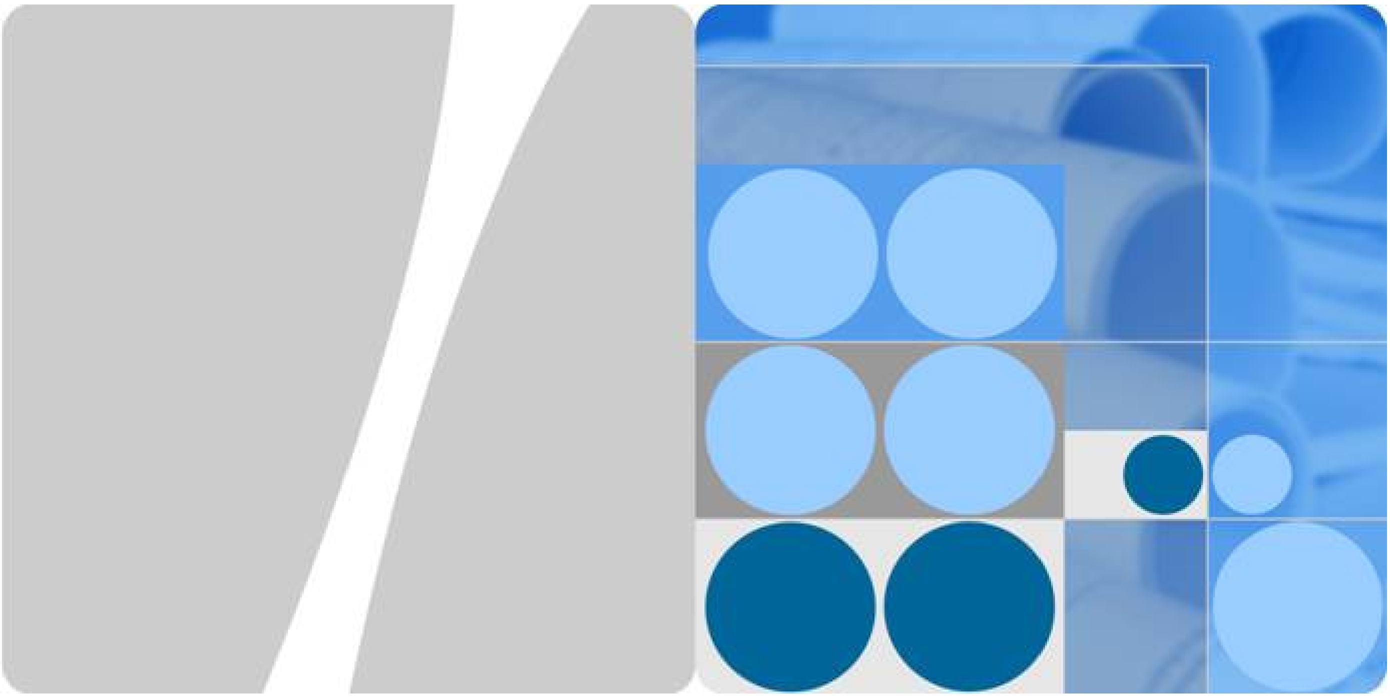


Huawei eSight AppBase

V200R001C00

Product Description

Issue 02

Date 2011-09-30

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

Contents

1 Product Features and Positioning

About This Chapter

This chapter describes features of the eSight AppBase and lists the types of devices that can be managed by the V200R001C00SPC200.

eSight AppBase is a new-generation management system oriented toward enterprise parks and tributary networks. The eSight AppBase supports unified management and intelligent interaction for enterprise resources, services, and users. In addition, the eSight AppBase can manage IT devices, IP devices, and third-party devices in a unified manner, and make intelligent analysis of network traffic and access authentication roles. It adjusts network control strategies automatically to ensure the security of enterprise networks comprehensively. Moreover, the eSight AppBase provides a flexible open platform, which lays a foundation for enterprises to build their own intelligent management systems.

1.1 Positioning

eSight AppBase is a new-generation management system oriented toward enterprise parks and tributary networks. The eSight AppBase supports unified management and intelligent interaction for enterprise resources, services, and users. In addition, the eSight AppBase can manage IT devices, IP devices, and third-party devices in a unified manner, and make intelligent analysis of network traffic and access authentication roles. It adjusts network control strategies automatically to ensure the security of enterprise networks comprehensively. Moreover, the eSight AppBase provides a flexible open platform, which lays a foundation for enterprises to build their own intelligent management systems.

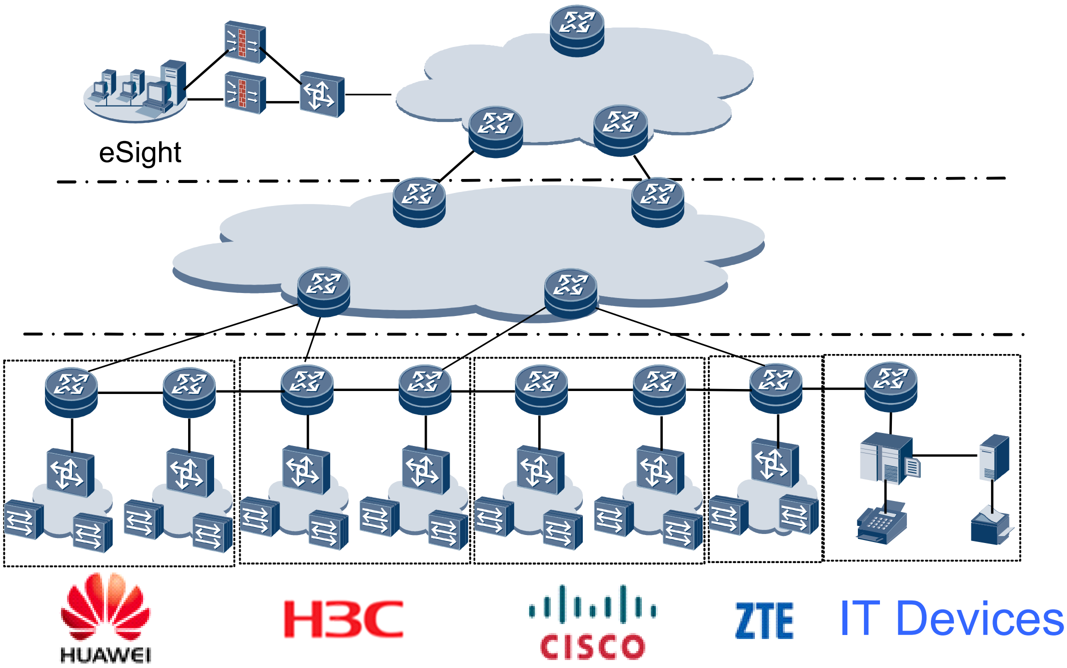
1.2 Features

1.2.1 Providing Flexible Third-Party Device Management Capability

The eSight AppBase can manage network devices manufactured by Huawei, H3C, Cisco, and ZTE in a unified manner, as shown in **Figure 1-1**.

- It manages network devices from manufacturers such as Huawei, H3C, Cisco, and ZTE, and IT devices from manufacturers such as IBM, HP, and Sun in a unified manner.
- It manages preconfigured mainstream devices from manufacturers such as H3C, Cisco, and ZTE, and provides flexible user-defined capability. It allows you to customize devices that are not preconfigured and manages them as preconfigured devices after customization.
- It adopts customized settings to manage third-party devices that support the standard MIBs (RFC 1213-MIB, Entity-MIB, SNMPv2-MIB, and IF-MIB) as preconfigured third-party devices, and uses NE patches for adaptation to manage third-party devices that do not support the standard MIBs.

Figure 1-1 Third-party device management



1.2.2 Supporting Multiple OSs

The eSight AppBase, used as an independent application, can be installed on different OSs and databases. Hence, it is compatible with multiple OSs.

The eSight AppBase is based on the Huawei unified application platform OMS that adopts the browser/server architecture. The eSight AppBase supports Windows and SuSE Linux OSs and Oracle and MySQL databases.

1.2.3 Providing Differentiated Versions Based on Management Requirements

Huawei supplies three versions of the eSight AppBase: compact version, standard version, and professional version. Service components can be added to the standard version and professional version based on service development requirements.

- The compact version meets management requirements of small-scale networks and features low cost and simple deployment. It supports only basic management functions and cannot be added with service components as required.
- The standard version meets most network management requirements. It can be used as a lower level NMS in hierarchical management, and can be upgraded to the professional version by means of patch installation.
- The professional version meets management requirements of large-scale networks. It can be used as an upper level NMS in hierarchical management.

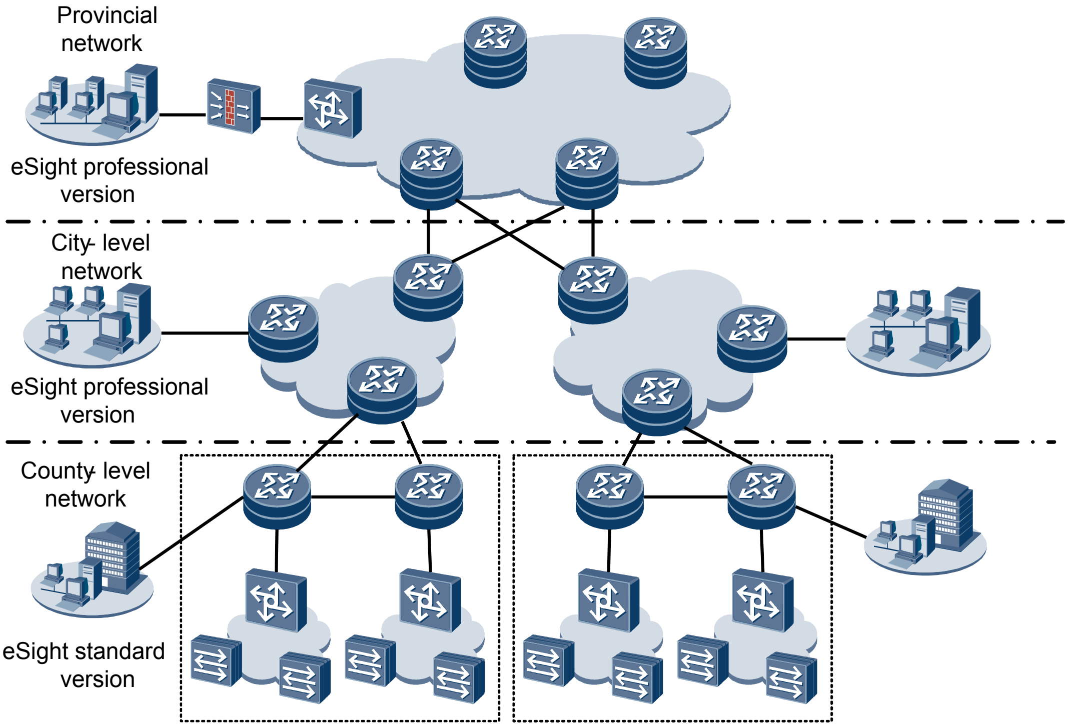
1.2.4 Functioning as a Multiple-Service Management Bearer Platform

The eSight AppBase implements management functions such as the topology management, fault management, performance management, configuration management, and security management on the basis of network resource management. In addition, the eSight AppBase functions as the bearer platform of other service management components and jointly achieves close convergence and interaction in management. The eSight AppBase instructs you in using functions by means of the process wizard, to provide refined management for you.

1.2.5 Adopting Hierarchical Management

A large number of devices can be widely distributed in different regions and devices in each region can be deployed in a centralized manner. For networks in such scenarios, the eSight AppBase provides hierarchical management to achieve authority-based management and load sharing for the entire network. In such a case, the eSight AppBase professional version is often deployed in the HQ and the eSight AppBase standard version is deployed in branches to form double-level or triple-level management, as shown in **Figure 1-2**.

Figure 1-2 Adopting hierarchical management



2 Product Architecture

About This Chapter

The eSight AppBase adopts the component-based design and uses excellent components in the industry such as OSGI, Spring dynamic module (DM), Hessian, and Birt.

By using the extension point mechanism, the eSight AppBase implements incremental development of functions and NE version adaptation packages. Therefore, new functions or new NE adaptation packages can be added without changing release package codes. The modular framework that is based on the OSGI platform enables service components to be upgraded and patched independently.

2.1 Web-Based Architecture

Adopting the browser/server architecture, the eSight AppBase owns innate advantages of the browser/server architecture. It runs on the browser of a client. Therefore, only the server software needs to be updated during system upgrade or maintenance, which decreases the load of the computer installed with the client, reduces the cost and workload of system maintenance and upgrade, and lowers the total cost of operation (TCO) of users. In addition, the browser/server architecture has the following advantages:

- The distribution feature supports operations such as query and browse at any place at any time.
- Services can be extended simply and conveniently, and Web pages can be added to add server functions.
- Maintenance is simple and convenient. Web pages can be modified to synchronize all user data.

2.2 Integration

By using Spring remote proxy, the eSight AppBase works with Hessian and Java Script Object Notation (JSON) to provide open service integration buses. The Hessian service implements interconnection with other Java systems, and the JSON service implements interconnection with multiple language systems. In addition, the eSight AppBase GUI framework provides multiple extension points such as the main menu, system menus, user menus, and Portal, to integrate with GUIs of third-party systems.

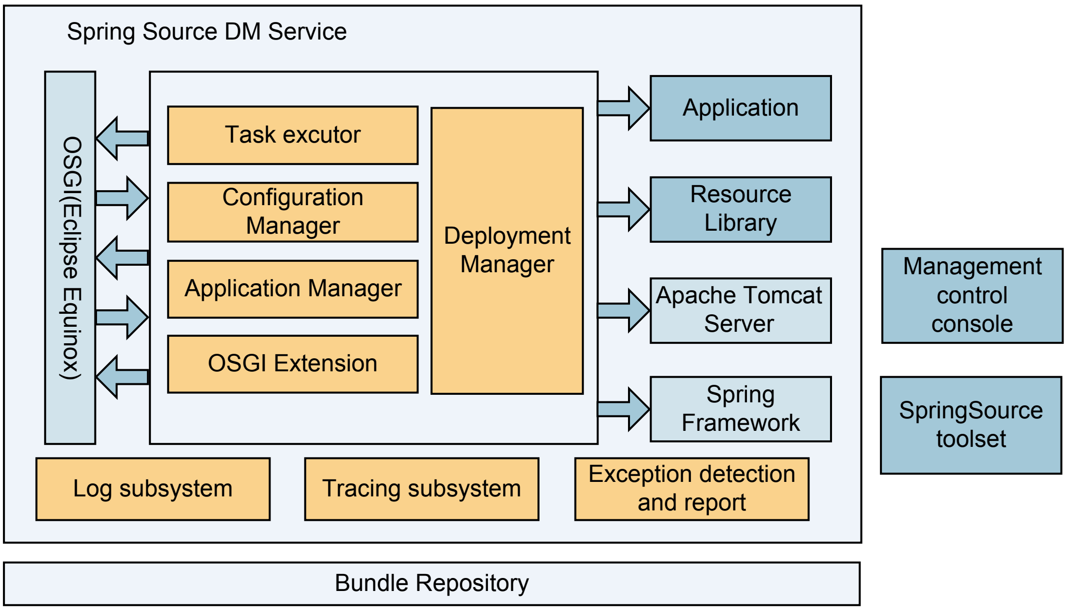
2.3 Component-based Design

The eSight AppBase adopts the component-based design and uses excellent components in the industry such as OSGI, Spring dynamic module (DM), Hessian, and Birt.

- Adopts the OSGI, a Java-oriented dynamic model system, to provide the dynamic pluggable capability of application components. Allows applications to use refined, reusable, and collaborative components to construct standard primitives.
- Deploys these components to one application and supports the dynamic pluggable capability of application components.
- Integrates Web services with application services by using Virgo. Virgo is a Spring DM implementation mode. It allows development engineers to construct the Spring application, which can be deployed in the OSGI container. The Spring application provides the Web container and supports the OSGI dynamic deployment capability. This application has the following advantages, as shown in **Figure 2-1**.
  1. Better separates the application logic from the module.
  2. Deploys the same module of different versions.
  3. Supports services that are discovered dynamically and services provided by other modules in the system.
  4. Installs and updates modules on and unloads modules from the running system dynamically.

5. Achieves component instances, component configuration, and component integration inside modules and between modules by using the Spring framework.
6. Allows application development engineers of enterprises to develop OSGI platform functions by using simple and familiar programming models.

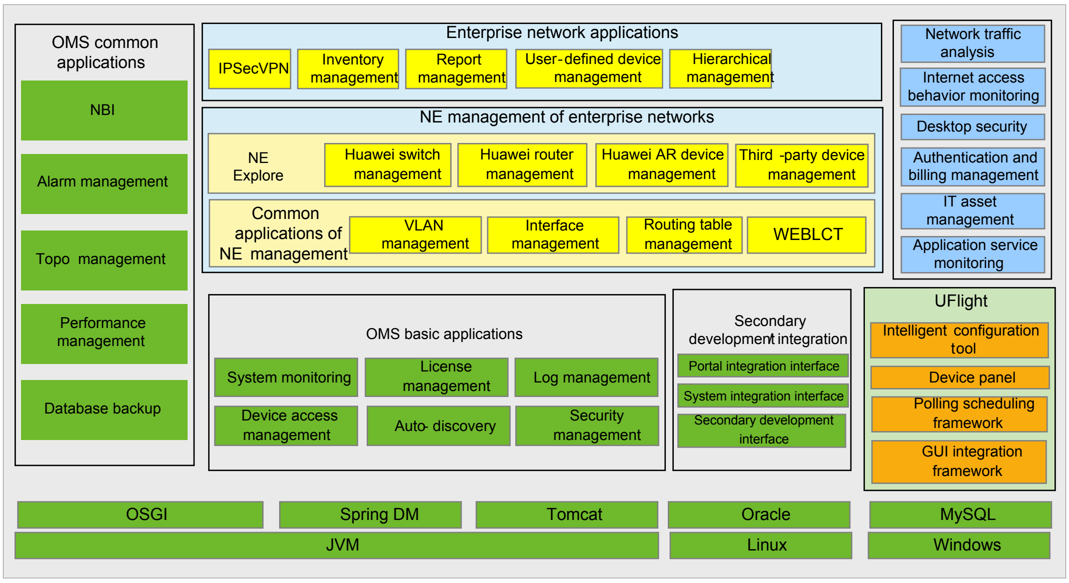
Figure 2-1 Modular architecture



- Uses open integration interfaces provided by Hessian and JSON. Hessian is a lightweight remote onhttp tool. It provides RMI functions by using a simple method. Compared with WebService, Hessian is simpler and faster. JSON is a lightweight data interchange format. It is easy to read and compile and can be parsed and generated by machines easily. In addition, JSON is a subnet based on Java script (Standard ECMA-262 3rd Edition - December 1999). It adopts a language-independent text format. These features make JSON become an ideal data interchange language. With JSON services, the eSight AppBase can integrate with other non-Java language systems.
- Provides flexible scalability and secondary development by using the extension point mechanism. The eSight AppBase adopts Eclipse-similar extension point mechanism and encapsulates NE version adaptation functions based on this mechanism to implement the development of incremental functions and the adaptation of incremental NE versions.

