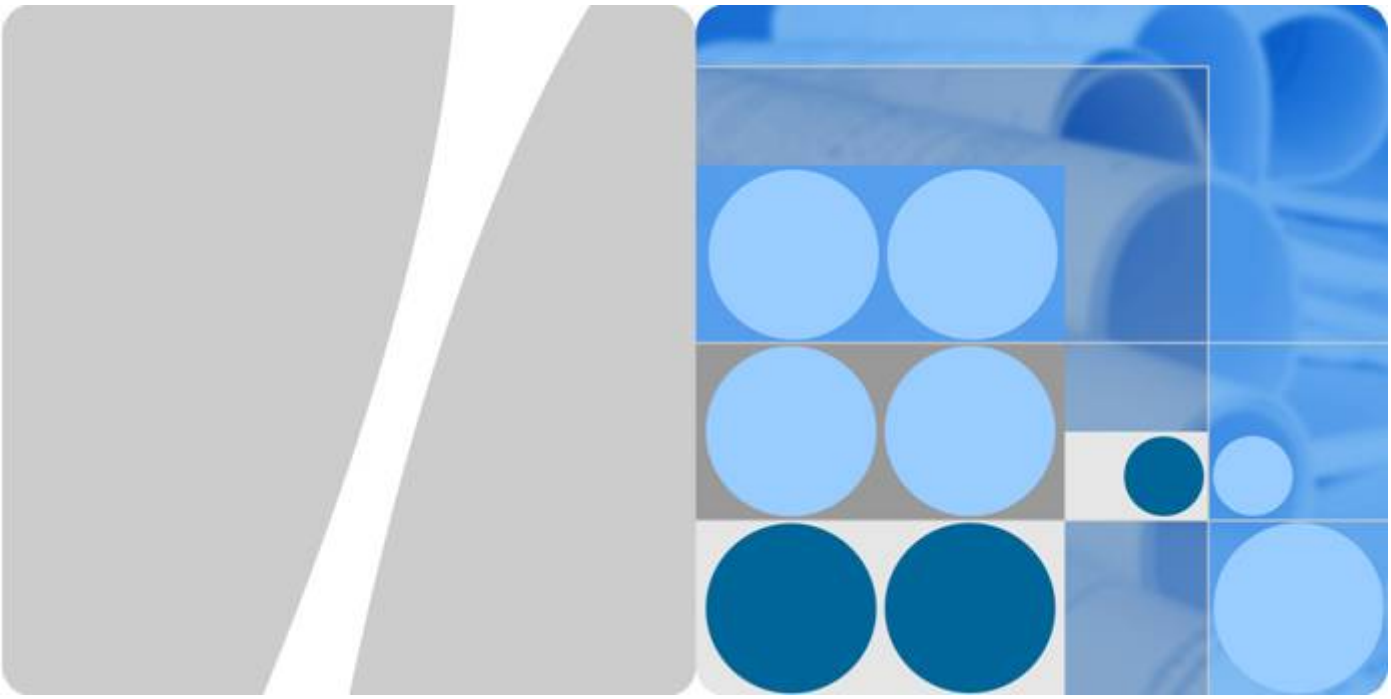


eSight

V300R001C10

Product Description

Issue 02

Date 2014-01-28

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


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

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://enterprise.huawei.com

About This Document

Purpose

This document describes the product positioning, architecture, functions, and applications of eSight ICT Unified Management System (eSight for short) and provides configuration requirements and technical counters for eSight.

This document helps you understand eSight functions and basic operations in eSight.

Intended Audience

This document is intended for:

- Huawei pre-sales engineers
- Huawei technical support engineers
- Partner pre-sales engineers
- Partner technical support engineers
- Enterprise pre-sales engineers
- Enterprise administrators

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Indicates an imminently hazardous situation which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a potentially hazardous situation which, if not avoided, could result in death or serious injury.
 CAUTION	Indicates a potentially hazardous situation which, if not avoided, may result in minor or moderate injury.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

Change History

Changes between document issues are cumulative.The latest document issue contains all the changes made in earlier issues.

Issue 02 (2014-01-28)

This issue is the second official release, which incorporates the following changes:

Chapter 1 Product Positioning and Features

Added the description about the eSight Compact (server), eSight Server Device Manager, eSight MicroDC Device Manager, eSight LogCenter Log Manager, eSight Server Stateless Computing Manager and eSight Server Deployment Manager.

Chapter 2 Product Architecture

Added the description about the HTTPS interface.

Chapter 3 Product and Application Scenarios

Added the LogCenter log collector in the distributed deployment network diagram.

Added the eSight server management networking in the section "eSight and NE Networking."

Chapter 4 Functions and Features

Added the description about the eSight Server Device Manager, eSight MicroDC Device Manager, eSight LogCenter Log Manager, eSight Server Stateless Computing Manager and eSight Server Deployment Manager.

Updated the security policy management.

Chapter 5 Configuration

Added configuration requirements on the eSight Server Device Manager, eSight MicroDC Device Manager, eSight LogCenter Log Manager, eSight Server Stateless Computing Manager and eSight Server Deployment Manager.

Added the bandwidth calculation method.

Issue 01 (2013-12-10)

This issue is the first official release.

Contents

1 Product Positioning and Features

1.1 Positioning

The eSight system is a new-generation comprehensive operation and maintenance solution developed by Huawei for the network infrastructure, unified communications, telepresence conferencing, video surveillance, and data center in enterprises. eSight supports unified monitoring and configuration management over devices of various types and from various vendors, monitors and analyzes network and service quality, and delivers unified management over and association analysis among enterprise resources, services, and users. Meanwhile, eSight offers a flexible and open platform for enterprises to customize software development and build an intelligent management system tailored to individual needs.

1.2 Features

The eSight provides a lightweight and web-based client and mutually independent subsystems. It can work across various operating systems. The eSight manages a maximum of 20000 NEs and supports a maximum of 100 online clients.

Comprehensive Device Management Capabilities

eSight can manage devices from multiple manufacturers, including network devices from Huawei, H3C, Cisco, and ZTE, and IT devices from IBM, HP, and Sun. It also allows you to customize device types for management. Customized device types can be managed in the same way as preconfigured device types.

- eSight manages non-Huawei devices that support standard management information base (MIB) (RFC1213-MIB, Entity-MIB, SNMPv2-MIB, and IF-MIB) through user-defined settings.
- eSight manages non-Huawei devices that do not support MIB through network element (NE) adaptation packages.

Multiple Editions Catering for Differentiated Needs

To serve enterprise customers with different needs, eSight System is classified into Compact, Standard, and Professional editions, as described in the following table.

Edition	Function
eSight Compact (network device)	● Offers the following functions for network devices: alarm management, performance management, topology management, configuration file management, network element (NE) management, link management, log management, physical resources, electronic label, IP topology, smart configuration tool, custom device management, security management, terminal access management, MIB management and VLAN management. ● System monitoring tool, database backup/restoration tool.
eSight Compact (server)	● Offers the following functions for servers: alarm management, performance management, topology management, NE management, device configuration, smart information management for hard disks, log management and security management,. ● System monitoring tool, database backup/restoration tool. ● Server stateless computing management, server deployment management.
eSight Standard	In addition to the functions in the eSight Compact (network device), the eSight Standard edition also offers the following functions: ● Device management (UC, telepresence, video surveillance, storage, server, host, FusionAccess, FusionCompute, MicroDC, and eLTE terminal). ● Service management: OpenSDK management, smart report, storage report, WLAN management, MPLS VPN management, MPLS VPN tunnel management, SLA management, network traffic analyzer (NTA), security policy management (Secure Center), log management (LogCenter), IPSec VPN management, server stateless computing management, server deployment management and infrastructure management.
eSight Professional	In addition to the functions in the eSight Standard edition, the eSight Professional edition also offers the following functions: ● Hierarchical network management. ● Data center management (nCenter). ● The Linux two-node cluster system supports two-node cluster hot standby.

Multiple Service Management Components

eSight allows users to construct custom management systems based on the component-based design. The following table lists components supported by eSight.

Type	Conmponent	Description
Management platform	eSight Platform	Offers basic network management functions, such as resource, topology, fault, and performance management.
Device management components	eSight Network Device Manager	Offers basic management and configuration over network devices, including network device discovery and maintenance, route configuration, interface management, Layer-2 link management, IP topology, and device accessories.
	eSight Server Device Manager	Manages and monitors Huawei servers in a unified manner by offering an impressive array of functions, including centralized fault monitoring, performance analysis and report, keyboard, video, and mouse (KVM), and integrated virtual media management.
	eSight Storage Device Manager	Offers unified management over storage devices of different types and from different vendors, including storage device discovery, maintenance, and query.
	eSight MicroDC Device Manager	Offers unified management over Huawei micro data centers, including L1 device monitoring and visualized device view management.
	eSight UC/CC Device Manager	Offers convenient and quick UC device configuration, wizard-based service installation and configuration, one-stop service rollout, end-to-end visual network surveillance, and intuitive display of fault information, helping users quickly locate and rectify problems.
	eSight Video Surveillance Device Manager	Offers end-to-end management over video surveillance devices, including resource discovery, topology, performance, and data analysis, which effectively improves video surveillance device management quality and efficiency. Users can view the performance and alarm data about surveillance devices to learn about the device running status and quickly locate faults.

Type	Conmponent	Description
	eSight Telepresence Device Manager	Offers end-to-end management over telepresence conference devices, including resource discovery, topology, and performance, which effectively improves telepresence conference device management quality and efficiency. Users can view the performance and alarm data about surveillance devices to learn about the device running status and quickly locate faults.
	eSight eLTE Device Manager	Manages Huawei's enterprise Long Term Evolution (eLTE) devices, including plug and play (PnP), device firmware upgrade, device configuration management, and remote device maintenance.
Service management components	eSight Open SDK	Provides SNMP and HTTP interfaces to be integrated by third-party systems.
	eSight Smart Reporter	Pre-integrates rich report templates, meets network O&M report requirements, and allows users to customize report templates.
	eSight Storage Reporter	Offers storage capacity and performance analysis reports, which helps users to analyze the performance bottleneck, implement balancing policies, and expand storage capacity.
	eSight WLAN Manager	Manages wireless network resources (AC/AP), diagnoses wireless network faults, and displays wired and wireless devices in the topology.
	eSight MPLS VPN Manager	Automatically discovers MPLS VPN services, presents the logical architecture of the VPN network, and monitors and collects statistical information about the VPN service status and quality.
	eSight MPLS Tunnel Manager	Automatically discovers deployed MPLS TE and LDP tunnels, dynamically presents the network channel status change, and enables visual route management.
	eSight Network SLA Manager	Automatically performs periodical and temporary diagnosis over network lines, which helps users to assess network service quality.
	eSight DC nCenter	Manages data center networks in a unified manner, particularly the access network of the virtualized data center.

Type	Conmponent	Description
	eSight Network Traffic Analyzer Manager	Analyzes network traffic packets based on the packet source, destination, protocol, and application, which helps users to understand network traffic distribution.
	eSight IPSec VPN Manager	Manages IPSec VPN services on the GUI as follows: discovers IPSec VPN services, displays IPSec VPN services in the topology, and supports VPN tunnel information query.
	eSight Secure Center	Centrally manages policies for Huawei network security devices, including firewall, intrusion prevention system (IPS), and antivirus policies.
	eSight LogCenter Log Manager	Offers log collection, analysis, and management functions.
	eSight Server Stateless Computing Manager	Virtualizes server hardware to configure and manage stateless Huawei servers through configuration files.
	eSight Server Deployment Manager	Configures Huawei servers in batches, including BIOS configuration, network configuration, RAID card configuration, and operating system deployment.
	eSight Infrastructure Manager	Manages basic facilities in an equipment room, including power supply, cooling, access control, physical security, environment, firefighting, and lighting devices, as well as cabinets and collectors. Offers enhanced energy, temperature, and capacity management.

Supporting Various Operating Systems

Based on Huawei's unified browser/server (B/S) application platform Intelligent Enterprise Management Platform (iEMP), eSight can be installed on the Windows and SUSE Linux operating systems and supports Oracle, MySQL, SQL Server and GaussDB databases.

Lightweight and Web-Based Client

The eSight is web-based, with its client software running on the web browser. During system upgrade and maintenance, you need only to update the server software. This feature greatly reduces the load on clients and simplifies operations.

System Reliability

The eSight supports automatic restart when a process exception occurs.

The maintenance tool can monitor eSight processes. When the maintenance tool detects that these processes are unexpectedly terminated, the maintenance tool automatically restarts the eSight processes, which keeps the system running properly in unattended mode and reduces the fault recovery time.

The eSight supports automatic and manual data backup and restore. The eSight can automatically back up data in a preset backup period. Alternatively, users can manually back up data any time. Users can save the backup data to an external device. The restore mechanism allows users to restore the system using the latest backup data if the system breaks down or an upgrade fails.

Security

The eSight provides security mechanisms in terms of system, network, data, and operation and maintenance.

- System security

  The system security mechanism ensures that the operating system, database, and middleware are running properly to support normal application operation.

  - Patch policies
  - Security hardening policies
  - Password policies
  - Authentication and authorization
  - Data encryption
  - Security logs
  - Minimum permission rule
  - File property management
- Network security

  The network security mechanism ensures that the switches, routers, and firewalls are running properly.

  The security policies are as follows:

  - Routers are deployed to separate local area networks from external networks, enhancing data communication security.
  - A network firewall is configured for the eSight, ensuring network security.
  - Rights accessible to external systems are controlled and managed.
- Data security

  The data security mechanism ensures storage, transmission, and management security of user information, system configuration information, run operations, and database data.

  - Encryption policies define encrypted storage and transmission of sensitive data.
  - User management policies specify minimum authorization.
  - Backup and restore policies ensure important data backup.
  - Data storage security supports switchover of the HA system to recover system running in a timely manner.
- Operation and maintenance security

  The operation and maintenance security mechanism provides security for users, applications, and audits.

- Access mechanism by group and permission

  An operator can log in to the system only after entering the correct user name and password, and perform operations within the user permissions. Centralized user management and authentication ensure that users are managed by group and permission. A trust mechanism is provided to control information and resource sharing, preventing unauthorized users from accessing the system.

- Access control policies

  Access control policies include password policies, login lock and unlock, and authentication policies.

- Log audit

  Logs consist of security logs, operation logs, and system logs.

- Automatic client logout mechanism

  If an operator does not perform any operation for a period of time, the client is automatically locked, preventing unauthorized operations.

- Application security mechanism

  The eSight provides password and identity authentication. The system encrypts and stores sensitive user information using a strong data encryption algorithm. The system assigns a password to each user, and verifies the user password when providing services. This ensures user information security.

Scalable Architecture

The eSight provides a scalable architecture to expand the management capacity by adding servers. This architecture allows old hardware to be used to expand a live network, which ensures smooth expansion with the existing investment.

Integration Capability

The eSight is based on open buses, open interfaces, and information modeling. It supports heterogeneous system integration and can be quickly interconnected with a third-party system.

2 Product Architecture

2.1 Web-Based Architecture

The B/S architecture allows you to access eSight anywhere and anytime using a standard web browser. Only the server software needs to be updated during system upgrade or maintenance, reducing the costs and workload involved in system maintenance and upgrades, and therefore lowering customers' total cost of operation (TCO).

The B/S architecture also has the following advantages:

- With the distributed feature, you can perform operations like querying and browsing anywhere anytime.
- When a new service is released, you only need to update the server.

2.2 Component-based Architecture

Depending on the component-based design, eSight offers a diversity of components for users to choose.

2.3 Independent NE Adaptation Capability

eSight provides an extension point mechanism, which allows incremental development of functions and NE version adaptation packages. New functions and NE adaptation packages can be added without changing code in earlier release packages. The modular Open Services Gateway initiative (OSGi)-based framework enables service components to be upgraded and patched independently.

To add new functions, develop new function plug-in packages and deploy them in eSight. To manage new devices, simply add new NE adaptation packages. Function plug-in packages and NE adaptation packages are deployed in the eSight OSGi container as bundles (plug-ins).

2.4 Northbound Interfaces

eSight northbound interfaces are used to integrate the eSight with different OSSs.

2.5 Southbound Interfaces

eSight southbound interfaces are used to interconnect the eSight and devices for the eSight to manage the devices.

eSight supports the SNMP, Telnet/sTelnet, FTP/SFTP/FTPS, TR069, Huawei MML, SMI-S, Modbus southbound and HTTPS interfaces.

SNMP interfaces

The eSight supports SNMPv1, SNMPv2c, and SNMPv3 interfaces, through which the eSight interconnects with NEs. The SNMP interfaces help achieve basic management functions such as automatic NE discovery, service configuration data synchronization, fault management, and performance management. SNMP is a TCP/IP-based network management protocol at the application layer. Its transport protocol is UDP and it manages the NEs that support proxy processes.

Telnet/STelnet interfaces

Telnet and Secure Shell Telnet (STelnet) interfaces are basic NE management interfaces used for remote NE login and management. The Telnet and STelnet interfaces, as supplementation of the SNMP interfaces, also provide extra management functions. The eSight interconnects with NEs through the Telnet/STelnet interfaces.

- The Telnet interface is used to log in to an NE from the CLI on the eSight intelligent configuration tool or NMS and to maintain and configure the NE in CLI mode. Telnet is a TCP/IP-based network management protocol at the application layer. Its transport protocol is TCP and it provides services for network communication.

  NOTE

  The Telnet protocol transfers communication data in plaintext, which is risky. You are advised to use it together with other secure protocols such as SSH.

- Secure Shell (SSH) is a protocol similar to Telnet. With SSH adopted, data is transmitted in ciphertext mode. SSH ensures network security by means of authentication and encryption. Authentication can be performed using passwords or the Revist-Shamir-Adleman Algorithm (RSA). The data has been compressed before being transmitted, which improves the transmission speed. SSH is a TCP/IP-based network management protocol at the application layer. Its transport protocol is TCP and it encrypts data at the application layer.

TFTP/FTP/SFTP/FTPS interfaces

FTP, SFTP, and FTPS interfaces are used to back up NE data. FTP, SFTP, and FTPS are TCP/IP-based network management protocols at the application layer.

- The File Transfer Protocol (FTP) is used for file transmission.

  NOTE

  FTP is an insecure protocol. SFTP and FTPS are recommended because they are secure.

- SSH FTP (SFTP) provides secure file transmission and processing over SSH. With SFTP adopted, commands and data are transmitted in ciphertext mode.
- FTP over SSL (FTPS) provides data encryption and decryption during secure data transmission between a client and an SSL-based server.
- The Trivial File Transfer Protocol (TFTP) is a TCP/IP family member that provides simple and inexpensive file transfer services between clients and servers.

TR-069 Interface

Technical Report 069 (TR-069) is a Digital Subscriber Line (DSL) Forum (which was later renamed as Broadband Forum) technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end user devices.

This interface is used to connect to terminals such as IP phones, EGWs, ATs, SBCs and eLTE terminal.

MML Interface

In Huawei, the Man-Machine Language (MML) interface is mainly used for:

- Daily operation and maintenance. Compared with the graphical user interface (GUI), the MML interface is easy to use and supports scripts.
- Connecting to an upper-level operation support system (OSS). Compared with internal binary protocols, the MML protocol is more transparent and standard, and it can be easily analyzed by the upper-level OSS.

SMI-S Interface

The eSight supports storage device access and management through standard SMI-S interface, providing resource monitoring, performance analysis, and fault monitoring of storage devices.

Storage Management Initiative Specification (SMI-S) is formulated by the Storage Network Industry Association (SNIA). SMI-S functions like a middleware and defines the interaction mechanism between storage management software and management objects. It provides multiple functions to simplify SAN management. SMI-S manages storage networks based on the CIM/WBEM, a universal model for resource management. WBEM is a tool based on management technologies. WBEM uses CIM as its data format, XML for data encoding and transmission, and HTTP as interface.

Modbus Interface

The Modbus protocol is a universal language used on electronic controllers. This protocol allows controllers to communicate with other controllers and devices through networks (such as Ethernet). Modbus has become a universal industrial standard. It allows controllers from different vendors to form industrial networks and support centralized monitoring.

Modbus supports RS-232, RS-422, RS-485, and Ethernet devices. A broad range of industrial devices, including the PLC, DCS, and smart meter, use Modbus as the communication protocol.

HTTPS Interface

eSight obtains host, server CPU, memory, network port rate, and disk usage information through the HTTPS protocol, to support host and server management.

3 Product and Application Scenarios

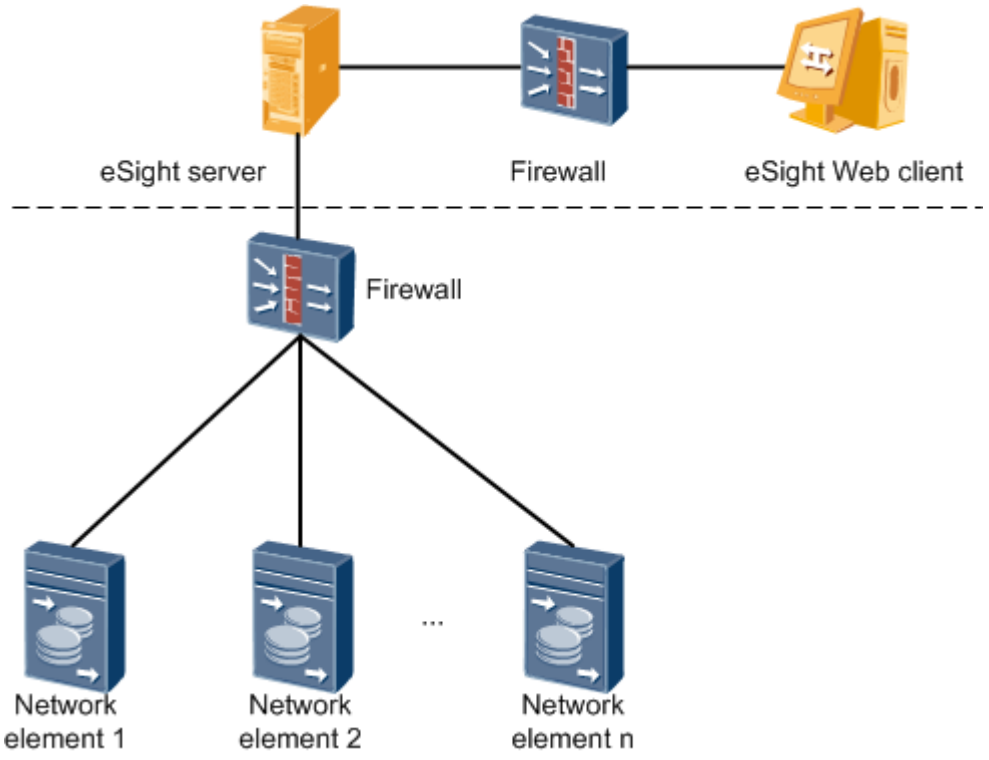
3.1 eSight Networking Mode

eSight supports two networking modes: standalone deployment, and hierarchical deployment.

3.1.1 Standalone Mode

This deployment mode applies to small-scale network management scenarios. In this deployment mode, the entire eSight system consists of one server, multiple clients, and related network devices.

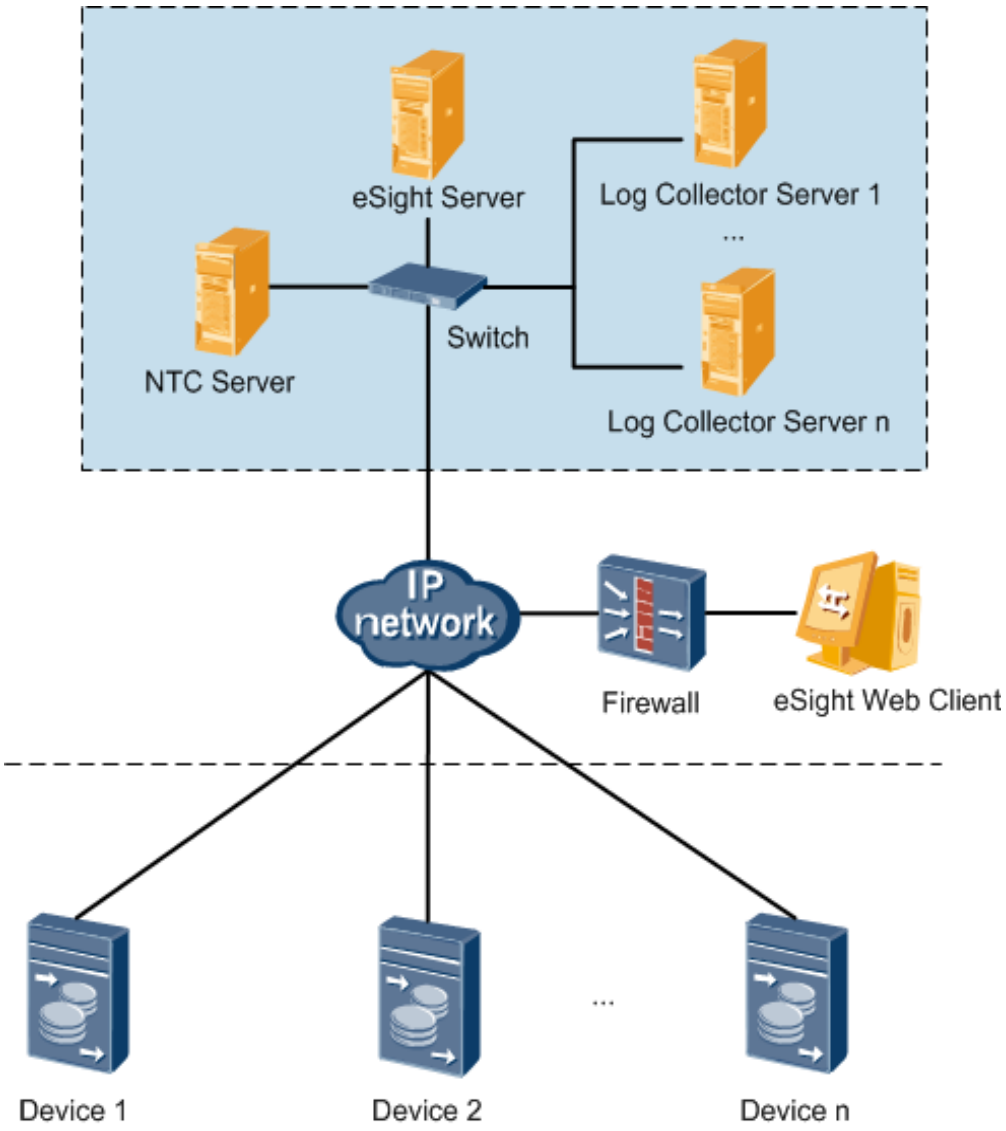
Figure 3-1 Standalone mode



3.1.2 Distributed Deployment Mode

This deployment mode applies to large-scale network management scenarios. The eSight server and the network traffic collector (NTC) or LogCenter log collector are deployed on different hosts, as shown in **Figure 3-2**.

Figure 3-2 Distributed deployment mode



NOTE

During eSight distributed deployment:

- Only one NTC can be deployed.
- Multiple log collectors can be deployed. The number of log collectors is determined by the device quantity, security gateway quantity, total campus egress bandwidth, and log storage time.

3.1.3 Two-Node Cluster Deployment Mode

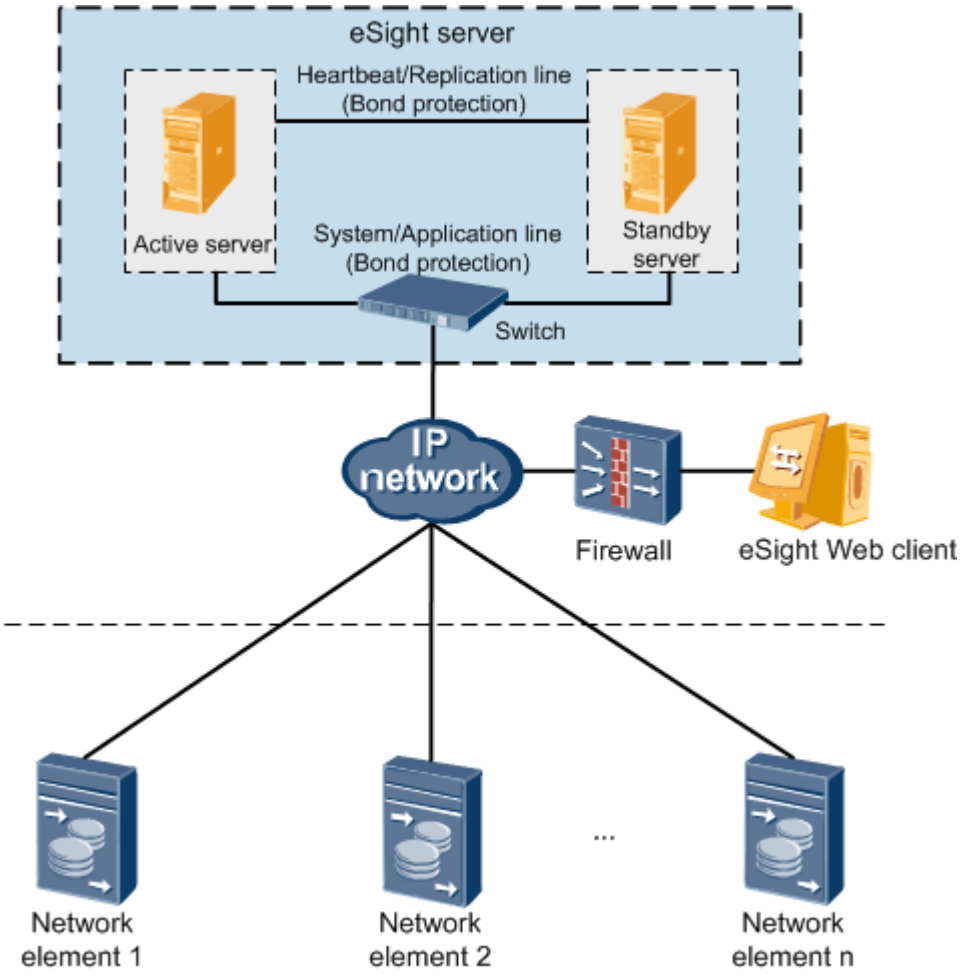
An eSight two-node cluster can be a local two-node cluster (where two servers are deployed at the same site) or a remote two-node cluster (where two servers are deployed at two different sites).

Local Two-Node Cluster

In this deployment mode, the eSight software is installed on both the active and standby servers. Data between active and standby servers is synchronized through a dedicated duplication line. When the active server fails, services are automatically switched to the standby server to ensure normal running of the entire system.

You can set a floating IP address between the active and standby servers. In this case, devices do not need to reconnect to eSight after active and standby switchover.

Figure 3-3 Local two-node cluster networking



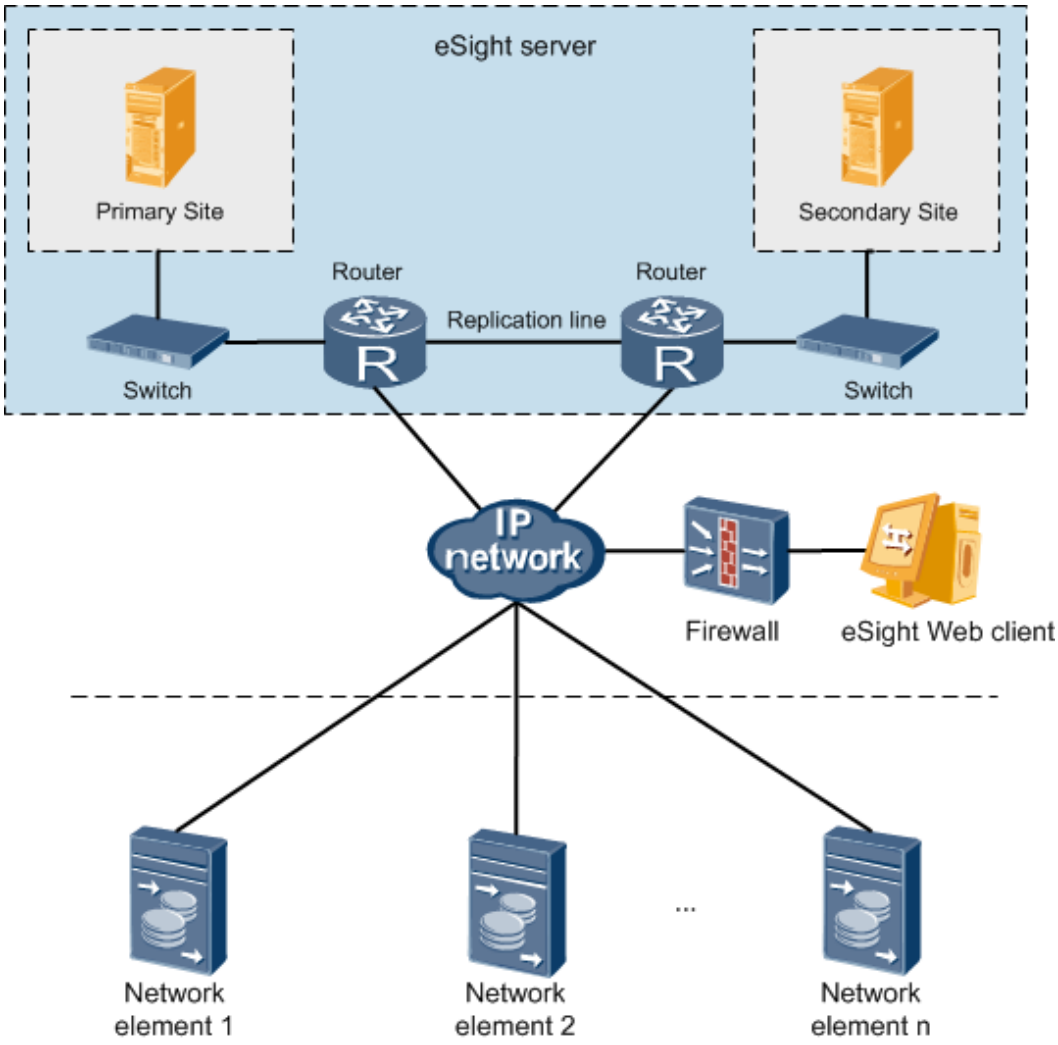
Remote Two-Node Cluster

In this deployment mode, the eSight software is installed on both the active and standby servers. The two servers can be deployed in geographically-dispersed places. In case of a fault on the active server, services are automatically switched to the standby server. Data between active and

standby servers is synchronized through a dedicated duplication line, which ensures normal running of the eSight system.

Because the two eSight servers use different IP addresses, you must set the IP addresses of the active and standby servers on managed devices. In this case, information, such as alarms, on the devices can be automatically sent to the standby server after active and standby switchover, which ensures normal device monitoring and management.

Figure 3-4 Remote two-node cluster networking



3.2 eSight and NE Networking

eSight has a scalable architecture with a modular design, enabling it to dynamically manage all devices on a data network.

Table 3-1 lists Huawei and non-Huawei devices that can be managed by eSight.

Table 3-1 Devices that can be managed by eSight

Domain	Device
Switches	S series and CE series switches
Routers	● NE series routers ● AR series routers
Security devices	● Eudemon series ● SRG series ● SVN series
Unified communications devices	eSpace series gateways, UC purchased devices, eSpace UC applications, and eSpace CC applications
Video surveillance devices	Huawei eSpace IVS V100R100C02 series video surveillance applications
Telepresence devices	Huawei telepresence conference terminals, multi-point control units (MCUs), TP, and gatekeepers (GKs).
Storage device	Huawei array, unified storage, virtual intelligent storage, mass storage, cloud storage, virtual tape library, third-party storage and Fibre Channel switch.
Server	Huawei rack server, blade server, and high-density server. Mainstream operating systems, including Windows, Redhat, and SUSE.
Virtual device	Huawei FusionCompute and FusionAccess
MicroDC device	Environment monitoring units (ECC and CCU), MicroDC camera
eLTE device	Huawei eA660 and eA661 CPEs
Infrastructure	Manages basic facilities in an equipment room, including power supply, cooling, access control, physical security, environment, firefighting, and lighting devices.
Non-Huawei devices	● Pre-integrated non-Huawei devices: H3C devices and Cisco devices ● Printers and servers

NOTE

For details about mapping relationships between eSight and devices, see **Device Versions** in the release notes delivered with the version.

In an enterprise park, employees working in branches and partners outside the core network need to connect to the enterprise park network through a wide area network (WAN) or the Internet.

The eSight intelligent management platform provides integrated management for multiple systems and unified management for IT and IP devices. Figure 3-6 shows a typical network for eSight solution in an enterprise park.

Figure 3-5 Network for eSight solution in an enterprise park

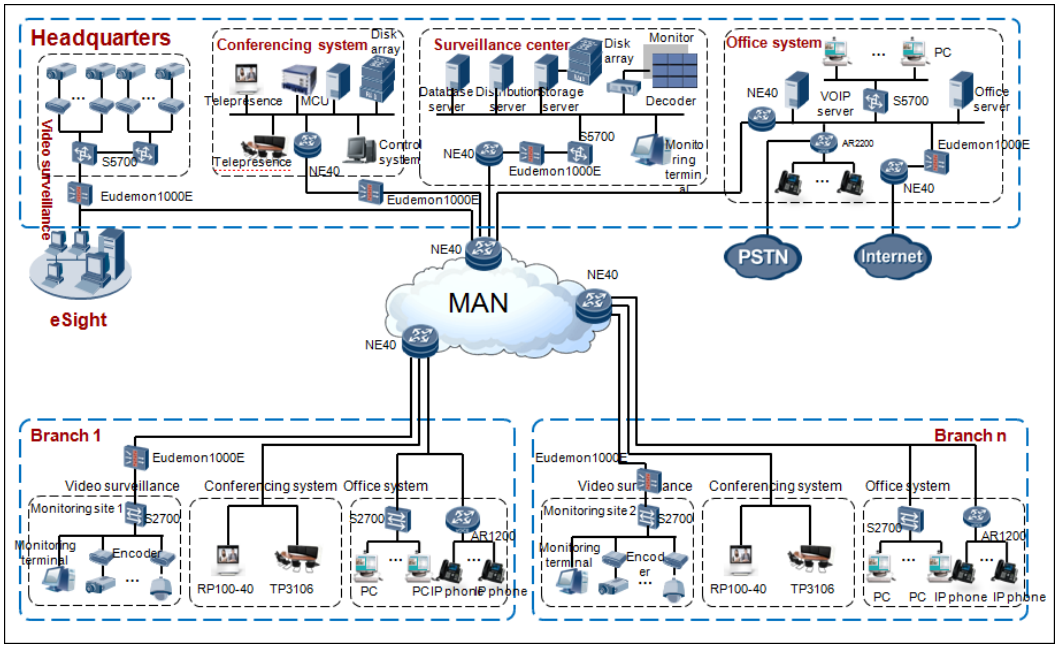
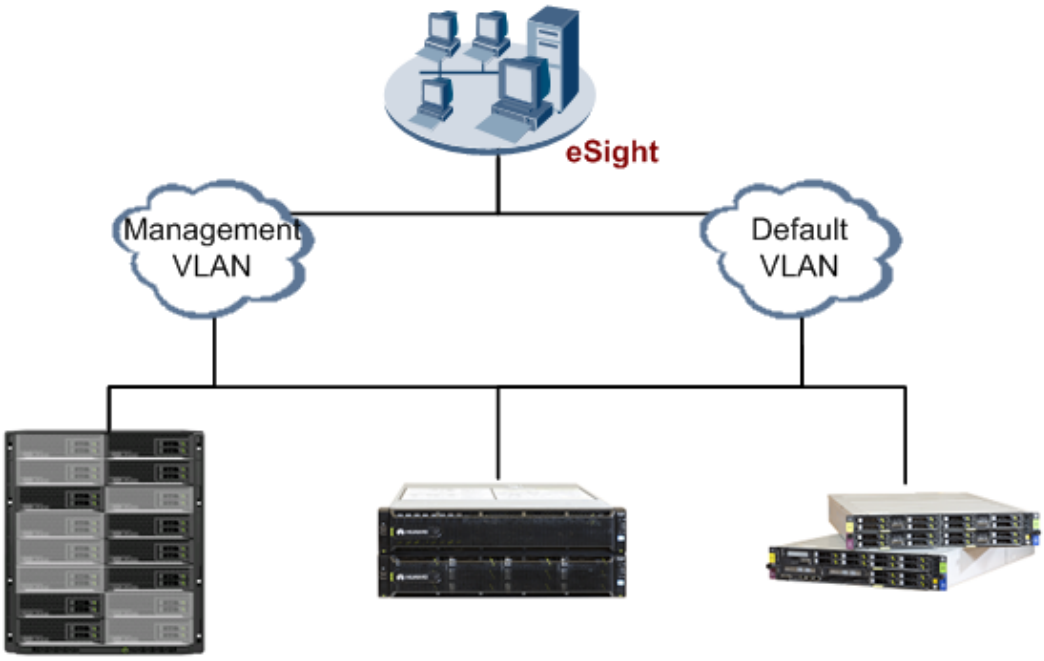


Figure 3-6 eSight server management networking



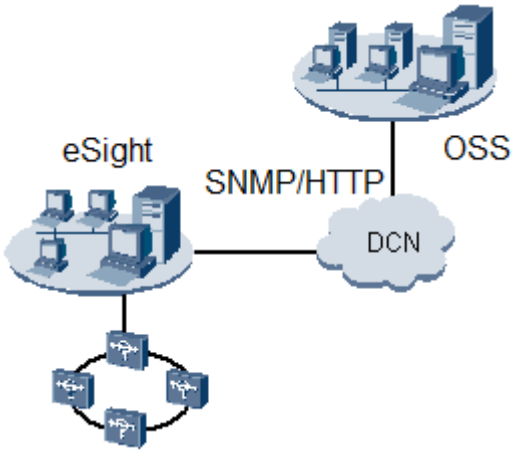
When eSight offers server management, it is recommended that the eSight server must offer at least two network ports for server management and that one management VLAN is planned for device management. One network port is used for basic device management and connected to

the management VLAN. The other network port is used for server deployment and connected to the default VLAN.

3.3 eSight and OSS Integration

eSight supports third-party systems including upper-level OSSs. Third-party systems can obtain network resources and alarms from the eSight system through the SNMP or HTTP interface.

Figure 3-7 Network between eSight and an OSS

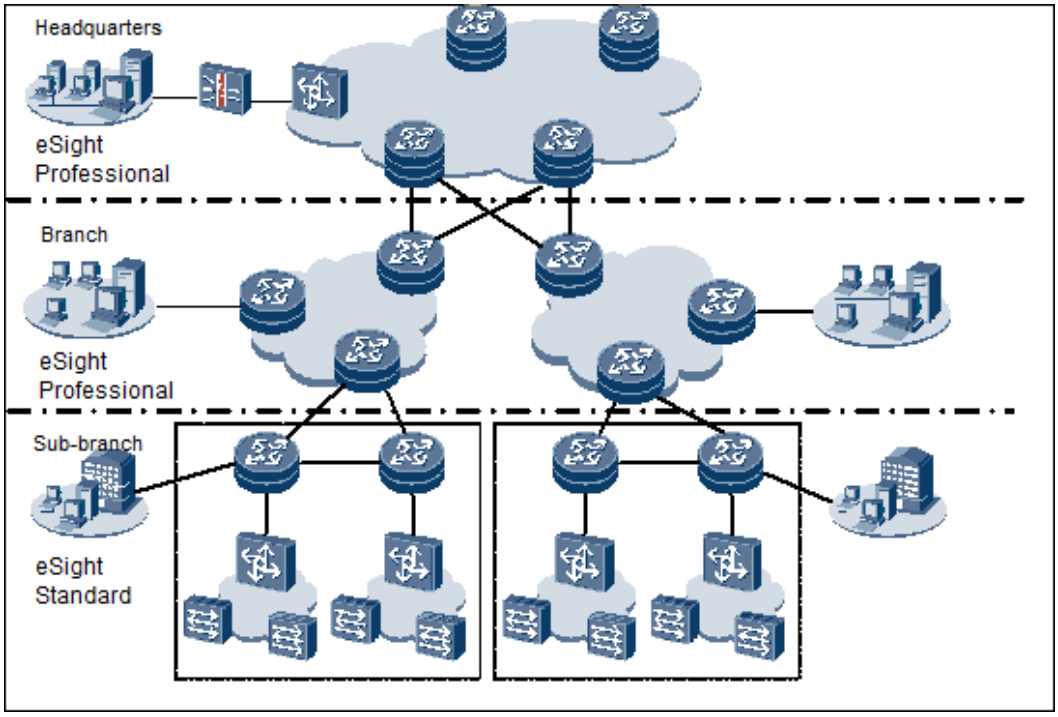


3.4 Hierarchical Deployment Mode

eSight supports hierarchical management, which enables an enterprise headquarters to manage networks in different physical locations.

You can add lower-level eSights to the upper-level eSight and provide links to lower-level eSights. When you click a link, a new browser window opens, displaying the login page of a lower-level eSight.

Figure 3-8 Hierarchical deployment mode



4 Functions and Features

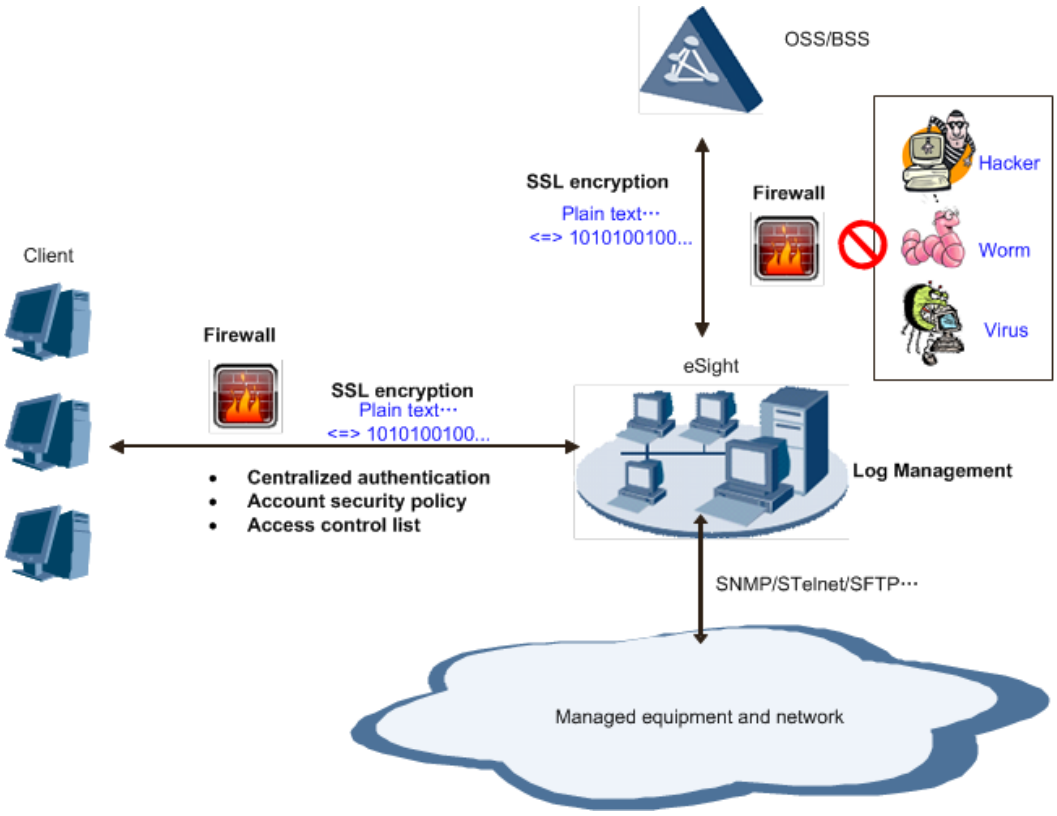
4.1 eSight Platform

4.1.1 Security Management

Security management controls the security of itself. Security management includes user management, role management (authorization management, that is, rights- and domain-based management), user login management, and a series of other security policies. These functions together safeguard the . The security solution of the is further improved by log management (recording user login, operation, and system logs) and database backup.

Figure 4-1 shows the implementation mechanism of eSight security management.

Figure 4-1 Security management overview



NOTE

This section focuses on eSight user security.

- For details about log management, see section **4.1.2 Log Management**.
- For details about database backup and restore, see section **4.1.7 Maintenance Tool**.

User Management

To successfully log in to an eSight client and perform maintenance and management operations, users must obtain a correct user name and password. A user name and password are used together to uniquely define the login and operation rights of a user.

User passwords are stored in the database and encrypted using SHA256, an irreversible encryption algorithm. A newly installed eSight provides only one default user **admin** who has all operation and management rights. Other users are directly or indirectly created by the **admin** user.

User attributes include the user name, password, roles, description, and access control. Users in different roles have different operation and management rights. Access control limits the time and IP addresses available for users to log in to the eSight, which ensures eSight access security.

The eSight has the following user management functions:

- Creating users one by one or in batches
- Deleting users
- Querying and modifying user attributes

- Changing user passwords, including:
  - Resetting a password

    If a user forgets the password when logging in to the eSight client, the user can contact the administrator with the security management permission to reset the password. In this way, the user can log in to the eSight client again using the new password.

    NOTE

    The password for the **admin** user cannot be reset.
  - Changing the password for the current user

    A logged-in user can change its own password on the eSight client. To keep user information secure, it is recommended to change user passwords regularly.
- Enabling and disabling users

  A user account is automatically disabled if it is unused within the period specified in the account policy. The user account can also be manually disabled if it is not needed.

  A disabled user account can be enabled if needed.

Role Management (Rights- and Domain-based Management)

Each role is a set of rights. If a user needs certain rights, the corresponding role must be granted to it. Role management makes user rights management easier. After an eSight user is planned, a role needs to be granted to it so that the new user has sufficient rights to manage devices.

Roles can be created, modified, and deleted on the eSight. Their attributes can be queried.

The eSight provides one default role **Administrators** who has operation rights for all managed objects (MOs) and cannot be modified.

Role attributes include the role name, user, MO, operation, and description.

- MO: This attribute specifies the objects and range of configuration data that can be managed by a role. If role A cannot manage device C or object group D, the topology view hides device C and devices in object group D from users in role A.

  An object group is a group of devices. Object groups can be created, modified, and deleted on the eSight.
- Operation: This attribute specifies the operations that can be performed by a role. Operation rights for a device may be assigned to different roles. Therefore, different roles have different operation rights for the same device.

The eSight achieves rights- and domain-based management by providing the MO and operation attributes:

- Domain-based management is the operation of assigning different MOs to different roles. This function allows engineers from different O&M departments to manage different network objects.
- Rights-based management is the operation of assigning different operations to different roles.

  Rights-based management and domain-based management together allow engineers with different duties (at different positions or from different O&M departments) to perform different operations on MOs in the same area. Users can perform operations only on the NEs they have rights for.

NOTE

Users in the **Administrators** role or with the user management rights can assign MOs and operations to other users.

Rights- and domain-based management unifies device and function management. Specifically, MOs are assigned based on devices; operation rights are assigned based on functions on devices.

User Authentication

The eSight uses three modes to authenticate users: local authentication, **Remote Authentication Dial In User Service** (RADIUS) authentication, and **Lightweight Directory Access Protocol** (LDAP) authentication.

- Local authentication: User management, authentication, and security policies are all controlled by the eSight server. The eSight uses this mode by default. For details about this mode, see the "**Local Authentication**" section.
- RADIUS authentication: When a user logs in, the eSight verifies and authenticates the login request through the RADIUS server, finds the role of the user based on the user group obtained from the RADIUS server, and authorizes the user. For details about this mode, see the "**RADIUS Authentication**" section.
- LDAP authentication: When a user logs in, the eSight verifies and authenticates the login request through the LDAP server, finds the role of the user based on the user group obtained from the LDAP server, and authorizes the user. LDAP authentication is similar to RADIUS authentication except that the two modes use different authentication protocols. For details about this mode, see the "**LDAP Authentication**" section.

Local Authentication

In the local authentication mode, user security management ensures the security of the eSight on multiple levels, including the local user management, rights management, password policy, account policy, login control, and automatic client logout. Password and account policies, after being configured, take effect on all eSight users.

- Password policy
  - Minimum password length (8 characters by default)
  - Maximum attempts to enter the password the same as old passwords (3 attempts by default)
  - Maximum number of occurrences of a character in a password (3 times by default)
  - Minimum time interval between password change attempts (5 minutes by default)
  - At least one special character in a password (not limited by default)
  - Password validity period, including the number of days (90 days by default) within which a password is valid and the time (7 days by default) when the eSight sends a warning before a password expires
- Account policy
  - Minimum length of a user name (6 characters by default)
  - Account invalidation: the number of days (60 days by default) within which an account is inactive

- Account locking: the maximum number of failed login attempts (5 attempts by default) within a certain period (10 minutes by default) before an account is automatically locked (for 30 minutes by default)

- Login control

  Login control includes time and IP address control.

  - Time control specifies the time during which users can log in. Users cannot log in to the eSight beyond the specified time.
  - IP address control specifies the IP addresses that the eSight clients can use to log in to the eSight server. IP address control prevents those who steal user names and passwords from logging in to the eSight server and therefore further enhances the eSight security.

- Automatic client logout

  To prevent other users from performing unauthorized operations, the eSight allows users to set the client to be automatically logged out. If a user does not perform any operations within a specified period of time, the client is automatically logged out.

RADIUS Authentication

When RADIUS authentication is adopted, the administrator does not need to create a user account on the eSight in advance. The user account for logging in to the eSight is an existing account that can pass the authentication of the RADIUS server.

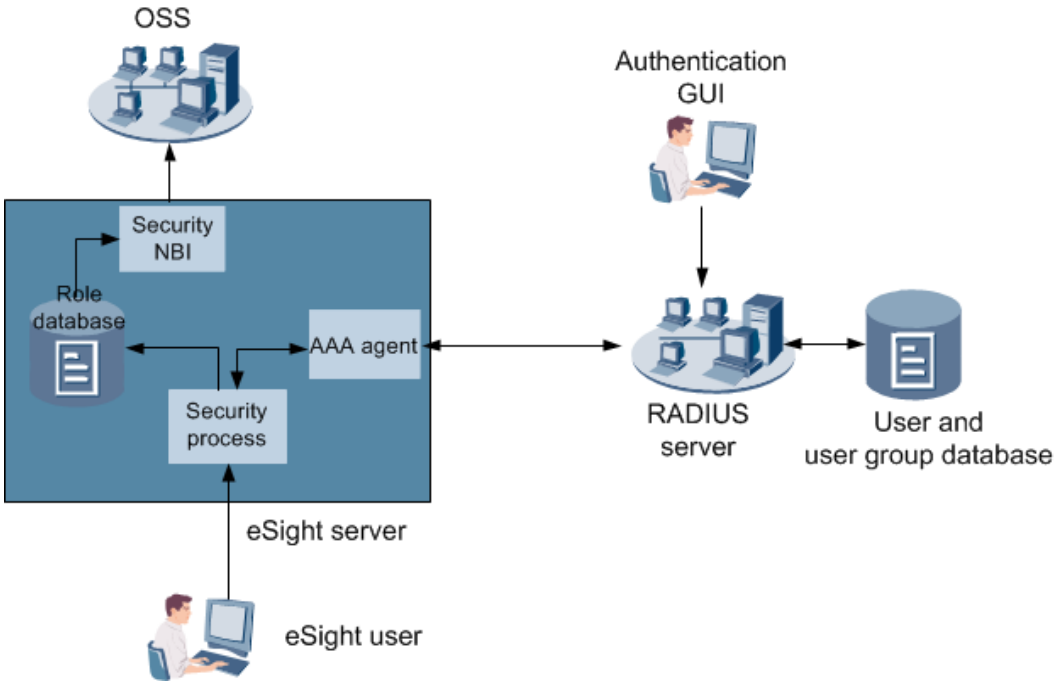
When a user enters the user name and password, the security process of the eSight server sends the user name and password to the RADIUS server. If the user is authenticated by the RADIUS server, the security process obtains the user group of the user from the RADIUS server, finds the matched role on the eSight, and authorizes the user.

NOTE

Before using the RADIUS authentication mode, ensure that the name of the role defined on the eSight is the same as that defined in the account database of the RADIUS server. In addition, ensure that the account to be authorized is added to a user group.

For the RADIUS authentication process, see **Figure 4-2**.

Figure 4-2 RADIUS authentication



LDAP Authentication

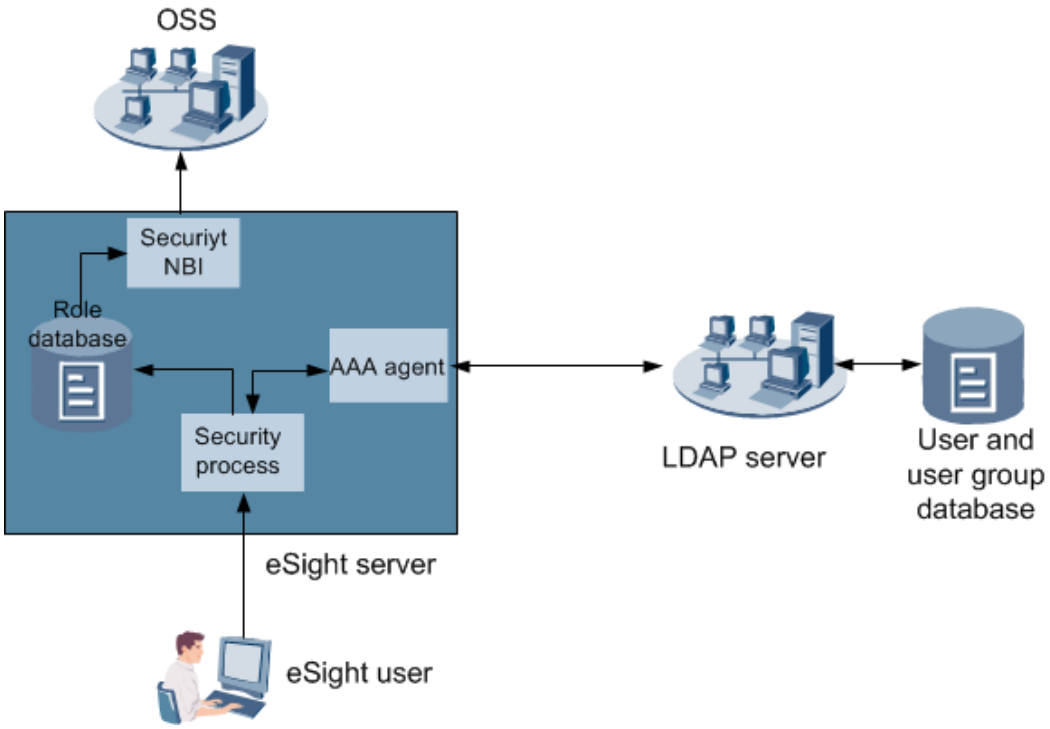
As a distributed client/server system protocol, LDAP is used in the VPN and WAN to control user access to the network and prevent unauthorized users from accessing the networks.

The LDAP authentication mode is similar to the RADIUS authentication mode, but they have different authentication protocols. The LDAP authentication mode supports the following features that are not supported by RADIUS authentication:

- Common mode (encryption-free), secure sockets layer (SSL) mode, and transport layer security (TLS) mode for communication between the eSight and LDAP servers.
- Multiple LDAP authentication servers.

For the LDAP authentication process, see **Figure 4-3**.

Figure 4-3 LDAP authentication



Online User Management

The eSight has the following online user management functions:

- Querying online users

  Online user information can be queried, including the user name, login time, and login IP address.

- Logging out of users

  When viewing online users, you can force an unauthorized user to log out. This prevents the unauthorized user from performing unauthorized operations on the eSightclient.

- Switching the user login mode

  The user login mode specifies whether to allow multiple users to log in to the eSight client concurrently. The multi-user mode is used in most cases. The single-user mode is used to prevent interference from other users when a user needs to perform special operations on the eSight server.

  - In single user mode, the eSight allows only the current user to log in to the eSight client, and other all online users are forcibly logged out.
  - After the current user exits the single user mode, other users can log in to the client again.

4.1.2 Log Management

eSight logs record important user operations. You can view the log list or details about a log, or export operation logs, operation logs, or system logs. The eSight provides information about logs with three levels (warning, minor, and critical).

Security Log

Security logs record the security operations that are performed on the eSight client, such as logging in to the server, changing passwords, creating users, and logging out of the server.

You can query security logs to understand the information about eSight security operations.

System Log

System logs record the events that occur on the eSight. For example, the eSight runs abnormally, the network is faulty, and the eSight is attacked. System logs help analyze the operating status of the eSight and rectify faults.

You can query system logs to understand the information about eSight system operations.

Operation Log

Operation logs record the operations that are performed on the eSight, such as adding a monitoring view and modifying the resource manager.

You can query operation logs to understand the information about user operations.

4.1.3 Resource Management

Resource management involves adding NEs and subnets, and managing NEs and subnets.

Adding NEs

- Auto Discovery for NEs:sets the eSight to automatically discover NEs.You can set the eSight to automatically search for NEs in a specified network segment and adds the found NEs.

  eSight supports SNMP, UC-SNMP, UC-TR069, UC-TCP, ICMP, SMI-S, TLV, and REST protocols.
- Adding a single NE: This mode applies to the scenario in which you want to add a few NEs with IP addresses and protocols available.
- Exporting NEs: You can record NE information to an .xls file and export the NEs to the eSight. This mode improves work efficiency for adding a large number of NEs.

Managing NEs or Subnets

NE or subnet management includes the following functions:

- Searches for NEs or subnets.

  You can search for NEs or subnets by setting search criteria.
- Creates, modifies, or deletes subnets.
  - You can group NEs into subnets based on the user-defined logic.
  - You need to modify the attributes of a subnet if the subnet information changes.
  - You can delete the subnets that do not need to be managed by the eSight.
- Views subnet information.

  You can view the basic information about a subnet.

- Views NEs information.

  You can view the basic information and protocol information about an NE.
- Adjusts the relationships between NEs and subnets or between subnets.

  You can adjust the relationships between NEs and subnets or between subnets if the network structure changes.

Adjusting Partitions for Devices

Partitions are used to handle device service data. You can plan device data on different partitions to prevent huge data volumes on certain partitions, which improves interaction efficiency between the eSight and the devices.

Group Management

Creating a Group

You can create a group and add NEs in different subnets to the group, which is considered as one object. You can assign the object (a group of NEs) to a user, which achieves NE assignment in batches.

- Viewing groups

  You can learn group details.
- Modifying groups

  You can modify groups to meet management requirements.
- Deleting groups

  You can delete groups that are not required by the system.

Device Resources

- You can search for device resources based on the network service classification, such as network devices, storage devices, unified communication devices, hosts and eLTE devices.
- You can perform service operations for a single device or devices in batches, such as deleting, setting protocol parameters, synchronizing devices, or moving to another subnet.

4.1.4 Alarm Management

When an exception occurs on a network, the needs to notify maintenance engineers in a timely manner so that they can recover the network quickly.

The eSight has the following alarm management functions:

- Monitoring network-wide alarms and remotely sending alarm notifications.

  The eSight informs maintenance engineers of faults immediately after the faults occur, ensuring troubleshooting in a timely manner.
- Masking alarms, and providing the alarm maintenance experience base.

  These functions improve alarm handling accuracy and efficiency.
- Synchronizing alarms, which ensures reliable alarm management.
- Providing customized functions such as alarm filter and alarm severity redefinition to meet requirements in various scenarios.

Alarm Severity

There are four alarm severities: critical, major, minor, and warning, as shown in **Table 4-1**. You can take different measures for different severities of alarms.

Table 4-1 Alarm severities

Alarm Severity	Description
Critical	An alarm severity that indicates a severe resource problem disrupting or severely impeding normal use.
Major	An alarm severity that indicates the possibility of some service-related problems with the resource. The severity of the problem is relatively high and the normal use of the resource is likely to be impaired.
Minor	An alarm severity that indicates the problems without affecting services. The problems of this severity may result serious faults, and therefore you need to take some corrective actions.
Warning	An alarm severity that indicates a condition exists that could potentially cause a problem with the resource.

