

# Huawei eSight Network Full Product Datasheet





# HUAWEI eSight Network







# Contents

- 01 | Huawei eSight Network Full Product Datasheet
- 05 | eSight Network Management Platform
- 11 | eSight Network Device Manager
- 15 | eSight Network Agile Reporter
- 17 | eSight Network SLA Manager
- 21 | eSight Network Traffic Analyzer
- 29 | eSight Network WLAN Manager
- 43 | eSight Mobile Manager
- 47 | eSight Network IPSec VPN Manager
- 51 | eSight Network Secure Center
- 54 | More Information

# Huawei eSight Network Full Product Datasheet

## Product Overview

With the development of enterprise network applications and the expansion of network scale, a large number of routers, gateways, and wireless local area network (WLAN) devices are used on enterprise campus and branch networks. Enterprises must provide multiple mobile offices, rather than a fixed location, for their employees, and support diversified services, complicating network management. They urgently need a unified network management system to improve efficiency and ensure normal operation of enterprise services.

Huawei eSight Network is based on the following concepts: topology-centric, simplified management, and improved operation and maintenance (O&M) efficiency. Network administrators can gain an overall understanding of the network status by viewing the topology. eSight Network not only provides basic network management capabilities (alarm, topology, performance, and configuration) but also proactive warnings of potential network faults. In addition, eSight Network provides abundant fault location methods to help administrators effectively locate and rectify faults. eSight Network provides an all-round, open, and unified management platform, and various service components, to implement unified management of devices, services, and applications.

## Product Features

### Ease to Use

- User-friendly Graphical User Interface (GUI) and smooth operations
- Active monitoring and visible O&M
- Mobile O&M, agile and open

### Unified Management

- Multi-type device management

### Smart O&M

- Plug-and-play
- Automatic network quality sensing
- Full lifecycle management



## Product Components

eSight Network provides a unified O&M platform and specific components to meet enterprise user requirements.

Component	Description
eSight Network Management Platform	Provides NMSs of the compact, standard, and professional editions for enterprise users. Supports unified management of devices from various types, topology management, fault management, performance management, and user right management.
eSight Network Device Manager	Manages network devices from multiple types. Provides the IP topology and link management functions for monitoring the network topology and changes in real time. Provides the smart configuration tool, configuration file management, and device software management to update configuration files and software versions.
eSight Network Agile Reporter	Analyzes report data from multiple dimensions and allows users to flexibly drag required content to be contained in reports, implementing complex query from Big Data. Displays reports in an easy-to-understand manner.
eSight Network Open SDK	Provides Simple Network Management Protocol (SNMP), RESTful Open APIs, and File Transfer Protocol (FTP) interfaces to integrate with third-party systems.
eSight Network SLA Manager	Implements visible monitoring on network quality by combining the following methods: simulation flow-based and real service flow-based network quality detection. Monitors network quality using simulation flows by integrating with devices' Network Quality Analysis (NQA) function to diagnose and measure link performance between network devices 24x7 and displays Quality of Service (QoS) statistics. eSight Network notifies administrators remotely when QoS reaches the threshold set by administrators. Administrators can use the quick diagnosis function to monitor link performance in real time and diagnose faults, which improves management efficiency. Implements network quality detection based on iPCA, which is the industry's first multiple-input-multiple-output quality measurement technology and solves the N <sup>2</sup> connection problem in traditional point-to-point quality measurement technologies. iPCA technology uses the enhanced area-based packet conservation mechanism to monitor the quality on a connectionless network and also provides accurate fault location capabilities.
eSight Network Traffic Analyzer	Analyzes network traffic based on NetFlow, NetStream, and sFlow protocols. This helps network administrators monitor traffic and bandwidth usage on enterprise campus egress and wireless campus networks, generate traffic analysis reports, and detect network bottlenecks in a timely manner, providing evidence for network planning and fault diagnosis.
eSight Network WLAN Manager	Provides integrated management of wired and wireless networks. Supports full lifecycle WLAN management, including visible planning (highly-efficient WLAN planning with professional tools), fast service provisioning in three steps, active O&M, all-round quality awareness regionally or globally. Provides search-centric E2E one-click fault diagnosis, interference source locating, and spectrum analysis to implement highly efficient troubleshooting. Provides position-based terminal location and northbound interfaces to achieve mutual benefits from the wireless network.



Component	Description
eSight Mobile Manager	Allows administrators to manage WLANs using mobile terminals with the 360-degree WLAN monitoring and fault diagnosis, and advertisement pushing apps. With eSight Mobile, administrators can manage WLANs anytime, anywhere. Provides open SDK to allow third parties to develop various industrial applications, building a win-win ecosystem.
eSight Network IPSec VPN Manager	Automatically discovers IPSec VPN services on the hub-spoke and site-to-site networks and provides all-round monitoring and diagnostic functions, including service alarm status monitoring, service topology, performance monitoring, service diagnosis, and historical tunnel information display.
eSight Network Secure Center	Provides unified security policy management functions for the firewalls.



A scenic winter landscape featuring a calm lake in the middle ground, surrounded by snow-covered rocks in the foreground and a dense forest of evergreen trees in the background. The sky is a clear, deep blue with some light, wispy clouds. The overall atmosphere is serene and cold.

# HUAWEI eSight Network



# eSight Network Management Platform

## Product Overview

As the network scales and the number of enterprise network applications continues to grow, more devices are deployed. Multiple service routers, security gateways, and wireless local area network (WLAN) access points (APs) are used to implement communications and collaboration services in decentralized enterprise campus and branch office networks. Enterprises are using an increasing number of core and access devices provided by multiple vendors. Each device has its own management system, creating confusion for system and network administrators.

To alleviate the operational burden, Huawei has developed the eSight Network Management Platform, a unified network management system that provides a comprehensive view and management of all network and system resources, ensures network stability, and improves O&M efficiency.

The eSight Network Management Platform provides compact, standard, and professional editions for enterprise users. It supports unified management of devices, topology management, fault management, performance management, and user right management.

## Features

eSight Network provides compact, standard, and professional editions for enterprise users.

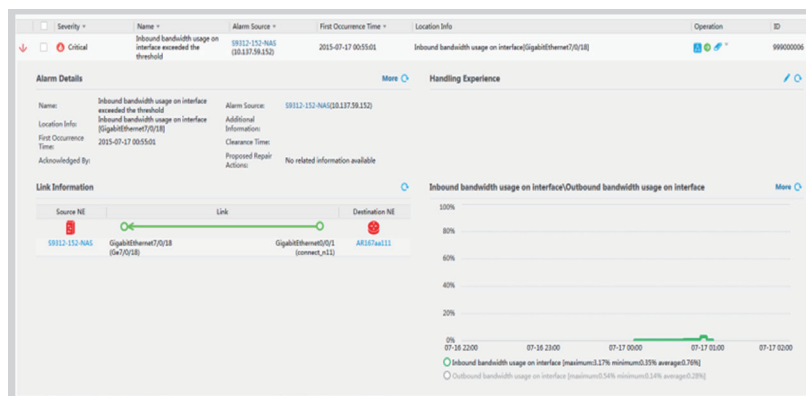
Edition	Functions
Compact edition	<ul style="list-style-type: none"> <li>• Basic network management capabilities: alarms, performance, topology management, Network Elements (NEs), logs, security management, maintenance tools, database backup tool, and fault collection tool.</li> <li>• Applies to monitoring on small-scale networks management with 40 NEs.</li> </ul>
Standard edition	<ul style="list-style-type: none"> <li>• Basic network management capabilities: alarms, performance, topology management, Network Elements (NEs), logs, security management, maintenance tools, database backup tool, and fault collection tool.</li> <li>• Supports service components that can be installed due to service needs.</li> <li>• Provides all-around network management functions that address most network management needs of 5000 NEs.</li> </ul>
Professional edition	<ul style="list-style-type: none"> <li>• All functions of the standard edition.</li> <li>• High Availability (HA).</li> <li>• A single NMS of the professional edition applies to large-scale network management with up to 20,000 NEs.</li> </ul>

eSight Network provides rights-based, domain-based, and time-based authorization, and flexible network user authentication methods.

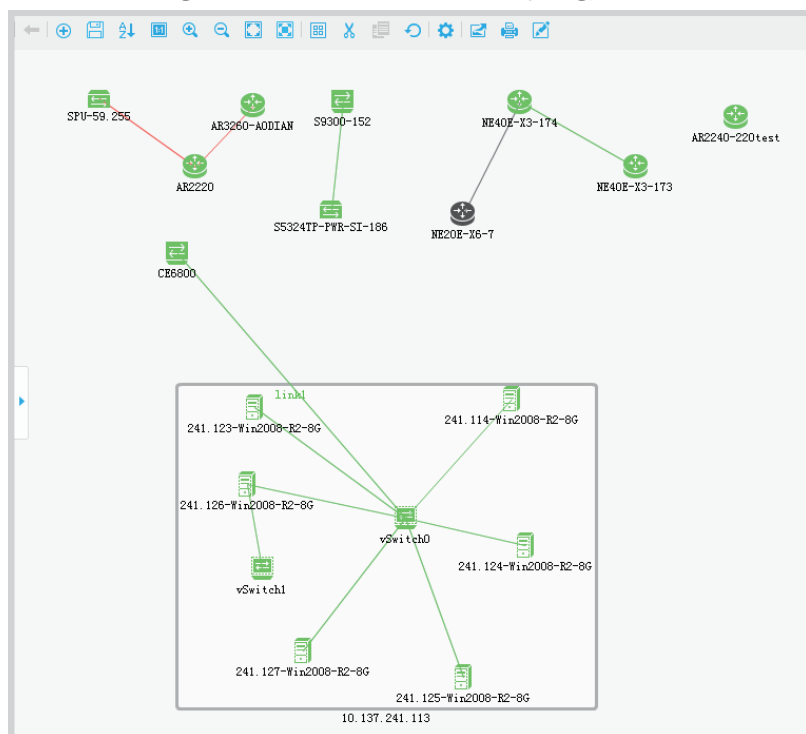
- eSight Network enables refined management authorization by assigning different user names and passwords to administrators and by controlling administrator management authority, management range, time range allowed to log in, and IP range allowed to log in.
- eSight Network supports Lightweight Directory Access Protocol (LDAP), RADIUS, and local authorization methods.

The comprehensive fault monitoring system enables real-time fault diagnosis and quick troubleshooting.

- eSight Network provides unified monitoring of alarms on the entire network and informs maintenance personnel of the alarms in the first instance through alarm sounds, remote alarm notification (email and SMS), and the alarm panel, ensuring timely troubleshooting.
- eSight Network supports alarm analysis and processing. eSight Network provides alarm locating functions to switch to NEs, ports, and services, shield, suppress, and categorize alarms, analyze alarm correlation, redefine the alarm severity, and maintain the experience library, improving troubleshooting accuracy and efficiency.
- eSight Network supports customization for alarm shield, redefinition, and alarm sounds to meet specific requirements in different scenarios.
- eSight Network provides correlation analysis for a large number of alarms to improve alarm effectiveness, and centrally displays alarms to improve management efficiency.



eSight Network provides visual management of the entire network topology and status monitoring.

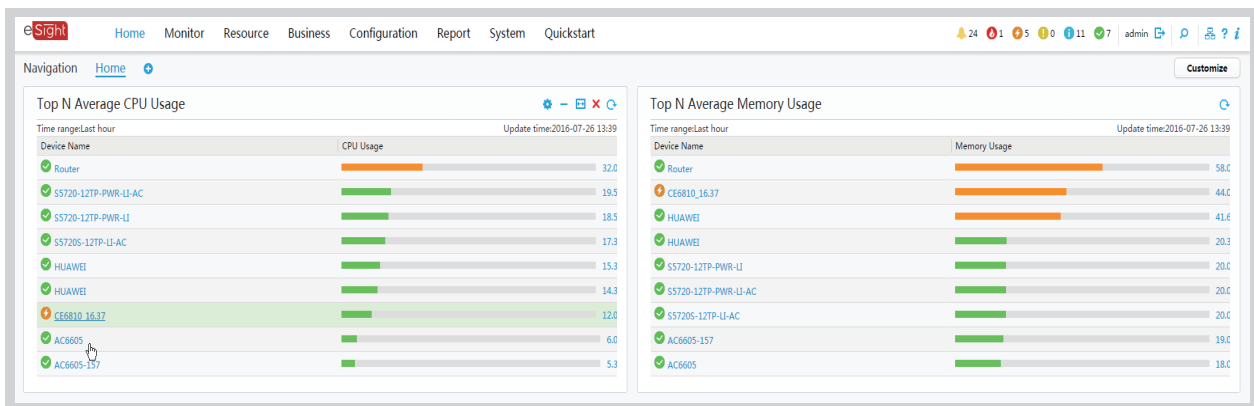




- Various device discovery methods: eSight Network can discover devices automatically, separately, or in a batch. The automatic device discovery model can add new devices periodically. eSight Network supports management of devices with IPv6 addresses.
- Simplified management on network topologies: eSight Network provides physical topologies and shows network structure hierarchically. Administrators can view network resource alarm states and basic link information. eSight Network also supports customization in the topology view.
- eSight Network shows device, frame, board, subcard, port on panel, and port state, and allows administrators to enable or disable ports.
- Powerful performance management: eSight Network provides performance parameter management templates, supports batch device performance monitoring, visual performance data view, and history date analysis. Administrators can set different alarm severity and threshold levels and determine whether to send an alarm based on the number of times that performance indexes exceed the threshold value, lowering report errors and improving alarm accuracy.
- Group-based management: After a device is added to eSight Network, the device is automatically added to the group based on the specified rules and is granted with policies in the group.

eSight Network displays key performance counters in portlets on the home page, and allows you to search for required portlets by keyword.

- The customized portal allows users to receive all information on the home page. eSight Network can also integrate third-party software portals with the home page.
- Convenient resource searching on the entire network helps administrators quickly locate resources and access corresponding services.



B/S architecture supports multiple operating systems.



- eSight Network uses Browser/Server (B/S) architecture, which does not require any client software. The server need only be updated when the software updates.
- The platform supports Windows and SUSE Linux operating systems and Oracle, and SQL Server databases.

Disaster Recovery (DR) protection ensures service continuity and system reliability.





- eSight Network supports two-node clusters in hot standby mode.
- eSight Network supports the Linux operating system.

## Operating Environment

Configuration requirements for the eSight Network Management Platform (compact edition) are as follows:

Operating System	Server Configuration Requirement	Virtual machine Configuration Requirement
Windows Server 2012 R2 standard (64 bits)	CPU: 2 x dual-core 2 GHz or higher Memory: 8 GB or higher Disk space: 300 GB or higher Database: Microsoft SQL Server 2012 standard Minimum disk IO speed greater than 100MB/s, recommended 180MB/s above.  <b>NOTE</b> PC servers are recommended.	VMWare ESXI 5.0/5.5、 FusionSphere V1R5、 Hyper-V CPU: 8 vCPU 2 GHz or higher Memory: 8 GB or higher Disk space: 300 GB or higher Database: Microsoft SQL Server 2012 standard  <b>NOTE</b> Determine the hardware specifications based on the network scale and required components.

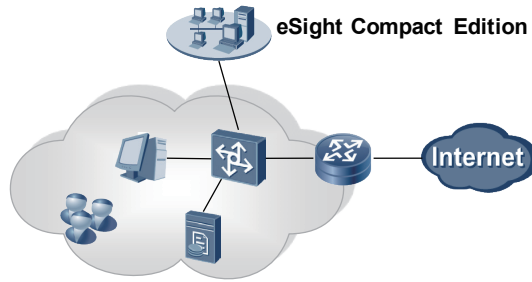
Configuration requirements for the eSight Network Management Platform (standard and professional editions) are as follows:

Operating System	Server Configuration Requirement	Virtual machine Configuration Requirement
Windows Server 2012 R2 standard (64 bits)	CPU: 2 x hexa-core 2 GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Minimum disk IO speed greater than 100MB/s, recommended 180MB/s above. Database: Microsoft SQL Server 2012 standard  <b>NOTE</b> PC servers are recommended. Determine the hardware specifications based on the network scale and required components.	VMWare ESXI 5.0/5.5、 FusionSphere V1R5、 Hyper-V CPU: 16 vCPU 2 GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Microsoft SQL Server 2012 standard  <b>NOTE</b> Determine the hardware specifications based on the network scale and required components.
Novell SUSE Linux Enterprise Server-Multi-language-Enterprise-12.0 SP2	CPU: 2 x hexa-core 2 GHz or higher Memory: 32 GB Disk space: 600 GB Minimum disk IO speed greater than 100MB/s, recommended 180MB/s above. Database: Oracle Database Standard Edition 11g R2  <b>NOTE</b> PC servers are recommended. Determine the hardware specifications based on the network scale and required components.	VMWare ESXI 5.0/5.5、 FusionSphere V1R5、 Hyper-V CPU: 16 vCPU 2 GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Oracle Database Standard Edition 11g R2  <b>NOTE</b> Determine the hardware specifications based on the network scale and required components.

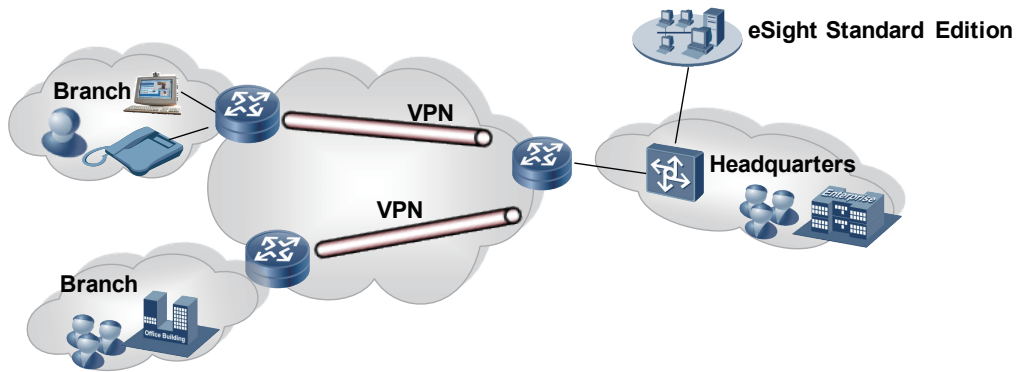


## Deployment Scenarios

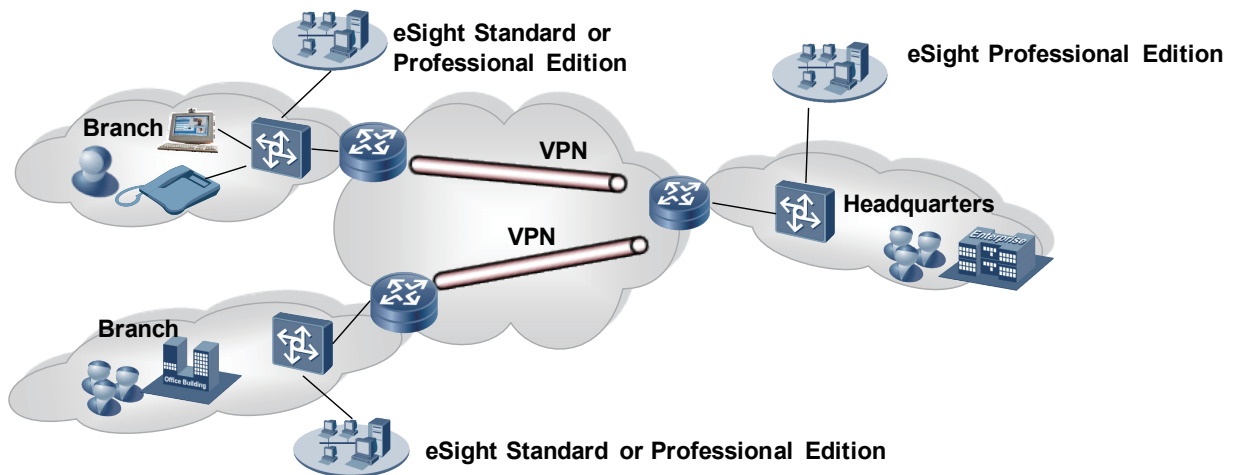
The eSight Network does not have special requirements when managed devices are connected to the eSight Network server and devices support the Simple Network Management Protocol (SNMP). eSight Network compact edition applies to small- and medium-sized enterprises.



eSight Network standard edition applies to medium- and large-sized enterprises.



eSight Network professional edition applies to ultra-large enterprises, management scale can be reached 20000 network element.



