Samsung Wireless Enterprise Security v1.0 (WES)

Operation Manual

Disclaimer

Every effort has been made to eliminate errors and ambiguities in the information contained in this document. Any questions concerning information presented here should be directed to SAMSUNG ELECTRONICS AMERICA, 1301 E. Lookout Dr., Richardson, TX 75082, (972) 889-6700. SAMSUNG ELECTRONICS AMERICA disclaims all liabilities for damages arising from the erroneous interpretation or use of information presented in this manual.

Publication Information

SAMSUNG ELECTRONICS AMERICA reserves the right without prior notice to revise information in this publication for any reason. SAMSUNG ELECTRONICS AMERICA also reserves the right without prior notice to make changes in design or components of equipment as engineering and manufacturing may warrant.

Copyright 2015

Trademarks

Product names mentioned in this manual may be trademarks and/or registered trademarks of their respective companies.

Before installation and operation of the product, please be sure to read this manual to use it in a safe and appropriate manner by following the instructions.

This manual is subject to change according to modifications of designs or for enhancing the functions of the product. If you need a revised manual or have any inquiries regarding the contents of the manual, please visit the following website for more information.

If you have any complaints or requests, please call our **Call Center at the following number**: **(972) 889-6700**

INTRODUCTION

Introduction to the manual

This manual explains the overview, management, and configuration methods for Samsung Wireless Enterprise Security (hereafter 'WES'). This manual is written in accordance with WES v1.0.

Document Content and Organization

This manual consists of four chapters and definitions of terms.

CHAPTER 1: Overview of WES

This chapter includes an overview of the WES product, which explains the general concept of its operation and the main security functions and characteristics, etc. In addition, it provides information on system requirements for installation and the components of the product, as well as instructions for initial operation procedures required for operating the product.

CHAPTER 2: Preferences

This chapter provides instructions for how to set the basic settings in the system in order to operate WES. It also includes the method of setting and managing Anyclick administrator and targeting equipment or devices as well as the method of managing the map information.

CHAPTER 3: Policy

This chapter provides instructions on how to set the security policy in order to prevent an invasion or breach through a wireless network.

CHAPTER 4: Monitoring

This chapter provides a description and explanation for the status (statistics) regarding operation of the product and how to make inquiries about various events or logs for the safe maintenance of a network. It also includes methods for making inquiries on the status of operating devices, printing out reports or performing an integrity test, and gives an explanation for the dashboard on which of the various information types can be viewed regarding WES operations, allowing real-time on-screen monitoring.

Definitions of Terminology

Explanations are provided for the terms to be used in this manual.

Conventions

The symbol to be used in this manual is provided as follows. The information accompanied with this symbol must be learned in order to use the system in a safe and proper manner.

Note

Additional information is provided for the text or the article.

Revision History

version	Date of creation	Remark
1.0	2015.03.13	First Version for North America

TABLE OF CONTENTS

Table of figures

CHAPTER 1. Overview of WES

This chapter includes general information such as the specifications, components, and system requirements, etc., of the product. It also provides explanations for the start-up and termination of the management console to operate the product as well as the management process for users and targeted devices.

1.1 Overview of WES

1.1.1 WES

Today's business environment which requires quick responses to changes, has a great effect on the IT environment providing the business infrastructure for an organization. One of the most remarkable alterations to the paradigm in Information Technology is the popularization of mobility is the popularization of mobility. A number of organizations provide wireless networking environments to increase the productivity of the users of information and business agility in commercial activities. However such strengths come with consequences such as vulnerability to illegal access by unauthorized users, network eavesdropping, and data theft, when compared to wired networks.

In numerous situations, wireless networks have demonstrated low performance due to various factors such as signal interference between wireless devices having similar frequencies or signal distortion and disturbance by obstacles. However, there are many cases where it is difficult to pinpoint the causes of poor performance. In addition, the security threat bywireless devices used without permission brings fatal results that may surpass the security threats for a wired network.

WES detects invasions via unauthorized wireless devices installed on the intranet or the gateway section detour of the employees who connect to the general-purpose wireless network illegally, etc. This serves as a solution to prevent invasions via wireless networks, bymonitoring the adequacy of the construction of the wireless network infrastructure and detecting security vulnerabilities in order to build safe and efficient wireless network environments.

1.1.2 Functions and characteristics of WES

Detection and blocking of wireless threats

To secure the availability of service and prevent internal information leakages, WES applies various event policies such as the managed AP policy, operation policy, and security policy in order to efficiently cope with a number of wireless security threats and prevent security-related accidents in advance.

Detection and monitoring

The system allows for the detection of all kinds of wireless devices having the Standard protocols of 802.11a/b/g/n/ac and may detect 2.4 GHz or 5 GHz of bandwidth simultaneously. Also, for efficient and systematic management of wireless devices, it provides the function of monitoring the information on status. This includes the configuration of detected wireless devices, the connected station, and the location, etc., As such information can be used as supplementary data for enhancing the performance of networks in the future and managing the life-cycle of traffic in such devices, it can also serve as a traffic-monitoring tool in checking trends in traffic changes. It additionally provides the function of monitoring all kinds of channels abroad which comply with the wireless networking standards of 802.11 a/b/g/n/ac and have 2.4 GHz/5 GHz of bandwidths.

Setting and management of wireless devices

Management of a Mis-Configured AP may control the security configuration of wireless devices such as SSID, wireless networking standards, data encryption methods, authenticationmethods or violation of manufacturer's responsibilities. This provides the ability to control the communication volume of stations in the AP and operation policies for the number of connected stations, based on thresholds, location of detected authorized or unauthorized AP, and channel areas by using specialized sensors using the Floor Plan.

Statistics and general functions

For the efficient monitoring of wireless device statuses, it provides a dashboard to check important information on the status of servers, wireless devices or even policy violations. At just one glance, the function of putting out logs, statistics, and reports can be viewed andused as supplementary data to enhance the performance of networks. It can also inspect and track information in the case of network failures.

1.1.3 User authority of WES

WES classifies administrators into root administrators, Supervising administrator, senior-administrator, and administrators according to their authorities. The authority and scope of each administrator are as follows:

Type	Description	
Root administrator	**Authority**	Root administrator performs all types of security functions related to the operation of WES and the management of administrator accounts. A root administrator receives training on the management functions of WES and performs duties in a proper manner.
	Scope	The overall management and operation of WES.
Supervising administrator	**Authority**	Supervising-administrator performs all of the functions in the same manner asa root administrator except for some functions in the management of security objects.
	Scope	All of the functions except for the management of security objects (account management)
Senior administrator	**Authority**	Senior-administrator performs all of the functions in the same manner as a supervising-administrator except for some functions in the setting and management of security objects.
	Scope	All of the functions except for the management of security objects (account management) and general setting (Preferences, MAP setting and sensor setting).
Administrator	**Authority**	Administrator performs some functions, such as making inquiries or monitoring, etc.
	Scope	All of the functions except for the management of security objects (account management) and general setting (Preferences, MAP setting, sensor settingand policy setting).

1.1.4 Server operation mode of WES

The operation mode operating after the installation of a WES server is as follows:

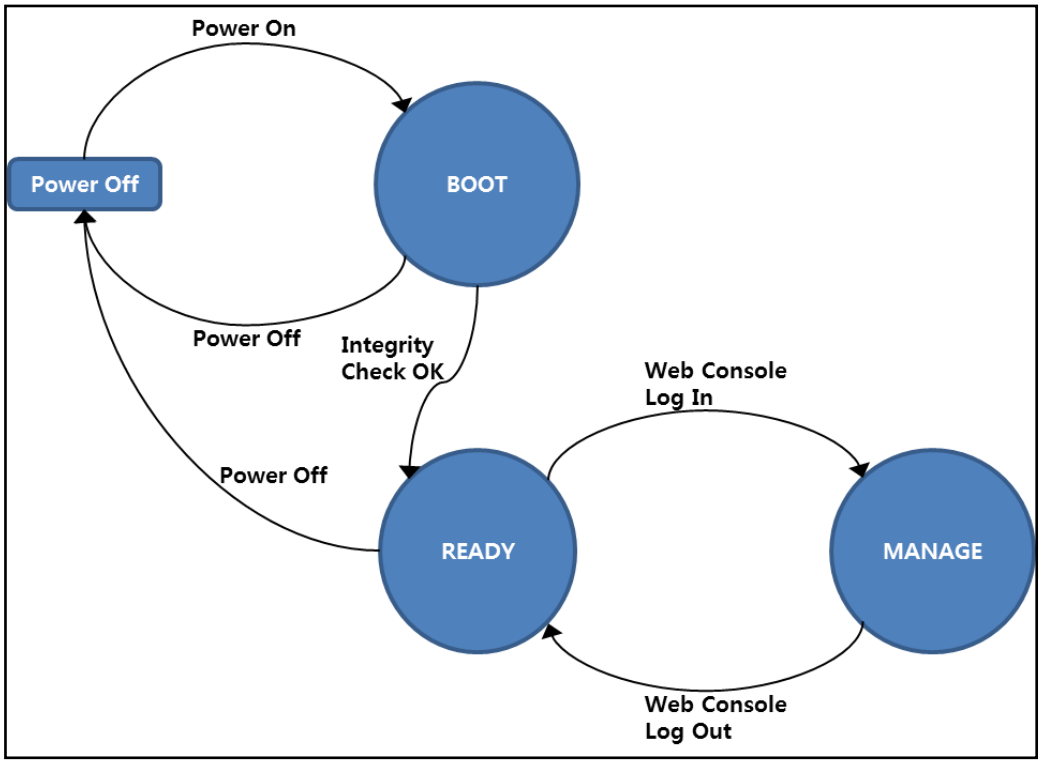


Figure 1. WES server operation mode

The WES server has BOOT, READY and MANAGE modes. BOOT mode is activated when the WES server is initiated by an administrator. Once the WES server is started, it checks the operation of each daemon the targeted files for integrity check.

In BOOT mode, the related daemons are implemented normally. Once the integrity test is finished, the server of WES is switched to READY mode. In READY mode, the header information of outgoing packets from backbone switches and the header information of wireless packets from the sensor of WES are collected and analysed.

If an authorized administrator logs into the web console, it will switch to MANAGE mode; he/she will be given the authority to manage all security-related functions for WES, as portrayed below

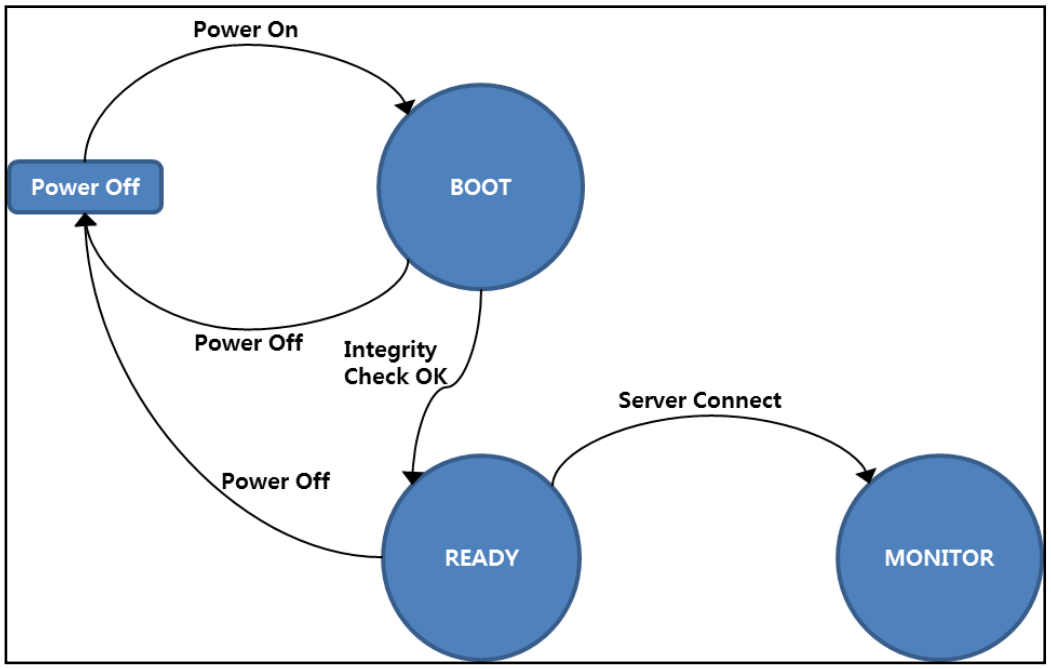


Figure 2. WES sensor operation mode

The WES sensors have BOOT, READY, and MONITOR modes. BOOT mode is implemented by an administrator in the case where the WES sensors become operated. If the sensors become activated they check the daemons to verify whether they are running in normal operation and inspect the targeted files for integrity tests.

In BOOT mode, the related daemons are implemented normally and once the integrity test is finished the WES sensors switch to READY mode. In READY mode the information of packets detected on wireless networks is collected and the connection is attempted through mutual authentication with servers. Once the communication is made to servers, it is switched to MONITOR mode; by transferring the collected information on wireless packets it detects wireless security threats. As a result it blocks wireless devices which generate security threats, according to commands received from the server.

1.1.5 System requirements in administrator PC

An administrator's PC when connecting to a WES server must meet the system requirements as follows:

Type	Item	System requirements
Hardware	CPU	INTEL Pentium4 1.4GHz or larger
	Memory	512MB
	HDD	Disk space with capacity of 10GB or larger
	NIC	One or more of Ethernet LAN cards
Software	OS	Windows 7 or later version
	Others	[Console security management connection] SSH connection program which may support SSHv2 (AES-256 / SHA-256) or better. [Web Console security management connection] Internet Explorer 8.0 or later version (all the later versions of web-browsers which support TLS V1.2), Adobe Flash Player 10 or later version

1.2 WES Administrator console

An administrator may manage all of the settings related to security functions by connectingthe WES server using web-browsers. Also for data protection in the WES server and administrator's console a HTTPS-based security communication channel is provided. HTTPS is a web protocol installed in the web browser in order to encrypt and decrypt the page requests of users at the sub-levels of SSL next to the HTTP (Hypertext Transfer Protocol) level.

1.2.1 Administrator login

By using the address window in a web-browser you can input the IP address of the web page for WES. When the login screen pops up as follows insert the administrator's ID and Password. After the first login, the ID and the password must be changed.

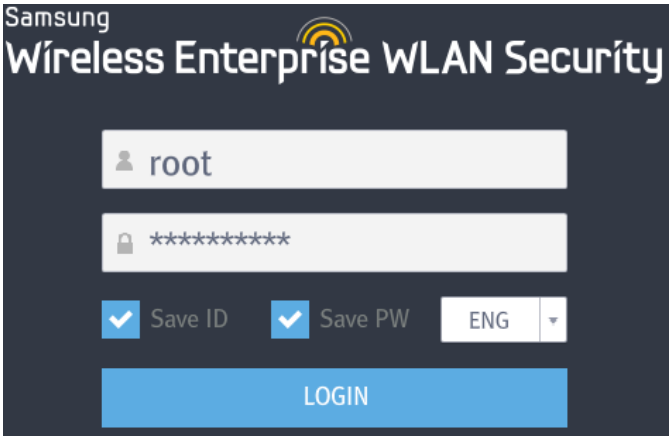


Figure 3. Login

If you log in for the first time after the server packages are installed the configuration of a root administrator's account information and IP for connecting as an administrator is obligatorily activated. **Please refer to section 2.3.6 ‘account management’ for more information on setting an administrator's password and to section 2.2.1 ‘System settings’ for accessible IP settings.**

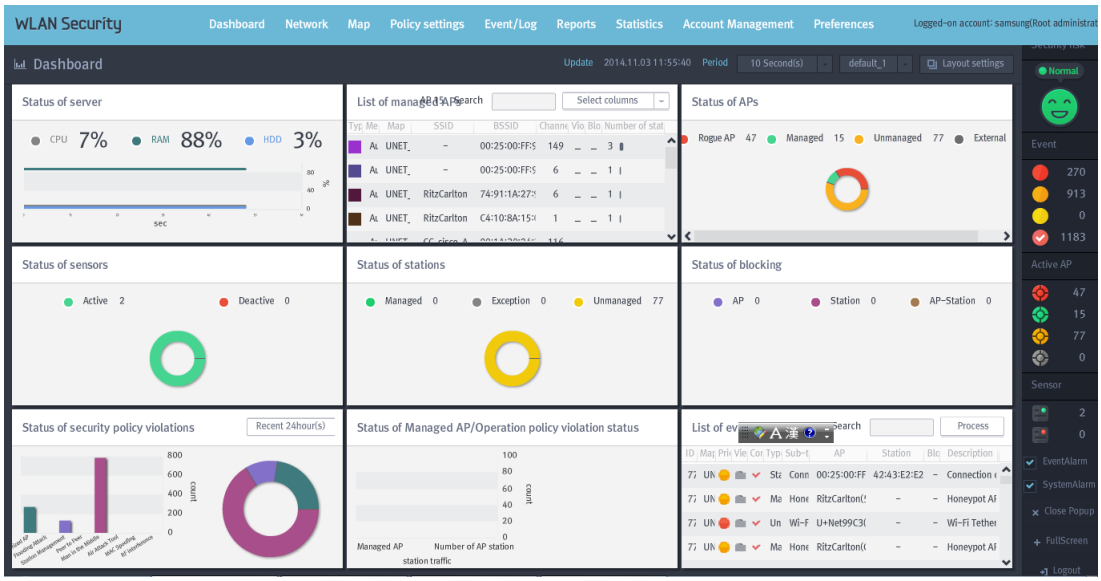
NOTE

In case display errors are generated after the installation or update of Adobe Flash Player, or if the login screen or dashboard screen is not properly displayed, you should check the Adobe Flash Player settings. In the pop-up window (accessed with a click of right mouse button on the login screen), if on the tab for **‘Global settings > storage’** the option of **‘allow the sites to save the information in this computer’** at the bottom is unchecked, please check the option and log in again on the screen.

1.2.2 Screen architecture

When you first connect to the WES server through the login process, the splash screen is displayed as follows: the main menu **on the top side** prints out the main menu by each function and log-on account and the main screen **on the bottom side** shows the dashboard screen. In the case of logging onto the web console (in the case of implementing the dashboard in the main menu) and the details screen in the case of selecting the details menu in the main menu. The sub-menu **on the right side** prints out the security risk status, information on Event/AP/Sensor status, event notification, system notification, integrity check, close pop-up, full screen, and log-out screen.

Figure 4. Dashboard



Main menu

For the operation of WES, you must set the various operation settings and objects in the system and security policies, etc. For this, 9 kinds of main menus are provided: **Dashboard,Network, Map, Policy settings, Event/Log, Reports, Statistics, Account management, andPreferences.** If there are sub-menus, such sub-menus are revealed upon selecting the main menu.

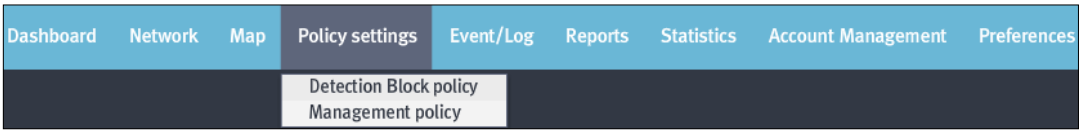


Figure 5. Main menu and sub-menu

10 kinds of additional information, besides the main menus, are also provided, and the contents regarding each additional type of information are as follows:

- **Logged-on account:** ID of the currently logged-on account is displayed.
- **Security Risk:** Security risk at the present status is displayed.
- **Event:** Depending on their priority, the events which have occurred in the recent 24 hours are classified into HIGH (RED)/MEDIUM (ORANGE)/LOW (YELLOW). The number of unidentified events is displayed as.

  - Active AP: The AP detected by sensors is classified and displayed by type.
  - Rogue AP (RED): despite their location within the intra-network among those detected these APs are not registered as targets to be managed, but are identified to be connected to other.
  - Managed APs (Green): located within the intra-network among those detected, these APs are registered as targets to be managed.
  - Unmanaged APs(Orange): despite their location within the intra-network among those detected, these APs are not registered as targets to be managed nor identified as those to be connected to other wireless stations.
  - External APs (Grey): these are not located within the intra-network among those detected.
- **Sensor:** Classified and marked as Activated (Green)/Deactivated (Red).
- **Event alarm:** Configures pop-up options for the event alarm window.
- **System alarm:** Configures pop-up options for the system alarm window.
- **Full Screen(window screen):** Switches from web-console screen to full screen (window screen).
- **Log-out:** Logs out of the web console.

NOTE

Sensors in the sub menu/Active AP/Event status are renewed according to the cycle of Dashboard updates. For more details, **please refer to section 4.6.1 'Dashboard'**

Dashboard/Details window

In the case of connecting to the web console or selecting the option of real-time status under the main menus, the dashboard screen is displayed. On the dashboard screen, 18 kindsof information can be viewed. These include: the status of a server, the list of managed APs, the sensor, the status of operation policy violations, the list of events, the status of real-time traffic in managed APs, the status of policy violations, the status of attempts to authenticate managed APs, the status of traffic in the managed AP, the status of security risks, the list of AP violating policies, the list of blocked APs and stations, and the list of connected stations. According to the layout settings, you may selectively check this information.

In order to process the events on the dashboard directly, you should use **'Event information'** which is displayed when you double-click on the event to be processed in the list of events. In order to process one or more events, you should select the events to be processed and click the **[Process]** button to process them all at once.

Also, when you select the main menus/sub-menus under them, the details screen\from the selected menu is revealed. The methods of setting in each menu will be explained in further detail from Chapter 2 to Chapter 4.

1.2.3 Log-out

You can terminate the web console by selecting the option or shutting down the windows in a web browser.

NOTE

If there is no more input for the predefined time set by the root administrator (1/3/5/10 minutes) after logging onto the web console, you will be logged out automatically.

CHAPTER 2. Preferences

This chapter explains the methods for setting the security functions of WES. Configuration options include those for system operation, the management of devices and users, and methods for setting map information, etc.

2.1 Overview

2.1.1 Preferences

- **System settings:** Information on the version of installed server/access restriction (accessible IP, the maximum number of allowable failed logins)/SMTP server for sending emails/NTP server address/AUS server address/external SYSLOG server address are set.
- **Log settings:** This sets the retention period or the threshold of disk storage for log aging.
- **OUI settings:** This registers the information on the manufacturer of network devices in a server.
- **Wired switch settings:** This deals with the information on the wired switch which will be used to block the wired connection.
- **DB backup/restoration:** This backs up the DB information or restores it from the backups.

2.1.2 Management of equipment and administrator

- **AP management: This adds/modifies/deletes the AP information.**
- **Station management:** This is used to check the information on stations connected to AP.
- **Sensor management:** This monitors the registered sensors or sets the blocking options for the firmware.
- **Connection management:** This manages the station connected to the network and the AP and set the connection graph between station and AP.
- **Account management: This manages the information on the administrators of WES.**

2.1.3 MAP info

You may find the location of APs detected by sensors or the sensors on each map.

2.2 Preferences

This chapter explains the methods of setting the operating environment as provided by WES.

2.2.1 System settings

WES supports access to a server and data synchronization with external servers through system configuration.

Preferences > System settings

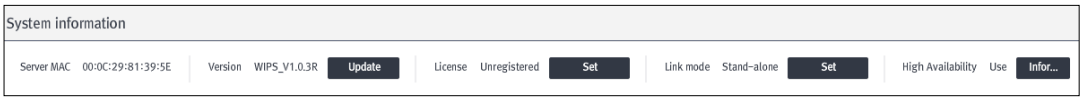


Figure 6. System settings-System Information

When **you click the [update]** button in the version menu, the explorer screen appears and you may select and upload the rpm files to be uploaded.

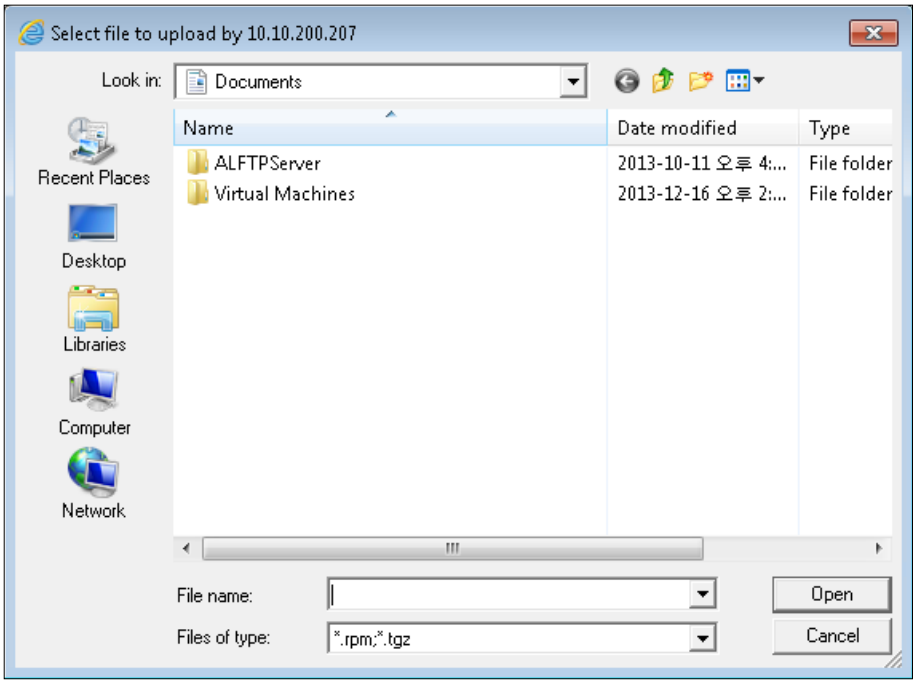


Figure 7. Selection of Server update File

From the License menu, you may check the information on the registered license; if it is unregistered, when you click on the **[Set]** button, the screen for setting License information will be displayed.

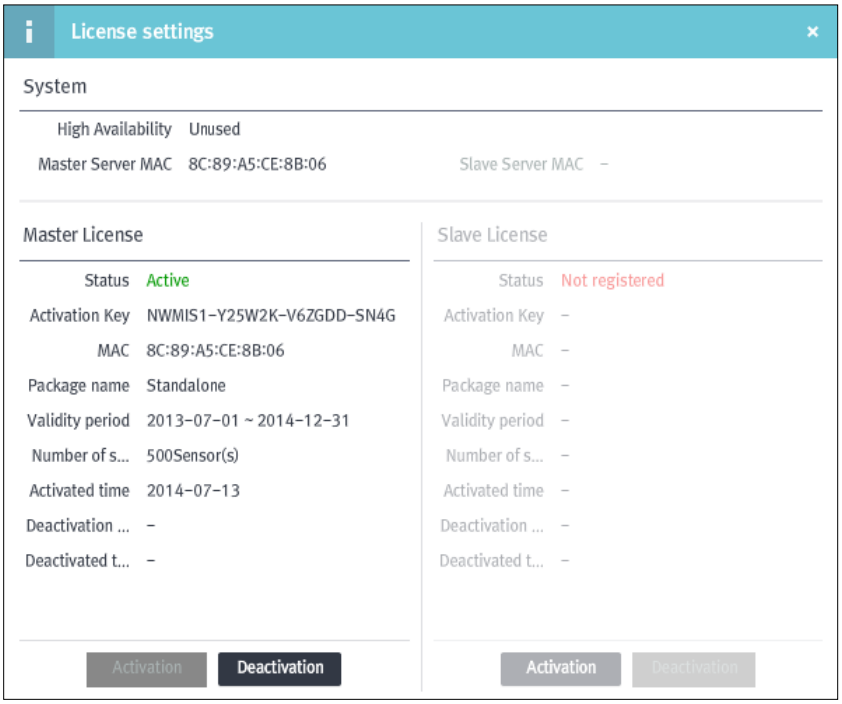


Figure 8. License settings

Clicking the **[Activation]** button will display the explorer screen and you may select and upload the activation key file.

From the link mode menu, you can click on the **[Set]** button to access the screen for setting link mode. When you set the mode to **'Stand-alone'** on the link mode screen, the screen will be displayed as below.

Figure 9. Stand-alone mode settings

When you set the link mode to **'APC link,'** the screen will be displayed as below.

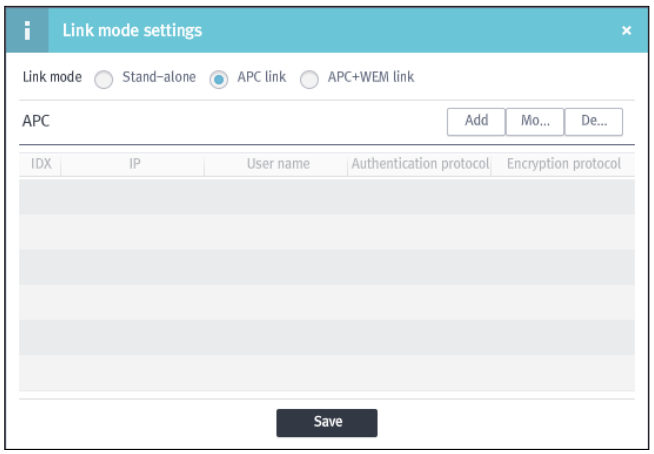


Figure 10. APC link mode settings

In the case of APC link mode, WES provides the functions to add/'modify/delete for managing the APC for linked WES.

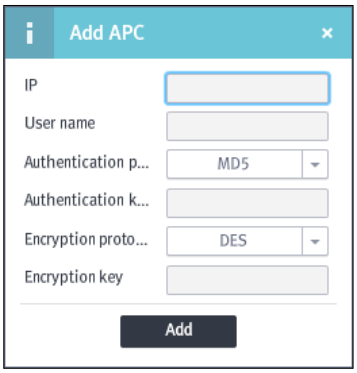


Figure 11. Add APC

Input Item	Description	Effective Value (Default)
IP	Sets the IP address of APC.	1.1.1.1~255.255.255.255 (None)
User Name	Sets the user names of APC.	8~15 characters (None)
Authentication Protocol	Sets the protocol to be used in the case of mutual authentication.	MD5 / SHA (MD5)
Authenticated Key	Sets the key value to be used in the case of mutual authentication.	8~20 characters (None)
Encryption Protocol	Sets the encryption protocol to be used in the case of mutual data communication.	DES / AES (DES)
Encrypted Key	Sets the encryption key value to be used in the case of mutual data communication.	8~20 characters (None)

[Modify]: After selecting the APC to be modified in the list of APCs, click the **Modify** button in the upper area. Once the screen for modifying the APC appears, you may modify the options of your choice.

[Delete]: After selecting the APC to be deleted from the list of APCs, click the **Delete** button.

In the case of the **'APC+WEM link'** mode, WES provides management functions such as add/modify/delete, etc., allowing APCs to be linked and functions for modifying WEM.

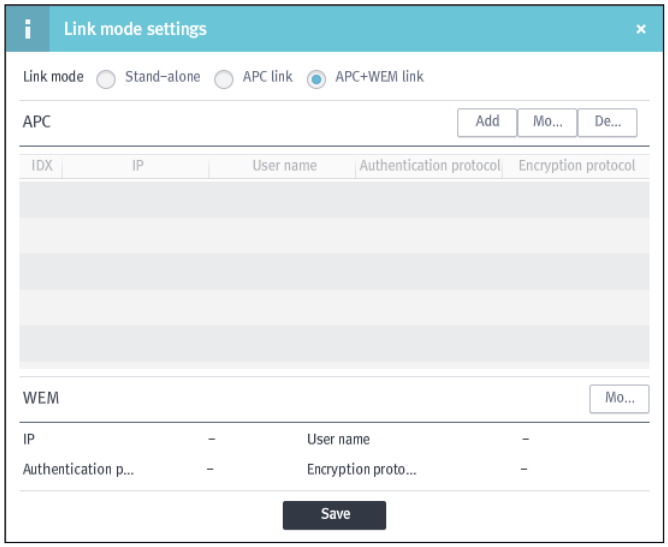


Figure 12. Modify WEM

[Modify]: In the WEM menu, click the **Modify** button near the top. Once the screen for modifying WEM appears, you may select the options of your choice.

From the High Availability menu, you may check the information on the configuration of High Availability.

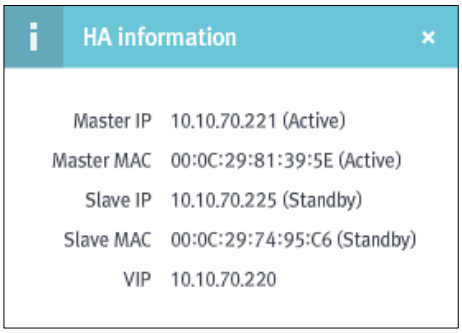


Figure 13. HA information

Figure 14. System settings-Access restriction

Input Item	Description	Effective Value (Default)
IP restricted use	Sets the options for accessible IP use.	Checked/Unchecked (Unchecked)
Accessible IP	Sets the IP address at which to allow access to console.	1.1.1.1~255.255.255.255 (None)
Automatic logout	In case you don't use the console, it set the automatic logout time. -When there is no activity for the predefined time, you will be automatically logged out.	1/3/5/10 minutes (5)
The number of allowable failed logins	Sets the number of password attempts allowed.	1~5 (5)

NOTE

In the case where the number of failed logins to a server surpasses the allowable value, different methods of processing failed authentication will be applied to the different levels of authority of each administrator.

- Root administrator: After an authentication delay of 5 minutes, the delay of authentication will be applied at every failed attempt
- Supervising administrator / Senior administrator / administrator: Account lockout

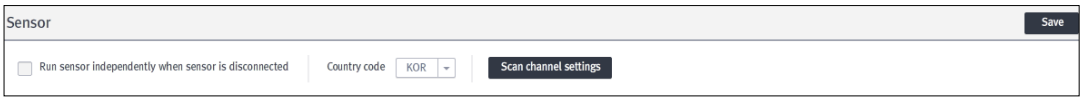


Figure 15. System settings-Sensor

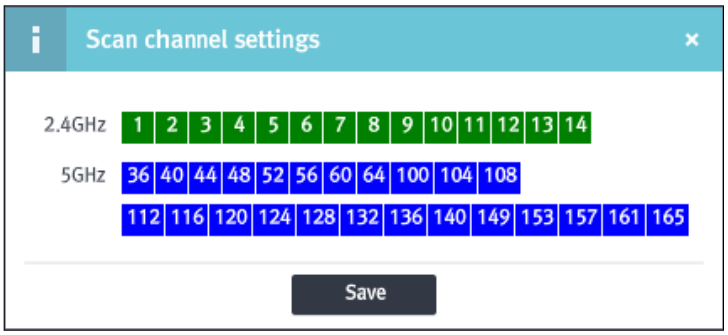


Figure 16. Scan channel settings

Input Item	Description	Effective Value (Default)
Run sensor independently when sensor is disconnected	In case of disconnection to a server, it sets the option for activating a sensor independently.	Checked/Unchecked (Unchecked)
Country code	Sets the country code of a sensor −Since the wireless channel which an AP uses is different for each country, the setting of a sensor for detection is additionally required.	KOR/USA/EU (KOR)
Scan Channel Settings	Sets the wireless channel to be scanned.	-

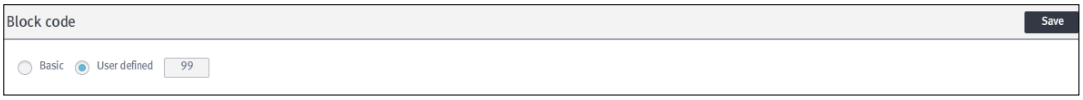


Figure 17. System settings-Block code

Input Item	Description	Effective Value (Default)
Block Code	Sets the code number to be used in block packet.	Basic/User defined(Basic)

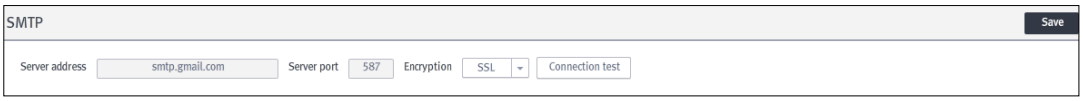


Figure 18. System settings-SMTP Server

Input Item	Description	Effective Value (Default)
Server address	Sets the IP address of a mail server.	1 to 50 characters (None)
Server Port	Sets the port number of a mail server.	Number 1~65535 (25)
Encryption	Sets the encryption method for communication with a mail server.	OPEN / TLS / SSL (TLS)
Connection Test	Performs the connection test to the mail server.	

NOTE

When you register the mail server, the warning email will be automatically sent to the root administrator in case errors appear in integrity test during the operation of a server or there are problems related to disk quotas. In the case of reports for processing results for each event, emails will be transferred between administrators at their discretion.

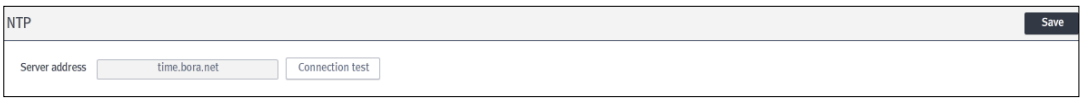


Figure 19. System settings-NTP Server

Input Item	Description	Effective Value (Default)
Server address	Sets the NTP server address for providing the information reliably and on time.	1 ~ 50 characters (time.bora.net)

Connection Test	Performs the connection test to the NTP server.	-

NOTE

When you register the NTP server, it implements the time synchronization with the NTP server at 00 every day.

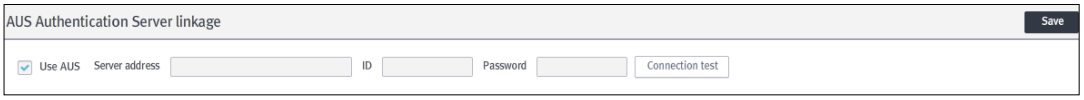


Figure 20. System settings-AUS Authentication Server linkage

Input Item	Description	Effective Value (Default)
use AUS	Sets the option for synchronizing with Anyclick AUS, which is the wireless authentication system. **− When you set the synchronized use, it fetches the account information on an hourly basis.**	Checked/Unchecked (Unchecked)
Server address	Sets the IP address of Anyclick AUS for synchronization.	0.0.0.0~255.255.255.255 (None)
ID	Sets the ID for connecting to the DB of Anyclick AUS for synchronization.	1~15 characters (None)
Password	Sets the Password for connecting to the DB of Anyclick AUS for synchronization.	1~15 characters (None)
Connection Test	Performs the connection test to the Wireless Authentication Server.	-

NOTE

In the case where the synchronization with Anyclick AUS (made by UNETsystem INC.), which is the wireless LAN authentication system, is set up, it retrieves the user information (MAC info, EAPID) registered in AUS every hour to save it in the reference DB. The WES server compares the MAC address of the detected station with the user account information in the reference DB to fetch and print out the user account information (EAPID) at the MAC address corresponding to that in the on-screen station.

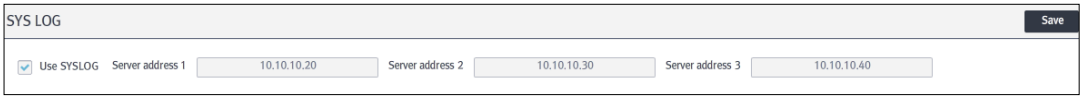


Figure 21. System settings-SYSLOG server

Input Item	Description	Effective Value (Default)
SYSLOG use	Sets the option for synchronization with the external SYSLOG server.	Checked/Unchecked (Unchecked)
SYSLOG Server address 1~3	Inputs the SYSLOG server address.	1.1.1.1~255.255.255.255 (None)

Figure 22. System settings-SNMP

Input Item	Description	Effective Value (Default)
sysname	Sets the name of the SNMP server.	-
syslocation	Sets the location of the SNMP server.	-
syscontact	Sets the password for connecting the SNMP server.	-

2.2.2 Log Settings

WES generates numerous logs during operation. Logs accumulated for an extended period of time may cause a lack of free disk space in the system. In order to cope with this situation, WES provides the automatic cleaning function for old logs and the function of setting up the threshold depending on the used disk space.