Alarm Status

Alarm status is determined by alarm acknowledgment and clearance.

- Alarm acknowledgment: A user has tracked or handled an alarm.
- Alarm clearance: When the fault triggering an alarm is rectified, the device recovers. The alarm status changes to cleared.

Alarms can be classified into different status based on whether the alarms are cleared or acknowledged. **Table 4-2** describes the four alarm status.

Table 4-2 Alarm status

Alarm Type	Alarm Status
Current Alarms	Unacknowledged and uncleared
	Acknowledged and uncleared
	Unacknowledged and cleared
Historical Alarms	Acknowledged and cleared

- Status Change

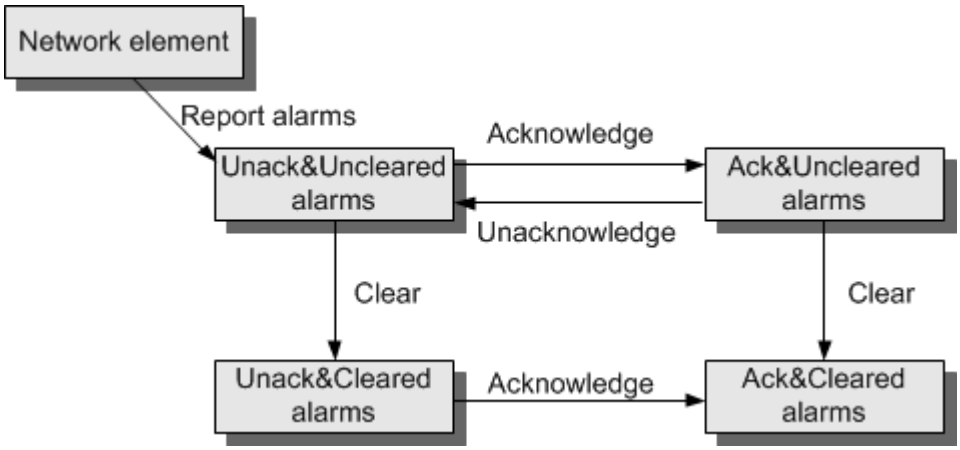
  Table 4-3 describes the alarm status change description.

Table 4-3 Status change

Status Change Type	Description
Clearance status change	If the condition that generated the alarm disappears, and the device becomes normal, the device reports a clear alarm and the alarm status is changed from uncleared to cleared.
Acknowledgment status change	The acknowledged alarms refer to alarms that have already been handled, or will be handled. When the alarm is acknowledged, the alarm is changed from unacknowledged to acknowledged. If you want to have concerns over the acknowledged alarm again, you can unacknowledge the alarm. When the alarm is unacknowledged, the alarm is changed from acknowledged to unacknowledged.

Figure 4-4 shows the relationship between alarm status.

Figure 4-4 Alarm status relationship



Faults, Alarms and Events

- Faults and alarms

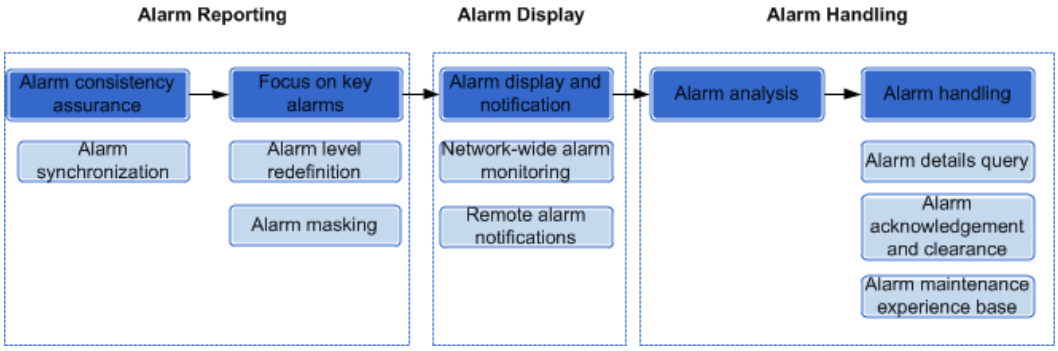
  An alarm is a message reported when a fault is detected. Not all faults result in alarms. Only the faults that the system can detect result in alarms. The others do not result in alarms, but they still persist.

- Alarms and events
  - Similarity: Both alarms and events are the presence of anything that takes place on the managed object detected by the eSight.
  - Difference: An alarm is a message reported when a fault is detected by eSight. An event is anything that takes place on a managed objects. When an alarm is generated, you need to troubleshoot the fault. Otherwise, the services may run abnormally. If an event occurs, the managed object has changes but the service may not be affected.

Alarm Reporting and Handling Flowchart

Figure 4-5 shows the alarm reporting and handling flowchart of the eSight.

Figure 4-5 Alarm reporting and handling flowchart



The following sections describe eSight alarm functions based on the flowchart.

Alarm Synchronization

After generating an alarm, a device reports the alarm to the eSight within less than 10s and the eSight then displays the alarm in the alarm list. After communication between the eSight and an NE recovers from an interruption, or the eSight is restarted, some alarms on the NE are not reported to the eSight. The NE alarms on the eSight are different from the actual alarms on the NE. In the case, you need to synchronize alarms to ensures that the eSight displays the current operating status of the NE correctly.

Alarms are synchronized according to the following rules:

- If an alarm is cleared from an NE but remains uncleared on the eSight, the alarm will be cleared from the eSight.
- If an alarm is present on an NE but absent on the eSight, the alarm will be added to the eSight.

Alarm Severity Redefinition

The eSight allows users to redefine (increase or reduce) the severities of some device alarms based on their actual concerns.

Alarm Masking

- Users can set alarm masking rules to mask unimportant alarms. Alarm masking rules include the date, time, alarm source, and alarm name.
- While an NE is being repaired, tested, or deployed, the NE may report a large number of alarms which can be ignored. In this case, you need to mask these alarms so that the eSight neither displays nor saves them.

Network-Wide Alarm Monitoring

In traditional domain-based maintenance, cross-domain faults are manually handled, which is inefficient. The eSight provides the network-wide alarm monitoring function that enables users

to learn the running status of the entire network. The eSight also provides the template-based alarm filter function. Specifically, the eSight allows users to set alarm filter templates with common filter criteria such as the location, type, and network layer of devices that generate alarms. The templates facilitate alarm queries.

On the eSight, users can monitor alarms by severity or device.

- By severity: Users can monitor network-wide alarms of each severity. For details, see the "**Alarm Monitoring by Severity**" section.
- By device: Users can view alarms of network-wide devices. For example, a user can view all current alarms of a device or a type of device. For details, see the "**Alarm Monitoring by Device**" section.

Alarm Monitoring by Severity

Alarms can be monitored by severity on the alarm panel and in the current-alarm list and by alarm sound. **Figure 4-6** shows the alarm panel.

Figure 4-6 Alarm board

Table 4-4 Alarm monitoring by severity

Function	Description
Alarm panel	The alarm panel displays the total number of current alarms of each severity on an MO. It provides an overall view of system faults and can serve as the monitoring board.
Alarm sound	Users can specify sounds for alarms of different severities. After an alarm is generated, the sound box on an eSight client plays the specified sound.
Current-alarm list	Users can set filter criteria and enter keywords to search for alarms that have not been acknowledged or cleared.

Figure 4-7 shows the **Current Alarms** page.

Figure 4-7 Current Alarms

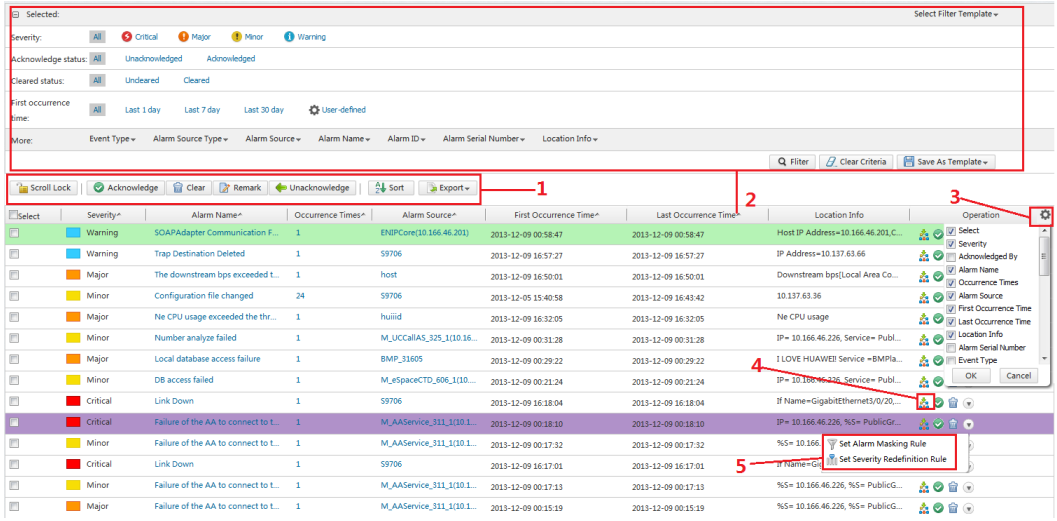


Table 4-5 lists the functions on the **Current Alarms** page, which are marked by numbers in Figure 4-7.

Table 4-5 Functions on the Current Alarms page

No.	Function Description
1	The following global operation buttons in this area take effect on all selected alarms: ● Lock/Unlock Users can click **Lock** or **Unlock** to specify whether newly generated alarms are added to the current-alarm list. In the lock state, newly generated alarms are not added to the current-alarm list; acknowledged and cleared alarms are not added to the historical-alarm list before the current-alarm list is unlocked. ● Export Users can click **Export** to export alarm information, which helps diagnose faults and back up data. ● Acknowledge Users can click **Acknowledge** to acknowledge alarms. Acknowledged alarms can be ignored by other users. ● Clear Users can click **Clear** to manually clear the alarms that cannot be automatically cleared or do not exist on devices. ● Remark Users can click **Remark** to enter information, for example, alarm handling progress and status.

No.	Function Description
2	Users can select or set filter criteria to browse desired current alarms. The eSight provides the following six default filter criteria: ● Alarm alarms ● Unacknowledeged critical alarms ● Unacknowledged major alarms ● Uncleared critical alarms ● Uncleared major alarms ● Alarms generated during the past 24 hours. Users can set desired filter criteria in the **Selected** area.
3	Users can customize the columns to be displayed in the alarm list.
4	Users can locate the object that generates an alarm in the topology view.
5	Users can perform other operations on an alarm, for example, setting alarm masking rules and redefining alarm severities.

Alarm Monitoring by Device

Users can view alarms of network-wide devices. For example, a user can view all current alarms of a device or a type of device. In the topology view, the device icons are color-coded by the highest severity of alarms generated on the devices.

Remote Alarm Notification

Users can set rules for sending remote alarm or event notifications. After alarms or events that match the rules are generated, the eSight sends them to specified recipients by short message or email. This helps remote maintenance personnel learn the alarms or events in a timely manner and take appropriate measures.

Users can customize the required notification template and recipient groups.

Alarm Analysis

By querying and analyzing historical alarms and events and masked alarms, users can learn the alarm status of a device and improve device performance accordingly. The eSight can collect alarm statistics based on the statistical conditions that are set by users. The statistical conditions include the subnet or device, alarm or event name, first generation time, and alarm severity. Users can use some of these conditions to collect alarm statistics.

Alarm Handling

- Viewing alarm details

  Users can click a current, historical, or masked alarm in the alarm list to view the alarm details in the **Alarm Details** dialog box. Alarm details include the alarm name, handling suggestions, and location information.

- Acknowledging and clearing alarms

  Figure 4-7 show the buttons for acknowledging and clearing alarms.

- Adding alarm maintenance experience

  In the **Alarm Details** dialog box, users can add alarm maintenance experience for maintenance personnel to refer to when they handle the same alarm in the future.

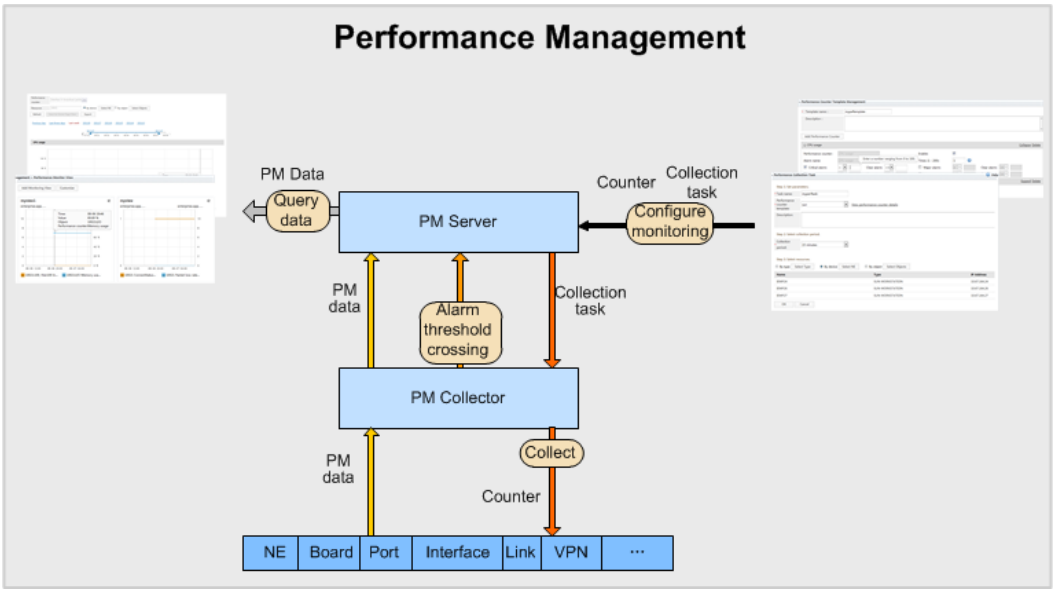
4.1.5 Performance Management

The performance of a network may deteriorate because of internal or external factors and faults may occur. To achieve good network performance for live networks and future networks while controlling costs, network planning and monitoring are necessary. In addition, network efficiency such as throughput rate and resource usage needs to be measured. The performance management function enables you to detect the deteriorating tendency in advance and solve the potential threats so that faults can be prevented.

Performance Management Process

The eSight uses a graphical user interface (GUI) to monitor key network indicators and display statistics on the collected performance data, as shown in **Figure 4-8**

Figure 4-8 Performance management process



eSight performance management includes an impressive array of functions, including counter template management, collection task management, historical performance data query, real-time performance data query, and performance counter collection status monitoring. The following describes performance management modules.

Counter Template Management

Devices of the same type have the same counter attributes that can be specified in a counter template. The counter template can be directly loaded to quickly set collection counters for specified devices when you create a performance collection task.

The eSight offers the following counter template management functions:

- Add, delete, or modify counter templates.
- Set counters in counter templates (performance data to collect).
- Specify performance counter thresholds in counter templates. If a counter has met threshold conditions for several consecutive times, an alarm is generated. You can monitor the performance of specified resources through alarms.

  Thresholds include the upper and lower limits for triggering and clearance. Threshold alarms are classified into upper limit alarms and lower limit alarms. **Table 4-6** lists relationships among the counter, threshold, and alarm.

Table 4-6 Performance counter, threshold, and alarm

Counter and Threshold Relationship	Threshold Alarm
Lower trigger value <= or < Performance counter < or <= Upper clearance value	Lower limit alarm
Lower clearance value <= or < Performance counter < or <= Upper trigger value	Upper limit alarm

Collection Task Management

The eSight allows you to manage performance data collection tasks. Collection tasks define the devices and counters to collect performance data. After the counter data about a device is collected, you can view historical performance data about the device.

By default, the eSight offers the following global collection tasks to collect performance data about network-wide devices:

- Connect Status Monitor
- CPU Usage Monitor
- Memory Usage Monitor
- Packet Loss Rate Monitor
- Port Usage Monitor
- Response Time Monitor

You can customize the following information about global collection tasks:

- Start or stop a collection task.
- Change the collection interval.
- Check the counter collection status of devices.

The eSight also offers the following performance task management functions:

- Add, delete, start, stop, and modify performance collection tasks.
- View the counter collection status.

Performance Counter Collection Status Monitoring

After a performance collection task is created, you can regularly monitor the performance counter collection status to rectify collection faults in a timely manner and ensure that the collection task collects correct data for your query and analysis.

The eSight allows you to monitor the performance counter collection status by resource type and collection task.

On the page where performance counter data is displayed, you can also view historical performance data and check statistical diagrams about historical data.

Querying Historical Performance Data

After the eSight collects device performance data, you can query historical performance data by counter and resource on the eSight client, which helps you keep abreast of the performance trend and prevent fault occurrence.

The eSight displays historical data in curve graphs.

- Querying historical performance data by specifying the collection object
  - You can query the historical performance data by specifying the counter, resource, or interval. Resource query modes include by device and object. **Table 4-7** lists the resource query modes.

Table 4-7 Resource query modes

Resource Query Mode	Description
By device	Select devices. After devices are selected, the data about objects of the same type on the devices is displayed. For example, if the counter is set to the CPU usage rate and a device that involves multiple CPUs is selected, the historical CPU usage rates about all CPUs on the device are displayed in curve graphs.
By object	Select an object on the device, for example, select one or more CPUs on a device.

  - You can export query results as .csv files.
  - You can save query results as a view on the homepage, which enables you to monitor historical performance data on the homepage.

    Because a two-dimensional graph displays a maximum of two vertical axes, each performance data curve diagram displays a maximum of two data units on the eSight. In addition, when you customize collection objects to check historical performance data, each performance data curve diagram displays a maximum of six performance data lines. Therefore, if the number of selected counter data units exceeds two or the number of performance data lines exceeds six, the eSight displays historical performance data in different views.

You can save query results as a view on the homepage only when the query results are displayed in a single curve graph. If the query results are displayed in multiple curve graphs, decompose the query several times if you want to use this function.

- Querying historical performance data in the performance monitoring view

  The eSight allows you to add key device performance counters as monitoring views, which enables you to monitor the device performance status in the performance monitoring view. Meanwhile, the added monitoring views can be displayed on the homepage.

Querying Real-Time Performance Data

You can query real-time performance data to monitor the running status of devices, which enables you to take prompt measures in response to exceptions. For example, when a threshold alarm (such as high CPU usage) is reported, you can check the real-time performance data and determine whether an exception occurred.

The eSight displays real-time data in curve graphs.

- You can query real-time performance data by specifying search criteria.
- You can export query results as .csv files.

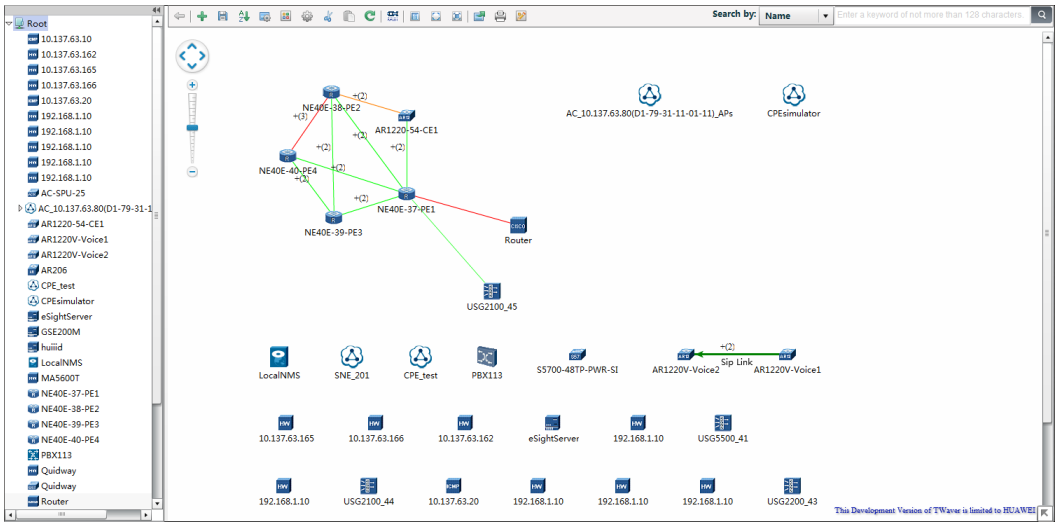
4.1.6 Topology Management

Topology management involves creating and managing the topology of the entire network. You can learn about the operating status of the entire network based on the colors and status of the NE icons in the physical view.

Table 4-8 Terms in topology management

Term	Description
NE	Core unit of topology management, which is used to identify managed devices. In a topology view, different icons indicate different types of NEs.
Subnet	Smaller networks divided from a large network based on the region or device type to simplify network management.
Link	Physical or logical connection between devices.

Figure 4-9 Topology Management page



Managing Topology Objects

Topology objects include subnets, physical NEs, virtual NEs, links, and subordinate resources.

- Creates or deletes a virtual NE

  Virtual NEs are those that cannot be managed by the eSight on the entire network.

  - Adding virtual NEs to the physical view helps you understand the operating status of the entire network.
  - You can delete unused virtual NEs from the physical view when the network structure changes.
- Creates or deletes a virtual link

  Virtual links do not actually exist on the network. They represent logical relationships between topology objects.

  - By creating virtual links, you can learn about the relationships between topology objects.
  - You can delete unused links from the physical view when the network structure changes.
- Deletes a subnet

  You can delete a subnet that does not need to be managed by the eSight.

Adjusting the Physical View

Physical view adjustment includes the following functions:

- Adjusts the relationship between an NE and a subnet

  When the network structure changes, you need to adjust the positions of NEs or subnets in the topology view to update the relationships between the subnets or NEs and other topology objects. Adjusting the relationship between an NE and a subnet involves:

  - Adjusts the positions of NEs or subnets in the physical view
  - Adjusts the relationships between NEs and subnets
  - Adjusts the relationship between subnets
- Sets the topology background

You can set a background based on the layout of topology objects. The background helps you understand the positions of the topology objects.

- Rearranges topology objects in a physical view

  The eSight allows users to arrange topology objects in the following ways:

  - Round: Topology objects are arranged in a loop.
  - Symmetry: Topology objects are symmetrically arranged.
  - Star: Topology objects are arranged in the form of a star.
  - From Top to Bottom: Topology objects are arranged from top to bottom.

Browsing the Physical View

- Searches for a topology object

  You can use the search function to quickly locate an object, such as an NE, a link, or a subnet.

- Zooms in or out on the physical view

  You can zoom in or zoom out on the physical view, restore the physical view to its initial state, and make the physical view fit into the screen or display the physical view in full screen.

- Views the physical view in full screen or aerial view

  You can view the physical view in full screen or in aerial view. The aerial view helps you browse the entire physical view and locate the area displayed in the topology window.

- Prints, exports, or saves the physical view
- Sets a device label

  The device label information includes the name, IP address and system name of a device.

Monitoring the Network Running Status in the Physical View

By monitoring the network running status in the physical view, you can:

- Monitor the NE alarm status

  The NE running status can be presented by rendering the NE icons. When an NE becomes faulty, the NE icon color changes to map the alarm severity.

- Monitoring the NE connection status

  The NE connection status can be presented by rendering the NE icons. When an NE becomes offline, the NE icon color changes to gray.

- Monitoring the alarm status of the device set on a subnet

  The device set running status on a subnet can be presented by rendering the subnet icon. When devices on the subnet become faulty, the subnet icon color changes to map the highest alarm severity of the device on the subnet.

- Monitoring the connection status of a device set on a subnet

  The device set connection status on a subnet can be presented by rendering the subnet icon. When a device on the subnet becomes offline, the subnet icon color changes to gray.

4.1.7 Maintenance Tool

The maintenance tool allows you to manage the eSight server and its databases and processes.You can monitor the running status of the eSight server and identify exceptions in a timely manner, which ensures normal running of the eSight server.

Monitoring the System

- View the status of all products managed by the maintenance tool.
- View the distributed deployment of a product.
- Start or stop a product.
- Start or stop a process.

Managing the eSight Server

- Views the basic server information.
- Views process information.
- Monitoring the thresholds of server resource usage

  You can use the maintenance tool to monitor the CPU usage, memory usage, disk usage, and database usage of the eSight server. When the usage reaches its threshold, the maintenance tool reports an alarm to the eSight.

Managing the Database

- Monitoring the database

  You can monitor the database status of the eSight server to view the information such as the database name, server name, and database status.
- Changing a database user password

  Changing database user passwords regularly can ensure data security.
  - Changes the password of a Database Administrators.

    NOTE

    Administrator names vary with databases. The administrators for different databases are as follows:

    root: MySQL database administrator

    sa: SQL Server database administrator

    system: Oracle database administrator

    guassdba: GuassDB database administrator
  - Changes the password of a NMS database user **commonuser**.

Managing the HA System

- Connecting the primary server to the secondary server

  After the eSight is installed at the primary and secondary servers, you can use the maintenance tool to connect the primary server to the secondary server.
- Forcibly making a server become the primary server

  When the HA system is in the recovery state, you can use the maintenance tool to forcibly make one server become the primary server to ensure proper running of the HA system.

- Disconnecting the primary server to the secondary server

  When you need to uninstall the eSight or do not need the HA system, you can use the maintenance tool to disconnect the primary server from the secondary server.

Backup and Restore

You can customize backup policies, or back up and restore data manually. The backups include configuration files and database data.

Managing the Maintenance Tool

- Changes the maintenance tool user password.

  Regularly changing the password of the **sys** user helps improve security of user information.

- Queries the operation logs of the maintenance tool.

  The operations that the **sys** user performs on the maintenance tool client are recorded, for example, starting and stopping the eSight and changing user passwords.

  NOTE

  The maintenance tool can record a maximum of 20000 operation logs. When there are more than 20000 operation logs, the maintenance tool automatically deletes the earliest 1000 logs.

4.1.8 Lower-Layer NMSs

eSight allows you to divide a network into several layers and manage NEs on the network by layer. Links of lower-layer NMSs are displayed on the eSight home page. You can click a link to access the lower-layer NMS management page and check alarms, performance counters, reports, and the network topology on a lower-layer NMS.

The following lower-layer NMS management functions are provided:

- On the lower-layer NMS management page, you can add, delete, and modify lower-layer NMSs and manually check the connections between eSight and lower-layer NMSs.

  Figure 4-10 Managing 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 4-11 Portal for lower-layer NMSs

4.1.9 License Management

License refers to the permission that the vendor grants for users with the eSight management capacity, number of connected clients, and duration. License management involves querying license information, obtaining an ESN, revoking a license, importing a license, and sending license alarms.

The eSight has the following license management functions:

Querying License Information

You can query the license authorization and consumption information about the eSight client.

Obtaining an ESN

You can obtain an ESN from the eSight client. The ESN is required when you apply for a new license.

Revoking a License

When the ESN changes or the network is adjusted, you can revoke the current license and use the generated invalidity code to apply for a new license.

NOTE

Only the user with the **Revoke License** permission can revoke the current license.

A trial license cannot be revoked.

Importing a License File

You can import a new license file from the eSight client to the eSight server.

NOTE

Only the users with the **Update License** permission can import license files.

Sending License Alarms

When a license becomes abnormal, the system displays the license status and sends a license alarm, which prevents service interruption due to license expiry.

4.1.10 View Display on Home Pages

The eSight can use portlets on home pages to display key device data. This helps you monitor device status, detect abnormal devices, and handle faults in a timely manner, which ensures proper device running.

Home Page Management

- Creating a home page

  The eSight provides only one default home page. You can create multiple home pages and display portlet views that you concern on different home pages by type.
- Modifying a home page name

You can modify a home page name to re-identify the home page.

- Displaying a home page on the top

  You can display a home page that you concern on the top.

- Deleting a home page

  You can delete redundant home pages.

Portlet Management

Portlets are views that display devices and network-wide device status in lists, curves, and bar charts. Portlets are displayed in areas of a home page.

- Creating a user-defined portlet

  You can integrate third-party interfaces to the eSight home page to monitor them.

- Displaying and hiding a portlet

  You can display only the portlets that you concern on a home page and hide those that you do not concern.

- Manually updating portlet data or setting the period for updating portlet data

  You can update monitoring data in real time.

- Zooming in on and zooming out of a portlet

  You can zoom in on and out of a portlet as required.

The following table lists portlets supported by eSight.

Table 4-9 eSight portlets

Type	Portlet	Function
AppBase Portal	Network Device Number Changes of Online Terminals	Display the changes in the number of online terminals in a period.
	Fibre Channel Switch Port Connection Status	Shows the Fibre Channel switch port connection status
	Storage Device Status	Shows the current status of storage devices
	eLTE Terminal Statistics	Display statistical information about online and offline eLTE devices
	Lower-Layer NMS	Displays some lower-layer NMSs and their status.
Monitor Portal	Alarms on TopN NEs	Shows the number of alarms on TopN NEs.
	Current alarms	Shows the number of alarms of each severity.

Type	Portlet	Function
	TopN Average Inbound bandwidth usage on interface	Displays TopN interfaces that occupy the highest average inbound bandwidth usage in the last hour, the last 24 hours, or the last 7 days.
	TopN Average Outbound bandwidth usage on interface	Displays TopN interfaces that occupy the highest average outbound bandwidth usage in the last hour, the last 24 hours, or the last 7 days.
	CPU Trend	Displays the CPU usage of the selected devices within the latest 24 hours.
	TopN Average CPU Usage(%)	Displays TopN online devices with the highest CPU usage within the latest one hour.
	TopN Average Memory Usage(%)	Displays TopN online devices with the highest memory usage within the latest one hour.
WLAN Portal	WLAN User Statistics	Display the trend chart of WLAN online users in a specified period.
	TopN AP Upstream Port Traffic and Channel Usage	Display TopN AP Upstream port traffic and Channel usage information.
	TopN WLAN Average CPU Usage	Display TopN AC and AP average CPU usage in last hour,the last 24 hours,or the last 7 days.
	Rogue Devices And Rogue Clients Statistics	Display WLAN Rogue Devices And Rogue Clients statistics.
	Interferers Statistics	Display WLAN Interferer statistics.
	TopN WLAN Average Memory Usage	Display TopN AC and AP average memory usage in last hour,the last 24 hours,or the last 7 days.
	User Statistics of Client Radio Types	Display user statistics of WLAN client radio types.
	TopN WLAN Latest Alarms	Display the latest WLAN topN alarm information.
	TopN Region Statistics	Display TopN region statistics.
	TopN SSID User Statistics	Display TopN SSID user statistics.
	TopN AP User Association Failure Rate	Display TopN AP user association failure rate information.

Type	Portlet	Function
	WLAN Channel Utilization Trend	Display the trend chart of WLAN channel utilization in a specified period.
	Wireless Resource Statistics on the Network	Display wireless resource distribution on the network.
DC nCenter	TopN Host Average CPU Usage	Displays TopN average CPU usage information of the hosts.
	TopN Host Average Memory Usage	Displays TopN average memory usage information of the hosts.
	TopN VM Average CPU Usage	Displays TopN average CPU usage information of the VMs.
	TopN VM Average Memory Usage	Displays TopN average memory usage information of the VMs.
MPLS VPN	BGP/MPLS VPN Alarm Statistics	Displays service alarm severity statistics.
	BGP/MPLS VPN Status Statistics	Displays VPN service status statistics.
SLA	Min. TopN SLA Compliance	Display TopN tasks with lowest SLA compliance.
	TopN SLA LSP PING Indicator	Display TopN SLA lsp ping tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA DNS Indicator	Display TopN SLA dns tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA TCP Indicator	Display TopN SLA tcp tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA UDP Indicator	Display TopN SLA udp tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA UDP JITTER Indicator	Display TopN SLA udp jitter tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA SNMP Indicator	Display TopN SLA snmp tasks with lowest SLA compliance in a specified SLA counter.
	Recent Smart Policy Tasks	Display Recent Smart Policy Tasks.

Type	Portlet	Function
	TopN SLA DHCP Indicator	Display TopN SLA dhcp tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA HTTP Indicator	Display TopN SLA http tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA ICMP JITTER Indicator	Display TopN SLA icmp jitter tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA LSP JITTER Indicator	Display TopN SLA lsp jitter tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA ICMP Indicator	Display TopN SLA icmp tasks with lowest SLA compliance in a specified SLA counter.
	TopN SLA FTP Indicator	Display TopN SLA ftp tasks with lowest SLA compliance in a specified SLA counter.
QoS	TopN Average Bandwidth Usage of Traffic Classifier	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Excess Bandwidth Rate	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Number of randomly dropped packets in WRED mode	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Number of tail-dropped packets in WRED mode	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Rate of Discarded Bits	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Rate of Matched Bits	Displays TopN tasks of highest QoS in a specified QoS counter.
	TopN Average Rate of bits transmitted	Displays TopN tasks of highest QoS in a specified QoS counter.
NTA	Top IP Group Traffic	Displays the top ip group traffic.
	TopN Application Group Traffic	Displays the top application group traffic.
	TopN Application Traffic	Displays the top application traffic.

Type	Portlet	Function
	TopN Conversation Traffic	Displays the top conversation traffic.
	TopN DSCP Group Traffic	Displays the top DSCP group traffic.
	TopN DSCP Traffic	Displays the top DSCP traffic.
	TopN Device Traffic	Displays the top device traffic.
	TopN Host Traffic	Displays the top host traffic.
	TopN Interface Group Utilization	Displays the top interface group utilization.
	TopN Interface Group Traffic	Displays the top interface group traffic.
	TopN Interface Traffic	Displays the top interface traffic.
	TopN Interface Utilization	Displays the top interface utilization.

4.1.11 Database Overflow Dump

eSight provides the database overflow dump function to ensure sufficient database space. eSight checks the database space every day for modules that have a large amount of data. If data overflow occurs, eSight automatically dumps data to the specified path.

Data overflow dump includes overflow dump for logs, alarms, performance data, SLA data, nCenter data, NTA data, config file manager data, and terminal access data.

4.1.12 Two-Node Cluster System

The eSight high-availability system offers two-node cluster hot standby and switchover functions. Software and hardware requirements for active and standby servers are the same. The Veritas remote hot standby technology is used to synchronize data between active and standby servers in real time, and dynamically monitor eSight running status. In case of a hardware, operating system, or key application fault, eSight automatically switches services to the standby server within 15 minutes.

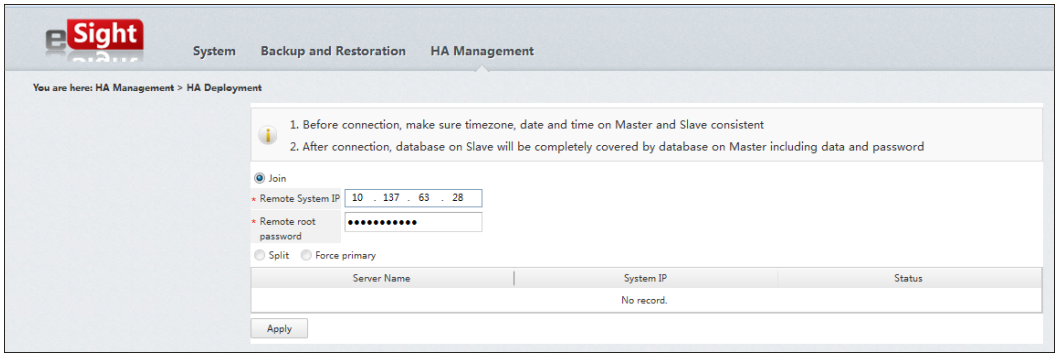
Two-Node Cluster Deployment

Two-node cluster deployment involves the installation of the RAID disk partition tool, Linux operating system, Veritas software, Oracle database, and eSight software. To reduce installation complexity and improve installation efficiency, the Linux operating system can be installed through a single mouse click. The Veritas software and Oracle database can be installed jointly.

Two-Node Cluster Association

After the software is installed, associate active and standby servers.

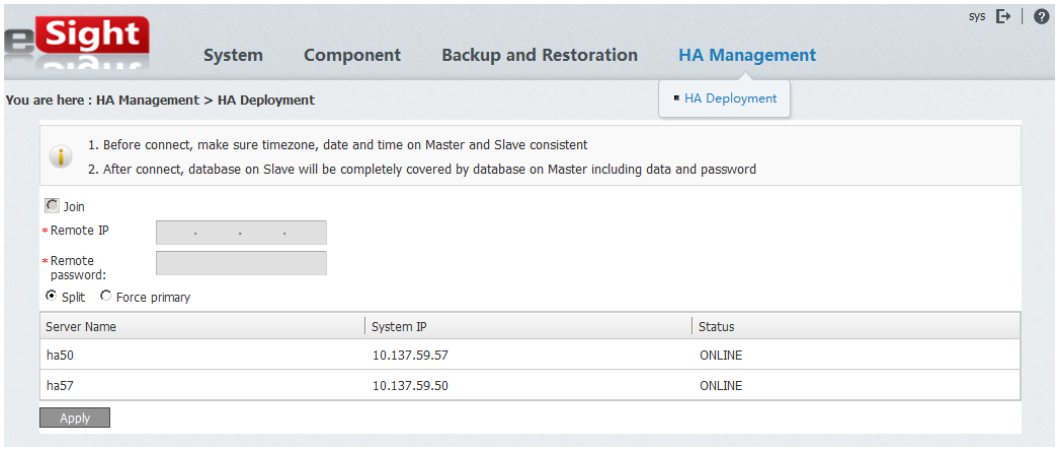
Figure 4-12 Associating active and standby servers



Two-Node Cluster Disassociation

You can also disassociate active and standby servers.

Figure 4-13 Disassociating active and standby servers



4.2 Device Management

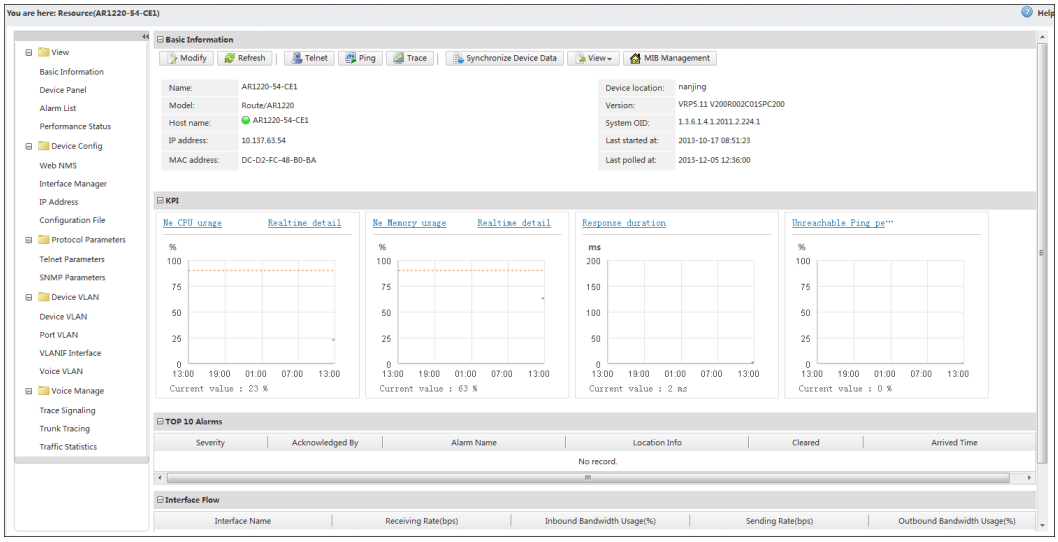
4.2.1 Network Equipment Management

Offers basic management and configuration over network devices, including network device discovery and maintenance, route configuration, interface management, Layer-2 link management, IP topology, and device accessories.

4.2.1.1 Network Equipment Management

eSight offers network equipment management functions, and integrates entries for information query, maintenance, and operation of a single NE to one page, which facilitates monitoring and maintenance of a single NE.

Figure 4-14 Viewing NE features

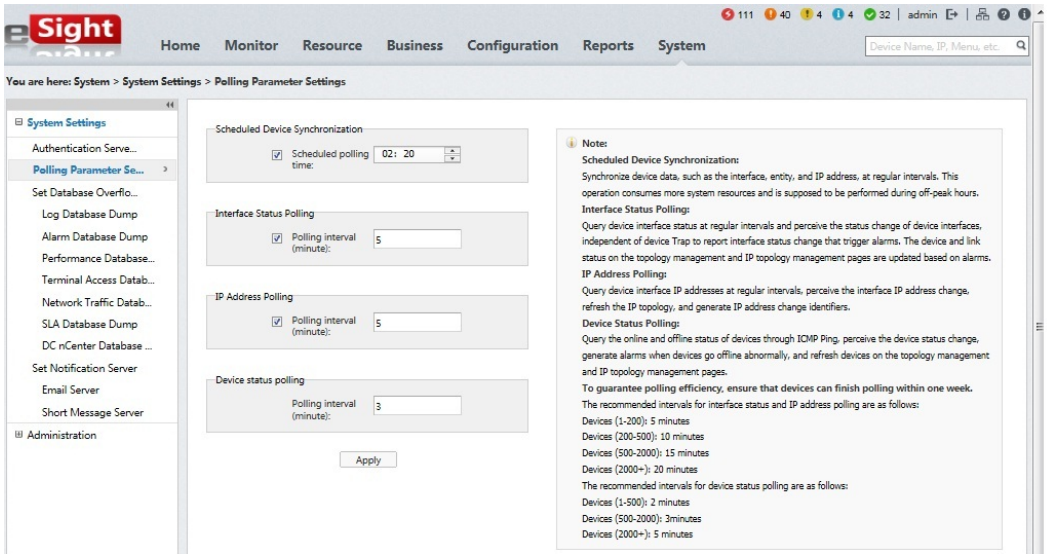


Functions

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

Polling Parameter Settings

Figure 4-15 Polling parameter settings



On the polling polling parameter settings page, you can set the periodical synchronization time and intervals for interface status polling, IP address polling, and device status polling.

Periodical device synchronization: Synchronizes device data, such as the interface, entity, and IP address, at regular intervals. This operation consumes more system resources and is supposed to be performed during off-peak hours.

Interface status polling: Queries device interface status at regular intervals and perceives the status change of device interfaces, independent of device Trap to report interface status change that trigger alarms. The device and link status on the topology management and IP topology management pages are updated based on alarms.

IP address polling: Queries device interface IP addresses at regular intervals, perceives the interface IP address change, refreshes the IP topology, and generates IP address change identifiers.

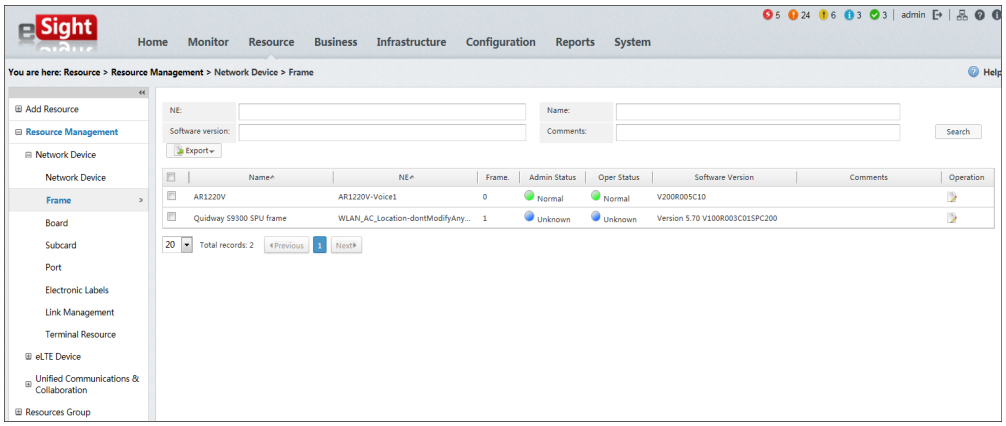
Device status polling: Queries the online and offline status of devices through ICMP Ping, perceives the device status change, generates alarms when devices go offline abnormally, and refreshes devices on the topology management and IP topology management pages.

Phisical Resource Management

- Frame Resources

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

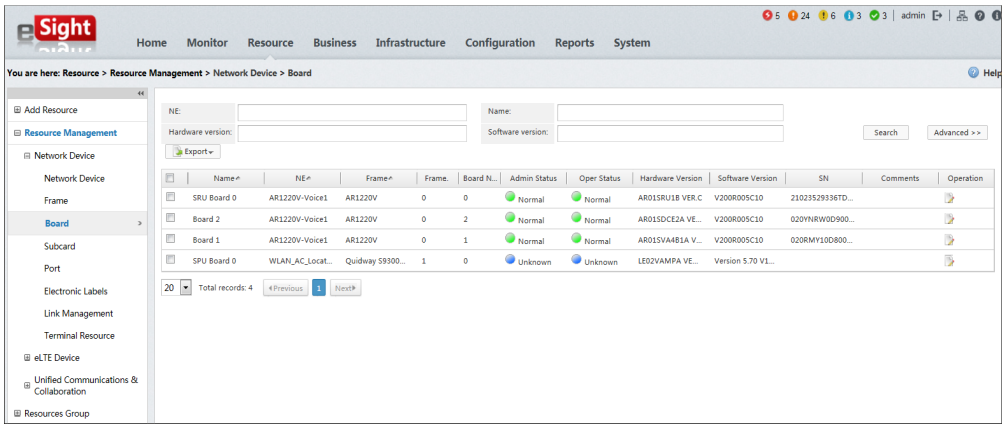
Figure 4-16 Frame Resources page



- Board Resources

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

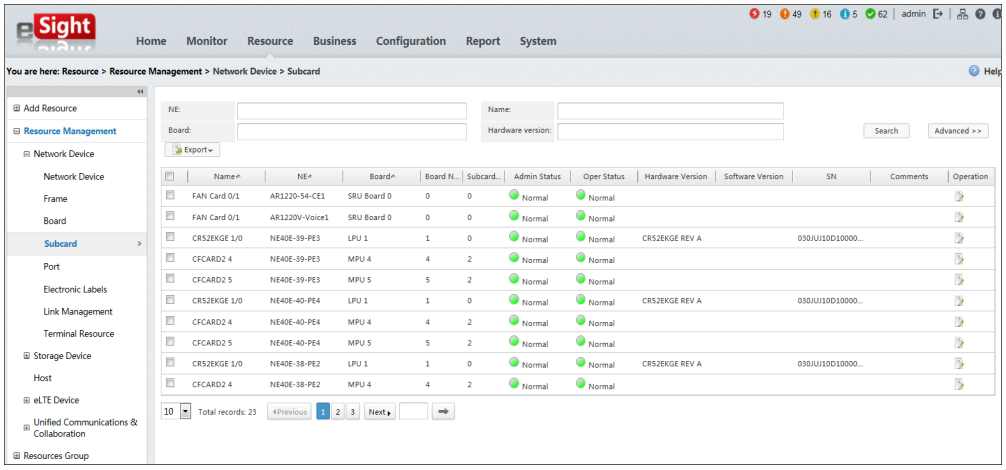
Figure 4-17 Board Resources page



- Subcard Resources

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

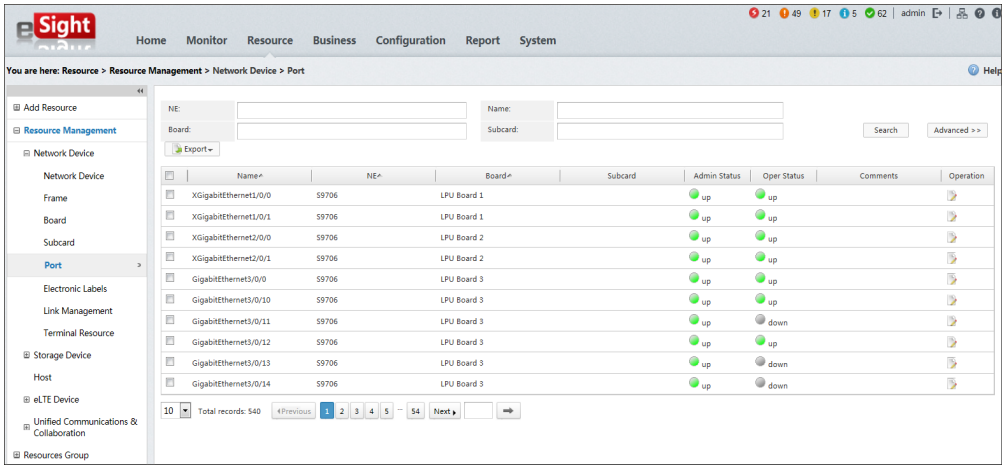
Figure 4-18 Subcard Resources page



- Port Resources

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

Figure 4-19 Port Resources page



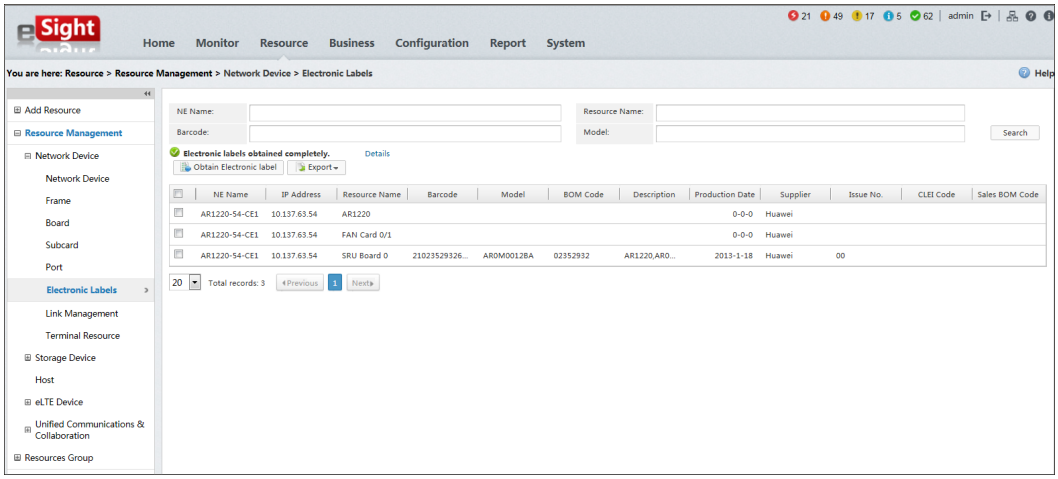
Electronic Labels

You can search for and export electronic labels of devices.

NOTE

Electronic labels are used to identify devices. They are used in network design, planning, and maintenance, asset management (including spare part management), order, account management, settlement, investment tracing, and warranty.

Figure 4-20 Electronic Labels

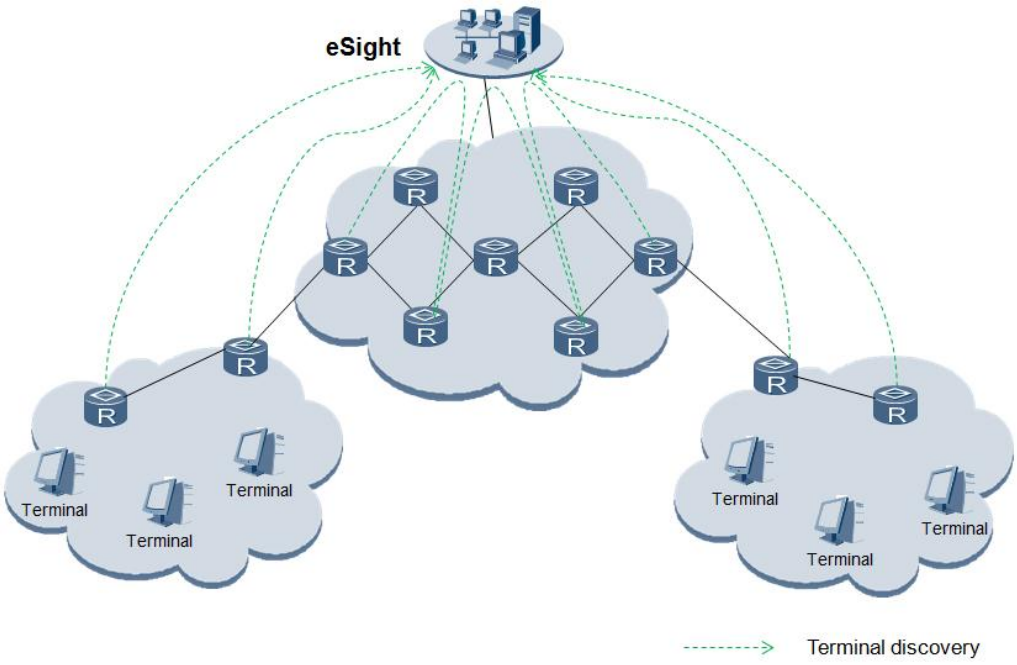


4.2.1.2 Terminal Resources

Terminal resources provides detailed information about access terminals and offers a unified approach for you to manage access terminals.

Terminals that have accessed the network can be discovered either by a manually conducted immediate discovery or a periodically conducted automatic discovery.

Figure 4-21 Terminal access solution

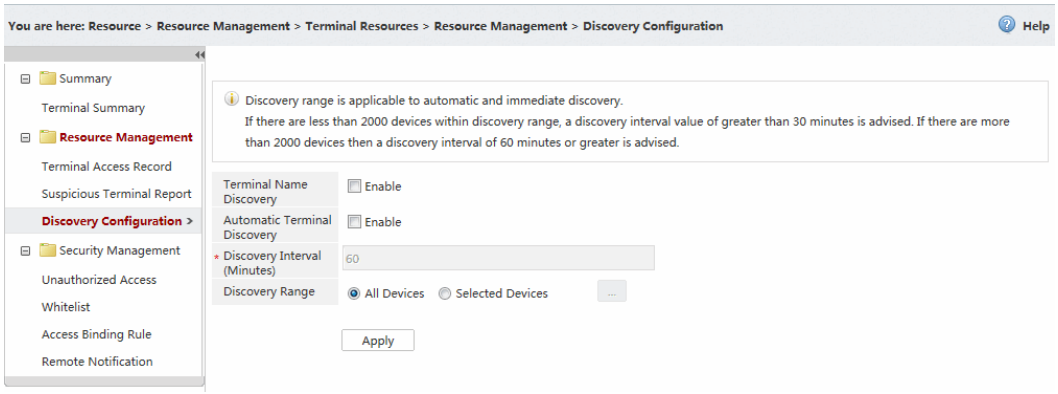


Terminal Discovery Configuration

You can configure:

- Whether to parse terminal names.
- Whether to enable automatic discovery.
- Intervals of automatic discovery.
- Discovery scope, which applies to both immediate discovery and automatic discovery.

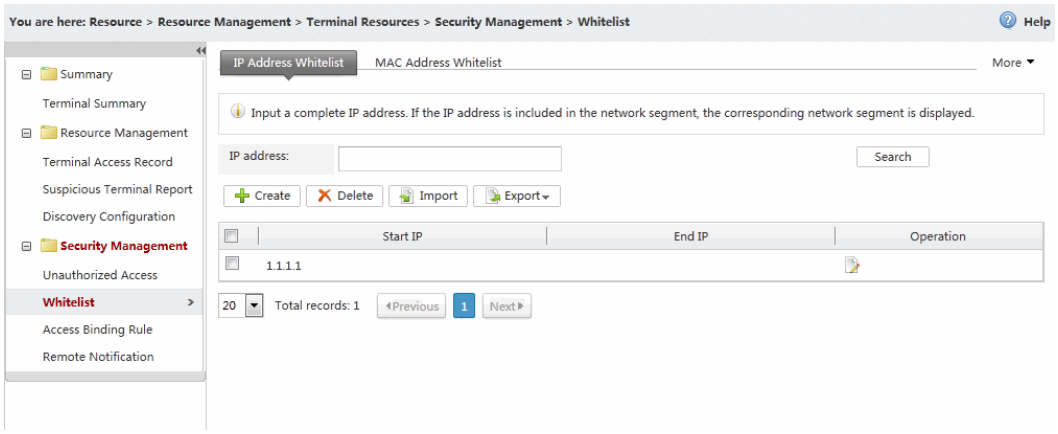
Figure 4-22 Discovery Configuration page



Whitelist

You can configure a whitelist that contains authorized IP addresses and MAC addresses. When the configuration takes effect, eSight checks whether a discovered terminal is authorized. If not, eSight records its details for you to acknowledge the unauthorized terminal.

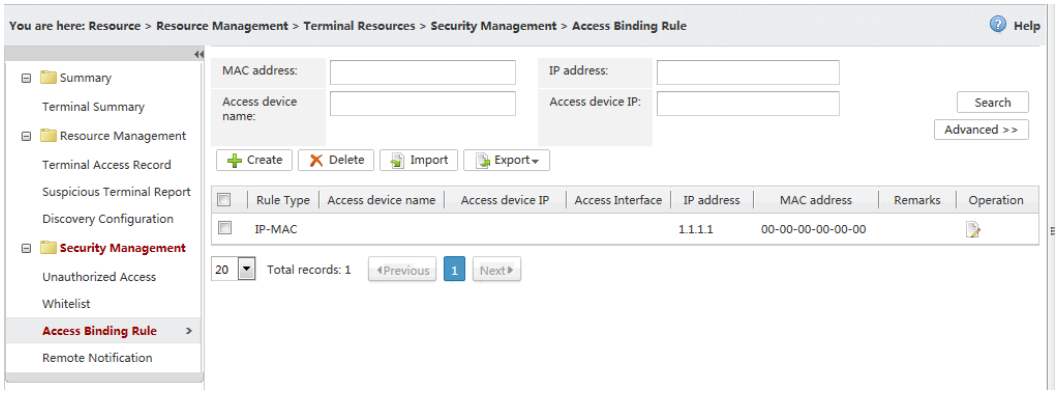
Figure 4-23 Whitelist page



Access Binding Rule

You can configure Port-IP or Port-MAC rules to restrict access terminals under device ports. Yon can also configure IP-MAC rules to restrict binding relationships between IP and MAC addresses. eSight identifies terminals that break these rules as unauthorized terminals and records detailed access information.

Figure 4-24 Access binding rule

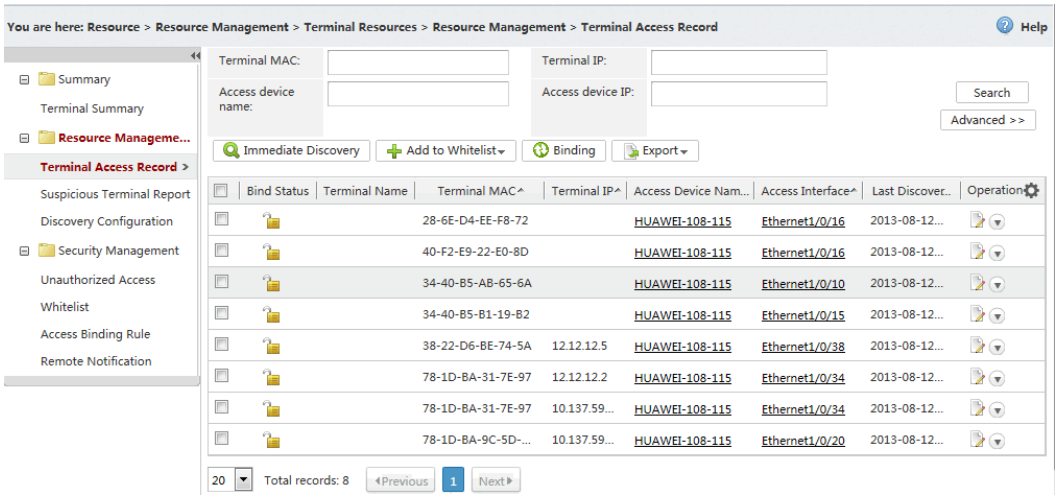


Terminal Access Record

In terminal access record, you can:

- Check terminal access details and history.
- Check unauthorized access logs.
- Jump to the topology view to view the access device of a terminal.
- Jump to the device panel to view the access port of a terminal.
- Configure remarks for a terminal.

Figure 4-25 Terminal Access Record page

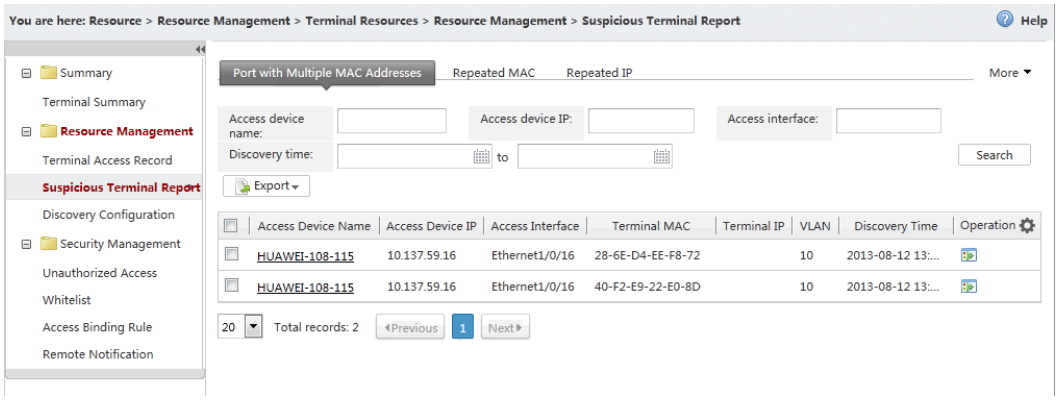


Suspicious Terminal Report

In suspicious terminal report, you can:

- Check for the ports connecting to multiple MAC addresses to detect devices accessing eSight with the same port.
- Check for duplicate MAC addresses to detect MAC address theft.
- Check for duplicate IP addresses to detect IP address theft.

Figure 4-26 Suspicious Terminal Report page

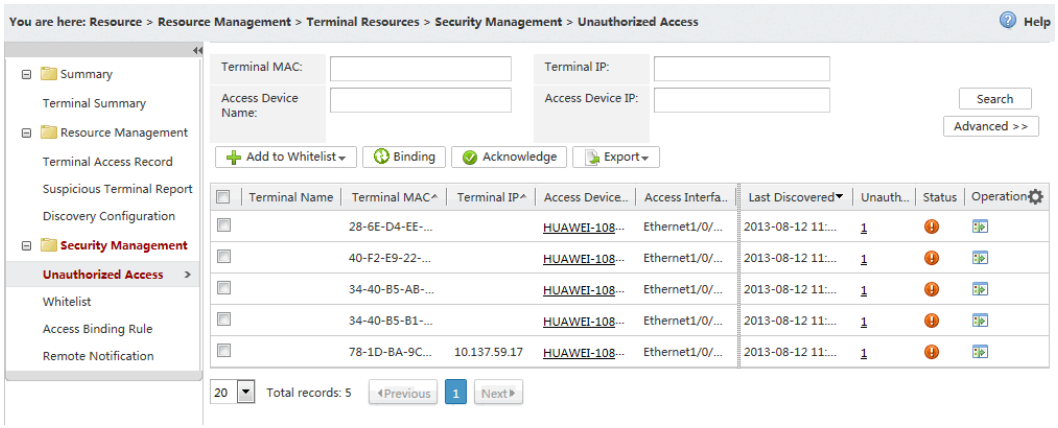


Unauthorized Access

eSight detects unauthorized terminal access based on the IP and MAC address whitelists configured. With unauthorized access management, you can:

- View unauthorized access logs and unauthorized terminal details.
- Export unauthorized terminal details.
- Acknowledge unauthorized terminals.