Figure 2-2 shows eSight AppBase components.

Figure 2-2 eSight AppBase components



NOTE

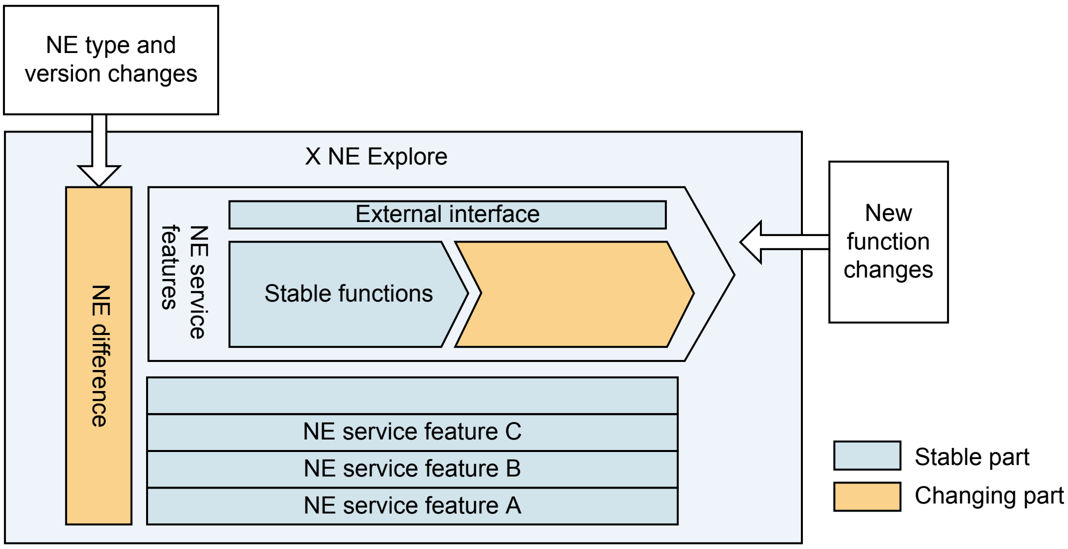
The eSight AppBase is based on the OSGI platform. Hence, its components share one Java process during running, and the components can be started or stopped separately as plug-ins when the status of dependent components meets requirements. Only third-party systems, report components, and GUI-based CLIs can run as independent processes.

2.4 Components That Can Be Recovered Independently

By using the extension point mechanism, the eSight AppBase implements incremental development of functions and NE version adaptation packages. Therefore, new functions or new NE adaptation packages can be added without changing release package codes. The modular framework that is based on the OSGI platform enables service components to be upgraded and patched independently.

Figure 2-3 shows recovery strategies in the case of eSight AppBase function changes or NE version changes. If new functions need to be supported, new function plug-in packages can be developed and deployed in the eSight AppBase. If new devices need to be adapted, only new NE adaptation packages need to be added. Function plug-in packages and NE adaptation packages are deployed in the OSGI container of the eSight AppBase as bundles (that is, plug-ins).

Figure 2-3 Recovery strategies



3 Product and Application Scenarios

About This Chapter

The eSight AppBase can manage network devices such as routers, switches, firewalls, printers, and servers, and can manage devices of new types by using the in-service customization function. In addition, the eSight AppBase provides standard external interfaces and supports integration with the operating support system (OSS), thereby meeting requirements for managing large-scale networks.

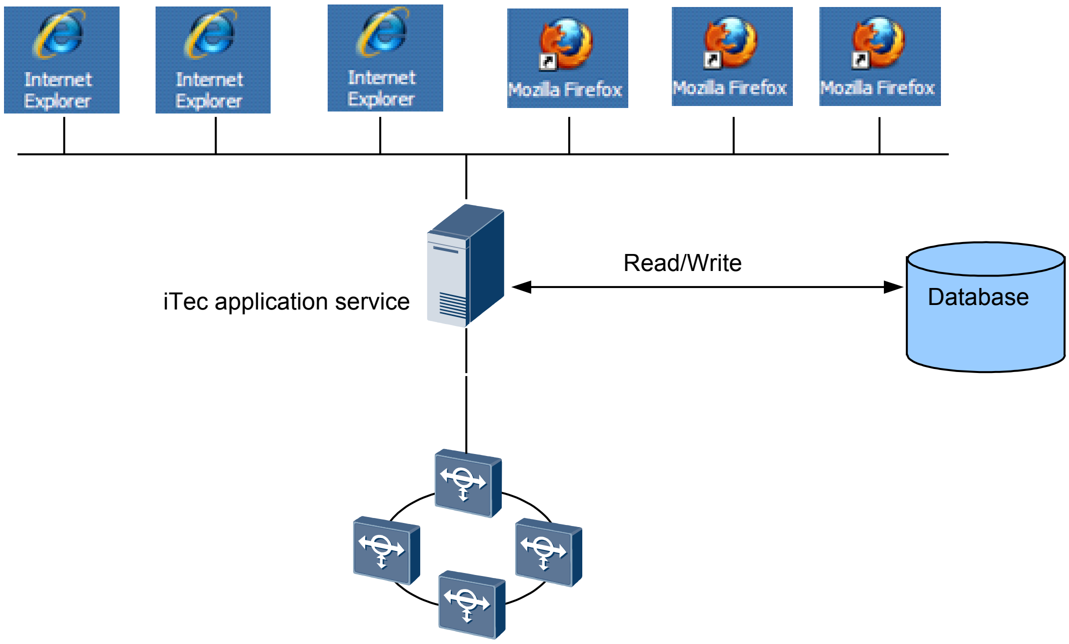
3.1 eSight AppBase Network

eSight AppBase supports two network modes: a single server and hierarchical deployment.

3.1.1 Single-Server Mode

Adopting the browser/server architecture, the eSight AppBase allows multiple browsers to connect to the eSight AppBase at the same time, as shown in **Figure 3-1**.

Figure 3-1 Single-Server Mode

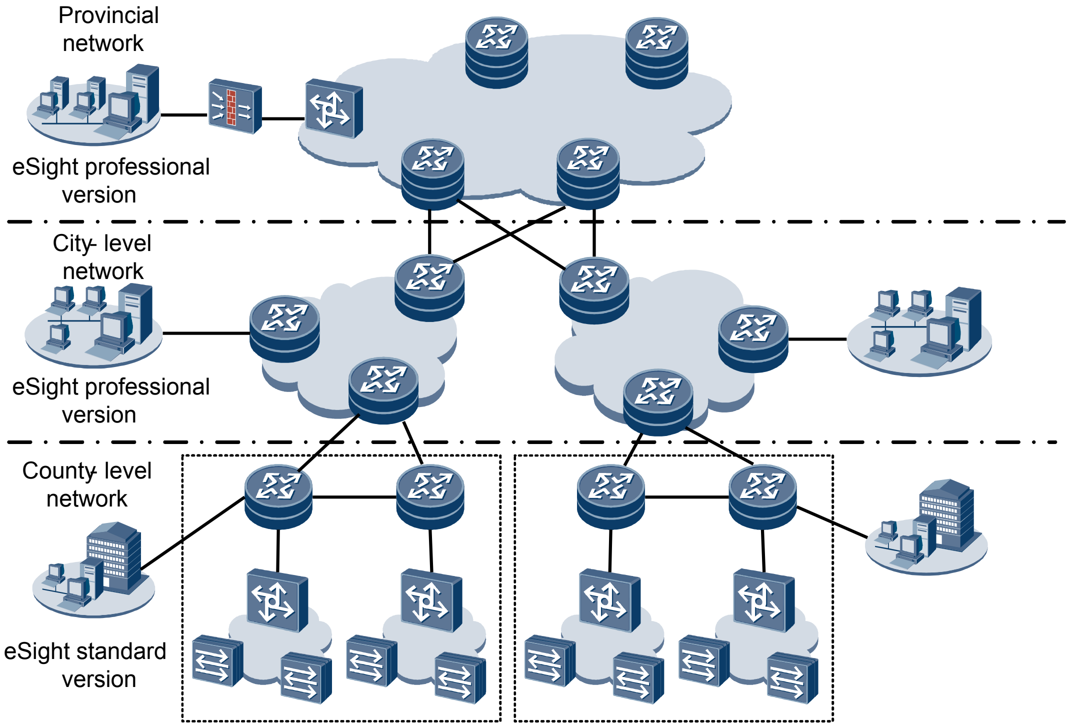


3.1.2 Hierarchical Deployment Mode

The eSight AppBase supports hierarchical management, which enables an enterprise HQ to manage networks in different areas.

The upper level NMS can add lower level NMSs to the system and provide links to lower level NMSs. When you click such a link, a new browser window is displayed, which shows the home page of a lower level NMS. When you open the home page of a lower level NMS from an upper level NMS, you do not need to log in manually and the single sign-on mechanism provided by the OMS is used for login. **Figure 3-2** shows hierarchical NMS deployment.

Figure 3-2 Hierarchical deployment mode



3.2 Networking of the eSight AppBase and NEs

The scalable architecture and modular design enable the eSight AppBase to manage data networks either separately or in a unified manner.

Table 3-1 lists Huawei-developed devices and third-party devices that can be managed by the eSight AppBase.

Table 3-1 Devices that can be managed by theeSight AppBase

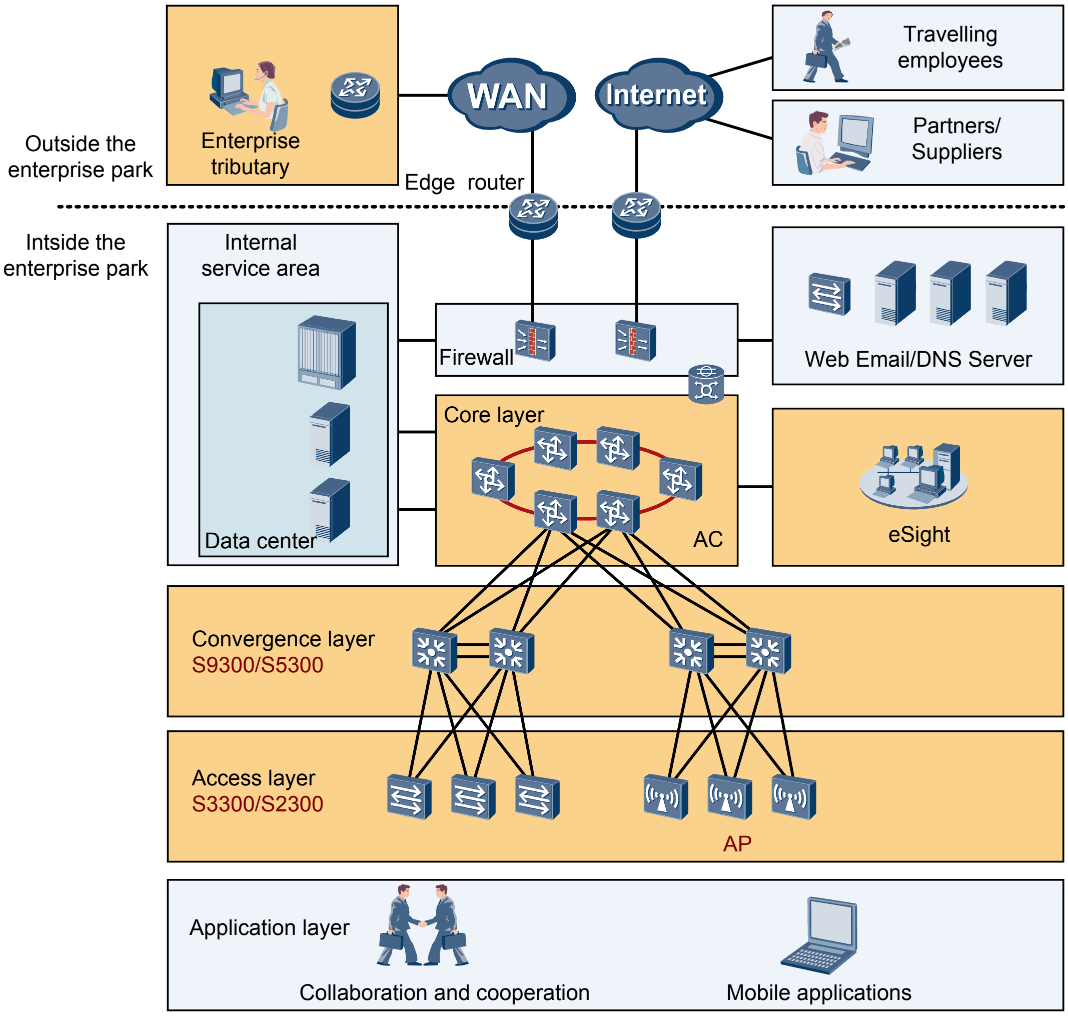
Domain	Device
Switches	S series switches
Routers	NE series routers, AR series routers
Security devices	Eudemon series, SRG series, SVN series
Third-party devices	● Pre-integrated third-party devices, H3C devices, and Cisco devices ● Printers and servers

NOTE

For details about devices that can be managed by eSight AppBase, see **7 Manageable Devices**.

In an enterprise park, tributary services, Internet mobile office services, and wireless user services need to connect to the enterprise park network. The eSight AppBase intelligent management platform can manage multiple systems in an integrated manner and manage IT and IP devices in a unified manner. **Figure 3-3** shows the scenario of the solution where the eSight AppBase and NEs are used.

Figure 3-3 Huawei solution for enterprise parks and tributary networks

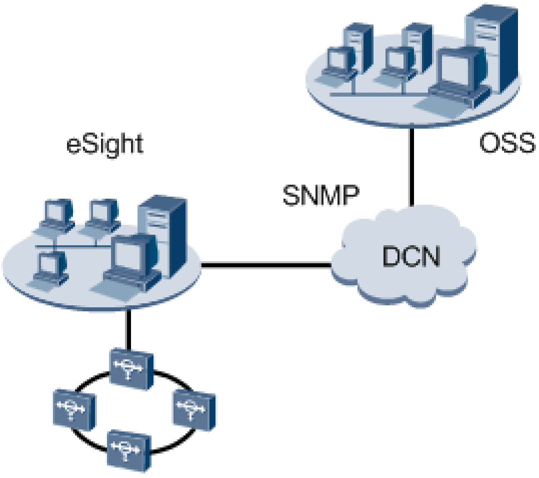


3.3 eSight AppBase and OSS Integration

The eSight AppBase supports integration with the OSS.

In **Figure 3-4**, the eSight AppBase reports network alarms and integrates with the OSS over SNMP.

Figure 3-4 eSight AppBaseand OSS integration



The advantages of integration with the OSS are as follows:

- Enhances network management capability by means of the OSS.
- Separates NE management functions from network management functions.
- Meets the requirements of the enterprise O&M mechanism.

4 Functions and Features

About This Chapter

The eSight AppBase provides the overall basic network management, NE management, service management, and system management functions.

a variety of report templates, fully meeting network operation and maintenance requirements. In addition, eSight AppBase provides a report design tool that allows you to flexibly customize report templates.

4.9 Customize Device
eSight AppBase provides user-defined device management to help enterprise users manage devices with many features. To manage basic device capabilities, you can customize the device types, performance counters, alarm parameters, configuration file management parameters, and device panels.

4.10 Configuration File Management
eSight AppBase allows you to back up, restore, and compare device configuration files, and manage baseline file versions. When the network is faulty, you can compare the configuration file in use with the one that was saved when the network was running normally. By checking the added, modified, and deleted information, you can quickly locate the fault and rectify it.

4.11 Smart Configuration Tool
The smart configuration tool is used to configure one or more Huawei devices.

4.12 WLAN Service Management
A WLAN is a network system that enables computers to communicate and share resources wirelessly. WLANs can access the Ethernet quickly.

4.13 Lower-Layer NMSs
eSight AppBase allows you to divide a network into several layers in order to manage the NEs on the network by layer. eSight AppBase provides links to lower-layer NMSs. By clicking a link, you can view alarms, performance counters, reports, and the network topology on a lower-layer NMS.

4.14 Single NE Feature Management
This topic describes features managed by eSight AppBase.

4.15 eSight AppBase Home Page
The eSight AppBase home page displays important monitoring information, and allows you to specify the type of monitoring information displayed.

4.16 Data Backup and Restore
eSight AppBase provides an independent Web service to back up or restore the database.

4.1 Security Management

This topic describes how to enhance eSight AppBase security by managing users, roles, rights, and operation sets.

To control user rights based on its role, eSight AppBase allows you to specify:

- Managed device set.
- Operation set.
- Time segment during which lower-level users access eSight AppBase.
- IP addresses and IP address segments with which users access eSight AppBase.
- Security policies for accounts and passwords.

User Management

With user management, you can use predefined roles and access control policies to control the managed device set, operation set, and access policies for users. You can also set the following user attributes:

- User name
- Password
- User status
- Role
- Time segment for login
- IP addresses and IP address segments for login
- User description

NOTE

By default, eSight AppBase has the **admin** user, which is the super administrator.