## Ordering Information

Ordering information for eSight Network compact edition

Item	Quantity	Remarks
eSight Network Application Base-Compact (includes 40 devices license)	1	Mandatory for eSight Network Management Platform

Ordering information for eSight Network standard edition

Item	Quantity	Remarks
eSight Network Management Platform-Standard	1	Mandatory for eSight Network Management Platform

Ordering information for eSight Network professional edition

Item	Quantity	Remarks
eSight Network Management Platform-Professional I	1	Mandatory for eSight Network Management Platform



# eSight Network Device Manager

## Product Overview

Manages network devices and provides the IP topology and link management functions for monitoring the network topology and changes in real time.

Provides the smart configuration tool, configuration file management, and device software management to update configuration files and software versions.

## Features

eSight Network monitors terminals connected to the network devices to prevent unauthorized users from consuming network resources.

- Terminal resource management: eSight Network provides comprehensive terminal access records, including MAC, IP address, device name, and port number, helping administrators find the switch and port on the switch through which a terminal is connected to the network. Administrators can configure the authorized terminal IP address, MAC address, and PORT-IP, PORT-MAC, and IP-MAC matching rules. When a terminal accesses the network illegally, eSight Network sends emails and records comprehensive information about the illegal terminal, providing the basis for audits of illegal users.

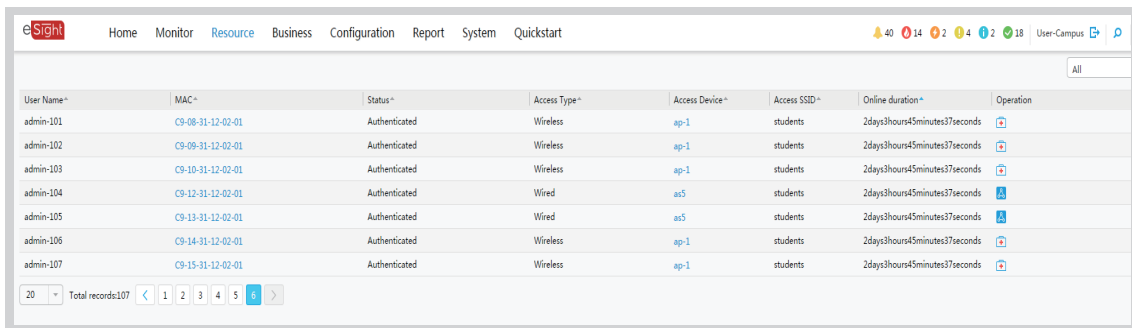
eSight Network supports wired and wireless convergence management.

- Unified configuration for wired and wireless services: eSight Network supports the unified configuration of wired and wireless services based on the service matrix (including resource groups and service profiles), improving configuration efficiency. When a device goes online, the device is automatically added to the specified resource group and is granted with the corresponding policies. Plug-and-play is therefore implemented.

Profile	AP System Profile	AP Port Profile	2G Radio Profile	5G Radio Profile	VAP Profile	NAC Profile
AP Group of Visitor	visitorSystemProfile	vistorWiredportProfile	visitor-20MHZ	visitor-5g-80MHz	visitorVapProfile	
AP Group of BYOD	byodSystemProfile	byodWiredportProfile		byod-5g-80MHz	byodVapProfile	
AP Group of RD	rdSystemProfile	rdWiredportProfile	rd-20MHZ	rd-5g-80MHz	rdVapProfile	
Port Group of Access						wireless-nac-profile

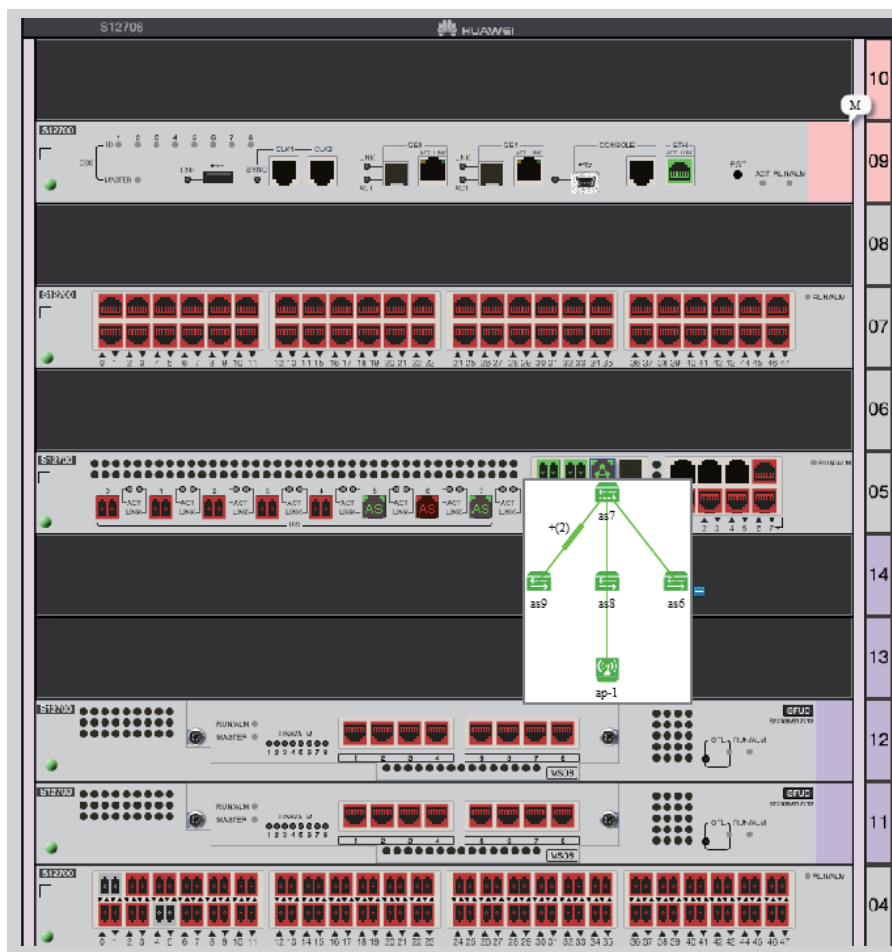


- Unified management on wired and wireless users: eSight Network monitors wired and wireless users in a unified manner. When associated with WLAN Manager, eSight Network can quickly rectify faults on wireless users.



User Name	MAC	Status	Access Type	Access Device	Access SSID	Online duration	Operation
admin-101	C9-08-31-12-02-01	Authenticated	Wireless	ap-1	students	2days3hours45minutes37seconds	[X]
admin-102	C9-09-31-12-02-01	Authenticated	Wireless	ap-1	students	2days3hours45minutes37seconds	[X]
admin-103	C9-10-31-12-02-01	Authenticated	Wireless	ap-1	students	2days3hours45minutes37seconds	[X]
admin-104	C9-12-31-12-02-01	Authenticated	Wired	as5	students	2days3hours45minutes37seconds	[X]
admin-105	C9-13-31-12-02-01	Authenticated	Wired	as5	students	2days3hours45minutes37seconds	[X]
admin-106	C9-14-31-12-02-01	Authenticated	Wireless	ap-1	students	2days3hours45minutes37seconds	[X]
admin-107	C9-15-31-12-02-01	Authenticated	Wireless	ap-1	students	2days3hours45minutes37seconds	[X]

- Display of wired and wireless devices on one panel: Based on super virtual fabric (SVF) technology, eSight Network manages multiple access and aggregation switches as one switch. Information about access switches, APs, and users is displayed on one panel.



Simple and convenient daily maintenance operations and lower technical requirements improve work efficiency.

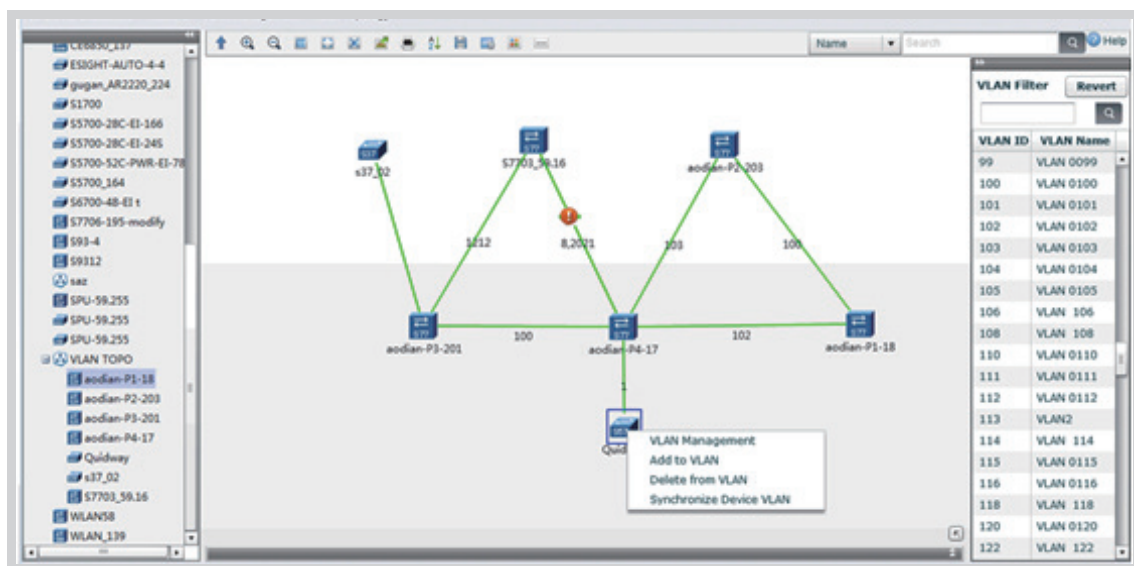
- Intelligent configuration: eSight Network is preconfigured with multiple common service configuration templates. Users can select an appropriate template to perform the same configurations on devices in a batch or use a file to perform configurations on groups of devices in a batch.
- Configuration file management: Configuration files for multiple devices can be backed up, compared, and restored. The backup function includes immediate backup and periodic backups, and backups triggered by device configuration changes. When the device configuration changes, eSight Network can trigger alarms and send alarm notification through email.

- MIB management: eSight Network provides Management Information Base (MIB) compilation, loading functions and Get, GetNext, Walk, and TableView operations.
- Supports device software upgrade and management.
- Compliance check: eSight Network supports to create, delete, modify and view the compliance check tasks. The tasks can be executed immediately and periodically. When compliance check fails, eSight Network can trigger alarms.

### eSight Network supports unified VLAN resource management.

eSight Network allows administrators to create and delete VLAN resources, deliver VLAN configurations, view resources in the VLAN topology, and collect VLAN statistics on the entire network.

- VLAN resource management: eSight Network displays VLAN resources on the entire network. Administrators can add, delete, and modify VLANs, and view devices and interfaces whose packets can pass through the specified VLAN. When administrators delete a VLAN, eSight Network can display all devices and interfaces related to the VLAN to prevent misoperation.
- VLAN device management: eSight Network allows administrators to perform interface and VLAN configurations for multiple devices in a batch and can quickly switch to the NE manager. Administrators can view, add, and modify VLAN information on the device panel of the NE manager and can also configure voice VLANs.
- Visible VLAN topology: eSight Network can filter device and link information based on the VLAN. Administrators can add or remove multiple devices and links to a VLAN. eSight Network can also filter MSTP loop prevention flags based on the VLAN.



## Operating Environment

eSight Network Device Manager is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.

## Deployment Scenarios

Deployment scenarios for eSight Network Device Manager are the same as those for eSight Network Management Platform.

## Ordering Information

Ordering information for eSight Network standard edition

Item	Quantity	Remarks
eSight Network Management Platform-Standard	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network Standard NMS License (for 25 incremental devices)	Optional	One license manages 25 incremental devices.
eSight Network Standard NMS License (for 50 incremental devices)	Optional	One license manages 50 incremental devices.
eSight Network Standard NMS License (for 100 incremental devices)	Optional	One license manages 100 incremental devices.
eSight Network Standard NMS License (for 200 incremental devices)	Optional	One license manages 200 incremental devices.
eSight Network Standard NMS License (for 300 incremental devices)	Optional	One license manages 300 incremental devices.
eSight Network Standard NMS License (for 500 incremental devices)	Optional	One license manages 500 incremental devices.
eSight Network Standard NMS License (for 1,000 incremental devices)	Optional	One license manages 1,000 incremental devices.

Ordering information for eSight Network professional edition

Item	Quantity	Remarks
eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network Professional NMS License (for 50 incremental devices)	Optional	One license manages 50 incremental devices.
eSight Network Professional NMS License (for 100 incremental devices)	Optional	One license manages 100 incremental devices.
eSight Network Professional NMS License (for 200 incremental devices)	Optional	One license manages 200 incremental devices.
eSight Network Professional NMS License (for 300 incremental devices)	Optional	One license manages 300 incremental devices.
eSight Network Professional NMS License (for 500 incremental devices)	Optional	One license manages 500 incremental devices.
eSight Network Professional NMS License (for 1,000 incremental devices)	Optional	One license manages 1,000 incremental devices.



# eSight Network Agile Reporter

## Product Overview

Huawei eSight Network Agile Reporter analyzes report data from multiple dimensions and allows users to flexibly drag required content to be contained in reports, implementing complex query from Big Data. It displays reports in an easy-to-understand manner.

## Features

eSight Network quickly generates reports in drag-and-drop mode, meeting requirements in specific scenarios.

- Measurement counters of various dimensions are predefined on eSight Network. Users can drag them to the corresponding lines or columns based on actual needs to generate customized reports.

The screenshot shows the eSight Network Agile Reporter interface. The top navigation bar includes Home, Monitor, Resource, Business, Configuration, Reports, System, and Quickstart. The main area is divided into several sections:

- Available Fields:** A list of fields for configuration, including Dimensions (Time, Area, Device Manufacturer, Device Category, Device Type, Interface) and Measures (Default Measures, Avg Outbound bandwidth, Max Outbound bandwidth, Avg Receiving rate, Max Receiving rate, Avg Sending rate, Max Sending rate, Avg Inbound bandwidth, Max Inbound bandwidth).
- Data Source:** Interface Statistics(23)
- Row and Column Configuration:** Fields for Year, Month, Day, Hour, Minute, Category, Type, Name, and Interface Description are selected for the Row. Measures for Avg Receiving rate and Avg Sending rate are selected for the Column.
- Table:** A data table with columns: Year, Month, Day, Hour, Minute, Category, Type, Name, Interface Description, Avg Receiving rate(Byte/s), and Avg Sending rate(Byte/s). The table displays data for various network devices and interfaces, including AR1220V, MSR30-20, and 2911.

- eSight Network supports data update in real time. It updates the query results in real time based on selected search criteria.
- Users can create, delete, edit, and execute scheduled reports.

eSight Network displays abundant data and provides data analysis capability to meet statistics requirements.

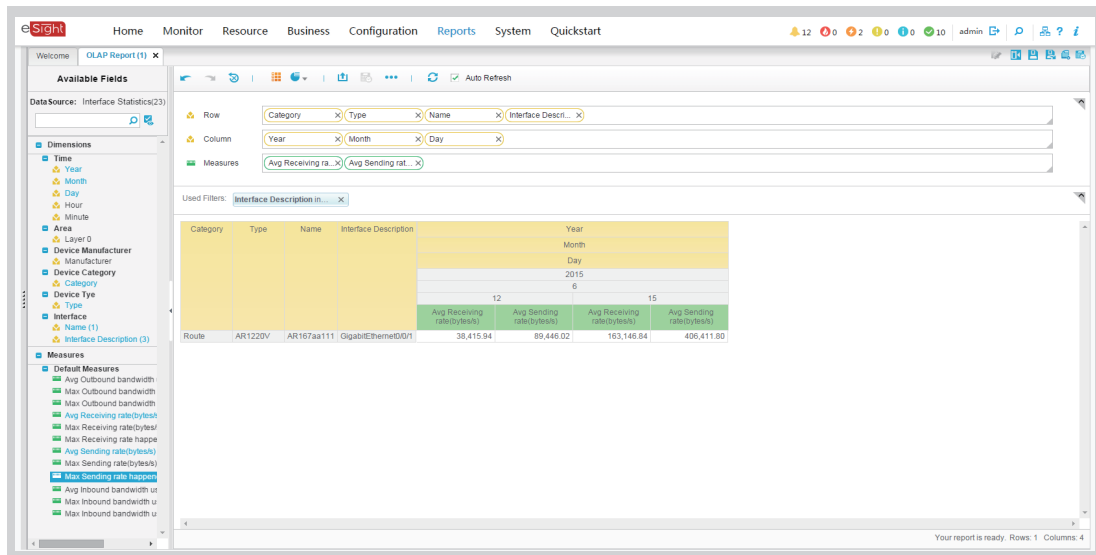
- Supports functions such as sorting, filtering, classification, and slicing, without secondary processing of Excel.

The screenshot shows the eSight Network Agile Reporter interface, similar to the previous one, but with a context menu open over the table. The menu options include:

- Edit Column Name
- Configure Header Background Color
- Merge
- Filter
- Filter by Top N...
- Sort (checked)
- Show Subtotals
- Hyperlink
- Remove from Report
- Also Show
- Show Priorities

The table data is the same as in the previous screenshot, showing network device statistics.

- Supports year-on-year and month-on-month data comparison to accurately evaluate the service change trend.



- Supports visible real-time monitoring and multiple display modes, including the line chart, bar chart, and pie chart.

eSight Network dynamically displays multi-dimensional data to facilitate quick data analysis.

- Supports details statistics, Top N sorting, threshold setting, and table-chart conversion.
- Supports space dimensions including NE, subnet, and region, and links, cards, APs, SSIDs, and radios.
- Supports comprehensive report statistics, such as interface information statistics (interface status, interface traffic, and interface performance), device resource usage statistics (CPU and memory), and wireless resource usage statistics (access users, AP traffic, AP rate, AP access failure, air interface usage, and AP radio frequency).

## Operating Environment

eSight Network Agile Reporter is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.

## Deployment Scenarios

Deployment scenarios for eSight Network Agile Reporter are the same as those for eSight Network Management Platform.

## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network Agile Reporter	1	Mandatory for eSight Network Agile Reporter

# eSight Network SLA Manager

## Product Overview

Currently, most IP networks use coarse-grained bandwidth management polices and do not have quality monitoring or guarantee mechanisms. Therefore, IP networks provide only connectivity and cannot ensure good user experience. Users often experience service quality issues such as video pixelation, fuzzy voice, slow network access, and slow response of cloud desktop. However, the networks and network administrators are unaware of these issues because there is no system to monitor service quality on the entire network. Administrators try to locate network problems only after receiving complaints from users. However, it often takes a long time to locate and solve a problem due to lack of real-time monitoring mechanisms and effective problem location methods. This problem location process is inefficient and severely affects user experience.

Huawei eSight Network SLA Manager implements visible monitoring on network quality by combining the following methods: simulation flow-based and real service flow-based network quality detection.

Huawei eSight Network SLA Manager monitors network quality using simulation flows by integrating with the devices' NQA function to diagnose and measure link performance between network devices 24 hours a day and displays QoS statistics. Administrators can set the QoS threshold, and eSight Network notifies administrators remotely when QoS reaches the threshold. Administrators can use the quick diagnosis function to monitor link performance in real time and diagnose faults, which improves management efficiency.

Huawei eSight Network SLA Manager implements network quality detection based on iPCA, which is the industry's first multiple-input-multiple-output quality measurement technology and solves the N2 connection problem in traditional point-to-point quality measurement technologies. iPCA technology uses the enhanced area-based packet conservation mechanism to monitor the quality on a connectionless network and also provides accurate fault location capabilities.

## Features

The network quality emulation test helps users discover network quality problems in advance.

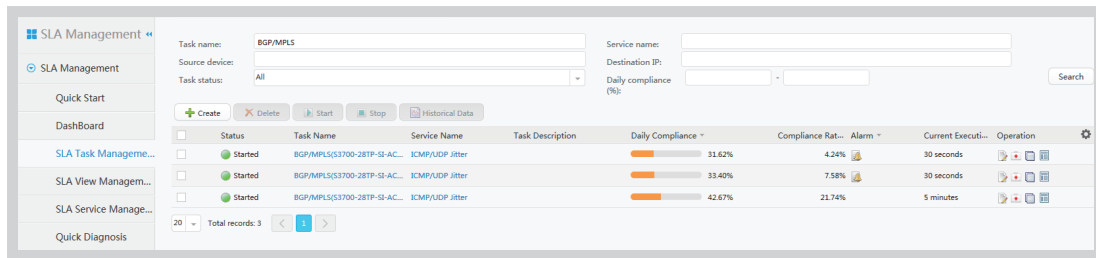
- Service-oriented SLA and easy operation simplify O&M needs. Users can create an SLA service to carry out E2E network QoS monitoring and evaluate network and service QoS based on SLA compliance. eSight Network has more than 20 SLA service configuration items for video, audio, and network applications, allowing customers to define SLA services to meet their unique requirements.

The screenshot displays the 'SLA Management' interface. At the top, there are search filters for 'Service name', 'Type', 'Status', and 'Rating'. Below the filters is a table listing various predefined SLA services. Each row includes a checkbox, the service name, a brief description, the rating (e.g., 4-star, 5-star), the compliance threshold (e.g., 80), the type (Predefined), the status (Unused), and an operation icon.

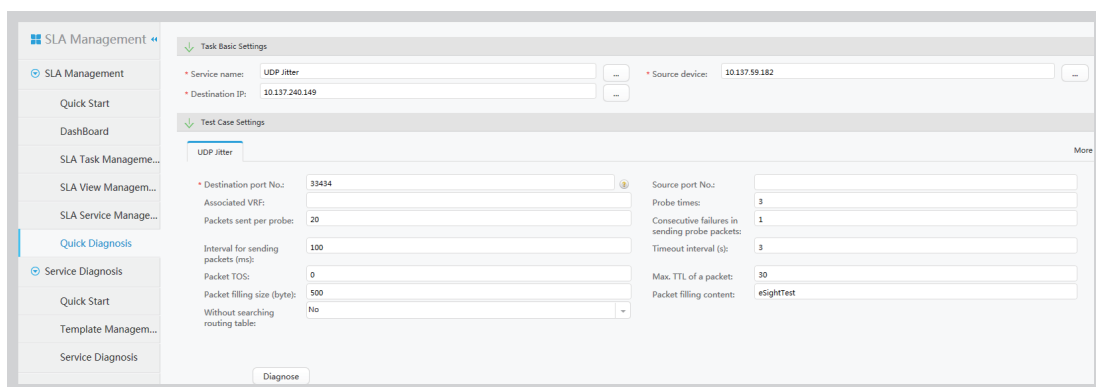
Service Name	Description	Rating	Compliance Thres...	Type	Status	Operation
<input type="checkbox"/> Signaling	Session layer protocol in a network, used to establish sessions before communication...	4-star	80	Predefined	Unused	
<input type="checkbox"/> High quality voice service	VoIP service. Example: voice service using IP phones	5-star	80	Predefined	Unused	
<input type="checkbox"/> Common voice service	VoIP service. Example: voice service using desktop eSpace	4-star	80	Predefined	Unused	
<input type="checkbox"/> Key data service	This service type is the most essential data service in a corporate information system...	4-star	80	Predefined	Unused	
<input type="checkbox"/> Real-time application	Some data applications have especially high demands for delay and jitter, and have L...	5-star	80	Predefined	Unused	
<input type="checkbox"/> Network management	Simple Network Management Protocol (SNMP), used for the communication between...	4-star	80	Predefined	Unused	
<input type="checkbox"/> High quality video service	High-quality and high-interaction real-time video service that has high demands for...	5-star	80	Predefined	Unused	
<input type="checkbox"/> Common video service	Video service that has normal video quality requirements. Example: IPTV or desktop v...	4-star	80	Predefined	Unused	
<input type="checkbox"/> Streaming media service	One-way video. Example: video on demand, video surveillance	3-star	80	Predefined	Unused	
<input type="checkbox"/> Web page browsing	This service type has low demands for delay, jitter, and packet loss rate. Example: ent...	3-star	80	Predefined	Unused	
<input type="checkbox"/> File transfer	This service type has high demands for bandwidth but low demands for delay, jitter...	3-star	80	Predefined	Unused	
<input type="checkbox"/> Common data service	This service type has high demands for bandwidth, but has low demands for delay. E...	3-star	80	Predefined	Unused	
<input type="checkbox"/> ICMP Echo	Tests the connectivity and packet transmission time between sources and destination...	4-star	80	Predefined	Unused	
<input type="checkbox"/> ICMP Jitter	Tests network transmission quality, including the packet loss, delay, and jitter.	4-star	80	Predefined	Unused	
<input type="checkbox"/> UDP Echo	Tests the response speed for UDP to connect to specified ports and tests the UDP pa...	4-star	80	Predefined	Unused	
<input type="checkbox"/> UDP Jitter	Tests the UDP packet transmission between sources and destinations, including infor...	4-star	80	Predefined	Unused	
<input type="checkbox"/> TCP Connect	Tests the TCP connection setup time between sources and destinations.	4-star	80	Predefined	Unused	
<input type="checkbox"/> SNMP	Tests the statistical information about communication between hosts and SNMP Age...	4-star	80	Predefined	Unused	
<input type="checkbox"/> DNS	Tests the resolution speed from specified DNS names to IP addresses.	4-star	80	Predefined	Unused	
<input type="checkbox"/> DHCP	Tests the speed for sources to allocate IP addresses.	4-star	80	Predefined	Unused	



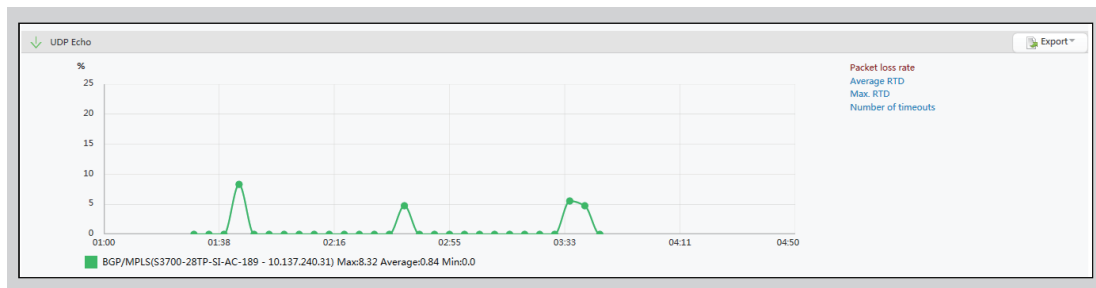
- eSight Network SLA Manager displays network QoS statistics and generates alarms in advance to ensure user experience. After a user creates an SLA task, it will be executed periodically. QoS statistics are displayed based on daily compliance. When QoS meets the threshold conditions, eSight Network notifies administrators remotely, enabling administrators to diagnose faults in advance to ensure user experience.



- eSight Network SLA Manager provides a quick diagnosis function to narrow the fault scope and shorten fault diagnosis time. The quick diagnosis function helps users locate faults by link segments, narrowing the fault scope.



- Visible historical network data provides a basis for network optimization. In actual applications, QoS values indicate services of different priorities. Different services on a same link can be compared, and the result shows whether QoS on a network has taken effect and provides a basis for QoS policy adjustment.



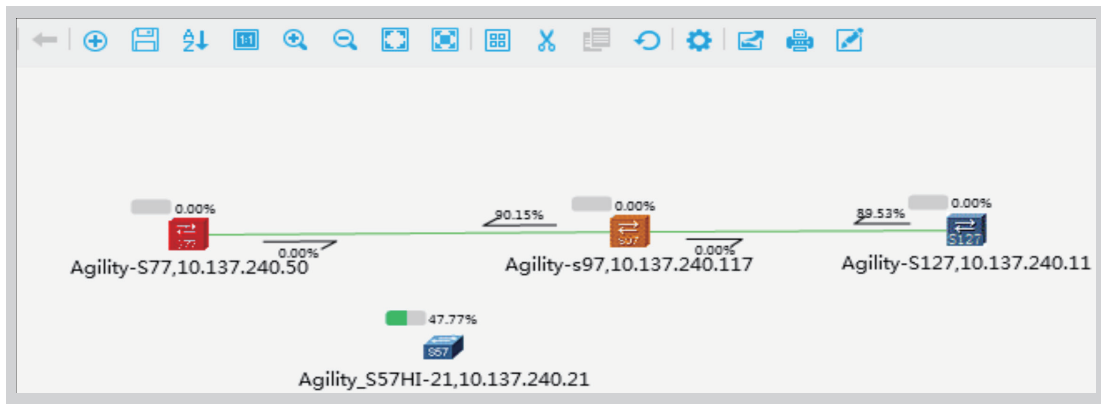
eSight Network SLA Manager provides real-time QoS monitoring, multi-dimensional data analysis, and graphical data display.

eSight Network uses the unified dashboard panel to vividly display QoS information, simplifying network management. The dashboard displays and manages various QoS information in a centralized manner to administrators, informing them of bandwidth usage and network exception information in real time. The QoS information includes top bandwidth usage, top discarding rate, top Peak Information Rate (PIR), and top matching rate.

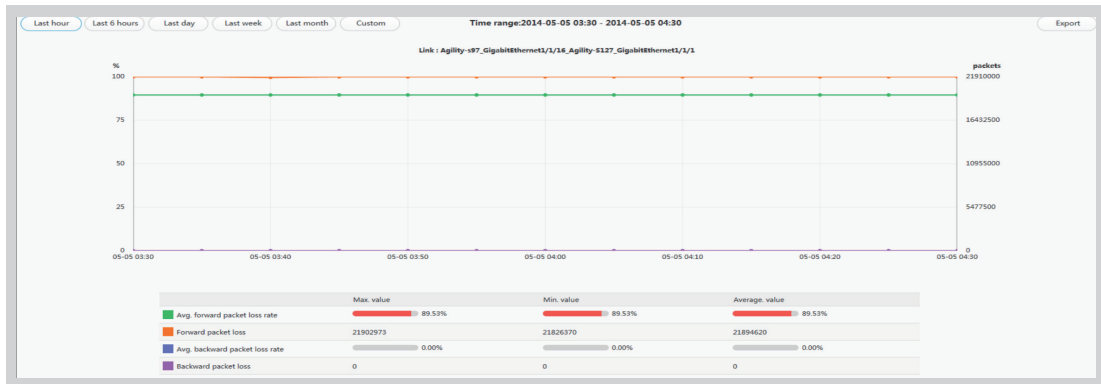
eSight Network supports network quality detection based on real service flows.

- Device- or link-level measurement**

After iPCA is enabled for agile devices and links in batches, quality status of devices and links is clearly displayed in the topology. When the device or link quality threshold is exceeded, an alarm is generated and reported to the administrator in a timely manner.

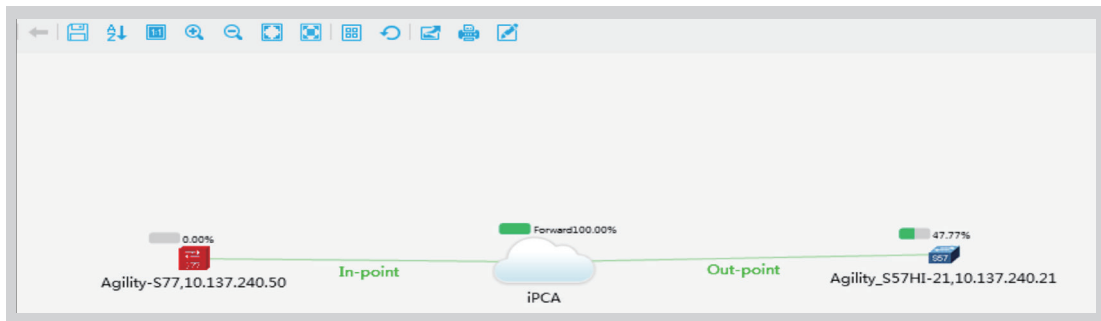


Users can further view real-time data on devices and links as well as packet loss in a port queue or on a port with the specified MAC address.

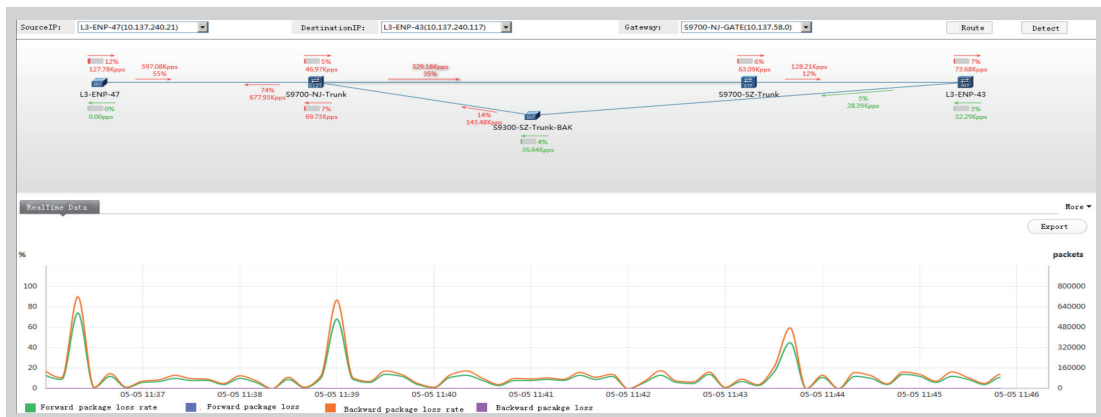


• Network-level measurement

Network-level measurement targets an area to implement visible monitoring on the area network quality.



Path hop-by-hop detection can locate the node or link where packets are lost in an area.



## Operating Environment

eSight Network SLA Manager is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.

## Deployment Scenarios

Deployment scenarios for eSight Network SLA Manager are the same as those for eSight Network Management Platform. Source devices must be added to eSight Network, and the IP addresses of the source and destination devices can be pinged.

## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network SLA Manager	1	Mandatory for eSight Network SLA Manager



# eSight Network Traffic Analyzer

## Product Overview

Fast and stable access speeds improve office work efficiency, while low access speeds can negatively affect productivity. Administrators must determine which applications consume the most bandwidth and generate heavy traffic, and which employees use these applications, and then change the network QoS policy and expand the network when necessary.

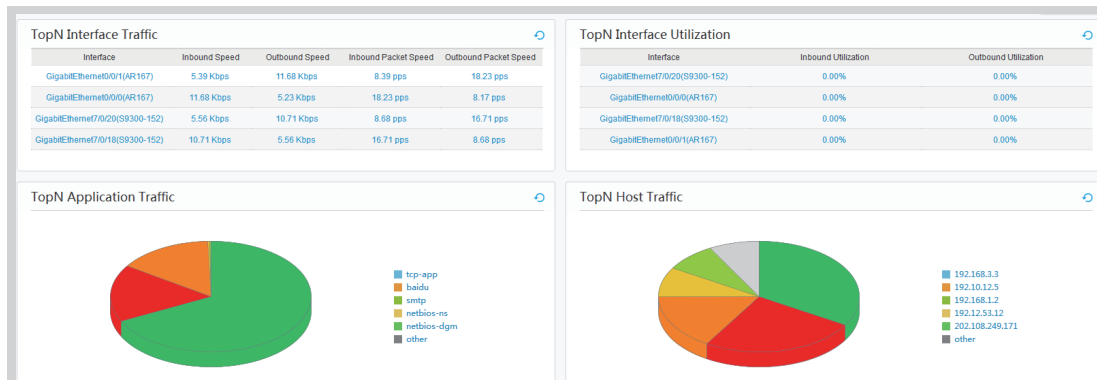
eSight Network Traffic Analyzer (NTA) analyzes network traffic based on NetFlow, NetStream, and sFlow protocols. This helps network administrators monitor traffic and bandwidth usage on enterprise campus egress and wireless campus networks, generate traffic analysis reports, and detect network bottlenecks in a timely manner, providing evidence for network planning and fault diagnosis.

## Features

eSight Network Traffic Analyzer supports mainstream network traffic protocols, including NetStream, NetFlow, and sFlow.

Figure 10-1 shows the customized dashboard that displays network status.

Customized dashboard



- Multiple dimensions: eSight Network Traffic Analyzer ranks the traffic on devices and interfaces, including interface usage, application, host, session, and Differentiated Services Code Point (DSCP) traffic.
- Customization: eSight Network Traffic Analyzer allows users to customize the presented content, format, and formatting style and supports partial traffic updates without changing the Graphical User Interface (GUI).
- The interface traffic and usage rankings display interface traffic statistics, including the incoming and outgoing rate and incoming and outgoing data packets. Clicking an interface will reveal information about the traffic composition at different times, in multiple dimensions, including the application, host, session, and DSCP.

### Customized Traffic Applications and Group Network Traffic

Customization options for traffic applications and group network traffic, as follows:

- Customized applications
- Customized DSCP group
- Customized application group
- Customized IP address group or interface group

### Customized Applications

eSight Network Traffic Analyzer components are recognized based on the protocol and port number, and hundreds of standard applications and common Layer 4 applications are preset. Protocols and port numbers can also be added for unknown applications, and network administrators can add applications as required. Users can customize applications based on the specified protocol, port number, and IP address ranges.

### Customized DSCP Group

DSCP group is a logical group, and users can create a group to differentiate DSCP composition. For example, in WAN QoS monitoring, users can create a voice group (EF), a video group (AF31), and a group for the other DSCP; therefore, eSight Network Traffic Analyzer can provide a reference for proper enterprise QoS bandwidth and key service bandwidth planning.