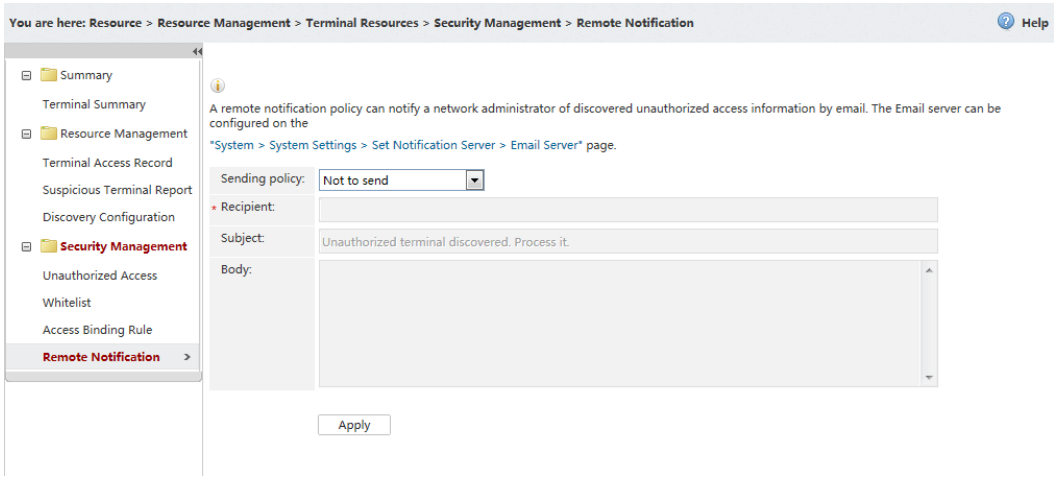
Figure 4-27 Unauthorized Access page



Remote Notification

You can configure eSight to send an email notification upon detecting unauthorized terminal access.

Figure 4-28 Remote Notification page



4.2.1.3 Link Management

A link is a channel that connects signaling points and signaling transfer points and transmits signaling messages. A communication path consists of multiple links. With link management, you can view the link status and maintain network links in a timely manner. Links can be displayed in the topology view. You can learn about the changes in the topology structure on the live network based on the link topology.

Links can be discovered automatically (after devices are added to eSight) or manually.

Link Discovery

eSight supports Link Layer Discovery Protocol (LLDP), Cisco Discovery Protocol (CDP), media access control (MAC), and IP (Side-By-Side) discovery algorithms. LLDP, CDP, and Side-By-Side algorithms support automatic and manual discovery, while MAC supports only manual discovery.

Discovery algorithms have the following restrictions:

- LLDP: LLDP is a public protocol. LLDP-based link discovery supports only LLDP-compliant and LLDP-enabled devices on which the iso view has been configured.
- CDP: CDP is Cisco's proprietary protocol. CDP-based link discovery supports only CDP-enabled Cisco devices.
- MAC: You can use the MAC forwarding table to discover links when devices (including third-party devices) are not LLDP-enabled or CDP-enabled. During MAC-based link discovery, a link must have at least one Layer 2 port.
- IP (Side-By-Side): During IP-based link discovery, IP addresses on the two sides of a link must be 30-bit masks.

The priority of link discovery algorithms (not perceived by users) is as follows in descending order: LLDP, CDP, IP (Side-By-Side), and MAC (for Layer 2 links).

Display Rule

On the display rule page, you can select fields required for link name rules and tips rules. Tips are displayed for links in the topology.

Figure 4-29 Display rule settings

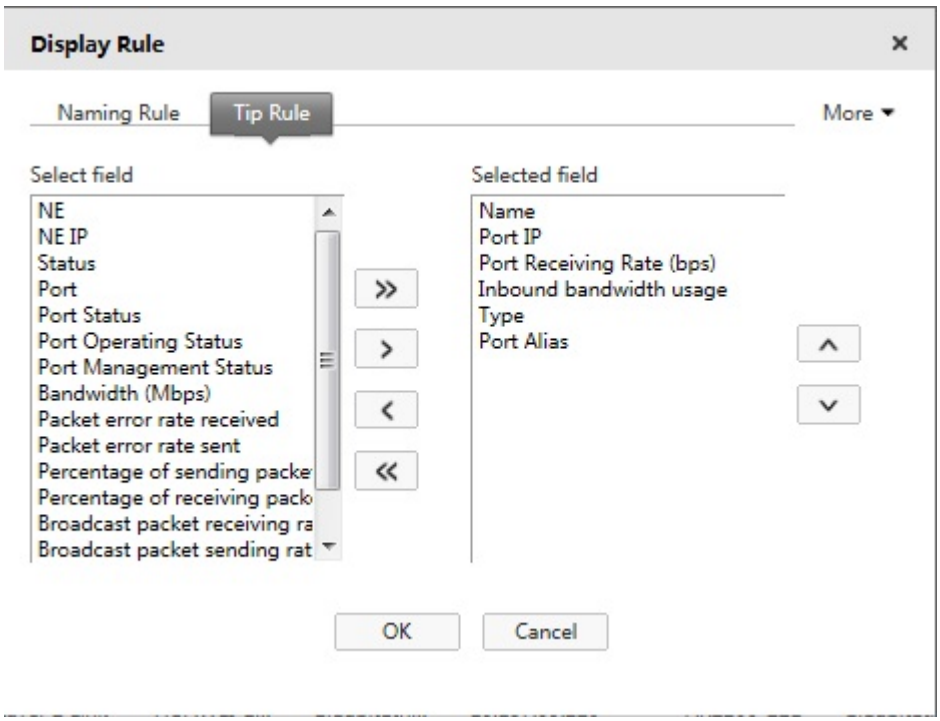
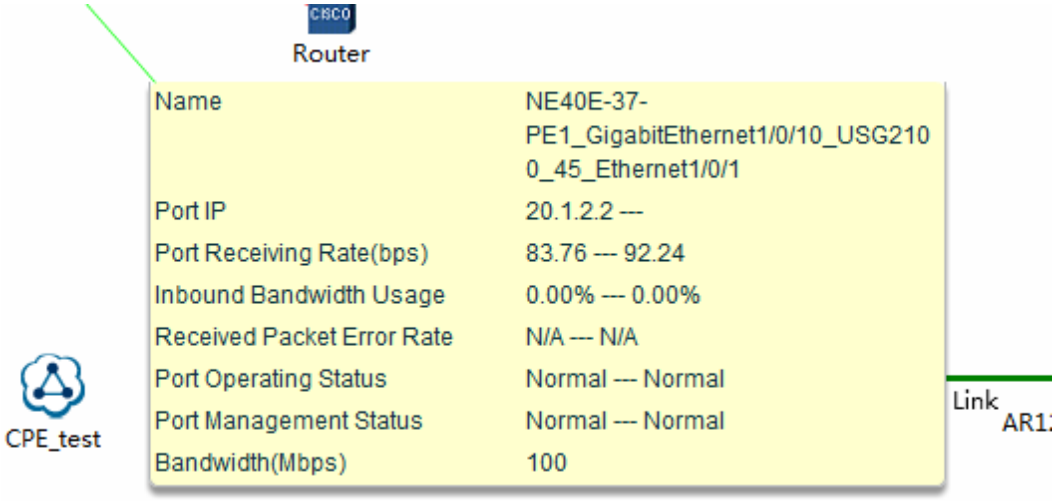


Figure 4-30 Default display effect for link tips



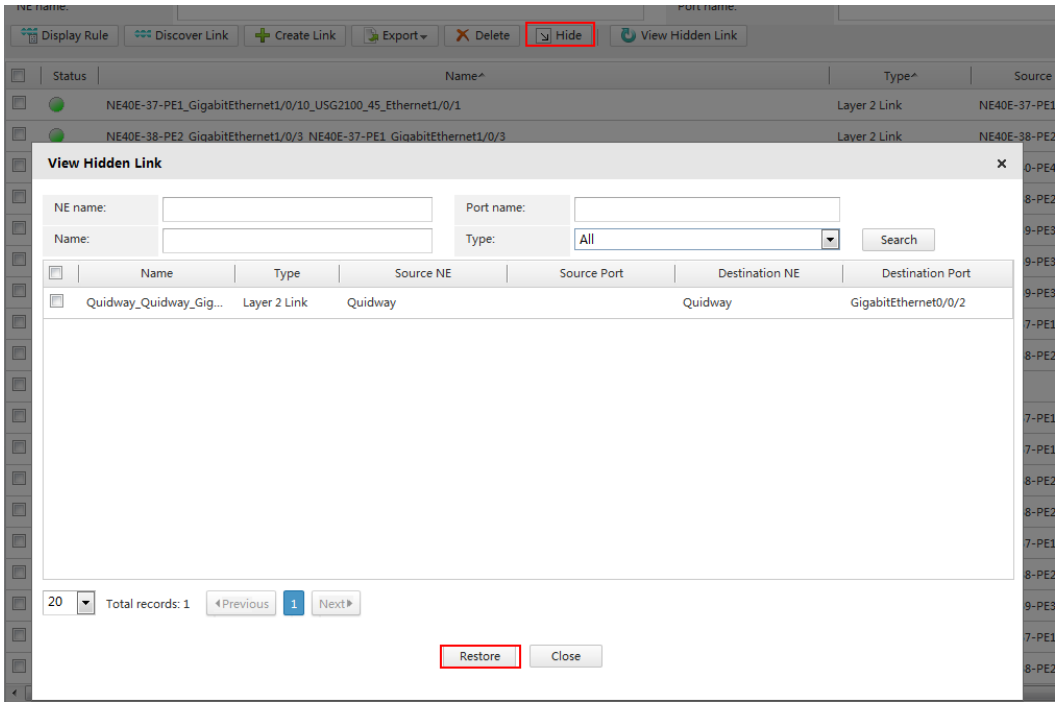
Link Hidden

The link deletion function applies to the following scenarios:

- Users want to hide a link in the physical topology and prevent it from being displayed during automatic and manual discovery.
- An incorrect link exists in the topology and needs to be hidden.

Users can hide a link from the physical topology and link management page. Users can also restore hidden links on the page for viewing hidden links, as shown in the following figure.

Figure 4-31 Restoring Hidden Links



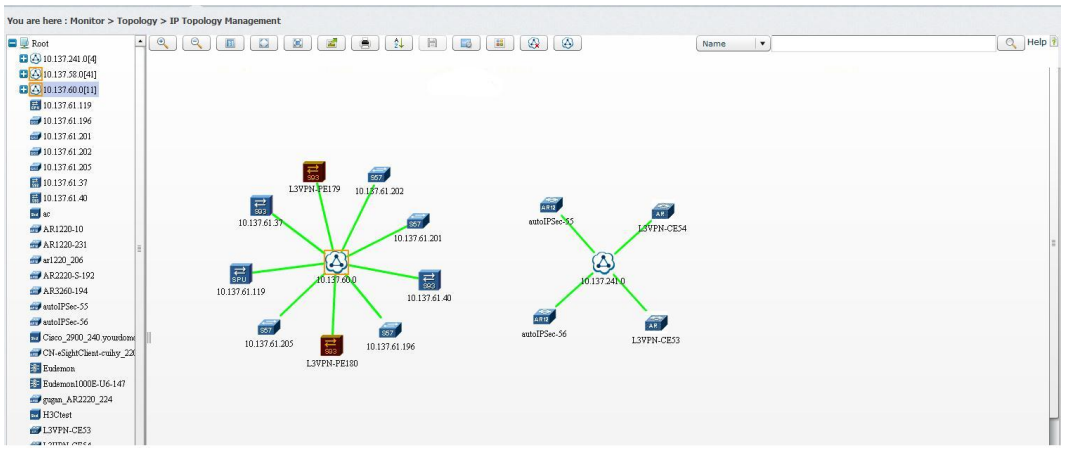
4.2.1.4 IP Topology Management

You can go to the IP topology management page to check the links between routing devices and layer-2 network devices.

Table 4-10 Terms in IP topology management

Term	Description
NE	Core unit of topology management, which is used to identify managed devices. In a topology view, different icons indicate different types of NEs.
IP subnet	IP network subdivision identified by a subnet mask and a range of IP addresses.
Link	Physical or logical connection between devices.
Routing device	Network device with routing capabilities.
Layer-2 device	Network device running on the data link layer of an Open System Interconnection/Reference Model (OSI/RM) network.

Figure 4-32 IP Topology Management page



Topology View

- The IP topology management page offers a tree structure on the left and a topology pane on the right. Topology objects are organized hierarchically by subnet.
- eSight allows you to zoom in or zoom out in a topology view. Meanwhile, an aerial view is provided for you to understand the entire topology structure.
- You can view the alarm status of devices and links. Detailed device or link information is displayed in a tip when you bring focus to the device or link.

Operations in a Topology View

In a topology view, you can:

- Zoom in or zoom out.
- Export and print topology images and set a picture as the background of the topology view.
- Move nodes and save their new positions.
- Use shortcut menus.

Display of Alarm Severities

The color of a node reflects the severity of the most severe alarm that the node is experiencing. Update of such colors is real-time so you can respond to emergencies promptly.

Shortcut Access to NE Management

The topology view offers a shortcut menu for you to access the NE management page.

IP Address Change History

You can view and delete the IP address change history of an NE or the whole network.

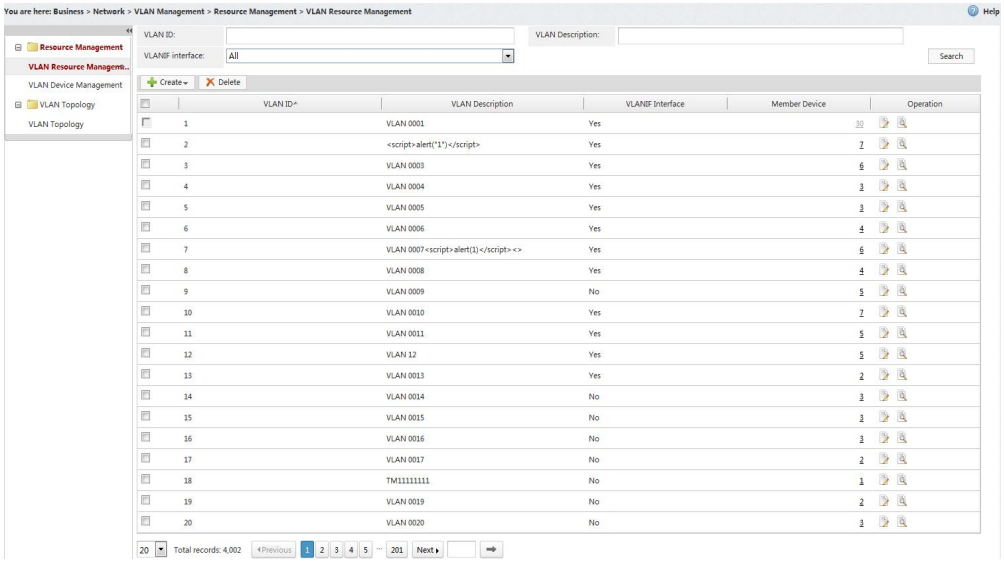
4.2.1.5 VLAN Management

The eSight VLAN Manager centrally manages and configures VLAN resources that have been added to eSight. The eSight VLAN Manager offers an impressive array of functions, including managing network-wide VLAN resources, delivering VLAN configurations to ports on devices (delivering only PVID for Access-type ports; PVID and allowed VLANs for Trunk-type ports; PVID, tagged VLANs, and untagged VLANs for Hybrid-type ports), automatically computing paths to display device and link VLAN topologies, and providing VLAN management for a single device.

VLAN Resource Management

eSight offers a unified entry to manage VLAN resources.

Figure 4-33 VLAN resource management

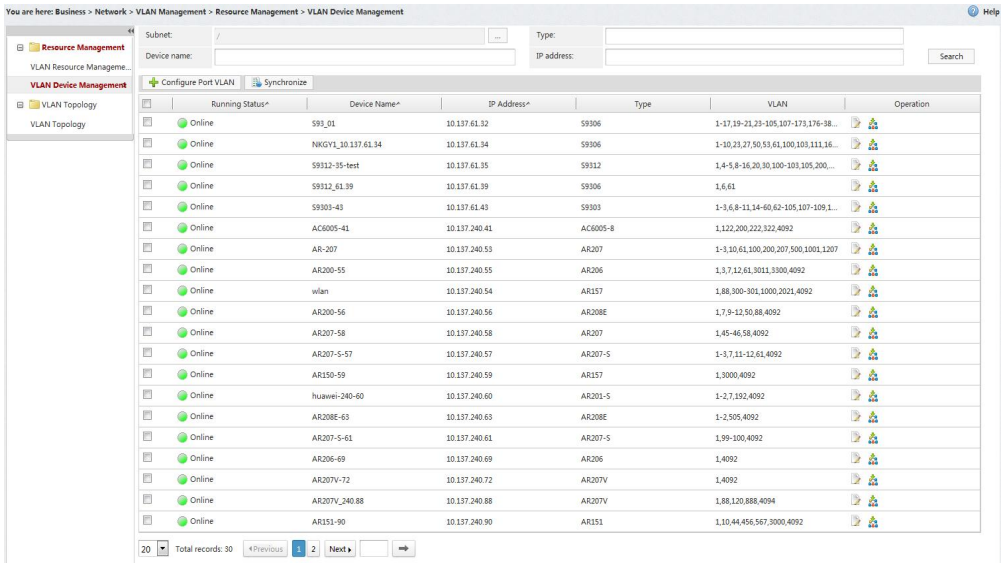


- You can search for VLAN resources by criteria, such as VLAN ID and VLANIF interface existence.
- You can create VLANs in batches and deliver created VLANs to selected devices.
- You can delete VLANs. If the ID of the VLAN is the PVID of a port, the PVID of this port will be restored to 1 after the VLAN is deleted.

VLAN Device Management

eSight offers a unified entry to manage VLAN devices.

Figure 4-34 VLAN device management

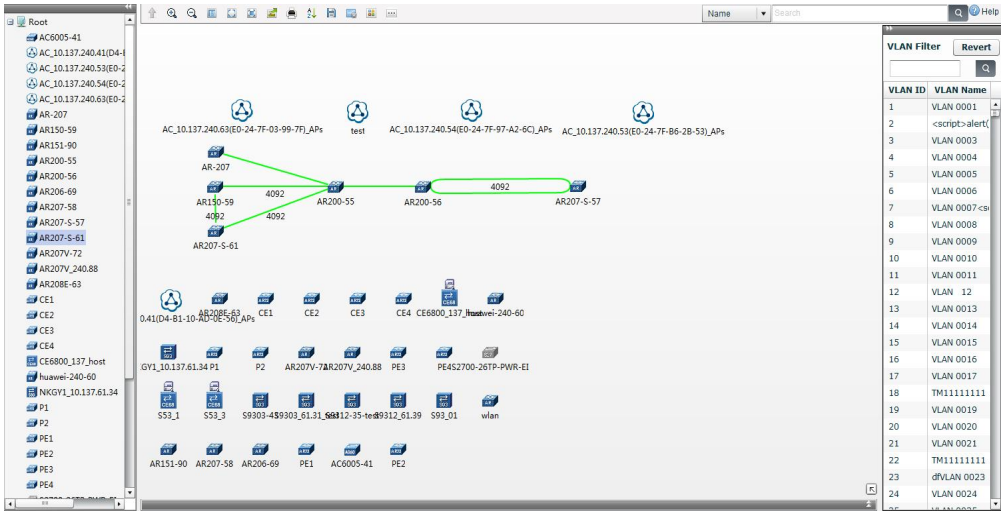


- You can search for VLAN devices by subnet, device type, device name, and device IP address.
- You can configure port VLANs and deliver the configurations to selected ports.
- You can go to the device management page to manage the VLAN of a single device.

VLAN Topology

eSight offers a unified topology view of network-wide VLAN devices and links.

Figure 4-35 VLAN topology

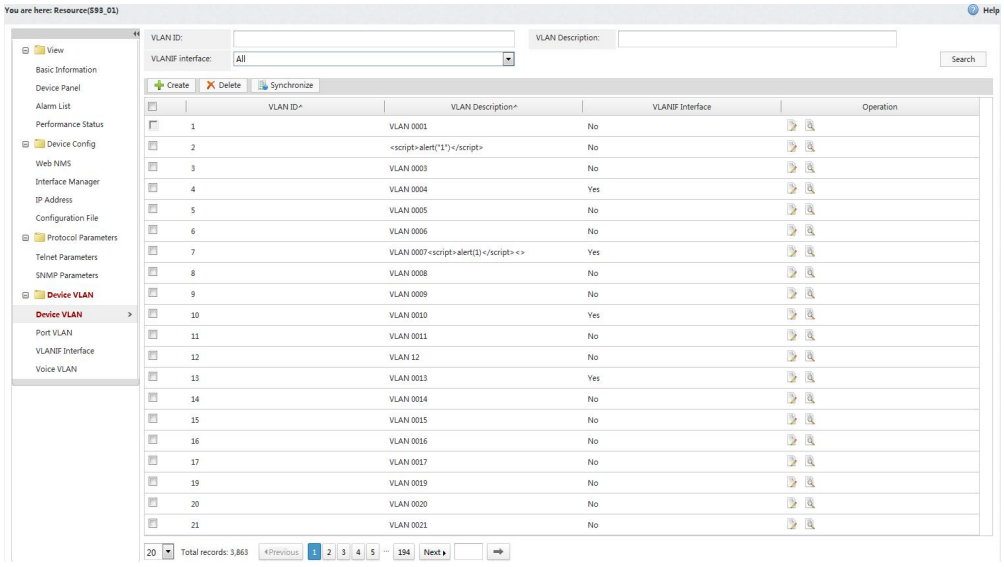


- You can check the device interface types and VLAN details about the two sides of a link, and check VLAN packets that are allowed to pass on the link.
- You can search for devices and links by VLAN ID, and check devices and links that allow the pass of a VLAN.
- You can directly add a device to or remove a device from a VLAN.

Single-Device VLAN Management

You can manage VLAN resources on a single device on the device management page.

Figure 4-36 Single-device VLAN management



- You can create VLANs on and delete VLANs from a single device.
- When you delete a VLAN: If the ID of the VLAN is the PVID of a port, the PVID of this port will be restored to 1 after the VLAN is deleted.

- You can bulk modify VLAN parameters for multiple ports under a device.
- You can create VLANIF on and delete VLANIF from a single device.
- You can manage voice VLANs on a single device and set communication parameters for voice VLANs on the device. the parameters include the lifecycle, protocol priority (802.1P/DSCP), source MAC address and mask for voice streams, and port used to receive voice streams.

4.2.1.6 Smart Configuration Tool

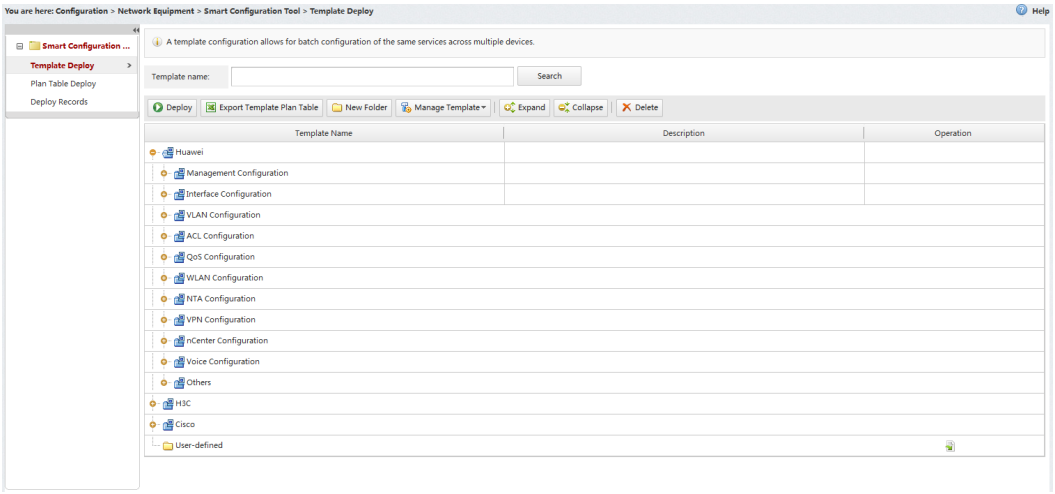
With the smart configuration tool, you can configure services for devices in batches by template and planning table.

A template is used to configure the same services for multiple NEs in batches. A planning table is used to configure similar services for multiple NEs in batches. You can receive task execution results by email for periodical delivery tasks.

Delivering Configurations Using a Template

You can use the preconfigured template or customize a template to deliver configurations to multiple devices. The tool provides a wizard to guide you through the delivery. The tool also allows you to verify the commands in the template.

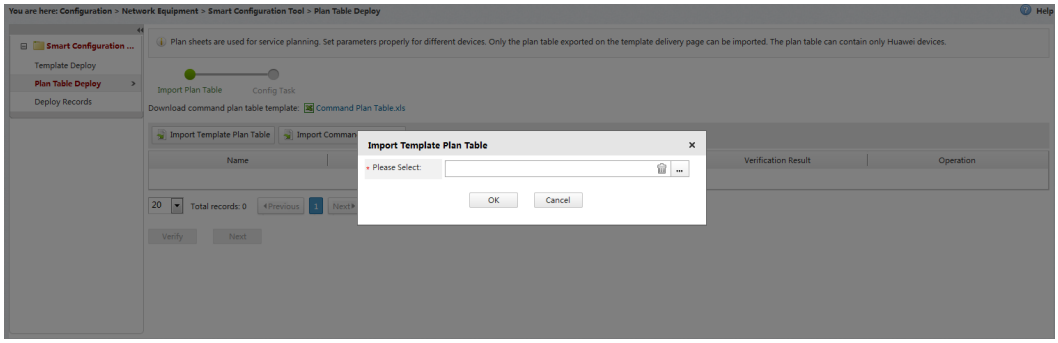
Figure 4-37 Delivering configurations using a template



Delivering Configurations Using a Template Planning Table

To deliver configurations to multiple devices using a template planning table, export the table and enter service configuration parameters in the table. Then import the table to the smart configuration tool. The tool provides a wizard to guide you through the delivery.

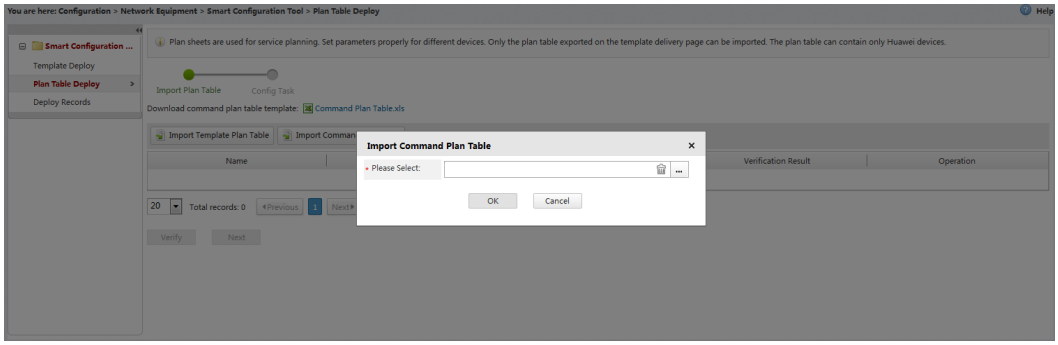
Figure 4-38 Delivering configurations using a template planning table



Delivering Configurations Using a Command Planning Table

To deliver configurations to multiple devices using a command planning table, export the table and enter CLI in the table. Then import the table to the smart configuration tool. The tool provides a wizard to guide you through the delivery.

Figure 4-39 Delivering configurations using a command planning table



4.2.1.7 Configuration File Management

eSight allows you to back up, restore, and compare device configuration files and manage baseline file versions. When faults occur on the network, you can compare the configuration file in use with the configuration file that was saved when the network was running properly. By checking the added, modified, and deleted information, you can quickly locate the fault and resolve it.

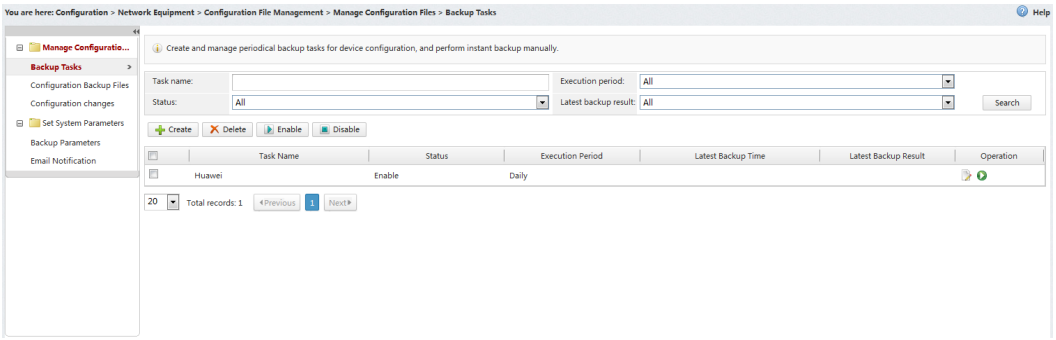
You can also manage configuration changes. eSight automatically compares the differences between backup and original configuration files to obtain configuration changes and notifies you of the changes by email.

Device Configuration Management

- Backup task

  eSight can be configured to periodically (daily, weekly, or monthly) back up configuration files of devices specified in a backup task, at a specified time. It can also be configured to trigger a backup upon the generation of a device configuration change alarm. You can receive backup implementation results by email. The devices that cannot be backed up are listed in the attachment. **Figure 4-40** shows the page for creating a backup task. eSight can also perform instant backups.

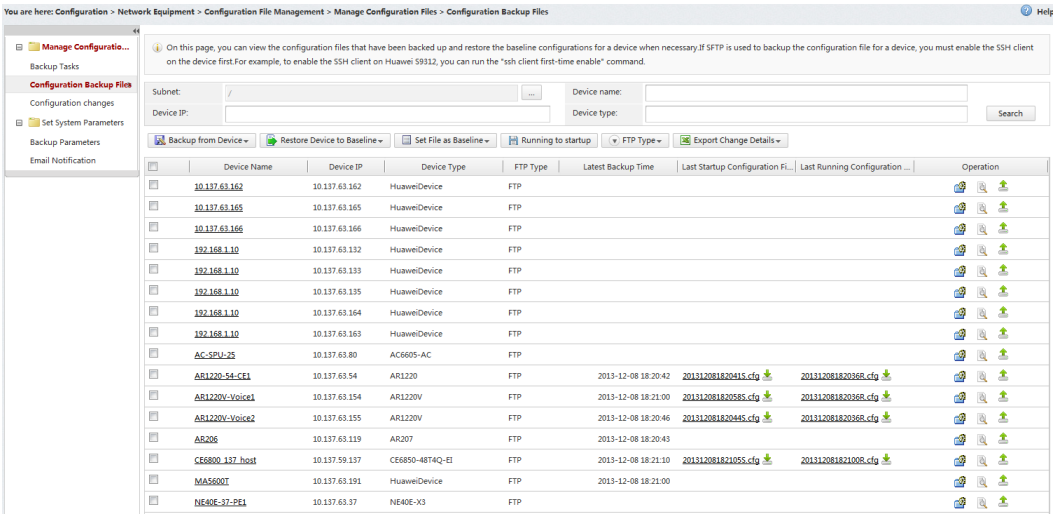
Figure 4-40 Creating a backup task



- Configuration file

  You can back up the configuration file of a specified device, configure a configuration file as a baseline version, use the backup configuration file to replace the existing configuration, and view the configuration on a device, as shown in **Figure 4-41**.

Figure 4-41 Setting a configuration file as a baseline version

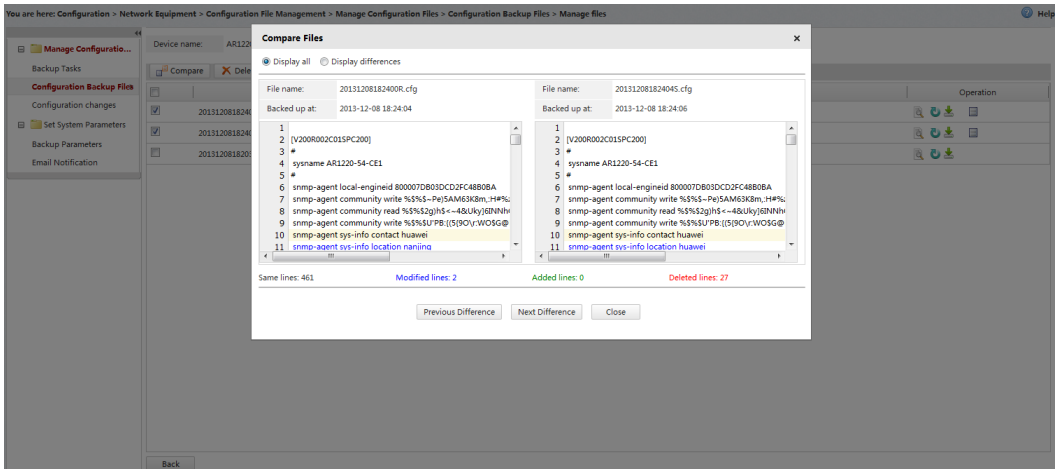


Configuration files that have been backed up to a local disk can be viewed online, as shown in **Figure 4-42**.

Figure 4-42 Viewing a configuration file online

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 server, as shown in **Figure 4-43**.

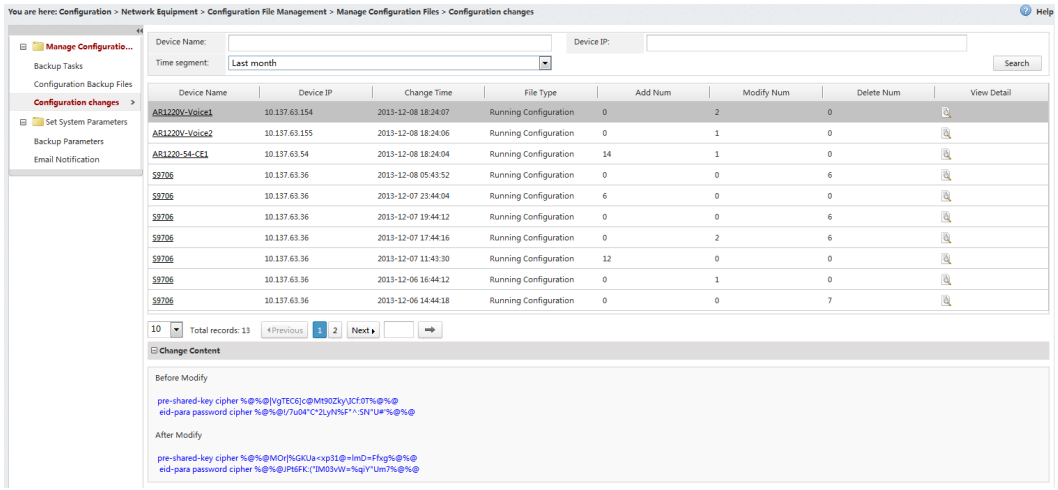
Figure 4-43 Comparing configuration files backed up on the eSight server



- Configuration change

After a configuration file is backed up, eSight automatically compares the differences between backup and original configuration files to obtain configuration changes. On the **Figure 4-44**, you can check the detailed configuration changes, including adds, deletes, and modifies.

Figure 4-44 Configuration change page



System Parameter Management

- Backup parameter

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

  You can determine whether to trigger a backup upon device configuration changes.

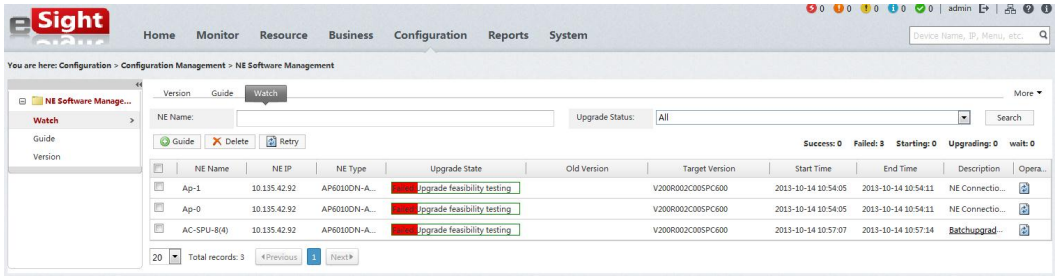
4.2.1.8 NE Software Management

NE software management is a functional module used to upgrade software versions of managed devices. Users can upgrade software versions of fit APs using ACs. This module offers task monitoring, wizard-based upgrade, and version management functions. The task monitoring submodule manages all device upgrade tasks and refreshes the upgrade task in real time. The wizard-based upgrade allows users to create upgrade tasks following a wizard. The version management submodule allows users to manage device software mapping files by device type.

Task Monitoring

The task monitoring submodule manages all device upgrade tasks and refreshes the upgrade task in real time.

Figure 4-45 Task Monitoring

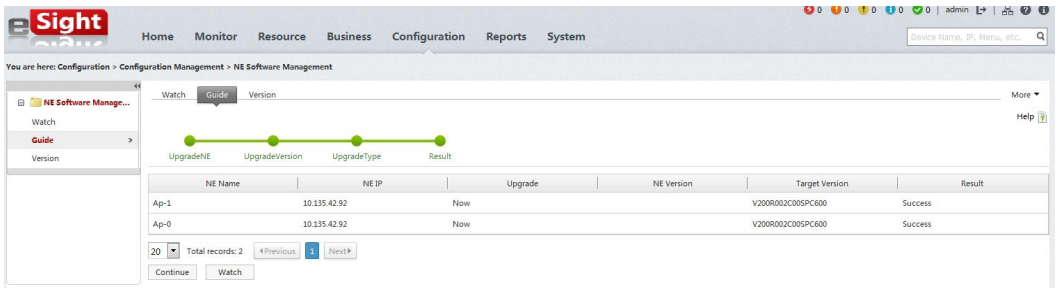


- The current version supports software upgrade of fit APs and displays the main menu and authentication processing when the WLAN service component is installed.
- Users can upgrade one or more fit APs. If selected fit APs are of the same type and belong to the same AC, only one task is created, improving efficiency and reducing the load of Telnet connection channels.
- The status of upgrade tasks is refreshed in real time. Users can re-execute failed tasks.

Wizard-based Upgrade

The wizard-based upgrade allows users to create upgrade tasks following a wizard.

Figure 4-46 Wizard-based Upgrade



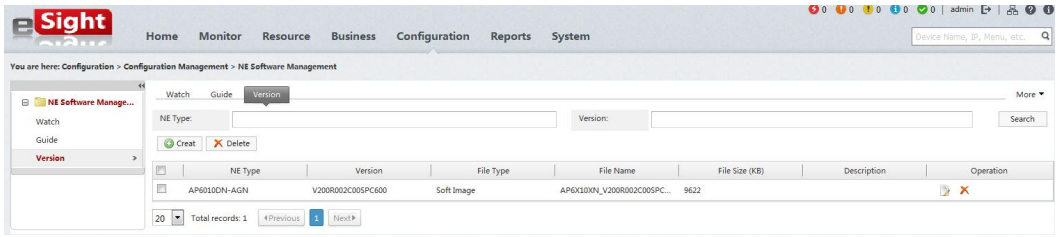
- The three-step wizard allows users to create upgrade tasks and check task summary information.

- Users can continue to create upgrade tasks or go to the task monitoring page to check task execution information.
- At the step for selecting an upgrade version, a link for creating a version is added, increasing the ease of operations.

Version Management

The version management submodule allows users to manage device software mapping files by device type.

Figure 4-47 Version Management



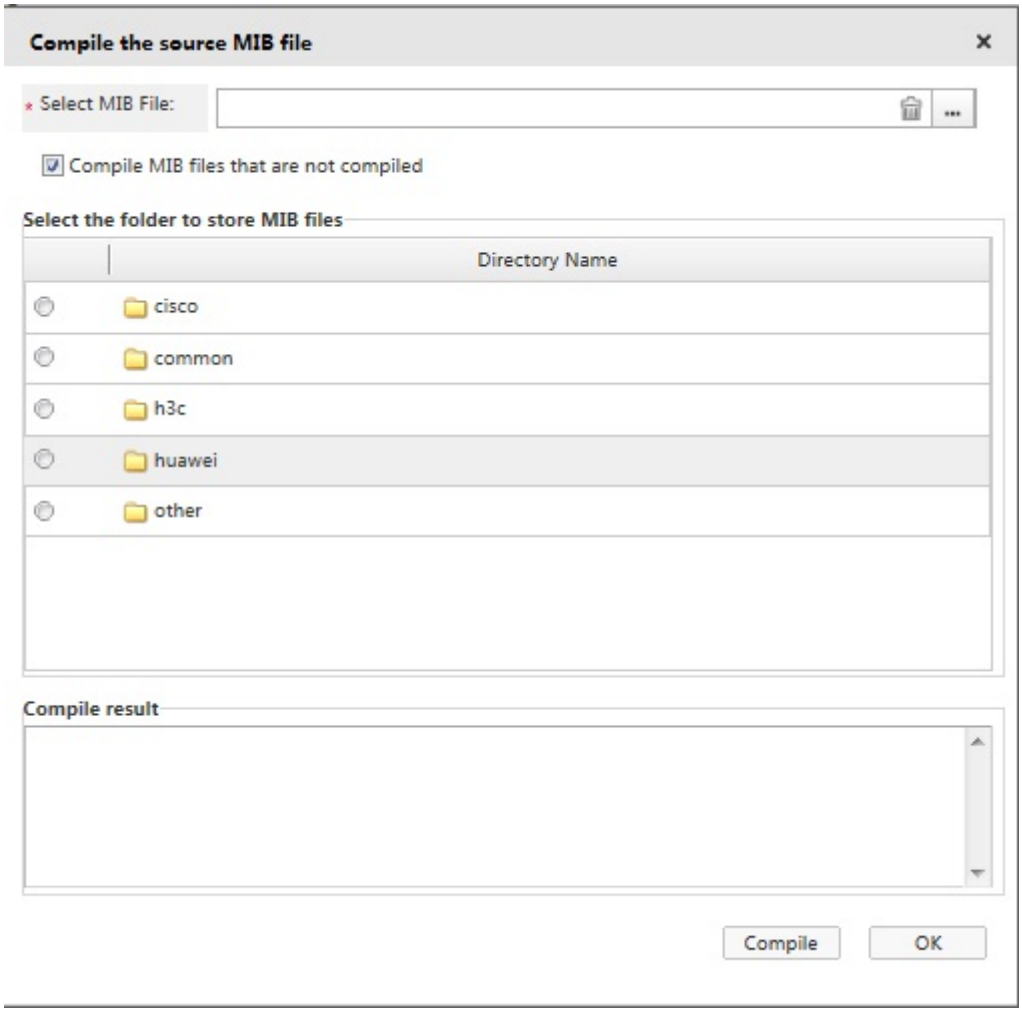
4.2.1.9 MIB Management

eSight offers the management information base (MIB) tool that can read, compile, store, and use .mib files. eSight reads and monitors MIB data through SNMP V1, V2c, or V3, which helps you to perform effective network management.

MIB Compiling

You can compile a MIB file and store the compiled file to a specified directory.

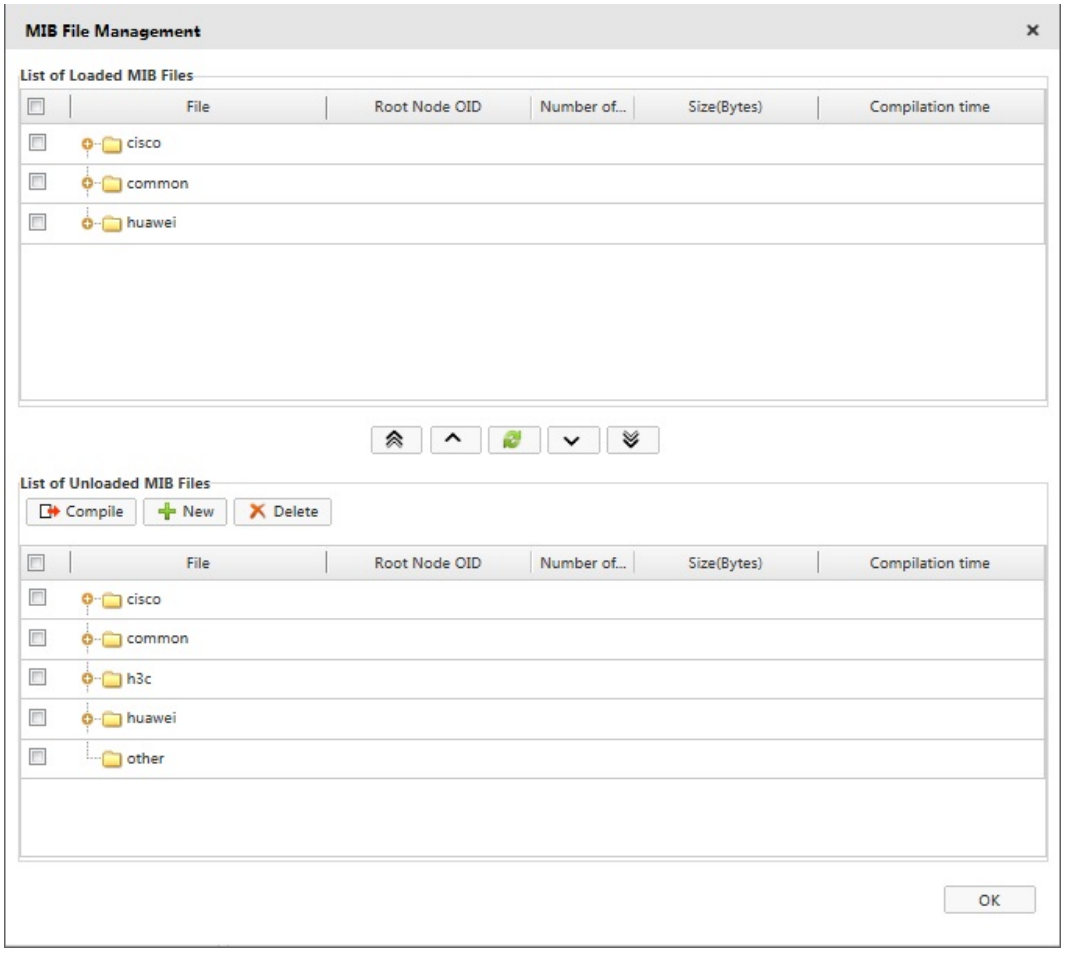
Figure 4-48 MIB compiling page



MIB Loading

You can upload, compile, load, unload, and delete MIB nodes, and create directories for MIB nodes.

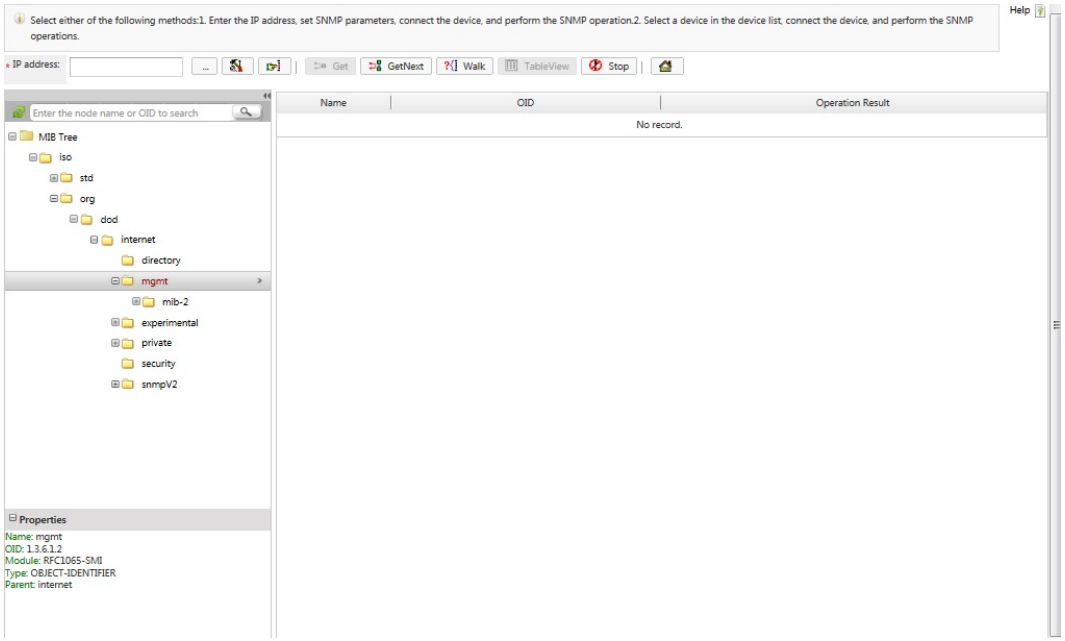
Figure 4-49 MIB loading page



MIB Operation

After you enter device IP addresses in IP address text boxes, you can use the MIB tool to perform Get/GetNext/Walk/TableView operations over SNMP-compliant devices.You can click **Stop**to stop data acquisition.

Figure 4-50 MIB operation page



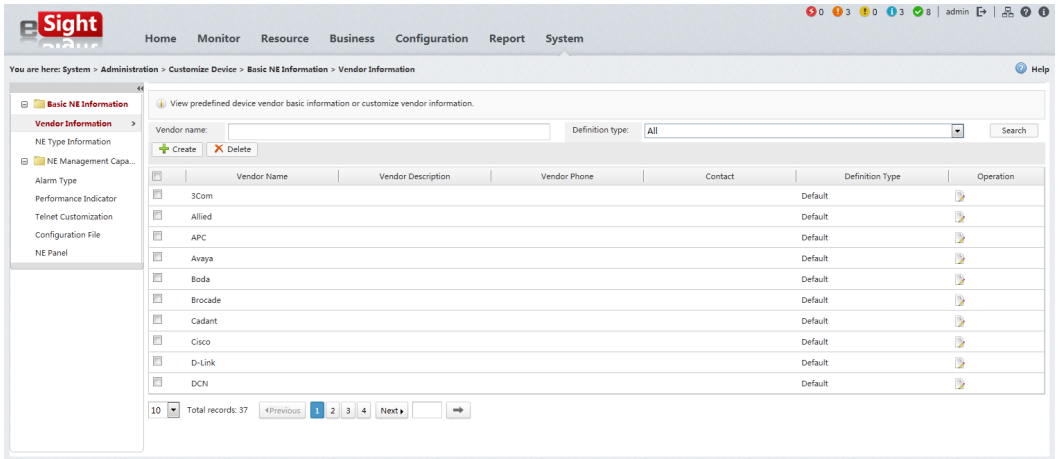
4.2.1.10 User-defined Device Management

eSight provides user-defined device management to help enterprise users manage devices from different vendors. You can customize device types, performance counters, alarm parameters, configuration file parameters, and device panels.

Vendor Information Customization

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

Figure 4-51 Customizing vendor information



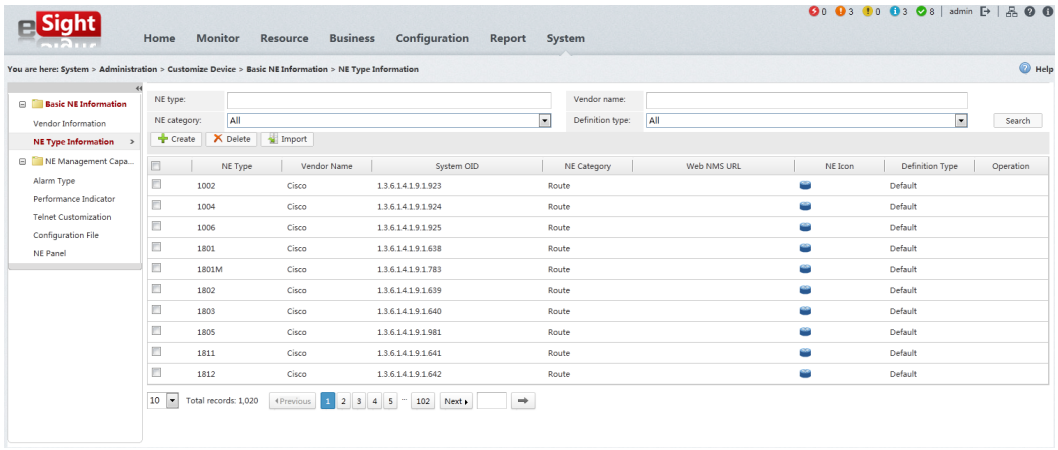
In the preceding figure:

- **Vendor Name**: name of a device manufacturer.
- **Vendor Description**: description of a device manufacturer. This parameter is optional.
- **Vendor Phone**: customer service phone number of a device manufacturer. This parameter is optional.
- **Vendor Contact**: device maintenance personnel of a device manufacturer. This parameter is optional.
- **Definition Type**: indicates whether the basic information about a device manufacturer is customized by eSight developers or users. The options are as follows: **Default**: The basic information is customized by eSight developers. **User-defined**: The basic information is customized by users.

NE Type Customization

When a non-predefined device type is added to eSight, the device type is shown as **unknown**. eSight allows you to view only basic information about unknown devices. Management capabilities, for example, alarm functions, are not provided. You must customize the device type so that eSight can display the device information and monitor alarms and performance counters of the device.

Figure 4-52 Customizing the NE type



In the preceding figure:

- **NE OID**: NE type identifier.
- **NE Category**: category of an NE, for example, switch, router, server, printer, or security device.
- **Web NMS URL**: URL of a web-based network management system (NMS). Some devices have their own web-based NMSs. After adding the link to a device's web-based NMS in eSight, you can click the link to access the web-based NMS.
- **Current NE Icon**: device type, which can be customized by users.
- **Definition Type**: indicates whether device information is customized by eSight developers or users.

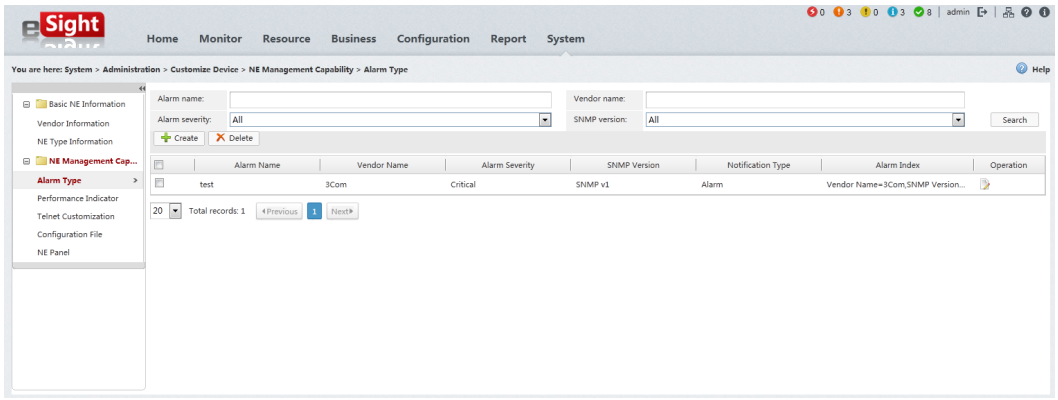
Alarm Parameter Customization

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

When you delete a user-defined alarm's parameters, eSight does not delete the alarm's historical information. eSight's alarm module, however, no longer parses or displays the alarm.

eSight allows you to modify the alarm severity, event type, alarm cause, handling method, details, and fault locating parameters.

Figure 4-53 Customizing alarm parameters



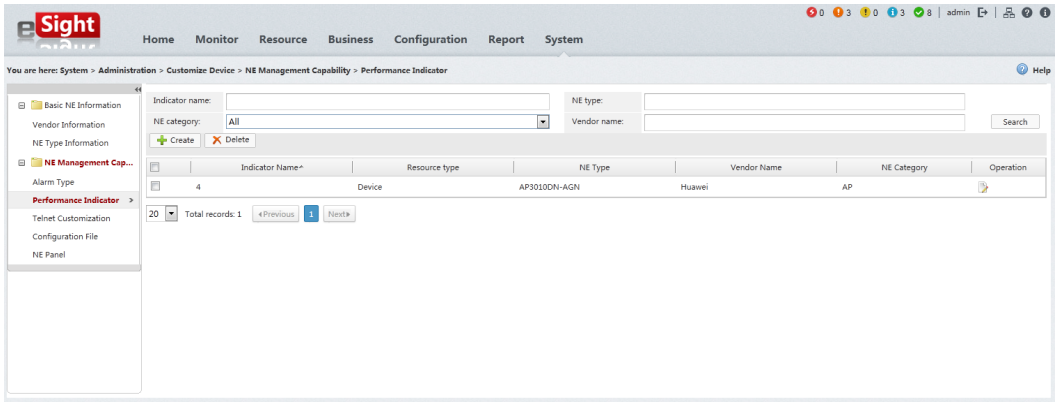
In the preceding figure:

- **Vendor Name**: name of a device manufacturer. Alarm customization varies according to device manufacturer because the alarm parameters differ depending on the device manufacturer.
- **Alarm Name**: name of an alarm.
- **Alarm Severity**: severity of an alarm. There are four alarm severities: warning, minor, major, and critical. They are the same as those defined in the alarm module.
- **Notification Type**: alarm category. There are three alarm categories: clear alarm, fault alarm, and event.
- **Event type**: alarm type. The following alarms are available: communications alarm, equipment alarm, processing error alarm, QoS alarm, environmental alarm, integrity alarm, operational alarm, physical resource alarm, and security alarm.
- **SNMP Version**: SNMP version supported by a device. eSight 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**: indicates alarm details.
- **New Parameter**: parameter for locating the fault that causes an alarm.

Performance Indicator Customization

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. The performance management module then collects the user-defined performance counters in the next data collection period.

Figure 4-54 Customizing performance indicators



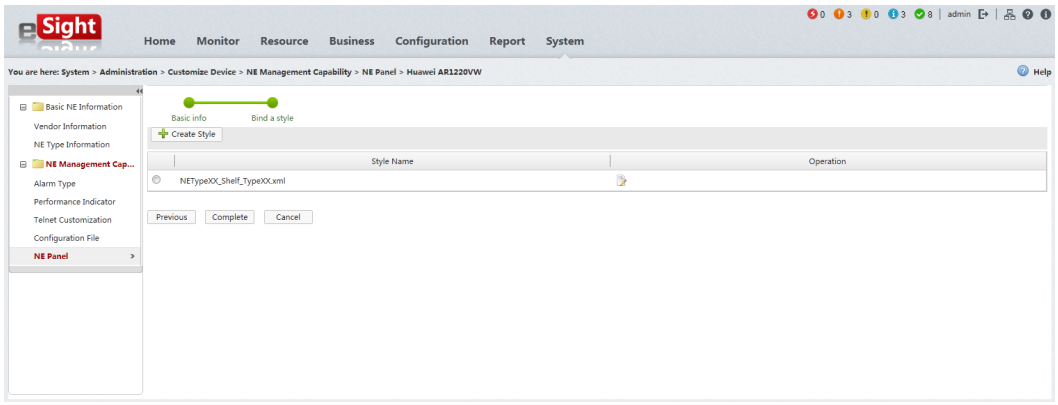
In the preceding figure:

- **Indicator Name**: name of a performance counter whose data needs to be collected.
- **Measurement Object Type**: group of collected performance counters whose data collection objects are the same, for example, user-defined device counter group, frame counter group, board counter group, and interface counter group. To collect a user-defined interface performance counter, select the user-defined interface counter group.
- **NE Type**: type of devices whose user-defined performance counters can be collected.
- **Calculation Formula**: expression for calculating performance counters for an MIB object.

NE Panel Customization

By default, eSight displays default NE panels for user-defined devices. You can upload a device photo or high-fidelity picture to customize the NE panel. An NE panel includes information about the frame, board, subcard, and ports. After customization, the device photo or high-fidelity picture is displayed when you open the NE panel.

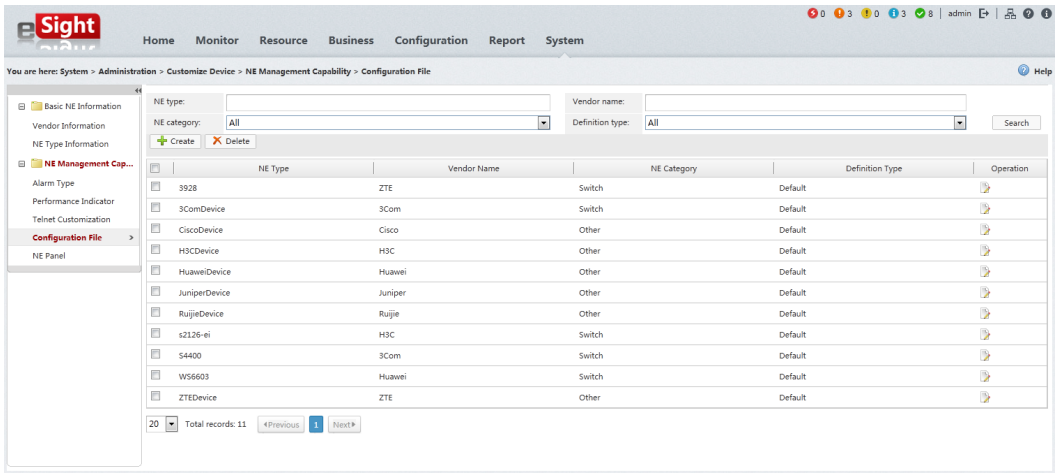
Figure 4-55 Customizing the NE panel



Configuration File Customization

You can customize configuration file backup, configuration file restoration, and restart commands for devices. After customizing a device's configuration file, you can create a backup task for the device in the configuration file management module. eSight then automatically backs up the device's configuration file.

Figure 4-56 Customizing the configuration file



In the preceding figure:

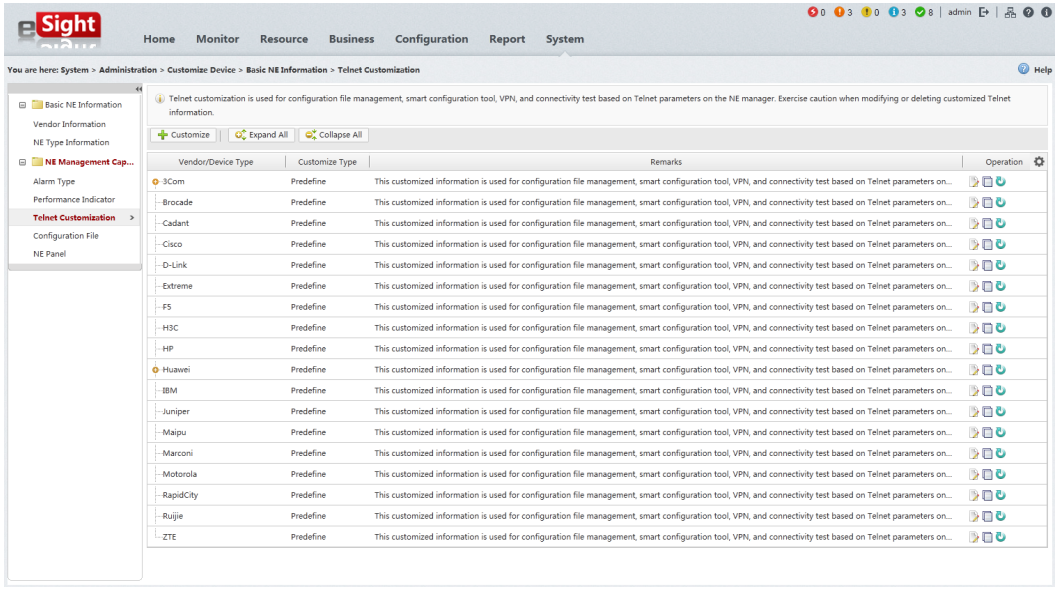
- **NE Type**: type of devices whose configuration file commands must be customized.
- **Backup command**: command for backing up a device's configuration file.
- **Restore command**: command for restoring a device's configuration file.
- **Restart command**: command for restarting a device.

Telnet Customization

With Telnet customization, you can customize Telnet parameters for different device types. Telnet parameters include basic Telnet information and privilege mode information. Basic Telnet information include prompts for the login user name and password, login failure, and command delivery; exit commands; and remarks. Privilege mode information include privilege commands, privilege password prompts, More prompts, output control commands, interactive selection prompts, interactive selection commands, failure prompts, and failure troubleshooting.

After Telnet parameters are customized, you can test the Telnet connectivity to devices. The system can read customized Telnet parameters to manage and back up configuration files, deliver configuration commands through the smart configuration tool, and configure and parse services, including VPN services.

