

Kyvision User Manual



Kyland Technology Co., Ltd.

Publication Date: Jun. 2013

Version: V4.1

FAX: +86-10-88796678

Website: <http://www.kyland.com>

E-mail: support@kyland.com

Disclaimer:

Kyland Technology Co., Ltd. tries to keep the content of this manual as accurate and as updated as possible. This document is not guaranteed to be error-free, and we reserve the right to amend it without notice to users.

Copyright © 2013 Kyland Technology Co., Ltd.

All rights reserved.

No part of this documentation may be excerpted, reproduced, translated, annotated or duplicated, in any form or by any means without the prior written permission of KYLAND Corporation.

Contents

Preface	1
1 Introduction.....	3
1.1 Overview	3
1.2 Structure.....	3
1.3 Features.....	4
2 Installation	6
2.1 Installation Mode	6
2.2 Configuration Requirements.....	6
2.3 Installation Steps	6
2.4 Reparative Installation.....	12
2.5 Uninstall	13
3 Login and Logout.....	15
3.1 Login in Server Mode	15
3.2 Login in Client Mode	16
3.3 Logout from the Client.....	17
3.4 Logout from the Server	17
4 User Interface (UI)	19
4.1 Menu Bar	20
4.2 Toolbar	22
4.3 Alarm Statistics Bar	23
4.4 Navigation Tree	24
4.5 Topology Toolbar	25
4.6 Topology Switch Area.....	28
4.7 Network Topology Area	28
4.8 Information Display Area	28
5 Topology Management	30
5.1 Overview	30

5.2	Auto-Topology	30
5.2.1	Specifying an IP Address	30
5.2.2	Specifying a Network Segment.....	31
5.3	Creating/Deleting a Device	33
5.4	Creating/Viewing/Deleting a Link	34
5.5	Subnet Topology Management.....	35
5.6	Topology Operations	36
6	Device Management.....	38
6.1	Device Local Information.....	38
6.2	Device Information	38
6.3	Device Panel.....	39
6.4	SNMP Configuration	40
6.5	Device State Information	42
6.6	Device Running State.....	43
6.7	Ping Device	44
6.8	Link Telnet.....	46
6.9	Start Web	47
6.10	All Alarms	48
6.11	Device Property Configuration	48
6.12	Maintenance	49
6.12.1	FTP Server Configuration	49
6.12.2	Export Device Configuration	51
6.12.3	Import Device Configuration	52
6.12.4	Upgrade Device Software.....	54
6.12.5	EMS Data Backup	54
6.12.6	EMS Data Recovery	59
6.12.7	EMS Data Cleaning	62
7	Rights Management.....	67
7.1	User Rights Management.....	67
7.1.1	User Management.....	67

7.2 Subnet Rights Management.....	71
7.3 Operation Rights Management	72
8 Alarm Management	73
8.1 Overview	73
8.2 Alarm Levels and Categories	73
8.3 Alarm Modes	75
8.4 Alarm List	75
8.4.1 Alarm Level-based Alarm List	75
8.4.2 Alarm Status-based Alarm List.....	76
8.5 Alarm Query and Export.....	78
8.6 Alarm Filtering.....	81
8.7 Alarm Acknowledgement.....	82
8.8 Alarm Notification by Email	82
9 Log Management.....	86
Appendix: Acronyms	89

Preface

This manual describes the installation and uninstall of Kyvision network management software. It also details the management and monitoring features of Kyvision based on Kyland switches.

Conventions in the manual

1. Text format conventions

Format	Explanation
< >	The content in < > is button name. For example, click <Apply> button.
[]	The content in [] is window name or menu name. For example, click [File] menu item.
→	Multi-level menus are separated by "→". For example, Start → All Programs → Accessories. Click [Start] menu, click the sub menu [All programs], then click the submenu [Accessories].
/	Use / to separate two or more options, and select one from all options. For example "Addition/Deduction" means addition or deduction.
~	It means a range. For example, "1~255" means the range from 1 to 255.

2. Symbol conventions

Symbol	Explanation
 Caution	The matters need attention during the operation and configuration, and it is supplement to the operation description
 Note	Necessary explanations to the operation description

**Warning**

The matters that call for special attention. Incorrect operation might cause data loss or damage to devices

Document Obtainment

You can obtain the documents from:

- CD or manual delivered with the device
- Kyland website: www.kyland.com

1 Introduction

1.1 Overview

Kyvision is the software developed by Kyland for managing Kyland switches and monitoring all SNMP supported devices. It can provide overall running information about the entire network, automatically identify network devices, display the current running status of devices in real time, automatically display and analyze network faults, automatically record operation and running logs, and maintain and upgrade network devices with high efficiency.

Kyvision provides user-friendly interface, which automatically displays the actual network connections and structure. The graphical design enables easy and intuitive operations. The complete full-simulation device panel, interface color changes, sound prompts, and device color changes facilitate your fault locating and diagnosis.

1.2 Structure

Kyvision employs the Client/Server structure. The server and client can be located on different PCs, as shown in Figure 1.

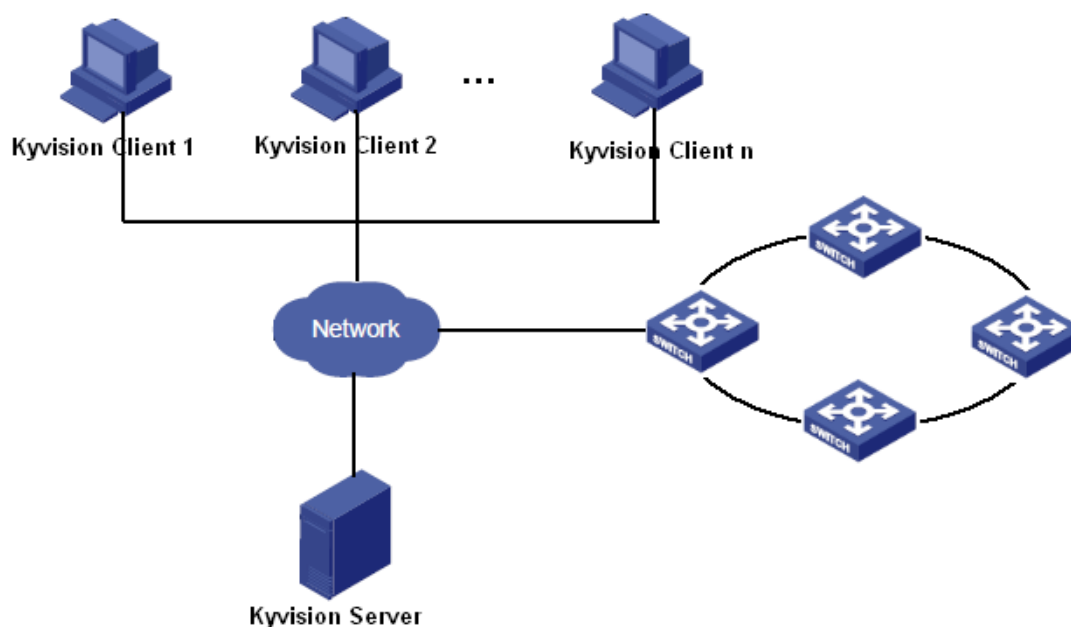


Figure 1 Kyvision System Structure

**Note:**

- In a Client/Server structure, multiple clients and the server are connected through a LAN or WAN. Users operate clients and share the same data stored on the server.
- The server communicates with and manages devices, while clients display and provide operation interfaces for users.

1.3 Features

Kyvision suits the needs of various customers by offering the following features:

- User-friendly and easy-to-use interface;
- Capable of managing multiple network segments;
- Intuitive and vivid HD images;
- High-performance EMS, supporting 10 users online at the same time and monitoring up to 1000 devices;
- Automatically discovering and displaying Kyland network devices through SNMP;
- Automatically mapping the link status of entities through LLDP;
- Automatically discovering and refreshing topology, supporting manual topology drawing;
- Recording operation logs and running logs, available for query and export;
- Detecting the status of Kyland devices in real time and notifying users of an alarm upon the occurrence.
- Notification by alarm bell or alarm email and acknowledgement mechanism;
- Alarm filtering to free users from irrelevant alarms;
- Historical alarm query and query condition setting. Query results can be exported in reports.
- Displaying devices and links with alarms in different colors.
- Socket interface for secondary development;

- Built-in FTP server, supporting configuration file upload and download in batches and software upgrade;
- Interface locking and unlocking, preventing illegitimate users.
- ...

2 Installation

2.1 Installation Mode

Kyvision can be installed in server&client or client mode. In server&client mode, both server and client programs are installed, while only the client program is installed in client mode.

2.2 Configuration Requirements

1. Software Requirements

OS: Windows XP/WIN 7/WIN2003 Server/ WIN2000 Server

2. Hardware Requirements

Table 1 Hardware Requirements

Item	Windows Server	Windows Client
Processor	Pentium 4	Pentium 4
CPU	3GHz	3GHz
Memory	1GB	512MB
HDD	40GB	20GB
CD-ROM	48X	48X
Network adapter	100Mbps	100Mbps
Sound card	Configured	Configured
Display	Resolution $\geq 1024*768$	Resolution $\geq 1024*768$

3. Browser Requirements

IE6.0 or a later version

2.3 Installation Steps

1.Insert the Kyvision software CD into the CD-ROM driver.

2.Double-click the setup file in the CD, for example, Kyvision_R3.2.18.exe.

The following dialog box is displayed. Select your preferred language (Chinese

or English). Click OK.



Figure 2 Language Selection

3.The following page is displayed. Click <Next>.

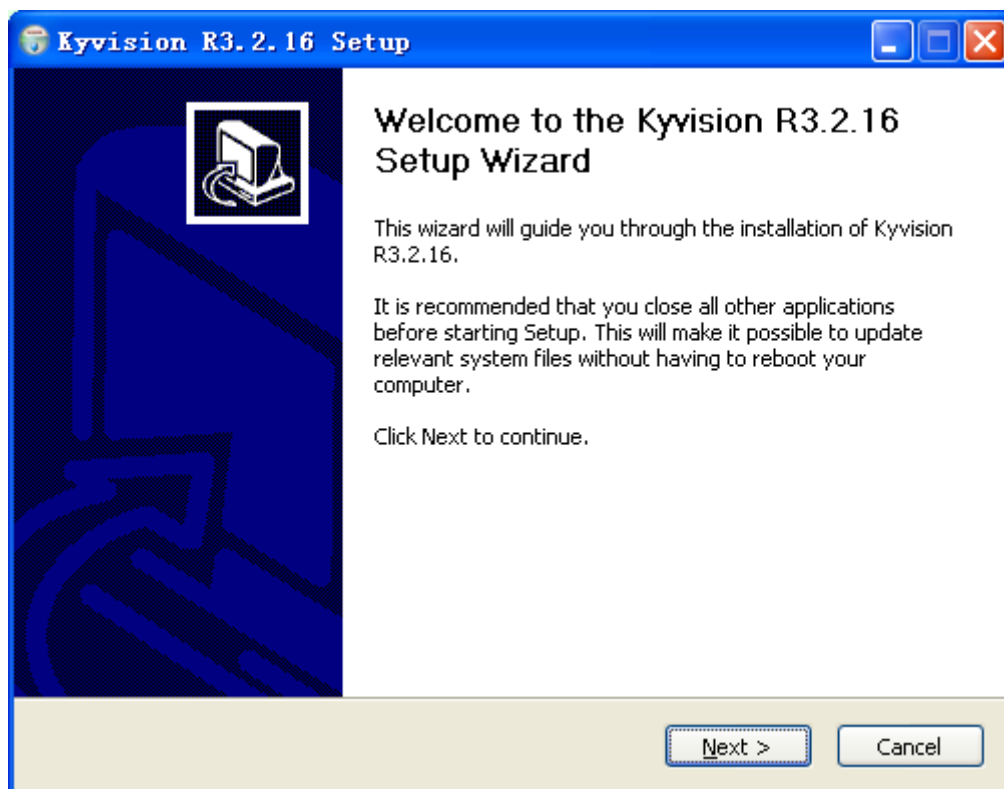


Figure 3 Installation Wizard

4.Select the installation mode, server&client (as shown in Figure 4) or client mode (as shown in Figure 5). Click <Next>.

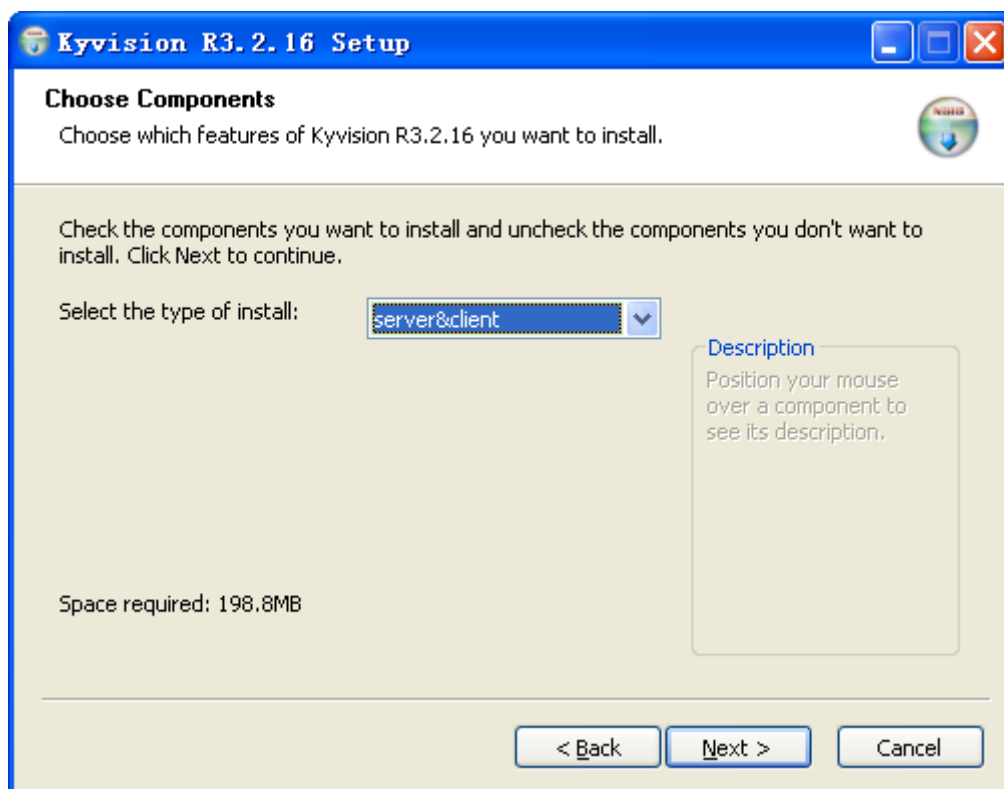


Figure 4 Server Components

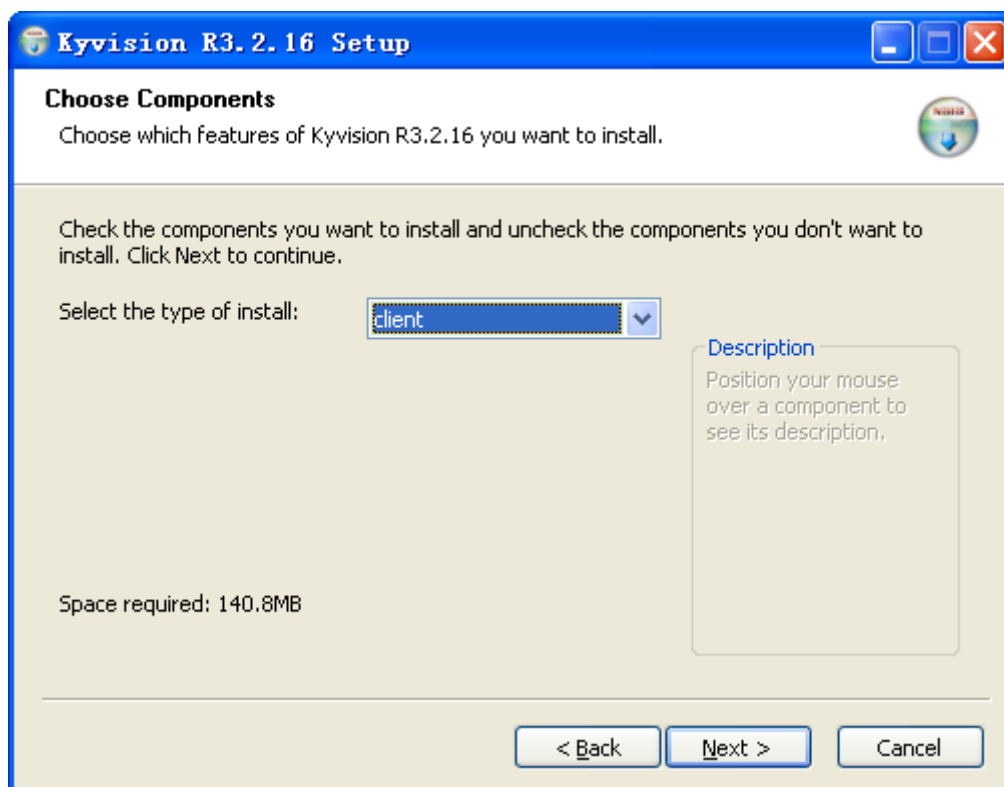


Figure 5 Client Components

5. Select the installation location, as shown in Figure 6. The default location is C:\Kyvision. If you want to select another location, you can enter the

installation path and file name in the text box or click <Browse> to specify the location. Then click <Next>.

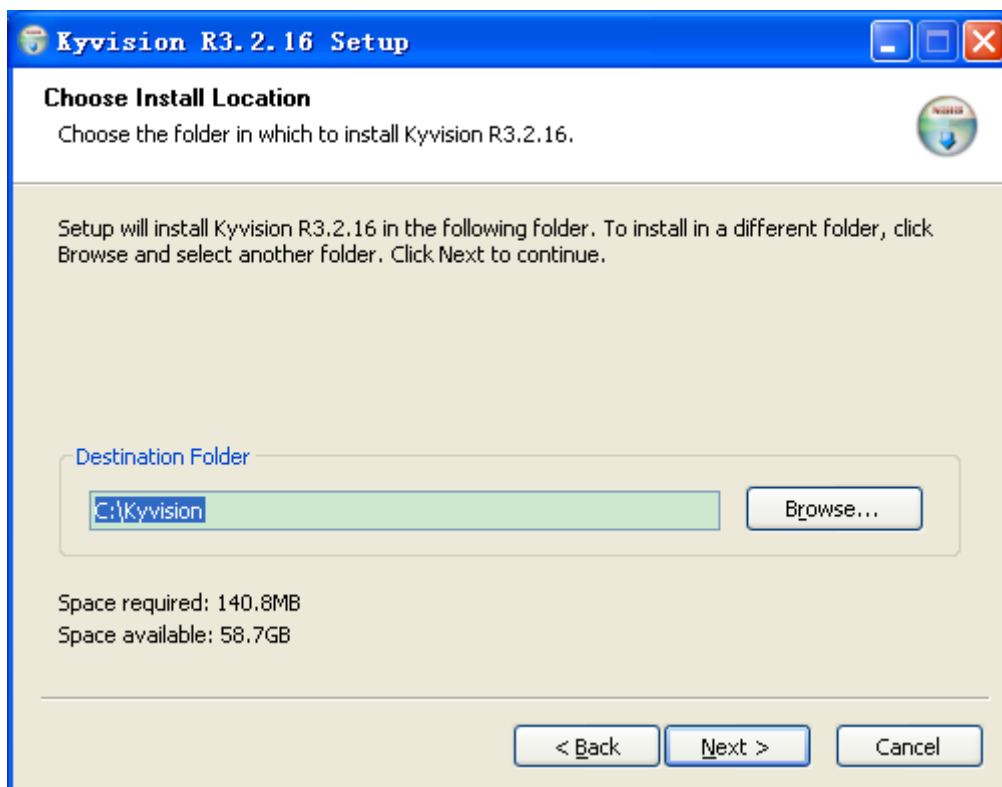


Figure 6 Selecting an Installation Location

6. Select a Start Menu folder. The default folder is Kyvision. You can enter a name in the text box to create a folder. Click <Install>, as shown in Figure 7.

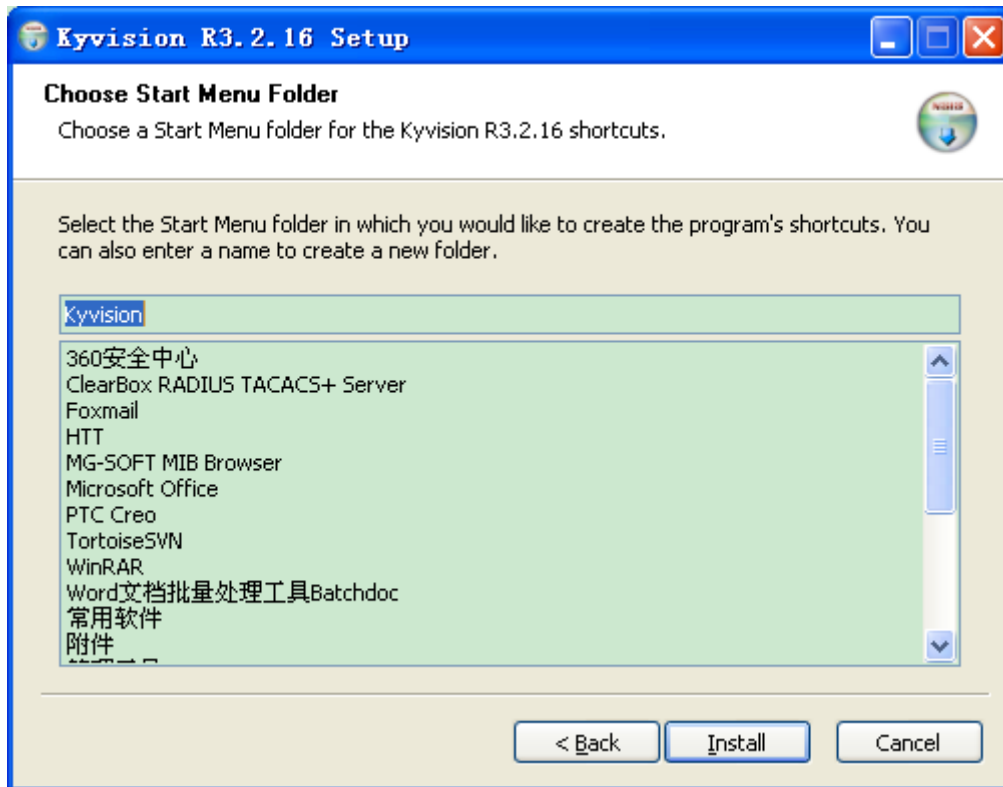


Figure 7 Selecting a Start Menu Folder

7. The installation process is displayed in the progress bar, as shown in Figure 8.

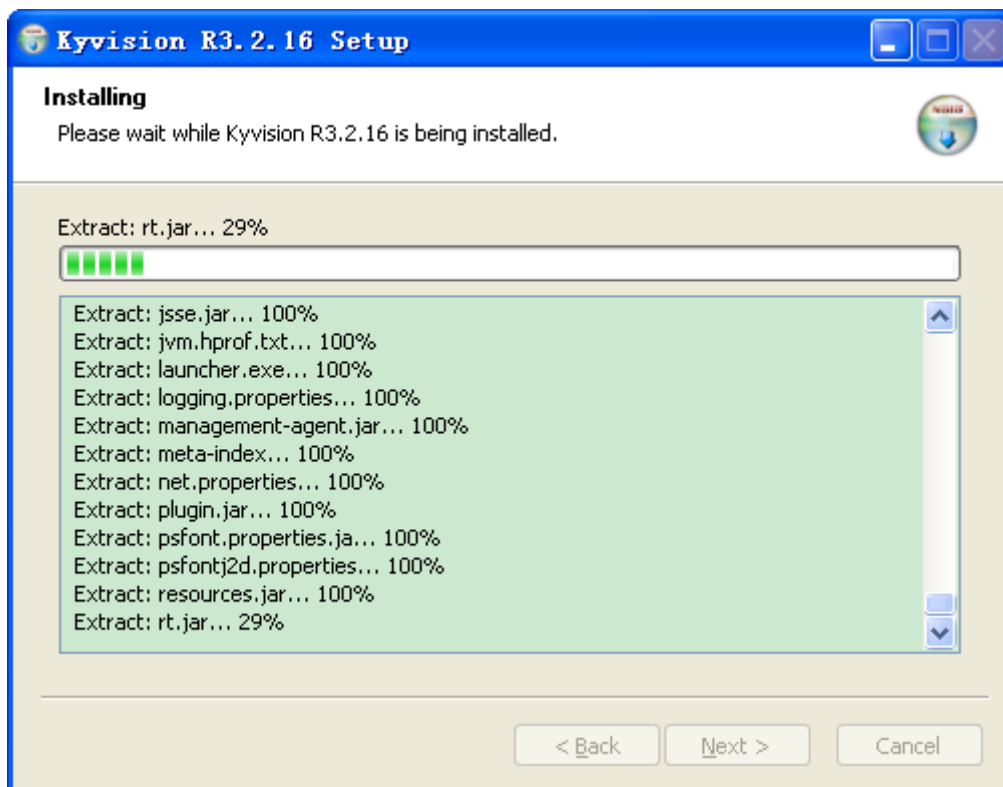


Figure 8 Installation Process

8.If you select the client mode, set the IP address of the server, as shown in Figure 9. Click <Next>. The IP address confirming dialog box is displayed, as shown in Figure 10. Click <Yes>.

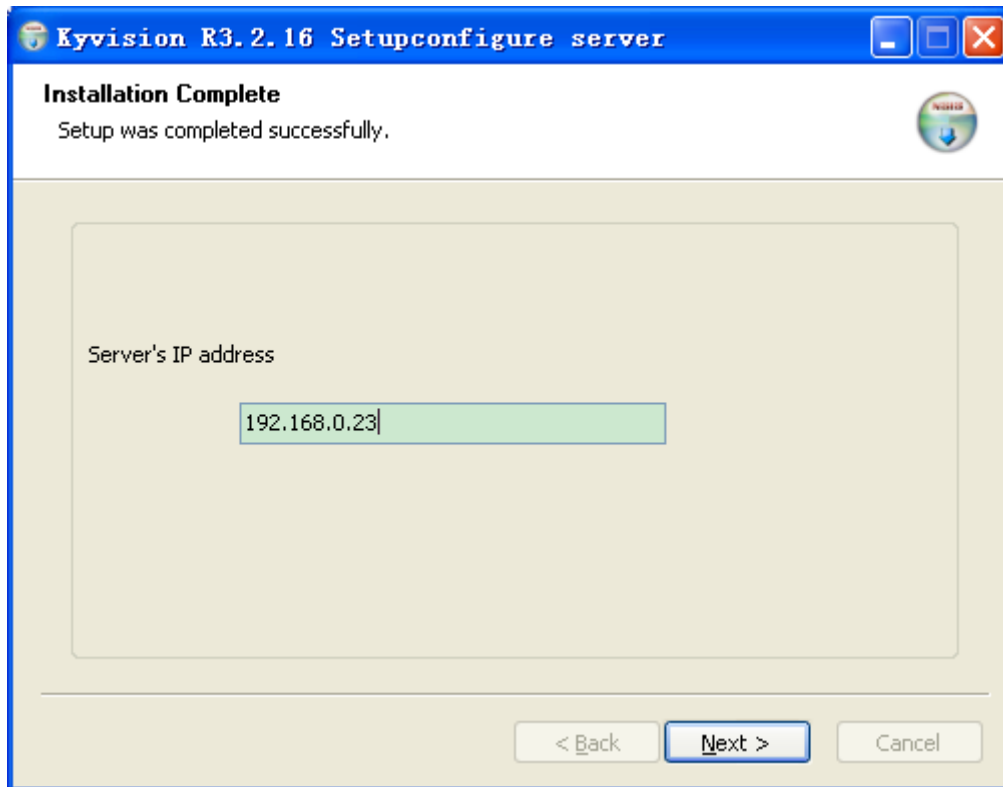


Figure 9 Setting the IP Address

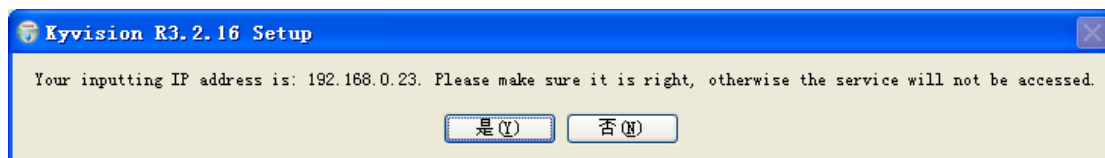


Figure 10 Confirming the IP Address



Caution:

The specified server can communicate with the client properly.

9.The installation is completed, as shown in Figure 11. Click <Finish>.