Preferences > Log settings

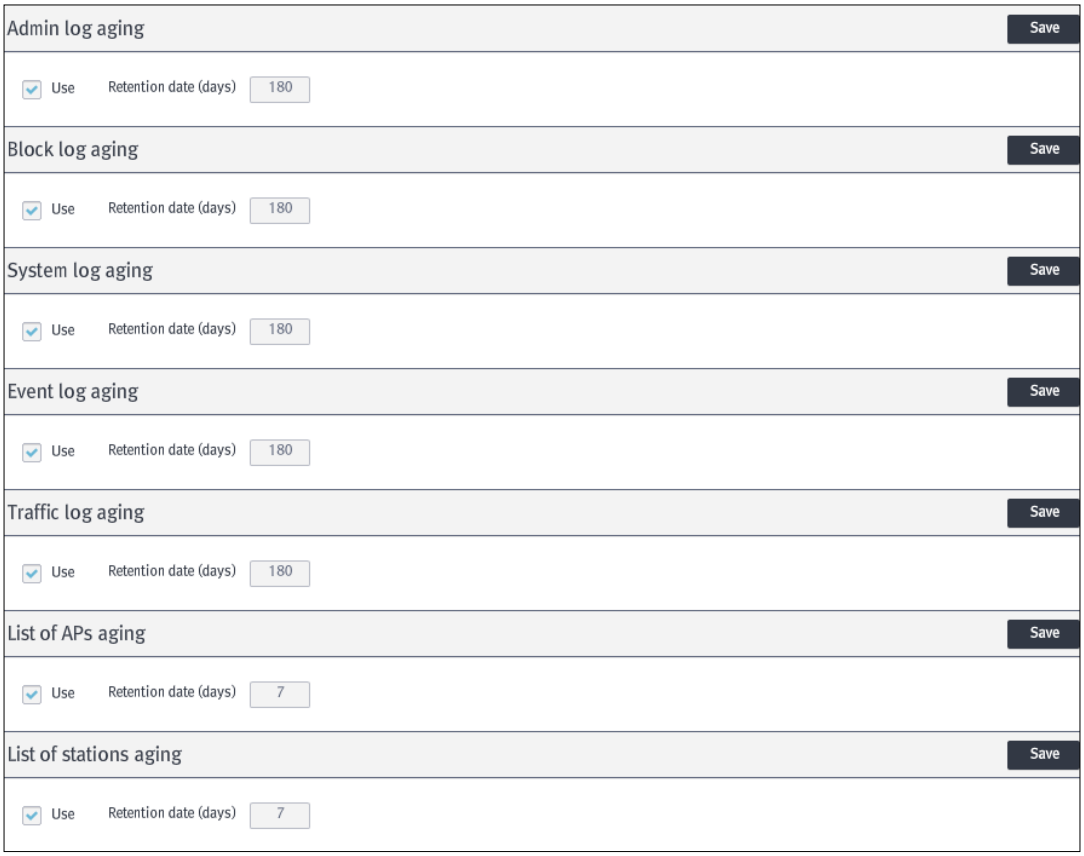


Figure 23. Log settings-Aging

Input Item	Description	Effective Value (Default)
Admin log Aging	Sets the options for the automatic deletion of admin logs.	Checked/Unchecked

		(Checked)
Retention date (days)	Sets the retention period for admin logs.	1~365 (180)
Block log Aging	Sets the options for the automatic deletion of block logs.	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for block logs.	1~365 (180)
System log Aging	Sets the options for the automatic deletion of system logs	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for system logs.	1~365 (180)
Event log Aging	Sets the options for the automatic deletion of event logs.	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for event logs.	1~365 (180)
Traffic log Aging	Sets the options for the automatic deletion of traffic logs.	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for traffic logs.	1~365 (180)
List of APs aging	Sets the options for the automatic deletion of List of APs.	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for List of APs.	1~365 (180)
List of station aging	Sets the options for the automatic deletion of Station list.	Checked/Unchecked (Checked)
Retention date (days)	Sets the retention period for Station list.	1~365 (180)

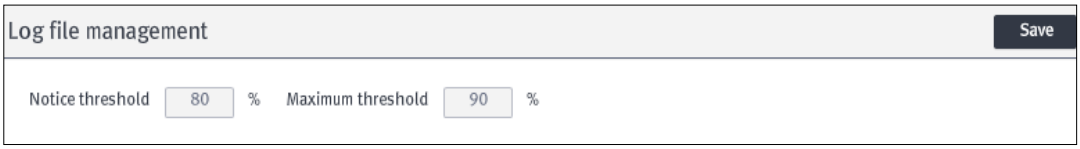


Figure 24. Log file management

Input Item	Description	Effective Value (Default)
Log file management	Sets the notice threshold for used disk space (threshold of email notifications) and the maximum threshold (threshold for automatic deletion).	1~100 (Notice threshold 80/ Maximum threshold 90)

NOTE

In the case where the used disk space reaches the threshold, a warning email will be sent to the administrator for every hour that the problem persists; if it reaches the maximum threshold, the logs will be automatically deleted, starting with the oldest, in order to save free disk space.

2.2.3 OUI Settings

Mobile/Egg OUI List

WES provides the functions for registering and using an OUI (Organizationally Unique Identifier) of worldwide manufacturers of all network devices.

Preferences > OUI settings > Mobile/Egg OUI List

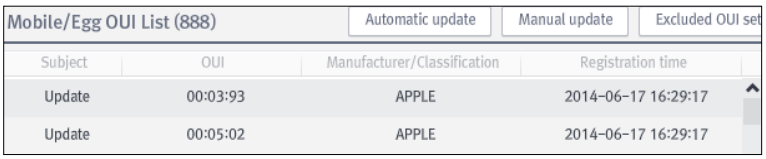


Figure 25. Mobile/Egg OUI List

[Automatic update]: This updates the OUI information automatically by downloading the MAC OUI information from the website.

[Manual update]: In case of restrictions to automatic updates due to some limitations in the environment, you may manually download and update the OUI information from a website for MAC OUI information.

[Excluded OUI settings]: This sets the exception settings for the Mobile OUI to be excluded in OUI updates.

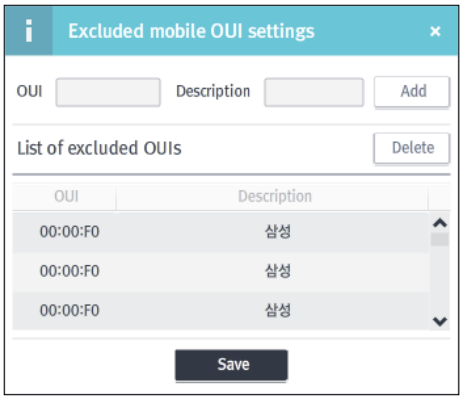


Figure 26. Excluded mobile OUI settings

Input Item	Description	Effective Value (Default)
OUI	Sets the OUIs to be excluded.	1~100 (80/90)
Description	Inputs the description for the OUIs to be excluded.	1~365(180)

When you place the mouse cursor over the **[Manual update]** button, the website address will appear through the tool tips so that you may download the list of MAC OUIs by manufacturer.

Figure 27. Information on MAC OUI download site

NOTE

At http://standards.ieee.org/develop/regauth/oui/public.html, you may download the list of MAC OUIs for the most up-to-date network devices to be updated on a daily basis.

Samsung OUIs

WES provides the list of OUIs for products made by Samsung separately.

Preferences > OUI settings > Samsung MAC List

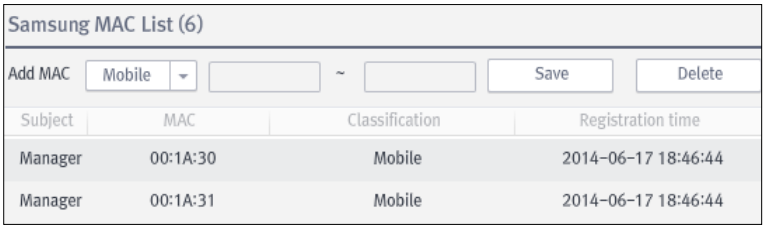


Figure 28. Samsung MAC List

[Type]: Sets the types of OUIs to be added (Mobile / TV).

[Scope]: Adds the OUI with the input of OUI information (1~8 characters, 00:00:00~FF:FF:FF).

[Delete]: After selecting the OUI to be deleted from the list, click the **Delete** button.

2.2.4 The wired switch settings

Additional functions for blocking the wired connection against unauthorized APs orstations will be provided, in addition to the function of blocking the wireless connection by sensors. In order to do so, WES provides the management functions such as Add/Modify/Delete, etc., for the wired switch.

Preferences > Wired switch settings

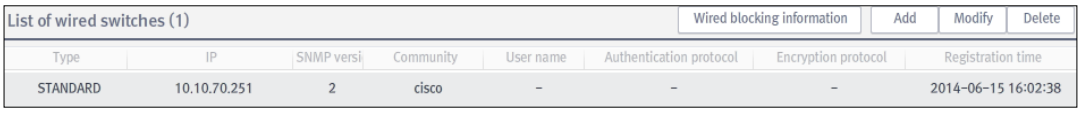


Figure 29. List of wired switches

In order to properly implement the blocking functions with switches, you should register the switches to WES by priority.

Preferences > Wired switch settings > Add

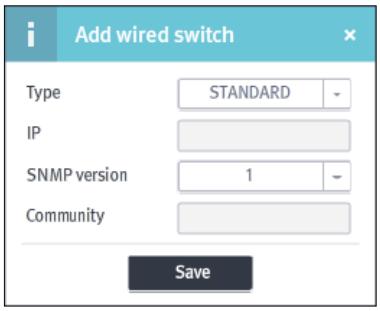


Figure 30. Add wired switch

Input Item	Description	Effective Value (Default)
Type	Sets the types of manufacturers for wired switches.	CISCO/Samsung (CISCO)
IP	Sets the information of IP addresses of the wired switches.	1.1.1.1~255.255.255.255 (None)
SMMP Version	Sets the SNMP version information.	1 ~ 3 (1)
Community	Sets the SNMP Community String value. - used only for 'SNMP version' 1 or 2.	3~15 characters (None)

[Modify]: After selecting the switches to be modified in the list of wired switches, click the **Modify** button at the top. Once the screen for modifying the wired switches is displayed, modify the details.

[Delete]: After selecting the switches to be deleted from the list of wired switches, click the **Delete** button at the top.

2.2.5 DB backup/restoration

WES can save input information on the DB during the operation of a server as a file. This DB contains various kinds of information required for the operation of the server, so you must back it up for secure management.

Preferences > DB backup/restoration

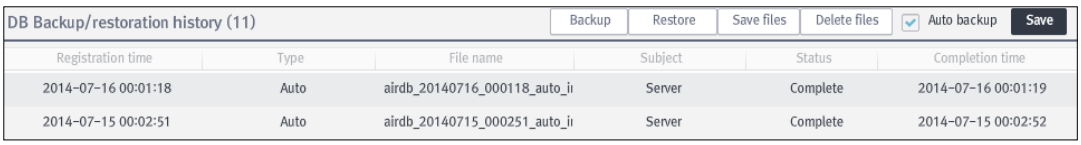


Figure 31. DB backup/restoration history

DB Backup

When you click the **[Backup]** button at the top, the screen for confirming the option of implementing the backup process will be displayed. In the case of a backup, information regarding backups will be registered in the list of tasks.

NOTE

In the case where the **Auto backup** option is selected, incremental backup on a daily basis or full back up on a weekly basis (to be performed every Sunday) will be implemented. In the case of incremental backup, the backup is implemented only for logs; in the case of a full backup, the total data, including logs and server value settings, etc., will be backed up.

In the case of a manual backup, an administrator will implement the backup process manually, which results in the full backup of logs and server value settings, etc.

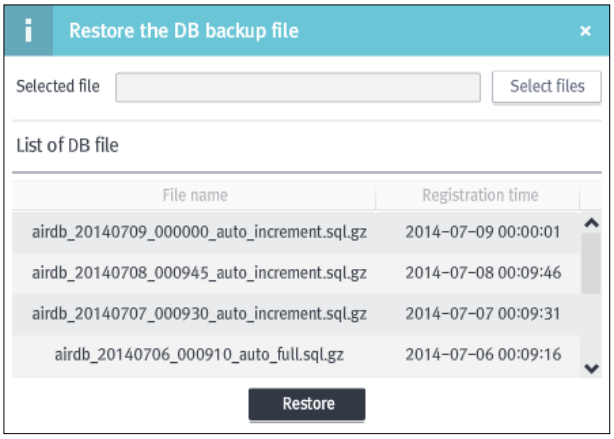
The DB backups saved in the server will be stored for 30 days and then deleted automatically after this retention period. If it is necessary to preserve them for more than 30 days, you should save them separately by using the **Save Backups** function.

After selecting the Auto backup option on the top, click [Save] button to save the settings.

DB Restoration

When you click on the **[Restore]** button at the top, the screen for selecting the DB file to be restored will be displayed. You may restore it by clicking the **[Select files]** button to retrieve the backup file saved in the local PC or may select the backup file to be restored from the list of backup files.

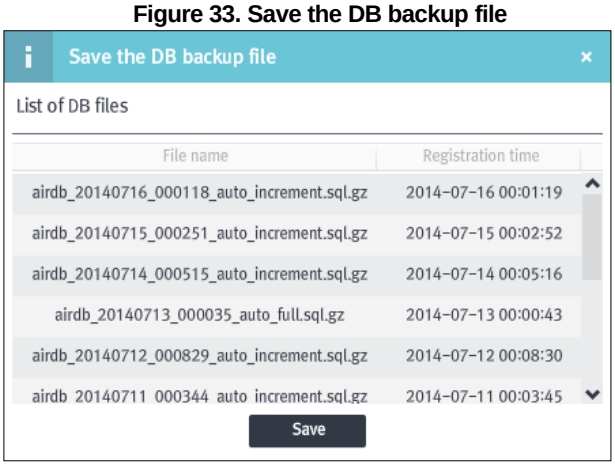
Figure 32. Restore the DB backup file



Save a backup file

When you click the **[Save files]** button at the top, the screen for selecting the backup file will be displayed. After selecting the backup file and click the **[Save]** button, you may download it by specifying the folder patch in your local PC.

Figure 33. Save the DB backup file



Delete a backup file

After selecting the backup file to delete from the DB backup/restoration history, Click **[Delete Files]** on the top to delete the file.

2.3 Managements of equipment and account

This chapter explains the management methods for the devices (sensors, AP, the station connected to AP) to be synchronized with the WES server and accounts.

2.3.1 List of devices

You may make inquiries about active AP, the station, and the list of sensors.

Network > List of devices > List of APs

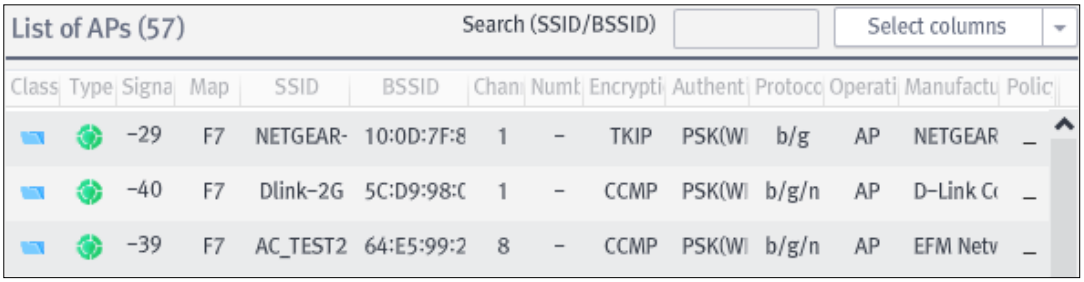


Figure 34. List of APs

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

Network > List of devices > List of stations

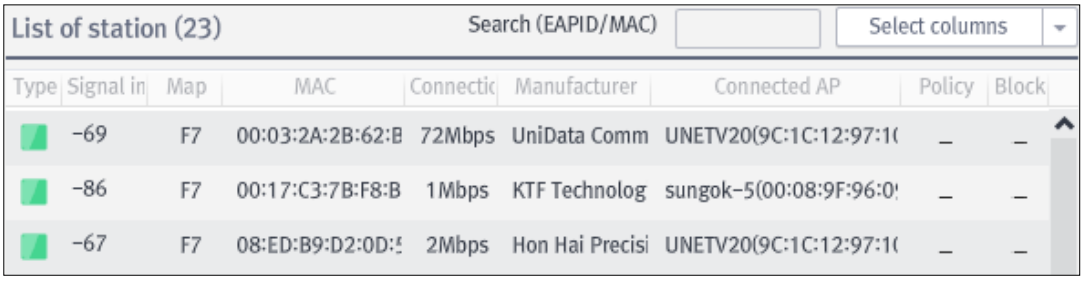


Figure 35. List of stations

[Search]: Makes inquiries about the station by inserting EAPID/MAC (1~17 characters).

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

Network > List of devices > List of sensors

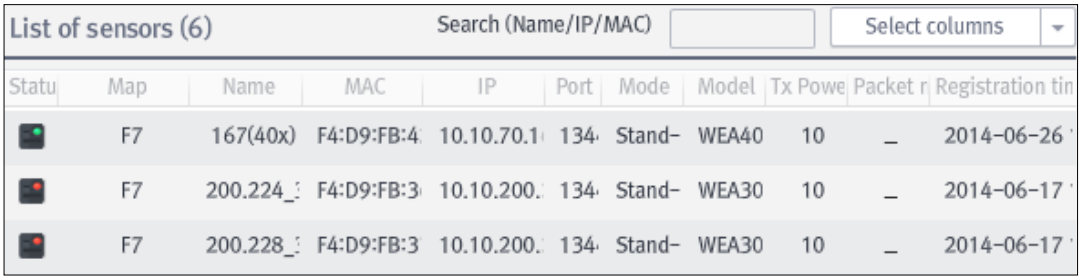


Figure 36. List of sensors

[Search]: Makes inquiries about the sensors by inserting Name/IP/MAC (1~17 characters).

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

2.3.2 AP management

List of APs

You can make inquiries about the list of all the APs detected through the sensors registered in the server.

Network > AP management > List of APs > List of APs

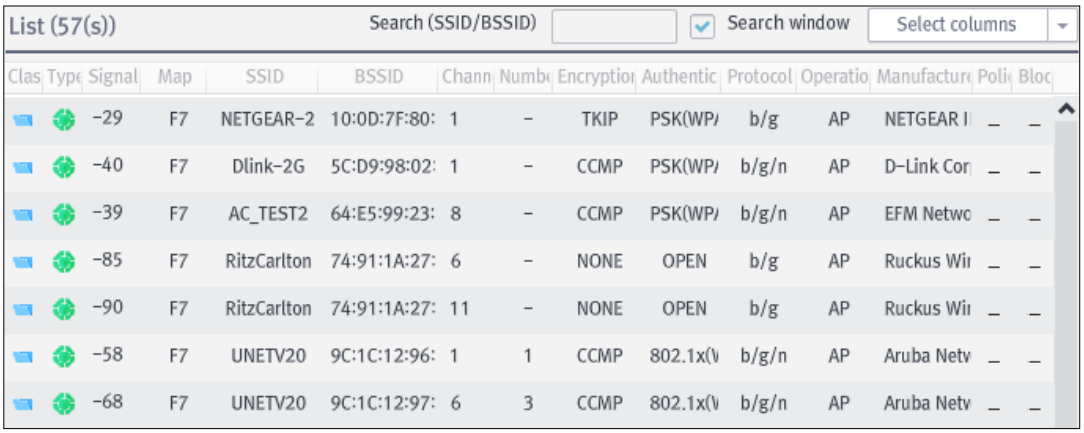


Figure 37. List of APs

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

[Search window]: Selects the option to display the window for inserting search criteria.

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

> **NOTE**
>
> In the list of APs, the list of all APs detected by a sensor will be printed out; the retention period is determined depending on the set values of aging in the list of APs. For instance, if the value of aging in the list of APs is set to 7 days, the list of APs that had been detected up to 7 days before that day would be displayed.
>
> 802.11a and 802.11bg have 20 MHz of bandwidth respectively; 802.11n has 20 MHz of bandwidth or 40 MHz of bandwidth; 802.11ac has 80 MHz of bandwidth or 160 MHz of bandwidth. So, they are classified into 802.11n20 / 802.11n40 and 802.11ac80 / 802.11ac160 to be printed out.

Depending on various search criteria, you may search for the wanted items; the search criteria are as follows:

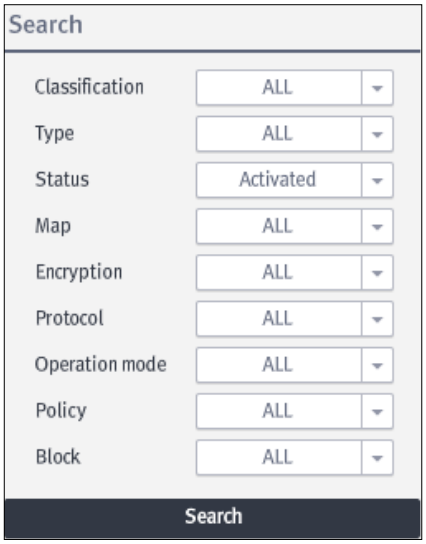


Figure 38. List of APs-Search Criteria

Input Item	Description	Effective Value (Default)
Classification	Selects the status of classification of AP.	Classified/Unclassified (ALL)
Type	Selects the type of APs.	Managed/Unmanaged/External/ Rogue AP (ALL)
Status	Selects whether an AP is activated and in operation.	Activated/Deactivated (ALL)
Map	Selects the location of an AP.	Registered list of map (ALL)
Encryption	Selects the encryption method of an AP.	OPEN/WEP/TKIP/CCMP (ALL)
Protocol	Selects the protocol of an AP.	802.11a,802.11b,802.11b/g, 802.11a/n, 802.11g/n, 802.11b/g/n, 802.11a/n/ac(ALL)
Operation mode	Selects the operation mode in an AP.	Infra/Ad-hoc/WDS/WiFi-Direct (ALL)
Policy	Decides whether an AP violates the policy.	Norma/Violated (ALL)
Block	Decides whether an AP is blocked.	Normal/Blocked (ALL)

The default value of the search criteria is Search (All); in order to search all again, after searching for individual criterion, you should choose ALL for the search criteria.

Summary displays a phi graph for information on the types of APs by default; you may select the 9 types, which include 'Classification, Type, Status, Map, Encryption, Protocol, Operation mode, Policy, and Block.'

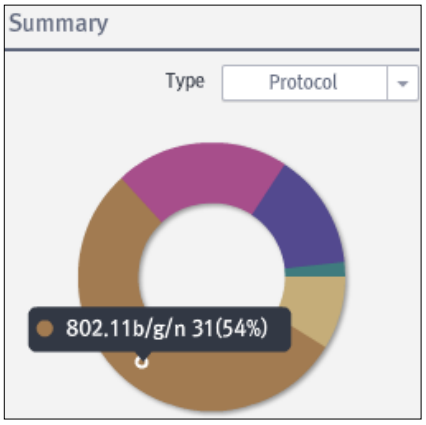


Figure 39. List of APs-Summary

NOTE

WES automatically classifies the AP detected by the sensors into Rogue AP, managed APs, unmanaged APs, and External APs, etc., by putting together various types of information such as signal intensity, location of detection, the status of managed AP register, and the status of connection to wireless devices, etc.

As smart phones are registered as managed APs for WiFi-Direct service, it is impossible to detect such phones with sensors if they can implement WiFi-Direct service for a deauthenticated attempt to connect.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Classification	Prints out the status of classification of the AP. - Classification: Blue, Unclassified: Grey
Type	Prints out the information on the Type of an AP. - Managed APs: Green, Unmanaged APs: Orange, External APs: Grey, Rogue AP: Red/ Common: For EGG, the icon is marked as E; for mobile devices, it is marked as M; in the case of disconnection, it is marked as X.
Signal intensity	Prints out the information on the signal intensity of an AP.
Map	Prints out the information on the location of an AP.
SSID	Prints out the information on the SSID of an AP.
BSSID	Prints out the information on the BSSID of an AP.
Channel	Prints out the information on the channel of an AP.
Number of station	Prints out the number of stations connected to an AP.
Encryption	Prints out the information on the encryption method of an AP.
Authentication	Prints out the information on the authentication method of an AP.
Protocol	Prints out the information on the protocol of an AP.
Operation mode	Prints out the information on the operation mode of an AP.
Manufacturer	Prints out the information on the manufacturer of an AP.
Policy	Prints out the information on the status of an AP and whether it violates the policy.
Block	Prints out the information on the status of an AP and whether it is blocked.

[CSV Import]: Saves the output status in the form of a CSV file to the local PC by specifying the path.

[Refresh]: Updates the list of connected station.

When you double-click on a particular AP in the list of APs, you may view the AP information. For details on the registered AP, **please refer to section 2.3.2 'AP management' for AP information.**

AP classification

WES provides the functions for manual classification/automatic classification of APs detected by the sensors.

Network > AP management > List of APs > AP classification

Figure 40. AP classification-Unclassified APs

[Operation]: Makes inquiries about the AP by selecting Operating information (Active/ALL).

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out the information on the Type of AP. - Managed APs: Green, Unmanaged APs: Orange, External APs: Grey, Rogue AP: Red/ Common: For EGG, it is marked as icon E; For mobile devices, it is marked as M; for disconnected devices, it is marked as X.
Map	Prints out the information on the location of an AP.
SSID	Prints out the information on the SSID of an AP.
BSSID	Prints out the information on the BSSID of an AP.
Channel	Prints out the information on the channel of an AP.
Encryption	Prints out the information on the encryption method of an AP.
Authentication	Prints out the information on the authentication method of an AP.
Protocol	Prints out the information on the protocol of an AP.
Operation mode	Prints out the information on the operation mode of AP.
Manufacturer	Prints out the information on the manufacturer of AP.

WES can register and manage the APs to be used as the managed APs within the company. The methods of registering the managed APs include automatic registration by policy, manual registration by an administrator and batch registration by CS files. Also, you may download the list of managed APs registered in a server to the local PC for backup.

Network > AP management > List of APs > AP classification> Managed APs

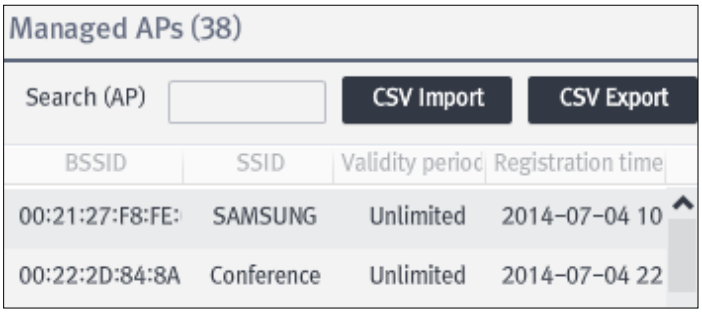


Figure 41. AP classification-Managed APs

[Search]: Makes inquiries about the AP by inserting BSSID (1~17 characters).

[CSV Import]: Retrieves the CSV files with the list of stations and registers them as the list of managed stations all at once.

[CSV Export]: Saves the output status in the form of a CSV file on the local PC by specifying the path.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
BSSID	Prints out the information on the BSSID of an AP.
SSID	Prints out the information on the SSID of an AP.
Validity Period	The validity period of the AP is printed out.
Registration Time	The information on the registration time for the AP is printed out.

There are 4 methods for registering the managed APs by an administrator.
They are as follows:

- First, you may add managed APs by manually inserting their information.

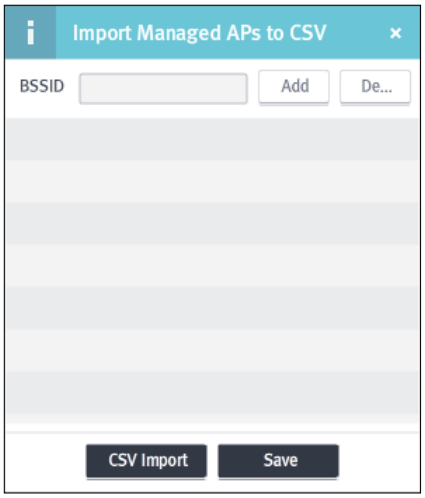


Figure 42. Managed APs-Manual registration

Input Item	Description	Effective Value (Default)
BSSID	Sets the BSSID of the AP.	00:00:00:00:00:00 ~ FF:FF:FF:FF:FF:FF (None)

- Second, by clicking the **[CSV Import]** button, you may register them by the CSV file with the list of managed APs all at once.

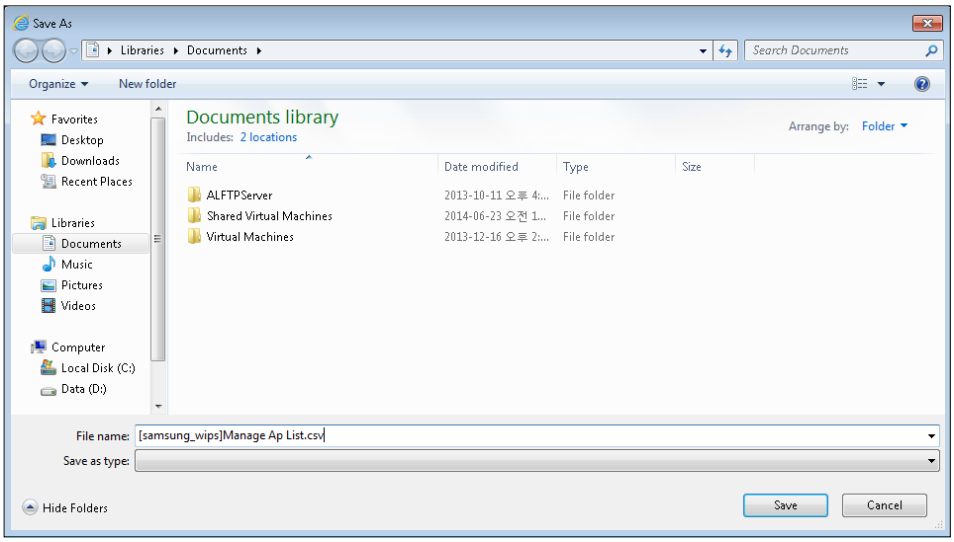


Figure 43. Managed APs-Batch registration

- Third, after selecting the AP to be added to the list of managed APs in the list of unmanaged APs, you may drag it to the list of managed APs while pressing the left button on the mouse.

- Fourth, when you double-click the AP to be classified in each list of the APs, you may view the information on the AP and may set the value of the classified items on the detailed information tab as 'the managed AP's.

There are two kinds of methods for deleting managed APs, which are as follows:

- First, after selecting the managed AP to be deleted from the list of managed APs, you may drag it to the list of unmanaged APs while pressing the left button on the mouse.

- Second, if you may change the classified item on the detailed information tab from the AP information to be displayed by double-clicking on the AP to be deleted from the list of managed APs.

There are two methods for registering Rogue AP and External APs by an administrator, which are as follows:

- First, after selecting a Rogue AP from the list of unmanaged APs, the AP you may want to add from the list of External APs, and drag it to the list of Rogue AP or External AP's while pressing the left button on the mouse.

- Second, if you select the AP, you may want to classify from each list of APs with a double-click. That way, you may view the information on the AP and set the value of classified items on the detailed information tab to 'Rogue AP' or 'External AP.'

There are two methods for deleting Rogue AP/External APs, which are as follows:

- First, after selecting the Rogue AP/External AP from the list of Rogue AP and External APs, respectively, drag it to the list of unmanaged APs while pressing the left button on the mouse.

- Second, change the classified item on the detailed information tab in the AP information to be displayed when you double-click the Rogue AP/External AP and delete it from the list of Rogue APs or External APs.

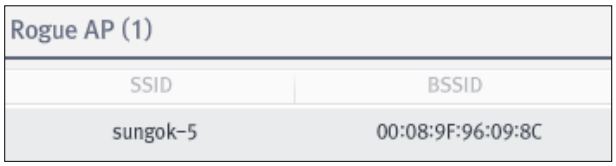


Figure 44. AP classification-Rogue AP

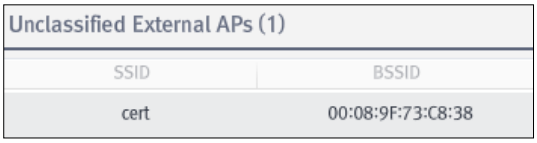


Figure 45. Classification of APs-External APs

NOTE

All the APs detected by sensors at the start-up are unclassified. In case management policy or security policy is set, managed APs, External APs, and Rogue AP are automatically classified;

otherwise, they are manually classified by an administrator. At this time, the manually classified APs are not subject to automatic classification by a server.

For more details, **please refer to section 3.2.1 'Management policy' and section 3.3.4 'Unauthorized APs in Security policy.'**

AP information

When you double-click and select a particular AP in the menu displaying the list of APs, the information on the AP will appear.

From the AP information, you may view Detailed information, Connected stations, Station speed, Policy violations, Block history, Traffic, Location history, and MAP. You may also find detailed information related to the AP from the Detailed information tab.

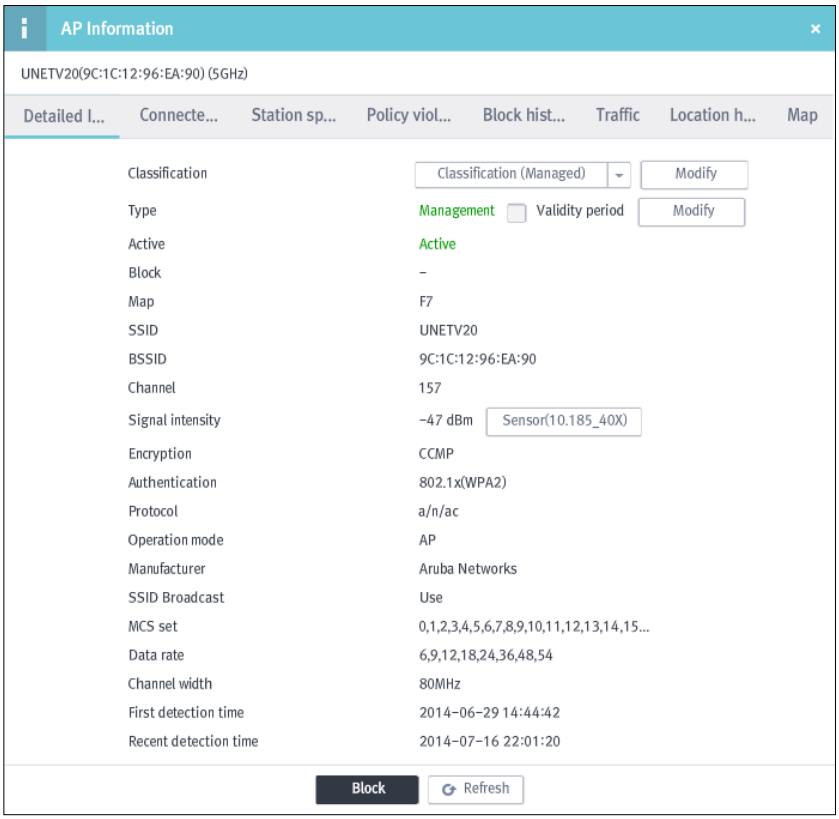


Figure 46. AP information-Detailed information

[Block / Unblock]: Blocks or unblocks the AP.

[Refresh]: Refreshes the AP information.

Output item	Description
Classification	Prints out the status of AP classification; you may set the status of classification manually. (Unclassified / Managed / Rogue AP / External)
Type	Prints out the information on the type of an AP. − Only if the AP is managed can you set the validity period.
Operation	Prints out the status of AP.
Block	Prints out the information on the status of an AP whether it is blocked.
Map	Prints out the information on the map on which an AP is marked.
SSID	Prints out the information on the SSID of an AP.
BSSID	Prints out the information on the BSSID of an AP.
Channel	Prints out the information on the communication channel of an AP.
Signal intensity	Prints out the information on signal intensity and detecting sensors of an AP.
Encryption	Prints out the information on the encryption method of an AP.
Authentication	Prints out the information on the authentication method of an AP.
Protocol	Prints out the information on the protocol of an AP.
Operation mode	Prints out the information on the operation mode to which an AP belongs.
Manufacturer	Prints out the information on the manufacturer of an AP.
SSID Broadcast	Prints out the information on whether an AP uses SSID Broadcast.
MCS set	Prints out the information on the MCS set of an AP.
Data rate	Prints out the data transfer rate of an AP.
Channel width	Prints out the information on the channel bandwidth of an AP.
First detection time	Prints out the information on the time when an AP was first detected by a sensor.
Recent detection time	Prints out the information on the most recent time an AP has been detected by a sensor.

From the Connected stations tab, you may view the history of previous connection and the information on the currently connected station; you are also able to set the options for blocking the station.

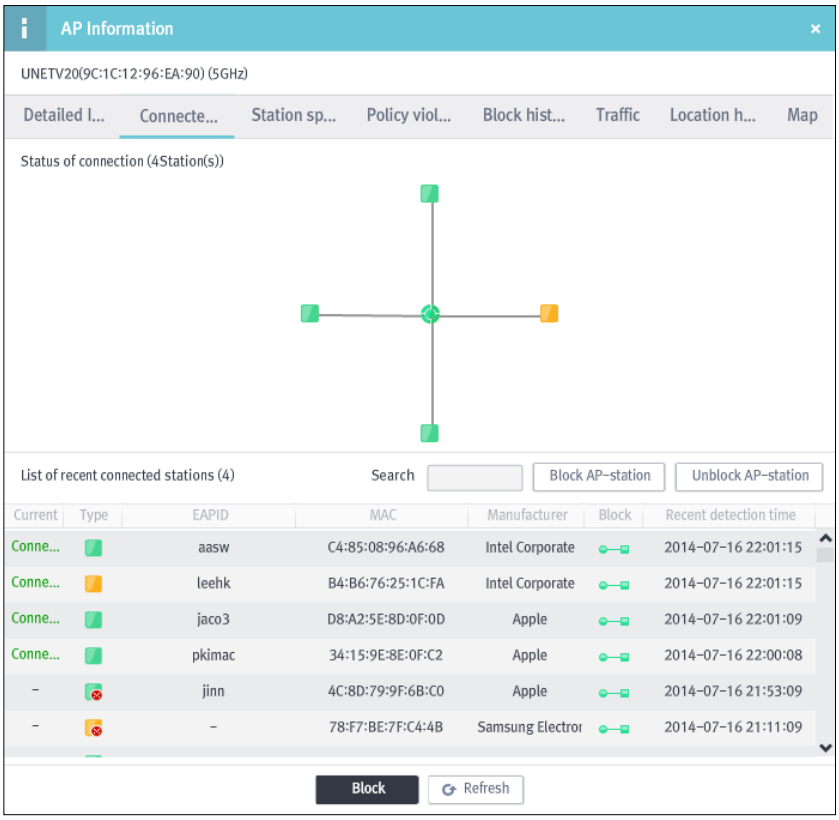


Figure 47. AP information-Connected stations

[Search]: Makes inquiries about the connected stations by inserting EAPID/MAC (1~17 characters).