Figure 4-57 Telnet customization



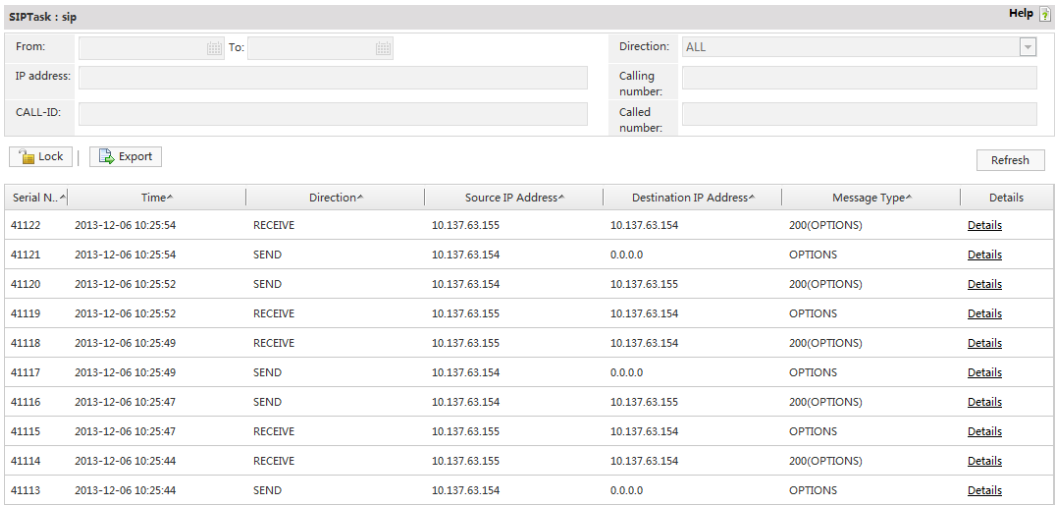
4.2.1.11 AR Voice Management

eSight offers the following AR voice functions: signaling tracing, trunk tracing, call traffic statistics, user resource statistics, and automatic NE connection.

Signaling Tracing

Signaling tracing is used to trace and monitor the protocol messages, connection of port signaling links, and service flows dynamically and in real time. With signaling tracing, users can know the signaling cooperation, facilitating fault location.

Figure 4-58 Signaling tracing



Trunk Tracing

With trunk tracing, users can learn about trunk information in real time.

Call Traffic Statistics

With call traffic statistics, users can collect traffic information about global, trunk incoming, and trunk outgoing calls placed through ARs.

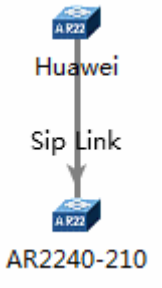
User Resources Statistics

With user resources statistics, users can learn about the number of callers, total users, and call rate in real time to facilitate AR management.

Automatic NE Connection

With this function, eSight automatically creates NE connections in the topology.

Figure 4-59 Automatic NE connection

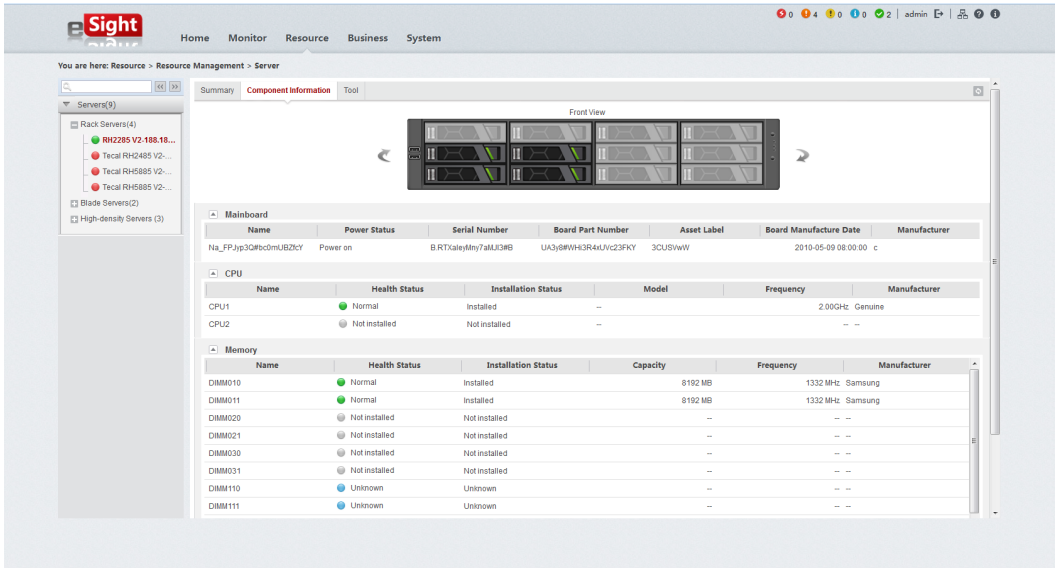


4.2.2 Server Management

eSight offers the following server management functions: centralized server fault monitoring, performance analysis, KVM, integrated virtual media tool. These functions greatly improve O&M efficiency while reducing costs.

Basic Server Information

Figure 4-60 Basic server information

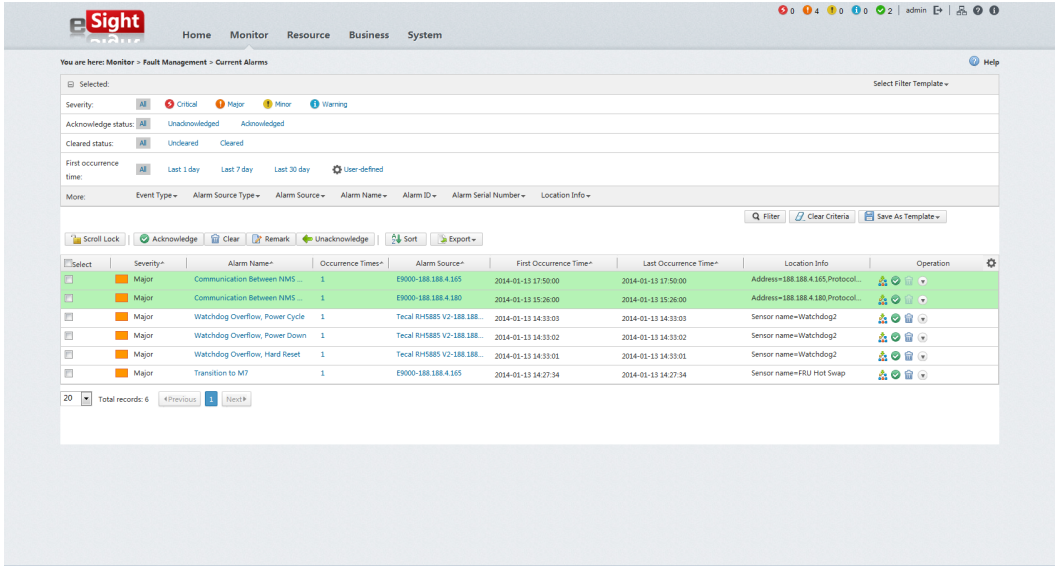


- Overview
  - Displays basic server information and health status.
- Component information
  - Displays basic component information and health status.
  - The device view visually displays server rack graphs and displays basic server information and health status.
- Tool
  - Tools offer KVM and virtual media functions.

Alarm Monitoring

Alarms can be forwarded through emails and repeated alarms can be consolidated.

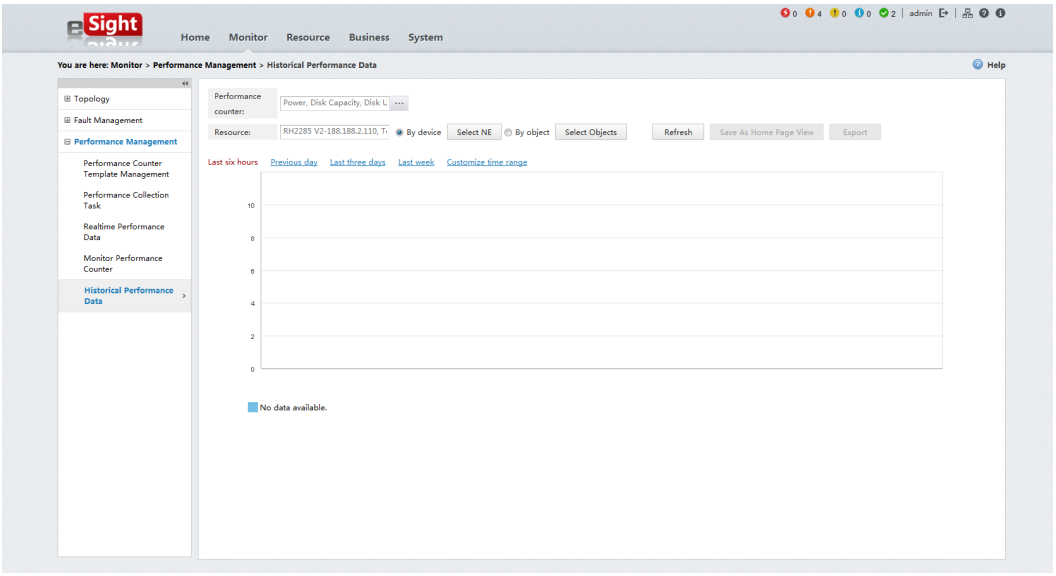
Figure 4-61 Alarm monitoring



Performance Analysis

eSight analyzes the following performance counters: network port performance, server power consumption, CPU usage, and memory usage. Users can create analysis tasks to analyze performance counters within a specific time segment.

Figure 4-62 Performance analysis



4.2.3 Host Management

eSight supports operating system statistics. Users can manage (query and delete) operating systems based on the site requirements.

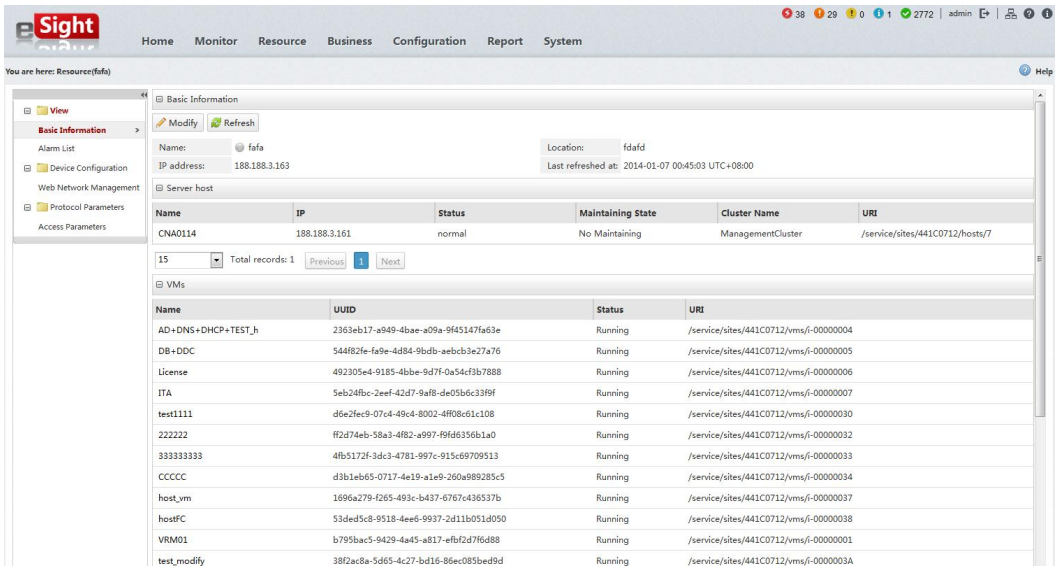
4.2.4 Computing Virtualization Management

Computing virtualization management implements virtual resource monitoring and management, including resource discovery, alarm, and topology. The current eSight version supports monitoring and management of FusionCompute and FusionAccess.

Virtual Resource Management

eSight provides basic management of virtual resources. It integrates the information and maintenance entries of a virtual resource into a page, facilitating monitoring and maintenance of a single network element (NE).

Figure 4-63 NE manager



- View
  - Basic information: displays basic virtual resource information, such as the name, IP address, and location of virtual resources and the latest update time.
  - Physical server information: displays basic information about physical servers, such as the name, IP address, running state, maintenance state, cluster name, and uniform resource identifier (URI) of servers. eSight supports only the monitoring of FusionCompute physical servers.
  - Virtual machine (VM) information: displays basic VM information, such as the name, universally unique identifier (UUID), status, and URI of VMs.
  - Alarm list: displays the active alarms of virtual resources.
- Configuration
  - Web network management: allows you to configure virtual resources on the web management page.
- Protocol parameters
  - Protocol parameter setting: allows you to set and modify protocol parameters for virtual resources.

4.2.5 Storage Device Management

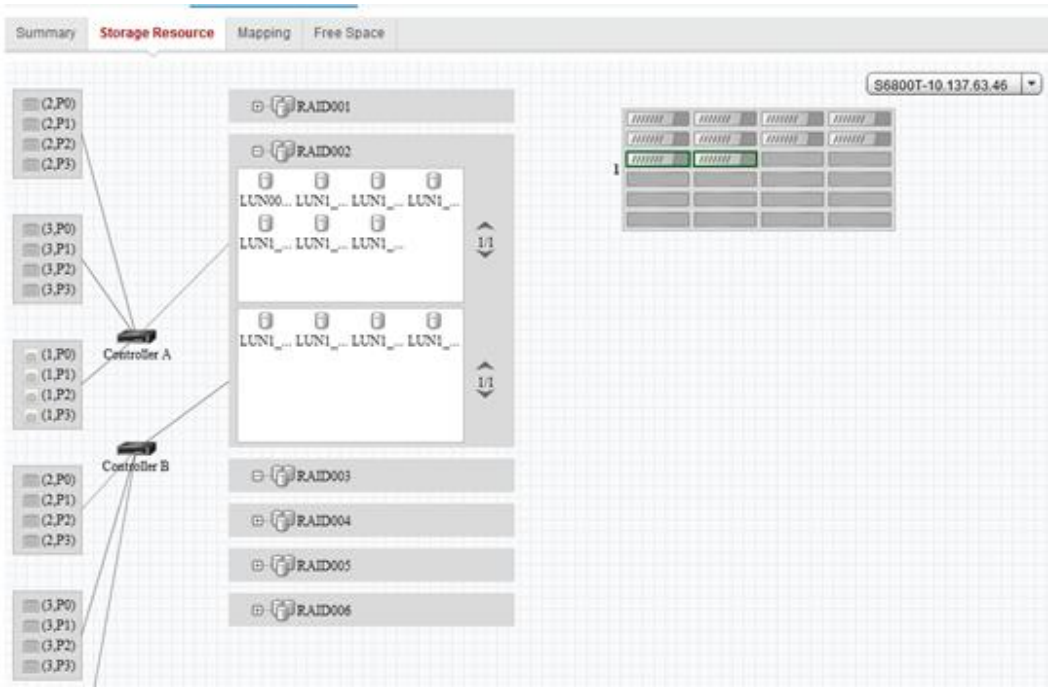
The eSight provides unified management for devices of multiple types and vendors in a graphic manner, improving O&M efficiency and lowering technical requirements for O&M personnel.

Internal Components Management of Storage System

Provides an intuitive view of mappings among physical and logical components of the storage system. On the view, the device status is clear, facilitating fault locating and service recovery.

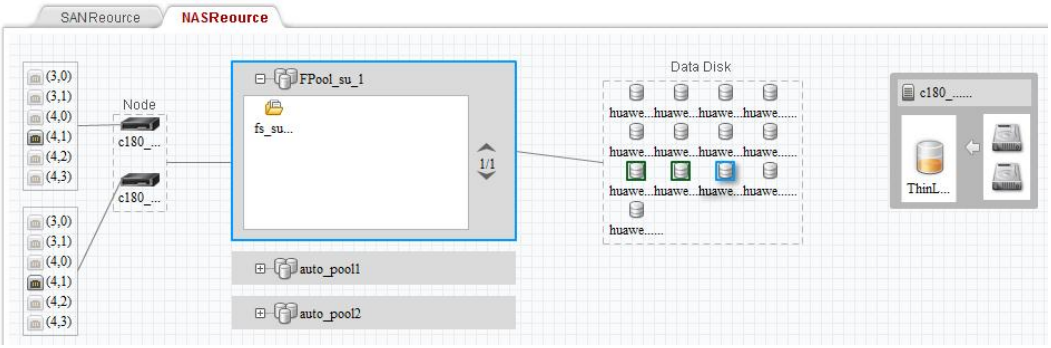
- Block storage: logical relationship between front-end ports, controllers, RAID groups, LUNs, and disks

Figure 4-64 Logical relationship (block storage)



- File storage: Shows logical mappings among front-end ports of NAS engines, NAS engine nodes, file storage pools, data disks, and LUNs and disks of storage units.

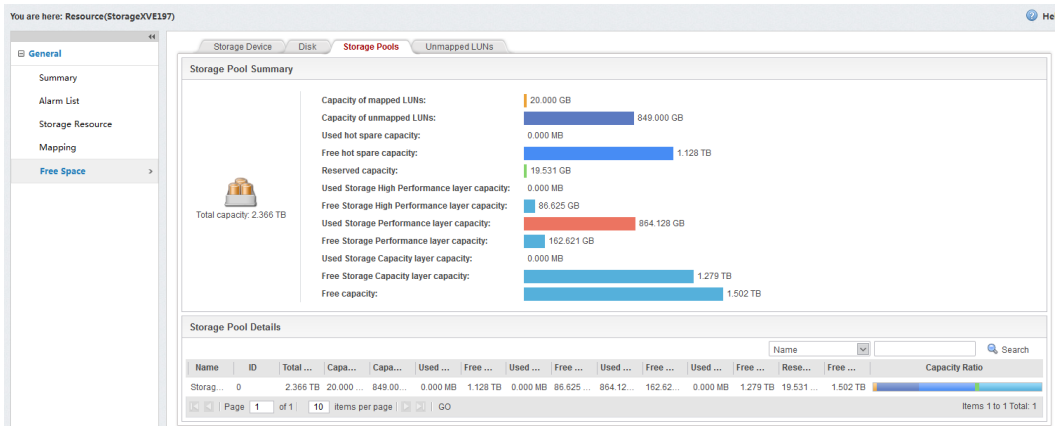
Figure 4-65 Logical Relationship (file storage)



Capacity Usage Management of Storage Systems

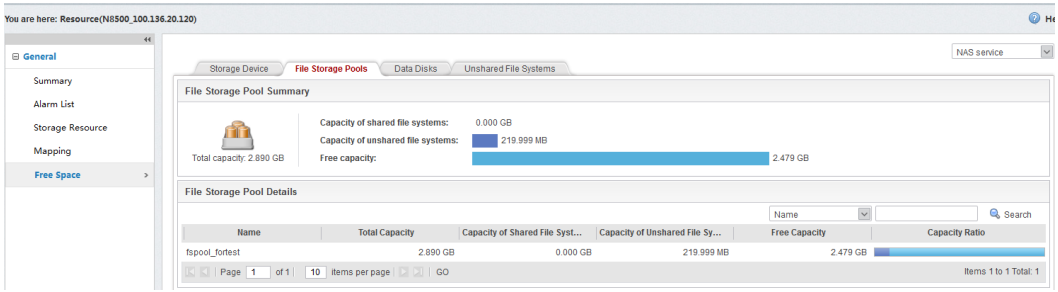
- Block storage: capacity usage management of storage devices, disks, block storage pools, and unmapped LUNs

Figure 4-66 Capacity usage management (block storage)



- File storage: capacity usage management of storage devices, file storage pools, data disks, and unshared file systems

Figure 4-67 Capacity usage management (file storage)



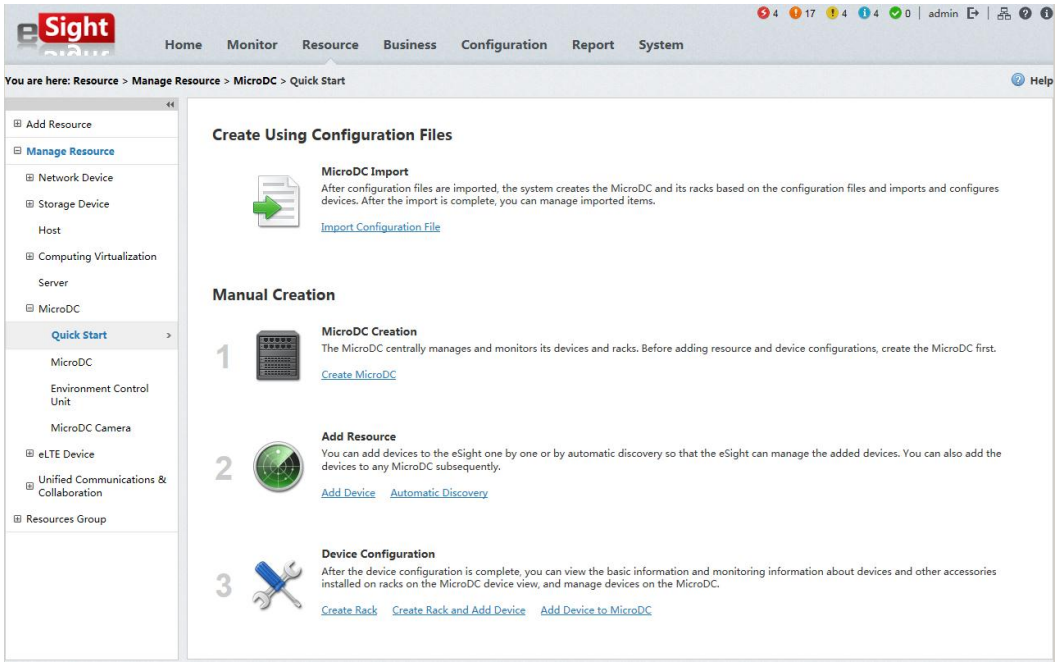
4.2.6 MicroDC Management

MicroDC management implements centralized monitoring and management of Huawei micro data centers. MicroDC management includes Quick Start, unified NE management, physical topology, batch import, and L1 resource management. eSight provides a unified interface to manage different types of L1 and L2 devices, increasing the operation and maintenance (O&M) efficiency and reducing technical requirements for O&M personnel.

Quick Start

Quick Start guides you through the configuration of MicroDC racks and devices. You can perform data configuration step by step or import a configuration file. With Quick Start, you can quickly complete MicroDC configuration and maintenance.

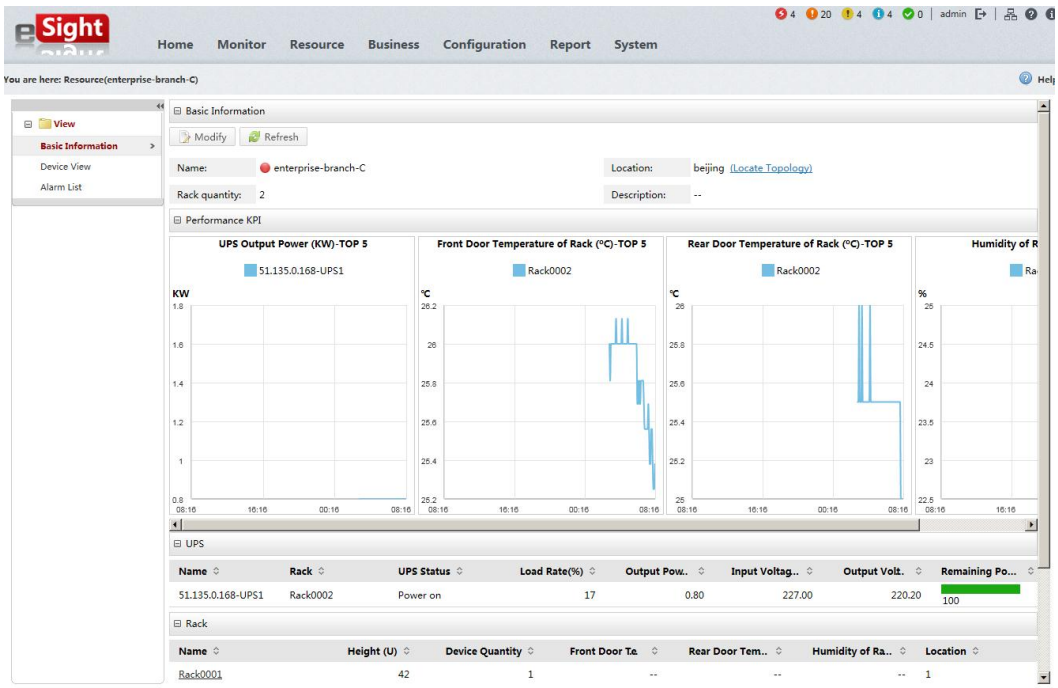
Figure 4-68 eSight Quick Start



Unified NE Management

eSight provides a unified interface to implement monitoring and maintenance of the MicroDC.

Figure 4-69 MicroDC NE manager



- View

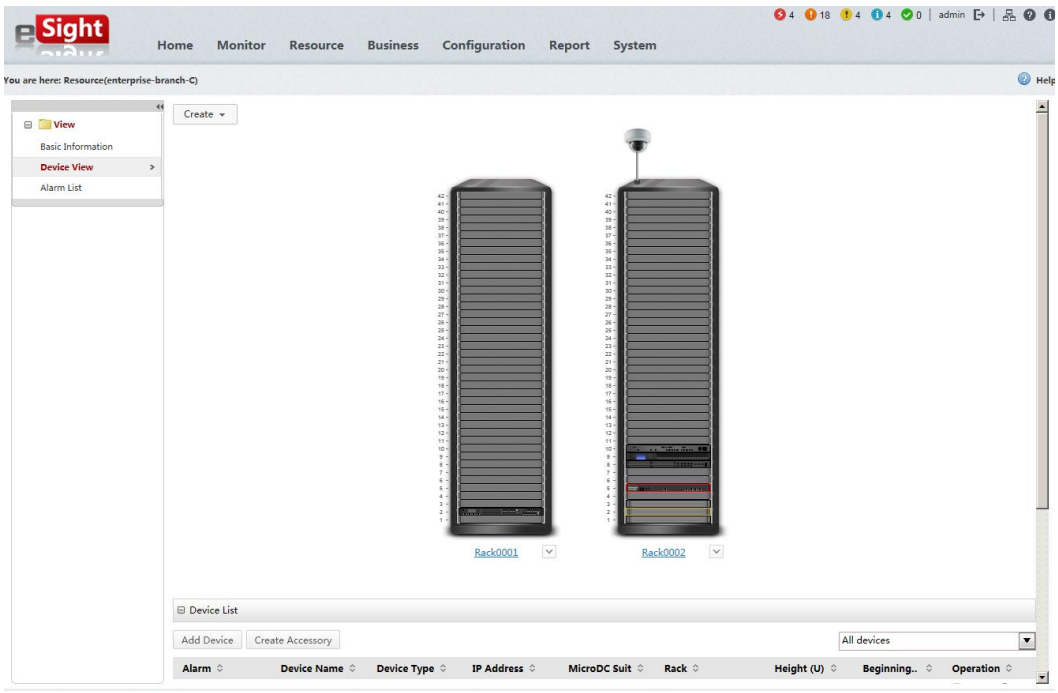
- Basic information: provides the basic MicroDC information, uninterruptible power supply (UPS) list, rack list, and the last 10 active alarms.
- Performance measurement: provides information about the top 5 racks sorted by front door temperature, rear door temperature, and humidity respectively, and top 5 UPSs sorted by power consumption.
- Alarm list: displays the active alarms of all NEs in the MicroDC.

- Device topology
  - eSight provides an intuitive view of MicroDC racks and implements configuration and management of the racks.

Physical Topology

eSight provides an intuitive view of MicroDC racks and implements configuration and management of the racks. You can also view alarms of racks and devices on this device topology. The intuitive device topology simplifies O&M operations and increases the O&M efficiency.

Figure 4-70 MicroDC device view



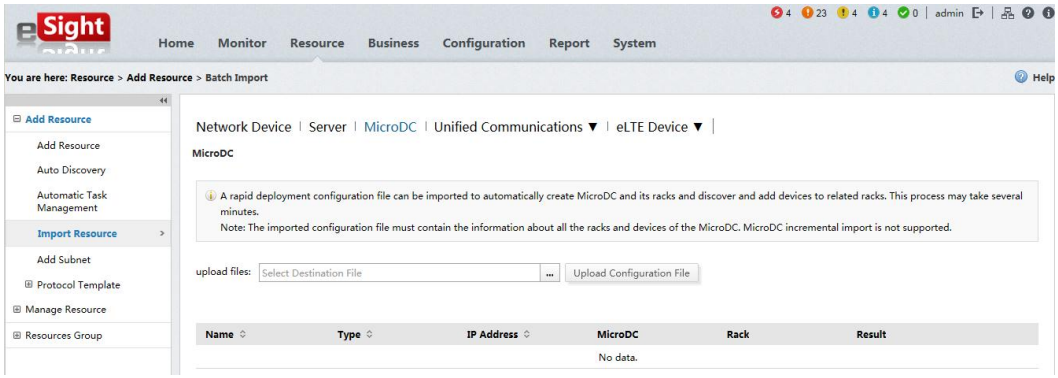
- Monitoring
  - Device presentation: displays all MicroDC devices and rack locations visually.
  - Alarm monitoring: displays alarms of devices in different colors.
  - Video monitoring: provides web network management links through the camera icons on the device topology. You can view video monitoring information in real time or replay the video monitoring information.
- Management
  - Rack configuration: allows you to add or delete a rack and provides a configuration wizard to help you add racks and devices.

- Device configuration: allows you to install, uninstall, or remove devices.
- Accessory configuration: allows you to install, uninstall, or remove accessories. MicroDC accessories include the battery pack, power distribution box (PDB), and UPS.

Batch Import

eSight provides the batch import function, which allows you to import the MicroDC rack and device configuration information. After the configuration information is imported, the system automatically creates a MicroDC, adds racks and devices to the MicroDC, and generates a device topology. With the batch import function, you can deploy the MicroDC by simply clicking the mouse. This function greatly increases the deployment efficiency.

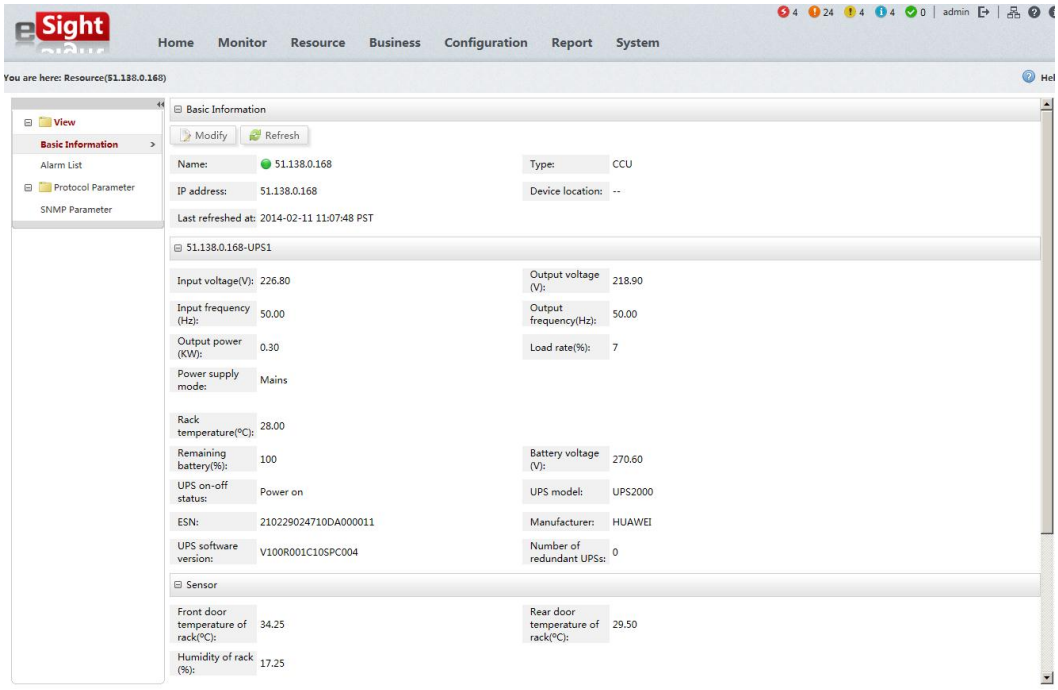
Figure 4-71 Batch import



L1 Resource Management

eSight provides basic management of L1 devices. L1 devices include environment monitoring units (EMUs) and MicroDC cameras.

Figure 4-72 L1 device NE manager



- View
  - Basic information: displays basic NE information. The EMU monitors power supply information, such as the input/output voltage, input/output frequency, active power output, load ratio, power supply mode, battery voltage, and battery remaining capacity. Environment indicator information includes the cabinet front/rear door temperature, cabinet humidity, cabinet front/rear door status, internal/external smoke sensor, water sensor, and motion detection information.
  - Alarm list: displays active alarms of the current NE.
- Configuration
  - Web network management: allows you to configure L1 devices.
- Protocol parameters
  - SNMP parameter setting: allows you to set or modify SNMP parameters.

4.2.7 UC Management

eSight provides a Unified Communications (UC) Device Manager component that offers an array of operation, administration, and maintenance (OAM) functions for the UC system. These functions include simplified UC device configuration, wizard-based service installation and configuration, one-stop service rollout, end-to-end visual network surveillance, and intuitive display of fault information.

NOTE

To use these functions, users must have the UC Device Manager installed.

4.2.7.1 Managing UC Devices

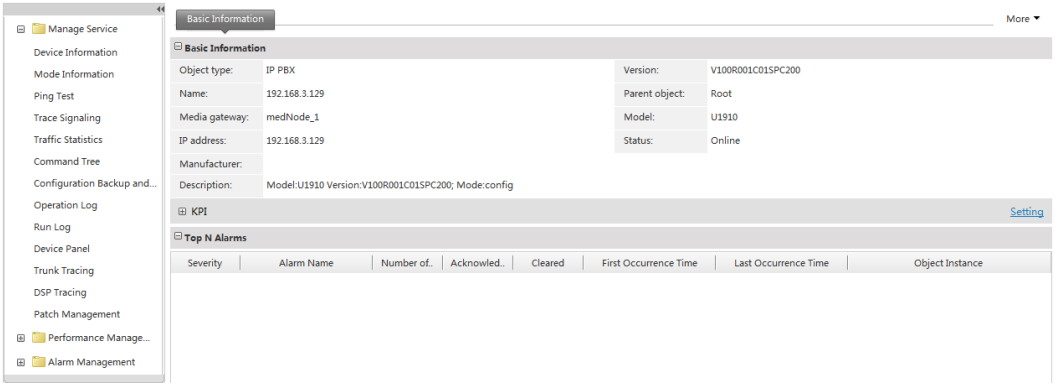
eSight supports unified management of a variety of UC devices, including IP PBXs, U2900s, EGWs, IADs, and UAP3300s.

4.2.7.1.1 IP PBX Management

eSight provides service, configuration, device panel, and log for the IP PBX.

Management Page

Figure 4-73 IP PBX management page



Service Management

- Device information viewing

  You can view the basic information, license information, version information, and patch information of IP PBXs on eSight.

- Ping test

  You can run the **ping** command to check the connection between an IP PBX and other devices.

- Signaling tracing

  eSight provides the signaling tracing management function for the IP PBX to trace and monitor protocol messages, connection of port signaling links, and service flows of the IP PBX dynamically. You can export the signaling data to .csv files, and view the files when the IP PBX is offline.

- Traffic statistics

  You can collect the statistics on IP PBX traffic, set the collection period of traffic statistics, set the start time and end time of a traffic statistics collection task, and export and delete traffic statistics. The statistical items include the numbers of global Real-Time Transfer Protocol (RTP) messages, total SIP sessions, SIP sessions on the outgoing trunk, SIP sessions on the incoming trunk, and duration of a SIP session.

- Configuration data backup and restoration

  The IP PBX configuration file **data.bin** can be manually or automatically backed up on eSight server or a local computer.

- Trunk tracing

  eSight traces IP PBX trunks based on the office route direction. You can view real-time and historical usage of trunks.

- Patch management

  You can view, load, activate, deactivate, save, and delete patches on eSight.

Configuration Management

eSight can configure an IP PBX or IP PBXs in batches.

- Batch configuration

  eSight enables you to configure the SIP trunks, active and standby IP PBXs, and call forwarding offline service for IP PBXs in batches.

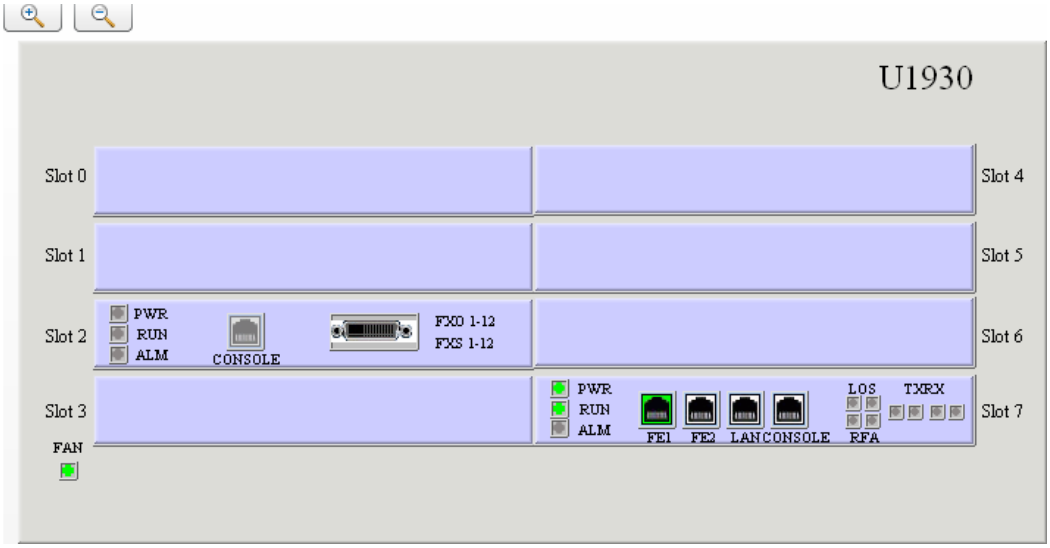
- Single configuration

  The command tree includes IP PBX commands. You can run the IP PBX commands to configure an IP PBX.

Device Panel Management

The IP PBX device panel provides a UI that enables you to query the IP PBX's running status, and add, modify, or delete boards.

Figure 4-74 Device panel



Log Management

- Operation log

  Operation logs record operations that users perform on the IP PBX. You can query and export operation logs.

- Run log

Run logs record information, alarms, and errors during system running. You can add, modify, pause, restart, or delete a run log task, search for run logs, and export them from eSight to a local computer.

Automatic NE Connection

When there are SIP registrations or SIP trunks between NEs or when IP PBXs work in active/standby mode, eSight automatically creates connections between NEs.

4.2.7.1.2 U2900 Management

eSight provides device panel management for the U2900.

Introduction

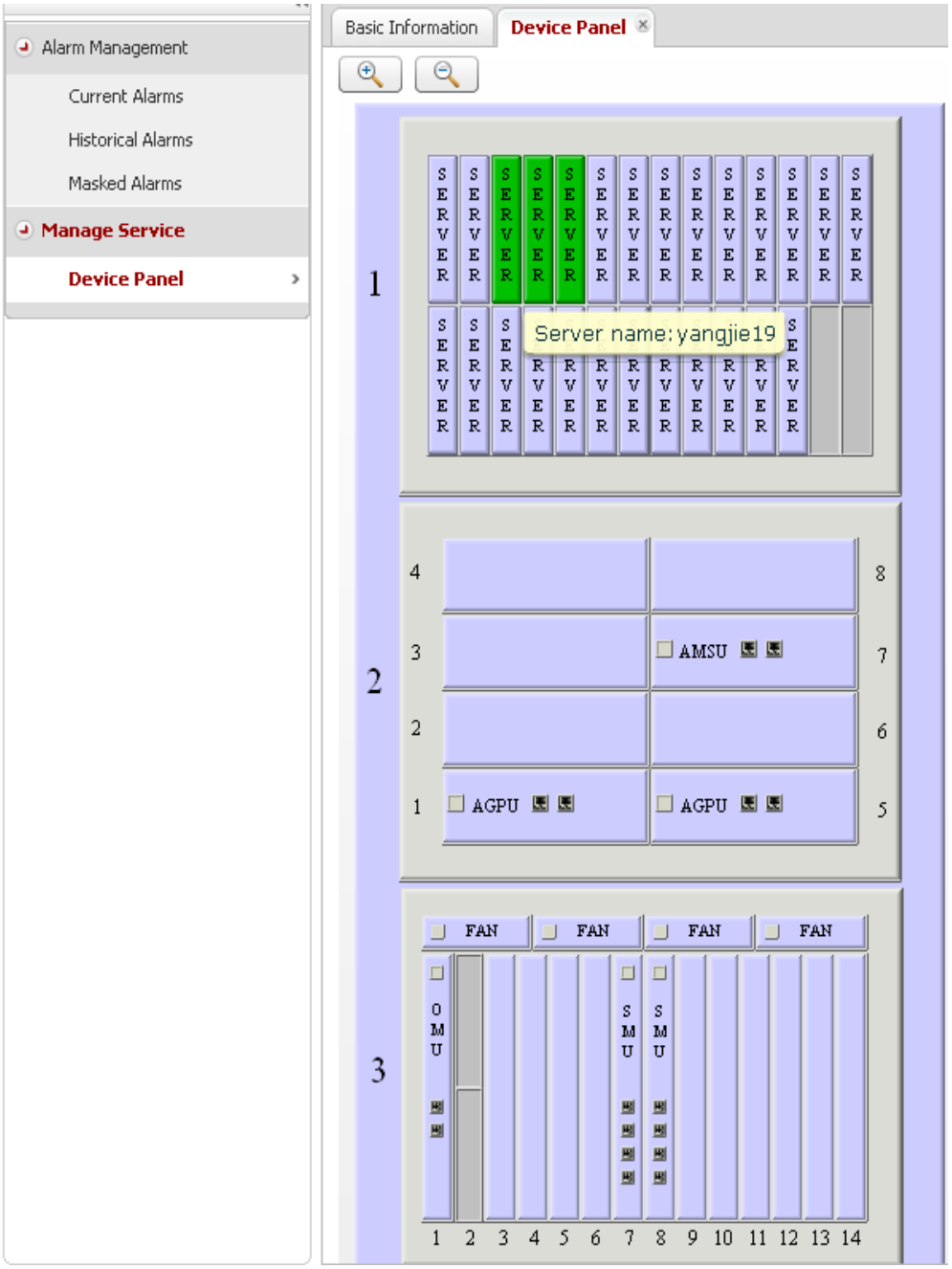
The U2900 series consist of the U2980 and U2990. Two types of NEs are mounted to the U2900, that is, Common Desktop Environment (CDE) and UAP. When you add a U2900 on eSight, the CDE and UAP are added automatically. The CDE is a logical NE, and the SoftMGC, MRP, and MGW function as UAPs.

Device Panel Management

eSight enables you to switch between front and rear simulated U2900 device panels and view the following information on either simulated panel:

- Real-time status of boards
- Time sequence of a Circuit Interface Unit (CIU) board

Figure 4-75 U2900 device panel

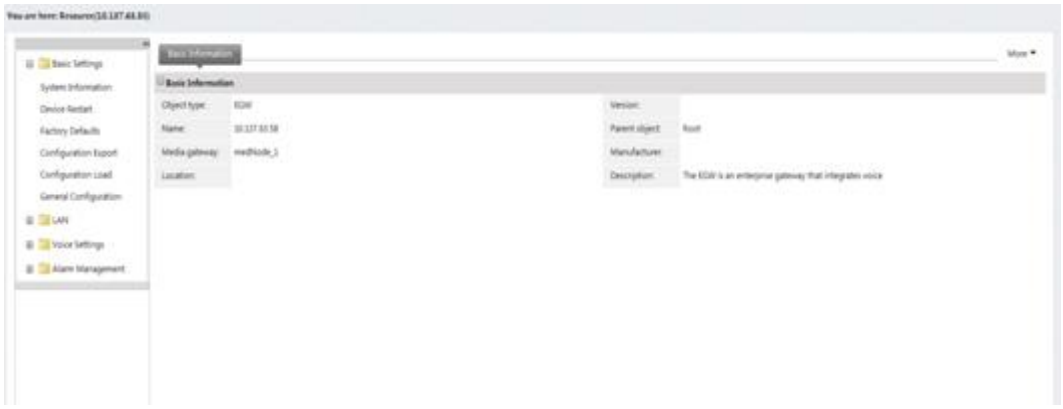


4.2.7.1.3 EGW Management

eSight provides configuration and maintenance management for the EGW.

Management Page

Figure 4-76 EGW management page



Configuration Management

- Basic configuration.
  Check basic EGW information, Configuration file load and backup, and restart an EGW.
- Local area network (LAN) configuration.
  Configuration of LAN basic information, firewall, and DHCP.
- Voice configuration.
  Configuration of the SIP server, FXO outgoing prefix, and data synchronization server.

Maintenance Management

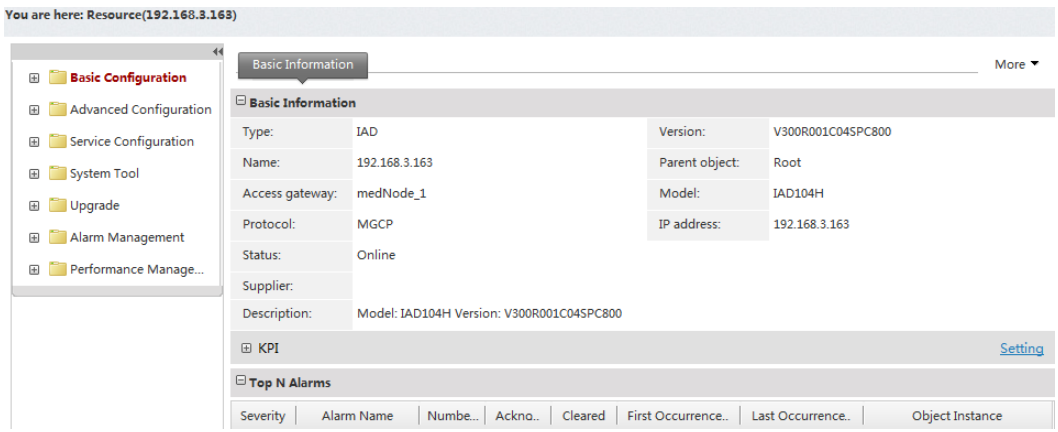
eSight enables you to upgrade EGWs in batches. You can upgrade EGWs immediately or at a scheduled time.

4.2.7.1.4 IAD Management

eSight enables users to manage IADs.

Management Page

Figure 4-77 IAD management page



IAD Configuration

NOTE

eSight provides varied IAD management functions depending on the IAD model. This topic lists all the IAD management functions that eSight provides. For details about the management functions that eSight provides for specific IAD models, see the **eSight Specification List**.

- For a single IAD, eSight provides the following functions:
  - Basic configuration

    This function enables users to configure the network parameters, network management settings, and device time.
  - Advanced configuration

    This function enables users to set the protocol switching, trap enable/disable, and duration of an alarm generated due to a locked port.
  - Service configuration

    This function enables users to configure the digitmap, proxy server, voice parameters, and fax parameters.
  - System tool support

    This function enables users to query the version information, set the network port status, reset configurations, restart the device, and query the country code.
- For a batch of IADs, eSight enables users to configure the proxy server, read and write communities, network management settings, and network parameters, and to save the configurations.

IAD Maintenance

- Upgrade
  - Manual upgrade

    Users can manually upgrade IADs one by one and in batches on eSight. All the IADs can be upgraded using the host software, except for the IAD132E (T) that must be upgraded using the Complex Programmable Logic Device (CPLD) software. Users can upgrade IADs immediately or at a scheduled time on eSight.
  - Automatic upgrade

    When the automatic upgrade function is enabled, an IAD periodically checks the latest version recorded in the upgrade file on the FTP server. If the IAD detects a new version, the IAD is upgraded automatically.
- Backup and restoration

  eSight enables users to back up IAD data (such as IAD configurations or SIP user information) to the eSight file server, to restore IAD data on the eSight file server to specific IADs, and to save IAD data onto a local computer.
- Ping test

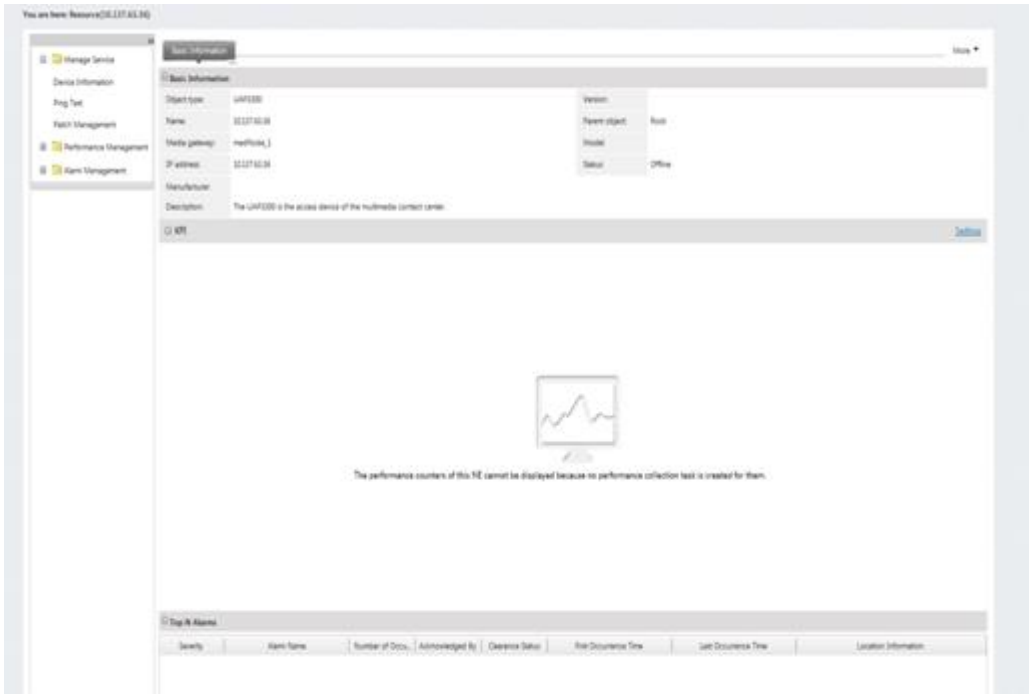
Users can run the **ping** command to check the connectivity between an IAD and other devices.

4.2.7.1.5 UAP3300 Management

eSight provides UAP3300 service management.

Management Page

Figure 4-78 UAP3300 management page



Service Management

- Device information

  You can view the basic information, license information, version information, and patch information of UAP3300s on eSight.

- Ping test

  You can run the **ping** command to test the connection between an UAP3300 and other devices.

- Patch management

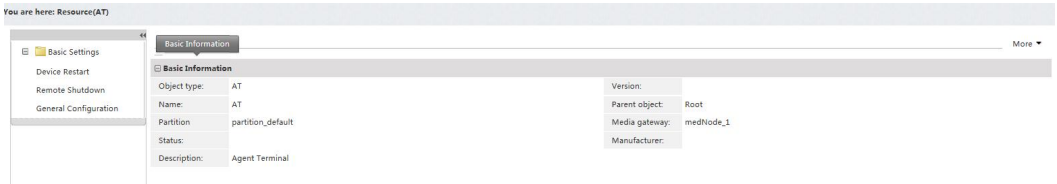
  You can view, load, activate, deactivate, save, and delete patches on eSight.

4.2.7.1.6 AT Management

eSight provides automatic deployment, batch configuration, and maintenance management for ATs.

Management Page

Figure 4-79 AT management page



Automatic Deployment

- Create AT subnets.

  You can create AT subnets on eSight. After an AT registers with eSight, the AT is added to a subnet. When the IP address of an AT is changed, eSight automatically adds the AT to the subnet where the IP address falls.

- Query ATs that have no matched subnets.

  eSight enables you to query ATs that have no matched subnets. You can create subnets for these ATs or extend the IP address range of the existing subnets to incorporate the ATs.

Configuration Management

- Batch Export ESNs.

  To apply for a license file for an AT, you must provide the ESN of the AT. eSight can batch export ESNs of ATs.

- Batch Load license files.

  After obtaining license files of ATs, you can use eSight to batch load the license files.

- View the license file loading history.

  You can view the historical records about loading the license file to an AT.

- Export AT information.

  You can export host information about ATs from eSight to an EXCEL file and use the exported information to install and configure service software on the ATs.

Maintenance Management

eSight allows you to bulk restart, and shut down ATs.

4.2.7.2 IP Phone Device Management

eSight provides IP phones management functions.

4.2.7.2.1 IP Phone Management

The eSight provides several management functions for IP phones. They are IP phone subnet creation, automatic deployment, device management, configuration management, service management, and certificate management.

NOTE

The management functions that the eSight provides vary depending on IP phone models. The following describes all the functions.

Creating an IP Phone Subnet

Create an IP phone subnet and add IP phone with matching IP addresses to the subnet. The subnet can be associated with a configuration file so that configurations in the configuration file can be delivered to IP phones in batches.

Automatic Deployment

- Automatically grouping IP phones to specified subnets

  Assume that certain IP phone subnets have been created on the eSight. When an IP phone registers with the eSight for the first time, the eSight automatically adds the IP phone to an appropriate subnet. When the IP address of the IP phone changes, the eSight automatically moves the IP phone to another IP phone subnet covering the new IP address of the IP phone.

- Automatically delivering configuration files

  Once you create a subnet, you can create a configuration file for the subnet. Then, the eSight can automatically deliver the configuration file to an IP phone when the IP phone is added to the subnet.

- Automatically upgrading version files

  After uploading IP phone version files on the eSight, IP phones that are added to the eSight using the automatic deployment function automatically compare their own versions with those in the corresponding version files on the eSight. If the versions are different, the IP phones automatically upgrade their version files.

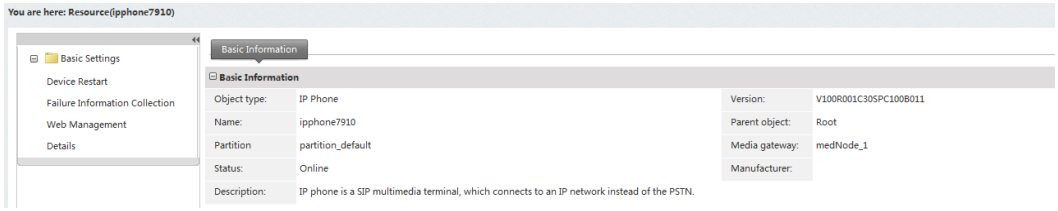
- Querying IP phones that match no subnet

  Querying IP phones that match no subnet help you know which IP phones are not contained in a subnet. Then you can add IP phone subnets or change the IP address segments of existing IP phone subnets so that these IP phones can be added to the subnets for management.

Device Management

You can perform operations **Device Restart** for an IP phone on the eSight.

Figure 4-80 IP phone device management page



Configuration Management

eSight allows you to bulk restart IP Phones.

Service Management

- Upgrade management

  You can use the eSight to upgrade the main programs of eSpace 6800 series IP phones, eSpace 7800 series IP phones and eSpace 8850 series IP phones immediately or in batches as scheduled. You can use the eSight to upgrade the main programs, language packages, font libraries, certificate files, and signal tones of eSpace 7900 series IP phones immediately or in batches as scheduled.

  After version files and configuration files are uploaded, you can upgrade them in batches.

NOTE

IP phone version files are stored on the file server. The file server can be one built in the eSight.

- Access scan

  When a great number of IP phones connect to the eSight, the eSight uses the access scan function to send ACS addresses and certificate paths to the IP phones. After IP phones automatically update their configurations based on the information received from the eSight, the IP phones automatically connect to corresponding IP phone subnets.

NOTICE

The access scan function applies to eSpace 7910 IP phones and eSpace 7950 IP phones with the version V100R001C02 or later.

- Voice quality inspection management

  The eSight provides the terminal voice quality function, which can be used to evaluate IP phone voice quality. The evaluation result can be displayed on the as reports, helping locate and rectify faults. For details, see .

- Management of IP phones that match no subnet

  If the IP address of an IP phone does not belong to the IP address segment of any IP phone subnet, the IP phone is automatically grouped to **Device that Matches NO Subnet**. You can modify the IP address segment to cover this IP address, or create a subnet and add the IP phone to this subnet.

Certificate Management

When a certificate updates or the customer wants to use their own certificates, upload the new certificates to the eSight so that IP phones can be authenticated by the eSight.

4.2.7.3 Managing UC Applications

eSight enables users to manage UC devices (BMP, AA, MAA, OBG, CallAS, Meeting AS, Meeting MS, PGM, Portal, eConf Portal, SEE, AP, Presence, Group and Message) in the eSpace UC solution. The management functions include creating an SNE subnet, adding a single UC solution device, device management, business trace, terminal voice quality, monitoring service status, collecting service logs, single sign-on (SSO), and common functions of alram management, performance management and topology management.

Creating an SNE subnet

After SNE subnets are created, the eSight automatically adds an SNE device to the matching subnet based on the SNE device's IP address.

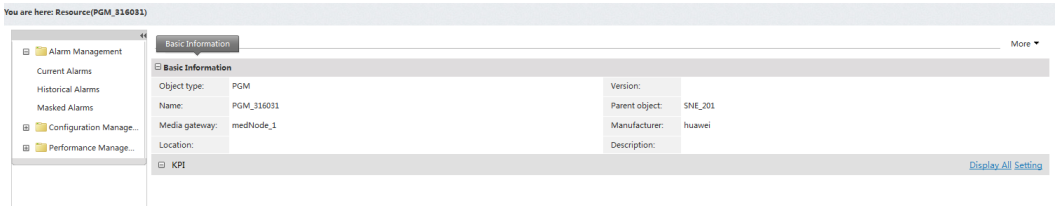
Adding a single UC solution device

If you want to add a single UC solution device after the SNE subnet has been created onsite, you can manually add the UC solution device.

Device Management

eSight provides configuration management (including database, service, and system configuration management) for the AA, OBG, Call AS, PGM and so on.

Figure 4-81 Device management page (PGM)



- Managing the BMP

  The eSight provides the alarm management and BMP manager functions for the BMP.

  - BMP System: Opens the **BMP Manager** page and configures the BMP disaster recovery (DR) switchover.
  - Database Config: Configures information about the BMP database to be connected. The **Database Config** is used to connect the database of BMP, and synchronize the user name from the BMP to eSight.
  - Operation Log and Security Log: Queries BMP operation logs and security logs. Logs that have been recorded in the database are queried. If no log has been recorded in the database, no data will be found.

- Managing the AA

  The eSight provides the configuration management, alarm management, and performance management functions for the AA.

  AA Config: Adds, modifies, deletes, synchronizes, imports, or exports AA configuration information.

- Managing the Call AS

  The details of Call AS manager functions as following:

  - CTD_AnncFileName: Adds, modifies, deletes, synchronizes, imports, or exports voice files.
  - CalleePAS and CallerPAS: Processes CTD service internal logic.
  - Default Language: Sets the default language.
  - ESG Service Name: Configures the ESG service name.
  - Max Call Time: Configures the maximum call duration.
  - Head Route Value: Configures the route header. Enter the route header in the same format of the default route header.

- Managing the PGM

  The eSight provides the configuration management, alarm management, and performance management functions for the PGM.

  The details of PGM manager functions as following:

  - svc_chat: Configures the NetworkProperties and ChatroomProperties.

  - PGMConfig Properties: Configures the PGMCommonConfig, GroupConfig, MessageConfig_GM, MessageConfig_SM, MessageConfig_SM_SPInfo, Incre Sync and CdrSwitch.

- Managing the Meeting AS

  The eSight provides the alarm management, performance management, and license management functions for the Meeting AS.

  View License: Views, refreshes, and uploads licenses and obtains ESNs.

- Managing the MAA

  The eSight provides the alarm management and performance management functions for the MAA.

- Managing the Meeting MS

  The eSight provides the alarm management and performance management functions for the Meeting MS.

Business Trace

After creating a message tracing task for managed objects, a user can trace the messages between the managed objects, and view tracing results in figures and tables. You can trace messages in the **User Trace** and **Scene Trace** modes.

Terminal Voice Quality

Terminal voice quality evaluates IP phone (eSpace 7910 and eSpace 7950) and eSpace Desktop voice quality. The evaluation result can be displayed on the eSight as reports, helping locate and rectify faults.

Monitoring service status

This function is used to monitor the running status of the UC solution NEs and databases to facilitate onsite fault locating.

Collecting service logs

The eSight can collect logs of eSpace UC solution NEs to help maintenance personnel analyze and locate faults.

SSO

eSight supports the SSO function. If users have logged in to the BMP, they can log in to eSight directly without being authenticated.

Alarm Management

For details, see **Fault Management** in **Functions and Features**.

Performance Management

For details, see **Performance Management** in **Functions and Features**.

Topology Management

For details, see **Topology Management** in **Functions and Features**.

Managed Objects

- BMP

  The Business Management Platform (BMP) provides unified service management for eSpace UC clients. It supports a wide array of services. After logging in to the BMP, the enterprise administrator can maintain enterprise information and register and deregister enterprise members.

- Portal

  The Portal is designed for enterprise users who have registered with eSpace UC. After logging in to the Portal, enterprise users can maintain their personal information and configure service functions such as Do-Not-Disturb (DND), call transfer, and advanced secretary.

- MAA

  The Multimedia Authentication Answer (MAA) connects third-party clients, especially mobile clients, to ASs and provides the following functions:

  - Interface conversion: The MAA converts various interface messages from eSpace UC's ASs into Transmission Control Protocol (TCP) interface messages and sends them to third-party clients.
  - Client session maintenance: After third-party clients connect to the MAA, the MAA generates a session for each client and maintains the session status based on the client status.
  - Service processing: The MAA processes service logic, such as the logic for heartbeat mechanism, reconnection after a short disconnection, and IM timeout processing.
  - TCPAdapter is a mobile terminal service module. It maintains sessions between the UC system and mobile terminals and processes TCP messages received from mobile terminals.

- AA

  The Access Agent (AA) is responsible for eSpace Desktop access and authentication. eSpace Desktop obtains login information from the AA and invokes the AA interface to gain access to services such as calling, instant messaging, and conferencing.

- OBG

  The Open Business Gateway (OBG) provides a service openness and integration platform. It connects to or integrates with the IT, Social Networking Site (SNS), and Internet systems of enterprises.

- Call AS

  The Call AS is a core component of eSpace UC and provides call control and service processing capabilities.

- PGM

  - MESSAGE

    The MESSAGE carries out messaging services and provides a uniform and integrated message processing center. Thus, users can experience uniform messaging services. As a messaging platform independent of services, the MESSAGE processes basic message

flows. The basic message flows include the following: Message accessing, Protocol adapting, Message storing, Service triggering and Message scheduling.

- Presence

  The Presence publishes and subscribes to presence information of each presentity as well as update presence information status in real time.

- Group

  The Group is a server that manages resource lists. Physically, the Group is an independent server or a two-node cluster.

- AP

  The AP consists of the APService and PolicyService. The AP accesses, authenticates, and dispatches XCAP messages, and allows you to query route information.

  The PGM cooperates with eSpace UC clients to provide the following functions:

- Presence: The real-time status of each enterprise user is displayed on the UC client so that users can view their contact status in real time. Based on a contact's status, such as online, offline, busy, or away, an enterprise user can select a proper way to reach the contact.
- Instant messaging: An enterprise user can send an instant message to an individual contact, contacts in a contact group, or contacts in a temporary group.
- Enterprise address book (also known as the corporate directory): The enterprise address book contains the contact information of departments and employees. The enterprise administrator manages and maintains the enterprise address book on the BMP.
- Personal address book: An enterprise user has a personal address book to store contact information. The user manages and maintains the personal address book on the UC client.

- Meeting AS

  The Meeting AS is a meeting control server that provides meeting control and management functions.