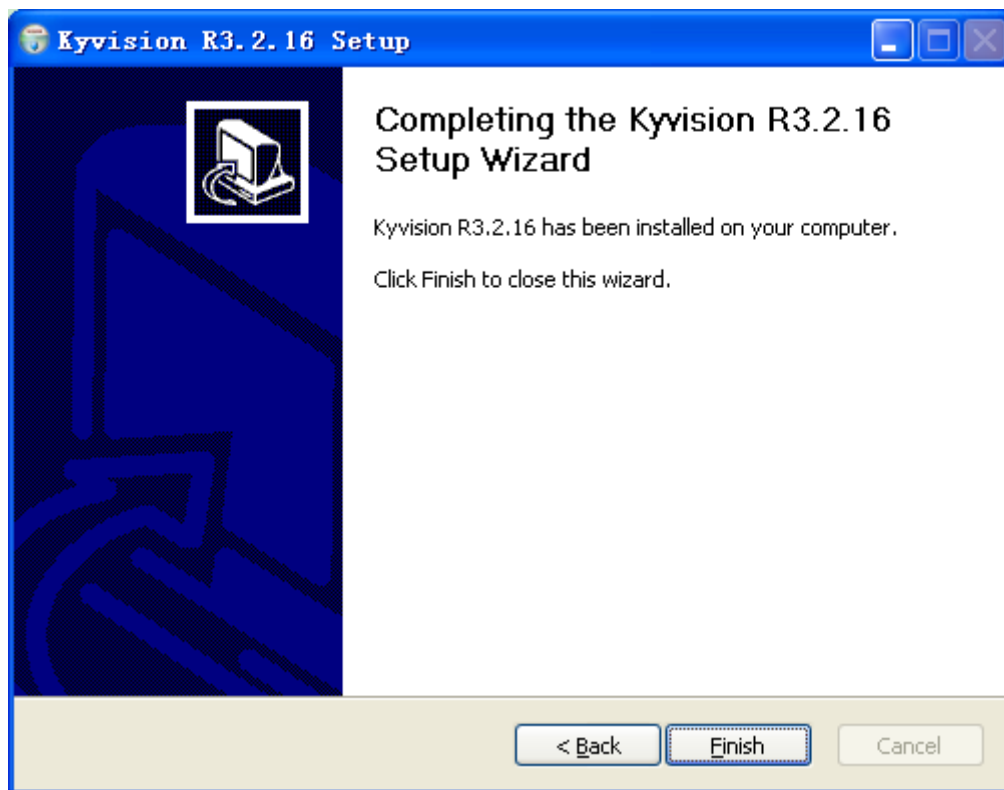


Figure 11 Completing Installation

**Note:**

During the installation process, you can click <Cancel> to stop the installation or <Back> to return to the previous page.

2.4 Reporative Installation

If Kyvision is already installed on a PC, the following page is displayed. Click <Next> until the installation process is completed.

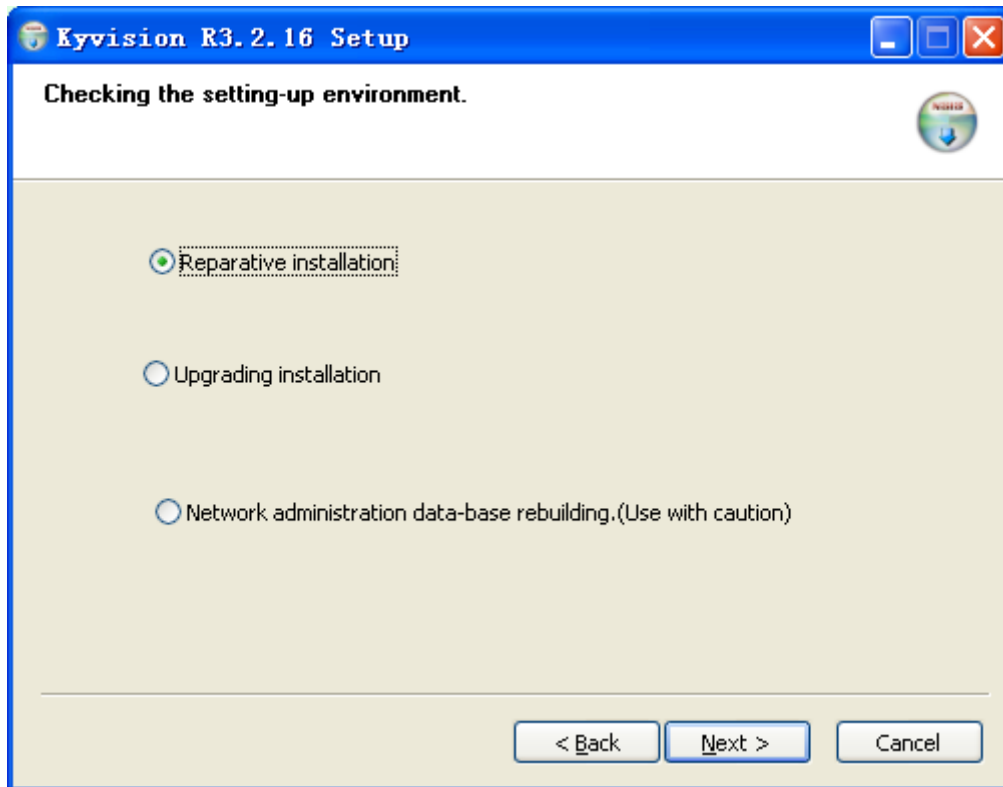


Figure 12 Reparative Installation

Reparative installation: repair the existing version.

Upgrading installation: keep original data and upgrade Kyvision.

Network administration data-base rebuilding: rebuild the database and install Kyvision.



Note:

- If you select reparative installation, try to adopt the original installation mode.
- Network administration data-base rebuilding is not recommended.

2.5 Uninstall

1.Close Kyvision server and client.

2.Click Start → All Programs → Kyvision → Uninstall. The following dialog box is displayed. Click <Yes> to uninstall Kyvision.

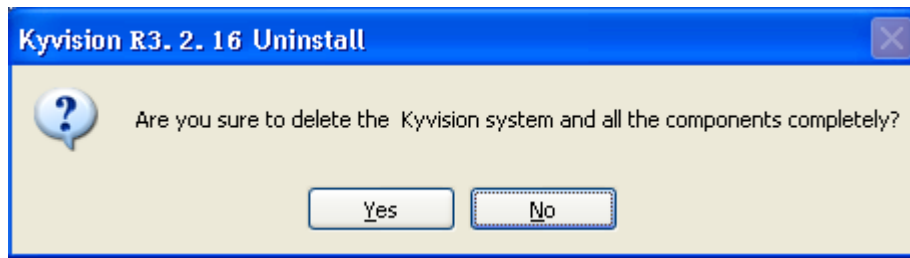


Figure 13 Uninstall

3.The uninstall process is displayed in the progress bar, as shown in Figure 14.

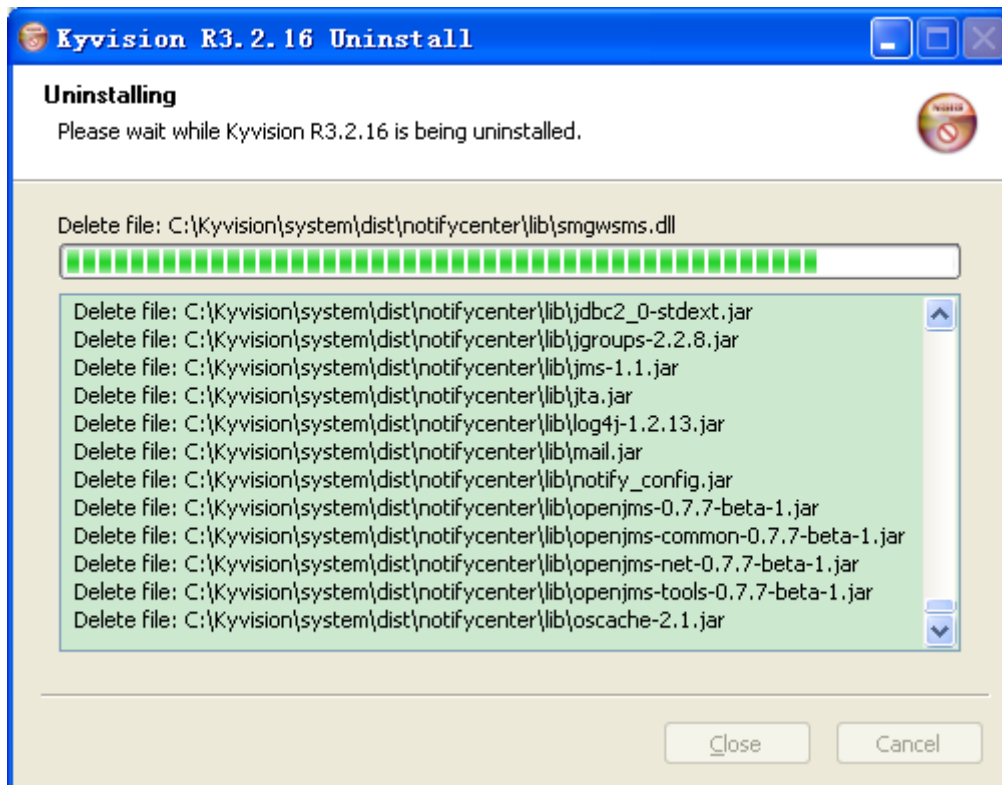


Figure 14 Uninstall Process

4.Uninstall is completed, as shown in Figure 15. Click <OK>.

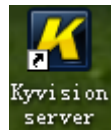


Figure 15 Completing Uninstall

3 Login and Logout

3.1 Login in Server Mode

In this mode, the client and server are installed on the same PC. In this case, login steps are as follows:



1. Double-click on the desktop to run the program.

2. The following dialog box is displayed. After all the red blocks turn green, the startup is completed. If the startup fails, click <Start> until the startup is completed successfully.



Figure 16 Server Startup



3. Double-click on the desktop to run the program.

4. The client login dialog box is displayed, as shown in Figure 17. Enter the user name and password (the default user name and password are admin). Click <Login>. The client interface is displayed, as shown in Figure 18.



Figure 17 Client Login 1

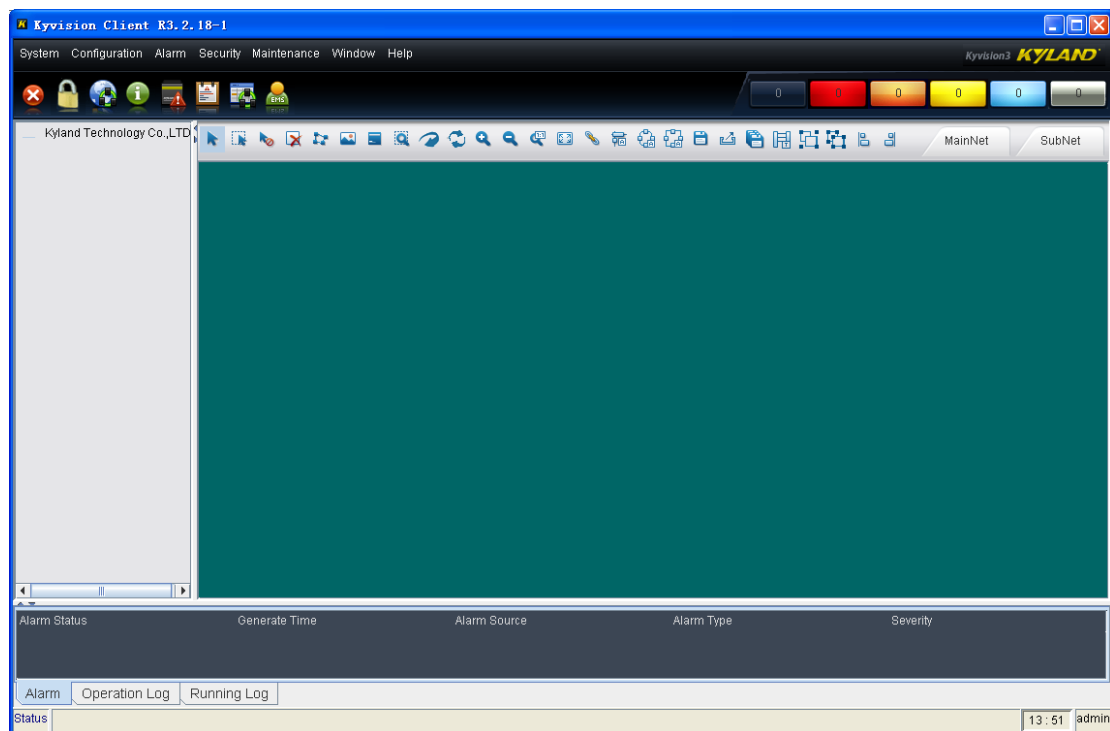


Figure 18 Client Interface

3.2 Login in Client Mode

In this mode, the client and server are installed on different PCs. In this case, login steps are as follows:

1. Make sure that the server is started.



2. Double-click  on the desktop to run the program.
3. The client login dialog box is displayed, as shown in Figure 19. Enter the user name and password (the default user name and password are admin). Click <Login>. The client interface is displayed, as shown in Figure 18.



Figure 19 Client Login 2

3.3 Logout from the Client

When you close the client, the following dialog box is displayed. Select a user and enter its password. Click <Yes> to exit the client.

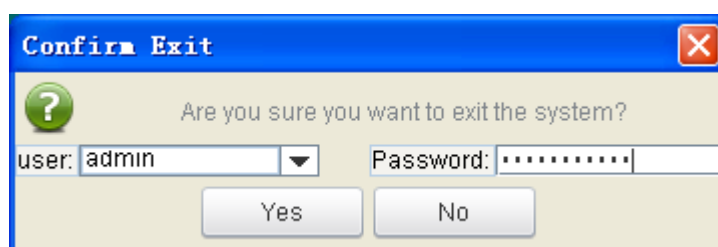


Figure 20 Client Logout

3.4 Logout from the Server

When you close the server, the Notice dialog box is displayed, as shown in Figure 21. Select a user and enter its password. Click <Yes>. The server stop dialog box is displayed, as shown in Figure 22. After all the green blocks turn

red, you can exit the server successfully.

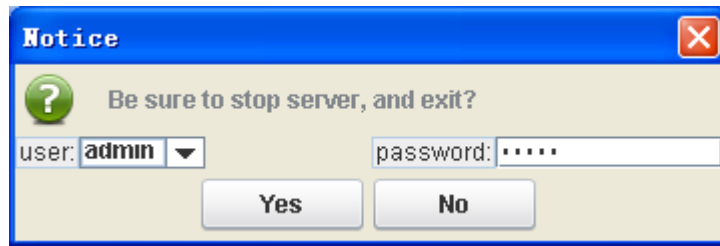


Figure 21 Server Logout



Figure 22 Server Stopping

4 User Interface (UI)

Figure 23 shows the main page of Kyvision.

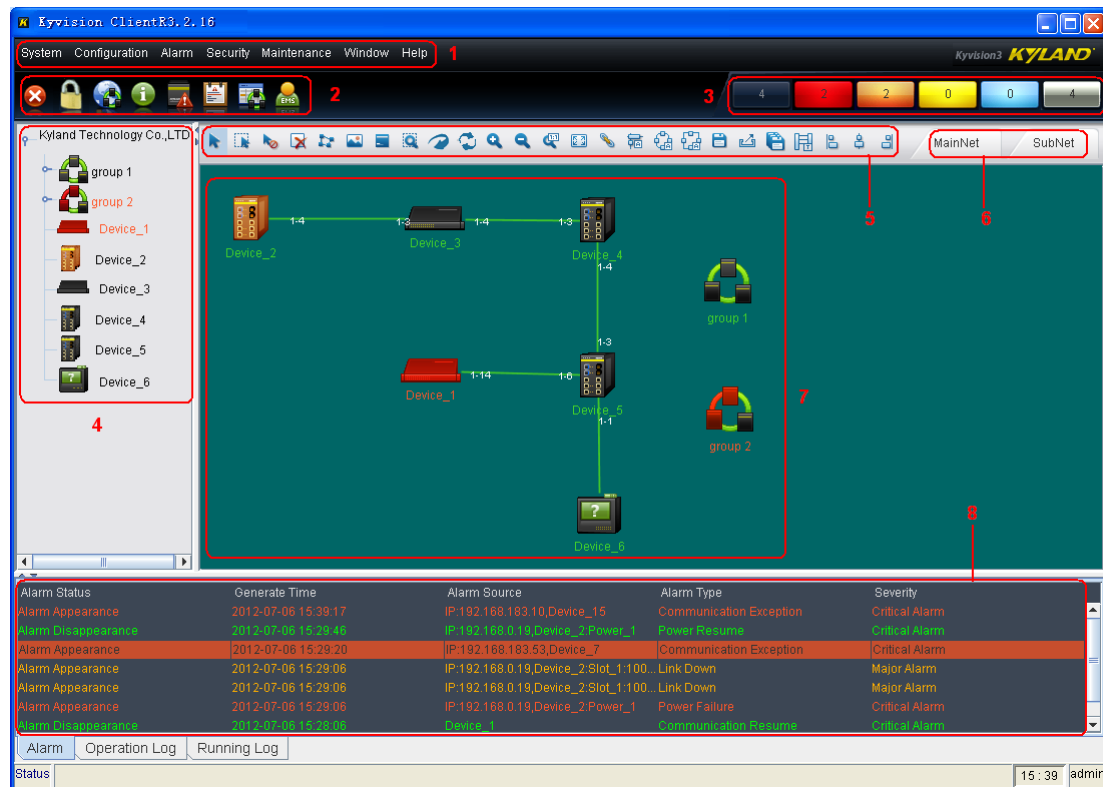


Figure 23 Kyvision UI

Table 2 lists the components of the main page.

Table 2 UI Components

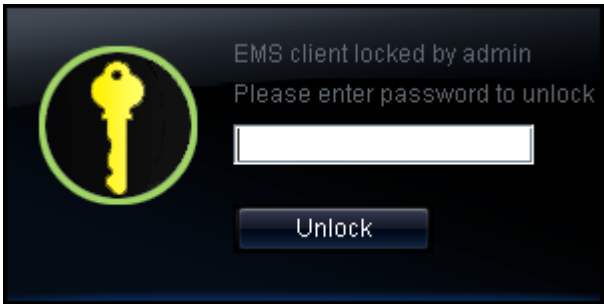
No.	Name	Description
1	Menu bar	System functions
2	Toolbar	Shortcuts for commonly used functions
3	Alarm statistics bar	Number of alarms at each level
4	Navigation tree	List of devices in the topology
5	Topology toolbar	Shortcuts for topology operations
6	Topology switch area	Switch between main network and subnet
7	Network topology area	Links between monitored devices and device status (You can customize the topology)

8	Information display area	Recording alarm information and log information in real time
---	--------------------------	--

4.1 Menu Bar

The menu bar consists of seven menus: System, Configuration, Alarm, Security, Maintenance, Window, and Help. The following table details these menus.

Table 3 Menu Functions

Menu	Submenu	Description
System	Lock Client	Lock the client manually. After you click the submenu, the following figure is displayed. The function prevents other users from operating the client illegitimately. Enter the login password of the current user in the text box. The system is unlocked and you can perform operations. 
	Auto-lock config	Enable the client to be locked at the specified time. The unlocking method is the same as that for manual locking.
	Exit	Exit the current client.
Configuration	Subnet Property Configuration	Create or delete subnets, modify subnet properties, or modify the subnet that a device belongs to by moving a device.
	Subnet Right	Create or delete a monitoring staff. The

	Manager	monitoring staff must be of the Monitor role.
	Device Property Configuration	Create or delete a device, modify device local information, export device property settings.
	Topo View Parameter Configuration	Set topology view parameters, including Interval Value of Auto Topo Square, Original Radius Value of Auto Topo Circle, and Radius Increment Value of Auto Topo Circle.
Alarm	Alarm Management	Manage and query alarms
	Live Alarm Table	Query the information about currently active alarms.
	Alarm Bell Config	Turn on or off alarm bell.
	Operation Log	Query or export operation logs.
	Running Log	Query or export running logs.
Security	EMS User	Manage users in the EMS, including creating or deleting a user, setting user properties, modifying a user password, and locking or unlocking a user. Note: For the default user "admin", only its password can be modified; the other operations are not available.
Maintenance	FTP Server Configuration	Start or stop the FTP server.
	Export Device Configuration	Export the configuration of multiple devices in batches and select the saving path.
	Import Device Configuration	Import configuration to multiple devices in batches.
	Upgrade Device Software	Devices using the same software version can be upgraded in batches.
	EMS Data Backup	EMS data is backed up in the system\dist\ftproot\ftp\datbackup folder of the

		installation directory of the server.
	EMS Data Recovery	Recover EMS data from the sever or local file.
	EMS Data Cleaning	Clean EMS data.
Window	Display Device IP	Select the displayed identifiers of devices in the navigation tree and topology.
	Cascade Windows	Cascade all currently opened windows. You can view the number of opened windows and their titles easily.
	Tile Windows	Tile all currently opened windows to occupy the entire interface. All the windows are displayed in the same size and form. You can view the content of all windows, but each window may be displayed in a small size if too many windows are opened.
Help	About	Display software version and license.

4.2 Toolbar

The toolbar provides shortcuts for commonly used functions, as listed in the following table.

Table 4 Toolbar Functions

Icon	Operation	Description
	Exit	Exit the current client. It brings the same result as clicking [System] → [Exit].
	Lock Client	Lock the client manually. It brings the same result as clicking [System] → [Lock Client].
	Subnet Property Configuration	Create or delete a subnet, or modify subnet properties. It brings the same result as clicking [Configuration] → [Subnet Property Configuration].

	Device Property Configuration	Create or delete a device, or modify device local configuration. It brings the same result as clicking [Configuration] → [Device Property Configuration].
	Alarm Management	Manage and query alarms. It brings the same result as clicking [Alarm] → [Alarm Management].
	Live Alarm Table	Display the information about currently active alarms. It brings the same result as clicking [Alarm] → [Live Alarm Table].
	Subnet Right Manager	Create or delete a monitoring staff. The monitoring staff must be of the Monitor role. It brings the same result as clicking [Configuration] → [Subnet Right Manager].
	EMS User	Manage users in the EMS, including creating or deleting a user, setting user properties, and locking or unlocking a user. It brings the same result as clicking [Security] → [User].

4.3 Alarm Statistics Bar

The alarm statistics bar displays the number of alarms, critical alarms, major alarms, minor alarms, warning alarms, unconfirmed alarms, as shown in the following figure.

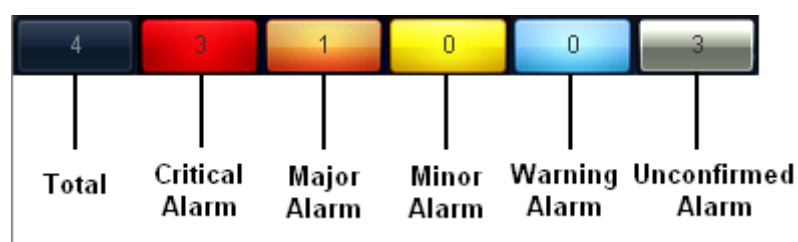
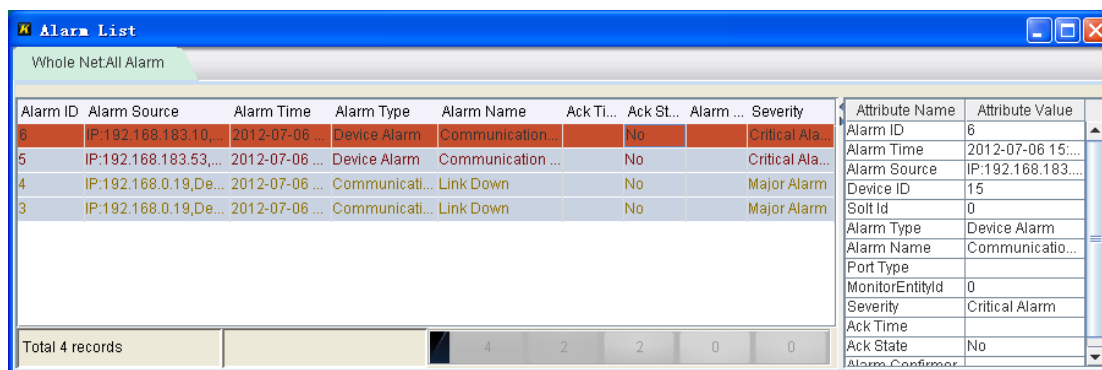


Figure 24 Alarm Statistics Bar

You can click each button to view the corresponding alarm list. Figure 25 shows the list of all alarms. The list contains details about every alarm in the current topology.



The screenshot shows a window titled 'Alarm List' with a tab 'Whole Net:All Alarm'. It contains a table of alarms and a details pane on the right.

Alarm ID	Alarm Source	Alarm Time	Alarm Type	Alarm Name	Ack Ti...	Ack St...	Alarm ...	Severity
6	IP:192.168.183.10...	2012-07-06 ...	Device Alarm	Communication...	No	No	Critical Ala...	Critical Ala...
5	IP:192.168.183.53...	2012-07-06 ...	Device Alarm	Communication ...	No	No	Critical Ala...	Critical Ala...
4	IP:192.168.0.19,De...	2012-07-06 ...	Communicati...	Link Down	No	No	Major Alarm	Major Alarm
3	IP:192.168.0.19,De...	2012-07-06 ...	Communicati...	Link Down	No	No	Major Alarm	Major Alarm

At the bottom left, it says 'Total 4 records'. The details pane on the right shows attributes for the selected alarm (ID 6):

Attribute Name	Attribute Value
Alarm ID	6
Alarm Time	2012-07-06 15:...
Alarm Source	IP:192.168.183.10...
Device ID	15
Soft Id	0
Alarm Type	Device Alarm
Alarm Name	Communication...
Port Type	
MonitorEntityId	0
Severity	Critical Alarm
Ack Time	
Ack State	No

Figure 25 List of All Alarms

4.4 Navigation Tree

The navigation tree displays the list of devices of each topology, as shown in Figure 26. You can view them and perform operations conveniently.

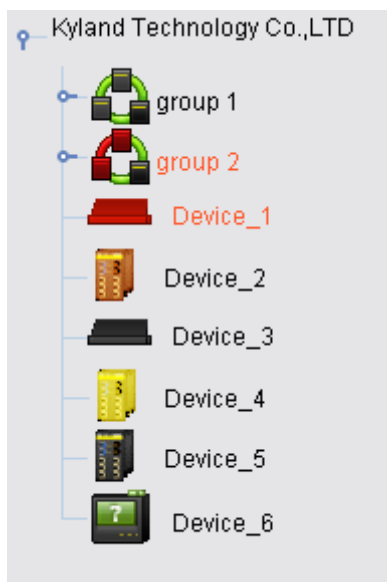


Figure 26 Navigation Tree

You can change the name of the navigation tree by right-clicking it. You can view all devices in the topology by right-clicking the blank area and selecting [Expand All]. Images vary with device types. Different colors represent varied device statuses. The colors are the same as those of alarm levels. For example, if the highest level of active alarms generated on a device is critical, the device is displayed in red (for critical alarm); if the highest level of active alarms generated on a device is major, the device is displayed in orange.

**Note:**

Alarm levels are critical (red), major (orange), minor (yellow), and warning (blue) in descending order.

Table 5 lists the descriptions of the images in Figure 26.

Table 5 Device List

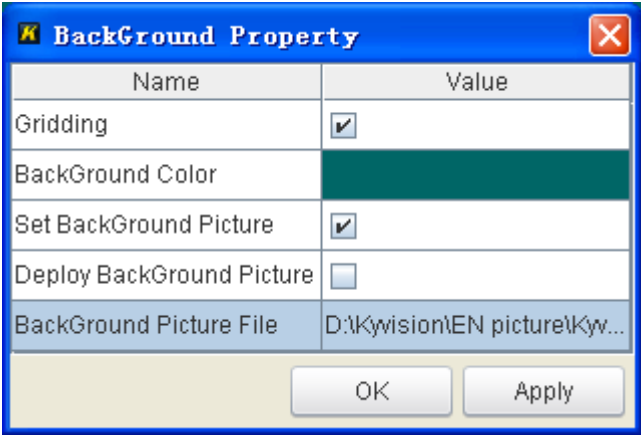
Identifier	Description
Group 1	Subnet in which all devices communicate properly
Group 2	Subnet in which alarms are generated
Device_1	Device whose highest alarm level is critical
Device_2	Device whose highest alarm level is major
Device_3	Rack mounted Kyland switch or an identifiable switch of another vendor
Device_4	Device whose highest alarm level is minor
Device_5	DIN-rail mounted Kyland switches in normal communication
Device_6	Other devices on the network. For these devices, auto-identification and auto-topology are not available. You need to add them to topology and draw related links manually.

Right-click the blank area in the navigation tree. Then you can expand or collapse the navigation tree, or add a subnet or device. Right-click a subnet in the navigation tree. Then you can manage the alarms of the subnet or delete the subnet. Right-click a device in the navigation tree. Then you can manage or configure the device, view the alarms of the device or device panel, or view device status.

4.5 Topology Toolbar

The topology toolbar provides shortcuts for topology building. Details are as follows:

Table 6 Topology Toolbar Functions

Icon	Operation	Description
	Select	Select the specified node or link.
	Select All	Select all the nodes and links in the topology.
	Not Select	Deselect the selected nodes and links.
	Delete Selections	Delete the selected devices.
	Airscape	Display the airscape of the topology. You can change the displayed range by moving the red box.
	Background Property	Display the Background Property dialog box. You can set the gridding, background color, and background picture, as shown in the following figure. To edit an item, you need to double-click it. When setting the background picture, specify the path of the picture file. 
	Modify Device Name	The default identifier of a device in the topology and navigation tree is the device name, which consists of the prefix and device ID. The default prefix is Device. If you click the icon, the Modify Device Name dialog box is displayed. Enter the original and new device name prefixes. Click OK. In this way, you can change the prefix of the specified device.