Role Management

With role management, you can manage role information, including the role name, managed objects, operations allowed, and description, based on the role model. After you set the managed object set and operation set for roles and associate a role with a user, the user can control devices in the managed object set and perform operations in the operation set.

- Managed object set: Specifies the set of subnets and devices that can be managed by a role. A user-defined managed device set (management domain) can be used.
- Operation set: Specifies the operations that users can perform.

Access Control Policies

With access control management, you can control the time segment, IP addresses, and IP address segments with which users log in to eSight AppBase .

- Login time control Policy: You can set the start date, end date, start time, end time, and days of the week when users can log in to eSight AppBase .

- Login IP Address Control Policy: You can set the IP addresses and IP address segments with which users log in to eSight AppBase .

NOTE

By default, eSight AppBase has four roles: super administrator, security administrator, operator, and inspector.

Security Policy Management

With security policy management, you can set security policies, including the account policy and password policy, for all accounts.

1. In an account policy, you must set:
   - Minimum account length
   - Number of login attempt failures before the account is locked
   - Account suspension with no access in a long period of time
2. In a password policy, you must set:
   - Minimum password length
   - Password policy
   - Maximum number of times that a character can be used in a same password
   - Special characters that are allowed in a password
   - Minimum password change interval
   - Mandatory password change upon password expiration

Security Monitoring

With security monitoring, you can monitor online eSight AppBase users using their user name, IP address, login time, and role information. You can also force a user offline.

User-defined Management Domain

A user-defined management domain is a set of managed devices compiled for ease of management, which can be associated with a role when you define one.

4.2 Log Management

Logs record important user operations. With log management, you can view and filter log lists, and view detailed system logs. eSight AppBase can manage operation logs, security logs, and system logs. Logs are classified into warning, minor, and major logs.

Operation Logs

Operation logs record operations performed by users.

Security Logs

Security logs record events related to system security.

System Logs

System logs record key information generated during eSight AppBase normal operation and task execution.

4.3 Resource Management

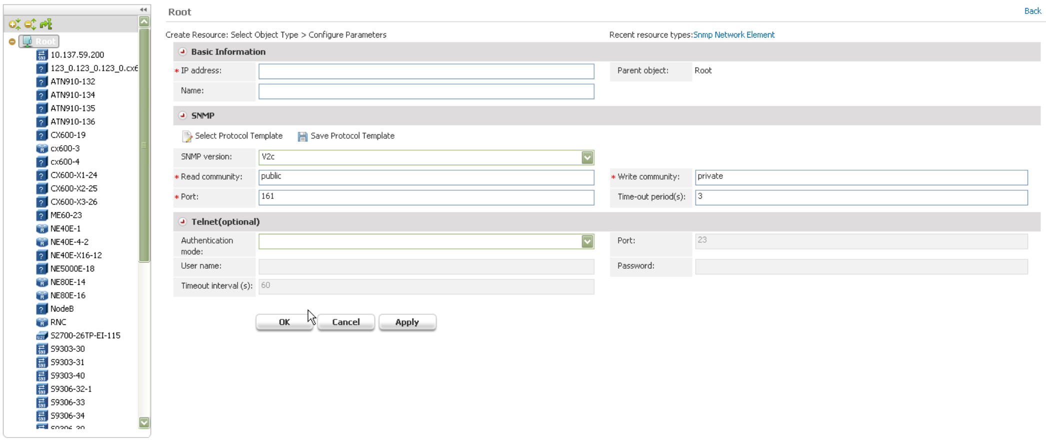
With Resource management, you can add and delete NEs, and manage them by subnet based on their physical locations.

You can add NEs in one of the following ways: adding an NE manually, allowing eSight AppBase to discover NEs on a network segment automatically, or importing a file to add NEs in a batch.

Single Resource Adding

With this method, you enter an NE IP address manually and set the NE's SNMP parameters to add an NE to eSight AppBase. You can also create a subnet, as shown in **Figure 4-1**.

Figure 4-1 Adding an Resource



Root

Create Resource: Select Object Type > Configure Parameters

Recent resource types:Snmp Network Element

Basic Information

* IP address:		Parent object:	Root
Name:			

SNMP

SNMP version:	V2c		
* Read community:	public	* Write community:	private
* Port:	161	Time-out period(s):	3

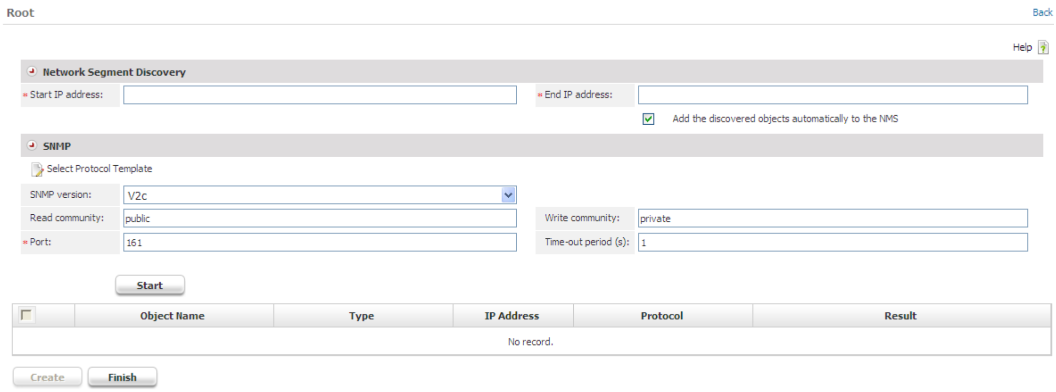
Telnet(optional)

Authentication mode:		Port:	23
User name:		Password:	
Timeout interval (s):	60		

Automatic NE Discovery

With eSight AppBase, you can search for NEs on an IP address segment. eSight AppBase automatically adds any IP addresses it finds, as shown in **Figure 4-2**.

Figure 4-2 Discovering NEs automatically



* Start IP address:

* End IP address:

☑ Add the discovered objects automatically to the NMS

SNMP version: V2c

Read community: public

Write community: private

* Port: 161

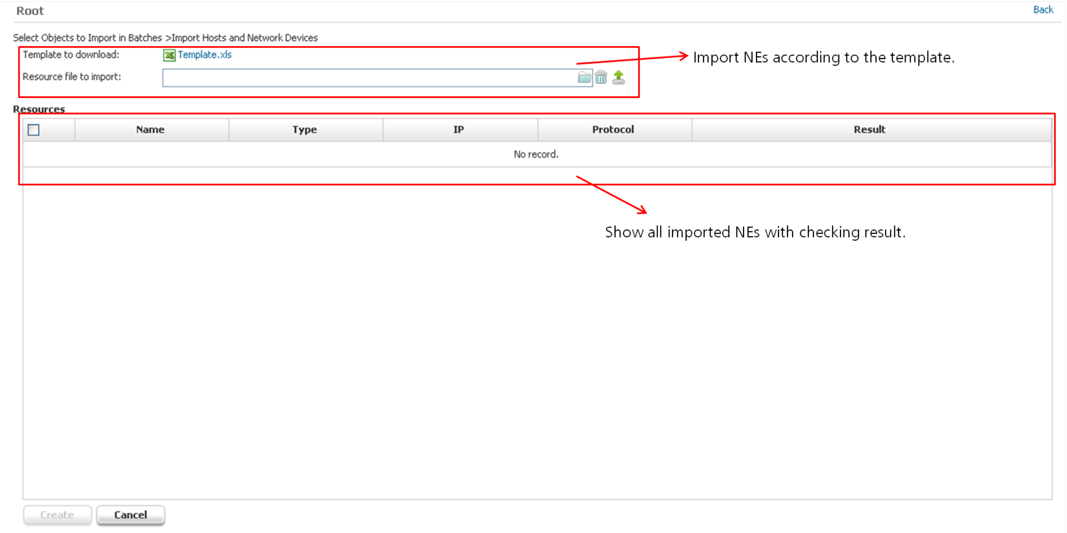
Time-out period (s): 1

□	Object Name	Type	IP Address	Protocol	Result
No record.					

Batch NE Import

You can add NEs in batches by importing a file that contains the NE IP addresses and SNMP parameters, as shown in **Figure 4-3**.

Figure 4-3 Importing NEs in batches


Root
Back
Create
Cancel
Import NEs according to the template.
Show all imported NEs with checking result.

Select Objects to Import in Batches >Import Hosts and Network Devices

Template to download: Template.xls

Resource file to import:

Resources

□	Name	Type	IP	Protocol	Result
No record.					

NE Deletion

You can delete NEs that are not being managed by eSight AppBase.

Subnet Management

You can create and delete subnets on eSight AppBase. eSight AppBase allows you to manage NEs by subnet based on their physical locations.

NE Move

You can move NEs between subnets. eSight AppBase allows you to change the subnet of an NE based on the NE's physical location.

4.4 Topology Management

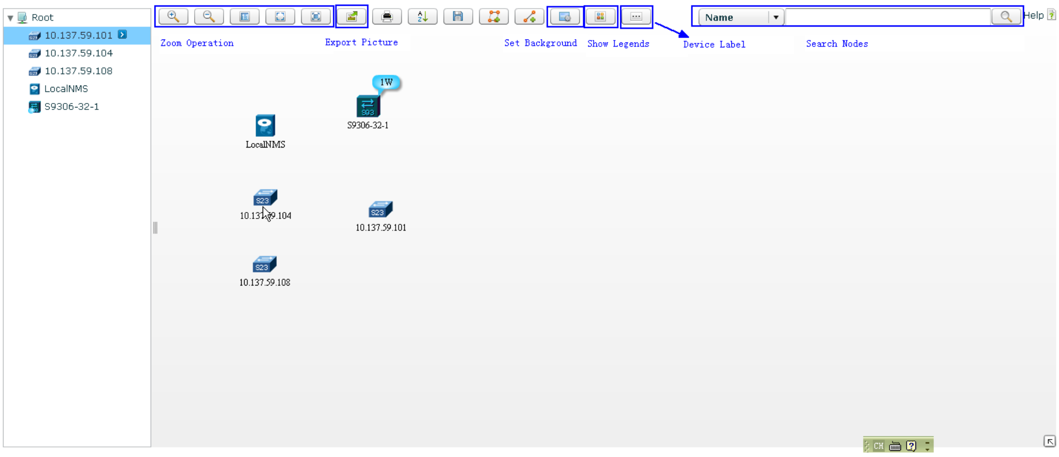
With topology management, managed NEs and their connection status are displayed in the topology view. The managed objects are organized in submaps. You can use the topology view to check the status of the entire network in real time.

Term	Description
NE	NEs are core units in topology management. In the topology view, different icons represent different NE types.
Subnet	For ease of management, a large network is divided into several subnets based on a specific rule (such as by region or device type).
Link	Links represent physical or logical connections between NEs.

Topology View

On eSight AppBase, the topology view displays the NE status and links between NEs. With topology management, it is easy to visualize the architecture and determine the running status of all NEs, as shown in **Figure 4-4**.

Figure 4-4 Topology view



Topology View Browsing

- The NE navigation tree is displayed in the pane on the left and the topology view is displayed in the pane on the right, where NEs in different subnets are displayed in different layers.

- eSight AppBase provides the full screen and Aerial View functions to display the full topology view or just a partial view of it, respectively.
- The topology view displays the alarm status of NEs and link, displays tips of NEs and link, and provide the legend to show the meaning of color.
- The topology view provide Topo logical object search ability.
- The topology view provide topological object name setting ability, support network elements in the network topology in accordance with the name, IP address display settings.

Operations on a Topology View

With the topology view, you can:

- Zoom in or zoom out.
- Export and print images, and set the background image.
- Move nodes and save the settings.
- Use shortcut menus.

Alarm Severity Display

The topology node color reflects the highest alarm severity of the node. The color is updated in real time based on the alarm severity. During an emergency, you can acknowledge and rectify faults promptly.

Shortcut Menus for NE Management

From the topology view, you can click an NE, click the button that is displayed, and choose **Manage** from the shortcut menu. Then the object manager page is displayed, and you can use it to manage the NE.

4.5 Alarm Management

Alarm management is used to monitor the network running status in real time. The network administrator can browse alarms, handle alarms, set alarm rules (such as alarm suppression rules and alarm sound), and send remote alarm notifications to ensure that the network runs properly.

With real-time alarm management, you can view the alarm board and event list and browse real-time and historical alarms.

You can set alarm remote notification rules, alarm suppression rules, and the alarm sound.

Alarm Browsing

You can browse alarms on several pages.

- Alarm board

  Displays the number of active alarms for each alarm severity.
- **Active Alarms** tab page

  Lists active alarms, as shown in **Figure 4-5**.
- **History Alarm** tab page

  Lists archived historical alarms.

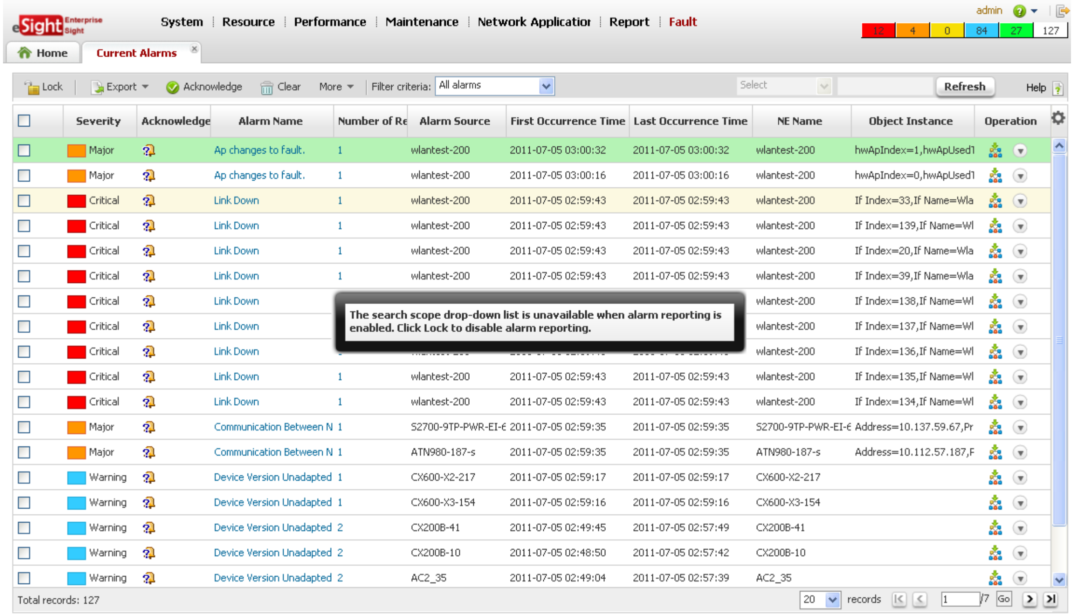
- **Event Browse** tab page

  Lists events reported by NEs.

- **Suppressed Alarms** tab page

  Lists suppressed alarms.

Figure 4-5 Active alarms



□	Severity	Acknowledge	Alarm Name	Number of Re	Alarm Source	First Occurrence Time	Last Occurrence Time	NE Name	Object Instance	Operation
□	🟧 Major		Ap changes to fault.	1	wlantest-200	2011-07-05 03:00:32	2011-07-05 03:00:32	wlantest-200	hwApIndex=1,hwApUsed1	
□	🟧 Major		Ap changes to fault.	1	wlantest-200	2011-07-05 03:00:16	2011-07-05 03:00:16	wlantest-200	hwApIndex=0,hwApUsed1	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=33,If Name=Wla	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=139,If Name=Wl	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=20,If Name=Wla	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=39,If Name=Wla	
□	🟥 Critical		Link Down					wlantest-200	If Index=138,If Name=Wl	
□	🟥 Critical		Link Down					wlantest-200	If Index=137,If Name=Wl	
□	🟥 Critical		Link Down					wlantest-200	If Index=136,If Name=Wl	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=135,If Name=Wl	
□	🟥 Critical		Link Down	1	wlantest-200	2011-07-05 02:59:43	2011-07-05 02:59:43	wlantest-200	If Index=134,If Name=Wl	
□	🟧 Major		Communication Between N	1	S2700-9TP-PWR-EI-6	2011-07-05 02:59:35	2011-07-05 02:59:35	S2700-9TP-PWR-EI-6	Address=10.137.59.67,Pr	
□	🟧 Major		Communication Between N	1	ATN980-187-s	2011-07-05 02:59:35	2011-07-05 02:59:35	ATN980-187-s	Address=10.112.57.187,F	
□	🟦 Warning		Device Version Unadapted	1	CX600-X2-217	2011-07-05 02:59:17	2011-07-05 02:59:17	CX600-X2-217		
□	🟦 Warning		Device Version Unadapted	1	CX600-X3-154	2011-07-05 02:59:16	2011-07-05 02:59:16	CX600-X3-154		
□	🟦 Warning		Device Version Unadapted	2	CX200B-41	2011-07-05 02:49:45	2011-07-05 02:57:49	CX200B-41		
□	🟦 Warning		Device Version Unadapted	2	CX200B-10	2011-07-05 02:48:50	2011-07-05 02:57:42	CX200B-10		
□	🟦 Warning		Device Version Unadapted	2	AC2_35	2011-07-05 02:49:04	2011-07-05 02:57:39	AC2_35		

The search scope drop-down list is unavailable when alarm reporting is enabled. Click Lock to disable alarm reporting.

Total records: 127

20 records 1 /7 Go

Alarm Handling

- Locking an alarm

  You can lock current alarm interface, then the alarm interface no longer refreshes new alarm. so that you can view existing alarm information.

- Acknowledging an alarm

  You can check whether an alarm has been acknowledged and acknowledge any that have not yet been. After acknowledgment, the alarm statistical graph is updated.

- Clearing an alarm

  You can manually remove alarm to the alarm historical database, Then the alarm no longer displayed on the current alarm interface.

- Exporting an alarm

  You can export selected or all alarms to an EXCEL file.