- Meeting MS

  The Meeting MS is a video and data meeting application server that provides multimedia meeting capabilities, including video, screen sharing, file transfer, whiteboard, and text chatting services.

- SEE

  The SEE allows network protocols to be accessed. The SEE loads and executes all types of service logic.

4.2.7.4 Management of Meeting Applications

eSight enables users to manage meeting devices (eConf AS, eConf Portal and Media Server) in the eSpace Meeting system. The management functions include adding a single meeting device, device management, and common functions of alram management and topology management.

Adding a single meeting device

If you want to add a single meeting device after setting SNMP protocol parameters on meeting devices, you can manually add the meeting device.

Device Management

Figure 4-82 Device management page (eConf AS)

- Managing the eConf AS

  The eSight provides the alarm management, performance management and eConf AS manager functions for the eConf AS.

  eConf AS manager functions: The eSight allows you to configure the following related to the eConf AS: AS global parameters, Meeting global parameters, Call global parameters, Call billing parameters, CSipServer module, Database parameters, IVR parameters, FTP parameters, Media server parameters, Resource parameters and SIP head and protocol stack parameters.

- Managing the eConf Portal

  The eSight provides the alarm management and performance management functions for the eConf Portal.

- Managing the Media Server

  The eSight provides the alarm management and performance management functions for the Media Server.

Alarm Management

For details, see **Fault Management** in **Functions and Features**.

Topology Management

For details, see **Topology Management** in **Functions and Features**.

Managed Objects

- eConf AS

  As the core component in the eSpace Meeting system, the eConf AS controls and connects other components in the system, manages all meeting services, functions as a bridge between multiple meeting systems to expand the meeting capacity, connects a gateway to transmit voice data, read license information, generates meeting event detail records (EDRs), and provides interfaces for external components.

- eConf portal

  The eConf portal allows enterprise users to create instant conferences and scheduled conferences, and to manage those conferences. When creating a conference, users can set conference information including the topic, duration, and participants. Two types of conferences are supported: voice conference and multimedia conference.

- Media server

  The Media server provides multimedia conference functions in the eSpace Meeting system, including text, voice, and video communication, desktop sharing, file transfer, and e-whiteboard.

4.2.7.5 Managing CC Applications

eSight provides CC devices (Agent, eSpace Agent Desktop, HPS, CMS, ICS, BIR, Intelligent Scripting and CTI) for the eSpace Contact Center (CC) solution, including creating a CC subnet, adding a single CC solution device, device management, and common functions of alram management and topology management.

Creating a CC subnet

After CC subnets are created, you can manager CC solution devices.

Adding a single CC solution device

If you want to add a single CC solution device after the CC subnet has been created onsite, you can manually add the CC solution device.

Device management

Figure 4-83 Device management page (Agent)

Alarm Management

For details, see **Fault Management** in **Functions and Features**.

Topology Management

For details, see **Topology Management** in **Functions and Features**.

Managed Objects

- Agent

  Agent is a comprehensive call processing system based on Huawei eSpace CC. It provides agent services for Huawei eSpace CC-enabled enterprises and enables attendants of such enterprises to process calls, manage recording files, and monitor incoming calls in real time.

- HPS

HPS is a configuration and management system for outbound call services. It helps improve the work efficiency of attendants, reduce the Operating Expense (OPEX), and increase customer satisfaction.

- CMS

  CMS is an integral part of the eSpace CC solution and provides quality management and monitoring functions.

- ICS

  ICS is a social media service system based on Huawei eSpace CC. It helps enterprises search out the most desired information from massive microblog information based on keywords. In addition, it saves the microblog information, according to which the service representatives of enterprises can answer questions and handle issues raised by customers.

- BIR

  BIR, a report system deployed in browser/server (B/S) mode, provides complete and flexible web-based report application services such as generating, distributing, and managing reports. It supports manual report and periodic report generation, comprehensive report distribution, and powerful data collection.

- Intelligent Scripting

  Intelligent Scripting is a questionnaire system and allows users to release questionnaires (designed with the aid of the SDT component) to the questionnaire server. The questionnaires can be obtained when released to the questionnaire server. The Intelligent Scripting can be integrated with agents. After the integration, the system, once detecting hotline calls, displays corresponding questionnaires for attendants, helping attendants to complete the questionnaire survey.

- CTI

  The CTI combines telephony and data communications technologies to distribute various call types to the appropriate users.

4.2.7.6 Managing VTM Devices

eSight enables users to manage the Virtual Teller Machine (VTM) Manager and VTM terminals contained in the Huawei eSpace VTM remote bank solution. The management functions include fault location and alarm management.

Managed Objects

- VTM Manager

  The VTM Manager, a component of the Virtual Teller Center (VTC), is used to remotely monitor, maintain, and manage VTM terminals. It provides VTM terminal status information and service reports.

- VTC

  The VTC provides remote virtual teller services for customers. The VTC system includes an MCC module and an MCMS module. The MCC controls calls and provides interfaces for information query; The MCMS is used by inspectors to monitor tellers, check teller service quality, and manage the system.

4.2.7.7 Managing UC Outsourced Devices

eSight enables users to manage UC outsourced devices, including SBCs (SX1000s), GS8s and Movius Unified Messaging System (UMS).

Management Page

Figure 4-84 Management page (SBC)

Upgrade Management

eSight enables you to upgrade SBCs in batches. You can upgrade SBCs immediately or at a scheduled time.

4.2.7.8 Voice Quality Monitoring

eSight monitors voice quality of gateways and terminals.

Introduction

eSight monitors voice quality of the following gateways and terminals:

- Gateways

  eSpace U1980, eSpace U1960, eSpace U1930, eSpace U1910, SoftCo9500, SoftCo5500, and IAD1224.

- Terminals

  eSpace Desktop, eSpace 7910, and eSpace 7950.

Gateway Voice Quality Monitoring

The gateway voice quality monitoring includes:

- Monitoring management

  You can configure monitored subnets and NEs, start time and end time of a monitoring task, and data collection periods on eSight. Then, eSight delivers configuration data to NEs while the NEs report QoS data to eSight.

- Data viewing

  eSight provides the Detailed Data, Report Data, and Report View tab pages for you to view the voice quality, MOS, time delay, jitter, and packet loss rate. eSight enables you to query data depending on the calling or called area, device, number, and time range.

Figure 4-85 Gateway data report view

- Data sampling

  eSight enables you to view the calling and called numbers that are involved in a call with the maximum or minimum MOS, time delay, jitter, or packet loss rate.

- Report export

  eSight enables you to export data from the Report Data and Report View tab pages.

Terminal Voice Quality Monitoring

The terminal voice quality monitoring includes:

- Data viewing

  eSight provides the Detailed Data and Report View tab pages for you to view the voice quality, MOS, time delay, jitter, and packet loss rate. eSight enables you to query data depending on the calling or called area, device, number, and time range.

Figure 4-86 Terminal data report view

- Data sampling

  eSight enables you to view the calling and called numbers that are involved in a call with the maximum or minimum MOS, time delay, jitter, or packet loss rate.

- Report export

  eSight enables you to export data from the Detailed Data and Report View tab pages.

Threshold Crossing Alert

You can set the conditions for generating or clearing alarms. For example, when the MOS exceeds the threshold for N consecutive times, an alarm is automatically generated.

Figure 4-87 Configuring alarm thresholds

4.2.7.9 Managing the certificate

eSight provides the Transport Layer Security (TLS) certificate management and restart function to meet the network device certificate change requirements.

eSight enables users to upload a TLS certificate to an independent file server and the SFTP server embedded into eSight. Devices can obtain the uploaded TLS certificate from the two servers.

NOTE

It is recommended that the default certificate and pubic/private key pair be replaced with the certificate and public/private key pair provided by the enterprise after the eSight is installed.

eSight provides TLS certificate management for multiple devices including the eSpace U19XX and U29XX series, IADs, EGWs, IP phone 79XX series, and eSpace clients. For details about device models, see the **eSight** Specification List.

4.2.7.10 Device Information Export

The eSight enables you to export device information to .csv and .xls files, including the device name, type, IP address, version information, model, and description.

4.2.8 IVS Management

eSight provides an IVS Device Manager component that offers an array of OAM functions for the Intelligent Video Surveillance (IVS) system, which ensures better device management. These functions include the video surveillance resource discovery, system topology display, and performance data management. Users can view the performance and alarm data of surveillance devices to learn about the device running status and quickly locate faults.

NOTE

To use these functions, users must have the IVS Device Manager installed.

4.2.8.1 Management of IVS Applications

eSight enables users to manage applications contained in the Huawei eSpace Intelligent Video Surveillance (IVS) solution. The management functions include fault and configuration management.

Management Page

Figure 4-88 Management page (MAU)

Managed Objects

eSight can manage the following IVS-related applications:

- MAU: the main control unit of the intelligent analysis subsystem in the eSpace IVS solution. The MAU manages intelligent analysis tasks and reports the analysis results to eSight.
- MBU: a media backup unit in the eSpace IVS solution.
- MPU: a media processing unit in the eSpace IVS solution.
- MTU: a media transcoding unit in the eSpace IVS solution that is responsible for transcoding and distributing media data.
- TAU: a terminal access unit in the eSpace IVS solution.
- VMU: a video management unit in the eSpace IVS solution.
- PU: a peripheral unit in the eSpace IVS solution that is responsible for collecting video data.

Configuration Management

eSight enables users to configure the configuration files for IVS application modules. It forwards configurations to specific modules through configuration interfaces on the UOA to ensure data synchronization with the modules.

IVS application modules include the OMU, CMU, DCG, SCU, MU, PCG, MAUS, and SMU. For detailed module information, see the **eSpace IVS Product Documentation**.

Service Tracing

eSight traces IVS applications, including tracing the PU registration and deregistration, live video browsing, recording download, recording playback, and live video play. Users can back up, delete, index, and download trace files.

4.2.8.2 Data Analysis

Users can create and manage immediate and periodic report tasks on the report management page.

- Immediate report task

  Users need to manually run an immediate report task. Once an immediate task is executed, a report reflecting the statistics at that time is generated. Users can click the **View Report Details** button to open the generated report. When viewing the report, users also can export it in a file of the specified format if needed.

- Periodic report task

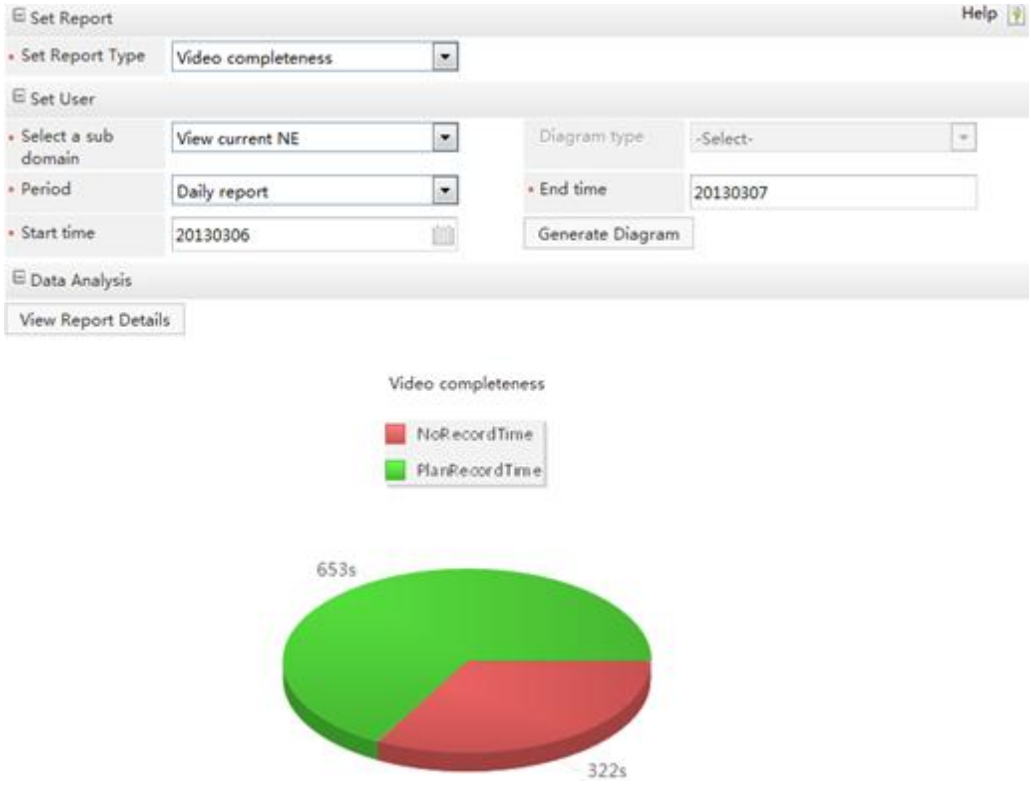
  The system runs a periodic report task automatically based on the specified period of time. Once a periodic task is executed, a report reflecting the statistics within the specified period of time is generated and saved on eSight. Users can view and manage all reports generated by a periodic report task.

Report Management

Users can create and manage immediate and periodic report tasks on the report management page.

Users need to manually run an immediate report task. Once an immediate task is executed, a report reflecting the statistics at that time is generated. Users can click the **View Report Details** button to open the generated report. When viewing the report, users also can export it in a file of the specified format if needed.

Figure 4-89 Report management page



4.2.9 Telepresence Management

eSight provides a Telepresence Device Manager component that offers an array of OAM functions for the telepresence system, which ensures better device management. These functions include the meeting resource discovery and system topology display management. Users can view the alarm data of telepresence devices to learn about the device running status and quickly locate faults.

NOTE

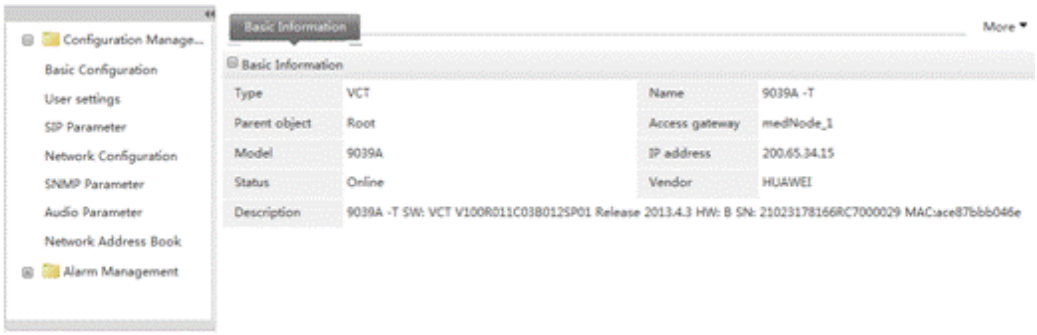
To use these functions, users must have the Telepresence Device Manager installed.

4.2.9.1 Telepresence Device Management

eSight enables users to manage telepresence devices. The management functions include fault location and alarm management.

Management Page

Figure 4-90 Management page (VCT)



Managed Objects

- Terminal

  In the telepresence system, terminals are endpoints that encode and decode audio and video signals.

- MCU

  The Multipoint Control Unit (MCU) is used for terminal access, video exchange, audio mixing, data processing, and signaling exchange.

- TP

  TP is a telepresence product developed by Huawei. It uses high-definition video encoding and digital image stitching technologies, bringing true-to-life widescreen video images. It also adopts professional multi-channel audio capture and reproduction technologies to achieve superior surround sound localization. Using the TP, users can enjoy remote conferencing with life-size participant display and face-to-face experience.

- GK

  The gateway keeper (GK) is a core component of the telepresence system. It is located at the network control layer to manage nodes including the MCU, terminals, and gateways. Node management functions provided by the GK include address resolution, domain management, access control, registration management, call management, bandwidth management, and route management.

Configuration inquiry

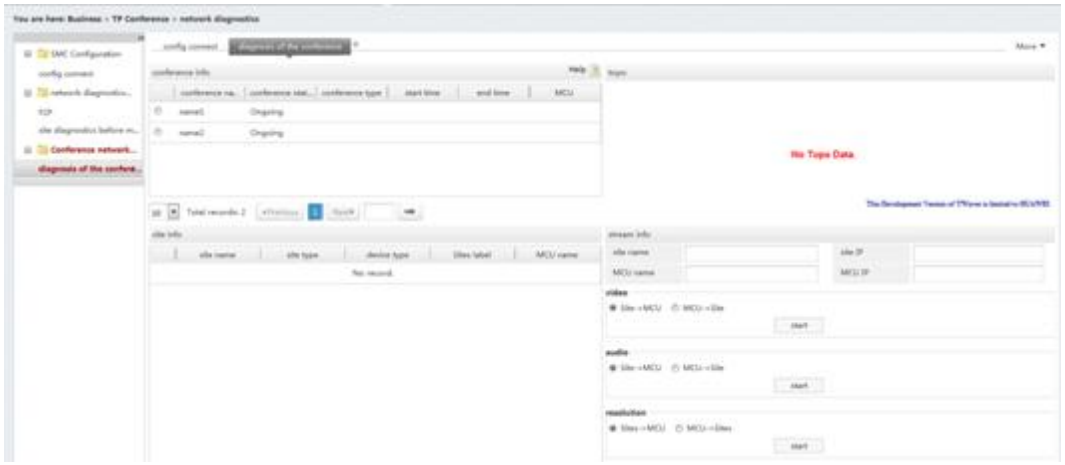
You can inquire the configuration information of MCU, TP and terminal devices in order to avoid logging on each device to configure.

4.2.9.2 Network Diagnosis

eSight collects and processes data about switches and routers in the telepresence system and displays the data on the client so that the administrator can learn about the device status and network conditions of the telepresence system.

Management Page

Figure 4-91 Management Page (Diagnosis during a meeting)



Connection Configuration

Users can configure SMC network connections on eSight to implement the network diagnosis functions for the telepresence system.

Meeting Management

eSight obtains meeting information from the SMC and displays the information on the client.

Network Connection Diagnosis

Network connection diagnosis can be performed before or during a meeting.

- Diagnosis before a meeting

  eSight can perform network connection diagnosis for the MCU of a scheduled meeting room.

- Diagnosis during a meeting

  After obtaining the meeting and media stream information from the MCU through the SMC, eSight collects statistics on the switches and routers along the selected route and evaluates the network connection of the route based on the collected data. If the connection fails to meet the requirements, eSight selects another route.

Route Management

eSight obtains route information from the MCU and collects statistics on the switches and routers that support network connection diagnosis along the route.

4.2.10 eLTE Device Management

eSight offers the following eLTE terminal management functions: automatic deployment, upgrade, configuration, and maintenance.

eLTE Terminal Management Portal

eSight offers a unified eLTE terminal management portal to manage eLTE terminals.

- Viewing basic terminal information

  You can view basic information about eLTE terminals.
- Performing general terminal configuration

  You can modify parameters through the TR069-data model tree.
- Jumping to the web-based eLTE terminal management page

  You can jump from the eSight web page to the eLTE terminal management web page.
- Exporting configuration files

  You can export the eLTE terminal configuration file for backup.
- Loading configuration files

  You can load configuration files for eLTE terminals.

Automatic Deployment

- Automatically assigning eLTE terminals to specified subnets

  You can add subnets for eLTE terminals on eSight. When a eLTE terminal registers with eSight, the eLTE terminal is automatically added to a specified subnet based on the authorized terminal list.
- Automatically delivering configuration files

  Once you create a subnet, it is recommended that you create a configuration file for the subnet. Then, eSight can automatically deliver the configuration file to a eLTE terminal when the eLTE terminal is added to the subnet.
- Automatic upgrading version files

  After a user uploads a eLTE terminals firmware version file, the system automatically upgrades version files if a latest version is available.

Downloading Configuration Files in Batches

You can download configuration files for specified eLTE terminals in batches.

Upgrading Terminal Firmware Versions in Batches

You can upgrade the eLTE Terminal firmware versions in batches immediately or at a scheduled time point.

Performing Remote Maintenance

You can remotely restart eLTE terminals, restore factory defaults, and use the ping command to check the connectivity.

4.3 Service Management

4.3.1 Network Report Management

eSight generates instant and periodic reports and allows you to export reports to a file in any of the following formats: PDF, Excel, and Word. eSight integrates a large number of report templates to meet common operation and maintenance requirements. eSight also allows you to customize report templates.

Report Task Management

You can create and manage report tasks on the eSight report task management page.

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

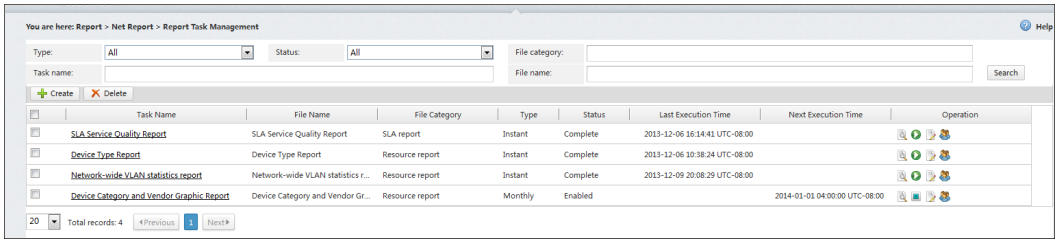
- Instant task

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

- Periodic task

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

Figure 4-92 Report Task Management page



Report System Configuration

- Reports Disk Usage: You can configure and view the disk space of reports.
- Customer Information: You can configure the customer logo and the location for displaying the logo.
- Busy Time Configuration: You can configure the system busy time to collect statistical reports only within a specified time segment when creating a report task.

Customized Report

eSight allows you to upload and use customized report templates.

You can design your own report templates using Business Intelligence and Reporting Tools (BIRT) and upload them to eSight for use.

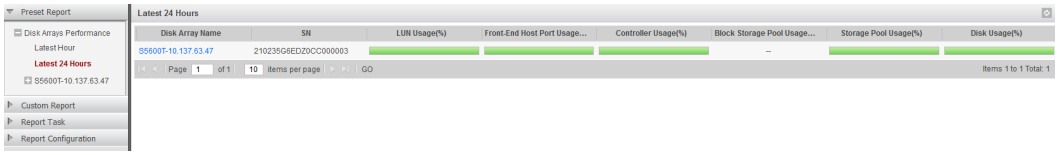
4.3.2 Storage Report Management

The eSight provides long-time performance and capacity analysis reports for storage systems, helping users analyze performance bottlenecks and plan capacity.

Preset report

Preset performance and capacity reports help users view storage system performance quickly and periodically. Storage system-level performance overview shows the performance statistics of LUNs, ports, controllers, and file systems in the latest 24 hours, 7 days, or 30 days. Object-level performance overview shows the performance statistics of disks, ports, CPUs, LUNs, and file systems in the latest 24 hours, 7 days, or 30 days, and sort the statistics by IOPS, bandwidth, and delay. Resource utilization of file systems, storage pools, and thin LUNs in the latest 24 hours, 7 days, or 30 days can be displayed.

Figure 4-93 Preset report



Customized report

Customized performance and capacity reports meet the needs of the customer. Storage system performance overview shows the performance overview of LUNs, controllers, ports, and disks in a past period of time. Object-level performance details show the performance statistics of ports, controllers, LUNs, disks, CPUs, file systems, or storage pools in the past period of time. Storage system and object-level capacity utilization reports show the capacity usage of storage systems, file systems, storage pools, or thin LUNs in a past period of time.

Task report

Customized reports along with periodic implementation policies periodically show performance and capacity statistics. Report implementation results are automatically sent to a specified administrator.

4.3.3 WLAN Service Management

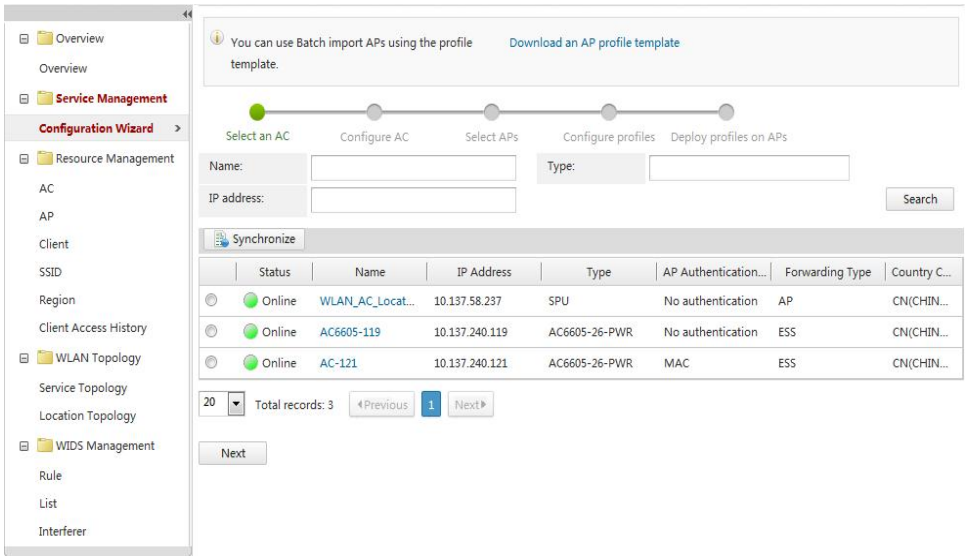
The WLAN Manager offers an integrated solution that manages wired and wireless networks.

- Wizard-based batch service deployment: Delivers wireless service configurations to APs in batches.
- Unified wireless resource management: Manages ACs, APs, wireless users, and regions.
- User fault diagnosis: Diagnoses users access network faults.
- Wireless network security check: Detects intrusion devices and non-Wi-Fi interference sources and offers spectrum analysis.
- Visual management over the wireless network topology: Displays the logical topology of ACs and APs, presents APs in the topology based on regions, and shows the AP hotspot coverage.

Service Management

The WLAN Manager supports wizard-based service configuration. Based on AP planning sheets, the WLAN Manager delivers and deploys AP services end to end, which improves the deployment efficiency (approximately 90% compared to manual deployment).

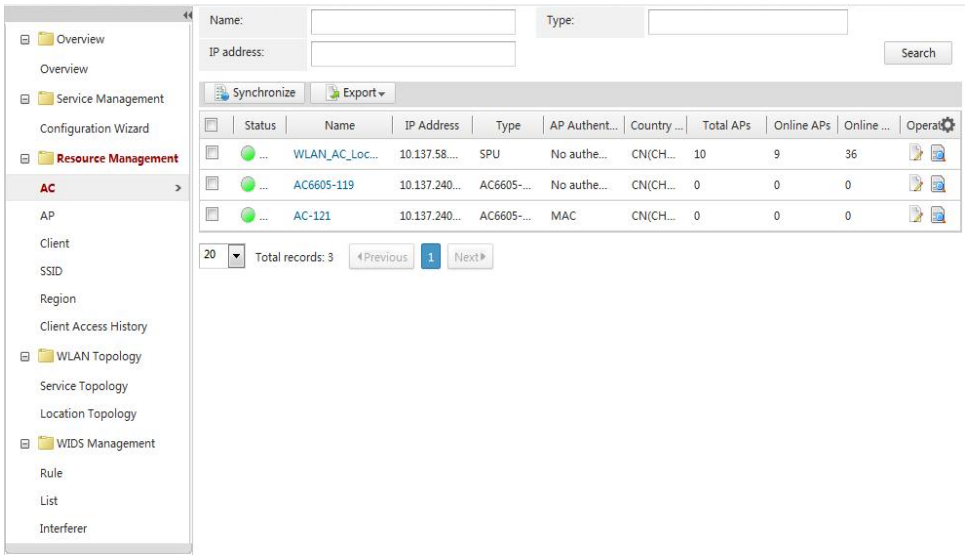
Figure 4-94 AC configuration wizard



Configuration Management

Figure 4-95 shows the AC management page.

Figure 4-95 Managing ACs



An AC controls and manages APs on WLAN. With AC management, you can connect an AP to WLAN in any of the following modes: confirm AP identities, add an AP in offline mode, and add an AP to the whitelist.

- AC information

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

- AP

  An AP functions as a bridge to convert frames transmitted between wireless terminals and a LAN. On eSight, you can configure basic AP information, manage radios, and bind an extended service set (ESS) profile to a radio when creating an AP. You can also import APs in batches from a predefined table and bind profiles to APs in batches. eSight allows you to reboot APs, recover APs and replace APs.

- AP whitelist

  You can configure a whitelist to allow authorized APs to go online. The AP whitelist contains the MAC address and serial numbers of authorized APs. When the AC uses a MAC address or an SN for authentication and automatically discovers that the MAC address or SN of an AP is in the whitelist, the AP automatically goes online.

- Unauthorized AP

  The **Unauthorized AP** page displays APs whose MAC addresses or SNs are not in the whitelist. On this page, you can acknowledge unauthorized APs in batches to add them to the whitelist. Then, whitelisted APs are brought online.

- 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, a deployment mode, an alias, and a default region, and eSight allows you to tune radio frequency (RF) of APs.

- AP blacklist

  Network administrators can add MAC addresses of APs to an AP blacklist, preventing unauthorized APs from going online.

- User blacklists

  Network administrators can add MAC addresses of wireless users to a user blacklist, preventing unauthorized users from connecting to APs. Network administrators can also blacklist unauthorized users and configure the AP countermeasure mode to user blacklist. The system performs countermeasure against devices from the user blacklist.

- SSID whitelist

  Network administrators can configure SSID whitelists to detect unauthorized devices in a more accurate and efficient manner. SSIDs that exist in surrounding environments but have no impact on the wireless network quality are whitelisted and will not be recognized as unauthorized devices.

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

- AP profile

  You can specify the maximum transmission unit of the AP Ethernet port and configure log backup.

- Radio profile

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

- ESS profile

The ESS profile is a set of service parameters, such as **SSID**, **Service VLAN**, **DataTraffer ESSIf**, **Access Max User**, and **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 wireless service functional entity.

Network Monitoring

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

- Physical resources

  AC: AC status, name, type, IP address, AP authentication mode, forwarding type, and country code

  AP: AP status, name, type, SN, MAC address, IP address, AC name, home region, location, bound radio profile, and bound ESS profile

  Client: user's MAC address, IP address, user name, AC name, AP name, radio ID, and service set identifier (SSID)

  SSID: AC name, ESS profile, number of fit APs, number of VAPs, and number of clients

  Region: region name, total number of APs, total number of online APs, and total number of clients.

- Resource statistics

  Network overview: line chart for online users, top SSID user statistics, AP resource statistics and WLAN latest alarms.

  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, and number of regions counted by forwarding mode; top 5 AC alarms; WLAN online user statistics (including last 1 hour, last 24 hours and last 7 days).

  AP statistics: top N AP alarms and AP performance counters

  SSID statistics: AC name, number of fit APs, number of VAPs, and number of terminals connected to APs.

- Performance statistics

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

  - Client access history query

    eSight supports client access history queries only when it is installed on a Linux server and the Linux server can receive syslogs. eSight periodically parses syslogs to extract client access information and imports syslogs to the database in batches to record client access information.

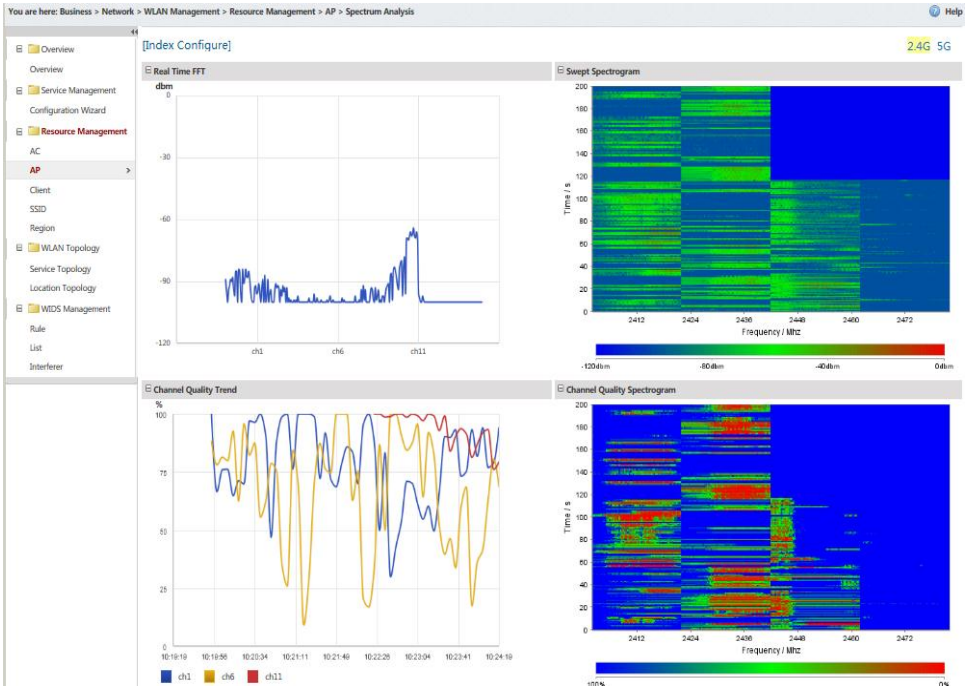
NOTE

Client access history queries are supported only when the Oracle database is used on the Linux platform.

- Spectrum Analysis

  After the AP radio spectrum function is enabled on devices, users can view the signal interference information around APs in the NMS. Users can judge the channel quality and surrounding interference sources on spectrum charts. Spectrum charts include real-time, depth, channel quality, channel quality trend, and device percentage charts.

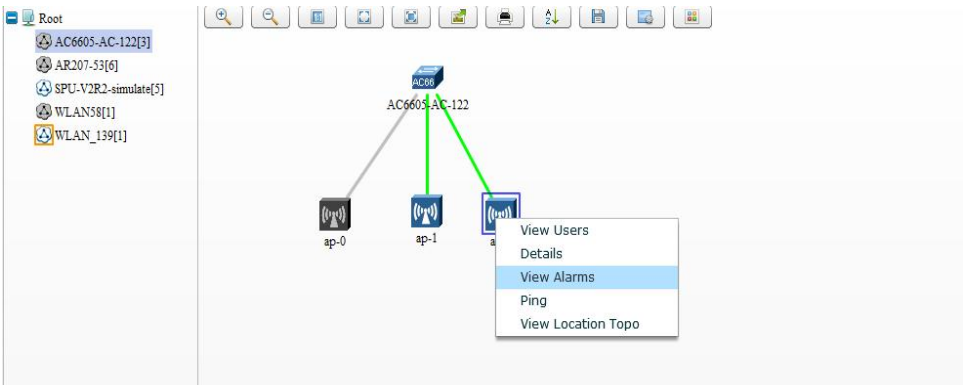
Figure 4-96 AP spectrum chart



WLAN Service Topology

eSight displays managed ACs, APs, and clients and their relationships in topology views. Topology views enable users to check the alarm status of wireless devices and provide quick links for users to check the detailed alarm information.

Figure 4-97 WLAN Service Topology page



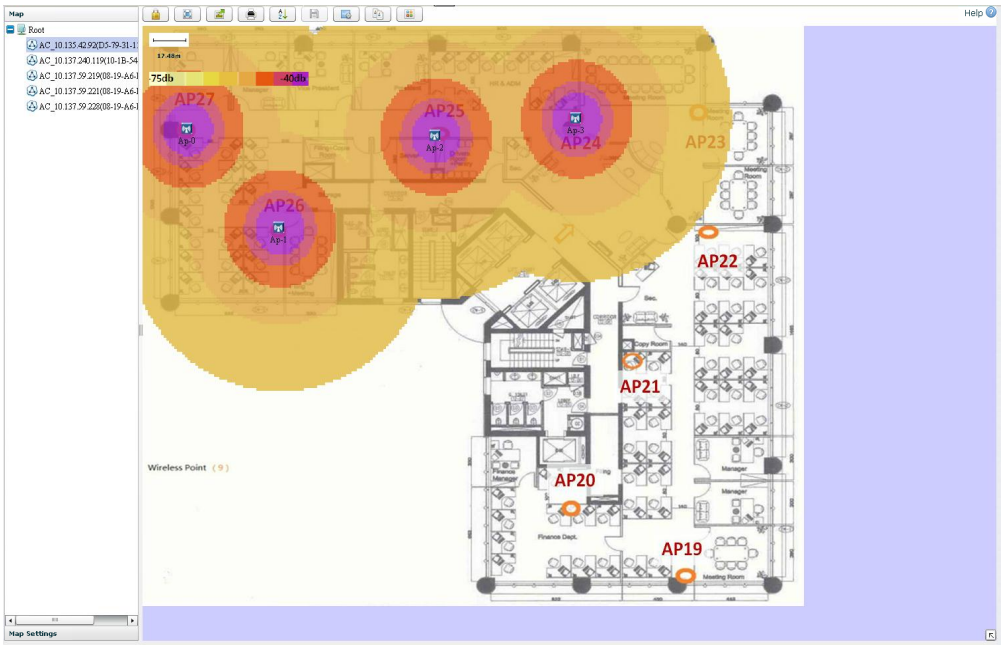
WLAN Location Topology

You can deploy APs in regions, view the hotspot coverage, and detect signal coverage blind spots and conflicts promptly. In regions where license is available and location is enabled, the topology refreshes the latest location of users, unauthorized devices, and Wi-Fi interferers in real time.

1. View the hotspot location and radio signal coverage in the location topology and mark conflict regions.

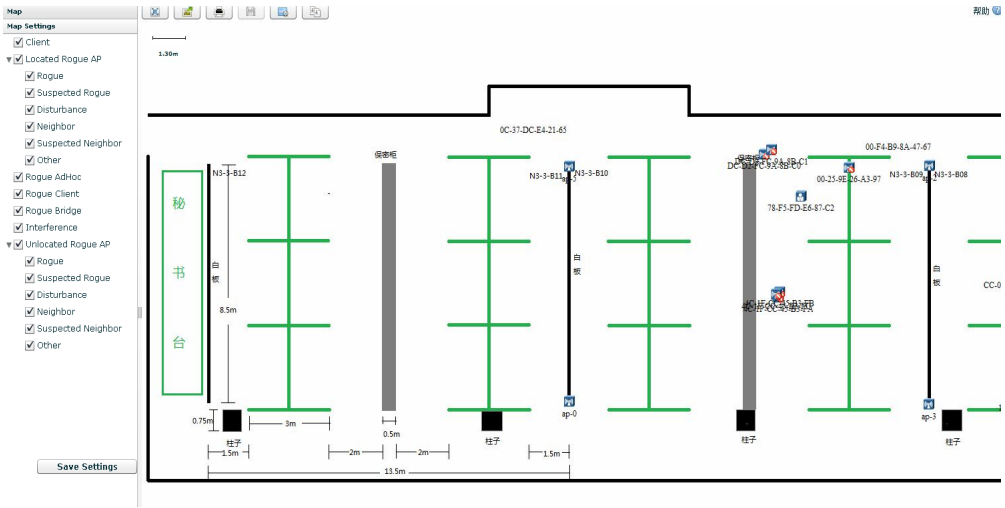
2. Pre-deploy APs, view the simulated radio coverage, and review the actual radio coverage after APs get online.

Figure 4-98 WLAN Location Topology page



3. Map settings: Hide and display nodes in regions by filter criteria. Filter criteria include the user, unauthorized AP, unauthorized user, unauthorized Ad Hoc, unauthorized bridge, and interferer. Unauthorized APs can be displayed based on finer-grained rules.
4. If the location AP license is applied and location is enabled in a region, the locations of users, unauthorized APs, and interferers are refreshed in the topology at regular intervals.

Figure 4-99 Topology node display control

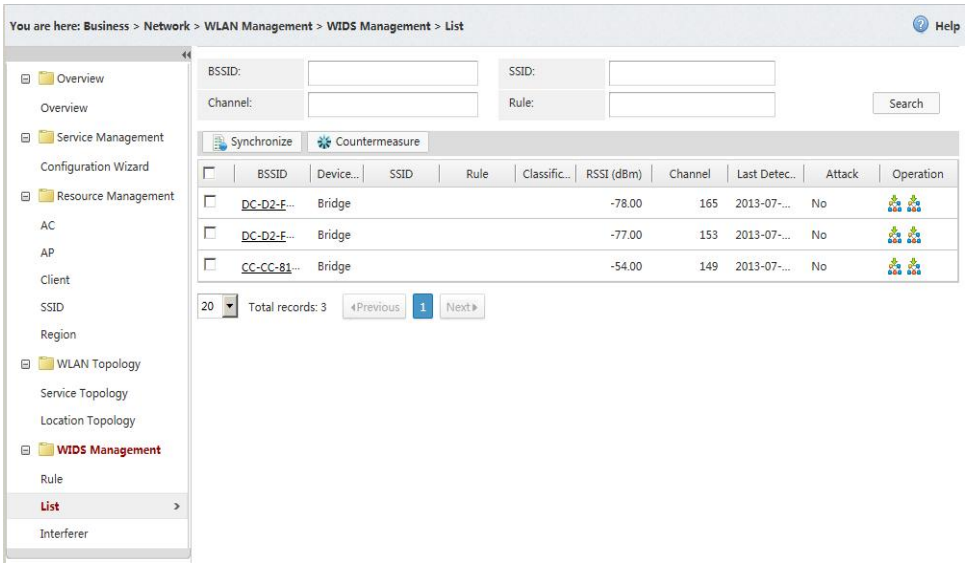


WIDS Management

With Wireless Intrusion Detection Systems (WIDS) management, eSight monitors and recognizes unauthorized devices, clients, interferers, and attacks based on user-defined rules, sends remote alarm notifications, and offers protection measures.

1. Support the statistics, display, and countermeasure of unauthorized devices.
2. Support the display, countermeasure, and suppression access protection of unauthorized devices.
3. Support the statistics and display of unauthorized Wi-Fi interferers.
4. Support the statistics, display, and countermeasure of attacks.
5. Classify unauthorized APs into: rogue, suspected-rogue, adjacent, suspected-adjacent, and interferer. Supported rules include adjacent or same frequency interference, signal strength, SSID (fuzzy or regular expression), number of detected APs, and attack.

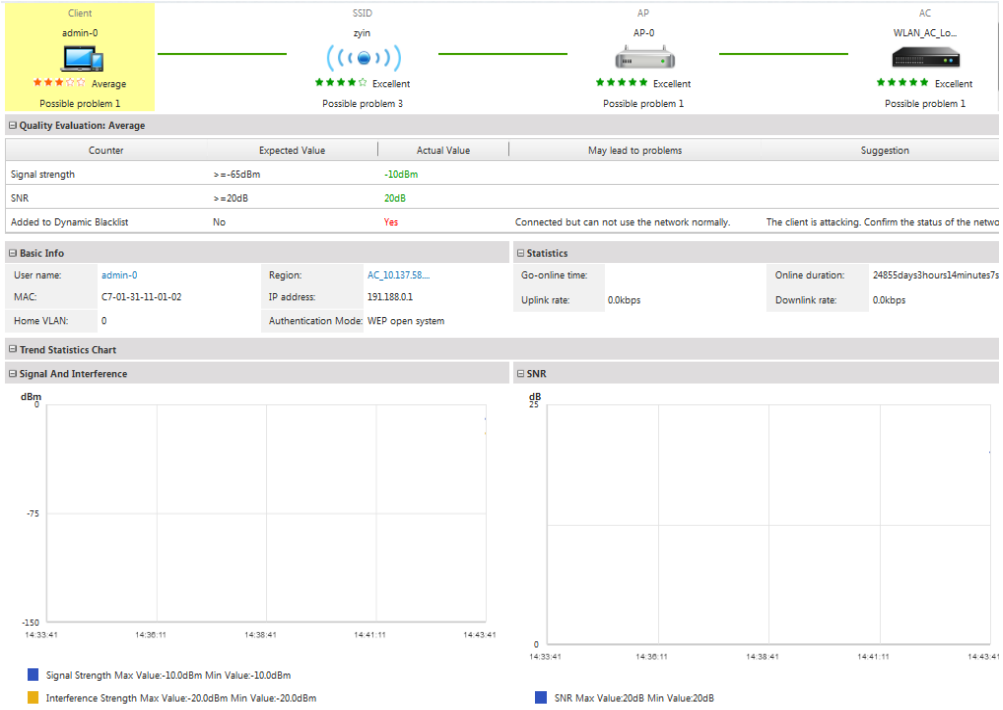
Figure 4-100 Unauthorized AP list



Fault Diagnosis

1. WLAN user fault diagnosis: Diagnoses network quality for online users in terms of users, SSIDs, APs, and ACs. If detecting any exception, the system displays potential problems and gives suggestions for users to rectify the exception.

Figure 4-101 User fault diagnosis

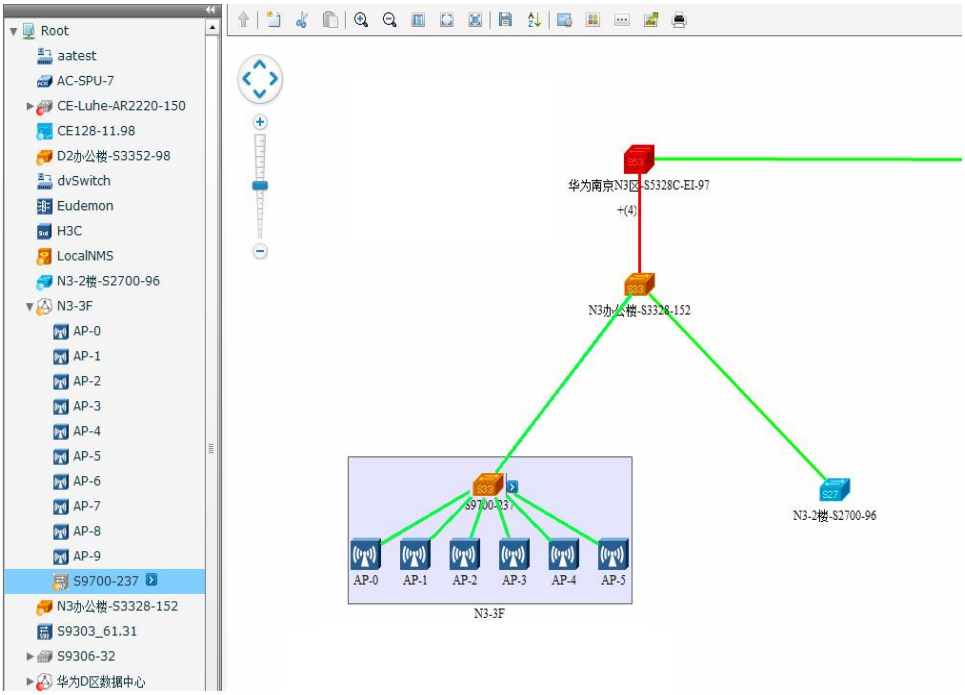


2. Offer related fault alarms about communications, environments, unauthorized devices, and unauthorized Wi-Fi interferers to help users locate and rectify faults.
3. Monitor WLAN network devices and resources to help users learn about the running status of the network and devices.

Integrated wired and wireless management

After the LLDP link discovery is enabled, users can view the links between wired POE switches and wireless APs in the physical topology, enabling integrated wired and wireless management.

Figure 4-102 Physical topology management



Report Management

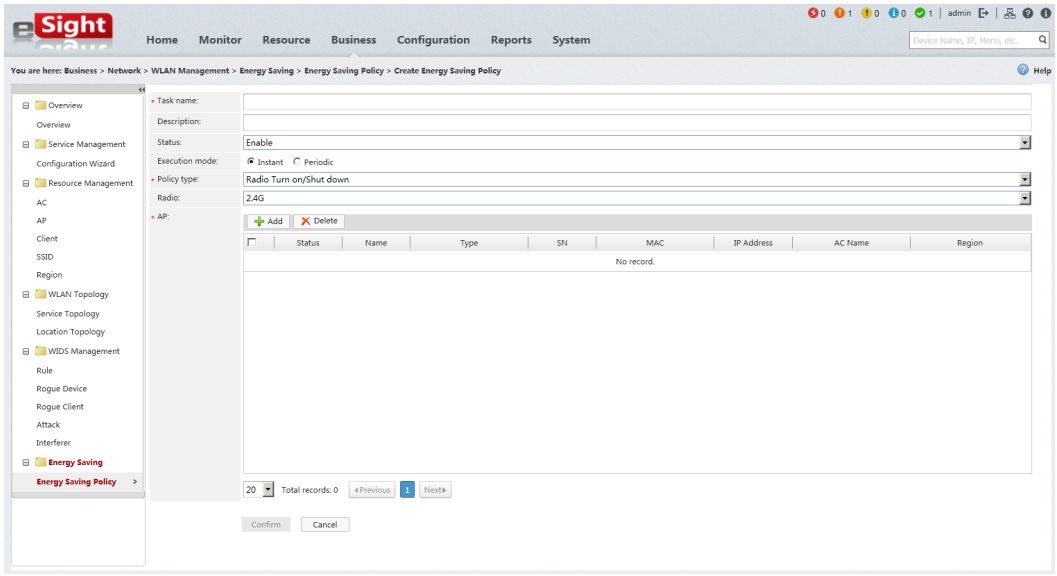
eSight provides predefined WLAN reports (such as AP upstream interface traffic report, AP channel usage report, online RF user report, and online clients report) and quick reports (such as AP association statistics, AP traffic statistics, and AP rate statistics). In an environment with Linux and Oracle, eSight provides one more predefined reports showing a specified number of users with the highest access failure rate and a specified number of users with the most accesses.

Energy Saving Management

eSight allows you to customize energy saving policies in terms of the AP, radio, and SSID.

You can immediately or periodically start energy saving tasks, or disable wireless signals.

Figure 4-103 Creating an energy efficiency policy



4.3.4 BGP/MPLS VPN Management

The BGP/MPLS VPN Manager offers end-to-end solutions for VPAN service deployment, monitoring, and fault diagnosis.

- Wizard-based batch service deployment: Deploys VRF, interface, and routing data for PEs and CEs in batches.
- Convenient and quick automatic discovery: Automatically discovers deployed VPN services without specifying device roles.
- Visualized service topology: Visually displays the logical architecture of PE-PE and PE-CE services, and shows service alarms in real time.
- Multi-dimensional service monitoring: Monitors the running status of monitoring services in terms of the alarm, performance, and service link SLA.
- One-click fault diagnosis: Diagnoses VPN service faults by segment and layer, and using diverse approaches.

Service Deployment

eSight offers graphical, wizard-based, and end-to-end service deployment capabilities and helps you easily and quickly deploy new VPN services, add VPN access points, and adjust existing VPN services, improving service maintenance efficiency. eSight allows you to deploy services in the Full-mesh, Hub-Sopke, MCE, and customized networking types, and deploy OSPF, ISIS, static, and EBGP routing protocols between PEs and CEs.

Figure 4-104 MPLS VPN service deployment

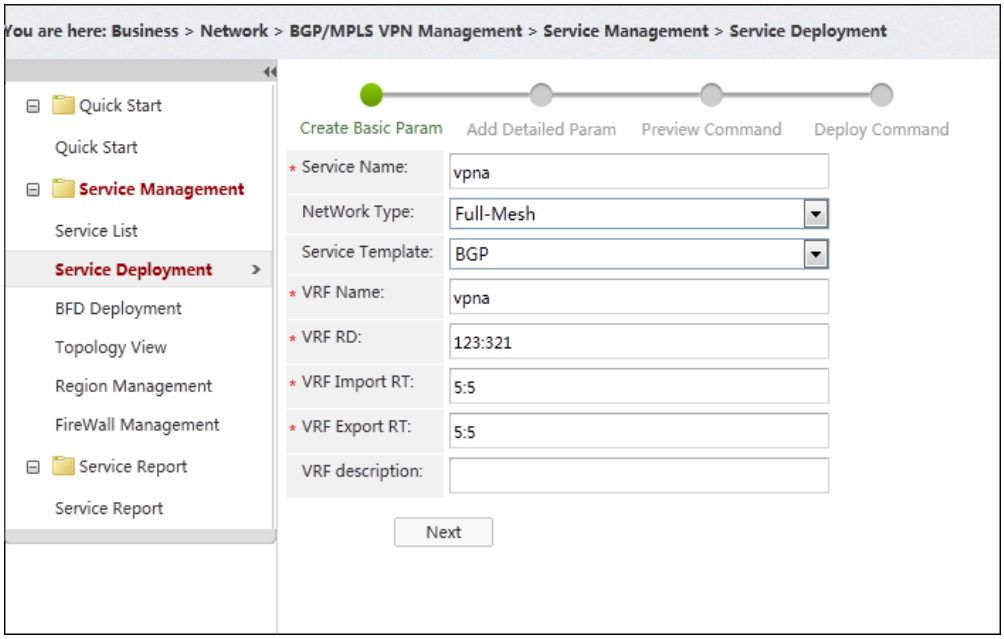
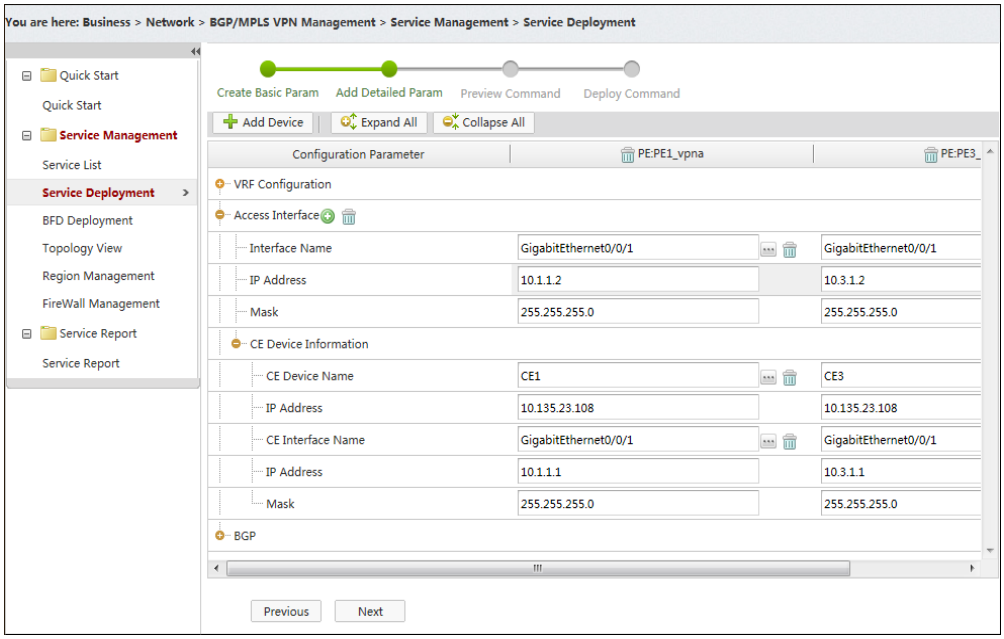


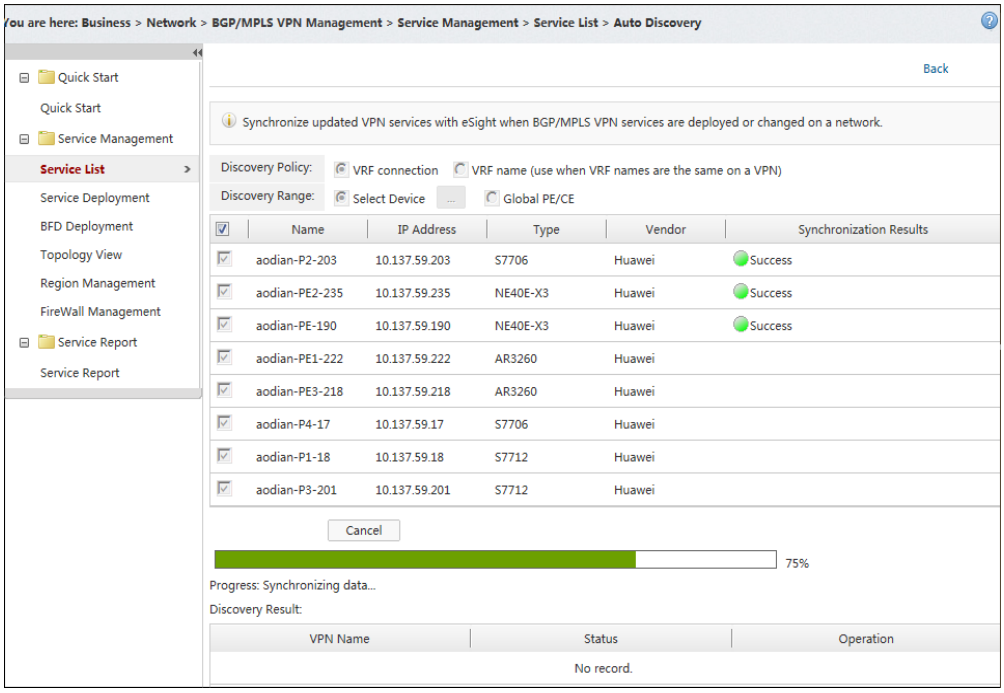
Figure 4-105 Creating detailed configuration



Automatic Discovery

eSight discovers MPLS VPN services automatically in the following network schemes: Full-Mesh, Hub-Spoke, Multi-VPN-Instance CE (MCE), HoVPN, inter-AS Option A, and inter-AS Option B. **Figure 4-106** shows the page for discovering MPLS VPNs automatically.

Figure 4-106 MPLS VPN automatic discovery



MPLS VPN Monitoring

eSight monitors MPLS VPN services and displays MPLS VPN service configurations, including configuration of links between PEs, configuration of links between PEs and CEs, VRF instance configurations, and routing configurations.

eSight provides the following statistics tasks to monitor MPLS VPN performance:

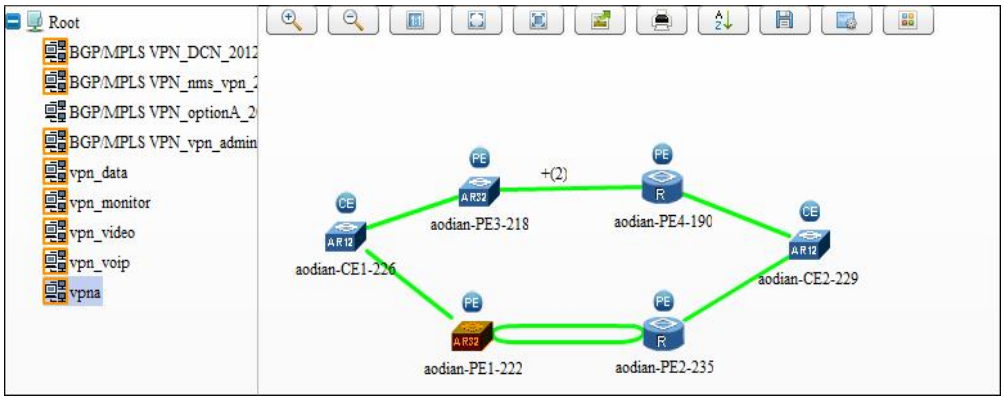
- Access Interface Performance
- VRF Flow Performance
- VRF Route Performance

In addition, eSight monitors MPLS VPN service quality.

MPLS VPN Service Topology

eSight monitors service topologies, displays the VPN logical architecture, and manages user-defined regions.

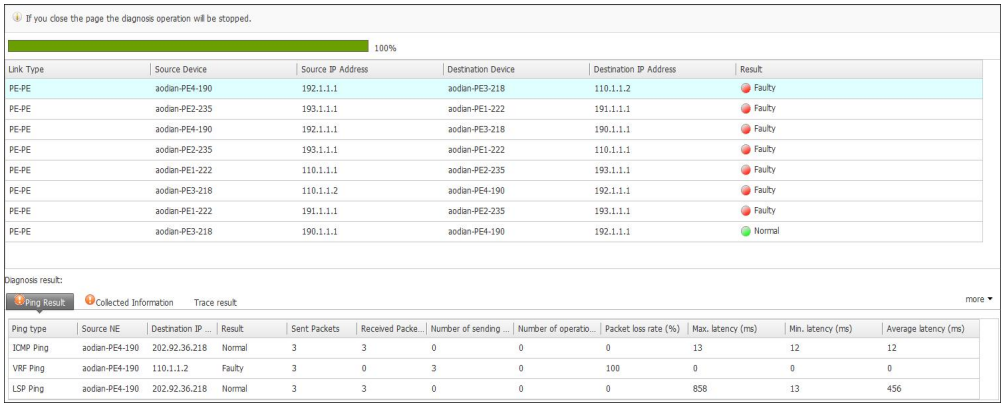
Figure 4-107 MPLS VPN service topology



Quick Diagnosis

eSight offers one-click fault diagnosis to diagnose faults by segment (PE-PE, PE-CE, CE-CE, and PE-remote CE) and layer (L3 routing and MPLS forwarding layer) using multiple approaches (ping, trace, and routing collection). eSight provides the causes to faults after diagnosis, allowing you to quickly locate faults.

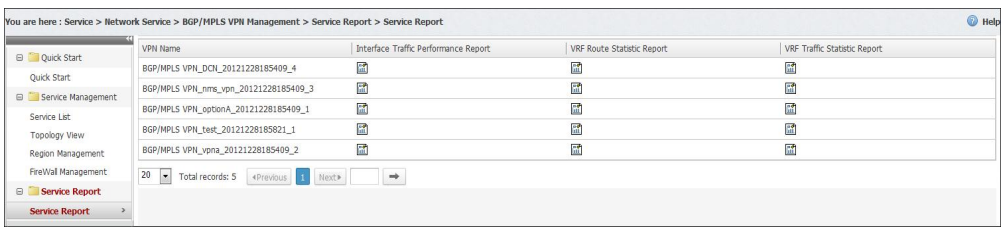
Figure 4-108 MPLS VPN quick diagnosis



Service Report

eSight offers statistical reports on interface traffic, VRF traffic, and VRF routing. Interface traffic reports allow you to learn about the historical interface data about each VPN service. VRF traffic reports allow you to learn about the distribution of VPN traffic on each PE. VRF routing reports allow you to learn about the routing change information about CE access of a VPN service. In terms of traffic and routing, the preceding three reports offer data reference for you to perform some operations, such as capacity expansion.

Figure 4-109 MPLS VPN service report



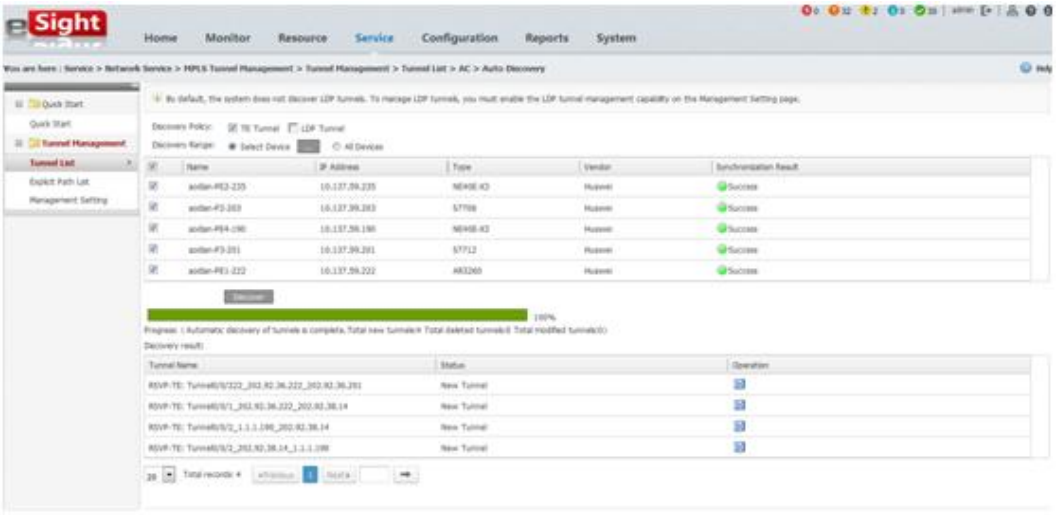
4.3.5 BGP/MPLS Tunnel Management

MPLS Tunnel Manager monitors MPLS TE and LDP tunnels, including the tunnel running status, backup status, tunnel topology, alarms, and tunnel-related VPN services.