		Note: Before clicking the icon, you need to select the device whose prefix is to be changed.
	Auto_Topology	Perform auto-topology for the specified network segment or IP address.
	Redo Auto Topology	Perform auto-topology again in the previous mode.
	Refresh Device Link	Refresh the links in the topology.
	Zoom In	Amplify the topology.
	Zoom Out	Shrink the topology.
	1:1	Display the topology in the original size.
	Fit Window	Adjust the topology to fit in the window.
	Link	Add links manually.
	Auto Layout	Perform auto-layout for all nodes in the topology.
	Auto Circle Layout	Change the topology to circle layout.
	Auto Square Layout	Change the topology to square layout.
	Save Current Topology	Save the current topology. The saved topology is displayed automatically upon the next login.
	Export Topology to File	Click the icon. The Save dialog box is displayed. Select the path for saving the file and enter the file name. In so doing, you can save the current topology in a .jpg picture.
	Save All Topology	Save all topologies. The saved topologies are displayed automatically upon the next login.
	Compile Link	Change the start and end positions of links.
	Group	Add all selected nodes to one group. You can group multiple devices based on actual requirements, forming

		topology vividly.
	Ungroup	Dissemble the selected group.
	Left Snap	Align all selected nodes at the left.
	Midway of Landscape	Center all selected nodes horizontally.
	Right Snap	Align all selected nodes at the right.
	Up Snap	Align all selected nodes at the top.
	Midway of Portrait	Center all selected nodes vertically.
	Down Snap	Align all selected nodes at the bottom.

4.6 Topology Switch Area

You can switch the topology between main network and subnet by clicking the <MainNet>/<SubNet> tab.

4.7 Network Topology Area

Display the structure of the current topology. You can modify the topology by clicking the buttons in the topology toolbar. The main network topology contains subnet nodes. You can open the subnet topology by double-clicking a subnet node.

Right-click the blank area in the network topology area. Then you can set background properties, or add a subnet or device. Right-click a subnet in the network topology area. Then you can set subnet properties, manage the alarms of the subnet, or delete the subnet. Right-click a device in the network topology area. Then you can manage or configure the device, view the alarms of the device or device panel, or view device status.

4.8 Information Display Area

The area displays alarm information, operation log information, and running

log information in real time. Kyvision provides a maximum of 500 records for each type of information. The most recent 500 records are kept.

Alarm Status	Generate Time	Alarm Source	Alarm Type	Severity
Alarm Appearance	2012-07-06 15:39:17	IP:192.168.183.10,Device_15	Communication Exception	Critical Alarm
Alarm Disappearance	2012-07-06 15:29:46	IP:192.168.0.19,Device_2 Power_1	Power Resume	Critical Alarm
Alarm Appearance	2012-07-06 15:29:20	IP:192.168.183.53,Device_7	Communication Exception	Critical Alarm
Alarm Appearance	2012-07-06 15:29:06	IP:192.168.0.19,Device_2 Slot_1:100	Link Down	Major Alarm
Alarm Appearance	2012-07-06 15:29:06	IP:192.168.0.19,Device_2 Slot_1:100	Link Down	Major Alarm
Alarm Appearance	2012-07-06 15:29:06	IP:192.168.0.19,Device_2 Power_1	Power Failure	Critical Alarm
Alarm Disappearance	2012-07-06 15:28:06	Device_1	Communication Resume	Critical Alarm
Alarm Appearance	2012-07-06 15:27:47	IP:192.168.0.19,Device_1	Communication Exception	Critical Alarm

Figure 27 Alarm Information

Alarm records are displayed in different colors according to alarm levels, as shown in Figure 27. A record in green indicates that the alarm has been cleaned. Select alarm records (hold Ctrl and click multiple alarm records). Then you can clean the selected alarms or all alarms by right-clicking a selected alarm.

User	Source	Type	Content	Generate Time
admin	Device_15	Device Create	Create Device_15,Type:OtherSwitch,I...	2012-07-06 15:38:33
admin	Device_14	Device Create	Create Device_14,Type:SICOM3306-...	2012-07-06 15:37:22
admin	Device_11	Device Delete	Delete Device_11	2012-07-06 15:37:20
admin	Device_13	Device Create	Create Device_13,Type:Others,IpAdd...	2012-07-06 15:37:14
admin	Device_12	Device Create	Create Device_12,Type:Others,IpAdd...	2012-07-06 15:37:14
admin	Device_11	Device Create	Create Device_11,Type:Others,IpAdd...	2012-07-06 15:37:14
admin	Device_10	Device Create	Create Device_10,Type:Others,IpAdd...	2012-07-06 15:37:14
admin	Device_10	Device Delete	Delete Device_10	2012-07-06 15:36:47
admin	Device_10	Device Create	Create Device_10,Type:Others,IpAdd...	2012-07-06 15:36:30

Figure 28 Operation Log Information

The operation log records user operation information, as shown in Figure 28.

Source	Type	Content	Generate Time
IP:192.168.183.10,Device_15	Device Logout	IP:192.168.183.10,Device_15 Logout	2012-07-06 15:39:17
IP:192.168.1.22,Device_14	Device Login	IP:192.168.1.22,Device_14 Login	2012-07-06 15:37:29
IP:192.168.1.22,Device_14	Device Logout	IP:192.168.1.22,Device_14 Logout	2012-07-06 15:37:29
IP:192.168.1.6,Device_13	Device Login	IP:192.168.1.6,Device_13 Login	2012-07-06 15:37:17
IP:192.168.1.33,Device_12	Device Login	IP:192.168.1.33,Device_12 Login	2012-07-06 15:37:17
IP:192.168.1.22,Device_11	Device Login	IP:192.168.1.22,Device_11 Login	2012-07-06 15:37:17
IP:192.168.1.23,Device_10	Device Login	IP:192.168.1.23,Device_10 Login	2012-07-06 15:37:17
IP:192.168.1.6,Device_10	Device Login	IP:192.168.1.6,Device_10 Login	2012-07-06 15:36:36
IP:192.168.1.6,Device_10	Device Login	IP:192.168.1.6,Device_10 Login	2012-07-06 15:35:54

Figure 29 Running Log Information

The running log records system running information, as shown in Figure 29.

5 Topology Management

5.1 Overview

With the topology management function, Kyvision can draw the topologies of the entire network and all subnets and display the managed network with physical links vividly. Meanwhile, you can also customize your topology. In the topology, links and nodes are displayed in different colors according to the highest alarm level of devices. The statuses of links and devices are updated in real time to facilitate the administrator in network monitoring and fault locating.

5.2 Auto-Topology

With the auto-topology function, Kyvision can create devices and links automatically. It supports two auto-topology modes: specifying an IP address or a network segment for auto-topology.

5.2.1 Specifying an IP Address

In this mode, the server first accesses the device at the specified IP address through SNMP, maps the online status of entities through LLDP, searches for all adjacent devices, and creates devices and links among devices. The process is repeated until all related devices are covered. The related devices refer to all the LLDP- and SNMP-enabled devices connected to the device at the specified IP address.

Auto-topology process:

1. Click  in the topology toolbar. The Auto_Topology dialog box is displayed, as shown in Figure 30.

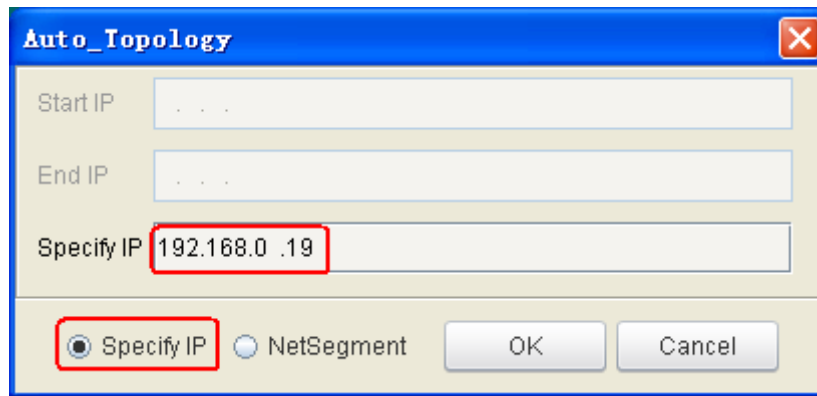


Figure 30 Specifying an IP Address for Auto-Topology

2. Select Specify IP and enter the IP address in the text box. Click <OK>. The Auto_Topology Process dialog box is displayed, as shown in Figure 31.

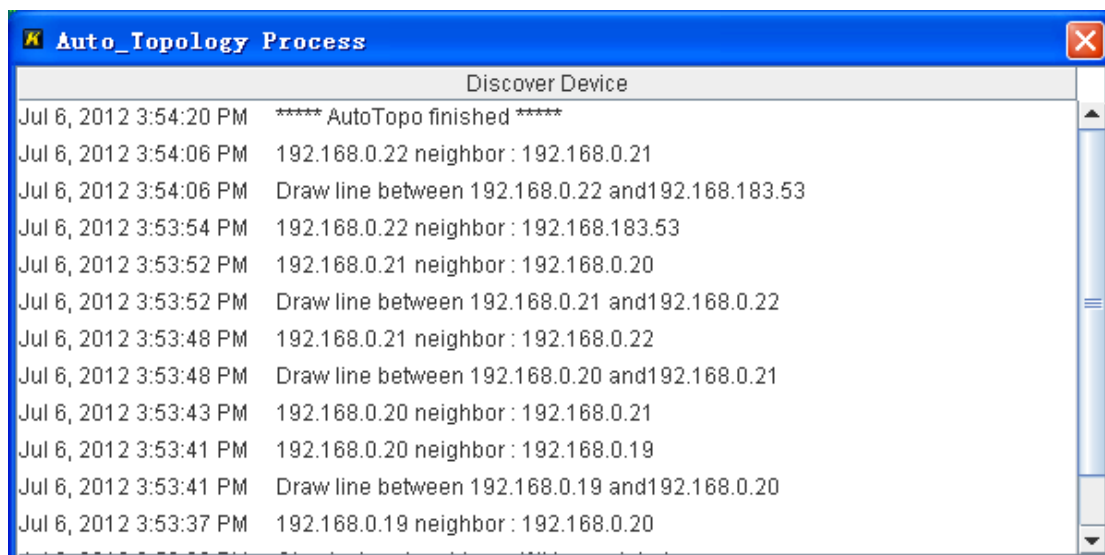


Figure 31 Auto-Topology Process

3. Click  in the topology toolbar to generate links among devices.



Warning:

Before using these automatic functions, you must enable LLDP and SNMP on network devices. Otherwise, the following anomalies may occur: the device may fail to be detected; auto-link is not available; detected devices are identified as other switches or devices; communication fails.

5.2.2 Specifying a Network Segment

In this mode, the server automatically searches for connected devices in the

specified network segment, identifies device types, and creates devices and links among devices. The auto-topology mode can find all connected devices in the specified network segment. Devices that cannot be identified are marked as others.

Auto-topology process:

1. Click  in the topology toolbar. The Auto_Topology dialog box is displayed, as shown in Figure 32.

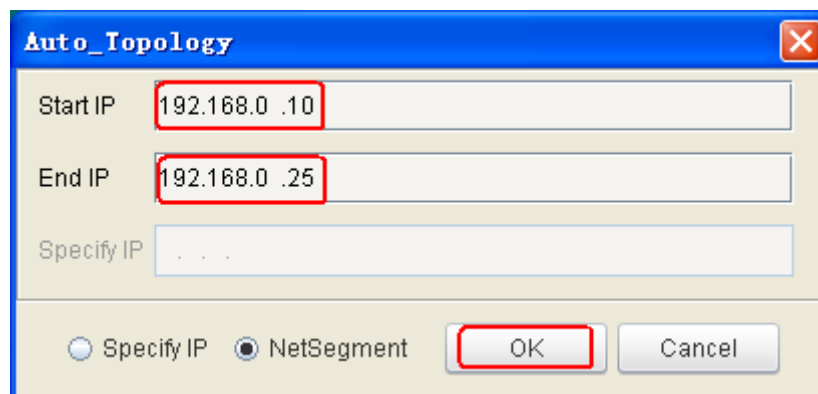


Figure 32 Specifying a Network Segment for Auto-Topology

2. Select NetSegment and enter the start and end IP addresses. Click <OK>. The Auto_Topology Process dialog box is displayed, as shown in Figure 33.

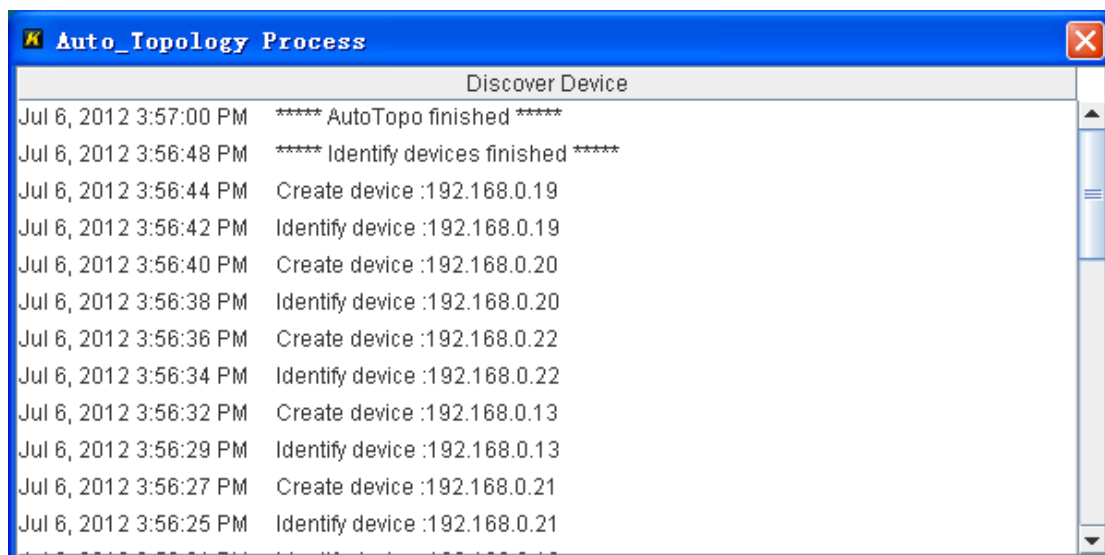


Figure 33 Auto-Topology Process

3. Click  in the topology toolbar to generate links among devices.

**Warning:**

- Before using these automatic functions, you must enable LLDP and SNMP on network devices. Otherwise, the following anomalies may occur: the device may fail to be detected; auto-link is not available; detected devices are identified as other switches or devices; communication fails.
- If network congestion occurs, a detected device may be inconsistent with the actual situation. In this case, you just need to delete the device and create it manually.

5.3 Creating/Deleting a Device

You can create or delete certain devices as needed.

1. Creating a Device

Right-click the network topology area or navigation tree and select [Add Device]. The Create Device dialog box is displayed, as shown in Figure 34. Enter the device ID, device name, and IP address. Select the device type and subnet. Click <OK>. The device is created successfully.

Device ID	1
Device Name	Device_1
Device Type	SICOM3000-2S-6T
IP Address	192.168.0 .23
Subnet Mask	255.255.255.0
Subnet	Not in subnet

Figure 34 Creating a Device

2. Deleting a Device

- Right-click the device to be deleted in the network topology area or navigation tree, and select [Delete Device]. In so doing, the device is

deleted successfully.

- Select devices (hold Ctrl and click multiple devices). Click  in the topology toolbar. In this way, you can delete selected devices. If you want to delete all devices, click  and then .

5.4 Creating/Viewing/Deleting a Link

1. Creating a Link

You can create a connection between two devices. The connection indicates the link between devices. Click  in the topology toolbar. Click the start device and then the end device. The Set Top Link Property dialog box is displayed, as shown in Figure 35.

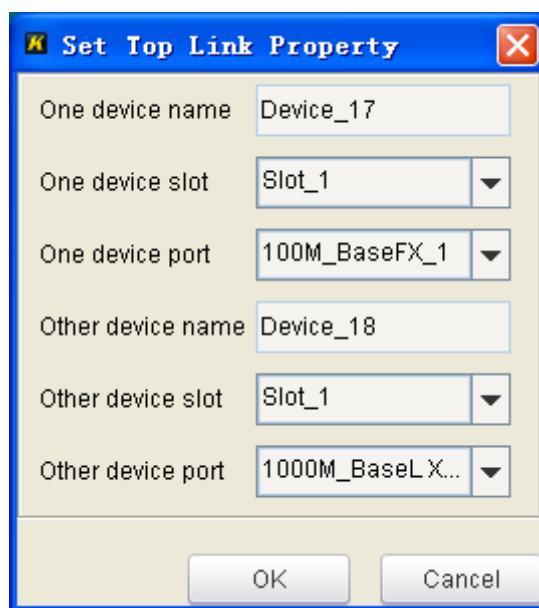


Figure 35 Creating a Link

Select the device slot and port. Click <OK>. A link is created successfully between the two devices.



Caution:

- For modular devices, the device slot is the slot housing the interface card. For non-modular devices, the slot number is 1.
- You can create a link only between online devices.

2. Editing a Link

Click  in the topology toolbar. Select a link. You can change the start and end devices of the link.

3. Viewing link properties

Click the link to be queried, or right-click the link and select [View Link Property]. The View Link Property dialog box is displayed, as shown in Figure 36.

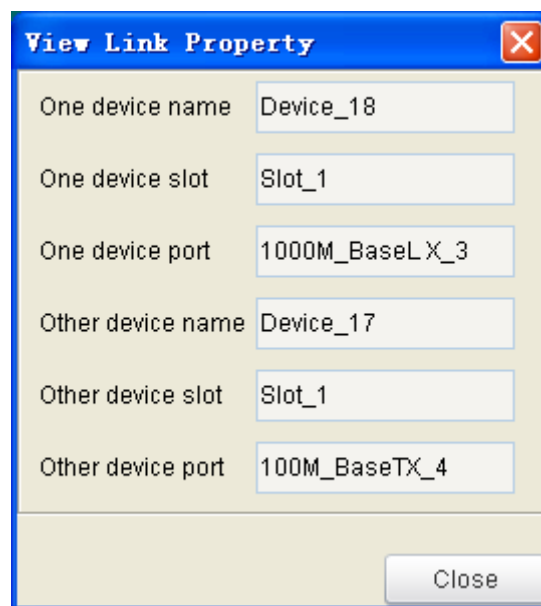


Figure 36 Viewing Link Properties

4. Deleting a Link

Right-click a link and select [Delete Link]. In this way, you can delete the link successfully.

5.5 Subnet Topology Management

In the EMS, you can add certain devices to a subnet as needed and draw topology for each subnet, simplifying network management.

1. Creating a Subnet

Right-click the network topology area or navigation tree and select [Add Subnet]. The Create Subnet dialog box is displayed, as shown in Figure 37.

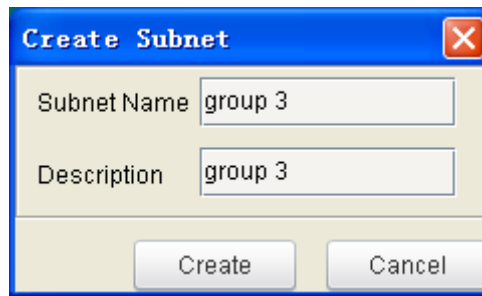


Figure 37 Creating a Subnet

The auto-topology, device, and link operations for a subnet are the same as those for the main network.

2. Querying Subnet Properties

Right-click the network topology area and select [Subnet Property]. The following dialog box is displayed.

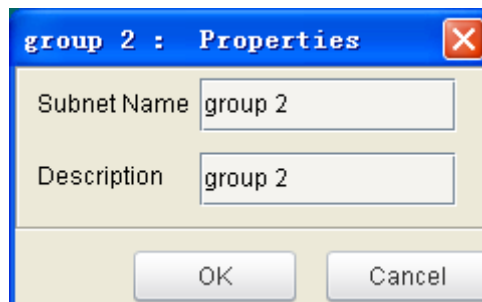


Figure 38 Viewing/Modifying Subnet Properties

3. Deleting a Subnet

Right-click the subnet to be deleted in the network topology area or navigation tree, and select [Delete Subnet]. In so doing, the subnet is deleted successfully.

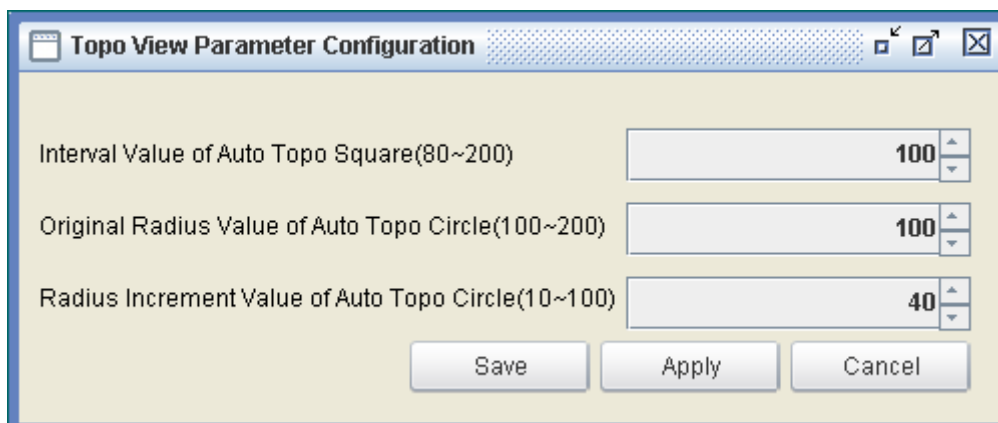
**Caution:**

Before deleting a subnet, you must delete all devices from the subnet.

5.6 Topology Operations

After a topology is created, you can perform operations on the topology by the topology toolbar, as listed in Table 6.

Click [Configuration] → [Topo View Parameter Configuration]. Then you can set the topology view parameters, as shown in Figure 39.



The screenshot shows a window titled "Topo View Parameter Configuration". It has three rows of configuration options, each with a text label and a numeric input field with up/down arrows:

- Interval Value of Auto Topo Square(80~200): 100
- Original Radius Value of Auto Topo Circle(100~200): 100
- Radius Increment Value of Auto Topo Circle(10~100): 40

At the bottom of the window are three buttons: "Save", "Apply", and "Cancel".

Figure 39 Setting Topology View Parameters



Caution:

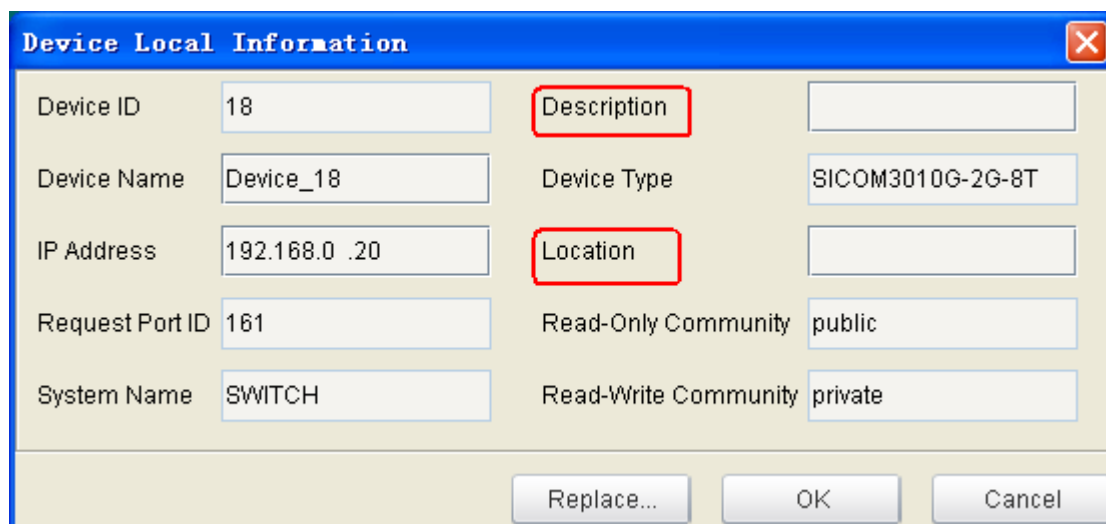
- Original Radius Value of Auto Topo Circle is the radius of the circle layout with less than 10 devices.
- Radius Increment Value of Auto Topo Circle is the radius increment for adding a device to a circle layout with more than 10 devices.

6 Device Management

You can view the details about devices and nodes managed by the EMS, modify device information, view device panel, and import and export device configuration.

6.1 Device Local Information

Right-click the device to be viewed in the network topology area or navigation tree, and select [Local Information]. The Device Local Information dialog box is displayed, as shown in Figure 40.



Device ID	18	Description	
Device Name	Device_18	Device Type	SICOM3010G-2G-8T
IP Address	192.168.0 .20	Location	
Request Port ID	161	Read-Only Community	public
System Name	SWITCH	Read-Write Community	private

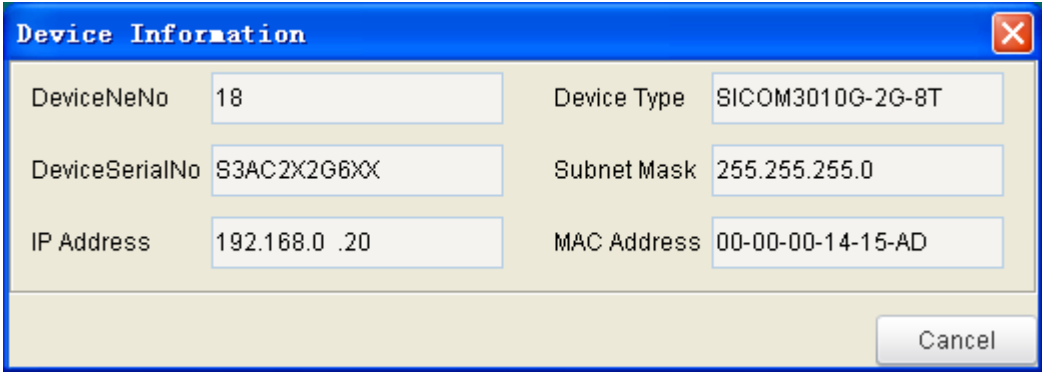
Replace... OK Cancel

Figure 40 Device Local Information

In the preceding figure, only the items in red boxes are configurable. The other items are automatically identified by the EMS. Click <Replace...>. The device name is replaced by the system-defined name. Click <OK>. All configuration and replacement take effect.

6.2 Device Information

Right-click the device to be viewed in the network topology area or navigation tree, and select [Device Basic Information]. The Device Information dialog box is displayed, including device ID, device SN, IP address, device type, subnet mask, and MAC address, as shown in Figure 41.



The 'Device Information' dialog box contains the following fields:

DeviceNo	18	Device Type	SICOM3010G-2G-8T
DeviceSerialNo	S3AC2X2G6XX	Subnet Mask	255.255.255.0
IP Address	192.168.0.20	MAC Address	00-00-00-14-15-AD

A 'Cancel' button is located at the bottom right of the dialog.

Figure 41 Device Information

6.3 Device Panel

Right-click the device to be viewed in the network topology area or navigation tree and select [Device Panel], or double-click the device in the topology. The device panel is displayed. The running statuses of ports are displayed in real time. The indicators of ports in up state are on. Figure 42 shows the panel of a SICOM3000. Port 3 and port 4 are connected, in up state.

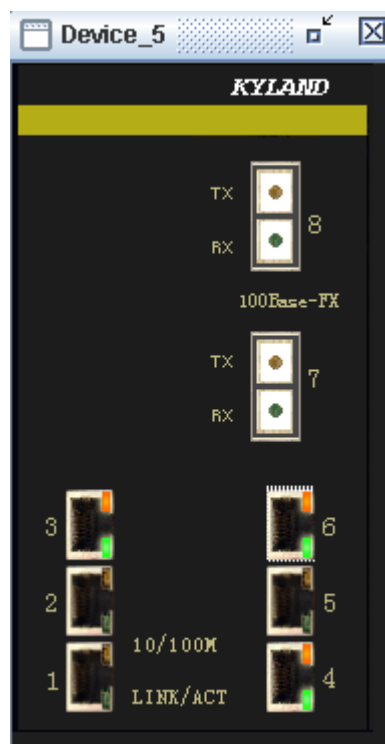


Figure 42 Device Panel

Right-click a port in up state, and select [Port Flow]. The Flux Analysis page is displayed, as shown in Figure 46.