[Block AP-Station]: Block the AP-Station connection.

[Unblock AP-Station]: Unblock the AP-Station connection.

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

The results of inquiries are displayed as follows, and each item can be sorted in consecutive (ascending or descending) order.

Output item	Description
Current status	Prints out the information on the current status of connection.
Type	Prints out the information on the connection status of stations connected to the APs. − Managed station: Green, unmanaged stations: Orange/Common conditions: for mobile devices, they are marked as icon M; for unconnected station, they are marked as icon X.
EAPID	Prints out the information on EAPID in the case of users synchronized with Anyclick AUS. − If they are not synchronized, no information will be displayed.
MAC	Prints out the MAC address of a station.
Manufacturer	Prints out the information on the manufacturer of a station.
Block	Sets the options for blocking the station. − If you choose to block it, the station will be registered in the Device list to be blocked.
Recent detection time	Prints out the information on the time the station was most recently connected to the AP.

If you double-click a certain station in the list of recent connected stations, you may view the Station information.

From the Station speed tab, you may view the connection speed of the station connected to the AP.

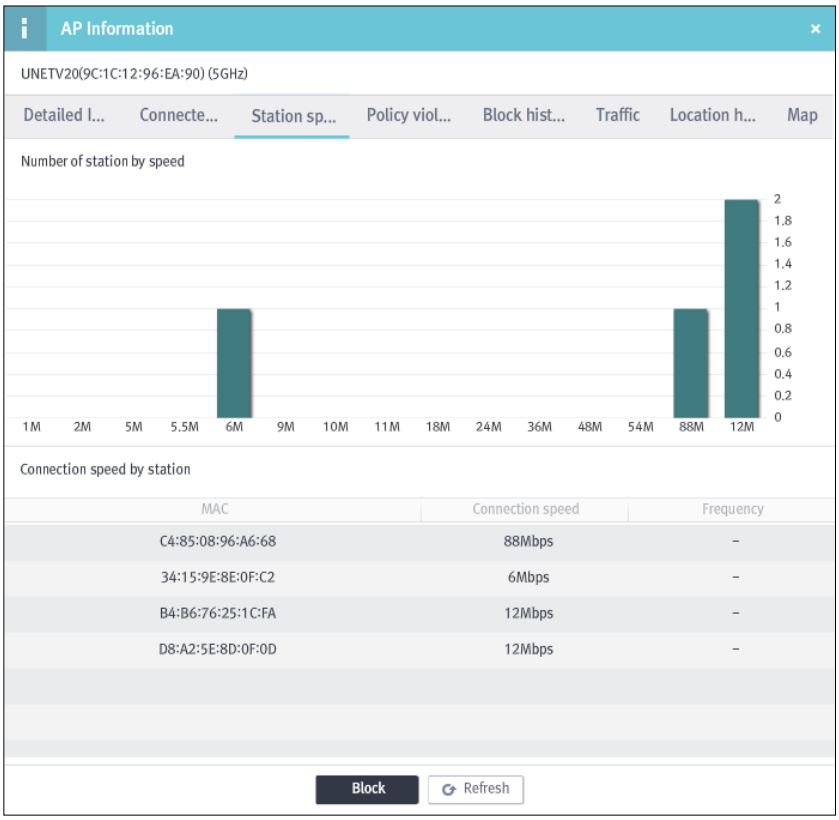


Figure 48. AP information-Station speed

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
MAC address	Prints out the MAC address of a station.
EAPID	Prints out information on the EAPID of users synchronized with Anyclick AUS. - If they are not synchronized, no information will be displayed.
Connection speed	Prints out the information on the connection speed of a station.
Frequency	Prints out the information on the frequency of the AP connected to a station.

If you double-click a certain station in the list of connection speed by station, you may view Station information.

From the Policy violations tab, you may view the policy violations information of the AP.

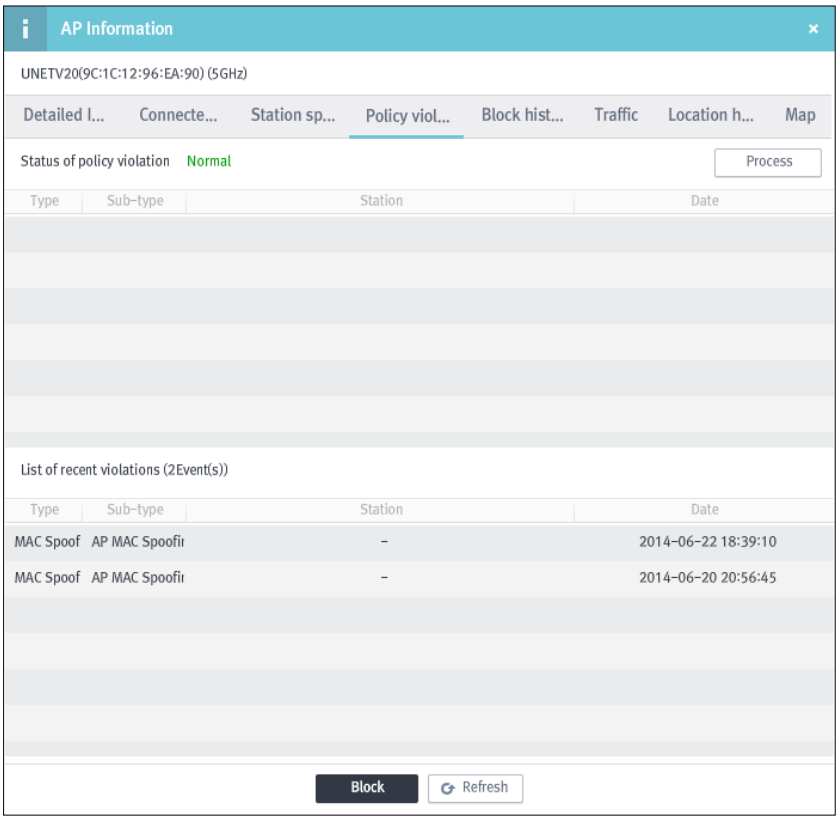


Figure 49. AP information-Policy violations

[Process]: Changes the status of the selected event to 'processed' status.

The results of inquiries are displayed as follows, and each item can be sorted in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out the information on the type of policy violation.
Sub-type	Prints out the information on the sub-type of policy violation.
Station	Prints out the information on the user name of stations connected to the AP/EAPID/MAC.
Time	Prints out the time of a policy violation.

If you double-click a certain event in the status of violations and the list of recent violations, you may view the Event information.

From the Block history tab, you may view information on the status or history of blocking an AP.

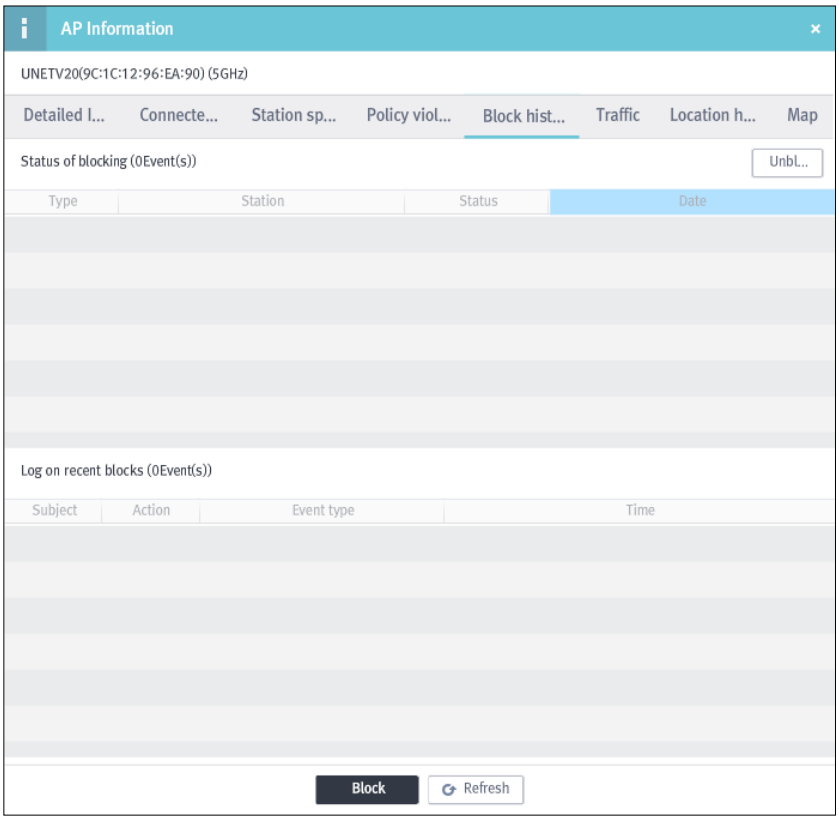


Figure 50. AP information-Block history

From the item for Status of blocking, you may view information on the status of blocking an AP.

[Unblock]: Unblocks the selected Device.

From the item for log on recent blocks, you may view the history of blocking an AP.

From the Traffic tab, you may view the volume of traffic transferred in the station connected to the AP.

Figure 51. AP information-Traffic

The total volume of traffic is printed out in a form of bar graph; if you place the mouse cursor over each section, you may view the traffic volume by station at a specified time.

If you double-click a particular section on the graph, you may view the Station information.

From the Location history tab, you may view the record of detecting the locations of an AP.

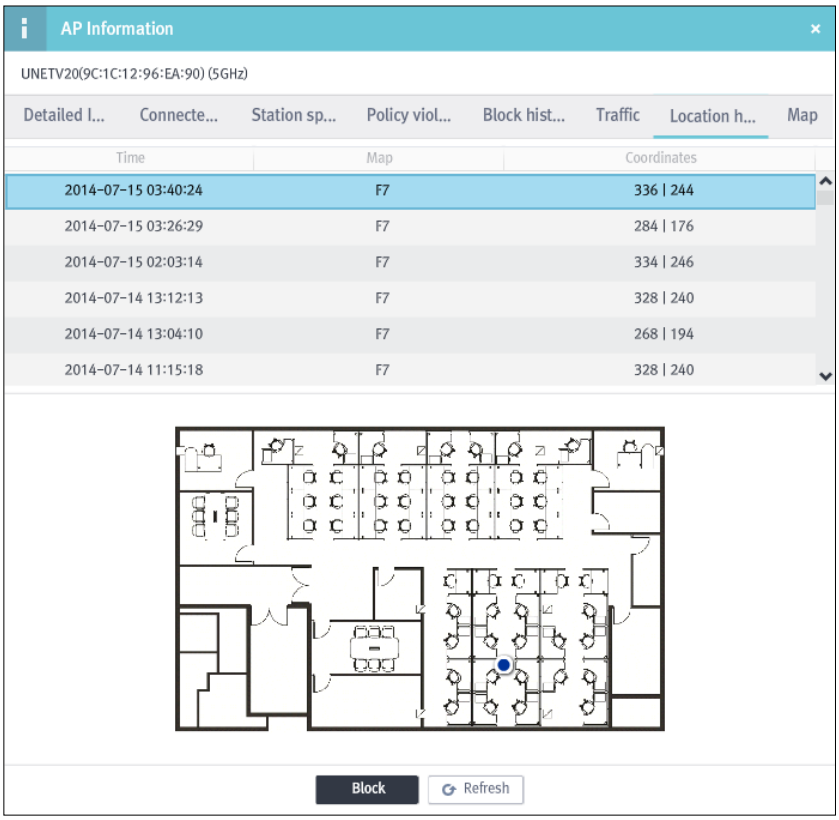


Figure 52. AP information-Location history

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Time	Prints out the information on the time when an AP is detected.
Map	Prints out the information on the map where an AP is detected.
Coordinates	Prints out the information on the coordinates indicating where an AP is detected.

From the Map tab, you may view the location of the AP on the map.

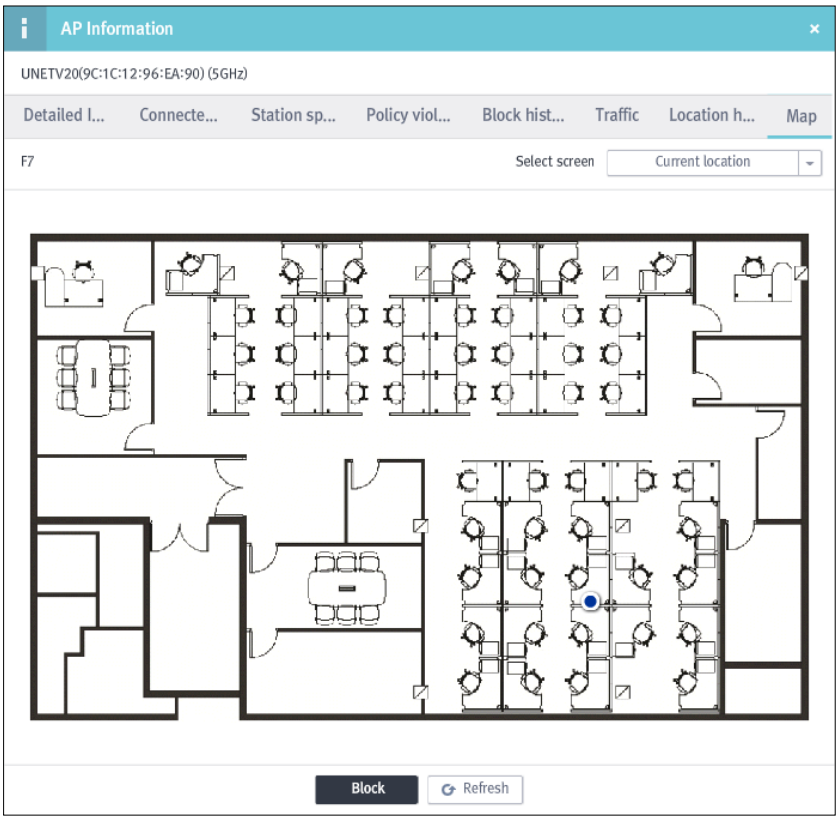


Figure 53. AP information-Map

Output item	Description
Current location	Puts together the results of estimated locations to produce the most reliable data.
Real-time location	Prints out the real-time location of the AP detected by each sensor.

2.3.3 Station Management

List of stations

You can check the information on the final connection for all stations detected by sensors.

Network > Station management > List of stations

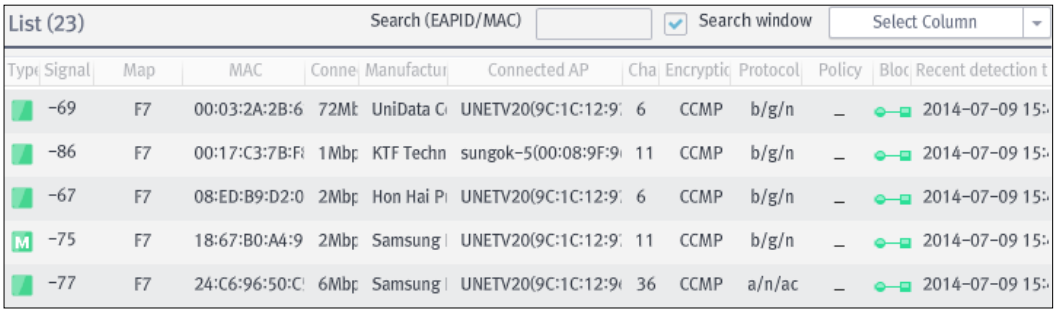


Figure 54. List of stations

[Search]: Makes inquiries about the AP by inserting EAPID/MAC (1~17 characters).

[Search window]: Selects the option to display the window for inserting search criteria.

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

> **NOTE**
>
> For the period specified in the aging of the list of stations, the information on the latest connection of the currently connected stations will be displayed. For example, if the aging in the list of stations is specified as 7 days, the list of stations which have been connected for 7 days up to the present date will be displayed. However, in the case of managed stations, regardless of the setting of aging in the list of stations, the information on the latest connection of all managed stations will be displayed.

Depending on various search criteria you may search for the item as you wish; the search criteria are as follows:

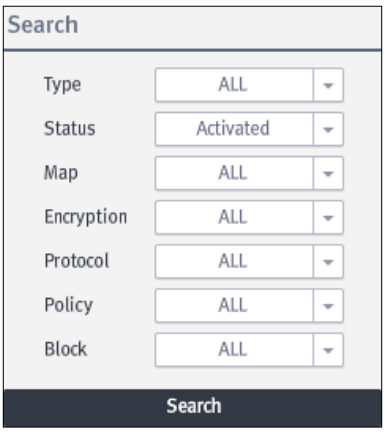


Figure 55. List of stations-By search criteria

Input Item	Description	Effective Value (Default)
Type	Selects the options for managing the stations.	Managed/Unmanaged (ALL)
Status	Selects the options for activating the stations.	Activated/Deactivated (ALL)
Map	Selects the locations of stations.	Registered list of map (ALL)
Encryption	Selects the encryption method of the stations.	OPEN/WEP/TKIP/CCMP (ALL)
Protocol	Selects the protocol of the stations.	802.11a,802.11b,802.11b/g, 802.11a/n, 802.11g/n, 802.11b/g/n, 802.11a/n/ac (ALL)
Policy	Selects the options for policy violations of the stations.	Normal/Violated (ALL)
Block	Selects the options for blocking the stations.	Normal/Blocked (ALL)

The default value of the search criteria is Search (All); in order to search all again, after searching for individual criterion, you should choose ALL for the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out the information on the type of station. - Managed stations: Green, Unmanaged stations: Orange, Exceptional stations: Grey/ Common conditions: For mobile devices, they are marked with icon M.
Signal intensity	Prints out the information on the signal intensity of a station.
Map	Prints out the information on the location of a station.
EAPID	Prints out the information on the EAPID of the station.
MAC	Prints out the information on the MAC address of a station.
Connection speed	Prints out the information on the connection speed of a station.
Manufacturer	Prints out the information on the manufacturer of a station.
Connected AP	Prints out the information on the AP a station is connected to.
Channel	Prints out the information on the channel of a station.
Encryption	Prints out the information on the encryption method of a station.
Protocol	Prints out the protocol of a station.
Policy	Prints out the information on the policy violations of a station.
Block	Prints out the information on the status of a station.
Recent detection time	Prints out the information on the recent connection time of a station.

[Refresh]: Updates the list of connected stations.

If you select and double-click a particular station in the list of the connected station, you may view the registered information on the station.
For more details, **please refer to section 2.3.3 'Station management' for the station information**.

Station classification

WES may check the station connected to all APs detected by sensors. By doing so, it may block stations which may cause security problems.

Network > Station management > Station classification > Unmanaged stations

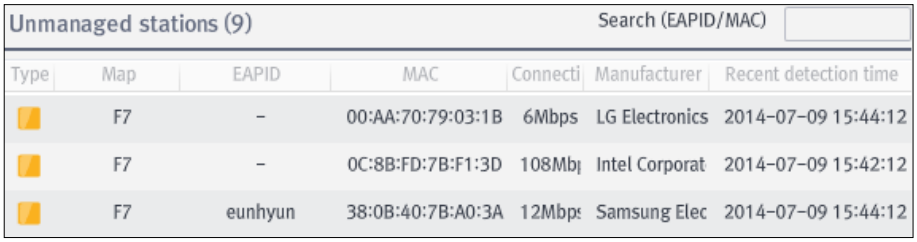


Figure 56. Unmanaged Stations

[Search]: Makes inquires about the AP by inserting EAPID/MAC (1~17 characters).

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out information on the type of stations (whether they are managed).
Map	Prints out the information on the building and floor where the AP is located.
EAPID	Prints out the information on the EAPID of a station.
MAC	Prints out the information on the MAC address of a station.
Connection speed	Prints out the information on the connection speed of a station.
Manufacturer	Prints out the information on the manufacturers of NICs (Network Interface Cards) of the station.
Recent detection time	Prints out the latest time when a station was connected to the AP.

NOTE

In the case where it is synchronized with Anyclick AUS, the information on an EAPID will be displayed as well; otherwise, only the MAC information will be displayed.

WES can manage the station to be used within a company by registering them as managed stations. The methods of registering managed stations include manual registration by an administrator, batch registration by CSV files, and synchronization with the DB. You may also download the list of managed stations registered in a server for backup.

Network > Station management > Station classification > Managed stations

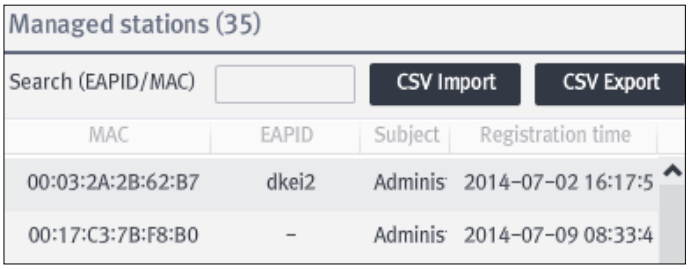


Figure 57. Managed Stations

[Search]: Makes inquiries about the stations by inserting EAPID/MAC (1~17 characters).

[CSV Import]: Retrieves the CSV files with the list of stations and registers them as the list of managed stations all at once.

[CSV Export]: Saves the output status in the form of a CSV file on the local PC by specifying the path.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
MAC address	Prints out the MAC address of the registered station.
EAPID	Prints out information on the EAPID of a station. − If it is synchronized with an Anyclick AUS server, information on the EAPID will be displayed as well; otherwise, only the MAC information will be displayed.
Subject	Prints out information on the subject registering the managed station. - Server: Stations registered automatically by a server, - User: Stations registered manually by an administrator
Registration Time	Prints out the information on the time when a station is registered.

There are two methods for manual registration by an administrator; the details are as follows:

- First, add the managed station by manually inserting the information on the stations.

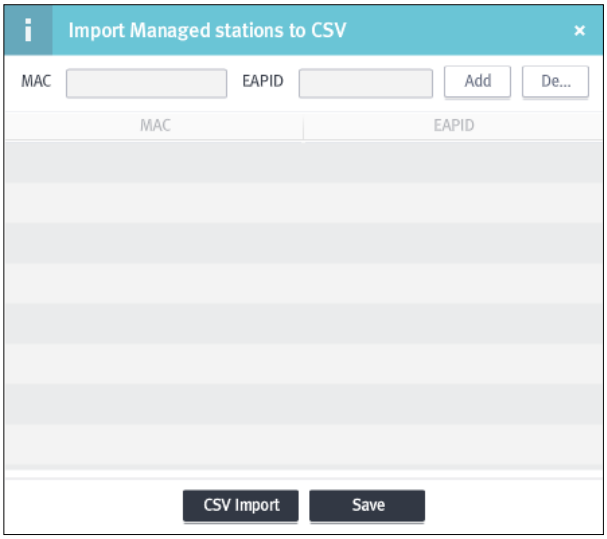


Figure 58. Managed Stations-Manual registration

Input Item	Description	Effective Value (Default)
MAC	Sets the MAC address of a station.	00:00:00:00:00:00~FF:FF:FF:FF:FF:FF (None)
EAPID	Sets the EAPID	1~17 characters (None)

- Second, **by clicking the [CSV Import]** button, you can register them through CSV files with the list of managed stations all at once.

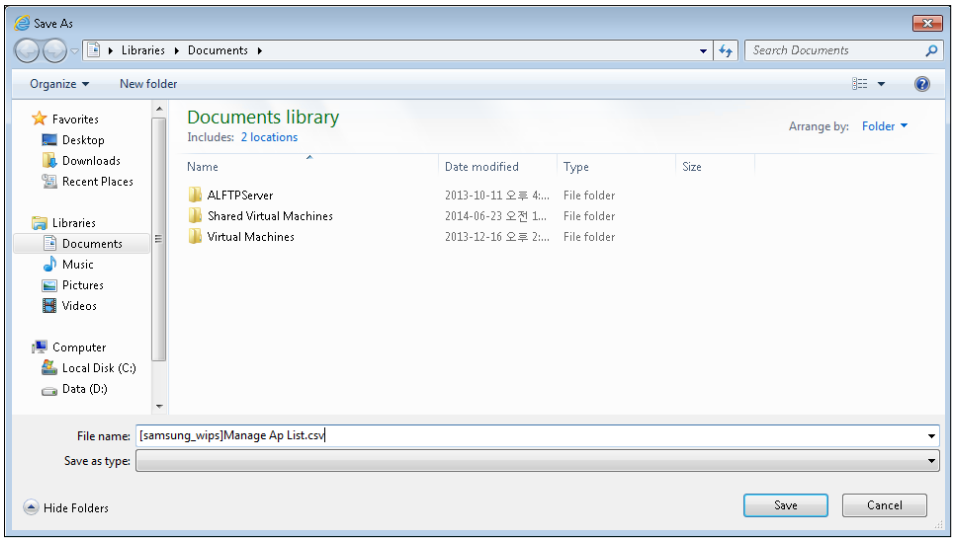


Figure 59. Managed station-Batch registration

- Third, after selecting the station to be added to the list of managed stations from the list of unmanaged stations, drag them to the list of managed stations while pressing the left mouse button.

- Fourth, when you select and double-click the station to be classified in each list of stations, you may view the information on the station; the value of the classified item on the detailed information tab will be set to 'managed stations.'

There are two methods for deleting managed stations; the details are as follows:
- First, after selecting the managed station to be deleted in the list of managed stations, drag them to the list of unmanaged stations while pressing the left mouse button.

- Second, change the classified item on the detailed information tab in the information on the station to be displayed by double-clicking the managed station to be deleted in the list of managed stations.

There are two methods for registering exceptional stations by an administrator; the details are as follows:
- First, after selecting the station to be added to the list of the exceptional stations from the list of unmanaged stations, drag them to the list of exceptional stations while pressing the left mouse button.

- Second, when you select and double-click the station to be classified in each list of station, you may view the information on the station; the value of the classified item on the detailed information tab will be set to 'exception.'

There are two methods for deleting exceptional stations; the details are as follows:
- First, after selecting the exceptional stations to be deleted in the list of exceptional stations drag it to the list of unmanaged stations while pressing the left mouse button.

- Second, change the classified item on the detailed information tab in the information on the AP to be displayed by double-clicking the exceptional stations to be deleted in the list.

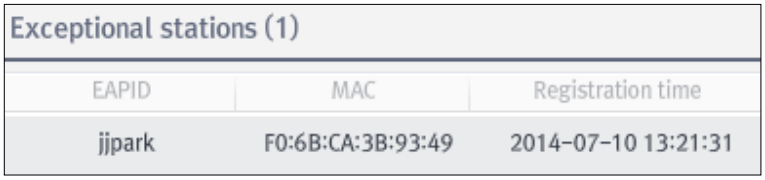


Figure 60. Station classification-Exceptional stations

NOTE

Once the stations are registered to the list of exceptions, even if they violate the security policy within a company, they are not additionally blocked with an alarming notification. This applies to the registration of a temporary user who should use the intra-network for business purposes even if a station is not registered as a managed one.

Station connection history

You may view the records of the connection of all stations detected by sensors.

Network > Station management > Station connection history

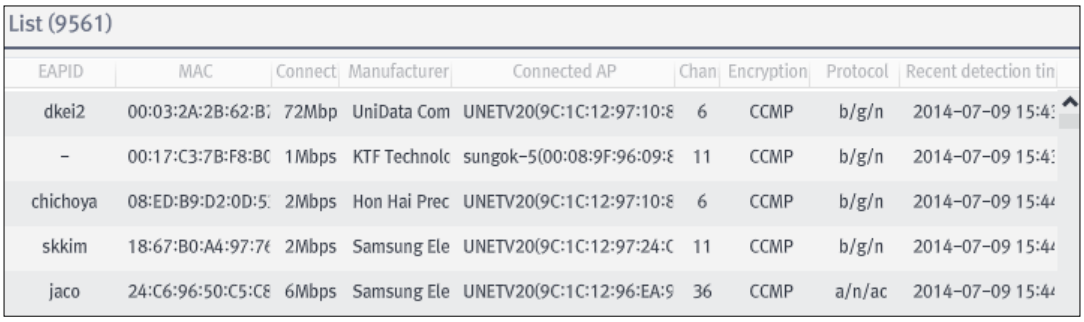


Figure 61. List of connected stations

NOTE

In the **list of' stations**, you may view the currently connected stations; in the **stations connection history**, you may view all stations previously connected. However, if a particular station is connected to only one AP, only the history of connection which has been confirmed most recently can be viewed. For example, if the particular station is connected to AP 'A' on day 1 and connected to AP 'B' on day 2, you may view the history of all connections to A and B; if it is connected to A on day 1 and day 2, you may view only the history of connections for day 2.

Depending on various search criteria you may search for items as you want. The search criteria are as follows:

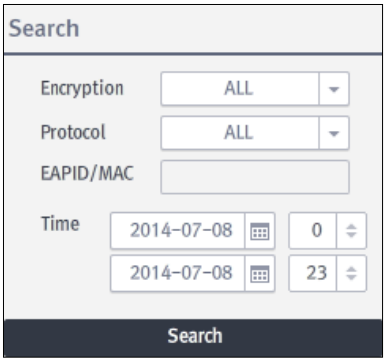


Figure 62. List of connected stations-By search criteria

Input Item	Description	Effective Value (Default)
Encryption	Selects the encryption method of the station.	OPEN/WEP/TKIP/CCMP (ALL)
Protocol	Selects the protocol of the station.	802.11a,802.11b,802.11b/g, 802.11a/n, 802.11g/n, 802.11b/g/n, 802.11a/n/ac(ALL)
EAPID/MAC	Inserts the information on EAPID/MAC.	1~17 characters (None)
Time	Specifies the search period.	Past-Present (Present date)

The default value of the search criteria is Search (All); in order to search all again, after searching for individual criterion, you should choose ALL for the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
EAPID	Prints out the EAPID of the user of the station.
MAC	Prints out the information on the MAC address of a station.
Connection Speed	Prints out the information on the connection speed of a station.
Manufacturer	Prints out the information on the manufacturer of a station.
Connected AP	Prints out the information of the AP to which a station is connected.
Channel	Prints out the information on the channel of a station.
Protocol	Prints out the information on the protocol of a station.
Encryption Method	Prints out the information on the encryption method of a station.
Recent detection time	Prints out the information on the recent detection time of a station.

[Refresh]: Updates the station connection history.

When you select and double-click a particular station in the history of station connections, you may view the registered information of the station.
For more details, **please refer to section 2.3.3 'Station management' for the station information**.

Station information

When you select and double-click a particular station in the list of stations, the registered station information will appear.

From the station information, you may view Detailed information, Connected Aps, Policy violations, Block history, Traffic, and Location history; From the Detailed information tab you may find the specific information related to the station .

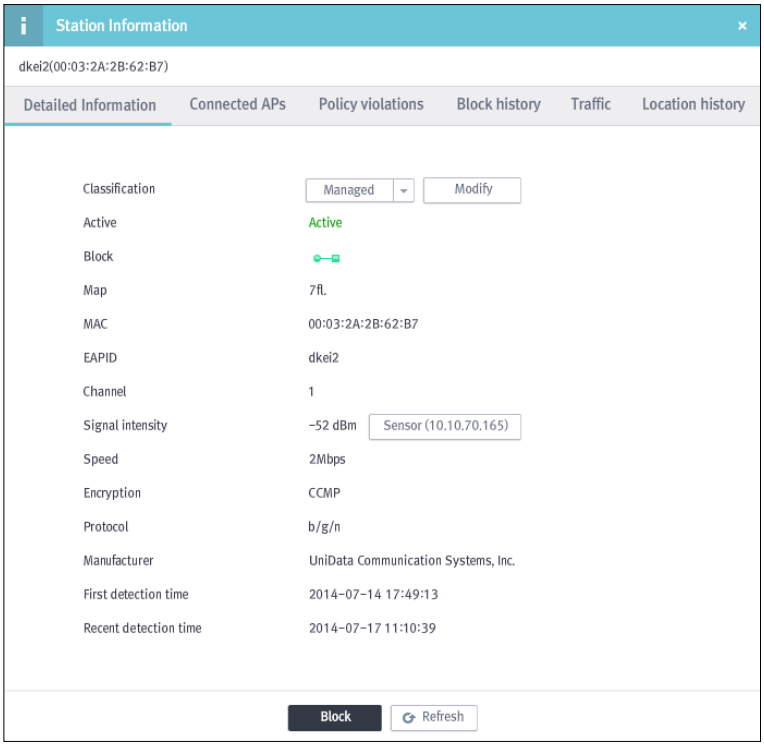


Figure 63. Station information-Detailed information

[Block / Unblock]: Blocks or unblocks the Station.

[Refresh]: Updates the Station information.


NOTE

When you click the [block] button at the bottom of the registered information on the station, you can set the options for blocking the connection of the station to all AP. In the case where it is set to be blocked from connecting to all AP, the information on the connected AP (SSID/BSSID) in the list of blocked stations shows '–(FF:FF:FF:FF:FF:FF)'.

For more details, **please refer to section 2.3.5 'Connection Management' for the station connection management**.

The search results are displayed as follows:

Output item	Description
Classification	Prints out the status of classification of station; you may set the status of classification manually. (Unmanaged/Managed/Exceptional)
Operation	Prints out the status of station.
Block	Prints out the status of blocked station.
Map	Prints out the information on a map marking where the AP is connected to a station.
MAC	Prints out the MAC address of a station.
EAPID	Prints out information on the EAPID in the case of users synchronized with Anyclick AUS. − If they are not synchronized, no information will be displayed.
IP	Prints out the IP address of a station.
Channel	Prints out information on the communication channels of a station.
Signal intensity	Prints out information on the detecting sensors and the signal intensity of a station; you may view the information on the sensors.
Speed	Prints out the information on the speed of a station.
Encryption	Prints out the encryption method of a station.
Protocol	Prints out the protocol of a station.
Frequency	Prints out the information on the frequency of a station.
Manufacturer	Prints out the information on the manufacturer of a station.
First detection time	Prints out the time when a station is first detected by a sensor.
Recent detection time	Prints out the time when a station has been most recently detected by a sensor.

From the Connected APs tab, you may view the history of previous connection and the information on currently connected APs; you can also set the options for blocking the station.

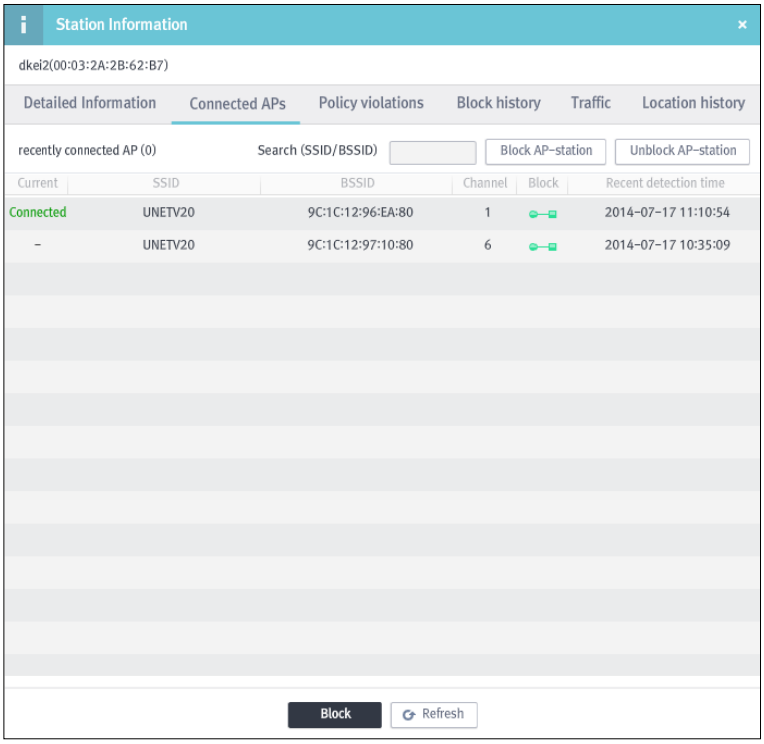


Figure 64. Station information-Connected APs

[Block AP-Station]: Blocks station from connecting to AP.

[Unblock AP-Station]: Allows station to connect to AP.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Current	Prints out information on the status of connection of a station.
SSID	Prints out information on the SSID of the AP a station is connected to.
BSSID	Prints out information on the BSSID of the AP a station is connected to.
Channel	Prints out information on the channel of the AP a station is connected to.
Block	Prints out information on the blocking of a station from connecting to the AP.
Recent detection time	Prints out the latest time when a station was connected to the AP.

If you double-click a certain AP in the list of APs a station was recently connected to, you may view the AP information.

NOTE

When you click the **[Block]** button in the history of a connected AP, you may set the options for blocking the station from connecting to the AP. In the case where you choose to block the

station from connecting to the AP, the information on the AP will be shown in the information on the connected AP (SSID/BSSID) in the list of blocked station. For more details, **please refer to section 2.3.5 'Connection Management' for the station connection management.**

From the Policy violations tab, you may view the policy violations information of the Station.

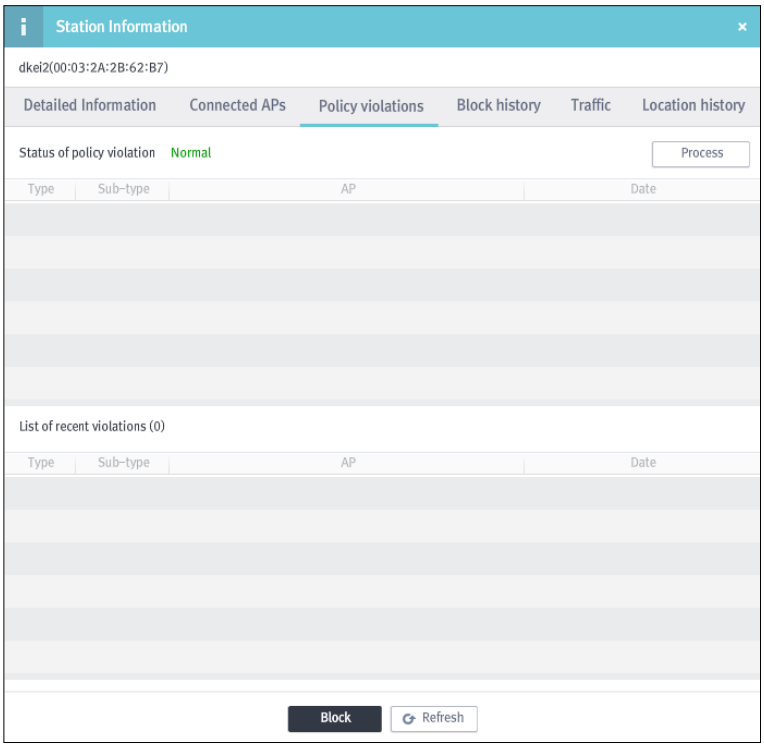


Figure 65. Station information-Policy violations

[Process]: Changes the status of the selected event to 'processed' status.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out information on the type of policy violation.
Sub-type	Prints out information on the sub-type of policy violation.
AP	Prints out information on the SSID/BSSID of the connected AP.
Time	Prints out the time of policy violation.

If you double-click a certain event in the status of violations and the list of recent violations, you may view the Event information.

From the block history tab, you may view information on the status or history of blocking a station.