Automatic Discovery

eSight automatically discovers MPLS tunnels on the network, including MPLS TE and LDP tunnels.

Figure 4-110 MPLS tunnel automatic discovery



Tunnel Monitoring

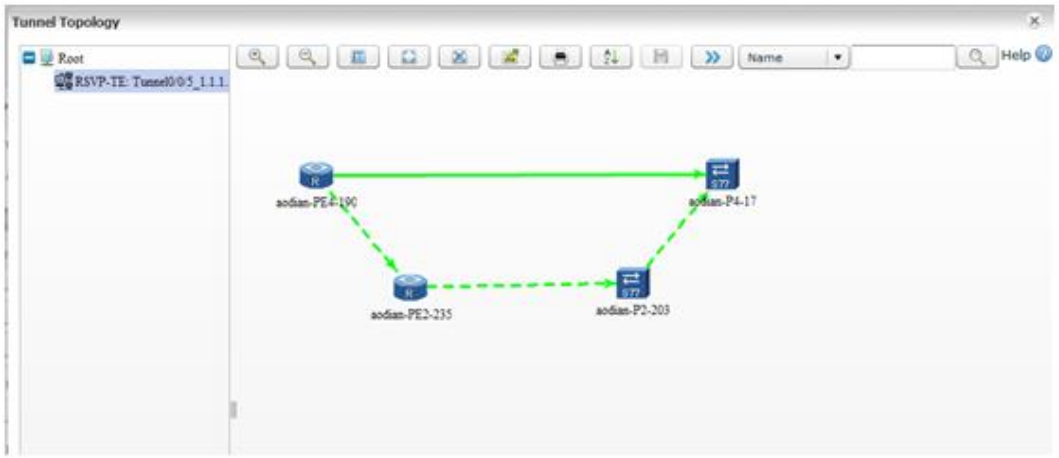
eSight supports active-standby and bypass protection for MPLS TE dynamic tunnels and monitors Static-CR signaling-based static tunnels. The following tunnel information is monitored: tunnel backup status, running status, and tunnel alarms.

eSight supports interaction between MPLS tunnels and L3VPN services and allows you to check VPN services carried on MPLS TE tunnels.

Tunnel Topology

eSight manages and monitors MPLS tunnels through tunnel topology and allows you to check the following:

Figure 4-111 Tunnel topology view



- MPLS capabilities of MPLS TE tunnels and interfaces, DS-TE information, and link bandwidth.
- MPLS capabilities of MPLS LDP virtual tunnels and interfaces.

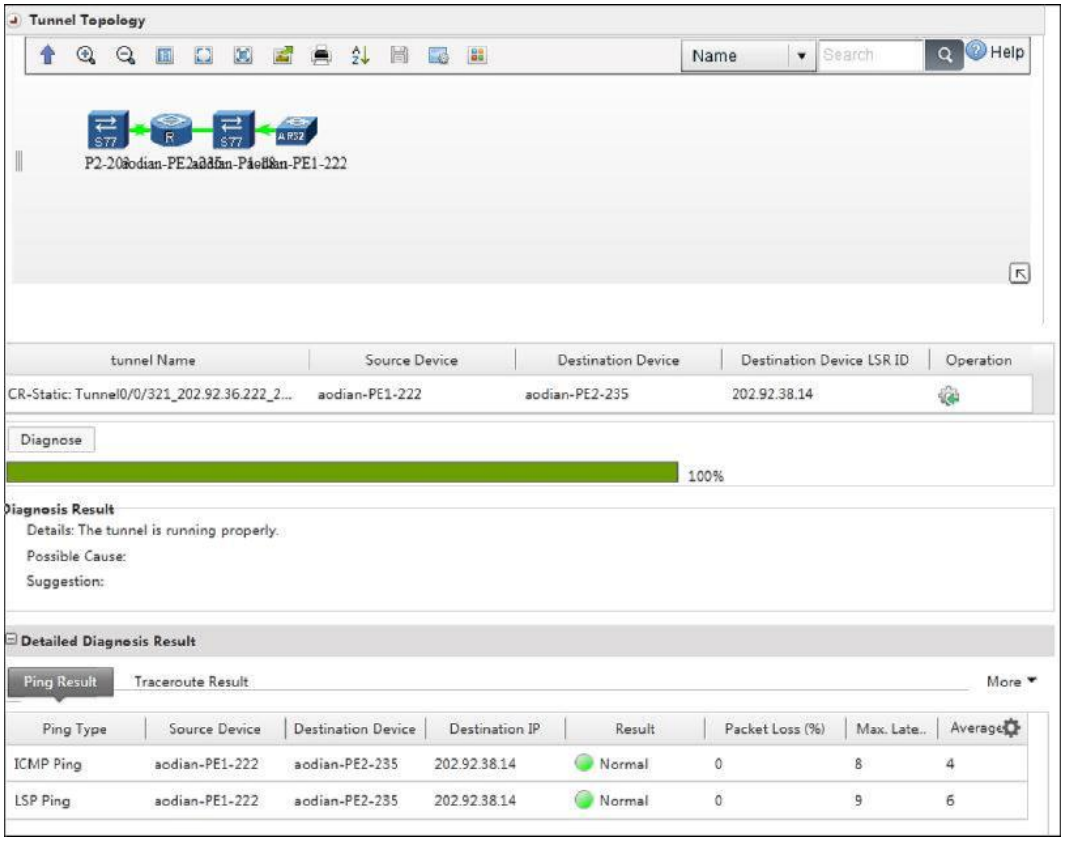
Explicit Path List

eSight provides an explicit path list. You can view the detailed information about each explicit path

Quick Diagnosis

eSight provides MPLS Tunnel quick diagnosis function, eSight can diagnose route forwarding, label forward, and tunnel configuration at tunnel nodes. If a fault occurs, eSight can diagnose and locate tunnel faults and give detailed diagnosis results. As shown in **Figure 4-112**.

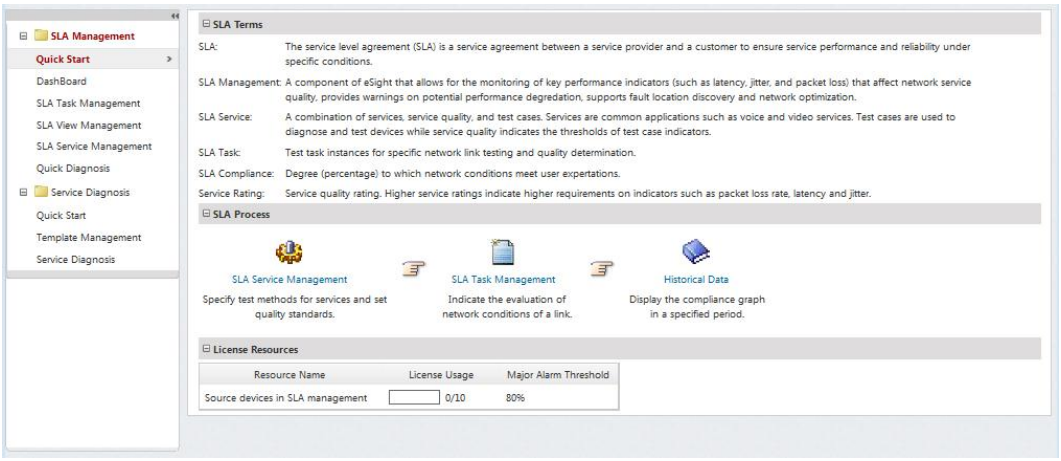
Figure 4-112 MPLS Tunnel quick diagnosis



4.3.6 SLA Management

Service Level Agreement (SLA) Manager measures and diagnoses network performance. You can create SLA tasks to periodically monitor the network delay, jitter, and packet loss, and calculate the compliance between SLA services and the live network. By default, SLA Manager offers 24 services. You can also customize services to meet your specific demands. SLA Manager offers the Dashboard to globally monitor SLA tasks and allows you to quickly learn about the quality of all or specific services on the live network. On the SLA view page, you can establish a view that consists of multiple tasks, which helps you to compare task data. Quick diagnosis helps you to quickly diagnose the links and carried services between source and destination devices, facilitating network fault location.

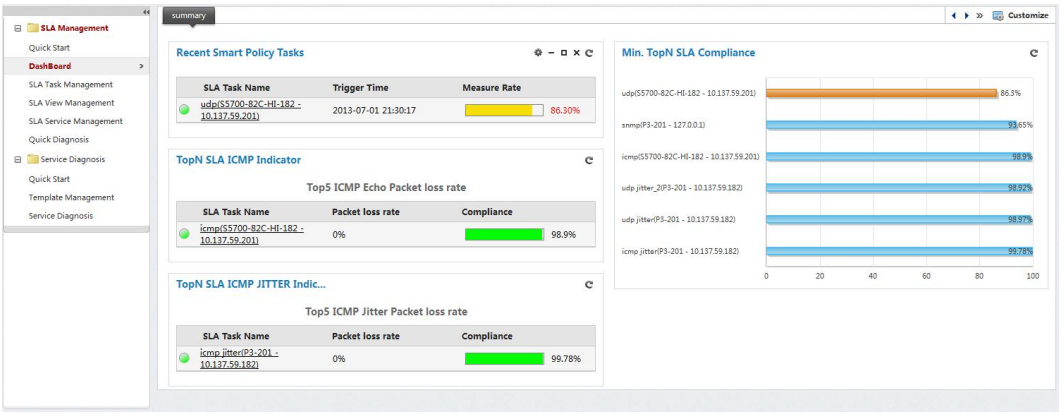
Figure 4-113 SLA management overview



Dashboard

The SLA dashboard globally monitors SLA tasks and displays the recent smart policy tasks, SLA test instance indicators, and minimum SLA compliance. You can add and delete dashboards and filter SLA tasks on the dashboard.

Figure 4-114 SLA Dashboard



SLA Service Management

With SLA service management, you can define SLA levels. More than 20 predefined templates are provided for common services such as voice over IP (VoIP), video, and data services. You can customize the compliance threshold and network quality counter threshold based on network conditions and operation and maintenance requirements.

Figure 4-115 SLA Srvice Management page

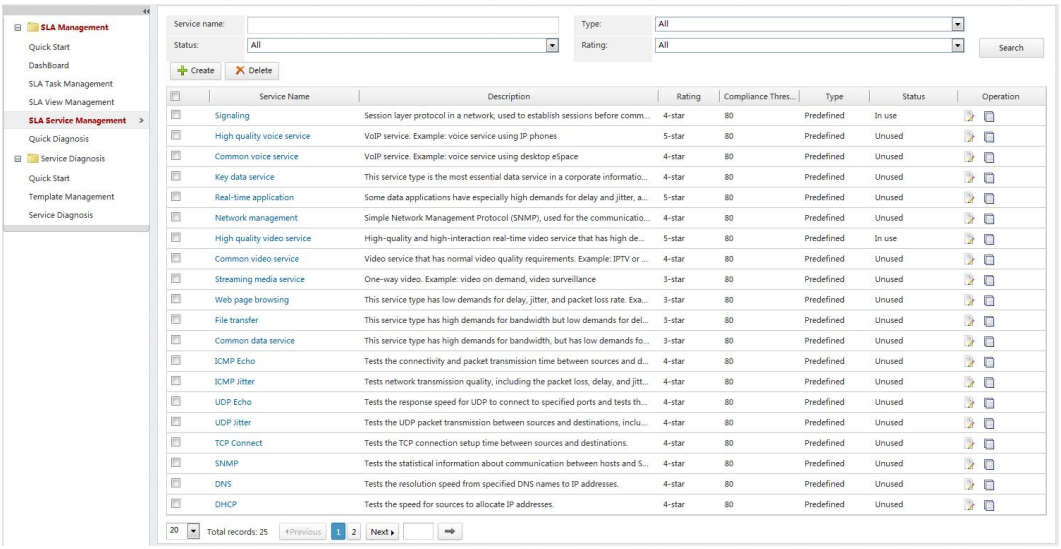
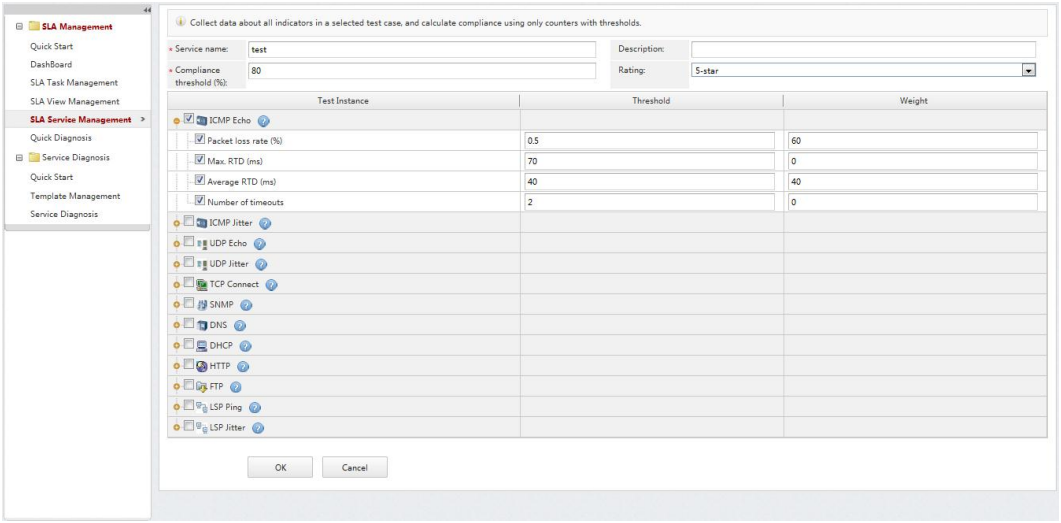


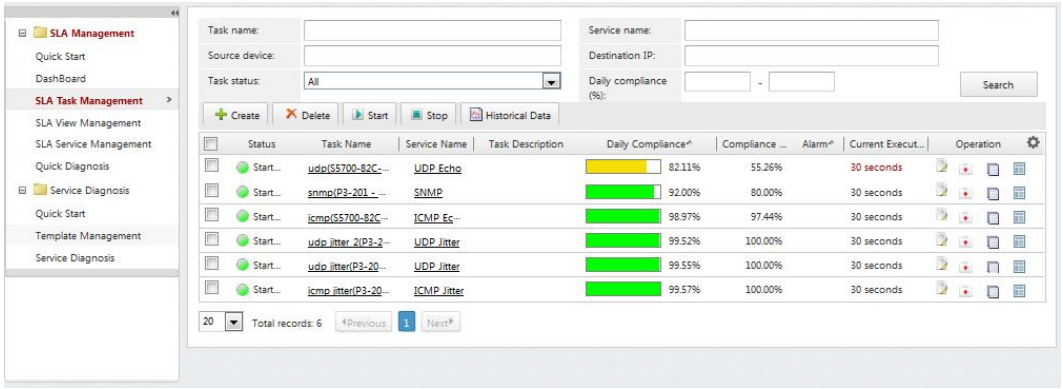
Figure 4-116 Creating an SLA service



SLA Task Management

eSight allows you to create, delete, start, and stop SLA tasks and copy an existing task to create a task. The SLA task execution interval can be adjusted automatically. When network quality degrades, the execution interval is shortened automatically to provide you with more quality degradation information.

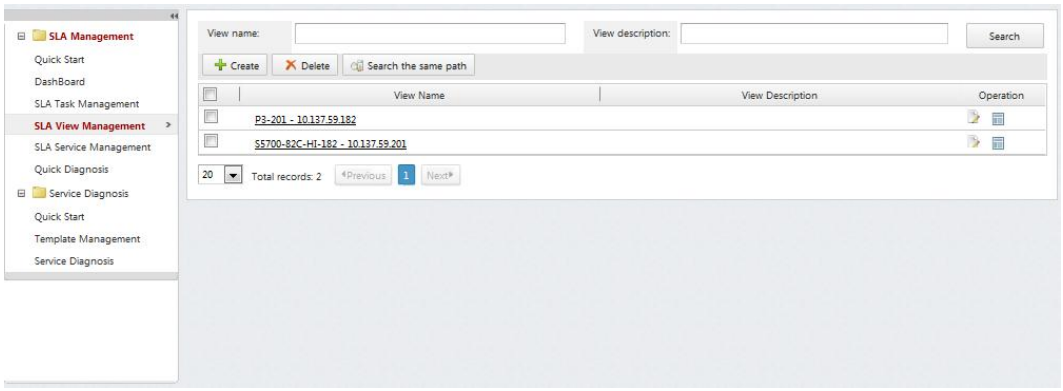
Figure 4-117 SLA Task Management page



SLA View Management

Multiple SLA tasks can be added to an SLA view, which enables you to view the historical data of multiple SLA tasks.

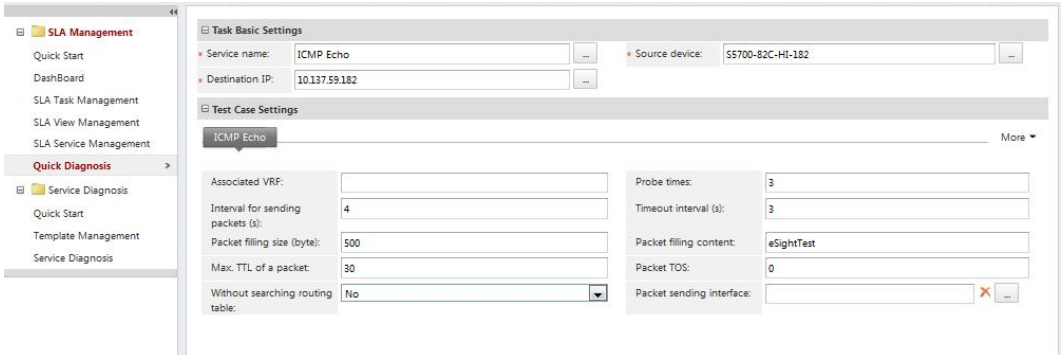
Figure 4-118 SLA View Management page



Quick Diagnosis

Quick diagnosis supports the function of checking the SLA service quality without creating any task.

Figure 4-119 Quick Diagnosis page



Historical Data

Historical service quality data such as the overall compliance and the data of a single counter is displayed in graphs.

Figure 4-120 Page for viewing historical data

The SLA view displays the historical data of multiple tasks.

Figure 4-121 Page for viewing the historical data of multiple tasks

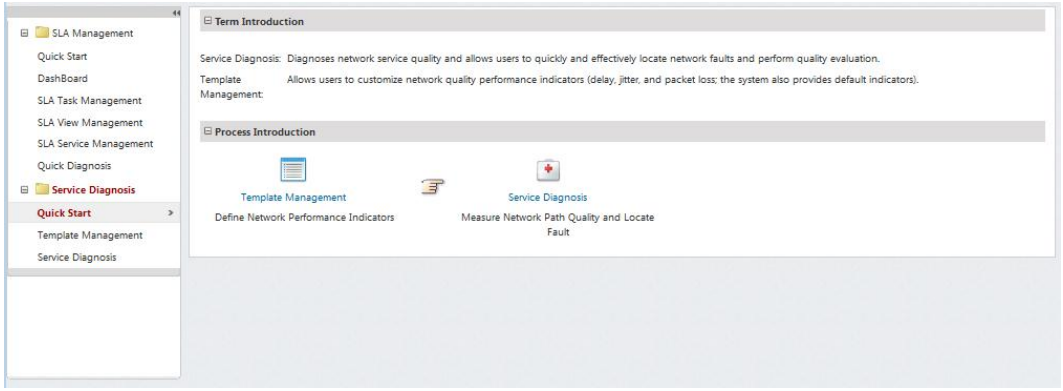
SLA Reports

You can export and print the SLA Service Quality Report, SLA Task Counter Reports, and TopN SLA Compliance Report.

Service Diagnosis

With service diagnosis, eSight detects network quality and displays collected data (such as the delay, jitter, packet loss rate, and DSCP value) by segment, helping you to assess service quality. eSight locates the network where a quality problem occurs based on statistical data, helping users rectify faults and ensuring service smoothness.

Figure 4-122 Quick Start



Template Management

eSight offers default network service quality assessment standards. You can also customize standard templates based on your site requirements.

(1) Telepresence diagnosis configuration template used to assess the network quality of telepresence systems.

(2) Desktop cloud diagnosis configuration template used to assess the network quality of desktop cloud systems.

Figure 4-123 Template management

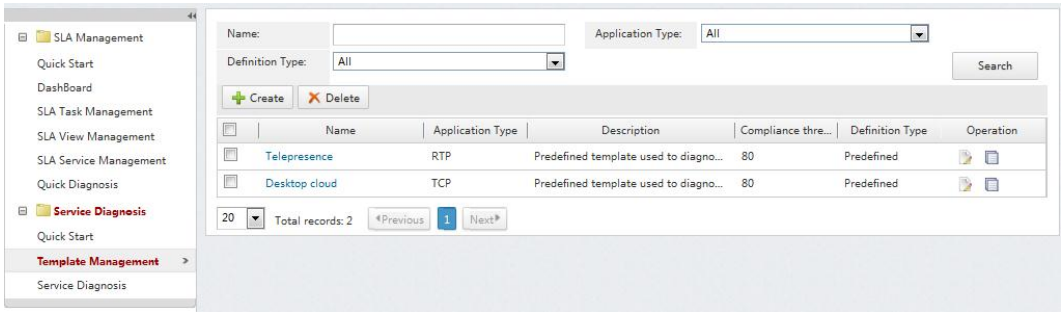
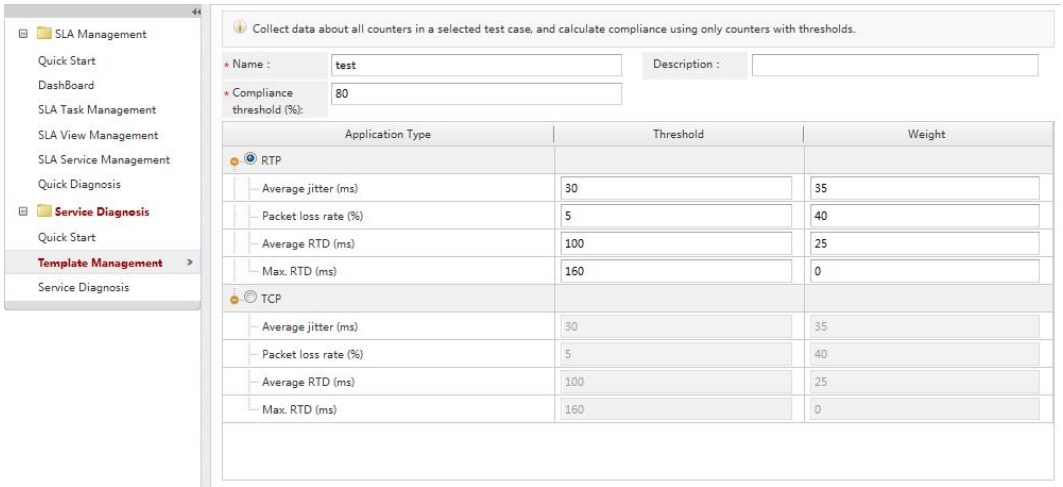


Figure 4-124 Creating a template

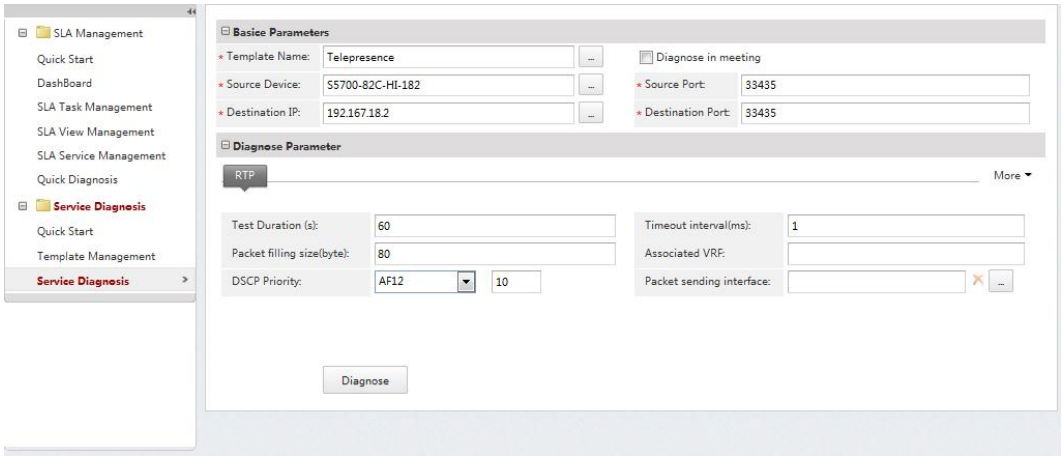


Service Diagnosis

eSight diagnoses the network service quality and allows users to efficiently locate network faults and assess network quality. Before performing service diagnosis, select the corresponding template.

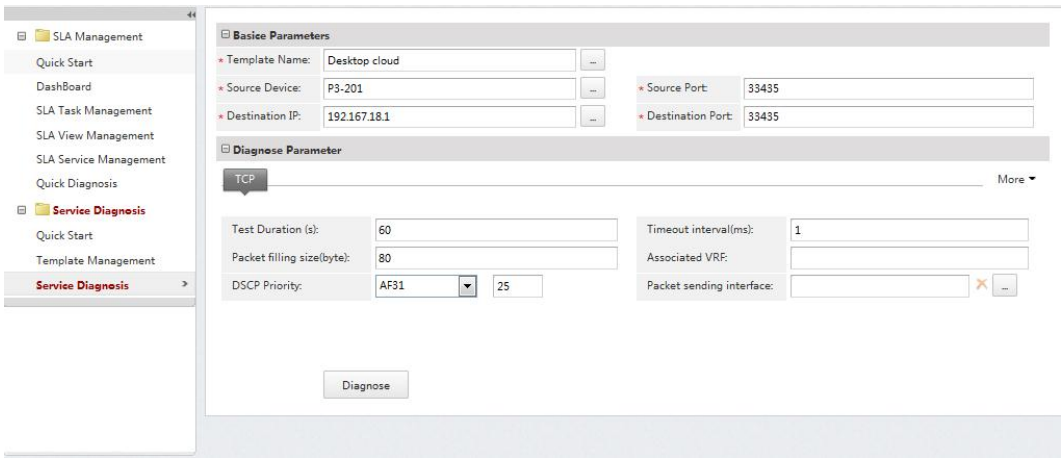
To perform telepresence diagnosis, select a telepresence diagnosis template.

Figure 4-125 Telepresence diagnosis parameters



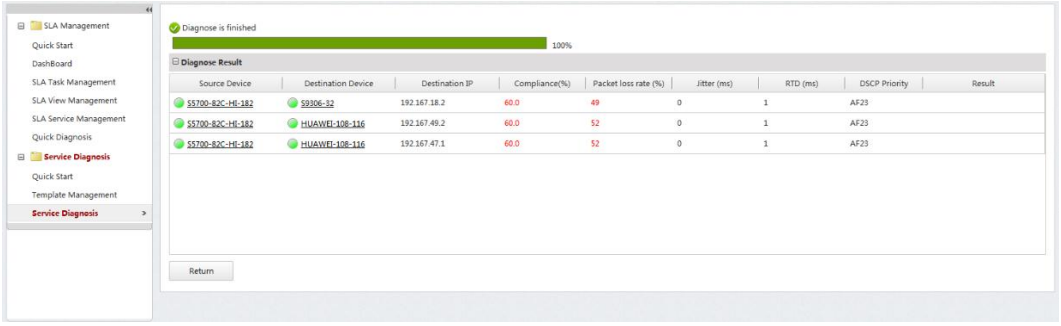
To perform desktop cloud diagnosis, select a desktop cloud template.

Figure 4-126 Desktop cloud diagnosis parameters



Diagnosis results are displayed by segment. Each record in the table indicates network conditions between source and destination devices.

Figure 4-127 Diagnosis result



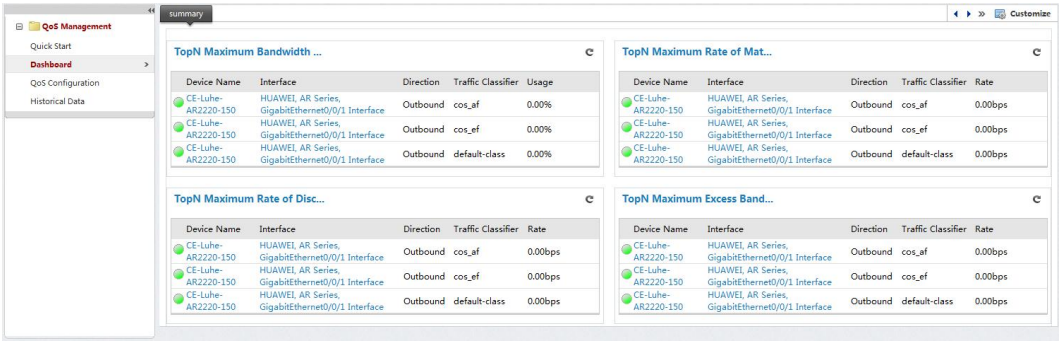
4.3.7 QoS Management

eSight provides QoS Manager to monitor traffic. When traffic policies are configured for interfaces, the tool measures network performance counters such as rate of matched bits, rate of discarded bits, excess bandwidth rate, and bandwidth usage for the interfaces.

Dashboard

The QoS dashboard displays the top 5 or 10 tasks with the highest QoS performance counters, which helps you find regions with excessively high traffic.

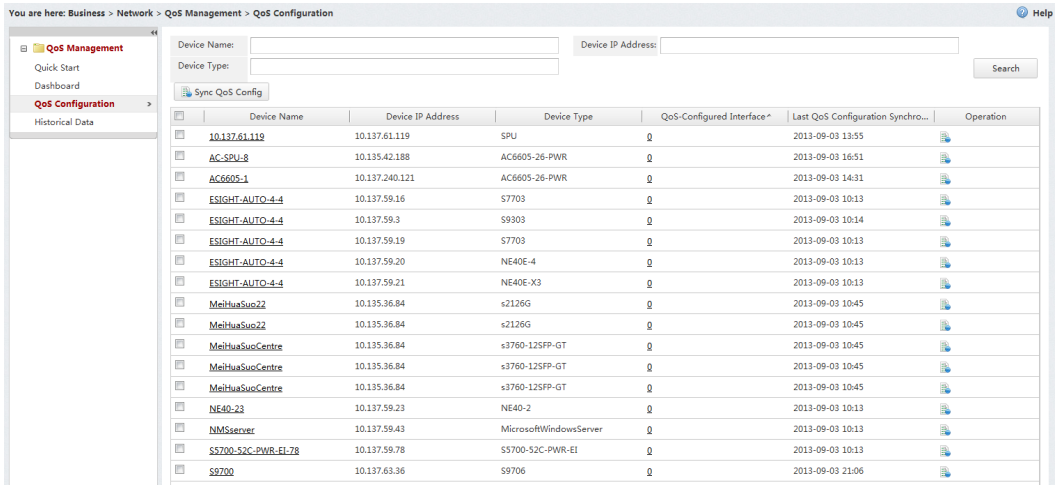
Figure 4-128 QoS Dashboard



QoS Configuration

Viewing QoS configuration of the devices.

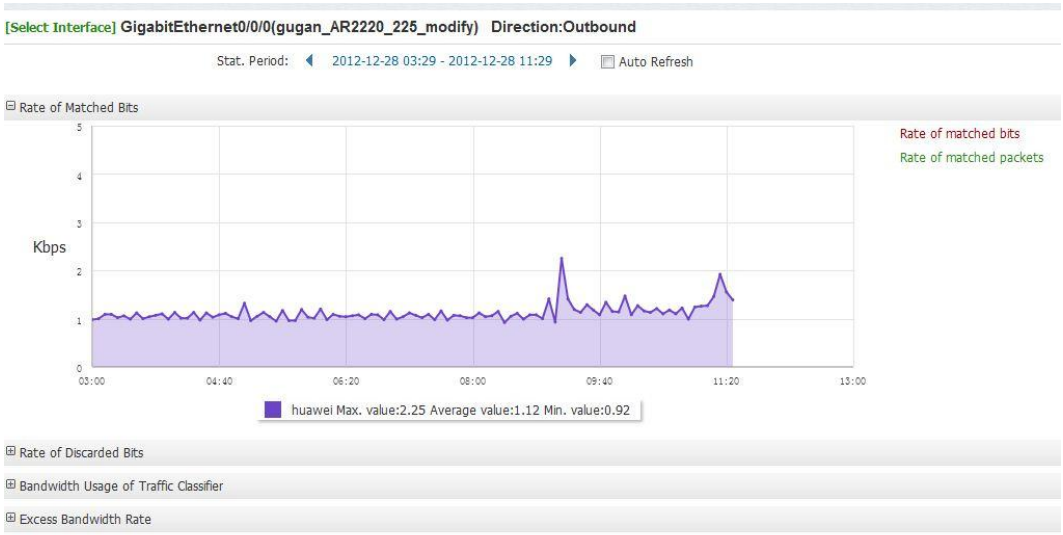
Figure 4-129 QoS Configuration



Historical Data

Historical QoS traffic data shows the change of QoS traffic.

Figure 4-130 Historical QoS data



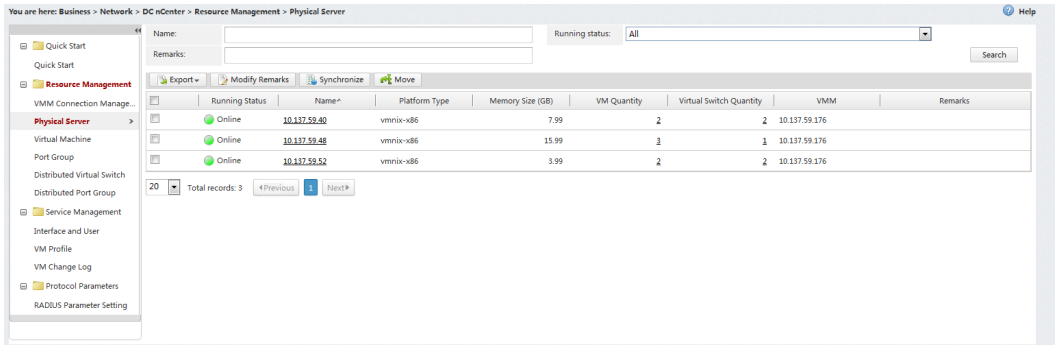
4.3.8 DC nCenter

DC nCenter delivers unified management of data center virtual networks. It monitors data center resources, dynamically detects virtual machine (VM) changes, automatically adjusts network policies and calculates topology paths, and displays the topology view of the entire data center network.

Resource Management

nCenter delivers unified management of virtual resources. With virtual resource management, you can:

Figure 4-131 Resource Management page

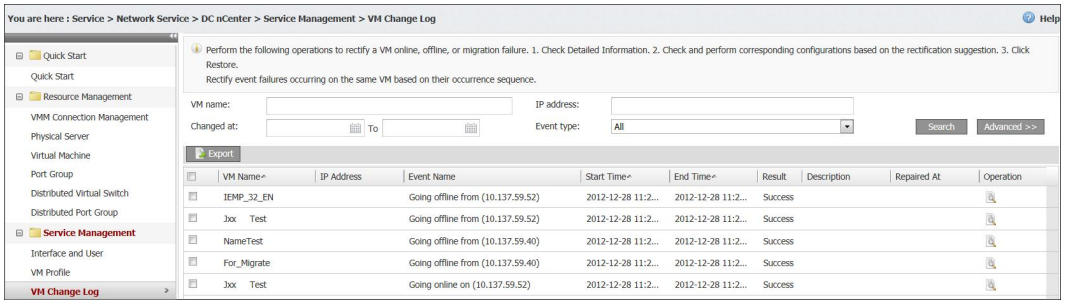


- Create a virtual machine manager (VMM). Then, nCenter automatically discovers and synchronizes all virtual resources in the VMM, including physical servers, VMs, standard virtual switches, and distributed virtual switches.
- Query and export information about the physical servers, VMs, port groups, distributed virtual switches, and distributed port groups in a VMM.
- Manually synchronize VMMs and physical servers either one after another or in batches.
- Create, delete, and modify standard virtual switches and port groups.
- Create, delete, and modify distributed virtual switches and port groups.

Service Management

nCenter configures services for virtual resources and manages VM change logs. With service management, you can:

Figure 4-132 Configuring services for virtual resources

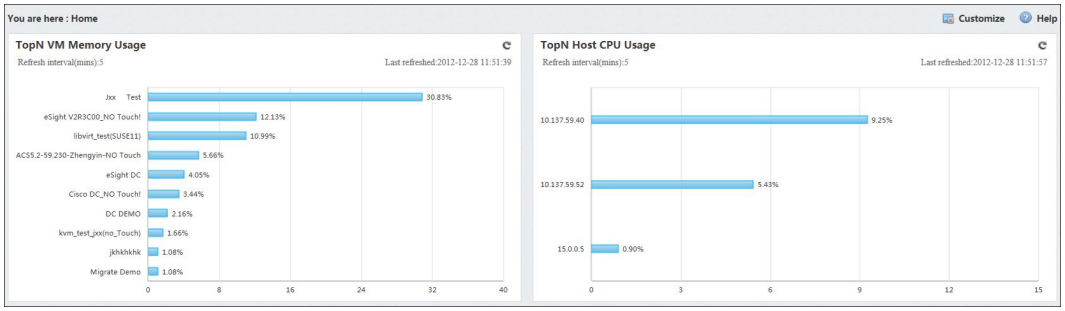


- Create a VM profile that contains physical network policies such as access control list (ACL) and quality of service (QoS) policies required by VMs.
- Bind a VM profile to a port group. Then, network policies can be delivered to devices uniformly.
- Check VM changes in the VM change logs and restore a VM profile.
- On the **Interface and User** page, check the detailed information about online VM users on a Top Of Rack (TOR) interface.

Service Monitoring

nCenter provides uniform virtual resource monitoring counters.

Figure 4-133 Monitoring services for virtual resources

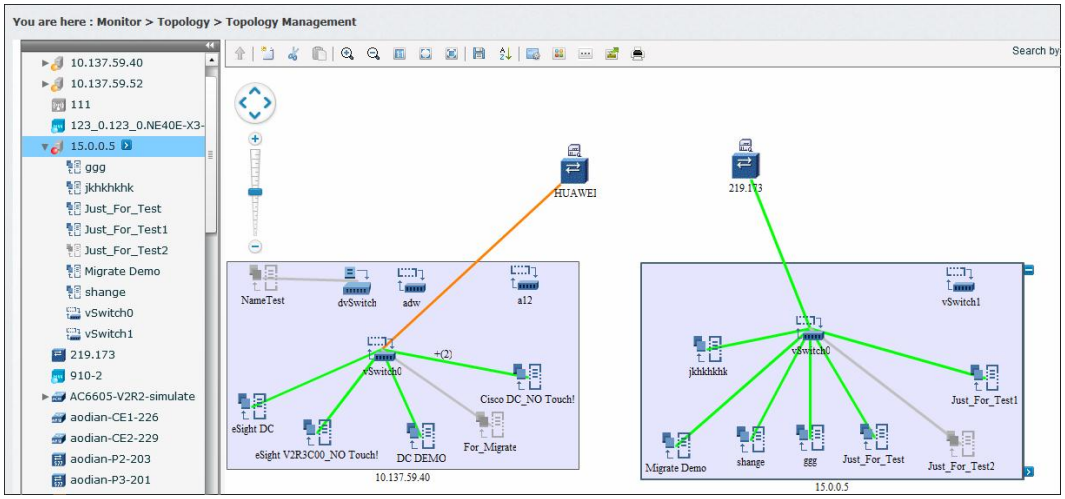


- With performance management, you can automatically or manually monitor performance counters, such as CPU usage, memory usage, disk IO rate, and network adapter IO rate, for physical servers and VMs.
- With alarm management, you can check alarms generated in a VMM.
- By customizing the portal, you can check the TopN performance counters of physical servers and VMs.

Topology View

nCenter allows you to view virtual resource relationships in topology views.

Figure 4-134 Topology view of virtual resource relationships



- With topologies, you can view the networking relationships between TOR switches, physical servers, standard virtual switches, distributed virtual switches, and VMs.
- Through topology redirection, you can view the detailed virtual resources and alarm list.

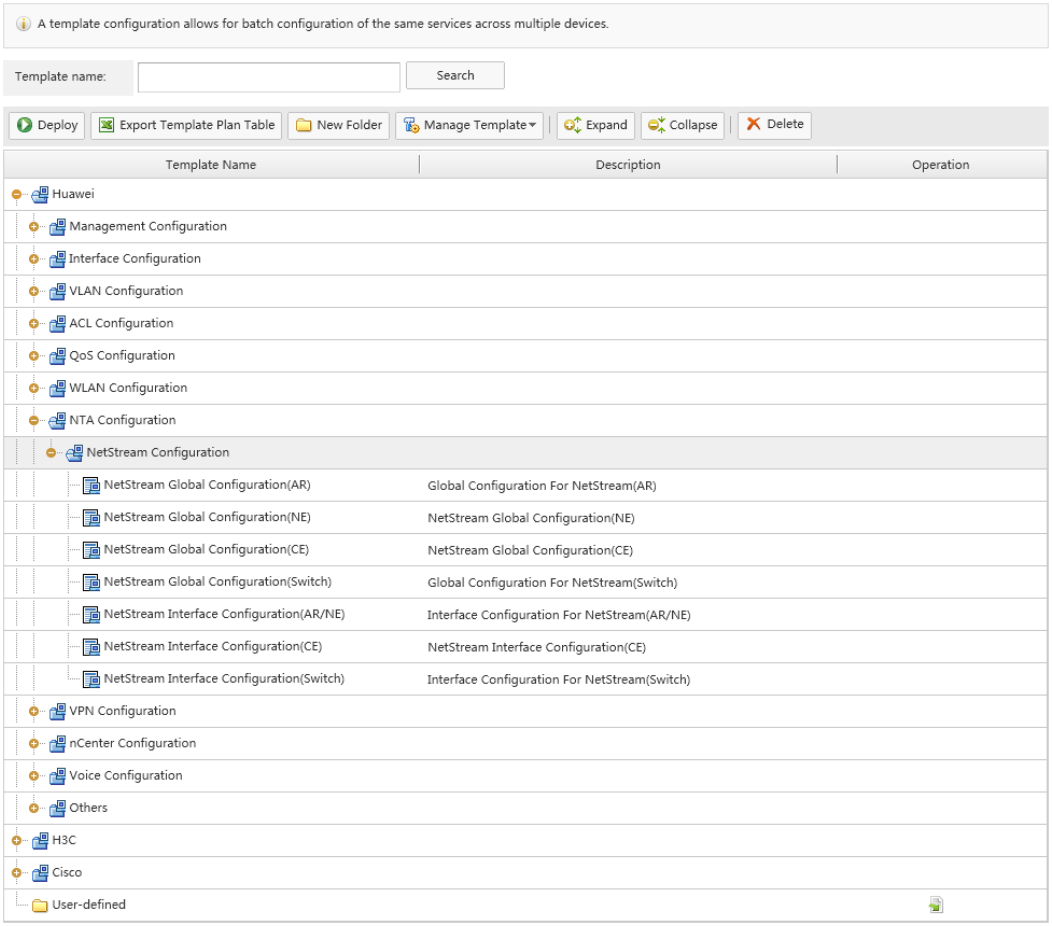
4.3.9 NTA

eSight Network Traffic Analyzer (NTA) can quickly and economically analyze network traffic and generate traffic reports. It enables users to detect abnormal traffic in a timely manner based on the real-time entire-network application traffic distribution and plan networks based on the long-term network traffic distribution. Therefore, NTA can implement transparent network management.

Enabling Device Interface NetStream

NetStream commands are delivered to devices through the smart configuration tool. Users do not need to configure NetStream on each device, which facilitates quicker deployment.

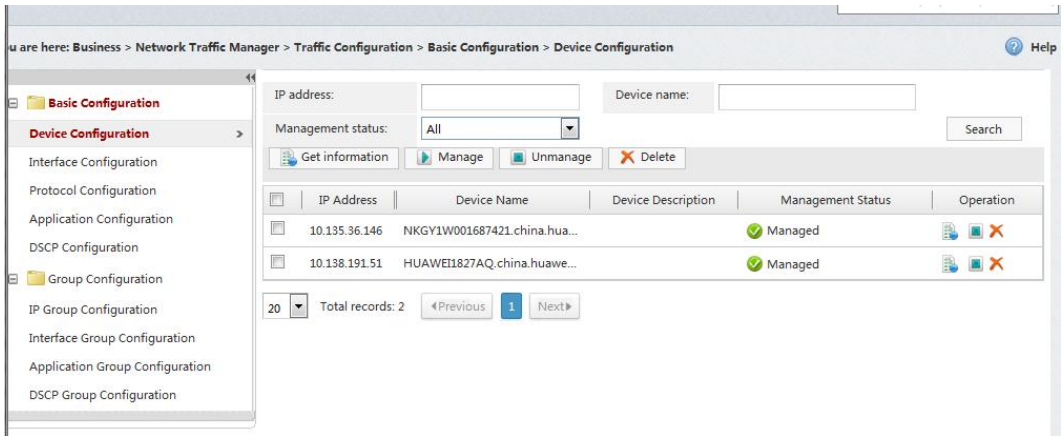
Figure 4-135 Enabling interface NetStream



Configuration Management

eSight NTA allows users to configure devices, interfaces, protocols, applications, DSCPs, IP groups, application groups, interface groups, and DSCP groups.

Figure 4-136 NTA device configuration wizard page



- Device configuration

  Displays all devices that report traffic. Users can monitor specific devices.

- Interface configuration

  Displays network-wide interfaces with network traffic. Users can configure the interface incoming traffic rate, outgoing traffic rate, and sampling rate to ensure network traffic data correctness. The sampling rate on eSight and devices must be set to the same value to show the actual network traffic.

- Protocol configuration

  Allows users to monitor specific protocols.

- Network application:

  Lists 543 frequently-used network applications and classifies them into Layer 4, Layer 7, protocol, and user-defined applications. Users can define important applications.

  - Layer 4 application: A network application identified by one or more groups of fixed network protocols and communication ports.
  - Layer 7 application: A network application with random ports and identified by the packets at the application layer.
  - Protocol application: A network application identified by protocols rather than ports.
  - User-defined application: A network application that is added by users and can be defined in terms of the protocol (UDP/TCP), port range, and IP address range.

- DSCP configuration

  Lists 22 frequently-used DSCPs and allows users to rename DSCPs.

- IP group configuration

  Groups IP addresses that have certain common attributes, which helps users to view traffic information about IP address groups.

- Application group configuration

  Groups user-concerned applications and helps users to view traffic information about application groups.

- DSCP group configuration

  Groups DSCPs and helps users to view traffic information about DSCP groups.

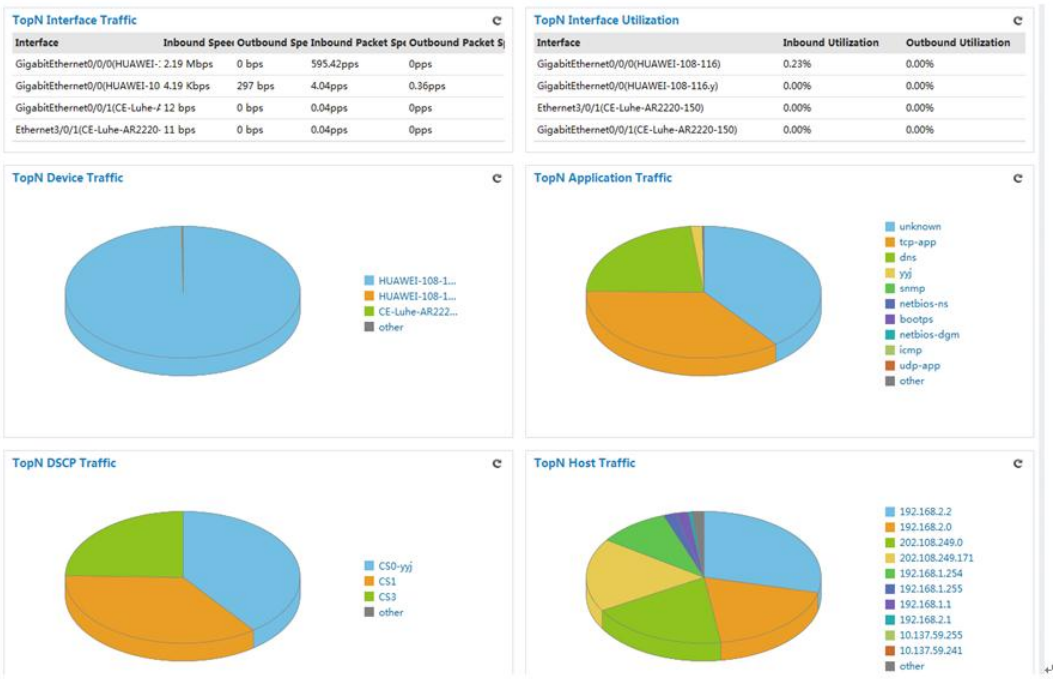
- Interface group configuration

  Groups related interfaces and helps users to view traffic information about interface groups.

Traffic Dashboard

NTA provides the traffic dashboards function and displays the real-time entire-network traffic, as shown in **Figure 4-137**.

Figure 4-137 Traffic analysis by Dashboard



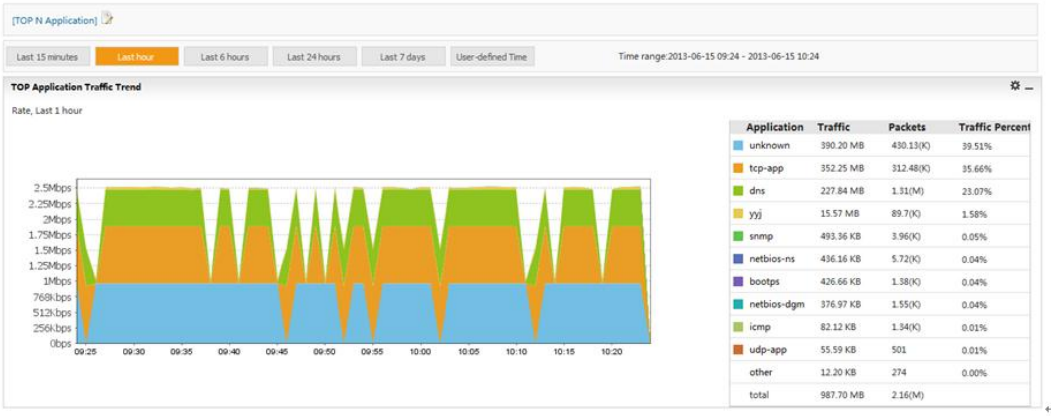
- The dashboard offers rankings about the interface traffic, interface utilization, device traffic, application traffic, host traffic, DSCP traffic, and session traffic.
- You can customize the display format and content. The following operations are available: Tool tips, links, switching between figures and tables, maximize, and minimize.

Traffic Analysis

eSight NTA offers drill-down network traffic analysis capabilities. Users can view more details about traffic step by step. eSight NTA allows users to view details traffic information about devices, interfaces, applications, DSCPs, hosts, sessions, interface groups, IP groups, and application groups.

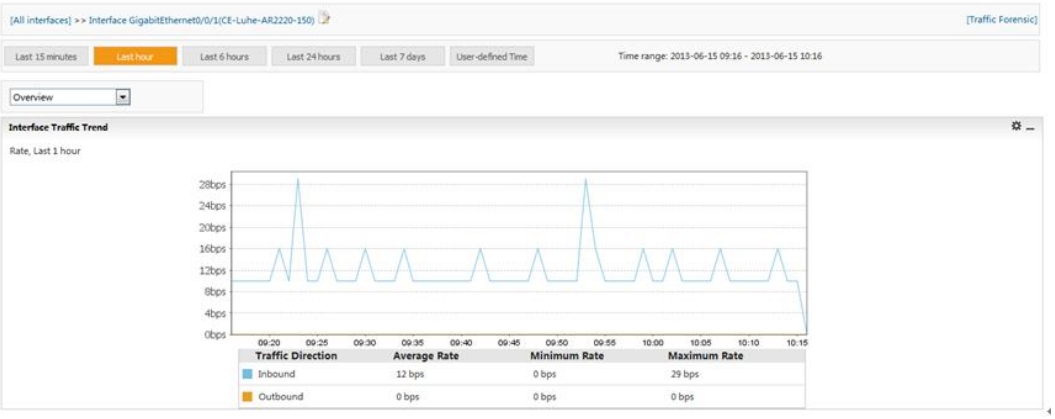
Users can view network-wide traffic information. The following figure takes example of application traffic analysis.

Figure 4-138 Application traffic analysis



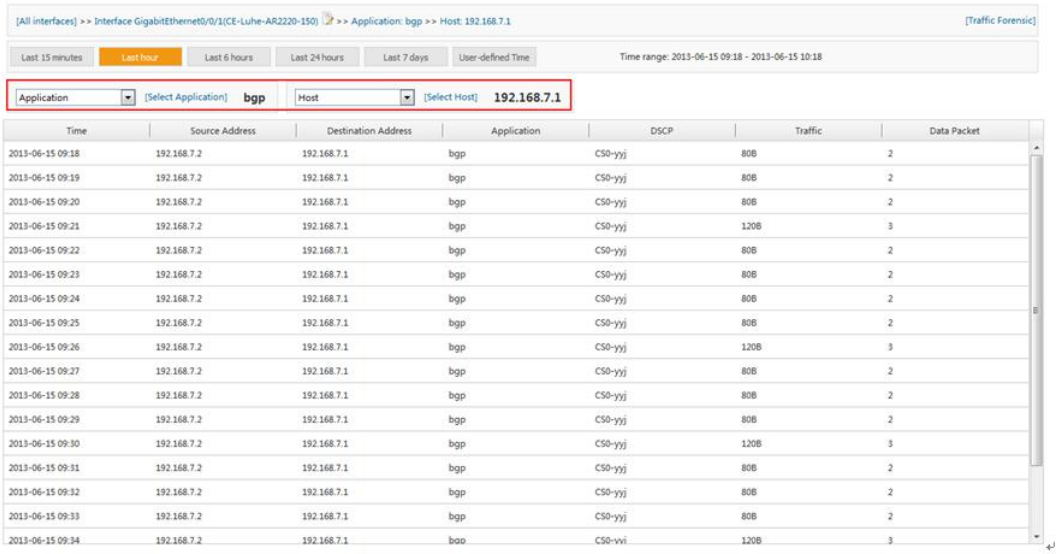
Users can view drill-down data. The following figure takes example of interface traffic analysis.

Figure 4-139 Interface traffic analysis



In addition, users can set filter criteria to view session details.

Figure 4-140 Session details



Network Traffic Report

NTA allows users to customize traffic reports as required. NTA provides the function of exporting reports. **Figure 4-141** and **Figure 4-142** shows how to create and view traffic reports.

Figure 4-141 Creating a network traffic report

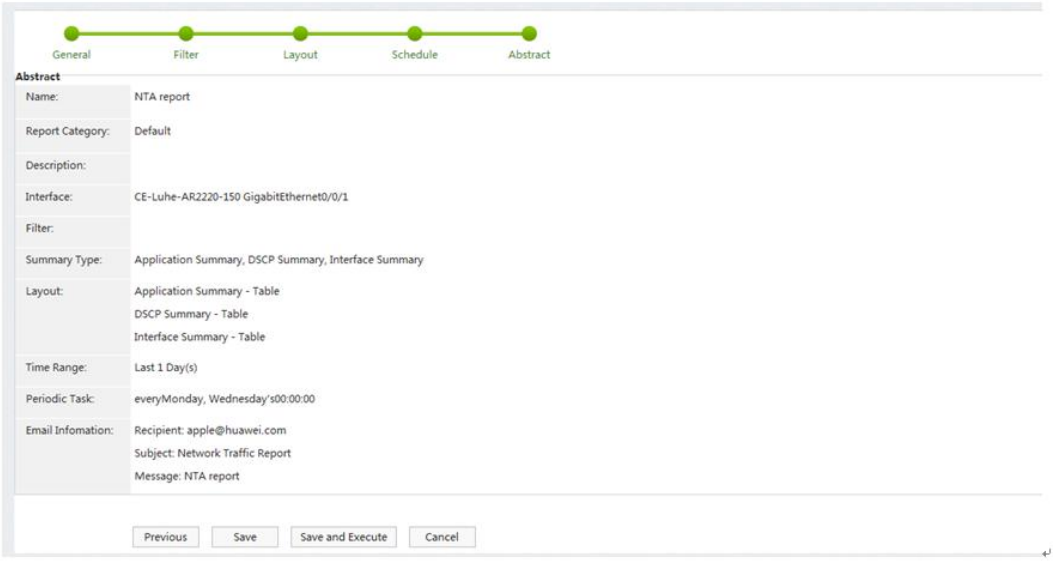
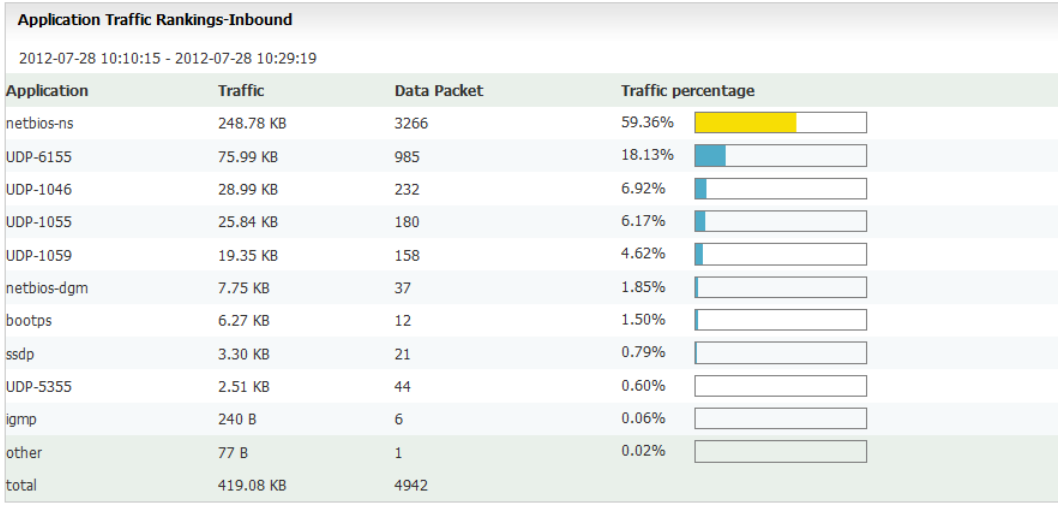


Figure 4-142 Viewing a network traffic report



Application Traffic Rankings-Inbound

2012-07-28 10:10:15 - 2012-07-28 10:29:19

Application	Traffic	Data Packet	Traffic percentage
netbios-ns	248.78 KB	3266	59.36%
UDP-6155	75.99 KB	985	18.13%
UDP-1046	28.99 KB	232	6.92%
UDP-1055	25.84 KB	180	6.17%
UDP-1059	19.35 KB	158	4.62%
netbios-dgm	7.75 KB	37	1.85%
bootps	6.27 KB	12	1.50%
ssdp	3.30 KB	21	0.79%
UDP-5355	2.51 KB	44	0.60%
igmp	240 B	6	0.06%
other	77 B	1	0.02%
total	419.08 KB	4942	

- Supports multiple modes to display the traffic data: Pie, Chart, Table, Line, Graph, and Region.
- Supports multiple summary types: Application summary, Session summary, DSCP summary, Source host summary, Destination host summary, and Interface summary.
- Supports multiple filtering conditions: by source address, by destination address, by application, and by DSCP.
- The report system can generate instant reports and periodical reports.
  - Instant report

    After you perform a task manually, the instant report statistics is displayed. After the task is performed successfully, the status is displayed on the page. You can open the report to view detailed traffic statistics.
  - Periodical report

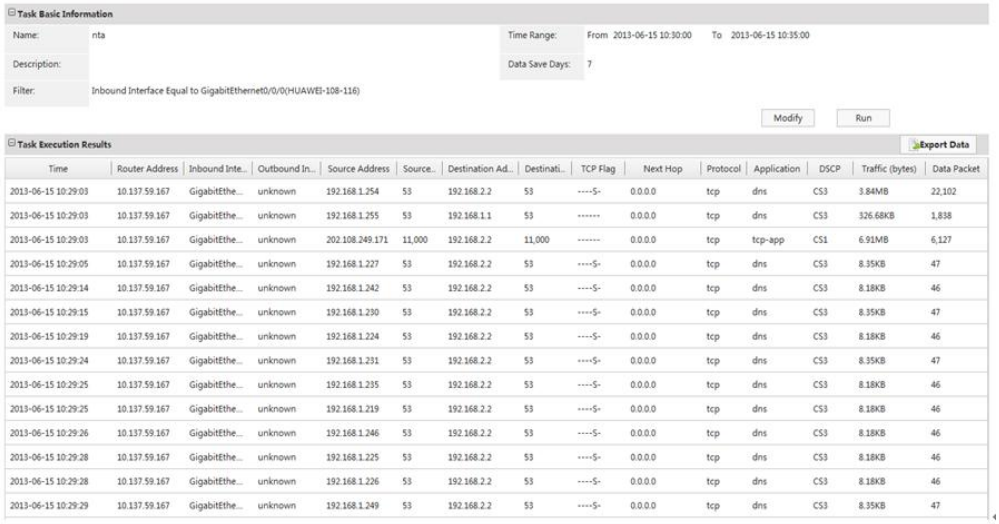
    After the system performs a task at an interval specified by the user, traffic statistics of this specified period is displayed.
- Supports batch report export.
- Sends reports by email.

Traffic Forensics

When detecting abnormal traffic in the network, the system allows users to obtain original traffic data which helps users to locate the network fault.

The system displays traffic forensics results by seven key fields. For example, users can check whether viruses exist by comparing protocols, ports, and packet rates, and check whether protocol attack threats exist by TCP flags.

Figure 4-143 Traffic forensics page



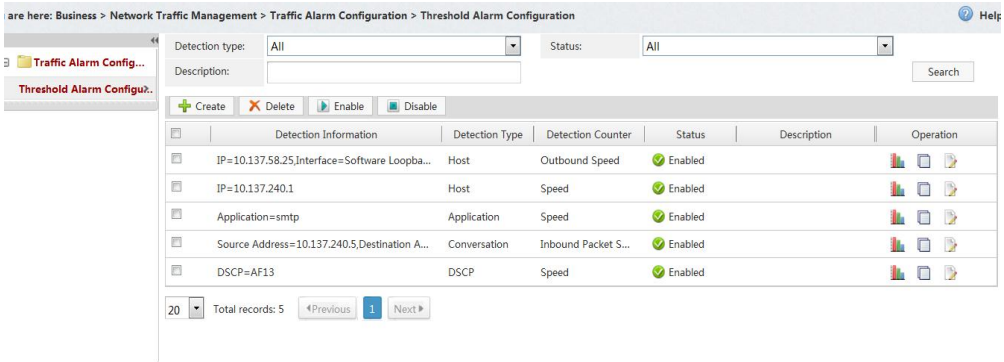
- Obtains original packets by time range.
- Supports diverse filter criteria: source IP address, destination IP address, source interface, destination interface, source port, destination port, protocol, application, DSCP, and TCP tag.
- Sets the storage duration (maximum: 30 days) for query results.
- Exports all or specified query results.

Traffic Alarm

You can create threshold alarms for seven traffic types, including the application, server, and session. When the traffic has reached the threshold for specified times within a specified time segment, an alarm is automatically generated. When the traffic meets alarm clearance conditions within a specified time segment, the alarm is automatically cleared. eSight can notify you of alarm generation or clearance by email.