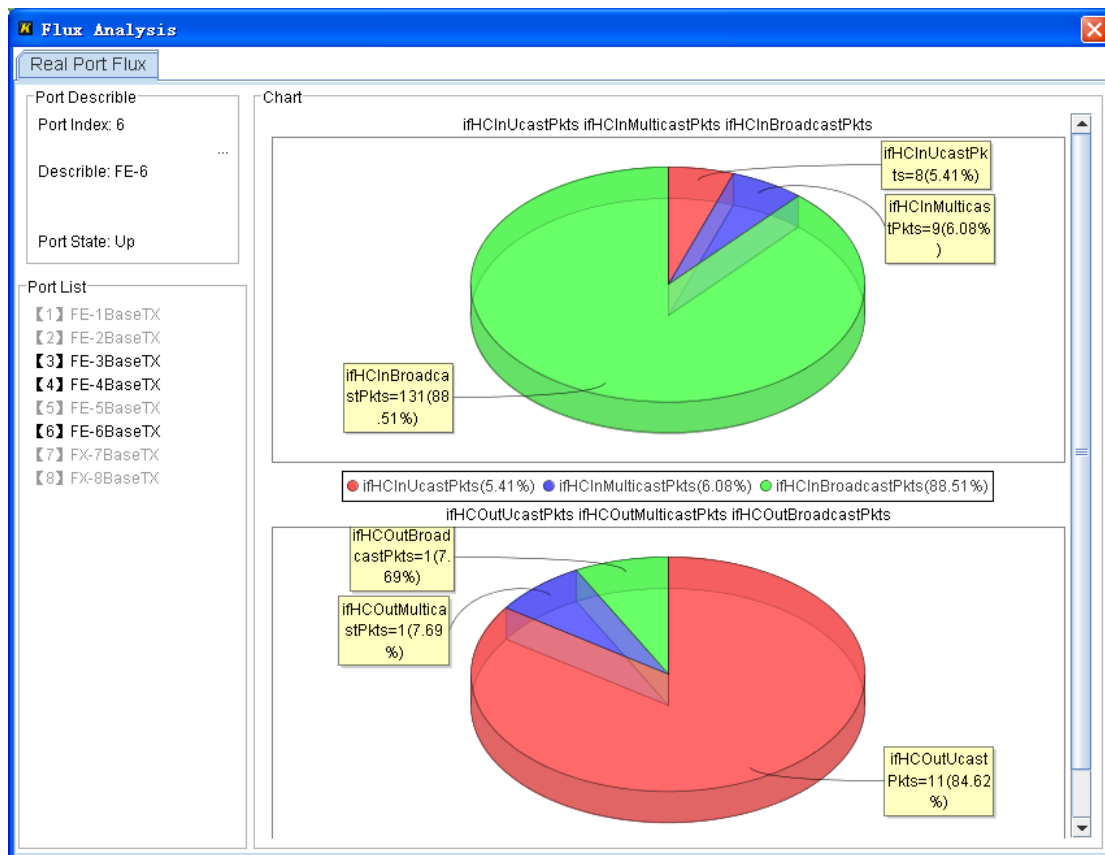


Figure 43 Flux Analysis

**Caution:**

To use this function, the device must support RFC2233.MIB.

6.4 Flux Analysis

Right-click the device to be queried in the network topology area or navigation tree. Select [Flux Analysis] to view the following data statistics on the ports in up state.

- InOctets/OutOctets: indicates the number of transmitted and received bytes per second.
- InUnicastPackets/OutUnicastPackets: indicates the number of transmitted and received unicast packets per second.
- InNUnicastPackets/OutNUnicastPackets: indicates the number of transmitted and received non unicast packets per second.

- Cumulative InErrors Packets/Cumulative OutErrors Packets: indicates the accumulated number of transmitted and received error packets.

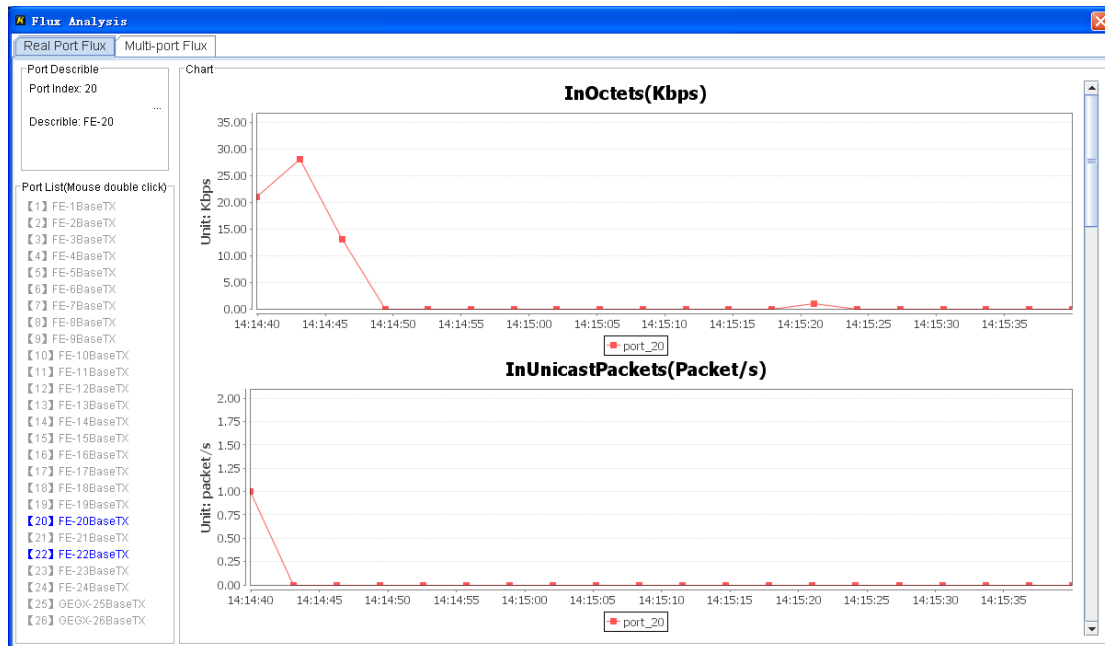


Figure 44 Real Port Flux

As shown in the preceding figure, you can view the transmitted and received data statistics of a port in up state by double-clicking the port on the left. You can also compare the statistics on multiple ports by clicking [Multi-port Flux], as shown in the following figure.

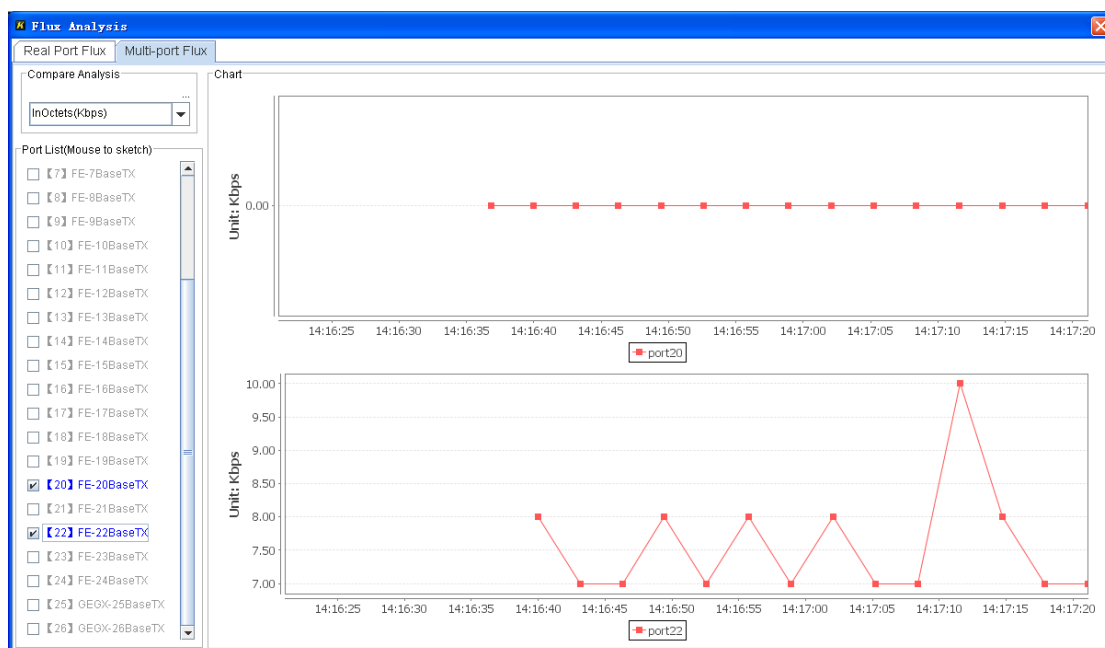


Figure 45 Multi-port Flux

Compare Analysis

Options: InOctets/InUnicastPackets/InNUnicastPackets/Cumulative InErrors
Packets/OutOctets/OutUnicastPackets/OutNUnicastPackets/Cumulative
OutErrors Packets

Function: Select the items to be compared.

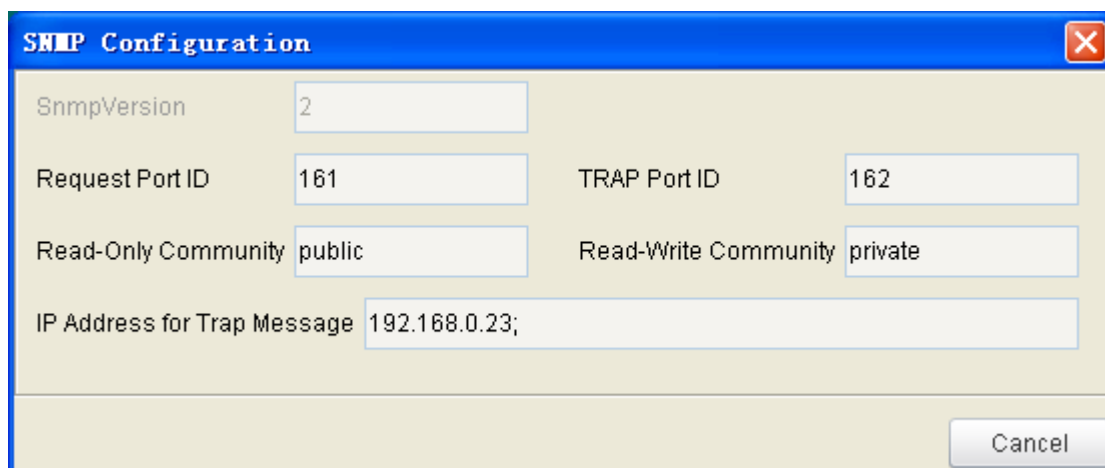
Port List

Options: ports in up state

Description: Select two or more ports for data comparison.

6.5 SNMP Configuration

Right-click the device to be viewed in the network topology area or navigation tree and select [SNMP Configuration]. The SNMP Configuration dialog box is displayed, as shown in Figure 46.



The image shows a 'SNMP Configuration' dialog box with a blue title bar and a close button in the top right corner. The dialog contains several input fields: 'SnmpVersion' with the value '2', 'Request Port ID' with '161', 'TRAP Port ID' with '162', 'Read-Only Community' with 'public', 'Read-Write Community' with 'private', and 'IP Address for Trap Message' with '192.168.0.23;'. A 'Cancel' button is located at the bottom right.

Figure 46 Viewing SNMP Configuration



Caution:

For SNMP, the default port receiving requests is port 161 and the default port sending trap packets is port 162. The community name of a read-only user is public and that of a read-write user is private. Kyvision can identify only the devices on which SNMP parameters are set to default values.

6.6 Device State Information

Right-click the device to be viewed in the network topology area or navigation

tree and select [Device State Information]. The Device State Information dialog box is displayed. Select the device name. Click <Query>. You can view the system, interface, IP address, routing information, and ring protocol information of the device, as shown in Figure 47.

System.system	
Device Description	KYLAND TECHNOLOGY CO., LTD. Industrial Ethernet Switch Software<0A>KYLAND-SICOM3010G Firmware Version VF001 Bootrom Version 2.2.6
sysOID	1.3.6.1.4.1.26067.5.29
Run Time	4 Day 22 Hour 33 Minute 18 Second
Contact Information	+86-10-88798888
System Name	SWITCH
Place Information	Chongxin Mansion Building, Xijing Road 3#, Shijingshan District, Beijing
Service	Link(2)

Figure 47 Device State Information

6.7 Device Running State

Right-click the device to be viewed in the network topology area or navigation tree and select [Device Running State]. The Device Running State dialog box is displayed, as shown in Figure 48.

Figure 48 Device Running State

6.8 CPU and Memory Threshold

Right-click the device to be queried in the network topology area or navigation tree. Select [Device CPU and Memory] to set the alarm thresholds for CPU and memory usage, as shown in the following figure.

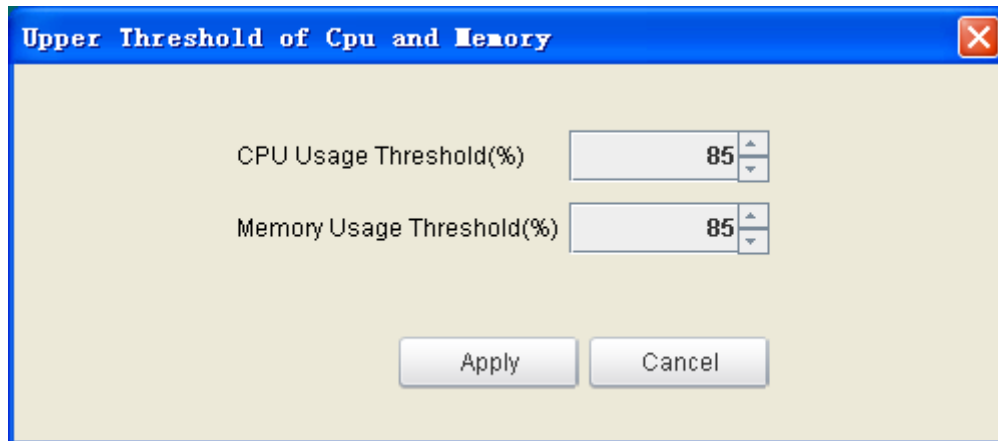


Figure 49 CPU and Memory Threshold

CPU Usage Threshold (%)

Range: 50~100

Default: 85

Function: Set the CPU usage threshold. When the CPU usage of the switch is higher than the threshold, an alarm is generated. The alarm is a minor alarm.

Description: If the CPU usage fluctuates around the threshold, alarms may be generated and cleared repeatedly. To prevent this phenomenon, you can specify a value (5% by default). The alarm will be cleared only if the CPU usage is lower than the threshold by the specified value or more. For example, the CPU usage threshold is set to 60% and the value is set to 5%. If the CPU usage of the switch is lower than or equal to 60%, no alarm is generated. If the CPU usage is higher than 60%, an alarm will be generated. The alarm will be cleared only if the CPU usage is equal to or lower than 55%.



Caution:

The CPU usage in this document refers to the average CPU usage in five minutes.

Memory Usage Threshold (%)

Range: 50~100

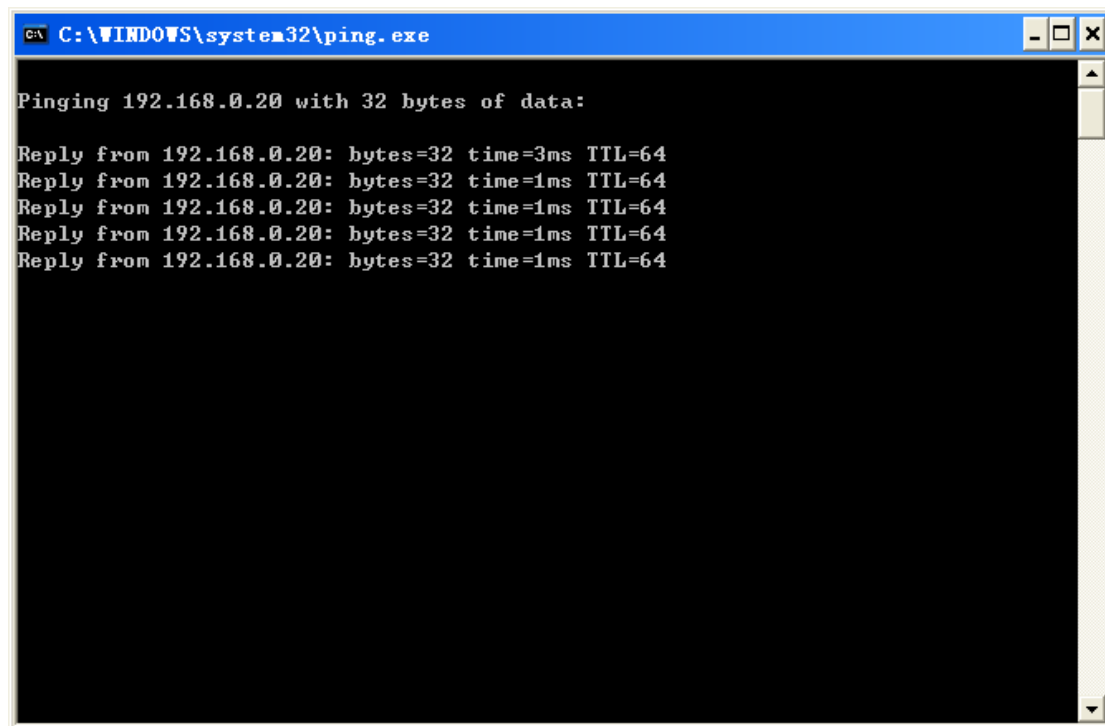
Default: 85

Function: Set the memory usage threshold. When the memory usage of the switch is higher than the threshold, an alarm is generated. The alarm is a minor alarm.

Description: If the memory usage fluctuates around the threshold, alarms may be generated and cleared repeatedly. To prevent this phenomenon, you can specify a value (5% by default). The alarm will be cleared only if the memory usage is lower than the threshold by the specified value or more. For example, the memory usage threshold is set to 60% and the value is set to 5%. If the memory usage of the switch is lower than or equal to 60%, no alarm is generated. If the memory usage is higher than 60%, an alarm will be generated. The alarm will be cleared only if the memory usage is equal to or lower than 55%.

6.9 Ping Device

Right-click the device to be pinged in the network topology area or navigation tree and select [Ping Device From Client]. The ping operation result is displayed, as shown in Figure 50.



```
C:\WINDOWS\system32\ping.exe

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time=3ms TTL=64
Reply from 192.168.0.20: bytes=32 time=1ms TTL=64
Reply from 192.168.0.20: bytes=32 time=1ms TTL=64
Reply from 192.168.0.20: bytes=32 time=1ms TTL=64
Reply from 192.168.0.20: bytes=32 time=1ms TTL=64
```

Figure 50 Ping Operation

**Caution:**

When a communication anomaly occurs, you can view whether the network connection between the device and the EMS by the ping operation.

6.10 Link Telnet

Right-click the device to be operated in the network topology area or navigation tree and select [Link Telnet]. The telnet interface is displayed. Enter user name "admin" and password "123". The switch CLI is displayed, as shown in Figure 51.

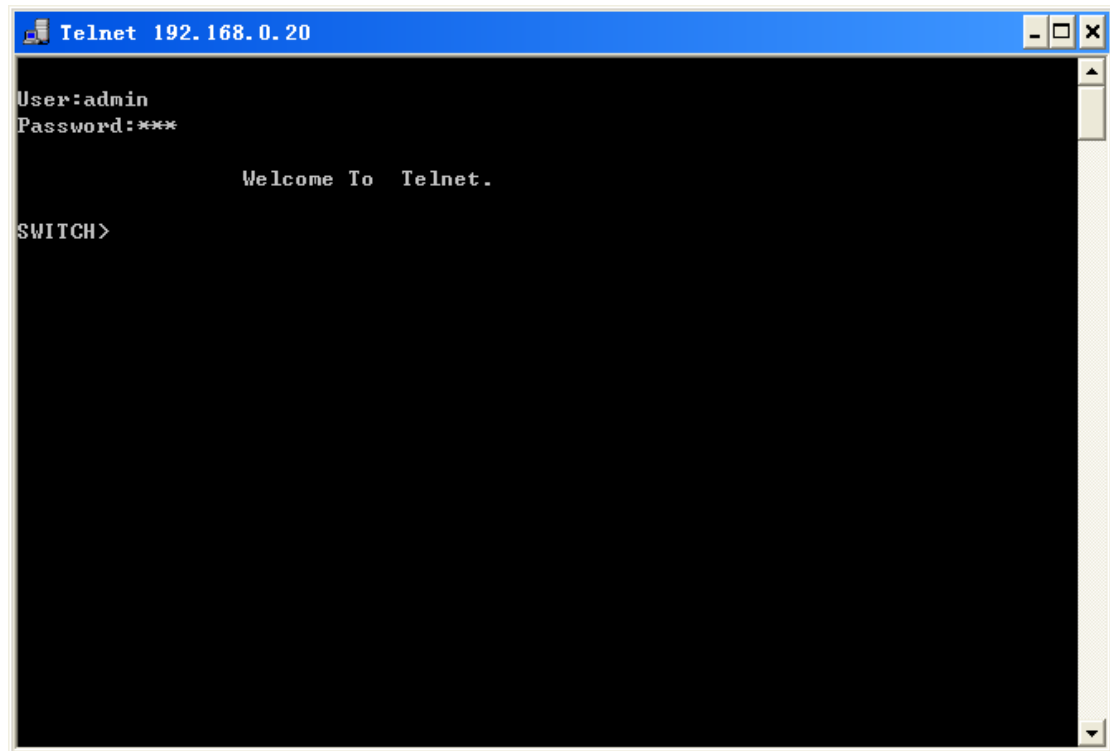
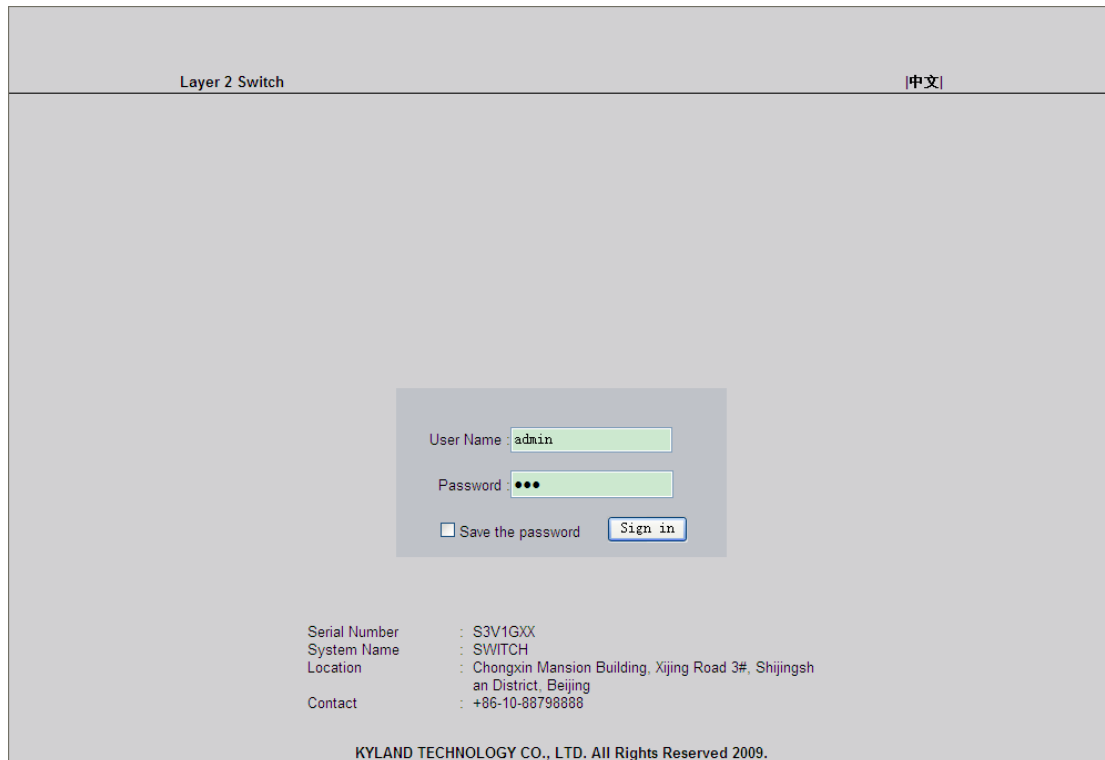


Figure 51 Telnet Interface

6.11 Start Web

Right-click the device to be operated in the network topology area or navigation tree and select [Start Web]. The Web login page is displayed, as shown in Figure 52. Enter user name "admin" and password "123". The switch Web UI is displayed.



Layer 2 Switch [中文]

User Name : admin

Password : ...

☐ Save the password Sign in

Serial Number	: S3V1GXX
System Name	: SWITCH
Location	: Chongxin Mansion Building, Xijing Road 3#, Shijingshan District, Beijing
Contact	: +86-10-88798888

KYLAND TECHNOLOGY CO., LTD. All Rights Reserved 2009.

Figure 52 Web Login

6.12 All Alarms

Right-click the device to be viewed in the network topology area or navigation tree and select [All Alarms]. The list of active alarms of the device is displayed. For details, see section 8.4.2 Alarm Status-based Alarm List.

6.13 Device Property Configuration

You can export device property settings and save them to the local device for further query.



Click [Configuration] → [Device Property Configuration] or . The Device Property Configuration page is displayed. You can click <Create> to create a device, select a device in the list and click <Delete>/<Modify> to delete or modify the selected device, or click <Export> to export the property settings of all devices in the subnet. The default name of the exported file is the date, with the extension of .xls.

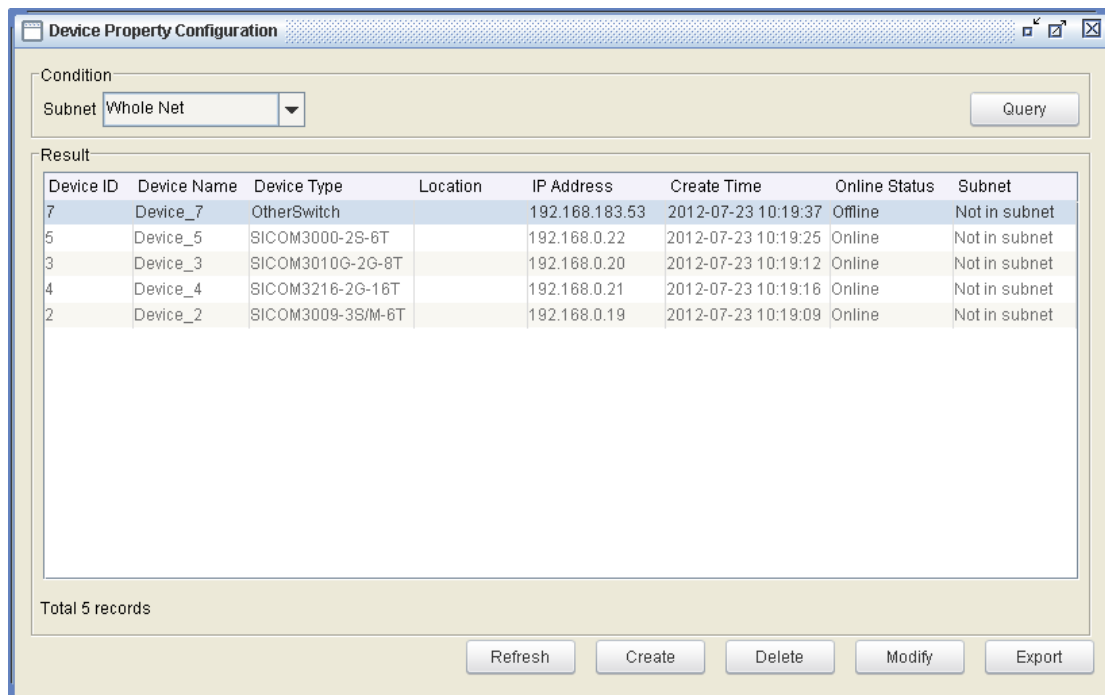


Figure 53 Device Property Configuration

6.14 Maintenance

You can import or export device configuration in batches, upgrade software version in batches, and back up, recover, or clean EMS data.



Caution:

To import or export device configuration, upgrade software version, or recover EMS data, the built-in FTP server is required.

6.14.1 FTP Server Configuration

Click [Maintenance] → [FTP Server Configuration]. The FTP Server Configuration page is displayed, as shown in Figure 54. Click <Start> to start the FTP server.

