KPI: There are 6 KPI groups for collecting performance data.
- Select interface: Interface is referred to the monitored interfaces. If the target device has no interface to be monitored, this function area will display nothing; if no more than 6 interfaces are monitored, a dropdown list will be displayed for each interface.

Note: The refresh rate is equal to the performance data sampling rate.

Note: Those interfaces that are not monitored will not appear in the selection list, since there is no interface at all.

Note: After you change the data sampling rate, it will cost some time for the system to collect data with new rate(it may take up to minutes).

Note: Operation like adding, deleting realtime monitored device, switching interface monitoring on/off will cause a change in the object being monitored and the change will be shown after the coming refresh.

5.8. Multiple Device Monitoring

In the multiple device monitoring page, you are able to select more than one device(or interface) and monitor them concurrently.

1) Open the **Performance Mgmt** page, and click **All View** to open the page.

On the realtime monitor page, move the mouse to the line on the chart, a tip will prompt up with sample time and value at that point.

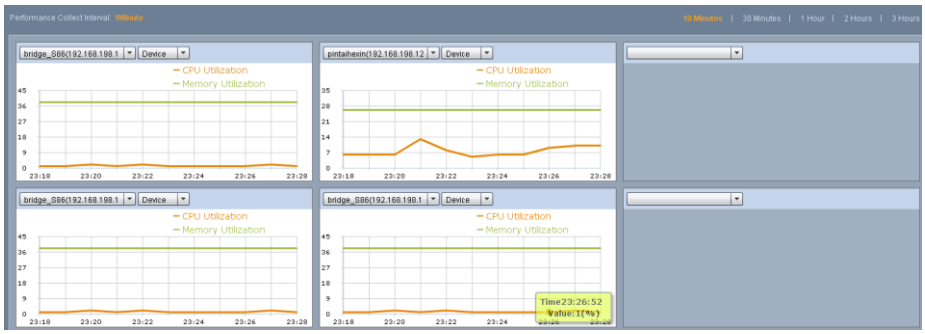


Figure 5.41. Multiple device monitoring page

On the device monitoring page, select the device you are interested in from the dropdown list box on the top left of the graph. Once the device is selected, you need to specify whether it is “device” or “interface” on the second dropdown list box. If “device” is specified, CPU/Memory data is displayed; if “interface” is specified, a third dropdown list will show up for you to choose which KPI’s chart should be drawn.

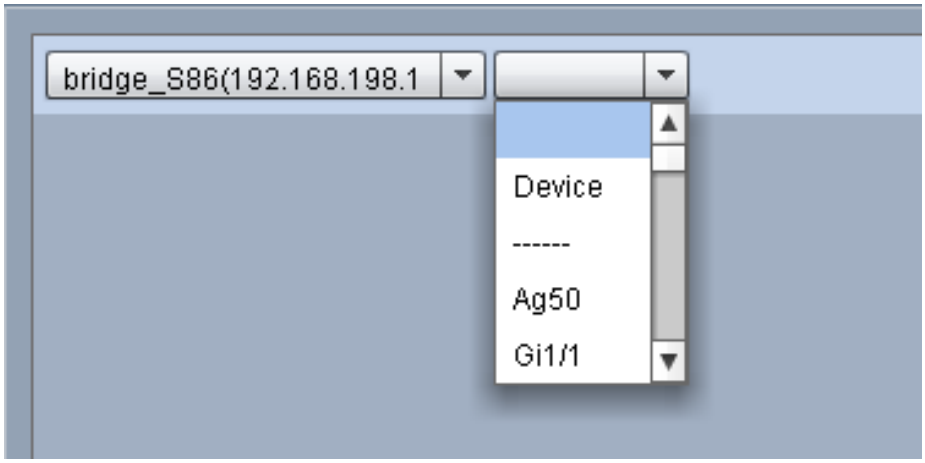


Figure 5.42. Multiple device monitoring page -- select device and interface

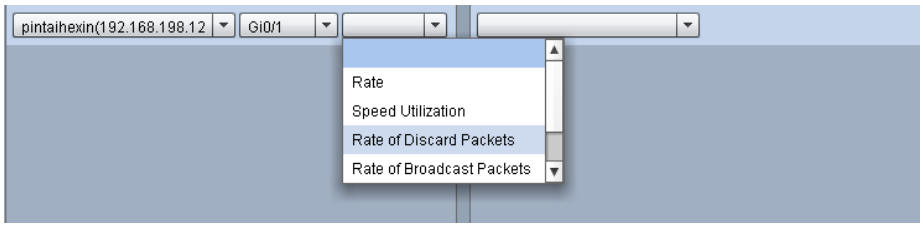


Figure 5.43. Multiple device monitoring page -- select KPI

On the “**Multiple device monitor**” page, you can select a performance data time range on the top right of the page. By default, 10 minutes is the used, that is, the system only display performance data from 10 minutes ago to now. Please be noted that the time range is applied to all devices.

Note	In the realtime monitoring page, the refresh rate is equal to the performance data sampling rate.
Note	Those interfaces that is not monitored will not appear in the selection list, since there is no interface at all.
Note	After you change the data sampling rate, it will cost some time for the system to collect data with new rate(it may take up to minutes).
Note	Operation like adding, deleting realtime monitored device, switching interface monitoring on/off will cause a change to the object being monitored and the change will be shown after the coming refresh.

Chapter 6 Alarm

The alarm module allows you to manage alarm information generated during device operation, including traps reported by all the managed devices, exceeding of performance thresholds, and configuration changes.

Function list

- Realtime Alarm Monitoring
- Historical Alarm Management
- Devices with Alarm
- Undefined Alarm Event
- Syslog realtime monitor
- Syslog Monitor History
- Alarm parameter
- Alarm notification
- Alarm rule
- Alarm Event Management
- Set SMS time range
- Alarm Forwarding
- Set the device event notification
- Syslog Template
- Syslog Overdue

6.1. Realtime Alarm Monitoring

This function enables you to view unacknowledged alarm events in real time, which are sorted in descending order of the alarm level.

Operation Steps

1) Click **Alarm** to go to the **Realtime Alarm View** page.

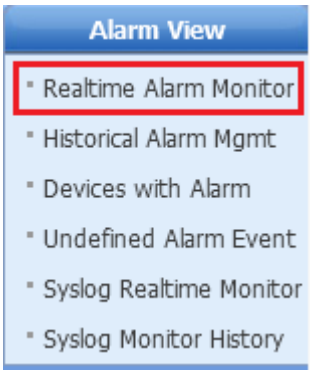
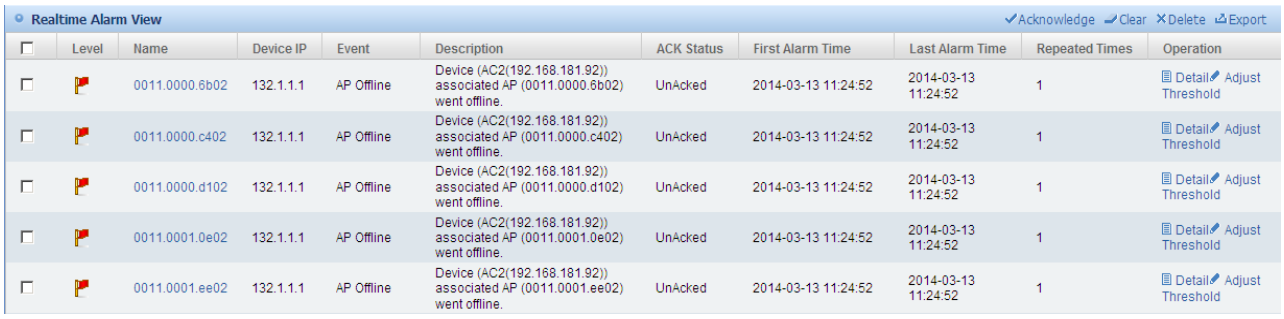


Figure 6.1. Realtime Alarm View Menu



Realtime Alarm View — Acknowledge Clear Delete Export

Level	Name	Device IP	Event	Description	ACK Status	First Alarm Time	Last Alarm Time	Repeated Times	Operation
	0011.0000.6b02	132.1.1.1	AP Offline	Device (AC2(192.168.181.92)) associated AP (0011.0000.6b02) went offline.	UnAcked	2014-03-13 11:24:52	2014-03-13 11:24:52	1	Detail Adjust Threshold
	0011.0000.c402	132.1.1.1	AP Offline	Device (AC2(192.168.181.92)) associated AP (0011.0000.c402) went offline.	UnAcked	2014-03-13 11:24:52	2014-03-13 11:24:52	1	Detail Adjust Threshold
	0011.0000.d102	132.1.1.1	AP Offline	Device (AC2(192.168.181.92)) associated AP (0011.0000.d102) went offline.	UnAcked	2014-03-13 11:24:52	2014-03-13 11:24:52	1	Detail Adjust Threshold
	0011.0001.0e02	132.1.1.1	AP Offline	Device (AC2(192.168.181.92)) associated AP (0011.0001.0e02) went offline.	UnAcked	2014-03-13 11:24:52	2014-03-13 11:24:52	1	Detail Adjust Threshold
	0011.0001.ee02	132.1.1.1	AP Offline	Device (AC2(192.168.181.92)) associated AP (0011.0001.ee02) went offline.	UnAcked	2014-03-13 11:24:52	2014-03-13 11:24:52	1	Detail Adjust Threshold

Figure 6.2. Realtime Alarm View

Major operations in Realtime Alarm View include: Tick the checkbox before the alarm event and click Acknowledge, Clear or Delete to change the alarm status or delete the alarm.
Select a value in the Display drop down box to change the number of alarms displayed in Realtime Alarm View.
Select a value in the Refresh Interval drop down box to change the page refresh interval.
Click the alarm device to go to the Device detail page.
Click to display the Alarm Details page.
Click to go to the Add Alarm Note page.

Major Functions

- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Delete alarm
- Alarm Details
- Add alarm remarks
- Modify Monitor Threshold
- Export alarm

Note: The acknowledged and cleared alarms are not displayed on the Realtime Alarm View page.

Note: If an alarm event is generated repeatedly, the alarm time is subject to the last alarm time. Otherwise, the alarm time is subject to the first alarm time.

Note: The alarm note cannot be modified or deleted.

Note: An alarm device in grey indicates that the device has been deleted.

Note: Click Adjust Threshold to go to the corresponding page.

6.1.1. Acknowledge Alarm/Cancel Acknowledgement

This function enables you to change the alarm ACK Status by performing the Acknowledge or Cancel Acknowledgement operation. The alarm status indicates whether the alarm has been managed.

Operation Steps

1) Click **Alarm** to go to the corresponding page.
Tick the checkbox before the alarm event.
Click **Acknowledge** or **Cancel Acknowledgement**, and the alarm ACK Status is changed.

Note: If you perform Cancel Acknowledgement on the acknowledged alarm, the alarm device is not affected.

Note: The Acknowledge or Cancel Acknowledgement operation should not be repeated.

Related Topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Clear Alarm
- Delete alarm
- Alarm Details

- Add alarm remarks

6.1.2. Clear Alarm

This function enables you to set the alarm Clear Status to cleared.

Operation Steps

1) Click **Alarm** to go to the corresponding page.
Tick the checkbox before the alarm event.
Click **Clear**, and the alarm Clear Status is changed to cleared.

Note The alarm ACK Status is changed to Acked if the alarm Clear Status is set to cleared.

Related Topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Delete alarm
- Alarm Details
- Add alarm remarks

6.1.3. Delete Alarm

You can delete an selected alarm from the alarm list.

Operation Steps

1) Select **Alarm** tab and open the page for realtime alarm monitor or historical alarm management.
Check the checkbox in front of the alarm entry.
Click **Delete** to delete the alarm.

Related topics

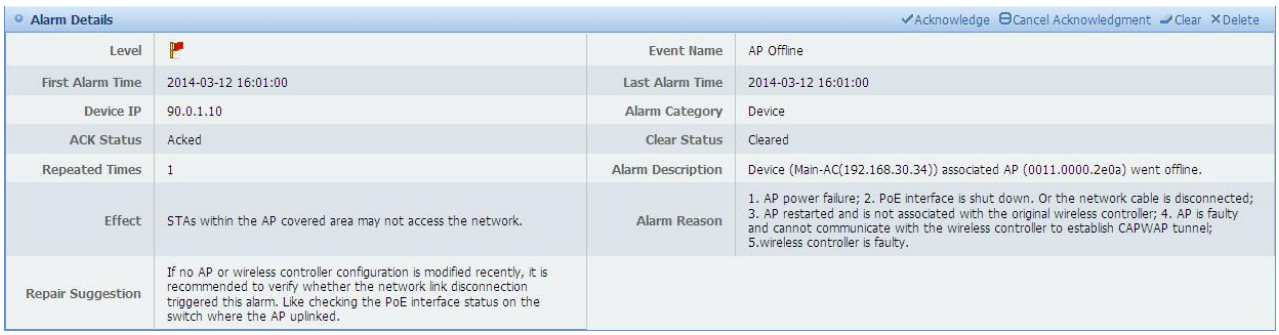
- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Alarm Details
- Add alarm remarks

6.1.4. Alarm Details

This function enables you to view the detailed information about an alarm, including alarm level, event, first alarm time, last alarm time, device, type, ACK status, ACK time, cause, repair suggestion. The cause and repair suggestion of an alarm help the administrator address similar faults. You can also add alarm notes and view the administrator's notes.

Operation Steps

1) Click **Alarm** to go to the corresponding page.



Alarm Details ✓Acknowledge ⊖Cancel Acknowledgment ✎Clear ✕Delete

Level		Event Name	AP Offline
First Alarm Time	2014-03-12 16:01:00	Last Alarm Time	2014-03-12 16:01:00
Device IP	90.0.1.10	Alarm Category	Device
ACK Status	Acked	Clear Status	Cleared
Repeated Times	1	Alarm Description	Device (Main-AC(192.168.30.34)) associated AP (0011.0000.2e0a) went offline.
Effect	STAs within the AP covered area may not access the network.	Alarm Reason	1. AP power failure; 2. PoE interface is shut down. Or the network cable is disconnected; 3. AP restarted and is not associated with the original wireless controller; 4. AP is faulty and cannot communicate with the wireless controller to establish CAPWAP tunnel; 5.wireless controller is faulty.
Repair Suggestion	If no AP or wireless controller configuration is modified recently, it is recommended to verify whether the network link disconnection triggered this alarm. Like checking the PoE interface status on the switch where the AP uplinked.		

Figure 6.3. Alarm Details

Click in the alarm list.

Related Topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Delete alarm
- Add alarm remarks

6.1.5. Add Alarm Remarks

Alarm remarks involve administrators' suggestions on alarm handling, suggestions, and methods; therefore providing clues for the administrator who needs to handle an alarm.

Operation Steps

1) Select **Alarm** tab, and you can view the page of realtime alarm monitoring or historical alarm management. Remarks for an alarm cannot be modified or deleted.

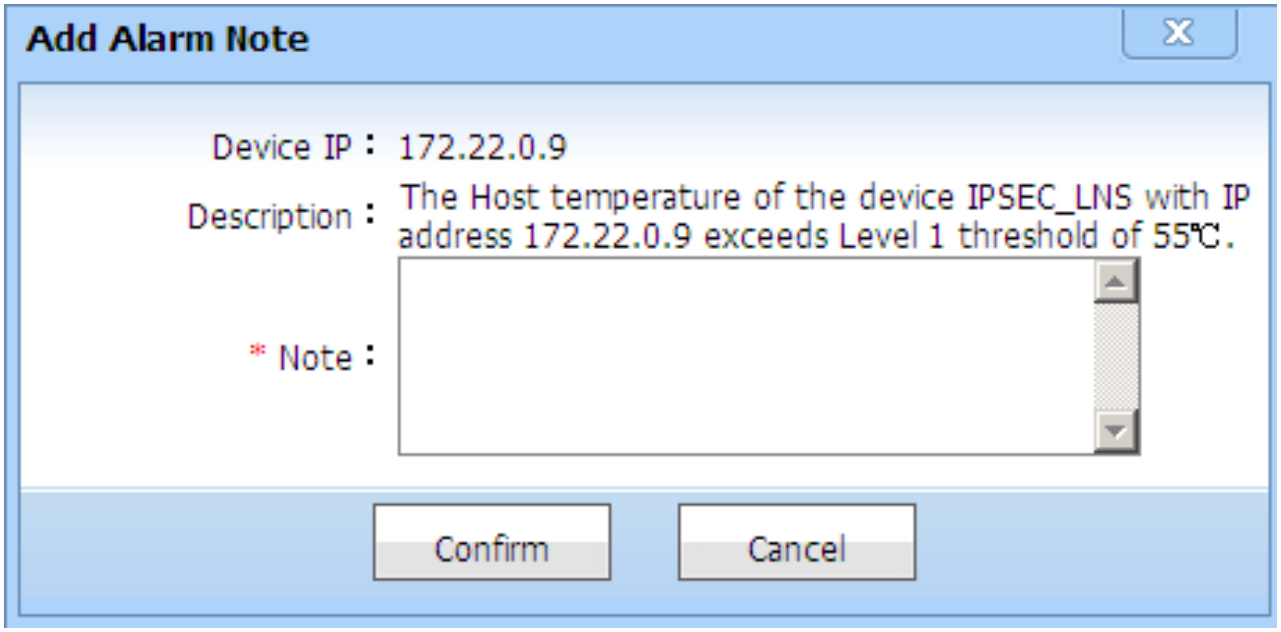


Figure 6.4. Add remarks to an alarm

Click the remark addition icon in the alarm list. .

Note Remarks cannot be modified or deleted after being added.

Related topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Delete alarm
- Alarm Details

6.1.6. Modify Monitor Threshold

This function enables you to modify the monitor threshold, including device performance indicator threshold and global performance indicator threshold.

Operation Steps

1) Click **Alarm** to go to the corresponding page. Click **Adjust Threshold** in **Realtime Alarm View**.

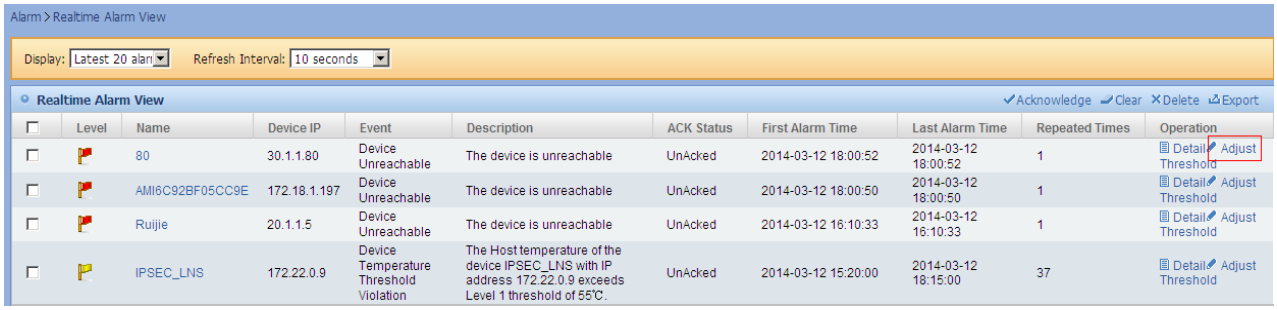


Figure 6.5. Modifying Monitor Threshold

Modify the device performance indicator threshold.

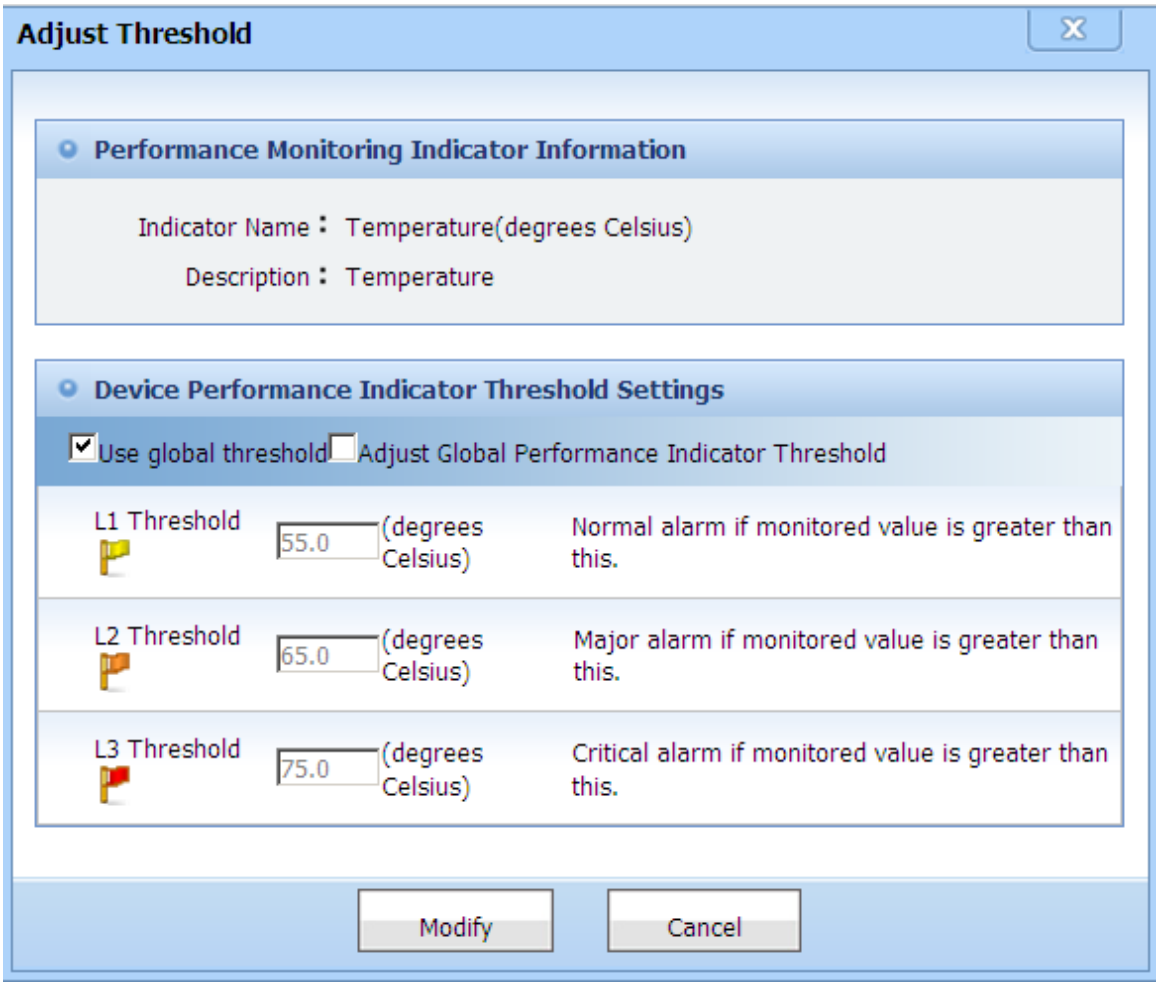


Figure 6.6. Modifying Device Performance Indicator Threshold

Modify and apply the global performance indicator threshold, or you can only apply the global performance indicator threshold.

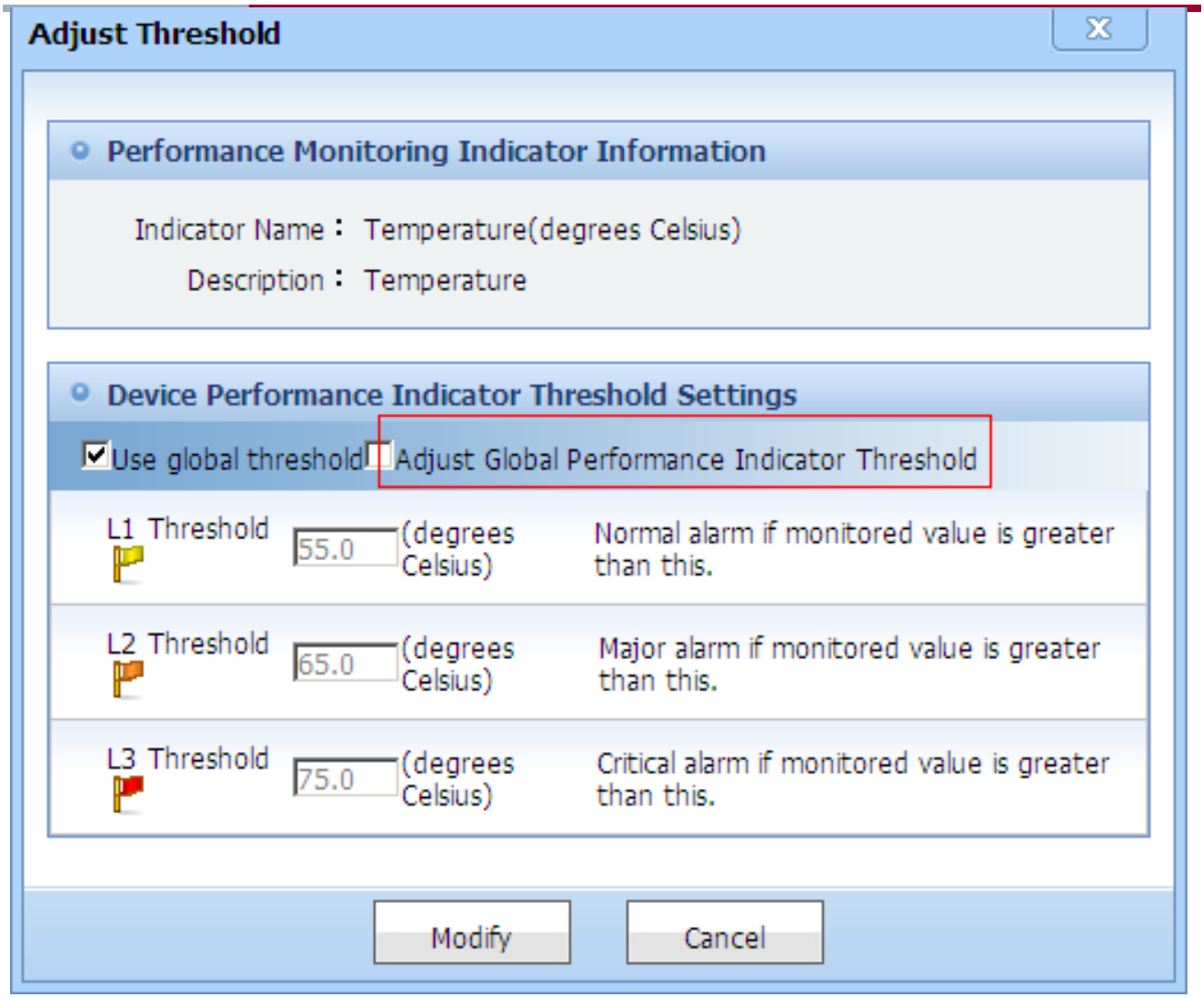


Figure 6.7. Modifying Global Performance Indicator Threshold

Click **Modify**, and the system returns to the **Realtime Alarm View** page.

Related Topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Delete alarm
- Add alarm remarks

6.1.7. Export Alarm

You can export an alarm from the alarm list.

Operation Steps

1) Select **Alarm** tab to open the realtime or history alarm management.
Click **Export** to export the alarm from the list.

Related Topics

- Realtime Alarm Monitoring
- Historical Alarm Management
- Acknowledge Alarm/Cancel Acknowledgement
- Clearing Alarm
- Alarm Details

- Adding alarm remarks

6.2. Historical Alarm Management

This function enables you to view alarm events in a list and search for the alarm based on the criteria.

Operation Steps

1) Click **Alarm** to go to the corresponding page. Click **Historical Alarm Mgmt** in the left column to go to the **Historical Alarm** page.

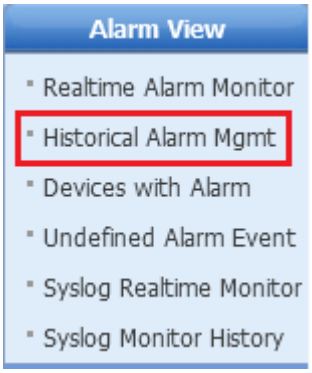


Figure 6.8. Historical Alarm Menu

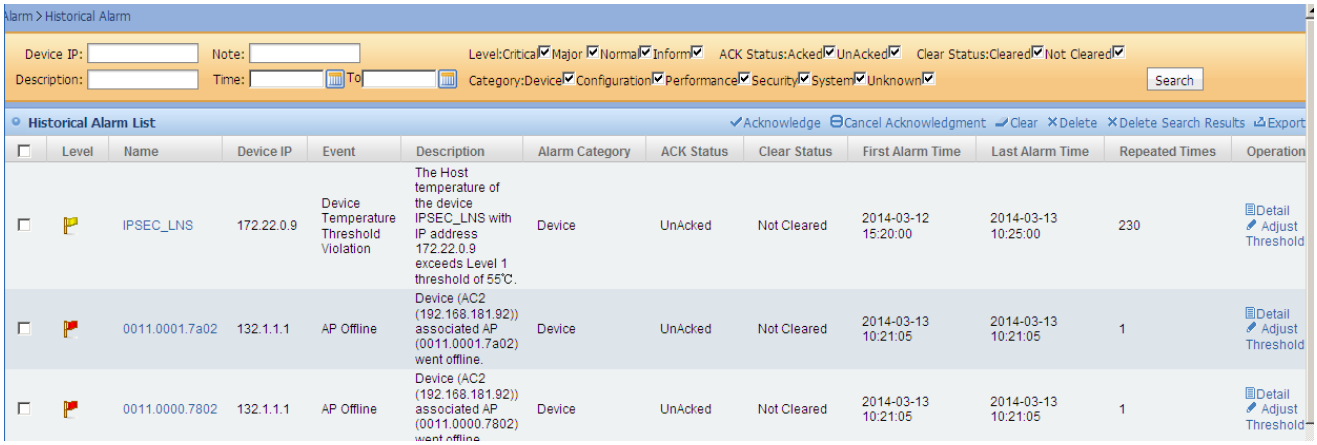


Figure 6.9. Historical Alarm List

Major operations in Historical Alarm List include: Tick the checkbox before the alarm event and click **Acknowledge**, **Clear** or **Delete** to change the alarm status or delete the alarm.
Click the alarm device to go to the **Device detail** page.
Click to display the Alarm Details page.
Click to go to the Add Alarm Note page.

Major Functions

- Acknowledge Alarm/Cancel Acknowledgement
- Clear Alarm
- Delete alarm
- Alarm Details
- Add alarm remarks

Note

Click Acknowledge, and ACK Status of the alarm turns to Acked. Click Cancel Acknowledgement, and ACK Status of the alarm turns to UnAcked. Click Clear, and Clear Status and ACK Status of the alarm turn to Acked and Cleared respectively.

Note

If an alarm message is generated repeatedly, the alarm time is subject to the last alarm time. Otherwise, the alarm time is subject to the first alarm time.

Note

The alarm note cannot be modified or deleted.

Note

An alarm device in grey indicates that the device has been deleted.

Note

The function of Adjust Threshold in Historical Alarm List is the same as that in Realtime Alarm View.

6.3. Devices with Alarm

In this page, the system will display all the devices that has unconfirmed alarms with a level no lower than “Normal” and this will help the administer to monitor the devices.

Operation Steps

1) Select **Alarm** tab and click the **Devices with Alarm** on the left to open the page.

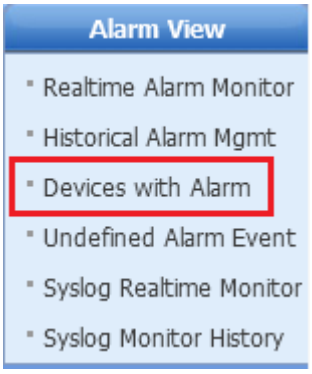


Figure 6.10. Devices with Alarm menu

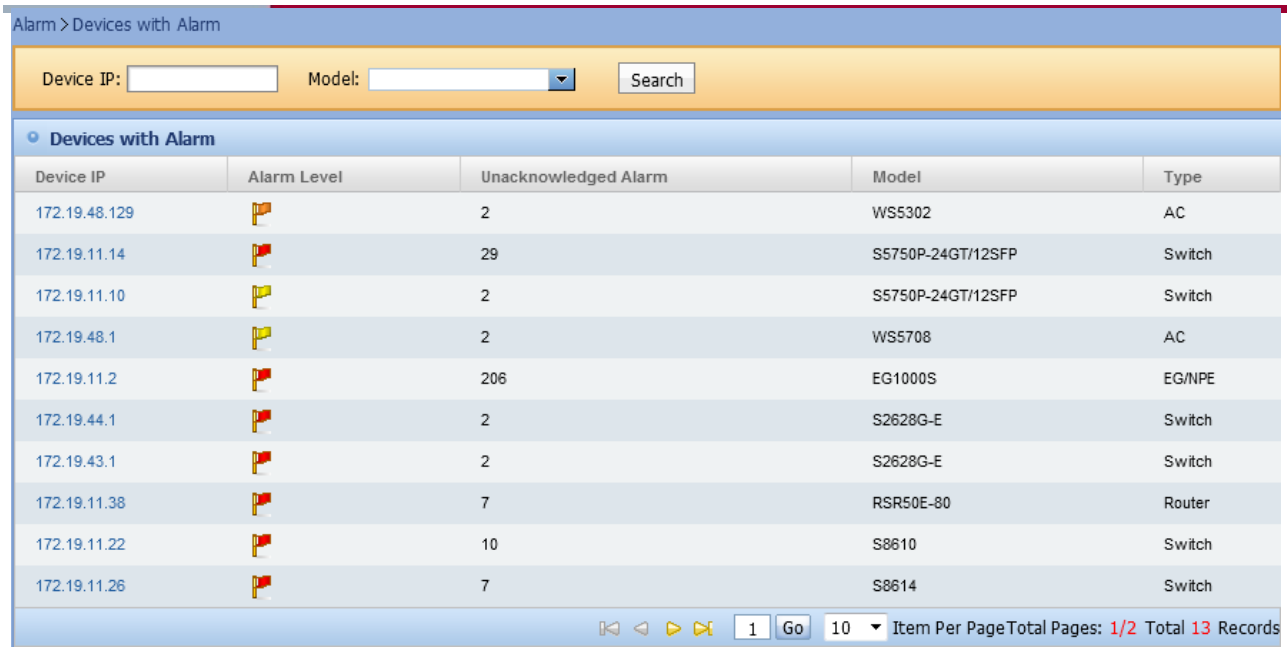


Figure 6.11. Device list with alarm

In the device list with alarm, you can do the following: Click **Device IP** link to open the device detail page.

Note

A device with alarm indicates that a device has an unconfirmed alarm with a level no lower than “Normal” level.

Note

In the device list with alarm, the “Unacknowledged Alarm” is the number of all the alarms with a level no lower than “Normal” level on the device.

6.4. Alarm Parameters

You can set alarm parameters.

Operation Steps

1) Select the **Alarm** tab and click **Alarm Parameter** on the left, and you can view the **Alarm Parameter** page.

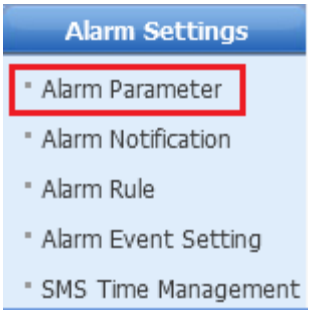


Figure 6.12. Alarm parameter menu

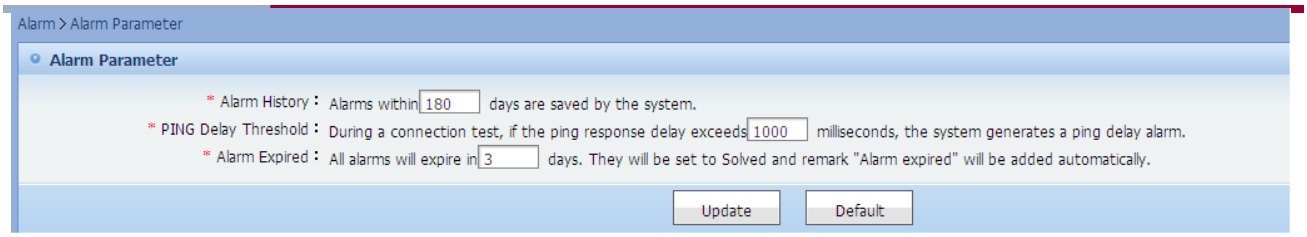


Figure 6.13. Alarm parameter setting page

6.5. Alarm Notification

This function allows you to select a role, device that generates alarms, alarm severity, and alarm events. In addition, you can select an alarm notification mode from the following: by voice, by mail, and by short message service (SMS).

Operation Steps

1) Select the **Alarm** tab and open the alarm notification page.

Figure 6.14. Alarm notification menu

Figure 6.15. Alarm notification list

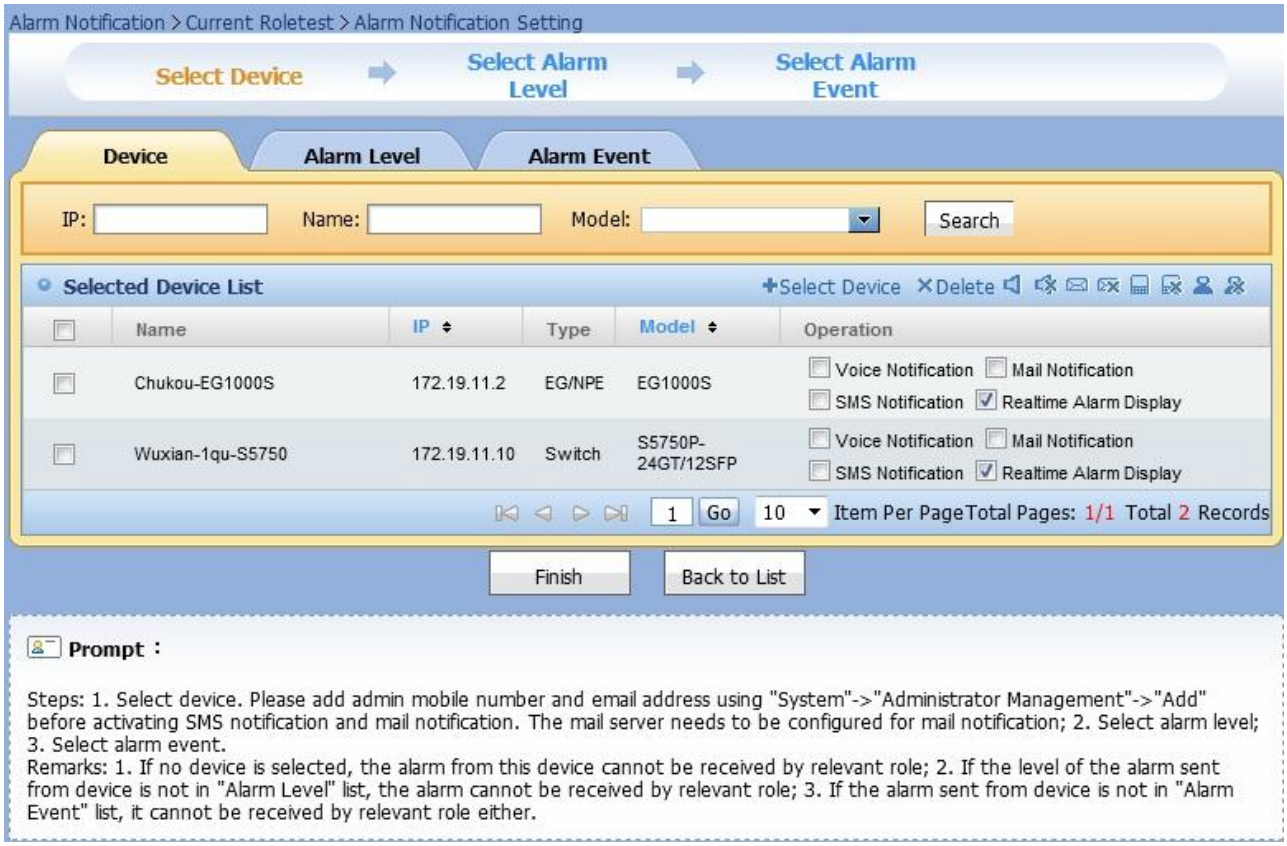


Figure 6.16. Alarm notification setting

Alarm notification involves the following operations: If you select a device, only the alarms generated by the selected device can be received.
If you select an alarm severity, only the alarms of the selected severity can be received.
If you select an event, only the alarms for the selected event can be received.

Note

If Status is displayed as Configuration Completed after you select a role, the setting of alarm notification is completed. If Status is displayed as Configuration Uncompleted, click Alarm Notification Setting and set alarm notification.

Note

If a device is not selected, the role cannot receive any alarm generated by the device. If the severity of an alarm generated by a device is excluded from the selected alarm severities, the role cannot receive the alarm. If an alarm generated by a device is irrelevant to the selected event, the role cannot receive the alarm.

Note

Select a device first. To enable alarm notification by SMS or Email, choose System -> Administrator Management > Add to add the mobile phone number or Email address of the administrator. If alarm notification by Email is required, you must set the mail server.

Note

After alarm notification by voice is enabled, only the Realtime Alarm Monitoring page adopts alarm notification by voice. If multiple alarms are generated concurrently, the system voices only once; in addition, the system voices for only the alarm of the highest severity.

Note

If alarm notification by Email is not enabled, the selected role is not notified of any alarm by Email.

Note

If alarm notification by SMS is not enabled, the selected role is not notified of any alarm by SMS.

6.6. Alarm Rule

You can define alarm generation rules based on event sources and event types. The system automatically converts the events that meet conditions into alarms. The list of alarm generation rules displays alarm generation rules predefined by the system and configured by the user, including rule names and descriptions.

Operation Steps

1) Select the **Alarm** tab and click **Alarm Generation Rule** on the left, and then you can open the page for alarm rule generation.

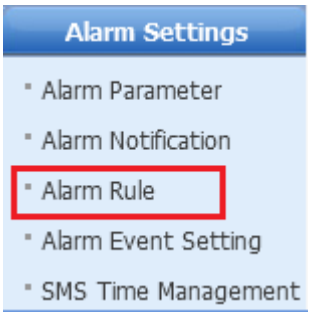


Figure 6.17. Menu of alarm generation rules

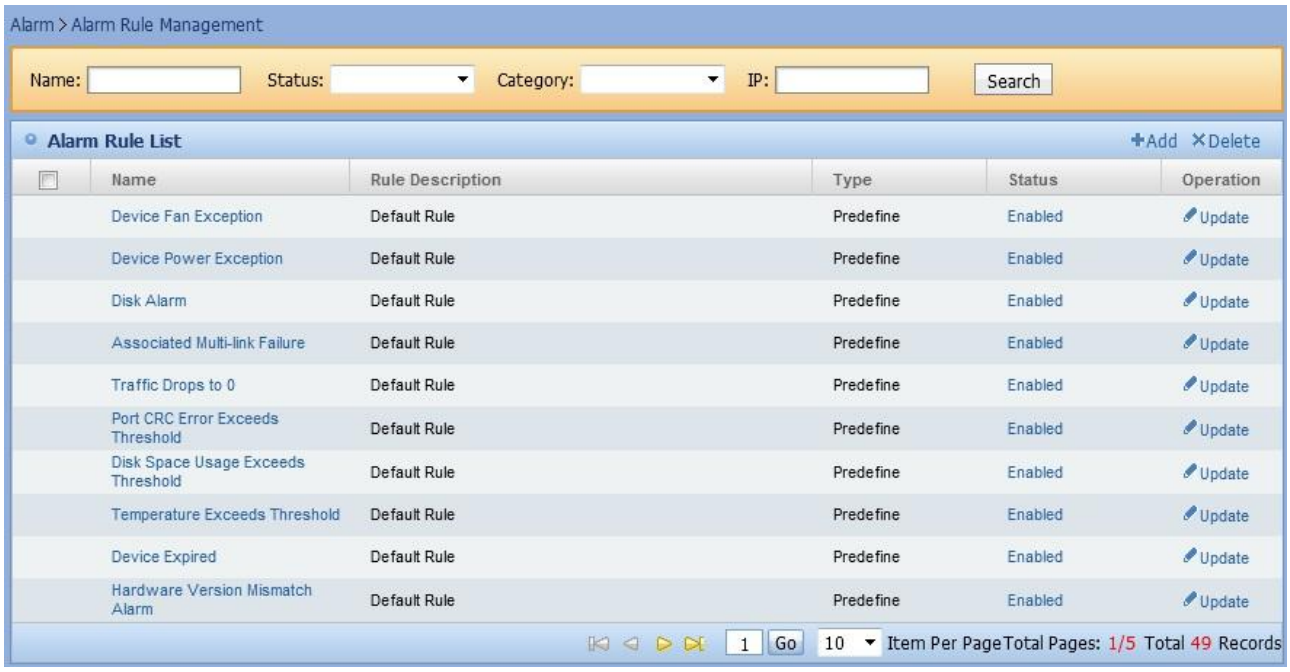


Figure 6.18. List of alarm generation rules

The list of alarm generation rules involves the following operations: Click the Rule Name link, and you can open the page of detailed information about alarm generation rules.
Click **Add** and you can open the page for adding alarm generation rules.

Select the alarm generation rule to be deleted and click Delete, and you can delete the selected alarm generation rule.
If the status of a rule in the list is Enabled, you can click the status link to change the status to Disabled; if the status of a rule in the list is Disabled, you can click the status link to change the status to Enabled.
Click the Update link in the list, and you can open the page for modifying alarm generation rules.

Function List

- Adding or modifying alarm generation rules.

Note Only a predefined alarm generation rule can be modified.

Note When a defined alarm generation rule is met, an alarm is generated regardless of whether the condition for generation of this alarm conflicts with other rules.

6.6.1. Adding or Modifying Alarm Generation Rules

You can add new alarm generation rules or modify existing alarm generation rules to determine whether an alarm is generated for a certain event or device.

Operation Steps

1) Select **Alarm** tab and click the **Alarm Rule** on the left to open the page for alarm rule generation.

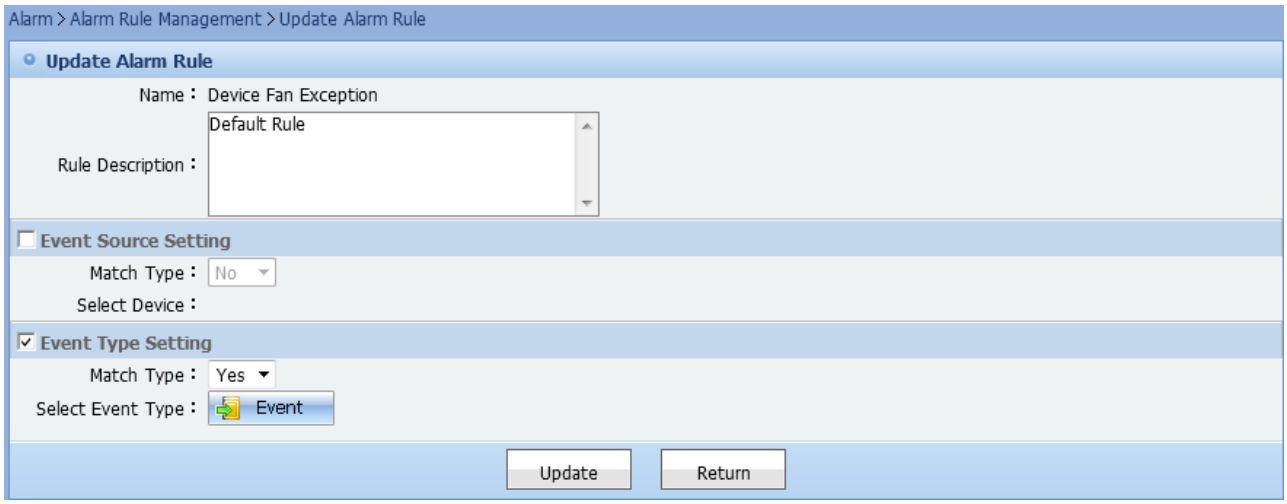


Figure 6.19. Add or modify alarm generation rule

Set the event source: Select “Yes” from matching type and click “**Select device**” button to select devices that match the rule.
Select “No” from matching type and click “Select device” button to select devices that do not match the rule.
Set event type: Select “Yes” from matching type and click “Select event type” button to select events that match the rule.
Select “No” from matching type and click “Select event type” button to select events that do not match the rule.

Note In the event source setting, if “Yes” type is selected but no device is selected, then this rule will be invalid to any device, that is, no device matches the rule.

Note In the event source setting, if “No” type is selected but no device is selected, then this rule will be valid to all the devices.

Note

In the event type setting, if “Yes” type is selected but no device is selected, then this rule will be invalid to any event, that is, no event matches the rule.

Note

In the event type setting, if “No” type is selected but no device is selected, then this rule will be valid to all the events.

Note

When a defined alarm generation rule is met, an alarm is generated regardless of whether the condition for generation of the alarm conflicts with other rules.

Related Topics

- Alarm rule

6.7. Alarm Event Management

The system will generate an event based on the event defined by the user. If there is no event defined for the received event, the event will be marked as unknown.

Operation Steps

1) Select **Alarm** tab and click **Alarm Event Setting** on the left to open the page.

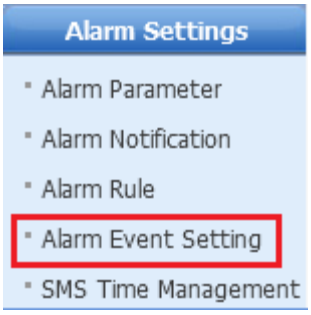


Figure 6.20. Alarm Event Setting menu

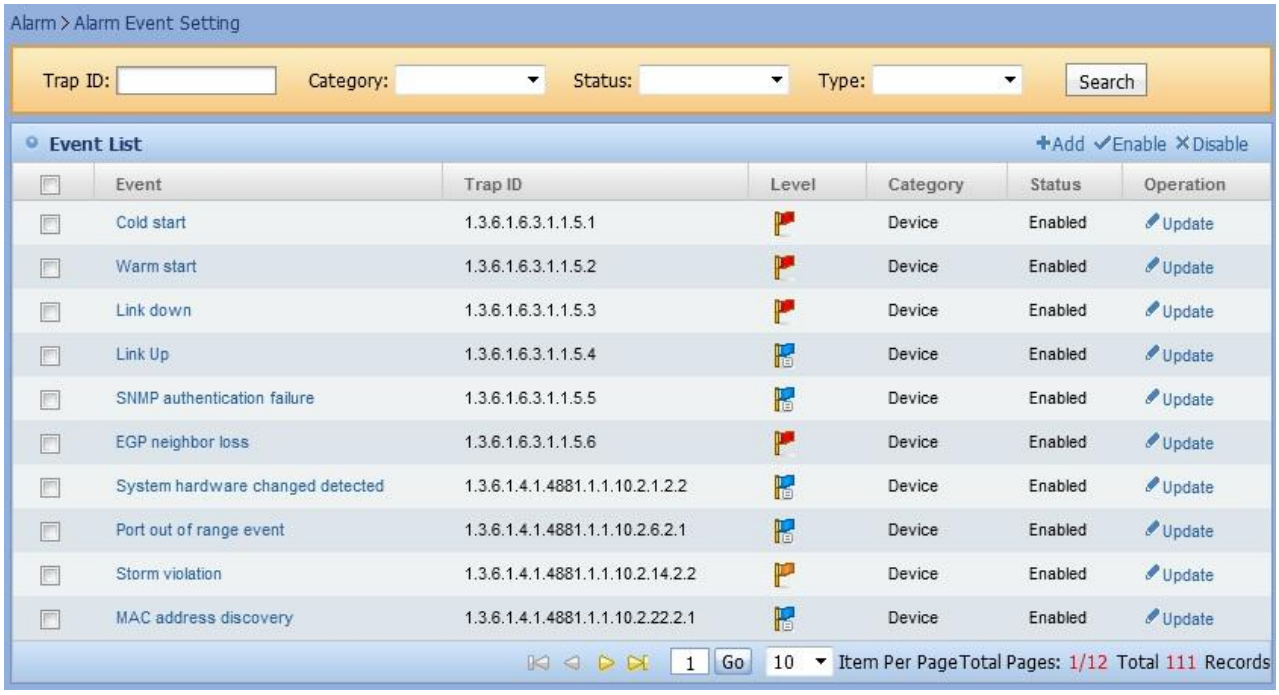


Figure 6.21. Alarm event list

In the alarm event list, you can do the following: Check the “Enable/Disable” checkbox to enable or disable the event.
Click the “Event” link to open the page for event detail information.
Click the “Update” link to open the page to modify the event.
Press Add to open the page to add event.

Function list

- Add or modify alarm event
- Enable Alarm Event
- Disable Alarm Event

Note	The system can only change the pre-defined event.
Note	If there exists alarm for the customized event, the event cannot be delete unless all the related alarms are deleted.
Note	If the event is disabled, no alarm will be emit even there exists a matching rule to generate alarm.

6.7.1. Add or Modify Alarm Event

You can define an alarm event to convert an unknown event into a known and identifiable event.

Operation Steps

1) Select **Alarm** tab and click **Alarm event setting** on the left to open the alarm rule page.

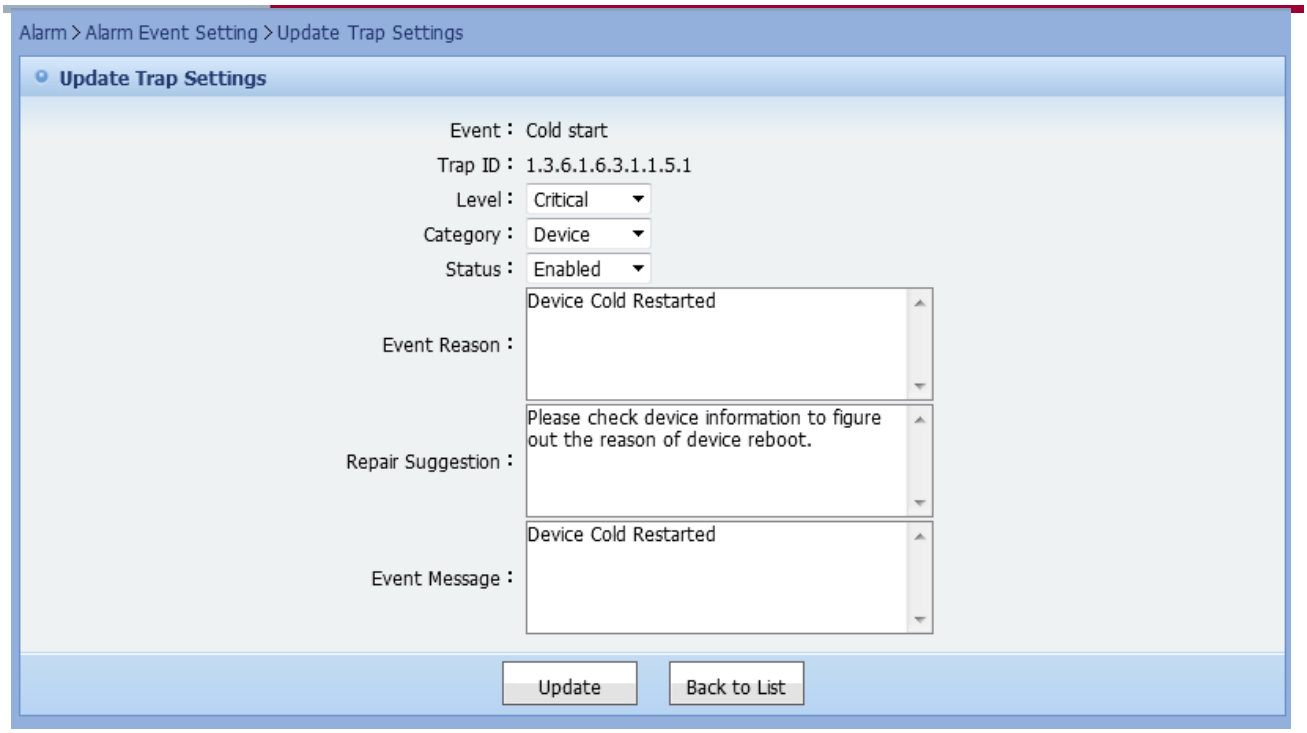


Figure 6.22. Add or modify alarm event

Click **Add**.
Input the following field for the event name, Trap ID, level, category, status, event reason, repair suggestion, event message(which will be displayed in the description).
Click **Add** or **Update**.

Note For those pre-defined events which contain “{ 0} ” or “{ 1} ” in the message body cannot be deleted.

Related Topics

- Alarm Event Management
- Enable Alarm Event
- Disable Alarm Event

6.7.2. Enable Alarm Event

You can enable those alarm events that have been disabled.

Operation Steps

1) Select **Alarm** tab to open the alarm event management page.

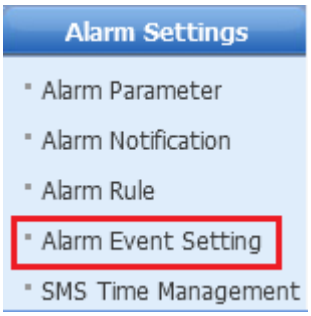


Figure 6.23. Alarm event management

Check the checkbox in front of the alarm event entry.
Click **Enable** to enable that alarm event

Related Topics

- Alarm Event Management
- Add or modify alarm event
- Disable Alarm Event

6.7.3. Disable Alarm Event

You can disable those alarm events that has been enabled.

Operation Steps

1) Select **Alarm** tab to open the alarm event management page.

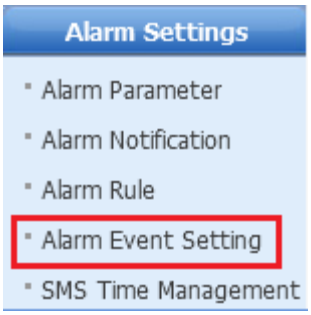


Figure 6.24. Alarm event management

Check the checkbox in front of the alarm event entry.
Click **Disable** to disable that alarm event.

Note

Once the alarm event is disabled, no alarm will be generated for it even there exists a matching alarm rule in the system.

Related Topics

- Alarm Event Management
- Add or modify alarm event
- Enable Alarm Event

6.8. Undefined Alarm Event

This function enables you to view alarm events in a list and search for the alarm based on the criteria.

Operation Steps

1) Click **Alarm** to go to the corresponding page. Click **Undefined Alarm Event** in the left column to go to the **Undefined Alarm Event** page.

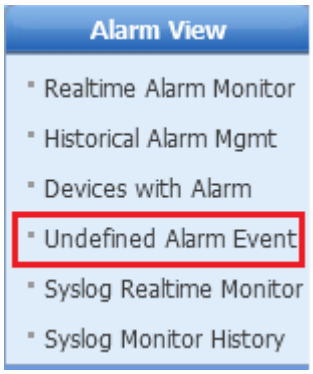


Figure 6.25. Undefined Alarm Event Menu

Name	Device IP	Alarm Level	Unacknowledged Alarm	Model	Type
IPSEC_LNS	172.22.0.9		1	EG1000M	EG/NPE
0011.0000.f701	90.0.1.3		337		AP
0011.0000.3202	132.1.1.1		367		AP
AMI6C92BF05B482	172.18.136.86		1	Red Hat Linux2	Host
RuckusAP	172.18.12.233		1	UNKNOWN	Unknown
AC2	192.168.181.92		1	M8600-WS(V1.0)	AC

Figure 6.26. Event List

Major operations in Undefined Alarm Event List include: Click **Enable Unspecified Alarm Generation** or **Disable Unspecified Alarm Generation**.
Tick the checkbox before the alarm event and click **Delete** to delete the event.
Click the alarm device to go to the **Device detail** page.

Note OID is displayed as the description of an unknown event for the purpose of location.

Note The parameters of an unknown event are displayed in OID or value format.

6.9. Alarm Forwarding

Alarm forwarding allows forwarding of traps and events.

Operation Steps

1) Select **Alarm** tab and click **Event Server** on the left of the page.

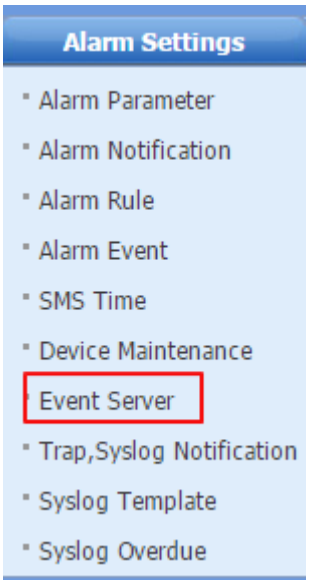
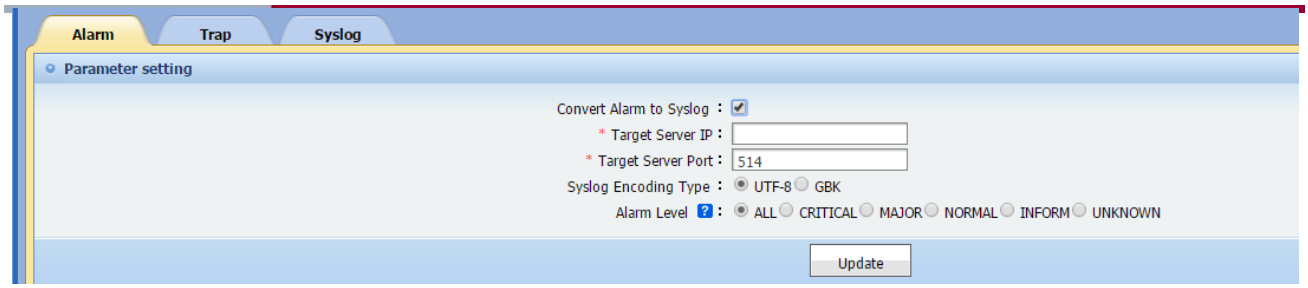
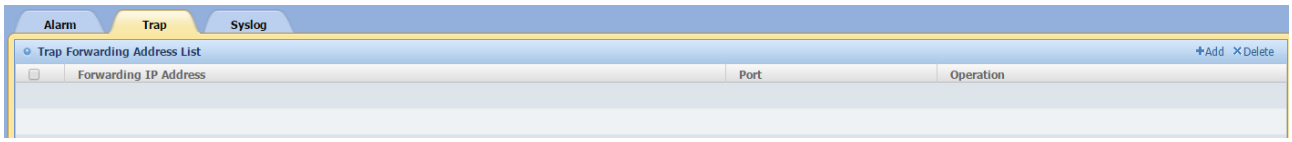


Figure 6.27. Event Server

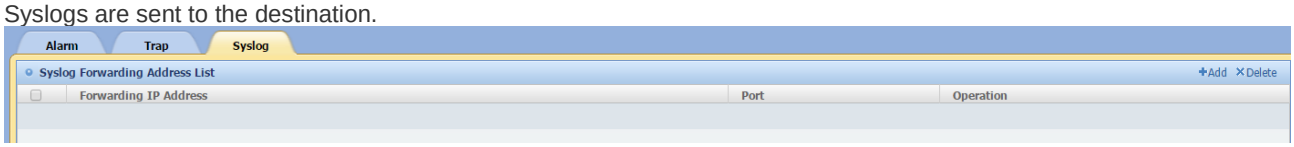
Alarms are sent to the destination after being converted to Syslogs.



Trap packets are sent to the destination in the format of Trap packets.



Syslogs are sent to the destination.



Note

You can set no more than 5 event server transmit addresses.

Note

The system will not check if the destination is reachable or the server at the IP address can deal with event message.

Note

You can set no more than 5 server URL and the system will use POST method to send the event to the target URL.

Note

The system will not check if the destination URL is reachable or the server at the URL can deal with the POST request. The sending rate may be different from the processing rate, therefore, the server at the destination URL must be able to handle the forwarded traps and events.

6.10. Set the Device Event Notification

Setting for device event notification

Operation Steps

1) Select **Alarm** tab and click the **Trap, Syslog Notification** on the left of the page.

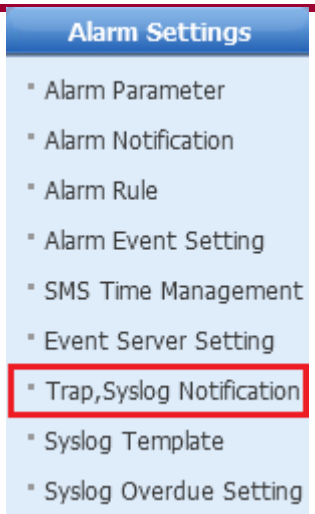


Figure 6.30. Trap, Syslog Notification

Open the page for trap and syslog notification.

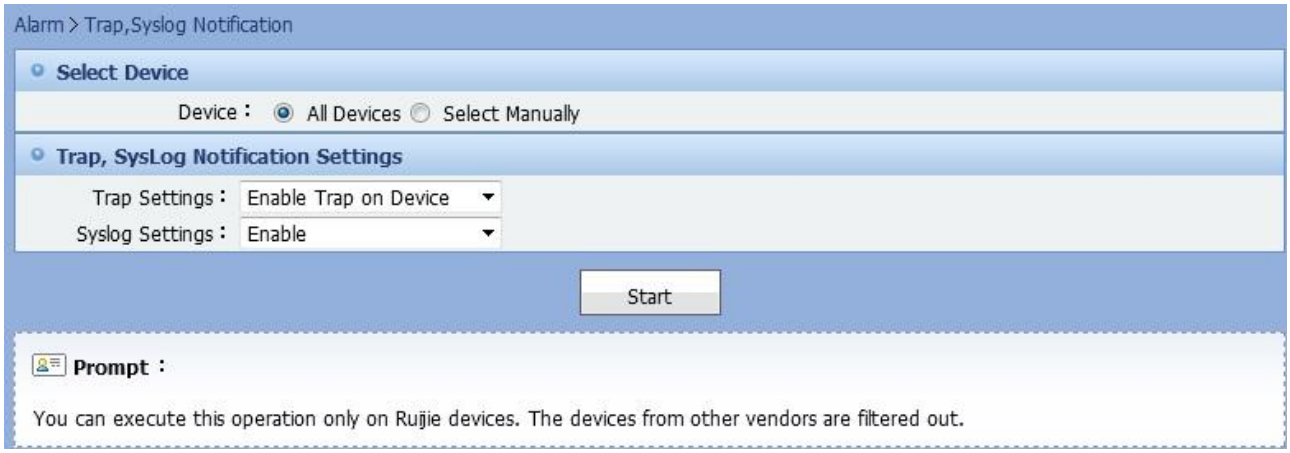


Figure 6.31. Set the device event notification

Note Only devices made by Ruijie support this setting, devices from other vendors are filtered out.

6.11. Set SMS Time Range

You can define the SMS sending time range and the system will deliver the SMS only in the specified time range. The SMS time range includes a start time, end time and the valid range in a week.

Operation Steps

1) Select **Alarm** tab and click **SMS Time Management** on the left of the page.

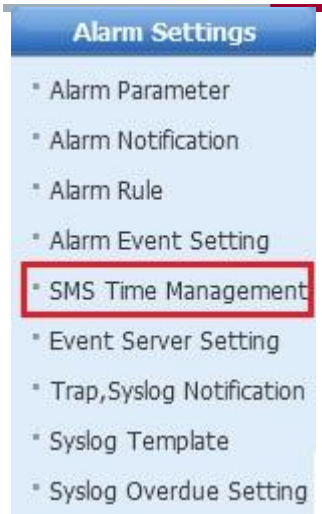


Figure 6.32. SMS time range

Figure 6.33. SMS time range list

You can click **Add** to add an SMS time range with a start time, end time and the valid range in a week.

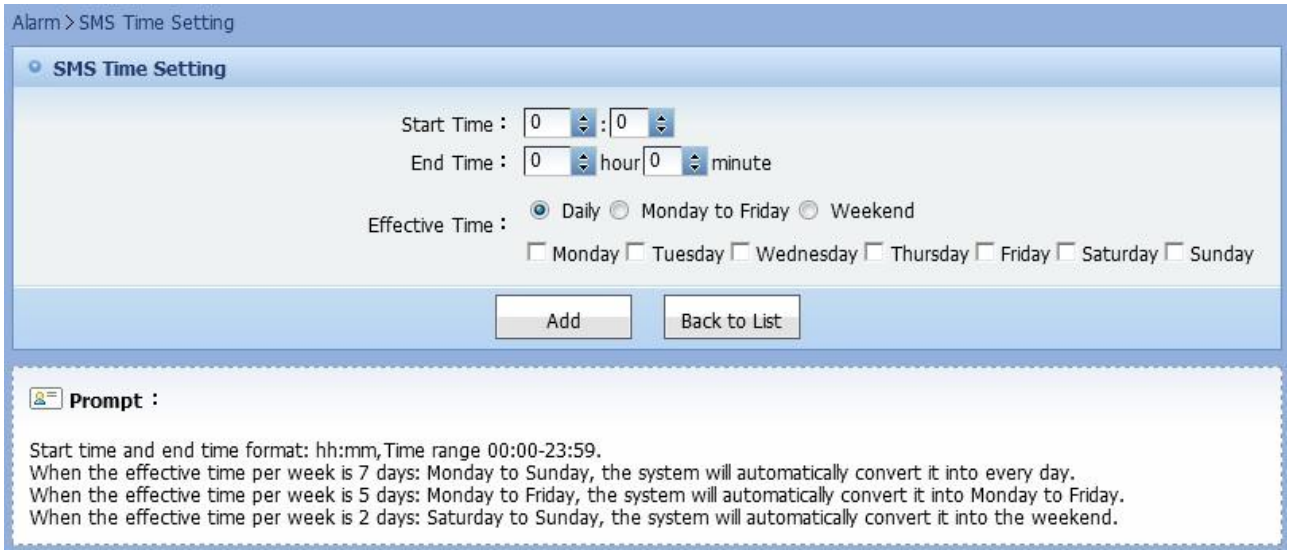


Figure 6.34. Add SMS time range

You can modify the existing SMS time range.

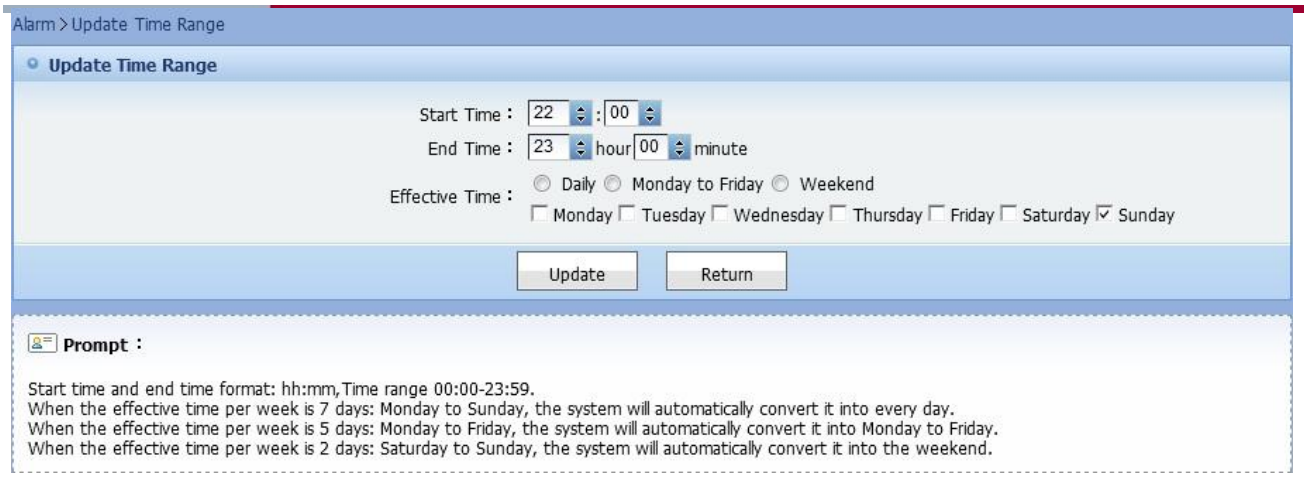


Figure 6.35. Modify the existing SMS time range

You can remove the existing SMS time range.

Figure 6.36. Remove the existing SMS time range

Note The system will deliver the SMS at any time if no SMS time range is specified.

6.12. Device Maintenance

This function enables you to set device maintenance schedule. In the schedule period, any alarms will not generate.

Operation Steps

1) Go to **Alarm** > **Device Maintenance**

Figure 7.37. Device Maintenance

2) Click Add to enter the **Add Device Maintenance Schedule** page.

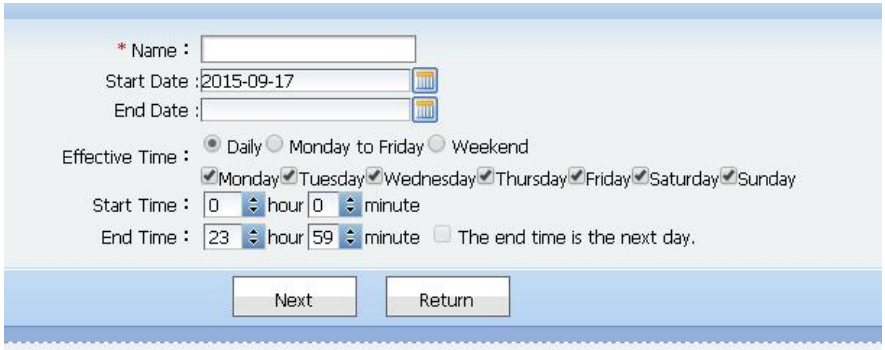


Figure 7.38. Adding Device Maintenance Schedule

3) Select a schedule, click **Update** to edit the device maintenance schedule.

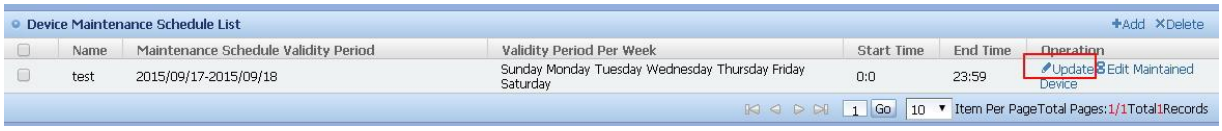


Figure 7.39. Editing Device Maintenance Schedule.

4. Select a schedule, click **Delete** to delete the device maintenance schedule.

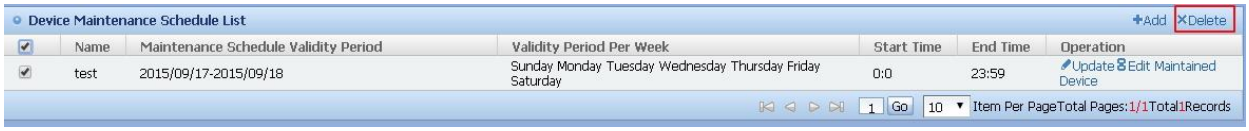


Figure 7.40. Deleting Device Maintenance Schedule

6.13. Syslog Template

With this function, you can leverage a log message which matches the “Syslog Template” to an alarm.

Operation Steps

1) Click **Syslog Template**.

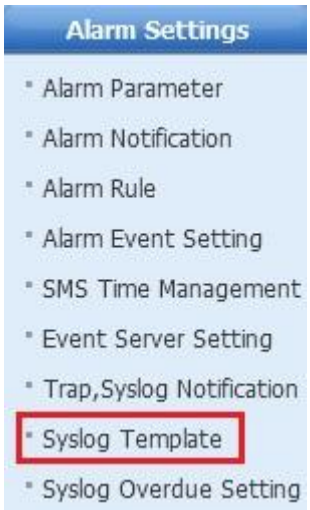


Figure 6.37. Syslog Template

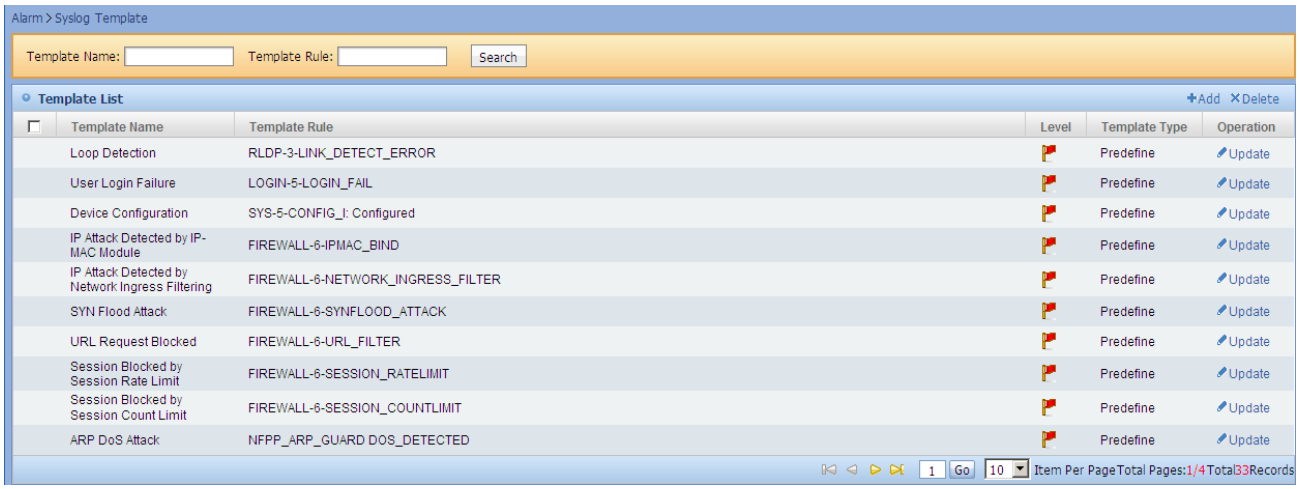


Figure 6.38. Syslog template list

Click **Add** to add new Syslog template.

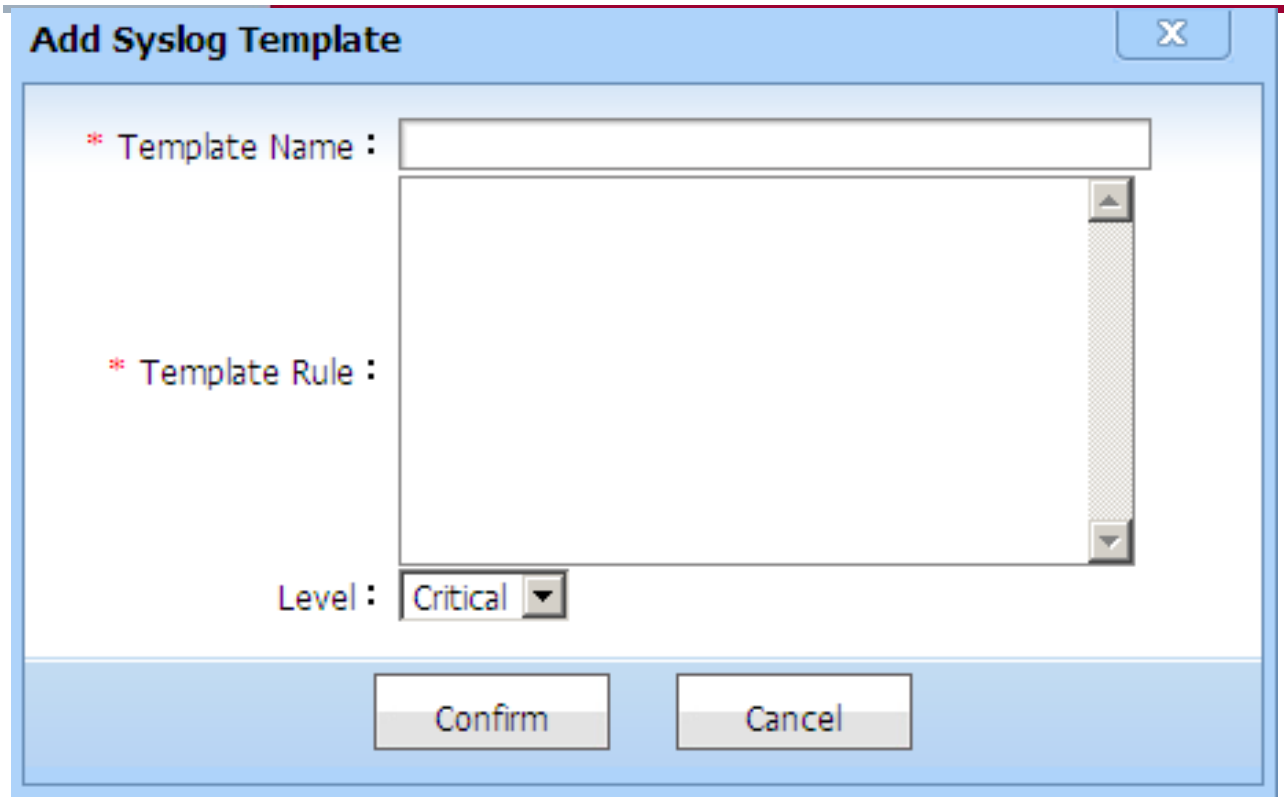


Figure 6.39. Add Syslog template

You can modify the existing Syslog template

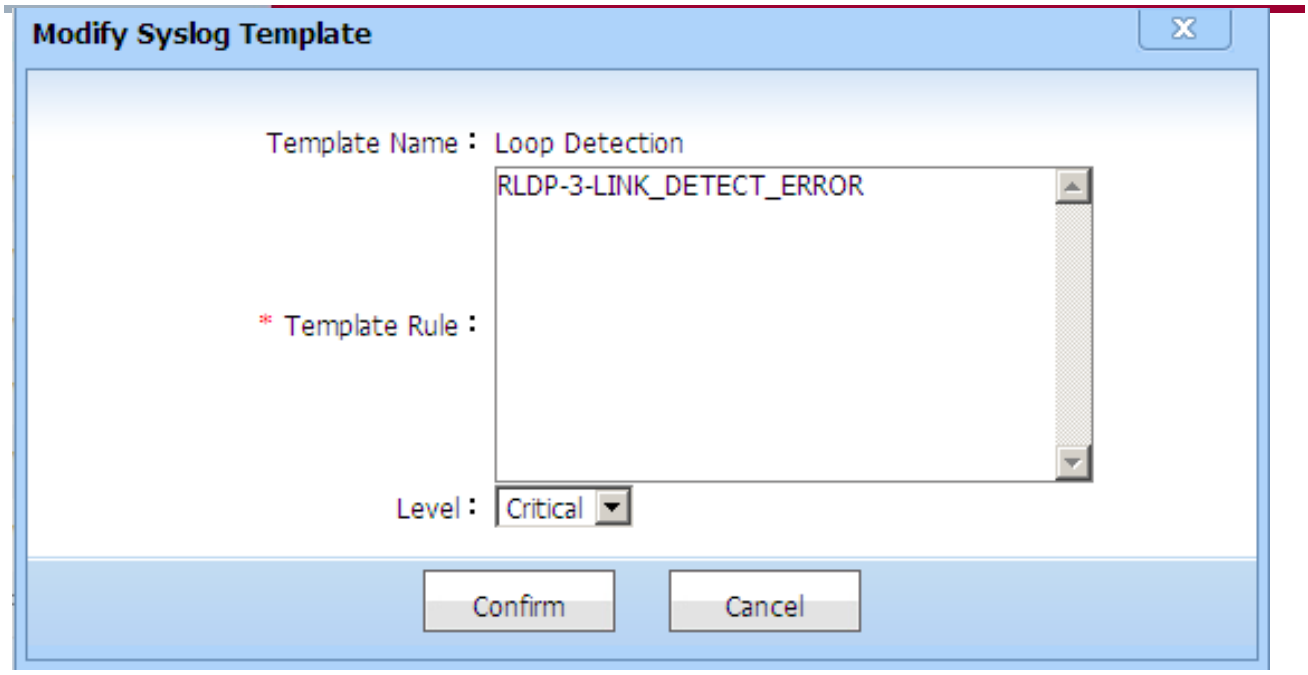


Figure 6.40. Modify existing Syslog template

You can delete customized Syslog template.

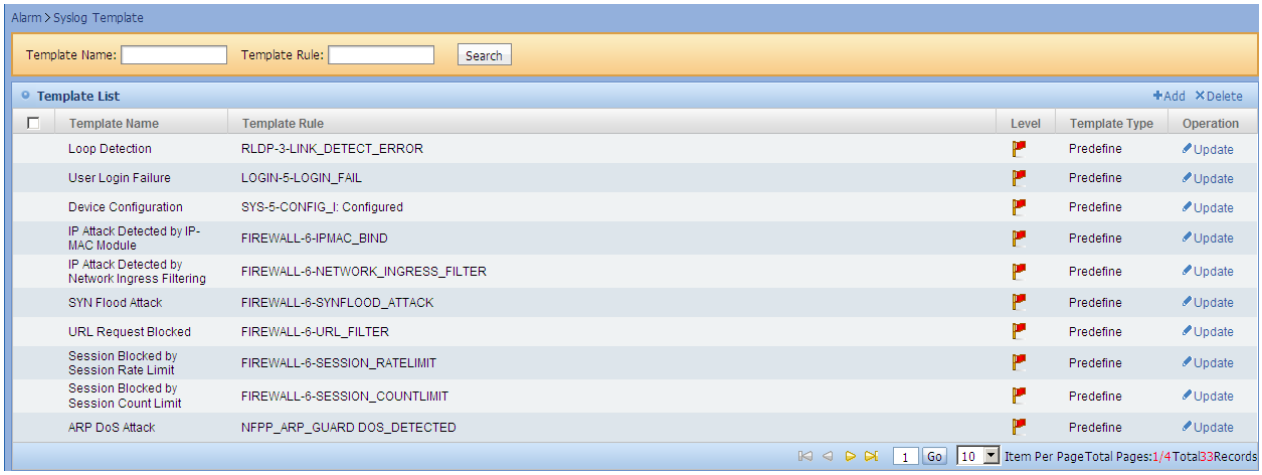


Figure 6.41. Delete customized Syslog template

Note

The system use the fuzzy way to match the content in the template, for example, a Syslog template is like "*Jan 2 10:54:10: %LOGIN-5-LOGIN_FAIL: User login from vty1 (192.168.197.18) failed.", the log content with "LOGIN-5-LOGIN_FAIL" will match this template. If there exists more than one templates for the Syslog, the system will choose the first one that matches and stop the finding, therefore, you should use rules that has no overlap as possible.

6.14. Syslog Realtime Monitor

You can view the realtime monitor for Syslog.

Operation Steps

1) Select **Syslog Realtime Monitor** tab to open the Syslog realtime monitor.

Figure 6.42. Syslog realtime monitor menu

Priority	Device Name	Module	Type	IP	Time	Log Detail
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 14:04:34	*Oct 31 13:52:16: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 14:04:26	*Oct 31 13:52:08: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 14:02:44	*Oct 31 13:50:26: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 13:59:50	*Oct 31 13:47:32: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 13:57:04	*Oct 31 13:44:46: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 13:56:53	*Oct 31 13:44:35: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))
5	Wuxian-1qu-S5750	SYS	CONFIG_I	172.19.11.10	2011-10-31 13:56:44	*Oct 31 13:44:26: %SYS-5-CONFIG_I: Configured from console by vty0 (172.19.21.101))

Figure 6.43. Syslog realtime monitor list

6.15. Syslog Monitor History

In the page, the system will display only the history of Syslog.

Operation Steps

1) Select **Syslog Monitor History** tab.

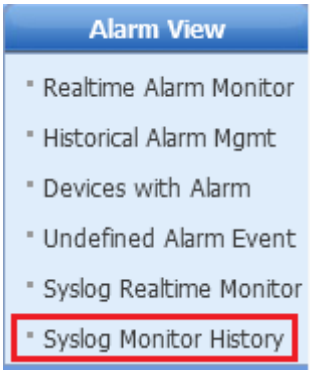


Figure 6.44. Syslog monitor history menu

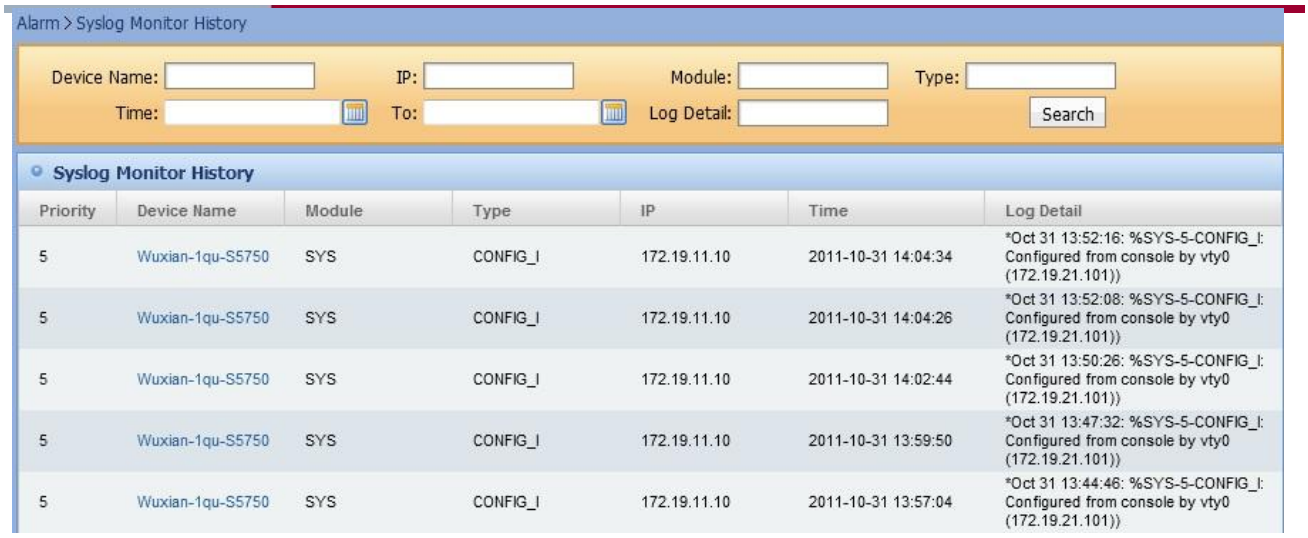


Figure 6.45. Syslog history list

6.16. Syslog Overdue

Syslog Overdue

Operation Steps

1) Select **Alarm** tab and click **Syslog Overdue Setting** on the left.

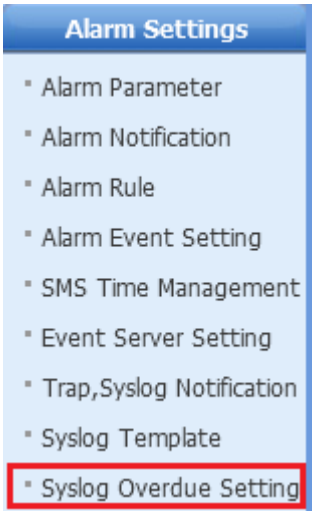


Figure 6.46. Syslog Overdue Setting menu

Syslog Overdue Setting page

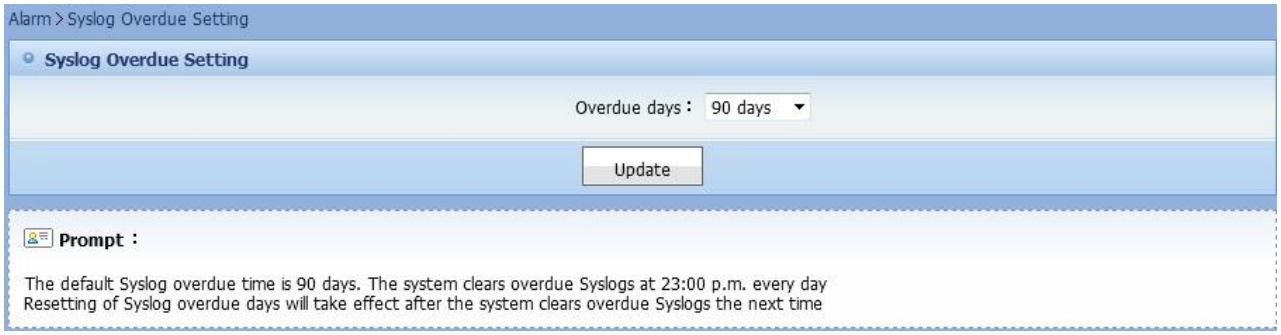


Figure 6.47. Syslog Overdue Setting page

Note

The default overdue period for Syslog is 90 days and the system will delete the expired Syslog at 23:00 every night.

Note

The newly overdue setting will take effect from the next time when the system start clearing the expired Syslog.

Configuration Guide
RG-SNC_2.30_EN_Build20151008

Copyright Statement

Exemption Statement

This document is provided "as is". The contents of this document are subject to change without any notice. Please obtain the latest information through the Ruijie Networks website. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Obtaining Technical Assistance

- Ruijie Networks website: http://www.ruijienetworks.com/
- Ruijie service portal: http://case.ruijienetworks.com

Chapter 7 WLAN

The WLAN page enables you to search, query, configure and manage WLAN devices, hotspots, STAs and alarms, including the Dashboard, Hotspot, AP, AC, STA, Alarm, Rogue AP, Troubleshooting Assistant modules.

Major Functions

- Dashboard
- Hotspot
- AP
- AC
- STA
- Alarm
- Rogue AP
- Troubleshooting Assistant
- Spectrum Analysis
- Wireless Logical Topology
- Fat AP Spectrum Analysis and Monitoring
- Permissions
- i-Share+ Mini AP
- eLTE
- Satellite AP

7.1. Dashboard

The **Dashboard** page displays overall system data statistics, including the following aspects: 1. AC Asset Information 2. AP Asset Information 3. Global Out-of-Service Rate Statistics 4. Top N Global Idle Traffic 5. Global STA Statistics 6. Top N Global Rate Statistics 7. Global Out-of-Service Rate Statistics 8. Global Idle Traffic Statistics 9. Global Rate Statistics 10. Rogue AP Statistics 11. Mini AP Asset Statistics 12. Top N Clients Statistics 13. WLAN Homepage Custom Settings.

Major Functions

- AC Asset Information
- AP Asset Information
- Top N Global Out-of-Service Rate Statistics
- Top N Global Idle Traffic
- Global STA Statistics
- Top N Global Rate Statistics
- Global Out-of-Service Rate Statistics
- Global Idle Traffic Statistics
- Global Rate Statistics
- Rogue AP Statistics
- Mini AP Asset Statistics
- Top N Clients Statistics
- WLAN Homepage Custom Settings

7.1.1. AC Asset Information

This function enables you to view the **AC Connection Status Statistics** and the **AC Alarm Status Statistics**.

Operation Steps

Click **Dashboard** to view **AC Asset Information**, as shown in the following figure:

Figure 7.1. AC Asset Information

7.1.2. AP Asset Information

This function enables you to view the **AP Connection Status Statistics** and the **AP Alarm Status Statistics**.

Operation Steps

Click **Dashboard** to view the **AP Asset Info**, as shown in the following figure:

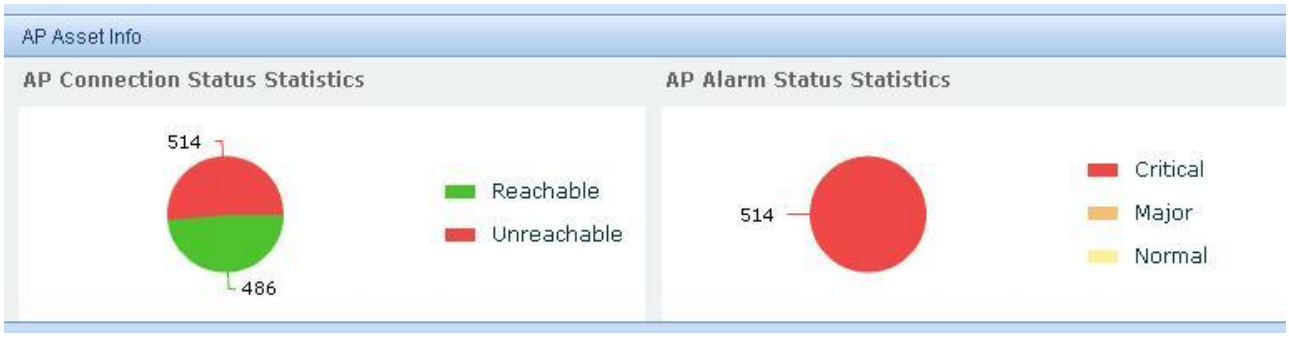


Figure 7.2. AP Asset Information

7.1.3. Top N Global Out-of-Service Rate Statistics

This function enables you to view the **Top N Hotspots** and **Top N APs** in global out-of-service rate in the statistics time.

Operation Steps

2) Click **Dashboard** to view the **Global Out-of-Service Rate Statistics**, as shown in the following figure:

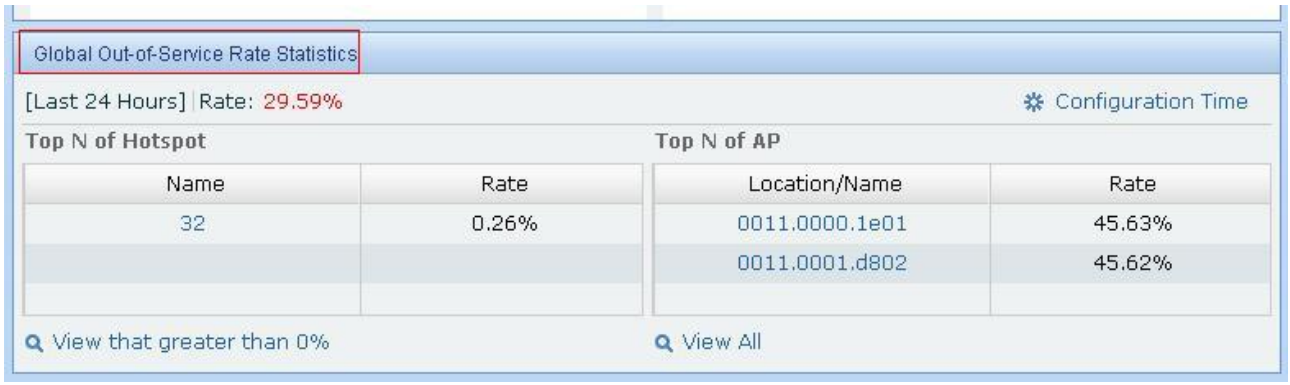


Figure 7.3. Global Out-of-Service Rate Statistics

Specify the time range of the **Global Out-of-Service Rate Statistics**.

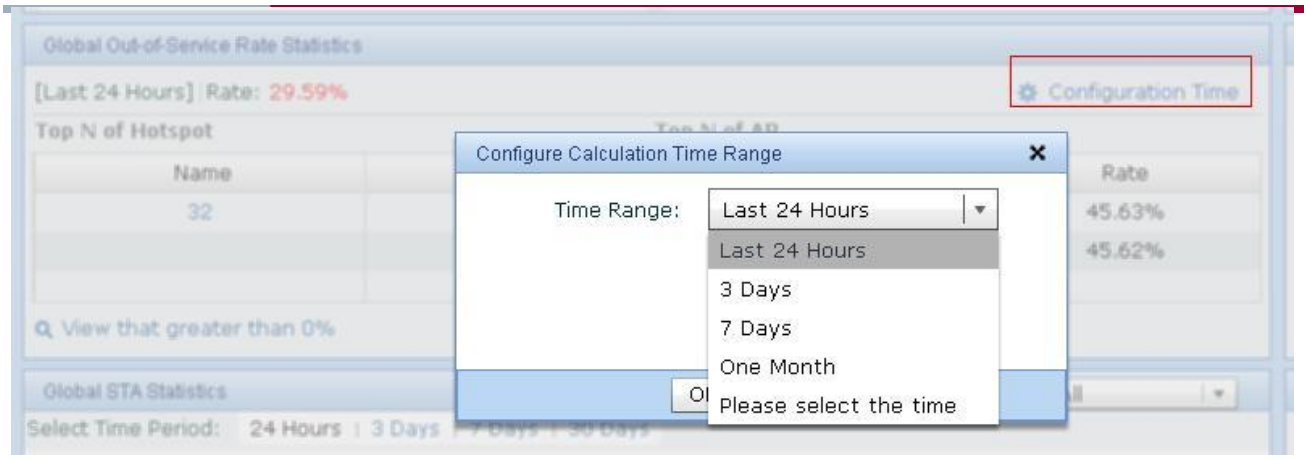


Figure 7.4. Configuring Time

Click **Save**, and the system returns to the **Dashboard** page.

7.1.4. Top N Global Idle Traffic

This function enables you to view the top N idle APs in the statistic time.

Operation Steps

3) Click **Dashboard** to view the Top N Global Idle Traffic, as shown in the following figure:

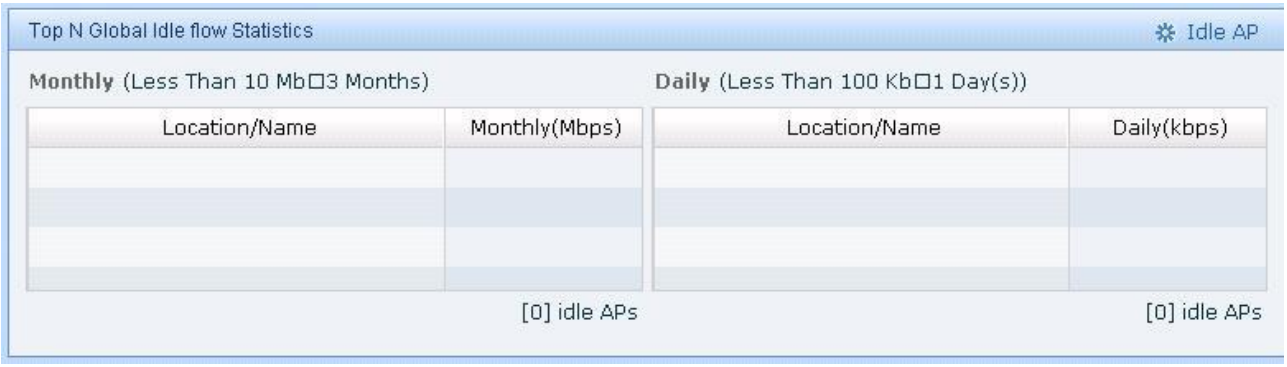


Figure 7.5. Top N Global Idle Traffic

Configure the definition of Idle AP in average traffic and statistics time.

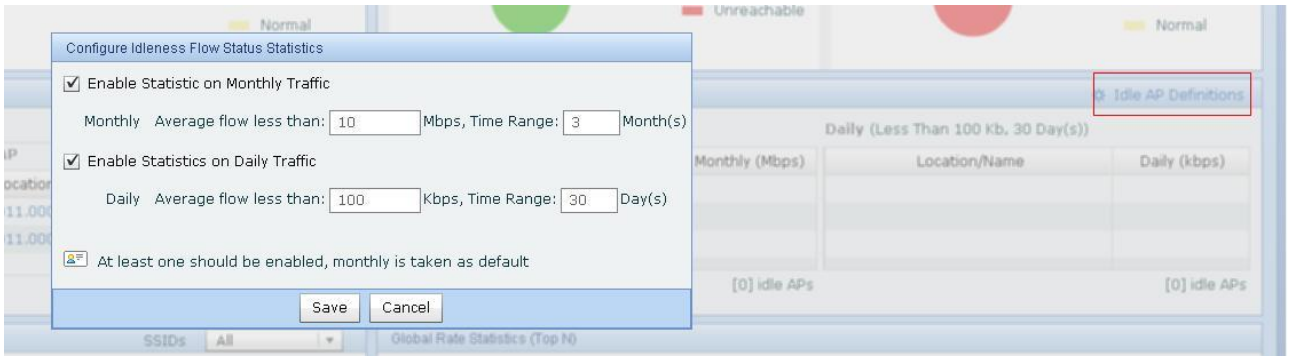


Figure 7.6. Configuring Time

Click **Save**, and the system returns to the **Dashboard** page.

7.1.5. Global STA Statistics

This function enables you to view the **Number of Authenticated STAs** and the **Number of Associated STAs**.

Operation Steps

4) Click Dashboard to view the **Global STA Statistics**, as shown in the following figure:

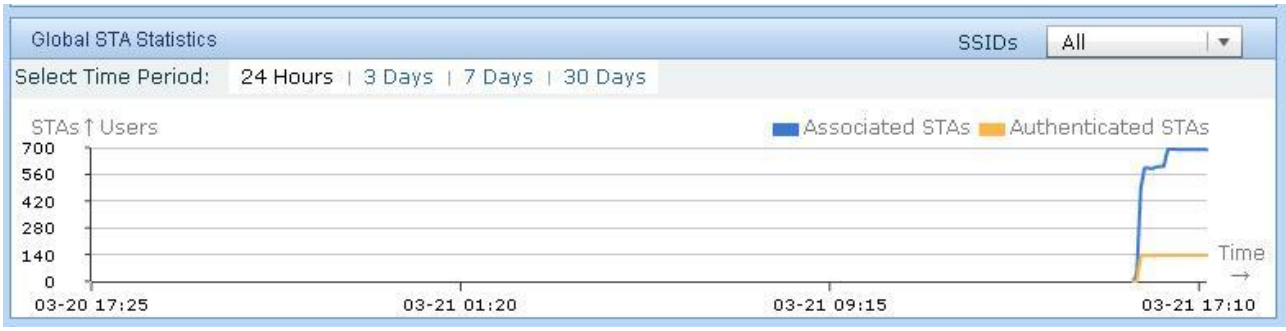


Figure 7.7. Global STA Statistics

When viewing the **Global STA Statistics**, you can select All or a specific SSID in the SSIDs field to view the STA statistics, as shown in the following figure:

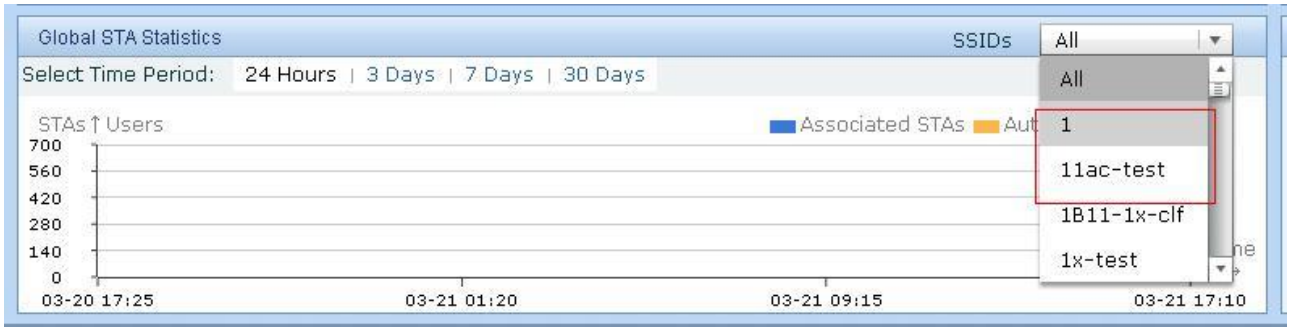


Figure 7.8. Selecting All or A Specific SSID

7.1.6. Top N Global Rate Statistics

This function enables you to view the top N Hotspots and the top N APs in rate.

Operation Steps

5) Click **Dashboard** to view the Global Rate Top N, as shown in the following figure:

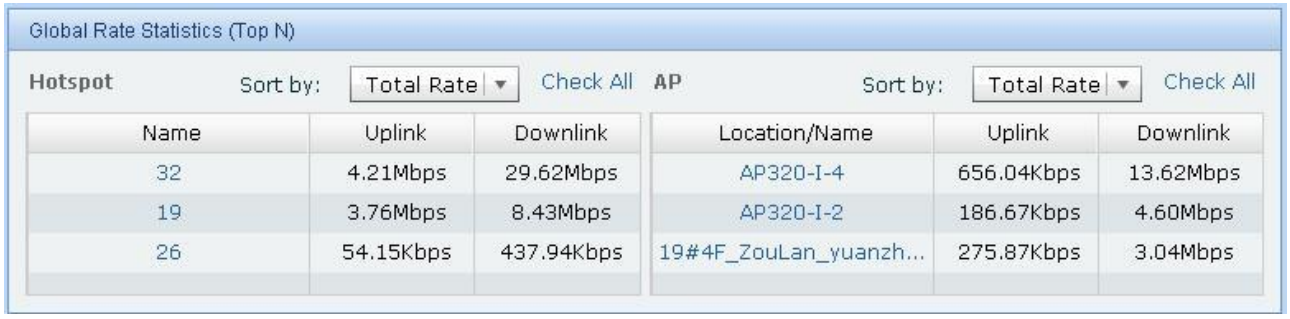


Figure 7.9. Global Rate Top N

Click **Check All** in the Hotspot Rate panel to view the Hotspot Rate Statistics, as shown in the following figure:

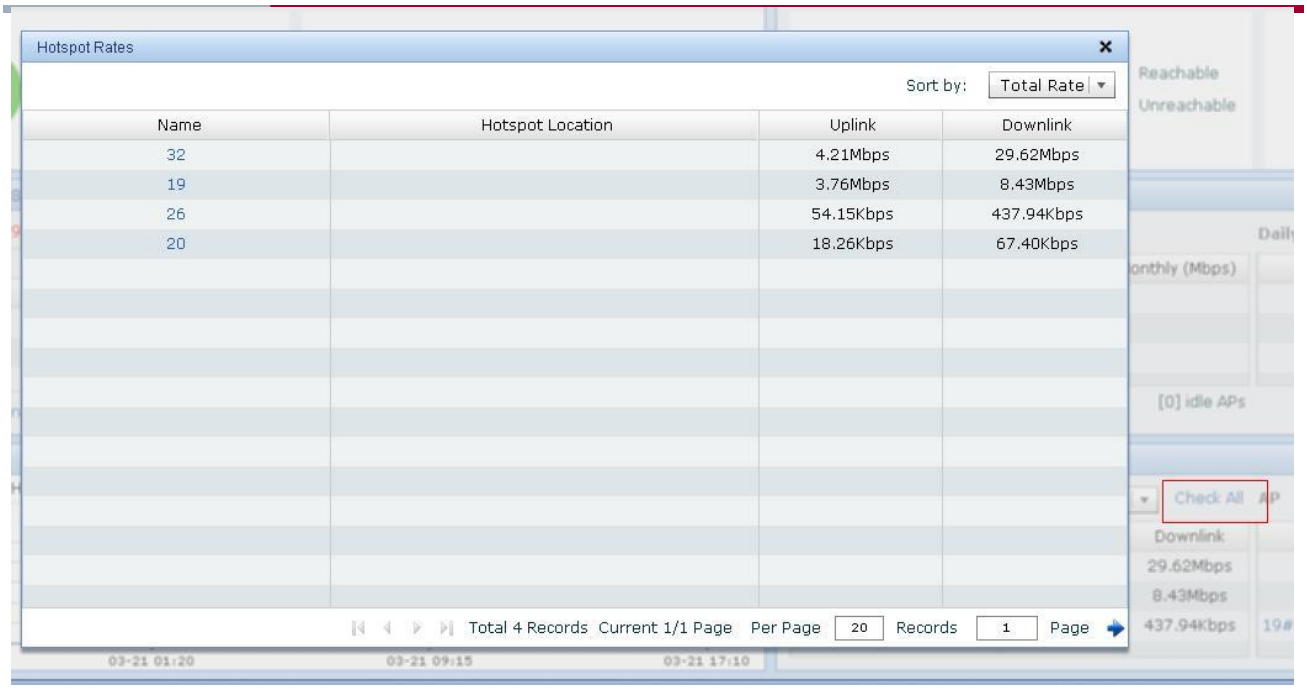


Figure 7.10. Hotspot Rate Statistics

Click **Check All** in the AP Rate panel to view the AP Rate Statistics, as shown in the following figure:

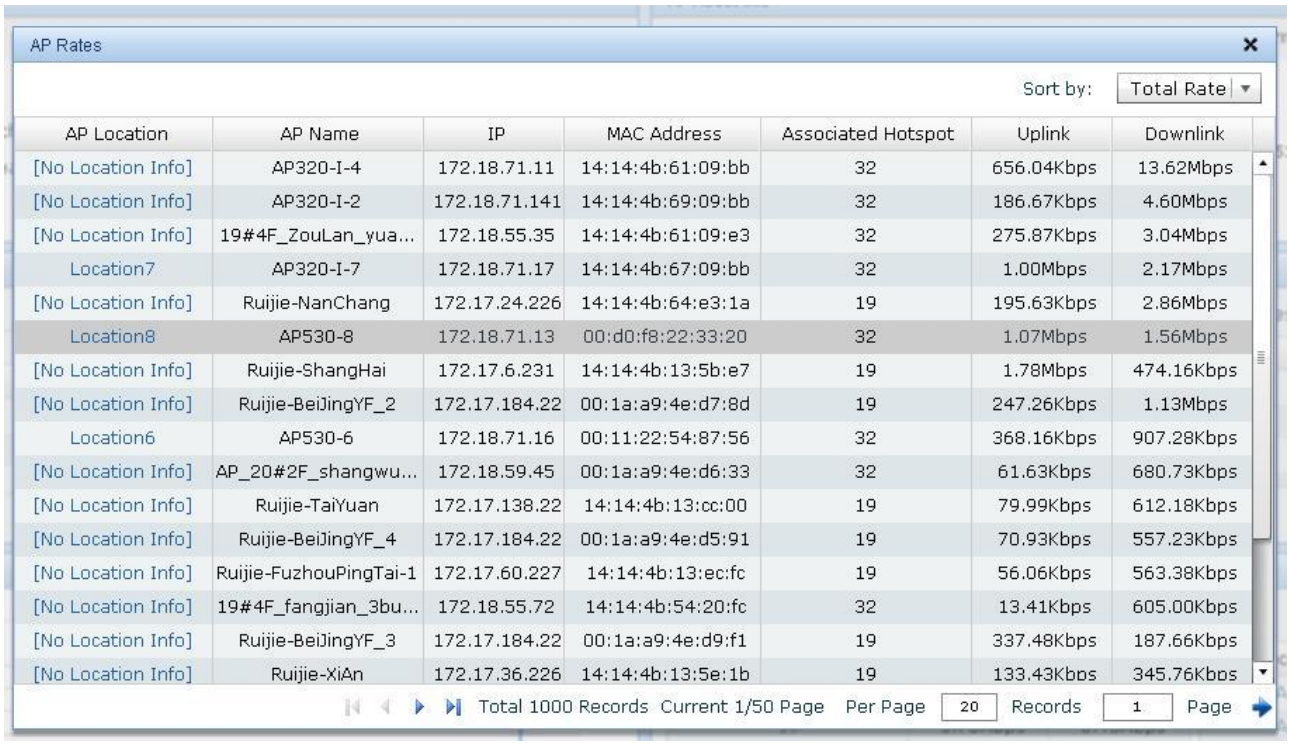


Figure 7.11. AP Rate Statistics

7.1.7. Global Out-of-Service Rate Statistics

This function enables you to view the **hotspot out-of-service rates** and the **AP out-of-service rates** in calculation time by pie charts.

Operation Steps

1. Click **Dashboard** to view the **global out-of-service rate statistics**, as shown in the following figure.

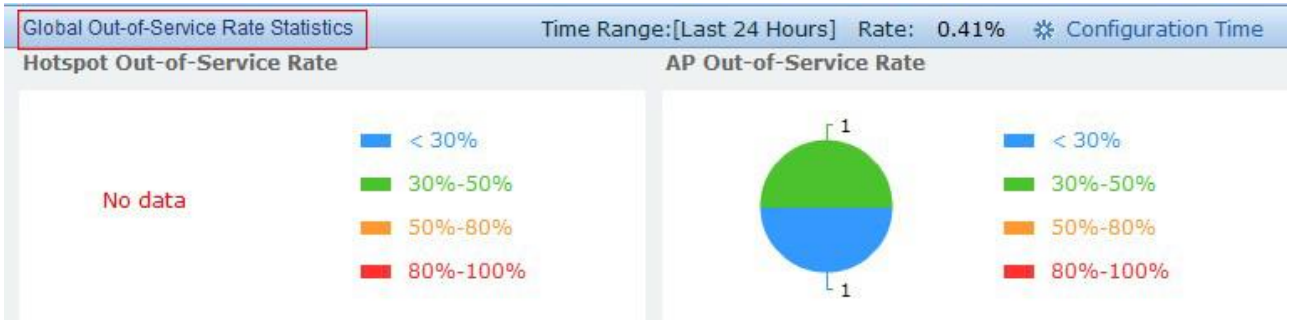


Figure 7.12. Global Out-of-Service Rate Statistics

2. Click **Configuration Time** to configure the calculation time range, as shown in the following figure.

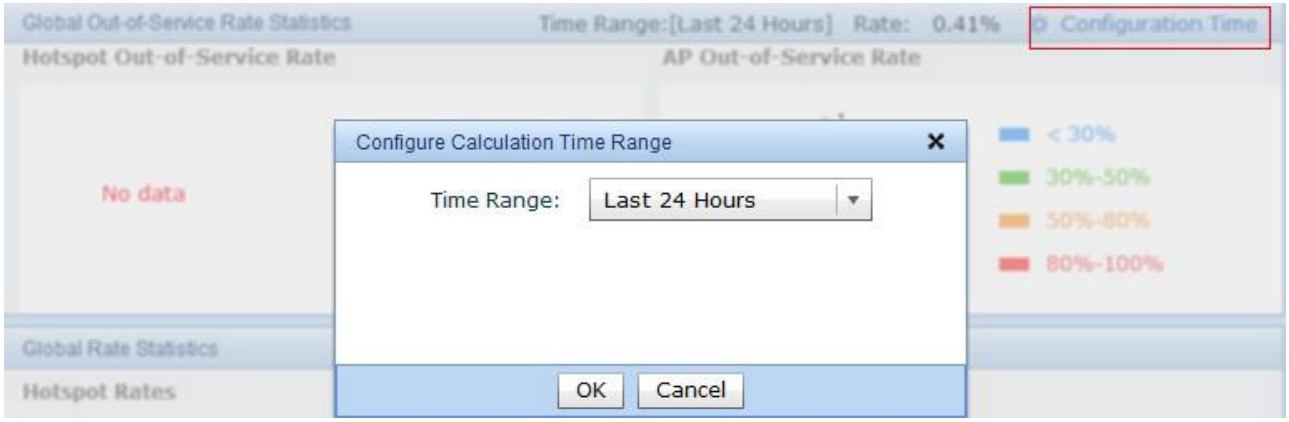


Figure 7.13. Calculation Time Range

3. Click **OK** and return to the **Dashboard** page.

7.1.8. Global Idle Traffic Statistics

This function enables you to view the idle traffic statistics of global Aps in calculation time.

Operation Steps

1. Click **Dashboard** to view the **global idle traffic statistics**, as shown in the following figure.

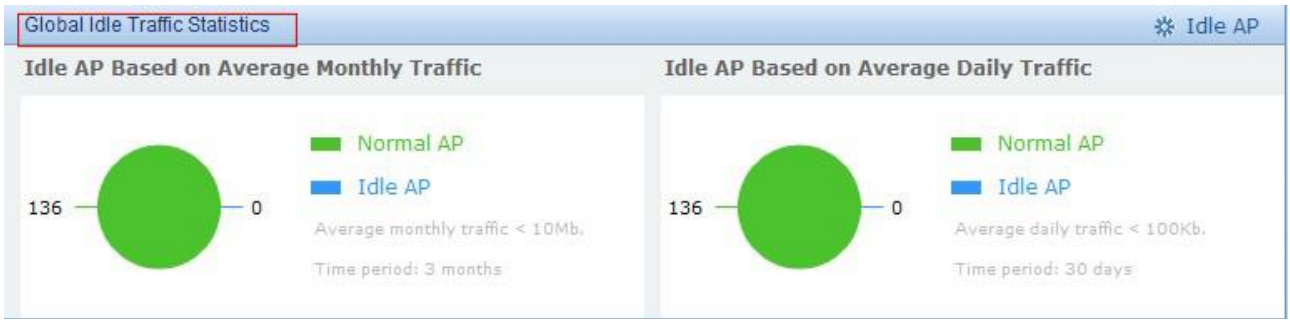


Figure 7.14. Global Idle Traffic Statistics

2. Click **Idle AP** to configure the flow threshold and time range for idle APs.

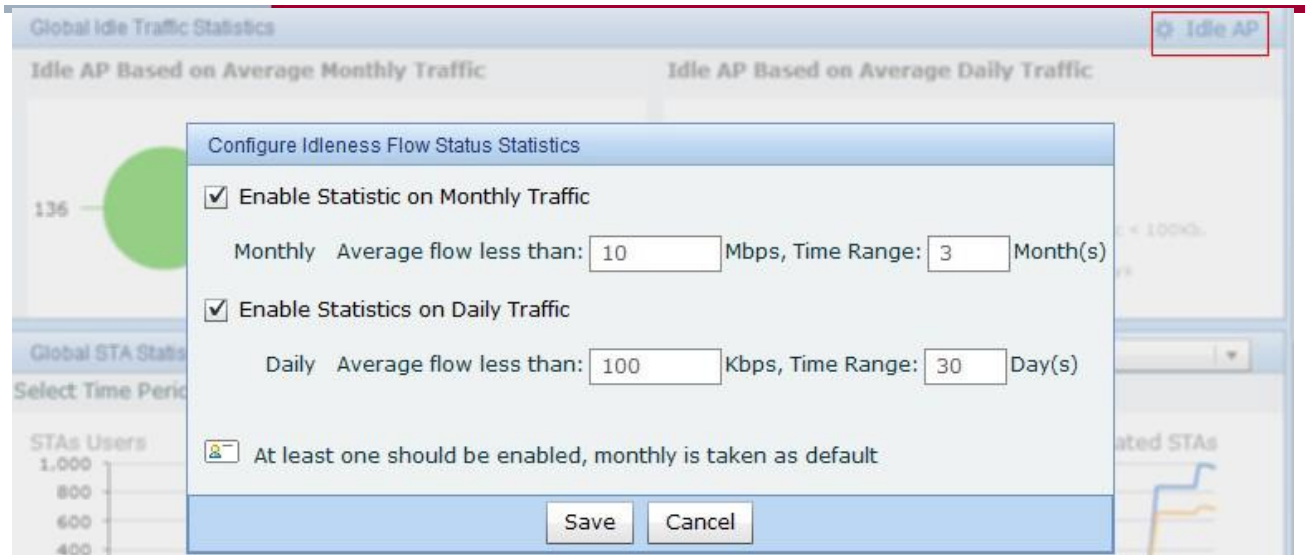


Figure 7.15. Flow Threshold and Time Range

3. Click **Save** and return to the **Dashboard** page.

7.1.9. Global Rate Statistics

This function enables you to view the hotspot rate statistics and AP rate statistics by bar charts.

Operation Steps

1. Click **Dashboard** to view the global rate statistics, as shown in the following figure.

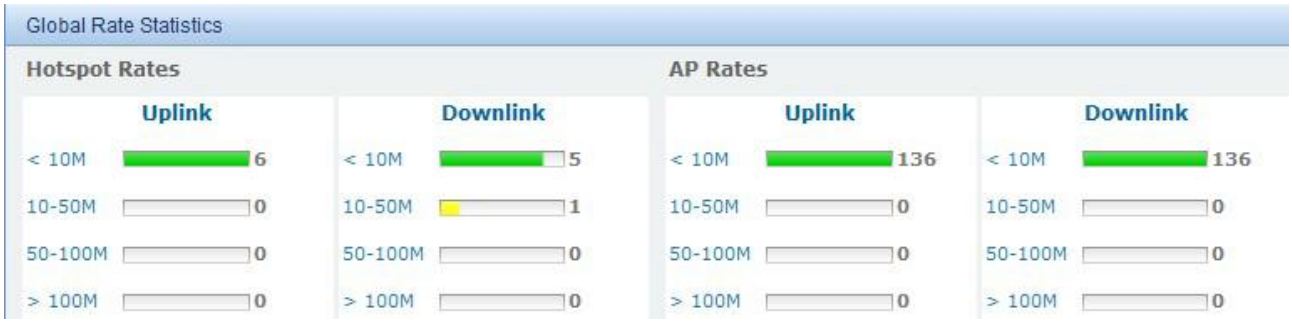


Figure 7.16. Global Rate Statistics

2. Click the **rate bar in Hotspot Rates** part to view the rate statistics of specific hotspots, as shown in the following figure.

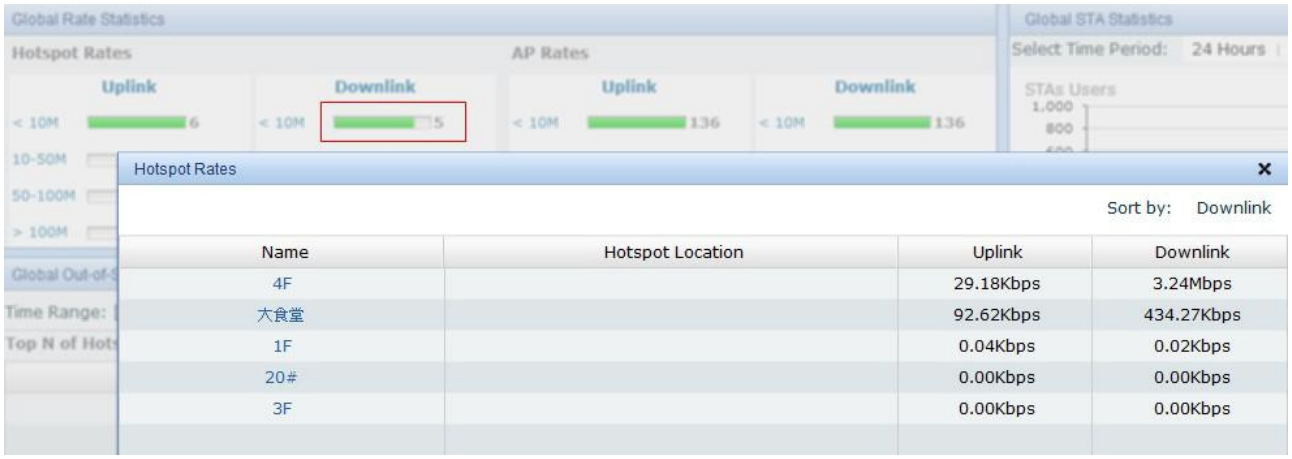


Figure 7.17. Hotspot Rates

3. Click the **rate bar in AP Rates** part to view the rate statistics of specific APs, as shown in the following figure.

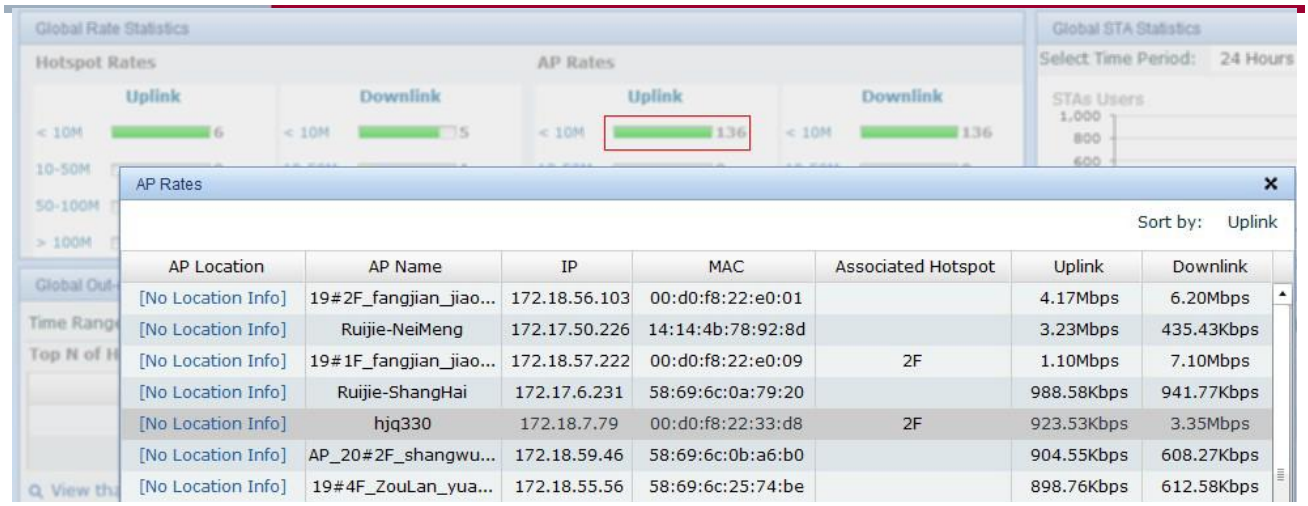


Figure 7.18. AP Rates

7.1.10. Rogue AP Statistics

This function enables you to view the statistics of AP working modes and rogue AP containment status by pie charts.

Operation Steps

1. Click **Dashboard** to show the **rogue AP statistics**, as shown in the following figure.

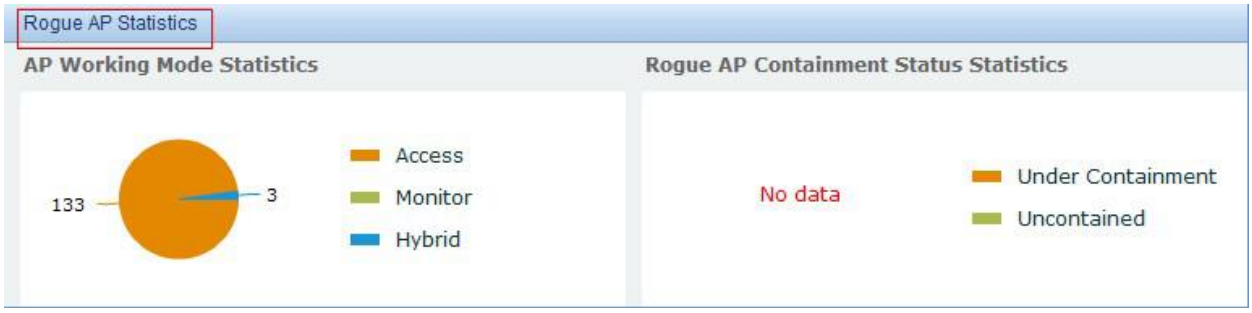


Figure 7.19. Rogue AP Statistics

7.1.11. Mini AP Asset Statistics

This function enables you to view the status and alarm statistics of Mini APs connected with i-Share+ APs.

Operation Steps

1. Click **Dashboard** to view the Mini AP asset statistics, as shown in the following figure.

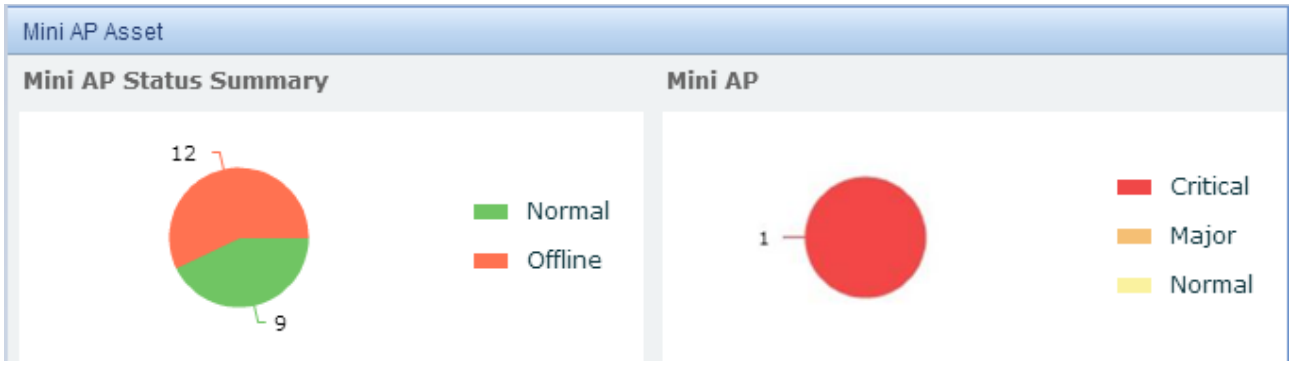


Figure 7.20. Mini AP Asset

2. Click the pie charts to go to the corresponding pages.

7.1.12. Top N Clients Statistics

This function enables you to view the statistics of top N clients in the SNC.

Operation Steps

1. Click **Dashboard** to view the statistics of top N clients, as shown in the following figure.

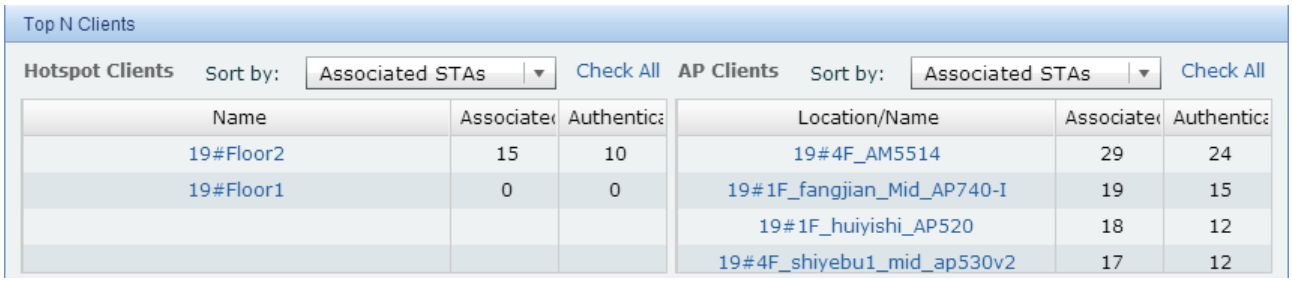


Figure 7.21. Top N Clients

2. Click a link to view all information about the SSID or AP details.

7.1.13. WLAN Homepage Custom Settings

This function enables you to customize the statistic items on the homepage.

Operation Steps

1. Choose **Dashboard** > **Custom**. WLAN Homepage Custom Settings is displayed, as shown in the following figure.

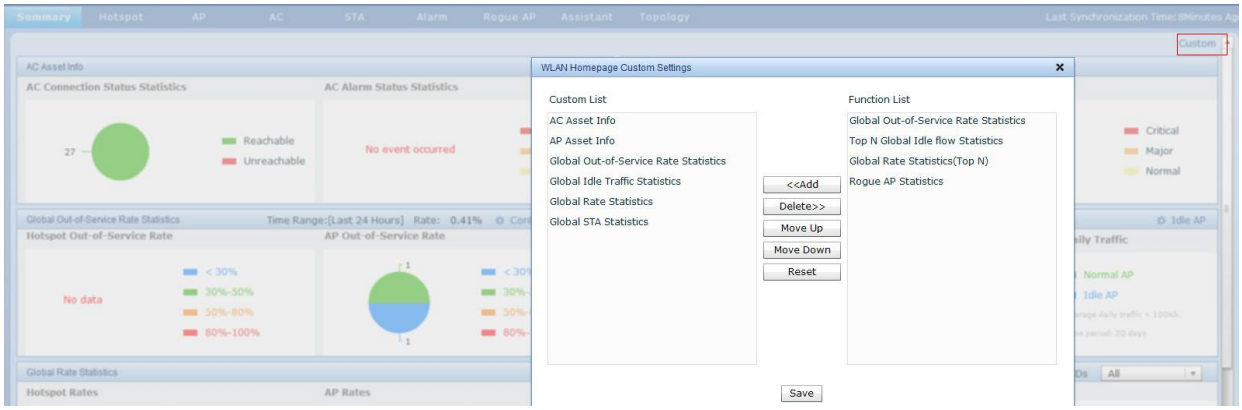


Figure 7.22. WLAN Homepage Custom Settings

2. Double click an item in the **Function List**, or choose one item in the Function List and click **Add** to add a statistic item, as shown in the following figure.

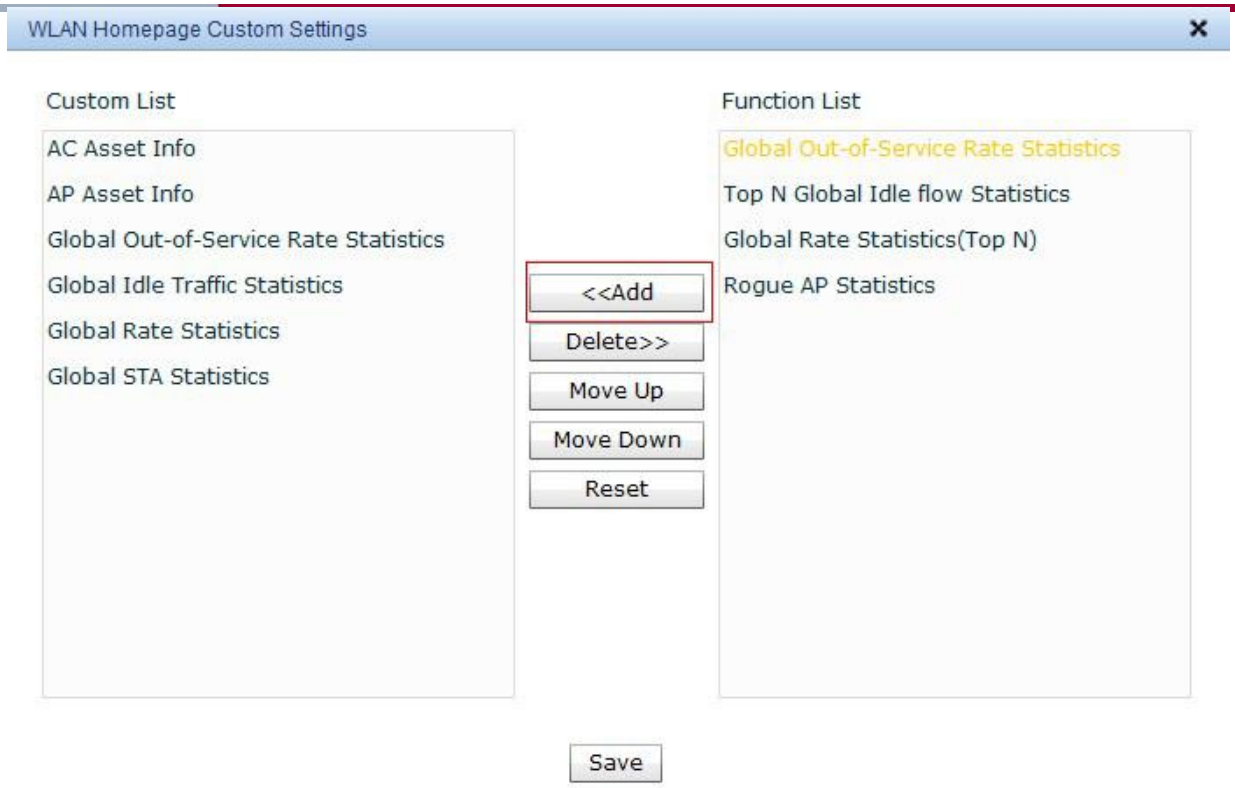


Figure 7.23. WLAN Homepage Custom Settings

3. Double click an item in the **Custom List**, or choose one item in the Custom List and click **Delete** to delete a statistic item, as shown in the following figure.

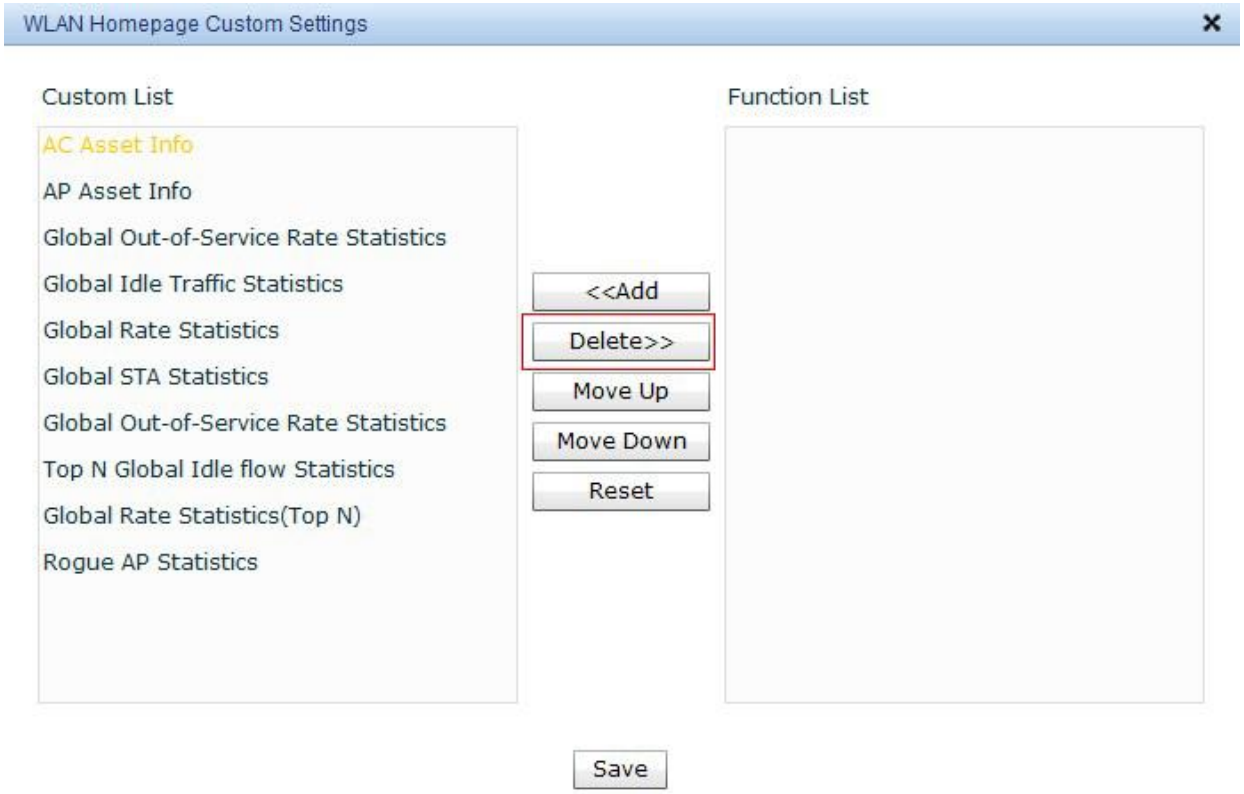


Figure 7.24. Custom Settings

4. Choose one item in the **Custom List** and click **Move Up** or **Move Down** to adjust the displaying order, as shown in the following figure.

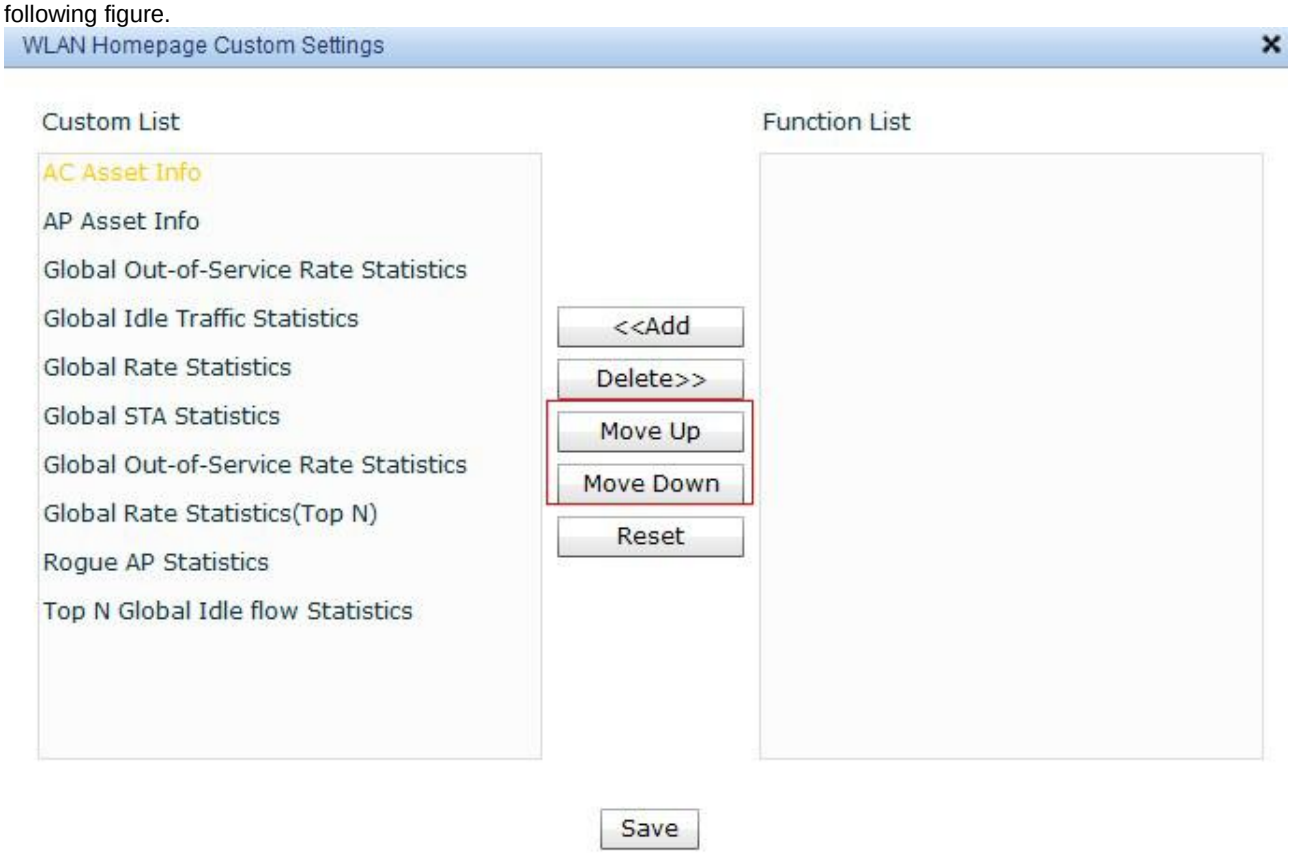


Figure 7.25. Custom Settings

5. Click **Reset** to restore the default settings, as shown in the following figure.

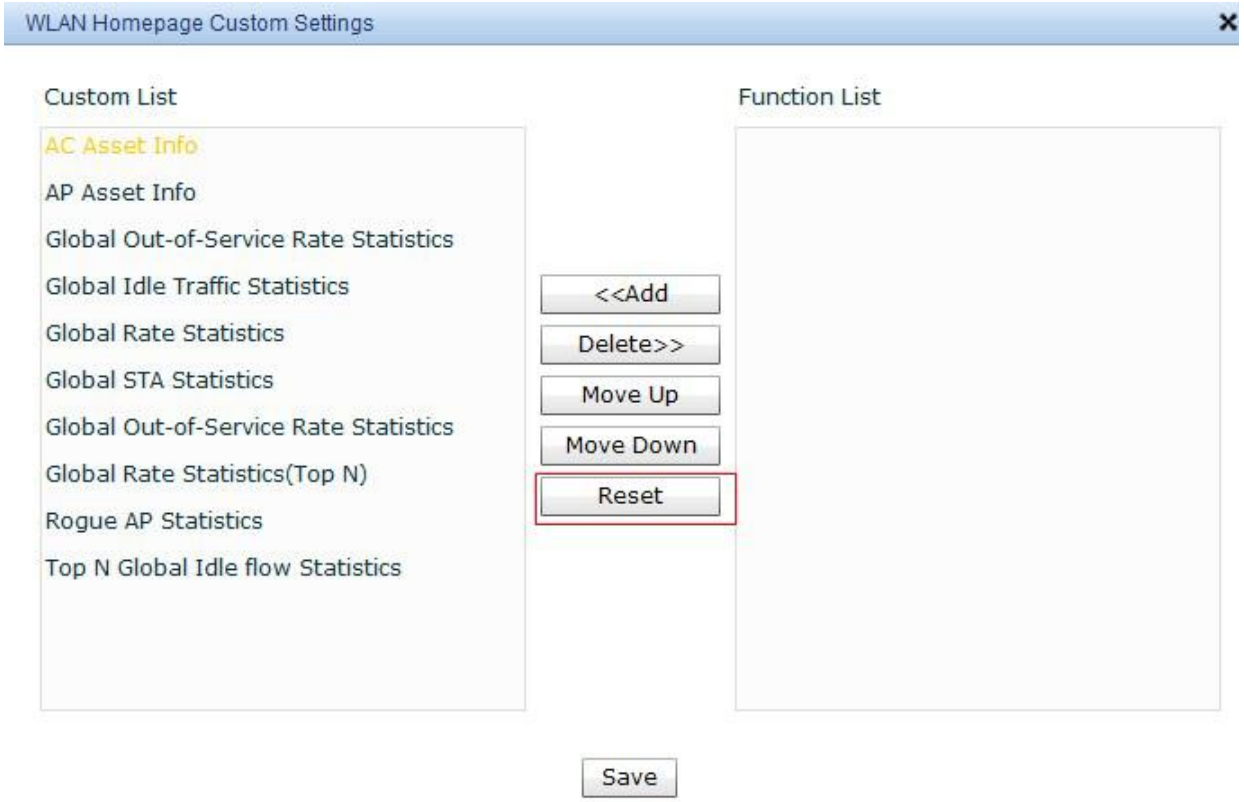


Figure 7.26. Custom Settings

6. Click **Save** and return to the **Dashboard** homepage for statistics.

7.2. Hotspot

The Hotpot module enables you to import, export, modify and count hotspot information as well as associating hotspots with the APs.

Major Functions

- Import and Exporting Hotspot
- Modify Hotspot
- Hotspot Details
- Hotspot Information Statistics
- WLAN Heat Map
- Configure AP Modes

7.2.1. Import and Exporting Hotspot

This function enables you to import and export hotspot information.

Import Hotspot Information

6) Click **Import**, as shown in the following figure:

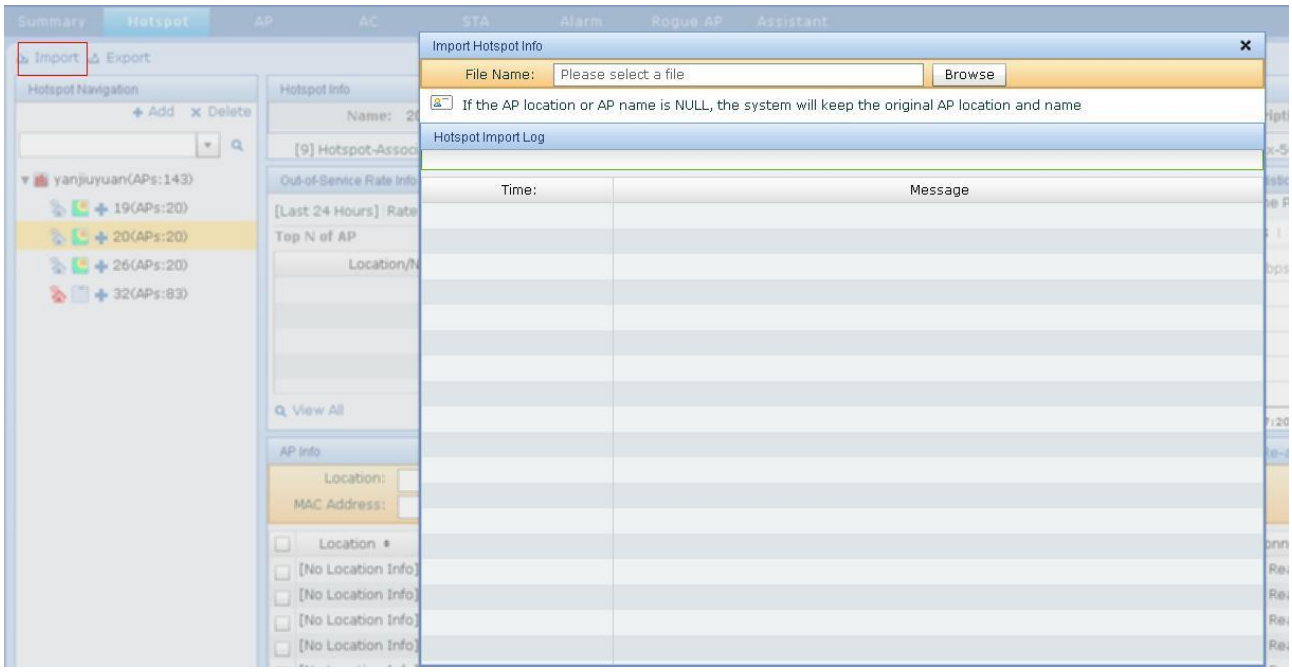


Figure 7.27. Import Page

Select a local excel file containing hotspot information and decide whether to inform the device of AP location and name. Click **Upload**, as shown in the following figure:

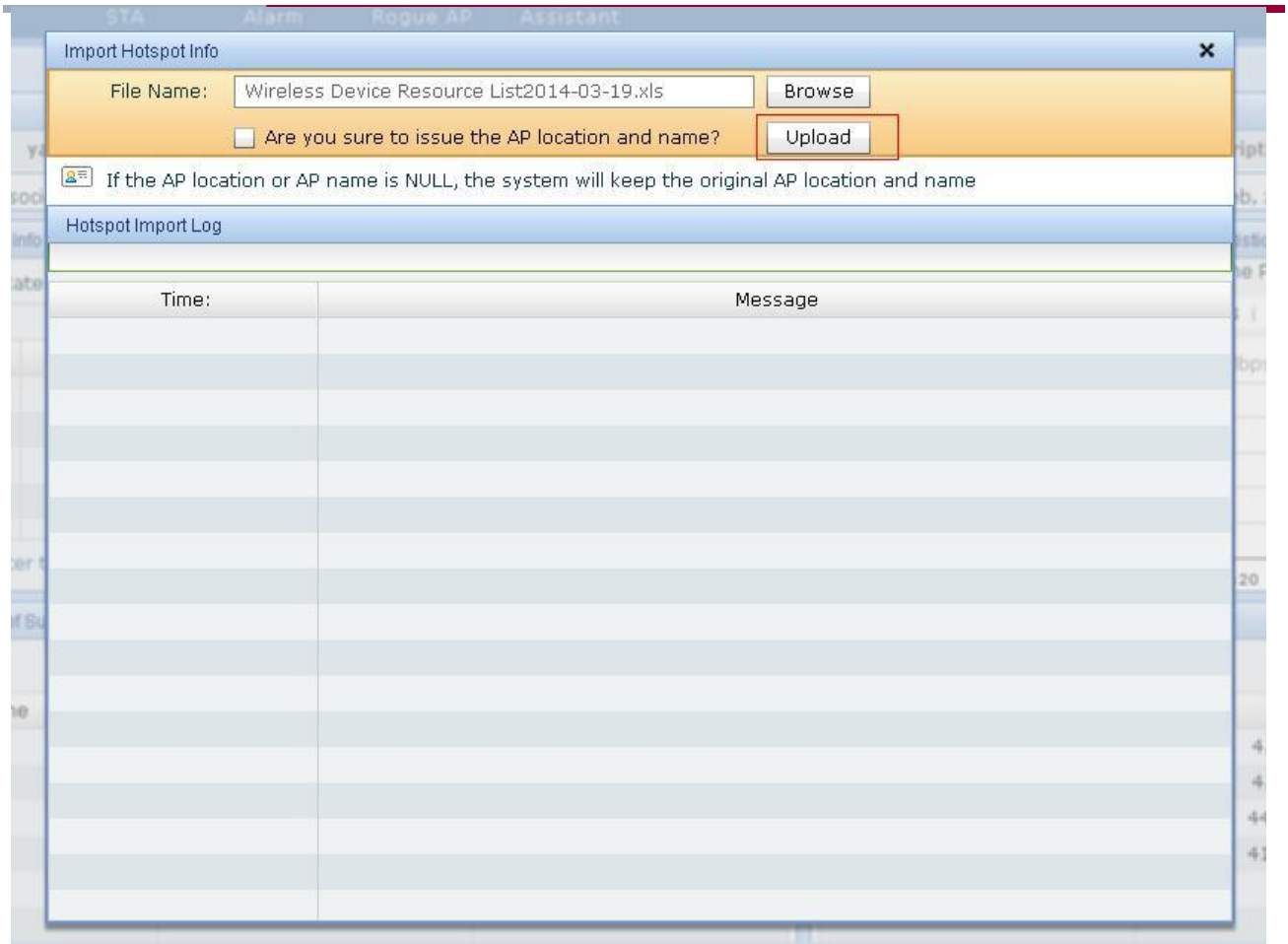


Figure 7.28. Importing Hotspot Information

Export Hotspot Information

7) Click **Export**. Select a directory and click **Save**, as shown in the following figure:

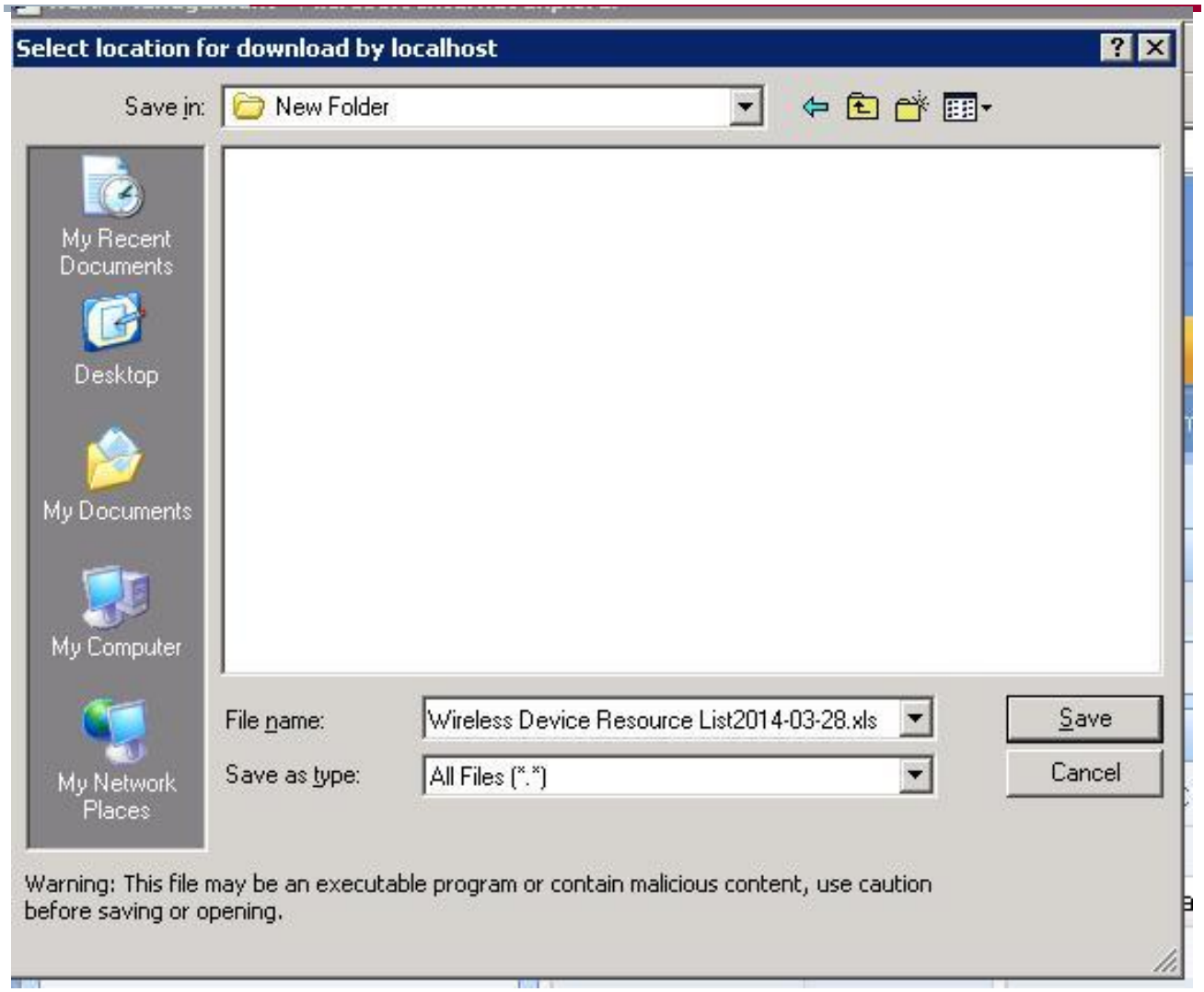


Figure 7.29. Exporting Hotspot Information

After the export is complete, the system returns to the **Hotspot Info** page.

7.2.2. Modify Hotspot

This function enables you to modify hotspot information, including the hotspot name, address and description.

Operation Steps

8) Select the hotspot and click **Modify**, as shown in the following figure:

Figure 7.30. Modifying Hotspot Information

Modify the information in the dialog box displayed and click **Save**.
After the modification is complete, the system returns to the **Hotspot Info** page.

7.2.3. Hotspot Details

This function enables you to view detailed information of the hotspot, including the hotspot name, AP count and alarm count.

Add AP

9) Select the hotspot, click **Add AP** on the **AP Info** page or **+** in H**otspot Navigation**, as shown in the following figure:

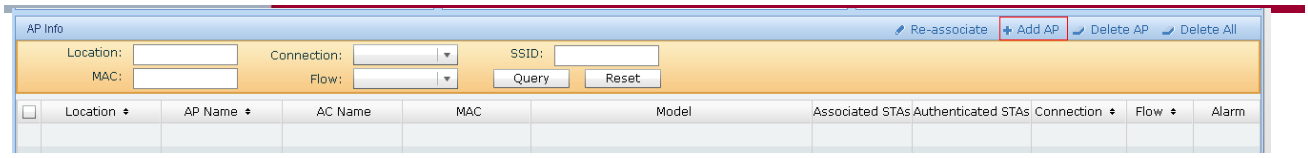


Figure 7.31. Clicking **Add AP** on **AP Info** Page

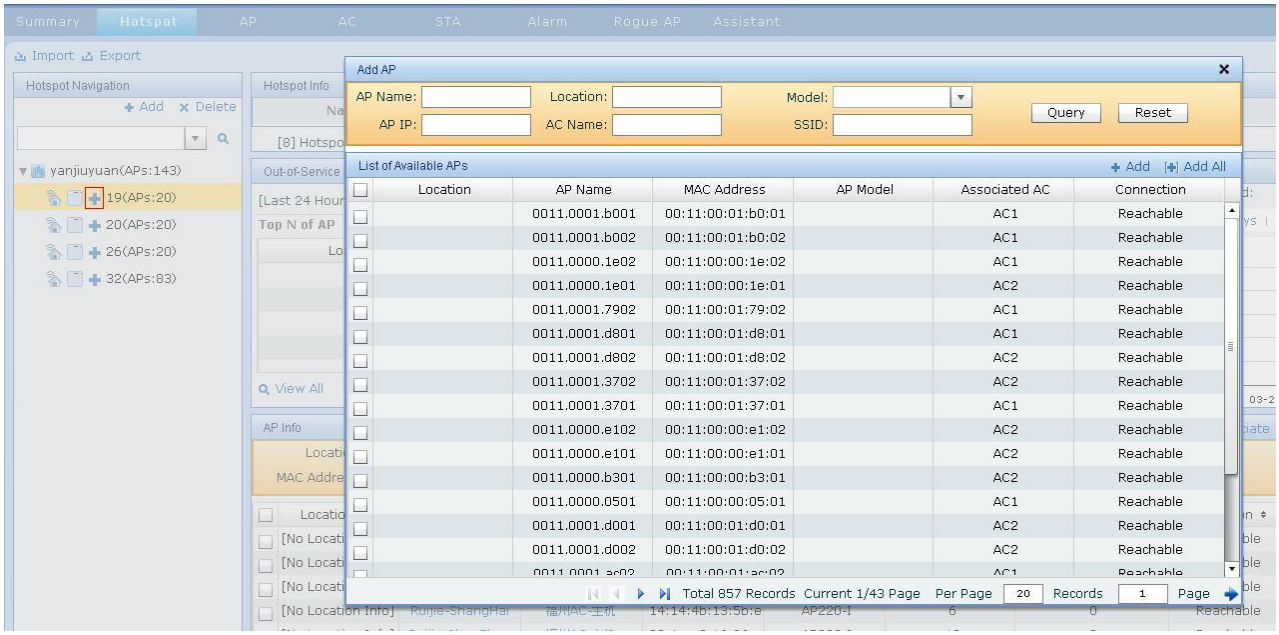


Figure 7.32. Clicking **+** in **AP Navigation**

If you click **+** in **Hotspot Navigation**, the **Add AP** page is displayed. You can add some or all APs, as shown in the following figure:

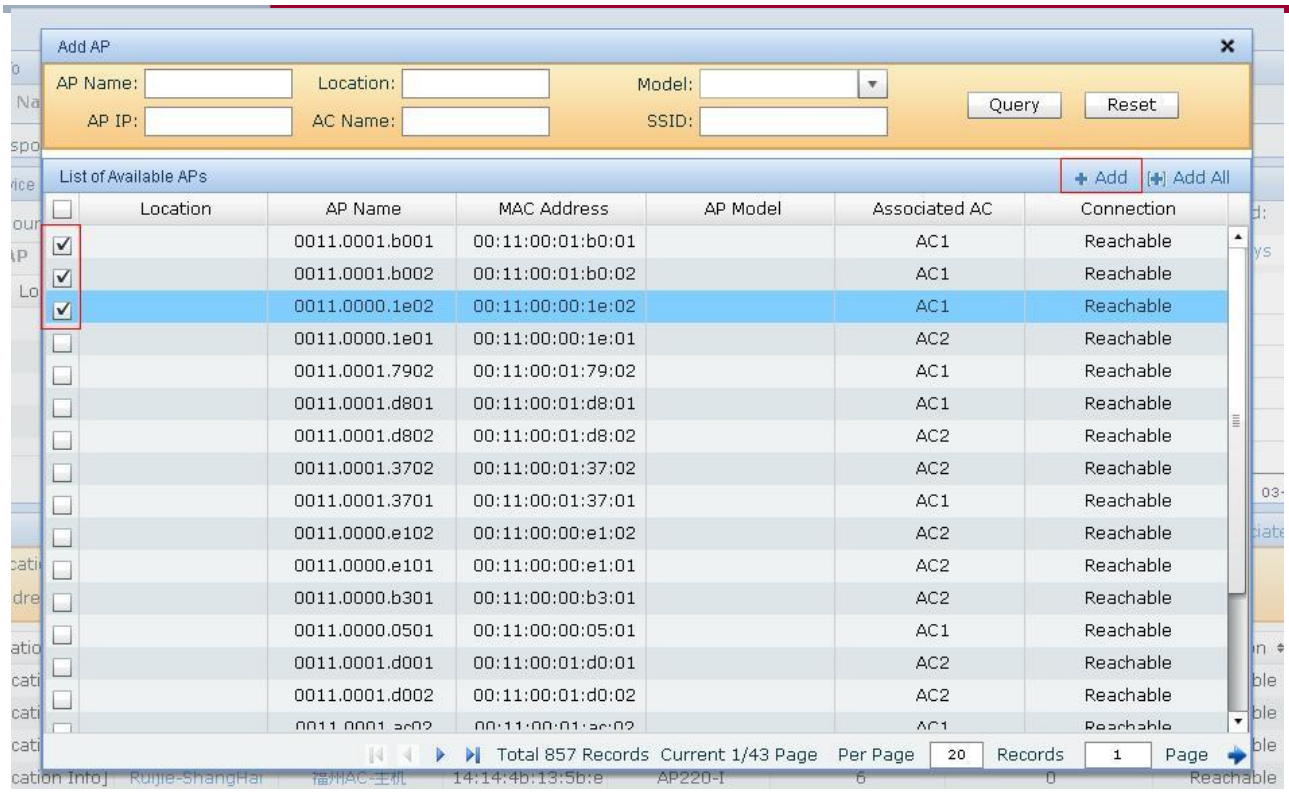


Figure 7.33. Selecting AP to Add

After the AP is added, the system returns to the hotspot details page.

Delete AP

10) Select the AP and click **Delete AP**, as shown in the following figure:

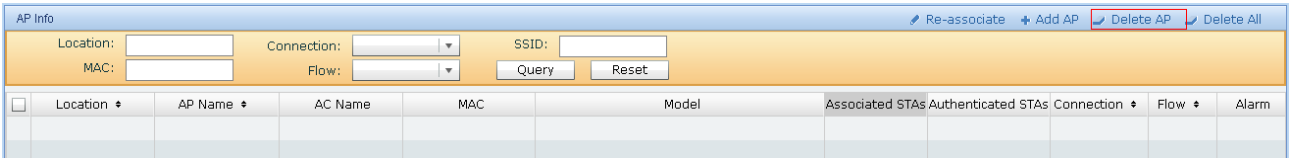


Figure 7.34. Deleting AP

After the AP is deleted, the system refreshes the **AP Info** page associated to the hotspot.

Delete All APs

11) Select the hotspot and click **Delete All**.
After all APs are deleted, the system refreshes the **AP Info** page associated to the hotspot.

Re-associate to Hotspot

12) Select the AP and click **Re-associate**, as shown in the following figure:

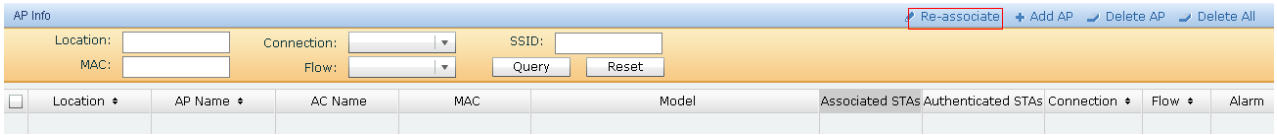


Figure 7.35. Re-associating to Hotspot

You can switch the hotspot the AP is associated to, as shown in the following figure:

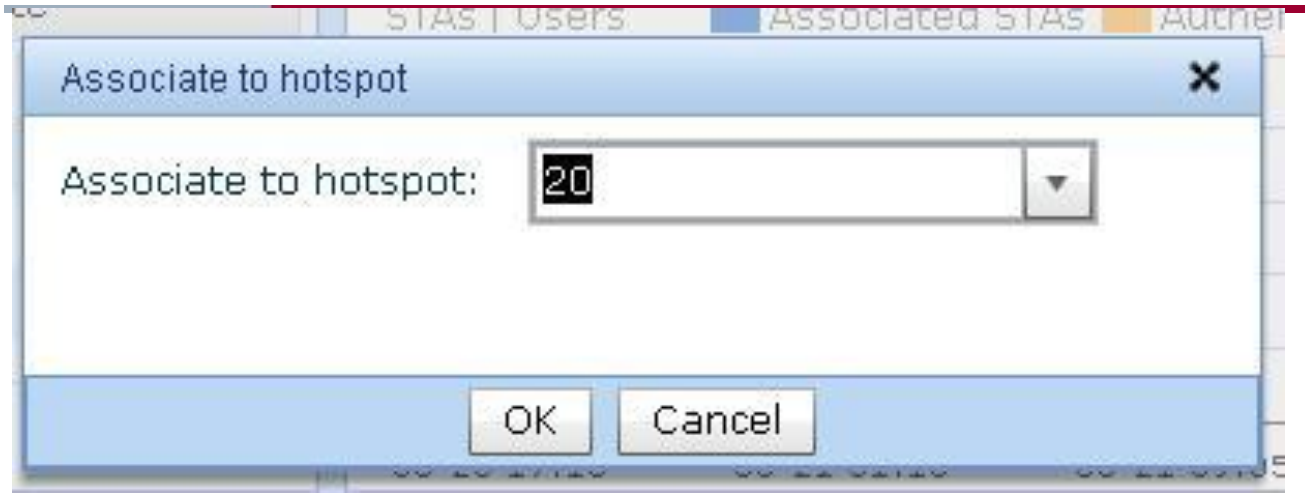


Figure 7.36. Switching Associated-Hotspot

Select the hotspot and click **OK**, and the system returns to the hotspot details page and refreshes the page.

7.2.4. Hotspot Information Statistics

This function enables you to view hotspot information statistics, including out-of-service rates, associated STA counts and uplink/downlink rates.

Select the hotspot and view its information statistics.

Hotspot information statistics includes out-of-service rates, associated STA counts, uplink/downlink rates, Top N STA counts and Top N rates of sub-hotspots/APs, as shown in the following figure:

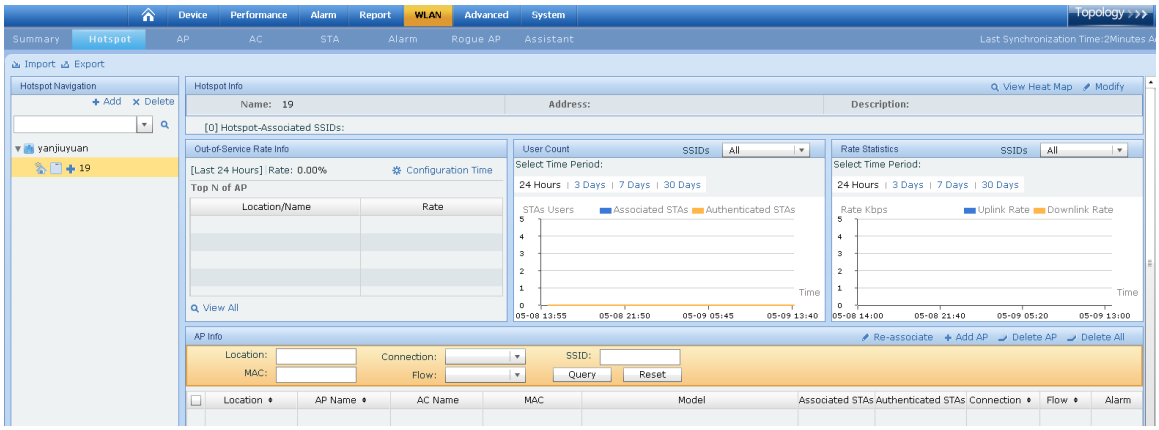


Figure 7.37. Hotspot Information Statistics

7.2.5. WLAN Heat Map

This function enables you to view the WLAN heat map, including operations of importing the background picture, setting the scale and barrier, and viewing coverage based on RSSI, rate or channel interference.

Go to Heat Map Page

Click the **Heat Map** icon or View **Heat Map** at the right upper corner, as shown in the following figure:

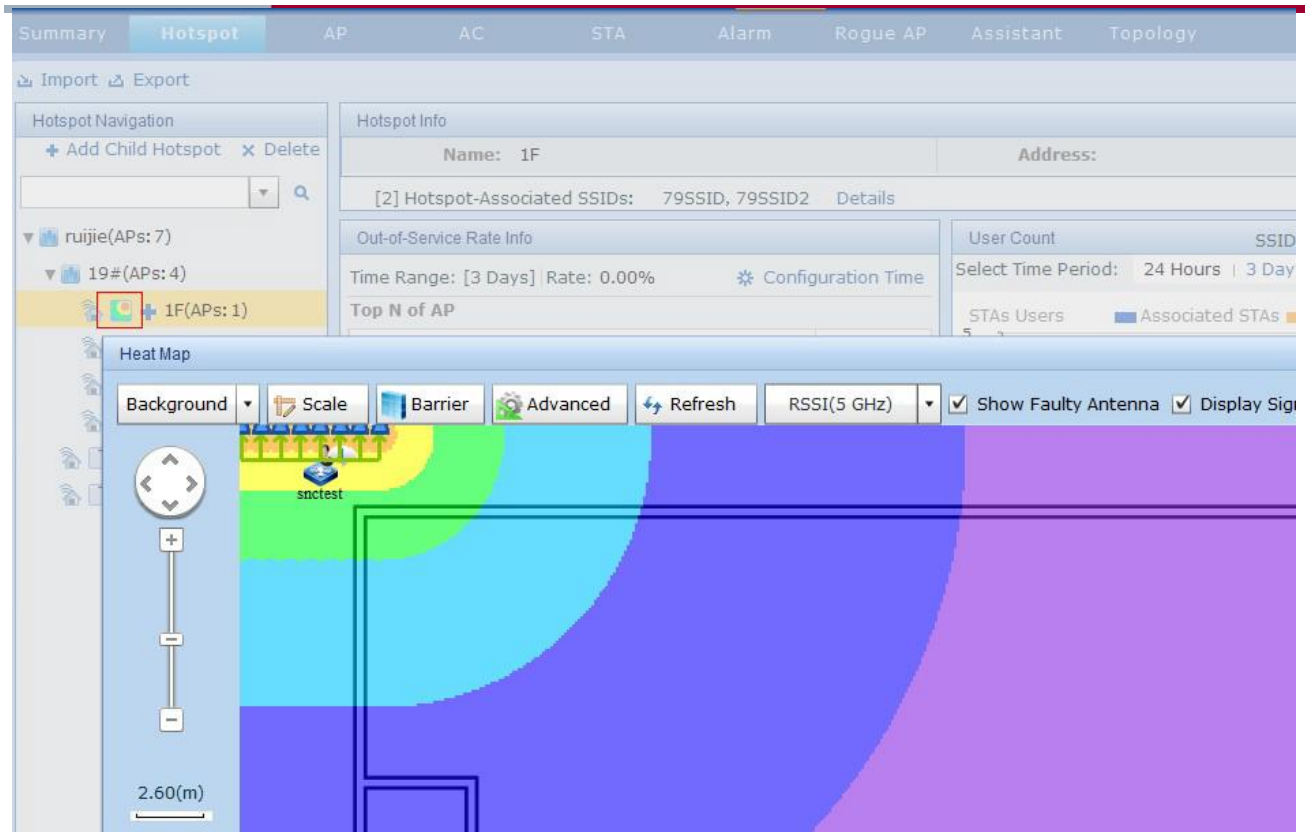


Figure 7.38. Going to Heat Map Page

Set Heat Map

13) Click **Background** and select **Import** in the menu displayed, as shown in the following figure:

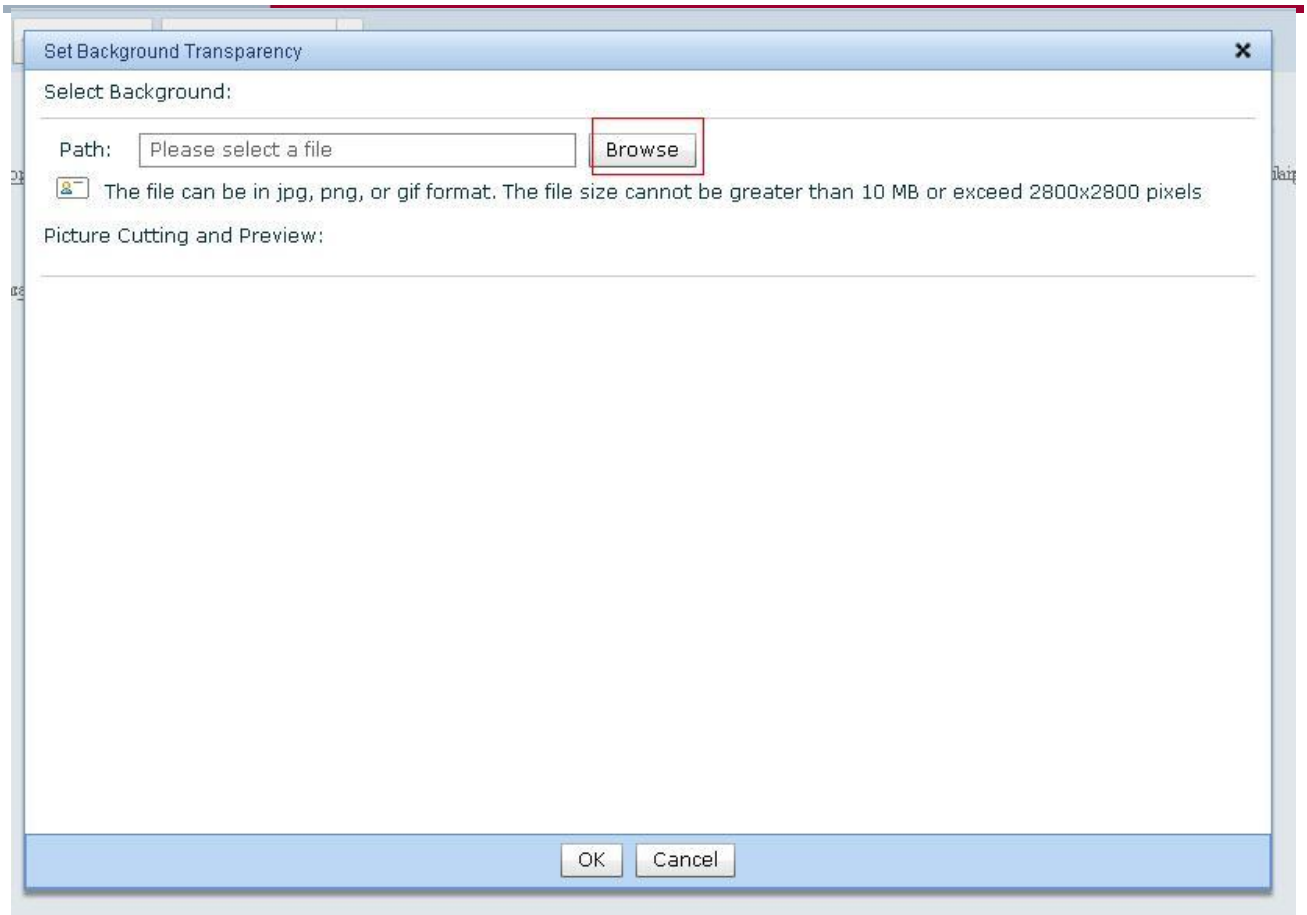


Figure 7.39. Importing Background Picture

Click **Browse** and select the picture to be imported. Cut the picture according to the requirement and click **OK**, as shown in the following figure:

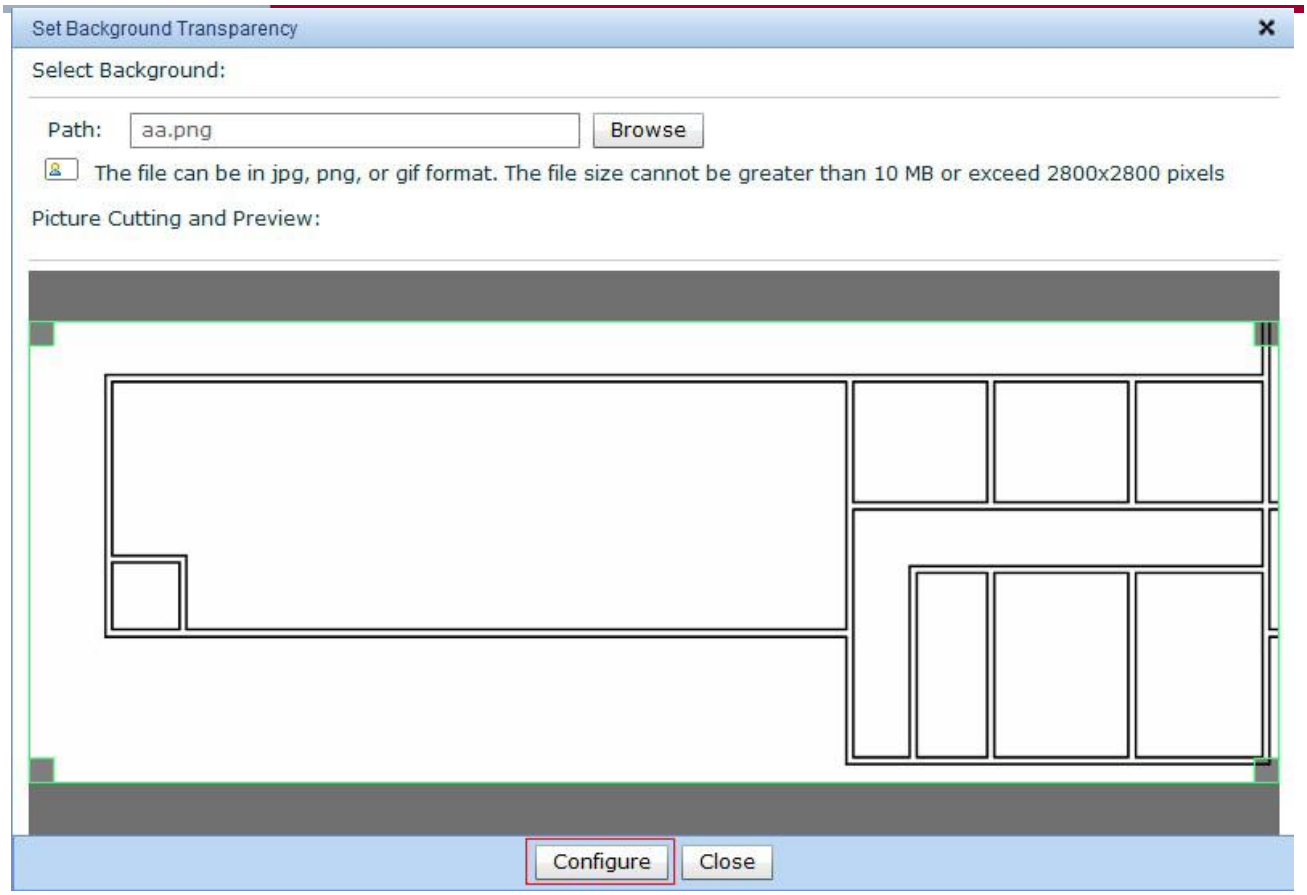


Figure 7.40. Configuring Background Picture

After the background picture is configured, the scale configuration notification is displayed, as shown in the following figure:

Figure 7.41. Scale Configuration Notification

Click **OK** or click **Scale** on the **Heat Map** page to set the scale of the picture. Press the mouse to draw a line on the background picture and set its physical length in the dialog box displayed. as shown in the following figure:

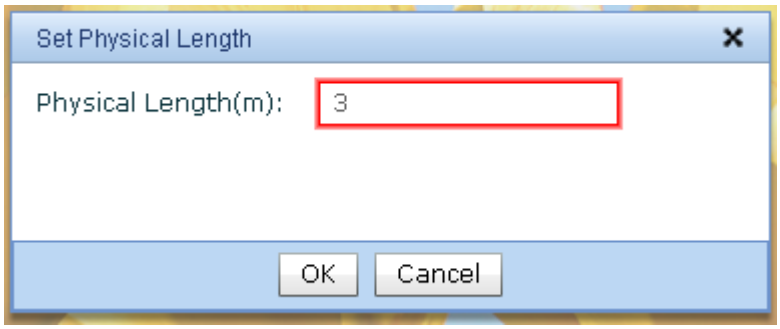


Figure 7.42. Setting Scale

After the scale is set, click **Barrier** (or right-click on the background picture and select **Add Barrier**) to set the barrier, including its shape, type and thickness, as shown in the following figure:

Figure 7.43. Setting Barrier

Check the **Show Faulty Antenna box** to view faulty antennas whose Radio/antenna is not enabled/connected, as shown in the following figure.

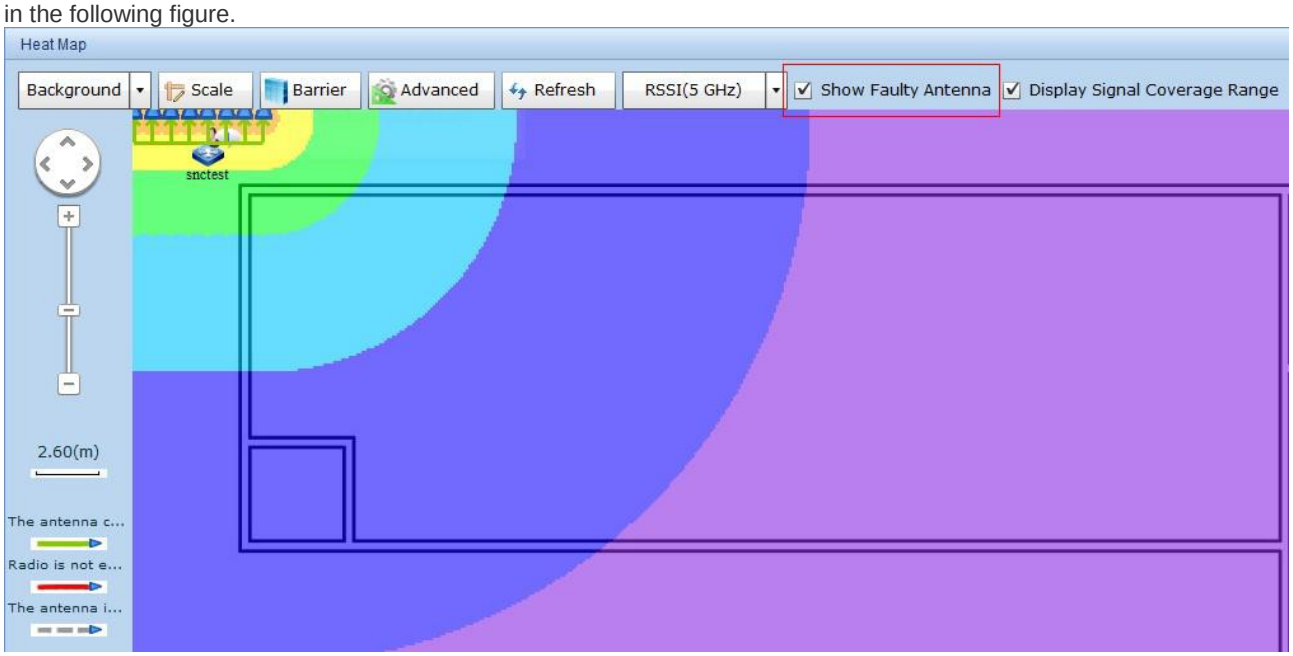


Figure 7.44. Viewing Faulty Antenna

Check the **Show Signal Coverage Range box** to view signal coverage range in the heat map, as shown in the following figure.

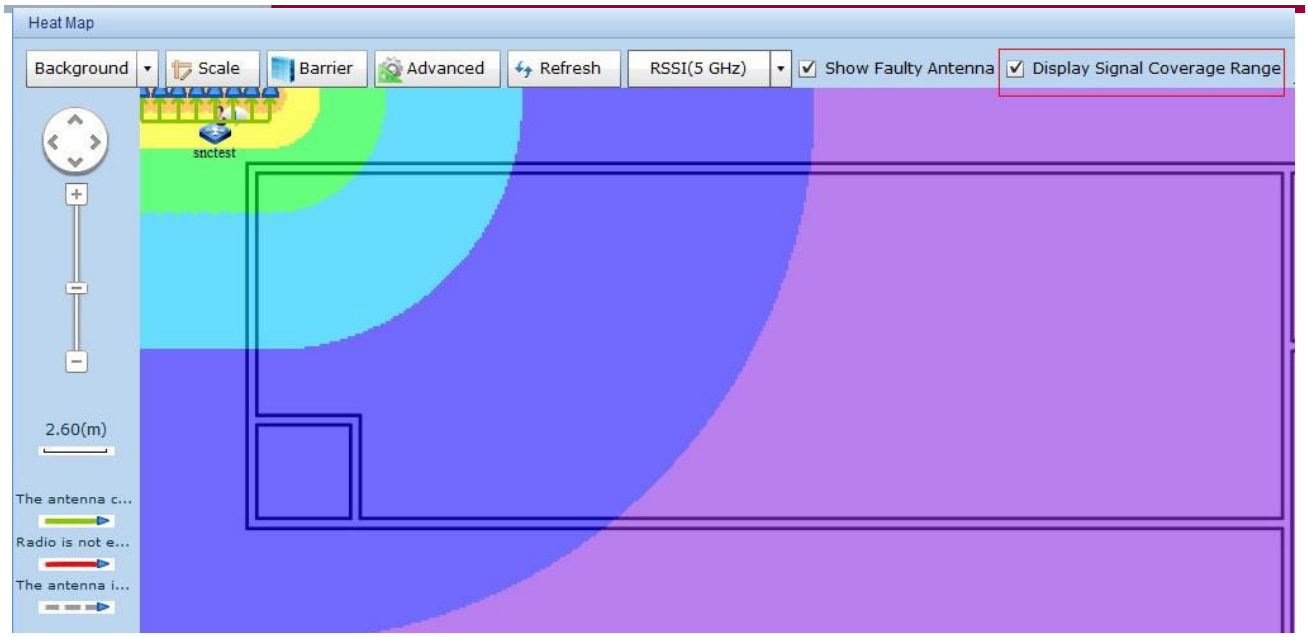


Figure7.45. Showing Signal Coverage Range

Click **RSSI** (2.4GHz) and view RSSI coverage, as shown in the following figure:

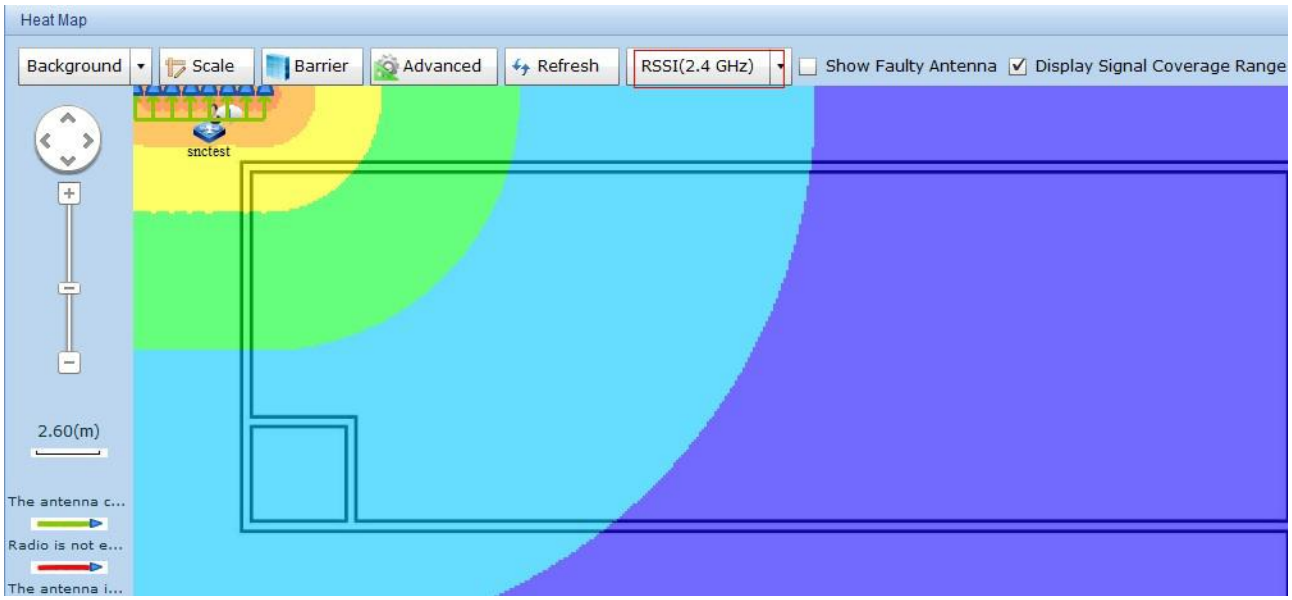


Figure 7.46. RSSI Coverage

Click **Rate** (2.4GHz) and view rate coverage, as shown in the following figure

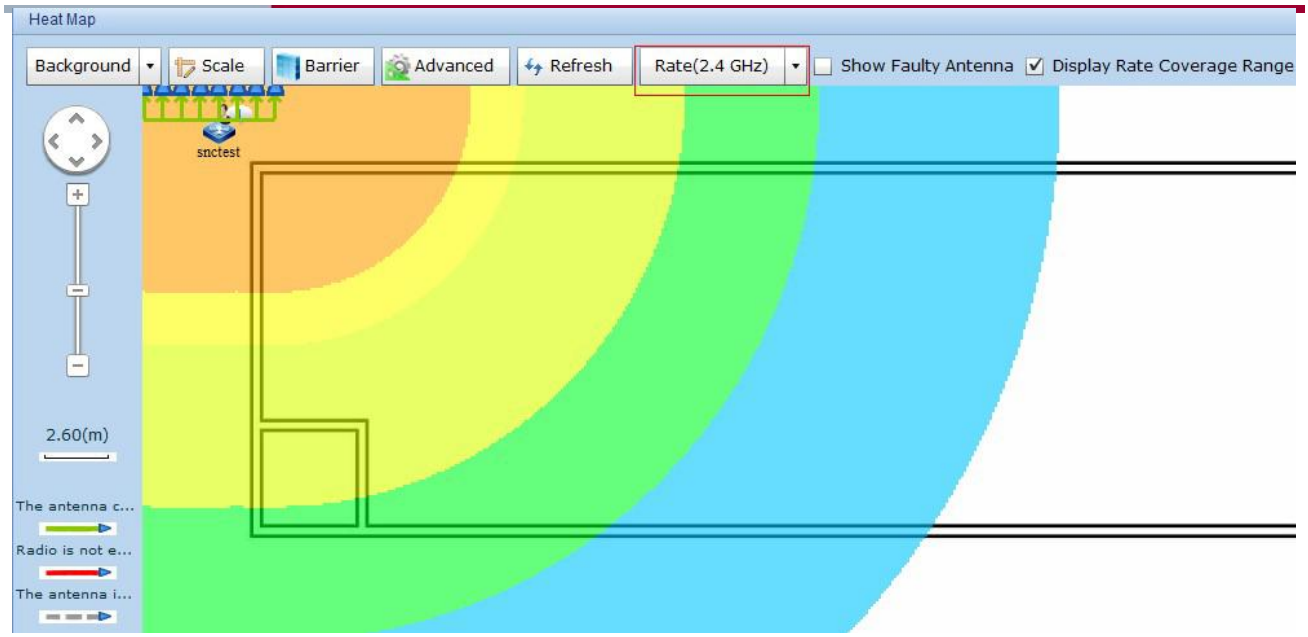


Figure 7.47. Rate Coverage

Click **Channel Interference** (2.4GHz) and view channel interference coverage, as shown in the following figure:

Figure 7.48. Chanel Interference Coverage

Synchronize APs in Hotspot

You can synchronize the AP information on the **Heat Map** page about their channels and rates to update the RSSI coverage and rate coverage, as shown in the following figure:

Figure 7.49. Synchronizing APs in Hotspot

Refresh Heat Map

You can refresh the heat map to show the RSSI coverage and rate coverage based on the latest AP status and barriers, as shown in the following figure:

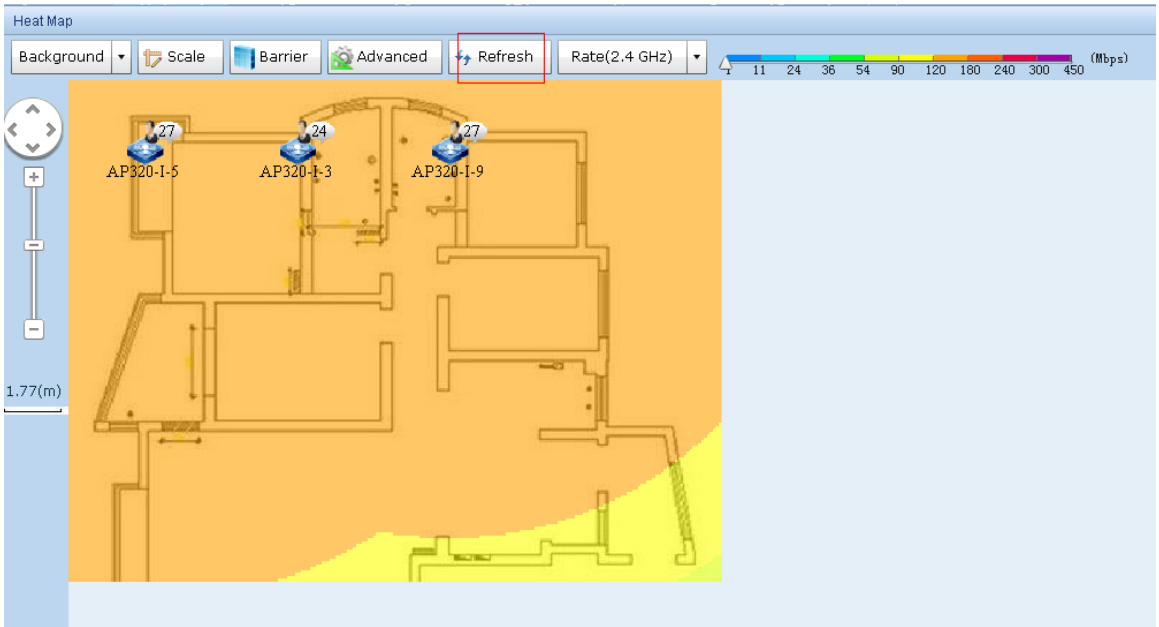


Figure 7.50. Refreshing Heat Map

View STA Info

Right-click on the **Hotspot Navigation** menu and select **View STA Info** on the menu displayed, as shown in the following figure:

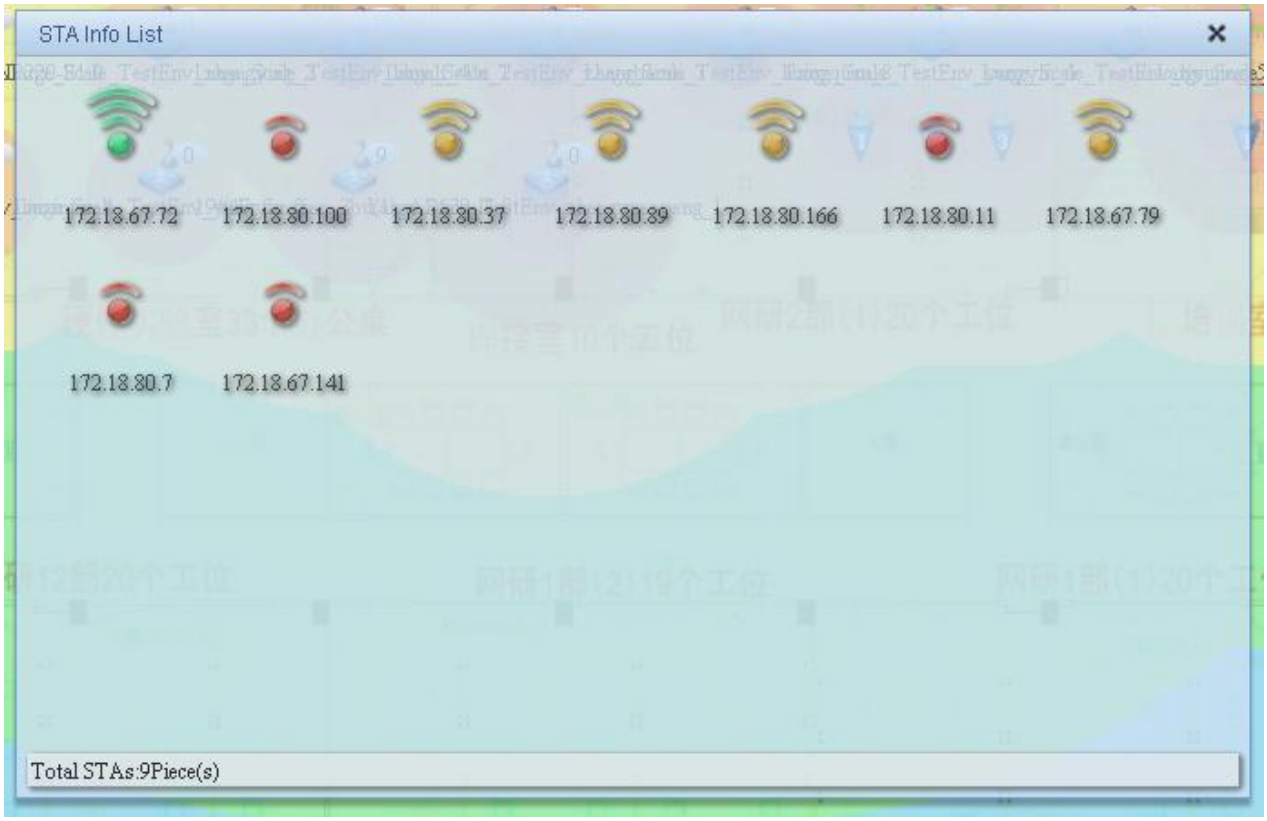


Figure 7.51. STA Info List

Configure AP Channel and Power

Right-click on the AP and select **Modify AP Configuration** on the menu displayed, as shown in the following figure:

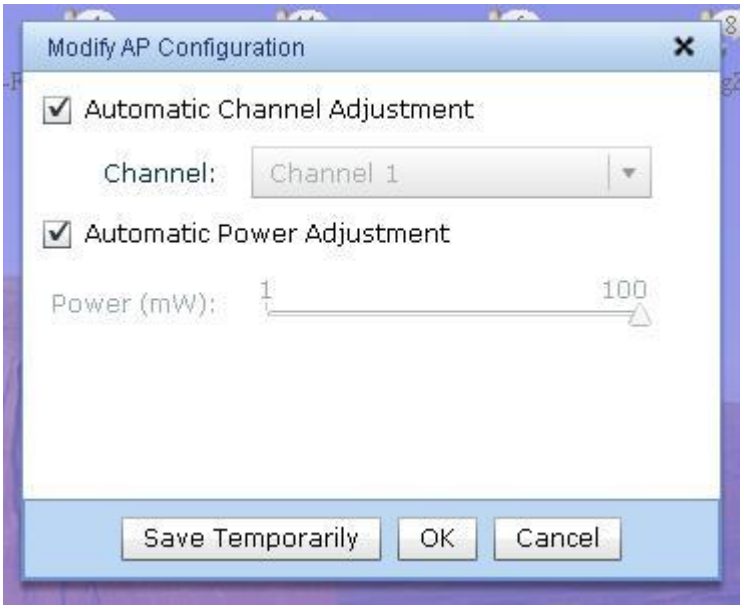


Figure 7.52. Configuring AP Channel and Power

View Conflict APs

Click the red area to view the conflict APs when the heat map is in the view of Channel Interference coverage, as shown in the following figure:

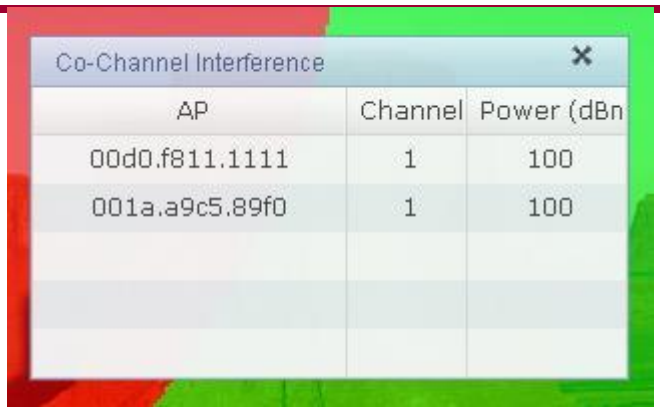


Figure 7.53. Conflict APs

Set Background Transparency

Click **Background** and select **Transparency** in the menu displayed, as shown in the following figure:

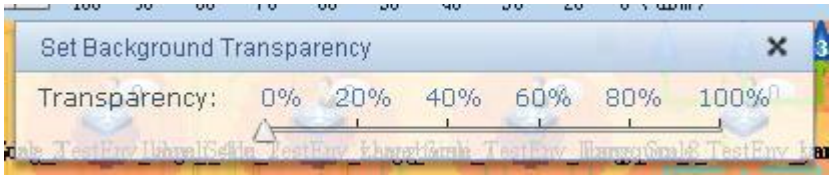


Figure 7.54. Setting Transparency

Draw and Remove Feeders

1. Click **Feeder**, draw a line from the AP to the APD-M, and set the feeder, as shown in the following figure.

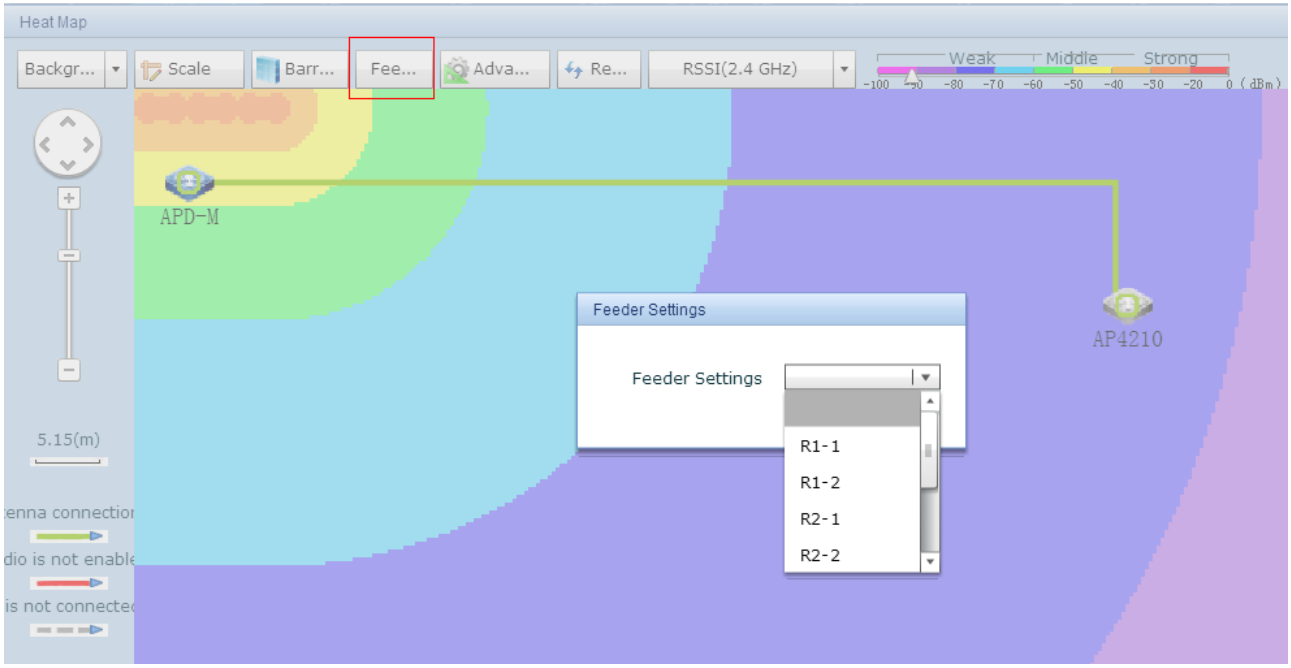


Figure 7.55. Drawing a Feeder

2. Select and right-click the feeder and choose **Remove Feeder** from the menu, as shown in the following figure.

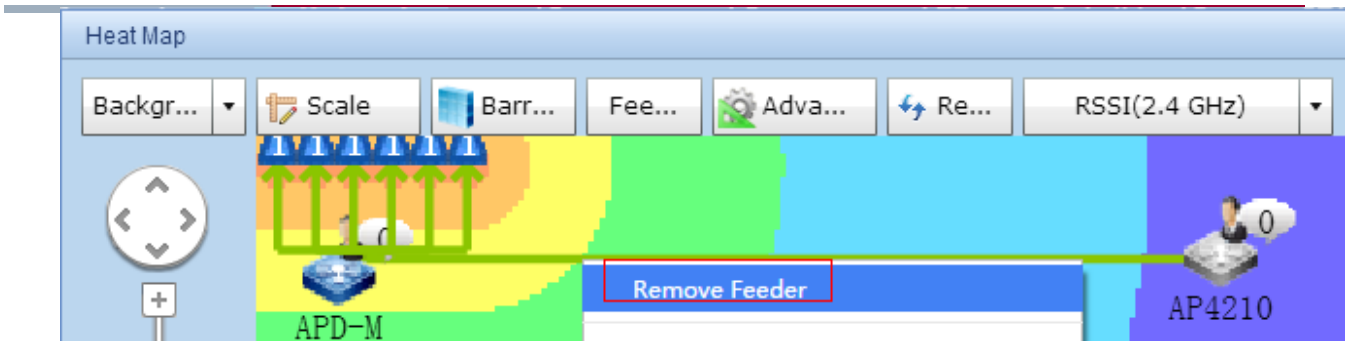


Figure 7.56. Removing a Feeder

Connect Feeders to Satellite APs Automatically

After the hotspot is associated with satellite APs, feeders are automatically connected between the satellite APs and master AP.

Export Heat Map

14) Click **Background** and select **Save As** in the menu displayed, as shown in the following figure:

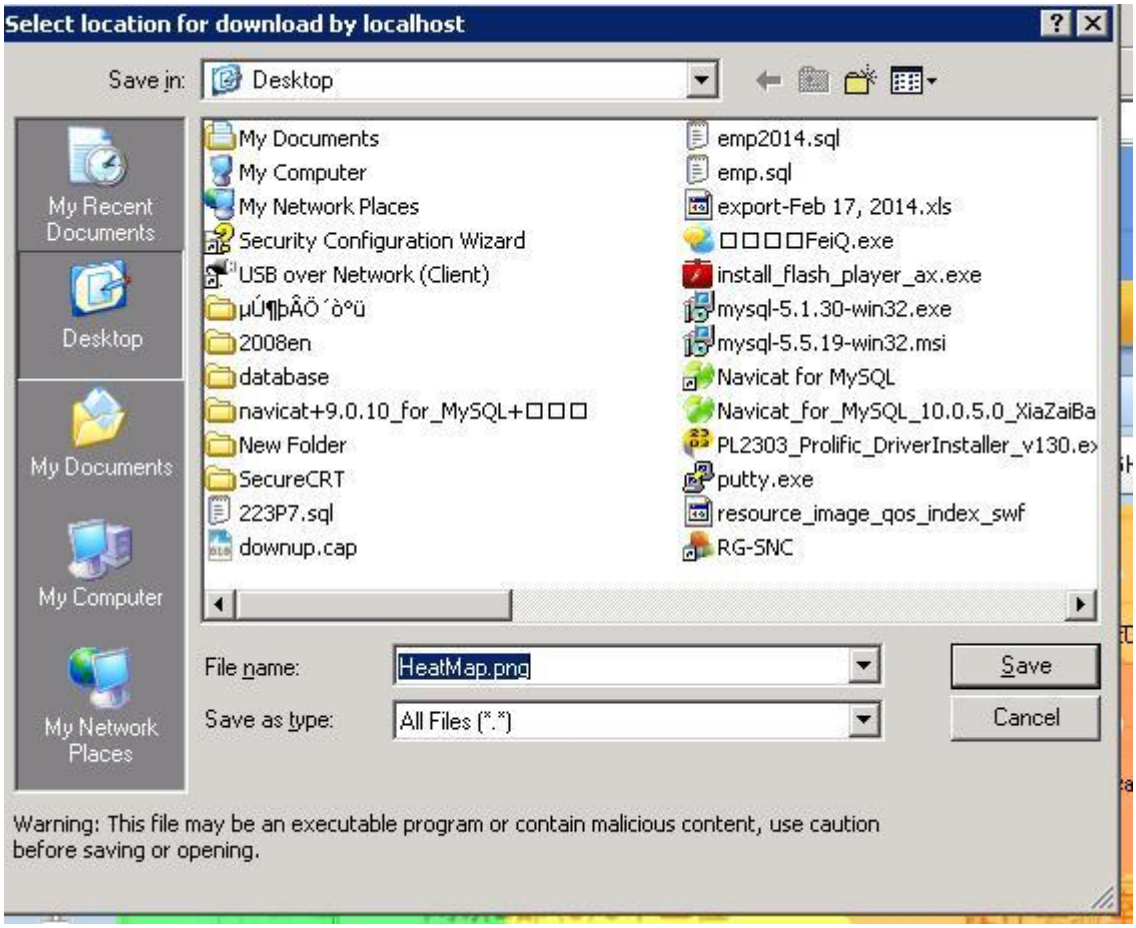


Figure 7.57. Exporting Heat Map

Advanced Settings

15) Click **Advanced**. Fill in the AP height and select the environment type, as shown in the following figure:

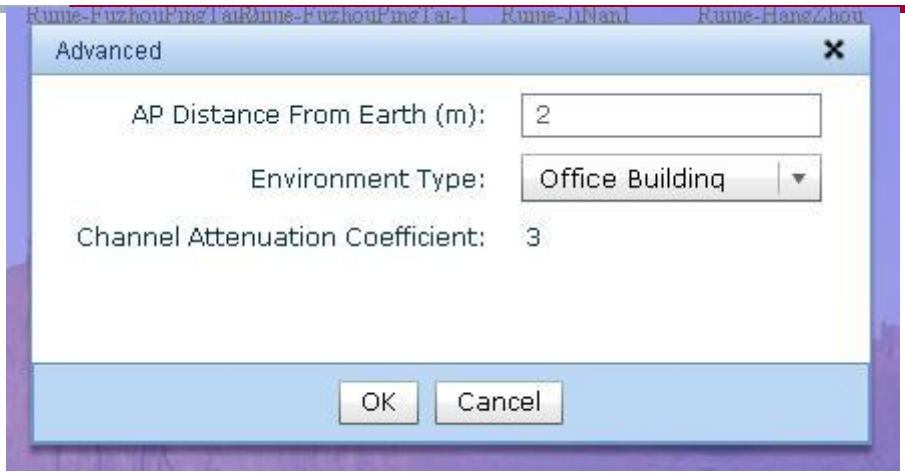


Figure 7.58. Advanced Settings

Click **OK**, and the system returns to the **Heat Map** page and refreshes the page.

Help

Click **?** at the right upper corner, and the **Help** dialog box is displayed, as shown in the following figure:

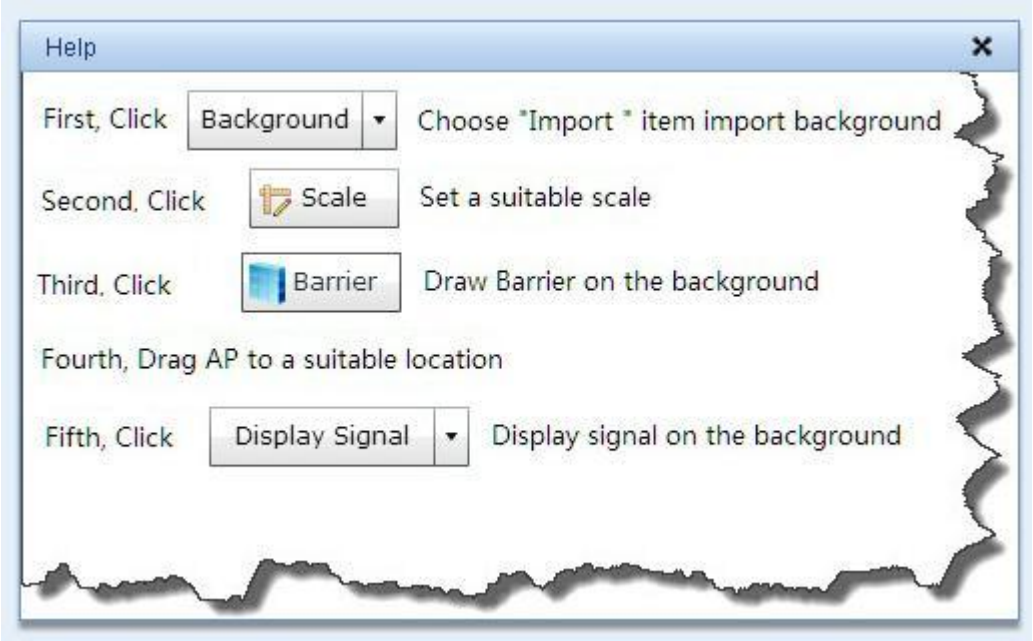


Figure 7.59. Instruction

8.2.6. Configure AP Modes

This function enables you to configure AP working mode and containment mode on the hotspot page.

Configure AP Working Mode and Containment Mode

16) Right-click on the **Hotspot Navigation** menu, and click **Rogue AP Configuration Wizard** on the menu displayed, as shown in the following figure:

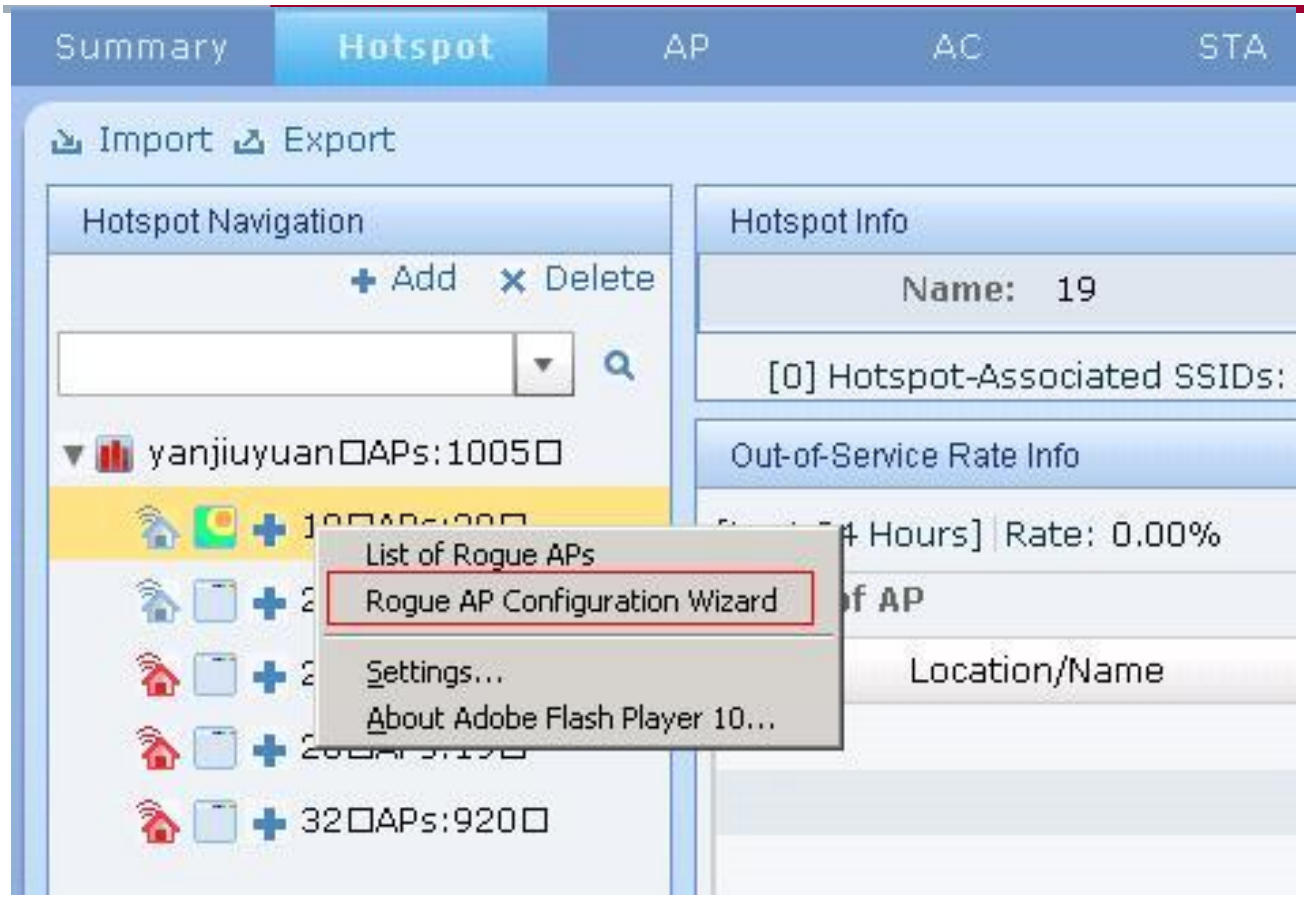


Figure 7.60. Rogue AP Configuration Wizard in Hotspot Navigation

Select **Simple Configuration Mode** or **User Configuration Mode** and click **Next**, as shown in the following figure:

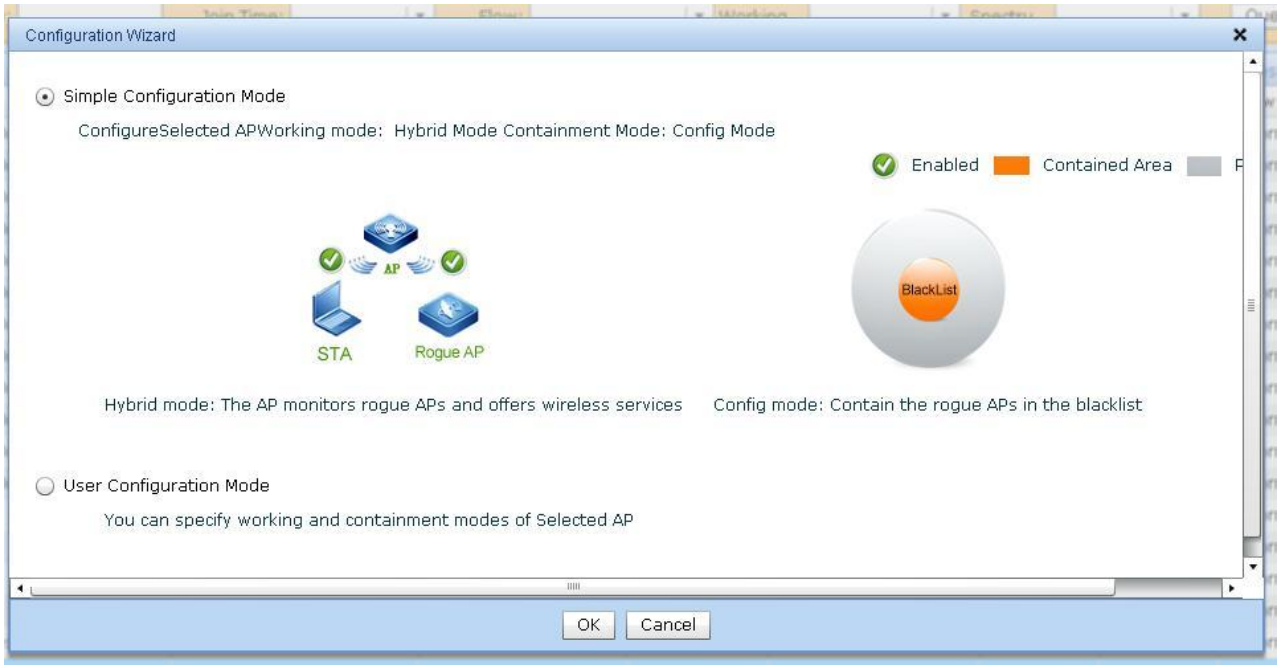


Figure 7.61. Configuration Wizard

If you have selected **User Configuration Mode**, the **Select AP Working Mode** page is displayed, as shown in the following figure:

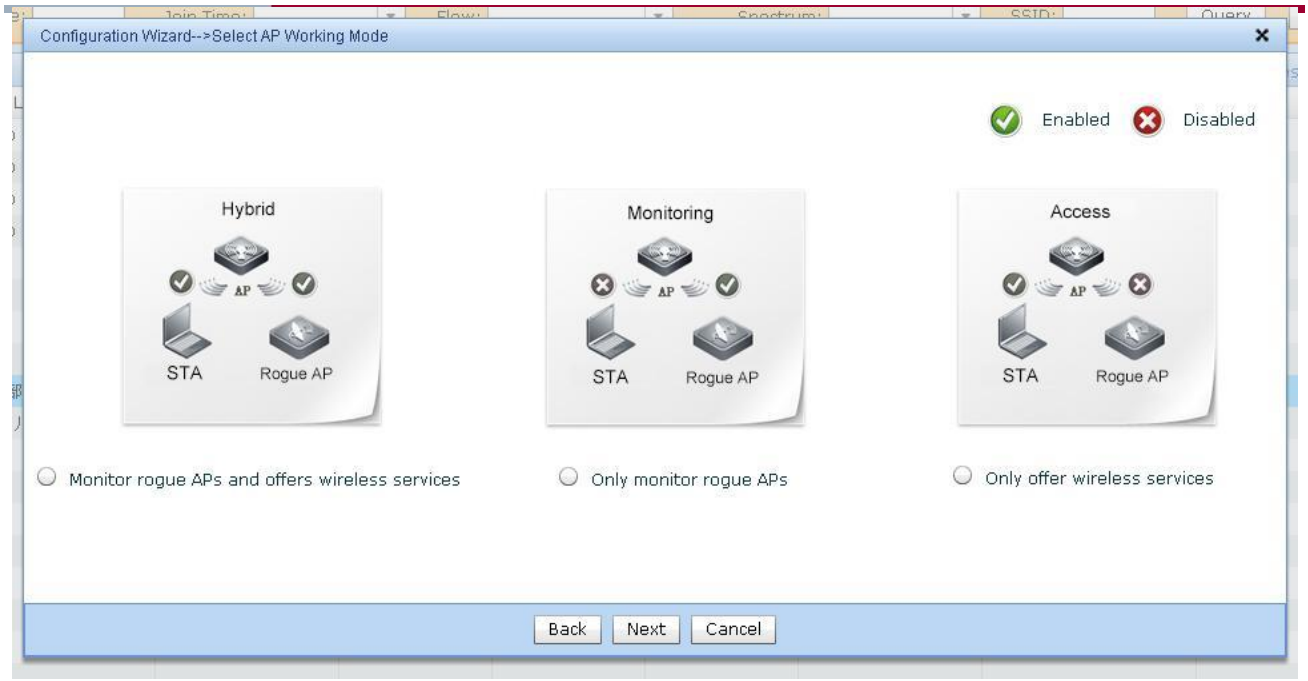


Figure 7.62. Configuring AP Working Mode

Click **Next**, and the **Select AP Containment Mode** page is displayed. You can select one or several modes, as shown in the following figure:

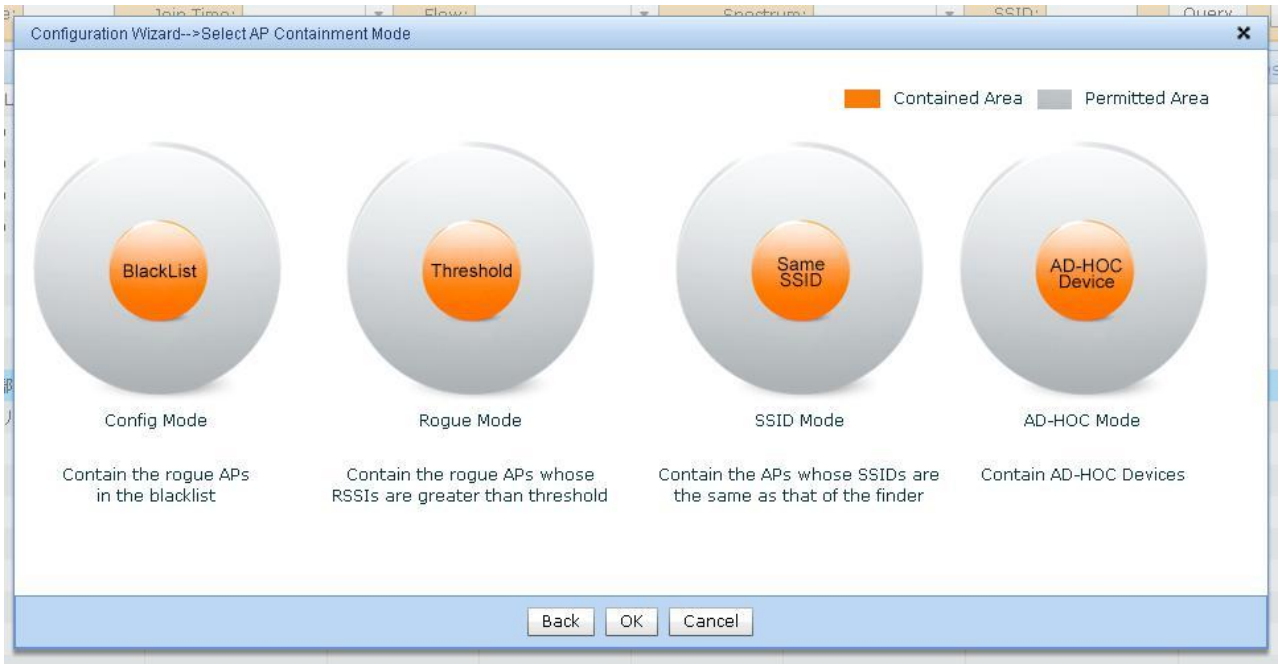


Figure 7.63. Configuring AP Containment Mode

After the configuration is complete, the system returns to the **Rogue AP List** page.

7.3. AP

Major Functions

- Query AP
- AP Operation
- AP Details
- RRM
- AP Radio-on/Radio-off Task
- AP Connectivity Test Task

7.3.1. Query AP

This function enables you to query the AP via conditions.

Query AP

17) Query the AP via conditions, as shown in the following figure:

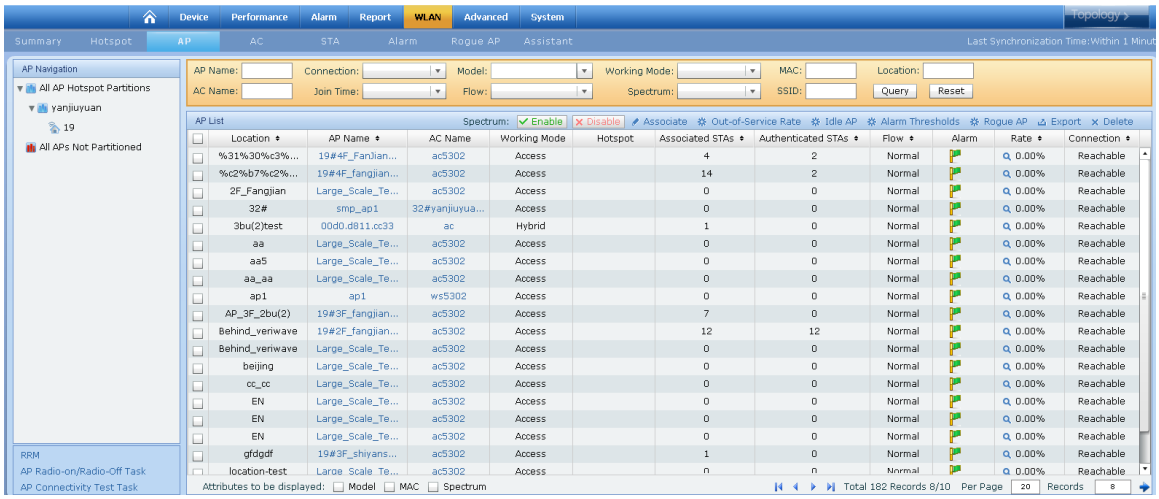


Figure 7.64. Querying AP

Select the attributes to be displayed, including **Device Model**, **MAC Address** and **Spectrum Analysis**, as shown in the following figure:

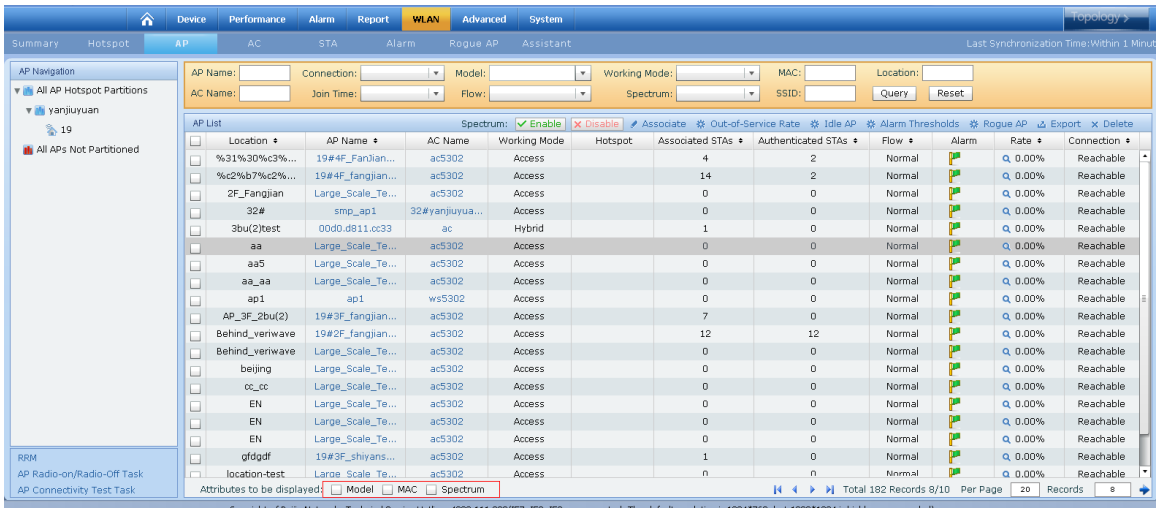


Figure 7.65. Selecting Attributes to be Displayed

7.3.2. AP Operation

This function enables you to perform operations on the AP.