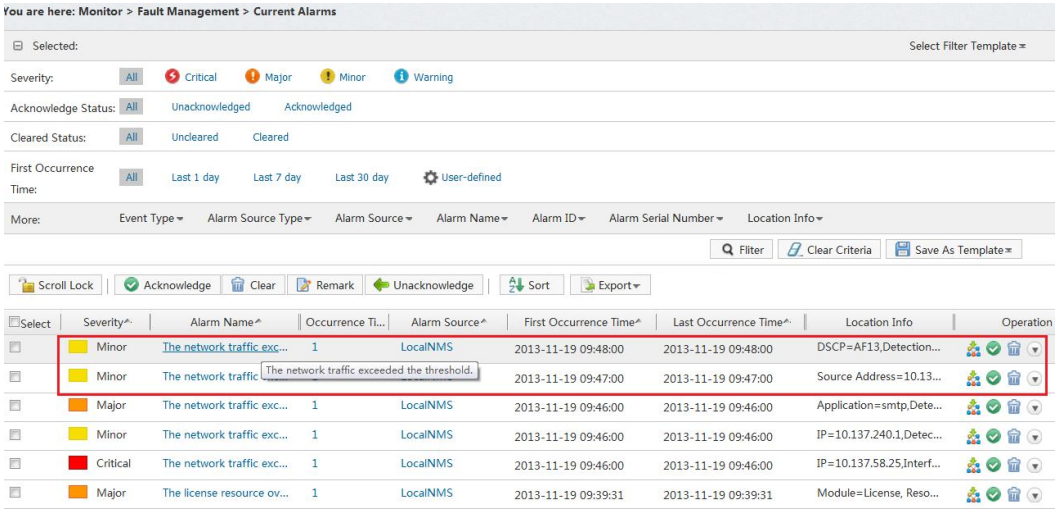
You can manage (create, copy to create, delete, enable, and disable) threshold alarms on the traffic threshold alarm configuration page. You can choose the objects to monitor, and set the alarm severity, threshold, and repetition times based on the historical traffic data.

Figure 4-144 Threshold alarm configuration page



You can check traffic alarms on the current alarm page, and go to the traffic analysis page to view traffic details within the time segment when alarms are generated.

Figure 4-145 Checking traffic alarms



4.3.10 Secure Center

The Secure Center effectively manages security policies on a large number of Huawei firewalls, switches, and routers. Main functions are as follows:

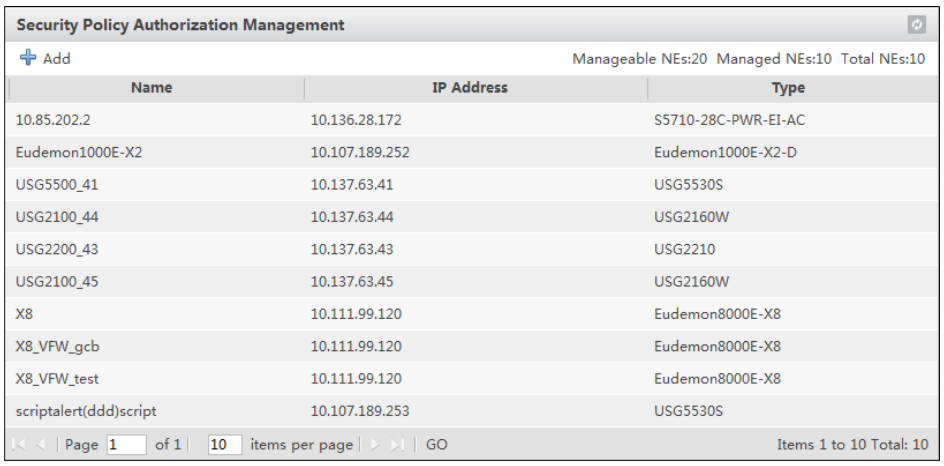
- Security policy analysis
  - Supports redundancy, risk, hit, and comprehensive analysis on security policies for firewalls.
- Firewall security policy management
  - Supports batch configuration and deployment of firewall security policies, IPS policies, and AV policies.
  - Supports centralized configuration of common objects, such as address sets, time ranges, services
  - Supports virtual firewall management and virtual firewall-based security policy configuration.
- Access authentication policy management
  - Supports batch configuration and deployment of access authentication policies for switches.
  - Supports centralized configuration of user groups, RADIUS server groups, and access policy templates.
  - Supports consistency audit of access authentication policies.
- AR policy management
  - Supports centralized configuration and batch deployment of interzone security policies.
- ACL management
  - Supports centralized configuration of basic and advanced ACLs.

Basic Configuration

- Security policy authorization management

  You can query the devices that the Secure Center is authorized to manage through licenses.

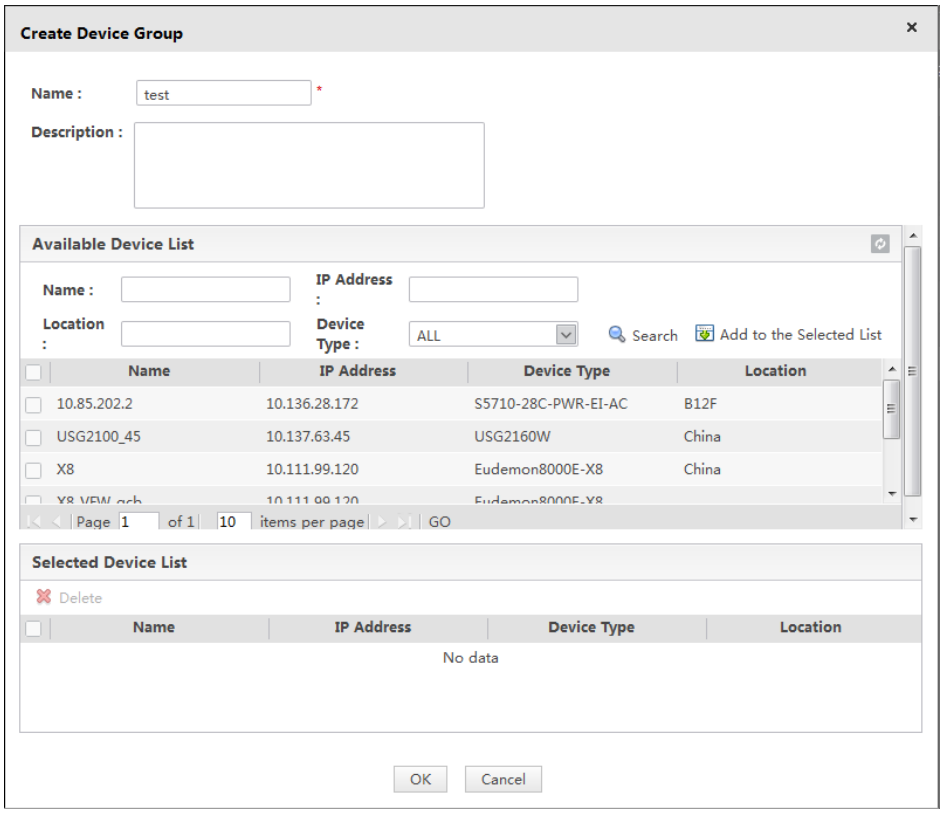
  Figure 4-146 Security policy authorization management



- Device group creation, deletion, modification, and query

  You can create, delete, modify, and query device groups.

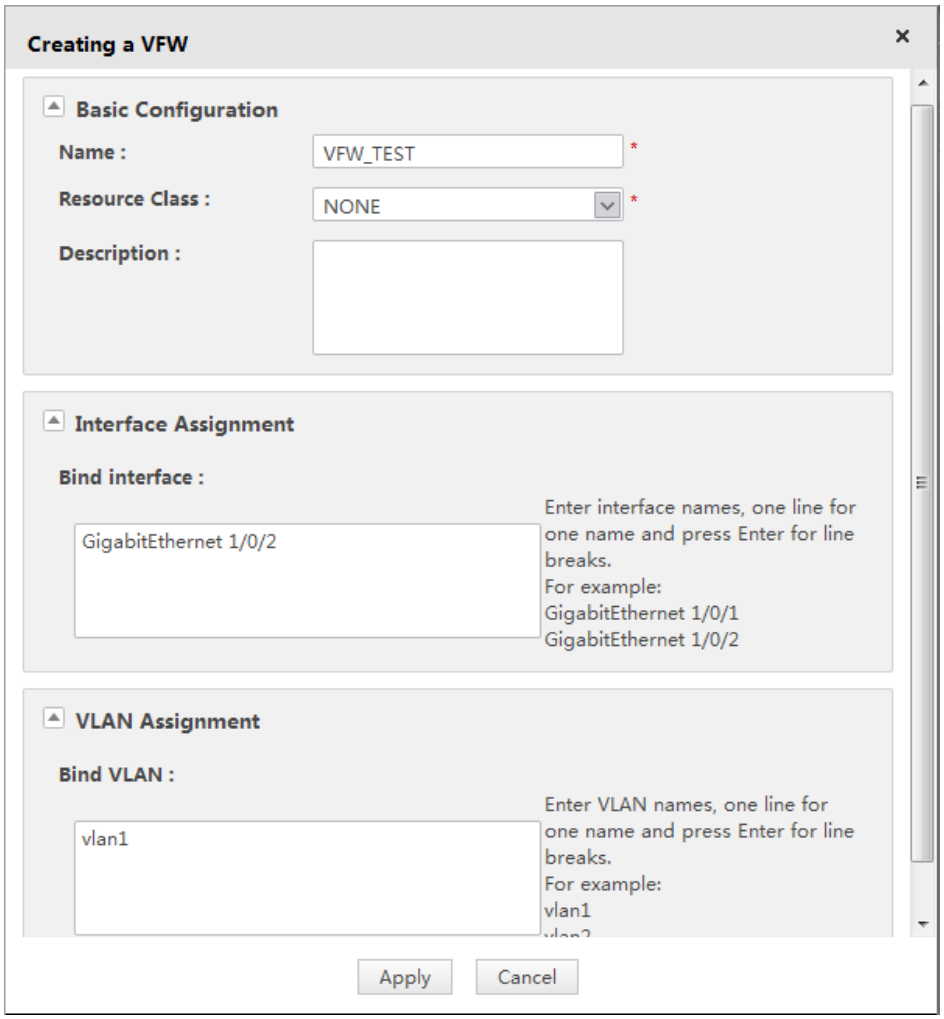
  Figure 4-147 Creating a device group



- Virtual firewall creation, deletion, and query

  You can create, delete, and query virtual firewalls.

Figure 4-148 Creating a virtual firewall



Security Policy Analysis

- Policy redundancy analysis

  The Secure Center can analyze the redundancy of security policies configured on the eSight and firewalls. Using an efficient redundancy analysis algorithm, the Secure Center can obtain the number of totally redundant policies, partially redundant policies, and non-redundant policies. A maximum of 20 devices can be analyzed at a time. The analysis result is displayed using a grouping histogram to show top 5 devices with totally redundant, partially redundant, or non-redundant policies.

  Policy redundancy details are displayed in either of the following modes:

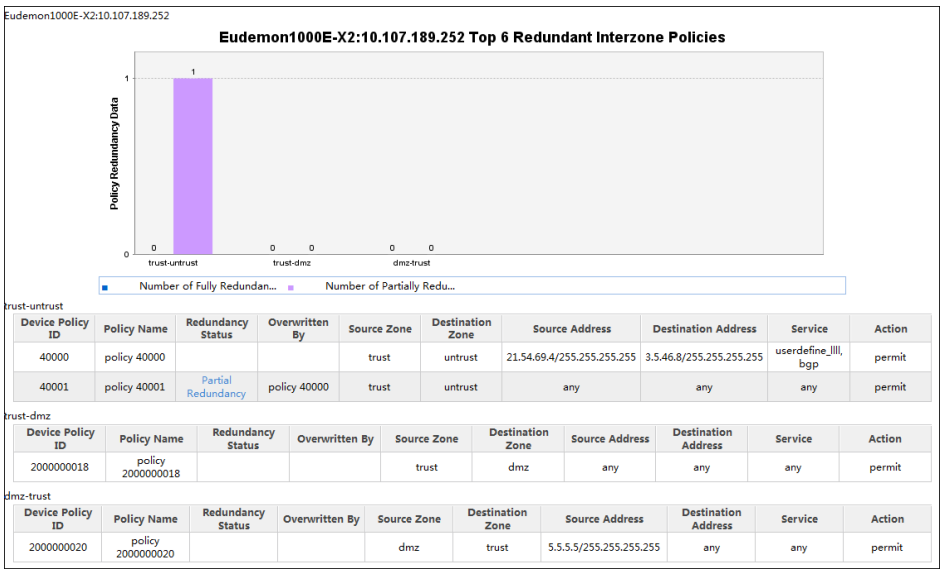
  - PDF file for a scheduled analysis task

    The PDF file lists all device interzone policy redundancy conditions in tables based on interzones and displays the policy redundancy status (either total redundancy or partial redundancy). For a redundant policy, the overlapping policies are provided.

- Web page for an immediately executed analysis task

  You can query the policy redundancy condition of a specific device or detailed redundancy condition of a specific policy.

Figure 4-149 Policy redundancy analysis result

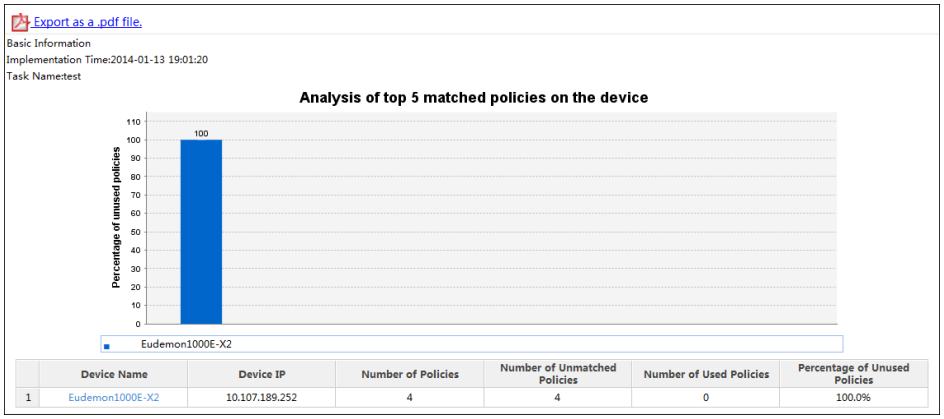


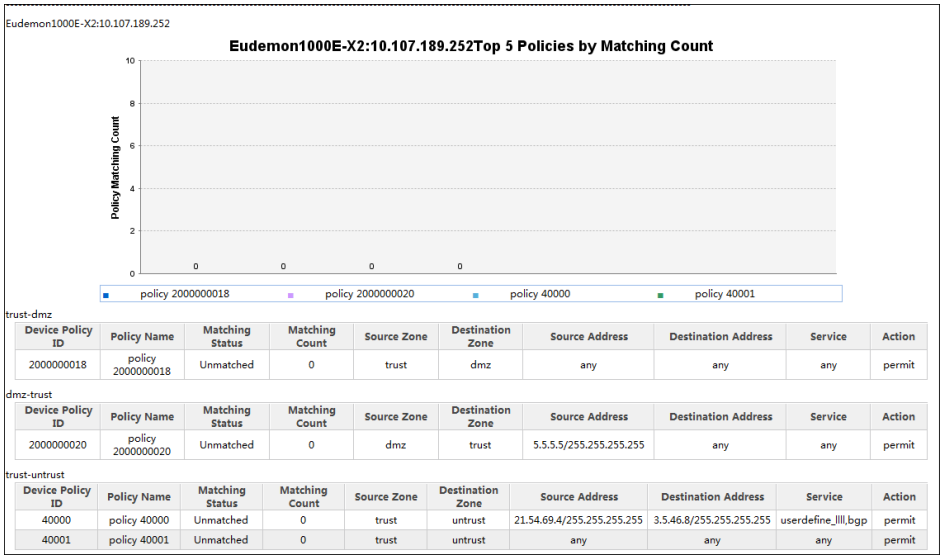
- Policy hit analysis

  The Secure Center can read the device policy hit data to analyze policy hit conditions for a maximum of 20 devices each time. The policy hit analysis result is displayed based on interzones in terms of the hit times and details about common objects configured for the policies.

  The policy hit analysis can be displayed in either of the following modes: PDF file and web page. The web page mode provides more interactive functions. You can query the policy hit condition of a specific device.

Figure 4-150 Policy hit analysis result





trust-dmz

Device Policy ID	Policy Name	Matching Status	Matching Count	Source Zone	Destination Zone	Source Address	Destination Address	Service	Action
2000000018	policy 2000000018	Unmatched	0	trust	dmz	any	any	any	permit

dmz-trust

Device Policy ID	Policy Name	Matching Status	Matching Count	Source Zone	Destination Zone	Source Address	Destination Address	Service	Action
2000000020	policy 2000000020	Unmatched	0	dmz	trust	5.5.5.5/255.255.255.255	any	any	permit

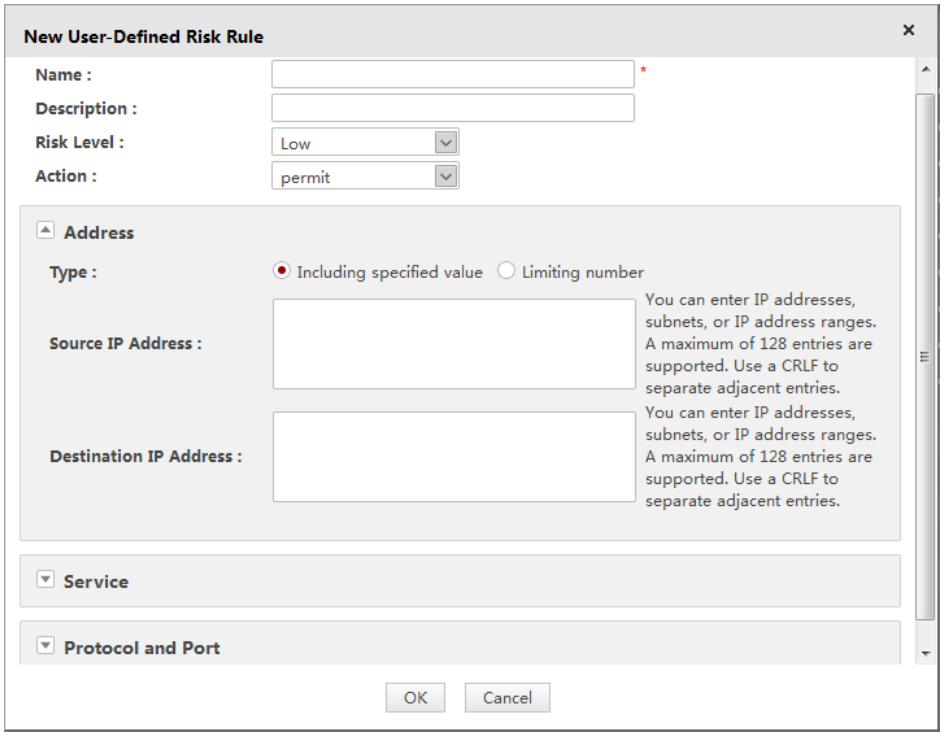
trust-untrust

Device Policy ID	Policy Name	Matching Status	Matching Count	Source Zone	Destination Zone	Source Address	Destination Address	Service	Action
40000	policy 40000	Unmatched	0	trust	untrust	21.54.69.4/255.255.255.255	3.5.46.8/255.255.255.255	userdefine_llll,bgp	permit
40001	policy 40001	Unmatched	0	trust	untrust	any	any	any	permit

- Policy risk analysis

  The Secure Center can check whether the security policies configured on the eSight are risky. If you select to synchronize firewall data before executing the analysis task, the Secure Center can analyze the risks of security policies configured on the firewalls. Using a risk analysis algorithm and based on the specified risk analysis rules, the Secure Center determines a device with high, medium, or low risks. In addition to default user-defined risk rules, you can create user-defined risk rules. The Secure Center can analyze the policy risks of up to 20 devices each time. The analysis result is displayed using a grouping histogram to show top 5 devices and the number of high-risk, medium-risk, and low-risk policies and using tables to show the number of high-risk, medium-risk, and low-risk policies of all selected devices.

Figure 4-151 Creating a user-defined risk rule



Policy risk details are displayed in either of the following modes:

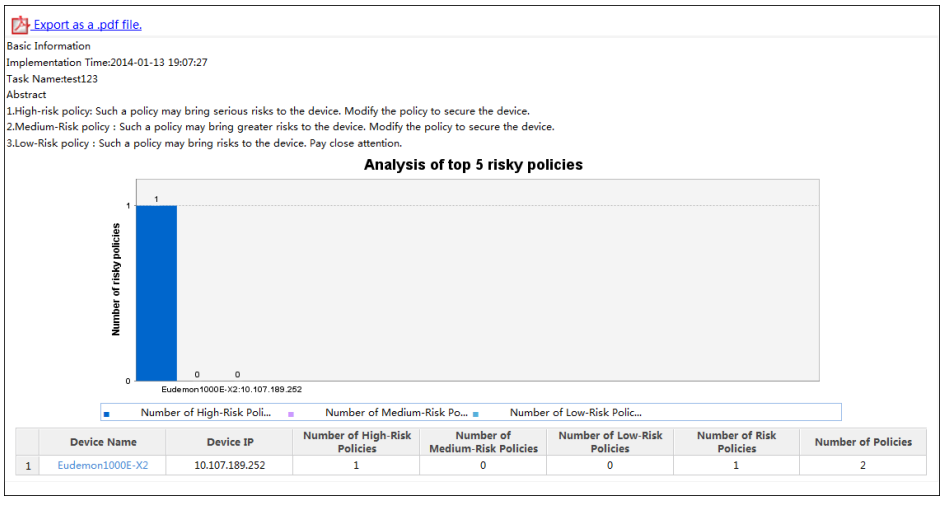
- PDF file for a scheduled analysis task

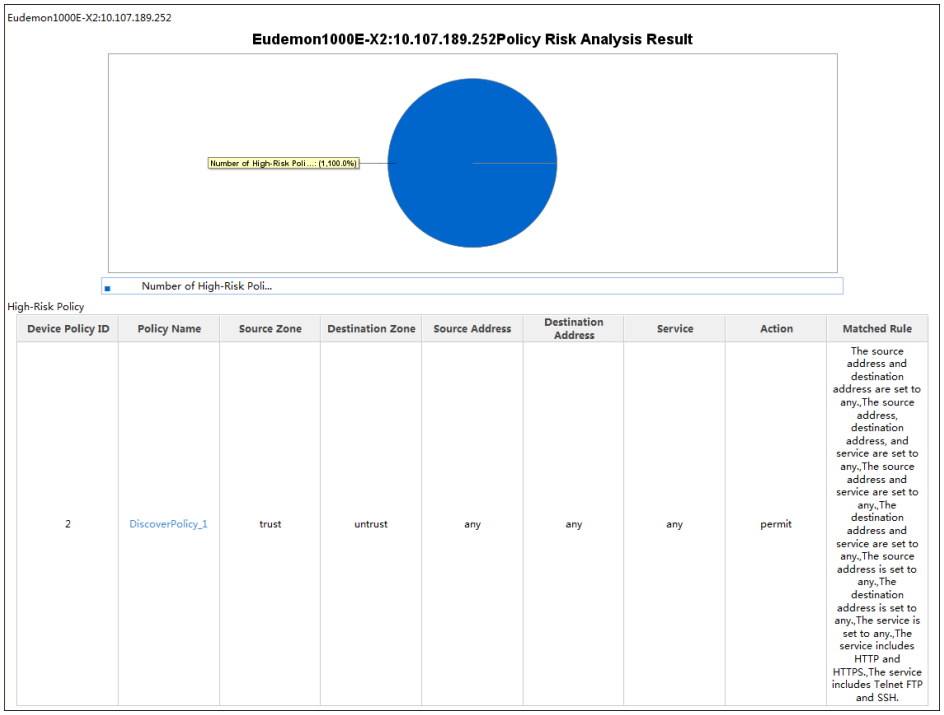
  The high-risk, medium-risk, and low-risk policies of all selected devices are listed in a PDF file.

- Web page for an immediately executed analysis task

  You can query the high-risk, medium-risk, and low-risk policies of a specific device. If needed, you can also query the risk rule matched by a risky policy.

Figure 4-152 Policy risk analysis result



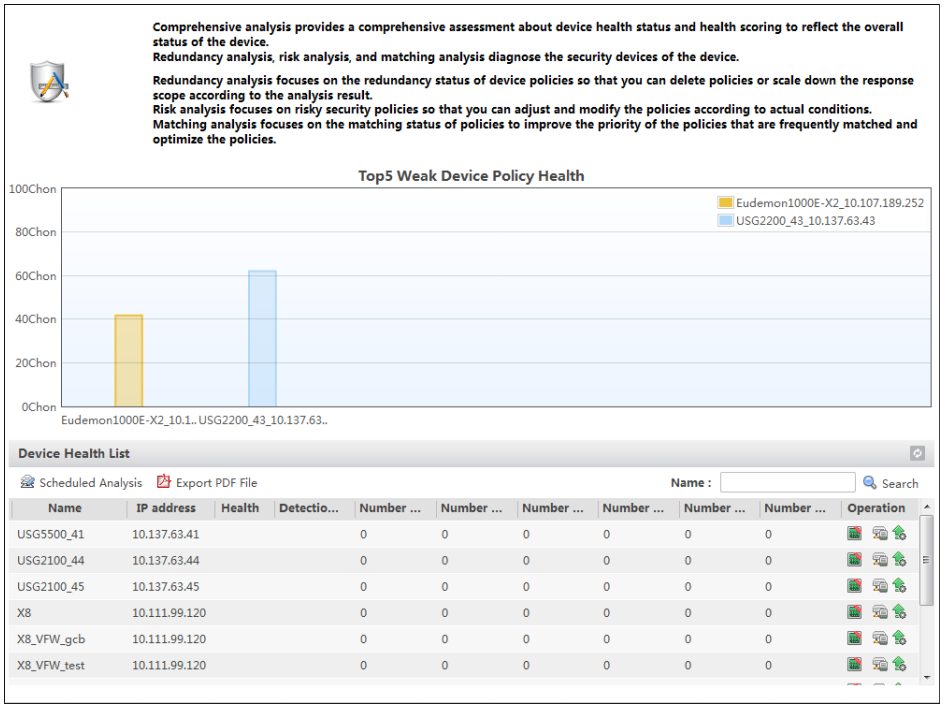


- Policy comprehensive analysis

  The Secure Center can comprehensively analyze firewall security policies. Based on the comprehensive analysis result (number of redundant policies, risky policies, and unmatched policies) and the health degree algorithm, the Secure Center provides a score for policy configuration on each firewall, helping the administrator understand the overall O&M condition of firewall policies.

  The comprehensive analysis task can be executed manually or periodically. The analysis result is displayed as lists and pie charts. You can obtain the device policy overview and device health degree historical curve and export the analysis result to a PDF report.

Figure 4-153 Comprehensively policy analysis result



Firewall Policy Management

- Common object configuration

  You can create, delete, modify, and query common objects, such as address sets, time ranges, and services, in a centralized manner.

Figure 4-154 Creating an address set

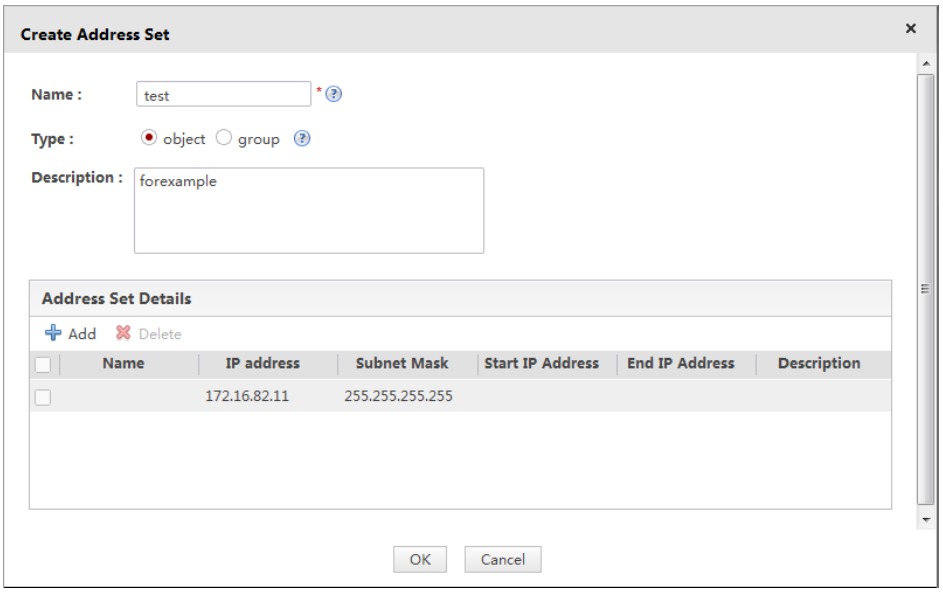
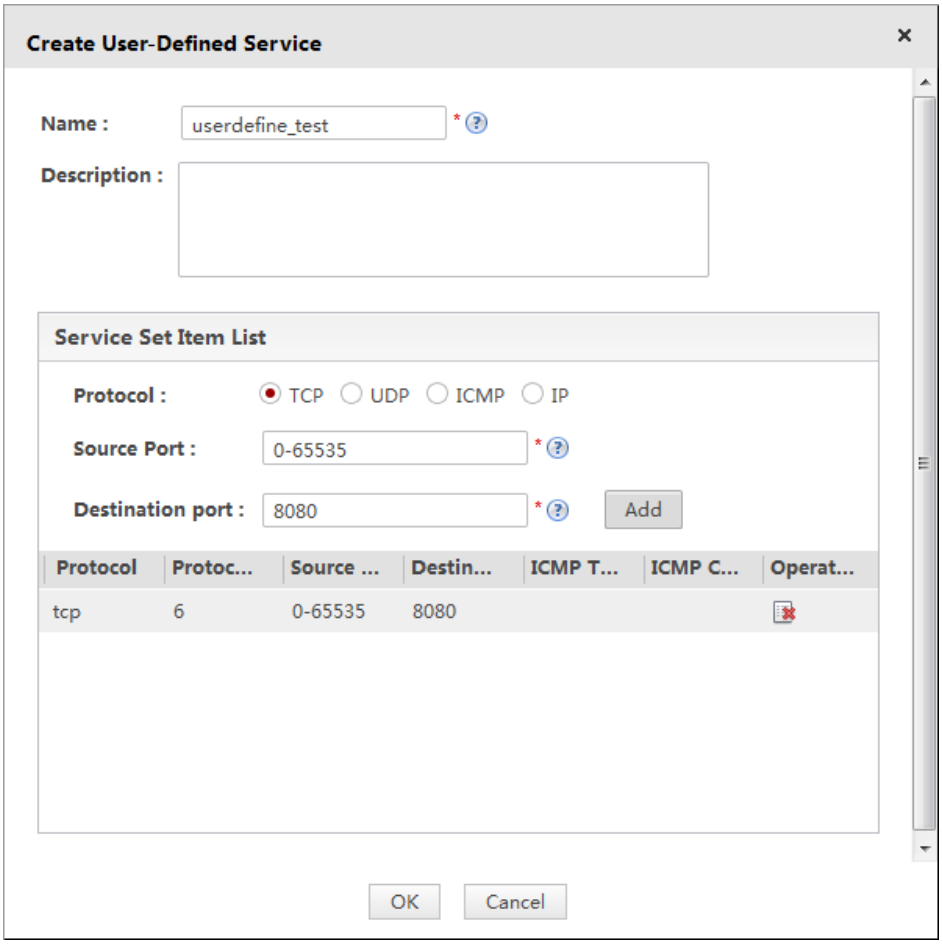


Figure 4-155 Creating a user-defined service

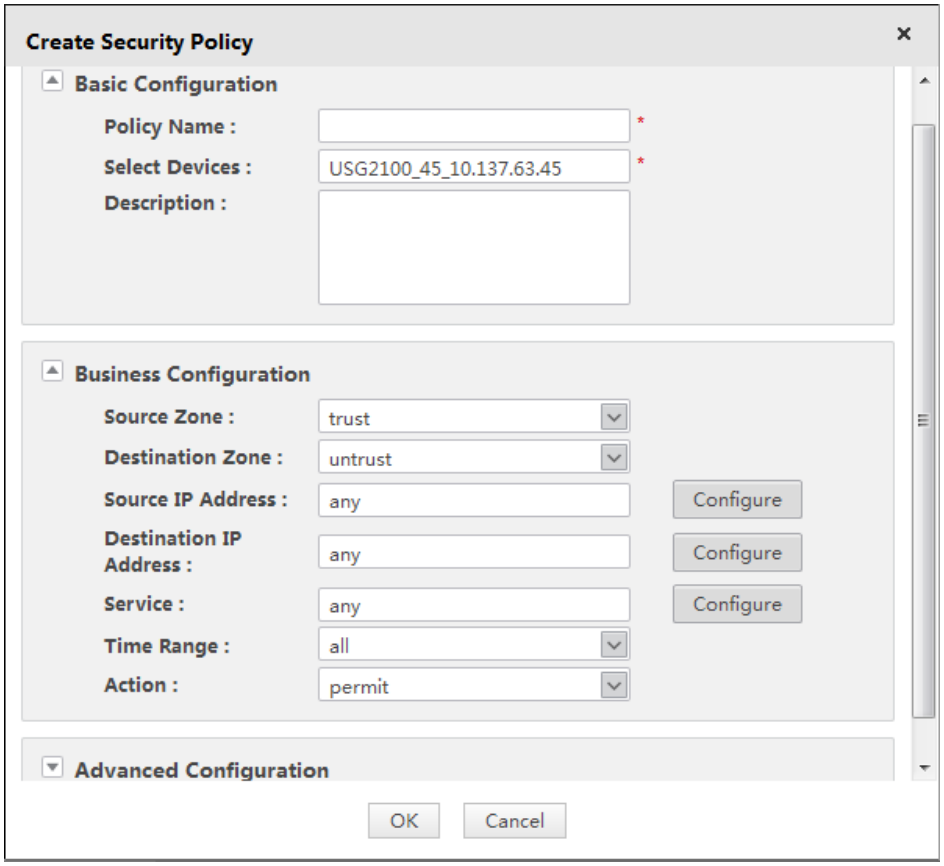


- Access control policy configuration

  The Secure Center provides the access control function. You can configure an access control policy based on the source address, destination address, service, and time range and set the action to permit or block.

  The Secure Center supports the creation, deletion, modification, and copying of security policies for devices and device groups.

Figure 4-156 Creating a firewall security policy



- Content security policy configuration

  The Secure Center supports IPS and AV policy configuration to control the content security for security zones, prevent hacker intrusion and virus spread, and secure enterprise networks.

Figure 4-157 Creating a content security policy

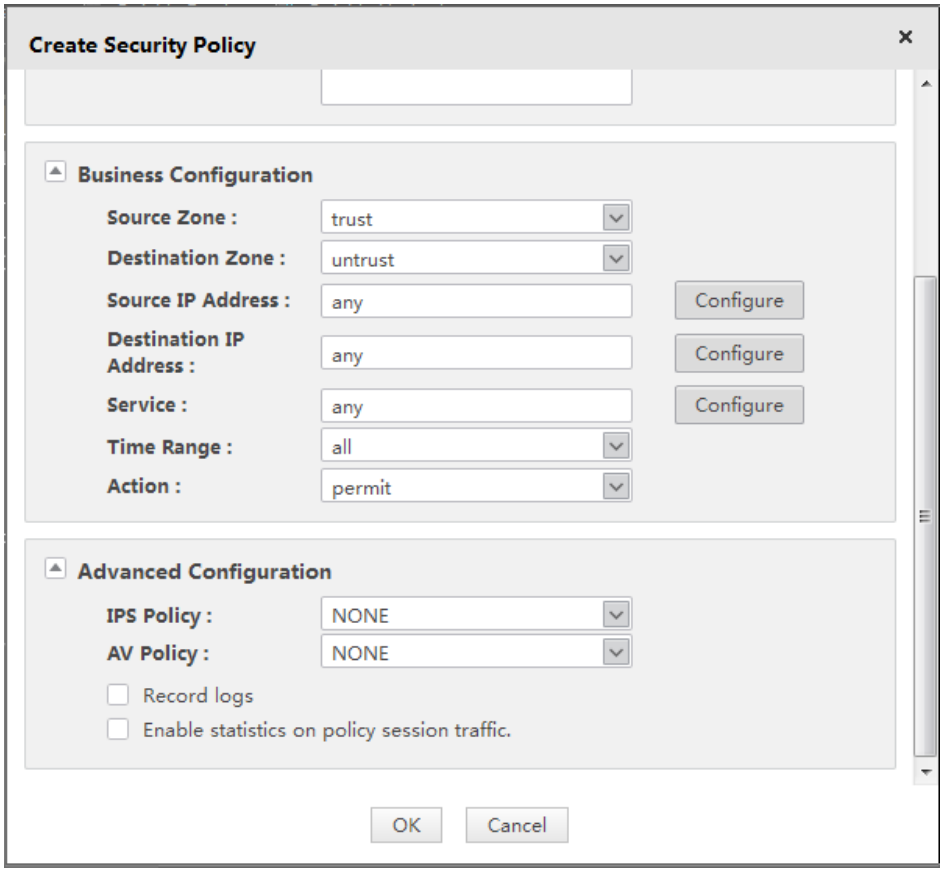
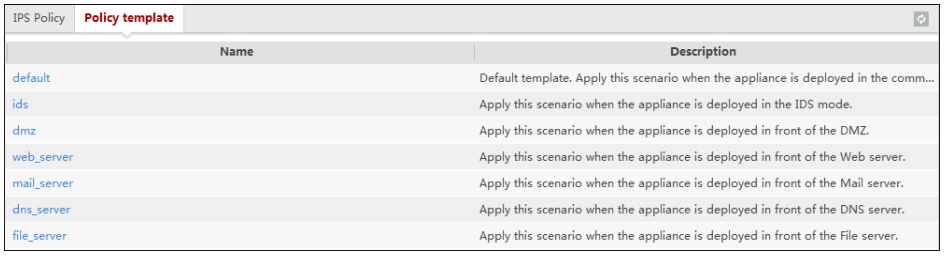
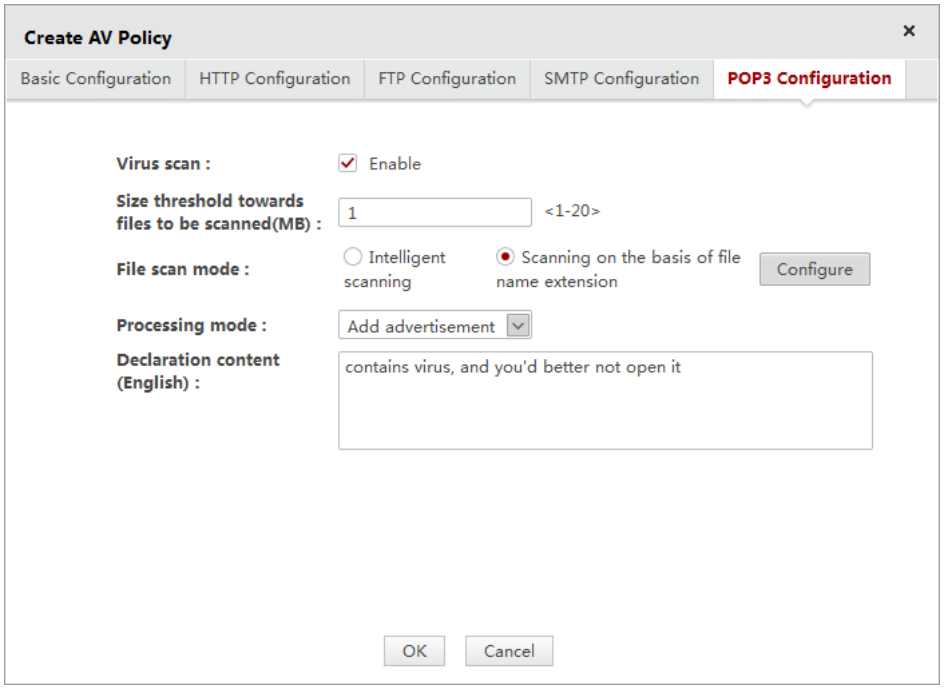


Figure 4-158 IPS policy template



The Secure Center provides a default IPS policy template and supports user-defined signatures.

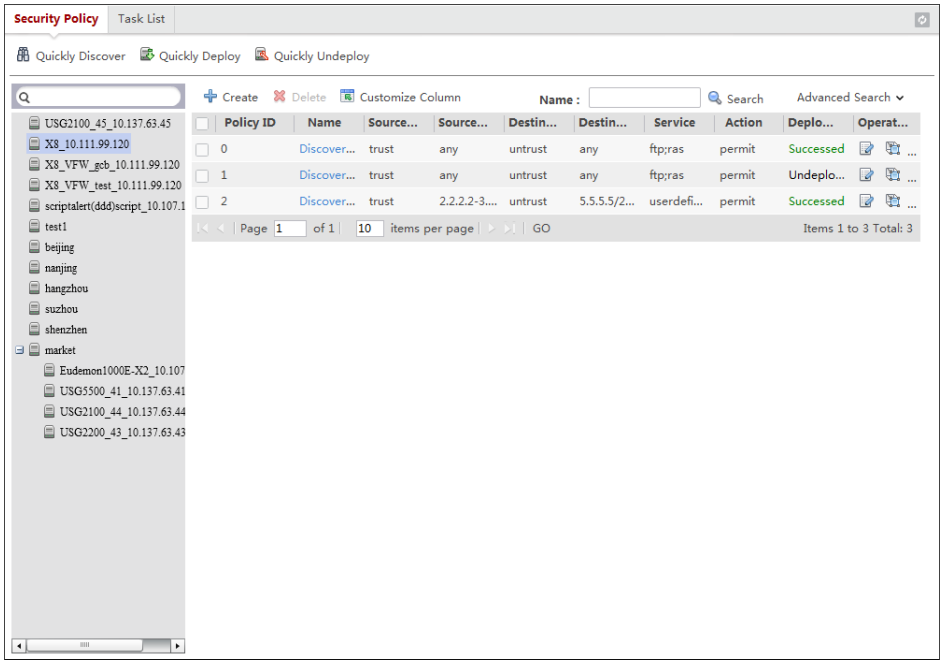
Figure 4-159 AV policy configuration



- Policy query

  You can query policy deployment status and policy context (interzone policy priorities) on the **Security Policy** page. Top policies are matched first.

Figure 4-160 Policy query page



- Policy deployment

The Secure Center supports centralized and batch policy deployment. After centralized policy configuration is complete, you can select physical or virtual firewalls and click **Deploy** to deliver security policies in batches, greatly reducing O&M workload.

Figure 4-161 Security policy deployment

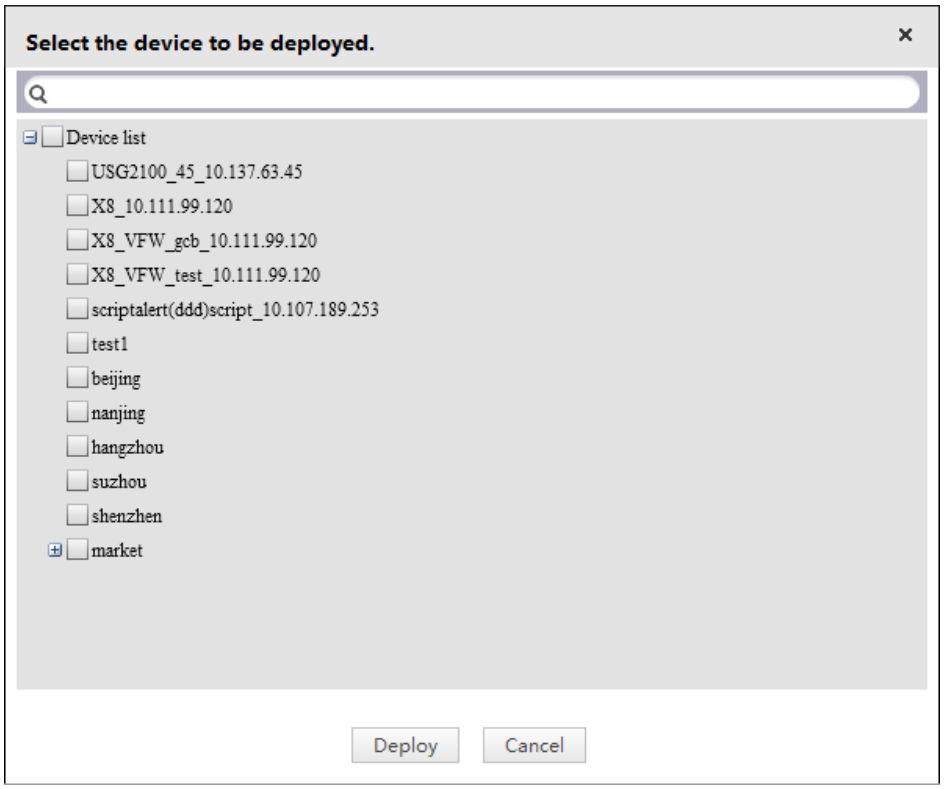
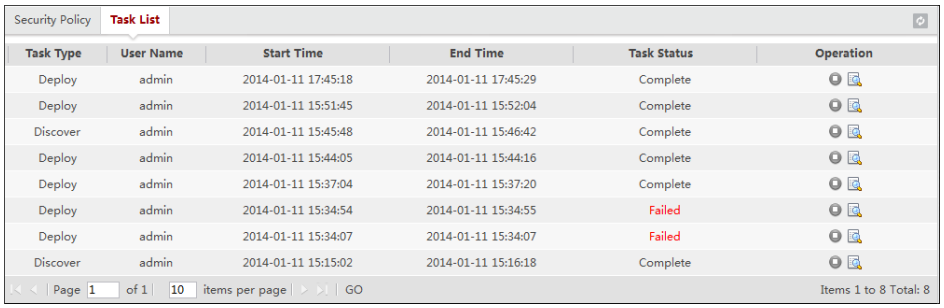


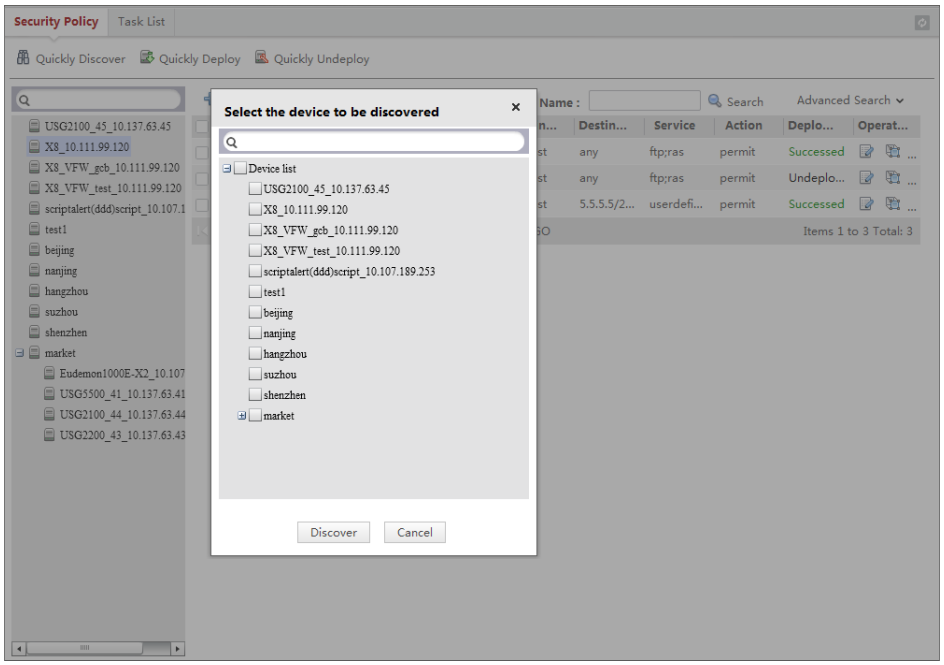
Figure 4-162 Policy deployment result



- Policy discovery

  The Secure Center supports centralized and batch policy discovery. You can synchronize policies configured on managed devices to the eSight.

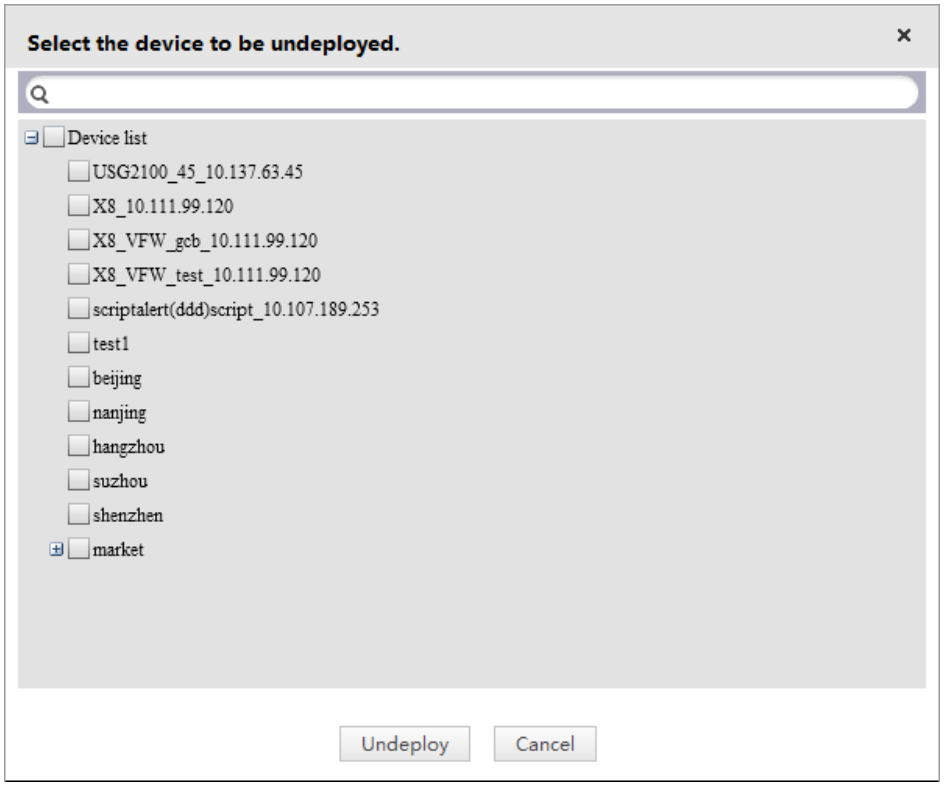
Figure 4-163 Batch policy discovery



- Policy removal

  The Secure Center supports centralized and batch policy removal. When the network is reconstructed or migrated, you can remove unneeded policies by one-click to secure enterprise information.

Figure 4-164 Batch policy removal

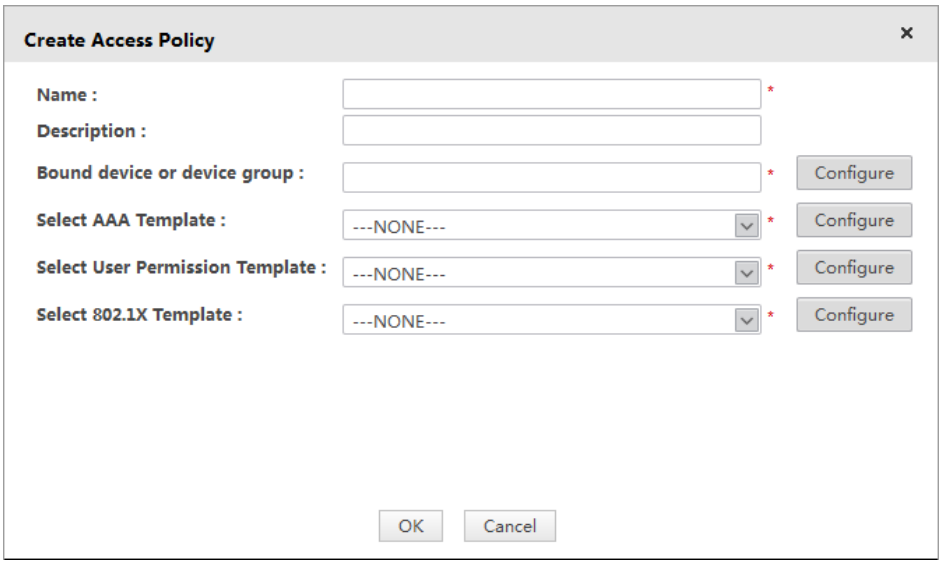


Switch Policy Management

- Access authentication policy configuration

  The Secure Center supports centralized and batch configuration of access authentication policies for Huawei switches.

  Figure 4-165 Creating an access authentication policy



  When creating an access authentication policy, you must select an AAA template, a user permission template, and an 802.1x template as well as the bound device or device group.

Figure 4-166 Binding a device or device group

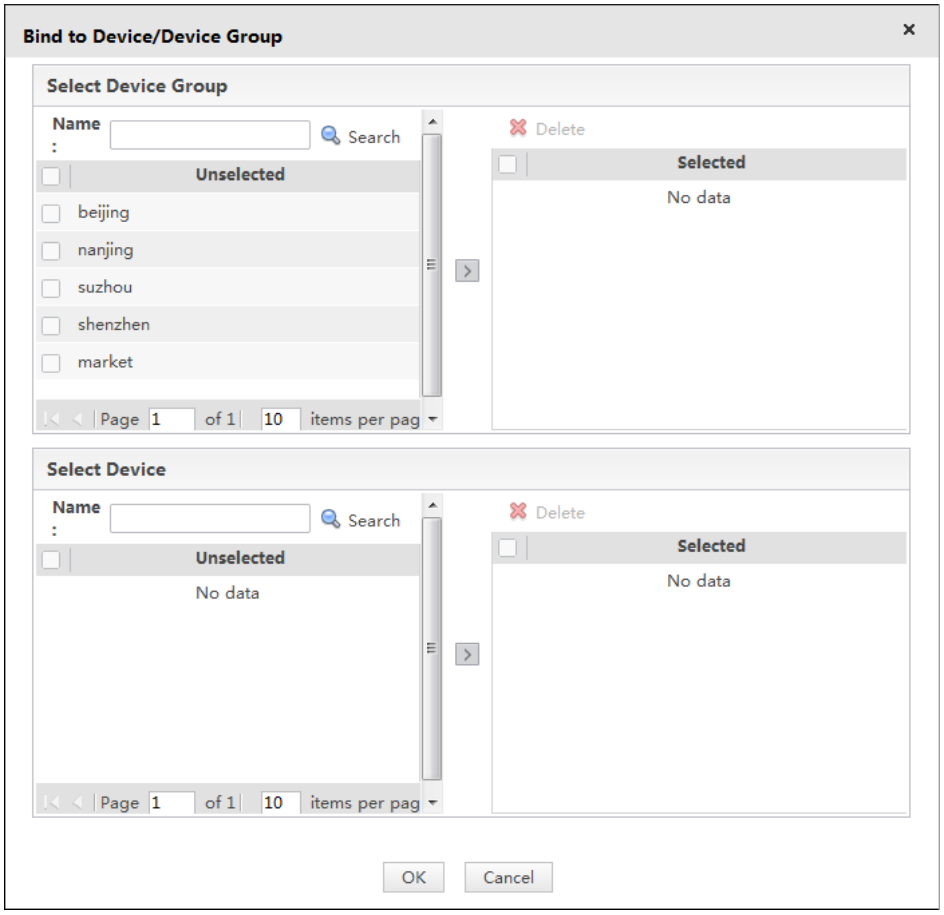


Figure 4-167 Creating an AAA template

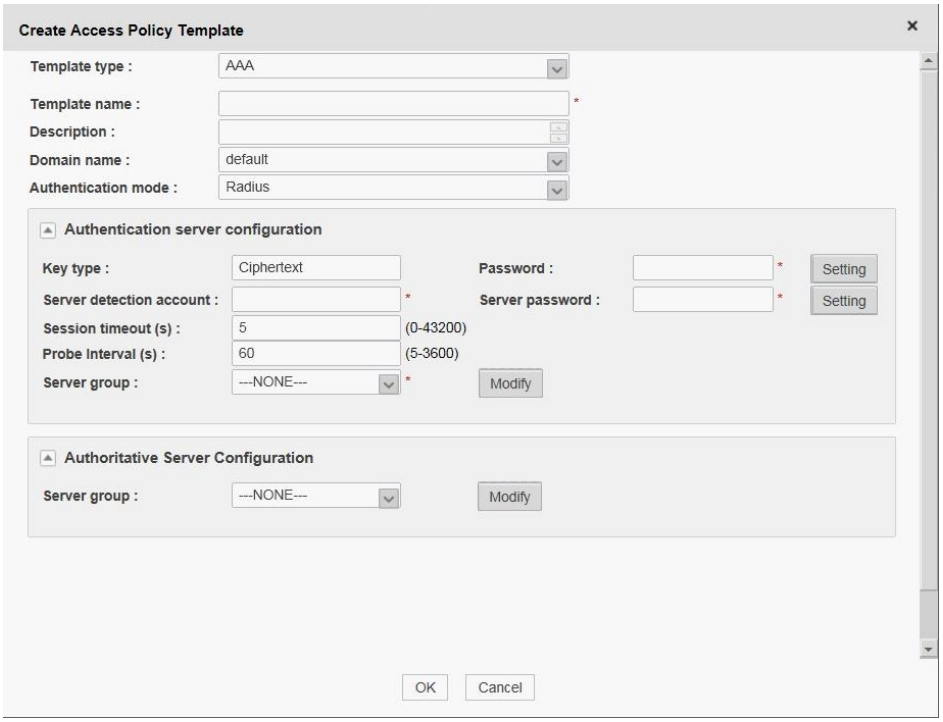


Figure 4-168 Creating a user permission template

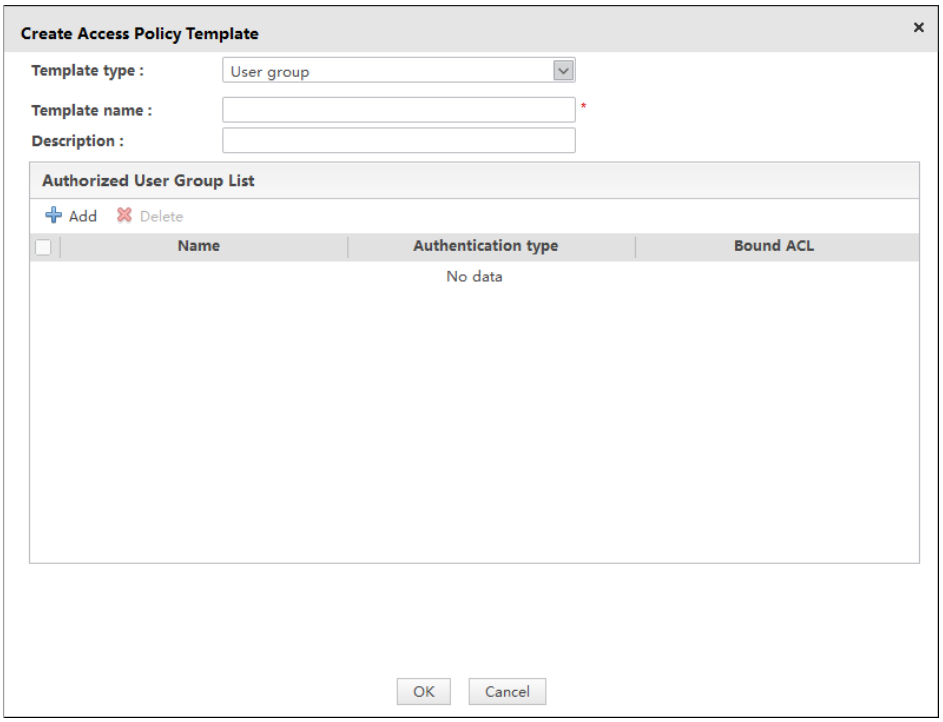
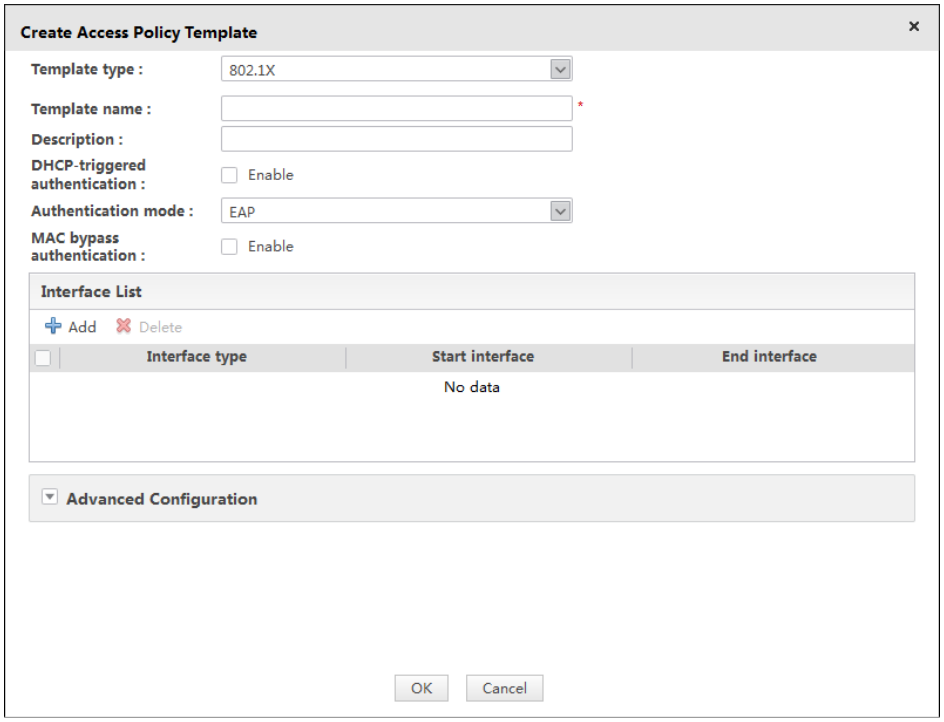


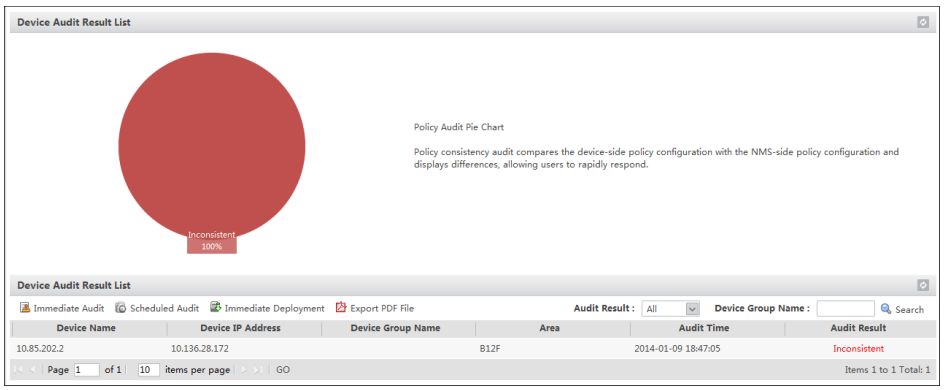
Figure 4-169 Creating an 802.1x template



- Consistency audit on access authentication policies

  The Secure Center supports manual or periodic consistency audit on access authentication policies configured for switches. The audit result can be exported as a report. You can also view details about consistency comparison.