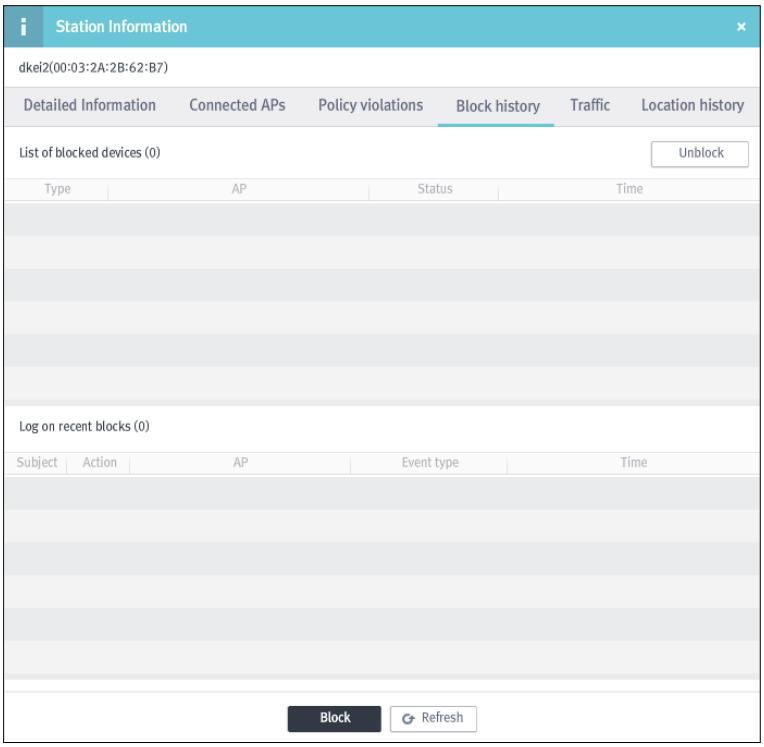


Figure 66. Station information-Block history

From the item for Status of blocking, you may view information on the status of blocking a station.

[Unblock]: Unblocks the selected Device.

From the item for log on recent blocks, you may view the history of blocking a station.

From the traffic tab, you may view the total volume of traffic for the station.

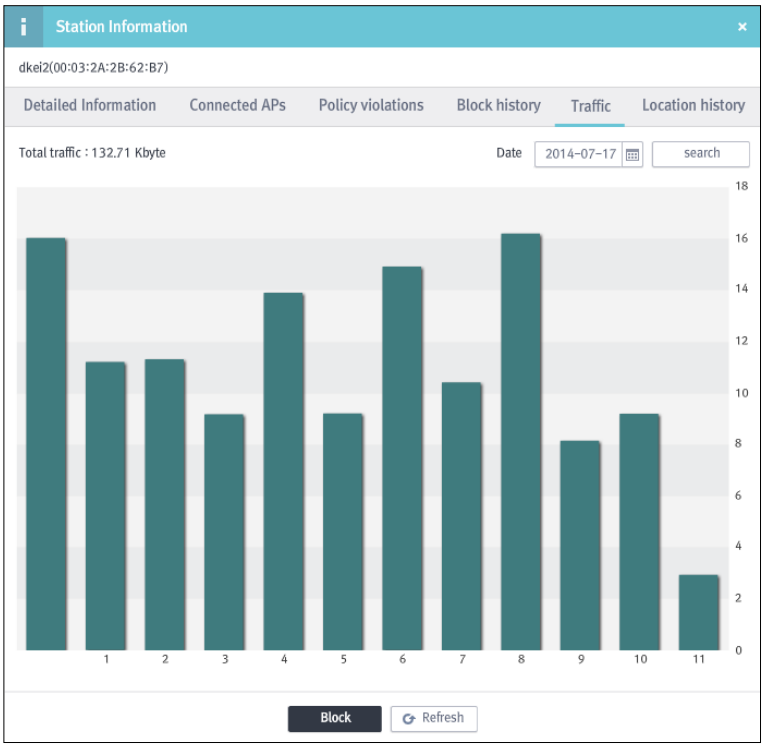


Figure 67. Station information-Traffic

The total volume of traffic is displayed in a bar graph; if you place the mouse cursor over each section, you may view the traffic volume by AP at the designated time.

If you double-click a particular section on the graph, you may view the AP information.

From the Location history tab, you may view the history of the detected locations of the station.

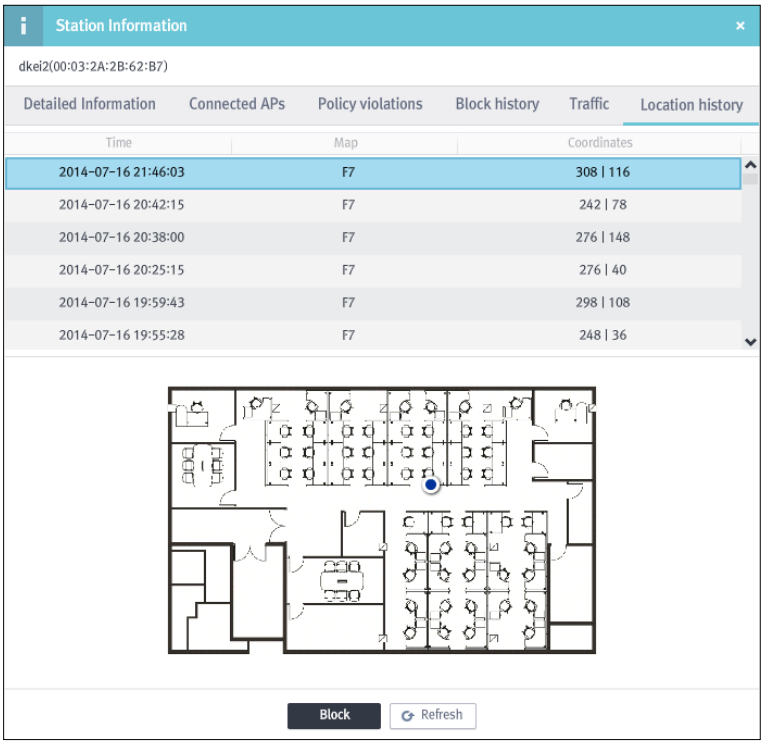


Figure 68. Station information-Location history

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Time	Prints out information on the time when an AP is detected.
Map	Prints out information on the map where an AP is detected.
Coordinates	Prints out information on the coordinates where an AP is detected.

2.3.4 Sensor management

List of sensors

You may make inquiries on all of the lists of sensors registered to a server.

Network > Sensor management > List of sensors

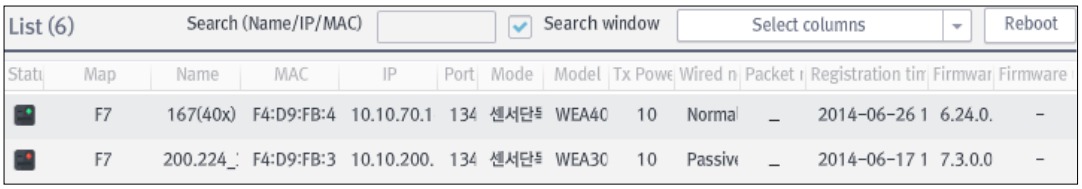


Figure 69. List of sensors

[Search]: Makes inquires about the AP by inserting Name/IP/MAC (1~17 characters).

[Search window]: Selects the option to display the window for inserting search criteria.

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

[Reboot]: Reboots the selected sensor.

Depending on various search criteria, you may search the items as you wish; the search criteria are as follows:

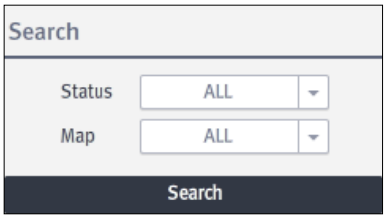


Figure 70. List of sensors-By search criteria

Input Item	Description	Effective Value (Default)
Status	Selects the status of sensors.	Activated/Deactivated (ALL)
Map	Selects information on the location of a sensor.	Location of the registered sensor (ALL)

A **ratio graph** displays the basic information on the types of sensors; the types can be selected among two kinds, ‘Type' or 'Location.’

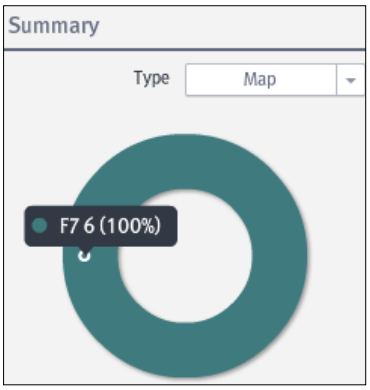


Figure 71. List of sensors-Summary

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Status	Prints out information on the status of a sensor. - Active sensor: Green, Inactive sensor: Red
Map	Prints out information on the map where sensors are located.
Name	Prints out information on the names of the sensors.
MAC	Prints out information on the MAC addresses of the sensors.
IP	Prints out information on the IP addresses of the sensors.
Port	Prints out information on the ports of the sensors.
Mode	Displays the active/inactive mode of a sensor. (Stand-alone sensor type/Sensor + AP integrated type)
Model	Prints out information on the model of a sensor.
TX Power	Sets the output range of transmission of a sensor.
Wired Network Detection Mode	Prints out information on the detection mode of wired networks by a sensor.
Packet Monitoring	Prints out options for performing packet monitoring for each channel in the bandwidth of 2.4 GHz/5 GHz.
Registration Time	Prints out information on the time when a sensor was registered.
Firmware version	Prints out information on the firmware version of a sensor.
Firmware update date	Prints out the date of a firmware update for a sensor.

[Refresh]: Updates the list of sensors.

When you select and double-click a particular sensor in the list of sensors, you may view registered information on the sensor. For more details about the registered information of a sensor, please refer to **section 2.3.4‘Sensors management’ for the information on a sensor.**

APC AP sensor mode settings

If APs are synchronized with APC, the APs registered to an APC may be set and managed as sensors.

Network > Sensor management > List of sensors > APC AP sensor mode settings

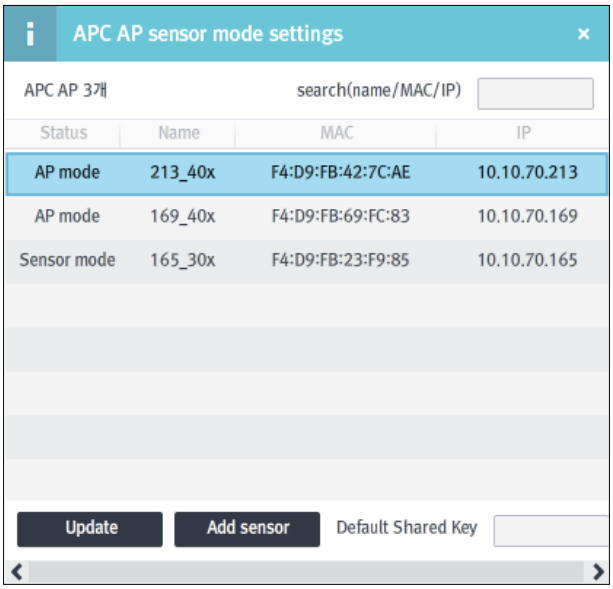


Figure 72. APC AP sensor mode settings

Click the **[Update]** button for updating the list of APs registered to the APC.
For registering an AP as a sensor, click the **[Add sensor]** button after selecting the AP.

[Default Shared Key]: Assign the shared key of the APs added as the sensor.

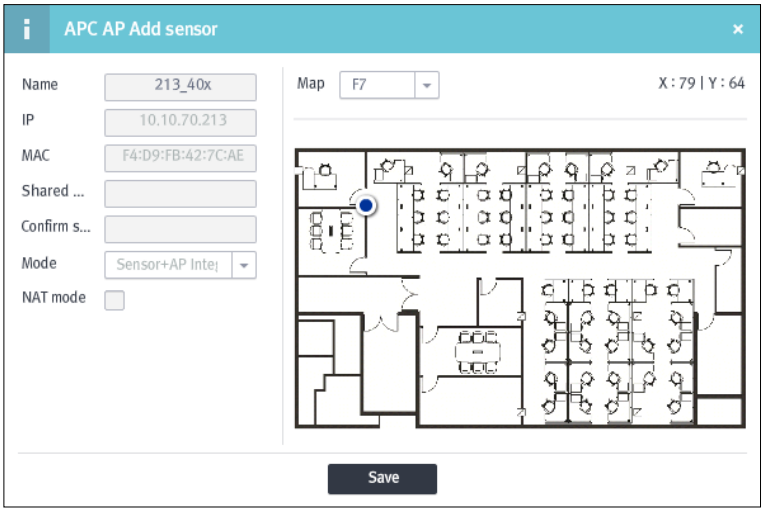


Figure 73. Add APC AP as the sensor

Input Item	Description	Effective Value(Default)
Name	Sets the name of an AP sensor.	3~15 characters (None)
IP	Prints out the IP address of the AP.	-
MAC	Sets the MAC address of a sensor. - Is activated only if the option for NAT mode is selected.	
Shared Key/ Confirm	Sets the password shared with the AP sensor.	3~15 characters(none)
Mode	Prints out the active mode of the AP sensor.	-
NAT Mode	Sets the options for using the NAT mode of the AP sensor.	Checked / Unchecked (Unchecked)
Map	Sets the map where AP sensors are located. - After selecting the map and placing the mouse cursor over the position where sensors are actually located, locate the sensors by clicking the left button of the mouse.	-

NOTE

When the '**Default Shared Key'** is assigned, it will be applied to all APs added as the sensor.
If not assigned, you can assign the shared key by AP.

Sensor settings

Depending on the areas requiring management/the number of AP, it is also necessary to manage the number of required sensors. In order to do so, WES provides management functions such as the addition, modification, and deletion of sensors.

Network > Sensor management > Sensor settings > List of sensors > Add

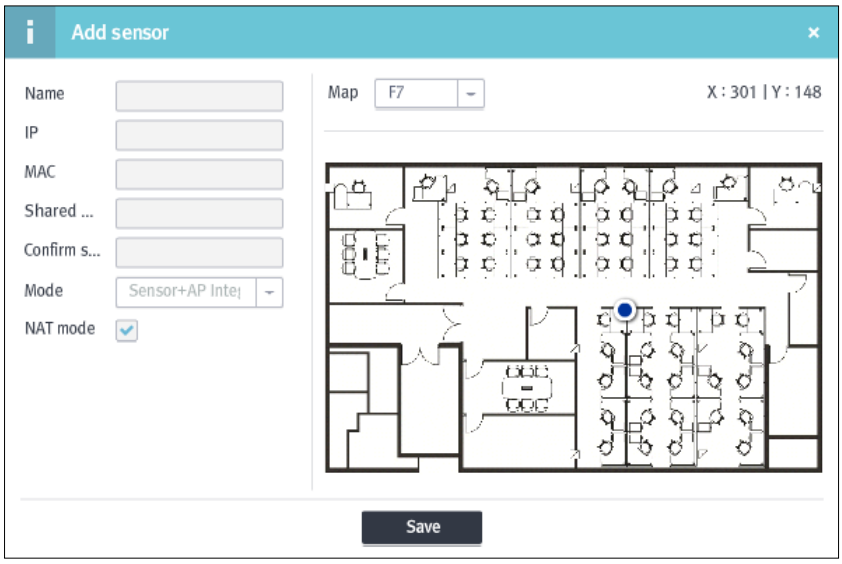


Figure 74. Add sensor

Input Item	Description	Effective Value (Default)
Name	Sets the name of a sensor.	3~15 characters (None)
IP	Sets the IP address of a sensor.	1.1.1.1~255.255.255.255 (None)
MAC	Sets the MAC address of a sensor. - Is activated only if the option for NAT mode is selected.	
Shared Key/ Confirm	Sets the password shared with a sensor.	3~15 characters (None)
Mode	Sets the active mode of AP.	Stand-alone sensor type/ Sensor+AP integrated type (Stand-alone sensor type)
NAT mode	Sets the options for NAT mode in a sensor.	Checked/Unchecked (unchecked)
Map	Sets the map on which a sensor is located. - After selecting a map and placing the mouse cursor over the position where the sensor will actually be located, locate it by clicking the left button of the mouse.	-

[Modify]: After selecting the sensor to be modified in the list of sensors, click the **Modify** button at the top. Once the screen for modifying the sensor appears, modify the details as you want. In the case of modifying the location of a sensor, you may change it by moving the mouse cursor over to the new location and clicking the left button of the mouse.

[Delete]: After selecting the sensor to be deleted from the list of sensors, click the **Delete** button.


NOTE

A sensor may also play a role in detecting the neighbouring AP and confirming their locations. In the case where a sensor is physically installed, you should consider the range of detection of a sensor for locating it to make sure that it may detect all ranges in a region.

There are the two methods for modifying the information on the location of a sensor:
- After selecting the sensor for which the information on the location should be modified, click the **Modify** button at the bottom to pull up the screen for modifying its location.

- After checking the option for **'Location change mode'** in the middle of the screen, select the sensor to be moved with the mouse cursor. Next, the colour of the sensor will become transparent; after that, place the mouse cursor over the new location and click it to move the sensor to the position of the cursor.


NOTE

In the **'Sensor Settings,'** you may view only the location of the sensor on the currently selected map; the sensors on other maps may be viewed in **'List of sensors** on other maps' on the right side of screen. If you want to move the sensors located on other maps to the current map, check 'Location change mode' and click the left button of the mouse to drag the sensor to be moved from the list of sensors to the current map in the middle of screen.

However, you may not move the sensor on the current map to the list of sensors.

Firmware management

You may register or delete firmware files for a sensor and view the registered information for registered firmware files.

Network > Sensor management > Firmware management > List of firmwares

Figure 75. List of firmwares

[Firmware update]: Updates the selected firmware file to sensor.

[Firmware upload]: Uploads the new firmware file to server.

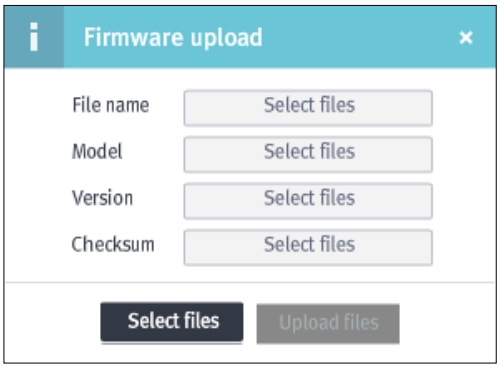


Figure 76. Firmware upload

[Select files]: If you click this button and select the firmware with the file name '*.bin' in the local PC, then the file information for the firmware (equipment type/version/checksum) will be displayed. Click **[Upload files]** button to register it to a server.

[Delete files]: Deletes the selected firmware.

A sensor checks the server every minute to determine whether there is a firmware update available. If there is updated firmware newer than the current firmware, it downloads the file and performs the update.

NOTE

Since a sensor downloads the new file and updates its firmware to the most up-to-date version available at reboot, it must be rebooted for a firmware update.

[Refresh]: Updates the list of connected station.

Channel analysis

You may view the analysis of the signal intensity or usage by channel in 2.4 GHz/5 GHz of bandwidth for the active sensors in the form of graphs or spectrums.

Network > Sensor management > Channel analysis

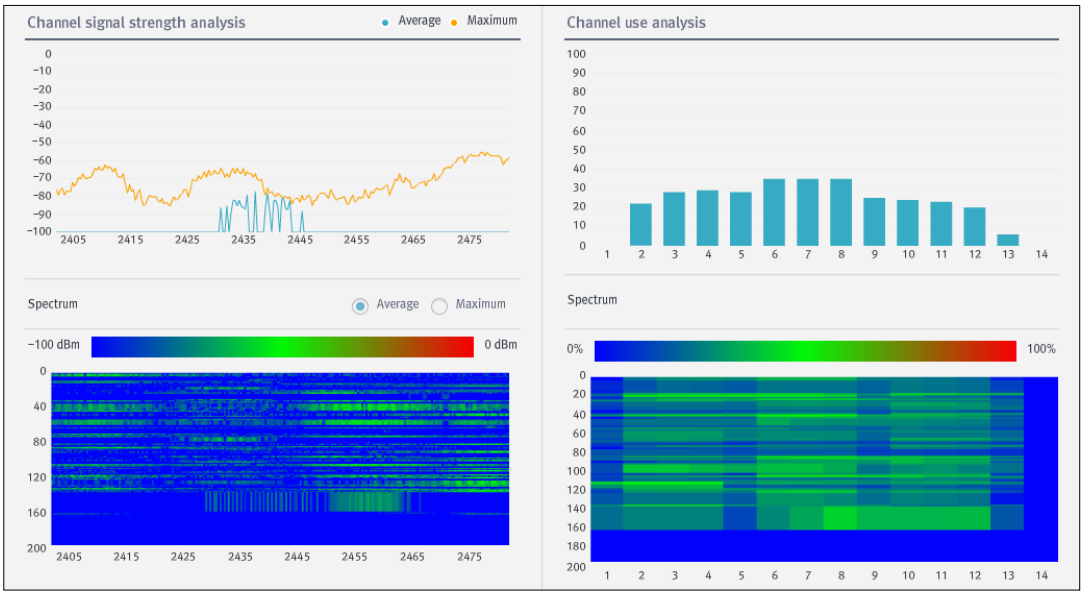


Figure 77. Channel analysis

Input Item	Description	Effective Value (Default)
Sensor	Selects the active sensor.	List of active sensors
Channel	Selects the bandwidth or channel to be analysed.	2.4 GHz 1~14/ 5 GHz 34~64/ 5 GHz 100~140/ 5 GHz 149~165 (2.4 GHz 1~14)

[Start/Stop]: You may start or stop the analysis of signal intensity or usage of the channel.

Sensor information

When you select and double-click a particular sensor in the list of sensors, the registered information on the sensor will be displayed.

From the Sensor information, you may view Detailed information, Disk information, Detected Aps, Detected stations, and Map. You may also find detailed information related to the AP from the Detailed information tab.

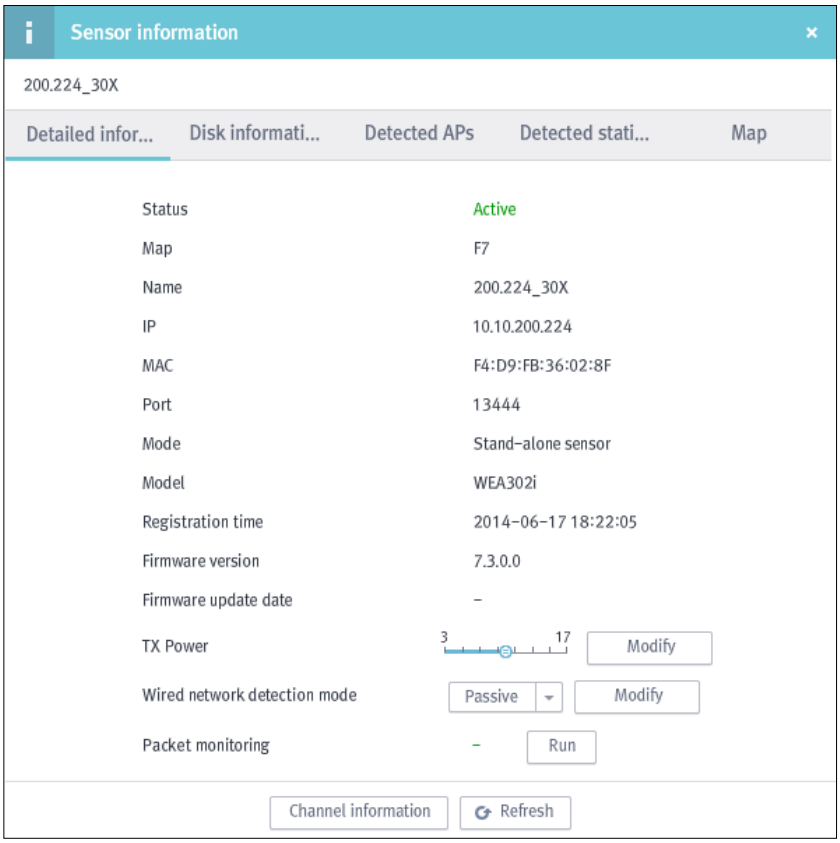


Figure 78. Sensor information-detailed information

[Channel information]: Prints out the monitoring information by channel for the sensor.

[Refresh]: Updates the sensor information.

Output item	Description
Status	Prints out the active status of a sensor.
Map	Prints out the information on the map where a sensor is marked.
Name	Prints out the name of a sensor.
IP	Prints out the IP address of a sensor.
MAC	Prints out the MAC address of a sensor.
Port	Prints out the port number of a sensor.
Mode	Displays the active / inactive mode of a sensor. (Stand-alone sensor type/Sensor + AP integrated type)
Model	Prints out the information on the model of a sensor.
Registration Time	Prints out the information on the time when a sensor was registered.
Firmware version	Prints out the firmware version installed in a sensor.
Firmware update date	Prints out the date when the installed firmware was updated.
TX Power	Sets the output range of transmission of a sensor.
Wired network Detection Mode	Sets the detection mode of a wired network by a sensor.
Packet monitoring	Sets the options for performing packet monitoring for each channel in the bandwidth of 2.4 GHz/5 GHz; to display whether the monitoring is being performed.

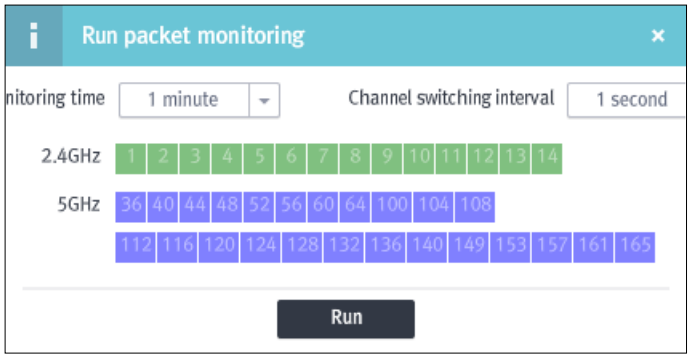


Figure 79. Sensor information-Detailed information (Packet-monitoring)

Input Item	Description	Effective Value (Default)
Monitoring time	Sets the packet-monitoring time.	1~10 minutes (1 minute)
Channel switching interval	Sets the channel switching interval of packet-monitoring.	1~10 seconds (1 second)
Channel	Selects the bandwidth and channel to be analysed.	

From the Disk information tab, you may view the memory usage information of a sensor.

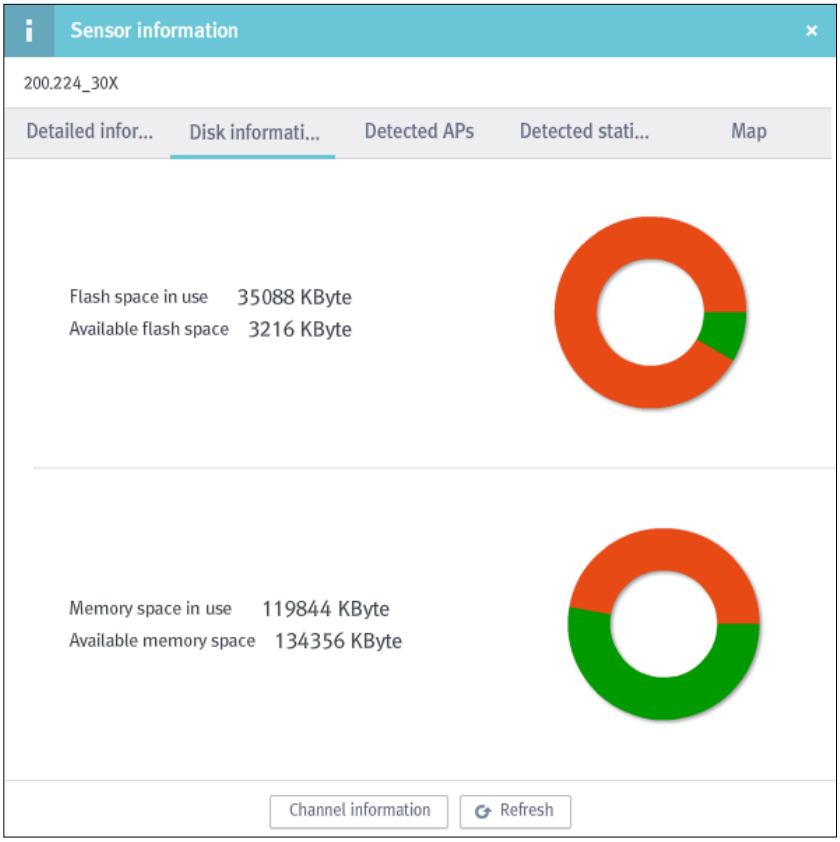


Figure 80. Sensor information-Disk information

Output item	Description
Flash space in use	Prints out the information on used Flash space.
Available flash space	Prints out the information on available Flash space.
Memory space in use	Prints out the information on used Memory space.
Available memory space	Prints out the information on available Memory space.

From the Detected APs tab you may view the information of an AP detected by the sensor.

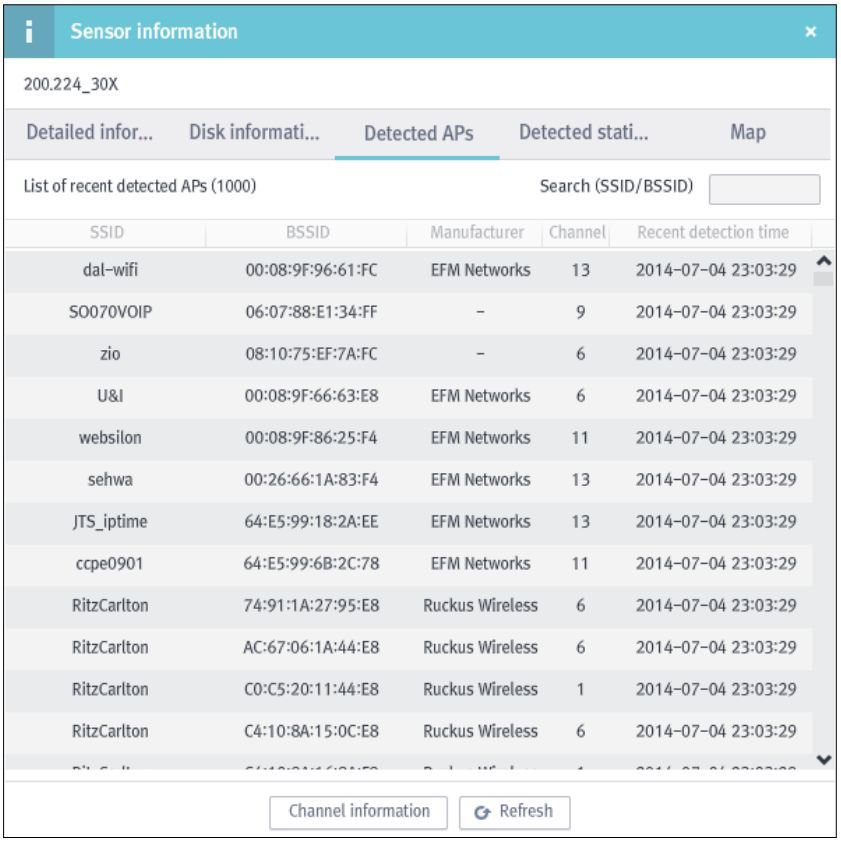


Figure 81. Sensor information-Detected APs

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
SSID	Prints out information on the SSID of an AP.
BSSID	Prints out information on the BSSID of an AP.
Manufacturer	Prints out the information on the manufacturer of an AP.
Channel	Prints out information on the channel of an AP.
Recent detection time	Prints out the time when an AP was recently detected.

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

From the Detected stations tab, you may view the information of station by the sensor.

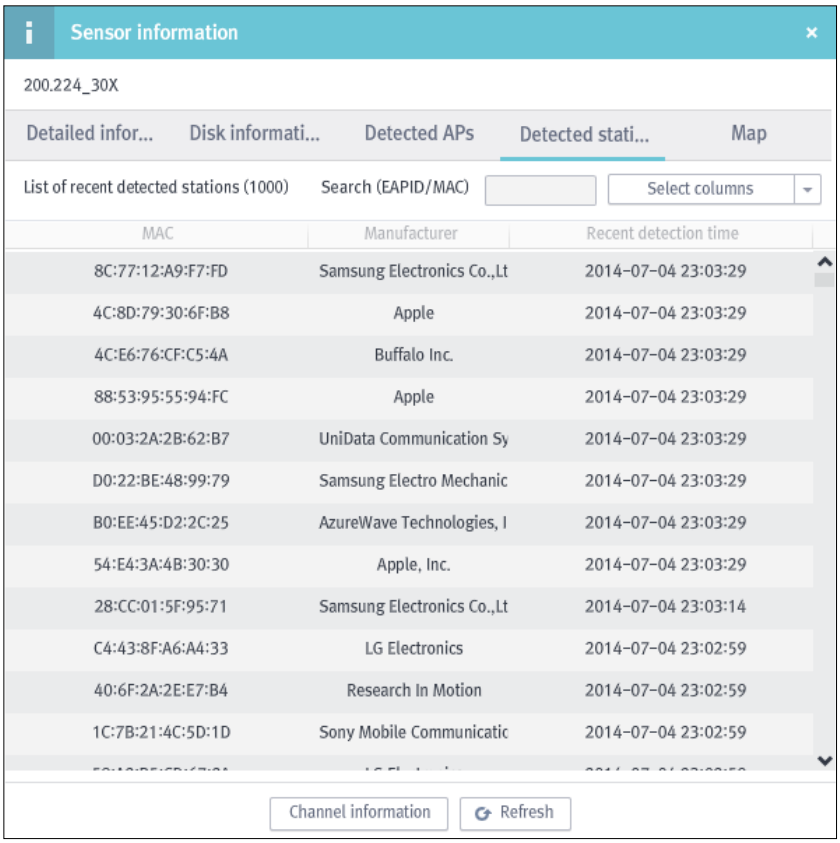


Figure 82. Sensor information-Detected stations

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
EAPID	Prints out the information on the EAPID of a station.
MAC	Prints out the information on the MAC of a station.
Manufacturer	Prints out the information on the manufacturer of a station.
Recent detection time	Prints out the time when a station was recently detected.

[Search]: Makes inquiries about the station by inserting EAPID/MAC (1~17 characters).

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

From Map tab you may view the location information of a sensor.

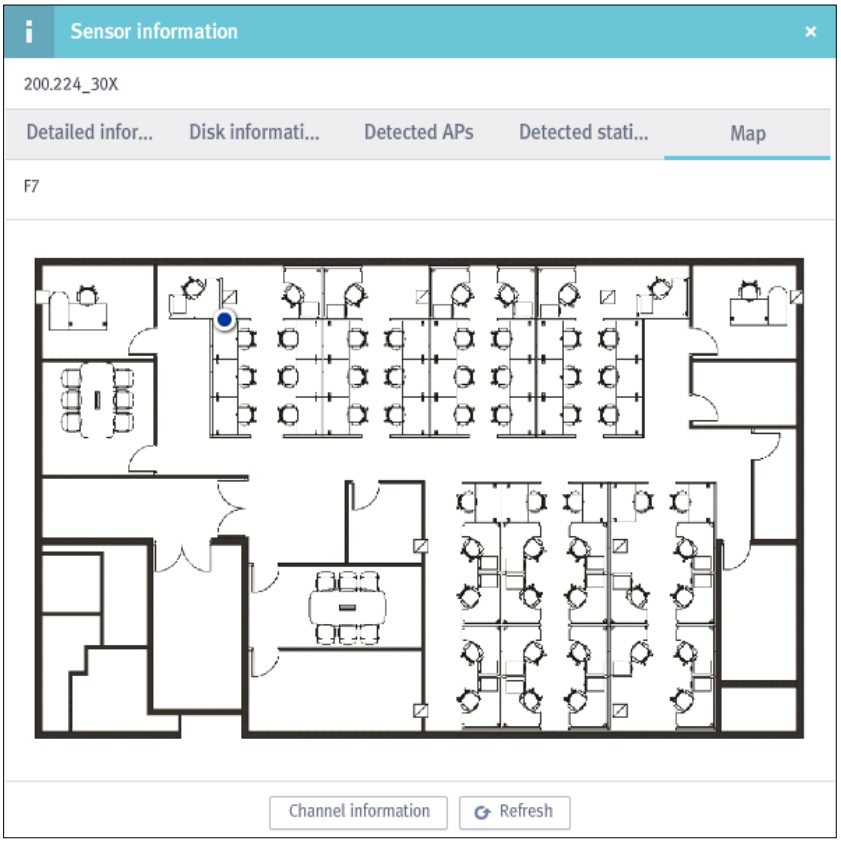


Figure 83. Sensor information-Map

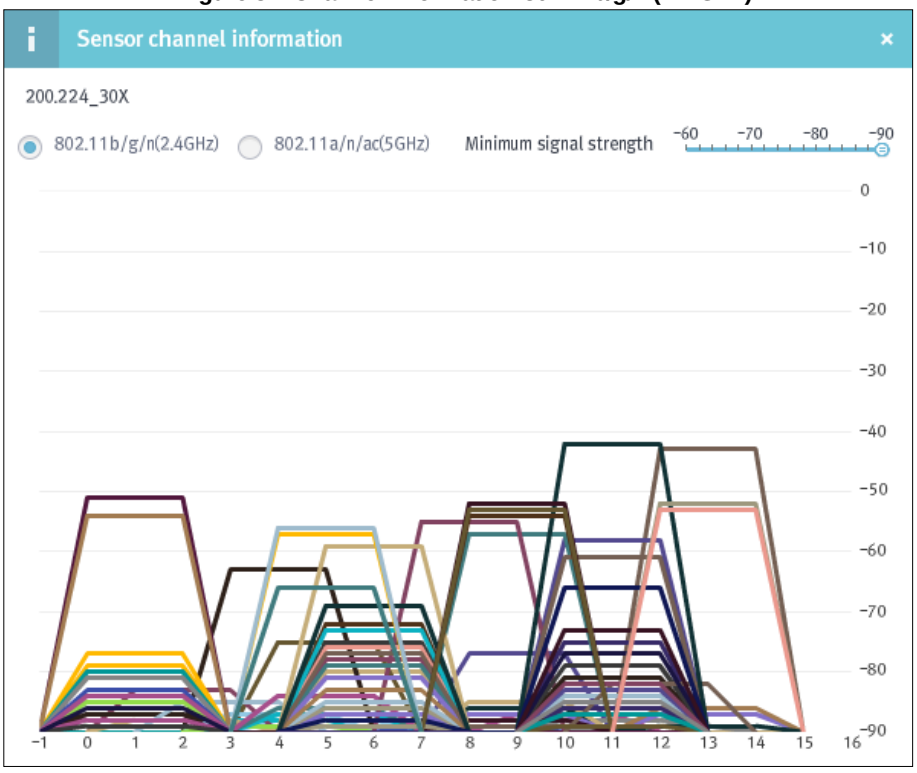
NOTE

A WES sensor may detect the bandwidth of 802.11a/n/ac (5 GHz) and 802.11b/g/n (2.4 GHz) simultaneously, using the dual antenna. From the information on the channel you may view the information on the channel of each bandwidth detected by the sensor.

Channel information

With the sensor, you may check the information on the channel with a bandwidth of 2.4 GHz/5 GHz.

Figure 84. Channel information-802.11b/g/n (2.4 GHz)



The signal intensity and the information on channels by the SSID detected in the bandwidth at 2.4 GHz are displayed; by adjusting or moving the slider for **the minimum value of signal intensity (dBm)**, you may selectively view only the information on the SSID having the predefined value or higher.

NOTE

The bandwidth of a 2.4 GHz Channel is usable in every country where there is no license; in Korea, a total of 85.5 MHz of bandwidths are allocated from channel 1 to 13{depending on the options, channel 14 (the channel used in Japan) may be detected aswell}. Since a variety of devices such as a Microwave oven or Bluetooth devices, etc., use these bandwidths, in frequent cases, there is interference; in order to prevent interference with the neighbouring channel, channel 1, 6, or 11 will generally be used because 20 MHz of bandwidths do not overlap at these channels.