Associate AP to Hotspot

18) Select the AP and click **Associate**, as shown in the following figure:

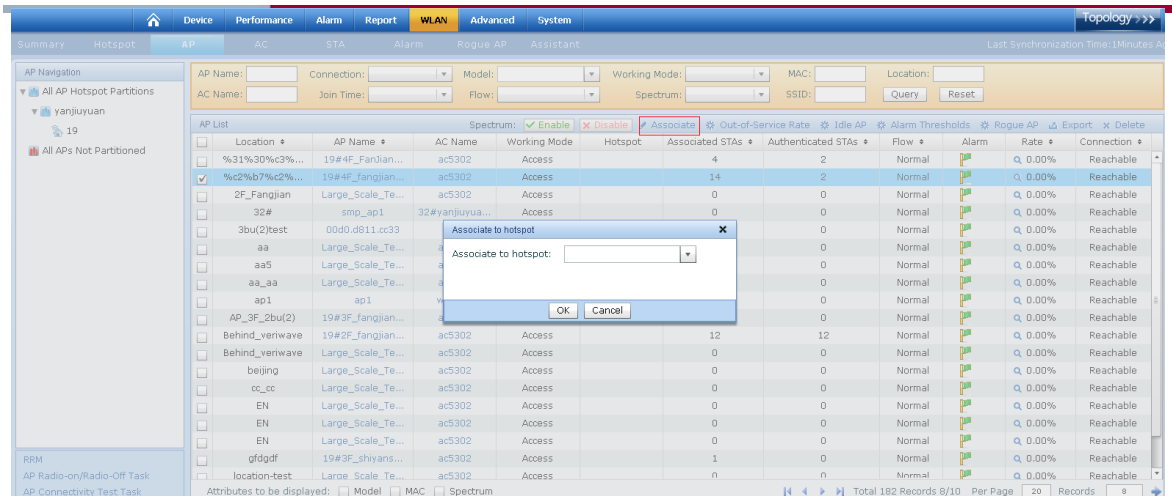


Figure 7.66. Selecting AP

Select a hotspot on the **Associate to Hotspot** page and click **OK**, as shown in the following figure:

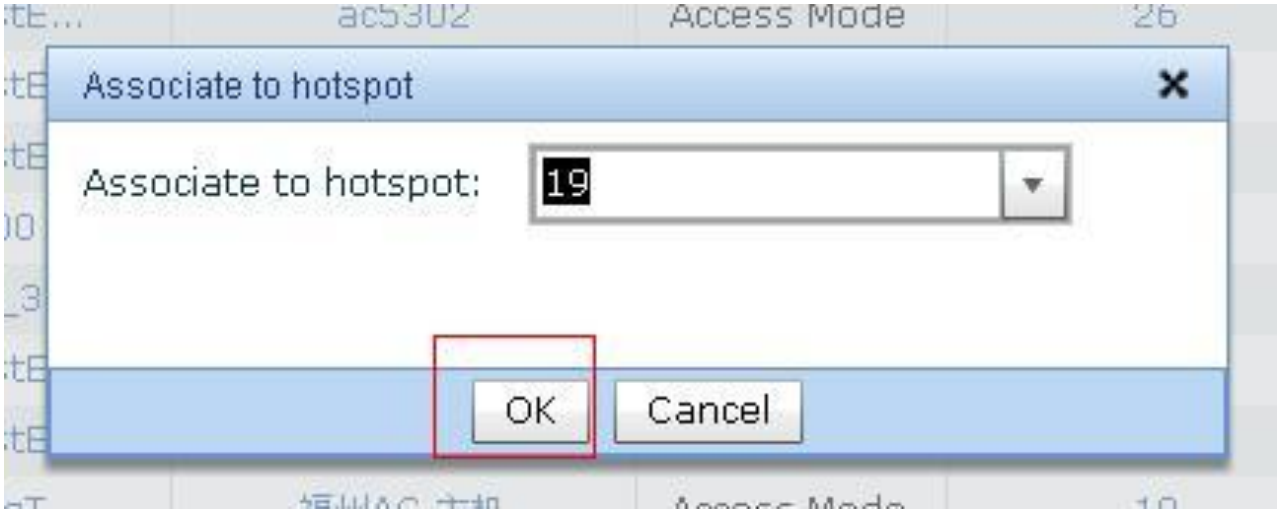


Figure 7.67. Associating AP to Hotspot

Configure Out-of-Service Rate Calculation Time

19) Click **Out-of-Service Rate**, as shown in the following figure:

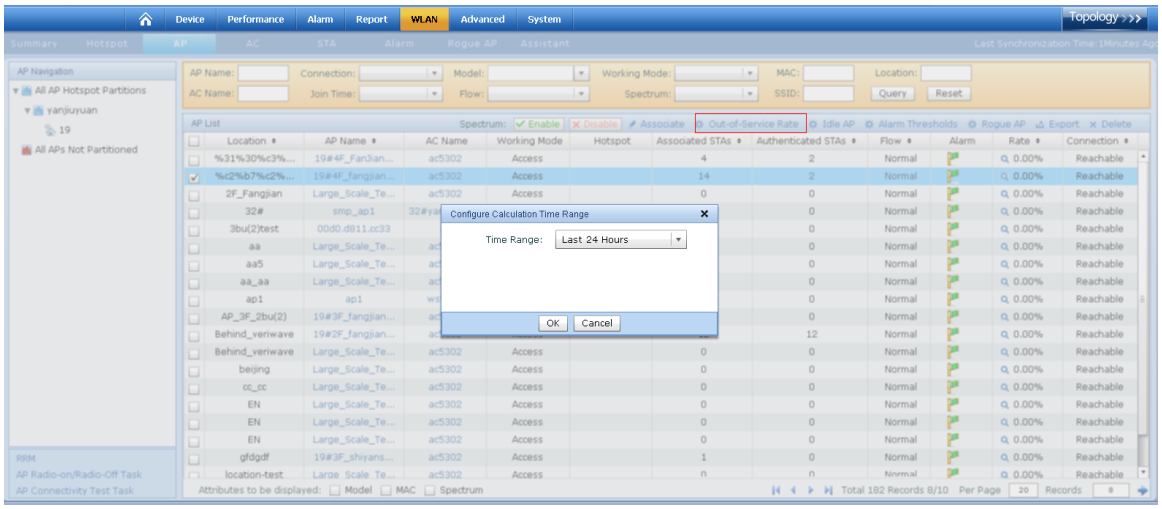


Figure 7.68. Hotspot Statistics

Select the calculation time range(24 hours by default), as shown in the following figure:

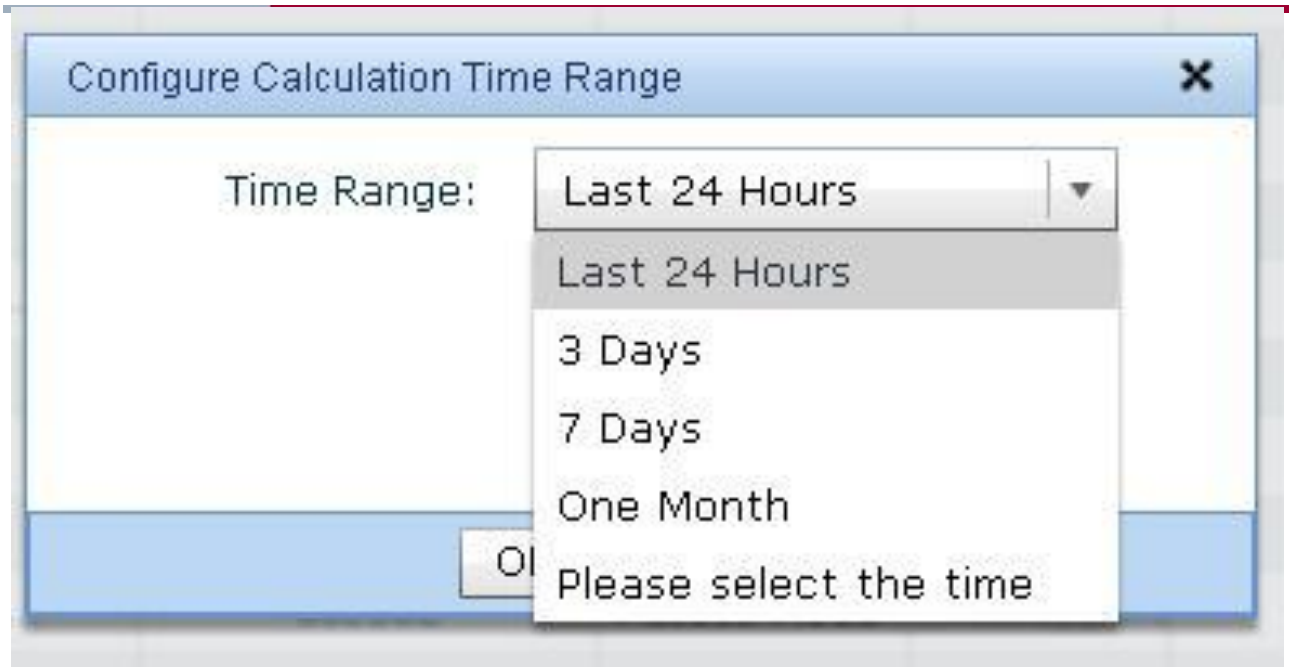


Figure 7.69. Select Calculation Time

Click **OK**, and the system returns to the **AP List** page.

Configure Idle AP Definition

20) Select the AP and click **Idle AP Definitions**, as shown in the following figure:

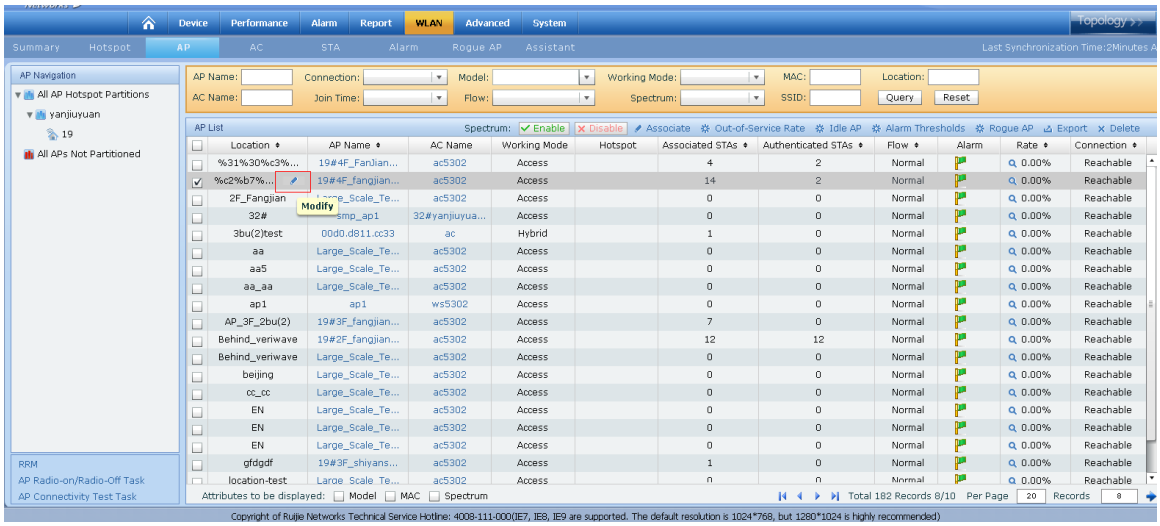


Figure 7.70. Selecting AP

Configure parameters for the idle AP, as shown in the following figure:

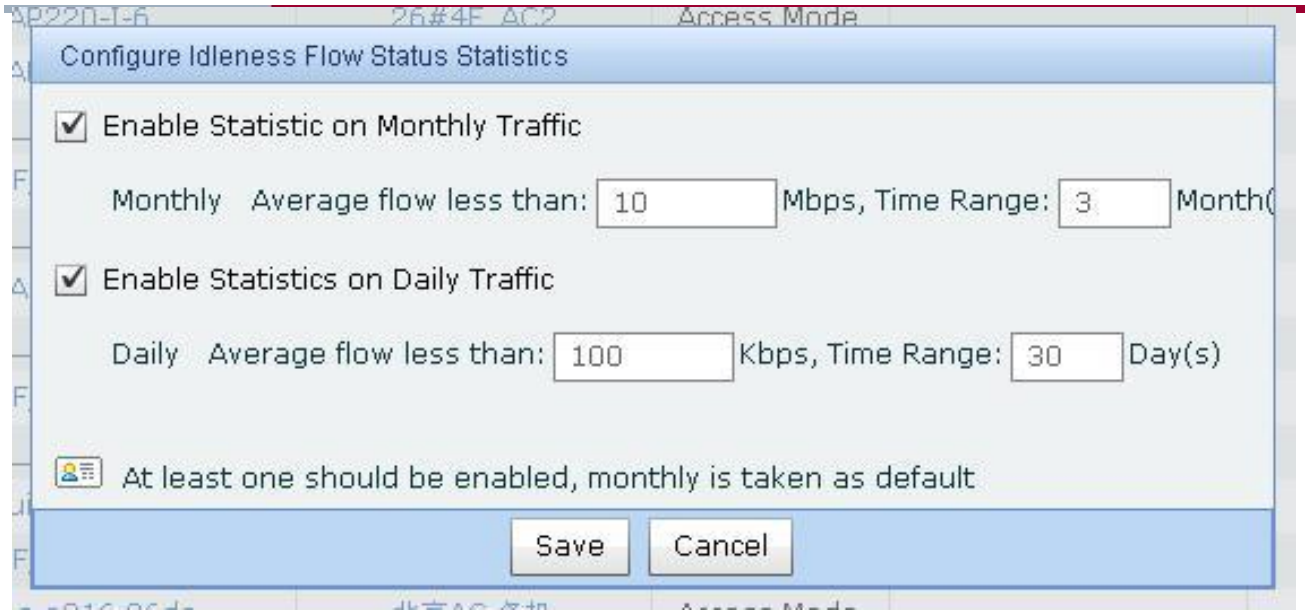


Figure 7.71. Configuring Idle AP Definition

Click **Save**, and the system returns to the **AP List** page.

Configure Alarm Threshold in Batches

21) Select the AP and click **Alarm Thresholds**, as shown in the following figure:

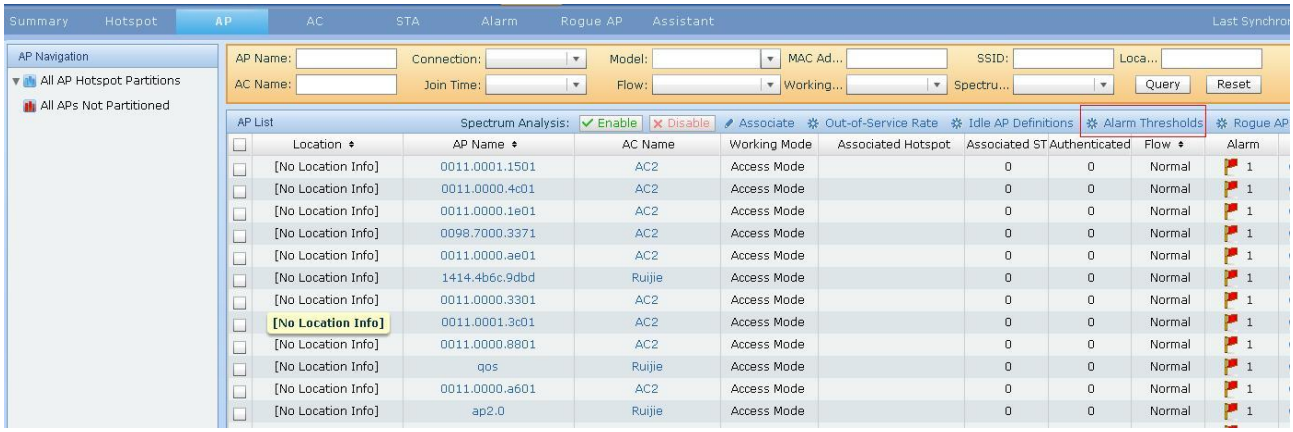


Figure 7.72. Selecting AP

Configure the alarm threshold parameters, as shown in the following figure:

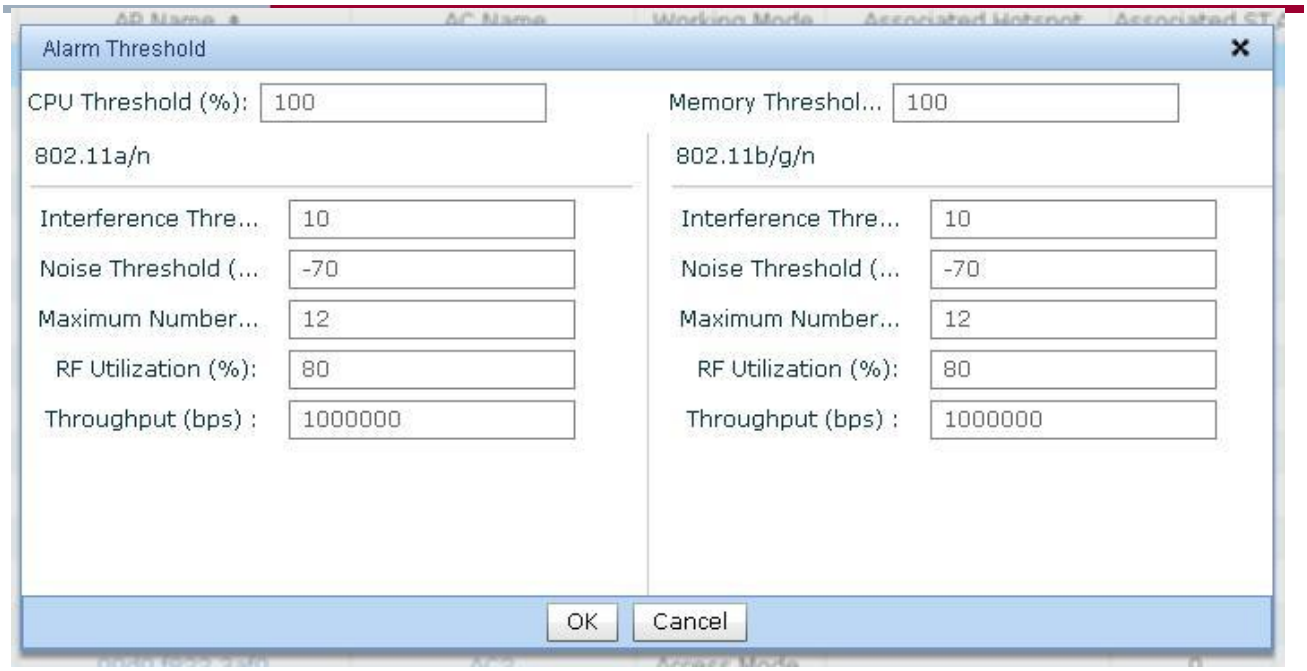


Figure 7.73. Configuring Alarm Threshold

Click **OK**, and the system returns to the **AP List** page.

Export Query Result

22) Enter the query condition and click **Query**, as shown in the following figure:

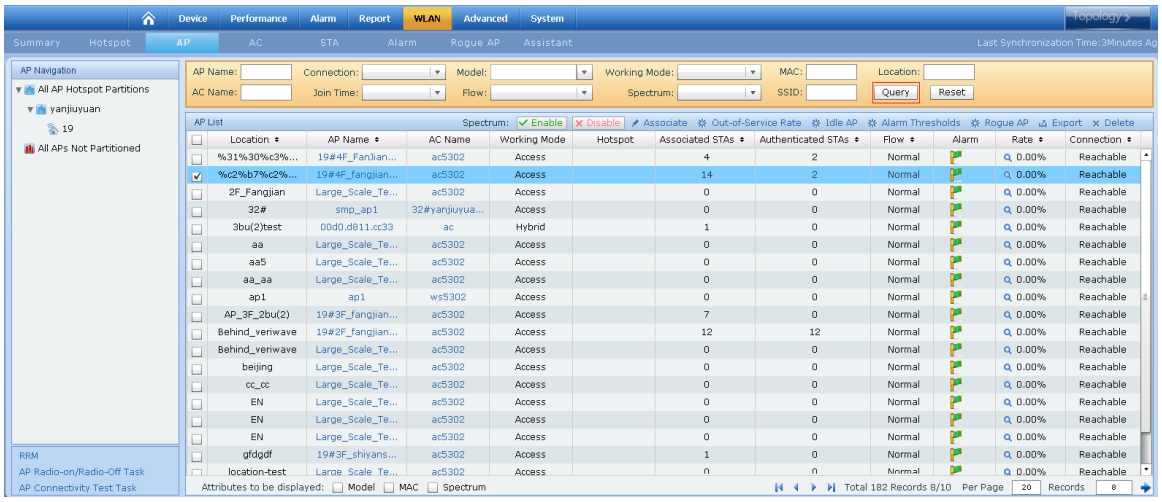


Figure 7.74. Querying AP

Click **Export Results**, as shown in the following figure:

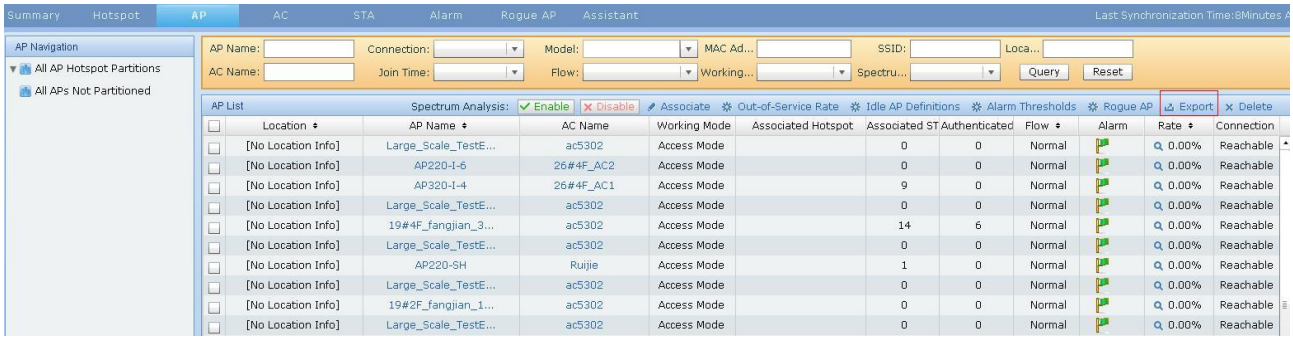


Figure 7.75. Exporting Query Results

Select the save directory. Click **Save**, and the system returns to the **AP List** page.

Delete AP

23) Select the AP and click **Delete**, as shown in the following figure:

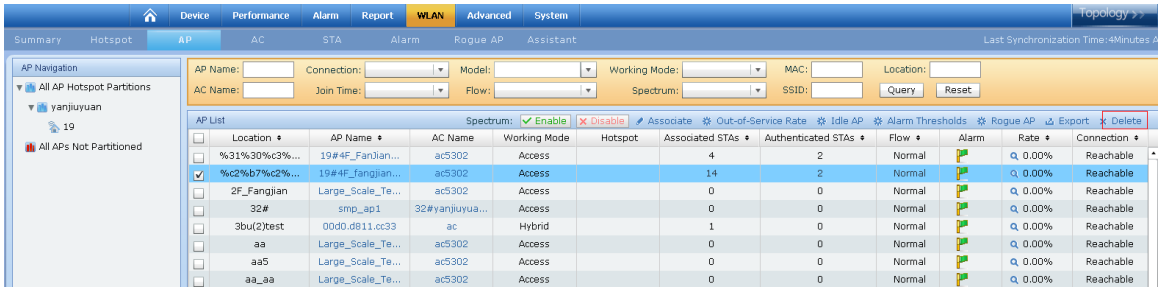


Figure 7.76. Deleting AP

After the AP is deleted, the system refreshes the **AP List** page.

Modify AP Location

24) Move the cursor to the location, and the **Modify** item is displayed. Click **Modify**, as shown in the following figure:

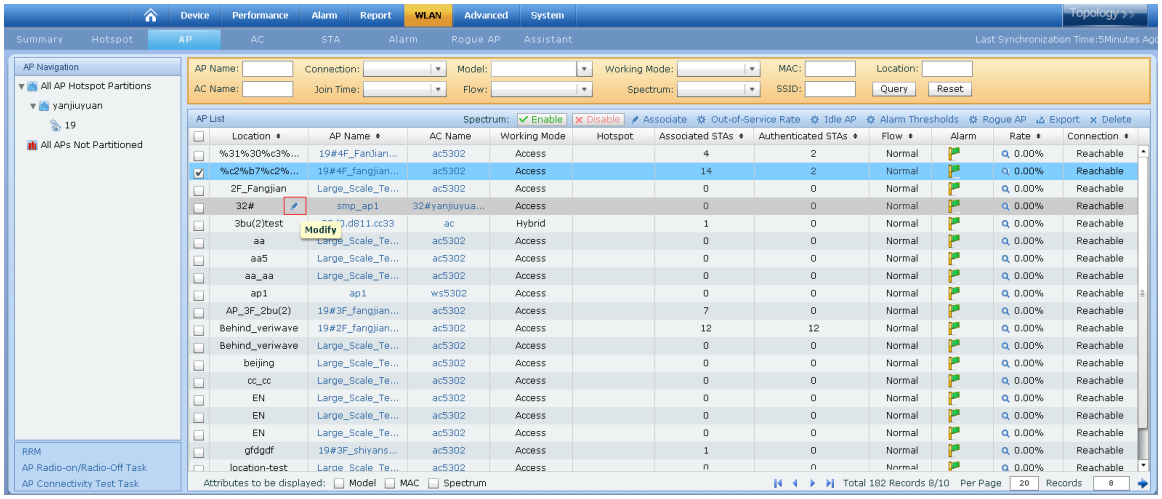


Figure 7.77. Modifying AP Location

Configure the AP location, as shown in the following figure:

Figure 7.78. Configuring AP location

Click **Save**, and the system returns to the **AP List** page.

Modify AP Name

25) Move the cursor to the AP name, and the **Modify** item is displayed. Click **Modify**, as shown in the following figure:

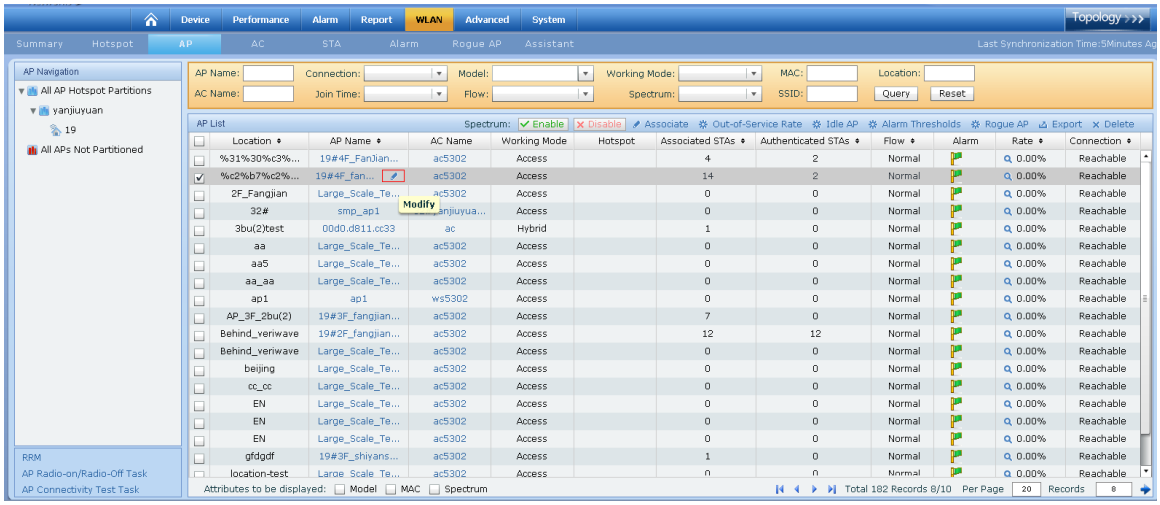


Figure 7.79. Modifying AP Name

Configure the AP Name, as shown in the following figure:

Figure 7.80. Configuring AP Name

Click **Save**, and the system returns to the **AP List** page.

7.3.3. AP Details

The AP Details page displays detailed AP information, including Synchronize AP, Alarm Threshold, Rogue AP, Rogue APs Statistics and Spectrum Analysis operations.

Display AP Details

26) Click the AP name, as shown in the following figure:

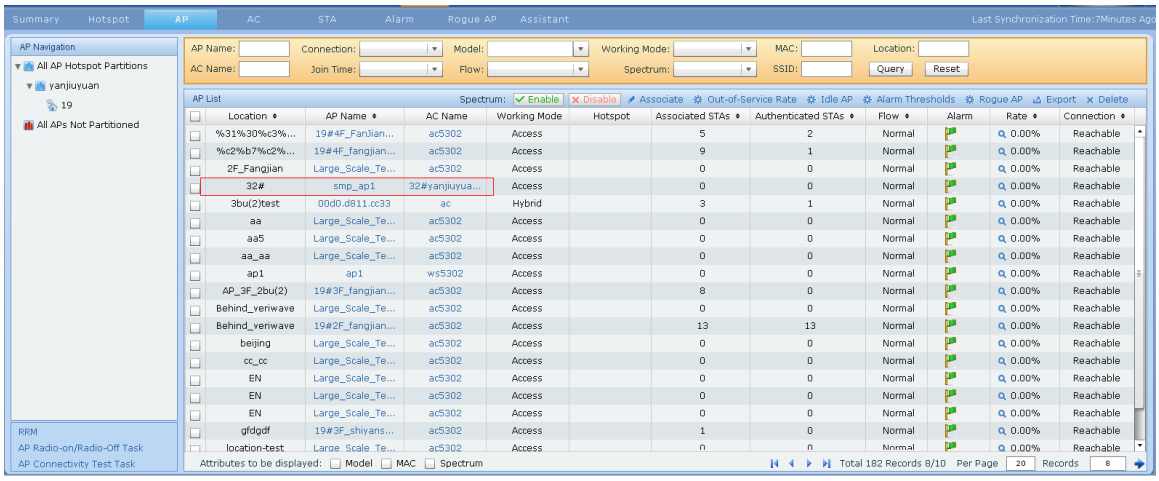


Figure 7.81. Clicking AP Name

View the AP details, as shown in the following figure:

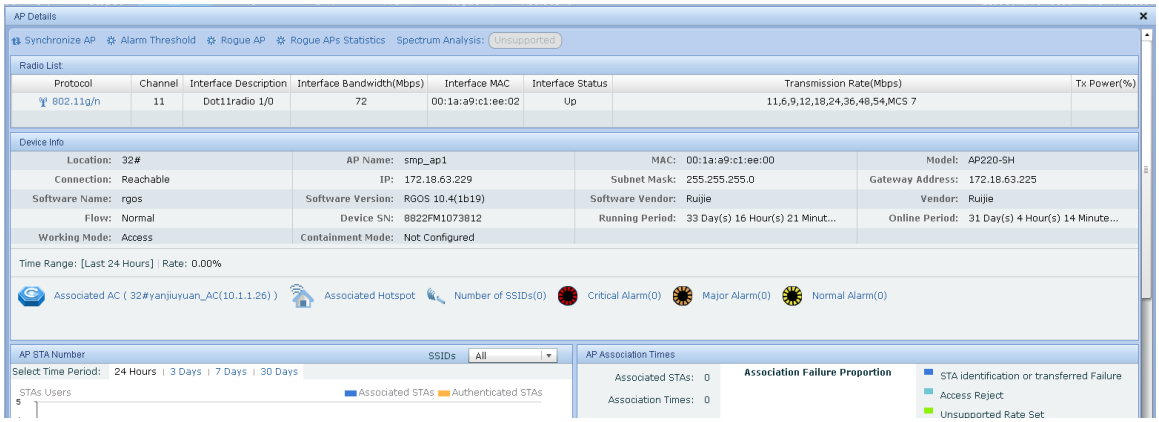


Figure 7.82. AP Details

Synchronize AP Information

27) Click the AP name, as shown in the following figure:

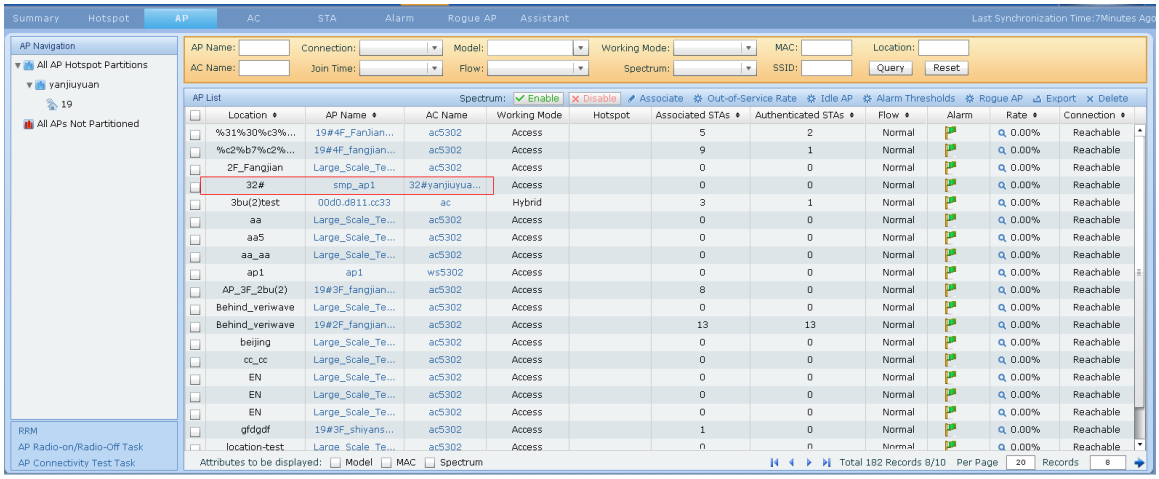


Figure 7.83. Clicking AP name

Click **Synchronize AP**, as shown in the following figure:

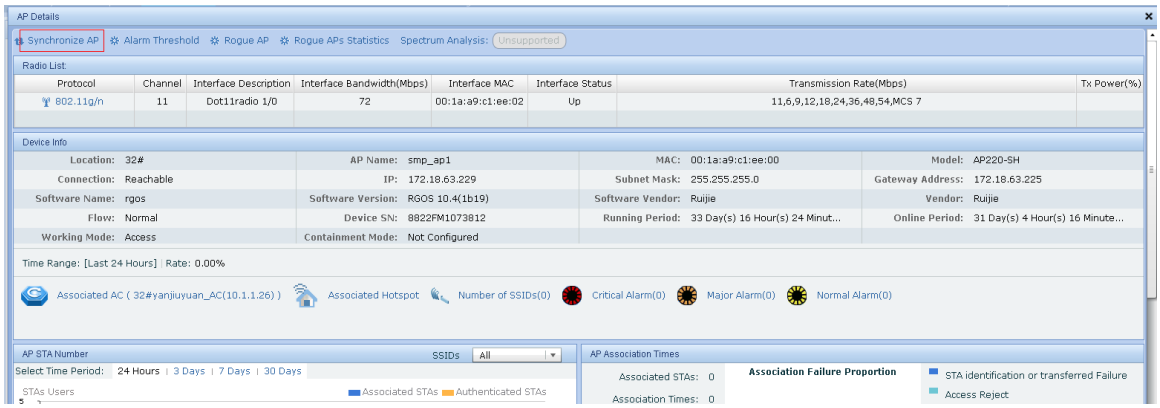


Figure 7.84. Synchronizing AP information

Configure AP Alarm Threshold

28) Click the AP name, as shown in the following figure:

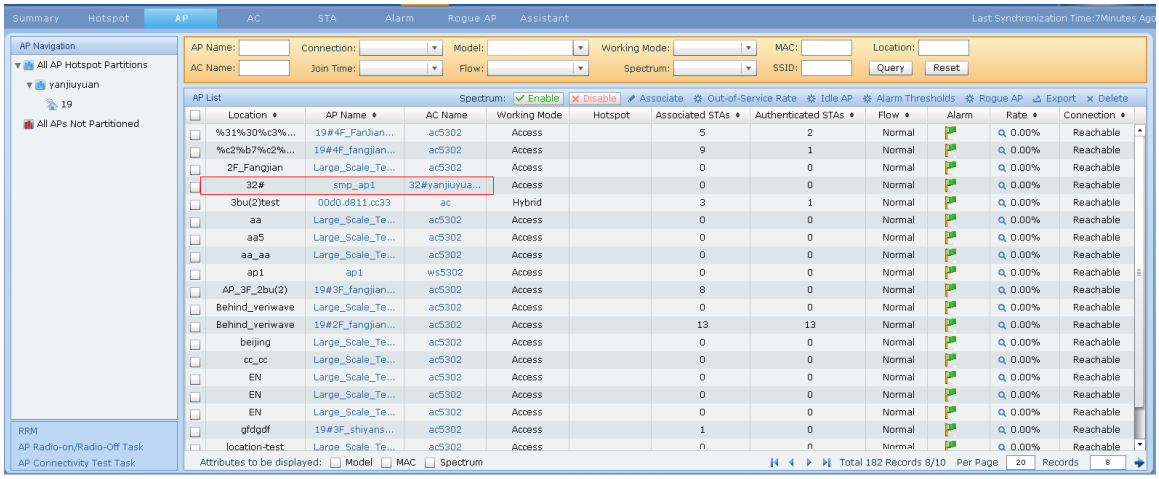


Figure 7.85. Clicking AP Name

Click **Alarm Threshold**, as shown in the following figure:

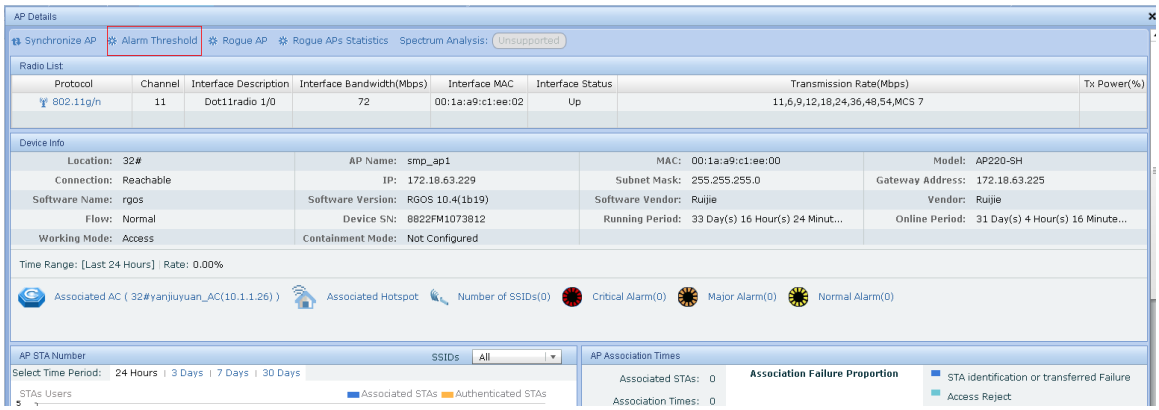


Figure 7.86. Alarm Threshold Configuration

Click **Edit** to configure the alarm threshold parameters, as shown in the following figure:

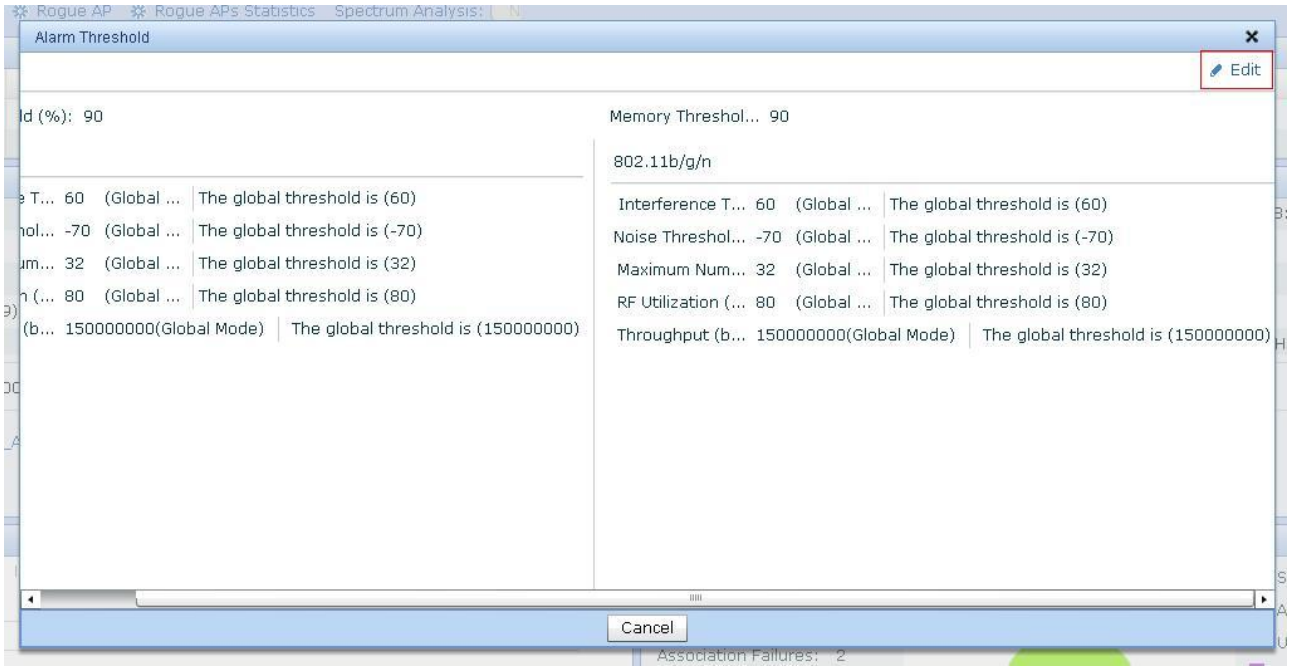


Figure 7.87. Alarm Threshold Configuration

Click **Save**, the system returns to the **AP Details** page.

View Statistics on Channel Occupancy by Rogue APs

29) Click the AP name, as shown in the following figure:

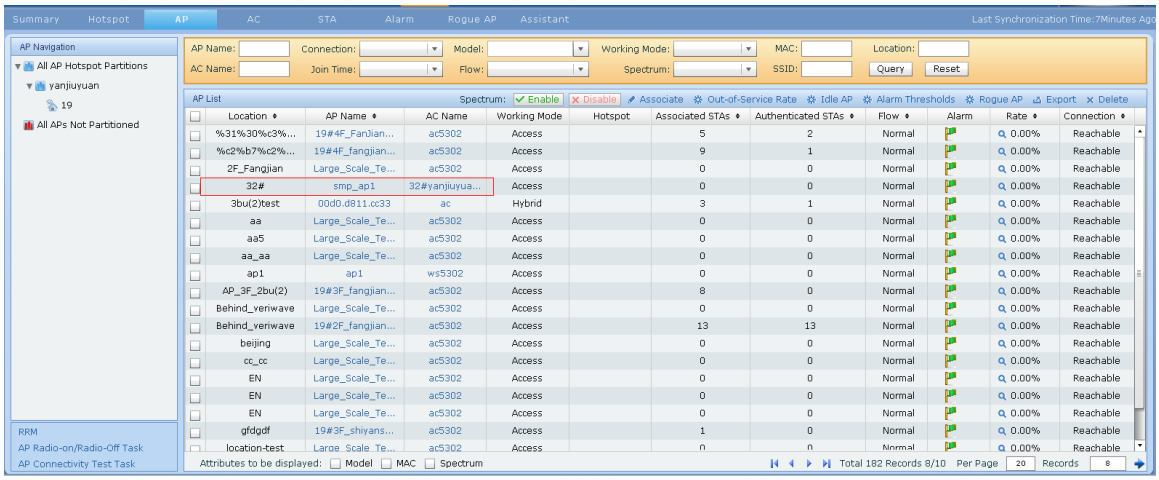


Figure 7.88. Clicking AP Name

Click **Rogue APs Statistics**, as shown in the following figure:

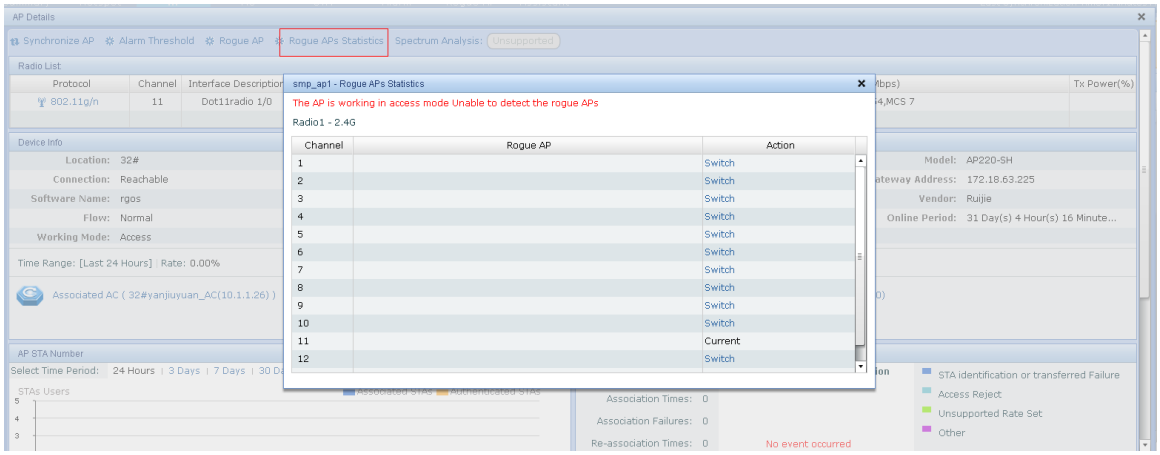


Figure 7.89. Statistics on Channel Occupancy by Rogue APs

If you want to change the working channel, please click **Adjust to This Channel** on the **Rogue APs Statistics** page, as shown in the following figure:

Figure 7.90. Changing Channel

7.3.4. RRM

This function enables you to view RRM statistics of the AP.

Operation Steps

30) Click **RRM** at the bottom left corner on the AP page, as shown in the following figure:

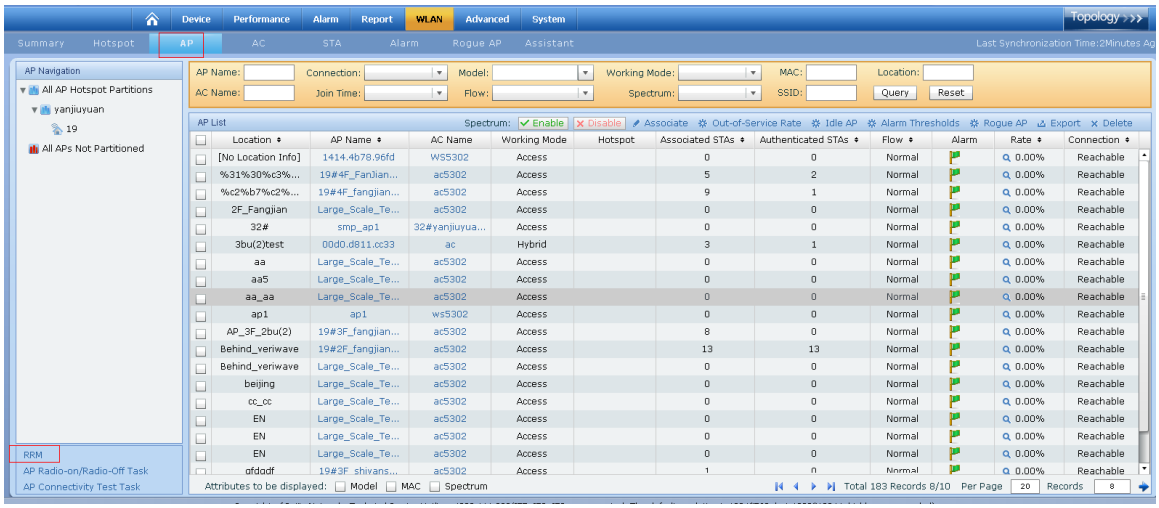


Figure 7.91. RRM

The **RRM Statistics** page is displayed, as shown in the following figure:

Figure 7.92. RRM Statistics

The statistics on channel changes in last 24 hours are displayed, as shown in the following figure:

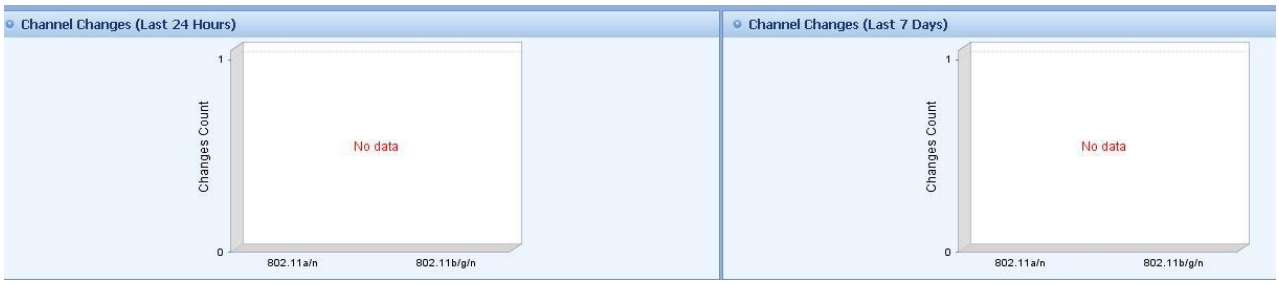


Figure 7.93. Channel Changes(Last 24 Hours)

The statistics on changing APs are displayed, as shown in the following figure:

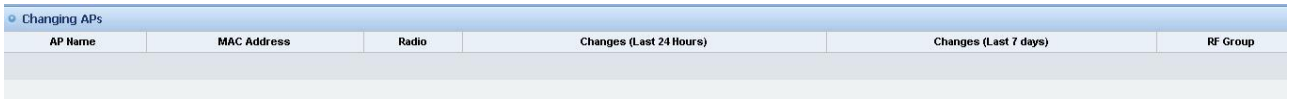


Figure 7.94. Statistics on changing APs

The statistics on APs working at the maximum power are displayed, as shown in the following figure:

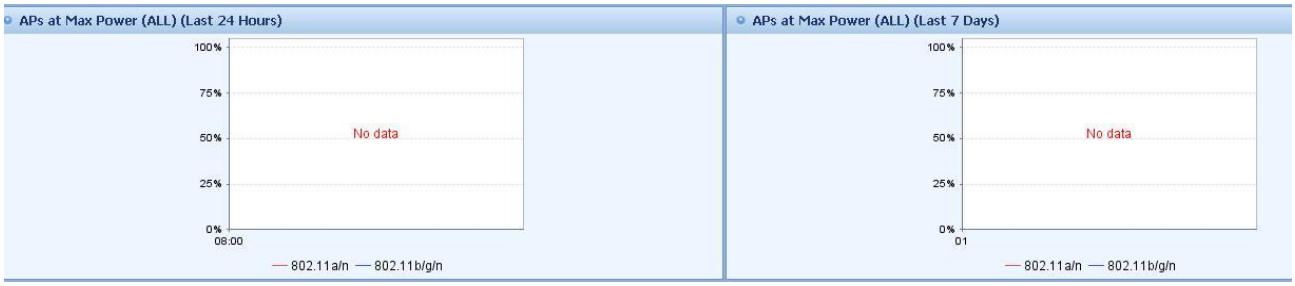


Figure 7.95. APs at Max Power

7.3.5. AP Radio-on/Radio-off Task

This function enables you to turn on/off Radio and restart APs in batches either manually or as scheduled. You can also view the task result.

AP Radio-on/Radio-off Task

1) Click **AP Radio-on/Radio-off Task** at the bottom left corner on the AP page, as shown in the following figure:

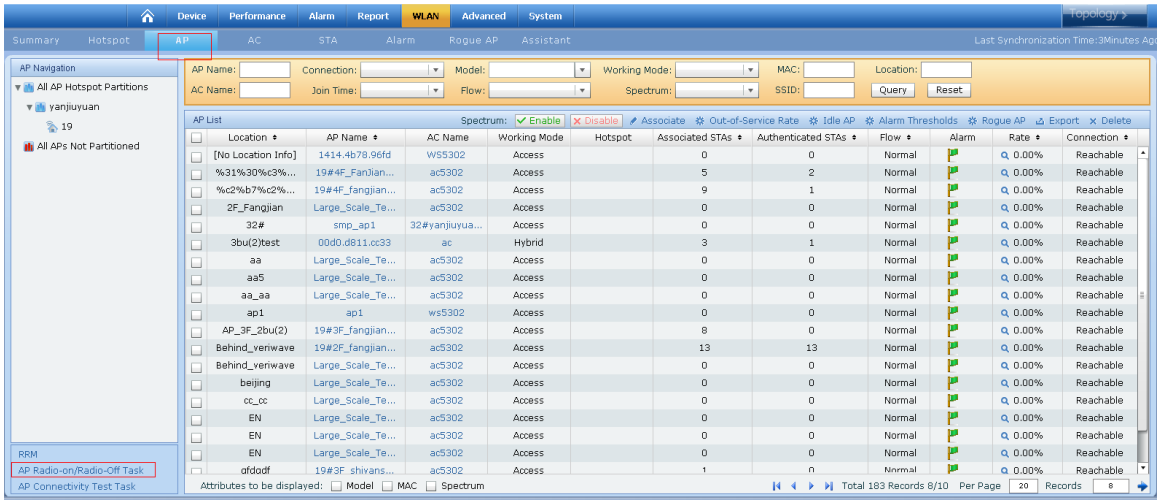


Figure 7.96. AP Radio-on/Radio-off Task

2) Click **Add** to add a Radio-on/Radio-off task, as shown in the following figure:

Figure 7.97. Add AP Radio-on/Radio-off Task

3) Configure the basic information of the plan and click **Next**, as shown in the following figure:

Figure 7.98. Configuring Basic Information

4) Select devices from existing plans or the device list and click **Next**, as shown in the following figure.

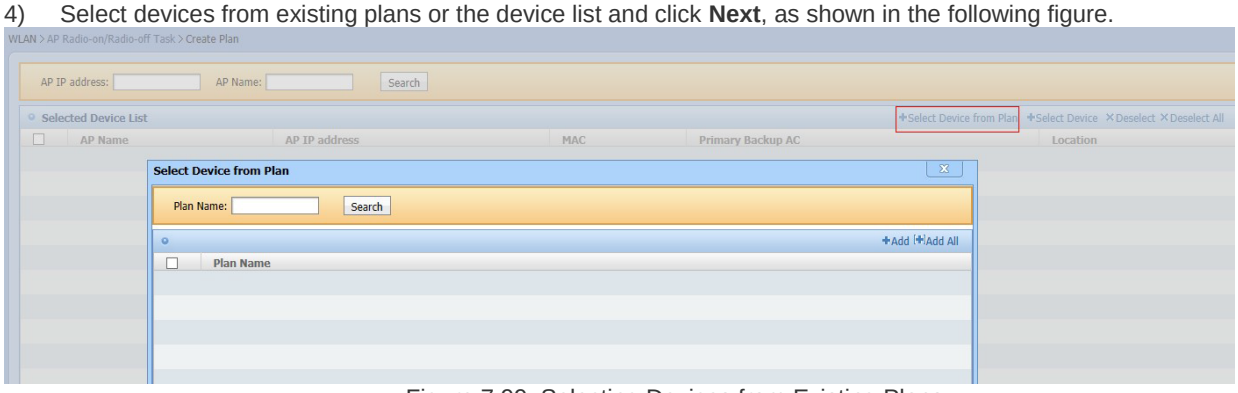


Figure 7.99. Selecting Devices from Existing Plans

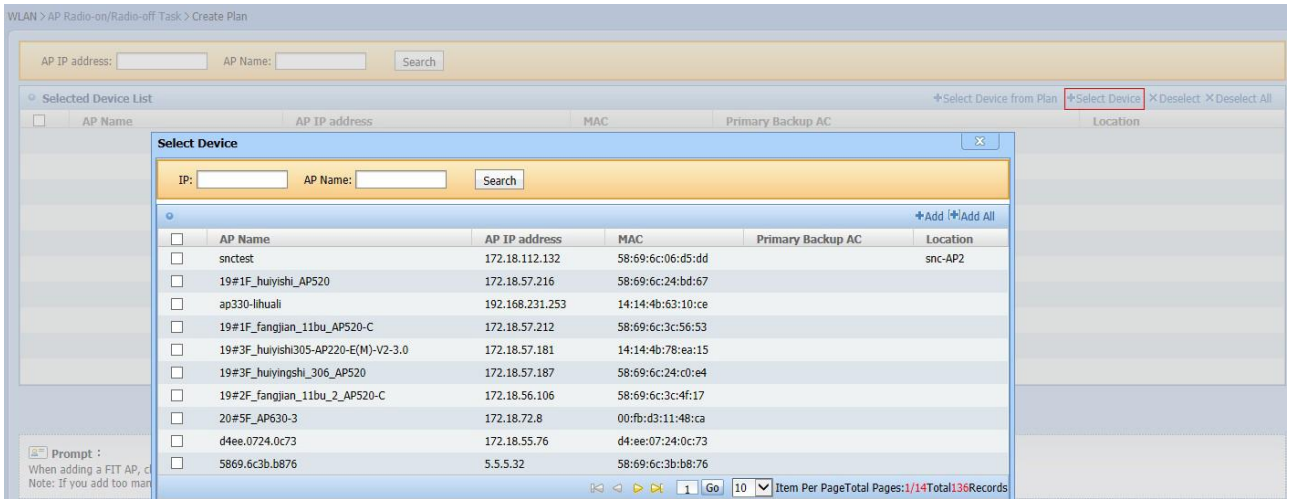


Figure 7.100. Selecting Devices from the Device List

5) Select the operation on AP in batches, as shown in the following figure:

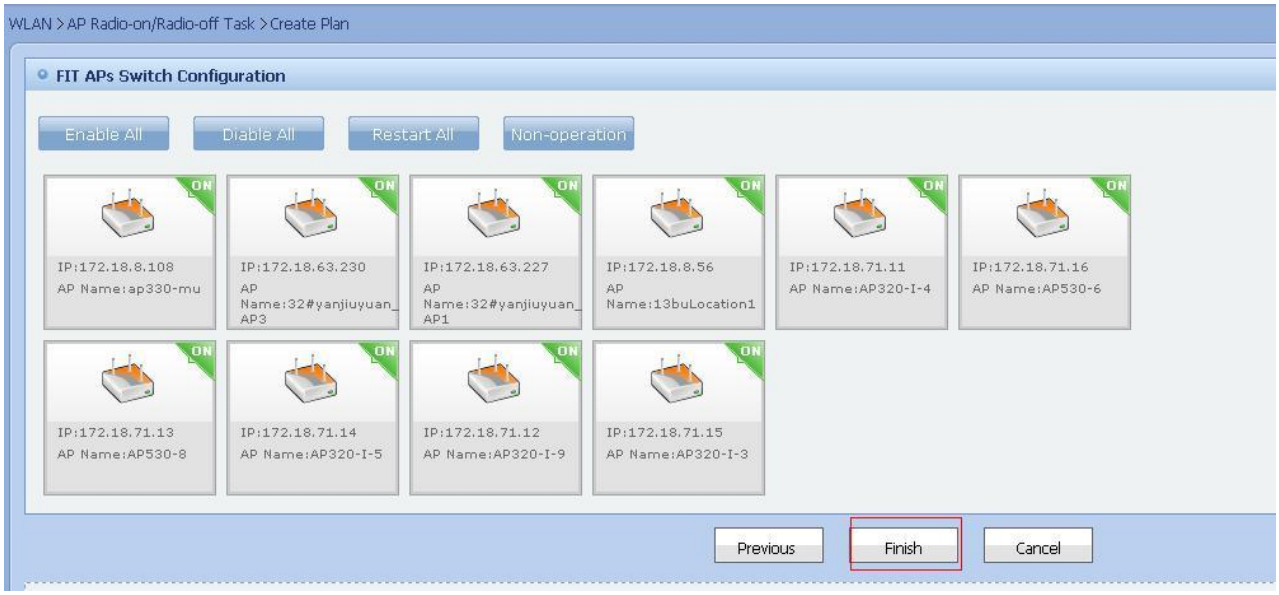


Figure 7.101. Selection Operation

6) Click **Finish**, and the system returns to the AP Radio-on/Radio-off Task list, as shown in the following figure:

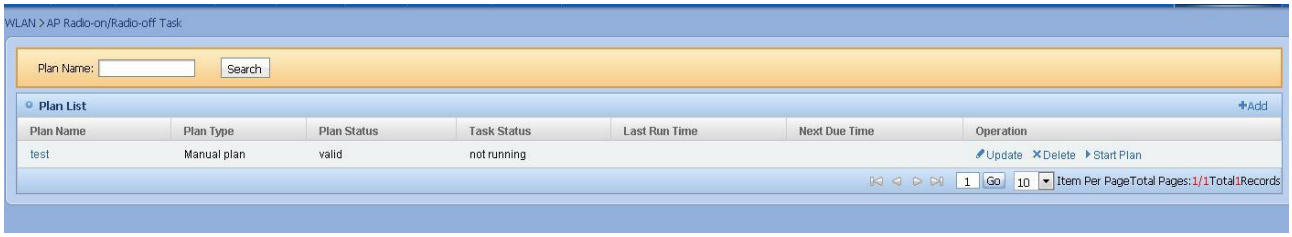


Figure 7.102. Returning to AP Radio-on/Radio-off List

7) Click **Activate**, as shown in the following figure:

Figure 7.103. Activating Plan

8) Click **Enable**, as shown in the following figure:

Figure 7.104. Enabling Plan

9) After the plan is performed, click the plan name to view the result, as shown in the following figure:

Figure 7.105. Viewing Result

10) View the operation logs, as shown in the following figure:

Figure 7.106. Operation Logs

7.3.6. AP Connectivity Test Task

This function enables you to perform the connectivity test on APs in batches either manually or as scheduled and view the test result.

AP Connectivity Test Task

1) Click **AP Connectivity Test Task** at the bottom left corner on the AP page, as shown in the following figure:

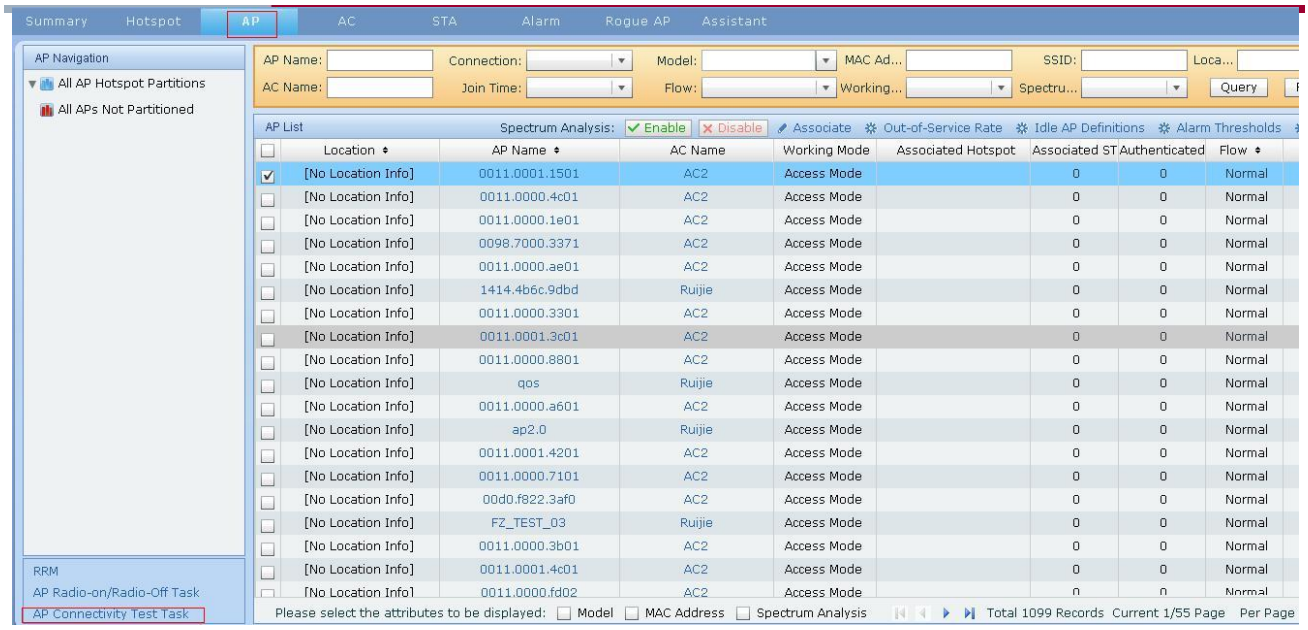


Figure 7.107. AP Connectivity Test Task

2) Click **Add** to add a connectivity test task, as shown in the following figure:

Figure 7.108. Adding Connectivity Test Task

3) Configure the basic configuration of the plan and click **Next**, as shown in the following figure:

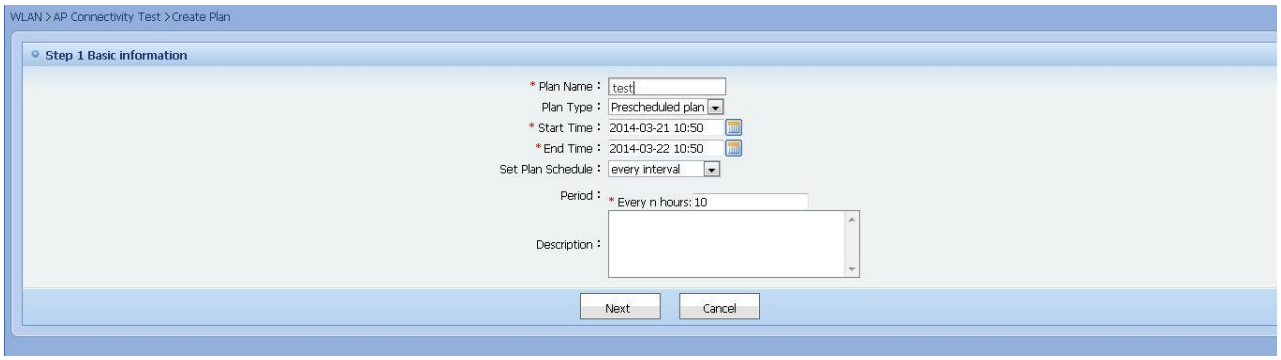


Figure 7.109. Configuring Basic Information

4) Select devices from existing plans or the device list and click **Next**, as shown in the following figure.

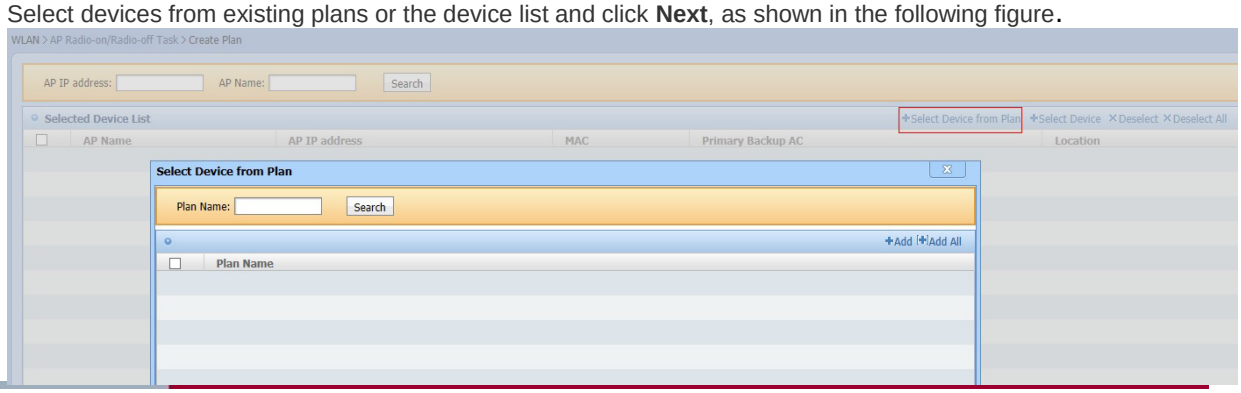


Figure 7.110 Selecting Devices from Existing Plans

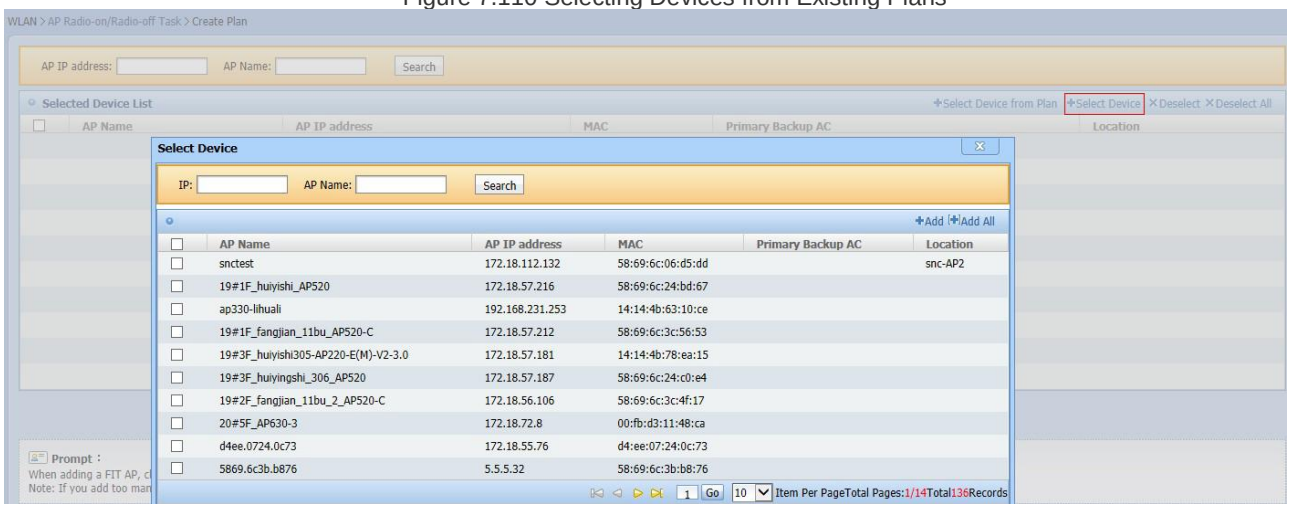


Figure 7.111. Selecting Devices from the Device List

5) Click **Finish**, and the system returns to the **AP Connectivity Test Task** list.

Click **Activate**, as shown in the following figure:

Figure 7.112. Activating Plan

6) After the plan is performed, click the plan name to view the result, as shown in the following figure:

Figure 7.113. Viewing Result

7) View the operation logs, as shown in the following figure:

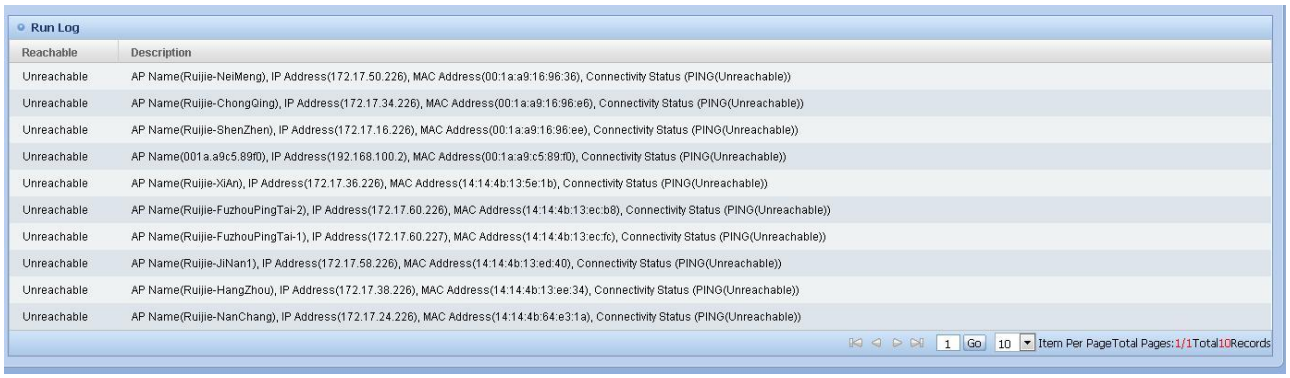


Figure 7.114. Operation Logs

7.3.7. Configure AP Modes

This function enables you to configure AP working mode and containment mode.

Configure AP Working Mode and Containment Mode

31) Click **Rogue AP** on the **AP List** page or **AP Details** page, or right-click on the **Hotspot Navigation** menu and select **Rogue AP Configuration Wizard** on the menu displayed, as shown in the following figure:

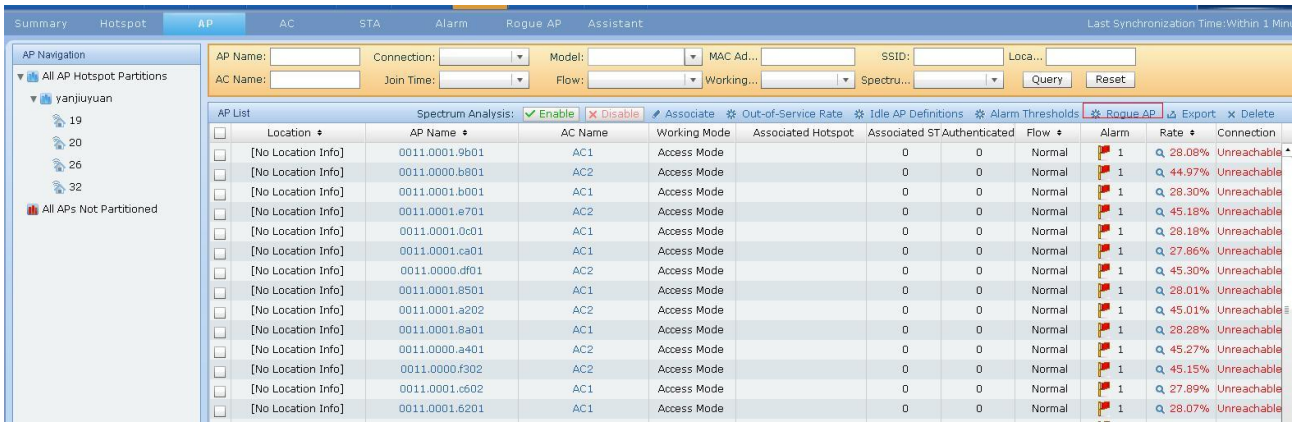


Figure 7.115. Configuring Rogue AP Configuration Wizard on **AP List** Page

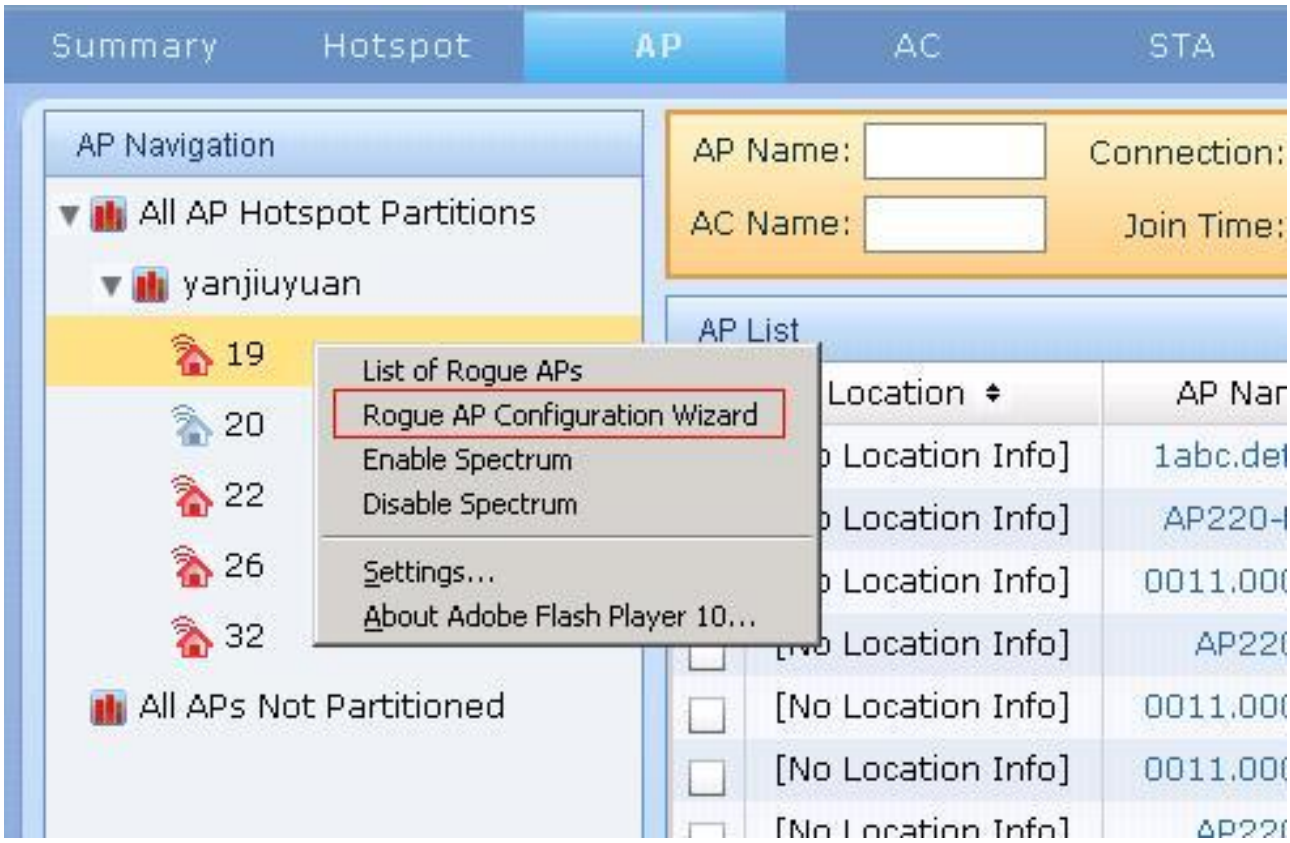


Figure 7.116. Rogue AP Configuration Wizard in **Hotspot Navigation** Menu

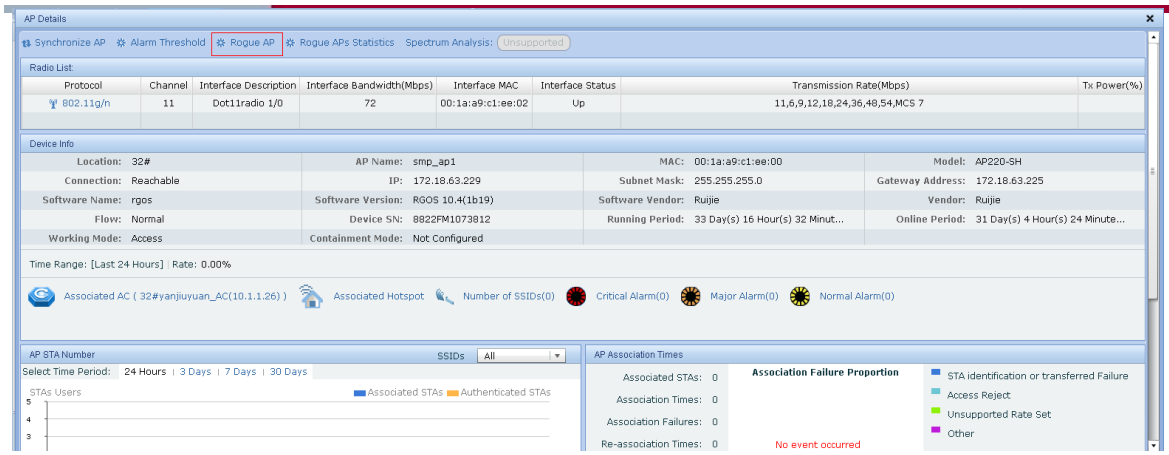


Figure 7.117. Rogue AP Configuration Wizard on **AP Details** Page

Select **Simple Configuration Mode** or **User Configuration Mode** and click **Next**, as shown in the following figure:

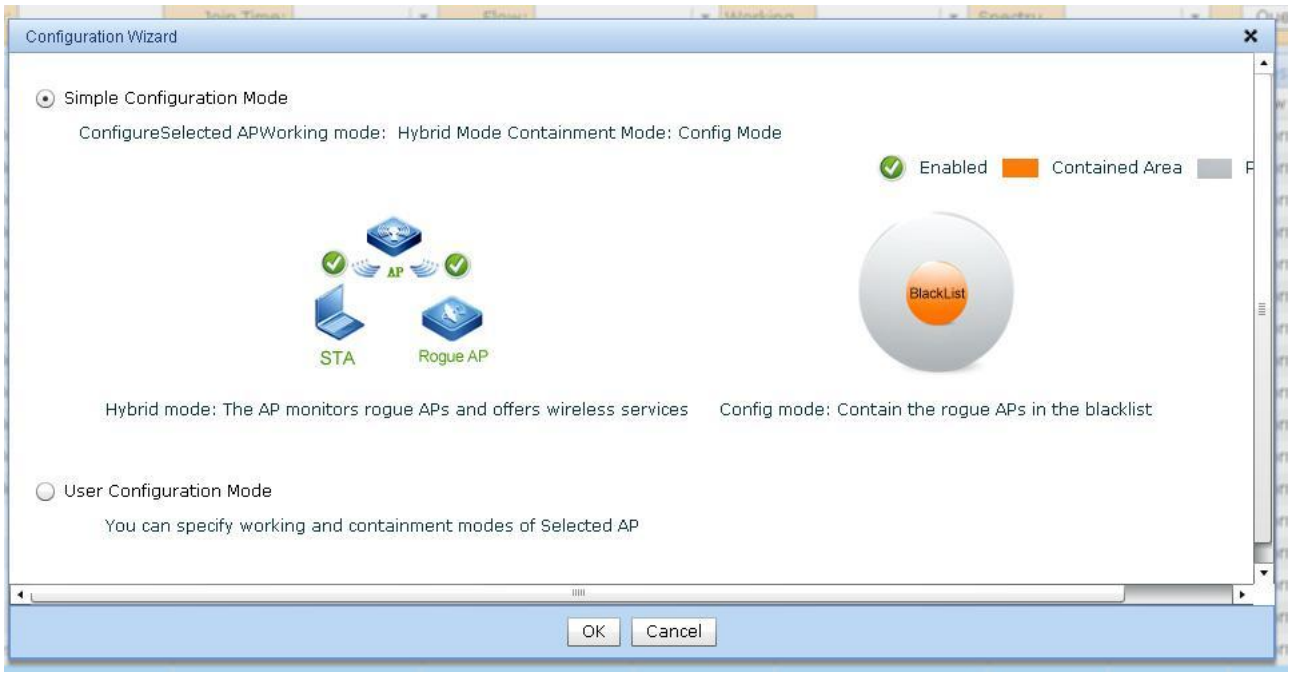


Figure 7.118. Configuration Wizard

If you have selected **User Configuration Mode**, the **Select AP Working Mode** page is displayed, as shown in the following figure:

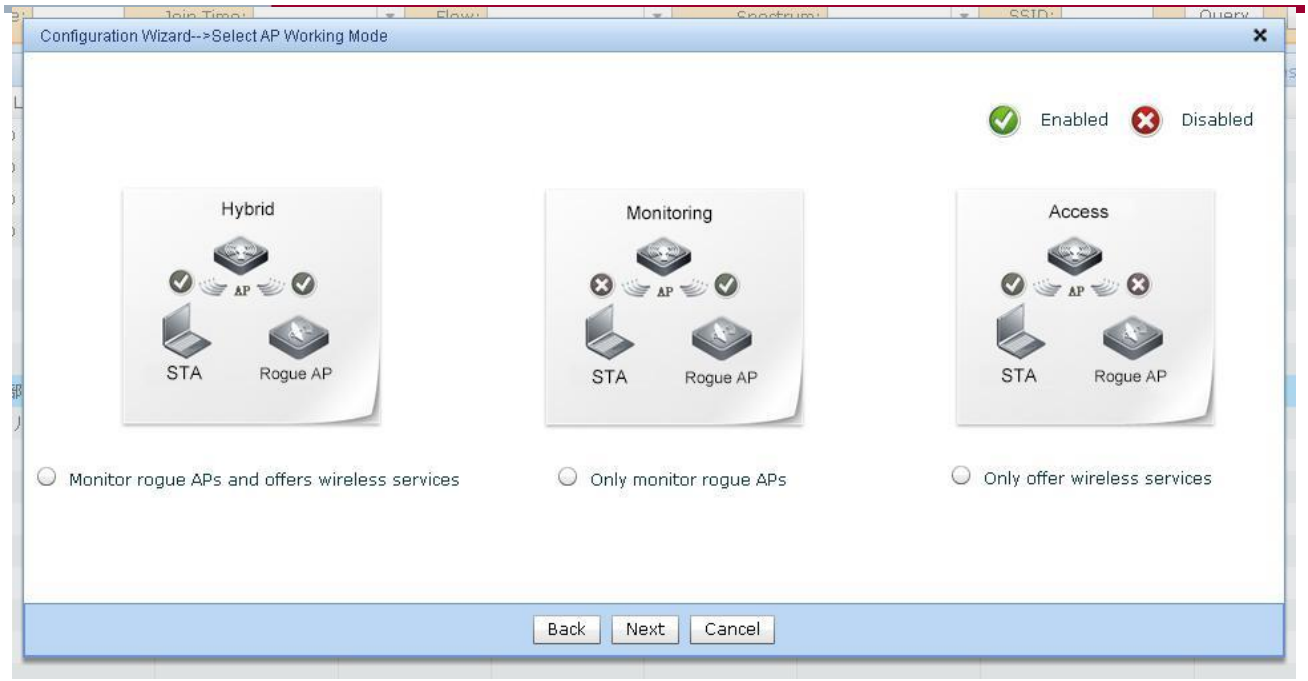


Figure 7.119. Configuring AP Working Mode

Click **Next**, and the **Select AP Containment Mode** page is displayed. You can select one or several modes, as shown in the following figure:

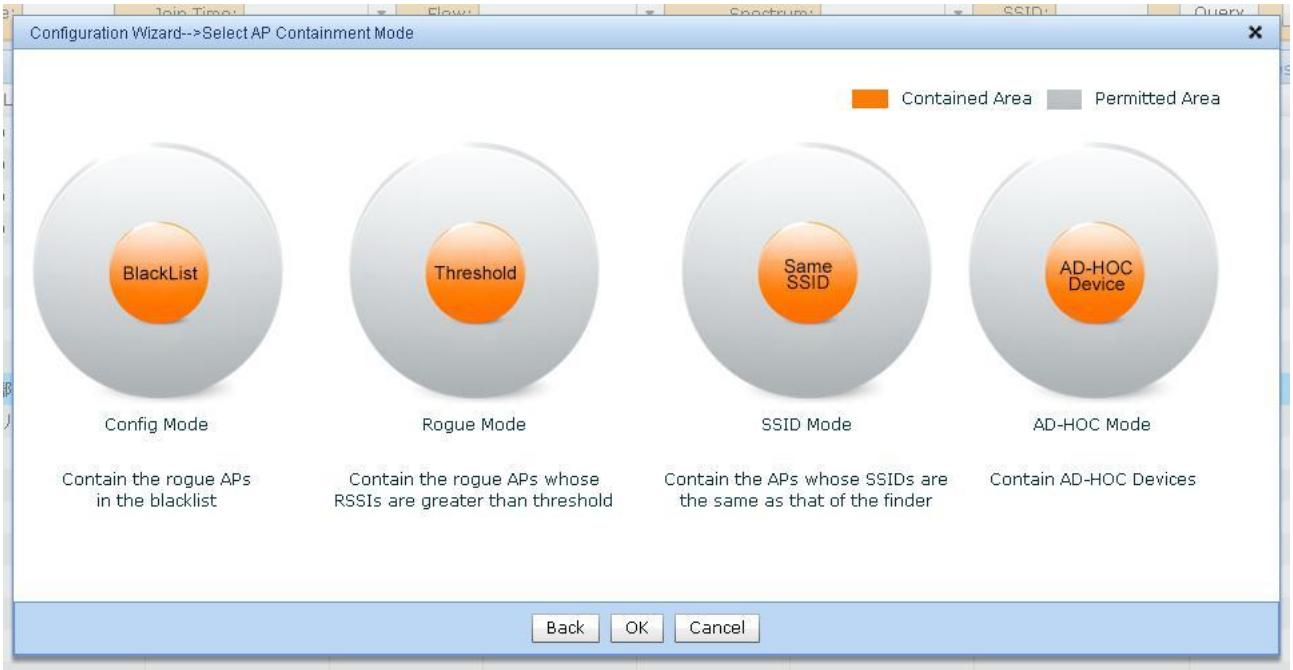


Figure 7.120. Configuring AP Containment Mode

After the configuration is complete, the system returns to the **Rogue AP List** page.

View AP Working Mode and Containment Mode

View AP working mode and containment mode on the AP Details page:

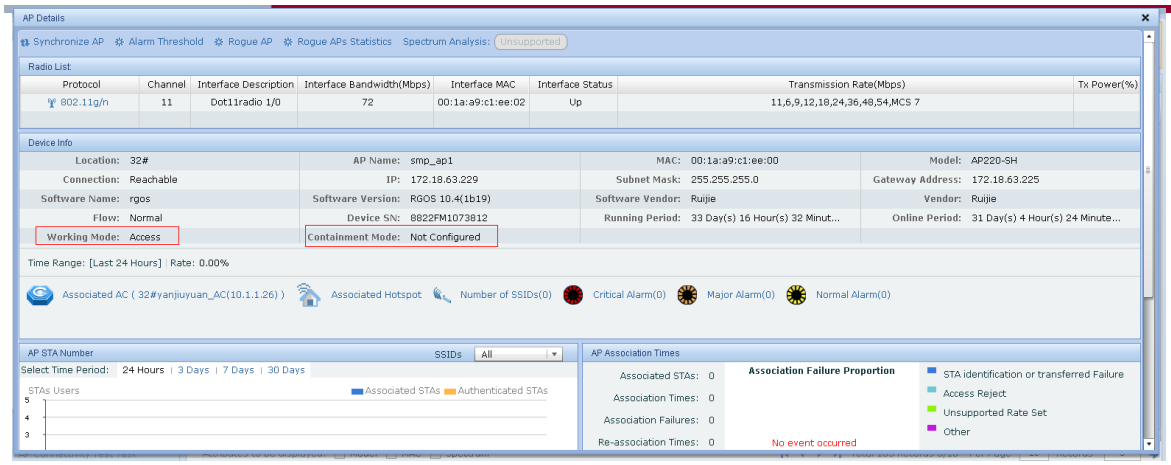


Figure 7.121. View AP Working Mode and Containment Mode

7.4. AC

Major Functions

- Add, Query and Delete AC
- AC Operation
- Synchronize AC
- Configure Alarm Threshold
- Details

7.4.1. Add, Query and Delete AC

This part describes how to add, query and delete the AC.

Add AC

32) Click **Add**, as shown in the following figure:

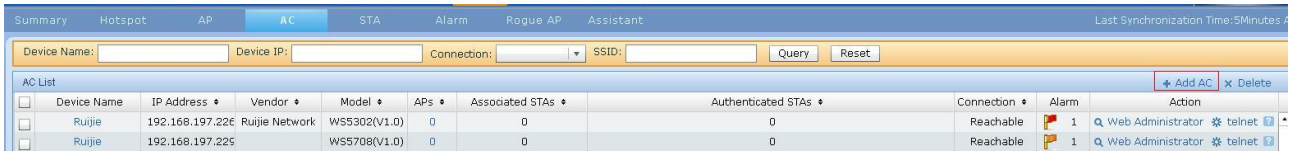


Figure 7.122. Clicking Add

Enter the IP address and select the template, as shown in the figure below.

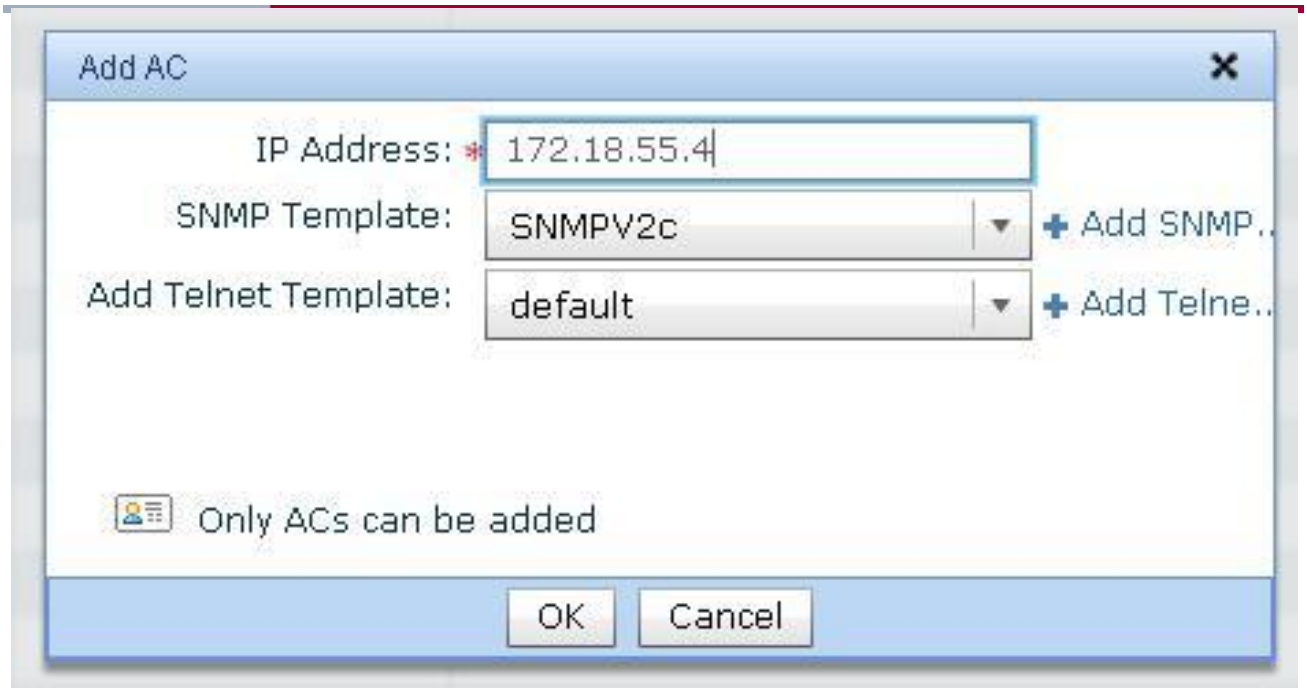


Figure 7.123. Entering IP Address and Selecting Template

Click **OK**, then the system returns to the **AC List** page.

Query AC

Enter the query criteria and click **Query**, as shown in the following figure:

Figure 7.124. Querying AC

Delete AC

33) Select the AC and click **Delete**, as shown in the following figure:

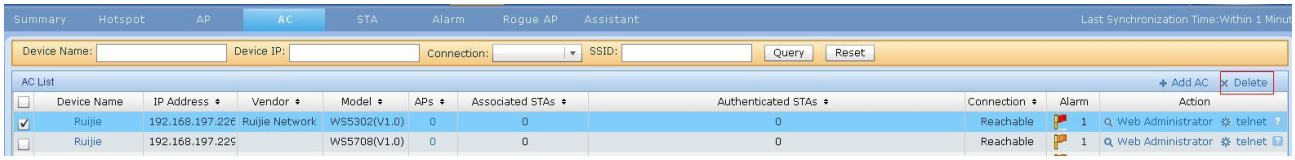


Figure 7.125. Deleting AC

After the AC is deleted, the system returns to the **AC List** page.

7.4.2. AC Operation

Web Management

34) Click **Web Management**

Figure 7.126. Click Web Management

Go to Web Management page. Enter the user name and password and click **Login**.

7.4.3. Synchronize AC

Operation Steps

35) Click the device name in the AC list, as shown in the following figure, to display its details.

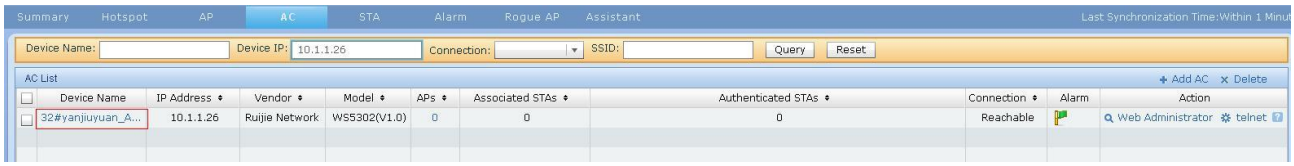


Figure 7.127. Displaying AC Details

Click **Synchronize AC**, as shown in the following figure:

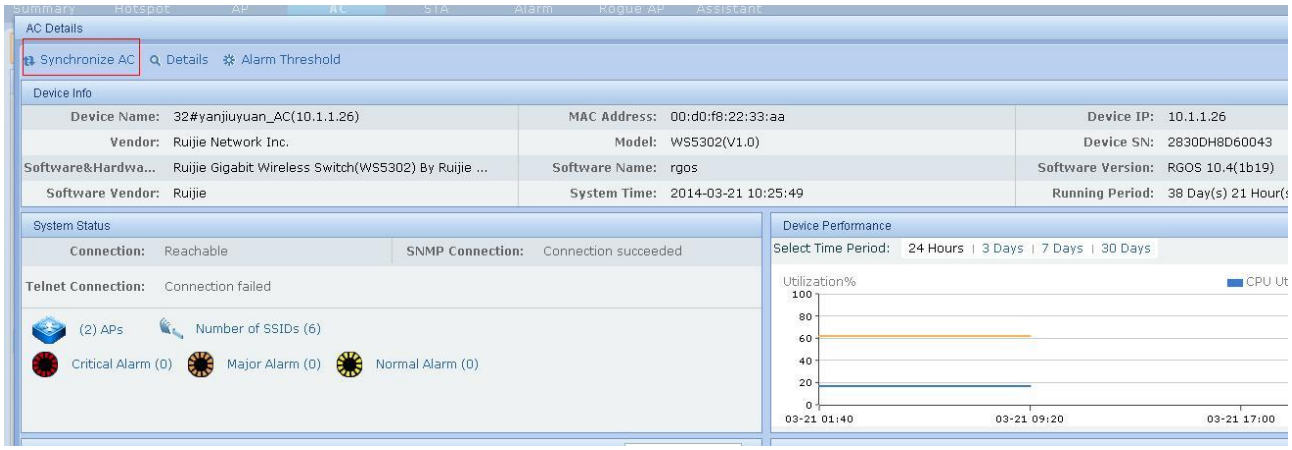


Figure 7.128. Synchronizing AC Information

7.4.4. Configure Alarm Threshold

Operation Steps

36) Click the device name in the AC list, as shown in the following figure, to display its details.

Figure 7.129. Displaying AC Details

Click **Alarm Threshold Configuration**

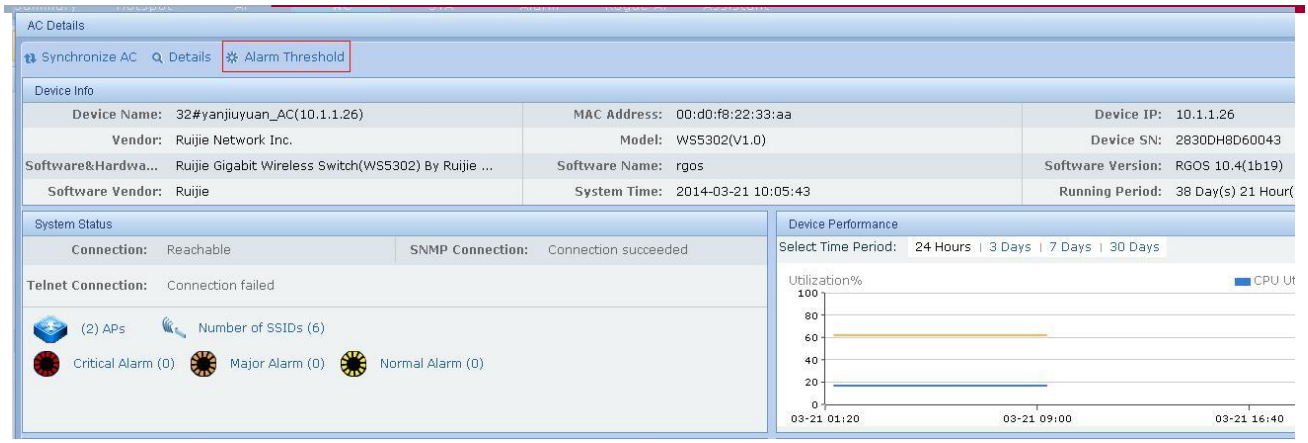


Figure 7.130. Alarm Threshold Configuration

Set alarm parameters as shown in the following figure:

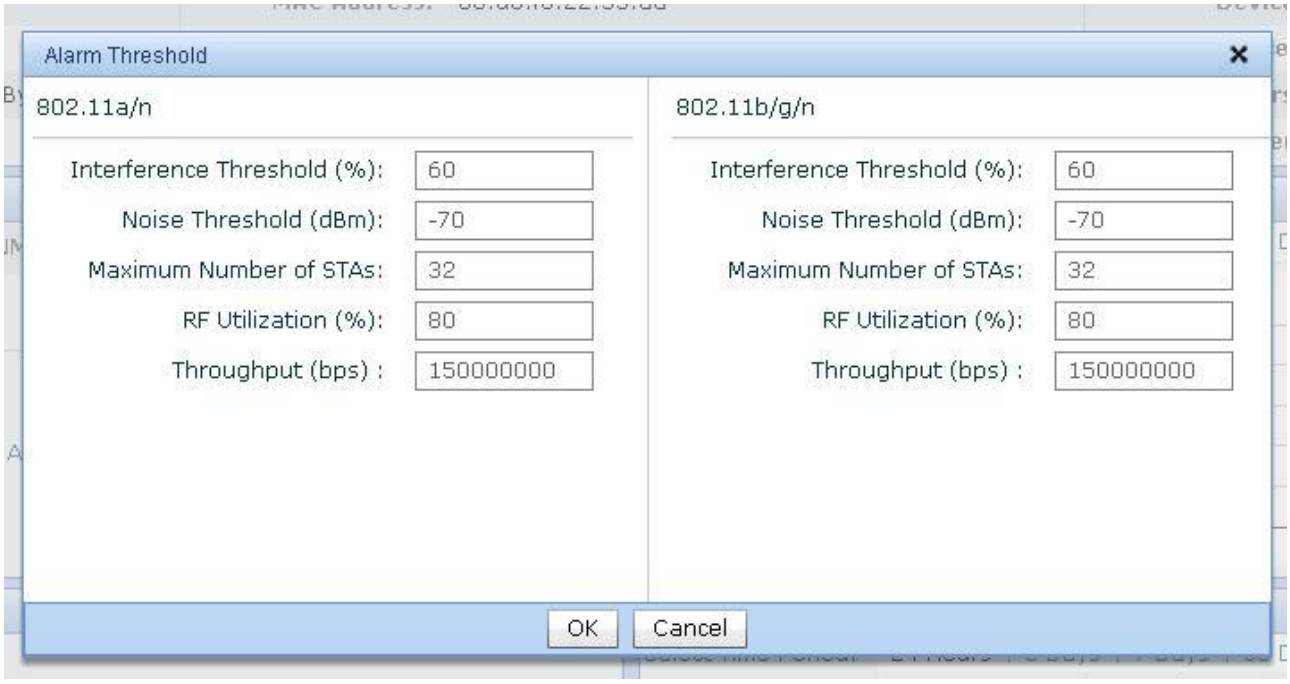


Figure 7.131. Configuring Alarm Threshold Parameters

7.4.5. Details

The AC page enables you to view information about WLAN, interface, device, 802.11a/b/g, WIDS and License.

Major Functions

- Access Controller

7.4.5.1. Access Controller

The AC page enables you to view information about WLAN, interface, device, 802.11a/b/g, WIDS and License.

Note The device type can be recognized only when it is reachable.

Major Functions

- Basic Information
- Static Route Management
- STP Setting

- Mobility Group List
- DHCP
- AC Redundancy Configuration
- WLAN Configuration
- Radius Server
- AP Group
- AP Group Configuration
- WIDS Configuration
- Interface Configuration
- Trap Receiver
- Trap Control
- Syslog Receiver
- Configure IGMP Snooping
- Country/Area Code
- 802.11a/n Configuration
- EDCA Configuration
- RRM Threshold
- RRM Interference
- RRM DCA Configuration
- RRM RF Grouping Configuration
- 802.11n Configuration
- License

7.4.5.1.1 Basic Information

This function enables you to go to the Basic Information page and modify the basic information.

Operation Steps

37) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

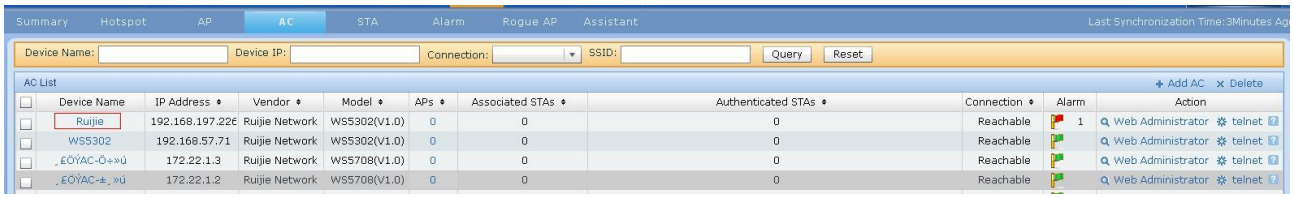


Figure 7.132. Going to AC Details

Click **Details**

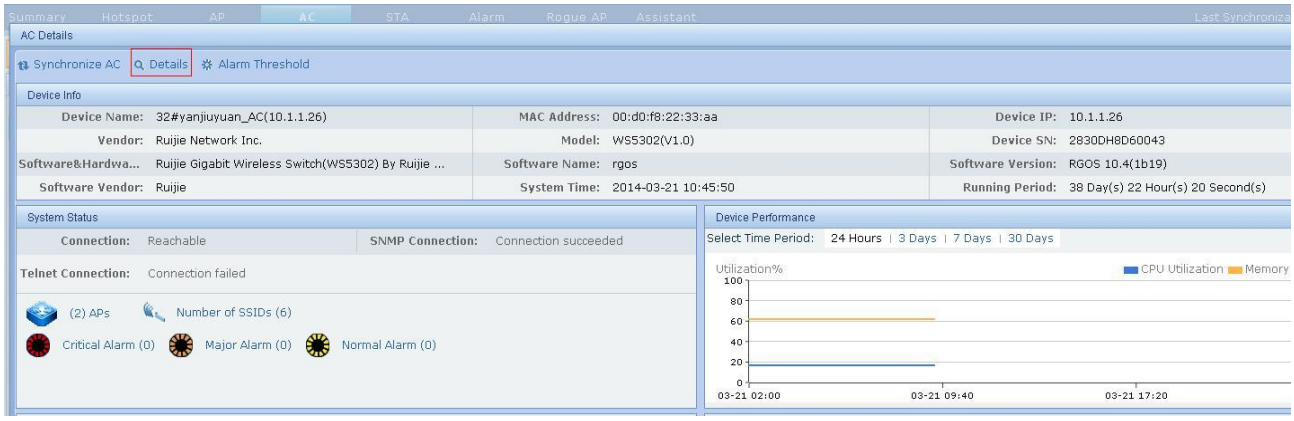


Figure 7.133. Details

The **Basic Information** page is displayed, as shown in the following figure:

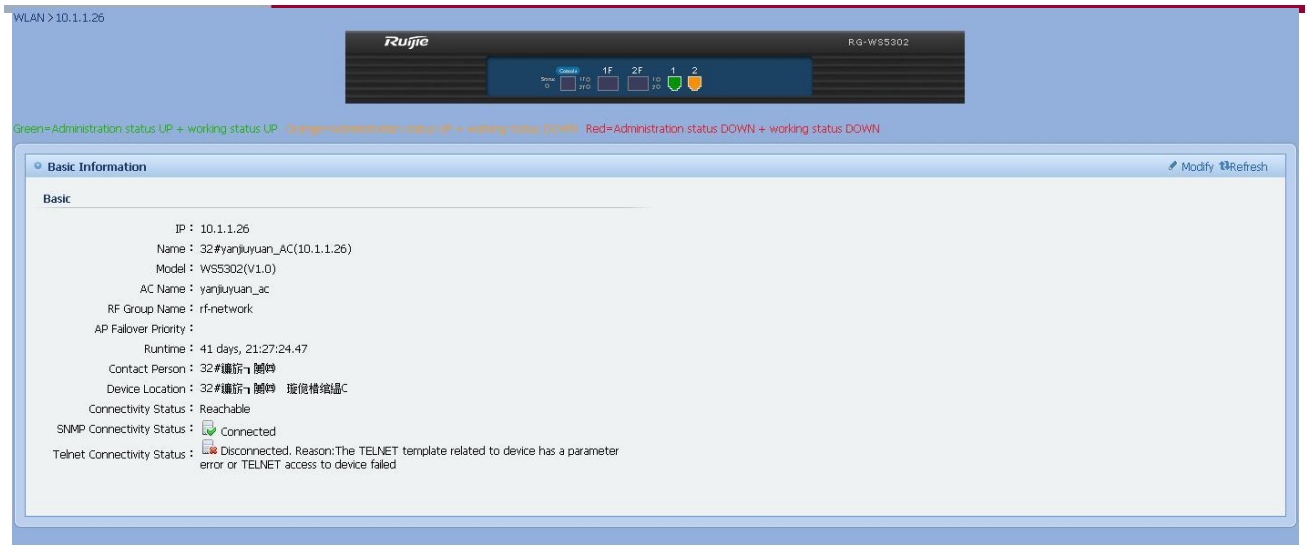


Figure 7.134. Basic Information

By clicking **Modify**, you are able to modify the basic information, as shown in the following figure:

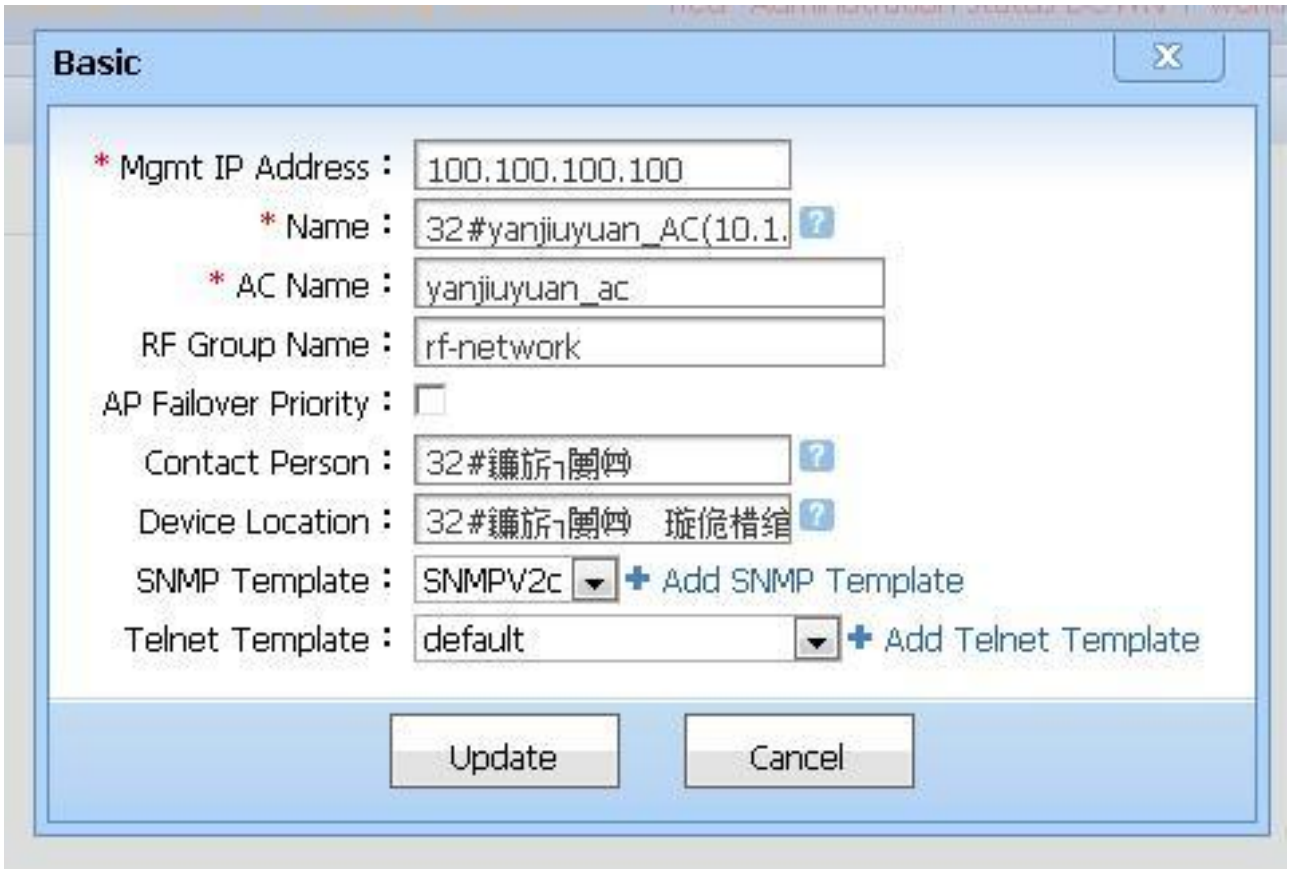


Figure 7.135. Basic Information

Note To ensure that this function works properly, please make sure SNMP Connectivity Status is connected.

7.4.5.1.2. Static Route Management

This function enables you to add and delete static routes.

38) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

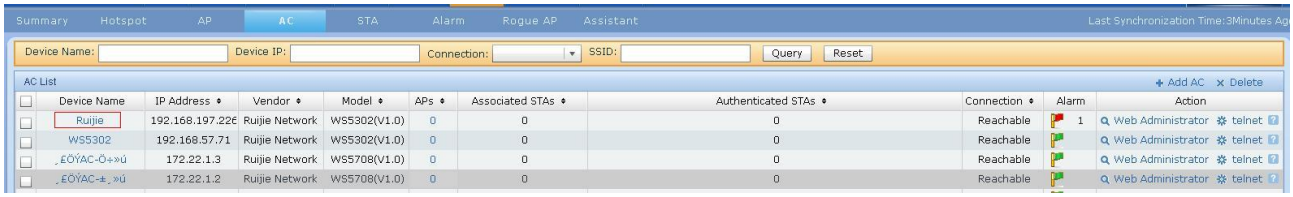


Figure 7.136. Going to AC Details Page

Click **Details**

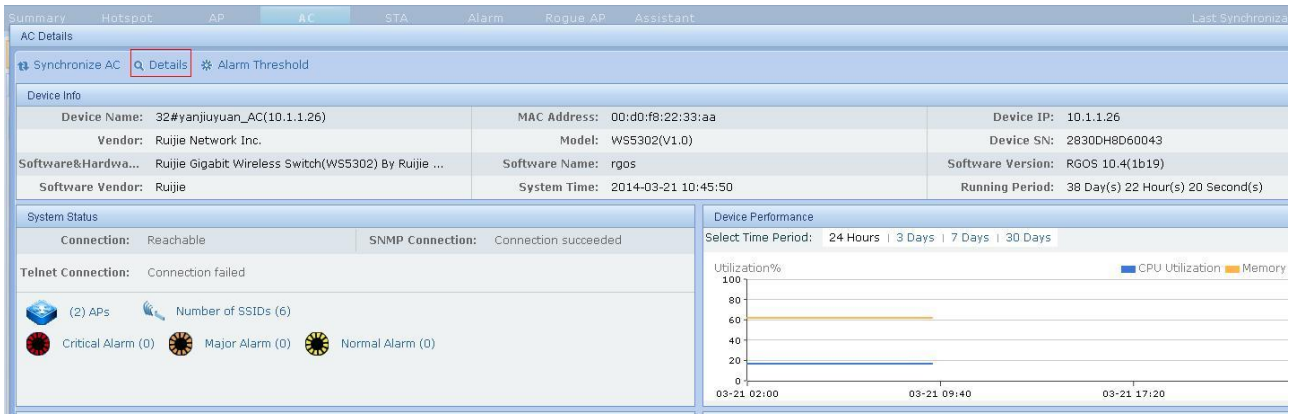


Figure 7.137. Details

In the **Controller** menu, unfold **System**, and click **Route Configuration** to go to the **Route Configuration** page, as shown in the following figure:

Figure 7.138. Clicking Route Configuration

Static routes are displayed on **Route Configuration**, as shown in the following figure:

Figure 7.139. Static routes on Route Configuration

You can add, delete and synchronize static routes on **Route Configuration**, as shown in the following figure:

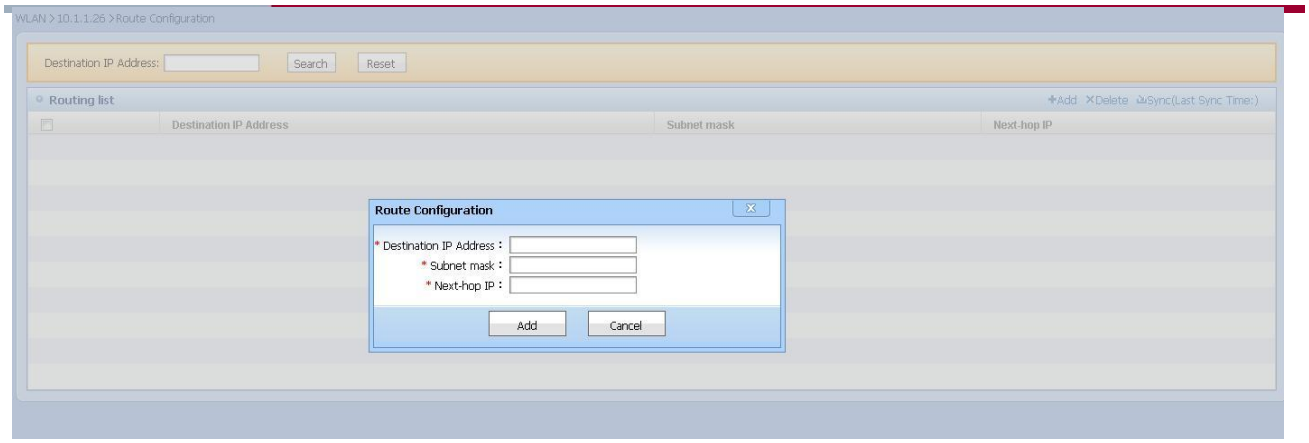


Figure 7.140. Adding Routes

Figure 7.141. Deleting and Synchronizing Static Routes

7.4.5.1.3. STP Setting

This function enables you to go to the **STP Setting** page, and modify the STP setting.

Operation Steps

39) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

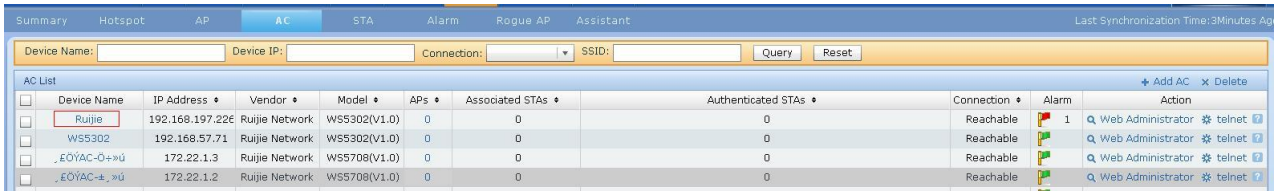


Figure 7.142. Going to AC Details Page

Click **Details**

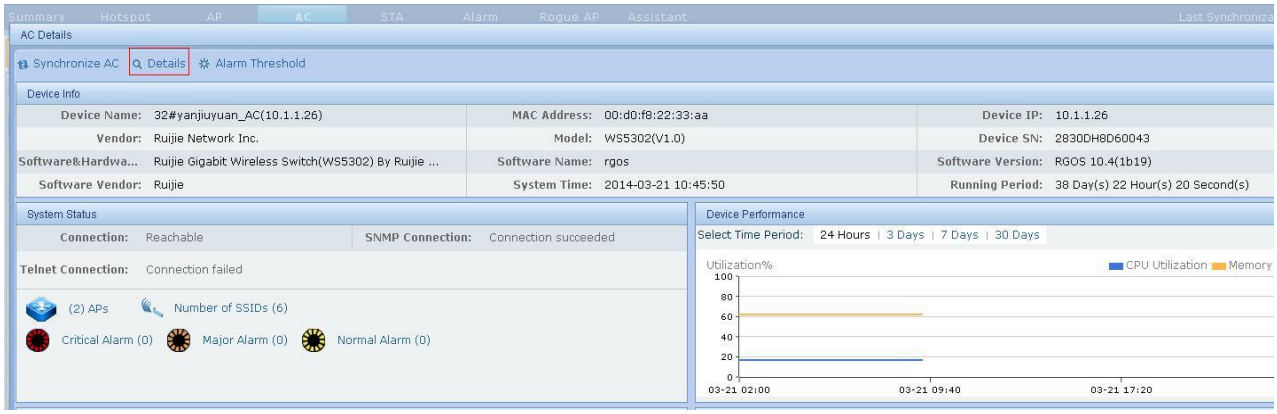


Figure 7.143. Details

In the **Controller** menu, unfold **System**, and click **STP Setting** to go to the **STP Setting** page, as shown in the following figure:

Figure 7.144. Clicking STP Setting

You can modify, restore and synchronize STP settings, as shown in the following figure:

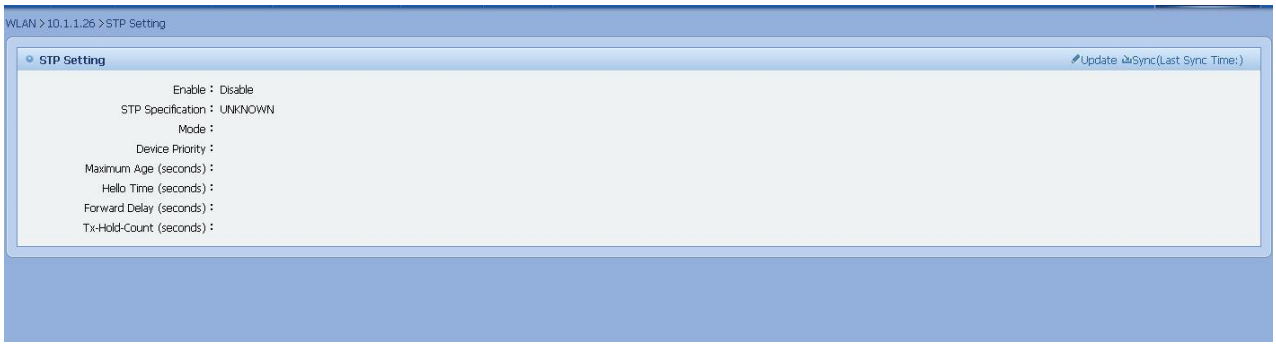


Figure 7.145. STP Setting

Note To ensure that this function works properly, please make sure the TELNET Connectivity Status is connected.

7.4.5.1.4. Mobility Group List

This function enables you to add, delete and synchronize mobility group on Mobility Group List.

Operation Steps

40) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

Figure 7.146. Going to AC Details Page

Click **Details**

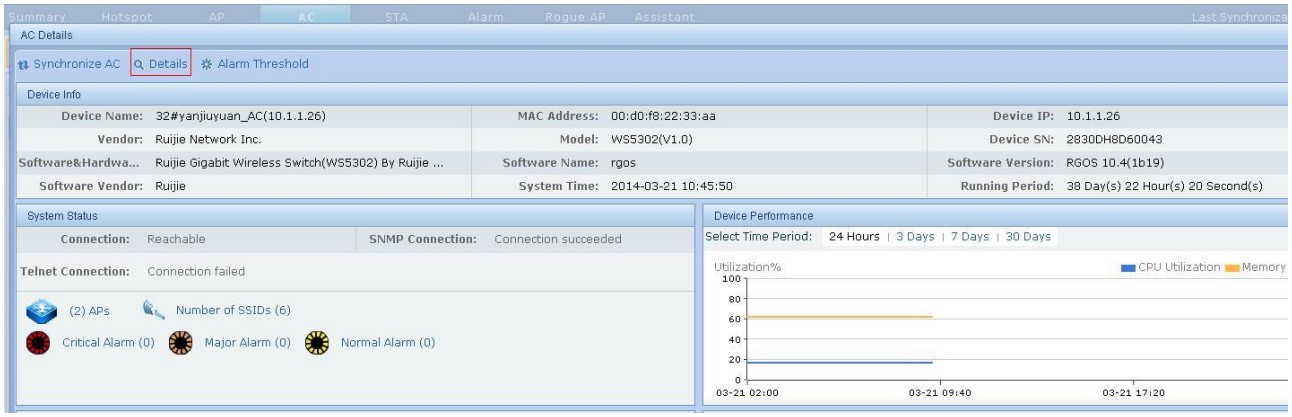


Figure 7.147. Details

In the **Controller** menu, unfold **Device Configuration**, and click **Syslog Receiver** to go to the **Syslog Receiver** page, as shown in the following figure:

Figure 7.148. Selecting Mobility Group List

Selecting **Mobility Group List**

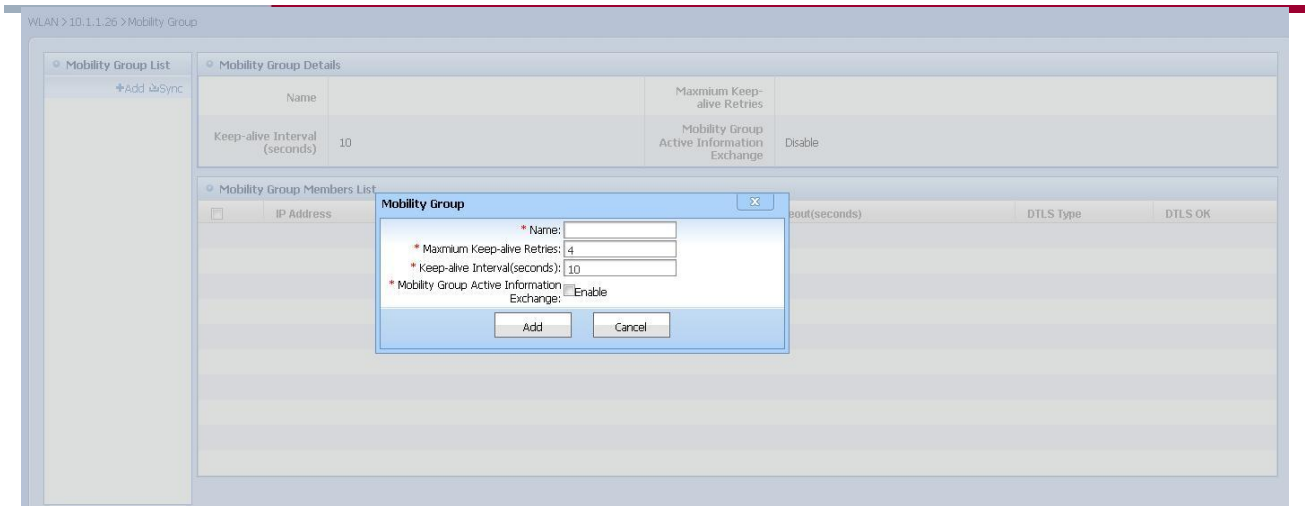


Figure 7.149. Adding Mobility Group

Figure 7.150. Deleting Mobility Group

Figure 7.151. Adding and Deleting Mobility Group Members

Figure 7.152. Synchronizing Mobility Group

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.5. DHCP

This function enables you to maintain the DHCP pool and DHCP server, enable and disable the DHCP service, and view DHCP statistics.

Operation Steps

41) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

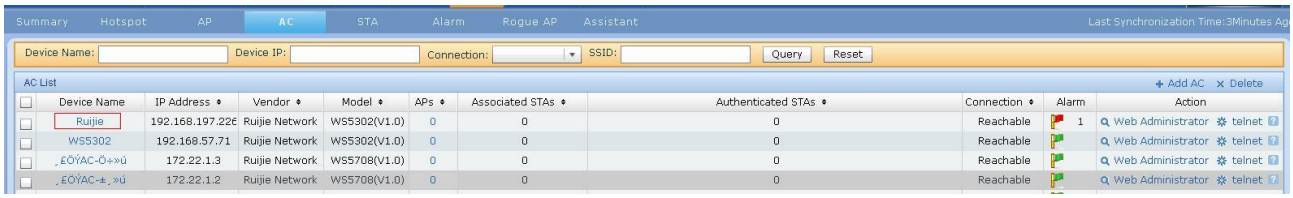


Figure 7.153. Going to **AC Details** Page

Click **Details**

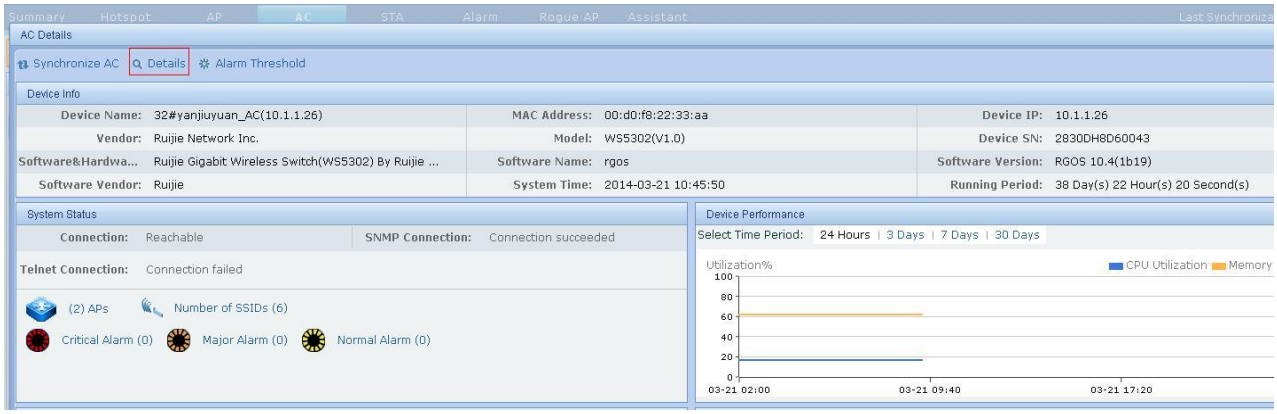


Figure 7.154. Details

In the **Controller** menu, unfold **System**, and click **DHCP Configuration** to go to the **DHCP Configuration** page, as shown in the following figure:

Figure 7.155. Clicking DHCP Configuration

You can add, modify and delete DHCP pools on **DHCP Pool List**, as shown in the following figure:

Figure 7.156. DHCP Pool List

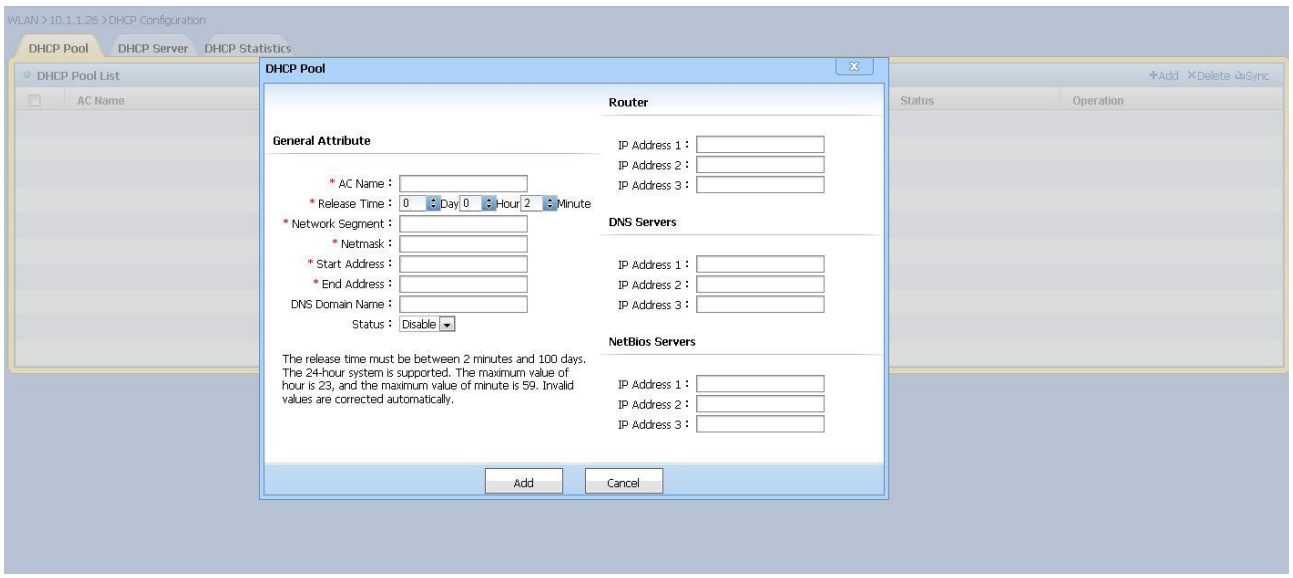


Figure 7.157. Adding DHCP Pool

You can add, modify and delete DHCP servers on **DHCP Server List**, as shown in the following figure:

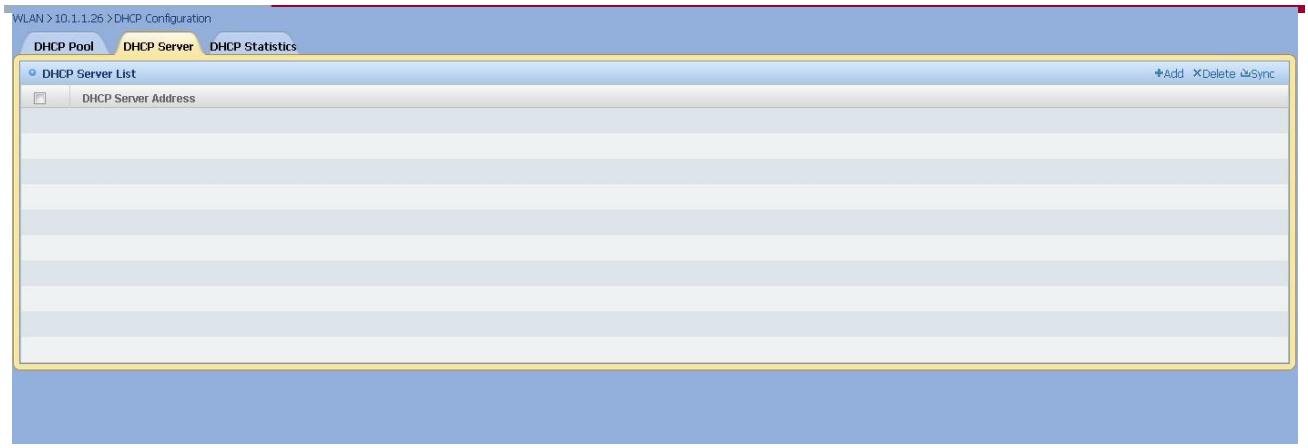


Figure 7.158. DHCP Server

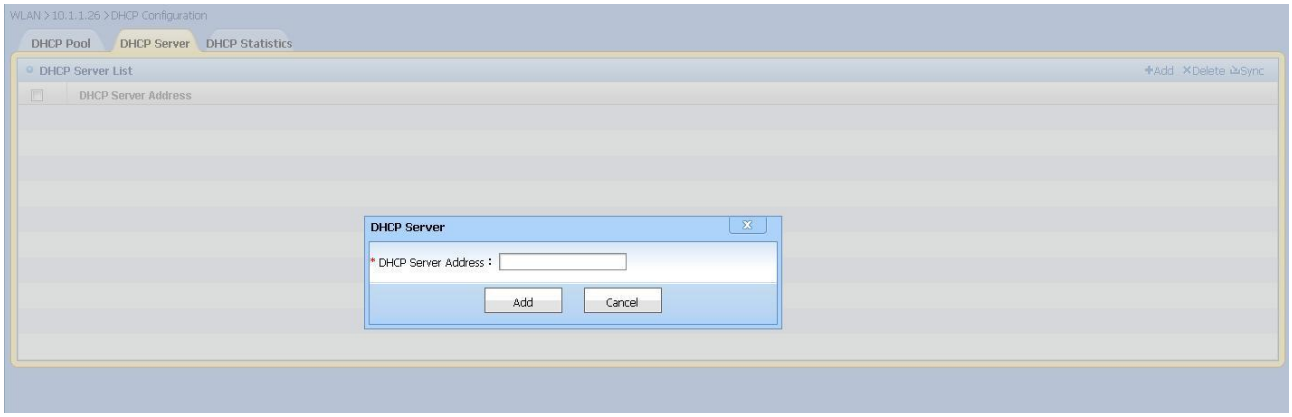


Figure 7.159. Adding DHCP Server

DHCP Statistics is shown in the following figure:

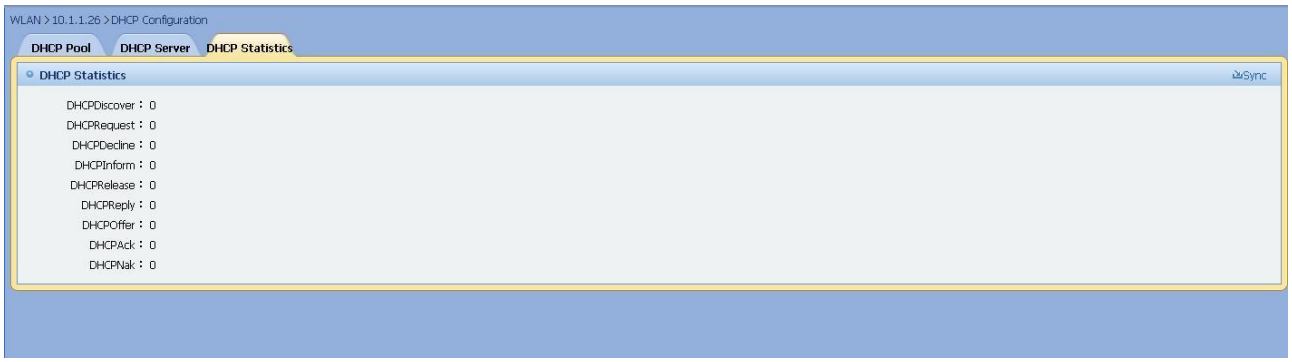


Figure 7.160. DHCP Statistics

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.6. AC Redundancy Configuration

This function enables you to perform AC redundancy configuration.

Operation Steps

42) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

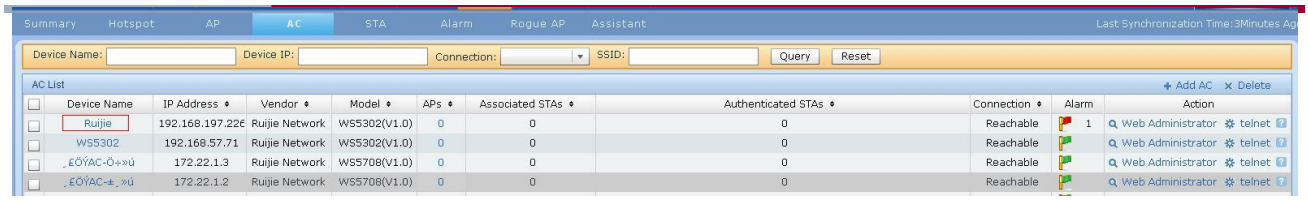


Figure 7.161. Going to **AC Details** Page

Click **Details**

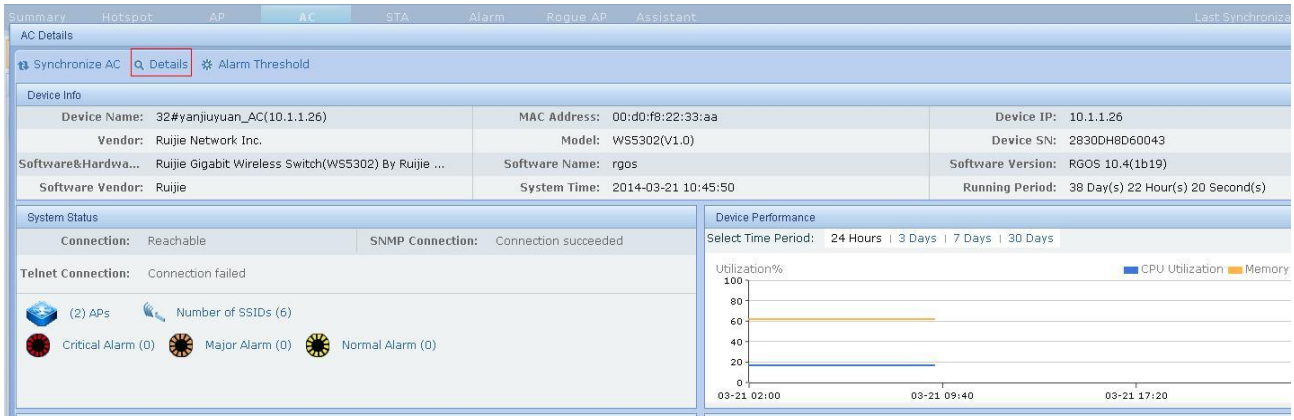


Figure 7.162. Details

In the **Controller** menu, Click **System**, as shown in the following figure:

Figure 7.163. AC Redundancy Configuration

Click **AC Redundancy Configuration**, as shown in the following figure:

Figure 7.164. AC Redundancy Configuration

Click **Update**. The system will load the data to device and AC redundancy configuration information of network management system will be also modified, as shown in the following figure:

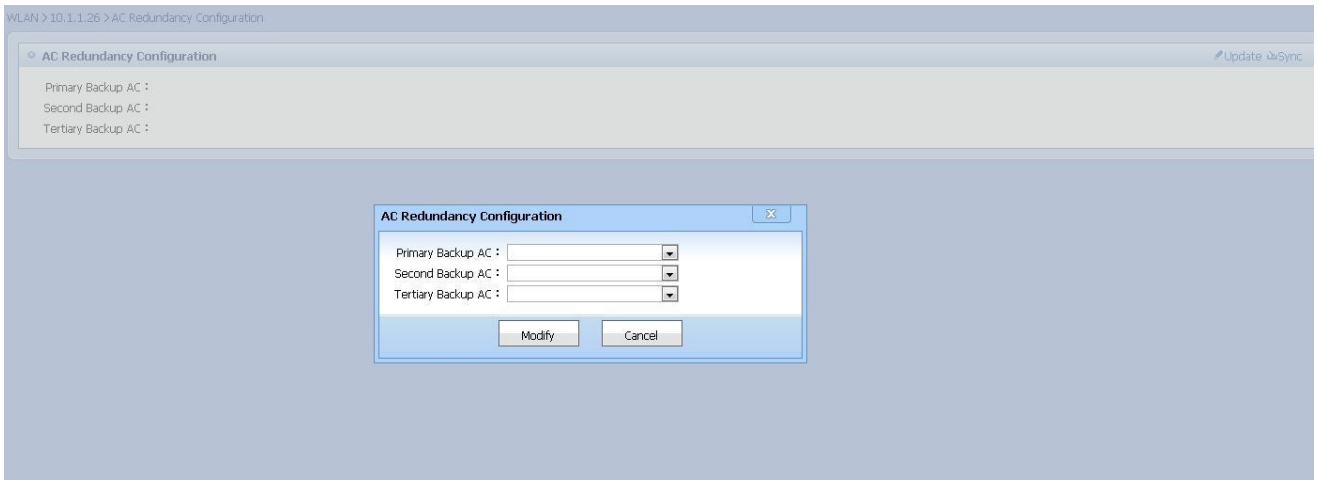


Figure 7.165. Modifying AC Redundancy Configuration

Note

The primary backup AC are mandatory. The second and tertiary backup ACs are optional.
The primary, second and tertiary backup ACs cannot be the same.
To make sure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.7. WLAN Configuration

This function enables you to add, delete and modify WLAN configuration.

Operation Steps

43) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

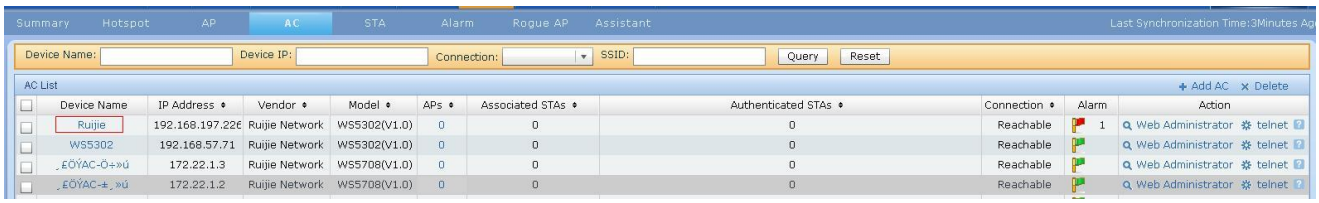


Figure 7.166. Going to AC Details

Click **Details**

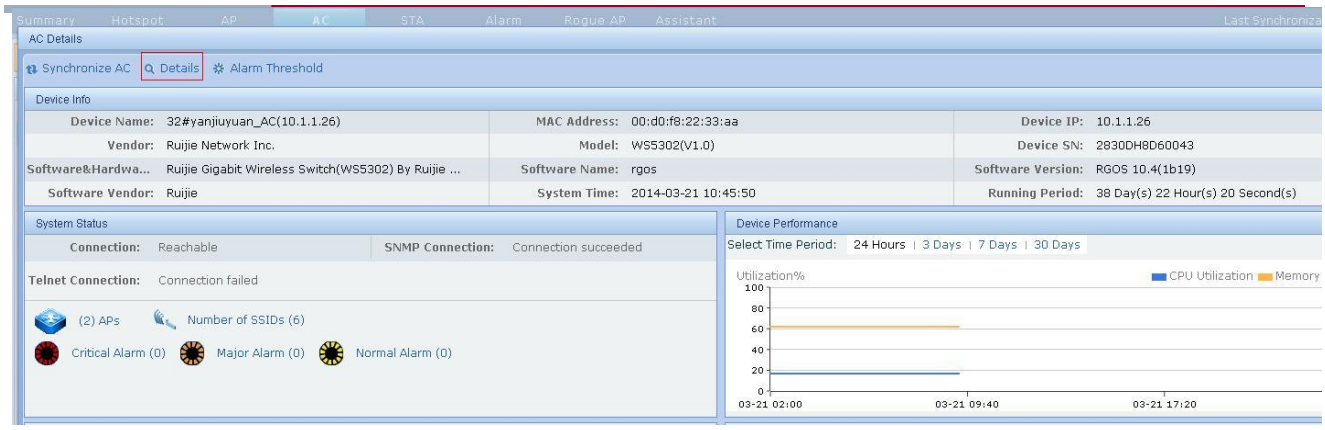


Figure 7.167. Details

In the **Controller** menu, unfold **WLAN**, and click **WLAN Configuration** to go to the **WLAN Configuration** page, as shown in the following figure:

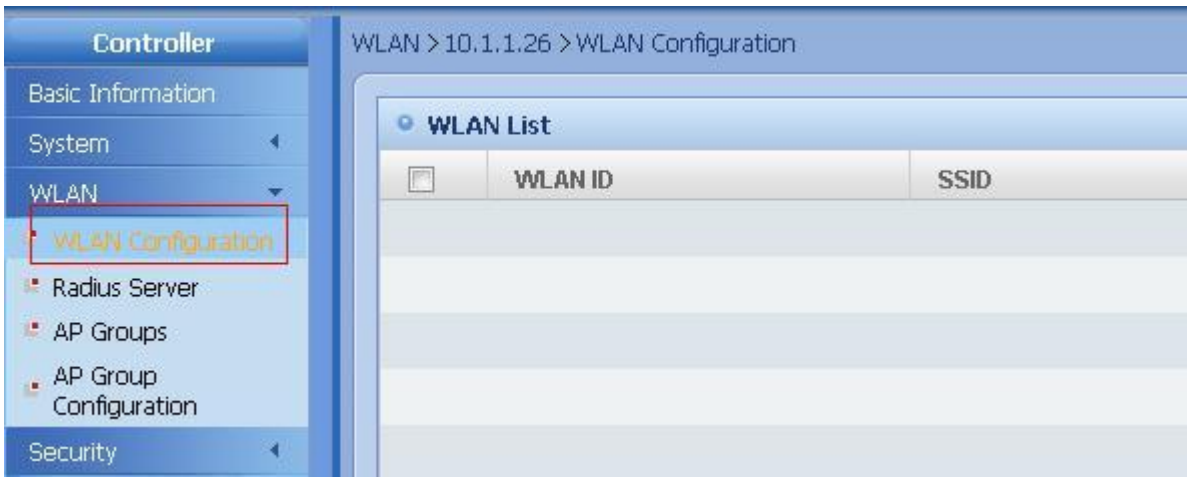


Figure 7.168. Clicking WLAN Configuration

The WLAN information is displayed, as shown in the following figure:

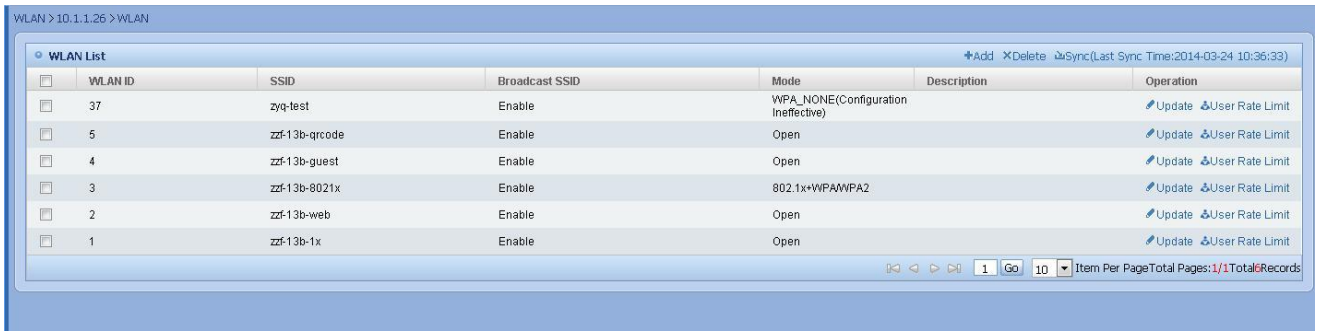


Figure 7.169. WLAN List

Related Operations

- Add WLAN Configuration
- Modify WLAN Configuration
- Delete WLAN Configuration
- Maintain User Rate

7.4.5.1.7.1. Add WLAN Configuration

Add WLAN info.

Operation Steps

44) On WLAN configuration list page, click **Add** to enter **Add WLAN configuration** page, as shown in the following figure:

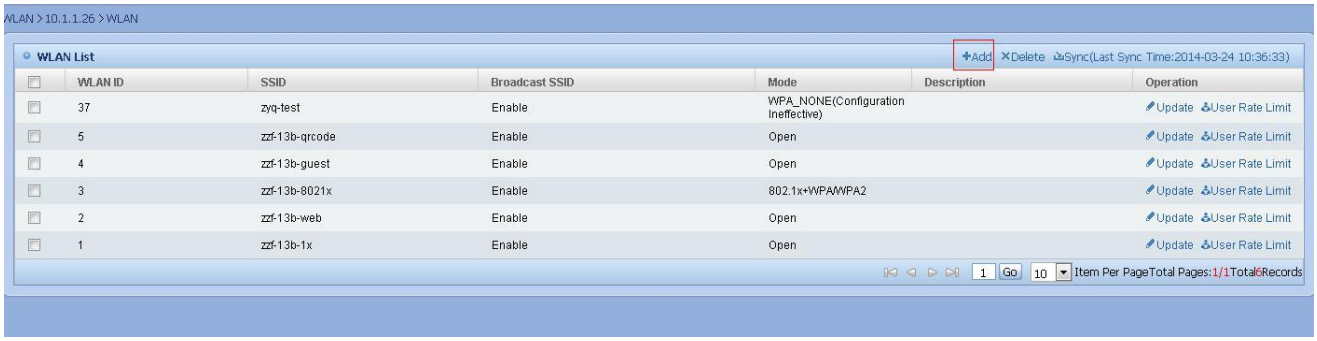


Figure7.170. Enter Add WLAN Configuration Page

On Add WLAN configuration page, click **Add** to finish the adding, as shown below:

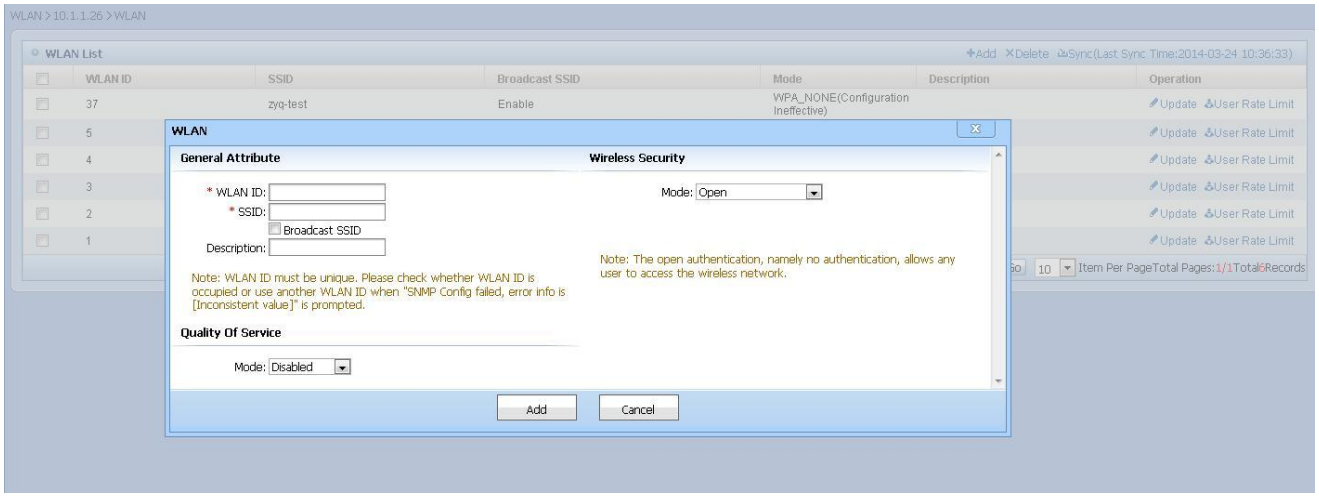


Figure 7.171. Add WLAN Configuration Page

Note To make this function work properly, please make sure that SNMP connection status is connectable.

7.4.5.1.7.2. Modify WLAN Configuration

Modify WLAN configuration info.

Operation Steps

45) On WLAN configuration list page, click **Update** to enter Modify WLAN configuration page, as shown in the following figure:

Figure 7.172. Enter Modify WLAN Configuration Page

On Modify WLAN configuration page, click **Modify** to finish the modification, as shown in the following figure:

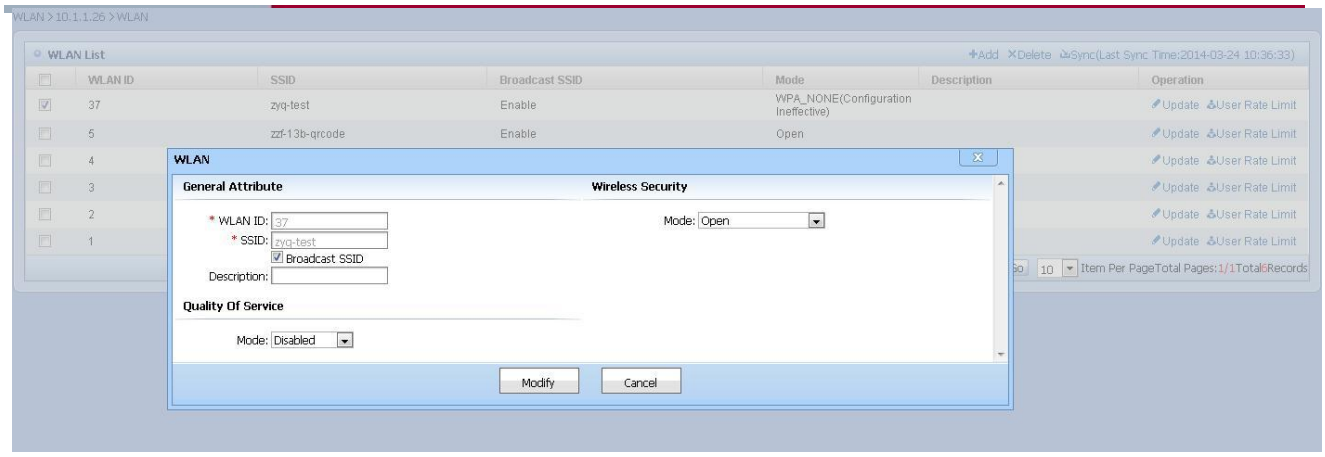


Figure 7.173. Modify WLAN Configuration Page

Note To make this function work properly, please make sure that Telnet connection status is connectable.

7.4.5.1.7.3. Delete WLAN Configuration

Delete WLAN info.

Operation Steps

On WLAN configuration list page, choose certain WLAN config, and click **Delete** to delete the info, as shown below:

Figure 7.174. Delete WLAN

Note To make this function work properly, please make sure that SNMP connection status is connectable.

7.4.5.1.7.4. Maintain User Rate

Maintain user rate.

Operation Steps

46) On Wireless network configuration list page, click **User Rate Limit** to enter User rate maintenance page, as shown below:

Figure 7.175. Enter User Rate Maintenance Page

On User rate maintenance page, **Add** and **Delete** operations can be performed on users, as shown below:

Figure 7.176. User Rate Maintenance Page

Note To make this function work properly, please make sure that SNMP connection status is connectable.

7.4.5.1.8. Radius Server

This function enables you to add and delete the Radius server.

Operation Steps

47) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

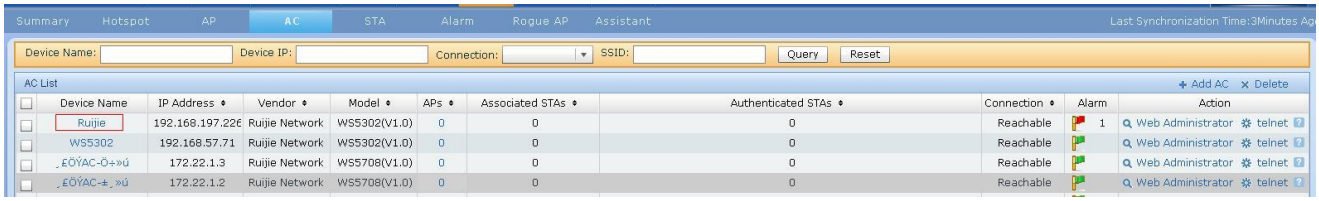


Figure 7.177. Going to **AC Details** Page

Click **Details**

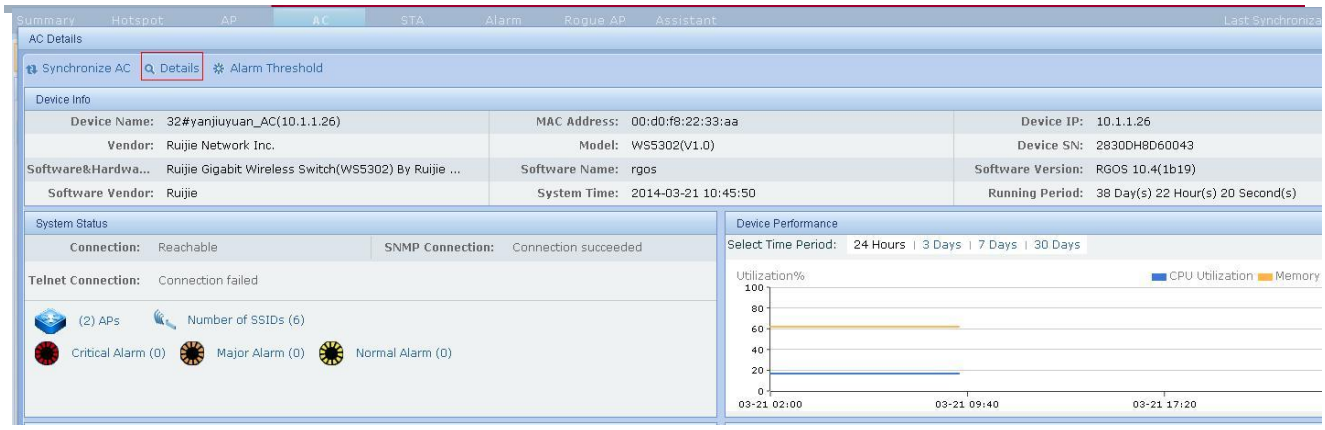


Figure 7.178. Details

In the **Controller** menu, unfold **WLAN**, and click **Radius Server** to go to the **Radius Server** page, as shown in the following figure:

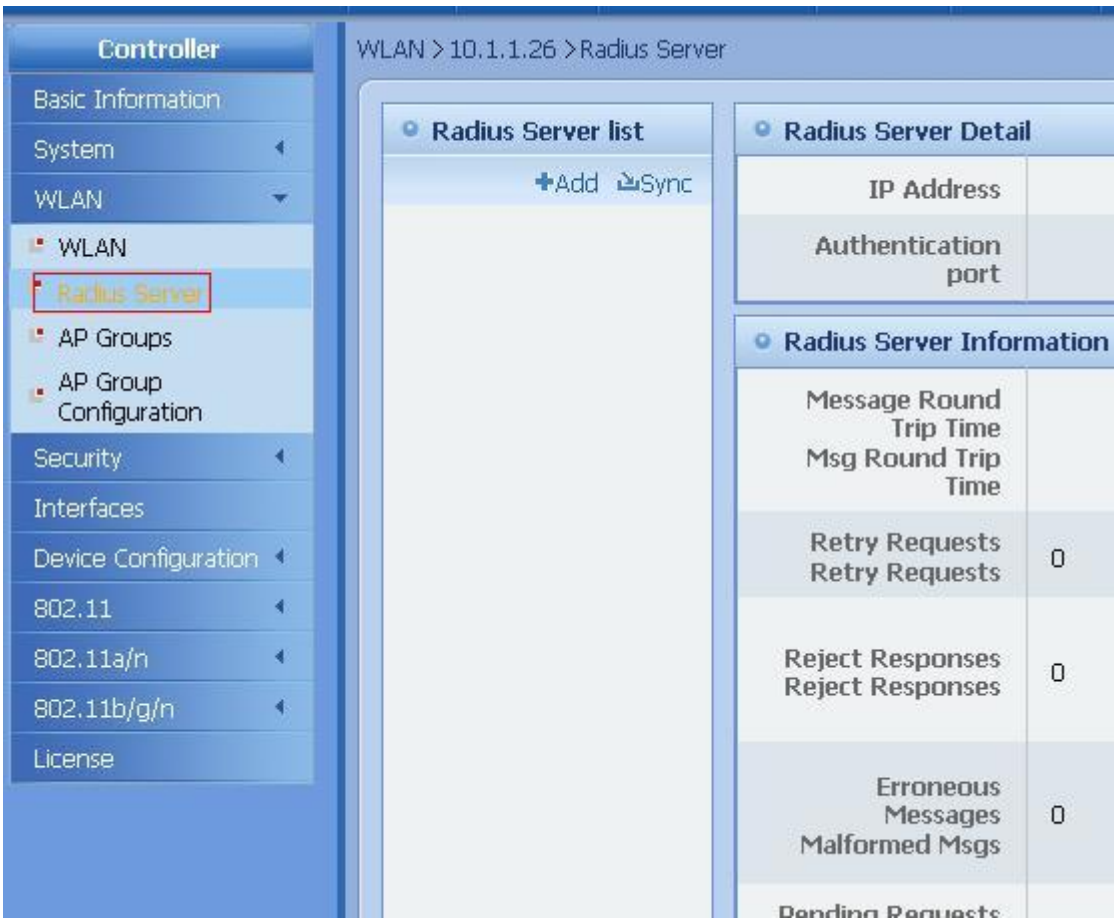


Figure 7.179. Clicking Radius Server

The Radius server information is displayed, as shown in the following figure:

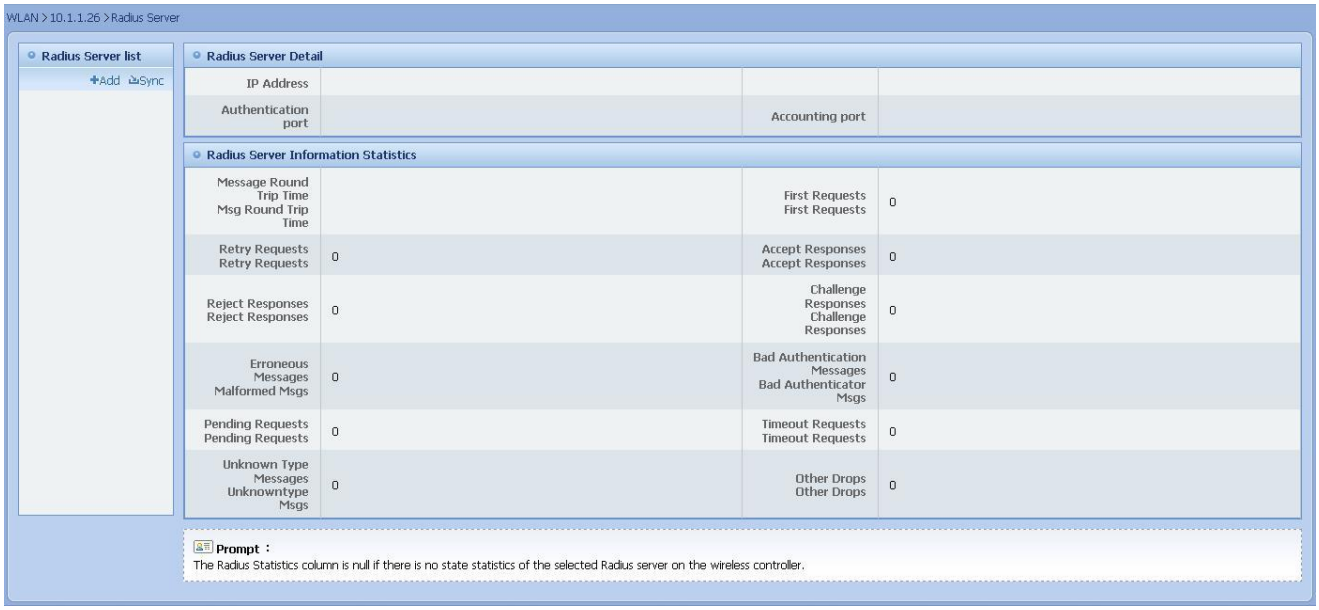


Figure 7.180. Radius Server

You can add and delete Radius servers, and view **Radius Server Information Statistics** on **Radius Server**, as shown in the following figure:

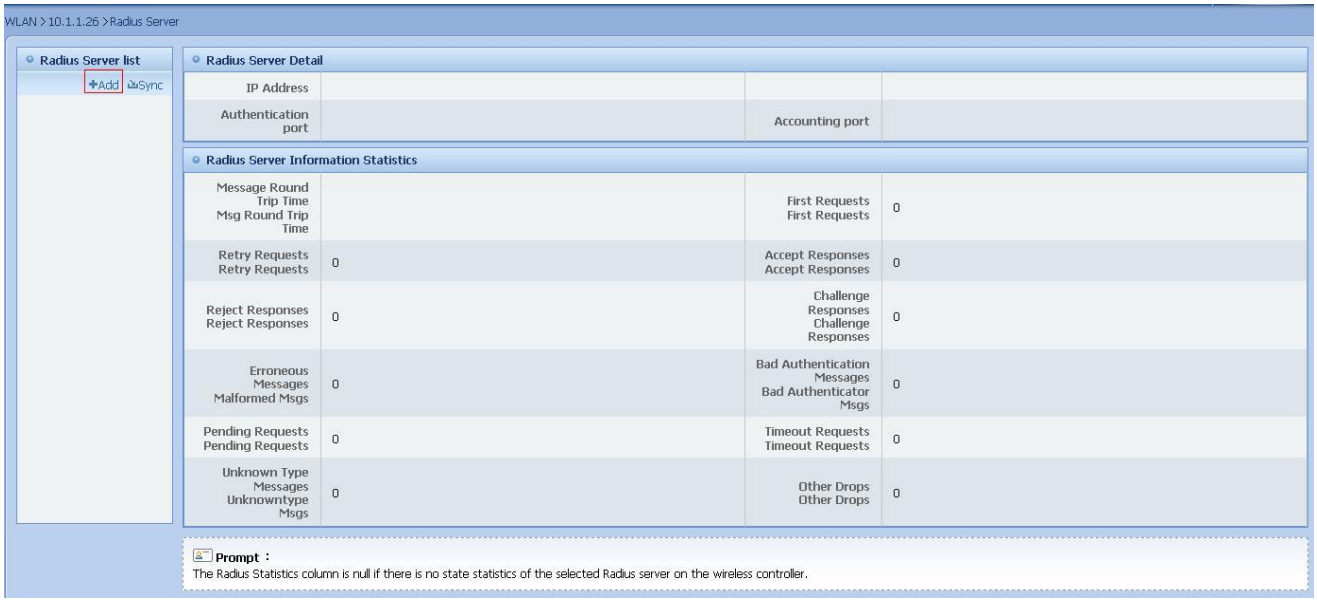


Figure 7.181. Adding Radius Server

Figure 7.182. Deleting Radius Server

Figure 7.183. Viewing Radius Server Information Statistics

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.9. AP Group

This function enables you to add and delete AP group information.

Operation Steps

48) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

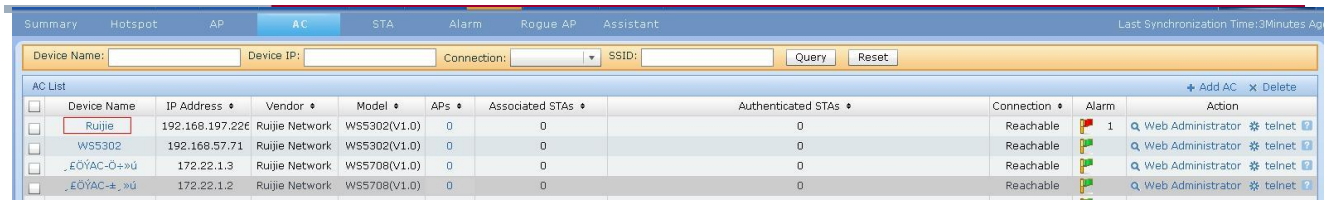


Figure 7.184. Going to **AC Details** Page

Click **Details**

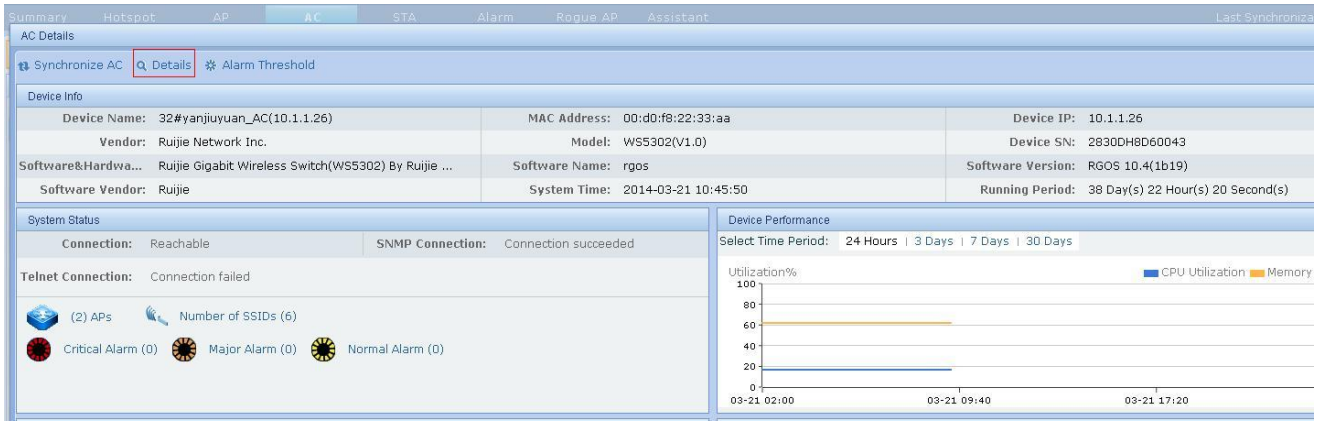


Figure 7.185. Details

In the **Controller** menu, unfold **WLAN**, and click **AP Groups** to go to the **Trap Control** page, as shown in the following figure:

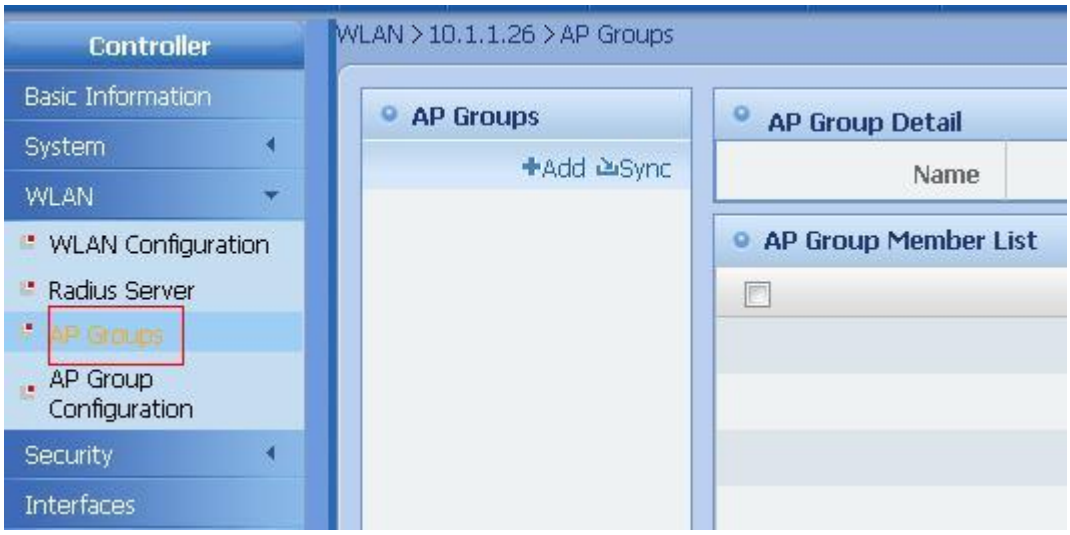


Figure 7.186. Clicking AP Groups

The AP group information is displayed, as shown in the following figure:

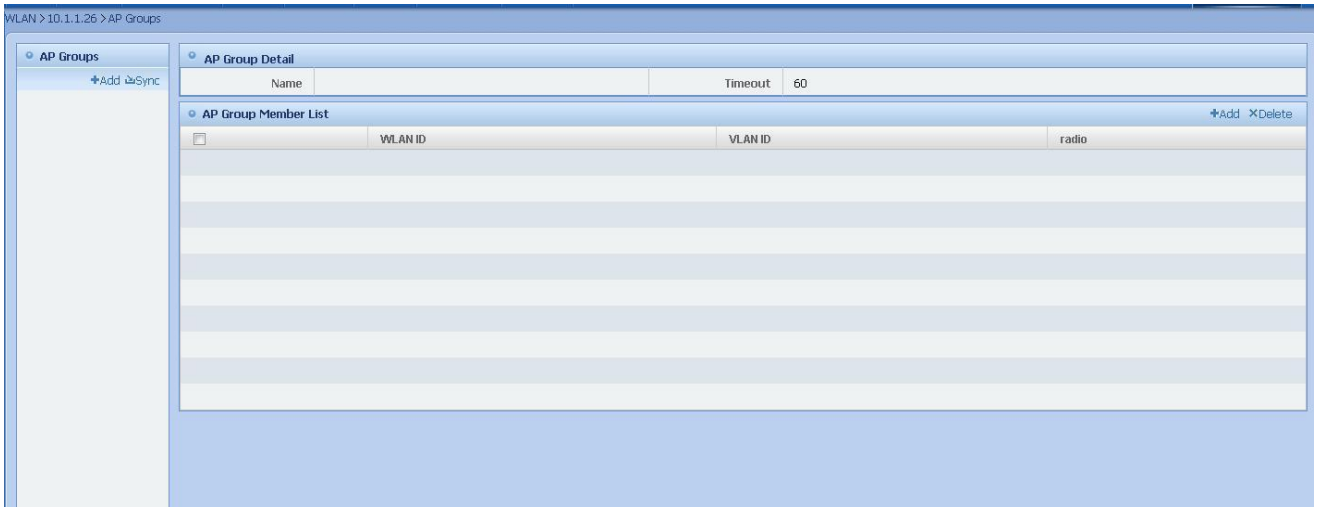


Figure 7.187. AP Group

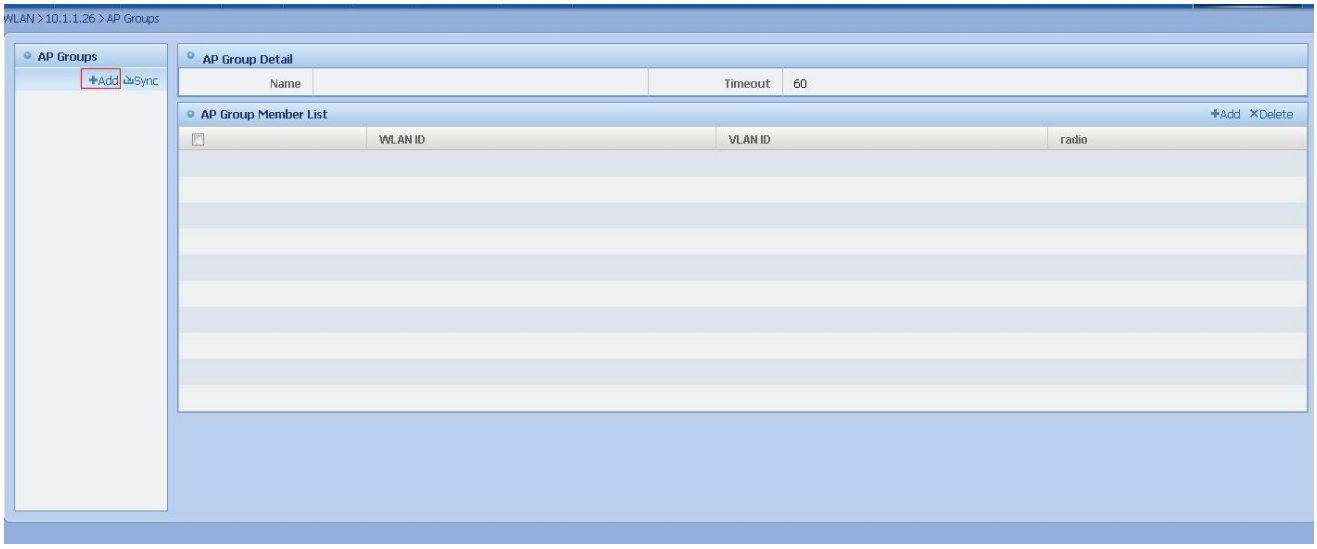


Figure 7.188. Adding AP Group

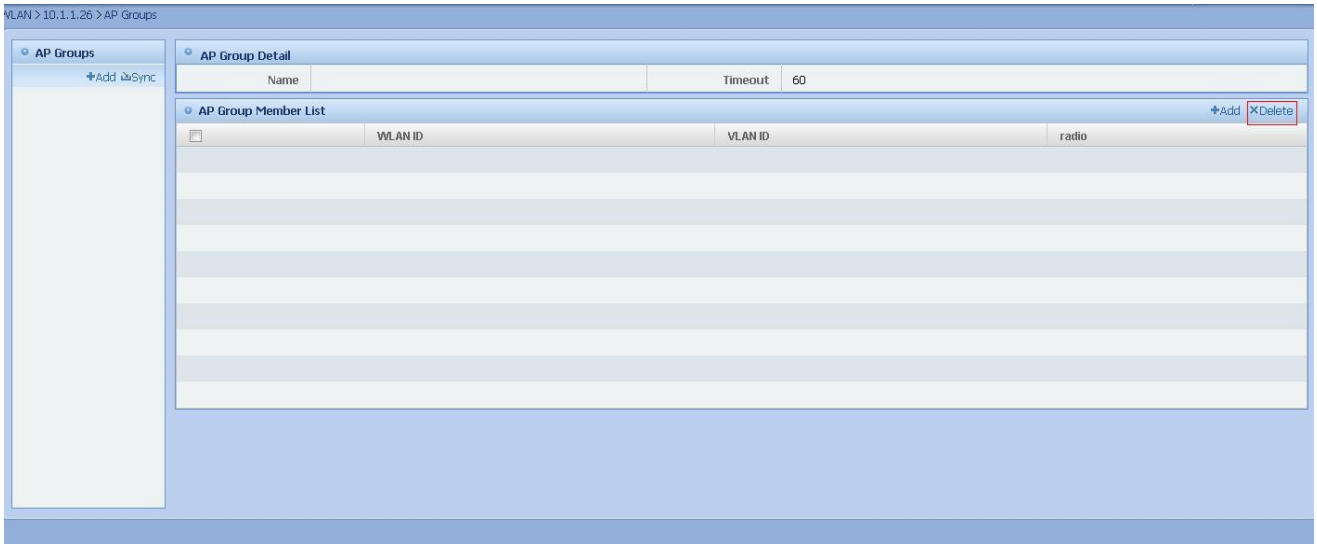


Figure 7.189. Deleting AP Group

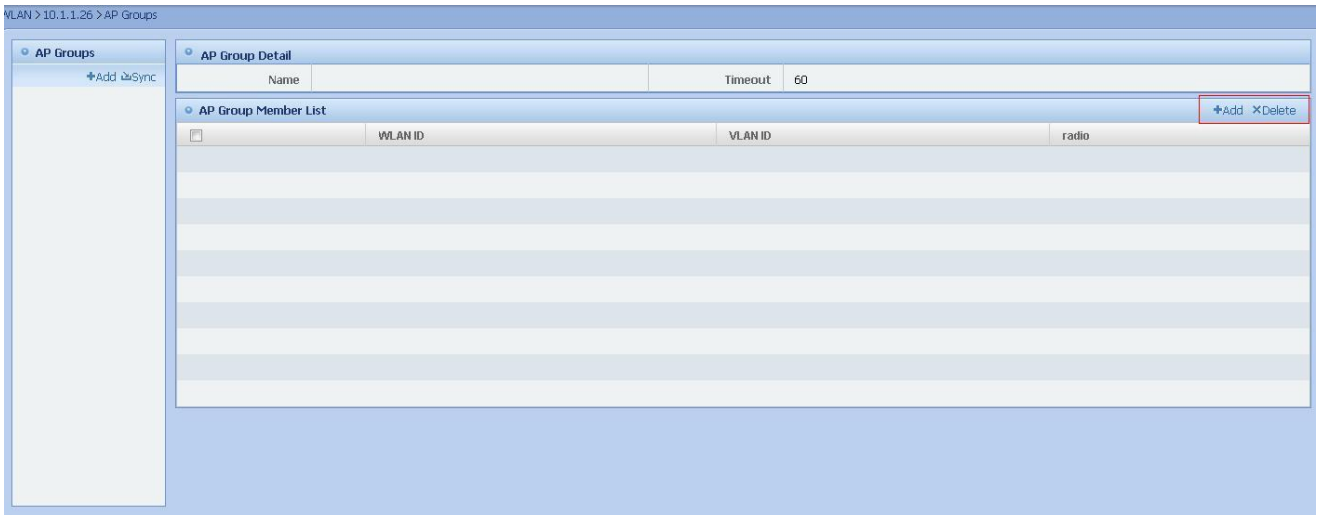


Figure 7.190. Adding and deleting group members on **AP Group Member List**

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.10. AP Group Configuration

This function enables you to view, modify and synchronize the relationships between APs and AP groups.

Operation Steps

49) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

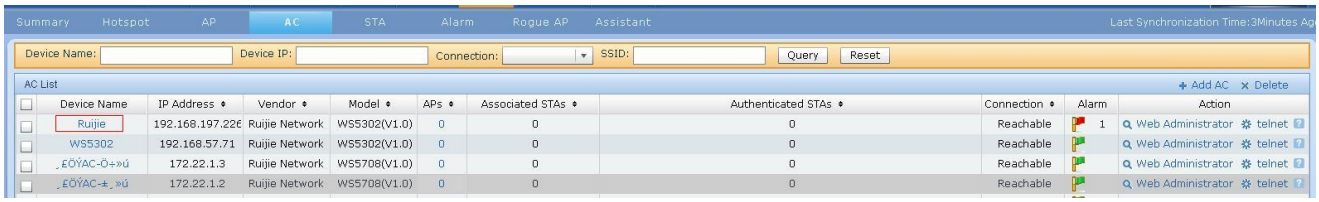


Figure 7.191. Going to **AC Details** Page

Click **Details**

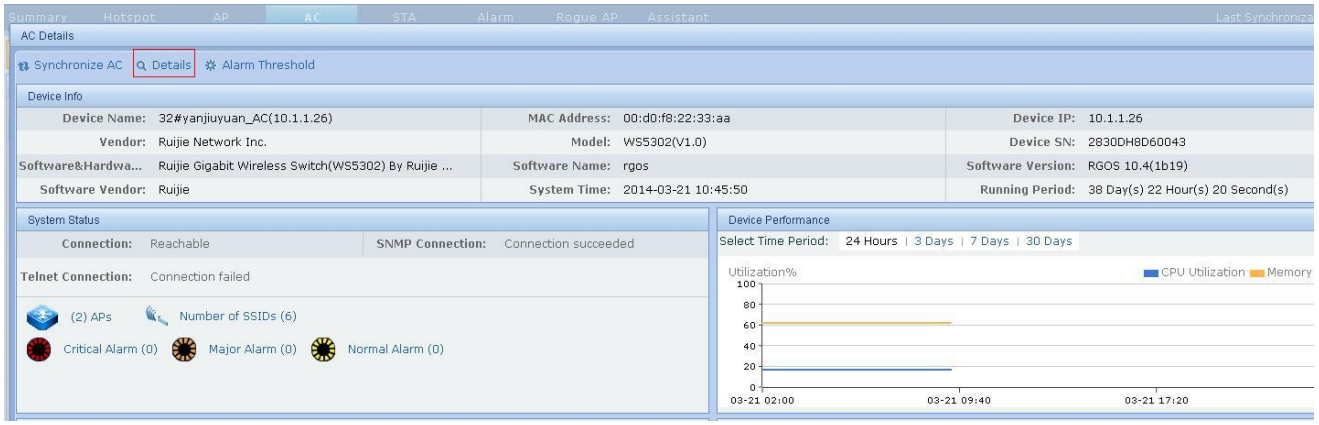


Figure 7.192. Details

In the **Controller** menu, unfold **WLAN**, and click **AP Group Configuration** to go to the **AP Group Configuration** page, as shown in the following figure:

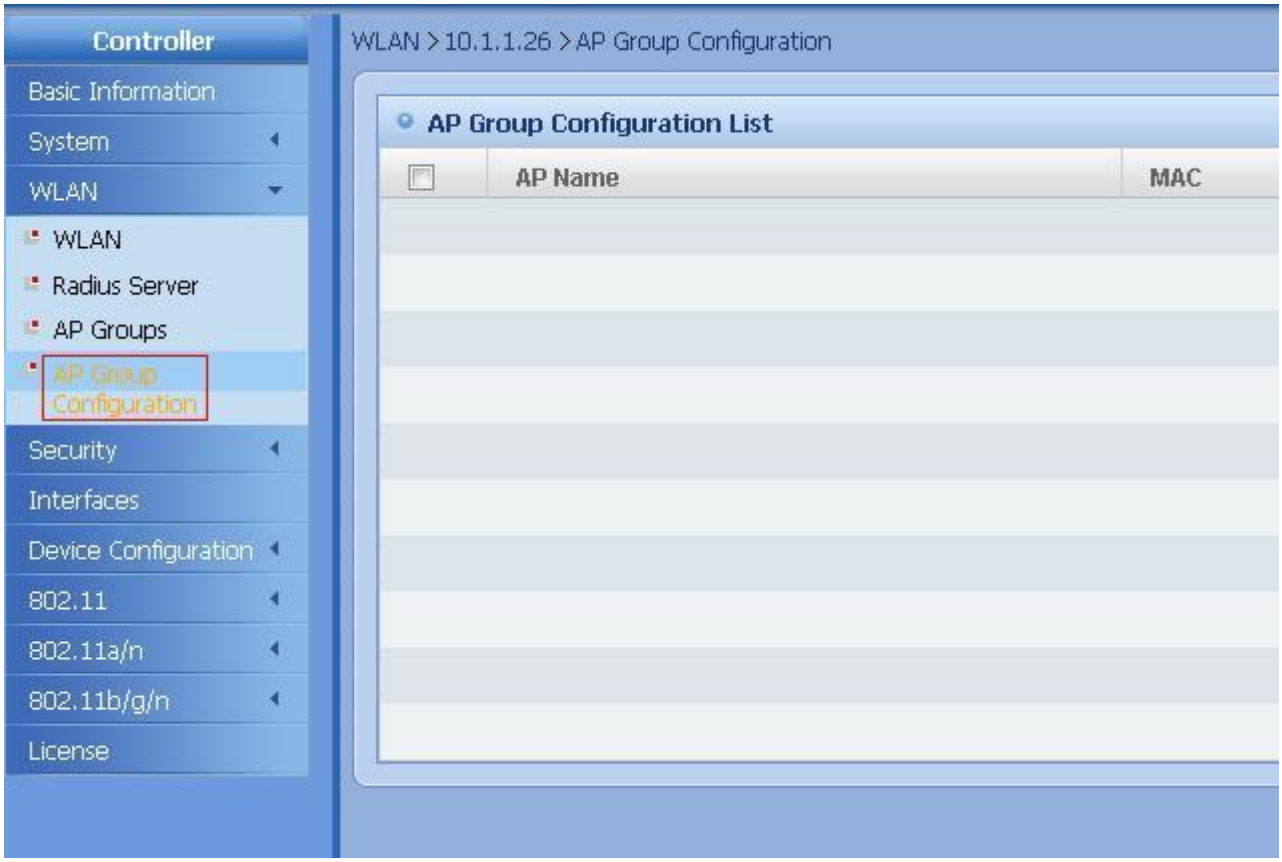


Figure 7.193. AP Group Configuration

You can view, modify and synchronize the relationships between APs and AP groups on **AP Group Configuration**, as shown in the following figure:

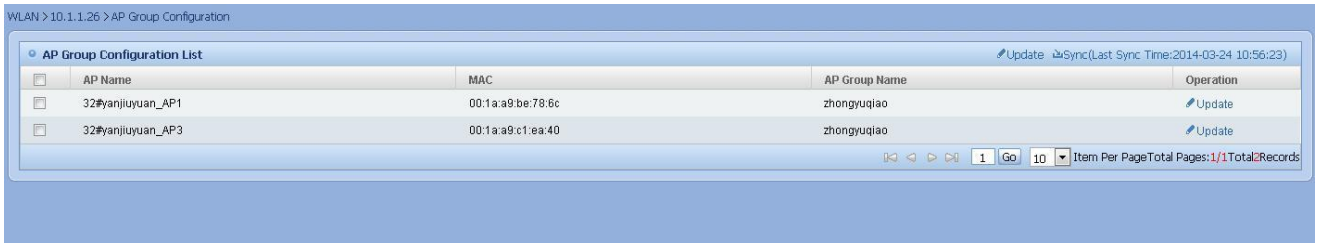


Figure 7.194. Viewing Relationships between APs and AP Groups

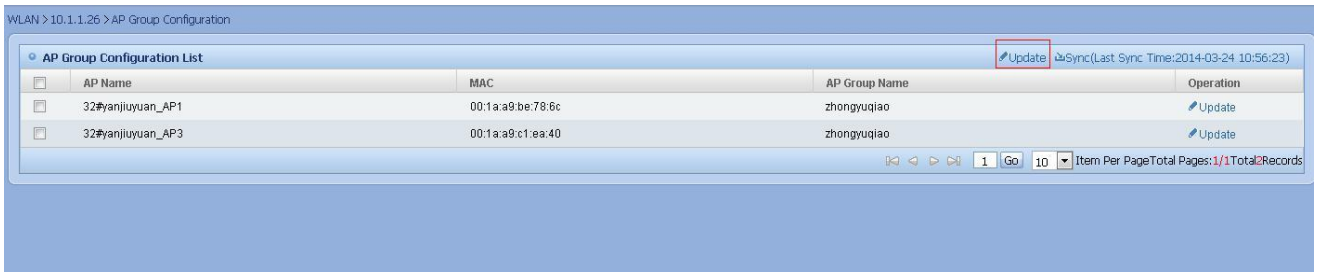


Figure 7.195. Modifying Relationships between APs and AP Groups

Figure 7.196. Synchronizing Relationships between APs and AP Groups

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.11. WIDS Configuration

This function enables you to configure WIDS on Rogue Device Detection.

Operation Steps

50) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

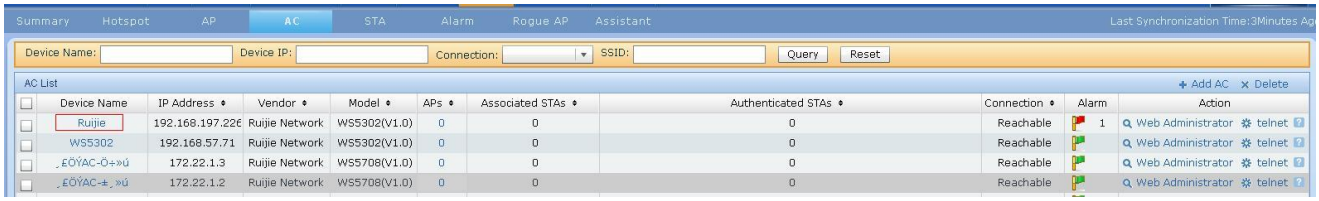


Figure 7.197. Going to **AC Details** Page

Click **Details**

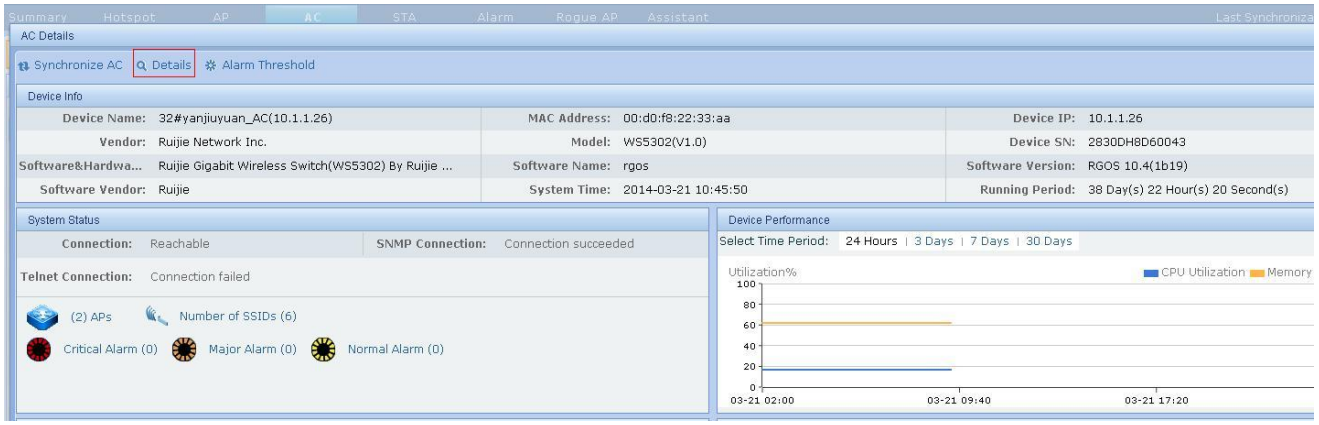


Figure 7.198. Details

In the **Controller** menu, unfold **Device Configuration**, and click **General** to go to the **General** page, as shown in the following figure:

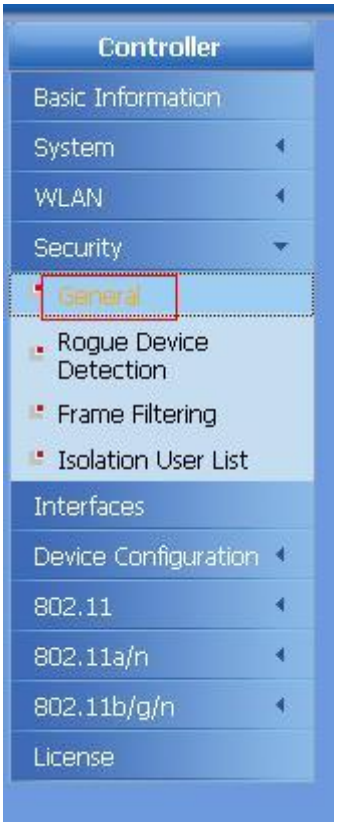


Figure 7.199. WIDS

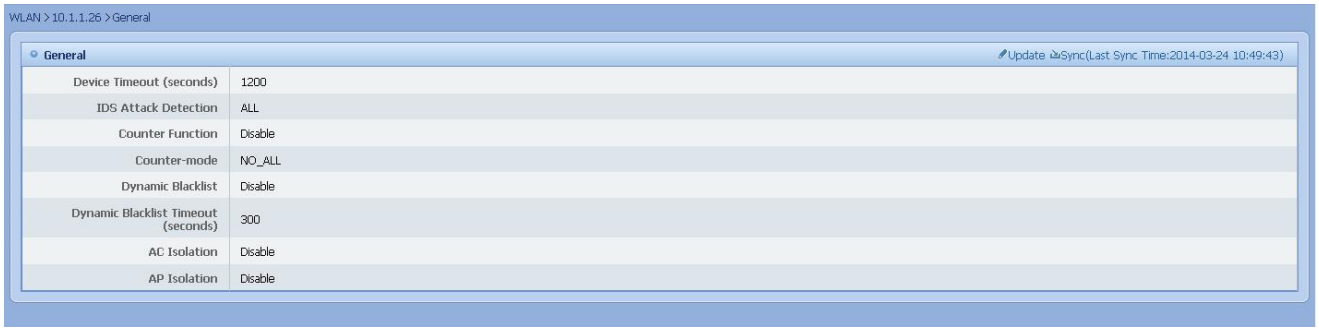


Figure 7.200. WIDS General Configuration

Rogue Device Detection is shown in the following figure:

Figure 7.201. Static Attack List

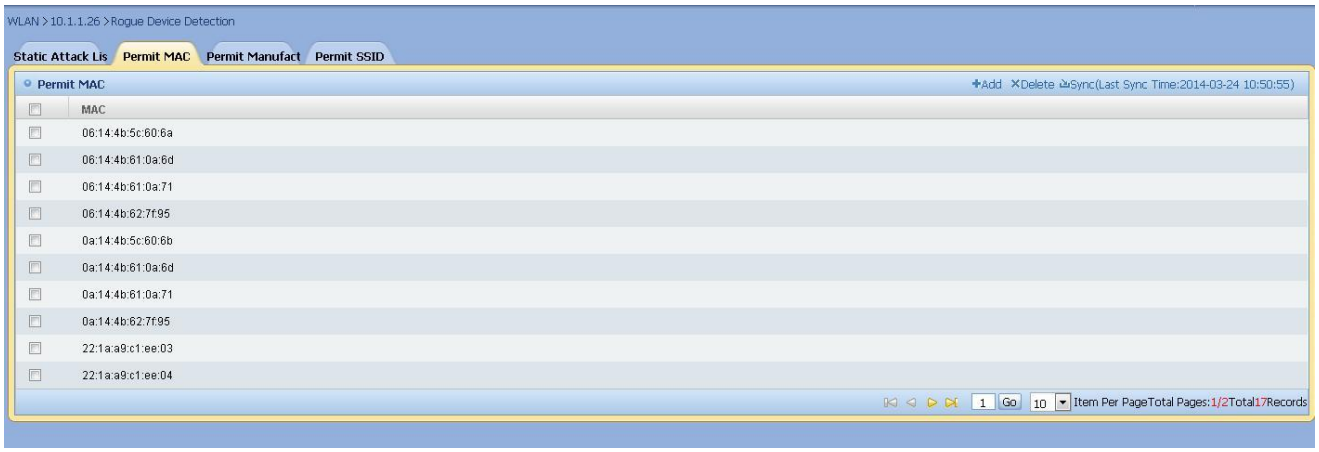


Figure 7.202. Permit MAC

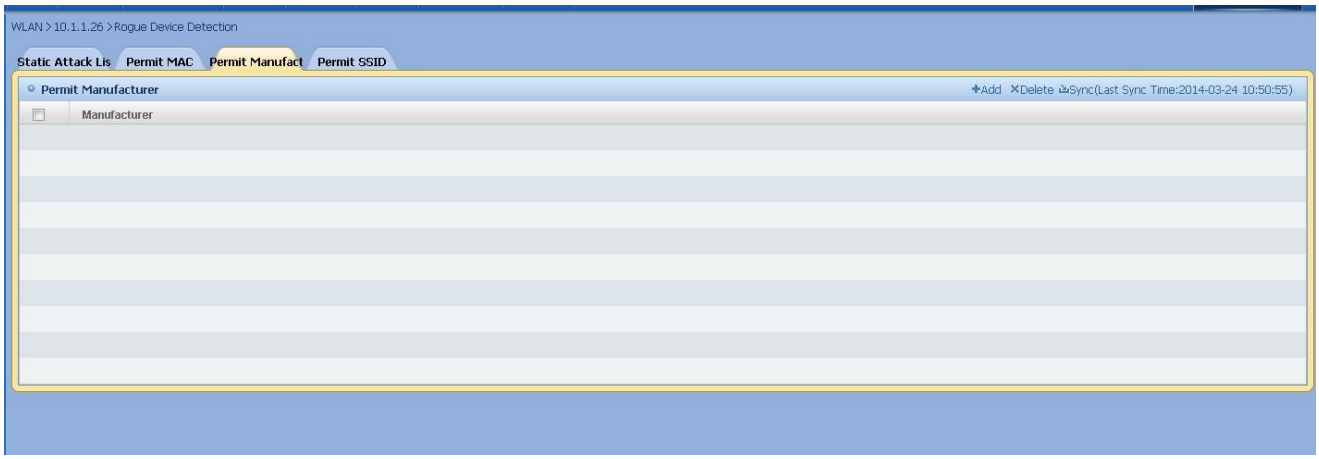


Figure 7.203. Permit Manufacturer

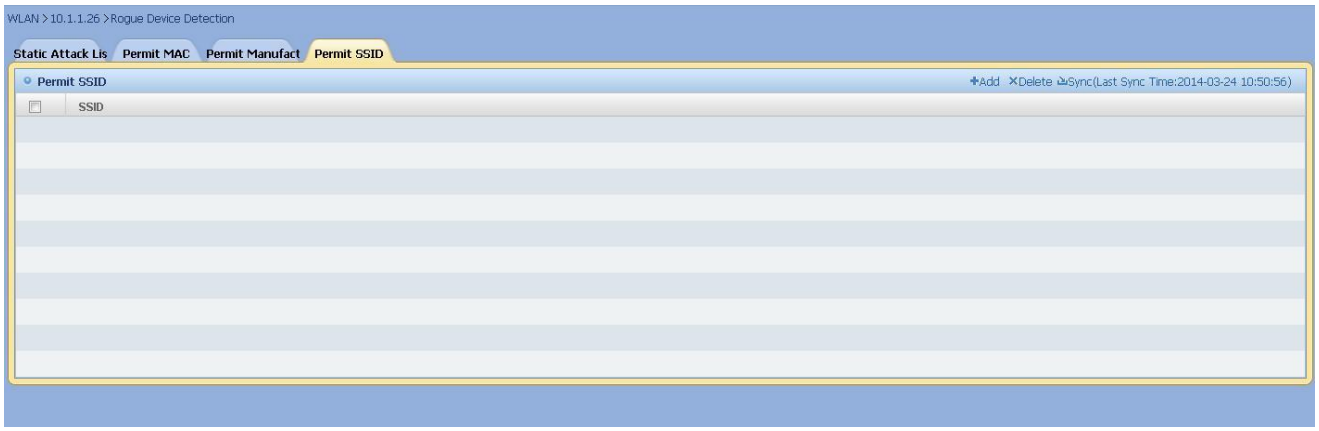


Figure 7.204. Permit SSID

Frame Filtering is shown in the following figure:

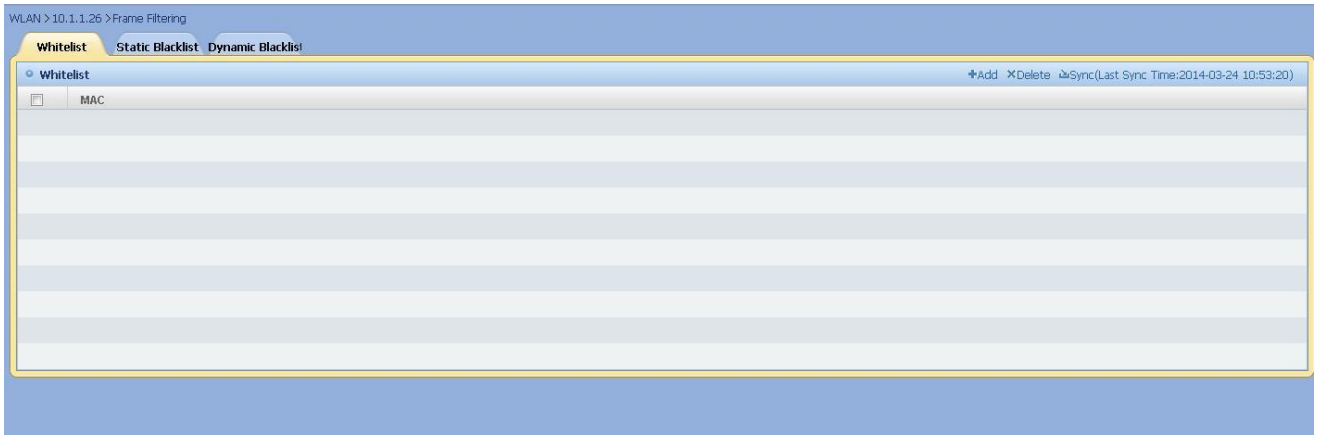


Figure 7.205. Whitelist

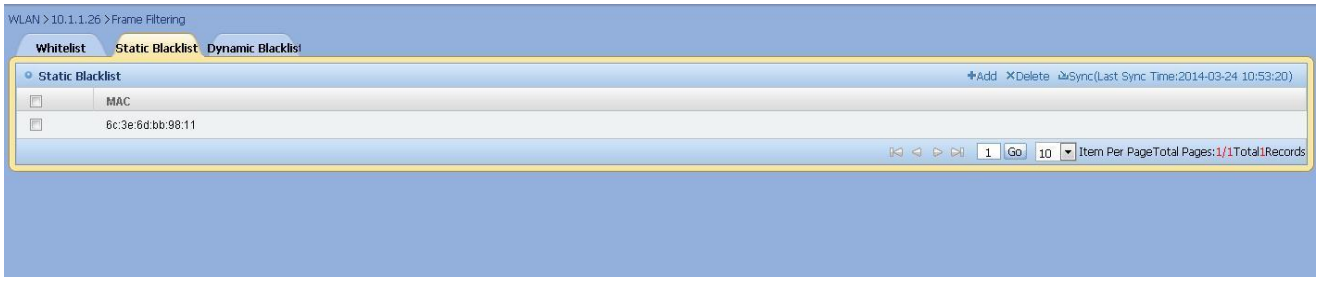


Figure 7.206. Static Blacklist

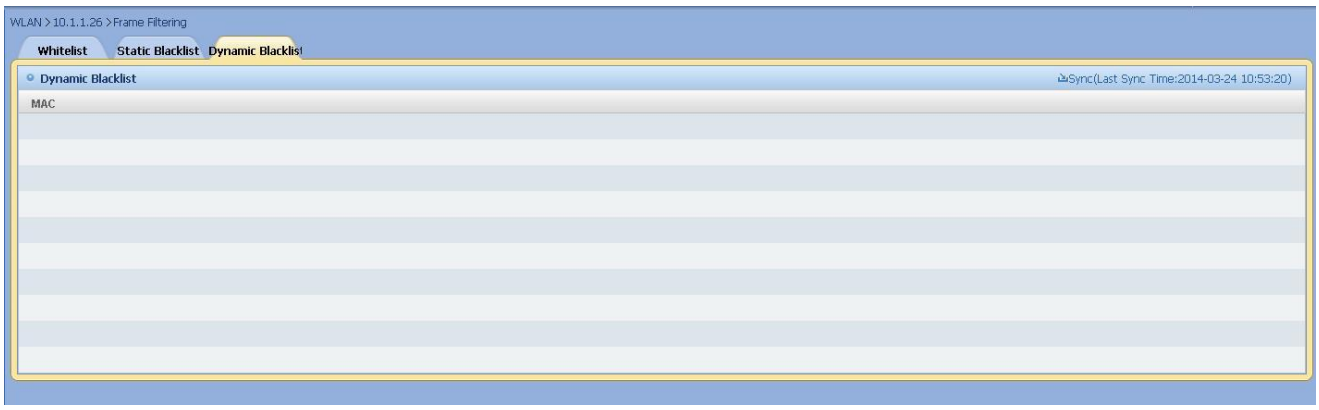


Figure 7.207. Dynamic Blacklist

Isolation User List is shown in the following figure:

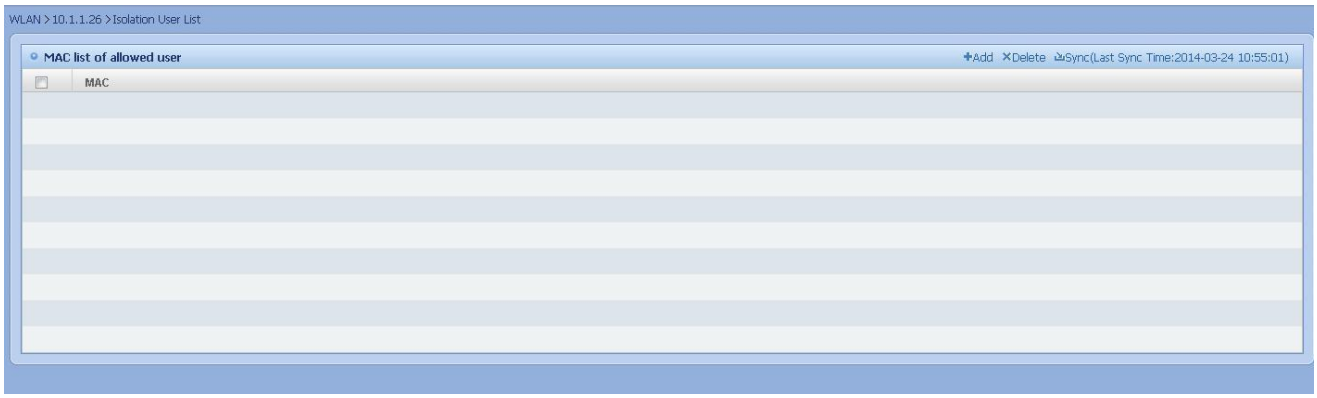


Figure 7.208. Isolation User List

Note To ensure that this function works properly, please make sure the TELNET Connectivity Status is connected.

7.4.5.1.12. Interface Configuration

This function enables you to configure interfaces and view interface details.

Operation Steps

51) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

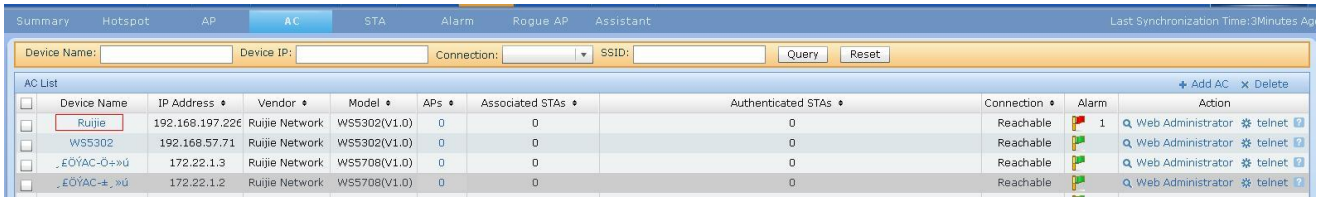


Figure 7.209. Going to **AC Details** Page

Click **Details**

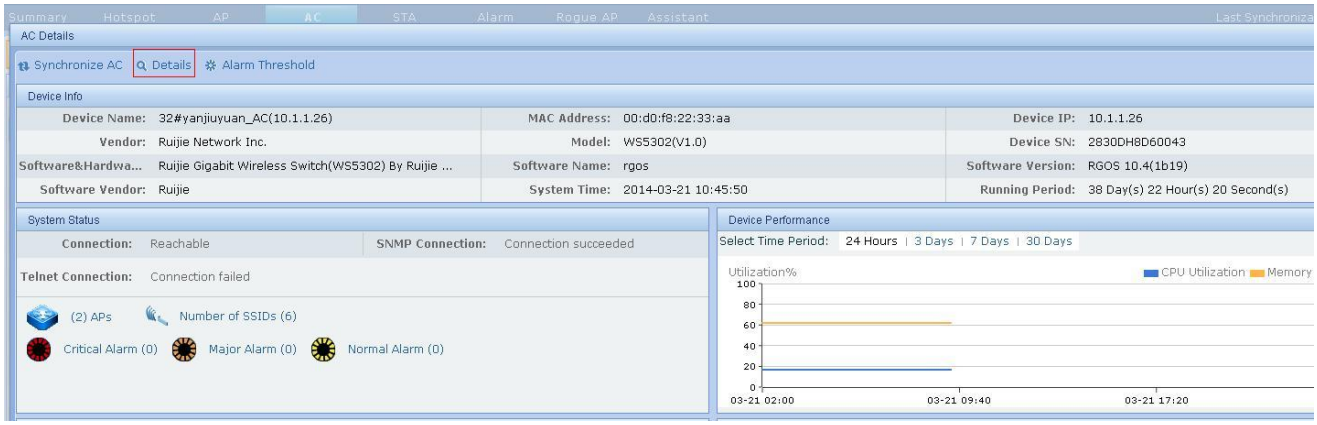


Figure 7.210. Details

Click **Interface Configuration** on the **Controller** menu, as shown in the following figure:

Figure 7.211. Clicking Interface Configuration

Click the button on **Operation** to perform the operation, as shown in the following figure:

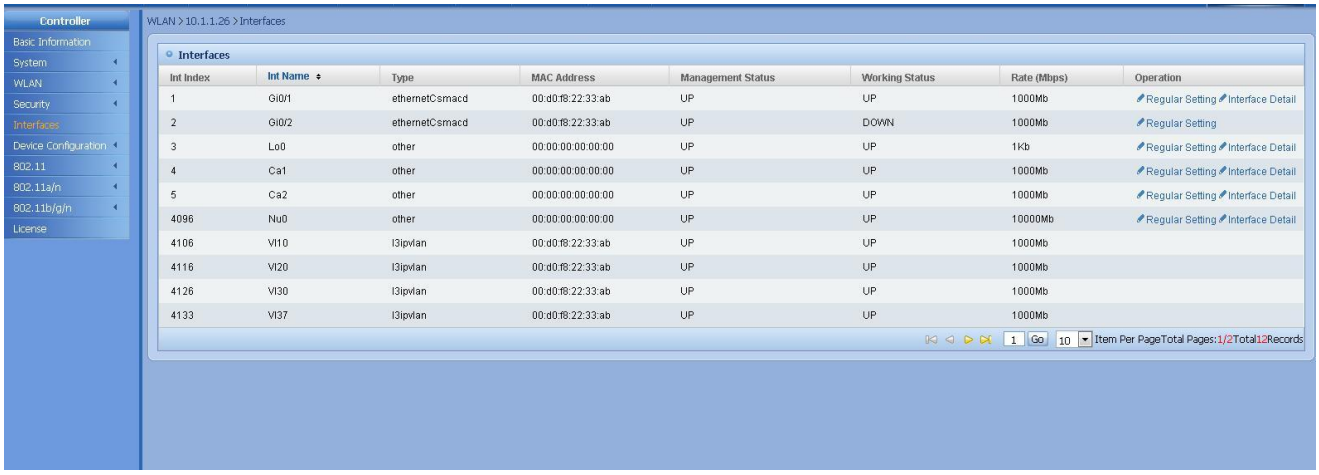


Figure 7.212. Interface Configuration

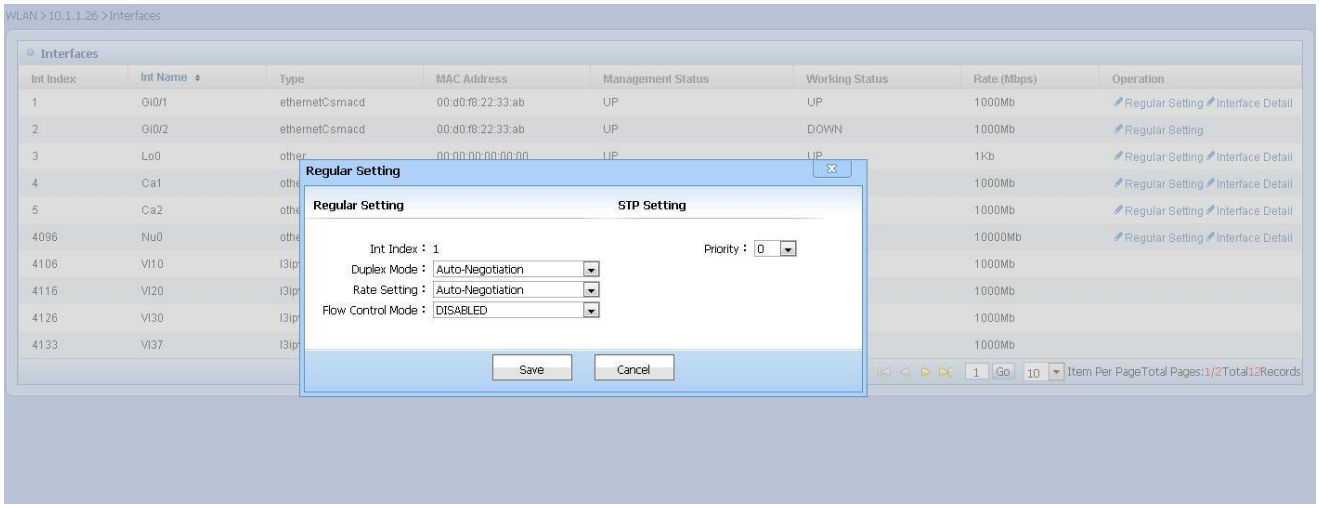


Figure 7.213. Regular Setting

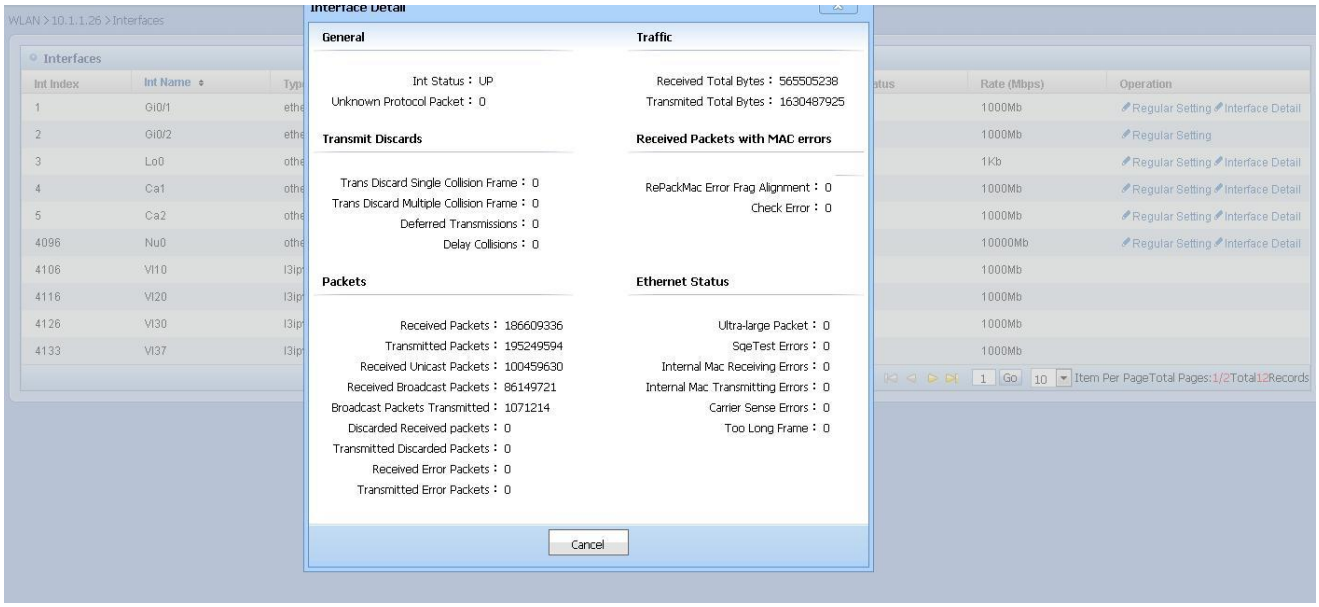


Figure 7.214. Interface Details

Note The regular setting and STP setting take effect only on physical ports.

7.4.5.1.13. Trap Receiver

This function enables you to add and delete the trap receiving server.

Operation Steps

52) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

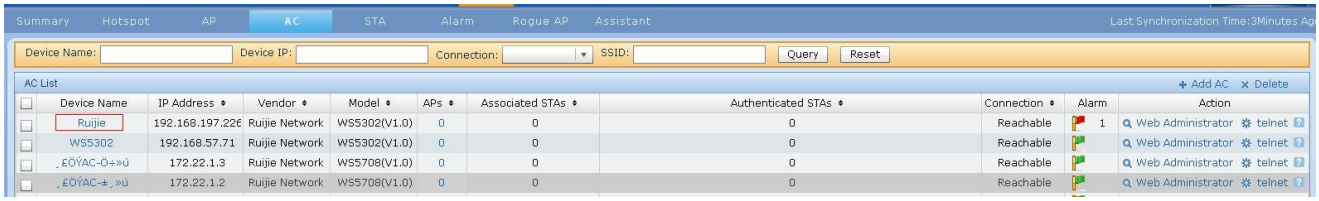


Figure 7.215. Going to **AC Details** Page

Click **Details**

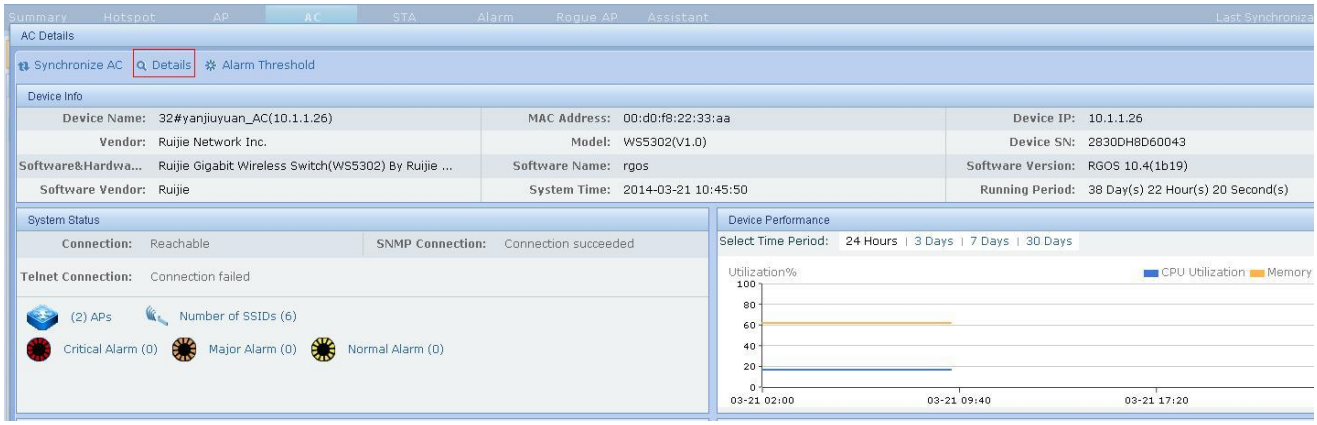


Figure 7.216. Details

In the **Controller** menu, unfold **Device Configuration**, and click **Trap Receiver** to go to the **Trap Receiver** page, as shown in the following figure:

Figure 7.217. Clicking Trap Receiver

You can add, delete and synchronize the trap receiving server on **Trap Receiver**, as shown in the following figure:

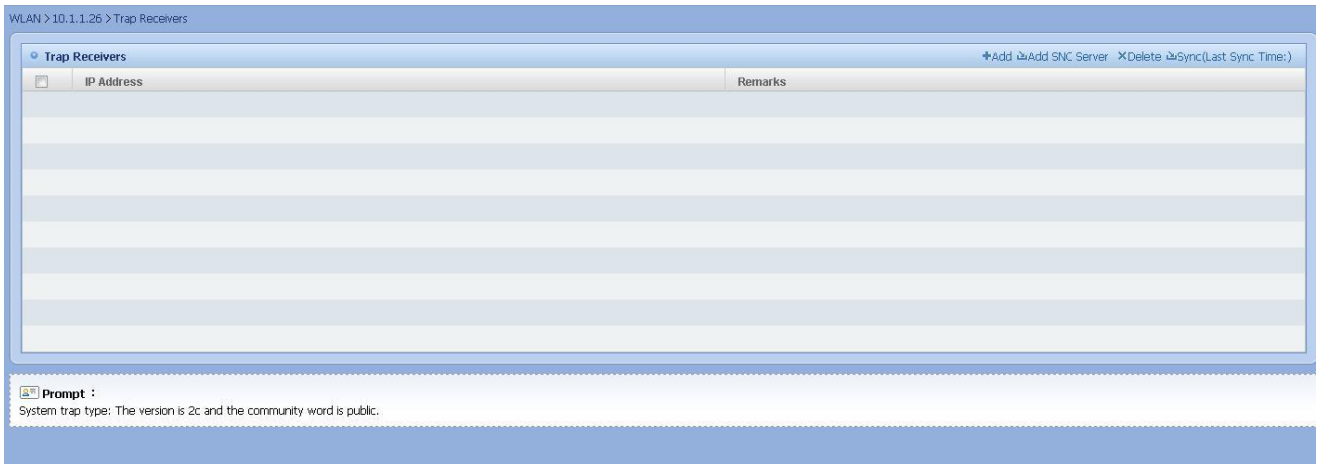


Figure 7.218. Trap Receiver

Note To ensure that this function works properly, please ensure the TELNET Connectivity Status is connected.

7.4.5.1.14. Trap Control

This function enables you to configure the type of sent Trap on **Trap Controller**.

Operation Steps

53) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

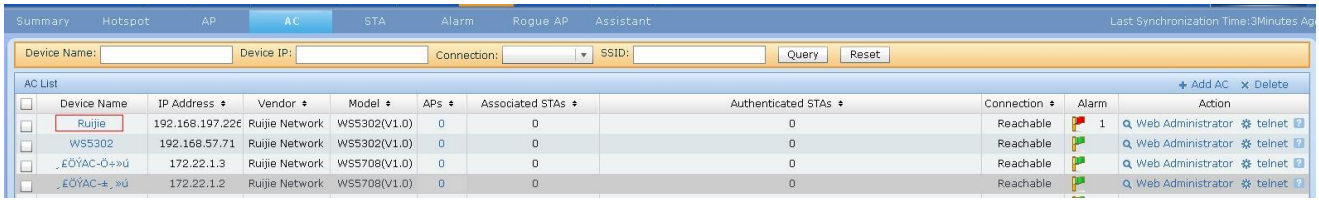


Figure 7.219. Going to **AC Details** Page

Click **Details**

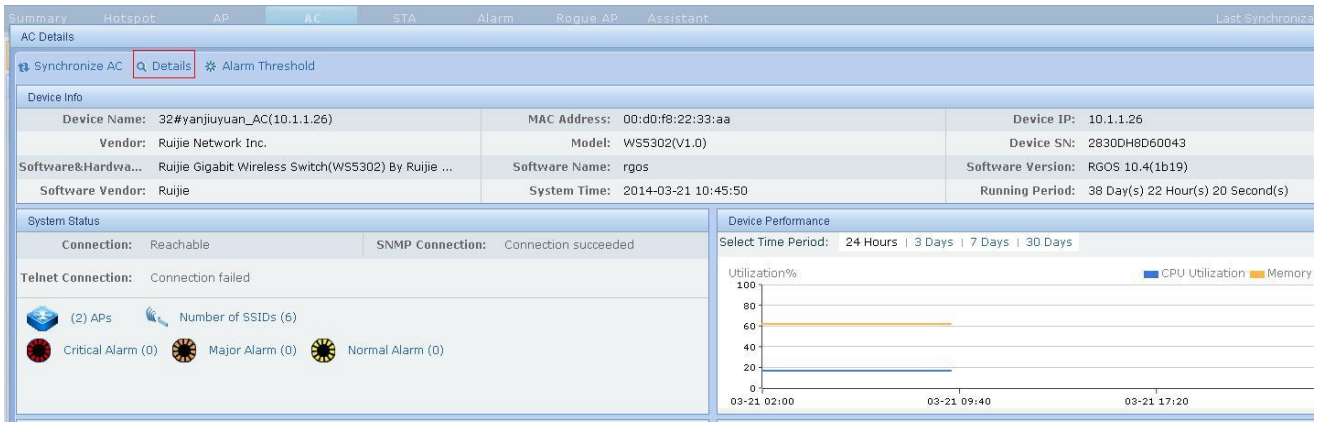


Figure 7.220. Details

In the **Controller** menu, unfold **Device Configuration**, and click **Trap Control** to go to the **Trap Control** page, as shown in the following figure:

Figure 7.221. Clicking Trap Control

You can modify and synchronize Trap parameters on **Trap Control**, as shown in the following figure:

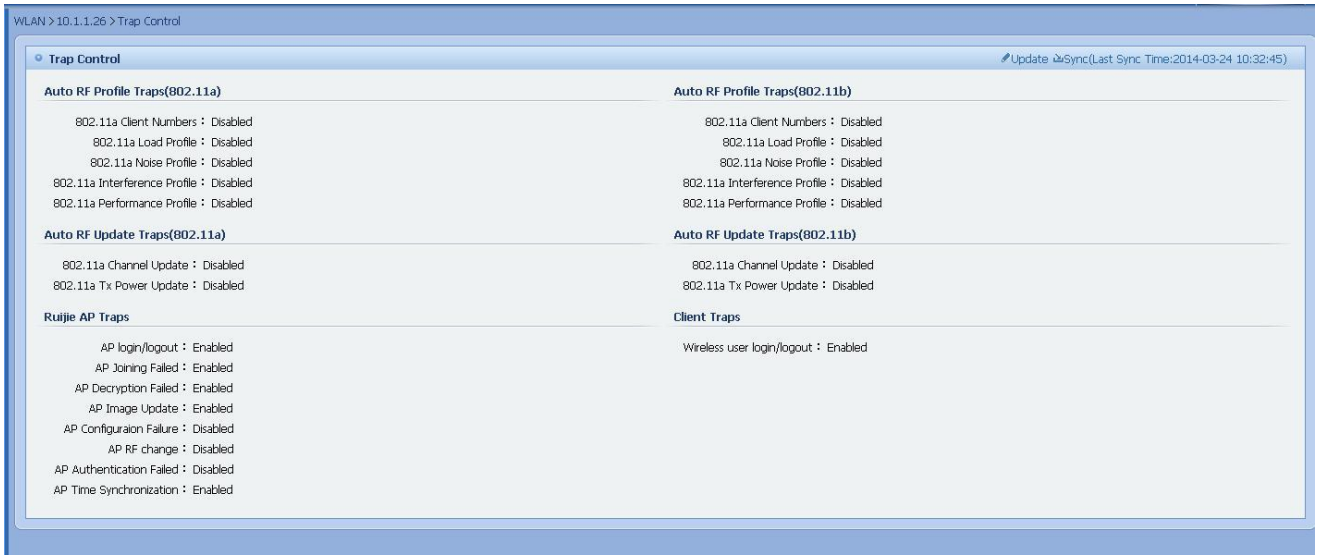


Figure 7.222. Trap Control

Note To ensure that this function works properly, please make sure the TELNET Connectivity Status is connected.

7.4.5.1.15. Syslog Receiver

Add and delete device log receiver server info.

Operation Steps

54) Go to **Controlle**r list page, and click **IP** link of certain device in device list to enter basic information page of the device, as shown below:

Figure 7.223. Enter Device Basic Information Page

In Wireless controller configuration navigation bar, expand **Device Configuration**, and click **Syslog Receiver** to enter Syslog receiver configuration page, as shown below:

Figure 7.224. Select Syslog Receiver

Addition, deletion and synchronization operations can be performed on syslog receiver server. As shown below:

Figure 7.225. Syslog Receiver List

Note To make this function work properly, please make sure that Telnet connection status is connectable.

7.4.5.1.16. Configure IGMP Snooping

This function enables you to perform IGMP Snooping configuration and view L2 multicast forwarding table (GDA).

Operation Steps

55) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

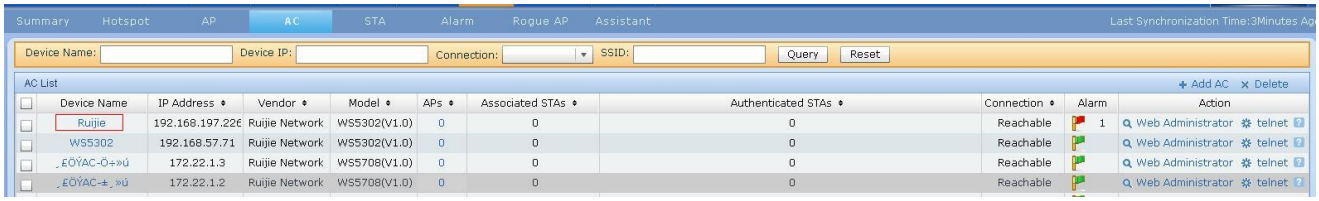


Figure 7.226. Going to AC details

Click **Details**

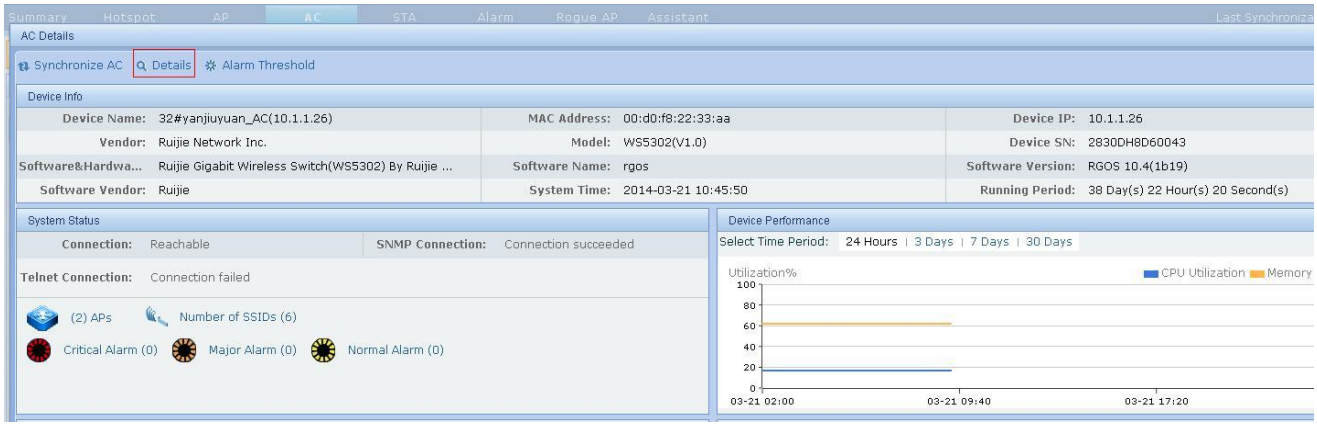


Figure 7.227. Details

Click **IGMP Snooping Configuration** on the **Controller** menu, as shown in the following figure, to go to the **IGMP Snooping Configuration** page:

Figure 7.228. Clicking IGMP Snooping Configuration

The **IGMP Snooping Configuration** page consists of **Working Mode Configuration** and **GDA**, as shown in the following figure:

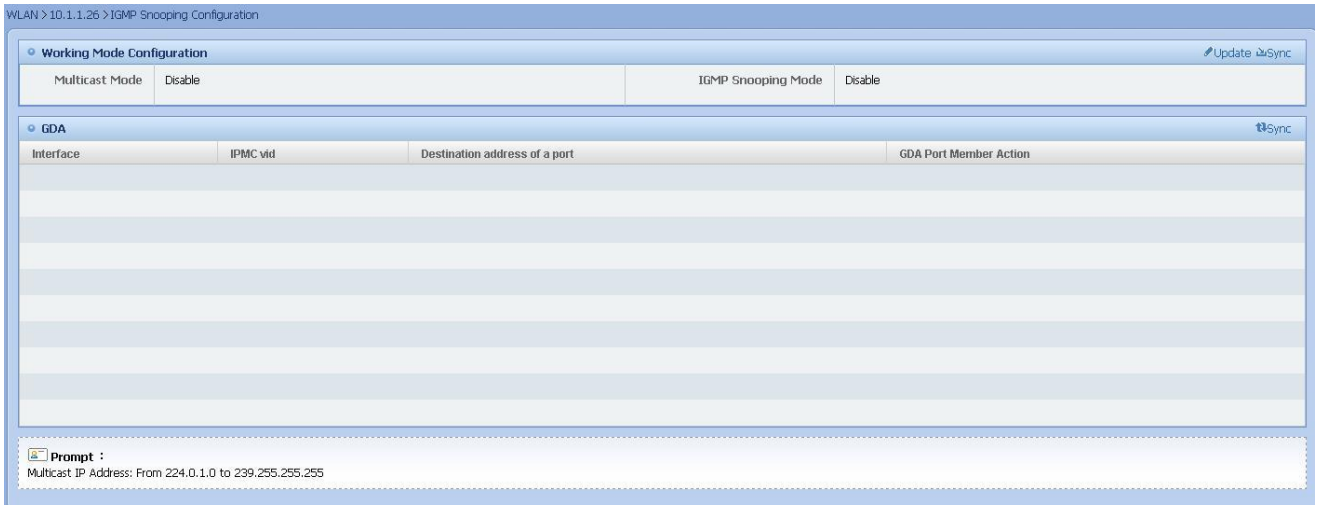


Figure 7.229. IGMP Snooping Configuration

You can modify IGMP Snooping properties on **IGMP Snooping Configuration** and click **Modify** to submit the modification.