- Locating an alarm

  You can locate faulty NEs or panels based on alarm information.

Alarm Configuration

- Setting alarm filters

You can set alarm filters so that only the desired alarms are displayed on the alarm page. The alarm filters include the date, time segment, alarm source (the NE that generates the alarm), and alarm severity.

- Setting alarm sounds

  You can set alarm sounds for each of the four alarm severities and the number of times the alarm sounds.

Remote Alarm Notifications

eSight AppBase supports remote alarm notifications. eSight AppBase can send emails and short message service (SMS) messages to notify remote maintenance personnel of alarm information.

- Email

  You can set an email server to receive emails sent by the alarm server.
- User-defined notification template

  You must set the email template.
- User group

  You must set the user group information including the email addresses for all users.
- Remote notification rule

  You must set notification rules by alarm severity or alarm name. The notification rules include the notification name, whether the alarm clearing notification function is enabled, and user group information.

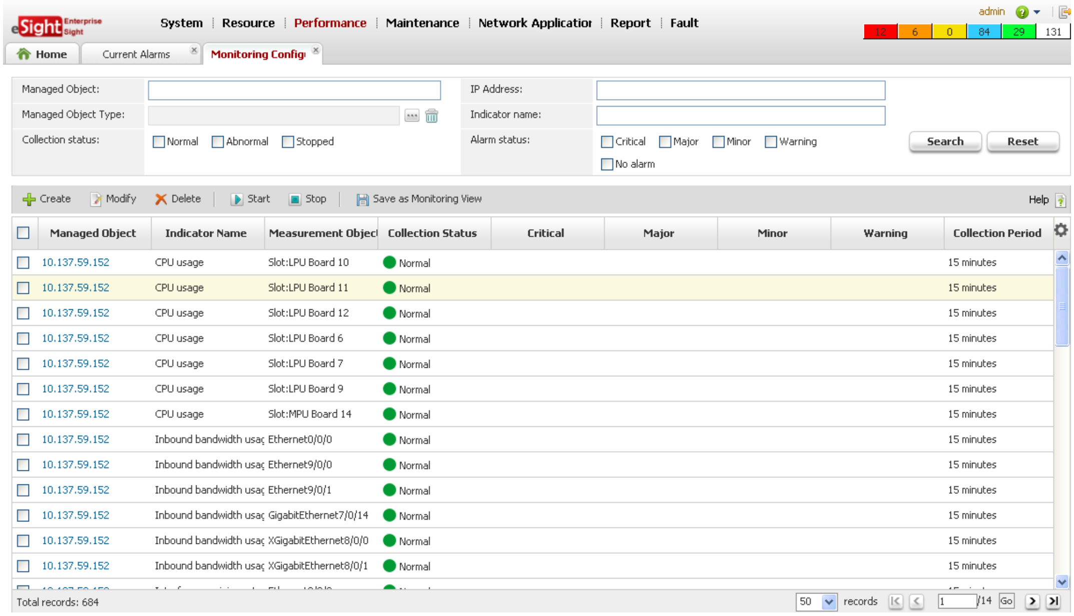
4.6 Performance Management

eSight AppBase can monitor the key performance indicators (KPIs) of a network in real time and collect performance statistics. With eSight AppBase graphical user interfaces (GUIs), you can manage network performance easily.

Performance Counter Configuration

Performance counters are managed uniformly, as shown in **Figure 4-6**.

Figure 4-6 Configuring performance counters



Managed Object:

IP Address:

Managed Object Type:

Indicator name:

Collection status: □ Normal □ Abnormal □ Stopped

Alarm status: □ Critical □ Major □ Minor □ Warning □ No alarm

□	Managed Object	Indicator Name	Measurement Objec	Collection Status	Critical	Major	Minor	Warning	Collection Period
□	10.137.59.152	CPU usage	Slot:LPU Board 10	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:LPU Board 11	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:LPU Board 12	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:LPU Board 6	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:LPU Board 7	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:LPU Board 9	● Normal					15 minutes
□	10.137.59.152	CPU usage	Slot:MPU Board 14	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	Ethernet0/0/0	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	Ethernet9/0/0	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	Ethernet9/0/1	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	GigabitEthernet7/0/14	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	XGigabitEthernet8/0/0	● Normal					15 minutes
□	10.137.59.152	Inbound bandwidth usag	XGigabitEthernet8/0/1	● Normal					15 minutes

Total records: 684 50 records 1 /14 Go

You can:

- Query monitored performance counters.
- Add, delete, enable, or disable performance counters in batches.
- Change the data collection period, thresholds, and whether the performance monitoring template is used for monitored counters in batches.
- View the collection status of each monitored performance counter.
- Set monitoring views quickly.

Performance Monitoring Template Configuration

A performance monitoring template provides default settings for creating a performance counter. You can set:

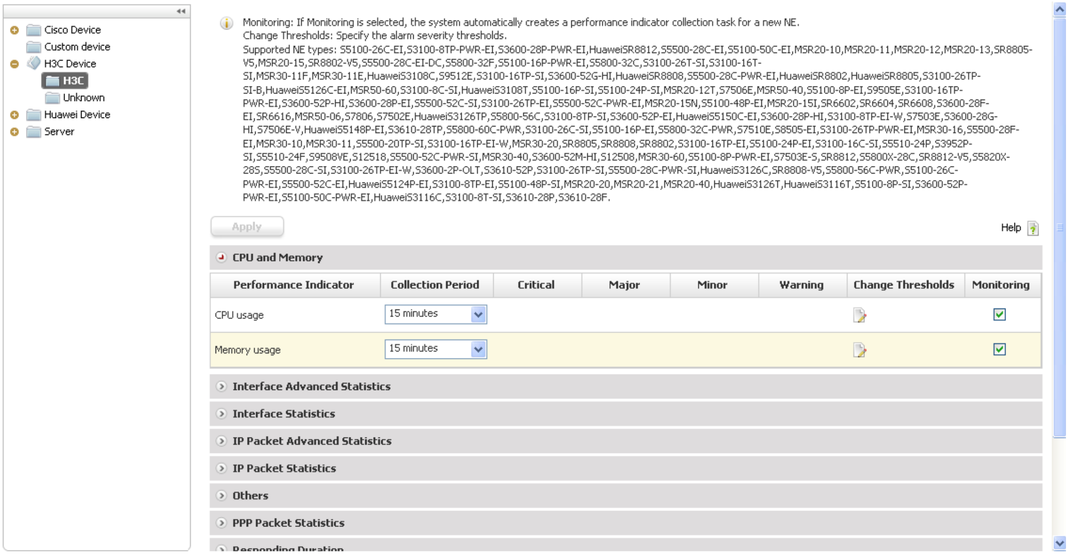
- Whether a counter in the template is monitored by default.
- A counter's default collection period.
- A counter's default threshold.

By default, eSight AppBase automatically collects the following counters:

- NE's CPU usage
- NE's memory usage
- NE's Unreachable percentage in a day
- NE's Responding duration
- NE network port traffic

You can also add other performance counters, which are shown in **Figure 4-7**.

Figure 4-7 Performance monitoring template



Monitoring: If Monitoring is selected, the system automatically creates a performance indicator collection task for a new NE.
Change Thresholds: Specify the alarm severity thresholds.
Supported NE types: S5100-26C-EI,S3100-8TP-PWR-EI,S3600-28P-PWR-EI,HuaweiSR8812,S5500-28C-EI,S5100-50C-EI,MSR20-10,MSR20-11,MSR20-12,MSR20-13,SR8805-V5,MSR20-15,SR8802-V5,S5500-28C-EI-DC,S5800-32F,S5100-16P-PWR-EI,S5800-32C,S3100-26T-SI,S3100-16T-SI,MSR30-11F,MSR30-11E,HuaweiS3108C,S9512E,S3100-16TP-SI,S3600-52G-HI,HuaweiSR8808,S5500-28C-PWR-EI,HuaweiSR8802,HuaweiSR8805,S3100-26TP-SI-B,HuaweiS5126C-EI,MSR50-60,S3100-8C-SI,HuaweiS3108T,S5100-16P-SI,S5100-24P-SI,MSR20-12T,S7506E,MSR50-40,S5100-8P-EI,S9505E,S3100-16TP-PWR-EI,S3600-52P-HI,S3600-28P-EI,S5500-52C-SI,S3100-26TP-EI,S5500-52C-PWR-EI,MSR20-15N,S5100-48P-EI,MSR20-15I,SR6602,SR6604,SR6608,S3600-28F-EI,SR6616,MSR50-06,S7806,S7502E,HuaweiS3126TP,S5800-56C,S3100-8TP-SI,S3600-52P-EI,HuaweiS5150C-EI,S3600-28P-HI,S3100-8TP-EI-W,S7503E,S3600-28G-HI,S7506E-V,HuaweiS5148P-EI,S3610-28TP,S5800-60C-PWR,S3100-26C-SI,S5100-16P-EI,S5800-32C-PWR,S7510E,S8505-EI,S3100-26TP-PWR-EI,MSR30-16,S5500-28F-EI,MSR30-10,MSR30-11,S5500-20TP-SI,S3100-16TP-EI-W,MSR30-20,SR8805,SR8808,SR8802,S3100-16TP-EI,S5100-24P-EI,S3100-16C-SI,S5510-24P,S3952P-SI,S5510-24F,S9508VE,S12518,S5500-52C-PWR-SI,MSR30-40,S3600-52M-HI,S12508,MSR30-60,S5100-8P-PWR-EI,S7503E-S,SR8812,S5800X-28C,SR8812-V5,S5820X-28S,S5500-28C-SI,S3100-26TP-EI-W,S3600-2P-OLT,S3610-52P,S3100-26TP-SI,S5500-28C-PWR-SI,HuaweiS3126C,SR8808-V5,S5800-56C-PWR,S5100-26C-PWR-EI,S5500-52C-EI,HuaweiS5124P-EI,S3100-8TP-EI,S5100-48P-SI,MSR20-20,MSR20-21,MSR20-40,HuaweiS3126T,HuaweiS3116T,S5100-8P-SI,S3600-52P-PWR-EI,S5100-50C-PWR-EI,HuaweiS3116C,S3100-8T-SI,S3610-28P,S3610-28F.

Performance Indicator	Collection Period	Critical	Major	Minor	Warning	Change Thresholds	Monitoring
CPU usage	15 minutes						☑
Memory usage	15 minutes						☑

Performance Monitoring View

After you obtain network performance data by configuring performance monitoring, the performance counters are displayed graphically. You can view the network performance status during a time segment, which is used to predict changes in network performance.

Historical Performance Data Query

- eSight AppBase allows you to query historical performance data.
- eSight AppBase displays historical performance data in graphs.
- eSight AppBase allows you to export query results to a CSV file.

4.7 Physical Resources

eSight AppBase allows you to query devices, frames, boards, subcards, and ports.

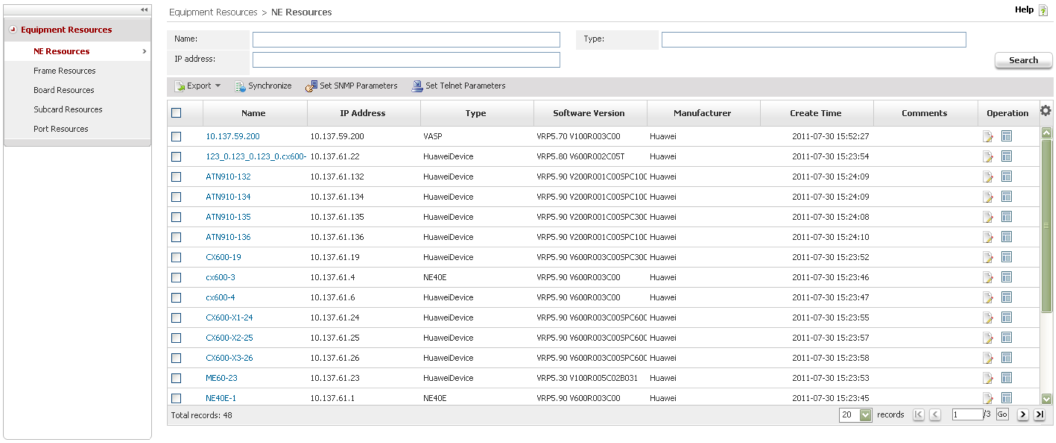
Device

With eSight AppBase, you can:

- Query and export device resources.
- Set SNMP and Telnet parameters in batches and synchronize device configurations in real time.
- Modify device remarks and maintenance information and query device information.

Figure 4-8 shows device resources.

Figure 4-8 Device resources



Name:
IP address:
Type:

□	Name	IP Address	Type	Software Version	Manufacturer	Create Time	Comments	Operation
□	10.137.59.200	10.137.59.200	VASP	VRP5.70 V100R003C00	Huawei	2011-07-30 15:52:27		
□	123_0.123_0.123_0.cx600-	10.137.61.22	HuaweiDevice	VRP5.80 V600R002C05T	Huawei	2011-07-30 15:23:54		
□	ATN910-132	10.137.61.132	HuaweiDevice	VRP5.90 V200R001C00SPC10C	Huawei	2011-07-30 15:24:09		
□	ATN910-134	10.137.61.134	HuaweiDevice	VRP5.90 V200R001C00SPC10C	Huawei	2011-07-30 15:24:09		
□	ATN910-135	10.137.61.135	HuaweiDevice	VRP5.90 V200R001C00SPC30C	Huawei	2011-07-30 15:24:08		
□	ATN910-136	10.137.61.136	HuaweiDevice	VRP5.90 V200R001C00SPC10C	Huawei	2011-07-30 15:24:10		
□	CX600-19	10.137.61.19	HuaweiDevice	VRP5.90 V600R003C00SPC30C	Huawei	2011-07-30 15:23:52		
□	cx600-3	10.137.61.4	NE40E	VRP5.90 V600R003C00	Huawei	2011-07-30 15:23:46		
□	cx600-4	10.137.61.6	HuaweiDevice	VRP5.90 V600R003C00	Huawei	2011-07-30 15:23:47		
□	CX600-X1-24	10.137.61.24	HuaweiDevice	VRP5.90 V600R003C00SPC60C	Huawei	2011-07-30 15:23:55		
□	CX600-X2-25	10.137.61.25	HuaweiDevice	VRP5.90 V600R003C00SPC60C	Huawei	2011-07-30 15:23:57		
□	CX600-X3-26	10.137.61.26	HuaweiDevice	VRP5.90 V600R003C00SPC60C	Huawei	2011-07-30 15:23:58		
□	ME60-23	10.137.61.23	HuaweiDevice	VRP5.30 V100R005C02B031	Huawei	2011-07-30 15:23:53		
□	NE40E-1	10.137.61.1	NE40E	VRP5.90 V600R003C00	Huawei	2011-07-30 15:23:45		

Total records: 48 20 records 1 /3 Go

frame

You can query and export frame resources and modify frame remarks.

Board

You can query and export board resources and modify board remarks.

Subcard

You can query and export subcard resources and modify subcard remarks.

Port

You can query and export port resources and modify port remarks.

4.8 Report Management

eSight AppBase generates instant and periodic reports when performing tasks, and allows you to export reports in PDF, Excel, Word, and PowerPoint formats. eSight AppBase also provides a variety of report templates, fully meeting network operation and maintenance requirements. In addition, eSight AppBase provides a report design tool that allows you to flexibly customize report templates.

Report Task Management

You can create and manage all report tasks on the eSight AppBase report task management page, as shown in **Figure 4-9**.

Report tasks are classified into instant tasks and periodic tasks. You can set email recipients in a task. After a task is executed, eSight AppBase sends the generated report to specified recipients by email.

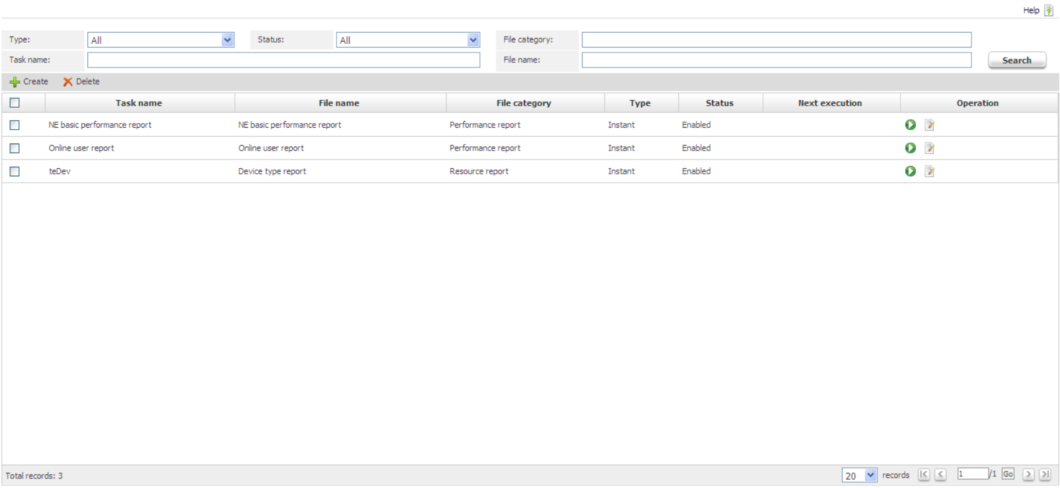
- Instant tasks

  Instant tasks must be executed manually. After a task is executed, you can view the generated report immediately and export the report in a specified format.

- Periodic tasks

  eSight AppBase executes a periodic task automatically based on the specified execution period. After a task is executed, eSight AppBase saves the generated reports. You can manage and view all reports generated by a periodic task, delete the reports in batches, or export them in batches and then send them in an email.