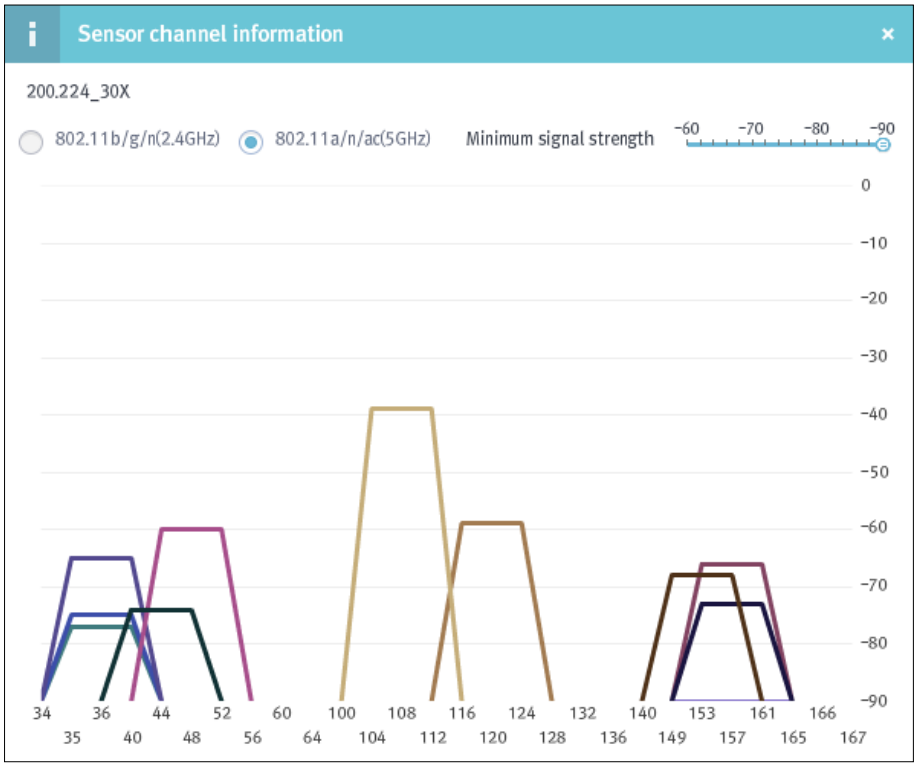


Figure 85. Channels information-802.11a/n/ac (5 GHz)

This displays the signal intensity by the SSID detected at 5 GHz of bandwidth and the information on channels; by moving the slider of **the minimum value of signal intensity (dBm)**, you may selectively view only the information on the SSID having the predefined signal intensity or stronger.

NOTE

There are the 5 bandwidths at the 5 GHz Channel used in Korea; each bandwidth is as follows in the table:

- UNII-1 (lower) / 5.150~5.250 GHz / exclusive for indoor wireless LAN, **4 Channels (36 / 40 / 44 / 48)**
- UNII-2 (Middle) / 5.250~5.350 GHz / DFS is required**, indoor-outdoor wireless LAN, **4 Channels (52 / 56 / 60 / 64)**
- UNII worldwide / 5.470~5.725 GHz / DFS required**, indoor-outdoor wireless LAN **8 Channels (100 / 104 / 108 / 112 / 116 / 120 / 124 / 128)**
- UNII-3 (upper, ISM) / 5.725~5.825 GHz / indoor-outdoor wireless LAN, **4 Channels (149 / 153 / 157 / 161)**

※ DFS (Dynamic Frequency Selection): if a Radar Signal is detected, it will move to the channel at which there is no interference. For other bandwidths, except for those in uses in Korea, only the function of detection will be provided.

2.3.5 Connection management

AP connection management

WES can check all the AP's detected by a sensor. By doing this it may block the AP causing a security problem.

Network > Connection management > AP connection management

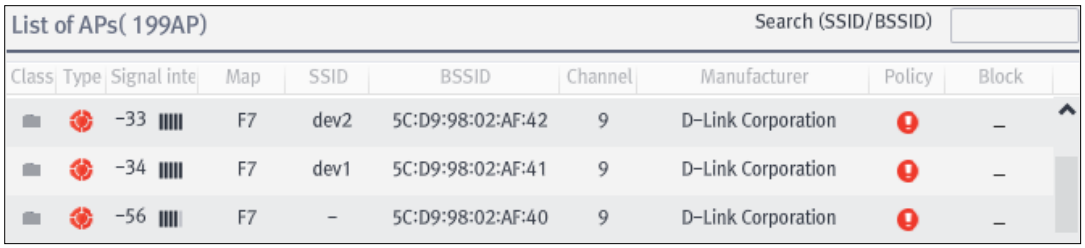


Figure 86. List of APs

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters) .

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Classification	Prints out the status of AP classification. - Classification: Blue, Unclassified: Grey
Type	Prints out information on AP type. - Managed APs: Green, Unmanaged APs: Orange, External APs: Grey, Rogue AP: Red/ Common: For EGG, it is marked as icon E; For mobile devices, it is marked as M.
Signal intensity	Prints out information on the signal intensity of an AP.
Map	Prints out information on the location of AP.
SSID	Prints out information on the SSID of an AP.
BSSID	Prints out information on the BSSID of an AP.
Channel	Prints out information on the communication channel of an AP.
Manufacturer	Prints out information on the manufacturers of an NIC (Network Interface Card).
Policy	Prints out the status of AP policy violations.
Block	Prints out information on the status of an AP and whether it is blocked.

When you double-click on the list of APs, you may view the detailed information on the AP. For more information on the AP, please refer to **section 2.3.2 'AP management' for AP information.**

In order to block an AP, select the AP to be blocked in the list and press the left button on the mouse to drag it to the list of the blocked APs for registration.

Network > Connection management > AP connection management > List of blocked APs

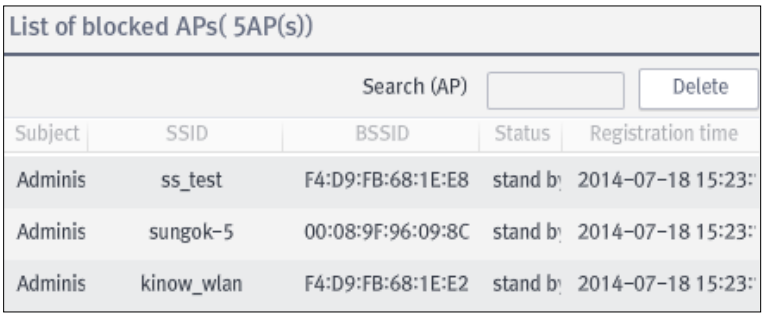


Figure 87. List of blocked APs

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

[Delete]: After selecting the blocked AP to be deleted from the list of blocked APs, click the **Delete** button.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Subject	Prints out information on the subject blocking the AP.
SSID	Prints out information on the SSID of an AP.
BSSID	Prints out information on the BSSID of an AP.
Status	Prints out information on the status of an AP and whether it is blocked.
Registration Time	Prints out the registration time for the AP.

Station connection management

WES checks the station connected to all of the AP detected by a sensor. By doing so, it may block stations, which may cause security problems.

Network > Connection management > Connection station management

Figure 88. List of Stations

[Search]: Makes inquiries about the station by inserting EAPID/MAC (1~17 characters).

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out information on Station type. - Managed stations: Green, Unmanaged stations: Orange, External stations: Grey/Common: For EGG, it is marked as icon E; For mobile devices, it is marked as M.
Signal intensity	Prints out information on the signal intensity of a station.
Map	Prints out information on the building and floor where the Stations is located.
EAPID	Prints out information on the EAPID for the station. - In the case where there is no synchronization with Anyclick AUS, an authentication system, no information is shown.
MAC	Prints out information on the MAC address.
Manufacturer	Prints out information on the manufacturers of an NIC (Network Interface Card).
Connected AP	Prints out information on the AP (SSID/BSSID) a station is connected to.
Policy	Prints out the policy violations of a station.
Block	Prints out the blocking status of a station.
Risk	Prints out the status of risk for a station.

NOTE

If there is synchronization with the Anyclick AUS server, the information on user names and EAPID will be displayed as well; otherwise, only the MAC information will be shown.

In order to block the station, select the station to be blocked in the list and drag it to the list of blocked stations (the list set by an administrator) by pressing the left mouse button.

Network > Connection management > Station connection management > List of blocked stations

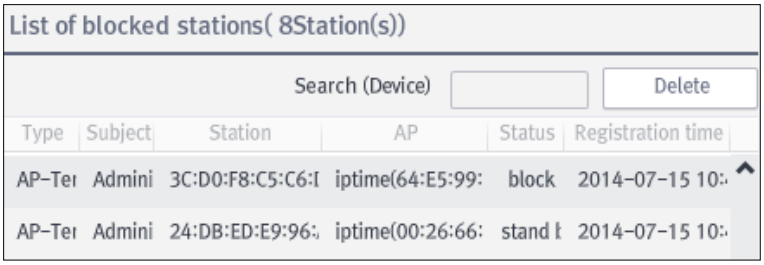


Figure 89. List of blocked stations

[Search]: Makes inquiries about the station by inserting MAC (1~17 characters).

[Delete]: After selecting the blocked station to be deleted from the list of blocked stations, click the Delete button.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out the blocking type of the blocked station.
Subject	Prints out information on the subject blocking the station.
Station	Prints out information on the EAPID(MAC address) of the blocked station.
AP	Prints out information on the SSID / BSSID of the AP connected to the blocked station.
Status	Prints out information on the status of blocking the station.
Registration Time	Prints out information on the date on which a station was registered.

NOTE

Once the station is registered in the list of blocked stations (the list set by an administrator), the neighbouring sensor will start monitoring. If the connection of the station registered in the list is detected, it will send the packets to the station to block its connection.

Connection graph

WES provides a topological graph in order to easily check the information on abnormal connection between stations and APs.

Network > Connection management > Connection graph

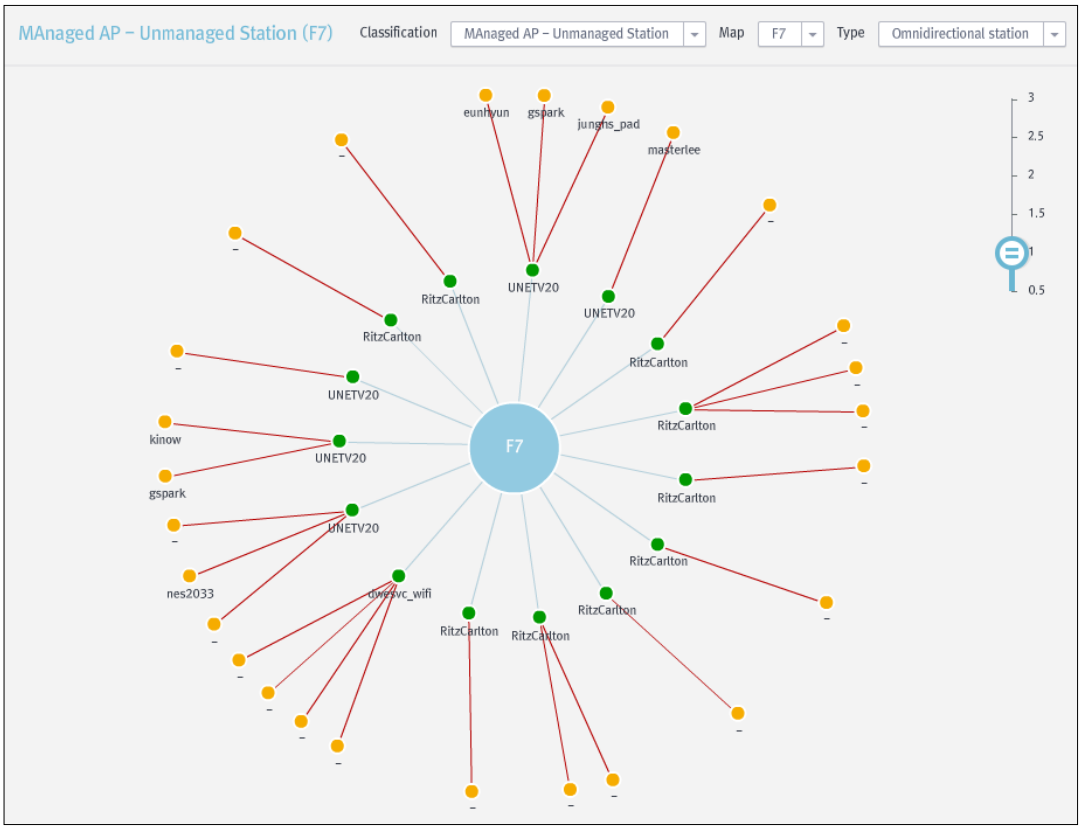


Figure 90. Connection graph

Input item	Description	Effective Value (Default)
Classification	Selects the information on the connection of the AP-Station.	Managed AP-Unmanaged AP/ Unmanaged AP-Managed station/ Rogue AP-Managed station/ External AP-Managed station (Managed AP-Unmanaged AP)
Map	Selects the information on the location of the intra-network.	Location list of the registered Infra-network
Type	Selects the graph of the connection status for the station by AP.	Omnidirectional station/ Omnidirectional AP/ Tree(LEFT)/Tree(TOP) (Omnidirectional station)
Ratio	Selects the ratio of graph representation.	0.5~3 (1)

The red connection line on the connection graph represents the abnormal status of connection; (Green) signifies a managed AP/station; (Grey) signifies an external AP/station; (Orange) signifies an unmanaged AP/station; (Red) signifies a Rogue AP.


NOTE

When you double-click a particular AP/station on the graph, you may view the registered information on the AP/station. By doing this you may set the options for blocking them.

2.3.6 Account management

This chapter explains the method of registering administrator information for system operation. On the root administrator's account, the ID of the value set at first login is the value set in the installation of a server; you may change the password after the first login.

Account management > List of accounts

Figure 91. List of accounts

[CSV Export]: Saves the output status in the form of a CSV file on the local PC by specifying the path.

Account management

The sensors or AP to be managed will be augmented in proportion to the network size. For effective management of these devices, it is necessary to operate additional administrators. Therefore, WES provides the function of managing the accounts (Add/Modify/Delete).

Account management > Add

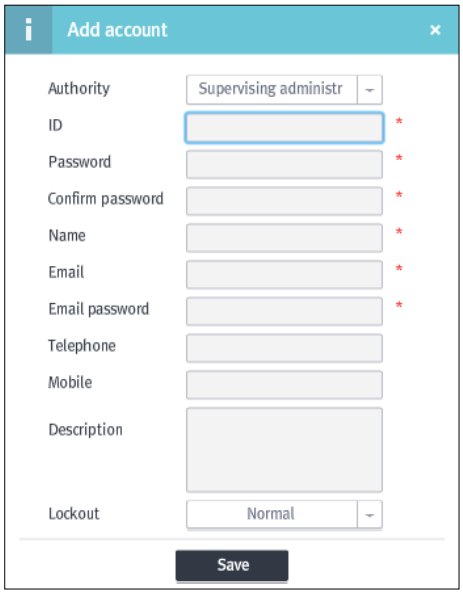


Figure 92. Add Account

Input Item	Description	Effective Value (Default)
Authority	Sets the type according to an administrator's level of	Supervising administrator /

	authority.	Senior administrator / Administrator (Supervising administrator)
ID*	Sets the ID of an administrator.	3~15 characters (None)
Password/ Confirm password*	Sets the password for the administrator.	9~15 characters (None)
Name*	Sets the name of an administrator.	3~15 characters (None)
Email*	Sets the email address of an administrator.	1~30 characters (None)
Email password*	Sets the email password of an administrator.	1~15 characters (None)
Telephone	Sets the telephone number of an administrator. (ex, XXX-XXXX-XXXX).	1~30 characters (None)
Mobile	Sets the mobile phone number of an administrator. (ex, XXX-XXXX-XXXX).	1~30 characters (None)
Description	Inserts a description for an administrator.	0~100 characters (None)
Lockout	Sets the status of an administrator's account.	Normal / Lockout (normal)


NOTE

When administrators are added or there are existing accounts, you may manually set them by modifying the account information. When logging on to the web console through an account in the normal status, if there is an excess of **'the number of allowable failed logins,'** the account status will change to **'lockout'** by the process of handling such failed logins.

The password must include at least one or more letters, numbers, and special characters.

The minimum length is 9 digits; the maximum length is 15 digits.

Special characters may include the following 27 symbols:
=> _ - = + \ | ( ) * & ^ % $ # @ ! ~ ` ? >< / ; , . :

[Modify]: After selecting the account to be modified in the list, click the **Modify** button at the top. Once the screen for modifying is displayed, you may modify the options of your choice.

[Delete]: After selecting the account to be deleted from the list of accounts, click the **Delete** button at the top.

2.4 Map info settings

2.4.1 MAP management

WES may mark the location of sensors/APs on the map by registering the map.

Map > Map information > Add

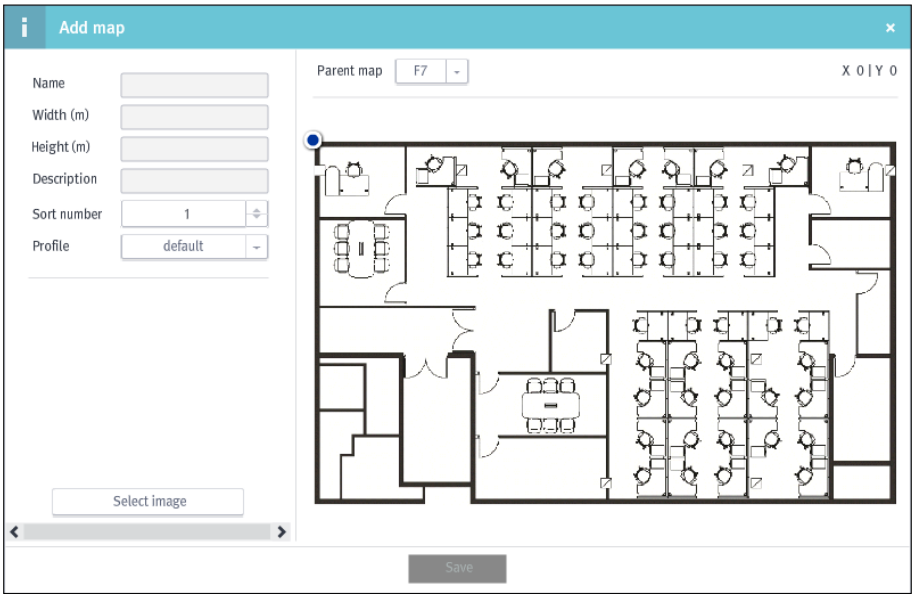


Figure 93. Add map

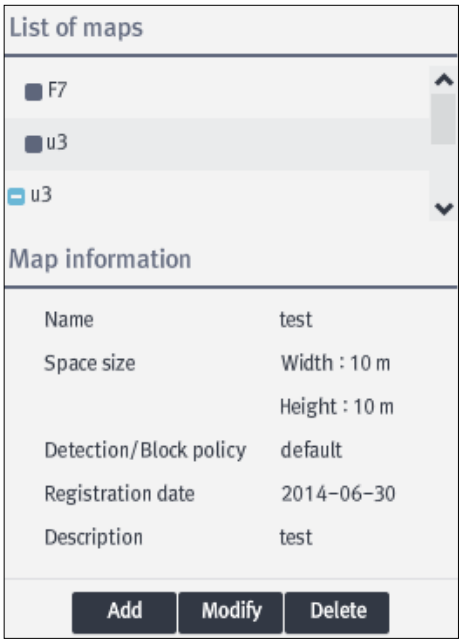
Input Item	Description	Effective Value (Default)
Name	Sets the name of the map. − Generally, it set the name of a building, the name of an office or the floor information.	1~15 characters (None)
Width (m)	Sets the information on the horizontal width.	Number 1~ 5 characters (None)
Height (m)	Sets the information on the vertical width.	Number 1~ 5 characters (None)
Description	Inserts a description for a map.	1~100 characters (None)
Sort Number	Sets the order in which items are sorted in the group list.	1~10 (1)
Profile	Sets the detection blocking policy to be applied to the office or floor. − Please refer to 'Detection Block policy.'	-
Select images	Sets the image of a map of the space where sensor is to be installed.	-
Parent map	Sets the information on the location of the map. − Basically, it is registered as a floor; depending on the selection of location, the previous registered information will change from the floor to the building.	-

NOTE

Select the profile to be applied to the map in the specified profile list from the detection block policy.

If you add the map information, you may view the list of registered maps on the left side of the screen. When you select **List of maps** and click on the map to be viewed, the image of the map will be displayed; in **Map information**, the detailed information on the map will be printed out.

Figure 94. List of maps/ MAP information



[Modify]: After selecting the map to be modified in the list, click the **Modify** button at the bottom of the screen. Once the screen for modifying the map is displayed, you may modify the options of your choice.

[Delete]: After selecting the map to be deleted from the list of maps, click the **Delete** button at the bottom.

Marks on the Map

You may view the physical location where a sensor is placed on the image screen of a map; the registered sensors will automatically detect the AP within their detectable range to display them on the map image screen.

Figure 95. Mark on the map

You may decide whether the sensors/APs represented on the map will be marked, depending on each option; depending on **the map scale** settings, you may magnify/reduce the map size.

By checking **[List]**, you may hide or reveal the **List of MAPs (number of maps)**, **List of APs (number of APs), and list of sensors (number of sensors)**; the AP/sensors marked on the map will be printed in the **List of APs (number of APs)** and the **list of sensors (number of sensors)** on the right side of the screen. By checking **[Location auto update]**, you may set the locations of the APs/sensors marked on the map so that they may be automatically updated (on a three-second basis); when you double-click the marker on the map or the particular sensor/AP in each list, you may view AP information (for more details, **please refer to section 2.3.2 'AP management' for AP information**)/sensor information (for more details, **please refer to section 2.3.4 'Sensor management' for Sensor information**).

When you click the **[Parent map]** button, you will be directed to the map group in a parent hierarchy; when you click the **[Refresh]** button, it updates the information on AP/the list of sensors.

The information on the list of maps, the list of APs, and the list of sensors marked on the map is as follows:

- List of maps

Output item	Description
Name	Prints out information on AP type.
Space size	Prints out physical size of the map.
Coordinates (pixel)	Prints out information on the location on the map.

- List of APs

Output item	Description
Type	Prints out information on AP type. − Managed APs: Green, Unmanaged APs: Orange, External APs: Grey, Rogue AP: Red
SSID	Prints out information on the SSID of an AP.
BSSID	Prints out information on the BSSID of an AP.
Channel	Prints out information on the communication channel of an AP.
Coordinates (pixel)	Prints out information on the location on the map.

NOTE

The number of AP on a **'MAP > List of APs'** may differ from the number of AP in the **'Network > AP management > List of APs.'** The number of AP in the **'Network > AP management > List of APs' represents the number of all Aps detected by a sensor;** the number of AP on a **'MAP > List of APs' represents the number of AP for which the location information is confirmed by 3 or more sensors.**

- List of sensors

Output item	Description
Status	Indicates the status of a sensor with an icon (Activated: Green, Deactivated: Red).
Name	Prints out the name of a sensor.
IP	Prints out the IP address of a sensor.
Port	Prints out the communication port number of a sensor.
Coordinates (pixel)	Prints out information on the location on the map.

CHAPTER 3. Policy

This chapter explains the methods of policy setting and application for using the security functions provided by WES.

3.1 Overview

As wireless network environments have become prevalent, the networking environments are getting more and more open. As a result, the methods for connecting to the intra-network through wireless connection in these environments are classified into Ad-Hoc and Infrastructure Modes. There are a number of security problems caused by wireless networks, but they are generally classified into 5 types.

First, Radar detection
Theft of important internal information and preparation for penetration into the intra-net

Second, Ad-Hoc connection
User negligence or deliberate connection of External station

Third, Gateway section detour
unauthorized internal AP/an attack on a security-vulnerable AP or misconfigured AP, the detour by Software AP.

Fourth, Detour connection to the external network
Unregistered Rogue AP, HoneyPot AP having the same SSID as the managed APs, deliberate connection to External APs or a wireless LAN service, WDS access for connection between wireless AP, Wi-Fi Direct access for connection between smart phones, and MAC Spoofing (AP/Station) for using the BSSID/MAC addresses of managed APs/stations illegally

Fifth, large-scale packet attack
DoS attack to compromise the service or ARP Injection for a WEP key crack

WES synthetically controls the wireless infrastructure through a number of security policies,guarantees service availability, and secures the efficient and safe wireless networking environment by detecting security vulnerabilities in the network and by preventing penetration from the outside.

3.2 Management policy

WES provides the functions of automatic registration/blocking according to aging or signal intensity in order to manage a list of the number of APs and stations detected by a sensor. This chapter explains the methods for setting the list aging and automatic registration/blocking functions.

3.2.1 Management policy

When you set aging, only the list of APs/stations which are set to be stored for the predefined retention period (before the number of days) on the basis of the present date will be retained; you may register AP/station as managed/blocked on the basis of signal intensity.

Policy settings > Management policy

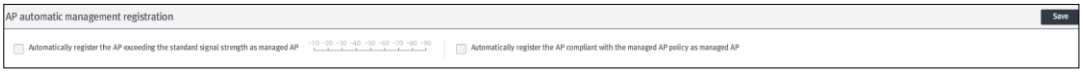


Figure 96. Management policy-AP automatic management registration

Input Item	Description	Effective Value (Default)
AP automatic management registration	Sets the AP having a signal intensity marked as strong as the predefined value or stronger so that they may be automatically registered as managed APs.	Checked/ Unchecked (Unchecked)
	Sets the reference signal intensity for automatic registration.	-90 ~ -10(-50)
	Sets the AP so that they may be automatically registered as managed in the case where they conform to the standard of managed AP policy.	Checked / Unchecked (Unchecked)

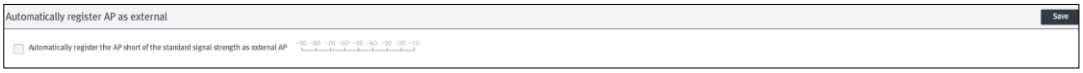


Figure 97. Management policy-AP automatic management registration

Input Item	Description	Effective Value (Default)
Automatically register AP as external	Sets the AP having a signal intensity marked as strong as the predefined value or weaker so that they may be automatically registered as external APs.	Checked/ Unchecked (Unchecked)
	Sets the reference signal intensity for automatic registration.	-90 ~ -10 (-50)

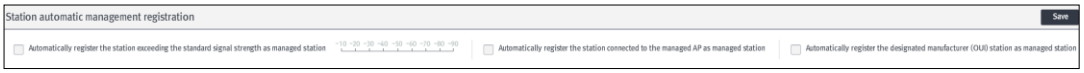


Figure 98. Management policy-Station automatic management registration

Input Item	Description	Effective Value (Default)
Station automatic management registration	Sets the station with the predefined signal intensity or stronger so that they may be automatically registered as managed stations.	Checked/ Unchecked (Unchecked)
	Sets the reference signal intensity for automatic registration.	-90 ~ -10 (-50)
	Sets the station connected to the managed AP so that they may be automatically registered as managed stations. - In the case where the security policy to be applied to the connection of unmanaged stations to managed APs is in use, it cannot be used.	Checked/ Unchecked (Unchecked)
	Sets the station made by certain manufacturers (OUI) so that they may be automatically registered as managed.	Checked/ Unchecked (Unchecked)

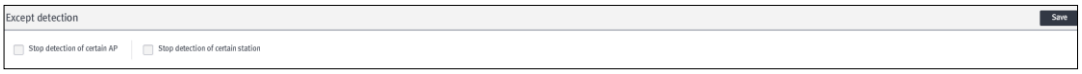


Figure 99. Management policy-Except detection

Input Item	Description	Effective Value (Default)
Except detection	Sets the options for stop detection of certain AP.	Checked / Unchecked (Unchecked)
	Sets the options for stop detection of certain Station.	Checked / Unchecked (Unchecked)

Allowed access group settings

WES can set to allow the interconnection between APs and Stations to authorize the access by group.
Generally, all managed APs and devices are included in the default group (AP/device), and the default groups allow interconnection with each other.

In addition, WES can add various AP groups (BSSID groups/SSID groups) and Station groups (MAC group) and authorize interconnection between groups (AP group–Station group).

Policy settings > Management policy > Allowed access group settings > AP group / Station MAC group > Add

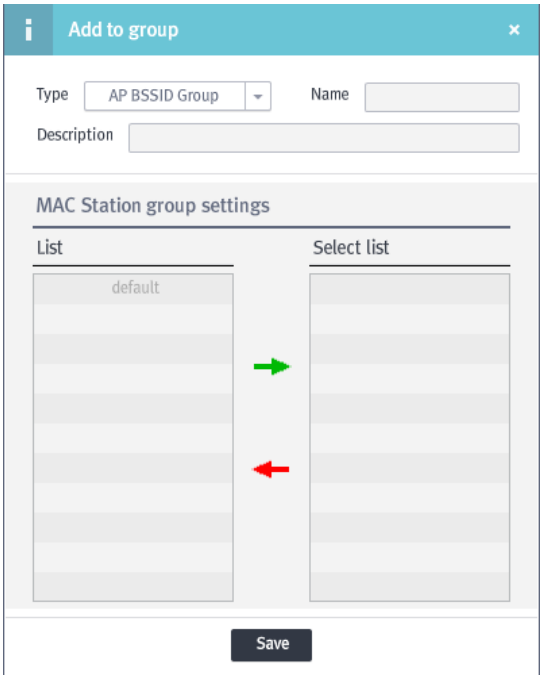


Figure 100. Add group

Input	Description	Effective Value (Default)
Type	Sets the type of the group.	AP BSSID group/ AP SSID group/ Station MAC group (AP BSSID group)
Name	Sets the name of the group.	1~30 characters
Description	Enters the description of the group.	1~100 characters
Station MAC group settings	Sets the station group that can access the AP group. To add, select the device list to add from the list and click →. To delete, select the device list to delete from the list and click ←. - It will be activated when the type category is 'AP BSSID group' or 'AP SSID group'.	

If you add the Station MAC group, you can set the station MAC group that will access the added AP group (BSSID group/SSID group).

If you added the AP group but not the Station MAC group, modify the AP group and add the device MAC group.

[Modify]: Select the AP group/Station MAC group to modify from the list of groups and click the **Modify** button at the bottom. When you see the screen where you can modify the AP group/Station MAC group, change the name, description, and Station MAC group (when modifying the AP group).

[Delete]: After selecting the group to be deleted from the list of groups, click the **Delete** button at the bottom.

You cannot modify or delete the default group (AP group/Station group).


NOTE

The managed APs and devices may overlap across multiple groups. When you select the group, the ones under the "**Selected List**" in the BSSID (AP)/SSID (AP)/MAC (device) settings on the right are a list of the APs (BSSID, SSID) or devices (MAC) that are included in the selected group. The ones in the **'List'** are not included in the group.

The managed APs and Stations that are excluded from the group added by the manager are included in the default group again.

To check the Station MAC group, go to “Station MAC Group > List of groups”

Policy settings > Management policy > Allowed access group settings > Station MAC group

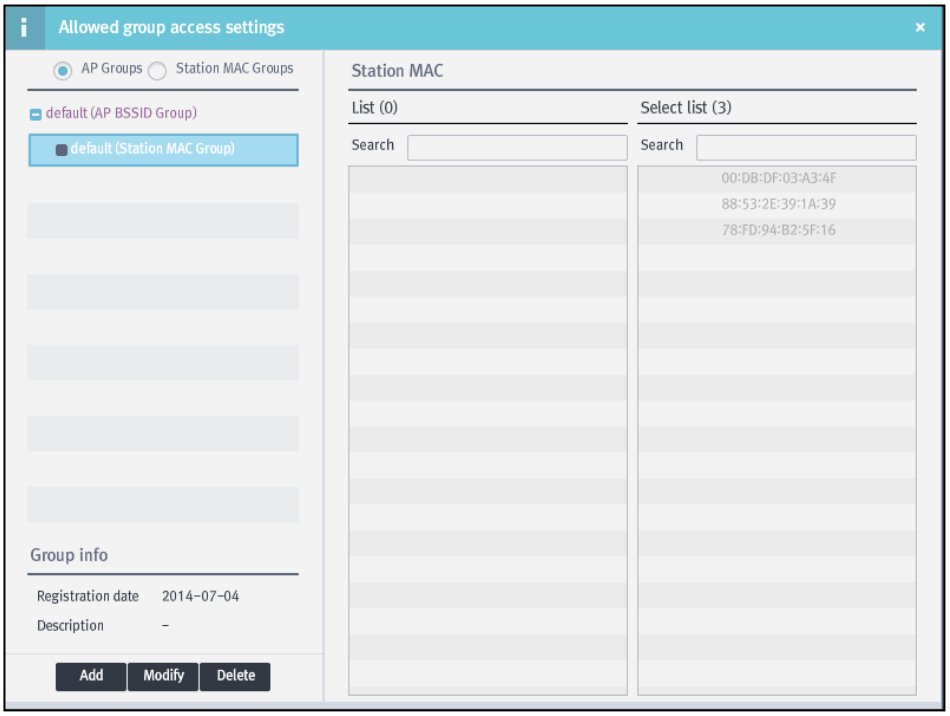


Figure 101. Allowed access group settings-Station MAC group

To add device MAC to the added Station MAC group, go to the **Group List** and select Station MAC group. Go to the **List** menu in the MAC settings, select Station MAC to add and click .

To delete device MAC, go to the **Selected List** menu, select device MAC you wish to delete and click .

To check the added AP group, go to **'AP Group > List of groups'**.

Policy settings > Management policy > Allowed access group settings > AP group

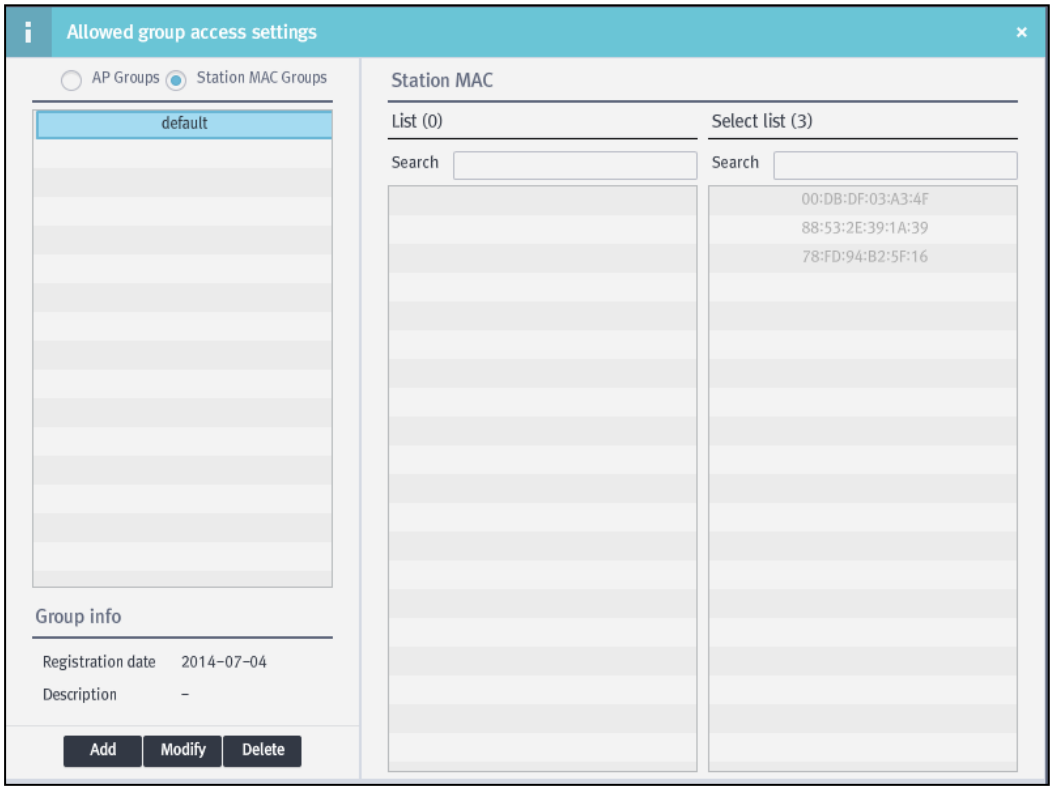


Figure 102. Allowed access group settings-AP group

To add BSSID/SSID to the added AP group (BSSID group/SSID group), go to Group List and select the AP group. Select the BSSID/SSID you wish to add from the List menu in the AP BSSID/AP SSID settings and click .

To delete BSSID/SSID, go to the Selected List menu, select BSSID/SSID you wish to delete and click .

Input	Description	Effective Value (Default)
SSID	Sets the ssid to be added manually.	1~30 characters

3.3 Detection Block policy

You must set the detection block policy in order to perform the functions of penetration detection and blocking in WES. This chapter explains the methods of setting the detection block policy in order to use the security functions in WES.

3.3.1 Profile management

Various security policies can be grouped together in a sort of profile; each profile can be applied to each map when the map info is set.

Policy settings > Detection Block policy > Add

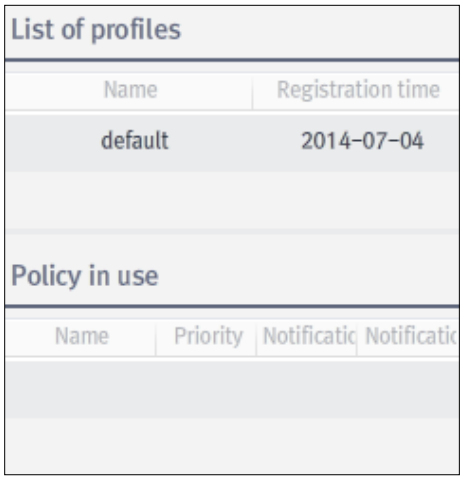


Figure 103. List of profiles

If you want to add the profile, click the **[Add]** button at the top to set each respective detection block policy and the profile name and then click the **[Save profiles]** button.

If you want to modify the profile, select the profile to be modified on the left, modify the details and click the **[Save profiles]** button.

If you want to delete the profile, select the profile to be deleted on the left and click the **[Delete]** button at the top.


NOTE

In the case where the Managed AP policy is to be saved as a profile, first register the Managed AP policy (SSID/Connection mode/Encryption/Manufacturer/Authentication/Channel (multi)/Data rate (multi)/SSID (Broadcast) and click the **[Save profiles]** button to save a profile.

If this is done, it will be saved as a normal profile. For operation and security policies, set the policies and then click the **[Save profiles]** button in order to save the profiles.

In the case where you want to make a new policy using the previous profile, the profile reproduction (duplication) function can be used. **In the 'List of profiles', select the profile to be copied** and click the **[Copy profiles]** button. Then, a copied version of the previous profile will be created. At this time, you may modify the profile and a copied version of the previous Managed AP policy.

3.3.2 Managed AP policy

Set the policy for detecting misconfigured AP.

Policy settings > Detection Block policy > Profile settings > Managed AP policy

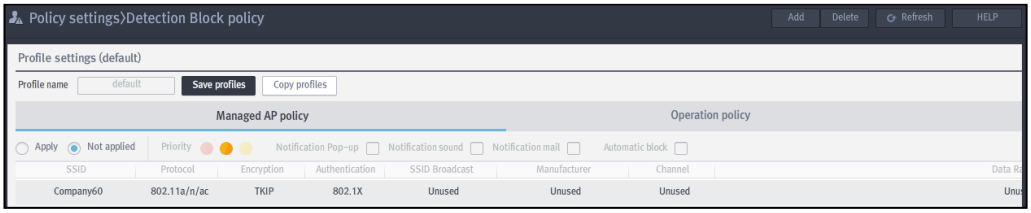


Figure 104. Managed AP policy

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for applying the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using a notification pop-up window in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using a notification sound in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic block function in the case of an event.	Checked/Unchecked (Unchecked)
Wired connection block	Sets the options for using the wired connection block function in the case of an event. − In the case where the option of automatic block is checked, it is activated.	Checked/Unchecked (Unchecked)

[Modify]: Select the policy to be modified in the list of policies for managed AP and click the **Modify** button at the top. Once the screen for the policy for managed APs is displayed, you may change the details as you wish.