### Customized Application Group

Create application groups as required to obtain comprehensive information about specific applications. For example, create an application group named Mail Service, and combine Lotus Notes, pop3, and SMTP applications into the group to learn mail application traffic.

### Customized IP Address Group or Interface Group

Users can consider the IP addresses or interfaces in a certain range as a whole to calculate traffic statistics. For example, assume that an enterprise has two floors and the total enterprise traffic must be calculated. Simply combine all switch interfaces on the two floors into an interface group and analyze the total traffic.

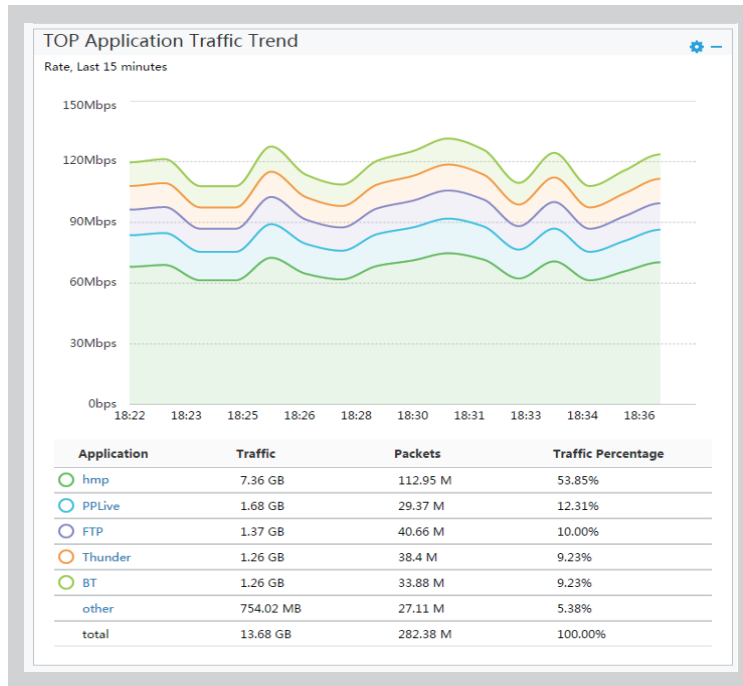
### Monitoring Multi-dimensional Traffic with Simple Configuration

- Overall network traffic analysis depends on high performance traffic analysis. Network administrators need only add a monitoring interface and configure the traffic sampling ratio before monitoring and analyzing interface traffic from multiple dimensions, including the following:
  - \* Interface traffic analysis
  - \* Application traffic analysis
  - \* Source/Destination host traffic analysis
  - \* DSCP traffic analysis
  - \* Session traffic analysis

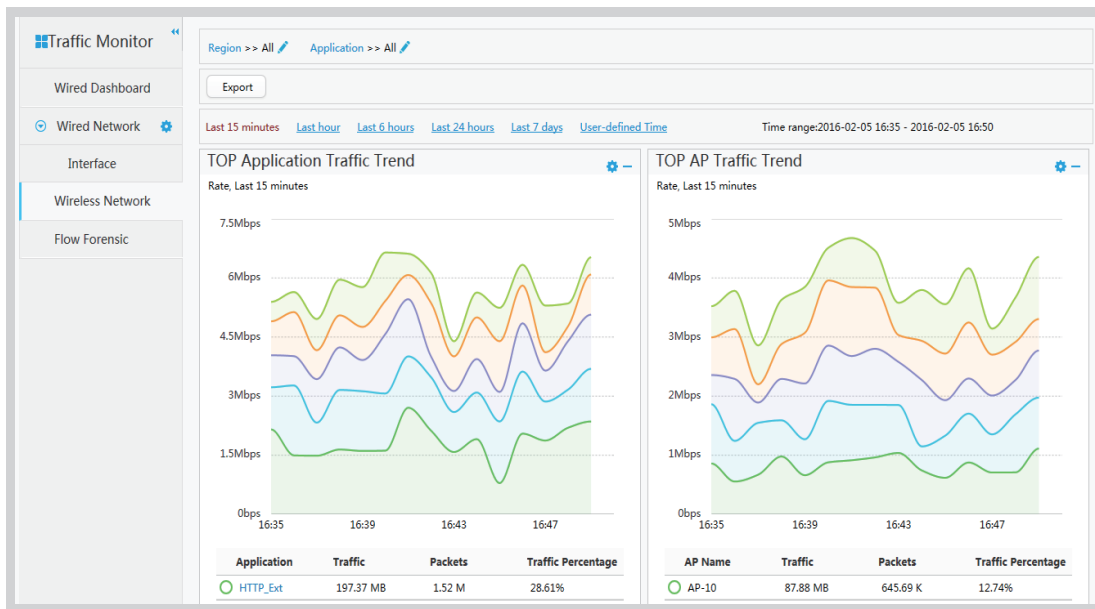
### NOTE

Users can analyze traffic on the traffic trend diagram, which displays traffic and packets, respectively, on two coordinates.

- eSight Network can work with Huawei devices to intelligently analyze bandwidth distribution of dynamic port applications, such as common P2P applications BT and eMule, and other websites.



- eSight Network can work with Huawei WLAN devices AC6005, AC6605 and ACU2 to display application traffic distribution of enterprise wireless campus networks and allow users to obtain the application development status in different regions.



- Device traffic analysis allows users to view the traffic trend and distribution of a single device. eSight Network can identify applications transmitted by the device, source and destination hosts, DSCP traffic distribution, and NetStream-enabled interface traffic on the device.

# Interface Traffic Analysis

[All interfaces] >> Interface GigabitEthernet7/0/20(59300-152)
[Traffic Forensic]

Last 15 minutes   Last hour   Last 6 hours   Last 24 hours   Last 7 days   User-defined Time
Time range: 2014-05-05 03:10 - 2014-05-05 04:10

Overview

### Interface Traffic Trend

Rate, Last 1 hour

Traffic Direction	Maximize	Minimize	Average
Inbound	16.40 Kbps	0 bps	5.29 Kbps
Outbound	24.60 Kbps	0 bps	10.17 Kbps

### TOP N Host - From

Rate, Last 1 hour

Source Host	Traffic	Packets	Traffic Percentage
192.10.12.5	3.42 MB	43.78 K	50.15%
192.12.53.12	1.24 MB	15.87 K	18.18%
10.192.53.1	1.10 MB	14.08 K	16.13%
202.108.249.171	1.06 MB	13.57 K	15.54%
other	0 B	0	0.00%
<b>total</b>	<b>6.83 MB</b>	<b>87.3 K</b>	

### TOP N Host - To

Rate, Last 1 hour

Destination Host	Traffic	Packets	Traffic Percentage
192.168.3.3	4.58 MB	58.62 K	67.16%
192.168.1.2	2.24 MB	28.67 K	32.84%
other	0 B	0	0.00%
<b>total</b>	<b>6.83 MB</b>	<b>87.3 K</b>	

### TOP N Application - In

Rate, Last 1 hour

Application	Traffic	Packets	Traffic Percentage
tcp-app	2.26 MB	28.93 K	100.00%
other	0 B	0	0.00%
<b>total</b>	<b>2.26 MB</b>	<b>28.93 K</b>	

### TOP N Application - Out

Rate, Last 1 hour

Application	Traffic	Packets	Traffic Percentage
tcp-app	2.42 MB	30.98 K	52.84%
smtp	1.10 MB	14.08 K	24.02%
baidu	1.06 MB	13.57 K	23.14%
other	0 B	0	0.00%
<b>total</b>	<b>4.58 MB</b>	<b>58.62 K</b>	

### TOP N Conversation - Total

Rate, Last 1 hour

Conversation	Traffic	Packets	Traffic Percentage
192.10.12.5 to 192.168.1.2	2.26 MB	28.93 K	33.14%
192.10.12.5 to 192.168.3.3	1.20 MB	15.36 K	17.60%
192.12.53.12 to 192.168.3.3	1.16 MB	14.85 K	17.01%
10.192.53.1 to 192.168.3.3	1.16 MB	14.85 K	17.01%
202.108.249.171 to 192.168...	1.04 MB	13.31 K	15.25%
other	0 B	0	0.00%
<b>total</b>	<b>6.83 MB</b>	<b>87.3 K</b>	



Interface traffic analysis checks the traffic trend for a specified interface, time range, and incoming and outgoing traffic. Based on interface traffic analysis, network administrators can identify the interfaces that are used most frequently on the network to gain a comprehensive understanding of the entire network status. Administrators can detect interfaces with abnormal traffic and locate faults before network performance is affected.

#### **Application Traffic Analysis**

Application traffic analysis checks the trend in application changes for a specified interface, time range, and incoming and outgoing traffic. Administrators can locate the host that causes performance problems based on the source ranking and destination hosts using a specific application.

#### **Source/Destination Host Traffic Analysis**

Source/destination host traffic analysis checks the trend in source/destination host bandwidth usage changes for a specified interface, time range, and incoming and outgoing traffic. Based on source/destination host analysis, network administrators can identify the host that consumes high bandwidth and solve any bandwidth problems in a timely manner to ensure bandwidth usage efficiency.

#### **Session Traffic Analysis**

Session traffic analysis checks the trend of session traffic for a specified interface and time range. Session traffic analysis provides detailed session information the network administrator can use for further fault location.

#### **DSCP Traffic Analysis**

DSCP traffic analysis checks the DSCP traffic trend for a specified interface and time range, ensuring proper QoS bandwidth planning and the quality of key services.

#### **Group Traffic Analysis**

Group traffic analysis displays the DSCP group, interface group, application group, and IP group traffic statistics on specified interfaces within a specific time range. Network administrators can conveniently analyze specific traffic as required to satisfy special maintenance requirements.

#### **Threshold Value Alarm**

eSight Network allows administrators to set traffic threshold values for applications and hosts. When the number of times that the monitored value exceeds the threshold values within a specified time reaches the preset value, eSight Network sends alarm notifications through email.

#### **Customized Traffic Report**

eSight Network Traffic Analyzer can customize reports by specifying filtering rules, report type, and report layout configuration. Traffic reports provide references for further network planning.



**Abstract**

Name: core\_nanjing

Report Category: Default

Description: nanjing output core line

Interface: S9300-152 GigabitEthernet7/0/20  
S9300-152 GigabitEthernet7/0/18  
AR167 GigabitEthernet0/0/1

Filter:

Summary Type: Application Summary, Conversation Summary, DSCP Summary, Interface Summary, Host Summary

Layout: Application Summary - Table  
Conversation Summary - Table  
DSCP Summary - Table  
Interface Summary - Table  
Host Summary - Table

Time Range: Last 1 Week(s)

Previous Save Save and Execute Cancel

## Original Data Stream Facilitates Fault Location

NTA can extract an original data stream based on a specified time range and filtering rules for further analysis and fault location. Original traffic information includes the router, source, and destination address, application, source and destination port, protocol, TCP flag, next hop, inbound and outbound interface, and DSCP, traffic, and data packets. Users can create traffic investigation tasks for suspected abnormal traffic on the NTA page to extract original data stream information about the current traffic.

Task Basic Information

Name: GigabitEthernet0/0/1(AR167)\_20140505043038 Time: From 2014-05-05 03:40:00 To 2014-05-05 04:30:00

Description: Inbound or Outbound Interface Equal to GigabitEthernet0/0/1(AR167) Data Save 7

Filter: Inbound or Outbound Interface Equal to GigabitEthernet0/0/1(AR167)

Modify Run

Task Execution Results [Export Data](#)

Time	Router Address	Inbound Inter...	Outbound Int...	Source Address	Source ...	Destination Ad...	Destination...	TCP Flag	Next Hop	Protocol	Application	DSCP	Traffic (bytes)	Data Pack
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	652	10.139.60.189	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.09KB	50
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	668	10.139.60.181	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.14KB	50
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	609	10.139.58.253	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.01KB	34
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	602	10.139.61.175	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	502B	16
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	613	10.139.58.252	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.11KB	27
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	647	10.139.58.170	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	525B	18
2014-05-25 02:38:19	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	657	10.139.61.145	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.17KB	47
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	631	10.139.60.19	33584	-A----	192.168.1.1	tcp	ipp	TCS 8	999B	58
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	693	10.139.60.140	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.46KB	20
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	656	10.139.60.172	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.09KB	31
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	667	10.139.59.58	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	558B	51
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	679	10.139.58.71	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.12KB	59
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	607	10.139.58.4	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.03KB	19
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	676	10.139.58.106	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.23KB	57
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	675	10.139.60.94	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	973B	19
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	675	10.139.58.32	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	802B	50
2014-05-25 02:38:20	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	637	10.139.58.74	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.26KB	17
2014-05-25 02:38:21	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	605	10.139.58.28	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	1.09KB	55
2014-05-25 02:38:21	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	621	10.139.59.75	33584	-A----	192.168.1.1	tcp	tcp-app	TCS 8	966B	47
2014-05-25 02:38:21	10.137.59.46	WAN Minipo...	WAN Minipo...	10.135.20.1	674	10.139.60.108	33584	-A----	192.168.1.1	tcp	ecap	TCS 8	1.27KB	47

## Operating Environment

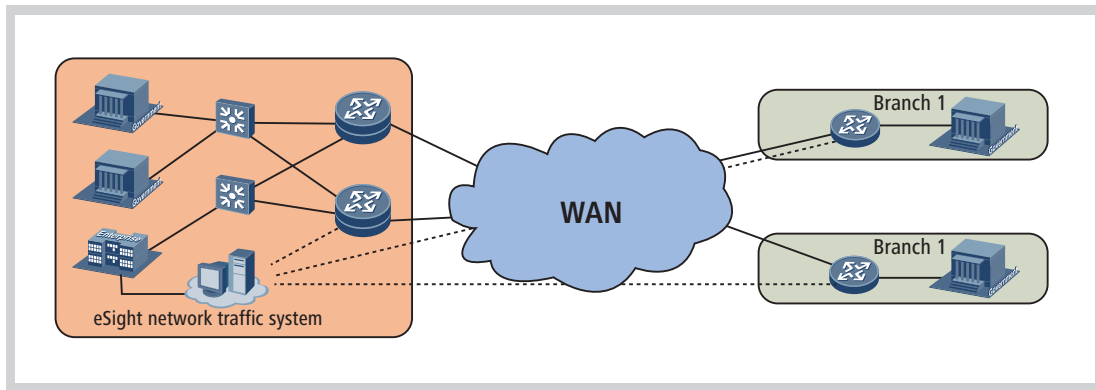
eSight Network Traffic Analyzer can be deployed on the same server as eSight Network Management Platform standard or professional edition, or on a different one. When they are configured on one server, they can manage no more than 10 NEs, and the configuration requirements are the same as those of the platform. When they are configured on different servers, configuration requirements are as follows:

Operating System	Configuration Requirement
Windows Server 2012 R2 standard (64 bits), Novell SUSE Linux Enterprise Server 12.0 SP2	CPU: 2 x hexa-core 2 GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> PC servers are recommended. Determine the hardware specifications based on the network scale.

When eSight Network Traffic Analyzer and eSight Network Management Platform are deployed on different servers, eSight Network Traffic Analyzer can be deployed on a VM when the number of nodes is less than 100. VM resource requirements are as follows:

Operating System	Resources Required by a VM
Windows Server 2012 R2 standard (64 bits), Novell SUSE Linux Enterprise Server 12.0 SP2	VMWare ESXI 5.0/5.5, FusionSphere V1R5, Hyper-V CPU: 16 vCPU 2 GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> PC servers are recommended. Determine the hardware specifications based on the network scale.

## Deployment Scenarios



eSight Network Traffic Analyzer enables NetStream on an enterprise's WAN-link device interfaces to send traffic information to the eSight Network Traffic Analyzer. eSight Network NTA provides the following functions in this scenario:

- Analyzes the current WAN link traffic composition.
- Helps recognize abnormal traffic and junk applications.
- Quickly locates the IP address of the terminal generating abnormal traffic.
- Optimizes link application traffic distribution.
- Improves WAN link usage.
- Recognizes DSCP bandwidth distribution on the enterprise branch egress.
- Adjusts service priority policies.
- Periodically generates a link interface traffic report.
- Detects network application traffic increase.
- Facilitates advance network planning and expansion.



## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network Traffic Analyzer	1	Mandatory for eSight Network Traffic Analyzer
eSight Network NTA License-Incremental 1 Device License	Optional	One license manages one incremental device.
eSight Network NTA License-Incremental 2 Devices license	Optional	One license manages two incremental devices.
eSight Network NTA License-Incremental 5 Devices license	Optional	One license manages five incremental devices.





# eSight Network WLAN Manager

## Product Overview

With network development, Wireless Fidelity (Wi-Fi), a low-cost and highly efficient network deployment and maintenance mode, has been widely recognized by customers. However, Wi-Fi's high requirements on the environment and distributed deployment of a large number of ACs and APs on WLAN networks make maintenance costly and difficult; therefore, an easy-to-use and efficient WLAN management system is the key to ensure enterprise E2E operations.

Huawei eSight Network WLAN Manager integrates the management of wired and wireless networks, supporting full lifecycle WLAN management, including visible planning (highly-efficient WLAN planning with professional tools), fast service provisioning in three steps, active O&M, all-round quality awareness regionally or globally. It provides search-centric E2E one-click fault diagnosis, interference source locating, and spectrum analysis to implement highly efficient troubleshooting. It also provides position-based terminal location, behavior analysis, and northbound interfaces to achieve mutual benefits from the wireless network.

## Features

### Unified Wired and Wireless Management

In eSight Network physical topology, users can monitor switches, routers, and security, IT, H3C, Aruba, and Cisco devices in a unified manner. Through centralized management of wired and wireless devices, such as ACs, Power over Ethernet (PoE) switches, and Fat APs, users can directly view device connections, status, and alarms on the entire network.

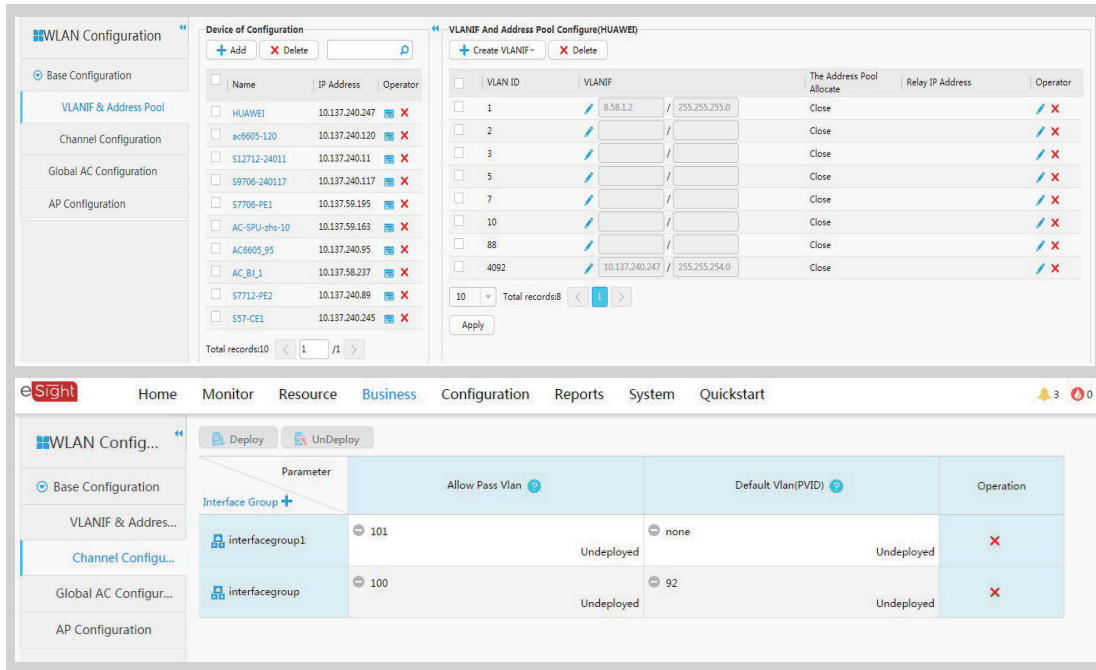
### Visible Network Planning, File Generating Through the WLAN Planner

Provides the network planning tool to import location pictures including the regional background pictures, scale, obstacles, Bluetooth Beacon, and pre-deployed APs to the WLAN topology.