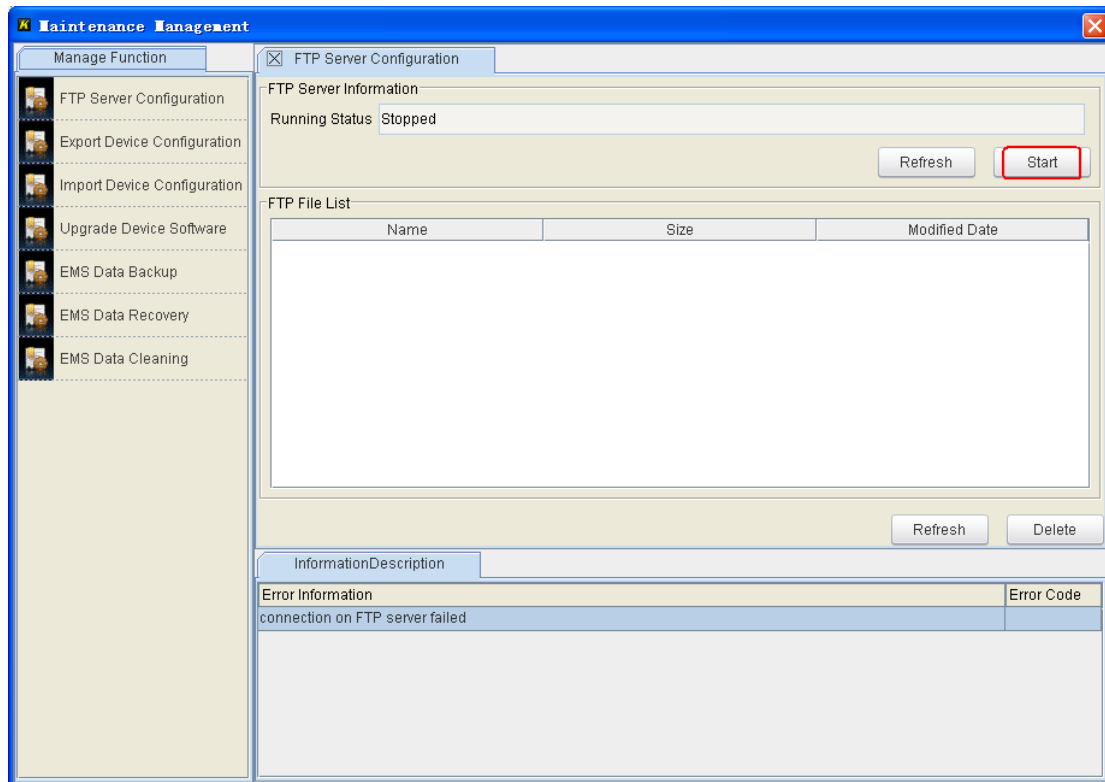


Figure 54 Starting FTP Server

When "FTP start successful" is displayed, as shown in Figure 55, the FTP server is started and running.

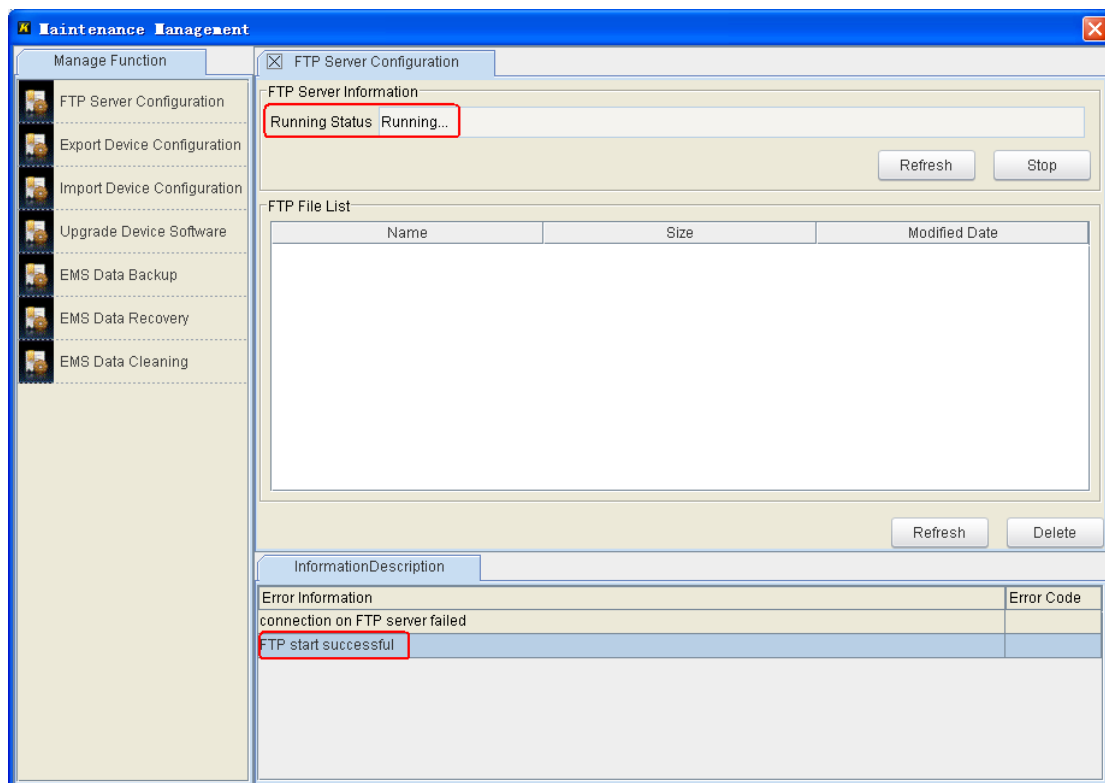


Figure 55 Starting FTP Server Successfully

6.14.2 Export Device Configuration

Click [Maintenance] → [Export Device Configuration]. The Export Device Configuration page is displayed, as shown in Figure 56. Select the devices whose configurations are to be exported. Click <Browse> and select the path for saving the file to be exported. Click <Export> to export the configurations of the devices in batches. If the page in Figure 57 is displayed, the configurations are exported successfully.



Caution:

- The default name of the exported file is the IP address of the device and the extension is .txt.
- The exported configurations are the latest saved configurations of the devices.
- Ensure that the FTP server is running.

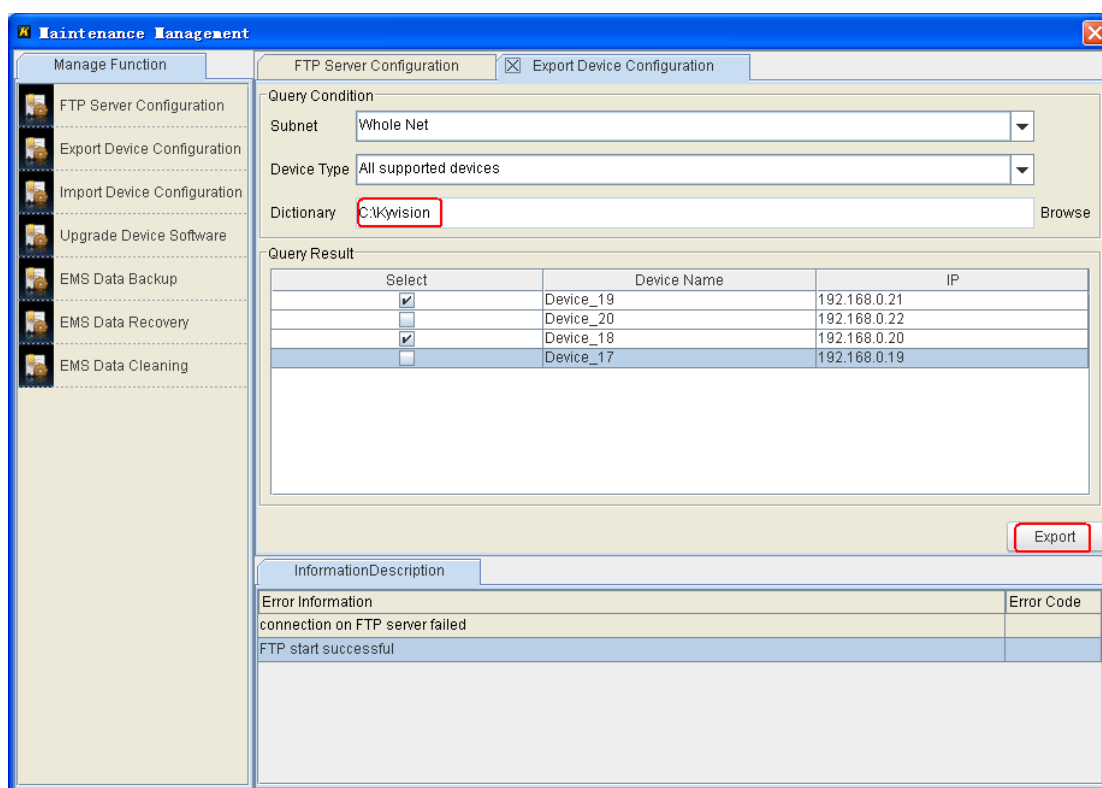


Figure 56 Exporting Device Configuration

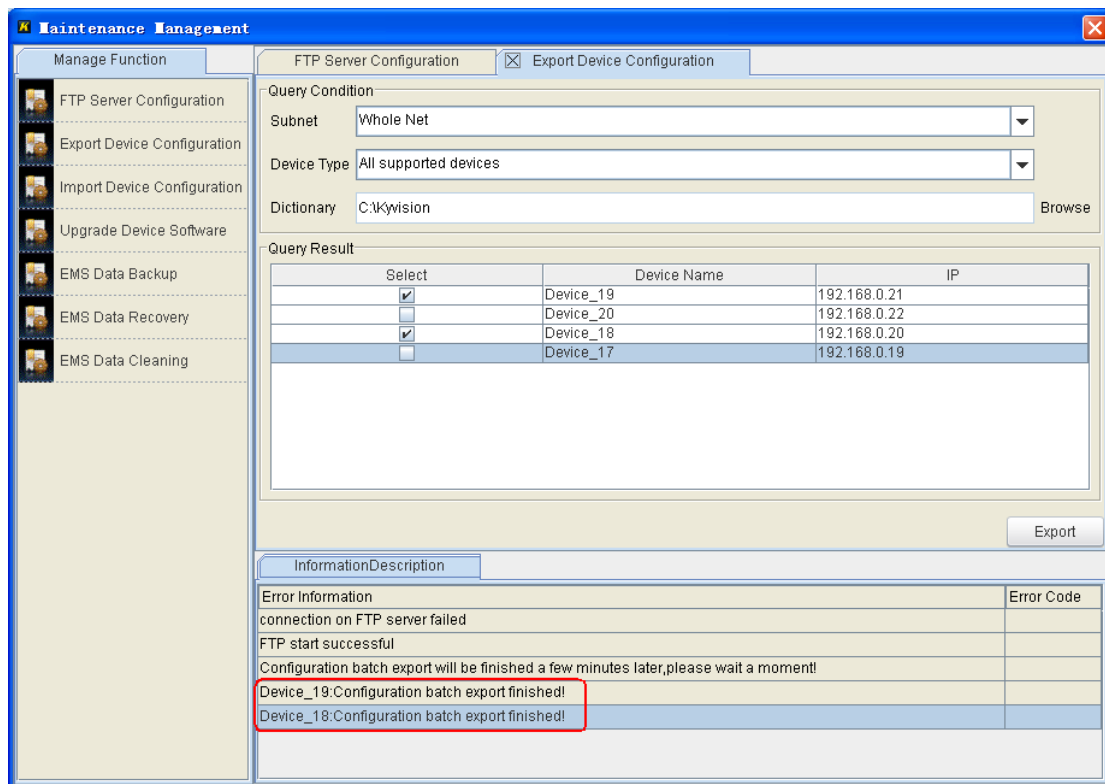


Figure 57 Exporting Device Configuration Successfully

6.14.3 Import Device Configuration

Click [Maintenance] → [Import Device Configuration]. The Import Device Configuration page is displayed, as shown in Figure 58. Select the devices whose configurations are to be imported. Click <Browse> and select the path for saving the file to be imported. Click <Import> to import the configurations to the devices in batches. If the page in Figure 59 is displayed, the configurations are imported successfully.



Caution:

- After configuration is imported, it takes effect only after the device is restarted.
- Ensure that the FTP server is running.

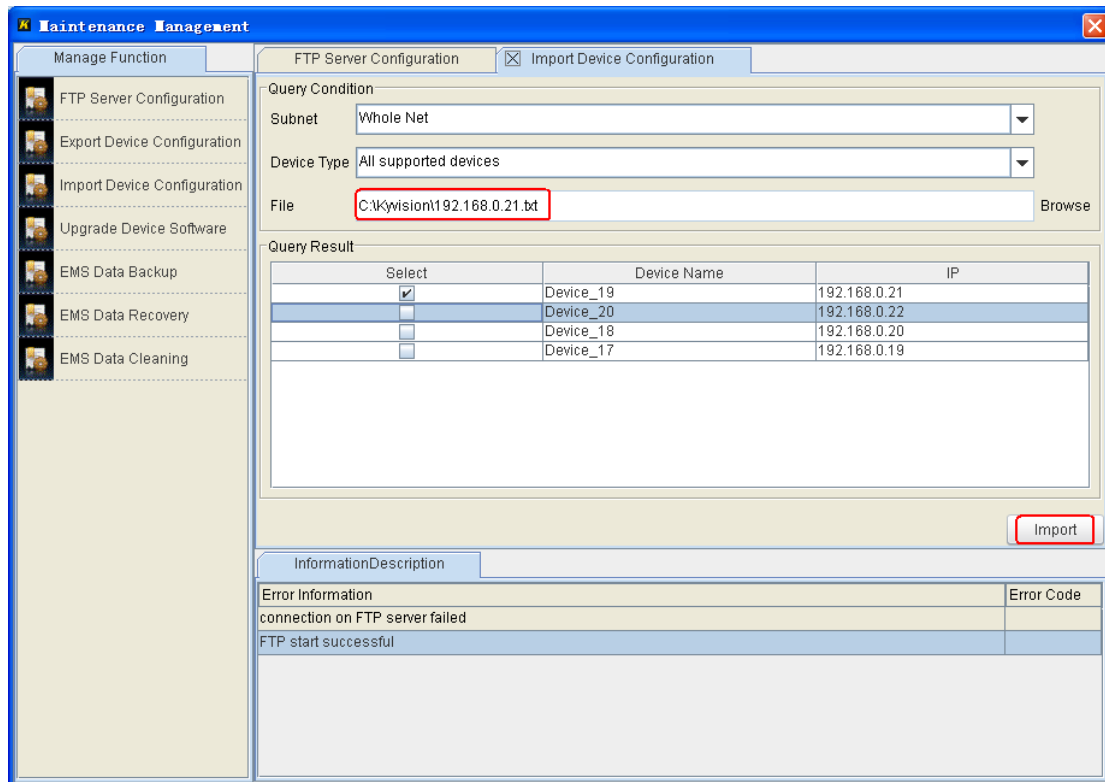


Figure 58 Importing Device Configuration

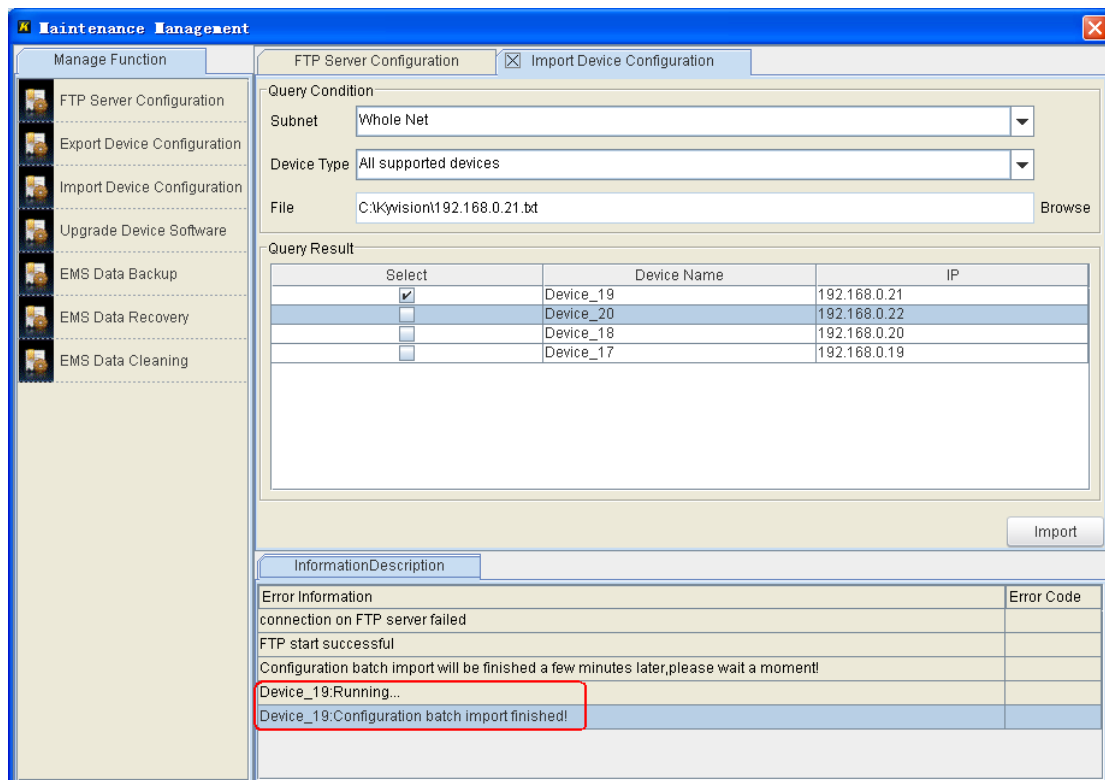


Figure 59 Importing Device Configuration Successfully

6.14.4 Upgrade Device Software

Click [Maintenance] → [Upgrade Device Software]. The Upgrade Device Software page is displayed, as shown in Figure 60. Select the devices whose software version is to be upgraded. Click <Browse> and select the path for saving the software version file. Click <Upgrade> to upgrade the devices in batches.



Caution:

- After software upgrade is completed, the new version takes effect only after the device is restarted.
- Devices to be upgraded in batches must use the same software version.
- Ensure that the FTP server is running.

The screenshot shows the 'Maintenance Management' window with the 'Upgrade Device Software' tab selected. The 'Query Condition' section has 'Subnet' set to 'Whole Net', 'Device Type' set to 'All supported devices', and a file path 'D:\WMsoft_kyland\SICOM3009A-T0029\SICOM3009A-T0029.bin' entered in the 'File' field. The 'Query Result' table lists four devices with their names and IP addresses. The 'Upgrade' button is highlighted with a red box. The 'Error Information' section shows a message 'connection on FTP server failed' with an empty 'Error Code' field.

Select	Device Name	IP
☒	Device_19	192.168.0.21
☒	Device_20	192.168.0.22
☒	Device_18	192.168.0.20
☐	Device_17	192.168.0.19

Error Information	Error Code
connection on FTP server failed	
FTP start successful	

Figure 60 Device Software Upgrade

6.14.5 EMS Data Backup

Click [Maintenance] → [EMS Data Backup]. The EMS Data Backup page is displayed. The EMS can back up data immediately or periodically. By default,

the EMS automatically backs up data at 00:20:00 every day.

1. Immediate Backup

As shown in Figure 61, click <Backup Immediately>. The Notice dialog box is displayed, as shown in Figure 62. Click <Yes>. The EMS backs up data immediately. When "Backup data successfully" is displayed, the data is backed up successfully, as shown in Figure 63.

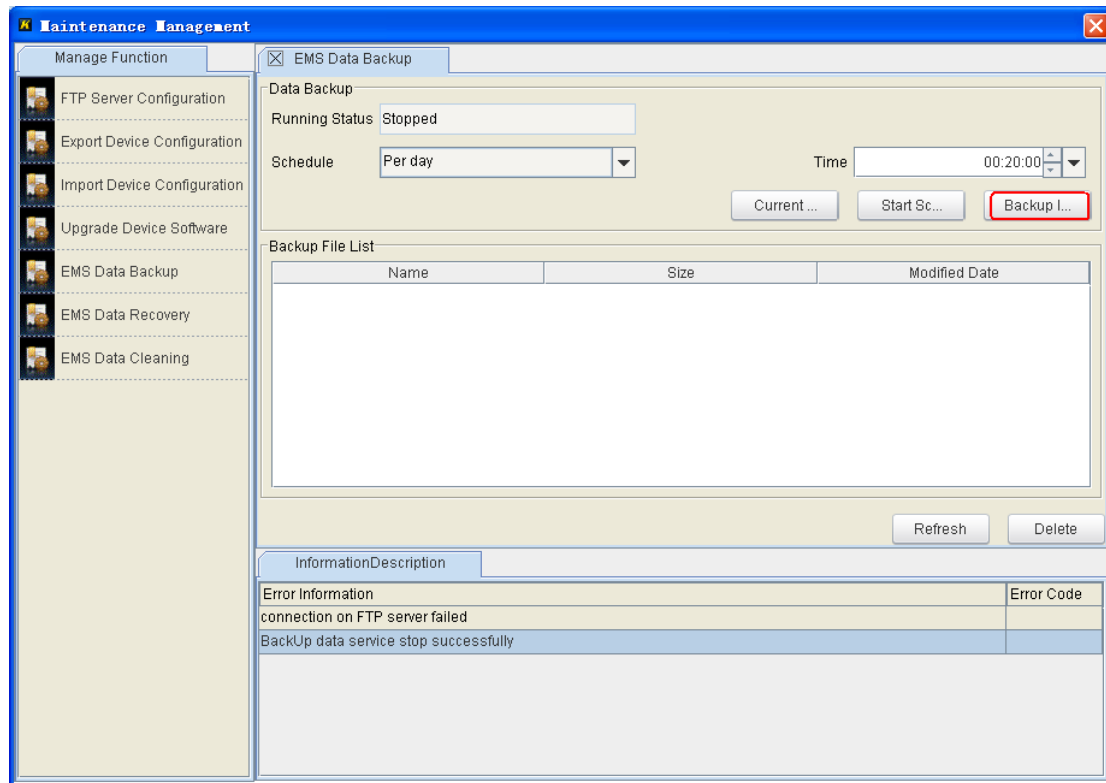


Figure 61 Immediate Backup

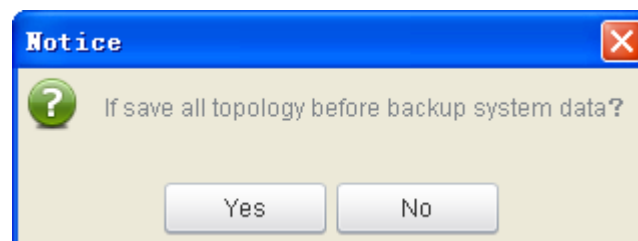


Figure 62 Topology Saving Confirmation

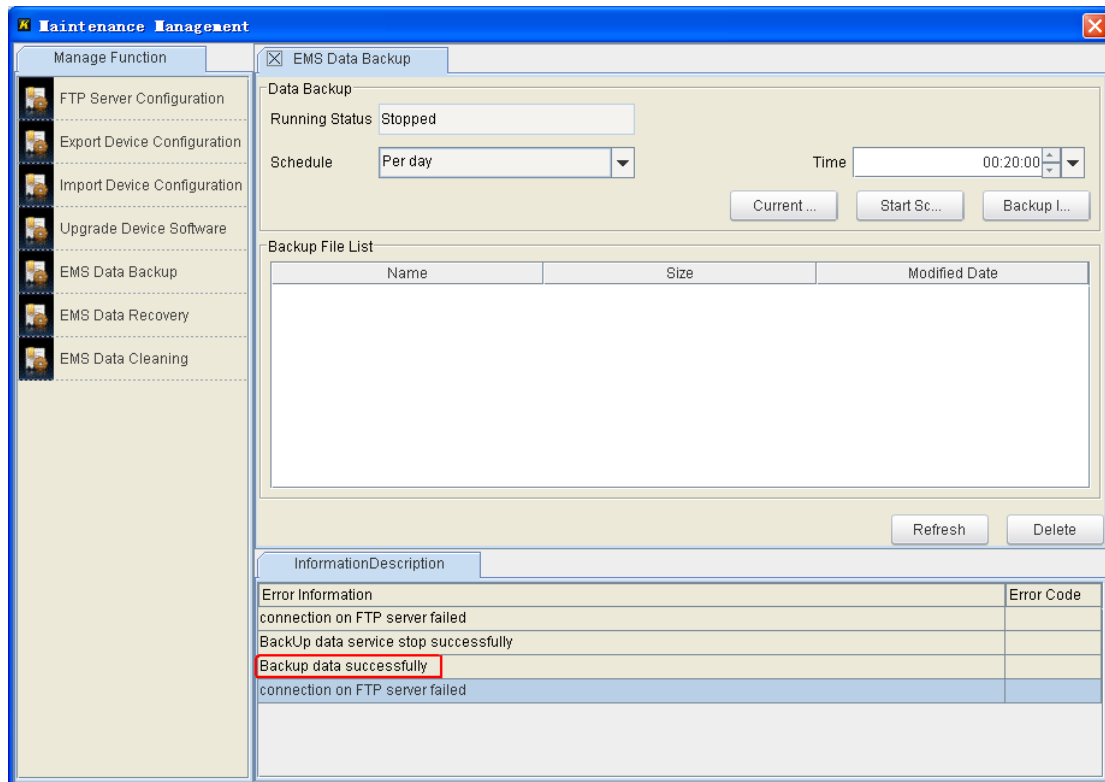


Figure 63 Backing up Data Successfully

2. Periodic Backup

You can configure the EMS to automatically back up data on a daily/weekly/monthly basis, as shown in Figure 64 to Figure 66. After setting the plan, click <Start Schedule>. The EMS will automatically back up data according to the plan.

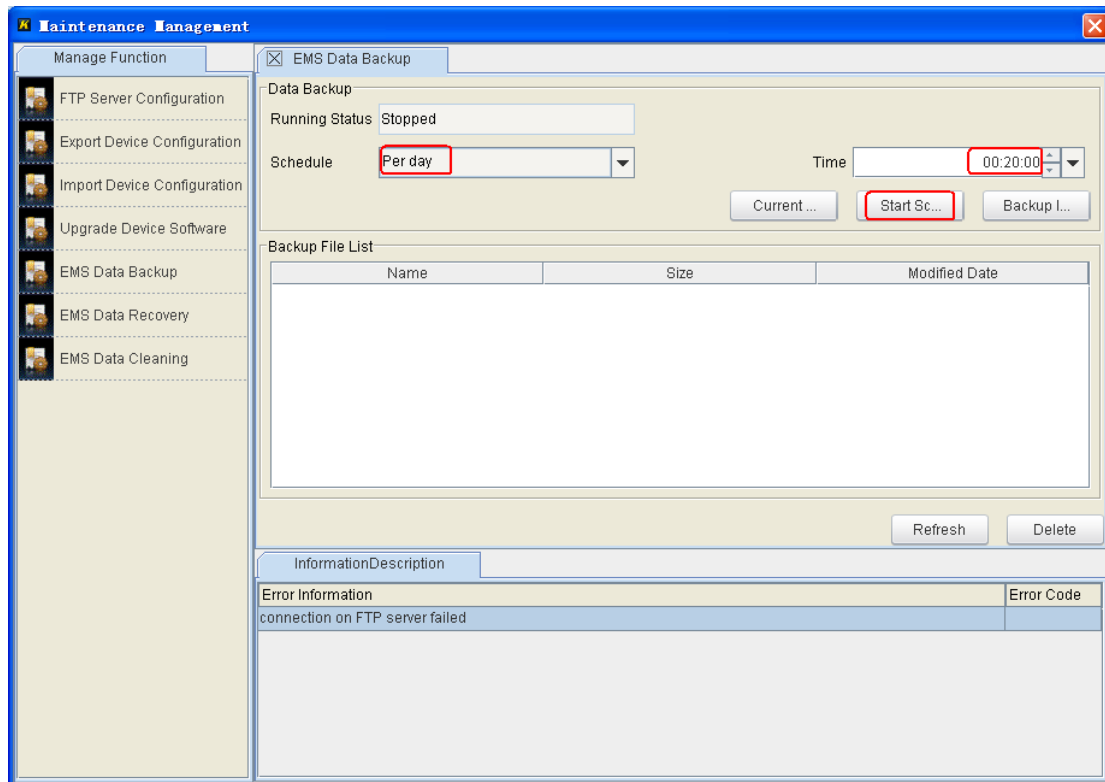


Figure 64 Backing up Data on a Daily Basis

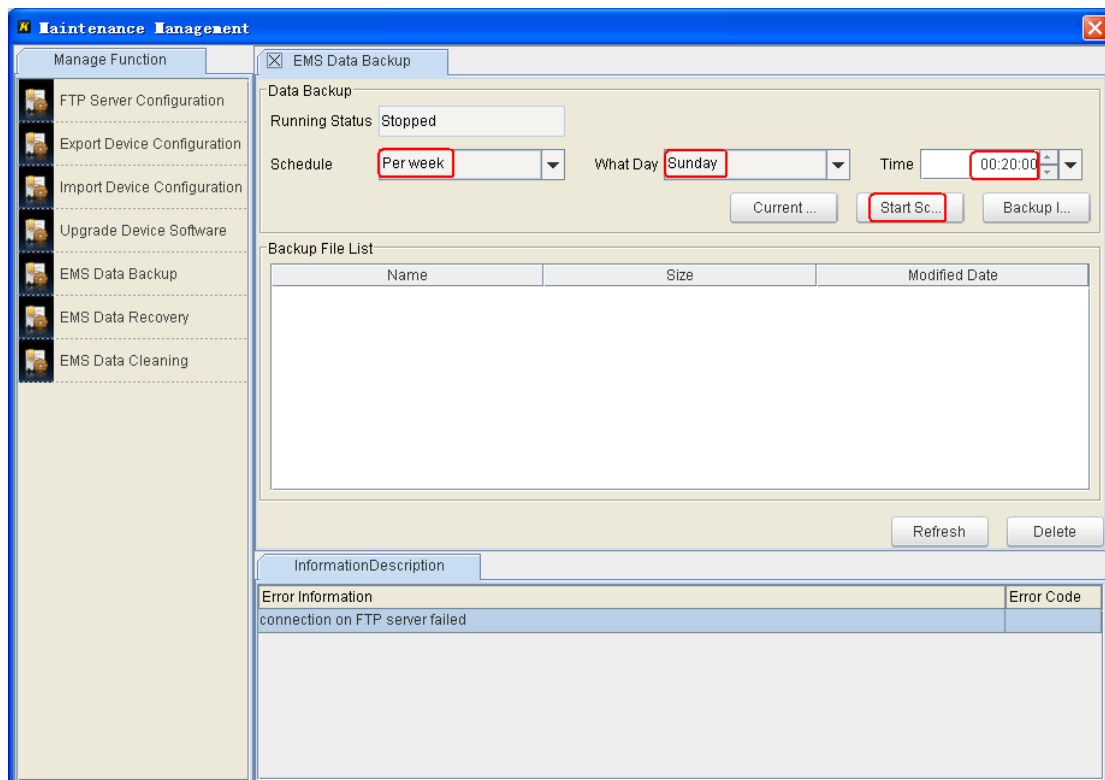


Figure 65 Backing up Data on a Weekly Basis

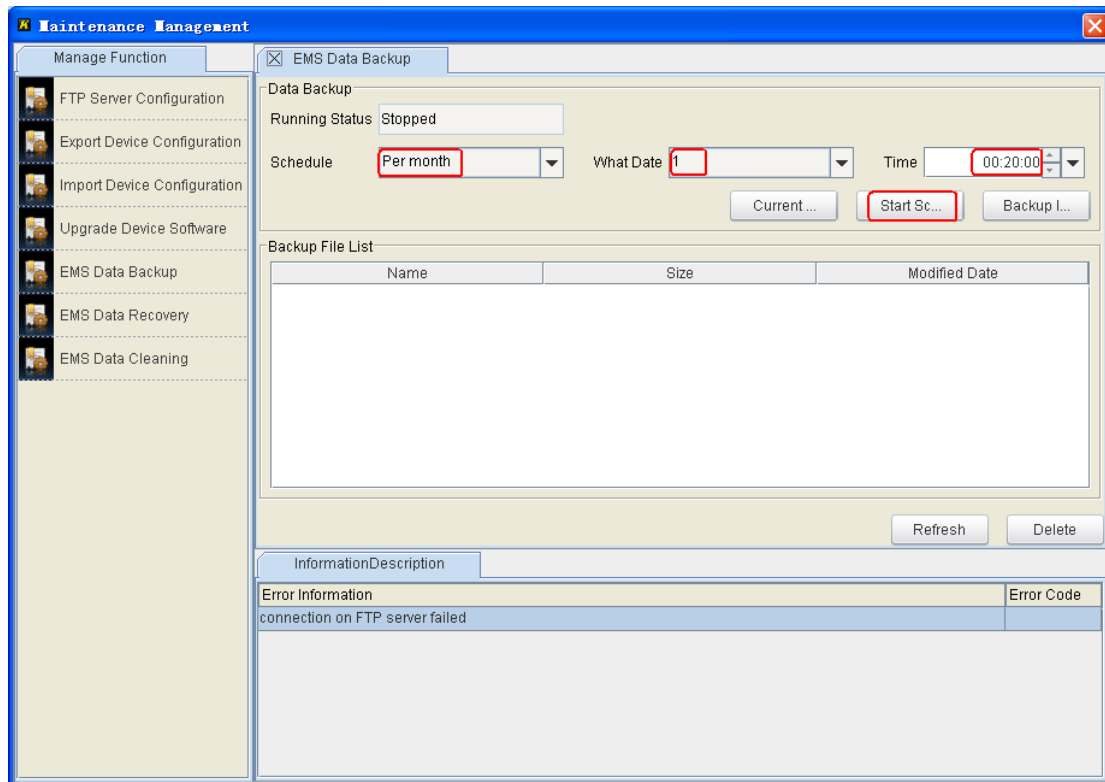


Figure 66 Backing up Data on a Monthly Basis

If you want to modify the periodic backup plan, click <Stop Schedule>, as shown in Figure 67. After setting the new backup plan, click <Start Schedule>. The backup plan is modified successfully.