Note To ensure that this function works properly, please make sure the SNMP Connectivity Status is connected.

7.4.5.1.17. Country/Area Code

This function enables you to perform Country/Area Code configuration on AC.

Operation Steps

56) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

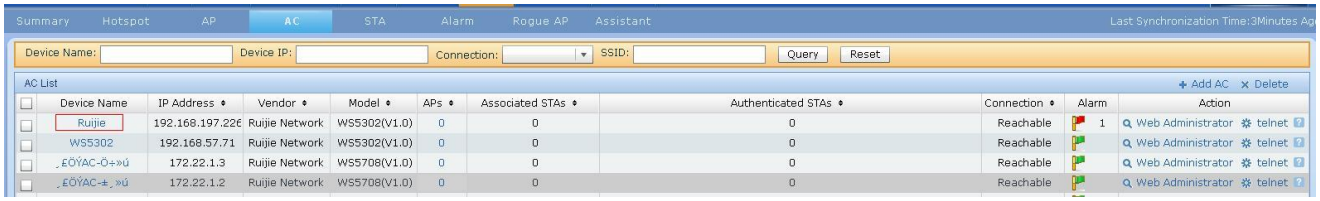


Figure 7.230. Going to **AC Details** Page

Click **Details**

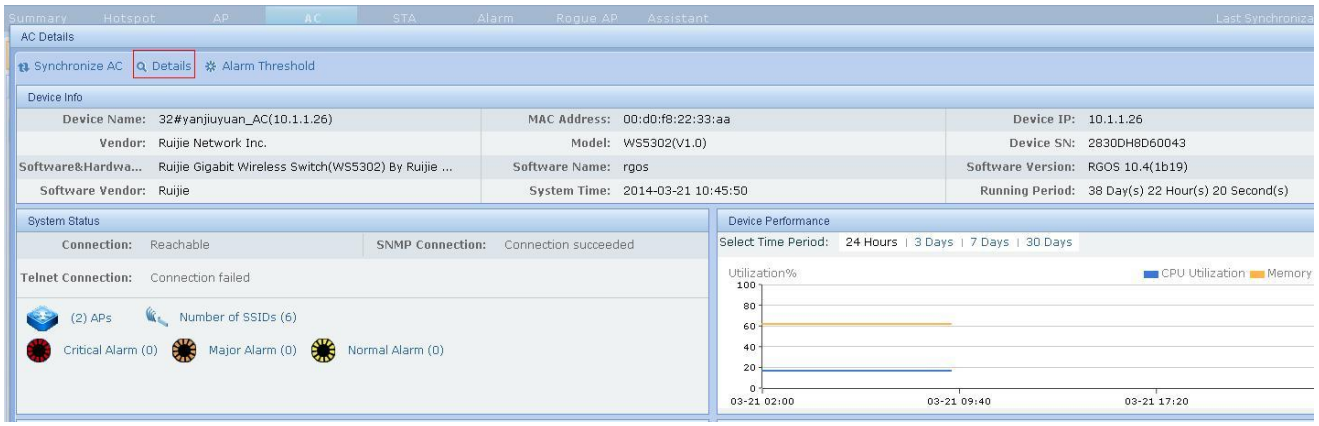


Figure 7.231. Details

Go to the **Controller** page, and select **Country/Area Code** in the menu on the left, as shown in the following figure:

Figure 7.232. Country/Area Code

Country/Area code configuration information is displayed.

Figure 7.233. Country/Area Code Configuration

Click **Save**, and the data will be saved on the system and device.

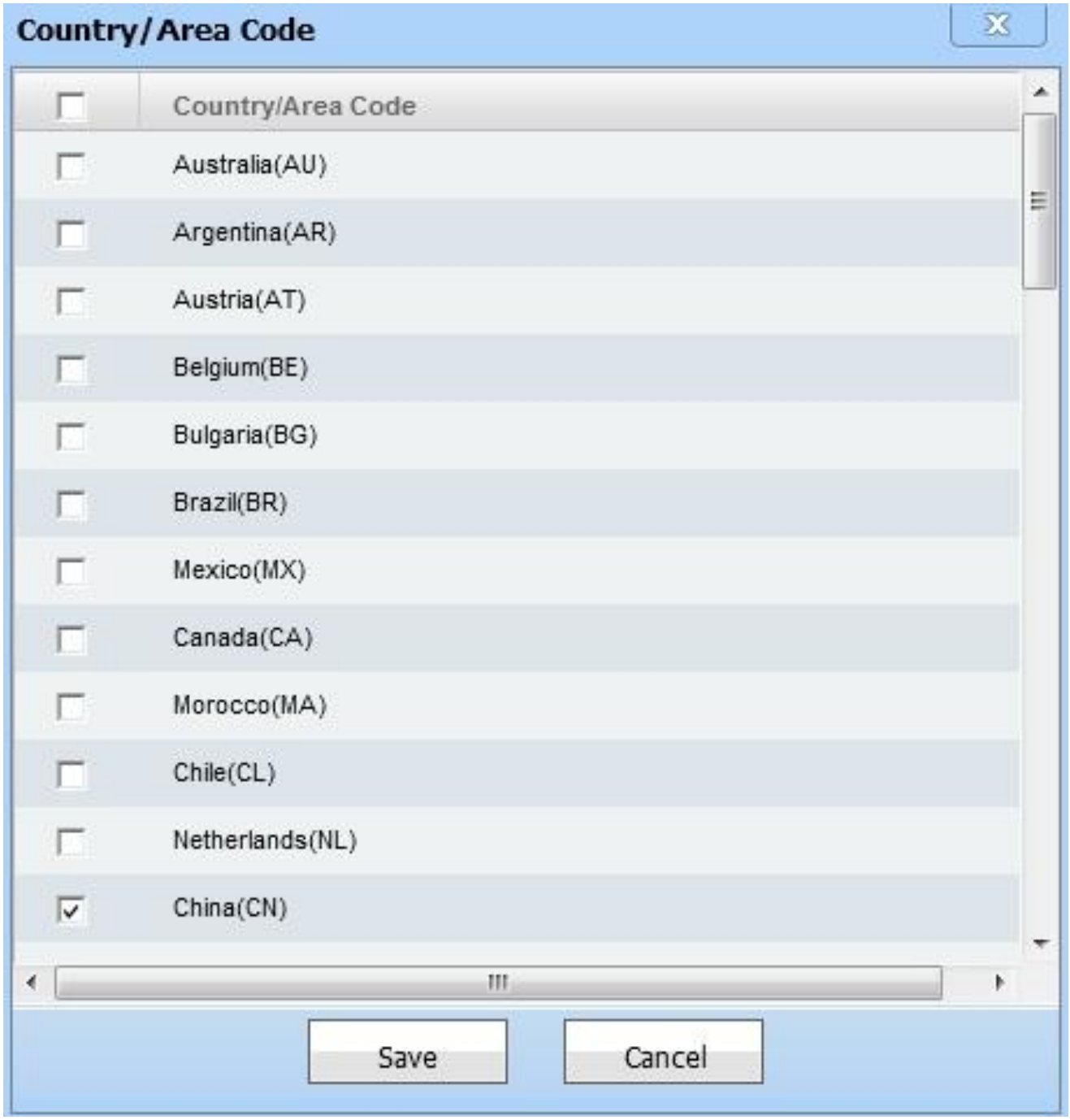


Figure 7.234. Country/Area code Modification

Note This function modifies both devices and network management system.

7.4.5.1.18. 802.11a/n Configuration

This function enables you to perform 802.11a/n configuration on AC.

Operation Steps

57) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

58)

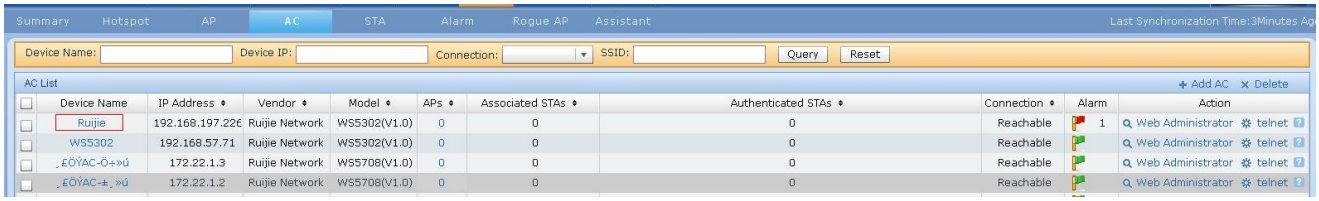


Figure 7.235. Going to **AC Details** Page

Click **Details**

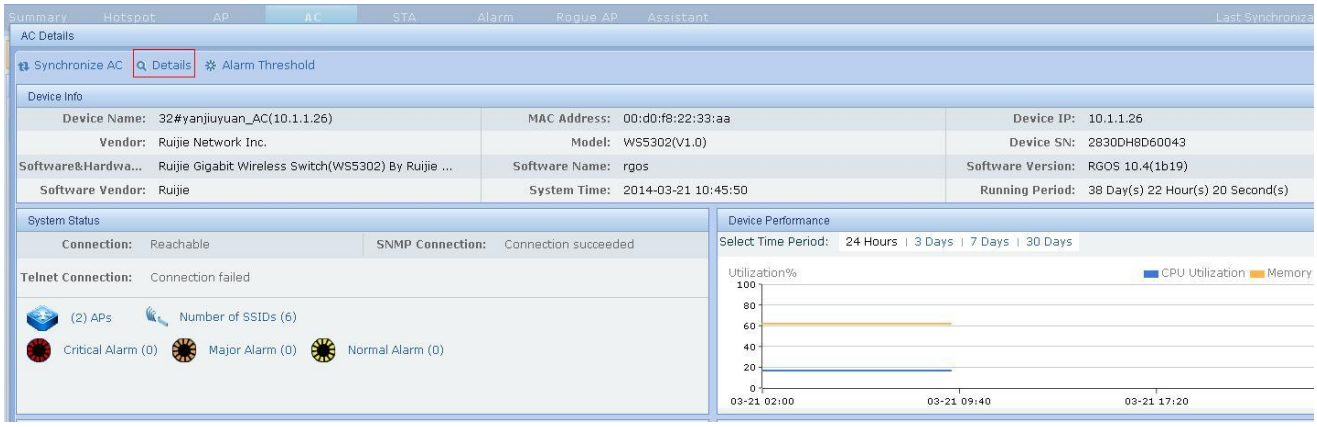


Figure 7.236. Details

Go to the **Controller** page, and select 802.11a/n in the menu on the left, as shown in the following figure:

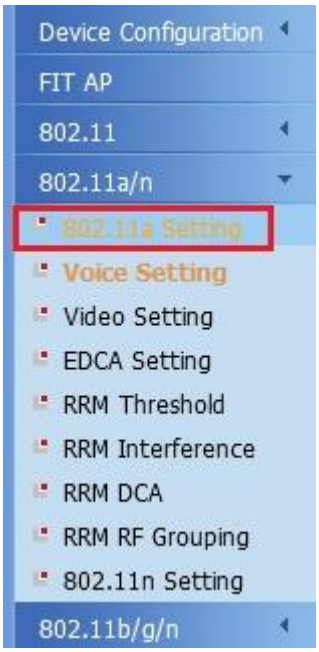


Figure 7.237. 802.11a/n Configuration

The 802.11a/n setting information is displayed, as shown in the following figure:

Figure 7.238. 802.11a/n Configuration

Click **Save**, and the data will be saved on the system and device.

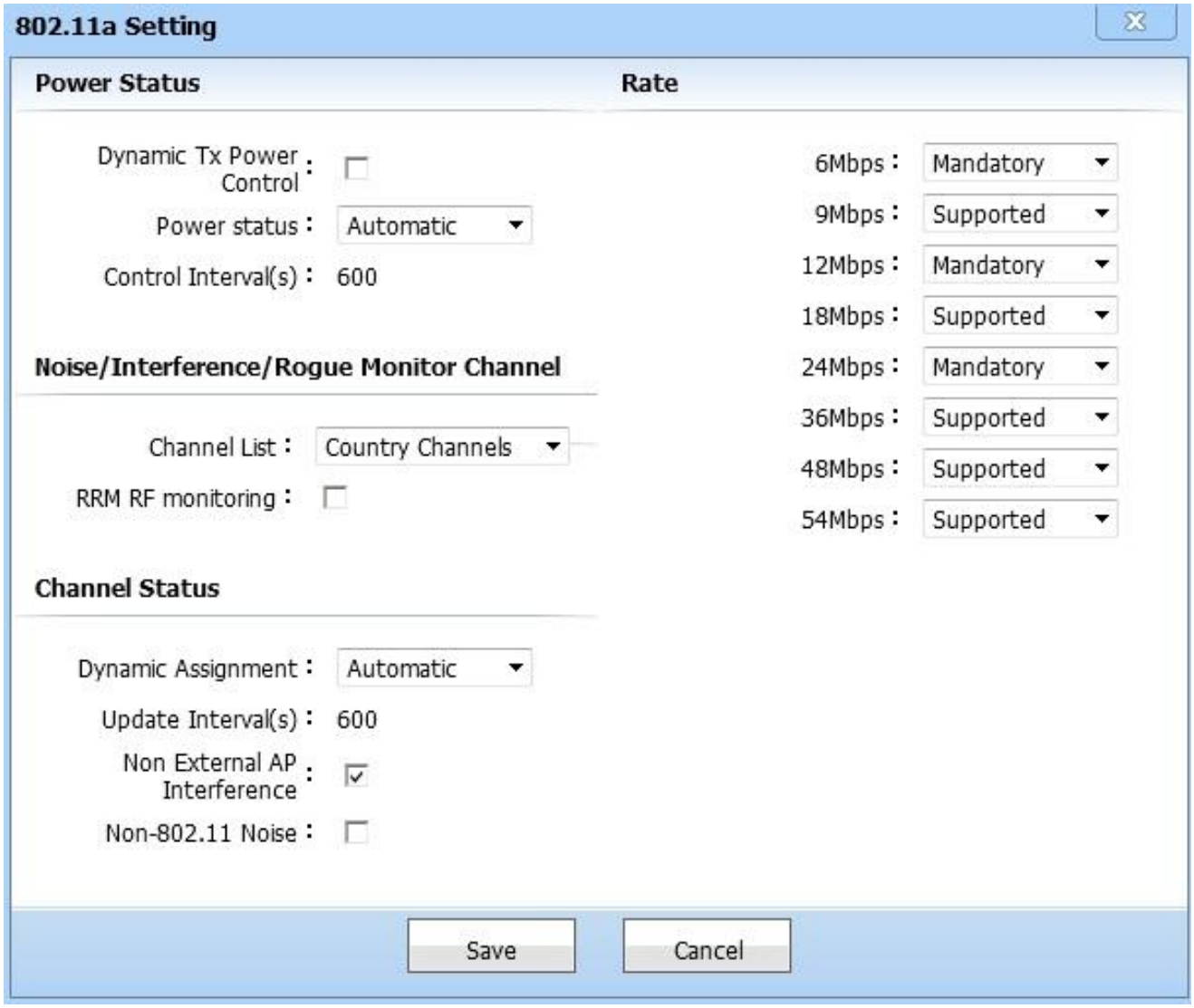


Figure 7.239. 802.11a/n Configuration

Note

This function modifies the device and updates network management system.
802.11b/g/n parameter modification is similar to 802.11a/n parameter modification. 80211b/g/n

7.4.5.1.19. EDCA Configuration

This function enables you to perform 802.11 EDCA configuration on AC.

Operation Steps

59) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

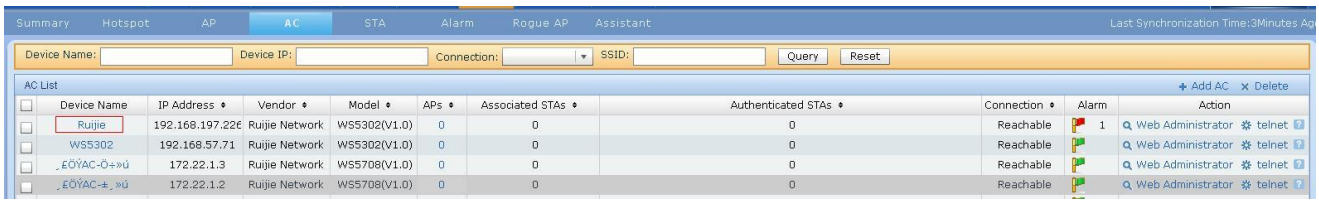


Figure 7.240. Going to AC Details Page

Click **Details**

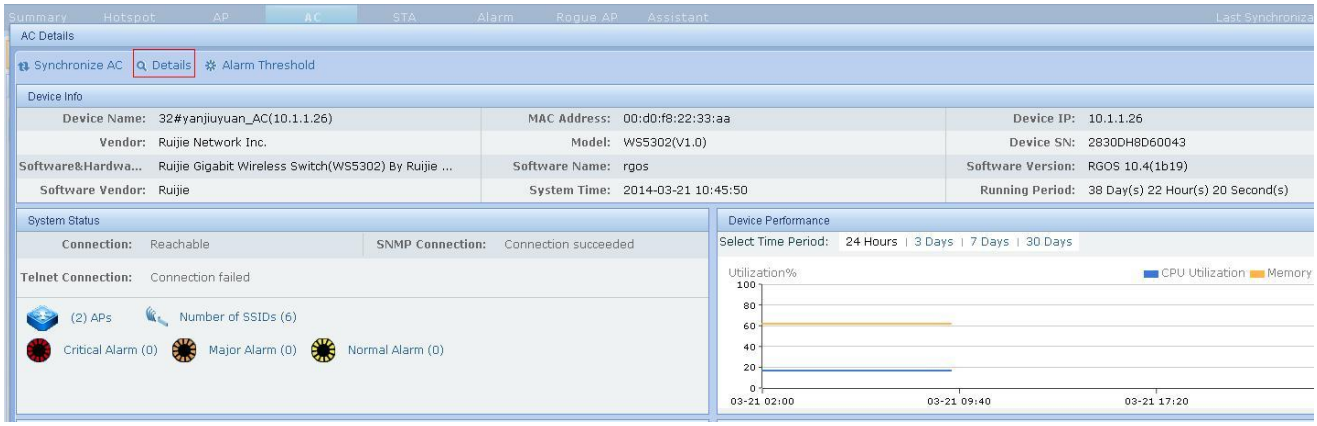


Figure 7.241. Details

Go to the **Controller** page, and select **EDCA Setting** in 802.11a/n on the left, as shown in the following figure:

Figure 7.242. EDCA Setting Menu

The EDCA setting information is displayed, as shown in the following figure:

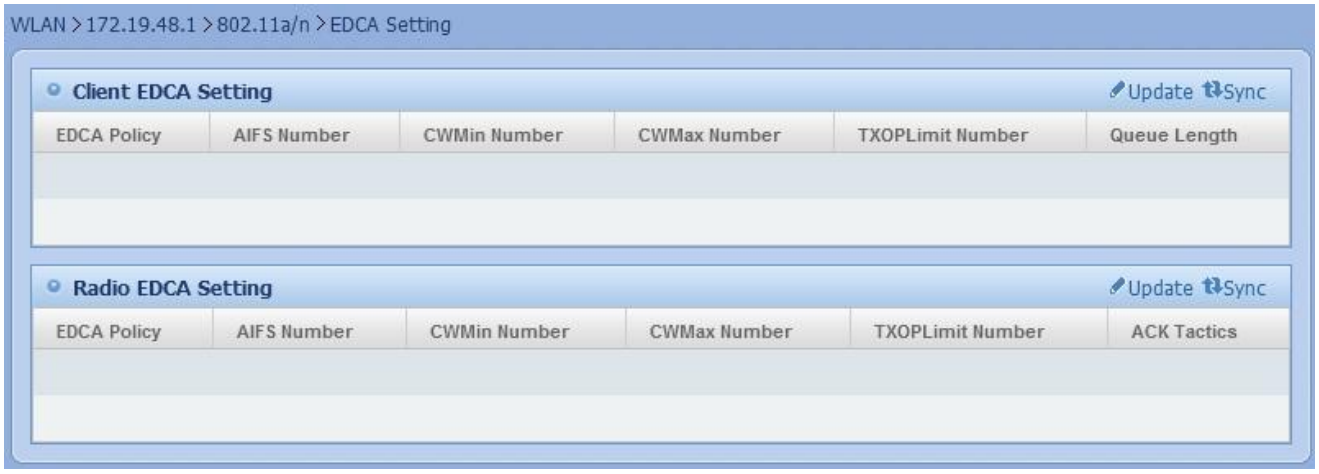


Figure 7.243. EDCA Setting

Click **Modify** to modify EDCA configuration information, as shown in the following figure:

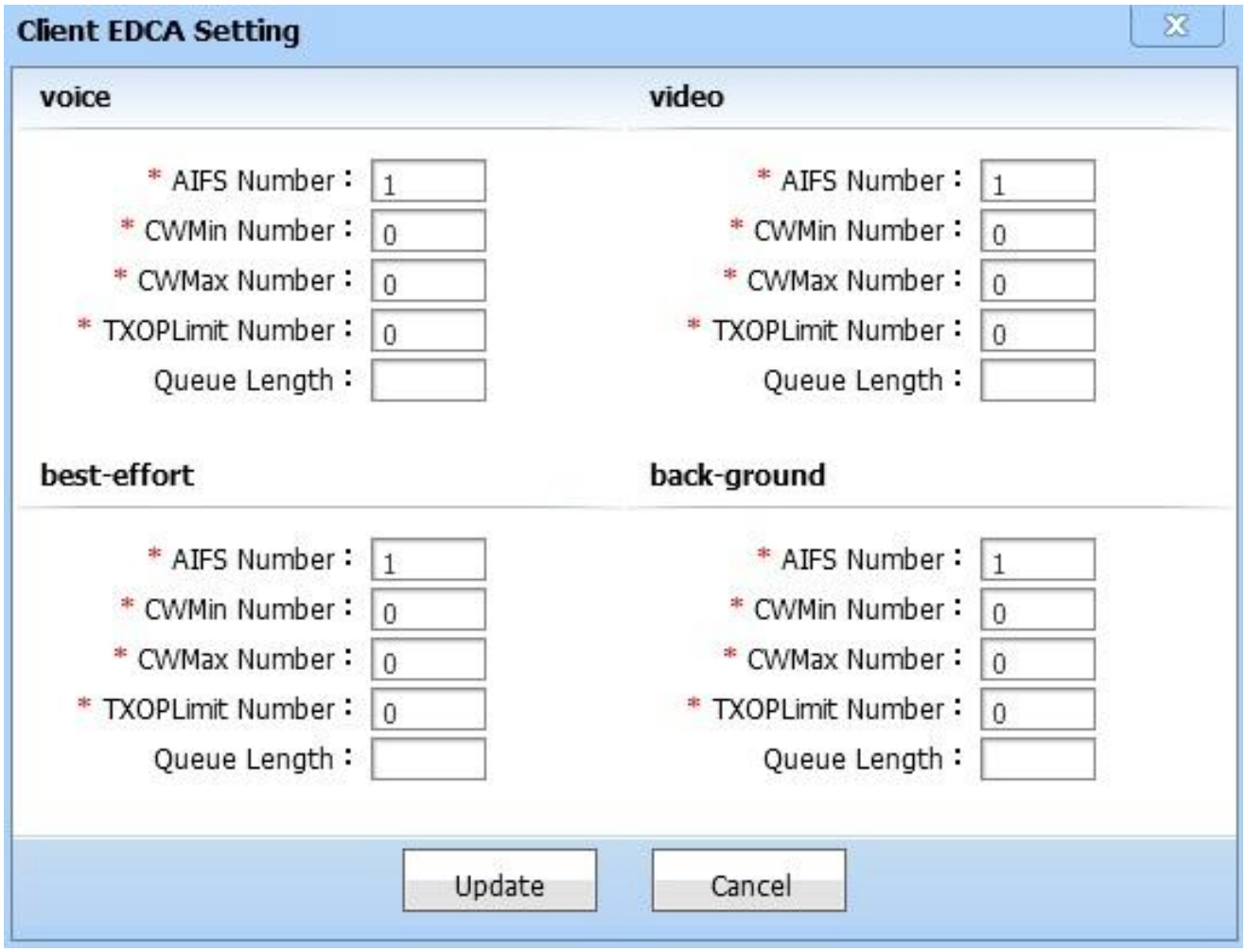


Figure 7.244. EDCA Modification

Note 802.11b/g/n EDCA Configuration is similar to 802.11 EDCA configuration.

7.4.5.1.20. RRM Threshold

This function enables you to perform RRM Threshold configuration on AC.

Operation Steps

60) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

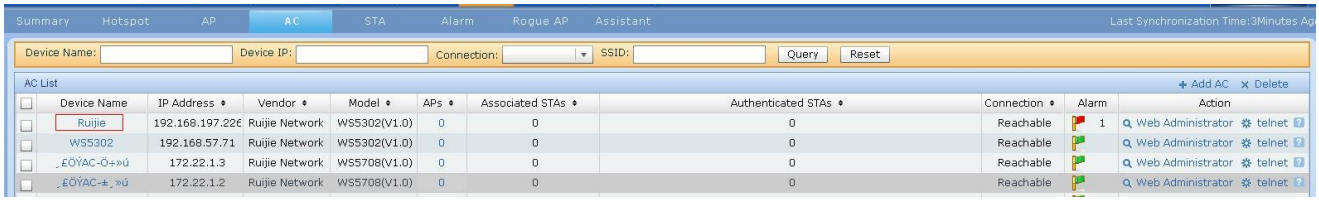


Figure 7.245. Going to **AC Details** Page

Click **Details**

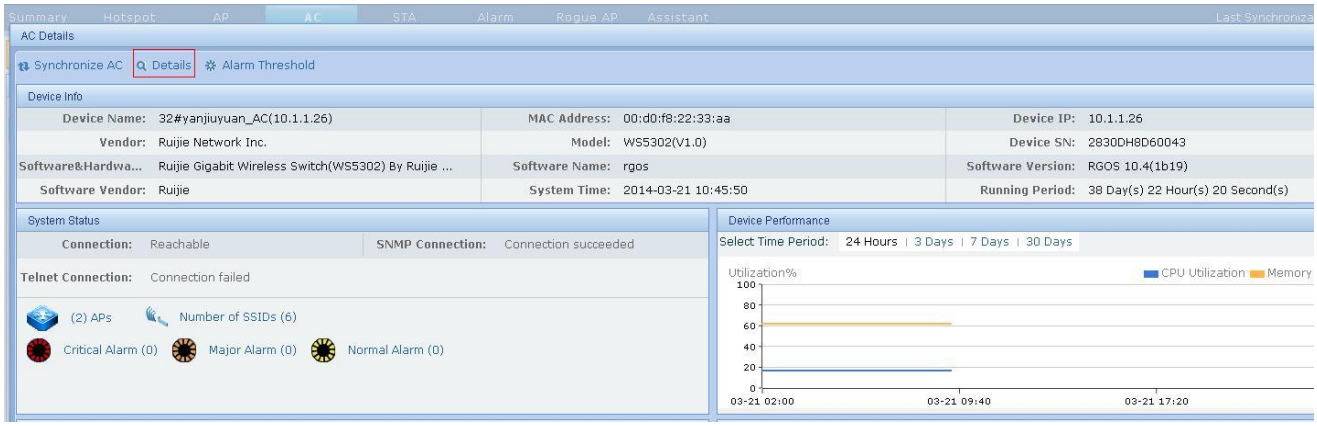


Figure 7.246. Details

Go to the **Controller** page, and select **RRM Threshold** in the menu on the left, as shown in the following figure:

Figure 7.247. RRM Threshold

The RRM Threshold setting information is displayed, as shown in the following figure:

Figure 7.248. RRM Threshold

Click **Modify**, and the data will be saved on the system and device.

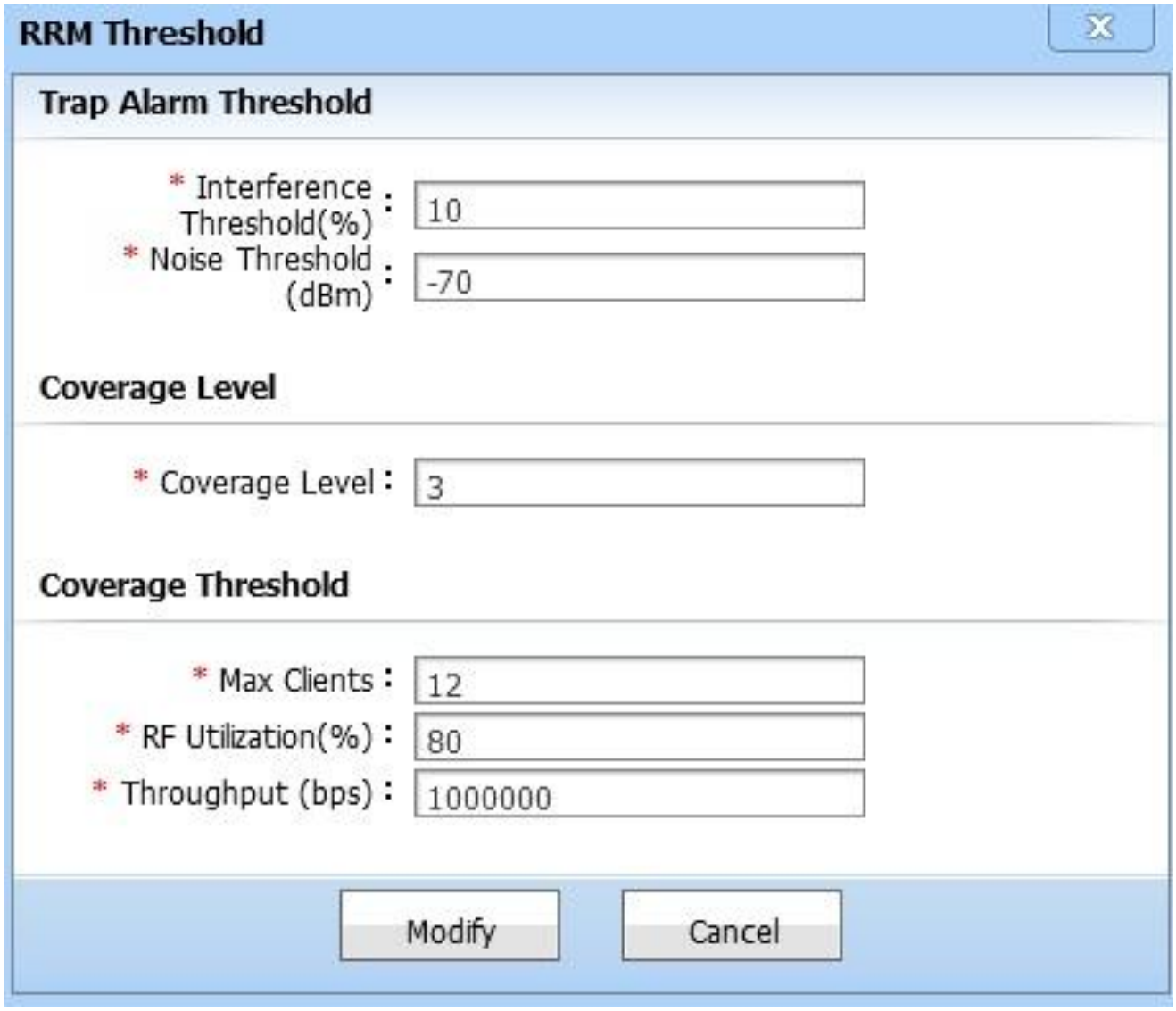


Figure 7.249. RRM Threshold Modification

Note 802.11b/g/n RRM threshold configuration is similar to 802.11a/n RRM threshold configuration.

7.4.5.1.21. RRM Interference

This function enables you to perform RRM interference configuration on AC.

Operation Steps

61) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

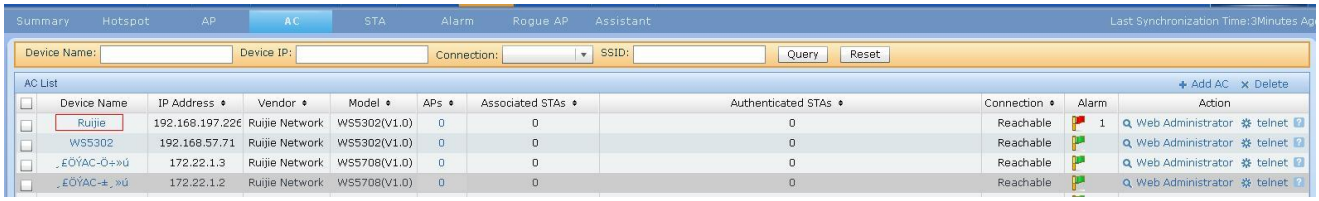


Figure 7.250. Going to **AC Details** Page

Click **Details**

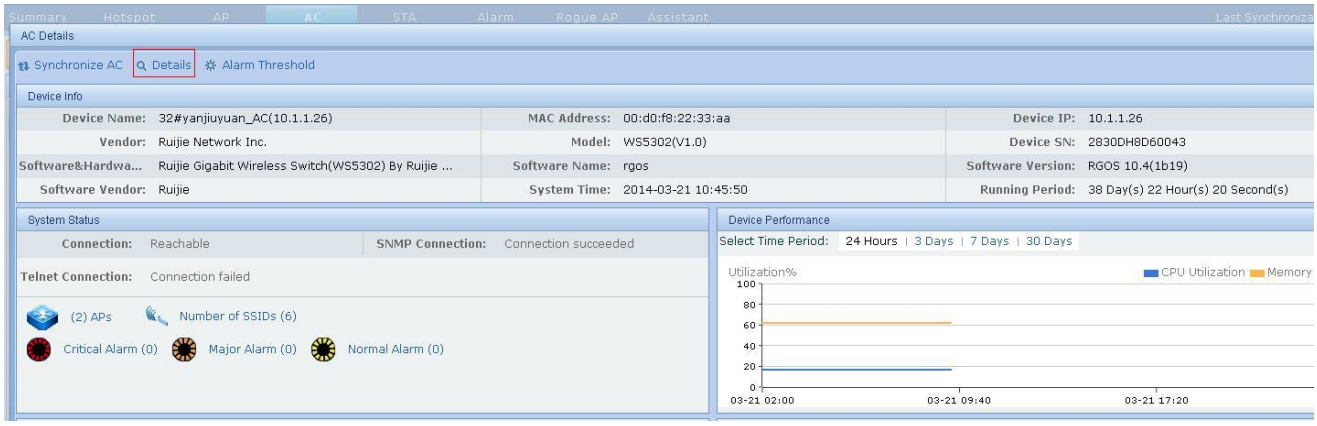


Figure 7.251. Details

Go to the **Controller** page, and select **RRM Interference** in the menu on the left, as shown in the following figure:

Figure 7.252. RRM Interference Menu

The RRM interference information is displayed, as shown in the following figure:

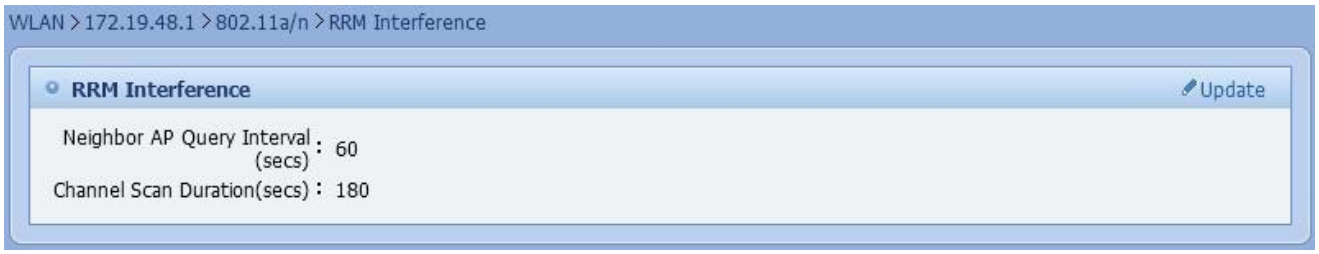


Figure 7.253. RRM Interference

Click **Modify**, and the data will be saved on the system and device.

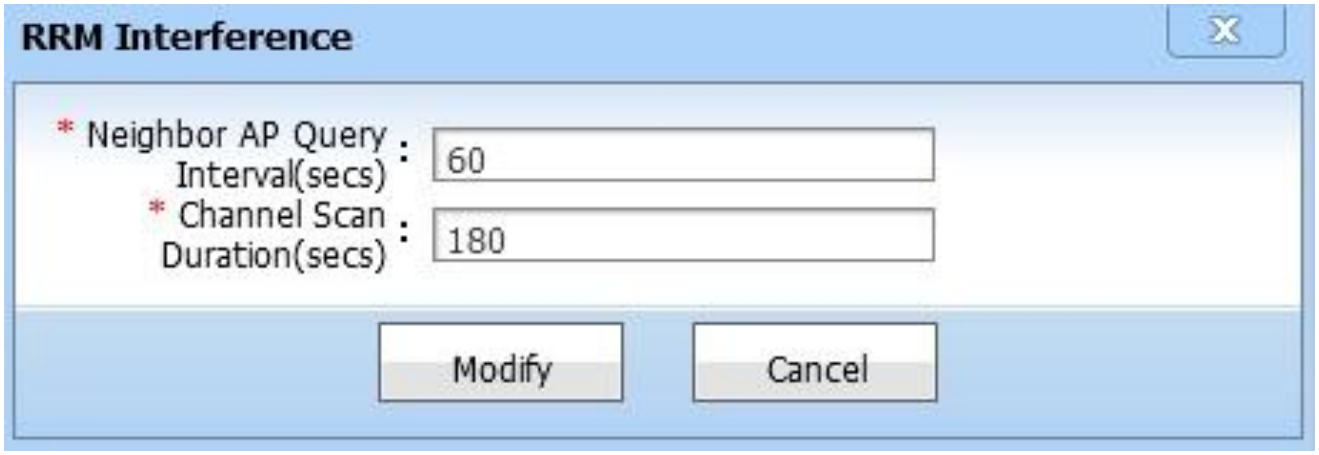


Figure 7.254. RRM Interference Modification

Note

This function modifies the device and updates network management system.
802.11b/g/n RRM interference configuration is similar to 802.11a/n RRM interference configuration.

7.4.5.1.22. RRM DCA Configuration

This function enables you to perform RRM CDA configuration on AC.

Operation Steps

62) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

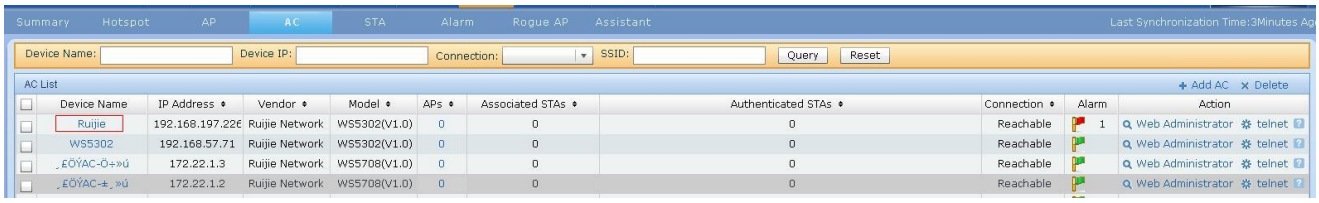


Figure 7.255. Going to **AC Details** Page

Click **Details**

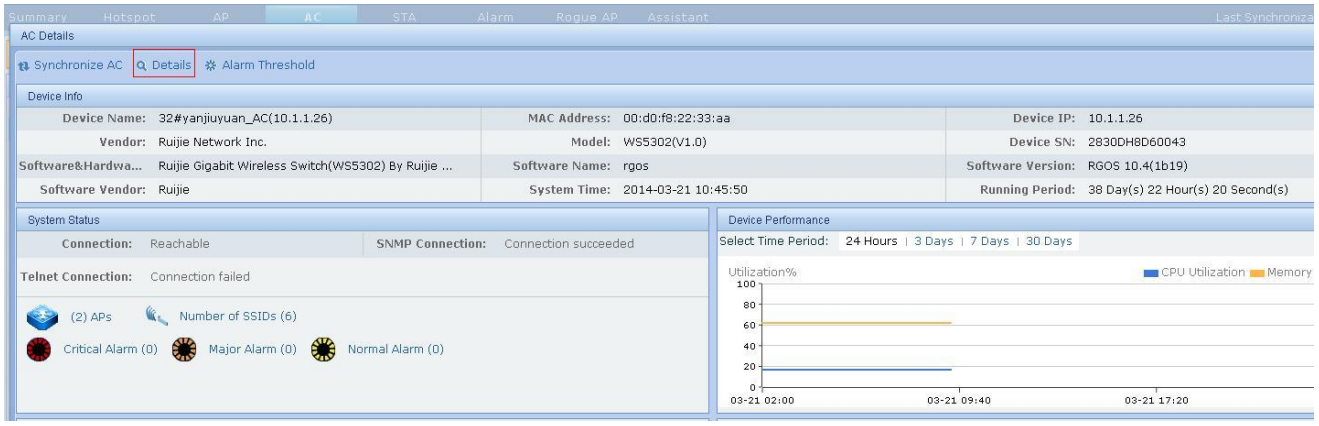


Figure 7.256. Details

Go to the **Controller** page, and select **RRM DCA Configuration** in the menu on the left, as shown in the following figure:

Figure 7.257. RRM DCA Configuration Menu

The RRM DCA information is displayed, as shown in the following figure:

Figure 7.258. RRM DCA Configuration

Click **Modify**, and the data will be saved on the system and device.

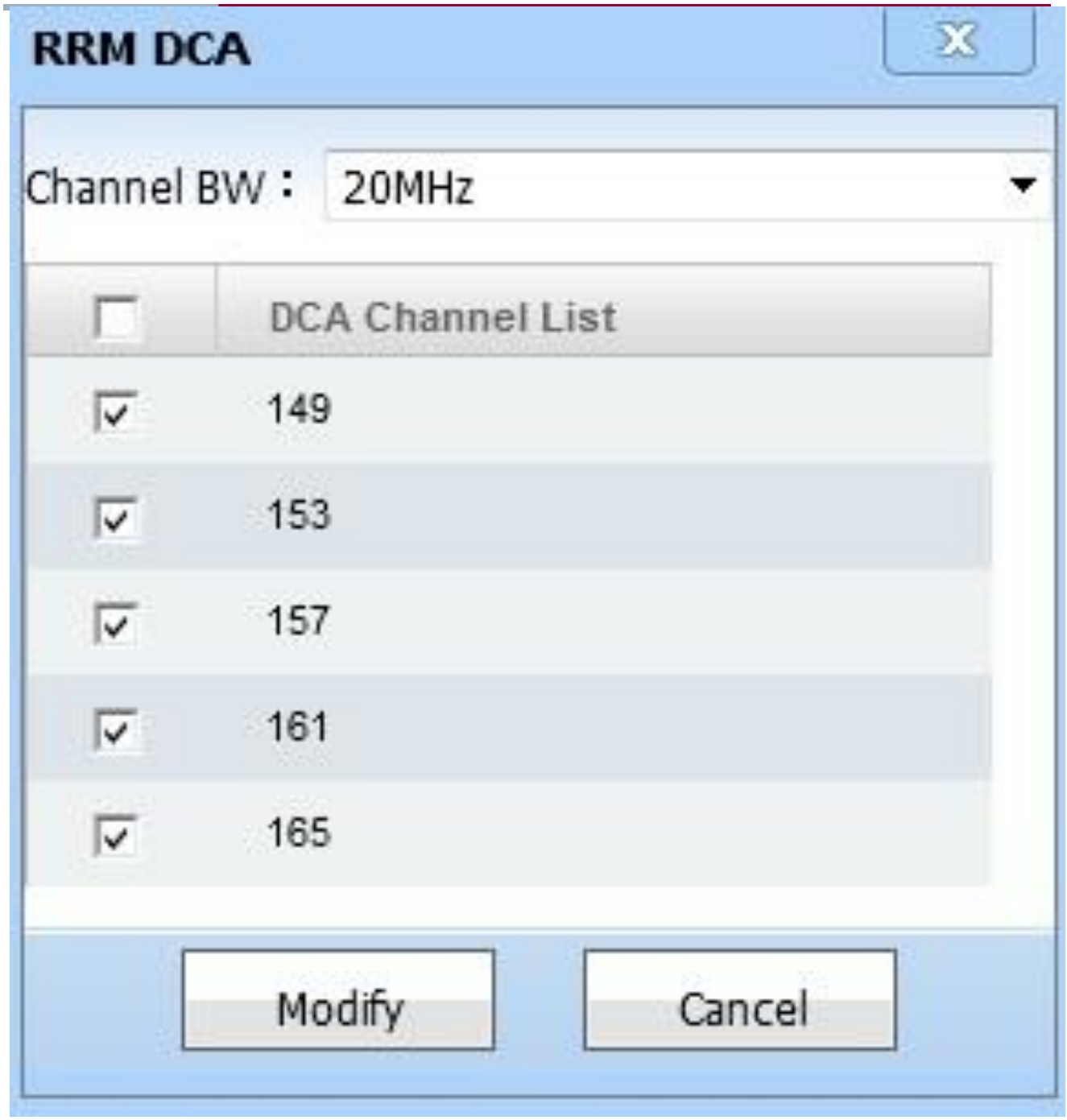


Figure 7.259. RRM DCA Modification

Note

This function modifies the device and updates network management system.
802.11b/g/n RRM DCA configuration is similar to 802.11a/n RRM DCA configuration.

7.4.5.1.23. RRM RF Grouping Configuration

This function enables you to perform RRM RF grouping configuration on AC.

Operation Steps

63) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

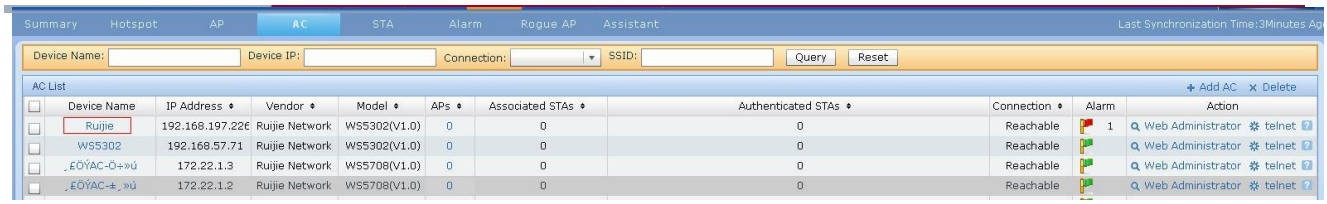


Figure 7.260. Going to **AC Details** Page

Click **Details**

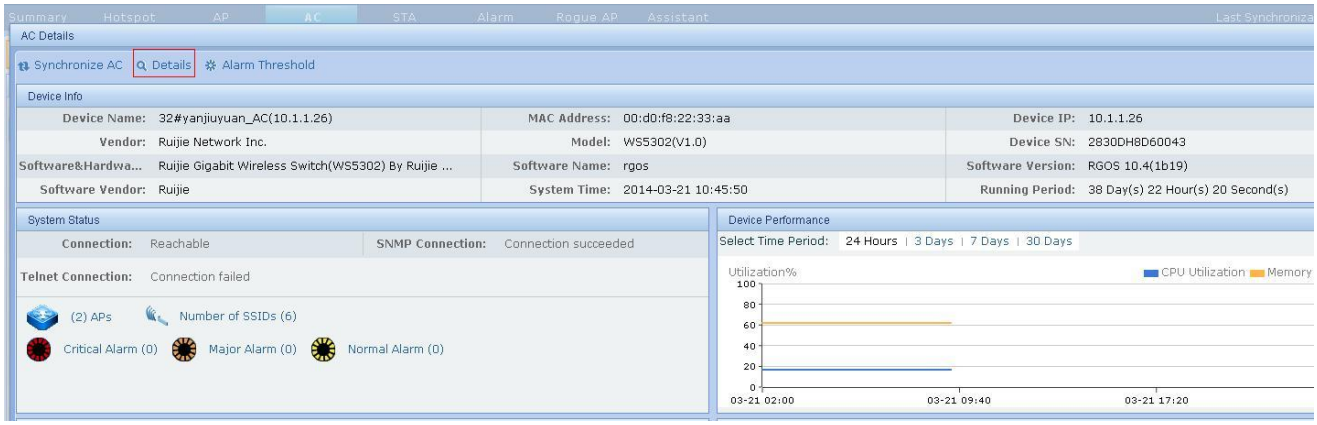


Figure 7.261. Details

Go to the **Controller** page, and select **802.11a/n** in the menu on the left, as shown in the following figure:

Figure 7.262. RRM RF Grouping Configuration Menu

The RRM RF Grouping information is displayed, as shown in the following figure:

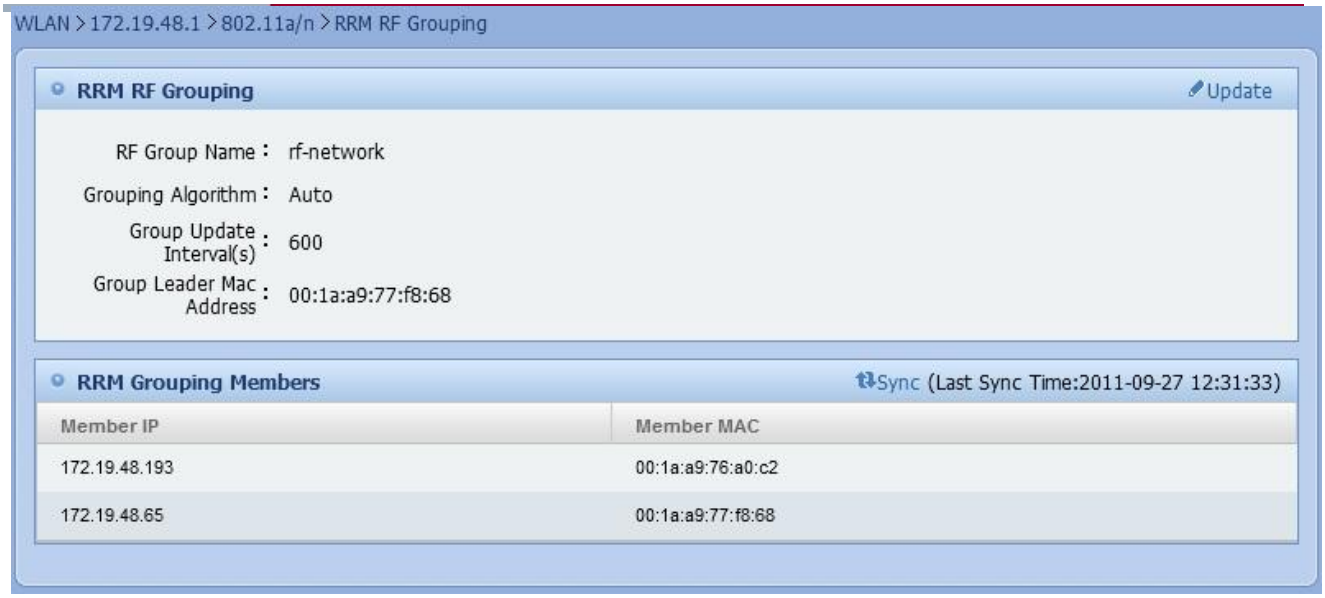


Figure 7.263. RRM RF Grouping

Click **Modify**, and the data will be saved on the system and device.

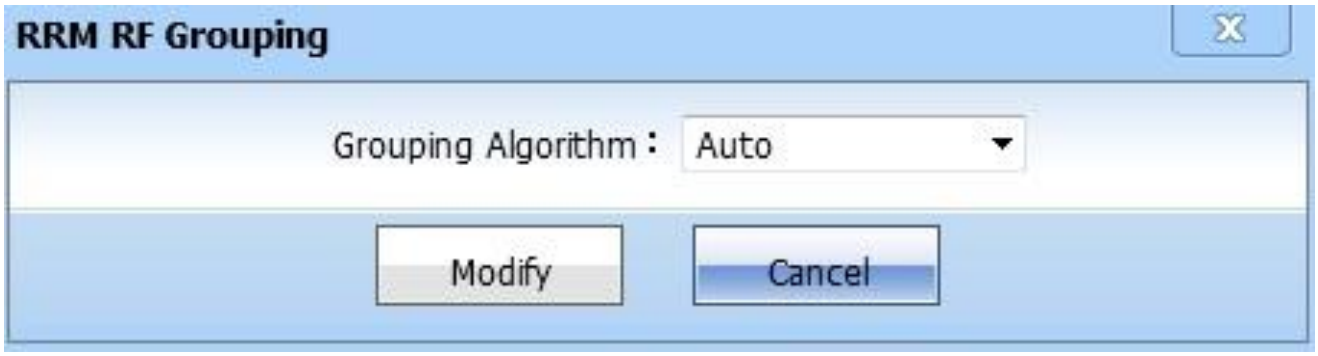


Figure 7.264. RRM RF Grouping Modification

Note

This function modifies the device and updates network management system.
802.11b/g/n RRM RF Grouping configuration is similar to RRM RF Grouping configuration.

7.4.5.1.24. 802.11n Configuration

This function enables you to perform 802.11n configuration on AC.

Operation Steps

64) Click a device name on **AC List** to go to the **AC Details** page, as shown in the following figure:

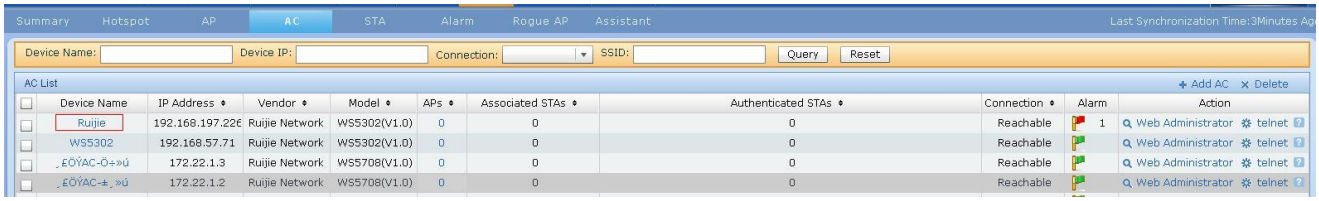


Figure 7.265. Going to **AC Details** Page

Click **Details**

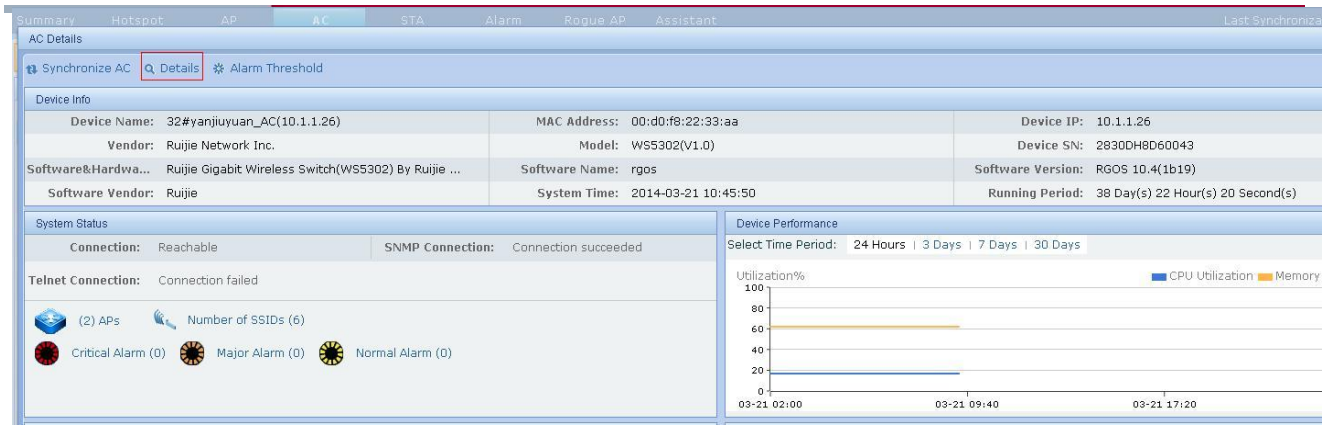


Figure 7.266. Details

Go to the **Controller** page, and select **802.11n** in the menu on the left, as shown in the following figure:

Figure 7.267. 802.11n Configuration

The 802.11n setting information is displayed, as shown in the following figure:

Figure 7.268. 802.11n Configuration

Click **Save**, and the data will be saved on the system and device.

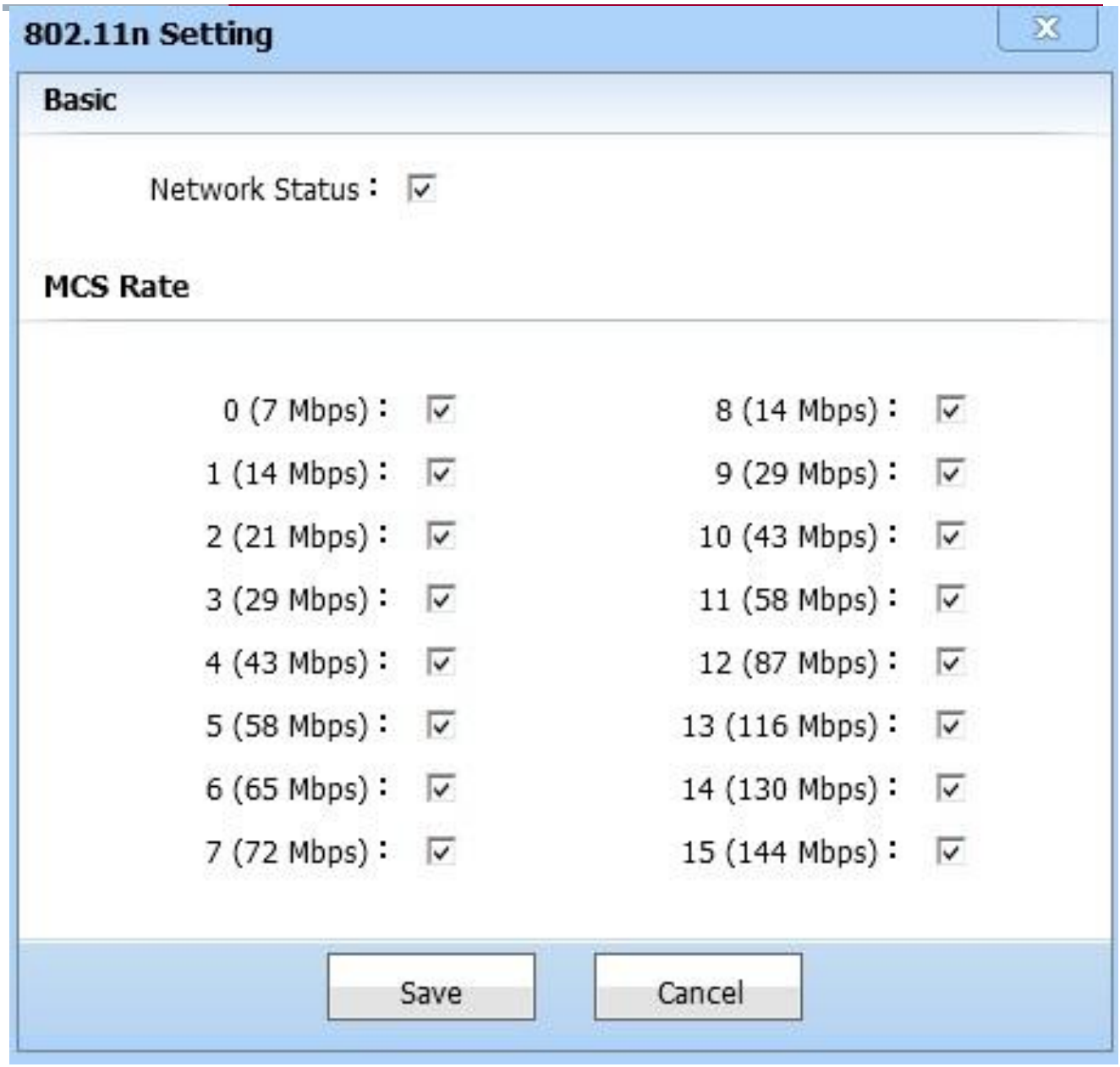


Figure 7.269. 802.11n Modification

Note

This function modifies the device and updates network management system.
802.11b/g/n configuration is similar to 802.11n configuration.

7.4.5.1.25. License

This function enables you to set the maximum number of APs allowed by an AC on the **License** page.

Operation Steps

65) Click **License** on the **Controller** menu, as shown in the following figure:

Figure 7.270. Clicking License

The maximum number of APs allowed by an AC is displayed on the **License** page, as shown in the following figure:

Figure 7.271. License Setting

7.5. STA

Major Functions

- • Global STA List
- • Key STA List
- • STA Statistics

7.5.1. Global STA List

This function enables you to view and query the information of global STAs, and set STAs as key monitored targets.

View Global STAs

1) Choose **STA > STA,** and select a STA group to view the STA list, as shown in the following figure.

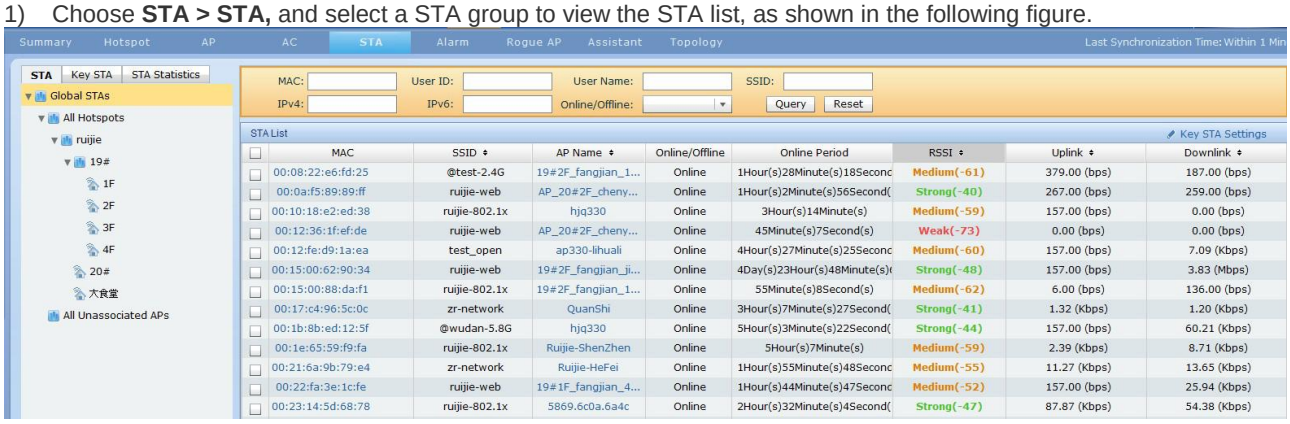


Figure 7.272. Global STA List

2) Above the STA List, enter filters in the boxes and click Query to query STA information, as shown in the following figure.

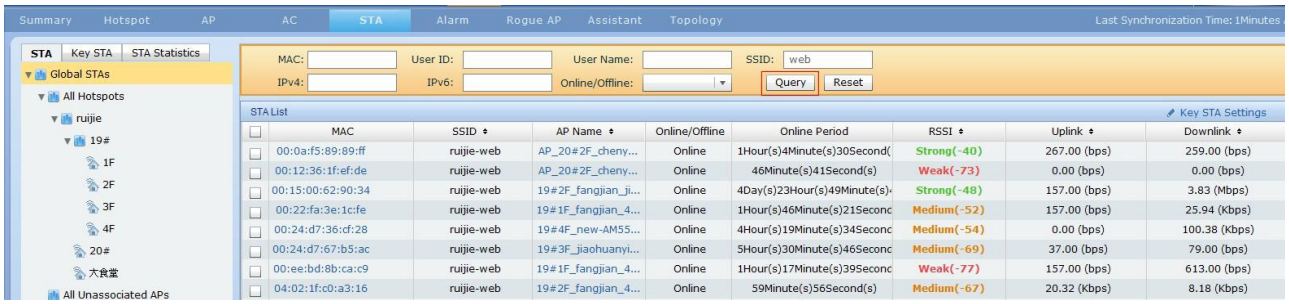


Figure 7.273. STA Query

3) Below the **STA List**, check the attribute boxes to view more STA details, as shown in the following figure. The attributes are user-defined.

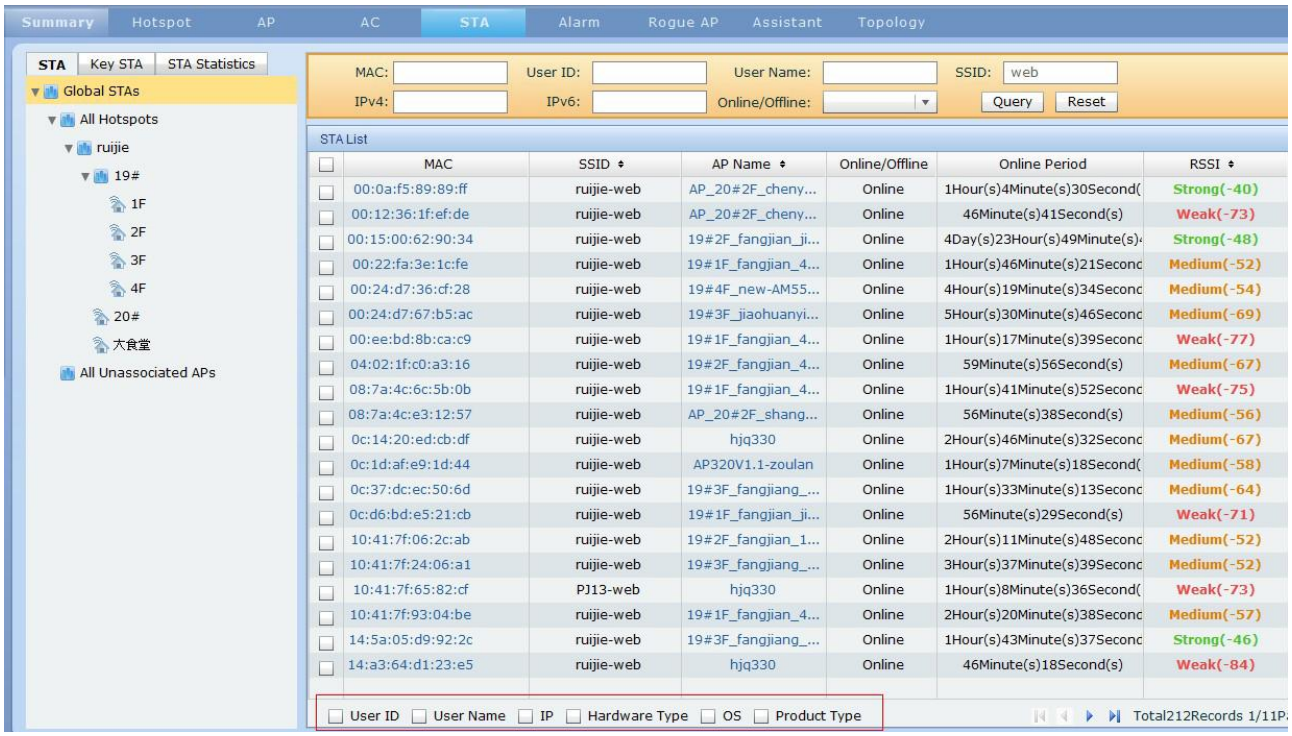


Figure 7.274. Viewing More STA Details

Set as Key STAs

1) Check the boxes in STA List to select STAs, as shown in the following figure.

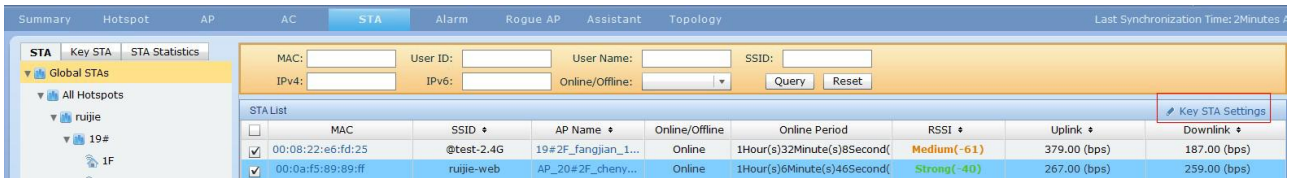


Figure 7.275. Selecting Key STA

2) Click **Key STA Settings**, enter the retransmit rate threshold, and click **OK**, as shown in the following figure.

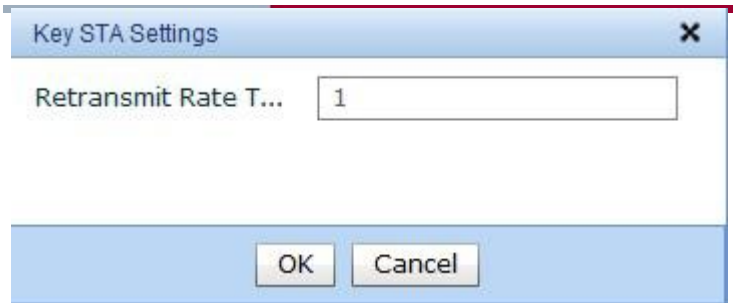


Figure 7.276. Setting Retransmit Rate Threshold

7.5.2. Key STA List

This function enables you to add, query, set, and remove key STAs.

Add Key STAs

1) Click **Add Key STA**, as shown in the following figure.

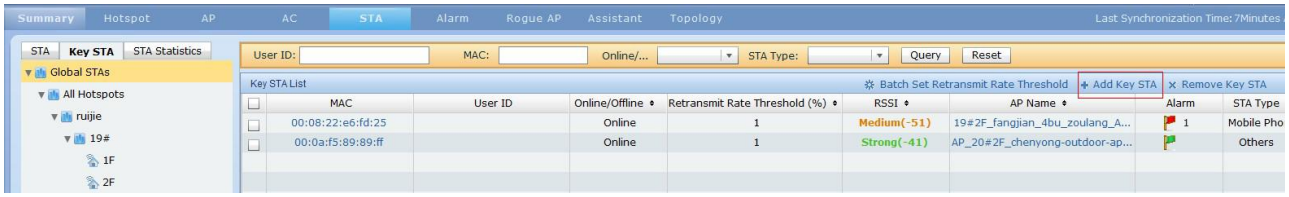


Figure 7.277. Adding Key STAs

2) Enter the key STA information, and click **OK**, as shown in the following figure

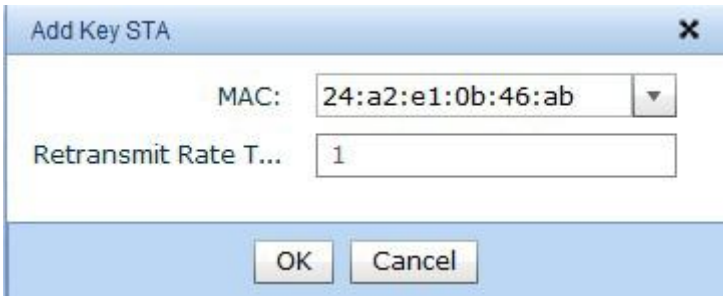


Figure 7.278. Entering Key STA Information

Query Key STAs

1) Above the Key STA List, enter filters to query specified key STAs, as shown in the following figure.

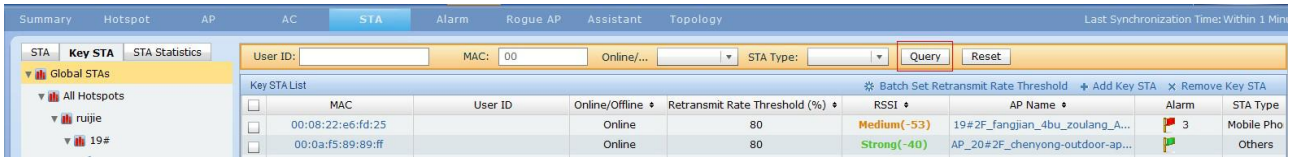


Figure 7.279. Querying Key STAs

Batch Set Key STA Threshold

1) Check the Key STA List boxes to select STAs, and click **Batch Set Retransmit Rate Threshold**, as shown in the figure.

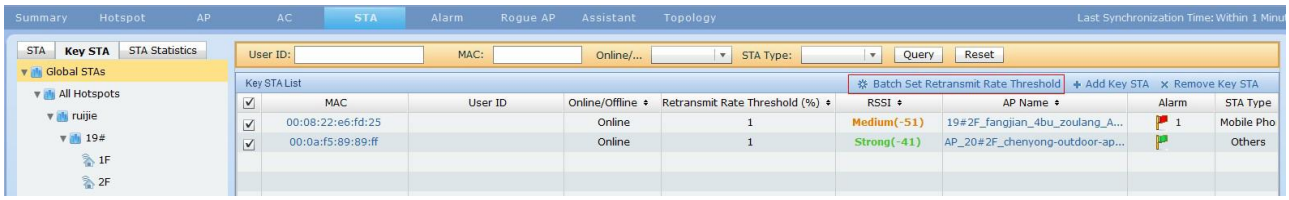


Figure 7.280. Selecting Key STAs

2) Enter the retransmit rate threshold and click **OK**, as shown in the following figure.

Figure 7.281. Setting Retransmit Rate Threshold

Remove Key STAs

1) Select STAs, click **Remove Key STA**, and click **OK**, as shown in the following figure.

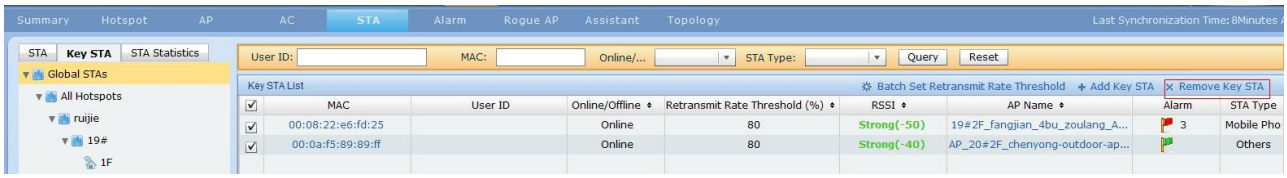


Figure 7.282. Removing Key STAs

7.5.3. STA Statistics

The **STA** page enables you to view User Count and Rate Statistics of all or specific SSIDs, the Top N APs /Hotspots in STA number or in rates, and online/all STA status statistics sorted by frequency bands or connection protocols.

Global WLAN STA Statistics

View global WLAN STA statistics, as shown in the following figure:

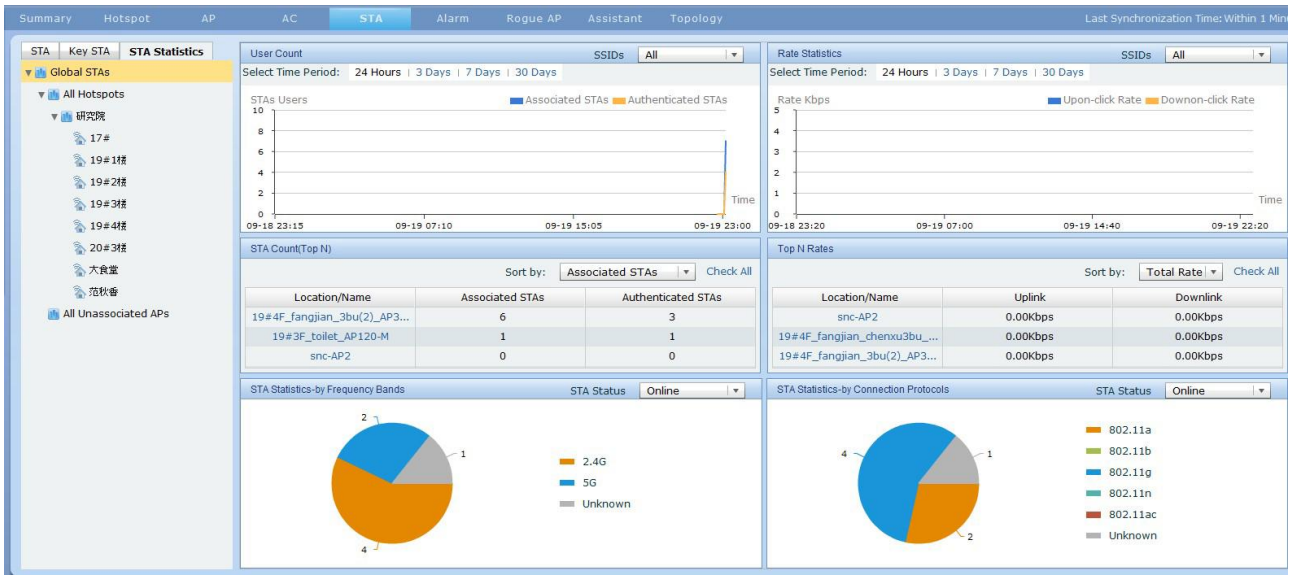


Figure 7.283. Global WLAN STA Statistics

Hotspot WLAN STA Statistics

View global hotspot STA statistics, as shown in the following figure:

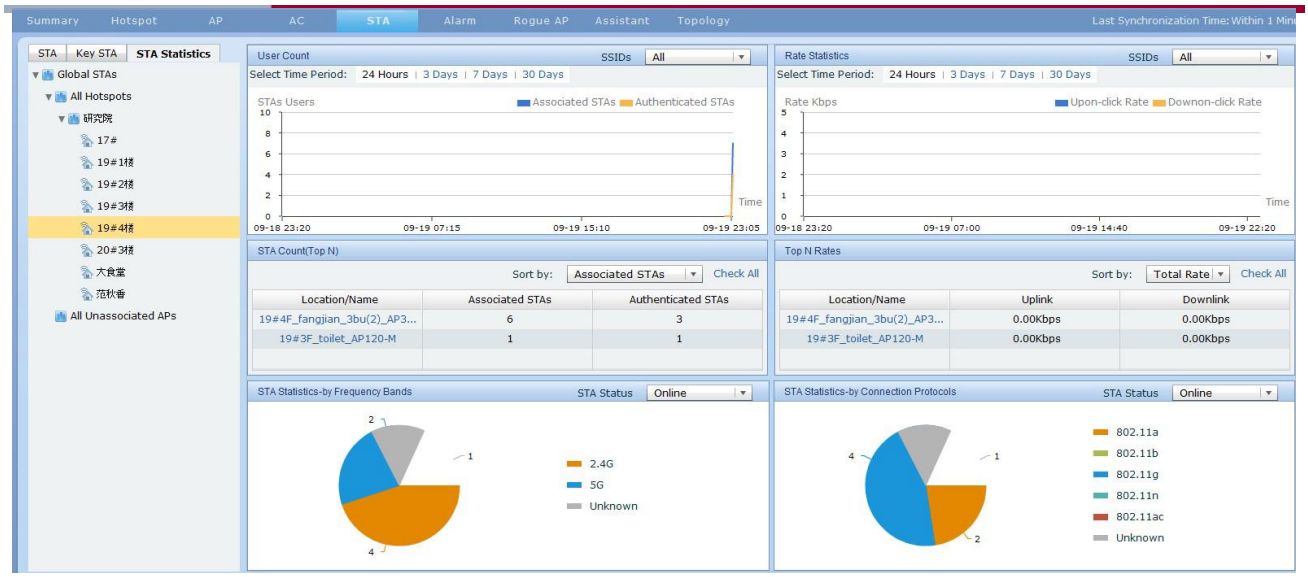


Figure 7.284. Hotspot WLAN STA Statistics

7.6. Alarm

The **Alarm** page enables you to manage alarms coming from wireless devices, including all Trap messages reported by managed devices and alarms concerning configuration modification.

Major Functions

- Alarm Source Navigation
- WLAN Alarm Operation

7.6.1. Alarm Source Navigation

The alarm list displays all alarms coming from the alarm source.

Operation Steps

66) Go to **WLAN** > **Alarm** and **view Alarm Source Navigation** in the left menu, as shown in the following figure:

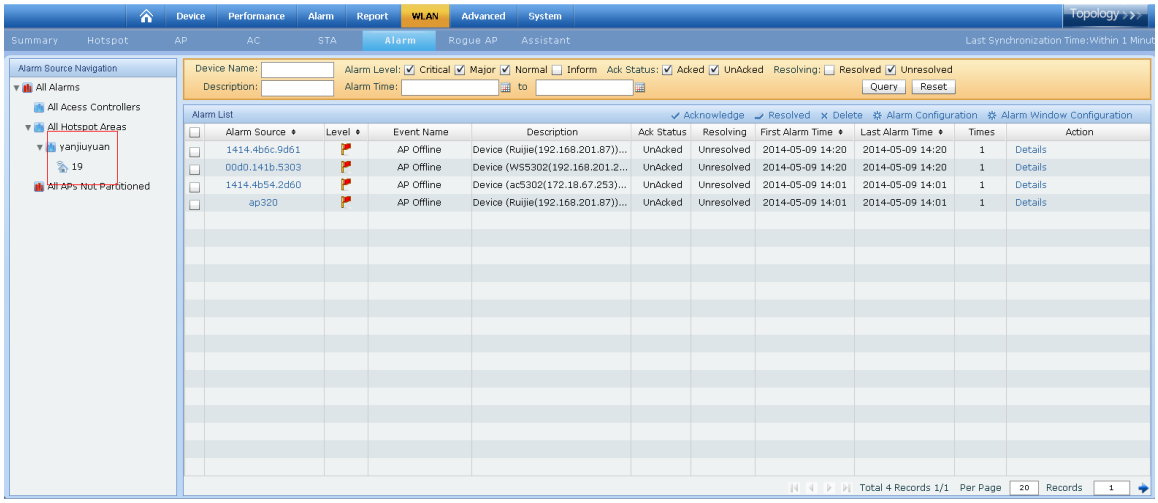


Figure 7.285. Alarm Source Navigation

Click  to unfold the navigation.
The child nodes are displayed, as shown in the following figure:

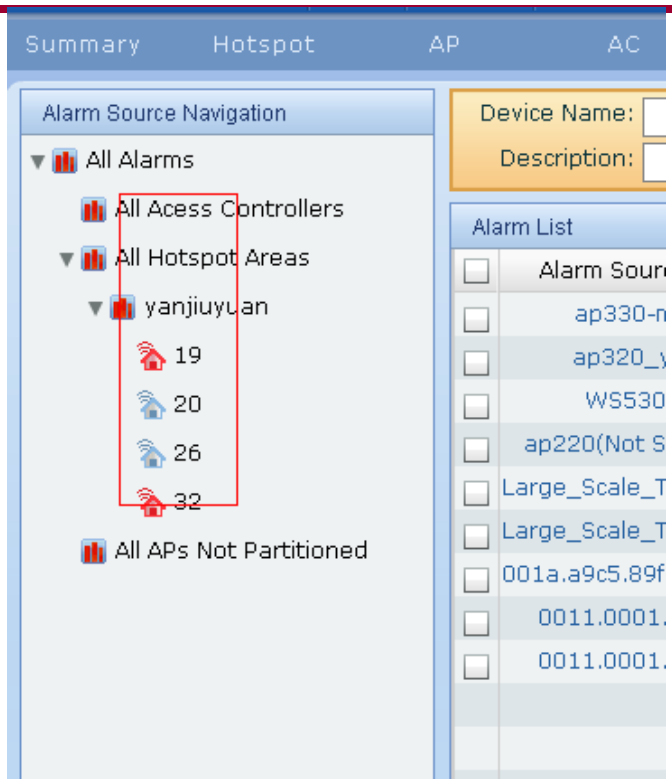


Figure 7.286. Selecting Child Node

The alarm list displays all alarms coming from the alarm source.

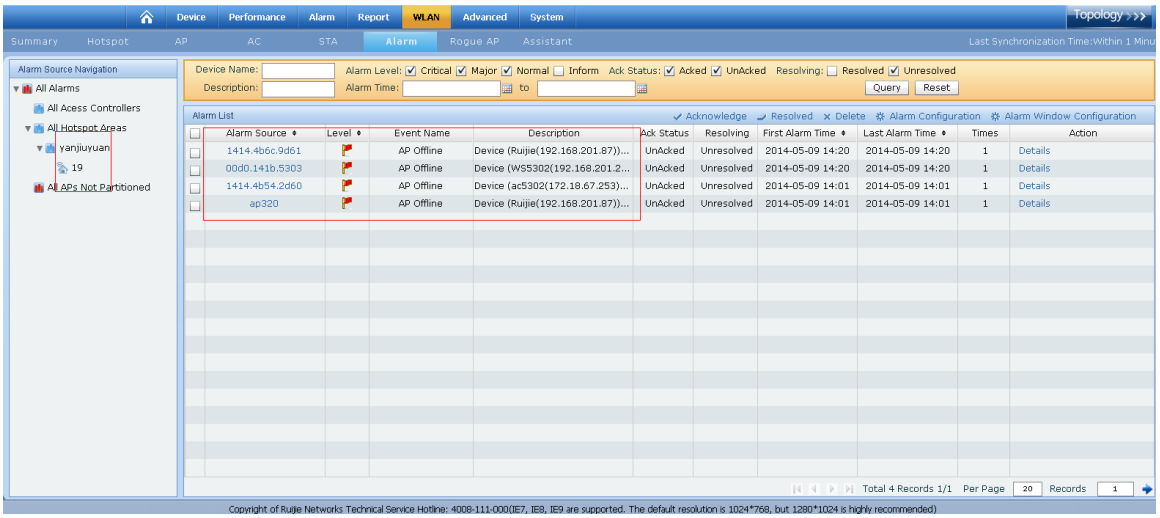


Figure 7.287. Alarm List

Note You can go to Wireless-->Hotspot to configure hotspots.

7.6.2. WLAN Alarm Operation

This function enables you to delete, acknowledge and configure WLAN alarms.

Major Functions

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm

- Configure Alarm Window
- Locate Alarm AP

7.6.2.1. Alarm Status(Acknowledge)

This function enables you to set the alarm status to **Acknowledge**. The **Acknowledge** status indicates whether the alarm has been managed.

Operation Steps

67) Go to **WLAN** > **Alarm**.
Tick the checkbox before the alarm source.
Click **Acknowledge**, and the alarm status is changed to acknowledged.
The operation steps are shown in the following figure:

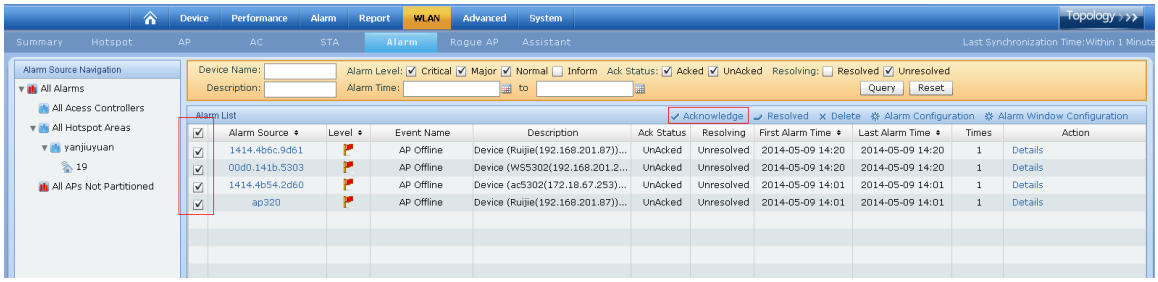


Figure 7.288. Alarm Acknowledged

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.2. Alarm Status(Resolved)

This function enables you to set the alarm status to Resolved. The Resolved status indicates if the alarm has been managed.

Operation Steps

68) Go to **WLAN** > **Alarm**.
Tick the checkbox before the alarm source.
Click Resolved, and the alarm status is changed to resolved.
The operation steps are shown in the following figure:

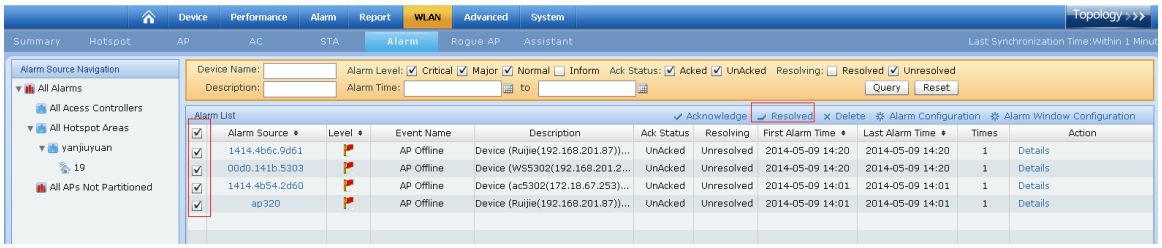


Figure 7.289. Alarm Resolved

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.3. Delete Alarm

This function enables you to delete the alarm in the alarm list.

Operation Steps

69) Go to **WLAN** > **Alarm**
Tick the checkbox before the alarm source.
Click Delete, and the selected alarm is deleted.

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.4. Configure Alarm

If the number of down APs on the hotspot exceeds the threshold, an alarm is generated.

Operation Steps

70) Go to **WLAN** > **Alarm** > **Alarm Configuration**, as shown in the following figure:

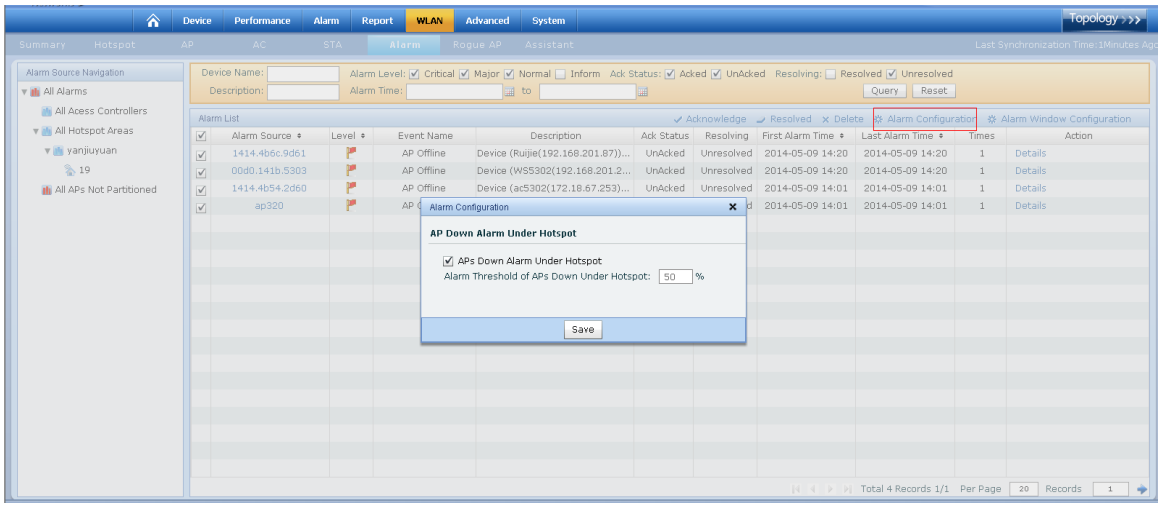


Figure 7.290. Alarm Configuration

Enable **APs Down Alarm Under Hotspot**, as shown in the following figure:

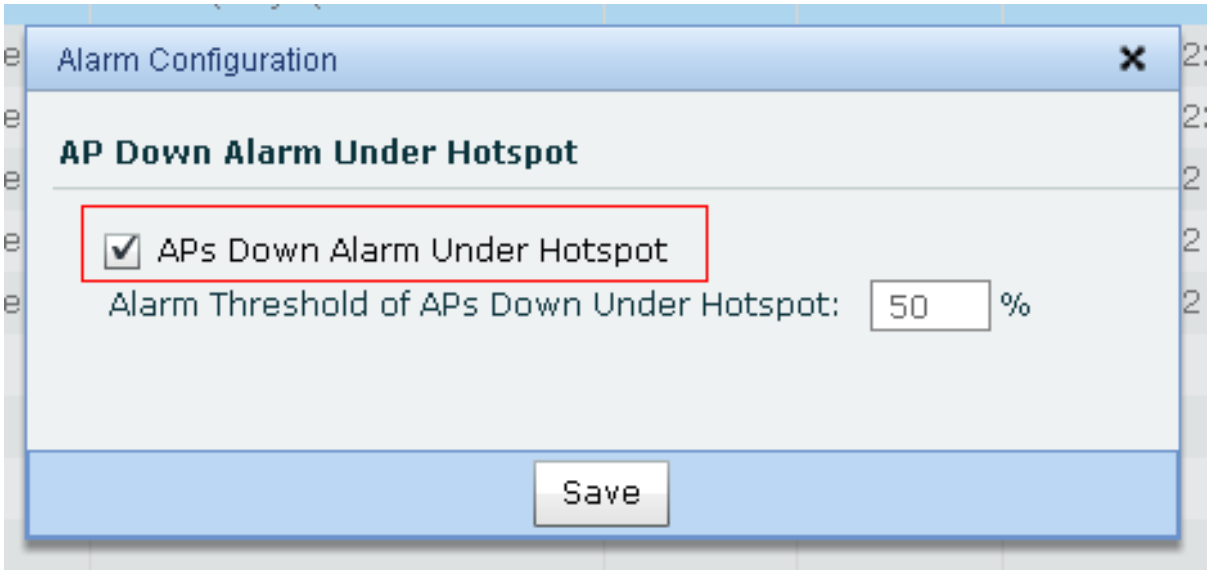


Figure 7.291. Enabling Alarm

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.5. Configure Alarm Window

This function enables you to manage the way to display the alarm.

Operation Steps

71) Go to **WLAN** > **Alarm** > **Alarm Window Configuration**, as shown in the following figure:

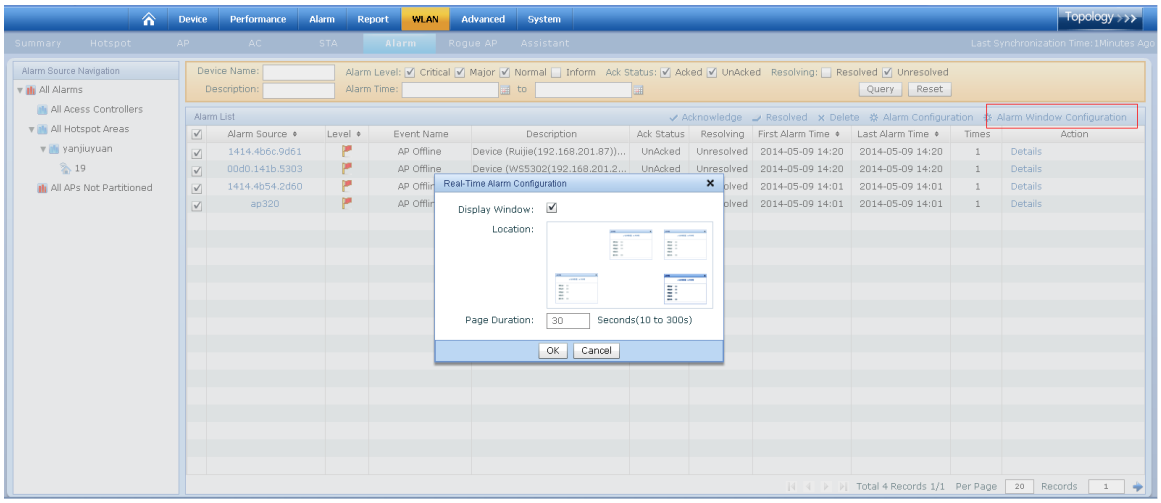


Figure 7.292. Configuring Alarm Window

Enable **Display Window**, as shown in the following figure:

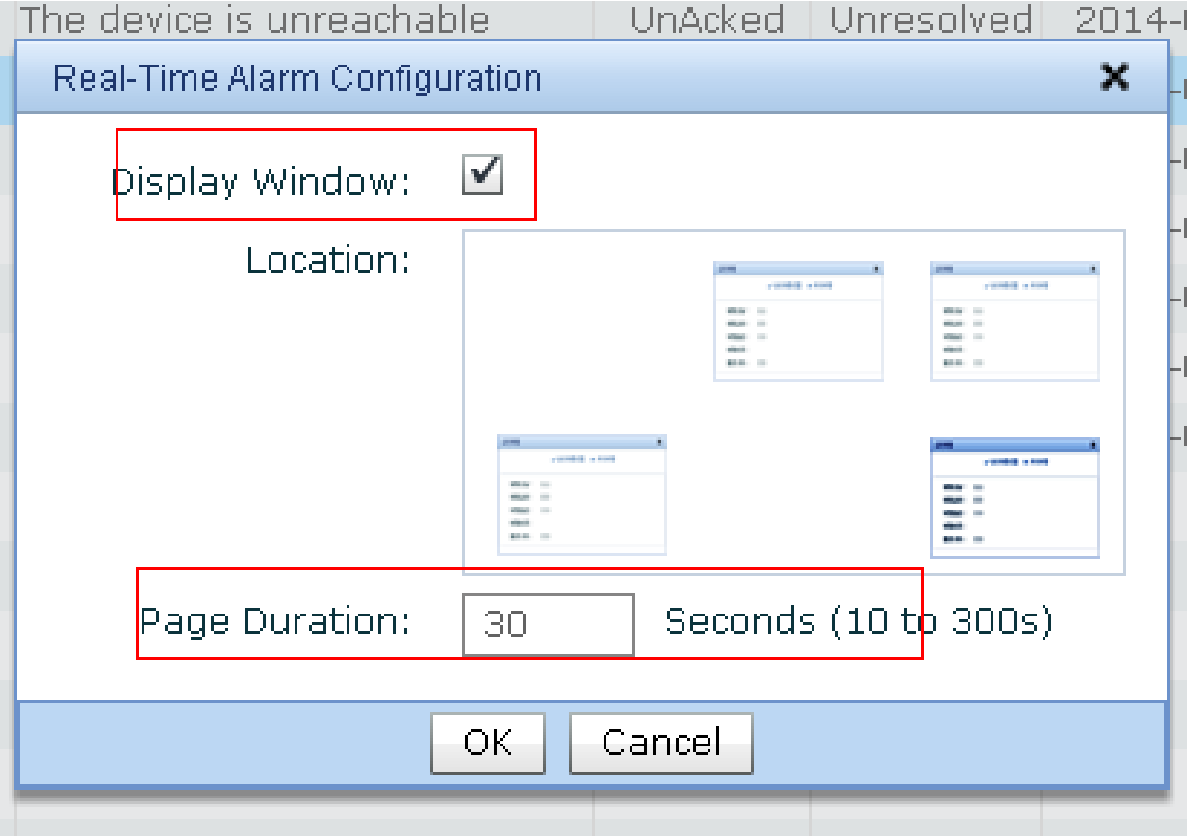


Figure 7.293. Enabling Display Alarm Window

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.6. Locate Alarm AP

This function enables you to locate the alarm AP in the heat map.

Operation Steps

72) Go to **WLAN** > **Alarm**.
Find the alarm AP in the alarm list.
Click **More** in the **Action** column, and **Heat Map Location** is displayed. Click **Heat Map Location** to locate the alarm AP in the heat map.

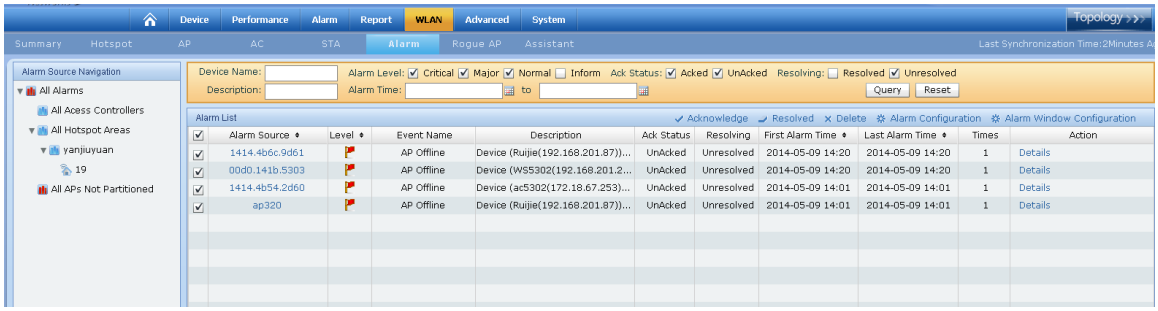


Figure 7.294. Heat Map Location

Related Topics

- Alarm Status(Acknowledge)
- Alarm Status(Resolved)
- Delete Alarm
- Configure Alarm
- Configure Alarm Window
- Locate Alarm AP

7.6.2.7. Alarm Export

This function enables you to export alarm records from the Alarm List.

Operation Steps

1) Choose **WLAN** > **Alarm**.

2) Select alarms, and click **Export**, as shown in the following figure.

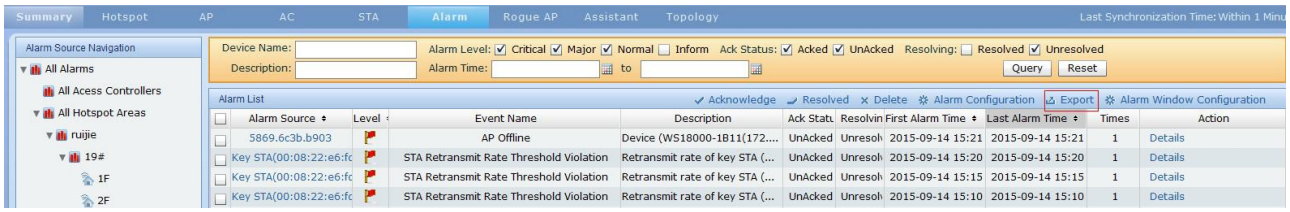


Figure 7.295. Alarm Export

7.7. Rogue AP

The **Rogue AP** page enables you to view the List of Rogue AP and add, delete and synchronize the Whitelist and Blacklist. You can also view Operation Logs.

Major Functions

- Rogue AP Operation
- Whitelist and Blacklist Operation
- Operation Log

7.7.1. Rogue AP Operation

This function enables you to perform operations on rogue APs.

View List of Rogue APs

73) You can find the **List of Rogue APs** link on **AP Navigation** on the AP page, and **Hotspot Navigation** on the Hotspot page, as shown in the following figure:

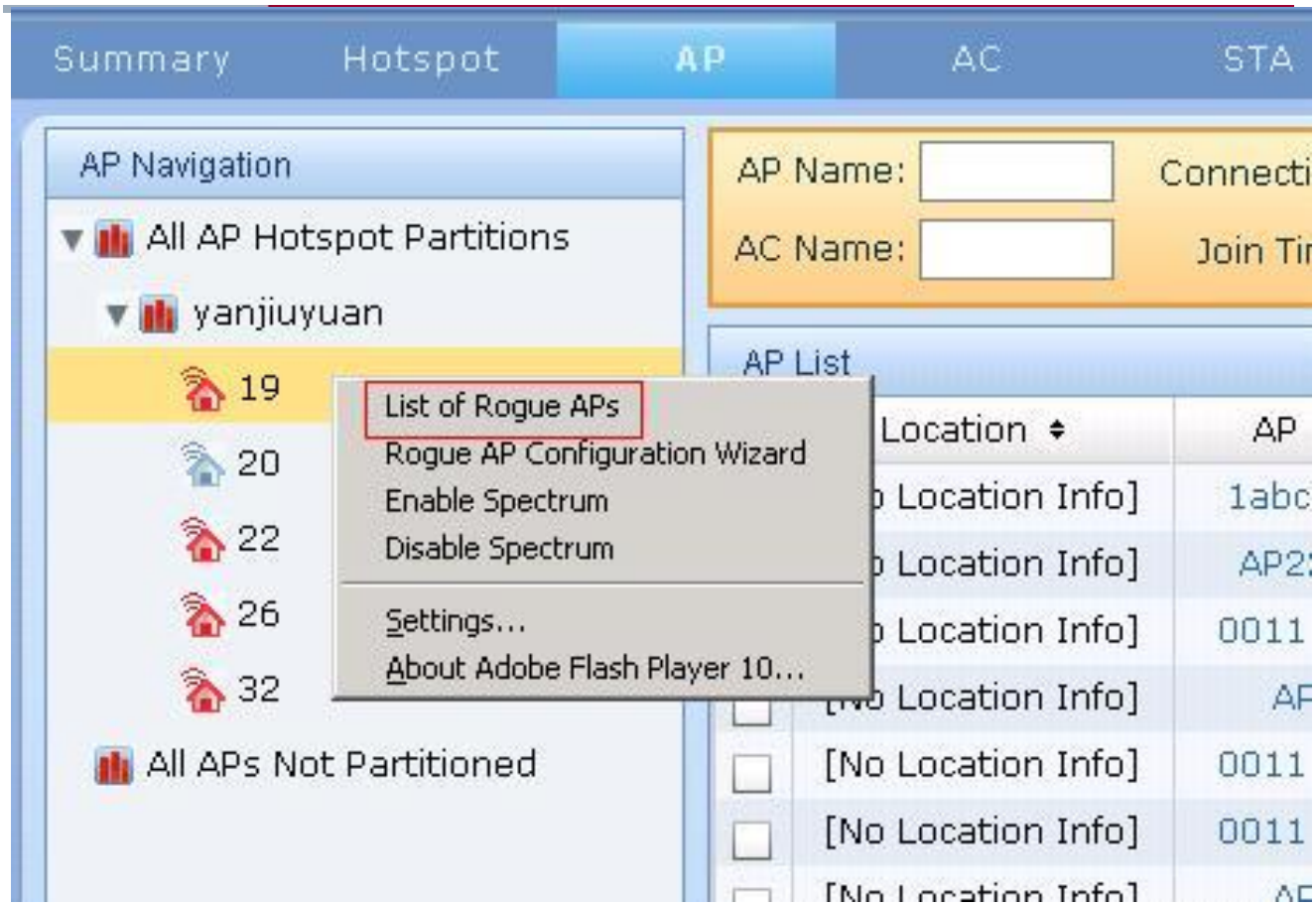


Figure 7.296. Viewing **List of Rogue APs** from **AP Navigation** on the AP page

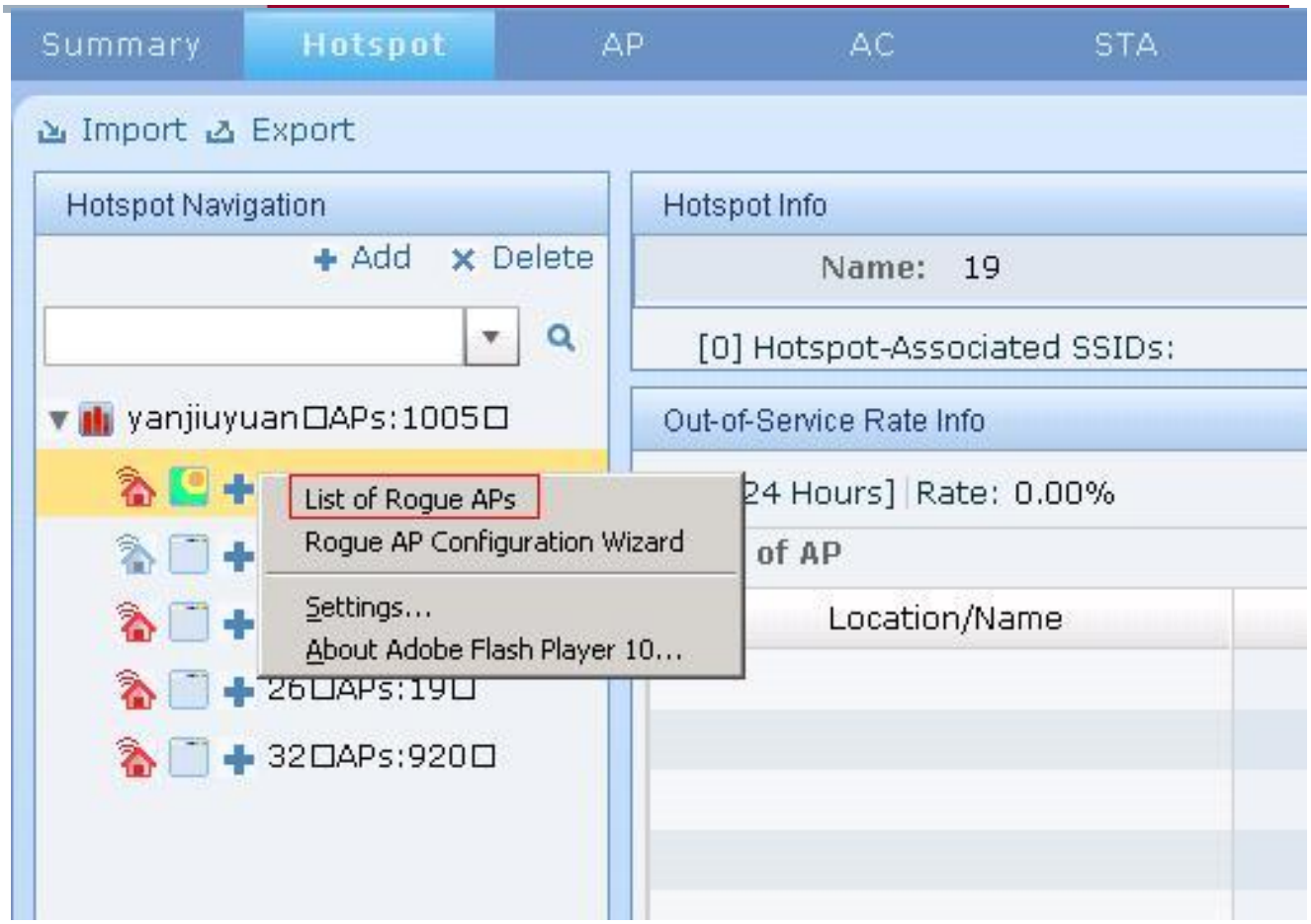


Figure 7.297. Viewing **List of Rogue APs** from **Hotspot Navigation** on the Hotspot page

You can also go to the **Rogue AP** page, and view **List of Rogue APs**, as shown in the following figure:

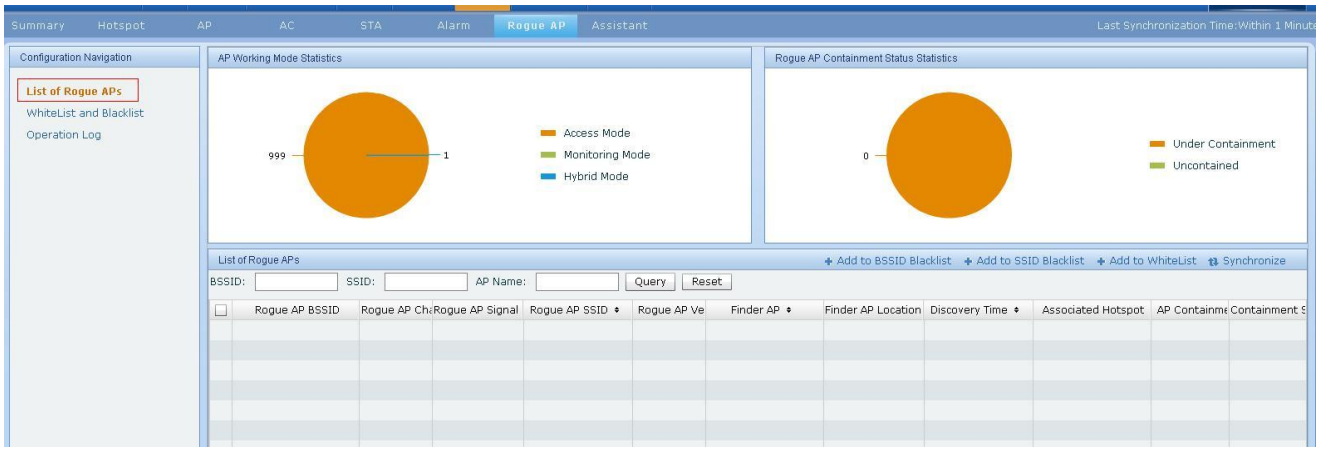


Figure 7.298. List of Rogue APs

Add to Blacklist

Select **Rogue APs**, and click **Add to BSSID Blacklist** or **Add to SSID Blacklist**, as shown in the following figure:

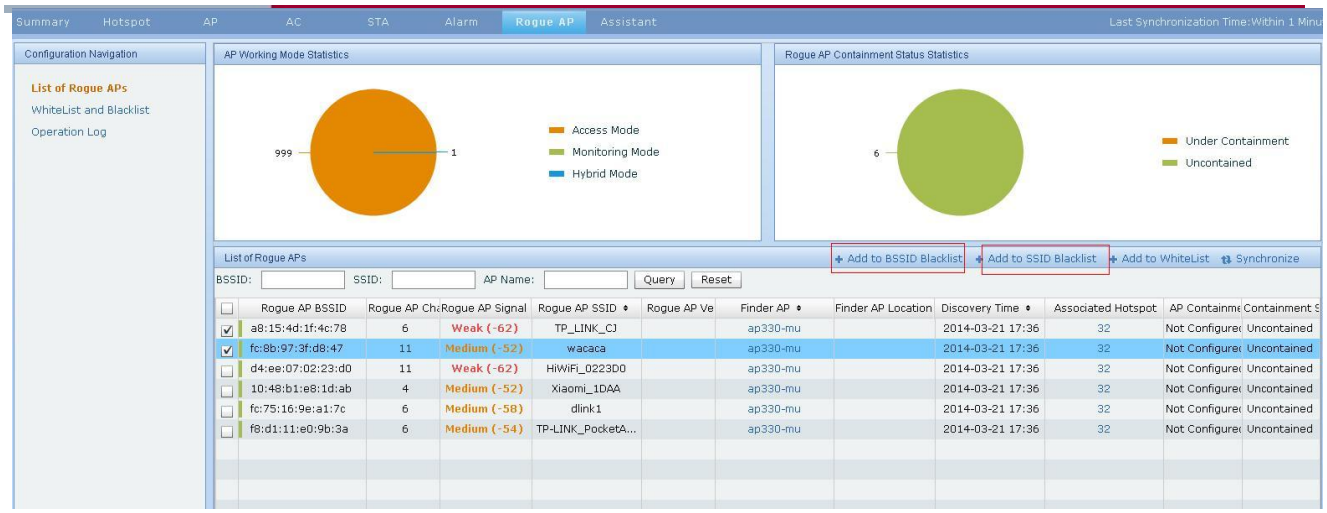


Figure 7.299. Adding to Blacklist

Add to Whitelist

Select **Rogue APs**, and click **Add to Whitelist**, as shown in the following figure:

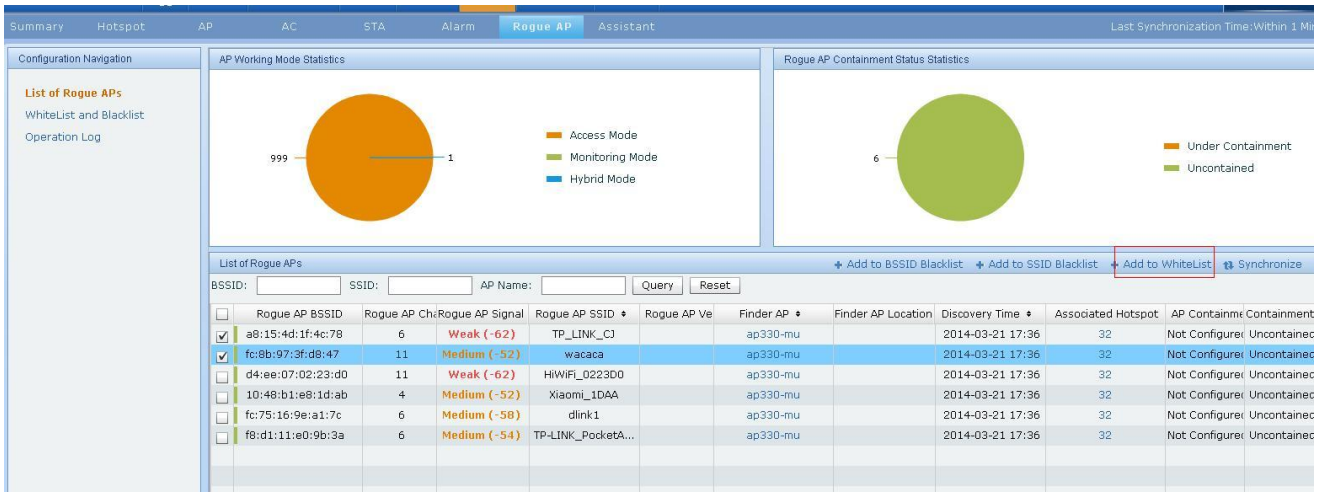


Figure 7.300. Adding to Whitelist

Synchronize Rogue APs

Click **Synchronize**, as shown in the following figure:

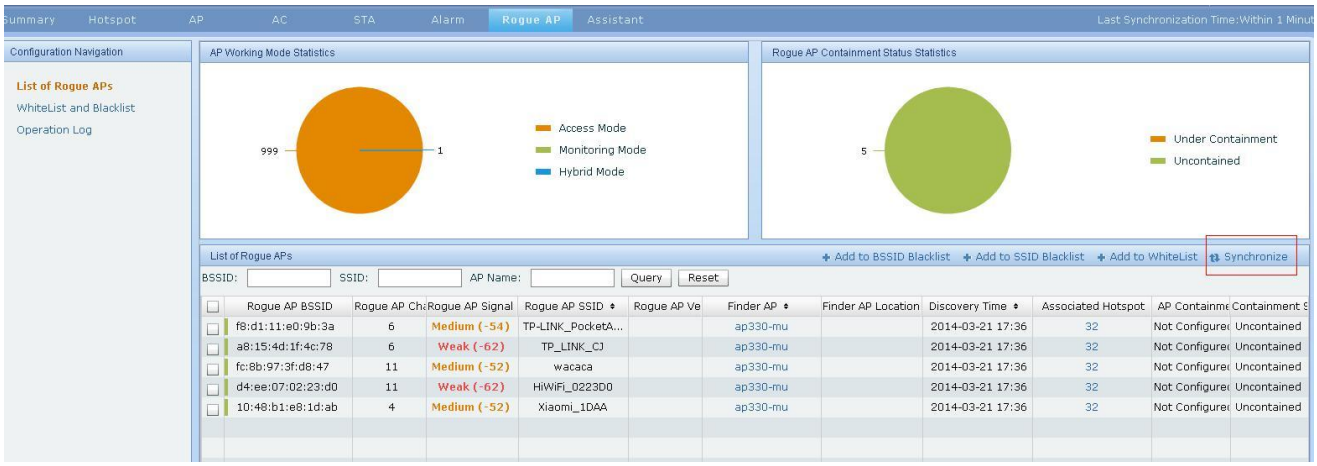


Figure 7.301. Synchronizing Rogue AP

7.7.2. Whitelist and Blacklist Operation

This function enables you to perform operations on Whitelist and Blacklist.

Synchronize Whitelist and Blacklist

74) Select the AC, as shown in the following figure:

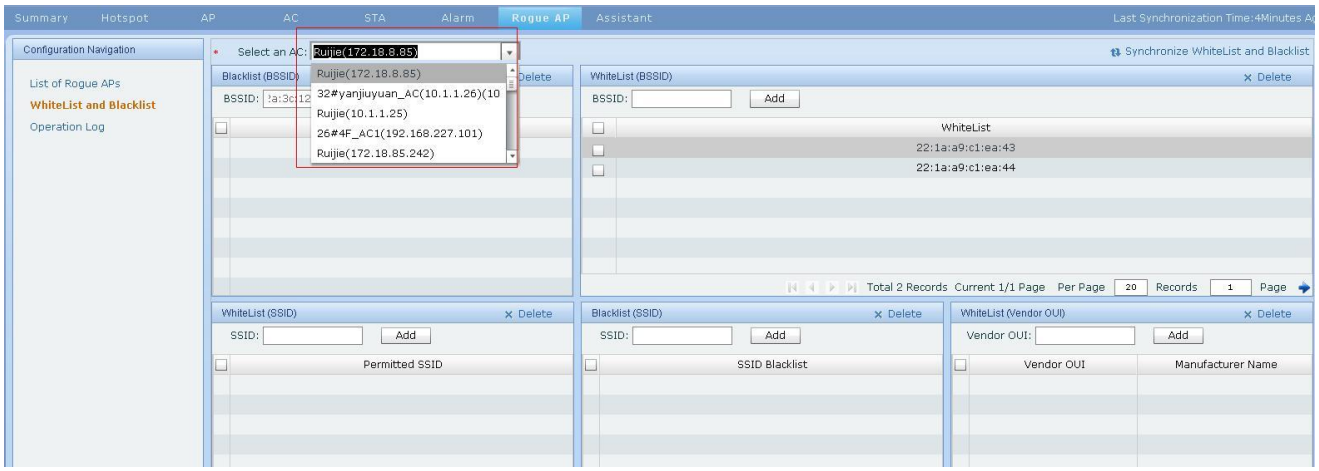


Figure 7.302 Selecting AC

Click **Synchronize Whitelist and Blacklist**, as shown in the following figure:

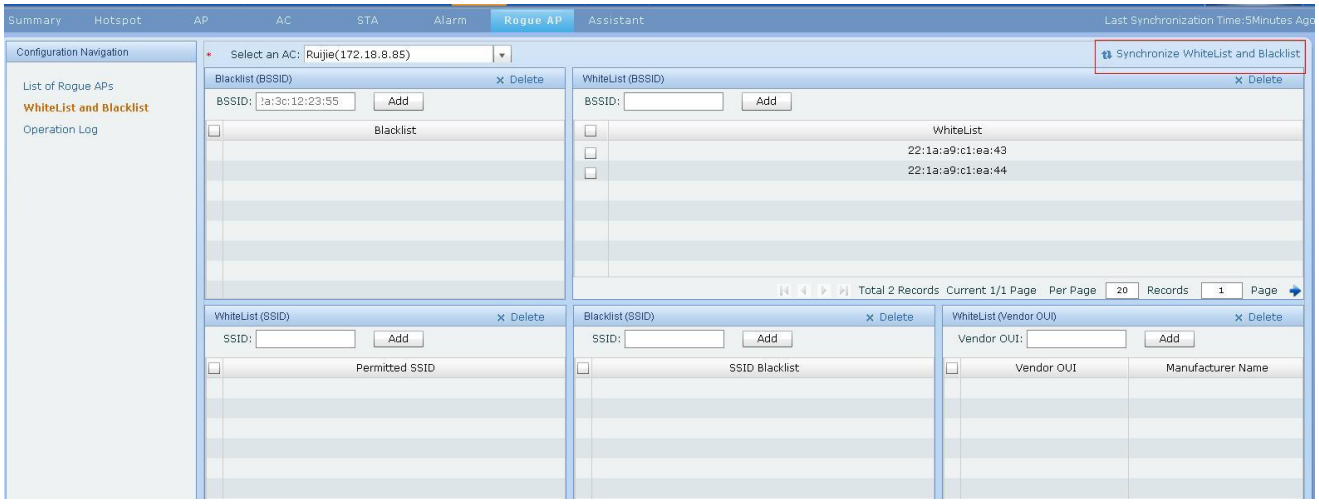


Figure 7.303. Synchronizing Whitelist and Blacklist

Add Blacklist Entry (BSSID)

75) Select the AC, as shown in the following figure:

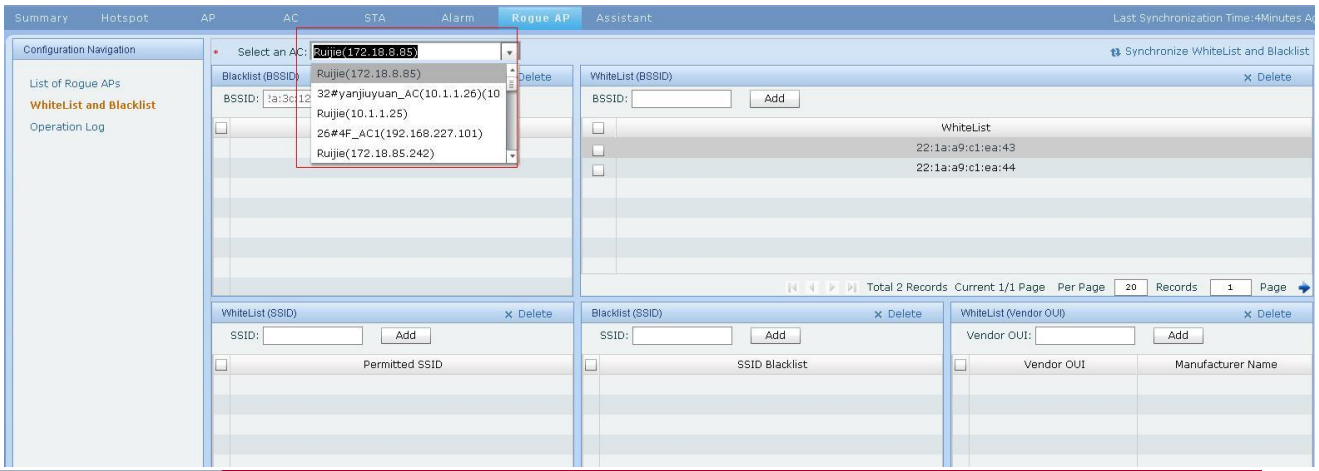


Figure 7.304. Selecting AC

Entering the BSSID, as shown in the following figure:

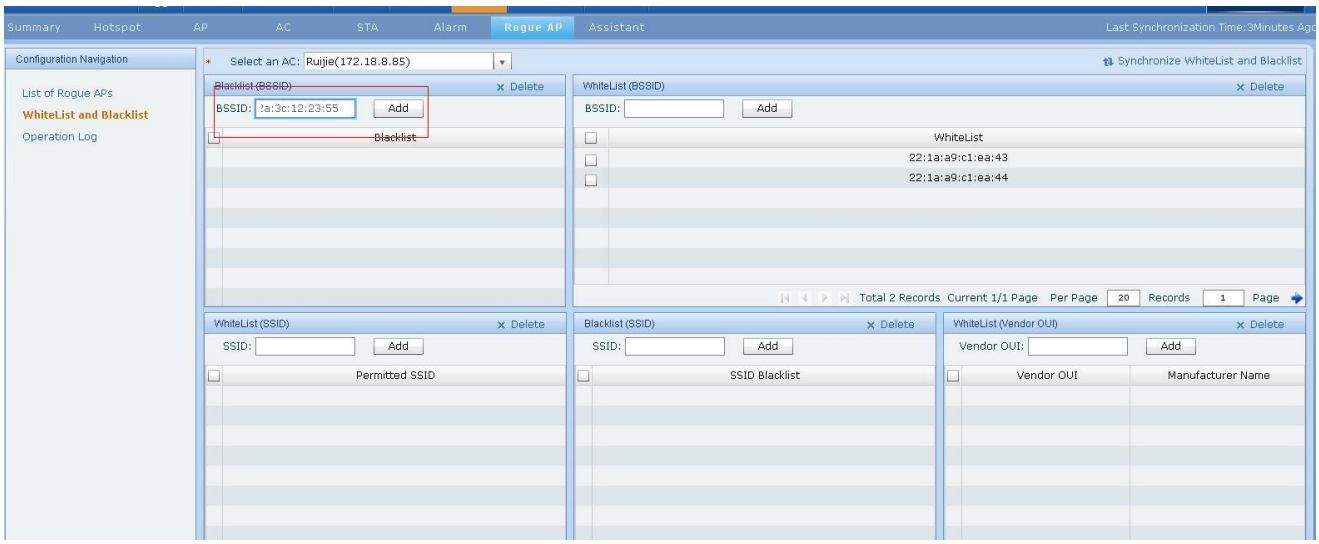


Figure 7.305. Entering BSSID

Click **Add**, as shown in the following figure:

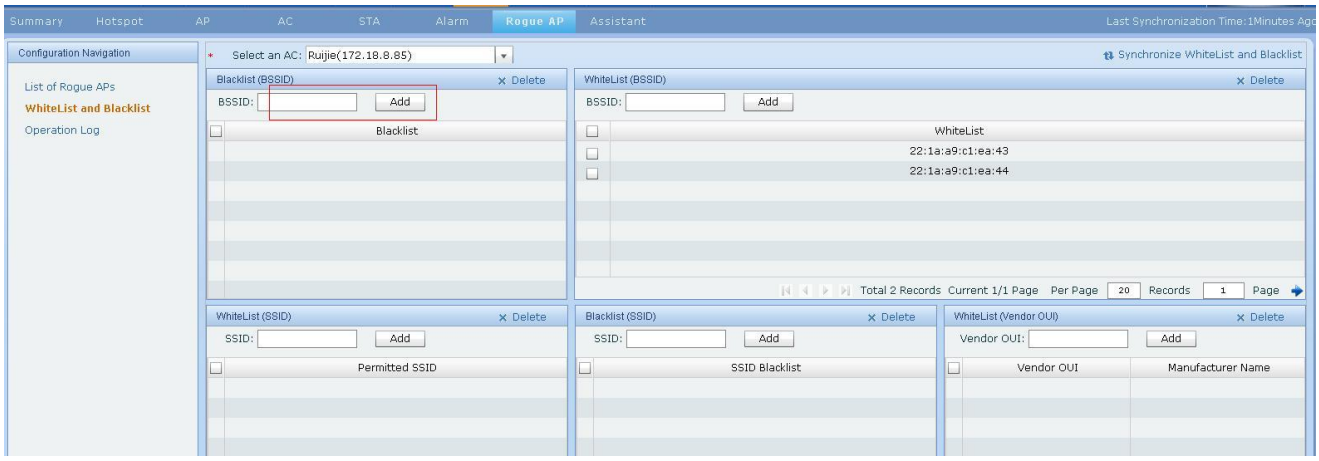


Figure 7.306. Adding Blacklist Entry (BSSID)

Delete Blacklist Entry (BSSID)

76) Select the AC, as shown in the following figure:

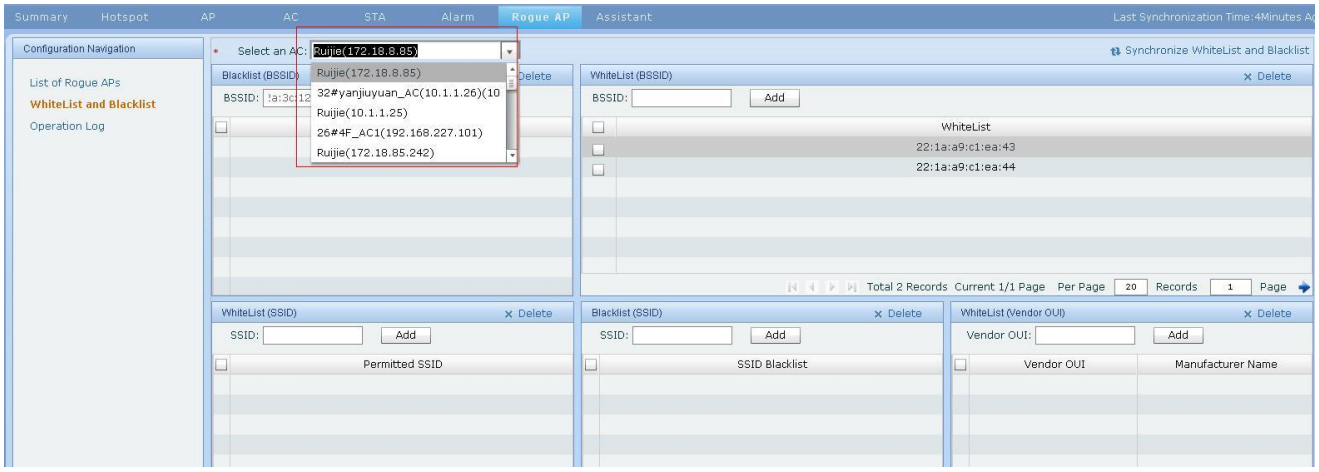


Figure 7.307. Selecting AC

Select the blacklist entry, and click **Delete**, as shown in the following figure:

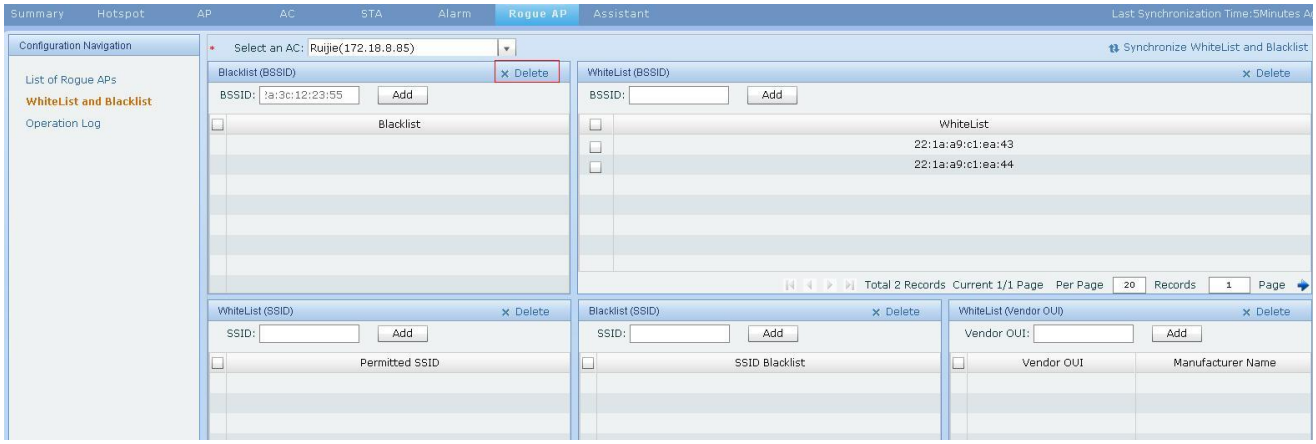


Figure 7.308. Deleting Blacklist Entry (BSSID)

Other Operations

Other Operations on Whitelist and Blacklist including adding/deleting the whitelist entry (BSSID), whitelist entry (SSID), blacklist entry (SSID), and whitelist entry (Manufacturer OUI). These operations are similar to those of adding/deleting the blacklist entry (BSSID).

7.7.3. Operation Log

This function enables you to view operation logs.

View Operation Logs

77) Click **Operation Log**, as shown in the following figure:

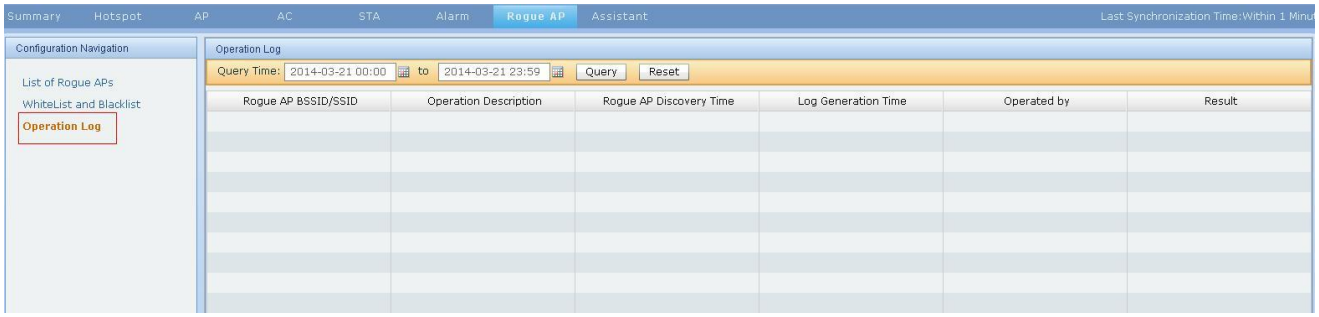


Figure 7.309. Viewing Operation Logs

Select the start time and the end time, and click **Query**, as shown in the following figure:

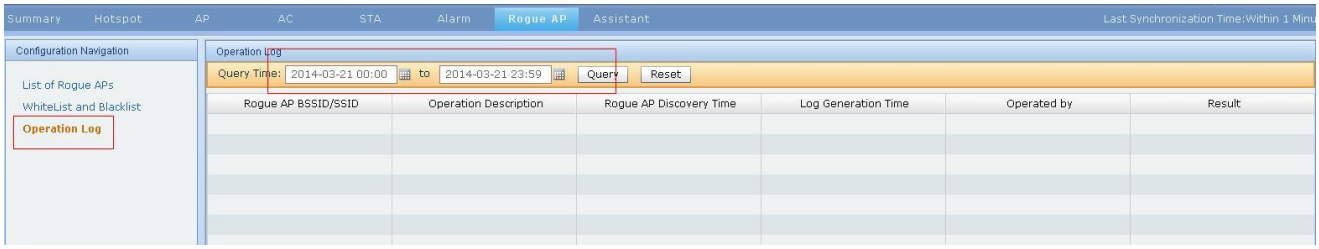


Figure 7.310 Searching Operation Logs

When the search is complete, the result will be displayed.

7.8. Troubleshooting Assistant

Major Functions

- Search
- Real-Time Network Search
- View STA Details

- View Authenticated STA Details

7.8.1. Search

This function enables you to search for the matched entry in accordance with search criteria, such as IP address, MAC address, User Name, Name, Device Name, AP Location, Hotspot Name.

Operation Steps

78) Enter search criteria or nothing, and click **Query**, as shown in the following figure:

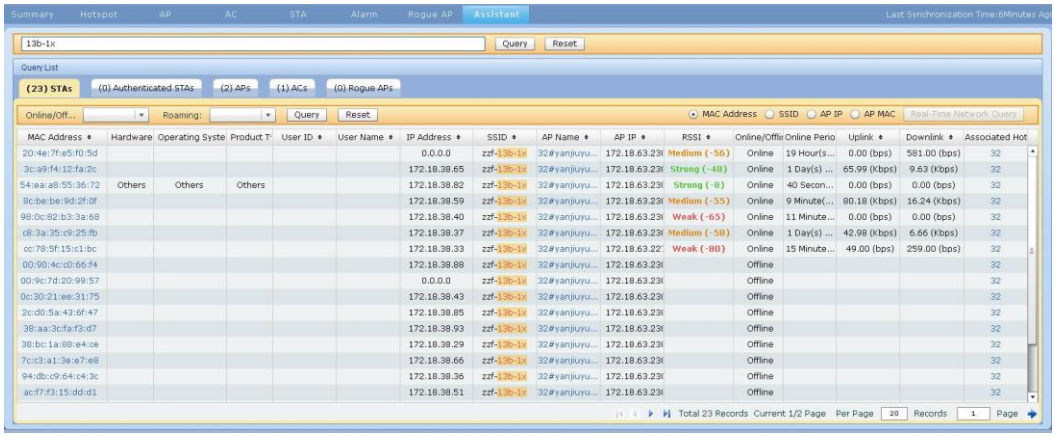


Figure 7.311. Matched Terminal

View the matched Authenticated STA, as shown in the following figure:

Figure 7.312. Matched Authenticated STA

View the matched AP, as shown in the following figure:

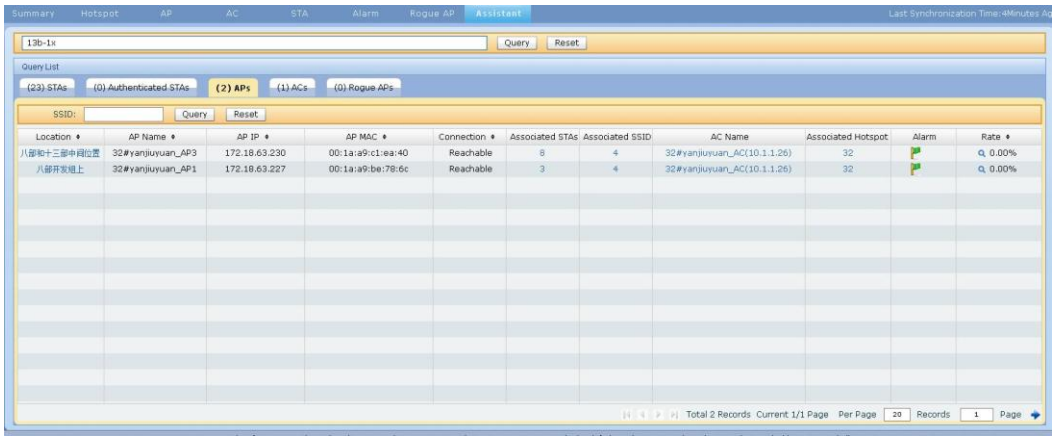


Figure 7.313. Matched AP

View the matched AC, as shown in the following figure:

Figure 7.314. Matched AC

View the matched rogue AP, as shown in the following figure:

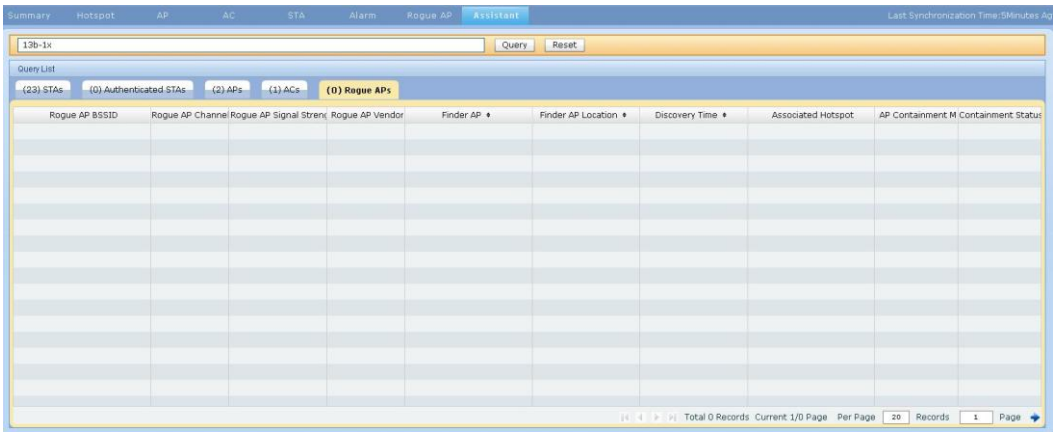


Figure 7.315. Matched Rogue AP

7.8.2. Real-Time Network Search

This function enables you to search for the latest STA information and displays all matched information according to the search criteria.

Operation Steps

79) Enter SSID as the search criteria, such as zzf-13b-1x, and click **Real-Time Network Search**, as shown in the following figure:

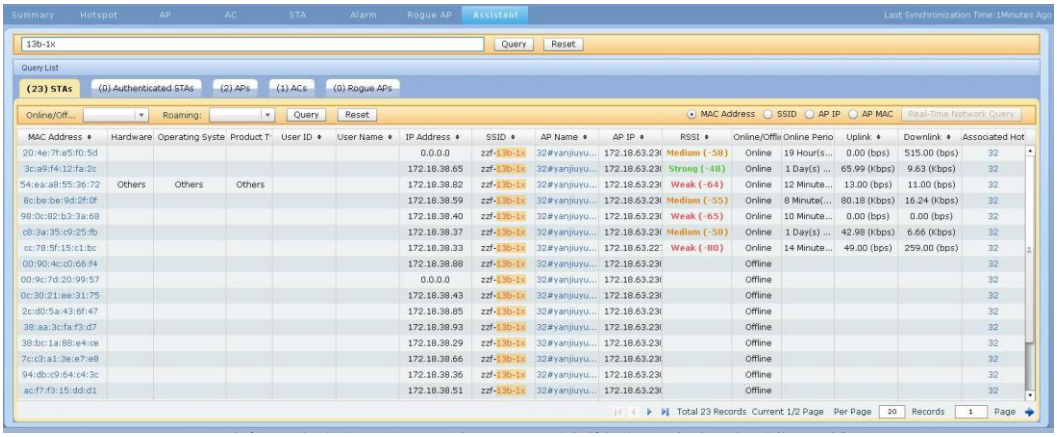


Figure 7.316. Real-Time Network Search

To perform Real-Time Network Search, operations of using other search criteria are similar to those of using SSID as search criteria as mentioned above.

7.8.3. View STA Details

This function enables you to view STA details, including STA Information, Basic STA Information, Associated Device Information, Security Information, Packets Statistics, Signal Quality, STA Online/Offline Record. You can also synchronize STA information, perform real-time performance monitoring (if the terminal is online), and view roaming track(if the terminal is online and it is a roaming user).

View STA Details

80) To view the STA details, click the terminal MAC address to go to the **STA Details** page, as shown in the following figure:

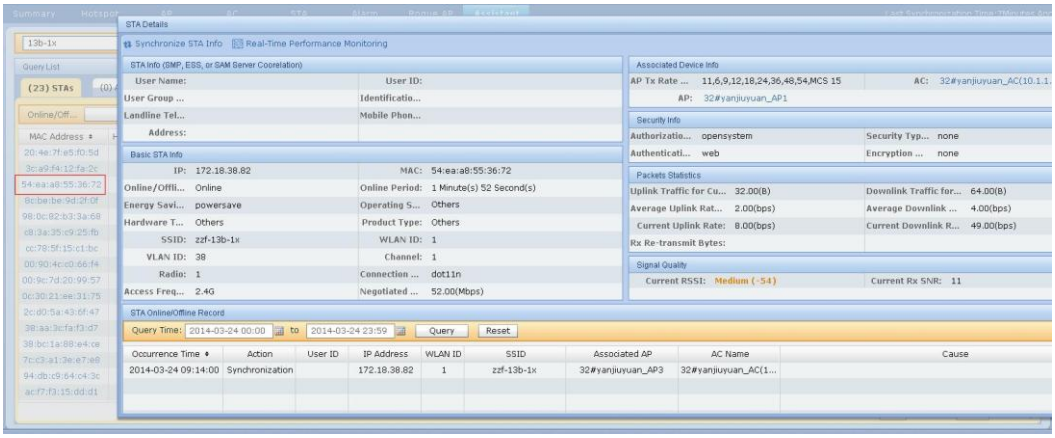


Figure 7.317. Viewing STA Details

Perform Real-Time Performance Monitoring is displayed, as shown in the following figure:

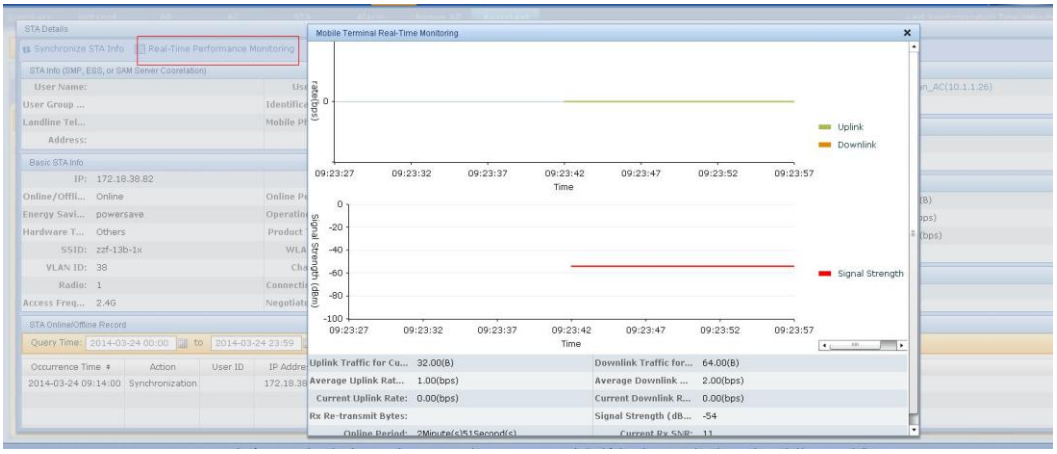


Figure 7.318. Real-Time Performance Monitoring

Select a roaming STA to view its roaming track, as shown in the following figure:

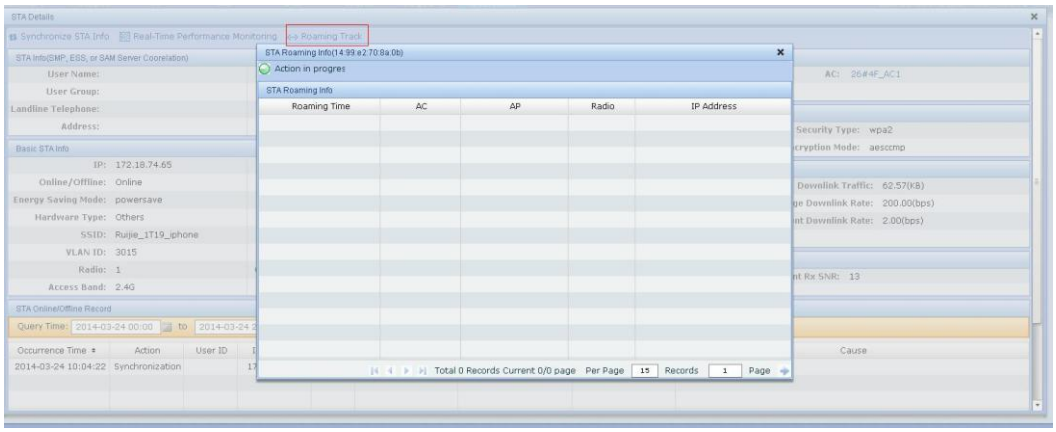


Figure 7.319. Viewing STA Roaming Track

7.8.4. View Authenticated STA Details

This function enables you to view authenticated STA details, including STA Details and STA Online/Offline Record.

View Authenticated STA Details

To view the authenticated STA information, click the STA name in authenticated STA list to go to **STA Details**, as shown in the following figure:

Figure 7.320. Viewing Authenticated STA Details

7.9. Spectrum Analysis

Major Functions

- Spectrum Interference Alarm
- Spectrum Analysis Configuration
- Spectrum Analysis and Monitoring

7.9.1. Spectrum Interference Alarm

Spectrum Interference Alarm is an alarm sent by the manager AC, indicating that the associated AP is interfered by Bluetooth, microwave, cordless phones, continuous wave, video bridges or other sources.

Spectrum Interference Alarm

Spectrum Interference Alarm is shown in the following figure:

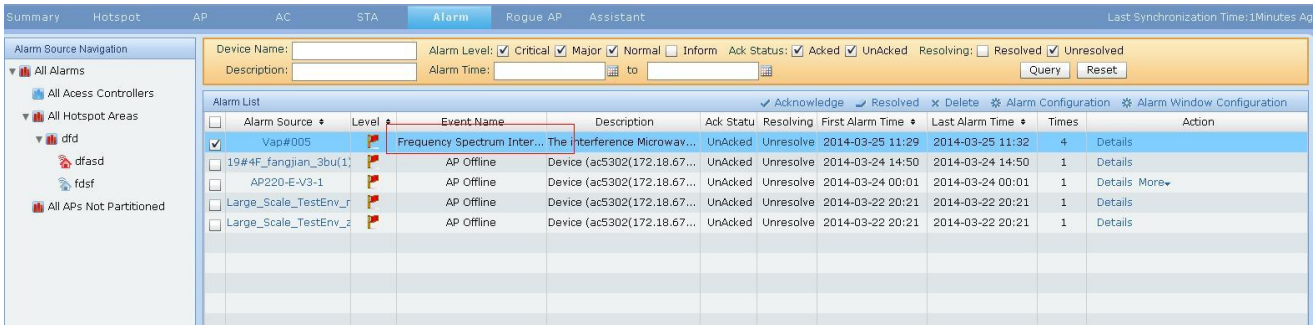


Figure 7.321. Spectrum Interference Alarm

7.9.2. Spectrum Analysis Configuration

This function enables you to enable/disable spectrum analysis on AP List, AP Details, and Alarm List.

Spectrum Analysis Configuration

81) Enable/disable spectrum analysis on **AP List**, as shown in the following figure:

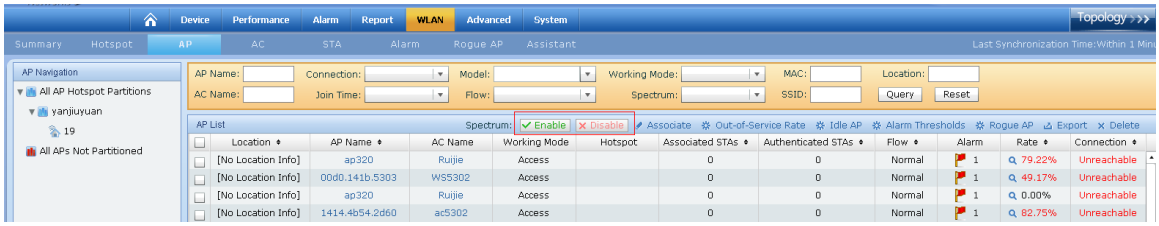


Figure 7.322. Configuring Spectrum Analysis on **AP List**

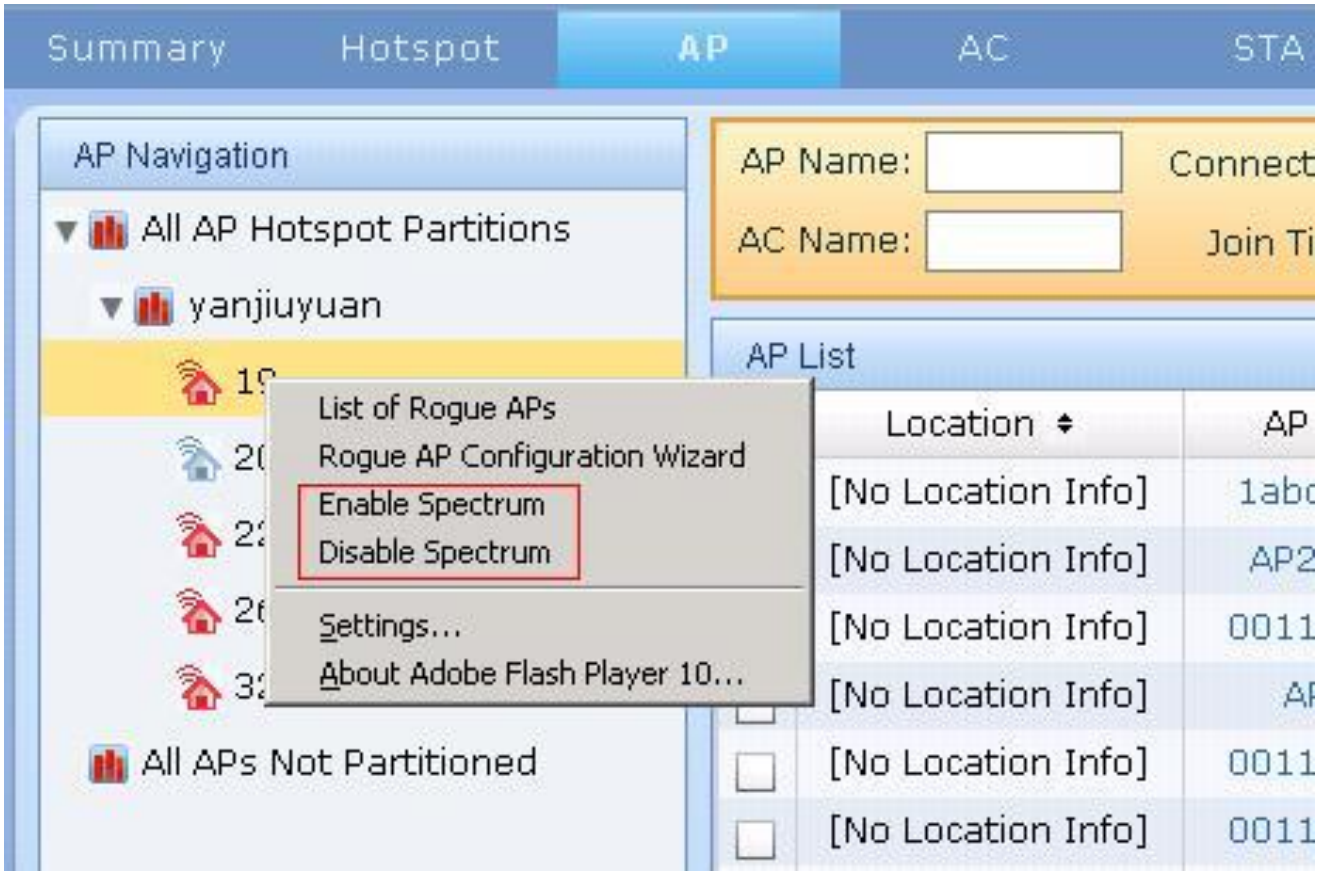


Figure 7.323. Configuring Spectrum Analysis on **AP Navigation**

Enable/disable spectrum analysis on **AP Details**, as shown in the following figure:

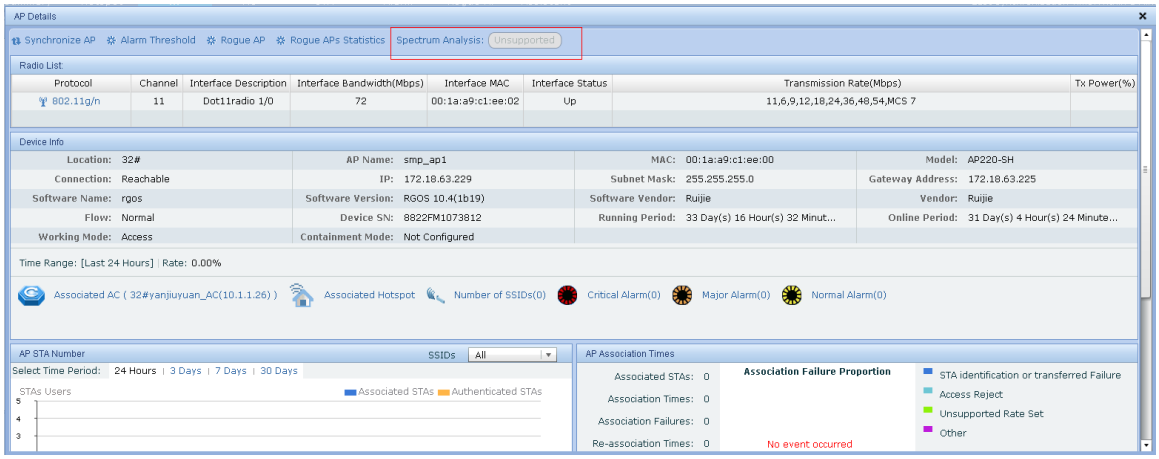


Figure 7.324. Configuring Spectrum Analysis on **AP Details**

Enable/disable spectrum analysis on **Alarm List**, as shown in the following figure:

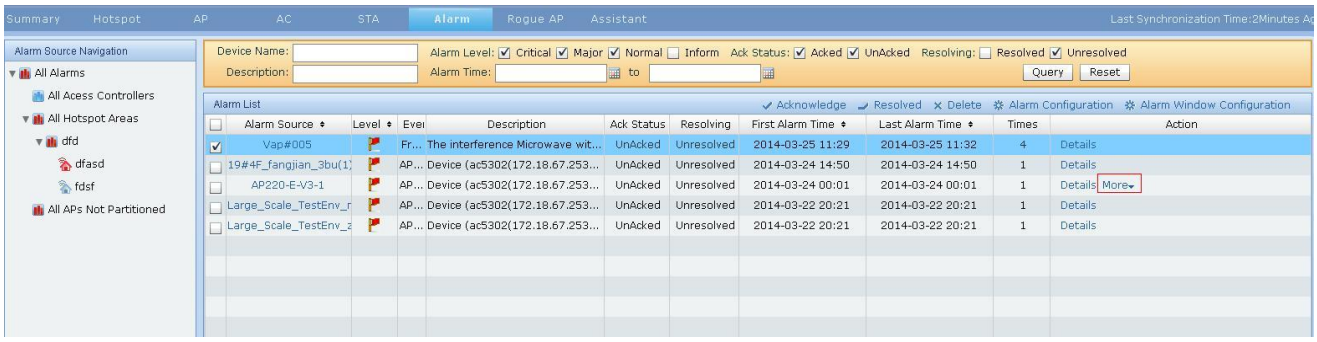


Figure 7.325. Configuring Spectrum Analysis on **Alarm List**

7.9.3. Spectrum Analysis and Monitoring

Spectrum Analysis and Monitoring consists of the following charts:

- Current Interference List indicates the interference type, frequency, channel, and signal strength
- Spectrum Chart presents a scrolling display of spectrum data including Frequency/Channel, Frequency/Time, Frequency/Signal in a two dimensional graph
- Real-Time FFT Chart provides real-time FFT curve graph in Power and Channel dimensions, showing the signal strength of every frequency points
- FFT Duty Cycle Chart, calculated by the duty cycle threshold of spectrum analysis in a period of time, displays the valid signal strength ratio on every frequency points
- Spectrum Density Chart displays the signal strength statistics on every frequency points in 30 seconds
- Channel Duty Cycle Chart, calculated by the duty cycle threshold of spectrum analysis in a period of time, displays the valid signal strength ratio on every channels, enabling you to know the channel utilization
- Channel Duty Cycle Chart displays Utilization Trend on the Selected Channel
- Power Trend Chart displays Power Trend on the Selected Frequency Point

Spectrum Analysis and Monitoring

82) Go to the **Spectrum Analysis** and **Monitoring** page on **AP Details**, as shown in the following figure:

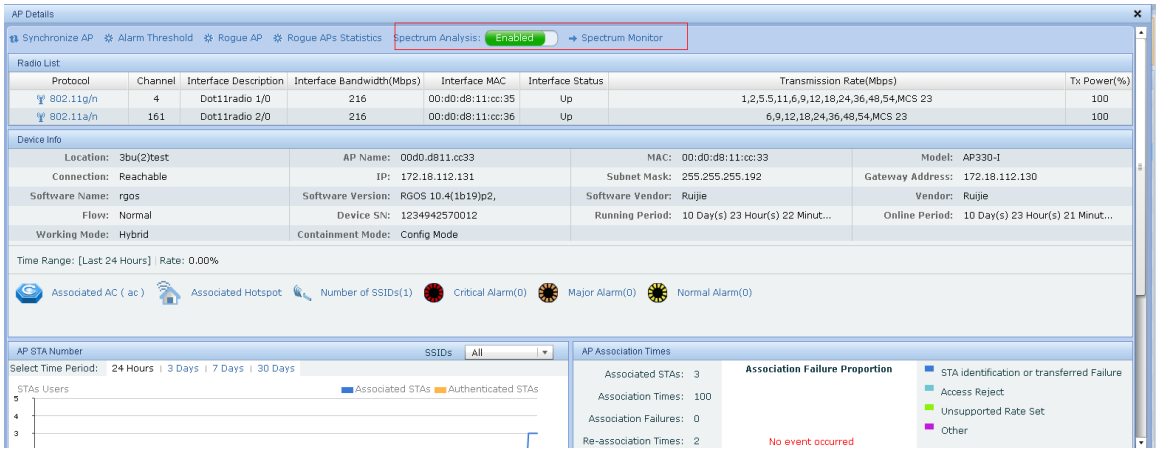


Figure 7.326. Going to **Spectrum Analysis** and **Monitoring** on **AP Details**

Go to the **Spectrum Analysis** and **Monitoring** page on **Alarm List**, as shown in the following figure:

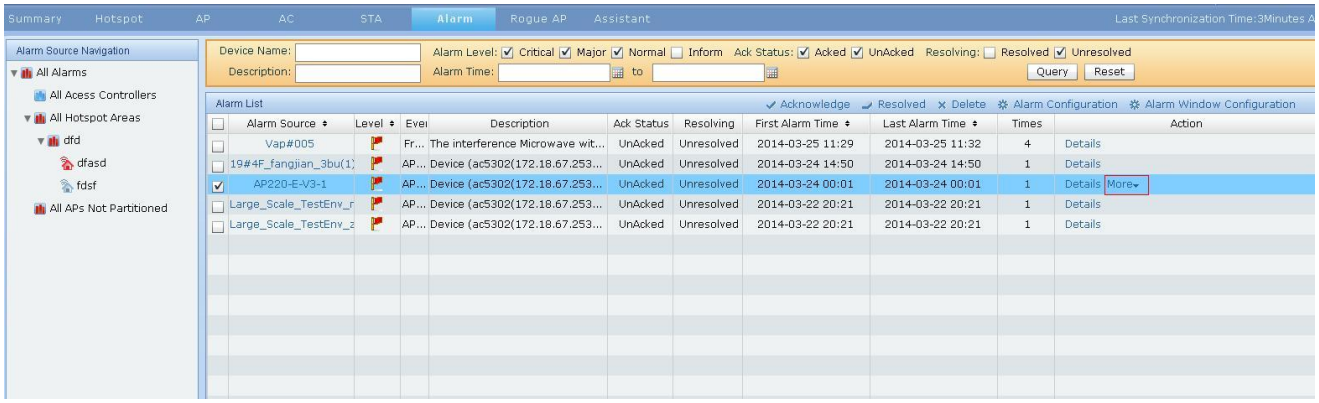


Figure 7.327. Going to **Spectrum Analysis** and **Monitoring** on **Alarm List**

Spectrum Analysis and Monitoring

83) Basic Spectrum Chart 1 includes Spectrum Chart, Real-Time FTT Chart, FTT Duty Cycle Chart, Spectrum Density Chart, as shown in the following figure:

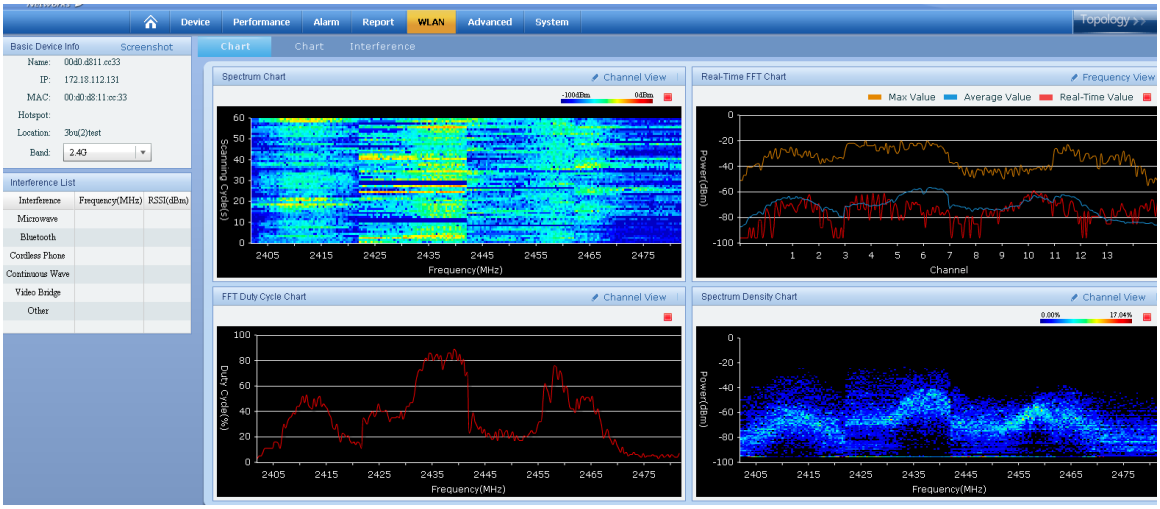


Figure 7.297. Spectrum Chart, Real-Time FTT Chart, FTT Duty Cycle Chart, Spectrum Density Chart

Basic Spectrum Chart 2 includes Channel Duty Cycle Chart, Channel Duty Cycle Trend Chart, Power Trend Chart, as shown in the following figure:

Figure 7.328. Channel Duty Cycle Chart, Channel Duty Cycle Trend Chart, Power Trend Chart

Interference List displays interference type (source), such as Bluetooth, microwave, cordless phones, continuous wave, video bridges or other sources.

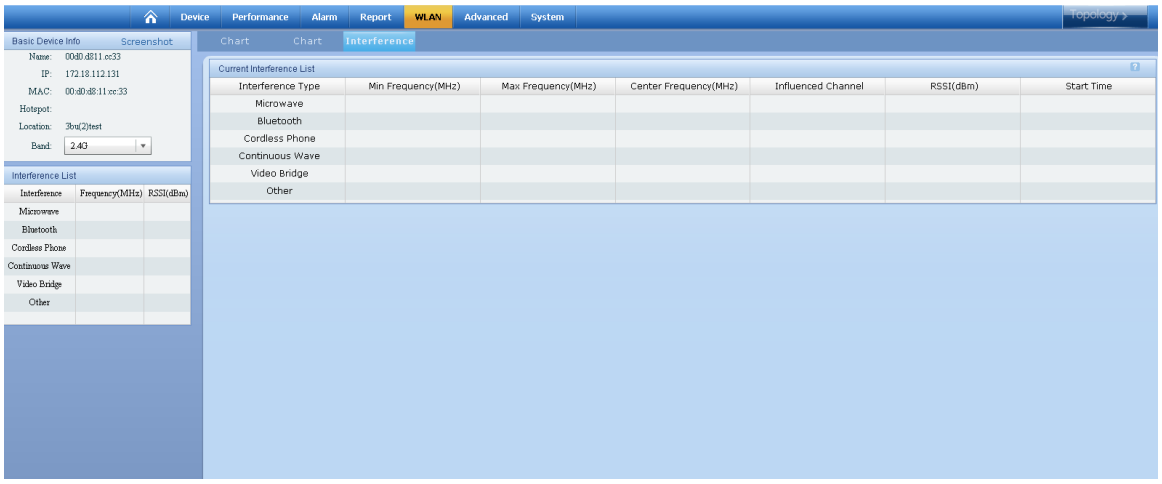


Figure 7.329. Current Interference List

7.10. Wireless Logical Topology

Operation Steps

1. Choose **WLAN** > **Topology**.
2. View the APs and STAs associated with all hotspots on the **Hotspot View** page.

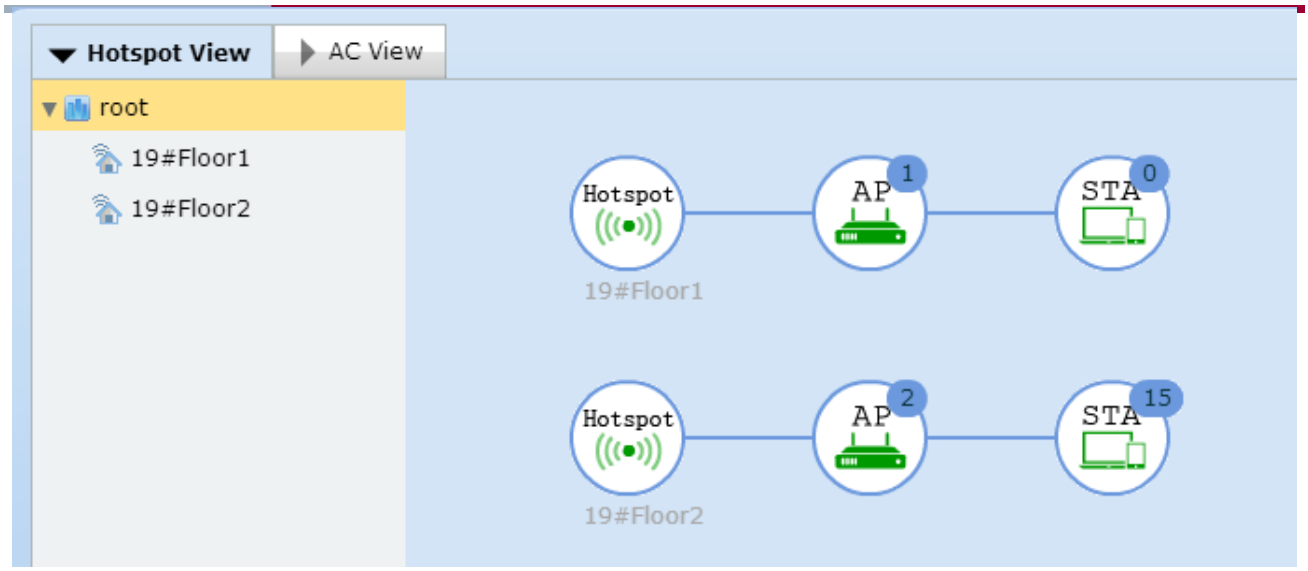


Figure 7.330. Hotspot View

3. View all ACs and associated APs and STAs on the **AC View** page.

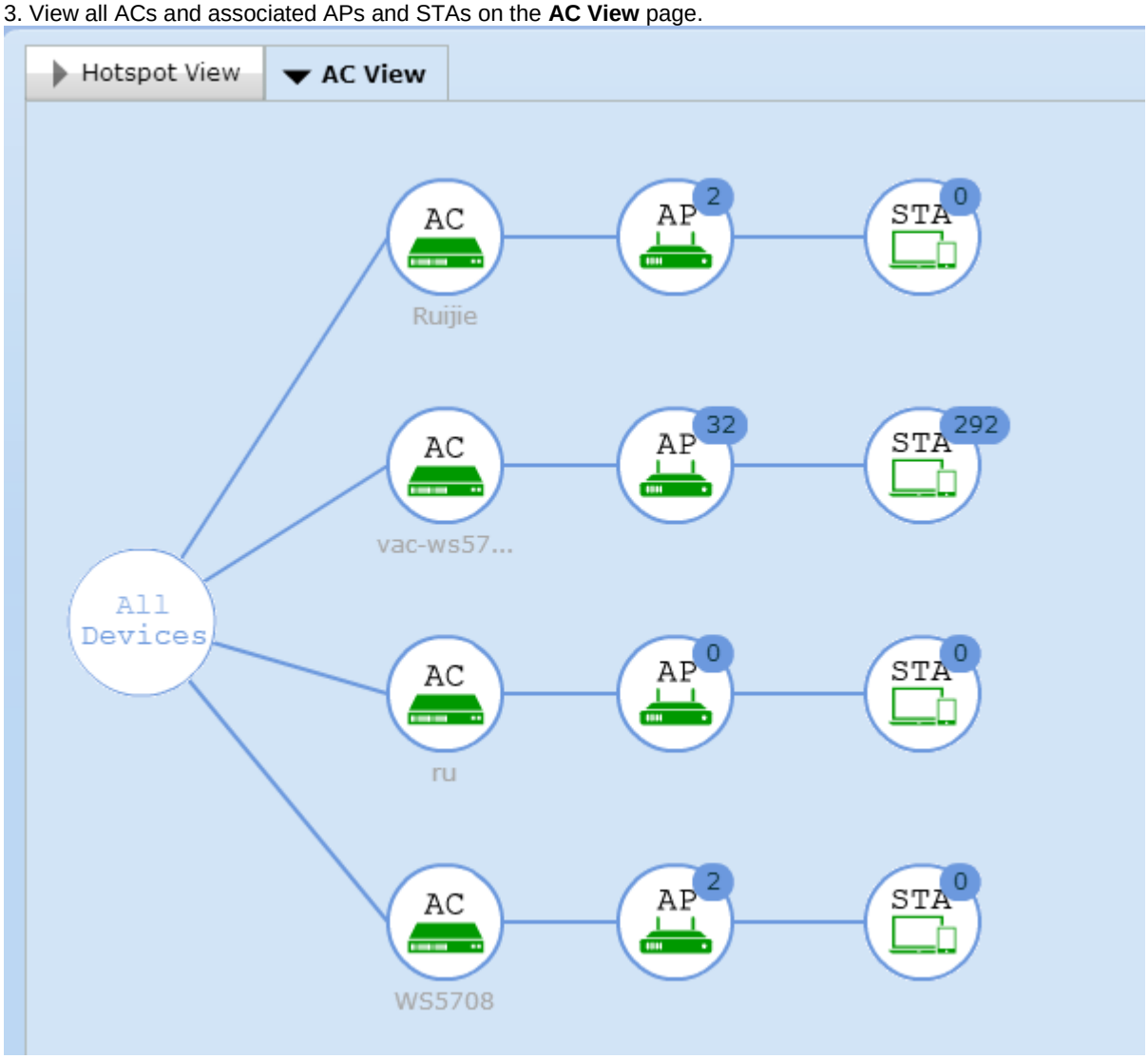


Figure 7.331. AC View

7.11. Fat AP Spectrum Analysis and Monitoring

Because WLAN does not support fat APs, added fat APs are displayed on the **Device** > **Device List** page.

1. Choose **Device** > **Add**, as shown in the following figure.

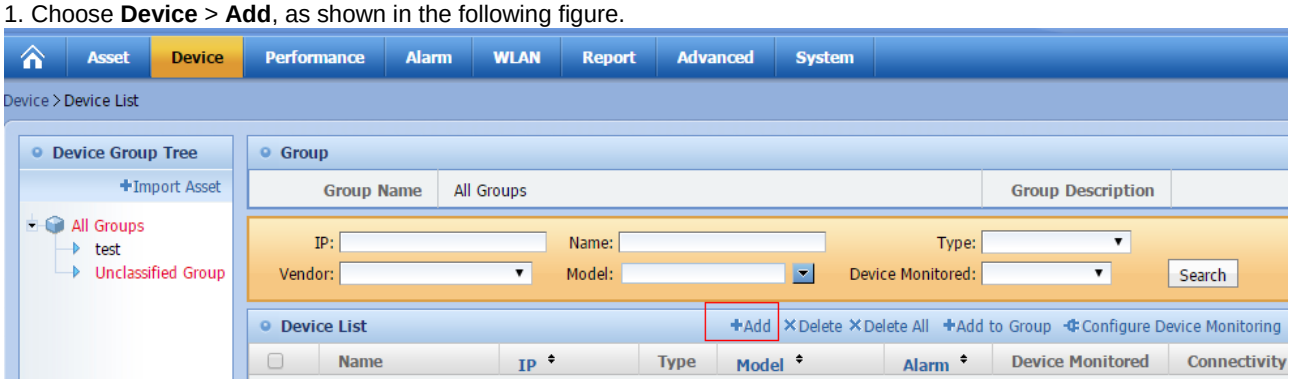


Figure 7.332. Clicking **Add**

2. Fill in fat AP information and click **Add**, as shown in the following figure.

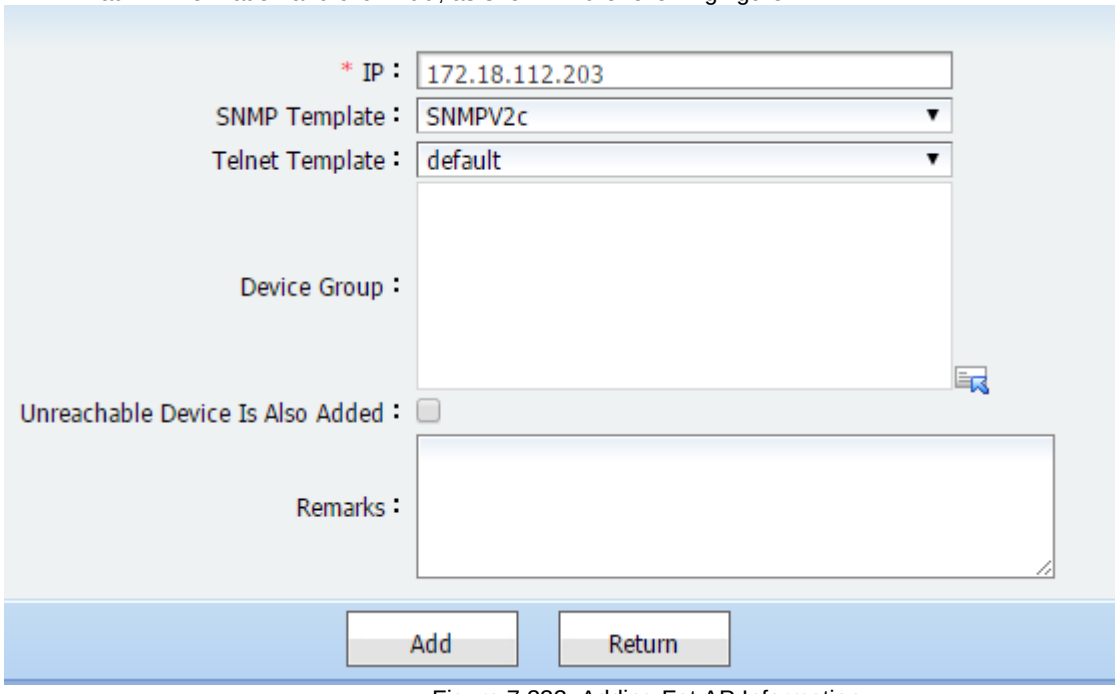


Figure 7.333. Adding Fat AP Information

3. Click a device link in the **Device List** to go to the detail page, as shown in the following figure.

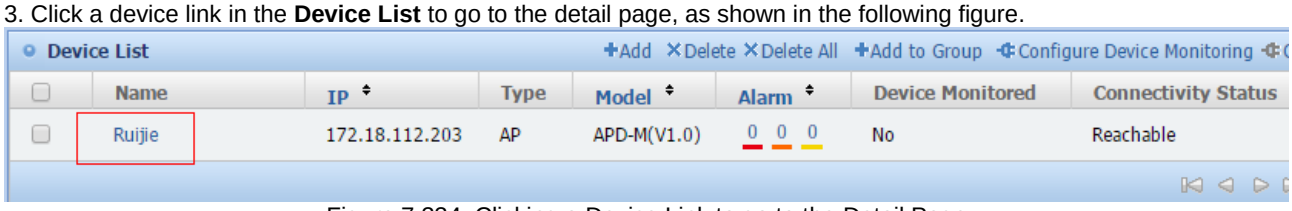


Figure 7.334. Clicking a Device Link to go to the Detail Page

4. Choose **WLAN** > **Spectrum Analysis and Monitoring** in the left-side navigation bar, as shown in the following figure.

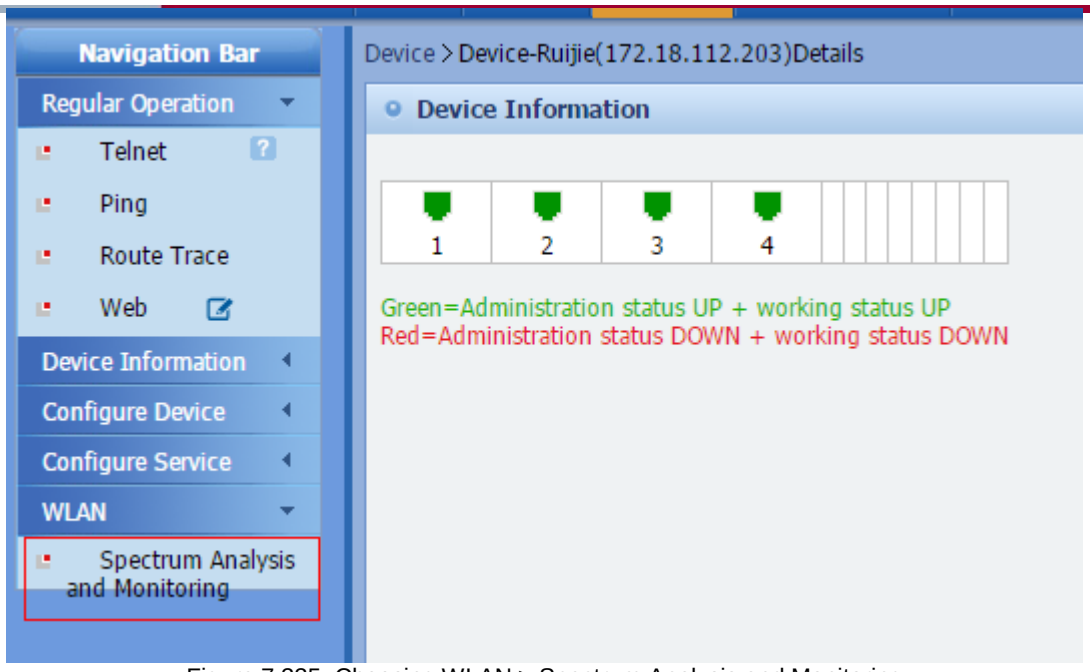


Figure 7.335. Choosing WLAN > Spectrum Analysis and Monitoring

5. View the spectrum analysis and monitoring charts of the fat AP, as shown in the following figure.

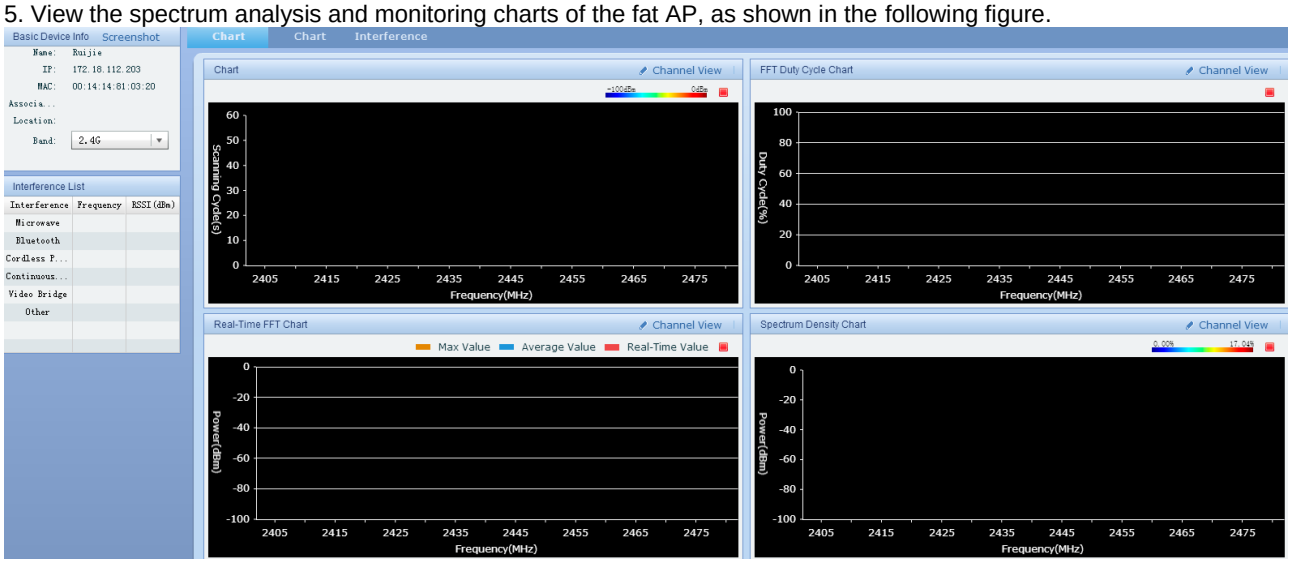


Figure 7.336. Spectrum Analysis and Monitoring Charts of the Fat AP

Note:
Enable spectrum analysis before you view the spectrum analysis and monitoring charts of fat APs.
Currently, only the spectrum analysis and monitoring of fat APs is supported, but spectrum analysis configuration and alarm is not supported.

7.12. Permissions

The super administrator can create subordinate administrators, and subordinate administrators can manage their respective SSIDs and APs. For example, the education commission of Xihu District has the super administrator permissions. It creates a school administrator account after login. The school administrator logs in to the SNC with this account to create SSIDs locally and select the desired authentication method. However, the school administrator cannot manage the SSIDs and APs of other schools. Related operations include:

- The super administrator adds and creates hotspots.
- The super administrator assigns permissions.
- The school administrator performs operations.

7.12.1. Adding and Creating Hotspots (Super Administrator)

The super administrator can create subordinate administrators, and subordinate administrators can manage their respective SSIDs and APs. For example, the education commission of Xihu District has the super administrator permissions. It creates a school administrator account after login. The school administrator logs in to the SNC with this account to create SSIDs locally and select the desired authentication method. However, the school administrator cannot manage the SSIDs and APs of other schools.

1. Log in to the SNC as super admin.

2. Choose **WLAN** > **AC** and add an AC. After the AC is successfully added, the AC and associated AP information is displayed, as shown in the following figure.

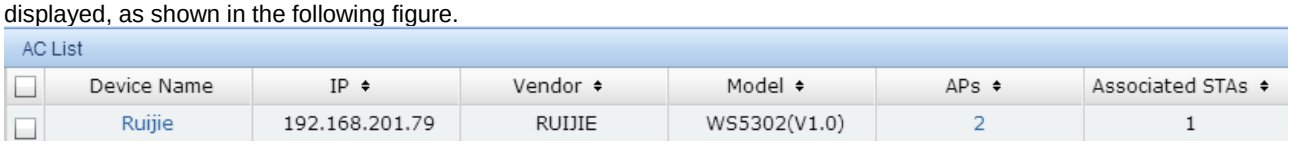


Figure 7.337. AC List

3. Click the device name to go to the **AC Details** page. Click **Details**, as shown in the following figure:

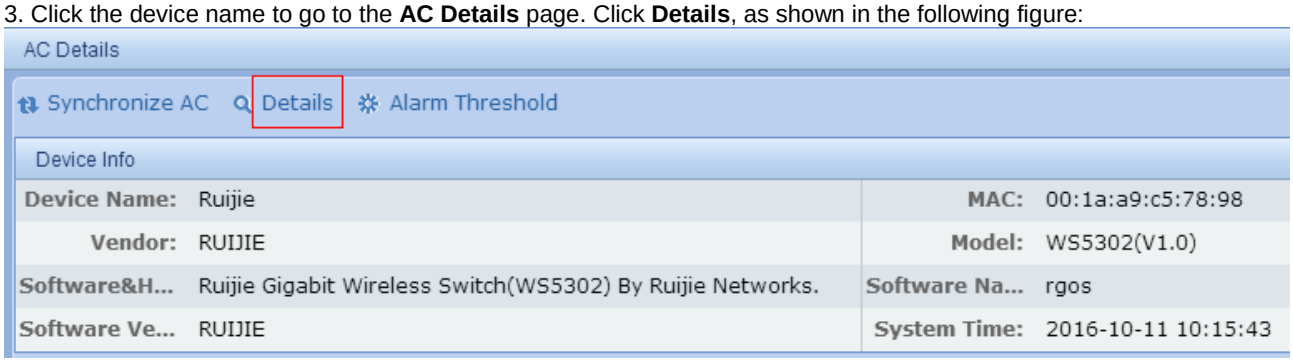


Figure 7.338. AC Details

4. Choose **WLAN** > **AC** and click a device name to display the **AC Details** page. Click **Details** to display the **Controller** page. Choose **WLAN** > **WLAN Configuration**, and click **Sync** in the displayed **WLAN Configuration** page, as shown in the following figure.

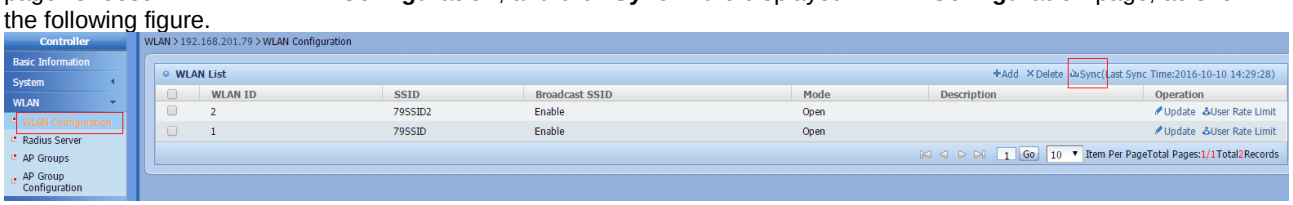


Figure 7.339. SSID Synchronization

5. Choose **WLAN** > **AC** and click a device name to display the **AC Details** page. Click **Details** to display the **Controller** page. Choose **WLAN** > **AP Groups**, and click **Sync** in the displayed **AP Groups** page, as shown in the following figure.

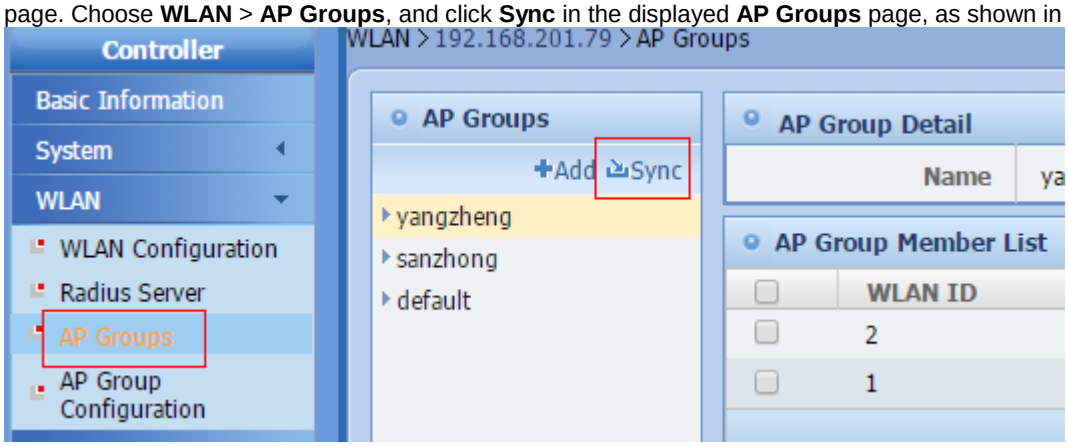


Figure 7.340. AP Group Synchronization

The **AP Group Configuration** page shows that each of the two AP groups has one AP.

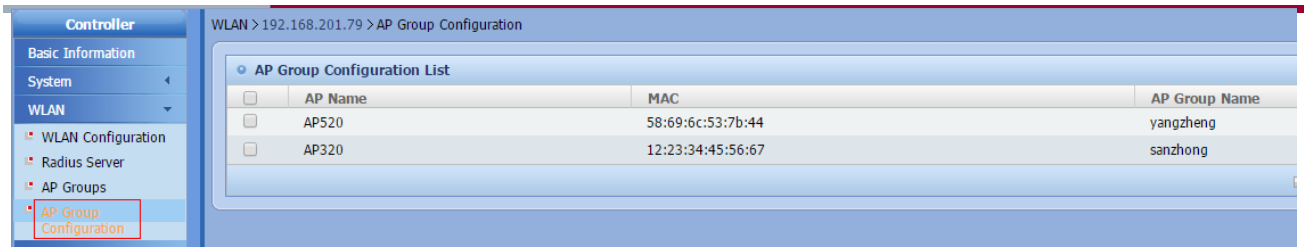


Figure 7.341. AP Group Members

6. Go to the **Hotspot** page to add hotspots and associate APs. The following figure shows that hotspots are created for two schools (**yangzheng** and **sanzhong**). Associate APs to each of the two hotspots.

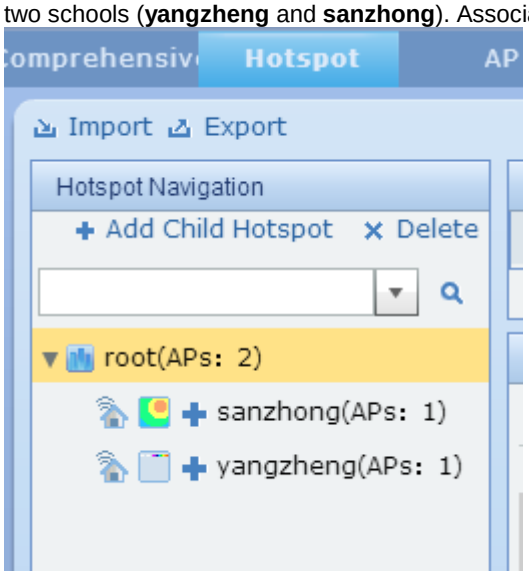


Figure 7.342. Associating APs to Hotspots

7.12.2. Assigning Permissions (Super Administrator)

Add the school administrator.

1. Log in to the SNC and choose **System** > **Admin** > **Role**, as shown in the following figure.

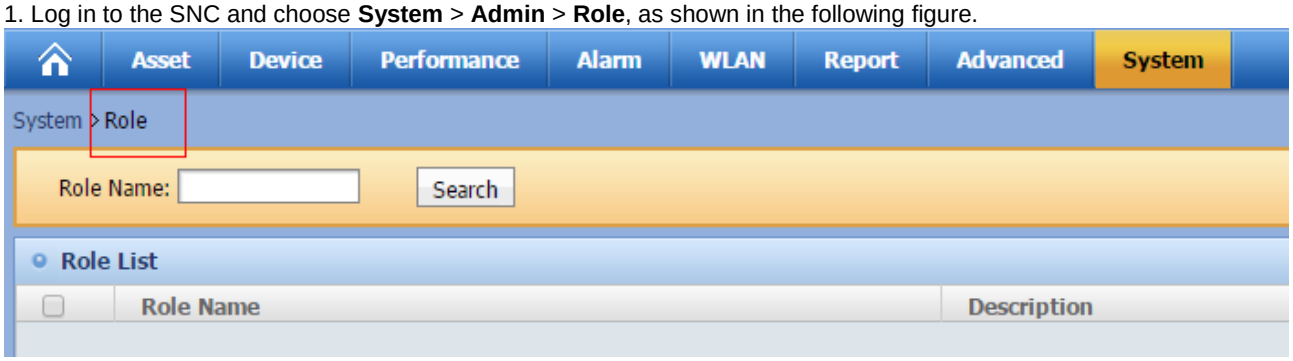


Figure 7.343. Role Management Page

2. Add the administrator to each school and select **READ-ONLY** permission, as shown in the following figure.

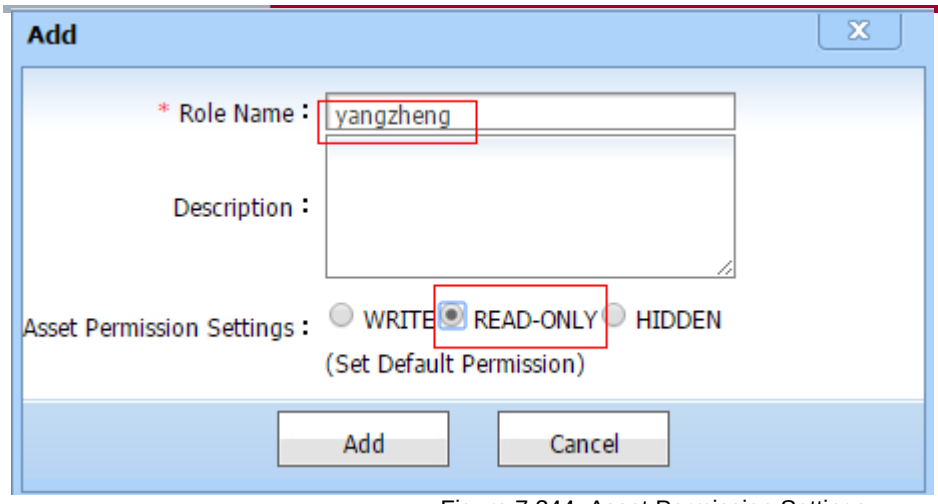


Figure 7.344. Asset Permission Settings

3. Click **Authorization** to assign the SNC system permissions (menu operation permissions) to role **yangzheng**, as shown in the following figure.

Figure 7.345. Permission Settings

4. Assign permissions based on requirements, as shown in the following figure.

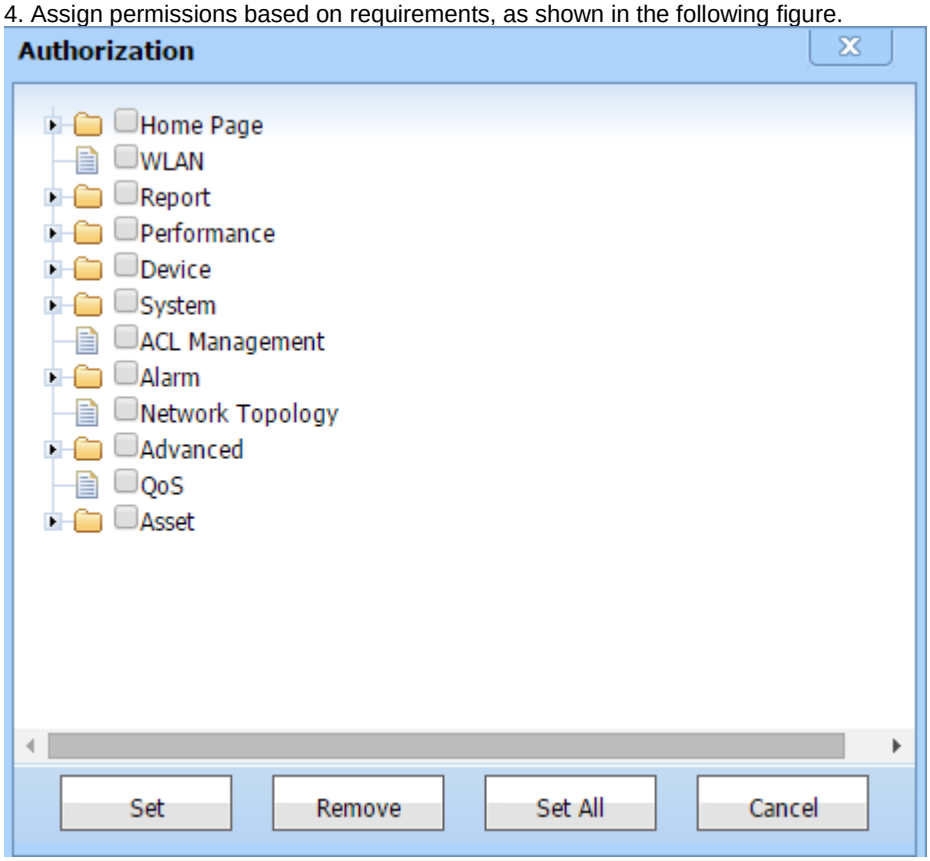


Figure 7.346. Permission Settings

5. Repeat the preceding steps to add role **sanzhong**, as shown in the following figure.

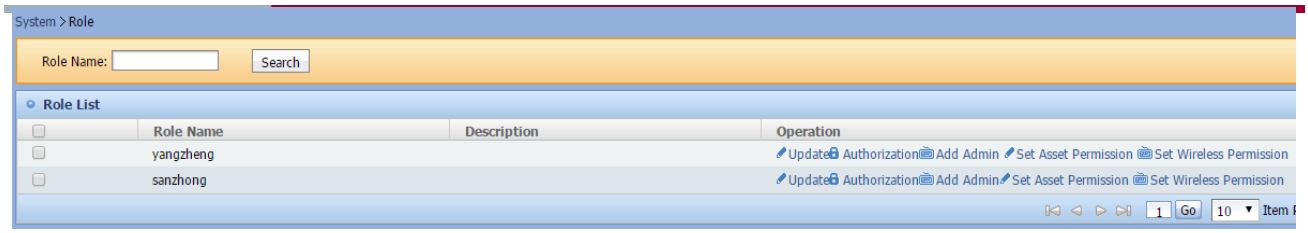


Figure 7.347. School Administrator List

6. Choose **System** > **Admin** > **Admin** to assign roles to the administrators, as shown in the following figure.

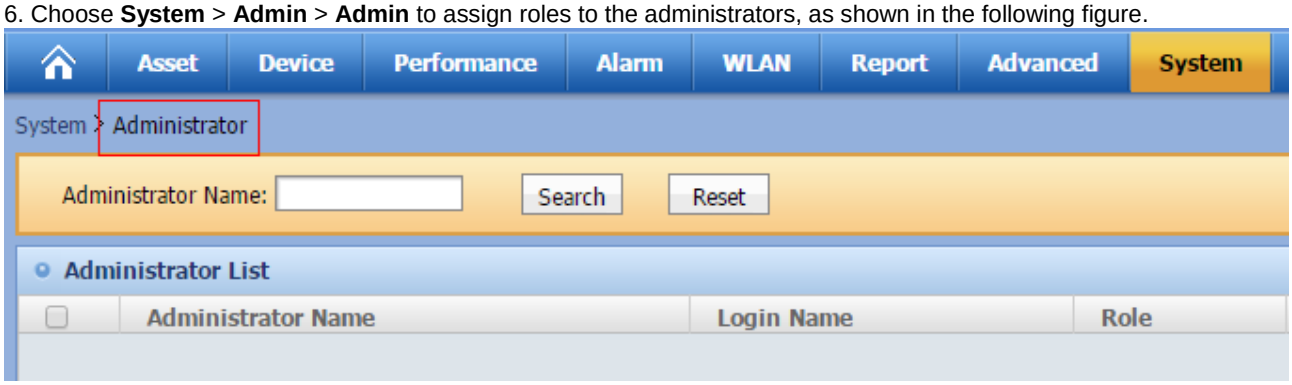


Figure 7.348. School Administrator List

7. To add an administrator for role **yangzheng**, select **yangzheng** for **Role** and set other mandatory items based on the actual condition, as shown in the following figure.

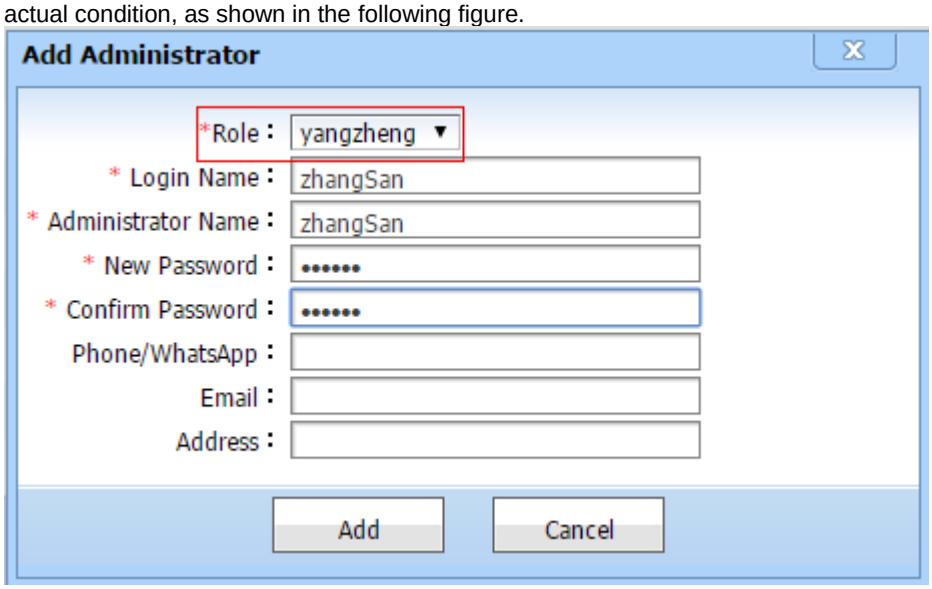


Figure 7.349. Role Assignment

8. Click **Add**. The **Administrator List** is displayed, as shown in the following figure.

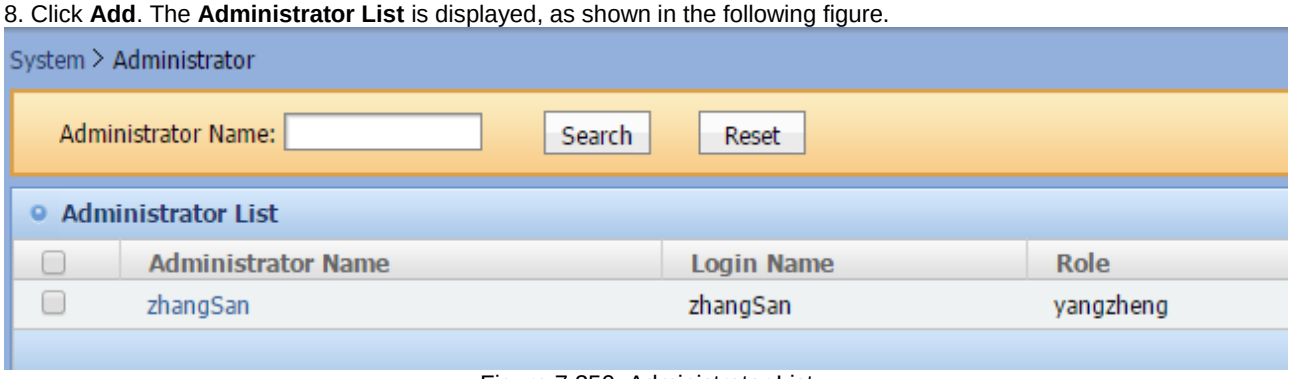


Figure 7.350. Administrator List

9. Repeat the preceding steps to add the other administrator accounts, as shown in the following figure.

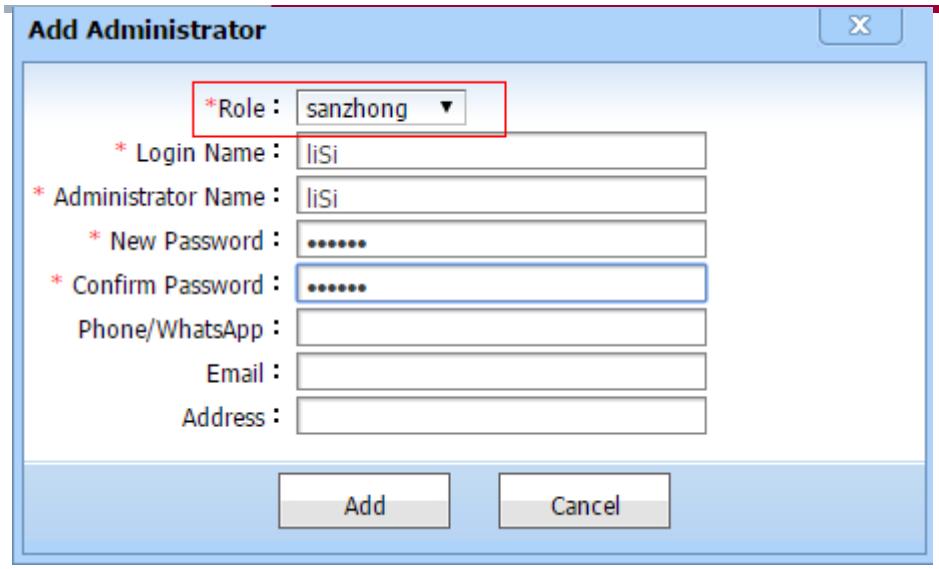


Figure 7.351. Role Assignment

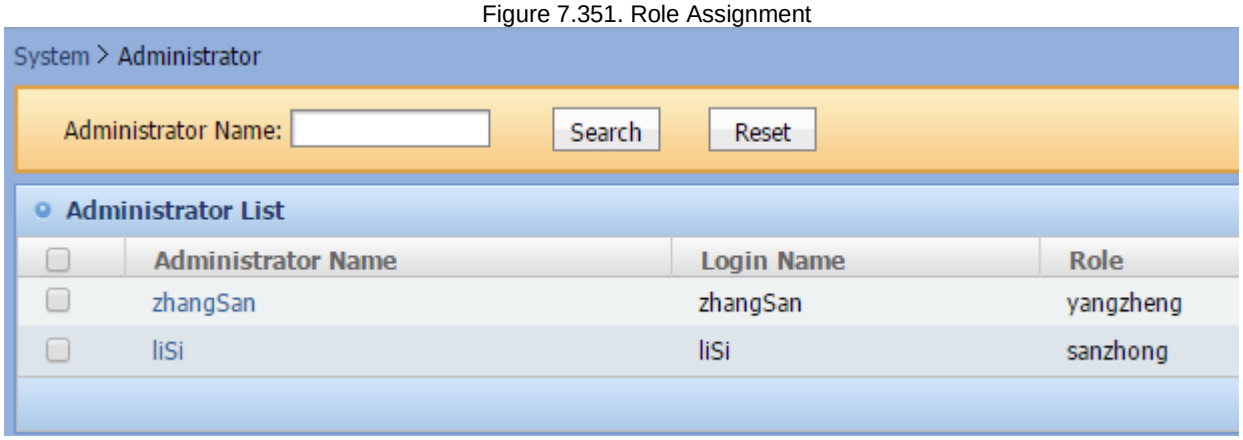


Figure 7.352. Administrator List

10. Choose **System** > **Admin** > **Role** and click **Set Wireless Permission** in the **Role List**, as shown in the following figure.

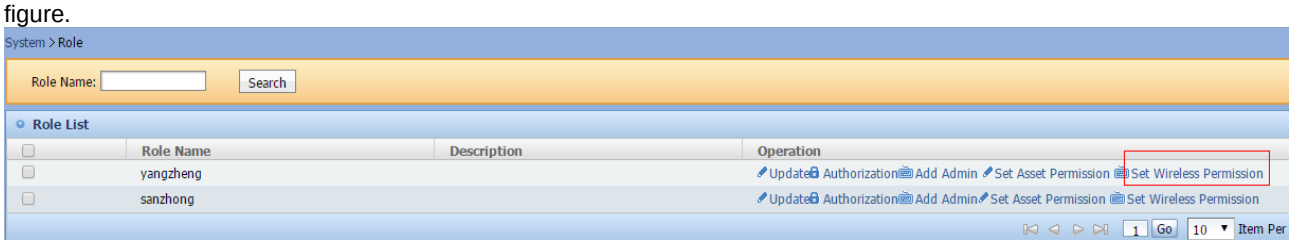


Figure 7.353. Set Wireless Permission

11. Assign hotspot permissions to role **yangzheng**, as shown in the following figure.

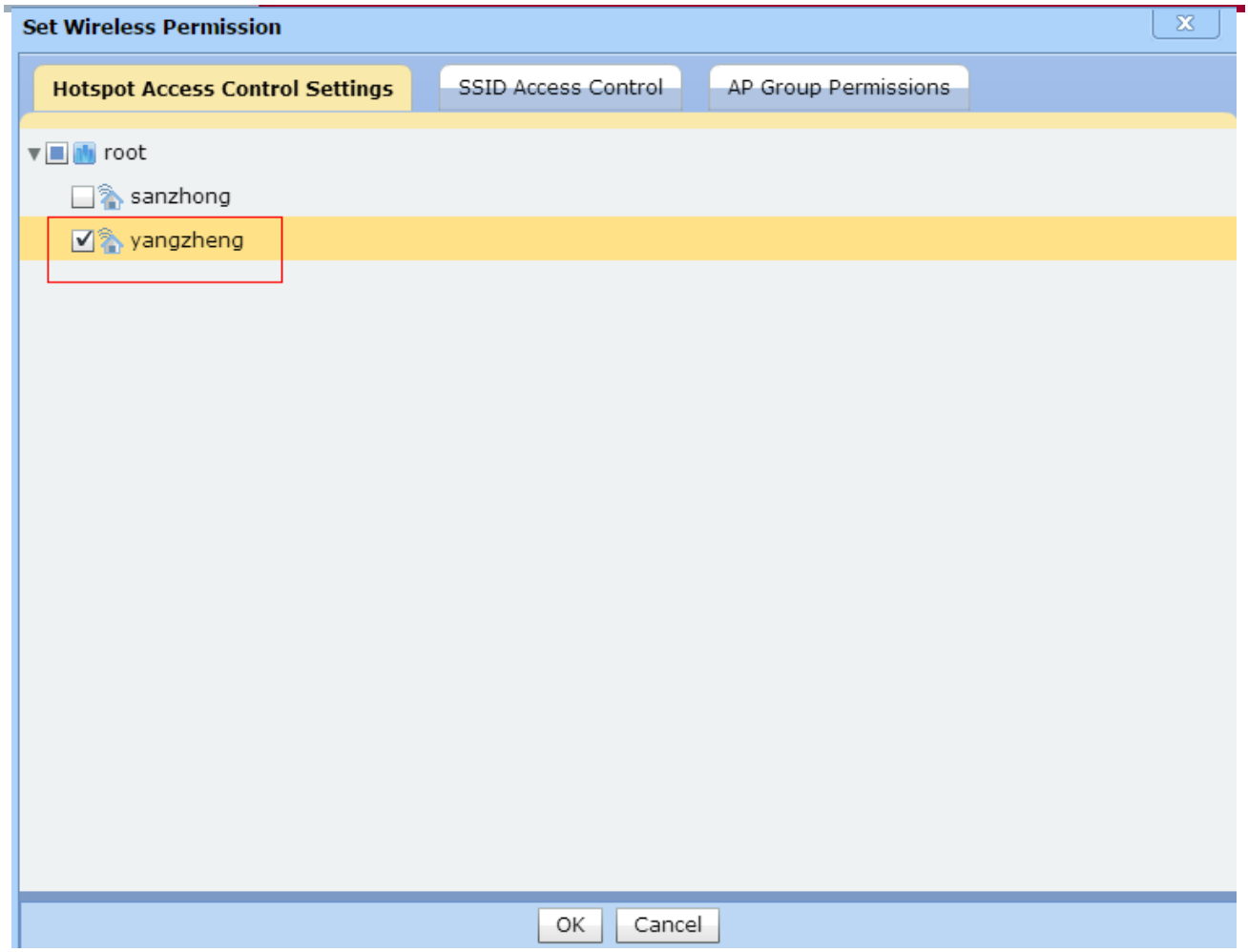


Figure 7.354. Hotspot Permission Assignment

12. Assign SSID permissions to role **yangzheng**. Select **Grant Permissions on SSID**, as shown in the following figure. After that, the administrator can create SSIDs after login.

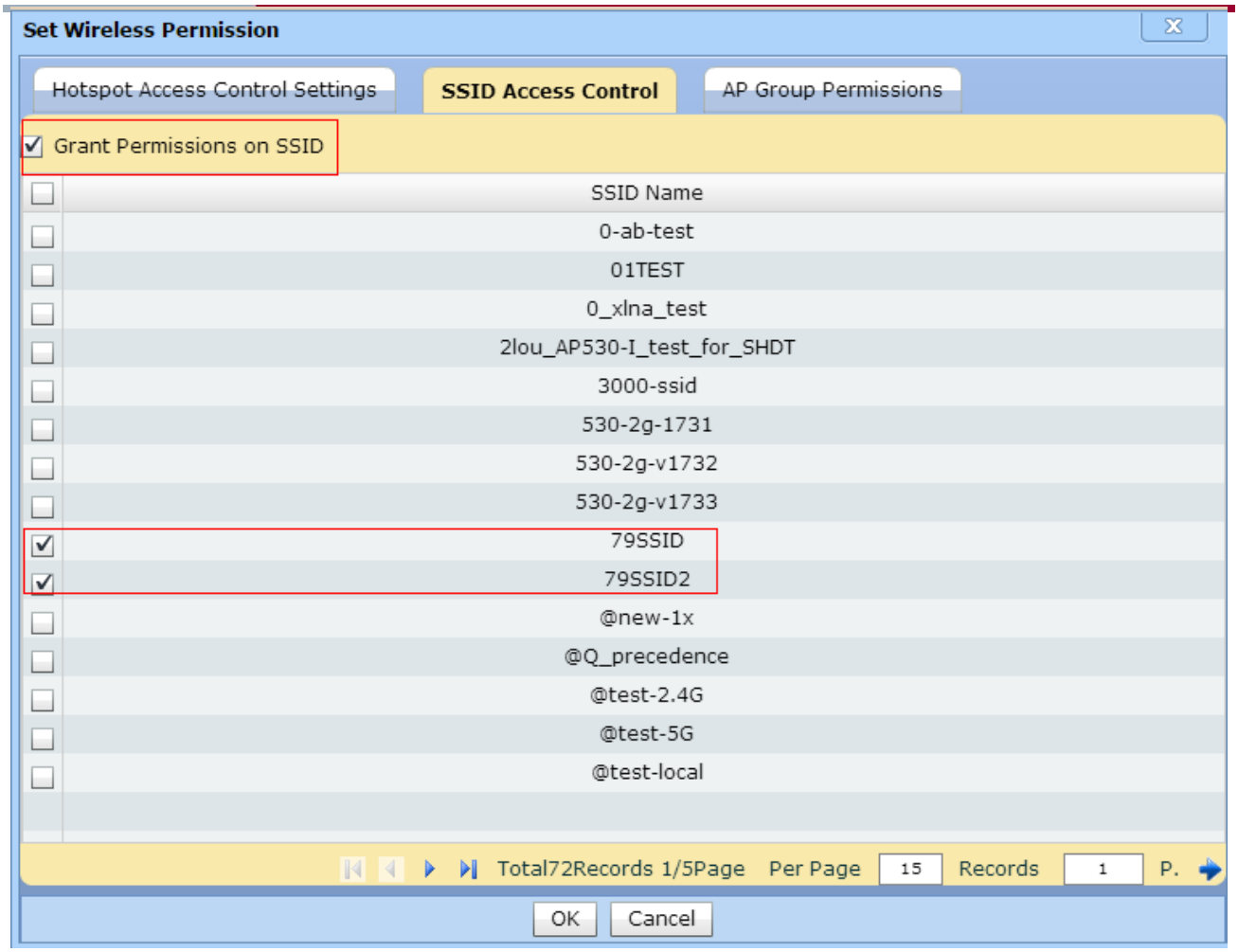


Figure 7.355. SSID Permission Assignment

13. Assign AP group permissions to role **yangzheng**. Select the corresponding AP group associated with the hotspot and click **OK**, as shown in the following figure.

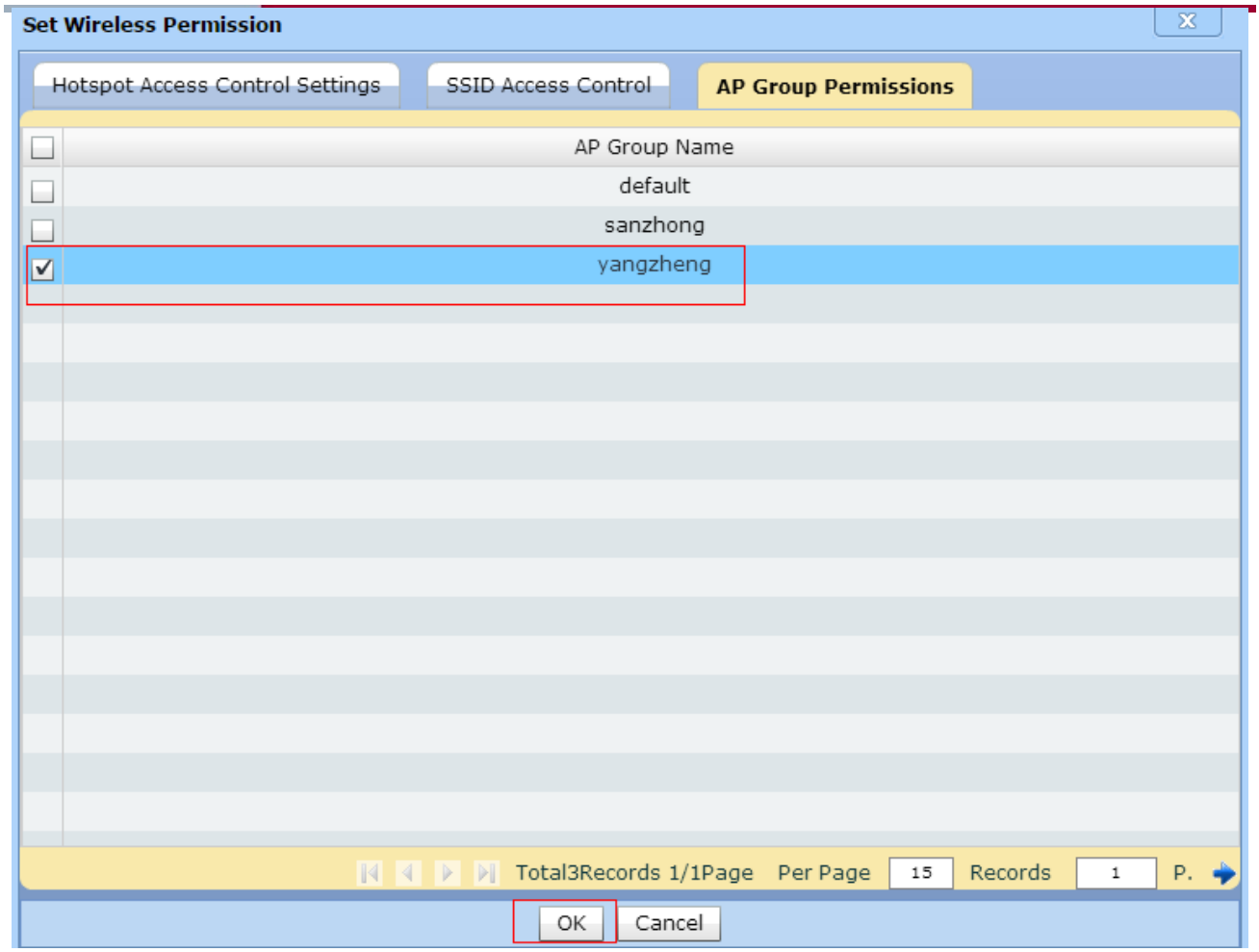


Figure 7.356. AP Group Permission Assignment

14. Repeat the preceding steps to assign the hotspot, SSID, and AP group permissions to role **sanzhong**.

7.12.3. School Administrator Operation

After logging in to the SNC, school administrators can manage the hotspots, APs, SSIDs, and AP groups of their respective schools.

1. Log in to the SNC with the administrator account of role **yangzheng**, as shown in the following figure.

Figure 7.357. School Administrator Login

2. Choose **WLAN** > **Hotspot**. The page only shows the hotspot and SSIDs assigned to the school, as shown in the following figure.

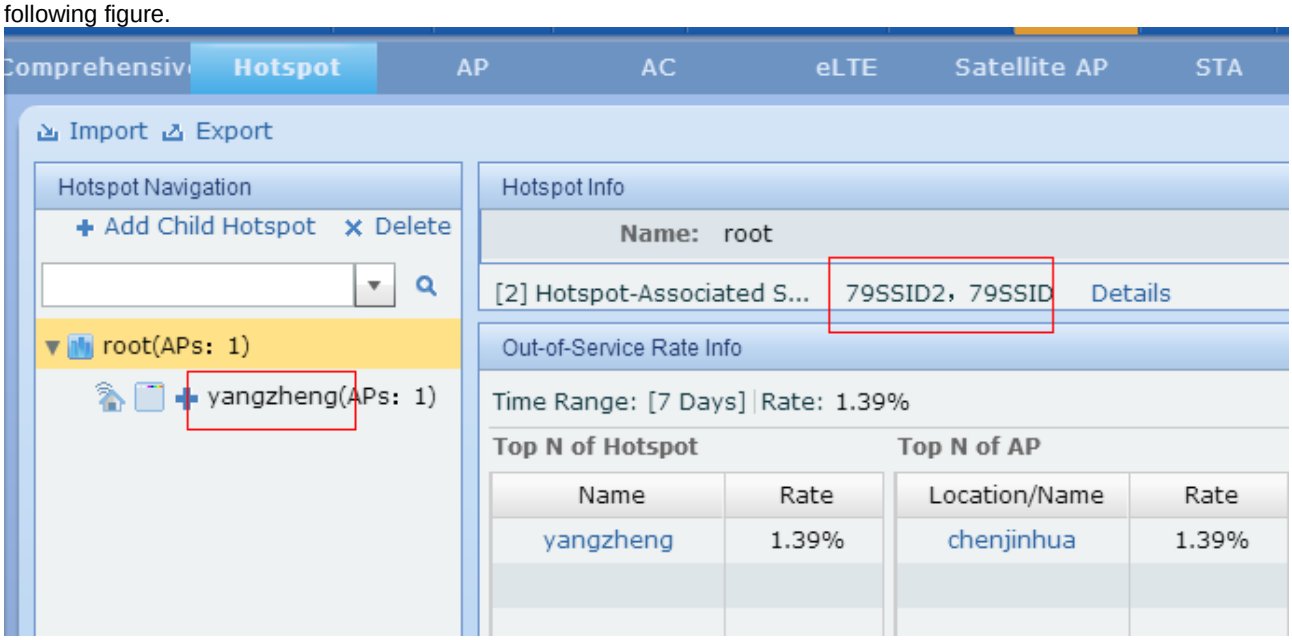


Figure 7.358. Hotspot and SSIDs Assigned to the School

3. Choose **WLAN** > **AP**. The page only shows the AP associated with the hotspot assigned to the school, as shown in the following figure.

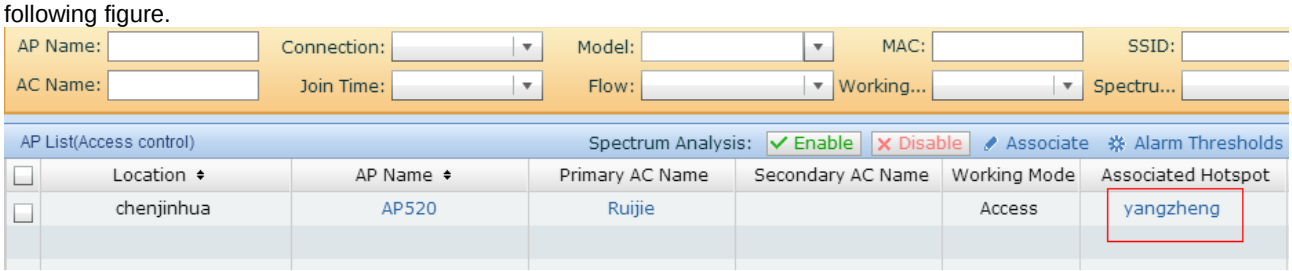


Figure 7.359. AP of the school

4. Choose **WLAN** > **Dashboard**. The **Global STA Statistics** page only shows the SSIDs that the super administrator assigns to the school, as shown in the following figure.

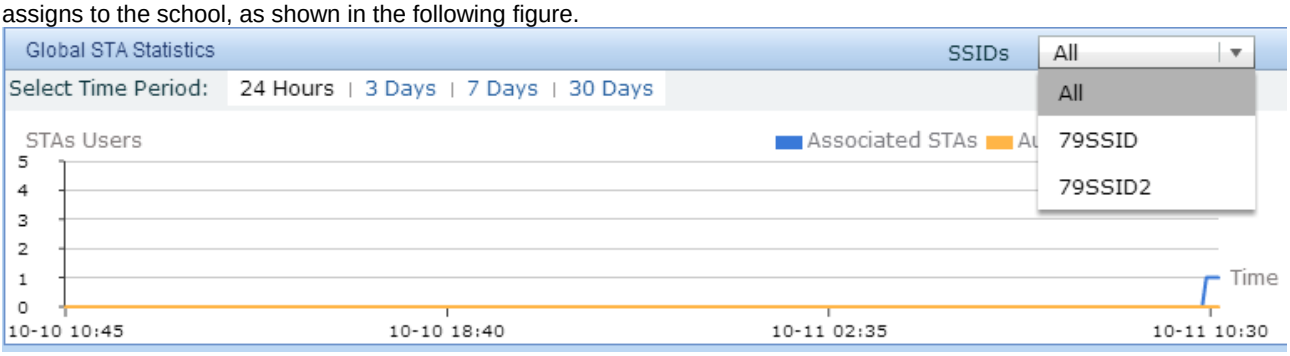


Figure 7.360. Global STA Statistics Page

5. Choose **WLAN** > **STA** > **STA Statistics**, as shown in the following figure.

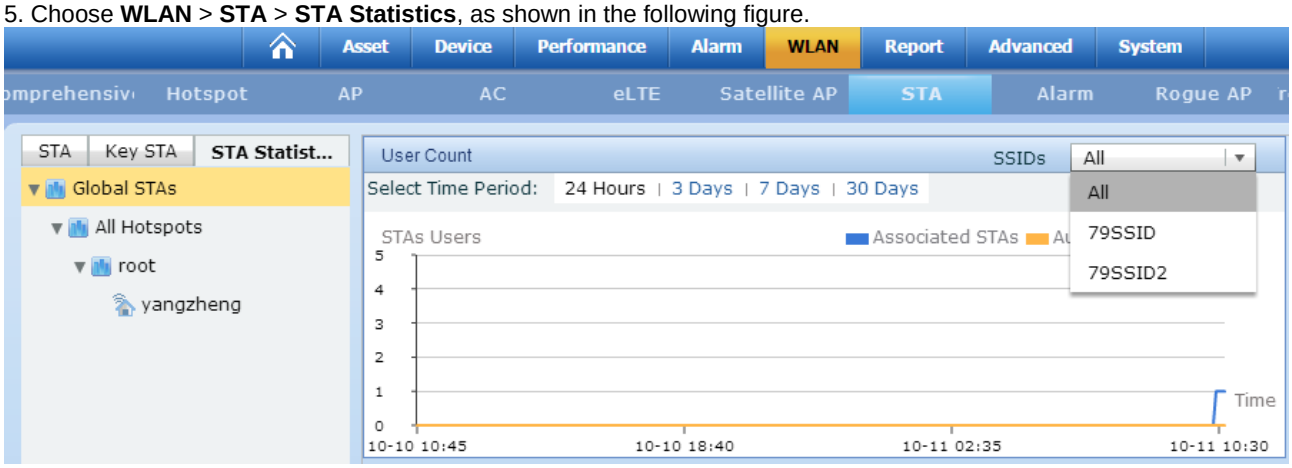


Figure 7.361. WLAN > STA > STA Statistics Page

6. Choose **WLAN** > **AC** and click a device name to display the **AC Details** page. Click **Details** to display the **Controller** page. Choose **WLAN** > **AP Groups** to display the **AP Groups** page, as shown in the following figure.

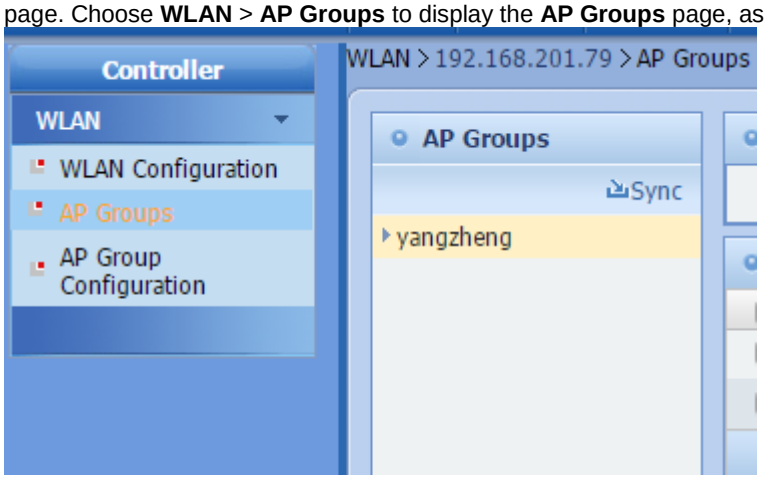


Figure 7.362. AP Group

7. Choose **WLAN** > **AC** and click a device name to display the **AC Details** page. Click **Details** to display the **Controller** page, as shown in the following figure.

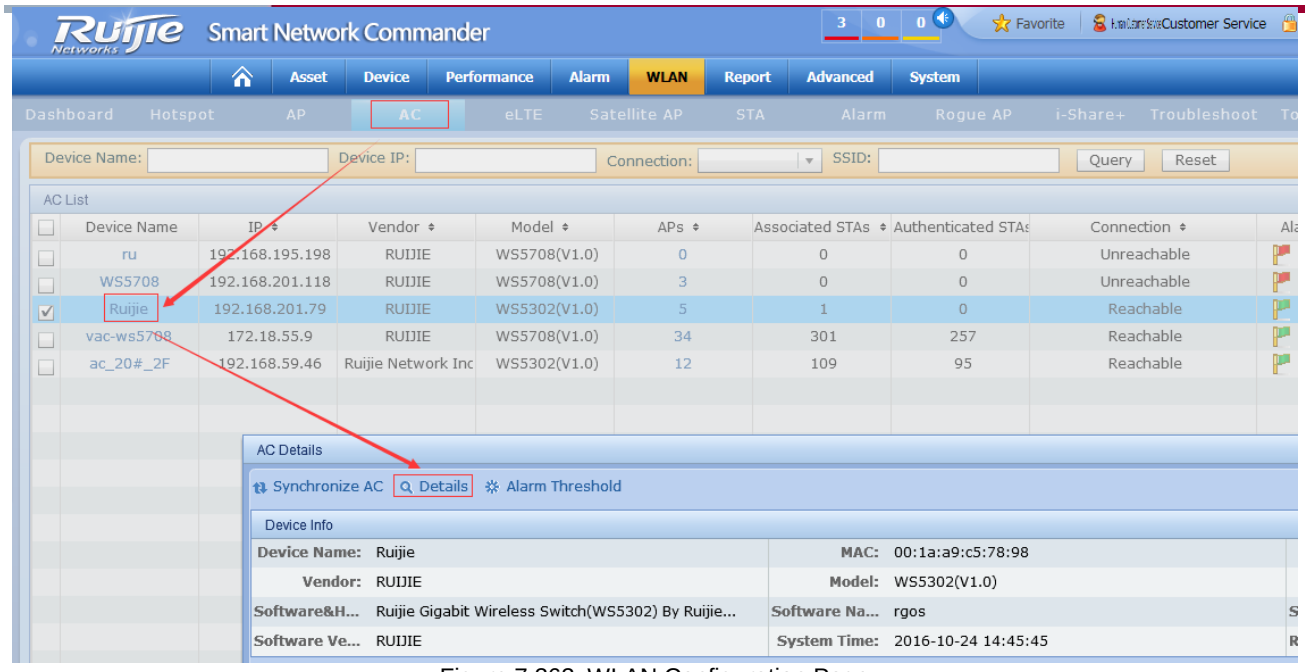


Figure 7.363. WLAN Configuration Page

8. Choose **WLAN** > **WLAN Configuration** under **Controller** on the left. The page shows the SSIDs that the super administrator assigns to the school. Click **Add** to add an SSID, as shown in the following figure.

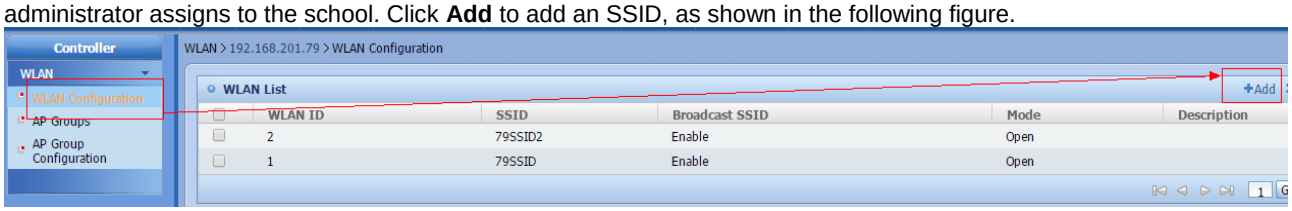


Figure 7.364. SSID List

9. Set the items on the **WLAN Configuration** page, including **WLAN ID**, **SSID**, **Broadcast SSID**, **Local Forwarding**, and **Mode**, as shown in the following figure.