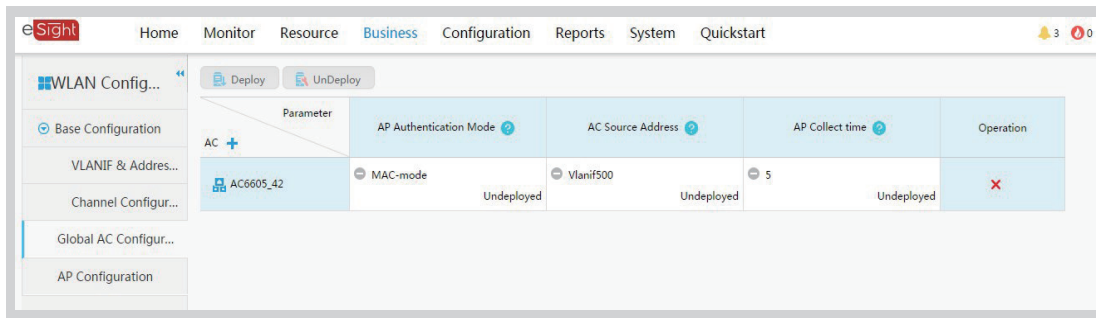
### Deploying Services on Wireless Devices in Batches, Improving Management Efficiency

Quickly provisions services in three steps using AP group-based matrix. This function provides profile-based configuration for WLAN devices of V2R6 and later versions.

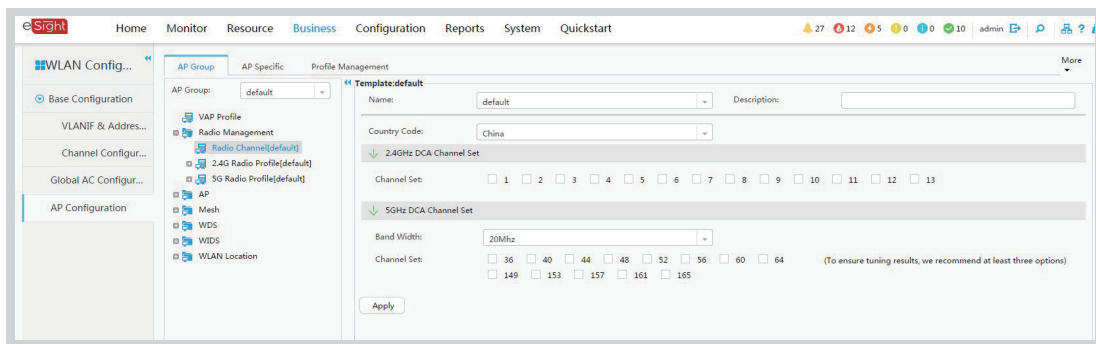
- After ACs and X7 series switches are automatically discovered and added to eSight Network, users can use configuration profiles to complete basic configurations for the ACs and X7 series switches. The configurations include VLANIF interfaces, address pools for establishment of service channels and management channels, and channel configuration for interface groups.



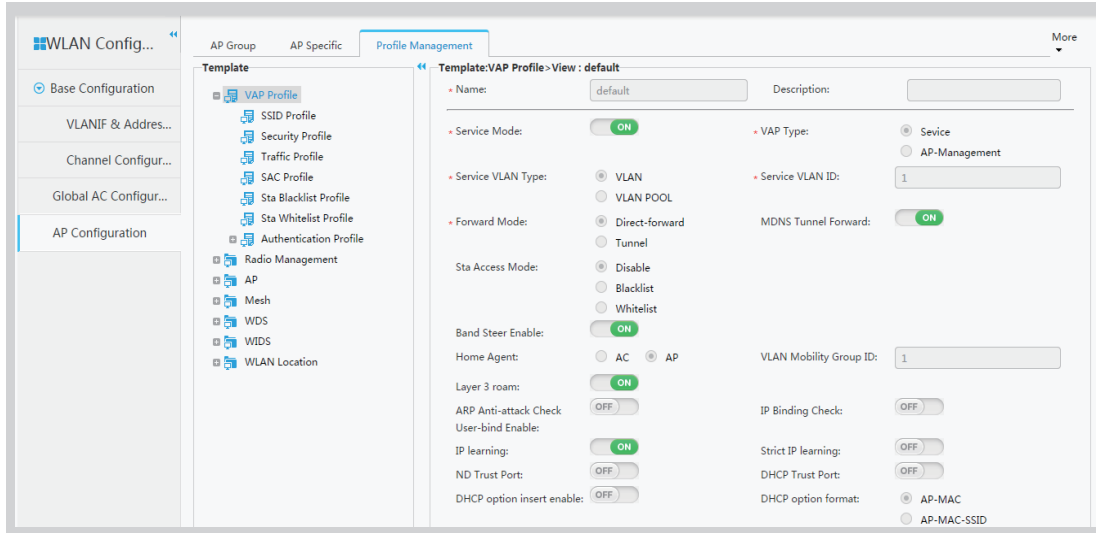
- Global AC configuration: Users can set global parameters for the ACs.



- Service configuration: eSight Network provides pre-defined profiles based on the AP group to quickly provision WLAN services, improving configuration efficiency. eSight Network displays the relationships between AP groups and profiles in the matrix. AP group profiles apply to multiple ACs.

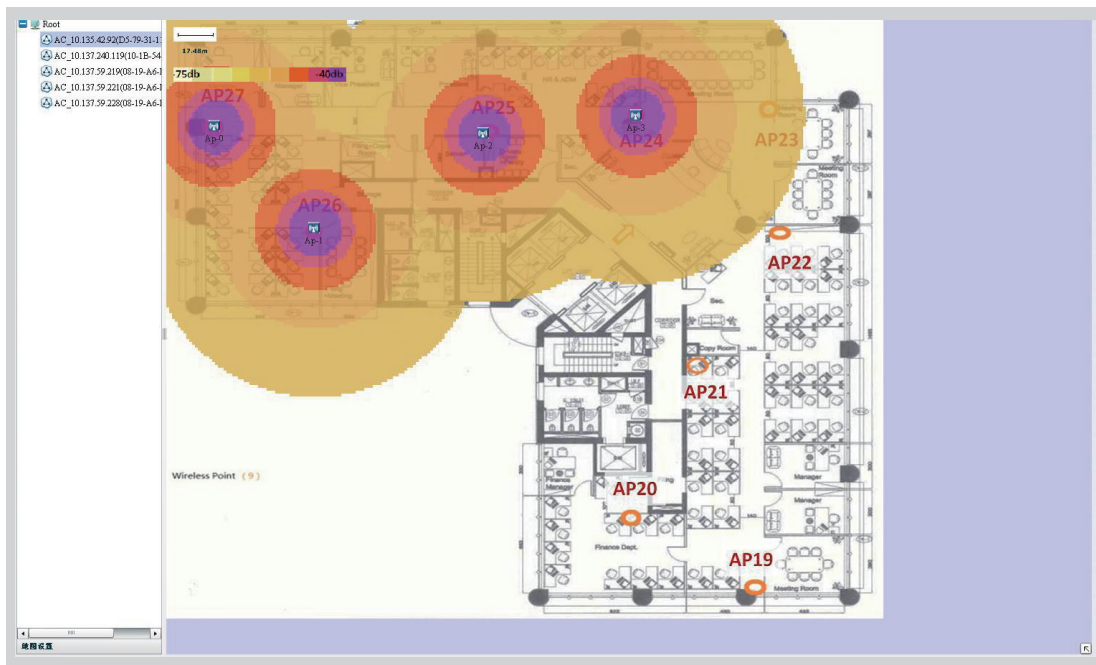


- Various VAP and radio profiles are preset and can be used repeatedly to improve the configuration efficiency. Parameters in the profiles are set based on administrators' experience, facilitating similar configurations by other administrators.

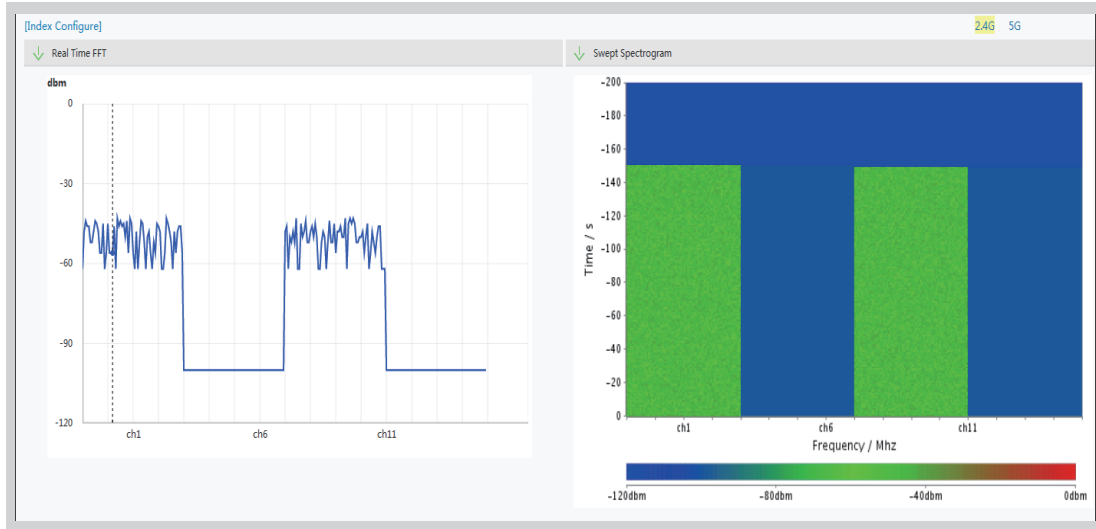


### Various Topology Views Show Wireless Network Status in Different Dimensions

Location topology: WLAN Manager can deploy APs and Beacon to different areas in the physical topology and display hotspots to help maintenance personnel discover radio signal coverage holes and channel collision areas. It supports locating users, unauthorized devices, and interference sources, and displays historical track and Beacon information. Administrators can determine whether to display or hide users of a specified area, rogue APs, unauthorized users, and interference sources.

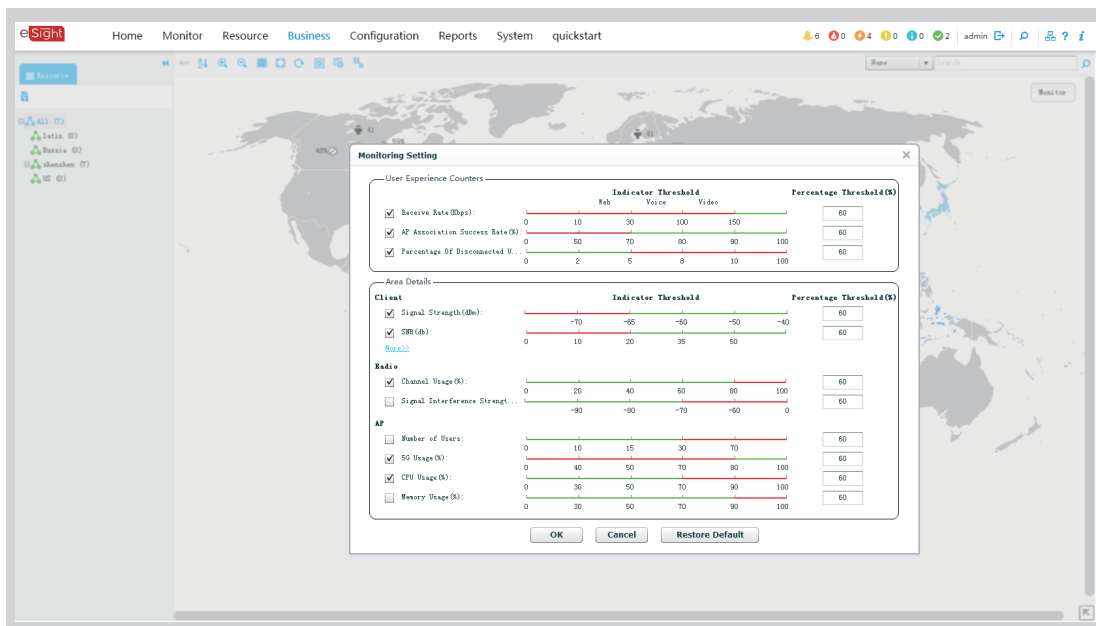


- Frequency spectrum analysis: Users can obtain the channel quality and interference source information from spectrograms, which contain real-time, in-depth, channel quality, and channel quality trend grams, and device duty cycle.



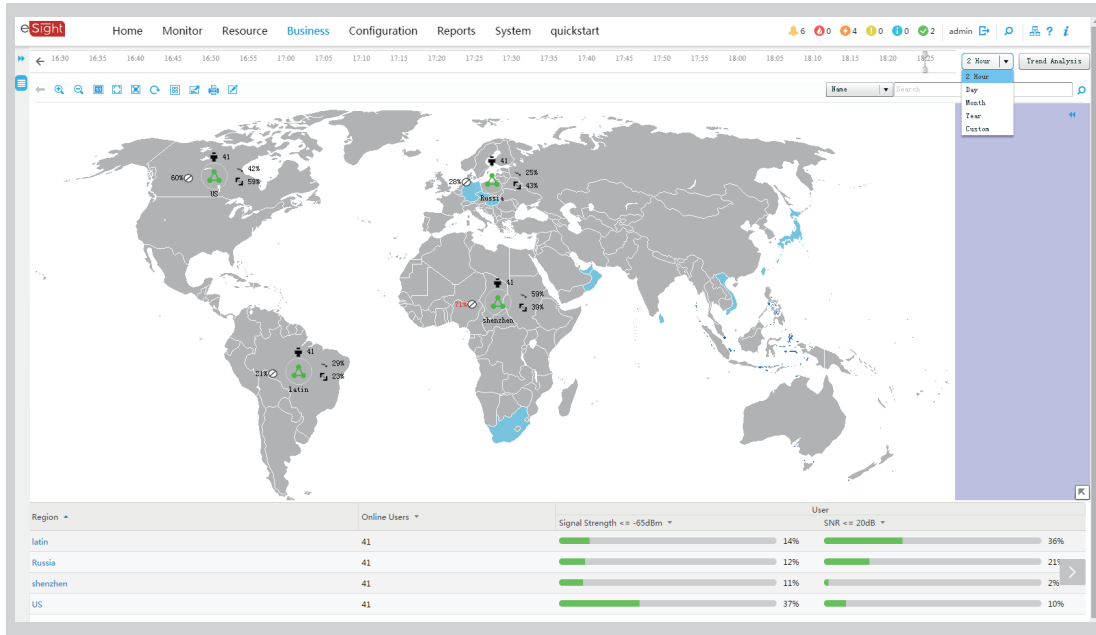
**Comprehensive monitoring: all-round quality awareness regionally or globally**

Region monitor makes user experience visible. eSight Network cleans original performance data by region, and dynamically cleans data by the levels of monitored indicators to generate proportion tables.

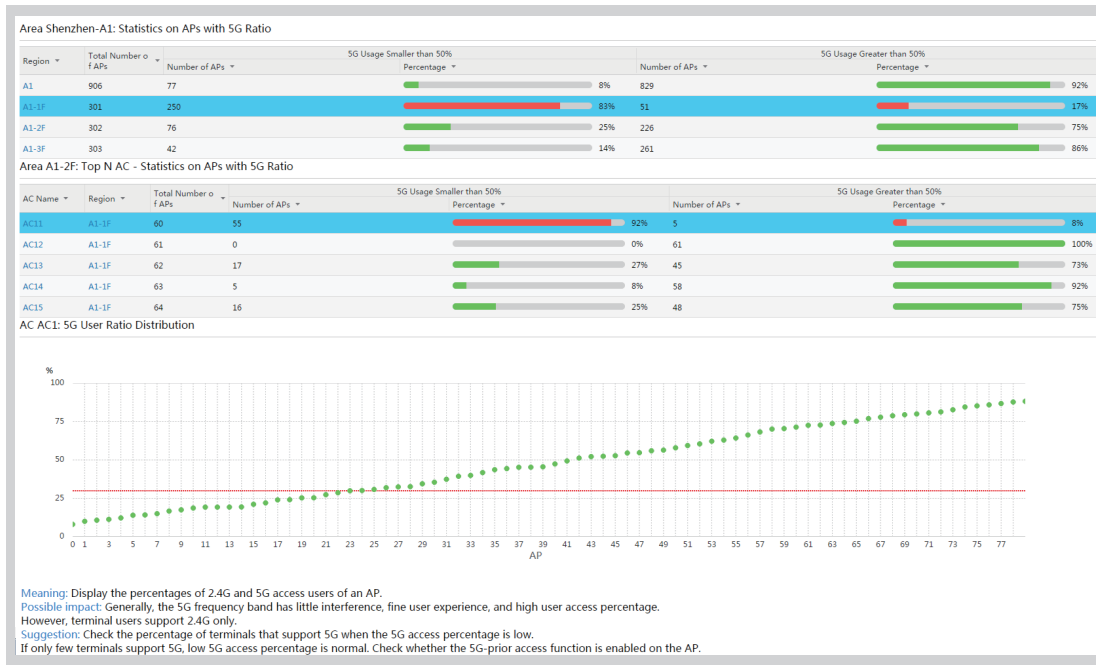




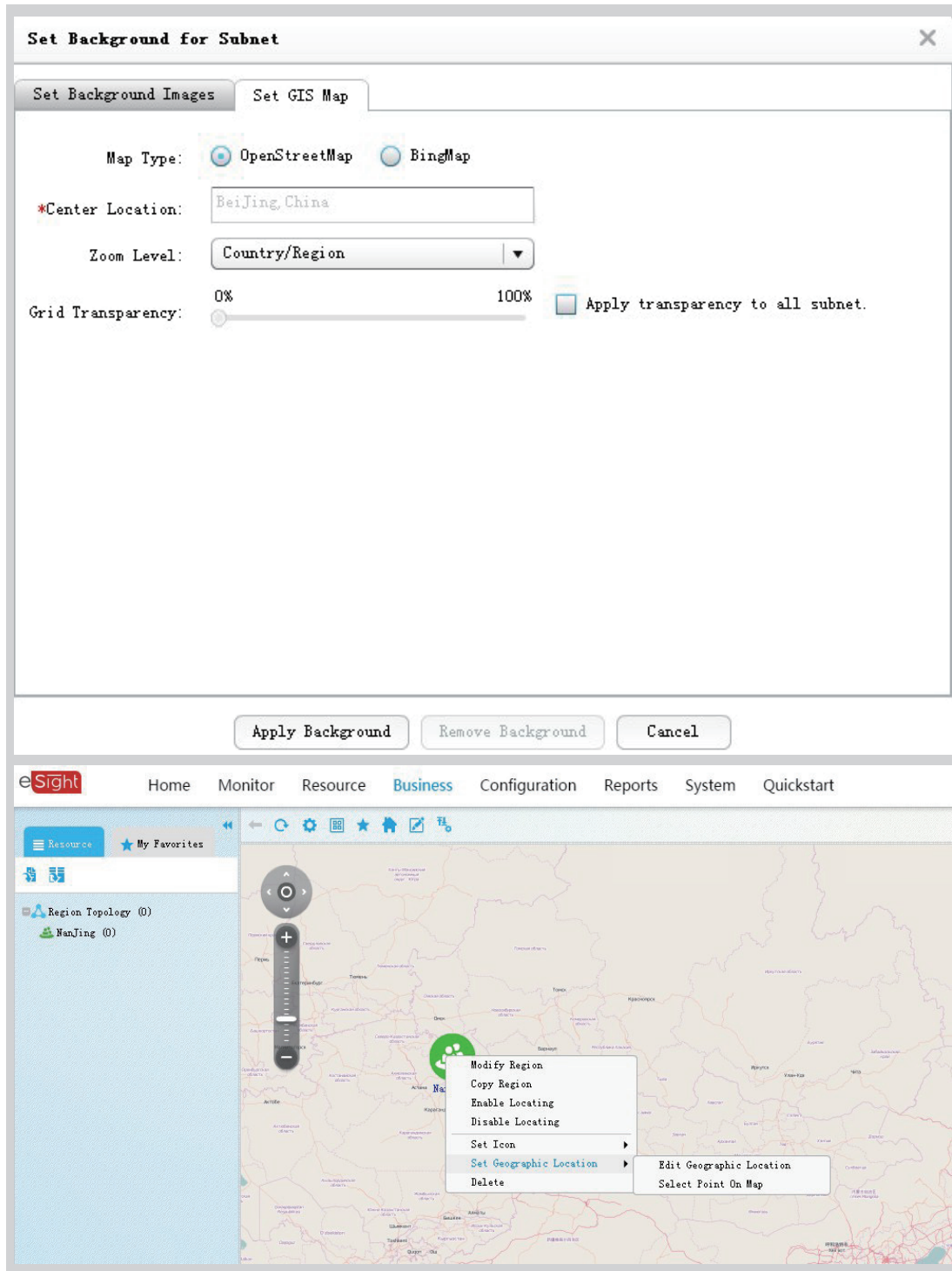
eSight Network integrates region-based user experience data to provide wireless signal coverage and interference distribution information by floor, helping IT personnel identify coverage holes and obtain interference information. In this way, Top 3% to Top 22% of WLAN problems can be quickly solved.