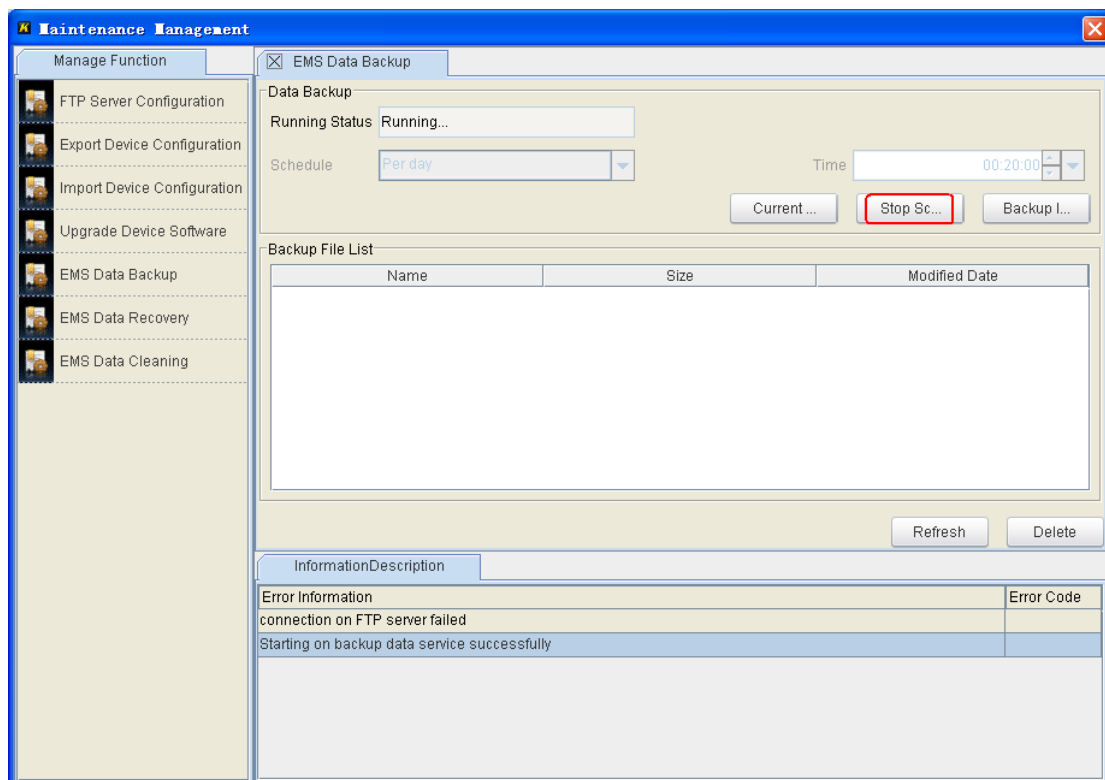


Figure 67 Modifying a Backup Plan

**Caution:**

EMS data is backed up in the system\dist\ftp\root\ftp\data\backup folder of the installation directory of the server.

6.14.6 EMS Data Recovery

Click [Maintenance] → [EMS Data Recovery]. The EMS Data Recovery page is displayed. You can use a local or server file to recover EMS data.

1. Using a Local File to Recover EMS Data

As shown in Figure 68, click <Browse> to select the path of the file to be imported. Click <Import> to import the selected file to the EMS. When "restoring data successfully" is displayed, as shown in Figure 69, data importing is completed.

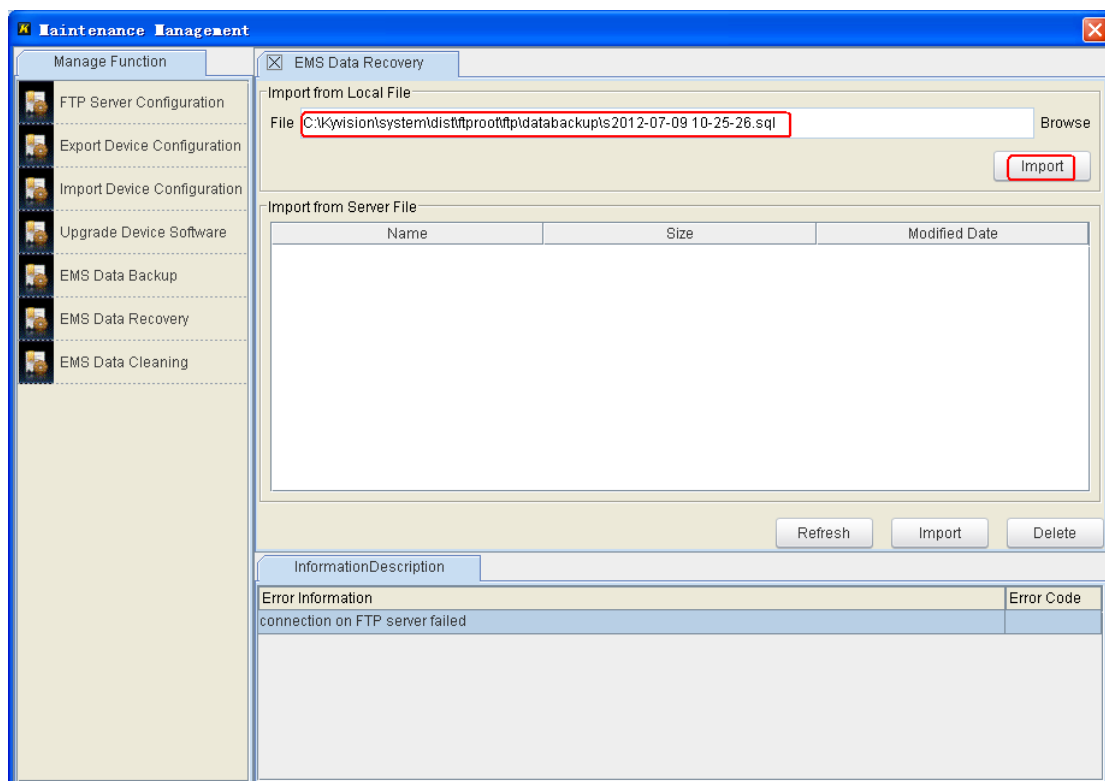


Figure 68 Using a Local File to Recover EMS Data

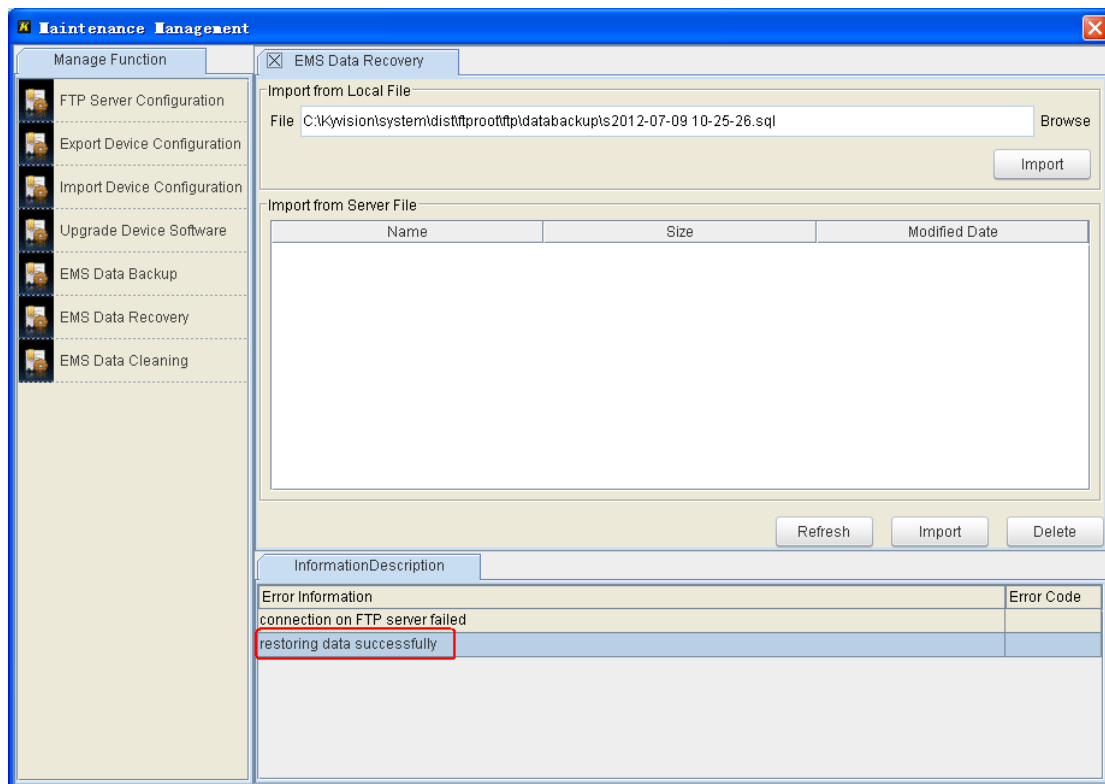


Figure 69 Recovering EMS Data Successfully

2. Using a Server File to Recover EMS Data

After the FTP server is started, EMS data files that have been backed up are displayed in the EMS Data Recovery page. Select the file to be used for recovery. Click <Import>, as shown in Figure 70. When "restoring data successfully" is displayed, the selected file is imported successfully.

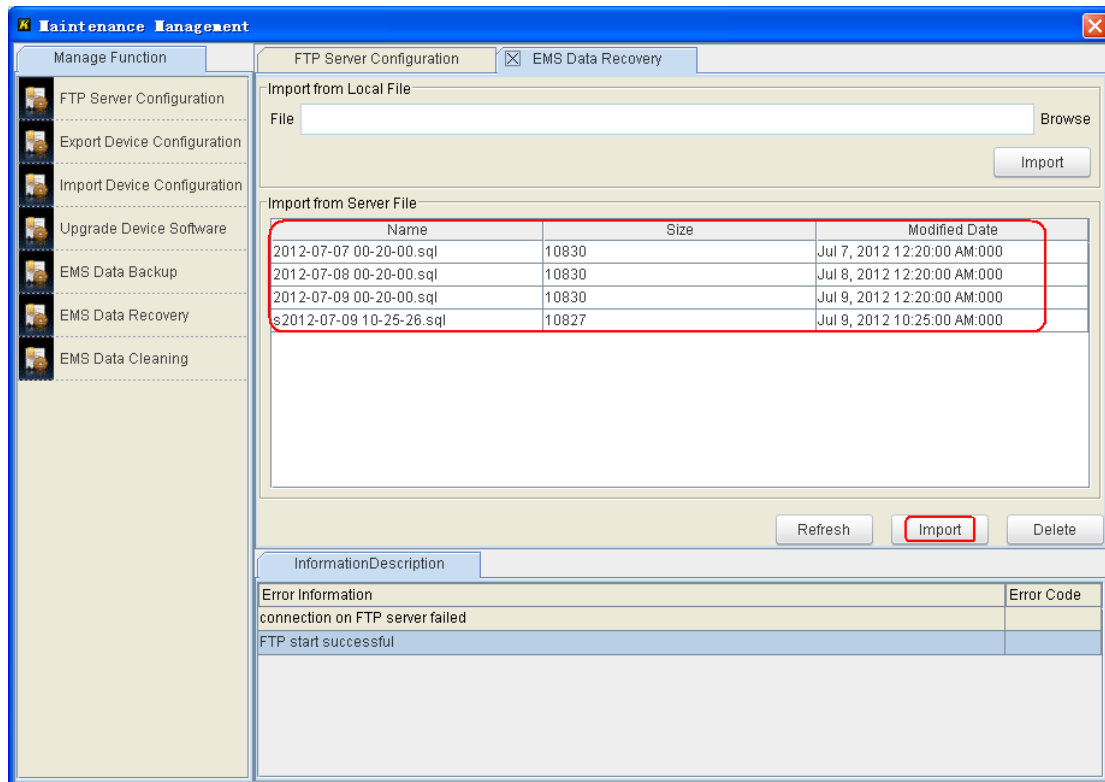


Figure 70 Using a Server File to Recover EMS Data

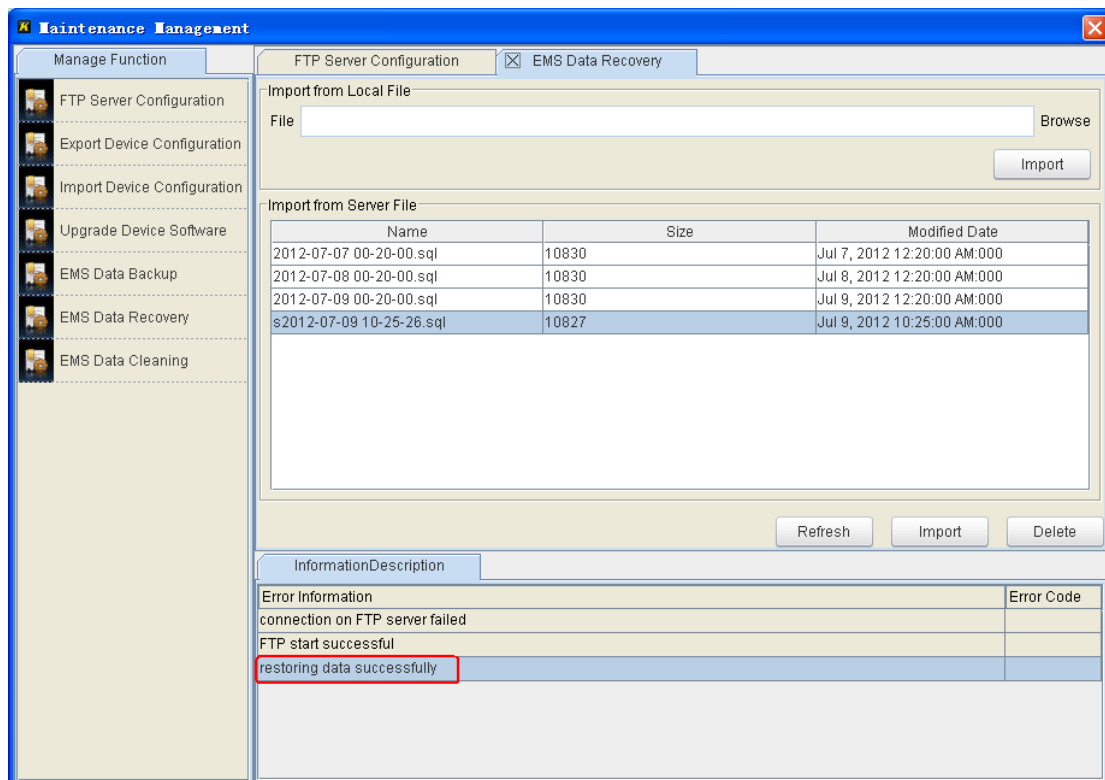


Figure 71 Recovering EMS Data Successfully

**Caution:**

- To use a server file to recover EMS data, you must start the FTP server first.
 - The server file is located in the system\dist\ftp\root\ftp\datbackup folder of the installation directory of the server.
 - After importing is completed, the recovered EMS data takes effect only after the EMS server and client are restarted.
-

6.14.7 EMS Data Cleaning

You can clean growing data such as EMS log and alarm information. The EMS can clean data immediately or periodically.

**Note:**

Before cleaning EMS data, you are recommended to back up EMS data first. Otherwise, the cleaned data cannot be recovered.

1. Immediate Cleaning

As shown in Figure 72, click <Cleaning Immediately>. Data beyond the reserved range ("Days to be reserved" or "RecordCount to be reserved") will be cleaned immediately. If "cleaning data successfully" is displayed, as shown in Figure 73, data cleaning is completed.

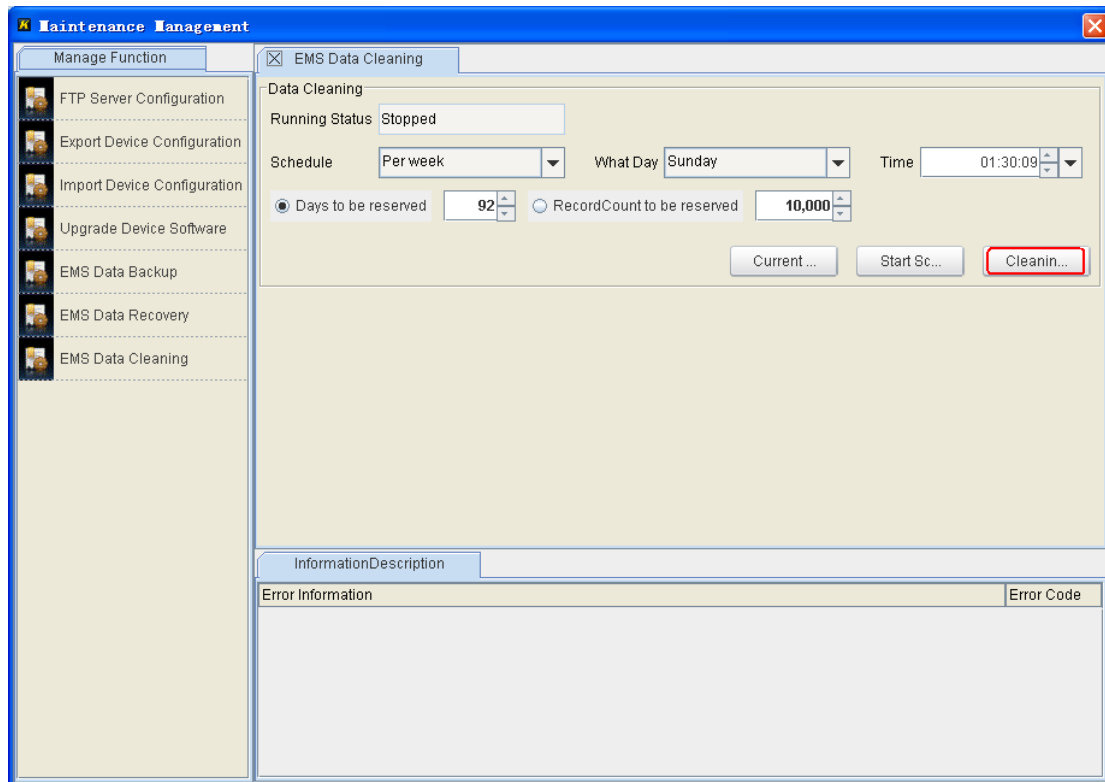


Figure 72 Cleaning EMS Data Immediately

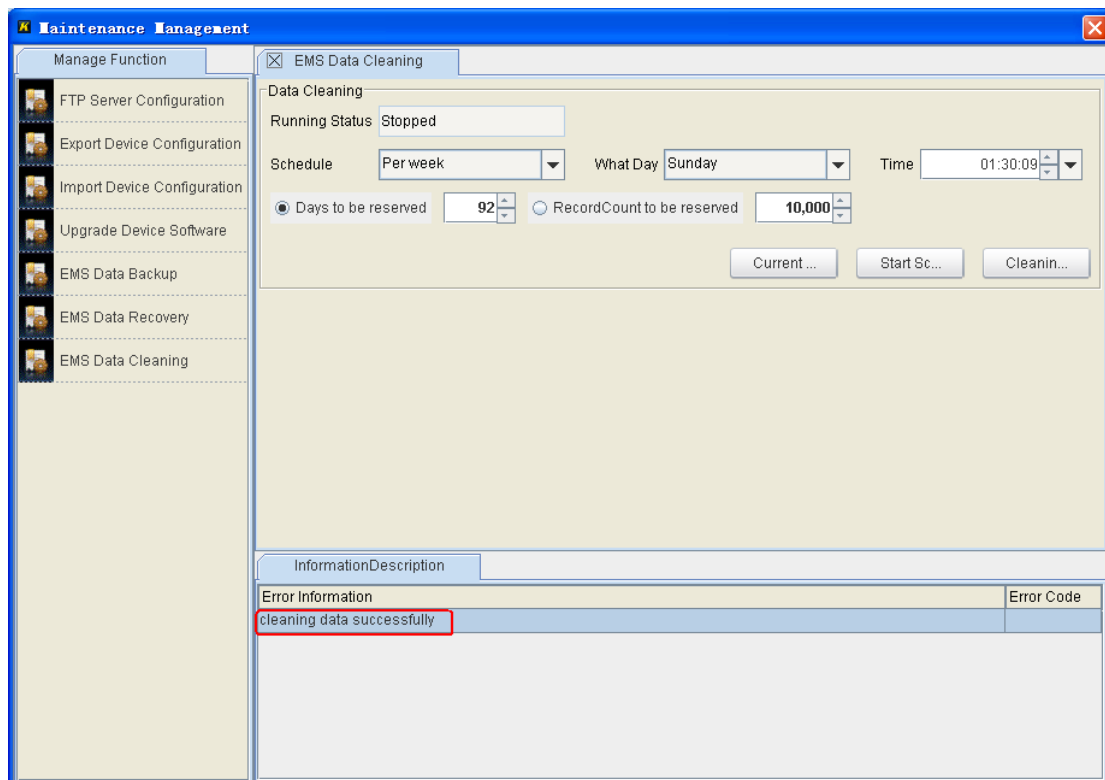


Figure 73 Cleaning EMS Data Successfully

**Caution:**

The days to be reserved are counted from the current time. 24 hours is one day.

2. Periodic Cleaning

You can configure the EMS to automatically clean data on a daily/weekly/monthly basis, as shown in Figure 74 to Figure 76. After setting the plan, click <Start Schedule>. The EMS will automatically clean data according to the plan.

