User Guide

Network Management System
tpNMS

1910012005 REV 1.1.0
March 2017

COPYRIGHT & TRADEMARKS

Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.

Conventions

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit *http://www.tp-link.com*.

When using this guide, please notice that features of the Pharos Control may vary slightly depending on the software version you have. All screenshots, images, parameters and descriptions documented in this guide are used for demonstration only.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

Content

1 Quick Start

The tpNMS (TP-Link Network Management System) is a centralized management software that allows you to discover, monitor and configure your TP-Link Managed Switches using a web browser. Follow the steps below to complete the basic settings of the tpNMS.

1. *Prepare for Installation*
2. *Download and Install tpNMS*
3. *Log in to the Application*
4. *Change Your Password and Email*
5. *Set the Email Server for Alarm Notifications*

1.1 Prepare for Installation

You can install the tpNMS to centrally manage the switches in the LAN or in different network segments.

- *Computer Requirements*
- *Compatible Devices*
- *Installation Topology*

1.1.1 Computer Requirements

- CPU: Duel Core 2.8GHz or above
- RAM: 4GB RAM (32-bit OS) or 8GB RAM (64-bit OS)
- HD Space: 20GB or above
- Operating System: Microsoft Windows XP/Vista/7/8/10
- Web Browser: Mozilla Firefox 32 (or above), Google Chrome 37 (or above), Opera 24 (or above), or Microsoft Internet Explorer 8-11.

Note:

We recommend you deploy the tpNMS on a 64-bit operating system to guarantee the software stability.

1.1.2 Compatible Devices

TP-Link 2/3/5/T series switches.

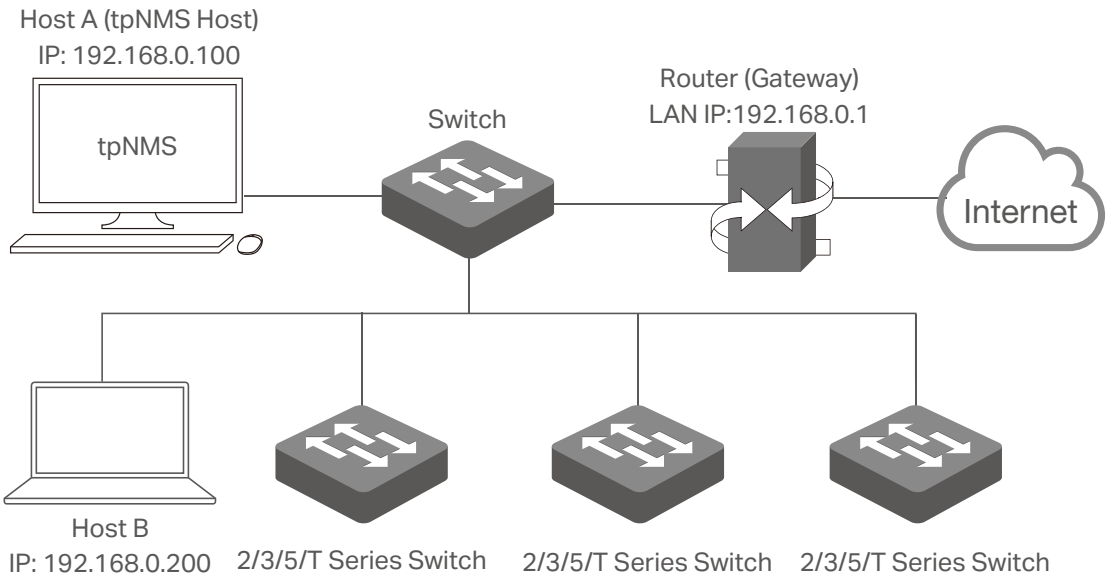
1.1.3 Installation Topology

You can deploy tpNMS to manage devices in three types of network topologies.

- In the Same LAN

If you want to manage the compatible switches in the same LAN with the tpNMS host, refer to the following network topology.

Figure 1-1 Topology of the same LAN



In the LAN, only one host needs to install tpNMS. The host is called as tpNMS Host. And the other hosts in the same LAN can access the tpNMS Host to manage the network. In this topology, you can visit tpNMS interface from Host B by entering "192.168.0.100: 8888" in a web browser. It's recommended to set a static IP address to the tpNMS Host for the convenient login to the tpNMS interface.

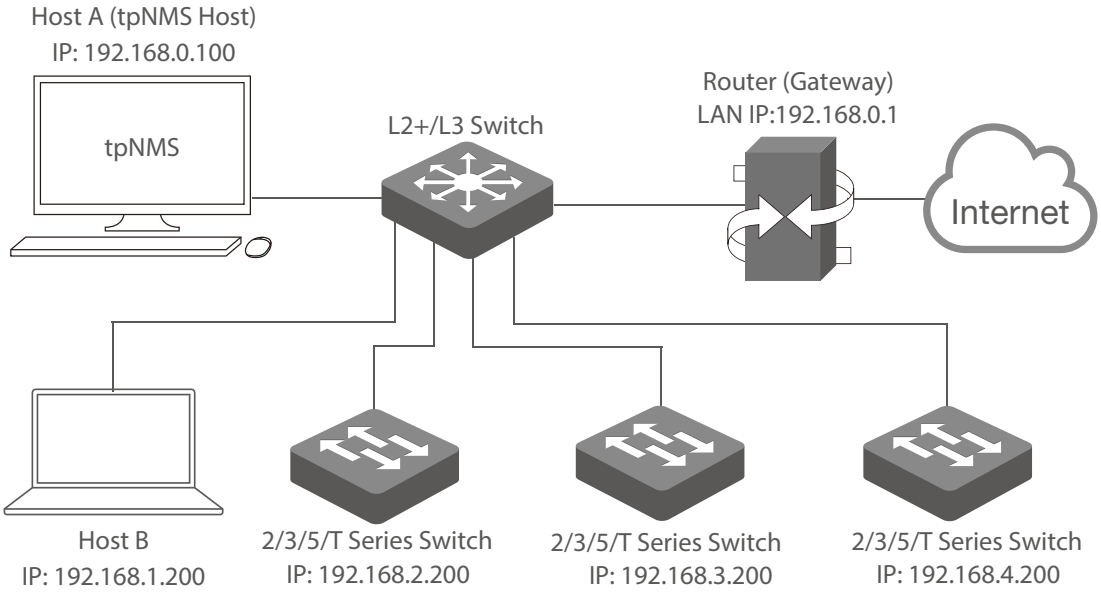
Note:

The tpNMS must be running all the time when you manage the network.

· In Different Network Segments

If the tpNMS Host needs to manage switches in different network segments, refer to the following topology. \

Figure 1-2 Topology with different subnets

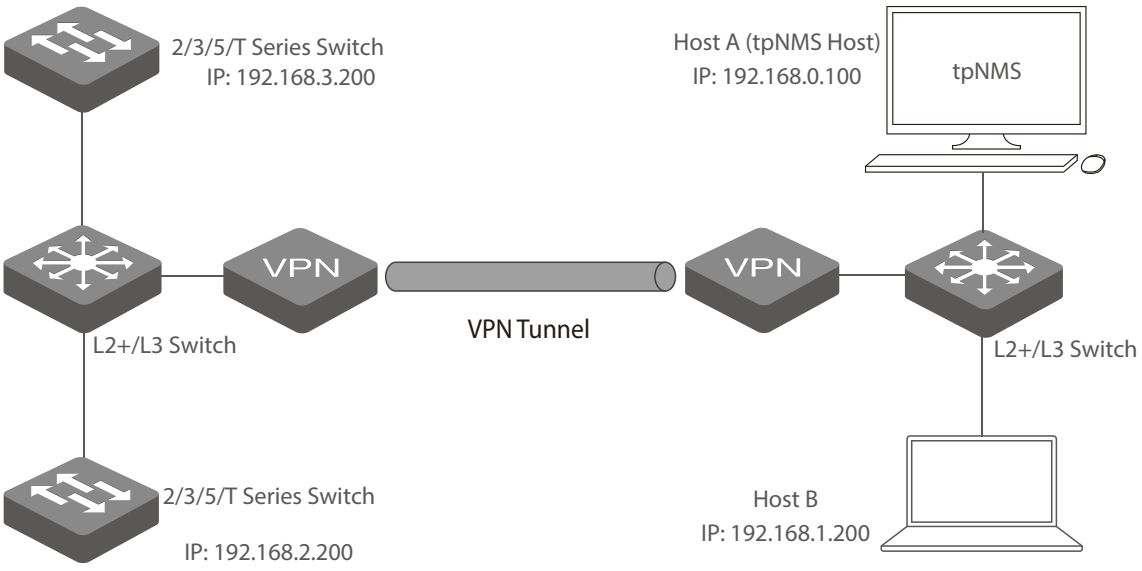


The tpNMS Host and the switches are connected to different ports on the L2+/L3 switch. The tpNMS Host and the switches can access each other via the routing interfaces configured on the L2+/L3 switch. To ensure the switches can be discovered by the tpNMS Host and be managed, configure the switches to send SNMP traps to the IP address of the tpNMS host.

· Over VPN Tunnel

The tpNMS Host can manage the switches over the VPN tunnel, referring to the following topology.

Figure 1-3 Topology over VPN tunnel



After the VPN tunnel is established, the tpNMS can manage the switches on the other side of the tunnel remotely.

1.2 Download and Install tpNMS

Get the installation file of tpNMS from our website www.tplink.com/en in this directory **For Business > Switches > Accessories**, or click this link. Then follow the on-screen instructions to properly install the tpNMS software. After successful installation, a shortcut icon of the tpNMS will be created on the tpNMS host's desktop.

1.3 Log in to the Application

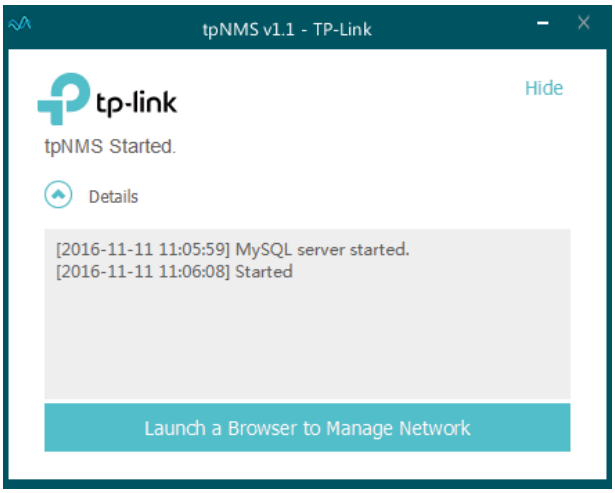
Launch the software on the tpNMS Host and follow the instructions to complete the basic configurations, and then you can log in to the management interface.

- *Launch the tpNMS*
- *Fix the Launch Problems*
- *Log in to tpNMS*

1.3.1 Launch the tpNMS

Launch the tpNMS and the following window will pop up. You can click **Hide** to hide this window but do not close it. After a while, your web browser will automatically open.

Figure 1-4 Launch window



Note:

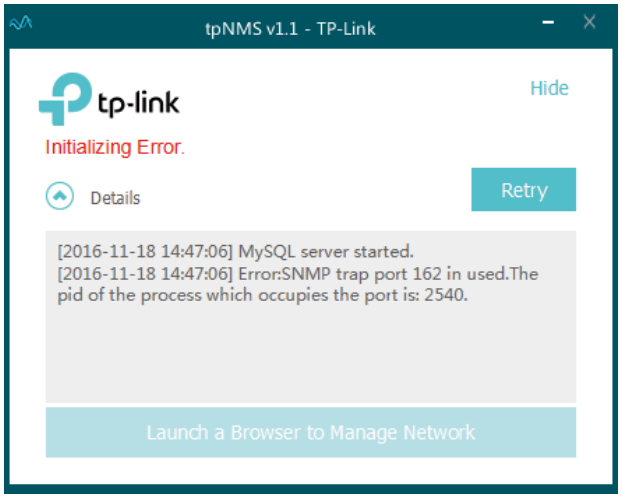
- If your browser does not open, please click **Launch a Browser to Manage Network**.
- If it opens but prompts a problem with the website's security certificate, please click Continue to this website.
- If the port 69, 162 and 1099 are already used by other processes, tpNMS will fail to initialize. Please kill the tasks occupying these ports and click **Retry** to launch tpNMS again.

1.3.2 Fix the Launch Problems

tpNMS will use several ports in its launch process, which include but are not limited to: 69, 162 and 1099. If any of these ports is occupied by the other processes, tpNMS will fail to initialize. The conflicting port and the PID of the process using this port will be displayed in the launch window. Please kill the process with this PID and click **Retry** to launch the tpNMS again.

1. For example, the tpNMS encounters with a port conflict in initialization.

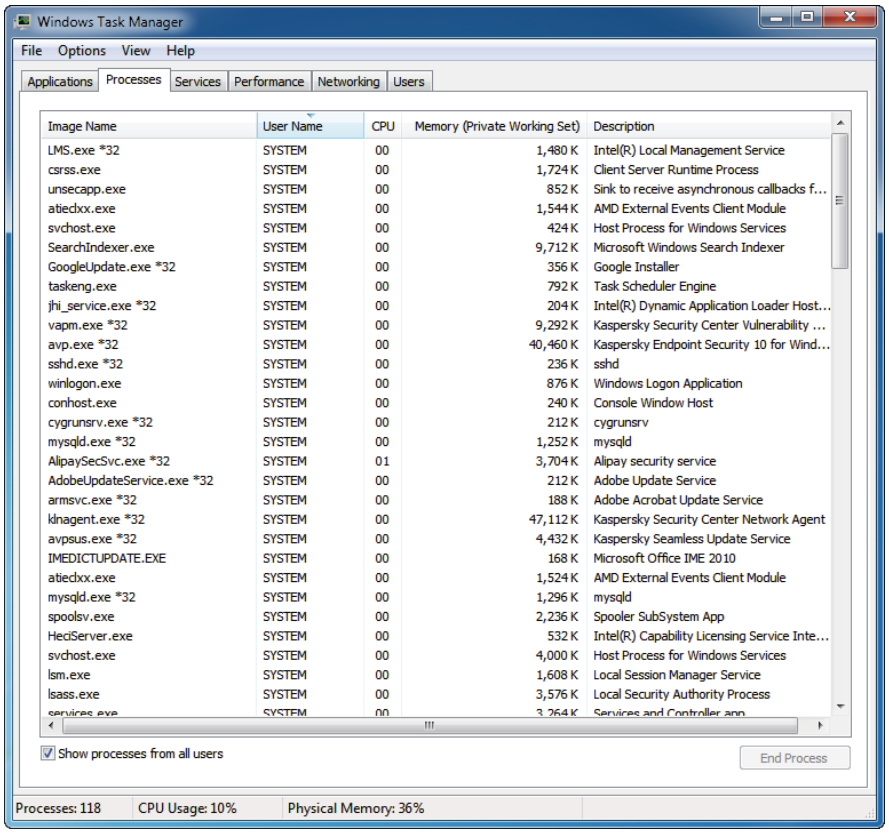
Figure 1-5 Initializing error



We can see that the conflict port is 162 and the process with PID 2540 is occupying this port.

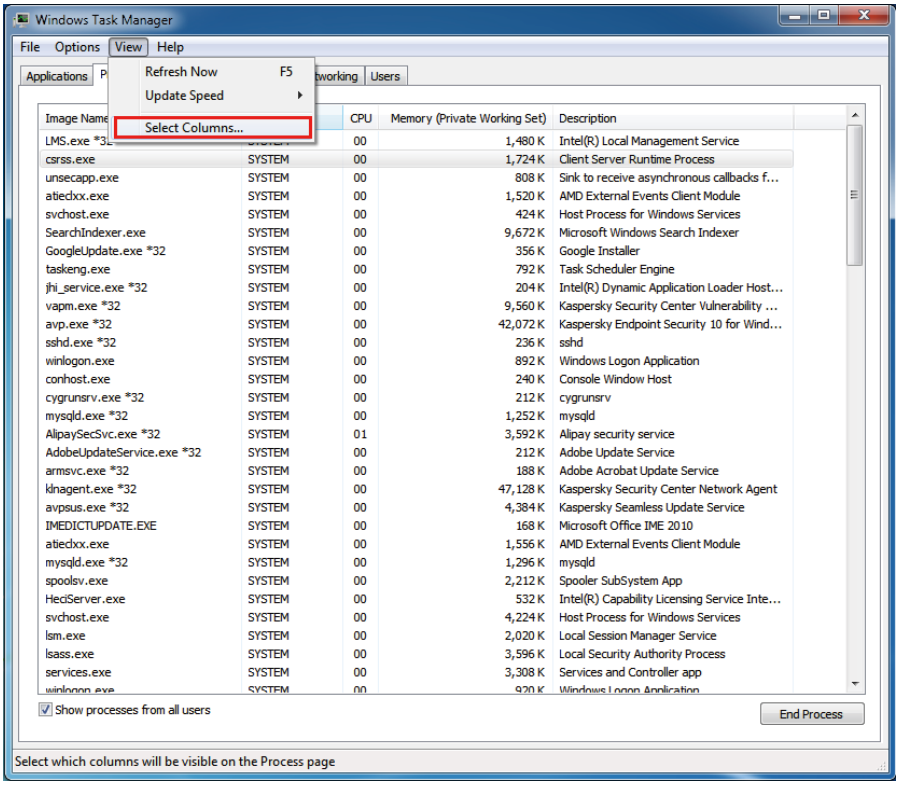
2. Open the **Processes** tab in the **Windows Task Manager**.

Figure 1-6 Windows task manager



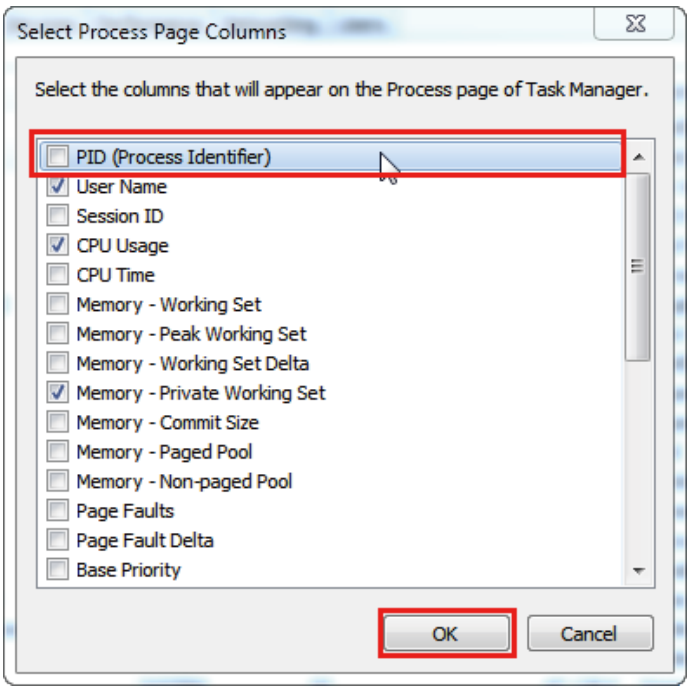
3. Click **View** and select **Select Columns...**.

Figure 1-7 Select columns



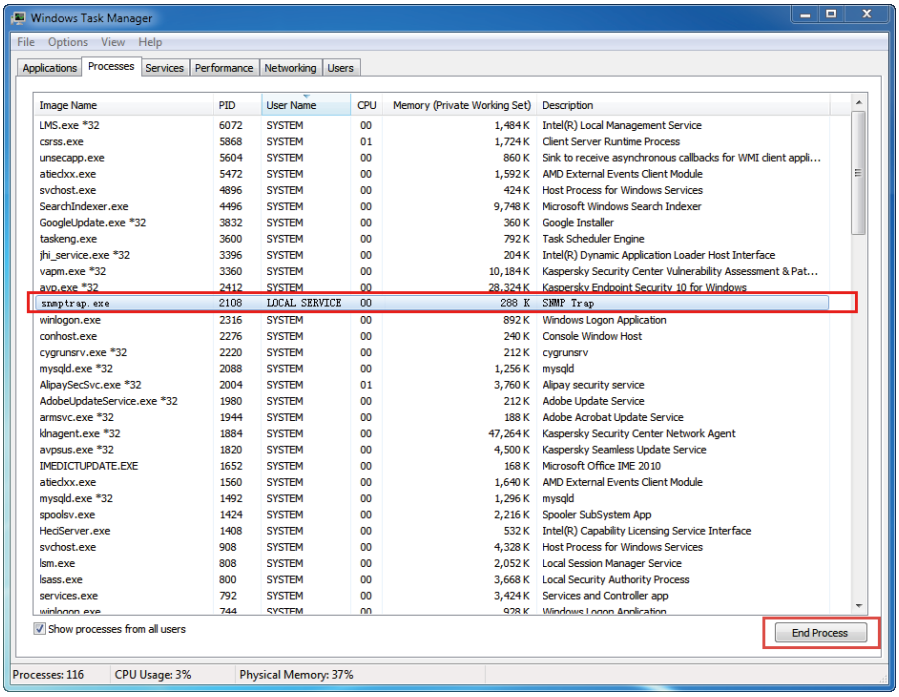
In the pop-up window, select the PID (Process Identification) and click **OK**.

Figure 1-8 Show the PID column



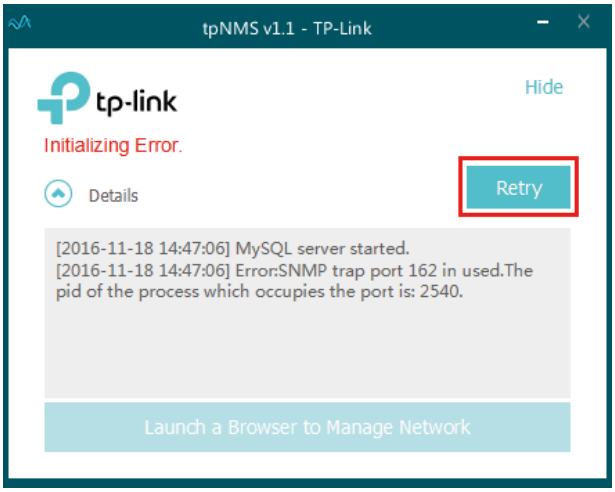
4. Kill the process that occupying the conflict port. Click the process with the specified PID and click the **End Process**.

Figure 1-9 Kill the conflicting process



5. Click **Retry** to launch tpNMS again.

Figure 1-10 Launch tpNMS again



1.3.3 Log in to tpNMS

tpNMS uses a browser-server architecture. Administrators and other types of users can access tpNMS from any accessible host in the network. Before you log in to tpNMS, please make sure that tpNMS host has a static IP address.

Note:

Since tpNMS supports multiple users' operations at the same time, we recommend that different users coordinate their application activities. Thus the modifications on the screen made by one user are not inadvertently changed by another user.

1. Open a browser and connect to tpNMS through the static IP address of the tpNMS host and the port 8843.

   · To connect to tpNMS from the tpNMS host, enter the URL **https://127.0.0.1:8843/**.

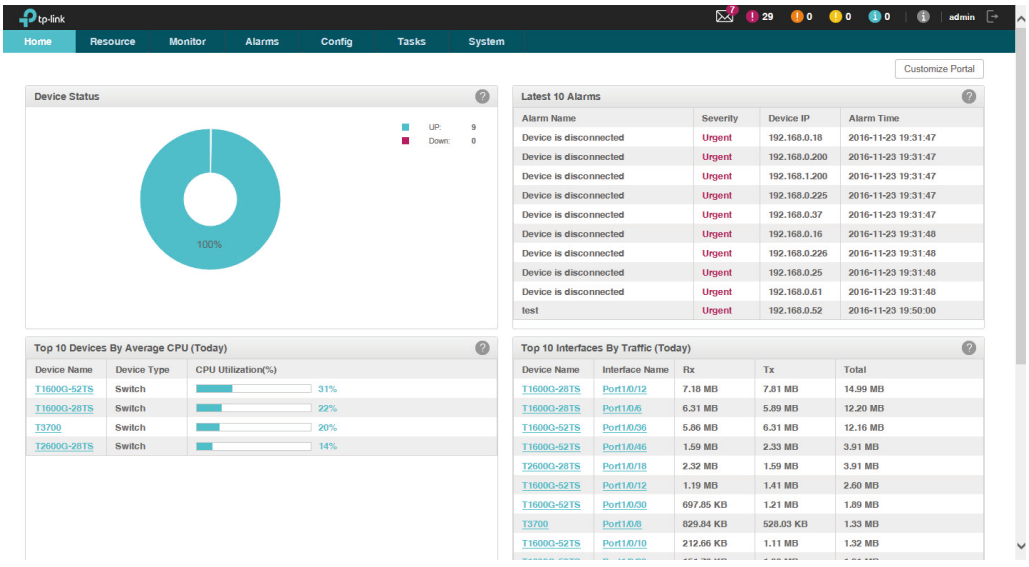
   · To connect to tpNMS from a remote computer, replace 127.0.0.1 with the IP address of the tpNMS host. For example, enter **https://1.1.1.100:8843/**, in which **1.1.1.100** is the IP address of the tpNMS host and **8843** is the port number for the tpNMS server.

2. After you connect to tpNMS, enter the default account and password (both are **admin**) in the Login screen to sign in.

   Figure 1-11 Login window

3. The Home screen displays as below.

   Figure 1-12 Home page



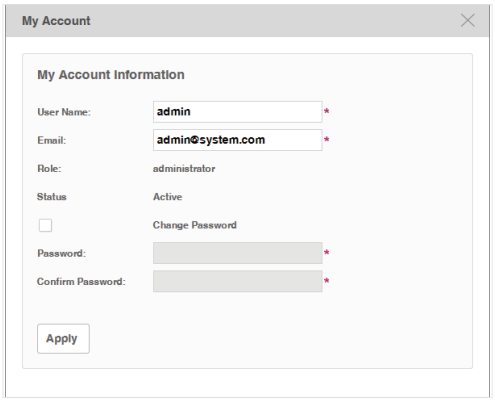
1.4 Change Your Password and Email

It is suggested to change the **admin** user's default password for safety considerations. tpNMS defines three types of roles: administrator, operator and observer. Only administrators have the authority to modify the user's user name, password and email.

Following the steps below to modify your password and email address.

1. Click admin in the top right corner of the page and the following My Account window will pop up.

Figure 1-13 Modify account information



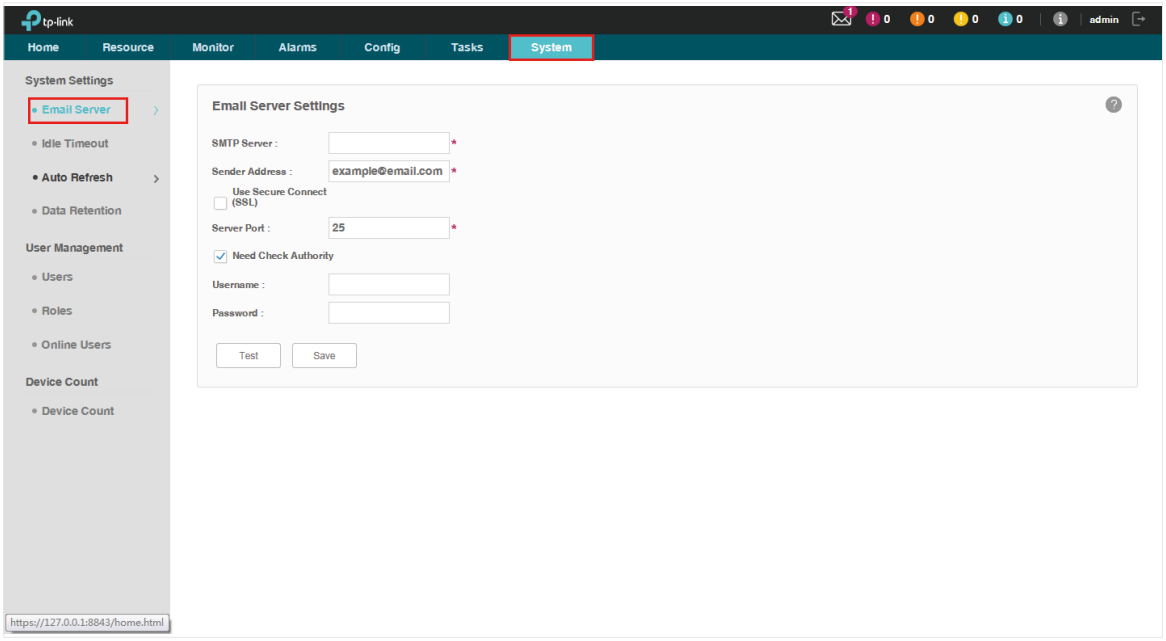
2. Modify the Email address of the **admin** user.
3. Select the **Change Password** check box. Enter the new password and re-enter to confirm.
4. Click **Apply** to save your changes.

1.5 Set the Email Server for Alarm Notifications

Before tpNMS can send alarm notifications, you should configure the email server settings. Only an administrator role user can configure the alarm email server settings.

1. Go to **System > System Settings > Email Server**.

Figure 1-14 Configure Email server settings



2. Enter your SMTP server address in the **SMTP Server** field. For example: smtp.gmail.com.
3. Enter your email address in the **Sender Address** field. For example: jerry@gmail.com.
4. If you want to encrypt the communications between the server and the recipient, select the **Use Secure Connect (SSL)** check box.
5. Enter your SMTP server port in the **Server Port** field.
6. If your SMTP server requires authentication, select the **Need Check Authority** check box and enter your user name and password for your email account.
7. Click the **Test** button to verify your email server settings. A test mail will be sent from the sender to itself, to verify the settings of the email server and the user credentials are correct.
8. Click the **Save** button to save your email server settings.

2 Monitor Network

With tpNMS you can monitor the summary information about the network, devices and interfaces. You can monitor the device status, the network topology, the latest alarms and the top 10 widgets for devices and interfaces by certain criteria. You can customize these widgets on the Home screen. This chapter includes the following sections:

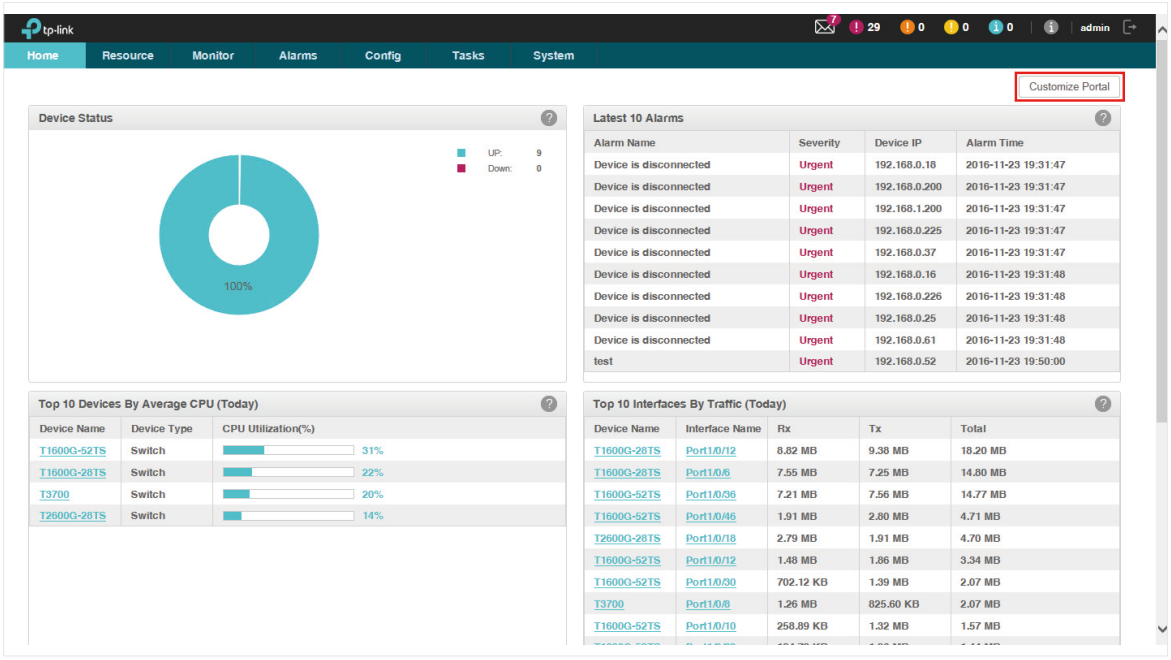
- *Customize the Widgets on the Home Screen*
- *View the Widgets*

2.1 Customize the Widgets on the Home Screen

You can add, delete or re-sort the widgets displayed on the Home screen.

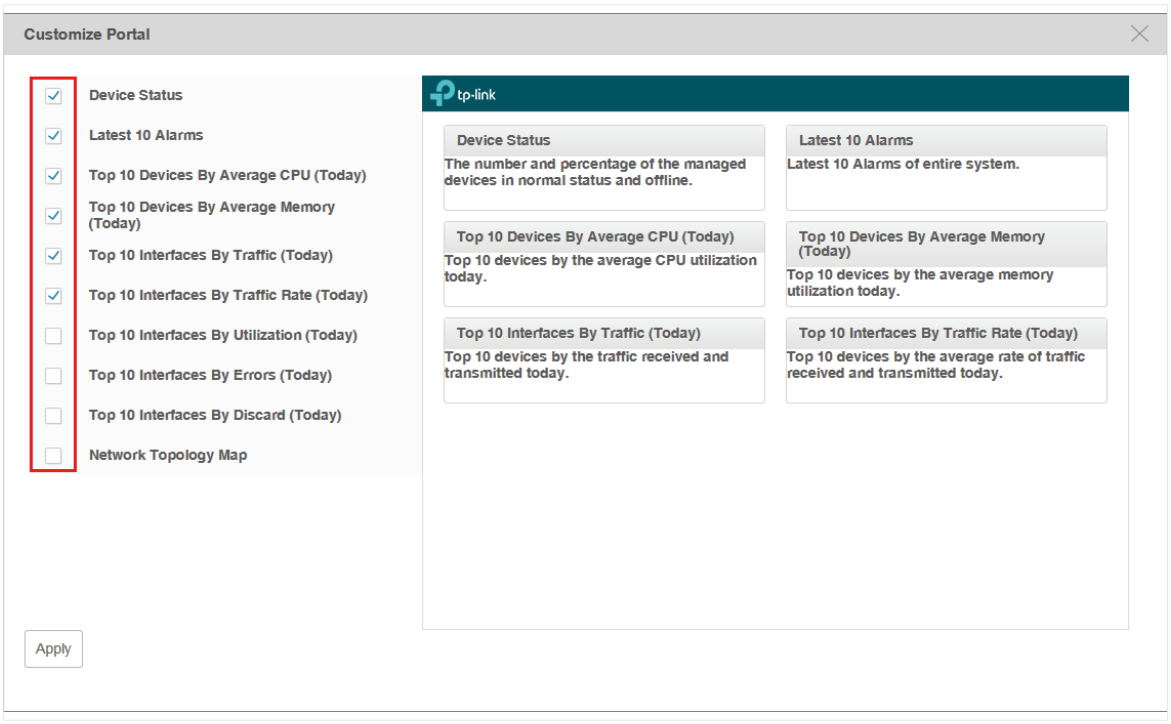
1. Go to **Home** screen.
2. Click **Customize Portal** in the upper right corner of the **Home** screen.

Figure 2-1 Home screen customize



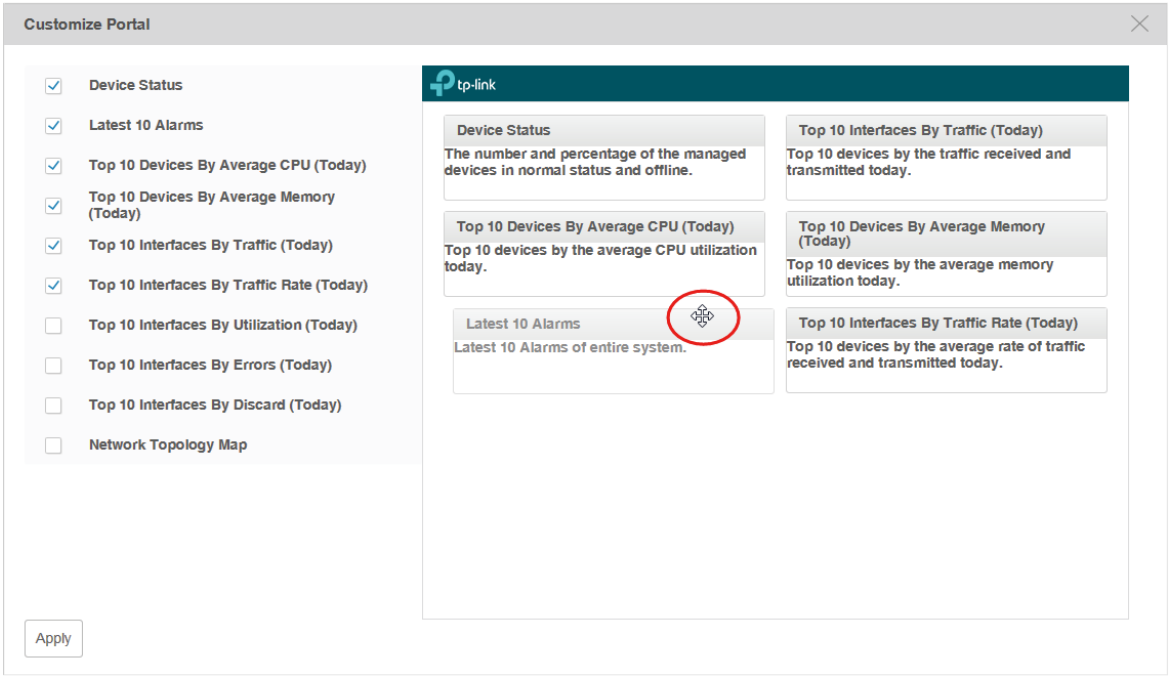
3. Select a checkbox to add the widget. Deselect a checkbox to delete the widget.

Figure 2-2 Add or delete the widgets



4. The right part is a thumbnail of the Home page. Drag the widgets to re-sort their display order. When you move the cursor onto the title bar of a widget, the cursor will turn into a four-head arrow. Click and hold the title bar to drag the widget to the place you want, and release the left button of your mouse to complete the operation.

Figure 2-3 Re-sort the widgets

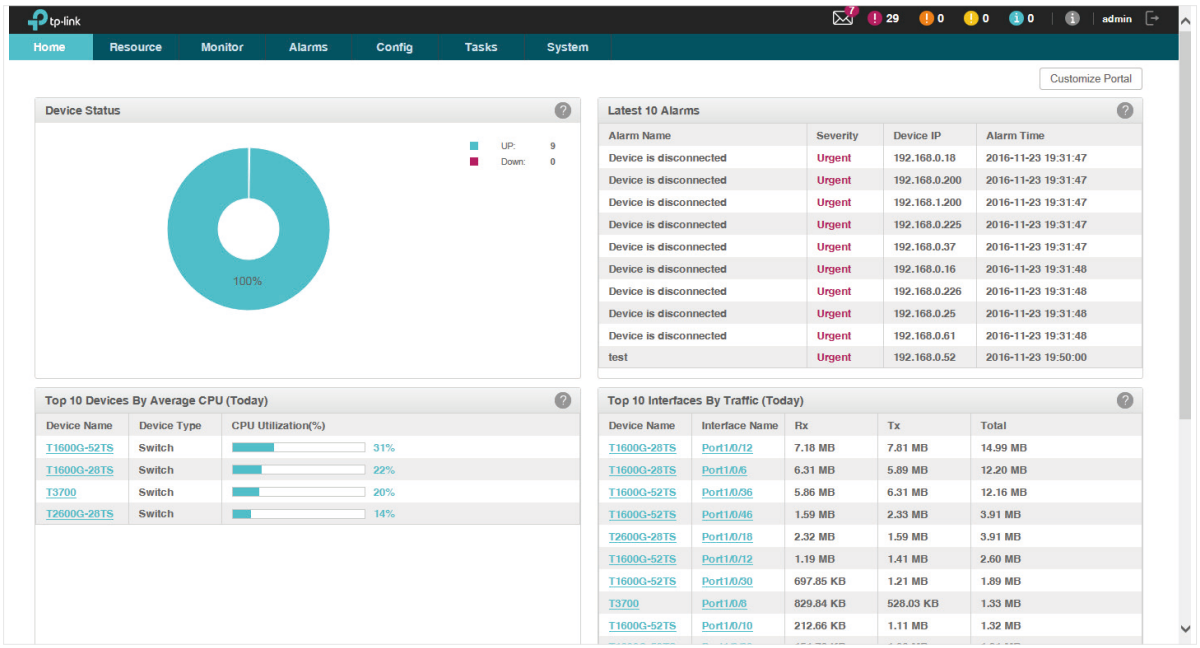


5. Click **Apply** to save your changes.

2.2 View the Widgets

You can view the widgets displayed on the Home page.

Figure 2-4 Home page view



You can click the device name or interface name in the tables to view their detailed information.

The widgets and the elements they contain are introduced below.

Widget Label	Description	Default Items Displayed
Device Status	The number and percentage of the managed devices online and offline.	**The percentage of the online devices** **The percentage of the offline devices** **The number of the online devices** **The number of the offline devices**
Latest 10 Alarms	The latest 10 alarms of the entire network.	**Alarm Name** **Severity** **Device IP** **Alarm Time**

Widget Label	Description	Default Items Displayed
Top 10 Devices By Average CPU (Today)	Top 10 devices by the average CPU utilization today. Click device name to show device detail view.	**Device Name** **Device Type** **CPU Utilization (%)**
Top 10 Devices By Average Memory (Today)	Top 10 devices by the average memory utilization today. Click device name to show device detail view.	Device Name Device Type Memory Utilization (%)
Top 10 Interfaces By Traffic (Today)	Top 10 devices by the traffic received and transmitted today. Click device name to show device detail view. Click interface name to show interface detail view.	Device Name Interface Name Rx Tx Total
Top 10 Interfaces By Traffic Rate (Today)	Top 10 devices by the average rate of traffic received and transmitted today. Click device name to show device detail view. Click interface name to show interface detail view.	Device Name Interface Name Rx (bps) Tx (bps) Total (bps)
Top 10 Interfaces By Utilization (Today)	Top 10 interfaces by the average utilization on both receiving and transmitting today. Click device name to show device detail view. Click interface name to show interface detail view.	Device Name Interface Name Rx Utilization Tx Utilization Total
Top 10 Interfaces By Errors (Today)	Top 10 devices by errors on both receiving and transmitting today. Click device name to show device detail view. Click interface name to show interface detail view.	Device Name Interface Name Rx Errors Tx Errors Total
Top 10 Interfaces By Discard (Today)	Top 10 devices by discards on both receiving and transmitting today. Click device name to show device detail view. Click interface name to show interface detail view.	Device Name Interface Name Rx Discards Tx Discards Total
Network Topology Map	The network topology of the managed devices. Double click the node in the map to jump to the Network Topology tab and see the detailed map information.	