[Delete]: After selecting the policy to be deleted from the list of policies for managed APs and click the **Delete** button at the top.

NOTE

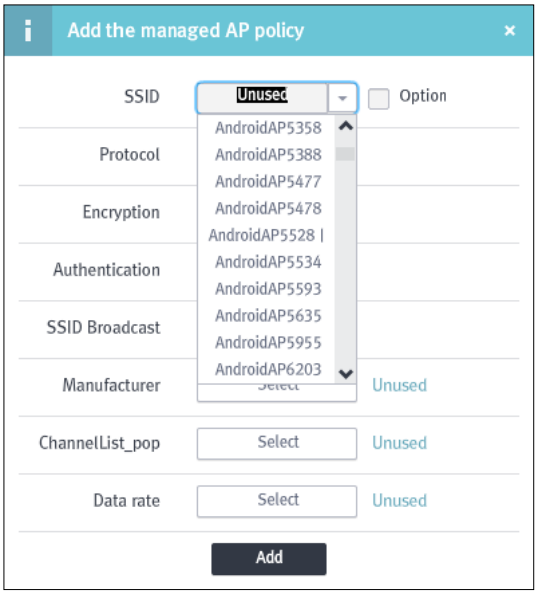
If there is no input during the predefined time set by root administrator after you log into the web console, you will be automatically logged out. For more details, p**lease refer to section 2.2.1 'System settings' for automatic log-out**. Setting of the options for using the policies for managed APs and for notification will be applied by the profiles. For example, in the case where there are a number of policies for a profile, the settings for using them or for notification will be applied to all of the files included in the profile.

SSID

Only APs using a registered SSID in the list of SSIDs will be accepted as normal; if APs using an unregistered SSID are detected, an event will be generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > SSID

Figure 105. Managed AP policy-SSID



Input Item	Description	Effective Value (Default)
SSID	Selects the SSID in the list of detected SSIDs or insert the SSID directly. − Place the mouse cursor over the item for the SSID and input the SSID directly.	If selected: Detected SSID (Unused) In the case of direct input: 1~17 characters
Options	Sets the options so that the policy may be applied to all of the SSIDs including the directly input character strings.	Checked / Unchecked (Unchecked)

NOTE

If an AP using the same SSID as the registered SSID is detected
- it will be recognized as normal, so no event is generated.

If an AP using an unregistered SSID is detected
- it will be recognized as one of the AP violating the policy, so an event is generated.

Protocol

Only the APs using the protocol registered in the list will be accepted as normal; if the APs using unregistered protocols are detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > Protocol

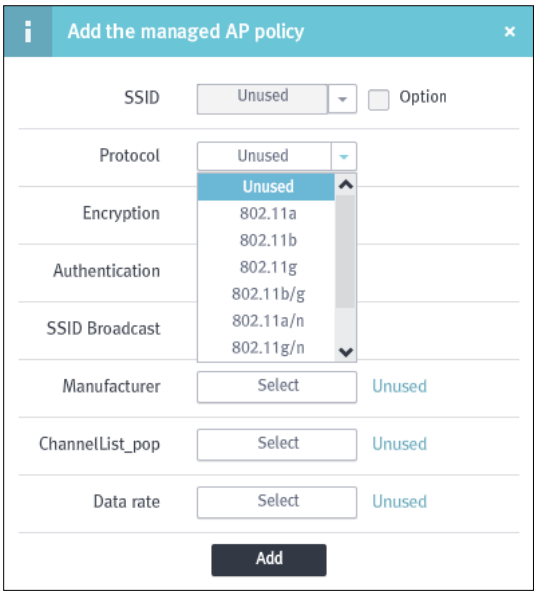


Figure 106. Managed AP policy-Protocol

Input Item	Description	Effective Value (Default)
Protocol	Selects the protocol to be applied as policy.	802.11a,802.11b,802.11b/g, 802.11a/n,802.11g/n, 802.11b/g/n, 802.11a/n/ac (Unchecked)

NOTE

If an AP using the same protocol as the registered mode is detected
- they are to be recognized as normal, so no event is generated.

If an AP using unregistered protocols is detected
- they will be recognized as AP violating the policy, so an event is generated.

Encryption

Only an AP using an encryption method registered in the list will be accepted as normal; if an AP using an unregistered encryption method is detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add> Encryption

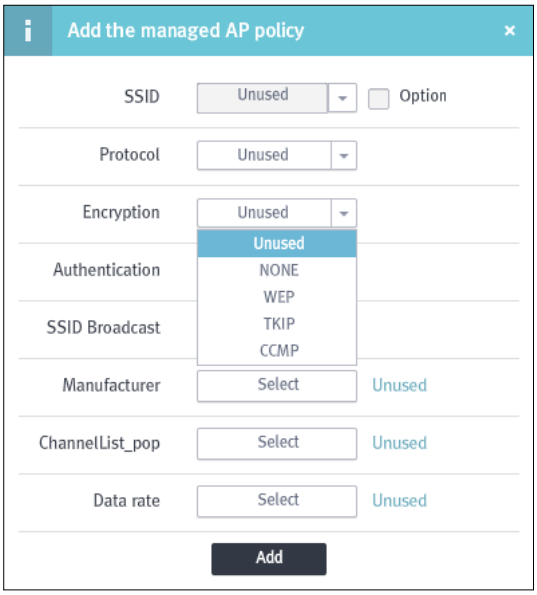


Figure 107. Managed AP policy-Encryption

Input Item	Description	Effective Value (Default)
Encryption	Selects the encryption method to be applied to a policy.	OPEN/WEP/TKIP/CCMP (Unused)

NOTE

If an AP using the same encryption method as the registered method is detected
- it will be recognized as normal, so no event is generated.

If an AP using an unregistered encryption method is detected
- it will be recognized as an AP violating the policy, so an event is generated.

Authentication

Only APs using the authentication method registered in the list will be accepted as normal; if APs using unregistered methods are detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > Authentication

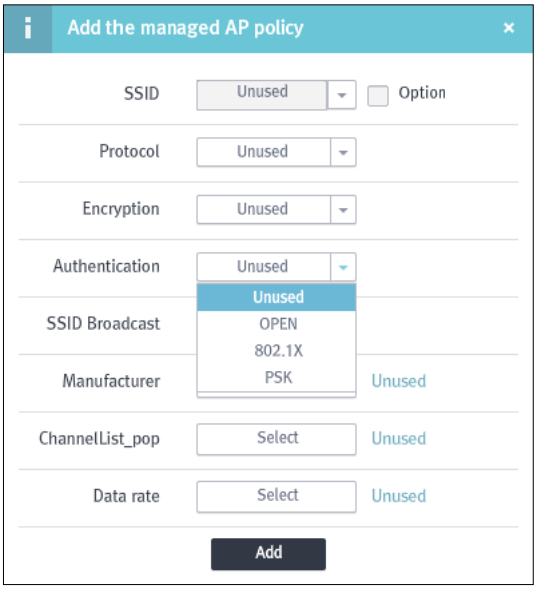


Figure 108. Managed AP policy-Authentication

Input Item	Description	Effective Value (Default)
Authentication	Selects the authentication method to be applied as policy.	OPEN/802.1X/PSK (Unused)

NOTE

If an AP using the same authentication method as the registered method is detected
- it will be recognized as normal, so no event is generated.

If an AP using an unregistered authentication method is detected
- it will be recognized as an AP violating the policy, so an event is generated.

SSID Broadcast

Only Aps using the SSID Broadcast method registered in the list will be accepted as a normal AP; if an AP using an unregistered SSID Broadcast method is detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add> SSID Broadcast

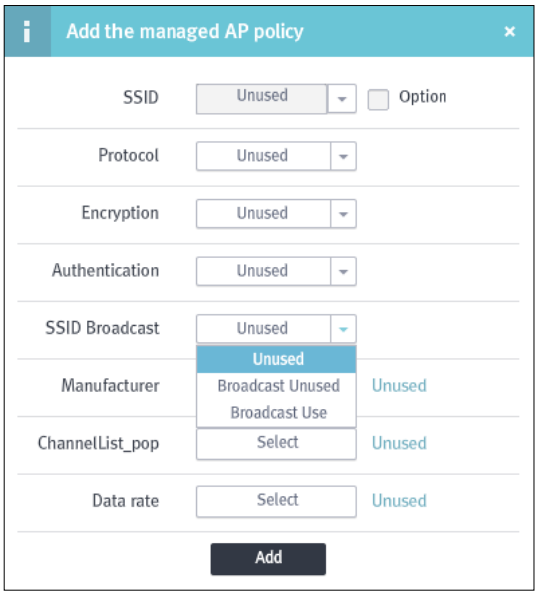


Figure 109. Managed AP policy-SSID Broadcast

Input Item	Description	Effective Value (Default)
SSID Broadcast	Selects the options for using SSID Broadcast.	Use Broadcast/ Do not use Broadcast (Unused)

NOTE

If an AP using the SSID Broadcast as the registered method is detected
- it will be recognized as normal, so no event is generated.

If an AP using an unregistered SSID Broadcast method is detected
- it will be recognized as an AP violating the policy, so an event is generated.

Manufacturer

Only APs made by the manufacturers registered in the list will be accepted as normal; if APs made by unregistered manufacturers are detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > Manufacturer

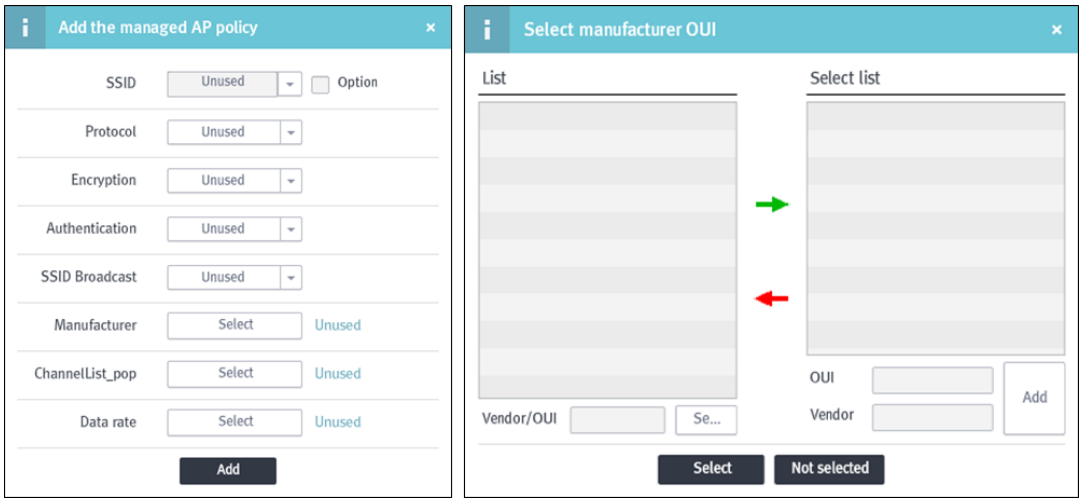


Figure 110. Managed AP policy-Manufacturer

Search for Vendor/OUI, select the vendor you wish to add from the list and click → to add to the Selected List. To delete from the Selected List, select the vendor you wish to delete from the Selected List and click ←.

[Search]: Makes inquiries about the manufacturer by inserting Vendor/OUI (1~30 characters).

Input Item	Description	Effective Value (Default)
OUI	Sets the OUIs to be added.	00:00:00~FF:FF:FF (None)
Vendor	Sets the Vendor to be added.	1~30 characters

NOTE

If APs made by the same manufacturers as those registered are detected
- they will be recognized as normal AP, and no event is generated.

If APs made by unregistered manufacturers are detected
- they will be recognized as AP violating the policy, so an event is generated.

Channel

Only Aps using registered channels from the list will be allowed as accepted;
if APs using unregistered channels are detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > Channel

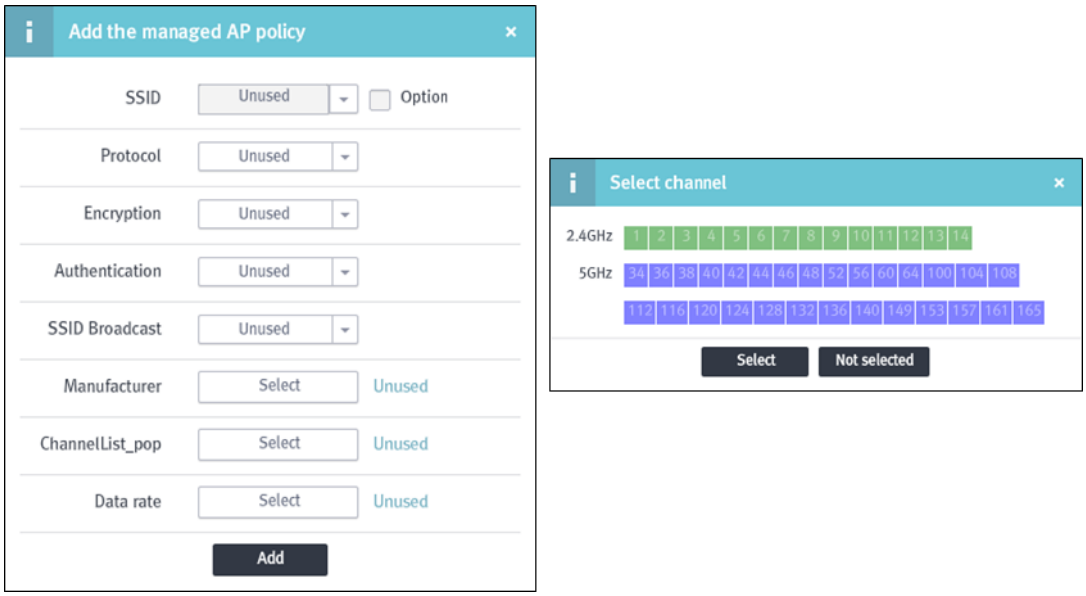


Figure 111. Managed AP policy-Channel

Input Item	Description	Effective Value (Default)
Channel	**'Select a Channel'** displays a screen for selecting channels.	-
2.4 GHz/5 GHz	Selects the channel to which the policy is to be applied.	(None)

NOTE

If APs using the same channels as those registered are detected
- they will be recognized as normal, so no event is generated.

If APs using unregistered channels are detected
- they will be recognized as AP violating the policy, so an event is generated.

Data rate

Only APs using the data rate registered in the list will be accepted as normal; if APs using unregistered data rates are detected, an event is generated.

Policy settings > Detection Block policy > Profile settings > Managed AP policy > Add > Data rate

Figure 112. Managed AP policy-Data rate

Input Item	Description	Effective Value (Default)
Data rate	Prints out the screen for selecting **'Data rate.'**	
Data rate /MCS set	Selects the data rate / MCS set to be applied as policy.	

NOTE

If an AP using the same data rate as the registered rate is detected
- it will be recognized as a normal AP, so no event is generated.

If an AP using unregistered data rates is detected
- it will be recognized as an AP violating the policy, so an event is generated.

3.3.3 Operation policy

This sets the operation policies for managed APs.

Policy settings > Detection Block policy > Operation policy

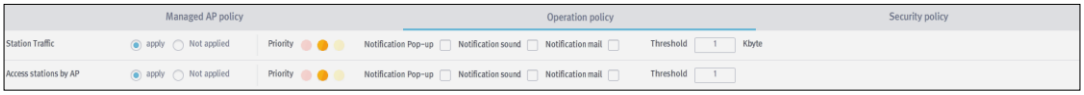


Figure 113. Operation policy

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for notification pop-ups in the case of an event.	Checked/Unchecked (Checked)
Notification sound	Sets the options for using notification sounds in the case of an event.	Checked/Unchecked (Checked)
Notification mail	Sets the options for using notification mail in the case of an event.	Checked/Unchecked (Checked)
Threshold	Sets the threshold of notifications for an event. − Traffic for a station by time (Kbyte)	Number 1~999999 (50000)
	Sets the threshold of notifications for an event. − The number of connected stations by AP (unit)	Number 1~999 (10)

NOTE

Traffic for a station by time

- Station traffic surpassing the hourly set threshold will be detected.
  Ex) if the threshold is set to 1000 Kbytes, a station generating traffic exceeding 1000 Kbytes for an hour will be detected.

The number of connected stations by AP

- AP for which the number of station connections by AP surpasses the predefined threshold will be detected.
  Ex) Detecting an AP connected to 6 or more stations when the threshold is set to 5.

3.3.4 Security policy

The security policy should be set in order to detect and cope with security risks on the wireless network.

Unauthorized AP

The security policy related to unauthorized AP is to be set.

Policy settings > Detection Block policy > Profile settings > Security policy > Unauthorized AP

Figure 114. Security policy-Unauthorized AP

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)

- Rogue AP

Input Item	Description	Effective Value (Default)
Wired connection block	The configuration should ensure the switch port a Rogue AP is connected to can be blocked. − It is applied to the switch registered to [Preferences > wired switch setting]. − Is activated only if the option for automatic block is selected.	Checked/Unchecked (Unchecked)

- Unmanaged AP

Input Item	Description	Effective Value (Default)
Unclassified External AP block	Sets the reference signal intensity for giving a notification or blocking unmanaged APs − The policy is only applied if the signal intensity is stronger than the predefined criterion.	-90 ~ -10 (-50)
Signal intensity	Sets the reference signal intensity for giving a notification or blocking unmanaged APs − The policy is only applied if the signal intensity is stronger than the predefined criterion.	-90 ~ -10 (-50)
Exception	Sets the targets to be excluded from the policy. − Even if the signal intensity is stronger than the predefined value, the excluded connection type is not subject to policy application.	WDS/ WIFI-Direct / WDS+WIFI-Direct (Unused)

Flooding Attack

This sets the security policy in regards to a flooding attack.

Policy settings > Detection Block policy > Profile settings > Security policy > Flooding Attack

Figure 115. Security policy-Flooding Attack

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. – Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Threshold (the number of packets every 10 seconds)	Sets the threshold of notifications for the event.	Number 1~9999 (0)

Station management

This sets the security policy related to the management of a station.

Policy settings > Detection Block policy > Profile setting > Security policy > Station management

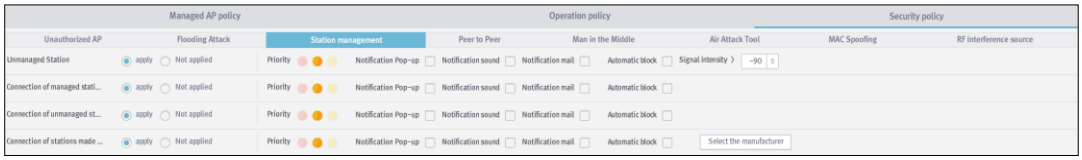


Figure 116. Security policy-Station management

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Degree of Priority	Sets the degree of priority of an event. – Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)

If the policy for **'Connection of stations made by certain manufacturers to managed APs'** is checked as 'Used,' the screen for selecting the option of the manufacturer OUI of a station will be displayed.

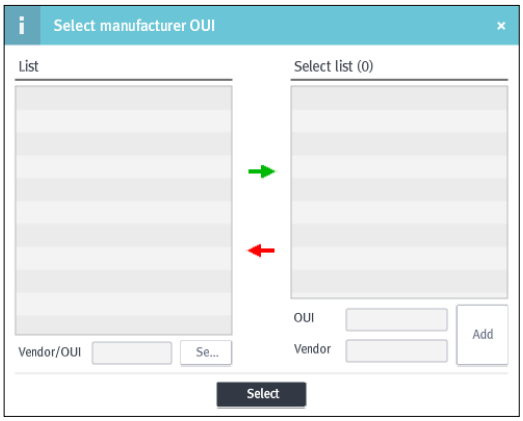


Figure 117. Select Manufacturer OUI

Peer to Peer

This sets the security policy regarding Peer to Peer.

Policy settings > Detection Block policy > Profile settings > Security policy > Peer to Peer

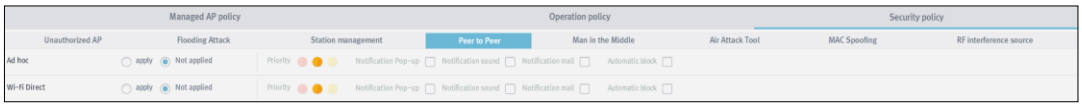


Figure 118. Security policy-Peer to Peer

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. - Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)

Man in the Middle

This sets the security policy regarding Man in the Middle.

Policy settings > Detection Block policy > Profile settings > Security policy > Man in the Middle

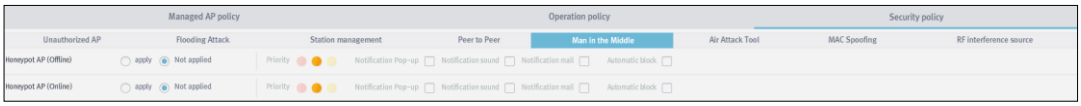


Figure 119. Security policy-Man in the Middle

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)

Air Attack Tool

This sets the security policy regarding the Air Attack Tool.

Policy settings > Detection Block policy > Profile settings > Security policy > Air Attack Tool

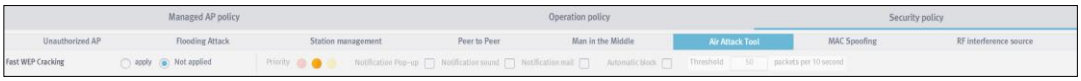


Figure 120. Security policy-Air Attack Tool

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)
Threshold (the number of packets every 10 seconds)	Sets the threshold of notification for the event.	Number 1~9999 (0)

MAC Spoofing

This sets the security policy regarding MAC Spoofing.

Policy settings > Detection Block policy > Profile settings > Security policy > MAC Spoofing

Figure 121. Security policy-MAC Spoofing

- Common issues

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. – Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)
Automatic block	Sets the options for using the automatic blocking function in the case of policy violations.	Checked/Unchecked (Unchecked)

RF interference source

This sets the security policy regarding an RF interference source.

Policy settings > Detection Block policy > Profile settings > Security policy > RF interference source

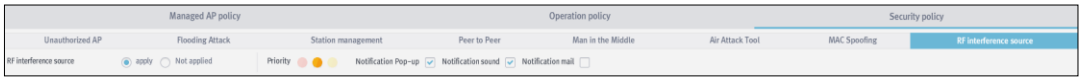


Figure 122. Security policy-RF interference source

Input Item	Description	Effective Value (Default)
Apply/Not applied	Sets the options for using the policy.	Apply/Not applied (Not applied)
Priority	Sets the degree of priority of an event. − Red: HIGH, Orange: MEDIUM, Yellow: LOW	Green/Yellow/Red (Yellow)
Notification Pop-up	Sets the options for using notification pop-up windows in the case of an event.	Checked/Unchecked (Unchecked)
Notification sound	Sets the options for using the notification sounds in the case of an event.	Checked/Unchecked (Unchecked)
Notification email	Sets the options for using the notification email in the case of an event.	Checked/Unchecked (Unchecked)

CHAPTER 4. Monitoring

This chapter explains the methods of setting the environment for monitoring the operational status of WES and of making inquiries about a number of statuses and records. Monitoring includes the functions of setting and making inquiries about a device's status, events/logs, statistics/reports, dashboard, and integrity check, etc.

4.1 Overview

WES compiles a variety of logs during operation and provides a number of events and statistics as well as monitoring functions so as to ensure quick coping with abnormal situations and for an administrator to check the network status on a periodic basis.

WES can make inquiries about information regarding AP by AP status, check a number of security risks and system status by way of events/logs, and perform the tasks of creating reports on stations connected to the network and their traffic by statistics and reports from the inquiries. It can also monitor the overall situation of the network in real time through the dashboard.

4.2 Status of AP

WES is synchronized with a number of AP. For the efficient management of each AP, it provides the function of making inquiries on AP status.

4.2.1 AP management

Status of managed AP connection

Inquiries can be made regarding the connection status of stations connected to managed AP.

Network > AP management > Status of managed AP connection

Figure 123. Status of managed AP connection

Connection status can be verified for 7 items, such as the List of APs/Number of station by AP time/Number of authentication attempts by AP time/Number of station by channel (2.4 GHz)/Number of station by channel (5 GHz)/Number of stations by protocol and Numberof station by encryption method. It can also make inquiries about information on different
dates when a specific date is selected.

If you select a particular AP in the list, you may view only the information on that AP. In order to return to the overall status, click the **[Initialize]** button.

In the item of **Number of station by AP time**, you may view the number of connected stations by hour per a managed AP and the accumulated value as a whole.

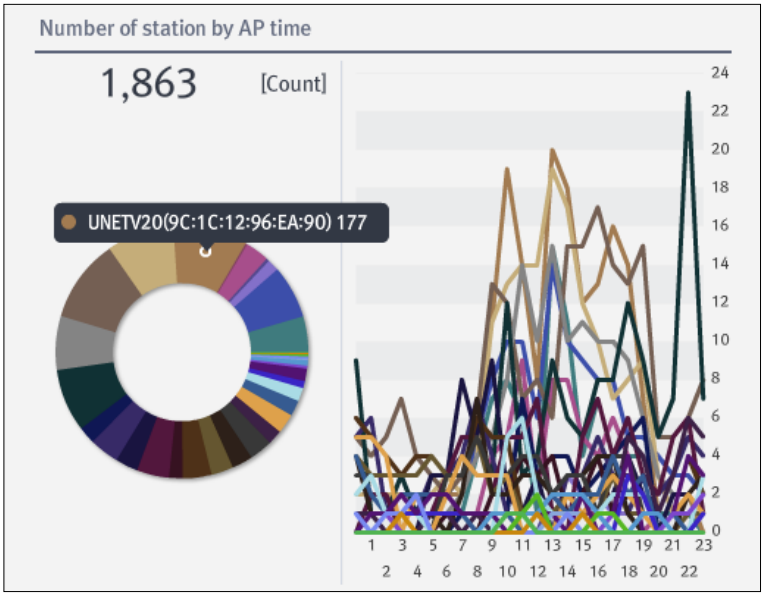


Figure 124. The accumulated number of stations by AP time / Number of connected stations per hour

If you place the mouse cursor over each point on the graph, 'SSID (BSSID) and the accumulated value of the number of connected station' in a phi graph and 'SSID (BSSID), time, and the number of connected station' in a line graph will be displayed; if you double-click it, you may view AP information.

In the item of **Number of authentication attempts by AP time,** you may view the number of authentication attempts by a managed AP and the accumulated value as a whole.

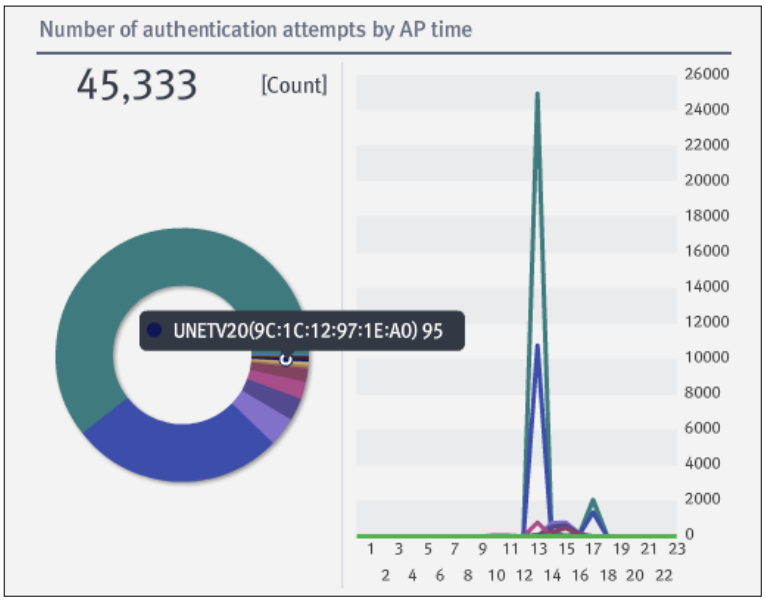


Figure 125. The # of authentication attempts by managed AP / # of authentication attempts per hour

If you place the mouse cursor over each point on the graph, 'SSID (BSSID) and the accumulated value of the number of connected station' in a phi graph and 'SSID (BSSID), time, and the number of connected station' in a line graph will be displayed; if you double-click it, you may view AP information.

In the item of **Number of stations by channel (2.4 GHz)**, you may view the number of connected stations by channel at 2.4 GHz bandwidth among the station connected to the AP.

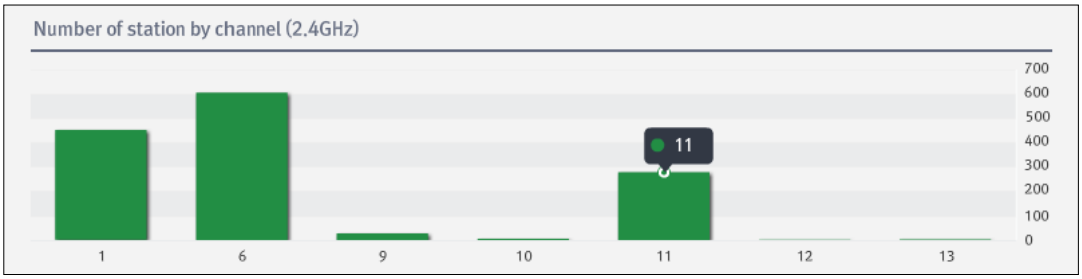


Figure 126. Number of stations by channel (2 GHz, 802.11b/g/n)

In the item of **Number of stations by Channel (5 GHz)**, you may view the number of connected stations by channel at 5 GHz bandwidth among the station connected to the AP.

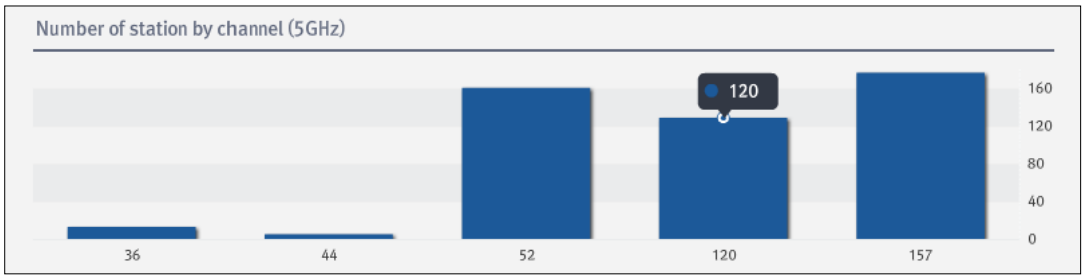


Figure 127. Number of stations by Channel (5 GHz, 802.11a/n)

In the item of **Number of stations by protocol**, you may view the ratio and the number of connected stations by channel among the ones connected to the AP.

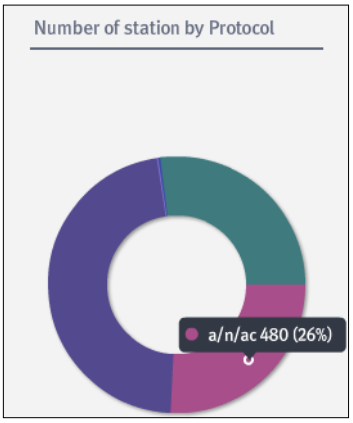


Figure 128. Number of stations by protocol

If you place the mouse cursor over each point on the graph, you may view the information on 'protocol, the number of cases, and ratio.'

In the **Number of stations by encryption method** item, you may view the ratio and the number of connections by encryption method among those connected to the AP.

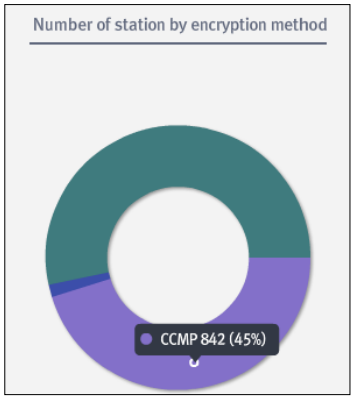


Figure 129. Number of station by encryption method

If you place the mouse cursor over each point on the graph, you may view information on encryption method, the number of cases, and ratio.

Status of managed AP traffic

From all of the managed AP, you may make inquiries about the volume of outgoing and incoming data.

Network > AP management > Status of managed AP traffic

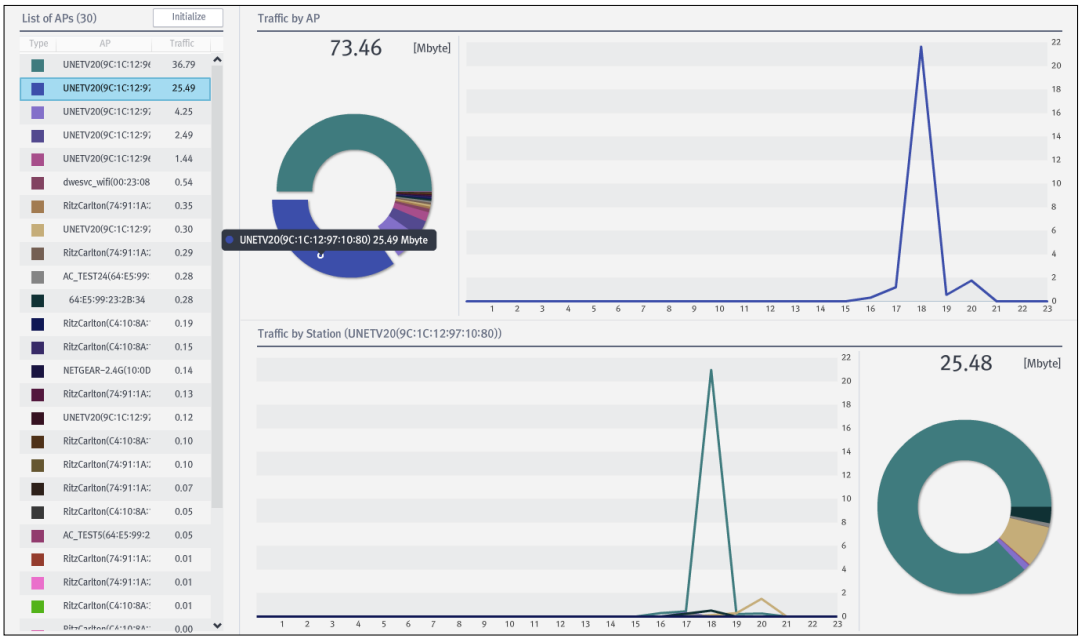


Figure 130. Status of managed AP traffic (all managed APs)

You may view the traffic status for 3 items, such as the List of APs, traffic by AP, and an AP's detailed traffic; you can make inquiries about the information on any date you want by selecting a specified date.

If you select a particular AP in the list, you may view only the information on that AP; in order to return to the overall status, click the **[Initialize]** button.

In the item, **Traffic by AP**, you may view the data volume for all AP in a phi/line graph with time slots.

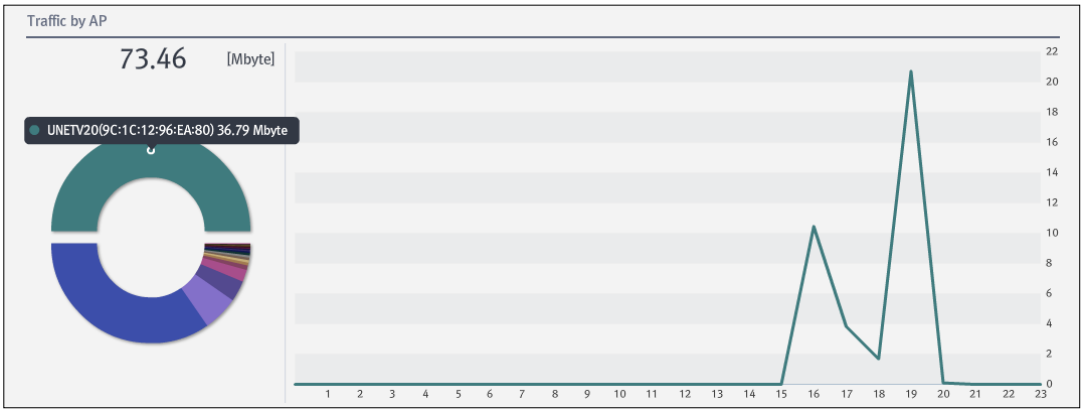


Figure 131. Traffic volume by AP

If you place the mouse cursor over any point on the graph, 'SSID (BSSID) and the accumulated value of traffic volume' in a phi graph and 'SSID (BSSID), time, and traffic volume' in a line graph will be displayed; if you double-click on it, you may view AP information.

In the item of **Traffic by Station**, you may view the traffic volume for a selected Station in a line/phi graph.

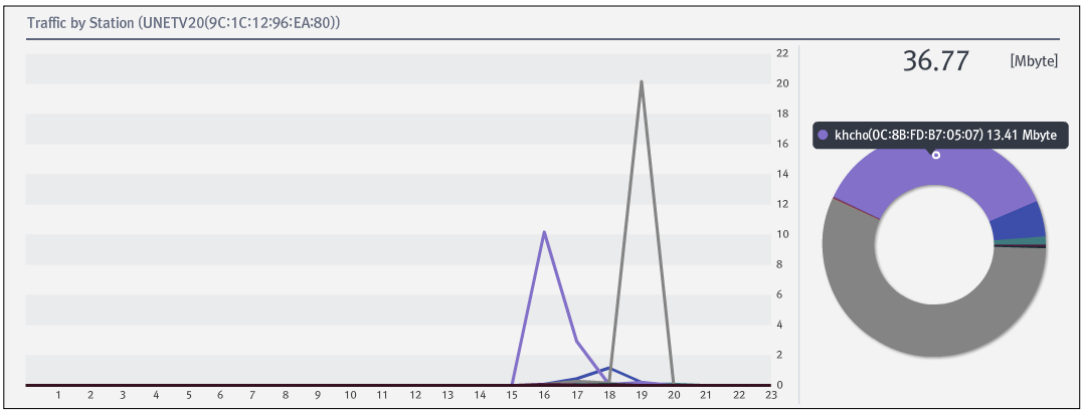


Figure 132. Traffic volume by Station (Line/Phi graph)

If you place the mouse cursor over any point on the graph, 'EAPID, MAC address, and the accumulated value of traffic volume' in a phi graph and 'EAPID, MAC address, time, and traffic volume' in a line graph will be displayed; if you double-click on the graph, you may view Station information.

4.3 Event / Log

WES creates a number of events and logs (records of inspection) during its operation. By checking and analysing these created events / logs, an administrator can understand and solve a number of problems which may occur or have already occurred. This chapter introduces the various kinds of logs created in WES and the methods for making inquiries.

4.3.1 List of events

You can make inquiries about a number of events that occur during the operation of WES.