The region monitor function provides a list of abnormal indicators to display abnormal indicators from various dimensions and provide troubleshooting suggestions, allowing users to view the trend of abnormal indicators.



For a non-bottom-layer region, you can set a GIS map as the subnet background. In addition, you can zoom in or out the map, move the map, and set locations on the map.



## Wireless Network Security Detection

The Wireless Intrusion Detection System (WIDS) monitors intrusion devices and non-Wi-Fi interferences and provides frequency spectrum analysis features.

- WIDS management: The WIDS manages wireless network interferences in different categories. Interferences are classified based on user customized rules. Upon detecting an interference, the WIDS chooses whether to generate an alarm based on user alarm configurations. The WIDS can also take countermeasures for unauthorized devices.

MAC	Device Type	SSID	Channel	Attack	Last Detect Time	Time Duration	Operation
87-01-15-08-01-42	Rogue bridge	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-44	Rogue AP	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-45	Rogue adHoc	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-46	Rogue bridge	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-48	Rogue AP	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-49	Rogue adHoc	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-4A	Rogue bridge	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-4C	Rogue AP	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-4D	Rogue adHoc	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-52	Rogue bridge	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-54	Rogue AP	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-55	Rogue adHoc	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-56	Rogue bridge	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-58	Rogue AP	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	
87-01-15-08-01-59	Rogue adHoc	wlanaccess100.0		1 No	2012-06-27 03:47:07	0days2hours46minutes40seconds	

## Search-based One-Click Fault Diagnosis, Quickly Locating Faults

- Quick network fault locating: Diagnose network quality from four aspects, including user, SSID, AP, and AC. List possible problems and give corresponding solutions to help troubleshooting. (Note: This function applies to WLAN V2R6 and earlier versions only.)
- After a user reports a fault, eSight Network quickly locates the user from a large number of users to start E2E one-click fault diagnosis.

WLAN Fault Diagnose [ bc448632a5c0 ]

Connect Info

Client: bc448632a5c0 | SSID: ac32 | AP: rpp-qp1 | AC: AC6605-92

Please click the client or ap or ac settings put corresponding information to fault diagnose.

Diagnose Result

Input user information

The device whose version is WLAN V200R006C00 or above can be selected.

bc  
bc -- bc448632a5c0 BC-44-86-32-A5-C0 ac32 Nanjing>N4>N4-4F

Diagnose

AAA Test | AC Ping | Trace | Log

KPI

RSST

dBm

Send and Receive Rate

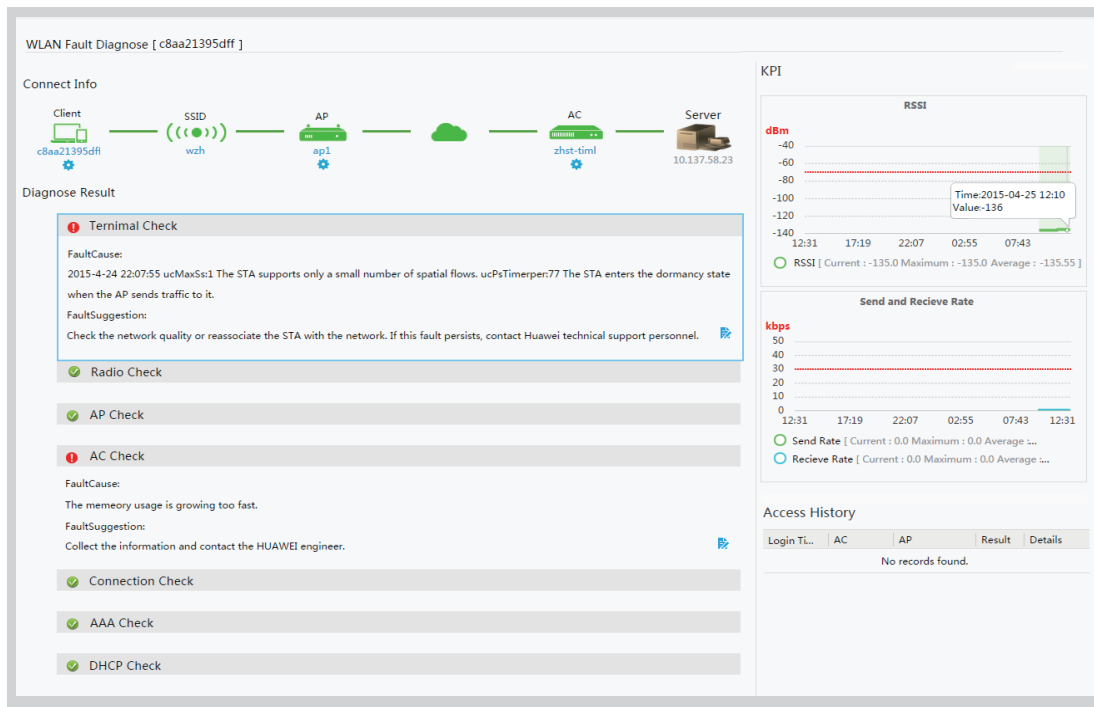
kbps

Access History

Log in TL... AC AP Result Details

No records found.

In addition to fault diagnosis functions as well as Syslogs and performance data, eSight Network provides diagnosis tools to help network administrators troubleshoot wireless network O&M problems, such as end user login failures, frequent logout, and poor signal. (This function applies to WLAN devices running V200R006 and later versions.)



## WLAN Location

### • User Location with High Precision and Low Delay

Based on the three-point location and fingerprint location algorithms which are widely used in the industry, eSight Network innovatively offers the patented PAIRS location algorithm which greatly reduces the impact of the transmit power difference on the location precision. eSight Network also provides the fingerprint collection tool to import signal strength eigenvalues measured at fingerprint points to eSight Network, so that more precise location results can be obtained. Additionally, the location update interval can be customized based on requirements in different scenarios. A large number of tests verify that the terminal location precision can reach 3 to 5 meters and the location delay can reach 3 seconds in an ideal situation.

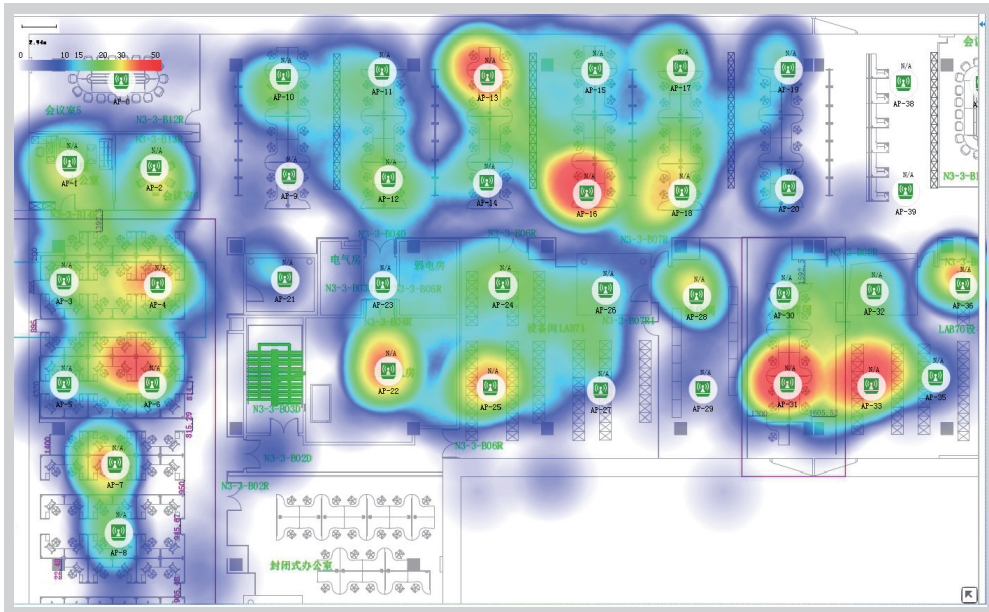
The Bluetooth location SDK provides the high-precision location terminal location solution, allowing third parties to carry out secondary development and implement applications of high-precision location, such as indoor navigation and car navigation. eSight Network can monitor the Beacon status on the entire network through interconnection with the AP with built-in Bluetooth module. It is verified that Bluetooth supports 1 m high-precision location and the delay is within 1s.

In addition, eSight Network supports Bluetooth tag-based location with the accuracy of 3 m to 5 m. eSight can play historical tracks of Bluetooth tags with a preset or user-defined time range.

### • Real-time Customer Distribution

WLAN location can be used to obtain location information about all users in a Wi-Fi coverage area. Based on the location information, eSight Network can intuitively present the distribution of people, that is, the heat map.



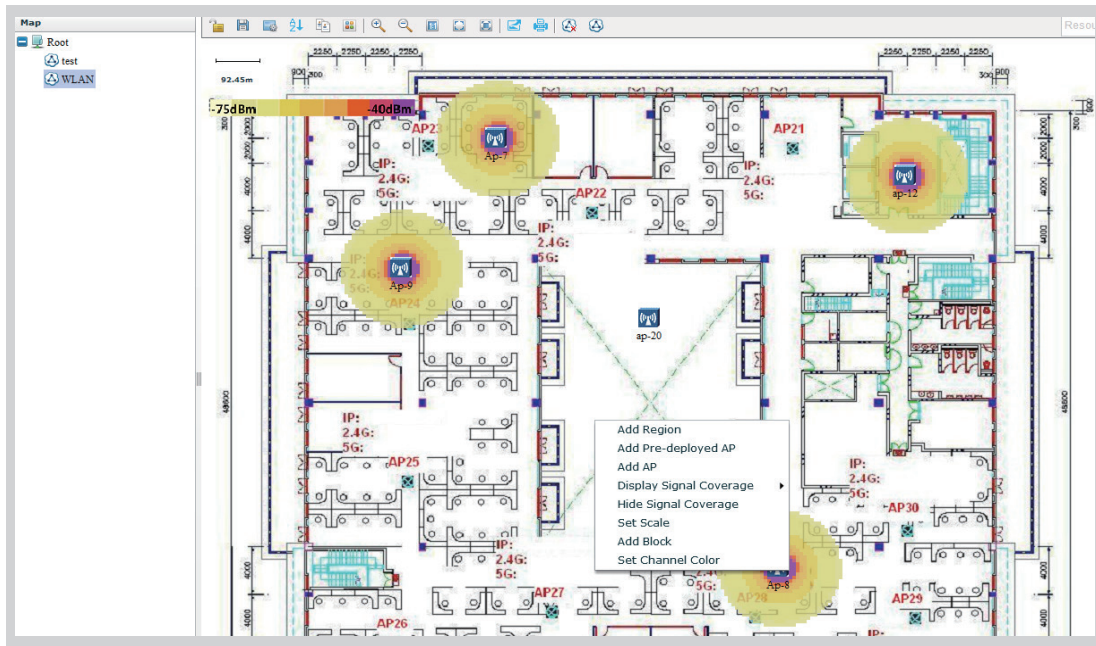


• Open Interfaces Provided to Construct a Win-Win Ecosystem with Third Parties

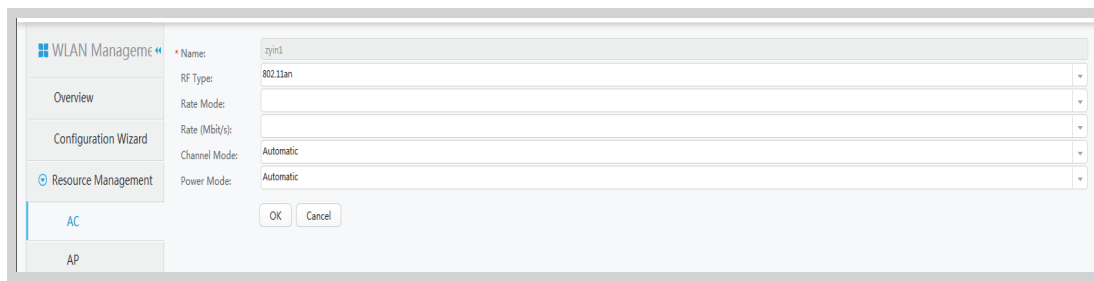
Huawei sticks to the integration strategy and provides open interfaces for integration. eSight Network can send user location information, including subscription to notifications of customer entry or leaving, to third-party systems, so that precision marketing can be implemented for target customer groups. Different advertisements and coupon information are pushed to users in different areas. This brings benefits for users, enhances their shopping experience, and improves the efficiency of targeted marketing methods. Based on user location information, Huawei partners can develop apps with business values, such as store navigation and car seeking.

Quick Service Adjustment, Covering Hotspots and Optimizing Radio Frequency

If a coverage hole exists on the network, users can use eSight Network WLAN Manager to quickly deploy services on new APs to cover hotspots.



When a carrier's APs or private APs occupy the planned channels and interfere with APs on the live network, users can use eSight Network WLAN Manager to quickly change the channel if negotiation is unavailable.



### Quick AP Fault Diagnosis

eSight Network can restart, replace, and restore APs to factory settings in a batch.

- During WLAN network debugging or when APs are faulty, users can remotely restore APs to factory settings in a batch.
- During WLAN network debugging or when APs are upgraded, users can remotely restart APs in a batch.
- If an AP is faulty, users can quickly replace the AP in eSight Network. The replacement does not affect AP configurations.



### Multi-dimensional Energy-saving Management

- Energy-saving policies based on locations are defined to disable wireless signals by radio, SSID, or AP to implement energy-saving management.
- Energy-saving policies are executed immediately or periodically.

### Resource Statistics Meeting O&M Requirements

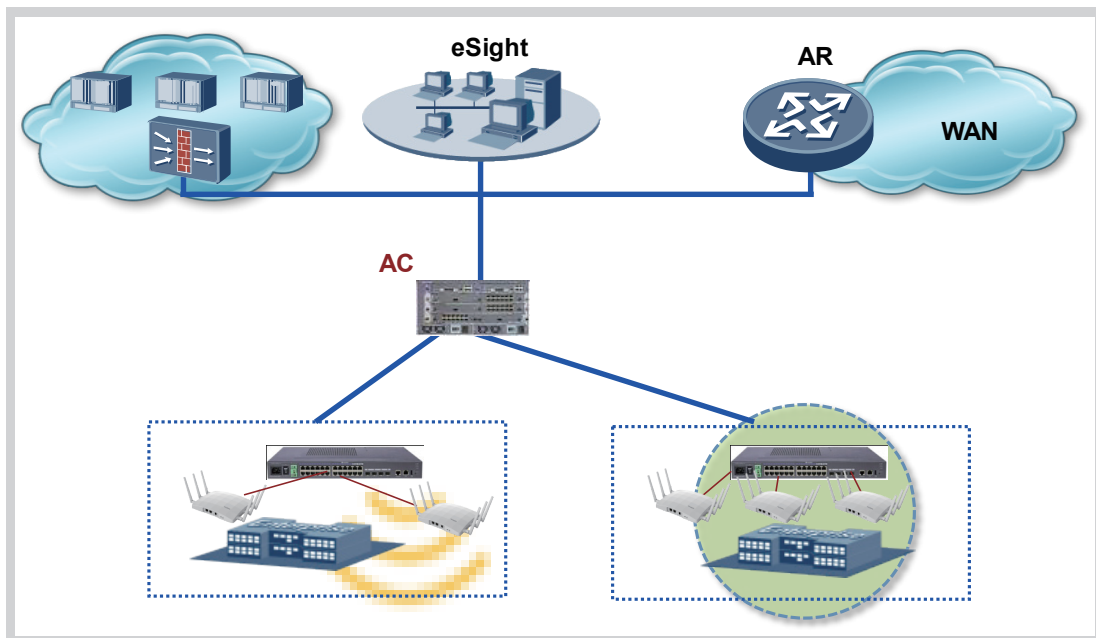
- Entire-network resource statistics: An online user line chart shows the top five accessed fit APs and SSIDs, top five device alarms, and physical resource statistics on the entire network.
- AC statistics: A line chart shows statistics about online users collected by the AC, including AP and domain information and the top five AC alarms.
- AP statistics: Shows the top five AP alarms and performance counters (including the number of terminals connected to APs, AP physical attributes and traffic, and radio traffic).
- SSID statistics: Shows the number of APs, number of VAPs, and number of terminals connected to APs.
- Region and location statistics: Displays the total number of APs, number of online APs, and number of online STAs by region and location.