3 Discover and Manage Resources

With tpNMS you can manage the resources in the network, including devices, interfaces and Topology. This chapter includes the following sections:

- *Discover Devices on Your Network*
- *View and Manage Devices*
- *Import Devices*
- *Add Devices into Groups*
- *View and Manage Links on Your Network*
- *Manage Maps and Topologies*

3.1 Discover Devices on Your Network

- *Schedule a Discovery Job*
- *Manage Discovery Templates*

3.1.1 Schedule a Discovery Job

The discovery profile can filter the devices that tpNMS can detect. tpNMS can discover devices by a single IP or in an IP range, device name, SNMP template and Telnet template.

To obtain the monitoring statistics from the target switch, you should configure the SNMP-related function in the target switch, and configure the SNMP Template in this section the same with the settings in the target switch.

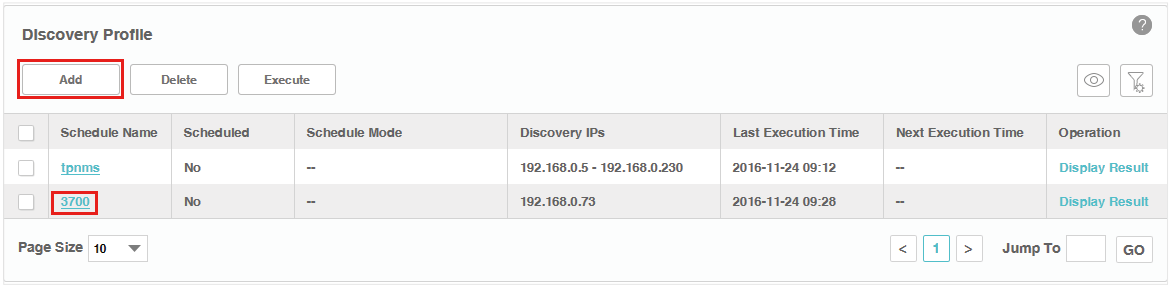
To backup, restore and upgrade the target switch successfully, you should configure the Telnet Template in this section the same with the telnet settings in the target switch.

- *Add or modify a discovery profile*
- *Delete a discovery profile*

Add or modify a discovery profile

1. Go to **Resource > Device Management > Device Discovery**.
2. Click **Add** to create a new discovery profile, or click the schedule name in the table to modify the schedule.

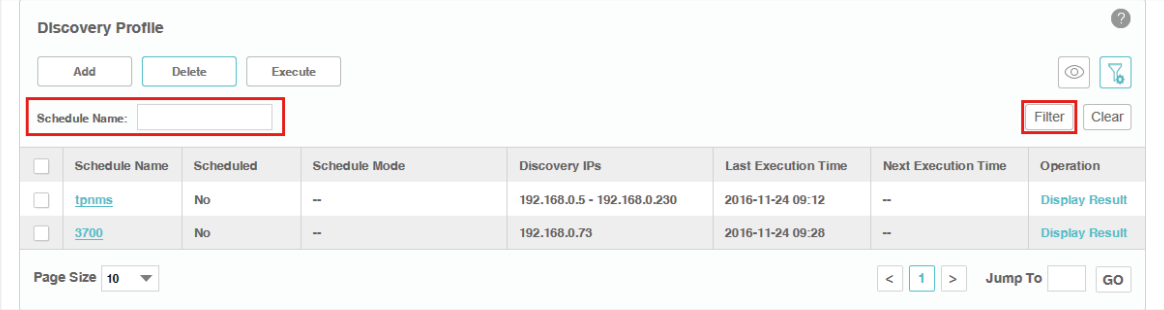
Figure 3-1 Schedule modify



To add or delete columns displayed in the device list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

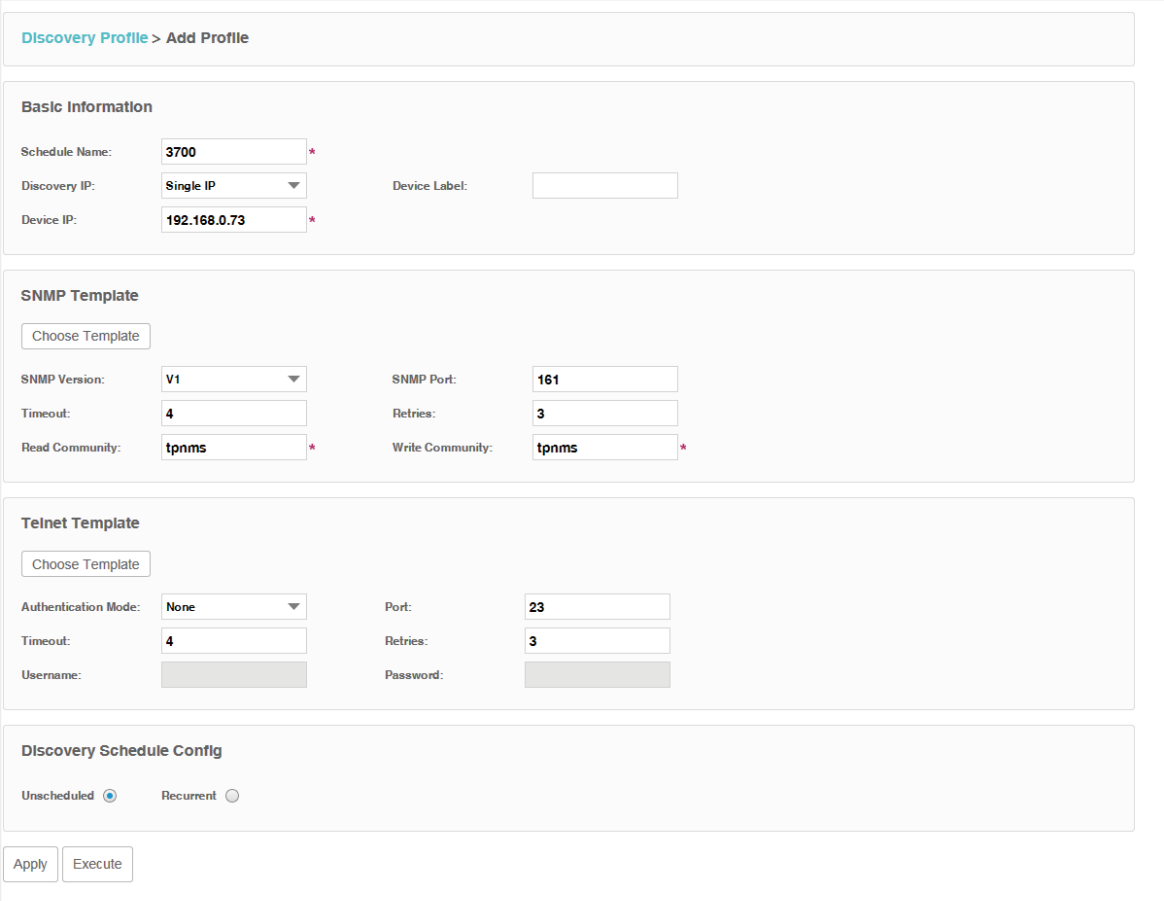
To filter the schedules in the list, click the  . Enter the Schedule Name and click **Filter**.

Figure 3-2 Schedule filter



3. Edit the discovery schedule's information.

Figure 3-3 Edit schedule's basic information



Basic Information

Schedule Name	Enter the name of the schedule.
Discovery IP	Specify the target IP type as Single IP or IP Range.
Device IP	Enter the target device's IP address or IP address range.

Device Label	Assign a device label to the device discovered if you select Single IP.

SNMP Template

Click **Choose Template** or edit the SNMP Template manually.

SNMP Version	Select the SNMP version.
SNMP Port	Enter the SNMP port, which is 161 by default.
Timeout	Enter the timeout value, which is 4 seconds by default. The target device will be assumed as unaccessible if it doesn't respond within the timeout value.
Retries	Enter the number of SNMP query messages that tpNMS sends, which is 3 by default.
Read Community (v1/v2c only)	Enter the read community strings to match the target device for authentication.
Write Community (v1/v2c only)	Enter the write community strings to match the target device for authentication.
Security Name (v3 only)	Enter the user name to log in the switch.
Context Name (v3 only)	Enter the SNMP context.
Authentication Mode (v3 only)	Select the Authentication Mode for the SNMP v3 User. • None: No authentication method is used. • MD5: The port authentication is performed via HMAC-MD5 algorithm. • SHA: The port authentication is performed via SHA (Secure Hash Algorithm). This authentication mode has a higher security than MD5 mode.
Authentication Key (v3 only)	Enter the password for authentication.
Privacy Mode (v3 only)	Select the Privacy Mode for the SNMP v3 User. • None: No privacy method is used. • DES: DES encryption method is used.
Privacy Key (v3 only)	Enter the Privacy Password.

Telnet Template

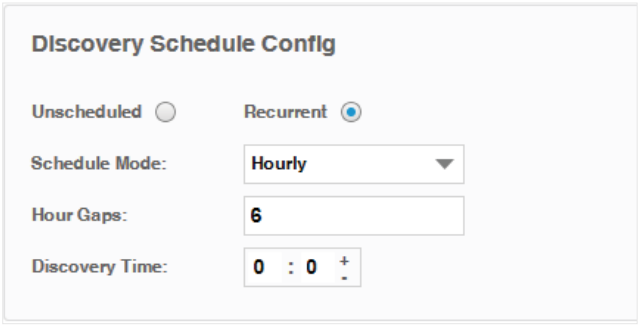
Click **Choose Template** or edit the Telnet Template manually. You must configure the correct telnet information for managing the device (backup, restore or upgrade actions). The name and password in the telnet template are the same user information

that you use to telnet in to the device to perform system configuration.

Authentication Mode	Select the authentication mode to telnet the target device.
Port	Enter the port for telnet connection, which is 23 by default.
Timeout	Enter the timeout value, which is 4 seconds by default.
Retries	Enter the number of retries, which is 3 by default.
Username	Enter the username for the telnet connection.
Password	Enter the password for the telnet connection.

Discovery Schedule Config

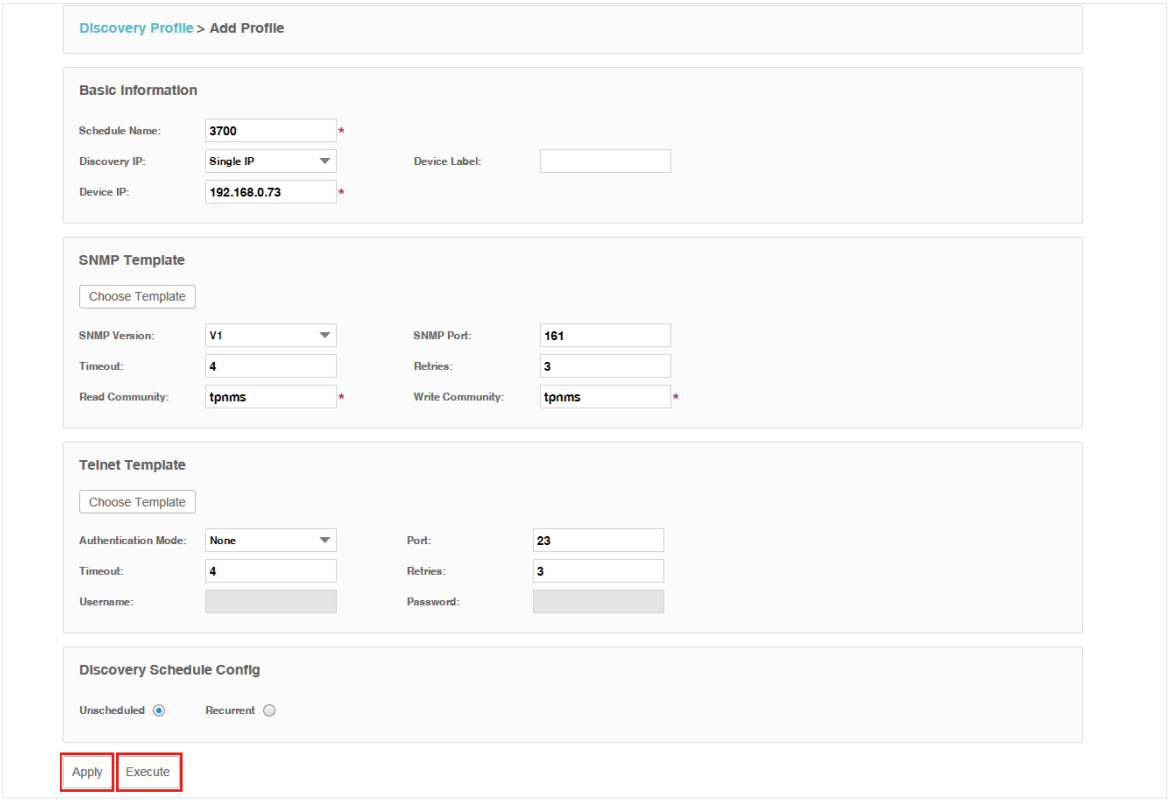
Figure 3-4 Choose schedule's execute circle



Unscheduled	Select Unscheduled and the discovery job will not be executed.
Recurrent	Select Recurrent and the discovery job will be executed periodically.
Schedule Mode	Select the recurrent mode as Hourly, Daily, Weekly or Monthly. Configure the exact time of the discovery schedule according to the schedule mode you choose.

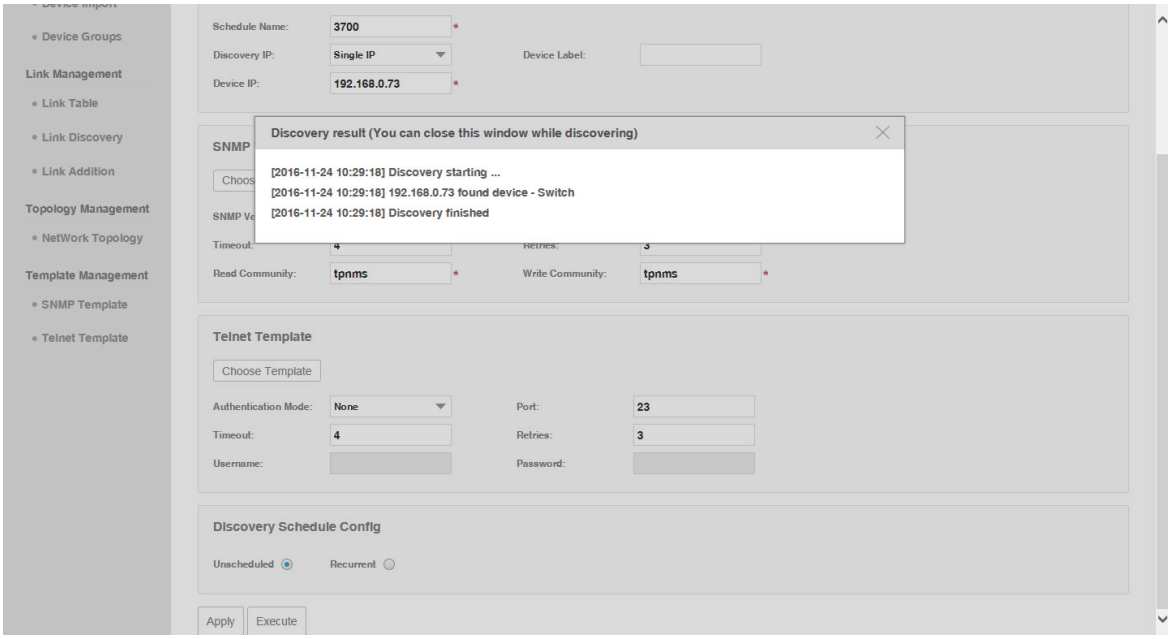
4. Click **Apply** to save this profile. Click **Execute** to run this schedule immediately.

Figure 3-5 Save or execute a schedule



5. An example of discovery result is displayed below.

Figure 3-6 Discovery result



Delete a discovery profile

Click **Delete** to remove the selected discovery schedule from the table.

Figure 3-7 Delete a discovery schedule

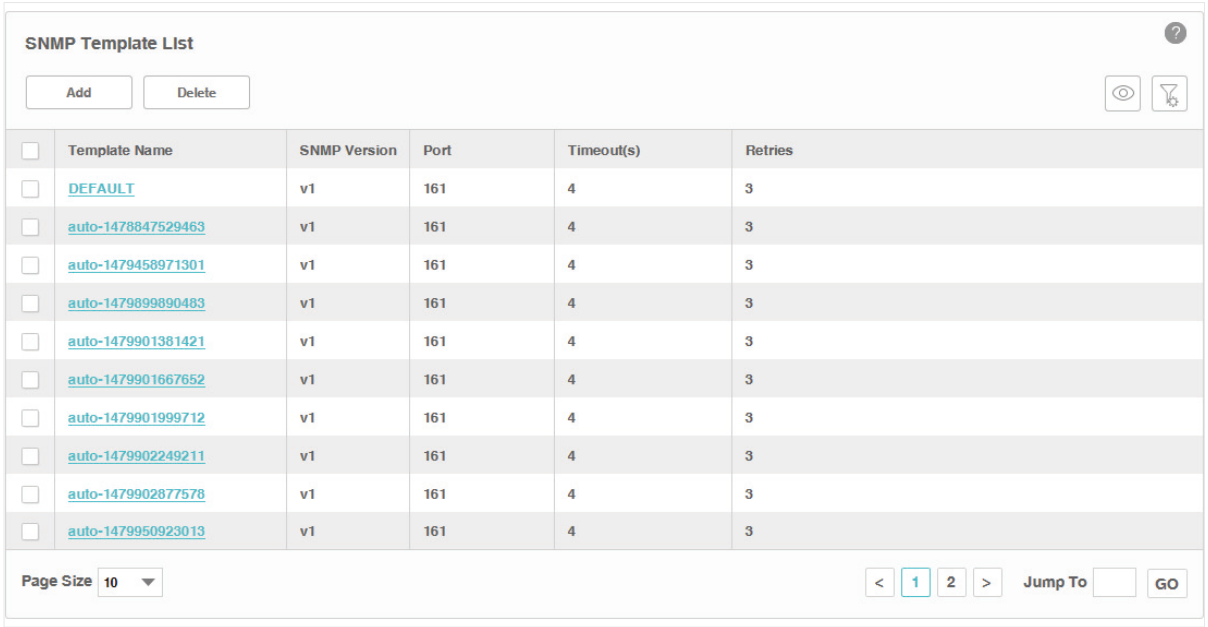
3.1.2 Manage Discovery Templates

- *Add or modify an SNMP Template*
- *Add or modify a Telnet Template*

Add or modify an SNMP Template

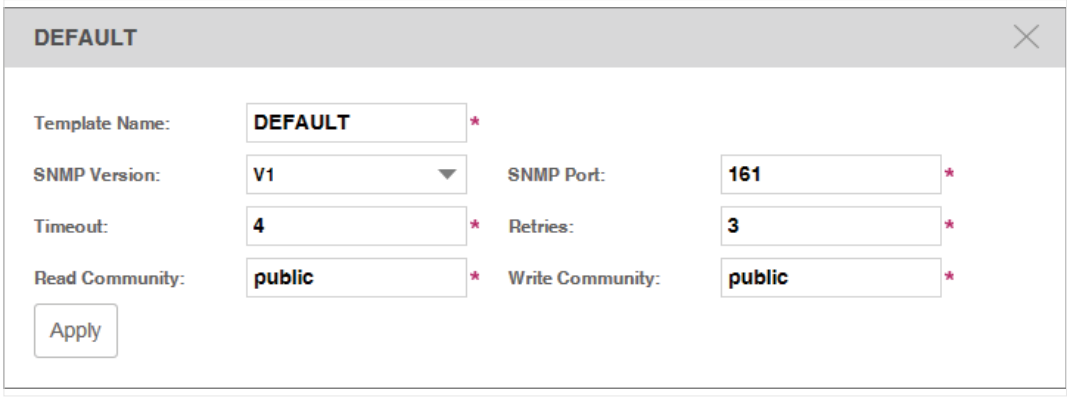
You can manage SNMP Templates on the **Resource > Template Management> SNMP Template** screen.

Figure 3-8 Manage SNMP templates



Click **Add** or click the template name in the table to edit the template.

Figure 3-9 Add or edit an SNMP template



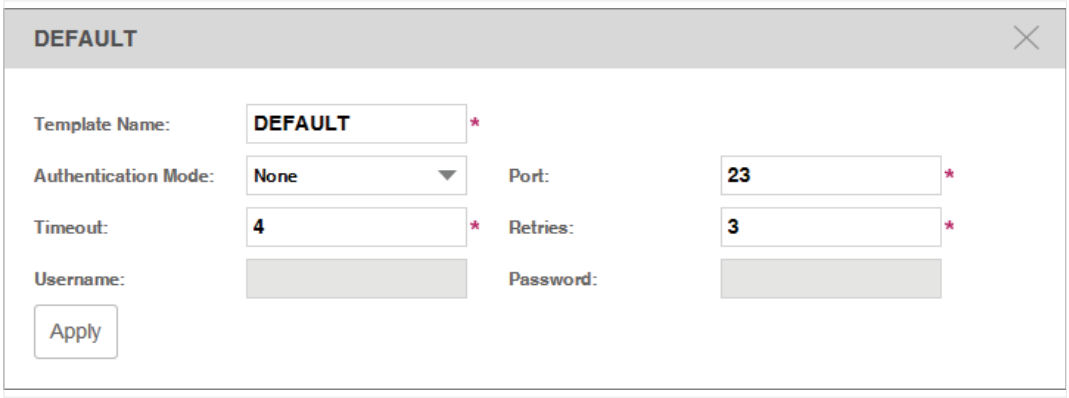
Add or modify a Telnet Template

You can manage Telnet Templates on the **Resource** > **Template Management** > **Telnet Template** screen.

Figure 3-10 Manage Telnet templates

Click **Add** or click the template name in the table to edit the template.

Figure 3-11 Add or edit an Telnet template



3.2 View and Manage Devices

This section describes the following tasks that you can perform:

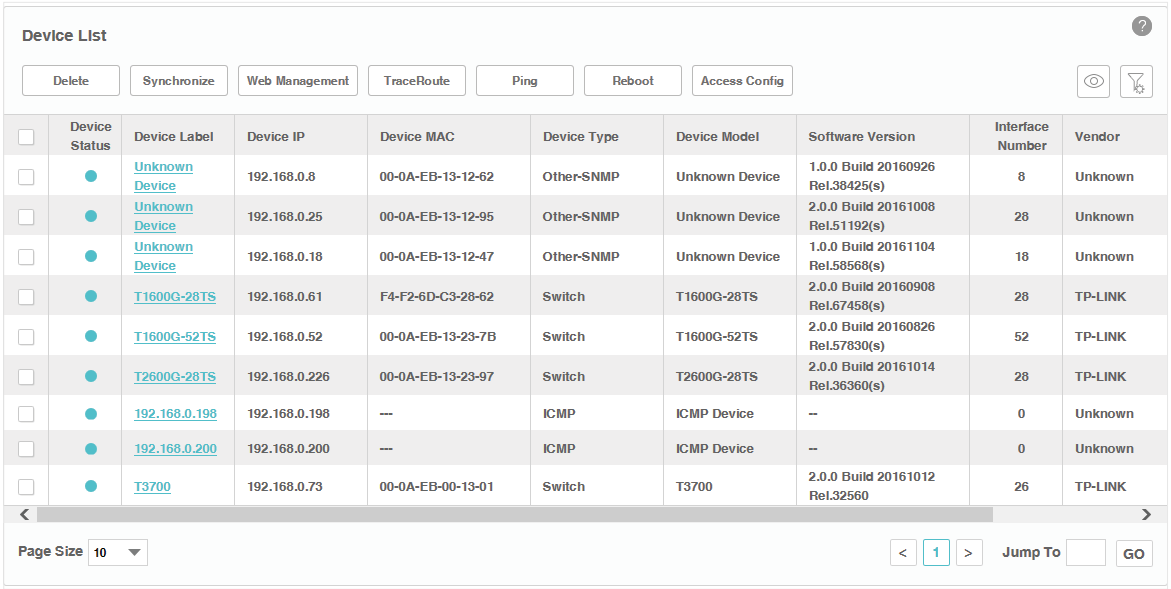
- *View the Device List*
- *Remove a Device*
- *Synchronize a Device*
- *Log in to a Device*
- *Ping or Traceroute a Device*
- *Reboot a Device*
- *Access Config*

You can manage devices on the **Resource > Device Management > Device Table** screen.

3.2.1 View the Device List

1. Go to **Resource > Device Management > Device Table**. The screen displays all the devices that the application has discovered.

Figure 3-12 Device list

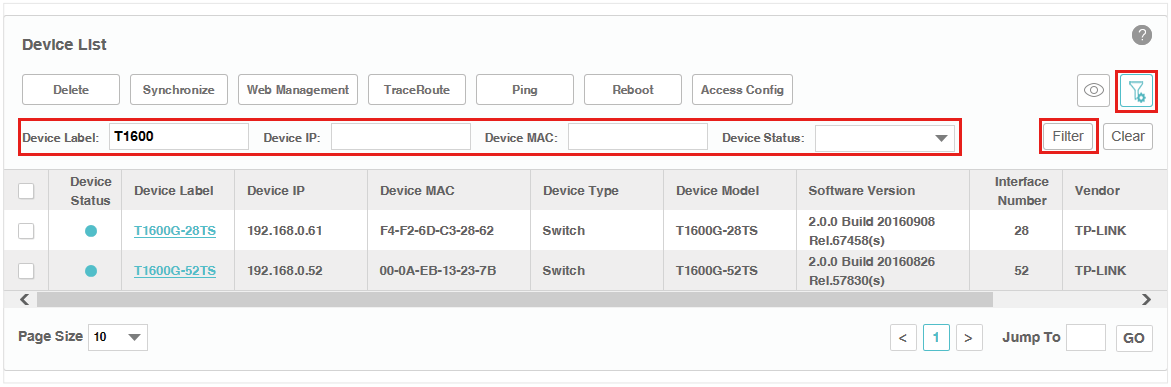


Device Status	Device Label	Device IP	Device MAC	Device Type	Device Model	Software Version	Interface Number	Vendor
●	Unknown Device	192.168.0.8	00-0A-EB-13-12-62	Other-SNMP	Unknown Device	1.0.0 Build 20160926 Rel.38425(s)	8	Unknown
●	Unknown Device	192.168.0.25	00-0A-EB-13-12-95	Other-SNMP	Unknown Device	2.0.0 Build 20161008 Rel.51192(s)	28	Unknown
●	Unknown Device	192.168.0.18	00-0A-EB-13-12-47	Other-SNMP	Unknown Device	1.0.0 Build 20161104 Rel.58568(s)	18	Unknown
●	T1600G-28TS	192.168.0.61	F4-F2-6D-C3-28-62	Switch	T1600G-28TS	2.0.0 Build 20160908 Rel.67458(s)	28	TP-LINK
●	T1600G-52TS	192.168.0.52	00-0A-EB-13-23-7B	Switch	T1600G-52TS	2.0.0 Build 20160826 Rel.57830(s)	52	TP-LINK
●	T2600G-28TS	192.168.0.226	00-0A-EB-13-23-97	Switch	T2600G-28TS	2.0.0 Build 20161014 Rel.36360(s)	28	TP-LINK
●	192.168.0.198	192.168.0.198	---	ICMP	ICMP Device	--	0	Unknown
●	192.168.0.200	192.168.0.200	---	ICMP	ICMP Device	--	0	Unknown
●	T3700	192.168.0.73	00-0A-EB-00-13-01	Switch	T3700	2.0.0 Build 20161012 Rel.32560	26	TP-LINK

2. To add or delete columns displayed in the device list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

3. To filter the devices in the list, click the  . Enter the filter conditions and click **Filter**.

Figure 3-13 An example of filtering the T1600 series switches



You can filter the listed devices through one or more of the following conditions: Device Label, Device IP, Device MAC and Device Status.

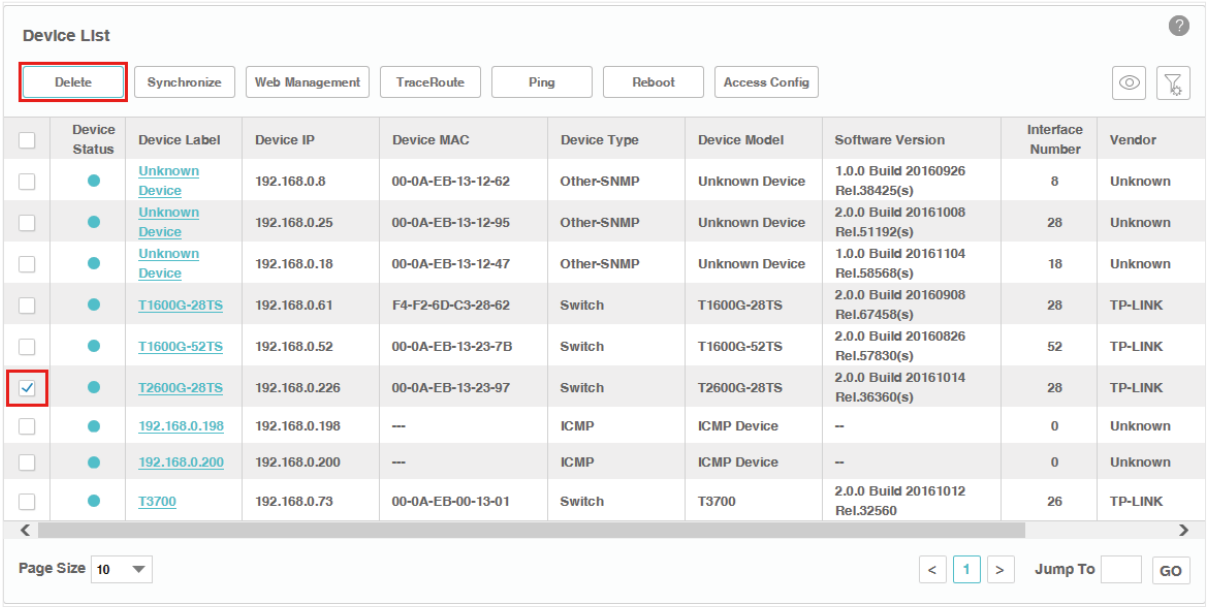
Click **Clear** to display all the discovered devices.

3.2.2 Remove a Device

Go to **Resource > Device Management > Device Table**.

Click **Delete** to remove the selected devices from the device table.

Figure 3-14 Remove a device

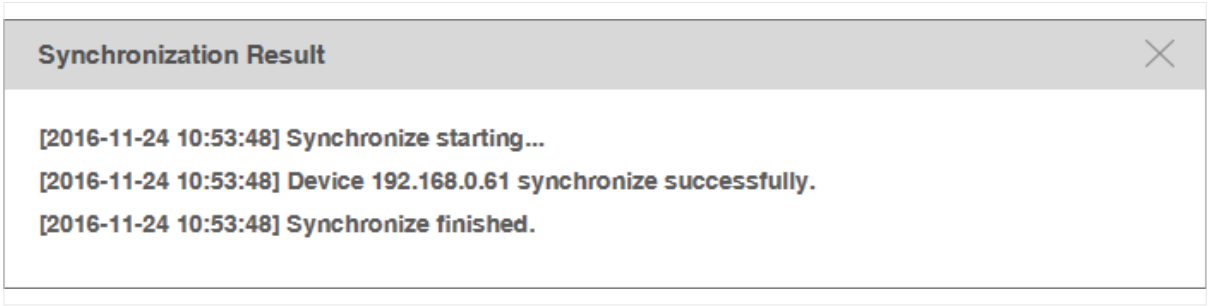


3.2.3 Synchronize a Device

Go to **Resource > Device Management > Device Table**.

Click **Synchronize** to synchronize the selected devices in the device table. The synchronization result pops up as below.

Figure 3-15 Synchronization result



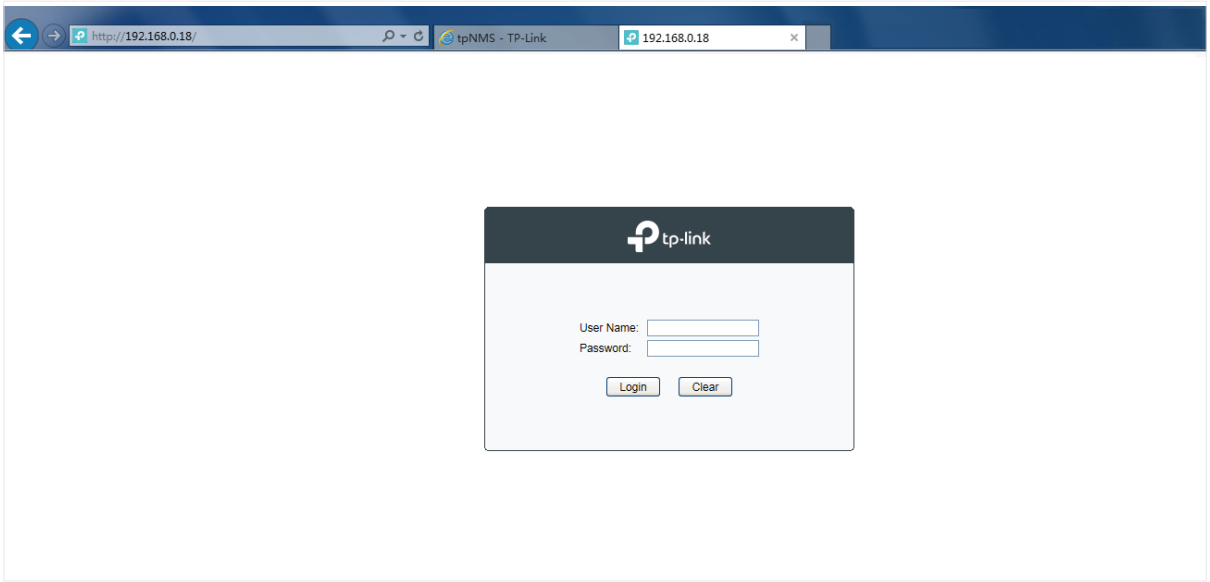
Your successful synchronization operation will synchronize the device's information to tpNMS immediately. By default the devices' information in this list is synchronized every 2 minutes.

3.2.4 Log in to a Device

Go to **Resource > Device Management > Device Table**.

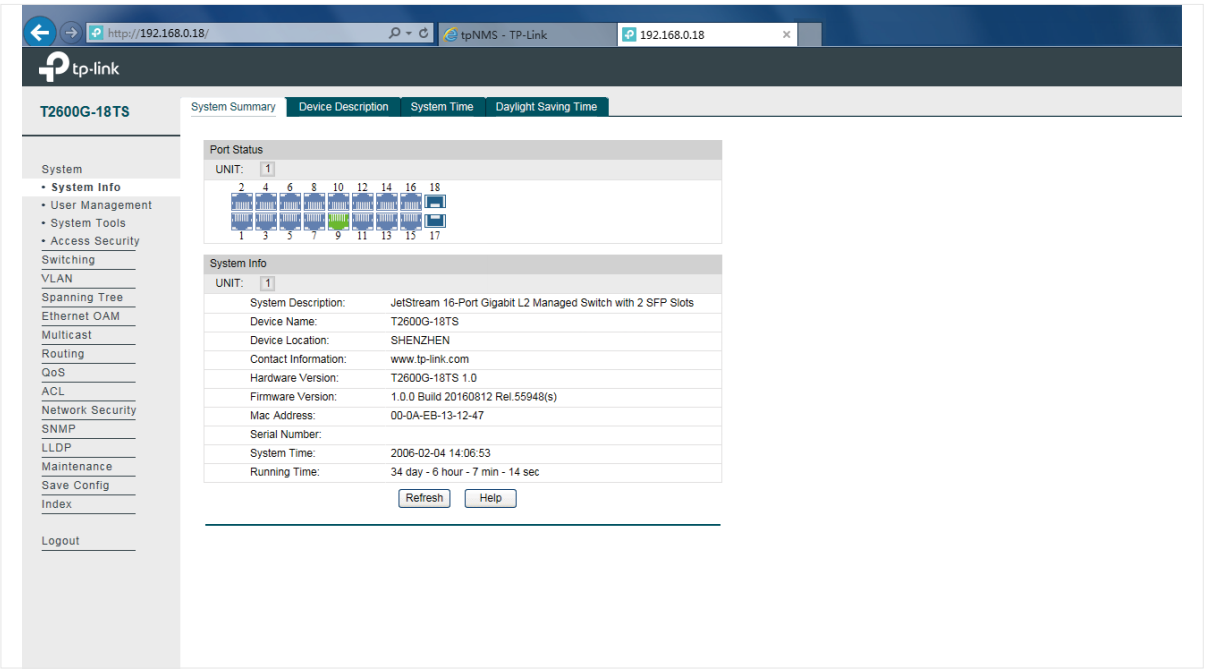
Select a device and click **Web Management** to log into the device's web interface. The login interface opens in a new tab. This connection uses the TCP port 80, which cannot be changed.

Figure 3-16 Log in to the device



Enter the username and password to log in to the device. For TP-Link switches, the default User Name is admin and the default Password is admin.

Figure 3-17 Login to the device's interface



3.2.5 Ping or Traceroute a Device

Go to **Resource > Device Management > Device Table**.

Click **Ping** or **Traceroute** to ping or traceroute the selected device in the device table. The result displays in the pop-up window.

Figure 3-18 Ping result

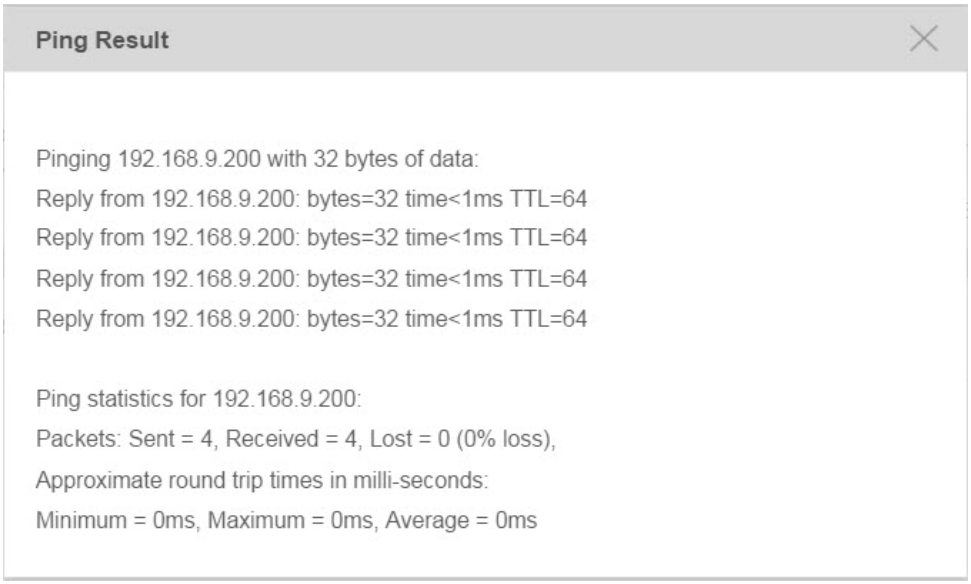
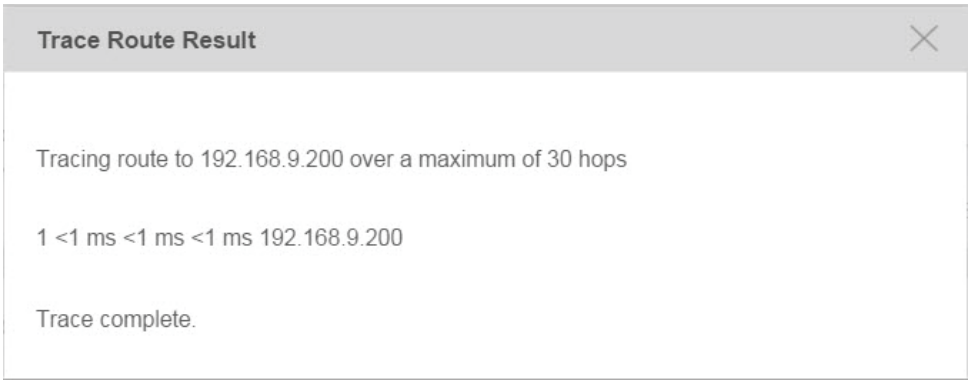


Figure 3-19 Traceroute result



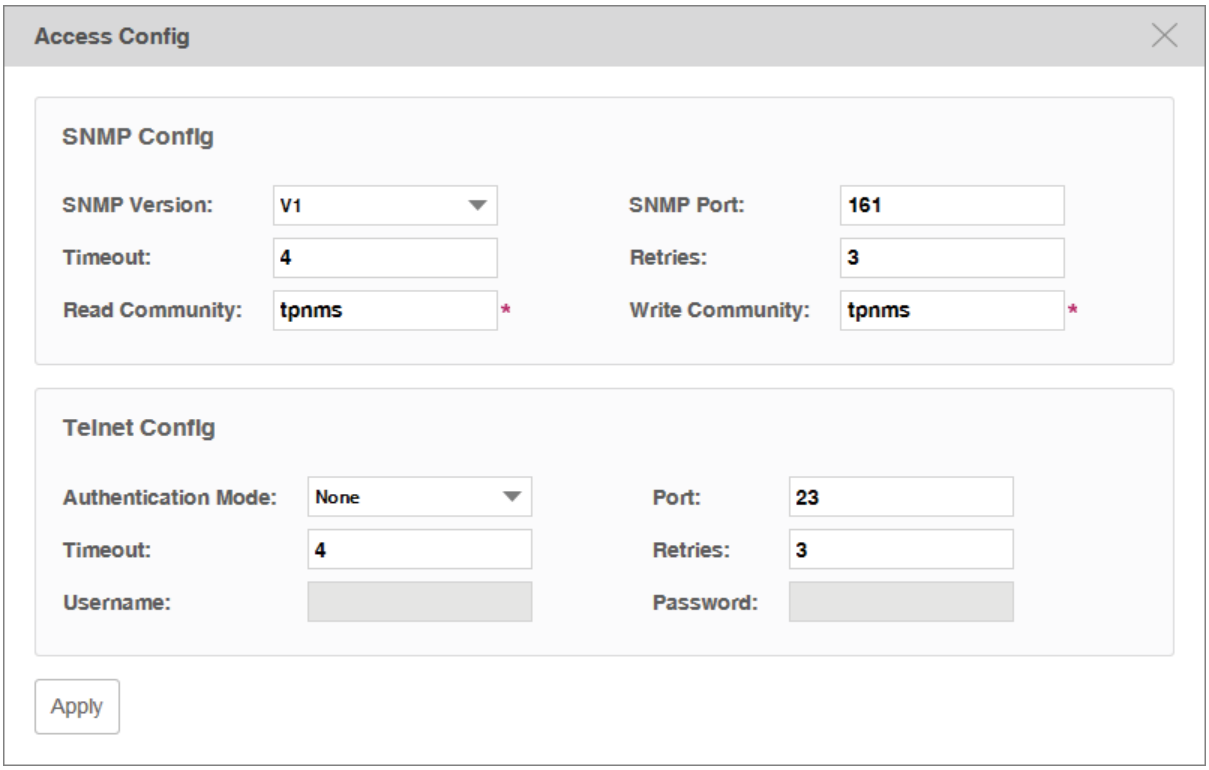
3.2.6 Reboot a Device

Go to **Resource > Device Management > Device Table**. Click **Reboot** to reboot the selected devices in the device table.