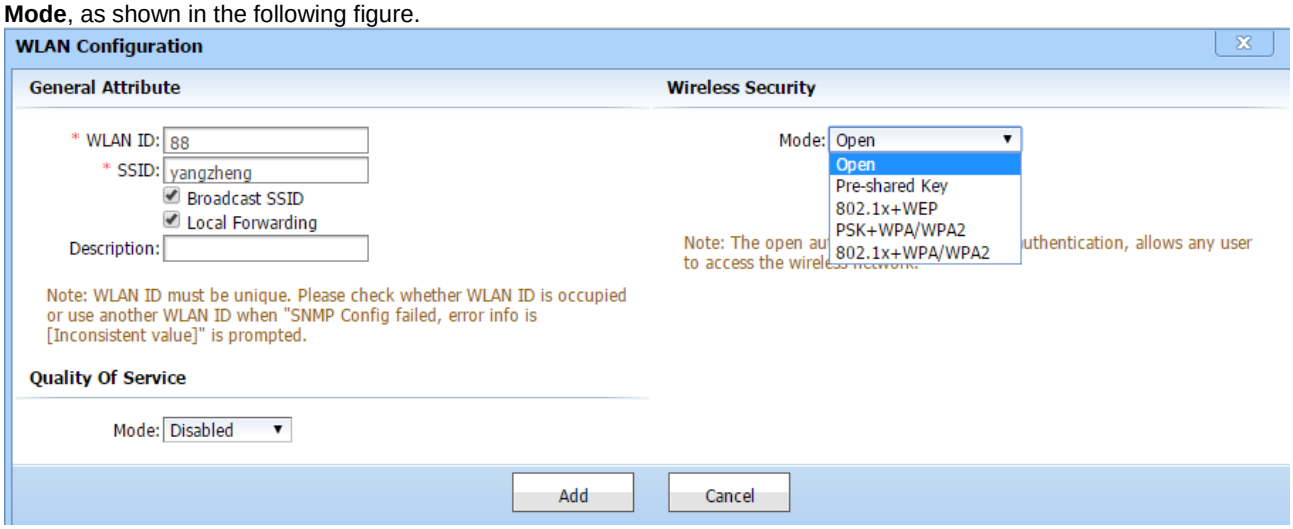


Figure 7.365. Adding WLAN

10. The **WLAN List** shows the new SSID, as shown in the following figure.

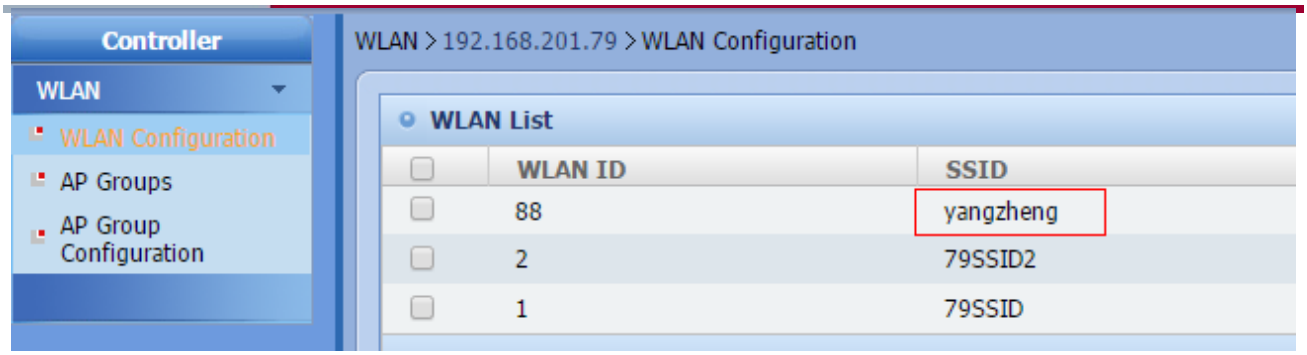


Figure 7.366. WLAN List

11. Choose **WLAN** > **AP Groups** under **Controller** on the left. The **AP Groups** page is displayed. Select an AP group to add members (WLAN-VLAN mappings), as shown in the following figure.

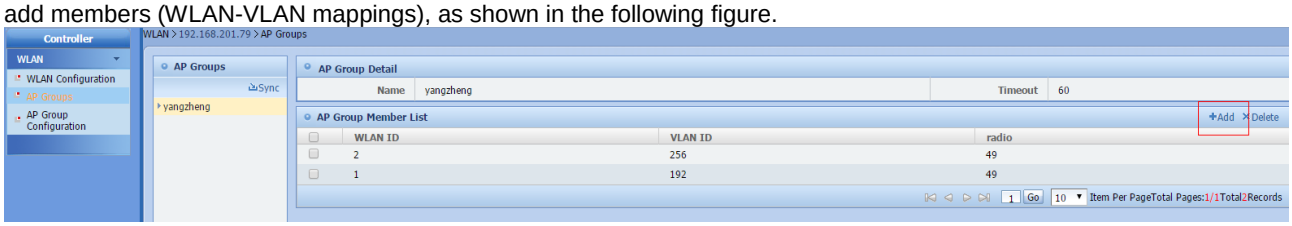


Figure 7.367. AP Group List

12. Click **Add** to add a member to the AP group and associate the WLAN and VLAN for the new SSID. In the **AP Group Member** dialog box, you can select a value ranging from 1 to 48 or **ALL** (indicating all radios) for **radio**, as shown in the following figure.

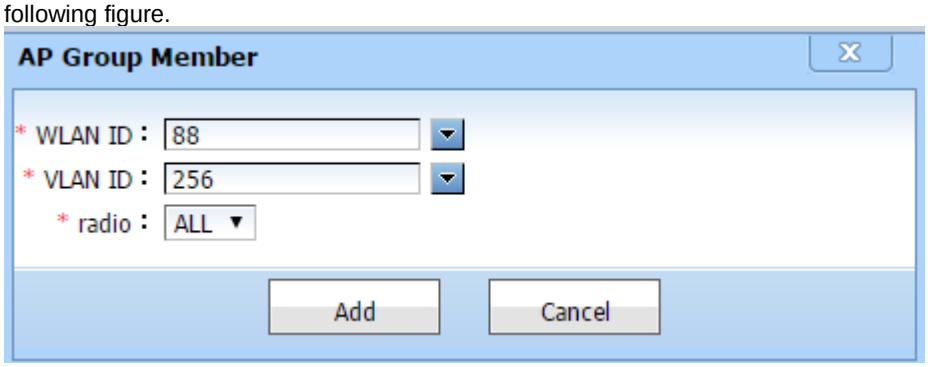


Figure 7.368. AP Group Member

13. Obtain VLAN information. Choose **Device** and click a device name to display the **Details** page. Choose **Device Information** > **VLAN Configuration** in the **Navigation Bar** and click **Synchronize,** as shown in the following figure.

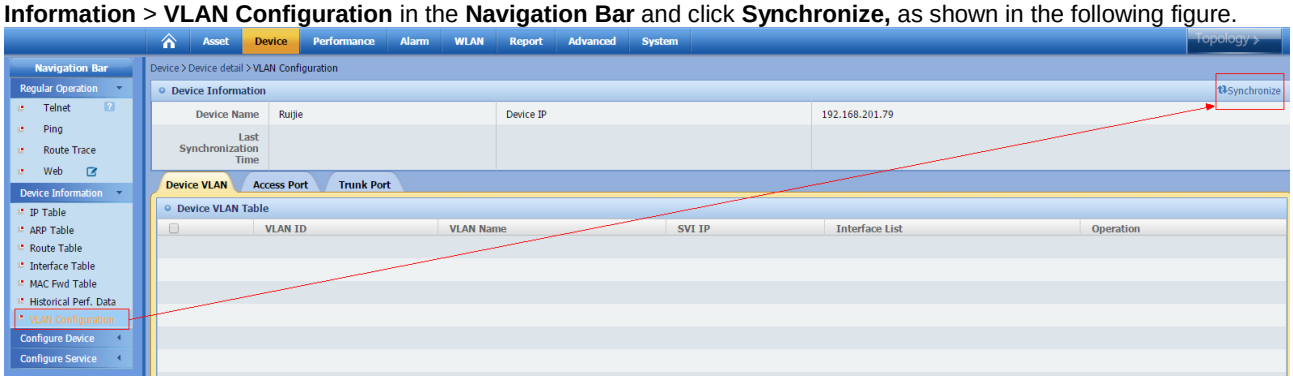


Figure 7.369. VLAN Information

14. Click **AP Group Configuration** on the left to adjust the AP group to which the school's AP belongs, as shown in the following figure.

Figure 7.370. AP Group Configuration

15. Select an AP and click **Update**. The **Modify AP Group** dialog box is displayed. You can select the AP group of the school (the AP group must be assigned to the school by the upper-level administrator), as shown in the following figure.

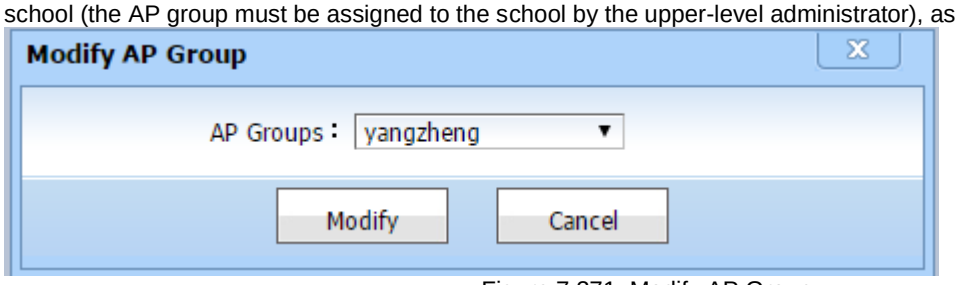


Figure 7.371. Modify AP Group

16. After the school administrator logs in to the SNC, the SNC only shows the hotspots, APs, SSIDs, and AP groups of the current school.

7.13. i-Share+ Mini AP

i-Share+ AP (AM5528) management covers Mini AP information, status information, and number of 2.4G and 5G clients so as to support the RG-AM5528 i-Share+ solution.

1. After you add an AC and synchronize the AC to the i-Share+ device, go to the **i-Share+** page to view the Mini AP names, Mini AP status, and number of clients, as shown in the following figure.

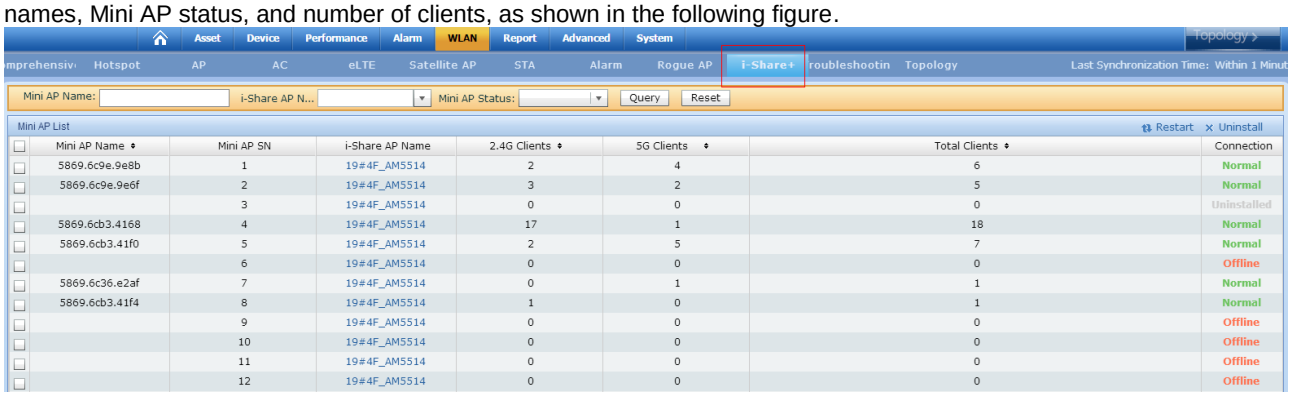


Figure 7.372. i-Share+ Mini AP Page

2. Move the cursor to **Mini AP Name** and click **Modify**, as shown in the following figure.

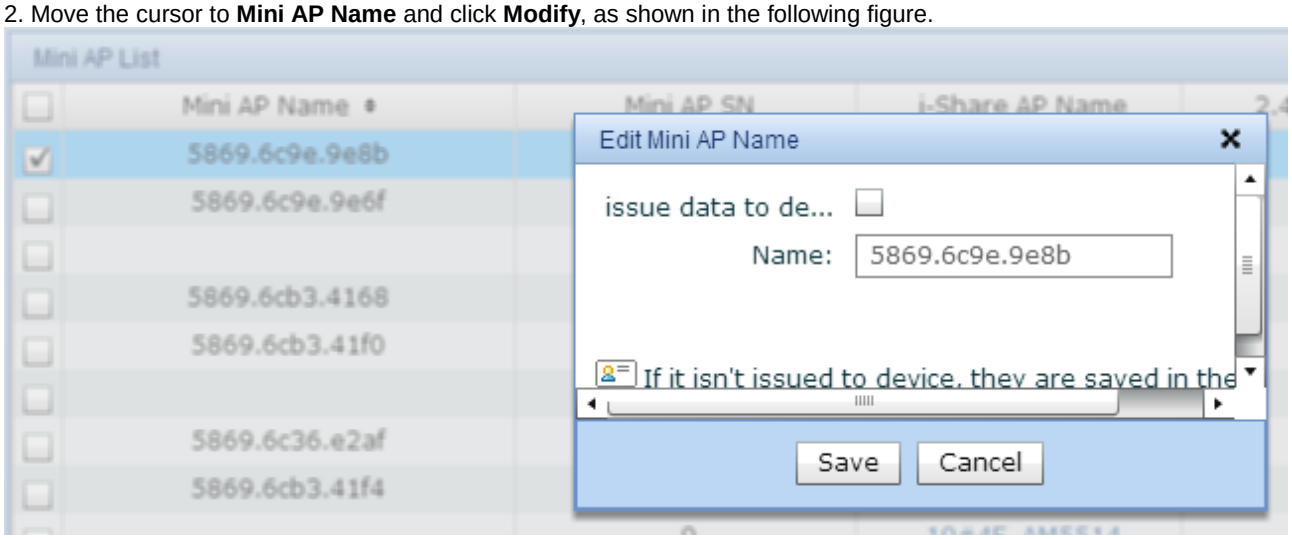


Figure 7.373. Edit Mini AP Name

3. Move the cursor to **i-Share AP Name** and click **Mini AP Details**, as shown in the following figure.

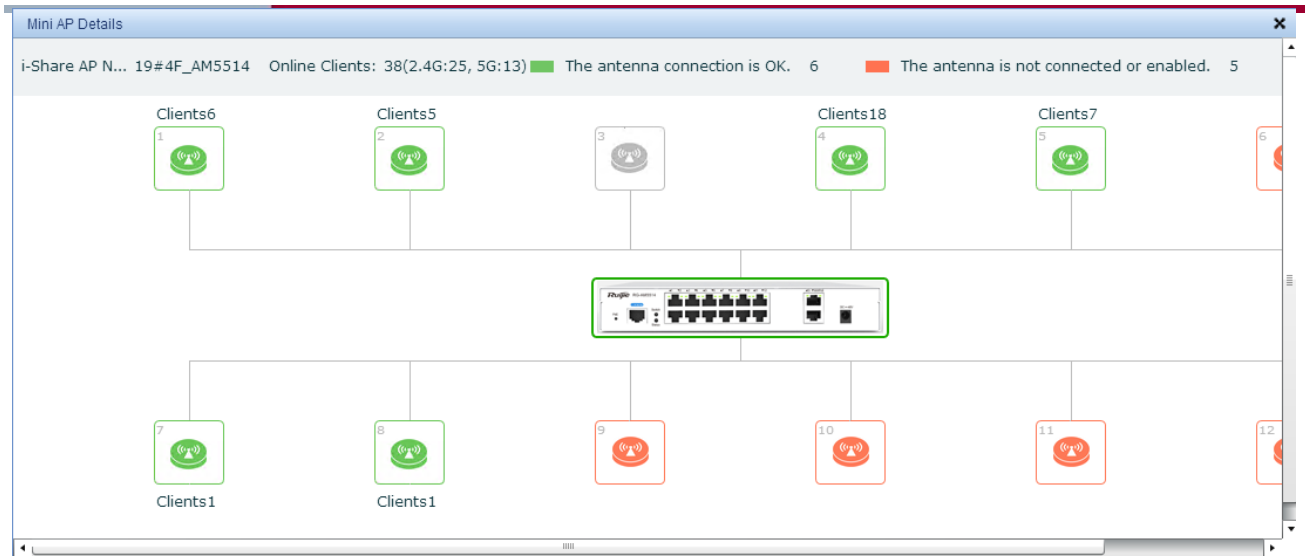
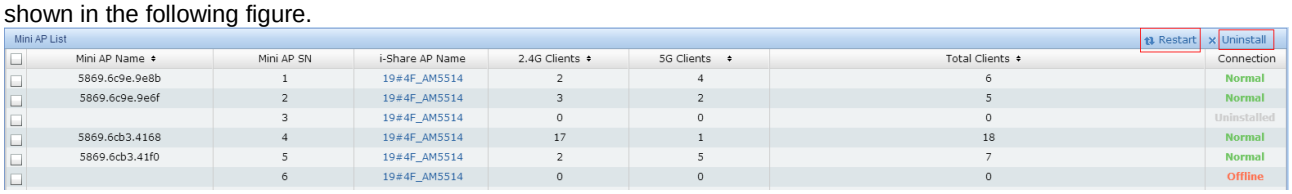


Figure 7.374. Mini AP Details

4. Select a Mini AP and click **Restart** or **Uninstall**. You can only restart online Mini APs and uninstall offline Mini APs, as shown in the following figure.



Mini AP Name	Mini AP SN	i-Share AP Name	2.4G Clients	5G Clients	Total Clients	Connection
5869.6c9e.9e8b	1	19#4F_AM5514	2	4	6	Normal
5869.6c9e.9e6f	2	19#4F_AM5514	3	2	5	Normal
	3	19#4F_AM5514	0	0	0	Uninstalled
5869.6cb3.4168	4	19#4F_AM5514	17	1	18	Normal
5869.6cb3.41f0	5	19#4F_AM5514	2	5	7	Normal
	6	19#4F_AM5514	0	0	0	Offline

Figure 7.375. Restarting or Uninstalling Mini APs

7.14. eLTE

7.14.1. Features

The SNC can be used to manage eLTE-related devices, including EPCs, eNodeBs, and UEs so as to support the eLTE wireless network coverage solution.

TThe **eLTE** menu is hidden when there is no eNodeB. Choose **WLAN** > **AC** to add an EPC (which is associated with eNodeBs).

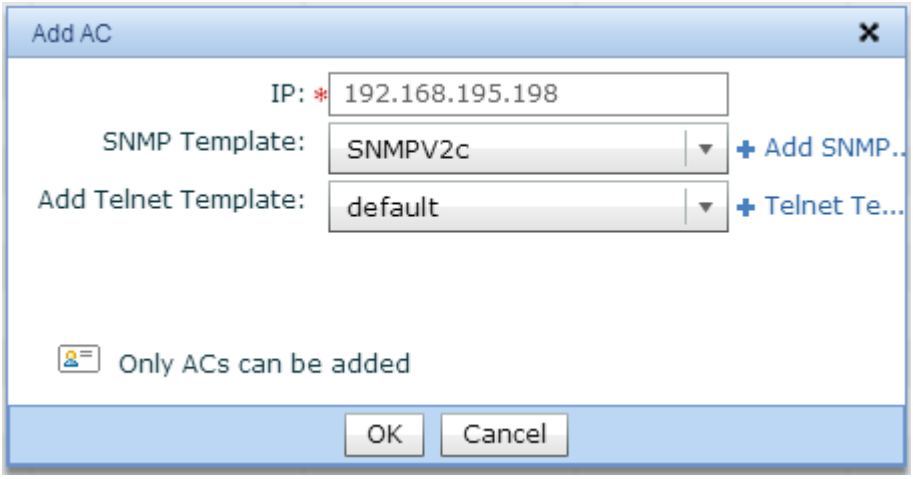


Figure 7.376. Adding an EPC

After the EPC is successfully added, the **eLTE** menu is displayed.

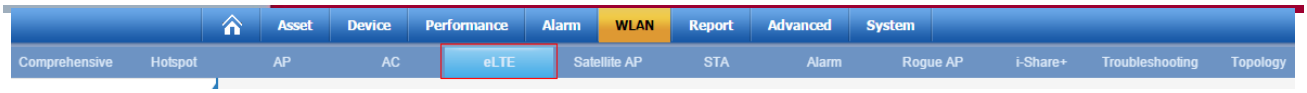


Figure 7.377. eLTE Menu

7.14.2. eLTE Monitoring

Choose **WLAN** > **eLTE** and click **eLTE-Monitoring** on the left. The page shows the statistical charts of the EPC, eNodeB, and UE status.

The statistics indicate the number and percentage of online and offline devices.

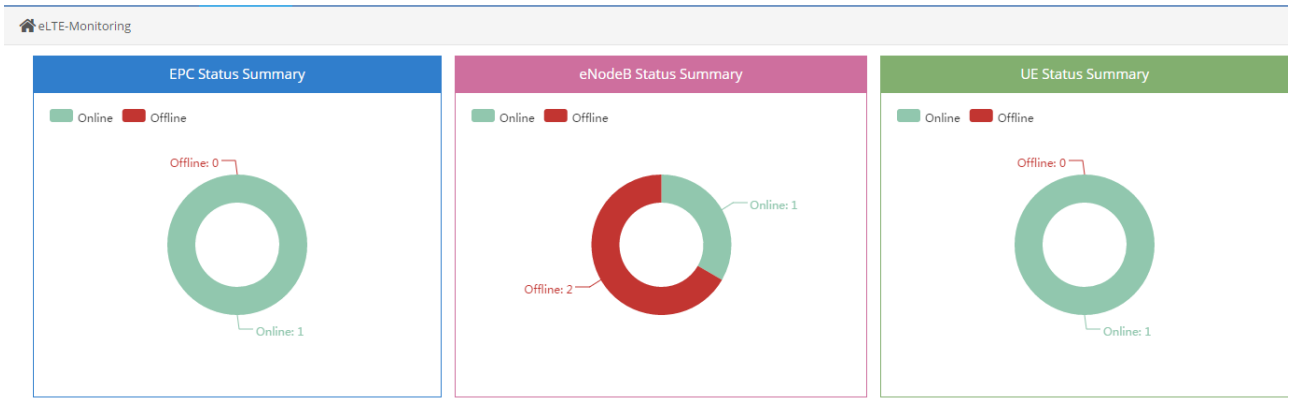


Figure 7.378. Status Statistics

7.14.3. EPC Management

Choose **WLAN** > **eLTE** and click **EPC Management** on the left. The **EPC List** is displayed.

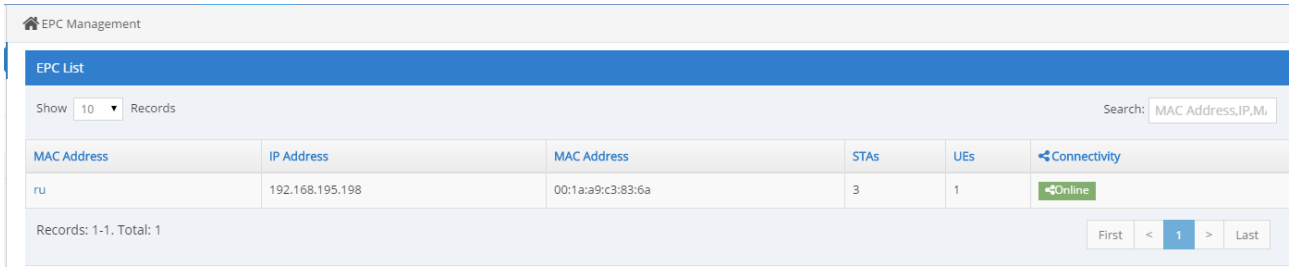


Figure 7.379. EPC List

Click an EPC name to display the **EPC Details** page.

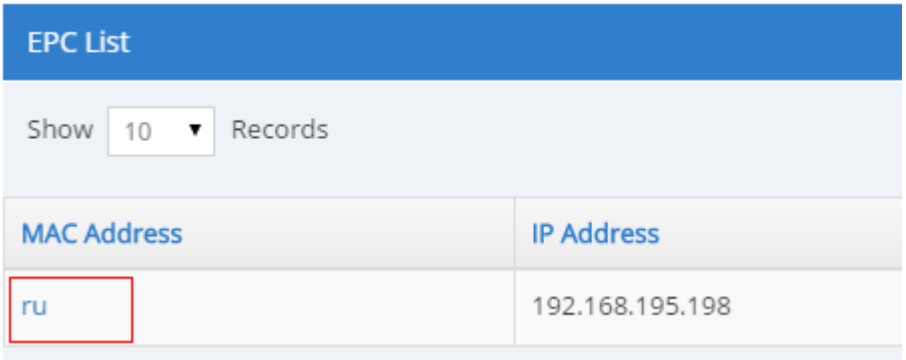


Figure 7.380. Going to the EPC Details Page

Modify the EPC information and then click **Save** on the **EPC Details** Page. The modifications are pushed to the EPC.

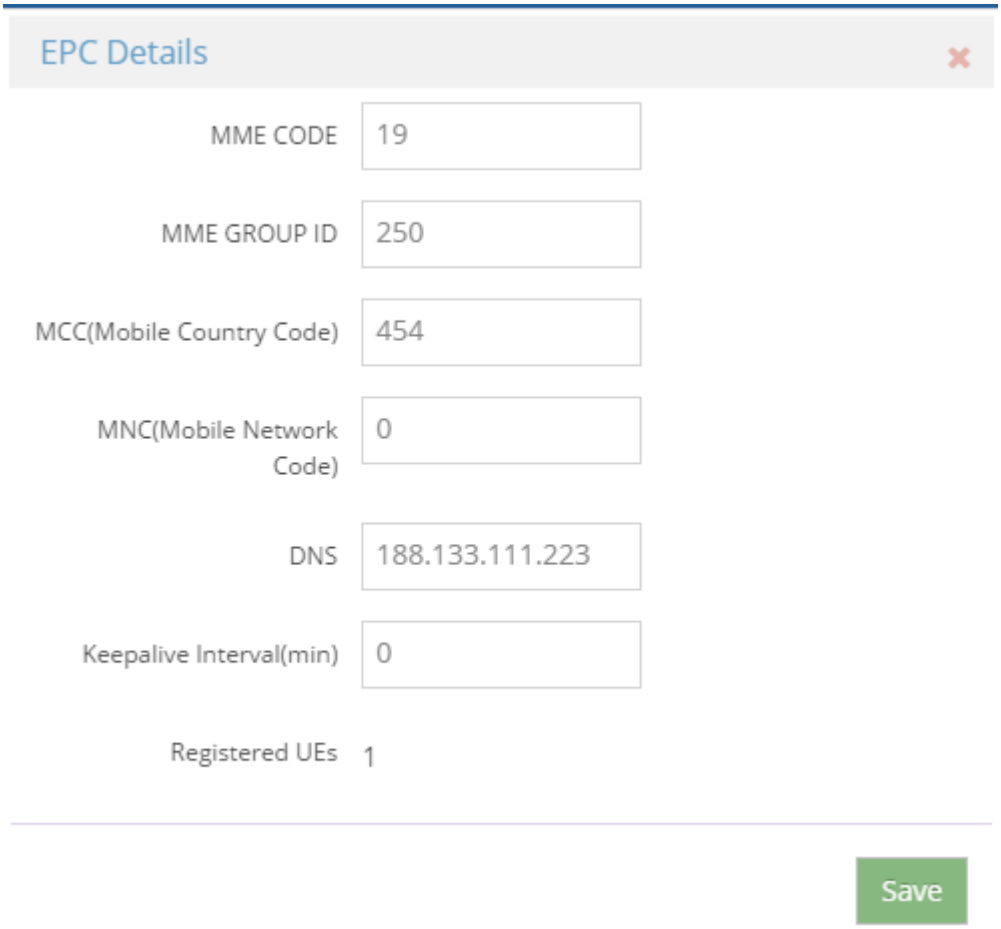


Figure 7.381. EPC Details Page

7.14.4. eNodeB Management

Choose **WLAN** > **eLTE** > **eNodeB** > **eNodeB List** on the left. The **eNodeB List** is displayed.

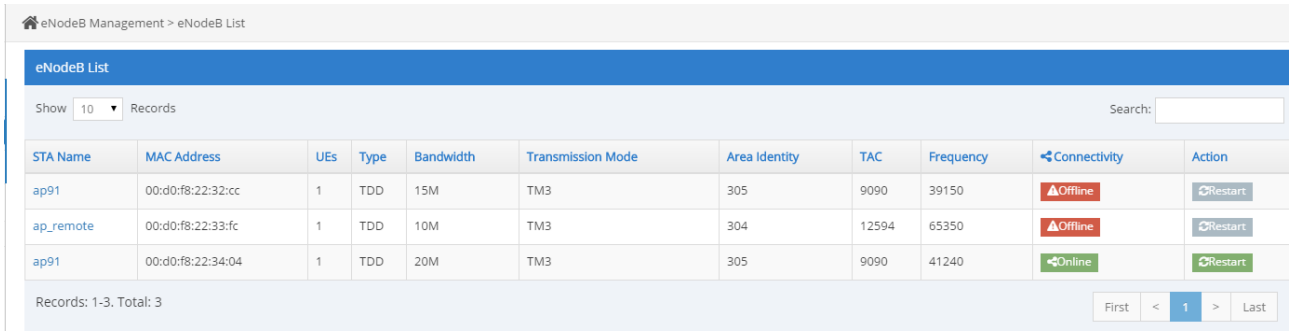


Figure 7.382. eNodeB List

Click an eNodeB name to display the **eNodeB Details** page.

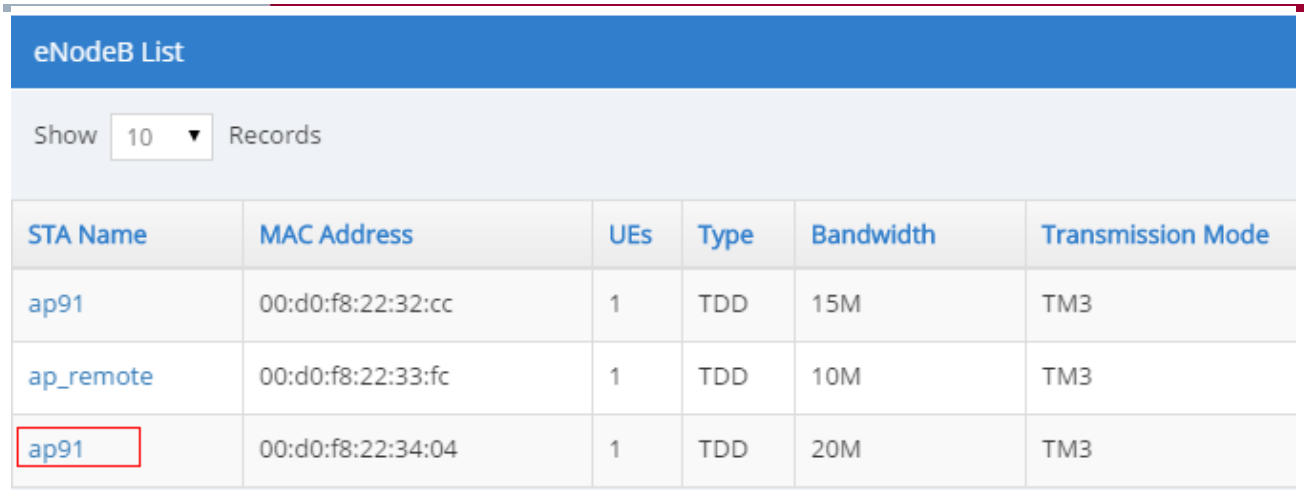


Figure 7.383. Going to the eNodeB Details Page

You can modify the following eNodeB information on the **eNodeB Details** page: **Basic Info**, **Power Settings**, **Measurement Settings**, and **RRM Settings**. Click **Save**, and the modifications are pushed to the eNodeB.

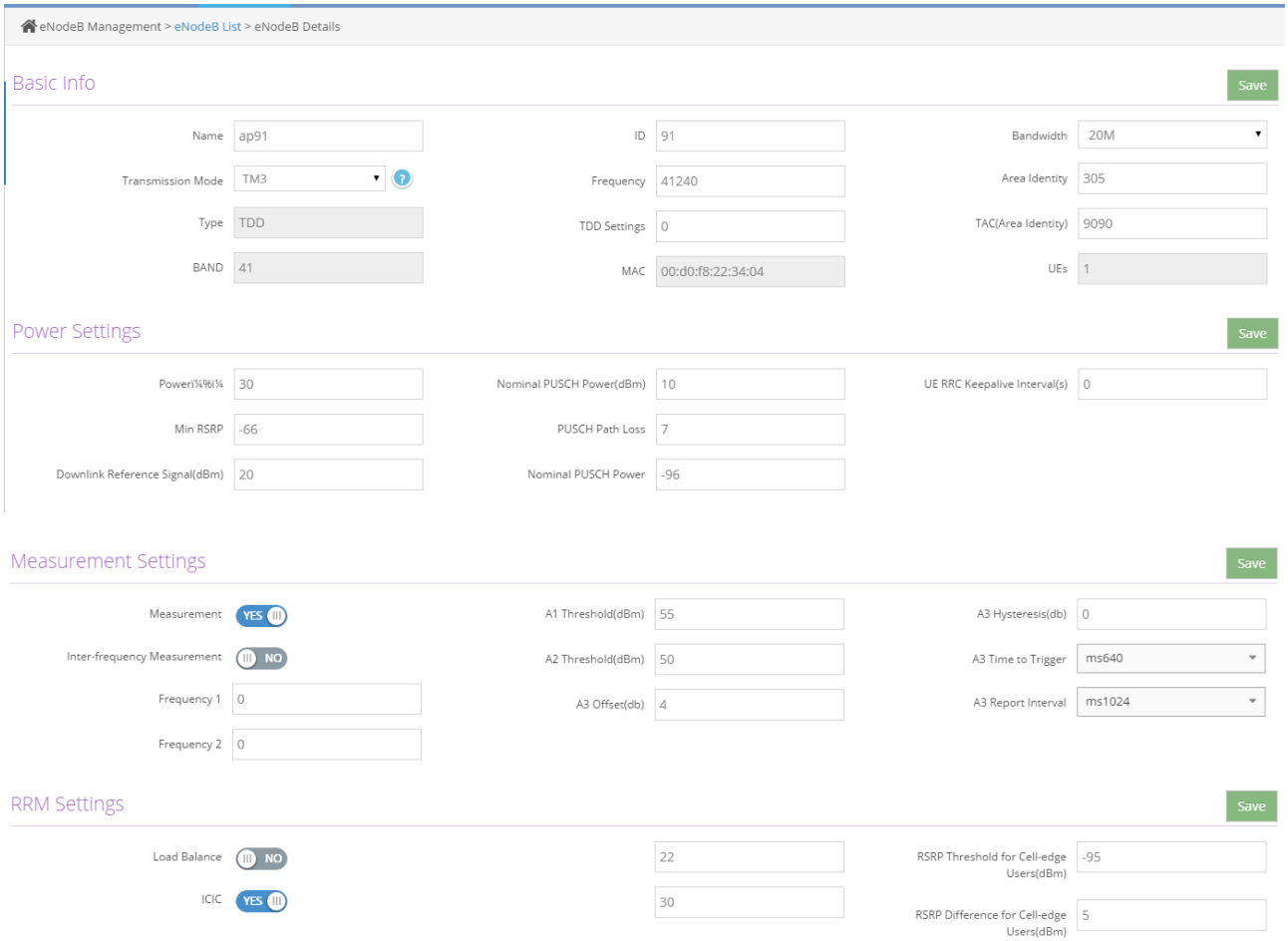


Figure 7.384. eNodeB Details Page

Click **eNodeB Alarm List** on the left. The **eNodeB Alarm List** is displayed.

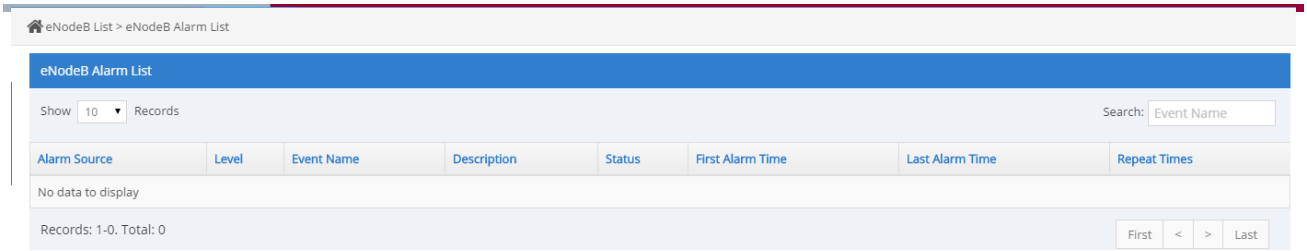


Figure 7.385. eNodeB Alarm List

7.14.5. UE Management

Choose **WLAN** > **eLTE** > **UE** > **UE List**. The **UE List** is displayed.

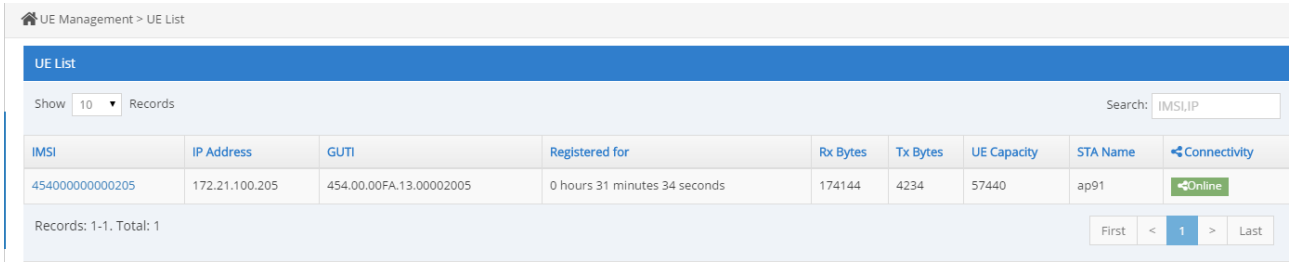


Figure 7.386. UE List

Click an IMSI to view the corresponding UE details.

Figure 7.387. Going to the UE Details Page

The following figure shows the **UE Details** page.

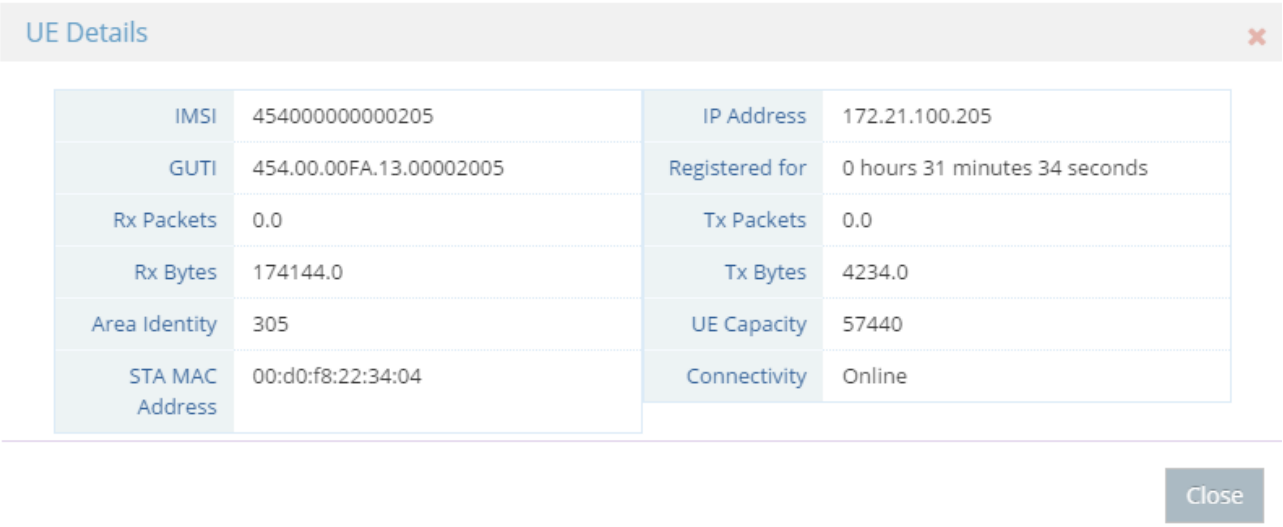


Figure 7.388. UE Details Page

Click **UE Mapping List** on the left. The **UE Mapping List** is displayed, showing the **Add Mapping**, **Edit**, **Delete** and **Batch Delete Mapping** buttons and the search box.

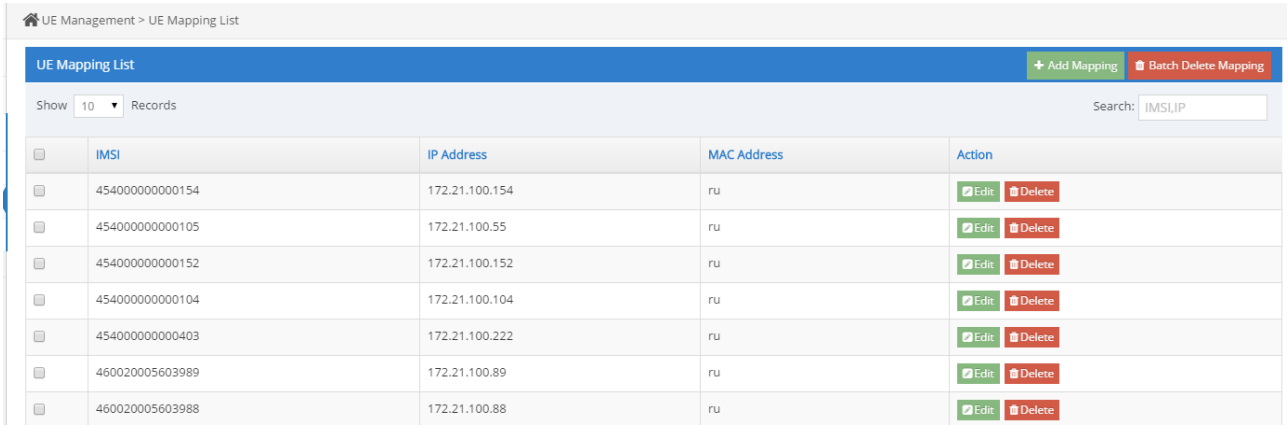


Figure 7.389. UE Mapping List

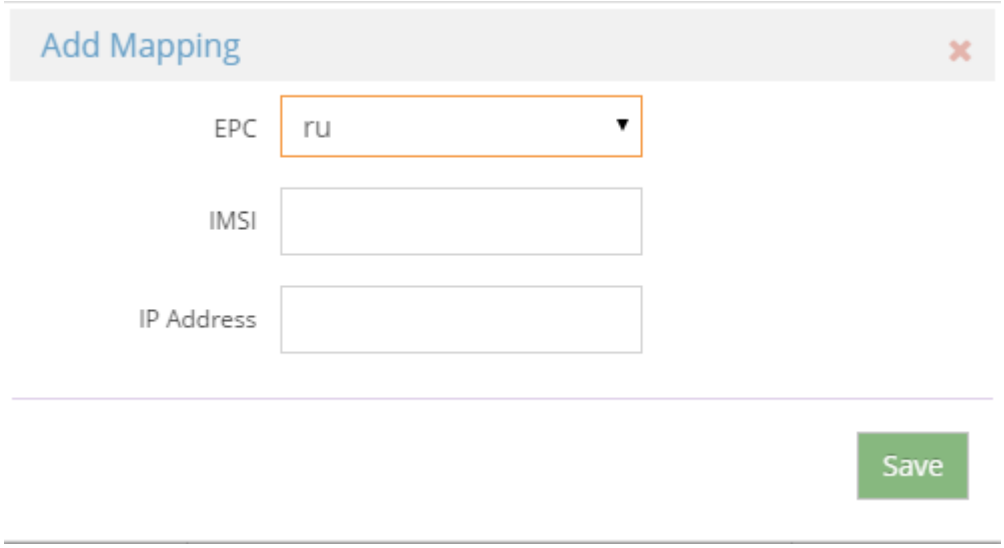


Figure 7.390. Add Mapping

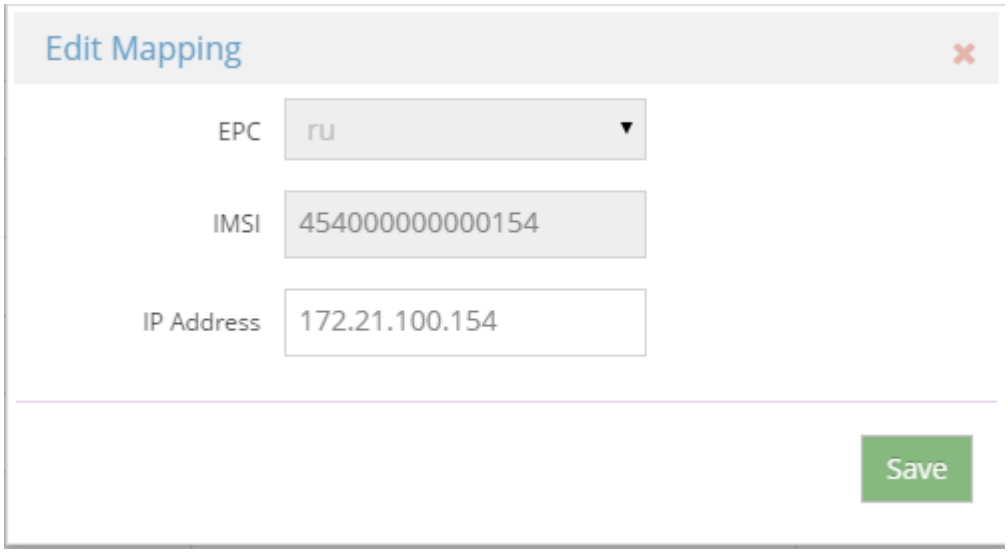


Figure 7.391. Edit Mapping

Click **UE Alarm List** on the left. The **UE Alarm List** is displayed.

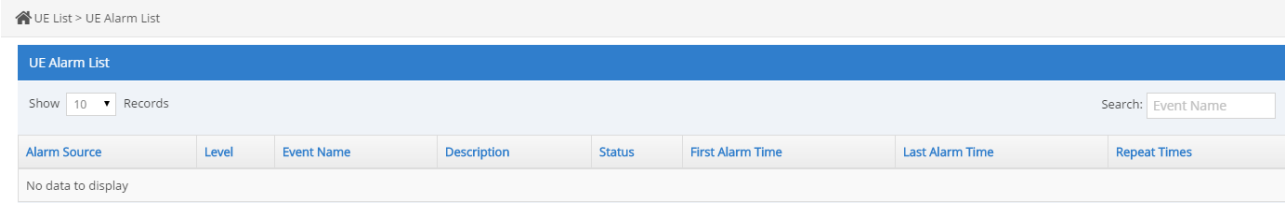


Figure 7.392. UE Alarm List

7.15. Satellite AP

7.15.1. Features

The SNC can be used to manage satellite package devices, including the AP520-I (G2) and MAP552 (SR), so as to support the use of satellite APs.

The **Satellite AP** menu is hidden when there is no satellite AP. The **Satellite AP** menu is displayed when a satellite AP is added.

Figure 7.393. Satellite AP Menu

7.15.2. Satellite AP List

Choose **WLAN** > **Satellite AP**. The **Satellite AP List** is displayed, showing the master AP and satellite APs as well as their relationships, number of associated STAs, number of authenticated STAs, connection status, spectrum analysis, and heat map.

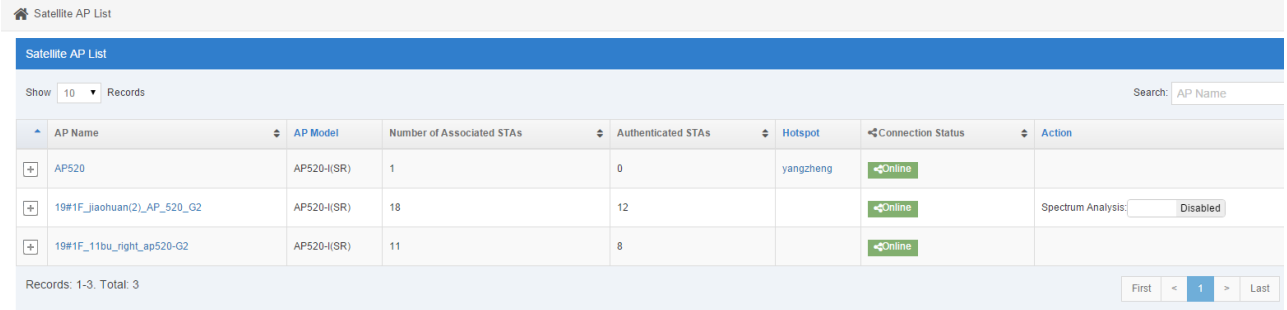


Figure 7.394. Satellite AP List

Expand a satellite AP package to show information about the master AP and satellite APs.

Figure 7.395. Information about the master AP and satellite APs

7.15.3. Satellite AP Details

Basic information about the master AP and satellite APs, and AP status

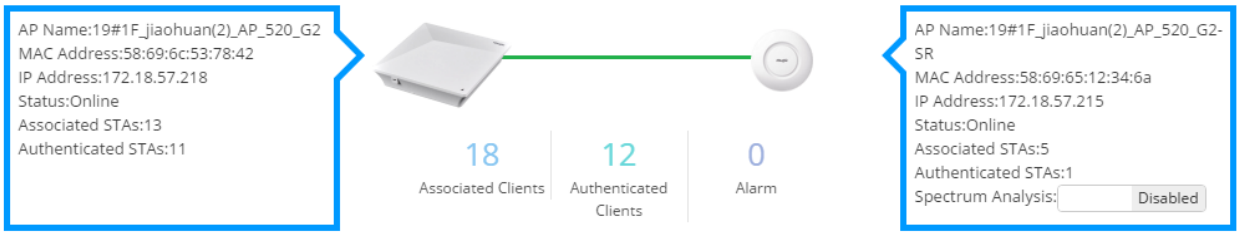


Figure 7.396. Information about the master AP and satellite APs

The following figure shows the **Radio List** page.

Radio List

Radio Index	AP	Protocol	Current Channel	Protocol Mode	Interface Description	Interface Bandwidth(Mbps)	Interface MAC Address	Current Interface Status	Transmission Rate(Mbps)	Current Power(%)	Number of Associated STAs	Authenticated STAs
1	19#1F_jiaohuan(2)_AP_520_G2	802.11b/g/n	11	802.11b(2.4G)	Dot11radio 1/0	144	00:69:6c:53:78:45	Up	1,2,5.5,6,9,11,12,18,24,36,48,54,MCS 15	10	13	11
2	19#1F_jiaohuan(2)_AP_520_G2	802.11a/n	157	802.11a(5G)	Dot11radio 2/0	173	00:69:6c:53:78:46	Up	9,12,18,24,36,48,54,MCS 15	100	0	0
3	19#1F_jiaohuan(2)_AP_520_G2-SR	802.11b/g/n	6	802.11b(2.4G)	Dot11radio 1/0	144	00:69:65:12:34:6c	Up	1,2,5.5,6,9,11,12,18,24,36,48,54,MCS 15	50	1	0
4	19#1F_jiaohuan(2)_AP_520_G2-SR	802.11a/n	161	802.11a(5G)	Dot11radio 2/0	400	00:69:65:12:34:6d	Up	9,12,18,24,36,48,54,MCS 15	80	4	1

Figure 7.397. Radio List

The following figure shows the **AP-Associated SSID List**.

AP-Associated SSID List

SSID Name	AP	Radio Index	WLAN	Available	Hide	802.11 Authentication	Authentication Mode	Security Type	Encryption Type	Number of Associated STAs	Authenticated STAs
@test-2.4G	19#1F_jiaohuan(2)_AP_520_G2	1	23	Available	Not Hidden	Open System	No Authentication	None	No Encryption	1	0
ruijie-iphone-5G	19#1F_jiaohuan(2)_AP_520_G2	2	7	Available	Not Hidden	Open System	Pre-shared Key	WAP2	AES CCMP	0	0
ruijie-web	19#1F_jiaohuan(2)_AP_520_G2	1,2	6	Available	Not Hidden	Open System	Web Authentication	None	No Encryption	8	7
ruijie-802.1x	19#1F_jiaohuan(2)_AP_520_G2	1,2	5	Available	Not Hidden	Open System	RADIUS Server Authentication	WAP2	AES CCMP	4	4
ruijie-guest	19#1F_jiaohuan(2)_AP_520_G2	1,2	4	Available	Not Hidden	Open System	Web Authentication	None	No Encryption	0	0

Figure 7.398. AP-Associated SSID List

The following figure shows the **Device Performance** page.

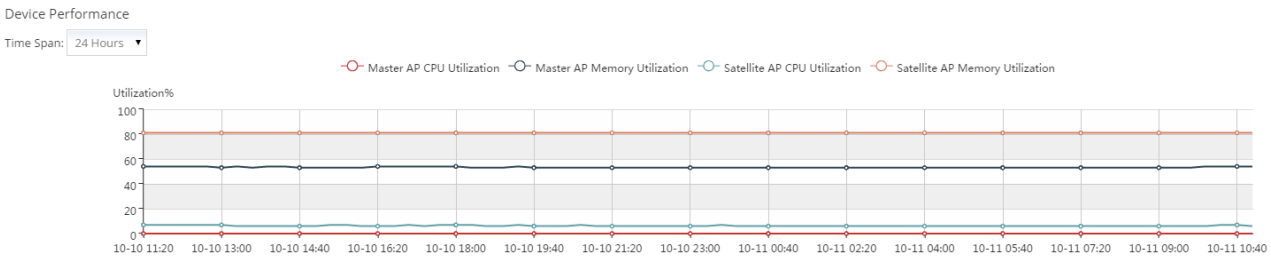


Figure 7.399. Device Performance

The following figure shows the **Number of Associated STAs** page.

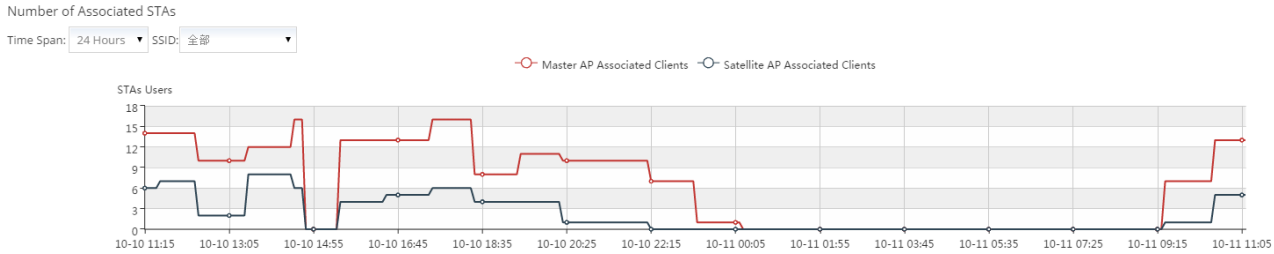


Figure 7.400. Number of Associated STAs

The following figure shows the **Authenticated Clients** page.

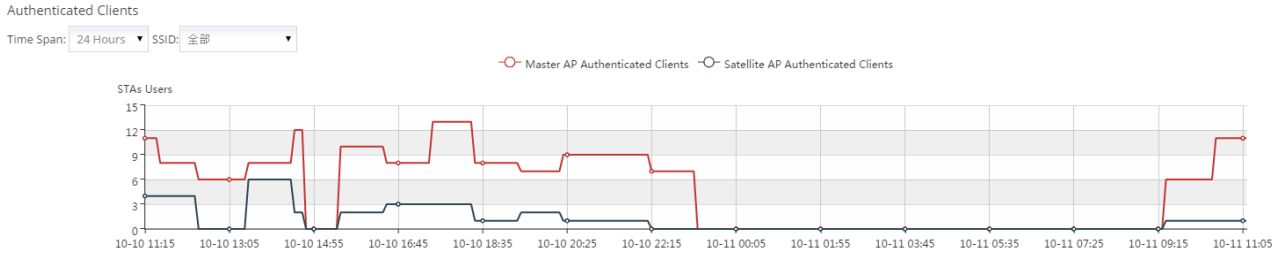


Figure 7.401. Authenticated Clients

The following figure shows the **Average AP Rates** page.

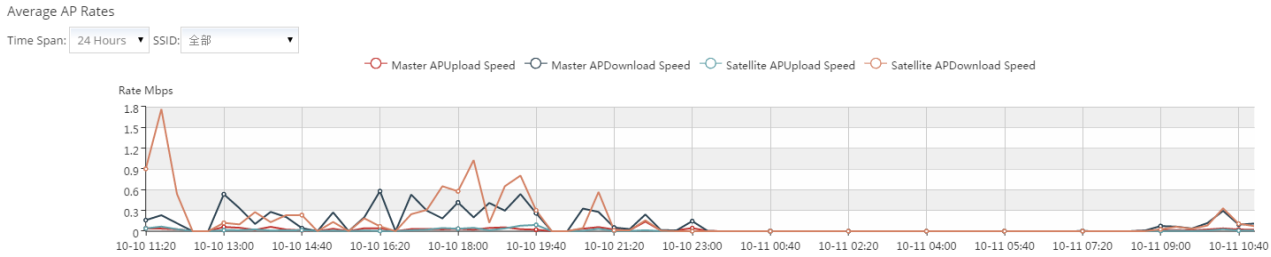


Figure 7.402 Average AP Rates

The following figure shows the **Alarm List** page.

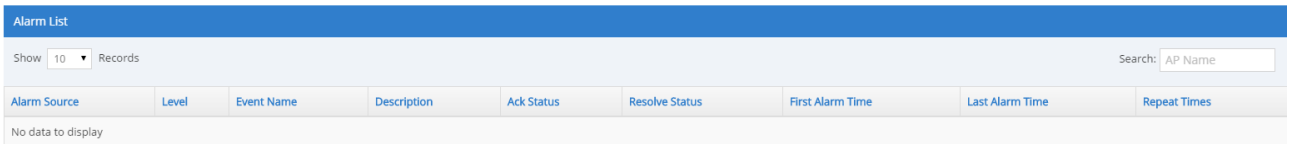


Figure 7.403. Alarm List

7.15.4. Satellite AP Spectrum Analysis

You can enable or disable satellite AP spectrum analysis on the **Satellite AP List** or **Satellite AP Details** page.

After satellite AP spectrum analysis is enabled, you can view the analysis results (which shows the rogue APs detected by satellite APs).

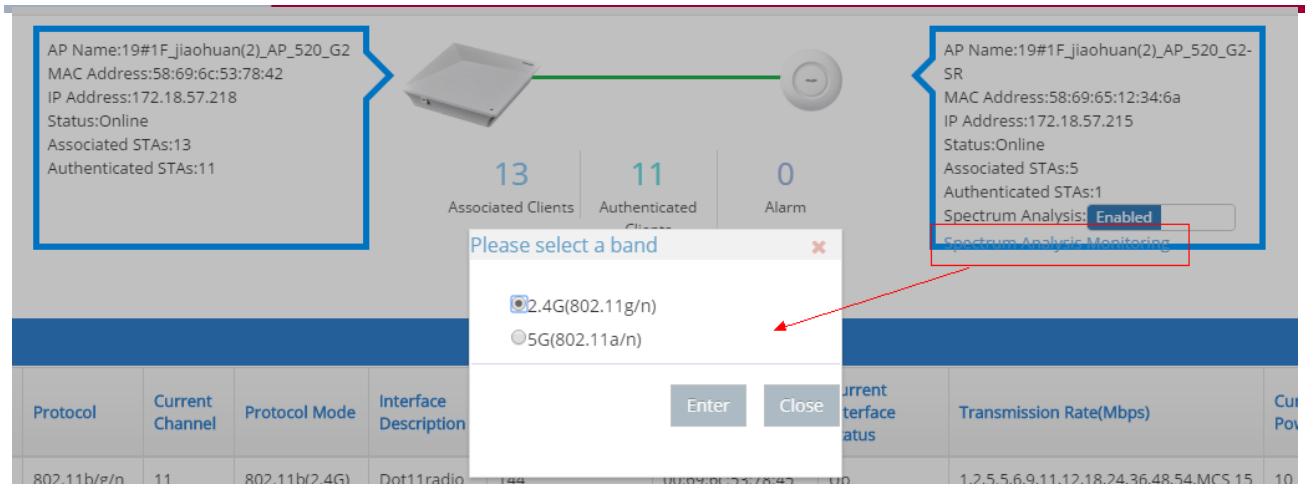


Figure 7.404. Satellite AP Spectrum Analysis

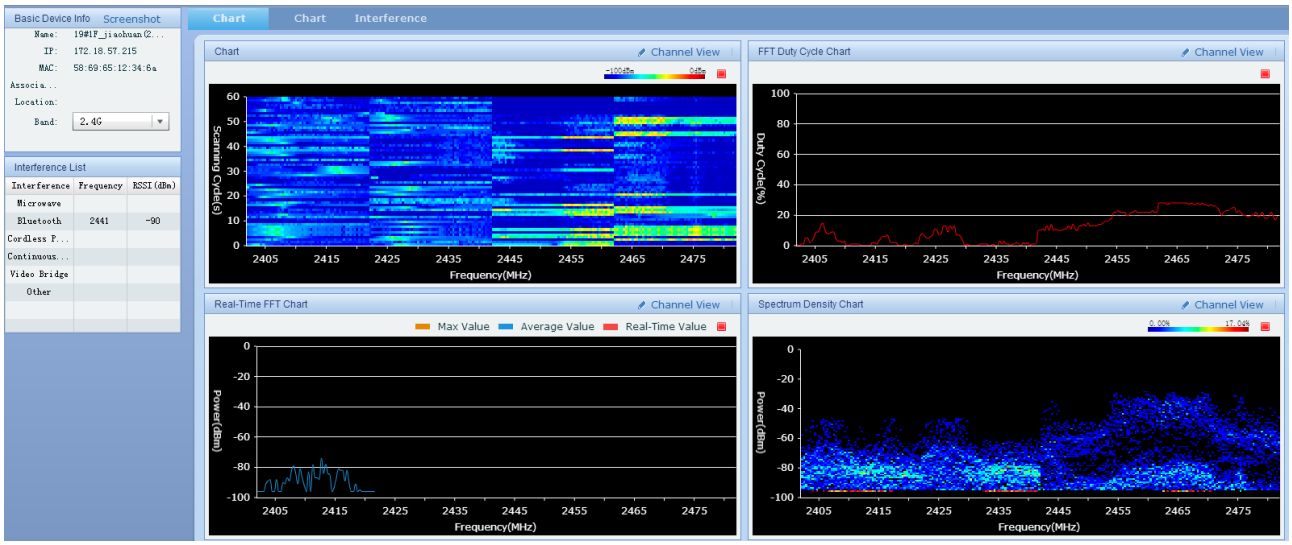


Figure 7.405. Viewing Spectrum Analysis Results

7.15.5. Satellite AP Heat Map

After you add the master AP and satellite APs to a hotspot, you can go to the **Satellite AP List** or **Satellite AP Details** page and click the hotspot name to view the heat map, which shows the signal coverage.

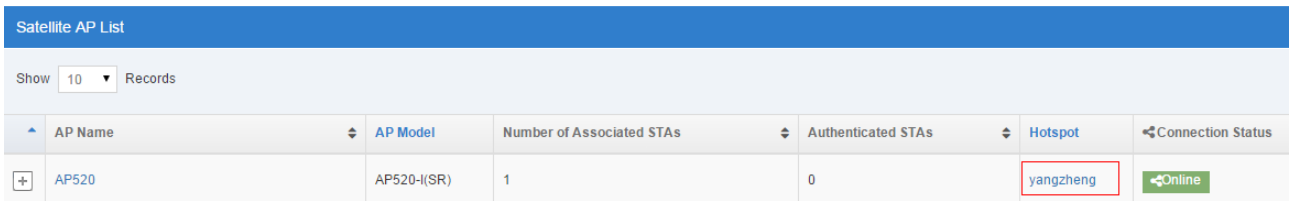


Figure 7.406. Displaying the Heat Map

View the 2.4G and 5G signal coverage.

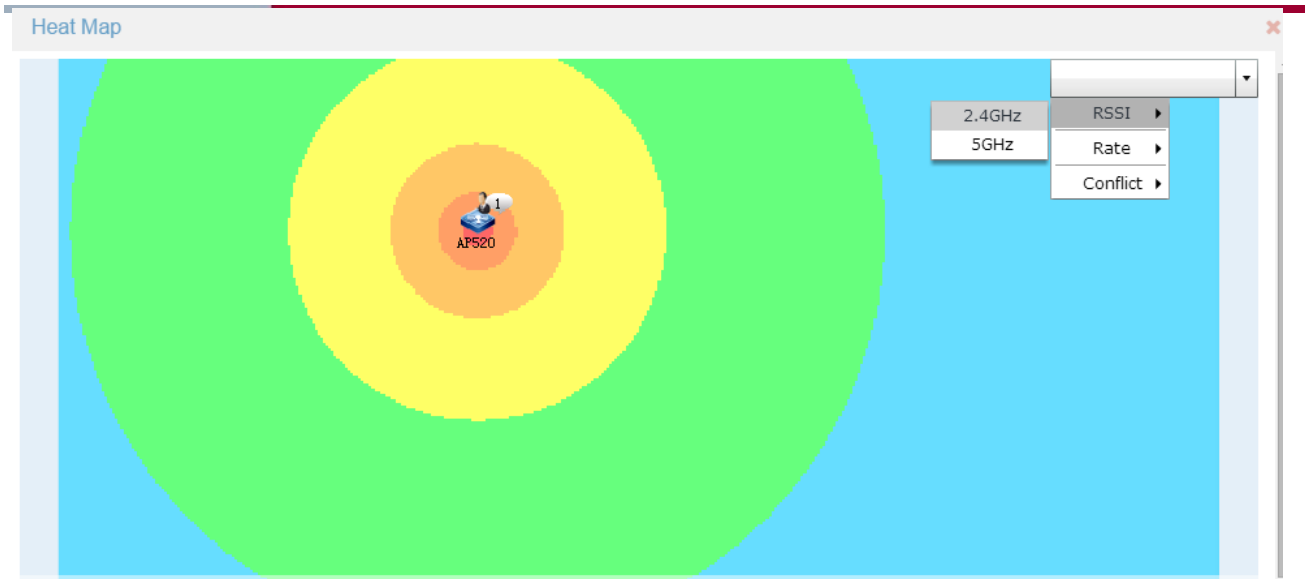


Figure 7.407. Viewing the Heat Map

Chapter 8 VLAN Management

VLAN management provides a graphic way to manage the VLAN information for the device. In SNC, you can configure and manage the VLANs for the device through the web page which will reduce the workload of maintenance for the administrator. Meanwhile, A specific VLAN configuration for device will hide the command differences between devices.

Function List

- VLAN basics
- Device VLAN management
- VLAN interface management
- VLAN FAQ

Note

Before you start your VLAN management work for the device, make sure that your device is connected to the network and the TELNET template is configured correctly.
Please be cautious when you configure the VLAN for the device. The network or some devices is inaccessible if you configure it improperly. In this case, you must log in the device using serial port to reconfigure it.

8.1. VLAN Basics

What is VLAN?

VLAN stands for Virtual Local Area Network. It is an logical network defined on a physical network and corresponds to the Layer 2 network in the ISO model. However, VLAN is not constrained by the physical location of the network interface. Except for the physical location, a VLAN is similar to an ordinary LAN and has the same attribute as a physical LAN. Unicast, broadcast, and multicast frames on Layer 2 are forwarded and spread within the same VLAN and do not enter other VLANs.

What is VLAN 1 different from other VLAN

A Ruijie device supports multiple VLANs and each of them is assigned a number and name. Being the default VLAN of a device, VLAN 1 can be modified but is undeletable.

Interface in a VLAN

From a VLAN point of view, a device has two types of interfaces: Access interface and Trunk interface. Access interface: An Access interface can only belong to one VLAN and can only forward messages belonging to that VLAN. By default, all the Access interfaces belongs only to VLAN 1.

Trunk interface: An Trunk interface can belong to more than one VLAN and can forward messages from one VLAN to another. By default, all the Trunk interfaces of a device belong to all VLANs.

What is SVI

SVI is an abbreviation for Switch virtual interface and is a logical interface used to implement Layer 3 switching. A VLAN limits the scope of lay 2 messages, therefore, if one host in a VLAN would connect to another host in other VLAN, the message must pass through a Layer 3 device on which SVI is the logical interface that connect between these two VLANs.

SVI is composed of an IP address and a mask. One VLAN has one main SVI and multiple secondary SVIs.

SVI information is only applicable on layer 3 device like RG-S3760 rather than Layer 2 device like RG-S2126G.

8.2. Device VLAN Management

With Device VLAN management, you can use web browser not only to browse the VLAN information of Ruijie devices but also add, modify, or delete VLANs.

Function List

- VLAN Configurations
- Synchronize VLAN information
- Add VLAN
- Delete VLAN

- Modify VLAN information

8.2.1. VLAN Configurations

1) When you click the device name in the device list, the system will open the device detail information page. When you click the **VLAN Configurations** link on the right in the device detail information page, the system will open **VLAN configurations** page, as shown in the following figure:

Figure 8.1. Device detail information

If no VLAN information is saved for the current device before, the page will display nothing. In this case, you need to click **Synchronize** to perform a VLAN information synchronization, as shown in the following figure:

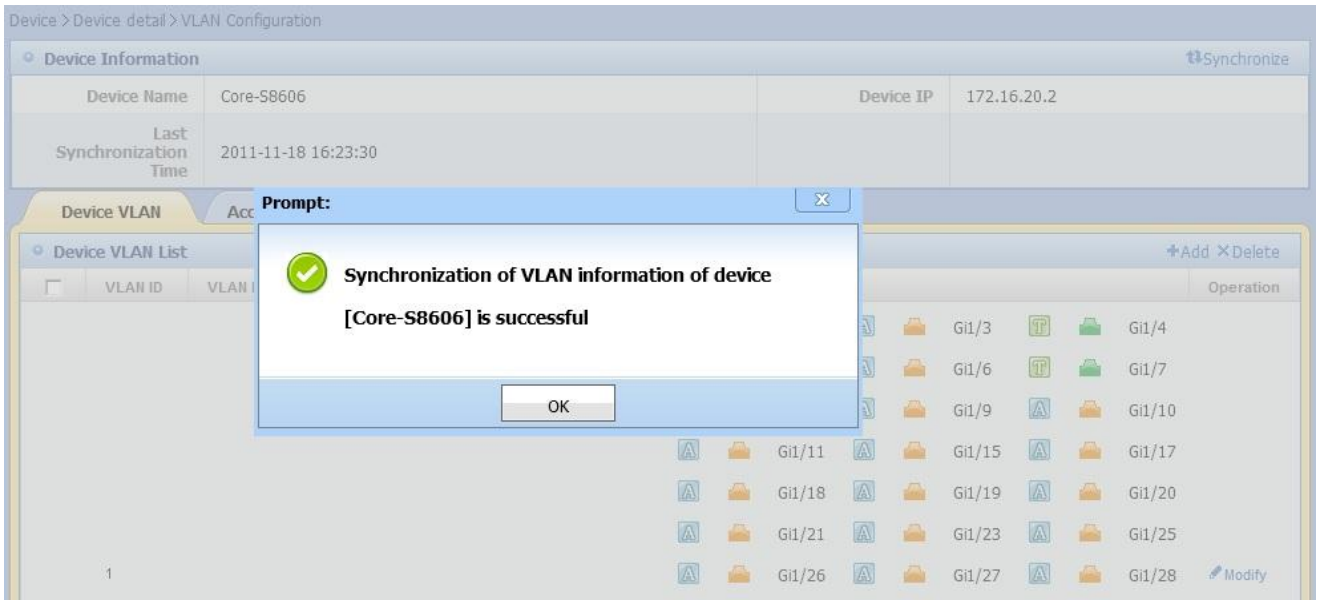


Figure 8.2. Device VLAN information

To synchronize the VLAN information, please refer to *Synchronize VLAN information*.

Once **Synchronize** is clicked, the system will try to acquire the VLAN information from the device immediately. After the VLAN information is fetched, the basic information of the device is displayed along with the last synchronization time. At the same time, the system will provide 3 more views -- **Device VLAN**, **Access Interface** and **Trunk Interface** -- for you to view the detail perspective, as shown in the following figure:

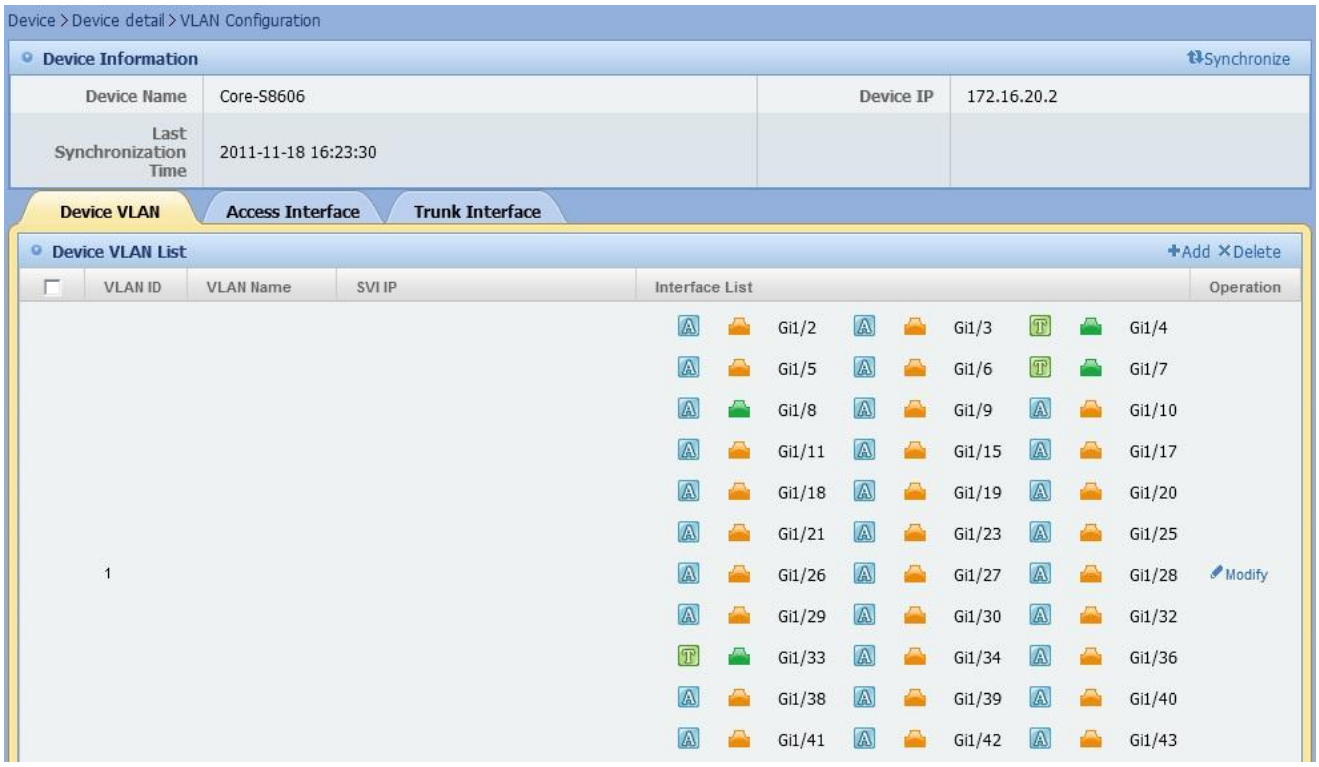


Figure 8.3. Device VLAN list

Figure 8.4. Access interface list

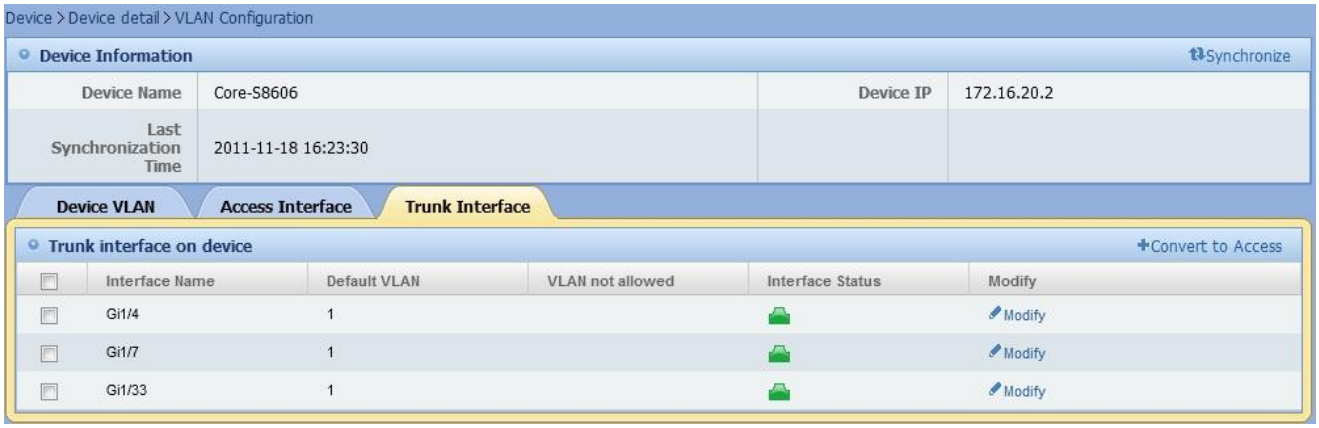


Figure 8.5. Trunk interface list

In the **Device VLAN** tab, click **Add** button to add new VLAN information to the device. For more information, please refer to *Add VLAN*.
In the **Device VLAN** tab, click **Modify** icon to change the VLAN information of the device. For more information, please refer to *Modify VLAN information*.
In the **Device VLAN** tab, tick the checkbox before the VLAN list and press **Delete** button to delete the VLAN information for the device. For more information, please refer to *Delete VLAN*.
In the **Access interface** tab, tick the checkbox before the Access interface name and press **Convert to Trunk** to open the **Convert to Trunk interface** page. For more information, please refer to *Convert to a Trunk Interface*.
In the **Access interface** tab, tick the checkbox before the Access interface name and press **Move** button to open **Move Access interface** page. For more information, please refer to *Move Access Interface*.
In the **Trunk interface** tab, tick the checkbox before the Trunk interface name and press **Convert to Access** button to open the **Convert Access interface** page. For more information, please refer to *Convert to an Access Interface*.
In the **Trunk interface** tab, press **Modify** icon to open **Update Trunk interface** page. For more information, please refer to *Modify Trunk Interface*.

8.2.2. Synchronize VLAN information

In the **Synchronize VLAN information** page, you can manually synchronize the VLAN information for the device.

Operation Step

In the **VLAN Configurations** page, press **Synchronize** button, the system will synchronize VLAN information for the device. As shown by the screenshot below:

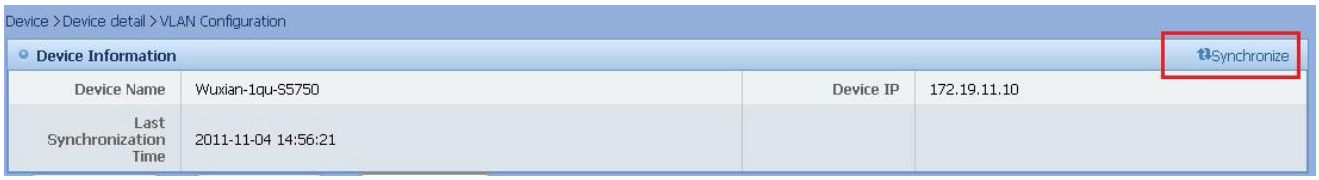


Figure 8.6. Synchronize VLAN information

Note

When you modify VLAN configuration for a device, the system will automatically synchronize VLAN information for you. During the synchronization, if the system detects a confliction in your configuration change, the VLAN configuration command will not be executed and you need to reconfigure the VLAN. You don't need to press the **Synchronize** button every day since the system will synchronize the VLAN information for you at 0:00 every night.
If you meet problem or have difficulty when synchronizing the VLAN information, refer to *VLAN FAQ*.

8.2.3. Add VLAN

In the **Add VLAN** page, the administrator is able to add VLAN and configure its interface and SVI information.

Operation Step

1) As shown by the screenshot below, **Add** button will open **Add VLAN** page in the **VLAN Configurations** page.

Figure 8.7. VLAN Configuration

As shown by the screenshot below, fill in all the VLAN information in the **Add VLAN** page and click the **Add** button to commit the VLAN information.

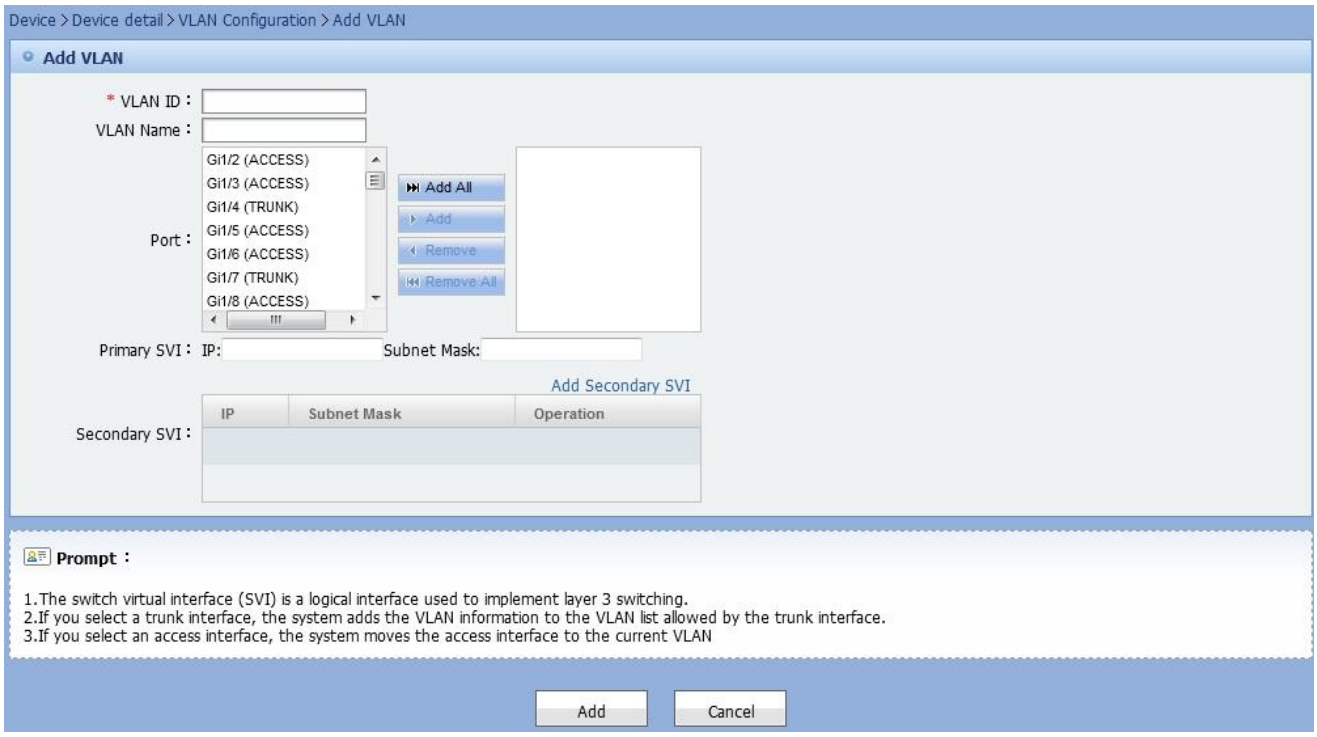


Figure 8.8. Add VLAN

By pressing **Cancel** button, system will discard all the changes you made and return to page **VLAN Configurations**.

Note

Neither duplicated VLAN ID nor empty VLAN ID is allowed.
Please be cautious when you add an interface. The network or some devices are inaccessible if you configure it improperly. In this case, you must log in to the device using serial port to reconfigure it.
SVI parameter is only applicable to Layer 3 devices, not to Layer 2 devices.
If you meet problem or difficulty when adding VLAN, refer to *VLAN FAQ*.

8.2.4. Delete VLAN

In **Delete VLAN** page, you are able to delete VLANs.

Operation Steps

In the **VLAN Configurations** page, select **Device VLAN** tab, tick the checkbox before the VLAN list and press **Delete** button, then all the selected information will be deleted from the device. As shown by the screenshot below:

Figure 8.9. Delete VLANs from the device

Note

VLAN 1 cannot be deleted because it is reserved as default VLAN for Ruijie device.
Once a VLAN is deleted, its Access interface will be automatically transferred to VLAN 1, while the configuration of its Trunk interface is kept intact.
If you meet problem or difficulty when deleting VLAN, refer to *VLAN FAQ*.

8.2.5. Modify VLAN information

In the **Modify VLAN** page, you can update device information like VLAN name, interface configuration and SVI information.

Operation Steps

1) In **VLAN Configurations** page, click **Modify** icon on VLAN list to enter **Modify VLAN** page. As shown below:

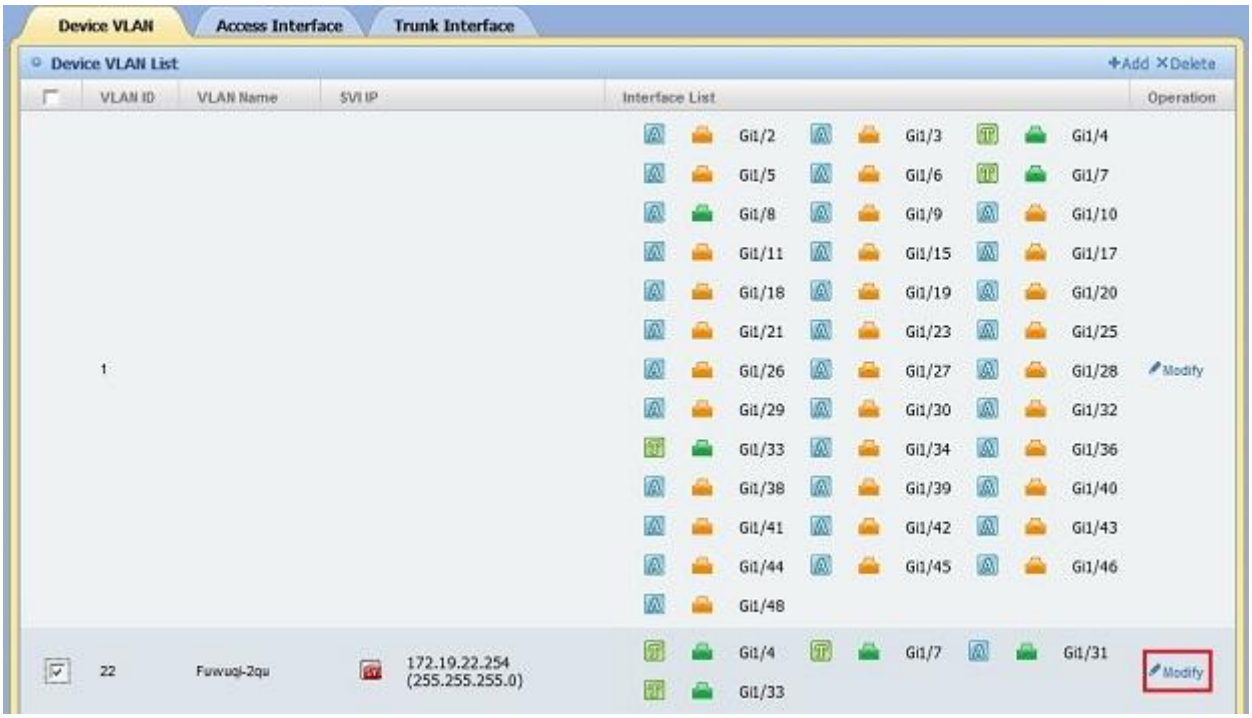


Figure 8.10. VLAN Configuration

In the **Modify VLAN** page, fill in all the information and press **Modify** button to commit the updates. As shown by the screenshot below:

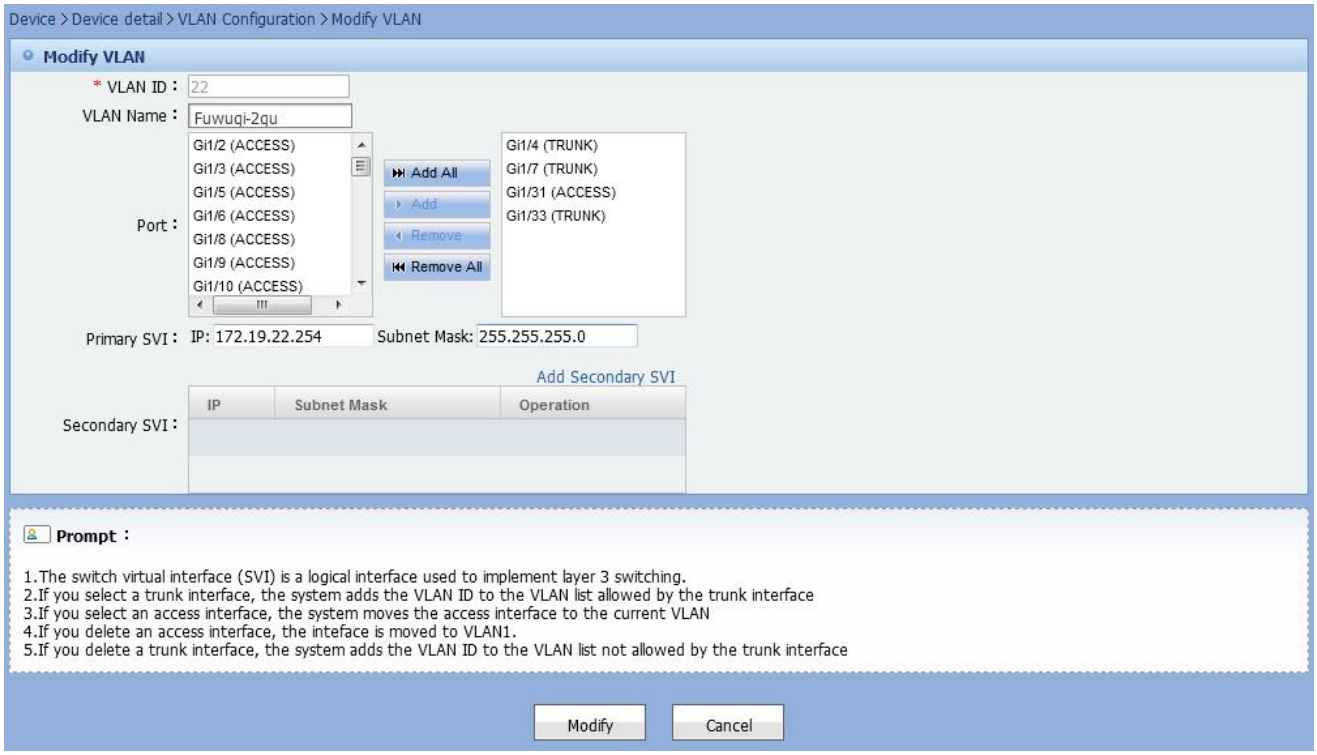


Figure 8.11. Modify VLAN information

In the **Modify VLAN** page, if you press **Cancel** button, the system will discard all the changes you made and return to the page **VLAN Configurations**.

Note

VLAN ID cannot be changed.
Please be cautious when you change the configuration of VLAN. The network or some devices is

inaccessible if you configure it improperly. In this case, you must log in to the device using serial port to reconfigure it.
SVI information is only supported by Layer 3 devices rather than Layer 2 devices.
If you meet problem or difficulty when updating VLAN information, refer to *VLAN FAQ*.

8.3. VLAN interface management

In VLAN interface management, you can browse and even change the configuration, such as interface mode, permitted VLAN list, for every interface on the device via the web browser application.

Function List

- Convert to a Trunk Interface
- Convert to an Access Interface
- Move Access Interface
- Modify Trunk Interface

8.3.1. Convert to a Trunk Interface

In the **Convert to a Trunk Interface** page, you are able to convert the selected Access interface to Trunk interface and configure that Trunk interface with default VLAN and its blacklist at the same time.

Operation Steps

1) In **VLAN Configurations** page, select **Access Interface** tab, select all the interfaces you need to convert and click **Convert an interface into a Trunk interface** button, the **Convert to Trunk** page is opened, as shown by the screenshot below:

Figure 8.12. VLAN Configuration

In the **Convert to Trunk** page, after you fill in all the information and press the **Convert** button, the selected interface will convert an interface into a Trunk interface, as shown by the screenshot below:

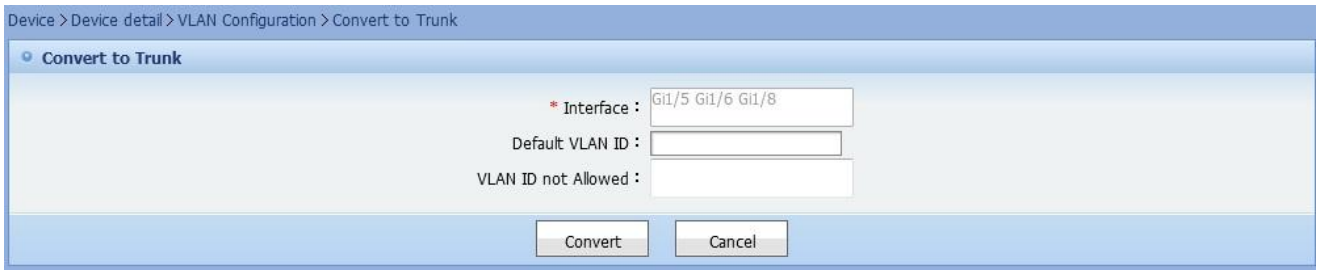


Figure 8.13. Convert an interface into a Trunk interface

In the **Convert to Trunk** page, if you press **Cancel** button, the system will discard all the changes you made and return to page **VLAN Configurations**.

Note

If you press **Convert** button without any information, the selected interface will be converted to Trunk interface with **VLAN 1** as its VLAN ID and **All VLAN** as its permit VLAN.
Please be cautious when you convert an interface. The network or some devices cannot be accessible if you

configure it improperly. In this case, you must login the device using serial port to reconfigure it.
If you meet problem or difficulty when changing the interface, Please refer to *VLAN FAQ*.

8.3.2. Convert to an Access Interface

In the **Convert to an Access Interface** page, you are able to convert the selected Trunk interface to an Access interface, and configure the VLAN whose packets are permitted to pass through the Access interface.

Operation Steps

1) In the **VLAN Configurations** page, select **Trunk Interface** tab, select all the interfaces you need to convert and click **Convert to Access** button, the **Convert to Access** page will be opened. As shown by the screenshot below:

Figure 8.14. VLAN configuration

In the **Convert to Access** page, you need to fill the configuration information and press **Convert** button, the selected interface will be converted to Access interface. As shown by the screenshot below:

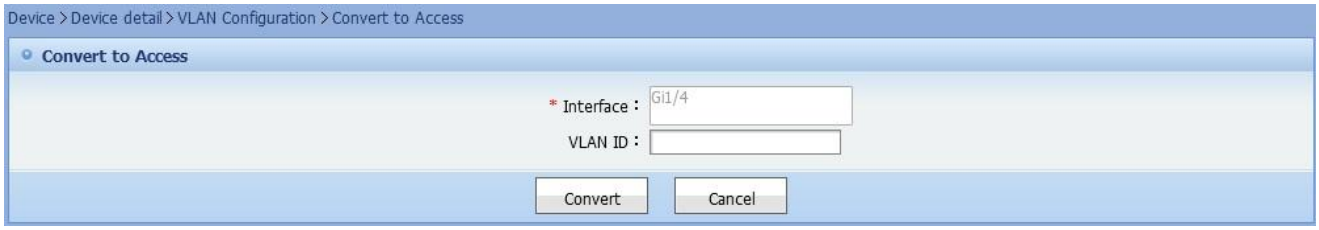


Figure 8.15. Convert to Access

In the **Convert to Access** page, if you press **Cancel** button, the system will discard all the changes you made and return to page **VLAN Configurations**.

Note

If you press **Convert** button without any information, the selected interface will be converted to Access interface and only messages of VLAN 1 are permitted.
Please be cautious when you convert the interface. The network or some devices in inaccessible if you configure it improperly. In this case, you must log in the device using serial port to reconfigure it.
If you meet problem or difficulty when changing the interface, refer to *VLAN FAQ*.

8.3.3. Move Access Interface

In the **Move Access Interface** page, you are able to move the selected interface to a VLAN that you specify.

Operation Steps

1) In the **VLAN Configurations** page, select **Access Interface** tab, select all the interfaces that you would like to move, and press **Move** button to open the **Move** page. As shown by the screenshot below:

Figure 8.16. VLAN configuration

In the **Move Access Interface** page, fill in all the information and press **Move** button, the system will convert all the selected interfaces into Access interfaces. As shown by the screenshot below:

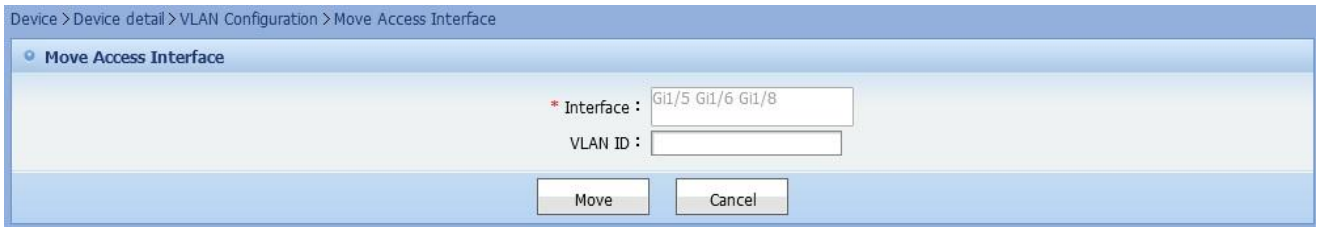


Figure 8.17. VLAN configuration

In the **Move Access Interface** page, press **Cancel** button and the system will discard all the changes you made and return to the page **VLAN Configurations**.

Note

If you press **Move** button without any input, all the selected interfaces will be transferred to VLAN 1.
Please be cautious when you are moving interfaces. The network or some devices is inaccessible if you configure it improperly. In this case, you must log in to the device using serial port to reconfigure it.
If you meet problem or difficulty when moving interfaces, refer to *VLAN FAQ.*

8.3.4. Modify Trunk Interface

In the **Modify Trunk Interface** page, you are able to modify the default VLAN ID and determine the IDs of the VLANs whose packets are not allowed to pass.

Operation Steps

1) In page **VLAN Configurations**, select **Trunk Interface** tab, press **Modify** icon and the system will open the **Modify Trunk Interface** page. As shown by the screenshot below:

Figure 8.18. VLAN configuration

In the **Modify Trunk Interface** page, modify the information and press **Modify** button to commit the change to the Trunk interface. As shown by the screenshot below:

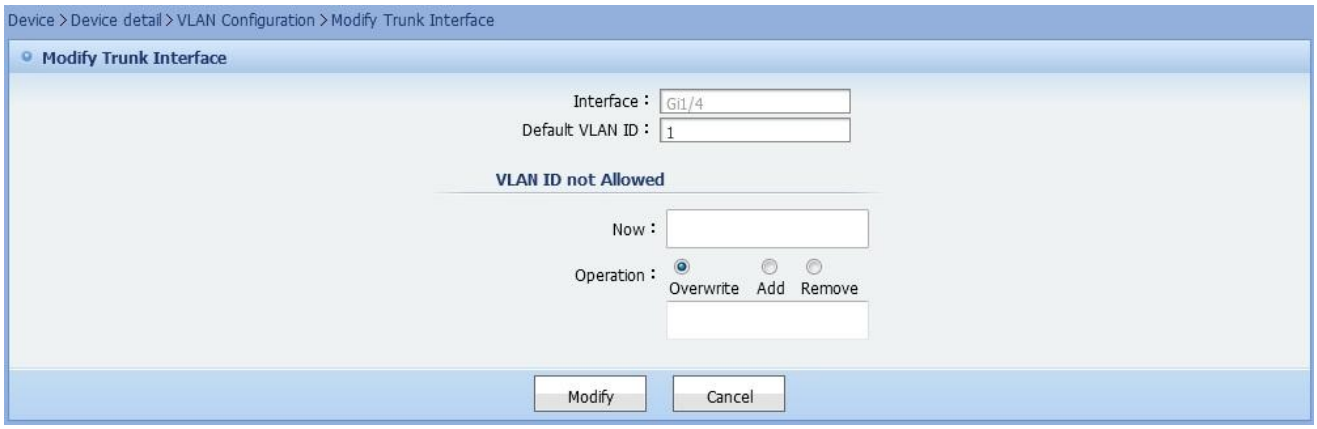


Figure 8.19. Modify Trunk Interface

In the **Modify Trunk Interface** page, if you press **Cancel** button, the system will discard all the changes you made and return to page **VLAN Configurations**.

Note

The system provides three approaches to configure a blacklist of VLANs whose packets are not allowed to pass through the Trunk interface. They are **Overwrite**, **Add** and **Delete**.
Overwrite: The system will replace the old blacklist configuration with the new one.
Add: The system will merge the new blacklist configuration with the old one.
Delete: The system will remove all the VLANs in the new blacklist from the old one.
Please be cautious when you modify the Trunk interface. The network or some devices cannot be accessible if you configure it improperly. In this case, you must login the device using serial port to reconfigure it.
If you meet problem or difficulty when modifying Trunk interface, Please refer to *VLAN FAQ*.

8.4. VLAN FAQ

Why the system cannot fetch or configure the VLAN information of the device?

Check whether the device is connected to the network first, then check if the TELNET template on the device is configured correctly and finally make sure the TELNET server on the device is started.

Why I cannot configure SVI information for the device?

Check whether the device is a Layer 2 device. Please be noted that SVI information is only supported by Layer 3 devices rather than Layer 2 devices.

How do I recover a device which is no longer configurable due to a wrong configuration operation?

Sorry, the system cannot recover the device for you. In this case, you must log in to the device from a serial port to reconfigure it correctly.

Chapter 9 MIB Management

This module describes the synchronization and display of MIB information. With this system, you can view MIB information of a device conveniently, which includes: BGP peer table, BGP4 receiving path attribute table, BGP receiving path attribute table, OSPF basic information, OSPF area table, OSPF STUB area table, OSPF LSDB table, OSPF interface table and OSPF interface metric table.

Function List

- View MIB Information
- Synchronize MIB Information

9.1. View MIB Information

With this system, you can view the MIB information of a device conveniently, which includes: BGP peer table, BGP4 receiving path attribute table, BGP receiving path attribute table, OSPF basic information, OSPF area table, OSPF STUB area table, OSPF LSDB table, OSPF interface table and OSPF interface metric table.

- View Information Of BGP Peer Table
- View BGP4 Receiving Path Attribute Table
- View Information Of BGP Receiving Path Attribute Table
- View Basic Information of OSPF
- View Information of OSPF Area Table
- View Information Of OSPF STUB Area Table
- View Information Of OSPF LSDB Table
- View Information Of OSPF Interface Table
- View Information Of OSPF Interface Metric Table

9.1.1. View Information Of BGP Peer Table

On routing protocol information page, you can view the information of BGP peer table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.1. Enter routing protocol information page

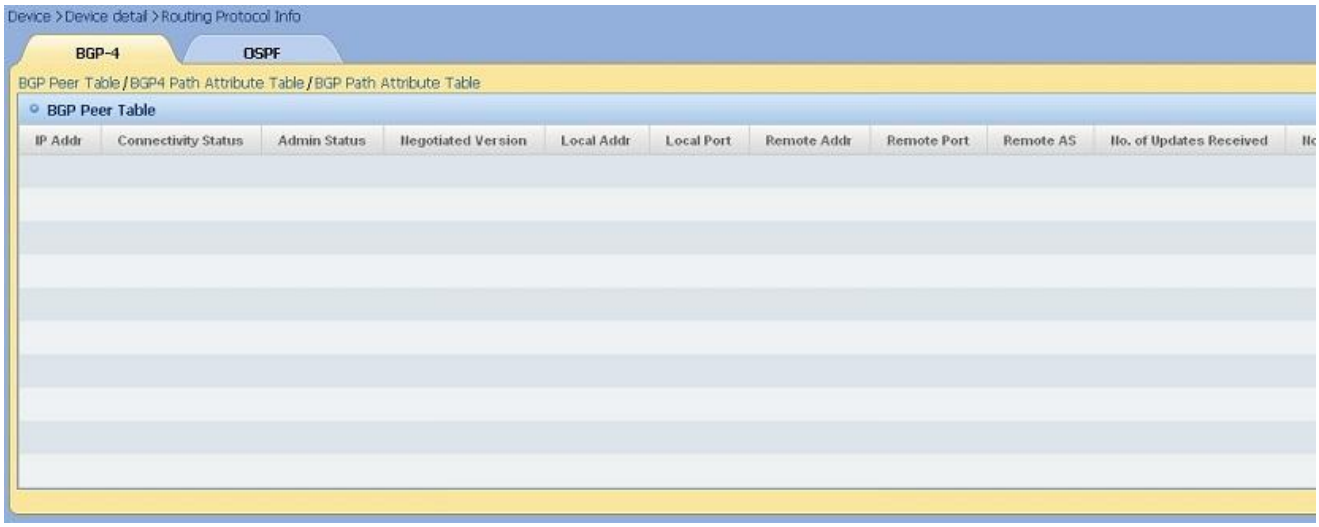


Figure 9.2. View BGP Peer Table Information in Routing Protocol information

9.1.2. View BGP4 Receiving Path Attribute Table

On the routing protocol information page, you can view BGP4 receiving path attribute table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.3. Enter routing protocol information page

Figure 9.4. Select BGP4 Receiving Path Attribute Table

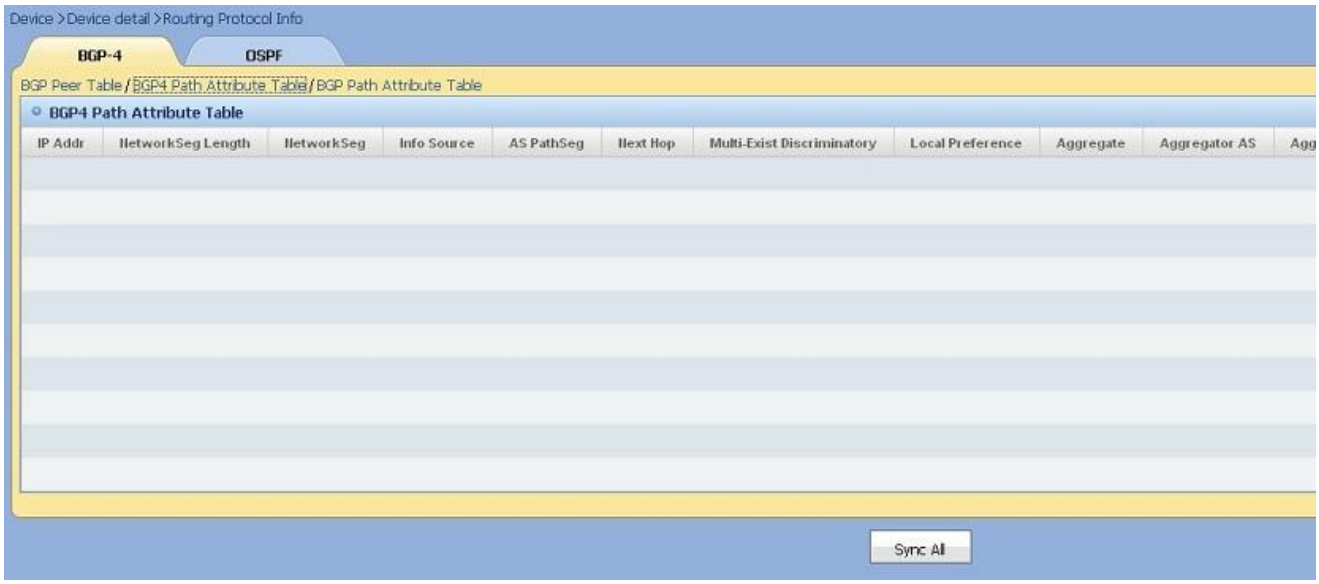


Figure 9.5. View BGP4 Receiving Path Attribute Table

9.1.3. View Information Of BGP Receiving Path Attribute Table

On routing protocol information page, you can view information of BGP receiving path attribute table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter R**outing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.6. Enter routing protocol information page

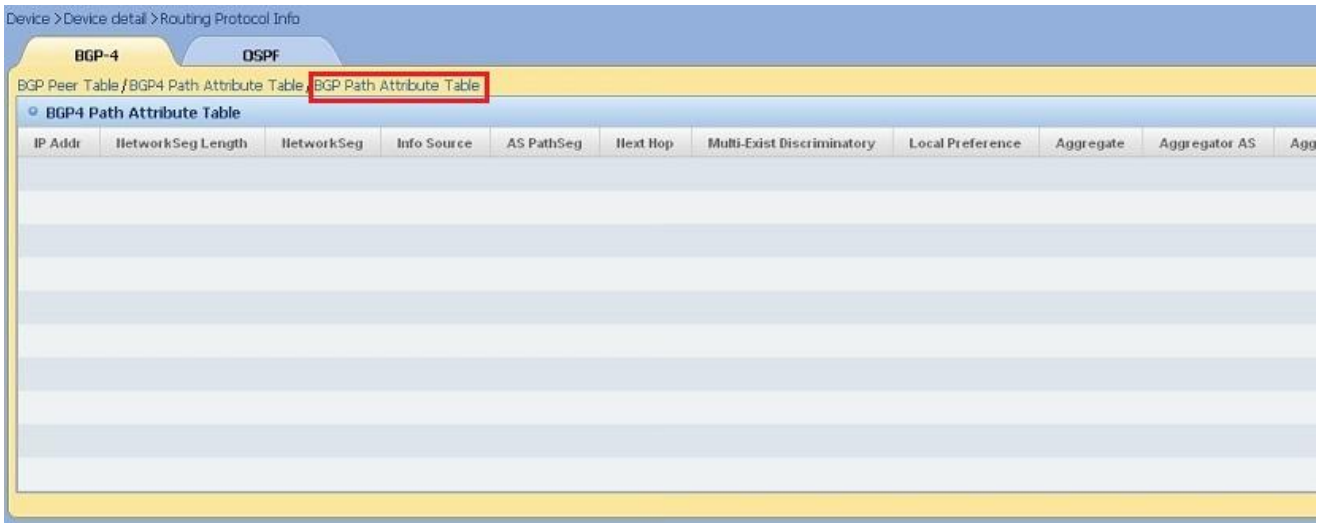


Figure 9.7. Select BGP Receiving Path Attribute Table

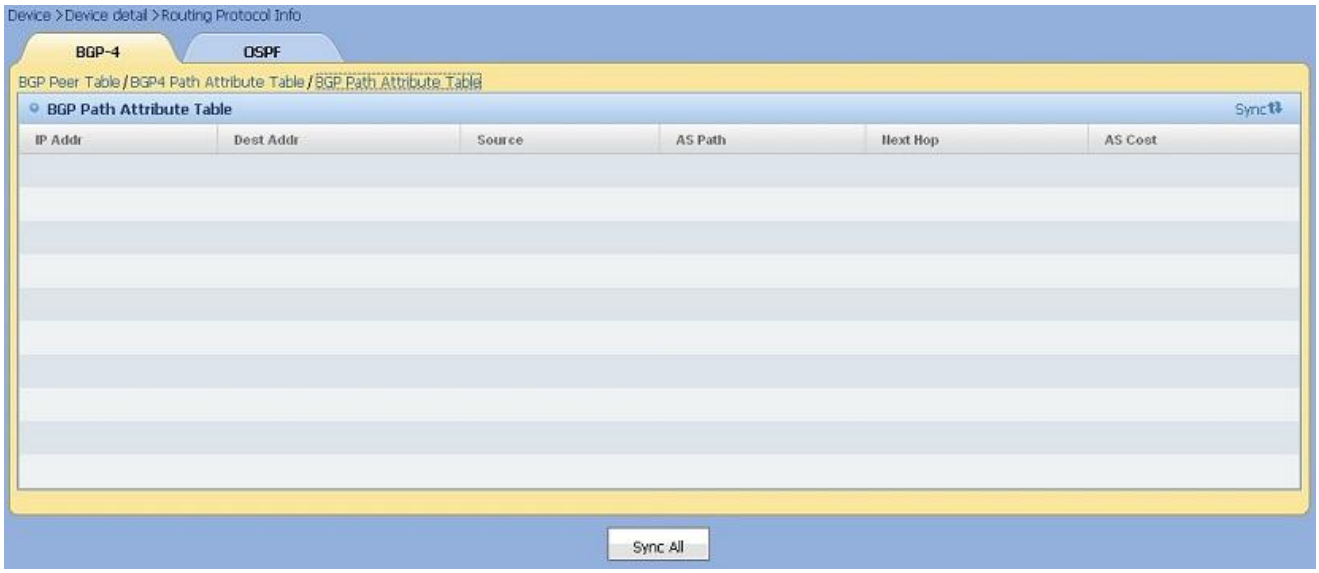


Figure 9.8. View Information Of BGP Receiving Path Attribute Table

9.1.4. View Basic Information of OSPF

On routing protocol information page, you can view basic information of OSPF.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.9. Enter routing protocol information page

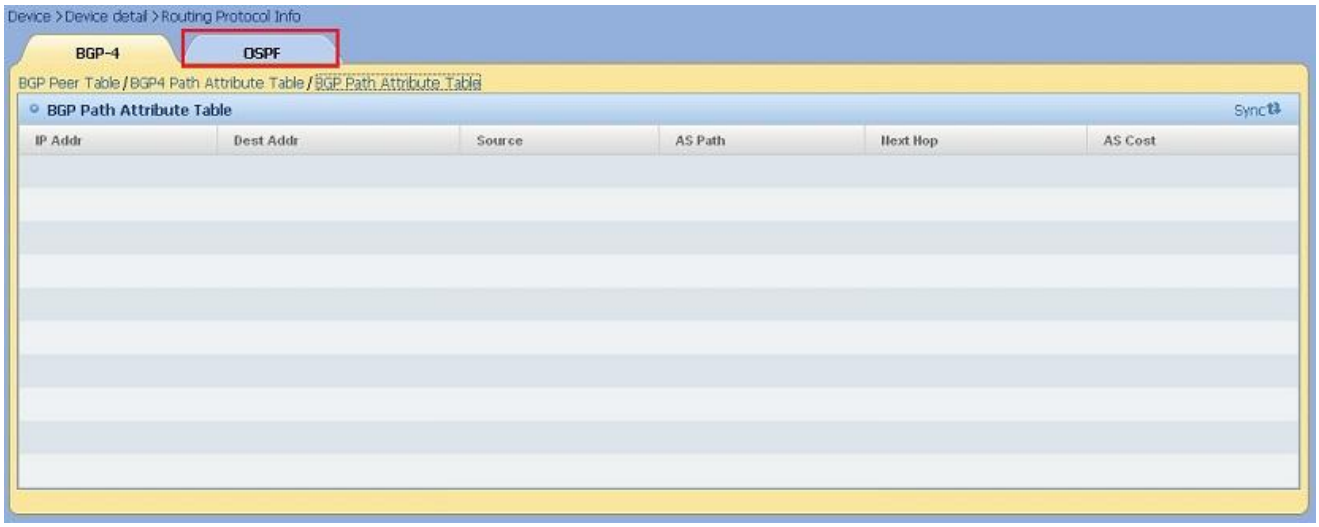


Figure 9.10. Select OSPF

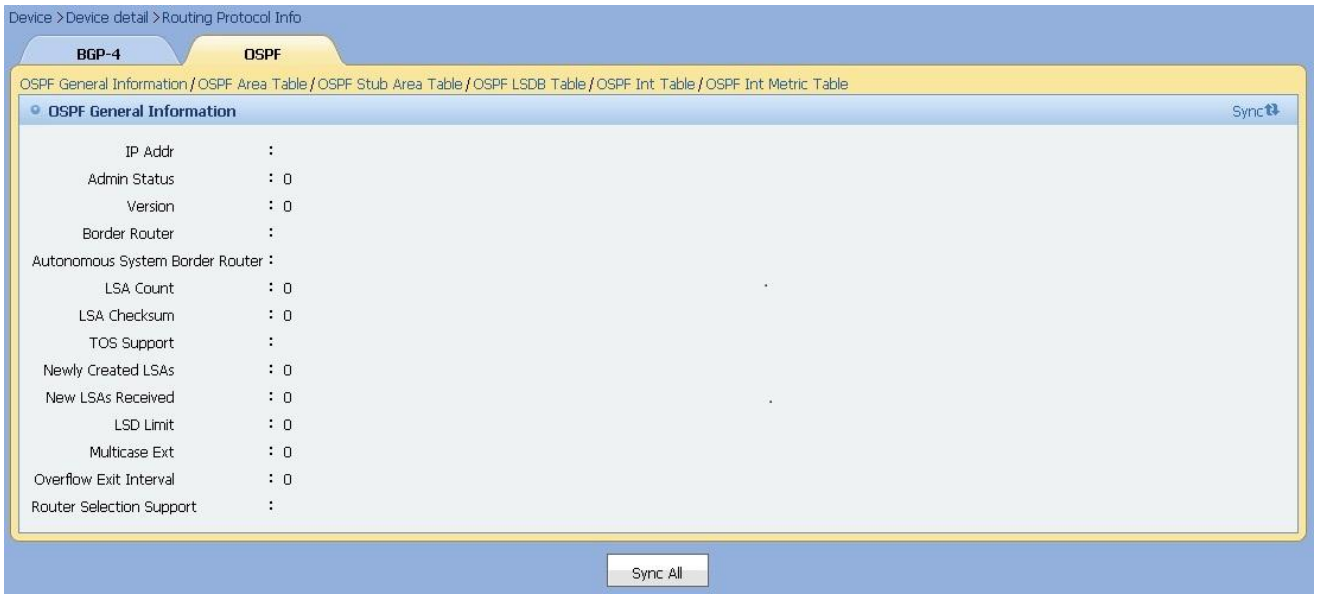


Figure 9.11. View Basic Information of OSPF

9.1.5. View Information of OSPF Area Table

On routing protocol information page, you can view information of OSPF area table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.12. Enter routing protocol information page

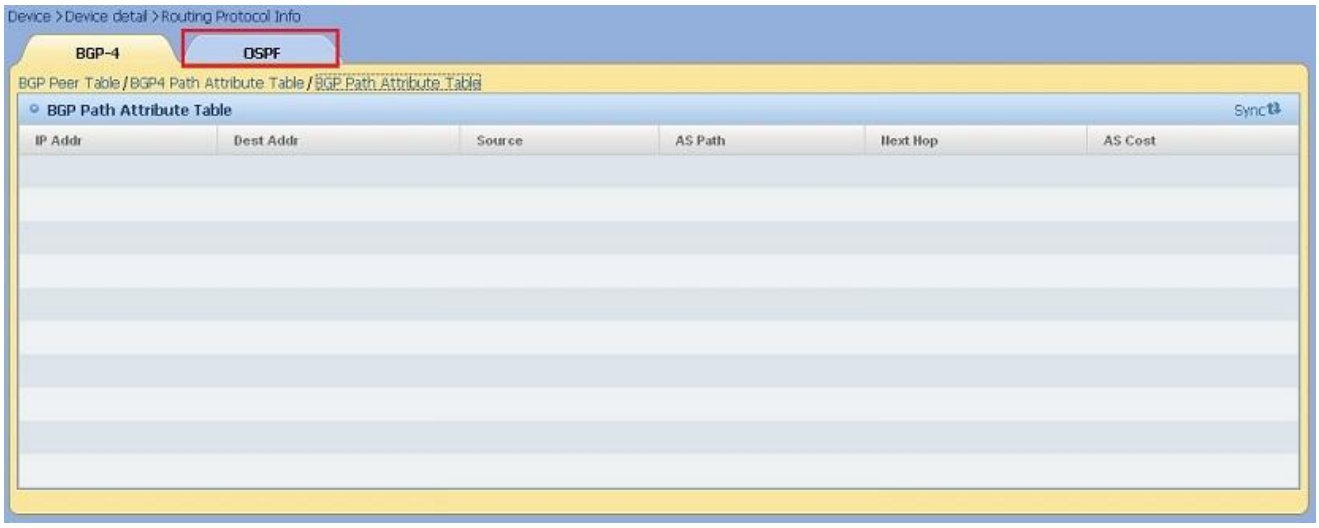


Figure 9.13. Select OSPF

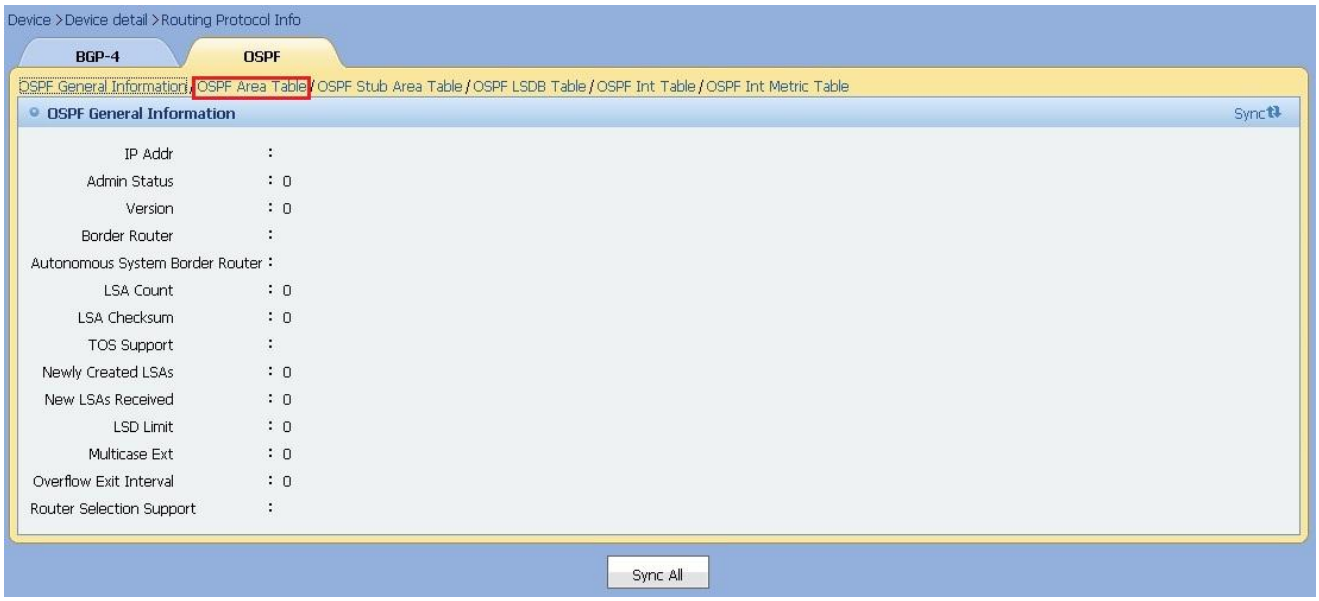


Figure 9.14. Select OSPF Area Table

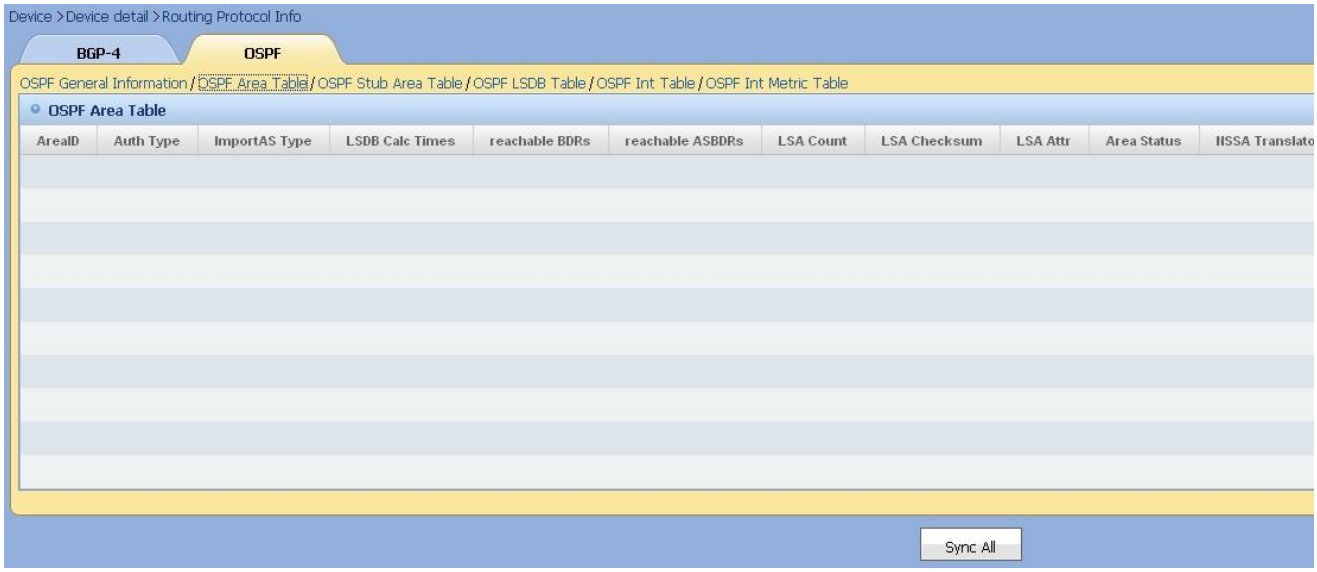


Figure 9.15. View Information Of OSPF Area Table

9.1.6. View Information Of OSPF STUB Area Table

On routing protocol information page, you can view information of OSPF STUB area table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.16. Enter routing protocol information page

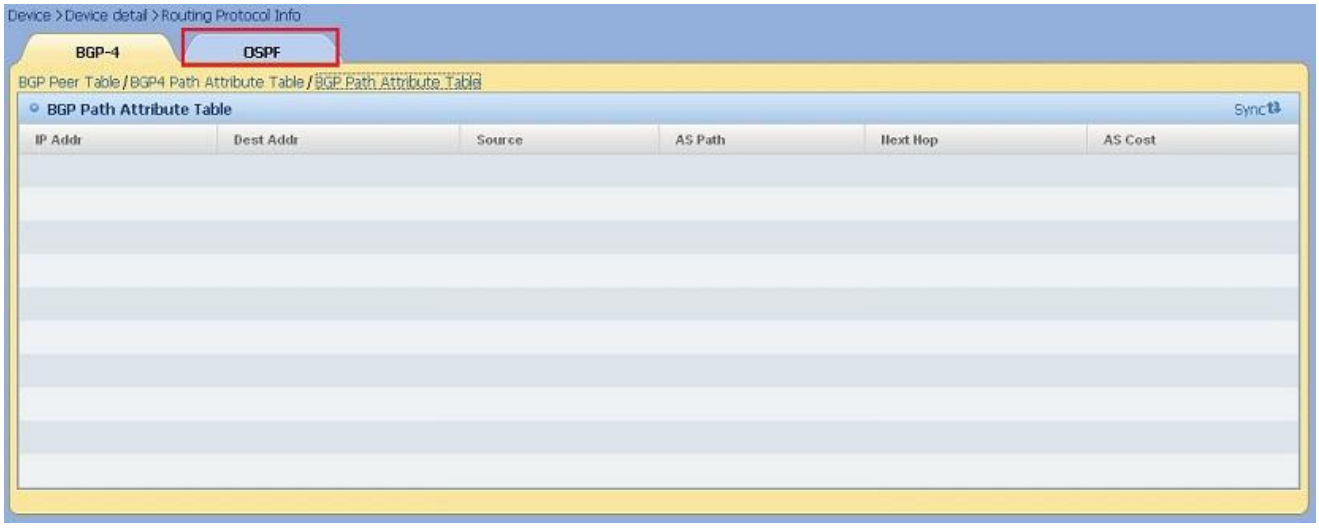


Figure 9.17. Select OSPF

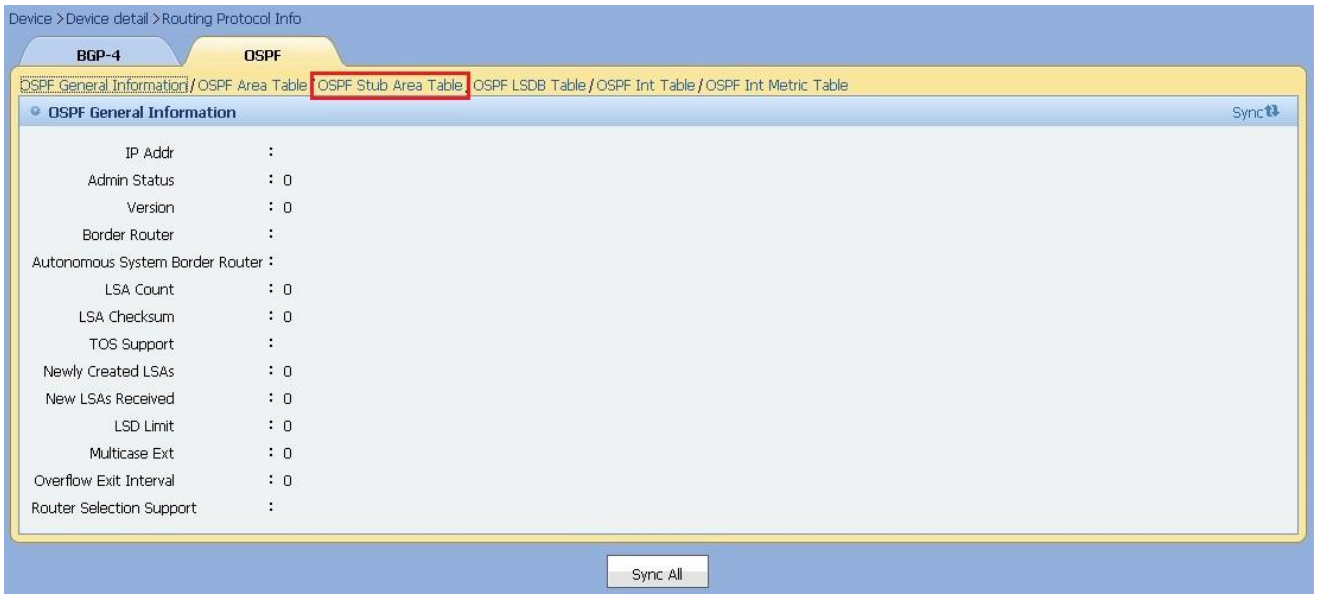


Figure 9.18. Select OSPF STUB Area Table

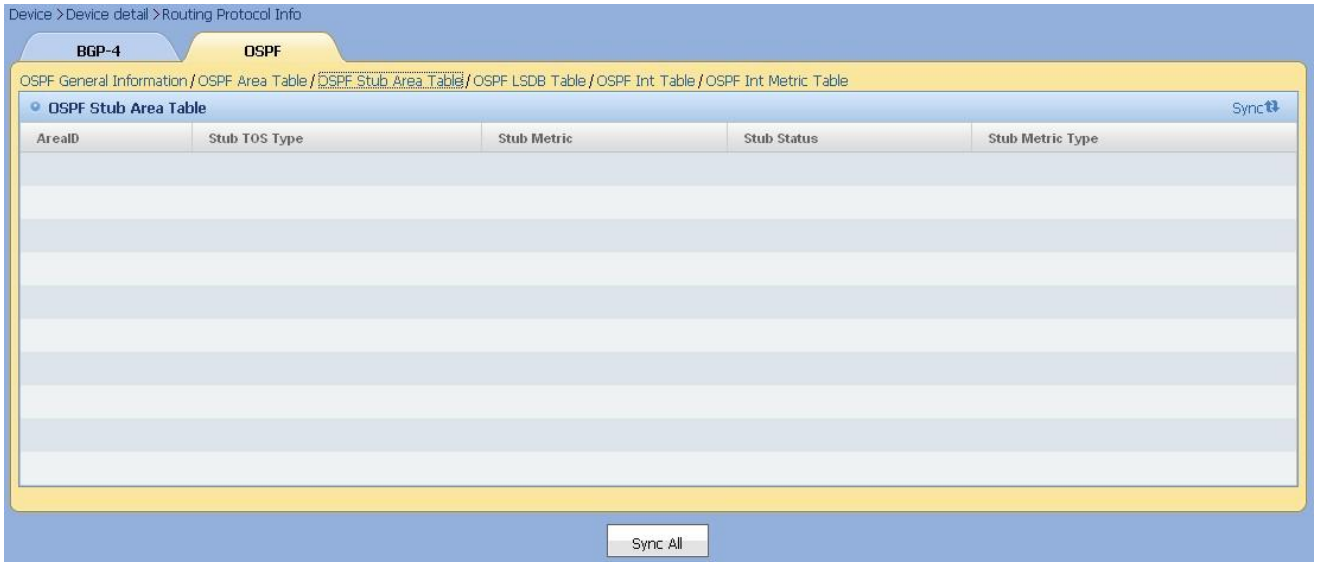


Figure 9.19. View Information Of OSPF STUB Area Table

9.1.7. View Information Of OSPF LSDB Table

On routing protocol information page, you can view information of OSPF LSDB table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.20. Enter routing protocol information page

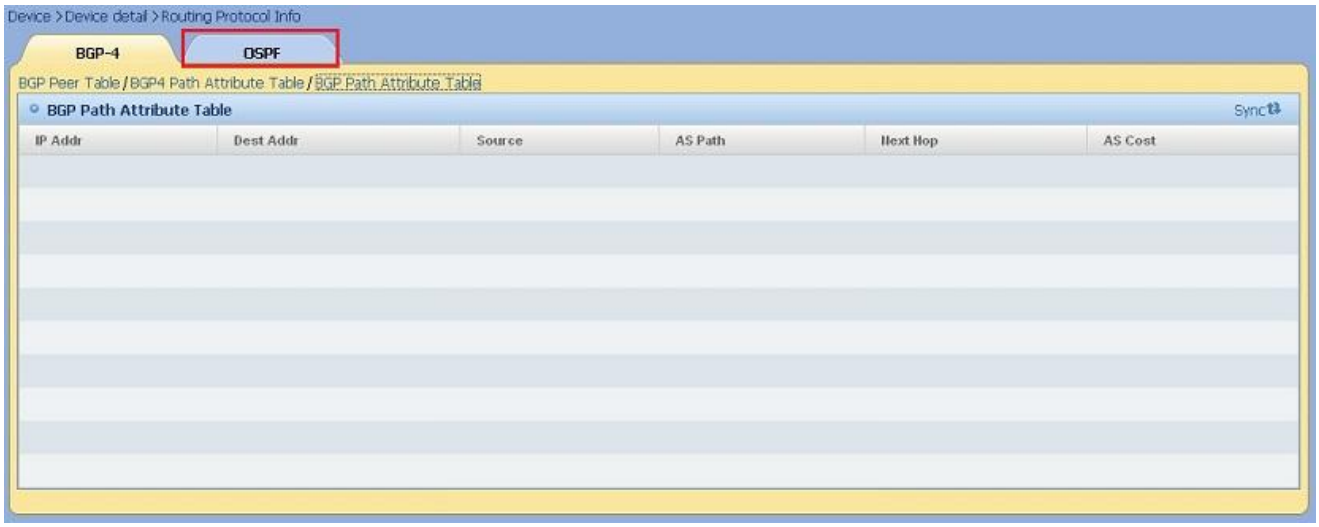


Figure 9.21. Select OSPF

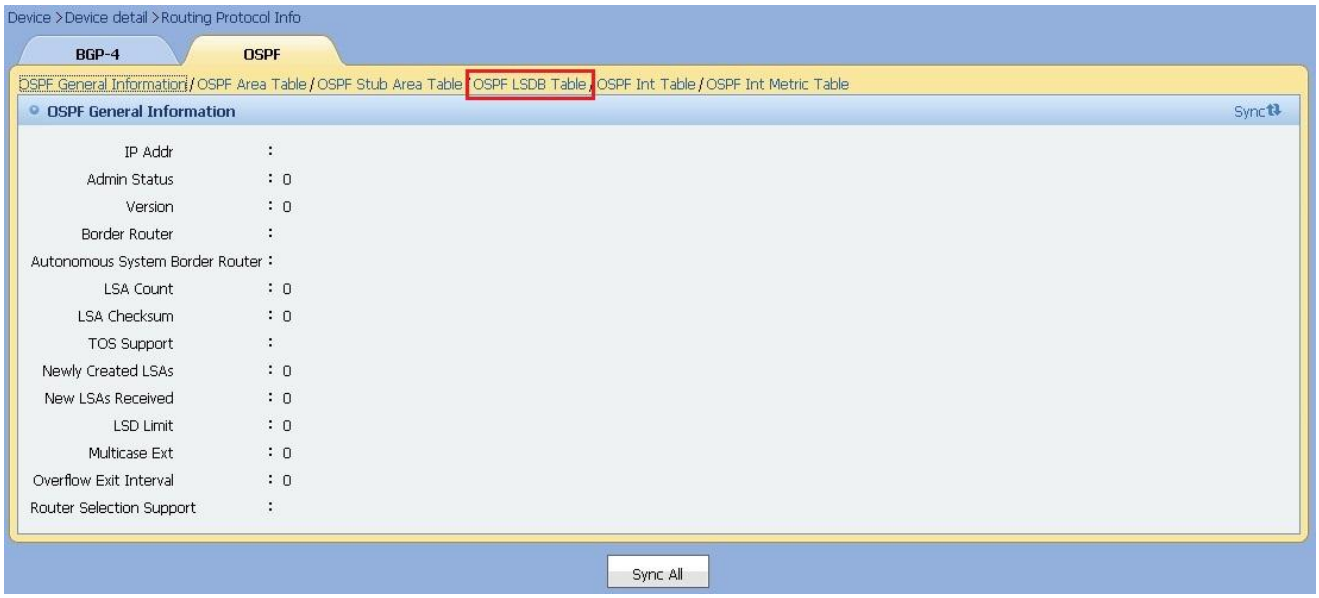


Figure 9.22. Select OSPF LSDB Table

Figure 9.23. View Information Of OSPF LSDB Table

9.1.8. View Information Of OSPF Interface Table

On routing protocol information page, you can view information of OSPF interface table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.24. Enter routing protocol information page

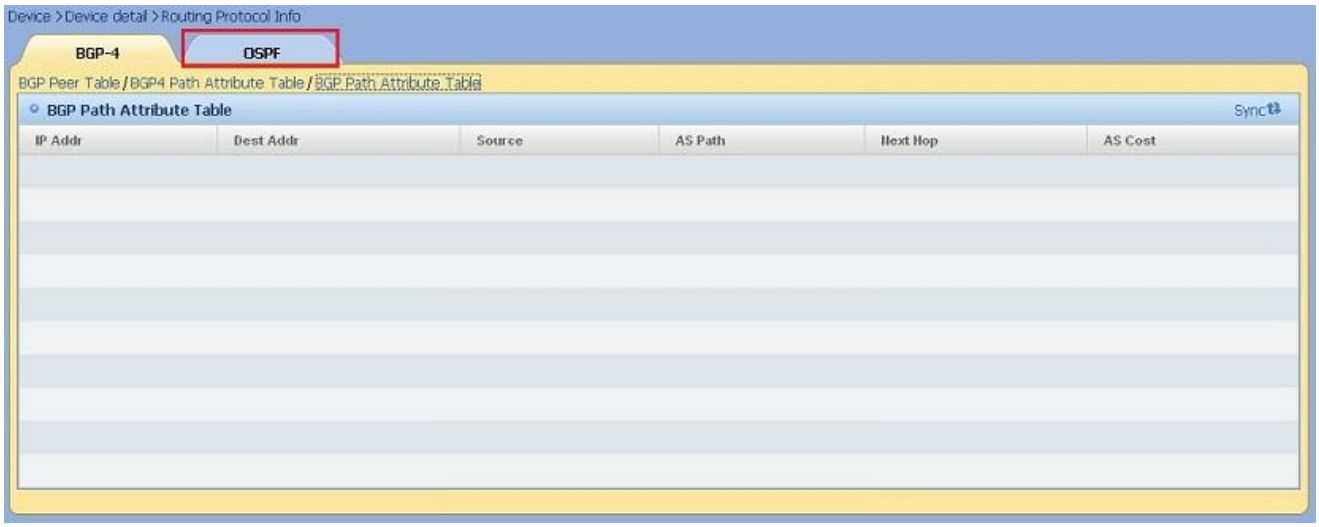


Figure 9.25. Select OSPF

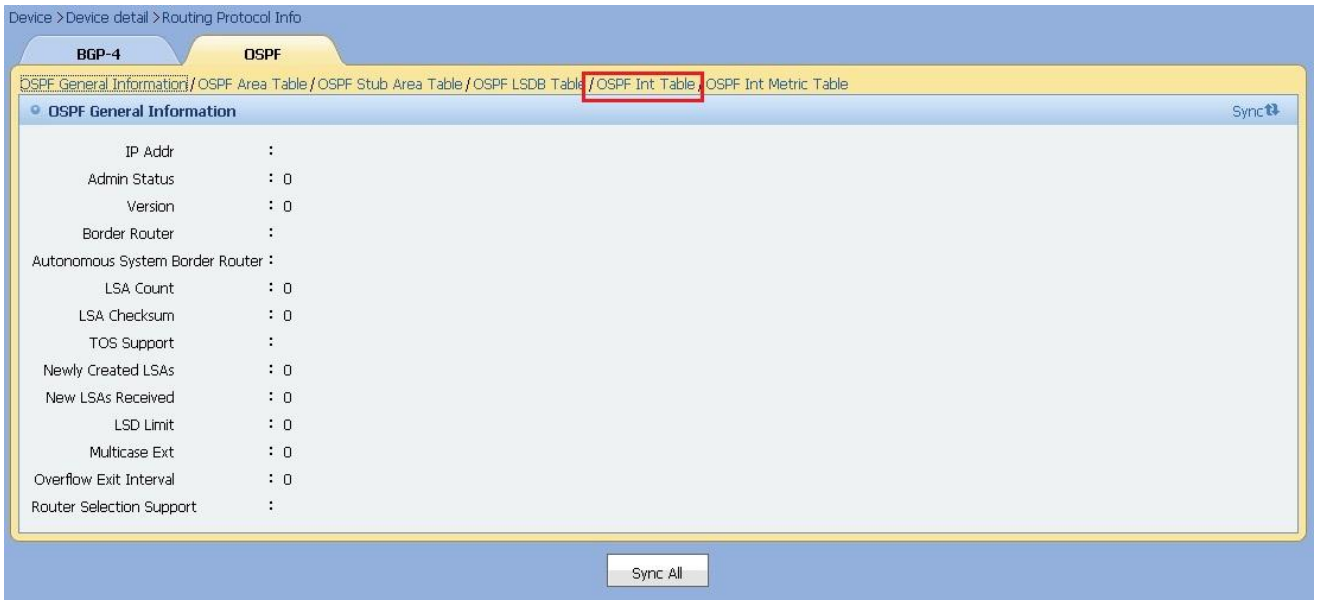


Figure 9.26. Select OSPF Interface Table

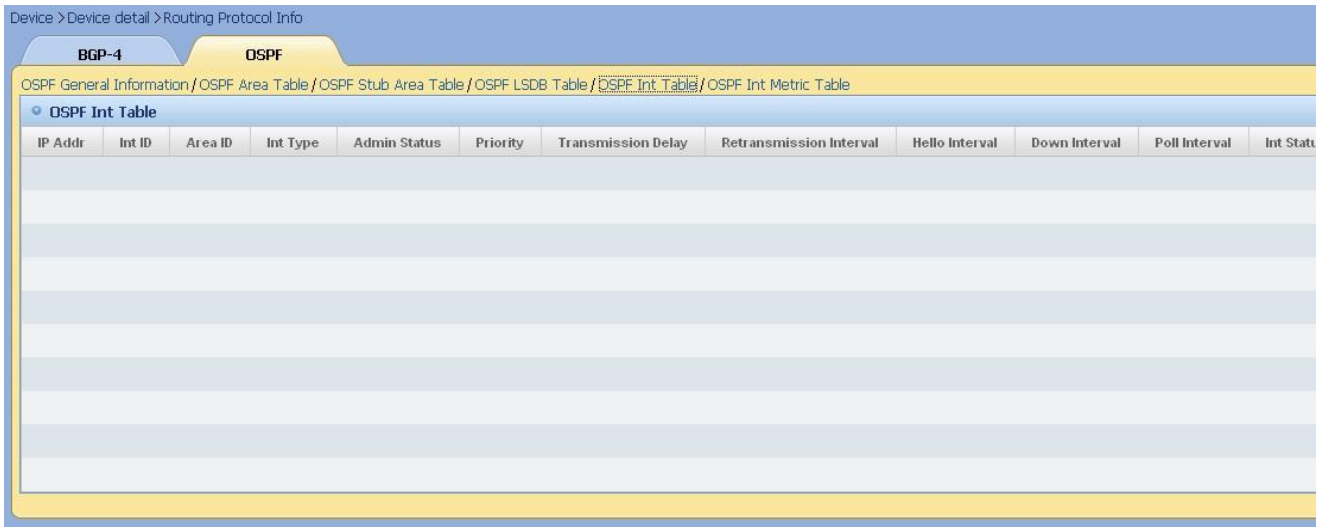


Figure 9.27. View Information Of OSPF Interface Table

9.1.9. View Information Of OSPF Interface Metric Table

On routing protocol information page, you can view information of OSPF interface metric table.

Operation Steps

Enter device detail information page, click **Routing Protocol Info** link to enter **Routing Protocol Info** page, the routing protocol information will be displayed. As shown below:

Figure 9.28. Enter routing protocol information page

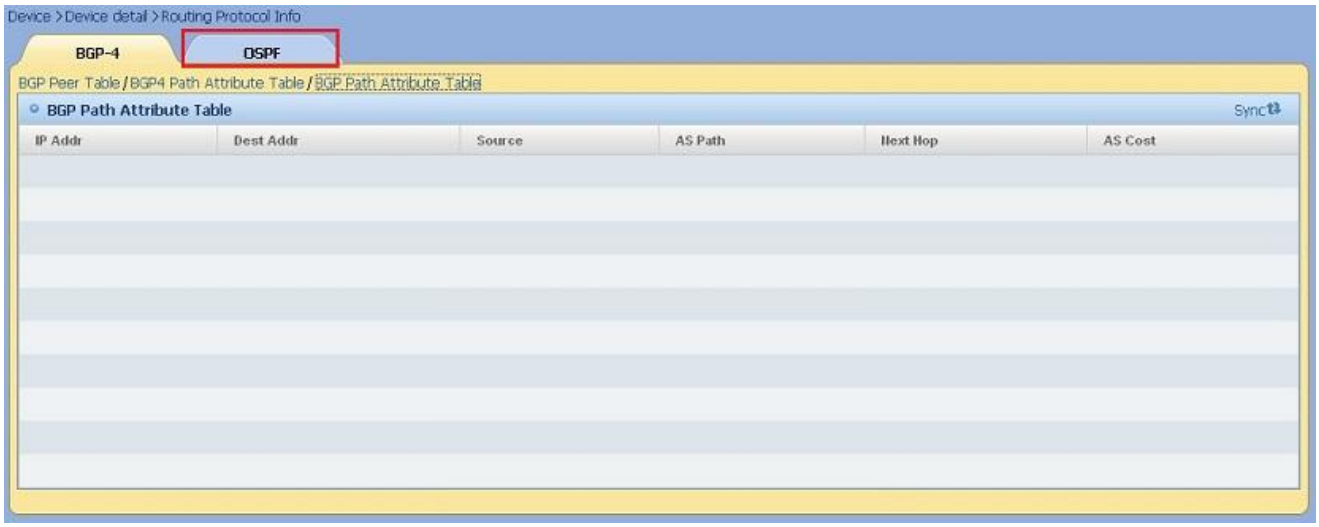


Figure 9.29. Select OSPF

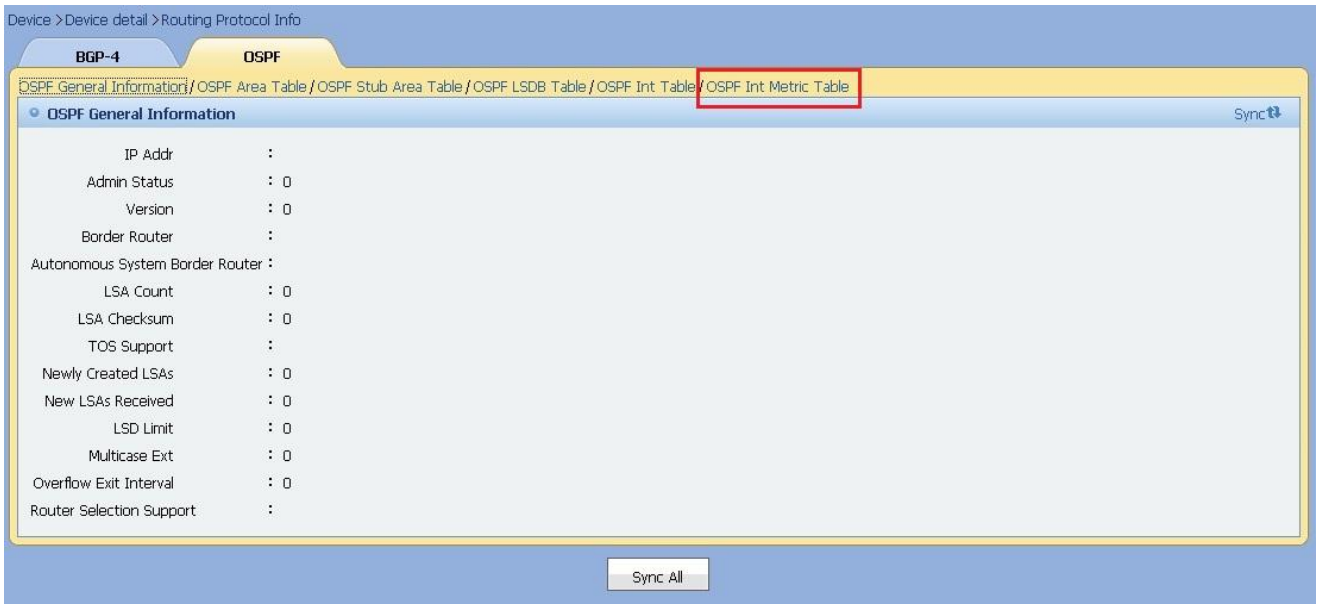


Figure 9.30. Select OSPF Interface Metric Table

Figure 9.31. View Information Of OSPF Interface Metric Table

9.2. Synchronize MIB Information

This module describes MIB synchronization.

- Synchronize All
- Synchronize Information Of BGP Peer Table
- Synchronize Information Of BGP4 Receiving Path Attribute Table
- Synchronize Information Of BGP Receiving Path Attribute Table
- Synchronize OSPF Basic Information
- Synchronize Information Of OSPF Area Table
- Synchronize Information Of OSPF STUB Area Table
- Synchronize Information Of OSPF LSDB Table
- Synchronize Information Of OSPF Interface Table
- Synchronize Information Of OSPF Interface Metric Table

9.2.1. Synchronize All

On routing protocol information page, you can synchronize all routing protocol information.

Operation Steps

Enter routing protocol information page, click **Sync All** link and you will see the prompt indicating the synchronization is in progress. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.32. Enter routing protocol information page

Figure 9.33. Synchronize All

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the information of the following tables needs to be acquired: BGP peer table, BGP4 receiving path attribute table, BGP receiving path attribute table, OSPF basic information, OSPF area table, OSPF STUB area table, OSPF LSDB table, OSPF interface table and OSPF interface metric table.

9.2.2. Synchronize Information Of BGP Peer Table

On routing protocol information page, you can synchronize information of BGP peer table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the prompt indicating synchronization in progress. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.34. Enter routing protocol information page

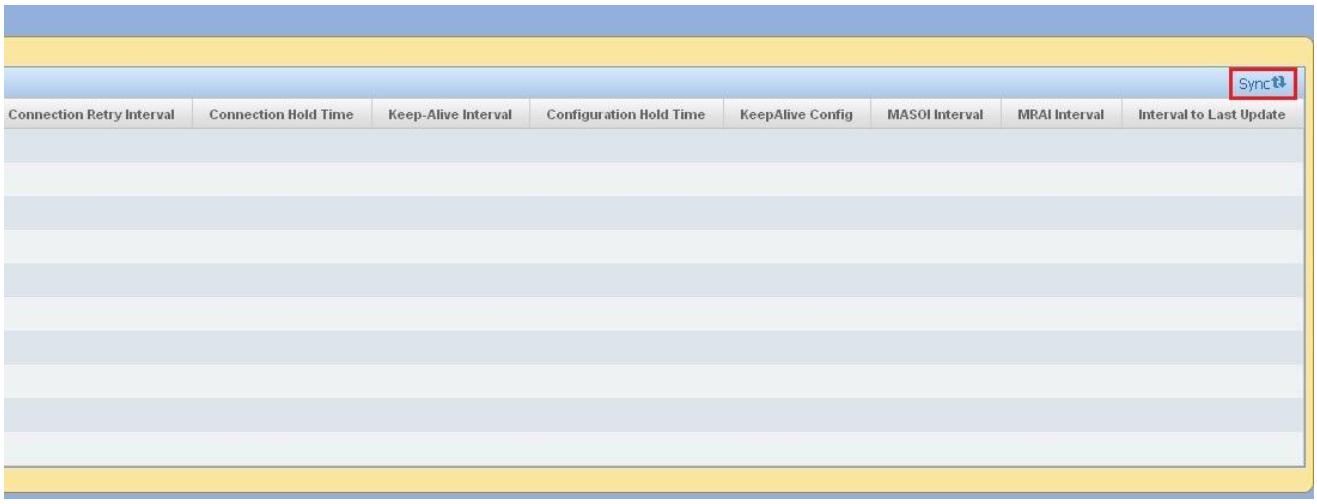


Figure 9.35. Synchronize Information Of BGP Peer Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is normal.
It may take long time for the synchronization process, because the system needs to acquire information of BGP4 peer table.

9.2.3. Synchronize Information Of BGP4 Receiving Path Attribute Table

On routing protocol information page, you can synchronize the information of BGP4 receiving path attribute table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.36. Enter routing protocol information page

Figure 9.37. Select BGP4 Receiving Path Attribute Table

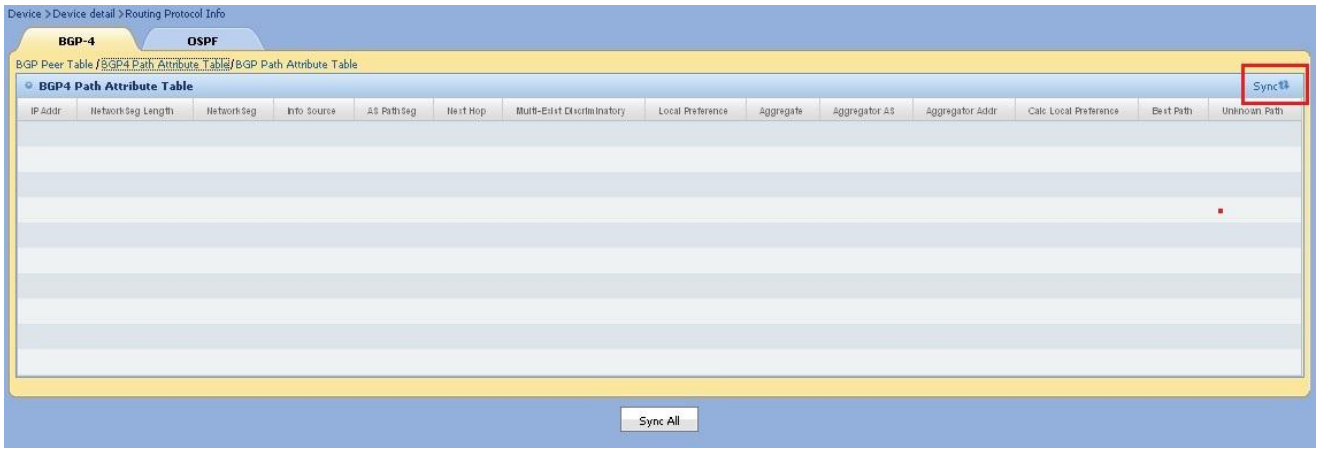


Figure 9.38. Synchronize Information Of BGP4 Receiving Path Attribute Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of BGP4 receiving path attribute table afresh.

9.2.4. Synchronize Information Of BGP Receiving Path Attribute Table

On routing protocol information page, you can synchronize the information of BGP receiving path attribute table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.39. Enter routing protocol information page

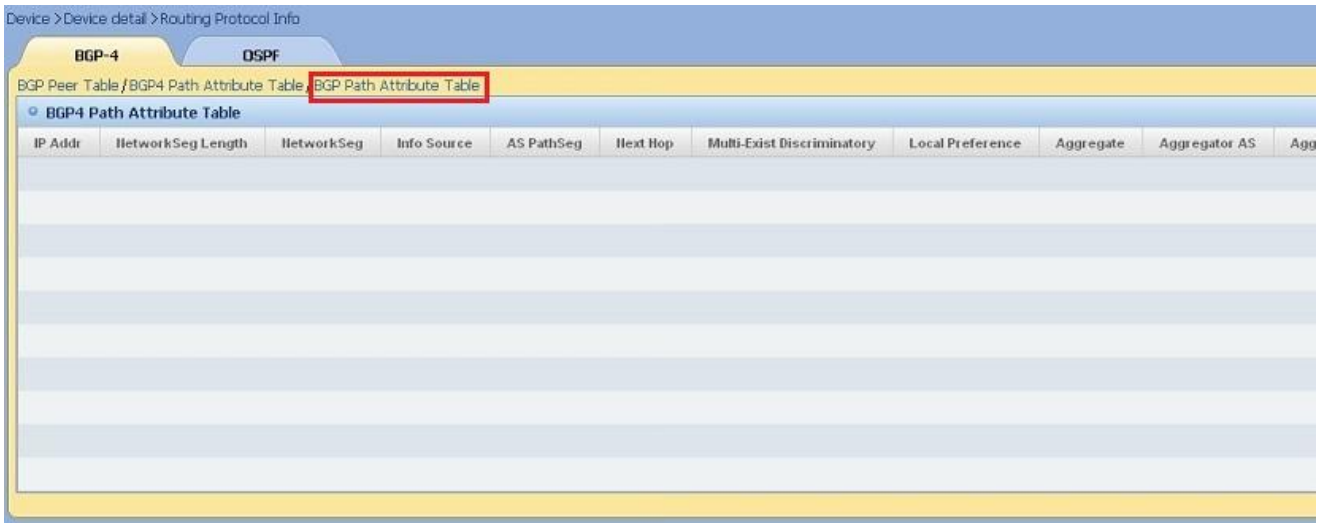


Figure 9.40. Select BGP Receiving Path Attribute Table

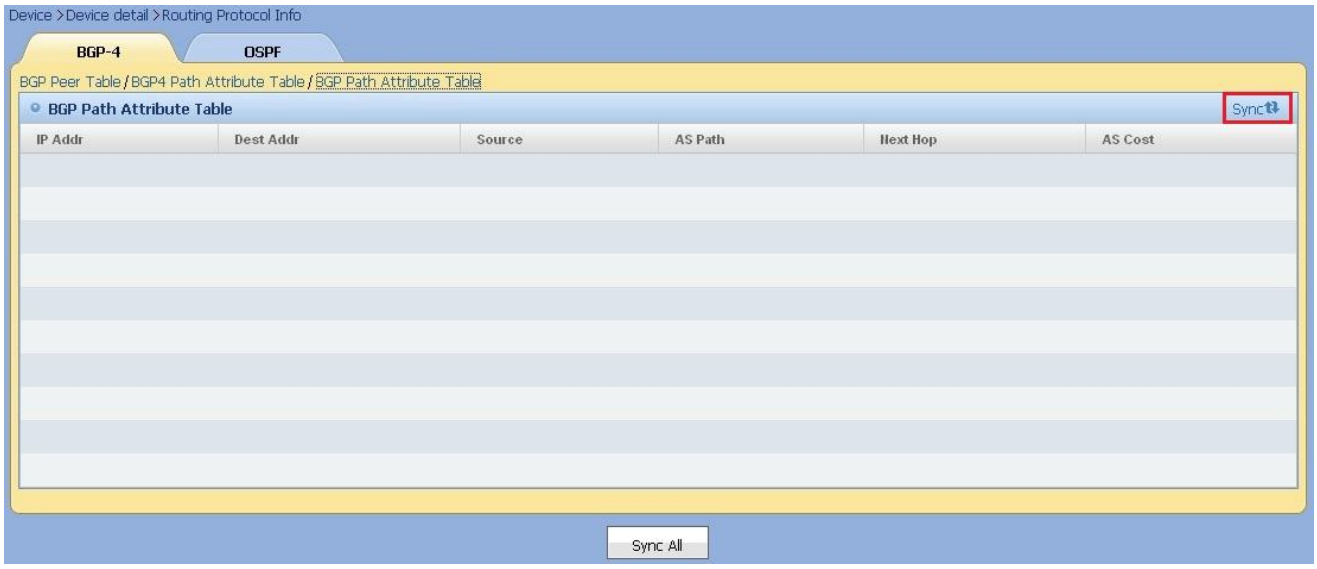


Figure 9.41. Synchronize Information Of BGP Receiving Path Attribute Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of BGP receiving path attribute table afresh.

9.2.5. Synchronize OSPF Basic Information

On the routing protocol information page, you can synchronize basic information of OSPF.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.42. Enter routing protocol information page

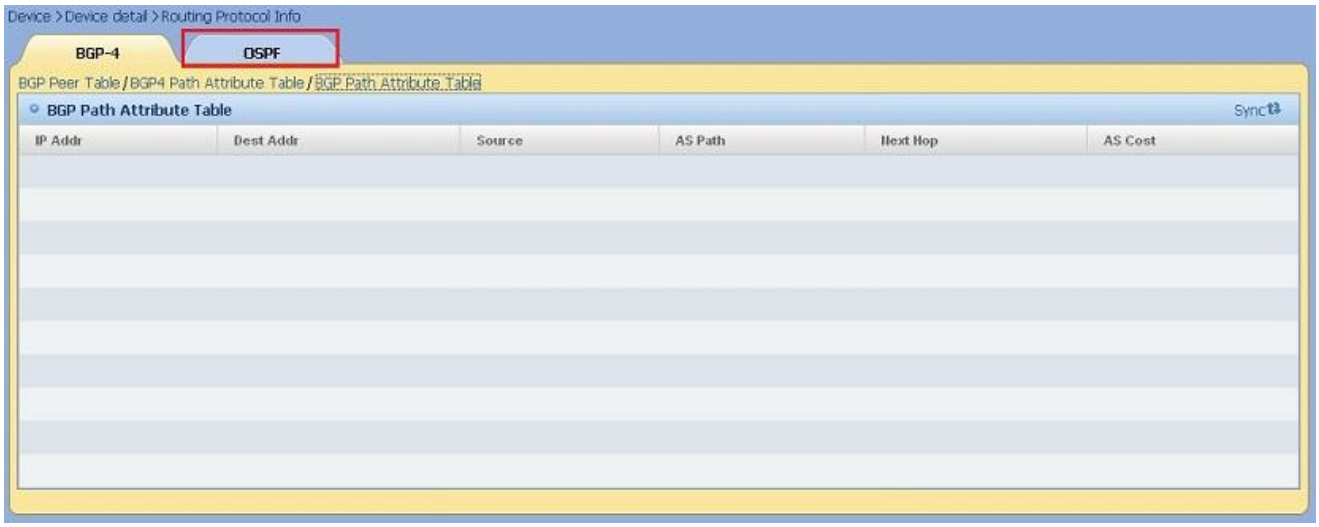


Figure 9.43. Select OSPF

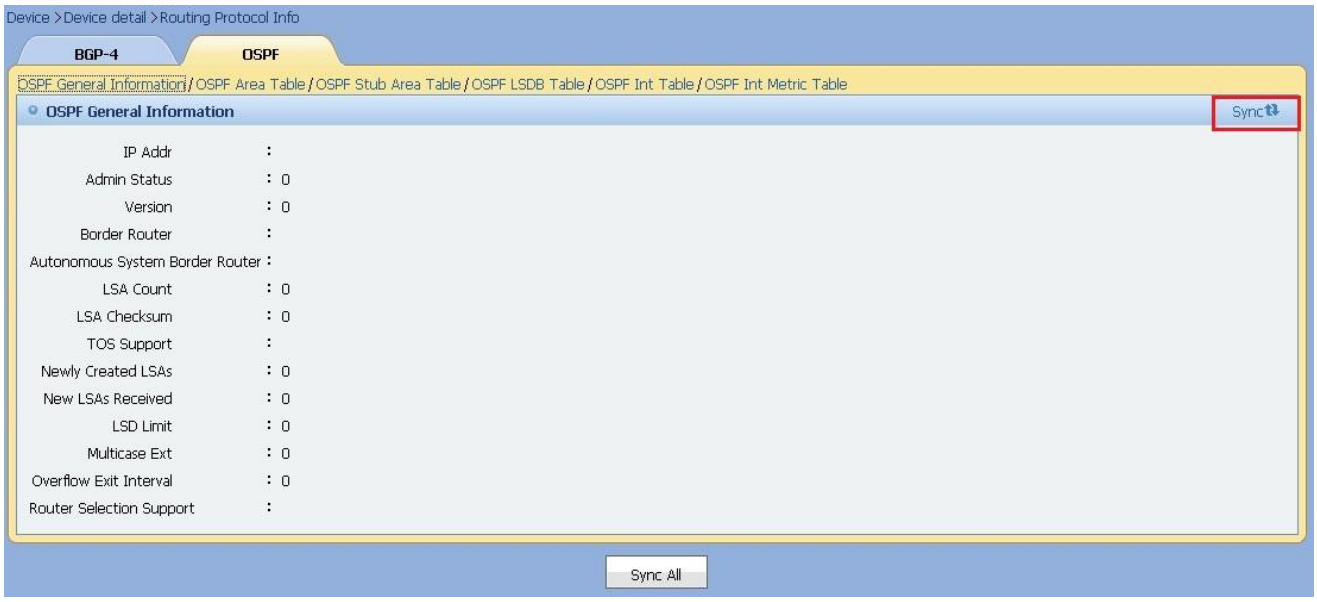


Figure 9.44. Synchronize Basic Information of OSPF

Note

The correct MIB information can be synchronized only when SNMP connectivity is normal.
It may take long time for the synchronization process, because the system needs to acquire basic information of OSPF information.

9.2.6. Synchronize Information Of OSPF Area Table

On routing protocol information page, you can synchronize the information of OSPF area table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.45. Enter routing protocol information page

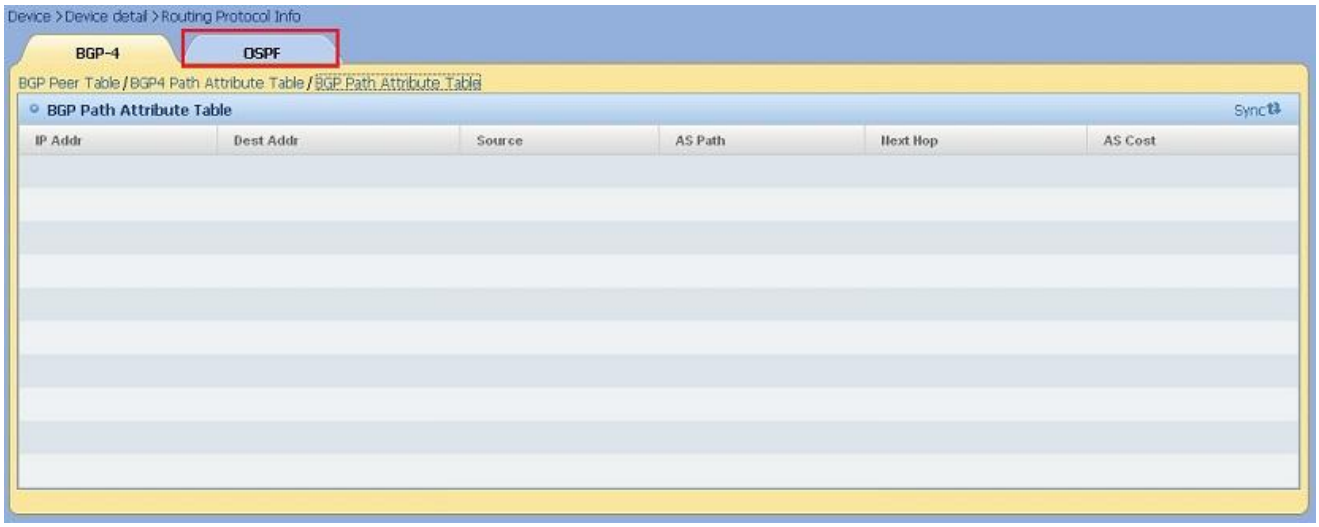


Figure 9.46. Select OSPF

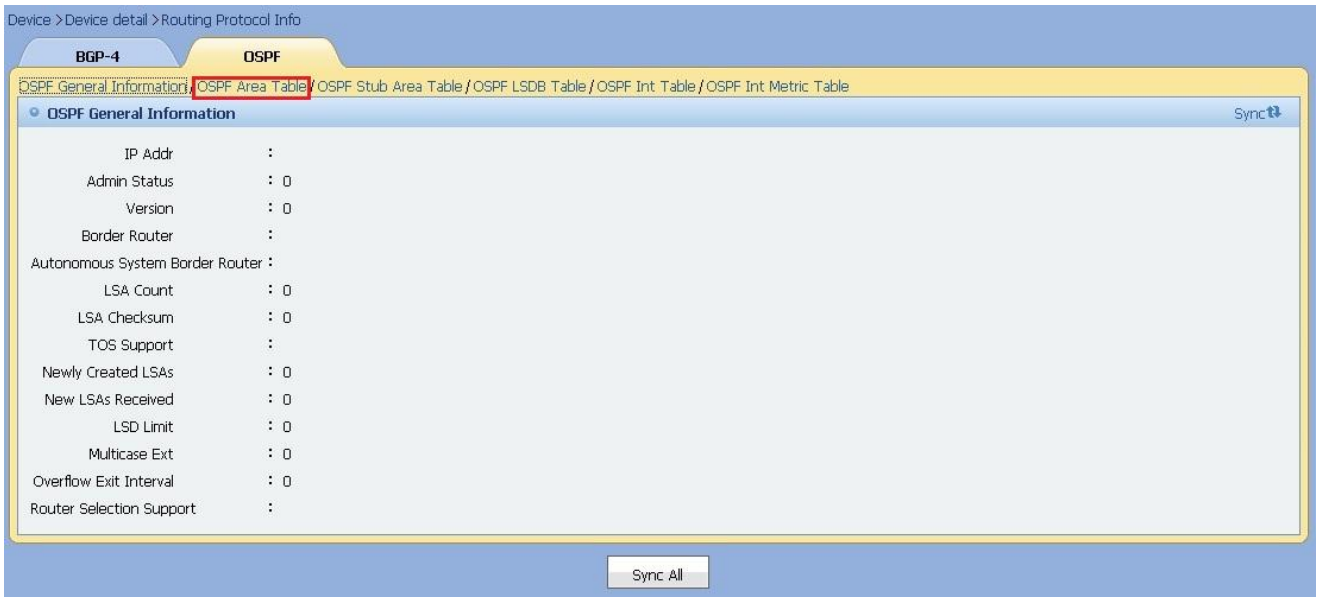


Figure 9.47. Select OSPF Area Table

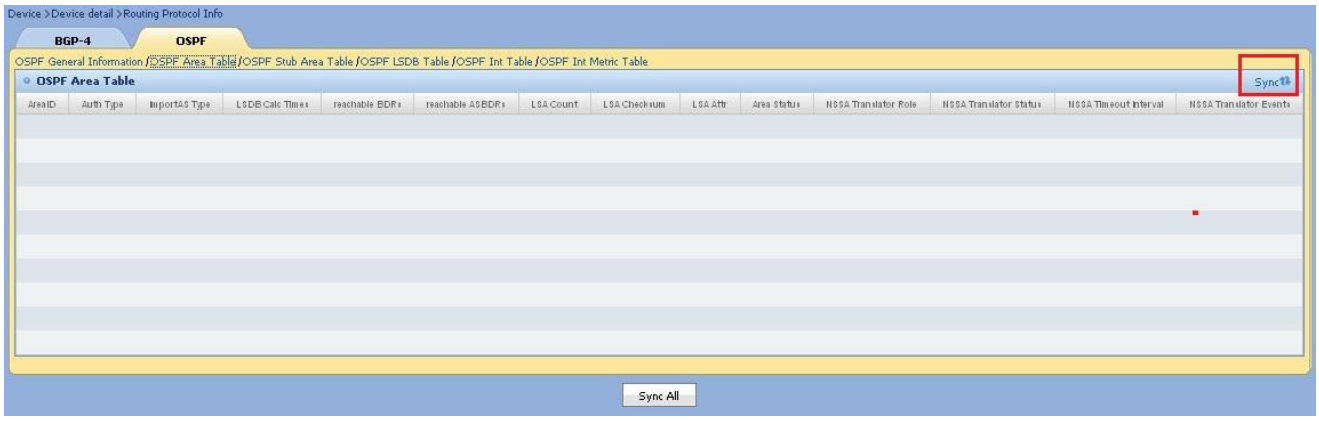


Figure 9.48. Synchronize Information Of OSPF Area Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of OSPF area table afresh.

9.2.7. Synchronize Information Of OSPF STUB Area Table

On routing protocol information page, you can synchronize the information of OSPF STUB area table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.49. Enter routing protocol information page

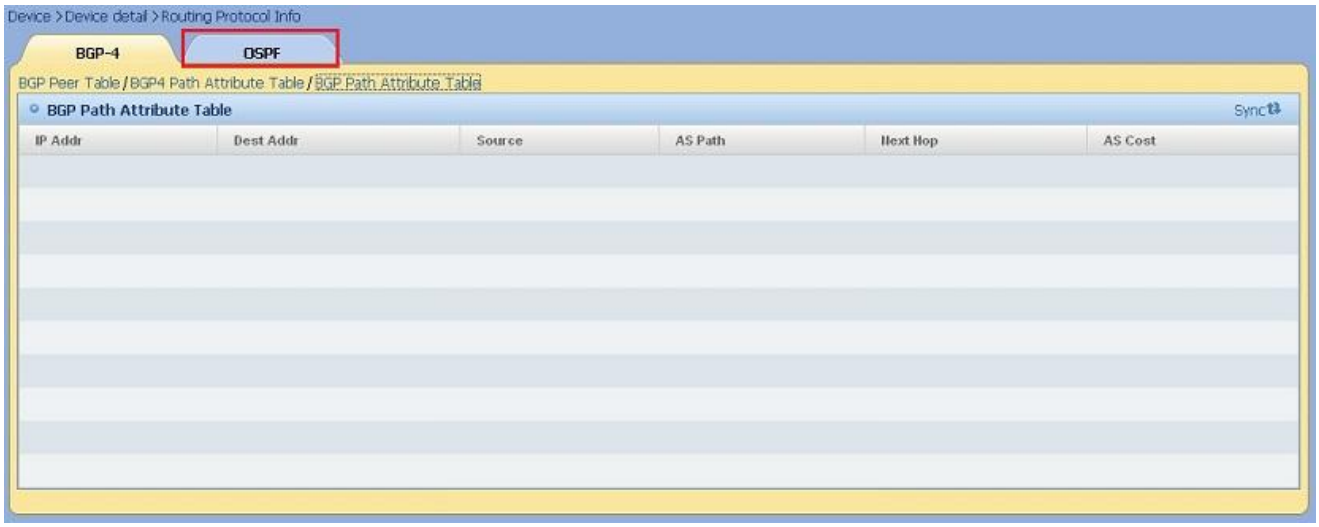


Figure 9.50. Select OSPF

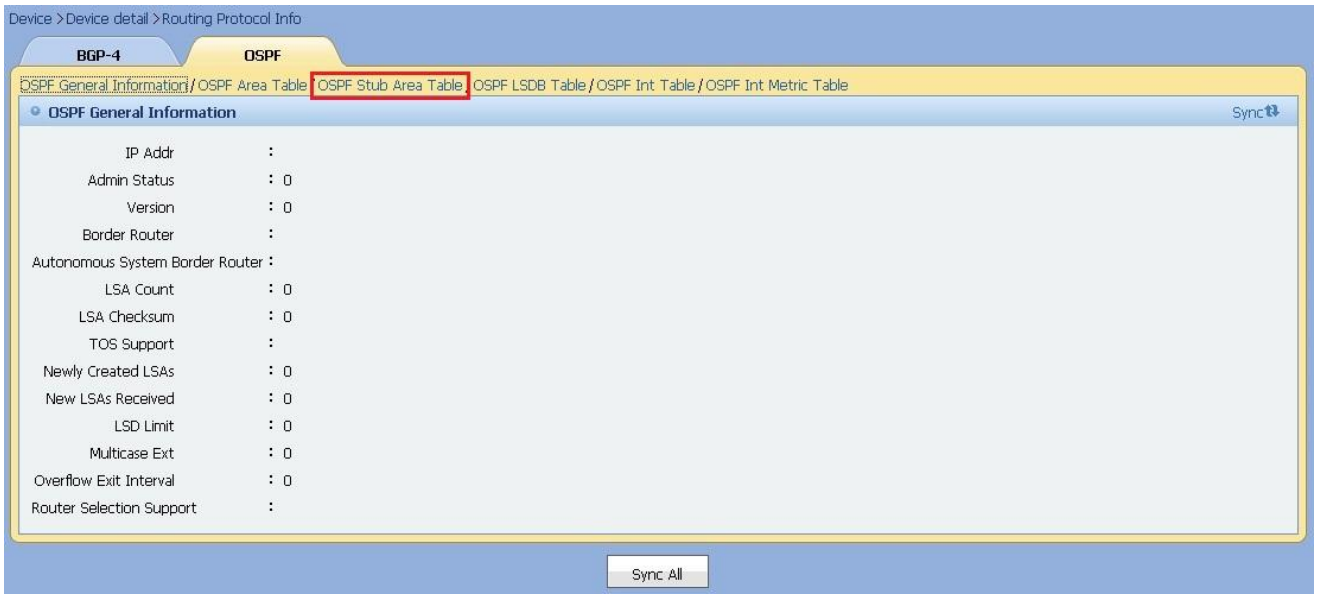


Figure 9.51. Select OSPF STUB Area Table

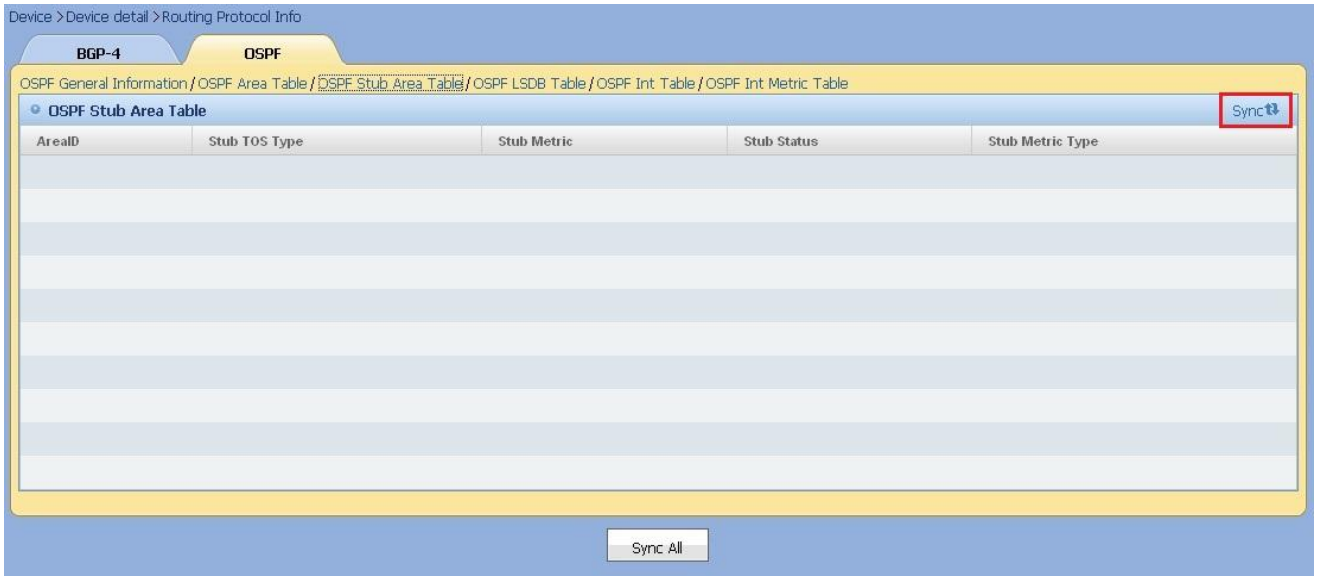


Figure 9.52. Synchronize Information Of OSPF STUB Area Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of OSPF STUB area table afresh.

9.2.8. Synchronize Information Of OSPF LSDB Table

On routing protocol information page, you can synchronize the information of OSPF LSDB table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.53. Enter routing protocol information page

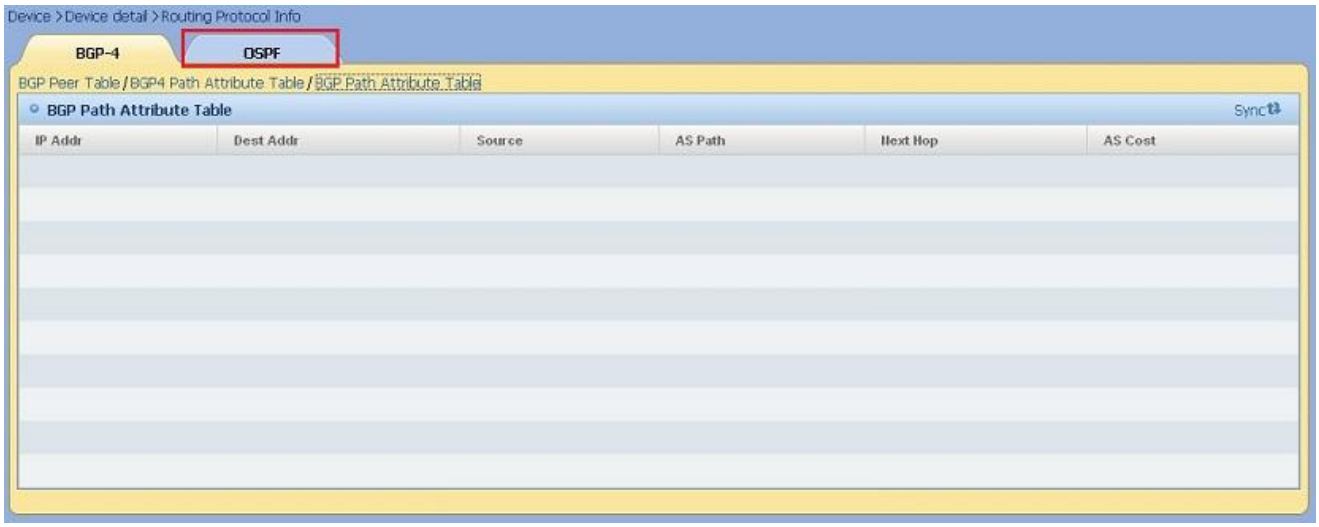


Figure 9.54. Select OSPF

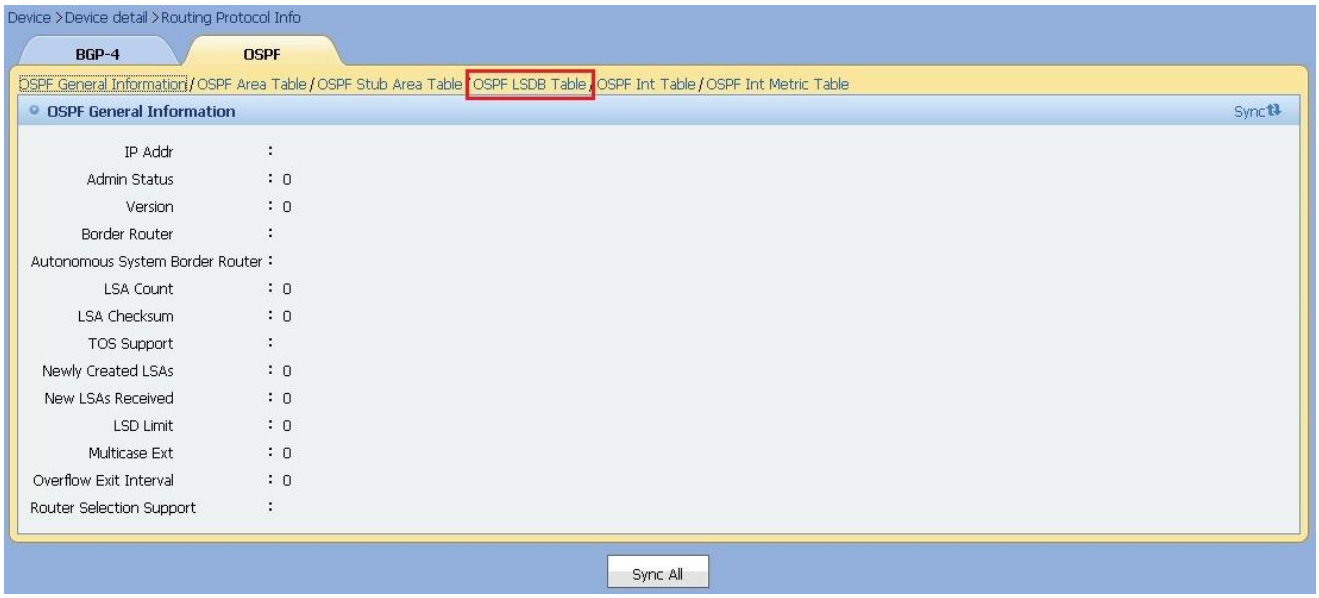


Figure 9.55. Select OSPF LSDB Table

Figure 9.56. Synchronize Information Of OSPF LSDB Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of OSPF LSDB table afresh.

9.2.9. Synchronize Information Of OSPF Interface Table

On routing protocol information page, you can synchronize the information of OSPF interface table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.57. Enter routing protocol information page

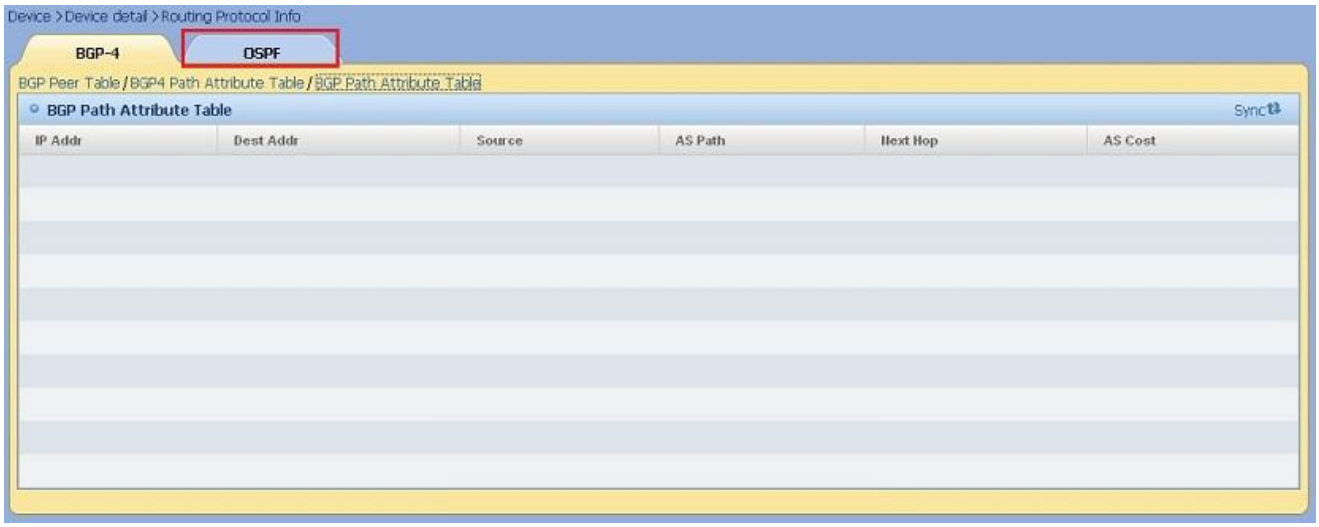


Figure 9.58. Select OSPF

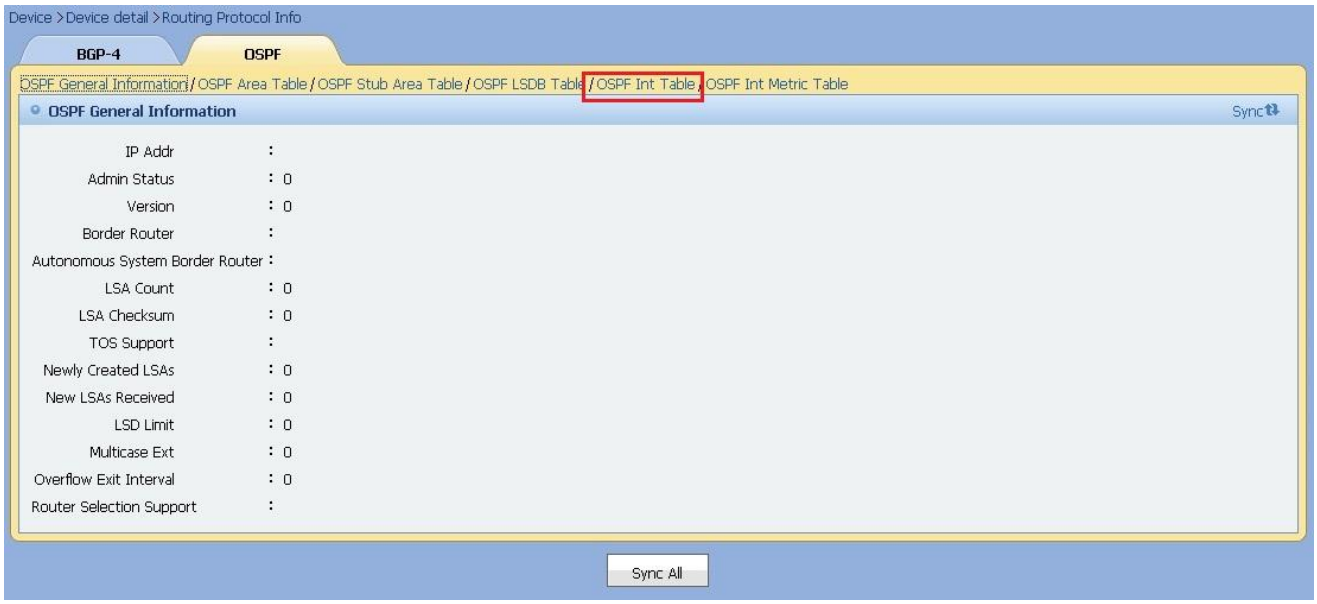


Figure 9.59. Select OSPF Interface Table

Figure 9.60. Synchronize Information Of OSPF Interface Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of OSPF interface table afresh.

9.2.10. Synchronize Information Of OSPF Interface Metric Table

On routing protocol information page, you can synchronize the information of OSPF interface metric table.

Operation Steps

Enter routing protocol information page, click **Sync** link and you will see the synchronization progress prompt. After the synchronization is finished, the device detail page will be refreshed. As shown below:

Figure 9.61. Enter routing protocol information page

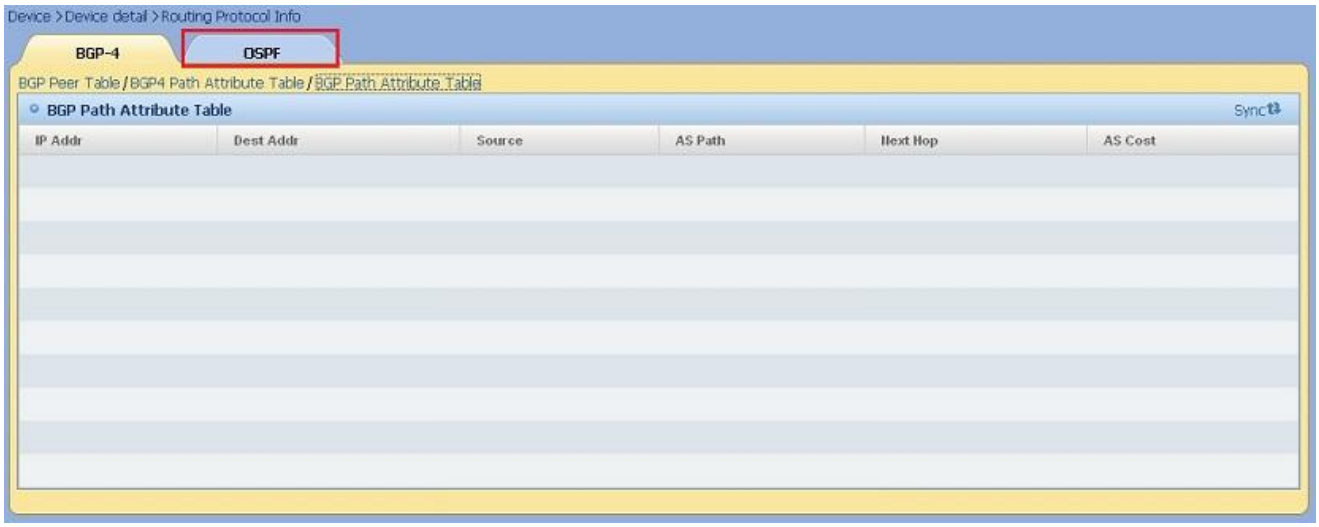


Figure 9.62. Select OSPF

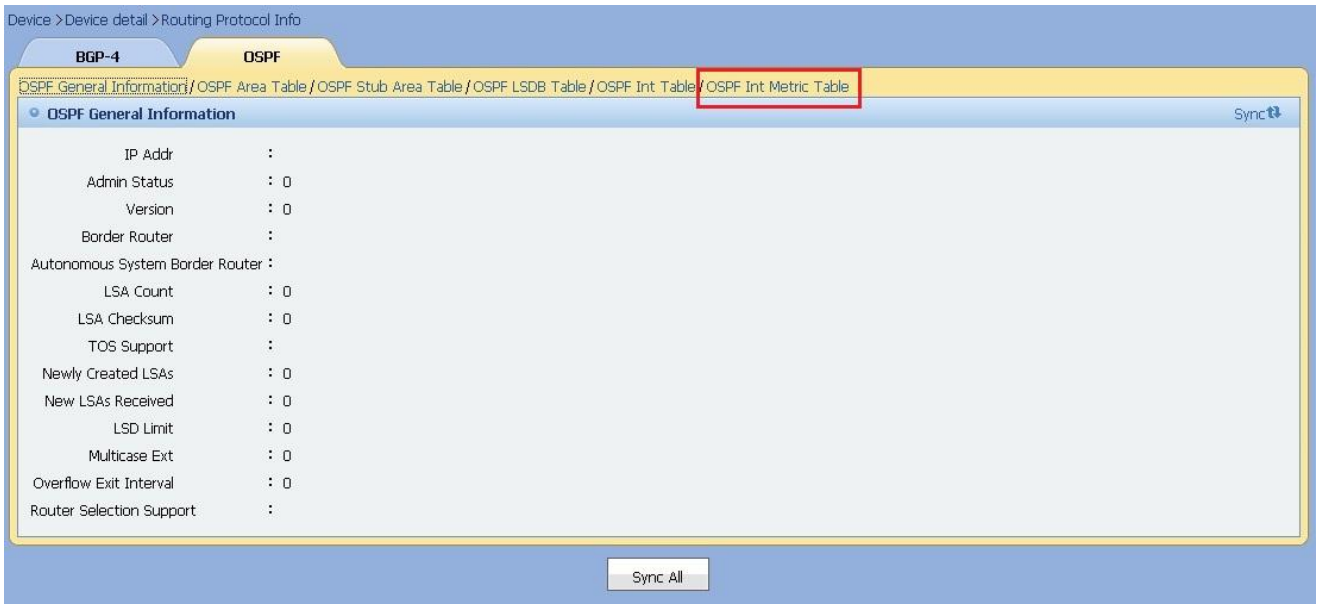


Figure 9.63. Select OSPF Interface Metric Table

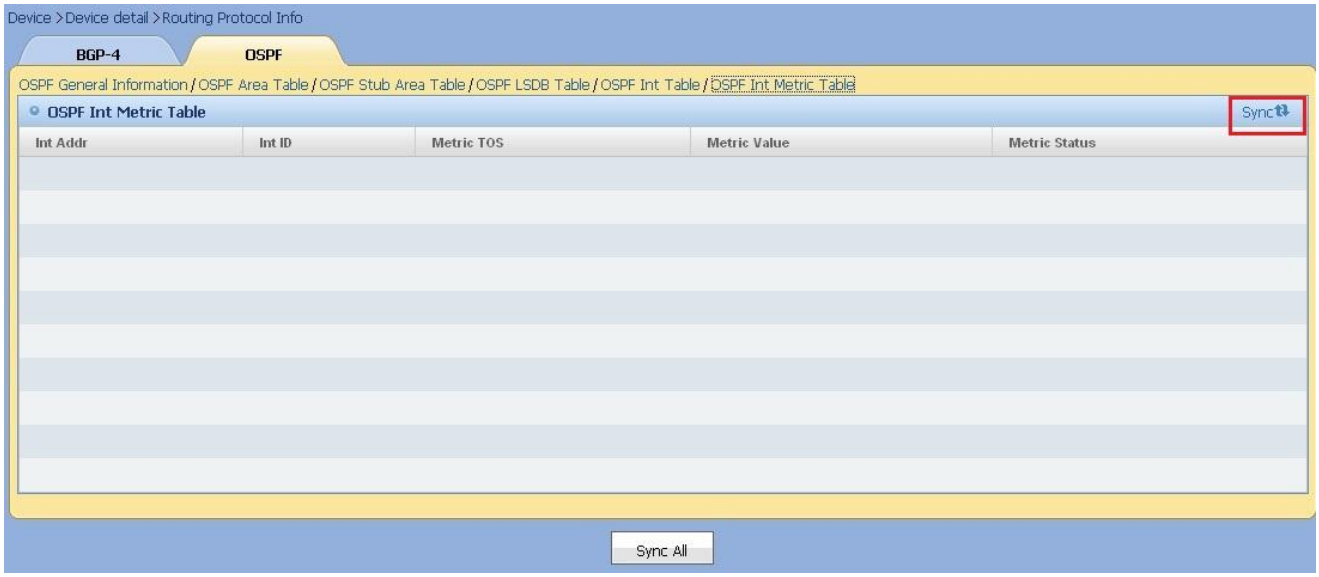


Figure 9.64. Synchronize Information Of OSPF Interface Metric Table

Note

The correct MIB information can be synchronized only when SNMP connectivity is OK.
It may take long time for the synchronization process, because the system needs to acquire information of OSPF interface metric table afresh.

Chapter 10 QoS Management

QoS management module provides management of QoS device and device interface. These functionalities are shown through QoS device management page and partially system management page.

Function List

- QoS Classification Management
- QoS Policy Management
- QoS Device Management
- QoS Deployment Management

10.1. QoS Classification Management

The QoS classification management is used for configuring QoS classification, which includes associated ACL.

- Add QoS Classification
- Associate QoS Classification with ACL
- Delete QoS Classification
- Search QoS Classification
- QoS Classification Detail
- Modify QoS Classification
- Modify Match Mode Of QoS Classification
- Redeploy QoS Classification

10.1.1. Add QoS Classification

QoS classification must be added into the system before it can be managed by the system.

Operation Steps

1) Enter QoS classification management page, click **Add** icon to enter QoS classification addition page. As shown below:

Figure 10.1. Enter Classification Addition Page

Input related information on **Add QoS Classification** page, then click **Add** button. As shown below:

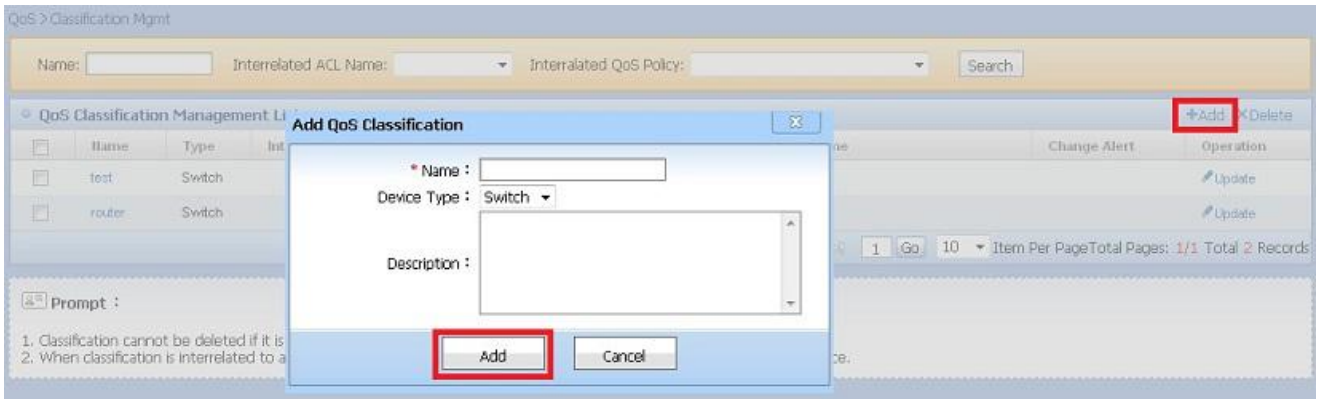


Figure 10.2. Add Classification Page

Click **Cancel** button on **Add QoS Classification** page, the system will ignore the changes of classification and return to **QoS Classification Management** page.

Note

The classification name cannot be null, and no Chinese character or full-length character is allowed.
If **Router** is selected as applicative type, the match type will also be required to be added.

10.1.2. Associate QoS Classification with ACL

An ACL that is associated with QoS classification must be added into the system before it can be managed by the system.

Operation Steps

1) Enter QoS classification management page, click **Name** link to enter **QoS Classification Detail** page. As shown below:

Figure 10.3. Enter **QoS Classification Detail** Page

On **QoS Classification Detail** page, click **Add** button on interrelated ACL list. The following will be shown:

Figure 10.4. Enter the **Add interrelated ACL** Page

The ACL list is shown on Add interrelated ACL page. If the classification is applicable to a switch, only one ACL can be selected. If the classification is applicable to a router, you can select multiple ACLs. As shown below:

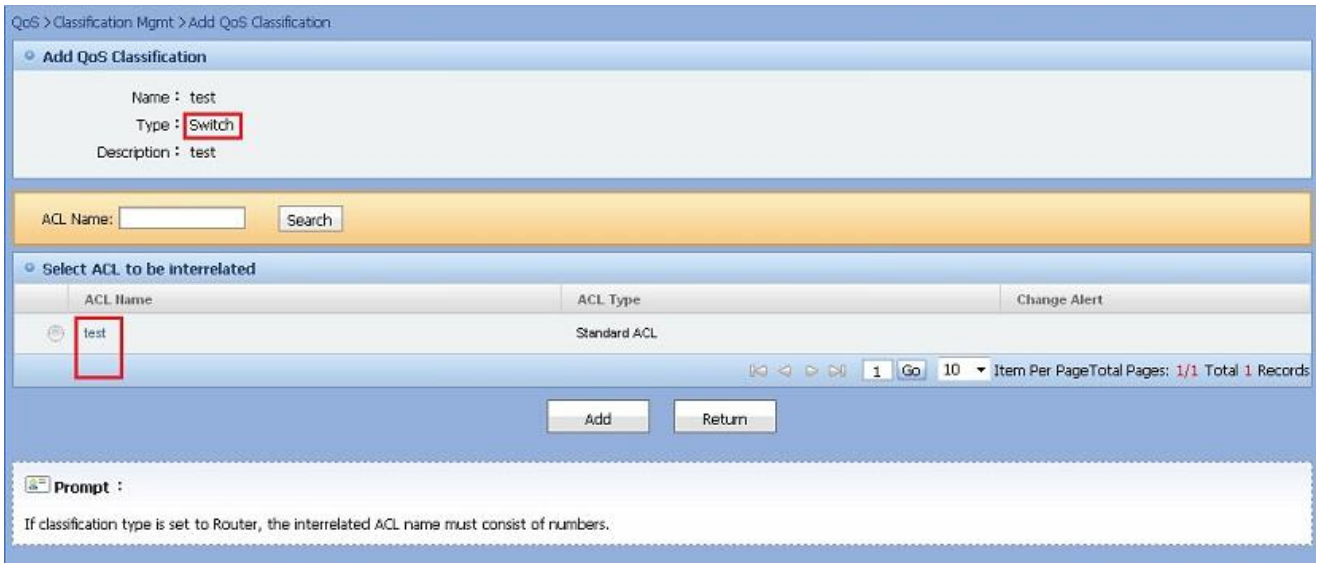


Figure10.5.Add interrelated ACL

Select the ACL to be associated and click **Add** button, the ACL will be associated and the system will return to **QoS Classification Management** page.
Click **Return** button, the system does not save any changes and return to **QoS Classification Detail** page.

Note

If the classification is applicable to a switch, only one ACL can be selected. If the classification is applicable to a router, you can select multiple ACLs.
If the classification is applicable to a router, the associated ACL name must consist of numbers only, or the distribution will fail.
If the classification has associated device, the **Inconsistent Configuration** warning will be shown when you add an ACL.

10.1.3. Delete QoS Classification

On **QoS Classification Management** page, the classification can be deleted in batches.

Operation Steps

Enter **QoS Classification Management** page, select the classifications on classification list then click **Delete** button, the system will prompt for confirmation, click **Confirm** for the deletion. As shown below:

Figure 10.6. Enter **Classification Deletion** Page

Note

The classification cannot be deleted when being associated with a policy.
If the classification is associated with a device, deletion of the classification will require deployment of a plan.

10.1.4. Search QoS Classification

On **QoS Classification Management** page, you can search classification by classification name, interrelated ACL or interrelated QoS policy.

Operation Steps

Enter **QoS Classification Management** page, input classification name, interrelated ACL or interrelated QoS policy, then click **Search** button, the eligible classifications will be listed. As shown below:

Figure 10.7. **QoS Classification Management** Page

Note

If the three condition fields are all left empty, all the classifications in the system will be listed.

10.1.5. QoS Classification Detail

QoS classification detail page will show the following: QoS classification detail, interrelated ACL and interrelated QoS policy.

Operation Steps

1) Enter QoS classification detail page, click **Name** link to enter **QoS Classification Detail** page. As shown below:

Figure 10.8. Enter **QoS Classification Detail** Page

On **QoS Classification Detail** page, the classification detail, interrelated ACL and interrelated QoS policy will be listed. As shown below:

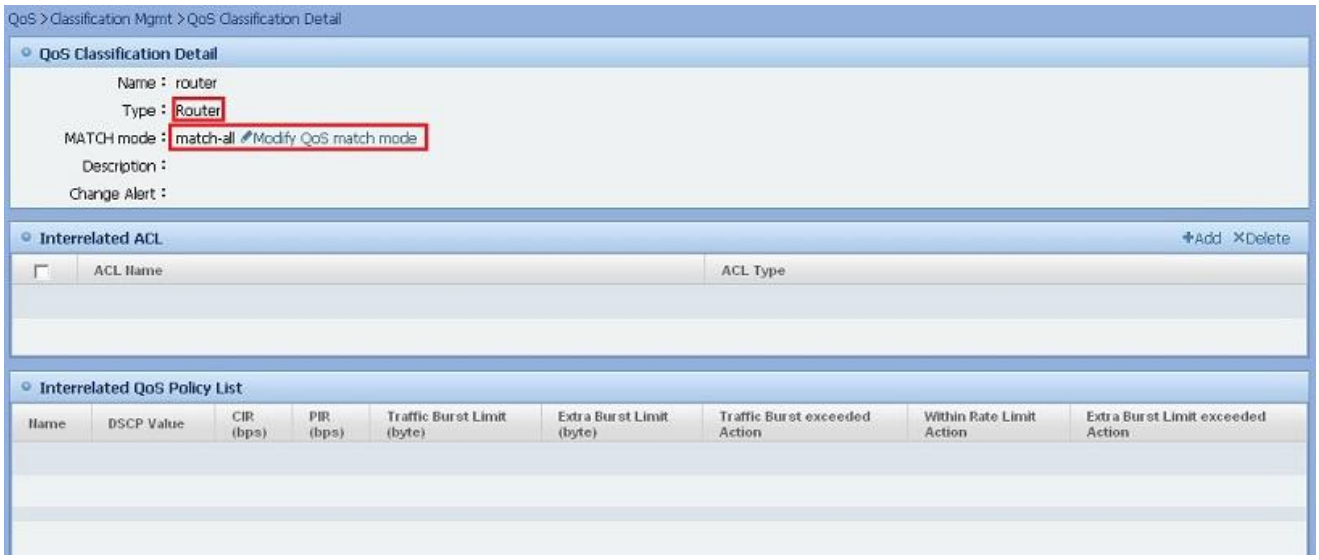


Figure 10.9. **QoS Classification Detail** Page

Note

If the classification is applicable to a router, it has match type and can have multiple interrelated ACL. If the classification is applicable to a switch, there is no match type and can have only one interrelated ACL.

10.1.6. Modify QoS Classification

After the QoS classification is modified, it will be saved to the database.

Operation Steps

1) Enter QoS classification management page, click **Update** button to enter **Modify QoS Classification** page. As shown below:

Figure 10.10. Enter **Classification Modification** Page

On **Modify QoS Classification** page, please fill in the descriptions and click **Update** button. As shown below:

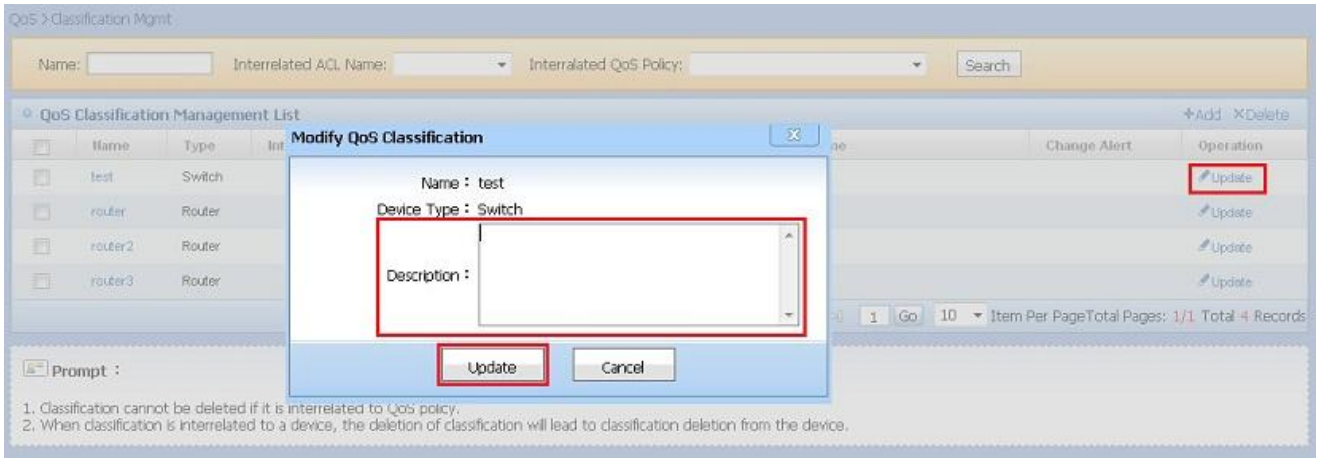


Figure 10.11. **Classification Modification** Page

On **Modify QoS Classification** page, click **Cancel** button to ignore any changes and the system will return to **QoS Classification Management** page.

Note No inconsistent data will be generated for classification modification. Only the description can be changed.

10.1.7. Modify Match Mode Of QoS Classification

The Match Mode of QoS classification must be added into the system before it can be managed by the system.

Operation Step

1) Enter QoS classification management page, click **Name** link to enter **QoS Classification Detail** page. As shown below:

Figure 10.12. Enter QoS Classification Detail Page

Click **Modify QoS match mode** button on **QoS Classification Detail** page to modify the Match Mode. If the classification application type is switch, there will be no Match Mode. As shown below:

Figure 10.13. **Classification Detail** Page

The Match Mode modification page will be popped up. As shown below:

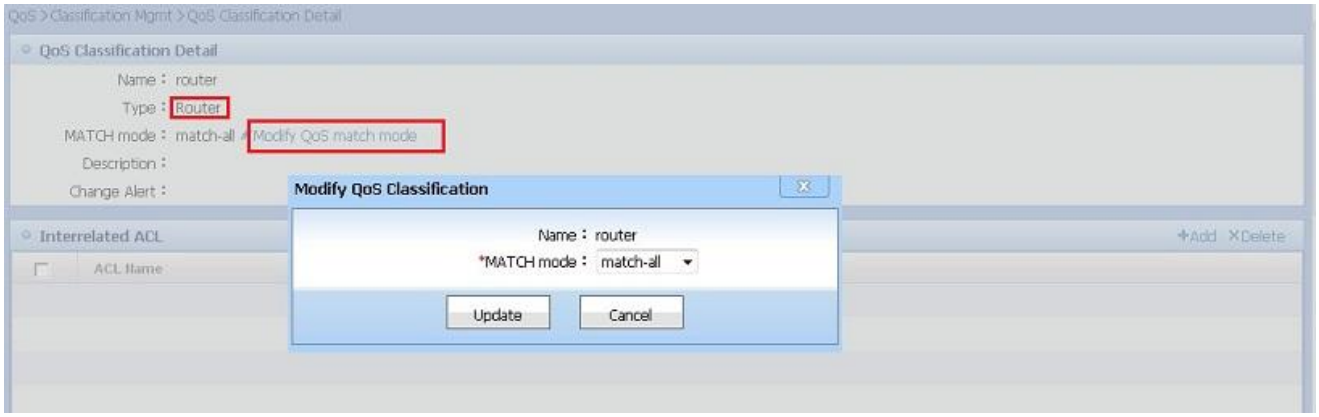


Figure 10.14. Modify Match Mode Page

After selecting Match Mode, please click **Update** button to save the modification into the system, and the system will return to **QoS Classification Detail** page.

Click the **X** button on the upright corner of the pop-up page, the modification will be ignored and the system will return to **QoS Classification Detail** page.

Note

The modification of Match Mode will probably generate **Inconsistent Changes** warning.
If the classification is applicable to a router, the Match Mode can be modified. If the classification is applicable to a switch, no Match Mode is available.

10.1.8. Redeploy QoS Classification

If the QoS classification is changed, you need to redeploy it.

Operation Steps

1) Enter QoS classification management page, if the value of **Change Alert** column shows inconsistent change, click the **Name l**ink to enter **QoS Classification Detail** page. As shown below:

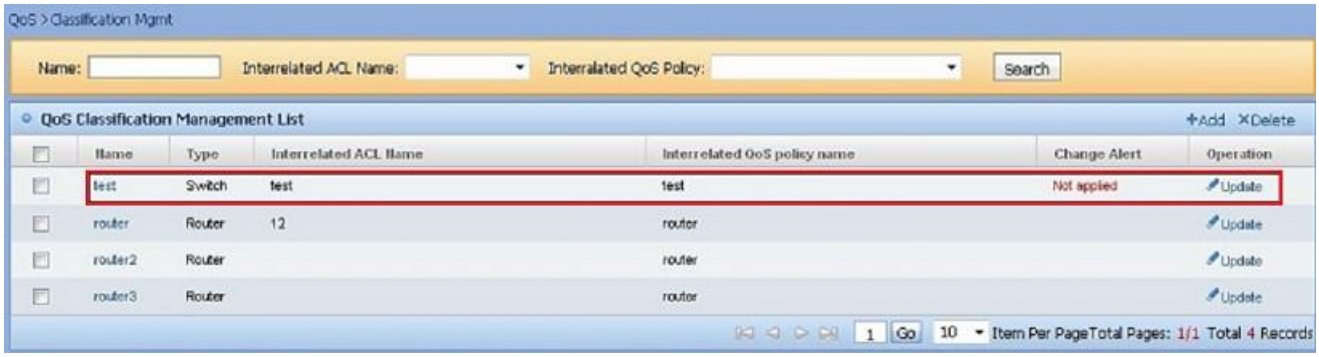


Figure 10.15. Enter **QoS Classification Detail** Page

If the **Change Alert** value on QoS classification detail page shows that the change is not applied, please click **Redeploy** button. As shown below:

Figure 10.16. **QoS Classification Detail** Page

Click **Redeploy** button, the system will prompt a message like “This will overwrite classification on all the devices”, click **Confirm** for redeployment confirmation. As shown below:

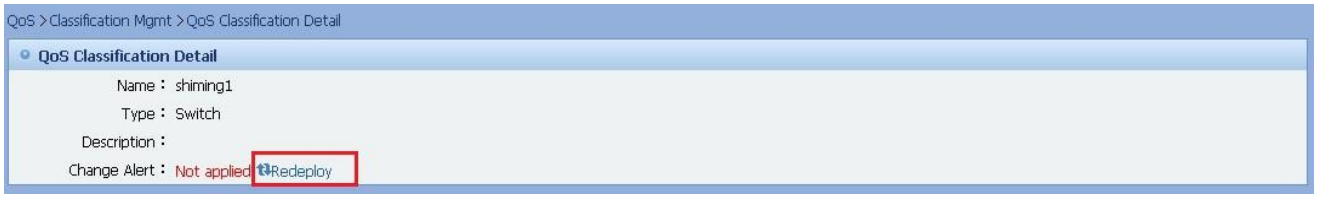


Figure 10.17. **QoS Classification Detail** Page

If you don’t want to deploy it to all the devices, you can deploy it to a single device using the interrelated QoS device list on the bottom. As shown below:

Figure 10.18. **QoS Classification Detail** Page

Note

Clicking the **Redeploy** button on the classification list will overwrite the classification on all the devices. If you want to deploy it to a single device, please use the interrelated QoS device list on the bottom.
Clicking the **Redeploy** button on the classification list will create a deployment plan, but you can only check the plan creation on plan management page. If you click the **Redeploy** button on the device, the distribution will be effective immediately without any plan created.

10.2. QoS Policy Management

QoS policy management provides management (add, delete, modify, view, and deploy) of QoS policy information, which includes management of classification association.

Function List

- Add QoS Policy
- Delete QoS Policy
- Modify QoS Policy
- Search QoS Policy
- View QoS Policy Detail
- Interrelated QoS Classification Management
- Management of Policy-Deployed Device
- Redeploy QoS Policy With Changes

10.2.1. Add QoS Policy

QoS policy must be added into the system before it can be managed by the system.

Operation Steps

1) Enter **QoS Policy Management** page, click **Add** button to enter **Add QoS Policy** page. As shown below:

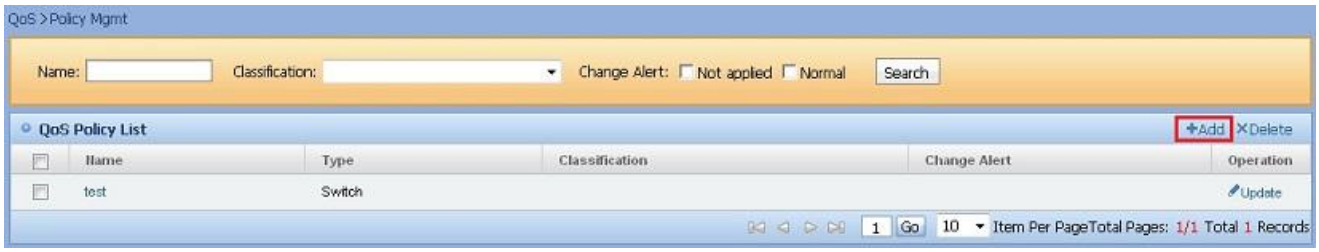


Figure 10.19. Enter Add QoS Policy

Fill QoS policy related information on **Add QoS Policy** page, then click **Add** button. As shown below:

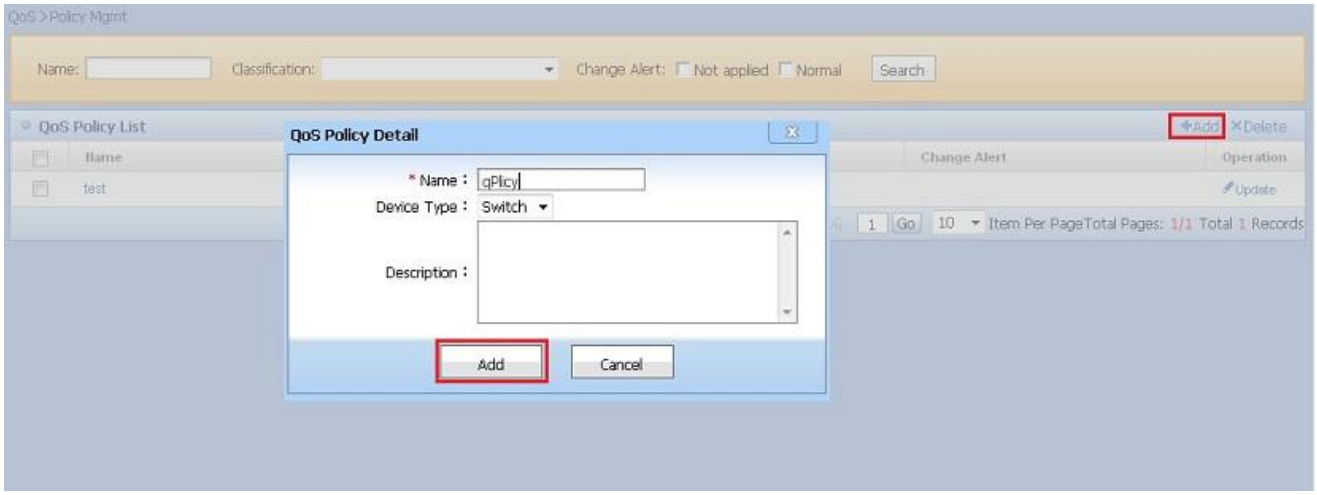


Figure 10.20. Add QoS Policy

Click **Cancel** button on **Add QoS Policy** page, the system will ignore any changes and return to **QoS Policy Management** page.

Note

Applied device type: Switch, and Router.
QoS policy name must be unique.
No Chinese character or full-length character is allowed in a QoS policy name, it can only consist of number, letter or underline. The QoS policy name can only be digits if it starts with a digit and cannot comprise any other character.

10.2.2. Delete QoS Policy

On **QoS Policy Management** page, you can delete QoS policy in batches.

Operation Steps

Enter **QoS Policy Management** page, select QoS policies on QoS policy list and click **Delete** button, the system will prompt for your confirmation. Click **Confirm** to delete selected QoS policies. As shown below:

Figure 10.21. Delete QoS Policy

Figure 10.22. Delete QoS Policy interrelated with Device

Note

When deleting QoS policy, if the QoS policy is interrelated with device, the system will automatically generate deployment plan and deploy it immediately.
If the background process is not running, the deployment plan won't be generated and the QoS policy cannot be deleted.

10.2.3. Modify QoS Policy

You can modify the description of QoS policy in the system.

Operation Steps

1) Enter QoS policy management page, click **Update** icon to enter **Modify QoS Policy** page. As shown below:

Figure 10.23. Enter Modify QoS Policy

On **Modify QoS Policy** page, modify the description of QoS policy and click **Update** button. As shown below:

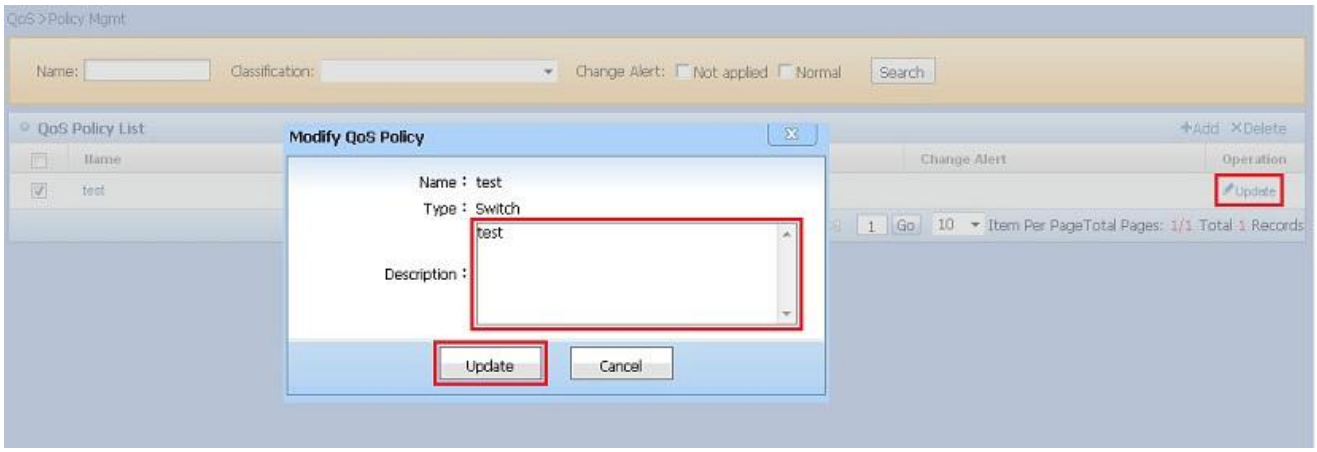


Figure 10.24. Modify QoS Policy

Click **Cancel** button on **Modify QoS Policy** page, the system will ignore any changes and return to **QoS Policy Management** page.

Note

Only the description can be modified, and the modification of description cannot change the change alert identification of QoS policy.

10.2.4. Search QoS Policy

On **QoS Policy Management** page, you can input QoS policy name, select interrelated QoS classification or change alert to search managed QoS policy.

Operation Steps

Enter **QoS Policy Management** page, input QoS policy name or select interrelated QoS classification or change alert, then click **Search** button, the system will list all matched QoS policy. As shown below:

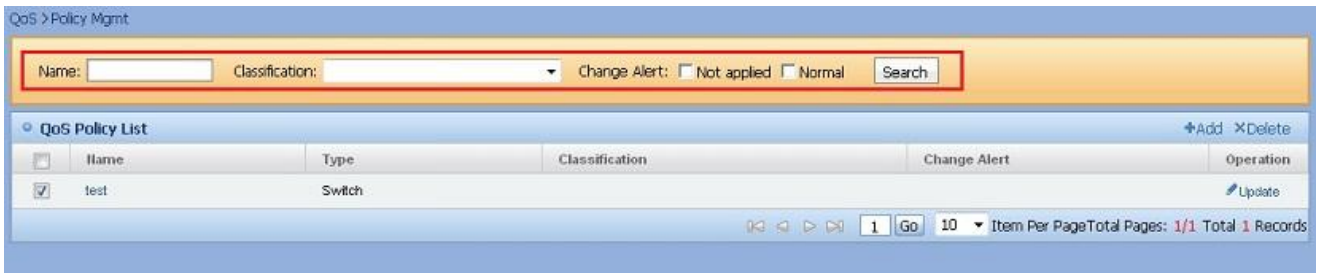


Figure 10.25. Search QoS Policy

10.2.5. View QoS Policy Detail

Enter **QoS Policy Detail** page, you can view QoS policy detail, QoS classifications interrelated to the QoS policy and QoS devices deployed with QoS policy.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

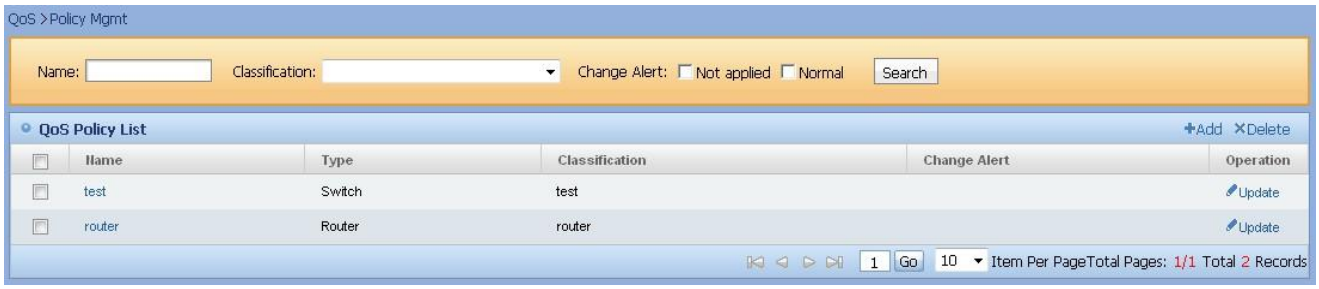


Figure 10.26. View QoS Policy

On **QoS Policy Detail** page, QoS policy detail, QoS classifications interrelated to the QoS policy and QoS devices deployed with QoS policy will be displayed. As shown below:

Figure 10.27. QoS Policy Detail

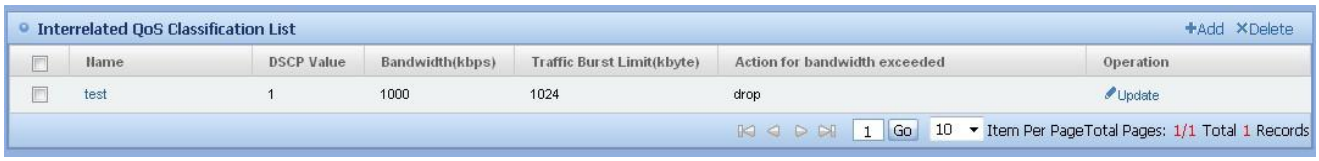


Figure 10.28. QoS Classifications Interrelated To QoS Policy

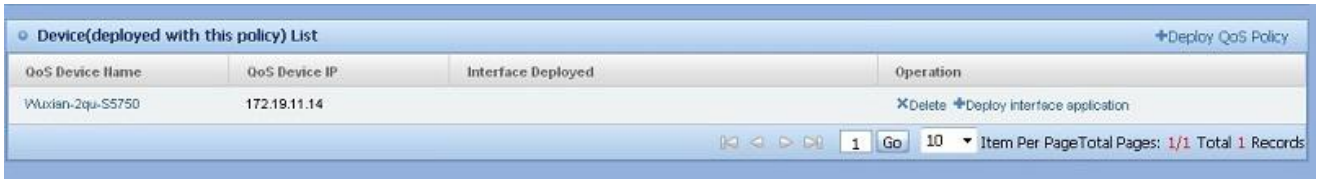


Figure 10.29. QoS Devices Deployed With QoS Policy

10.2.6. Interrelated QoS Classification Management

This module includes adding, deleting, modifying, viewing and adjusting the order of QoS classification of a QoS policy.

Function List

- Add Interrelated QoS Classification
- Modify Interrelated QoS Classification
- Delete Interrelated QoS Classification
- Order Adjustment for Interrelated QoS Classification

10.2.6.1. Add Interrelated QoS Classification

The Interrelated QoS classification can be applied for two types: Switch, Router. You can add the two types with this module.

- Add Interrelated QoS Classification For Type **Switch**
- Add Interrelated QoS Classification For Type **Router**

10.2.6.1.1. Add Interrelated QoS Classification For Type Switch

You can add interrelated QoS classification for type **Switch** using QoS policy management.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list for **Type** value **Switch** to enter **QoS Policy Detail** page. On **Interrelated QoS Classification List**, click **Add** button to enter **Add Interrelated QoS Classification** page. As shown below:

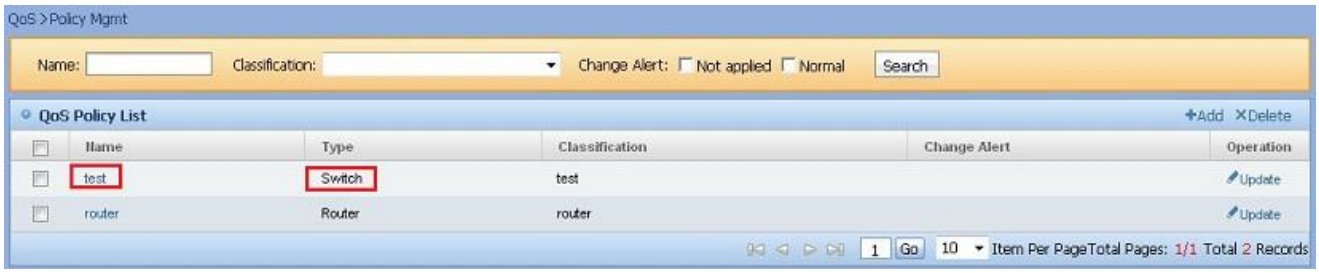


Figure 10.30. Enter **QoS Policy Detail** Page

Figure 10.31. Enter **Add Interrelated QoS Classification** Page

On **Add Interrelated QoS Classification** page, select the QoS classification you want to add interrelation, then click **Add** button. As shown below:

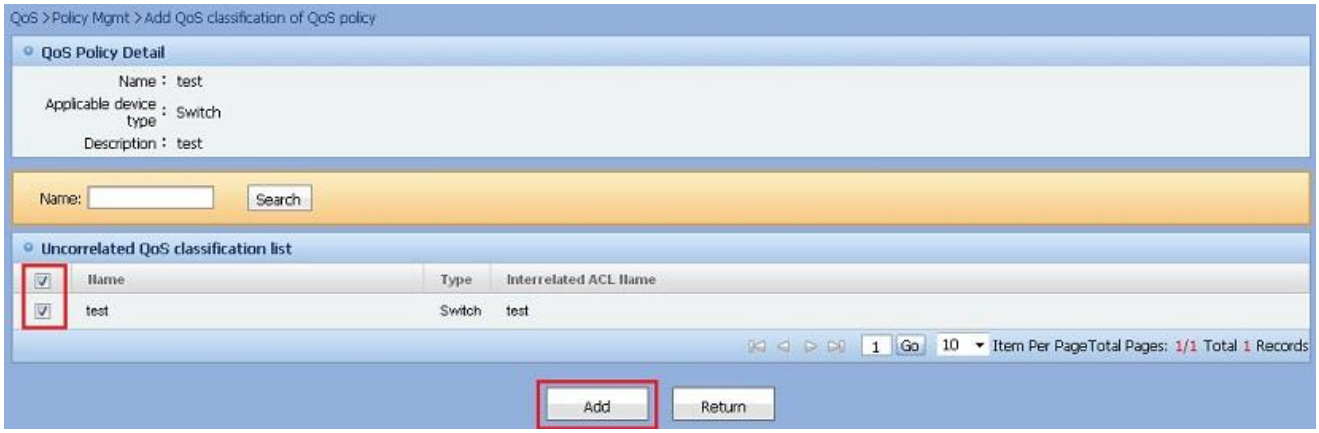


Figure 10.32. Add Interrelated QoS Classification For Type **Switch**

Click **Return** button on **Add Interrelated QoS Classification** page, the system will ignore any changes and return to **QoS Policy Detail** page.

Note

The uncorrelated QoS classification of a policy will be shown on **Uncorrelated QoS classification list**.
If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when adding interrelated QoS classification.
When the classification is deployed on device, some devices will adjust the order of classifications automatically.