Event / Log > Event > List of events

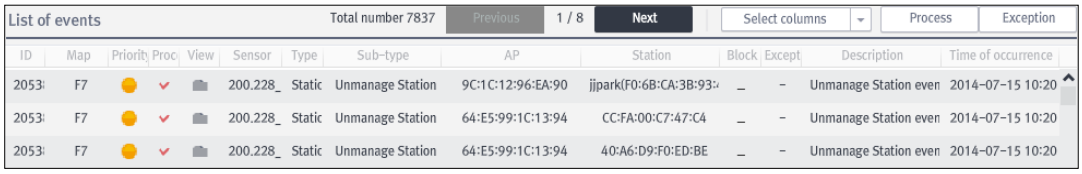


Figure 133. List of events

You may search the items as you wish with a variety of search criteria. The search criteria are as follows:

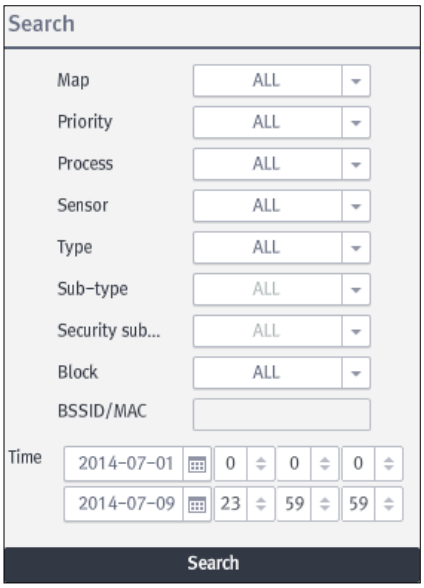


Figure 134. List of events-By search criteria

Input Item	Description	Effective Value (Default)
Map	Selects the map on which events are generated.	List of registered maps (All)
Priority	Selects the degree of priority for an event.	HIGH/MEDIUM/LOW (All)
Process	Selects the options for processed an event.	Processed/unprocessed (All)
Sensor	Selects the sensor for detecting events.	List of the registered sensors (All)
Type	Selects the types of events.	Managed AP/operation/security (All)
Sub-type	Selects the sub-type by event type.	**Managed AP:** SSID/Protocol/Encryption/ Manufacturer/Authentication/Channel/SSID Broadcast/Data rate (All) **Operation:** Traffic by time per station/The number of connected stations by AP (All) **Security:** Unauthorized AP/Flooding Attack/ Management of stations/Peer to Peer/ Man in the Middle/Air Attack Tool/MAC Spoofing/RF interference source (All)
Security sub-type	Selects the sub-type of security event. −This is used only when the specified type is security.	**Unauthorized AP:** Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack:** Association/Disassociation/ Disassociation Broadcast/Authentication/ Deauthentication/Deauthentication Broadcast/ Probe Request/RTS/CTS/EAPOL-Start/ EAPOL-Logoff/PS-Poll (All) **Station management:** Unmanaged stations/ Connection of managed stations to unmanaged APs/Connection of unmanaged stations to managed APs/connection of stations made by certain manufacturers to managed APs (All) **Peer to Peer:** Ad-hoc/WiFi-Direct (All) **Man in the Middle:** Honeypot AP (Offline)/ HoneypotAP (Online) (All) **Air Attack Tool:** Fast WEP Cracking (All) **MAC Spoofing:** AP MAC Spoofing/STA MAC Spoofing (All) **RF interference source:** RF interference source (All)
Block	Inserts information on blocking.	Normal/Blocked (All)
BSSID/MAC	Inserts information on BSSID or MAC.	1~17 characters (None)
Time	Selects the target date for a search.	(Present date)

The default value of search criteria are Search (All); in order to search all after a search for an individual criterion, you should make inquiries after choosing 'All' for all of the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
ID	Prints out the number of the event occurrence.
Map	Prints out information on the map where the event occurred.
Priority	Prints out the degree of priority for an event (HIGH: Red, MEDIUM: Yellow, LOW: Green).
Process	Prints out the status of processed of an event (Processed: Green, Unprocessed: Red)
Read	Prints out the status of reading an event (read: Yellow, unread: Grey)
Sensor	Prints out information on the sensor for detecting an event.
Type	Prints out the event type.
Sub-type	Prints out the sub-type by event type: **Managed AP:** Managed AP **Operation:** Traffic of stations/the number of AP station **Unauthorized AP (security)**: Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack (security):** Association/Disassociation/Disassociation Broadcast /Authentication/Deauthentication/Deauthentication/Broadcast /Probe Request/RTS/CTS/EAPOL-Start/EAPOL-Logoff/PS-Poll (All) **Station management(security):** Unmanaged stations/Connection of managed stations to unmanaged AP/Connection of unmanaged stations to managed AP/Connection of stations made by certain manufacturers to managed AP (All) **Peer to Peer (security):** Ad-hoc/WiFi-Direct (All) **Man in the Middle (security):** Honeypot AP (Offline)/HoneypotAP(Online) (All) Air Attack Tool (security): Fast WEP Cracking (All) **MAC Spoofing (security):** AP MAC Spoofing/STA MAC Spoofing (All) RF interference source (security): RF interference source (All)
AP	Prints out information on the SSID (BSSID) of the AP generating an event.
Station	Prints out information on the MAC address of the station generating an event. −In the case of synchronization with the Anyclick AUS server, the information on EAPID will be displayed as well; otherwise, only MAC information will be displayed.
Block	Prints out the status of blocking a station / AP generating an event.
Exception	Prints out the status of exceptions in the event.
Description	Prints out a description of the event.
Time of occurrence	Prints out the date of the event.

[Search window]: Selects the option to display the window for inserting search criteria.

[Refresh]: Updates the list of events.

[Event page]: Selects a page when a large amount of information is displayed on screen.

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

[Process]: Processes the selected event.

[Exception]: Makes an exception for the selected event.

If you select and double-click a particular event, the information on the event will be displayed.

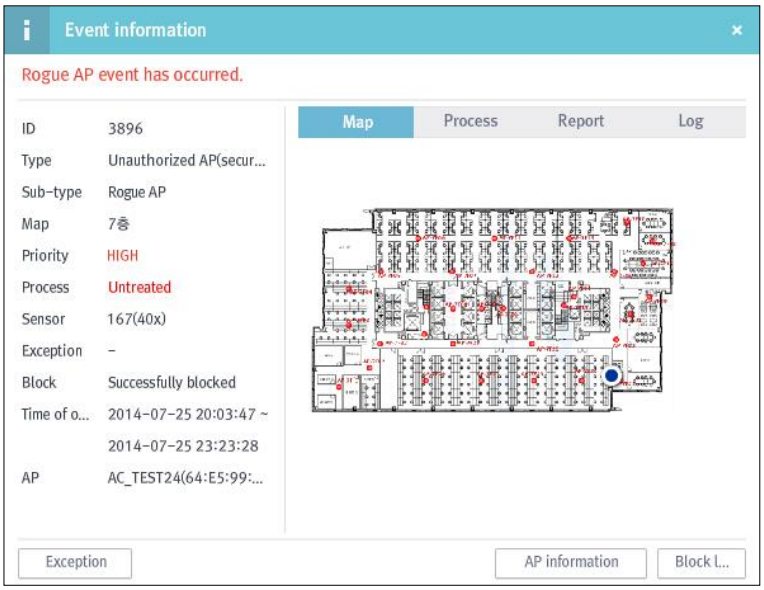


Figure 135. Event information

Output item	Description
ID	Prints out the number of an event.
Type	Prints out the type of event.
Sub-type	Prints out the sub-type by event type: **Managed AP:** Managed AP **Operation:** Traffic of stations/the number of AP station **Unauthorized AP (security)**: Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack (security):** Association/Disassociation/Disassociation Broadcast Authentication/Deauthentication/Deauthentication/Broadcast Probe Request/RTS/CTS/EAPOL-Start/EAPOL-Logoff/PS-Poll (All) **Station management(security):** Unmanaged stations/Connection of managed stations to unmanaged AP/Connection of unmanaged stations to managed AP/Connection of stations made by certain manufacturers to managed AP (All) **Peer to Peer (security):** Ad-hoc/WiFi-Direct (All) **Man in the Middle (security):** Honeypot AP (Offline)/HoneypotAP(Online) (All) Air Attack Tool (security): Fast WEP Cracking (All) **MAC Spoofing (security):** AP MAC Spoofing/STA MAC Spoofing (All) **RF interference source (security):** RF interference source (All)
Map	Prints out information on the map where the event occurred.
Priority	Prints out the degree of priority of the event (HIGH: Red, MEDIUM: Yellow, LOW: Green).
Process	Prints out the status of processed the event (Processed: Green, Unprocessed: Red)
Sensor	Prints out information on the sensor detecting the event.
Exception	Prints out the status of whether the event has been excluded.
Block	Prints out the status of whether the station/AP generating the events are blocked.
Time of occurrence	Prints out the date on which the event occurred.
AP/Station	Prints out information on the SSID (BSSID)/MAC of the AP or station generating the event.
Exception	Processes exceptions to the event.
AP information/ Station information	Prints out information on the AP/station generating the event.
Block log	Prints out information on the logs of blocked AP/station.

On the tab for **[Map]**, you may view the locations of the AP or station generating the event.

On the tab for **[Process]**, you may insert the processed result of the event.

On the tab for **[Report]**, you may designate the recipient for reporting the occurrence of the event.

4.3.2 List of exceptional events

Events requiring management among a number of events during the operation of WES can be registered in the list of exceptional events.

Event/Log > Event > List of exceptional events

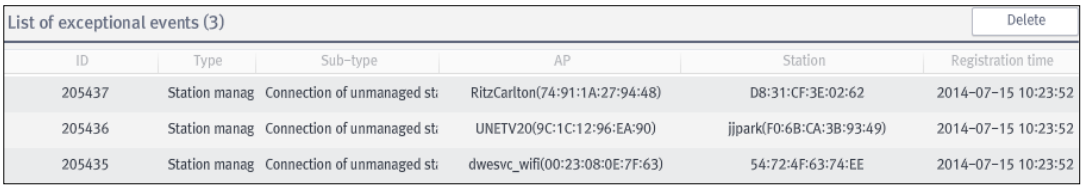


Figure 136. List of exceptional events

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
ID	Prints out the number of the event.
Type	Prints out the event type.
Sub-type	Prints out the sub-type by event type: **Managed AP:** Managed AP **Operation:** Traffic of stations/the number of AP station **Unauthorized AP (security)**: Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack (security):** Association/Disassociation/Disassociation Broadcast Authentication/Deauthentication/Deauthentication/Broadcast Probe Request/RTS/CTS/EAPOL-Start/EAPOL-Logoff/PS-Poll (All) **Station management(security):** Unmanaged stations/Connection of managed stations to unmanaged AP/Connection of unmanaged stations to managed AP/Connection of stations made by certain manufacturers to managed AP (All) **Peer to Peer (security):** Ad-hoc/WiFi-Direct (All) **Man in the Middle (security):** Honeypot AP (Offline)/HoneypotAP(Online) (All) Air Attack Tool (security): Fast WEP Cracking (All) **MAC Spoofing (security):** AP MAC Spoofing/STA MAC Spoofing (All) **RF interference source (security):** RF interference source (All)
AP	Prints out information on the SSID (BSSID) of the AP generating the event.
Station	Prints out information on the MAC address of the station generating the event.
Registration Time	Prints out the time when the event was registered as being exceptional.

In order to delete the registered list of exceptional events, select the event to be deleted and click the **[Disable]** button.

[Refresh]: Updates the list of exceptional events.

4.3.3 List of processed events

You may make inquiries about the list of the events processed by an administrator among a number of events generated during the operation of WES.

Event/Log > Event > List of processed event

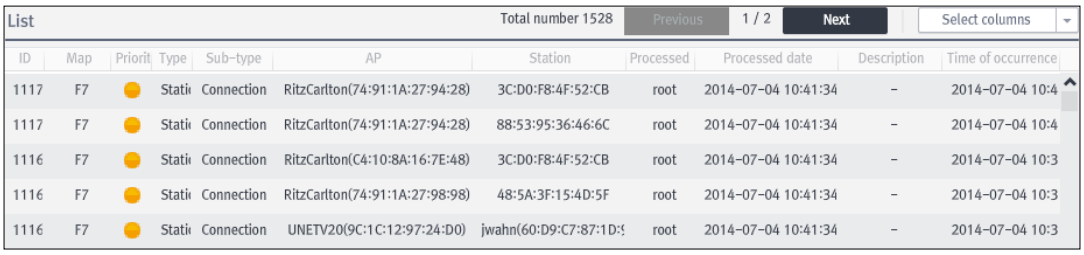


Figure 137. List of processed events

Depending on various search criteria, you may search for the items you want; the search criteria are as follows:

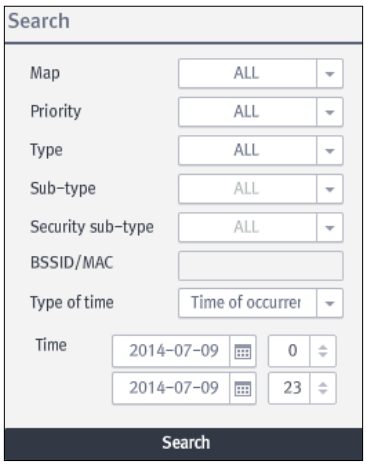


Figure 138. List of processed events-By search criteria

Input Item	Description	Effective Value (Default)
Map	Selects the map on which events are generated.	List of the registered maps (All)
Priority	Selects the degree of priority for an event.	HIGH/MEDIUM/LOW (All)
Type	Selects the type of events.	Managed AP/operation/security (All)
Sub-type	Selects the sub-type by event type.	**Managed AP:** SSID/Protocol/Encryption/ Manufacturer/Authentication/Channel/SSID Broadcast/Data rate (All) **Operation:** Traffic by time per station/The number of connected stations by AP (All) **Security:** Unauthorized AP/Flooding Attack/ Management of stations/Peer to Peer/ Man in the Middle/Air Attack Tool/MAC Spoofing/RF interference source (All)
Security Sub-type	Selects the sub-type of security event. - This is used only when the specified type is security.	**Unauthorized AP:** Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack:** Association/Disassociation/ Disassociation Broadcast/Authentication/ Deauthentication/Deauthentication Broadcast/ Probe Request/RTS/CTS/EAPOL-Start/ EAPOL-Logoff/PS-Poll (All) **Station management:** Unmanaged stations/ Connection of managed stations to unmanaged APs/Connection of unmanaged stations to managed APs/connection of stations made by certain manufacturers to managed APs (All) **Peer to Peer:** Ad-hoc/WiFi-Direct (All) **Man in the Middle:** Honeypot AP (Offline)/ HoneypotAP (Online) (All) **Air Attack Tool:** Fast WEP Cracking (All) **MAC Spoofing:** AP MAC Spoofing/STA MAC Spoofing (All) **RF interference source:** RF interference source (All)
BSSID/ MAC	Inputs information on the AP/station.	1~17 characters (None)
Type of time	Selects the type of time.	Time of occurrence/Processed time (Time of occurrence)
Time	Selects the targeted date for search.	(Present date)

The default value of search criteria are Search (All); in order to search all after a search for an individual criterion, you should make inquiries after choosing 'All' for all of the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
ID	Prints out the number of a generated event.
Map	Prints out information on the map on which an event is generated.
Priority	Prints out the degree of priority (HIGH: Red, MEDIUM: Yellow, LOW: Green).
Type	Prints out the type of event.
Sub-type	Prints out the sub-type by event type: **Managed AP:** Managed AP **Operation:** Traffic of stations/the number of AP station **Unauthorized AP (security)**: Rogue AP/Unmanaged AP/WDS/Wi-Fi Tethering AP (All) **Flooding Attack (security):** Association/Disassociation/Disassociation Broadcast Authentication/Deauthentication/Deauthentication/Broadcast Probe Request/RTS/CTS/EAPOL-Start/EAPOL-Logoff/PS-Poll (All) **Station management(security):** Unmanaged stations/Connection of managed stations to unmanaged AP/Connection of unmanaged stations to managed AP/Connection of stations made by certain manufacturers to managed AP (All) **Peer to Peer (security):** Ad-hoc/WiFi-Direct (All) **Man in the Middle (security):** Honeypot AP (Offline)/Honeypot AP(Online) (All) Air Attack Tool (security): Fast WEP Cracking (All) **MAC Spoofing (security):** AP MAC Spoofing/STA MAC Spoofing (All) **RF interference source (security):** RF interference source (All)
AP	Prints out information on the SSID (BSSID) of the AP generating an event.
Station	Prints out information on the user MAC address of the station generating an event. − Prints out information on the EAPID in the case where there is synchronization with an Anyclick AUS server; otherwise, it prints out the information only on the MAC.
Processed account	Prints out information on the account that processed the event.
Processed date	Prints out the date when an event was processed.
Description	Prints out description on processed the event.
Time of occurrence	Prints out the time when an event occurs.

[Search window]: Selects the option to display the window for inserting search criteria.

[Refresh]: Updates the list of processed events.

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

4.3.4 List of administrator logs

You can make inquiries about the results of tasks performed by an administrator.

Event / Log > Log > List of administrator logs

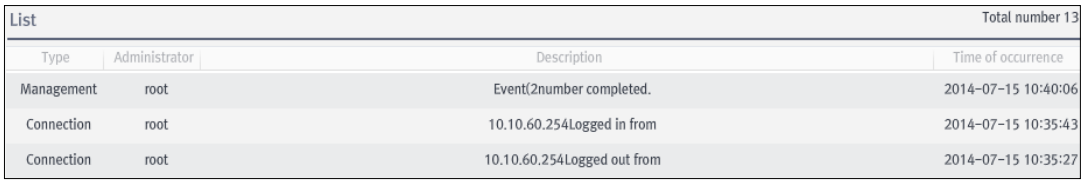


Figure 139. List of Administrator logs

[CSV Export]: Saves the output status in the form of a CSV file on the local PC by specifying the path.

You can search for wanted items with various search criteria; the search criteria are as follows:

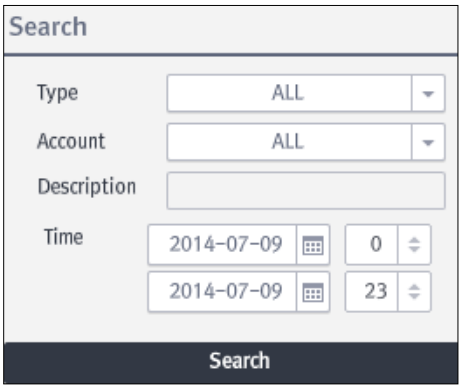


Figure 140. List of Administrator logs-By search criteria

Input Item	Description	Effective Value (Default)
Type	Selects the type of administrator log.	Connection/Policy/Management (All)
Account	Selects the administrator account.	List of registered accounts (ALL)
Description	Selects details of the search.	1~17 characters (None)
Time	Selects the target date for a search.	Past ~ Present (Present Date)

The default value of search criteria are Search (All); in order to search all after a search for an individual criterion, you should make inquiries after choosing 'All' for all of the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Type	Prints out the type of task. - Connection: Prints out only the details related to the web console connection. - Policy: Prints out only the details related to the policies for managed AP/operation/ security. - Management: Prints out all of the details excluding those related to connection/policy.
Account	Prints out information on the administrator performing the task.
Description	Prints out the details of a task.
Time of occurrence	Prints out the time when a log is generated.

4.3.5 List of block logs

You may make inquiries about the information on blocked stations / APs after the result of the performed task.

Event / Log > Log > List of block logs

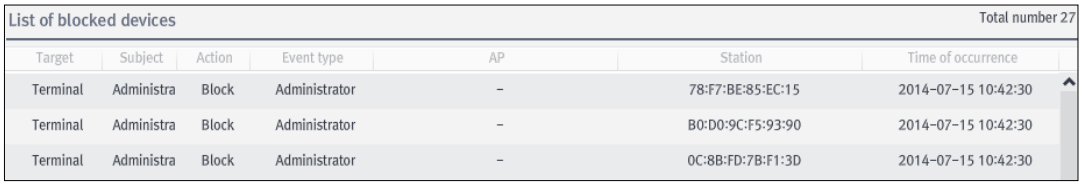


Figure 141. List of block logs

[CSV Export]: Saves the output status in the form of a CSV file on the local PC by specifying the path.

You can search for wanted items with various search criteria; the search criteria are as follows:

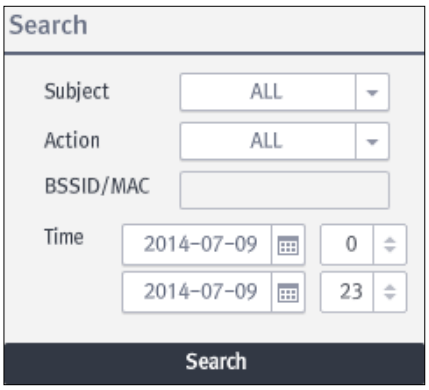


Figure 142. List of block logs-By search criteria

Input Item	Description	Effective Value (Default)
Subject	Selects information on subjects blocking stations or AP.	Server/Administrator/ Sensor (All)
Action	Selects information on the blocking action.	Block/Unblock (All)
BSSID/MAC	Inserts information on BSSID/MAC.	1~17 characters (None)
Time	Selects the target date for a search.	Past-Present (Present date)

The default value of search criteria are Search (All); in order to search all after a search for an individual criterion, you should make inquiries after choosing 'All' for all of the search criteria.

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description

Target	Prints out the target to block.
Subject	Prints out information on the subject blocking stations or APs.
Action	Prints out information on the blocking action.
Event Type	Prints out information on the event related to blocking.
AP	Prints out information on the SSID of the target AP.
Station	Prints out information on the MAC address of the target station.
Time of occurrence	Prints out the time when stations or AP are blocked.

[Search window]: Selects the option to display the window for inserting search criteria.

[Refresh]: Updates the list of processed events.

4.3.6 List of system logs

You may make inquiries about the logs on the status of connection to the sensor (successful/failed).

Event / Log > Log > List of system logs

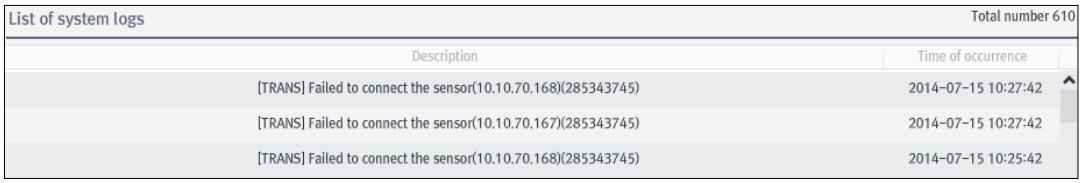


Figure 143. List of system logs

Depending on various search criteria, you may search for wanted items; the search criteria are as follows:

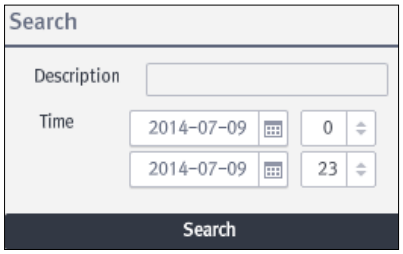


Figure 144. List of system logs-By search criteria

Input Item	Description	Effective Value (Default)
Description	Selects the details of a search.	1~17 characters
Time	Selects the target date for a search.	(Present date)

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Description	Prints out details of the log.
Time of occurrence	Prints out the time when the log was generated.

[Search window]: Selects the option to display the window for inserting search criteria.

[Refresh]: Updates the list of processed events.

4.4 Report

WES provides the function of generating reports for various events which occur during its operation. This chapter explains the methods of creating reports or setting the automatic creation of reports, etc.

4.4.1 Reports management

Generate reports

This generates reports with various conditions.

Reports > Generate reports

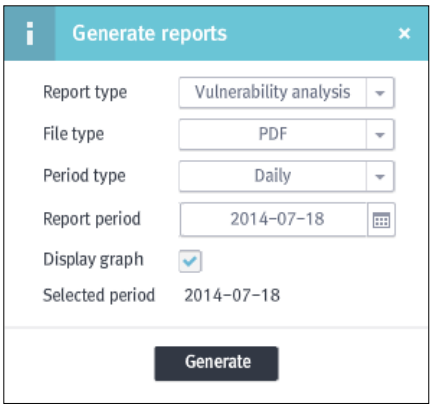


Figure 145. Generate reports

Input Item	Description	Effective Value (Default)
Report type	Selects the type of report to be generated.	Vulnerability analysis/ Record of occurrence of an event/ Record of the processing of an event (Vulnerability analysis)
File type	Selects the extension of a file for the form in which a report is to be saved.	PDF/PPT/HTML/CSV/ RTF/XML (PDF)
Period type	Selects the type of period during which the data of reports are collected. − **Daily basis:** Includes data on the target date. **Weekly basis:** Includes data for 7 days from one day before the target date. **Monthly basis:** Includes all data from the month when the target date is included.	Daily/Weekly/Monthly (Daily)
Report period	Choose the reference date when the report is generated.	(Present date)
Display graph	Selects the option for graphic representation.	Checked/Unchecked (Checked)
Selected period	Prints out information on the selected date.	-

Once you are done with inserting the criteria for generating the report, click the **[Generate report]** button to generate a report; the generated report will be registered to the list of reports.

Download and Deletion of a Report

You may download the generated report to your local PC or delete it.

Reports > List of reports

Figure 146. List of reports

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Report type	Prints out the types of reports.
File type	Prints out information on the report file type.
Period type	Prints out the period type of a report.
Report period	Prints out the period during which data in the report are collected.
Generation type	Prints out information on the type of subject (administrator: manual, server: automatic) generating a report.
Registration time	Prints out the time a report was created.

In order to save a report to your local PC, select the report to be saved from the list and click the **[Save files]** button at the top.

In order to delete a report file, select the report to be deleted from the list and click the **[Delete files]** button at the top.

Auto generation reports

Automatically generate the report by report type/file type/period type/date.

Reports > Automatically generated reports > Add

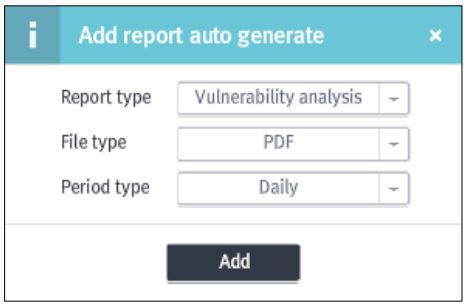


Figure 147. Add report auto generate

Input Item	Description	Effective Value (Default)
Report type	Selects the type of report to be generated.	Vulnerability analysis/ Record of occurrence of an event/ Record of the processing of an event (Vulnerability analysis)
File type	Selects the extension of a file for the form in which a report is to be saved.	PDF/PPT/HTML/CSV/ RTF/XML (PDF)
Period type	Selects the type of period during which the data of reports are collected. - **Daily basis:** Includes data on the target date. **Weekly basis:** Includes data for 7 days from one day **Before** the target date. **Monthly basis:** Includes all data from the month when the target date is included.	Daily/Weekly/Monthly (Daily)

The results of inquiries are displayed as follows, and each item can be sorted out in consecutive (ascending or descending) order.

Output item	Description
Report type	Prints out the types of reports.
File type	Prints out information on the report file type.
Period type	Prints out the period type of a report.
Registration time	Prints out the time a report was created.

[Modify]: After selecting the report settings to be modified in the automatically generated reports list, click the **Modify** button at the top. Once the screen for modifying the Modify report auto generate is displayed, modify the details.

[Delete]: After selecting the report settings to be deleted from the automatically generated reports list, click the **Delete** button at the top.

4.5 Statistics

WES provides a number of functions of statistics. If some problems occur in the network, the source of the problems can be found by using these functions to analyse patterns and infer the action. This chapter explains the methods of using a number of functions of statistics provided by WES.

4.5.1 Number of connected stations to the managed AP

You may make inquiries about the statistics of the station connected to each station for the designated period.

Statistics > Number of connected stations to the managed AP

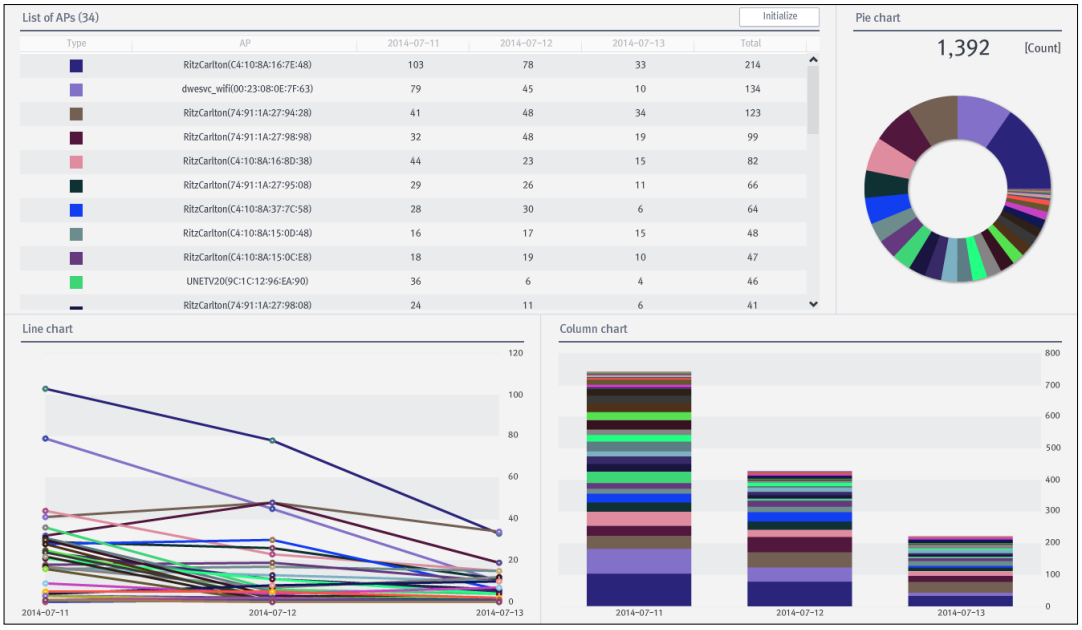


Figure 148. Number of connected stations to the managed AP

Depending on the search criteria at the top, you may search for items as you wish.

Input Item	Description	Effective Value (Default)
Date	Selects the date on which you want to make inquiries about the statistics(Sets the conditions by type of Year/Month/Day.).	(Present date)

Select the AP you want from the list of APs or graph to see the statistics on the selected AP. To see the total statistics, click the **[Initialize]** button.

4.5.2 Traffic for managed AP

You may make inquiries on the statistics for the volume of outgoing and incoming traffic for managed AP for a designated period.

Statistics > Traffic for managed AP

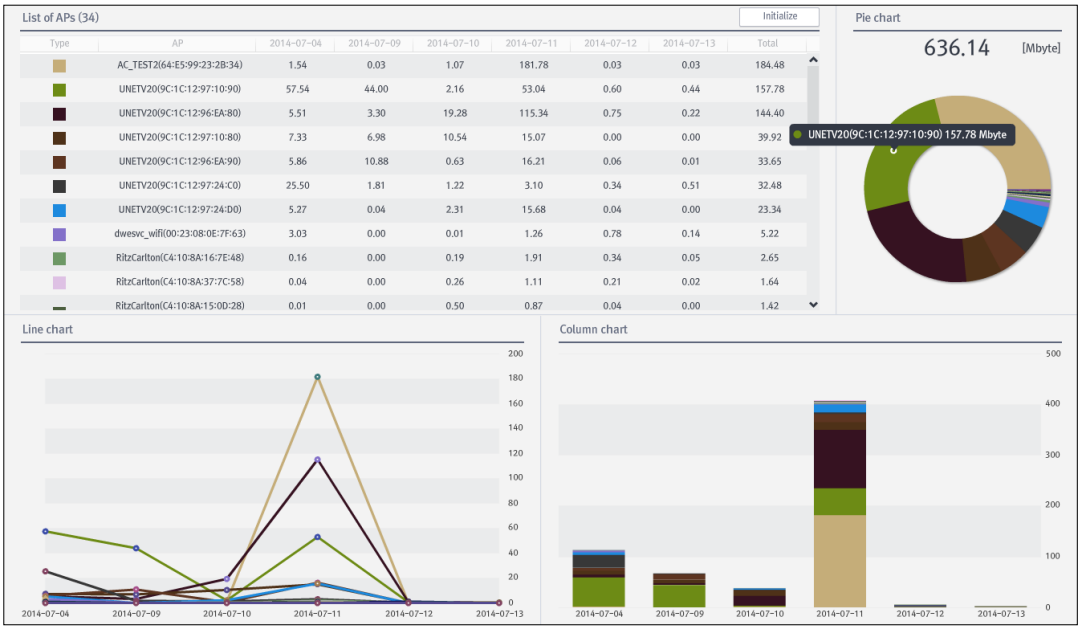


Figure 149. Traffic for managed AP

Depending on the search criteria at the top, you may search for items as you wish.

Input Item	Description	Effective Value (Default)
Date	Selects the date of inquiries made about the statistics. (Sets the conditions by type of Year / Month / Day.)	(Present date)

Select the AP you want from the list of APs or graph to see the statistics on the selected AP. To see the total statistics, click the **[Initialize]** button.

4.5.3 Traffic for the each managed AP

You may make inquiries about the statistics for the traffic volume of the connected stations by each AP for a designated period.

Statistics > Traffic for the each managed AP

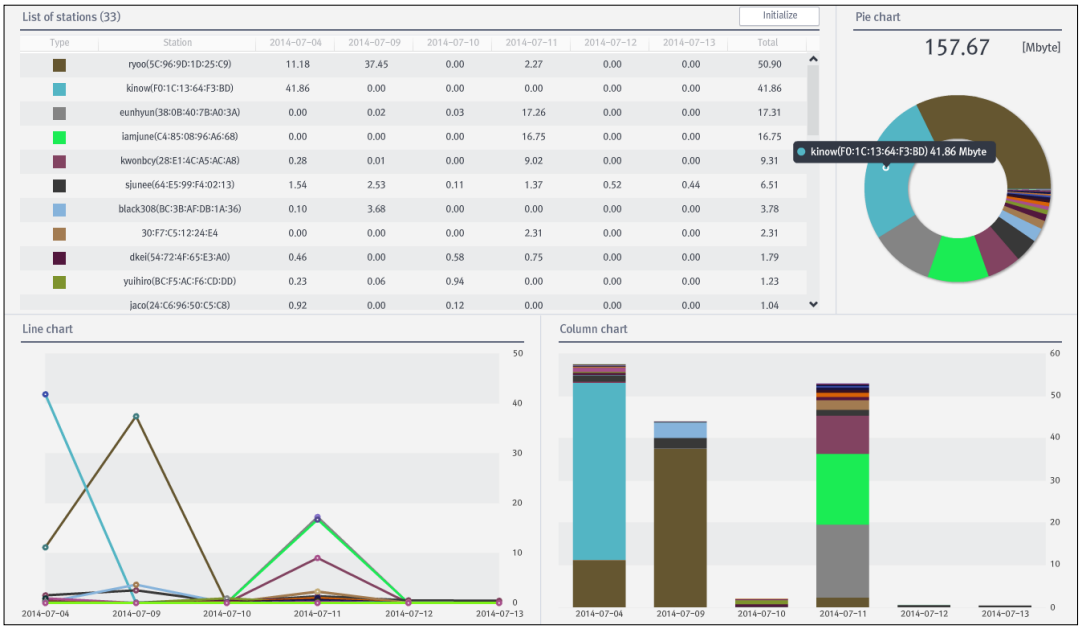


Figure 150. Traffic for the each managed AP

Depending on the search criteria at the top, you may search for the items as you wish.

Input Item	Description	Effective Value (Default)
AP	Selects the AP to be searched.	List of managed APs
Date	Selects the date on which you want to make inquiries about the statistics.	(Present date)

Select the Station from the list of stations on the top to see the stations accessing the AP as well as the traffic data of the station.

Select the Station you want from the list or graph to see the statistics on the selected Station. To see the total statistics, click the **[Initialize]** button.

4.5.4 Traffic for the each managed Station

You may make inquiries about the statistics for the volume of traffic used by each managed station for a designated period.

Statistics > Traffic for the each managed Station

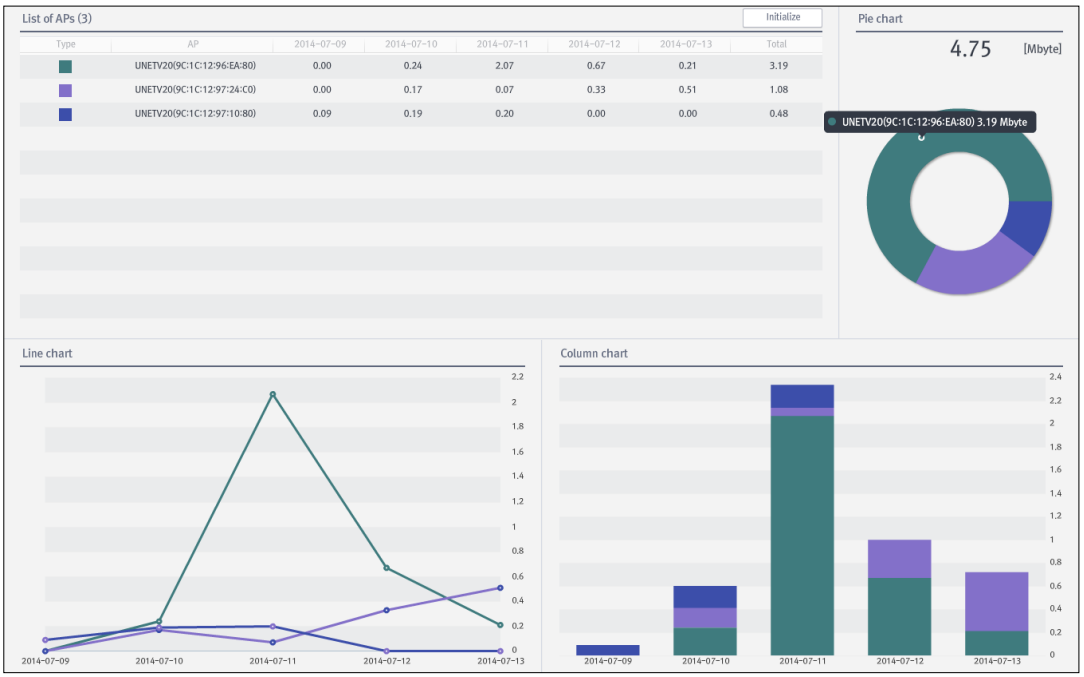


Figure 151. Traffic for the each managed Station

Depending on the search criteria at the top, you may search for the items as you wish.

Input Item	Description	Effective Value (Default)
Station	Selects the Station to be searched.	List of managed stations
Date	Selects the date on which you want to make inquiries about the statistics.	(Present date)

Select the AP from the list of APs on the top to see the station accessing the AP as well as the traffic data of the stations.

Select the AP you want from the list or graph to see the statistics on the selected AP. To see the total statistics, click the **[Initialize]** button.

4.5.5 Number of policy violations

You may make inquiries on the statistics for the number of cases of policy violations for a designated period.