3.2.7 Access Config

Go to **Resource > Device Management > Device Table**. Click **Access Config** to configure the credentials that pertain to the devices you are trying to access.

Figure 3-20 Access configurations



SNMP Template

Configure the SNMP template to match the SNMP configurations on the target switches.

SNMP Version	Select the SNMP version as v1,v2c or v3.
SNMP Port	Enter the SNMP port, which is 161 by default.
Timeout	Enter the timeout value, which is 4 seconds by default. The target device will be assumed as unaccessible if it doesn't respond within the timeout value.
Retries	Enter the number of SNMP query messages that tpNMS sends, which is 3 by default.
Read Community (v1/v2c only)	Enter the read community strings to match the target device for authentication.
Write Community (v1/v2c only)	Enter the write community strings to match the target device for authentication.
Security Name (v3 only)	Enter the user name to log in the switch.
Context Name (v3 only)	Enter the SNMP context.
Authentication Mode (v3 only)	Select the Authentication Mode for the SNMP v3 User. • None: No authentication method is used. • MD5: The port authentication is performed via HMAC-MD5 algorithm. • SHA: The port authentication is performed via SHA (Secure Hash Algorithm). This authentication mode has a higher security than MD5 mode.
Authentication Key (v3 only)	Enter the password for authentication.
Privacy Mode (v3 only)	Select the Privacy Mode for the SNMP v3 User. • None: No privacy method is used. • DES: DES encryption method is used.
Privacy Key (v3 only)	Enter the Privacy Password.

Telnet Template

Edit the Telnet Template manually. You must configure the correct telnet information for further managing the device (backup, restore or upgrade actions).

Authentication Mode	Select the authentication mode to telnet the target device.

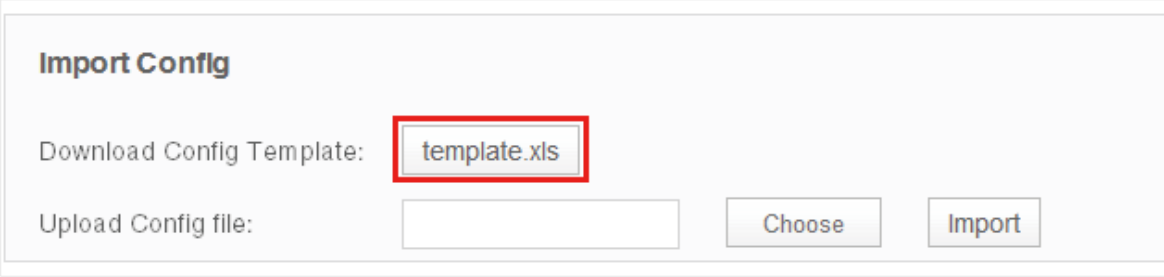
Port	Enter the port for telnet connection.
Timeout	Enter the timeout value, which is 4 seconds by default.
Retries	Enter the number of retries, which is 3 by default.
Username	Enter the username for the telnet connection.
Password	Enter the password for the telnet connection.

3.3 Import Devices

You can customize a template file and use the file as a criteria to search for devices in the network. Only the devices that match the customized conditions will be discovered. The Import Devices function gives you more control over the discovery process because the conditions you set are a bit more complicated.

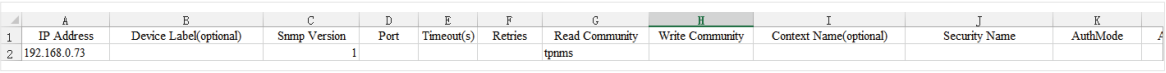
1. Go to **Resource > Device Management > Device Import**.
2. Click **template.xls** to download the excel file **Config Template**.

Figure 3-21 Download Config template



3. Edit the parameters in the downloaded template.xls.

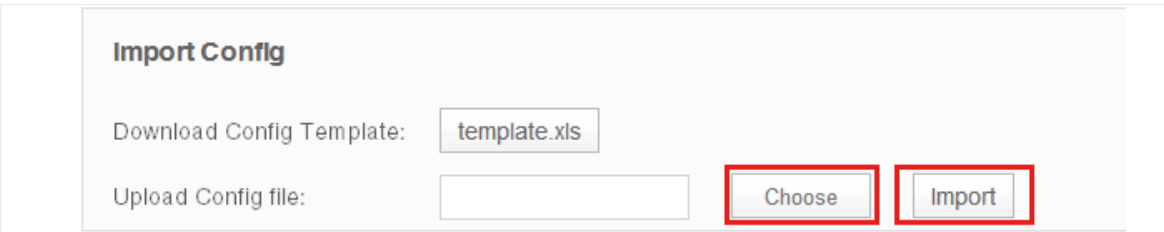
Figure 3-22 Edit template



	A	B	C	D	E	F	G	H	I	J	K
1	IP Address	Device Label(optional)	Snmp Version	Port	Timeout(s)	Retries	Read Community	Write Community	Context Name(optional)	Security Name	AuthMode
2	192.168.0.73		1				tpnms				

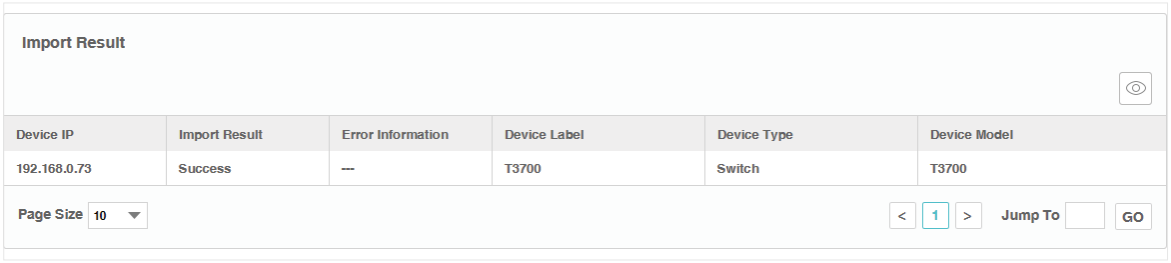
4. Upload customized template file to import devices that match the criteria.

Figure 3-23 Upload Config template and import devices



Click **Choose** to select your customized template file and click **Import** to search for devices that match the conditions.

Figure 3-24 Import result



Note:

If you want to manage the imported device (backup, restore or upgrade), you should go to the *Access Config* page and configure the device's telnet template. The name and password in the telnet template are the same user information that you use to telnet in to the device to perform system configuration.

3.4 Add Devices into Groups

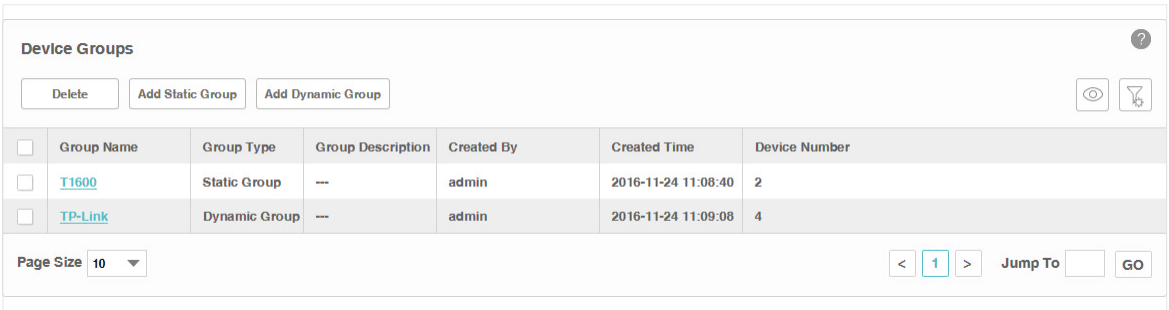
Once the devices are discovered, you can group them by model, category, location or other criteria. You can create static and dynamic device groups. Device group offers a convenient way for the batch backup, restore and update actions.

- *View Groups*
- *Add Devices to Static Group*
- *Add Devices to Dynamic Group*
- *Delete Groups*

3.4.1 View Groups

Go to **Resource > Device Management > Device Groups**. The device groups are displayed below.

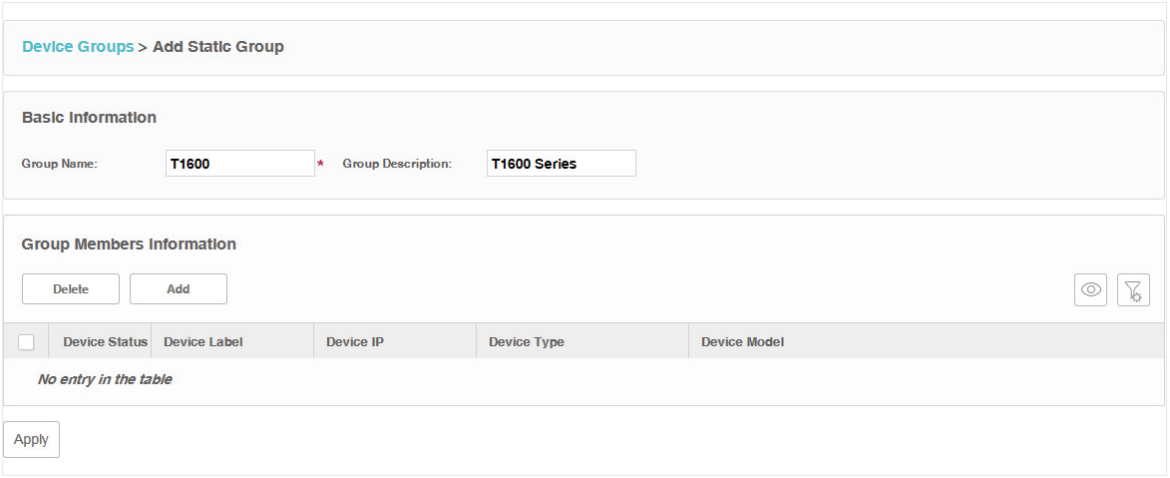
Figure 3-25 Device groups



3.4.2 Add Devices to Static Group

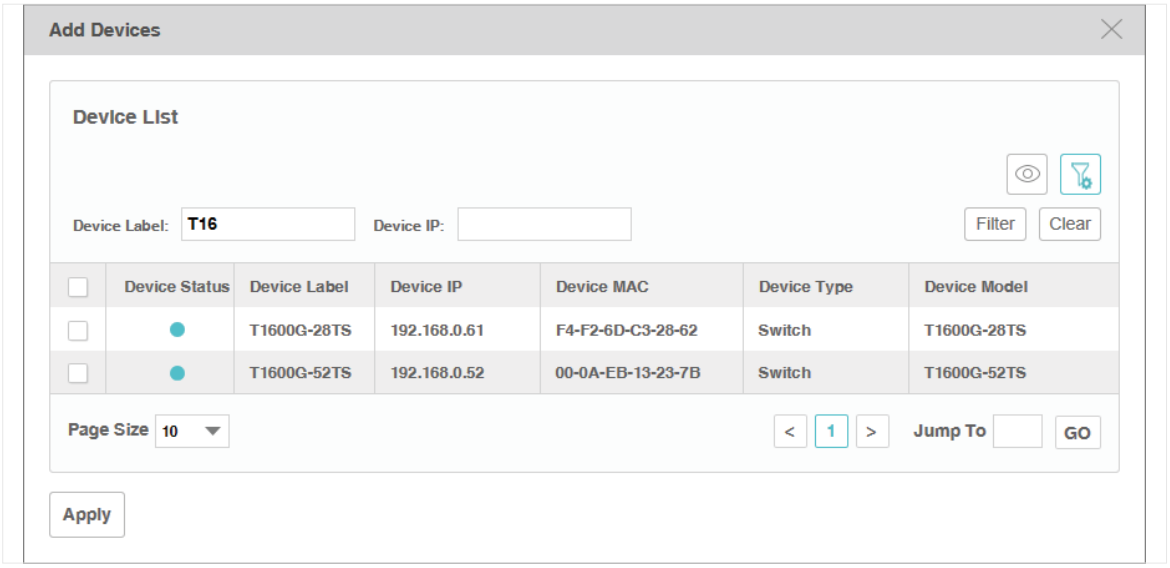
1. Go to **Resource > Device Management > Device Groups**.
2. Click **Add Static Group** to create a static device group. Enter the group name and description.

Figure 3-26 Create a static group



3. Click **Add** to add devices into the group.

Figure 3-27 Add Devices to a static group



You can select devices manually in the device list, or use the filter function to filter the specified devices. In this example all the T1600 series switches are filtered out.

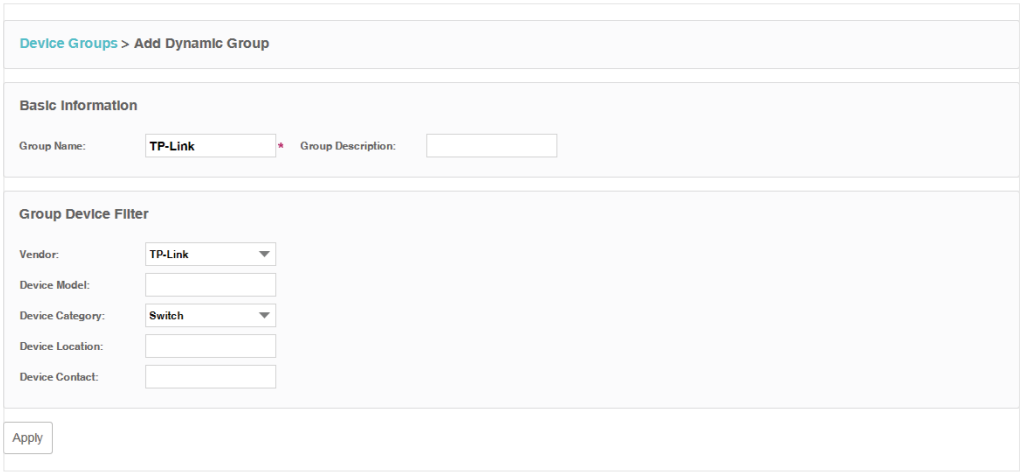
Select the devices and click **Apply** to add these devices to the group.

4. Click **Apply** to save the static group.

3.4.3 Add Devices to Dynamic Group

Go to **Resource > Device Management > Device Groups**. Click **Add Dynamic Group** to add the devices that match the specified criteria to a dynamic group.

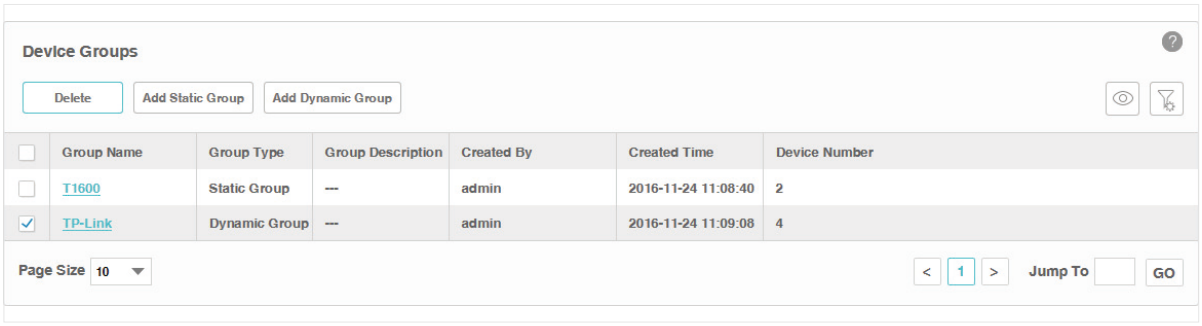
Figure 3-28 Add devices to a dynamic group



3.4.4 Delete Groups

Go to **Resource > Device Management > Device Groups**. Click **Delete** to remove the selected device groups from the group table.

Figure 3-29 Remove device groups



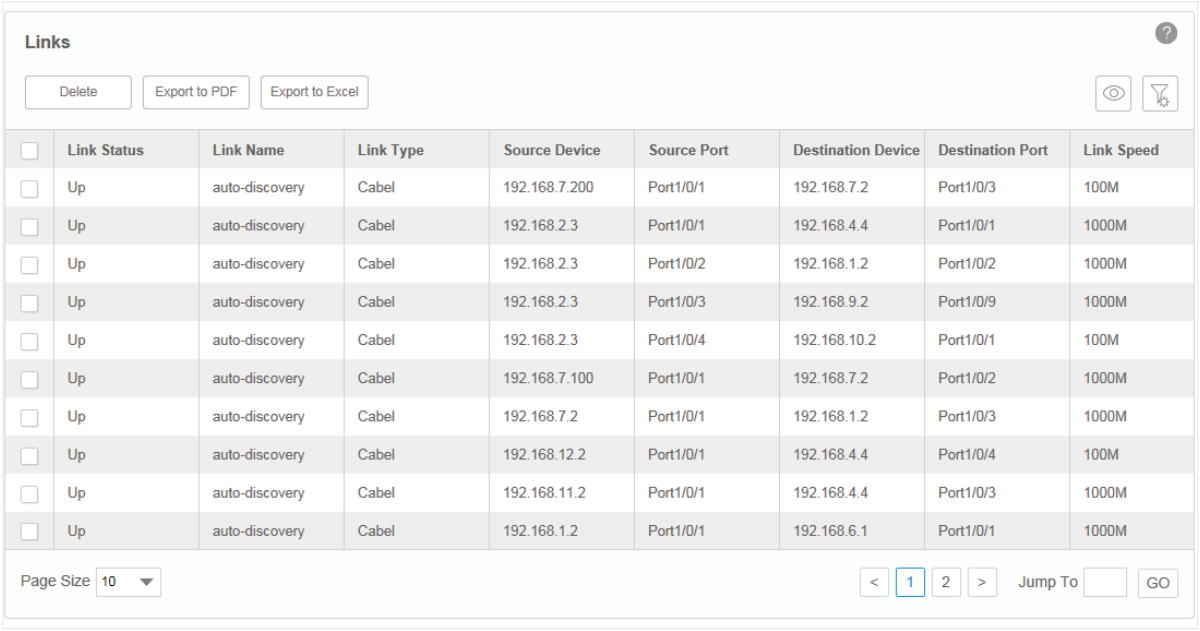
3.5 View and Manage Links on Your Network

- *View Links on Your Network*
- *Discover Links on Your Network*
- *Add a Link*

3.5.1 View Links on Your Network

Go to **Resource > Link Management > Link Table**. The links are displayed below.

Figure 3-30 View links



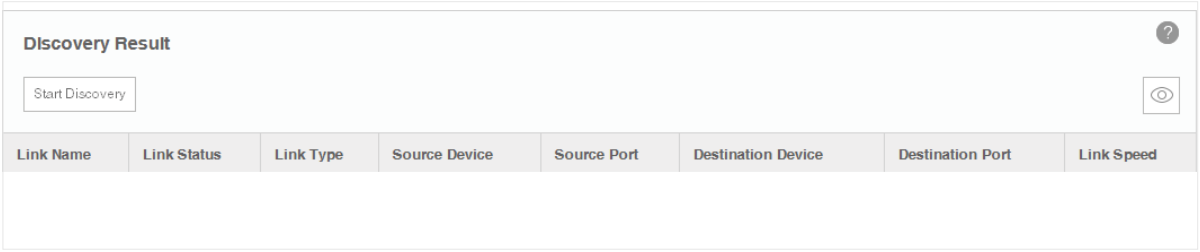
Link Status	Displays whether the link is up or down.
Link Name	Displays the link name. There are two types of link names. 'auto-discovery' means the link is established by LLDP automatically, while links with the other names are created by users manually.
Link Type	Displays the link type. Cable means it's a physical link. Link layer link means it's a link in layer 2.
Source Device	Displays the source device of the link.
Source Port	Displays the source port of the link.
Destination Device	Displays the destination device of the link.
Destination port	Displays the destination port of the link.
Link Speed	Displays the speed of the link.

3.5.2 Discover Links on Your Network

Go to **Resource > Link Management > Link Discovery**.

Click **Start Discovery** to discover all the links between the devices with LLDP enabled. For devices that do not support LLDP, you can manage links manually.

Figure 3-31 Link discovery

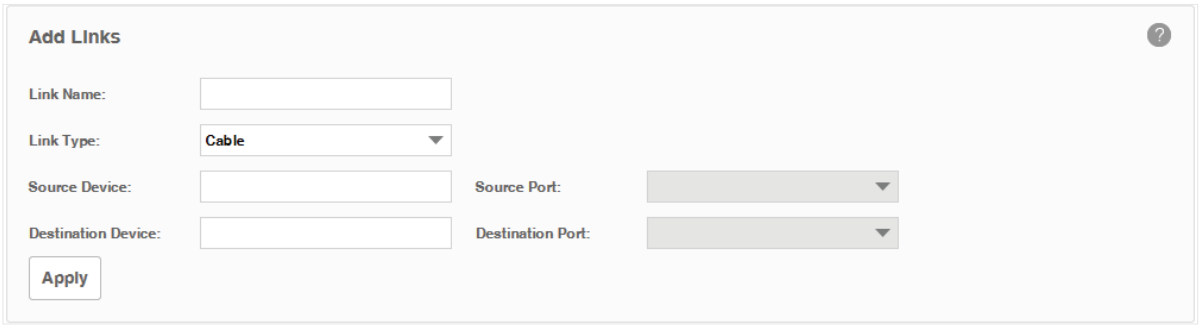


3.5.3 Add a Link

Go to **Resource > Link Management > Link Addition**.

You can add a link on this page manually. You can also draw these links manually on the map in Discovery and Manage Resources > Manage Maps and Topologies > Add a Link.

Figure 3-32 Add a link



Link Name	Enter the link's name.
Link Type	Select the link's type.
Source Device	Select source device from the device list.
Source Port	Select the port on source device as source port.
Destination Device	Select destination device from the device list.
Destination Port	Select the port on destination device as destination port.

Click **Apply** to save the configuration.

3.6 Manage Maps and Topologies

tpNMS provides a world map as the default map. The world map is the root map for any child map that you add. You can locate devices and links onto the maps manually, thus establishing visual topologies.

This section introduces the following tasks:

- *View the Maps in the Map List*
- *Add a Map*
- *Add a Device*
- *Add a Link*
- *Delete a Device, Link or Map*
- *Refresh the Topology*
- *Auto-Refresh*

Go to **Resource > Topology Management > Network Topology**. The default map displays below.

Figure 3-33 Network topology

3.6.1 View the Maps in the Map List

The map list contains the world map as the Root map by default. The map list is a hierarchical directory structure.

3.6.2 Add a Map

Click the icon  to upload a new child map to your selected map.

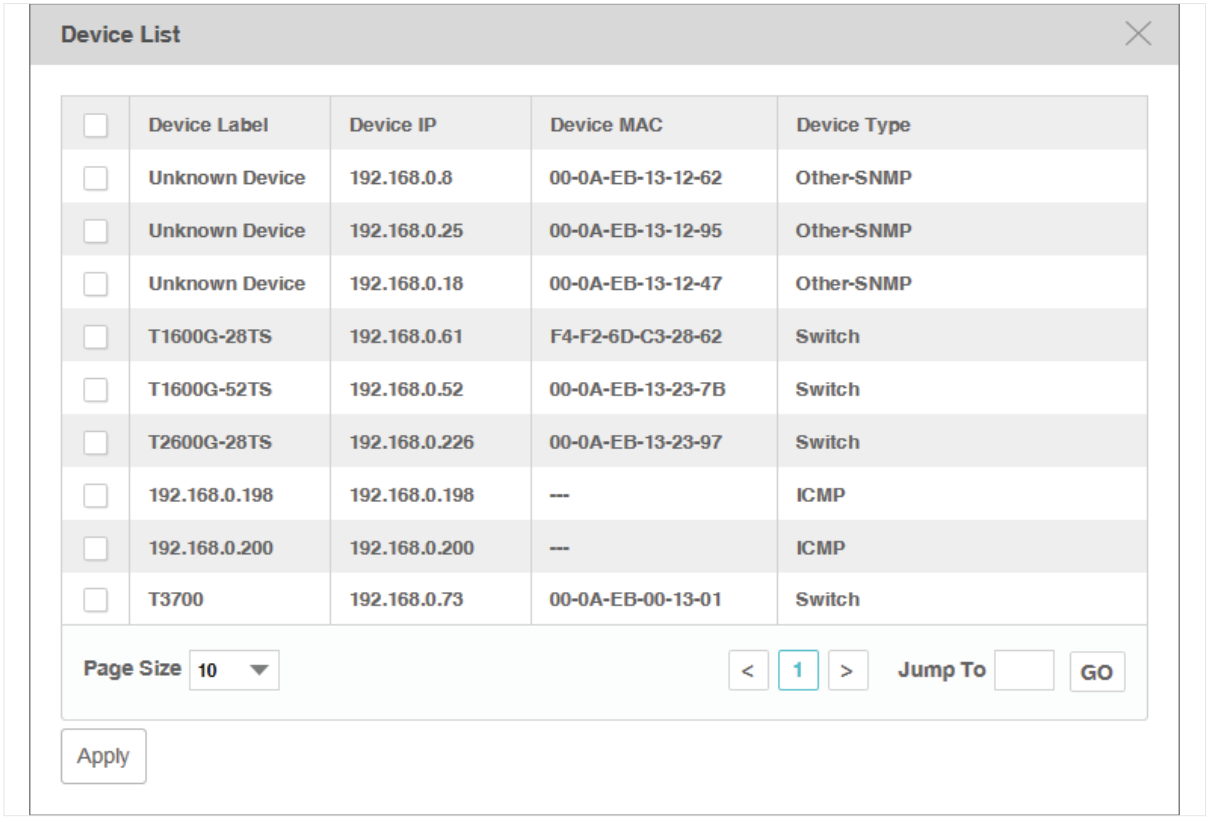
Figure 3-34 Add a map

Enter the map name and upload a map with **.png** or **.jpg** extension from your computer.

3.6.3 Add a Device

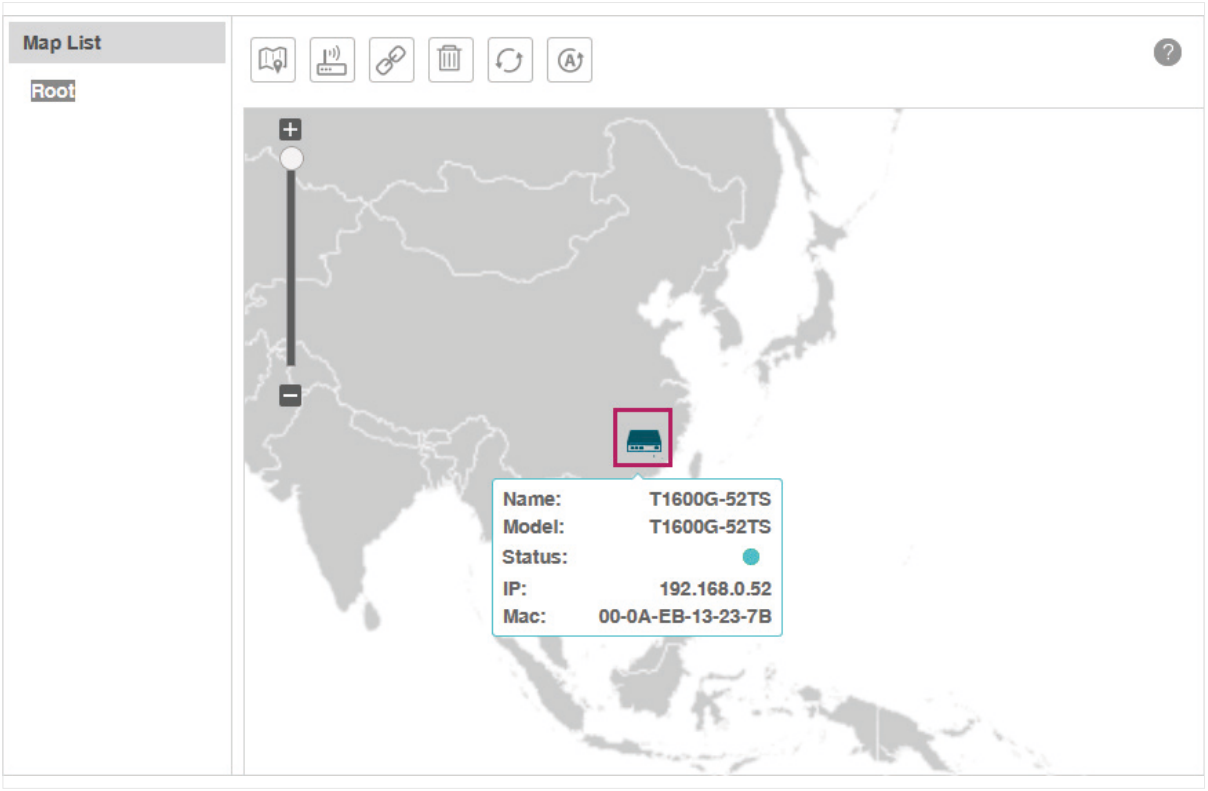
Click the icon  to add a device to the current map.

Figure 3-35 Add a device



Select the target device and click **Apply**. The device will appear on the map.

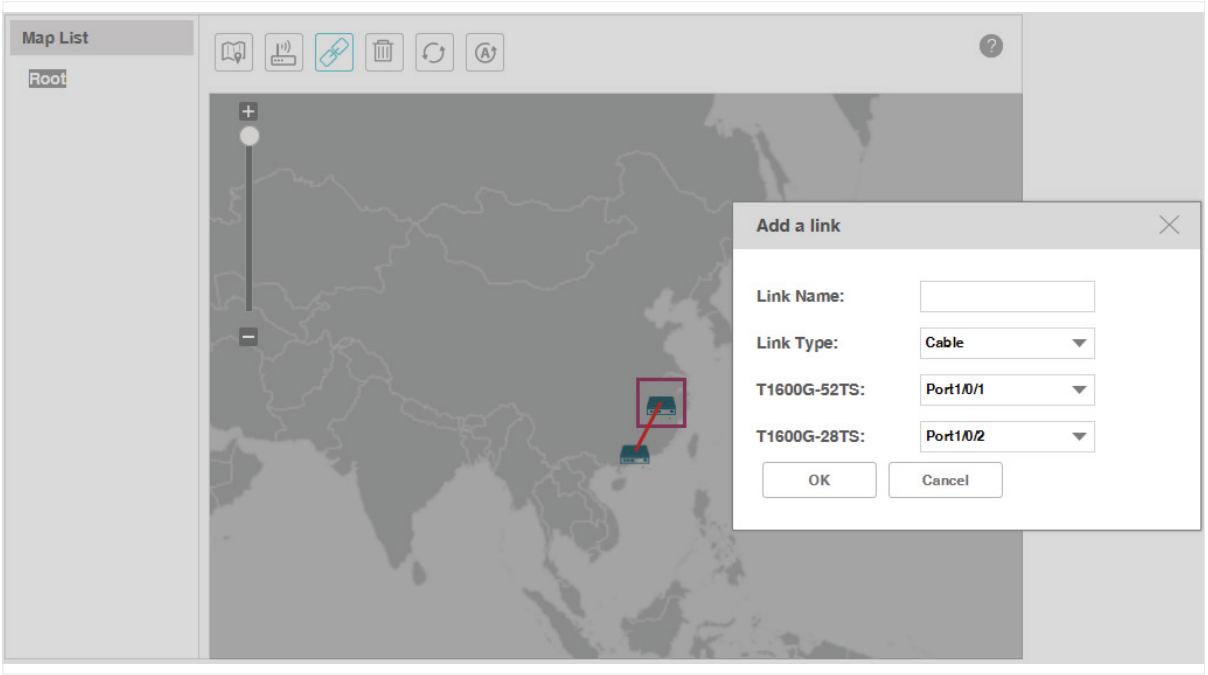
Figure 3-36 Device on the map



3.6.4 Add a Link

Click the icon  to add a new link between devices.

Figure 3-37 Add a link



Draw a line between the two target devices and complete the link information, which includes link name, link type and the connecting interfaces on both ends.

3.6.5 Delete a Device, Link or Map

Select a device, link or map and click  to remove your selected object.

3.6.6 Refresh the Topology

Click  to refresh the current topology manually.

3.6.7 Auto-Refresh

Click  and the topology will refresh every 2 minutes automatically.

Click this icon again to cancel the auto refresh.

4 Monitor Devices and Network

You can view summary and detailed information of the devices, interfaces and the network statistics.

This chapter includes the following sections:

Please note that only T-series models' CPU and Memory utilization can be monitored in tpNMS. For other models' utilization status, you can log in their web or CLI interface to view.

4.1 Monitor the Top 10 Devices

You can monitor today's top 10 devices by average CPU and by average memory. Go to **Monitor > TopN > TopN Devices**.

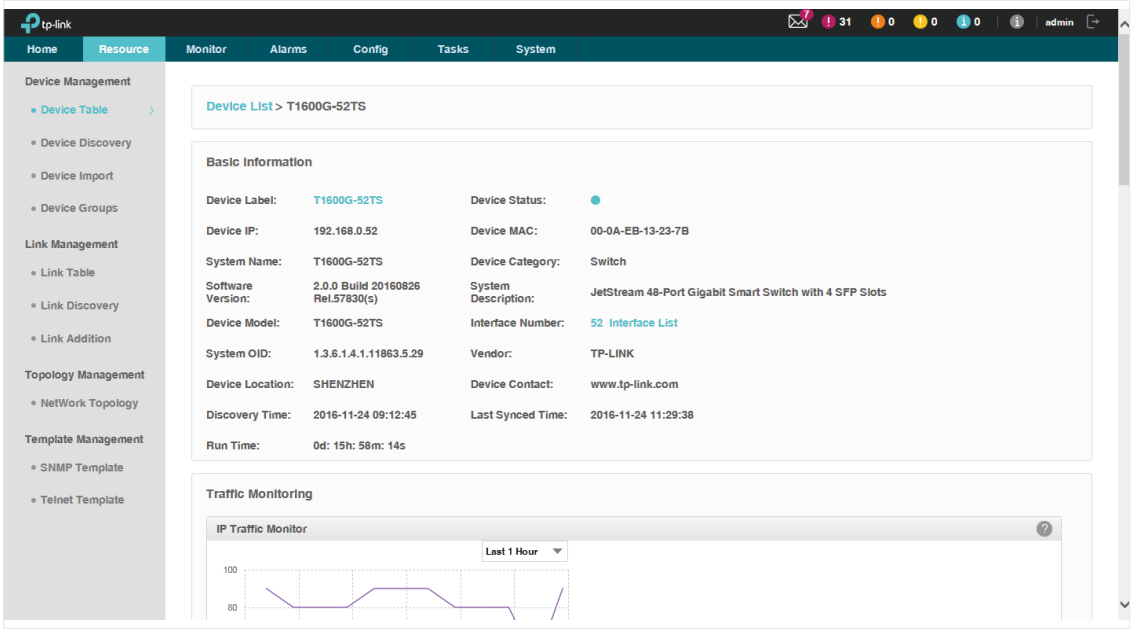
· Top 10 Devices by Average CPU (Today)

Figure 4-1 Top 10 devices by average CPU

Device Name	Displays the name of the device.
Device Type	Displays the type of the device.
CPU Utilization (%)	Displays the CPU utilization of the device.

Click the device name to view its detailed information.

Figure 4-2 Device information



· Top 10 Devices by Average Memory (Today)

Figure 4-3 Top 10 devices by average memory

Device Name	Displays the name of the device.
Device type	Displays the type of the device.
Memory Utilization (%)	Displays the memory utilization of the device.

Click the device name to view its detailed information.

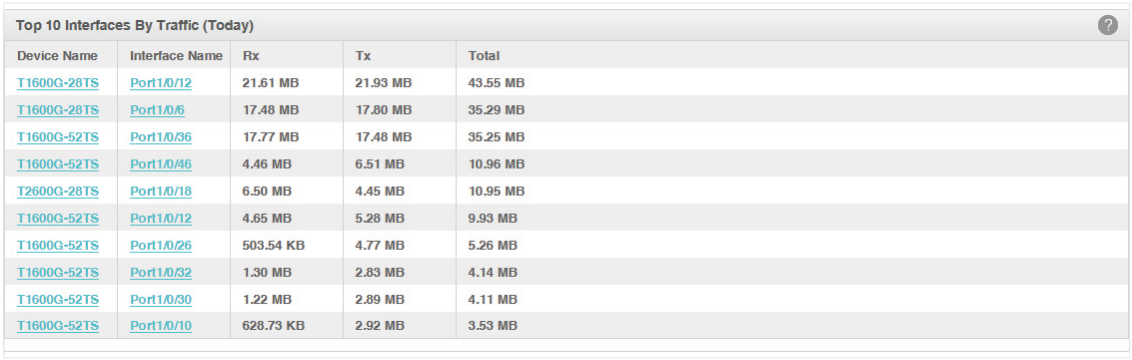
4.2 Monitor the Top 10 Interfaces

You can monitor today's top 10 interfaces by traffic, traffic rate, bandwidth utilization, error packets and discard packets.

Go to **Monitor > TopN > TopN Interfaces**.

· Top 10 Interfaces by Traffic (Today)

Figure 4-4 Top 10 interfaces by traffic

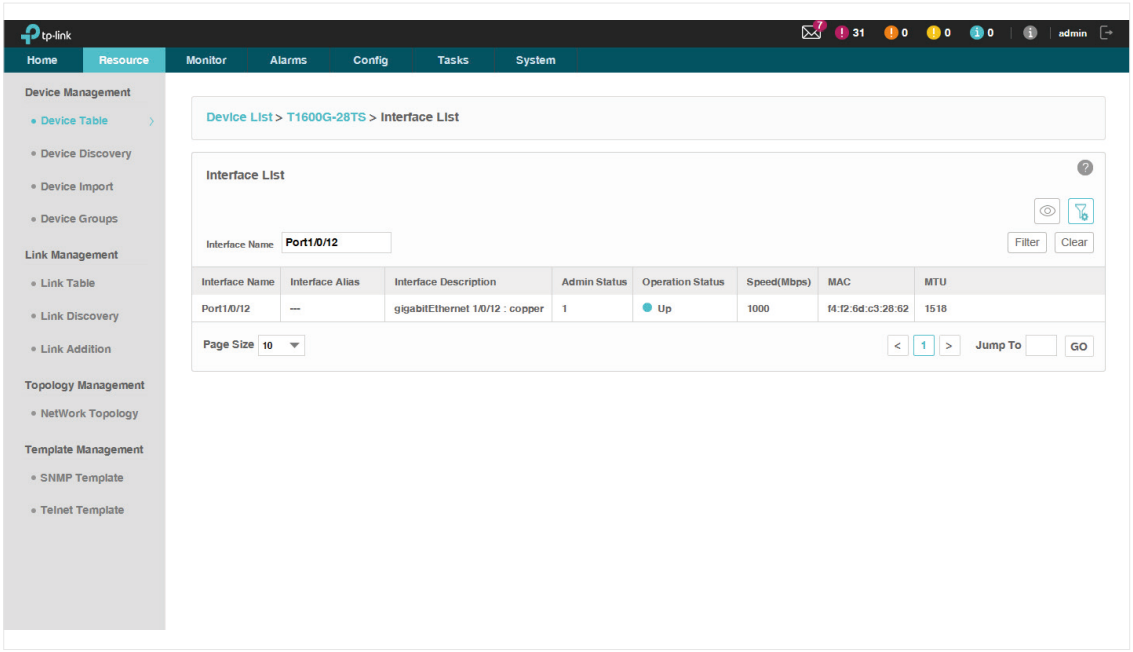


Device Name	The name of the device.
Interface Name	The name of the interface.
Rx	The received traffic on this interface.
Tx	The sent traffic on this interface.

Total	The total traffic forwarded on this interface.

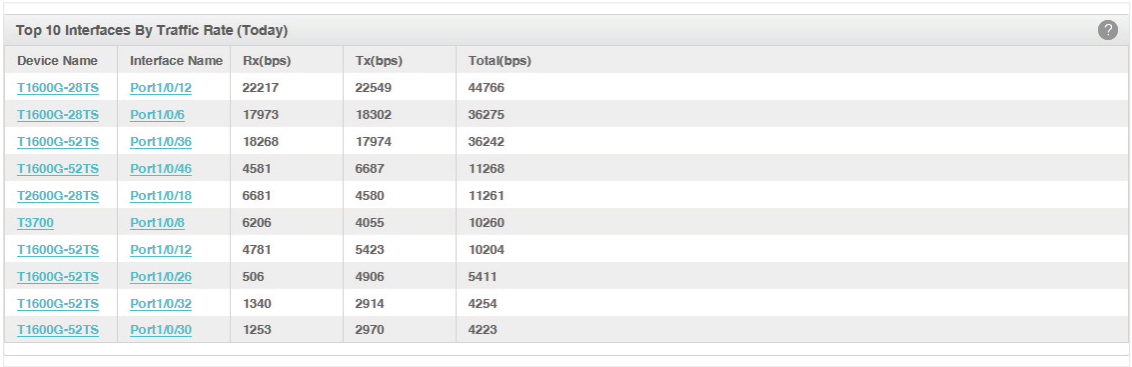
Click the device name to view detailed information about the device. Click the interface name to view detailed information about the interface.