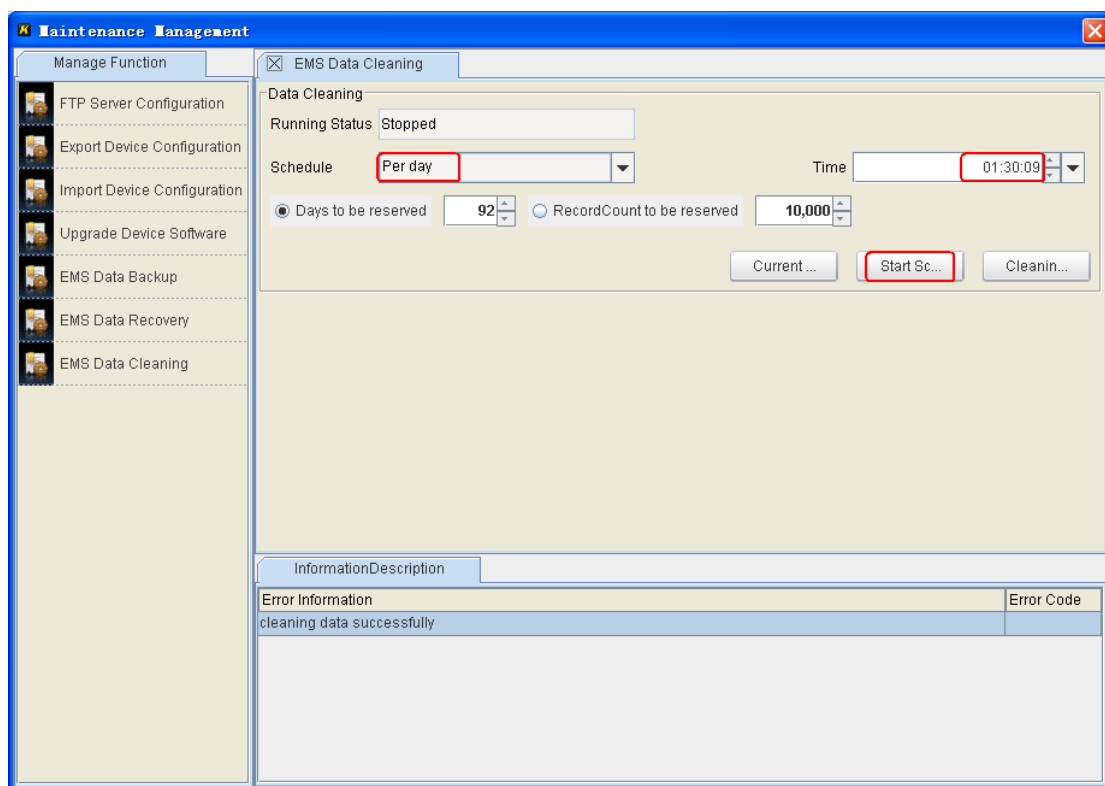


Figure 74 Cleaning EMS Data on a Daily Basis

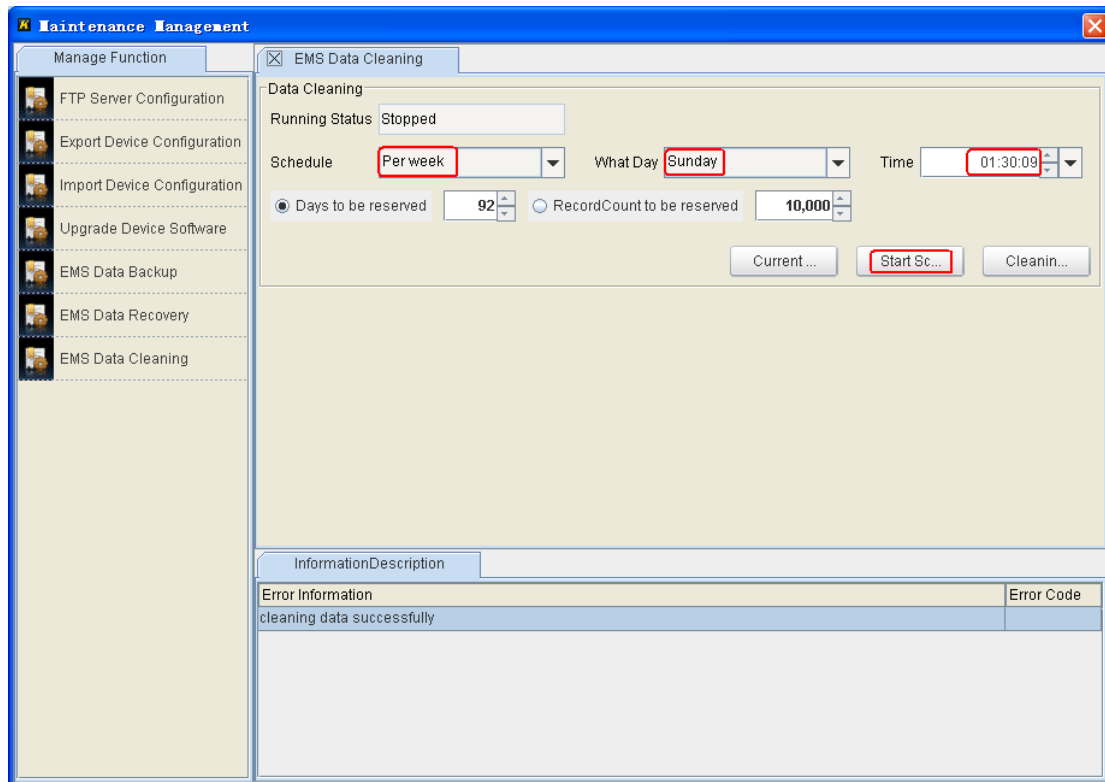


Figure 75 Cleaning EMS Data on a Weekly Basis

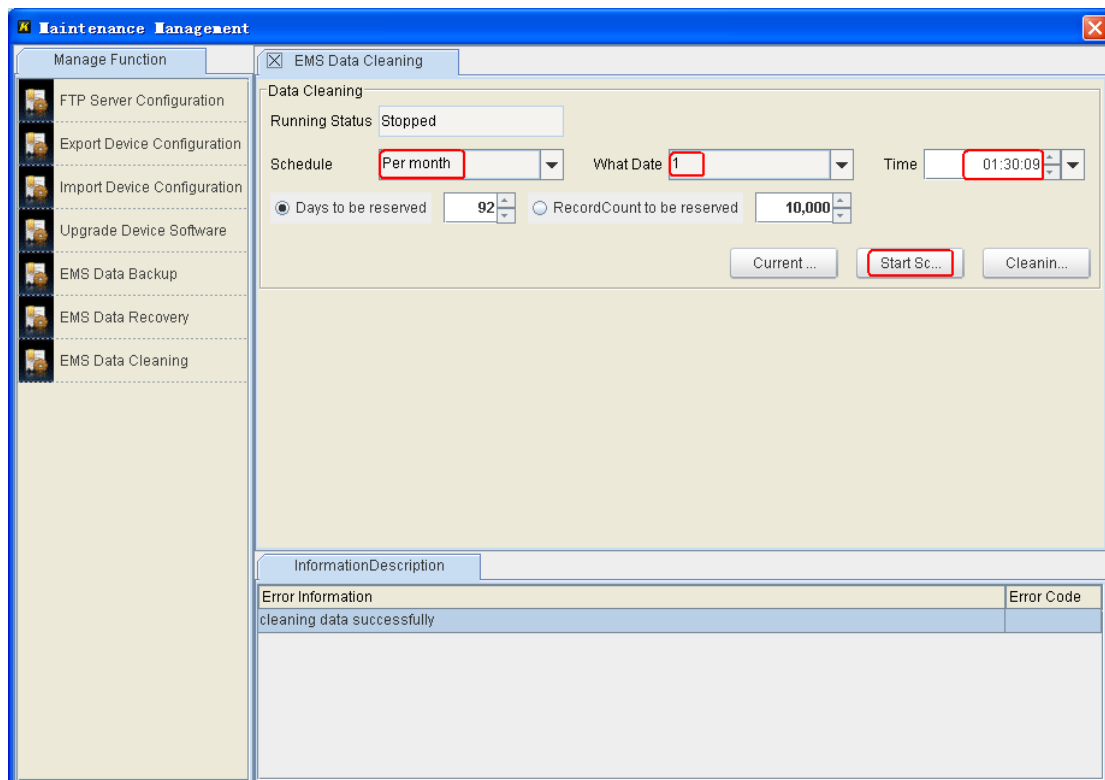


Figure 76 Cleaning EMS Data on a Monthly Basis

If you want to modify the periodic cleaning plan, click <Stop Schedule>, as shown in Figure 77. After setting the new cleaning plan, click <Start Schedule>.

The cleaning plan is modified successfully.

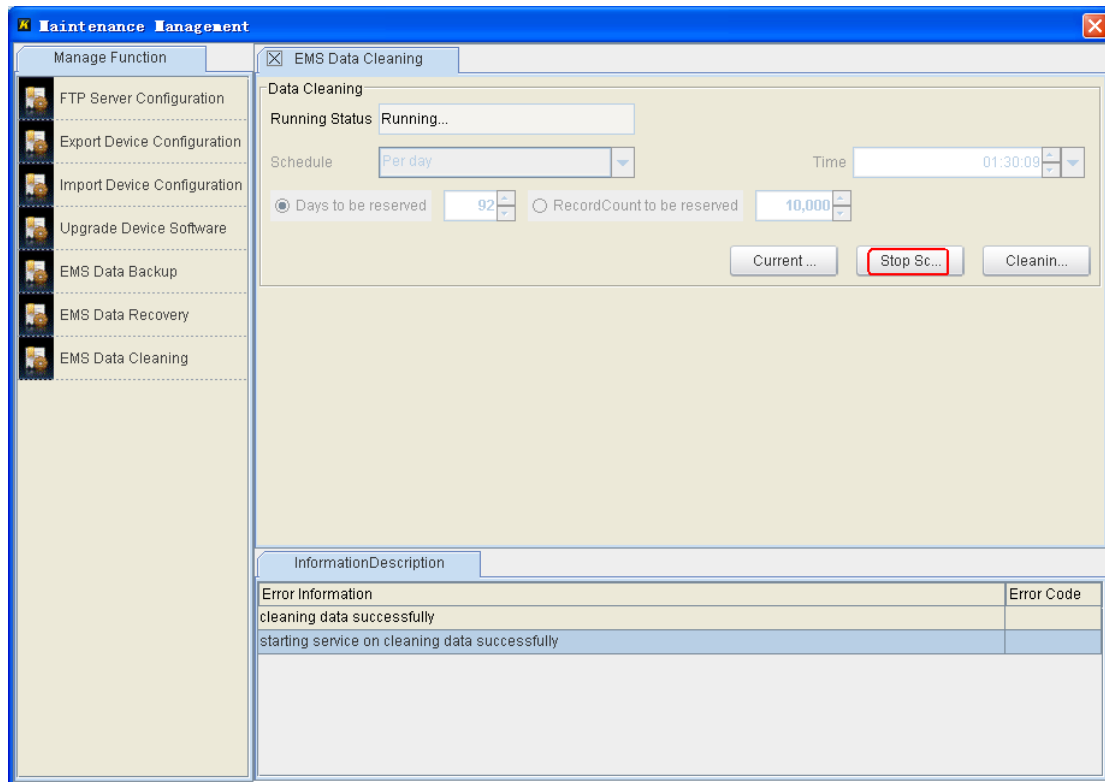


Figure 77 Modifying a Cleaning Plan

7 Rights Management

7.1 User Rights Management

Kyvision provides three roles: administrator, operator, and monitor. An administrator has the right to perform all operations, including device management, alarm management, user management, subnet rights management, and performance monitoring. An operator has the right to perform all operations except user management. A monitor has only the monitoring right. Table 7 lists the rights of the three roles.

Table 7 Comparison of User Rights

Role	Add/Delete	Configure	Set	Automatic	Add/Delete	Acknowledg	Clean an	User	Monitoring
Administrator	√	√	√	√	√	√	√	√	√
Operator	√	√	√	√	√	√	√	X	√
Monitor	X	X	X	X	X	X	X	X	√



Caution:

- A monitor cannot log out of the client. If a monitor wants to log out, it can only use the Task Manager to terminate the program.
- One user cannot log in to two clients at the same time.

7.1.1 User Management

An administrator can manage Kyvision users, including creating or deleting a user, setting user properties, changing the password, and locking or unlocking.

Click [Security] → [EMS User] or click  in the toolbar. The EMS User page is displayed, as shown in Figure 78.

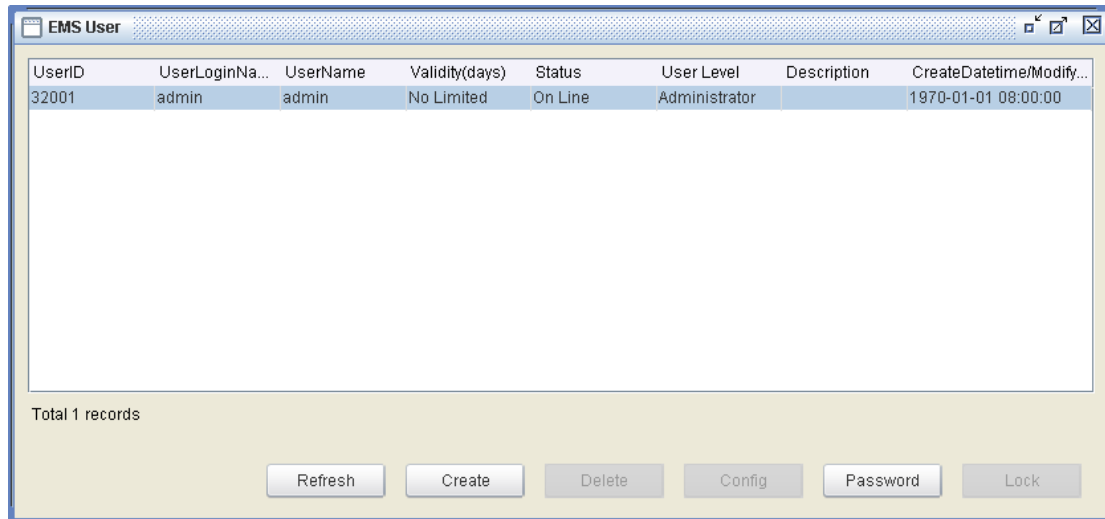


Figure 78 User Management

➤ Click <Create>. The Create User dialog box is displayed, as shown in Figure 79.

The screenshot shows a "Create User" dialog box with the following fields and values:

- Login Name: operator1
- Name: operator1
- Password:
- Confirm Password:
- Password Expiry: 0 days
- Level: Administrator (dropdown menu)
- Email: (empty field)

At the bottom, there are "Confirm" and "Cancel" buttons.

Figure 79 Creating a User

Login Name

Range: 1~20 characters

Password

Range: 5~10 characters

Confirm Password

Enter the password again.

Password Expiry

Range: 0~99999 days

If you enter 0, the password will be valid forever. The password validity starts from the time when it is created. 24 hours is one day.

Level

Options: Administrator/Operator/Monitor

Select the role for the created user. Different roles have differentiated rights.

Email

Bind an email to the current user. The email is used for receiving the alarm notification message.

- Select a user. Click <Delete>. You can delete the user successfully.



Caution:

The user "admin" cannot be deleted.

- Select a user. Click <Config>. The following dialog box is displayed. You can change the level, password validity, and email of the user.

The screenshot shows a Windows-style dialog box titled "User operator1 : Properties". It contains the following fields and controls:

- Login Name:** A text box containing "operator1".
- Name:** A text box containing "operator1".
- Level:** A dropdown menu with "Operator" selected.
- Status:** A dropdown menu with "Off Line" selected.
- Password Expiry:** A text box containing "0" followed by the text "days".
- Email:** An empty text box.
- Buttons:** "Update" and "Cancel" buttons at the bottom right.

Figure 80 Setting User Properties

**Caution:**

The properties of the user "admin" cannot be changed.

➤ Select a user. Click <Password>. The Change Password dialog box is displayed, as shown in Figure 81 and Figure 82. To change the password of the user "admin", you need to enter the old password. To change the password of another user, the old password is not required.

The dialog box is titled "User admin : Change Pa...". It contains four input fields: "Login Name" with the value "admin", "Old Password" with five dots, "New Password" with five dots, and "Confirm Password" with five dots. At the bottom are "Confirm" and "Cancel" buttons.

Figure 81 Changing the Password of "admin"

The dialog box is titled "User operator1 : Chang...". It contains four input fields: "Login Name" with the value "operator1", "Old Password" which is empty, "New Password" with seven dots, and "Confirm Password" with seven dots. At the bottom are "Confirm" and "Cancel" buttons.

Figure 82 Changing the Password of another User

➤ Select a user. Click <Lock> or <Unlock>. You can lock or unlock the user accordingly. If the user is locked, <Unlock> is displayed. If the user is not locked, <Lock> is displayed. A locked user cannot log in to the client.

**Caution:**

The user "admin" cannot be locked. Users with the same rights cannot lock each other.

7.2 Subnet Rights Management

A network may involve multiple subnets and management users distributed at different locations. An administrator or operator has the right to grant monitoring right to a monitor.



Click [Configuration] → [Subnet Right Manager] or click in the toolbar.

The Configuration Monitor dialog box is displayed, as shown in Figure 83.

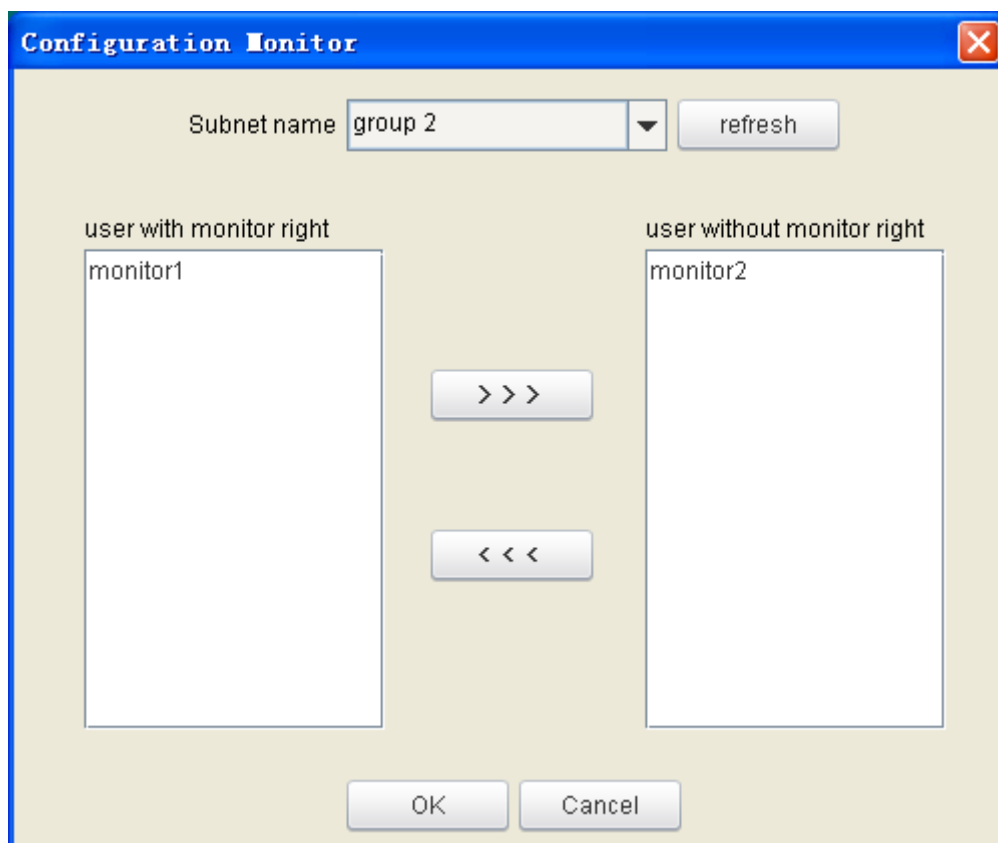


Figure 83 Configuring Monitoring Staff

Select a subnet and a user from the user without monitor right group box. Click

< < < > to add the user to the user with monitor right group box. Then

the user can monitor the specified subnet. Select a user from the user with monitor right group box. Click <  > to add the user to the user without monitor right group box. Then the user has no right to monitor the specified subnet.

7.3 Operation Rights Management

When the client serves as the monitoring interface, you can lock the client either manually or at scheduled time to prevent illegitimate users from operating the client.

1. Manual locking

Click [System] → [Lock Client] or click  in the toolbar. The client is locked manually and the following dialog box is displayed.

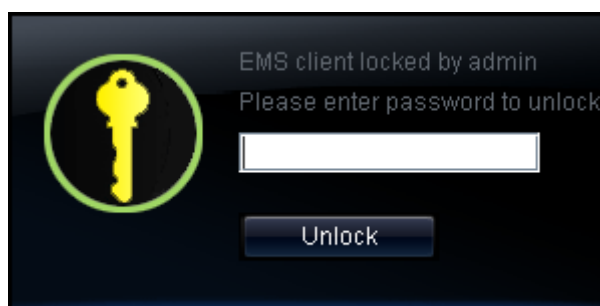


Figure 84 Locking the Client

Enter the login password of the current user in the text box. The system is unlocked and you can perform operations.

2. Scheduled locking

For scheduled locking, the timer starts from the last operation. If no operation is performed within the specified time, the client locking dialog box is displayed, as shown in Figure 84. The unlocking method is the same as that for manual locking.

Click [System] → [Auto-lock Config]. The submenu is displayed. You can select 3 minutes later, 5 minutes later, 10 minutes later, or Never auto-lock as needed.

8 Alarm Management

8.1 Overview

Alarm information includes:

1. Alarm information reported by managed devices.
2. Alarm information detected by Kyvision during polling.

With alarm management, you can record and process the alarms of all managed devices. To be specific, Kyvision supports real-time alarm monitoring, alarm bell, alarm acknowledgement, alarm filtering, alarm information query, and alarm information export.



Caution:

- A device can send Trap packets to the EMS only if SNMP and Trap are enabled on the device.
- The EMS can receive and detect the alarms of a device only if the port/power alarm function is enabled on the device.

8.2 Alarm Levels and Categories

Alarm levels, indicating the severity of alarms, include critical, major, minor, and warning in descending order. Alarm levels are identified by the system automatically.

Table 8 Alarm Levels and Categories

Alarm Level	Alarm Category	Description	Remarks
Critical Alarm	Device communication anomaly	The alarm is generated when the EMS fails to communicate with a device.	
	Power alarm	After the function is enabled, an alarm is generated when one power supply fails and the other power supply works properly.	Applicable to dual power

			supply only
	Power failure alarm	The alarm is generated when a device fails to work due to power failure.	
	Temperature alarm	After the function is enabled, an alarm is generated when the switch temperature exceeds the specified threshold.	
	IP conflict alarm	After the function is enabled, an alarm is generated when the IP address of a switch conflicts with that of another device on the network.	
	MAC conflict alarm	After the function is enabled, an alarm is generated when the MAC address of a switch conflicts with that of another device on the network.	
Major Alarm	Port alarm	After the function is enabled, an alarm is generated when the status of a port changes to Link Down.	
	Ring alarm	After the function is enabled, an alarm is generated when a ring is open.	
	AC/DC alarm		
	Port traffic alarm	After the function is enabled, an alarm is generated when the traffic of a port exceeds the specified threshold.	
	CRC error alarm	After the function is enabled, an alarm is generated when the number of CRC errors of a port exceeds the specified threshold.	
Minor Alarm	CPU and memory usage alarm	After the function is enabled, an alarm is generated when the CPU or memory usage exceeds the specified threshold.	

8.3 Alarm Modes

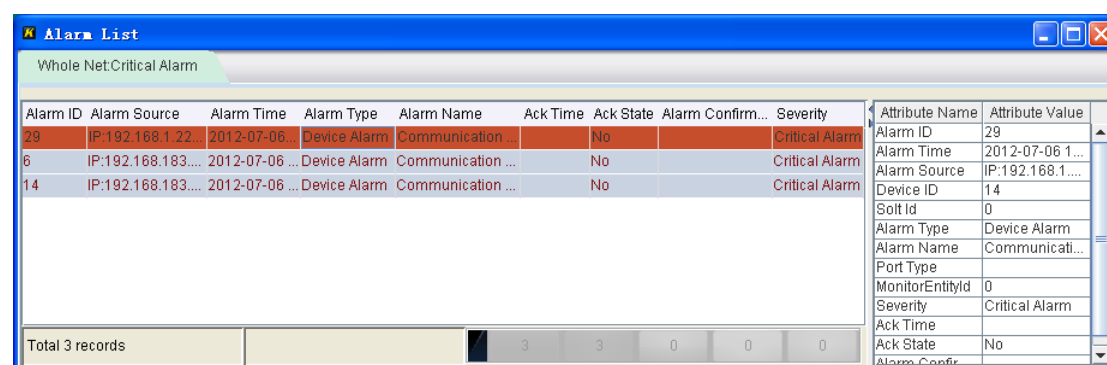
The EMS can indicate alarm information in the following ways:

- Real-time alarm display: Kyvision displays alarm information in a table in real time. This allows users to know the running status of devices in real time. Alarms are displayed in different colors according to their levels. Critical ones are displayed in red, major ones in orange, and cleared alarms are displayed in green.
- Devices in the topology are displayed according to their highest active alarm levels. For example, devices whose highest active alarm level is critical are displayed in red.
- Devices/Subnets in the navigation tree are displayed according to their highest active alarm levels. For example, devices/subnets whose highest active alarm level is major are displayed in orange.
- When alarm bell is enabled (click [Alarm] → [Alarm Bell Config] → [Turn on]), Kyvision will ring bells to notify user if an alarm occurs.

8.4 Alarm List

8.4.1 Alarm Level-based Alarm List

Click a button in the Alarm Statistics Bar. The list of all alarms of the level is displayed. For example, Figure 85 shows the details about all critical alarms.



Alarm ID	Alarm Source	Alarm Time	Alarm Type	Alarm Name	Ack Time	Ack State	Alarm Confirm...	Severity
29	IP:192.168.1.22...	2012-07-06 ...	Device Alarm	Communication ...		No		Critical Alarm
6	IP:192.168.183....	2012-07-06 ...	Device Alarm	Communication ...		No		Critical Alarm
14	IP:192.168.183....	2012-07-06 ...	Device Alarm	Communication ...		No		Critical Alarm

Attribute Name	Attribute Value
Alarm ID	29
Alarm Time	2012-07-06 1...
Alarm Source	IP:192.168.1...
Device ID	14
Soft Id	0
Alarm Type	Device Alarm
Alarm Name	Communicati...
Port Type	
MonitorEntityId	0
Severity	Critical Alarm
Ack Time	
Ack State	No
Alarm Confir...	

Total 3 records

Figure 85 Critical Alarms — Alarm List

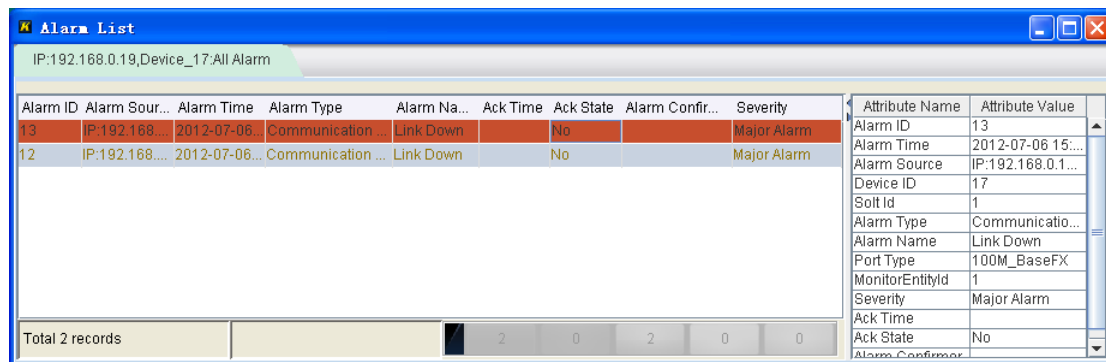
Select one or multiple alarms. Right-click the selected alarm(s). Then you can select or deselect all alarms in the page, or acknowledge or delete the selected

alarm(s).

8.4.2 Alarm Status-based Alarm List

1. Alarm List of a Single Device

Right-click a switch in the network topology area or navigation tree, and select [All Alarms]. The details about all active alarms of the switch are displayed, as shown in Figure 86.



Alarm ID	Alarm Sour...	Alarm Time	Alarm Type	Alarm Na...	Ack Time	Ack State	Alarm Confir...	Severity
13	IP:192.168...	2012-07-06...	Communication...	Link Down		No		Major Alarm
12	IP:192.168...	2012-07-06...	Communication ...	Link Down		No		Major Alarm

Attribute Name	Attribute Value
Alarm ID	13
Alarm Time	2012-07-06 15:...
Alarm Source	IP:192.168.0.1...
Device ID	17
Soft Id	1
Alarm Type	Communicatio...
Alarm Name	Link Down
Port Type	100M_BaseFX
MonitorEntityId	1
Severity	Major Alarm
Ack Time	
Ack State	No

Figure 86 Alarm List of a Specified Device

Select one or multiple alarms. Right-click the selected alarm(s). Then you can select or deselect all alarms in the page, or acknowledge or delete the selected alarm(s).



Caution:

Kyvision allows you to view only the alarms of switches automatically identified by the EMS.

2. Alarm List of All Devices in a Subnet

Right-click a subnet in the network topology area or navigation tree, and select [Fault Management]. The Alarm Management page for the subnet is displayed. By default, the list of active alarms of the subnet is displayed, as shown in Figure 87.

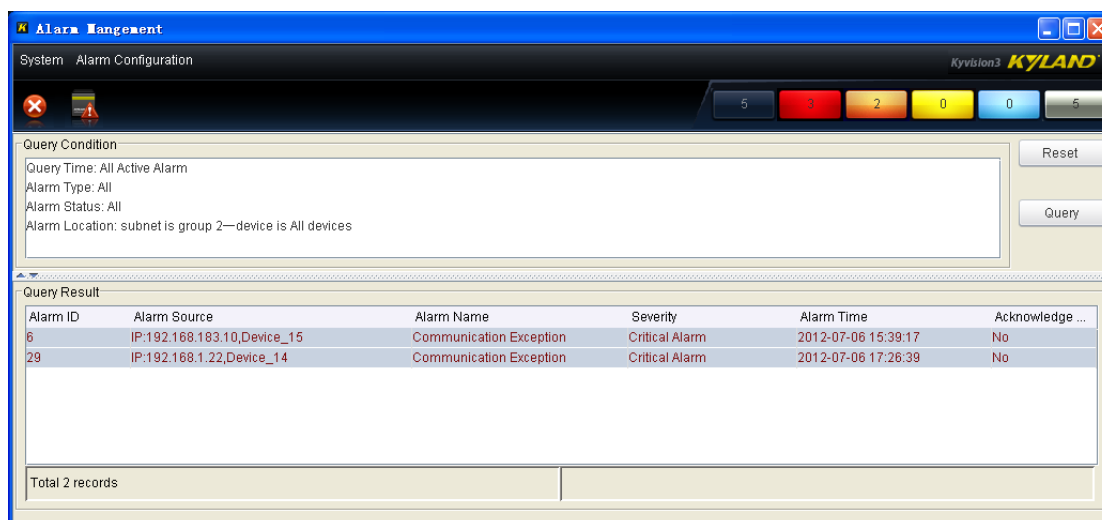


Figure 87 Alarm List of a Subnet

3. Alarm List of All Devices in All Subnets

- Click [Alarm] → [Live Alarm Table] or  in the toolbar. The list of active alarms of all subnets is displayed, as shown in Figure 88.

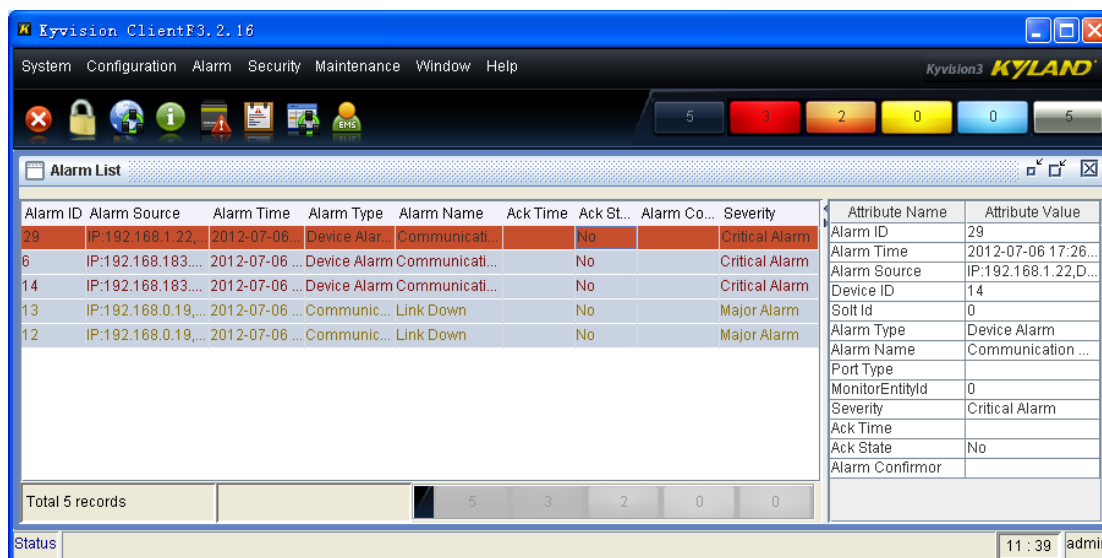


Figure 88 Alarm List of All Subnets

Select one or multiple alarms. Right-click the selected alarm(s). Then you can select or deselect all alarms in the page, or filter, acknowledge, or delete the selected alarm(s).