Figure 4-170 Policy consistency audit

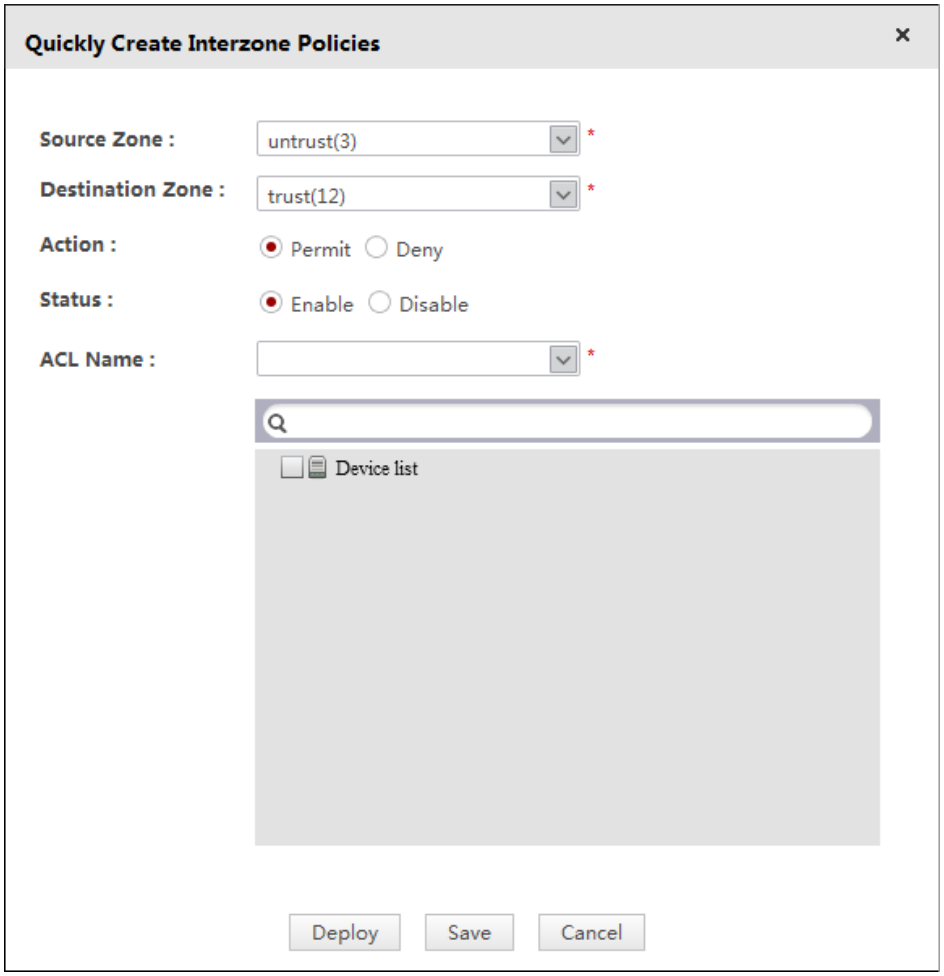


AR Policy Management

- AR security policy configuration

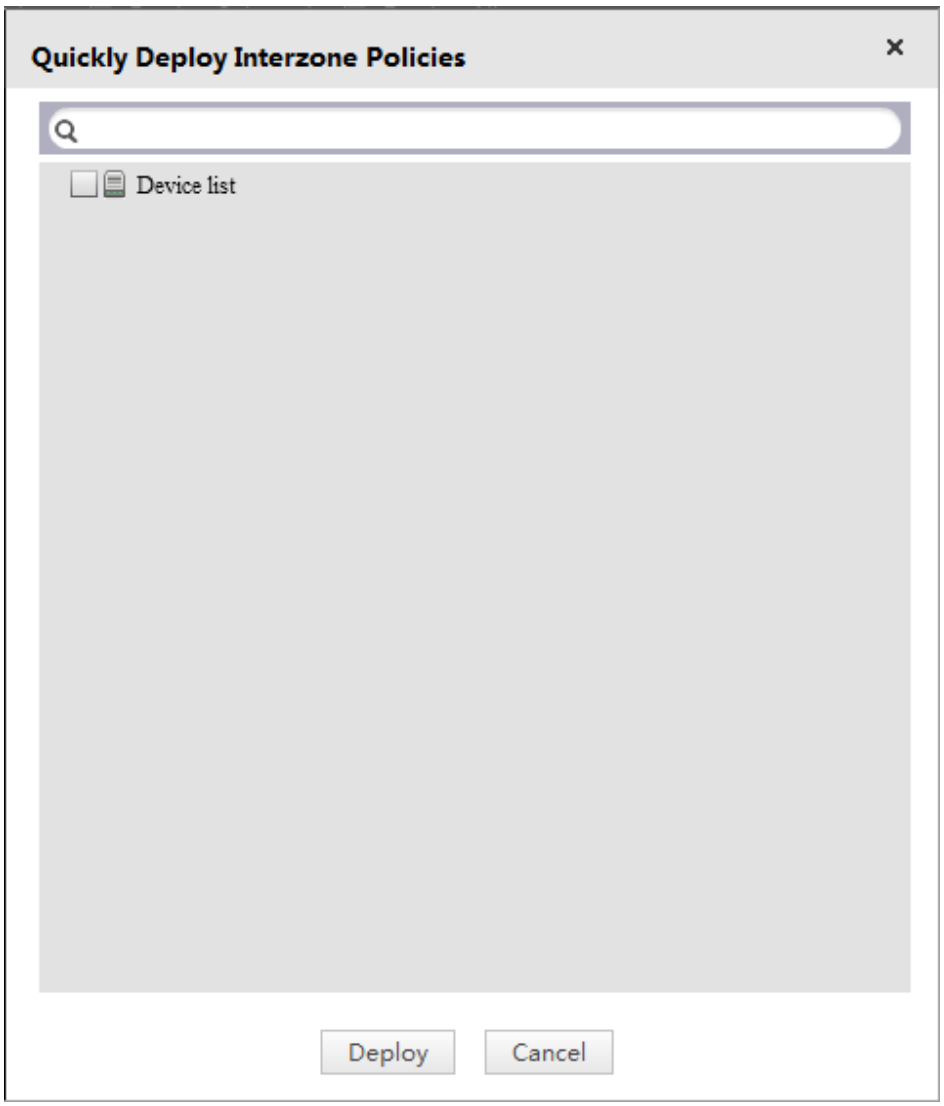
  The Secure Center supports centralized and batch configuration of security policies for Huawei ARs.

Figure 4-171 Quickly creating interzone policies



You can use the quick deployment function to deploy an interzone policy to multiple ARs when creating the interzone policy or deploy policies in batches after the interzone policy is created.

Figure 4-172 Quickly deploying AR interzone policies

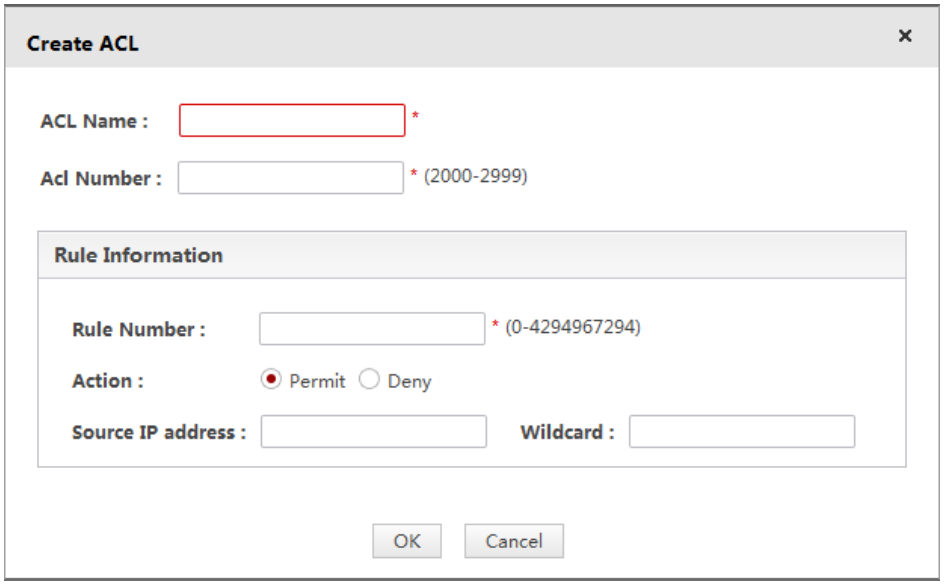


ACL Management

- Basic ACL configuration

  You can create, delete, copy, and modify basic ACLs.

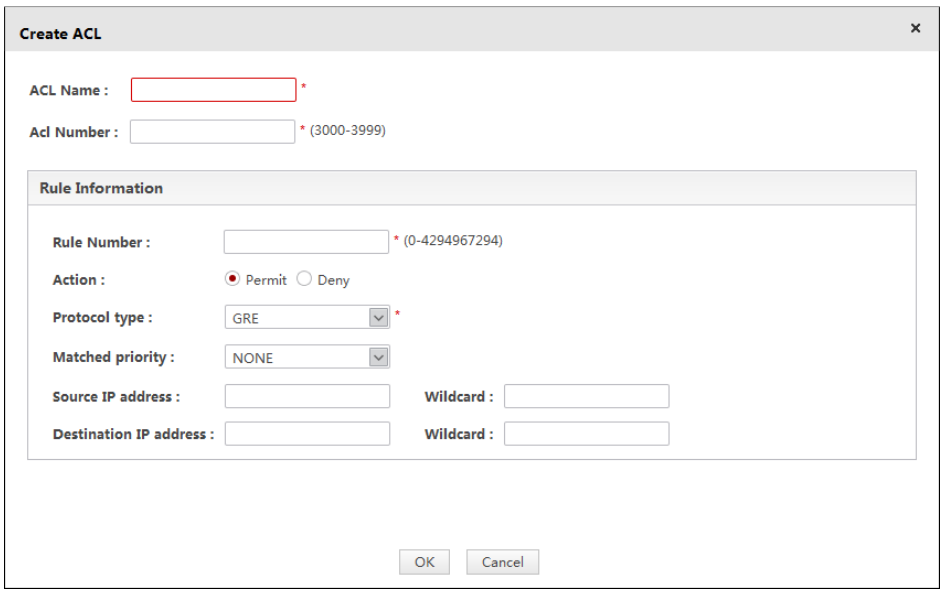
Figure 4-173 Creating a basic ACL



- Advanced ACL configuration

  You can create, delete, copy, and modify advanced ACLs and import advanced ACLs from a text file.

Figure 4-174 Creating an advanced ACL



4.3.11 LogCenter

The eSight LogCenter collects, compresses, and stores logs for Huawei's all-series and mainstream third-party security and network devices. The component performs fine-grained analysis to offer a variety of functions, including log auditing, network security analysis, NAT tracing, and intelligent log retrieval.

Unified Log Management and Analysis

With a large number of routers, switches, and firewalls deployed on internal networks, enterprises are facing a series of problems in unified log management, such as inconsistent log formats, poor readability, and difficulty in massive log storage. The NMS finds difficulty in discovering potential security risks from logs in real time.

eSight LogCenter, however, can address the preceding problems. It can collect log files in diverse modes, including SYSLOG, SESSION, SFTP, FTP (both static and dynamic), and WMI (supported only on the Windows operating system). After logs are collected from application systems and NEs, eSight LogCenter can classify, filter, consolidate, analyze, store, and monitor the logs. These functions enable administrators to manage massive logs in a more efficient manner to keep abreast of the running conditions of network and security NEs, trace Internet user behaviors, and quickly identify and eliminate security threats.

In addition to unified log management, eSight LogCenter generates alarms in real time when detecting exceptions from logs.

NAT-based Traceability

eSight LogCenter provides Network Address Translation (NAT)-based traceability of Internet user behaviors. When tracing Internet user behaviors, eSight LogCenter collects session logs from network and security NEs such as MA5200G, NE40E/80E, and USG firewalls. Then eSight LogCenter analyzes the logs in combination with user data sources (such as the AAA server) to obtain NAT information. NAT information includes the destination IP address, destination port, source IP address, and protocol.

Internet Behavior Management

In the Internet behavior management scenario, eSight LogCenter collects and analyzes session and security logs of NEs (such as USG firewalls) to trace Internet user behaviors (such as P2P, email, HTTP, MSN, and QQ). Then eSight LogCenter queries and analyzes users' Internet traffic, online time length, keywords, web access, mail sending and receiving, application usage, network threats encountered, and file transfer operations. Administrators can use the analysis results to manage Internet user behaviors.

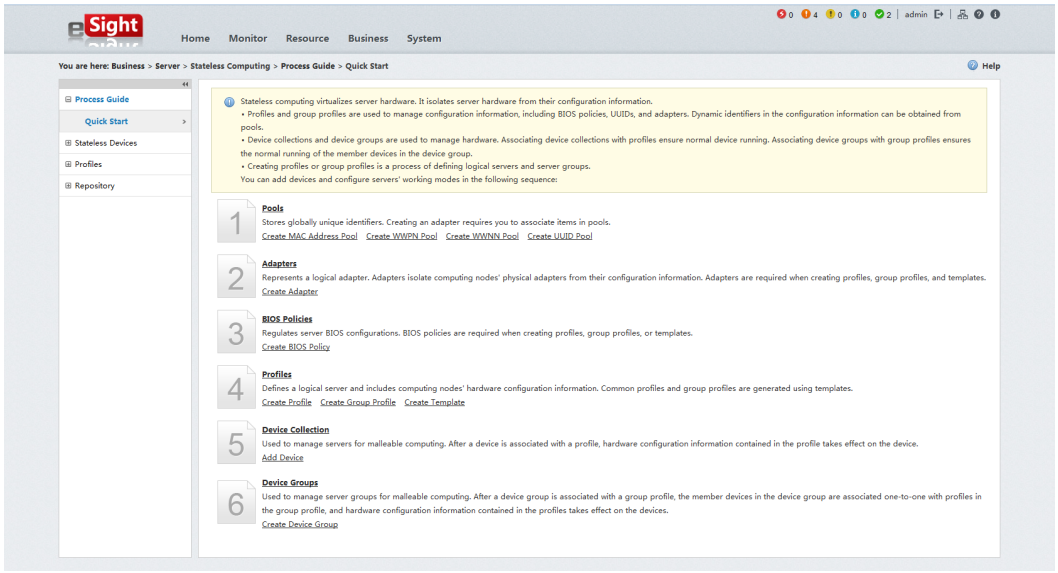
4.3.12 Server Stateless Computing Management

The eSight Server Stateless Computing Manager extracts server hardware configuration as a file to flexibly change configuration, improving fault rectification and capacity expansion efficiency.

Quick Start

Stateless computing offers quick start, guiding users to define server configurations for logic servers. The configurations can be loaded to activate specific servers.

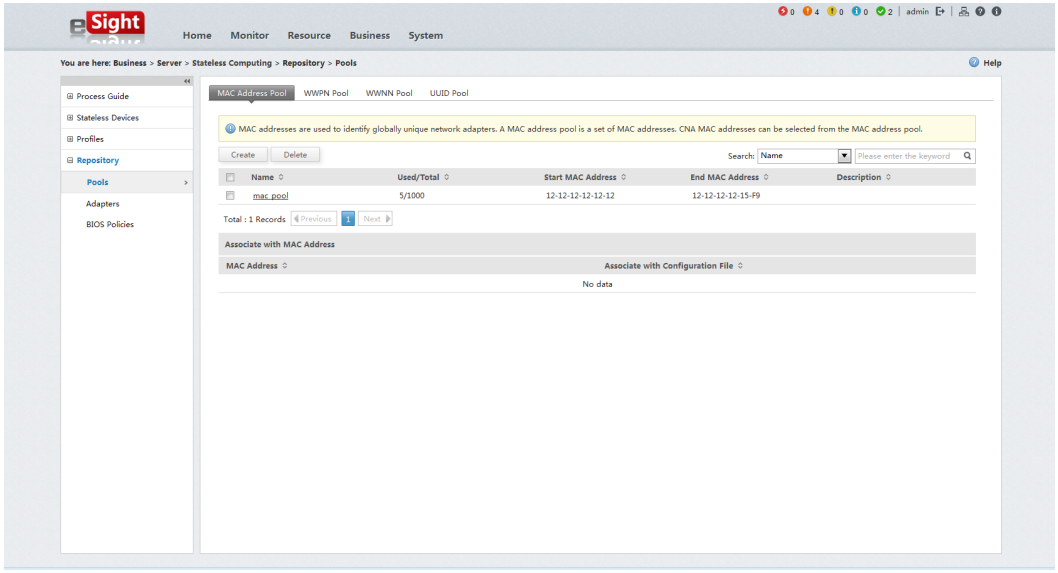
Figure 4-175 Stateless computing quick start



Pool Configuration

A pool defines the network adapter, HBA card, and ID information, and dynamically manages IDs.

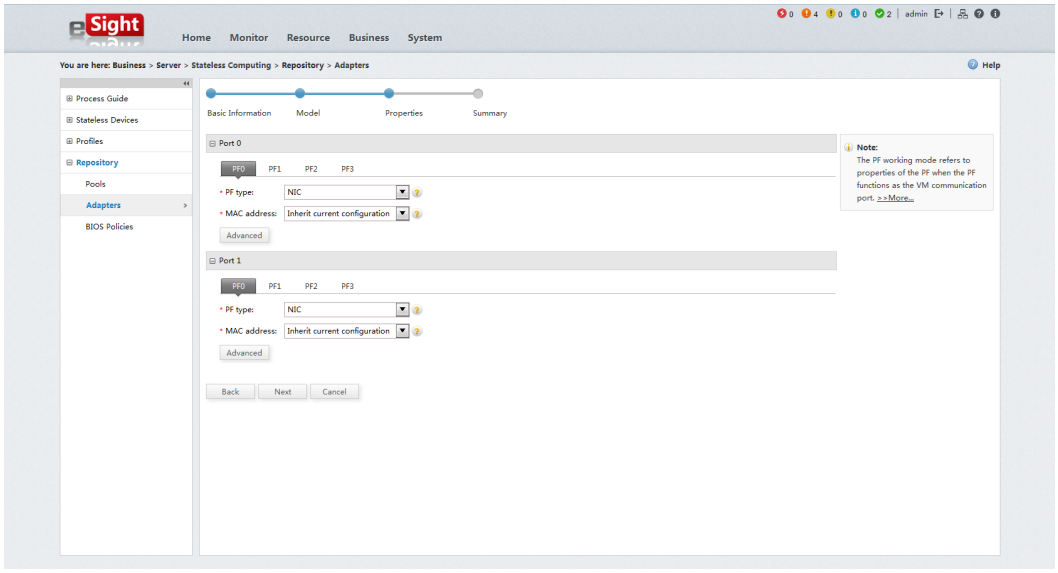
Figure 4-176 Pool configuration



Adapter

An adapter defines the HBA, CNA, and RAID configuration. Creating a profile requires existing adapter information to define adapter information inside a logic server.

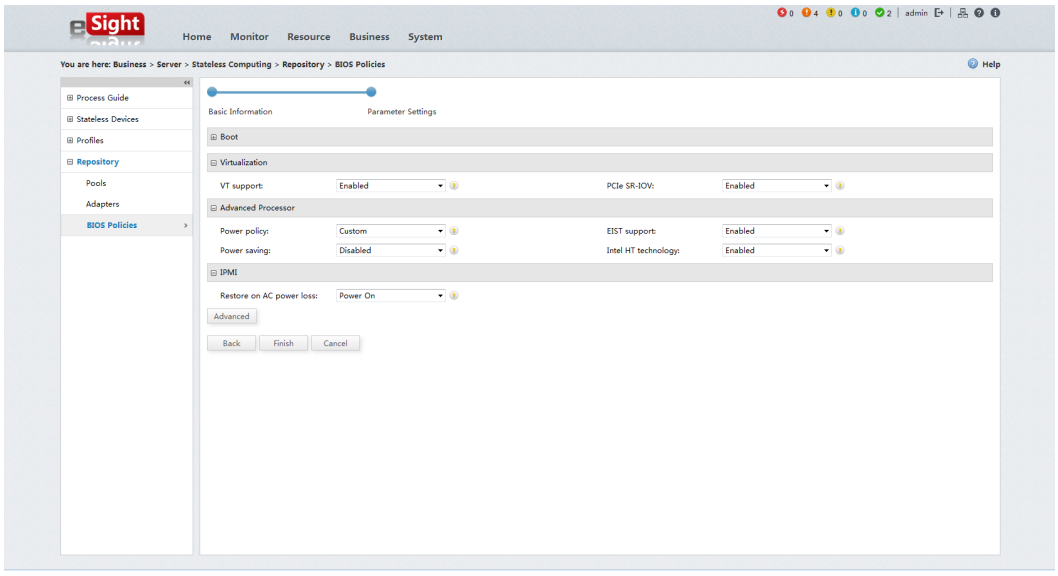
Figure 4-177 Adapter configuration



BIOS Policy

Users can define BIOS policies. Creating a profile requires an existing BIOS policy to define BIOS information inside a logic server.

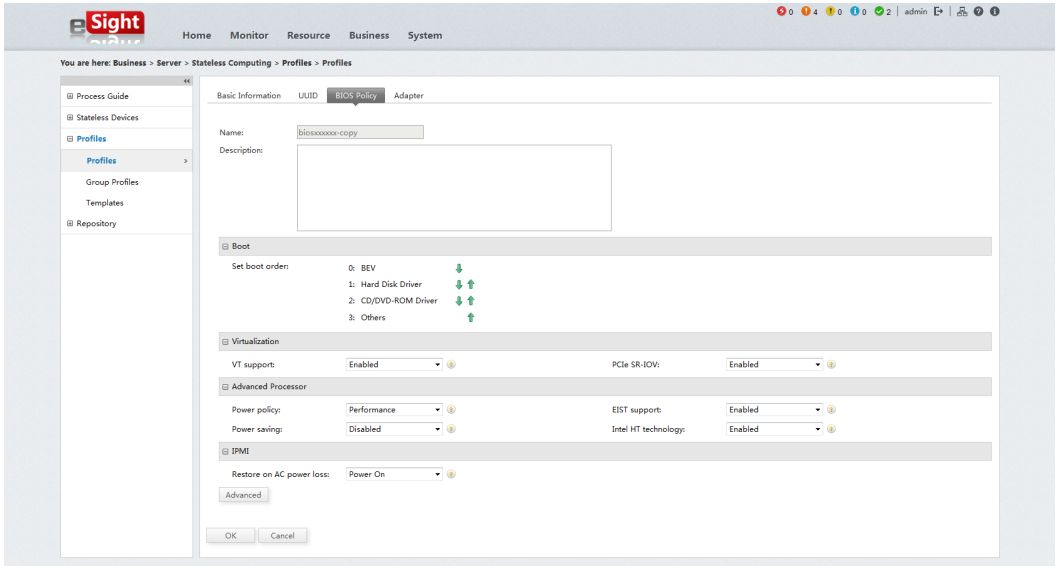
Figure 4-178 BIOS policy configuration



Profile

Users can use a profile to freely combine hardware configuration information, including BIOS policy and adapter information, to form an available server with new configuration.

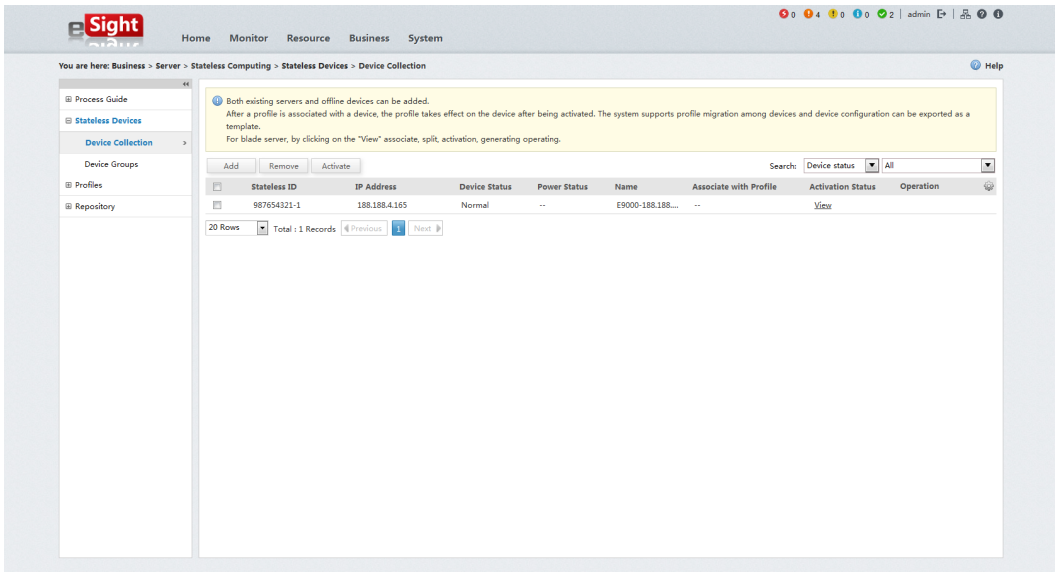
Figure 4-179 Profile sample



Device Set

A device set is used to manage devices that support stateless computing. Users can use device sets to associate devices and profiles. After device sets are activated, hardware configuration information in the profiles are applied to devices.

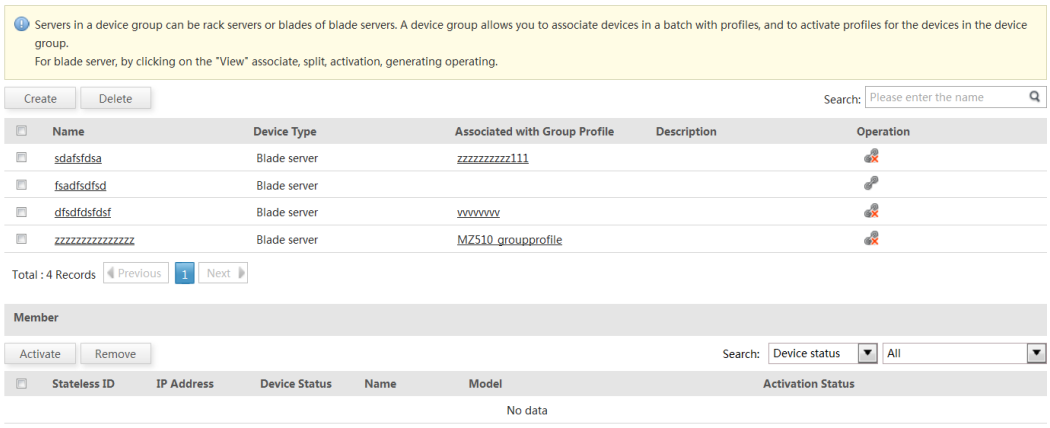
Figure 4-180 Stateless computing device set



Device Group

Users can divide devices in to a group where devices share the same profile, loading server configurations in batches.

Figure 4-181 Stateless computing device group



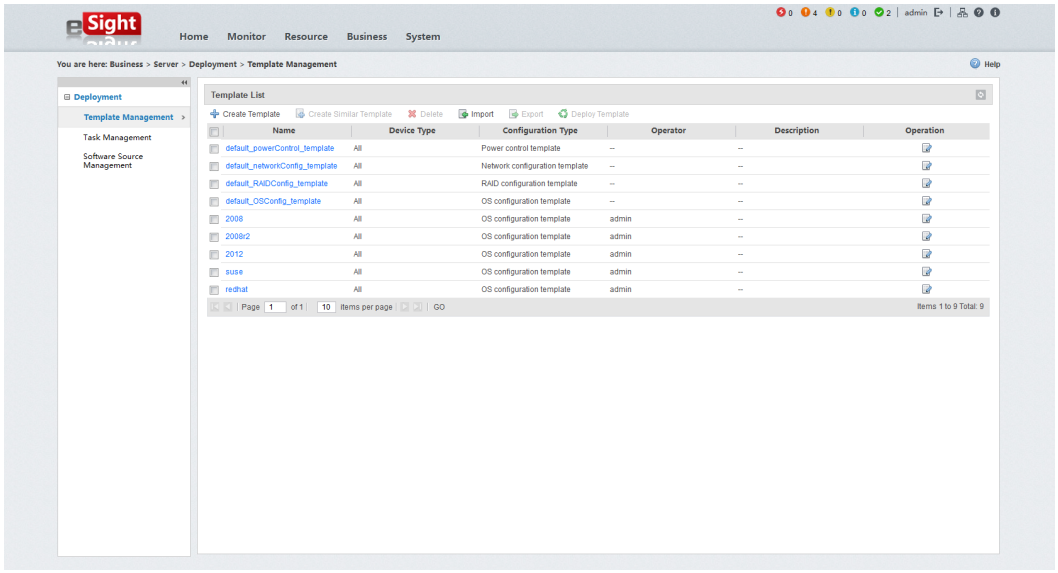
4.3.13 Server Deployment Management

The eSight Server Device Manager allows users to configure the following information about Huawei servers in batches: BIOS configuration, network configuration, RAID card configuration, and operating system deployment.

Configuration Template

A configuration template is used to quickly create configuration files.

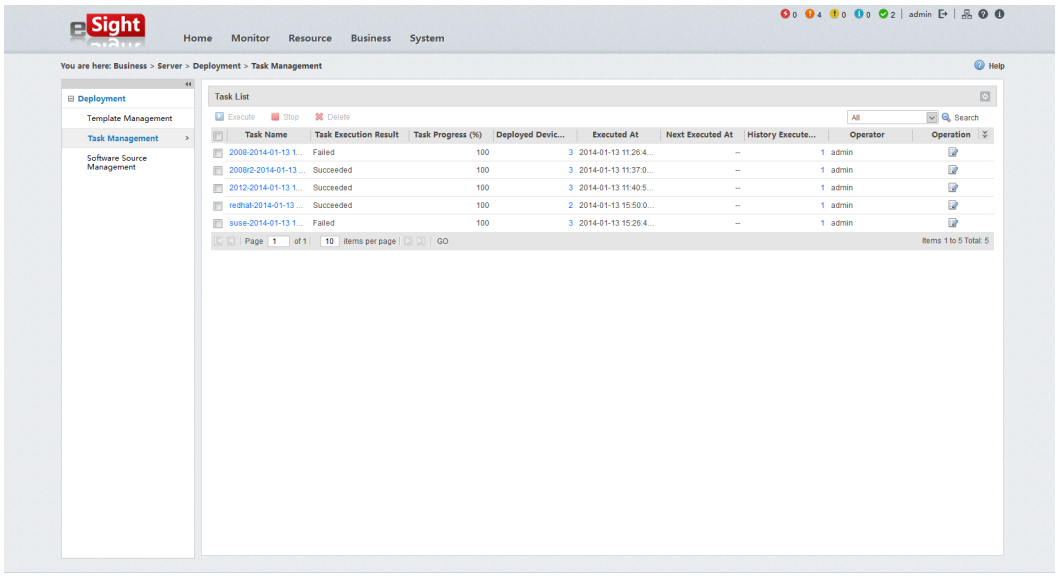
Figure 4-182 Configuration template



Configuration Task Management

Users can implement, stop, delete, modify, and view configuration tasks.

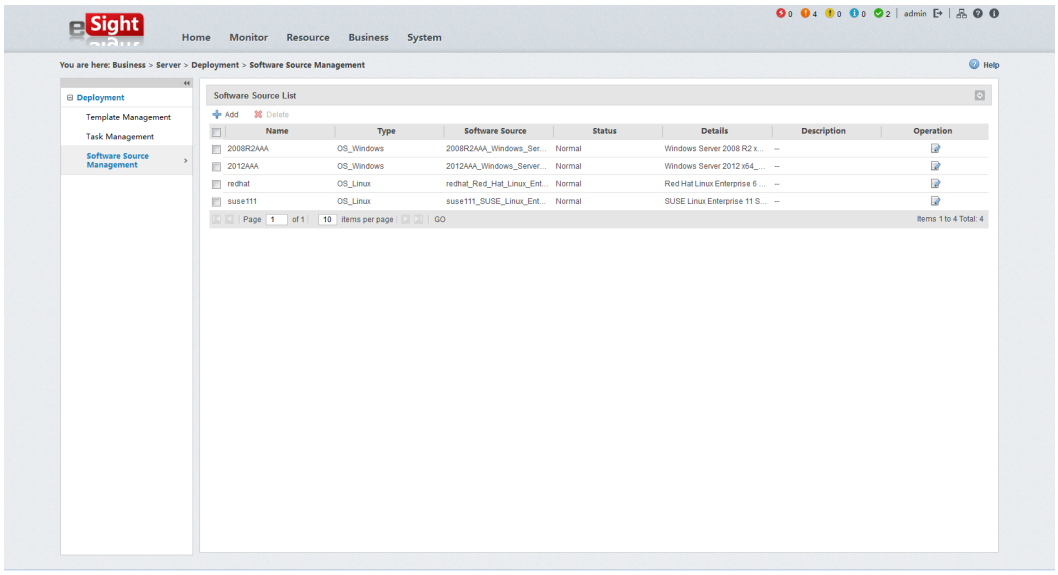
Figure 4-183 Configuration task management



Software Source Management

With software source management, users can manage system mirroring files required during operating system deployment.

Figure 4-184 Software source management



4.3.14 Infrastructure Management

The eSight Infrastructure Manager provides comprehensive management functions for the data center infrastructures, including:

- Power equipment: The power equipment includes precision air conditioners, uninterruptible power systems (UPSs), power distribution frames (PDFs), and AC transfer switches (ATSs). The eSight Infrastructure Manager allows you to view real-time data of power equipment, such as the operating status, parameters, and alarm information.
- Engine room air conditioning: The eSight Infrastructure Manager allows you to remotely start or shut down a precision air conditioner, and change the temperature and humidity thresholds.
- Cabinet: The eSight Infrastructure Manager manages the micro-environment of a cabinet. This allows you to view cabinet environment information and learn about the usage of resources, such as space, power supply, heat dissipation, and loads.
- Environment: The eSight Infrastructure Manager uses collectors to monitor environment parameters, such as smoke, temperature, humidity, and water leakage, in a data center. This allows you to view smoke density, temperature, and humidity in the data center or its modules in real time.
- Security equipment: The video monitoring equipment includes cameras and network video recorders (NVRs). The eSight Infrastructure Manager monitors the data center and its modules in real time and stores videos for future replay.
- Access Control System: This is an integrated access card-based user management solution, making the access right controllable and auditable.

Resource Management

The eSight Infrastructure Manager provides the following resource management functions:

- Lists the information about the selected managed devices and their sub managed devices in three modes.
  - All: lists all managed devices.
  - Management domain: lists all managed domains under the selected node.
  - Physical device: lists all devices in the selected management domain.
- Displays different managed devices with different icons.
- Allows you to add and delete management domains and change management domains properties.
- Allows you to query management domains based on names or types.
- Allows you to create management domains one by one or in batches.

View Management

The eSight Infrastructure Manager provides views displaying the positions and operating status of all the devices in the data center. This function allows you to monitor the devices in real time.

Energy Efficiency Analysis

Provides the power consumption statistics, PUE, electricity cost counting, power consumption reports, and historical power consumption data analysis. You can query power consumption

status of various management domains, such as IT equipment, lighting facilities, and the total power consumption. In this manner, you are provided with the real-time power consumption status, historical power consumption status, and power consumption distribution of each subsystem, helping optimize the power consumption of the data center.

- Energy consumption assessment on a layer or level basis

  You can customize consumption nodes in districts and equipment rooms in the power distribution view to calculate energy consumption of various layers or levels.
- Dashboard display of energy consumption analysis

  One page fully demonstrates all power efficiency information of one management domain.
- Historical data analysis

  You are allowed to query the historical data of a certain period to analyze the power consumption trends.
- Multistep electricity price

  The energy consumption cost of the data center can be vividly displayed.
- You can customize tariff strategies, add monthly or time period-based tariff strategies, and modify or delete tariff strategies.

Video Management

The video management develops the following functions:

- The eSight can connect to an IP cameras.
- The eSight can also independently deploy video integration over the web user interface (WebUI).
- The eSight allows you to view real-time videos, query video source configurations, and save the configuration information.
- Camera management

  You can create or delete a camera, query cameras based on the name or IP address, view detailed information about a camera, such as the name, No., recorded location, supplier, IP address, model, and status, and modify the information.

Report Management

The eSight Infrastructure Manager presents reports in graphics, such as curves, histograms, and pie charts.

- The eSight Infrastructure Manager allows you to export reports as an Excel or PDF file and print reports for analysis.
- The eSight Infrastructure Manager allows you to modify the report storage capacity and upload customer logos.
- The eSight Infrastructure Manager generates reports based on tasks, saves periodic reports in a report storage disk, and sends reports by email as configured.

Access Control

The eSight Infrastructure Manager provides an access control system that manages access controllers and access control card holders of cabinet-level access controllers.

- The access management function enables you to configure IP addresses for access controllers and configure the management server.
- The time management function enables you to manage the access control in the specified time periods or holidays.

  NOTE

  The cabinet-level door status sensor does not support the time management function.
- The user management function enables you to manage the users and user groups.

Capacity Statistics and Analysis

Analyses of capacity on space, location, cooling, configuration, and weight bearing are supported:

- Rack and cabinet location, capacity of power distribution, cooling, and weight bearing can be collected and analyzed.
- Capacities can be synchronized based on the expansion and migration.

Capacity Optimization Design

Optimize the configuration of the cabinet based on the properties of devices:

- Optimal device location for migration can be identified and automatically matched.
- Automatically allocated and config the optimized resources.

Temperature Map

The overall temperature distribution of the equipment room is clearly displayed.

The cold and the hot spots can be effectively identified:

- The analyses of temperature distributions on top, middle, and bottom levels are available.
- Place the mouse where you want to query and temperature and related device information can be displayed.
- The top 5 high temperatures and top 5 low temperatures can be analyzed.

Linkage Control

The following two linkage controls are available:

- Modular data center skylight ceiling linkage control
- Container data center humidifier linkage control.

5 Configuration

5.1 Software Configuration Requirements

- eSight Compact (network device) supports Windows 7 (32-bit) operating system and MySQL 5.5 database.
- eSight Compact (server) supports the following combinations of operating systems and databases:
  - Windows Server 2008 R2 Standard (64-bit) + MySQL 5.5
  - Windows Server 2008 R2 Standard (64-bit) + Microsoft SQL Server 2008 R2 Standard
- eSight Standard and Professional support the following combinations of operating systems and databases:
  - Windows Server 2008 R2 Standard (64-bit) + MySQL 5.5
  - Windows Server 2008 R2 Standard (64-bit) + Microsoft SQL Server 2008 R2 Standard
  - SUSE Linux 11 SP1 (64-bit) + Oracle 11g R2 Standard
  - SUSE Linux 11 SP1 (64-bit) + GaussDB

NOTICE

The languages for the operating system and database must be the same, either Simplified Chinese or English.

NOTE

- Only the SUSE Linux + Oracle combination is supported when managed devices range from 5000 to 20, 000.
- Certain components do not support OS+DB combinations. For details, see **Table 5-1**.

Table 5-1 Description about components supporting OS+DB

Type	Conmponent	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
Management platform	eSight Platform	√	√	√	√ **NOTE** Does not support hierarchical network management.
Device management components	eSight Network Device Manager	√	√	√	×
	eSight Server Device Manager	√	√	√	√
	eSight Storage Device Manager	√	√	√	√
	eSight MicroDC Device Manager	√	×	×	×
	eSight UC/CC Device Manager	√	√	√	√
	eSight Video Surveillance Device Manager	√	√	√	√
	eSight Telepresence Device Manager	√	√	√	×
	eSight eLTE Device Manager	√	×	√	×
Service management components	eSight Open SDK	√	√	√	√
	eSight Smart Reporter	√	√	√	×

Type	Conmponent	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
	eSight Storage Reporter	√ **NOTE** Use an independent MySQL database if this component is deployed.	√ **NOTE** Use an independent MySQL database if this component is deployed.	√ **NOTE** Use an independent MySQL database if this component is deployed.	√ **NOTE** Use an independent MySQL database if this component is deployed.
	eSight WLAN Manager	√	√	√	×
	eSight MPLS VPN Manager	√	√	√	×
	eSight MPLS Tunnel Manager	√	√	√	×
	eSight Network SLA Manager	√	√	√	×
	eSight DC nCenter	√	√	√	×
	eSight Network Traffic Analyzer Manager	√	√	×	×
	eSight IPSec VPN Manager	√	√	√	×
	eSight Secure Center	√	√	×	×
	eSight LogCenter Log Manager	×	√	×	×
	eSight Server Stateless Computing Manager	√	√	√	√
	eSight Server Deployment Manager	√	√	√	√

Type	Conmponent	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
	eSight Infrastructure Manager	×	×	√ **NOTE** Use an independent MySQL database if this component is deployed.	×

NOTE

- √: The component supports the operating system and database.
- ×: The component does not support the operating system or database.

5.2 Hardware Configuration Requirements

Different combinations of the eSight platform and components have different server hardware requirements.

Table 5-2 eSight basic management

Edition	Management Scale	Server Configuration Requirement	Delivery Server Configuration
eSight Compact (network device)	40 nodes (fixed value)	● CPU: 1 x dual-core 2 GHz or above ● Memory: 4GB ● Disk space: 40GB	N/A
eSight Compact (server)	100 rack servers and 5 blade servers (fixed)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 8GB ● Disk space: 120GB **NOTE** A PC server is recommended.	N/A

Edition	Management Scale	Server Configuration Requirement	Delivery Server Configuration
Standard	0-200 nodes (management platform + device management, excluding value-added components)	● CPU: 1 x dual-core 2 GHz or above ● Memory: 6GB ● Disk space: 40GB **NOTE** A PC server is recommended.	● X3650M4,1*E5-2640 6c2.5GHz Or Above,8G (2*4G),2*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,No Monitor, 2*750W HE(1+1), 100V~240VAC ● Tecal RH2288 V2,BC1M13SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 2*4G,2*300G SAS 2.5,1*4GE LOM,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	200-500 nodes (management platform + device management, excluding value-added components)	● CPU: 2 x dual-core 2 GHz or above ● Memory: 6GB ● Disk space: 60GB **NOTE** A PC server is recommended.	
	500-2000 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 8GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G (Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),1*1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE (1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 32G(4*8G),3*300G SAS 2.5,1*4GE LOM, 1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	2000-5000 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	

Edition	Management Scale	Server Configuration Requirement	Delivery Server Configuration
Professional	0-200 nodes (management platform + device management, excluding value-added components)	● CPU: 1 x dual-core 2 GHz or above ● Memory: 6GB ● Disk space: 40GB **NOTE** A PC server is recommended.	● X3650M4,1*E5-2640 6c2.5GHz Or Above,8G (2*4G),2*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,No Monitor, 2*750W HE(1+1), 100V~240VAC ● Tecal RH2288 V2,BC1M13SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 2*4G,2*300G SAS 2.5,1*4GE LOM,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	200-500 nodes (management platform + device management, excluding value-added components)	● CPU: 2 x dual-core 2 GHz or above ● Memory: 6GB ● Disk space: 60GB **NOTE** A PC server is recommended.	
	500-2000 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 8GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G (Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),1*1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE (1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 32G(4*8G),3*300G SAS 2.5,1*4GE LOM, 1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	2000-5000 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	

Edition	Management Scale	Server Configuration Requirement	Delivery Server Configuration
	5000-20,000 nodes	● CPU: 4 x quad-core 2 GHz or above ● Memory: 64GB ● Disk space: 320GB **NOTE** A PC server is recommended.	● IBM X3850X5,4*Xeon 8C E7-4820 2.0G Or Above,64G(8*8G), 8*300G,DVDRW, 1*Integrated 1000M NIC (dual),1*1000M NIC (dual),1*1000M NIC (4Port),ServeRAID M5015(512M),iMM System management card,3Y5*8-2*1975W(1+1)-100V~240VAC ● Tecal RH5885 V2,CH91M05RGPU, RH5885,4*E7-4820 8kernel,2.0GHz-64G (8*8G),8*300G SAS, 4XGE Ethernet Card, 1*4GE network board,RAID 0/1/5/10 512M,Battery protection,DVDRW, 100V~240VAC, 2*3000W(1+1)

NOTE

- eSight basic management involves the management platform, device management (network device, UC, TP, IVS, storage, server, host, FusionAccess, FusionCompute, MicroDC, and eLTE terminal), WLAN management, nCenter management, MPLS VPN/MPLS Tunnel management, SLA management, IPSec VPN management, and security policy management.
- The management node quantity is calculated as follows: terminal device (IP phone, eLTE terminal) 1:5, high-end storage device 160:1, mid-range storage device 40:1, low-end storage device 10:1, hierarchical storage device 10:1, rack server 2:1, blade server 40:1, other device 1:1.

Table 5-3 eSight basic management + storage report management

Management Scale	Server Configuration Requirement	Delivery Server Configuration
0-500 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 8GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above,32G(4*8G), 3*300G(Dual 6Gbps SAS Port),DVDRW,1*Integrated 1000M NIC(4Port),1*1000M NIC (4Port),ServeRAID M5110e

Management Scale	Server Configuration Requirement	Delivery Server Configuration
500-2000 nodes	● CPU: 2 x six-core CPUs, 2.5 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	(512M) Battery protection, 2*750W HE(1 +1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU,32G(4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
2000-5000 nodes	● CPU: 2 x six-core CPUs, 2.5 GHz or above ● Memory: 24GB ● Disk space: 250GB **NOTE** A PC server is recommended.	
5000-20,000 nodes	● CPU: 4 x quad-core 2 GHz or above ● Memory: 64GB ● Disk space: 320GB **NOTE** A PC server is recommended.	● IBM X3850X5,4*Xeon 8C E7-4820 2.0G Or Above,64G (8*8G),8*300G,DVDRW, 1*Integrated 1000M NIC(dual), 1*1000M NIC(dual),1*1000M NIC(4Port),ServeRAID M5015 (512M),iMM System management card,3Y5*8-2*1975W(1 +1)-100V~240VAC ● Tecal RH5885 V2,CH91M05RGPU, RH5885,4*E7-4820 8kernel, 2.0GHz-64G(8*8G),8*300G SAS, 4XGE Ethernet Card,1*4GE network board,RAID 0/1/5/10 512M,Battery protection,DVDRW, 100V~240VAC,2*3000W(1+1)

Table 5-4 eSight basic management + network traffic analysis

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
● Combination 1: Integrated deployment of eSight basic management + network traffic analyzer + network traffic collector ● Combination 2: Integrated deployment of eSight basic management + network traffic analyzer (excluding the network traffic collector) **NOTE** Configurations are the same in the two scenarios.	● Basic: 0-500 nodes ● Network traffic: 0-10 nodes (2000 flows/s)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 8GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),1*1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE(1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU,32G (4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	● Basic: 500-2000 nodes ● Network traffic: 0-10 nodes (2000 flows/s)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	
	● Basic: 2000-5000 nodes ● Network traffic: 0-10 nodes (2000 flows/s)	● CPU: 4 x quad-core 2 GHz or above ● Memory: 32GB ● Disk space: 320GB **NOTE** A PC server is recommended.	● IBM X3850X5,4*Xeon 8C E7-4820 2.0G Or Above,64G(8*8G), 8*300G,DVDRW, 1*Integrated 1000M NIC (dual),1*1000M NIC (dual),1*1000M NIC (4Port),ServeRAID M5015(512M),iMM System management card, 3Y5*8-2*1975W(1+1)-100V~240VAC ● Tecal RH5885 V2,CH91M05RGPU, RH5885,4*E7-4820 8kernel,2.0GHz-64G (8*8G),8*300G SAS, 4XGE Ethernet Card, 1*4GE network board,RAID 0/1/5/10 512M,Battery protection,DVDRW, 100V~240VAC,2*3000W (1+1)

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
Collector deployed on a different host	0-100 nodes (0-10,000 flows/s)	● CPU: 1 x quad-core 2 GHz or above ● Memory: 4GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,1*E5-2640 6c2.5GHz Or Above,8G(2*4G),2*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC(4Port),ServeRAID M5110e(512M) Battery protection,No Monitor, 2*750W HE(1+1), 100V~240VAC ● Tecal RH2288 V2,BC1M13SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 2*4G,2*300G SAS 2.5,1*4GE LOM,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
	100-350 nodes (10,000-30,000 flows/s)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC(4Port),1*1000M NIC(4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE(1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU,32G(4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))

NOTE

- When the eSight server is planned to manage over 5000 devices, the NTC server must be deployed on a different host from the eSight server.
- When the eSight Network Traffic Analyzer is planned to manage over 100 devices, the NTC server must be deployed on a different host from the eSight server.
- When NTC and eSight platform are deployed on different servers, the database is not required to be installed on the NTC server, but the operating systems must be the same on the NTC and the eSight servers.

Table 5-5 eSight basic management + storage report+ network traffic analysis

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
● Combination 1: Integrated deployment of eSight basic management + network traffic analyzer + network traffic collector ● Combination 2: Integrated deployment of eSight basic management + network traffic analyzer (excluding the network traffic collector) **NOTE** Configurations are the same in the two scenarios.	● Basic: 0-2000 nodes ● Network traffic: 0-10 nodes (2000 flows/s)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 24GB ● Disk space: 250GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),1*1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE(1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU,32G (4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
	● Basic: 2000-5000 nodes ● Network traffic: 0-10 nodes (2000 flows/s)	● CPU: 4 x quad-core 2 GHz or above ● Memory: 32GB ● Disk space: 320GB **NOTE** A PC server is recommended.	● IBM X3850X5,4*Xeon 8C E7-4820 2.0G Or Above,64G(8*8G), 8*300G,DVDRW, 1*Integrated 1000M NIC (dual),1*1000M NIC (dual),1*1000M NIC (4Port),ServeRAID M5015(512M),iMM System management card, 3Y5*8-2*1975W(1 +1)-100V~240VAC ● Tecal RH5885 V2,CH91M05RGPU, RH5885,4*E7-4820 8kernel,2.0GHz-64G (8*8G),8*300G SAS, 4XGE Ethernet Card, 1*4GE network board,RAID 0/1/5/10 512M,Battery protection,DVDRW, 100V~240VAC,2*3000W (1+1)
Network traffic collector deployed on a different host	0-100 nodes (0-10,000 flows/s)	● CPU: 1 x quad-core 2 GHz or above ● Memory: 4GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,1*E5-2640 6c2.5GHz Or Above,8G (2*4G),2*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,No Monitor, 2*750W HE(1+1), 100V~240VAC ● Tecal RH2288 V2,BC1M13SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 2*4G,2*300G SAS 2.5,1*4GE LOM,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
	100-350 nodes (10,000-30,000 flows/s)	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16GB ● Disk space: 250GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above, 32G(4*8G),3*300G(Dual 6Gbps SAS Port),DVDRW, 1*Integrated 1000M NIC (4Port),1*1000M NIC (4Port),ServeRAID M5110e(512M) Battery protection,2*750W HE(1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU,32G (4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))

NOTE

- When the eSight server is planned to manage over 5000 devices, the NTC server must be deployed on a different host from the eSight server.
- When the eSight Network Traffic Analyzer is planned to manage over 100 devices, the NTC server must be deployed on a different host from the eSight server.
- When NTC and eSight platform are deployed on different servers, the database is not required to be installed on the NTC server, but the operating systems must be the same on the NTC and the eSight servers.

Table 5-6 eSight basic management + LogCenter log management

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
● Combination 1: Integrated deployment of eSight basic management + LogCenter log analyzer + LogCenter log collector ● Combination 2: Integrated deployment of eSight basic management + LogCenter log analyzer (excluding the LogCenter log collector) **NOTE** Configurations are the same in the two scenarios.	● Basic: 0-500 nodes ● LogCenter : Syslog 0 - 2000EPS or NAT 0 - 10000EPS	● CPU: 1 x 6-core 2.5 GHz or above ● Memory: 8 GB ● Disk space: 8 TB (Available space: 6 TB) **NOTE** A PC server is recommended.	● Tecal RH2288H V2,BC1M66SRSG,Single Server RH2288H V2 (1*E5-2640 CPU,2*4GB Mem,2*1TB SATA, 4*GE,SR320BC-512MB +BBU,2*460W AC PS) ● Servers,BC1HDD66,HardDisk-1TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD67,HardDisk-2TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD68,HardDisk-3TB-SATA-7200rpm-3.5"-64M
	● Basic: 500-2000 nodes ● LogCenter : Syslog 0-2000EPS or NAT 0-10000EPS	● CPU: 2 x 6-core 2.5 GHz or above ● Memory: 16 GB ● Disk space: 8 TB (Available space: 6 TB) **NOTE** A PC server is recommend	● Tecal RH2288H V2,BC1M67SRSG,Single Server RH2288H V2 (2*E5-2640 CPU,4*8GB Mem,2*1TB SATA, 4*GE,SR320BC-512MB +BBU,2*750W AC PS) ● Servers,BC1HDD66,HardDisk-1TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD67,HardDisk-2TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD68,HardDisk-3TB-SATA-7200rpm-3.5"-64M

Combination	Management Scale	Server Configuration Requirement	Delivery Server Configuration
Log collector deployed on a different host	Distributed deployment 1: Per collector: ● Syslog 0-7000 EPS ● NAT 0-160000 EPS	● CPU: 1 x 6-core 2.5 GHz or above ● Memory: 8 GB ● Disk space: 36 TB (Available space: 33 TB) **NOTE** A PC server is recommend In case of insufficient hard disk space, more servers can be used.	● Tecal RH2288H V2,BC1M66SRSG,Single Server RH2288H V2 (1*E5-2640 CPU,2*4GB Mem,2*1TB SATA, 4*GE,SR320BC-512MB +BBU,2*460W AC PS) ● Servers,BC1HDD66,HardDisk-1TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD67,HardDisk-2TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD68,HardDisk-3TB-SATA-7200rpm-3.5"-64M
	Distributed deployment 2: Per collector: ● Syslog 0-10500 EPS ● NAT 0-240000 EPS	● CPU: 2 x 6-core 2 GHz or above ● Memory: 32 GB ● Disk space: 36 TB (Available space: 33 TB) **NOTE** A PC server is recommend In case of insufficient hard disk space, more servers can be used.	● Tecal RH2288H V2,BC1M67SRSG,Single Server RH2288H V2 (2*E5-2640 CPU,4*8GB Mem,2*1TB SATA, 4*GE,SR320BC-512MB +BBU,2*750W AC PS) ● Servers,BC1HDD66,HardDisk-1TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD67,HardDisk-2TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD68,HardDisk-3TB-SATA-7200rpm-3.5"-64M

Table 5-7 eSight basic management + storage report management + infrastructure management

Management Scale	Server Configuration Requirement	Delivery Server Configuration
0-500 nodes	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16 GB ● Disk space: 120GB **NOTE** A PC server is recommended.	● X3650M4,2*Xeon 6C E5-2640 2.5G Or Above,32G(4*8G), 3*300G(Dual 6Gbps SAS Port),DVDRW,1*Integrated 1000M NIC(4Port),1*1000M NIC (4Port),ServeRAID M5110e (512M) Battery protection, 2*750W HE(1+1)-100V~240VAC ● Tecal RH2288 V2,BC1M12SRSB,Tecal RH2288-(2*E5-2640 6_core 2.5GHz CPU, 32G(4*8G),3*300G SAS 2.5,1*4GE LOM,1*4GE NIC,RAID 0/1/5/10,DVD-RW, 512M-2*750W(1+1))
500-5000 nodes	● CPU: 2 x six-core CPUs, 2.5 GHz or above ● Memory: 32 GB ● Disk space: 250 GB **NOTE** A PC server is recommended.	

Table 5-8 Integrated deployment of all components (basic management, storage report, network traffic analysis, and LogCenter, excluding infrastructure management)

Management Scale	Server Configuration Requirement	Delivery Server Configuration
● Basic: 0-200 nodes ● Network traffic: 0-10 nodes (2000 flows/s) ● LogCenter: Syslog 0-1000EPS or NAT 0-5000EPS	● CPU: 2 x quad-core 2 GHz or above ● Memory: 16 GB ● Disk space: 4 TB (Available space: 3 TB) **NOTE** A PC server is recommended.	● Tecal RH2288H V2,BC1M67SRSG,Single Server RH2288H V2(2*E5-2640 CPU, 4*8GB Mem,2*1TB SATA, 4*GE,SR320BC-512MB+BBU, 2*750W AC PS) ● Servers,BC1HDD66,HardDisk-1TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD67,HardDisk-2TB-SATA-7200rpm-3.5"-64M ● Servers,BC1HDD68,HardDisk-3TB-SATA-7200rpm-3.5"-64M

5.3 Client Configuration Requirements

The eSight client has no special requirement on the operating system, but has the following requirements on the memory and browser:

- Browser: Internet Explorer 8 or 9; Firefox 22.

NOTE

The recommended web browser is Internet Explorer 9 or Firefox 22.

- Memory: 1 GB or above

5.4 Network Bandwidth Requirements

To ensure the normal running of the eSight system, ensure that network bandwidths meet the basic network bandwidth requirements.

The method for calculating network bandwidth required in the eSight system is as follows:

Bandwidth between the eSight server and client: 2 Mbit/s

Bandwidth between active and standby servers in a two-node cluster: 50 Mbit/s

Total bandwidth between eSight and devices = Device management bandwidth + Additional bandwidth for terminal upgrade + Additional bandwidth for network traffic + Additional LogCenter bandwidth + Additional bandwidth for deploying the operating system for servers

- Device management bandwidth (X indicates the total number of devices, including terminals and other box devices):
  - X < 2000, required bandwidth: 2 Mbit/s
  - X > 2000, required bandwidth: 2 Mbit/s + (X – 2000) x 0.8 kbit/s
- Additional bandwidth for terminal (IP phones and CPEs) upgrade (Y indicates the number of terminals):

  (Y/10) x 256 kbit/s

  NOTE

  The planned bandwidth for each terminal upgrade is 256 kbit/s. In the formula, **Y/10** indicates that 10% terminals are concurrently upgraded. eSight allows users to upgrade 100 terminals at the same time, requiring 25.6 Mbit/s.
- Additional bandwidth for network traffic:

  N x 400 bit/s

  NOTE

  - In the formula, **N** indicates the number of flows and its unit is flow/s.
  - The bandwidth for a flow is calculated as follows: (1500/30) x 8 bit/s = 400 bit/s. Here, 1500 indicates that the average size of a NetStream packet is 1500 bytes, and 30 indicates that a NetStream packet has about 30 flows.
  - 10000 flows require a bandwidth of 3.8 Mbit/s.
- Additional LogCenter bandwidth (between the LogCenter collector and devices)
  - Integrated deployment of the collector and eSight: 1.5 Mbit/s (300 bytes per syslog and 150 bytes per session log)
  - Distributed deployment 1 (see **Table 5-6**): 24 Mbit/s
  - Distributed deployment 2 (see **Table 5-6**): 36 Mbit/s
- Additional bandwidth for deploying the operating system for servers

  15 Mbit/s

NOTE

eSight allows users to load and deploy the operating system mirroring file through PXE. Deploying the operating system for each server requires 1.5 Mbit/s. eSight allows users to deploy the operating system for a maximum of 10 servers at the same time, requiring 15 Mbit/s.

6 Technical Counters

eSight can manage a maximum of 20,000 NEs and allows a maximum of 100 online clients concurrently. The technical counters for eSight are as follows.

Table 6-1 Technical counters

Counter	Value
Capacity for storing current alarms	20,000
Capacity for storing historical alarms	15 million
Capacity for storing events	2 million
Capacity for storing audit logs	3 million
Alarm processing capacity (number/second)	100
Maximum number of topology objects supported by a subnet	500
Maximum number of topology object layers supported by topology management	11

7 Standard and Protocol Compliance

eSight complies with the following standards and protocols:

- SNMP and MIB-II standards for interfaces between eSight and devices
  - RFC1155: structure and identification of management information for TCP/IP-based Internet
  - RFC1157: simple network management protocol
  - RFC1213: version 2 of management information base (MIB-II) for network management of TCP/IP-based Internet
- XML 1.0
- ITU-T X.733: fault management specification
- JSR-286 Portlets specifications: Java Portlet specification v2.0
- HTTP/1.0|HTTP/1.1: Hypertext Transfer Protocol
- HTTPS: Hypertext Transfer Protocol Secure
- SIP (RFC3261)
- TCP (RFC0872)
- TCP/UDP (RFC1356)
- SMI-S Storage Management Suggestion and Guide
- Modbus

A Glossary

Glossary	Description
A	
Aerial view	A window of the eSight, which displays a thumbnail of the current topology view.
Alarm	A message reported when a fault is detected by a device or by the network management system during the process of polling devices. Each alarm corresponds to a recovery alarm. After a clear alarm is received, the status of the corresponding alarm changes to cleared.
Alarm locating	A function that helps locate the topology object generating the alarm when an alarm is selected.
Alarm masking	An alarm management method. Alarms that are set to be masked are not displayed on the NMS or the NMS does not monitor unimportant alarms.
Alarm panel	A pane that displays on the eSight client. It displays the statistics of current alarms in different colors. By watching the alarm board, you can monitor the entire network in real-time and know the severity of an alarm and its related statistics.
C	
CLI	Command Line Interface: A form of human interface to cloud storage software characterized by non-directive prompting and character string user input.
Client	A device that sends requests, receives responses, and obtains services from the server.
Collection period	An interval at which the measurement results are output. During the measurement time, the system selects the given period as granularity to perform test and output the results.
CPU	Central Processing Unit.

Glossary	Description
D	
Data backup	A method that is used to copy key data to the standby storage area, to prevent data loss in the case of damage or failure in the original storage area.
Dump	To export alarm data from the database to the customized file. Meanwhile the exported data is cleared in the database.
E	
eLTE	Enterprise Long Term Evolution
Encryption	A function used to transform data so as to hide its information content to prevent it's unauthorized use.
ESN	Equipment Serial Number.
Event	Anything that takes place on the managed object. For example, the managed object is added, deleted, or modified.
eWL	Enterprise Wireless
F	
Fault	A failure to implement the function while the specified operations are performed. A fault does not involve the failure caused by preventive maintenance, insufficiency of external resources or intentional settings.
FTP	File Transfer Protocol.
I	
iEMP	Intelligent Enterprise Management Platform.
IP	Internet Protocol.
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector.
M	
Masked alarm	An alarm whose correlation action is set to masked in alarm correlation analysis.
MIB	Management Information Base: A type of database used for managing the devices in a communications network. It comprises a collection of objects in a (virtual) database used to manage entities (such as routers and switches) in a network.
N	

Glossary	Description
NBI	NorthBound Interface: An interface that connects to the upper-layer device to provision services and report alarms and performance statistics.
NE	An entity that contains hardware and software. A network element(NE) has at least one main control board that manages and monitors the entire network element. The NE software runs on the main control board.
O	
Operation log	A list of information about operation events.
OSS	Operating Support System.
P	
Performance alarm	An alarm generated when the actual result of a measurement entity equals the predefined logical expression for threshold or exceeds the predefined threshold.
Physical view	The default view that is used to display all devices and the topology partition (according to the area or the maintenance relationship) in the network.
Plaintext	In cryptography, the original readable text before it is encrypted.
R	
RSA	Revist-Shamir-Adleman Algorithm.
S	
Security log	A type of log that records the security operations on the eSight, such as logging in to the eSight, modifying the password, and logging out of the eSight.
Session	A logical connection between two nodes on a network for the exchange of data. It generally can apply to any link between any two data devices. A session is also used simply to describe the connection time.
SFTP	Secure File Transfer Protocol.
SNMP	Simple Network Management Protocol.
SOAP	Simple Object Access Protocol.
Southbound interface	The interface that is used to connect the lower layer NMS to the device and implement the functions of providing services and performance index data.
STelnet	Secure Shell Telnet.

Glossary	Description
Subnet	A type of smaller networks that form a larger network according to a rule, for example, according to different districts. This facilitates the management of the large network.
System log	System log tracks miscellaneous system events like startup, shutdown and events like hardware and controller failures.
T	
TCP	Transmission Control Protocol.
Topology object	A basic element in the eSight topology view, which includes submap, node, connection, and so on.
Topology view	A basic component for the man-machine interface. The topology view directly displays the networking of a network as well as the alarm and communication status of each network element and subnet. The topology view reflects the basic running conditions of the network.
U	
UDP	User Datagram Protocol.
V	
Virtual link	The logical connection between topological objects in the eSight topology view.
Virtual NE	Virtual NEs are NEs that cannot be managed by the eSight in the entire network.An object similar to a common NE and is also displayed with an icon on a view. A virtual NE, however, is only an NE simulated according to the practical situation, which does not represent an actual NE. Therefore, the actual status of this NE cannot be queried and its alarm status cannot be displayed with colors.
X	
XML	Extensible Markup Language.