Figure 4-5 Interface information



· Top 10 Devices by Traffic Rate (Today)

Figure 4-6 Top 10 interfaces by traffic rate



Top 10 Interfaces By Traffic Rate (Today)

Device Name	Interface Name	Rx(bps)	Tx(bps)	Total(bps)
T1600G-28TS	Port1/0/12	22217	22549	44766
T1600G-28TS	Port1/0/6	17973	18302	36275
T1600G-52TS	Port1/0/36	18268	17974	36242
T1600G-52TS	Port1/0/46	4581	6687	11268
T2600G-28TS	Port1/0/18	6681	4580	11261
T3700	Port1/0/8	6206	4055	10260
T1600G-52TS	Port1/0/12	4781	5423	10204
T1600G-52TS	Port1/0/26	506	4906	5411
T1600G-52TS	Port1/0/32	1340	2914	4254
T1600G-52TS	Port1/0/30	1253	2970	4223

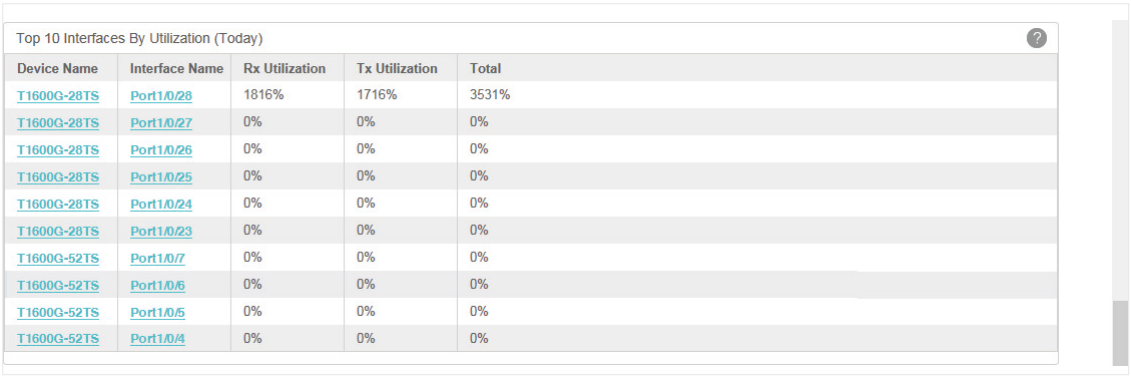
Device Name	The name of the device.
Interface Name	The name of the interface.
Rx (bps)	The received traffic rate on this interface.
Tx (bps)	The sent traffic rate on this interface.

Total (bps)	The total traffic rate forwarded on this interface.

Click the device name to view detailed information about the device. Click the interface name to view detailed information about the interface.

· Top 10 Interfaces by Utilization (Today)

Figure 4-7 Top 10 interfaces by utilization


Top 10 Interfaces By Utilization (Today)

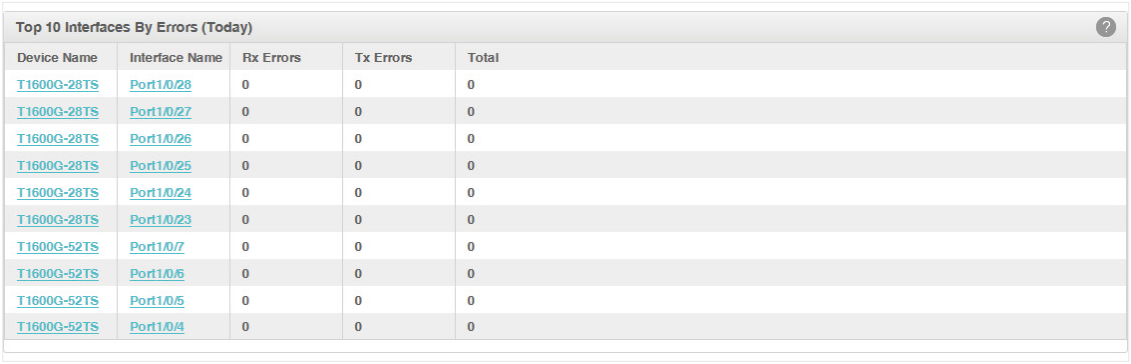
Device Name	Interface Name	Rx Utilization	Tx Utilization	Total
T1600G-28TS	Port1/0/28	1816%	1716%	3531%
T1600G-28TS	Port1/0/27	0%	0%	0%
T1600G-28TS	Port1/0/26	0%	0%	0%
T1600G-28TS	Port1/0/25	0%	0%	0%
T1600G-28TS	Port1/0/24	0%	0%	0%
T1600G-28TS	Port1/0/23	0%	0%	0%
T1600G-52TS	Port1/0/7	0%	0%	0%
T1600G-52TS	Port1/0/6	0%	0%	0%
T1600G-52TS	Port1/0/5	0%	0%	0%
T1600G-52TS	Port1/0/4	0%	0%	0%

Device Name	The name of the device.
Interface Name	The name of the interface.
Rx Utilization	The interface's utilization on receiving bandwidth.
Tx Utilization	The interface's utilization on sending bandwidth.
Total	The total utilization of the interface.

Click the device name to view detailed information about the device. Click the interface name to view detailed information about the interface.

· Top 10 Interfaces by Errors (Today)

Figure 4-8 Top 10 interfaces by errors


Top 10 Interfaces By Errors (Today)

Device Name	Interface Name	Rx Errors	Tx Errors	Total
T1600G-28TS	Port1/0/28	0	0	0
T1600G-28TS	Port1/0/27	0	0	0
T1600G-28TS	Port1/0/26	0	0	0
T1600G-28TS	Port1/0/25	0	0	0
T1600G-28TS	Port1/0/24	0	0	0
T1600G-28TS	Port1/0/23	0	0	0
T1600G-52TS	Port1/0/7	0	0	0
T1600G-52TS	Port1/0/6	0	0	0
T1600G-52TS	Port1/0/5	0	0	0
T1600G-52TS	Port1/0/4	0	0	0

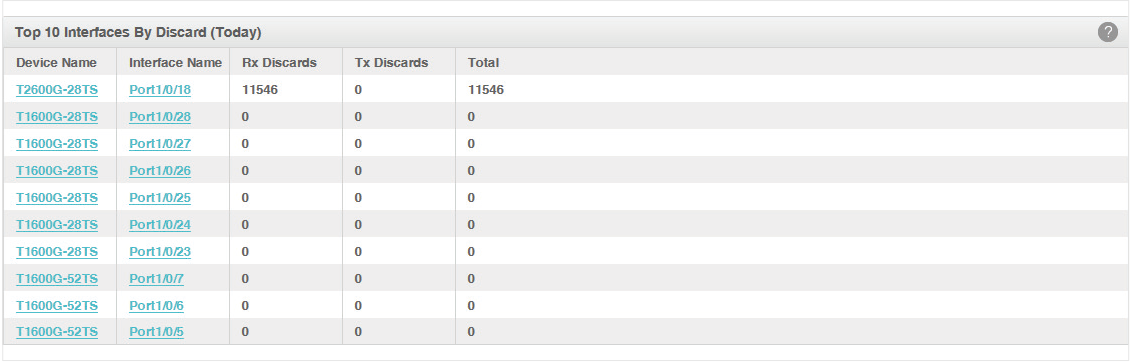
Device Name	The name of the device.
Interface Name	The name of the interface.

Rx Errors	The error packets received on the interface.
Tx Errors	The error packets sent on the interface.
Total	The total error packets forwarded on the interface.

Click the device name to view detailed information about the device. Click the interface name to view detailed information about the interface.

· Top 10 Devices by Discard (Today)

Figure 4-9 Top 10 interfaces by discard



Top 10 Interfaces By Discard (Today)

Device Name	Interface Name	Rx Discards	Tx Discards	Total
T2600G-28TS	Port1/0/18	11546	0	11546
T1600G-28TS	Port1/0/28	0	0	0
T1600G-28TS	Port1/0/27	0	0	0
T1600G-28TS	Port1/0/26	0	0	0
T1600G-28TS	Port1/0/25	0	0	0
T1600G-28TS	Port1/0/24	0	0	0
T1600G-28TS	Port1/0/23	0	0	0
T1600G-52TS	Port1/0/7	0	0	0
T1600G-52TS	Port1/0/6	0	0	0
T1600G-52TS	Port1/0/5	0	0	0

Device Name	The name of the device.
Interface Name	The name of the interface.
Rx Discards	The discarded packets in the interface's received packets.
Tx Discards	The discarded packets in the interface's sent packets.
Total	The total discarded packets on the interface.

Click the device name to view detailed information about the device. Click the interface name to view detailed information about the interface.

4.3 Specify the Device Monitor

tpNMS provides monitors for the following device metrics:

· IP Traffic

· ICMP Traffic

· TCP Traffic

· UDP Traffic

· SNMP Traffic

· Interface Traffic

· CPU

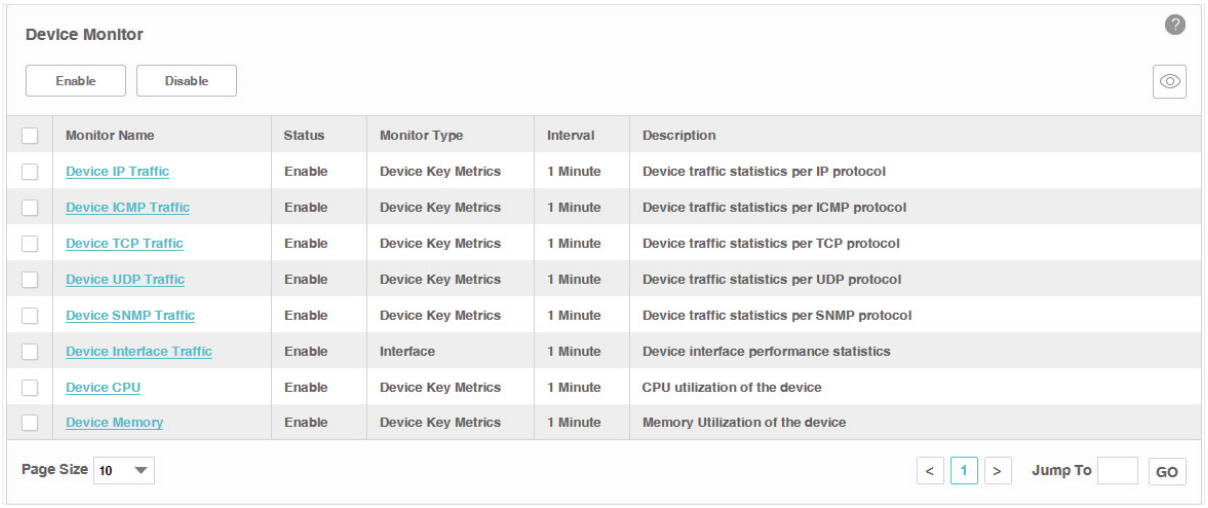
· Memory

By default all the monitors are enabled. You can enable/disable and specify these monitors on the page **Monitor > Monitor Management > Device Monitor**.

For information about how to configure alarms basing on these monitors, please refer to *View and Manage Alarm Configurations*.

Go to **Monitor > Monitor Management > Device Monitor**.

Figure 4-10 Monitor devices



Monitor Name	The name of the monitor.
Status	The status of the monitor.
Monitor Type	The monitor type.
Interval	The interval of the monitor obtains the parameters from the target devices.
Description	The description for this monitor.

Enable/Disable the Monitors

Click **Enable/Disable** to enable/disable the selected monitors.

Specify the information of the Monitors

Click the monitor name to modify its detailed information.

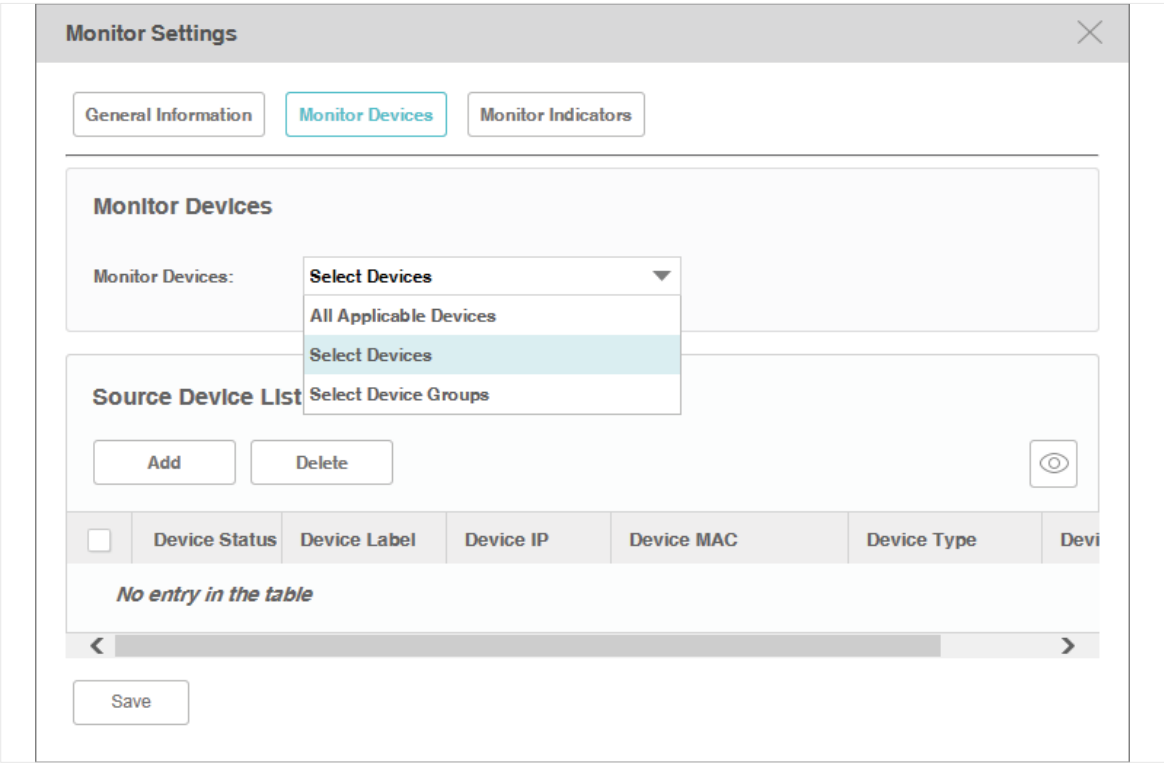
1. Click **General Information** to edit the monitor's basic information.

Figure 4-11 General Settings

Monitor Name	The name of the monitor.
Enable	Enable or disable this monitor.
Interval	Select the interval of the monitor obtains the parameters from the target devices.
Description	Description for this monitor.

2. Click **Monitor Devices** to specify the devices or device groups that are monitored.

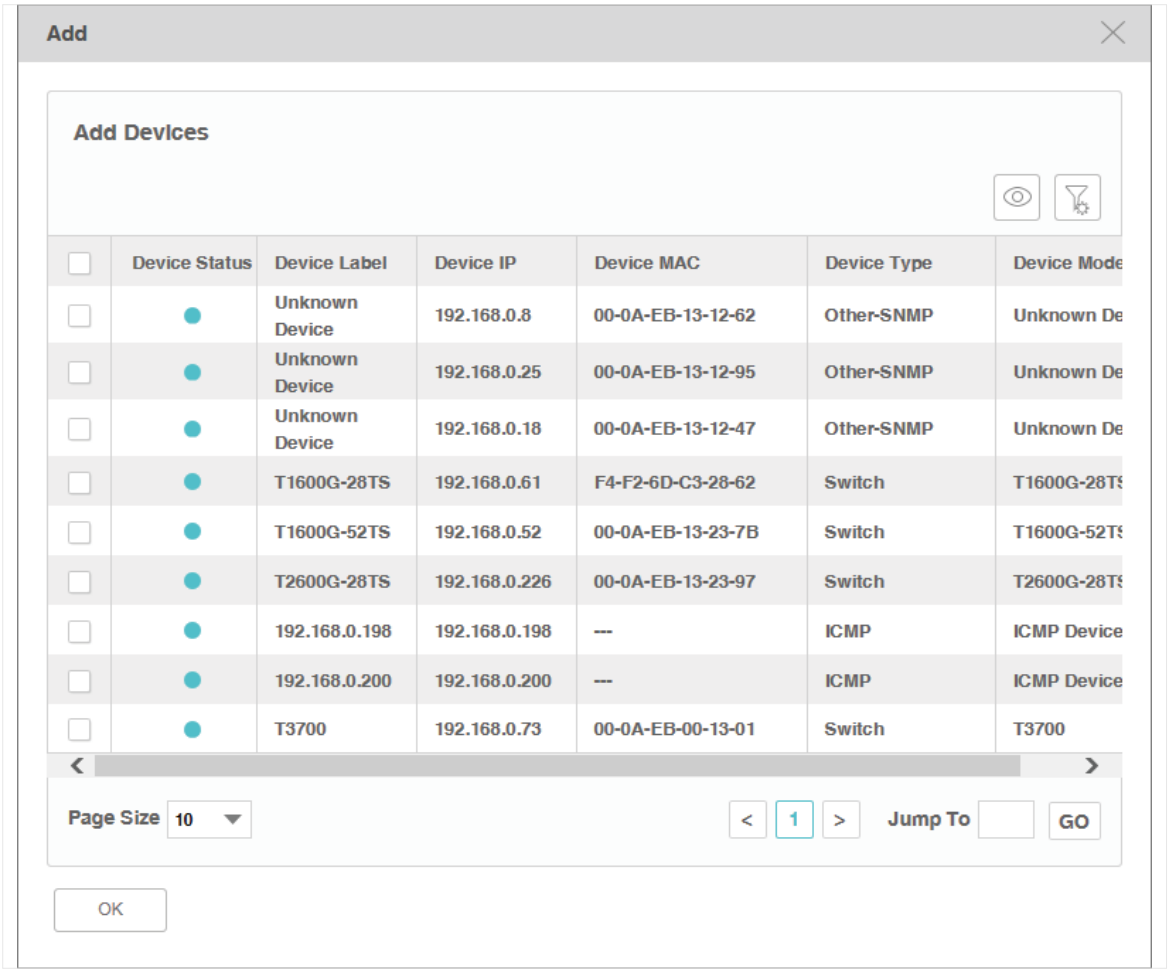
Figure 4-12 Add monitor devices



Monitor Devices	Specify the devices that are monitored. The options are All Applicable Devices, Select Devices and Select Device Groups. Use the **Add** and **Delete** button to edit the target devices or device groups, and click **Save** to save the changes.

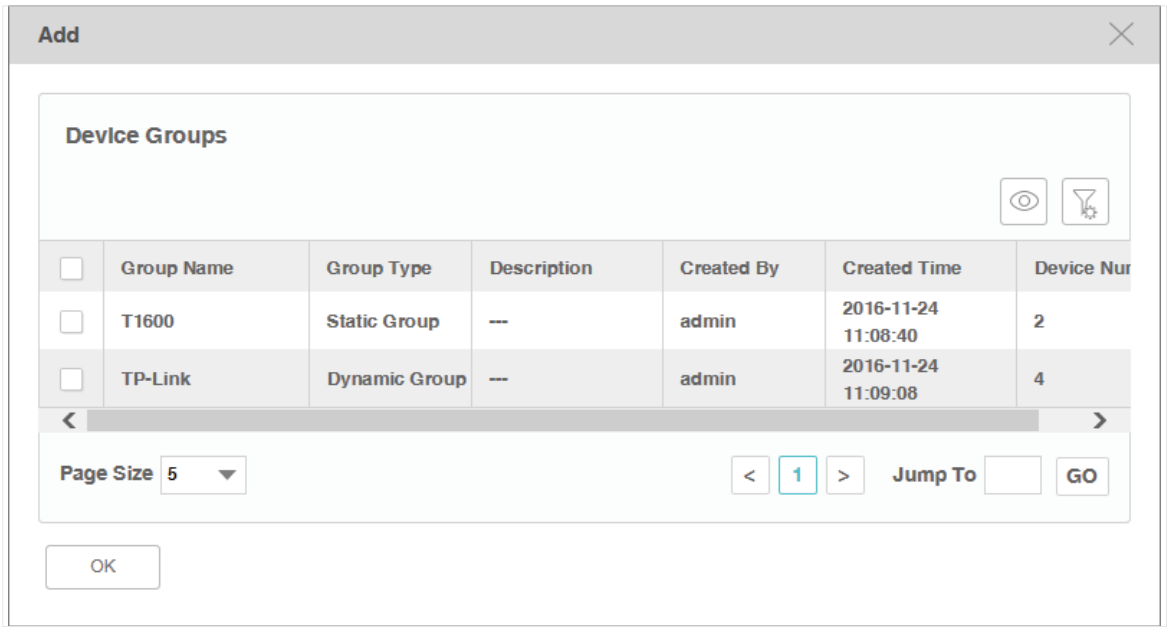
The Select Devices window displays as below.

Figure 4-13 Add devices



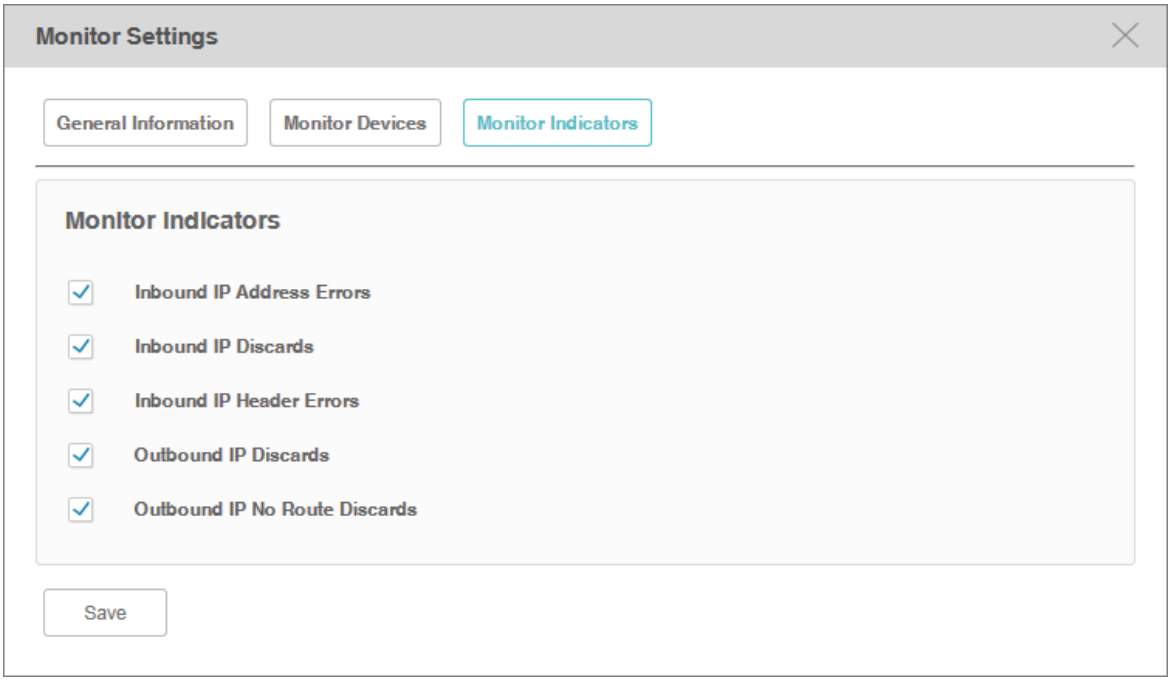
The Select Device Groups window displays as below.

Figure 4-14 Add device groups



3. Click **Monitor Indicators** to specify the parameters that are monitored by this monitor.

Figure 4-15 Add indicators



Edit the parameters that are monitored. By default all the parameters are selected. Click **Save** to save the changes.

4.4 Manage and View Dashboard

You can create and customize network information to be displayed on the tpNMS dashboard.

- *Create or Modify a Dashboard View*
- *Launch a Dashboard View*
- *Display the Dashboard View*

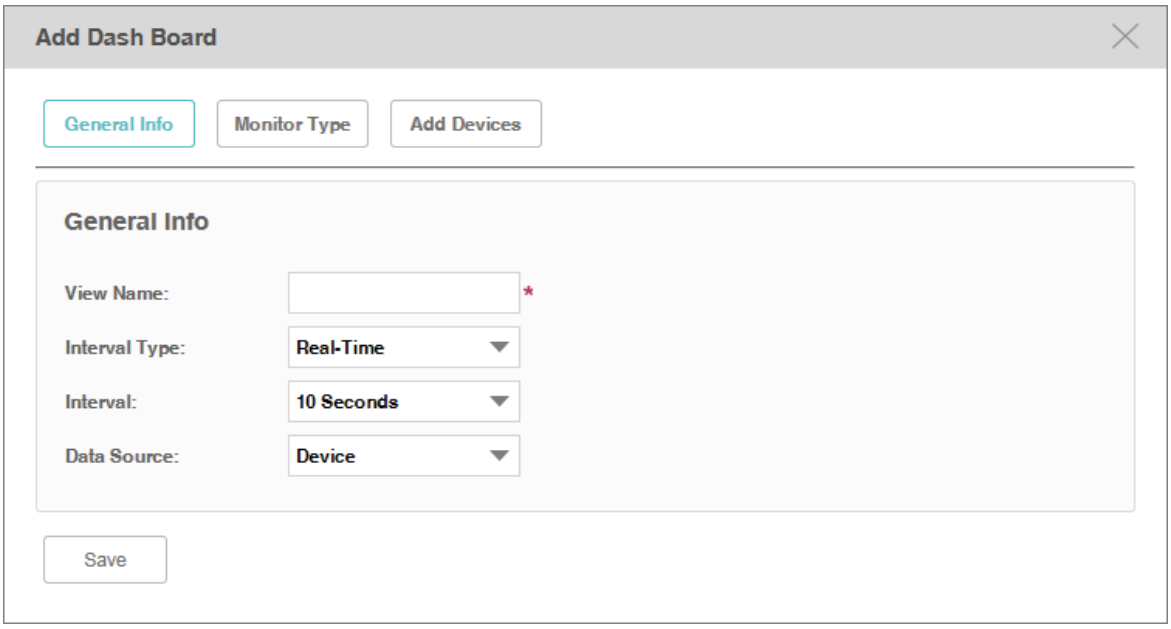
4.4.1 Create or Modify a Dashboard View

Go to **Monitor > Dash Board > Dash Board Setting**.

Figure 4-16 Dash board view

1. Click **Add** to create a new dashboard view, or click the view name in the table to edit the existed dashboard view.
2. Click **General Info** to edit the basic information of the dashboard view.

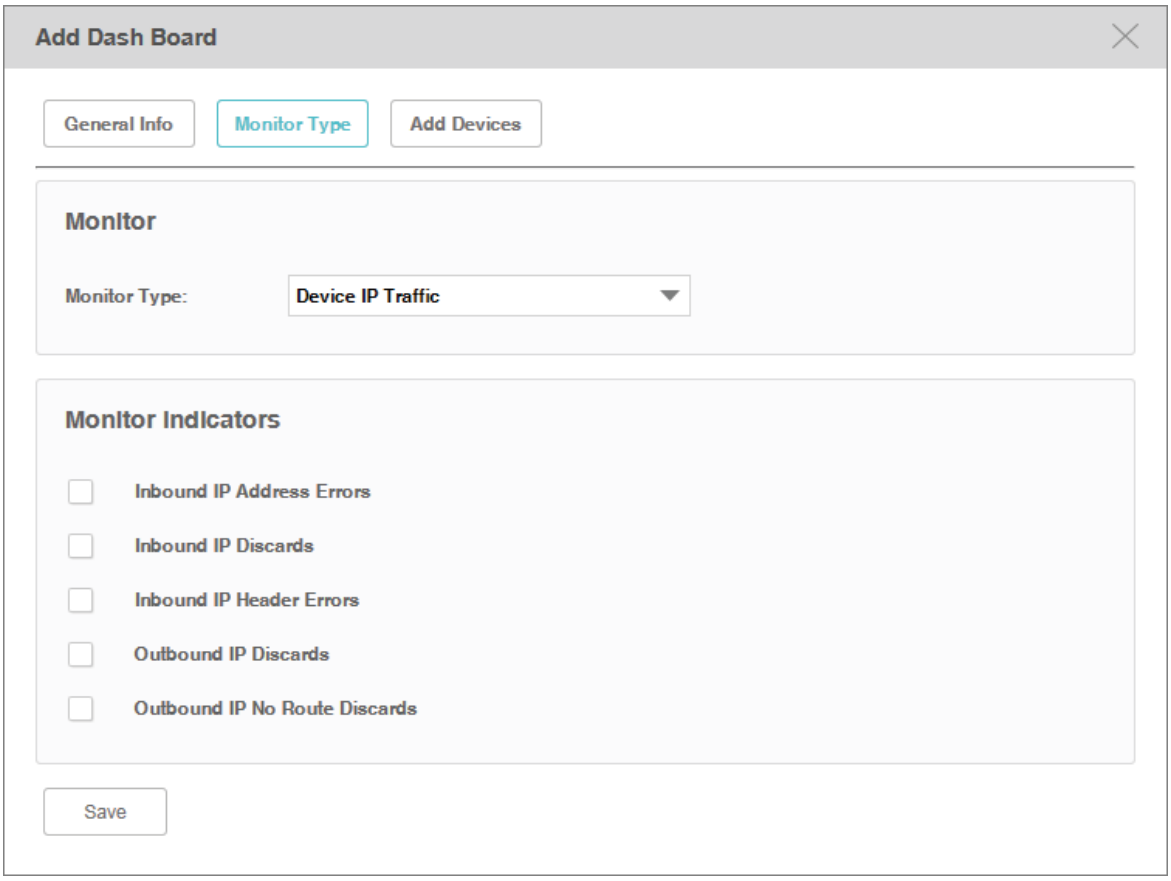
Figure 4-17 Dashboard general information



View Name	Enter or modify the name for the dashboard view.
Interval Type	Specify the time period over which you want to view the performance. • Real Time: View the performance in real time. • Last 1 Hour: View the performance over the last 1 hour. • Last 24 Hours: View the performance over the last 24 hours. • Last 7 Days: View the performance over the last 7 days. • Last 30 Days: View the performance over the last 30 days.
Interval	If you select Real Time, select the refresh frequency of the view here. The information of this dashboard refreshes in the interval you set.
Data Source	Specify the data source as **Device** or **Interface.**

3. Click **Monitor Type** to configure the monitors of the dashboard view.

Figure 4-18 Dashboard monitor type

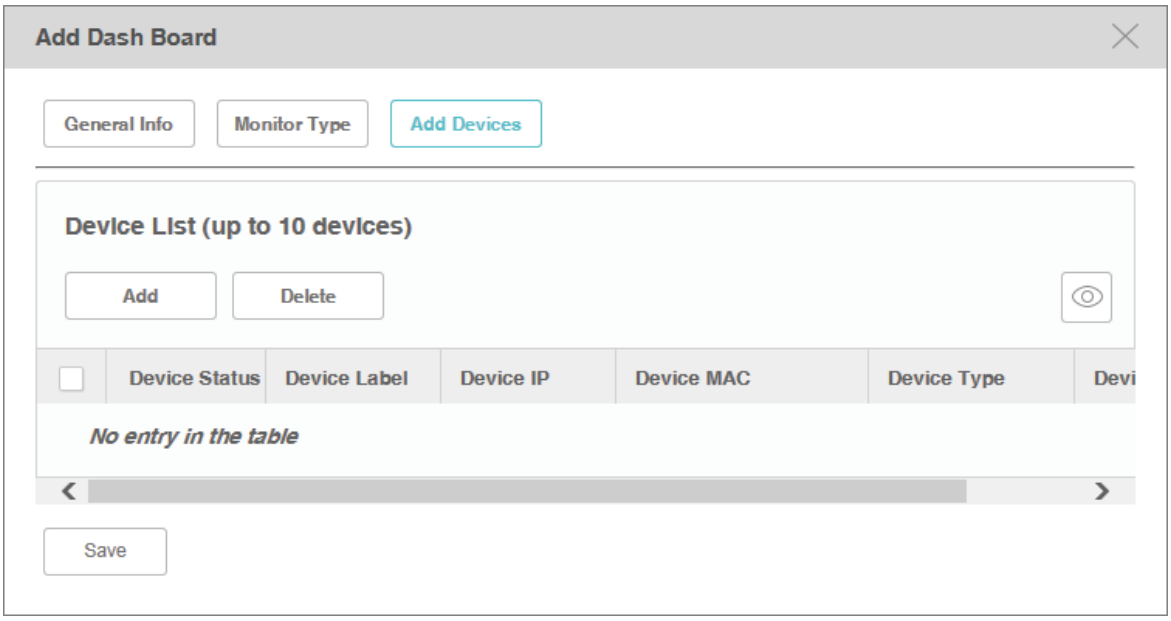


Monitor Type	Select the monitor type. There are a series of monitors for devices and a series of monitors for interfaces.
Monitor Indicators	Specify the monitor sources.

4. Click **Add Devices/Add Interfaces** to configure the target devices/interfaces of the monitor.

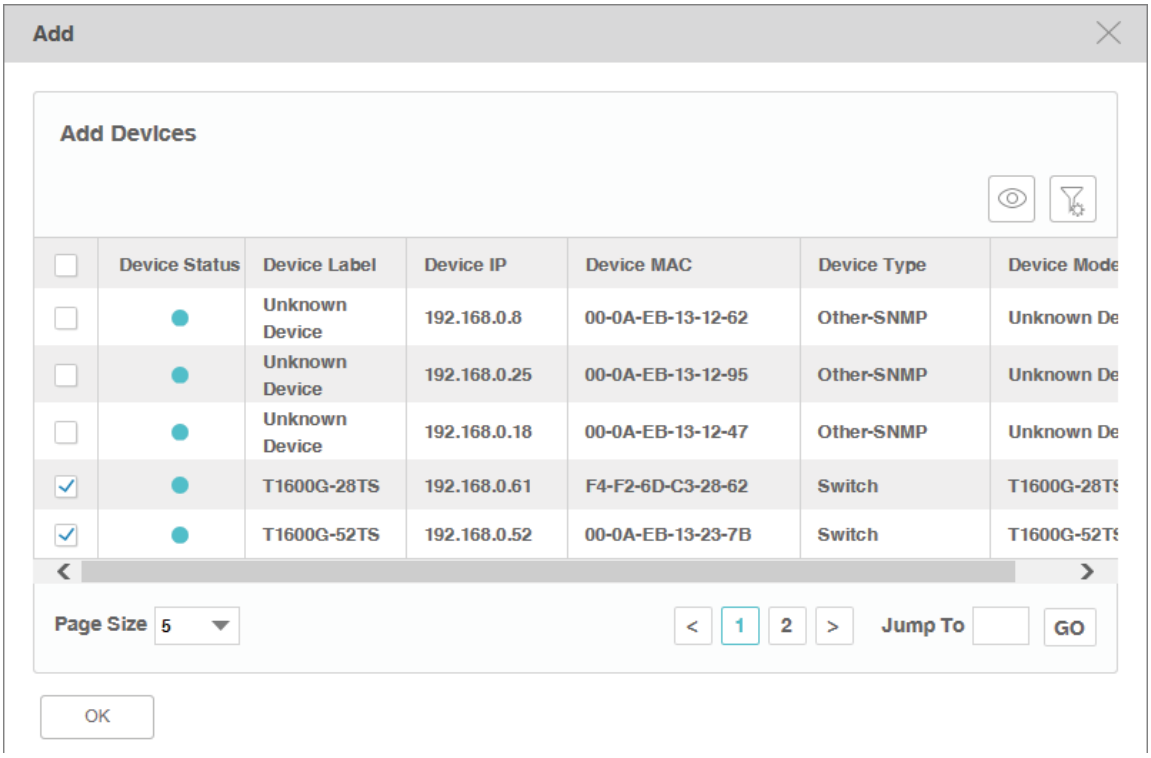
   The following screenshots use **Devices** as an example.

Figure 4-19 Dashboard target devices



Click **Add** to add devices in the device table. Click **OK** to save your selections.

Figure 4-20 Add target devices



5. Click **Apply** to save your configurations on the dashboard.

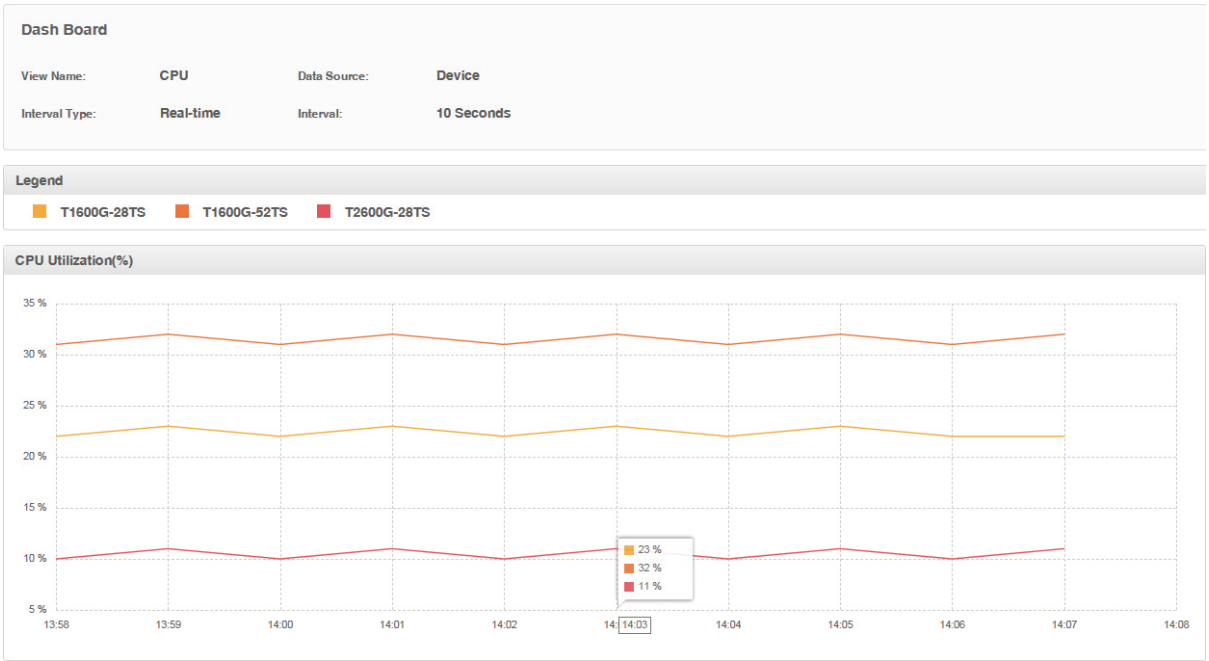
4.4.2 Launch a Dashboard View

Go to **Monitor > Dash Board > Dash Board Setting**. Select a dashboard view in the table and click **Launch**.

Figure 4-21 Launch a dashboard

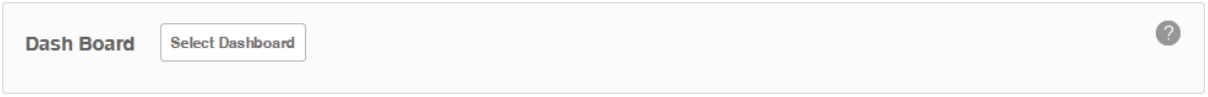
The dashboard view will be displayed in a new tab of the browser. The following tab is the dashboard monitoring the CPU utilization of several T-series switches.

Figure 4-22 Display a dashboard



4.4.3 Display the Dashboard View

Go to **Monitor > Dash Board > Dash Board View**. Click **Select Dashboard** and select one dashboard name for display.



The dashboard will be displayed on current page.

5 Manage Alarms and Traps

tpNMS can manage the traps sent from the devices.

tpNMS can define alarms basing on traps, monitor and the tpNMS system.

tpNMS can define the recipients to receive the notification emails when the specific alarms are triggered.

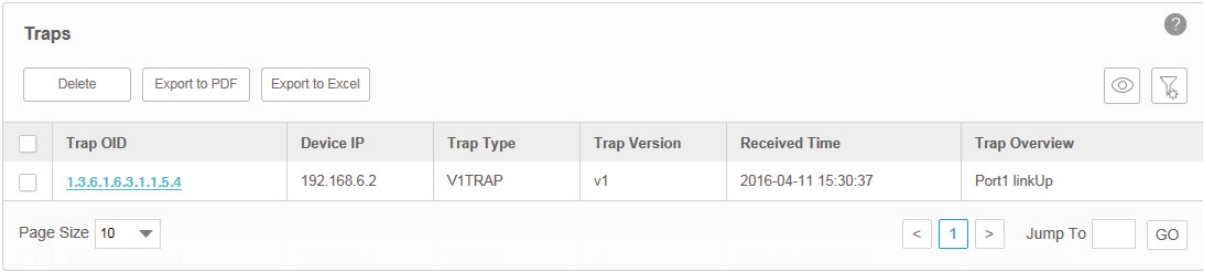
This chapter includes the following contents:

5.1 View and Manage Traps Sent from Devices

Go to **Alarms > Trap Management > Traps**.

The Trap table displays the traps sent from devices. On this screen, you can view details of the traps, remove the traps and export the traps.

Figure 5-1 Trap list



5.1.1 View the Traps

Click the trap OID to view the trap's detail information.

5.1.2 Delete the Traps

Select the traps and click **Delete** to remove them from the Trap table.

5.1.3 Export the Traps

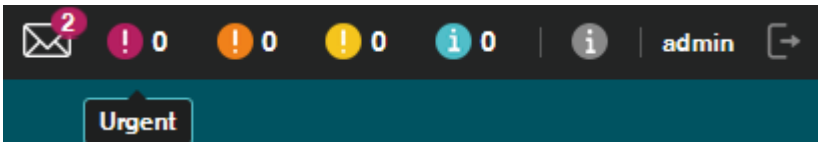
Select the traps and click **Export to PDF** or **Export to Excel** to save the traps to your computer.