- Click [Alarm] → [Alarm Management] or  in the toolbar. The Alarm Management page for all subnets is displayed. By default, the list of active

alarms of all subnets is displayed, as shown in Figure 89.

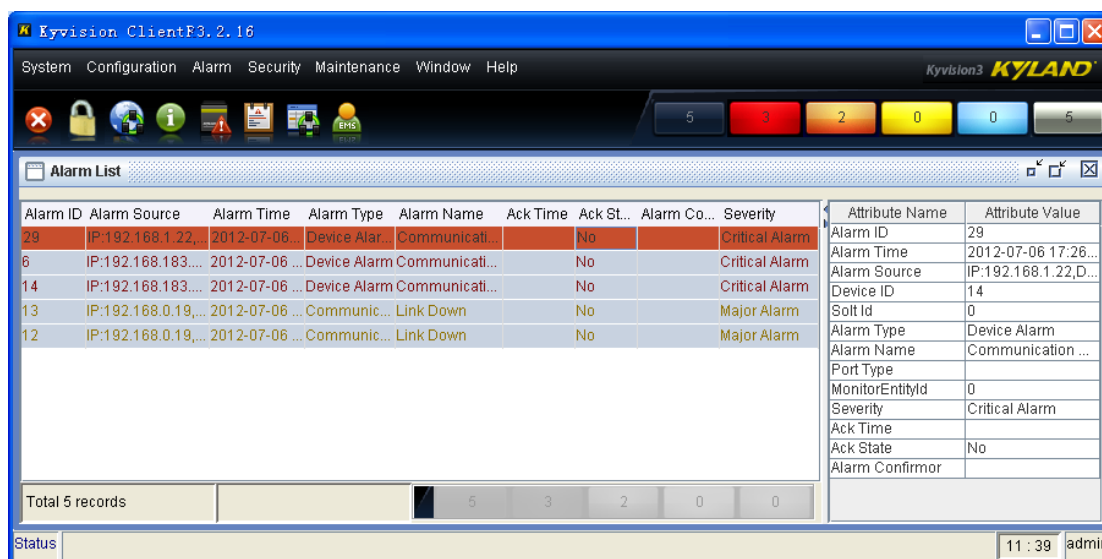


Figure 89 Alarm List of All Subnets

8.5 Alarm Query and Export

You can query both active and historical alarms. Active alarms indicate the ones in active state and not cleared yet. Historical alarms indicate all generated alarms. By setting query conditions, the administrator can view only desired alarm information and export the information to the local device.

1. Querying and Exporting Alarms of a Subnet

Right-click a subnet in the network topology area or navigation tree. Select [Fault Management]. The Alarm Management page of the subnet is displayed, as shown in Figure 90. Click <Reset>. The Reset Query Condition dialog box is displayed, as shown in Figure 91.

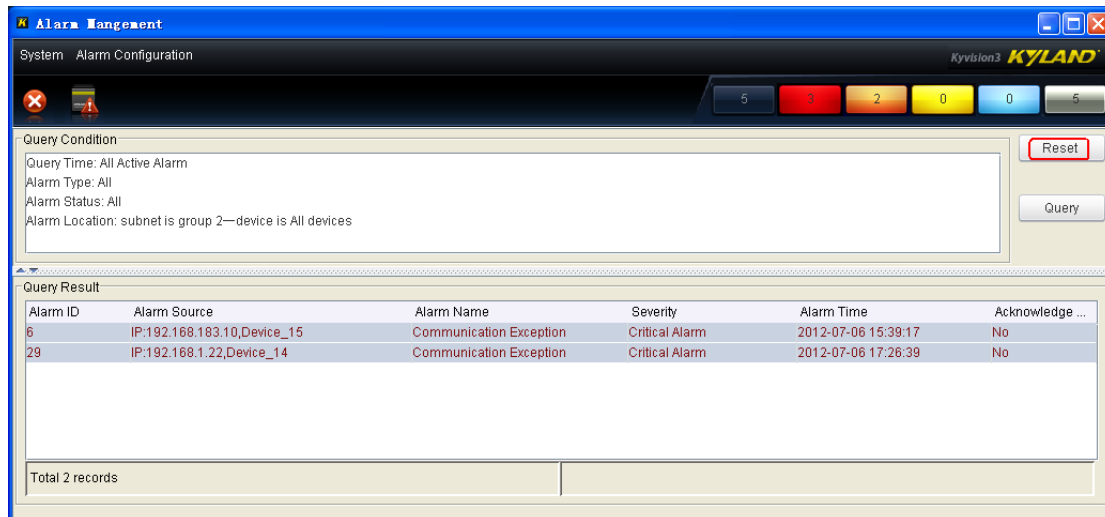


Figure 90 Alarm Management of a Subnet

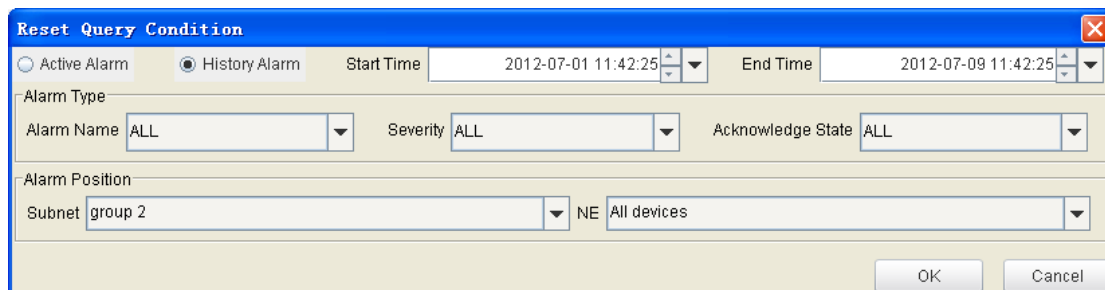


Figure 91 Setting Query Conditions

Set the alarm start and end time, name, level, acknowledgement state, subnet name, and device name. Click <OK>. The qualified alarms are displayed, as shown in Figure 92.

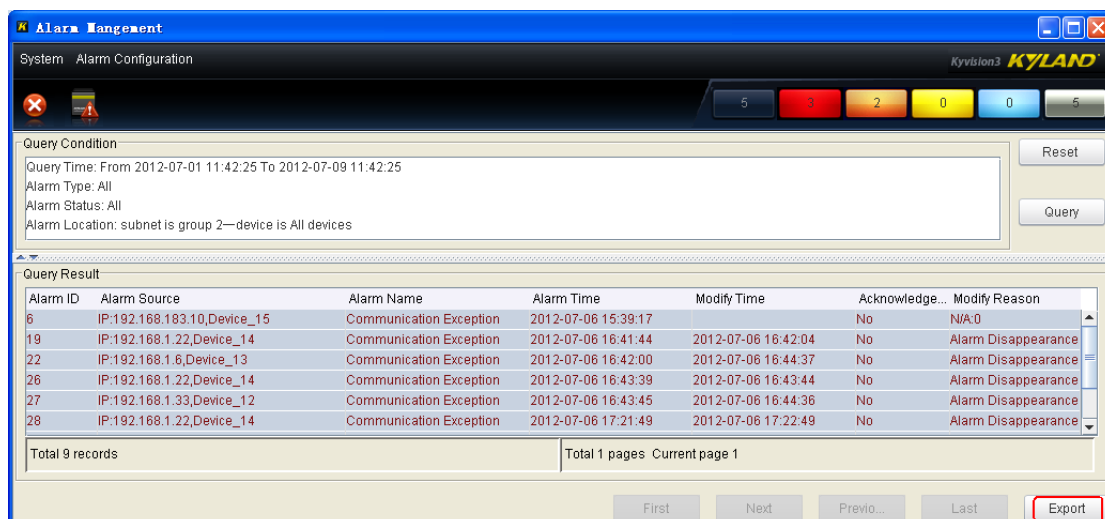


Figure 92 Alarm Query Result of a Subnet

Click <Export>. You can export the query result to a .xls file on the local device for fault locating.

**Caution:**

The relationship among query conditions is logical "AND".

2. Querying and Exporting Alarms of All Subnets



Click [Alarm] → [Alarm Management] or  in the toolbar. The Alarm Management page for all subnets is displayed, as shown in Figure 93. Click <Reset>. The Reset Query Condition dialog box is displayed, as shown in Figure 91. Set the alarm start and end time, name, level, acknowledgement state, subnet name, and device name. Click <OK>. The qualified alarms are displayed, as shown in Figure 92.

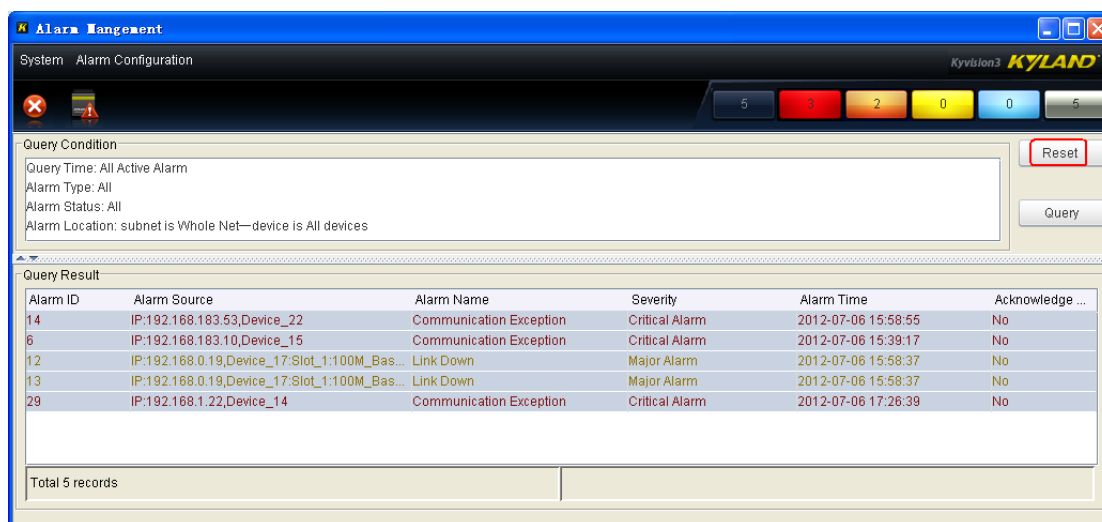


Figure 93 Alarm Management of All Subnets

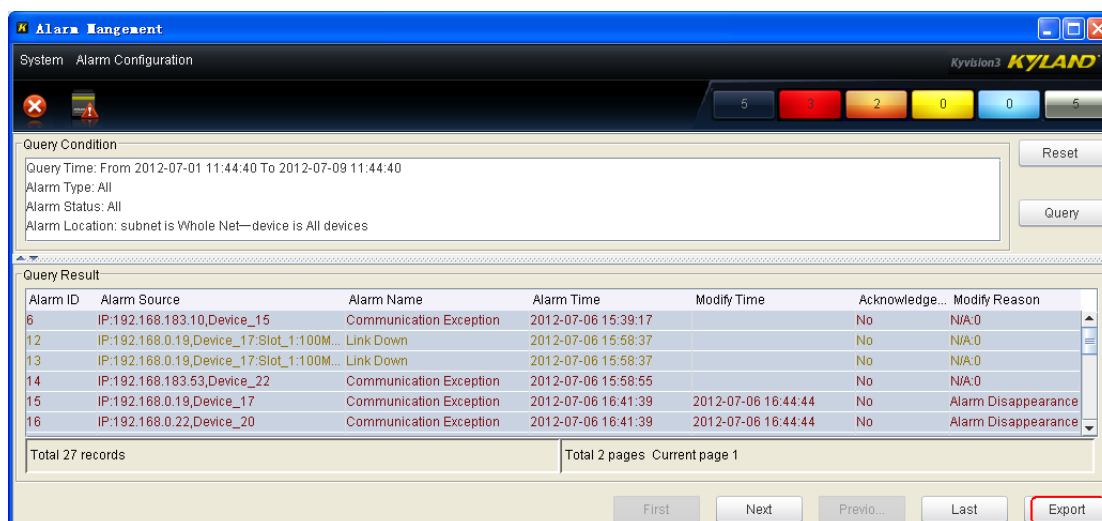


Figure 94 Alarm Query Result

Click <Export>. You can export the query result to a .xls file on the local device for fault locating.



Caution:

The relationship among query conditions is logical "AND".

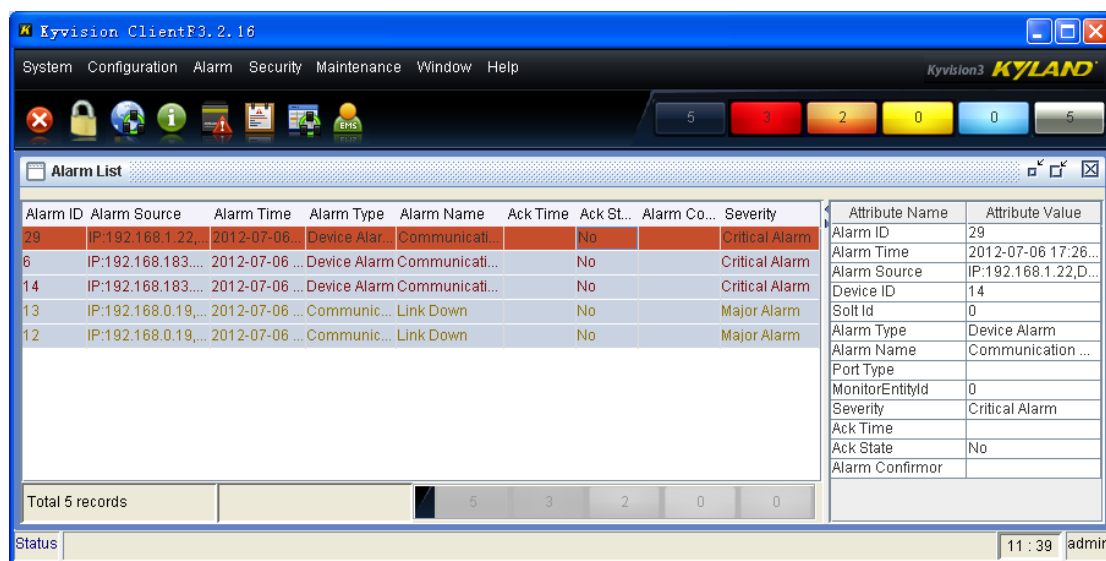
8.6 Alarm Filtering

The alarm filtering function filters the currently active alarms. With the alarm filtering function, you can obtain the desired alarm information in real time to manage network with high efficiency.

You can set three filtering conditions: device name, alarm level, and acknowledgement state.



Click [Alarm] → [Live Alarm Table] or  in the toolbar. The list of active alarms of all subnets is displayed, as shown in Figure 95.



Alarm ID	Alarm Source	Alarm Time	Alarm Type	Alarm Name	Ack Time	Ack St...	Alarm Co...	Severity
29	IP:192.168.1.22...	2012-07-06	Device Alar...	Communicati...		No		Critical Alarm
6	IP:192.168.183....	2012-07-06	Device Alarm Communicati...			No		Critical Alarm
14	IP:192.168.183....	2012-07-06	Device Alarm Communicati...			No		Critical Alarm
13	IP:192.168.0.19,...	2012-07-06	Communic...	Link Down		No		Major Alarm
12	IP:192.168.0.19,...	2012-07-06	Communic...	Link Down		No		Major Alarm

Attribute Name	Attribute Value
Alarm ID	29
Alarm Time	2012-07-06 17:26...
Alarm Source	IP:192.168.1.22,D...
Device ID	14
Soft Id	0
Alarm Type	Device Alarm
Alarm Name	Communication ...
Port Type	
MonitorEntityId	0
Severity	Critical Alarm
Ack Time	
Ack State	No
Alarm Confirmer	

Figure 95 Alarm List of All Subnets

Right-click an alarm record and select [Filter Alarm]. The Alarm Query dialog box is displayed, as shown in Figure 96.

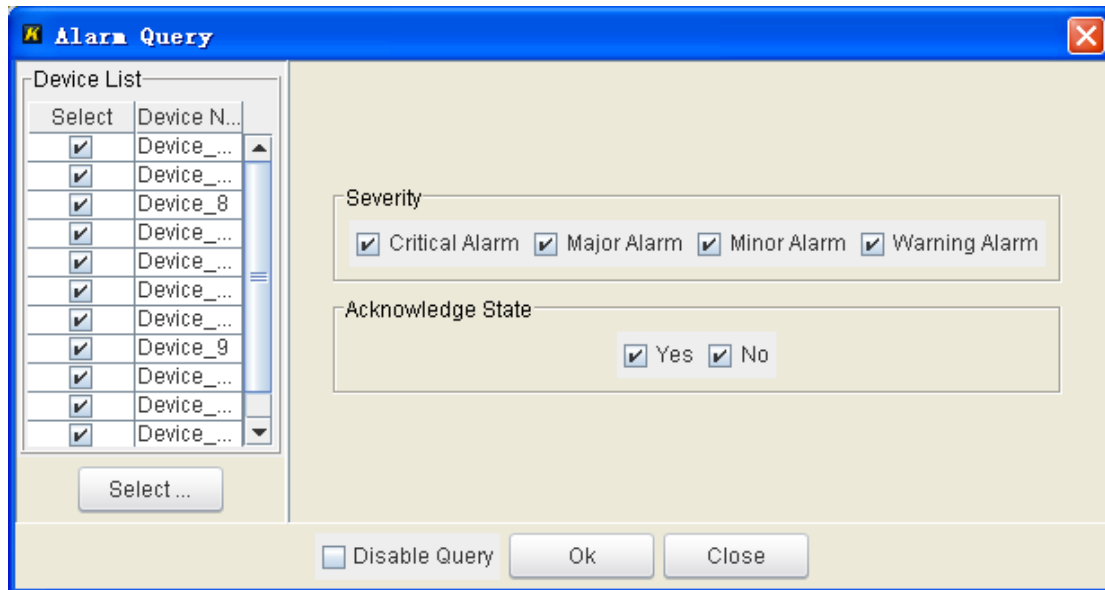


Figure 96 Setting Alarm Filtering Conditions

Deselect undesired conditions. Click <OK>. The unqualified alarms are filtered out. After [Disable Query] is selected, the filtering conditions become invalid. All active alarms are displayed in the alarm list.

8.7 Alarm Acknowledgement

Alarm acknowledgement stops ringing an alarm. After an alarm is acknowledged, the acknowledgement information is added to the database.



Caution:

You can acknowledge only active alarms. Historical alarms cannot be acknowledged.

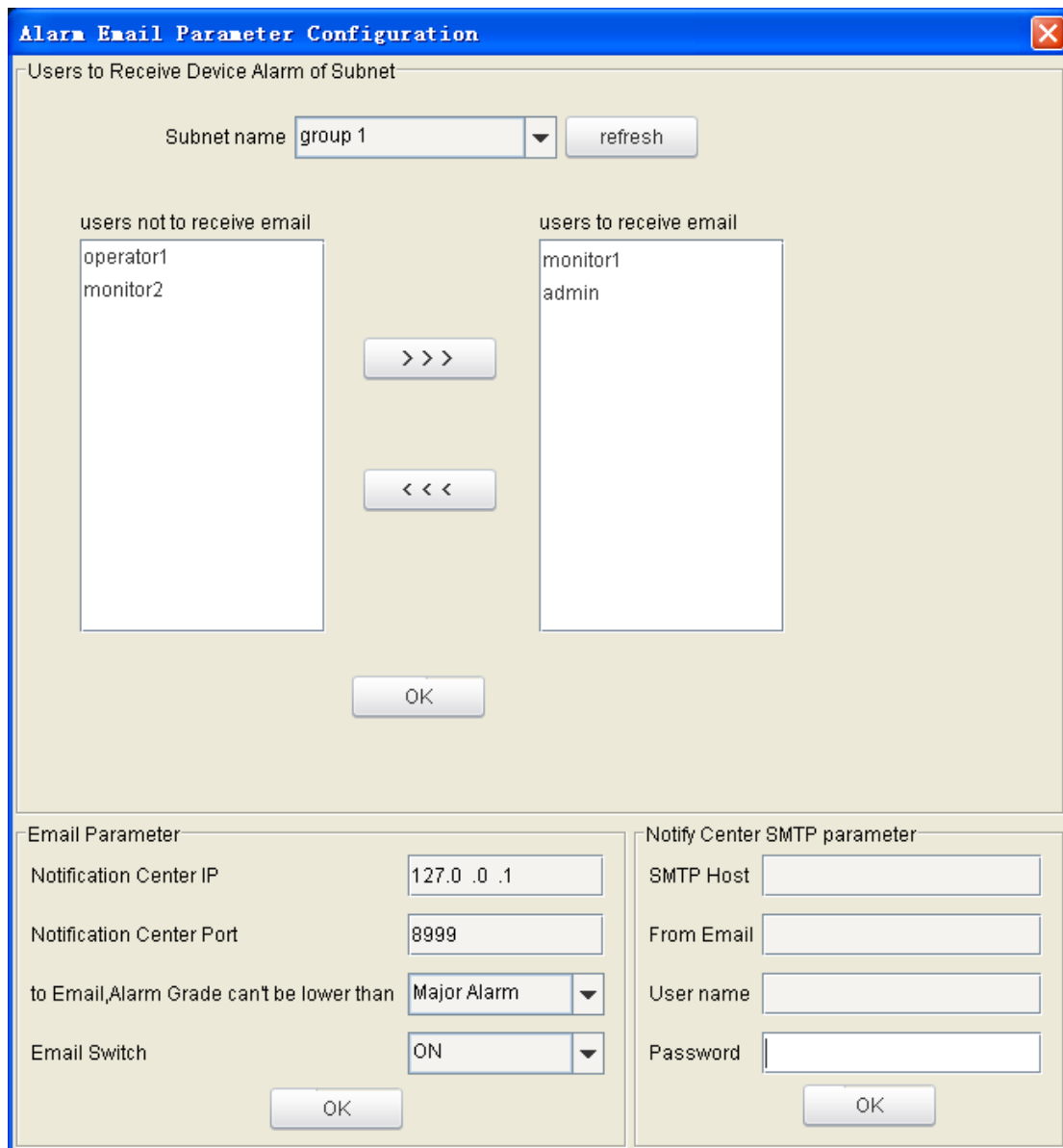
In the alarm list in Figure 85, Figure 86, or Figure 88, select one or multiple unacknowledged alarms. Right-click the selected alarm(s), and select [Acknowledge Alarm].

8.8 Alarm Notification by Email

With the function, you can send alarm (generation/clearing) information to the email bound to the user, so that the maintenance personnel can be notified of alarm information remotely.

Click [Configuration] → [Alarm Email Parameter Configuration]. The following

page is displayed.



The dialog box is titled "Alarm Email Parameter Configuration". It contains two main sections: "Users to Receive Device Alarm of Subnet" and "Email Parameter".

Users to Receive Device Alarm of Subnet:

- Subnet name: group 1 (dropdown menu)
- refresh button
- users not to receive email list: operator1, monitor2
- users to receive email list: monitor1, admin
- >>> button (move users from 'not to receive' to 'to receive')
- <<< button (move users from 'to receive' to 'not to receive')
- OK button

Email Parameter:

- Notification Center IP: 127.0.0.1
- Notification Center Port: 8999
- to Email, Alarm Grade can't be lower than: Major Alarm (dropdown menu)
- Email Switch: ON (dropdown menu)
- OK button

Notify Center SMTP parameter:

- SMTP Host
- From Email
- User name
- Password
- OK button

Figure 97 Alarm Email Parameter Configuration

Select a subnet. Select users from the users not to receive email group box and click  to add the users to the users to receive email group box. Then the emails of the users can receive alarm notifications. You can also select users from the users to receive email group box and click  to add the users to the users not to receive email group box. Then the users will not receive alarm notifications.

Notification Center IP

Format: A.B.C.D

Default: 127.0.0.1

Function: Set the IP address of the notification center.



Note:

- After installation is completed, both the server and the client contain a notification center. The IP address determines which notification center is being used. If the IP address is set to 127.0.0.1, the notification center of the server is used.
 - All the notification centers mentioned in this document refer to valid ones.
-

Notification Center Port

Range: 8901~60000

Default: 8999

Function: Configure the number of port on the EMS server for communicating with the notification center. The notification center listens to the port and receives alarm emails. Thus, the port number must be identical with that in the notify.xml file of the notification center.



Caution:

- The notify.xml file is located in the Kyvision\system\dist\notifycenter\conf folder of the installation directory of the notification center
 - After the port number is changed, you need to restart the client where the notification center resides to make the new port number take effect.
-

to Email, Alarm Grade can't be lower than

Options: Critical Alarm/Major Alarm/Minor Alarm/Warning Alarm

Function: Configure the lowest alarm level for sending an email. Emails will be sent for all the alarms of the configured level and a higher level.

Description: The alarm levels include critical, major, minor, and warning in

descending order.

Email Switch

Options: ON/OFF

Default: OFF

Function: Enable or disable the email sending function.



Caution:

The email parameters of the last client are valid. They are saved in the Kyvision\system\dist\resources\config\EmailCfg.xml file of the installation directory of the server.

Notify Center SMTP parameter

Function: Set the SMTP server, user name and password for server login, and local email address. Only the email address specified on the client where the notification center resides can send alarm notification emails.

9 Log Management

Logs fall into two types: operation log and system running log. The operation log records the operations of all users, making operations traceable. The running log records the system running information. Log management enables you to record query, and export logs.

Click [Alarm] → [Operation Log]/[Running Log]. The Operation Log Query/Running Log Query page is displayed, as shown in Figure 98 and Figure 99. Set query conditions and click [Query]. The logs meeting these conditions are displayed, as shown in Figure 100 and Figure 101.

Operation Log Query

Condition

User: User admin

Type: Source Device Config, Object Device, Type

Location: Device, Slot, Port

Time: From 2012-07-17 00:00:00 To 2012-07-23 10:30:59

Query

Result

User	Source	Type	Content	Generate Time
------	--------	------	---------	---------------

First P... Previo... Next P... Last P... Export Close

Figure 98 Operation Log Query

Running Log Query

Condition

Type

Source: EventTypes:

Location

Device: Slot: Port:

Time

From: To:

Result

Source	Type	Content	Generate Time
--------	------	---------	---------------

First P... Previo... Next P... Last P... Export Close

Figure 99 Running Log Query

Operation Log Query

Condition

User

User: Type

Source: Object: Type:

Location

Device: Slot: Port:

Time

From: To:

Result

User	Source	Type	Content	Generate Time
admin	Device_1	Device Create	Create Device_1,Type:Other...	2012-07-23 10:19:06
admin	Device_1	Device Delete	Delete Device_1	2012-07-23 10:19:08
admin	Device_2	Device Create	Create Device_2,Type:SICO...	2012-07-23 10:19:09
admin	Device_3	Device Create	Create Device_3,Type:SICO...	2012-07-23 10:19:12
admin	Device_4	Device Create	Create Device_4,Type:SICO...	2012-07-23 10:19:16
admin	Device_5	Device Create	Create Device_5,Type:SICO...	2012-07-23 10:19:25
admin	Device_6	Device Create	Create Device_6,Type:SICO...	2012-07-23 10:19:31
admin	Device_6	Device Delete	Delete Device_6	2012-07-23 10:19:37

Total 9 records Total 1 pages Current page 1

First P... Previo... Next P... Last P... Close

Figure 100 Operation Log Query Result

Running Log Query

Condition

Type

Source: Equipment Service EventTypes: Device Login

Location

Device: Slot: Port:

Time

From: 2012-07-17 00:00:00 To: 2012-07-23 10:32:48

Query

Result

Source	Type	Content	Generate Time
192.168.0.22,Device_5	Device Login	192.168.0.22,Device_5 Login	2012-07-23 10:19:30
192.168.0.21,Device_4	Device Login	192.168.0.21,Device_4 Login	2012-07-23 10:19:25
192.168.0.20,Device_3	Device Login	192.168.0.20,Device_3 Login	2012-07-23 10:19:20
192.168.0.19,Device_2	Device Login	192.168.0.19,Device_2 Login	2012-07-23 10:19:15
Device_1	Device Login	Device_1 Login	2012-07-23 10:19:07

Total 5 records Total 1 pages Current page 1

First P... Previo... Next P... Last P... **Export** Close

Figure 101 Running Log Query Result

Click <Export>. You can export the query result to a .xls file on the local device for further query.

**Caution:**

The relationship among query conditions is logical "AND".

Appendix: Acronyms

Acronym	Full Spelling
EMS	Element Management System
FTP	File Transfer Protocol
LLDP	Link Layer Discovery Protocol
SNMP	Simple Network Management Protocol