Figure 4-9 Report task management



Type: All
Status: All
File category:
Task name:
File name:

□	Task name	File name	File category	Type	Status	Next execution	Operation
□	NE basic performance report	NE basic performance report	Performance report	Instant	Enabled		
□	Online user report	Online user report	Performance report	Instant	Enabled		
□	teDev	Device type report	Resource report	Instant	Enabled		

Total records: 3
20 records 1 /1

Predefined Reports

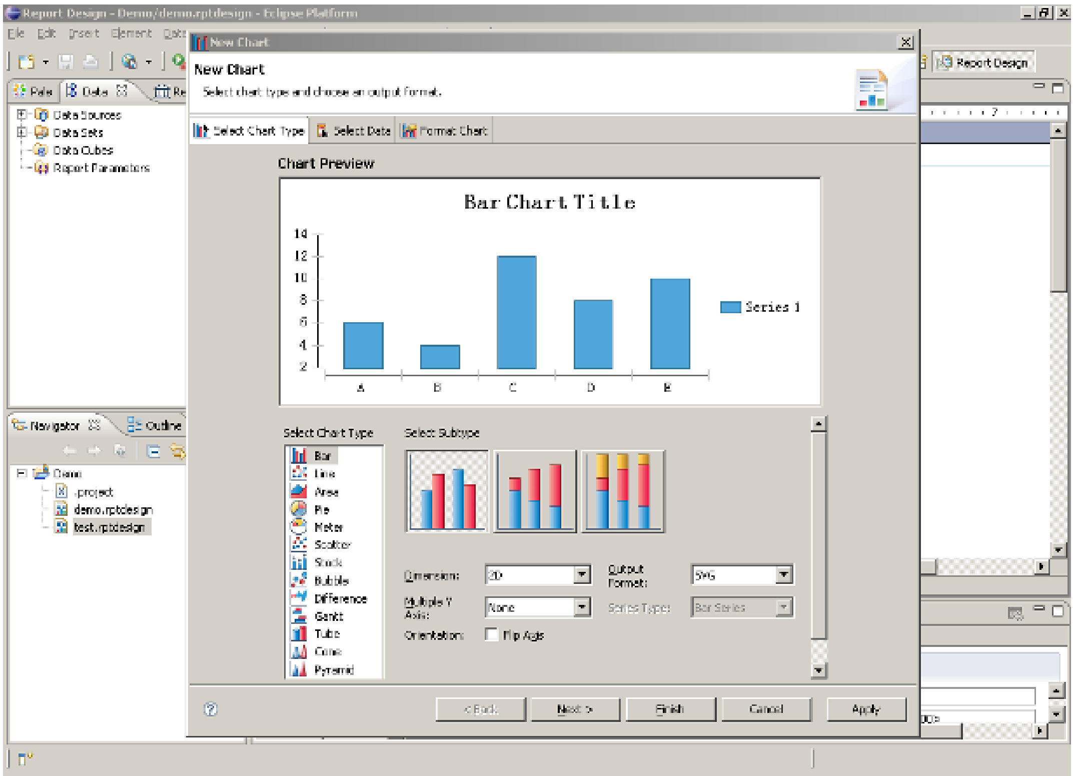
eSight AppBase provides predefined reports for the following:

- Device type report
- Device alarm severity report
- Link connection report
- NE connection report
- Interface connection report
- NE basic cpu usage report
- NE basic memory usage report
- Interface traffic performance report
-

User-defined Reports

eSight AppBase provides a powerful report design tool, which allows you to design reports and view the statistics immediately, as shown in **Figure 4-10**.

Figure 4-10 Report design tool



Report Design - Demo/demo.rptdesign - Eclipse Platform

New Chart

Select chart type and choose an output format.

Dimension: 2D

Output Format: SVG

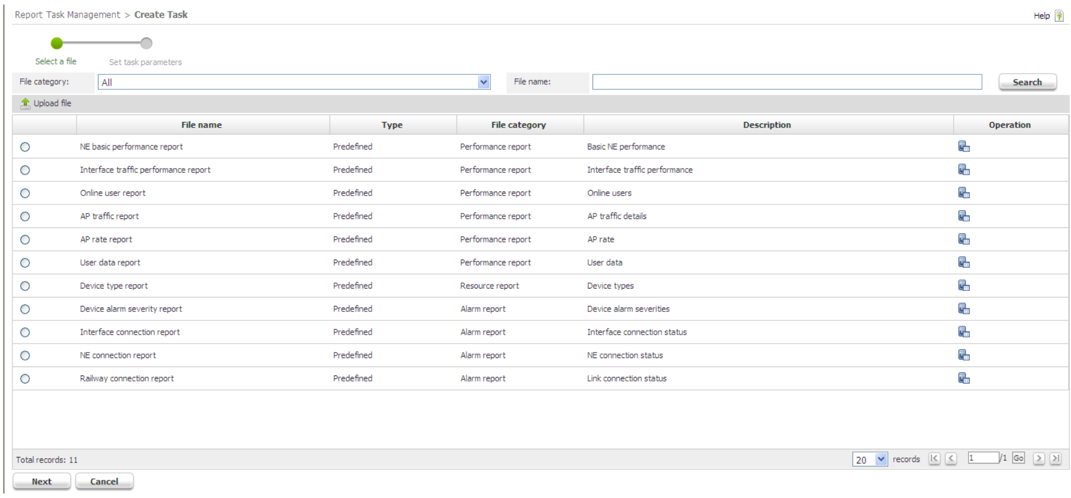
Multiple Y Axis: None

Series Type: Bar Series

Orientation: □ Flip Axis

The report design tool supports 13 flexible statistical methods. You can modify existing report design files or create a design file based on the template. You can also upload a design file to eSight AppBase, as shown in **Figure 4-11**.

Figure 4-11 Uploading a design file



Report Task Management > Create Task

File category: All

File name:

	File name	Type	File category	Description	Operation
○	NE basic performance report	Predefined	Performance report	Basic NE performance	
○	Interface traffic performance report	Predefined	Performance report	Interface traffic performance	
○	Online user report	Predefined	Performance report	Online users	
○	AP traffic report	Predefined	Performance report	AP traffic details	
○	AP rate report	Predefined	Performance report	AP rate	
○	User data report	Predefined	Performance report	User data	
○	Device type report	Predefined	Resource report	Device types	
○	Device alarm severity report	Predefined	Alarm report	Device alarm severities	
○	Interface connection report	Predefined	Alarm report	Interface connection status	
○	NE connection report	Predefined	Alarm report	NE connection status	
○	Railway connection report	Predefined	Alarm report	Link connection status	

Total records: 11

4.9 Customize Device

eSight AppBase provides user-defined device management to help enterprise users manage devices with many features. To manage basic device capabilities, you can customize the device types, performance counters, alarm parameters, configuration file management parameters, and device panels.

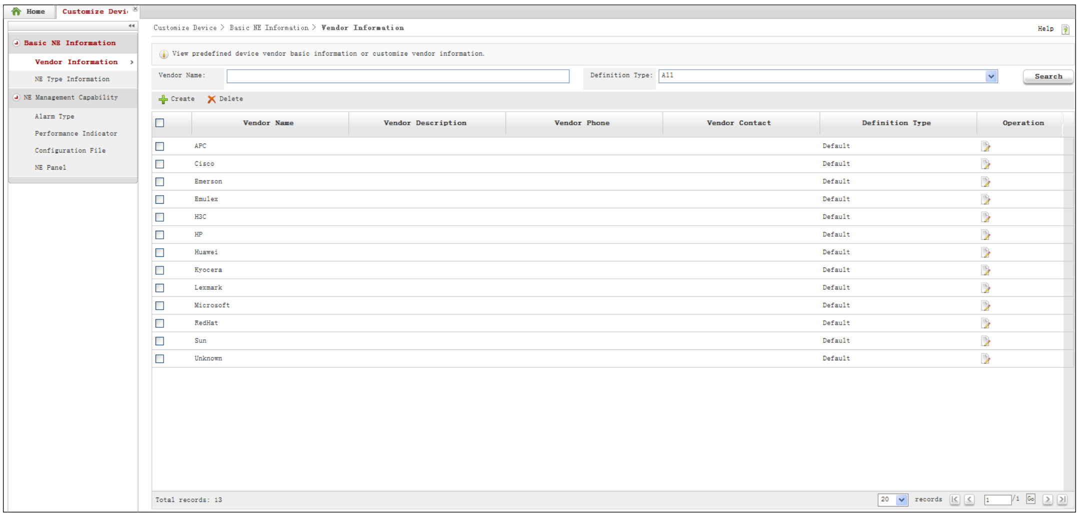
Vendor Information

You can add, delete, and modify parameters to customize the basic information about a device manufacturer.

- **Vendor Name**: Name of a device manufacturer.
- **Vendor Description**: Description of a device manufacturer. (Optional)
- **Vendor Phone**: Customer service phone number of a device manufacturer. (Optional)
- **Vendor Contact**: Contact person of a device manufacturer. The contact person is usually in charge of device maintenance. (Optional)
- **Definition Type**: Whether the basic information about a device manufacturer is customized by eSight AppBase developers or users. The options are **Default** and **User-defined**. **Default** indicates that the basic information is customized by eSight AppBase developers and **User-defined** indicates that the basic information can be customized by users.

Figure 4-12 shows user-defined information about a device manufacturer.

Figure 4-12 Vendor information



Customize Device > Basic NE Information > **Vendor Information**

View predefined device vendor basic information or customize vendor information.

Vendor Name:

Definition Type: All

□	Vendor Name	Vendor Description	Vendor Phone	Vendor Contact	Definition Type	Operation
□	APC				Default	
□	Cisco				Default	
□	Emerson				Default	
□	Emulex				Default	
□	H3C				Default	
□	HP				Default	
□	Huawei				Default	
□	Kyocera				Default	
□	Lexmark				Default	
□	Microsoft				Default	
□	RedHat				Default	
□	Sun				Default	
□	Unknown				Default	

Total records: 13 20 records 1/1 Go

NE Type Information

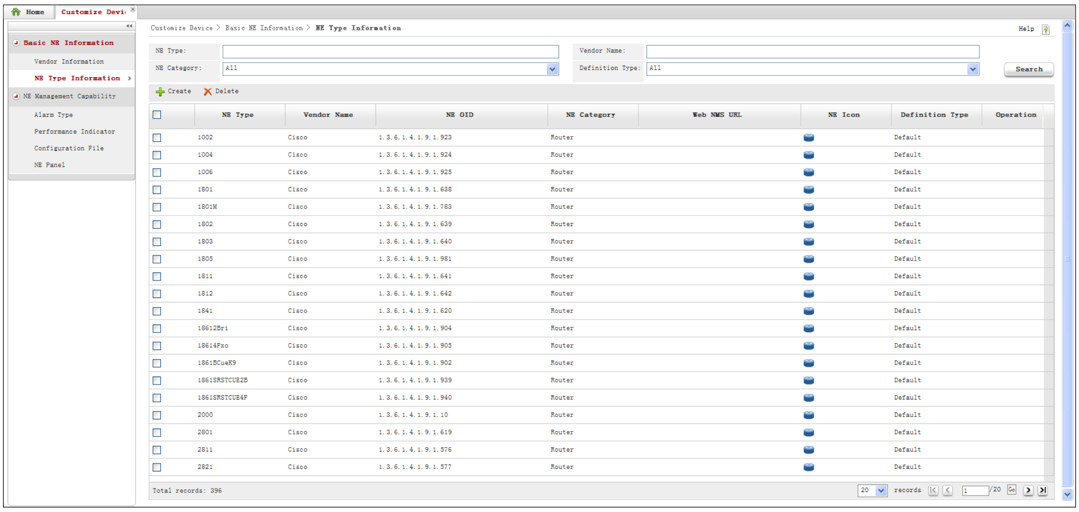
Before a device is added to eSight AppBase, the device is shown as **unknown** if eSight AppBase does not contain predefined information for the device. eSight AppBase allows you only to view the basic device information. Management capabilities, for example, alarm functions, are not provided. eSight AppBase then displays the customized device information and monitors certain information, such as alarms and performance counters.

- **NE OID**: NE type identifier.
- **NE Category**: NE category, such as switch, router, server, printer, and security device.
- **Web NMS URL**: Some devices have Web network management systems (NMSs). After adding the link to a device's Web NMS, you can click the link to access the Web NMS.

- **Current NE Icon**: Icon that identifies a device type, which can be customized by users.
- **Definition Type**: Whether device information is customized by eSight AppBase developers or users.

Figure 4-13 shows the page for customizing device information.

Figure 4-13 NE type information



NE Type:

NE Category: All

Vendor Name:

Definition Type: All

□	NE Type	Vendor Name	NE OID	NE Category	Web NMS URL	NE Icon	Definition Type	Operation
□	1002	Cisco	1.3.6.1.4.1.9.1.923	Router		●	Default	
□	1004	Cisco	1.3.6.1.4.1.9.1.924	Router		●	Default	
□	1006	Cisco	1.3.6.1.4.1.9.1.925	Router		●	Default	
□	1801	Cisco	1.3.6.1.4.1.9.1.638	Router		●	Default	
□	1801M	Cisco	1.3.6.1.4.1.9.1.783	Router		●	Default	
□	1802	Cisco	1.3.6.1.4.1.9.1.639	Router		●	Default	
□	1803	Cisco	1.3.6.1.4.1.9.1.640	Router		●	Default	
□	1805	Cisco	1.3.6.1.4.1.9.1.981	Router		●	Default	
□	1811	Cisco	1.3.6.1.4.1.9.1.641	Router		●	Default	
□	1812	Cisco	1.3.6.1.4.1.9.1.642	Router		●	Default	
□	1841	Cisco	1.3.6.1.4.1.9.1.620	Router		●	Default	
□	18612Bri	Cisco	1.3.6.1.4.1.9.1.904	Router		●	Default	
□	18614Fxo	Cisco	1.3.6.1.4.1.9.1.905	Router		●	Default	
□	1861BCueK9	Cisco	1.3.6.1.4.1.9.1.902	Router		●	Default	
□	1861SRSTCUE2B	Cisco	1.3.6.1.4.1.9.1.939	Router		●	Default	
□	1861SRSTCUE4F	Cisco	1.3.6.1.4.1.9.1.940	Router		●	Default	
□	2000	Cisco	1.3.6.1.4.1.9.1.10	Router		●	Default	
□	2801	Cisco	1.3.6.1.4.1.9.1.619	Router		●	Default	
□	2811	Cisco	1.3.6.1.4.1.9.1.576	Router		●	Default	
□	2821	Cisco	1.3.6.1.4.1.9.1.577	Router		●	Default	

Total records: 396 20 records 1 /20

Alarm Type

You can add, delete, and modify SNMP v1 or SNMP v2c/v3 alarm parameters as required. eSight AppBase discards alarms that are not predefined. When an alarm is customized, eSight AppBase's alarm module parses and displays the alarm on eSight AppBase.

When you delete a user-defined alarm parameter, eSight AppBase does not delete the alarm's historical information. eSight AppBase's alarm module, however, no longer processes the alarm.

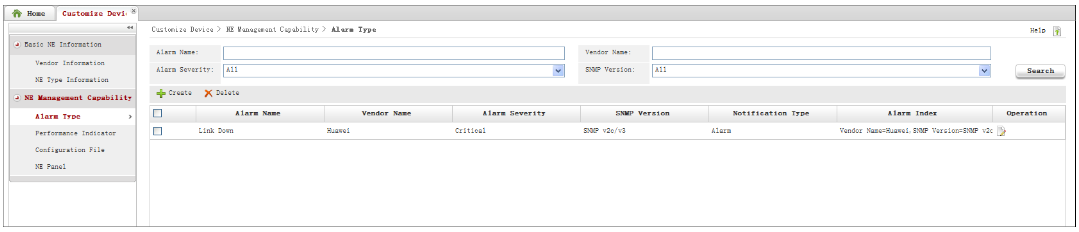
eSight AppBase allows you to change the alarm severity and event type, and modify the alarm cause, suggestion, details, and alarm locating parameters.

- **Vendor Name**: Name of a device manufacturer. Alarms are customized by device manufacturer because the alarm parameters differ depending on the device manufacturer.
- **Alarm Name**: Name of an alarm.
- **Alarm Severity**: Severity of an alarm. Alarm severities are warning, minor, major, and critical, which are the same as those defined in the alarm module.
- **Notification Type**: Alarm category. Alarm categories include the clear alarm, fault alarm, or event.
- **Event type**: Alarm types include communication alarm, device alarm, processing error alarm, QoS alarm, environmental alarm, integrity alarm, operation alarm, physical resource alarm, and security alarm.
- **SNMP Version**: SNMP versions that are supported on eSight AppBase. eSight AppBase supports **SNMPv1** and **SNMP v2c/v3**.
- **Generic**, **Specific**, and **Enterprise ID**: Key parameters for locating an SNMP v1 alarm.

- **Alarm OID**: Identifier of an SNMP v2c/v3 alarm, which is the same as the trap OID in an alarm packet.
- **Alarm Cause**: Possible cause of an alarm.
- **Clearance Suggestion**: Method of clearing an alarm.
- **Details**: Further alarm details.
- **New Parameter**: Parameters for locating an alarm.
-

Figure 4-14 and Figure 4-15 show the pages for customizing and adding alarm parameters.