5.2 View and Manage Alarm Configurations

tpNMS provides three types of alarms depending on their sources: Trap Alarms, Monitor Alarms and System Alarms. Trap alarms, system alarms and some of the monitor alarms are system built-in alarms which cannot be deleted. Users can add new monitor-type alarms.

tpNMS provides the following four severity levels for alarms. Four shortcut icons representing the four level alarms are placed in the upper-right region of the main page. The color represents the severity, while red represents the highest level

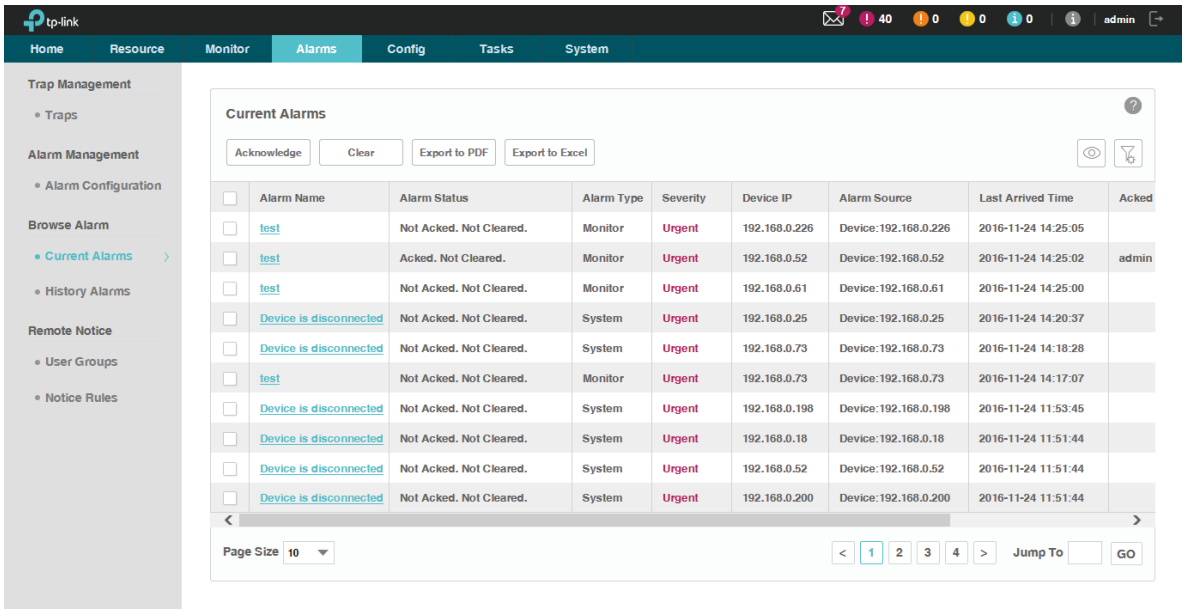
severity and blue represents the lowest severity. The numbers beside these icons represent each alarm's current quantity.



- Urgent (Red)
- Serious (Orange)
- Normal (Yellow)
- Hint (Blue)

Click on the alarm icon to view the alarm's detail information.

Figure 5-2 Urgent alarm details



The following sections describe the alarm-related tasks:

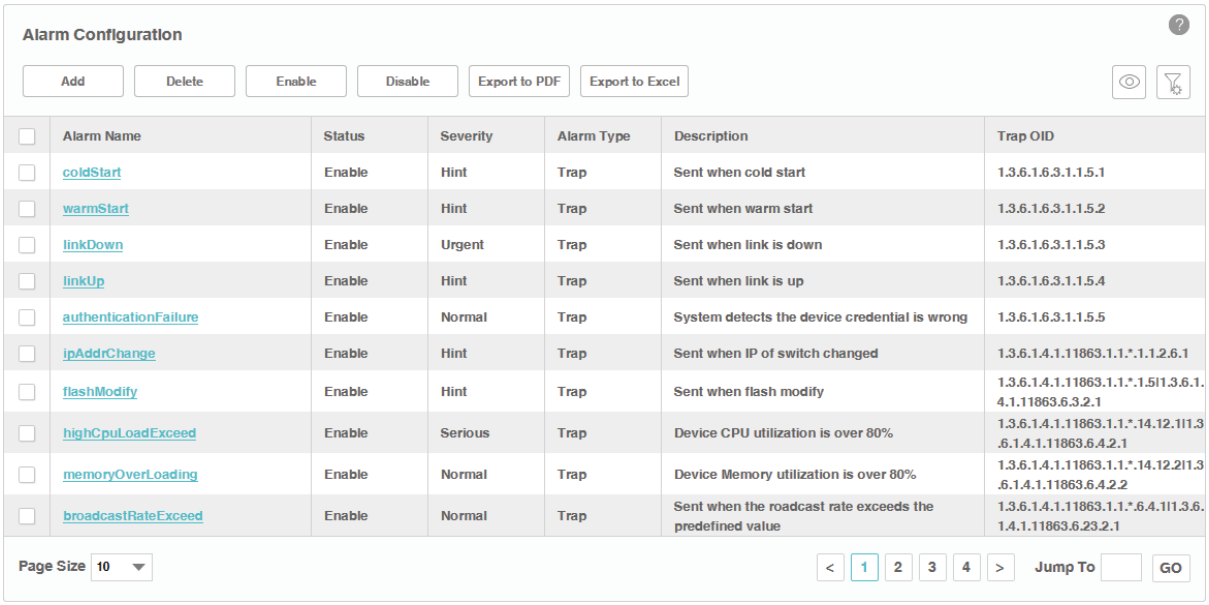
- *View and Manage Current Alarm Configurations*
- *Add a New Alarm Configuration*
- *Modify Current Alarm Configurations*

5.2.1 View and Manage Current Alarm Configurations

Go to **Alarms > Alarm Management > Alarm Configuration**.

You can view, enable, disable, delete and export alarm configurations on this page.

Figure 5-3 Alarm configuration list



View the alarms

To add or delete columns displayed in the alarm list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

To filter the alarms in the list, click the  . Enter the filter conditions and click **Filter**.

Alarm Name	The name of the alarm. Click it to view the alarm's detailed configurations.
Status	The status displays whether this alarm is valid.
Severity	Four levels of severity: Urgent, Serious, Normal and Hint.
Alarm Type	Three types of alarms: Trap, Monitor and System.
Description	Displays the trigger conditions of the alarm.
Trap OID	Displays the trap OID if this is a trap-type alarm.

Click the alarm name to view and edit the alarm's configuration.

Enable/Disable the alarms

Select alarms and click the **Enable/Disable** button to enable/disable the corresponding alarm configurations.

Delete the alarms

Click the **Delete** button to remove the selected alarm configurations. The system built-in alarms cannot be deleted.

Export the alarms

Select alarms and click the **Export to PDF**/**Export to Excel** button to export the corresponding alarm configurations to your computer.

5.2.2 Add a New Alarm Configuration

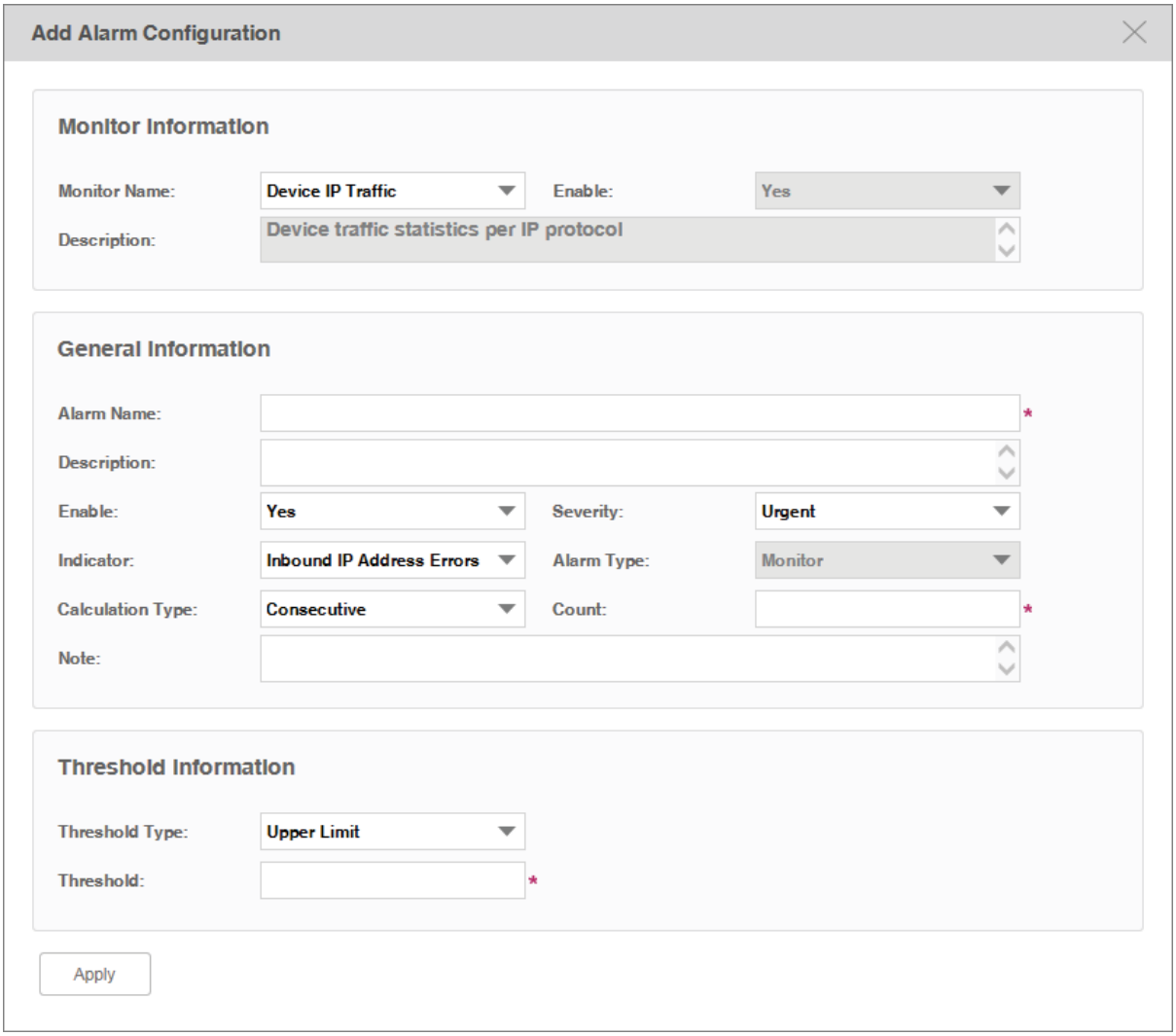
Go to **Alarms > Alarm Management > Alarm Configuration**.

You can define new alarms for the monitors. The monitors can be configured on the following page: **Monitor > Monitor Management > Device Monitor**.

The alarm you add is based on an existing monitor and includes a threshold.

Click **Add** to add a monitor-type alarm.

Figure 5-4 Add an alarm configuration



Monitor Information

Monitor Name	Select a monitor.
Enable	Displays whether this monitor is valid.
Description	Displays the detailed information of this monitor.

General Information

Alarm Name	Enter a name for the alarm.
Description	Enter a description for the alarm.
Enable	Select whether to make this alarm configuration effective.
Severity	Select the alarm's severity. tpNMS supports four levels of severity: Urgent, Serious, Normal and Hint.
Indicator	Select one indicator in the monitor you chose.

Alarm Type	You can only create monitor-type alarms.
Calculate Type	Select a consecutive or average calculation type.
Count	Select a number of times that a particular event must occur before the threshold is met.
Note	Enter a note for this alarm.

Threshold Information

Threshold Type	Select an upper or lower threshold.
Threshold	Enter. If this threshold is exceeded, the alarm will be triggered.

Click **Apply** to save your alarm configurations.

5.2.3 Modify Current Alarm Configurations

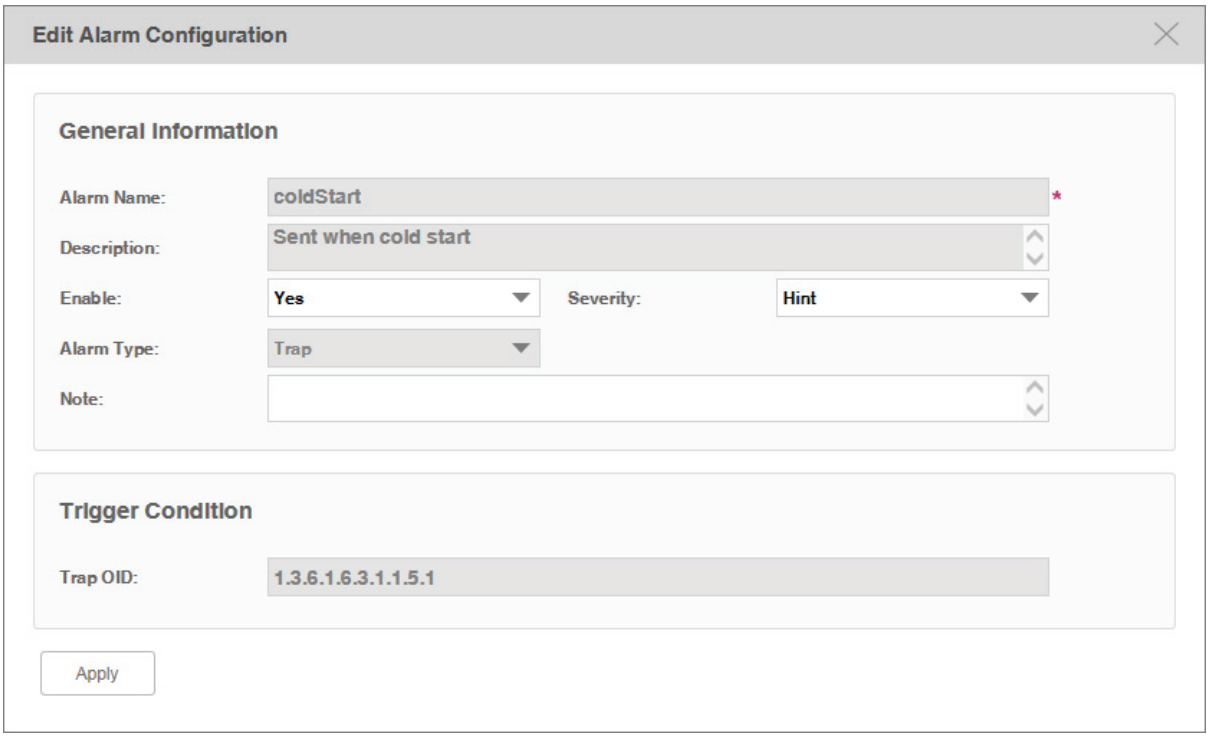
Go to **Alarms > Alarm Management > Alarm Configuration**.

You can modify the current alarm configurations on this page.

Modify a trap-type alarm

Click the trap-type alarm name to modify this alarm.

Figure 5-5 Modify a trap-type alarm configuration

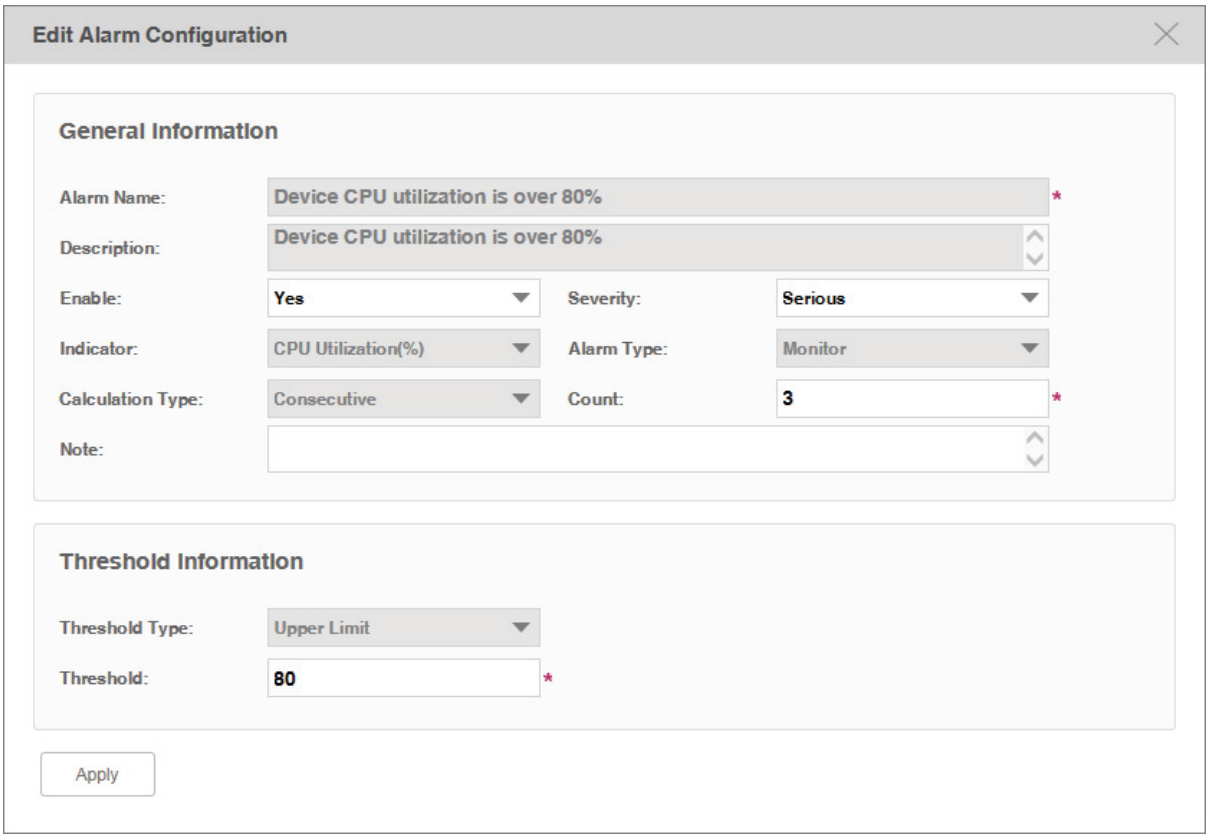


Enable	Enable or disable this alarm configuration.
Severity	Modify the alarm's severity. tpNMS supports four levels of severity: Urgent, Serious, Normal and Hint.
Note	Add a note to this alarm.

Modify a monitor-type alarm

Click the monitor-type alarm name to modify this alarm.

Figure 5-6 Modify a monitor-type alarm configuration

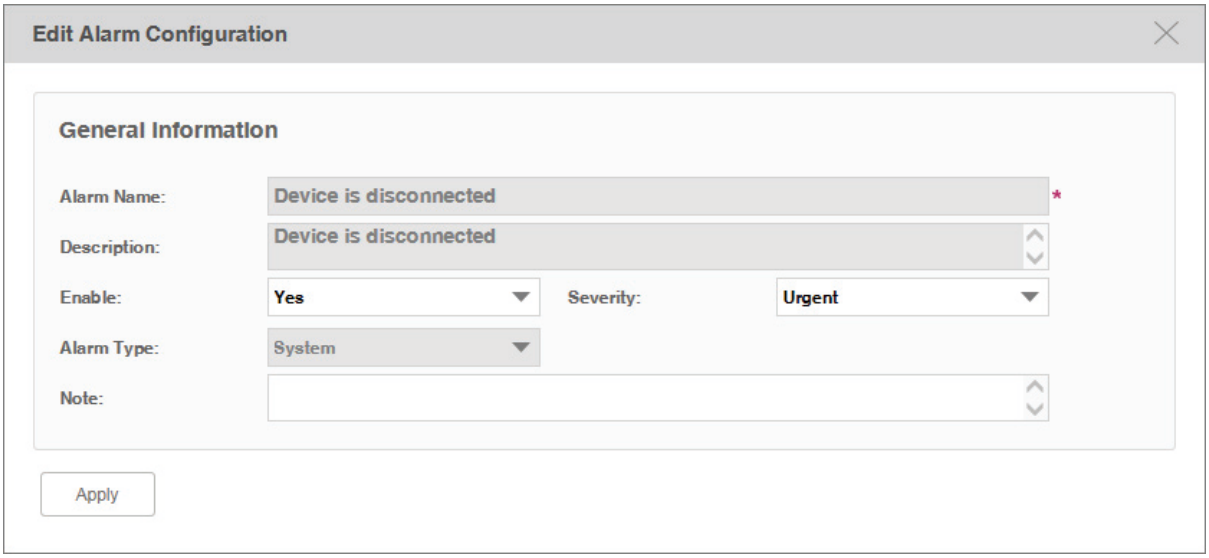


Enable	Enable or disable this alarm configuration.
Severity	Modify the alarm's severity. tpNMS supports four levels of severity: Urgent, Serious, Normal and Hint.
Count	Specify the number of times that a particular event must occur before the threshold is met.
Note	Add a note to this alarm.
Threshold	Modify the threshold. If this threshold is exceeded, the alarm will be triggered.

Modify a system-type alarm

Click the system-type alarm name to modify this alarm.

Figure 5-7 Modify a system-type alarm configuration



Enable	Enable or disable this alarm configuration.
Severity	Modify the alarm's severity. tpNMS supports four levels of severity: Urgent, Serious, Normal and Hint.
Note	Add a note to this alarm.

5.3 View and Manage Alarms

You can view and manage the current alarms and history alarms.

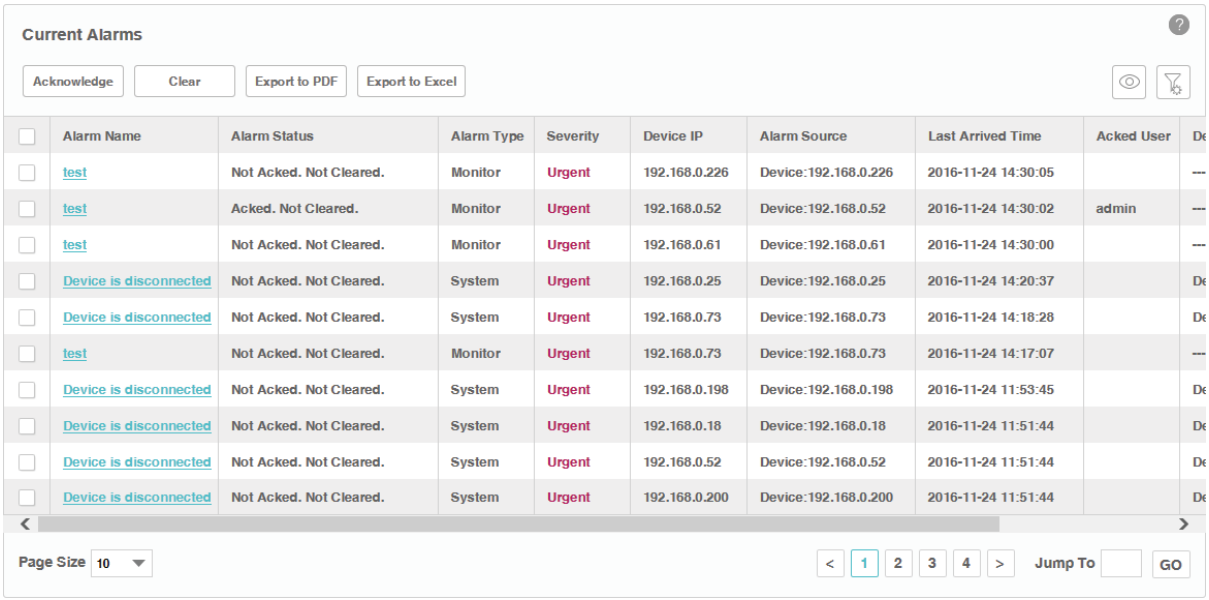
- *View and Manage Current Alarms*
- *View and Manage History Alarms*

5.3.1 View and Manage Current Alarms

Go to **Alarms > Browse Alarm > Current Alarms**.

The alarm list on this page displays the current active alarms of the network. You can acknowledge, clear and export alarms.

Figure 5-8 Current alarm list



View the current alarms

To add or delete columns displayed in the alarm list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

To filter the alarms in the list, click the  . Enter the filter conditions and click **Filter**.

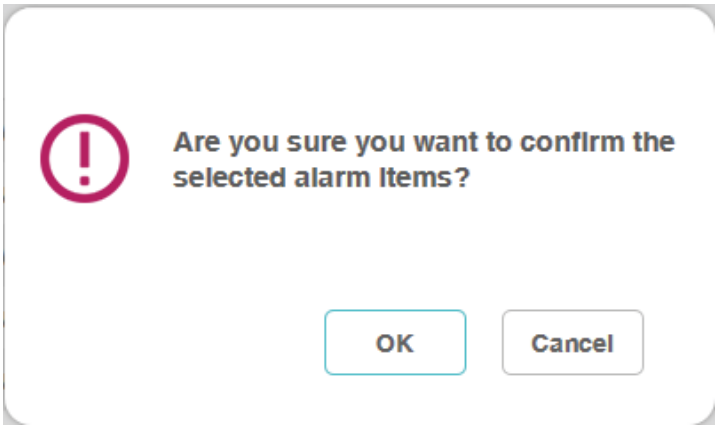
Alarm Name	The name of the alarm. Click it to view the alarm's detailed configurations.
Alarm Status	Whether this alarm is valid.
Alarm Type	Three types of alarms: Trap, Monitor and System.
Severity	Four levels of severity: Urgent, Serious, Normal and Hint.
Device IP	The device IP on which the alarm occurred.
Alarm Source	The source of the alarm.
Last Arrived Time	Displays the last time the alarm arrived at tpNMS.
Acked User	User who confirmed the alarm.
Description	The description of this alarm.

Click the alarm name to view the detailed information of the alarm.

Acknowledge the current alarms

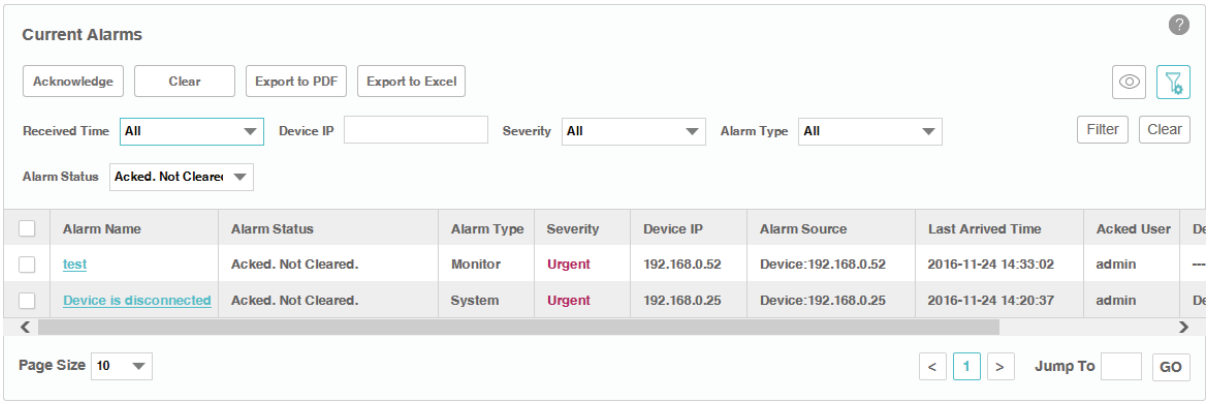
Select your desired alarms and click **Acknowledge** to confirm the alarms. Acknowledging an alarm means that you are in charge of this alarm.

Figure 5-9 Confirm an alarm



When an alarm is confirmed, the confirmed user's name will be filled in the Acked User column.

Figure 5-10 Confirmed alarm



Remove the current alarms

Select your desired alarms and click **Clear** to remove the alarms from this table. The alarms you cleared here will be displayed in the History Alarms list.

Export the current alarms

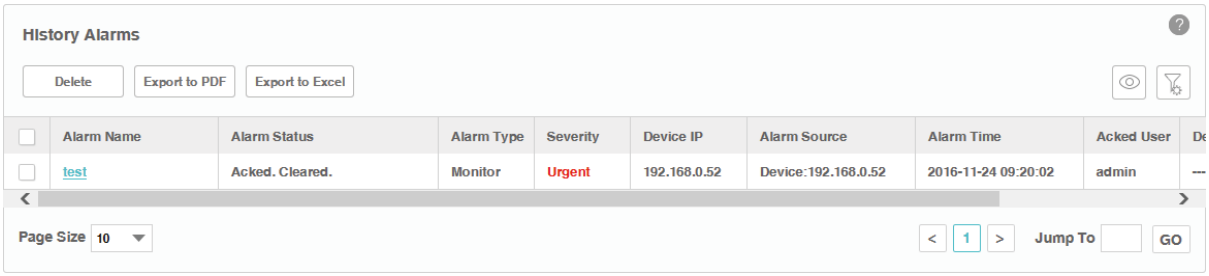
Select your desired alarms and click **Export to PDF** or **Export to Excel** to save the alarms to your computer.

5.3.2 View and Manage History Alarms

Go to **Alarms > Browse Alarm > History Alarms**.

You can remove and export history alarms on this page.

Figure 5-11 History alarm list



View the history alarms

To add or delete columns displayed in the alarm list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

To filter the alarms in the list, click the  . Enter the filter conditions and click **Filter**.

Alarm Name	The name of the alarm. Click it to view the alarm's detailed configurations.
Alarm Status	Whether this alarm is valid.
Alarm Type	Three types of alarms: Trap, Monitor and System.
Severity	Four levels of severity: Urgent, Serious, Normal and Hint.
Device IP	The device IP on which the alarm occurred.
Alarm Source	The source of the alarm.
Alarm Time	Displays the time the alarm arrived at tpNMS.
Acked User	User who confirmed the alarm.
Description	The description of this alarm.

Click the alarm name to view the detailed information of the alarm.

Remove the history alarms

Select your desired alarms and click **Clear** to remove the alarms from this table.

Export the history alarms

Select your desired alarms and click **Export to PDF** or **Export to Excel** to save the alarms to your computer.

5.4 View and Manage Remote Notice Profiles

A remote notice profile defines certain criteria basing on the alarms. tpNMS will generate and send alarm notice emails when specified alarm occurs. The recipients can be customized.

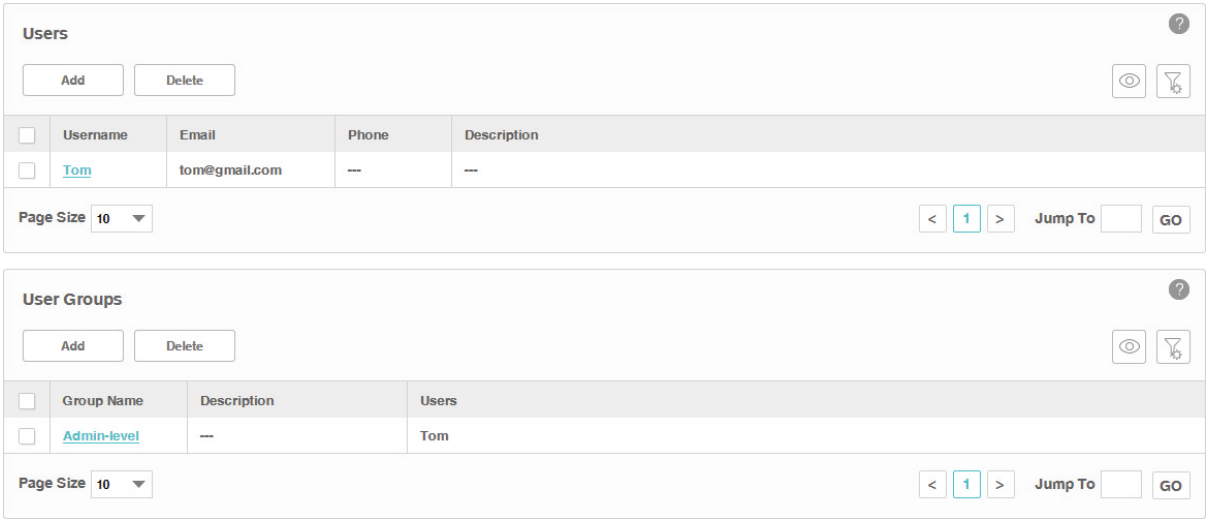
Before the application can send notice emails, you should provide the email addresses of the recipients.

- *View and Manage the Recipients*
- *View and Manage the Notice Rules*

5.4.1 View and Manage the Recipients

Go to **Alarms > Remote Notice > User Groups**.

Figure 5-12 Notification recipients

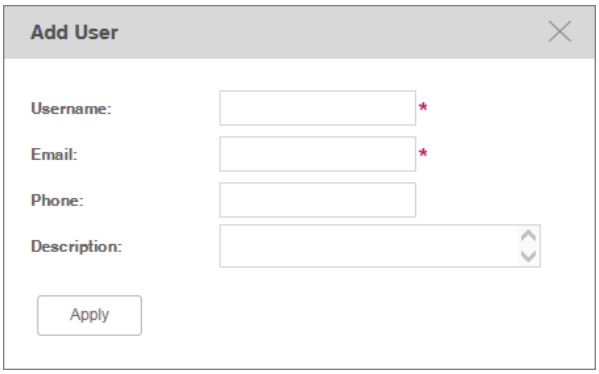


Add or modify a user

· To add a user, click the **Add** button.

· To modify an existing user, click the username.

Figure 5-13 Add or modify a user

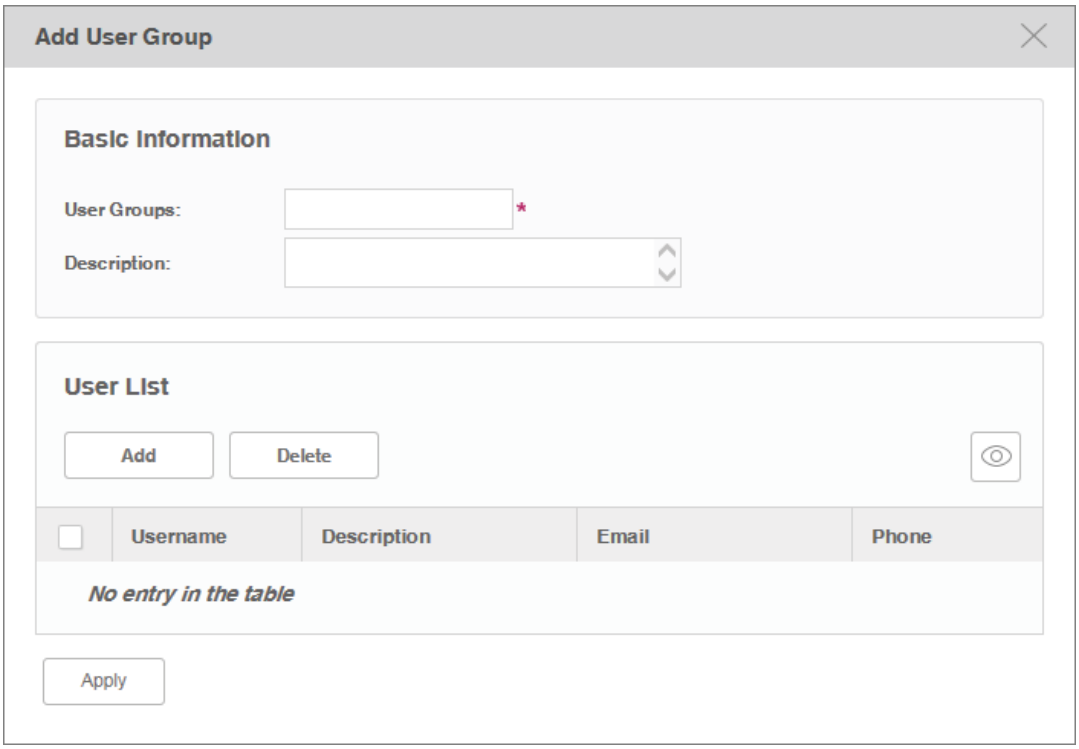


Username	Enter the username.
Email	Enter the email address of the user. The alarm notice emails will be sent to this email address.
Phone	Optional. Enter the phone number of the user.
Description	Optional. Enter the description for this user.

Add or modify a user group

- To add a user group, click the **Add** button.
- To modify an existing user group, click the group name.

Figure 5-14 Add or modify a user group



Basic Information

User Group	Enter the user group name.
Description	Optional. Enter the description for this group.

User List

Click **Add** or **Delete** to manage users in this user group.

View the current users and user groups

To add or delete columns displayed in the alarm list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

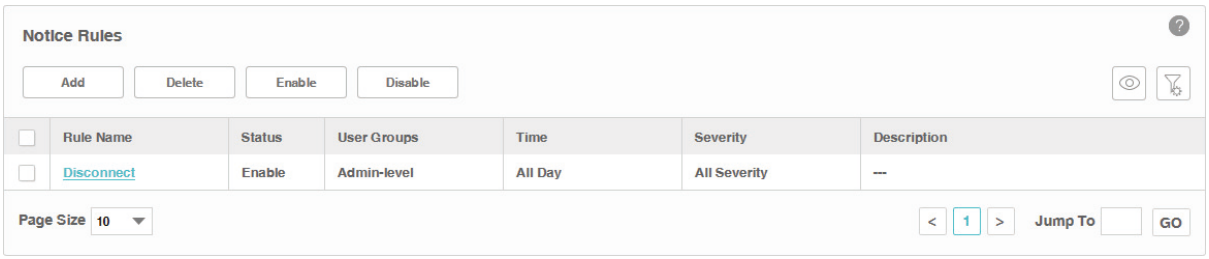
To filter the notice rules in the list, click the  . Enter the filter conditions and click **Filter**.

Click the user/user group name to view the detailed information of the users/user groups.

5.4.2 View and Manage the Notice Rules

Go to **Alarms > Remote Notice > Notice Rules**.

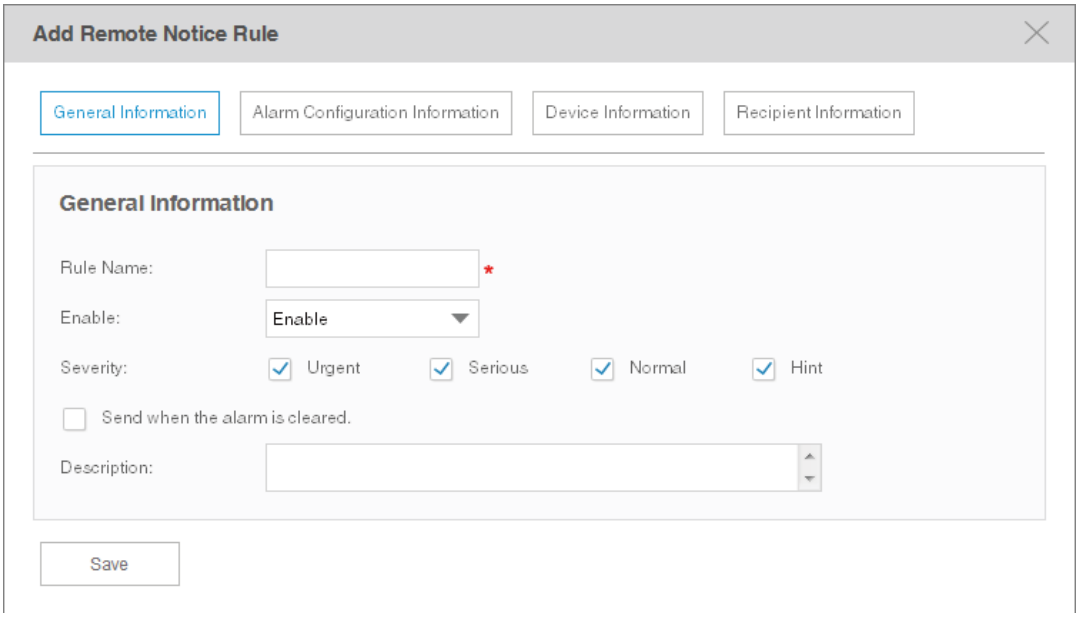
Figure 5-15 Notice rule list



Add or Modify the notice rules

- To add a notice rule, click the **Add** button.
- To modify an existing notice rule, click the rule name.

Figure 5-16 Add or modify a notice rule (general information)



General Information

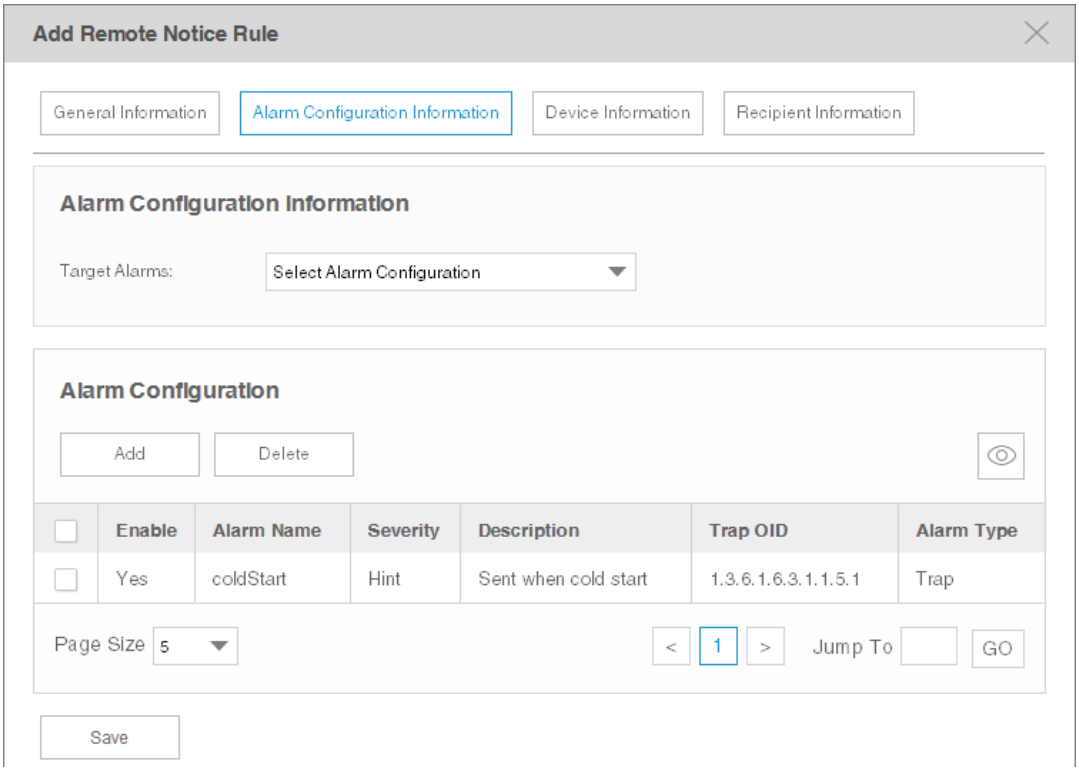
Configure the basic information of the remote rule.