10.2.6.1.2. Add Interrelated QoS Classification For Type Router

You can add Interrelated QoS classification for type **Router** using QoS policy management.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name link** on QoS policy list for **Type** value **Router** to enter QoS **Policy Detail** page. On **Interrelated QoS Classification List**, click **Add** button to enter **Add Interrelated QoS Classification** page. As shown below:

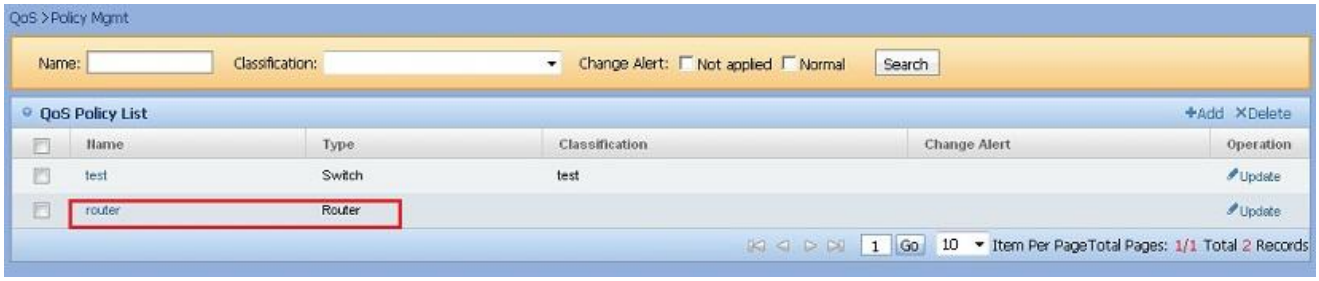


Figure 10.33. Enter **QoS Policy Detail** Page

Figure 10.34. Enter **Add Interrelated QoS Classification** Page

On **Add Interrelated QoS Classification** page, select the QoS classification you want to add interrelation, then click **Add** button. As shown below:

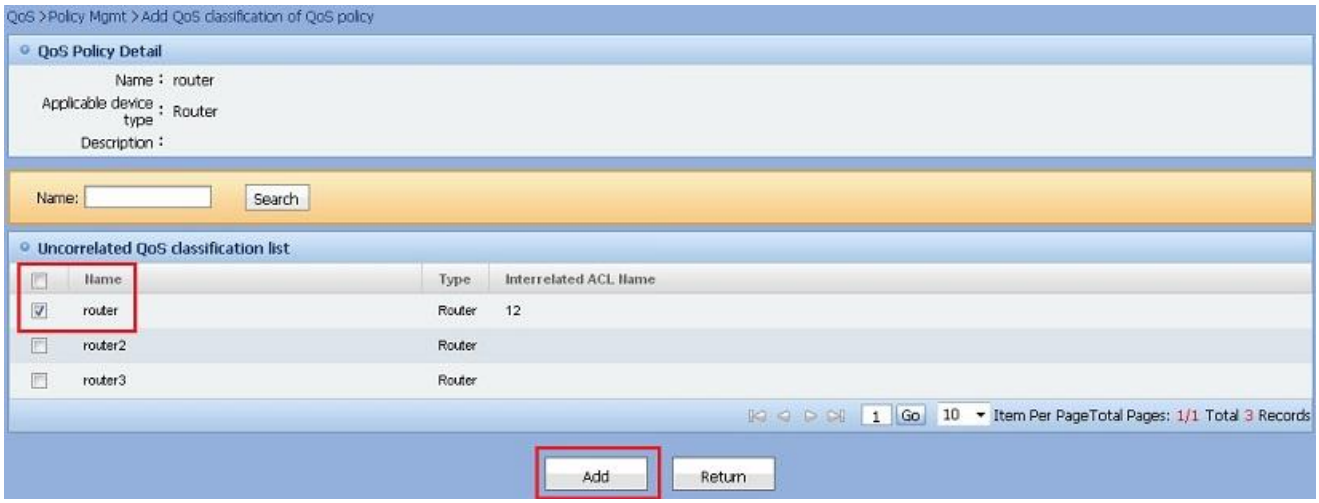


Figure 10.35. Add Interrelated QoS Classification For Type **Router**

Click **Return** button on **Add Interrelated QoS Classification** page, the system will ignore any changes and return to **QoS Policy Detail** page.

Note

The uncorrelated QoS classification of a policy will be shown on **Uncorrelated QoS classification list**. If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when adding interrelated QoS classification. When the classification is deployed on device, some devices will adjust the order of classifications automatically.

10.2.6.2. Modify Interrelated QoS Classification

The interrelated QoS classification can be applied for two types: Switch, Router. You can modify the two types with this module.

- Modify Interrelated QoS Classification For Type **Switch**
- Modify Interrelated QoS Classification For Type **Router**

10.2.6.2.1. Modify Interrelated QoS Classification For Type Switch

You can modify interrelated QoS classification for type **Switch** using QoS policy management.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list for **Type** value **Switch** to enter QoS **Policy Detail** page. On **Interrelated QoS Classification List**, click **Update** button to enter **Modify Interrelated QoS Classification** page. As shown below:

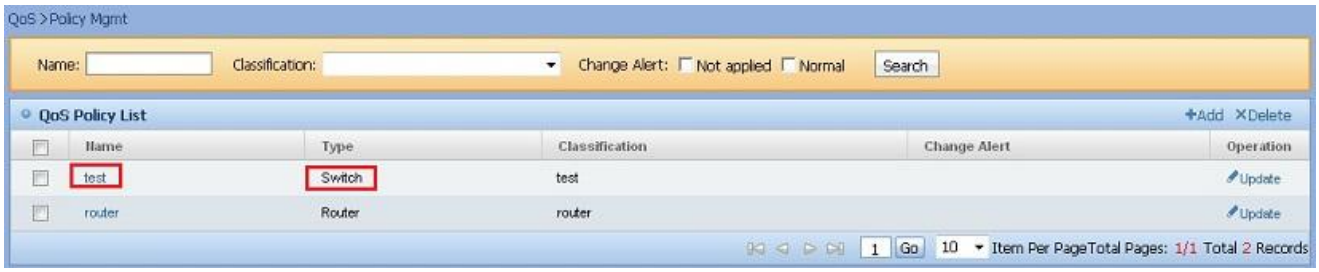


Figure 10.36. Enter **QoS Policy Detail** Page For Type **Switch**

Figure 10.37. Enter **Modify Interrelated QoS Classification** Page For Type **Switch**

On **Modify Interrelated QoS Classification** page, fill the related information of interrelated QoS classification, then click **Update** button. As shown below:

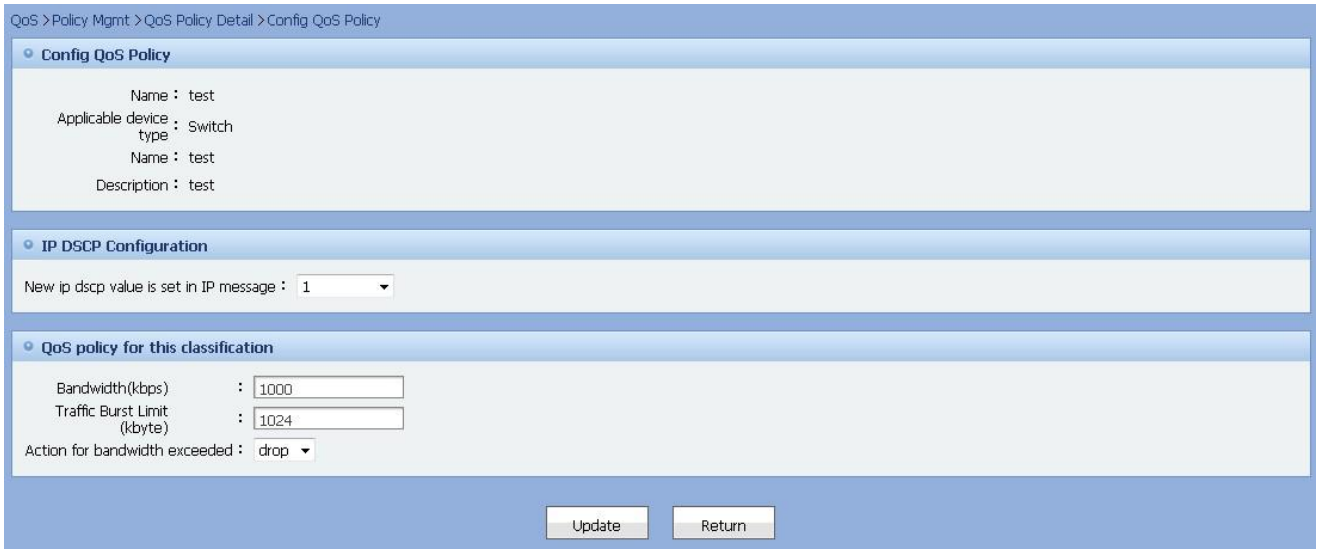


Figure 10.38. Modify Interrelated QoS Classification For Type **Switch**

Click **Return** button on **Modify Interrelated QoS Classification** page, the system will ignore any changes and return to **QoS Policy Detail** page.

Note

The new ip dscp value range of IP message is 0-63, the value in bracket beside is equivalent value.
If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when modifying interrelated QoS classification.

10.2.6.2.2. Modify Interrelated QoS Classification For Type Router

You can modify Interrelated QoS classification for type **Router** using QoS policy management.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list for **Type** value **Router** to enter QoS **Policy Detail** page. On **Interrelated QoS Classification List**, click **Update** button to enter **Modify Interrelated QoS Classification** page. As shown below:

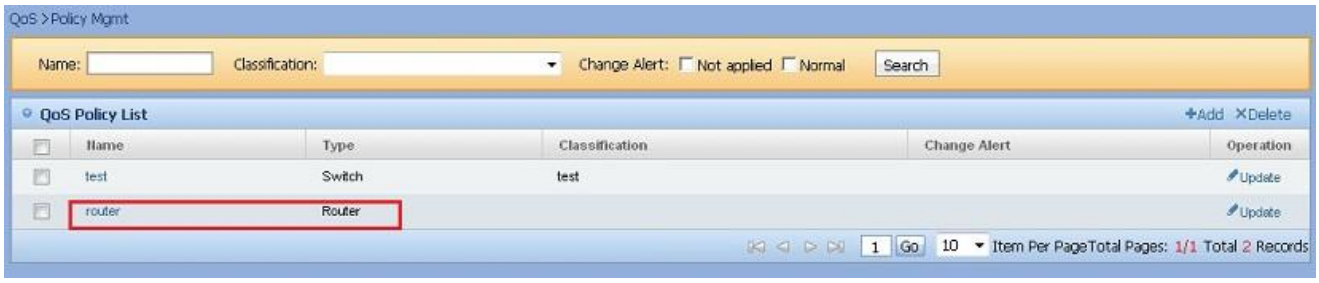


Figure 10.39. Enter **QoS Policy Detail** Page For Type **Router**

Figure 10.40. Enter Modify Interrelated QoS Classification Page For Type **Router**

On **Modify Interrelated QoS Classification** page, fill the related information of interrelated QoS classification, then click **Update** button. As shown below:

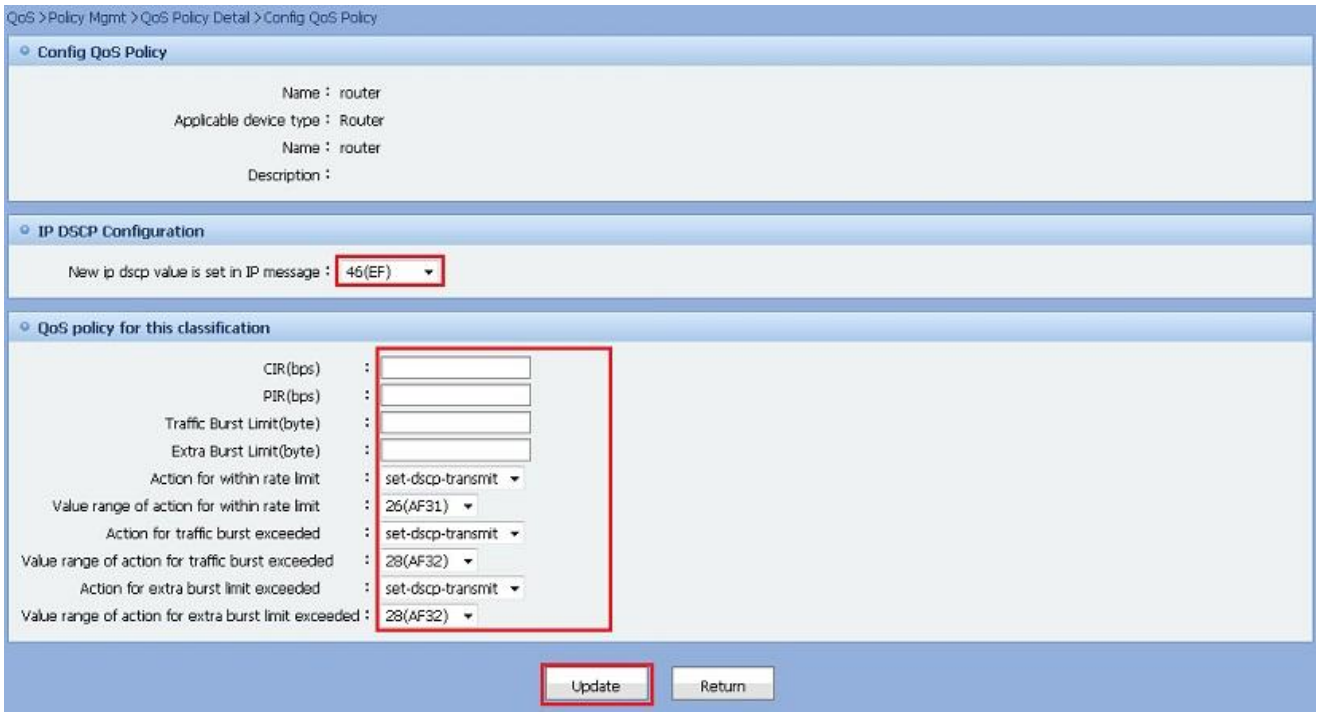


Figure 10.41. Modify Interrelated QoS Classification For Type **Router**

Click **Return** button on **Modify Interrelated QoS Classification** page, the system will ignore any changes and return to **QoS Policy Detail** page.

Note

Rate limit value(bps) range is 0-63, the value in bracket beside is equivalent value.
If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when modifying interrelated QoS classification.

10.2.6.3. Delete Interrelated QoS Classification

You can delete interrelated QoS classification on QoS policy detail page.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

Figure 10.42. Enter **QoS Policy Detail** Page

Click **Delete** button on **Interrelated QoS Classification List**, the system will prompt for your confirmation. Click **Confirm** to execute deletion. As shown below:

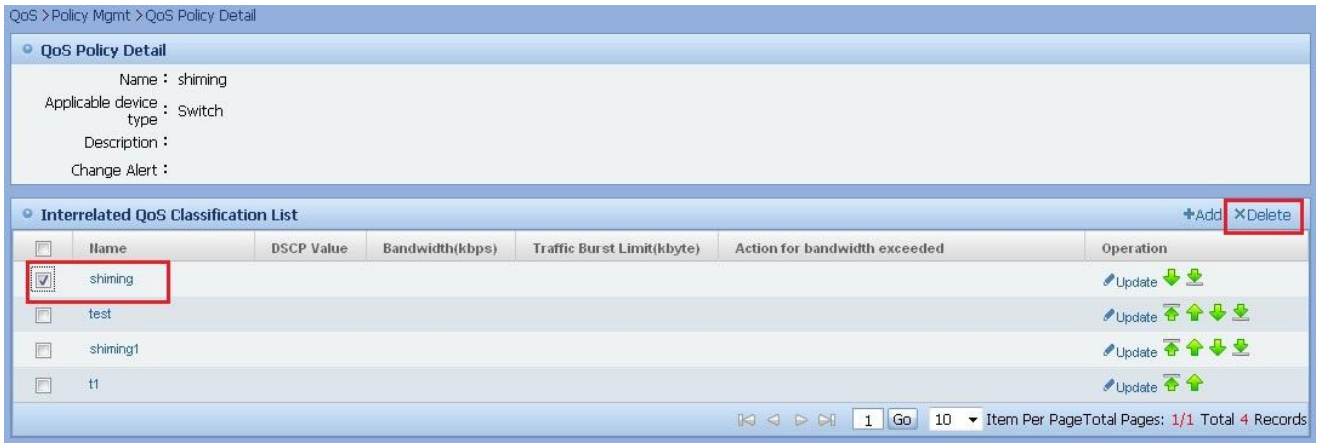


Figure 10.43. Delete Interrelated QoS Classification

Note

If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when deleting the interrelated QoS classification.

10.2.6.4. Order Adjustment for Interrelated QoS Classification

You can adjust the order of interrelated QoS classification on QoS policy detail page.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

Figure 10.44. Enter **QoS Policy Detail** Page

On **Interrelated QoS Classification List**, click the move button under **Operation** column to adjust the order of QoS classification. As shown below:

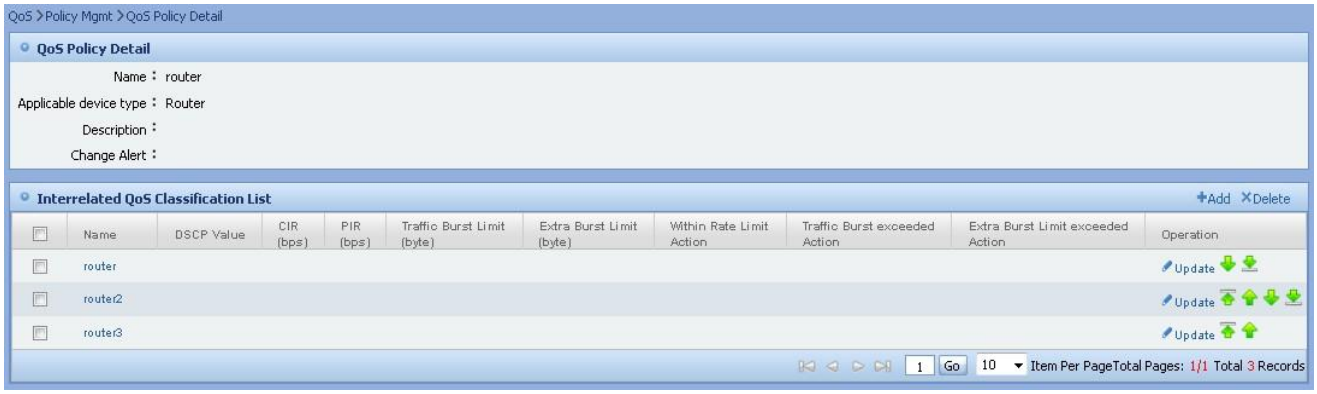


Figure 10.45. Adjust the order of Interrelated QoS Classification

Note

If the QoS policy with the interrelated QoS classification had been deployed on device, the system will automatically update the change alert of QoS policy when adjusting the order of interrelated QoS classification.
First (**Last**) means move the classification to the first(last) of all the classifications, not the first(last) classification of the classifications on the current page.
Under **Operation** column, from left to right, the move buttons are **First, Up, Down** and **Last.** You can refer to the prompt if you put mouse pointer on the button.

10.2.7. Management of Policy-Deployed Device

This module provides management of devices with QoS policy deployed.

- Delete QoS Policy from Device
- Deploy QoS Policy on Device
- Redeploy QoS Policy on Device
- Deploy QoS Policy on Interface

10.2.7.1. Delete QoS Policy from Device

On QoS policy detail page, you can delete QoS policy from a device.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

Figure 10.46. Enter **QoS Policy Detail** Page

On **Device List,** click **Delete** button under **Operation** column of related device, the system will prompt for your confirmation. Click **Confirm** to delete QoS policy from the device. As shown below:

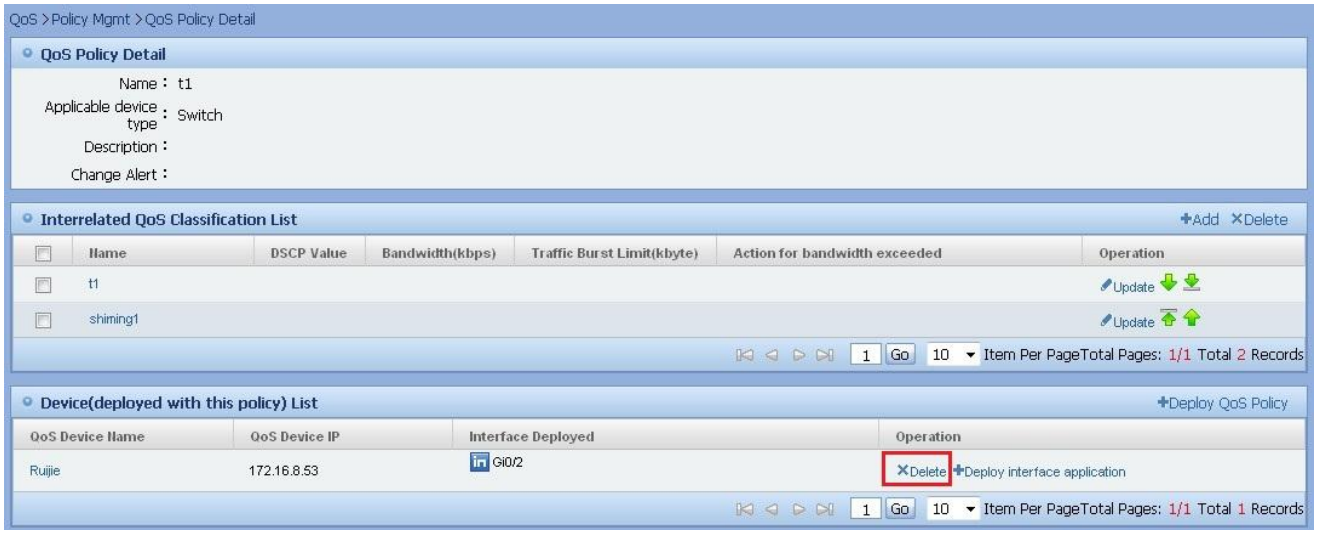


Figure 10.47. Delete QoS Policy from Device

Note

Deleting QoS policy from device will operate on single device and deploy to the device directly, the system won't generate deployment plan.

10.2.7.2. Deploy QoS Policy on Device

On QoS policy detail page, you can add a QoS deployment plan.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

Figure 10.48. Enter **QoS Policy Detail** Page

On **Device List**, click **Deploy QoS Policy** button to enter **Deploy QoS Policy** page. For other operations, please refer to *Add QoS Deployment Plan*. As shown below:

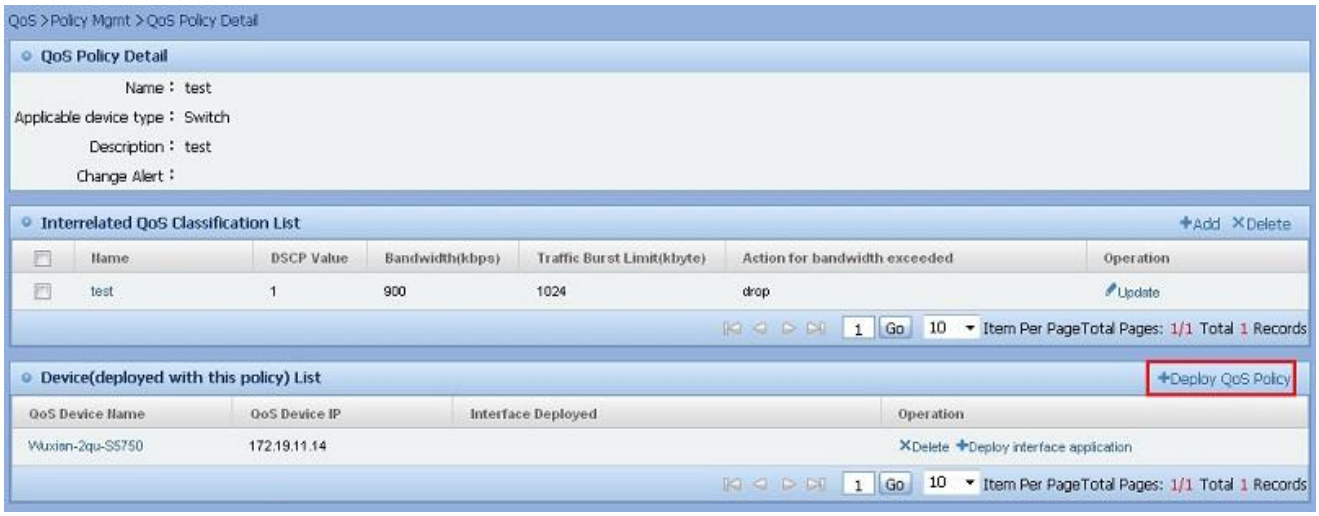


Figure 10.49. Deploy QoS Policy

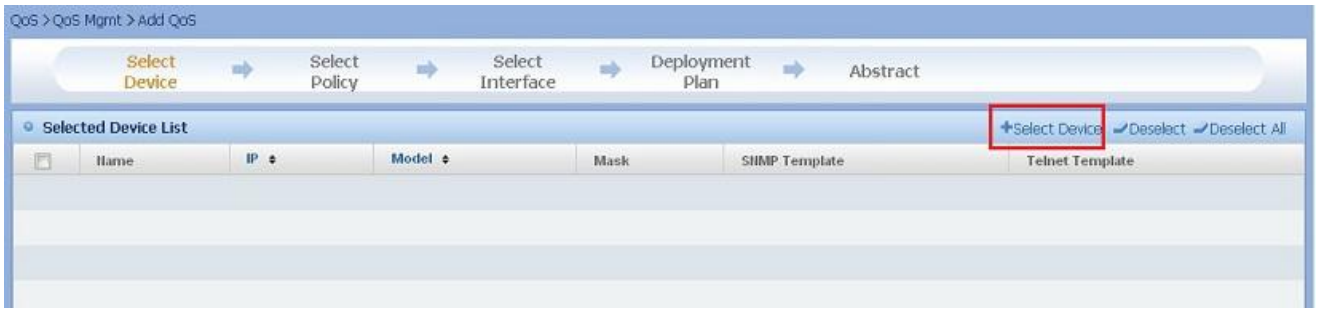


Figure 10.50. Enter **Add Deployment Plan** Page

Note

After deploying QoS policy, the system will forward to **Add QoS Deployment Plan** page.
In the process of adding QoS deployment, this QoS policy has been set as QoS policy.

10.2.7.3. Redeploy QoS Policy on Device

On QoS policy detail page, you can redeploy the QoS policy on a device.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

Figure 10.51. Enter **QoS Policy Detail** Page

On **Device List**, click **Redeploy** button under **Operation** column of corresponding device, the system will prompt for your confirmation. Click **Confirm** to redeploy the QoS policy on device. As shown below:

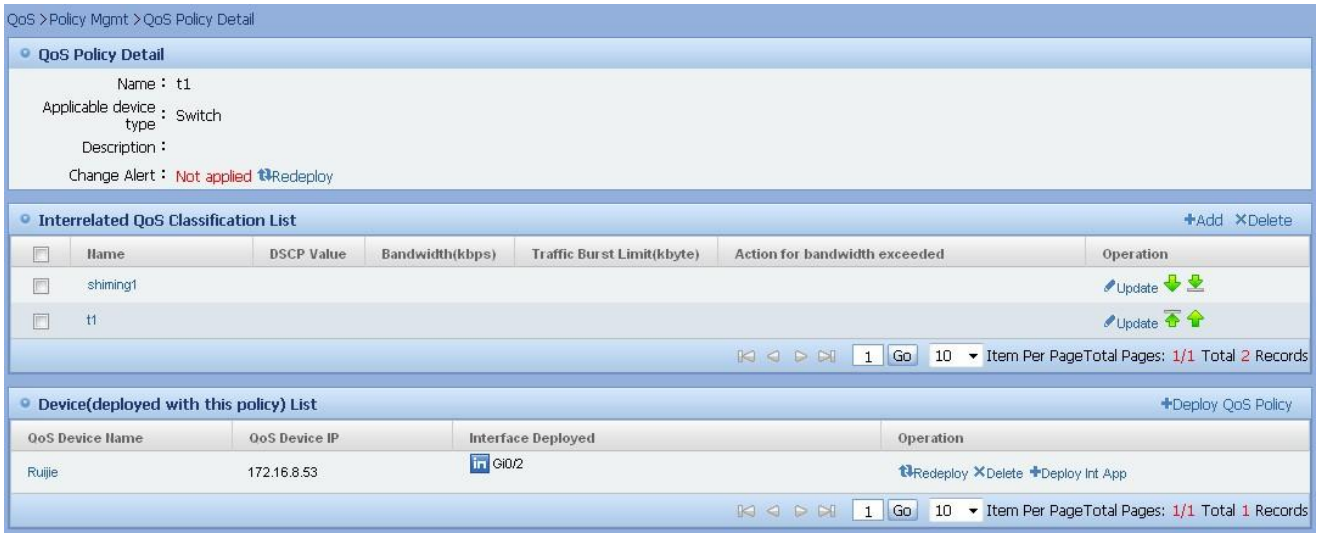


Figure 10.52. Redeploy QoS Policy

Note

When the QoS policy is redeployed on device, this will operate on single device and deploy to device directly. No deployment plan will be generated.

10.2.7.4. Deploy QoS Policy on Interface

You can select an interface and deploy QoS policy on it.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

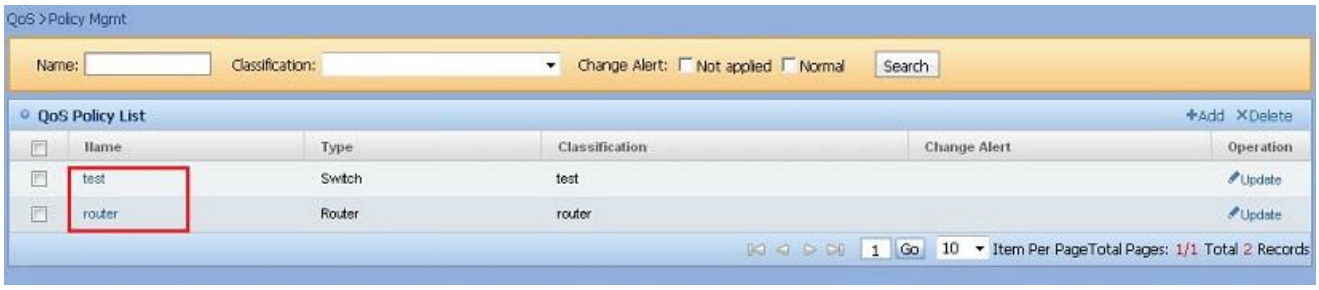


Figure 10.53. View QoS Policy

Enter **QoS Policy Detail** page, click **Deploy Int App** button on **Device List** to enter **Add QoS Interface Deployment** page, it shows the deployed interface. As shown below:

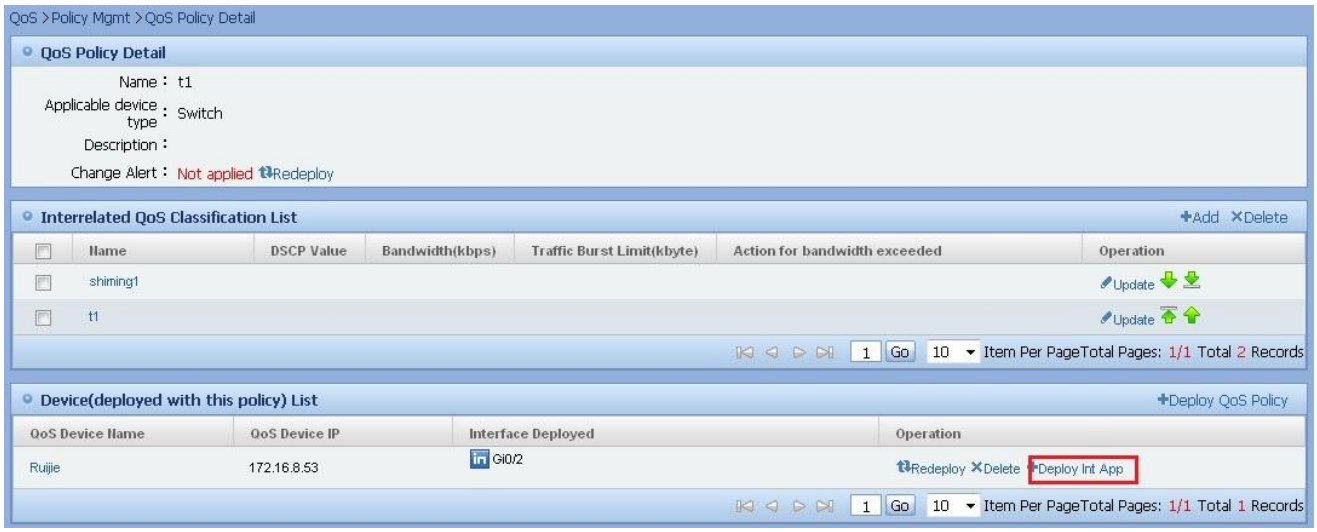


Figure 10.54. Enter Add QoS Interface Deployment

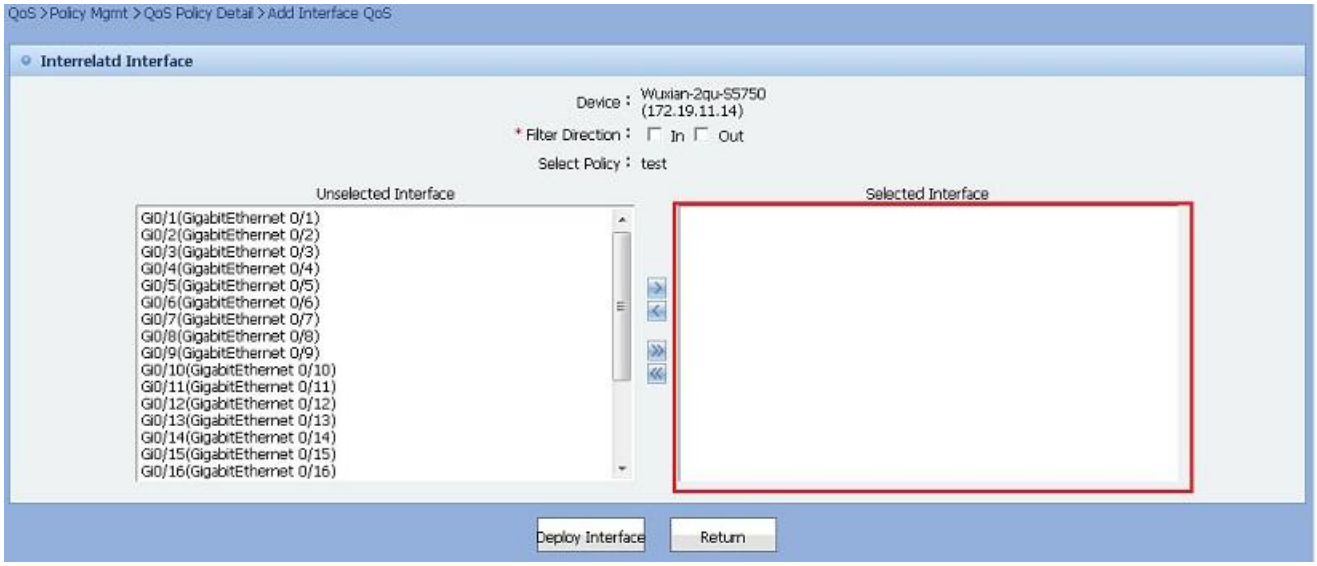


Figure 10.55. Add QoS Interface Deployment

After selecting interface from **Filter Direction** and **Unselected Interface**, double click interface or click **>** button, the interface will be added into **Selected Interface** and displayed with format: Interface Name[Filter Direction]QoS Policy Name, then click **Deploy Interface** to deploy the QoS policy to selected interface.

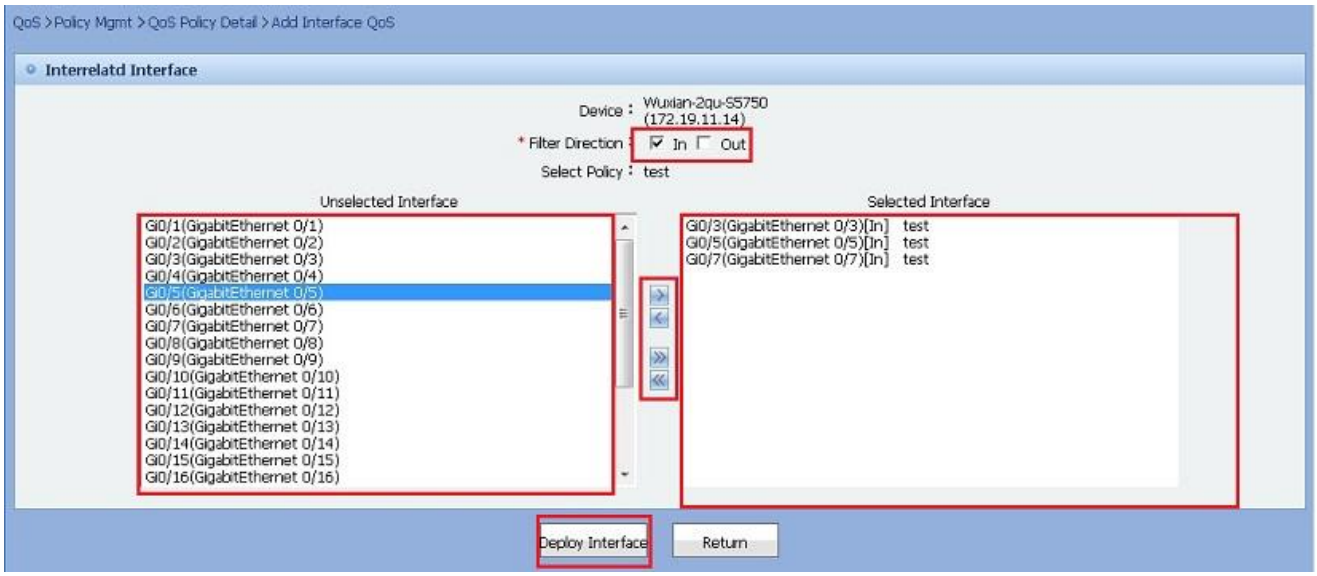


Figure 10.56. Add QoS Interface Deployment

On **Unselected Interface**, double click the interface or click **>** button configure single interface, you can also click **>>** to configure interface in batches.
On **Selected Interface**, double click the interface or click **<** button remove single interface, you can also click **<<** to remove interface in batches.
Click **Return** button on **Add QoS Interface Deployment** page, the system will ignore any changes and return to **QoS Device Detail** page.

Note The filter direction and unselected interface must be selected for configuring QoS interface.

10.2.8. Redeploy QoS Policy With Changes

You can redeploy the QoS policy on a device, which the QoS policy has been deployed on and has change alert.

Operation Steps

1) On **QoS Policy Management** page, click **QoS Policy Name** link on QoS policy list to enter **QoS Policy Detail** page. As shown below:

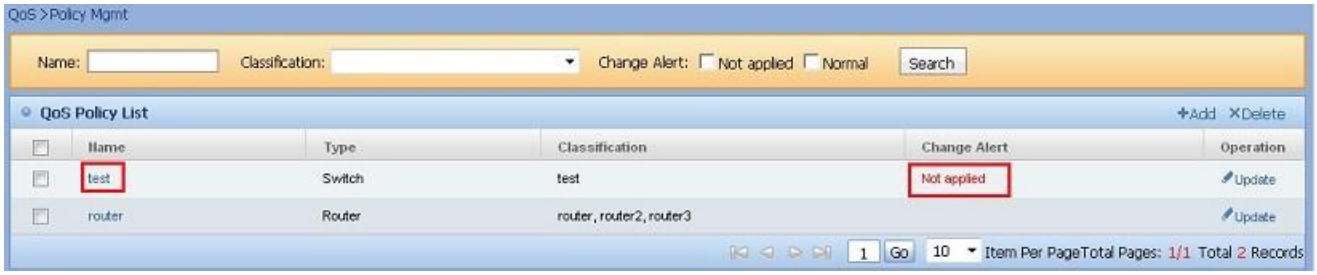


Figure 10.57. Enter Redeploy QoS Policy With Changes Page

Enter **QoS Policy Detail** page, click **Redeploy** button under change alert column, the system will prompt with “Are you sure to overwrite the policies with the same name on all the device?”. Click **Confirm** to finish the redeployment and **Not Applied** under change alert column will disappear. As shown below:

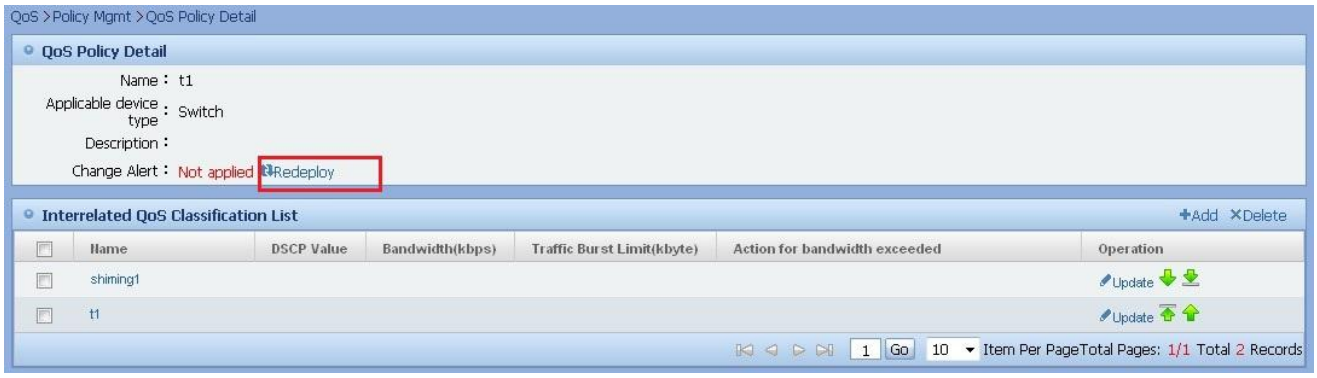


Figure 10.58. Redeploy QoS Policy With Changes

Figure 10.59. Redeploy QoS Policy With Changes Succeeded

Enter **QoS Deployment Plan Management** page, click the latest **Plan Name** link to view the progress of QoS policy redeployment. As shown below:

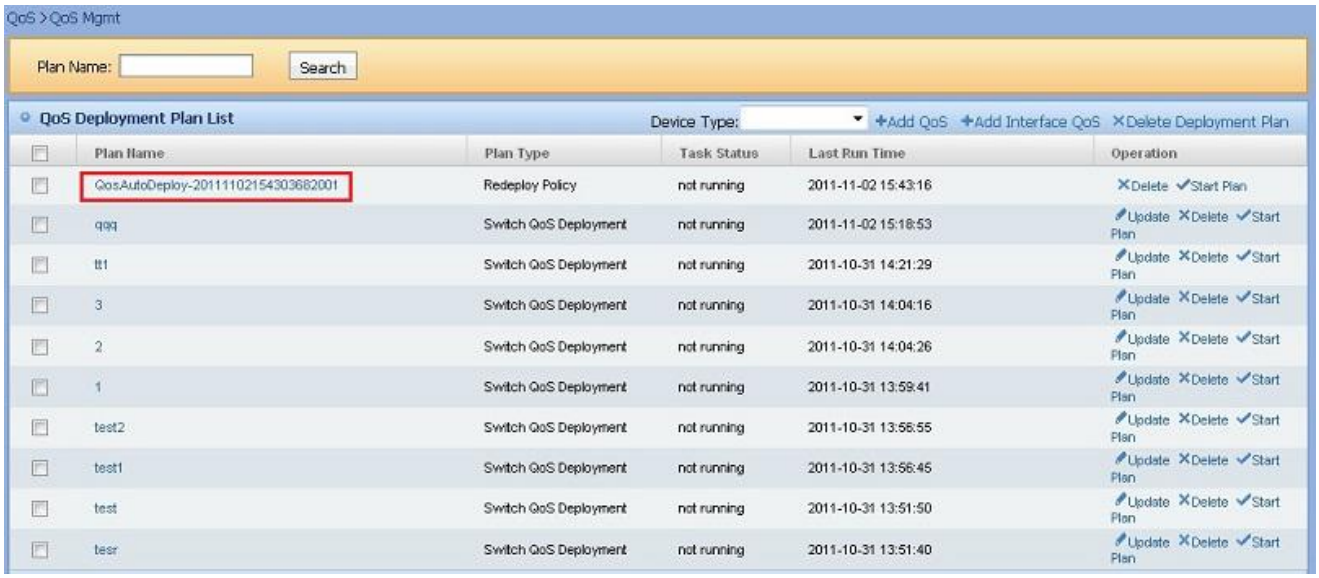


Figure 10.60. Enter View QoS Policy Redeployment With Changes Page

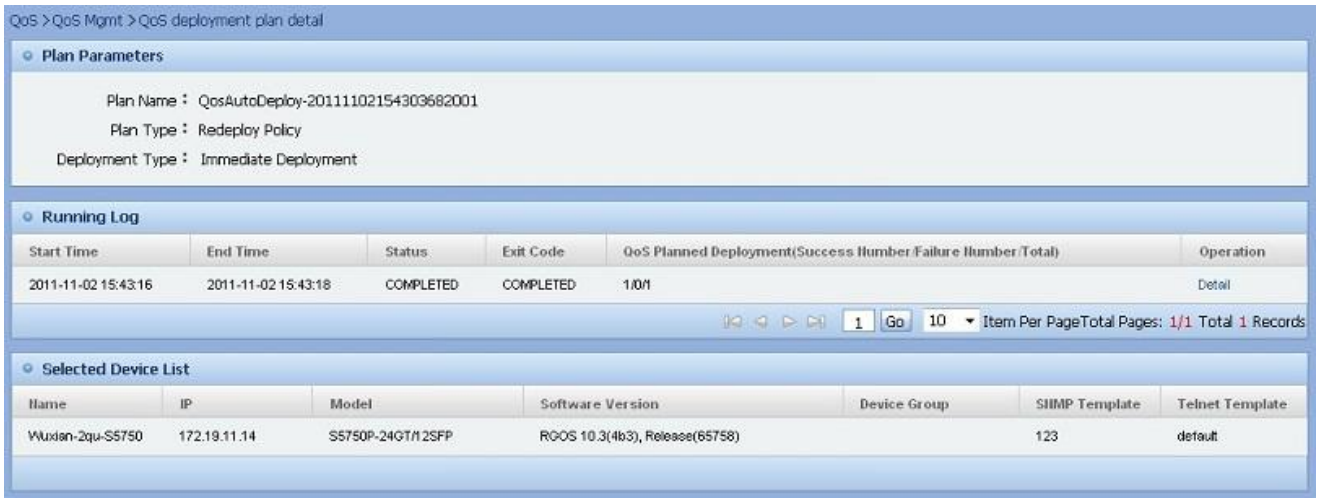


Figure 10.61. View QoS Policy Redeployment With Changes

Note

After the QoS policy is redeployed, the system will generate deployment plan automatically and deploy it immediately. If the background process is not running, the deployment plan won't be generated.
After the QoS policy is redeployed, the system will change QoS policy of interrelated QoS devices with consistent identification.

10.3. QoS Device Management

QoS device management targets at managing devices in the management network. It manages QoS classification, QoS policy and interface list of devices.

Function List

- Add QoS Device
- Delete QoS Device
- Search QoS Device
- QoS Device Detail
- Modify QoS Device
- Delete QoS Device Classification
- Delete QoS Policy from a Device
- QoS Device Interface Configuration
- Redeploy QoS Device Classification
- Redeploy QoS Policy on a Device
- Redeploy QoS Device Policy
- QoS Device Synchronization
- QoS Device Classification Contrast
- QoS Policy Contrast
- Delete the Policy Associated with a QoS Device Interface
- Delete Inbound Rate Limit Info Of Interface
- Delete Outbound Rate Limit Info Of Interface
- Add Inbound Rate Limit Info Of Interface
- Add Outbound Rate Limit Info Of Interface
- QoS Device Interface Deployment
- QoS Device Interface Detail
- Redeploy Interface Information

10.3.1. Add QoS Device

QoS device must be added into the system before it can be managed by the system.

Operation Steps

1) Enter QoS device management page, click **Add Device** icon to enter **Import QoS Device** page. As shown below:

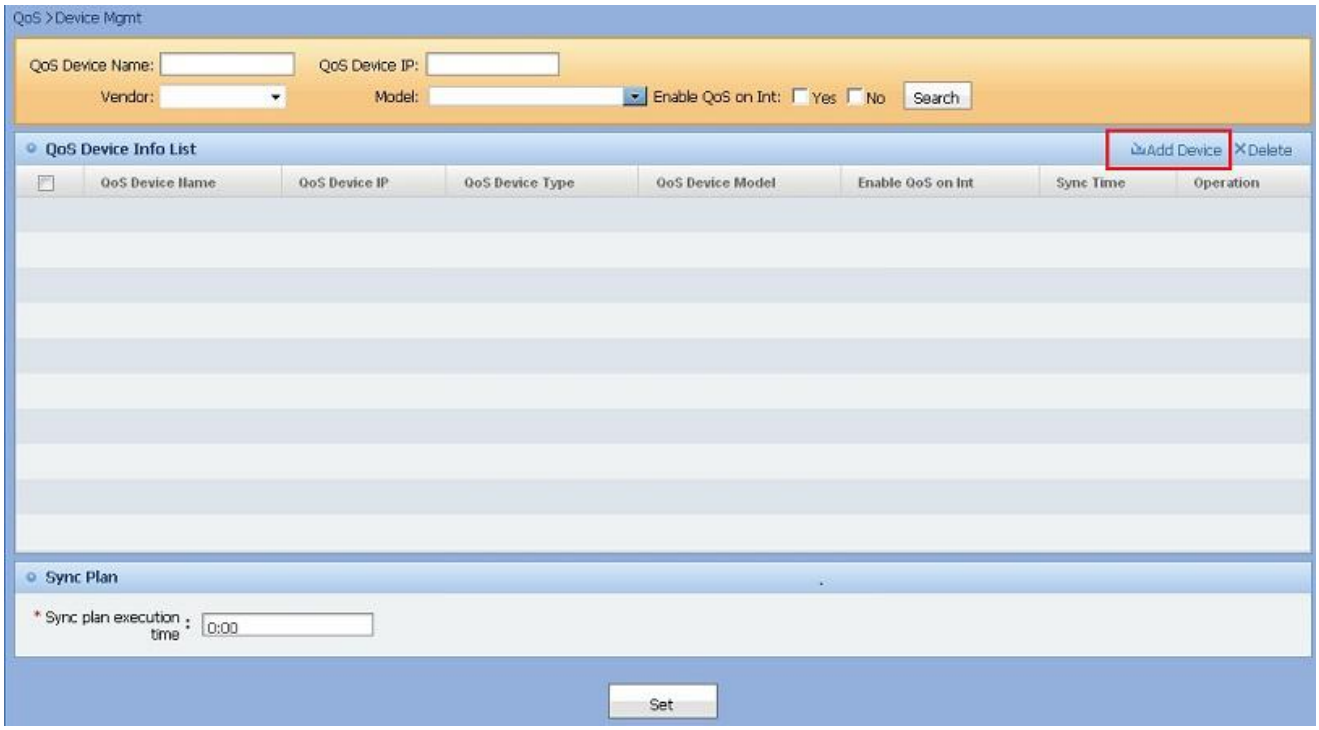


Figure 10.62. Enter **Import QoS Device** Page

Click **Select Device** on **Import QoS Device** page. As shown below:

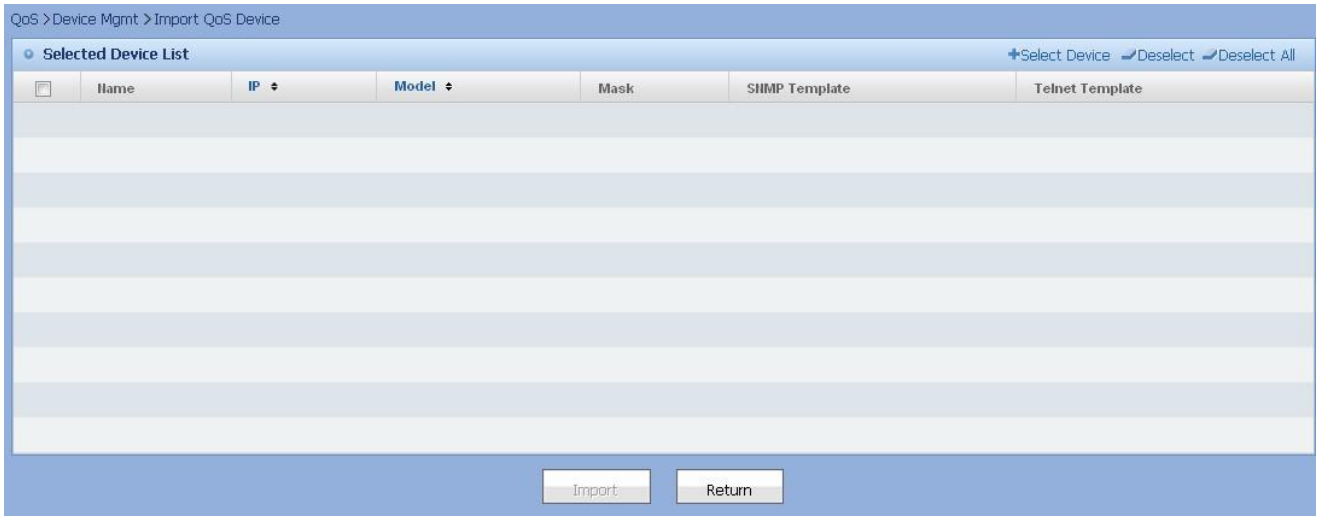


Figure 10.63.**Import QoS Device** Page

The device list will be popped up. As shown below:

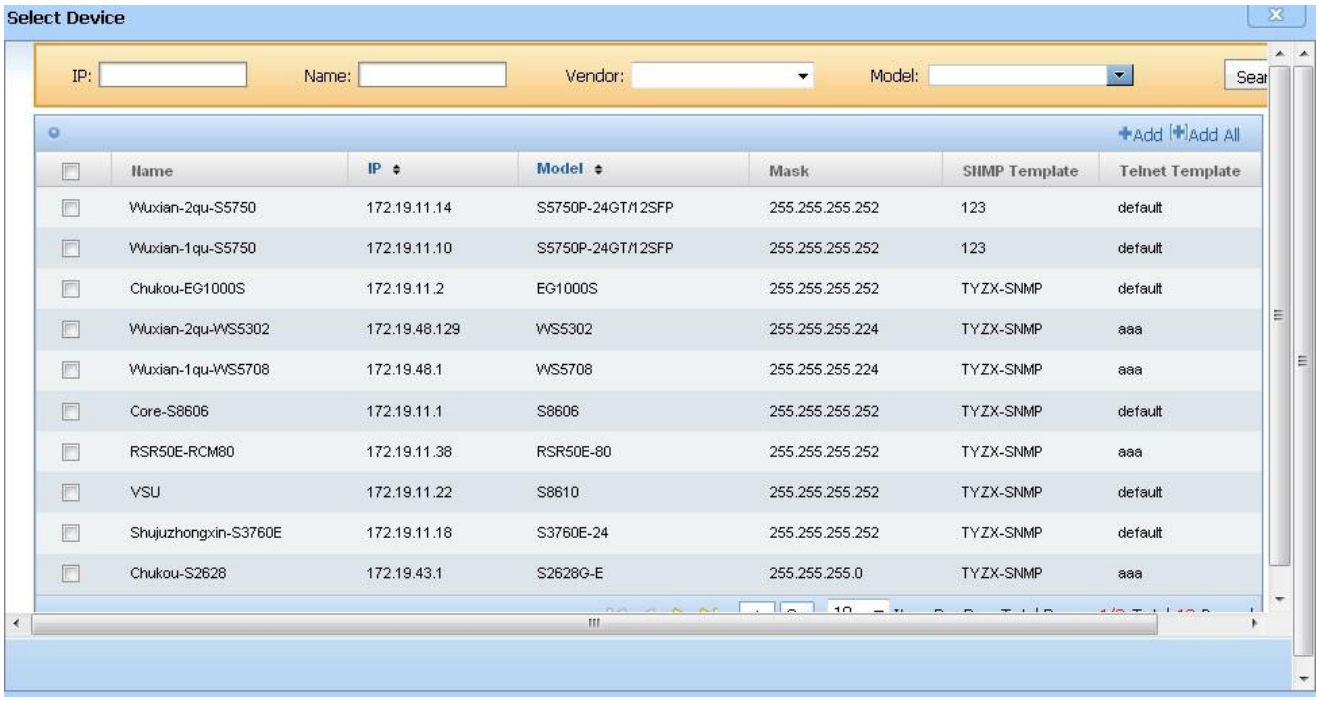


Figure 10.64. **Device List** Page

Select the device you want to import, then click **Add** button. As shown below:

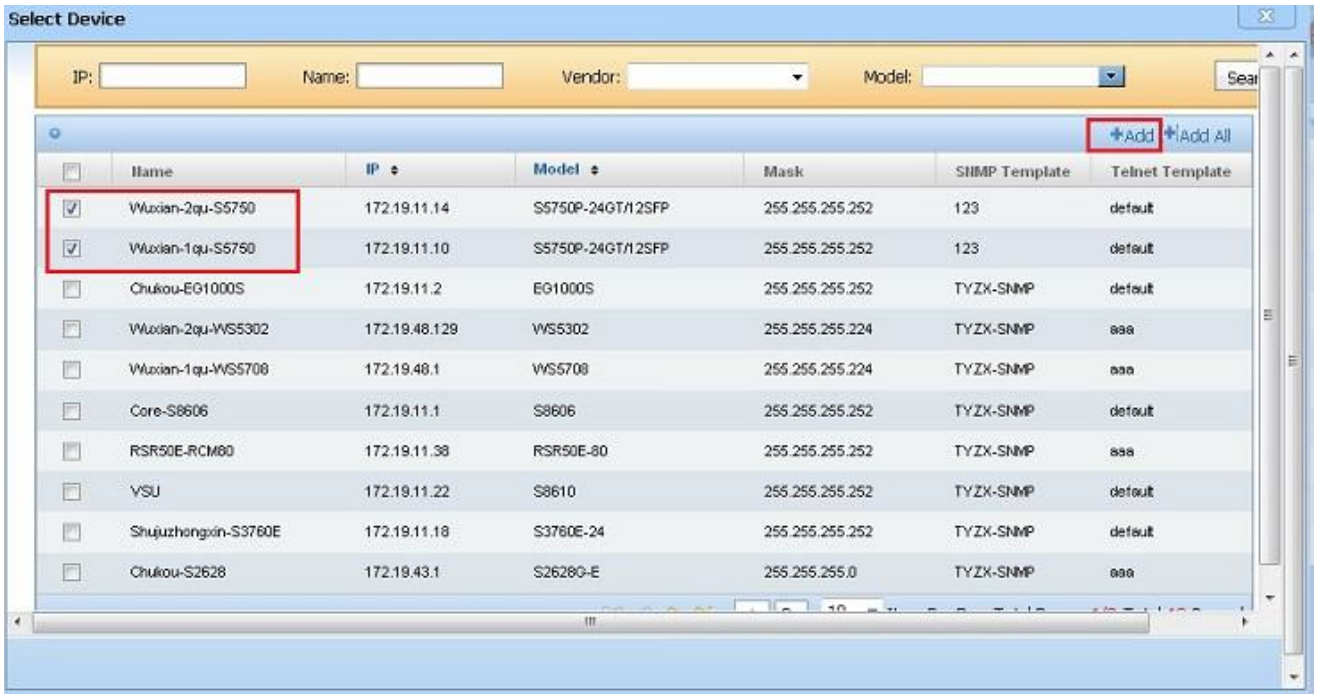


Figure 10.65. **Add Device** Page

The selected device will be shown on importing QoS device page, click **Import** button to save the data into database. As shown below:

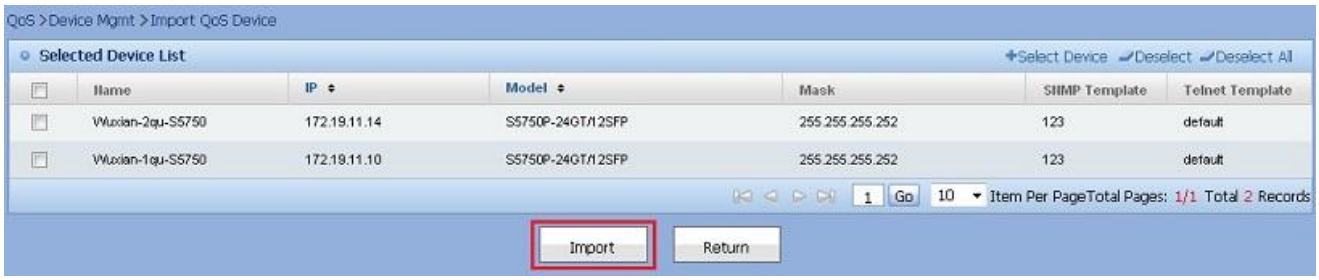


Figure 10.66. **Import QoS Device** Page

Click **Import** button, the device import log will be displayed. As shown below:

Figure 10.67. Device Import Log Page

After the device is successfully imported, click **Return** button to return to device management page. The imported device information will be displayed. As shown below:

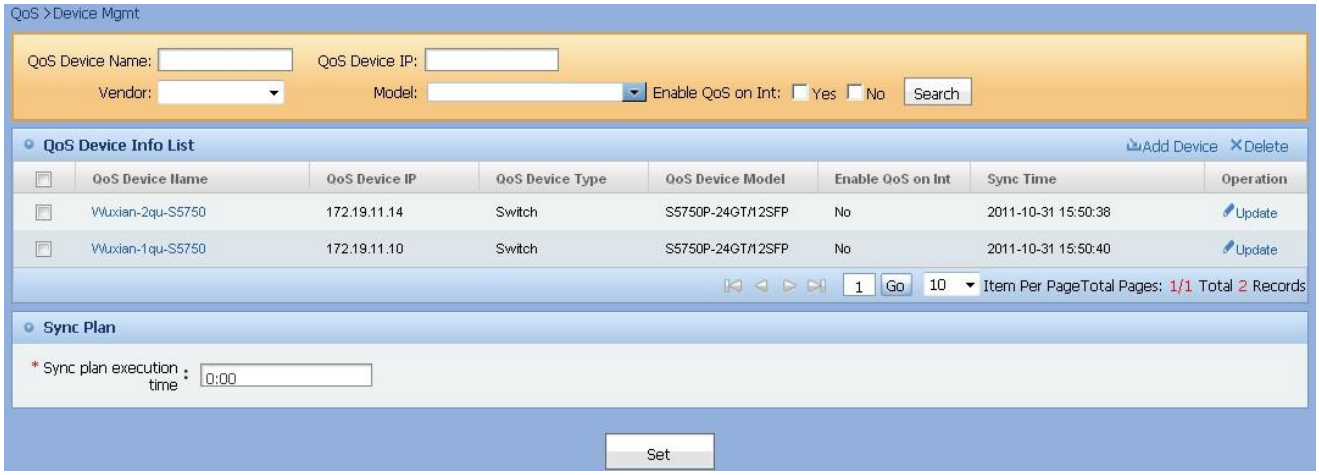


Figure 10.68. Return To **Device Management** Page

Click **Return** button on **Import QoS Device** page, the system will ignore any changes and return to **QoS Device Management** page.

Note: If the device import fails, the device information will not be saved into database.

10.3.2. Delete QoS Device

On **QoS Device Management** page, you can delete QoS devices in batches.

Operation Steps

1) Enter **QoS Device Management** page, select devices from the device list and click **Delete** button, the system will prompt for your confirmation, then click **Confirm** to delete the selected devices. As shown below:

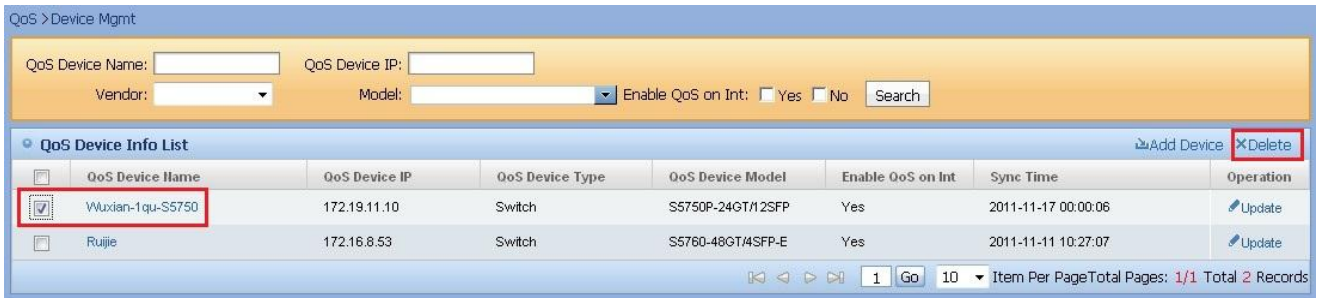


Figure 10.69. **Device Management** Page

After deletion is accomplished, the system will show a success prompt and the information of deleted device is removed.

10.3.3. Search QoS Device

On **QoS Device Management** page, you can search devices by device name, IP address, vendor, device model or interface deployed.

Operation Steps

Enter **QoS Device Management** page, input device name, device IP address, vendor, device model or interface deployed, then click **Search** button, the system will list all the matched devices information. As shown below:

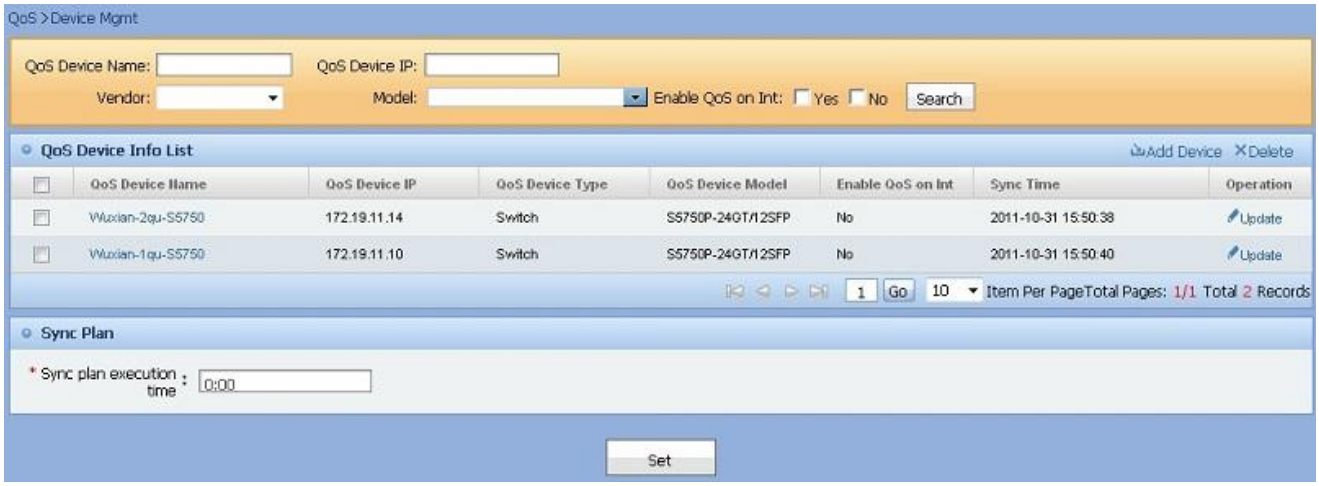


Figure 10.70. **QoS Device Management** Page

Note The system will list all the devices if the four conditions are left empty.

10.3.4. QoS Device Detail

The QoS device detail page shows device detail information, interrelated QoS classification information, interrelated QoS policy list and device interface list.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

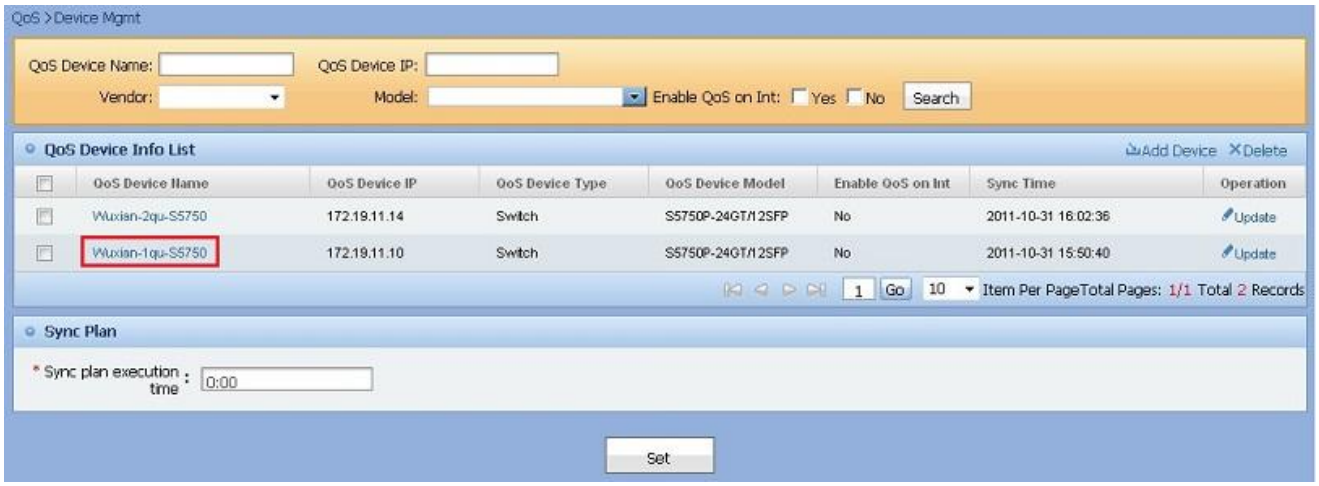


Figure 10.71. Enter **QoS Device Detail** Page

On **QoS Device Detail** page, the device detail information, interrelated QoS classification information, interrelated QoS policy list and device interface list will be displayed. As shown below:

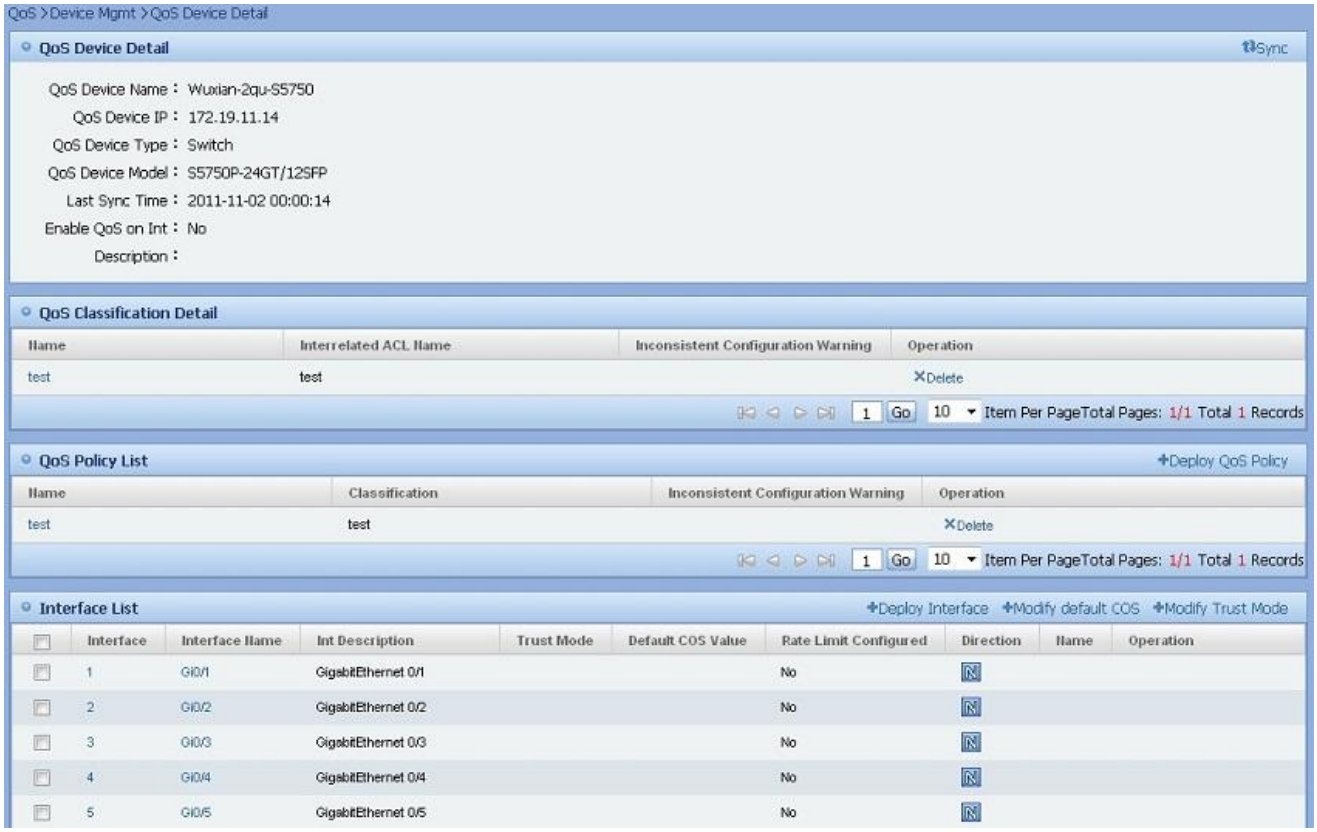


Figure 10.72. **QoS Device Detail** Page

10.3.5. Modify QoS Device

After you modify QoS device, the data will be saved into system database.

Operation Steps

1) Enter QoS device management page, click **Update** icon to enter **Modify Device** page. As shown below:

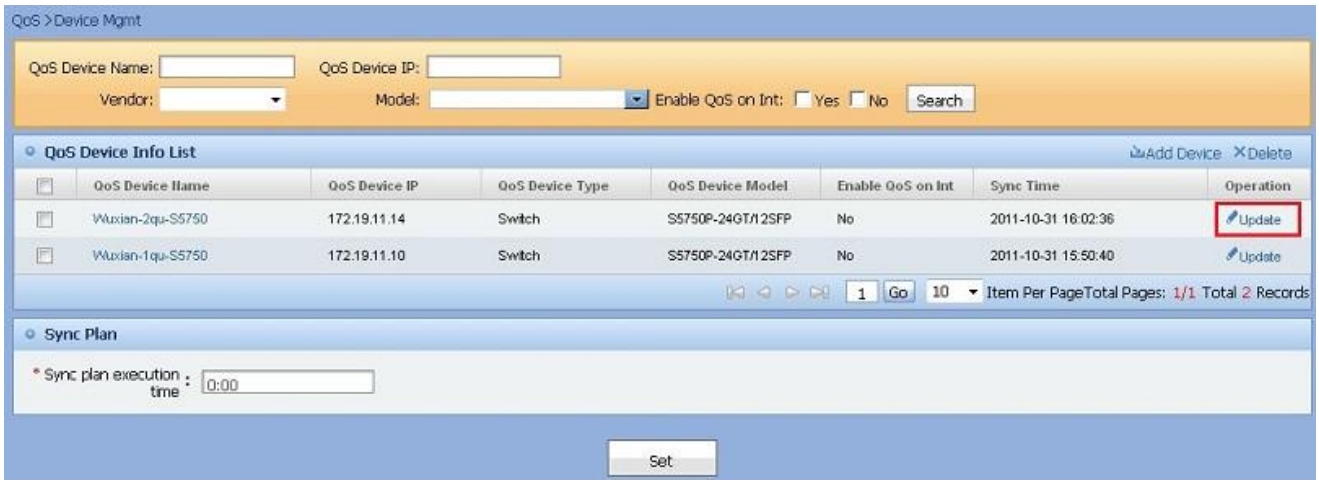


Figure 10.73. Enter **Modify Device** Page

Fill in the device description on **Modify Device** page, then click **Update** button. As shown below:

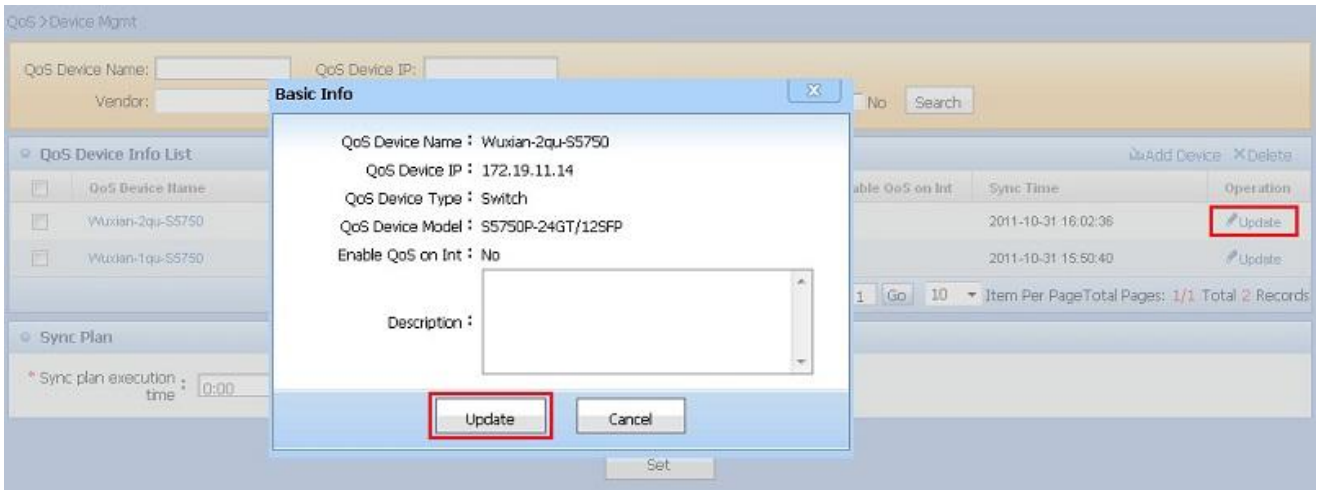


Figure 10.74. **Modify Device** Page

Click **Cancel** button on **Modify Device** page, the system will ignore any changes and return to **QoS Device Management** page.

Note No inconsistent changes will be generated.

10.3.6. Delete QoS Device Classification

On **QoS Device Detail** page, you can delete device classification.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

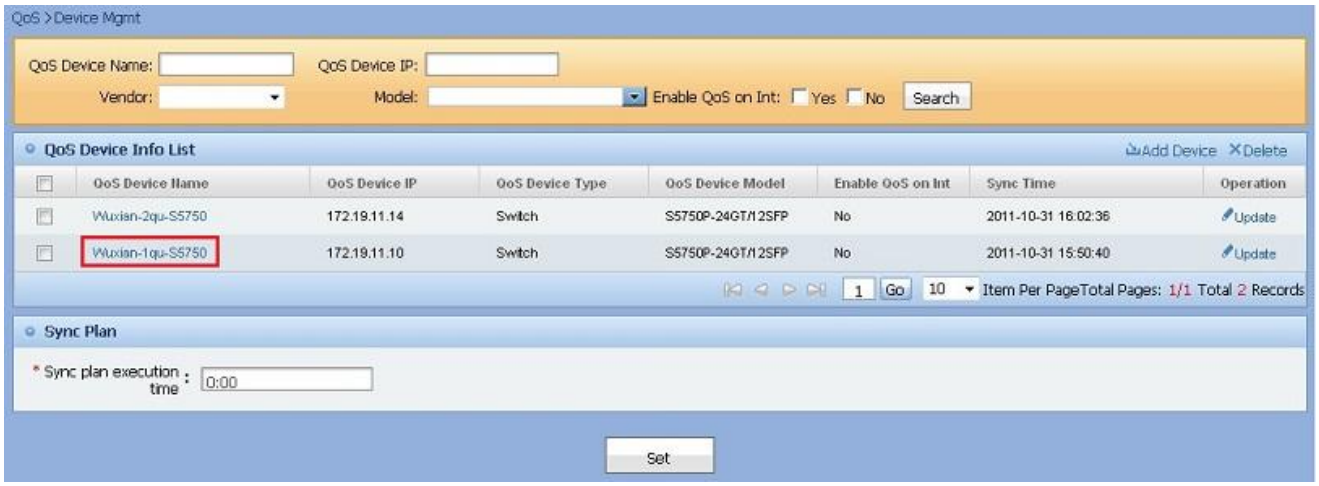


Figure 10.75. Enter **QoS Device Detail** Page

Click **Delete** icon under operation column on classification list, and the system will prompt for your confirmation. As shown below:

Figure 10.76. Delete QoS Device Classification

After deletion is accomplished, the system will show a success prompt.

10.3.7. QoS Device Interface Configuration

Enter device detail page, click **Interface QoS Configuration** icon to enter QoS parameter info page.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **Device Detail** page. As shown below:

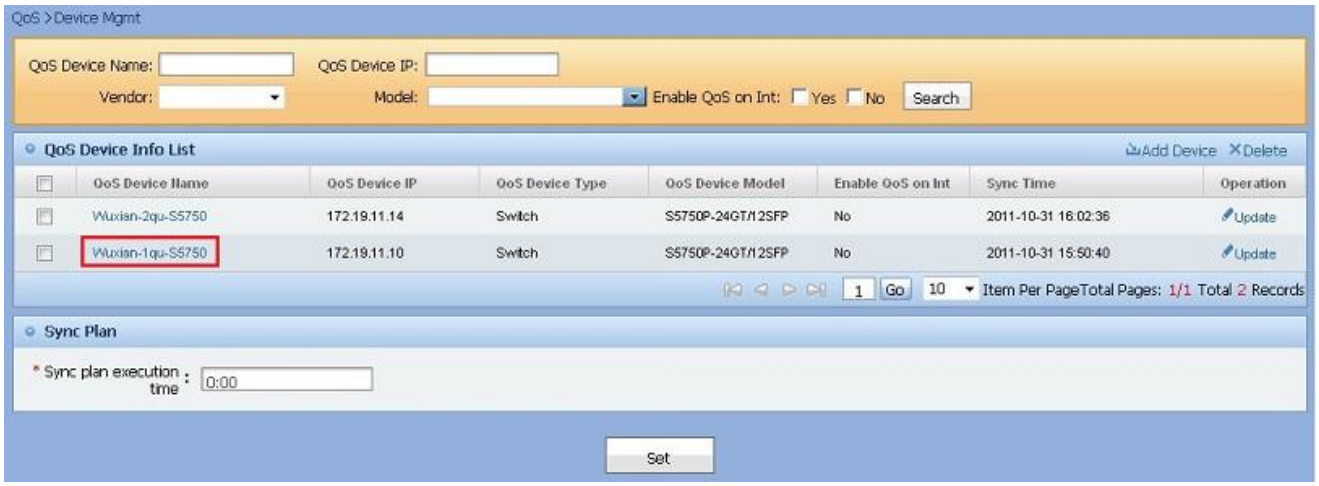


Figure 10.77. Enter **Device Detail** Page

Click **Interface QoS Configuration** icon under operation column on interface list to enter QoS parameter information page. As shown below:

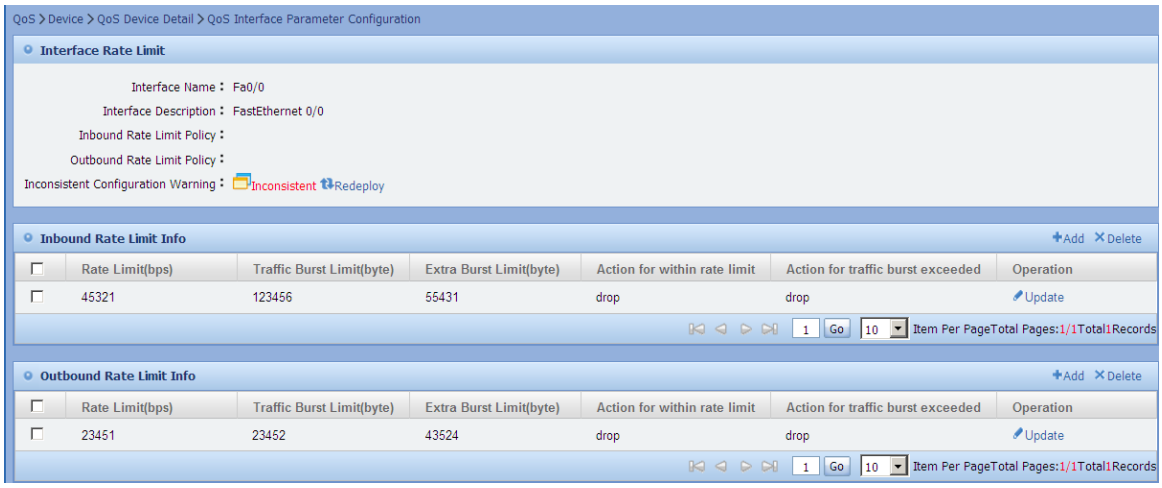


Figure 10.78. Parameter Info Page

10.3.8. Delete QoS Policy from a Device

On **QoS Device Detail** page, you can delete QoS policy from a device.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

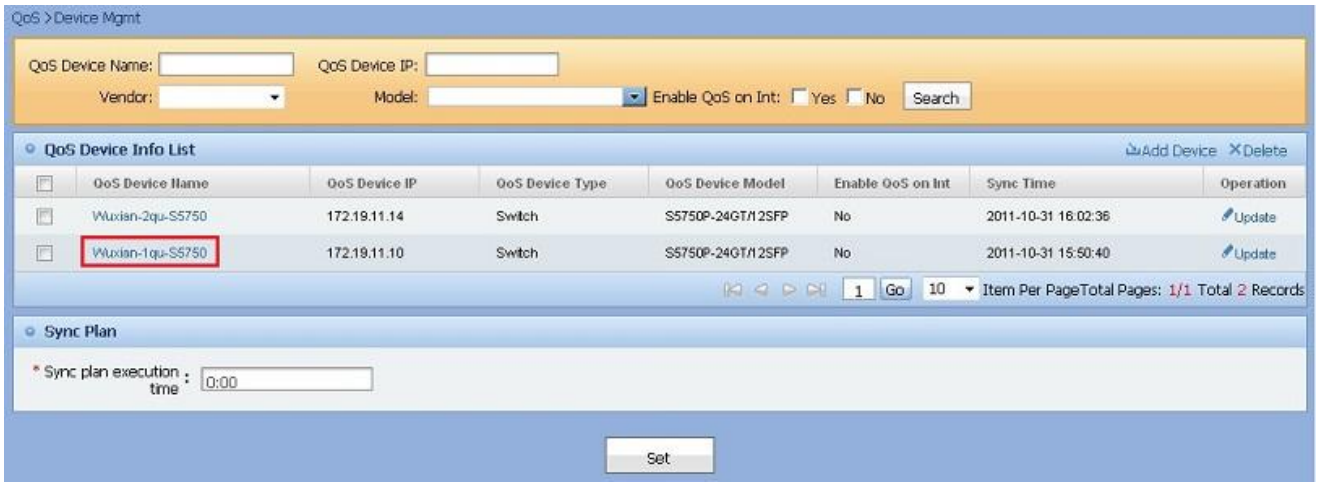


Figure 10.79. Enter **QoS Device Detail** Page

Click **Delete** icon under operation column on policy list, the system prompt for your confirmation. As shown below:

Figure 10.80. Delete Device Policy

After deletion is accomplished, the system will show a success prompt.

10.3.9. Redeploy QoS Device Classification

On **QoS Device Detail** page, you can redeploy device classification.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

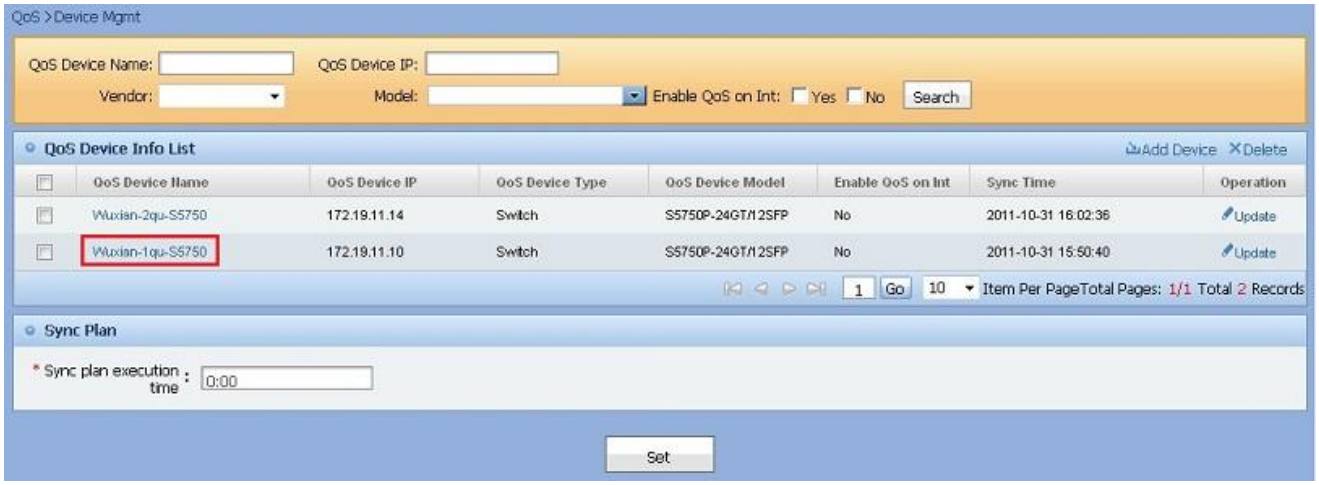


Figure 10.81. Enter **QoS Device Detail** Page

Click **Redeploy** icon under operation column on classification list, the system will prompt for your confirmation. As shown below:

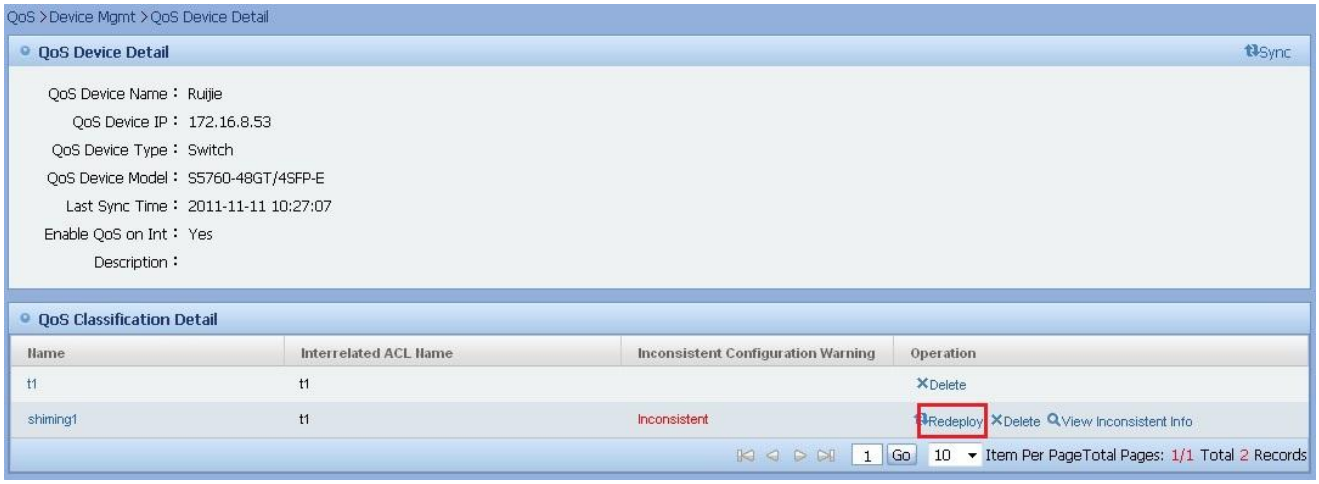


Figure 10.82. Redeploy QoS Device Classification

Note After redeployment, the inconsistent sign will no longer exist.

10.3.10. Redeploy QoS Policy on a Device

On **QoS Device Detail** page, you can redeploy QoS policy on a device.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

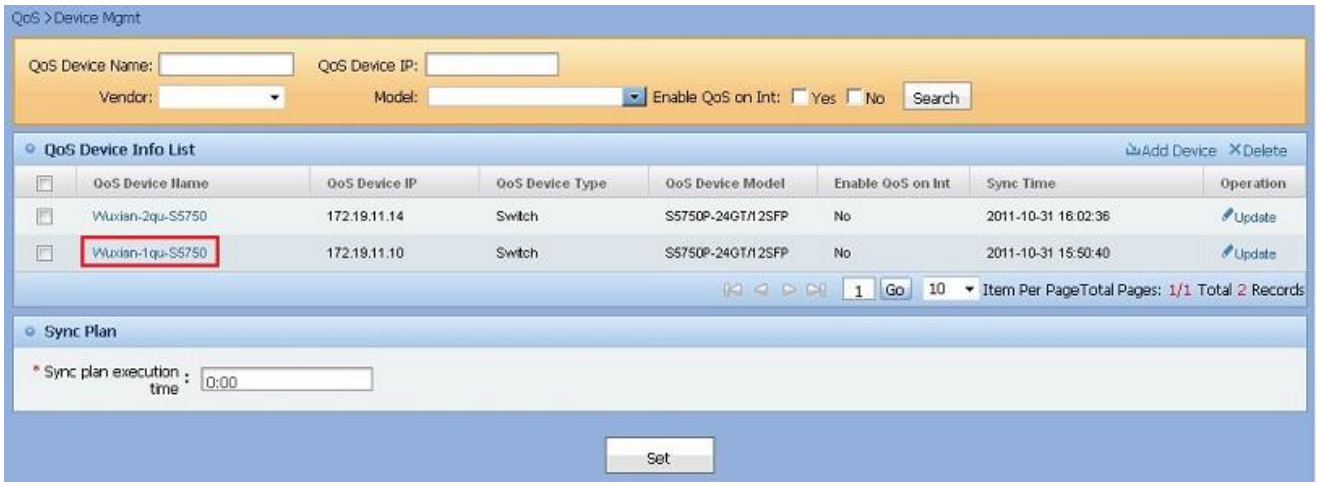


Figure 10.83. Enter **QoS Device Detail** Page

Click **Redeploy** icon under operation column on policy list, the system will prompt for your confirmation. As shown below:

Figure 10.84. Redeploy QoS Device Policy

Note After redeployment, the inconsistent sign will no longer exist.

10.3.11. Redeploy QoS Device Policy

On **QoS Device Detail** page, you can redeploy QoS policy on a device.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

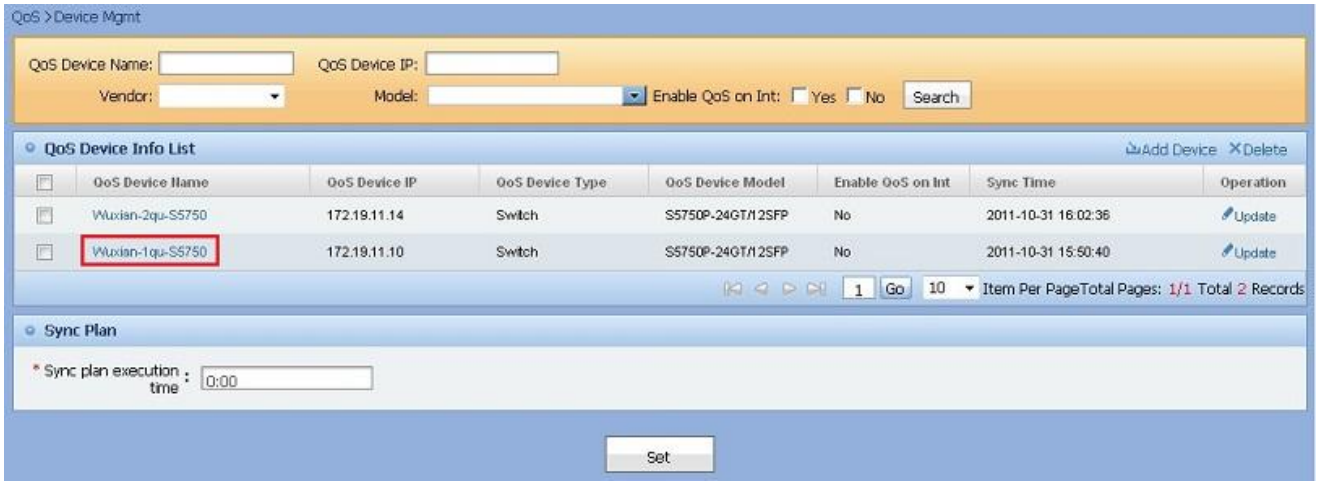


Figure 10.85. Enter **QoS Device Detail** Page

Click **Deploy QoS Policy** on policy list to enter **Select Policy** page. As shown below:

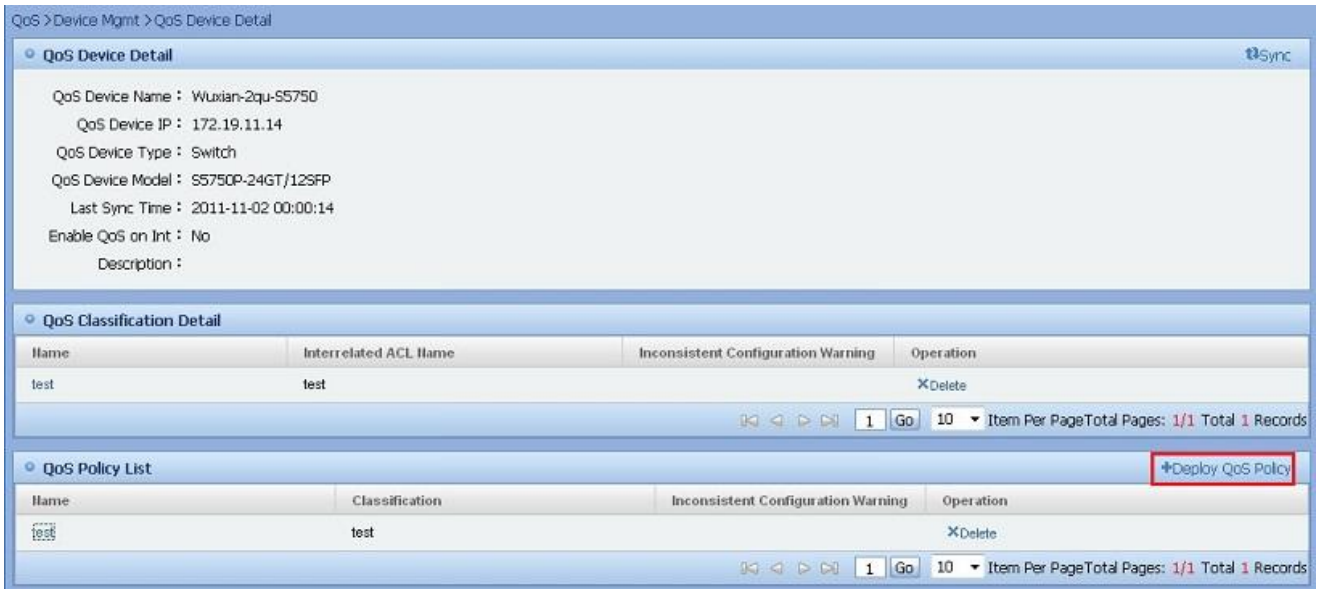


Figure 10.86. Enter **Select Policy** Page

The system will display policy list. As shown below:

Figure 10.87. **Select Policy** Page

Select the policy you want to deploy and click **Deploy** button. As shown below:

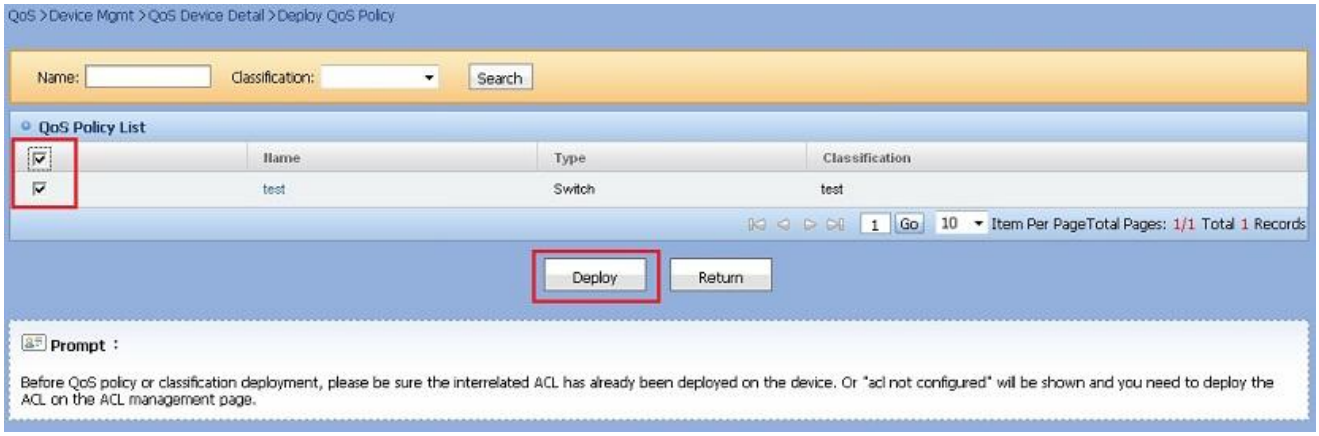


Figure 10.88. **Select Policy** Page

After deployment, the system will return to device detail page.

10.3.12. QoS Device Synchronization

On **QoS Device Detail** page, you can synchronize device.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

Figure10.89. Enter **QoS Device Detail** Page

Click **Sync** button on upright corner of device detail list to execute device synchronization. As shown below:

Figure 10.90. QoS Device Synchronization

10.3.13. QoS Device Classification Contrast

Enter device detail page, click **View inconsistent info** icon to conduct classification contrast.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

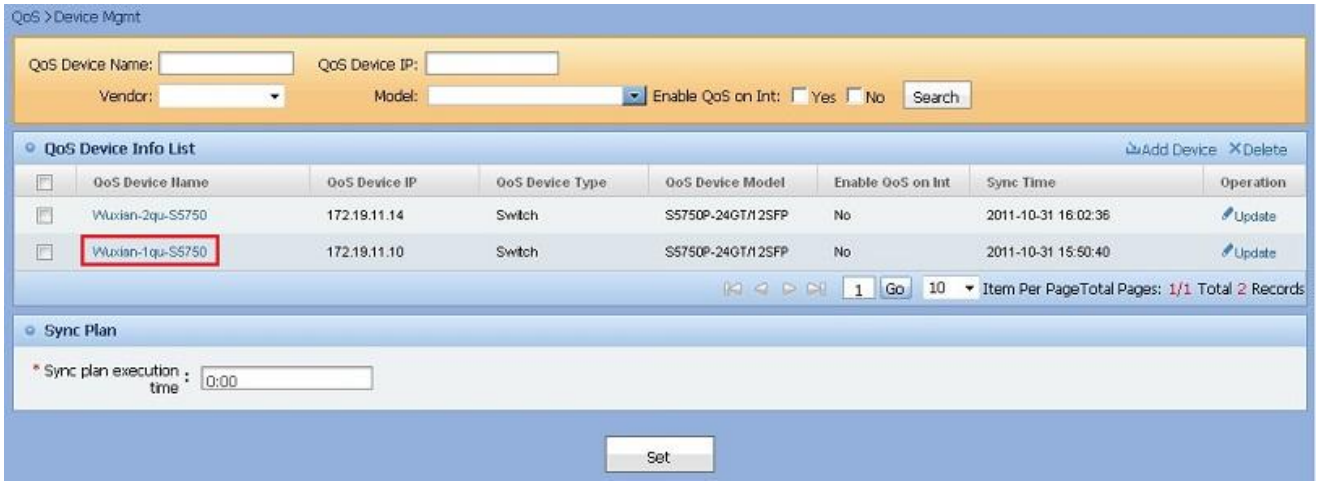


Figure 10.91. Enter **QoS Device Detail** Page

Click **View inconsistent info** icon under operation column of classification list to enter classification contrast page. As shown below:

Figure 10.92. Enter **Classification Contrast** Page

The difference between the device classification in the system and the actual device classification is displayed on classification contrast page. As shown below:

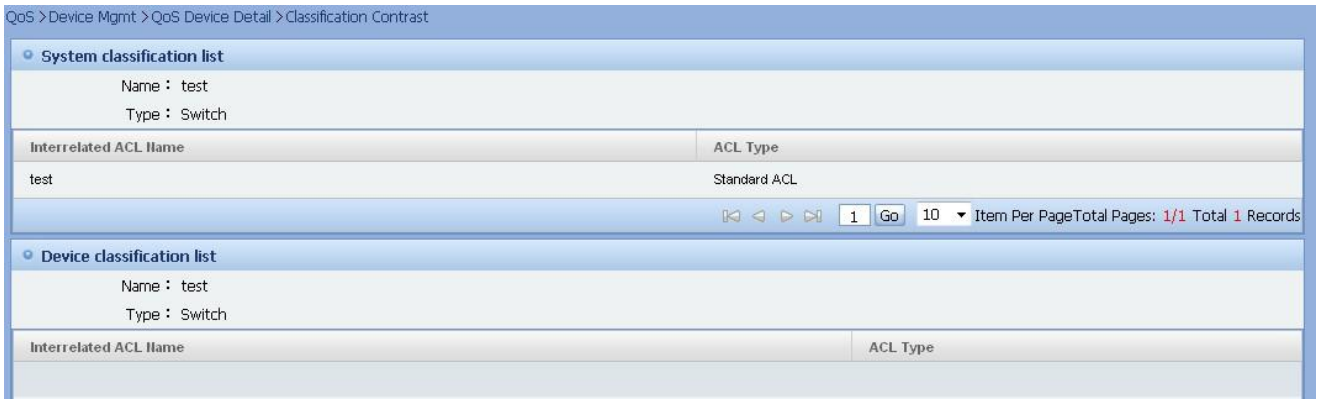


Figure 10.93. Classification Contrast Page

Note

If the device classification in the system is the same as the actual device classification, the contrast icon will not be shown.

10.3.14.QoS Policy Contrast

Enter device detail page, click contrast icon to conduct policy contrast.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **QoS Device Detail** page. As shown below:

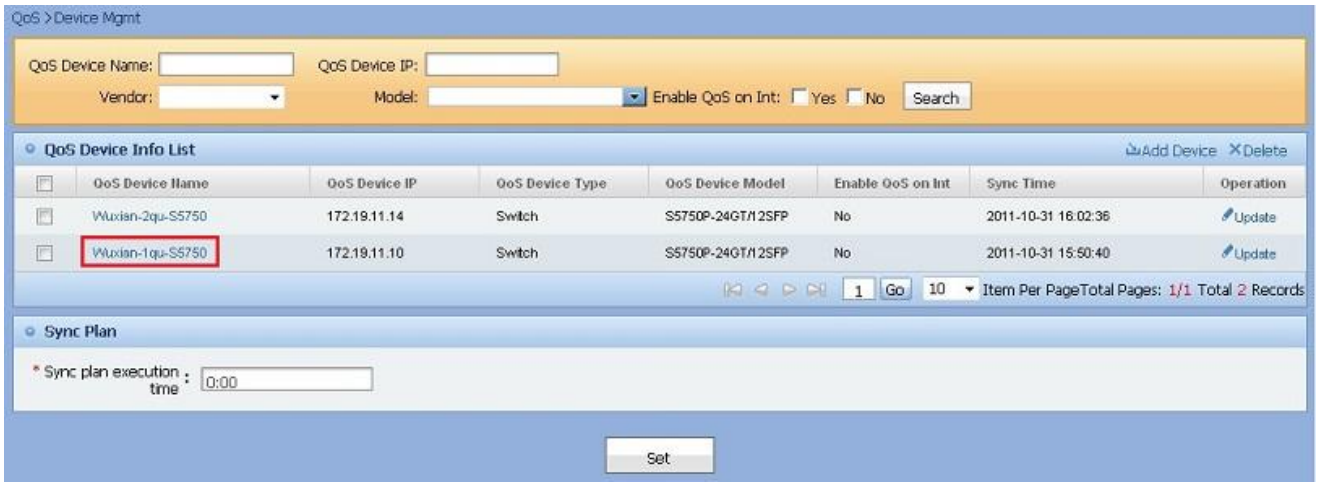


Figure 10.94. Enter **QoS Device Detail** Page

Click **View inconsistent info** icon under operation column on policy list to enter QoS policy contrast page. As shown below:

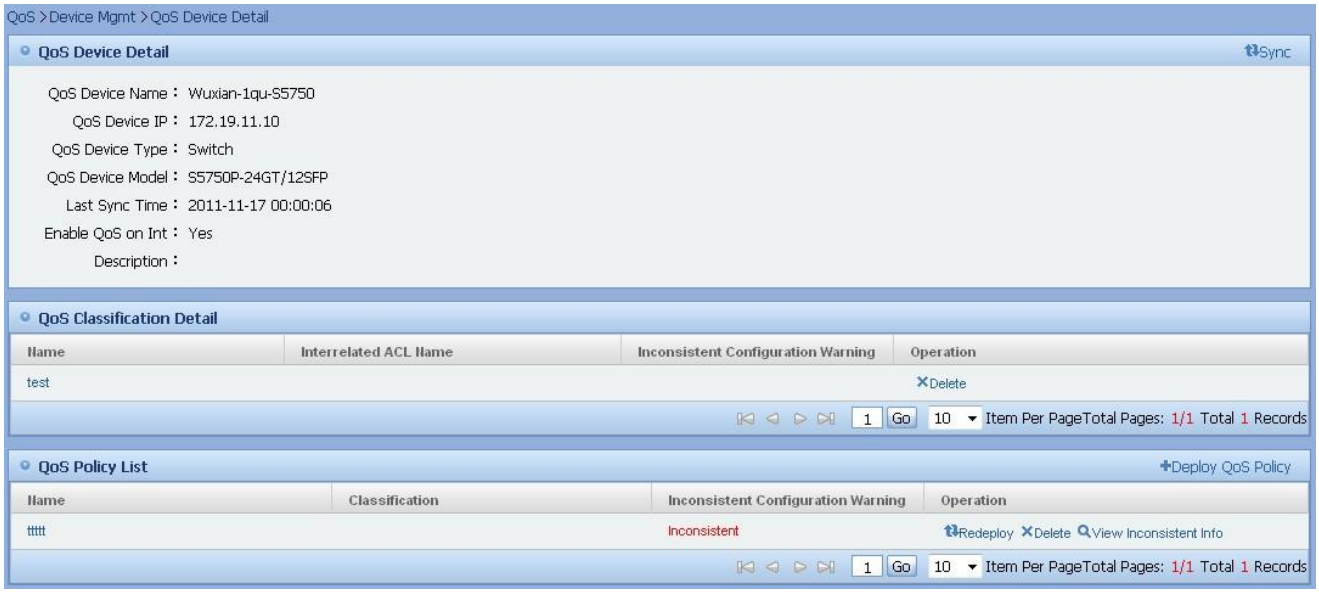


Figure 10.95. Enter Policy Contrast Page

The difference between the QoS Policy for the device in the system and the actual QoS Policy for the device will be displayed on QoS policy contrast page. As shown below:

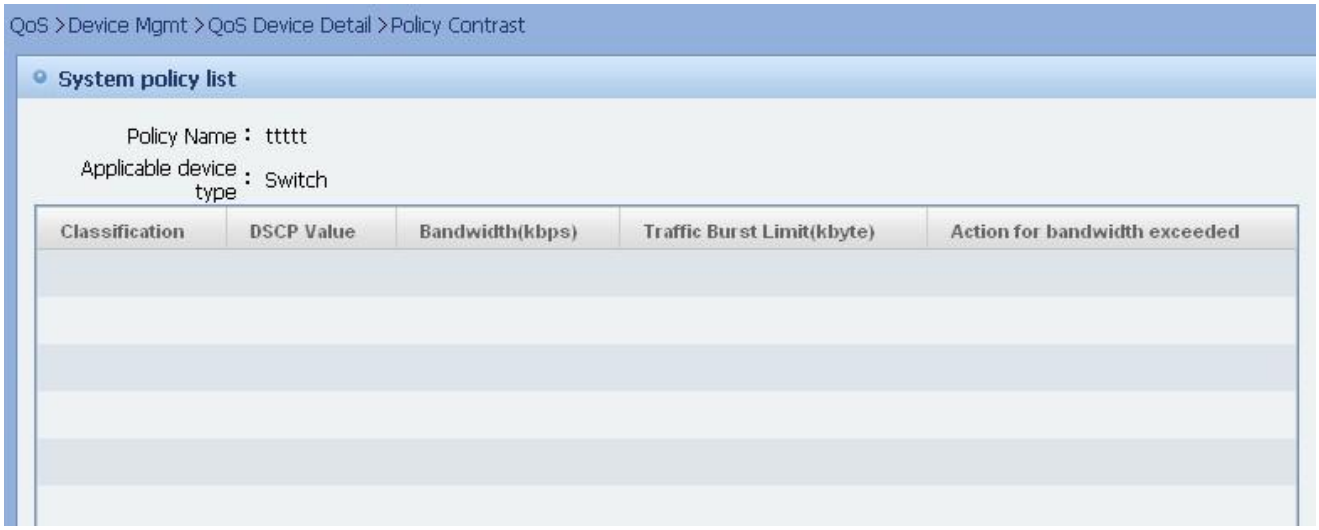


Figure 10.96. Policy Contrast Page

Note The contrast icon will not be shown if the QoS policy in the system is the same as the actual policy.

10.3.15. QoS Device Interface Detail

On **QoS Device Detail** page, you can click interface name to enter interface detail page.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **Device Detail** page. As shown below:

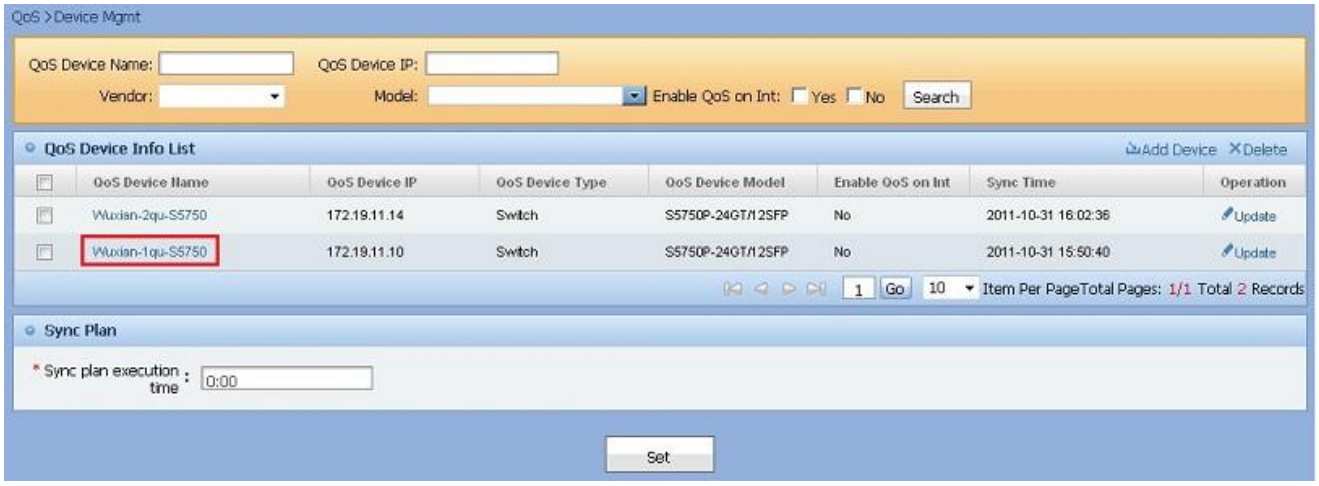


Figure10.97.Enter **Device Detail** Page

Click interface name on interface list to enter interface detail page. As shown below:

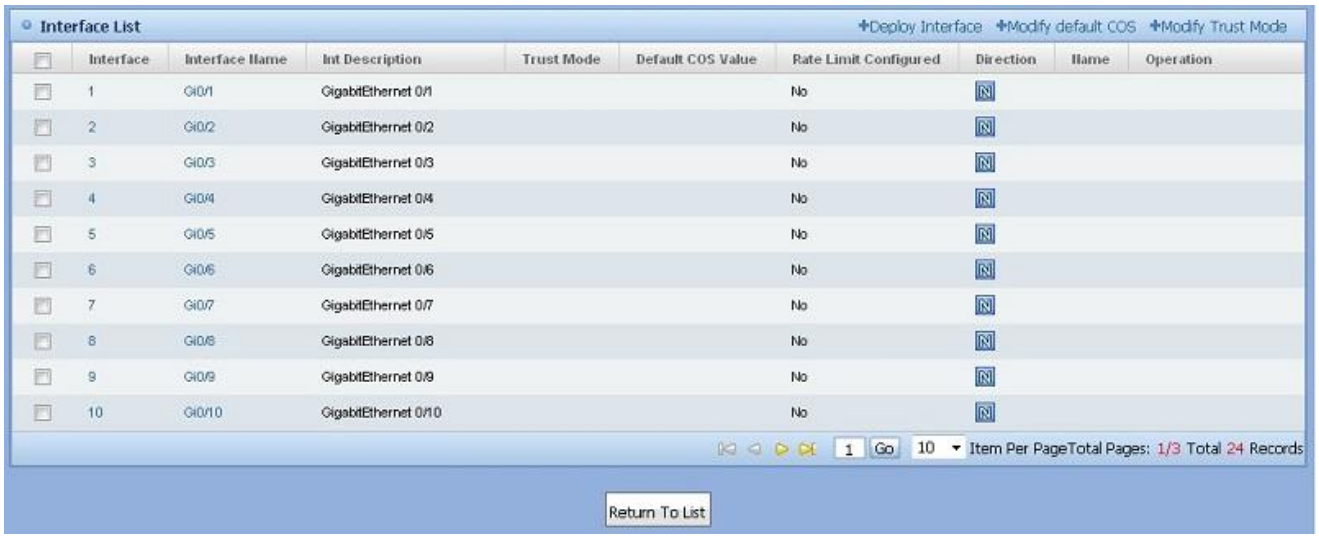


Figure 10.98. Enter **Interface Detail** Page

The following will be listed by the system: **Interface Rate Limit**, **Inbound Rate Limit Info** and **Outbound Rate Limit**. As shown below:

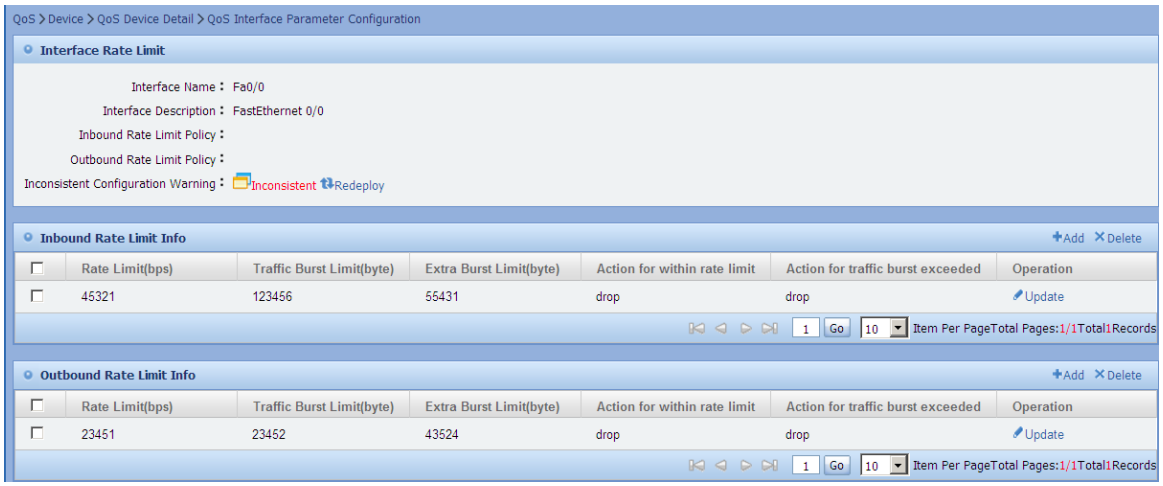


Figure 10.99. Enter **Interface Detail** Page

10.3.16. Delete the Policy Associated with a QoS Device Interface

On **QoS Device Detail** page, you can delete a policy associated with device interface.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **Device Detail** page. As shown below:

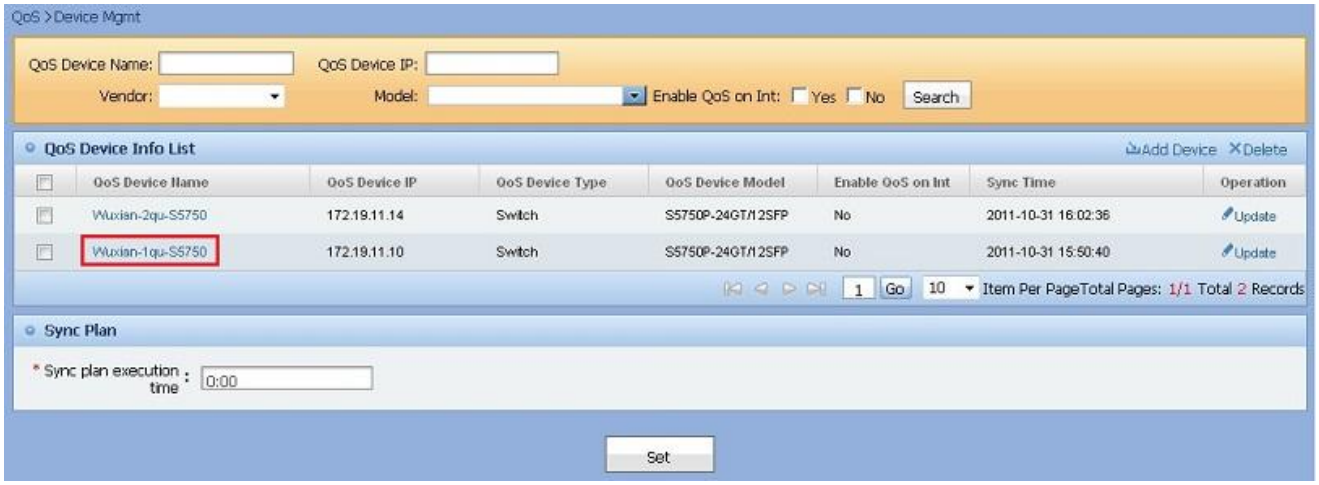


Figure 10.100. Enter **Device Detail** Page

Click the interface icon on interface list, the system will prompt for your confirmation. Click **Confirm** to remove policy associated with interface. As shown below:

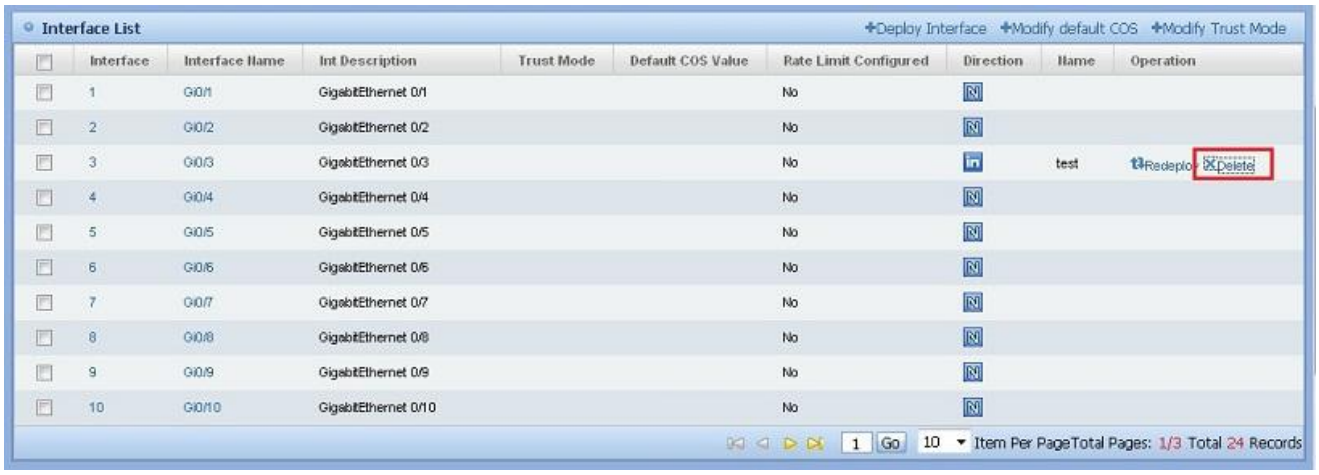


Figure 10.101. **Device Detail** Page

After deletion is accomplished, the system will show a success prompt and the information of deleted device interface is removed.

10.3.17. Delete Inbound Rate Limit Info Of Interface

On **QoS Device Interface Detail** page, you can delete inbound rate limit information of a device interface.

Operation Steps

1) Use **QoS Device Interface Detail** to enter interface detail page.

On detail page, select the column you want to delete on **Inbound Rate Limit Info** list, then click **Delete** button and the system will prompt for your confirmation. Click **OK** button for the deletion. As shown below:

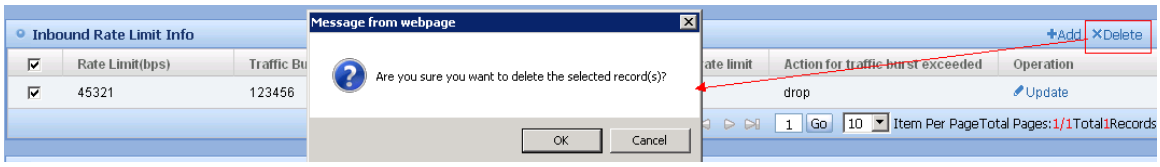


Figure 10.102. **Device Detail** Page

After deletion is accomplished, the system will show a success prompt and the deleted information is no longer displayed.

10.3.18. Delete Outbound Rate Limit Info Of Interface

On **QoS Device Interface Detail** page, you can delete outbound rate limit information of a device interface.

Operation Steps

1) Use **QoS Device Interface Detail** to enter interface detail page.

On detail page, select the column you want to delete on **Outbound Rate Limit Info** list, then click **Delete** button and the system will prompt for your confirmation. Click **OK** button for the deletion. As shown below:

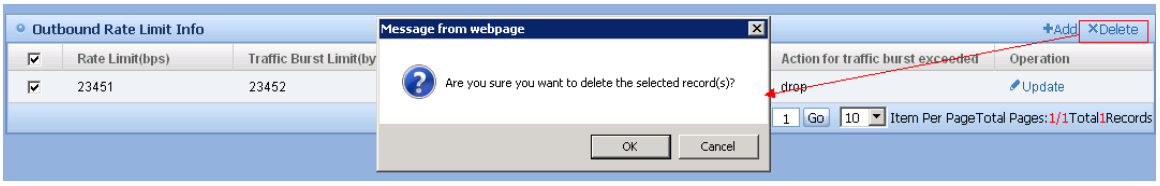


Figure 10.103. **Device Detail** Page

After deletion is accomplished, the system will show a success prompt and the deleted information is no longer displayed.

10.3.19. Add Inbound Rate Limit Info Of Interface

On **QoS Device Interface Detail** page, you can add inbound rate limit information of device interface.

Operation Steps

1) Use **QoS Device Interface Detail** to enter interface detail page.

On detail page, click **Add** button on **Inbound Rate Limit Info** list to enter add page. As shown below:

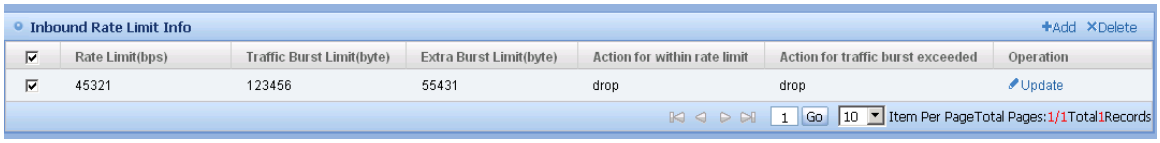


Figure 10.104. **Device Interface Detail** Page

On add page, input related value and click **Add**, the system will save the input value and return to interface detail page. As shown below:

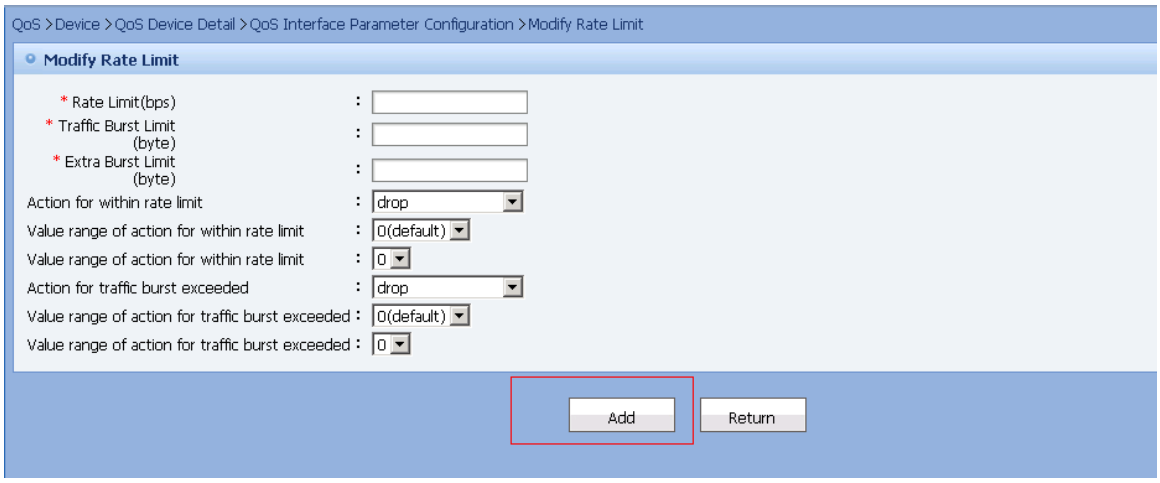


Figure 10.105. Add Page

10.3.20. Add Outbound Rate Limit Info Of Interface

On **QoS Device Interface Detail** page, you can add outbound rate limit information of device interface.

Operation Steps

1) Use **QoS Device Interface Detail** to enter interface detail page.

On detail page, click **Add** button on **Outbound Rate Limit Info** list to enter add page. As shown below:

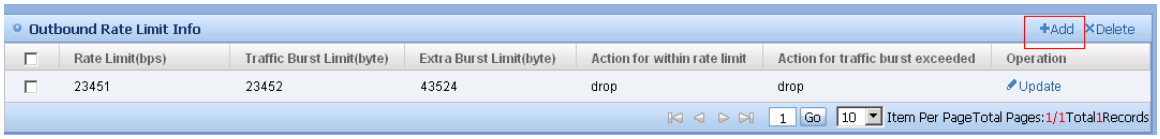


Figure 10.106. **Device Interface Detail** Page

On the add page, enter related value and click **Add**, the system will save the input value and return to interface detail page. As shown below:

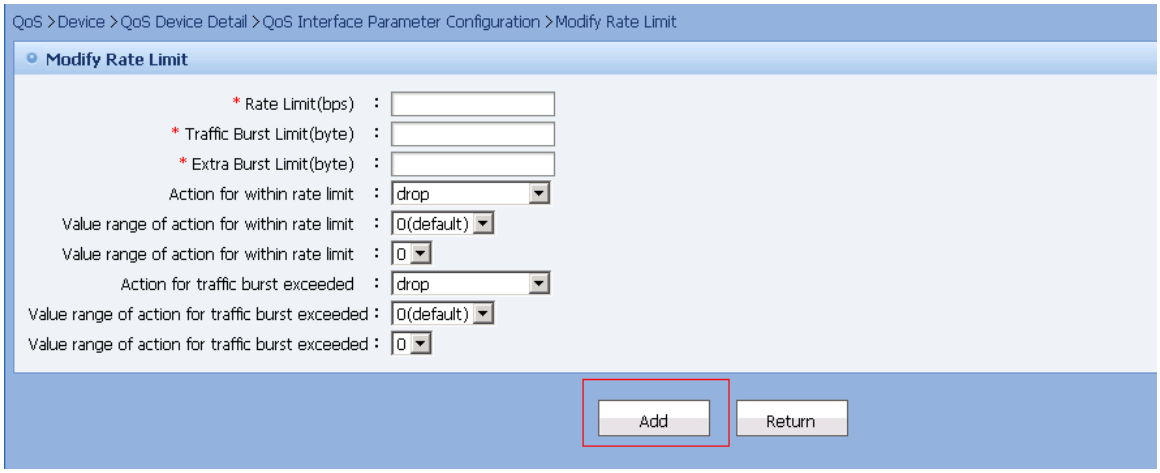


Figure 10.107. Add Page

10.3.21. QoS Device Interface Deployment

Enter QoS device detail page, click **Deploy Interface** on interface list to deploy.

Operation Steps

1) Enter QoS device management page, click **Device Name** link to enter **Device Detail** page. As shown below:

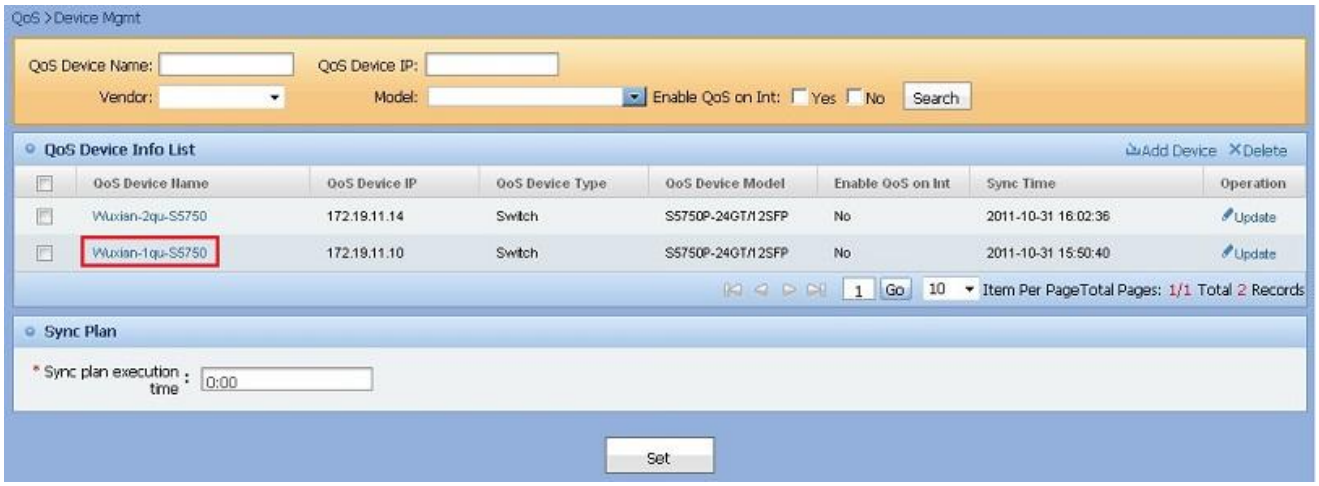


Figure 10.108. Enter **Device Detail** Page

On **Device Detail** page, click **Deploy Interface** button to deploy the interface. As shown below:

Figure10.109. **Device Detail** Page

On **Deploy Interface** page, select **Filter Direction**, **Select Policy** and **Select Interface**, then click **Deploy Interface** button to deploy the interface. As shown below:

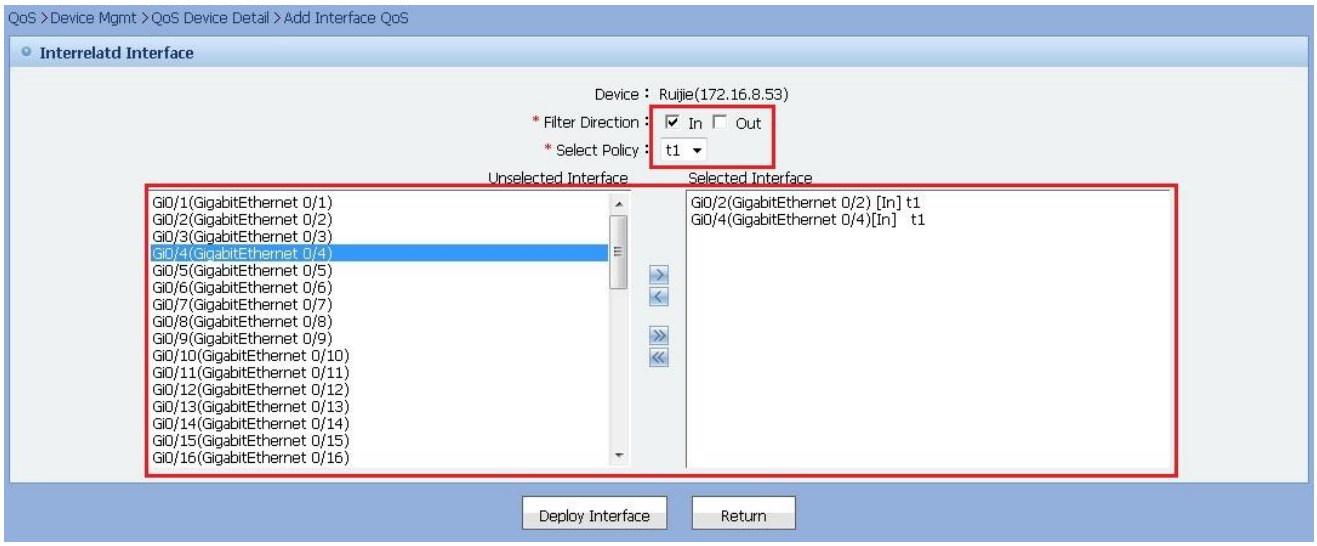


Figure 10.110. **Device Detail** Page

After the deployment is accomplished, the system will return to device detail page.

10.3.22. Redeploy Interface Information

On **QoS Device Interface Detail** page, you can redeploy the interface.

Operation Steps

1) Use **QoS Device Interface Detail** to enter interface detail page.

On detail page, click **Redeploy** button on **Interface Rate Limit** list to redeploy the interface information. As shown below:

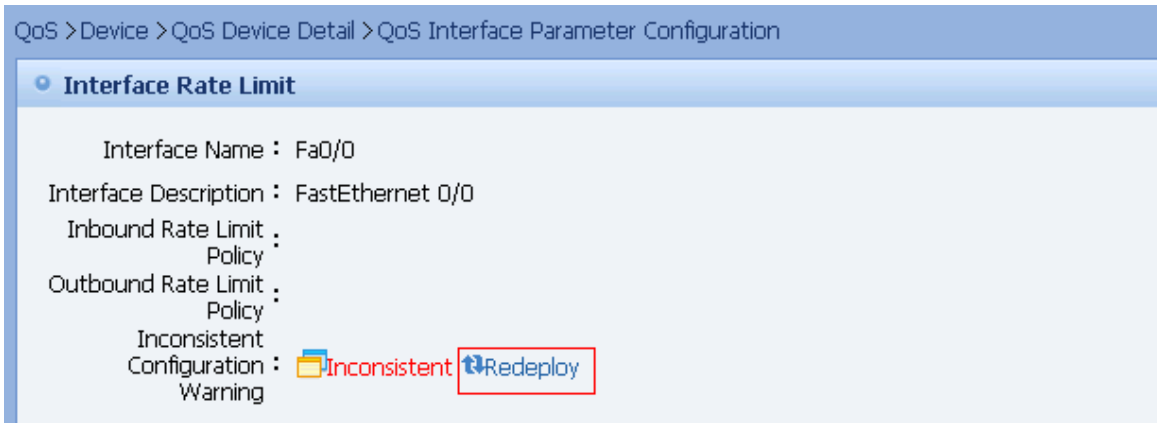


Figure 10.111. Device Interface Detail Page

10.4. QoS Deployment Management

QoS deployment management targets at generating deployment plan for QoS policy, QoS classification and interface batch deployed to device.

- Search QoS Deployment Plan
- Delete QoS Deployment Plan
- Modify QoS Deployment Plan
- Modify QoS Interface Deployment Plan
- Stop Plan
- Start Plan
- View Deployment Plan
- View Deployment Plan Execution Log
- Add QoS Deployment Plan
- Add QoS Interface Deployment Plan

10.4.1. Search QoS Deployment Plan

On **QoS Deployment Plan Management** page, you can enter plan name to search the QoS deployment plan.

Operation Steps

Enter **QoS Deployment Plan Management** page, input plan name then click **Search** button, the system will show the matched QoS deployment plan list. As shown below:

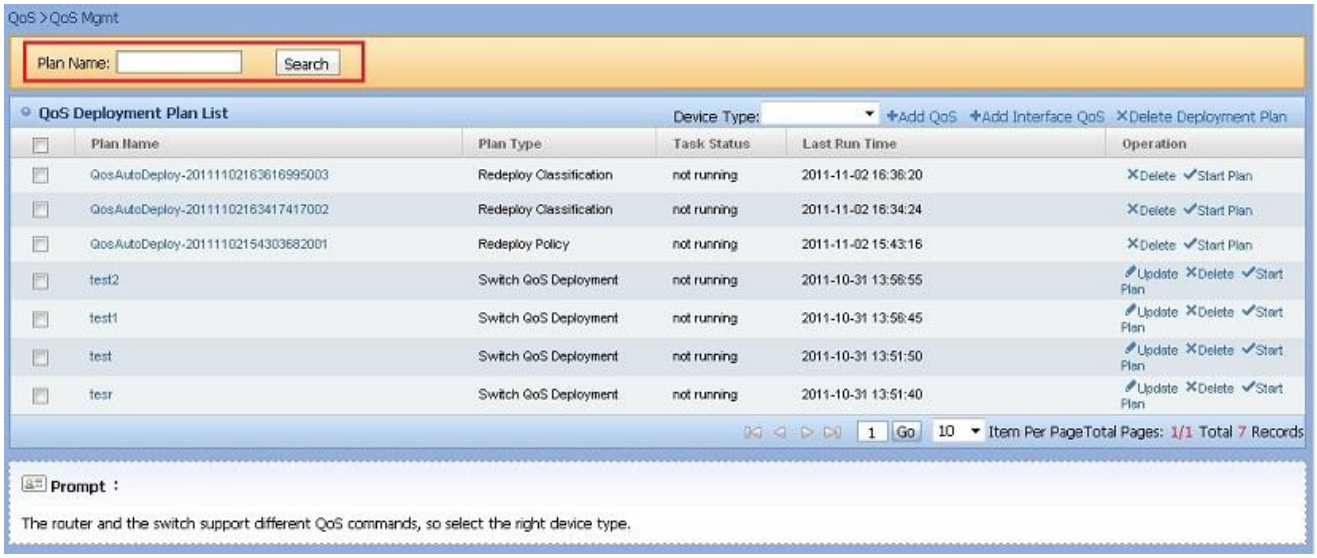


Figure 10.112. Search QoS Deployment Plan

10.4.2. Delete QoS Deployment Plan

On **QoS Deployment Plan Management** page, you can delete the QoS deployment plan one by one.

Operation Steps

Enter **QoS Deployment Plan Management** page, click **Delete** button on deployment plan list, the system will prompt **Are you sure to delete this plan?** for confirmation. Click **Confirm** to delete the plan from system. As shown below:

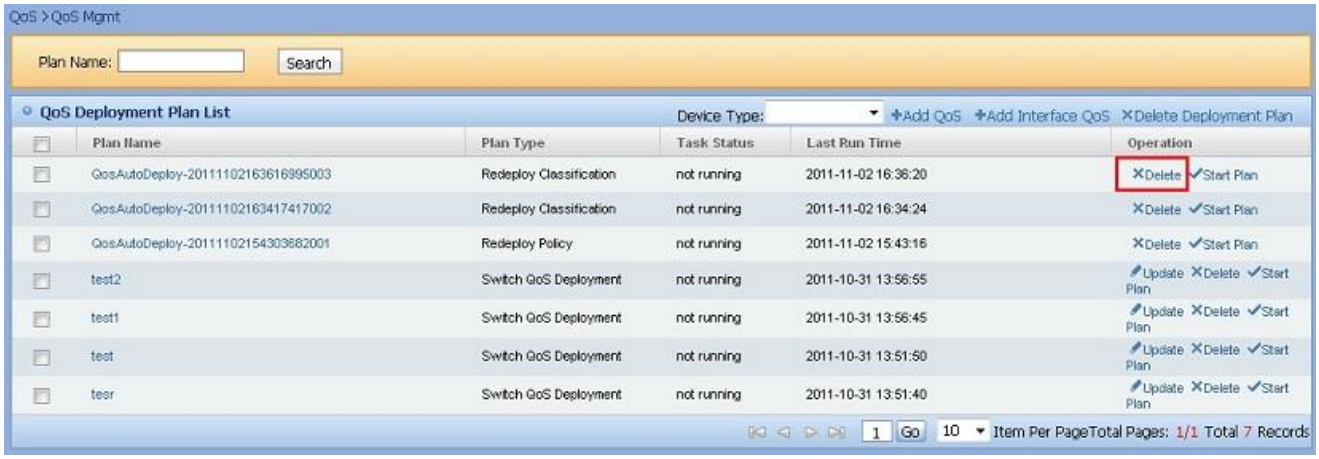


Figure 10.113. Delete QoS Deployment Plan

10.4.3. Modify QoS Deployment Plan

On **QoS Deployment Plan Management** page, the QoS deployment can be modified.

Operation Steps

1) On **QoS Deployment Plan Management** page, select the QoS deployment plan with plan type **QoS Deployment** and click **Update** button to enter **Modify QoS Deployment Plan** page. As shown below:

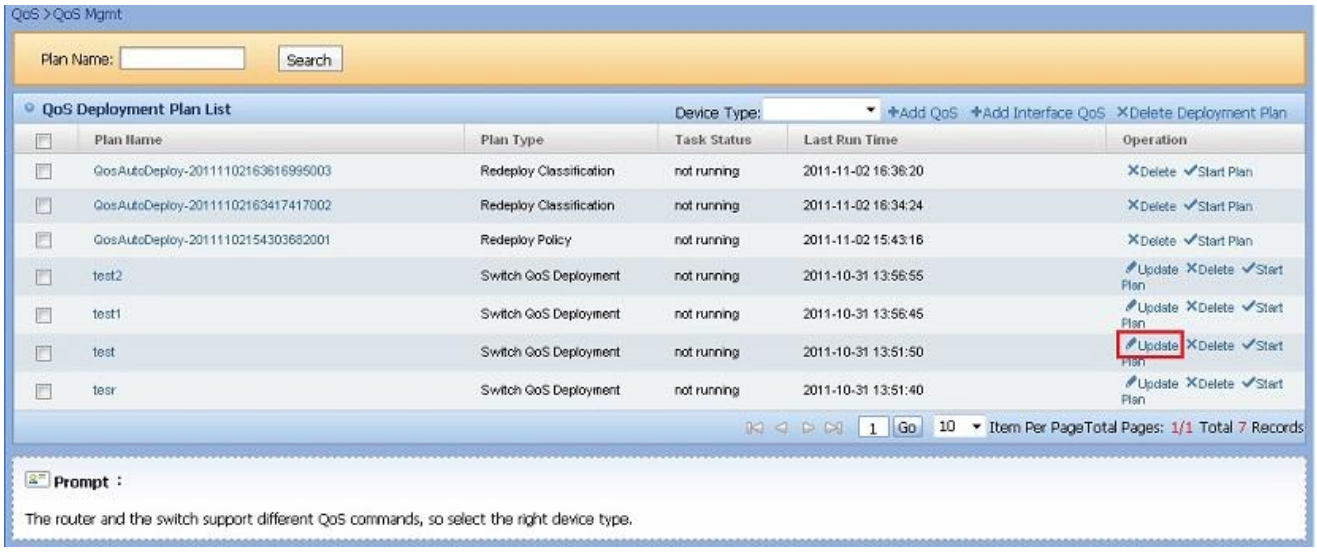


Figure 10.114. Enter QoS Deployment Plan Modification Page

2) Enter **Selected Device List** page

Figure 10.115. Enter **Selected Device List** page. As shown below:

3) Click **Select Device** button, the device list page will be popped up for selection. As shown below:

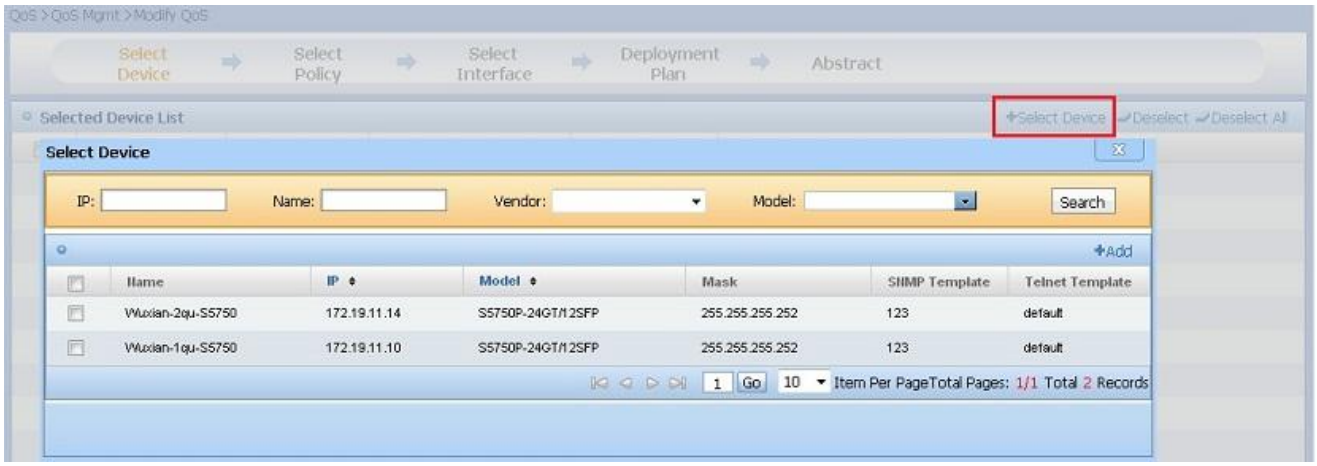


Figure 10.116. Select Device

4) After selecting device, click **Add** button, the following page will be shown:

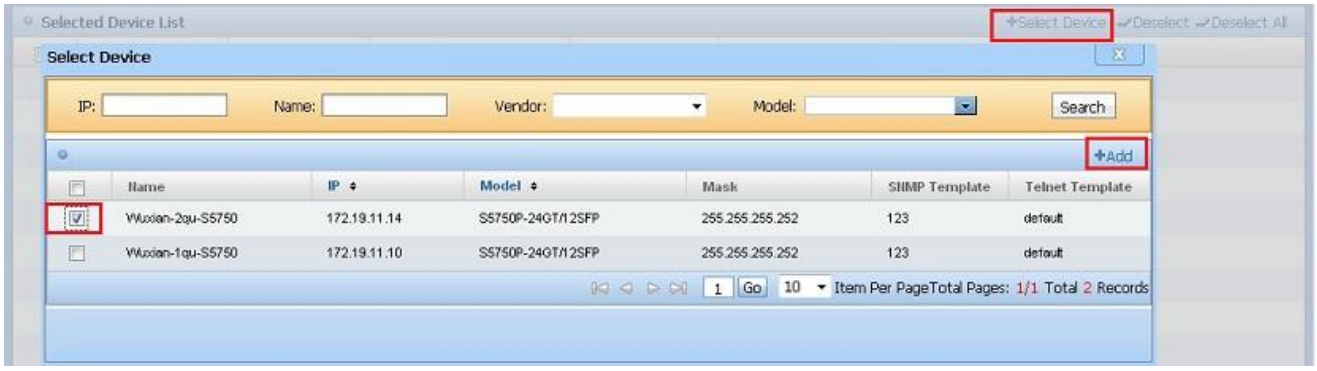


Figure 10.117. Add Device

5) Enter **Selected Device List** page, then click **Next: Select QoS Policy** button. As shown below:

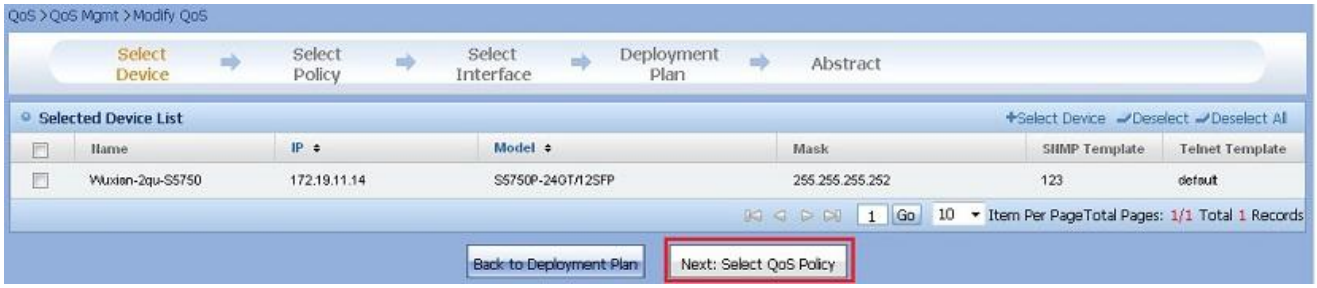


Figure 10.118. Next: Select QoS Policy

6) Enter **Selected QoS Policy List** page. As shown below:

Figure 10.119. Select QoS Policy

7) Click **Select QoS Policy** button to enter **QoS Policy List** page for selection. As shown below:

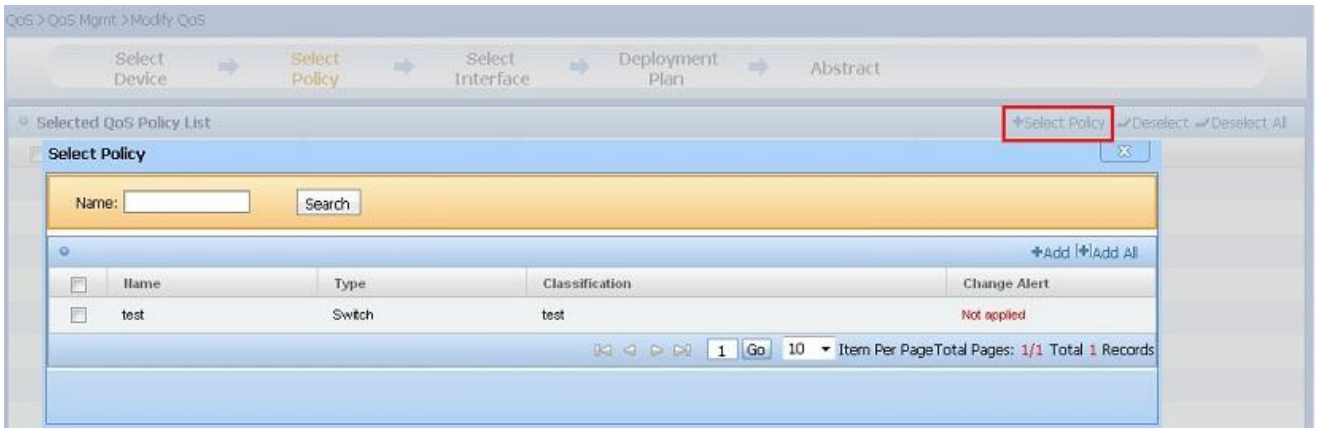


Figure 10.120. Select QoS Policy

8) After the QoS policy is selected, click **Add** button. As shown below:

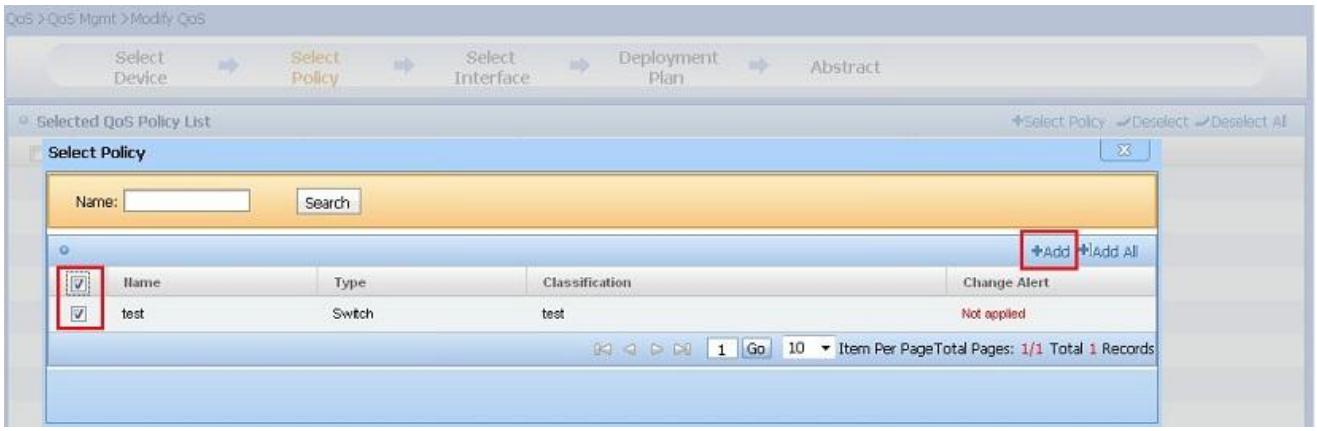


Figure 10.121. Add QoS Policy

9) Enter **Selected QoS Policy List** page, click **Previous: Select Device** to return to **Selected Device List** page. As shown below:

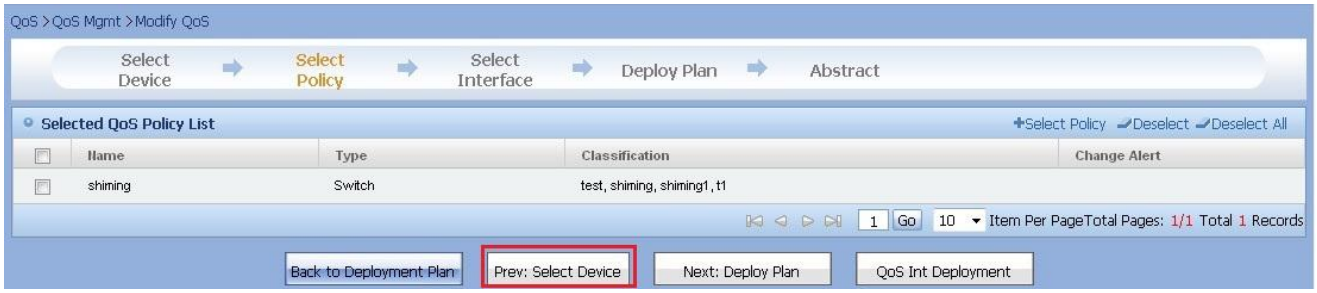


Figure 10.122. Previous: Select Device

10) Enter **Selected QoS Policy List** page, click **Deploy Plan** button to enter **Deploy Plan** page. As shown below:

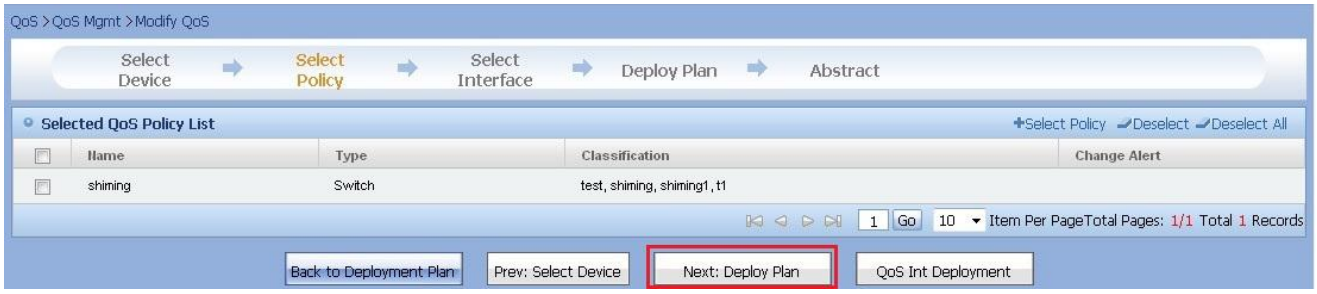


Figure 10.123. Deploy Plan

11) Enter **Selected QoS Policy List** page, click **QoS Interface Deployment** button to enter **Select Interface** page. As shown below:

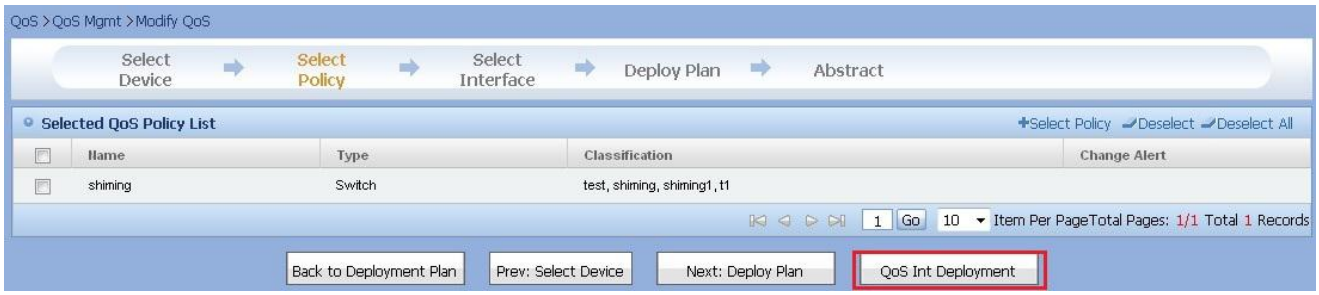


Figure 10.124. QoS Interface Deployment

12) Enter **Select Interface** page, it shows **Selected Device List**, click the button of operation column on **Selected Device List** to configure the interface.

Figure 10.125. Select Interface

13) Enter **Device Interrelated Interface** page, it shows the deployed interfaces.

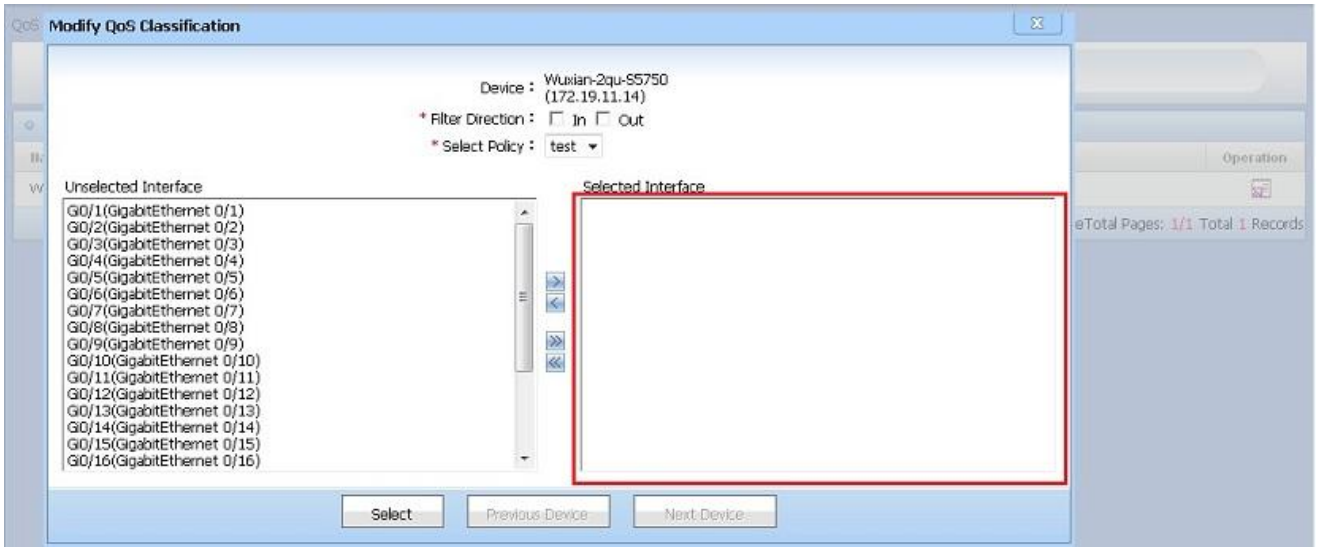


Figure 10.126. Device Interrelated Interface

14) Select interface in **Filter Direction**, **QoS Policy** and **Unselected Interface** list, then double click it or click **>** button to add the interface into **Selected Interface** list, the selected interface will be displayed with format **Interface Name[Filter Direction]Qos Policy Name**.

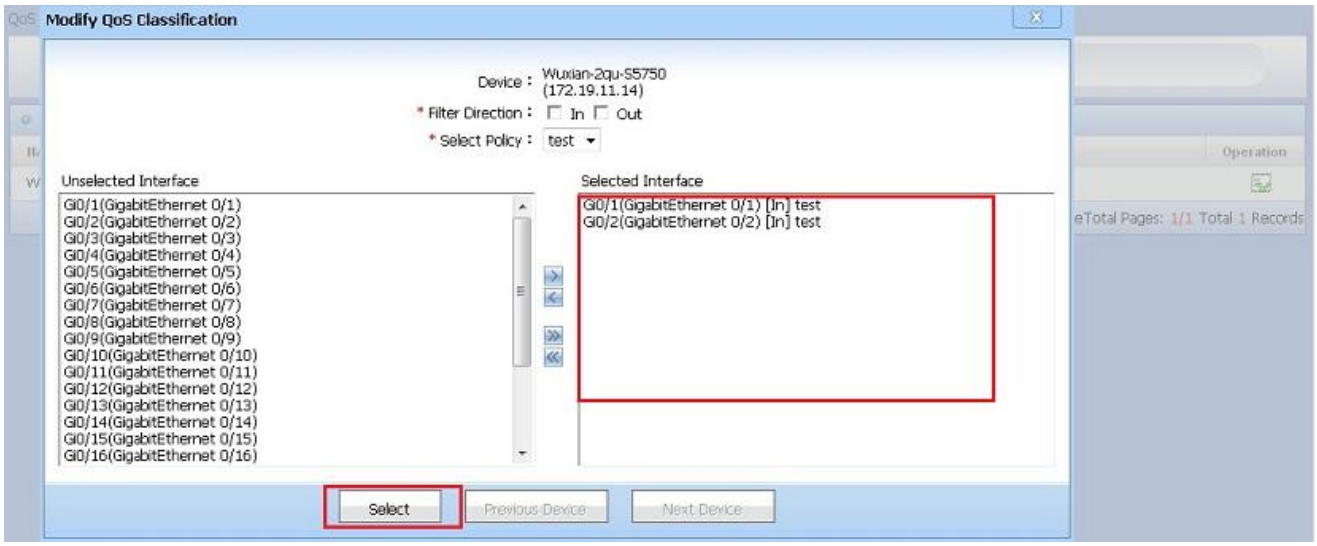


Figure 10.127. Add QoS Interface Deployment

15) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Previous: Select QoS Policy** button to return to **Selected QoS Policy List** page. As shown below:

Figure 10.128. Previous: Select QoS Policy

16) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Next: Deploy Plan** button. As shown below:

Figure 10.129. Next: Deploy Plan

17) Enter **Deploy Plan** page, click **Previous: Select Interface** button to return to **Select Interface** page. As shown below:

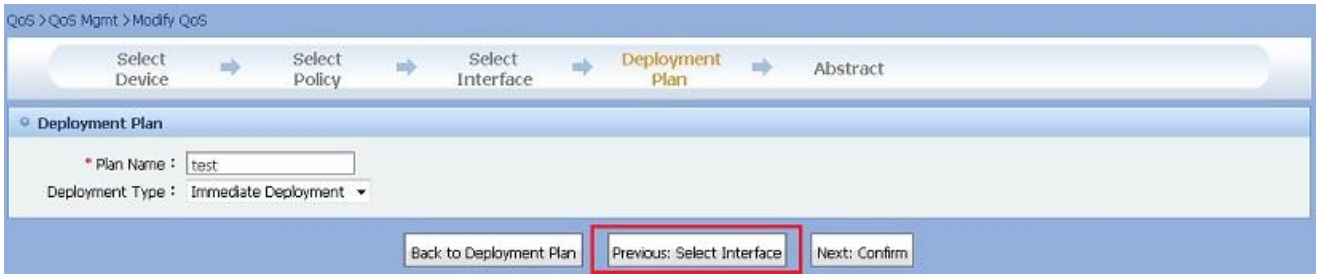


Figure 10.130. Previous: Select Interface

18) Enter **Deploy Plan** page, modify plan name and select deployment type, then click **Next: Confirm** button. As shown below:

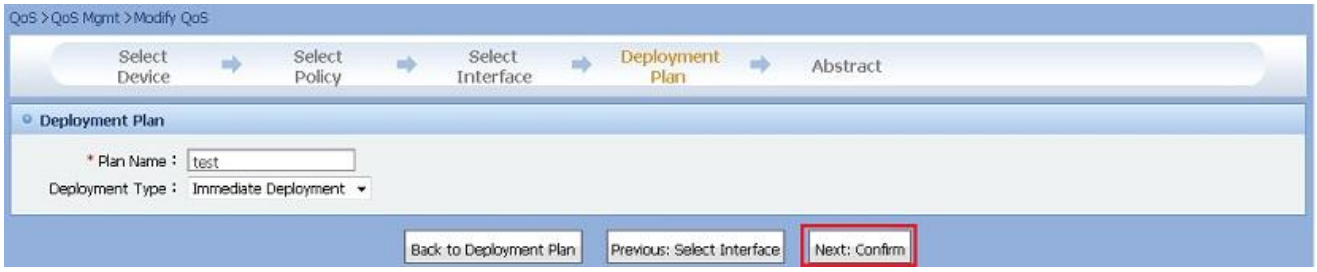


Figure 10.131. Next: Confirm

19) Enter **Confirm** page, click **Previous: Deploy Plan** to return to **Deploy Plan** page. As shown below:

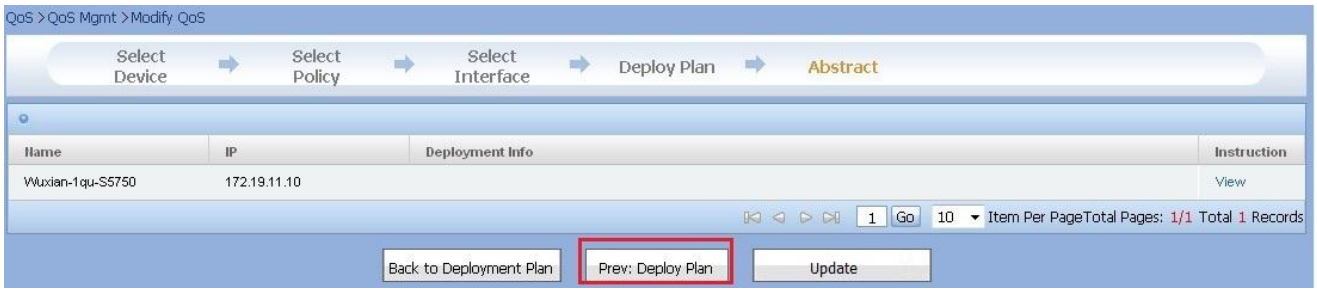


Figure 10.132. Previous: Deploy Plan

20) Click **View** button to view generated instructions on a pop-up page. As shown below:

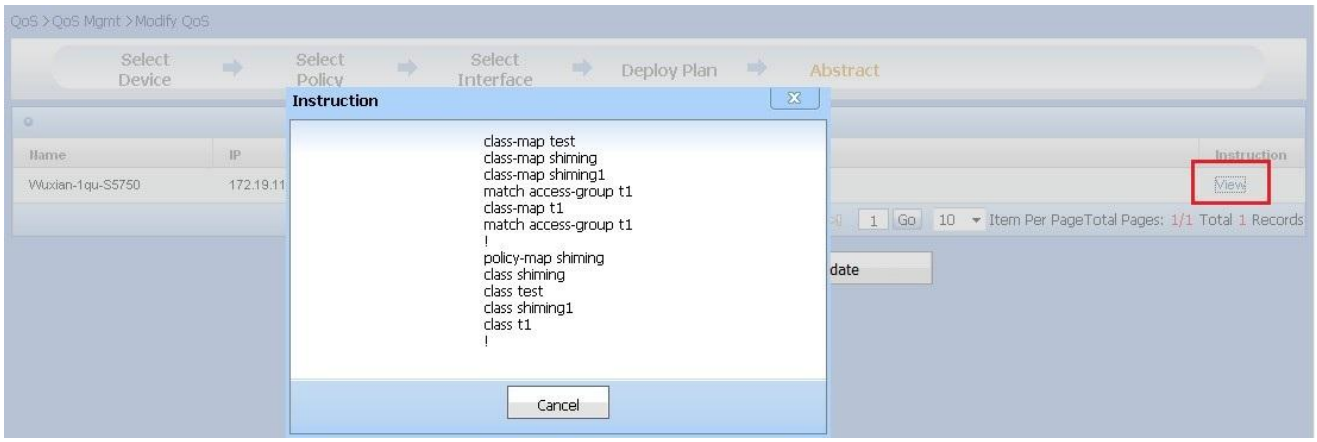


Figure 10.133. View Instructions

21) Click **Update**, the system will update the deployment plan then return to **QoS Deployment Plan Management** page. As shown below:

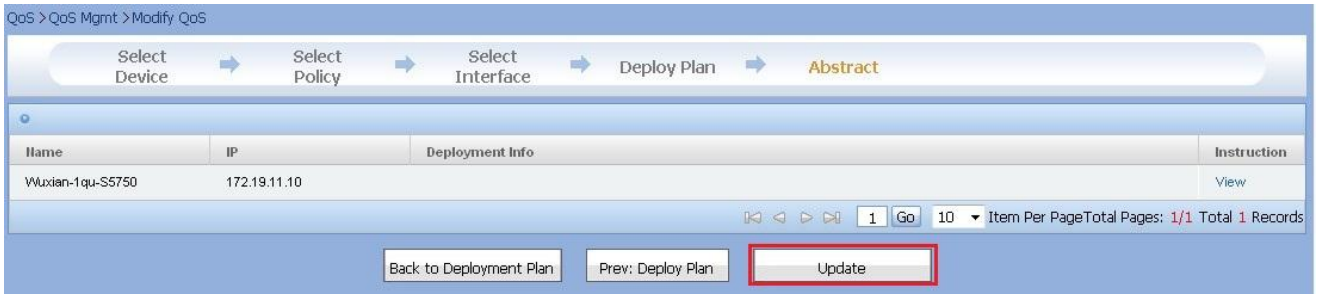


Figure 10.134. Update QoS Deployment Plan

On **Device List** for selection page, click **Add All** button to add all devices into **Selected Device List**. You don't need to select any device for **Add All** operation.

On **Selected Device List** page, click **Deselect** or **Deselect All** button to remove devices from **Selected Device List**. You don't need to select any device for **Deselect All** operation.

On **Selected QoS Policy List** page, click **Deselect** or **Deselect All** button to remove QoS policies from **Selected QoS Policy List**. You don't need to select any QoS policy for **Deselect All** operation.

On **QoS Policy List** for selection page, click **Add All** button to add all QoS policies into **Selected QoS Policy List**. You don't need to select any QoS policy for **Add All** operation.

On the **Unselected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **>** button to add single interface, you can also click **>>** button to select interface in batches.

On the **Selected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **<** button to remove single interface, you can also click **<<** button to remove interface in batches.

On **Device Interrelated Interface** page, click **Previous Device** button to show the **Selected Interface** information of previous device.

On **Device Interrelated Interface** page, click **Next Device** button to show the **Selected Interface** information of next device.

Note

The plan automatically generated by the system cannot be modified.

If there is no selected device, you cannot click **Next: Select QoS Policy** button.

If there is no selected QoS policy, you cannot click **QoS Interface Deployment** button.

If no interface is selected, you cannot click **Next: Deploy Plan** button.

After modifying a deployment plan, you must **Start Plan** before the plan can be executed.

10.4.4. Modify QoS Interface Deployment Plan

On **QoS Deployment Plan Management** page, you can modify QoS interface deployment plan.

Operation Steps

1) Enter **QoS Deployment Plan Management** page, select QoS deployment plan with plan type **Interface Deployment** and click **Update** button. As shown below:

Figure 10.135. Enter QoS Interface Deployment Plan Modification Page

2) Enter **Selected Device List** page. As shown below:

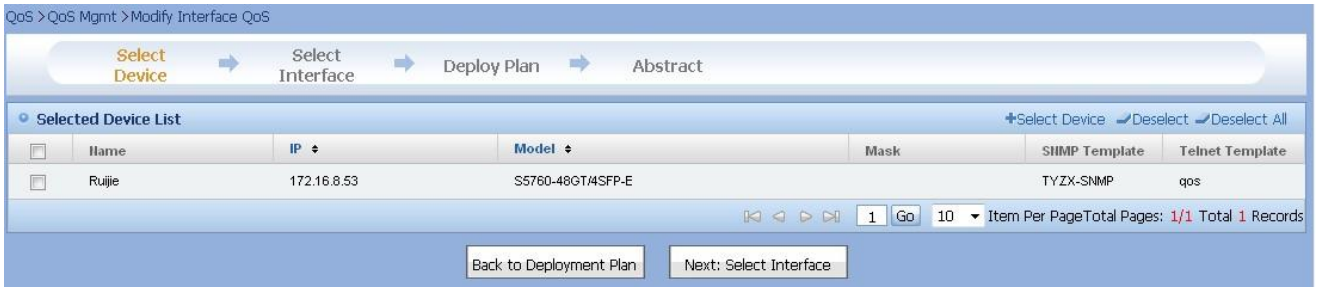


Figure 10.136. Enter **Selected Device List** Page

3) Click **Select Device** button, the **Device List** for selection page will be popped up. As shown below:

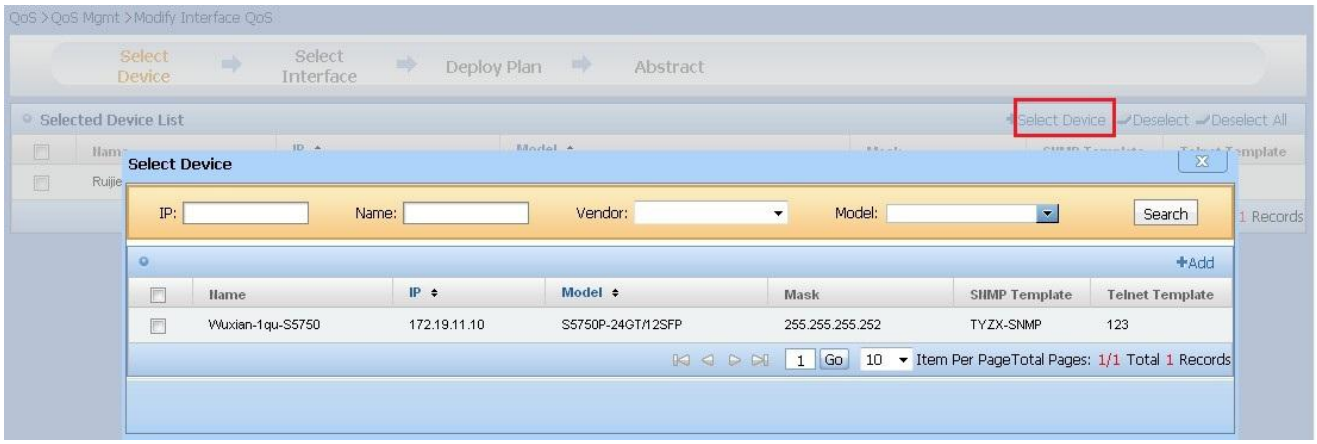


Figure 10.137. Select Device

4) After selecting device, click **Add**. As shown below:

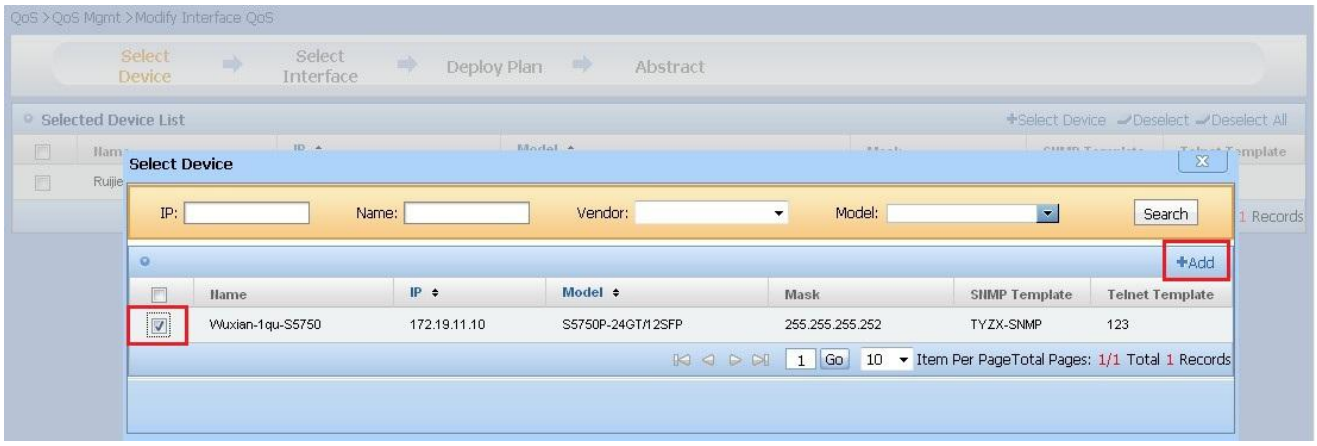


Figure 10.138. Add Device

5) Enter **Selected Device List** page, click **Next: Select Interface** button. As shown below:

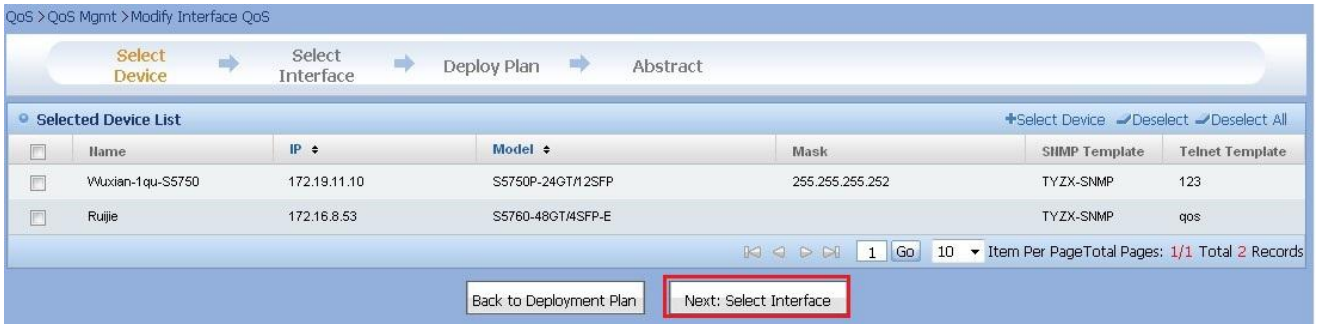


Figure 10.139. Next: Select Interface

6) Enter **Select Interface** page, it shows **Selected Device List**. Click icon on operation column of **Selected Device List** to configure interface.

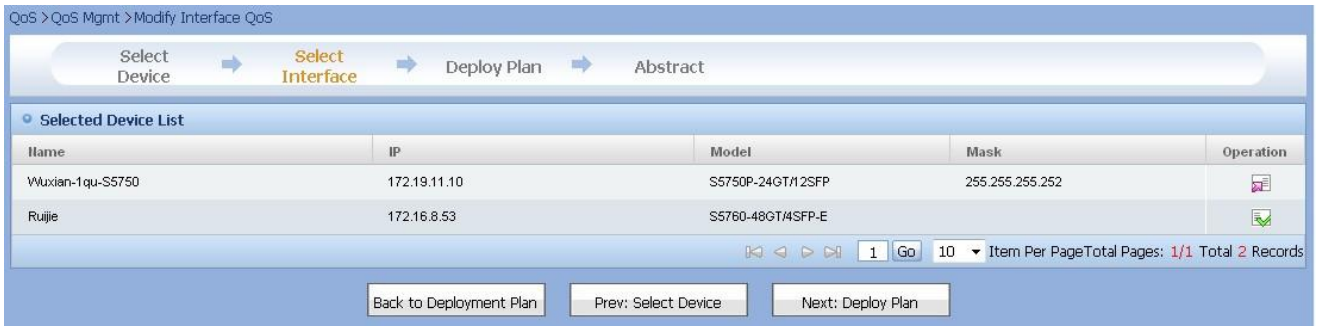


Figure 10.140. Select Interface

7) Enter **Device Interrelated Interface** page, the **Selected Interface** box shows the deployed interfaces.

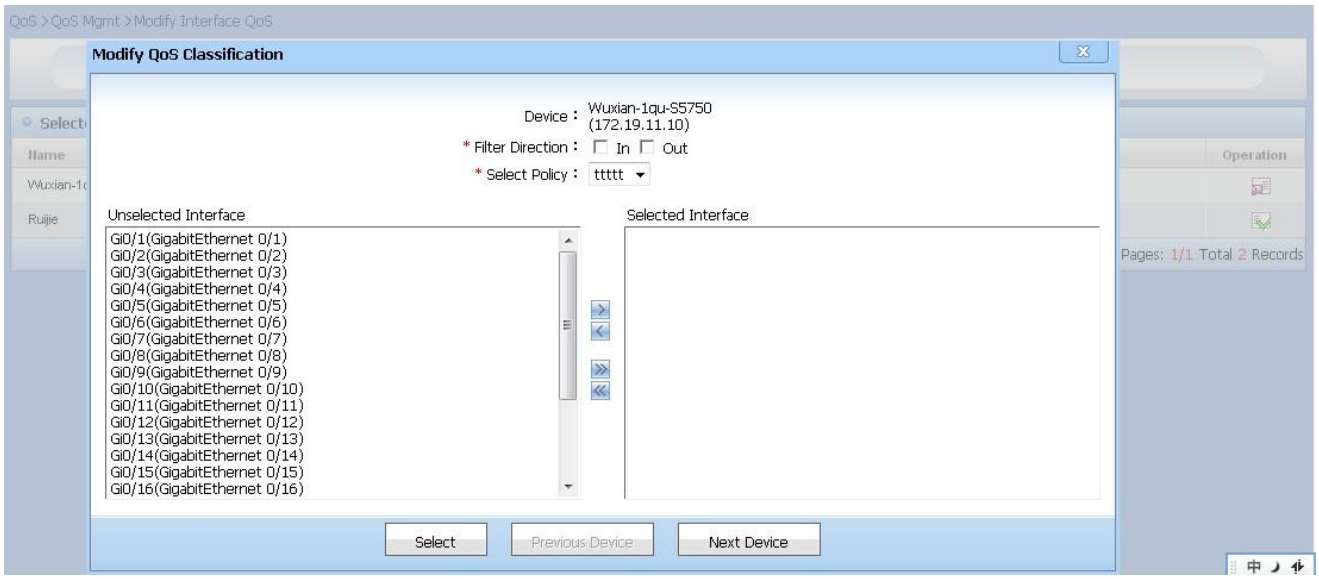


Figure 10.141. Device Interrelated Interface

8) Select interface in **Filter Direction**, **QoS Policy** and **Unselected Interface** list, then double click it or click **>** button to add the interface into **Selected Interface** list, the selected interface will be displayed with format **Interface Name[Filter Direction]Qos Policy Name**.

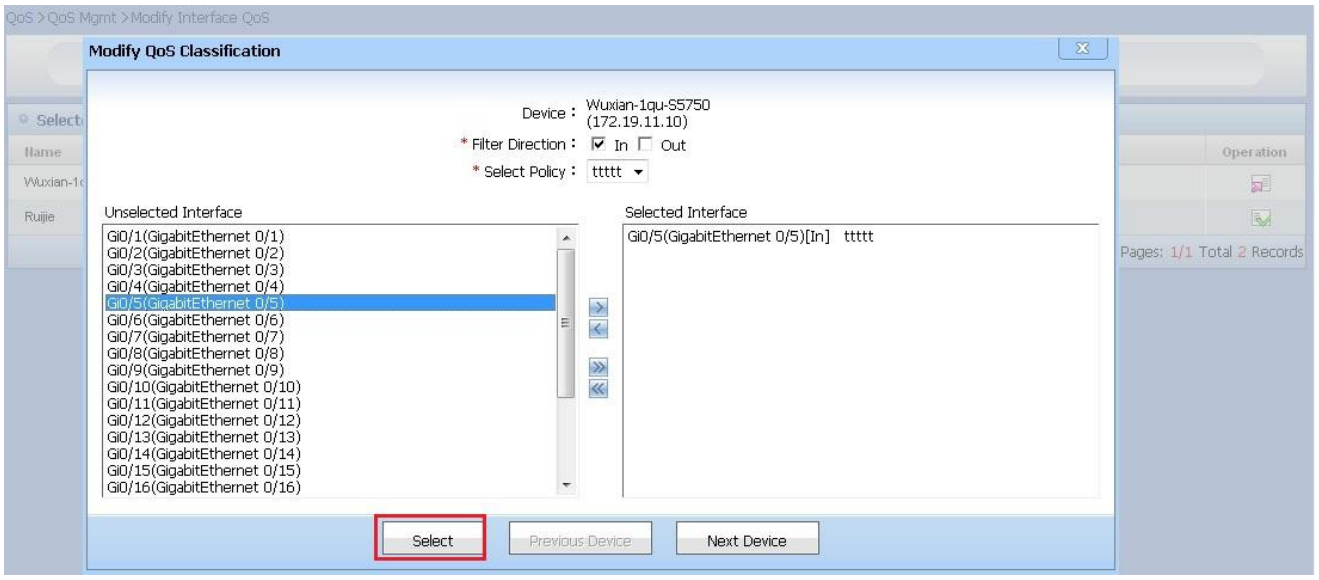


Figure 10.142. Add QoS Interface Deployment

9) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Previous: Select Device** button to return to **Selected QoS Device List** page. As shown below:

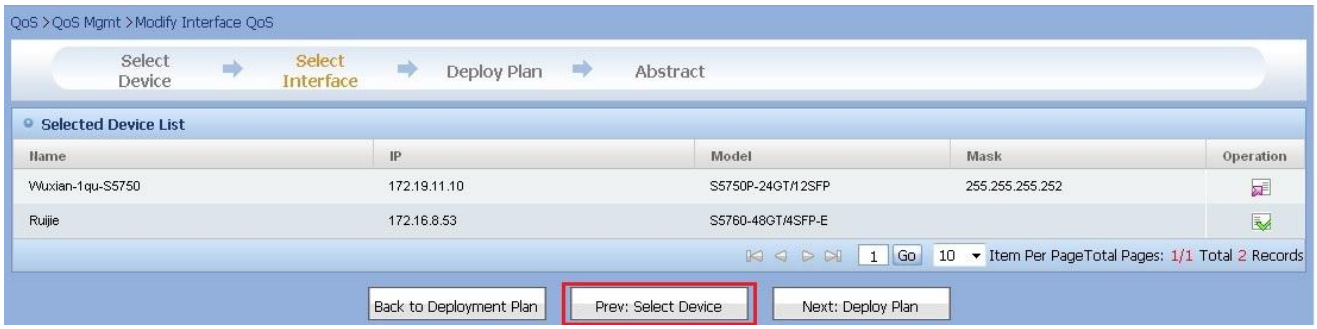


Figure 10.143. Previous: Select Device

10) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Next: Deploy Plan** button. As shown below:

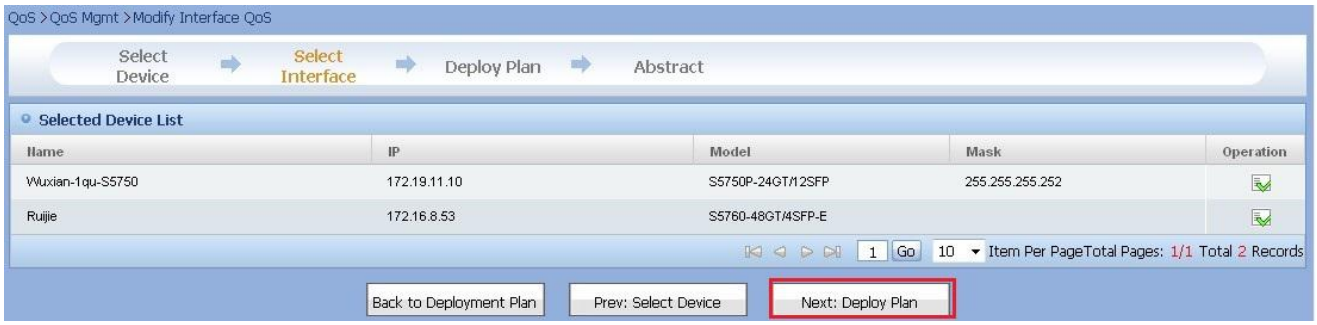


Figure 10.144. Next: Deploy Plan

11) Enter **Deploy Plan** page, click **Previous: Select Interface** button to return to **Select Interface** page. As shown below:

Figure 10.145. Previous: Select Interface

12) Enter **Deploy Plan** page, modify plan name and select deployment type, then click **Next: Confirm** button. As shown below:

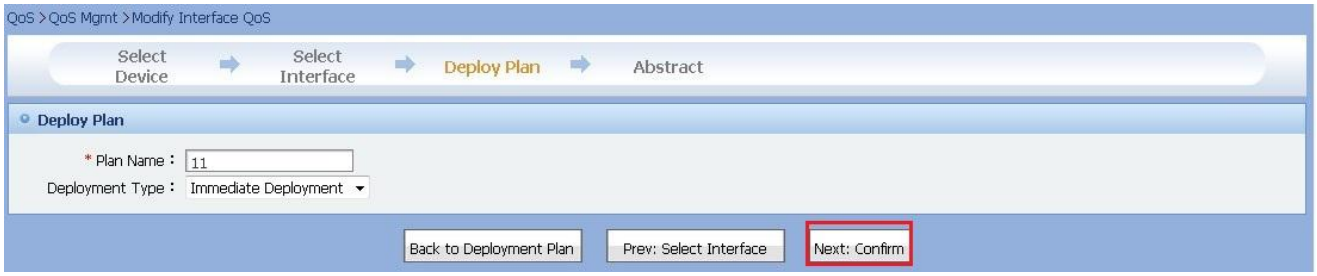


Figure 10.146. Next: Confirm

13) Enter **Confirm** page, click **Previous: Deploy Plan** to return to **Deploy Plan** page. As shown below:

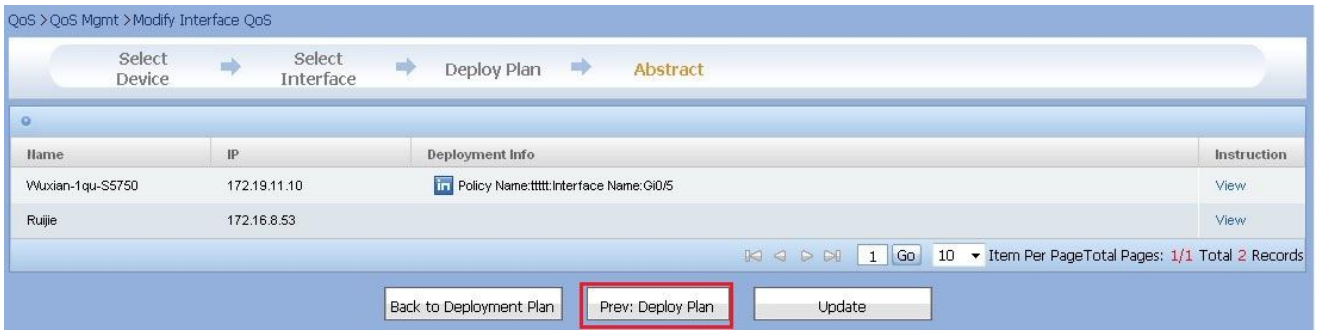


Figure 10.147. Previous: Deploy Plan

14) Click **View** button to view generated instructions on a pop-up page. As shown below:

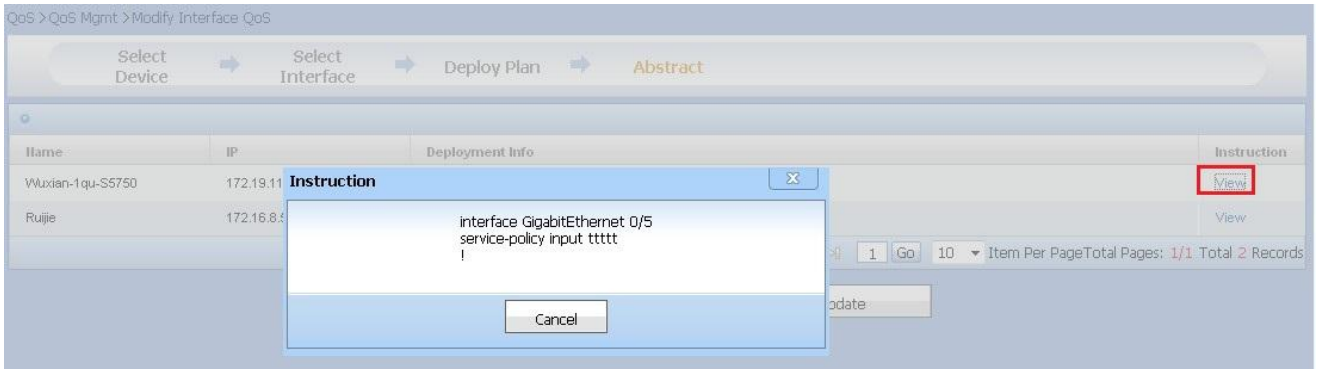


Figure 10.148. View Instructions

15) Click **Update**, the system will update the deployment plan then return to **QoS Deployment Plan Management** page. As shown below:

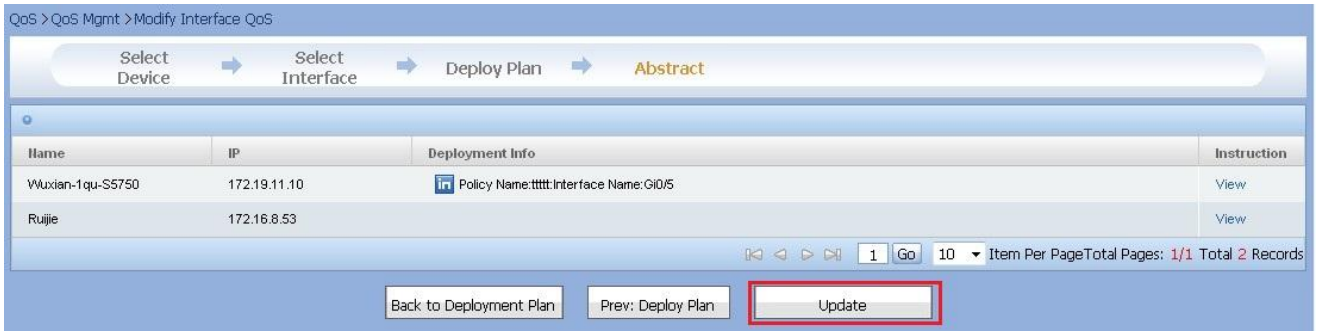


Figure 10.149. Update QoS Deployment Plan

On **Device List** for selection page, click **Add All** button to add all devices into **Selected Device List**. You don't need to select any device for **Add All** operation.

On **Selected Device List** page, click **Deselect** or **Deselect All** button to remove devices from **Selected Device List**. You don't need to select any device for **Deselect All** operation.

On the **Unselected Interface** box of **Device Interrelated Interface** page, you can double click the interface or click **>** button to add single interface, you can also click **>>** button to select interface in batches.

On the **Selected Interface** box of **Device Interrelated Interface** page, you can double click the interface or click **<** button to remove single interface, you can also click **<<** button to remove interface in batches.

On **Device Interrelated Interface** page, click **Previous Device** button to show the **Selected Interface** information of previous device.

On **Device Interrelated Interface** page, click **Next Device** button to show the **Selected Interface** information of next device.

Note

The plan automatically generated by the system cannot be modified.

If there is no selected device, you cannot click Next: Select Interface button.

If no interface is selected, you cannot click Next: Deploy Plan button.

After modifying a QoS interface deployment plan, you must **Start Plan** before the plan can be executed.

10.4.5. Stop Plan

On **QoS Deployment Plan Management** page, you can stop the running of a plan.

Operation Steps

On **QoS Deployment Plan Management** page, click **Stop Plan** button on plan list to stop the running of corresponding QoS deployment plan. As shown below:

Figure 10.150. Stop Plan

Note

Stopping plan execution: this will stop the running of a plan.

10.4.6. Start Plan

On **QoS Deployment Plan Management** page, you can start plan.

Operation Steps

On **QoS Deployment Plan Management** page, click **Start Plan** button to start the corresponding QoS deployment plan. As shown below:

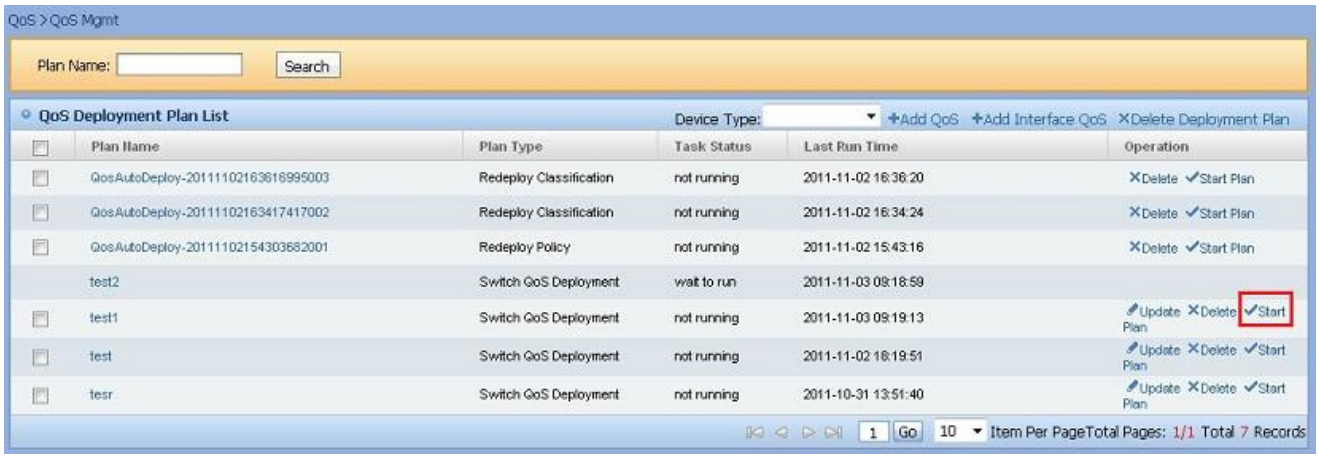


Figure 10.151. Start Plan

Note

After the plan is started, if the background process is running, the system will prompt **Operation succeeded. Waiting for background process to start the plan**; or **Background process is not running** will be prompted.

10.4.7. View Deployment Plan

On **QoS Deployment Plan Management** page, you can enter **QoS Deployment Plan Detail** page to view the plan related parameters, execution log and selected device list.

Operation Steps

1) Enter **QoS Deployment Plan Management** page, click **Plan Name** link to enter the plan detail information page. As shown below:

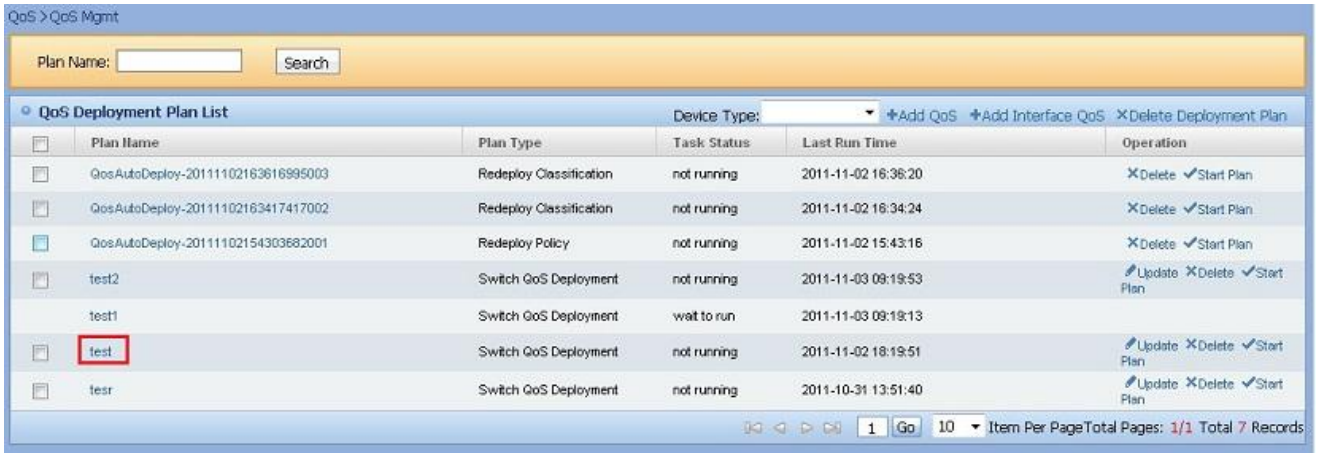


Figure 10.152. Enter QoS Deployment Plan Detail

2) It shows plan related parameters, execution log and selected device list. As shown below:

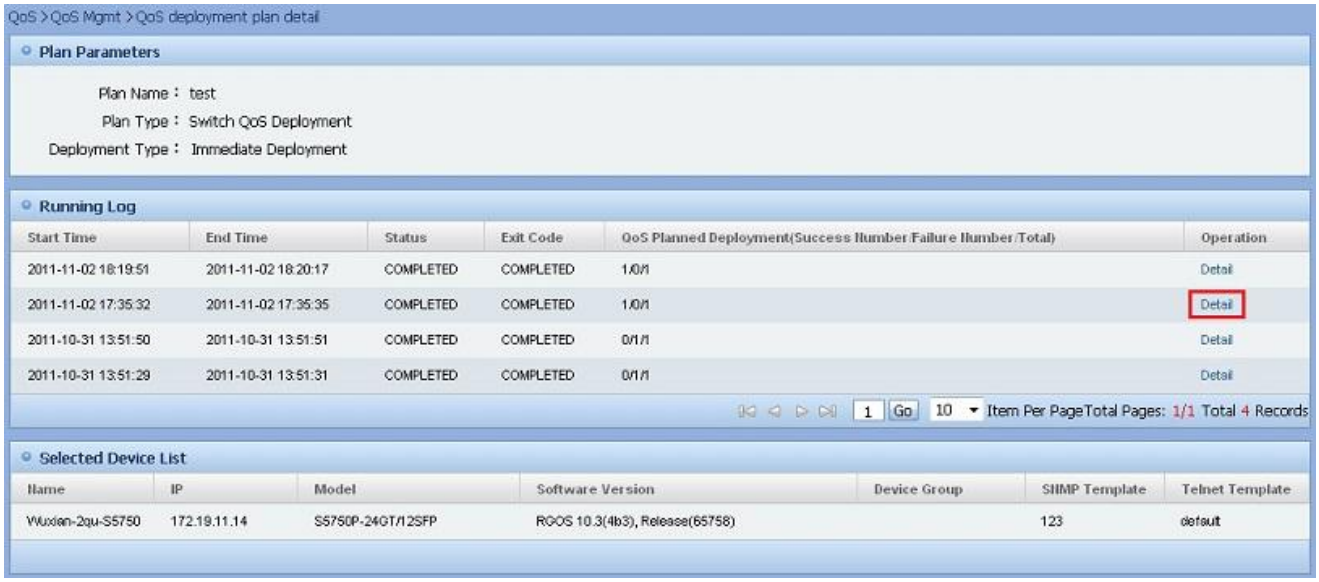


Figure 10.153. QoS Deployment Plan Detail

10.4.8. View Deployment Plan Execution Log

On **QoS Deployment Plan Management** page, you can enter **QoS Deployment Plan Detail** page to view the plan related parameters, execution log and selected device list.

Operation Steps

1) Enter **QoS Deployment Plan Management** page, click **Plan Name** link to enter the plan detail information page. As shown below:

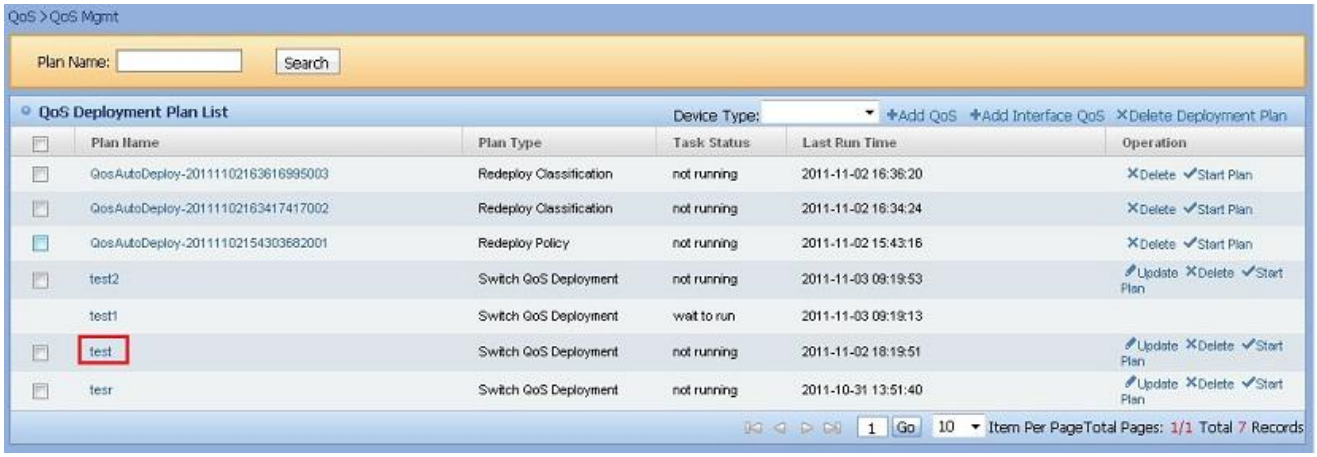


Figure 10.154. Enter QoS Deployment Plan Detail

2) It shows the plan related parameters, execution log and selected device list. Click link under **Detail** column to enter execution log detail page. As shown below:

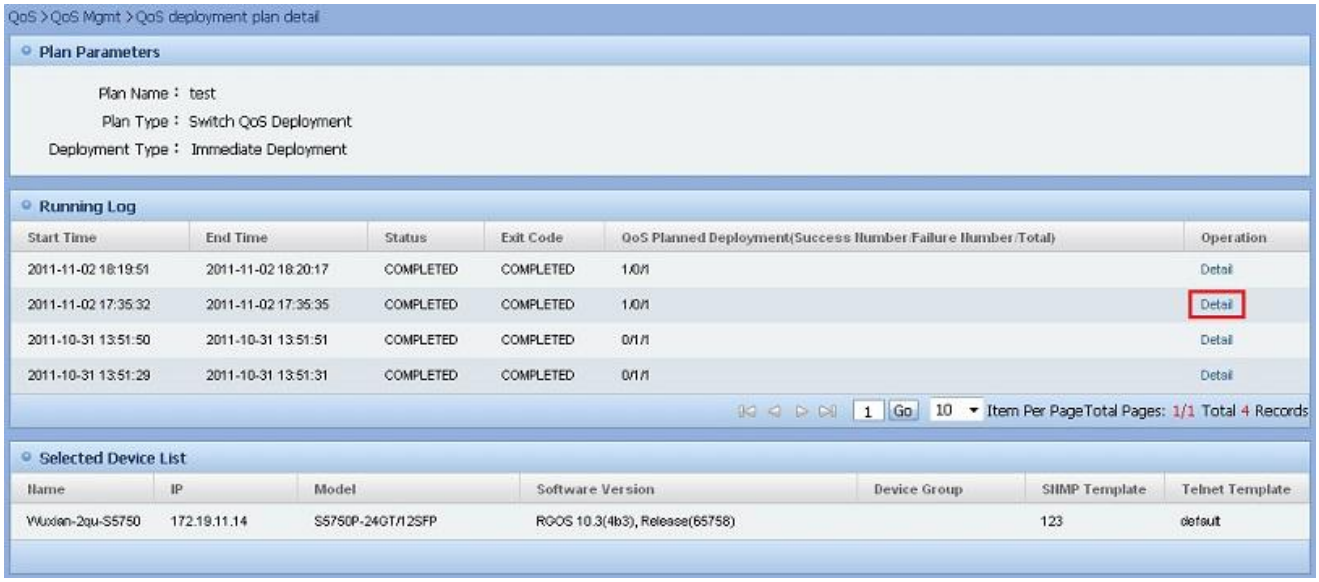


Figure 10.155. Enter Execution Log Detail

3) It shows basic information and details of execution log. As shown below:

Figure 10.156. Execution Log Detail

10.4.9. Add QoS Deployment Plan

On **QoS Deployment Plan Management** page, the QoS deployment can be added.

Operation Steps

1) Enter **QoS Deployment Plan Management** page, click **Add QoS** button. As shown below:

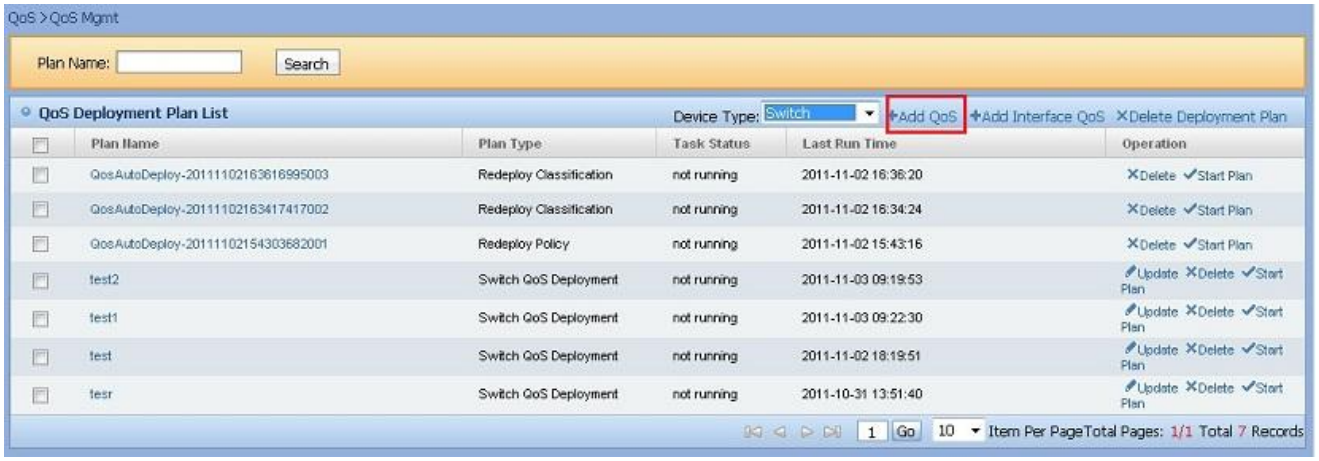


Figure 10.157. Add QoS Deployment

2) Enter **Selected Device List** page. As shown below:

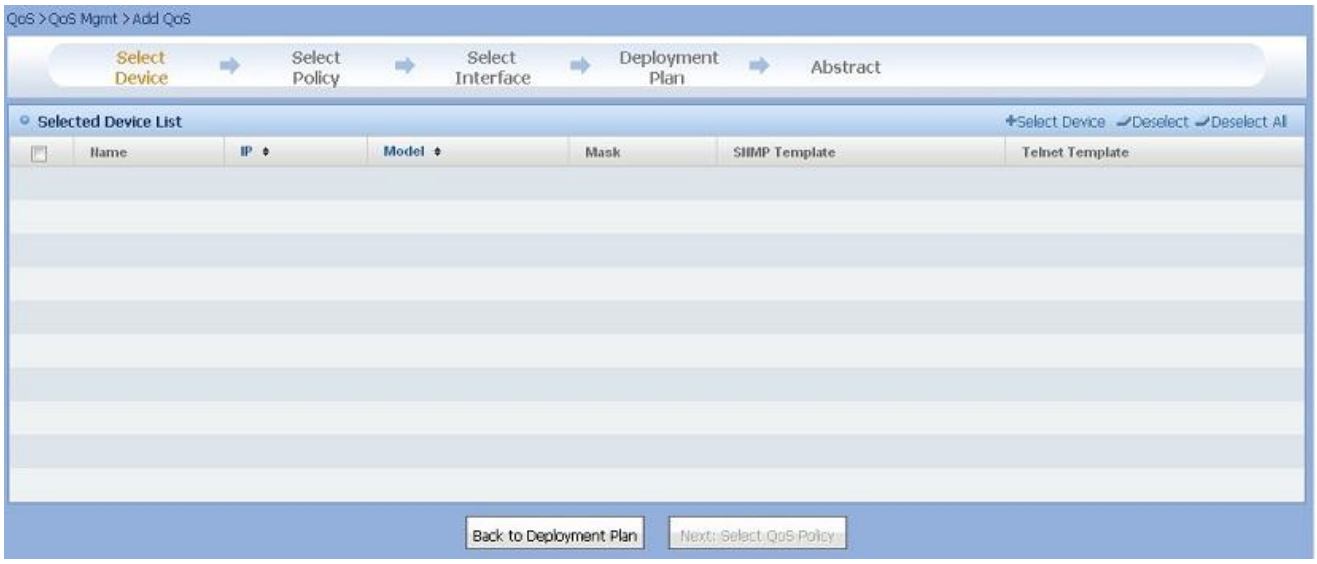


Figure 10.158. Enter **Selected Device List** Page

3) Click **Select Device** button, the device list page will be popped up for your selection. As shown below:

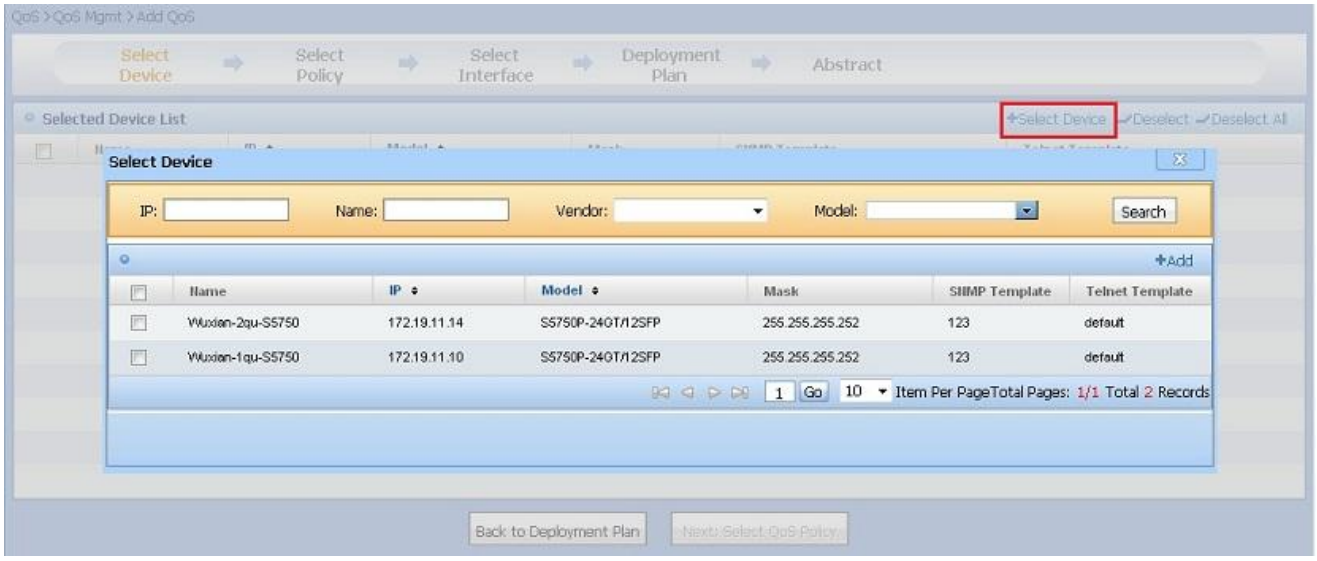


Figure 10.159. Select Device

4) After selecting device, click **Add** button, the following page will be shown:

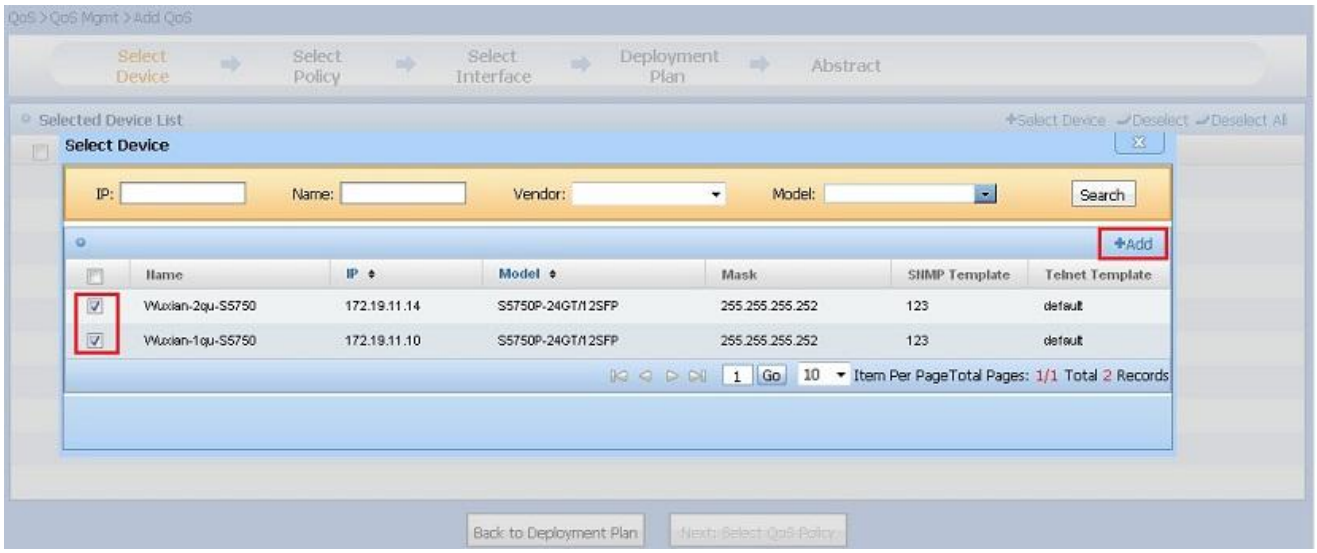


Figure 10.160. Add Device

5) Enter **Selected Device List** page, then click **Next: Select QoS Policy** button. As shown below:

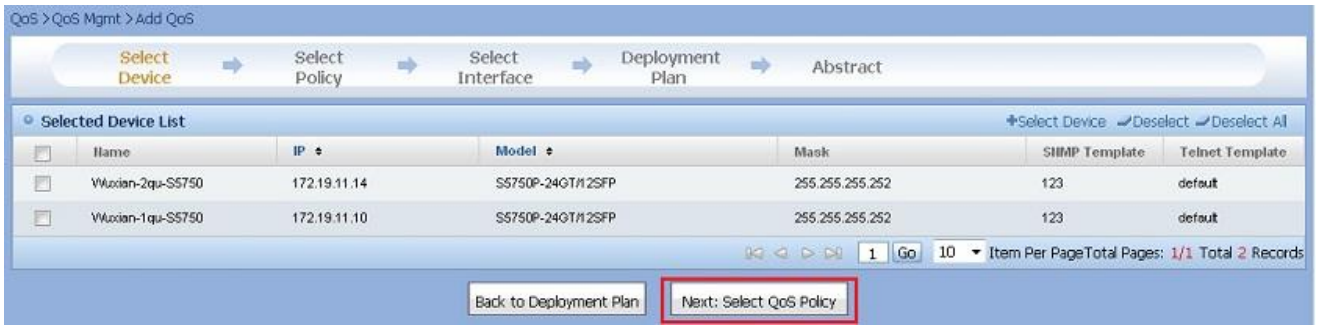


Figure 10.161. Next: Select QoS Policy

6) Enter **Selected QoS Policy List** page. As shown below:

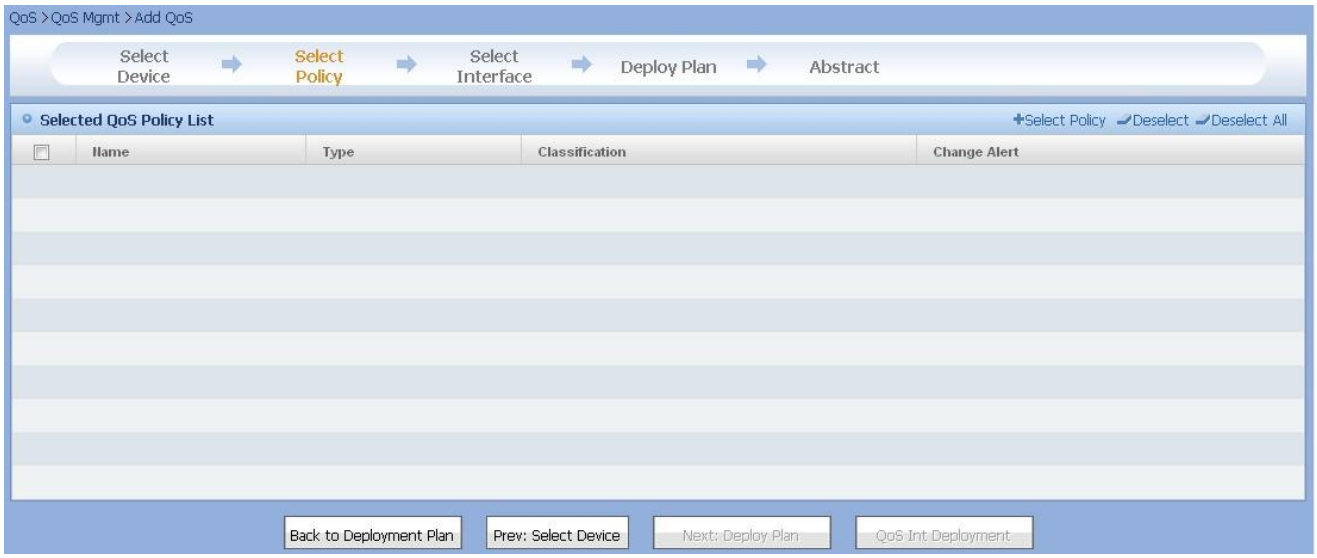


Figure 10.162. Select QoS Policy

7) Click **Select QoS Policy** button to enter **QoS Policy List** page for selection. As shown below:

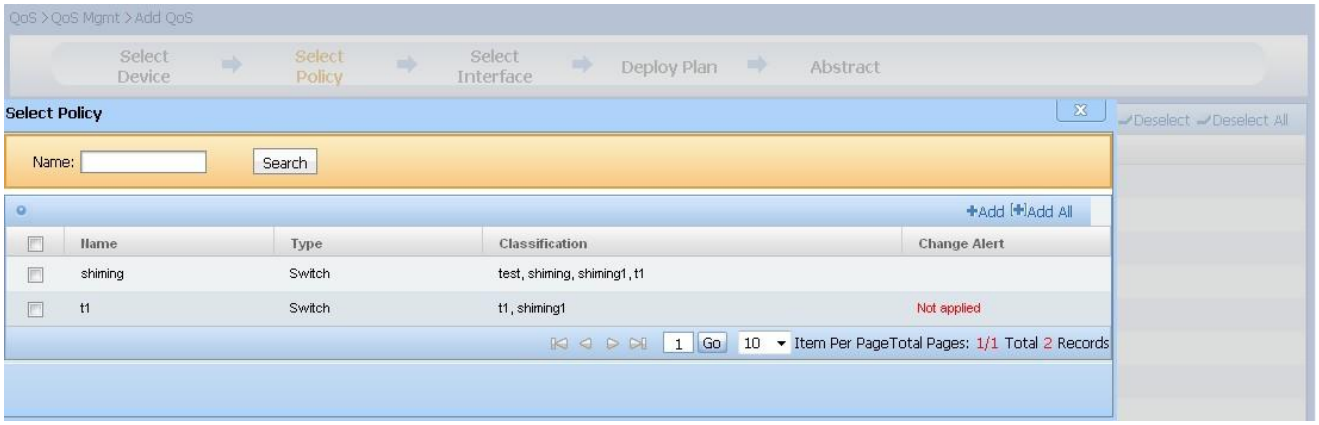


Figure 10.163. Select QoS Policy

8) After the QoS policy is selected, click **Add** button. As shown below:

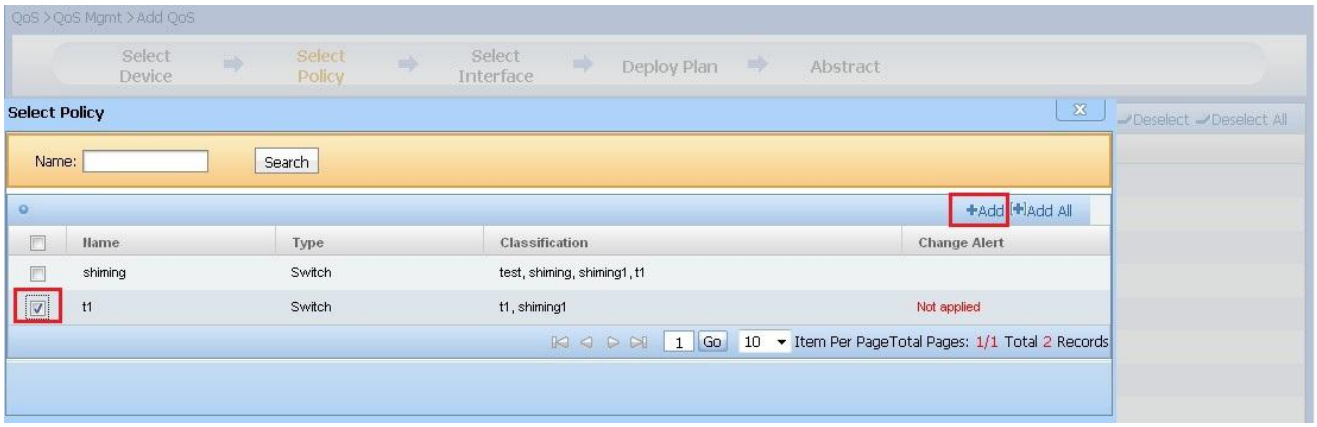


Figure 10.164. Add QoS Policy

9) Enter **Selected QoS Policy List** page, click **Previous: Select Device** to return to **Selected Device List** page. As shown below:

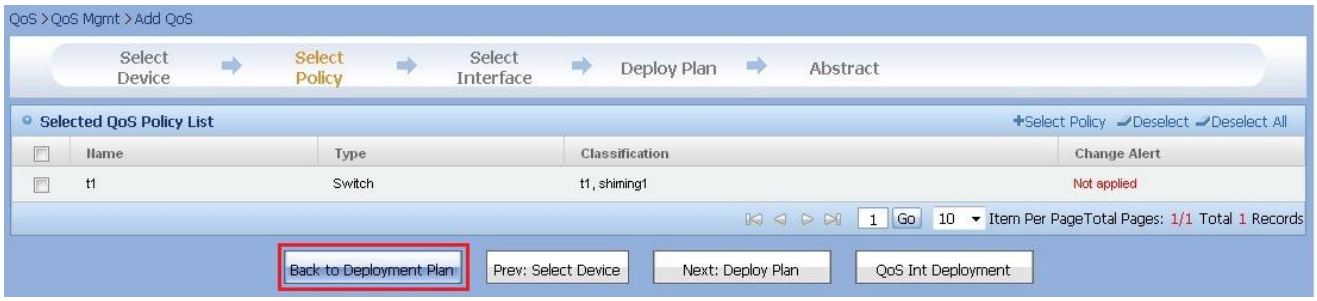


Figure 10.165. Previous: Select Device

10) Enter **Selected QoS Policy List** page, click **Deploy Plan** button to enter **Deploy Plan** page. As shown below:

Figure 10.166. Deploy Plan

11) Enter **Selected QoS Policy List** page, click **QoS Interface Deployment** button to enter **Select Interface** page. As shown below:

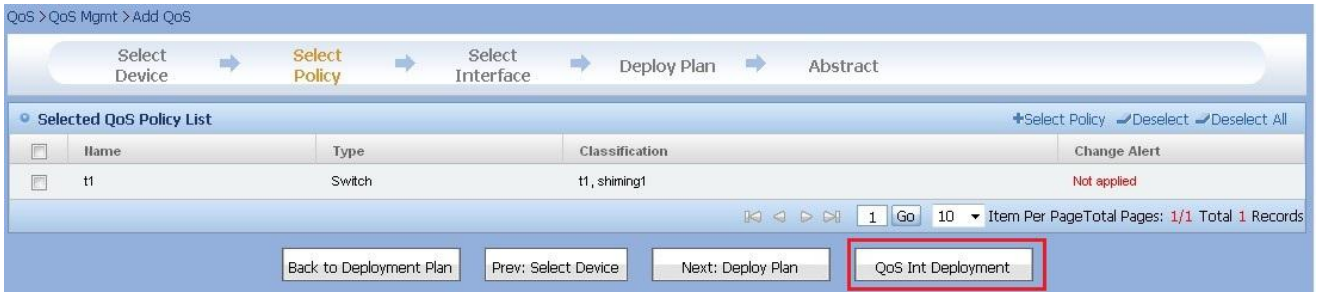


Figure 10.167. QoS Interface Deployment

12) Enter **Select Interface** page, it shows **Selected Device List**, click the button of operation column on **Selected Device List** to configure the interface.

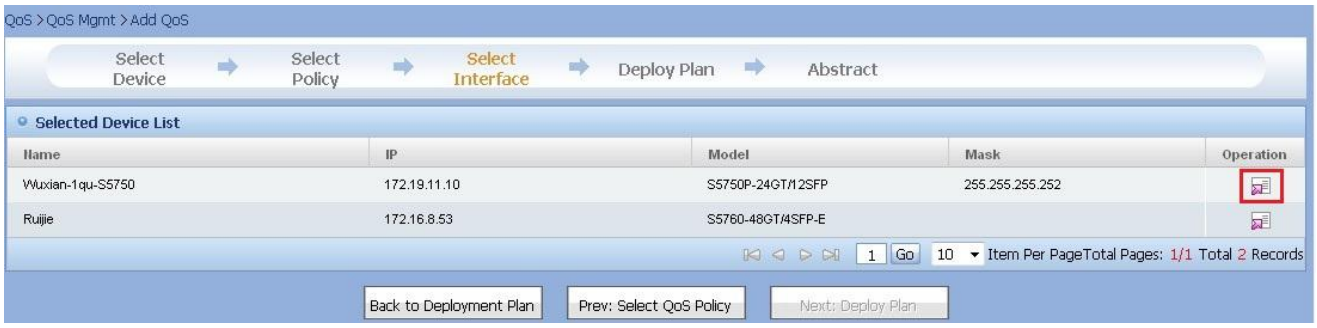


Figure 10.168. Select Interface

13) Enter **Device Interface** page, it shows the deployed interfaces.

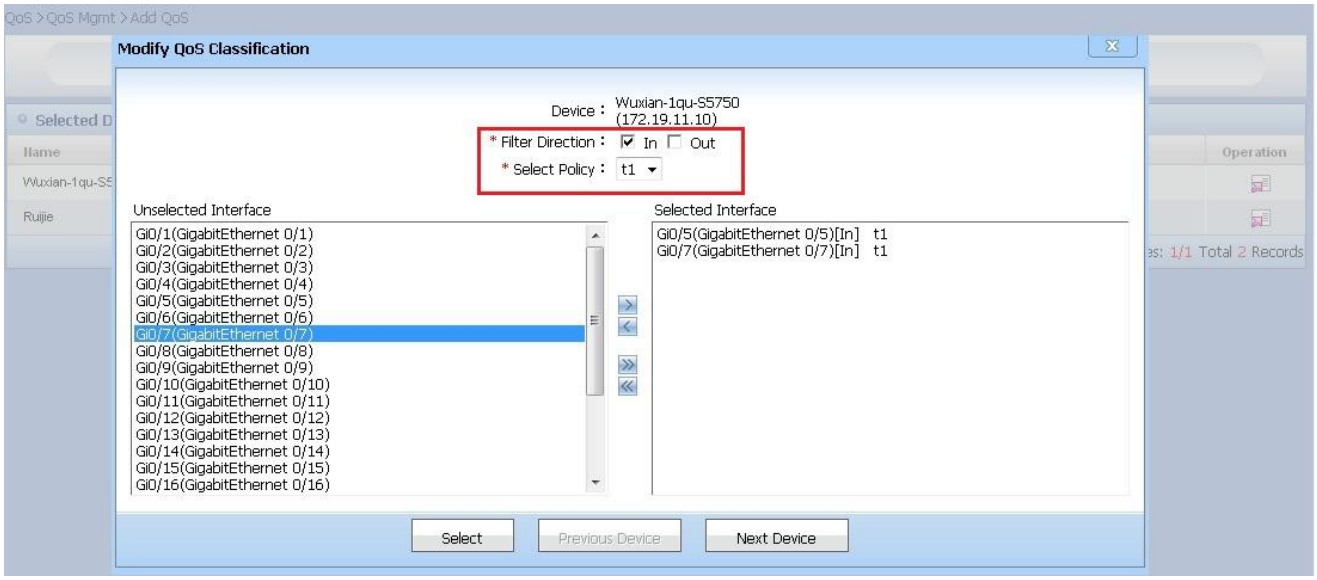


Figure 10.169. Device Interface

14) Select interface in **Filter Direction**, **QoS Policy** and **Unselected Interface** list, then double click it or click **>** button to add the interface into **Selected Interface** list, the selected interface will be displayed with format **Interface Name[Filter Direction]Qos Policy Name**. Click **Select** button after selection is finished.