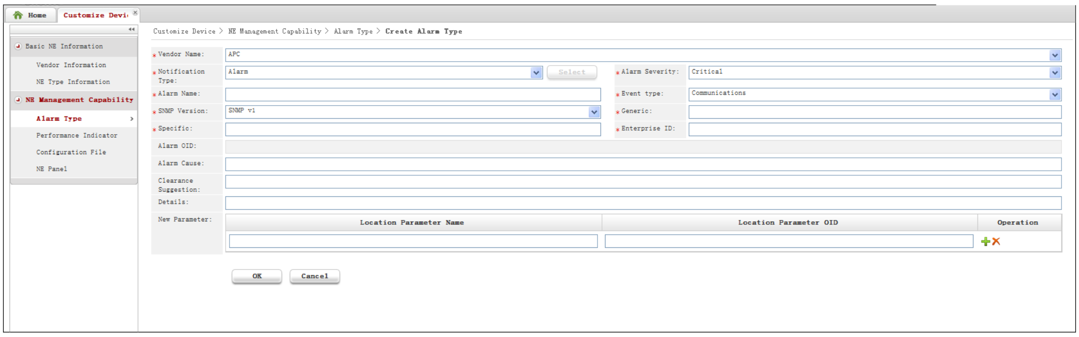
Figure 4-14 Alarm Type



Alarm Name:
Alarm Severity: All
Vendor Name:
SNMP Version: All

□	Alarm Name	Vendor Name	Alarm Severity	SNMP Version	Notification Type	Alarm Index	Operation
□	Link Down	Huawei	Critical	SNMP v2c/v3	Alarm	Vendor Name=Huawei, SNMP Version=SNMP v2c	

Figure 4-15 Adding alarm Type



*Vendor Name: APC
*Notification Type: Alarm
*Alarm Severity: Critical
*Alarm Name:
*Event type: Communications
*SNMP Version: SNMP v1
*Generic:
*Specific:
*Enterprise ID:
Alarm OID:
Alarm Cause:
Clearance Suggestion:
Details:
New Parameter:

Location Parameter Name	Location Parameter OID	Operation

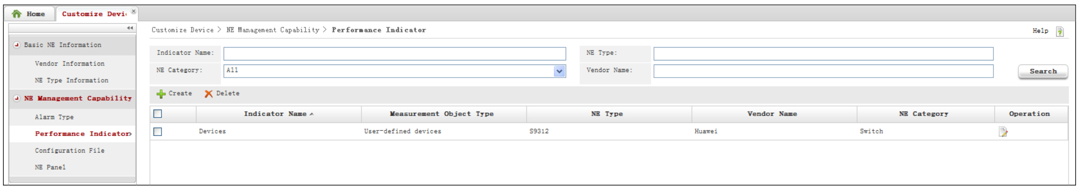
Performance Indicator

You can add, delete, and modify performance counters as required. After customizing performance counters, you can create a monitoring instance in the performance management module. Then the performance management module will collect the user-defined performance counters in the next collection period.

- **Indicator Name**: Name of a collected performance counter.
- **Measurement Object Type**: Group of collected performance counters whose collection objects are the same. For example, user-defined device counter group, frame counter group, board counter group, or interface counter group. To collect a user-defined interface performance counter, select the user-defined interface counter group.
- **NE Type**: Model of a device whose user-defined performance counters can be collected.
- **Calculation Formula**: Expression for calculating performance counters for an MIB object.

Figure 4-16 and **Figure 4-17** show the pages for viewing and customizing performance counters.

Figure 4-16 Viewing performance counters

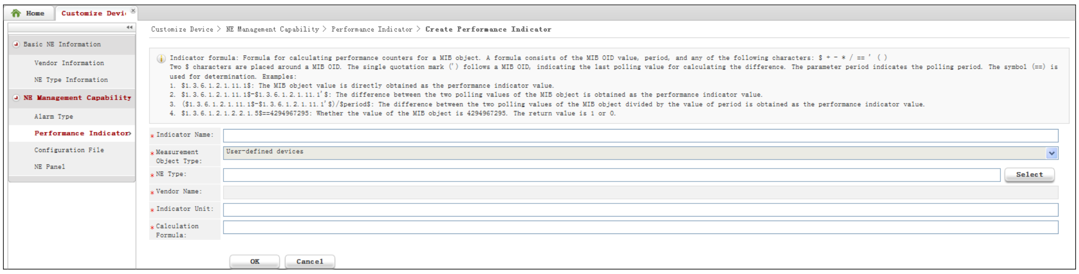


Customize Device > NE Management Capability > **Performance Indicator**

Indicator Name:
NE Type:
NE Category: All
Vendor Name:

□	Indicator Name	Measurement Object Type	NE Type	Vendor Name	NE Category	Operation
□	Devices	User-defined devices	S9312	Huawei	Switch	

Figure 4-17 Customizing performance counters



Customize Device > NE Management Capability > Performance Indicator > **Create Performance Indicator**

Indicator formula: Formula for calculating performance counters for a MIB object. A formula consists of the MIB OID value, period, and any of the following characters: $ + - * / == ' ( )
Two $ characters are placed around a MIB OID. The single quotation mark (') follows a MIB OID, indicating the last polling value for calculating the difference. The parameter period indicates the polling period. The symbol (==) is used for determination. Examples:
1. $1.3.6.1.2.1.11.1$: The MIB object value is directly obtained as the performance indicator value.
2. $1.3.6.1.2.1.11.1$-$1.3.6.1.2.1.11.1'$: The difference between the two polling values of the MIB object is obtained as the performance indicator value.
3. ($1.3.6.1.2.1.11.1$-$1.3.6.1.2.1.11.1'$)/$period$: The difference between the two polling values of the MIB object divided by the value of period is obtained as the performance indicator value.
4. $1.3.6.1.2.1.2.2.1.5$==4294967295: Whether the value of the MIB object is 4294967295. The return value is 1 or 0.

* Indicator Name:
* Measurement Object Type: User-defined devices
* NE Type:
* Vendor Name:
* Indicator Unit:
* Calculation Formula:

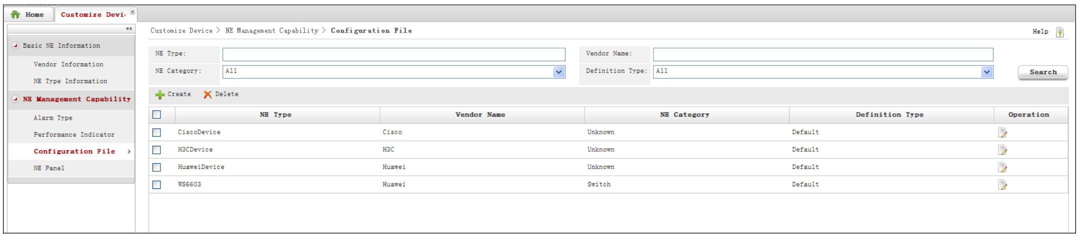
Configuration File

You can customize three commands for a configuration file. After customizing a device's configuration file, you can create a backup task for the device in the configuration file management module. Then eSight AppBase can manage the device's configuration file backup.

- **NE Type**: Type of the device whose configuration file commands must be customized.
- **Backup command**: Command for backing up a device's configuration file.
- **Restore command**: Command for restoring a device's configuration file.
- **Restart command**: Command for restarting a device.

Figure 4-18 shows the page for customizing a configuration file.

Figure 4-18 Customizing a configuration file



Customize Device > NE Management Capability > **Configuration File**

NE Type:
Vendor Name:
NE Category: All
Definition Type: All

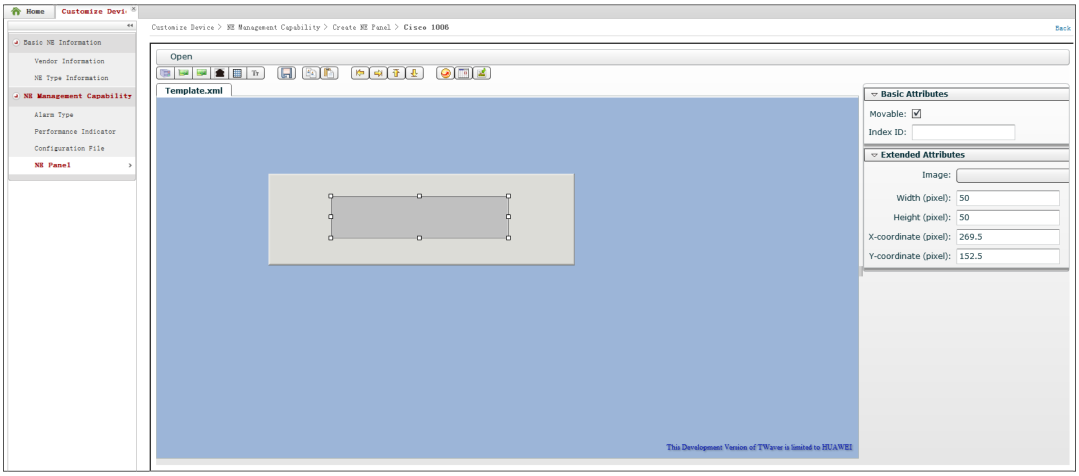
□	NE Type	Vendor Name	NE Category	Definition Type	Operation
□	CiscoDevice	Cisco	Unknown	Default	
□	H3CDevice	H3C	Unknown	Default	
□	HuaweiDevice	Huawei	Unknown	Default	
□	WS6603	Huawei	Switch	Default	

NE Panel

By default, eSight AppBase displays default NE panels for user-defined devices. You can upload a device photo or high-fidelity picture to customize the NE panel for a subrack, panel, subcard, or port. After customization, the device photo or high-fidelity picture is displayed when you open the NE panel.

Figure 4-19 shows the page for customizing an NE panel.

Figure 4-19 Customizing an NE panel



Movable: ☑

Index ID:

Image:

Width (pixel): 50

Height (pixel): 50

X-coordinate (pixel): 269.5

Y-coordinate (pixel): 152.5

4.10 Configuration File Management

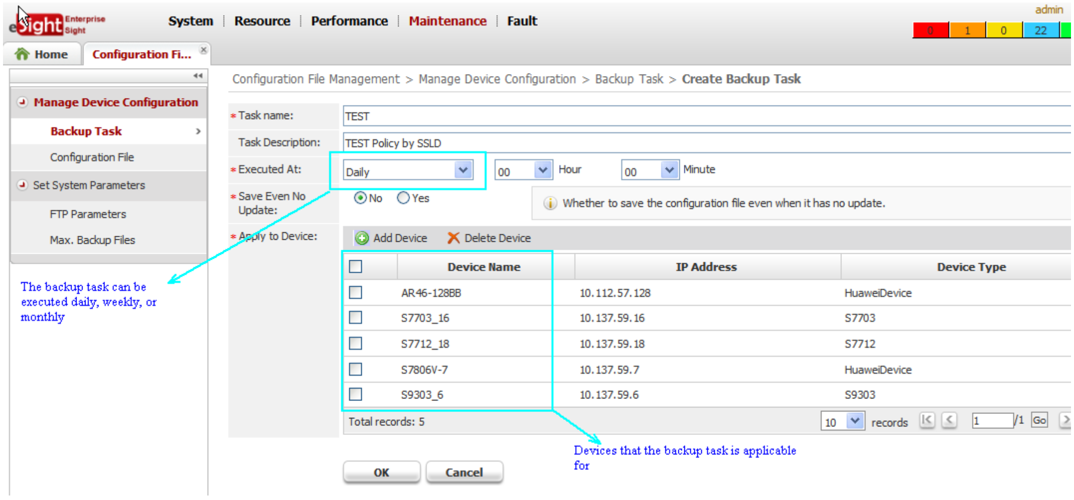
eSight AppBase allows you to back up, restore, and compare device configuration files, and manage baseline file versions. When the network is faulty, you can compare the configuration file in use with the one that was saved when the network was running normally. By checking the added, modified, and deleted information, you can quickly locate the fault and rectify it.

Device Configuration Management

- Backup Tasks

  eSight AppBase can be configured to periodically back up the configuration files of devices specified in a backup task daily, weekly, or monthly at a specified time, as shown in **Figure 4-20**. eSight AppBase can also perform instant backups.

Figure 4-20 Managing device configuration



Configuration File Management > Manage Device Configuration > Backup Task > **Create Backup Task**

* Task name: TEST

Task Description: TEST Policy by SSLD

* Executed At: Daily; 00 Hour; 00 Minute

* Save Even No Update: ● No ○ Yes — Whether to save the configuration file even when it has no update.

* Apply to Device:

□	Device Name	IP Address	Device Type
□	AR46-128BB	10.112.57.128	HuaweiDevice
□	S7703_16	10.137.59.16	S7703
□	S7712_18	10.137.59.18	S7712
□	S7806V-7	10.137.59.7	HuaweiDevice
□	S9303_6	10.137.59.6	S9303

Total records: 5 — 10 records — 1 /1 Go

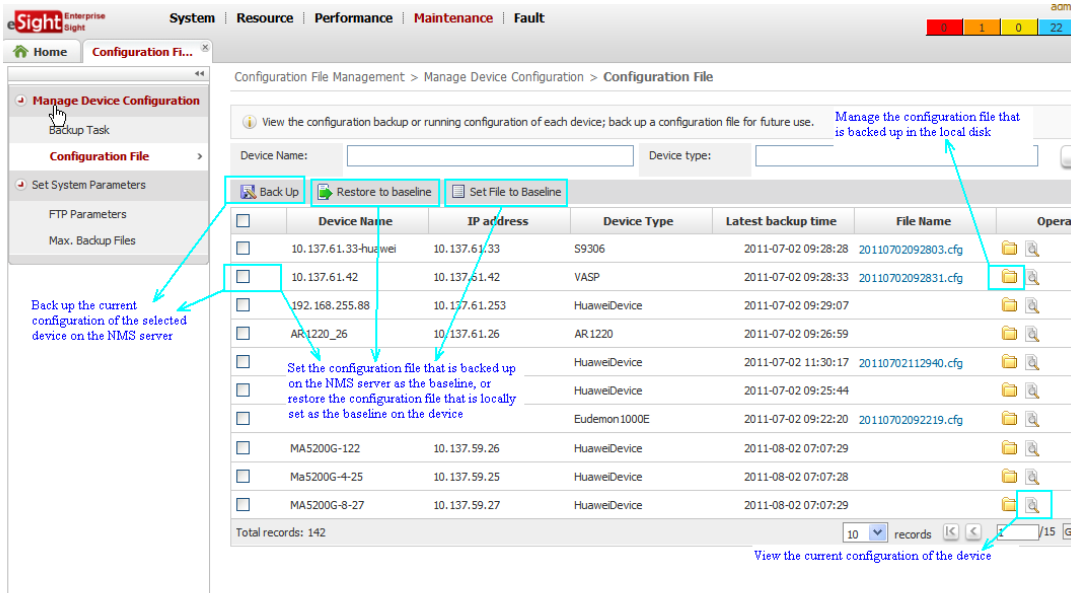
The backup task can be executed daily, weekly, or monthly

Devices that the backup task is applicable for

- Configuration Backup Files

  You can back up the configuration file of a specified device, upload a backup configuration file, set a configuration file as a baseline version, and view the configuration on a device, as shown in **Figure 4-21**.

Figure 4-21 Setting a configuration file as a baseline version



Configuration File Management > Manage Device Configuration > **Configuration File**

View the configuration backup or running configuration of each device; back up a configuration file for future use.

Device Name:

Device type:

□	Device Name	IP address	Device Type	Latest backup time	File Name	Opera
□	10.137.61.33-huawei	10.137.61.33	S9306	2011-07-02 09:28:28	20110702092803.cfg	
□	10.137.61.42	10.137.61.42	VASP	2011-07-02 09:28:33	20110702092831.cfg	
□	192.168.255.88	10.137.61.253	HuaweiDevice	2011-07-02 09:29:07		
□	AR1220_26	10.137.61.26	AR1220	2011-07-02 09:26:59		
□			HuaweiDevice	2011-07-02 11:30:17	20110702112940.cfg	
□			HuaweiDevice	2011-07-02 09:25:44		
□			Eudemon1000E	2011-07-02 09:22:20	20110702092219.cfg	
□	MA5200G-122	10.137.59.26	HuaweiDevice	2011-08-02 07:07:29		
□	Ma5200G-4-25	10.137.59.25	HuaweiDevice	2011-08-02 07:07:28		
□	MA5200G-8-27	10.137.59.27	HuaweiDevice	2011-08-02 07:07:29		

Total records: 142 — 10 records — 1 /15

Manage the configuration file that is backed up in the local disk

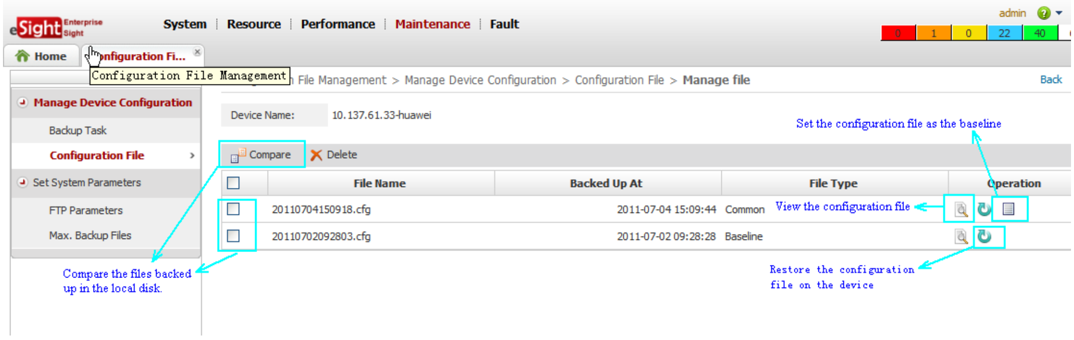
Back up the current configuration of the selected device on the NMS server

Set the configuration file that is backed up on the NMS server as the baseline, or restore the configuration file that is locally set as the baseline on the device

View the current configuration of the device

You can view, compare, and delete configuration files that are backed up on a local computer. The file comparison function allows you to compare configuration files backed up on the eSight AppBase server, as shown in **Figure 4-22**.

Figure 4-22 Comparing configuration files



Device Name: 10.137.61.33-huawei

□	File Name	Backed Up At	File Type	Operation
□	20110704150918.cfg	2011-07-04 15:09:44	Common	
□	20110702092803.cfg	2011-07-02 09:28:28	Baseline	

Set the configuration file as the baseline

View the configuration file

Compare the files backed up in the local disk.

Restore the configuration file on the device

System Parameter Management

- FTP parameters

  You can set the FTP service user name, password, and root directory on the eSight AppBase server. The FTP service running status is displayed on the **FTP Parameters** page.

- Maximum number of configuration files

  You can set the maximum number of configuration files on the eSight AppBase server for each device. If the number of a device's configuration files on the eSight AppBase server exceeds the maximum, eSight AppBase automatically deletes the earliest configuration file.