Statistics > Number of policy violations

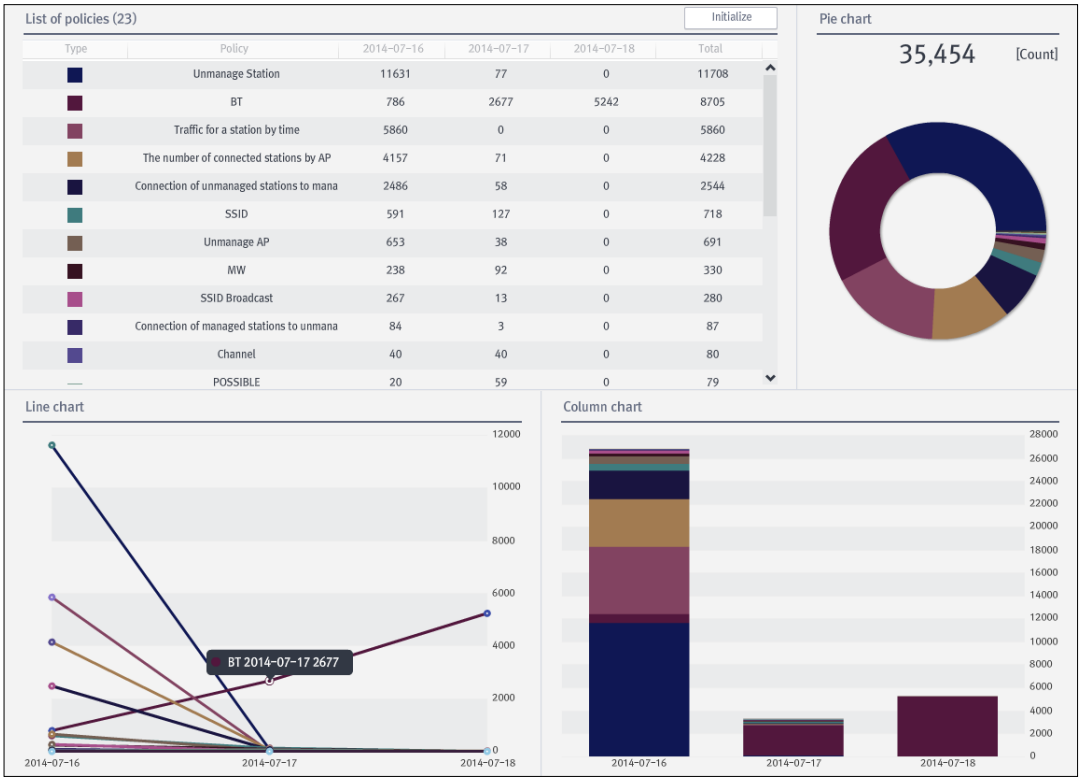


Figure 152. Number of policy violations

Depending on the search criteria at the top, you may search for the items as you wish.

Input Item	Description	Effective Value (Default)
Date	Selects the date inquiries are made about the statistics.	(Present date)

Select the policy you want from the list of policies on the top to check for any policy violation status.

Select the Policy you want from the list of policies or graph to see the statistics on the selected policy. To see the total statistics, click the **[Initialize]** button.

4.6 Dashboard

The dashboard is a comprehensive bulletin in WES. You may monitor main data in one window; if necessary you can look at detailed information immediately on each screen.

4.6.1 Dashboard

You may monitor the overall situation in WES on a periodic basis.

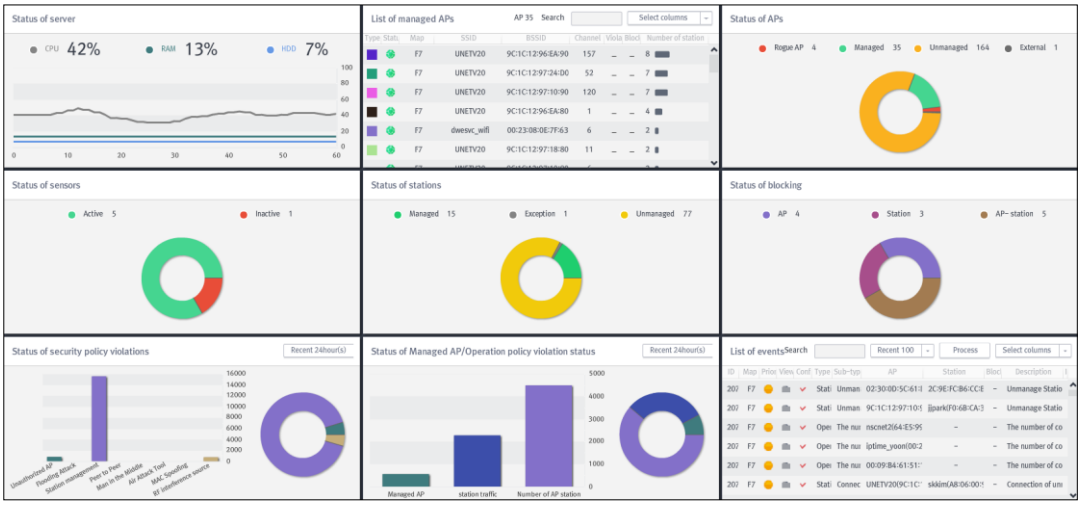


Figure 153. Dashboard

[Update]: Prints out the update time for dashboard.

[Period]: Sets the update time for dashboard (Unused/10/20/30/60 seconds).

[Layout]: Prints out the dashboard in the layout form set in the layout settings.

[Layout settings]: Sets the layout for organizing the dashboard screen.

In order to organize the screen on the dashboard only with the information required by an administrator, WES provides the function of setting the layout settings based on dashboard.

Dashboard> Layout settings > Add

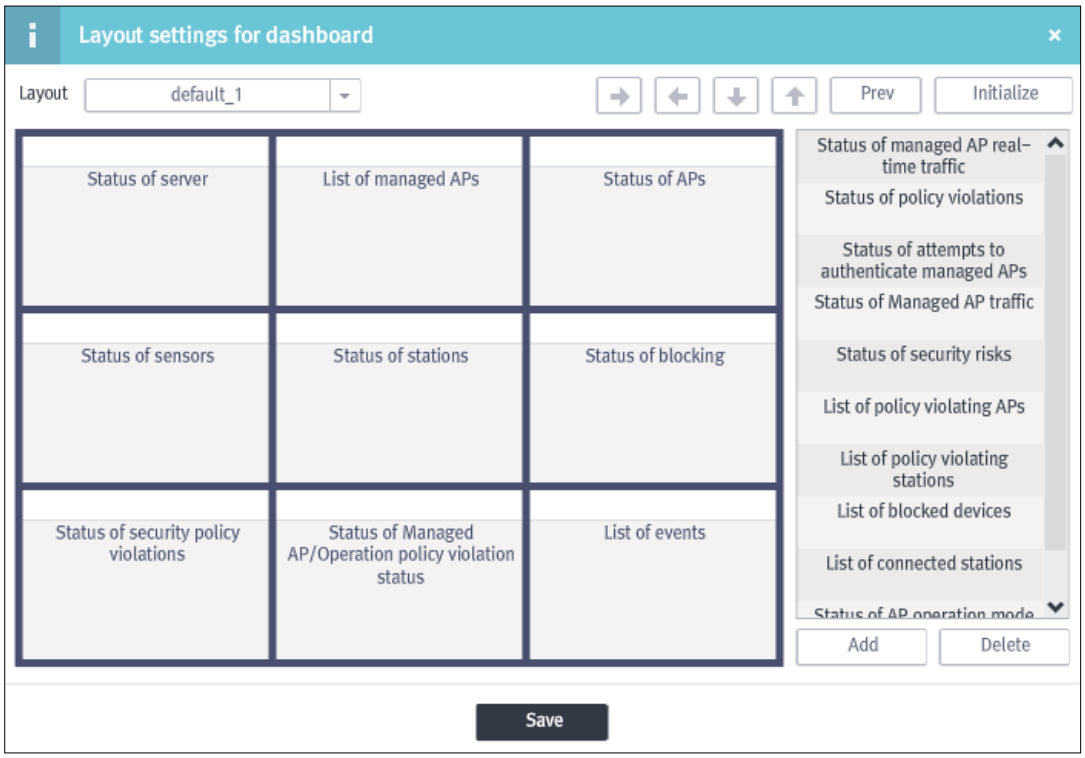


Figure 154. Layout settings for dashboard

Input Item	Description	Effective Value (Default)
Name	Sets the name of a layout.	3~15 characters(None)

[Layout settings] You may choose the two basic layouts (default 1, default 2) on screen. You may also add new layouts. In order to add new layouts, click the **[Add]** button at the bottom for setting the name. At this time, the screen in the basic settings with 9 columns will be displayed; after selecting the specific layout here, you may change the layout settings, using the arrow keys (right, left, down, up) at the top.

For example, after selecting 'Status of station' in the middle, click the **[left]** arrow key to expand the layout up to 'sensor status' on the left. In order to revert back to the default layout, click the **[Initialize]** button.

[Modify]: After selecting the layout list to be modified in the combo box for layout at the top, modify the details and click the **Save** button at the bottom.

[Delete]: After selecting the layout list in the combo box for layout at the top, click the **Delete** button on the bottom right.

> **NOTE**
>
> Default layouts cannot be modified or deleted.

Status of server

You may check the information on the status of CPU/Memory/HDD in a server.

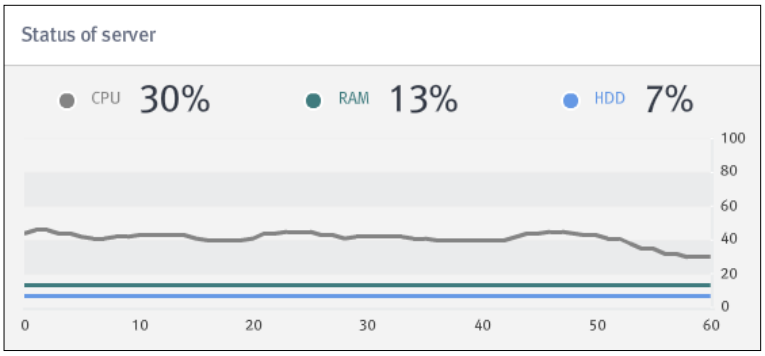


Figure 155. Status of server

List of managed APs

You may check the managed List of APs and information on the status (channel information or On/Off status, and the number of connected station).

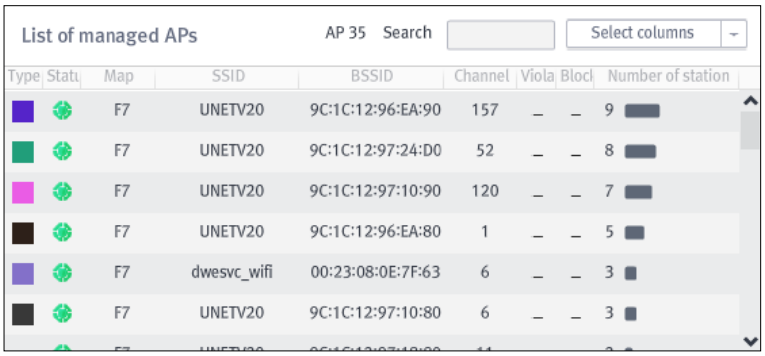


Figure 156. List of managed APs

[Search]: By inserting the information on the SSID/BSSID (1~17 characters), you may make inquiries about the AP.

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

If you double-click a particular AP in the list, you may view the AP information.

Status of APs

You may check the status of an AP detected by a sensor.

Figure 157. Status of AP

If you place the mouse cursor over the graph, the type and number of AP in the item will be displayed; if you double-click it, you may view the list of APs included in the item.

If you double-click a particular AP in the list, you may view the AP information.

Status of sensors

You may view the status of the sensors registered in a server.

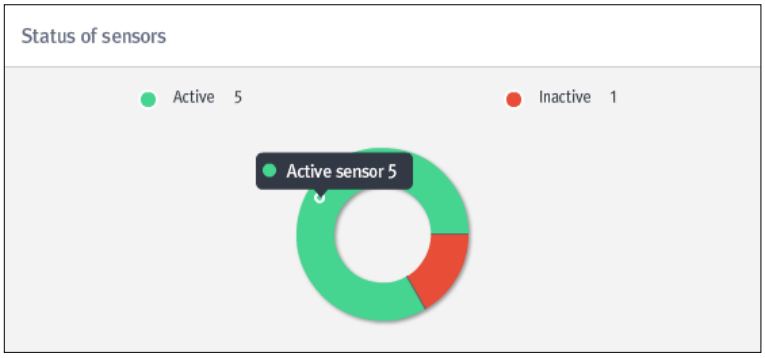


Figure 158. Status of sensors

If you place the mouse cursor over the graph, the type and number of sensors in the item will be displayed; if you double-click it, you may view the list of sensors included in the item.

If you double-click a particular sensor in the list, you may view the Sensor information.

Status of stations

You may view the status of the station detected by a sensor.

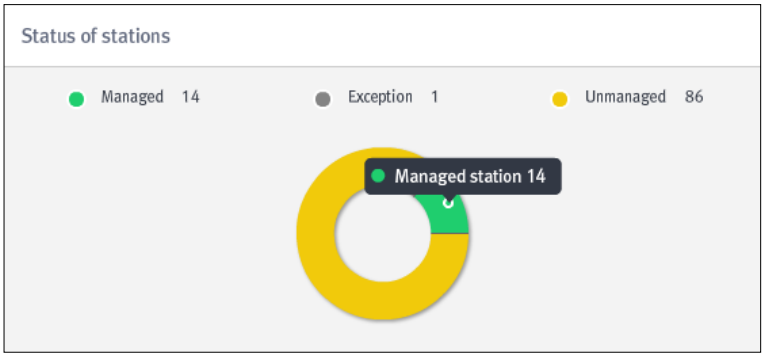


Figure 159. Status of stations

[Recent time]: The status of the station having been recently detected will be displayed (1/2/3/6/12/18/24 hours).

If you place the mouse cursor over the graph, the type and number of stations in the item will be displayed; if you double-click it, you may view the list of stations included in the item.

If you double-click a particular station in the list, you may view the Station information.

Status of blocking

You may view the status of blocked AP/Station due to policy violations.

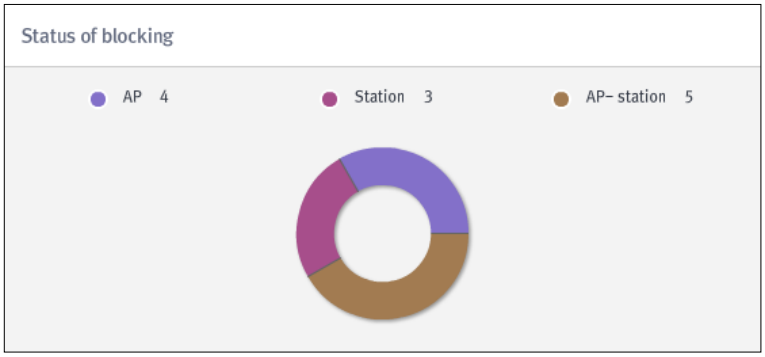


Figure 160. Status of blocking

If you place the mouse cursor over the graph, the type of blocking and the number of blocking cases will be displayed; if you double-click them, you may view the list of blocked AP and Station. If you double-click a particular AP or station from the list of blocked AP and Station, you may view the registered information on the AP or station.

Status of security policy violations

You may view the status of security policy violations.

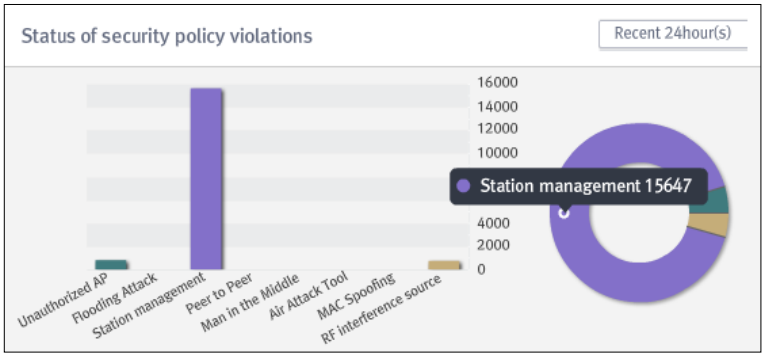


Figure 161. Status of security policy violations

[Recent time]: The status of security policy violations within the most recent time period will be displayed (1/2/3/6/12/18/24 hours).

Violation status by security policy will be displayed in a line chart or a phi chart. If you place the mouse cursor over each graph, the kind of policy and the number of cases of violations for the item will be displayed; if you double-click, you may view a list of the events included in the item.

Status of Managed AP/Operation policy violations

You may view the status of managed AP/operation policy violations.

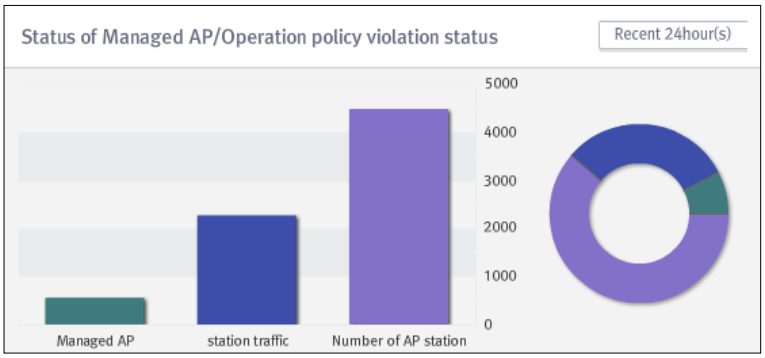


Figure 162. Status of Managed AP/Operation policy violations

[Recent time]: The status of managed AP/operation policy violations within the most recent time period will be displayed (1/2/3/6/12/18/24 hours).

The status of violations by managed AP/operation policy will be displayed in a line chart or a phi graph; if you place the mouse cursor over each graph, the type of policy/the number of cases in violation for the item will be displayed; if you double-click them, you may view the list of events included in the item.

List of events

You may view the information on all kinds of events generated due to policy violations.

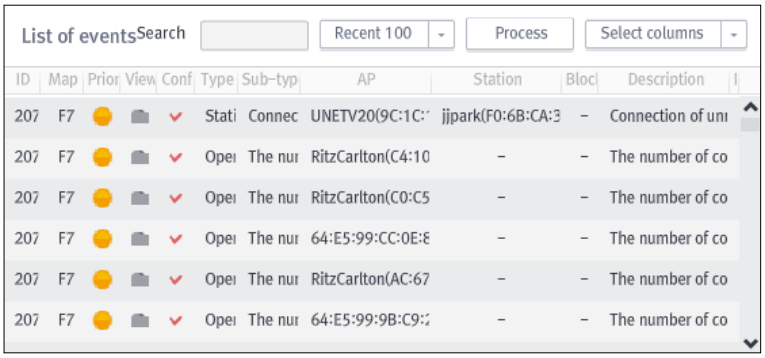


Figure 163. List of events

[Search]: Makes inquiries about the APs and stations by inserting BSSID/MAC (1~17 characters).

[Recent]: The list of events for the number of selected cases from the most recent event will be displayed (100/200/300/500 cases).

[Process]: Changes the status of the selected event to 'processed' status.

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

If you double-click a particular event, you may view the Event information.

NOTE

The detailed information on the event will be printed out in various forms depending on the kind of the event. For more details, **please refer to section 4.3 'Event/Log'.**

Status of managed AP real-time traffic

You may monitor the real-time data or packets sent to and received from managed AP.

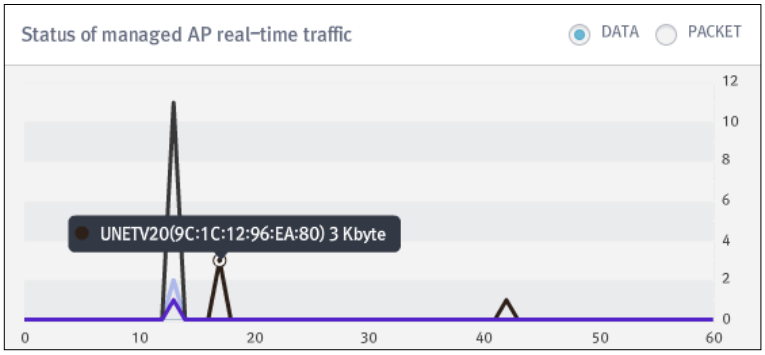


Figure 164. Status of managed AP real-time traffic

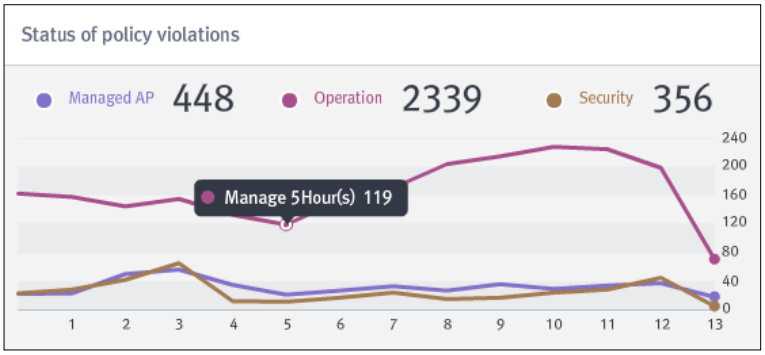
[Type of data]: Selects the type of traffic, e.g., DATA/PACKET, etc.

The real-time traffic status of a managed AP will be displayed in a line chart. If you place the mouse cursor over the graph, the SSID (BSSID)/data volume (packet volume) of the AP will be displayed; if you double-click it, you may view the AP information.

Status of policy violations

For all those detected, you may monitor the number of cases per hour where the policy is violated.

Figure 165. Status of policy violations



You may check the status of violations per hour by policy with a line chart.

If you place the mouse cursor over the graph, the type, time, and number of cases of policy violations occurring at the time will be displayed in a line chart, as well as a phi graph showing the total number of cases and the ratio of policy violations; if you double-click them, you may view the list of events.

Status of attempts to authenticate managed APs

You may view the status of authentication attempts per hour for stations attempting to connect to managed APs.

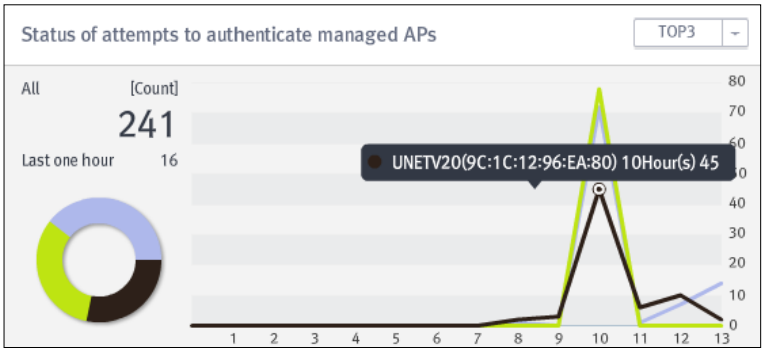


Figure 166. Status of attempts to authenticate managed APs

[TOP]: Prints out the AP with the highest number of authentication attempts according to the selected ranking (3/5/10).

You may view the status of authentication attempts at each time period in a line chart and the status of the accumulated number of attempts in a phi chart.

Place the mouse cursor over the graph to display the SSID (BSSID)/time/the number of cases for the AP in a line chart and the accumulated ratios of total authentication attempts in a phi chart; if you double-click them, you may view the list of the stations which have attempted to authenticate themselves to managed APs.

Status of Managed AP traffic

You may view the status of traffic sent to and received from managed APs by time.

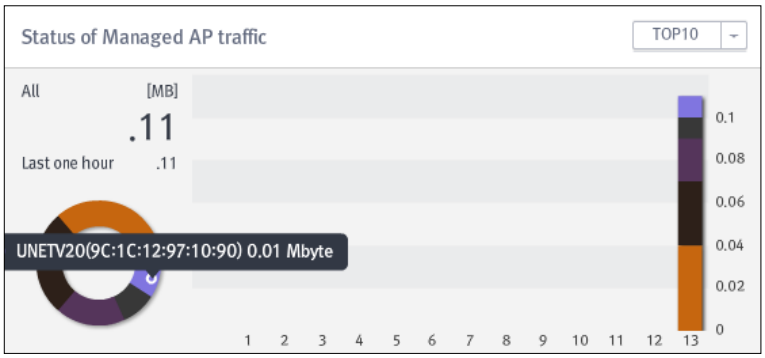


Figure 167. Status of Managed AP traffic

[TOP]: Prints out the AP with the highest volume of traffic according to the selected ranking (3/5/10).

The status of traffic by time will be displayed in a column chart; the status of accumulated traffic can be viewed in a phi chart.

If you place the mouse cursor over the graph, the SSID (BSSID)/time/the number of cases for the AP will be displayed; the accumulated volume of total traffic can be viewed in a phi chart. If you double-click them, you may view the information on traffic for the AP.

For more details about AP traffic status, **please refer to section 4.2.1‘AP management' for status of traffic of managed APs.**

Status of security risks (Setting time)

You may view the current situation of security risks from the status of security policy violations that have most recently occurred.

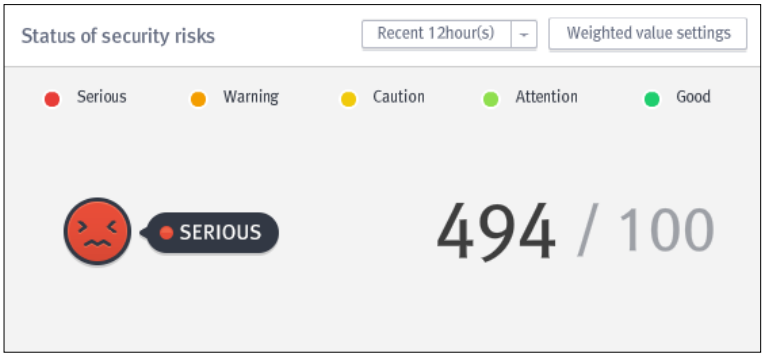


Figure 168. Status of security risks

[Recent time]: Prints out the security risk status by how recent the status of security policy violations occurred (1/2/3/6/12/18/24 hours).

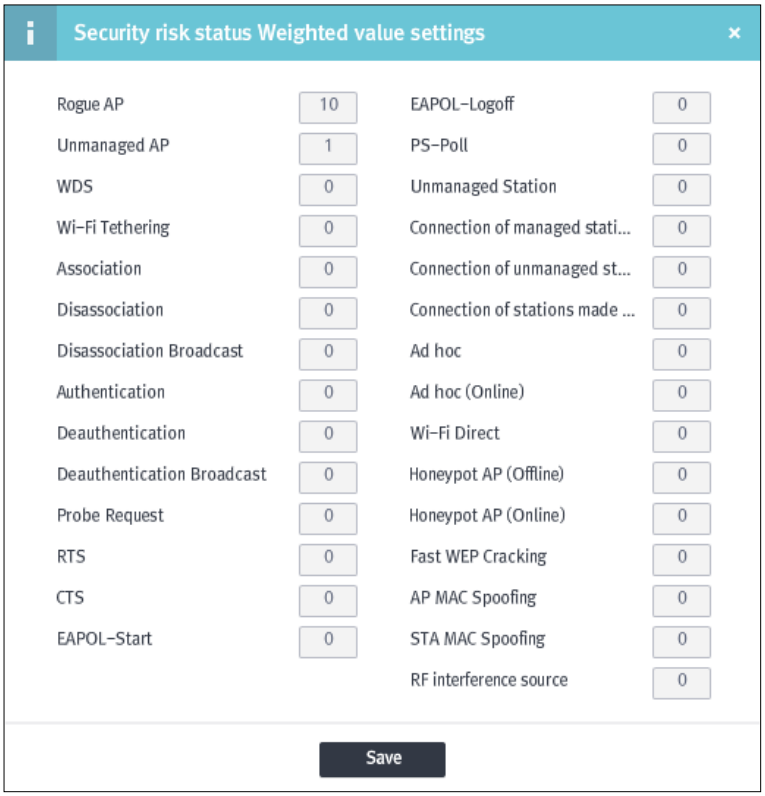


Figure 169. Security risk status weighted value settings

The weighted value can be arbitrarily set for different operating environments, according to the decision of an administrator.

NOTE

This represents the current degree of risk due to a security threat. The degree of risk will be classified into **Good (~20) / Attention (~40) / Caution (~60) / Warning (~80) / Serious (80~), by each policy with the set weighted values and the number of cases in the policy violation collected**, the total sum of which is 100.

For example, as shown in the figure, with a weighted value of 1, the number of cases of policy violations is 41 for managed APs, 13 for unmanaged stations, 16 for Rogue AP, 10 for Ad Hoc, and 6 for Honey Pot, respectively. The weighted value (1) x the number of cases in violation (86) would have a degree of risk being 86, which indicates a **'serious'** status.

List of policy violating APs

You may view all of the APs violating the policy.

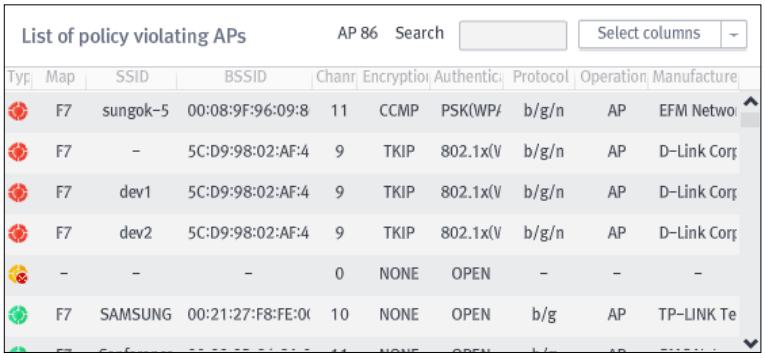


Figure 170. List of policy violating APs

[Search]: Makes inquiries about the AP by inserting SSID/BSSID (1~17 characters).

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

If you double-click a particular AP, you may view the AP information.

List of policy violating stations

You may view information on all stations violating the policy.

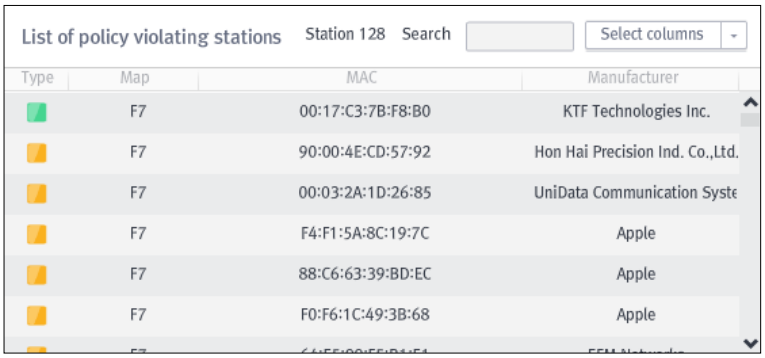


Figure 171. List of policy violating stations

[Search]: Makes inquiries about the station by inserting MAC/EAPID/IP (1~17 characters).

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

If you double-click a particular station, you may view the Station information.

List of blocked devices

You may view information on all of the APs and stations blocked due to policy violations.

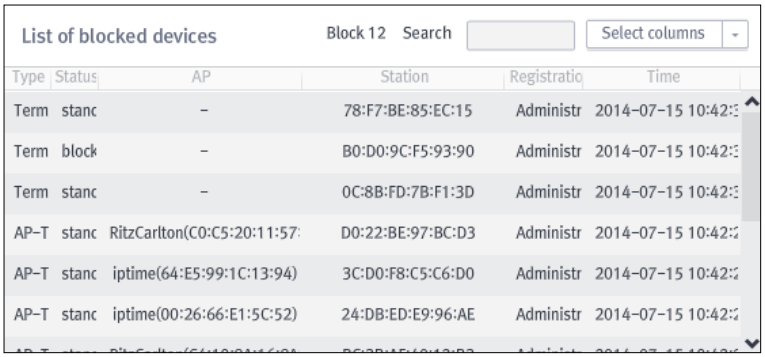


Figure 172. List of blocked devices

[Search]: Makes inquiries about the APs and stations by inserting AP/station (1~17 characters).

[Select columns]: Provides the option of only displaying the items in ‘Select columns’.

If you double-click a particular station, you may view the block logs and Station information.

List of connected stations

You may view information on all stations violating the policy.

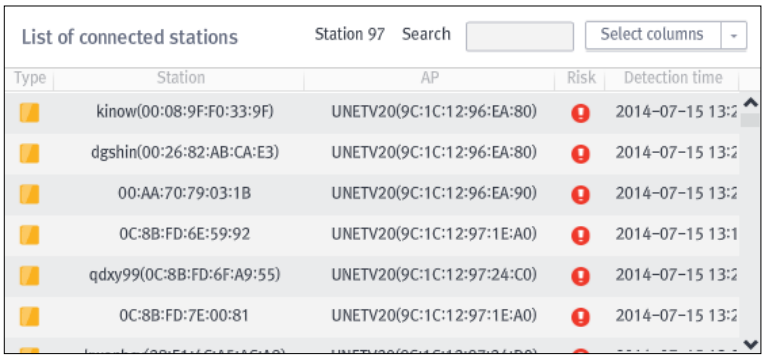


Figure 173. List of connected stations

[Search]: Makes inquiries about the APs and stations by inserting AP/station (1~17 characters).

[Select columns]: Provides the option of only displaying the items in 'Select columns'.

If you double-click a particular station, you may view the Station information.

Status of AP operation mode

You may view the status of AP operation mode.

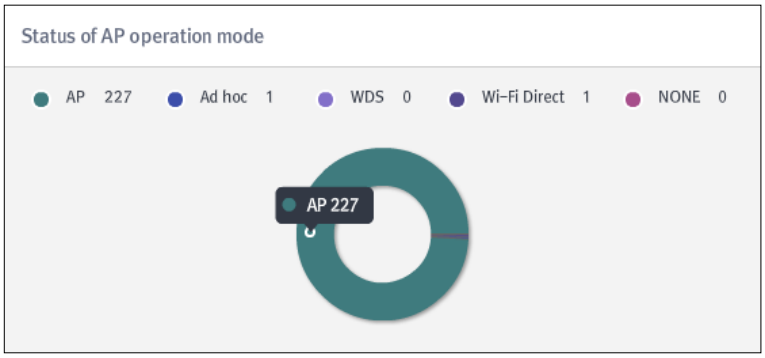


Figure 174. Status of AP operation mode

If you place the mouse cursor over the graph, the type of AP operation mode and the number of cases will be displayed; if you double-click them, you may view the list of APs. If you double-click a particular AP from the list of APs, you may view the AP information.

Glossary

802.11a

As one of the wireless LAN protocols developed by the Institute of Electrical and Electronic Engineers (hereafter, IEEE) and as the path-sharing protocol, it uses Ethernet protocol and carrier wave detection multi-access / collision avoidance (CSMA / CA) protocols. It is applied to a wireless asynchronous transmission system (ATM), is operated at frequencies from 5 GHz to 6 GHz, and uses the orthogonal frequency-type multiplexing (OFDM) method. Its maximum data speed is 54 Mbps but the communication speed in general is 6 Mbps, 12 Mbps, or 24 Mbps.

IEEE 802.11b

It is a next-generation standard that will substitute IEEE 802.11, a wireless LAN standard defined by IEEE in 1997. It is also called 'IEEE 802.11b high rate' and uses the frequency bandwidth at 2.4 GHz. Its data transfer speed is up to 2 Mbps for IEEE 802.11 but increases to up to 11 Mbps for 802.11b. It is also compatible with IEEE 802.11.

IEEE 802.11g

It is a type of IEEE 802.11b, the wireless LAN protocol developed by IEEE. Data is transmitted at the speed of 11 Mbps and at the frequency bandwidth of 2.4 GHz for 802.11b. While data is transmitted at the speed of 54 Mbps and the frequency bandwidth of 5 GHz for 802.11a, data is transferred at the speed of 54 Mbps and the frequency bandwidth of 2.4 GHz

IEEE 802.11n

It is an updated version of IEEE 802.11-2007, the wireless networking standard for improving the bandwidth of the previous standards, 802.11a and 802.11g. With the technologies of Multi-Input & Multi-Output (MIMO) using multi-antennae and of frame aggregation with physical layers being added, the maximum data transfer rate increases from 54 Mbps to 600 Mbps per second. The Orthogonal Frequency-Type Multiplexing method and multiplexed preparatory configuration enable it to enhance its reliability.

IEEE 802.11ac

It is an 802.11 wireless computer networking standard developed to provide the local area network (LAN) with higher speeds. It supports the high bandwidth (80 ~160 MHz) at a frequency of 5 GHz. According to this standard, the wireless LAN speed of multi-stations can reach up to 1 G bit/s and the maximum single link speed can be 500 Mbit/s, at least. It can be realized by expanding the concepts of wireless interface, which we reaccepted in 802.11n, such as the wider range of wireless frequency bandwidth (160 MHz at maximum), more MIMO streams (8 at maximum), multi-user's MIMO, and a high density of modulation, etc.

AP (Access Point)

It is a device performing the function of a wired or wireless synchronous bridge that relays the frames carried over from the wireless station to other station.

SSID (Service Set Identifier)

Wireless Access Point (Access Point, hereafter 'AP') is a generic identifier used for wireless nodes and APs to communicate with each other. It is included in the header of every packet exchanged within the designated wireless LAN BSS (Basic Service Set). Since this one wireless LAN can be differentiated from other wireless LAN, all APs or wireless devices attempting to connect to a particular wireless network must use the certain Service Set Identifier (SSID). If the SSID is changed, they cannot connect to the BSS.

BSSID (Basic Service Set Identifier)

It is a standard of IEEE 802.11, a wireless LAN standard. It represents the identifier or network ID with a length of 48 bit, which identifies the Basic Service Set (BSS). In general, it means the MAC Address of the AP.

BSS (Basic Service Set)

As a basic unit of a wireless LAN network, it represents a form of organization in which an AP and a number of stations (nodes) get together to communicate with each other within the wireless area where one moderator (such as an AP) transmits a signal.

Rogue AP (Rogue Access Point)

It represents an AP which may cause security risks that outsiders or insiders may penetrate into the intra-network with a malicious purpose while being installed illegally without the permission of an administrator.

Ad-Hoc

It represents a network in an autonomous structure allowing wireless devices to communicate without AP. There is a vulnerability that unauthorized users can connect to the intra-network by connecting to authorized stations in an Ad-Hoc manner.

HoneyPot AP

Originally, HoneyPot was one of the cutting-edge technologies to lure hackers with a view to preventing cyber terrorist attacks; however, a HoneyPot AP, which is its modified version, spoofs the SSID of the authorized AP to disguise itself as a user's connection to the normal AP. So, it represents the AP which induces the stealing of user's information such as the ID/PW.

DOS (Denial of Service)

In order to paralyse a particular server (target for attack), an attacker uses many zombie PCs in order to induce a multitude of connections to the target. By this, the target will be paralyzed due to deficiency of resources. This kind of attacking method is called DOS (Denial of Service).

Unauthorized Association/Client Mis-association

The risk by which an unauthorized user may connect to the authorized AP within a company is called 'Unauthorized Association.' The risk by which an authorized user inside may connect to unauthorized APs outside to leak internal data outside of the range of security control is called 'Client Mis-association.'

Wi-Fi Direct

It is a method by which devices with Wi-Fi installed communicate directly with each other not via the AP supporting a connection between Wi-Fi Alliance devices. It supports a connection speed of up to 300 Mbps, which is 22 times as fast as Bluetooth with its maximum connection speed being 22 Mbps. In addition, unlike Bluetooth, which supports 1 on 1 connection, it supports one-to-N simultaneous connection.

WDS (Wireless Distribution System)

It is a method for setting the wireless network between wired or wireless routers or AP in general use. By this, it is possible to expand the available wireless communication range. By using WDS, you can set one shared wireless network with a number of AP or wired/wireless routers.

MAC Spoofing (AP/Station)

It is an attacking method at the Layer 2 level, which forges the only MAC address of an NIC (Network Interface Card) of the AP or station for a malicious purpose.

CTS/RTS Flooding

As one of the DOS attacking methods, it causes a temporary communication failure by arbitrarily carrying the NAV value (duration time) of the CTS (Clear to Send)/RTS (Request to Send) packets between a station and AP.

Samsung Wireless Enterprise Security v1.0
Operation Manual