Rule Name	Enter the rule name.
Enable	Enable or disable this notice rule.
Severity	Select which level alarms will trigger this notice.
Send when the alarm is cleared.	A notice mail will be sent when the alarm is cleared if you check this box.
Description	Enter the description for this notice rule.

Alarm Configuration Information

Configure the alarms in this notice rule.

Figure 5-17 Add or modify a notice rule (alarm configuration)

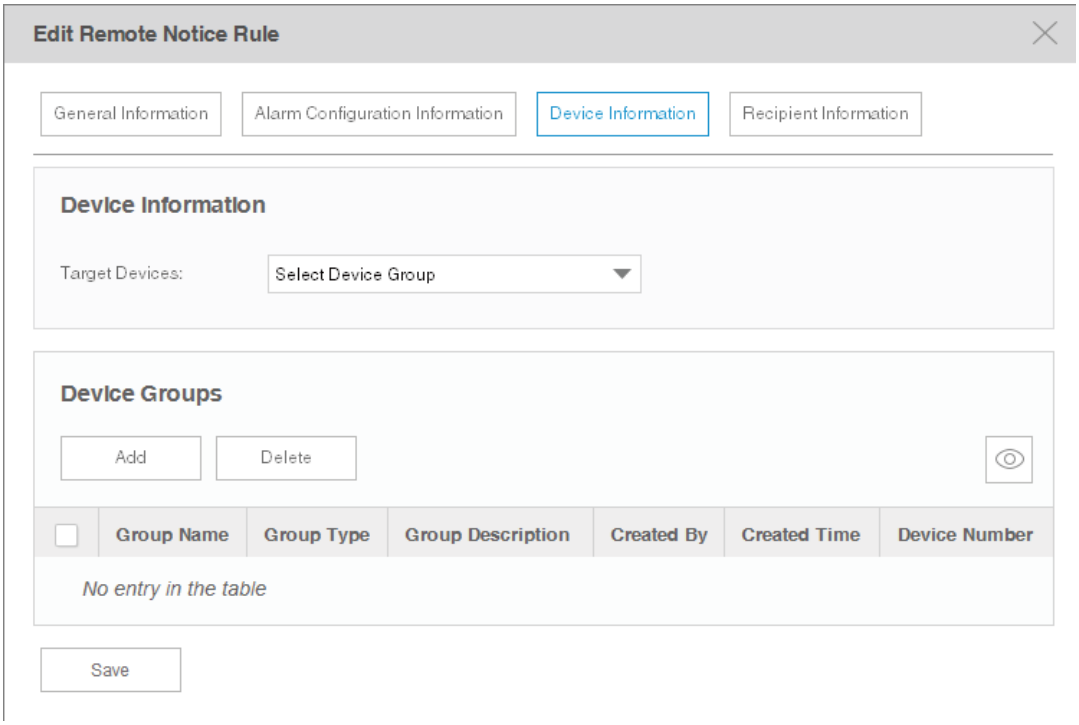


Target Alarms	Select **All Applicable Alarm Configuration,** or select **Select Alarm Configuration** to add the alarm configurations manually.
Add	Click **Add** to add the existing alarm configurations. It is multi-optional.
Delete	Delete the alarm configurations in the Alarm table below.

Device Information

Configure the target devices that the alarms are monitoring.

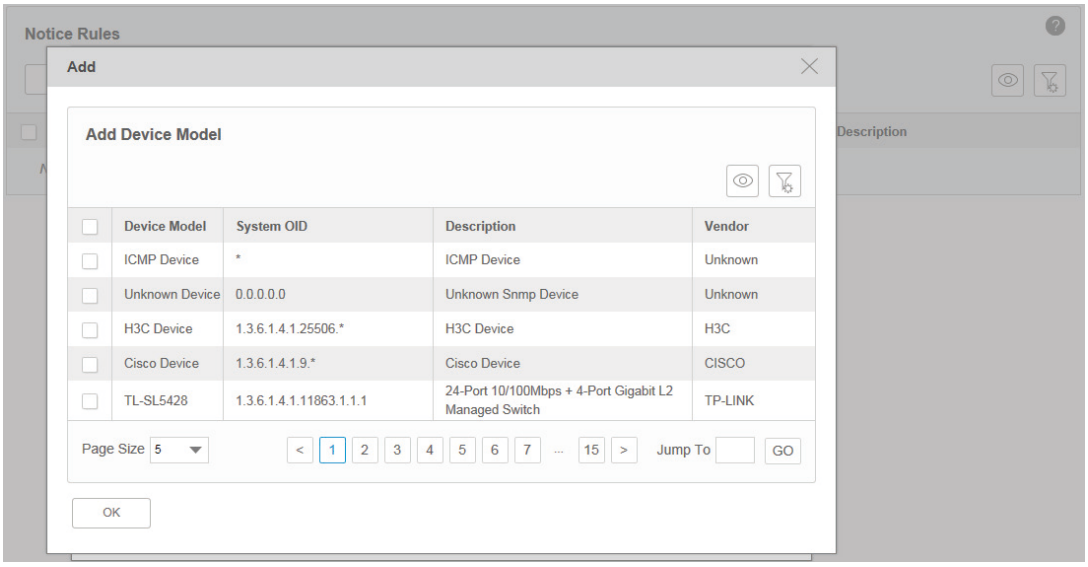
Figure 5-18 Add or modify a notice rule (device information)



Target Devices	Select all the applicable devices or select devices by model, by group or separately.
Add	Click **Add** to add devices according to their model, group or separately.
Delete	Delete the devices in the device table below.

The **Device Add** page displays as below.

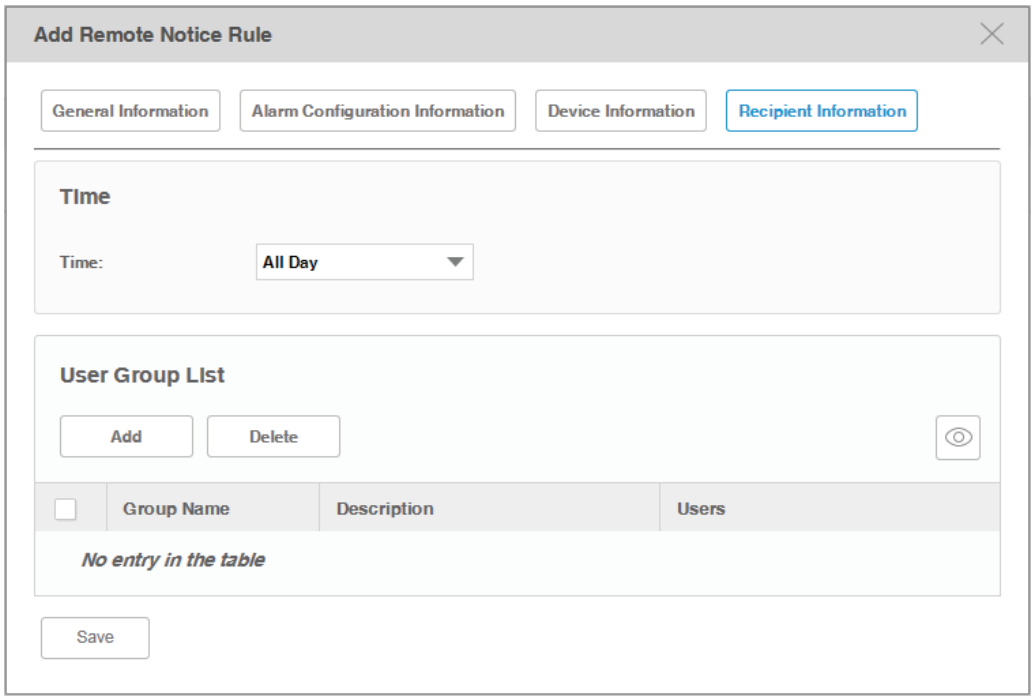
Figure 5-19 Add or modify a notice rule (add device)



Recipient Information

Configure the recipients of the notice, and the alarm's time-range restriction.

Figure 5-20 Add or modify a notice rule (recipient information)



Time	Select the time-range restriction on the alarms. All Day: Alarms that occurs at any time of the day will trigger the notice mail. Specified Time: Specify a time-range. tpNMS will send notice mail only when the alarms occurs in this specified time-range.

Add	Click **Add** to add user groups who will receive the notice email.
Delete	Delete the user groups in the recipient list table below.

Click **Save** to save your modifications.

View the current notice rules

To add or delete columns displayed in the alarm list table, click the  and specify the columns by selecting or deselecting the corresponding checkboxes.

To filter the notice rules in the list, click the  . Enter the filter conditions and click **Filter**.

Click the rule name to view the detailed information of the notice rules.

Rule Name	The name of the notice rule. Click it to view and edit the rule's configurations.
Status	The status displays whether this rule is valid.
User Groups	Displays the recipients of the notification email.
Time	The sending time period of the notification email.
Severity	Displays the filtering criteria of the alarms. Only the alarms of the severity levels displayed will be sent in the email.
Description	Displays the description on this notice rule.

6 Manage the Configuration and Firmware Files

This chapter mainly introduces how to manage the device's configuration files and firmware files.

If you want to manage the discovered device (backup, restore or upgrade), you should go to the *Access Config* page and configure the device's telnet template. The name and password in the telnet template are the same user information that you use to telnet in to the device to perform system configuration.

6.1 Back Up Device Configurations

You can schedule a backup task to back up the configurations of the devices on your network.

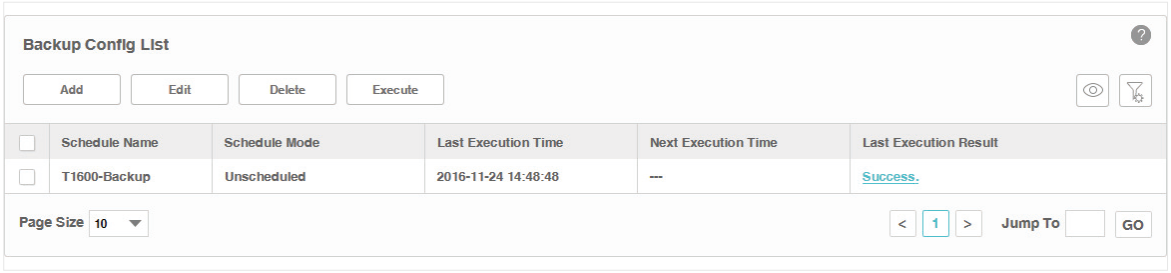
The backup configuration files will be saved in the **\data\tftpDir** in the tpNMS's installation directory.

- *Add or Modify a Backup Schedule*
- *Execute a Backup Schedule*
- *View the Execution Result of a Backup Schedule*
- *Remove a Backup Schedule*

6.1.1 Add or Modify a Backup Schedule

1. Go to **Config > Backup Management > Backup Schedule**.

Figure 6-1 Backup schedule list



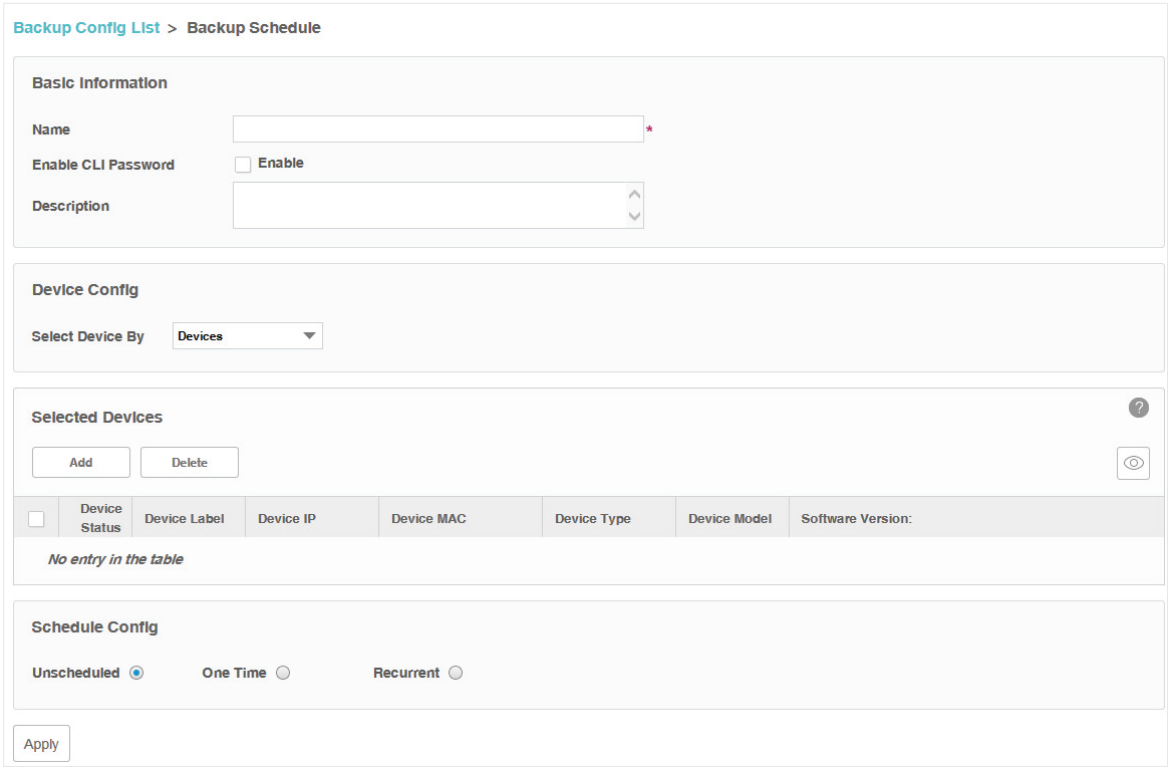
2. Add a backup schedule or modify an existing backup schedule.

   · To add a backup schedule, click the **Add** button.

   · To modify an existing backup schedule, select your desired schedule entry and click **Edit**.

The following screen displays.

Figure 6-2 Add or modify a backup schedule



Basic Information

Name	Enter the name of the backup schedule.
Enable CLI Password	Check this box and enter the device's privilege-mode password if necessary.
Description	Enter the description for this schedule.

Device Config

Select Device By	Select the target device by device or by device group.

Selected Devices

Add	Add a device/device group whose configuration files will be backed up.
Delete	Remove the selected device/device group from the table below.

Schedule Config

Unscheduled	The unscheduled backup task will be displayed in the schedule list, but will not be executed automatically. You can manually perform the backup task on the screen **Config > Backup Management > Backup Schedule** with the **Execute** button.

One Time	Select One Time and enter the Execution Time, the schedule task will be executed automatically at the time you set.
Recurrent	Select Recurrent and complete the schedule mode and frequency below, the schedule task will be executed recurrently.

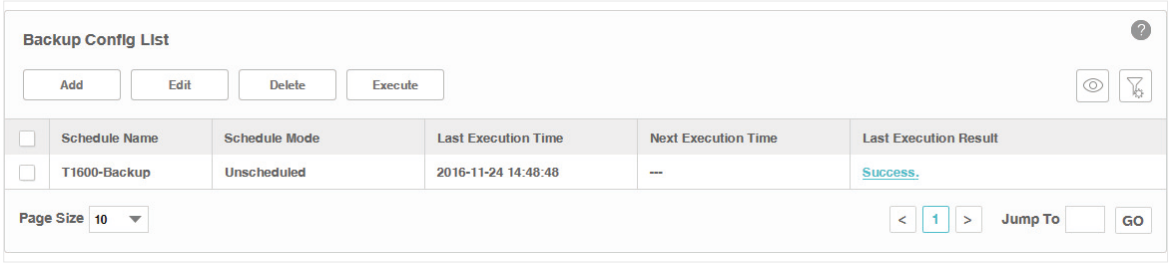
Click **Apply** to save your configurations.

6.1.2 Execute a Backup Schedule

You can execute a backup task in the schedule table immediately, either the task is unscheduled or recurred.

1. Go to **Config > Backup Management > Backup Schedule**.

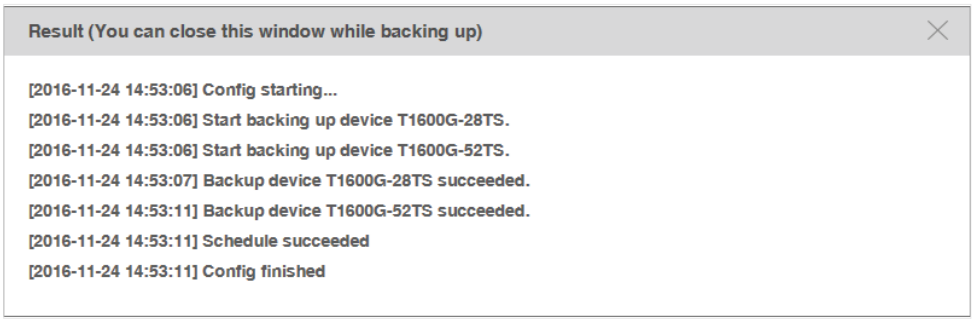
Figure 6-3 Backup schedule list



Schedule Name	Displays the name of the backup schedule.
Schedule Mode	Displays the mode of the backup schedule.
Last Execution Time	Displays the last execution time of this backup time.
Next Execution Time	Displays the next execution time of this backup time.
Last Execution Result	Click the link to view the detailed information of this backup task's last execution result.

2. Click the **Execute** button to execute your selected backup schedule immediately. A window will pop up to display the execution result.

Figure 6-4 Backup process



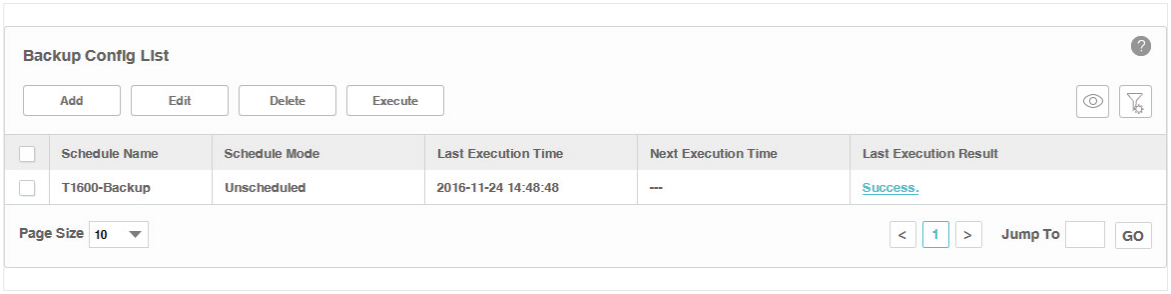
Click the ✕ in the upper-right corner to close this pop-up window. You can close this window and perform some other operations with tpNMS during the backup process. The backup process will run in the background. You can view the backup's progress on the screen **Tasks > Task Management > Tasks**.

6.1.3 View the Execution Result of a Backup Schedule

You can view the execution status of your desired backup job to ensure that the device's configuration is backed up as scheduled.

1. Go to **Config > Backup Management > Backup Schedule**.

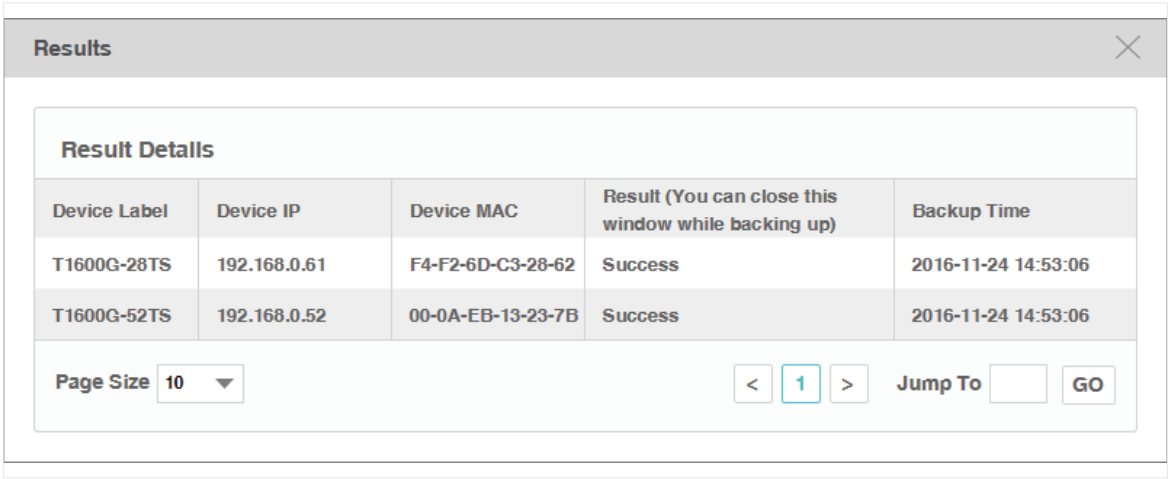
Figure 6-5 Backup schedule list



Schedule Name	Displays the name of the backup schedule.
Schedule Mode	Displays the mode of the backup schedule.
Last Execution Time	Displays the last execution time of this backup time.
Next Execution Time	Displays the next execution time of this backup time.
Last Execution Result	Click the link to view the detailed information of this backup task's last execution result.

2. Click the link in the last row of the schedule table to view the detailed execution result.

Figure 6-6 Backup result



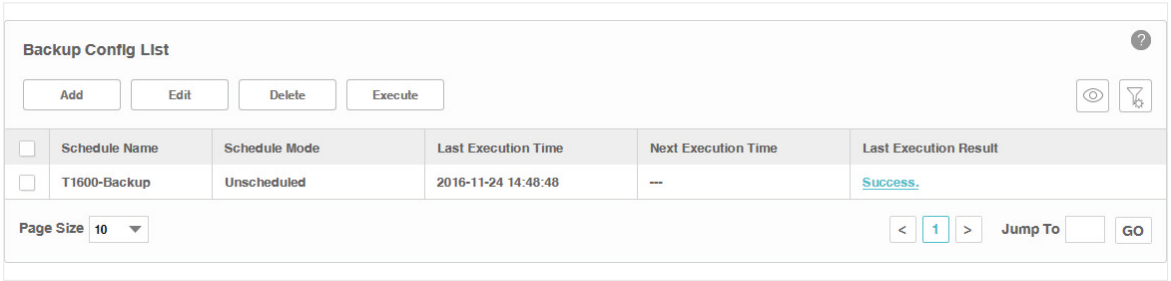
Schedule Name	Displays the label of the device.
Device IP	Displays the IP address of the device.
Device MAC	Displays the MAC address of the device.
Result (You can close this window while backing up)	Displays the backing up result.
Backup Time	Displays the time of the backup operation.

6.1.4 Remove a Backup Schedule

You can remove your selected backup schedule task in the schedule Table.

1. Go to **Config > Backup Management > Backup Schedule**.

Figure 6-7 Backup schedule list



Schedule Name	Displays the name of the backup schedule.
Schedule Mode	Displays the mode of the backup schedule.

Last Execution Time	Displays the last execution time of this backup time.
Next Execution Time	Displays the next execution time of this backup time.
Last Execution Result	Click the link to view the detailed information of this backup task's last execution result.

2. Select the backup profile and click **Delete** to remove the profile from this table.

6.2 Restore Device Configurations

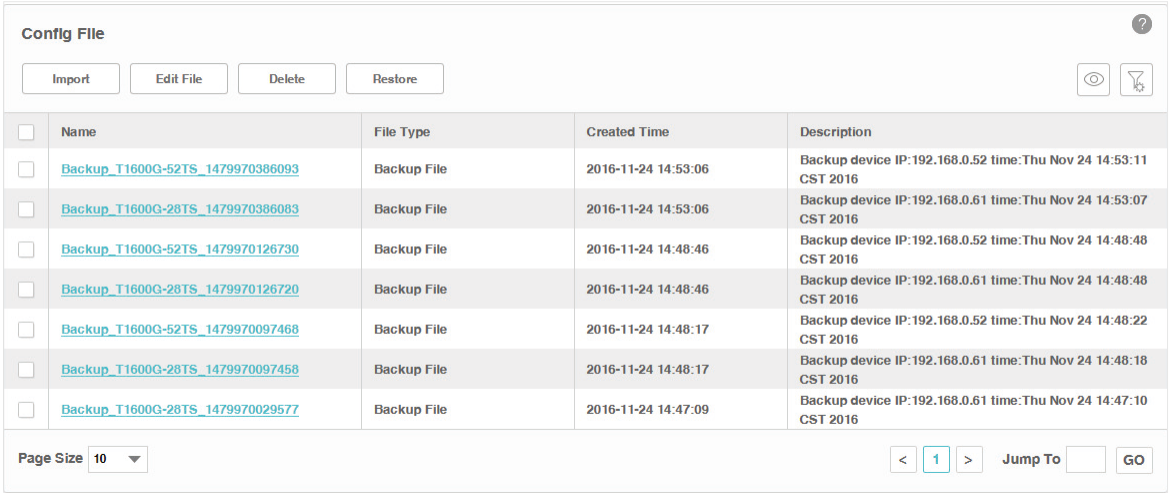
You can upload the configuration files of the devices to tpNMS, and restore the configuration files to corresponding device(s) on your network.

- *Import a Configuration File*
- *Modify a Configuration File*
- *Remove a Configuration File*
- *Add a Restore Schedule*

6.2.1 Import a Configuration File

1. Go to **Config > Deploy Management > Config File**.

Figure 6-8 Configuration file list



2. Click **Import** to upload the configuration file with **.cfg** extension from your computer.

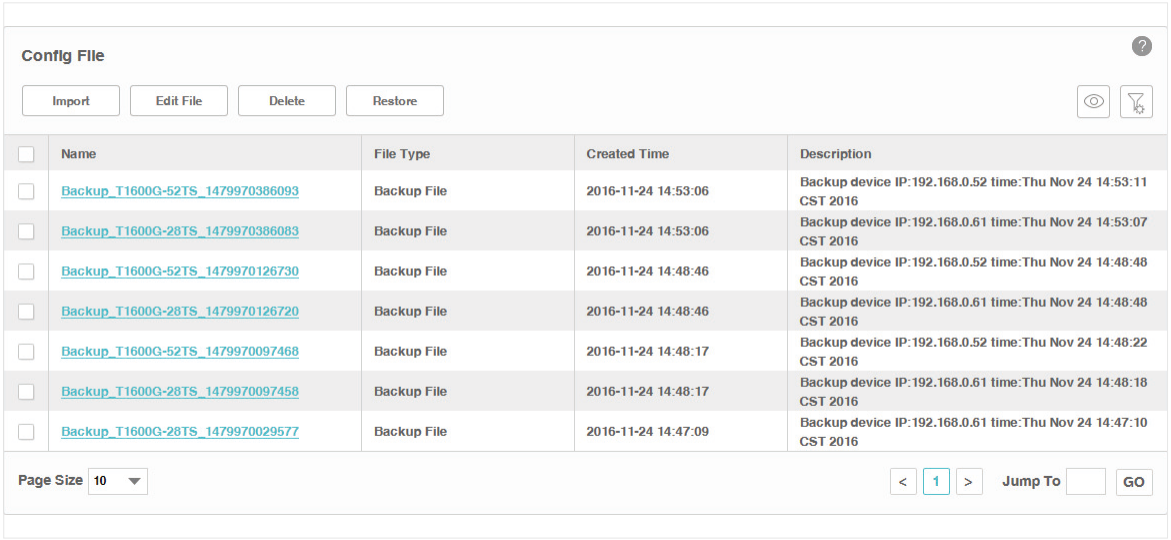
Figure 6-9 Upload a configuration file

3. Click **Apply** and the configuration file is listed in the Config File table.

6.2.2 Modify a Configuration File

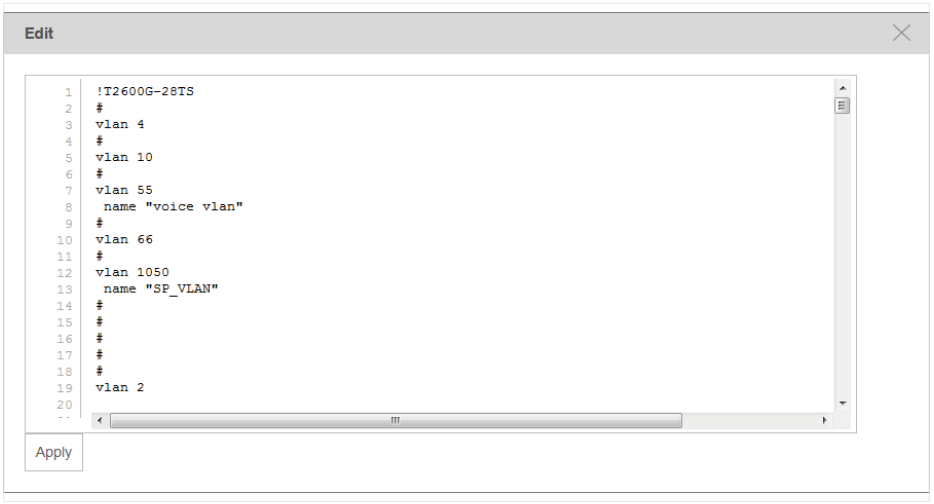
1. Go to **Config > Deploy Management > Config File**.

Figure 6-10 Configuration file list



2. Select the desired configuration file in the table and click **Edit File** to modify this file.

Figure 6-11 Edit a configuration file

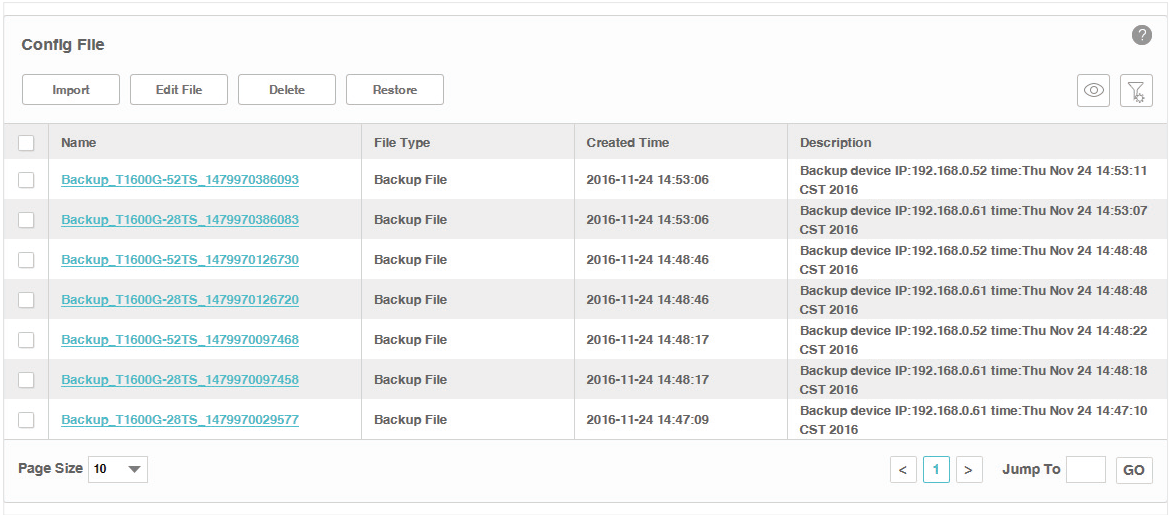


3. Click **Apply** to save your modifications to the configuration file.

6.2.3 Remove a Configuration File

1. Go to **Config > Deploy Management > Config File**.

Figure 6-12 Configuration file list



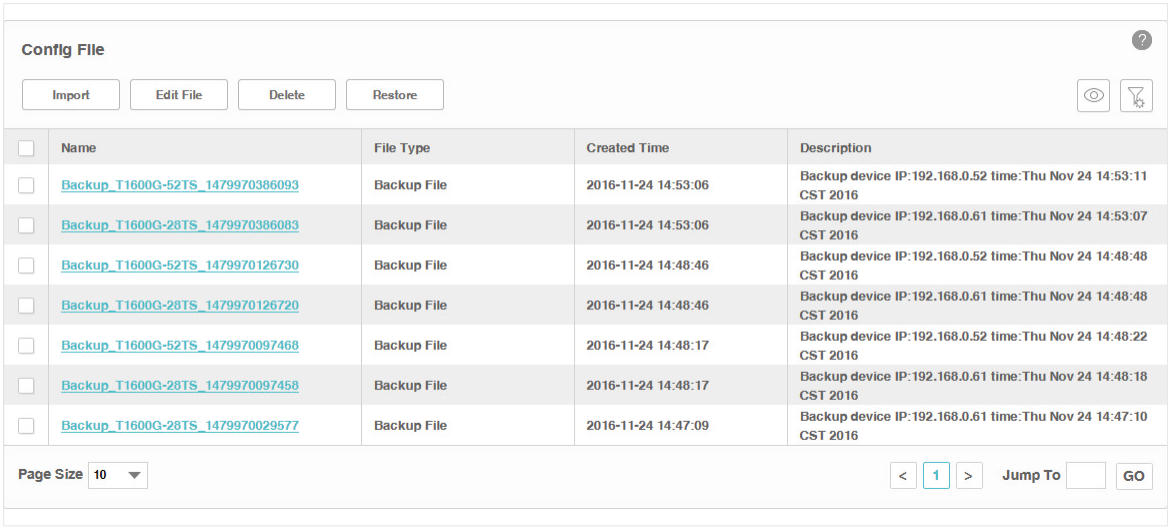
2. Select the desired configuration file and click **Delete** to remove this file from the table.

3. Click **OK** in the pop-up confirm window to complete the deletion.

6.2.4 Add a Restore Schedule

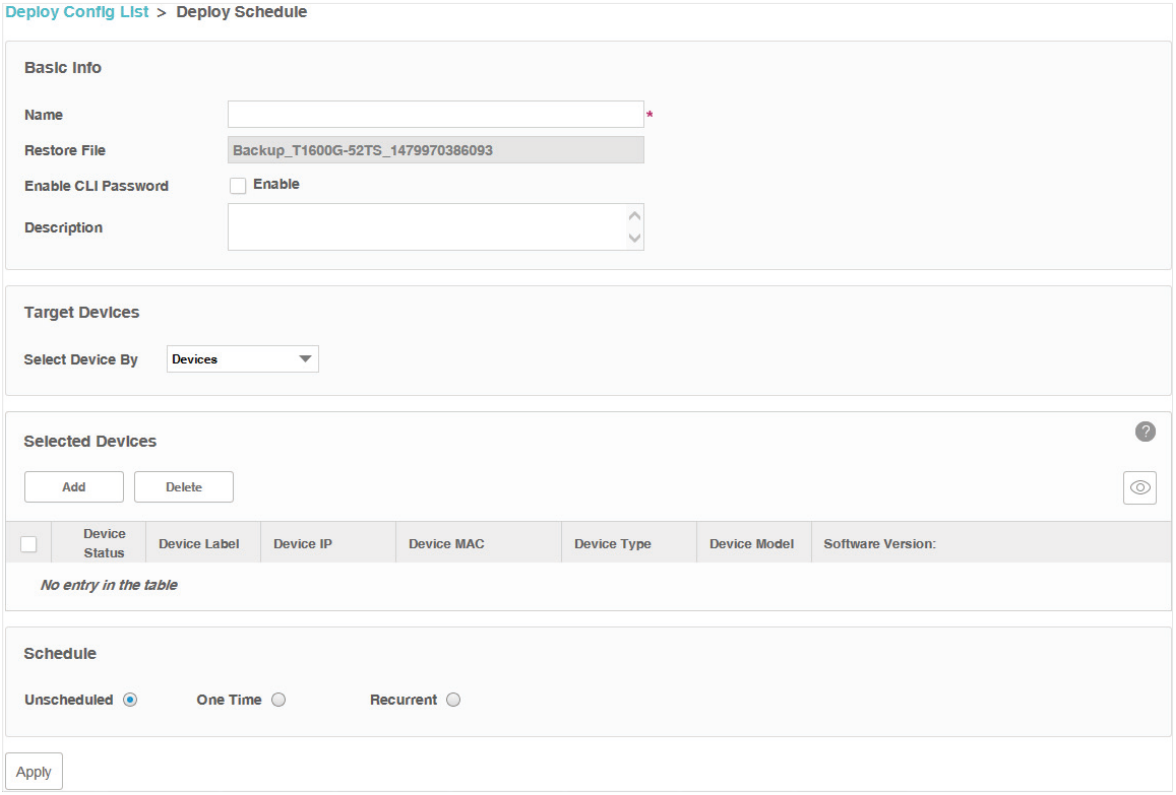
1. Go to **Config > Deploy Management > Config File**.

Figure 6-13 Configuration file list



2. Select the configuration file in the table and click **Restore**.
3. In the **Deploy Config List > Deploy Schedule** window, edit the schedule's information.

Figure 6-14 Edit a restore schedule



Basic Info

Name	Enter the name of the restore schedule.
Restore File	Display the name of the configuration file.
Enable password	Click the checkbox to enter the device's privileged password if necessary.
Description	Enter the description of the restore schedule.

Target Devices

Select Device By	Select the target devices by devices or by device groups.

Selected Devices

Add/Delete	Edit the target devices or device groups.

Schedule

Unscheduled	The unscheduled restore task will be displayed in the schedule list, but will not be executed automatically. You can manually perform the restore task on the screen **Config > Deploy Management > Deploy Schedule** with the **Execute** button.
One Time	Select One Time and enter the Execution Time, the schedule task will be executed automatically at the time you set.
Recurrent	Select Recurrent and complete the schedule mode and frequency below. The schedule task will be executed recurrently.

Click **Apply** to save the restore schedule information.

6.3 Upgrade Device Firmwares

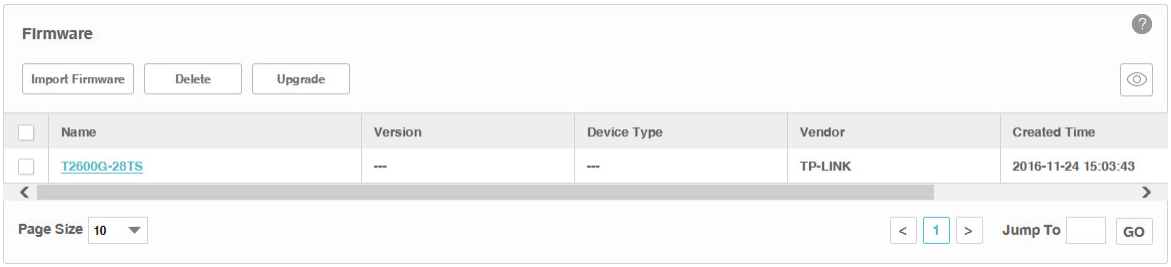
You can upload the firmware files of the devices to tpNMS, and upgrade corresponding device(s) on your network with the configuration files.

- *Import a Firmware File*
- *Remove a Firmware File*
- *Add a Firmware Upgrade Schedule*

6.3.1 Import a Firmware File

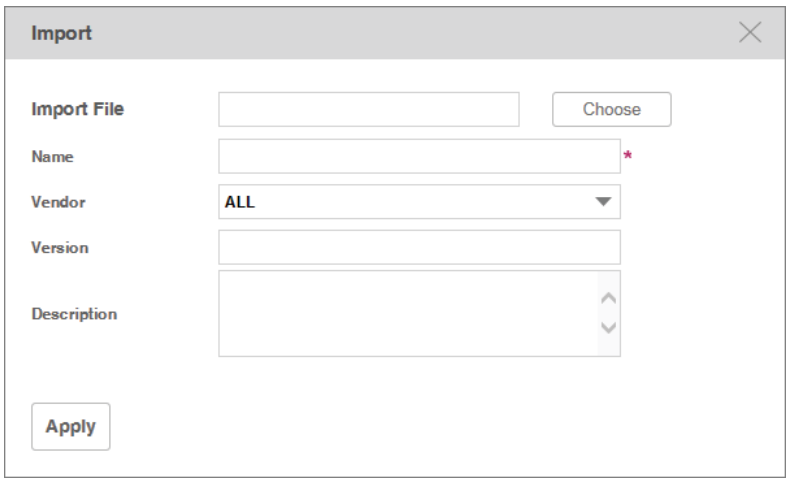
1. Go to **Config > Deploy Management > Firmware**.

Figure 6-15 Firmware file list



2. Click **Import** to upload the firmware file from your computer.

Figure 6-16 Import a firmware file



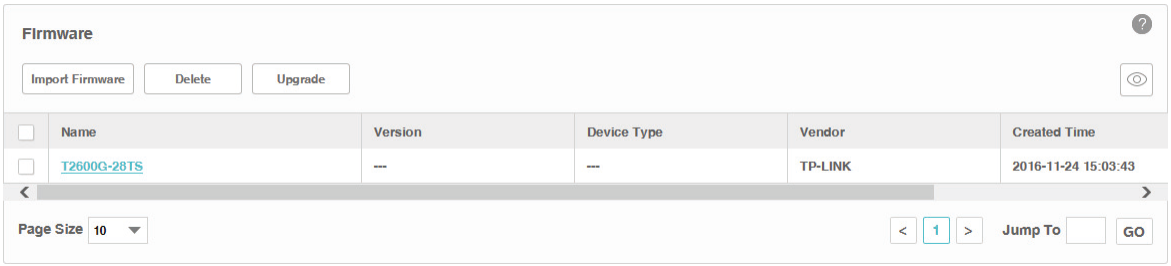
Import File	Click **Choose** to select the firmware file from your computer.
Name	Enter the name of this firmware file.
Vendor	Select the vendor of the device corresponding to this firmware.
Version	Enter the firmware version.
Description	Enter the description of this firmware file.