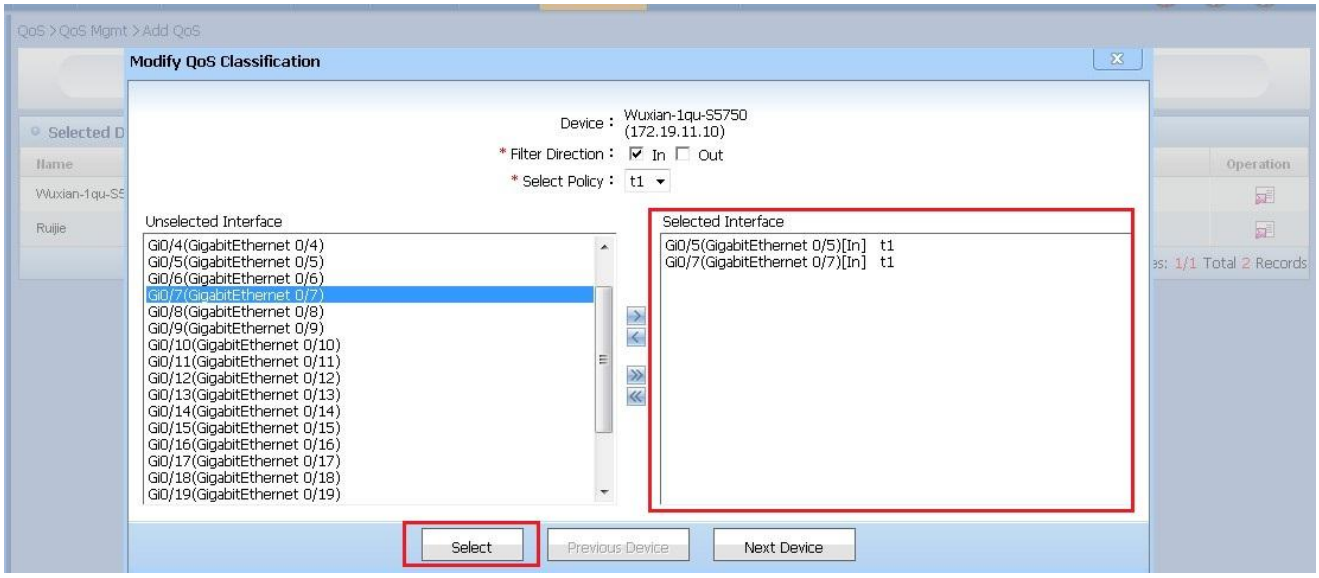


Figure 10.170. Add QoS Interface Deployment

15) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Previous: Select QoS Policy** button to return to **Selected QoS Policy List** page. As shown below:

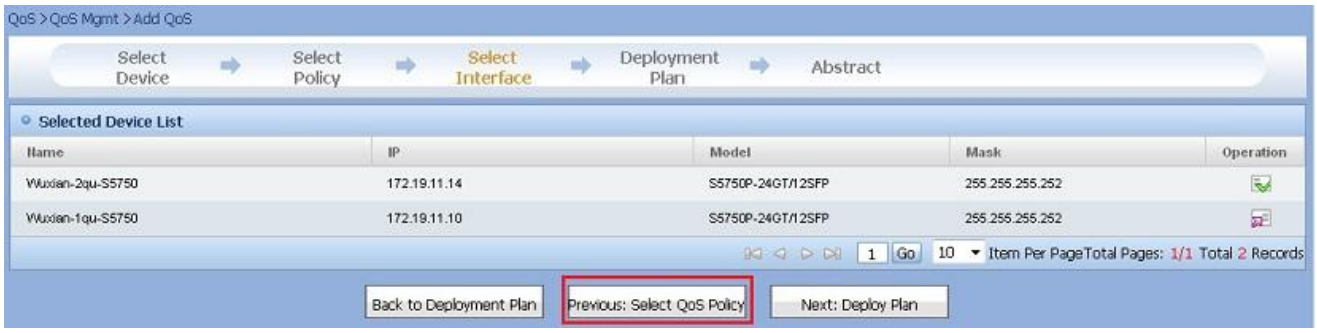


Figure 10.171. Previous: Select QoS Policy

16) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Next: Deploy Plan** button. As shown below:

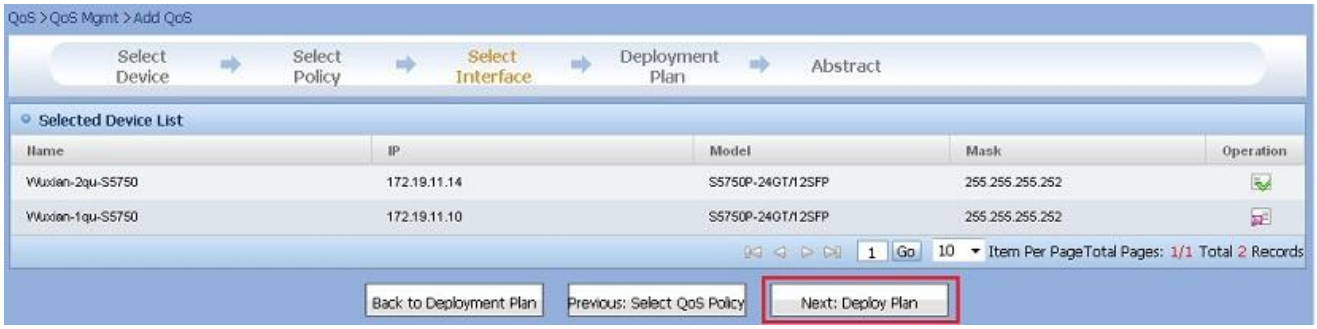


Figure 10.172. Next: Deploy Plan

17) Enter **Deploy Plan** page, click **Previous: Select Interface** button to return to **Select Interface** page. As shown below:

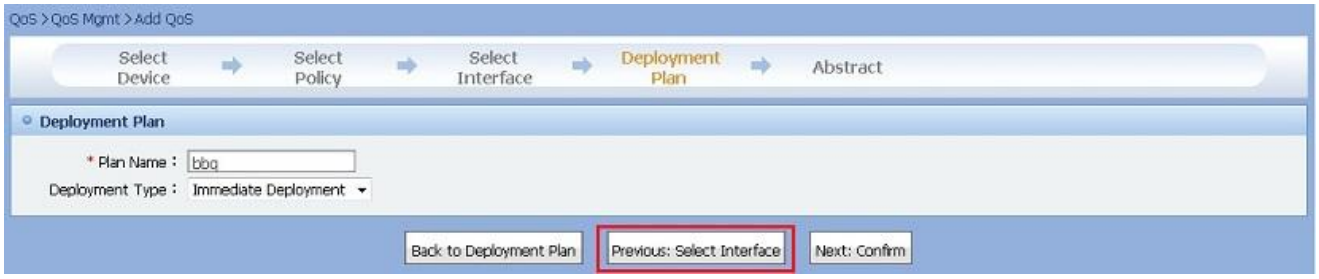


Figure 10.173. Previous: Select Interface

18) Enter **Deploy Plan** page, input plan name and select deployment type (Can also select periodic deployment), then click **Next: Confirm** button. As shown below:

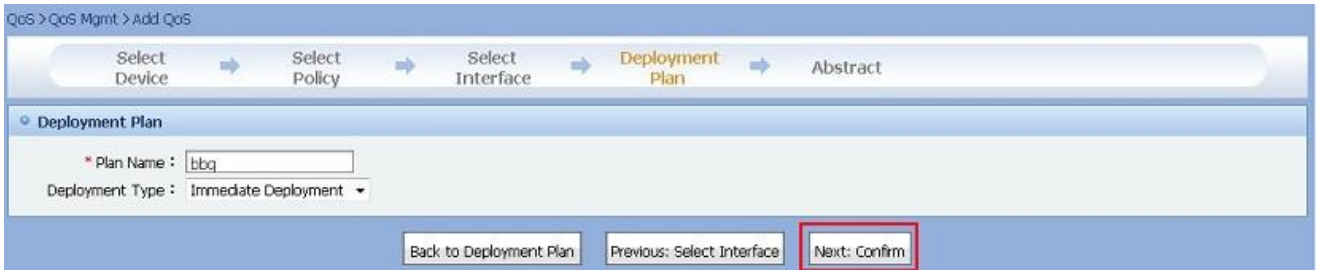


Figure 10.174. Next: Confirm

19) Enter **Confirm** page, click **Previous: Deploy Plan** to return to **Deploy Plan** page. As shown below:

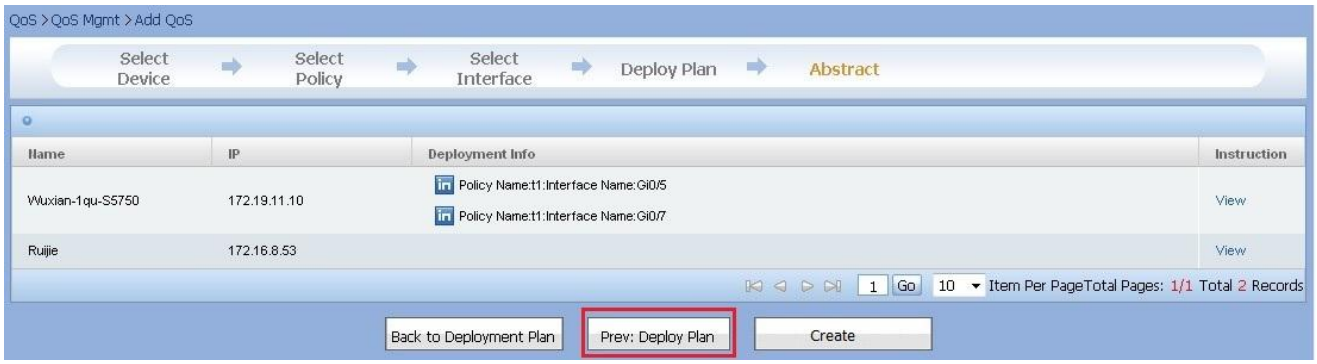


Figure 10.175. Previous: Deploy Plan

20) Click **View** button to view generated instructions on a pop-up page. As shown below:

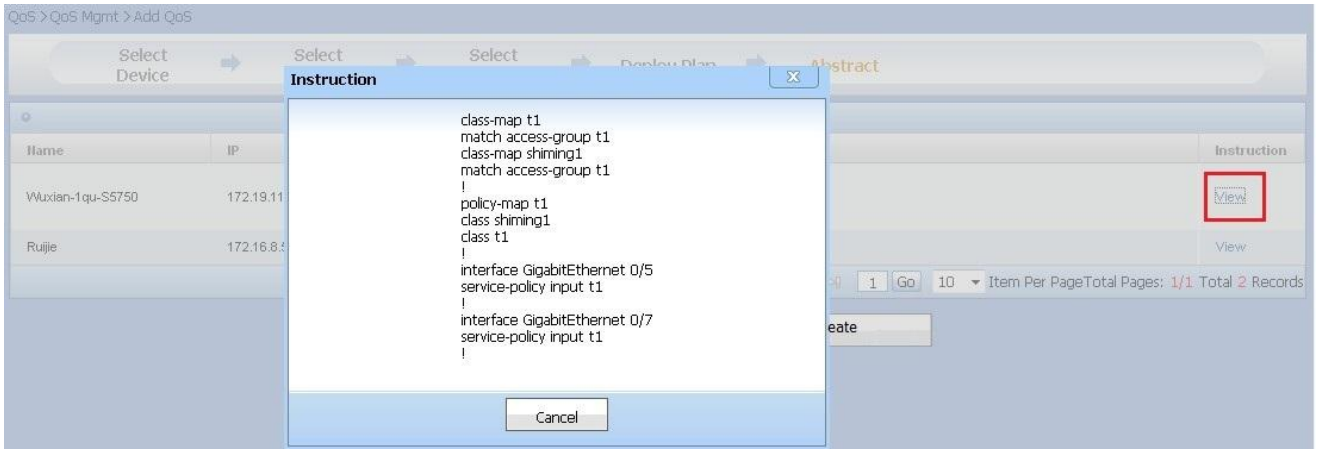


Figure 10.176. View Instructions

21) Click **Create**, the system will create the deployment plan then return to **QoS Deployment Plan Management** page. As shown below:

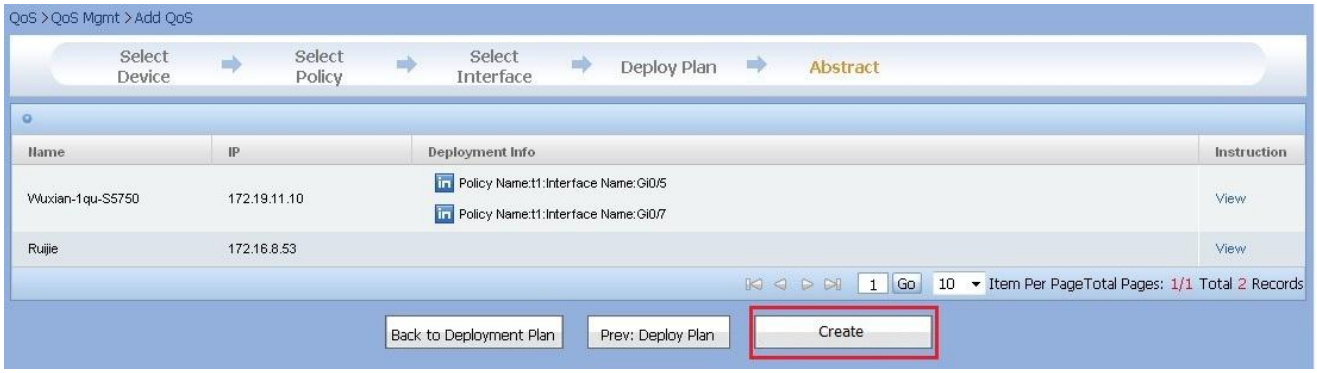


Figure 10.177. Start to Create Deployment Plan

On **Device List** for selection page, click **Add All** button to add all devices into **Selected Device List**. You don't need to select any device for **Add All** operation.

On **Selected Device List** page, click **Deselect** or **Deselect All** button to remove devices from **Selected Device List**. You don't need to select any device for **Deselect All** operation.

On **Selected QoS Policy List** page, click **Deselect** or **Deselect All** button to remove QoS policies from **Selected QoS Policy List**. You don't need to select any QoS policy for **Deselect All** operation.

On **QoS Policy List** for selection page, click **Add All** button to add all QoS policies into **Selected QoS Policy List**. You don't need to select any QoS policy for **Add All** operation.

On the **Unselected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **>** button to add single interface, you can also click **>>** button to select interface in batches.

On the **Selected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **<** button to remove single interface, you can also click **<<** button to remove interface in batches.

On **Device associated Interface** page, click **Previous Device** button to show the **Selected Interface** information of previous device.

On **Device associated Interface** page, click **Next Device** button to show the **Selected Interface** information of next device.

Note

If there is no selected device, you cannot click **Next: Select QoS Policy** button.

If there is no selected QoS policy, you cannot click **QoS Interface Deployment** button.

If no interface is selected, you cannot click **Next: Deploy Plan** button.

After adding a deployment plan, you must **Start Plan** before the plan can be executed.

10.4.10. Add QoS Interface Deployment Plan

On **QoS Deployment Plan Management** page, you can add QoS interface deployment plan.

Operation Steps

1) Enter **QoS Deployment Plan Management** page, click **Add QoS Interface Deployment Plan** button. As shown below:

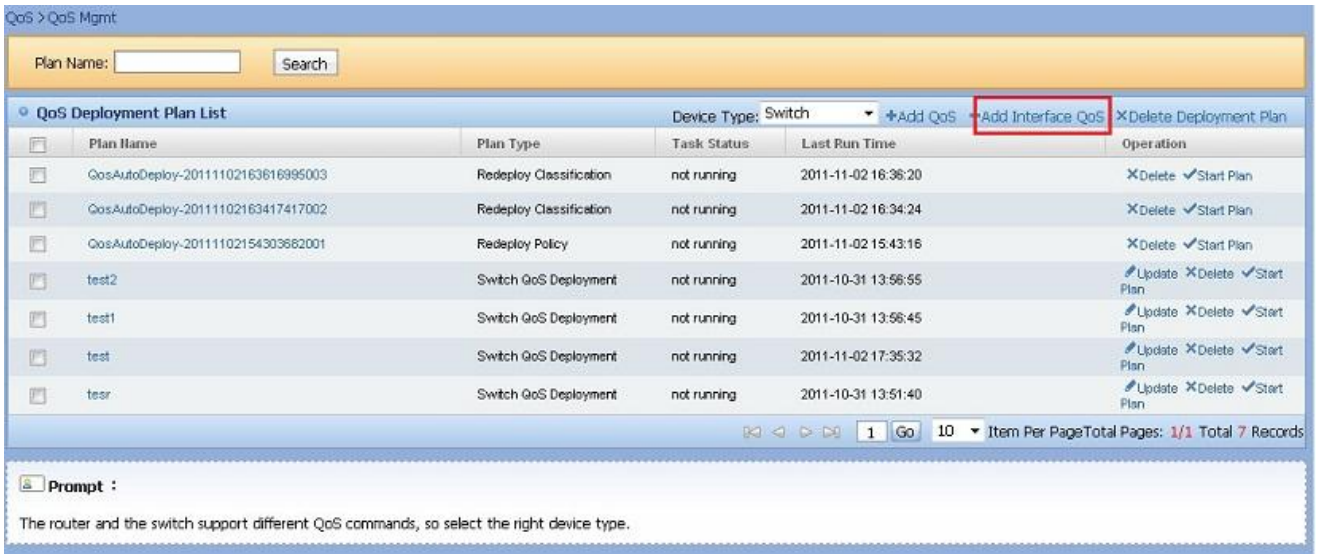


Figure 10.178. Add QoS Interface Deployment Plan

2) Enter **Selected Device List** page. As shown below:

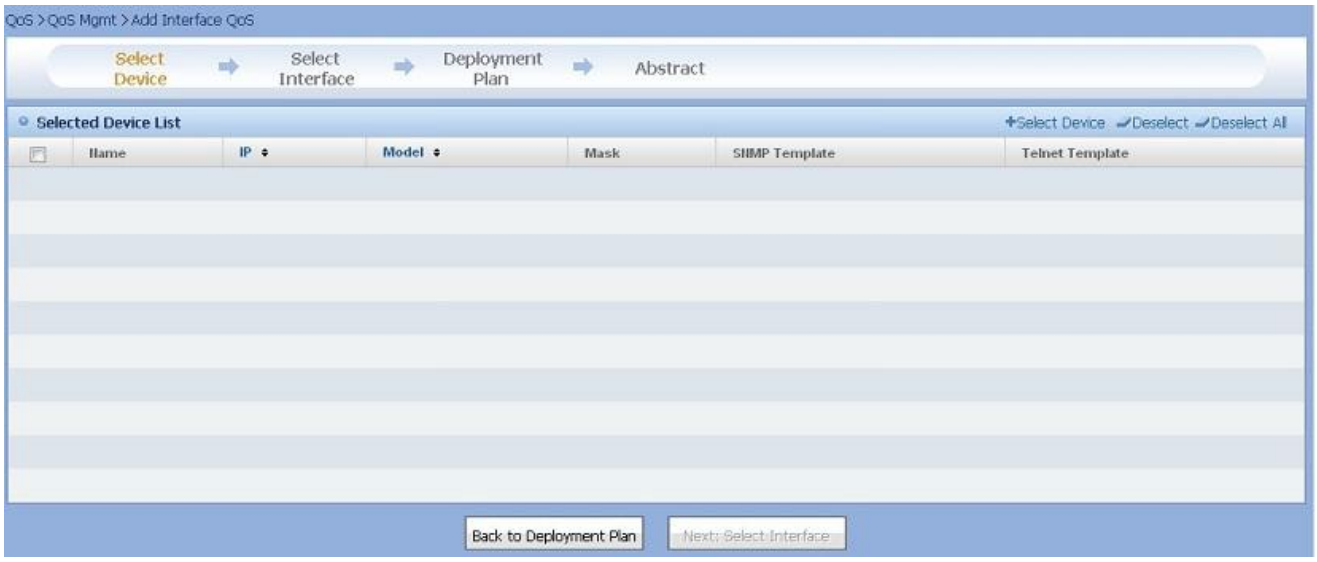


Figure 10.179. Enter **Selected Device List** Page

3) Click **Select Device** button, the **Device List** for selection page will be popped up. As shown below:

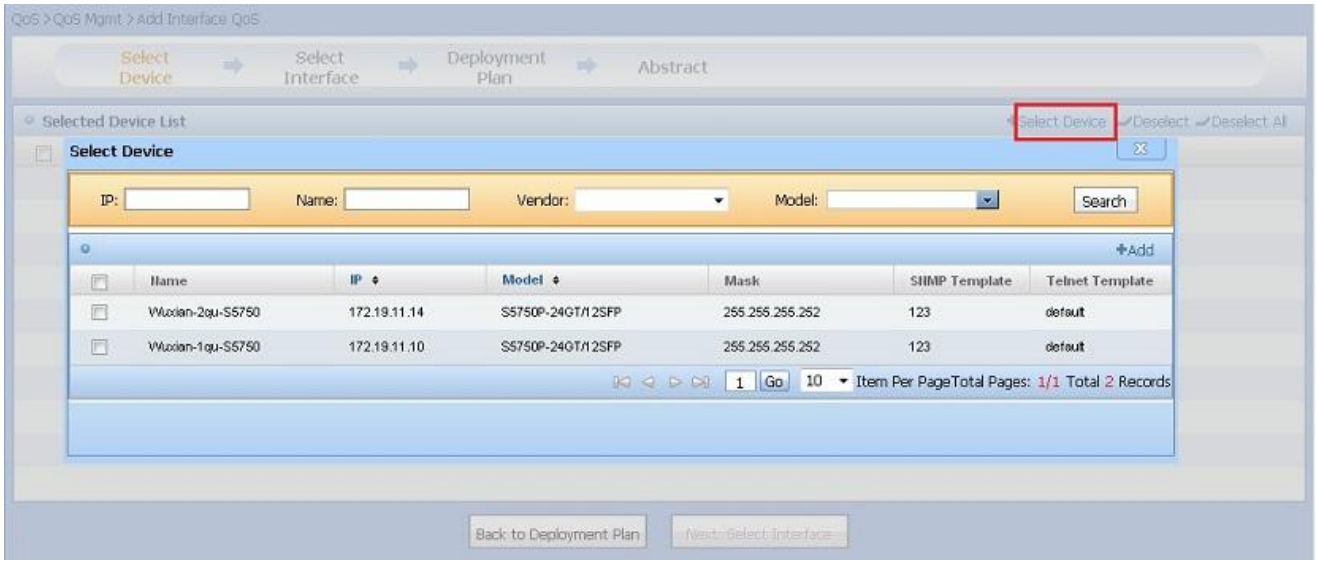


Figure 10.180. Select Device

4) After selecting device, click **Add**. As shown below:

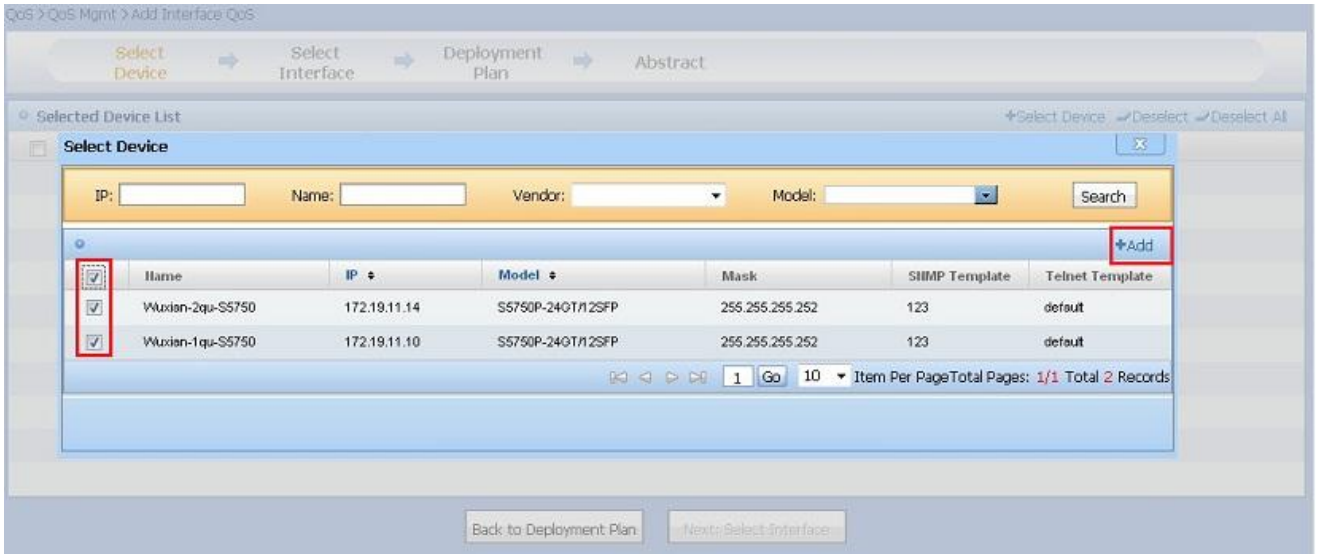


Figure 10.181. Add Device

5) Enter **Selected Device List** page, click **Next: Select Interface** button. As shown below:

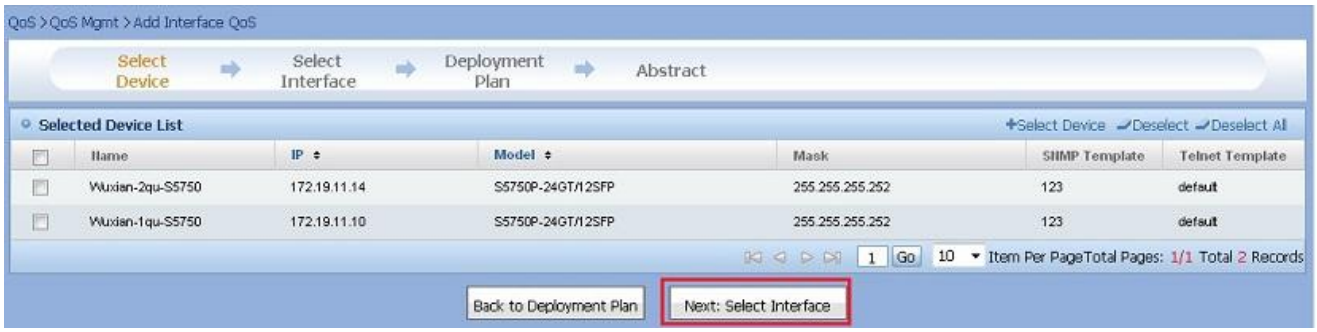


Figure 10.182. Next: Select Interface

6) Enter **Select Interface** page, it shows **Selected Device List**. Click icon on operation column of **Selected Device List** to configure interface.

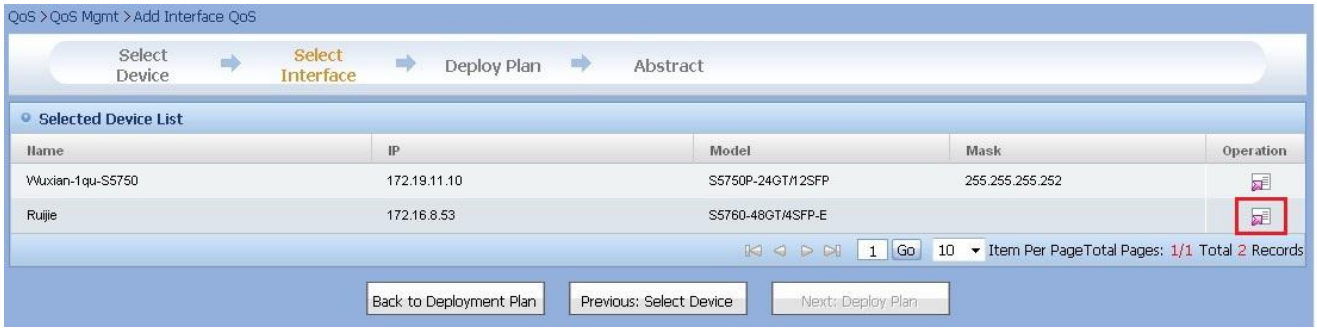


Figure 10.183. Select Interface

7) Enter **Device Interrelated Interface** page.

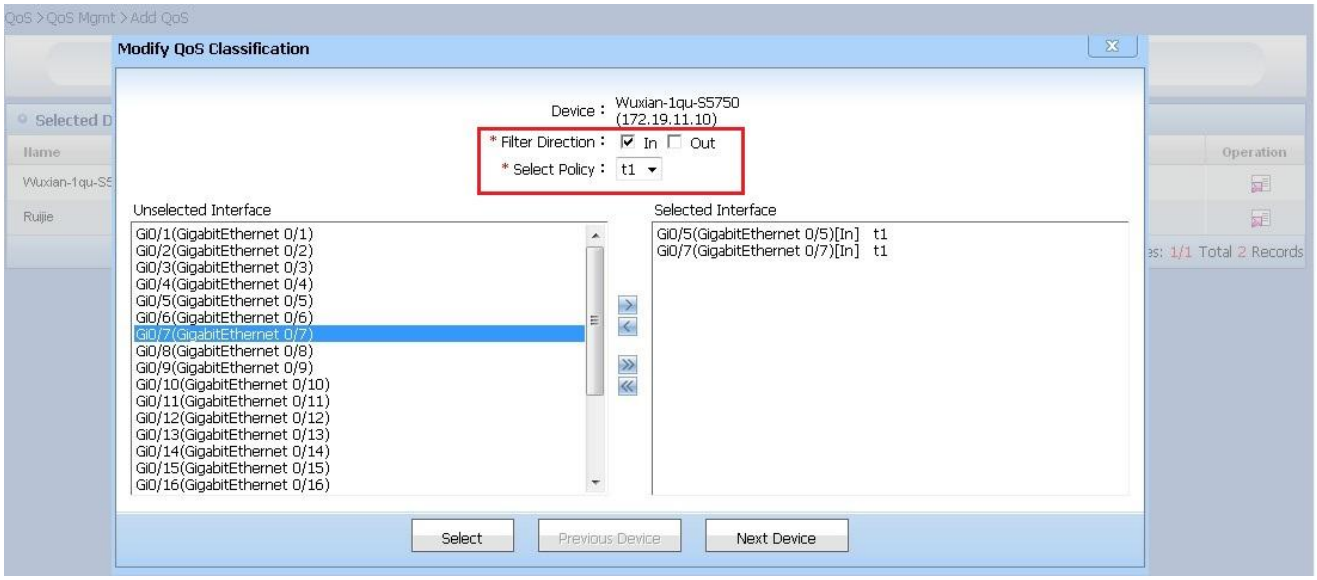


Figure 10.184. Device Interrelated Interface

8) Select interface in **Filter Direction**, **QoS Policy** and **Unselected Interface** list, then double click it or click **>** button to add the interface into **Selected Interface** list, the selected interface will be displayed with format **Interface Name[Filter Direction]Qos Policy Name**.

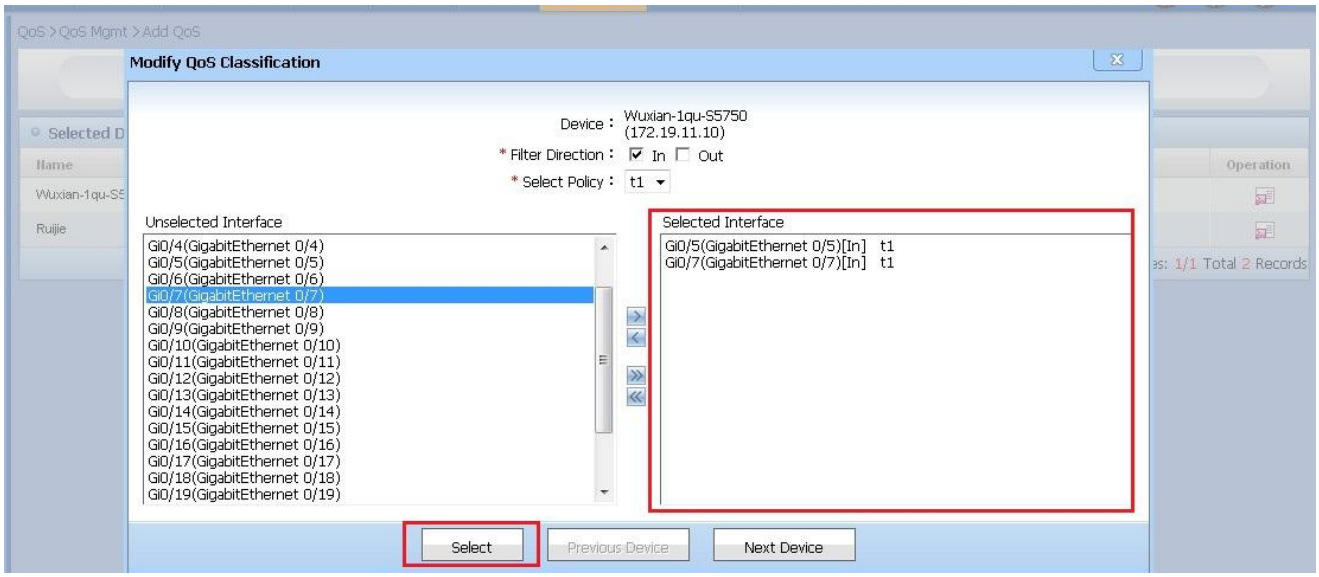


Figure 10.185. Add QoS Interface Deployment

9) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Previous: Select Device** button to return to **Selected QoS Device List** page. As shown below:

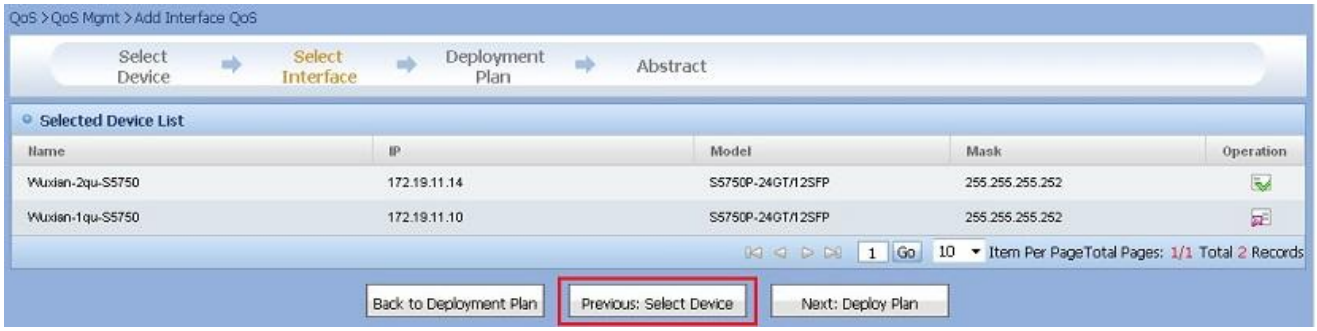


Figure 10.186. Previous: Select Device

10) Enter **Selected Device List** page, the selected device and unselected device are shown with different icons. Click **Next: Deploy Plan** button. As shown below:

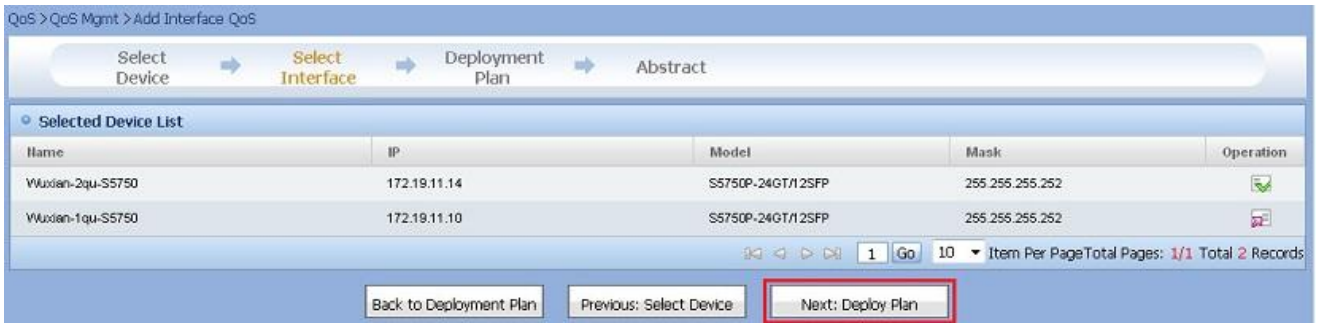


Figure 10.187. Next: Deploy Plan

11) Enter **Deploy Plan** page, click **Previous: Select Interface** button to return to **Select Interface** page. As shown below:

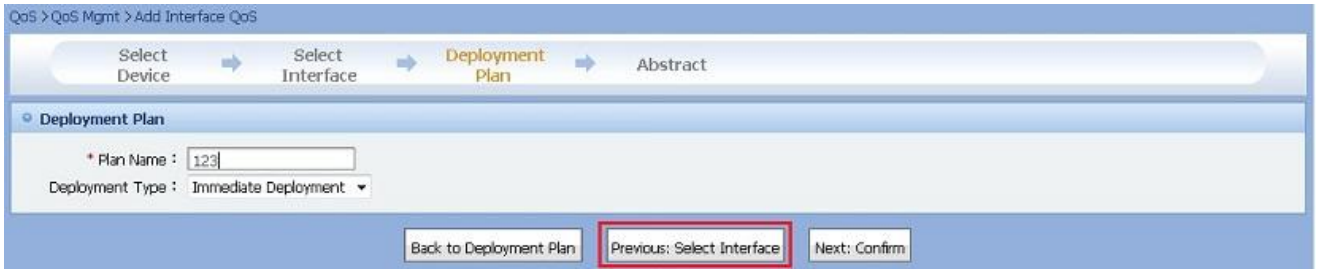


Figure 10.188. Previous: Select Interface

12) Enter **Deploy Plan** page, input plan name and select deployment type, then click **Next: Confirm** button. As shown below:

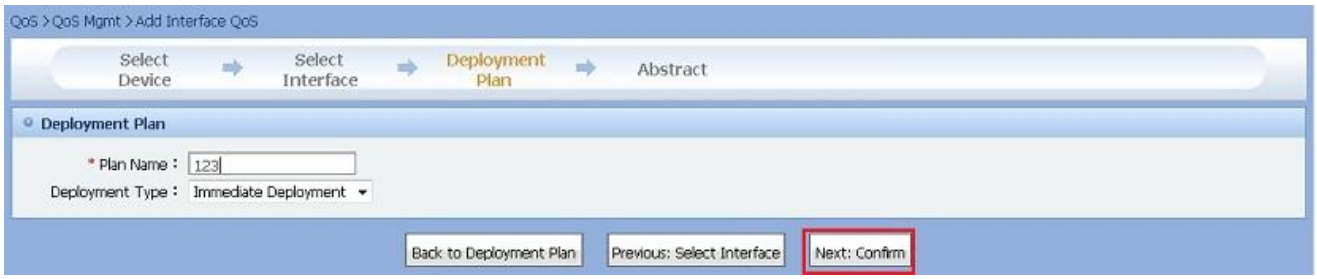


Figure 10.189. Next: Confirm

13) Enter **Confirm** page, click **Previous: Deploy Plan** to return to **Deploy Plan** page. As shown below:

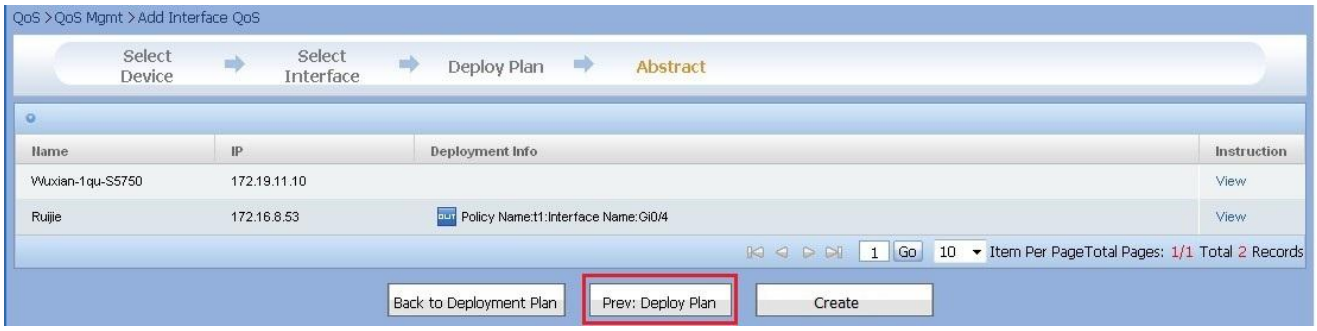


Figure 10.190. Previous: Deploy Plan

14) Click **View** button to view generated instructions on a pop-up page. As shown below:

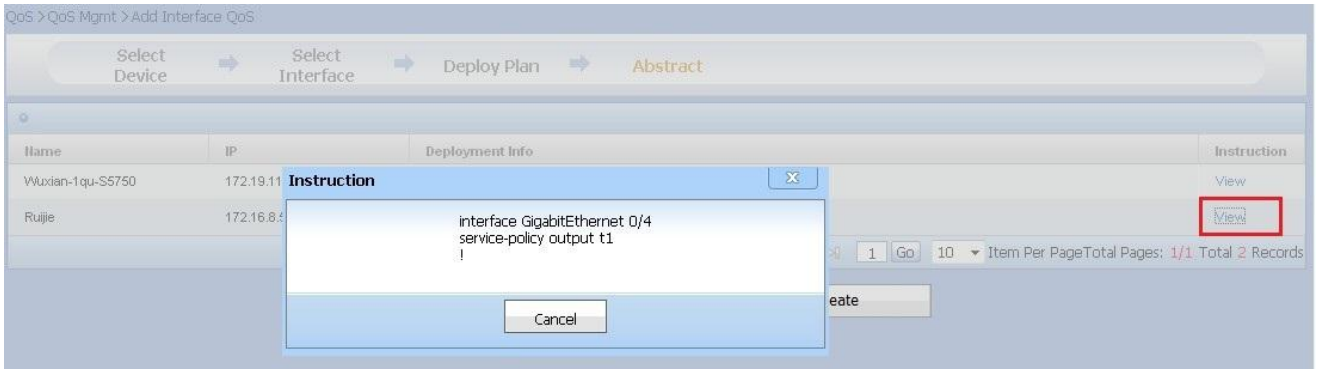


Figure 10.191. View Instructions

15) Click **Create**, the system will create the deployment plan then return to **QoS Deployment Plan Management** page. As shown below:

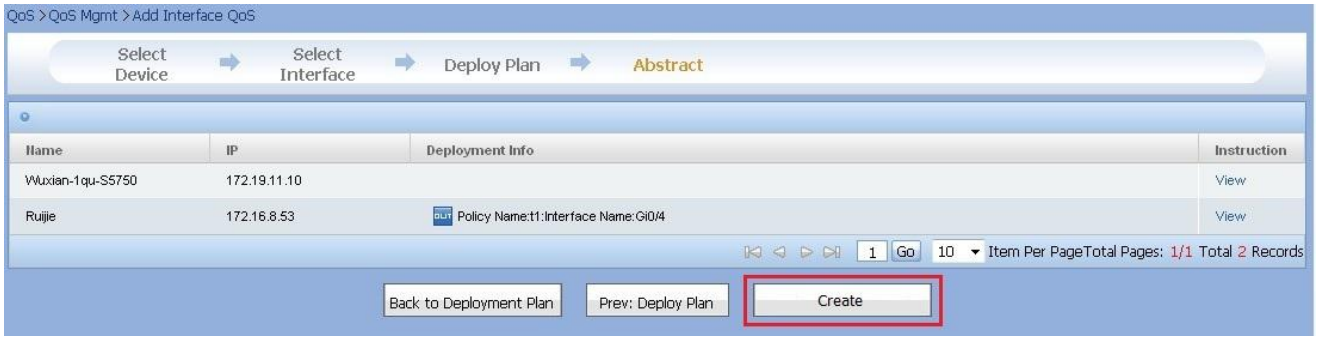


Figure 10.192. Create QoS Deployment Plan

On **Device List** for selection page, click **Add All** button to add all devices into **Selected Device List**. You don't need to select any device for **Add All** operation.

On **Selected Device List** page, click **Deselect** or **Deselect All** button to remove devices from **Selected Device List**. You don't need to select any device for **Deselect All** operation.

On the **Unselected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **>** button to add single interface, you can also click **>>** button to select interface in batches.

On the **Selected Interface** frame of **Device Interrelated Interface** page, you can double click the interface or click **<** button to remove single interface, you can also click **<<** button to remove interface in batches.

On **Device Interrelated Interface** page, click **Previous Device** button to show the **Selected Interface** information of previous device.

On **Device Interrelated Interface** page, click **Next Device** button to show the **Selected Interface** information of next device.

Note

If no device is selected, you cannot click **Next: Select Interface** button.

If no interface is selected, you cannot click **Next: Deploy Plan** button.

After adding a QoS interface deployment plan, you must **Start Plan** before the plan can be executed.

Chapter 11 ACL Management

This module includes ACL Time Range Management, ACL Management, ACL Device Management, ACL Template Management and ACL Deployment Plan Management.

- ACL Time Range Management
- ACL Management
- ACL Device Management
- ACL Template Management
- ACL Deployment Plan Management

11.1. ACL Time Range Management

ACL Time Range Management is to configure the effective time of ACL rules, which contains time information management.

- Add Time Range
- Search Time Range
- Delete Time Range
- View Time Range
- Modify Time Range
- Redeploy Time Range
- Redeploy Time Range in Device
- Absolute Time Management
- Time Information Management

11.1.1. Add Time Range

Time Range has to be added to the system to be managed by the system.

Operation Steps

1) Go to page **Time Range Management**, and click the button **Add** to enter page **Add Time Range**, as shown in the following figure:

Figure 11.1. Go to page **Add Time Range**

2) Go to page **Add Time Range**, fill in the information related to Time Range, and click on **Add** button, as shown in the following figure:

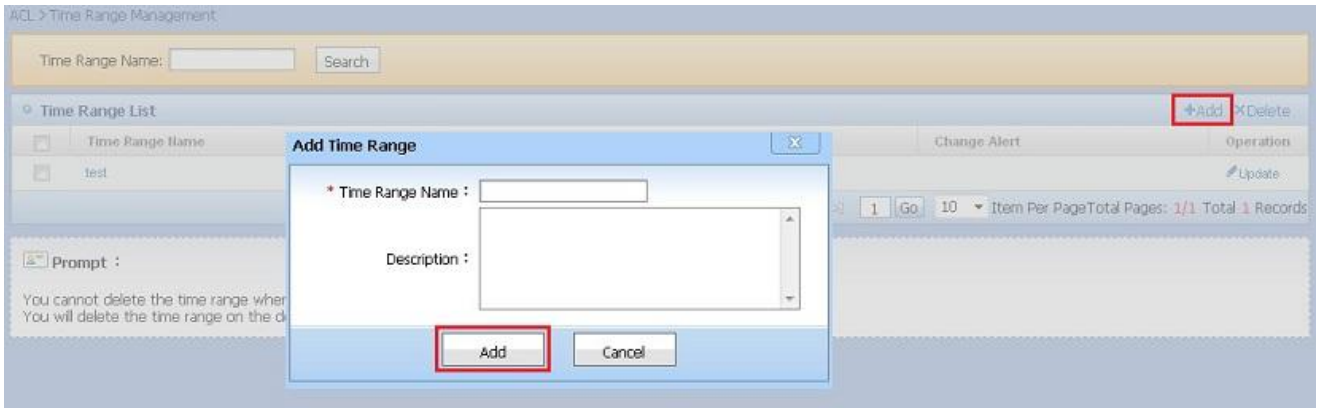


Figure 11.2. Add Time Range

On page **Add Time Range**, if **Cancel** is clicked, the system saves no modification and returns to **Time Range Management** page directly.

Note

Time range name cannot be repeated.

Maximum length of time range name is 32 characters.

Because some devices do not support Chinese, Chinese characters and full-width characters are not allowed in time range name.

11.1.2. Search Time Range

Time Range name can be filled in to search for system-managed time ranges on page **Time Range Management**.

Operation Steps

Go to Page **Time Range management**, fill in Time Range name and then click **Search** button. The system will return Time Range list which satisfies search conditions, as shown in the following figure:

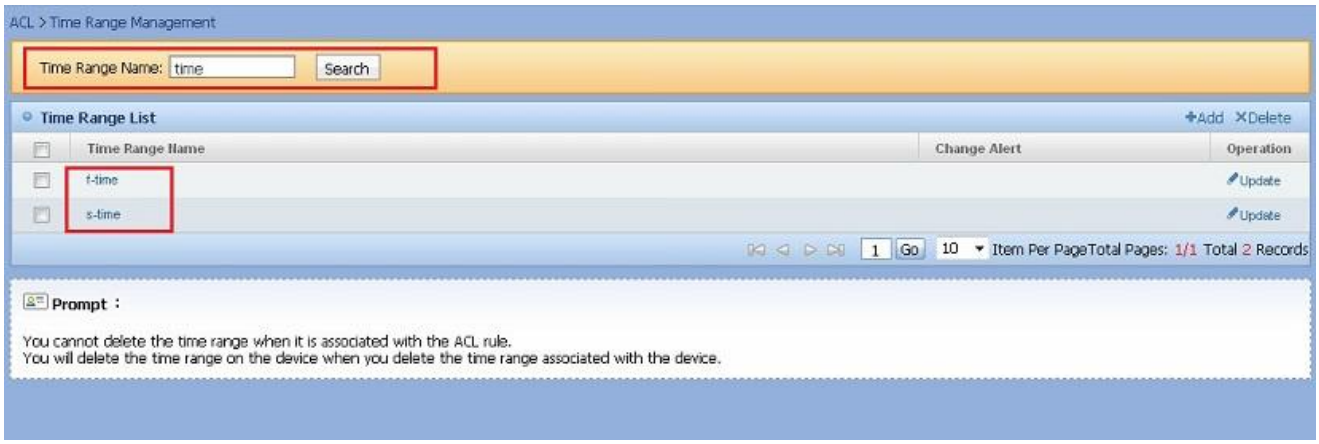


Figure 11.3. Search Time Range

11.1.3. Delete Time Range

Time Range can be deleted in batch on page **Time Range Management**.

Operation Steps

1) Go to page **Time Range Management**, select some time ranges and click button **Delete** in time range list. The system will prompt you to confirm the deletion operation. Click **Confirm** to delete selected time ranges, as shown in the following figure:

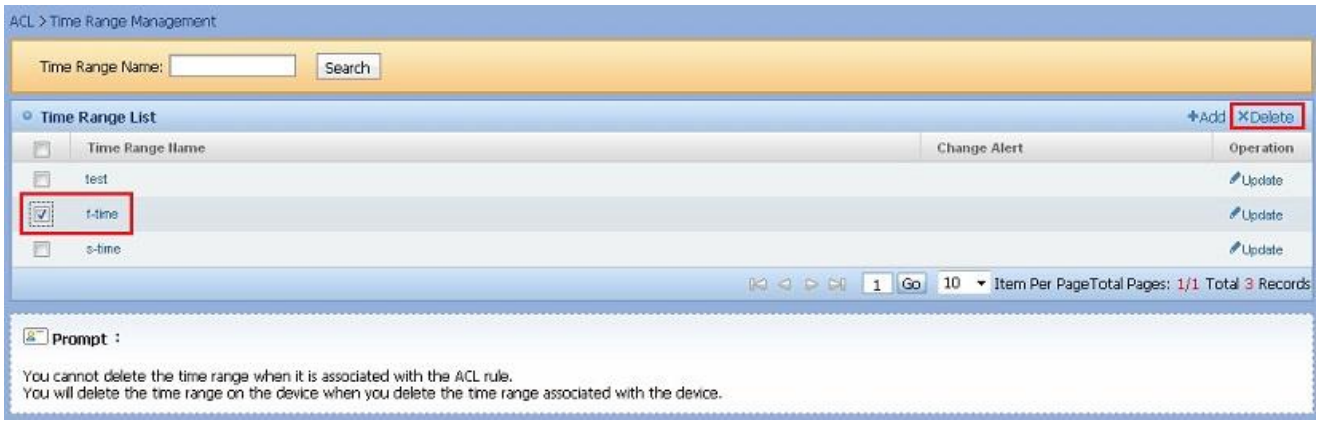


Figure 11.4. Delete Time Range

Figure 11.5. Delete Time Range related to ACL Rule in Device

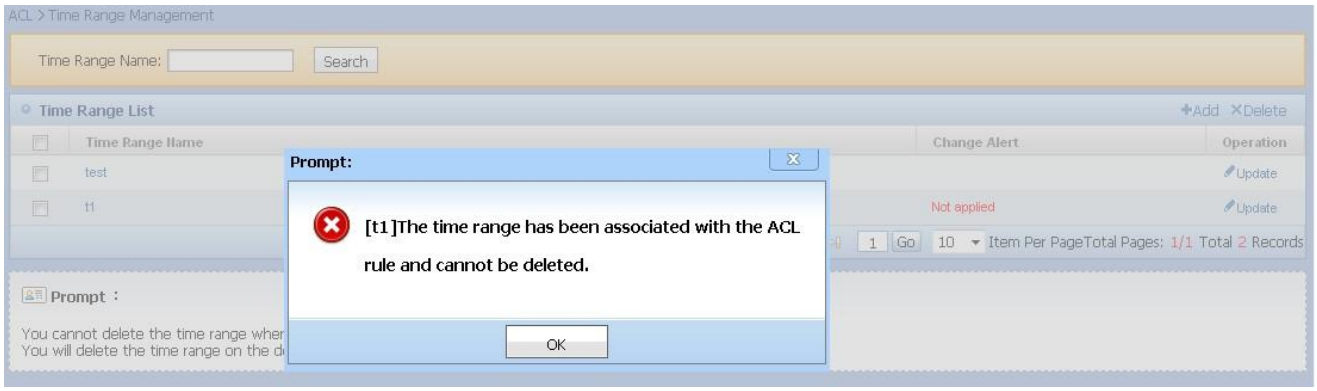


Figure 11.6. Fail to Delete Time Range related to ACL Rule in Device

Note

If Time Range is related to ACL Rule, it's not allowed to be deleted.

When deleting the time range, if it is related to the ACL device, the system will generate the deployment plan automatically and issue it immediately. When the background service does not start, you cannot generate a deployment plan or delete time range.

11.1.4. View Time Range

Detail information of time range, time list related to the time range, ACL rules list and device list can be viewed on page Detail Information of Time Range.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** of all the Time Ranges in the Time Range list to enter page **Detail Information of Time Range** for this Time Range, as shown in the following figure:

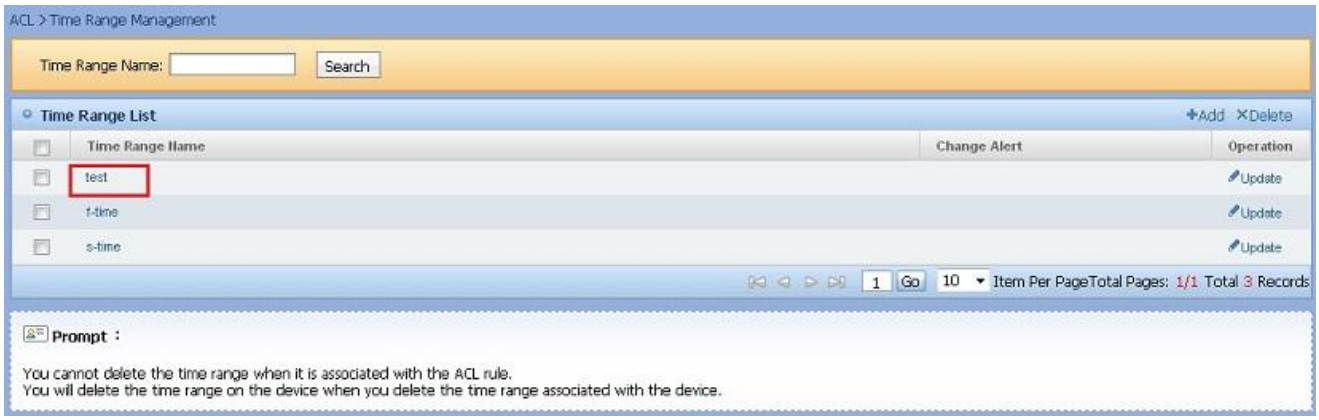


Figure 11.7. View Time Range

2) On page **Detail Information of Time Range**, detail information of time range, absolute time information, time list, ACL rules list and device list can be viewed, as shown in the following figure:

Figure 11.8. Detail Information of Time Range

Figure 11.9. Absolute time Information

Figure 11.10. Time List

Figure 11.11. ACL Rules List

Figure 11.12. Device List

11.1.5. Modify Time Range

Description information of Time Range can be modified in the system.

Operation Steps

1) On page **Time Range Management**, click icon **Update** to enter page **Edit Time Range**, as shown in the following figure:

Figure 11.13. Go to page **Modify Time Range**

2) Go to page **Modify Time Range**, fill in the information related to Time Range, and click **Modify** button, as shown in the following figure:

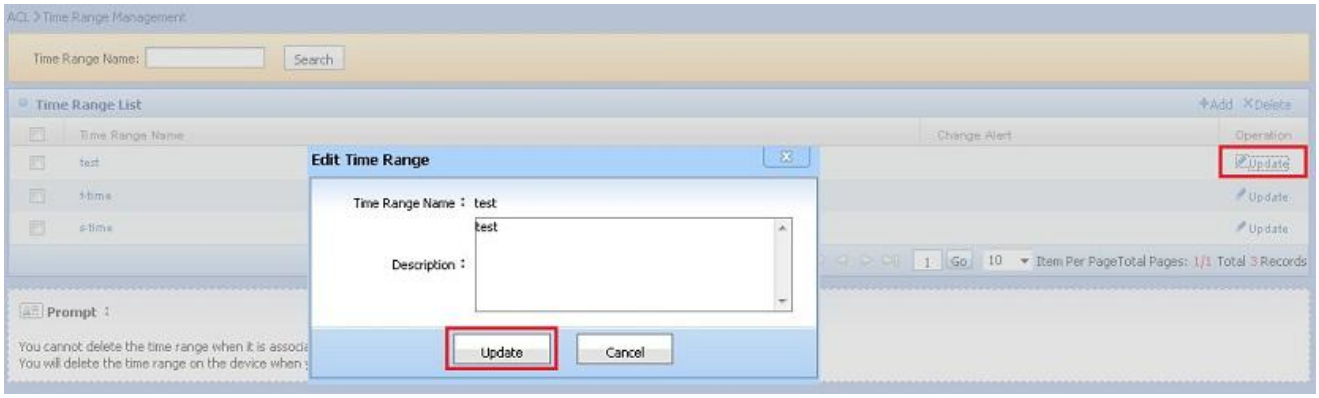


Figure 11.14. Edit Time Range

On page **Edit Time Range**, if **Cancel** is clicked, the system saves no modification and returns to **Detail Information of Time Range** page directly.

Note

Time range name must be consistent with the name deployed in device, and may affect the deployment of ACL rules. So it does not provide modification function for time rang name. Users can only modify the Description field, and modification of Description field does not affect the change warning of Time Range.

11.1.6. Redeploy Time Range

If a change warning is generated for a time range deployed on a device, the time range can be redeployed on this device.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** of Time Range in the Time Range list to enter page **Detail Information of Time Range** of this Time Range, as shown in the following figure:

Figure 11.15. Go to page **Redeploy Time Range**

2) Go to page **Detail Information of Time Range**, and click button **Redeploy** in change warning field. The system will prompt **Are you sure to overwrite all the Time Ranges with the same name on the device?** Click **Confirm** to execute the redeployment operation. **Change not applied** disappears in change warning field, as shown in the following figure:

Figure 11.16. Redeploy Time Range

Note

During redeploying time range, the system generates a deployment plan automatically and issues it immediately. If the background service does not start, deployment plan cannot be generated.

After redeploying time range, the system will update the signs of time range related to ACL device from inconsistent to consistent automatically.

11.1.7. Redeploy Time Range in Device

Time range already deployed can be redeployed in this device.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** of the Time Range in the Time Range list to enter page **Detail Information of Time Range** for this Time Range, as shown in the following figure:

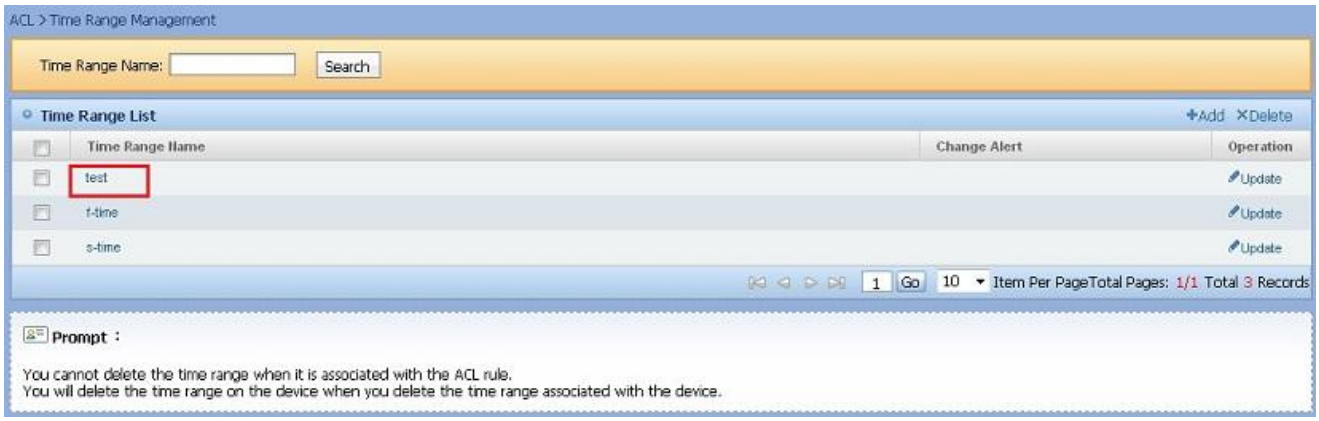


Figure 11.17. Go to page **Redeploy Time Range in Device**

2) Go to page **Detail Information of Time Range**, select corresponding device and click button **Redeploy** in device list. The system will prompt **Are you sure to overwrite the Time Range with the same name on the device?** Click **Confirm** to execute the redeployment operation, as shown in the following figure:

Figure 11.18. Redeploy Time Range in Device

Note Since redeploying the time range in device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.1.8. Absolute Time Management

This module describes the functionality of adding, deleting and modifying Absolute Time of Time Range.

- Add Absolute Time Information
- Modify Absolute Time Information
- Delete Absolute Time Information

11.1.8.1. Add Absolute Time Information

Absolute time has to be added to the system to be managed by the system.

Operation Steps

1) On page **Time Range Management**, click the link of **Time Range Name** in the time range of time ranges list to enter page **Detail Information of Time Range** for the time period, as shown in following figure:

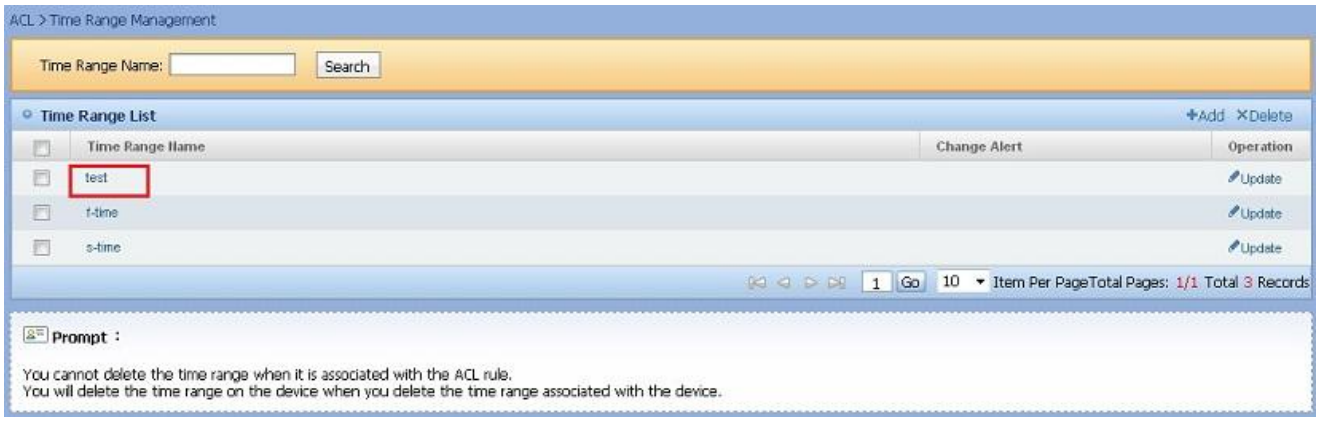


Figure 11.19. View Time Range

2) Go to page **Detail Information of Time Range**, click the button **Add Absolute Time Information** in the basic information to enter page **Add Absolute Time Information** for the time period, as shown in following figure:

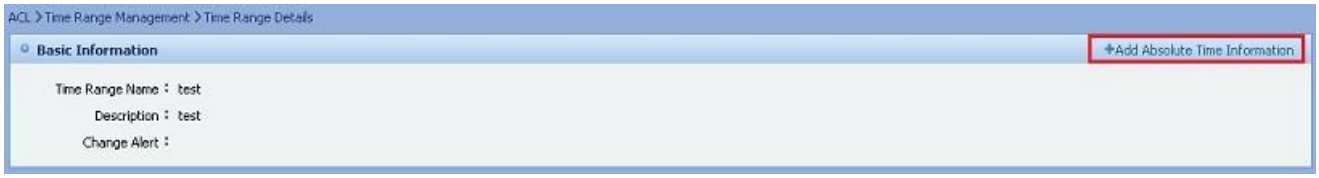


Figure 11.20. Go to page **Add Absolute Time Information**

3) Go to page **Add Absolute Time Information**, fill in time information, and click **Add** button, as shown in following figure:

Figure 11.21. Add Absolute Time Information

Note

End time is not allowed to be earlier then start time.

If the time range which Absolute Time Information belongs to has been deployed to the device, then change warning for this Time Range appears.

11.1.8.2. Modify Absolute Time Information

Absolute Time Information can be modified in the system.

Operation Steps

1) On page **Time Range Management**, click the link of **Time Range Name** in the time range of time ranges list to enter page **Detail Information of Time Range** for the time period, as shown in following figure:

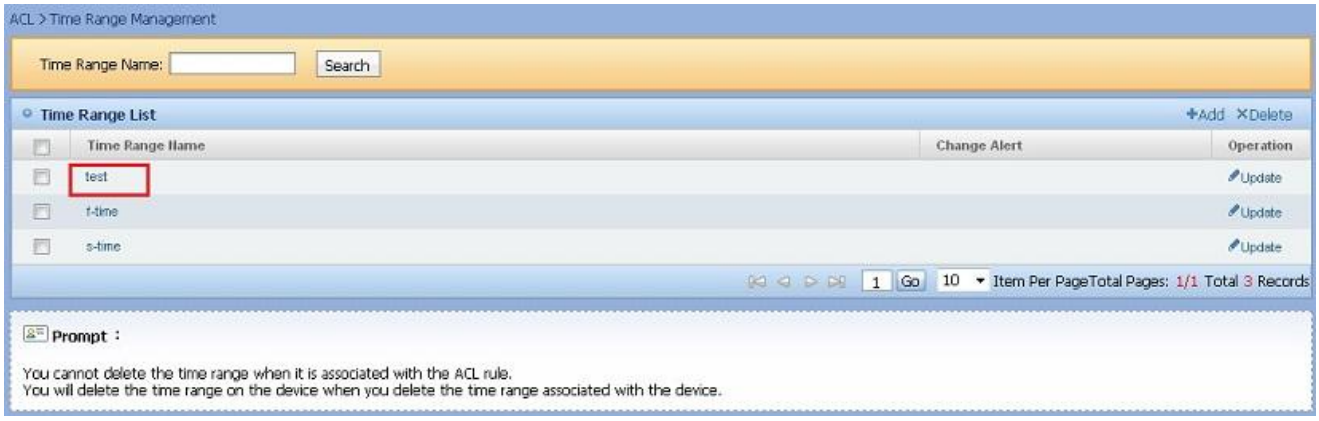


Figure 11.22. View Time Range

2) Go to page **Detail Information of Time Range**, click the button **Update** in the Absolute Time Information list, enter page **Modify Absolute Time Information** for the time period, as shown in following figure:

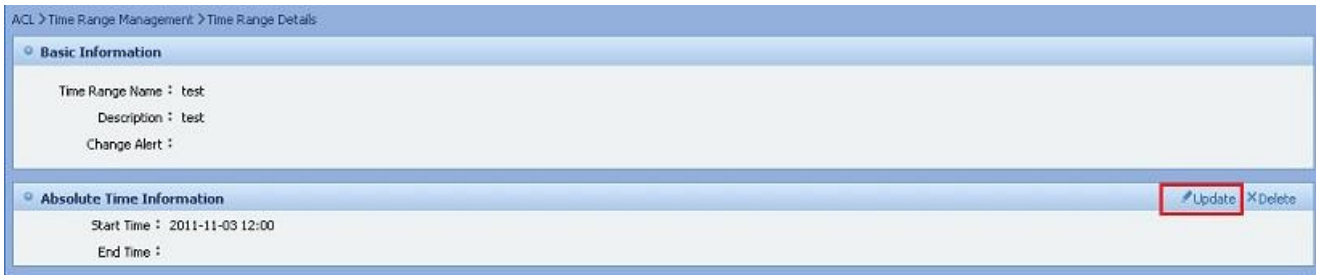


Figure 11.23. Go to page **Modify Absolute Time Information**

3) Go to page **Modify Absolute Time Information**, fill in time information, and click **Update** button, as shown in following figure:

Figure 11.24. Modify Absolute Time Information

Note

End time is not allowed to be earlier then start time.

If the time range which Absolute Time Information belongs to has been deployed to the device, then change warning for this Time Range appears.

11.1.8.3. Delete Absolute Time Information

Absolute Time Information can be deleted on page **Detail Information of Time Range**.

Operation Steps

1) On page **Time Range Management**, click the link of **Time Range Name** in the time range of time ranges list to enter page **Detail Information of Time Range** for the time period, as shown in following figure:

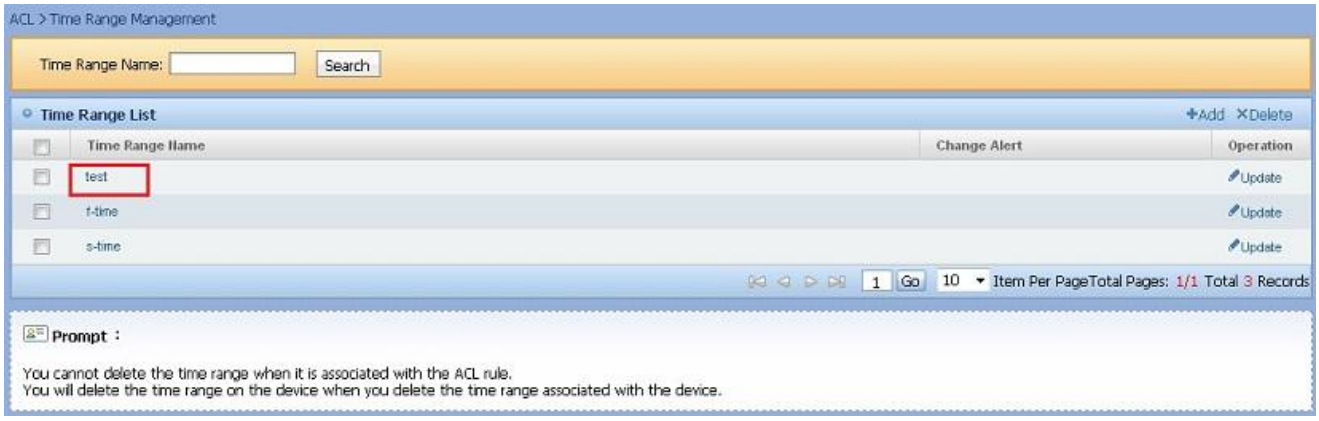


Figure 11.25. View Time Range

2) Go to page **Detail Information of Time Range**, click the button **Delete** in the Absolute Time Information list. The system will prompts you to confirm the deletion. Click **OK** to complete the deletion, as shown in following figure:

Figure 11.26. Delete Absolute Time Information

Note

If the time range which Absolute Time Information belongs to has been deployed to the device, then change warning for this Time Range appears.

11.1.9. Time Information Management

This module describes functions of adding, deleting, modifying and viewing time information of time range.

- Add Time Information
- Modify Time Information
- Delete Time Information

11.1.9.1. Add Time Information

Time Information has to be added to the system to be managed by the system.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** of the Time Range in the Time Range list to enter page **Detail Information of Time Range** for this Time Range, as shown in the following figure:

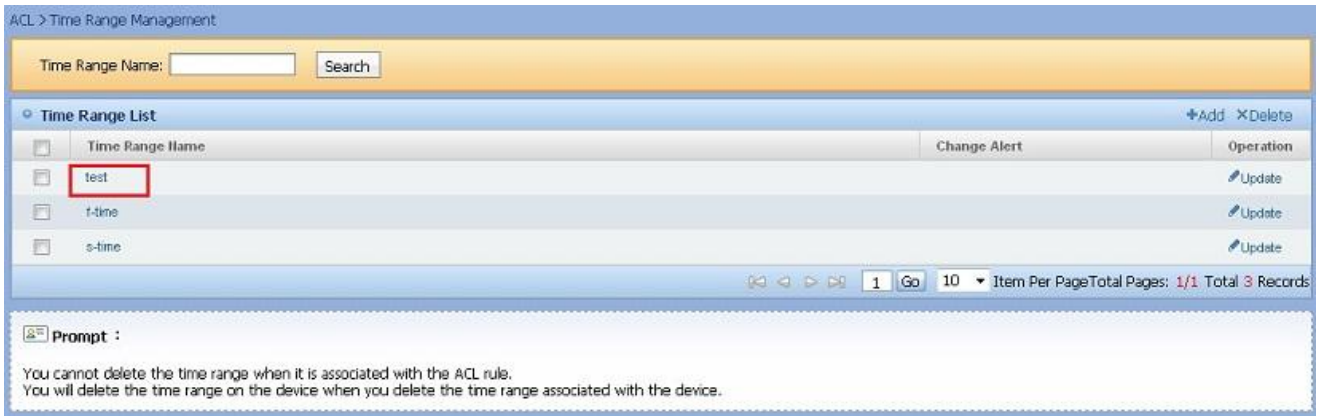


Figure 11.27. View Time Range

2) Go to page **Detail Information of Time Range**, and click **Add** button in the Time Range list to enter page **Add Time Information**, as shown in the following figure:

Figure 11.28. Go to page **Add Time Information**

3) Go to page **Add Time Information**, fill in the information related to Time Range, and click **Add** button, as shown in the following figure:

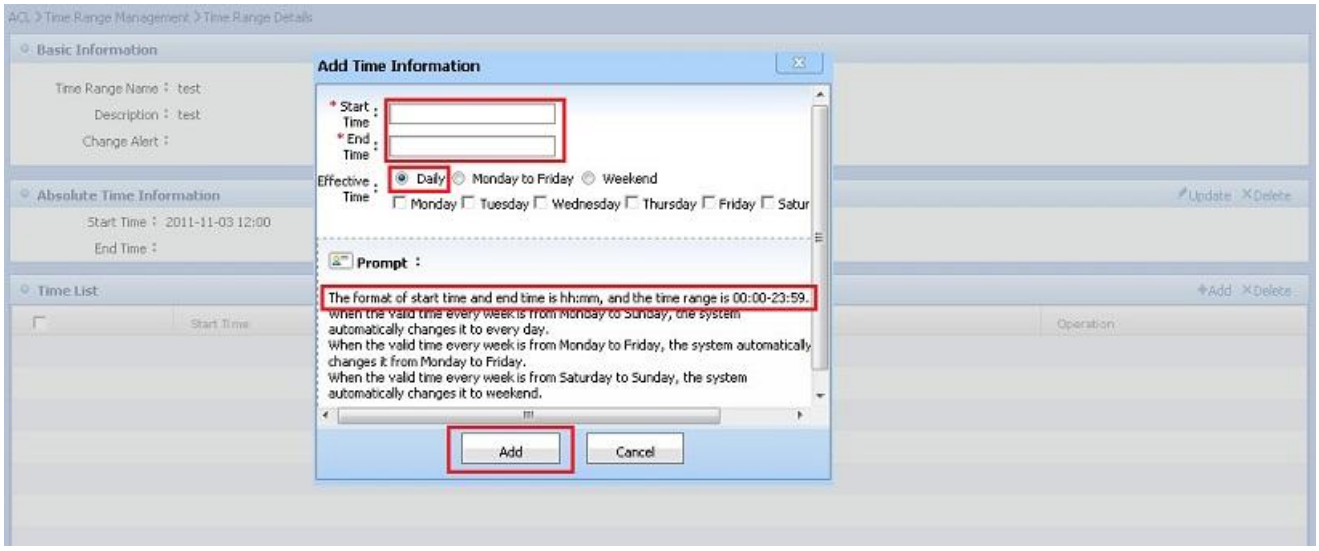


Figure 11.29. Add Time Information

On page **Add Time Range**, if **Cancel** is clicked, the system saves no modification and returns to **Detail Information of Time Range** page directly.

Note

Start time and end time must be in the format hh: mm. Time range is 0:00-23:59.

End time should not be earlier than start time.

Valid time per week: The range is as follows: From Monday to Sunday, several options can be selected; Daily, Monday to Friday and Weekends, these three options are mutually exclusive to each other and to **Monday to Sunday**.

If the time range which the time information belongs to has been deployed to device, then change warning of this time range appears.

If you select the valid time per week as Monday, Tuesday, Wednesday, Thursday, Friday, the system will convert it to from Monday to Friday automatically; if you select Saturday, Sunday, the system will convert it to Weekend automatically; if you select all the days from Monday to Sunday, the system will convert it into Daily automatically.

11.1.9.2. Modify Time Information

Basic information of Time Information can be modified in the system.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** of the Time Range in the Time Range list to enter page **Detail Information of Time Range** for this Time Range, as shown in the following figure:

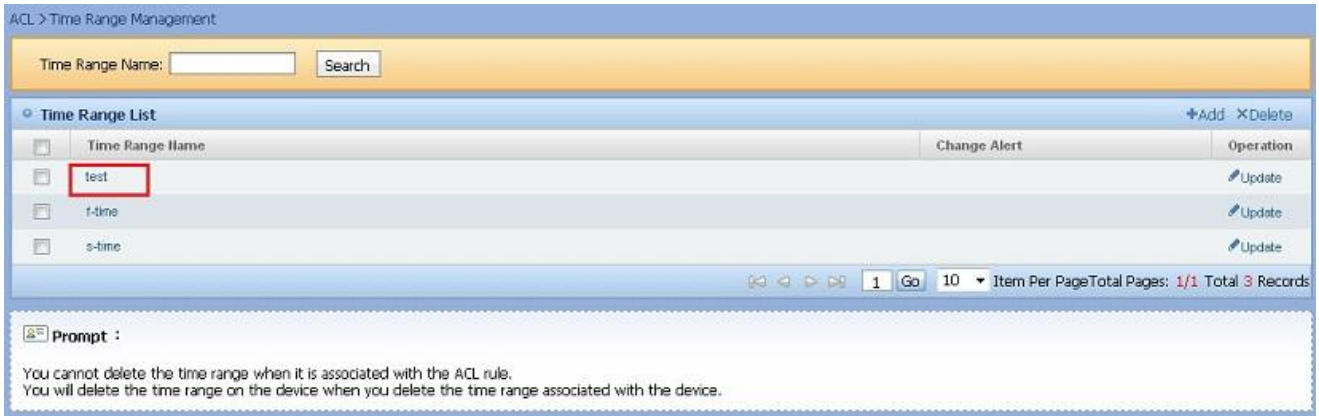


Figure 11.30. View Time Range

2) Go to page **Detail Information of Time Range**, and click on **Update** button in the Time Range list to enter page **Edit Time Information**, as shown in the following figure:

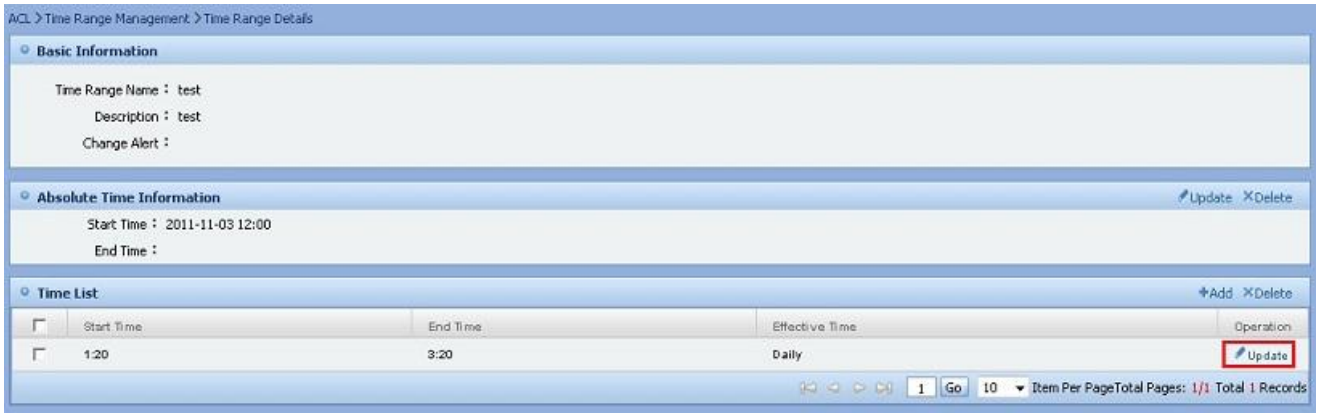


Figure 11.31. Go to page **Edit Time Information**

3) Go to page **Edit Time Information**, fill in the information related to Time Range, and click **Update** button, as shown in the following figure:

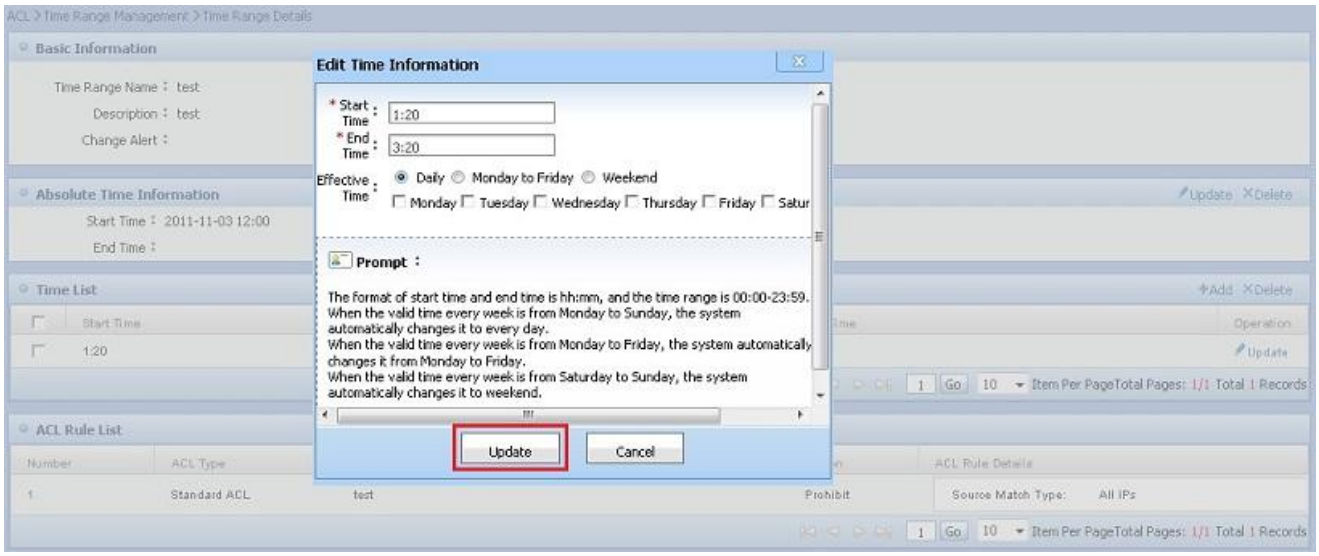


Figure 11.32. Edit Time Information

On page **Edit Time Range**, if **Cancel** is clicked, the system saves no modification and returns to **Detail Information of Time Range** page directly.

Note

Start time and end time must be in the format hh: mm. Time range is 0:00-23:59.

End time should not be earlier than start time.

Valid time per week: The range is as follows: From Monday to Sunday, several options can be selected; Daily, Monday to Friday and Weekends, these three options are mutually exclusive to each other and to **Monday to Sunday**.

If the time range which the time information belongs to has been deployed to device, then change warning of this time range appears.

If you select the valid time per week as Monday, Tuesday, Wednesday, Thursday, Friday, the system will convert it to from Monday to Friday automatically; if you select Saturday, Sunday, the system will convert it to Weekend automatically ; if you select all the days from Monday to Sunday, the system will convert it into Daily automatically.

11.1.9.3. Delete Time Information

Time Information can be deleted on page **Detail Information of Time Range**.

Operation Steps

1) On page **Time Range Management**, click the link **Time Range Name** in the Time Range list to enter page **Detail Information of Time Range** for this Time Range, as shown in the following figure:

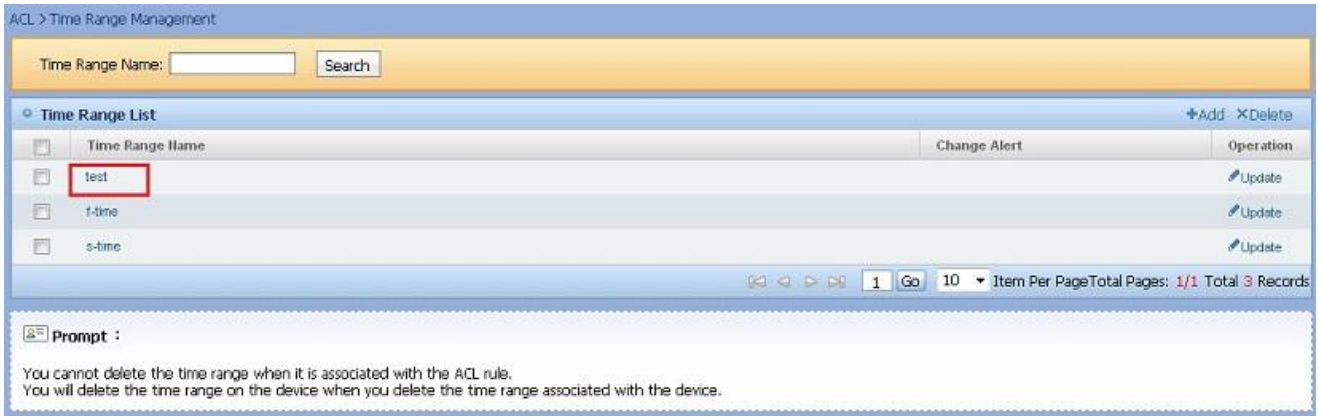


Figure 11.33. View Time Range

2) In **Time Range Management**, click button **Delete** in time range list. The system will prompt you to confirm the deletion operation. Click button **Confirm** to perform the deletion operation, as shown in the following figure:

Figure 11.34. Delete Time Information

Note If the time range which the time information belongs to has been deployed to device, then change warning of this time range appears.

11.2. ACL Management

ACL is used to determine the type of ACL rule, and ACL management also includes management of ACL rules.

- Add ACL
- Search ACL
- Delete ACL
- View ACL
- Modify ACL
- Import ACL
- Export ACL
- Redeploy Changed ACL
- ACL Rule Management
- ACL Rule Management on Device

11.2.1. Add ACL

ACL has to be added to the system to be managed by the system.

Operation Steps

1) On page **ACL Management**, click button **Add** to enter page **Add ACL**, as shown in following figure:

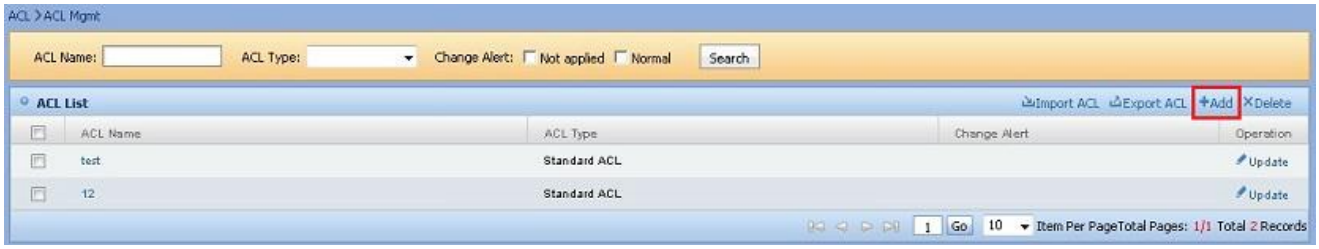


Figure 11.35. Go to page **Add ACL**

2) Go to page **Add ACL**, fill in the information related to ACL, and click **Add** button, as shown in following figure:

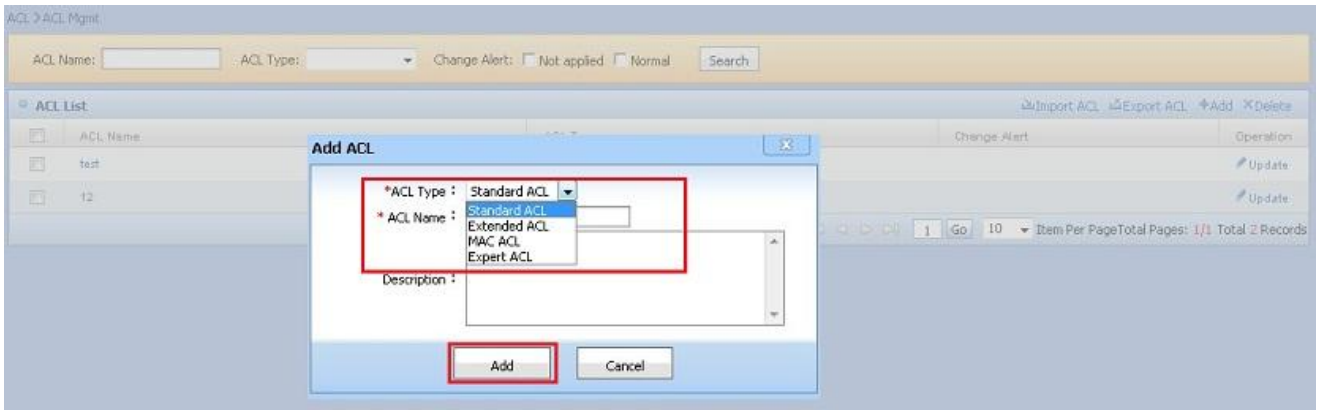


Figure 11.36. Add ACL

On page **Add ACL**, if **Cancel** is clicked, the system saves no modification and returns to **ACL Management** page directly.

Note

ACL types: standard IP access, extended IP access, MAC extended access, and expert extended access.

ACL name cannot be repeated.

ACL name cannot contain Chinese or full-width characters. If it starts with a digit, it cannot contain characters other than digits. A numerical value is regarded as a serial number and must comply with the numbering rules. As equipment of different manufacturers has different numbering rules, the limitations need to considered. Distinguish them according to the type of ACL. The numbering rules of Ruijie ACL devices are as follows:

a) Standard IP access list: number range is 1-99,1300-1999

b) Extended IP access list: number range is 100-199,2000-2699

c) MAC extended access list: number range is 700-799

d) Expert extended access list: number range is 2700-2899

11.2.2. Search ACL

ACL name, ACL type and change alert can be filled in to searched for ACL managed by system on page **ACL management**.

Operating Steps

Go to page **ACL management**, fill in ACL name, ACL type and change alert, and then click **Search** button. The system will return ACL list which satisfy search conditions, as shown in the following figure:

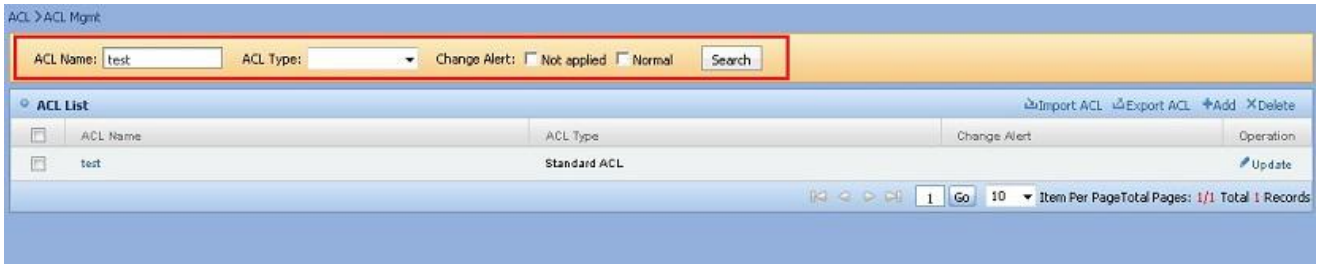


Figure 11.37. Search ACL

11.2.3. Delete ACL

ACL can be deleted in batch on page **ACL Management**.

Operation Steps

On page **ACL Management**, select some ACLs in the ACL list, and click button **Delete**. The system will prompt you to confirm the deletion. Click **Confirm** to delete selected ACL, as shown in following figure:

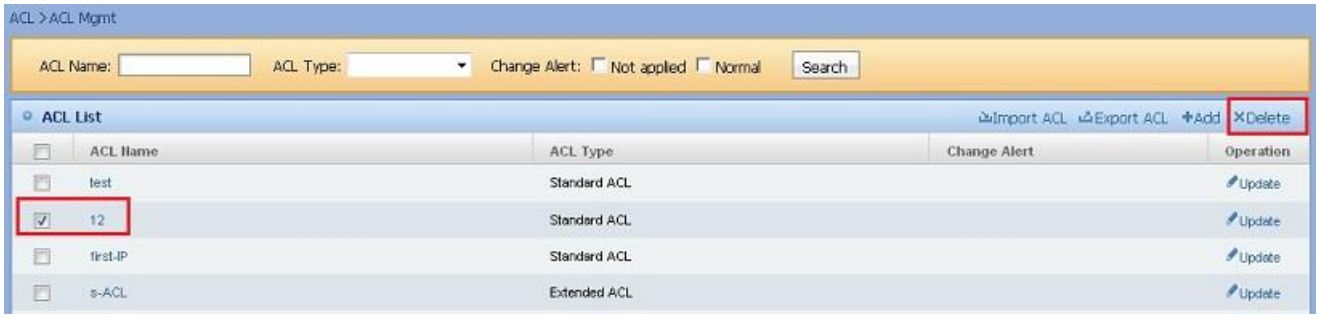


Figure 11.38. Delete ACL

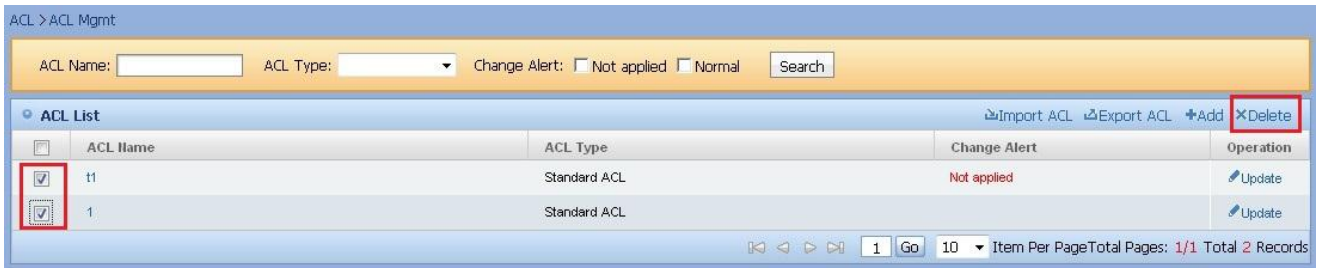


Figure 11.39. Delete the ACL associated to device

Note

When deleting ACL, if the ACL is associated to device, the system will generate the deployment plan automatically and issue it immediately.

If the background services are not started, you cannot create a deployment plan or delete ACL.

11.2.4. View ACL

Detail Information of ACL, Time list associated with the ACL, ACL rules list and device list can be viewed on page Detail Information of ACL.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

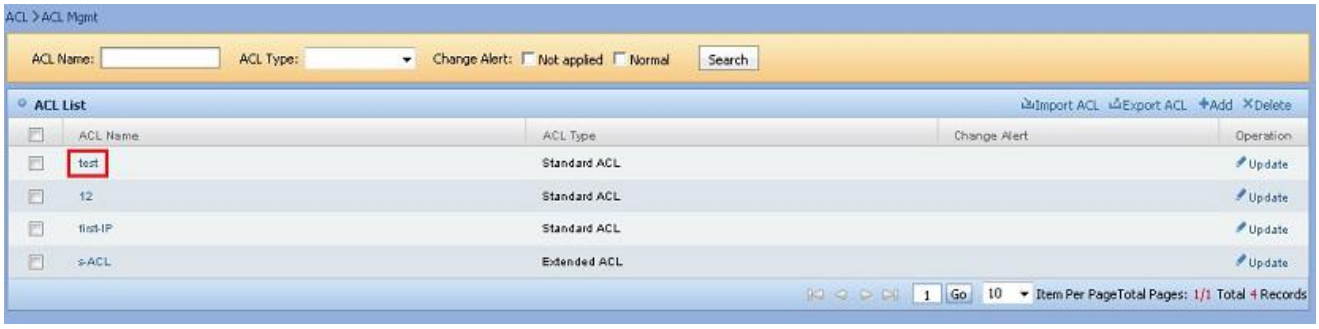


Figure 11.40. View ACL

2) On page **Detail Information of ACL**, Detail Information of ACL, ACL rules list and device list can be viewed, as shown in following figure:

Figure 11.41. Detail Information of ACL

Figure 11.42. ACL Rules List

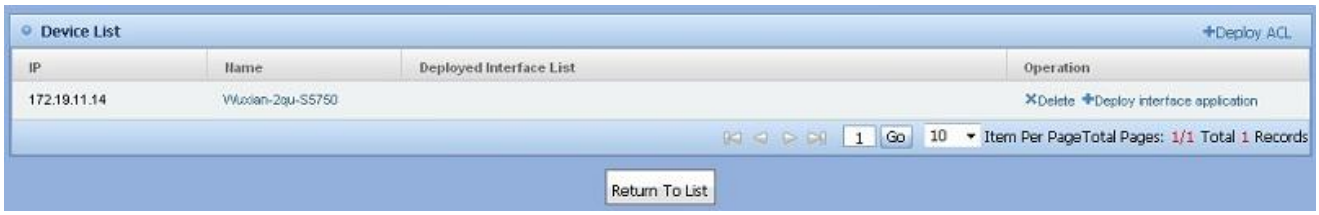


Figure 11.43. Device List

11.2.5. Modify ACL

Description of ACL can be modified in the system.

Operation Steps

1) On page **ACL Management**, click icon **Update** to enter page **Edit ACL**, as shown in following figure:

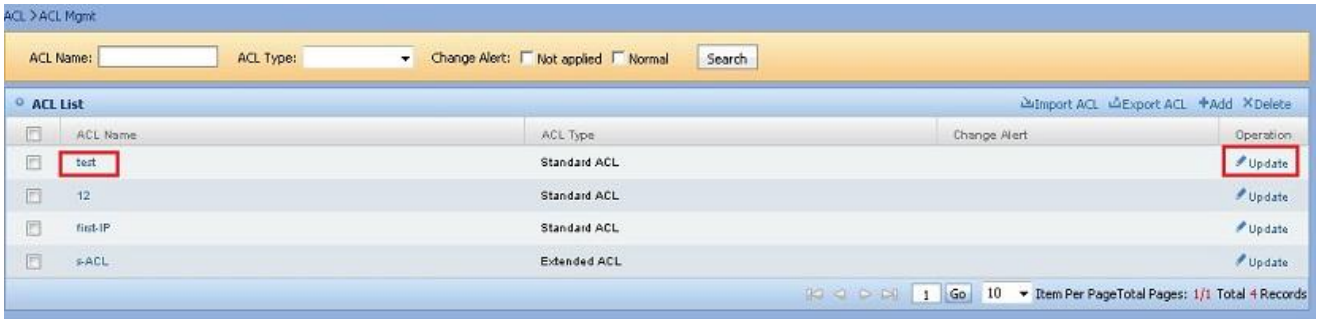


Figure 11.44. Go to page **Edit ACL**

2) Go to page **Edit ACL**, fill in the information related to ACL, and click **Update** button, as shown in following figure:

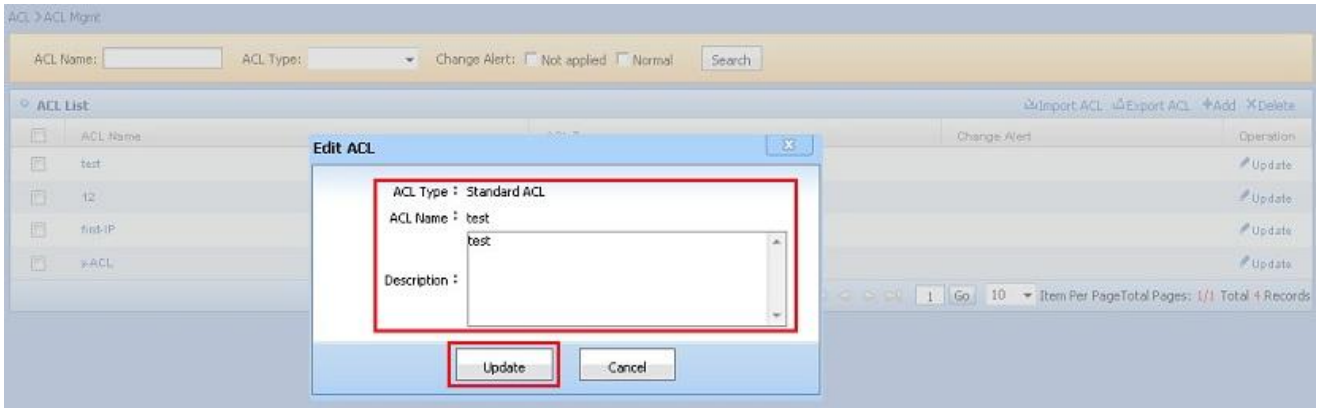


Figure 11.45. Edit ACL

On page **Edit ACL**, if **Cancel** is clicked, the system saves no modification and returns to **ACL Management** page directly.

Note

Only description can be modified, and the modification does not change the description of change alert of ACL.

11.2.6. Import ACL

The rules and time range information associated with the ACL can be imported from text.

Operation Steps

1) On page **ACL Management**, click the **Import ACL** button to enter page **Import ACL**, as shown in following figure:

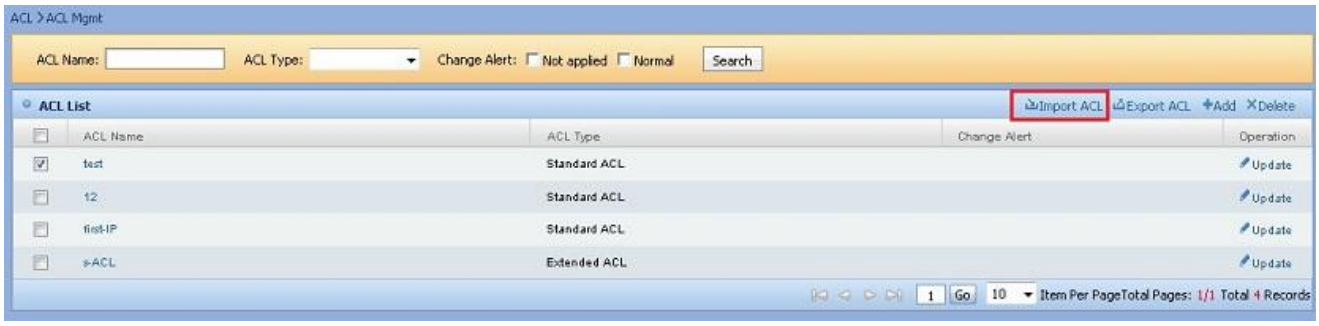


Figure 11.46. Import ACL

2) On page **Import ACL**, click the button **Select Imported File**, and select file to be imported from the Select File dialog box, and click **Open** to select the file to be imported, as shown in following figure:

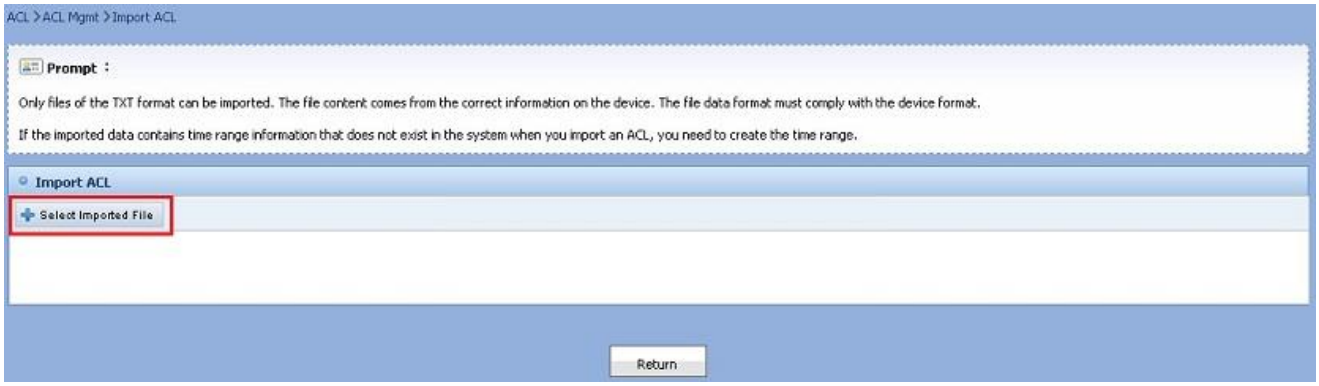


Figure 11.47. Select Imported File

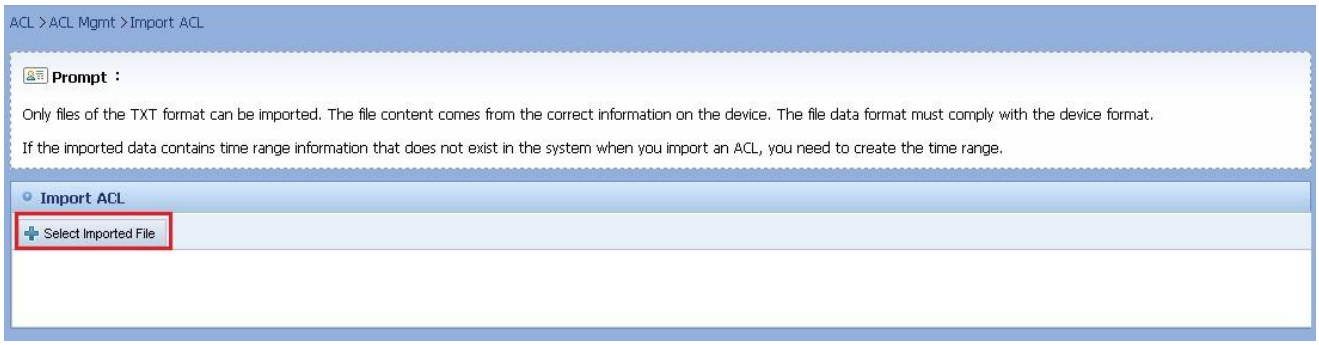


Figure 11.48. Confirm selected file

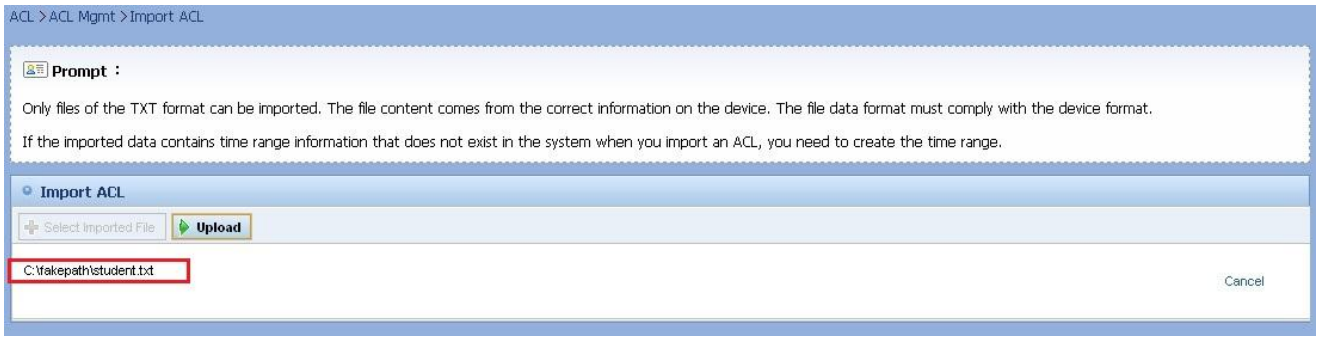


Figure 11.49. Select file successfully

3) After successfully selecting a file, click **Upload** button. The system will upload the file and import ACL in the file, as shown in following figure:

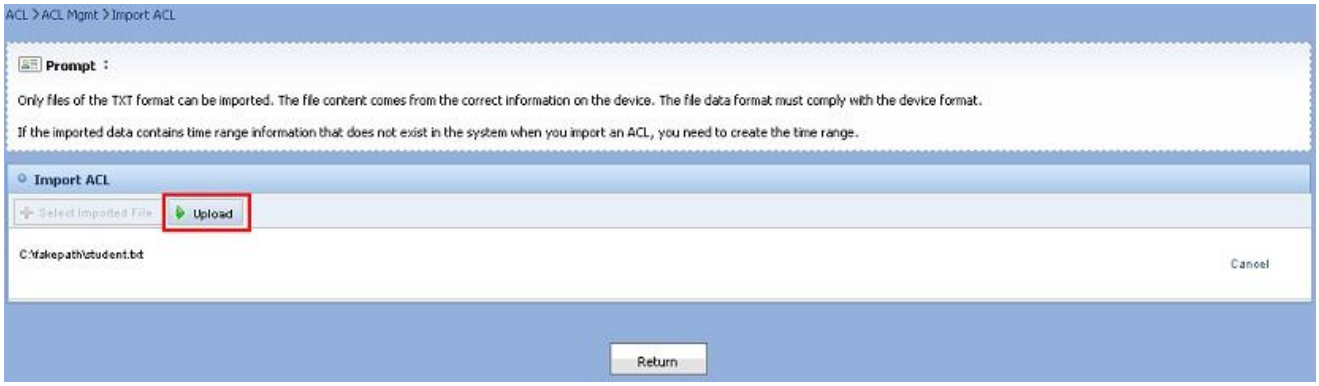


Figure 11.50. Upload File

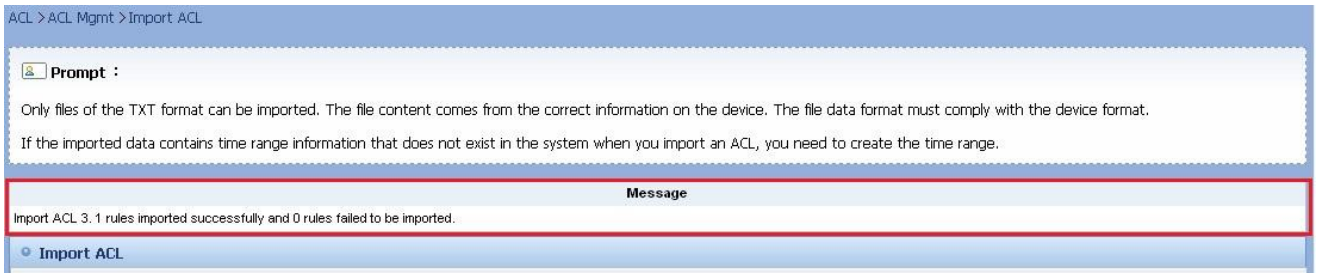


Figure 11.51. Upload File Successfully

After importing ACL successfully, click the **Return** button to return to **ACL Management** page.

Note

Only txt (text) format file can be imported. The contents and format of the file should be the same as that on device.

If the irrelevant data is imported, the system prompts data resolution failure.

If the same name already exists, the system prompts repeated name and importing failure.

During importing, if the time range in the text does not exist, create and save time range; if time range of the same name already exists, do not create a new time range and reference the system time range directly.

11.2.7. Export ACL

You can export the rules and time range information associated with the ACL in batch.

Operation Steps

On page **ACL Management**, select ACL to be exported, and then click the **Export ACL** button. The system will display download dialog box. Select download, as shown in following figure:

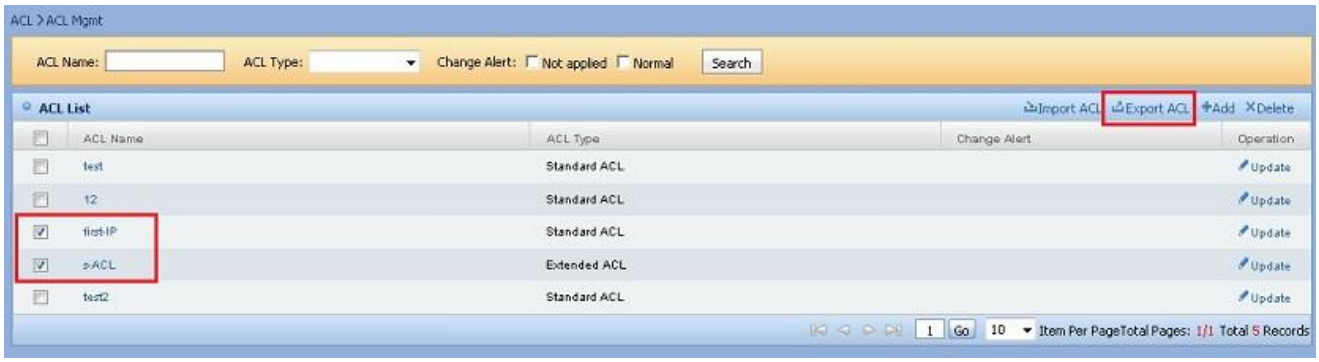


Figure 11.52. Export ACL

Figure 11.53. Download Dialog Box for ACL

Note Export object: ACL, ACL rules and related time ranges.

11.2.8. Redeploy Changed ACL

If a change alert is generated for an ACL deployed on device, the ACL can be redeployed.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

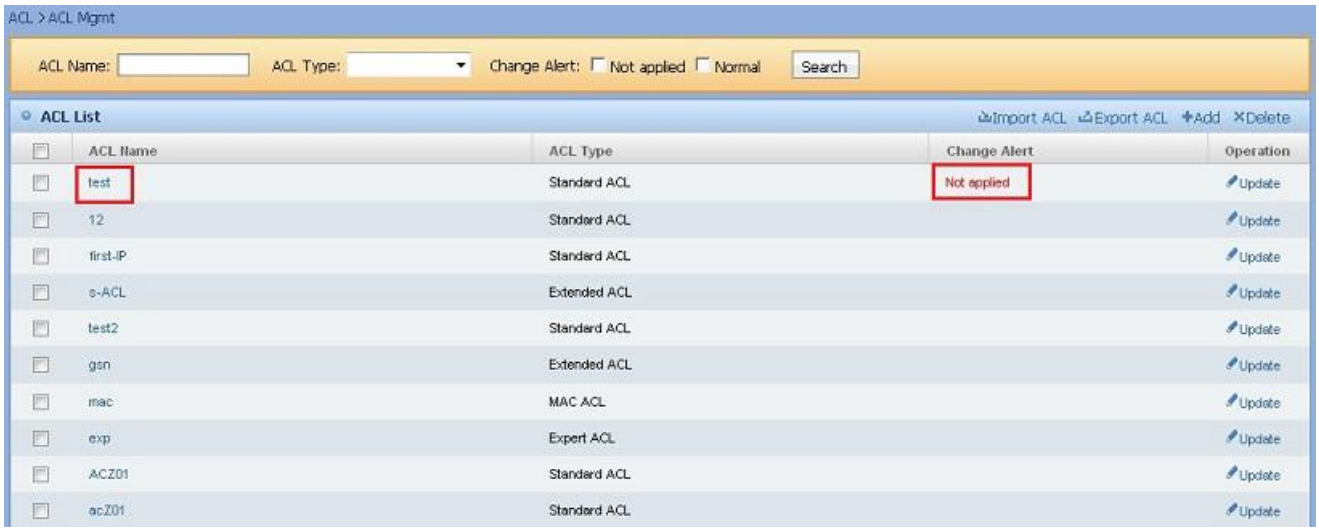


Figure 11.54. Go to page **Detail Information of ACL**

2) In **Device List**, click the button **Redeploy** in **operation** bar. The system will prompt **Are you sure to overwrite ACL with the same name on all the devices?** Click **Confirm** to complete the redeployment operation. **Not applied** will disappear in change alert field, as shown in following figure:

Figure 11.55. Redeploy Changed ACL

Figure 11.56. Redeploy Changed ACL Successfully

3) Enter page **ACL Deployment Plan management**, and click **Plan Name** link of the most recently generated plan to view the status of redeployment of changed ACL, as shown in following figure:

Figure 11.57. Enter page **View the status of redeployment of changed ACL**

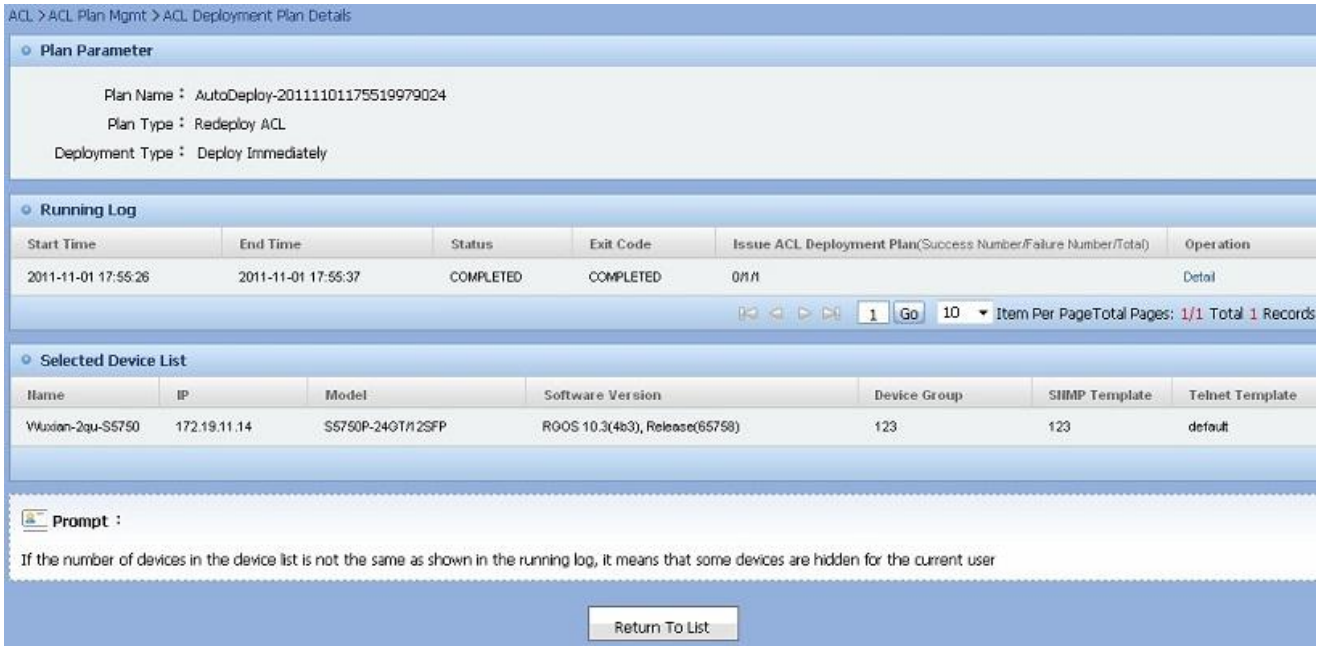


Figure 11.58. View the Status of Redeployment of Changed ACL

Note

When redeploying ACL on device, the system will generate a deployment plan automatically and issue it directly. If background service is not started, no deployment plan is generated.

After ACL redeployment, the system will change the inconsistent sign of ACL associated with ACL device to consistent sign automatically.

11.2.9. ACL Rule Management

This module describes the functionality of adding, deleting, modifying, showing and adjusting the order of ACL rules in ACL.

- Add ACL Rule
- Modify ACL Rule
- Delete ACL Rule
- View ACL Rule
- Adjust Order of ACL Rule

11.2.9.1. Add ACL Rule

There are four types of ACL rules: Standard ACL Rule, Extended ACL Rule, MAC ACL Rule, Expert ACL Rule. All the rules can be added in this module.

- Add Standard ACL Rule
- Add Extended ACL Rule
- Add MAC ACL Rule
- Add Expert ACL Rule

11.2.9.1.1. Add Standard ACL Rule

Standard ACL Rule can be added in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **Standard ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Add** in the **ACL List** to enter page **Add ACL Rule**, as shown in following figure:

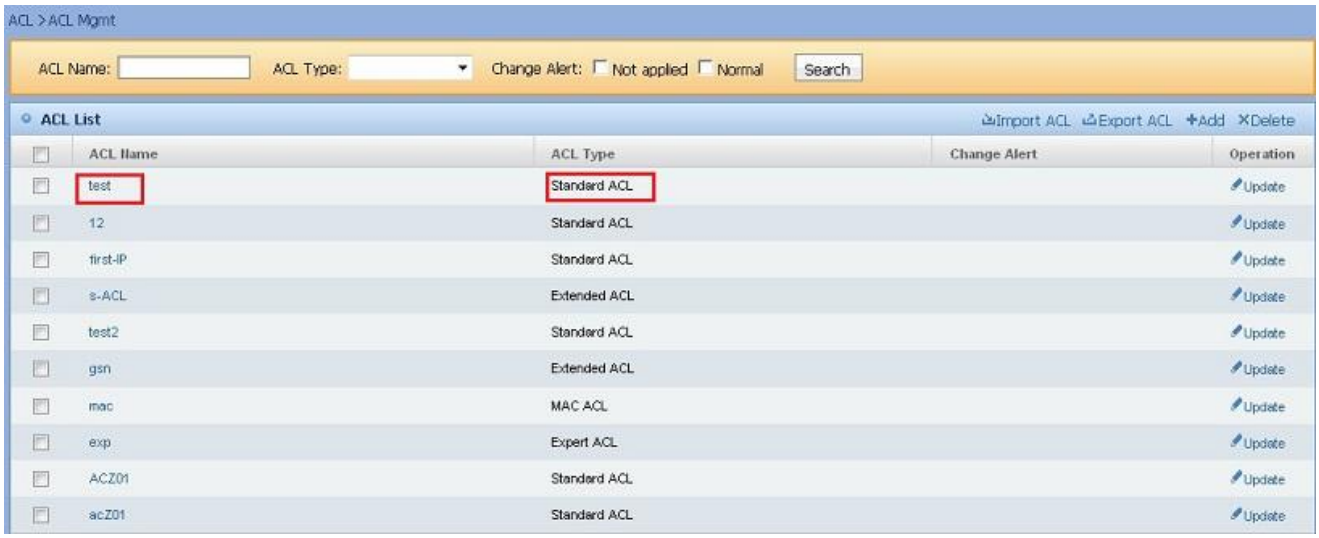


Figure 11.59. Go to page **Detail information of Standard ACL**

Figure 11.60. Go to page **Add Standard ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in following figure:

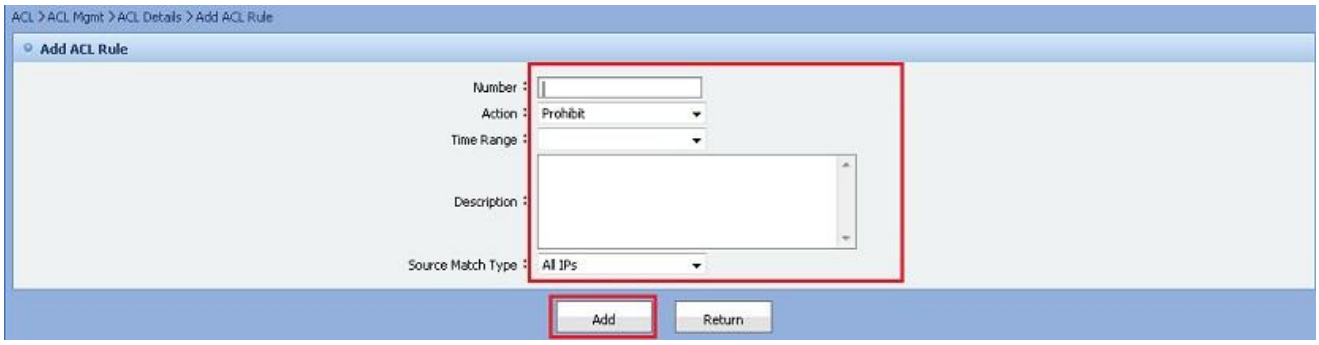


Figure 11.61. Add Standard ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs have been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

Source address: When the source match type is **Host** or **Network segment**, it can be display and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

If protocol type of some devices is not filled in, IP protocol will be added to the device automatically.

When rules are issued to device, some devices will adjust the order of the rules automatically.

11.2.9.1.2. Add Extended ACL Rule

Extended ACL Rule can be added in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **Extended ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in following figure:

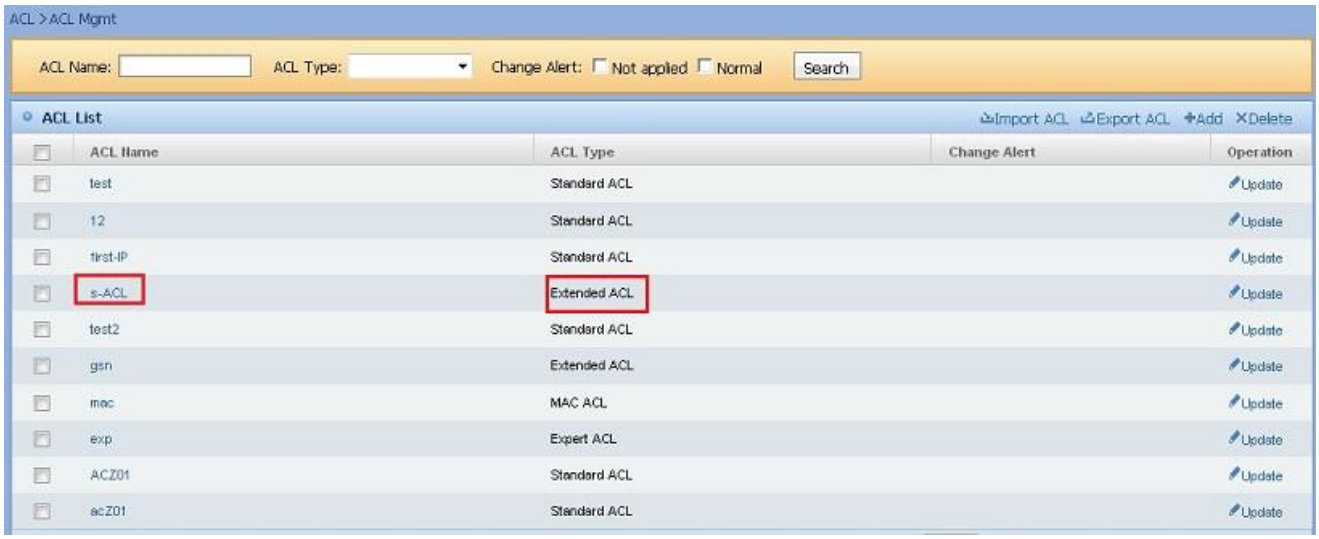


Figure 11.62. Go to page **Detail information of Extended ACL**

Figure 11.63. Go to page **Add Extended ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in following figure:

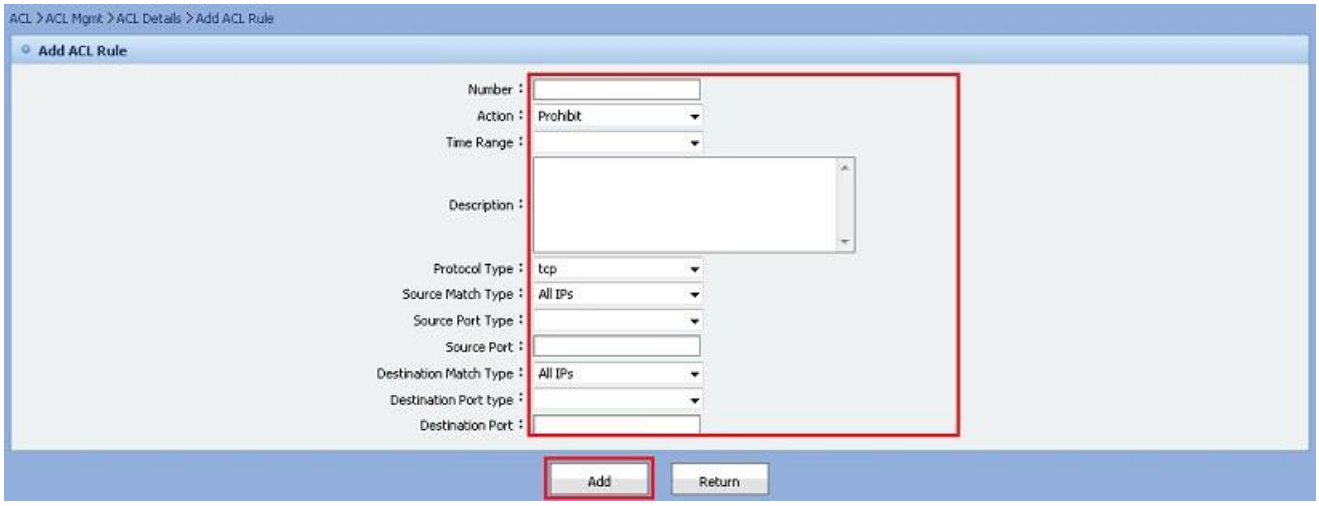


Figure 11.64. Add Extended ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

Source address: When the source matching type is **Host** or **Network segment**, it can be display and input. IP address does not support input with range.

Source wildcard: Only when the source matching type is **Network Segment**, it can be displayed and input.

Source(Destination) port: Only when the protocol type is TCP or UDP, it can be displayed and input. Port operator in the current system supports only eq.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

If protocol type of some devices is not filled in, IP protocol will be added to the device automatically.

When rules are issued to device, some devices will adjust the order of the rules automatically.

11.2.9.1.3. Add MAC ACL Rule

MAC ACL Rule can be added in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **MAC ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in following figure:

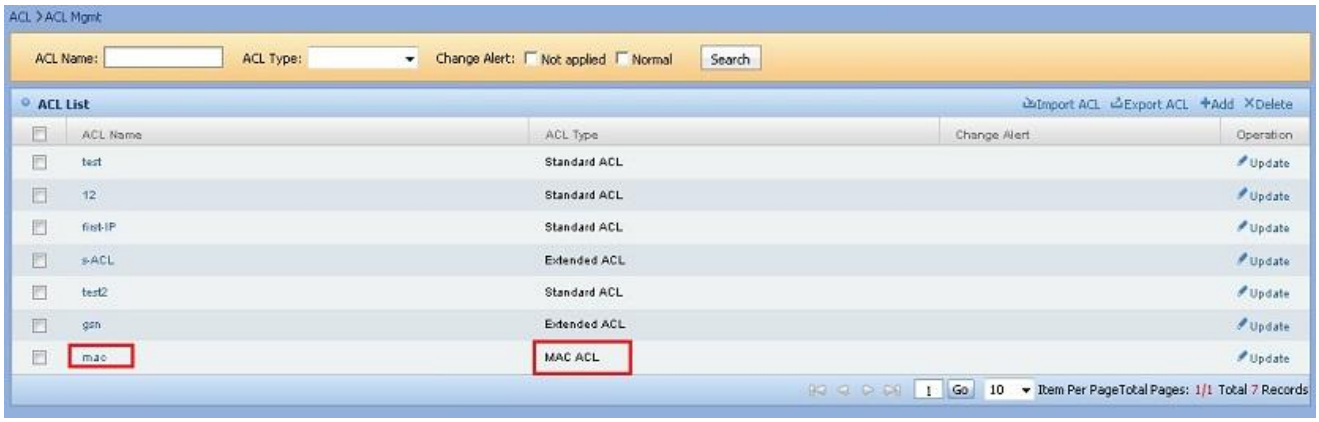


Figure 11.65. Go to page **Detail information of MAC ACL**

Figure 11.66. Go to page **Add MAC ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in following figure:

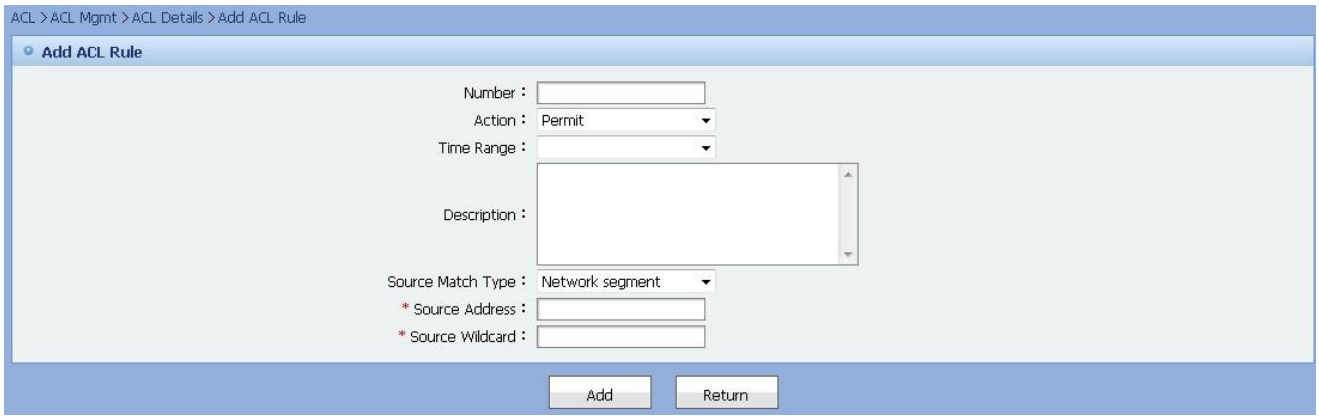


Figure 11.67. Add MAC ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

Ethernet protocol type can be empty.

Source (Destination) MAC address: When the source MAC match type is **Host**, it can be displayed and input.

If protocol type of some devices is not filled in, IP protocol will be added to the device automatically.

When rules are issued to device, some devices will adjust the order of the rules automatically.

11.2.9.1.4. Add Expert ACL Rule

Expert ACL Rule can be added in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **Expert ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click **Add** in the **ACL List** to enter page **Add ACL Rule**, as shown in following figure:

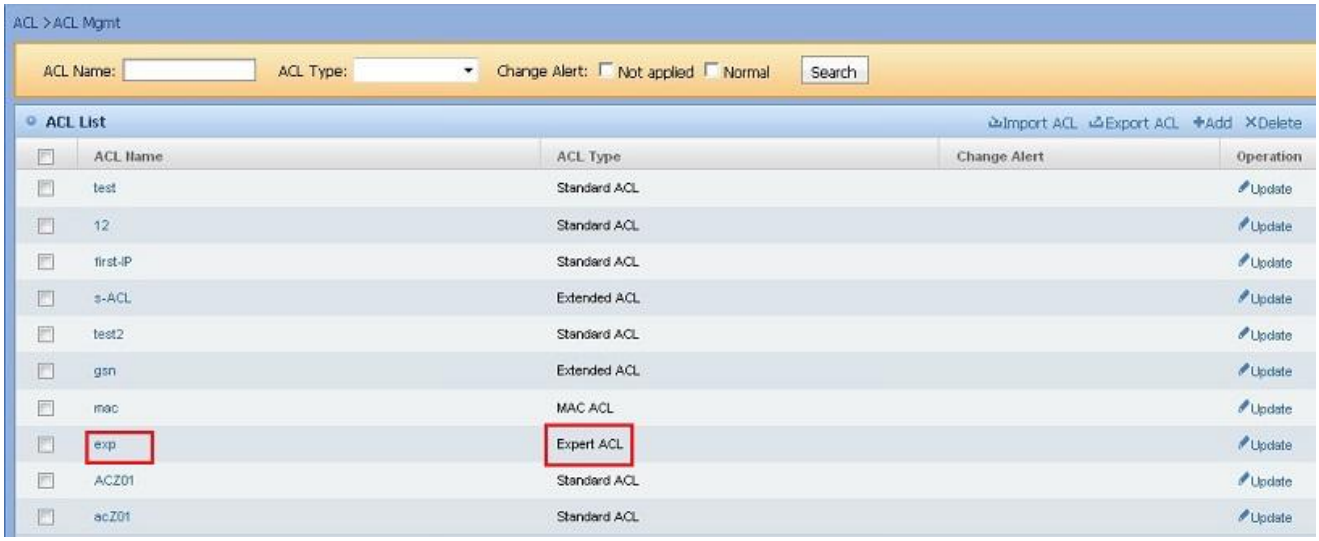


Figure 11.68. Go to page **Detail information of Expert ACL**

Figure 11.69. Go to page **Add Expert ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in following figure:

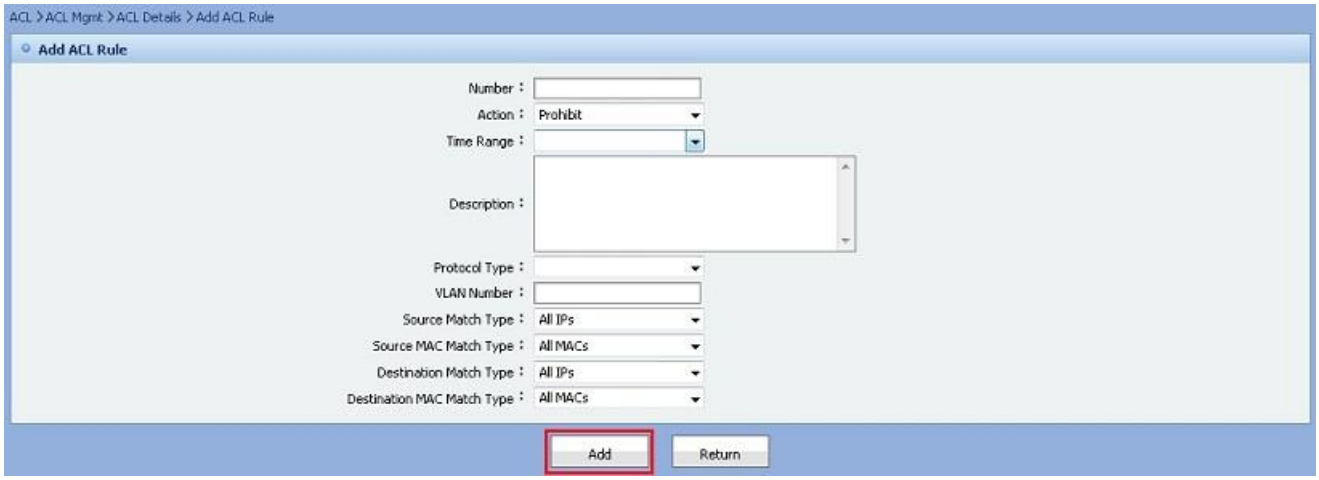


Figure 11.70. Add Expert ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

In cases of different protocol types, the system will display different input field.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

If serial number is not filled in or the filled serial number is greater than the actual number of rules, this rule is added as the last one; if filled serial number already exists, then this rule will be added before specified serial number rules.

If protocol type of some devices is not filled in, IP protocol will be added to the device automatically.

When rules are issued to device, some devices will adjust the order of the rules automatically.

11.2.9.2. Modify ACL Rule

There are four types of ACL rules: Standard ACL Rule, Extended ACL Rule, MAC ACL Rule, and Expert ACL Rule. All the rules can be modified in this module.

- Modify Standard ACL Rule
- Modify Extended ACL Rule
- Modify MAC ACL Rule
- Modify Expert ACL Rule

11.2.9.2.1. Modify Standard ACL Rule

Standard ACL Rule can be modified in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **Standard ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Update** in the **ACL List** to enter page **Edit ACL Rule**, as shown in following figure:

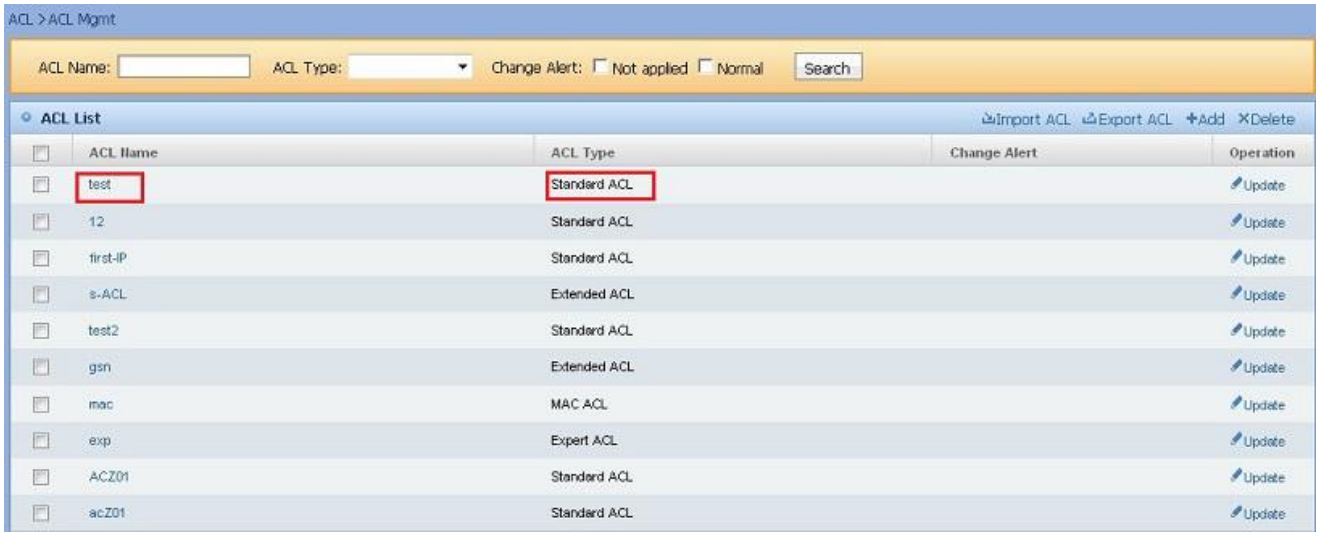


Figure 11.71. Go to page **Detail Information of Standard ACL**

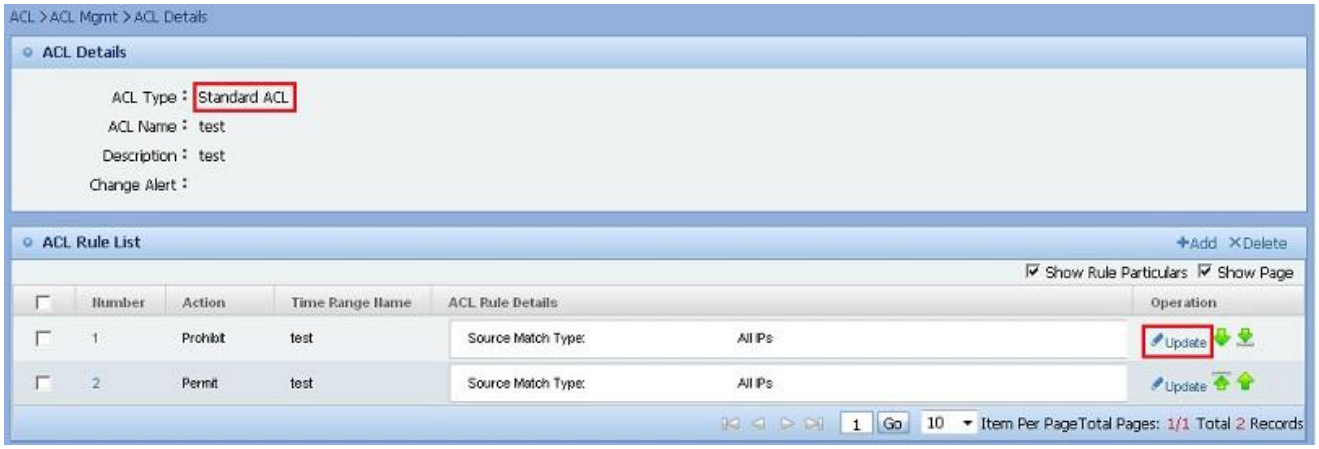


Figure 11.72. Go to page **Edit Standard ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in following figure:

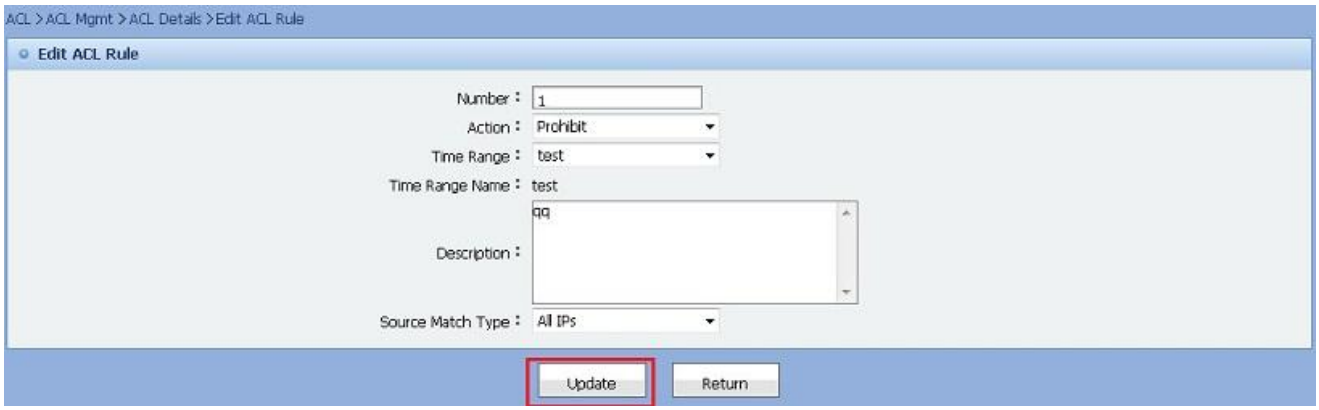


Figure 11.73. Edit Standard ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be modified automatically.

Source address: When the source match the type is **Host** or **Network segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

11.2.9.2.2. Modify Extended ACL Rule

Extended ACL Rule could be updated in ACL Management.

Operating Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL which **ACL Type** is **Extended ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Update** in the **ACL List** to enter page **Edit ACL Rule**, as shown in following figure:

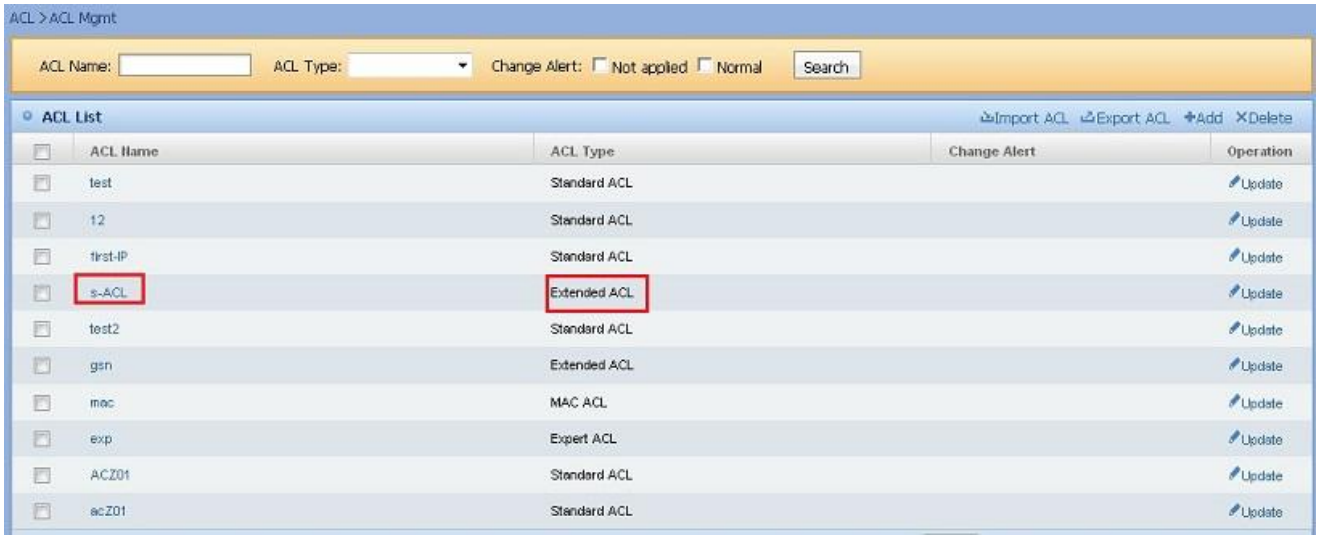


Figure 11.74. Go to page **Detail information of Extended ACL**

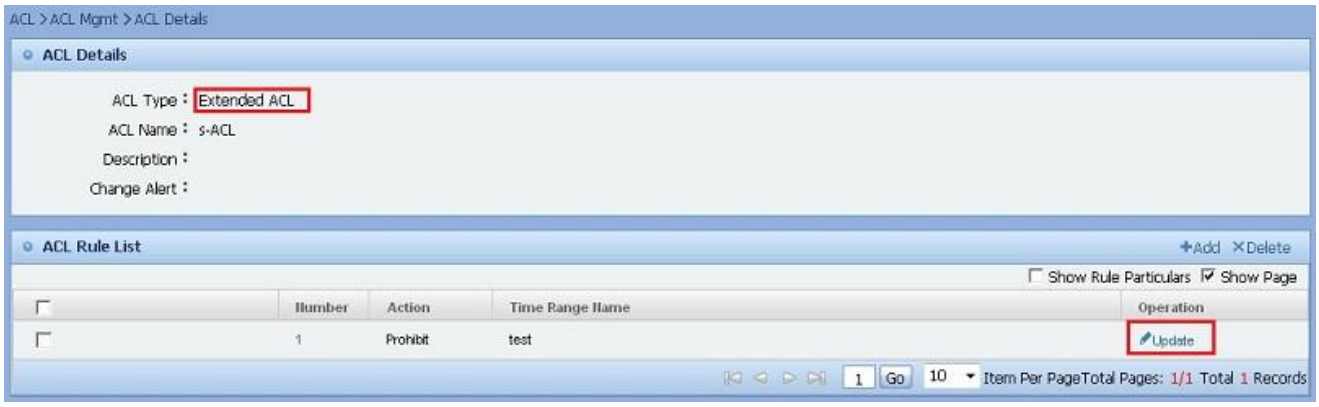


Figure 11.75. Go to page **Edit Extended ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in following figure:

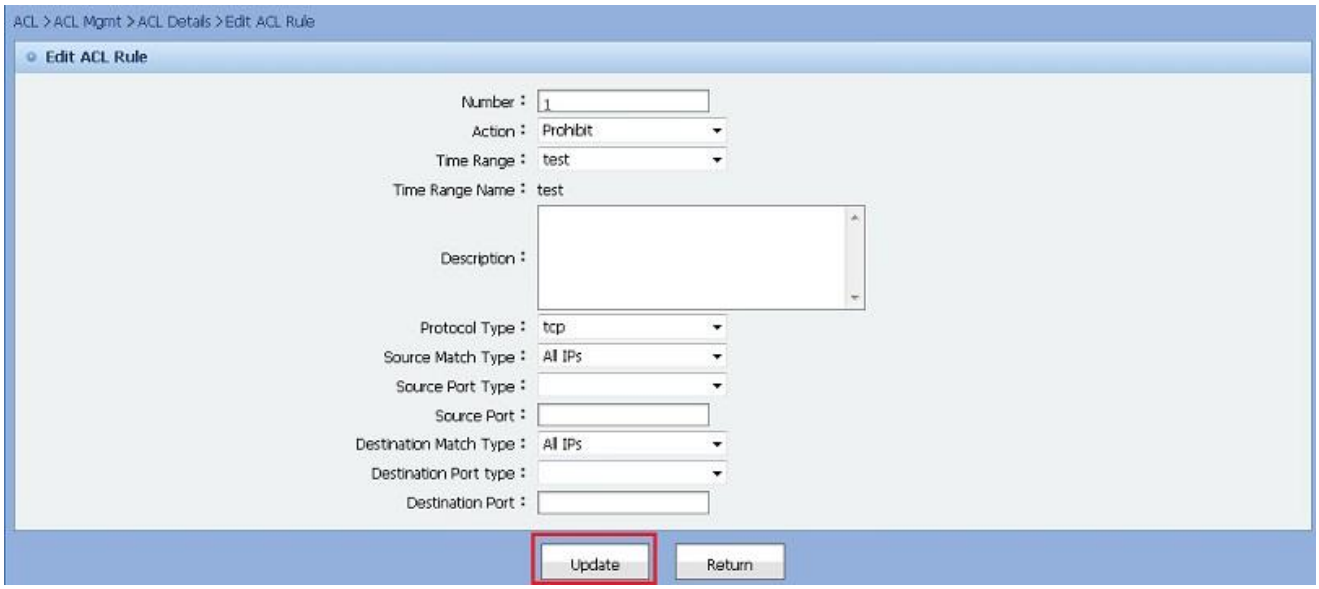


Figure 11.76. Edit Extended ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

Source address: When the source match the type is **Host** or **Network Segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

Source (Destination) port: Only when the protocol type is TCP or UDP, it can be displayed and input. Port operator in the current system supports only eq.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

11.2.9.2.3. Modify MAC ACL Rule

MAC ACL Rule can be modified in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **MAC ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Update** in the **ACL List** to enter page **Edit ACL Rule**, as shown in following figure:

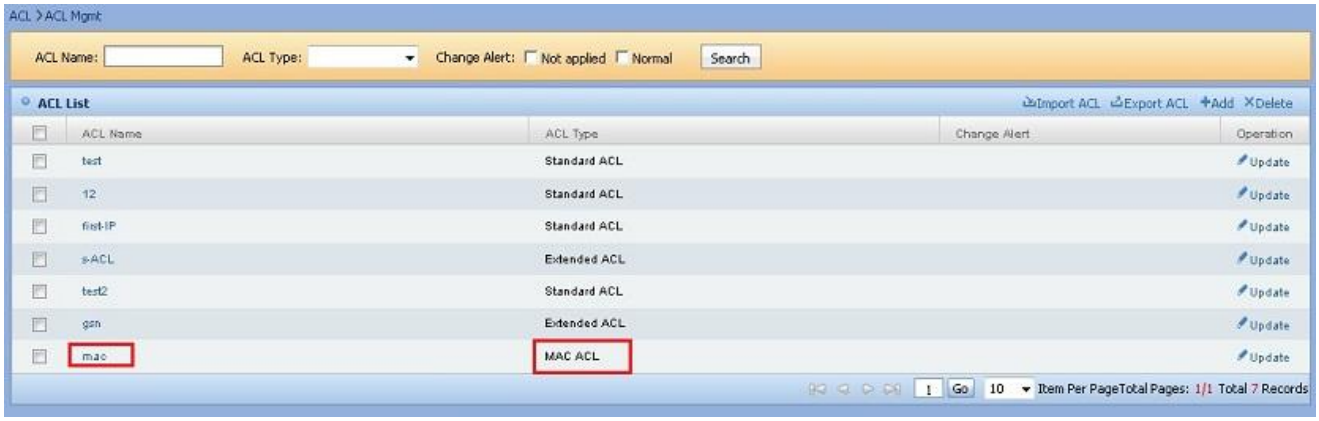


Figure 11.77. Go to page **Detail Information of MAC ACL**

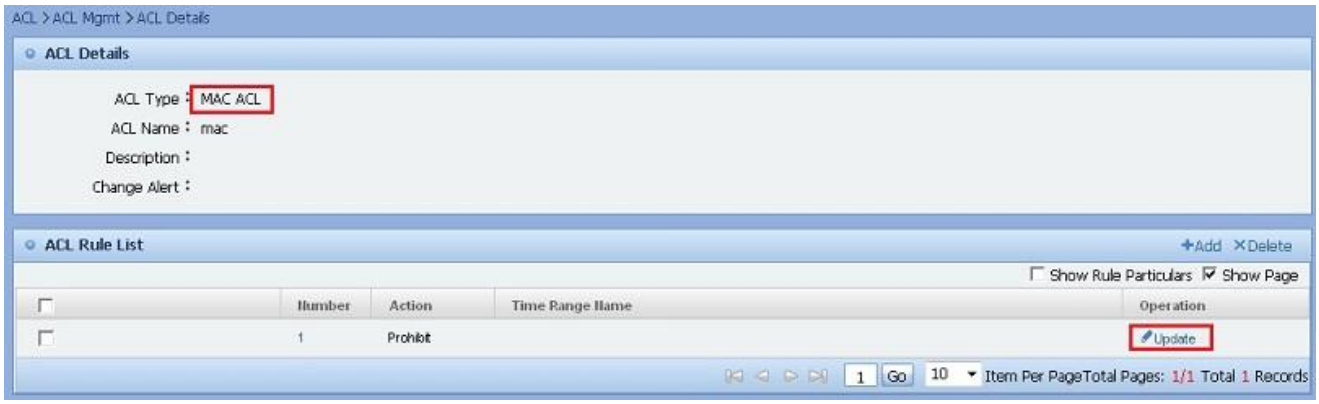


Figure 11.78. Go to page **Edit MAC ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in following figure:

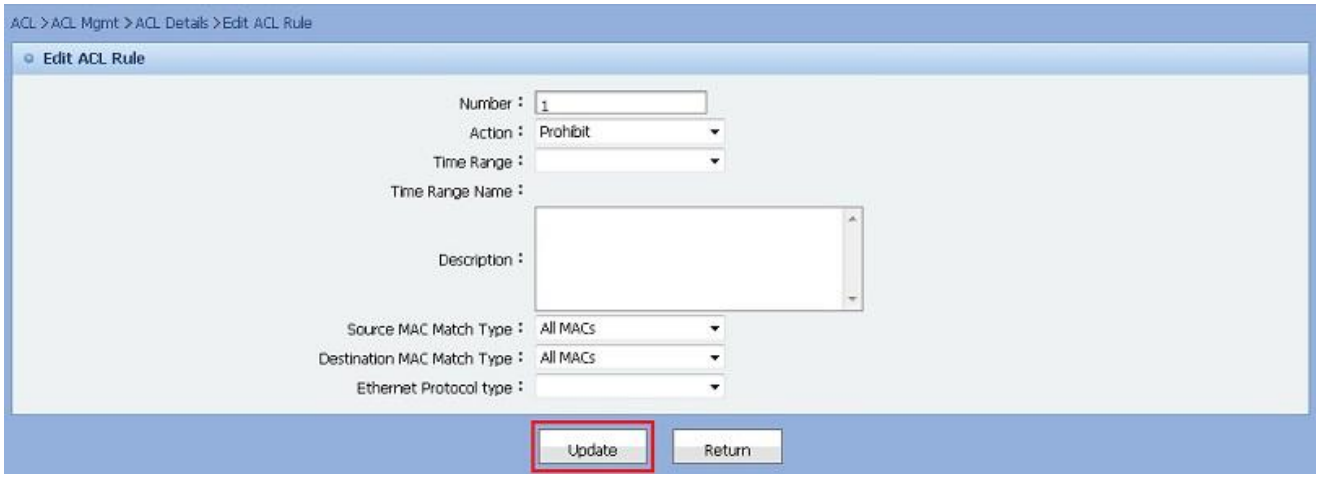


Figure 11.79. Modify MAC ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

If the ACL to which ACL rule belongs has been deployed to the device, then when adding ACL rules, the change alert of ACL will be updated automatically.

Ethernet protocol type can be empty.

Source (Destination) MAC address: When the source MAC match type is **Host**, it can be displayed and input.

11.2.9.2.4. Modify Expert ACL Rule

Expert ACL Rule can be modified in ACL Management.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** of the ACL whose **ACL Type** is **Expert ACL** in the ACL list to enter page **Detail Information of ACL** for ACL. Click button **Update** in the **ACL List** to enter page **Edit ACL Rule**, as shown in following figure:

Figure 11.80. Go to page **Detail information of Expert ACL**

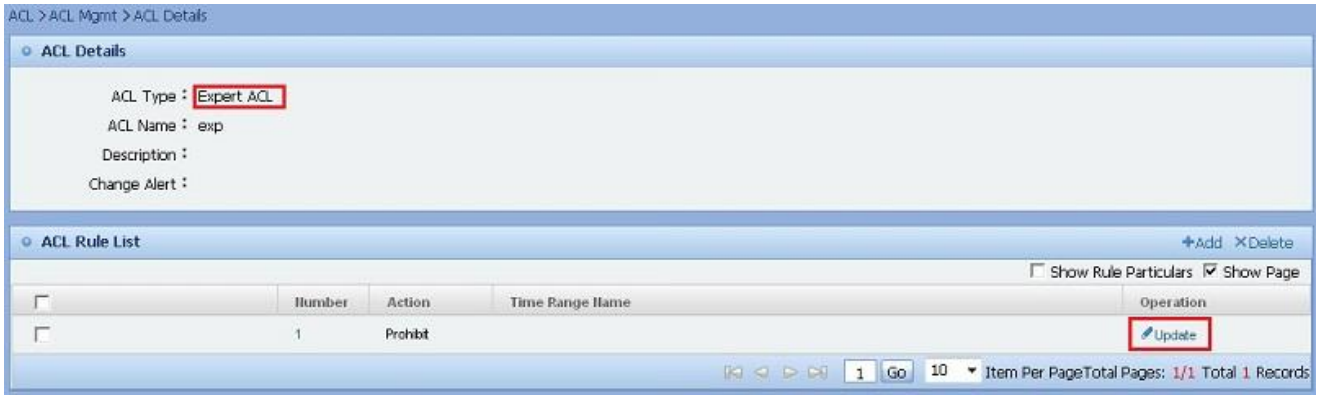


Figure 11.81. Go to page **Edit Expert ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in following figure:

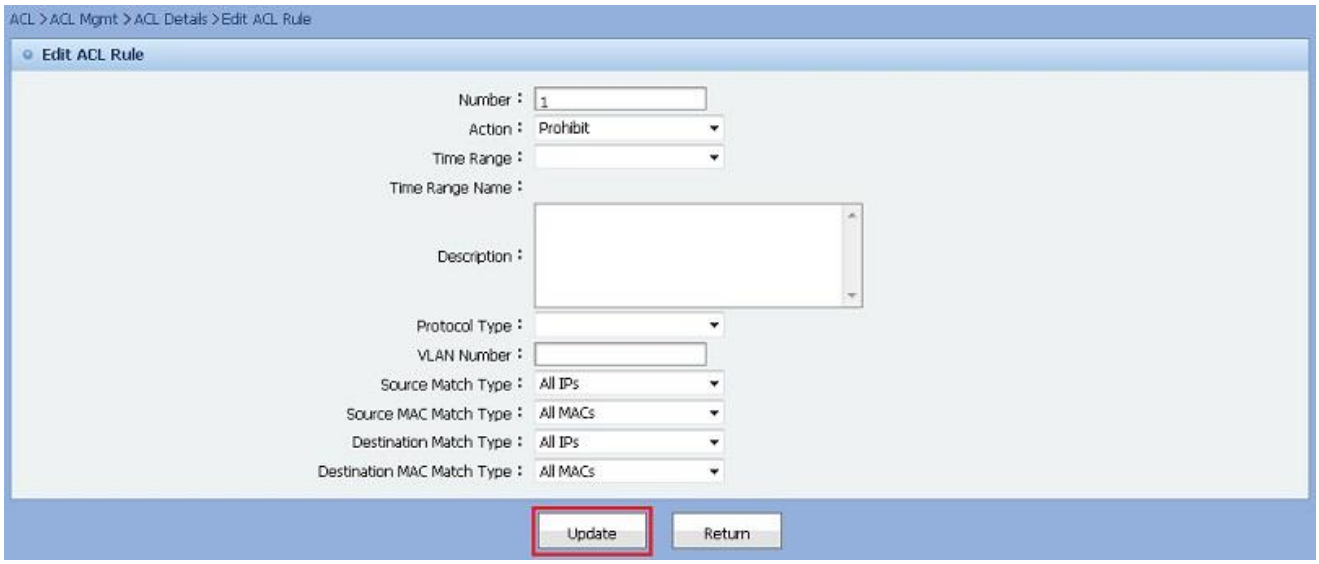


Figure 11.82. Edit Expert ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

When rules are issued to device, some devices will adjust the order of the rules automatically.

In cases of different protocol types, the system will display different input fields.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

11.2.9.3. Delete ACL Rule

The ACL Rule can be deleted on page Detail Information of ACL.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.83. Go to page **Detail information of ACL**

2) In **ACL Rule list**, click button **Delete**. The system will prompt you to confirm the deletion. Click **Confirm** to complete the deletion operation, as shown in following figure:

Figure 11.84. Delete ACL Rule

Note

If the ACL to which ACL rule belongs has been deployed to the device, then when deleting ACL rules, the change alert of ACL will be updated automatically.

11.2.9.4. View ACL Rule

The ACL Rule can be viewed on page Detail Information of ACL.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.85. Go to page **Detail information of ACL**

2) In **ACL Rule list**, click the link **Number** of ACL Rule to be viewed to enter page **Detail Information of ACL Rule**, as shown in following figure:

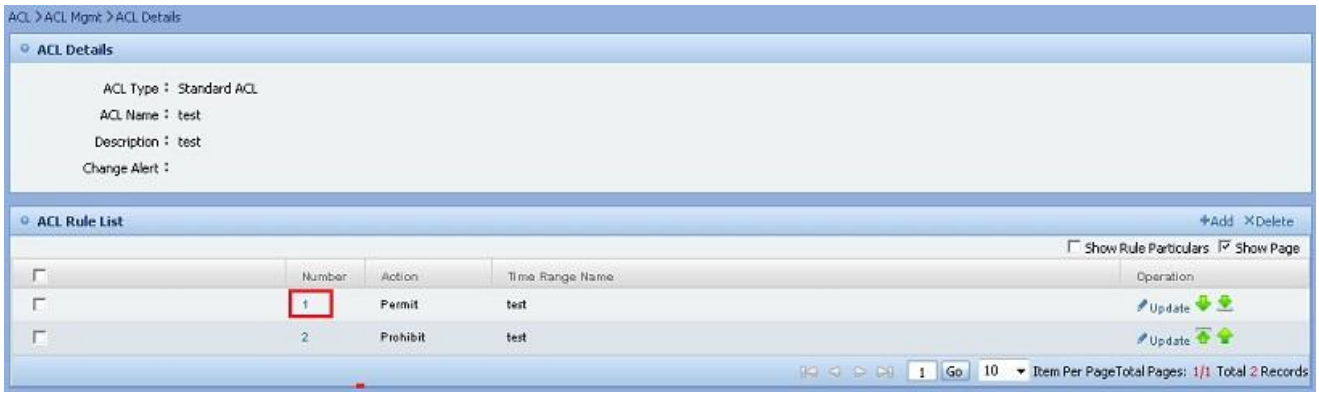


Figure 11.86. Go to page **Detail information of ACL Rule**

Figure 11.87. Detail information of ACL Rule

Note Position of extended field depends on the specific ACL rule.

11.2.9.5. Adjust Order of ACL Rule

The order of ACL rule can be adjusted on page Detail Information of ACL.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.88. Go to page **Detail information of ACL**

2) In **ACL Rule list**, according to the ACL rule to be adjusted, click moving button in **operation** bar to adjust the order of ACL rule, as shown in following figure:

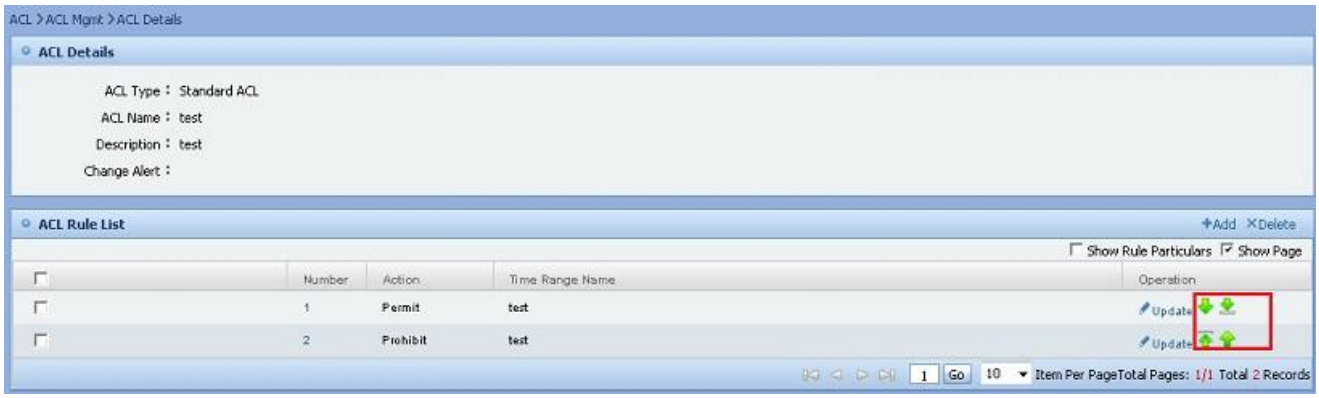


Figure 11.89. Adjust Order of ACL Rule

Note

If the ACL to which ACL rule belongs has been deployed to the device, then when adjusting the order of ACL rules, the change alert of ACL will be updated automatically.

Move to first (Move to last) is to move to the head (tail) of all rules, not the head (tail) of this page.

11.2.10. ACL Rule Management on Device

In this module, devices deployed with this ACL rule can be managed on page **Detail Information of ACL**.

- Delete ACL Rule from Device
- Deploy ACL on Device
- Redeploy ACL on Device
- Deploy ACL on Device Interface

11.2.10.1. Delete ACL Rule from Device

The ACL rule can be deleted from device on page Detail Information of ACL.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.90. Go to page **Detail Information of ACL**

2) In **Device list**, click the **Delete** button in **Operation** bar of corresponding device. The system will prompt you to confirm the deletion. Click button **Confirm** to delete the ACL rule from the device, as shown in following figure:

Figure 11.91. Delete ACL Rule from Device

Note

Since deleting ACL from device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.2.10.2. Deploy ACL on Device

The deployment plan for ACL can be added on page **Detail Information of ACL**.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.92. Go to page **Detail Information of ACL**

2) In **Device List**, click the button **Deploy ACL** to enter page **Add ACL**. For the other operations, please refer to **Add Deployment Plan**, as shown in following figure:

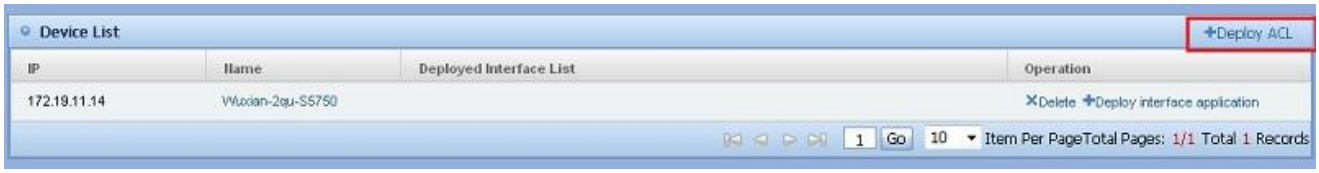


Figure 11.93. Deploy ACL

Figure 11.94. Go to page **Add ACL**

Note

When deploying ACL, it will go to page **Add ACL**.

In the process of **Add ACL**, ACL is set to this ACL already.

11.2.10.3. Redeploy ACL on Device

ACL can be redeployed on device on page **Detail Information of ACL**.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

Figure 11.95. Go to page **Detail Information of ACL**

2) In **Device List**, click the button **Redeploy** in **Operation** bar. The system will display confirmation dialog box. Click **Confirm** to redeploy ACL on the device, as shown in following figure:

Figure 11.96. Redeploy ACL on Device

Note

Since redeploying ACL on device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.2.10.4. Deploy ACL on Device Interface

Users can select interface and deploy ACL to the interface.

Operation Steps

1) On page **ACL Management**, click the link **ACL Name** in the ACL list to enter page **Detail Information of ACL** for ACL, as shown in following figure:

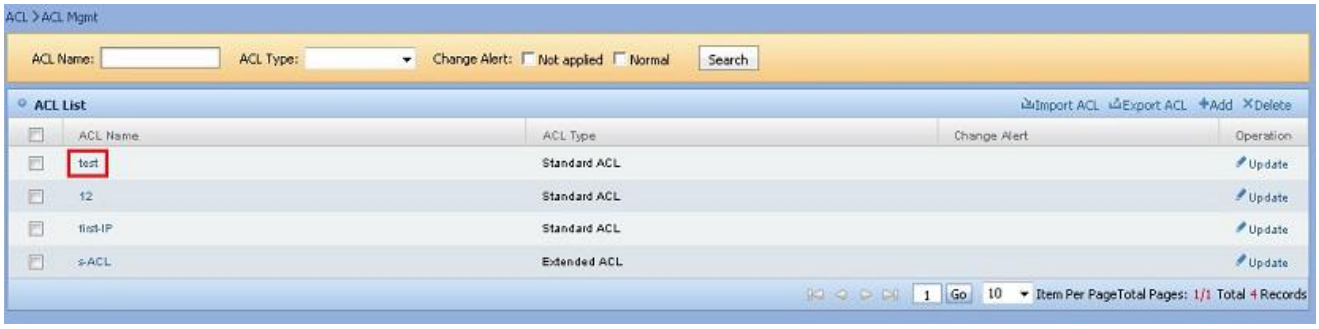


Figure 11.97. ACL List

2) On page **Detail Information of ACL**, click the button **Deploy Int App** in the device list to enter page **Add Interface Application ACL** and show the interface already deployed, as shown in following figure:

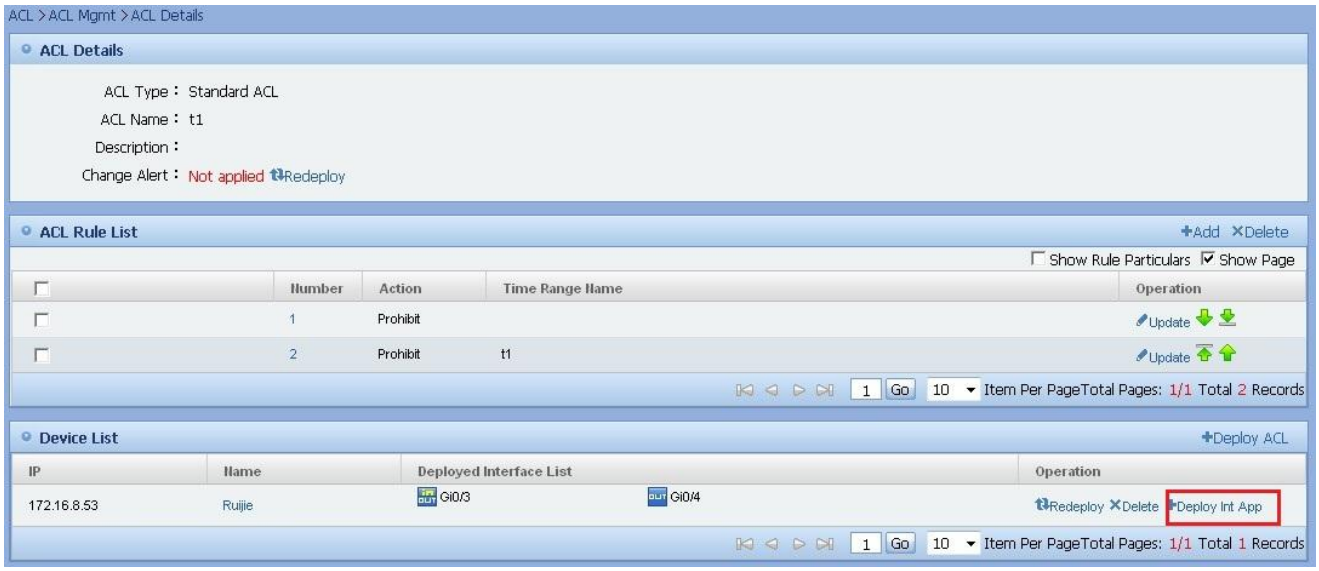


Figure 11.98. Go to Page **Add Interface Application ACL**

Figure 11.99. Add Interface Application ACL

3) Select **Filter direction** and **Unselected Interface** and double-click interface or click the **>** button. In **Selected Interface**, it will be shown with format **Interface Name [Filter Direction]ACL name**. Click **Deploy Interface**, and the system will deploy the ACL on the selected interface.

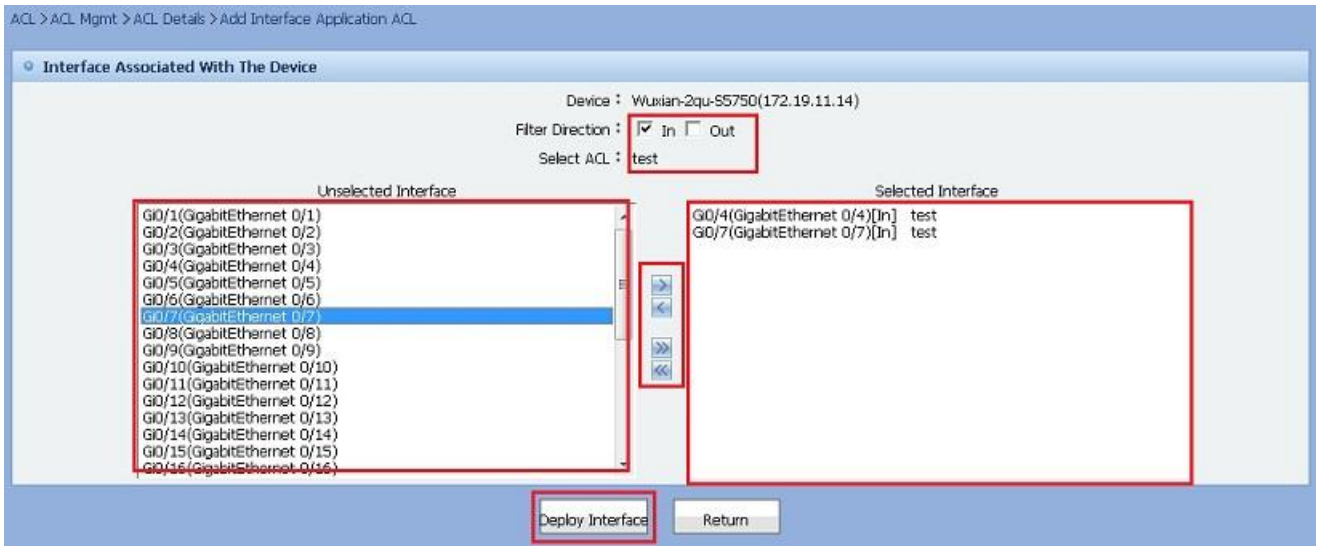


Figure 11.100. Add Interface Application ACL

In **Unselected Interface**, double-click interface or click the **>** button to configure interface one by one. Or click the **>>** button to batch configure interfaces

In **Selected Interface**, double-click interface or click the **<** button to remove interfaces one by one or click the **<<** button to remove interfaces in batch.

On page **Add Interface Application ACL**, click **Return** button, and the system saves no modification and returns to **Detail Information of ACL** page directly.

Note Filter direction and the interface must be selected to configure the ACL on interface.

11.3. ACL Device Management

ACL device management is to manage the device in the network. Time range, rule and interfaces list can be managed.

- Import ACL Device
- Delete ACL Device
- Modify ACL Device
- View ACL Device Information
- Search ACL Device
- Synchronization Plan for ACL Device
- Device Time Range Management
- ACL Management on Device
- ACL Management on Device Interface
- Synchronize ACL on Device

11.3.1. Import ACL Device

ACL device has to be added to the system before it can be managed by the system. The module describes importing of the ACL device.

Operation Steps

1) Go to page **ACL Device Management**, and click **Add Device**, as shown in the following figure:

Figure 11.101. Import Device

2) Click **Select Device**, as shown in the following figure:

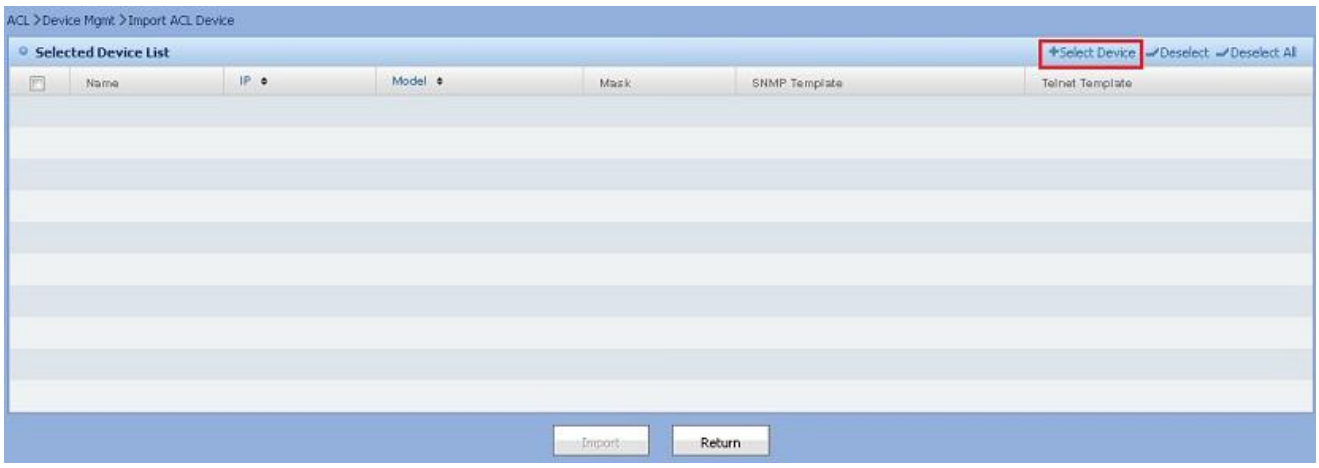


Figure 11.102. Select Device

3) Click **Add**, as shown in the following figure:

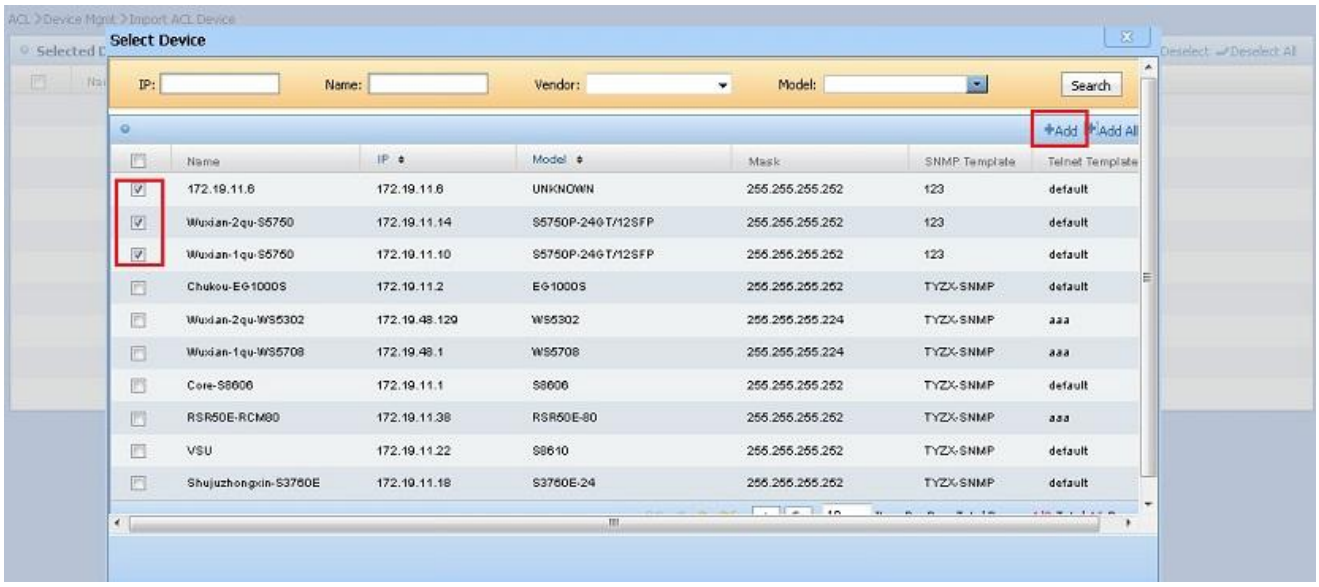


Figure 11.103. Add Device

4) Click **Import**, as shown in the following figure:

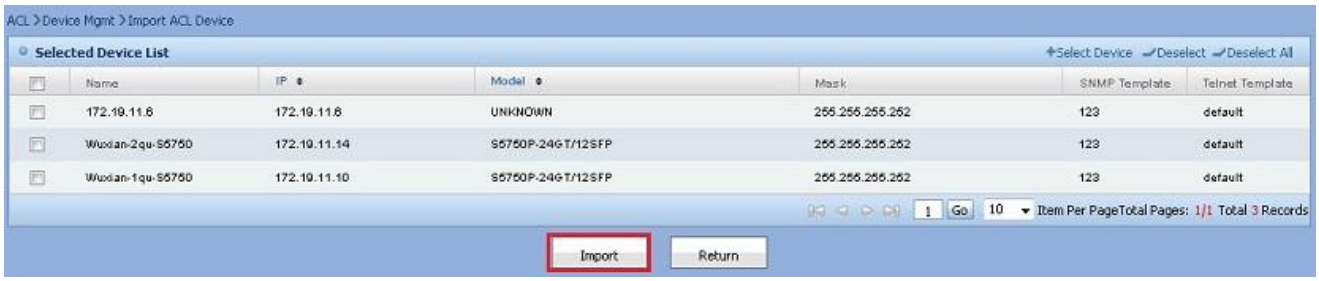


Figure 11.104. Import Device

5) When the importing of ACL device starts, the system will go to page **ACL Device Import Log** to show the importing progress of current ACL device, information of importing device and possible error information dynamically, as shown in the following figure:

Figure 11.105. ACL Device Import Log

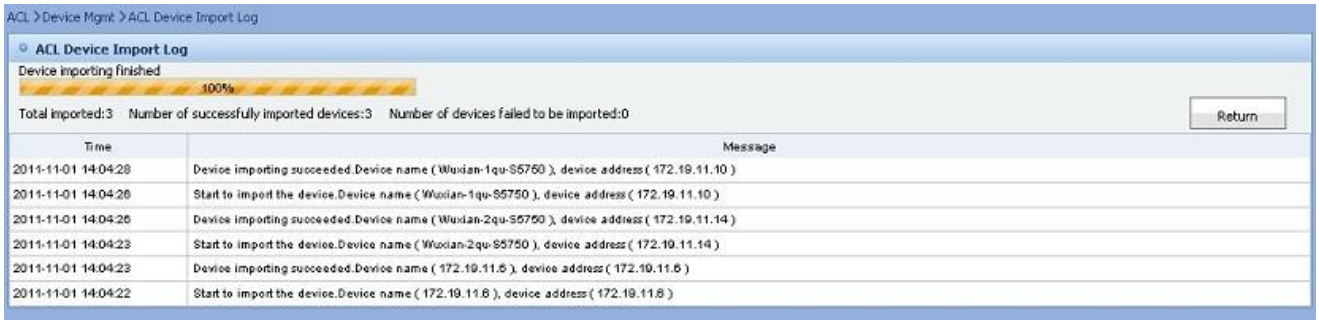


Figure 11.106. Import ACL Device Successfully

On page **Add ACL Device**, click **Deselect** or **Deselect All** button to remove all the devices in **Selected device list**. When clicking **Deselect All** button, you do not need to select devices.

On page **Available Device List** page, click **Add All** button to add all the devices to **Selected device list**. When clicking **Add All** button, you do not need to select devices.

On page **ACL Device Import Log**, click **Stop** or **Return** button to stop importing devices.

On page **Import ACL Device**, click **Return** button. The system will not import any ACL device and return to page **ACL Device Management** directly.

Note

If the device to be imported already exists in the device list of page **ACL Device Management**, it will be synchronized.

11.3.2. Delete ACL Device

ACL Device can be deleted in batch on page **ACL Device Management**.

Operation Steps

Go to page **ACL Device Management**, select some devices in device list, and click button **Delete**. The system will prompt you to confirm the deletion operation. Click button **Confirm** to delete the selected device, as shown in following figure:

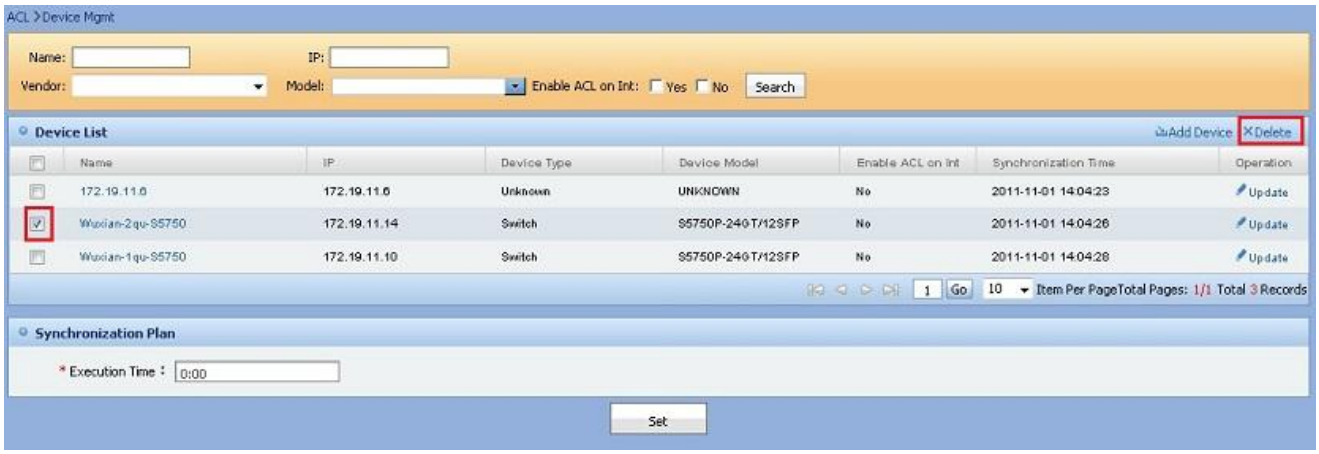


Figure 11.107. Delete ACL Device

11.3.3. Modify ACL Device

ACL Device can be selected and modified on page **ACL Device Management**.

Operation Steps

1) Go to page **ACL Device Management**, and click **Update** to enter page **Modify ACL Device**, as shown in following figure:

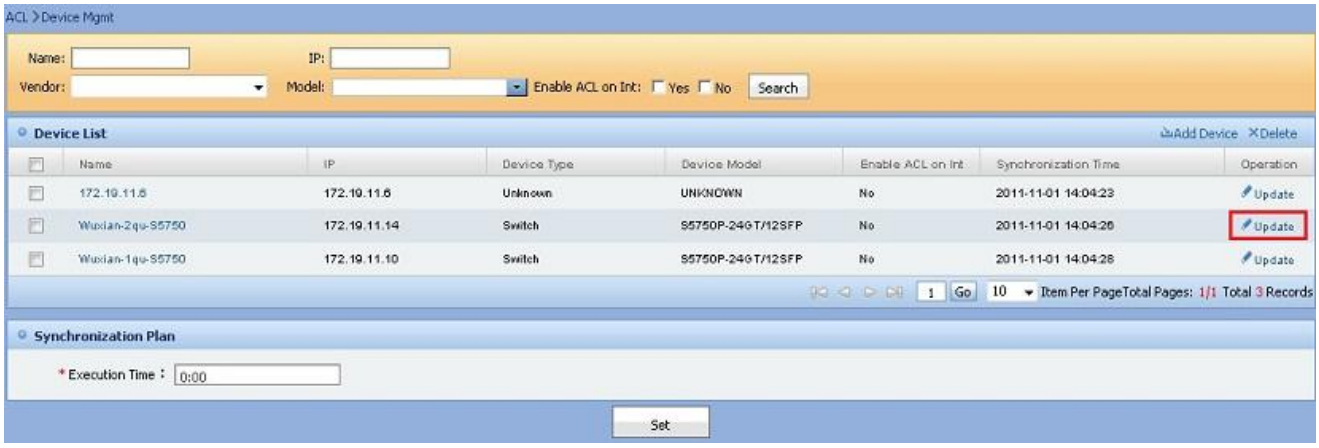


Figure 11.108. Go to page **Modify ACL Device**

2) Go to page **Modify ACL Device**, and modify related information of ACL device and click **Update**, as shown in following figure:

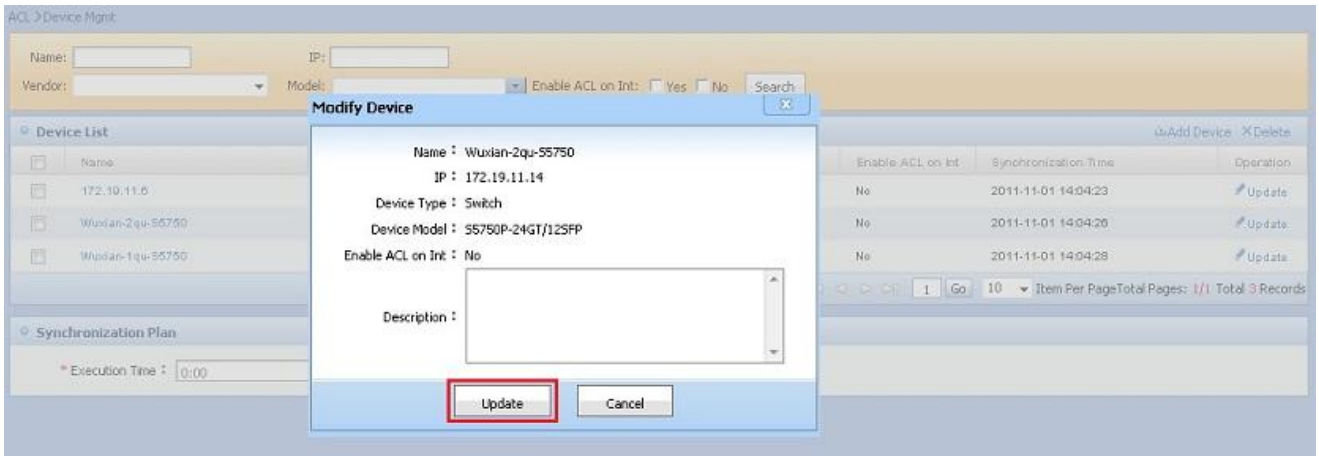


Figure 11.109. Modify ACL Device

Click **Cancel** on page **Modify ACL Device**. The system saves no modification and returns to **ACL Device Management** page directly.

Note Only description field could be modified in ACL device.

11.3.4. View ACL Device Information

From page **ACL Device Management**, users can enter page **Detail Information of ACL Device** to view Detail Information of ACL Device, Time Range Information, ACL Group Information and Interface Information.

Operation Steps

1) Go to page **ACL Device Management**, click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in the following figure:

Figure 11.110. Go to page **Detail Information of ACL Device**

2) Show Detail Information of ACL Device, Time Range Information, ACL Information and Interface Information, as shown in the following figure:

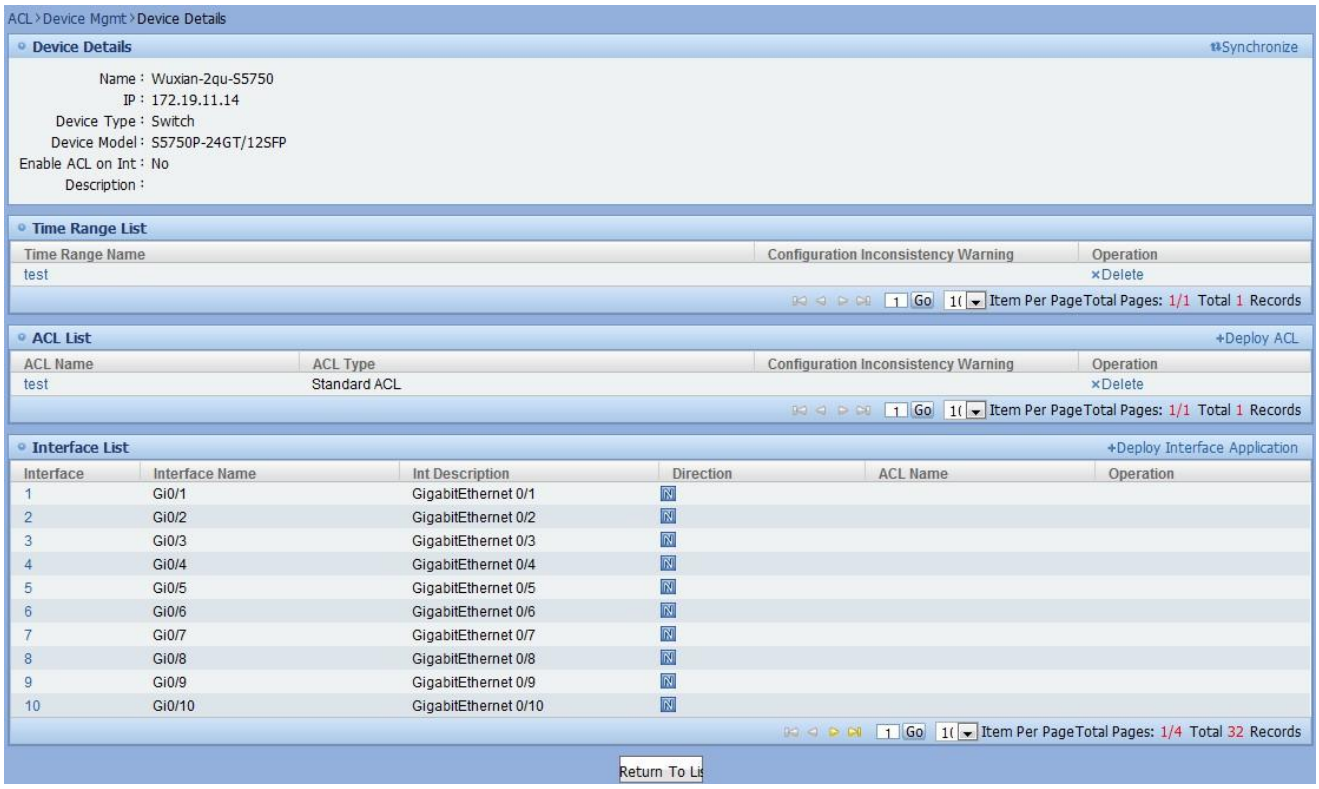


Figure 11.111. Page **Detail Information of ACL Device**

11.3.5. Search ACL Device

ACL device name, IP of ACL device, vendor, device model and interface deployed flag can be filled in or selected to search for ACL devices managed by system on page **ACL Device Management**.

Operation Steps

Go to page **ACL Device Management**, fill in ACL device name, IP of ACL device, vendor name, device model and interface deployed flag, and then click **Search** button. The system will return ACL Device list which satisfies search conditions, as shown in the following figure:

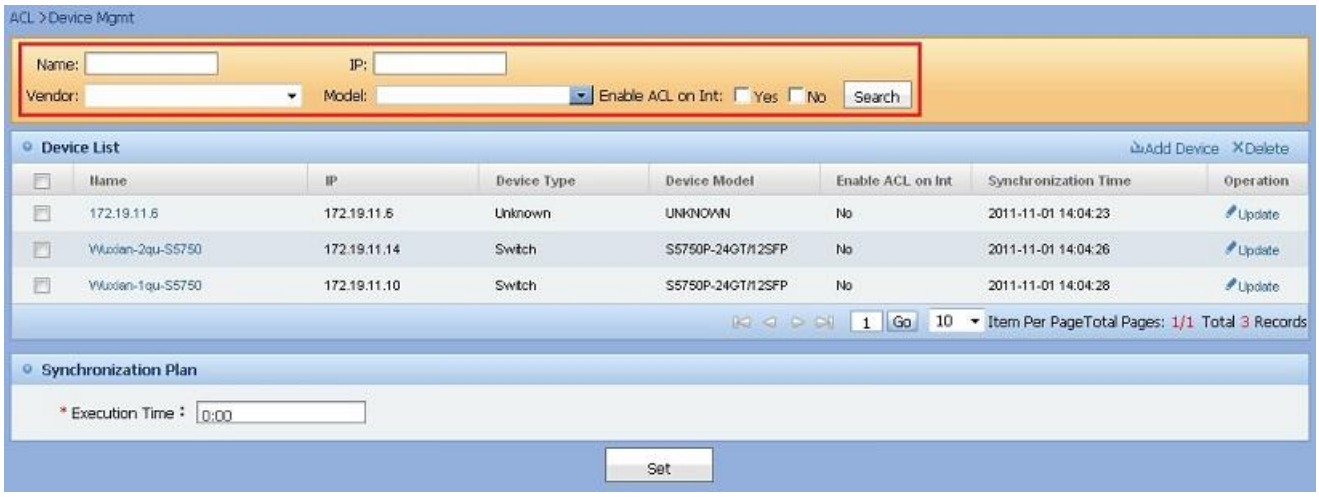


Figure 11.112. Search ACL Device

11.3.6. Synchronization Plan for ACL Device

Synchronization time for ACL device can be entered on page **ACL Device Management**, and ACL device can be synchronized at configured time point.

Operation Steps

Go to page **ACL Device Management**, fill in **Execution Time** for **Synchronization Plan** and click **Set**, as shown in the following figure:

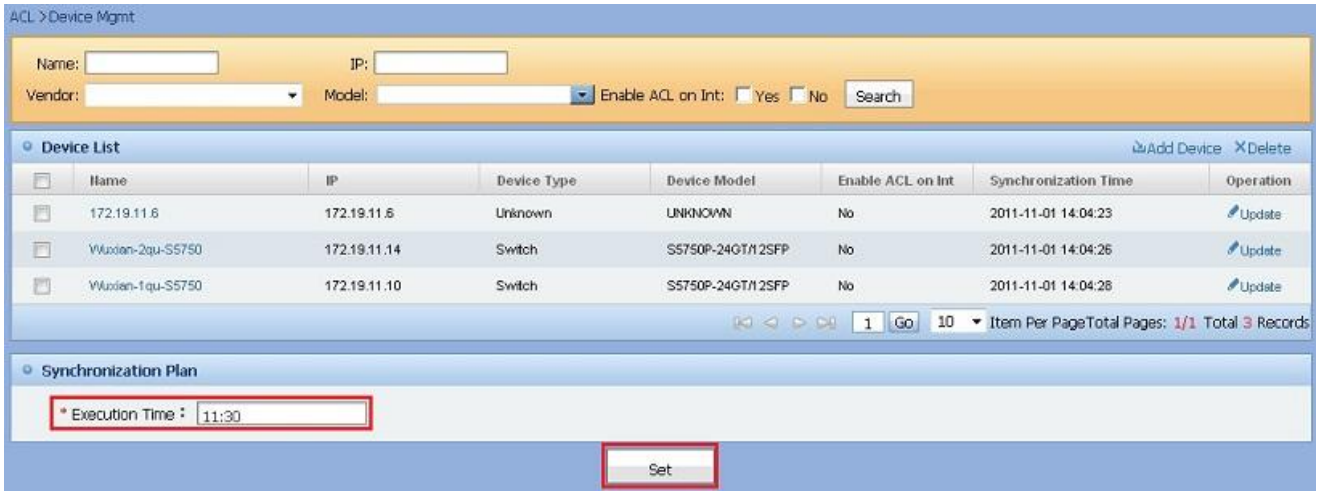


Figure 11.113. Set the **Execution Time of Synchronization Plan** for ACL Device

Note Configured time must meet the time format. Synchronizing ACL device will happen at configured time.

11.3.7. Device Time Range Management

Deployed Time Range can be redeployed, deleted and contrasted on this device.

Operation Steps

- Redeploy Time Range in Device
- Delete Time Range on Device
- Contrast Time Range on Device

11.3.7.1. Redeploy Time Range in Device

Time range deployed already can be redeployed in this device.

Operation Steps

1) On page **ACL Device Management**, click the link of **ACL Device Name** to enter page **Detail information of ACL Device**, as shown in following figure:

Figure 11.114. Go to page **Time Range List**

2) On page **Detail Information of ACL Device**, select corresponding Time Range in Time Range List, and click the button **Redeploy**. The system will prompt **Are you sure to overwrite the Time Range with the same name on the device?** Click **Confirm** to execute the redeployment operation, as shown in following figure:

Figure 11.115. Redeploy ACL Group in Device

Note

Since redeploying the time range in device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.7.2. Delete Time Range on Device

Time Range deployed on the device can be deleted.

Operation Steps

1) Go to page **ACL Device Management**, click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in following figure:

Figure 11.116. Go to page **Time Range List**

2) Go to page **Detail Information of ACL Device**, select corresponding Time Range and click button **Delete** in Time Range list. The system will prompt **Are you sure to delete this record?**, click button **Confirm** to complete the deletion operation, as shown in following figure:

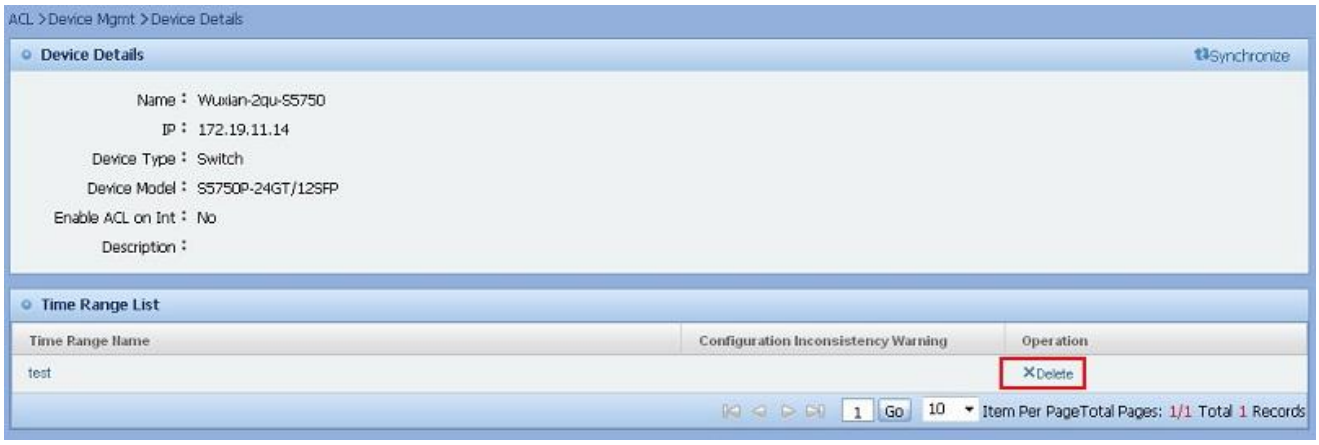


Figure 11.117. Delete Time Range on Device

Note

Since deleting time range from device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.7.3. Contrast Time Range on Device

Only when Time Range deployed on device and the Time Range in system are inconsistent, you can execute the contrast operation.

Operation Steps

1) Go to page **ACL Device Management**, and click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in following figure:

Figure 11.118. Go to page **Time Range List**

2) Go to page **Detail Information of ACL Device**, select corresponding Time Range and click button **Time Comparison**. The system will display a new page and show the contrast result, as shown in following figure:

Figure 11.119. Contrast Time Range

Note

Only when Time Range information on the device and that on the system are inconsistent, this button will be shown.

11.3.8. ACL Management on Device

The ACL rule deployed on device can be redeployed, deleted and compared in this module.

Operating Steps

- Redeploy ACL on Device
- Delete ACL on Device
- Contrast ACL on Device

11.3.8.1. Redeploy ACL on Device

ACL deployed already can be redeployed on this device.

Operation Steps

1) On page **ACL Device Management**, and click the link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in following figure:

Figure 11.120. Go to page **ACL List**

2) On page **Detail Information of ACL Device**, select corresponding ACL in ACL List, and click the button **Redeploy**. The system will prompt **Are you sure to overwrite the ACL with the same name on the device?** Click **Confirm** to execute the redeployment operation, as shown in following figure:

Figure 11.121. Redeploy ACL on Device

Note

Since redeploying the ACL on device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.8.2. Delete ACL on Device

ACL deployed on the device can be deleted.

Operation Steps

1) Go to page **ACL Device Management**, click link of **ACL Device Name** to enter page **Detail information of ACL Device**, as shown in following figure:

Figure 11.122. Go to page **ACL List**

2) Go to page **Detail information of ACL Device**, select corresponding ACL and click button **Delete** in ACL list. The system will prompt **Are you sure to delete this record?** Click button **Confirm** to complete the deletion operation, as shown in following figure:

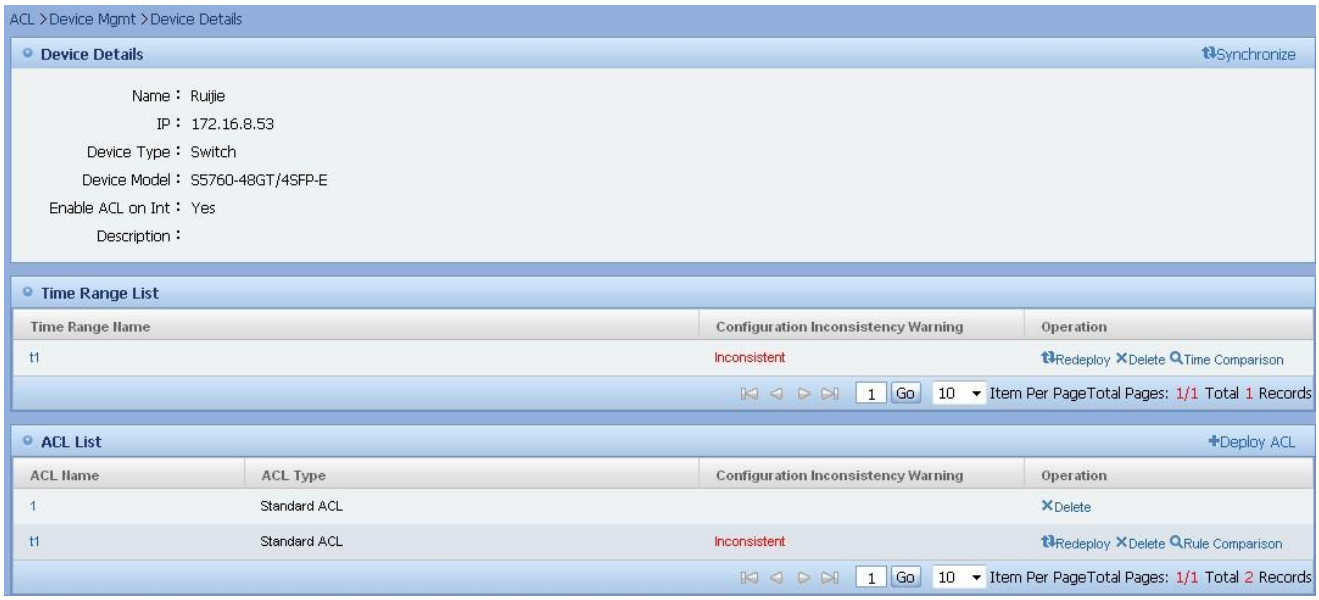


Figure 11.123. Delete ACL on Device

Note

Since deleting ACL from device operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.8.3. Contrast ACL on Device

Only when ACL deployed on device and the ACL in system are inconsistent, you can execute the contrast operation.

Operation Steps

1) Go to page **ACL Device Management**, and click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in following figure:

Figure 11.124. Go to page **ACL List**

2) Go to page **Detail Information of ACL Device**, and select corresponding ACL and click button **Rule Comparison**. The system will display a new page and show the contrast result, as shown in following figure:

Figure 11.125. Contrast ACL on Device

Note Only when ACL information on the device and that on the system are inconsistent, this button will be shown.

11.3.9. ACL Management on Device Interface

The ACL deployed on device interface can be redeployed, deleted and applied in this module.

Operating Steps

- Redeploy ACL on Device Interface
- Delete ACL from Device Interface
- Select Interface to Deploy ACL

11.3.9.1. Redeploy ACL on Device Interface

ACL can be redeployed on device interface.

Operation Steps

1) On page **ACL Device Management**, click the link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in the following figure:

Figure 11.126. Go to page **ACL List**

2) On page **Detail Information of ACL Device**, select corresponding interface in Interface List, and click the button **Redeploy**. The system will execute the redeployment operation, as shown in the following figure:

Figure 11.127. Redeploy ACL on Device Interface

Note Since redeploying ACL on device interface operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.9.2. Delete ACL from Device Interface

The ACL deployment can be deleted from device interface.

Operation Steps

1) Go to page **ACL Device Management**, click link of **ACL Device Name** to enter page **Detail information of ACL Device**, as shown in following figure:

Figure 11.128. Go to page **Interface List**

2) Go to page **Detail Information of ACL Device**, select corresponding interface and click button **Delete** in the Interface list. The system will prompt **Are you sure to delete this record?**. Click button **Confirm** to complete the deletion operation, as shown in following figure:

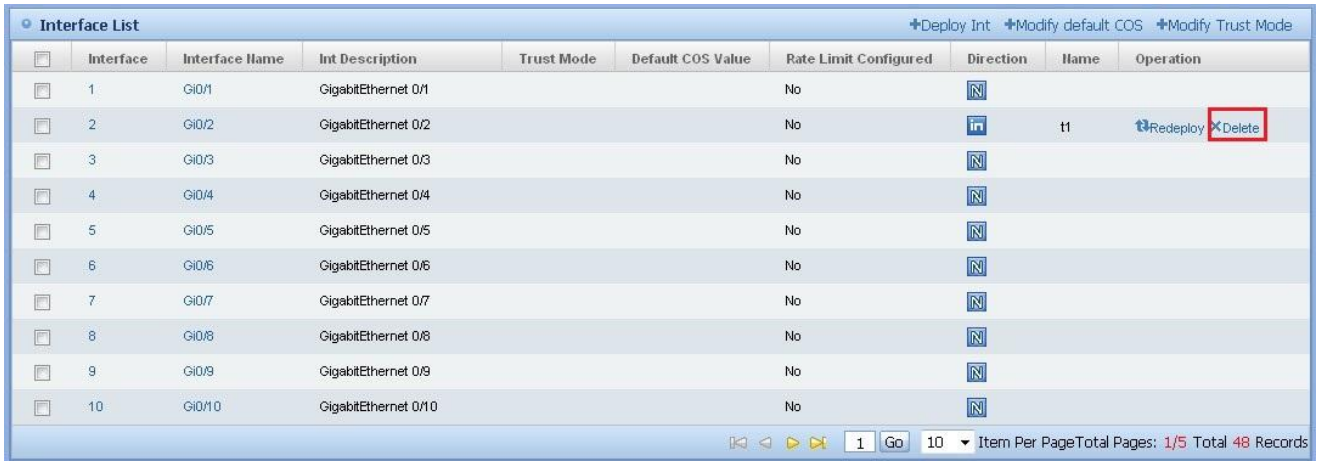


Figure 11.129. Delete Device Interface

Note Since deleting device interface operates a single device, no deployment plan is generated, and issuing is performed directly.

11.3.9.3. Select Interface to Deploy ACL

User can select the ACL which deployed on this device already and deploy it to device interface.

Operation Steps

1) Go to page **ACL Device Management**, click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in the following figure:

Figure 11.130. Go to page **Interface List**

2) Go to page **Detail Information of ACL Device**, click button **Deploy Int App** in the Interface list. The system will go to page **Add Interface Application ACL** and show interface deployed already, as shown in the following figure:

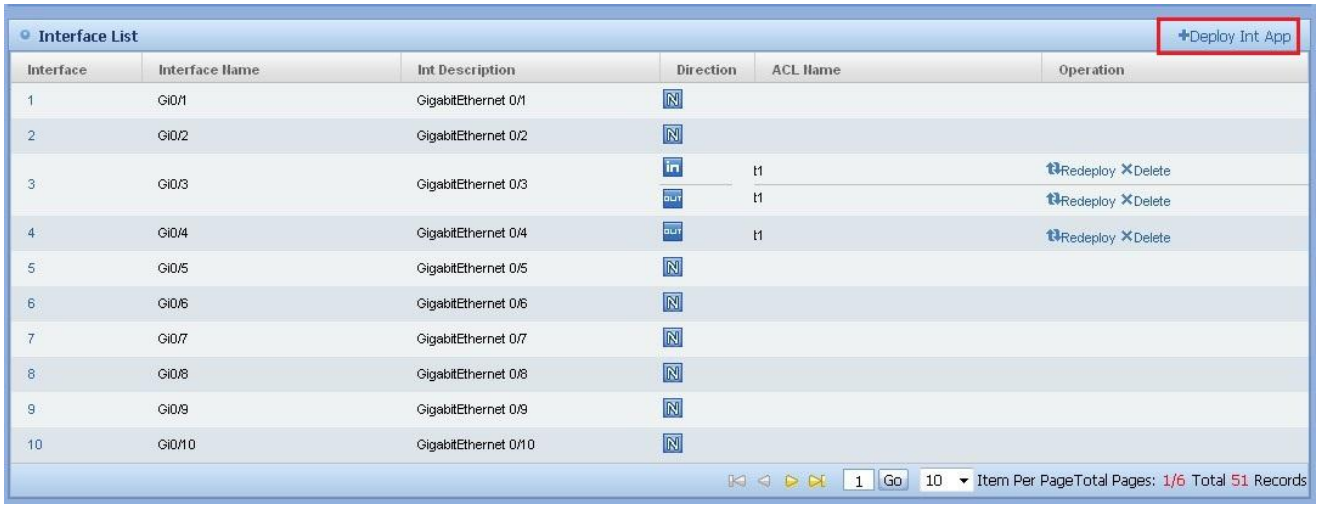


Figure 11.131. Go to page **Add Interface Application ACL**

3) Select **Filter Direction**, **ACL** and **Unselected Interface**, and double-click interface or click button **>**. The interface will be shown in format **Interface Name[Filter Direction]ACL Name** in **Selected Interface**. Then click **Deploy Interface**

Figure 11.132. Add Interface Application ACL

In box **Unselected Interface**, double-click interface or click the **>** button to configure interface one by one or click the **>>** button to select interfaces in batch.

In box **Selected Interface**, double-click interface or click the **<** button to remove interface from the box or click the **<<** button to remove interfaces in batch.

In page **Add Interface Application ACL**, click button **Return**. The system saves no information and returns to **Detail Information of ACL** page directly.

Note

Filter Direction, **ACL** and **Unselected Interface** have to be selected to configure ACL interface.

11.3.10. Synchronize ACL on Device

Selected ACL Device can be synchronized on page **Detail Information of ACL Device**.

Operation Steps

1) Go to page **ACL Device Management**, and click link of **ACL Device Name** to enter page **Detail Information of ACL Device**, as shown in the following figure:

Figure 11.133. Go to page **Detail Information of ACL Device**

2) Click button **Synchronize** on page **Detail Information of ACL Device**, as shown in the following figure:

Figure 11.134. Execute operation **Synchronize ACL Device Information**

Note

Detail Information of ACL Device, Time Range Information, ACL Information and Interface Information should be re-obtained during synchronization.

11.4. ACL Template Management

ACL Template Management is primarily used to generate ACLs. The system can import from text information or group information in device and generate the corresponding templates. ACL template management includes management of ACL variables. Users can add a variable in the generated template which will be used for replacing corresponding field of ACL rule during creating ACL.

- Add ACL Template

- Delete ACL Template
- Modify ACL Template
- Search ACL Template
- View ACL Template
- Import Template from Device
- Import Template from Text File
- Export ACL Template
- Variable Management
- ACL Rule Management in ACL Template

11.4.1. Add ACL Template

ACL Template has to be added to the system to be managed by the system.

Operation Steps

1) On page **ACL Template Management**, click button **Add** to enter page **Add ACL Template**, as shown in the following figure:

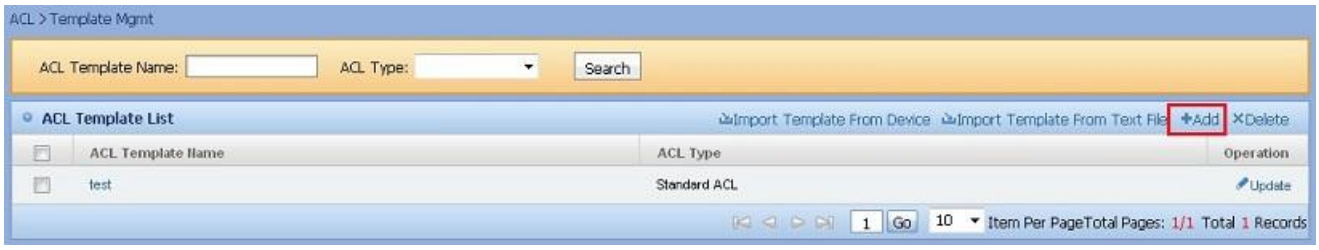


Figure 11.135. Go to page **Add ACL Template**

2) Go to page **Add ACL Template**, fill in the information related to ACL Template, and click **Add** button, as shown in the following figure:

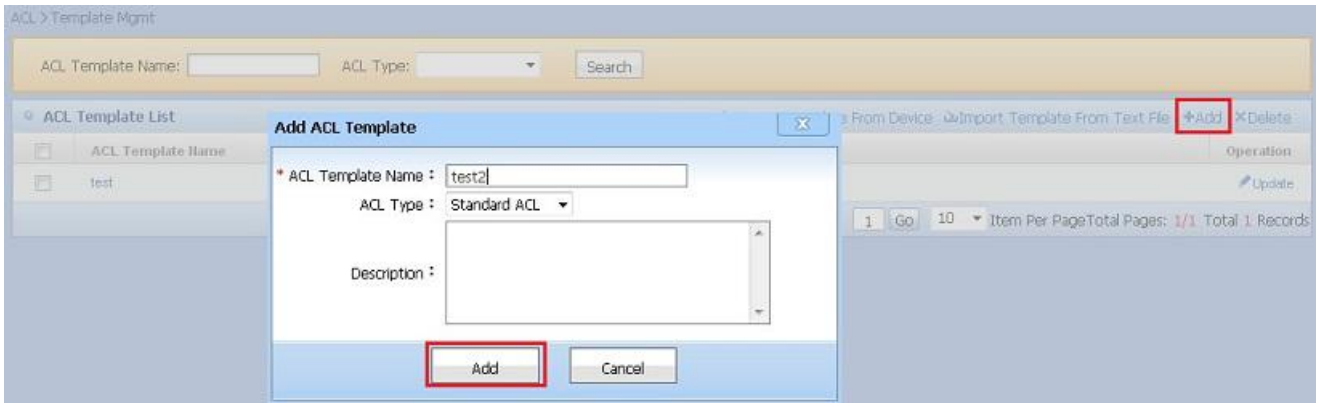


Figure 11.136. Add ACL Template

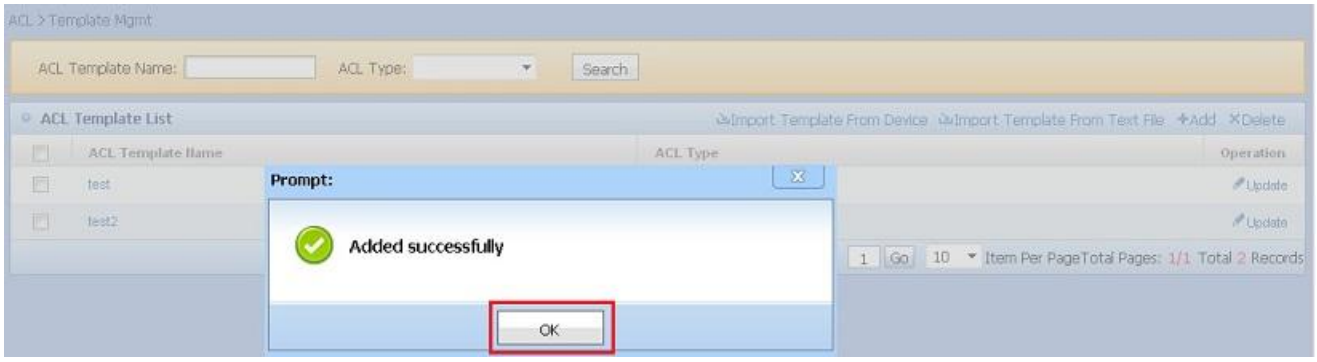


Figure 11.137. Add ACL Template Successfully

On page **Add ACL Template**, if **Cancel** is clicked, the system saves no modification and returns to **ACL Template Management** page directly.

Note ACL template name cannot be repeated.

11.4.2. Delete ACL Template

ACL templates can be deleted in batch on page **ACL Template Management**.

Operation Steps

On page **ACL Template Management**, select some ACL templates in the ACL Template list, and click button **Delete**. The system will prompt to confirm the deletion operation. Click button **Confirm** to delete selected ACL templates, as shown in the following figure:

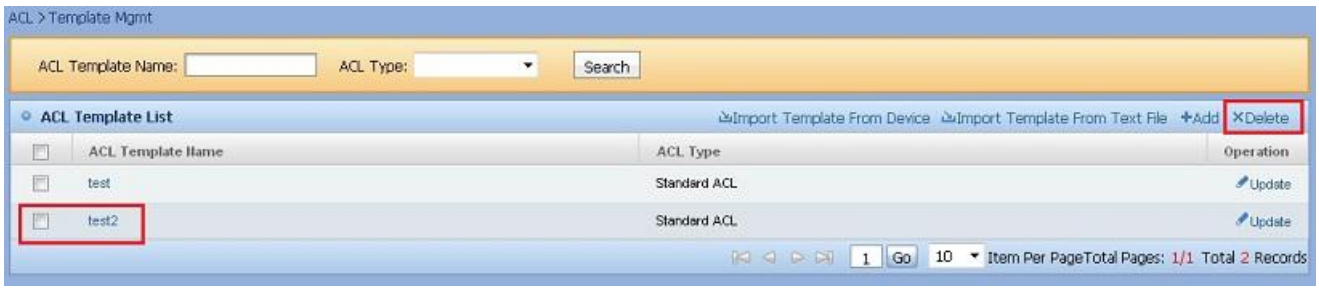


Figure 11.138. Delete ACL Template

11.4.3. Modify ACL Template

Name and description of ACL template can be modified in the system.

Operation Steps

1) On page **ACL Template Management**, click icon **Update** to enter page **Edit ACL Template**, as shown in the following figure:

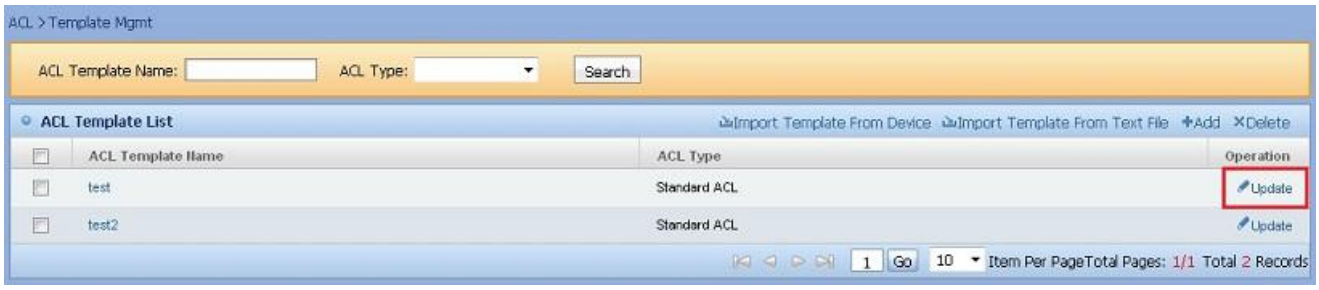


Figure 11.139. Go to page **Edit ACL Template**

2) Go to page **Edit ACL Template**, fill in the description information of ACL Template, and click on **Update** button, as shown in the following figure:

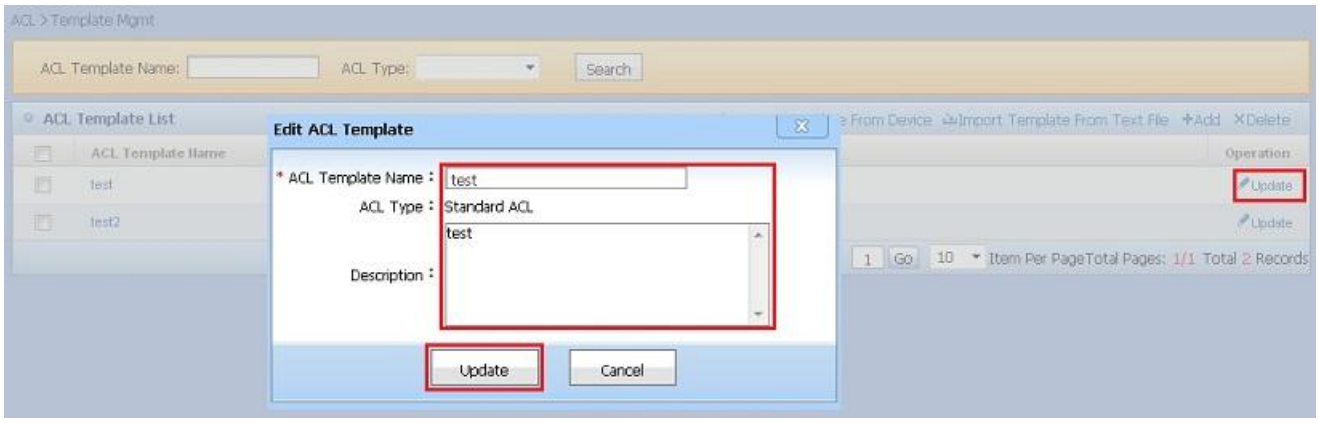


Figure 11.140. Edit ACL Template

On page **Edit ACL Template**, if **Cancel** is clicked, the system saves no modification and returns to **ACL Template Management** page directly.

Note ACL template name cannot be repeated.

11.4.4. Search ACL Template

ACL template name and ACL type can be filled in to searched for system-managed ACL templates on page **ACL Template Management**.

Operation Steps

Go to page **ACL Template Management**, fill in ACL template name and ACL type, and then click **Search** button. The system will return ACL template list which satisfies search conditions, as shown in the following figure:

Figure 11.141. Search ACL Template

11.4.5. View ACL Template

Detail information of ACL template, variable list associated with the ACL template, ACL rules list and device list can be viewed on page Detail Information of ACL Template.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

Figure 11.142. Show ACL Template

2) On page **Detail Information of ACL Template**, detail information of ACL template, variable list and ACL rules list can be viewed, as shown in the following figure:

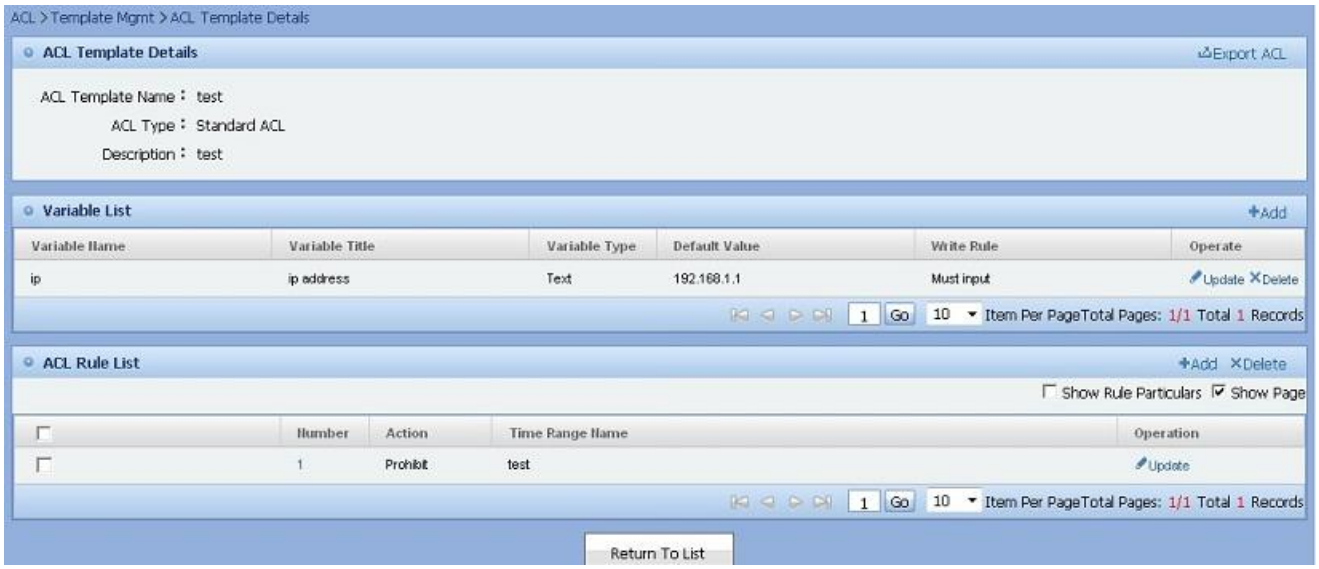


Figure 11.143. Page **Detail Information of ACL Template**

11.4.6. Import Template from Device

ACL template can be imported from device to create corresponding template according to the ACL in device.

Operation Steps

1) On page **ACL Template Management**, click button **Import Template from Device** to enter page **Import Template from Device**, as shown in the following figure:

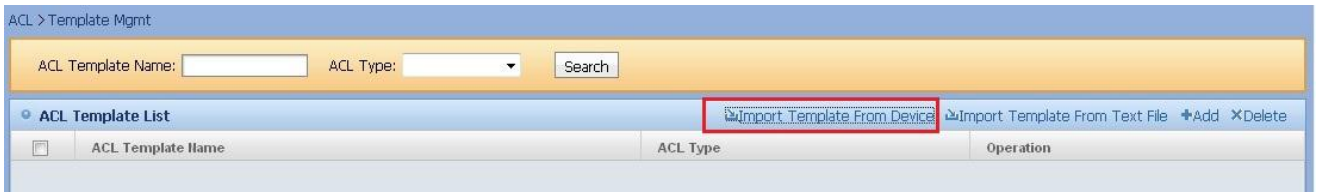


Figure 11.144. Go to page **Import Template from Device**

2) Go to page **Import Template from Device**, select corresponding ACL, and click **Import** button. Corresponding ACL template will be created according to the selected ACL, as shown in the following figure:

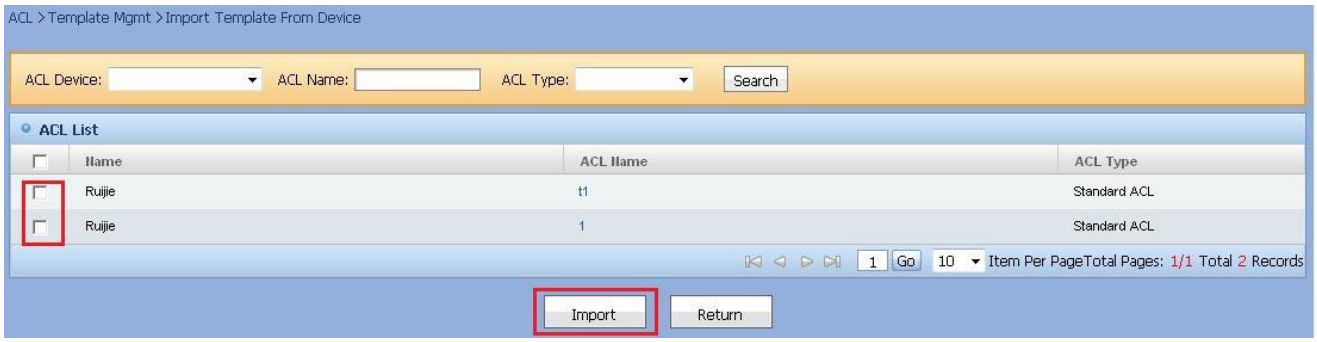


Figure 11.145. Page **Import Template from Device**

Note

If the same name already exists, the system will prompt repeated template name and importing failure.

Generated template name should be the same as imported ACL name.

Multiple templates can be imported at the same time.

During importing, if time range in the text does not exist, create and save the time range; if the same name of

time range already exists, new time range will not be created, and the time range in the system is referenced directly.

11.4.7. Import Template from Text File

ACL template, the rules in the template, and time range related to the rule can be imported from text file.