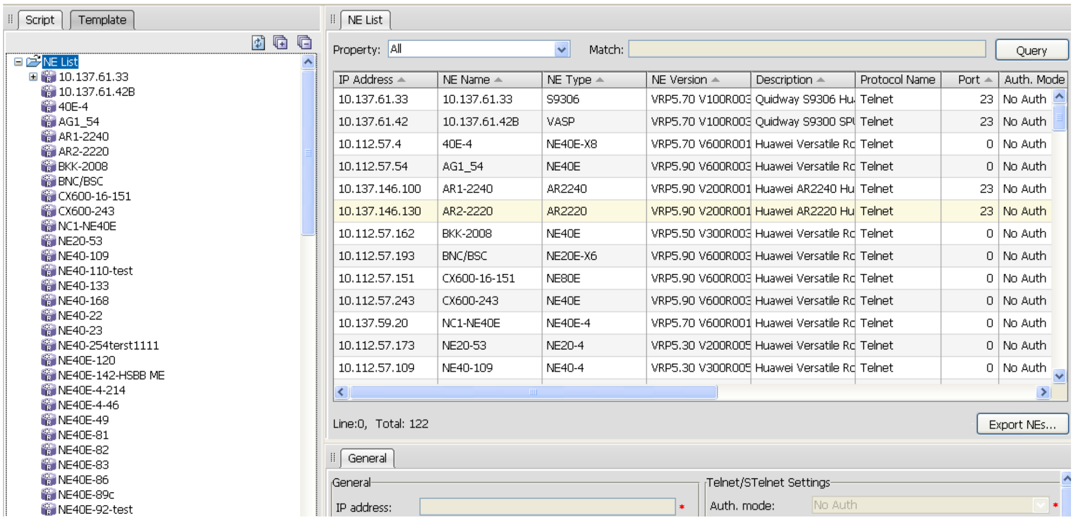
4.11 Smart Configuration Tool

The smart configuration tool is used to configure one or more Huawei devices.

Multi-Switch Configuration

You can customize the batch configuration script and configure services for Huawei NEs in batches, as shown in **Figure 4-23**.

Figure 4-23 Configuring multiple switches



NE List
10.137.61.33
10.137.61.42B
40E-4
AG1_54
AR1-2240
AR2-2220
BKK-2008
BNC/BSC
CX600-16-151
CX600-243
NC1-NE40E
NE20-53
NE40-109
NE40-110-test
NE40-133
NE40-168
NE40-22
NE40-23
NE40-254terst1111
NE40E-120
NE40E-142-HSBB ME
NE40E-4-214
NE40E-4-46
NE40E-49
NE40E-81
NE40E-82
NE40E-83
NE40E-86
NE40E-89c
NE40E-92-test

Property: All Match:

IP Address	NE Name	NE Type	NE Version	Description	Protocol Name	Port	Auth. Mode
10.137.61.33	10.137.61.33	S9306	VRP5.70 V100R003	Quidway S9306 Hu	Telnet	23	No Auth
10.137.61.42	10.137.61.42B	VASP	VRP5.70 V100R003	Quidway S9300 SPI	Telnet	23	No Auth
10.112.57.4	40E-4	NE40E-X8	VRP5.70 V600R001	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.54	AG1_54	NE40E	VRP5.90 V600R003	Huawei Versatile Rc	Telnet	0	No Auth
10.137.146.100	AR1-2240	AR2240	VRP5.90 V200R001	Huawei AR2240 Hu	Telnet	23	No Auth
10.137.146.130	AR2-2220	AR2220	VRP5.90 V200R001	Huawei AR2220 Hu	Telnet	23	No Auth
10.112.57.162	BKK-2008	NE40E	VRP5.50 V300R003	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.193	BNC/BSC	NE20E-X6	VRP5.90 V600R003	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.151	CX600-16-151	NE80E	VRP5.90 V600R003	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.243	CX600-243	NE40E	VRP5.90 V600R003	Huawei Versatile Rc	Telnet	0	No Auth
10.137.59.20	NC1-NE40E	NE40E-4	VRP5.70 V600R001	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.173	NE20-53	NE20-4	VRP5.30 V200R005	Huawei Versatile Rc	Telnet	0	No Auth
10.112.57.109	NE40-109	NE40-4	VRP5.30 V300R005	Huawei Versatile Rc	Telnet	0	No Auth

Line:0, Total: 122

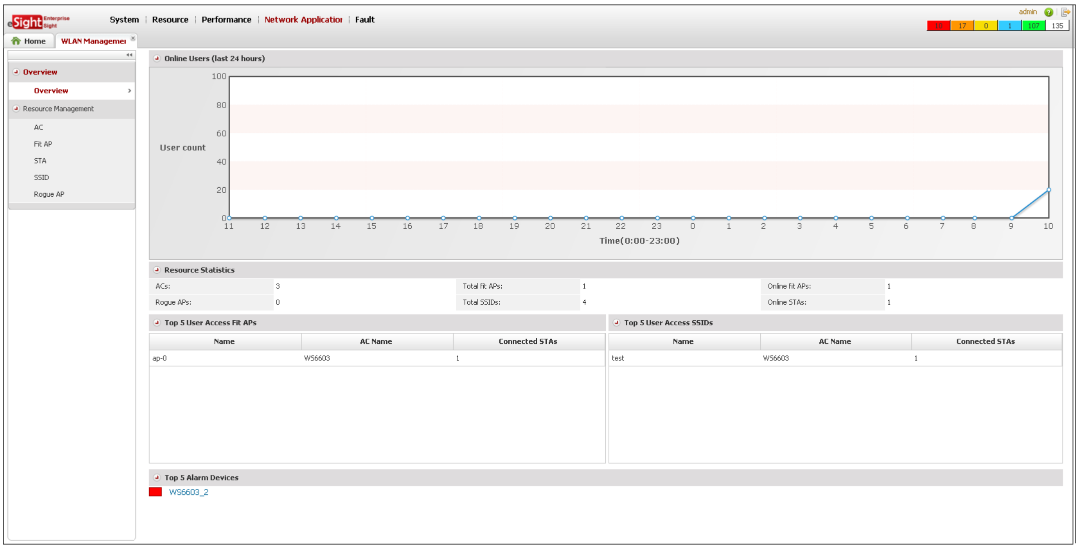
General
IP address:

Telnet/STelnet Settings
Auth. mode: No Auth

4.12 WLAN Service Management

A WLAN is a network system that enables computers to communicate and share resources wirelessly. WLANs can access the Ethernet quickly.

Figure 4-24 WLAN service management



Resource Statistics

ACs:	3	Total fit APs:	1	Online fit APs:	1
Rogue APs:	0	Total SSIDs:	4	Online STAs:	1

Top 5 User Access Fit APs

Name	AC Name	Connected STAs
ap-0	WS6603	1

Top 5 User Access SSIDs

Name	AC Name	Connected STAs
test	WS6603	1

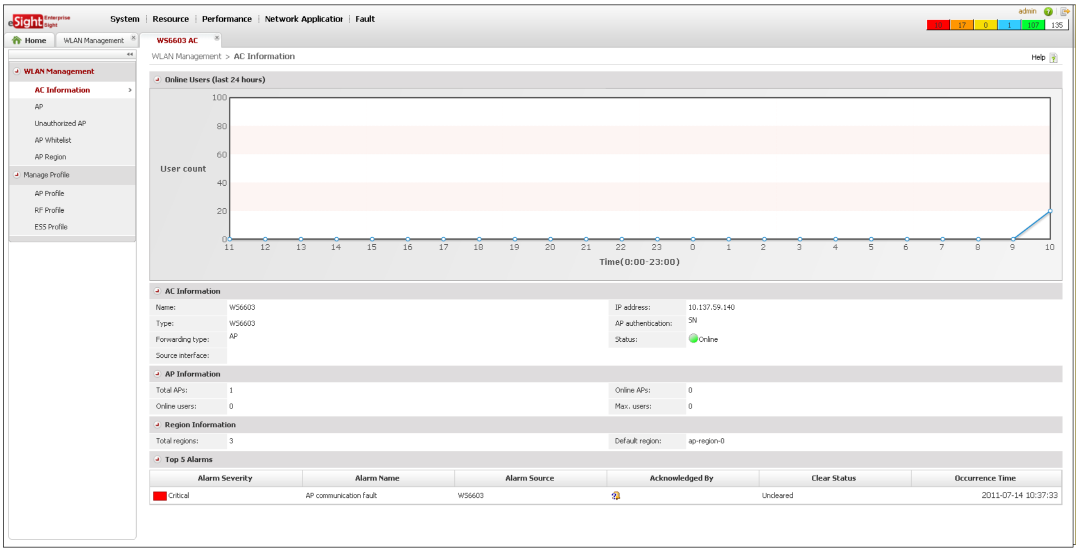
Top 5 Alarm Devices

🟥 WS6603_2

Configuration Management

Figure 4-25 shows the AC management.

Figure 4-25 AC management



AC Information

Name:	WS6603	IP address:	10.137.59.140
Type:	WS6603	AP authentication:	SN
Forwarding type:	AP	Status:	● Online
Source interface:			

AP Information

Total APs:	1	Online APs:	0
Online users:	0	Max. users:	0

Region Information

Total regions:	3	Default region:	ap-region-0

Top 5 Alarms

Alarm Severity	Alarm Name	Alarm Source	Acknowledged By	Clear Status	Occurrence Time
🟥 Critical	AP communication fault	WS6603		Uncleared	2011-07-14 10:37:33

The WLAN configuration management function allows you to configure WLAN devices. You can enable APs to communicate with an AC by setting the AP whitelist, confirming APs' identities manually, and deploying APs offline.

- AC Information

  On the AC management page, you can add VASPs and set the source port, AP authentication mode, and forwarding type.

- AP

  An AP functions as a bridge to convert frames transmitted between wireless terminals and a LAN. On eSight AppBase, you can configure basic AP information, manage radios, and bind an ESS profile to a radio when creating an AP. You can also import APs in batches from a predefined table and bind the three types of profiles to APs in batches.

- Unauthorized AP

  You can view unauthorized APs discovered by the current AC, confirm their identities, and add them to the whitelist so that they can go online.

- AP whitelist

  You can configure the AP whitelist to allow authorized APs to go online. You can import one or multiple AP MAC addresses or SNs to the AP whitelist.

- AP region

  APs are added to different regions to reduce the time spent in adjusting AP parameters and the impact of AP parameter adjustment on user access. Each AP region has a name, deployment mode, alias, and default region.

The profile management function allows you to configure NE predefined profiles.

- AP profile

  Used to specify the maximum transmission unit of the access point (AP) Ethernet port and configure log backup.

- Radio profile

Used to specify parameters, such as the radio type, rate, power, and whether to occupy a channel during wireless transmission.

- ESS profile

  The extended service set (ESS) profile is a set of service parameters, such as **SSID**, **Service VLAN**, **DataTraffer ESSIf**, **Access Max User**, **WLAN User Access Security Manager**. After an ESS profile is bound to a specified radio on an AP, the service parameters are applied to a virtual access point (VAP), a WLAN service entity.

Network Monitoring

This function allows you to view information such as all physical resources, rogue APs, statistics, and performance counters.

- Physical resources

  Basic AC information: AC status, name, type, AP authentication mode, and forwarding type

  Basic AP information: AP status, name, type, AC name, home region, location, bound radio profile, and bound ESS profile

  Spanning tree algorithm (STA): user's MAC address, AC name, AP name, radio ID, and SSID
- Rogue AP

  Information about rogue APs and affected APs
- Resource statistics

  Network overview: line chart for online users, top 5 accessed fit APs and SSIDs, AC resource statistics, and key device statistics by alarm severity

  AC statistics: AP information, including the total number of APs, number of online APs, number of online users, and maximum number of users; AC region information, including the total number of regions, default region name, number of regions counted by forwarding mode; top 5 AC alarms; line chart for online users in last 24 hours

  AP statistics: AP top 5 alarms and AP performance counters

  SSID statistics: AC name, number of fit APs, number of virtual access points (VAP), and number of terminals connected to APs
- Performance statistics

  Terminals associated with APs, AP physical resources, AP traffic, radio traffic, and real-time STA traffic performance statistics

Fault Management

eSight AppBase provides alarms related to communication, the surrounding environment, and AP deployment to help locate and rectify faults.

eSight AppBase provides the Event for AP deployment process, is convenient for User inspect the current status of NE.

Report Management

eSight AppBase provides predefined reports about AP traffic details, line charts for online STA users, AP rates, and STA information.

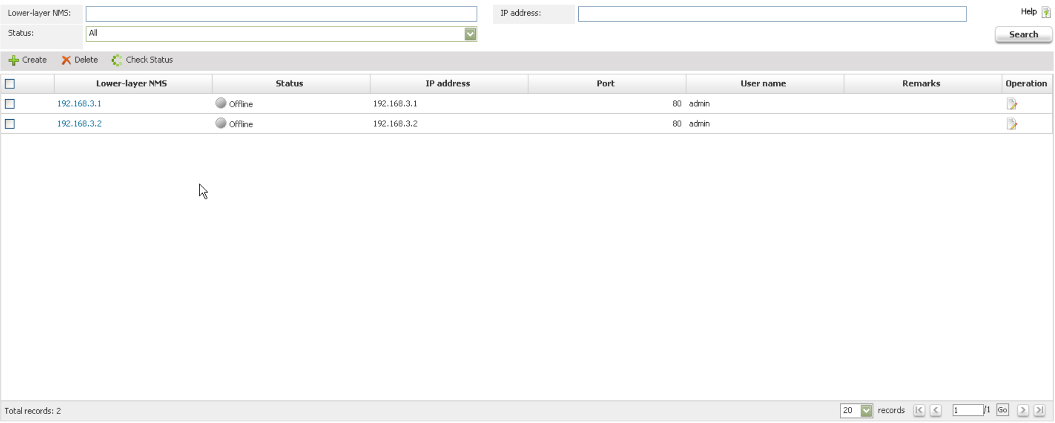
4.13 Lower-Layer NMSs

eSight AppBase allows you to divide a network into several layers in order to manage the NEs on the network by layer. eSight AppBase provides links to lower-layer NMSs. By clicking a link, you can view alarms, performance counters, reports, and the network topology on a lower-layer NMS.

Figure 4-26 and **Figure 4-27** show the two modes for managing lower-layer NMSs.

- On the lower-layer NMS management page, you can add, delete, and modify lower-layer NMSs, and manually check the connections between eSight AppBase and lower-layer NMSs.
- On the Portal for lower-layer NMSs, you can monitor the connections in real time and click a link to access a lower-layer NMS.

Figure 4-26 Managing lower-layer NMSs

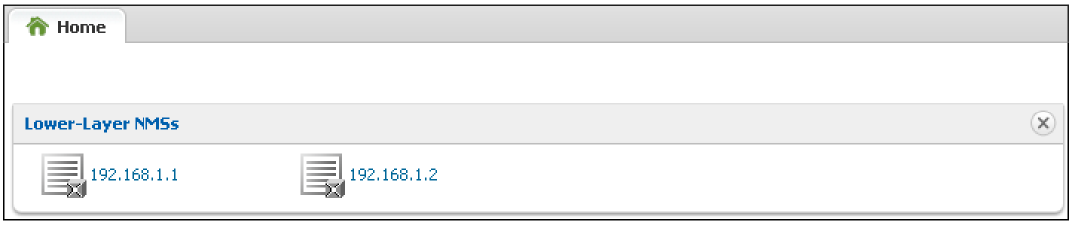


Lower-layer NMS:
IP address:
Status: All

□	Lower-layer NMS	Status	IP address	Port	User name	Remarks	Operation
□	192.168.3.1	Offline	192.168.3.1	80	admin		
□	192.168.3.2	Offline	192.168.3.2	80	admin		

Total records: 2 20 records 1 /1 Go

Figure 4-27 Portal for lower-layer NMSs

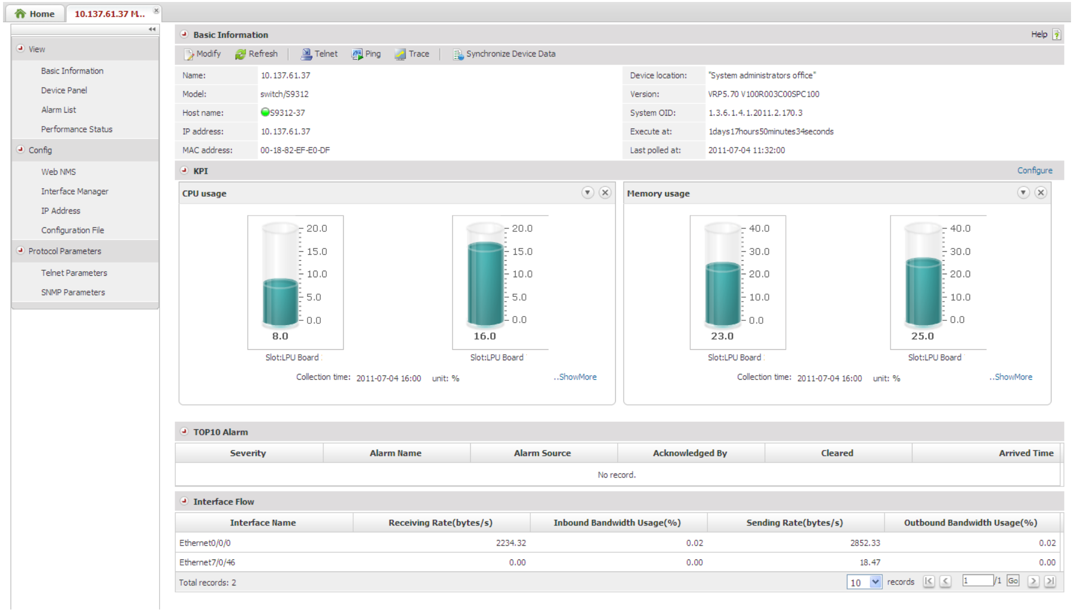


4.14 Single NE Feature Management

This topic describes features managed by eSight AppBase.

Figure 4-28 shows the page for managing NEs.