3. Click **Apply** and the firmware file is listed in the Firmware File table.

6.3.2 Remove a Firmware File

1. Go to **Config > Deploy Management > Firmware**.

Figure 6-17 Firmware file list

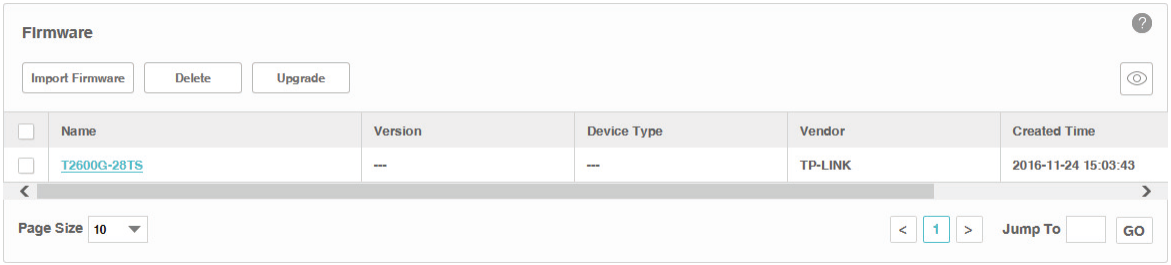


2. Select the desired firmware file and click **Delete** to remove this file from the table.
3. Click **OK** on the pop-up confirm window to complete the deletion.

6.3.3 Add a Firmware Upgrade Schedule

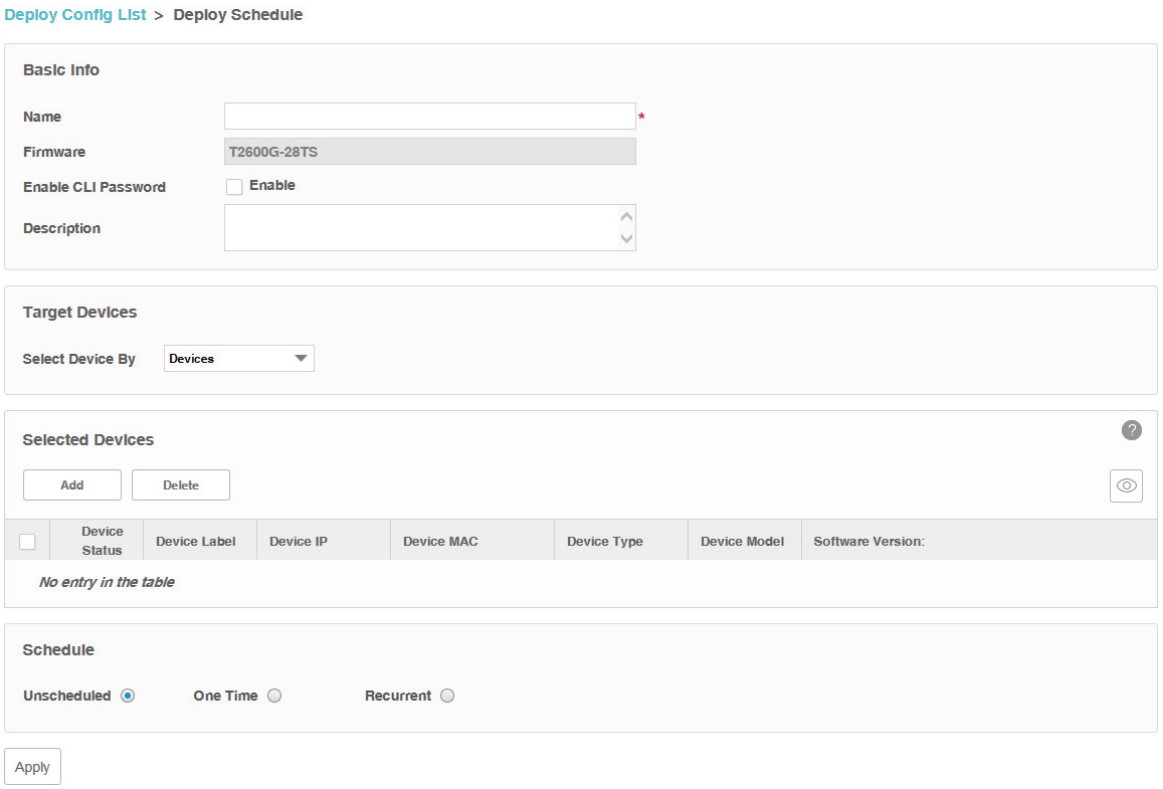
1. Go to **Config > Deploy Management > Firmware**.

Figure 6-18 Firmware file list



2. Select the firmware file in the table and click **Upgrade**.
3. In the **Deploy Config List > Deploy Schedule** window, edit the schedule's information.

Figure 6-19 Edit a upgrade schedule



Basic Info

Name	Enter the name of the upgrade schedule.

Firmware	Display the name of the firmware file.
Enable password	Click the checkbox to enter the device's privileged password if necessary.
Description	Enter the name of the upgrade schedule.

Target Devices

Select Device By	Select the target devices by devices or by device groups.

Selected Devices

Add/Delete	Edit the target devices or device groups.

Schedule

Unscheduled	The unscheduled upgrade task will be displayed in the schedule list, but will not be executed automatically. You can manually perform the upgrade task on the screen **Config > Deploy Management > Deploy Schedule** with the **Execute** button.
One Time	Select One Time and enter the Execution Time. The schedule task will be executed automatically at the time you set.
Recurrent	Select Recurrent and complete the schedule mode and frequency below, the schedule task will be executed recurrently.

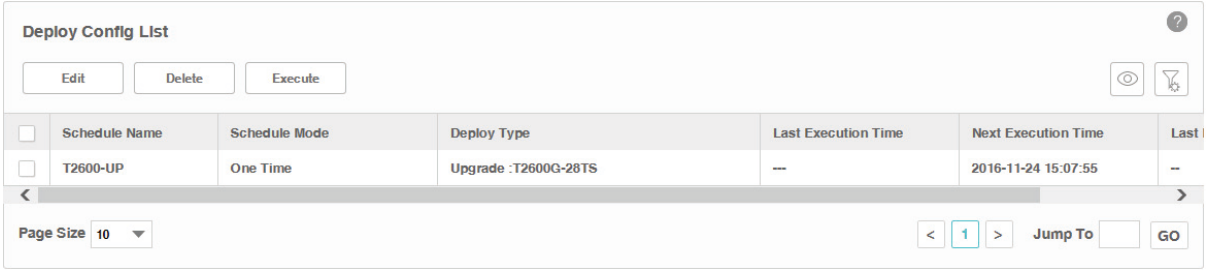
Click **Apply** to save the upgrade schedule information.

6.4 View and Manage Schedules

Go to **Config > Deploy Management > Deploy Schedule**.

Your configuration-restore schedules and firmware-upgrade schedules can be viewed and managed on this page.

Figure 6-20 Schedule list



- *View the Execution Status of the Schedules*
- *Edit a Schedule*
- *Remove a Schedule*
- *Execute a Schedule*

6.4.1 View the Execution Status of the Schedules

Go to **Config > Deploy Management > Deploy Schedule**.

The schedule table displays the following items:

Schedule Name	Displays the name of the schedule.
Schedule Mode	Displays the schedule mode.
Deploy Type	Displays the detail type of the schedule task.
Last Execution Time	Displays the last time when the schedule task was executed.
Next Execution Time	Displays the next time when the schedule task will be executed.
Last Execution Result	Displays the general result of the schedule's last execution.

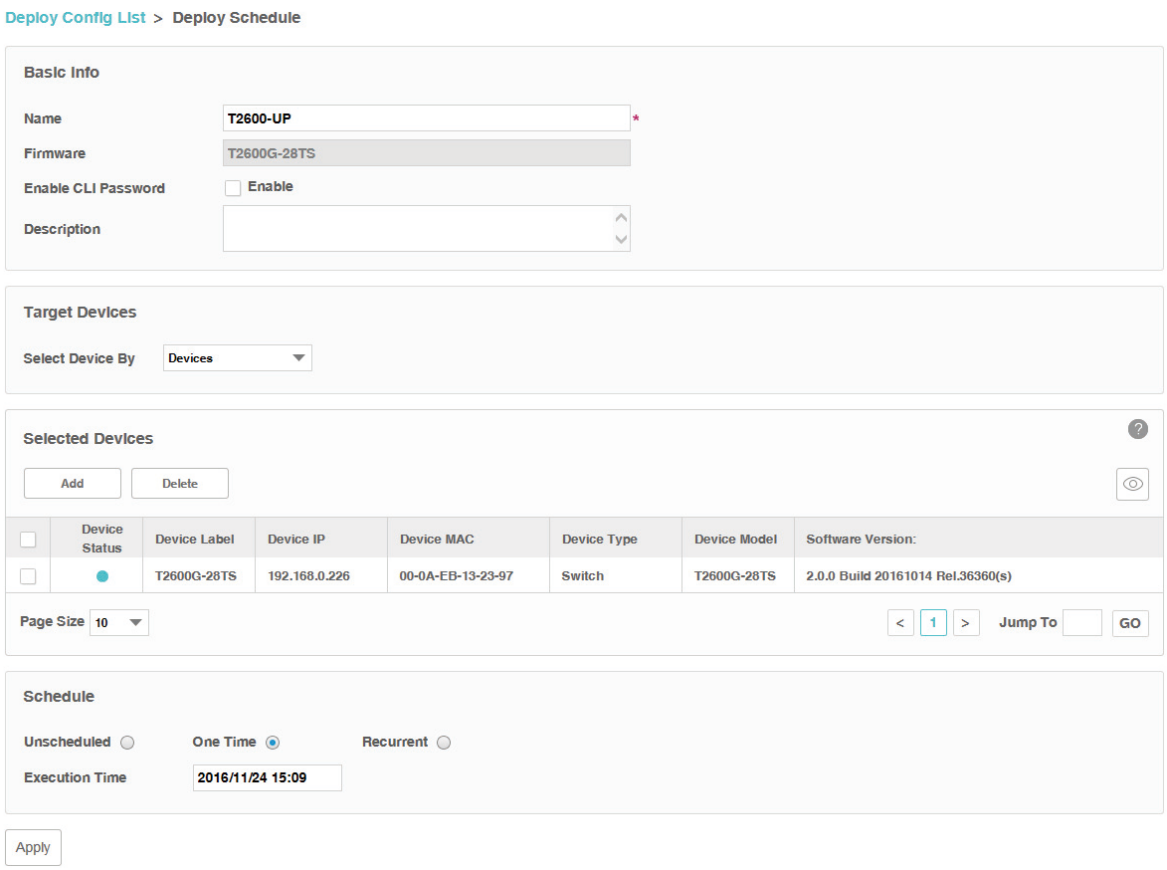
Click the link in the Last Execution Result Row to view the detailed execution result.

6.4.2 Edit a Schedule

Go to **Config > Deploy Management > Deploy Schedule**.

Select a schedule and click **Edit** to modify the detailed configuration of the schedule task.

Figure 6-21 Edit a schedule



Basic Info

Name	Enter the name for the schedule.
Restore File/ Firmware	Display the name of the restore file/firmware file.
Enable password	Click the checkbox to enter the device's privileged password if necessary.
Description	Enter the name for the schedule.

Target Devices

Select Device By	Select the target devices by devices or by device groups.

Selected Devices

Add/Delete	Edit the target devices or device groups.

Schedule

Unscheduled	The unscheduled task will be displayed in the schedule list, but will not be executed automatically. You can manually perform the task on the screen **Config > Deploy Management > Deploy Schedule** with the **Execute** button.
One Time	Select One Time and enter the Execution Time, the schedule task will be executed automatically at the time you set.
Recurrent	Select Recurrent and complete the schedule mode and frequency below, the schedule task will be executed recurrently.

Click **Apply** to save the schedule's configuration.

6.4.3 Remove a Schedule

Go to **Config > Deploy Management > Deploy Schedule**.

Select a schedule and click **Delete** to remove the schedule from the table.

6.4.4 Execute a Schedule

Go to **Config > Deploy Management > Deploy Schedule**.

Click the **Execute** button to execute your selected restore schedule/upgrade schedule immediately. A window will pop up to display the execution result.

Figure 6-22 Schedule's running status

You can close this window and perform some other operations with tpNMS during the backup process. The restore/upgrade process will run in the background. You can view the execution progress on the screen **Tasks > Task Management > Tasks**.

Note::

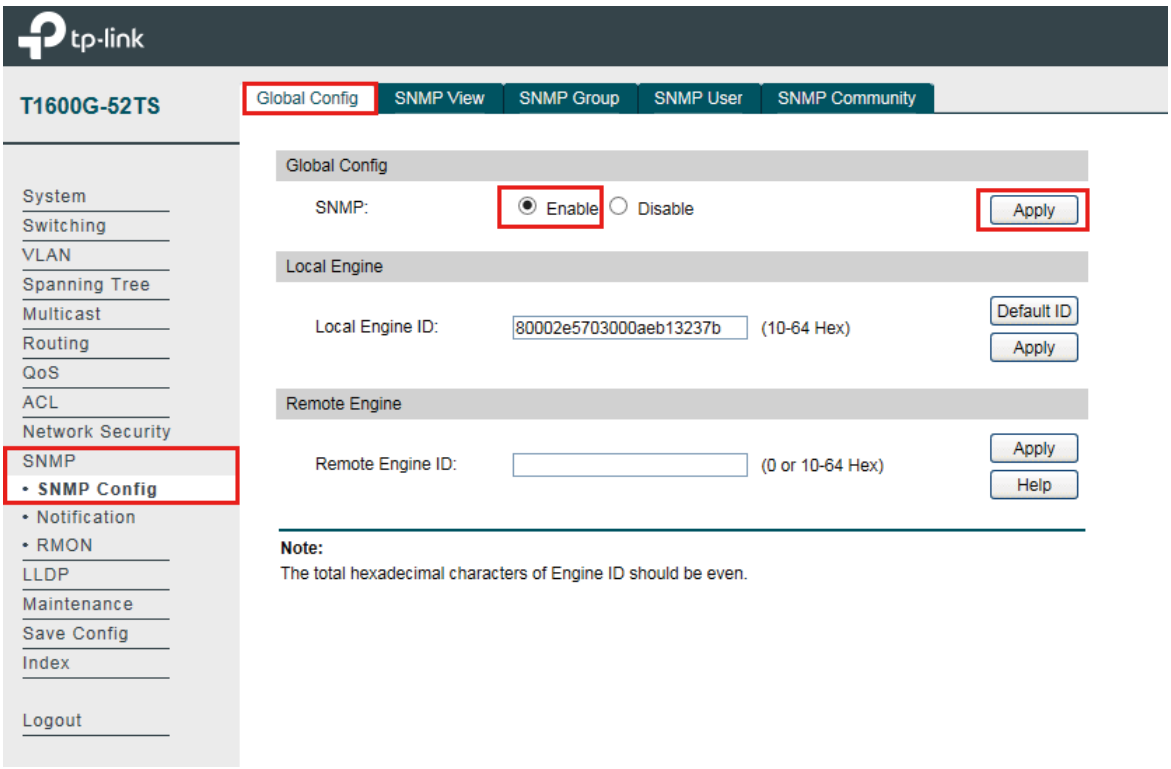
If the switch you want to upgrade is a dual-image switch, the upgrade schedule will only upgrade the switch's backup image. You should configure the switch to reboot with the backup image after the upgrade schedule is finished.

6.5 Example: Backup Configuration File for a Device

tpNMS host and T1600G-52TS are in the same subnet. The IP address of T1600G-52TS is 192.168.0.52. The configuration task is to backup T1600G-52TS's configuration file with tpNMS.

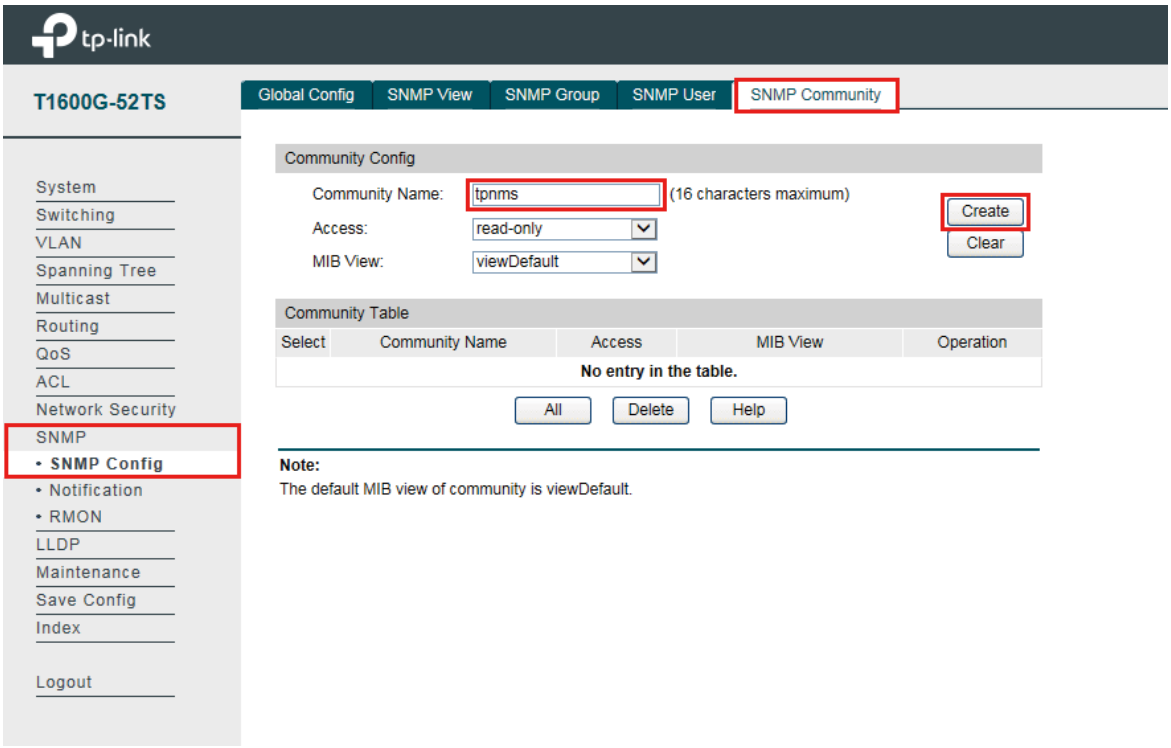
1. Log in to T1600G-52TS's web interface.
2. Go to **SNMP > SNMP Config > Global Config**. Select **Enable** and click **Apply** to enable SNMP function globally.

Figure 6-23 Enable SNMP in T1600G-52TS



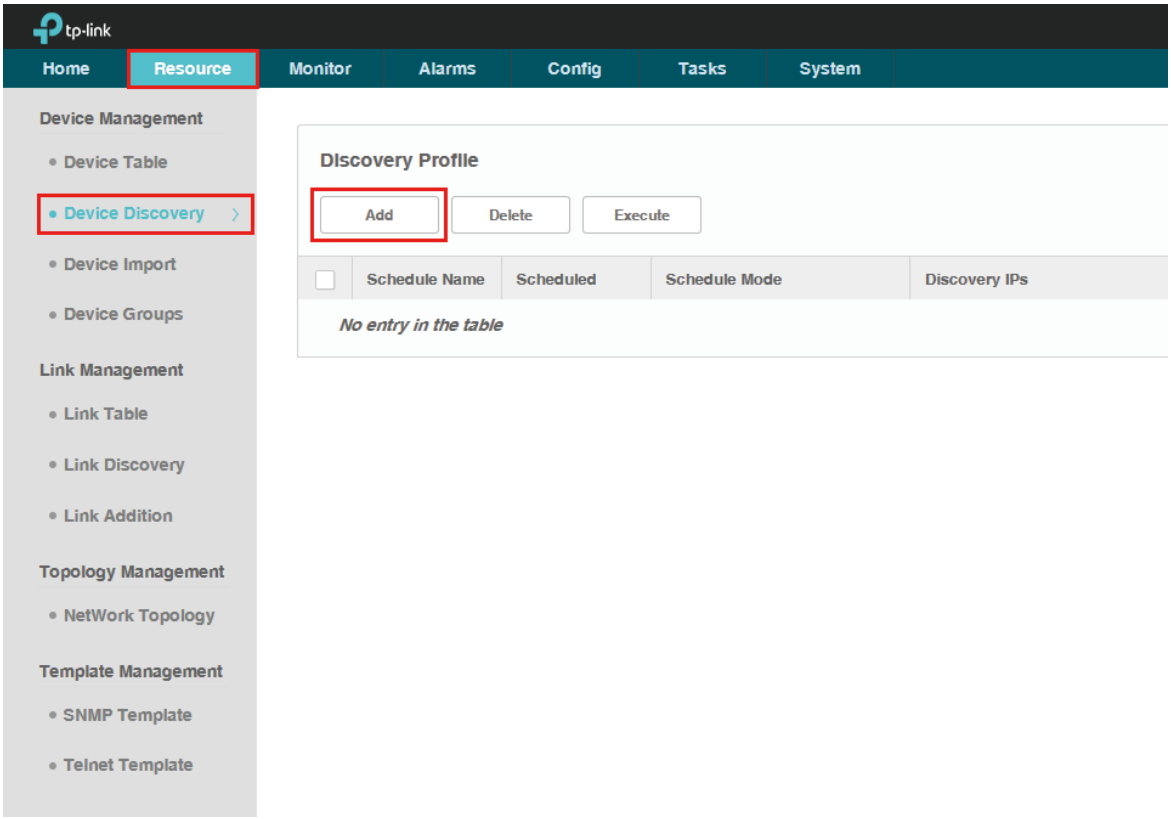
3. Go to **SNMP > SNMP Config > SNMP Community**. Create a community with the name **tpnms** and click **Create**.

Figure 6-24 Create SNMP community in T1600G-52TS



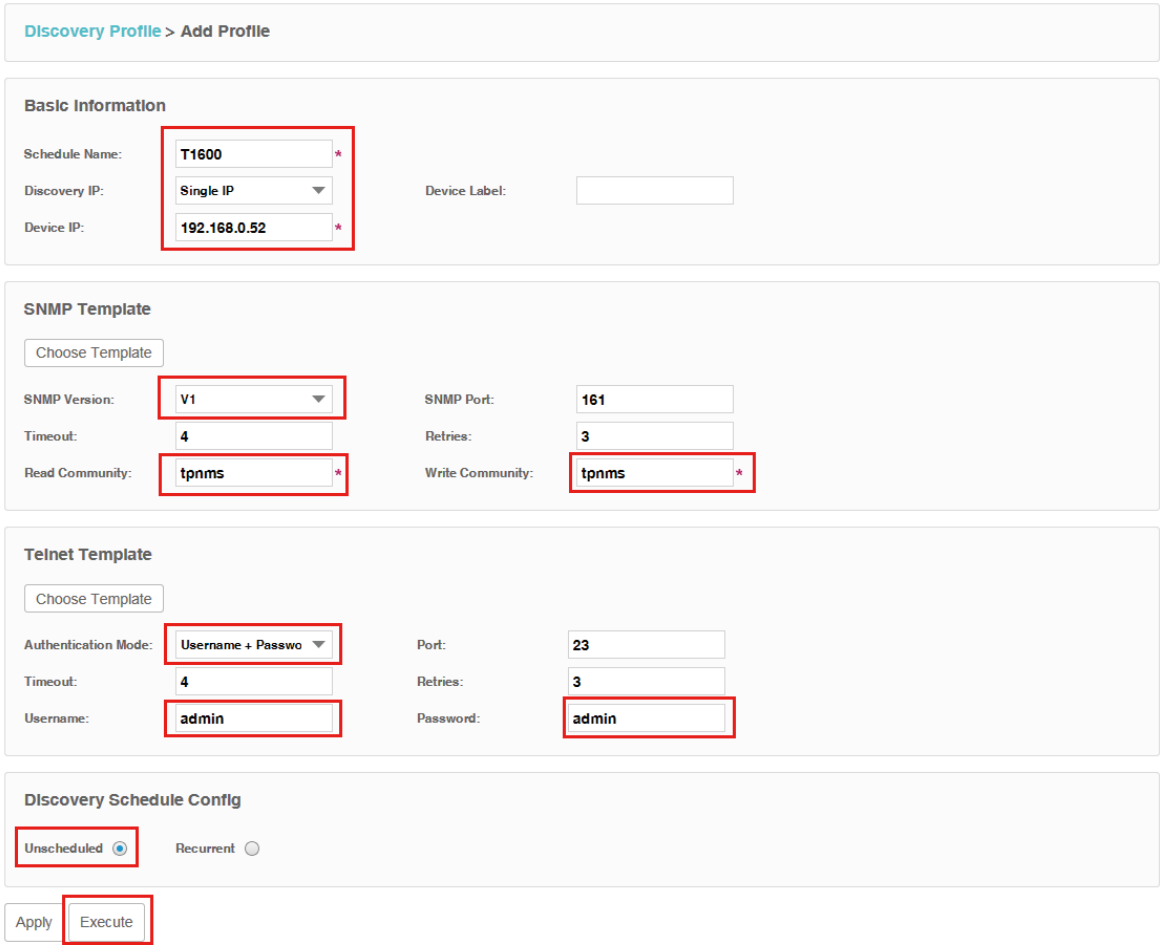
4. Log in to tpNMS.
5. Go to **Resource > Device Management > Device Discovery**. Click **Add** to create a discovery profile.

Figure 6-25 Add a discovery profile



6. Enter the profile information on this page, and click **Execute** to discover T1600G-52TS.

Figure 6-26 Add a discovery profile



Basic Information

Specify the Schedule Name **T1600**, select Discovery IP as **Single IP** and enter **192.168.0.52** in the Device IP.

SNMP Template

Select **V1** as SNMP Version, and enter **tpnms** in the Read Community and Write Community field.

Telnet Template

The T1600G-52TS's default telnet mode is Login Local Mode, and the username and password are both admin. If you want to customize the telnet configuration, please refer to T1600G-52TS's Command-Line Interface Guide.

Select **Username + Password** as Authentication Mode, and enter **admin** in both the Username and Password.

Discovery Schedule Config

Select **Unscheduled**.

At last, leave the rest fields with their default values and click **Execute**.

7. The discovery result shows in the pop-up window. You can view the discovered deivce in the device list.

Figure 6-27 Discovery result

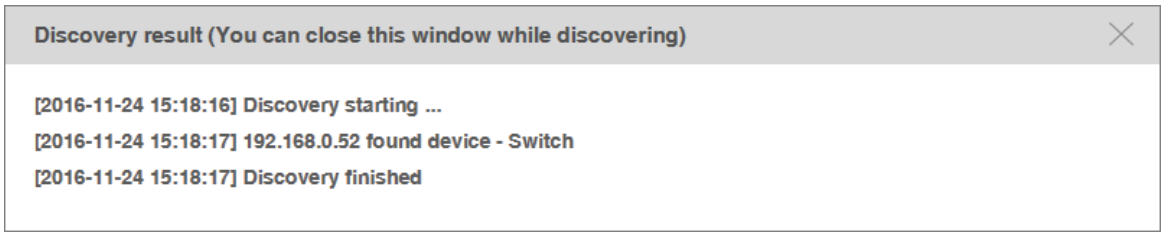
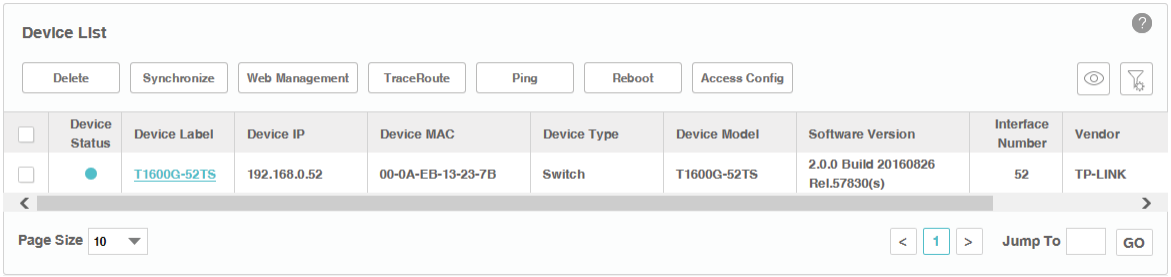
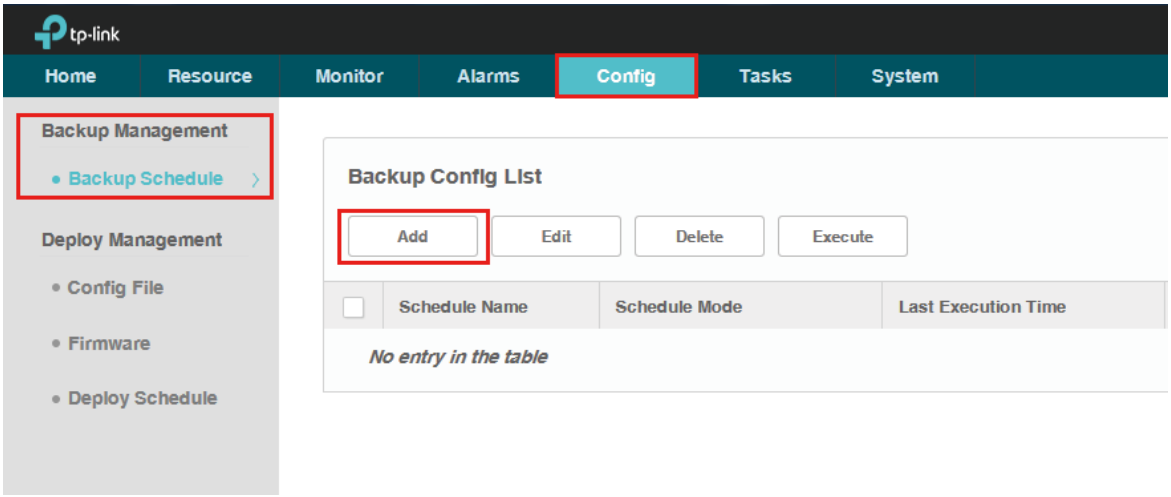


Figure 6-28 Device list



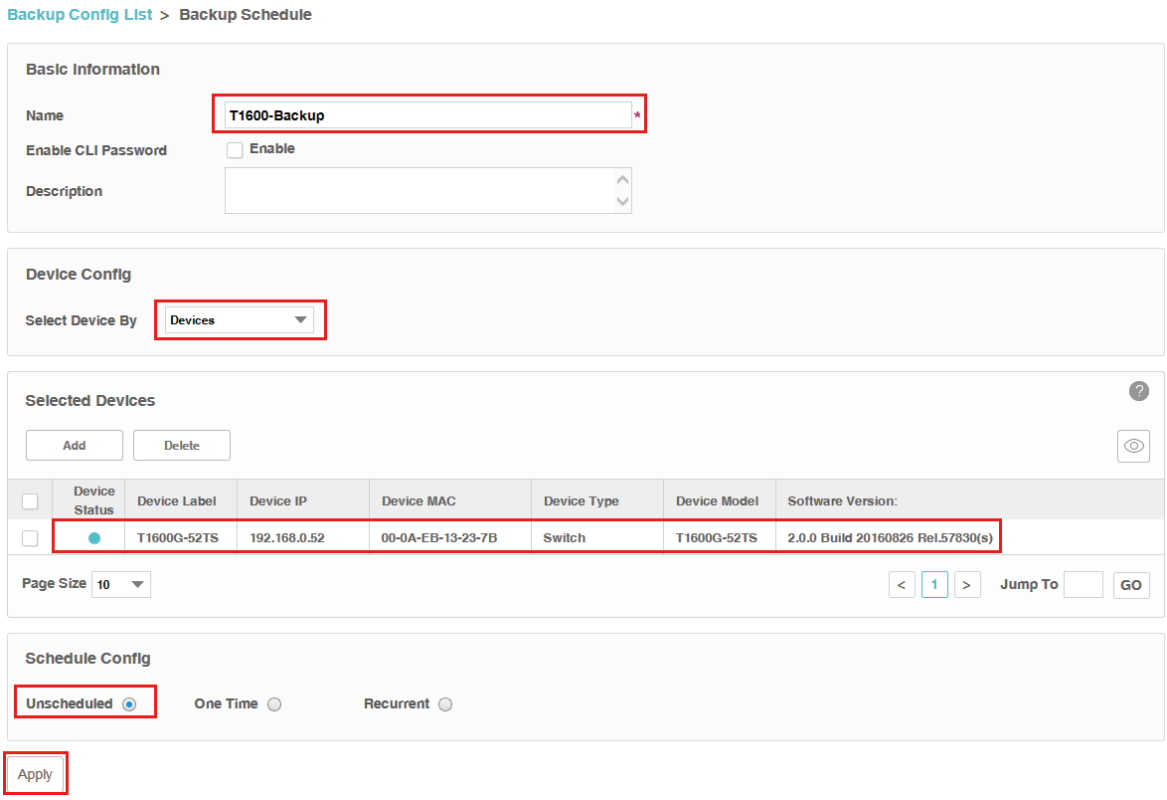
8. Go to **Config > Backup Management > Backup Schedule**. Click **Add** to create a backup schedule.

Figure 6-29 Create a backup schedule



9. Enter the schedule information on this page, and click **Apply** to save this schedule task.

Figure 6-30 Add a backup schedule



Basic Information

Enter **T1600-Backup** in the Name field. The T1600G-52TS has no Enable CLI Password by default.

Device Config

Select Device By **Devices**.

Selected Devices

Click **Add** and select the discovered T1600G-52TS previously.

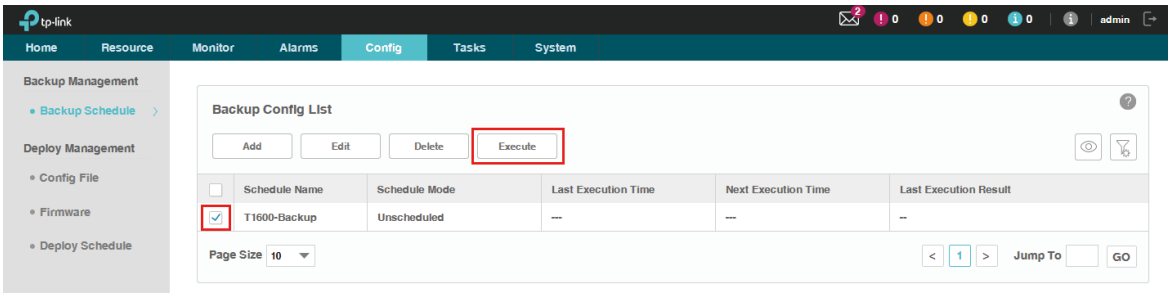
Schedule Config

Select **Unscheduled**.

At last, click **Apply** to save this backup schedule.

10. Select the schedule **T1600-Backup** in the Backup Config List, and click **Execute** to backup T1600G-52TS's configuration file.

Figure 6-31 Execute the backup schedule



11. The backup result is shown in the following window.

Figure 6-32 Backup result

12. You can view the backuped configuration file's information in the Config File list in **Config > Deploy Management > Config file**. You can also locate the backuped configuration file in **\data\tftpDir** in the tpNMS's installation directory.

Figure 6-33 Config File list

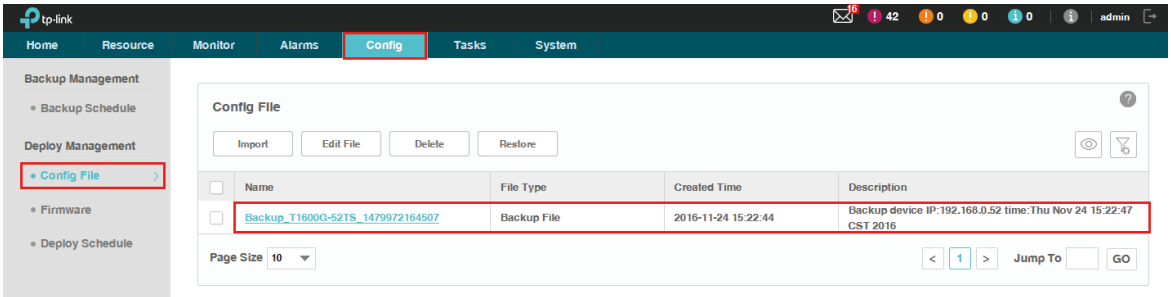
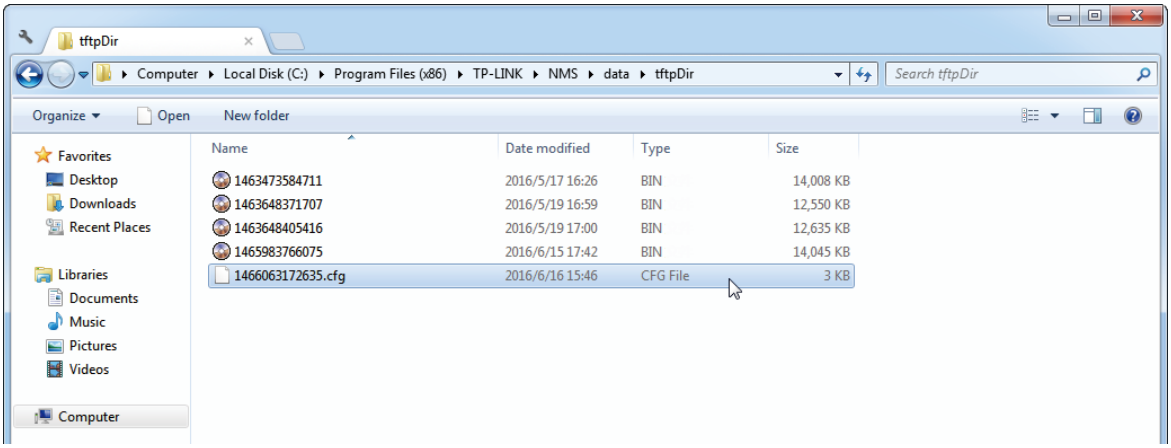


Figure 6-34 Configuration file's location (C:\Program Files (x86)\TP-Link\NMS\data\tftpDir)

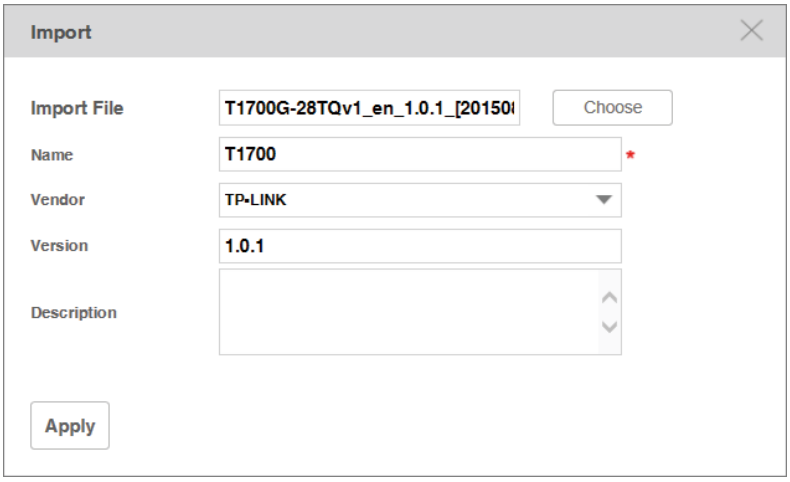


6.6 Example: Upgrade Firmware for Several Devices

The following example shows how to upgrade two TP-Link T1700G-28TQ switches at the same time. The telnet credentials to these two switches are correctly configured already.

1. Go to **Config > Deploy Management > Firmware**. Click **Import Firmware** to upload the firmware file for T1700G-28TQ.

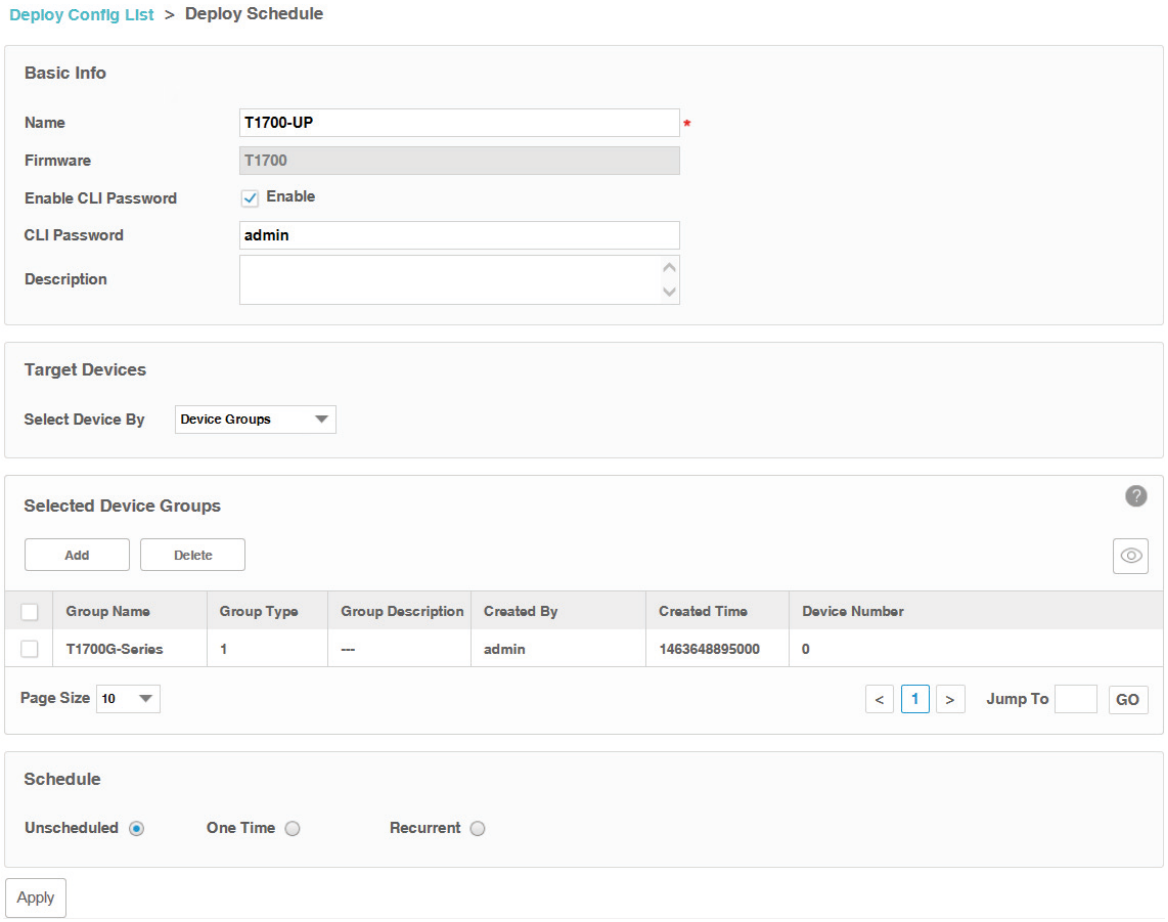
Figure 6-35 Import a firmware file



Name the firmware as **T1700**, enter the version information and select the vendor as **TP-Link**.