Operation Steps

1) On page **ACL Template Management**, and click button **Import Template From Text File** to enter page **Import Template From Text File**, as shown in the following figure:

Figure 11.146. Import Template From Text File

2) On page Import Template From Text File, click button **Select Imported File** to select the text file to be imported in the pop-up file selection dialog box, and click **Open**. The system successfully selects the file to be imported, as shown in the following figure:

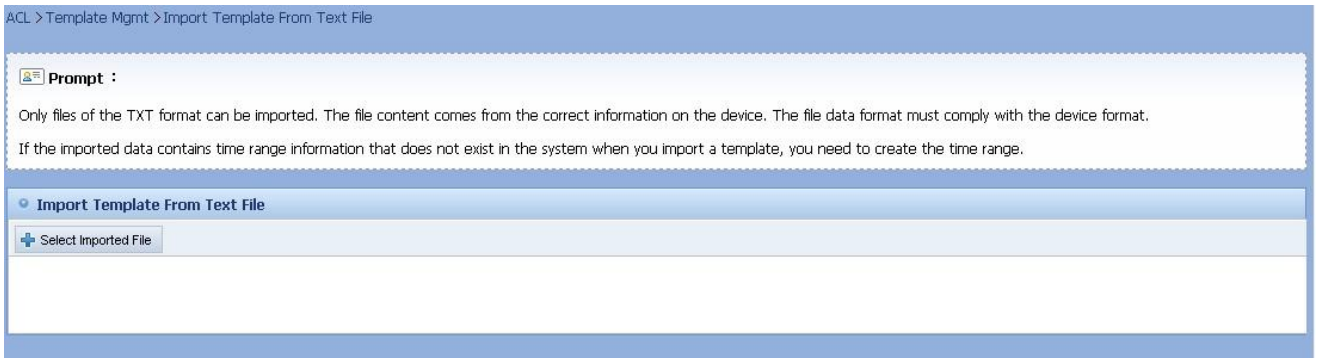


Figure 11.147. Select and Import File

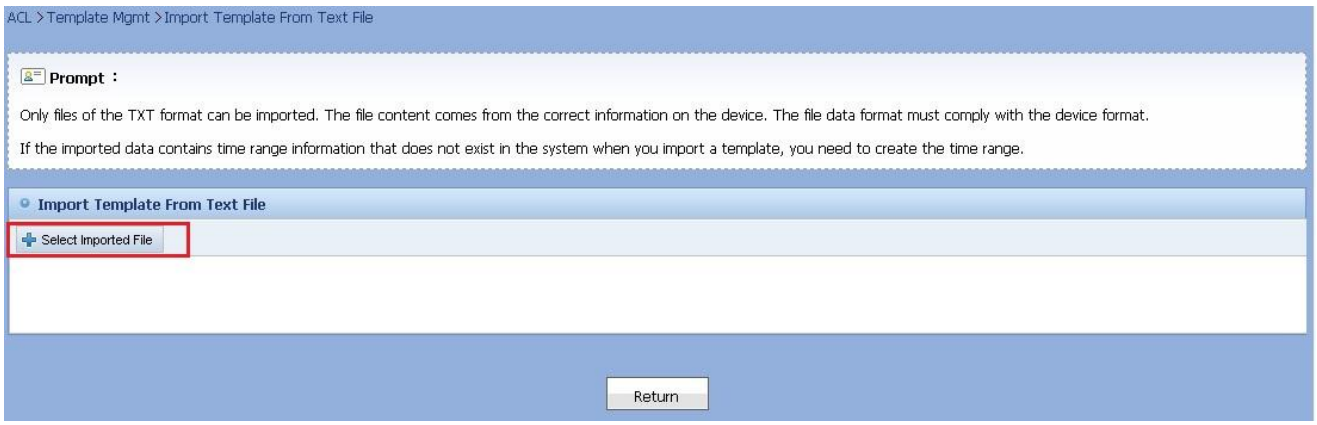


Figure 11.148. Confirm Selected File

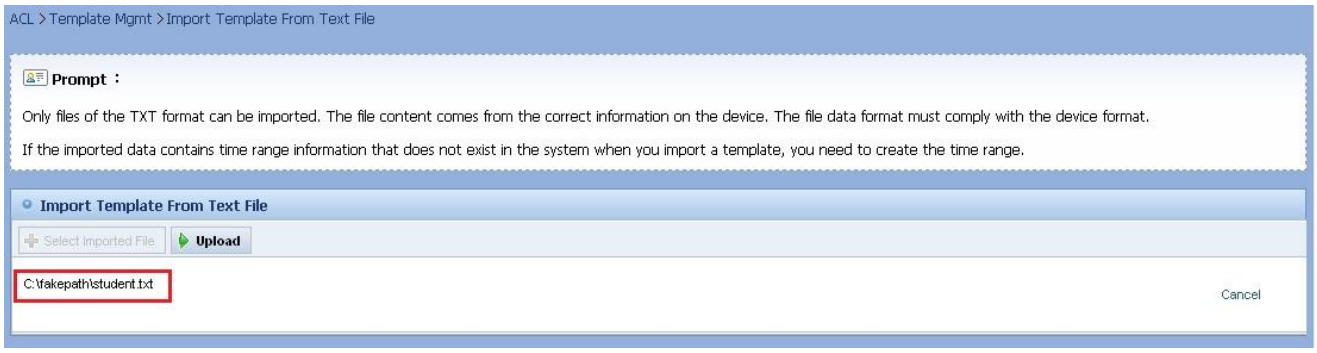


Figure 11.149. Select File Successfully

3) After successfully selecting the file, click **Upload** button. The system will upload the file and import the ACL template in the file, as shown in the following figure:

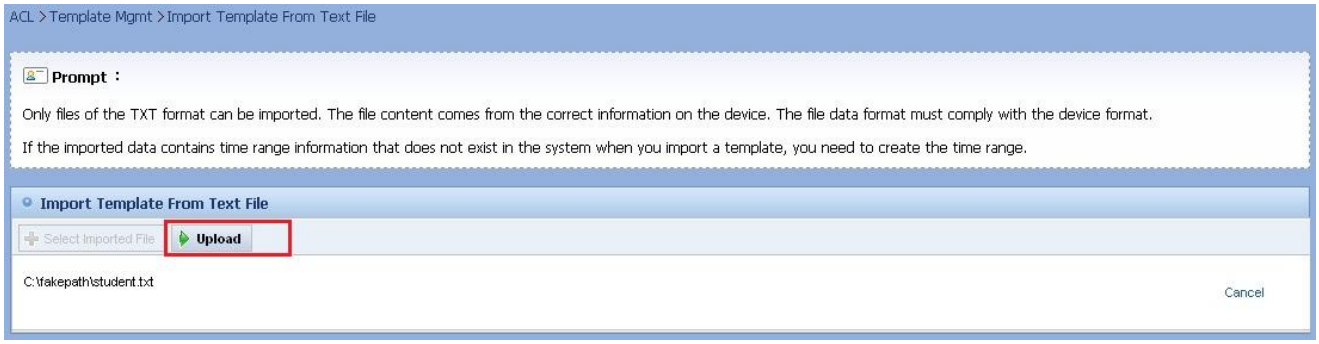


Figure 11.150. Upload File

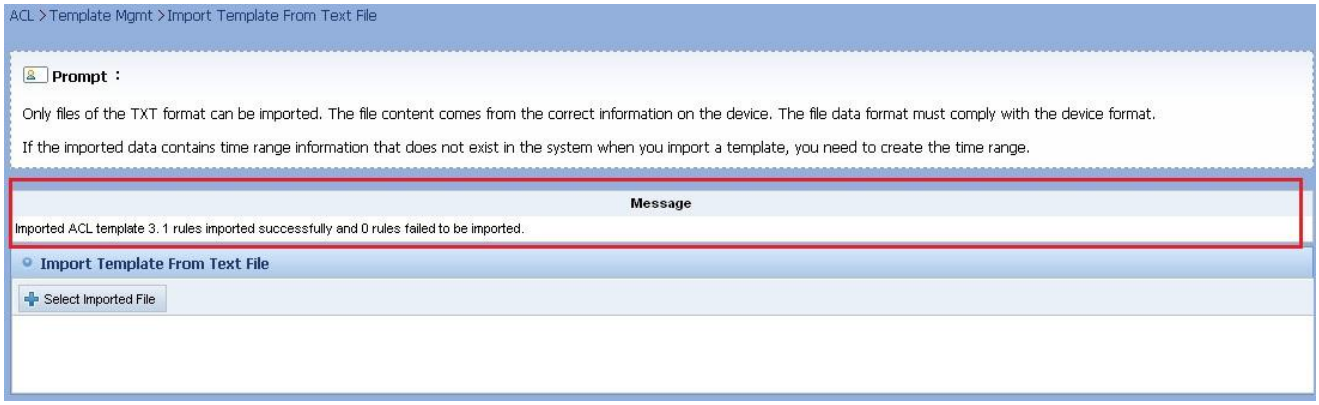


Figure 11.151. Upload File Successfully

After importing ACL template successfully, click button **Return** to return to page **ACL Template Management**.

Note

Only txt (i.e. text) file can be imported. The contents and format of the file should be the same as those on the device.

If wrong data are imported, the system will prompt data analysis failure.

If the same name already exists, the system will prompt repeated template name and importing failure.

During importing, if time range in the text does not exist, create and save the time range; if the same name of time range already exists, new time range will not be created, and the time range in the system is referenced directly.

11.4.8. Export ACL Template

Users can export the ACL template to ACL on page **Detail Information of ACL Template**.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template in the ACL Template list to enter page **Detail Information of ACL Template** of this ACL Template, as shown in the following figure:

Figure 11.152. Show ACL Template

2) On page **Detail Information of ACL Template**, click the button **Export ACL** to enter page **Export ACL**, as shown in the following figure:

Figure 11.153. Go to page **Export ACL**

3) On page **Export ACL**, enter the ACL name and the value of the variable, and click **Export** button. The system will replace variable placeholders in the ACL rule fields with the value of each variable, and add the rule to the ACL. After successful exporting, it will return to page **Detail Information of ACL template** and show importing information, as shown in the following figure:

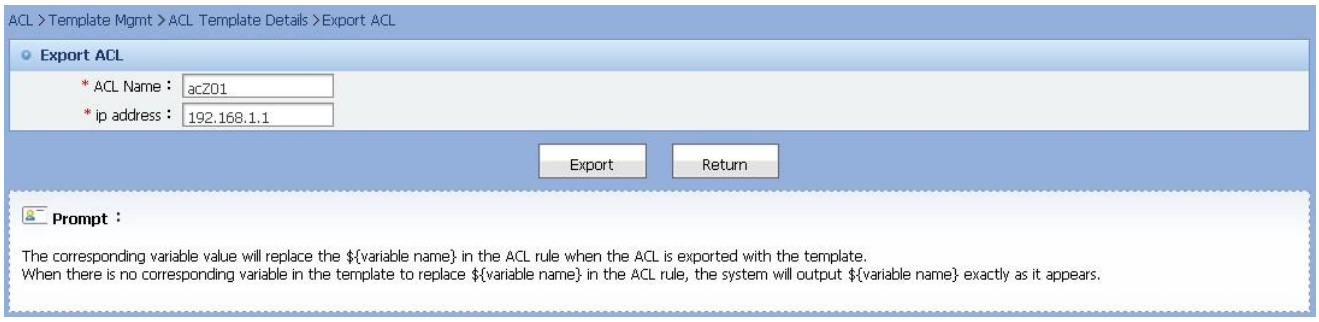


Figure 11.154. Page **Export ACL**

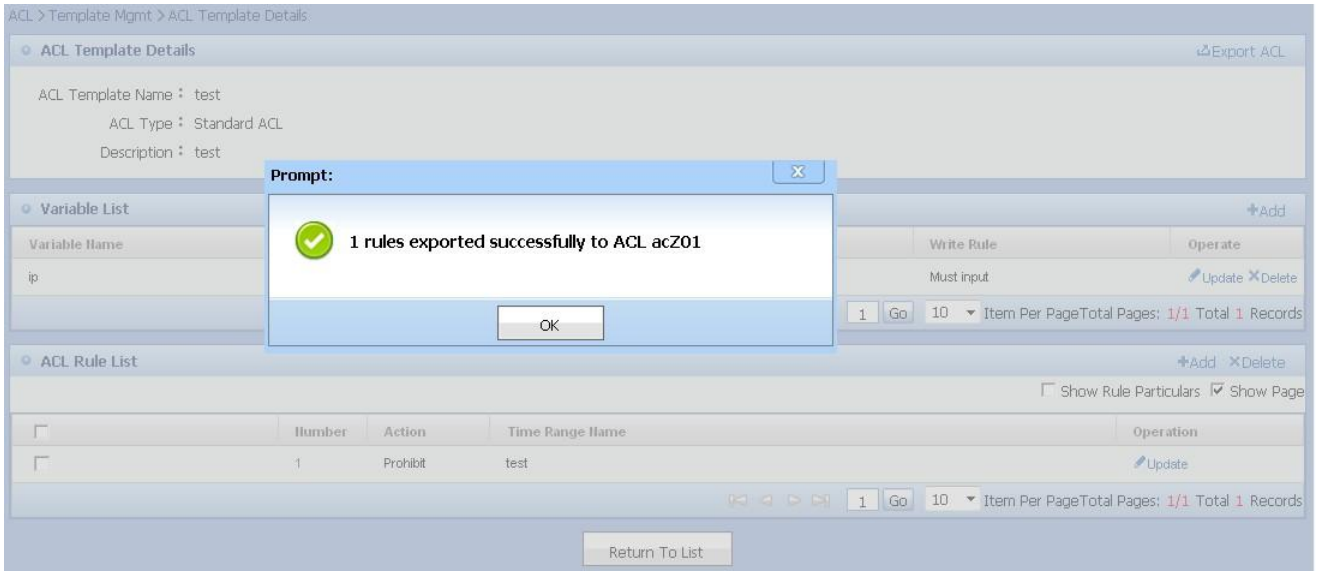


Figure 11.155. Page **Export ACL Successfully**

Note

If variable filling rule is **Ignore when not filled** and the variable in ACL rule is not entered, this rule will not be exported to the corresponding ACL.

When the variable is assigned, if the ACL rule validation fails, ACL template exporting will fail.

When exporting template to ACL, the corresponding variable's value in the template replaces the ${ variable name} in the ACL rule.

If there is no appropriate variable in the template to replace the ${ variable name} in the ACL rule, the system will output ${ variable name} exactly as it appears.

11.4.9. Variable Management

This module provides functions of adding, modifying and deleting variables.

- Add Variable
- Modify Variable
- Delete Variable

11.4.9.1. Add Variable

Go to page **Detail Information of ACL Template** to add variable. Variable will be assigned with a value during template exporting and replace variable placeholders of ACL rule.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

Figure 11.156. View ACL Template

2) On page **Detail Information of ACL Template**, click the button **Add** in variable list to enter page **Add Variable**, as shown in the following figure:

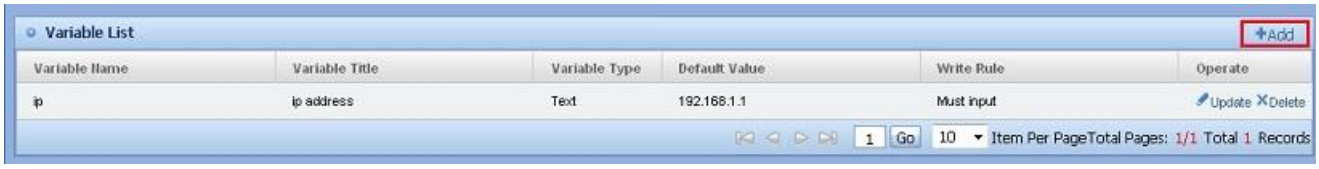


Figure 11.157. Go to page **Add Variable**

3) Go to page **Add Variable**, fill in the corresponding field value, and click **Add** button. The system will add variable to ACL template successfully, as shown in the following figure:

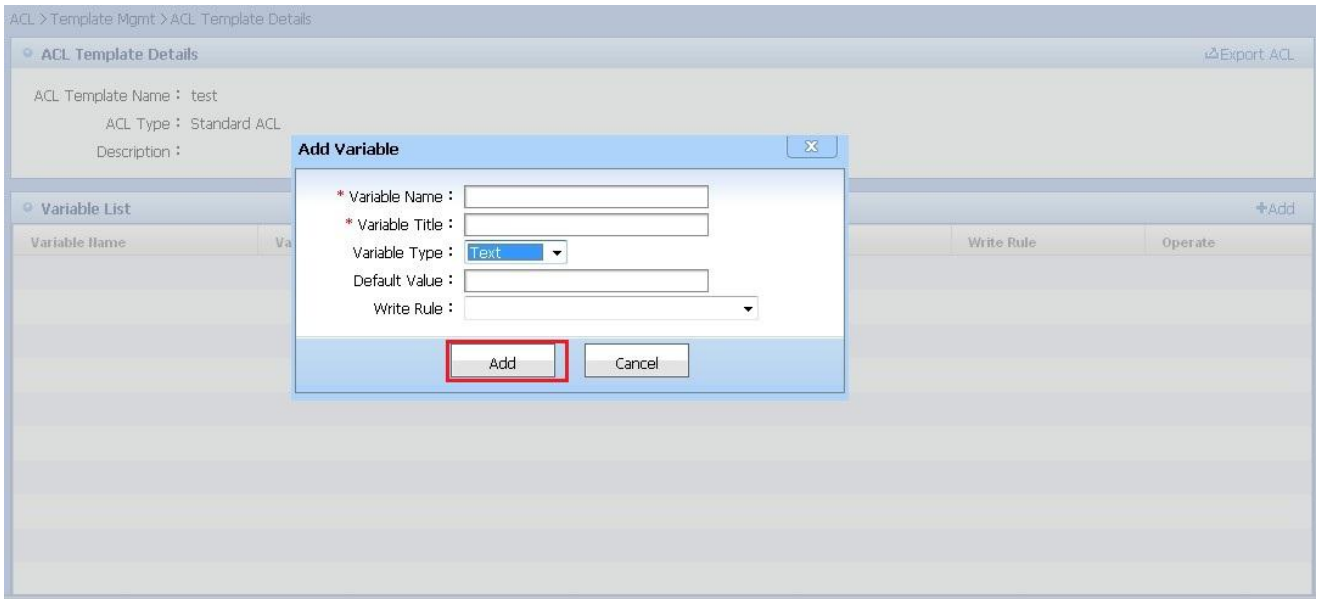


Figure 11.158. Page **Add Variable**

Note

Variable Name: comprises English letters, numbers and underscores. The maximum length is 15 English characters.

Default Value: Default value type must comply with the variable type.

Writing Rule is **Null**: When validation for ACL rule which the variable belongs to fails, the exporting for ACL template which the rule belongs to will fail.

Writing Rule is **Must input**: The variable value must be filled in; when validation for ACL rule which the variable belongs to fails, the exporting for ACL template which the rule belongs to will fail.

Writing Rule is **Ignore ACL rule when there is no input**: If the value is not entered, this rule is ignored, and this does not affect the success of ACL template exporting; if the variable is assigned with a value, when validation for ACL rule which the variable belongs to fails, the exporting for ACL template which the rule belongs to will fail.

11.4.9.2. Modify Variable

Variable can be modified on page **Detail Information of ACL Template** to modify variable. The variable will be assigned with a value during template exporting and replace variable placeholders of ACL rule.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

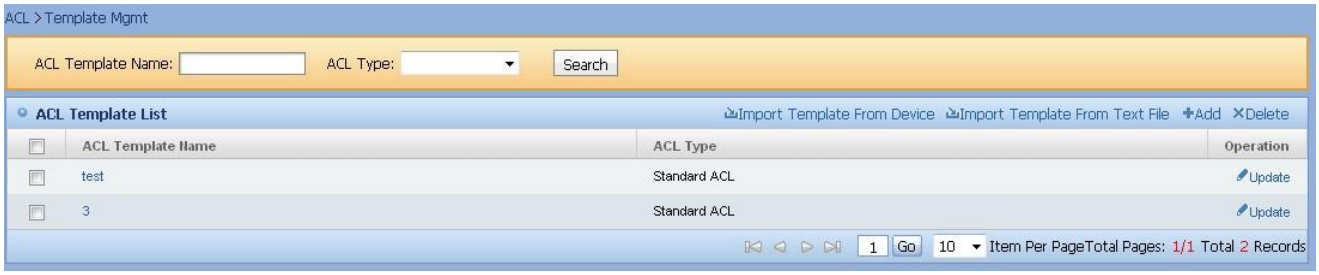


Figure 11.159. View ACL Template

2) On page **Detail Information of ACL Template**, click the button **Update** in variable list to enter page **Edit Variable**, as shown in the following figure:

Figure 11.160. Go to page **Edit Variable**

3) Go to page **Edit Variable**, fill in the corresponding field value, and click **Update** button. The system will update variable to ACL template successfully, as shown in the following figure:

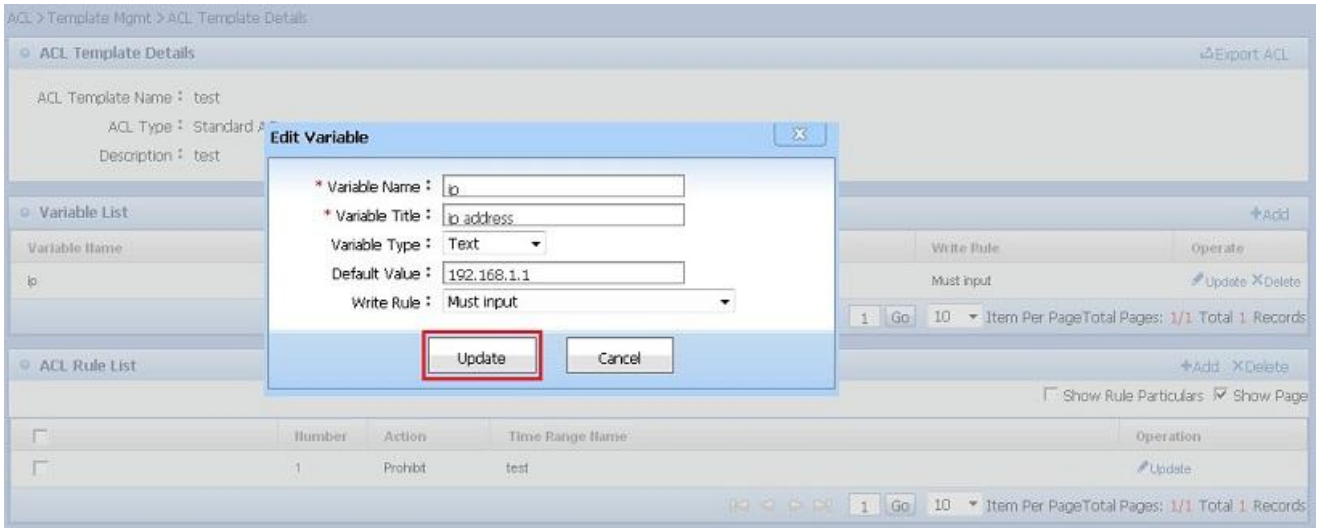


Figure 11.161. Page **Edit Variable**

11.4.9.3. Delete Variable

Variable can be deleted on page **Detail Information of ACL Template**.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

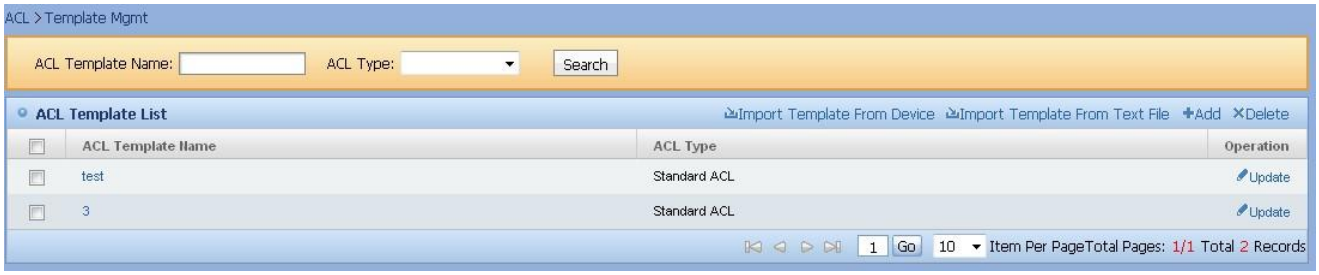


Figure 11.162. View ACL Template

2) In **Detail Information of ACL Template**, click button **Delete** in variable list. The system will prompt you to confirm the deletion operation. Click button **Confirm** to perform the deletion operation, as shown in following figure:

Figure 11.163. Delete Variable

11.4.10. ACL Rule Management in ACL Template

This module describes the functionality of adding, deleting, modifying and viewing ACL rules in ACL Template.

- Add ACL Rule
- Modify ACL Rule
- Delete ACL Rule
- View ACL Rule
- Adjust Order of ACL Rule

11.4.10.1. Add ACL Rule

There are four types of ACL rules: Standard ACL Rule, Extended ACL Rule, MAC ACL Rule, and Expert ACL Rule. All the rules can be added in this module.

- Add Standard ACL Rule
- Add Extended ACL Rule
- Add MAC ACL Rule
- Add Expert ACL Rule

11.4.10.1.1. Add Standard ACL Rule

Standard ACL Rule can be added in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Standard ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in the following figure:

Figure 11.164. Go to page **Detail Information of Standard ACL Group**

Figure 11.165. Go to page **Add Standard ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL rule, and click **Add** button, as shown in the following figure:

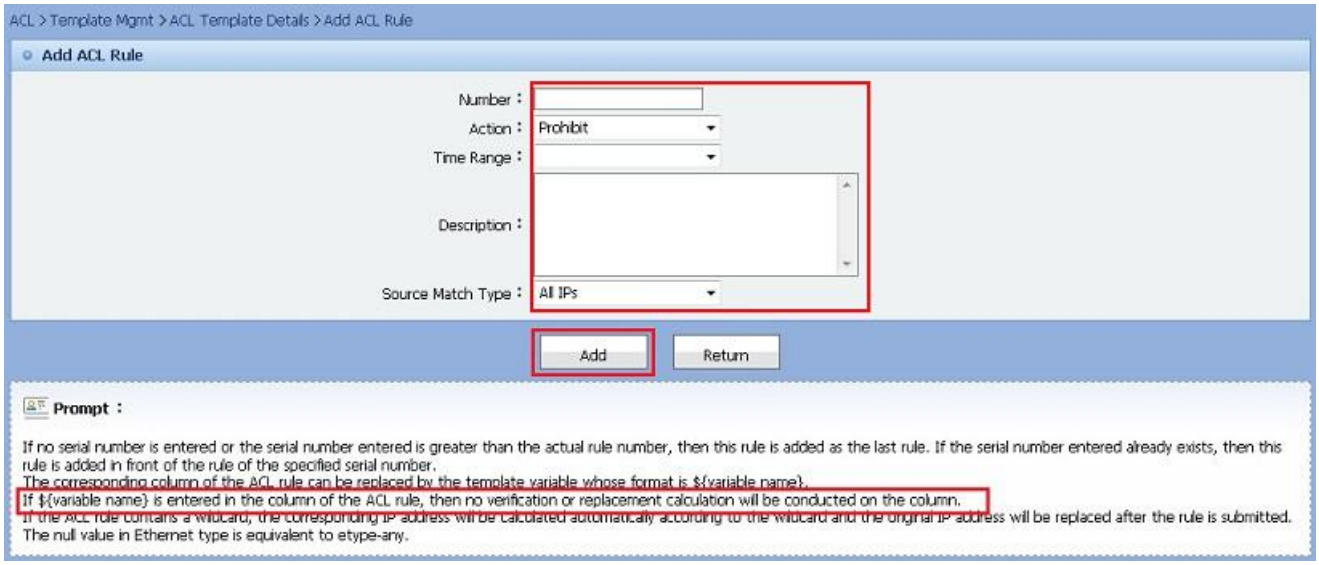


Figure 11.166. Add Standard ACL Rule

on page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Source address: When the source match the type is **Host** or **Network segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

Corresponding field of ACL rules can be replaced with the template variables, variables format: ${ variable name} .

If serial number is not filled in or the filled serial number is greater than the actual number of rules, this rule is added as the last one; if filled serial number already exists, then this rule will be added before specified serial number rules.

11.4.10.1.2. Add Extended ACL Rule

Extended ACL Rule can be added in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Extended ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in the following figure:

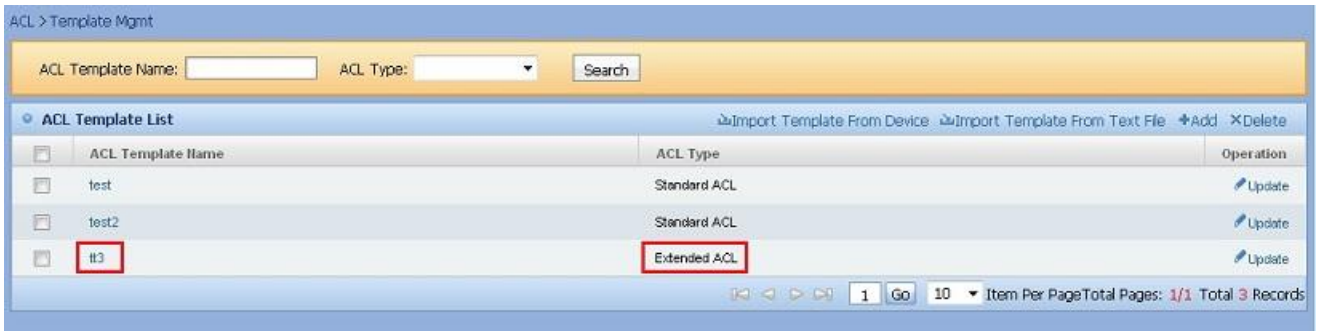


Figure 11.167. Go to page **Detail Information of Extended ACL Template**

Figure 11.168. Go to page **Add Extended ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in the following figure:

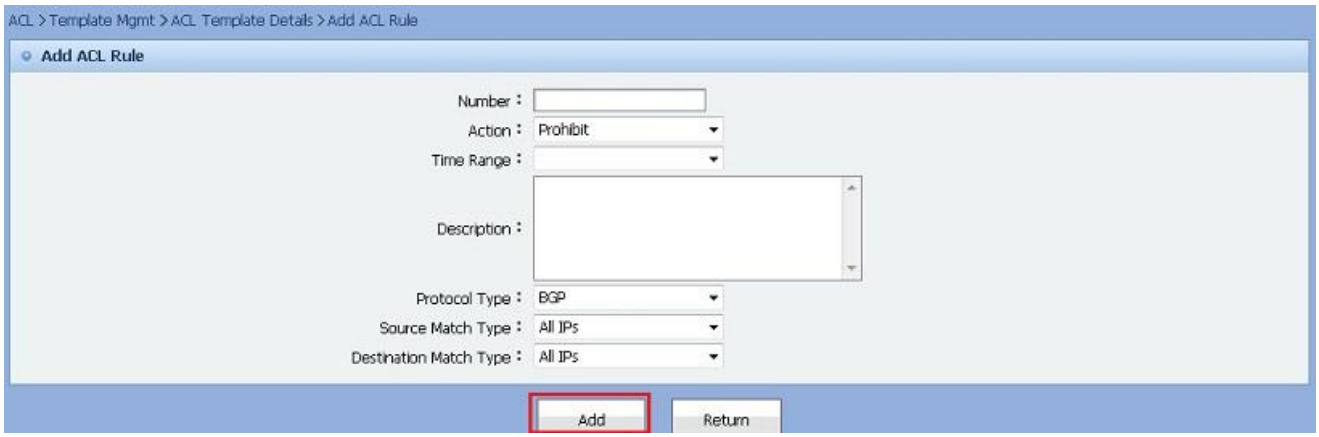


Figure 11.169. Add Extended ACL Rule

On page **Add ACL Rule** click button **Return**. the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Source address: When the source match the type is **Host** or **Network segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

Source (Destination) port: Only when the protocol type is TCP or UDP, it can be displayed and input. Port operator in the current system supports only eq.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

If serial number is not filled in or the filled serial number is greater than the actual number of rules, this rule is added as the last one; if filled serial number already exists, then this rule will be added before specified serial number rules.

11.4.10.1.3. Add MAC ACL Rule

MAC ACL Rule can be added in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **MAC ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in the following figure:

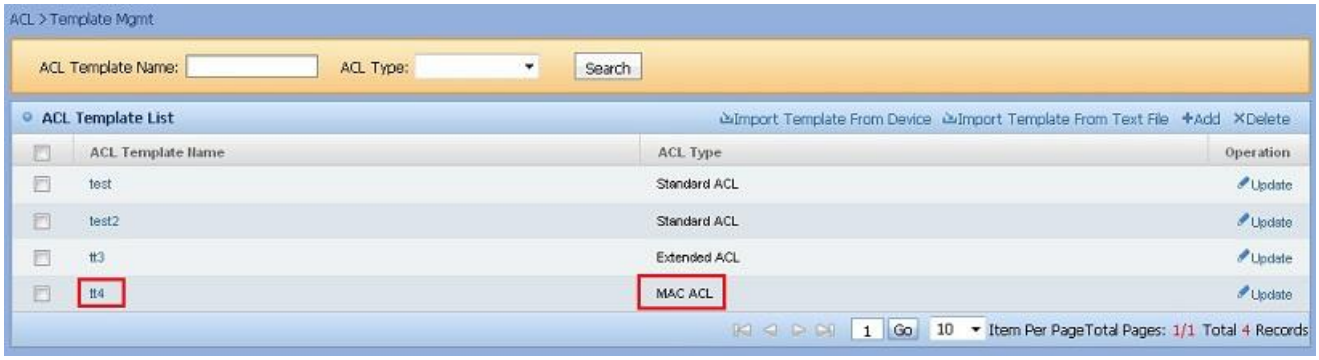


Figure 11.170. Go to page **Detail Information of MAC ACL Template**

Figure 11.171. Go to page **Add MAC ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in the following figure:

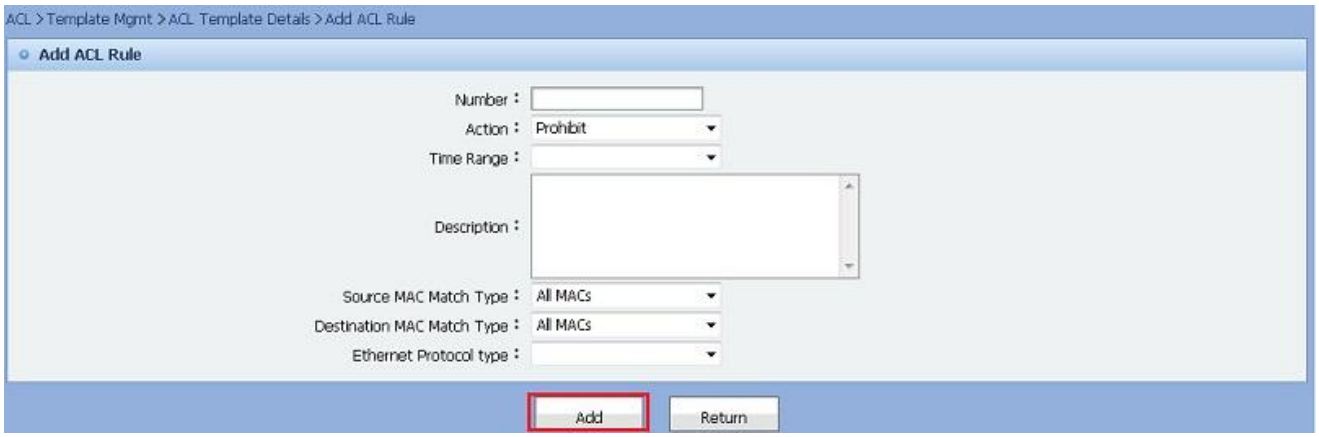


Figure 11.172. Add MAC ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Ethernet protocol type can be empty.

Source (Destination) MAC address: When the source MAC match type is **Host**, it can be displayed and input.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

If serial number is not filled in or the filled serial number is greater than the actual number of rules, this rule is added as the last one; if filled serial number already exists, then this rule will be added before specified serial number rules.

11.4.10.1.4. Add Expert ACL Rule

Expert ACL Rule can be added in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Expert ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Add** in the **ACL Rule List** to enter page **Add ACL Rule**, as shown in the following figure:

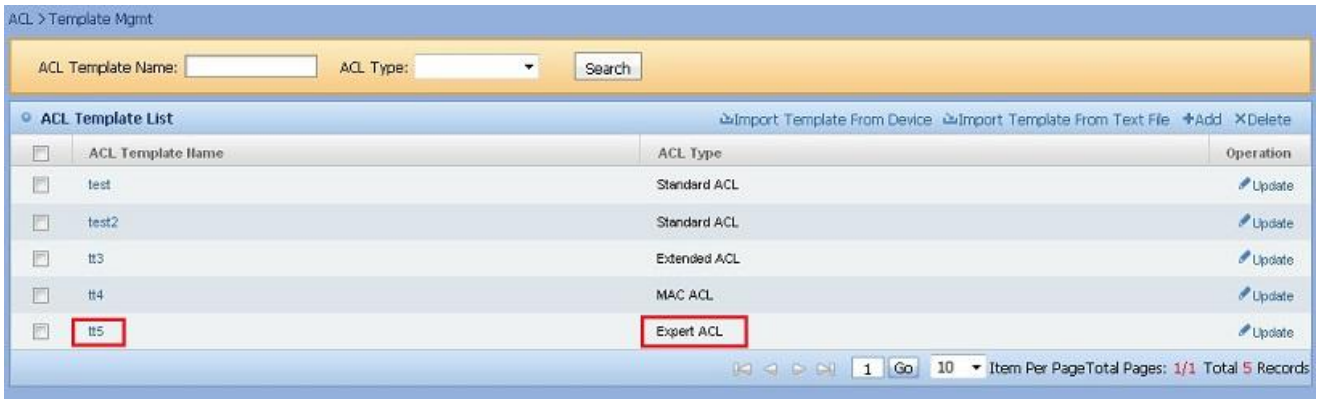


Figure 11.173. Go to page **Detail Information of Expert ACL Template**

Figure 11.174. Go to page **Add Expert ACL Rule**

2) Go to page **Add ACL Rule**, fill in the information related to ACL Rule, and click **Add** button, as shown in the following figure:

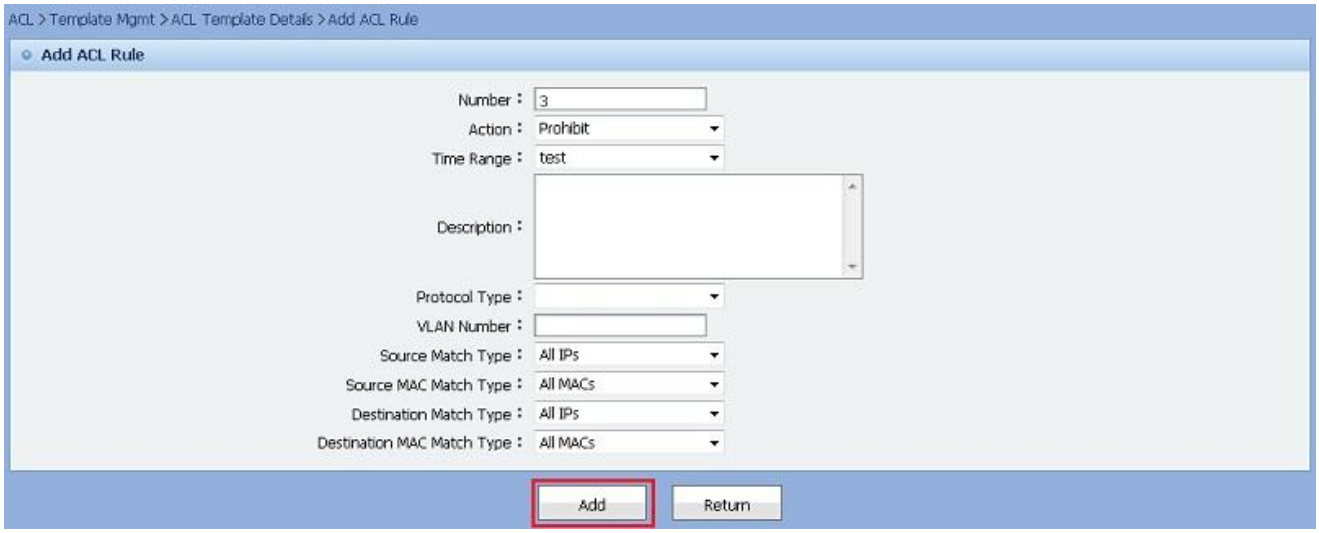


Figure 11.175. Add Expert ACL Rule

On page **Add ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

In cases of different protocol types, the system will display different input fields.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

If serial number is not filled in or the filled serial number is greater than the actual number of rules, this rule is added as the last one; if filled serial number already exists, then this rule will be added before specified serial number rules.

11.4.10.2. Modify ACL Rule

There are four types of ACL rules: Standard ACL Rule, Extended ACL Rule, MAC ACL Rule, and Expert ACL Rule. All the rules can be modified in this module.

- Modify Standard ACL Rule
- Modify Extended ACL Rule
- Modify MAC ACL Rule
- Modify Expert ACL Rule

11.4.10.2.1. Modify Standard ACL Rule

Standard ACL Rule can be modified in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Standard ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Update** in the **ACL Rule List** to enter page **Edit ACL Rule**, as shown in the following figure:

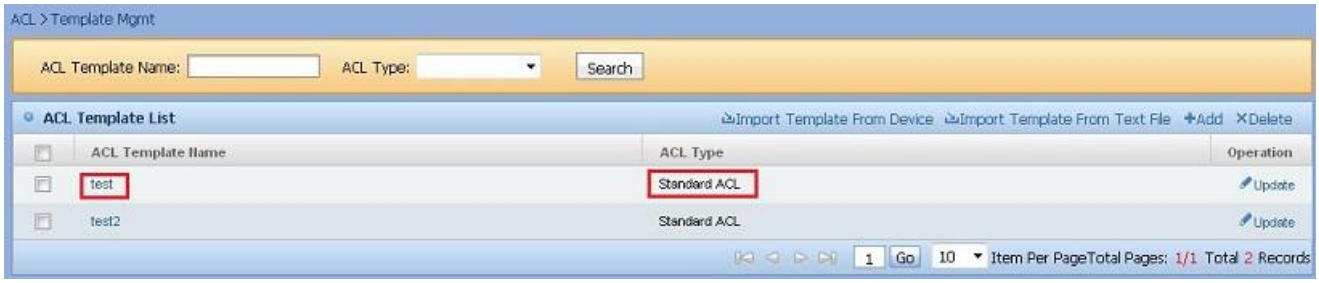


Figure 11.176. Go to page **Detail Information of Standard ACL Template**

Figure 11.177. Go to page **Edit Standard ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in the following figure:

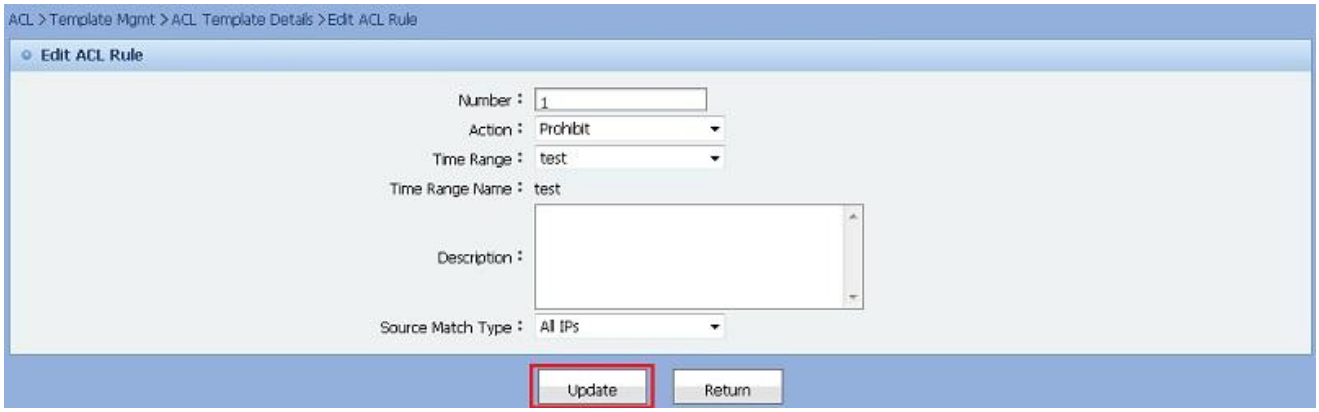


Figure 11.178. Edit Standard ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Source address: When the source match the type is **Host** or **Network segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

11.4.10.2.2. Modify Extended ACL Rule

Extended ACL Rule can be modified in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Extended ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Update** in the **ACL Rule List** to enter page **Edit ACL Rule**, as shown in the following figure:

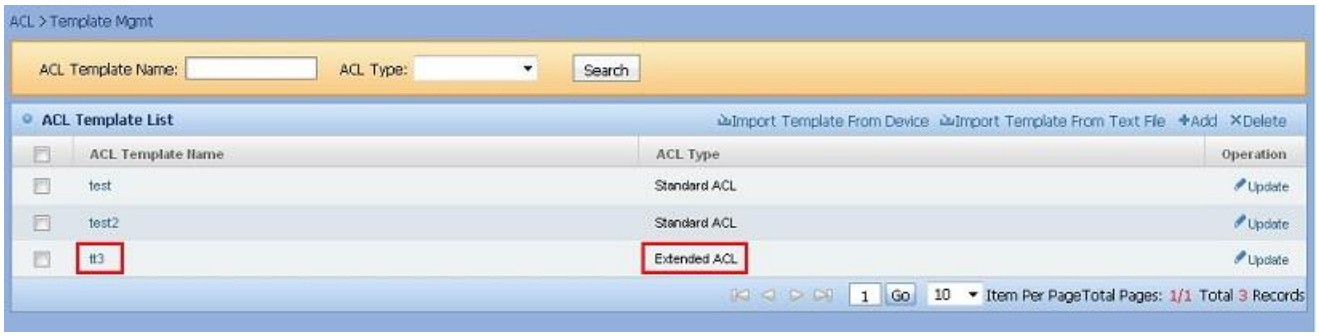


Figure 11.179. Go to page **Detail Information of Extended ACL Rule**

Figure 11.180. Go to page **Edit Extended ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in the following figure:

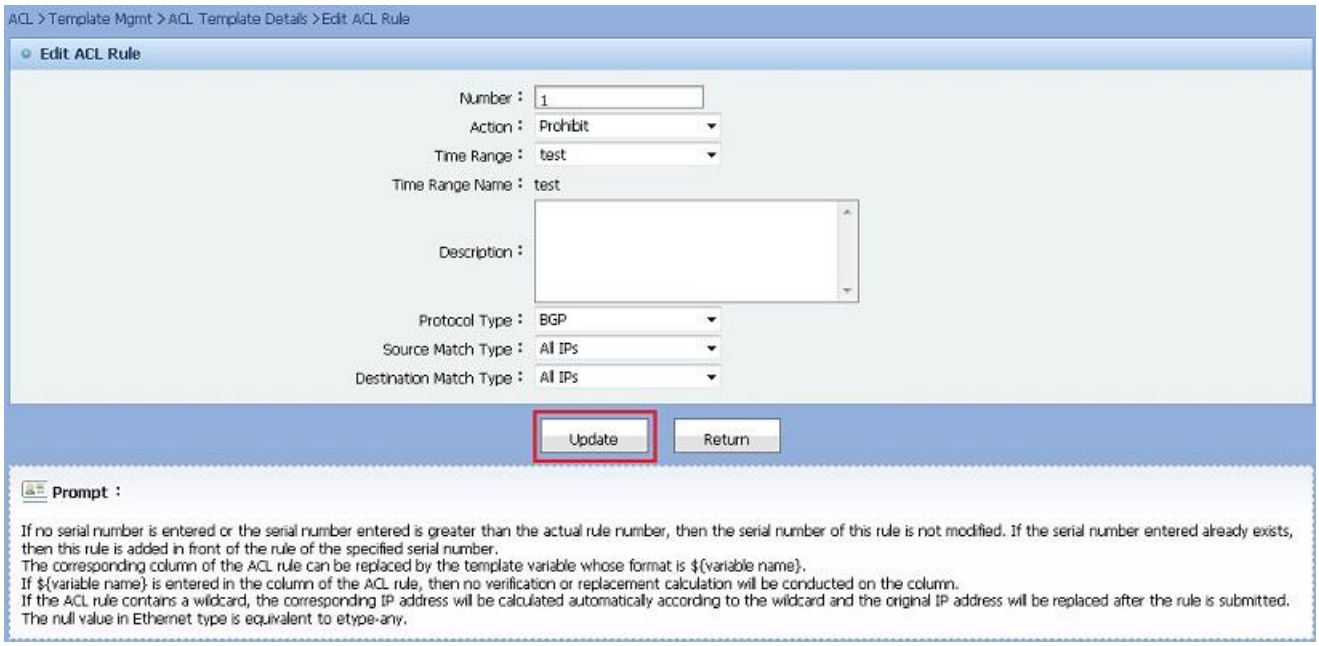


Figure 11.181. Edit Extended ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Source address: When the source match the type is **Host** or **Network segment**, it can be displayed and input. IP address does not support input with range.

Source wildcard: Only when the source match type is **Network Segment**, it can be displayed and input.

Source (Destination) port: Only when the protocol type is TCP or UDP, it can be displayed and input. Port operator in the current system supports only eq.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

11.4.10.2.3. Modify MAC ACL Rule

MAC ACL Rule can be modified in ACL Template Management.

Operating Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template which **ACL Type** is **MAC ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Update** in the **ACL Rule List** to enter page **Edit ACL Rule**, as shown in the following figure:

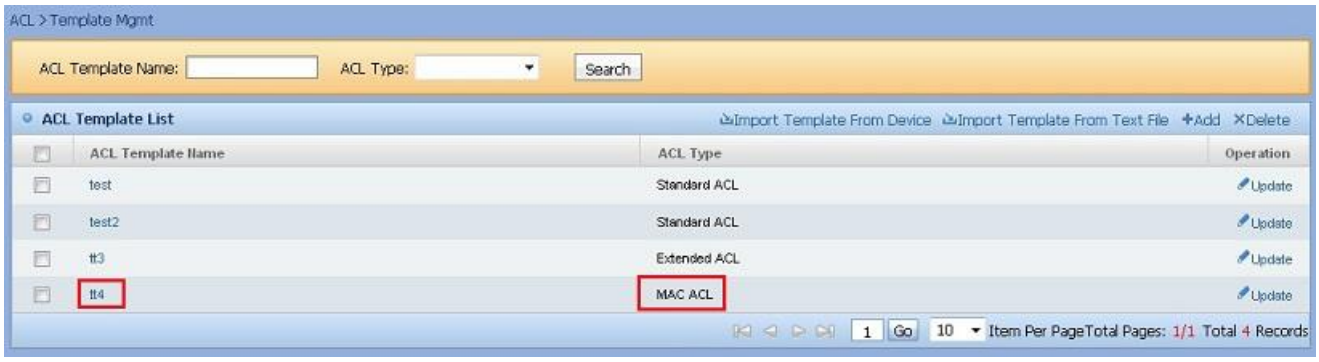


Figure 11.182. Go to page **Detail Information of MAC ACL Template**

Figure 11.183. Go to page **Edit MAC ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in the following figure:

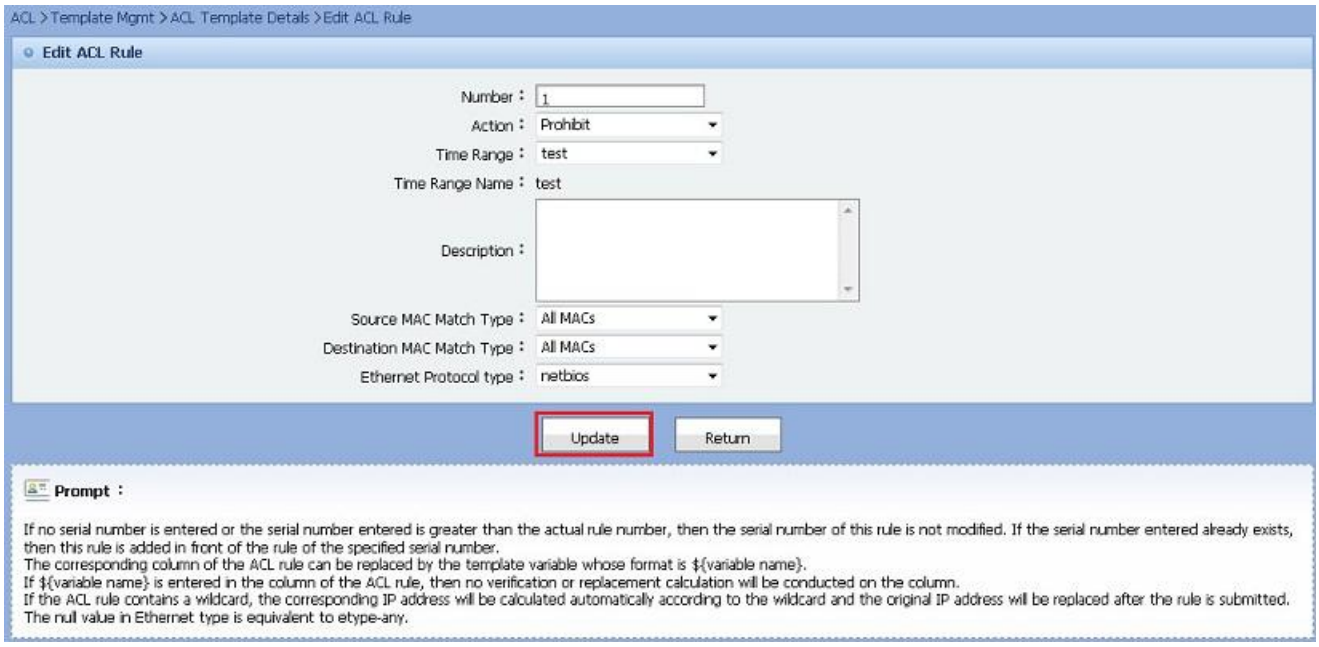


Figure 11.184. Edit MAC ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

Ethernet protocol type can be empty.

Source (Destination) MAC address: When the source MAC match type is **Host**, it can be displayed and input.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name} .

11.4.10.2.4. Modify Expert ACL Rule

Expert ACL Rule can be modified in ACL Template Management.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** of the ACL Template whose **ACL Type** is **Expert ACL** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template. Click button **Update** in the **ACL Rule List** to enter page **Edit ACL Rule**, as shown in the following figure:

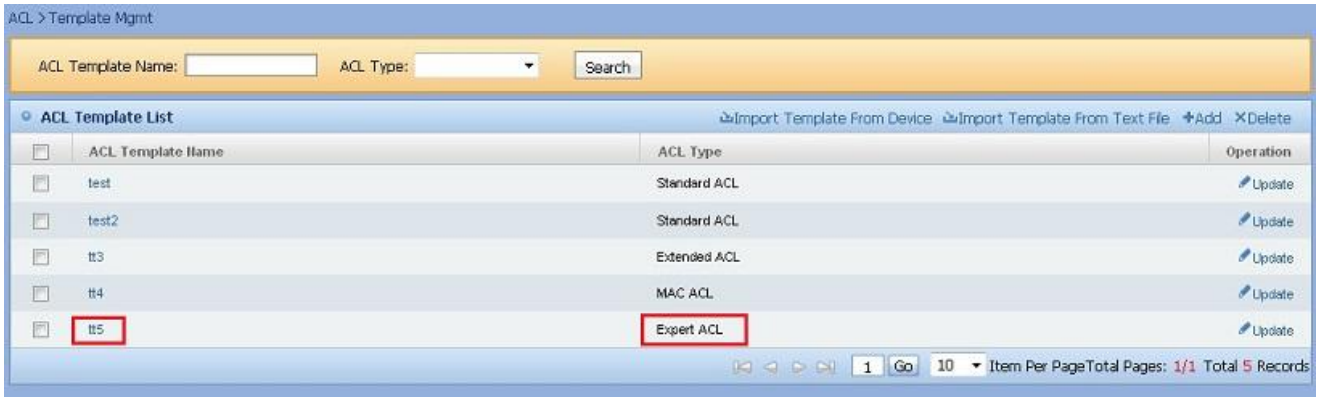


Figure 11.185. Go to page **Detail Information of Expert ACL Template**

Figure 11.186. Go to page **Edit Expert ACL Rule**

2) Go to page **Edit ACL Rule**, fill in the information related to ACL Rule, and click **Update** button, as shown in the following figure:

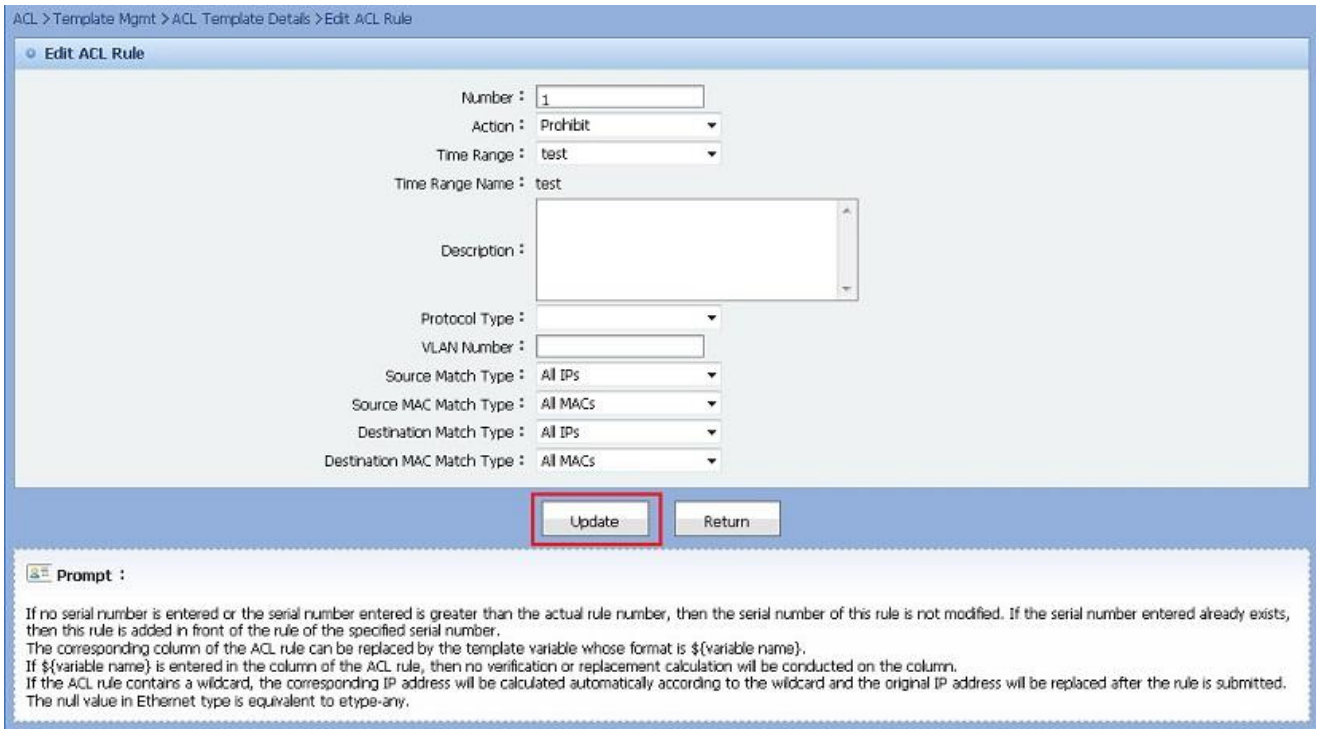


Figure 11.187. Edit Expert ACL Rule

On page **Edit ACL Rule**, if **Return** is clicked, the system saves no modification and returns to **Detail Information of ACL Template** page directly.

Note

Time Range Name: optional, not required. If not entered, it means that valid time is all the time.

In cases of different protocol types, the system will display different input fields.

If wildcard is filled in the ACL rules, the corresponding IP address will be automatically calculated according to the wildcard and replace the original IP address after being submitted.

Corresponding field of ACL rules can be replaced with the template variables, variables format: $ { variable name}.

11.4.10.3. Delete ACL Rule

The ACL Rule can be deleted on page Detail Information of ACL Template.

Operation Steps

1) On page **ACL Template Management**, and click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

Figure 11.188. Go to page **Detail Information of ACL Template**

2) In **ACL Rule list**, click button **Delete**. The system will prompt to you confirm the deletion operation. Click button **Confirm** to perform the deletion operation, as shown in the following figure:

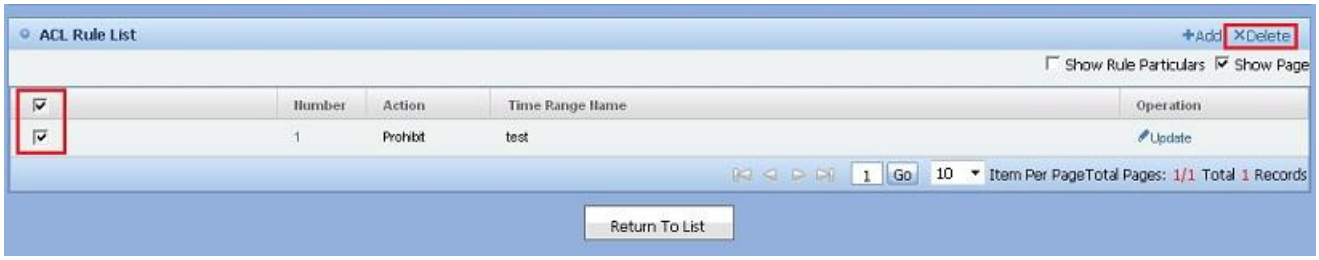


Figure 11.189. Delete ACL Rule

11.4.10.4. View ACL Rule

The ACL Rule can be viewed on page Detail Information of ACL Template.

Operation Steps

1) On page **ACL Template Management**, click the link **ACL Template Name** in the ACL Template list to enter page **Detail Information of ACL Template** for ACL Template, as shown in the following figure:

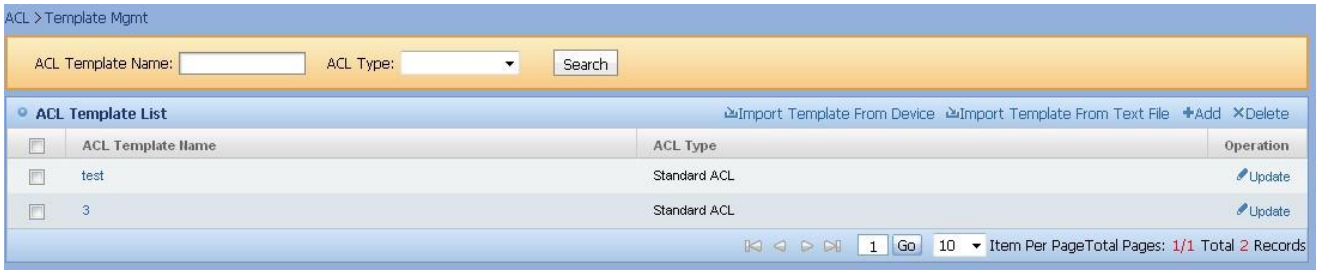


Figure 11.190. Go to page **Detail Information of ACL Template**

2) In **ACL Rule List**, click the link **Number** of ACL rule to be viewed to enter page **Detail Information of ACL Rule**, as shown in the following figure:

Figure 11.191. Go to page **Detail information of ACL Rule**

Figure 11.192. Page **Detail Information of ACL Rule**

Note

Position of extended field depends on the specific ACL rule type.

11.4.10.5. Adjust Order of ACL Rule

The order of ACL rule can be adjusted on page **Detail Information of ACL Template**.

Operation Steps

1) On page **ACL Template Management**, and click the link **ACL Template Name** to enter page **Detail Information of ACL Template** for this ACL Template, as shown in the following figure:

Figure 11.193. Go to page **Detail Information of ACL Template**

2) In **ACL rule list**, according to the ACL rules to be adjusted, click the move button in **Operation** bar to adjust the order of ACL rules, as shown in the following figure:

Figure 11.194. Adjust the Order of ACL Rules

Note

Move to the first one (Move to the last one) is to move to the head (tail) of all rules, not head (tail) of this page.

11.5. ACL Deployment Plan Management

This module includes: creating deployment plan and deploying ACL rule, time range and interface ACL to devices in batch.

- Search ACL Deployment Plan
- Delete Deployment Plan
- Modify Deployment Plan
- Modify Interface Deployment Plan
- Stop Deployment Plan
- Start Deployment Plan
- View Deployment Plan
- View Detail Log of Deployment Plan
- Add Deployment Plan
- Add Interface Deployment Plan

11.5.1. Search ACL Deployment Plan

Plan name can be filled in to search for ACL Deployment Plan on page **ACL Deployment Plan Management**.

Operation Steps

Go to page **ACL Deployment Plan Management**, fill in plan name, and then click **Search** button. The system will search and return ACL Deployment Plan list which satisfy search conditions, as shown in the following figure:

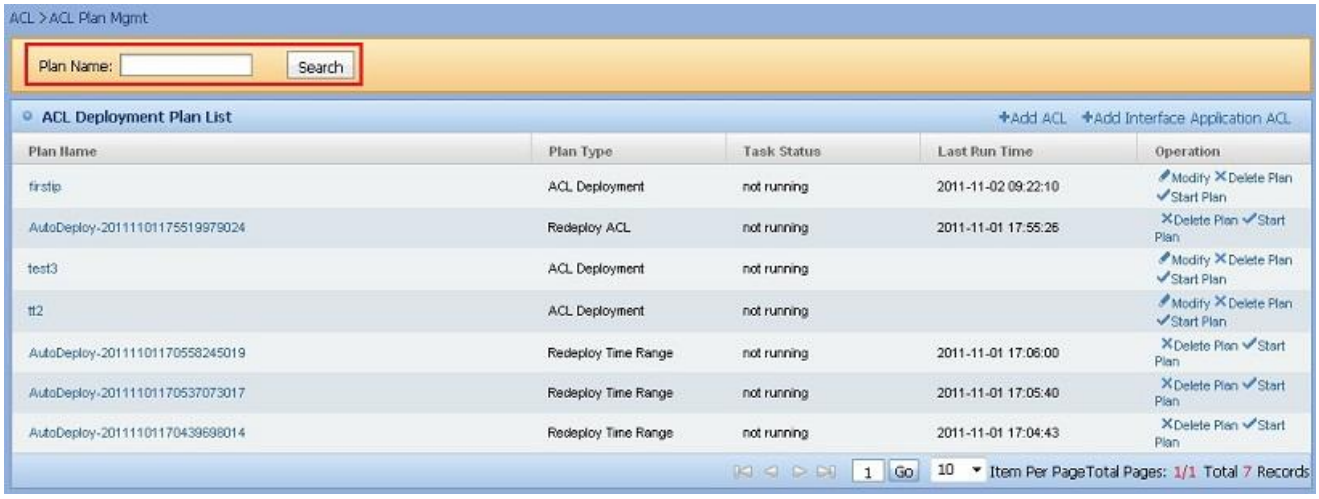


Figure 11.195. Search ACL Deployment Plan

11.5.2. Delete Deployment Plan

Users can delete Deployment Plan one by one on page **ACL Deployment Plan Management**.

Operation Steps

Go to page **ACL Deployment Plan Management** ,click button **Delete Plan** in plan list. The system will prompt you to confirm the deletion operation. Click button **Confirm** to delete the corresponding ACL deployment plan, as shown in following figure:

Figure 11.196. Delete Deployment Plan

11.5.3. Modify Deployment Plan

Deployment Plan can be modified on page **ACL Deployment Plan Management**

Operating Steps

1) On page **ACL Deployment Plan Management**, select the ACL Deployment Plan whose plan type is **ACL Deployment**, and click button **Modify** to enter page **Modify ACL Deployment Plan**, as shown in the following figure:

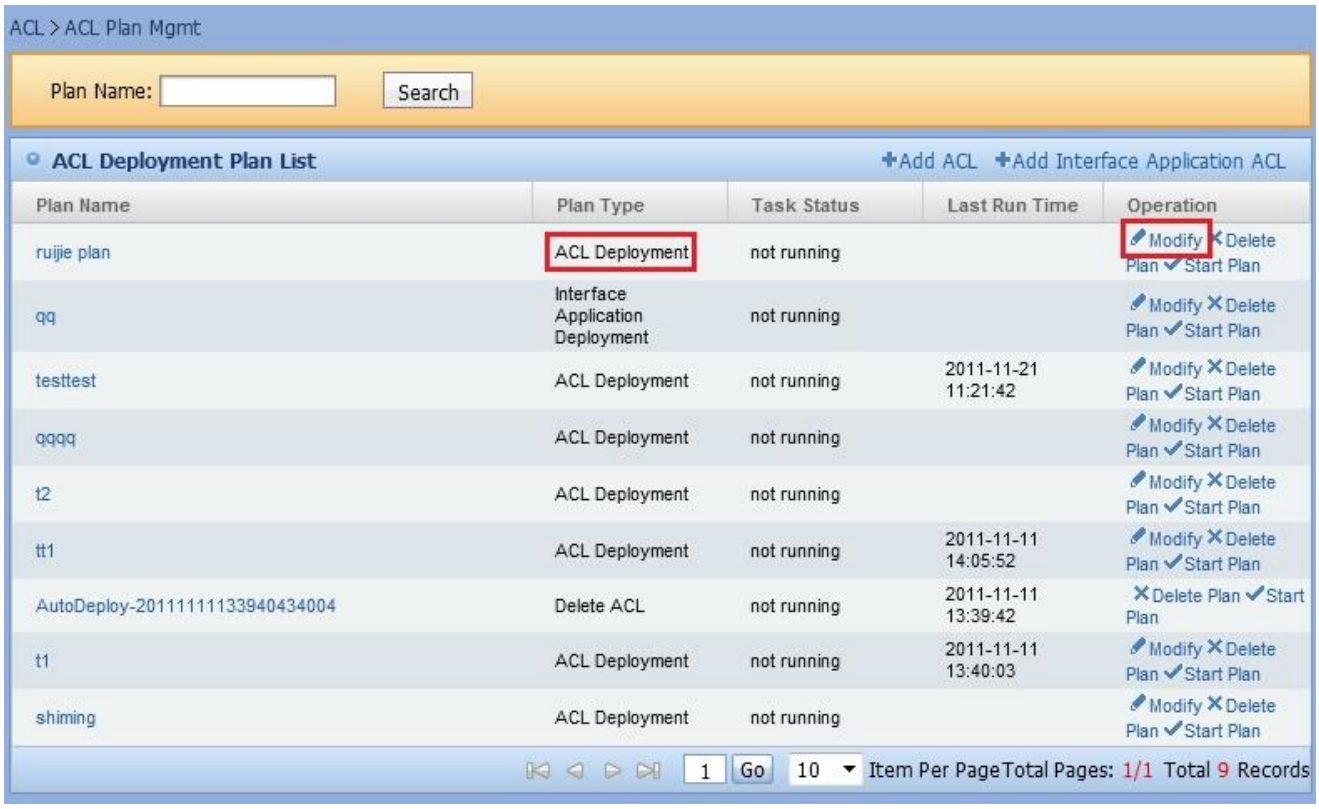


Figure 11.197. Go to page **Modify ACL Deployment Plan**

2) Show page **Selected Device List**, as shown in the following figure:

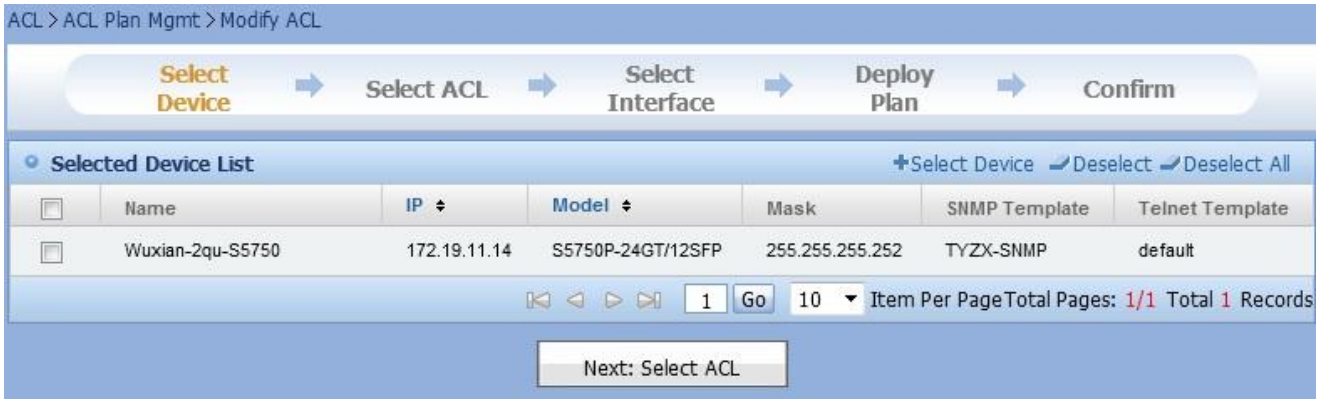


Figure 11.198. Show page **Selected Device list**

3) Click **Select Device** button to display page **Select Device**, as shown in the following figure:

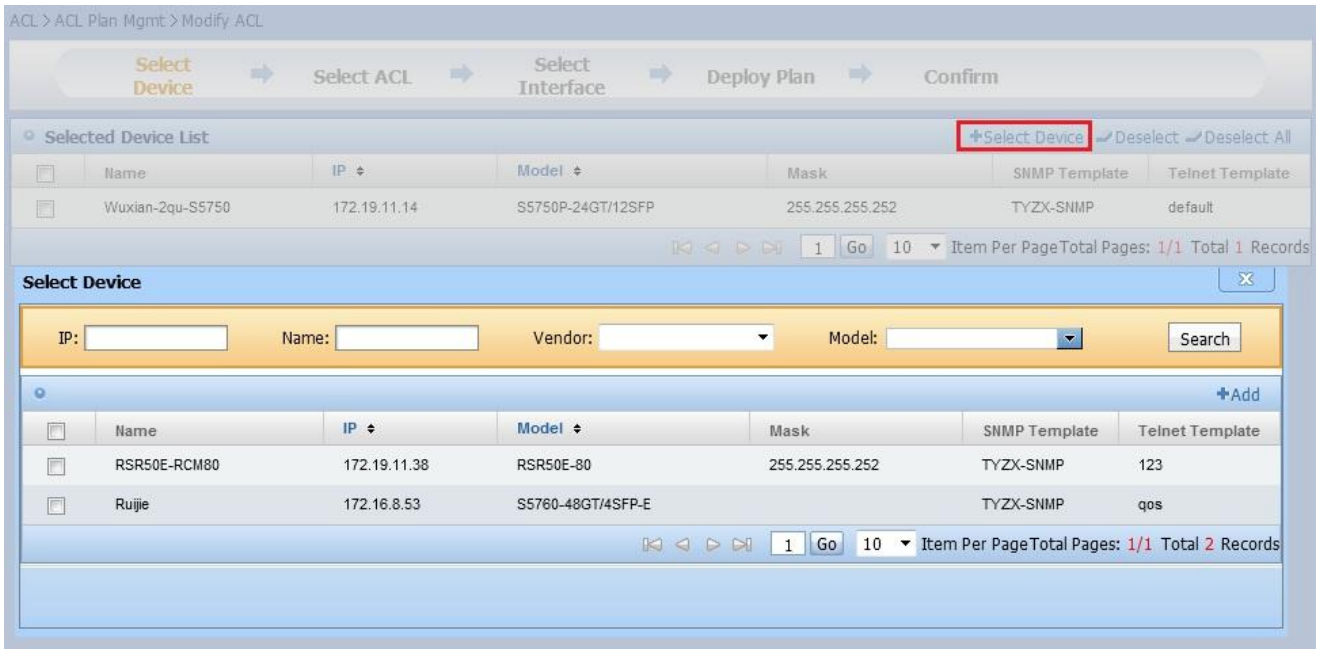


Figure 11.199. Select Device

4) After selecting device, click the **Add** button, as shown in the following figure:

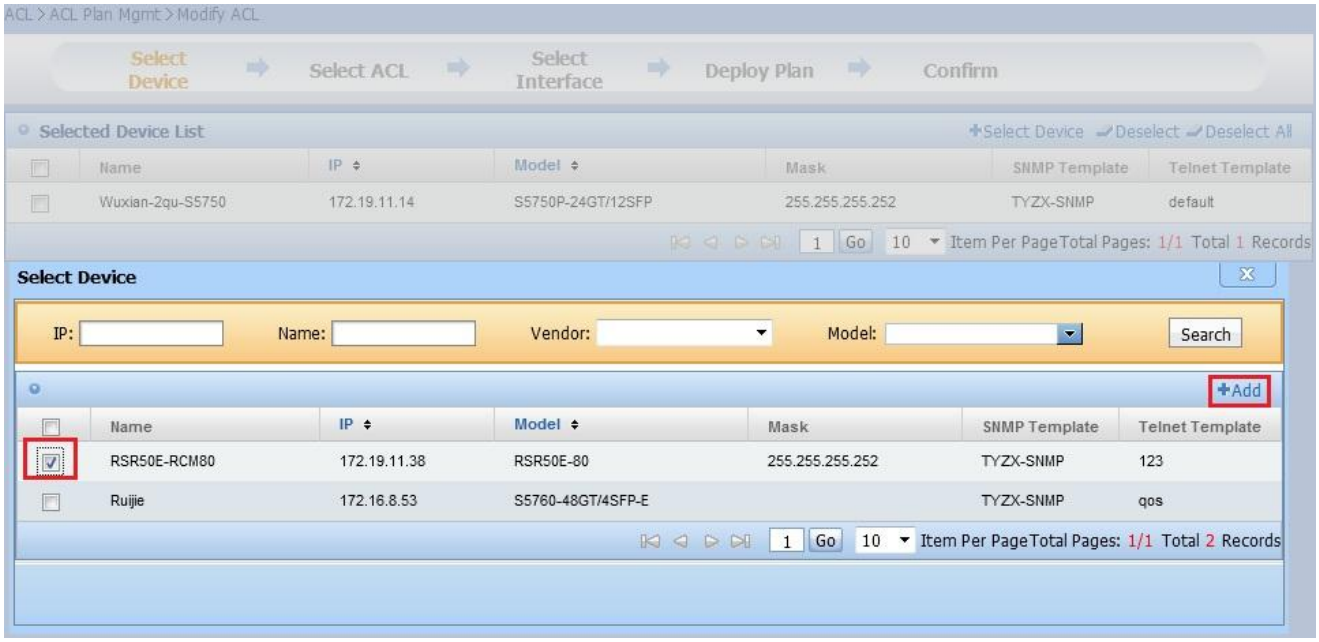


Figure 11.200. Add Device

5) Show page **Selected Device List**, and click button **Next: Select ACL**, as shown in the following figure:

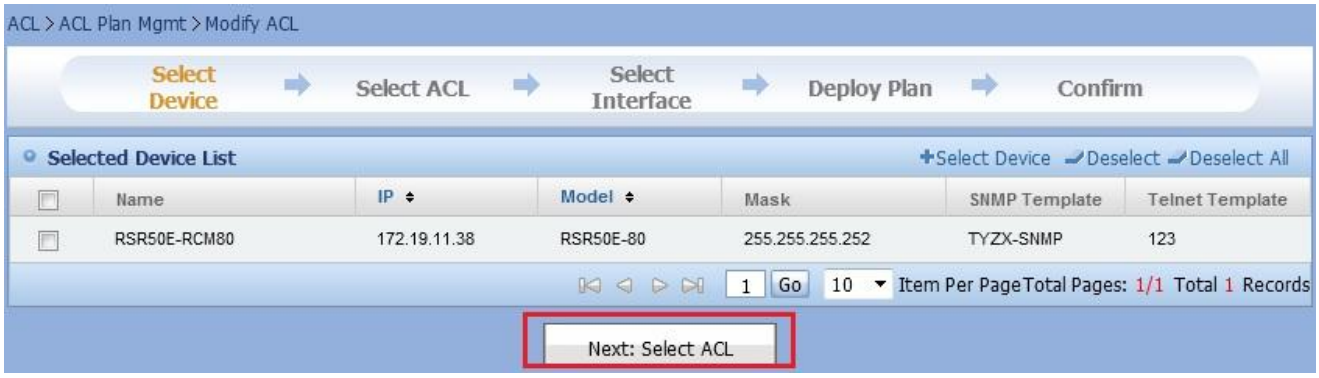


Figure 11.201. Next: Select ACL

6) Show page **Selected ACL List**, as shown in the following figure:

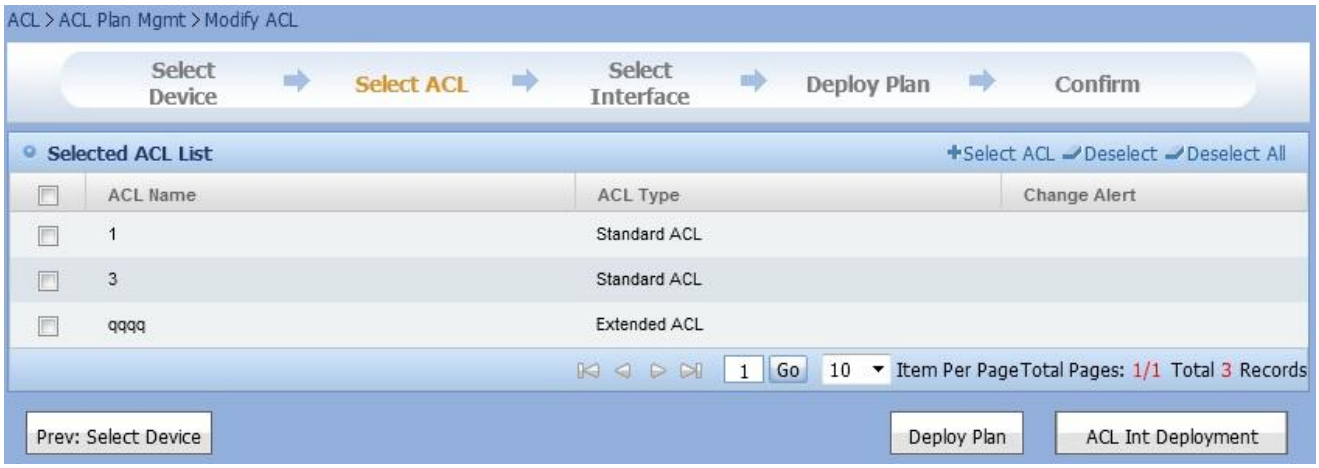


Figure 11.202. Select ACL

7) Click **Select ACL** button to enter page **Available ACL List**, as shown in the following figure:

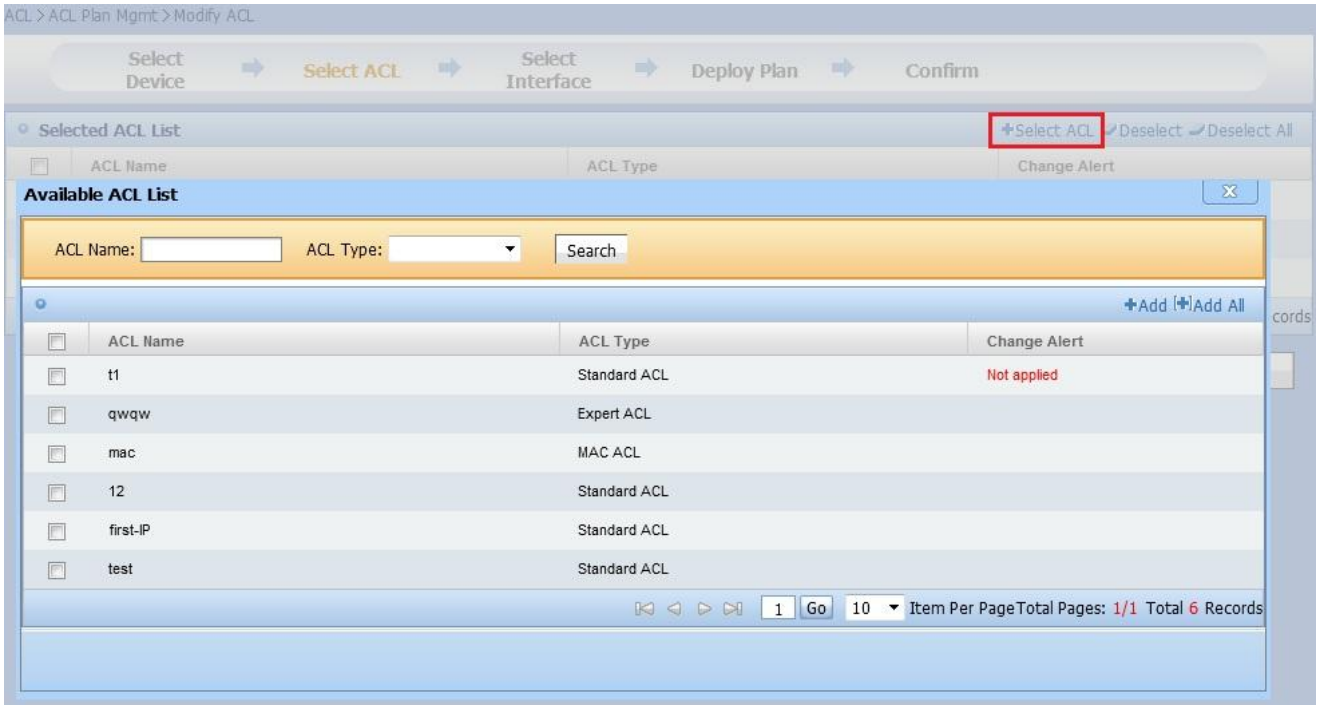


Figure 11.203. Select ACL

8) After selecting ACL, click the **Add** button, as shown in the following figure:

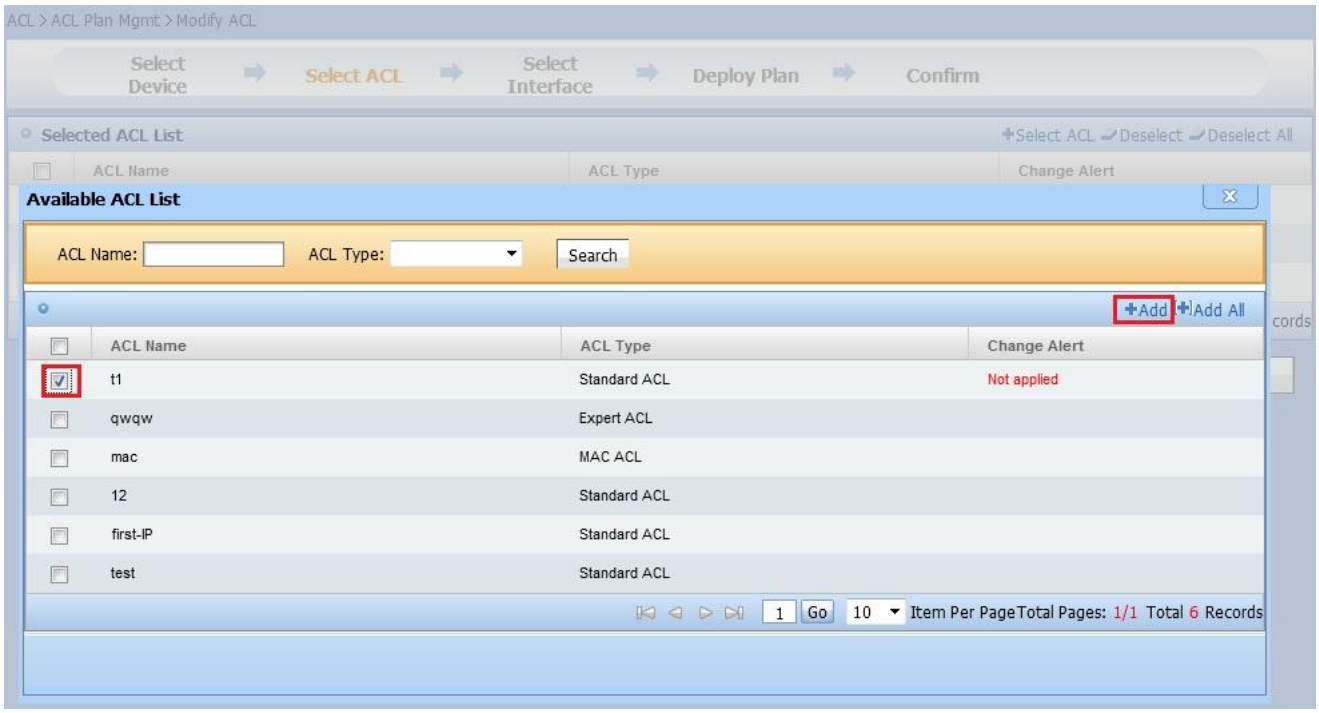


Figure 11.204. Add ACL

9) Show page **Selected ACL List**, and click button **Previous: Select Device** to return to page **Selected Device List**, as shown in the following figure:

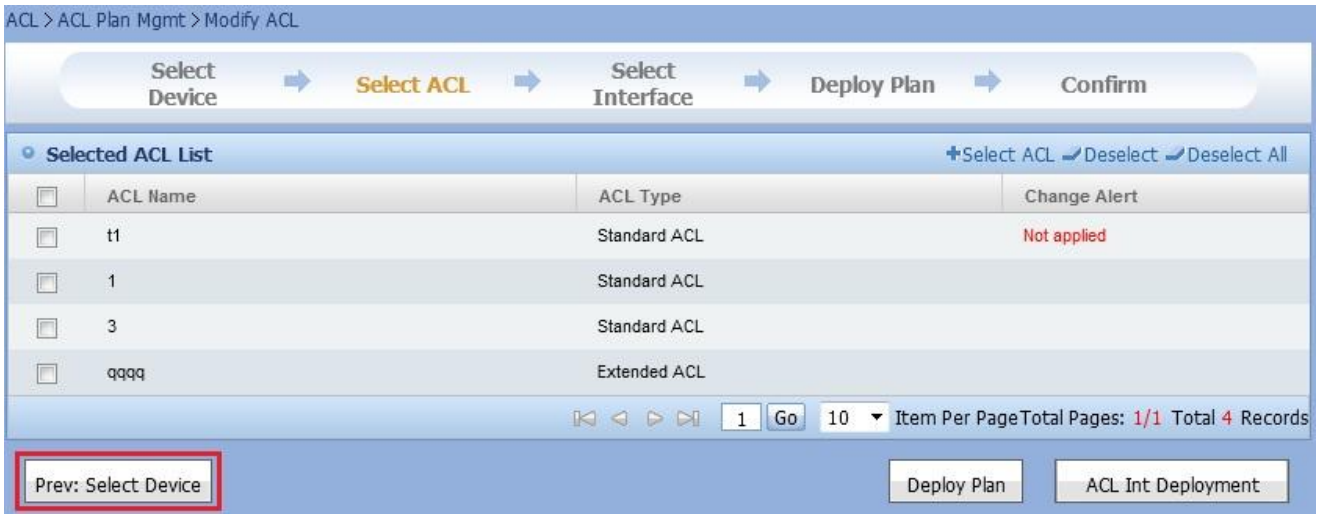


Figure 11.205. Previous: Select Device

10) Show page **Selected ACL List**, and click button **Deploy Plan** to enter page **Deploy Plan**, as shown in the following figure:

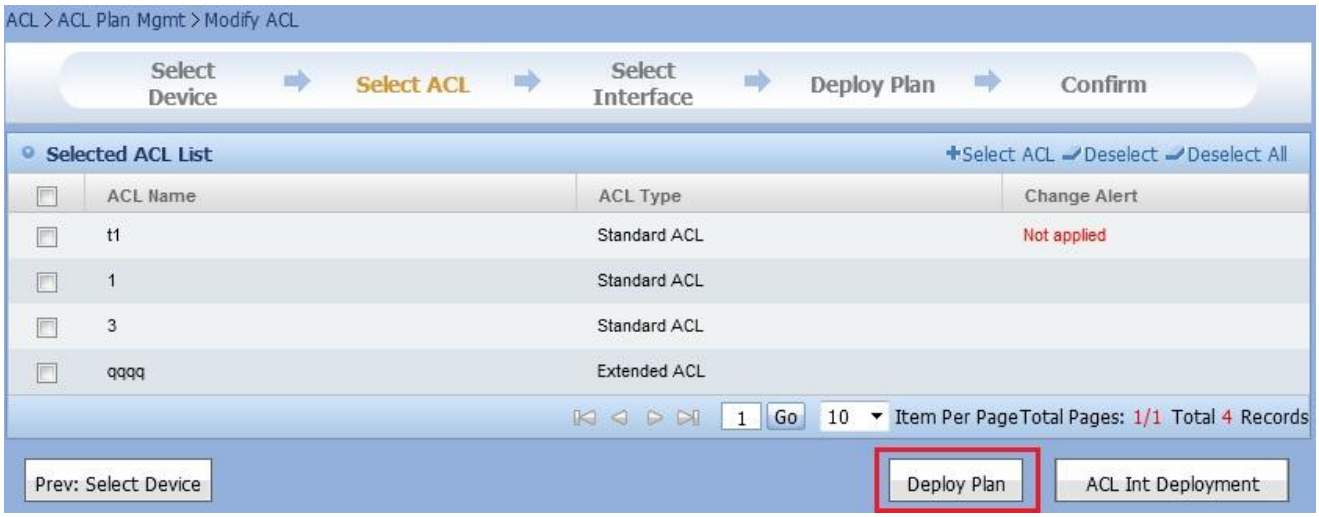


Figure 11.206. Deploy Plan

11) Show page **Selected ACL List**, and click button **ACL Int Deployment** to enter page **Select Interface**, as shown in the following figure:

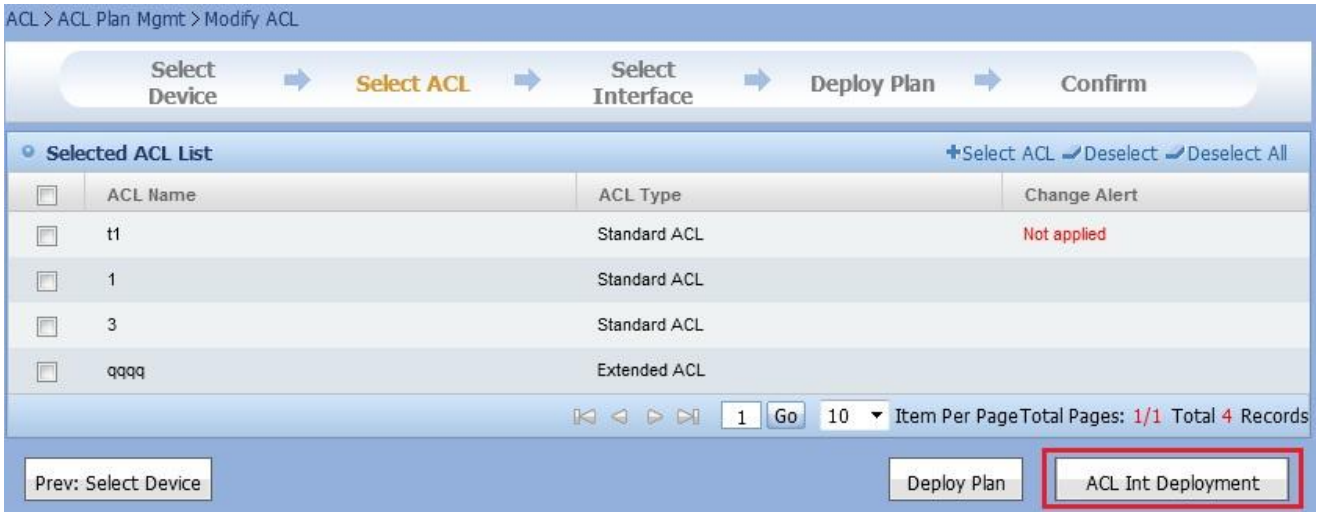


Figure 11.207. Deploy ACL on Interface

12) Show page **Select Interface** to click **Configure Interface** icon under **Operation** column to enter page **Select Interface**, as shown in the following figure:

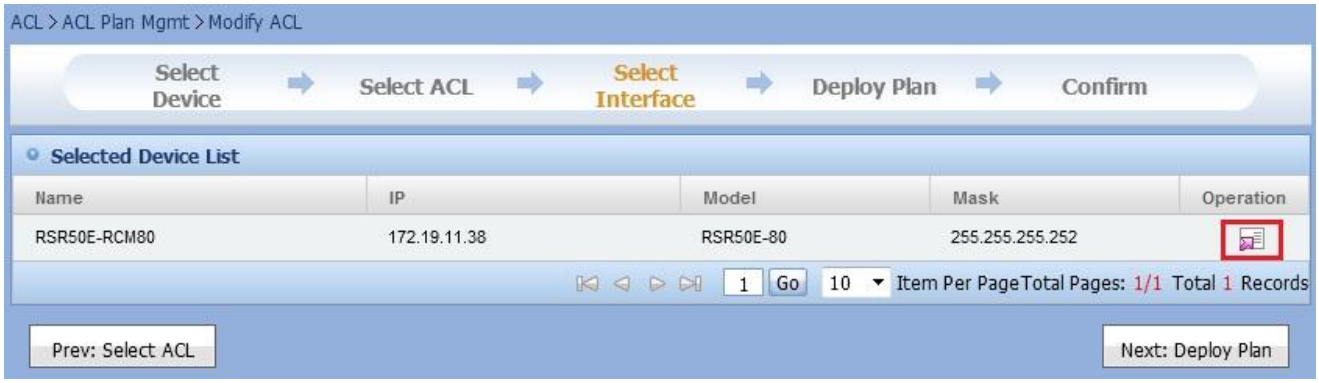


Figure 11.208. Select Interface

13) Show page **Interface Associated With The Device** to view the deployed interfaces:

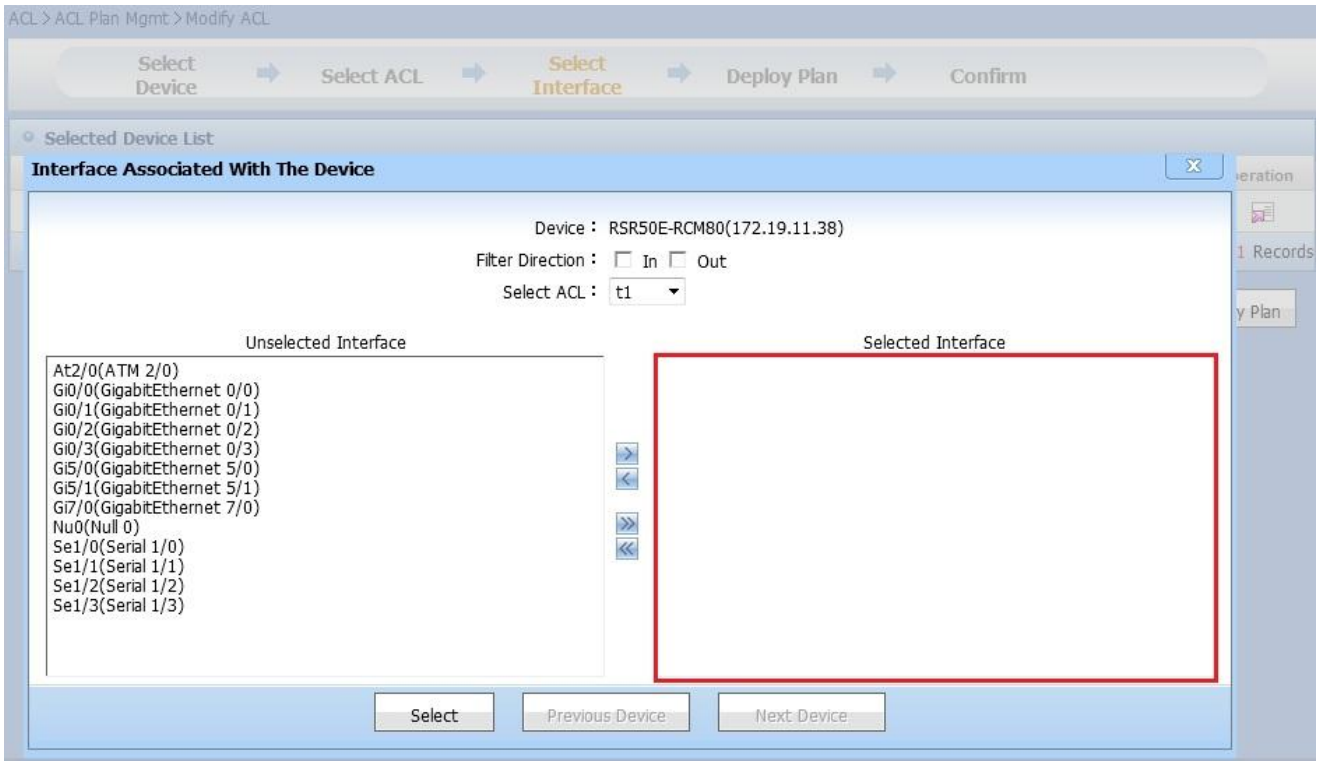


Figure 11.209. Interface Associated With The Device

14) Select **Filter direction**, **ACL** and interface in **Unselected Interface**, and double-click interface or click button **>**. The interface will be shown in format **Interface Name[Filter Direction]ACL name**. Click **Select** button to finish the selection.

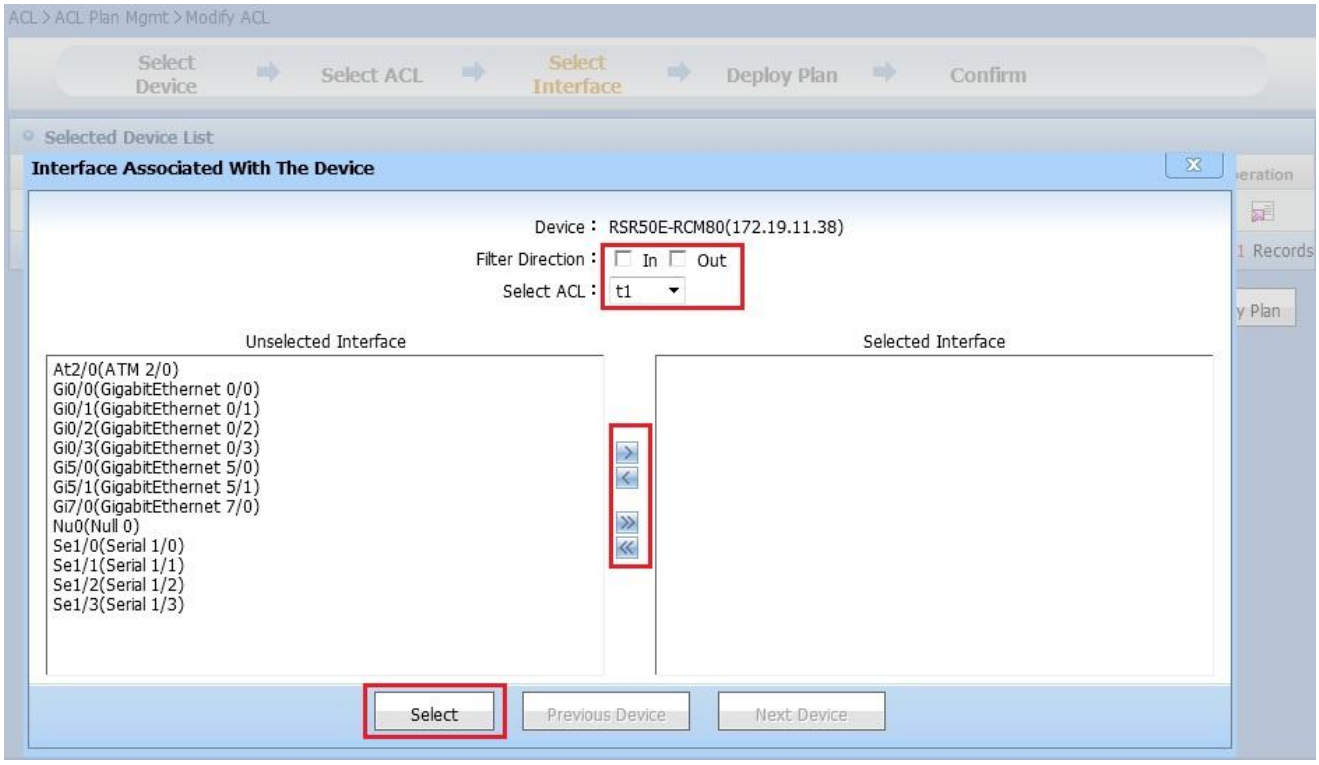


Figure 11.210. Interface Associated With The Device

15) Show **Selected Device List**, and device with interface selected or unselected will be identified with different icons. Click button **Previous: Select ACL** to return to page **Selected ACL List**.

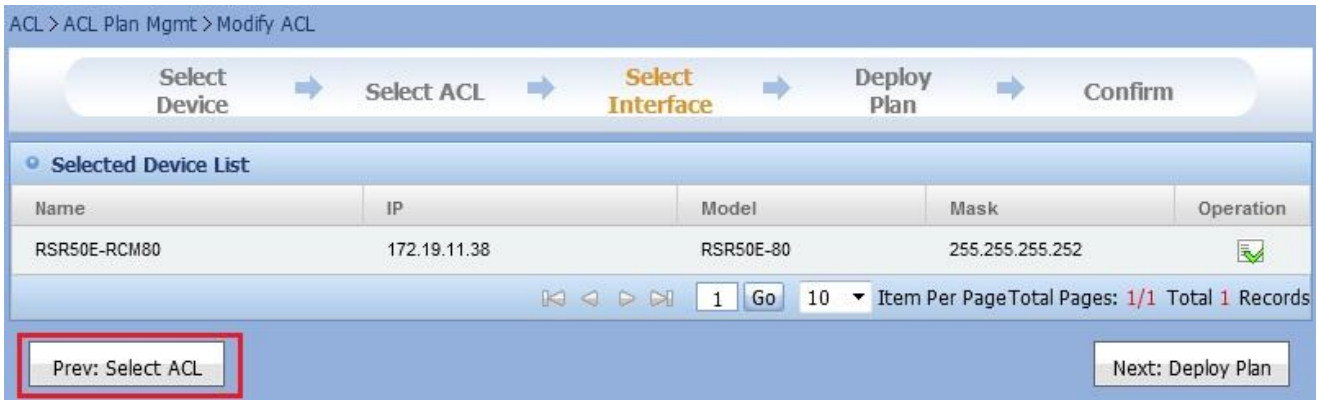


Figure 11.211. Previous: Select ACL

16) Show **Selected Device List**, and device with interface selected or unselected will be identified with different icons. Click button **Next: Deploy Plan**, as shown in the following figure:

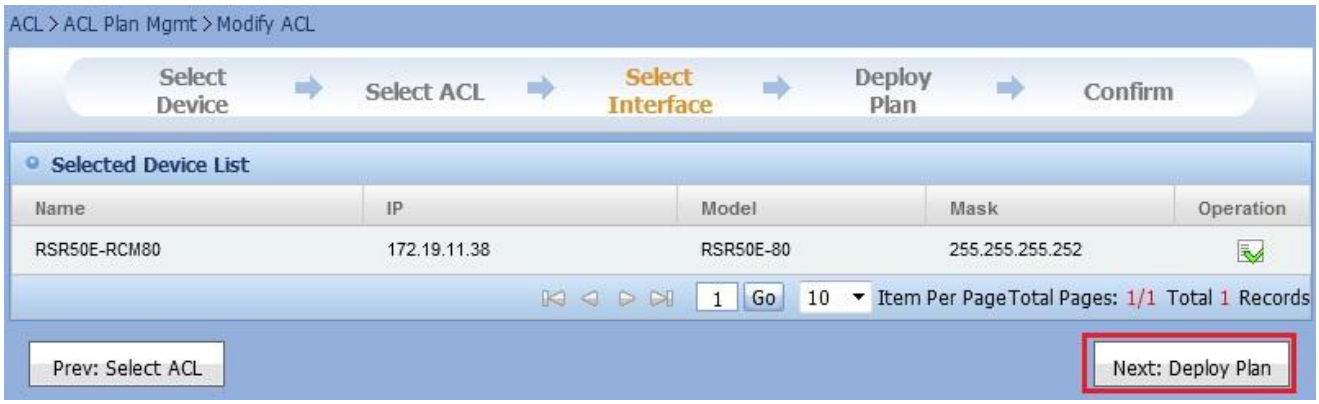


Figure 11.212. Next: Deploy Plan

17) Show **Deploy Plan**, and click button **Previous: Select Interface** to return to page **Select Interface**, as shown in following figure:

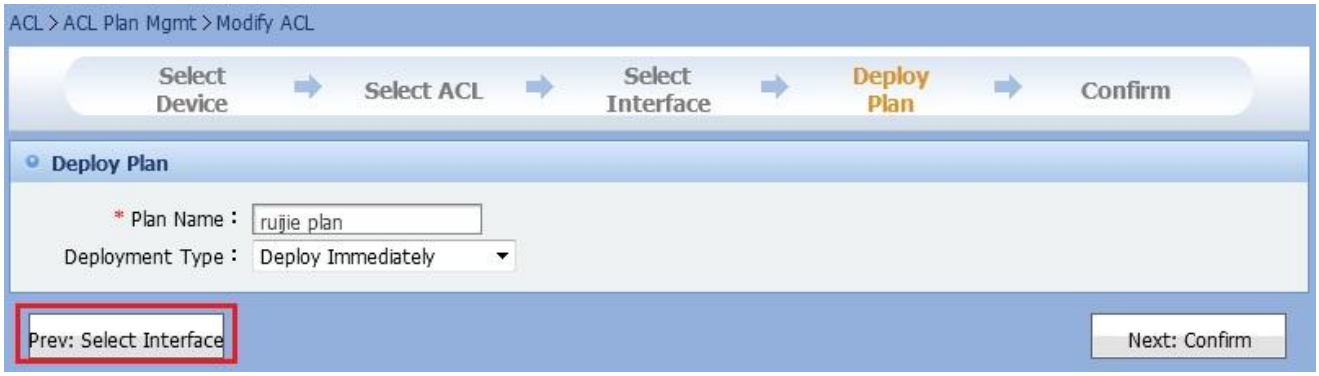


Figure 11.213. Previous: Select Interface

18) Show **Deploy Plan**, fill in the plan name and select deployment type, and click button **Next: Confirm**, as shown in following figure:

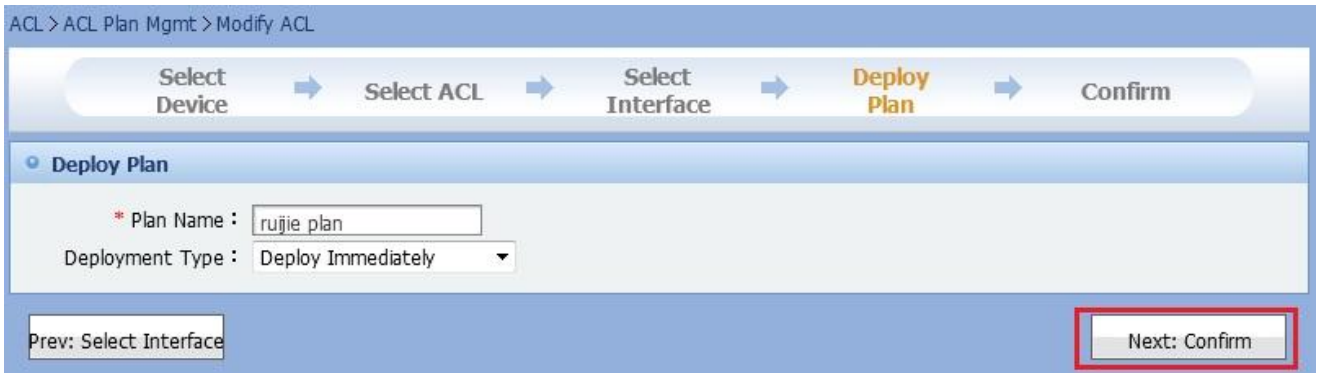


Figure 11.214. Next: Confirm

19) Show **Confirm** to click button **Previous: Deploy Plan** to return to page **Deploy Plan**, as shown in the following figure:

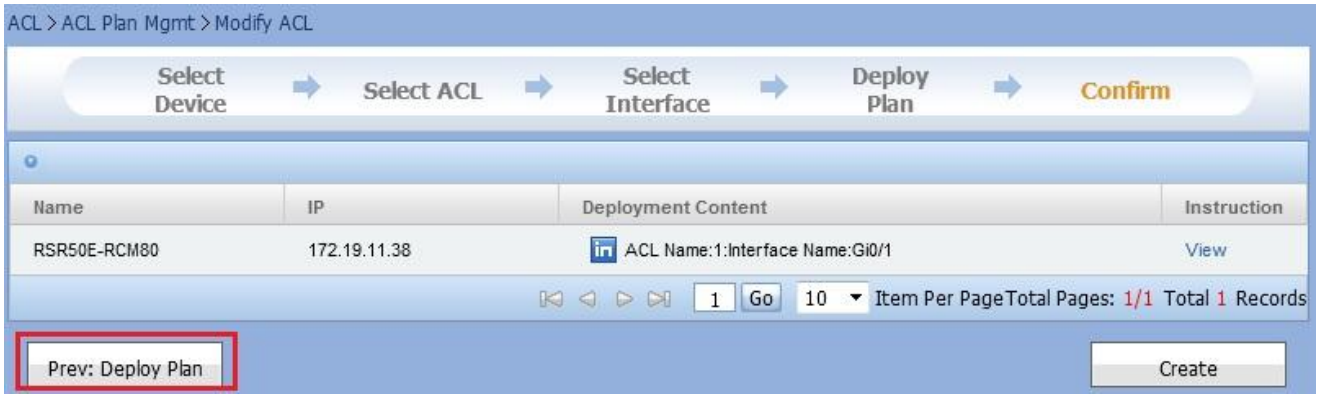


Figure 11.215. Back: Deploy Plan

20) Click button **View** to display a new page and the generated instruction, as shown in the following figure:

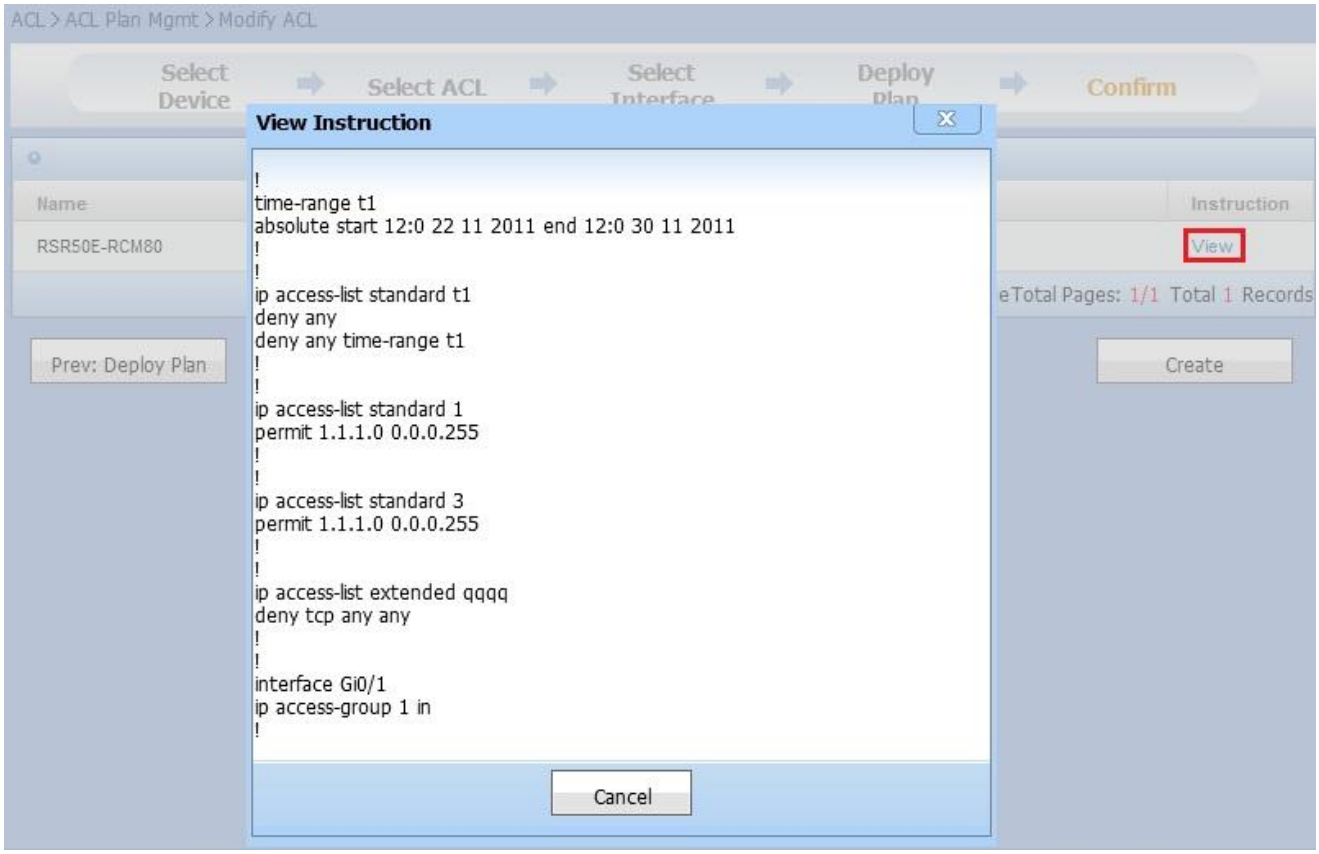


Figure 11.216. View Instruction

21) Click **Create** to generate a deployment plan and return to page **ACL Deployment Plan Management**, as shown in the following figure:

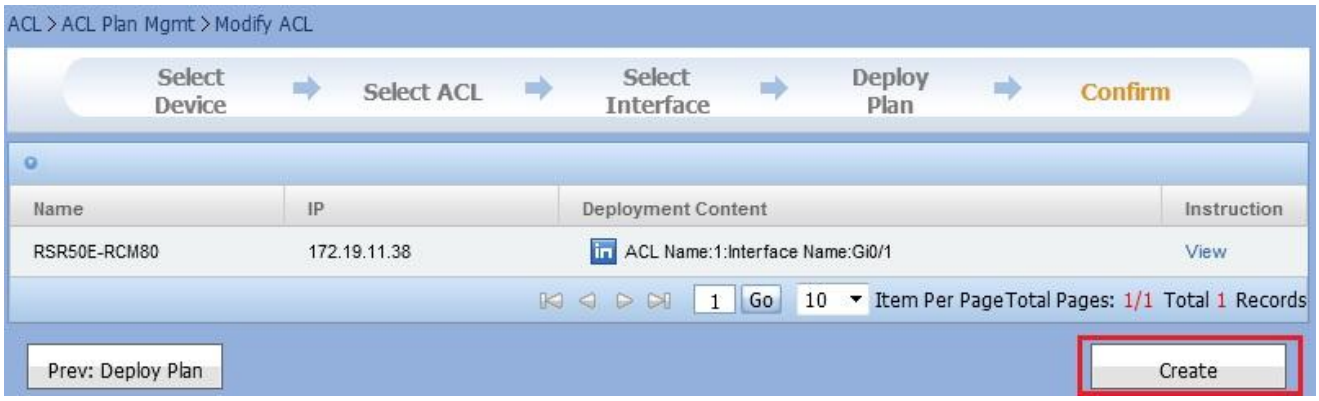


Figure 11.217. Start to create a deployment plan

On page **Select Device**, click **Add All** button to add all the devices to **Selected Device List**. When clicking **Add All** button, you do not need to select devices.

On page **Selected Device List**, click **Deselect** or **Deselect All** button to remove all the devices in **Selected Device List**. When clicking **Deselect All** button, you do not need to select devices.

On page **Selected ACL List**, click **Deselect** or **Deselect All** button to remove all the ACLs in **Selected ACL list**. When clicking **Deselect All** button, you do not need to select ACL.

On page **Selected ACL List**, click **Add All** button to add all the ACLs to **Selected ACL list**. When clicking **Add All** button, you do not need to select ACL.

In box **Unselected Interface** of page **Interface Associated With The Device**, double-click interface or click the **>** button to configure interface one by one or click the **>>** button to select interfaces in batch.

In box **Selected Interface** of page **Interface Associated With The Device**, double-click interface or click the **<** button to remove interface from the box or click the **<<** button to remove interfaces in batch.

On page **Interface Associated With The Device**, click button **Previous Device** to show information of **Selected Interface** for previous device.

On page **Interface Associated With The Device**, click button **Next Device** to show information of **Selected Interface** for next device.

Note

Plan created by system automatically cannot be modified.

If there is no record for the selected device list, you cannot click **Next: Select the ACL** button.

If there is no record for the selected ACL list, you cannot click **Deploy Plan** and **Previous: ACL Int Deployment** button.

If interface is not selected, you cannot click **Next: Deploy Plan** button.

After a deployment plan is added, you must click **Start Deployment Plan** to execute it.

11.5.4. Modify Interface Deployment Plan

Users can modify the interface deployment plan on page **ACL Deployment Plan Management**.

Operation Steps

1) On page **ACL Deployment Plan Management**, select the ACL Deploy Plan whose plan type is **Interface Application Deployment**, and click button **Modify**, as shown in following figure:

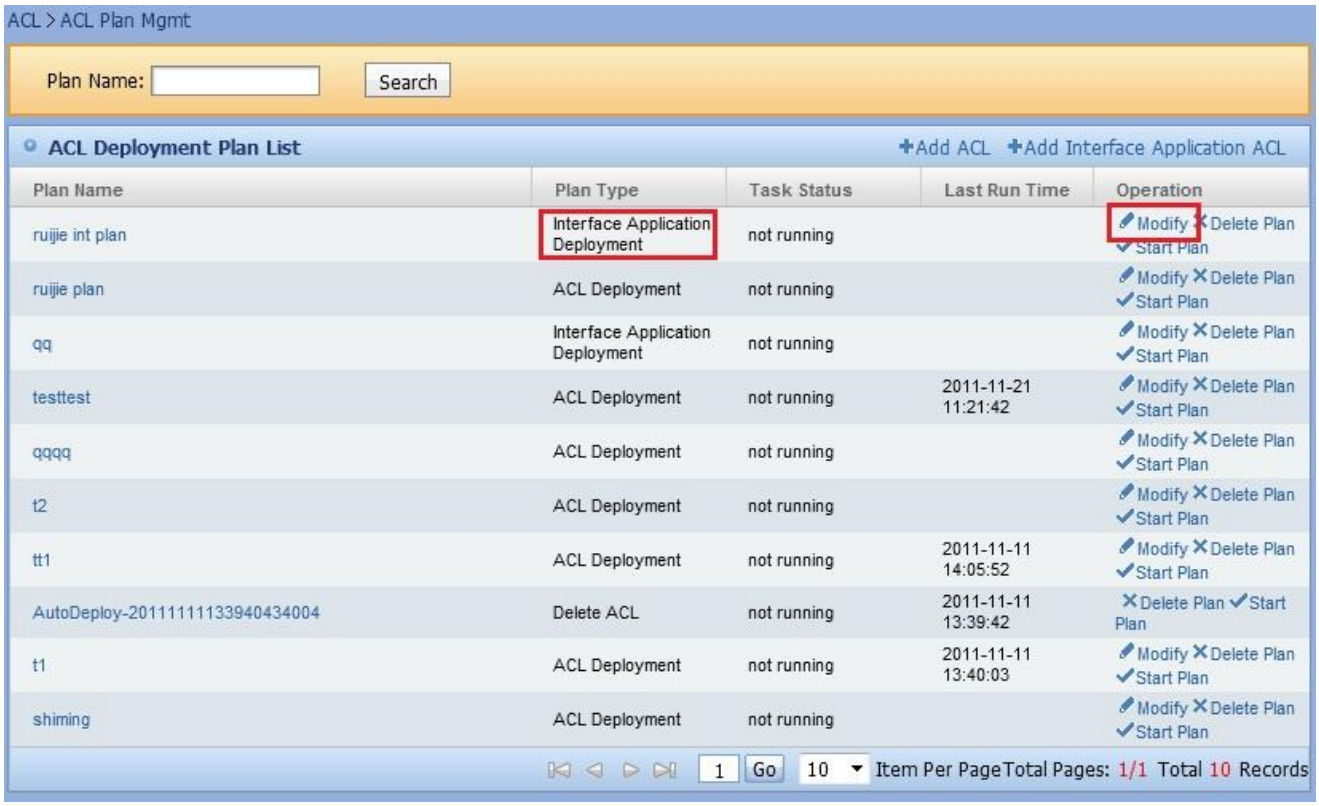


Figure 11.218. Go to Page **Modify Interface Deployment Plan**

2) Show page **Selected Device List**, as shown in following figure:

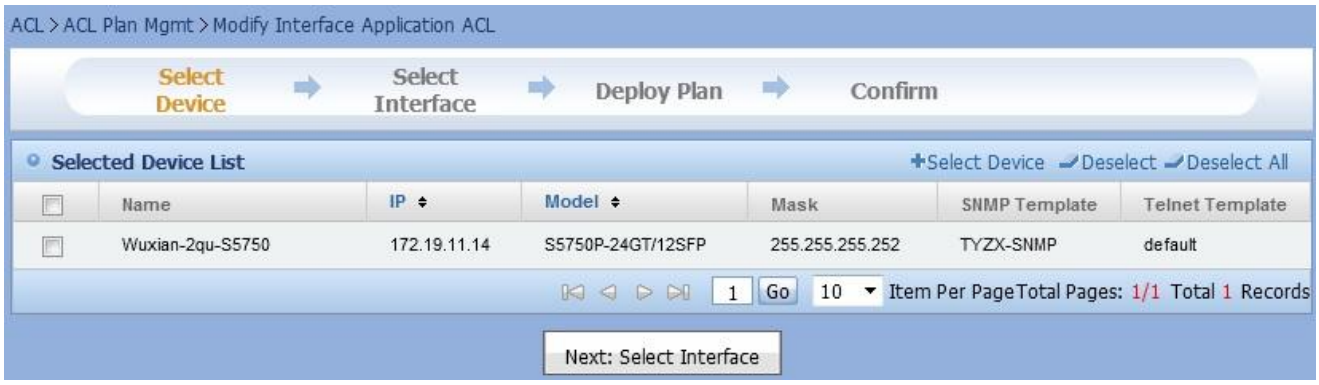


Figure 11.219. Show page **Selected Device List**

3) Click **Select Device** button to display page **Select Device**, as shown in following figure:

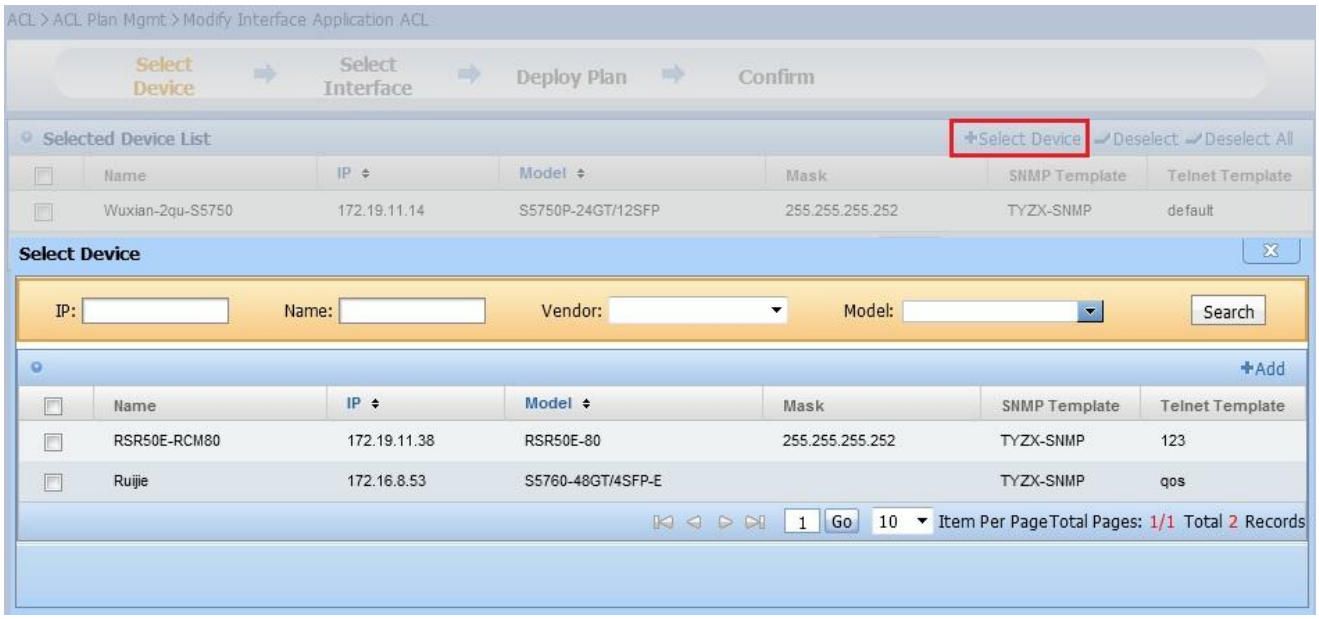


Figure 11.220. Select Device

4) After selecting device, click the **Add** button, as shown in following figure:

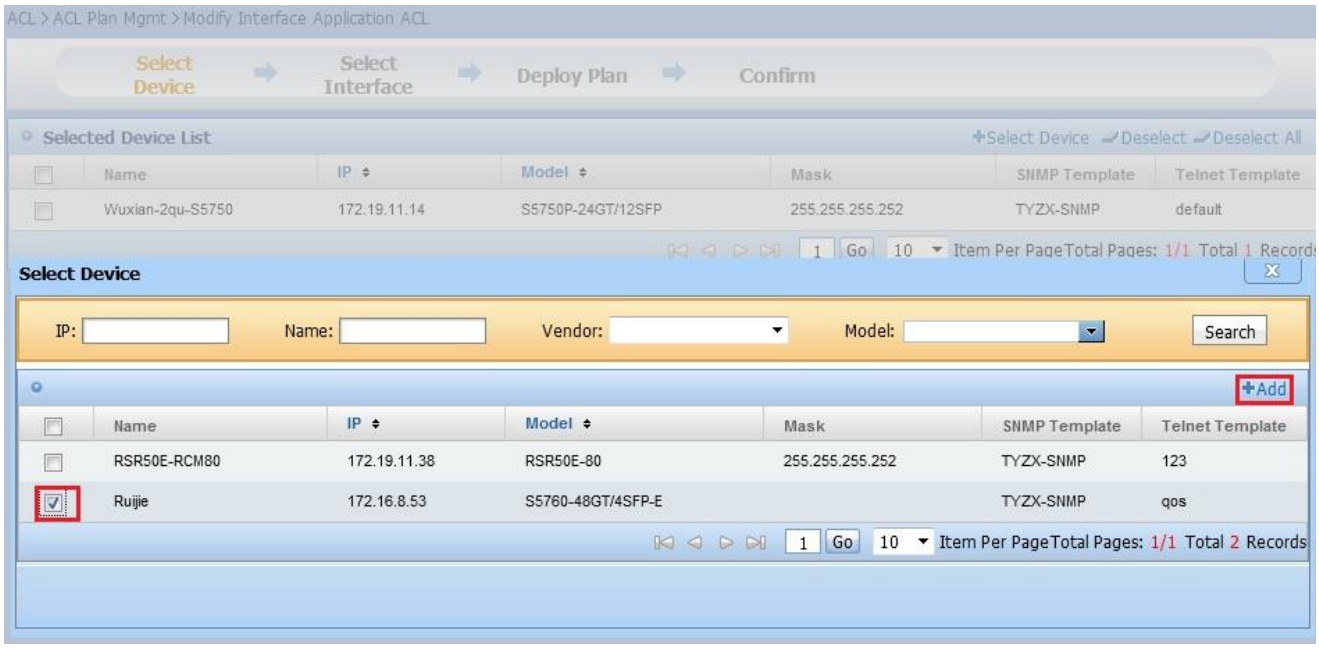


Figure 11.221. Add Device

5) Show page **Selected Device list**, and click button **Next: Select Interface**, as shown in following figure:

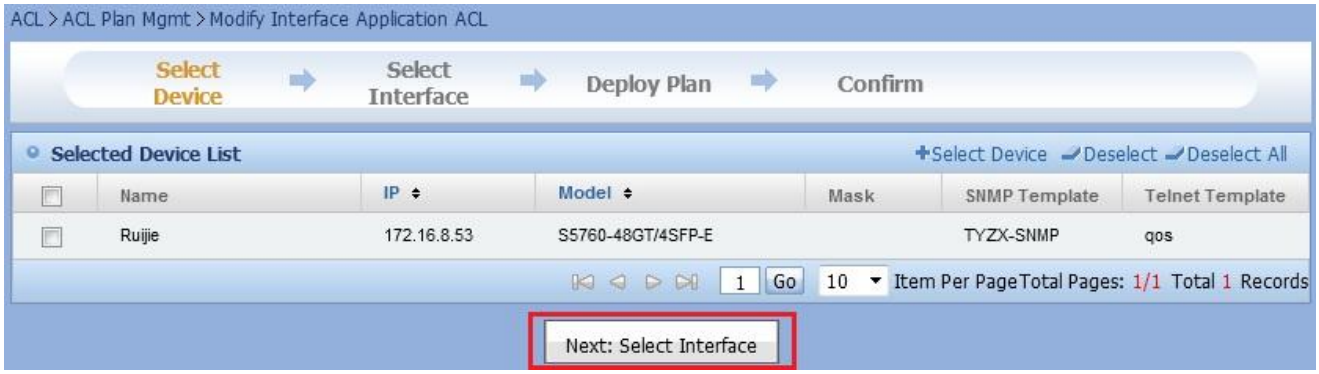


Figure 11.222. Next: Select Interface

6) Go to page **Select Interface**, show **Selected Device List**, and click button in operation bar of **Selected Device List** to enter page **Interface Associated With The Device**, as shown in following figure:

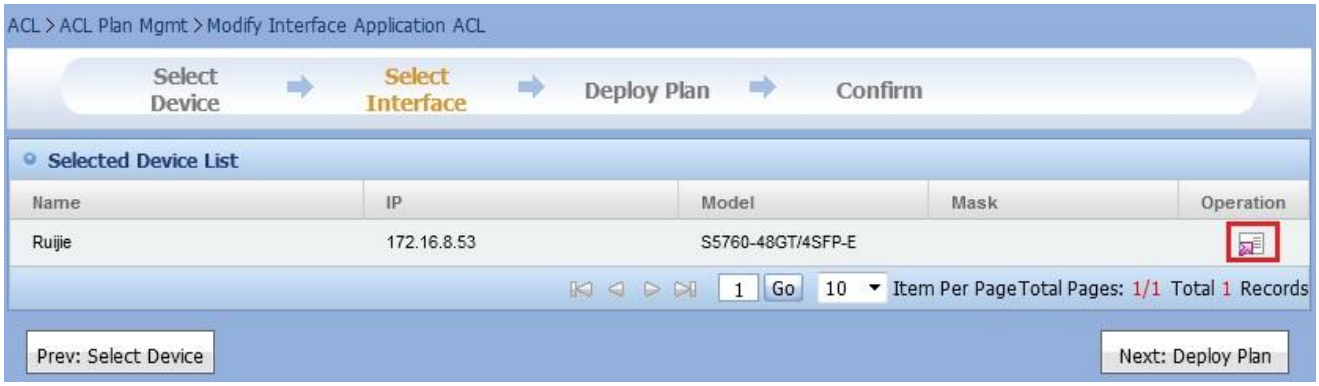


Figure 11.223. Select Interface

7) Show page **Interface Associated With The Device**:

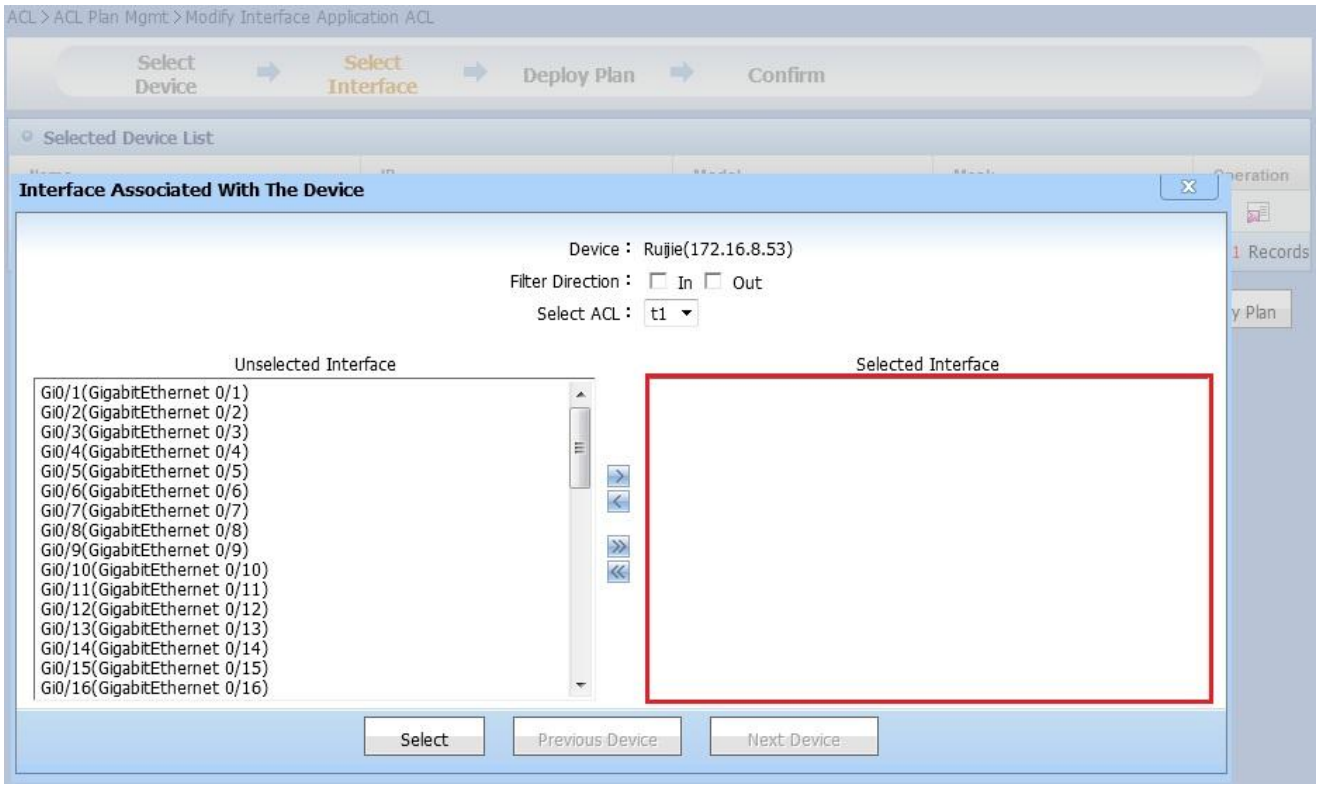


Figure 11.224. Interface Associated With The Device

8) Select **Filter Direction**, **ACL** and interface in **Unselected Interface**, and double-click interface or click button **>**. The interface will be shown in format **Interface Name[Filter Direction]ACL name**.

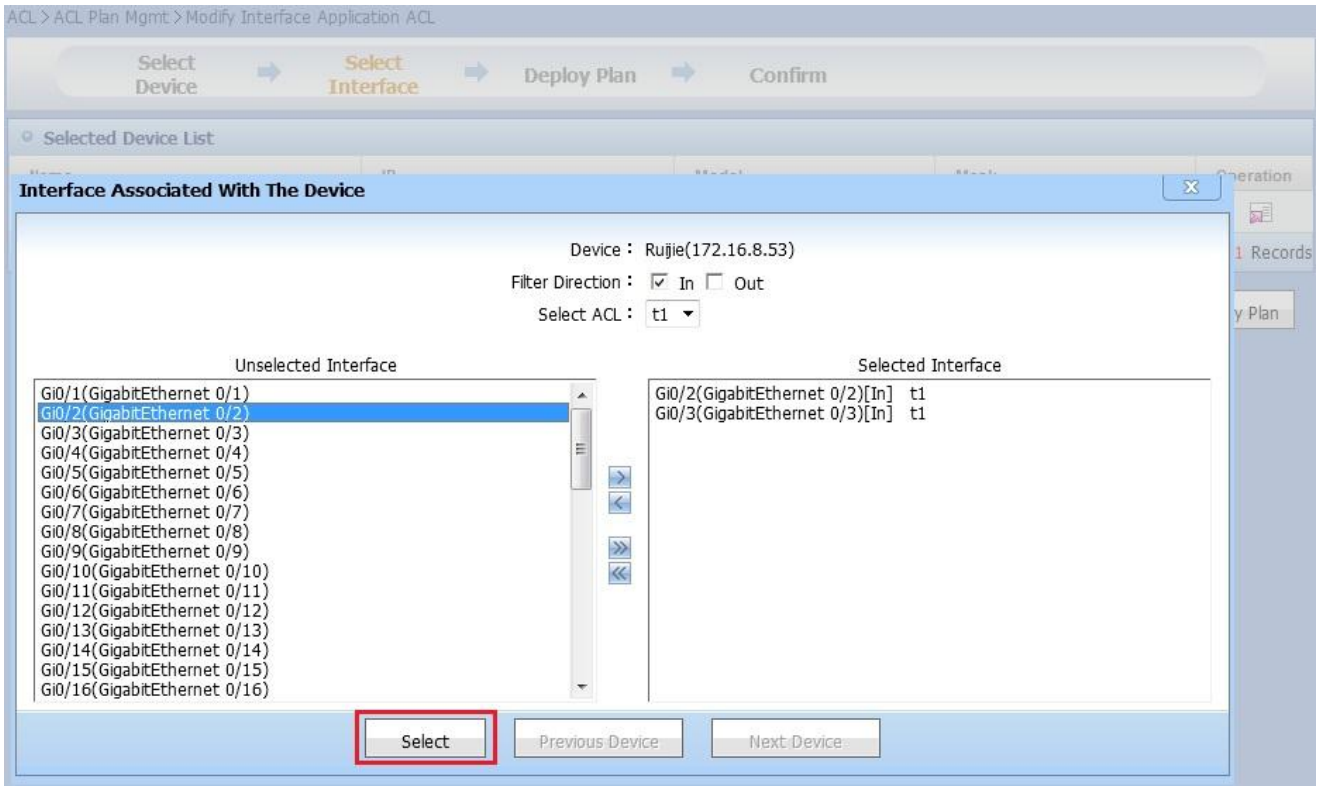


Figure 11.225. Interface Associated With The Device

9) Show **Selected Device List**, and the device with interface selected or unselected will be identified with different icons. Click button **Previous: Select Device** to return to page **Selected ACL List**, as shown in following figure:

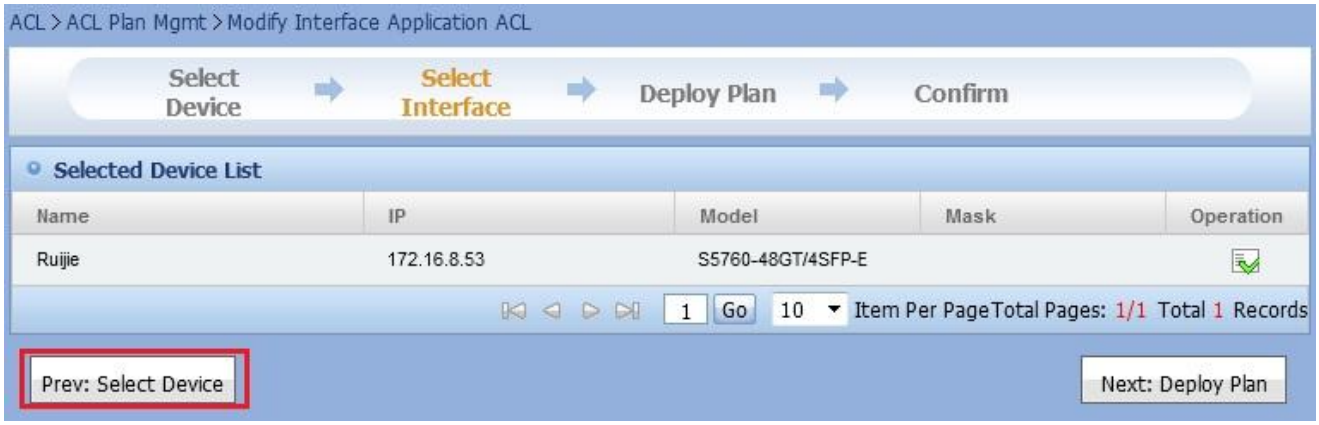


Figure 11.226. Previous: Select Device

10) Show **Selected Device List**, and the device with interface selected or unselected will be identified with different icons. Click button **Next: Deploy Plan**, as shown in following figure:

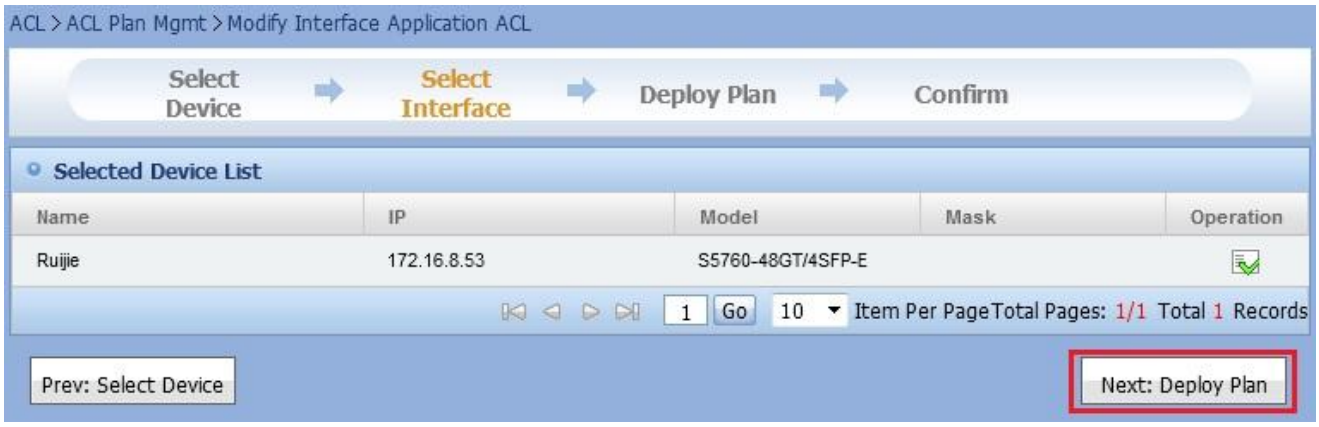


Figure 11.227. Next: Deploy Plan

11) Show **Deployment Plan**, and click button **Previous: Select Interface** to return to page **Select Interface**, as shown in following figure:

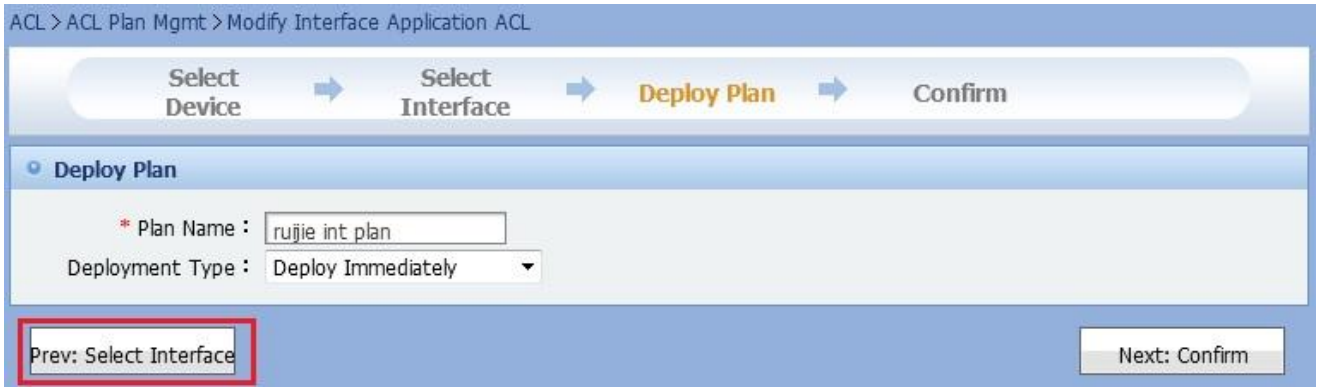


Figure 11.228. Previous: Select Interface

12) Show **Deploy Plan**, fill in the plan name and select deployment type, and click button **Next: Confirm**, as shown in following figure:

Figure 11.229. Next: Confirm

13) Show **Confirm**, and click button **Previous: Deploy Plan** to return to page **Deploy Plan**, as shown in following figure:

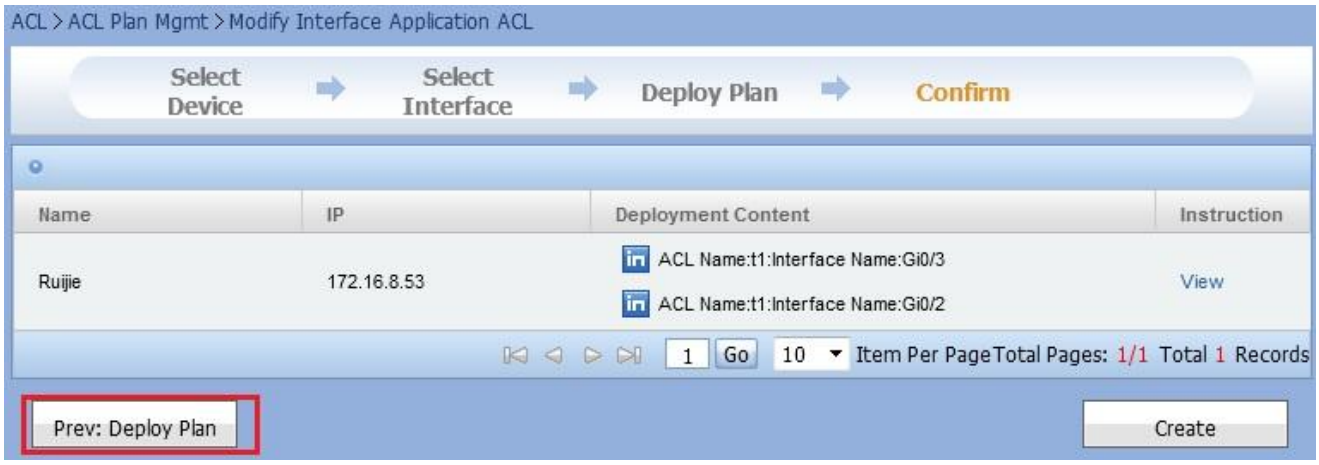


Figure 11.230. Previous: Deploy Plan

14) Click button **View** to display a new page for the generated instruction, as shown in following figure:

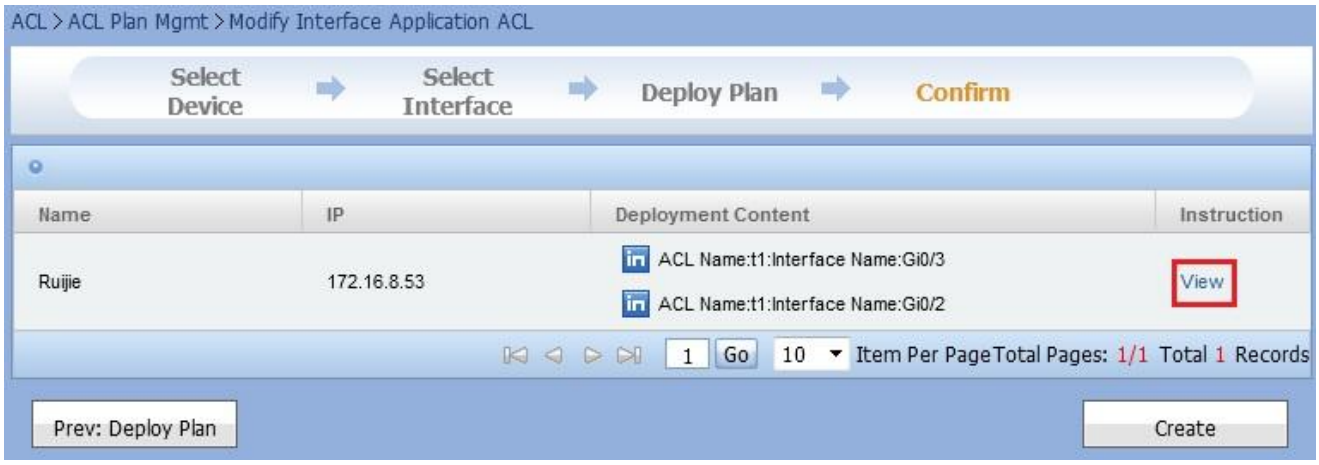


Figure 11.231. View Instruction

15) Click **Create** to generate a deployment plan and return to page **ACL Deployment Plan Management**, as shown in following figure:

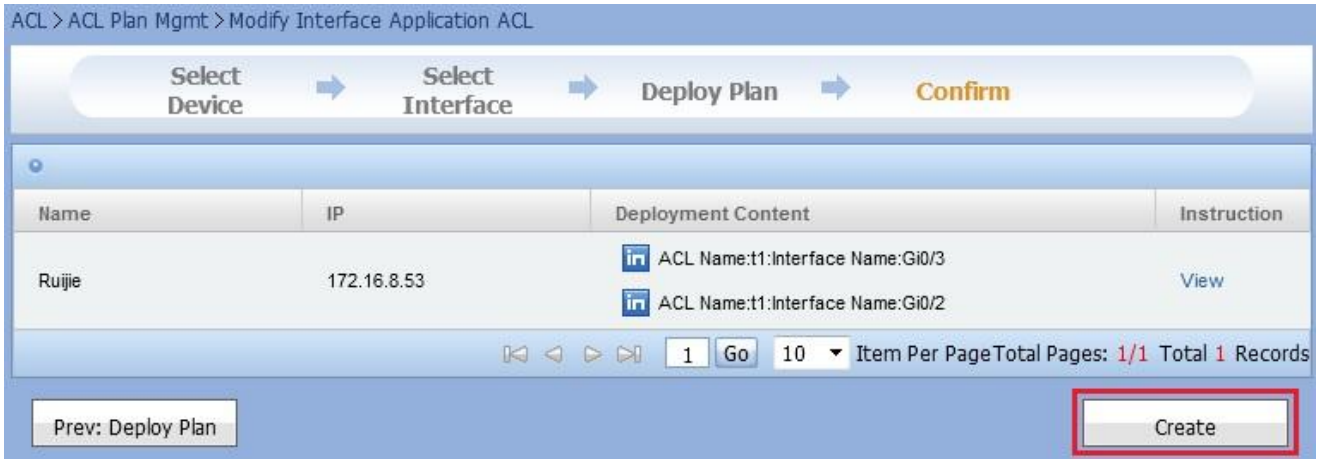


Figure 11.232. Start to update the interface deployment plan

On page **Select Device**, click **Add All** button to add all the devices to **Selected Device List**. When clicking **Add All** button, you do not need to select devices.

On page **Selected Device List**, click **Deselect** or **Deselect All** button to remove all the devices in **Selected Device List**. When clicking **Deselect All** button, you do not need to select devices.

In box **Unselected Interface** of page **Interface Associated With The Device**, and double-click interface or click the **>** button to configure interface one by one or click the **>>** button to select interfaces in batch.

In box **Selected Interface** of page **Interface Associated With The Device**, and double-click interface or click the **<** button to remove interface from the box or click the **<<** button to remove interfaces in batch.

On page **Interface Associated With The Device**, and click button **Previous Device** to show information of **Selected Interface** for previous device.

On page **Interface Associated With The Device**, and click button **Next Device** to show information of **Selected Interface** for next device.

Note

Plan created by system automatically cannot be modified.

If there is no record of the selected device list, you cannot click **Next: Select ACL** button.

If interface is not selected, you cannot click **Next: Deploy Plan** button.

After a deployment plan is added, you must click **Start Deployment Plan** to execute it.

11.5.5. Stop Deployment Plan

Deployment Plan can be stopped on page **ACL Deployment Plan Management**.

Operation Steps

On page **ACL Deployment Plan Management**, click button **Stop Plan** in plan list to stop corresponding ACL deployment plan immediately, as shown in following figure:

Figure 11.233. Stop Deployment Plan

Note

Stop Plan: Running plan can be stopped.

11.5.6. Start Deployment Plan

Deployment Plan can be started on page **ACL Deployment Plan Management**.

Operation Steps

On page **ACL Deployment Plan Management**, click button **Start Plan** in plan list to start corresponding ACL deployment plan immediately, as shown in following figure:

Figure 11.234. Start Deployment Plan

Note

After plan is started, the system displays the prompt message. If the background has been started, **operation successful, waiting for plan being started by background service** is prompted; if the background does not start, **the background service is not started** is prompted.

11.5.7. View Deployment Plan

Plan parameters, running logs and selected device list can be viewed on page Detail Information of ACL Deployment Plan.

Operation Steps

1) On page **ACL Deployment Plan Management**, click the link **Plan Name** to enter page **Detail Information of ACL Deployment Plan**, as shown in following figure:

Figure 11.235. Go to page **Detail Information of ACL Deployment Plan**

2) View plan parameters, running logs and selected device list, as shown in following figure:

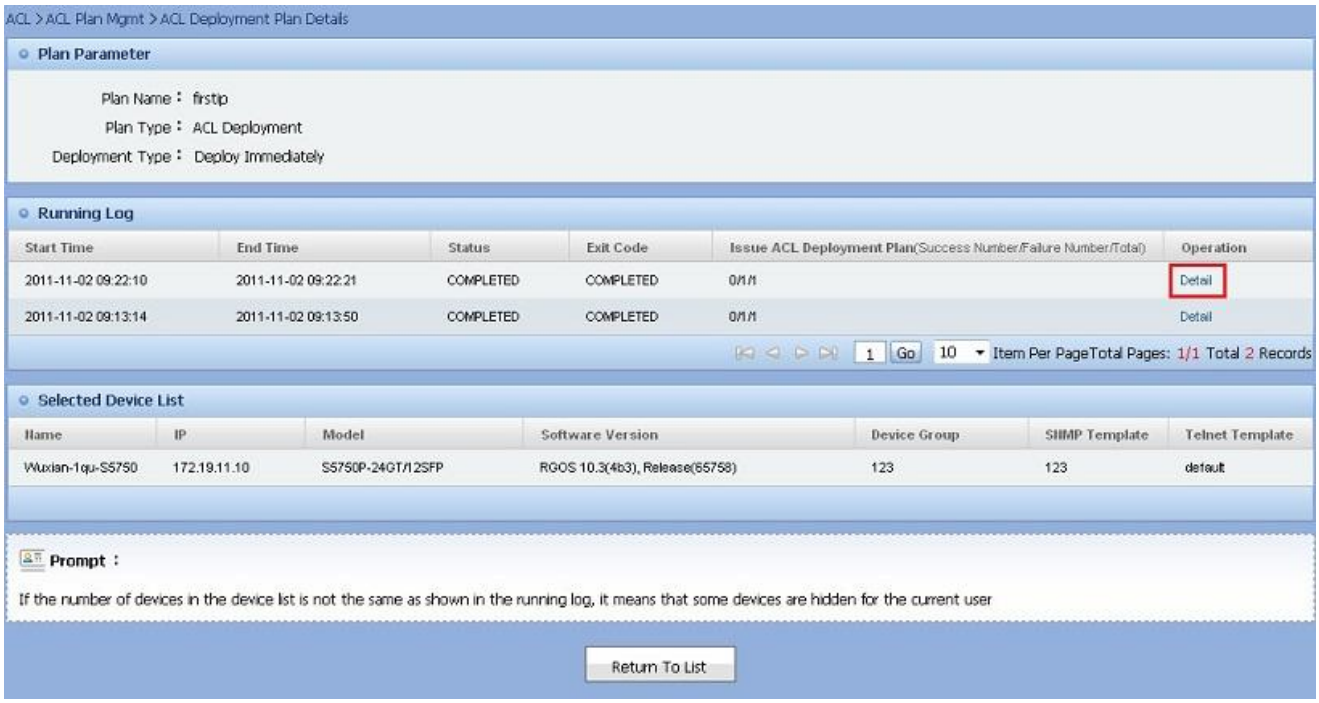


Figure 11.236. Detail Information of ACL Deployment Plan

11.5.8. View Detail Log of Deployment Plan

From page **ACL Deployment Plan Management**, you can enter page **Detail Information of ACL Deployment Plan** to view corresponding plan parameters, running logs and selected device list.

Operation Steps

1) On page **ACL Deployment Plan Management**, click the link **Plan Name** to enter page **Detail Information of ACL Deployment Plan**, as shown in following figure:

Figure 11.237. Go to page **Detail Information of ACL Deployment Plan**

2) Show plan parameters, running logs and selected device list. Click the link **Detail** to enter page **Running Log Detail**, as shown in following figure:

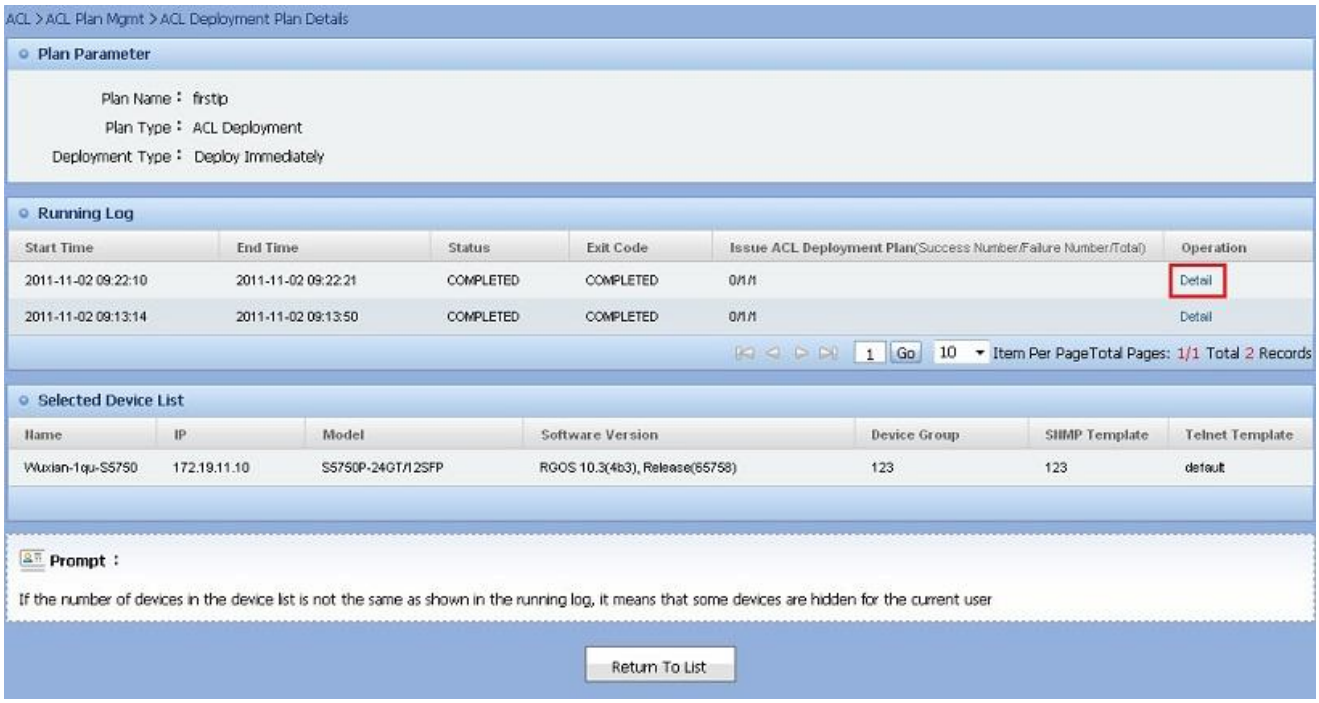


Figure 11.238. Go to page **Running Log Detail**

3) List basic information of **Running Log Detail**, as shown in following figure:

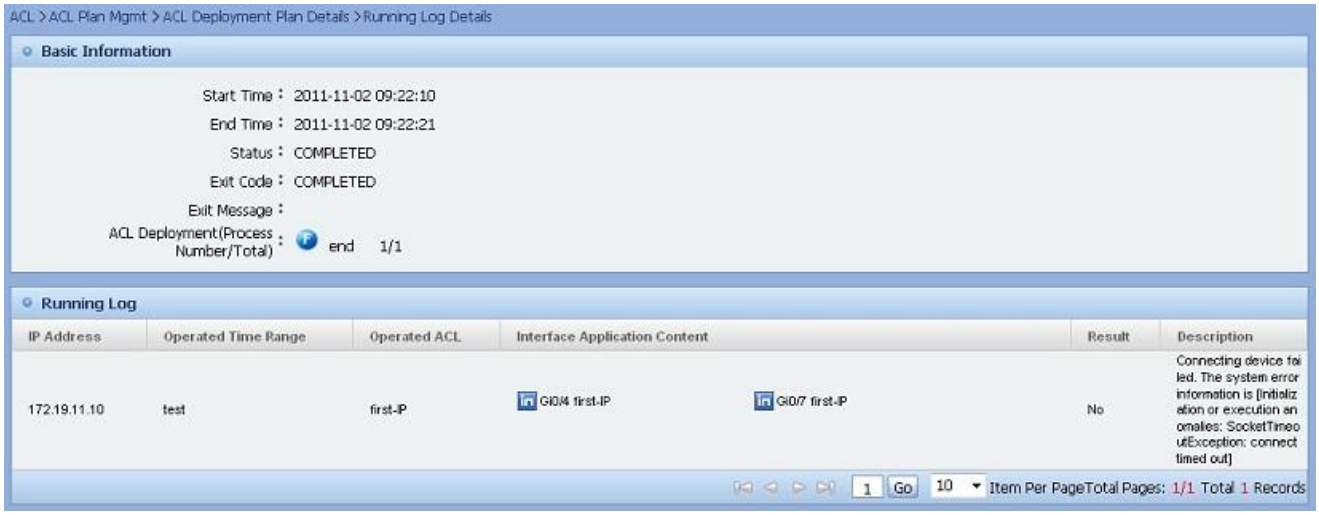


Figure 11.239. Running Log Detail

11.5.9. Add Deployment Plan

Deployment Plan can be added on page **ACL Deployment Plan Management**

Operation Steps

1) On page **ACL Deployment Plan Management**, click button **Add ACL**, as shown in following figure:

Figure 11.240. Go to page **Add ACL Deployment Plan**

2) View page **Selected Device List**, as shown in following figure:

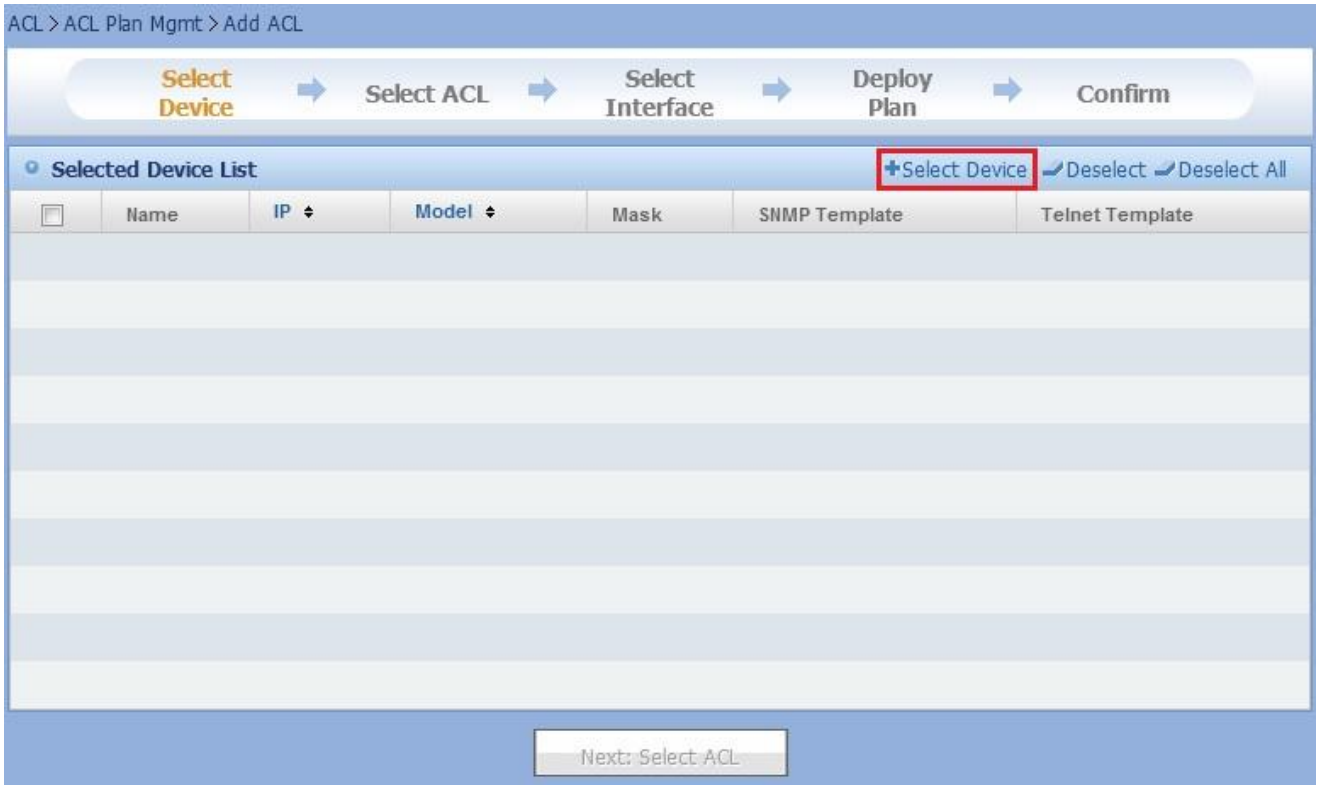


Figure 11.241. View page **Selected Device list**

3) Click **Select Device** button to display page **Select Device**, as shown in following figure:

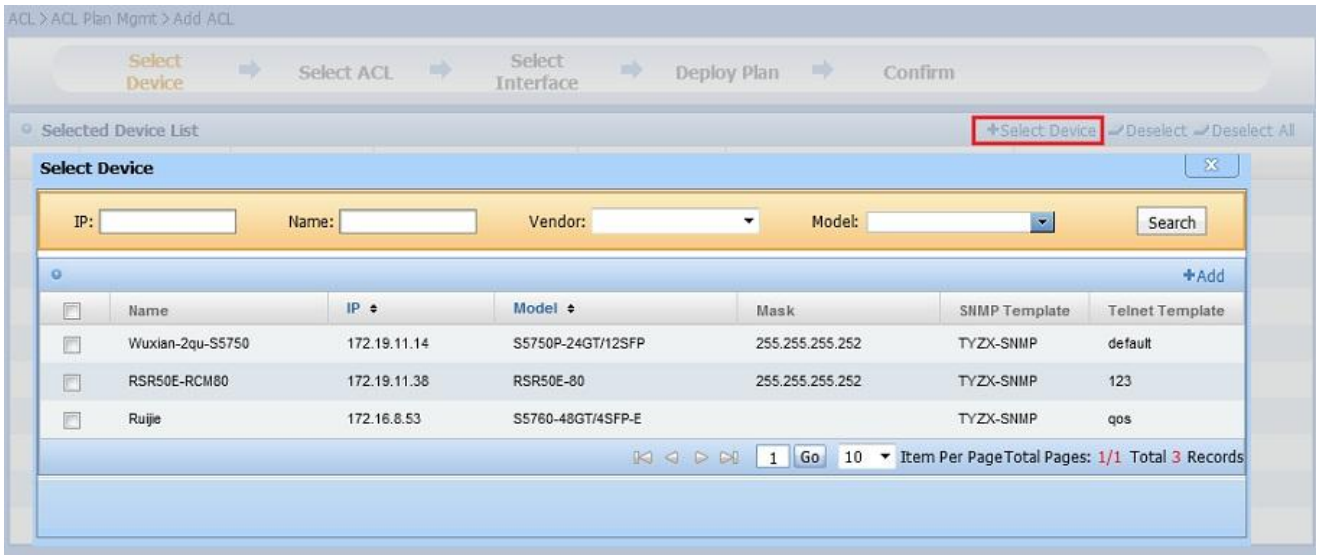


Figure 11.242. Select Device

4) After selecting device, click the **Add** button, as shown in following figure:

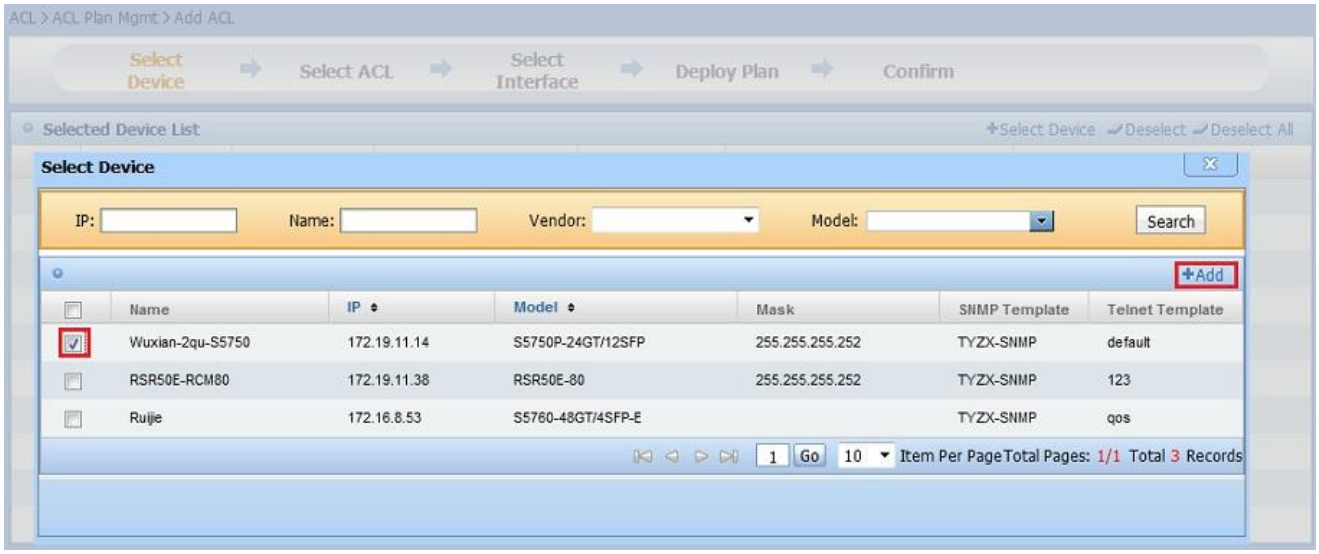


Figure 11.243. Add Device

5) View page **Selected Device List**, and click button **Next: Select ACL**, as shown in following figure:

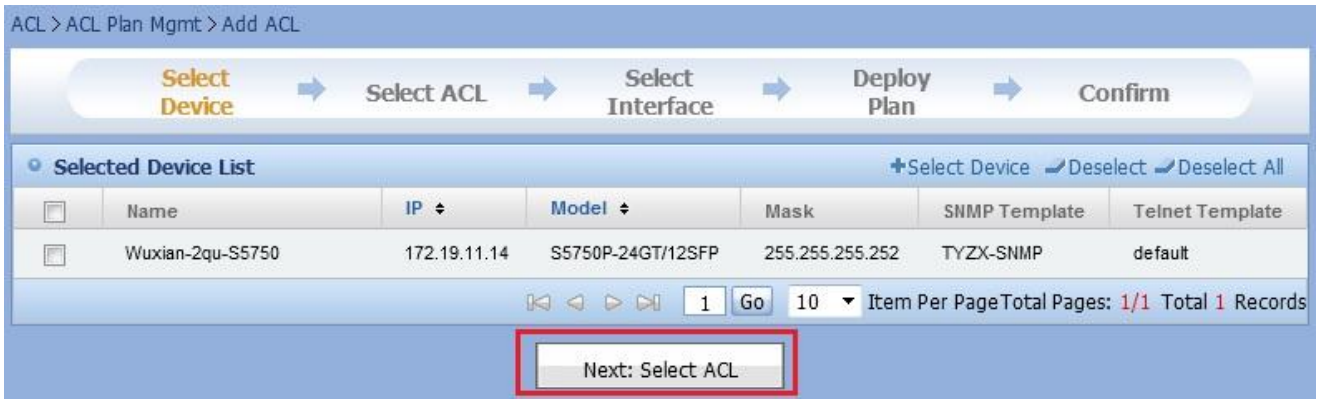


Figure 11.244. Next: Select ACL

6) View page **Selected ACL List**, as shown in following figure:

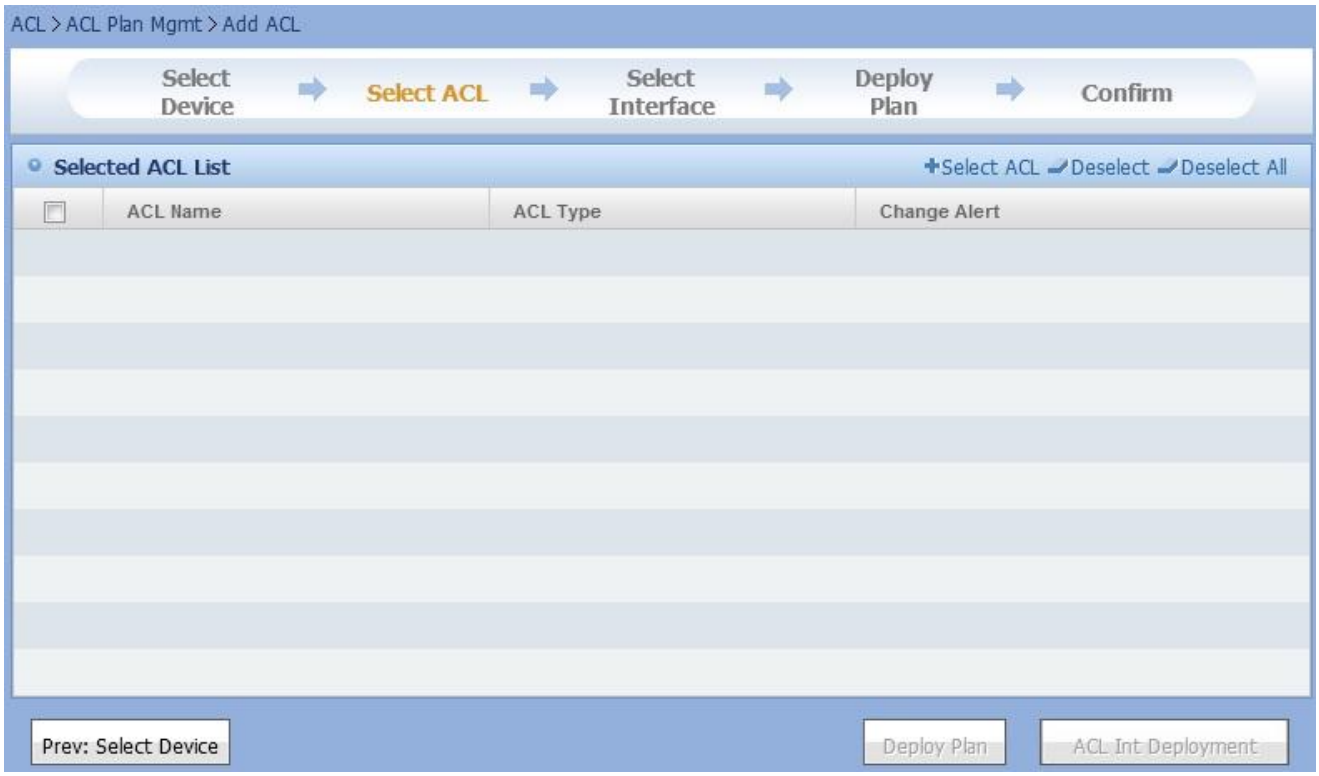


Figure 11.245. Select ACL

7) Click **Select ACL** button to enter page **Available ACL List**, as shown in following figure:

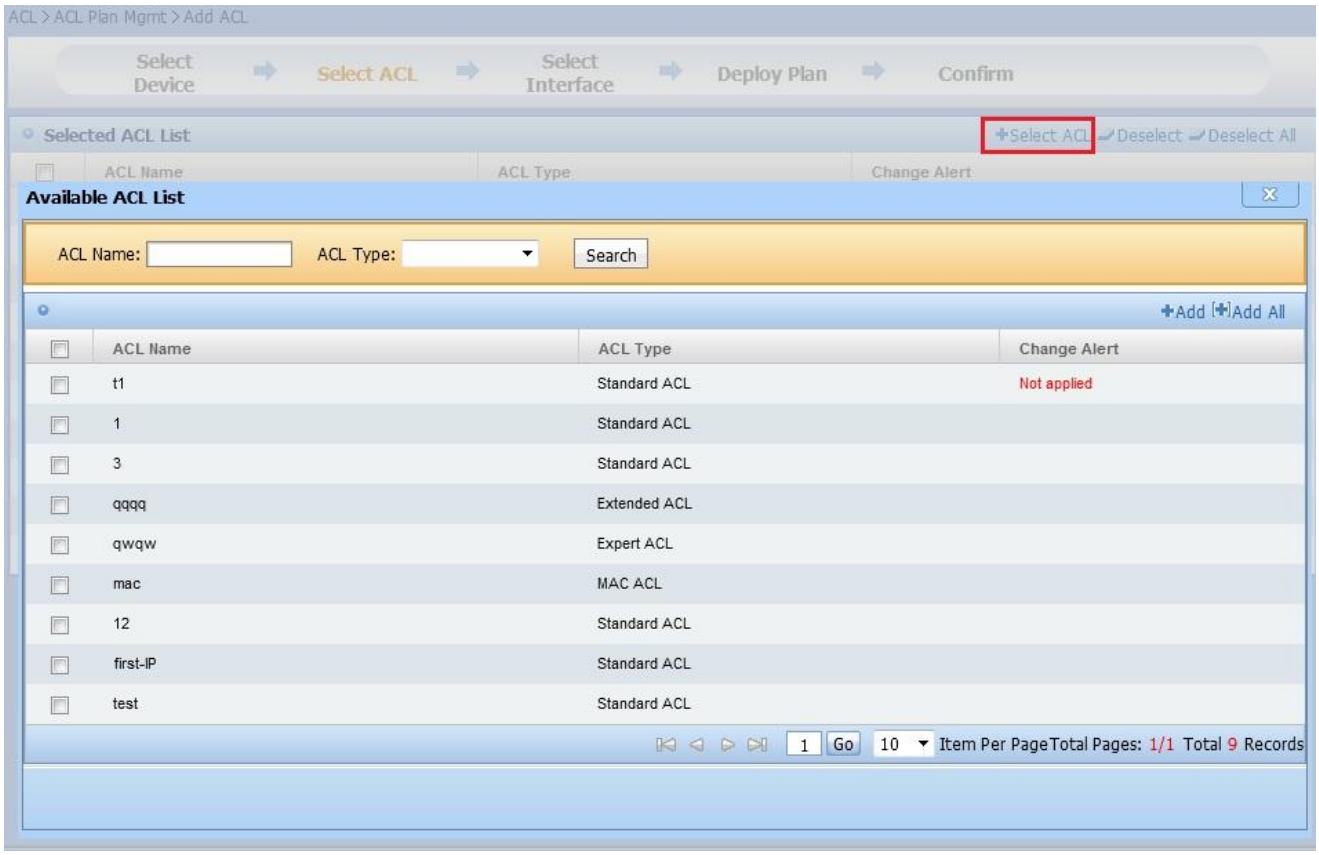


Figure 11.246. Select ACL

8) After selecting ACL, click the **Add** button, as shown in following figure:

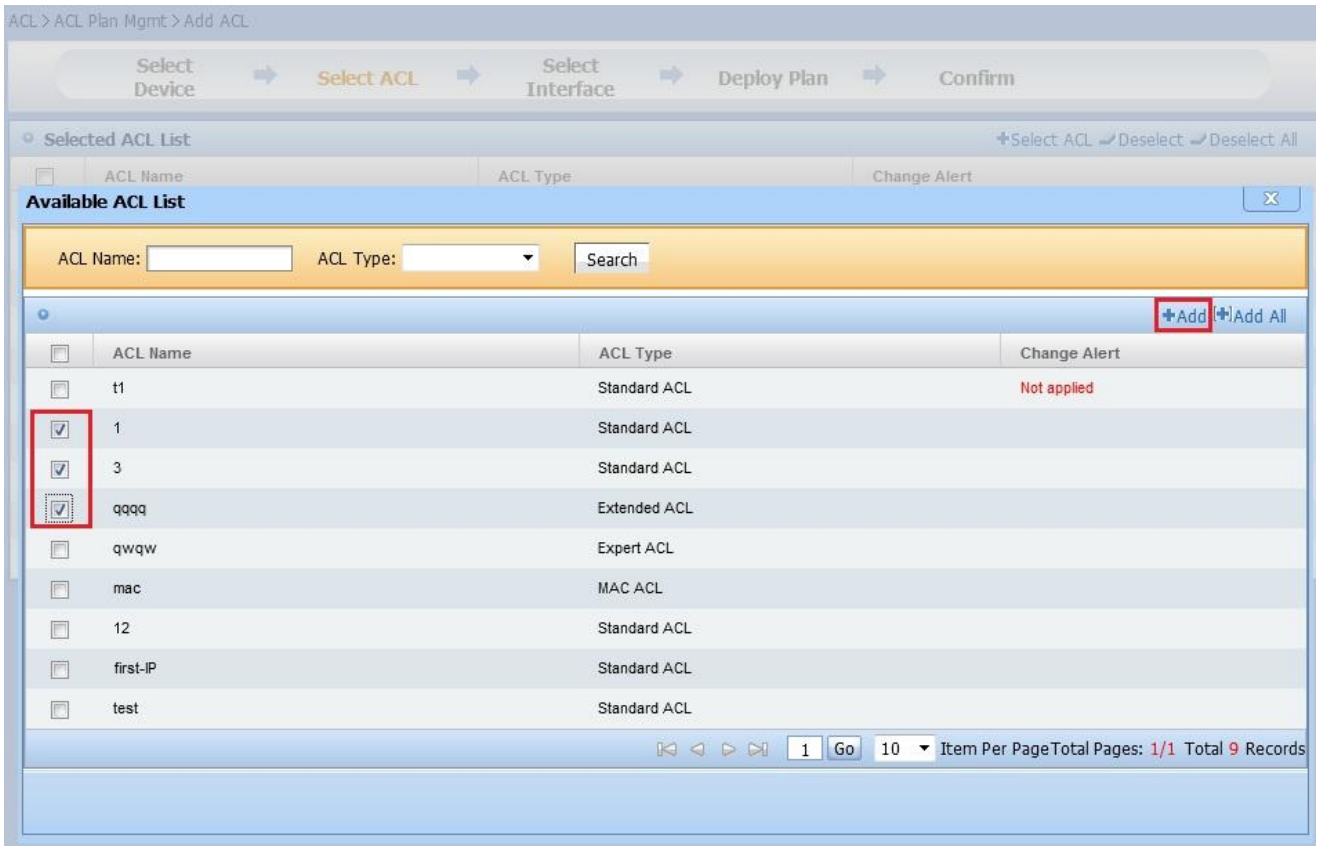


Figure 11.247. Add ACL

9) View page **Selected ACL List**, and click button **Previous: Select Device** to return to page **Selected Device List**, as shown in following figure:

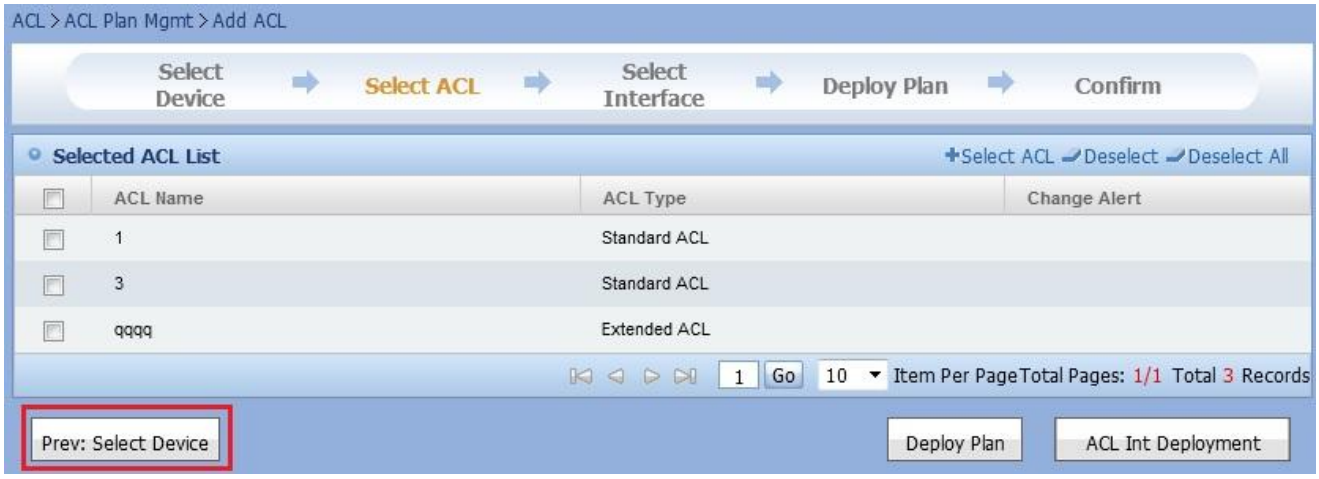


Figure 11.248. Previous: Select Device

10) View page **Selected ACL List**, and click button **Deploy Plan** to enter page **Deploy Plan**, as shown in following figure:

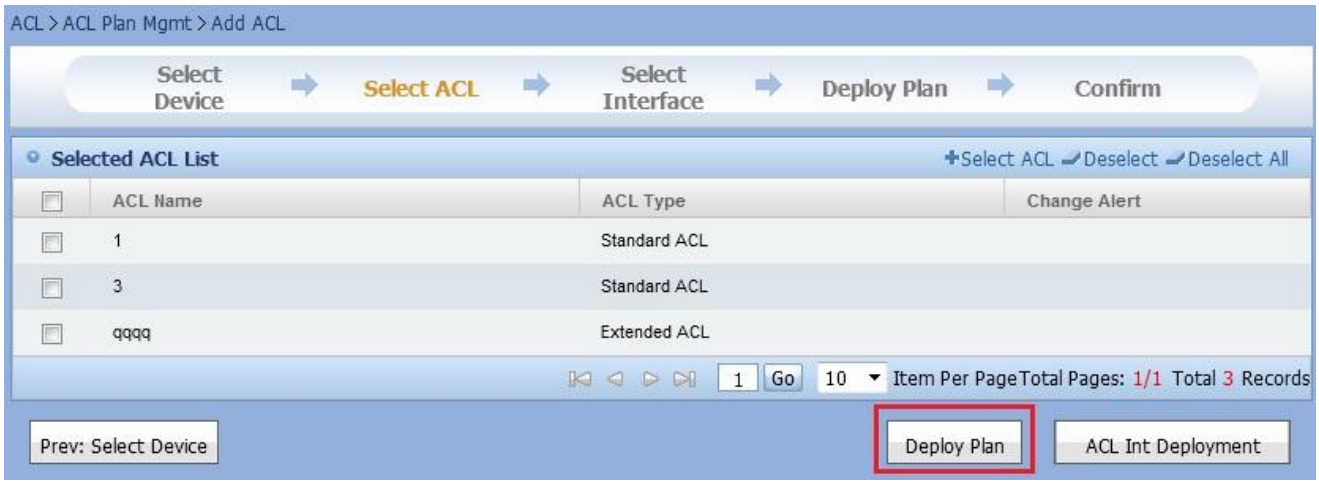


Figure 11.249. Deploy Plan

11) View page **Selected ACL List**, and click button **ACL Int Deployment** to enter page **Select Interface**, as shown in following figure:

Figure 11.250. Deploy ACL on Interface

12) View page **Select Interface**, click **Configure Interface** icon under **Operation** column to enter page **Select Interface**, as shown in following figure:

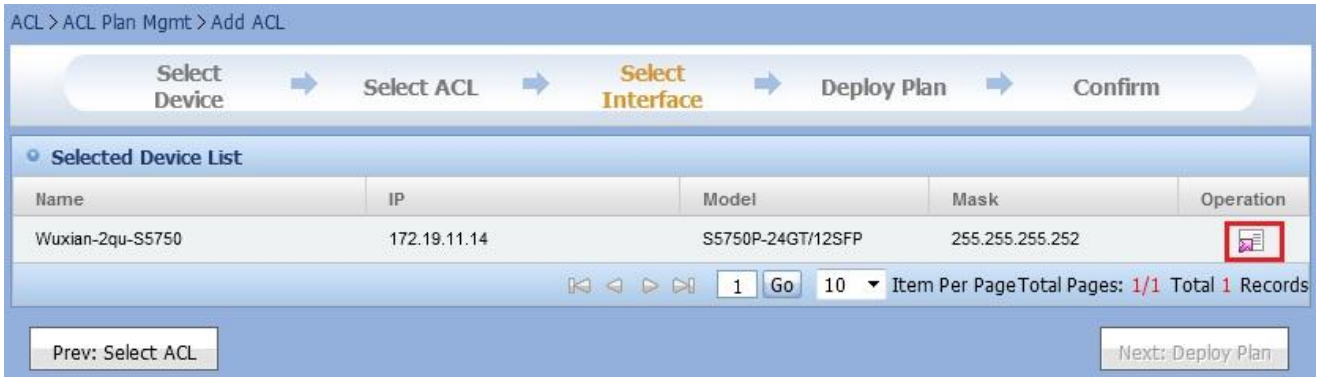


Figure 11.251. Select Interface

13) Enter page **Interface Associated With The Device** to view deployed interfaces:

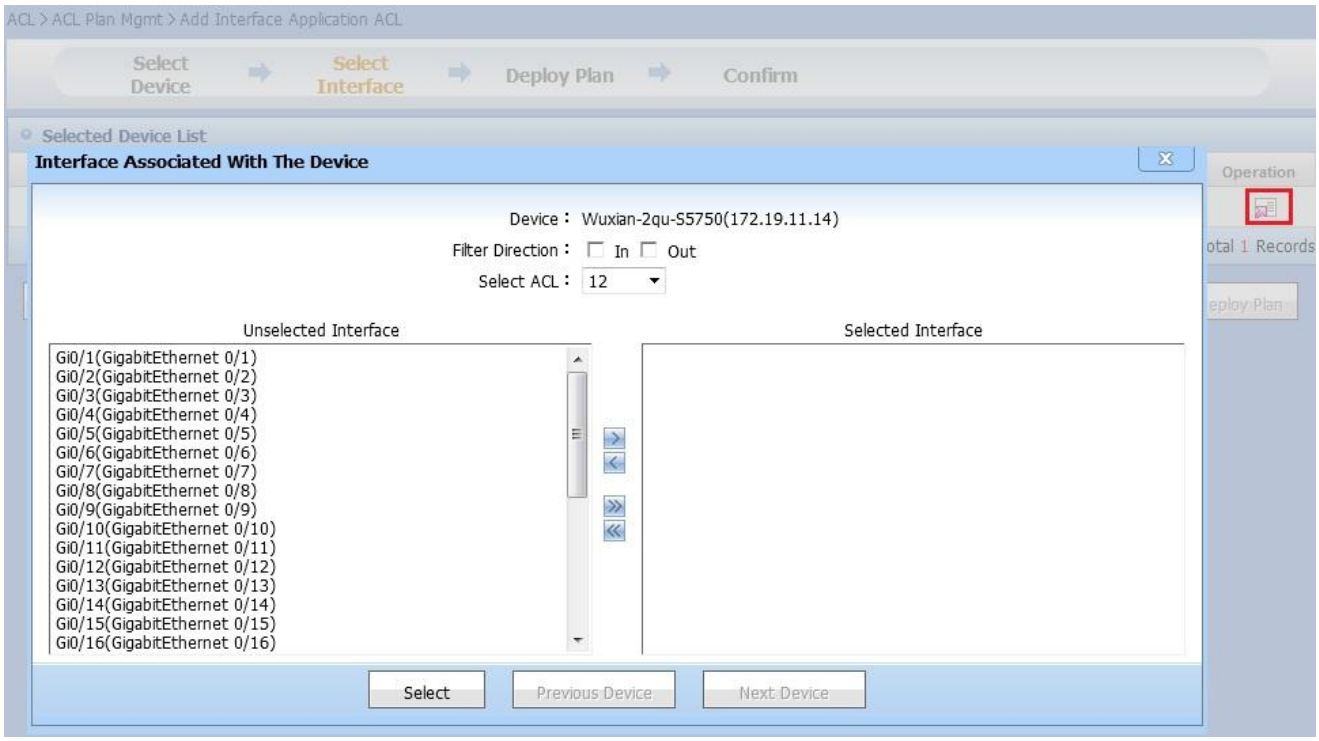


Figure 11.252. Interface Associated With The Device

14) Select **Filter Direction**, **ACL** and interfaces in **Unselected Interface**, and double-click interface or click button **>**. The selected interface will be shown in format **Interface Name[Filter Direction]ACL Name**. Click **Select** button to complete the selection.

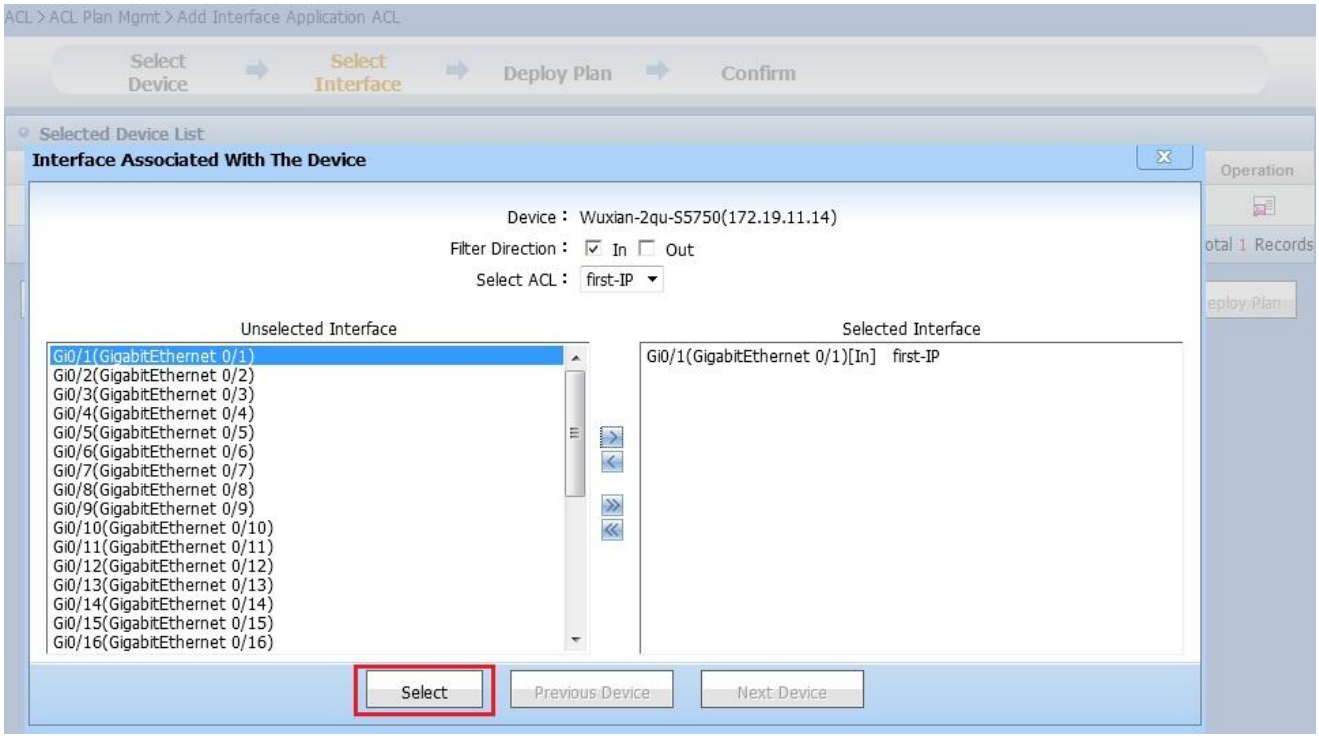


Figure 11.253. Interface Associated With The Device

15) Show **Selected Device List**, and device with interface selected or unselected will be identified with different icons. Click button **Previous: Select ACL**, and the system will return to page **Selected ACL List**.

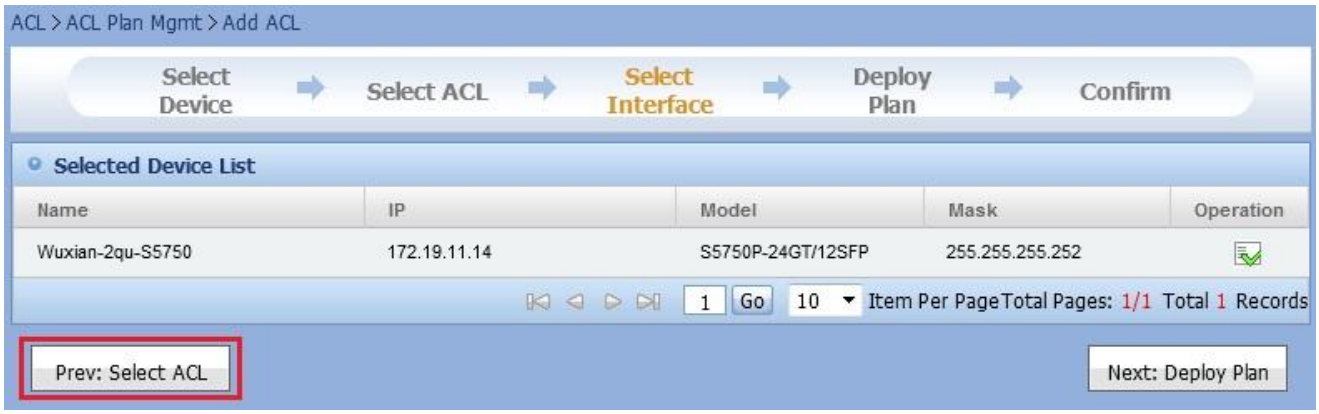


Figure 11.254. Previous: Select ACL

16) Show **Selected Device List**, and device with interface selected or unselected will be identified with different icons. Click button **Next: Deploy Plan**, as shown in following figure:

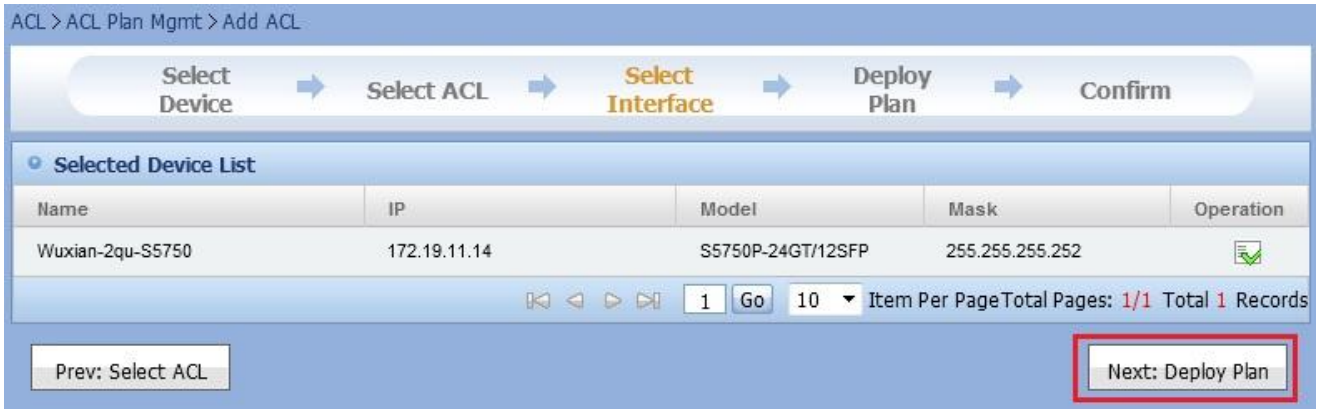


Figure 11.255. Next: Deploy Plan

17) Show **Deploy Plan**, and click button **Previous: Select Interface**. The system will return to page **Select Interface**, as shown in following figure:

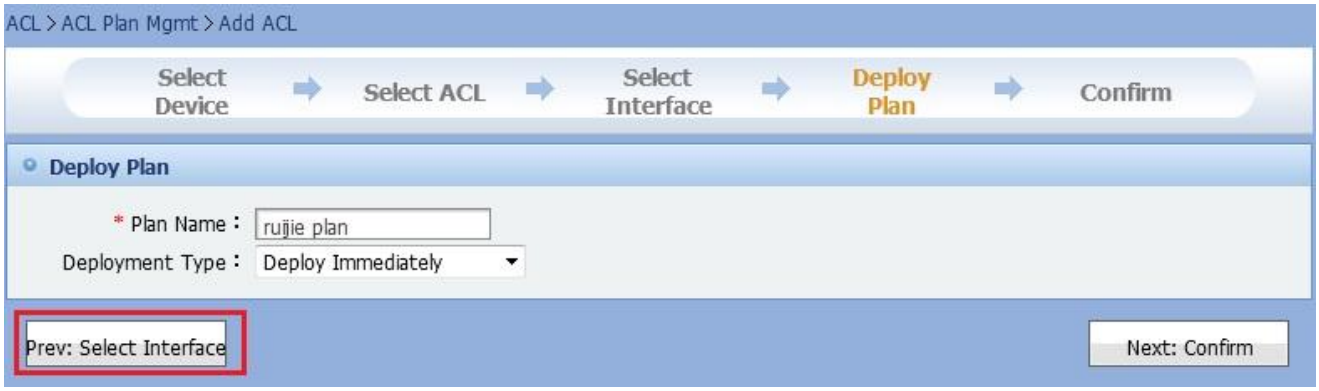


Figure 11.256. Previous: Select Interface

18) Show **Deploy Plan**, fill in the plan name and select deployment type, and click button **Next: Confirm**, as shown in following figure:

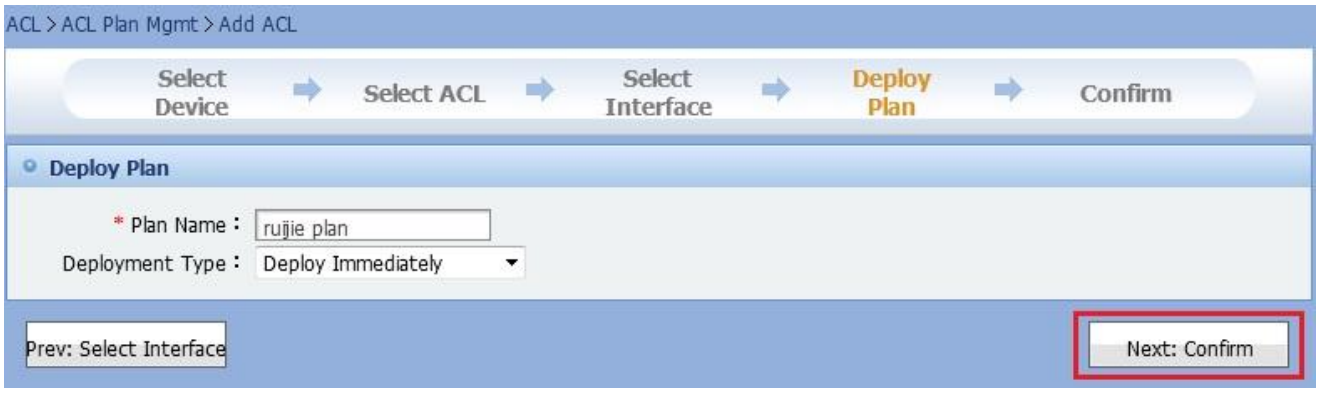


Figure 11.257. Next: Confirm

19) Show **Confirm**, and click button **Previous: Deploy Plan** to return to page **Deploy Plan**, as shown in following figure:

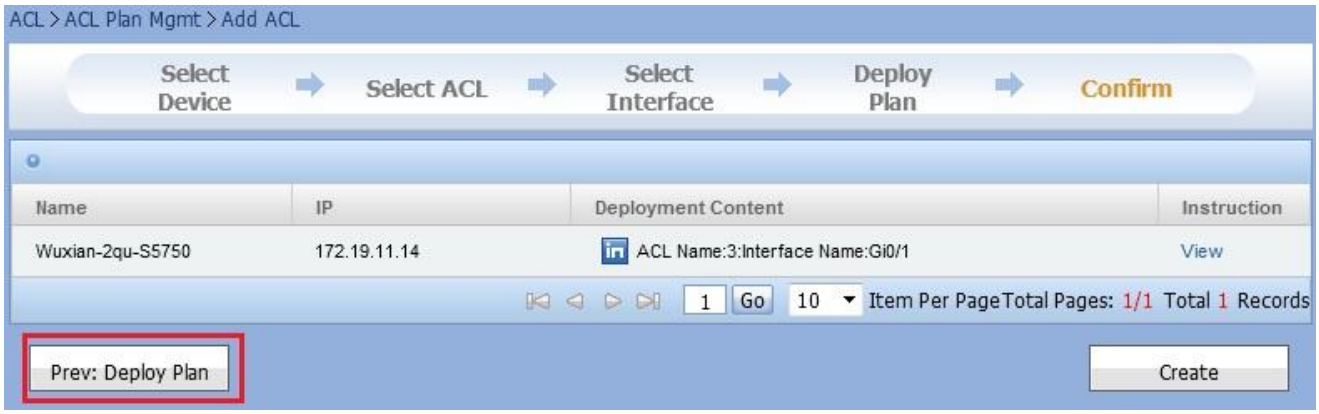


Figure 11.258. Previous: Deploy Plan

20) Click button **View** to display a new page will be pop-up for generated instruction, as shown in following figure:

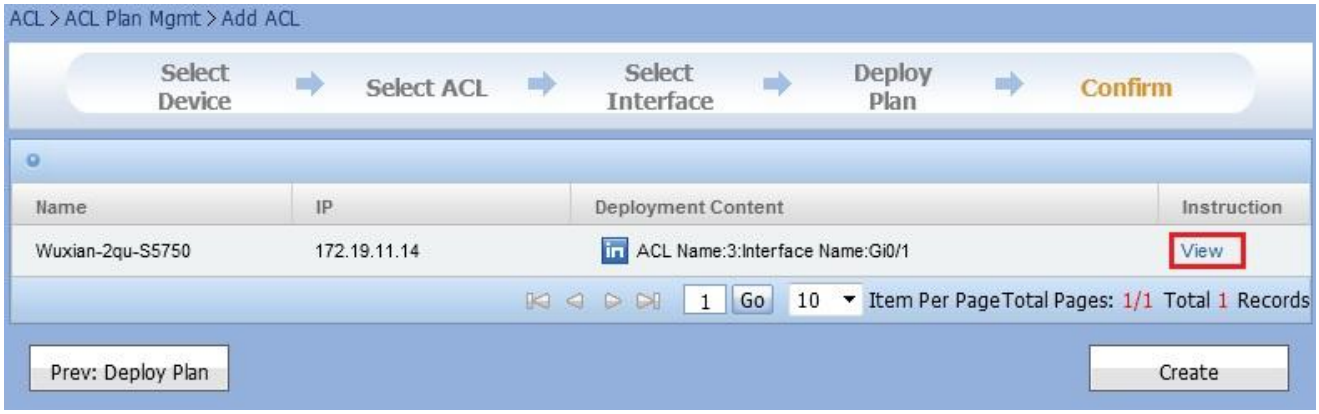


Figure 11.259. View Instruction

21) Click **Create** to generate a deployment plan and return to page **ACL Deployment Plan Management**, as shown in following figure:

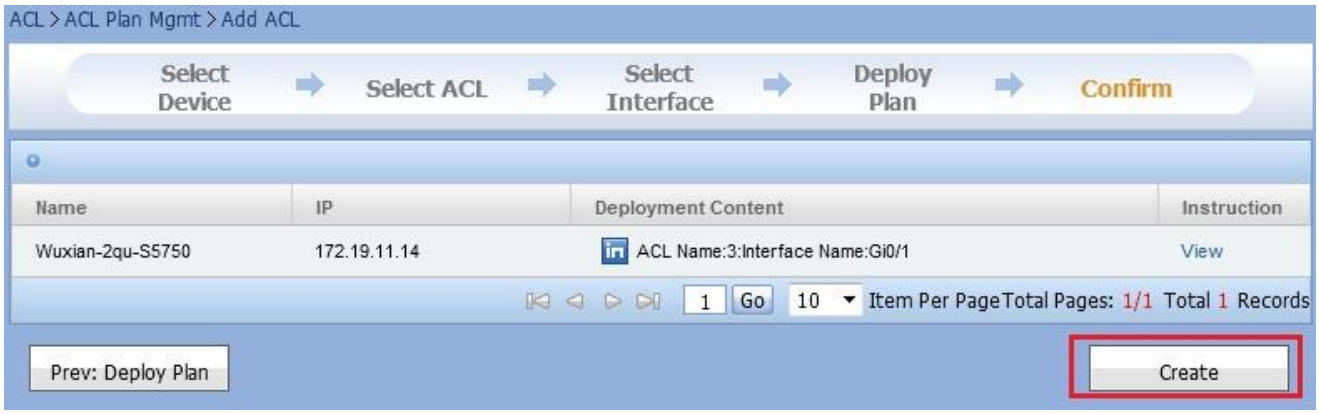


Figure 11.260. Start to create a deployment plan

On page **Select Device**, click **Add All** button to add all the devices to **Selected Device List**. When clicking **Add All** button, you do not need to select devices.

On page **Selected Device List**, click **Deselect** or **Deselect All** button to remove all the devices in **Selected Device List**. When clicking **Deselect All** button, you do not need to select devices.

On page **Selected ACL List**, click **Deselect** or **Deselect All** button to remove all the ACLs in **Selected ACL list**. When clicking **Deselect All** button, you do not need to select ACL.

On page **Selected ACL List**, click **Add All** button to add all the ACLs to **Selected ACL list**. When clicking **Add All** button, you do not need to select ACL.

In box **Unselected Interface** of page **Interface Associated With The Device**, double-click interface or click the **>** button to configure interface one by one or click the **>>** button to select interfaces in batch.

In box **Selected Interface** of page **Interface Associated With The Device**, double-click interface or click the **<** button to remove interface from the box or click the **<<** button to remove interfaces in batch.

On page **Interface Associated With The Device**, click button **Previous Device** to show information of **Selected Interface** for previous device.

On page **Interface Associated With The Device**, click button **Next Device** to show information of **Selected Interface** for next device.

Note

If there is no record of the selected device list, you cannot click **Next: Select ACL** button.

If there is no record of the selected ACL list, you cannot click **Deploy Plan** and **Previous: ACL Int Deployment** button.

If interface is not selected, you cannot click **Next: Deploy Plan** button.

After a deployment plan is added, you must click **Start Deployment Plan** to execute it.

11.5.10. Add Interface Deployment Plan

User can add interface deployment plan on page **ACL Deployment Plan Management**.

Operation Steps

1) On page **ACL Deployment Plan Management**, click the link **Add Interface Application ACL** in the ACL list, as shown in following figure:

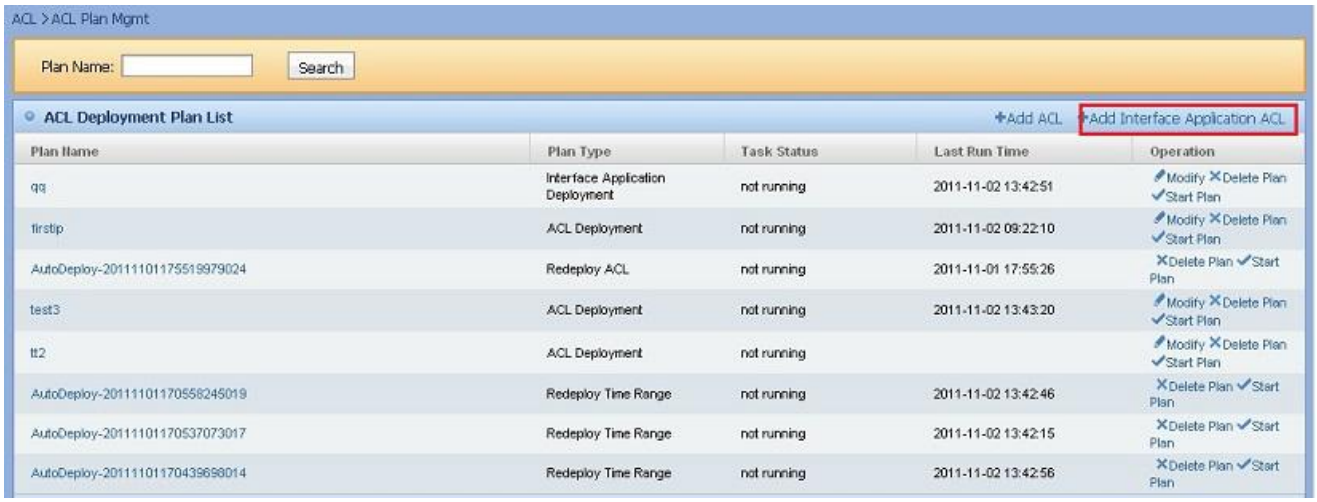


Figure 11.261. Add Interface Deployment Plan

2) Show page **Selected Device List**, as shown in following figure:

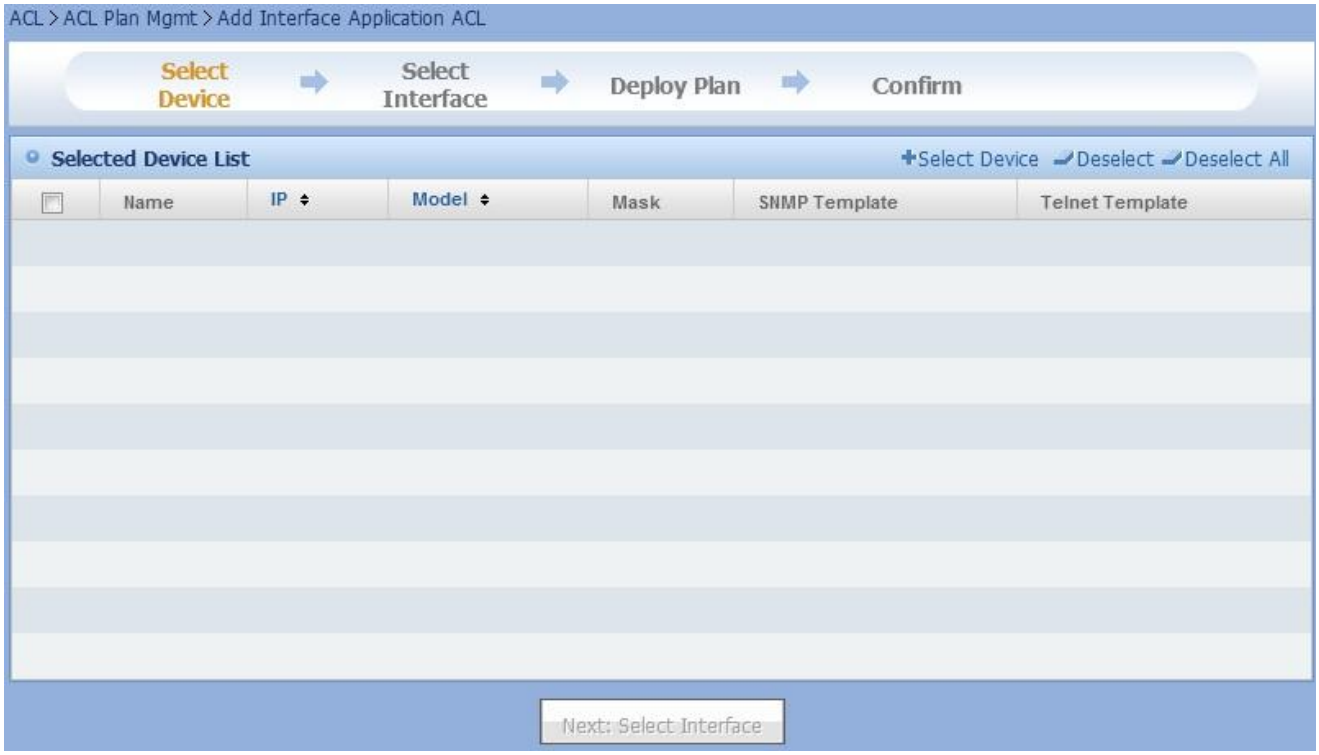


Figure 11.262. Show page **Selected Device List**

3) Click **Select Device** button to display page **Select Device**, as shown in following figure:

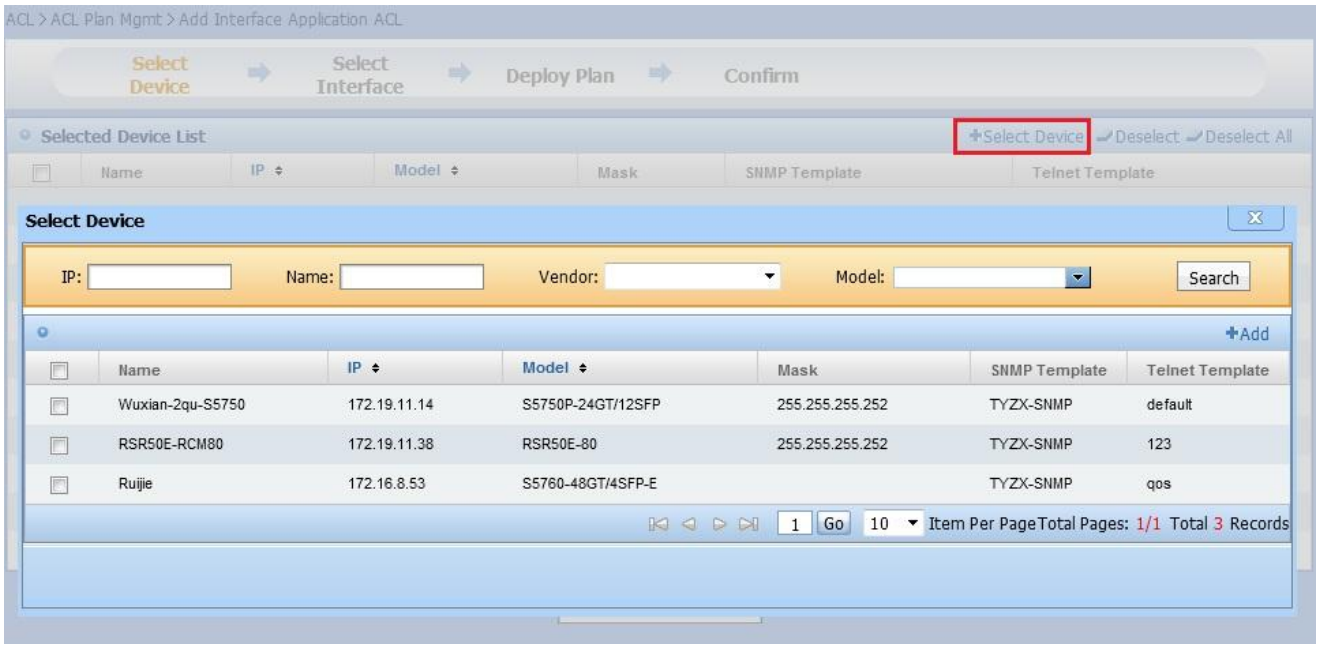


Figure 11.263. Select Device

4) After selecting device, click the **Add** button, as shown in following figure:

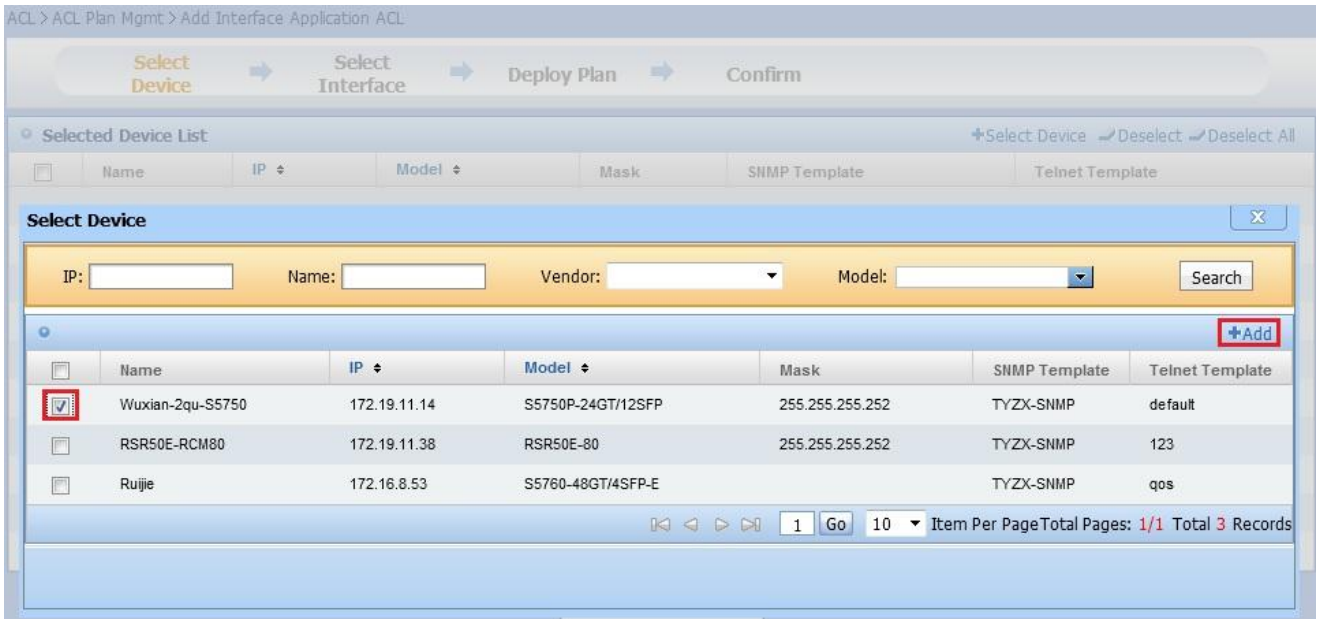


Figure 11.264. Add Device

5) Show page **Selected Device List**, and click button **Next: Select Interface**, as shown in following figure:

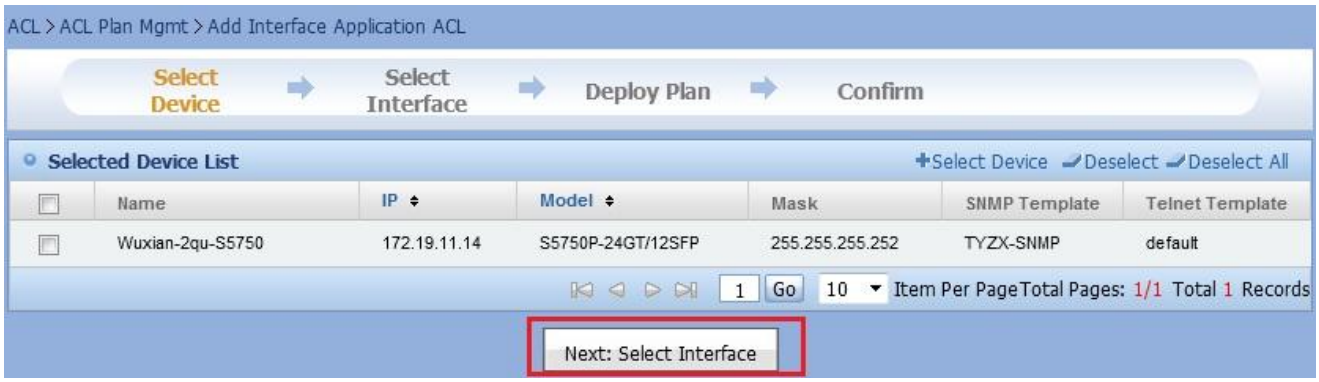


Figure 11.265. Next: Select Interface

6) Go to page **Select Interface**, show **Selected Device List**, and click the button in operation bar of **Selected Device List** to enter page **Interface Associated With The Device**, as shown in following figure:

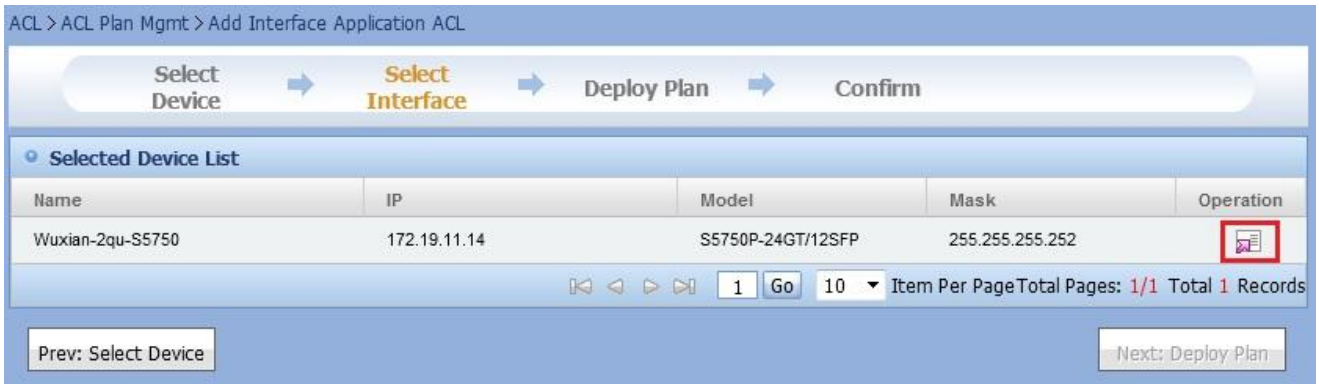


Figure 11.266. Select Interface

7) Show page **Interface Associated With The Device**:

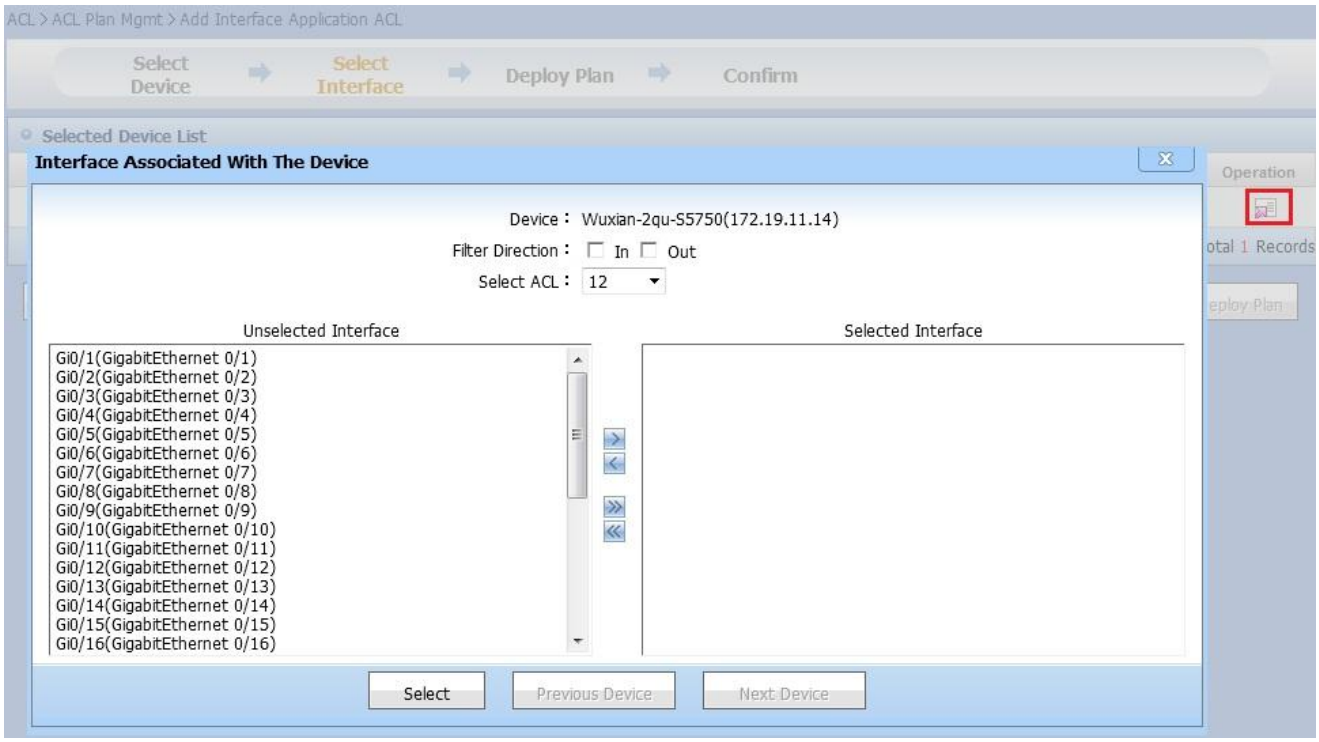


Figure 11.267. Interface Associated With The Device

8) Select **Filter Direction**, **ACL** and interface in **Unselected Interface**, and double-click interface or click button **>**. The interface will be shown in format **Interface Name[Filter Direction]ACL Name**.