## Operating Environment

eSight Network WLAN RTLS can be deployed on the same server as eSight Network Management Platform standard or professional edition, or on a different one. When they are configured on one server, they can manage no more than 500 APs of standard edition or 1000 APs of professional edition, and the configuration requirements are the same as those of the platform. When they are configured on different servers, configuration requirements are as follows:

Managed Nodes	Operating System	Server Configuration Requirement	Virtual machine Configuration Requirement
WLAN RTLS AP numbers: 0-2000 Terminal numbers: 24000	Windows Server 2012 R2 standard (64 bits), Novell SUSE Linux Enterprise Server 12.0 SP2	CPU: 2 x hexa-core 2GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> PC servers are recommended. Determine the hardware specifications based on the network scale.	VMWare-ESXI 5.0/5.5、FusionSphere V1R5、Hyper-V CPU: 16vCPU 2GHz or higher Memory: 32 GB or higher Disk space: 600 GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> Determine the hardware specifications based on the network scale.
WLAN RTLS AP numbers: 2000-5000 Terminal numbers: 64000		CPU: 4 x octa-core 2GHz or higher Memory: 64GB or higher Disk space: 600GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> Determine the hardware specifications based on the network scale.	VMWare-ESXI 5.0/5.5、FusionSphere V1R5、Hyper-V CPU: 32vCPU 2GHz or higher Memory: 64GB or higher Disk space: 600GB or higher Database: Microsoft SQL Server 2012 standard, Oracle Database Standard Edition 11g R2 <b>NOTE</b> Determine the hardware specifications based on the network scale.

## Deployment Scenarios



## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network WLAN Manager (includes 5 APs)	1	Mandatory
eSight Network WLAN License-Incremental 5 AP Licenses	Optional	One license manages 5 incremental APs
eSight Network WLAN License-Incremental 50 AP Licenses	Optional	One license manages 50 incremental APs.
eSight Network WLAN License-Incremental 100 AP Licenses	Optional	One license manages 100 incremental APs.
eSight Network WLAN License-Incremental 200 AP Licenses	Optional	One license manages 200 incremental APs.
eSight Network WLAN License-Incremental 500 AP Licenses	Optional	One license manages 500 incremental APs.
eSight Network WLAN License-Incremental 1,000 AP Licenses	Optional	One license manages 1,000 incremental APs.
eSight Network WLAN License-Incremental 2,000 AP Licenses	Optional	One license manages 2,000 incremental APs.
eSight Network WLAN License-Incremental 5,000 AP Licenses	Optional	One license manages 5,000 incremental APs.
eSight Network WLAN Real-Time Location System (RTLS)	Optional	WLAN location function for interference sources, rogue devices, and terminals
eSight Network WLAN RTLS-5AP	Optional	One license manages 5 incremental RTLS APs.
eSight Network WLAN RTLS-25AP	Optional	One license manages 25 incremental RTLS APs.
eSight Network WLAN RTLS-50AP	Optional	One license manages 50 incremental RTLS APs.
eSight Network WLAN RTLS-100AP	Optional	One license manages 100 incremental RTLS APs.
eSight Network WLAN RTLS-500AP	Optional	One license manages 500 incremental RTLS APs.
eSight Network WLAN RTLS-1000AP	Optional	One license manages 1000 incremental RTLS APs.
eSight Network WLAN RTLS API	Optional	To use the WLAN location function, the eSight Network Open SDK component is required.



# eSight Mobile Manager

## Product Overview

The rapid development of the Internet and wide application of Wi-Fi networks in various sectors, such as the government, enterprise, finance, and education, increase O&M workloads and difficulties. Network O&M personnel have to deal with an increasing number of network issues to ensure that customers can make the most of the convenience of Wi-Fi networks.

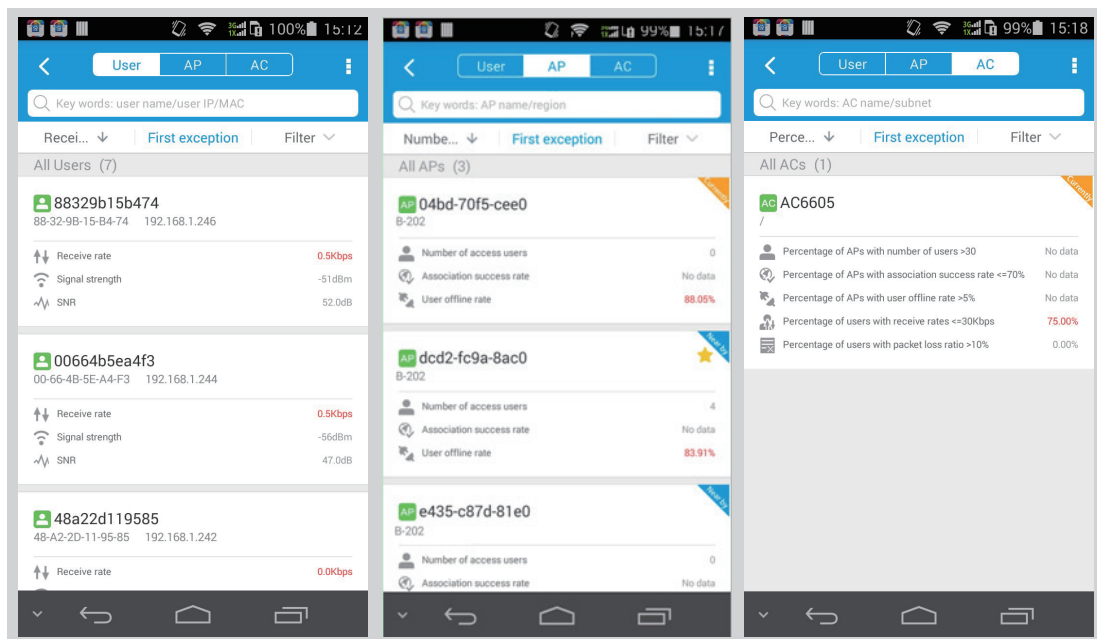
The O&M personnel can only rectify network faults after receiving user reports and may fail to accurately locate faults. In addition, troubleshooting is considerably complex and time-consuming. They urgently need a solution that can simplify O&M, improve user satisfaction, and also guarantee enterprises' benefits.

Huawei eSight Mobile is an application that can be installed on mobile terminals. Providing multiple core features, eSight Mobile allows operations and maintenance (O&M) personnel to manage Wi-Fi networks anywhere, anytime, simplifying network management and control. As an extension to Huawei's PC-based network management software eSight Network, eSight Mobile supports lightweight installation and more widespread applications, enabling enterprises to perform O&M with minimum costs while yielding higher efficiency.

## Features

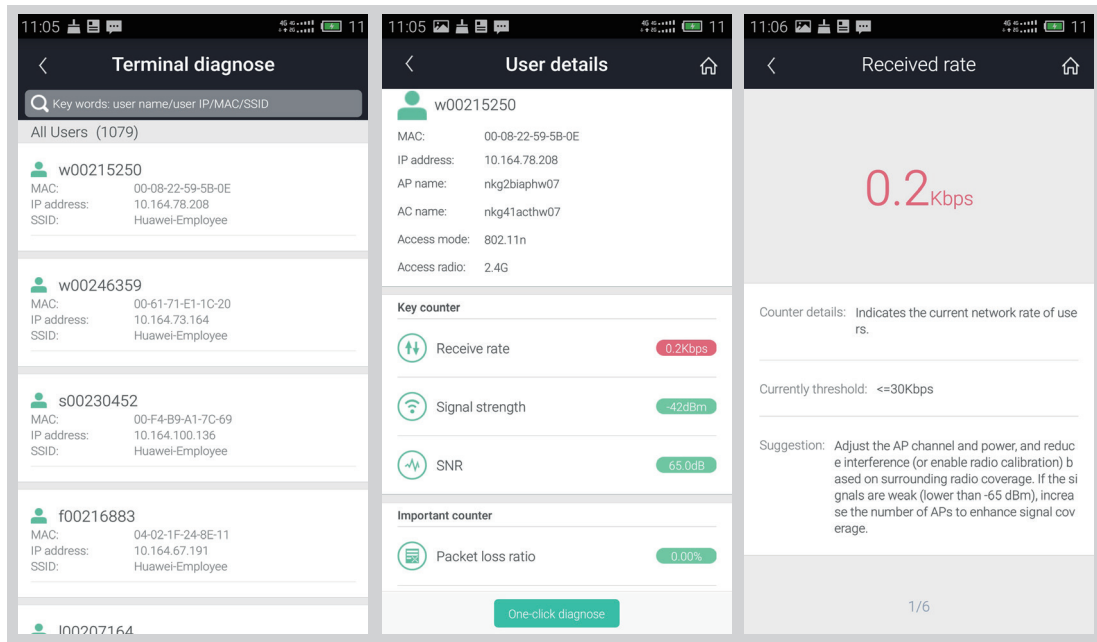
### 360-degree WLAN Monitoring

eSight Mobile displays monitored key counters and provides optimization suggestions.



## Fault Diagnosis

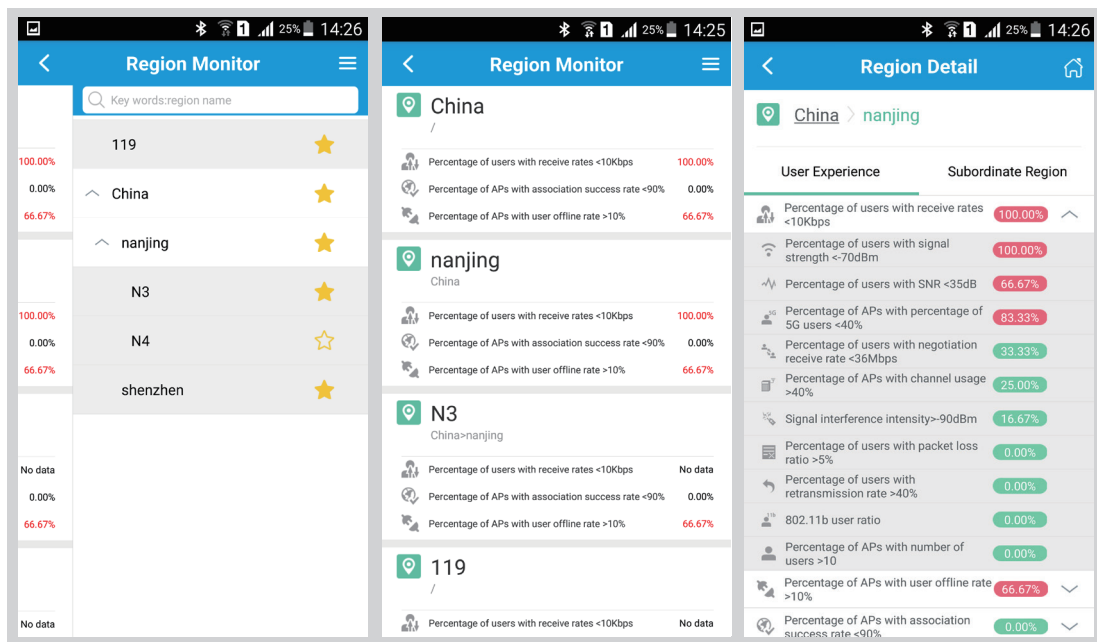
eSight Mobile searches the user who reports a fault to quickly locate the fault cause, and checks user logs to determine whether the problem is solved.



## Region Monitor

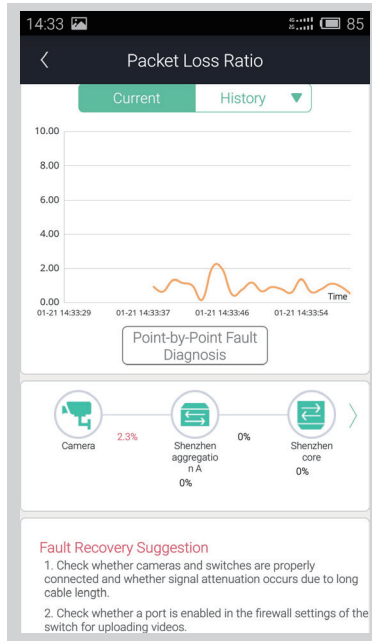
eSight provides a region monitor app that can be installed on mobile terminals to monitor the WLAN network quality by region.

- You can follow a region to monitor user experience information in the region, including the receive rate, association success ratio, and user offline ratio. You can view detailed information about a region, including user experience counters in this region and basic information about its lower-layer regions.



### iPCA

eSight Mobile releases the iPCA application to provide the iPCA capability on mobile terminals. The application enables users to create, manage, and view iPCA tasks and perform hop-by-hop network quality measurement on terminals. iPCA task list and management on terminal

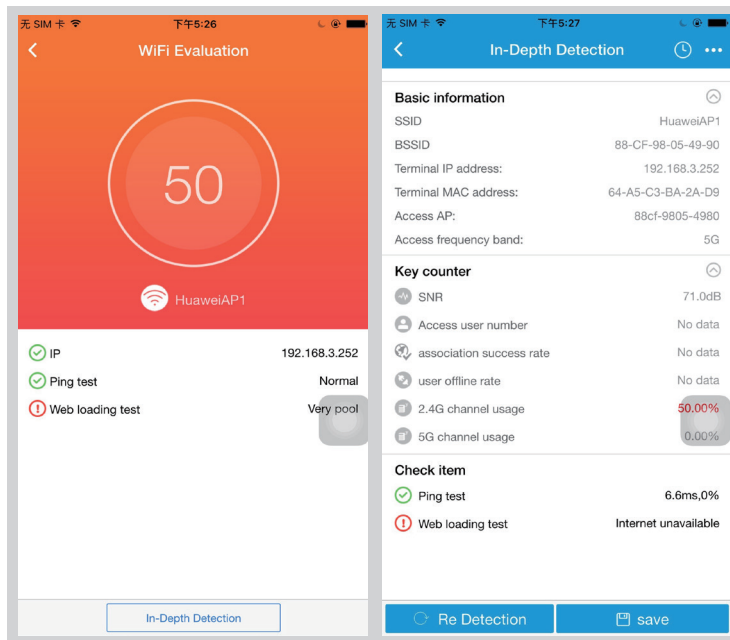


### Open SDK, Building a Win-Win Ecosystem

eSight Mobile releases the open SDK to allow enterprises or third parties to develop their own applications based on service needs, building a win-win ecosystem.

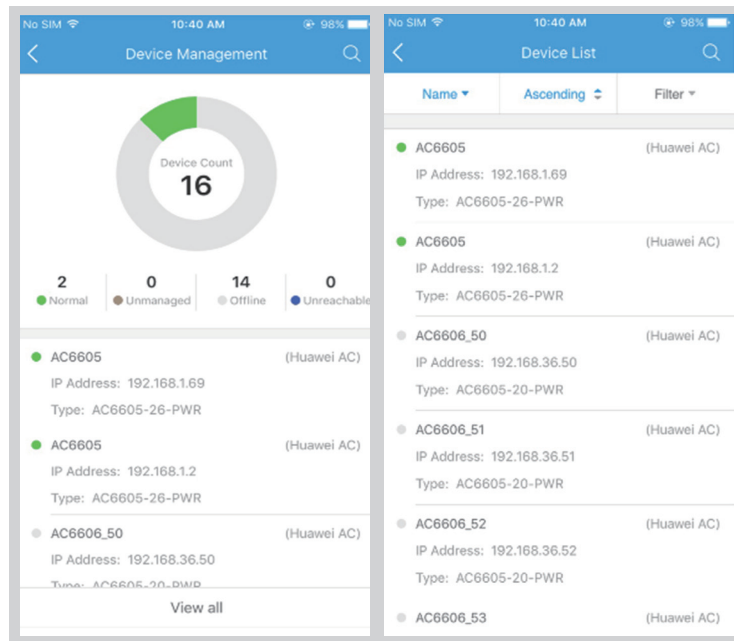
### WLAN Evaluation

The WLAN evaluation function can rapidly test the connected wireless networks and score the networks. The function can also deeply test the networks. You can configure the test items, and view, save, or export inspection records.



## Device Management

You can use your mobile phone to monitor status statistics of wired devices, expand the device list, and filter information about a specified device. You can tap a specific device to view basic device information, health status, and key performance indicators (KPIs). You can also perform ping and trace operations on a specific device.



## Operating Environment

1. eSight Mobile Manager is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.
2. The eSight Mobile app can be installed on the Android 4.2+ and IOS8.0+ system.

## Deployment Scenarios

1. Deployment scenarios for eSight Mobile Manager are the same as those for eSight Network WLAN Manager.
2. The mobile phone on which the eSight Mobile app is installed must be able to communicate with the server where WLAN Manager is installed.

## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Mobile Manager	1	eSight Mobile can be used for free, you can download from the mobile phone application market or APP Store.



# eSight Network IPSec VPN Manager

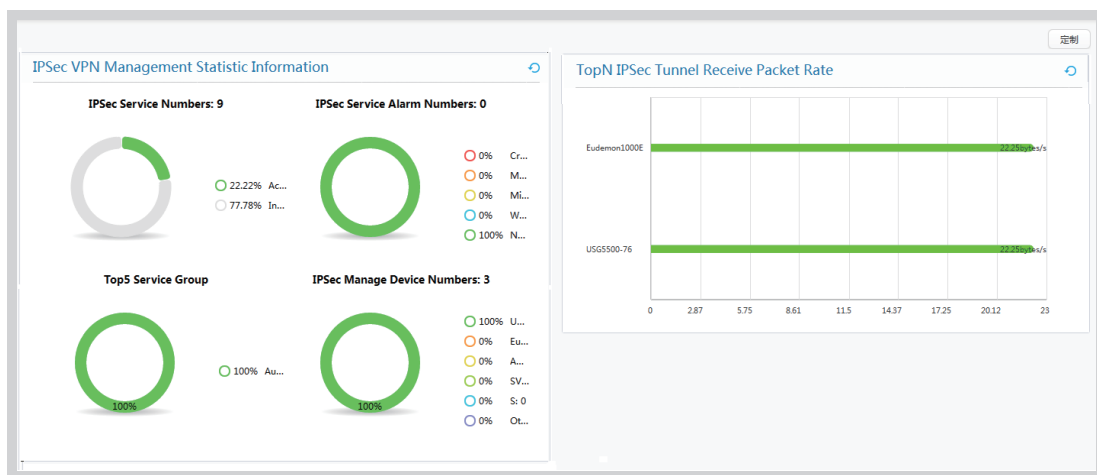
## Product Overview

Enterprises use the IPSec VPN network to carry service data, ensuring data security; however, IPSec VPN technology is complex with multiple configuration parameters and commands, leading to troubleshooting and routine maintenance difficulties.

The eSight Network IPSec VPN management component automatically discovers IPSec VPN services on a hub-spoke or site-to-site network to provide all-round monitoring and diagnosis, facilitating troubleshooting and maintenance on the IPSec VPN network.