2. Select the firmware **T1700** and click **Upgrade** to configure the deploy schedule.

Figure 6-36 Edit T1700_UP upgrade schedule



Basic Info

Name	Enter the name **T1700-Up**.
Firmware	Display the name of the firmware file.
Enable password	Click the checkbox to enter the device's privileged password.
CLI Password	Enter the default password **admin**.

Target Devices

Select Device By	Select the target devices by devices or by device groups. You can choose **Devices** to add the two T1700G-28TQ, or choose **Device Groups** and add the group containing the two T1700G-28TQ. Here we take **Device Groups** as an example.

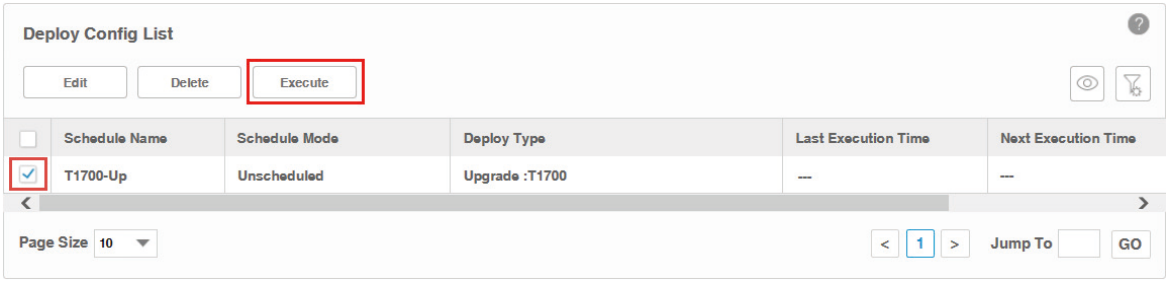
Selected Device Groups	
Add	Click **Add** to add the group **T1700G-Series** which contains the two T1700G-28TQ. The device group is configured on page **Resource > Device Management > Device Groups**.

Schedule	
Unscheduled	Select **Unscheduled**.

Click **Apply** to save the upgrade schedule information.

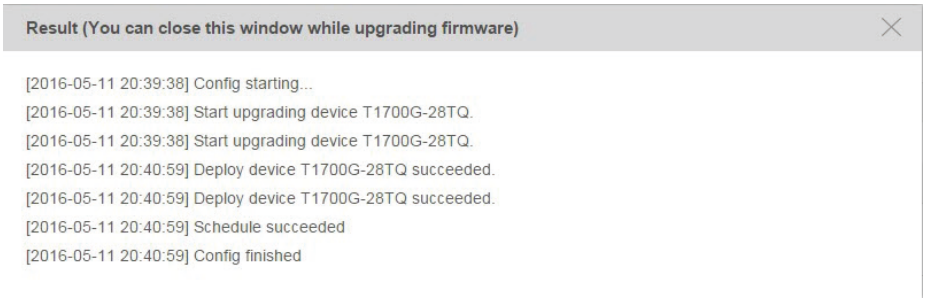
3. Go to **Config > Deploy Management > Deploy Schedule**. Select the upgrade schedule **T1700-Up** and click **Execute** to upgrade the two T1700G-28TQ switches.

Figure 6-37 Execute T1700-Up upgrade schedule



4. Check the result in the result window.

Figure 6-38 Execute T1700-Up result



7 View and Manage Tasks

View and Manage the discovery, backup, restore and upgrade tasks on this page.

This chapter covers the following topics.

- *Enable/Disable the Tasks*
- *Remove the Tasks*
- *View Task Execution Results*

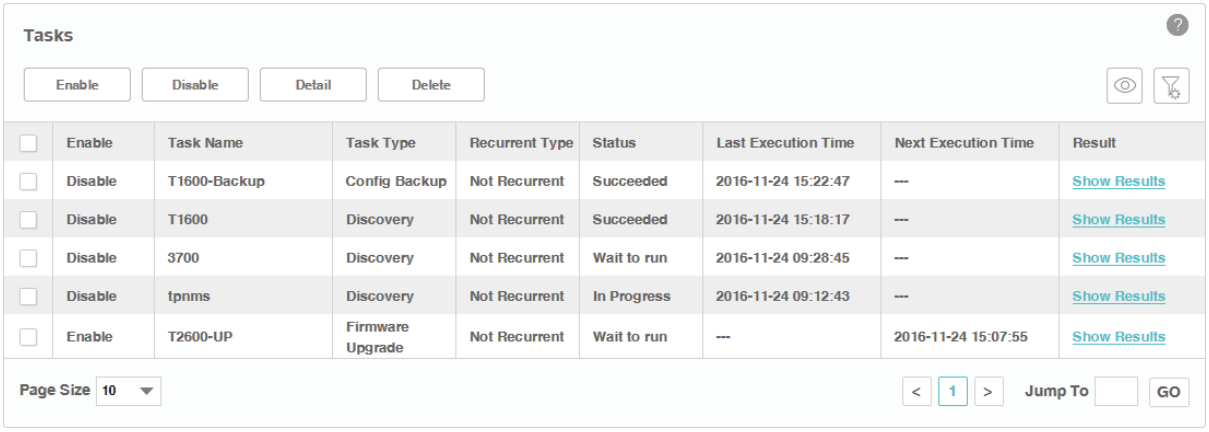
7.1 View and Manage the Tasks

You can view task details and execution results. You can also enable, disable and remove tasks on this page.

The task types include Discovery, Configuration Backup, Configuration Restore and Firmware Upgrade.

Go to **Tasks > Task Management > Tasks**.

Figure 7-1 Task list



7.1.1 View the Tasks

Executed and to-be-executed tasks are displayed in this table.

Enable	Displays the status of the task.
Task Name	Displays the task name.
Task Type	The task type includes: Discovery, Config Backup, Config Restore and Firmware Upgrade.
Recurrent Type	The task recurrent type includes: Not Recurrent, Hourly, Daily, Weekly and monthly.
Status	The execution status of the task, including Succeeded, Failed and Wait to run.
Last Execution Time	Displays the last time when the task was executed.
Next Execution Time	Displays the next time when the task will be executed.
Result	Click **Show Results** to view the detailed running result of the task.

Click the **Detail** button to view the detailed configuration of the selected tasks.

7.1.2 Enable/Disable the Tasks

Click the **Enable/Disable** button to enable/disable the selected tasks. Only tasks in Wait to run status can be enabled or disabled.

7.1.3 Delete the Tasks

Click the **Delete** button to remove the selected tasks from the table.

8 Manage Users

You can manage the users and roles on this section.

- *View and Manage Roles*
- *View and Manage Users*
- *View and Log off Users*

8.1 View and Manage Roles

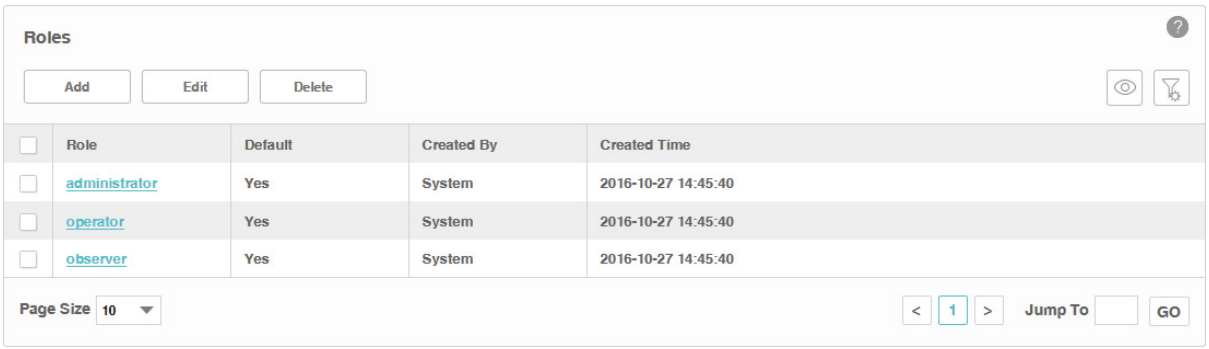
The role is the permission attribute of the user. Uses with different roles have different access permissions to each configuration module of tpNMS (Resource, Monitor, Alarm, Config, Task and System).

tpNMS provides the following default roles:

- Administrator. The administrator user can view and modify all the modules of tpNMS.
- Operator. The operator user can view all the modules, and can modify all the modules except the System Module.
- Observer. The observer user can only view all the modules.

Go to **System > User Management > Roles**.

Figure 8-1 View roles



- *View Roles*
- *Add a Role*
- *Modify a Role*
- *Delete a Role*

8.1.1 View Roles

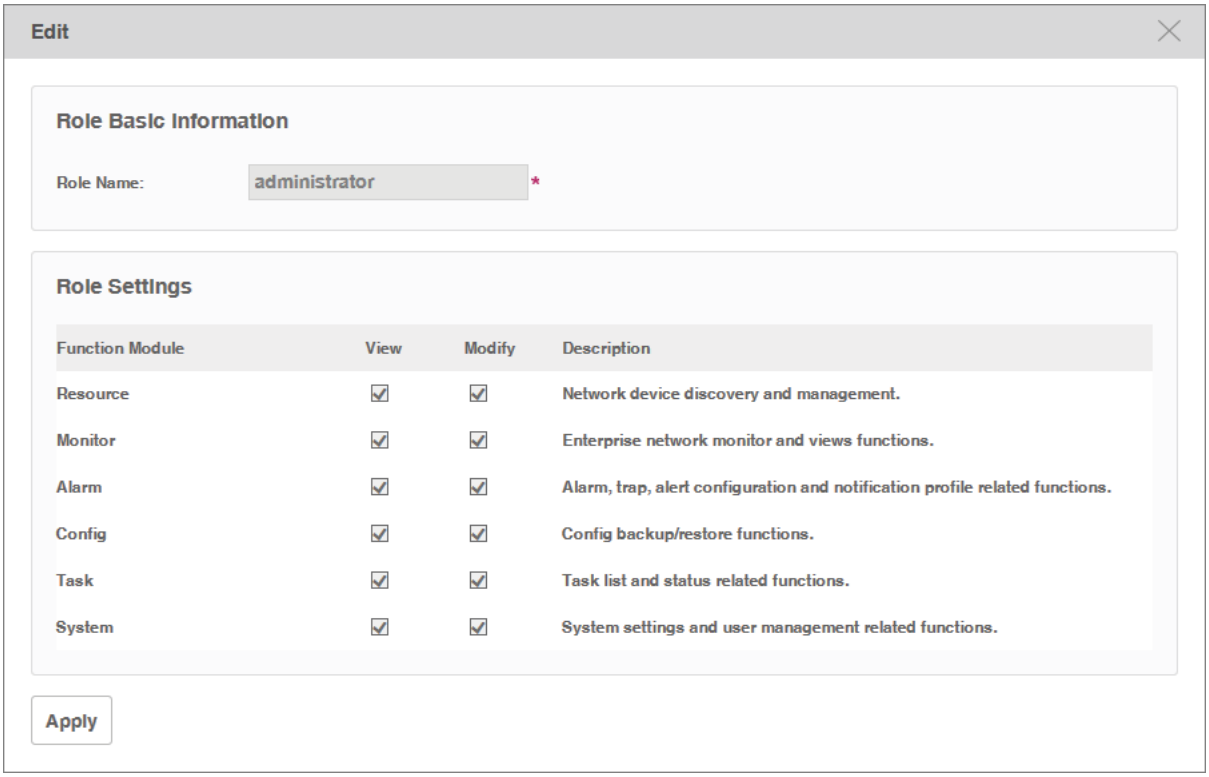
Go to **System > User Management > Roles**.

The default 3 roles are displayed in the role table.

Role	Displays the name of the role.
Default	Whether the role is a system default role.
Created By	The Creator of the role.
Created Time	The created time of the role.

Click the role name to view its detailed privilege to each module.

Figure 8-2 Role privilege

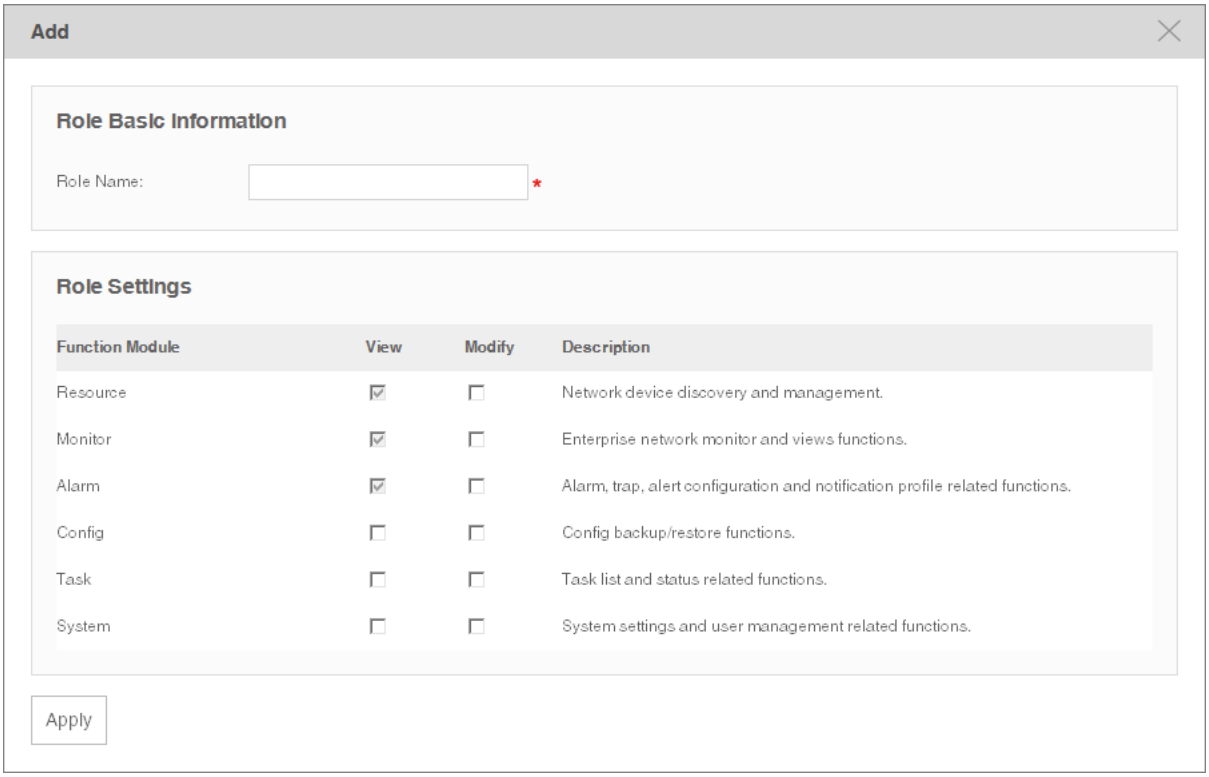


8.1.2 Add a Role

Go to **System > User Management > Roles**.

Click **Add** to create a new role with customized privileges.

Figure 8-3 Create a role



Enter the role name and select the checkboxes to specify the role's access privilege to each module.

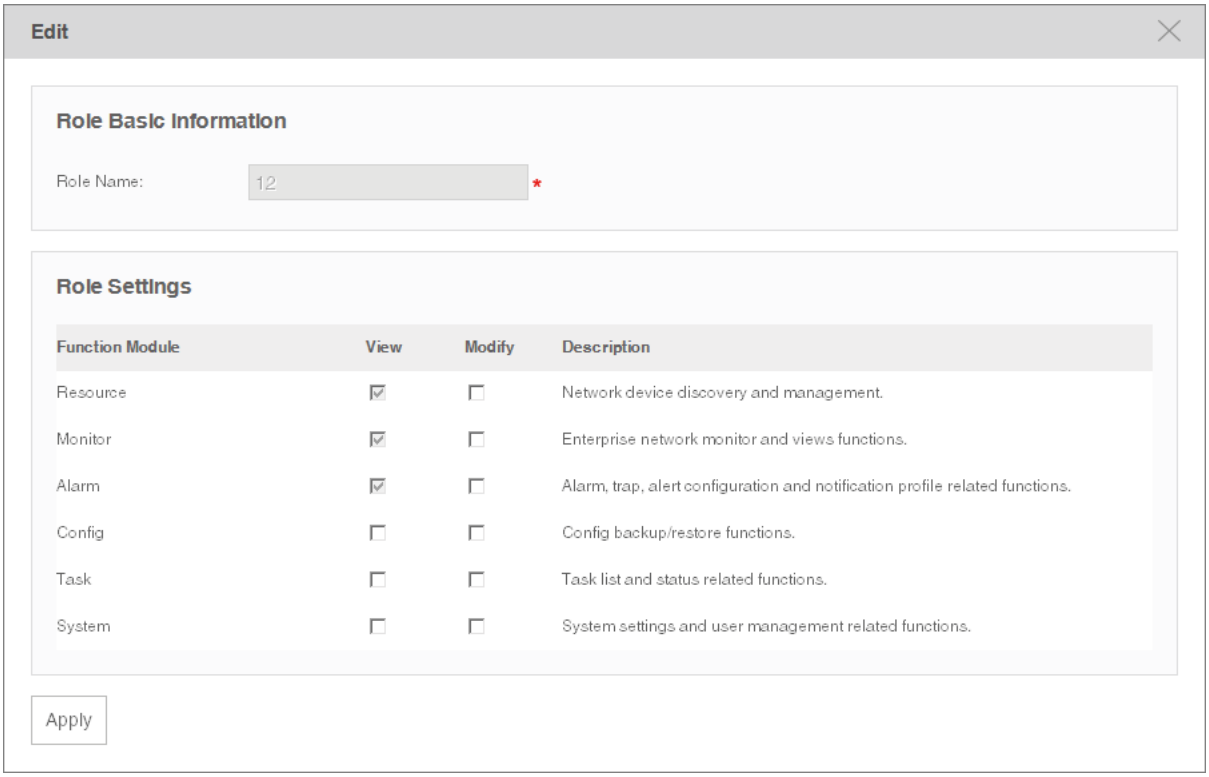
Click **Apply** to save the role's configuration.

8.1.3 Modify a Role

Go to **System > User Management > Roles**.

Click **Edit** to customize the role's privileges.

Figure 8-4 Modify a role



Select or deselect the checkboxes to specify the role's access privilege to each module.

Note:

The system default roles cannot be edited.

8.1.4 Delete a Role

Go to **System > User Management > Roles**.

Click **Delete** to remove the selected roles.

Note:

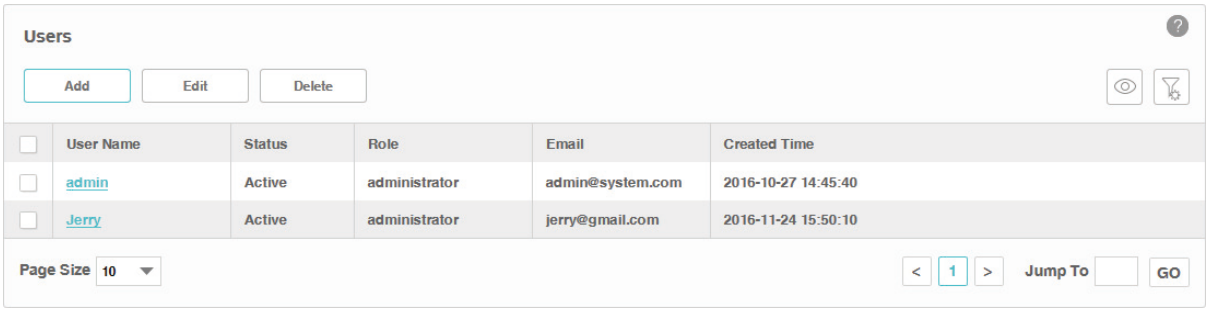
The system default roles cannot be deleted.

8.2 View and Manage Users

You can view and manage the users of tpNMS on this page.

Go to **System > User Management > Users**.

Figure 8-5 User list



- *View Users*
- *Add a User*
- *Modify a User*
- *Delete a User*

8.2.1 View Users

Go to **System > User Management > Users**.

View the users in the user table.

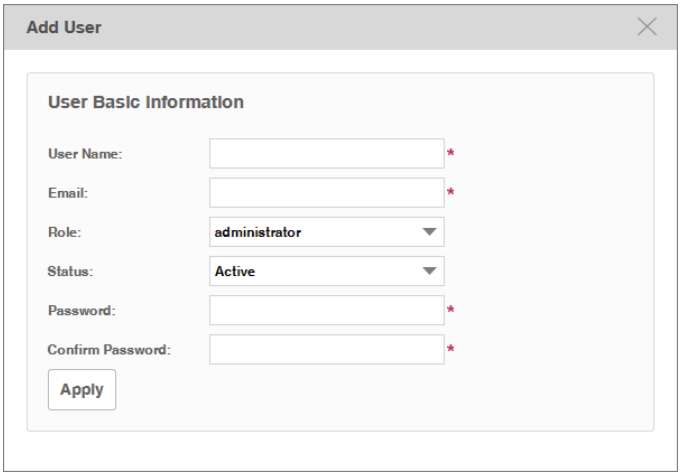
User Name	Displays the name of the user.
Status	Displays the status of the user.
Role	Displays the role of the user. The role defines the privilege of the user.
Email	Displays the user's email address.
Created Time	The created time of the user.

8.2.2 Add a User

Go to **System > User Management > Users**.

Click **Add** to add a user to the user table. Enter the user's basic information and click **Apply**.

Figure 8-6 Add a user



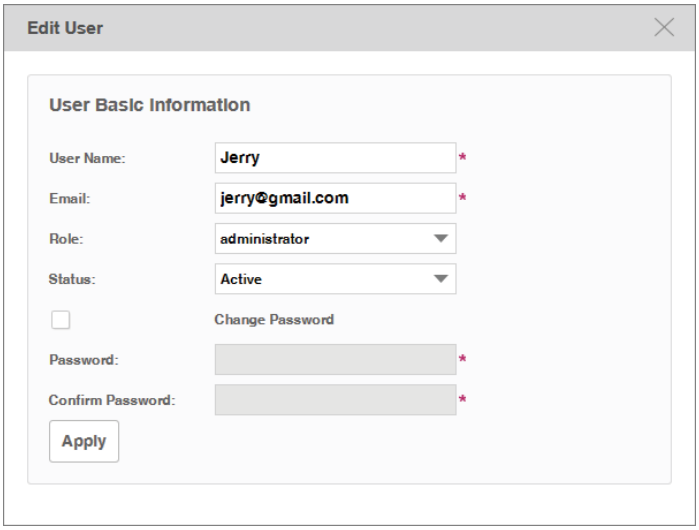
User Name	Enter the name of the user. The user name is case-sensitive.
Email	Enter the user's email address.
Role	Select the role of the user. The role defines the privilege of the user.
Status	Specify the status of the user as active or inactive.
Password	Enter the password for this user.
Confirm Password	Enter the password again to confirm.

8.2.3 Modify a User

Go to **System > User Management > Users**.

Select a user and click **Edit** to modify a user's configuration and click **Apply**.

Figure 8-7 Modify a user



User Name	Enter the name of the user. The user name is case-sensitive.
Email	Enter the user's email address.
Role	Select the role of the user. The role defines the privilege of the user.
Status	Specify the status of the user as active or inactive.
Change Password	Select the checkbox to modify the user's password.
Password	Enter the password for this user.
Confirm Password	Enter the password again to confirm.

8.2.4 Delete a User

Go to **System > User Management > Users**.

Click **Delete** to remove the selected users.

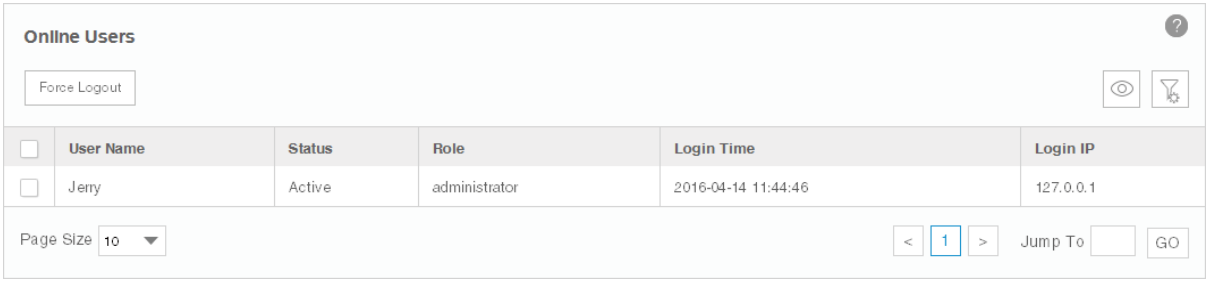
Note:
The system default users cannot be deleted.

8.3 View and Log off Users

You can view the users who are currently online and log them off. Only the administrator-role user have the privilege to log off the other online users.

Go to **System > User Management > Online Users**.

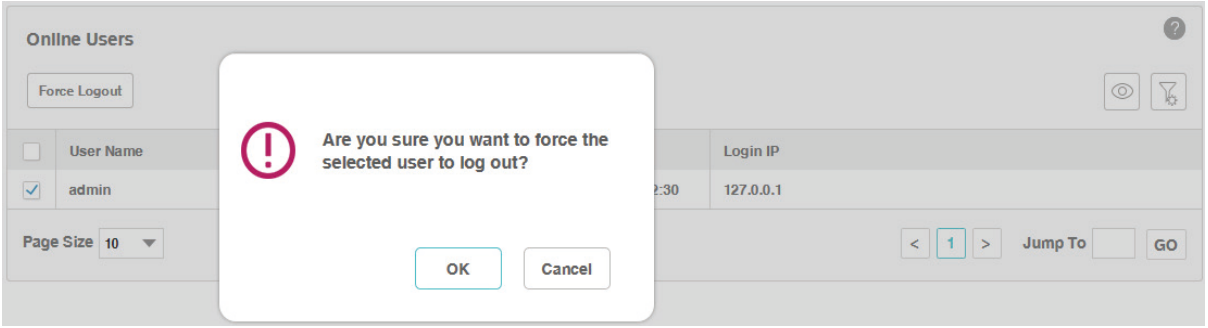
Figure 8-8 Online user list



The currently online users are displayed in this table.

1. Select one or more users and click **Force Logout**.
2. Click **OK** in the pop-up confirm window. The selected user will be forced to log off.

Figure 8-9 Log out a user



9 System and Global Settings

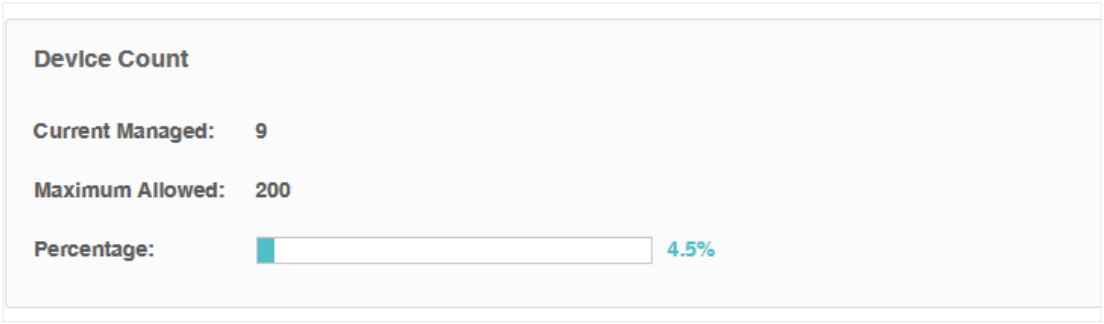
You can configure tpNMS system and global settings in this section.

9.1 Device Count

You can view the number of devices being managed currently. tpNMS can manage up to 200 devices simultaneously.

Go to **System > Device Count > Device Count** to view the managed device count.

Figure 9-1 View device count



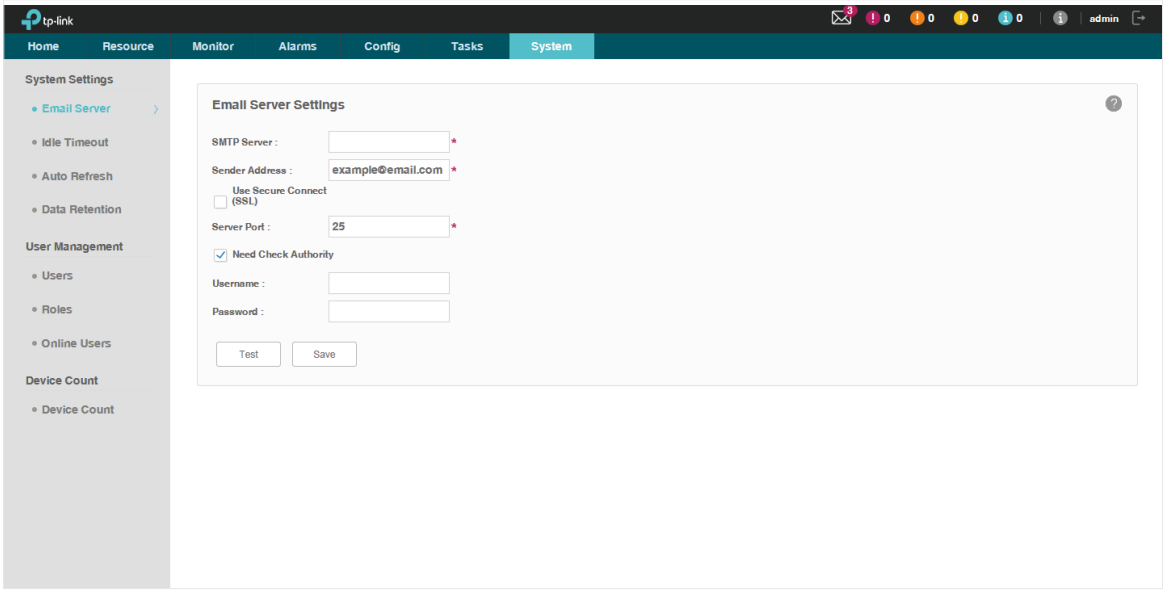
Current Managed	Displayed the number of devices currently managed by tpNMS.
Maximum Allowed	The maximum devices tpNMS can managed simultaneously. By default it's 200.
Percentage	The ratio of managed devices to total allowed device.

9.2 Configure Email Server

Configure the sender email information for sending notification emails when the configured alarms are triggered.

1. Go to **System > System Settings > Email Server**.

Figure 9-2 Configure email server settings



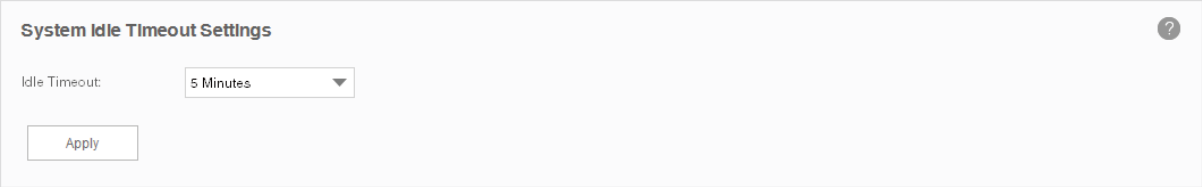
2. Enter your SMTP server address in the **SMTP Server** field. For example: smtp.gmail.com.
3. Enter your email address in the **Sender Address** field. For example: jerry@gmail.com.
4. If you want to encrypt the data sent from the server, select the **Use Secure Connect (SSL)** check box.
5. Enter your SMTP server port in the **Server Port** field.
6. If your SMTP server requires authentication, select the **Need Check Authority** check box and enter your user name and password for your email account.
7. Click the **Test** button to verify your email server settings.
8. Click the **Save** button to save your email server settings.

9.3 Configure Idle Timeout

Configure the idle timeout on this page. If the user has no operations on tpNMS within the timeout period, the application will log the user out automatically. The default idle timeout is 5 minutes.

Go to **System > System Settings > Idle Timeout**.

Figure 9-3 Configure the idle timeout



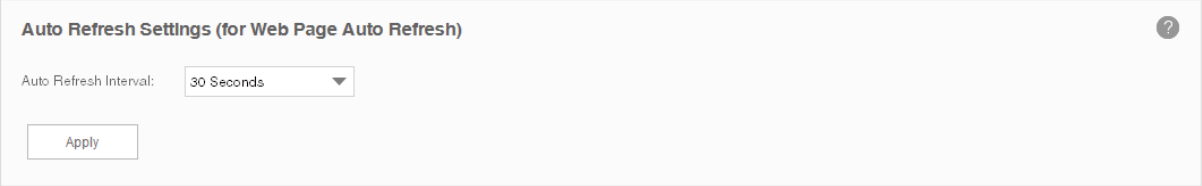
Select the idle timeout and click **Apply** to save your configuration.

9.4 Configure Auto Refresh Interval

Configure the frequency that tpNMS refreshes the browser screen for the web management interface. By default the web refreshes every 30 seconds.

Go to **System > System Settings > Auto Refresh.**

Figure 9-4 Configure the refresh interval



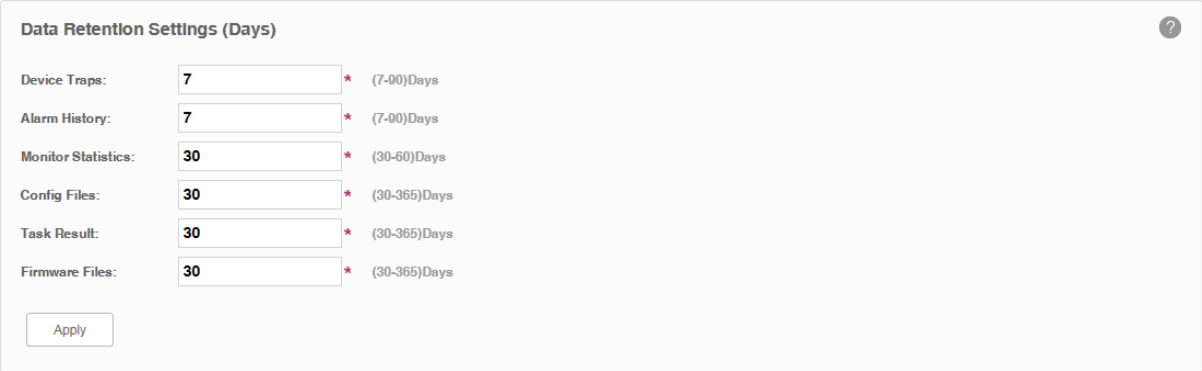
Select the auto refresh interval and click **Apply** to save your configuration.

9.5 Configure Data Retention

Configure how long tpNMS retains your network data. The longer the data are retained, the more disk space is required on the tpNMS server. Different types of information can be specified with different data retention periods.

Go to **System > System Settings > Data Retention.**

Figure 9-5 Configure the data retention period



Enter the data retention period for these types of data and click **Apply** to save your configuration.

9.6 Icons in the Upper-Right Region

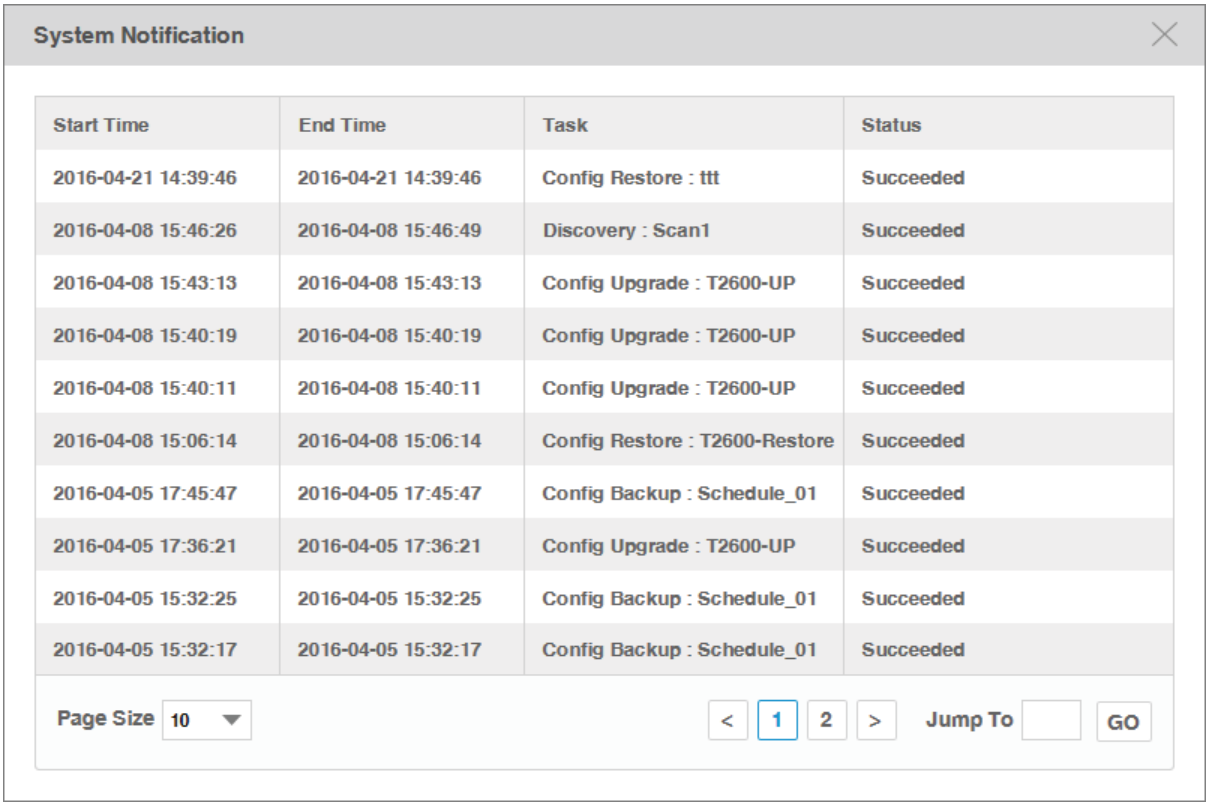
The following introduces the shortcut icons on the upper-right area of tpNMS.

- *Notification Messages*
- *Current Alarms*
- *System Information*
- *Current Account*
- *Log out*

9.6.1 Notification Messages

Click the envelope icon to view the system notifications. The application generates a notification when a backup/restore/upgrade task is completed. The number in the red-colored circle on the top of the envelope icon indicates the number of the newly generated notifications.

Figure 9-6 System notifications



9.6.2 Current Alarms

Four shortcut icons represent the current four level alarms. The color represents the severity, while red represents the highest level severity and blue represents the lowest severity. The numbers beside these icons represent each alarm's current quantity.

- Urgent (Red)
- Serious (Orange)
- Normal (Yellow)
- Hint (Blue)

Click the alarm icon to view the alarm's detail information.

9.6.3 System Information

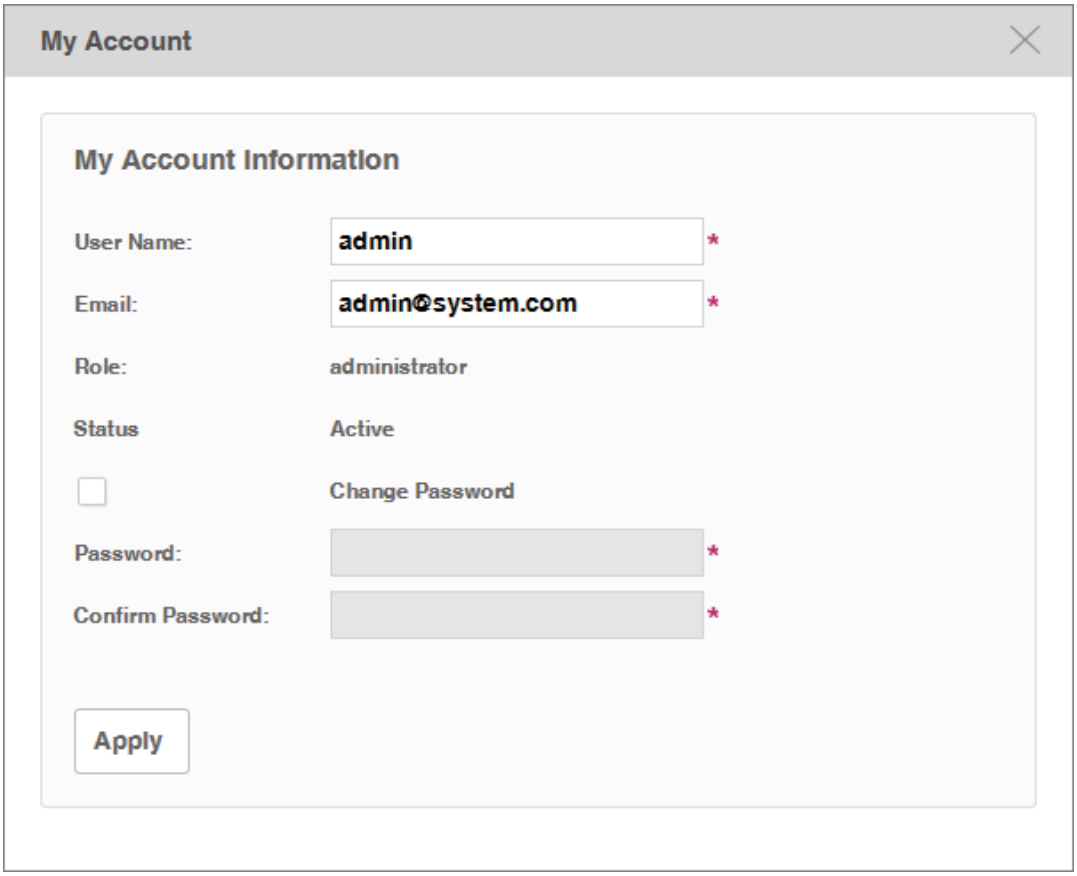
Click the icon to view tpNMS's version and copyright information.

Figure 9-7 Version and copyright

9.6.4 Current Account

Click the user name to view and edit the information of the current user.

Figure 9-8 Current user



9.6.5 Log out

Click the icon to log out tpNMS.