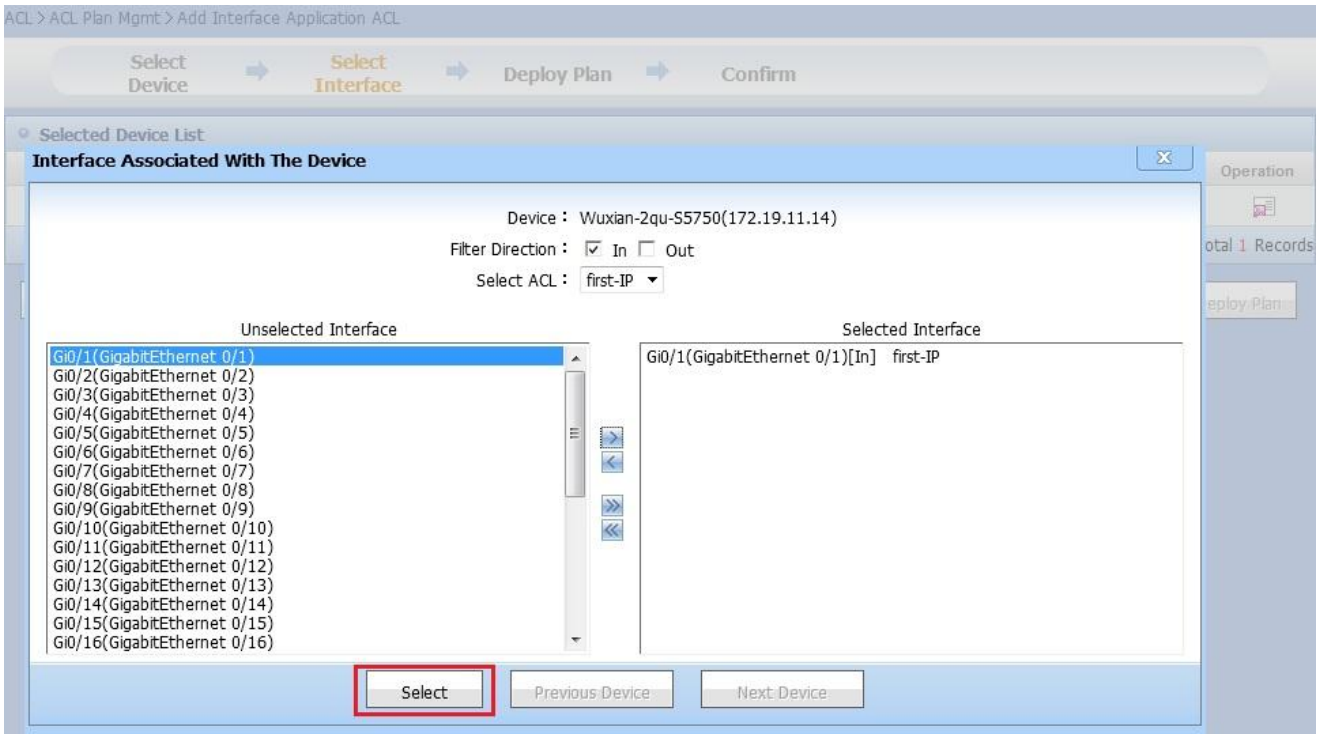


Figure 11.268. Interface Associated With The Device

9) Show **Selected Device List**, and the device with interface selected or unselected will be identified with different icons. Click button **Previous: Select Device**, and the system will return to page **Selected Device List**, as shown in following figure:

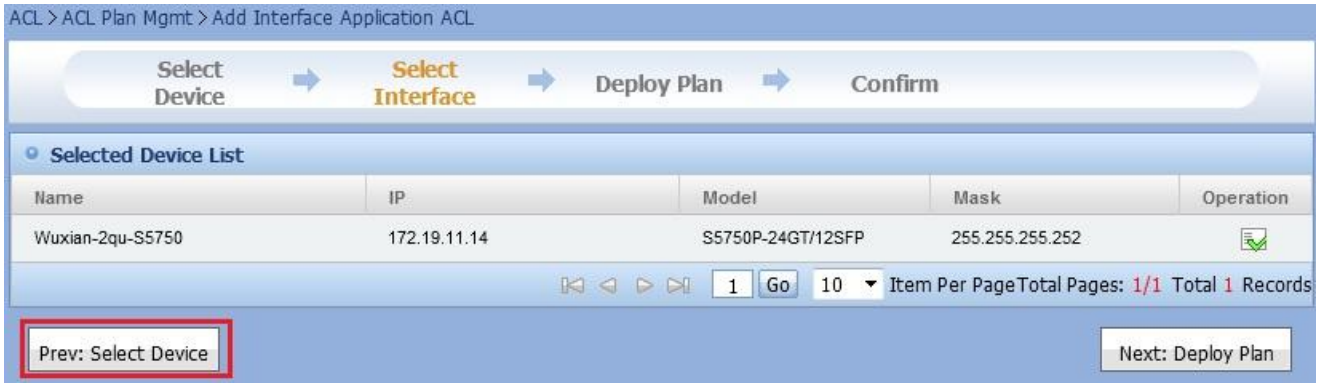


Figure 11.269. Previous: Select Device

10) Show **Selected Device List**, and the device with interface selected or unselected will be identified with different icons. Click button **Next: Deploy Plan**, as shown in following figure:

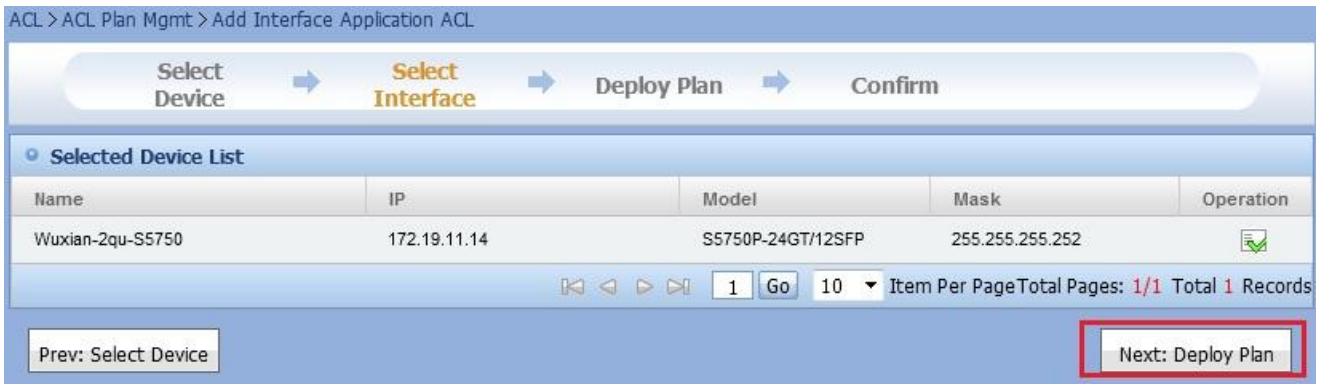


Figure 11.270. Next: Deploy Plan

11) Show **Deploy Plan**, and click button **Previous: Select Interface** to return to page **Select Interface**, as shown in following figure:

Figure 11.271. Previous: Select Interface

12) Show **Deploy Plan**, fill in the plan name and select deployment type, and click button **Next: Confirm**, as shown in following figure:

Figure 11.272. Next: Confirm

13) Show **Confirm**, and click button **Previous: Deploy Plan** to return to page **Deploy Plan**, as shown in following figure:

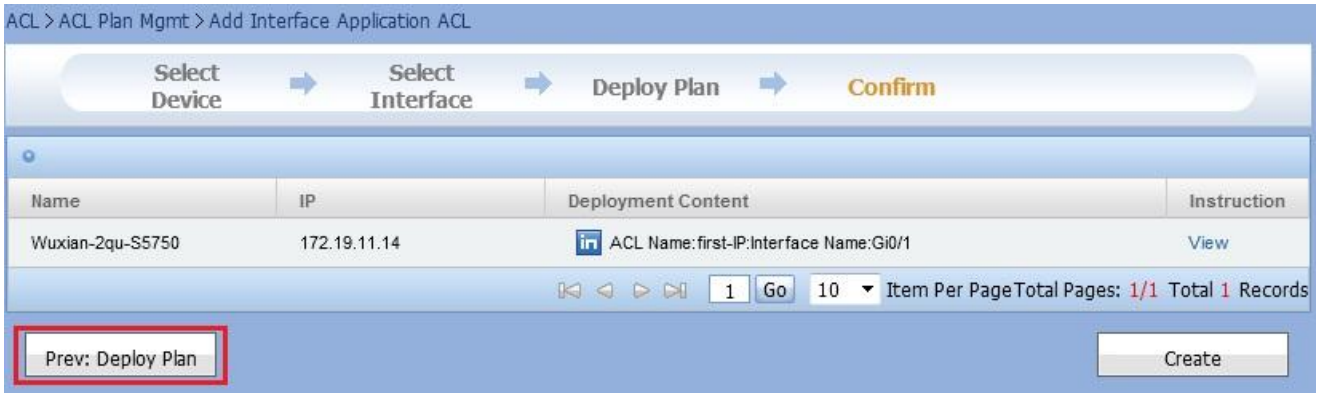


Figure 11.273. Previous: Deploy Plan

14) Click button **View** to display a new page for the generated instruction, as shown in following figure:

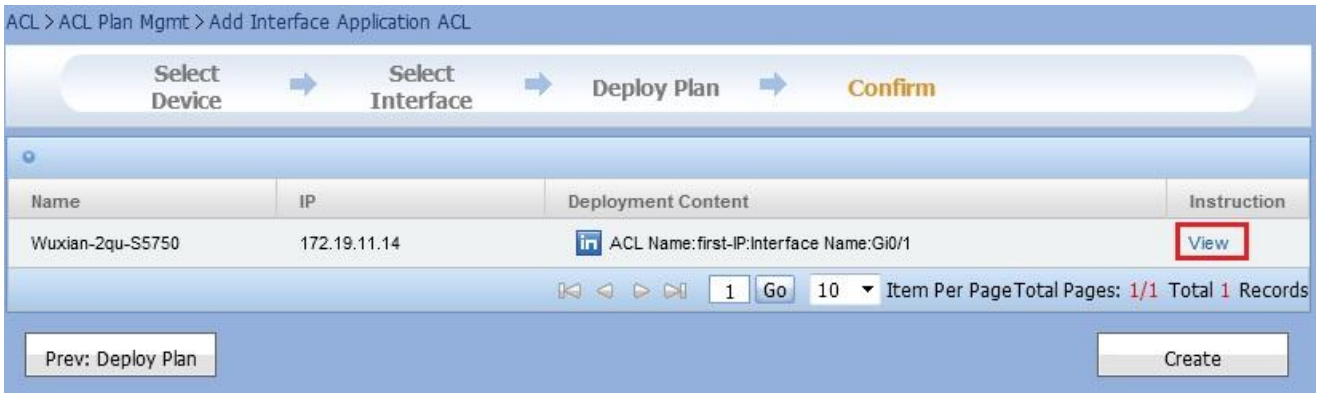


Figure 11.274. View Instruction

15) Click **Create** to generate a deployment plan and return to page **ACL Deployment Plan Management**, as shown in following figure:

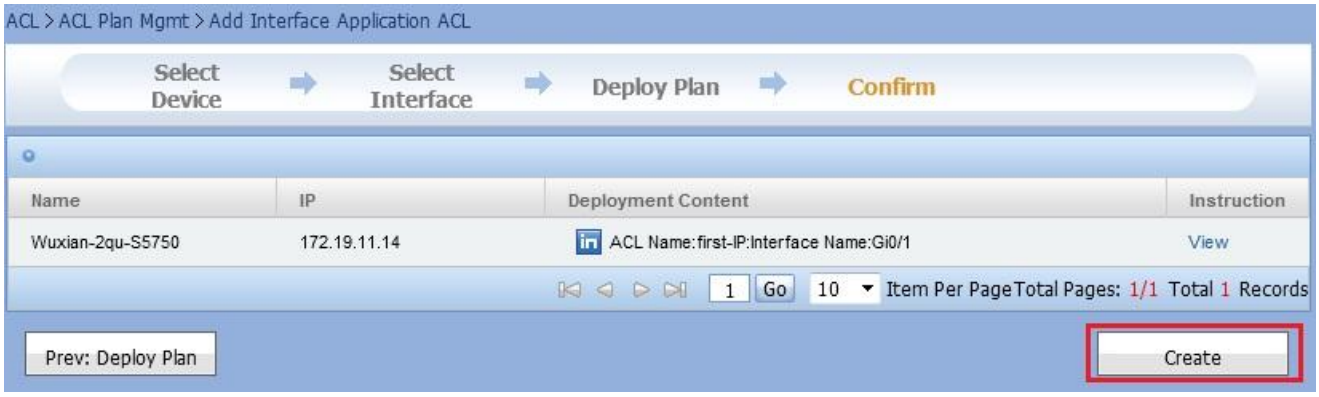


Figure 11.275. Start to create an interface deployment plan

On page **Select Device**, and click **Add All** button to add all the device to **Selected Device List**. When clicking **Add All** button, you do not need to select devices.

On page **Selected Device List**, click **Deselect** or **Deselect All** button to remove all the devices in **Selected Device List**. When clicking **Deselect All** button, you do not need to select devices.

In box **Unselected Interface** of page **Interface Associated With The Device**, double-click interface or click the **>** button to configure interface one by one or click the **>>** button to select interfaces in batch.

In box **Selected Interface** of page **Interface Associated With The Device**, double-click interface or click the **<** button to remove interface from the box or click the **<<** button to remove interfaces in batch.

On page **Interface Associated With The Device**, click button **Previous Device** to show information of **Selected Interface** for previous device.

On page **Interface Associated With The Device**, click button **Next Device** to show information of **Selected Interface** for next device.

Note

If there is no record of the selected device list, you cannot click **Next: Select ACL** button.

If interface is not selected, you cannot click **Next: Deploy Plan** button.

After a deployment plan is added, you must click **Start Deployment Plan** to execute it.

Chapter 12 System Management

In System Management, super administrator can configure device series, device model, system parameters, email server, user management and etc.

Functionalities

- Device Vendor Management
- Device Model Management
- Device Series Management
- Device Type Management
- System Parameter Management
- Mail Server Setting
- Correlated Server Registration
- Software Upgrade Prompt
- Favorite Menu
- Security Log
- Plan Execution Log
- Change Log
- Administrator Management
- Role Management
- Change Password
- Concurrent Logon Control
- Device Software Summary
- VLAN Summary Report
- SMS Modem Setting

12.1. Device Vendor Management

Some device vendors are pre-defined in the system. Administrators can define device vendors by themselves, so that those vendors which are not defined in the system can be added easily.

Functionalities

- Search Device Vendor
- Add Device Vendor
- Modify Device Vendor
- Delete Device Vendor

12.1.1. Search Device Vendor

Search device vendors existing in the system based on query conditions.

Input vendor name, and click **Search**, as shown below:

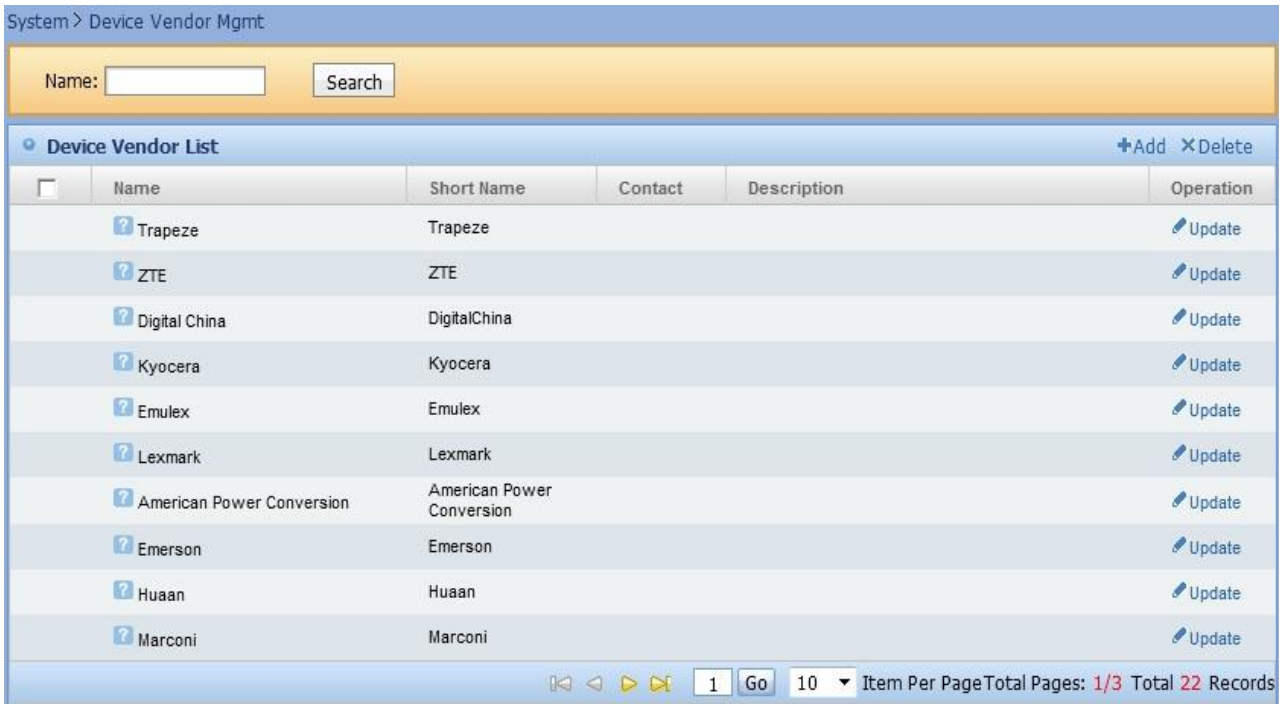


Figure 12.1. Search Device Vendor

12.1.2. Add Device Vendor

Add one or more device vendors to put multiple device vendors into centralized management.

Operation Steps

1) Select **Device Mgmt** tab, and click **Device Vendor Mgmt** menu in the navigation tree to enter Device Vendor Management page.

Figure 12.2. Device Vendor Management Page

2) Click **Add** to enter the **Add Vendor** page, as shown below:

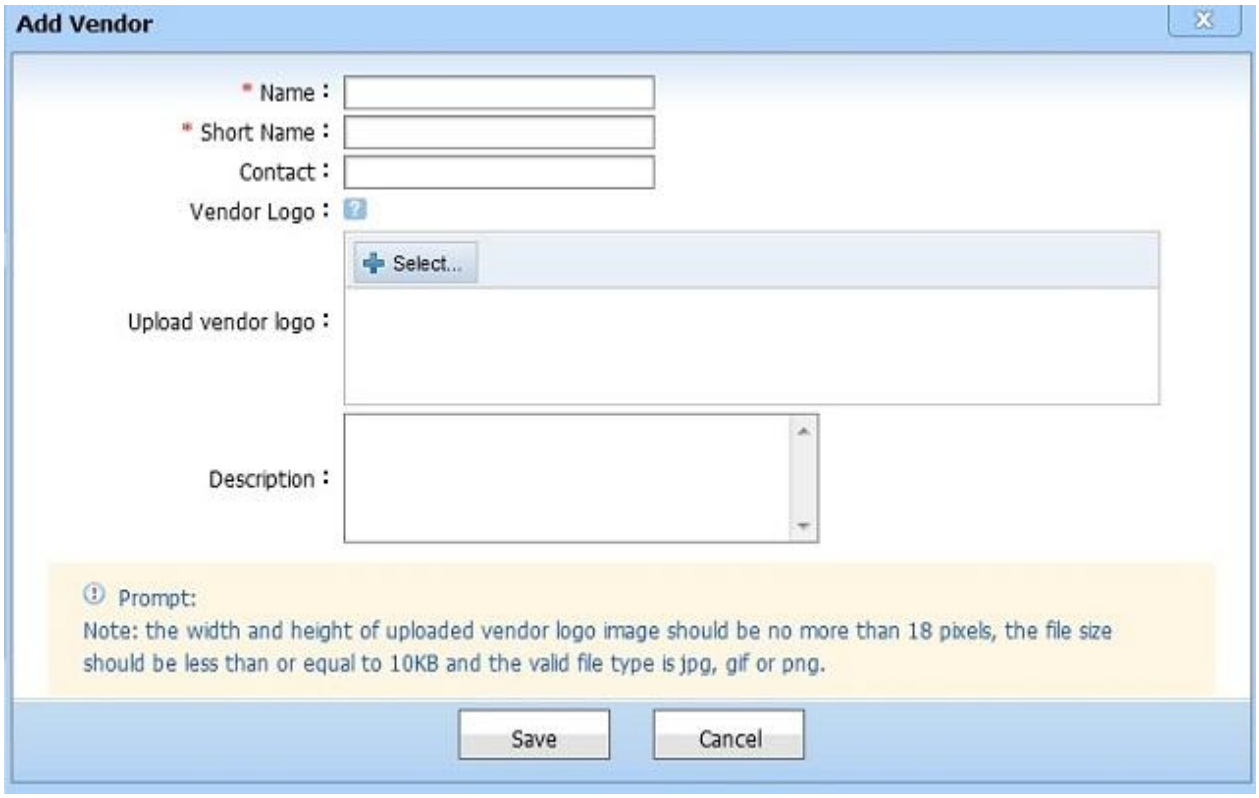


Figure 12.3. Add Device Vendor

Enter the device vendor name, abbreviation, contact info and description, and click **Save**.

12.1.3. Modify Device Vendor

Customized device vendors can be updated in the system.

Operation Steps

Choose one device vendor record, and click **Update** link in the **Operation** column to enter modify device vendor page, as shown below:

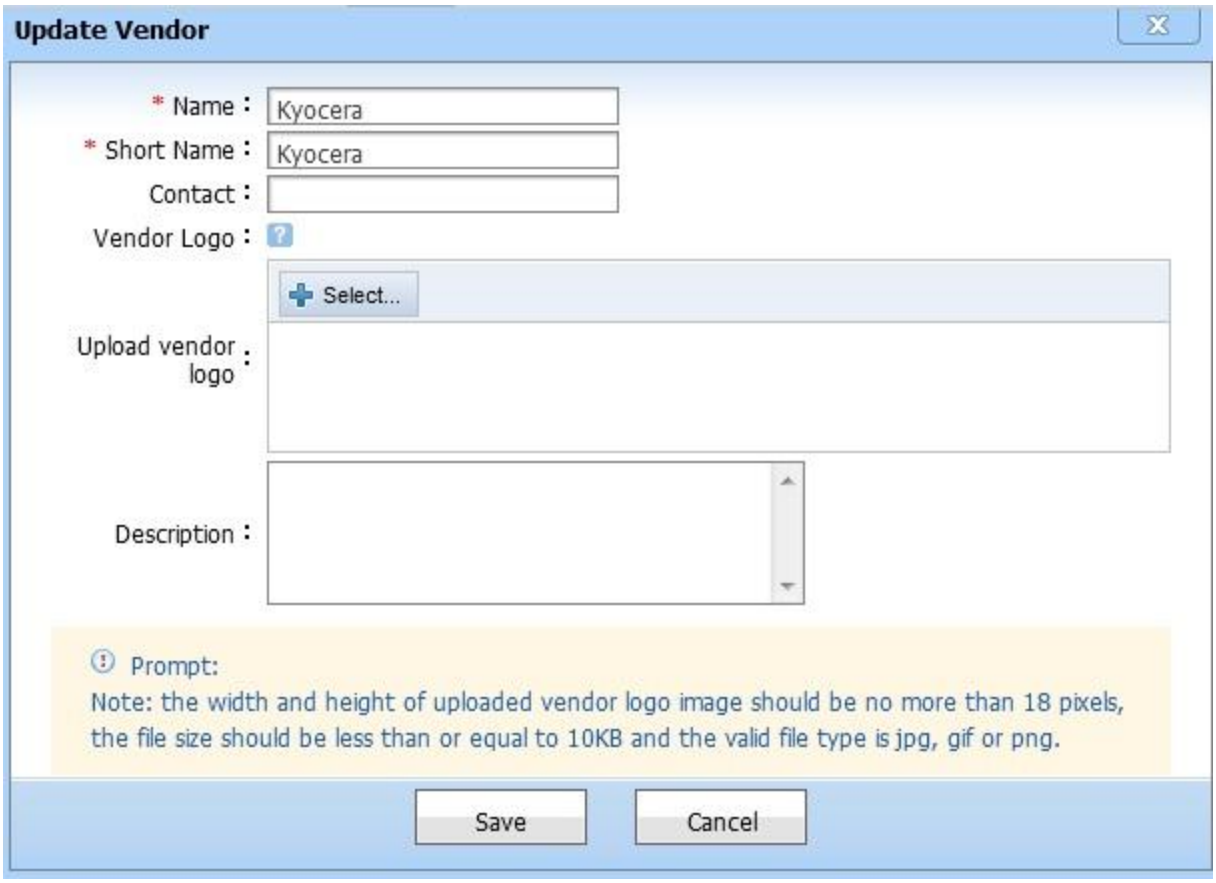


Figure 12.4. Modify Device Vendor Page

12.1.4. Delete Device Vendor

Go to **Device Vendor Mgmt** page, choose a record to be deleted, and click **Delete**, as shown below:

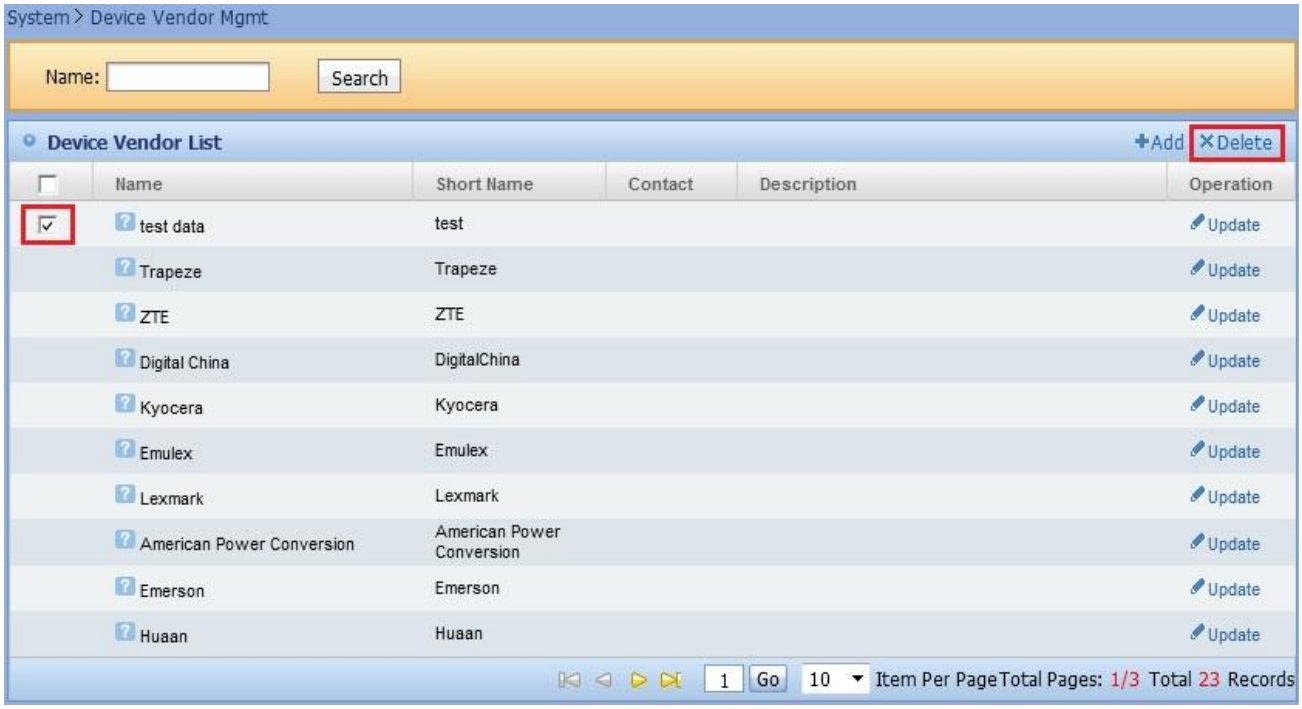


Figure 12.5. Delete Device Vendor

12.2. Device Model Management

Some device models are pre-defined in the system. Administrators can define models by themselves, so that those Ruijie device models which are not defined in the system can be added easily.

Functionalities

- Device Model List
- Add Device Model
- Modify Device Model

12.2.1. Device Model List

Operation Steps

1) Click **Device Model Mgmt** in Device Mgmt.

Figure 12.6. Device Model Management

2) Device model list supports search based on vendor name, model name, system OID or device type.

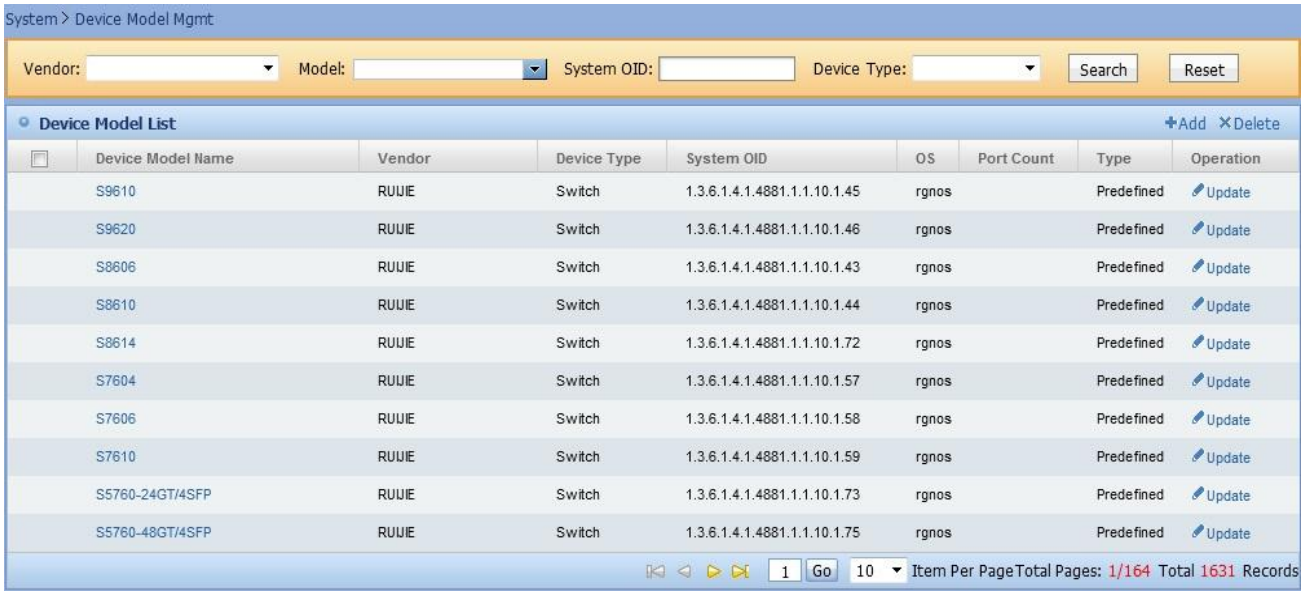


Figure 12.7. Device Model List

3) Choose at least one device model record, and click **Delete** to perform the deletion operation.

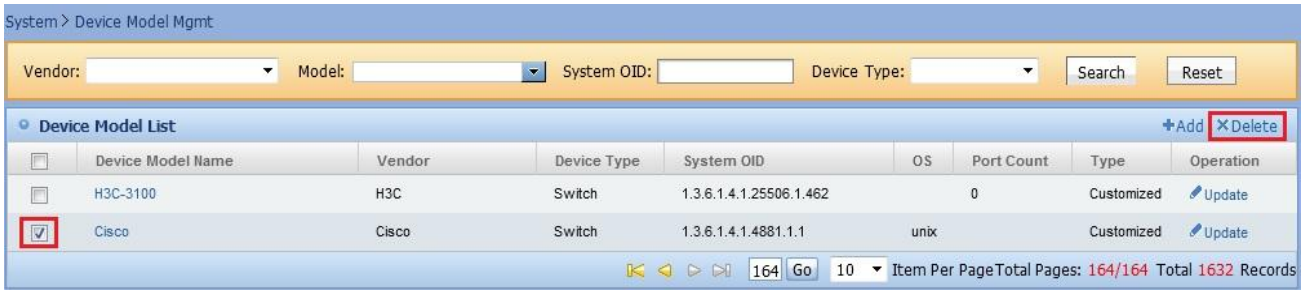


Figure 12.8. Delete Device Model

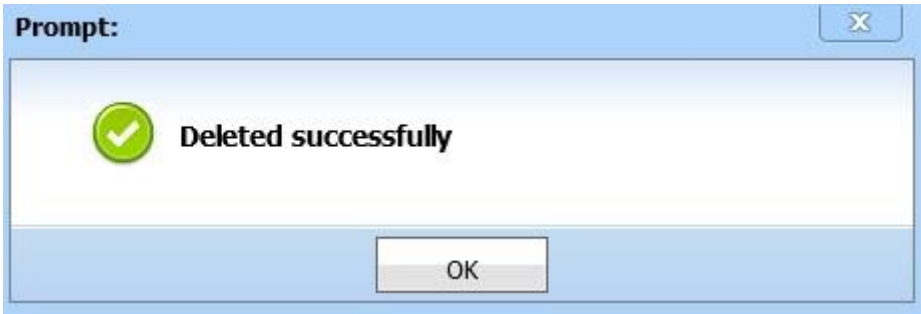


Figure 12.9. Delete Success Prompt

4) Click model name in the list to view model info.

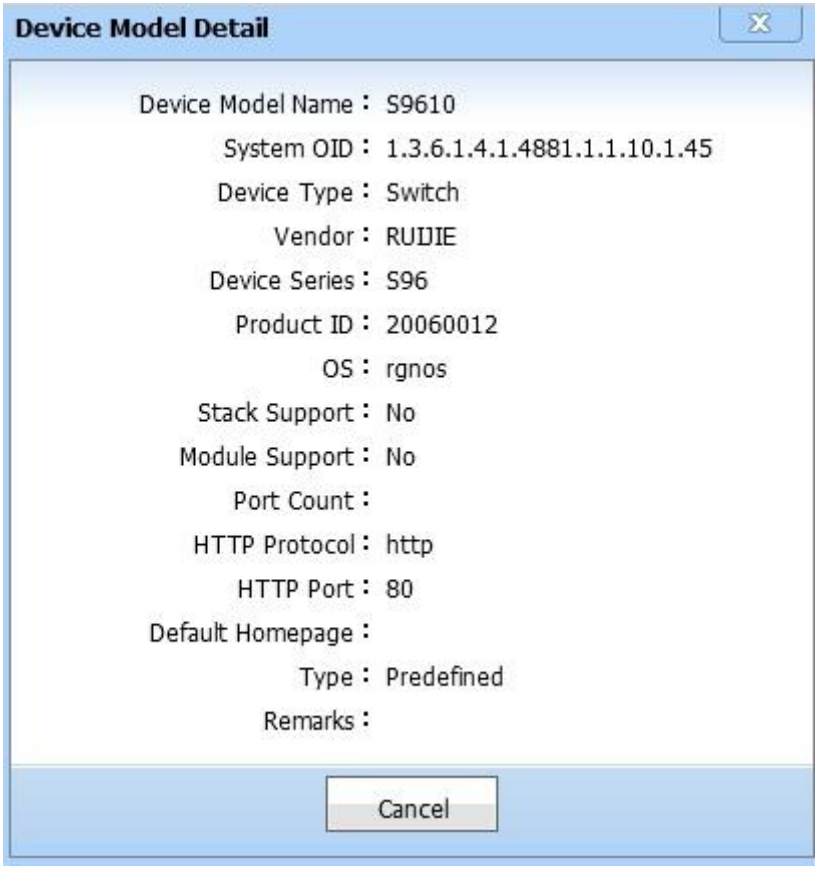


Figure 12.10. Device Model Detail

Note

Super administrator can add, delete, modify and search self-defined device model records.

Only self-defined device model can be deleted.

Product ID is a proprietary field of Ruijie devices. Please refer to device manual for info of OS, stacking support, modularity support and interface number.

12.2.2. Add Device Model

On **Add Device Model** page, you can add device model info such as model name, device series and product ID.

Operation Steps

1) On **Device Model List** page, click **Add** to enter **Add Device Model** page, as shown below:

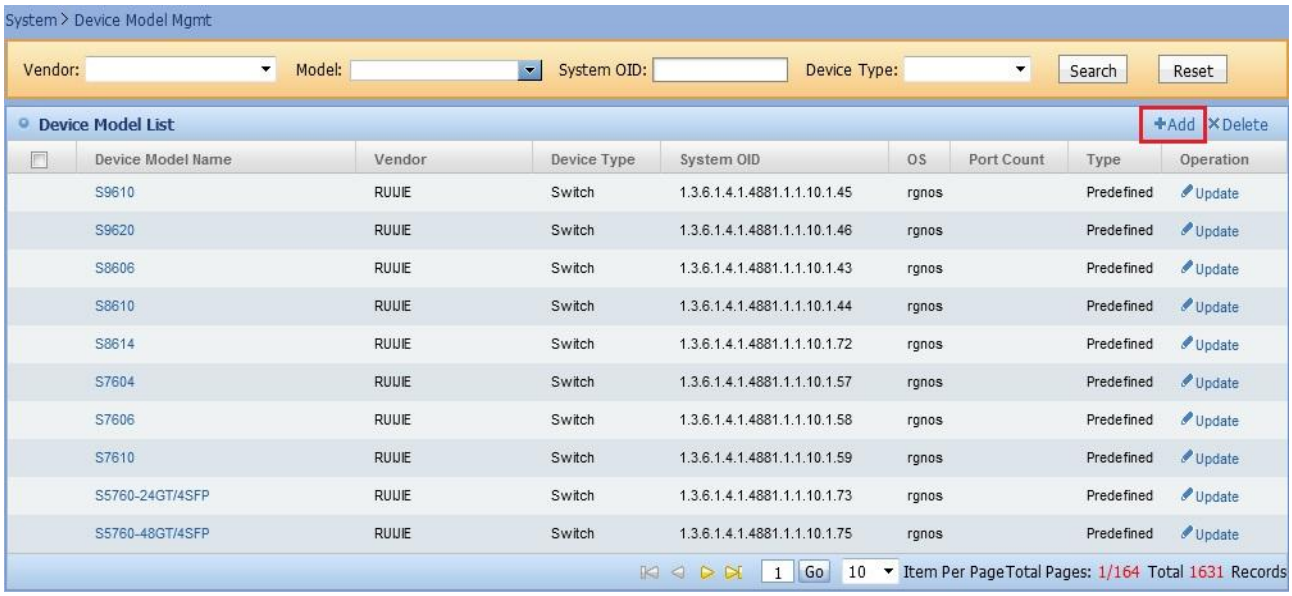


Figure 12.11. Device Model Page

2) Enter the device information, and then click **Save** to add a piece of device model info, as shown below:

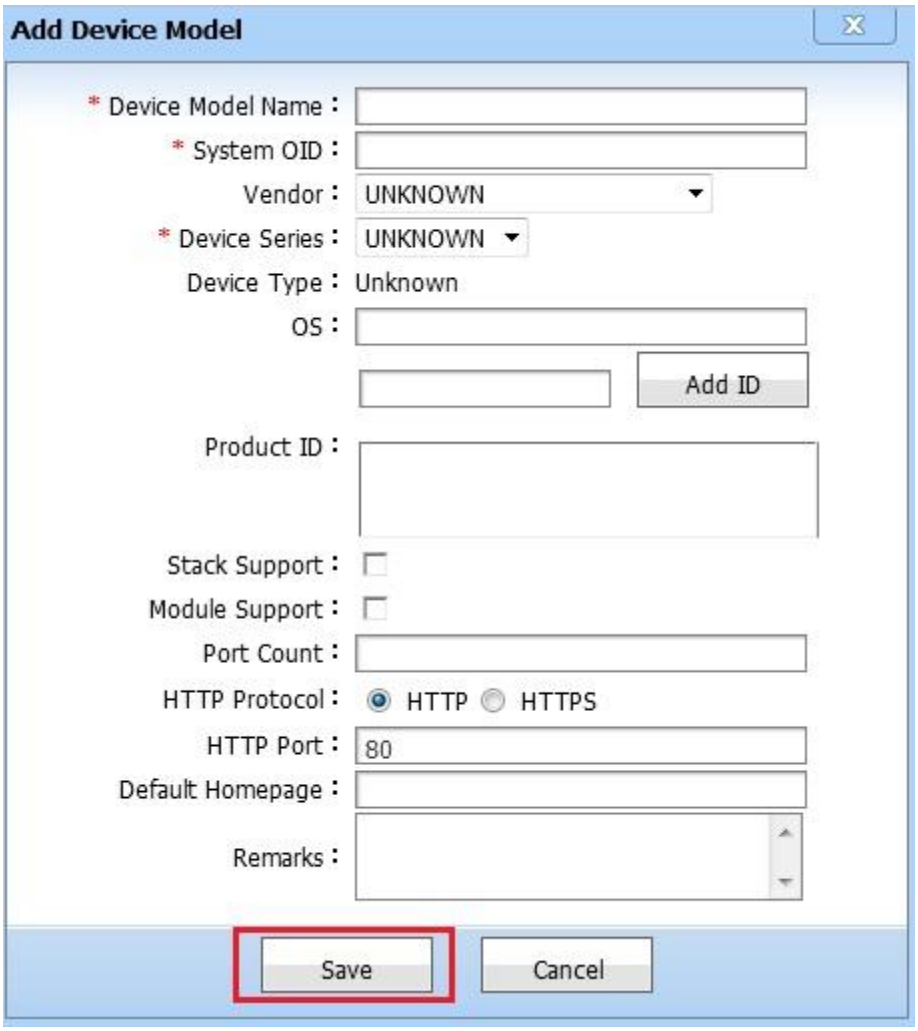


Figure 12.12. Add Device Model

Click **Cancel**. The system will not save the entered device information, and will return to **Device Model List** page.

Note

Value of System OID comes from sysObjectOID of System group of RFC1213.

Product ID: Product ID is assigned to Ruijie devices based on device model and hardware version, and it is a proprietary field of Ruijie devices. For system pre-defined Ruijie device types, the admin can only add product ID and cannot modify other info. For non-system pre-defined ones, the admin can add and delete product ID.

12.2.3. Modify Device Model

Model name, system OID, product ID and etc. can be modified on Modify Device Model Info page. Please note that some info of system pre-defined device model cannot be modified.

Operation Steps

1) On **Device Model List** page, click **Update** of certain device model record in the list to enter **Update Device Model** page, as shown below:

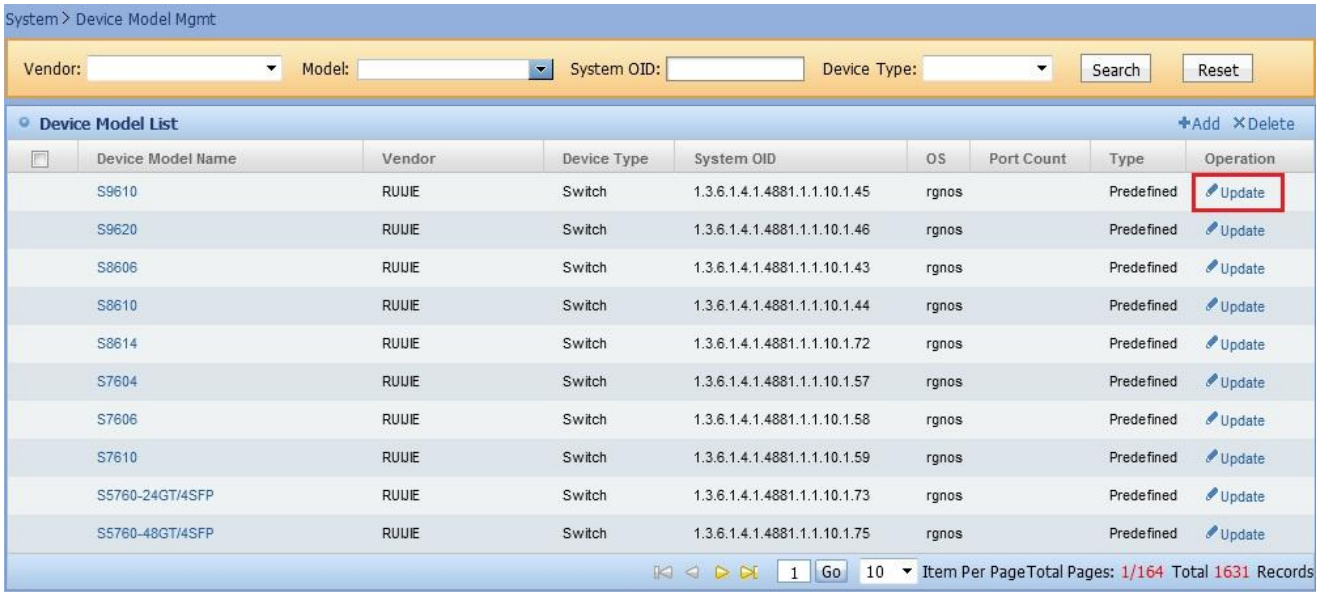


Figure 12.13. Enter Update Device Model Page

2) If the type of a device model is **Pre-defined**, only some info of it can be modified, as shown below:

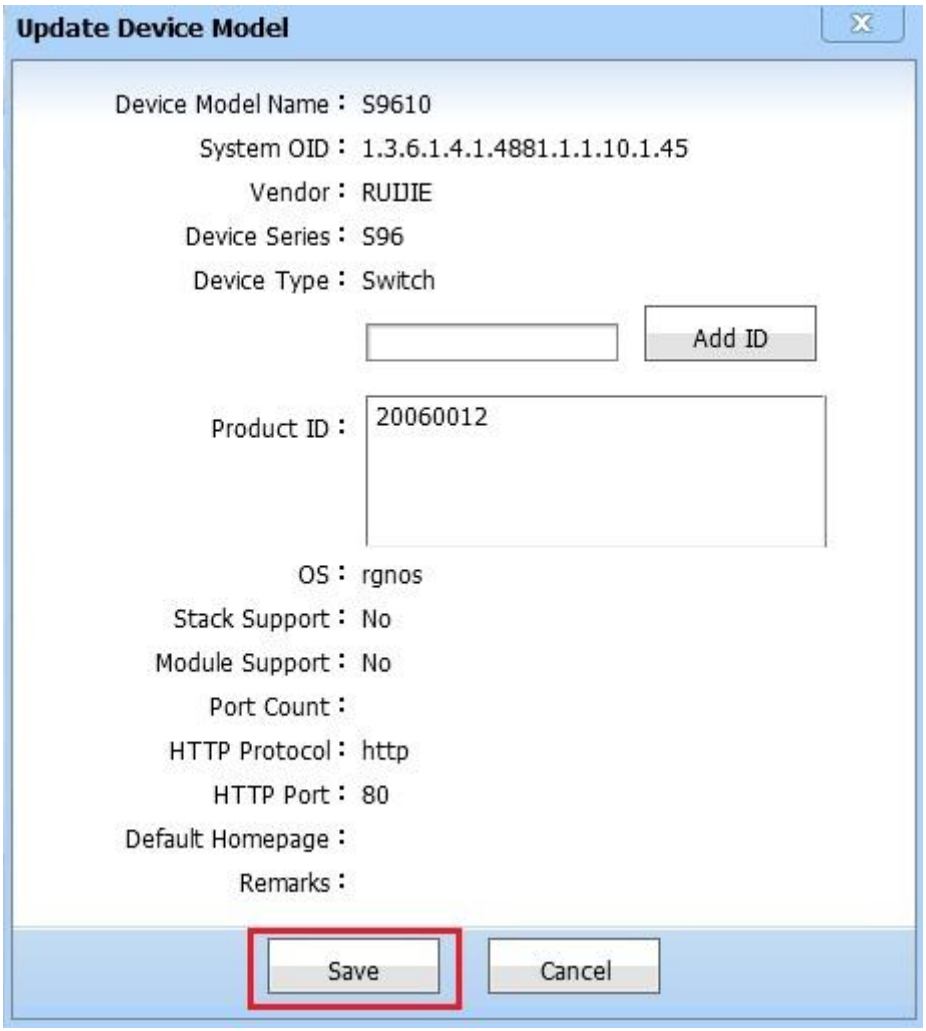


Figure 12.14. Update Device Model (Pre-defined)

3) If the type of a device model is **Self-defined**, all its info can be modified, as shown below:

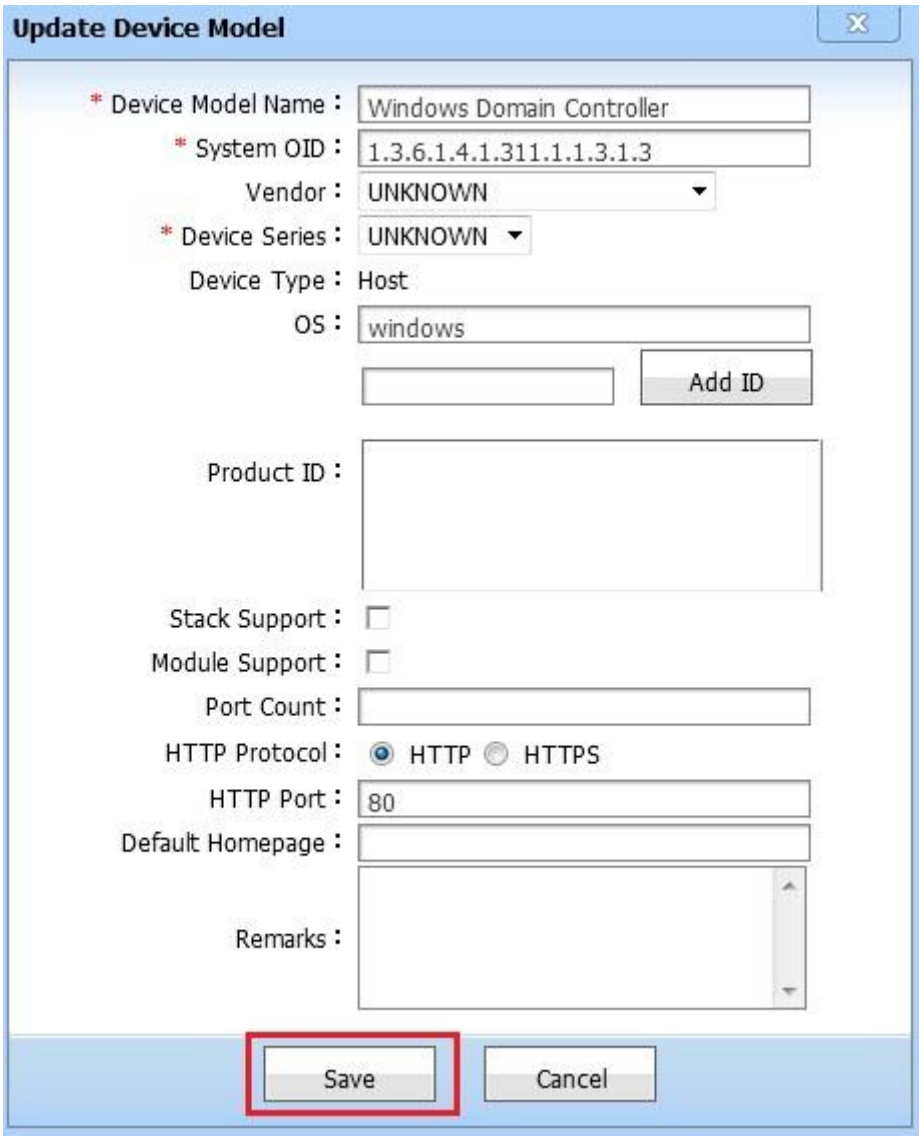


Figure 12.15. Update Device Model (Self-defined)

On **Update Device Model** page, if **Cancel** is clicked, the system will not save device changes and will return to **Device Model List** page directly.

Note

Value of OID comes from sysObjectOID of System group of RFC1213.

Product ID: Product ID is assigned to Ruijie devices based on device model and hardware version, and it is a proprietary field of Ruijie devices. For system pre-defined Ruijie device types, the admin can only add product ID. Also, No other info can be modified except product ID info. For non-system pre-defined ones, the admin can add and delete product ID.

12.3. Device Series Management

This module is used to define device series and device types of device series.

Functionalities

- Search Device Series
- Add Device Series
- Modify Device Series
- Delete Device Series
- View Device Series Detail

12.3.1. Search Device Series

Users can search device series existing in the system with various query conditions.

Enter device series name or vendor, and then click **Search** to search, as shown below:

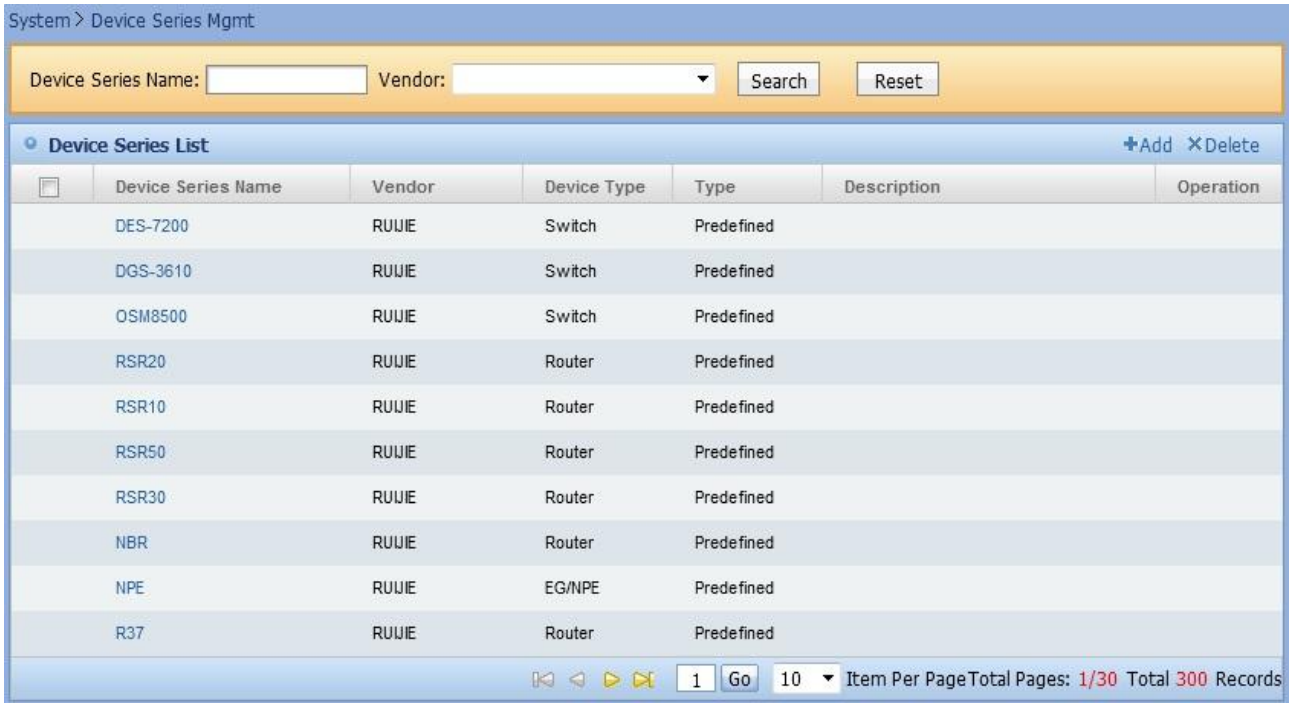


Figure 12.16. Search Device Series

12.3.2. Add Device Series

One or more device series can be added to the system to put multiple device series into centralized management.

Operation Steps

1) Select **System Mgmt** tab, click **Device Series Mgmt** in the navigation tree to enter device series management page.

Figure 12.17. Device Series Search Page

2) Click **Add** to enter Add device series page, as shown below:

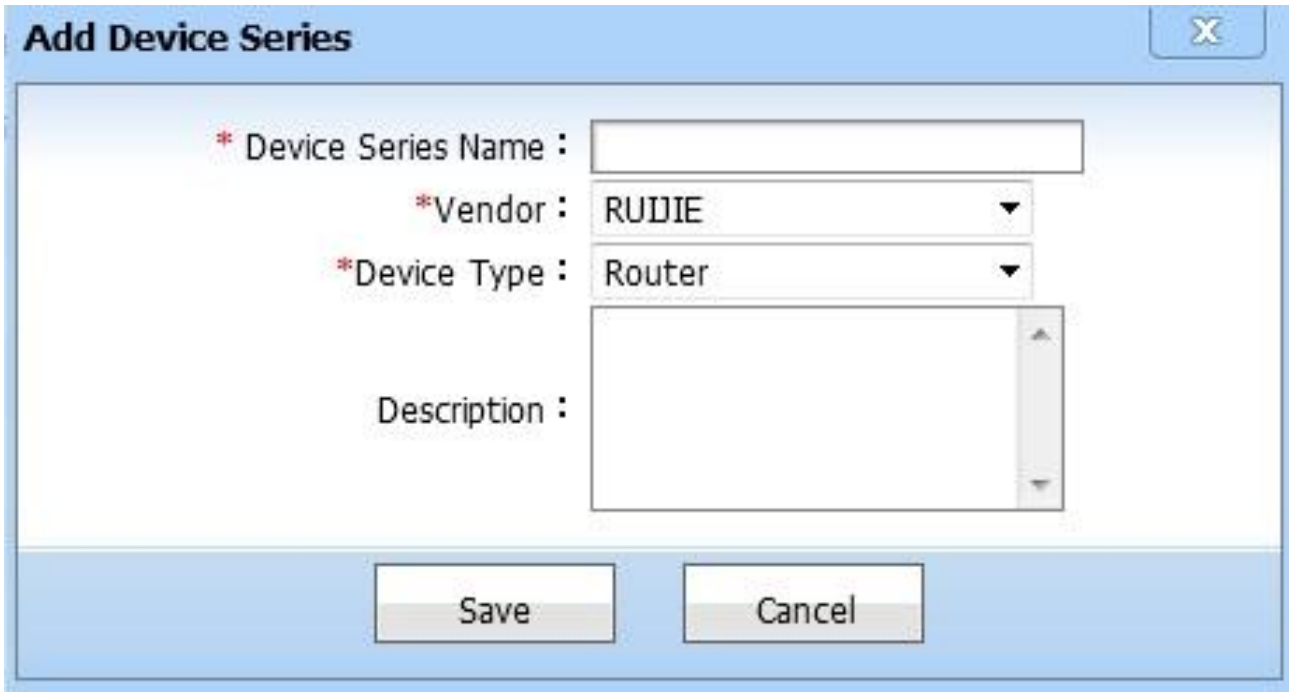


Figure 12.18. Add Device Series

Enter the device series name, select vendor and device type, and device description, and then click **Save**.

12.3.3. Modify Device Series

The system can modify customized device series.

Operation Steps

Choose a device series record, click **Update** in the **Operation** column to enter update device series page, as shown below:

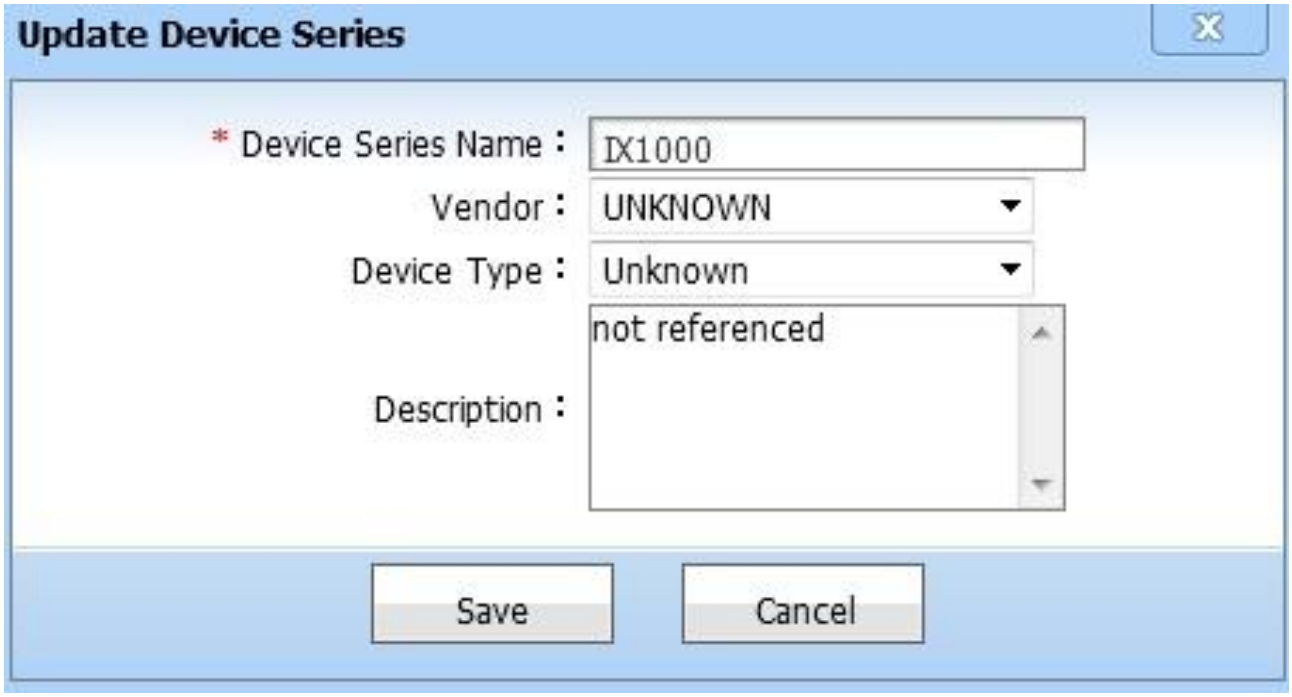


Figure 12.19. Update Device Series Page

12.3.4. Delete Device Series

Go to **Device Series Mgmt** page, choose device series record for deletion, and then click **Delete**, as shown below:

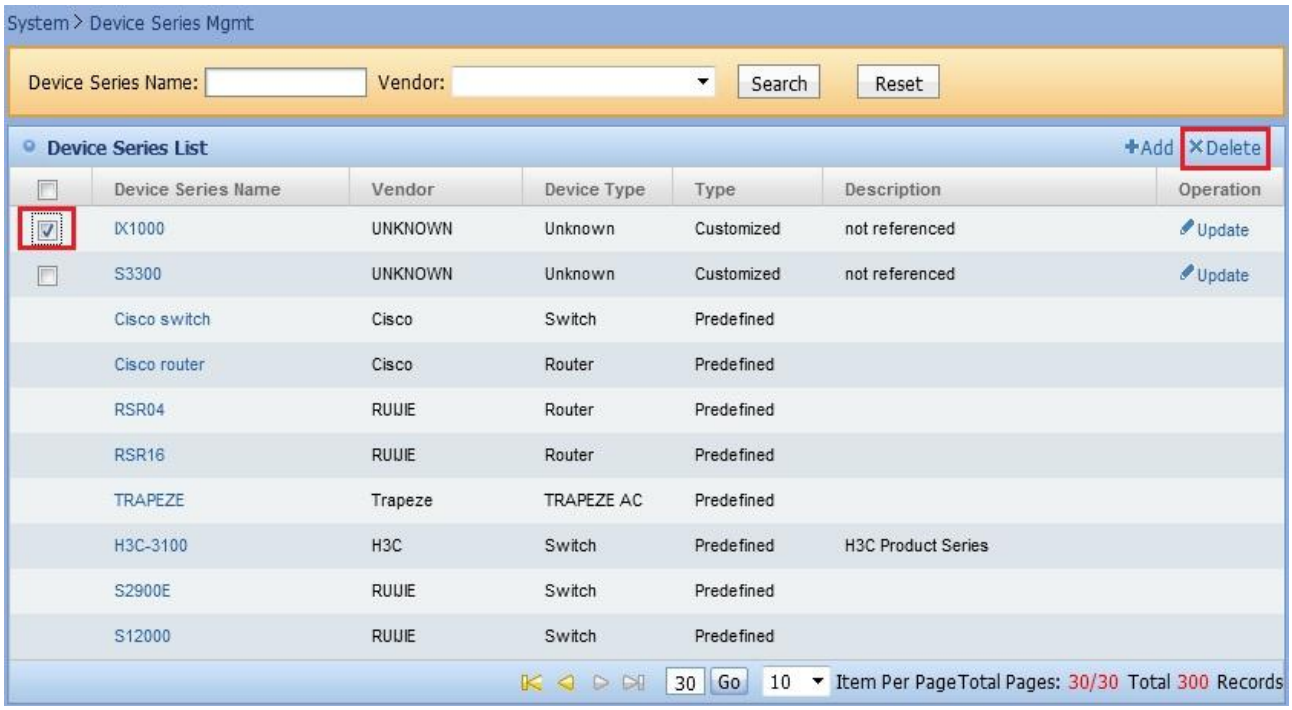


Figure 12.20. Delete Device Series

12.3.5. View Device Series Detail

Go to **Device Series Mgmt** page, click the View device series detail link of a record to enter detail info page, as shown below:

Figure 12.21. View Device Series Detail

Modify and delete operation links are in the operation bar on the right side of View Device Series Detail page. Device series can be modified or deleted by those links. Note: Modify and delete operation links are only available for customized device series.

12.4. Device Type Management

Some device types are pre-defined in the system. Administrators can define device types by themselves, so that those device types which are not defined in the system can be added easily.

Functionalities

- Device Type List
- Add Device Type
- Modify Device Type

12.4.1. Device Type List

Operation Steps

1) Click **Device Type Mgmt** in System management.

Figure 12.22. Device Type Management

2) Device type list supports search based on type code or device type.

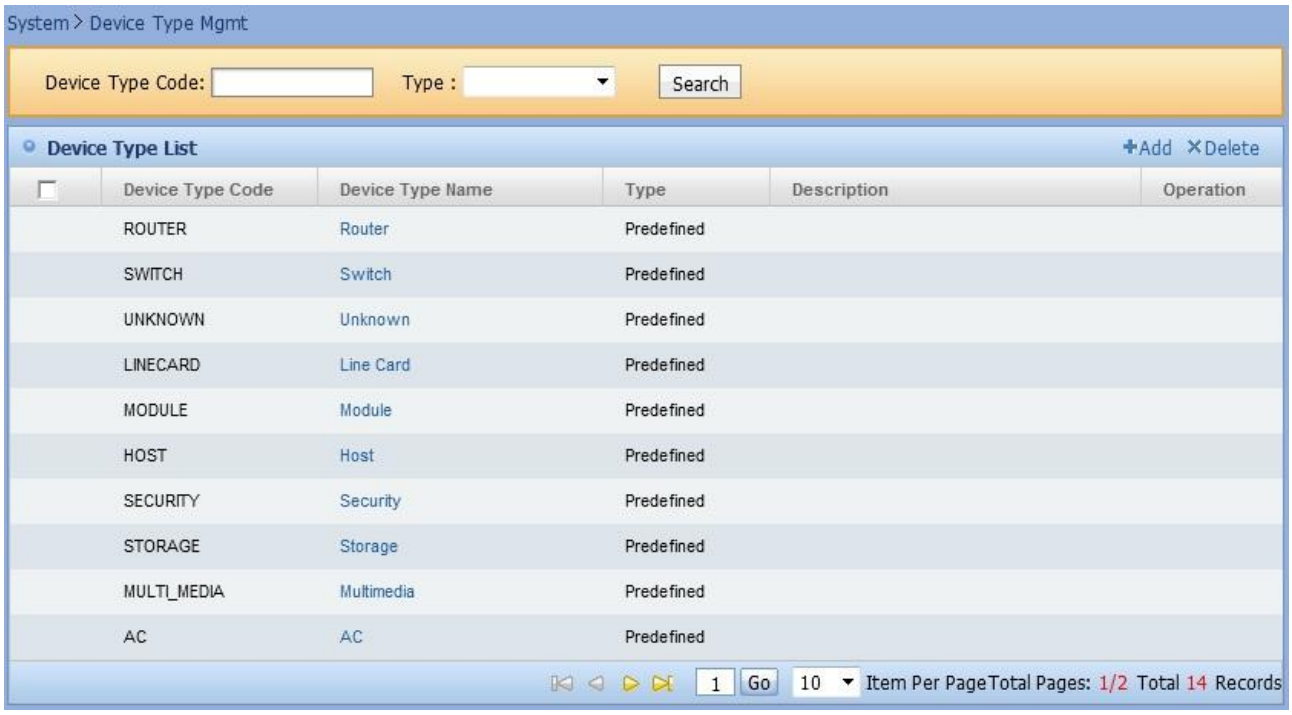


Figure 12.23. Device Type List

3) Choose at least one device type record, click **Delete** to perform the deletion operation.

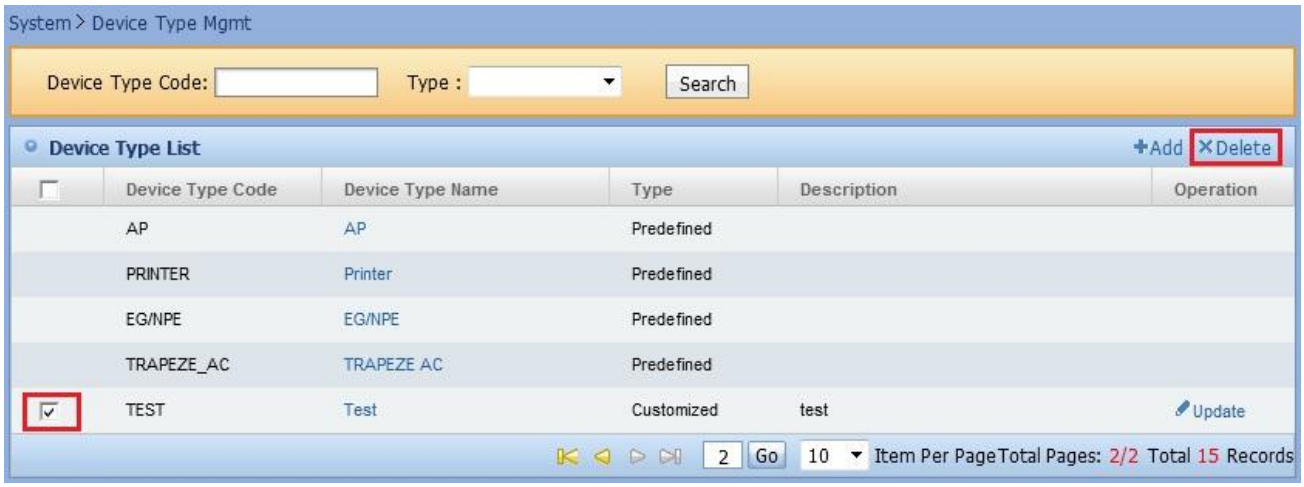


Figure 12.24. Delete Device Type

4) Click type name in the list to view info of the type.

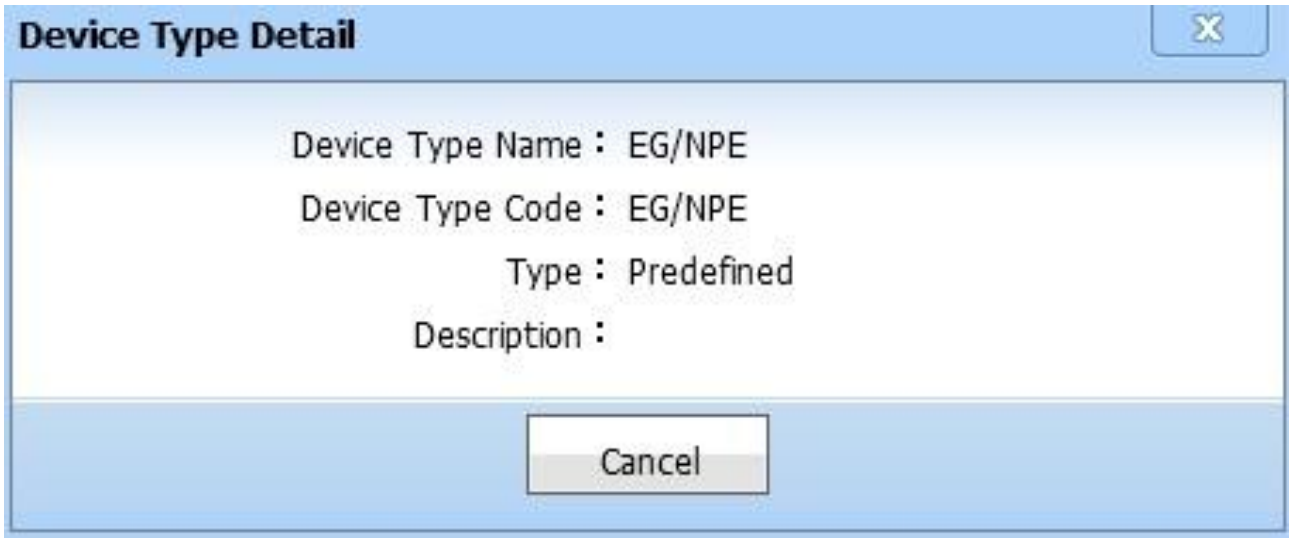


Figure 12.25. Device Type Detail

Note

Super administrator can add, delete, modify and search self-defined device type records.

Only self-defined device type can be deleted.

12.4.2. Add Device Type

On **Add Device Type** page, you can add device type info such as type name, type code, description and etc.

Operation Steps

1) On **Device Type List** page, click **Add** to enter **Add Device Type** page, as shown below:

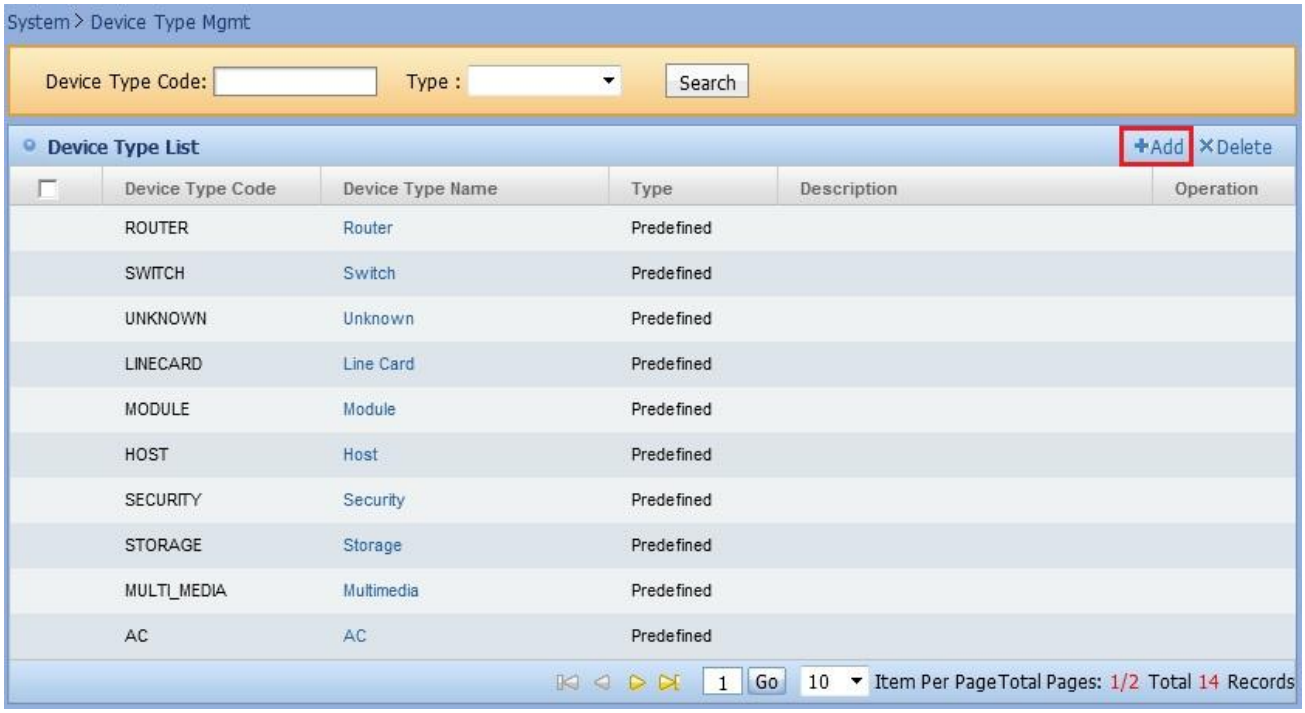


Figure 12.26. Device Type Page

2) Enter the device information, click **Save** to add a piece of type info, as shown below:

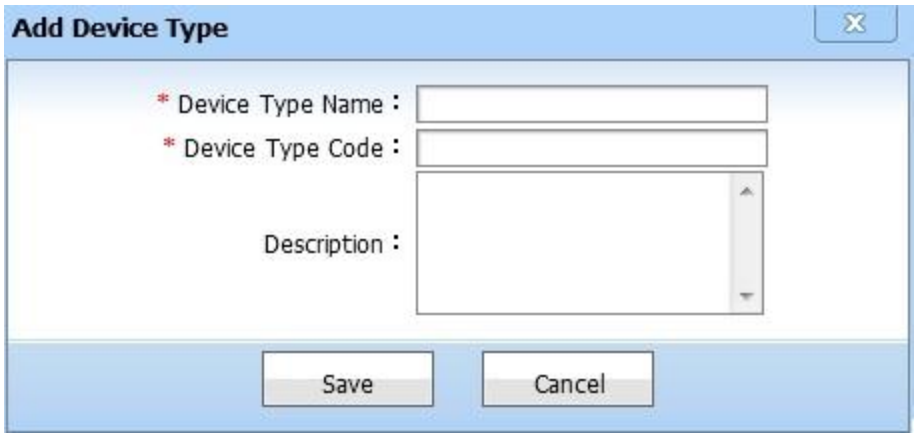


Figure 12.27. Add Device Type

Click **Cancel** button. The system will not save the entered device information, and will return to **Device Type List** page.

12.4.3. Modify Device Type

Type name, type code and description can be modified on **Modify Device Type Info** page.

Operation Steps

1) On **Device Type List** page, click **Update** icon of certain device type record in the list to enter Modify page, as shown below:

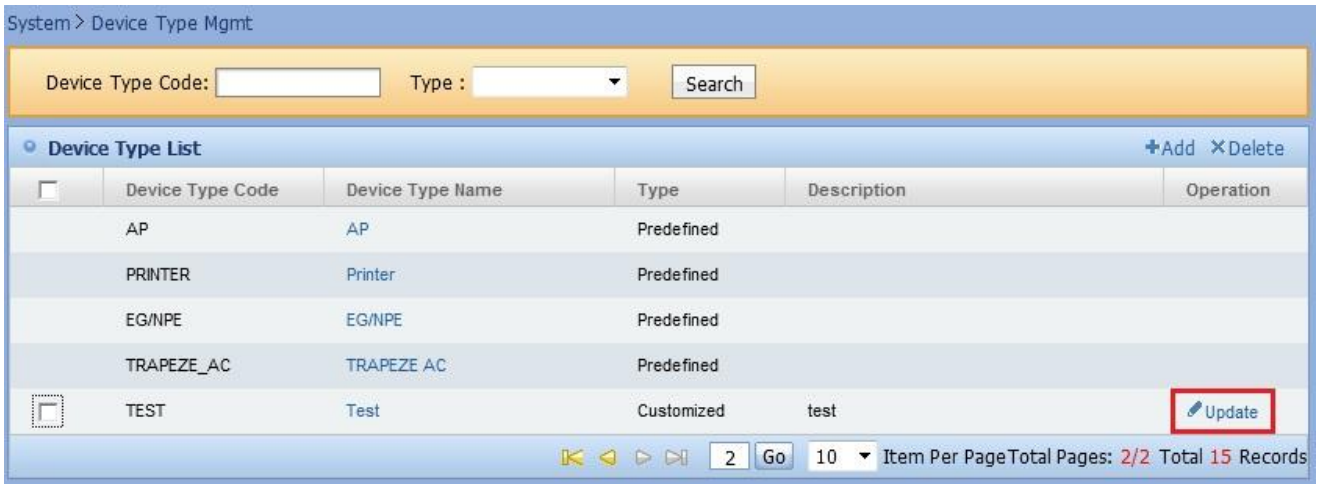


Figure 12.28. Enter Modify Device Type Page

2) If the type of a device type is **Pre-defined**, its info can be modified, as shown below:

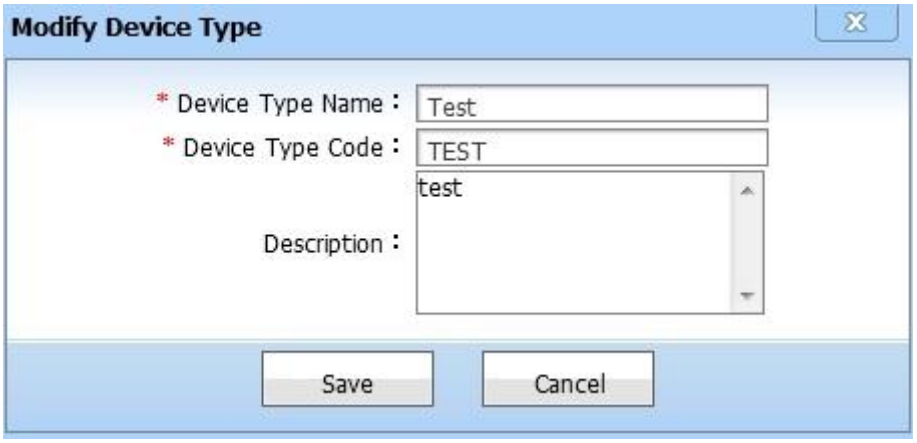


Figure 12.29. Modify Device Type (Pre-defined)

On **Modify Device Type** page, if **Cancel** is clicked, the system will not save the entered information, and will return to **Device Type List** page directly.

Note

Info of **Pre-defined** device type cannot be modified.

12.5. System Parameter Management

System Parameter Setting

Operation Steps

1) Click **System Parameter** in System Setting.

Figure 12.30. System Parameter Management

2) Modify system parameter.

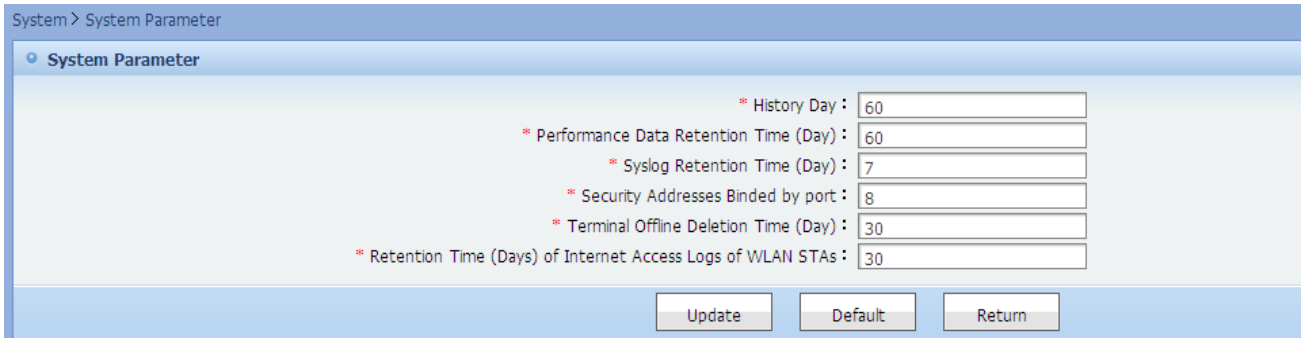


Figure 12.31. Modify System Parameter

Note

Use **Default** to restore system parameters to initial values if they are set wrongly.

12.6. Mail Server Setting

This function enables you to configure the Email server to send alarms to the specified Email box.

Operation Steps

1) Click **Mail Server Setting** in System Setting.

Figure 12.32. Mail Server Setting

2) Enter the mail server address, port number, mail user name, password, confirm password and mail destination address, and select whether authentication is required.

Configure the secondary mail server. When the primary server is not available, the secondary server sends the Email.

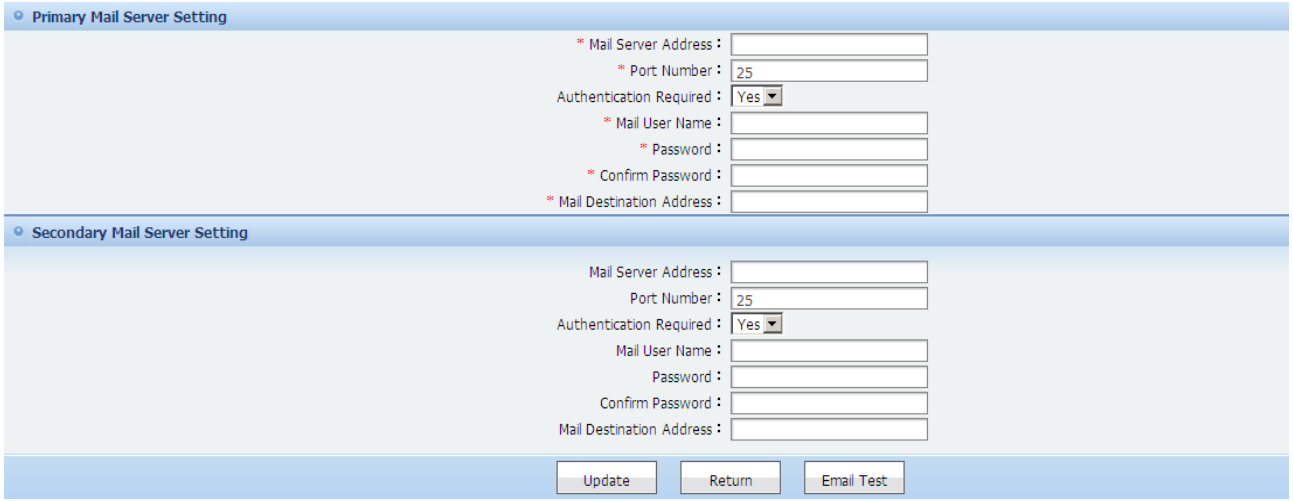


Figure 12.33. Mail Server Parameter Setting

Major operations in mail server setting include: Click Update to save the server setting.

Click **Return** to return to the System page.

Click **Email Test** to check whether the primary and secondary mail sever settings are correct.

Note This function is used to send alarm Emails.

12.7. Correlated Server Registration

This function enables you to register SAM, SMP and ESS servers launched by Ruijie to receive information about online users on a specific interface on a specific switch.

Operation Steps

1) Click **System** to go to the corresponding page. Click **SAM/SMP Register** in System Setting, as shown in the following figure:

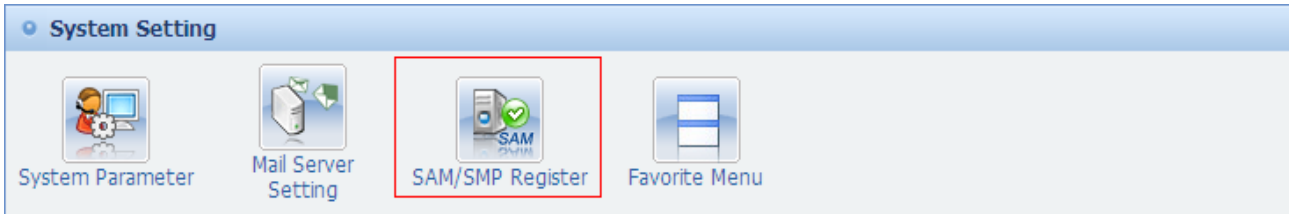


Figure 12.34. Correlated Server Registration

2) Major operations include registration and unregistration, as shown in the following figures: Registration: Select the server type and enter the server IP address. Click **Add**.
Unregistration: Click **Unregister** in Server List Registered.

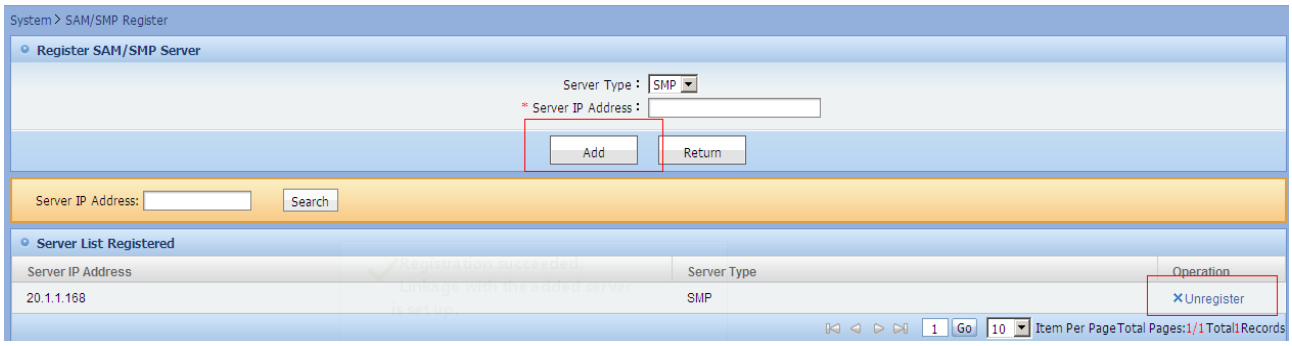


Figure 12.35. Registration/ Unregistration

Note

The system receives information about online users only with the SAM, SMP or ESS server registered.

The system does not receive information about online users once the SAM, SMP or ESS server is unregistered.

12.8. Software Upgrade Prompt

Software Upgrade Prompt is used to prompt users to download software upgrade package from FTP server when the system detects a new software version.

Operation Steps

On user login homepage, there will be prompt if the system detects a new software version.

Figure 12.36. Software Upgrade Prompt

Note

FTP server parameters in system management module need to be configured before Software Upgrade Prompt can work.

Software upgrade prompt will be closed automatically after 1 minute.

12.9 Favorite Menu

Favorite Menu is for users to collect frequently used functionalities.

Operation Steps

1) Click **Favorite Menu** in System Setting to view favorite menu list.

Figure 12.37. Favorite Menu

Figure 12.38. Menus in Favorite

2) Users can add menus to favorite. Click **Add** to show menus in the system which are not in favorite.

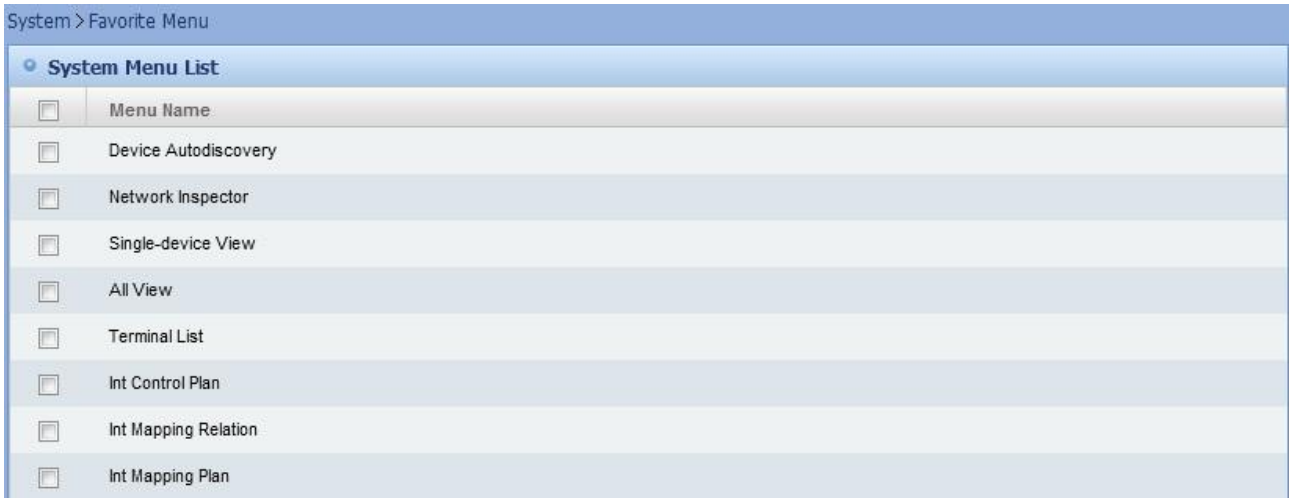


Figure 12.39. Menus not in Favorite

3) Select items and click **Save**. The selected menus will be added to favorite.

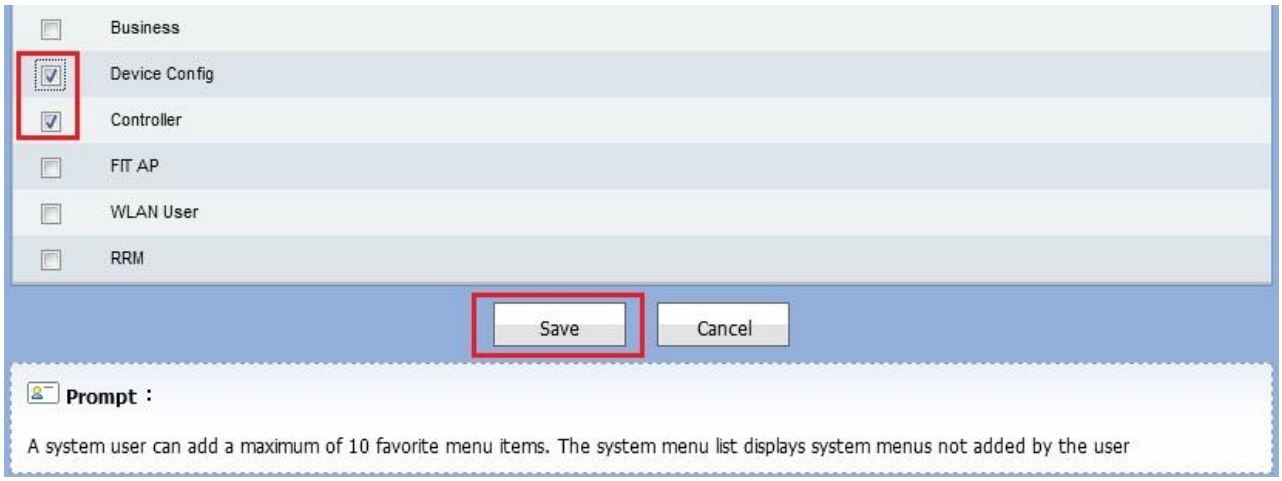


Figure 12.40. Save Favorite Menu

4) Saved favorite menus will be shown on a fixed position on upper left corner of the system.

Figure 12.41. Favorite Menu

Note System users can add up to 10 menus.

12.10. Administrator Management

The system comes with a super administrator and an audit administrator, which cannot be deleted. There can be only one super administrator and one audition administrator in the system. Super administrator is the only user who can manage administrators and grant permissions to administrators. Super administrator, audit administrator and system administrator can change their passwords.

Operation Steps

1) Click **Admin Mgmt** in Admin Mgmt.

Figure 12.42. Administrator Management

2) System administrator list.

Figure 12.43. System Administrator List

3) Super administrator adds an administrator.

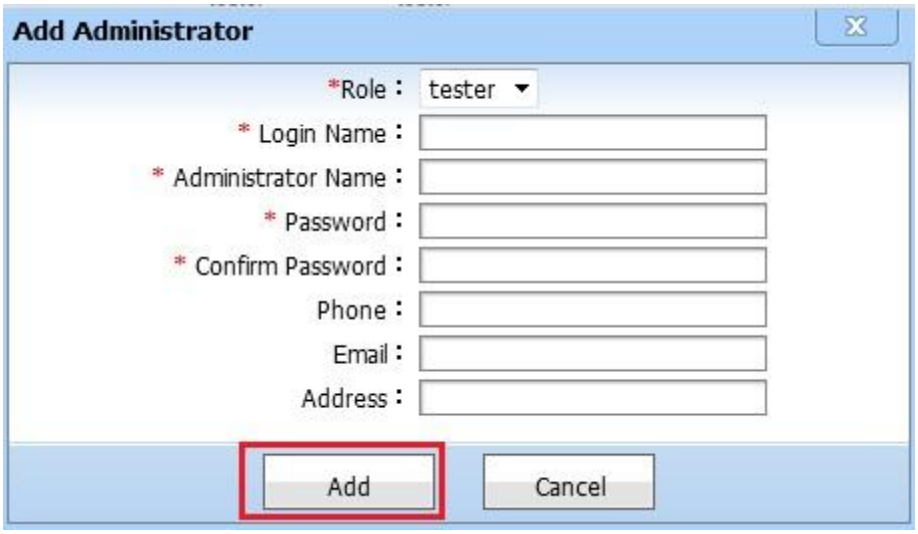


Figure 12.44. Add Administrator

4) Super administrator can delete administrators.

Figure 12.45. Delete Administrator

5) Super administrator can reset passwords of administrators.

Figure 12.46. Password Resetting

Figure 12.47. Password Resetting

Note

Remember the password when changing super administrator password.

The system comes with super administrator (login name is admin) and audit administrator (login name is auditor).

12.11. Role Management

This function enables you to divide users into different **role** groups and grant different permissions to different roles to facilitate permission management.

Operation Steps

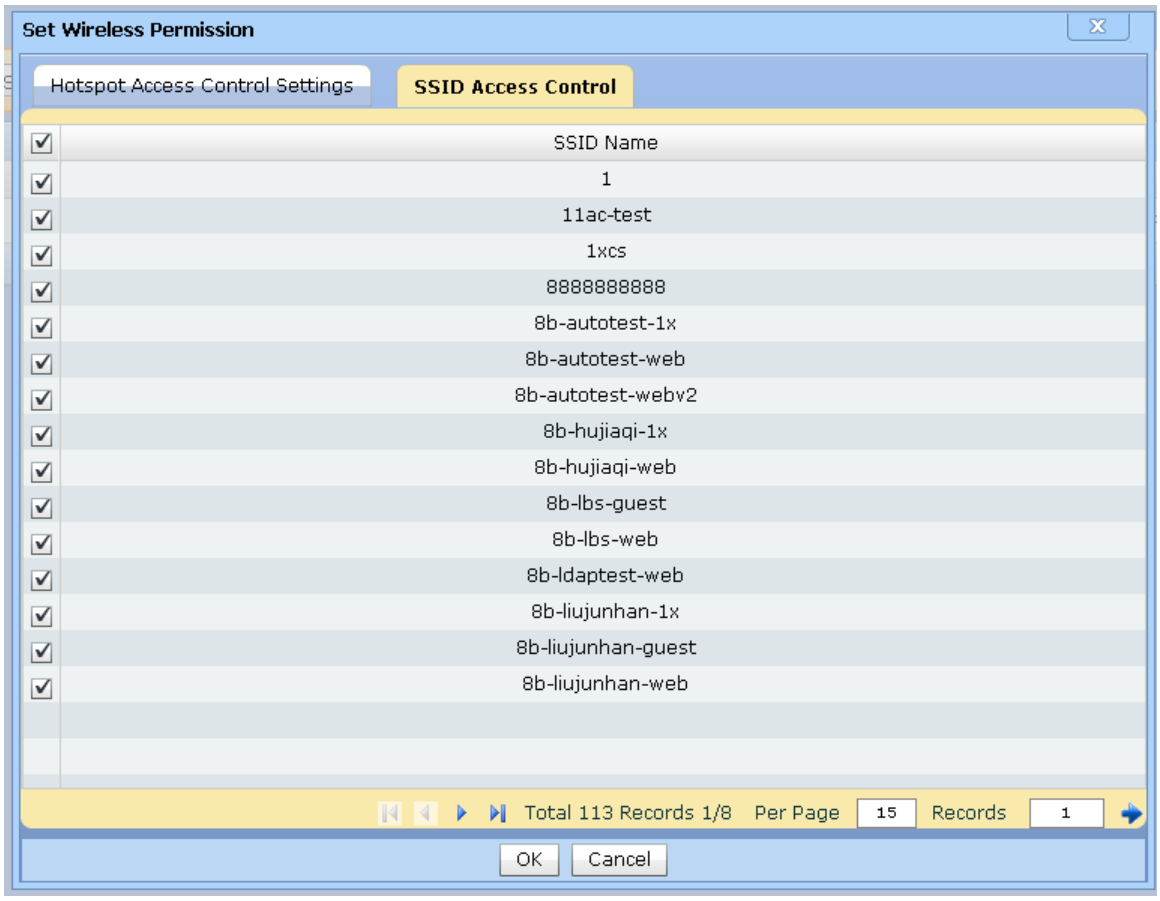


Figure 12.58. SSID Permission Setting

1) Click **Role Mgmt** in Admin Mgmt, as shown in the following figure:

Figure 12.48. Role Management

2) Role List is displayed, as shown in the following figure:

Figure 12.49. Role List

3) Click **Add**, and enter the role name and description on the page displayed, as shown in the following figure:

Figure 12.50. Adding Role

4) A role not configured with the administrator or permission can be deleted, as shown in the following figure:

Figure 12.51. Deleting Role

5) Click **Add**, and add the administrator on the page displayed, as shown in the following figure:

Figure 12.52. Administrator Setting

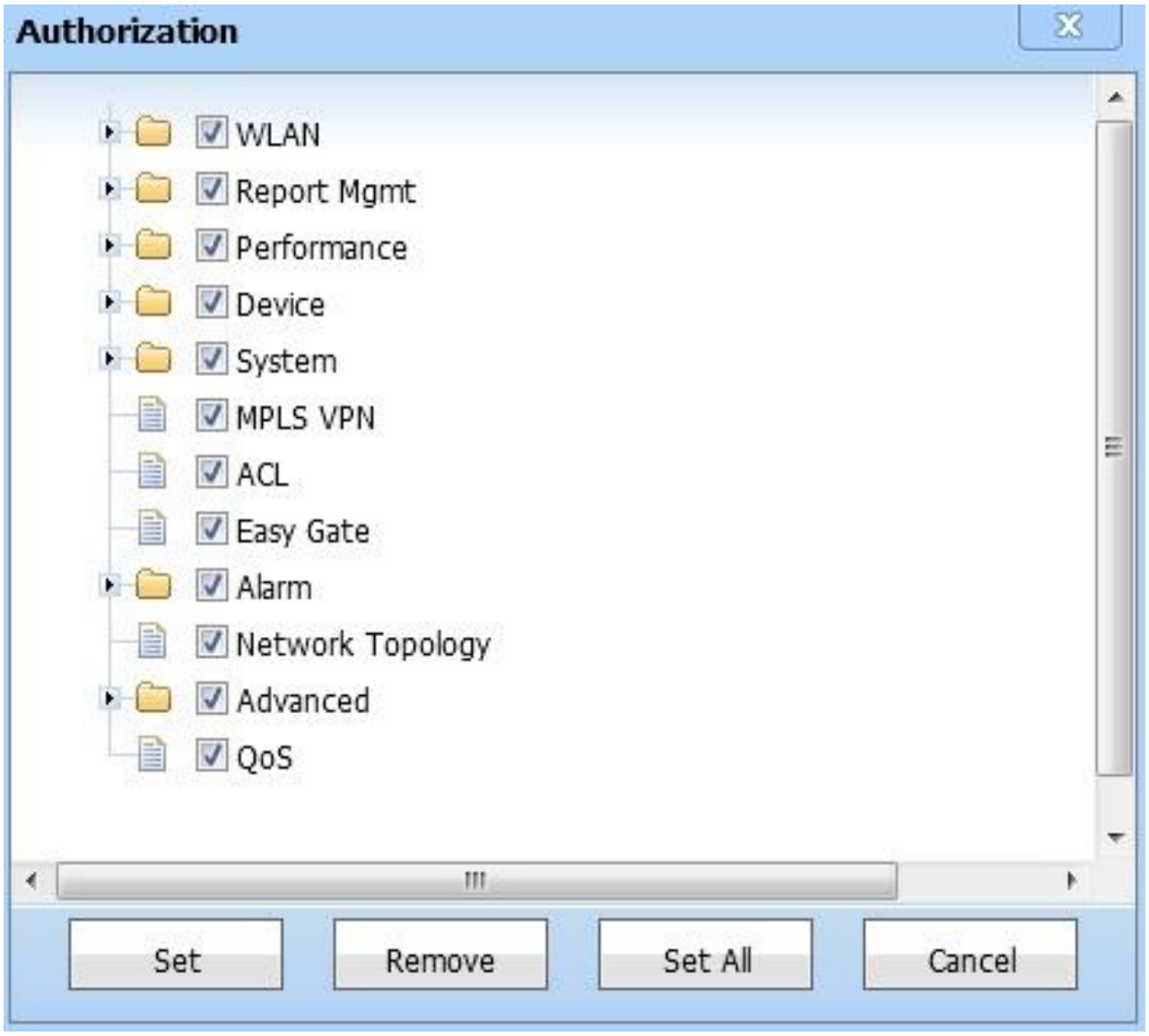


Figure 12.53. Permission Setting

6) Click **Read/Write Privilege**, and modify the permission on the device for the role on the page displayed, as shown in the following figure:

Figure 12.54. Configuring Device Permission

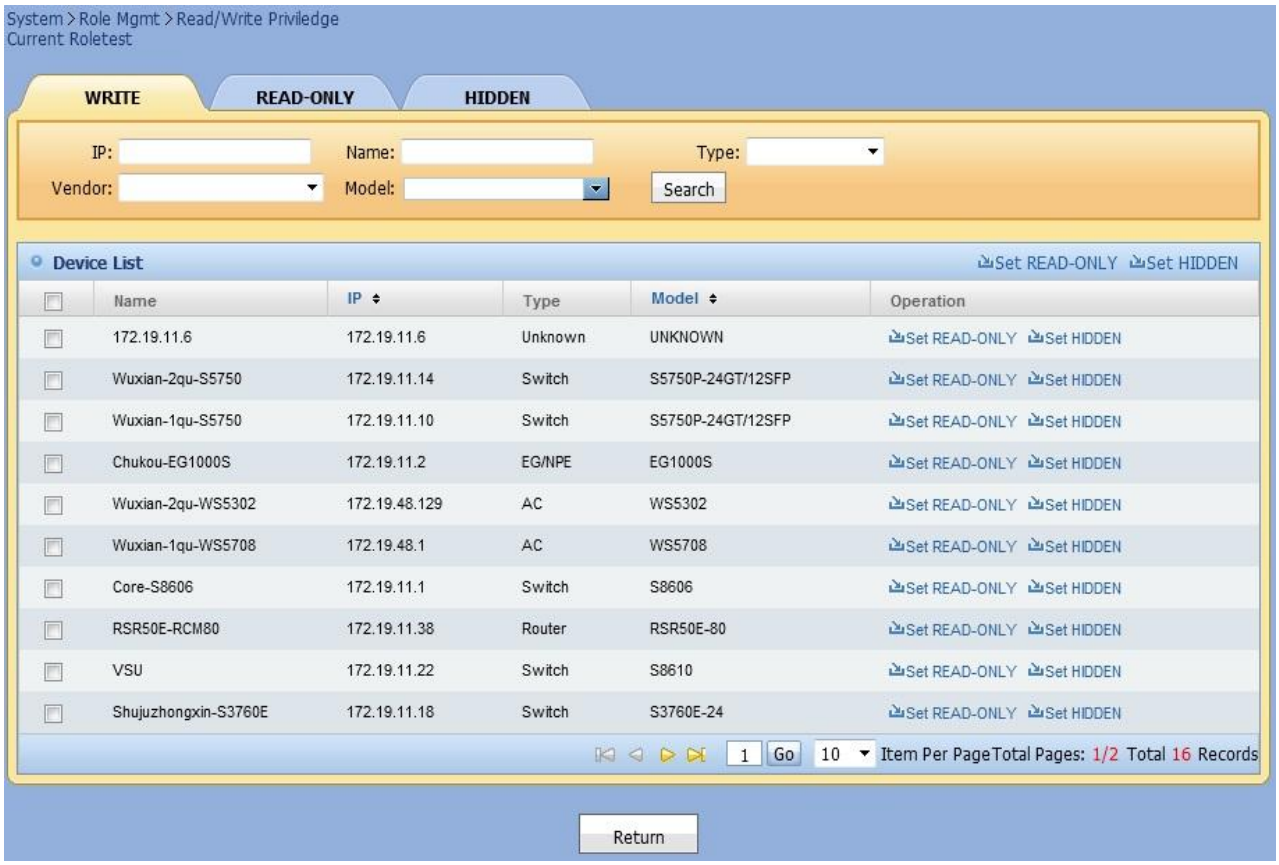


Figure 12.55. Saving Device Permission

7) Click **Set Wireless Permission**, and configure wireless permission for the role entitled to wireless administration, including hotspot permission and SSID permission.

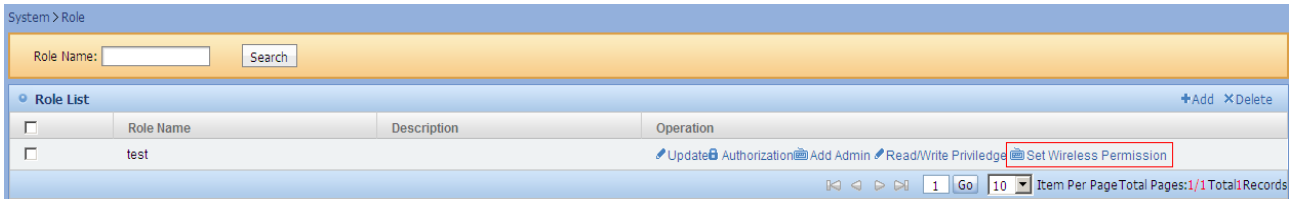


Figure 12.56. Wireless Permission Setting

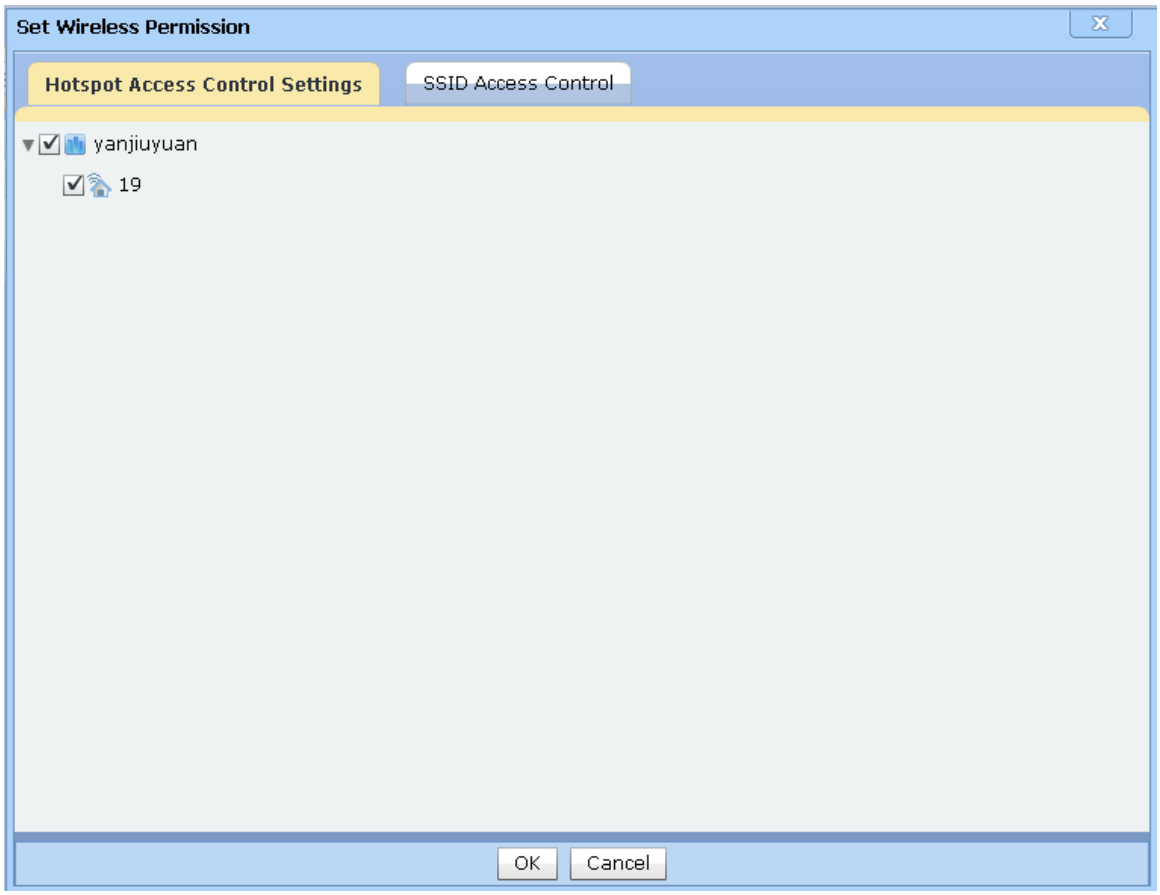


Figure 12.57. Hotspot Permission Setting

Note

If you want to configure role permissions, the role administrator should be configured first.

If you want to delete a role, the administrator and permission corresponding to the role should be removed first.

If you want to add a role, the role name cannot be duplicate.

12.12. Change Password

Administrators can modify their own passwords.

Operation Steps

1) Click **Change Password** in Admin Mgmt.

Figure 12.59. Change Password

2) Enter the old password, and then enter the new password twice. Click **Save** to change password for current administrator. Click **Cancel** to return to system management page.

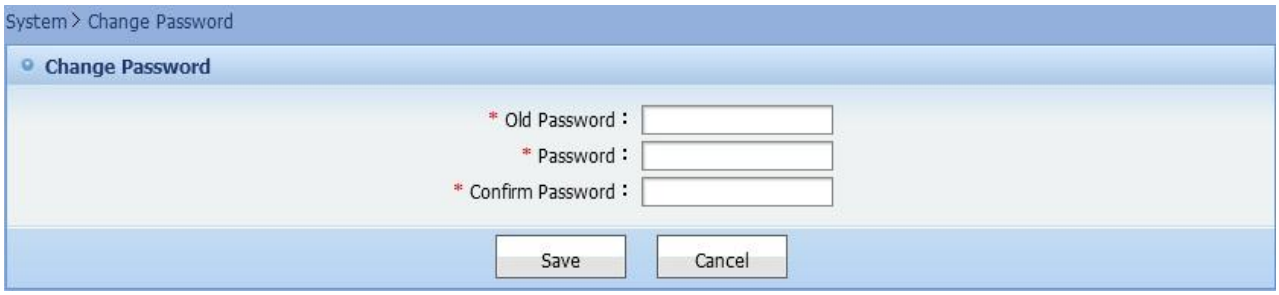


Figure 12.60. Change Password

Note Please be sure to remember the password when changing super administrator password.

12.13. Concurrent Logon Control

By default, one administrator is only allowed to have one logon session in the system. The maximum number of concurrent logon sessions can be 10 by Concurrent Logon Control.

Operation Steps

1) Click **Concurrent Control** in Admin Mgmt.

Figure 12.61. Concurrent Logon Control

2) Update Concurrent Logon Control

Figure 12.62. Update Concurrent Logon Control

12.14. Security Log

Security Log keeps access logs for administrators login. Each log includes login name, administrator name, security operation (login or logout), operation result, operation time, additional message and session ID.

Operation Steps

1) Click **Security Log** in system management to view security log list.

Figure 12.63. Security Log

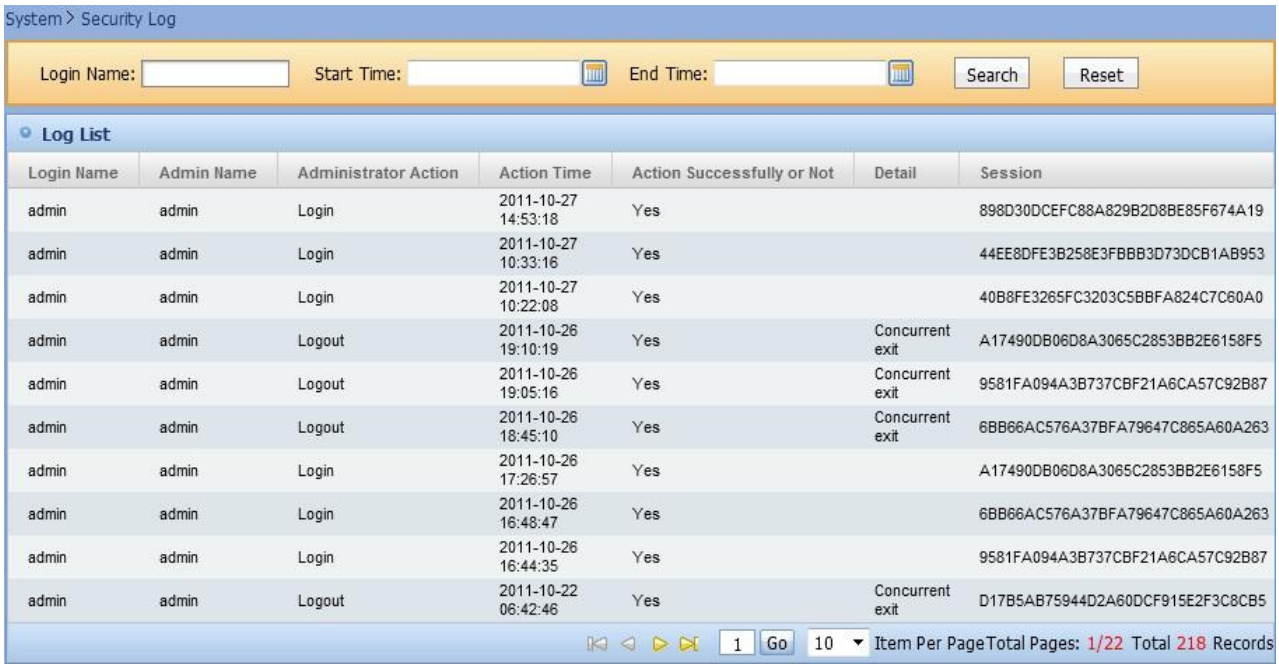


Figure 12.64. Security Log List

2) Click **Export Search Results** to export current logs to local as axles file.

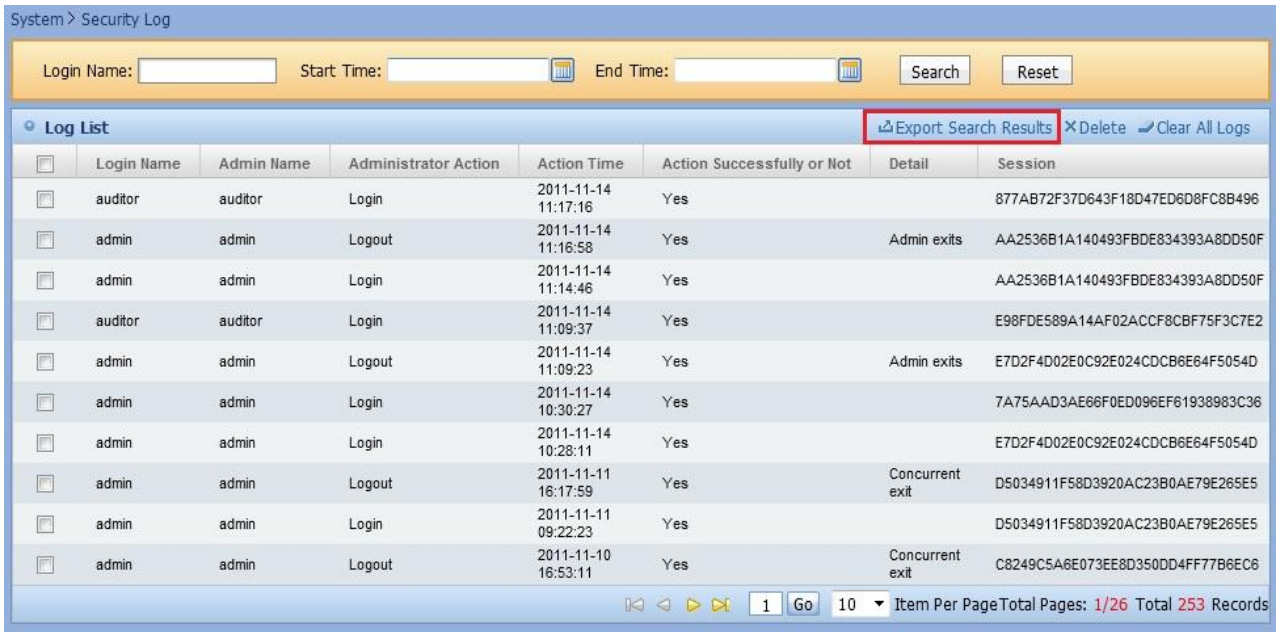


Figure 12.65. Export Search Result

3) Click **Log File Download** to open the file or save it locally. Click **Return** to return to security log list.

Figure 12.66. Save to Local

4) Click **Clear All Logs** to delete all security logs.

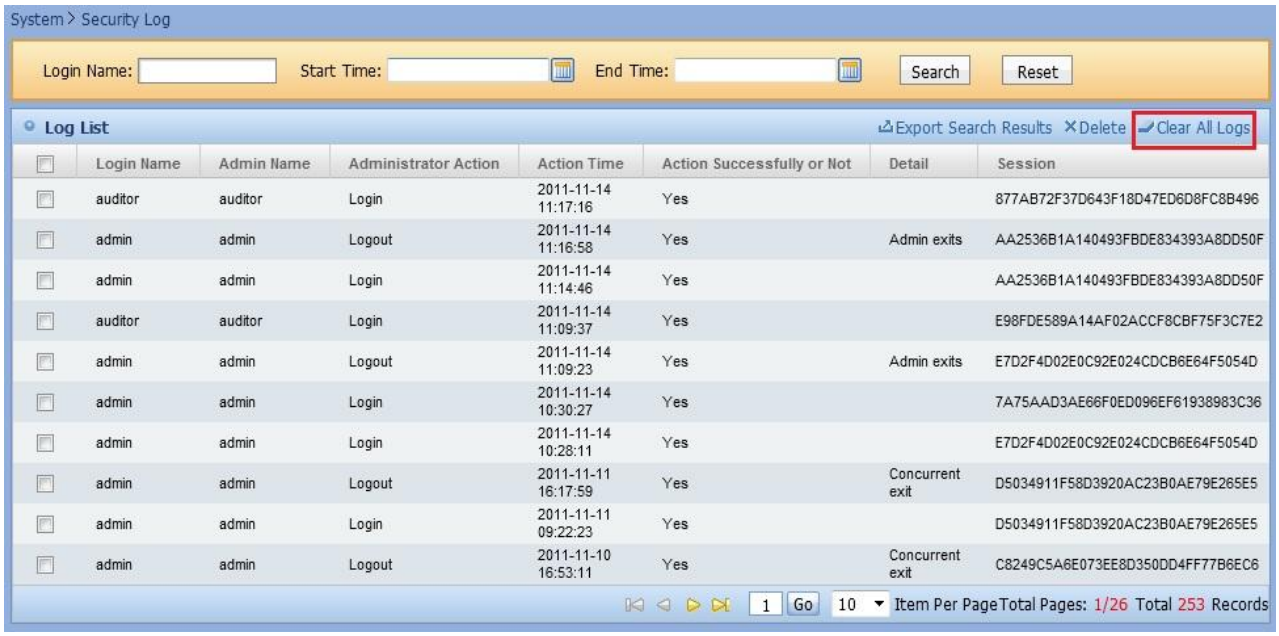


Figure 12.67. Clear All Logs

Note

Security log detail info instructions

Concurrency Exit: If a user logs in repeatedly, the last login will be forced to log out by the system.

Session Expired: If a user performs no operation for a long time after login or close the page instead of clicking Exit, the user will be forced to log out by the system.

User Exit: A user click Exit after login.

Password Error: A user inputs wrong password when login.

12.15. Plan Execution Log

Plan Execution Log keeps logs for plan execution. Each log includes plan name, scheduled start time, actual start time, actual end time, execution state, completion situation, and completion description.

Operation Steps

1) Click **Plan Execution Log** in system management to view plan execution log list.

Figure 12.68. Plan Execution Log

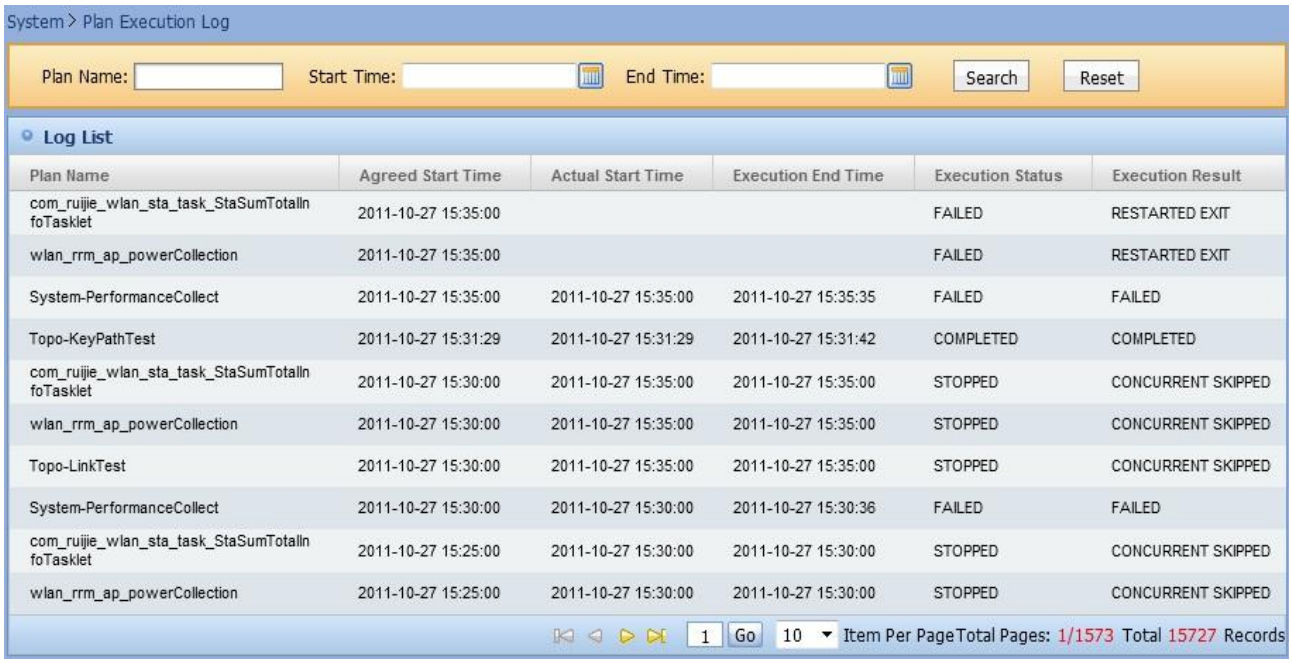


Figure 12.69. Plan Execution Log List

2) If current login user is auditor, the user can click **Export Search Results** to export current logs to local as caves file.

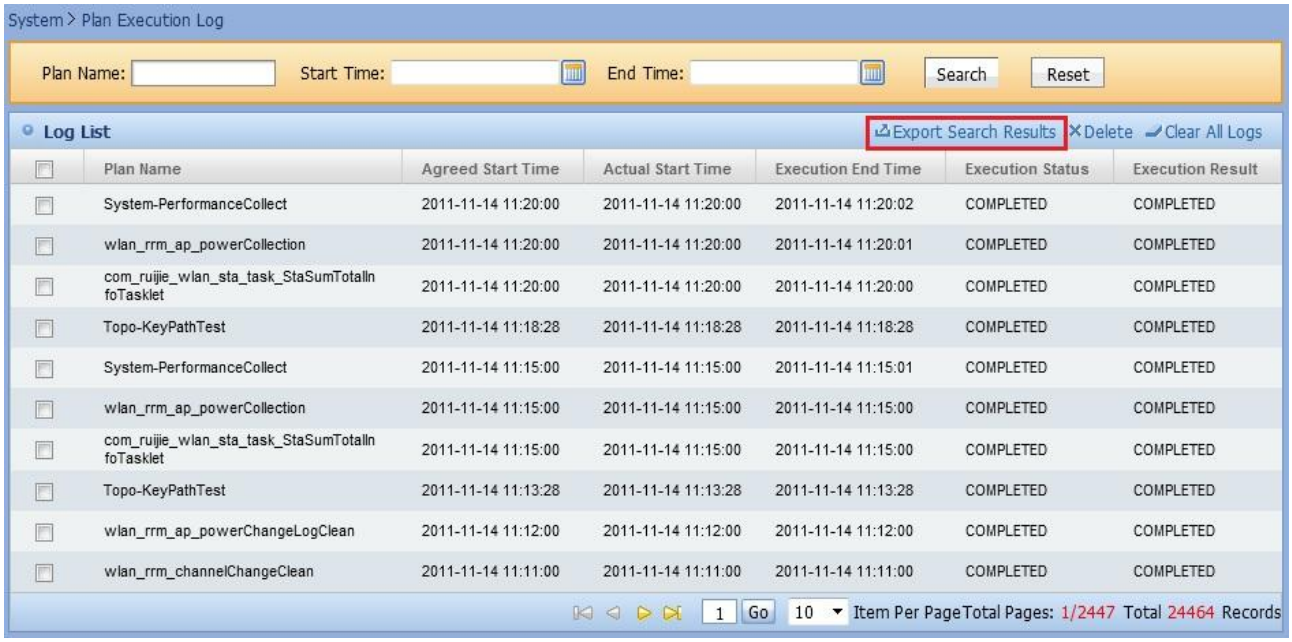


Figure 12.70. Export Search Result

3) Click **Log File Download** to open the file or save it locally. Click **Return** to return to Plan Execution Log List.

Figure 12.71. Save to Local

4) If current login user is auditor, the user can click **Clear All Logs** to delete logs of all plans which have finished running.

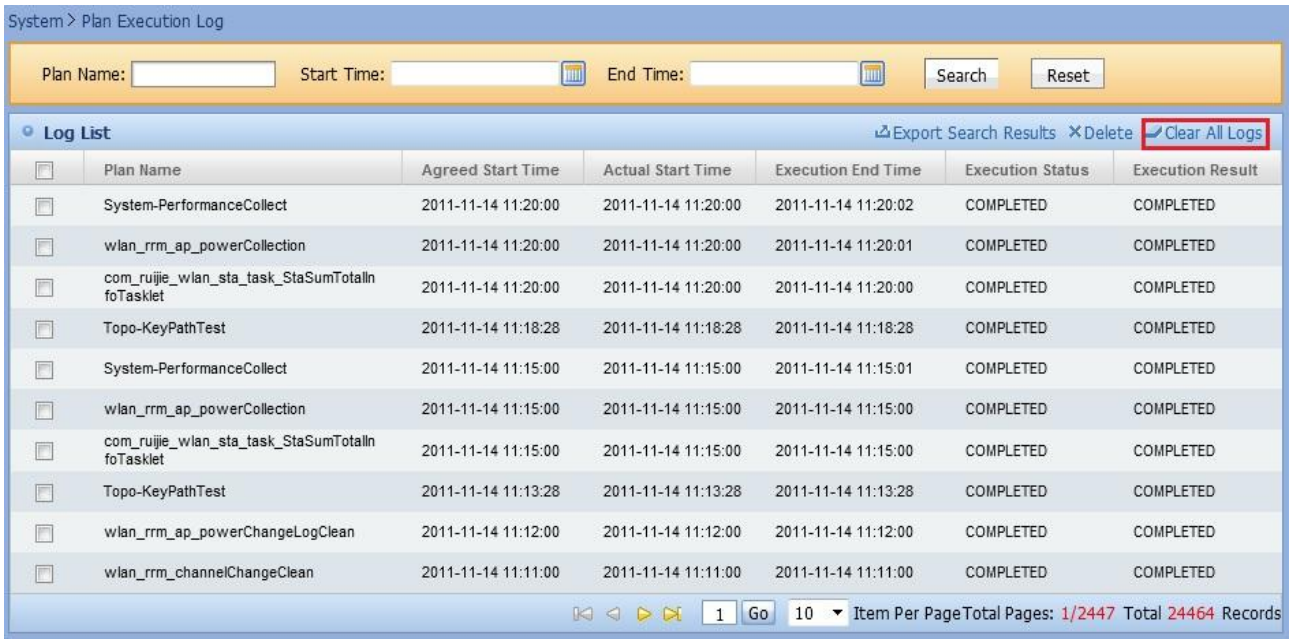


Figure 12.72. Clear All Logs

Note

Plan log execution state instructions

Common states are as follows: Unknown, Starting, Executing, Complete.

If failed, states are as follows: Unknown, Starting, Executing, Failed.

If stopped, states are as follows: Unknown, Starting, Executing, Stopping, Stopped.

Plan log completion instructions

Executing: The plan is being executed.

Succeeded: Plan execution succeeded. Note: This does not necessarily mean operations on every device succeeded.

Failed: Plan execution failed. The usual cause is system exception.

Expiration Skip: If the time difference between plan start time and scheduled time is greater than 5 minutes, the execution will be skipped.

Exception Exit: In plan execution, the execution exits if operation on some device fails.

Concurrency Exit: If one run of periodical plan takes longer than the interval of the plan, subsequent run of the periodical plan will be blocked.

Restart Exit: When plan scheduling service is restarted, the system will set completion situation of plans whose execution states are Unknown, Starting, Executing and Stopping to be Restart Exit.

Stop Exit: Plan is stopped by users when it is being executed.

Plan category and search instructions

Plan has two categories: system plan and user plan.

System plan is pre-defined in the system, which cannot be deleted or modified by users.

User plan is defined by users, which can be deleted and modified.

12.16. Change Log

Change Log function records logs of admin operations. Each log includes admin name, operation, change time and change result.

Operation Steps

1) Click **Change Log** in System Management to view change log list.

Figure 12.73. Change Log

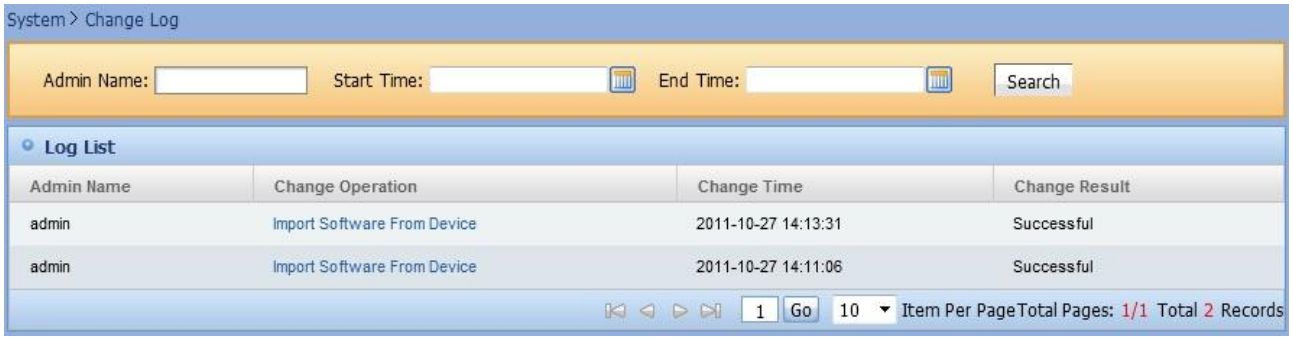


Figure 12.74. Change Log List

2) Click **Export Search Results** to export current log list to local as axles file.

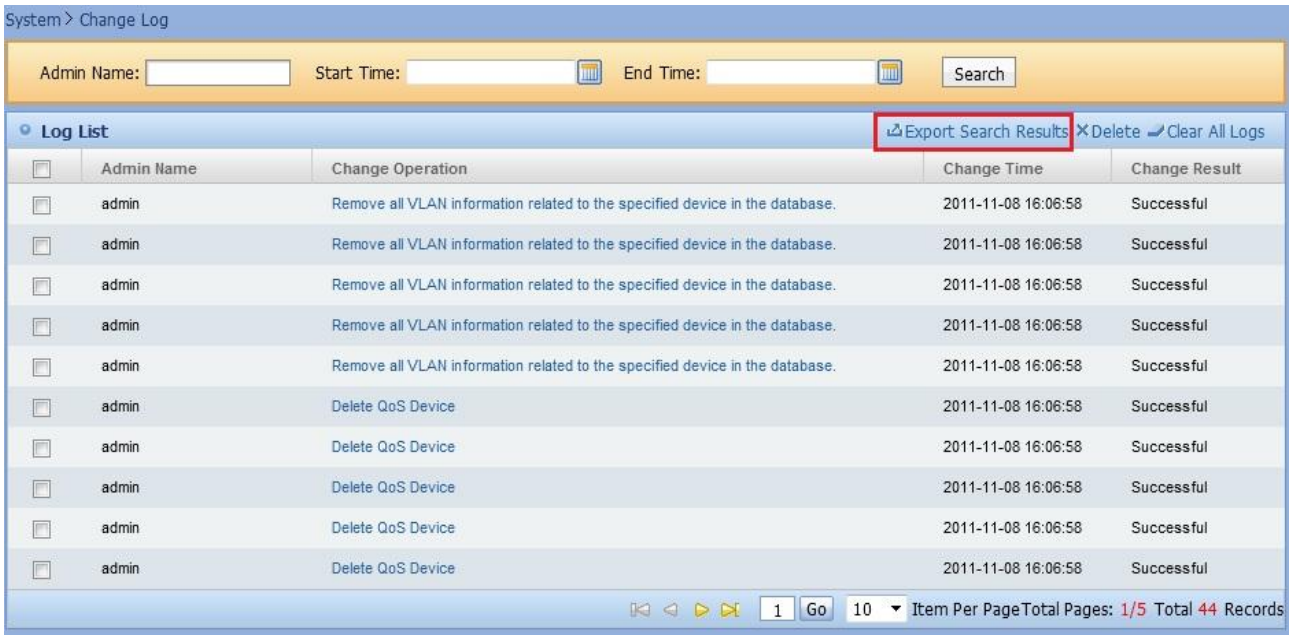


Figure 12.75. Export Search Result

3) Click **Log File Download** to open the file or save it locally. Click **Return** to return to change log list.

Figure 12.76. Save to Local

4) Click **Clear All Logs** to clear all change logs.

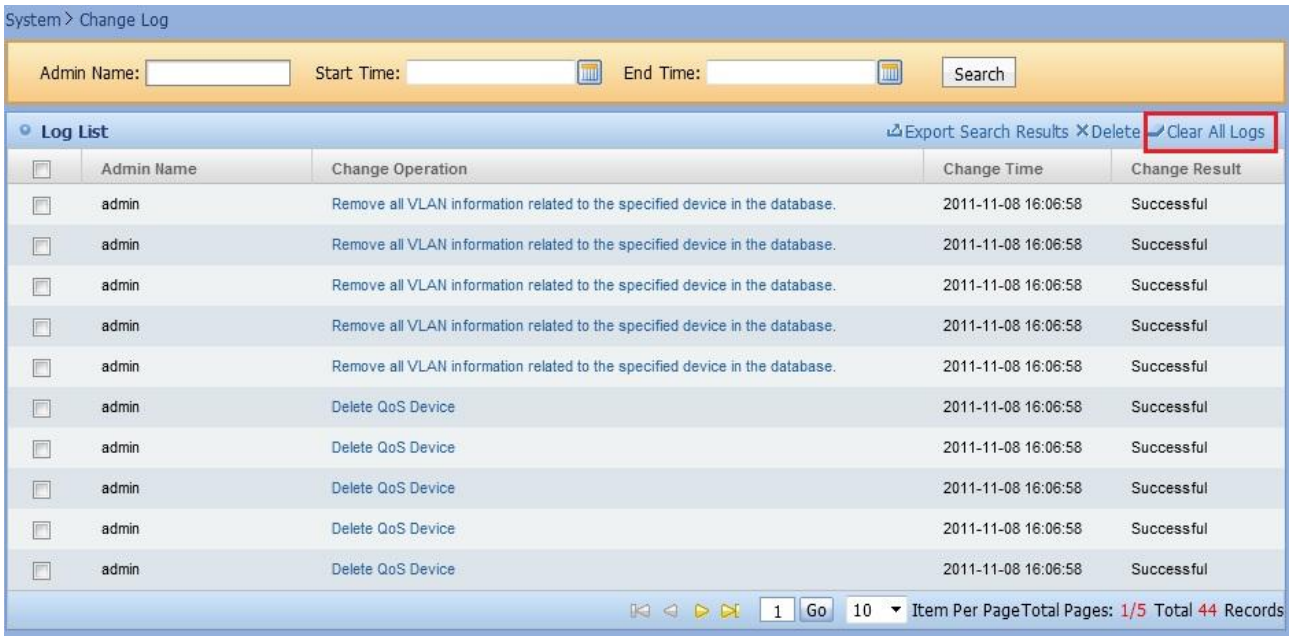


Figure 12.77. Clear All Logs

Note This function mainly records logs of VLAN operations.

12.17. Device Software Summary

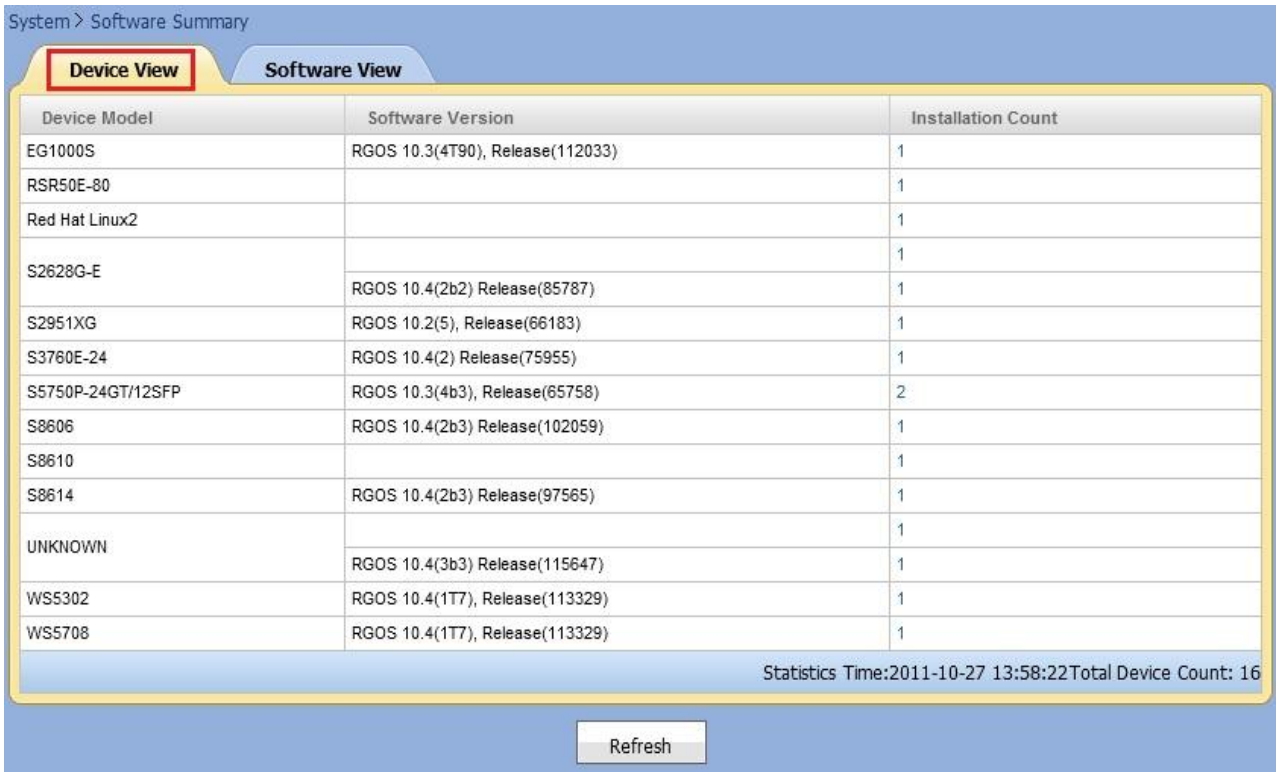
View current device software summary report of the system. The summary is divided into device model view and device software version view.

Operation Steps

1) Click **Software Summar**y in System management.

Figure 12.78. Device Software Summary

2) Summary by device model view.

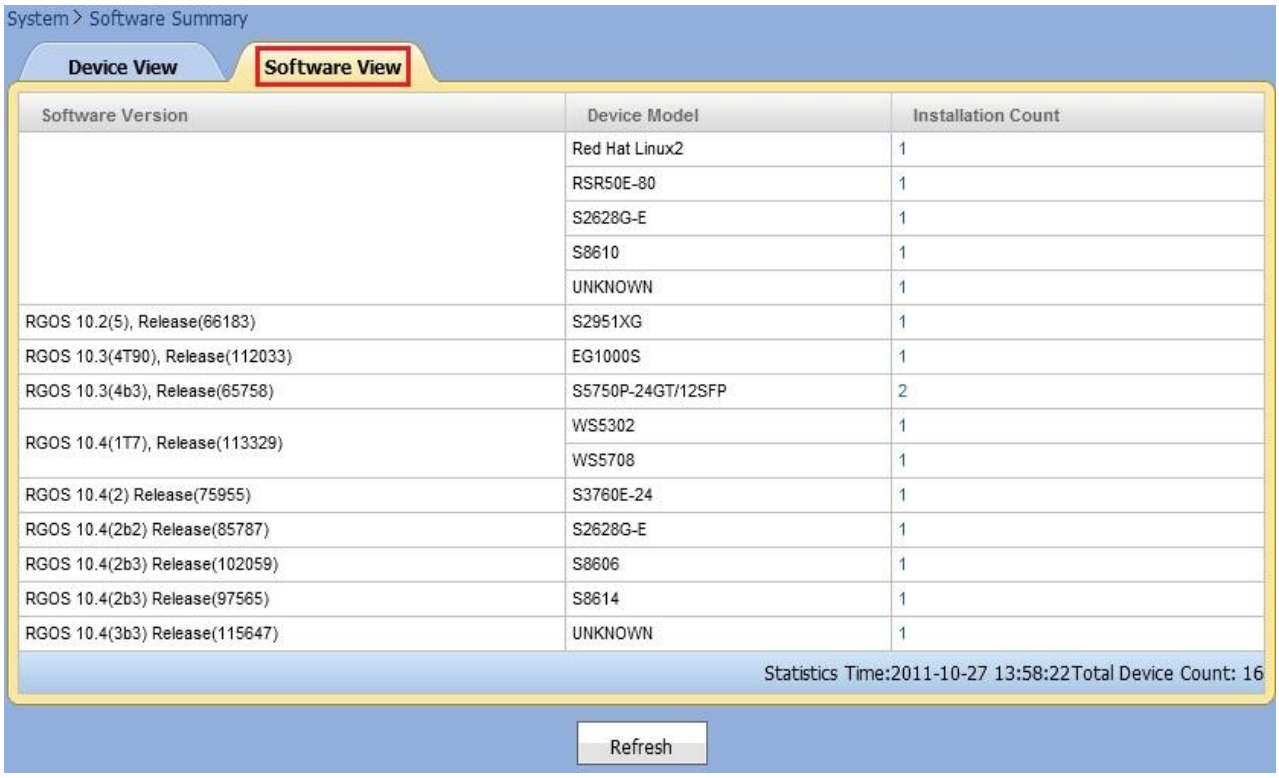


Device Model	Software Version	Installation Count
EG1000S	RGOS 10.3(4T90), Release(112033)	1
RSR50E-80		1
Red Hat Linux2		1
S2628G-E		1
	RGOS 10.4(2b2) Release(85787)	1
S2951XG	RGOS 10.2(5), Release(66183)	1
S3760E-24	RGOS 10.4(2) Release(75955)	1
S5750P-24GT/12SFP	RGOS 10.3(4b3), Release(65758)	2
S8606	RGOS 10.4(2b3) Release(102059)	1
S8610		1
S8614	RGOS 10.4(2b3) Release(97565)	1
UNKNOWN		1
	RGOS 10.4(3b3) Release(115647)	1
WS5302	RGOS 10.4(1T7), Release(113329)	1
WS5708	RGOS 10.4(1T7), Release(113329)	1

Statistics Time:2011-10-27 13:58:22Total Device Count: 16

Figure 12.79. Device Model View

3) Summary by device software version view.



Software Version	Device Model	Installation Count
	Red Hat Linux2	1
	RSR50E-80	1
	S2628G-E	1
	S8610	1
	UNKNOWN	1
RGOS 10.2(5), Release(66183)	S2951XG	1
RGOS 10.3(4T90), Release(112033)	EG1000S	1
RGOS 10.3(4b3), Release(65758)	S5750P-24GT/12SFP	2
RGOS 10.4(1T7), Release(113329)	WS5302	1
	WS5708	1
RGOS 10.4(2) Release(75955)	S3760E-24	1
RGOS 10.4(2b2) Release(85787)	S2628G-E	1
RGOS 10.4(2b3) Release(102059)	S8606	1
RGOS 10.4(2b3) Release(97565)	S8614	1
RGOS 10.4(3b3) Release(115647)	UNKNOWN	1

Statistics Time:2011-10-27 13:58:22Total Device Count: 16

Figure 12.80. Software Version View

4) Click the installation count in summary list to view devices of the same model and software version existing in the system.

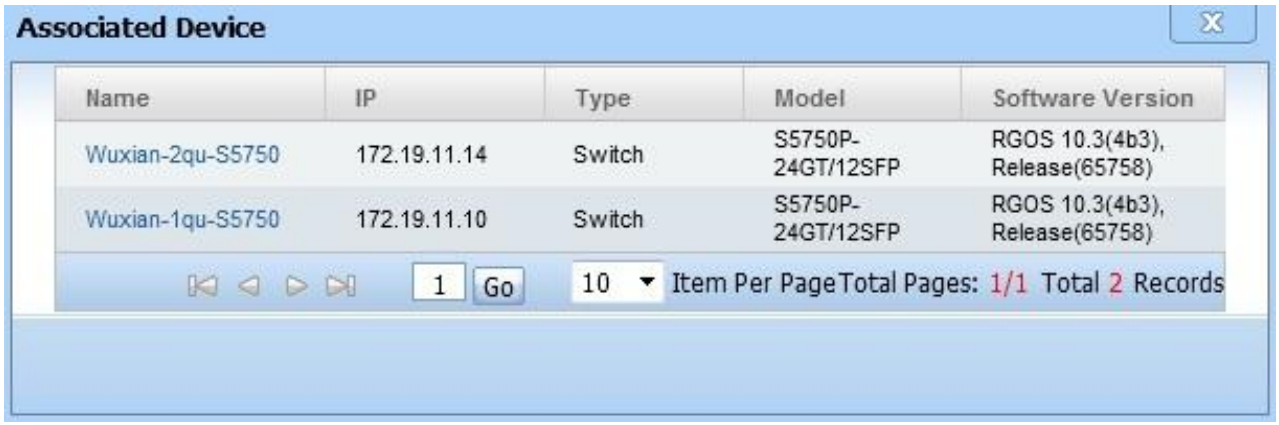


Figure 12.81. Associated Device

5) Click **Refresh** to recount devices info in the system and refresh device software summary report.

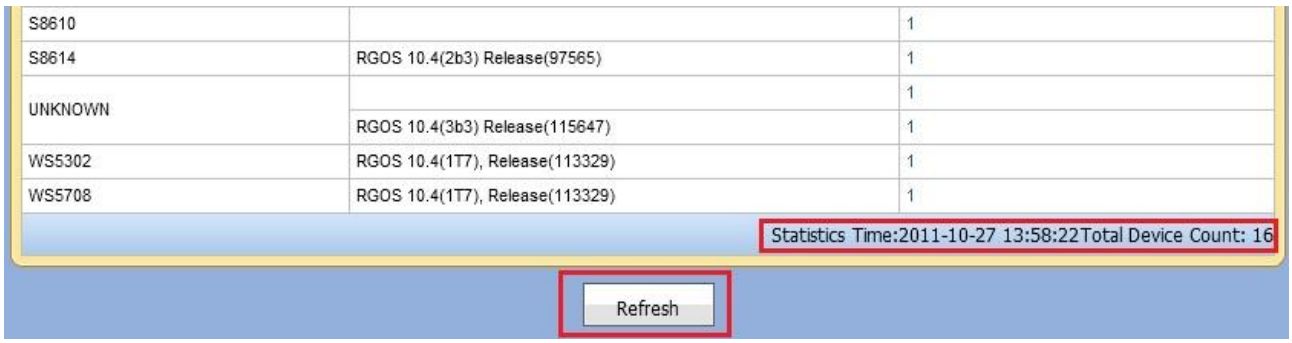


Figure 12.82. Device Software Summary Report (Before Refresh)

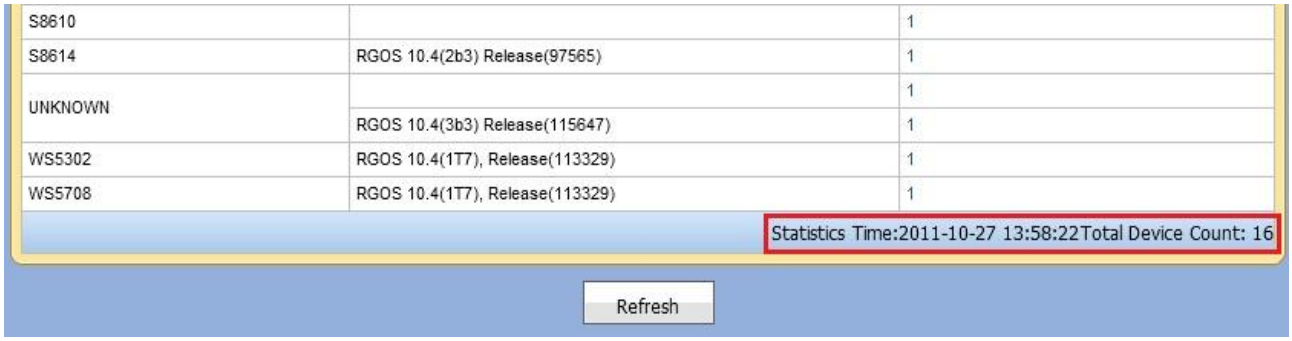


Figure 12.83. Device Software Summary Report (After Refresh)

Note This function applies to software version distribution of Ruijie devices only.

12.18. VLAN Summary Report

View the VLAN summary report.

Steps

1) Click the **VLAN Summary Report** in system management.

Figure 12.84. VLAN Summary Report

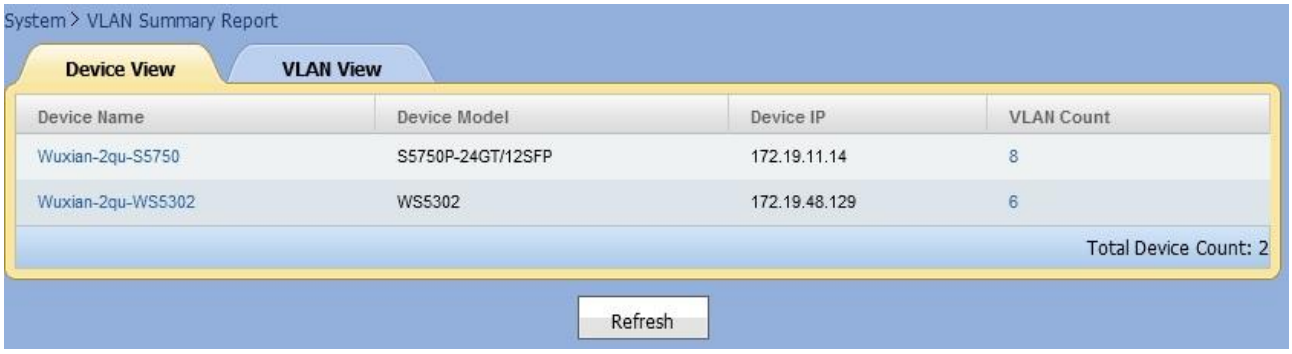


Figure 12.85. View the report from the perspective of the device

2) View the detail information of the interface from the perspective of the device.

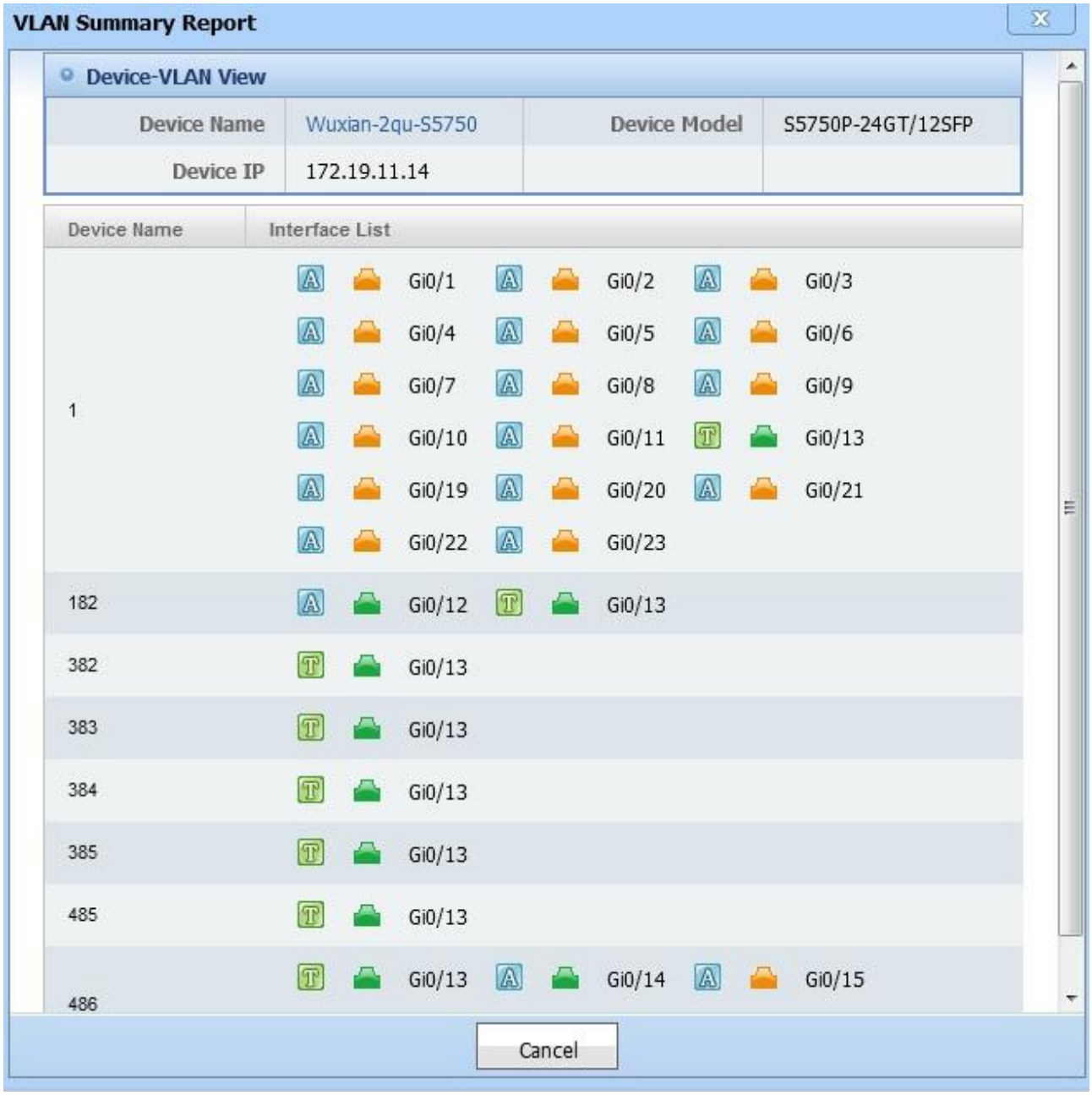


Figure 12.86. detail information of the interface

Figure 12.87. View report from the perspective of the VLAN

3) View device detail information from the perspective of the VLAN.

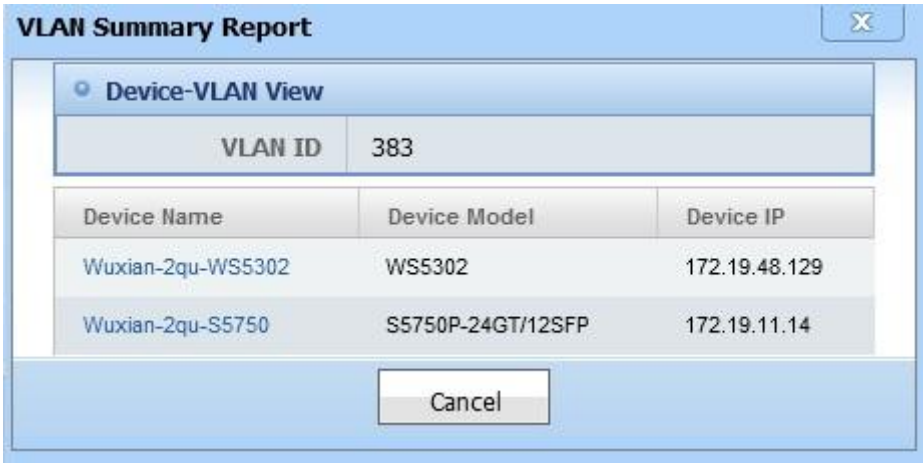


Figure 12.88. device detail information

12.19. SMS Modem Setting

SMS Modem Setting.

SMS Modem

1) Click **SMS Modem Setting** in System.

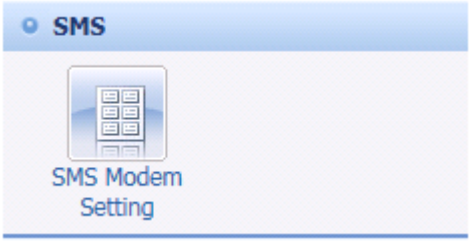


Figure 12.89. SMS Modem Setting

2) Check **SMS Setting**.

Figure 12.90. Check SMS Setting

3) Enter the information of SMS modem.

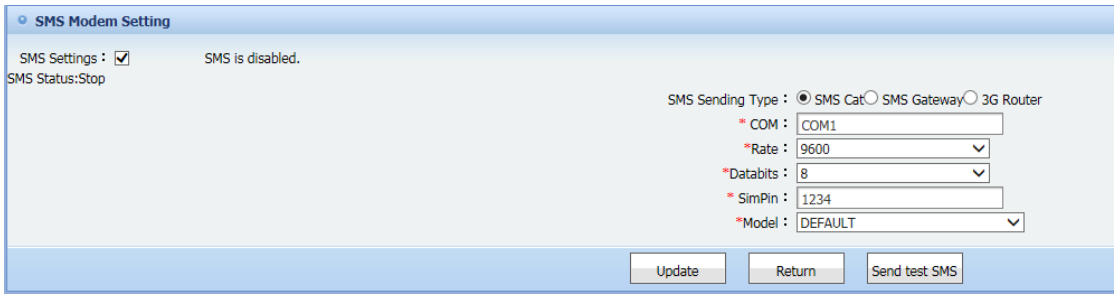


Figure 12.91. Enter the information of SMS Modem

SMS Gateway

1) Click **SMS Modem Setting** in System.

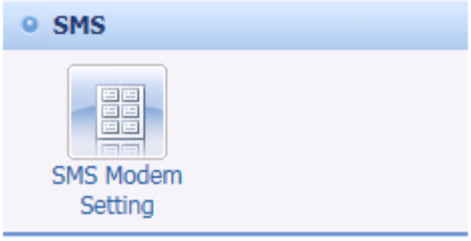


Figure 12.92. SMS Modem Setting

2) Check **SMS Setting**.

Figure 12.93. Check SMS Setting

3) Enter the information of SMS Gateway.

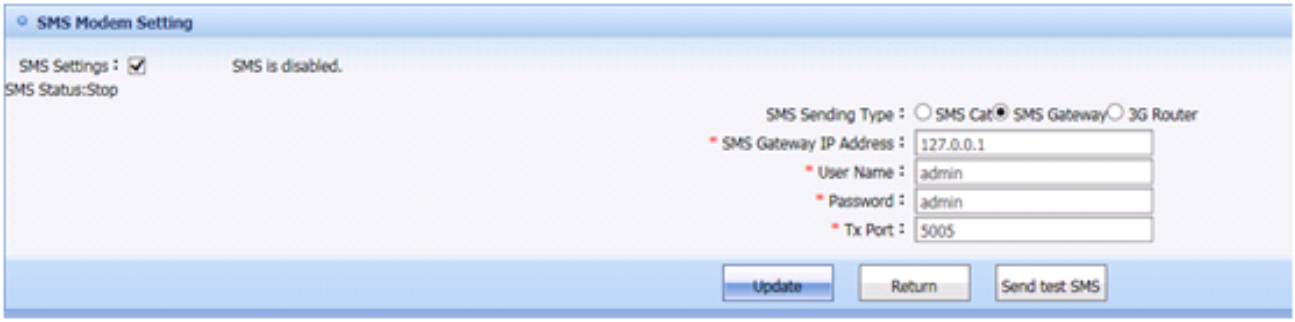


Figure 12.94. Input the information of SMS Gateway

3G Router as SMS Gateway

1) Telnet the RSR Router, then input these command: con -> smm-role gateway -> diff-carrier-comm support -> w.

Click **SMS Modem Setting** in System.

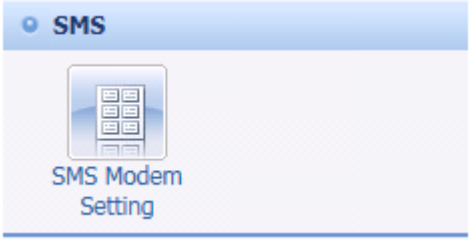


Figure 12.95. SMS Modem Setting

2) Check **SMS Setting**.

Figure 12.96. Check SMS Setting

3) Enter the information of 3G Router. Ensure that the 3G Router is inserted with an SMS-enabled 3G card and must be reachable from the SNC server, and vice versa.

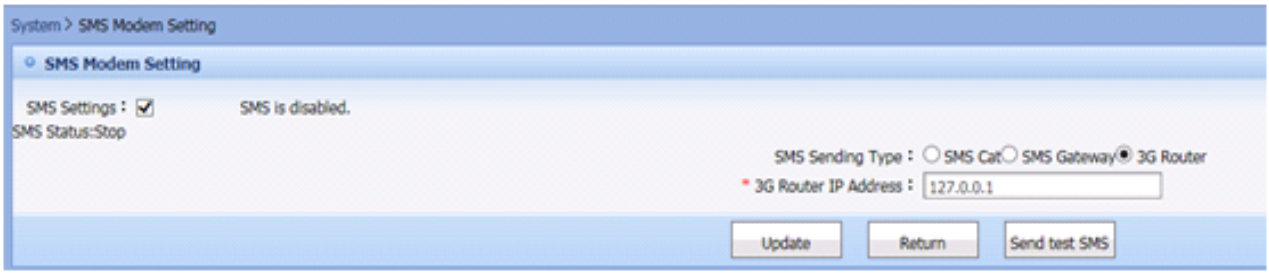


Figure 12.97. Input the information of 3G Router

4) Check the availability of 3G Router as SMS Gateway.

Figure 12.98. Click Send test SMS

Figure 12.99. Input the recipient cellphone number

Chapter 13 Report

Major Functions

- Report List
- Historical Report

13.1. Report List

Major Functions

- Create Report
- Query Report
- Modify Report
- Delete Report
- Preview List
- Set Report Cycle
- Configure Publishing Location

13.1.1. Create Report

Operation Steps

On report list page, click **Create** to enter the report creation page. As shown below:

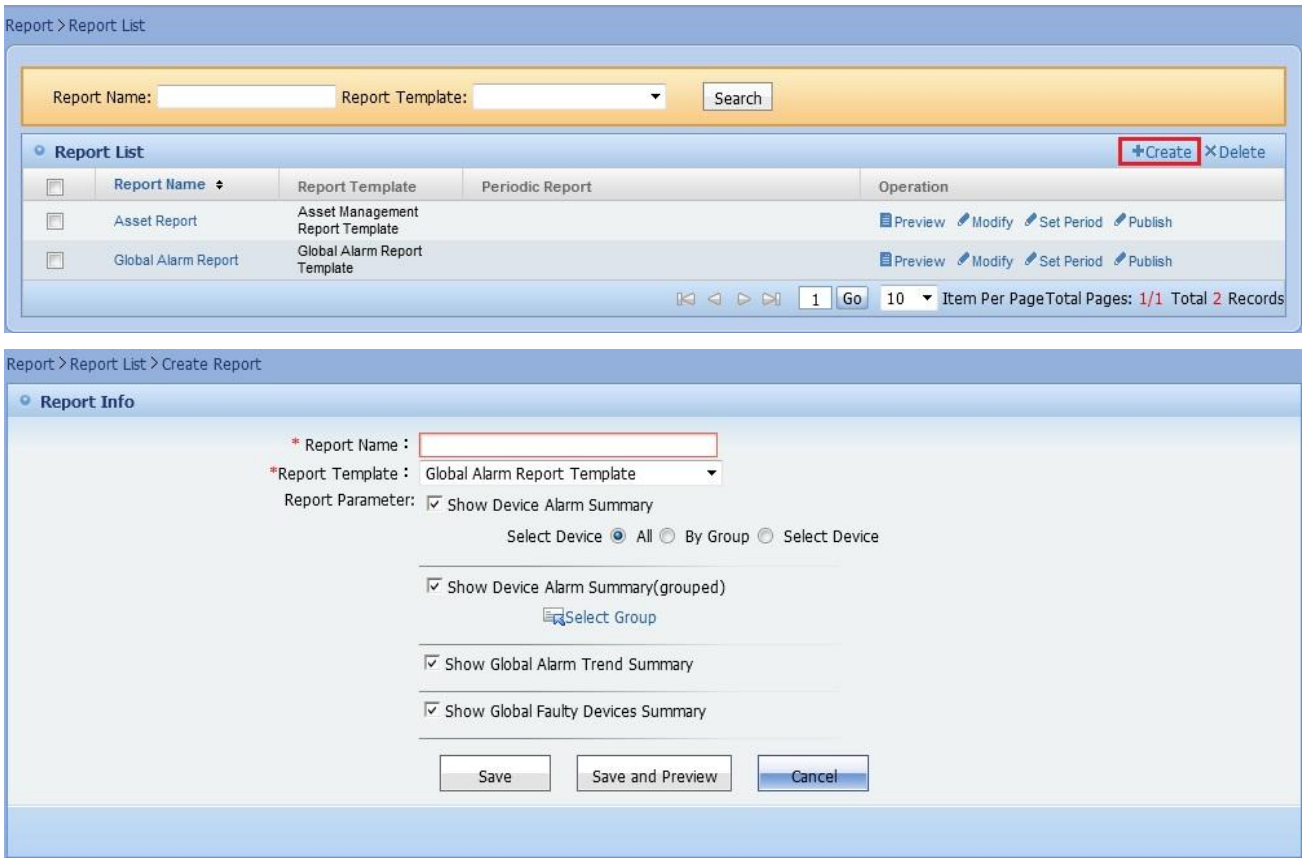


Figure 13.1. Create Report

Enter the report name, report template and report parameters, then click **Save** button to save the report.

13.1.2. Query Report

Operation Steps

On report list page, enter **Report Name** or **Report Template** to query existing reports in the system. As shown below:

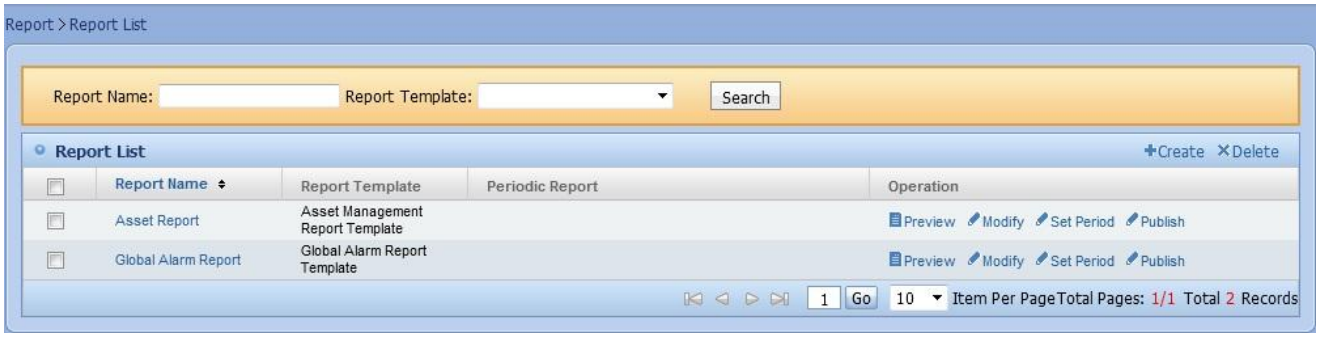


Figure 13.2. Query Report

13.1.3. Modify Report

Operation Steps

On report list page, select one report record and click **Modify** link under **Operation** column to enter report modification page. As shown below:

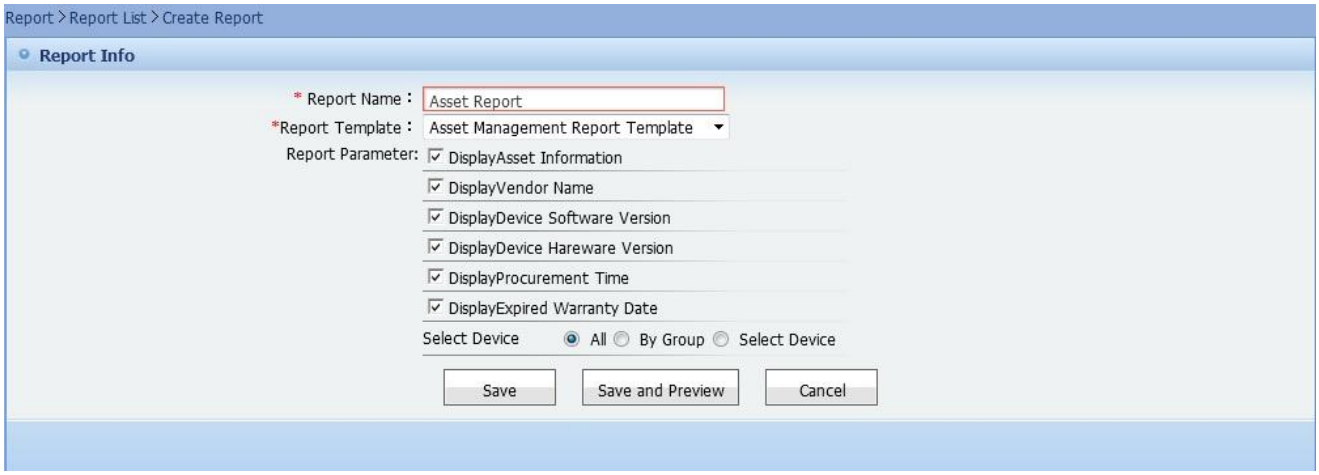


Figure 13.3. Modify Report

13.1.4. Delete Report

Operation Steps

On report list page, select the reports you want delete, then click **Delete** button the delete the selected reports. As shown below:

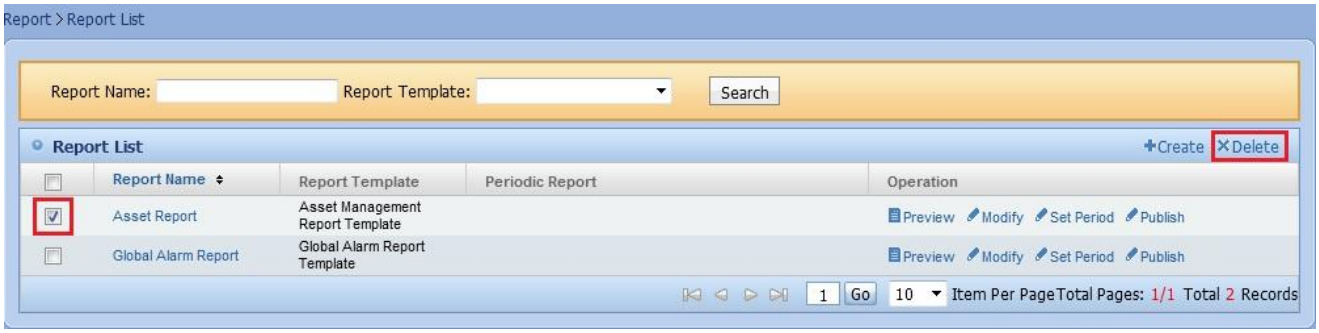


Figure 13.4. Delete Report

13.1.5. Preview List

Operation Steps

1) On the Report List page, click the report name or Preview to go to the Preview page of the corresponding report, as shown in the following figure:

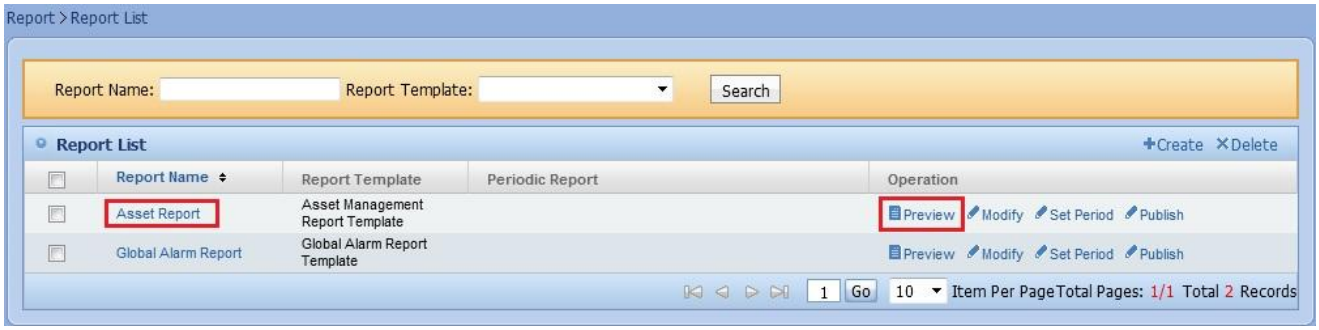


Figure 13.5. Preview List

2) On the Preview page, click Modify to modify the report configuration, as shown in the following figure:

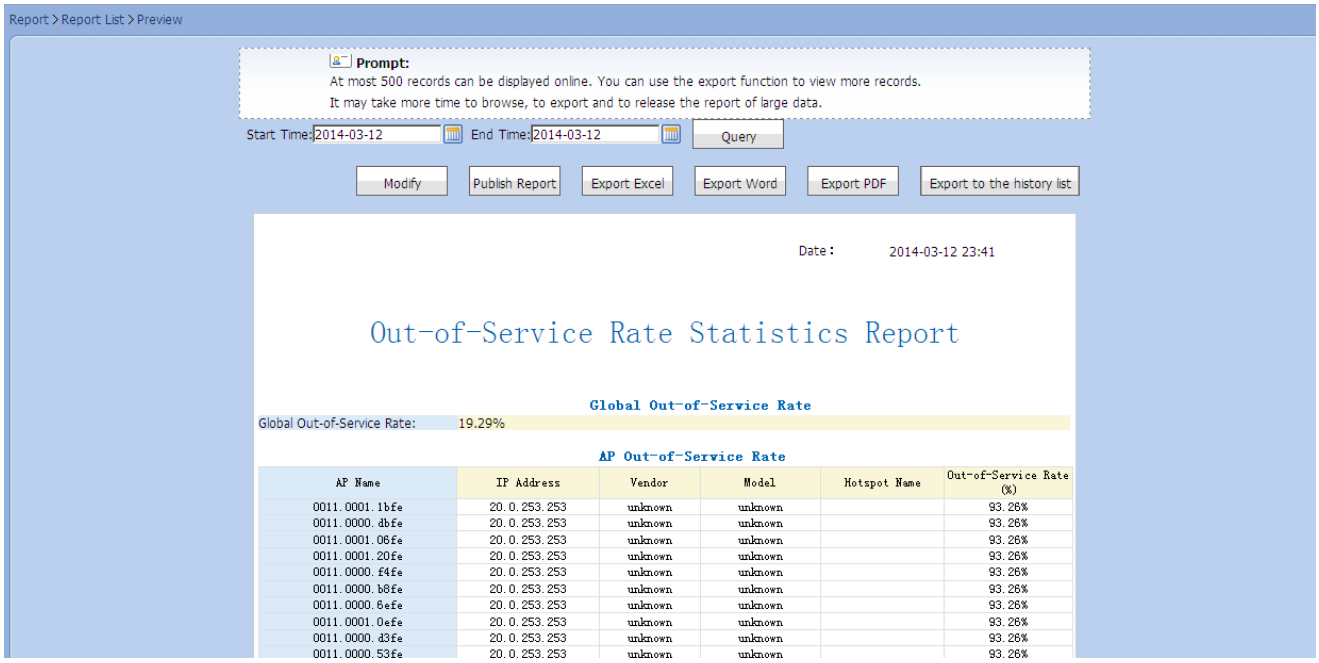


Figure 13.6. Modifying Configuration

3) On the Preview page, click Publish Report to publish the report immediately, as shown in the following figure:

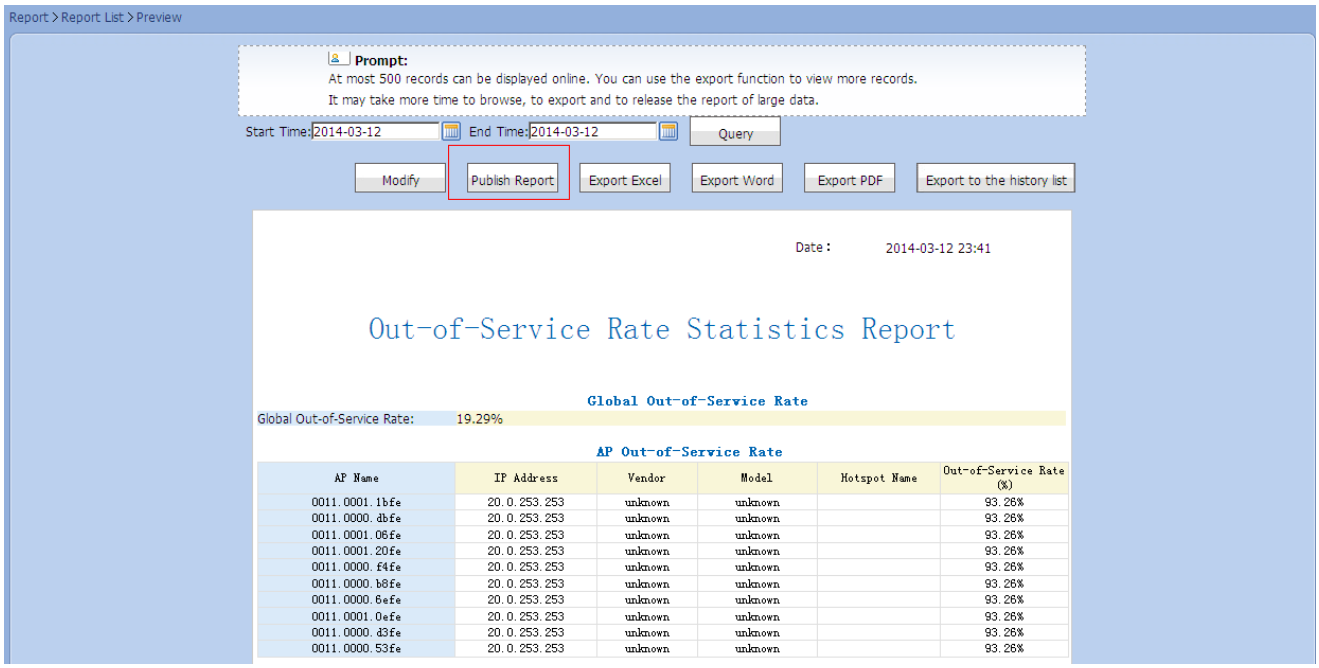


Figure 13.7. Publishing Report

4) On the Preview page, click Export Excel to export the Excel file to the local computer, as shown in the following figure:

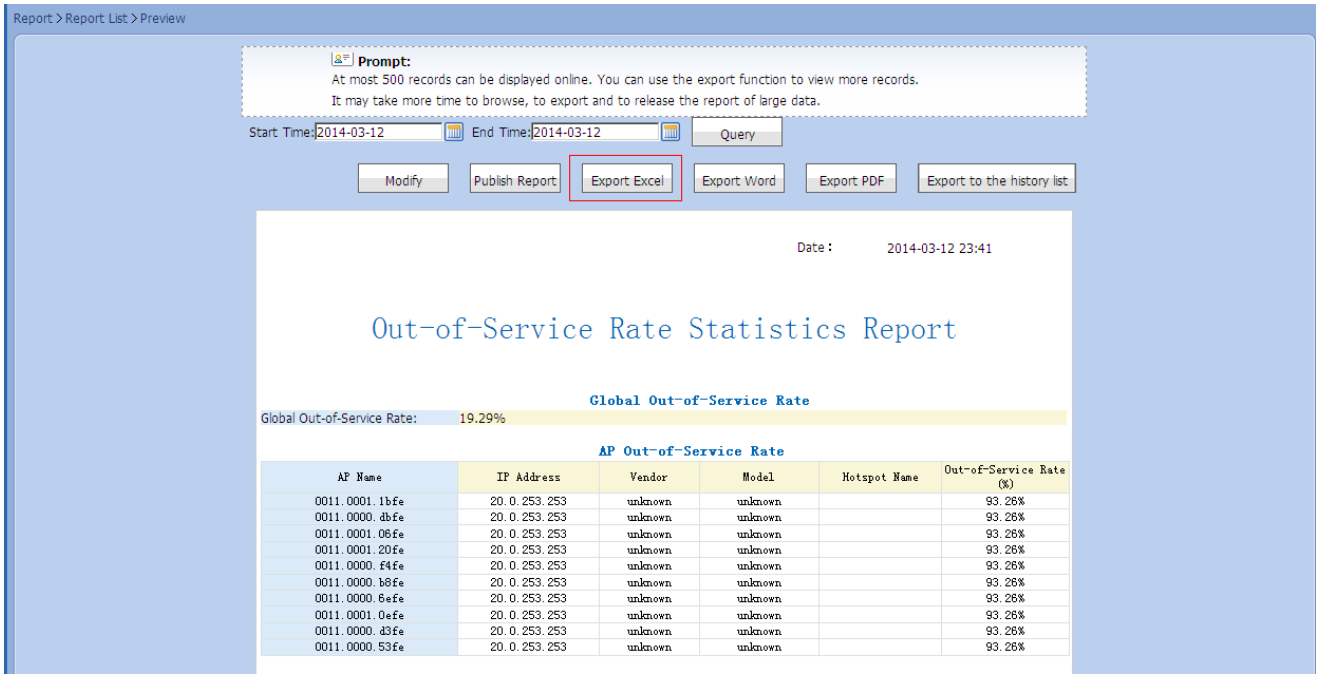


Figure 13.8. Exporting Excel

5) On the Preview page, click Export Word to export the Word file to the local computer, as shown in the following figure:

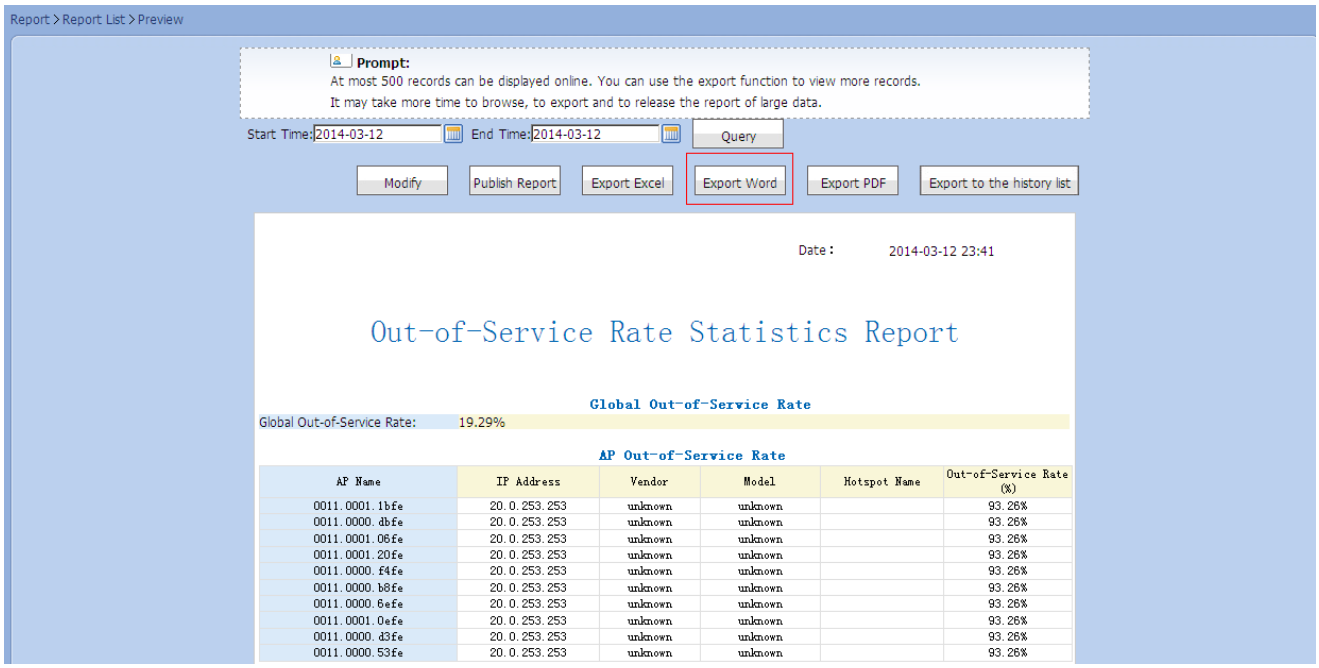


Figure 13.9. Exporting Word

6) On the Preview page, click Export PDF to export the PDF file to the local computer, as shown in the following figure:

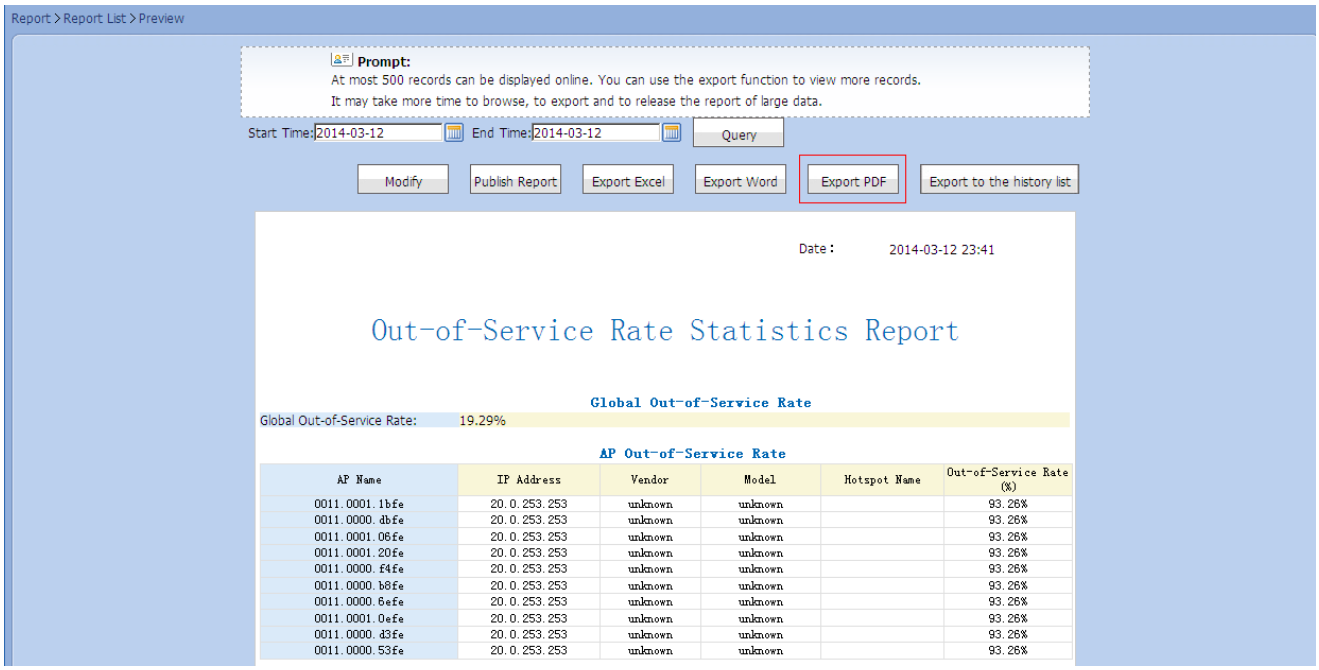


Figure 13.10. Exporting PDF

7) On the Preview page, click Export to the history list to export the report in PDF format to the historical report, as shown in the following figure:

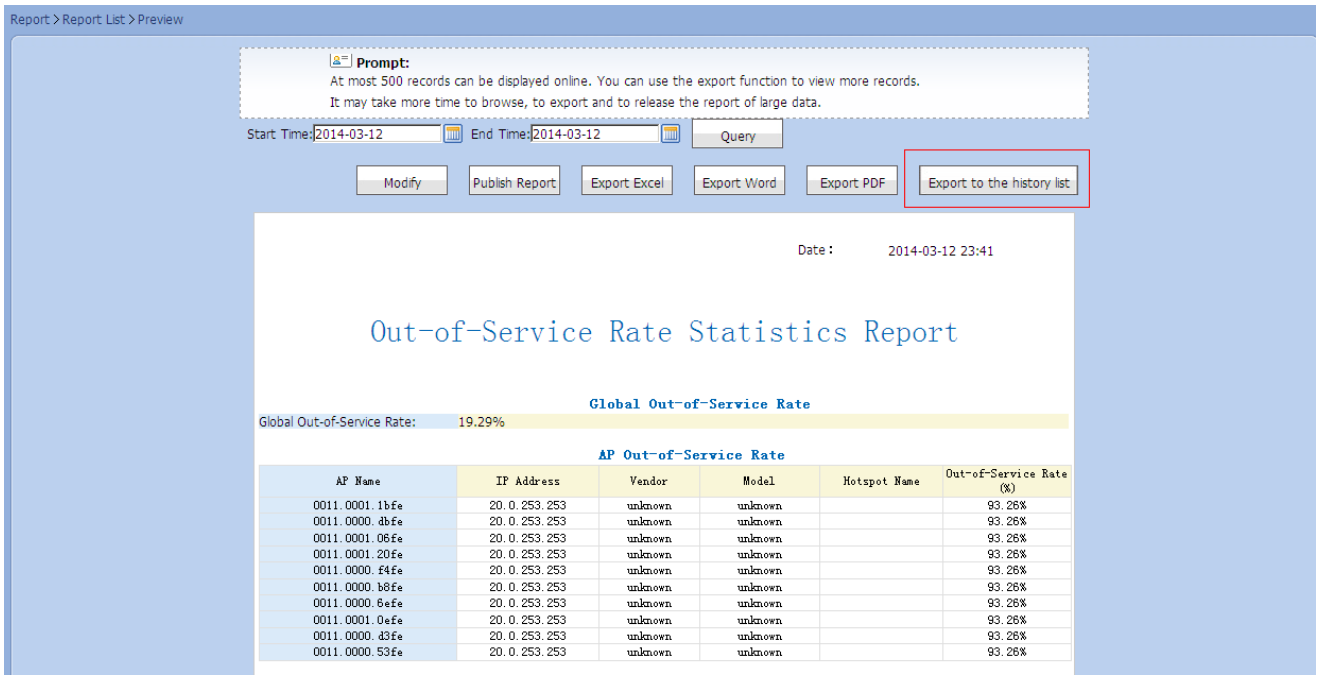
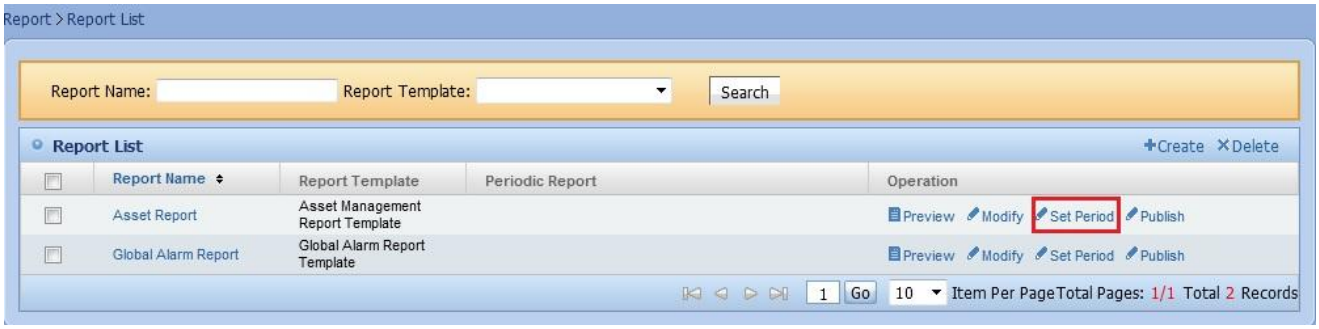


Figure 13.11. Exporting to Historical Report

13.1.6. Set Report Cycle

Operation Steps

On report list page, click **Set Period** link under **Operation** column to enter **Set Periodic Report** page. As shown below:



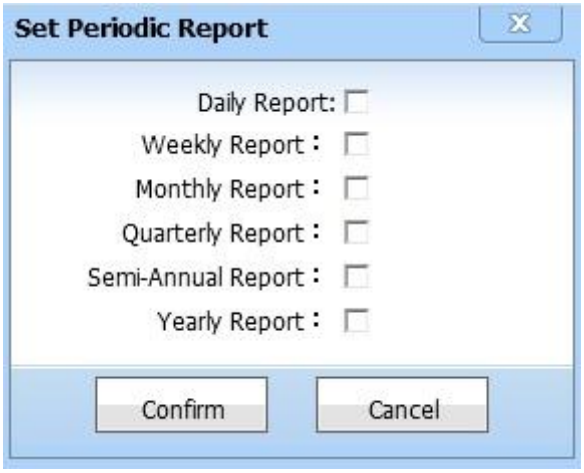


Figure 13.12. Set Periodic Report

13.1.7. Configure Publishing Location

Operation Steps

On report list page, click **Publish** link under **Operation** column to enter **Config report publishing location** page. As shown below:

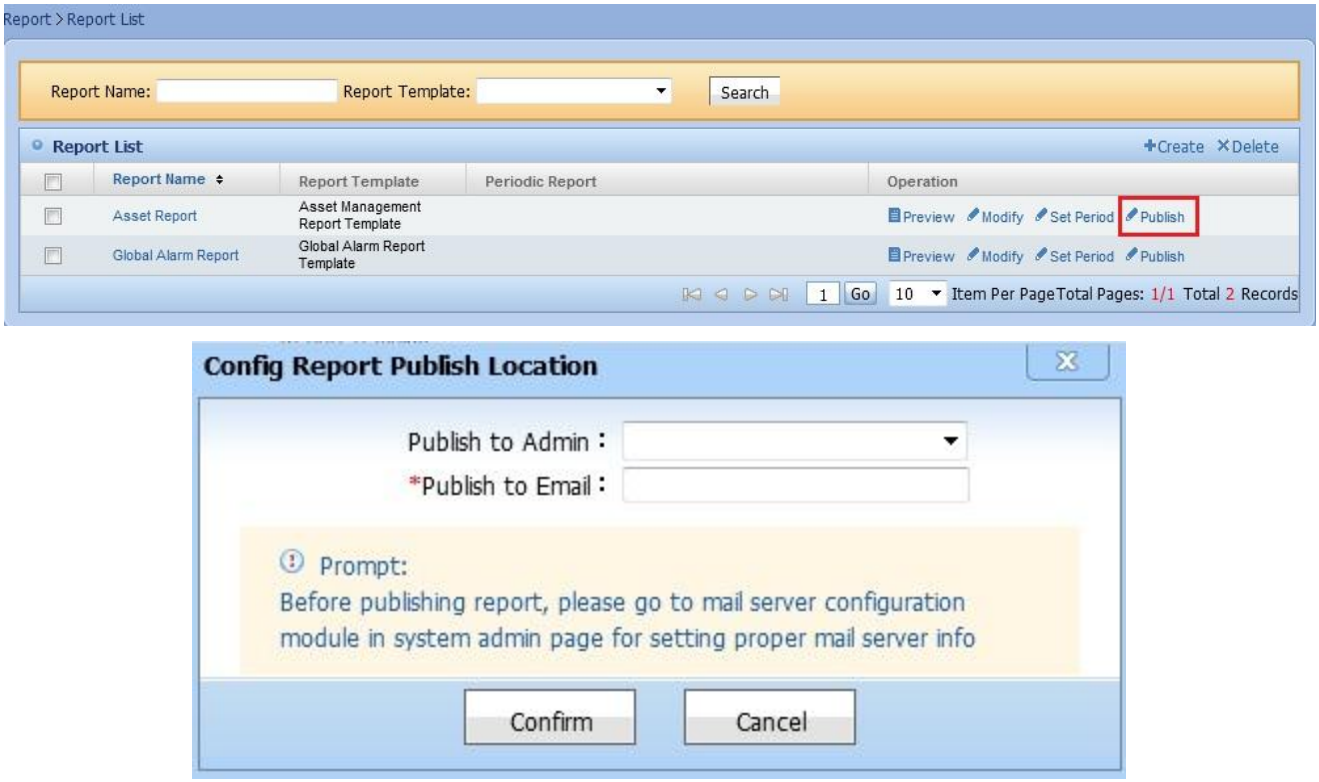


Figure 13.13. Configure Publishing Location

13.2. Historical Report

Major Functions

- Query Historical Report
- View Historical Report
- Delete Historical Report
- Download Historical Report
- Publish Report

13.2.1. Query Historical Report

Operation Steps

On historical report list page, enter search conditions, then click **Search** button query historical report. As shown below:

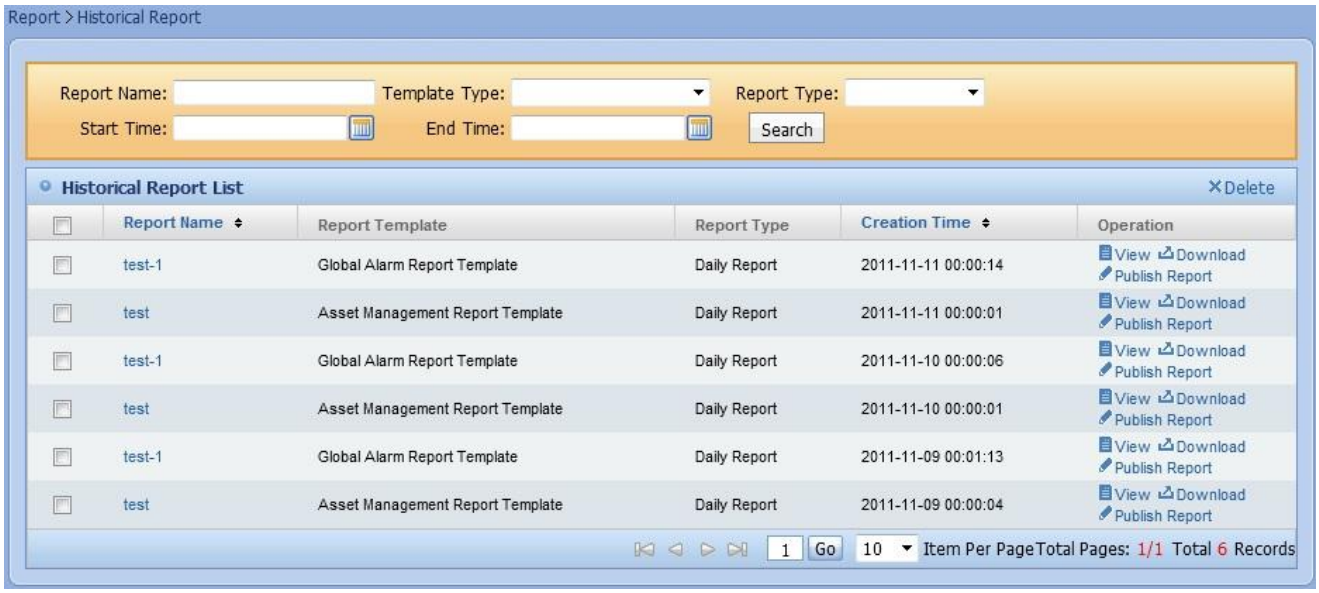


Figure 13.14. Query Historical Report

13.2.2. View Historical Report

Operation Steps

On historical report list page, click the report name link or **View** link under **Operation** column to view the historical report. As shown below:

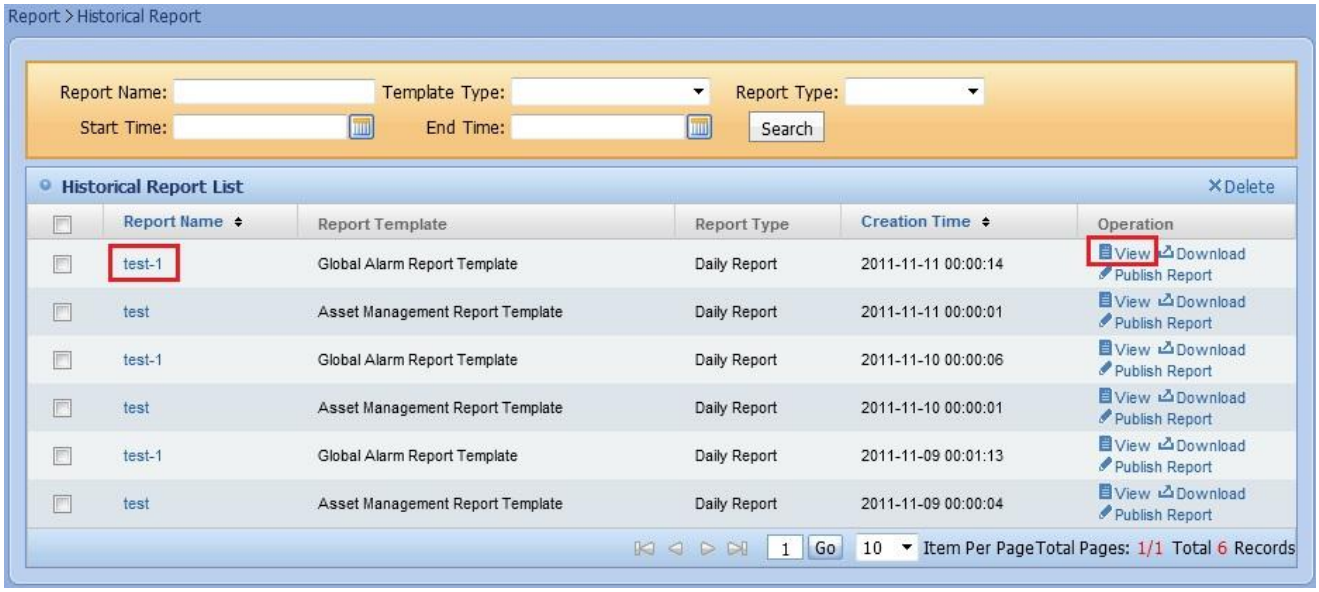


Figure 13.15. View Historical Report

13.2.3. Delete Historical Report

Operation Steps

On historical report list page, select the reports you want delete, then click **Delete** button the delete the selected historical reports. As shown below:

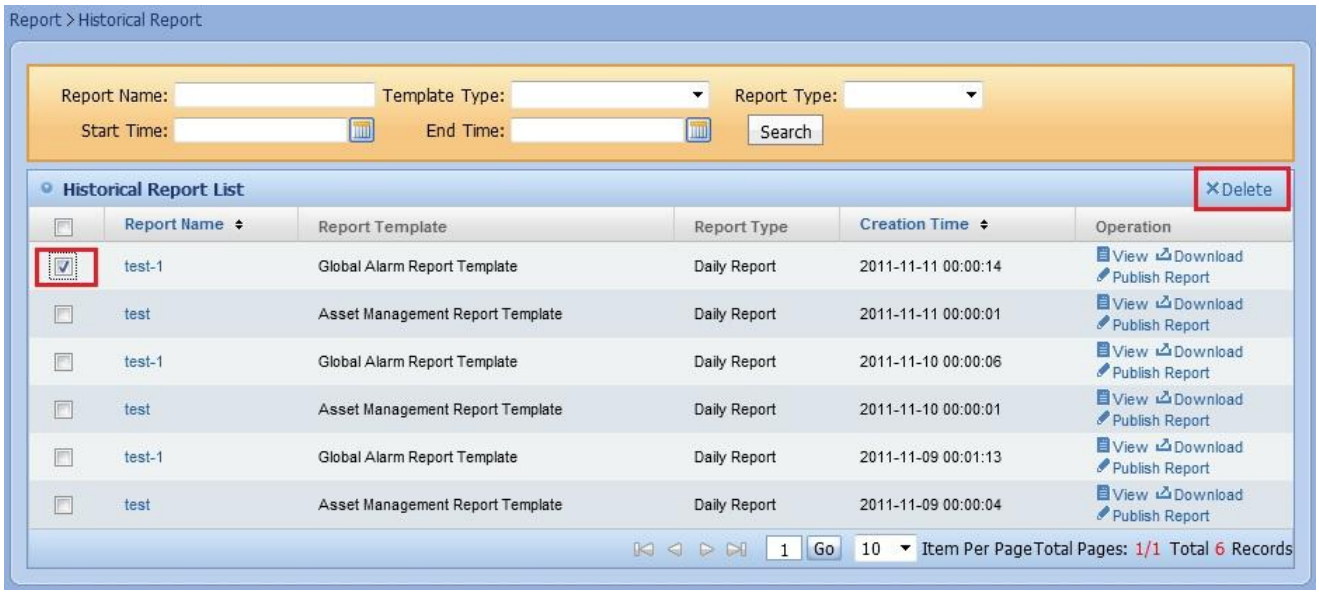


Figure 13.16. Delete Historical Report

13.2.4. Download Historical Report

Operation Steps

On historical report list page, click **Download** link under **Operation** column to download the report. As shown below:

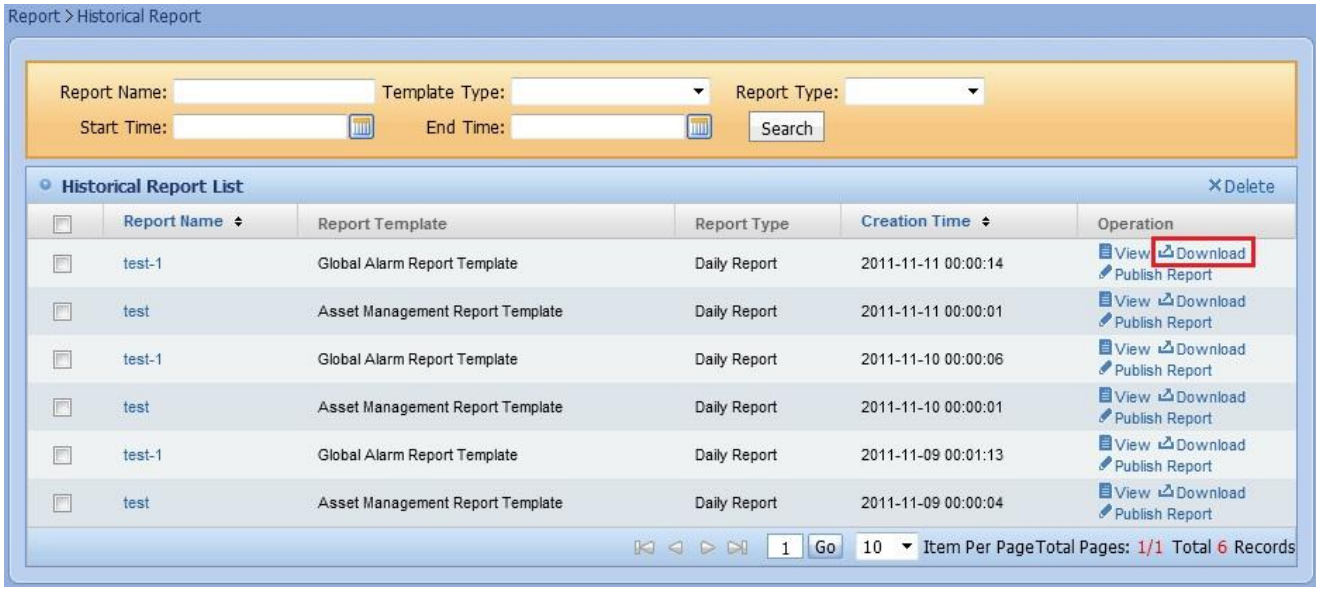


Figure 13.17. Download Historical Report

13.2.5. Publish Report

Operation Steps

On historical report page, click **Publish Report** link under **Operation** column to publish the report. As shown below:

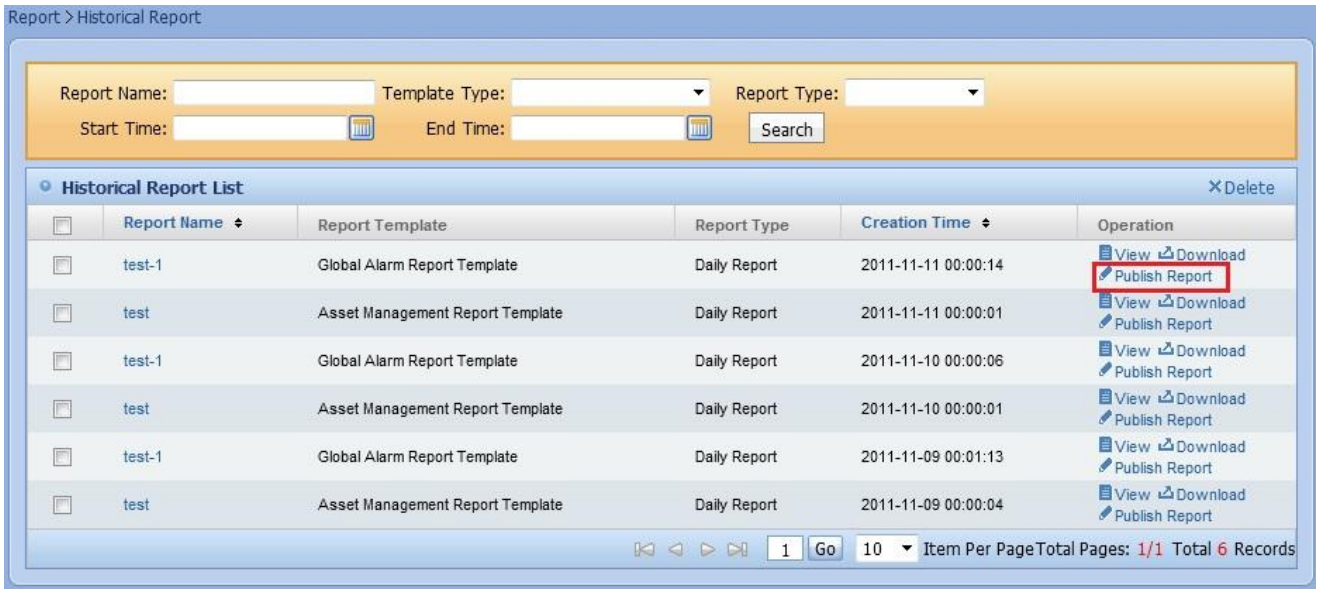


Figure 13.18. Publish Report

Chapter 14 Asset

This module includes the following operation:

- Add Group
- Delete Group
- Add Asset
- Edit Asset
- Delete Asset
- Add Asset to Group
- Import Asset
- Search Asset
- Export Asset
- Custom Property

14.1. Add Group

1) Select a parent group and click **Add**, as shown in the following figure:

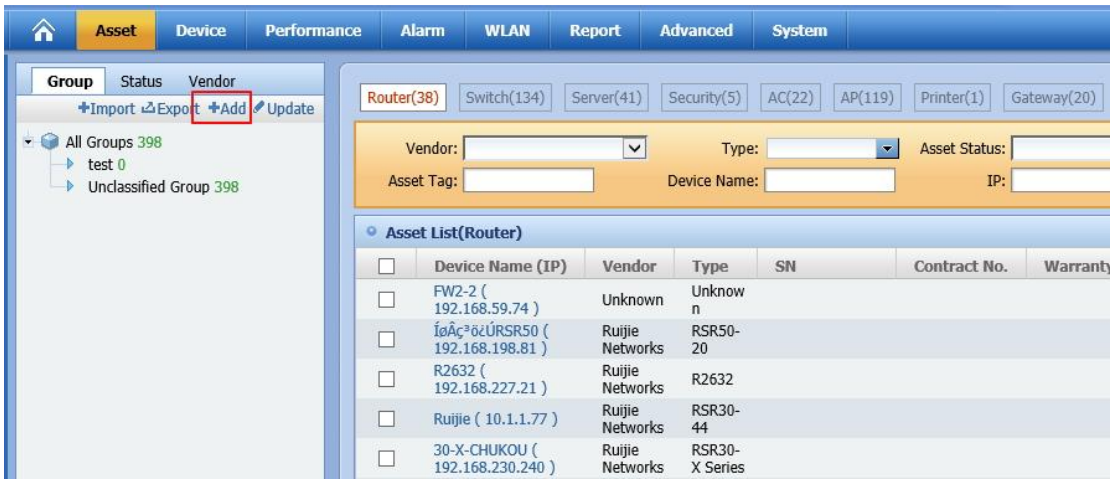


Figure 14.1. Clicking Add

2) Enter group name and click **Add**, as shown in the following figure:

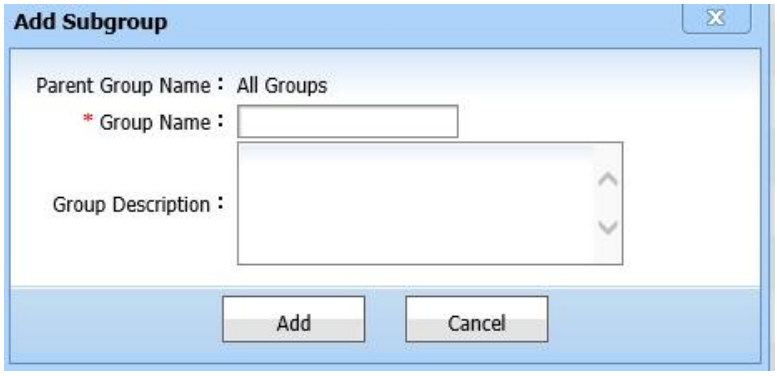


Figure 14.2. Entering Information

3) The added group is displayed in the group list, as shown in the following figure:

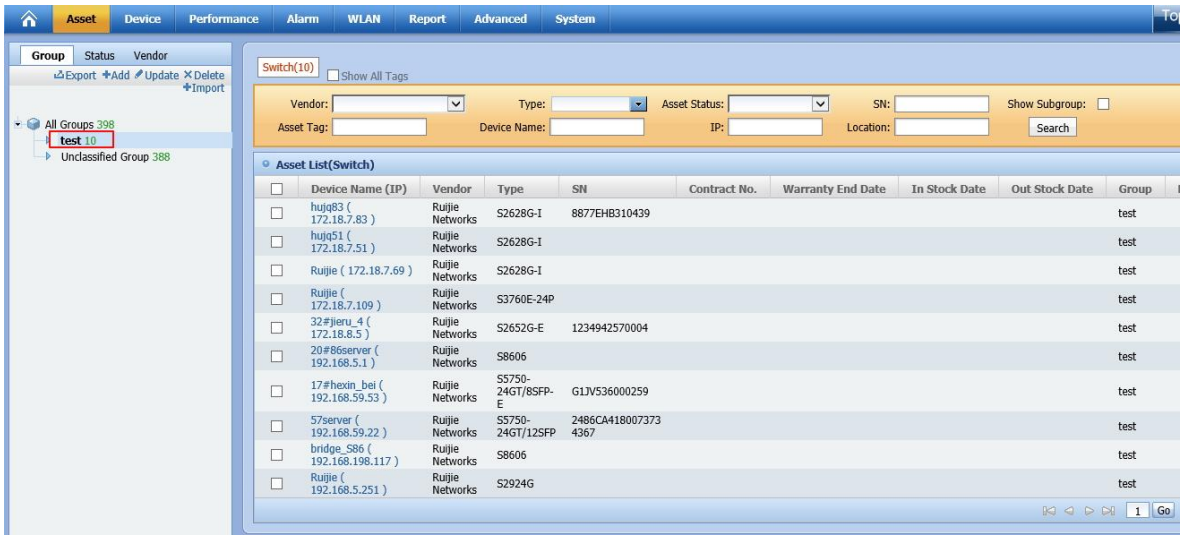


Figure 14.3. Add Success

14.2. Delete Group

Operation Steps

1) Select a group and click **Delete**, as shown in the following figure:

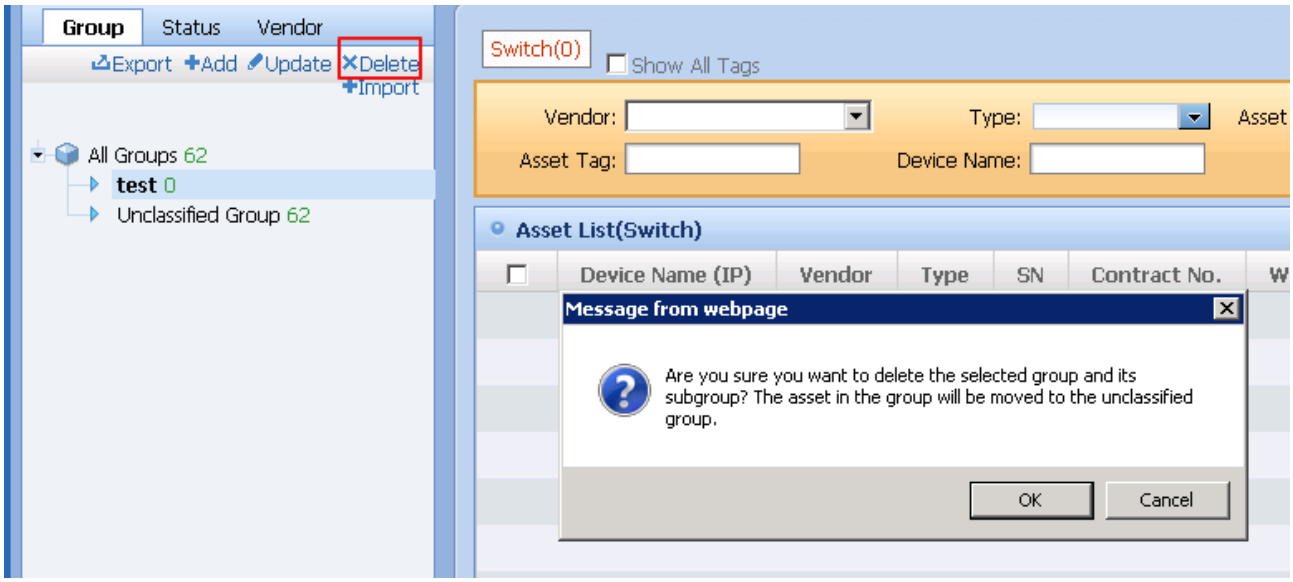


Figure 14.4. Deleting Group

14.3. Add Asset

Operation Steps

1) Select a type of asset, e.g., Router, and click **Add**, as shown in the following figure:

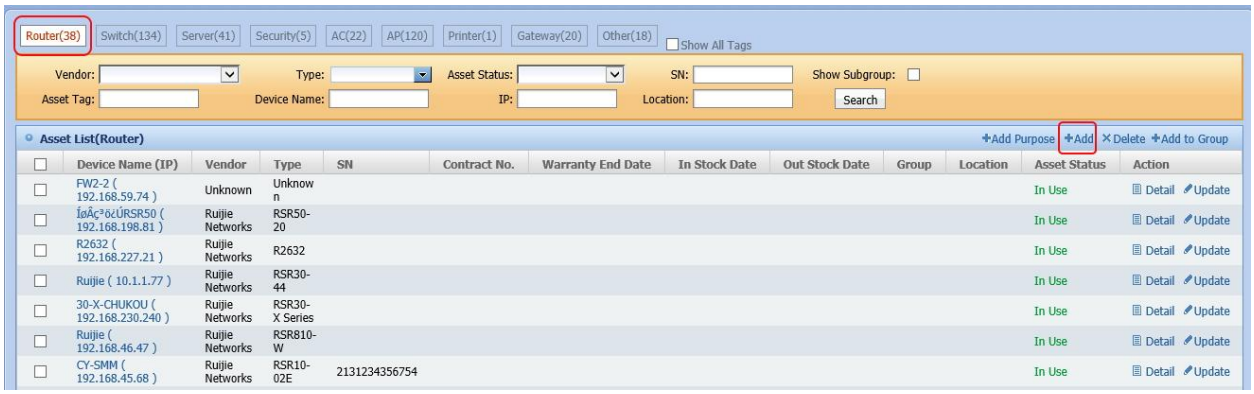


Figure 14.5. Clicking Add

2) Enter asset information and click **Save**, as shown in the following figure:

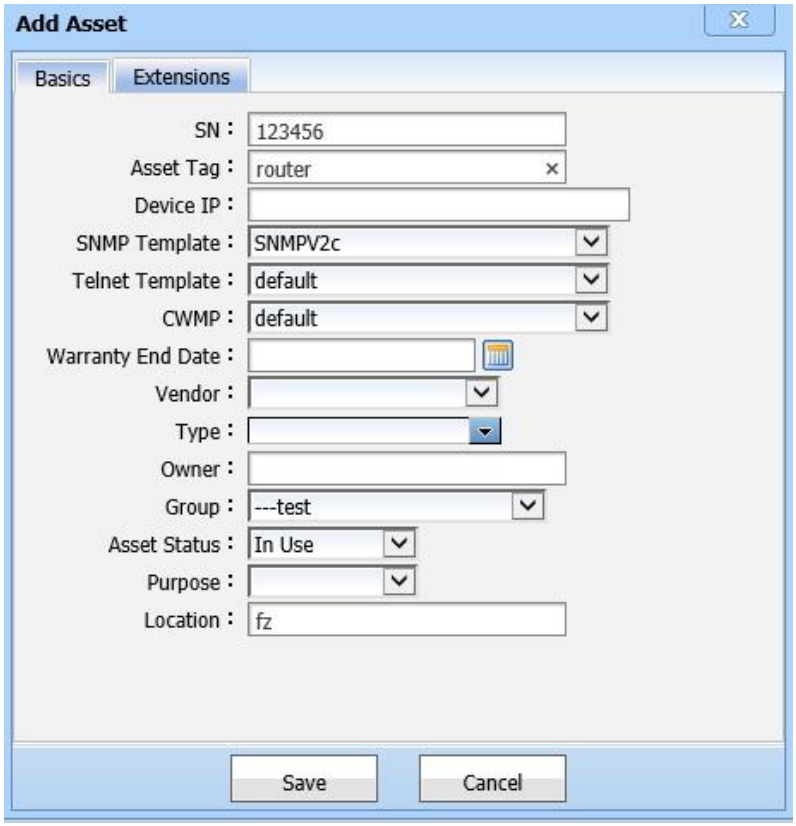


Figure 14.6. Entering Information and Clicking Save

3) The added asset is displayed in the asset list, as shown in the following figure:

Figure 14.7. Add Success

14.4. Edit Asset

Operation Steps

1) Click **Edit** to edit the asset information, as shown in the following figure:

Figure 14.8. Editing Asset Information

14.5. Delete Asset

Operation Steps

1) Select an asset and click **Delete**, as shown in the following figure:

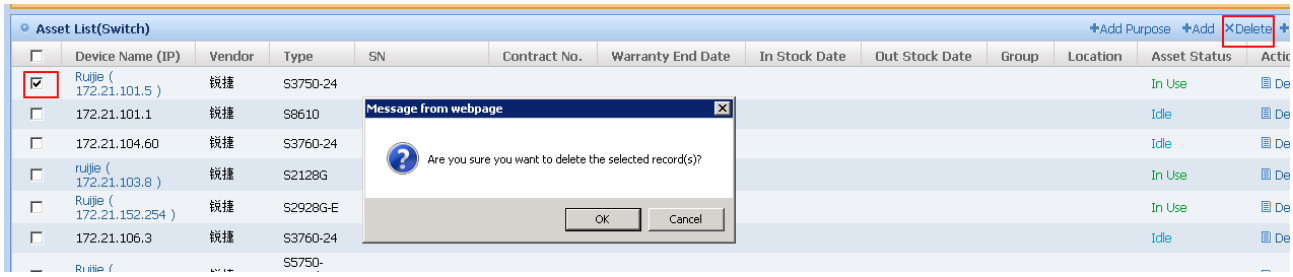


Figure 14.9. Deleting Asset

14.6. Add Asset to Group

Operation Steps

1) Select an asset and click **Add** to Group, as shown in the following figure:

Figure 14.10. Clicking Add to Group

2) Select a group in the displayed list, as shown in the following figure:

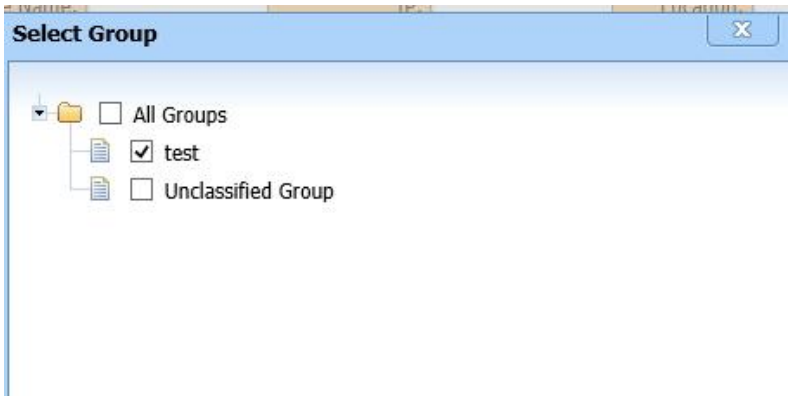


Figure 14.11. Selecting Group

14.7. Import Asset

Operation Steps

1) Click **Import**, as shown in the following figure:

Figure 14.12. Clicking Import

2) Download the import template and enter the information, as shown in the f0llowing figure:

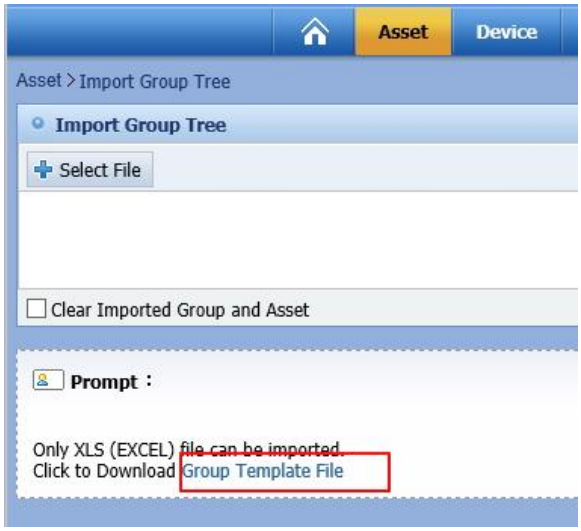


Figure 14.13. Downloading Template

3) Select a file, as shown in the following figure: Note: If you tick **Clear Imported Group and Asset,** all groups on the device will be deleted. Do not tick this option if you import increment.

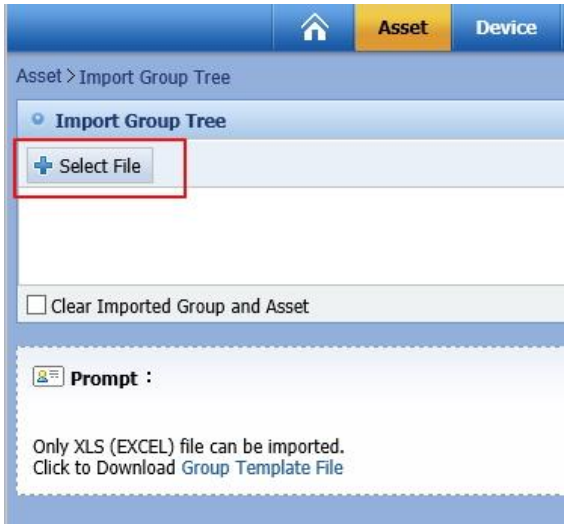


Figure 14.14. Selecting Import File

14.8. Search Asset

Operation Steps

1) You can search for the asset based on group, vendor, model or status, as shown in the following figure:

Figure 14.15. Searching Asset1

Figure 14.16. Searching Asset2

Figure 14.17. Searching Asset3

14.9. Export Asset

Operation Steps

1) Click **Export**, as shown in the following figure:

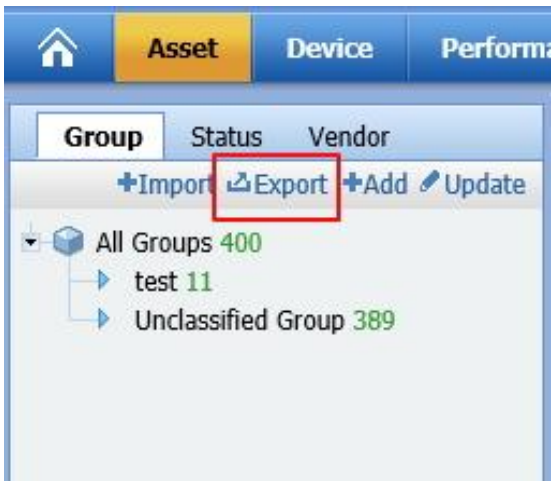


Figure 14.18. Exporting Asset

14.10 Custom Property

Operation Steps

1) Click **Custom Property**, as shown in the following figure:

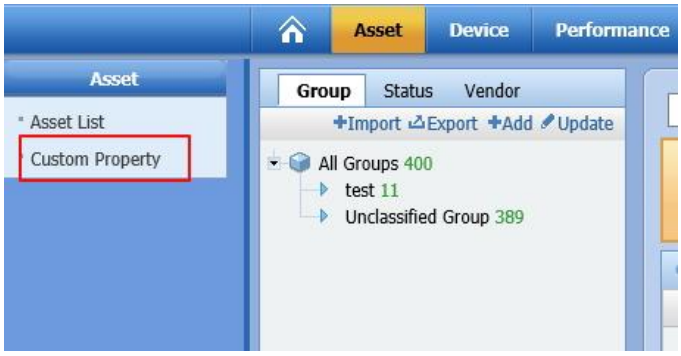


Figure 14.19. Clicking Custom Property

2) Click **Add** to add custom property, as shown in the following figure:

Figure 14.20. Clicking Add

Enter custom information, as shown in the following figure:

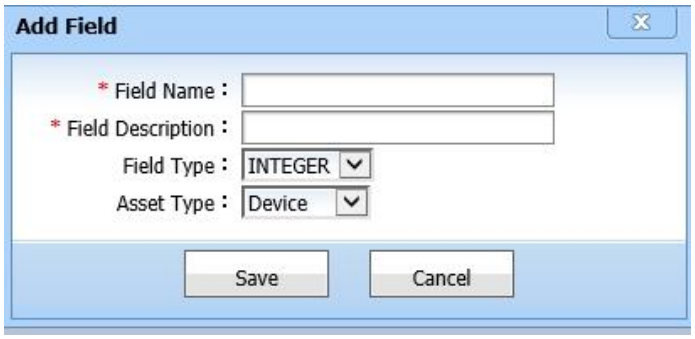


Figure 14.21. Entering Custom Information

3) Edit custom property, as shown in the following information:

Figure 14.22. Clicking Update

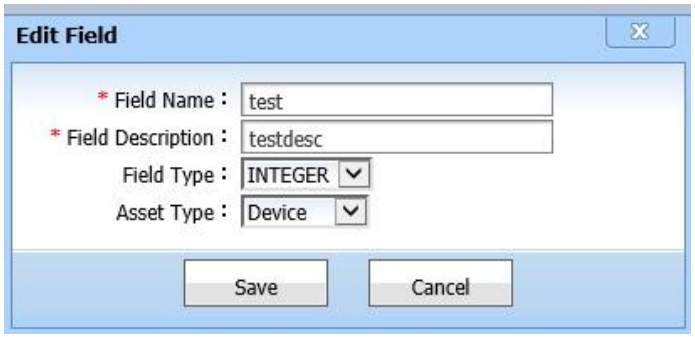


Figure 14.23. Editing Custom Property

4) Delete custom property, as shown in the following information:

Figure 14.24. Clicking Delete

Chapter 15 Appendix

15.1. FAQ

Q: How to get understood of the system quickly?

A: Primarily, if you have any questions or suggestions on using the system, you are welcome to contact our technical support team. From the technical point of view, you need to understand SNMP related knowledge and know-how of maintaining devices using TELNET and CLI.

Q: Which database is used in the system? How to access it? What should I pay attention to when installing the system?

A: MySQL is selected as database of the system. The access port of the database is 3307. When you are installing the system, please make sure that port 3307 is not blocked by the firewall (Allowing TCP on port 3307 in firewall setting) and no host with the same hostname exists in the network. The username for accessing database is root. You can use MySQL client tool to access and manage the database directly. For further information on using MySQL, please refer to **MySQL 5.1 user manual** or MySQL official website. [http://dev.mysql.com/doc/refman/5.1/zh/index.html] . Please be sure to configure the host time correctly and the host time MUST not be earlier than the current time.

Q: Why some devices are shown as unknown models or unknown types after being added to the system?

A: Ruijie device models and device series are predefined in the system database. If the devices are made by other manufacturer, please add related **Device Series** and **Device Model** data. After the device related information is added to the system, the device information will be shown correctly (no **unknown model** or **unknown type** any more).

Q: What should I do when an error is prompted?

A: Most error prompts come up with service prompt information, you need to just follow the service instructions.

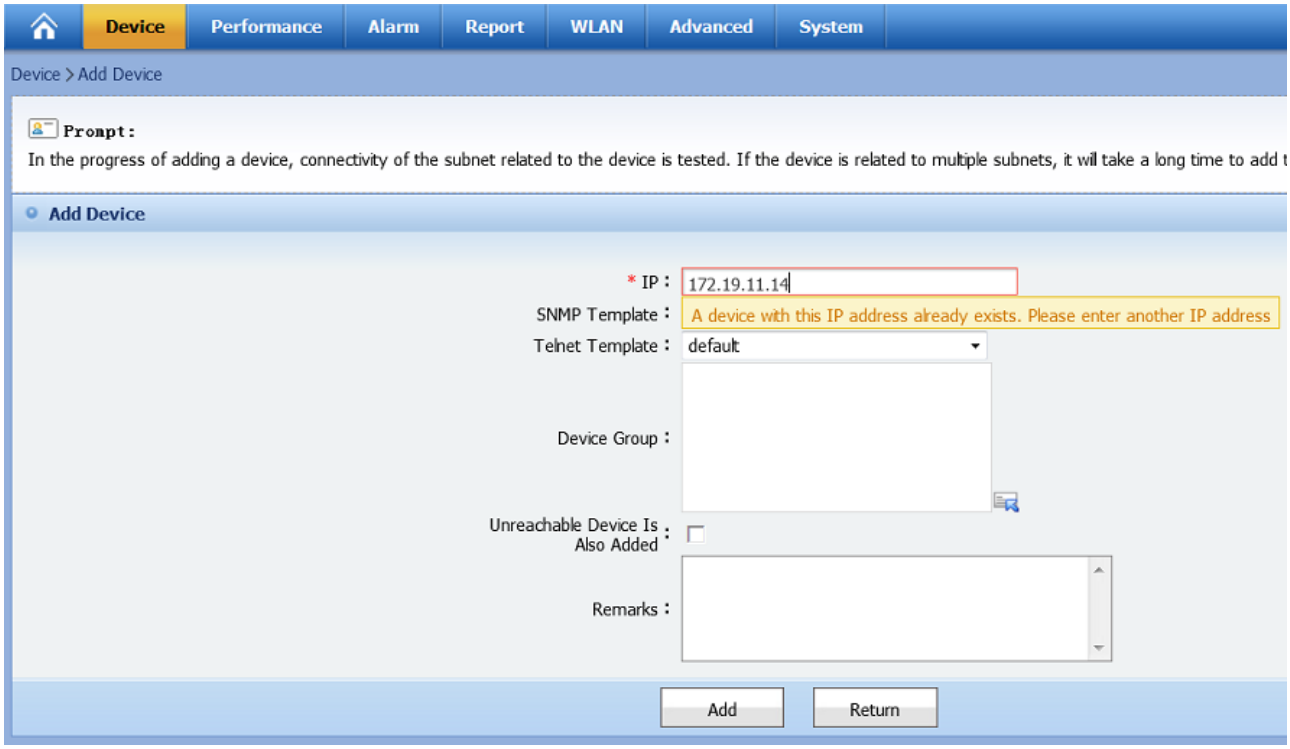


Figure 14.1. Service Prompt

Furthermore: Occasionally, error pages with **Unexpected failure: Deadlock found while trying to get lock; try restarting transaction**, **Unexpected failure: A client timed out while waiting to acquire a resource from com...**, or **Unexpected failure: session expired** will be shown when you make regular usage, please just try the same operation a second time.

Q: Why different topo results are shown when I do L2 topo discovery twice?

A: ARP table is used when executing L2 topo discovery, and the content of ARP table varies much possibly in different time. Normally, the best L2 topo discovery results will be generated when a great number of users go online concurrently.

Q: Why sometimes I cannot access the system but the service manager and MySQL database are still in working state?

A: The system uses C3P0 open-source database connection pool. According to the bug statement of C3P0 on its official site, C3P0 has deadlock issue. To solve this issue, restarting the web service and related application services are required. The link of bug statement on C3P0 official site is [http://sourceforge.net/tracker/?func=detail&aid=1892195&group_id=25357&atid=383690] . We will keep tracking further upgrades of C3P0 and solve it in the future version. We regret for any inconvenience brought to you.

15.2. Terminology

- Super Administrator

It is the role who has the rights to execute all the operations and has access to all the resources of the system.

- Seed IP

In the auto discovery process, you need to set at least one seed IP address. The system will start searching managable devices from routing table or ARP table of the device with seed IP. Normally, the seed IP address is the IP address of the gateway.

- Access Control List

It lists the IP address or IP address range from which the operator can access the system. In other words, the operator can log in to the system only from the IP addresses allowed by the ACL.

- SNMP

Simple Network Management Protocol, the three popular versions are SNMPv1, SNMPv2c, and SNMPv3.

- Alarm Level

Alarm level is used to identify the alarm severity. The degression order of alarm level is CRITICAL, MAJOR, NORMAL, INFORM and CLEAR. The state of a device is decided by the highest level of alarm generated by the device.

15.3. Icons

Alarm Severity

	CLEAR
	INFORM
	NORMAL
	MAJOR
	CRITICAL

Device Icon In Topology

	Router
	Switch

	Server
	Dumb Device
	PC
	Unknown