Figure 4-28 Managing NEs



Name:	10.137.61.37	Device location:	"System administrators office"
Model:	switch/S9312	Version:	VRP5.70 V100R003C00SPC100
Host name:	●S9312-37	System OID:	1.3.6.1.4.1.2011.2.170.3
IP address:	10.137.61.37	Execute at:	1days17hours50minutes34seconds
MAC address:	00-18-82-EF-E0-DF	Last polled at:	2011-07-04 11:32:00

Collection time: 2011-07-04 16:00 unit: %

Collection time: 2011-07-04 16:00 unit: %

TOP10 Alarm

Severity	Alarm Name	Alarm Source	Acknowledged By	Cleared	Arrived Time
No record.					

Interface Flow

Interface Name	Receiving Rate(bytes/s)	Inbound Bandwidth Usage(%)	Sending Rate(bytes/s)	Outbound Bandwidth Usage(%)
Ethernet0/0/0	2234.32	0.02	2852.33	0.02
Ethernet7/0/46	0.00	0.00	18.47	0.00

Total records: 2 10 records 1 /1 Go

Functions

View

- **Basic Information**: provides an overview of NE management, including basic information about the NE, KPIs, top *n* alarms, and interface traffic.
- **Device Panel**: graphically displays an NE.
- **Alarm List**: displays an NE's active alarms.
- **Performance Status**: displays an NE's performance counters.

Config

- **WEB NMS**: displays the Web management page provided by an NE.
- **Interface Manager**: lists an NE's interfaces and allows you to enable or disable an interface and suppress or allow an alarm.
- **IP Addresses**: lists an NE's IP addresses.
- **Configuration Files**: allows you to view and back up an NE's configuration files.

Protocol Parameters

- **Telnet Parameters**: allows you to modify an NE's Telnet parameters.
- **SNMP Parameters**: allows you to modify an NE's SNMP parameters.

Information Displayed on Basic Information

- **Basic Information**: displays parameters such as **Name**, **Model**, **SYSOID**, and **Version**. You can also click **Telnet**, **Ping**, and **Trace** to perform the corresponding operations.
- **KPI**: charts an NE's KPIs.

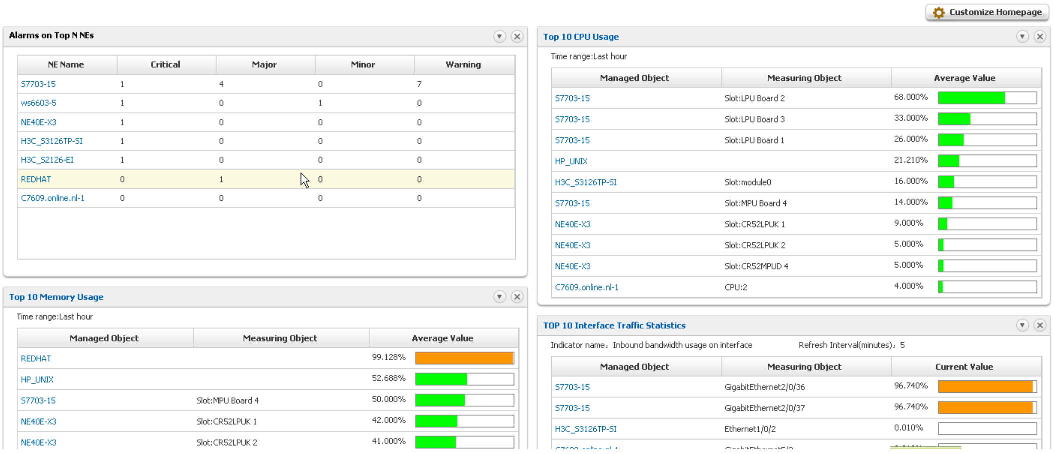
- **TOP10 Alarm**: displays an NE's top *n* alarms. Alarms are sorted by alarm severity and then are sorted by time, both in descending order.
- **Interface Flow**: displays an NE's interface traffic.

4.15 eSight AppBase Home Page

The eSight AppBase home page displays important monitoring information, and allows you to specify the type of monitoring information displayed.

Figure 4-29 shows the eSight AppBase home page.

Figure 4-29 eSight AppBase home page



Alarms on Top N NEs

NE Name	Critical	Major	Minor	Warning
S7703-15	1	4	0	7
ws6603-5	1	0	1	0
NE40E-X3	1	0	0	0
H3C_S3126TP-SI	1	0	0	0
H3C_S2126-EI	1	0	0	0
REDHAT	0	1	0	0
C7609.online.nl-1	0	0	0	0

Top 10 CPU Usage

Time range:Last hour

Managed Object	Measuring Object	Average Value
S7703-15	Slot:LPU Board 2	68.000%
S7703-15	Slot:LPU Board 3	33.000%
S7703-15	Slot:LPU Board 1	26.000%
HP_UNIX		21.210%
H3C_S3126TP-SI	Slot:module0	16.000%
S7703-15	Slot:MPU Board 4	14.000%
NE40E-X3	Slot:CR52LPUK 1	9.000%
NE40E-X3	Slot:CR52LPUK 2	5.000%
NE40E-X3	Slot:CR52MPUD 4	5.000%
C7609.online.nl-1	CPU:2	4.000%

Top 10 Memory Usage

Time range:Last hour

Managed Object	Measuring Object	Average Value
REDHAT		99.128%
HP_UNIX		52.688%
S7703-15	Slot:MPU Board 4	50.000%
NE40E-X3	Slot:CR52LPUK 1	42.000%
NE40E-X3	Slot:CR52LPUK 2	41.000%

TOP 10 Interface Traffic Statistics

Indicator name：Inbound bandwidth usage on interface   Refresh Interval(minutes)：5

Managed Object	Measuring Object	Current Value
S7703-15	GigabitEthernet2/0/36	96.740%
S7703-15	GigabitEthernet2/0/37	96.740%
H3C_S3126TP-SI	Ethernet1/0/2	0.010%

The eSight AppBase home page provides the following types of monitoring information:

Resource Statistics

- Lower-layer NMS
- Subnet List

Important Information

- Alarms on Top N NEs
- Top 10 CPU Usage
- Top 10 Memory Usage
- TOP 10 Inbound bandwidth usage on interface
- TOP 10 Outbound bandwidth usage on interface

4.16 Data Backup and Restore

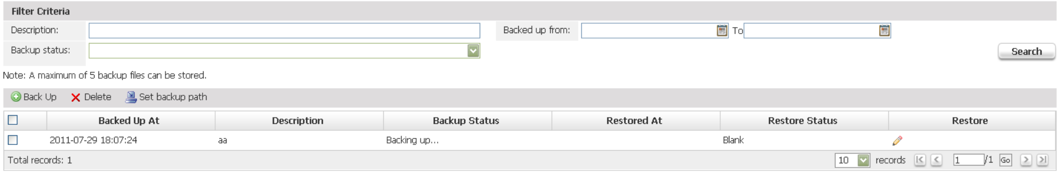
eSight AppBase provides an independent Web service to back up or restore the database.

Database Backup

Users can back up objects and data in the database to the eSight AppBase server and name the generated files by backup time, as shown in **Figure 4-30**.

You can back up objects and data when eSight AppBase is running.

Figure 4-30 Backing up and restoring the database



Filter Criteria

Description:

Backup status:

Backed up from: To

Note: A maximum of 5 backup files can be stored.

□	Backed Up At	Description	Backup Status	Restored At	Restore Status	Restore
□	2011-07-29 18:07:24	aa	Backing up...		Blank	✎

Total records: 1

Backup File Management

When managing backup files, you can:

- Enter the search criteria to search for backup files.
- View the backup time, description, backup status, restore time, and restore status.
- Restore the database.
- Delete backup files.

Database Restore

Before restoring the database, ensure that eSight AppBase has stopped running.

5 Configuration

About This Chapter

This topic describes differences between eSight AppBase versions.

5.1 Software Functions

The three versions of the eSight AppBase provide differentiated network management solutions based on different network scales and function requirements.

Table 5-1 shows differences between eSight AppBase versions.

Table 5-1 Edition description

Edition	Function
Compact	● Provides the Topology Management, Resource Management, Link Management, Equipment resources, Electronic Labels, Fault , Performance, Configuration File Management. ● Supports only the single user mode.
Standard	● Provides the intelligent configuration tool, database backup tool, fault collection tool, and all the functions of the Compact edition. ● Manages user-defined devices, reports, and security. ● Supports WLAN, Internet Protocol Security (IPSec VPN), SNMP alarm northbound interface, and multi-user mode.
Professional	Provides all functions of the standard edition and manages NEs by Lower-Layer NMSs.

5.2 Hardware and Software Configurations

eSight AppBase versions require different hardware and software configurations, different hardware platforms also affect the management capability.

Table 5-2 lists each eSight AppBase version's hardware and software configurations.

Table 5-2 Server configuration requirements

Edition	Managed Nodes	Server Configuration	Recommended Server	Operating System	Database
Compact	60	CPU: dual core 2 GHz or above Memory: 2 GB Hard disk: 40 GB	N/A	Windows 7 (32 bit)	MySQL 5.5 (preinstalled)

Edition	Managed Nodes	Server Configuration	Recommended Server	Operating System	Database
Standard	0~200	CPU: 1 x dual core 2 GHz or above Memory: 4 GB Hard disk: 40 GB **NOTE** Please choose PC Server	IBM X3650M3-1 x Xeon quad core E5506-4 GB (1 x 4 GB)-300 GB	Windows Server 2008 R2 Standard (64 bit)	MySQL 5.5
	200~500	CPU: 2 x dual core 2 GHz or above Memory: 4 GB Hard disk: 60 GB **NOTE** Please choose PC Server			
	500~2000	CPU: 2 x quad core 2 GHz or above Memory: 8 GB Hard disk: 120 GB **NOTE** Please choose PC Server	IBM X3650M3-2 x Xeon quad core E5506-8 GB (2 x 4 GB)-300 GB		
Professional	0~200	CPU: 1 x dual core 2 GHz or above Memory: 4 GB Hard disk: 40 GB **NOTE** Please choose PC Server	IBM X3650M3-1 x Xeon quad core E5506-4 GB (1 x 4 GB)-300 GB	Windows Server 2008 R2 Standard (64 bit) + MySQL 5.5 or SuSE Linux 11 SP1 (64 bit) + Oracle 11g Standard Edition Release 11.1.0.6.0	
	200~500	CPU: 2 x dual core 2 GHz or above Memory: 4 GB Hard disk: 60 GB **NOTE** Please choose PC Server			

Edition	Managed Nodes	Server Configuration	Recommended Server	Operating System	Database
	500~2000	CPU: 2 x quad core 2 GHz or above Memory: 8 GB Hard disk: 120 GB **NOTE** Please choose PC Server	IBM X3650M3-2 x Xeon quad core E5506-8 GB (2 x 4 GB)-300 GB		
	2000~5000	CPU: 4 x dual core 2.5 GHz or above Memory: 16 GB Hard disk: 250 GB	IBM X3650M3-2 x Xeon quad core E5620-16 GB (2 x 8 GB)-300 GB	SuSE Linux 11 SP1 (64 bit)	Oracle 11g Standard Edition Release 11.1.0.6.0

The client configuration requirements are as follows:

- Web browser: Windows Internet Explorer 8 or Firefox 3.6
- Recommended resolution: 1024 x 768 pixels
- Memory: at least 1 GB

6 Technical Indicators

This chapter describes performance indicators of the eSight AppBase.

Table 6-1 lists eSight AppBase technical indicators.

Table 6-1 Performance indicators

Indicator	Counter	Simplified	Standard	Professional
Management capacity	Number of managed NEs	60	2,000	5,000
Resource usage	CPU usage	N/A	CPU Usage, not lasting 15 minutes over 30%	CPU Usage, not lasting 15 minutes over 30%
Storage capacity	Active alarms	20,000 pieces	20,000 pieces	20,000 pieces
	Historical alarms	N/A	1.5 million pieces	1.5 million pieces
	Logs	1 million pieces	1 million pieces	1 million pieces
	Performance data	N/A	60 million pieces	60 million pieces
Processing capability	Alarm processing duration	eSight AppBase displays an alarm within 30 seconds after the alarm is generated on an NE.	eSight AppBase displays an alarm within 30 seconds after the alarm is generated on an NE.	eSight AppBase displays an alarm within 30 seconds after the alarm is generated on an NE.
	Performance data collection speed	N/A	30,000 pieces every 15 minutes	30,000 pieces every 15 minutes
	Page response time	≤ 3 seconds	≤ 3 seconds	≤ 3 seconds

Indicator	Counter	Simplified	Standard	Professional
Status update interval	Device status	N/A	⩽ 300 seconds	⩽ 300 seconds
	Link status	N/A	⩽ 35 seconds	⩽ 35 seconds

NOTE

The formula for calculating storage space occupied by performance events, alarms, and logs is as follows: [(Performance event quantity + Alarm quantity + Log quantity) x 0.5]/(1024 x 1024)

Unit: GB

Calculation rule: One performance event, alarm, or log occupies about 0.5 KB space in the database.

7 Manageable Devices

V200R001C00SPC200 can manage SNMP-compliant devices and matched devices, as shown in **Table 7-1**, **Table 7-2**, **Table 7-3**.

Table 7-1 Huawei device versions

Device	Model
S2300 series	S2309TP-SI
	S2309TP-EI
	S2318TP-SI
	S2318TP-EI
	S2326TP-SI
	S2326TP-EI
	S2352P-EI
	S2309TP-PWR-EI
	S2326TP-PWR-EI
S3300 series	S3328TP-SI
	S3328TP-EI(-24S)
	S3352P-SI
	S3352P-EI(-24S)(-48S)
	S3328TP-PWR-EI
	S3352P-PWR-EI
	S3326C-HI
S5300 series	S5324TP-SI
	S5328C-SI

Device	Model
	S5328C-EI(-24S)
	S5348TP-SI
	S5352C-SI
	S5352C-EI
	S5324TP-PWR-SI
	S5328C-PWR-SI
	S5328C-PWR-EI
	S5348TP-PWR-SI
	S5352C-PWR-SI
	S5352C-PWR-EI
	S5324TP-PWR-S
	S5306TP-LI-AC
	S5328C-HI
	S5328C-HI-24S
	S5306TP-SI
S2700 series	S2700-18TP-EI-AC
	S2700-18TP-SI-AC
	S2700-26TP-EI-AC
	S2700-26TP-PWR-EI
	S2700-26TP-SI-AC
	S2700-52P-EI-AC
	S2700-9TP-EI -AC
	S2700-9TP-PWR-EI
	S2700-9TP-SI-AC
	S2700-9TP-PWR-EI
	S2700-9TP-SI-AC
	S2700-26TP-EI-DC
	S2700-9TP-EI -DC
S3700 series	S3700-28TP-EI-24S-AC
	S3700-28TP-EI-AC

Device	Model
	S3700-28TP-EI-MC-AC
	S3700-28TP-PWR-EI
	S3700-28TP-SI-AC
	S3700-52P-EI-24S-AC
	S3700-52P-EI-48S-AC
	S3700-52P-EI-AC
	S3700-52P-PWR-EI
	S3700-52P-SI-AC
	S3700-28TP-EI-DC
	S3700-28TP-SI-DC
	S3700-52P-EI-24S-DC
S5700	S5700-24TP-PWR-SI
	S5700-24TP-SI-AC
	S5700-28C-EI
	S5700-28C-EI-24S
	S5700-28C-SI
	S5700-48TP-PWR-SI
	S5700-48TP-SI-AC
	S5700-52C-EI
	S5700-52C-PWR-EI
	S5700-52C-SI
	S5700-24TP-SI-DC
S6300 series	S6348-EI
	S6324-EI
S6700 series	S6700-48-EI
	S6700-24-EI
S9300 series	S9300-3
	S9300-6
	S9300-12
S7700 series	S7700-3

Device	Model
	S7700-6
	S7700-12
WS6600 series	WS6603
NE40E&NE80E series	NE40E
	NE40E-4
	NE40E-X3
	NE80E
NE40&NE40 series	NE40
	NE80
NE20E&NE20 series	NE20E-8
	NE20-2/4/8
	NE20E-X6
AR series	AR 1220
	AR 1220V
	AR 1220W
	AR 1220VW
	AR 2220
	AR 2240
	AR 3260
Eudemon series	Eudemon 8000E series
	Eudemon 1000E series
	E200E series
SIG series	SIG series
SVN series	SVN series

Table 7-2 Non-Huawei device versions

Manufacturer	Device
H3C	S9500E series
	S12500 series

Manufacturer	Device
	S5800 series
	S5500 series
	S5510 series
	S3610 series
	S5100 series
	S3600 series
	MSR20 series
	MSR30 series
	MSR50 series
	SR66 series
	SR88 series
Cisco	Cisco Catalyst 6500 Series Switches
	Cisco Catalyst 4500 Series Switches
	Cisco Catalyst 3750 Series Switches
	Cisco Catalyst 3560 Series Switches
	Cisco Catalyst 2960 Series Switches
	Cisco Catalyst 4900 Series Switches
	Cisco ME 3400 Series Ethernet Access Switches
	Cisco Catalyst 3750 Metro Series Switches
	Cisco ME 6500 Series Ethernet Switches
	Cisco 7000 Series
	Cisco Catalyst 5000 Series Switches
	Cisco 2000 Series Routers
	Cisco ASR 1000 Series Aggregation Services Routers
	Cisco 7600 Series Routers
	ISR 1861
	Cisco 2800 Series Integrated Services Routers
	Cisco 1800 Series Integrated Services Routers
	Cisco 3800 Series Integrated Services Routers

Manufacturer	Device
	Cisco 2800 Series Integrated Services Routers
	Data Center Switches

Table 7-3 IT device versions

Device	Model
Printer	HP Printer
	HP Network Plotter
	HP ETHERNET JETDIRECT
	Kyocera Printer
	Lexmark Printer
	Emulex Printer
	SunOS-HP Agent
	Sun Solaris
	Red Hat Linux
	MP 3640B
	Red Hat Linux
	American Power Conversion UPS
	Emerson UPS
	HP-UX
	HP-UX
Server	Microsoft Windows Workstation
	Microsoft Windows Server
	Microsoft Windows Domain Controller