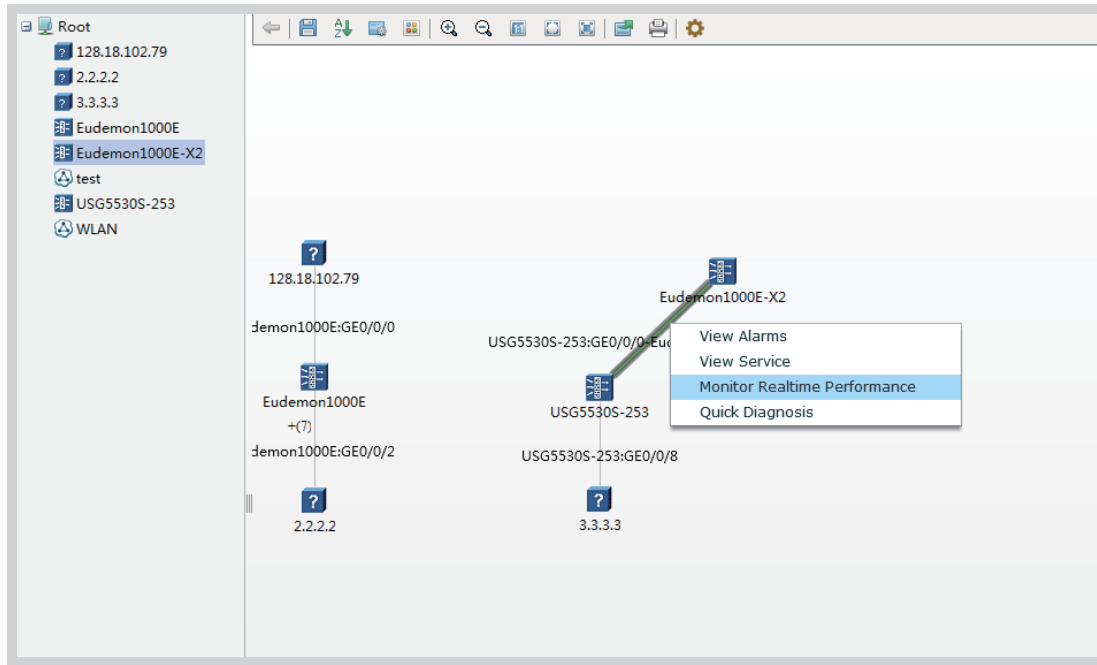
## Features

Various Statistics Display, Showing IPSec VPN Network Performance Status



## Automatic Service Discovery, Simplifying User Operation

eSight Network IPSec VPN Manager automatically discovers all or specified IPSec VPN services on a hub-spoke or site-to-site network. Users can view service alarm status, encrypted service data direction, and packet loss information on the service topology. Users can also view tunnel information and historical information about tunnel setup to help locate service faults.



## Quick Diagnosis, Improving Troubleshooting Efficiency

The quick diagnosis function allows users to find detailed causes for service faults, such as failure of activating services and VPN faults. The following information can be diagnosed: interface status at two ends, whether IPSec policies are applied to interfaces, whether the policies can initiate IPSec negotiation, IPSec policy integrity, Internet Key Exchange (IKE) negotiation result, and IPSec negotiation result. Users can export diagnosis results.

The quick diagnosis function helps you rapidly identify the fault cause. After the diagnosis is complete, you can click the Start Diagnose button to diagnose the current service.

Export All

Service Diagnose Item	Local Diagnose Result	Remote Diagnose Result
USG5530S-253:GE0/0/0-Eudemon1000E-X2:GE0/0/0	Success	Success
Interface Status	The physical layer status is Up, and the protocol layer status is Up.	The physical layer status is Up, and the protocol layer status is Up.
Apply IPSec Policy to Interface	Applied	Applied
Apply Policy That Initiates IPSec Negotiation on Interface	Applied	Applied
IPSec Policy Configuration Integrity	Configuration Integrity	Configuration Integrity
IKE Negotiation Result	The tunnel already exists.	The tunnel already exists.
IPSec Negotiation Result	The tunnel already exists.	The tunnel already exists.

20 Total records: 1

## Operating Environment

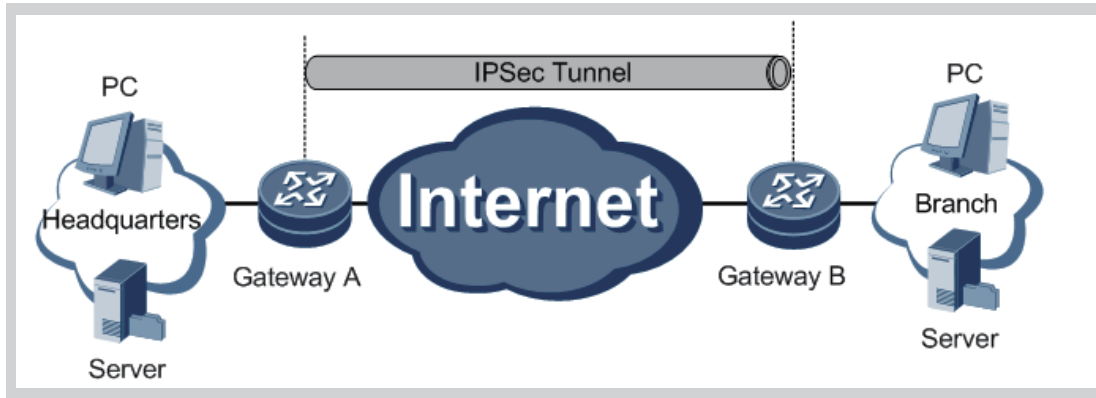
eSight Network IPSec VPN Manager is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.

## Deployment Scenarios

Currently, eSight Network supports two IPSec VPN networking scenarios: site-to-site VPN (point-to-point) and hub-spoke VPN (point-to-multipoint).

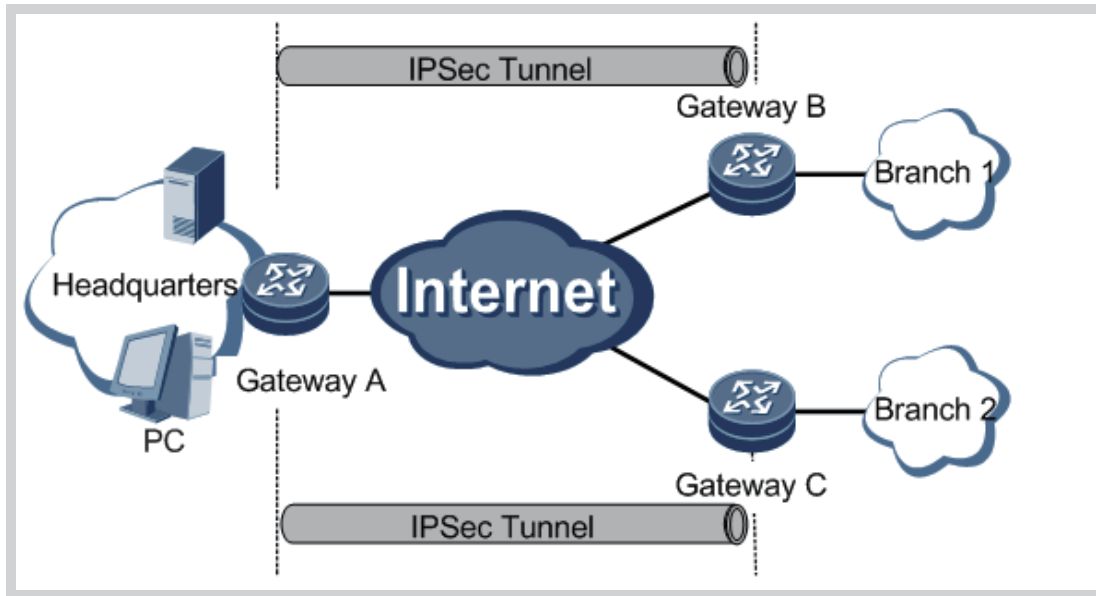
- Site-to-site VPN

A site-to-site VPN implements communication between LANs; therefore, it is also called LAN-to-LAN VPN or gateway-to-gateway VPN. Typical networking is shown below:



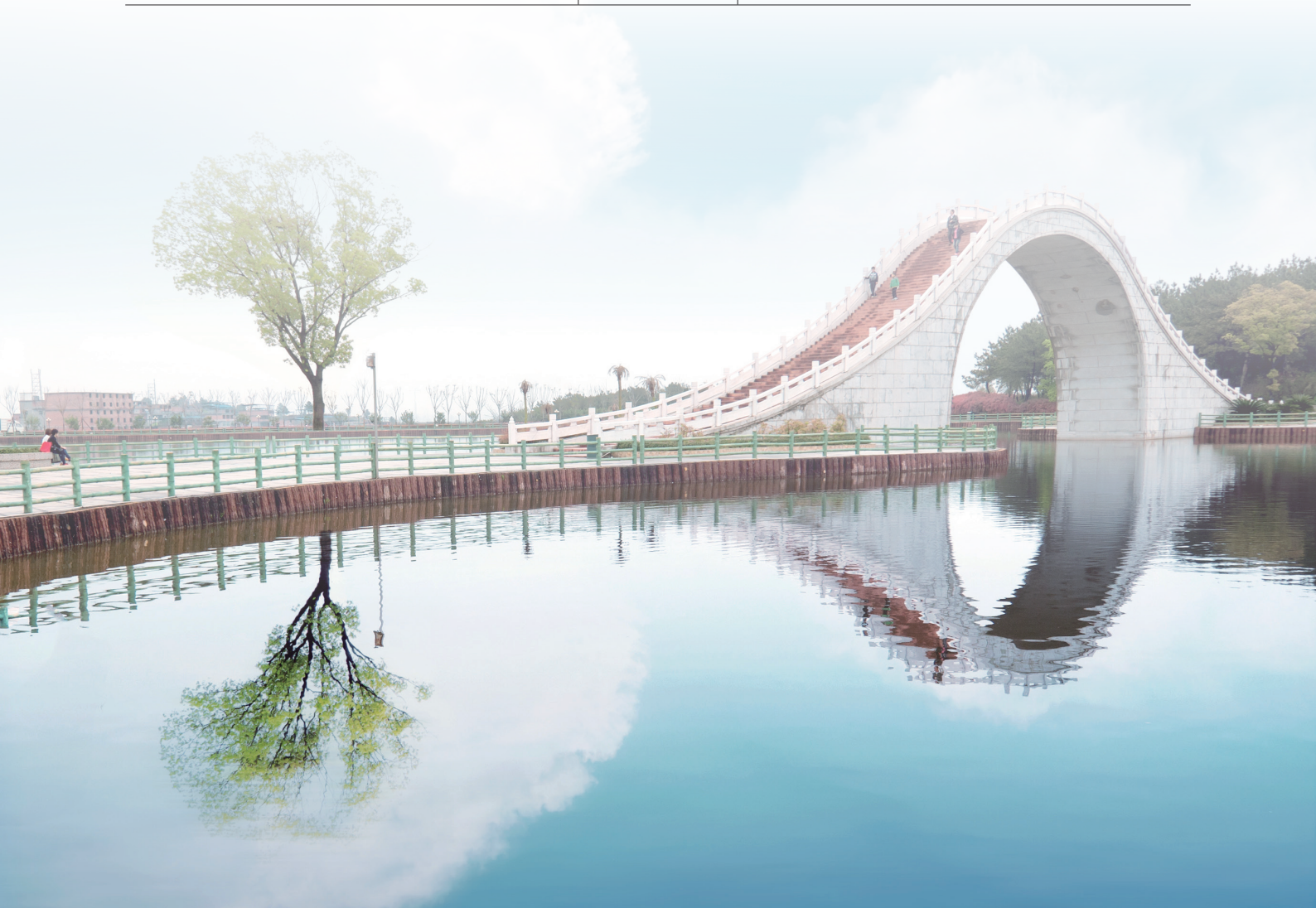
- Hub-spoke VPN

Hub-spoke VPN implements IPsec VPN communication between an enterprise headquarters and its multiple branches. Typical networking is shown below:



## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network IPSec VPN Manager (includes 60 devices license)	1	Mandatory. One license manages 60 devices.
eSight Network IPSec VPN License-Incremental 50 Devices license	Optional	One license manages 50 devices.
eSight Network IPSec VPN License-Incremental 100 Devices license	Optional	One license manages 100 devices.
eSight Network IPSec VPN License-Incremental 200 Devices license	Optional	One license manages 200 devices.
eSight Network IPSec VPN License-Incremental 500 Devices license	Optional	One license manages 500 devices.
eSight Network IPSec VPN License-Incremental 1,000 Devices license	Optional	One license manages 1,000 devices.





# eSight Network Secure Center

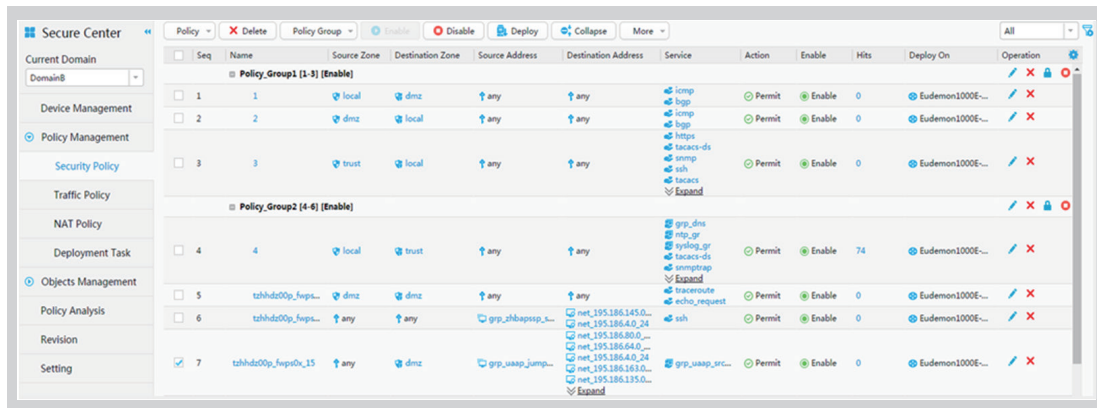
## Product Overview

eSight Network Secure Center provides security policy management functions (such as unified configuration and deployment of security application policies on the entire network) for firewalls, helping users manage multiple security devices in a unified manner and reducing security O&M costs.

## Features

eSight Network Secure Center supports the unified configuration of security application policies.

eSight Network Secure Center centrally manages security application policies on firewalls. Administrators can manage security policies from multiple dimensions, such as user, user group, and device. They can create, modify, copy, move, enable, disable, deploy, lock, unlock, batch import, and batch export security policies and manage policy groups. Secure Center also supports global configuration of service-based policies and objects to simplify device configuration. In addition, administrative domains are defined to grant administrators operation rights on different domains, isolating their managed data.



eSight Network Secure Center supports quick backup and restoration of policies and objects.

eSight Network Secure Center supports manual and automatic backup and restoration of firewall policies and objects. After planning and deploying policies and objects, administrators can manually back up policies and objects or Secure Center automatically backs up data periodically. Administrators can also compare backup data to determine the one used for restoring network configurations. If incorrect data is planned and leads to abnormal service running, administrators can quickly replace incorrect data on eSight with backup data and deliver the data to devices to ensure that the network can quickly restore the normal status.

eSight Network Secure Center supports configuration source tracing for users' operations, to see the difference between every operation.

The screenshot shows the 'Secure Center' interface with a table of configuration operations. The table has columns for Name, Category, Operation, Operation Source, Users, Date, and Comment. The current data shows a list of Traffic Policy operations (d1 to d10) performed by 'admin' via 'Synchronization' on 2017-09-19 10:34:09. A sidebar on the left contains navigation options like Device Management, Policy Management, Objects Management, etc. The bottom of the table shows pagination: Total records: 148, with page 10 selected.

Name	Category	Operation	Operation Source	Users	Date	Comment
d10	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
Current Data						
Name=d10 Enable=true Outbound interface1=Eth-Trunk2 Action=limit Traffic profile1=d_max_single_down Deploy on1=Kudemon1000E-N61-99.42 Add after=d9						
d9	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d8	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d7	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d6	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d5	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d4	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d3	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d2	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	
d1	Traffic Policy	Add	Synchronization	admin	2017-09-19 10:34:09	

eSight Network Secure Center supports virtual firewall management.

eSight Network Secure Center automatically detects virtual firewalls and configures security policies on them and can configure and manage security policies on hundreds of virtual firewalls in a unified manner.

The screenshot shows the 'Virtual System' management interface. It displays a table of virtual systems with columns for Name, Deploy Status, Resource Class, VLAN ID, Interface, and Operate. The table lists various virtual systems (aaa, auto\_1, cc\_test\_cmd\_address, etc.) and their deployment status. The interface includes a sidebar with navigation options like View, Device Config, Web NMS, etc. The bottom of the table shows pagination: Total records: 15, with page 1 selected.

Name	Deploy Status	Resource Class	VLAN ID	Interface	Operate
aaa	Deployed				✓ ✗
asdf	Deployed				✓ ✗
auto_1	Deployed	auto_1	9	GigabitEthernet0/3	✓ ✗
cc_test_cmd_address	Deployed				✓ ✗
ccTest	Deployed				✓ ✗
cctest	Deployed				✓ ✗
qc	Deployed				✓ ✗
qc1	Deployed				✓ ✗
qc3	Deployed				✓ ✗
qc4	Deployed				✓ ✗
qc_205.10	Deployed			GigabitEthernet0/4	✓ ✗
test_10	Deployed				✓ ✗
vsys1	Deployed			GigabitEthernet0/7	✓ ✗
vsys2	Deployed				✓ ✗
www	Deployed				✓ ✗

## Operating Environment

eSight Network Secure Center is installed on the same server as eSight Network Management Platform standard or professional edition; therefore, the operating environment configuration requirements are the same.

## Deployment Scenarios

Deployment scenarios for eSight Network Security Center are the same as those for eSight Network Management Platform.

## Ordering Information

Item	Quantity	Remarks
eSight Network Management Platform-Standard Or eSight Network Management Platform-Professional	1	Mandatory for eSight Network Management Platform
eSight Network Device Manager(includes 60 devices license)	1	Mandatory for eSight Network Device Manager
eSight Network Secure Center (includes 5 devices license)	1	Mandatory. The eSight Network Secure Center provides basic functions of security policy management, including five device management licenses.
eSight Network Secure Center License-Incremental 5 Devices	Optional 0 to 600	One license manages five incremental devices.
eSight Network Secure Center License-Incremental 25 Devices	Optional 0 to 120	One license manages 25 incremental devices.





# HUAWEI eSight Network



# More Information

For more information, visit <http://enterprise.huawei.com/en>.

## Professional Service and Support

Huawei Professional Services provides expert network design and service optimization tasks, helping customers design and deploy a reliable, secure, high-performance network, maximizing return on investment and reducing operational expenses.

## Company Addendum

For more information, visit <http://enterprise.huawei.com/en/> or contact your local Huawei office.

Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

## NO WARRANTY

Unless otherwise specified, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees, or representations of any kind, either express or implied.

To the maximum extent permitted by applicable law, in no event shall Huawei Technologies Co., Ltd. be liable for any special, incidental, indirect, or consequential damages, or lost profits, anticipated savings, business, revenue, data, or goodwill.

Huawei Technologies Co., Ltd.

Huawei Industrial Base

Bantian, Longgang

Shenzhen 518129

People's Republic of China

Tel: +86 755 287 80808

Website: <http://www.huawei.com.cn>

**Copyright © Huawei Technologies Co., Ltd. 2017. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

#### **Trademark Notice**



HUAWEI, HUAWEI, and  are trademarks or registered trademarks of Huawei Technologies Co., Ltd.

Other trademarks, product, service and company names mentioned are the property of their respective owners.

#### **General Disclaimer**

The information in this document may contain predictive statements including, without limitation, statements regarding the future financial and operating results, future product portfolio, new technology, etc. There are a number of factors that could cause actual results and developments to differ materially from those expressed or implied in the predictive statements. Therefore, such information is provided for reference purpose only and constitutes neither an offer nor an acceptance. Huawei may change the information at any time without notice.

HUAWEI TECHNOLOGIES CO.,LTD.  
Huawei Industrial Base  
Bantian Longgang  
Shenzhen 518129,P.R.China  
Tel: +86 755 28780808

[www.huawei.com](http://www.huawei.com)