Wireless Enerprise Manager (WEM)

Operation Manual

COPYRIGHT

TRADEMARKS

This manual should be read and used as a guideline for properly installing and operating the product.
All reasonable care has been made to ensure that this document is accurate.

INTRODUCTION

Purpose

This manual provides explanations about necessary information for using Wireless Enterprise Manager (WEM) such as registering and managing users and instructions on various menu options.

Document Content and Organization

This manual consists of 9 Chapters and 2 Annex and an Abbreviation section.
The summary of the Chapters are as follows:

CHAPTER 1. WEM Overview

This chapter describes the WEM system information and basic functions.

CHAPTER 2. WEM Interface

This chapter describes the log-in procedure for the WEM, the basic operation methods for operating WEM and the methods of the network management.

CHAPTER 3. Monitor

This chapter describes WEM's Monitoring windows and their functions.

CHAPTER 4. Configuration

This chapter describes WEM's Configuration windows and their functions.

CHAPTER 5. Admin

This chapter describes WEM's Operation Management windows and their functions.

CHAPTER 6. Tools

This chapter describes WEM's Tool windows and their functions.

CHAPTER 7. General

This chapter describes WEM's General management windows and their functions.

CHAPTER 8. Security

This chapter describes WEM's Security windows and their functions.

CHAPTER 9. Help

This chapter describes WEM server information using Help window.

ANNEX A. Alarm List

Describes Alarm List.

ANNEX B. Open Source Announcement

Describes Open Source Announcement.

ABBREVIATION

Describes the acronyms used in this manual.

Conventions

The following types of paragraphs contain special information that must be carefully read and thoroughly understood. Such information may or may not be enclosed in a rectangular box, separating it from the main text, but is always preceded by an icon and/or a bold title.

CHECKPOINT

Provides the operator with checkpoints for stable system operation.

NOTE

Indicates additional information as a reference.

Revision History

VERSION	DATE OF ISSUE	REMARKS
1.0	July 2015	North America Release Version

TABLE OF CONTENTS

LIST OF FIGURES

CHAPTER 1. WEM Overview

This chapter describes the functions and specifications of Samsung Wireless Enterprise Manager.

1.1 WEM

The WEM is a powerful centralized management system that provides to manage and configure the WLAN network and check the status of the Samsung Network Elements (Access Point Controller, Access Point and Switch).

The WEM operates in Client-Server Processing Mode. The Server provides the interface between the Client and Network Elements by directly connecting to the WEM Server, and manages various databases as well.

The Client functions as a terminal that provides the operator interface to access the WLAN Network Elements through WEM Server. The WEM Server was developed using Java Server Page (JSP), Servlet, Remote Method Invocation (RMI), Java Database Connectivity (JDBC), and Extensible Markup Language (XML). WEM Client was developed using Hypertext Markup Language (HTML), Java Applet, Java Script, and Flex.
The interface between WEM and Network Elements (NE) are as follows:

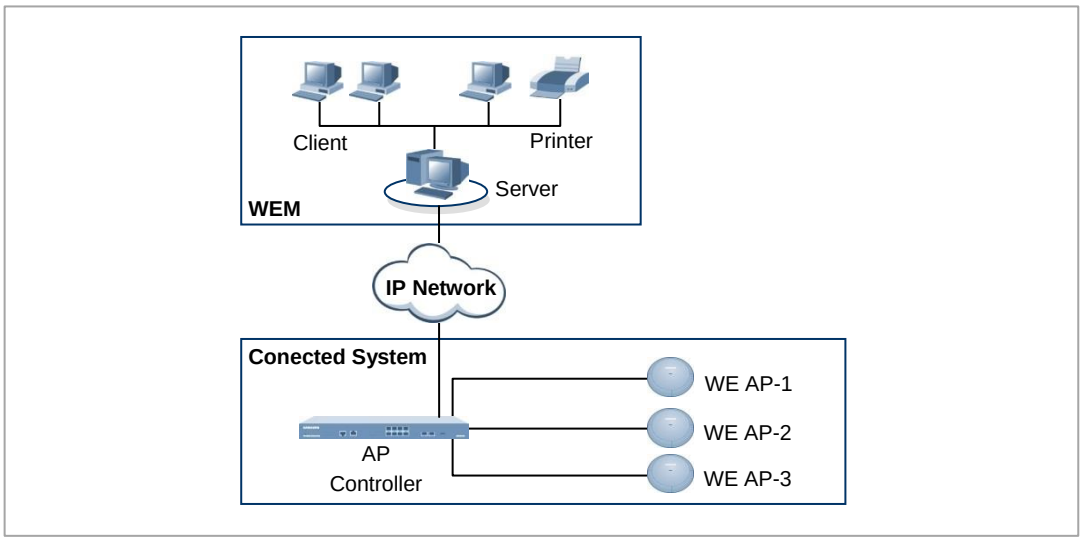


Figure 1. Samsung WLAN Network Configuration

The WEM provides the following various functions.

Real-Time System Status Monitoring

WEM collects various fault statuses that have occurred in the system in real-time using the Simple Network Management Protocol (SNMP).

Graphic User interface

The standard graphic interface was used to develop WEM. All orders are configured with graphic menus so operators can easily understand and operate the WEM functions.

Various Statistics Reports

The WEM provides the operator with the data such as information on defects, performance, and traffic in the type of text, graph, and statistics. This statistics data can be retrieved as a file or can be printed.

Object Oriented Design

The Object-oriented approach was used to design WEM. Since various sub-systems are separated into objects, it is easy to add or upgrade required functions.

Error Handling

If WEM is unable to handle the input order properly, error messages will be displayed before performing subsequent tasks. Operators can operate the system accurately and effectively by checking the error messages before performing the fault orders.

Flexible Platform

WEM can be installed and operated in various platforms such as a regular PC or work station. Therefore, operators can select the appropriate WEM platforms in accordance with network size or management range.

1.2 System Specifications

1.2.1 Hardware Specifications

Server

Category	Specification
CPU (Central Processing Unit)	3.0 GHz (Intel Zeon Quad core processor) or higher
Main Memory	16 GB or higher
Hard Disk	300 GB or higher Hard Disk
Drive	DVD-ROM Drive
Monitor	1280 × 1024 resolution
LAN Card	10/100 Base-T (RJ-45 Connector)

Client

Category	Specification
CPU	3.0 GHz (Pentium Core 2 Duo Processor) or higher
Main Memory	2 GB or higher
Hard Disk	100 GB hard disk or higher
Driver	CD-ROM Driver
Monitor	1280 × 1024 resolution
LAN Card	10/100 Base-T (RJ-45 Connector)

Hardware Specifications

Above Description and specifications are mentioned based on Large Scale Network HW specification shall be changed according to the Network size and configuration.

1.2.2 Software Specifications

Server

Category	Software
OS	Linux (Red Hat Enterprise ES 5.5~6.3) Not Included
JSP/Servlet engine	Tomcat 5.0.28
Database	MySQL Enterprise 5.5
JVM	JDK 1.6.0_20
Management Protocol	SNMP
Others Protocol	FTP (File Transfer Protocol), Telnet (SSH)

To ensure optimum performance, we recommend using the same version as stated above.

Client

Category	Software
OS	Windows XP~Windows 7
Web Browser	Microsoft Internet Explorer Version 8.0~10.0 recommended
Java	JRE 1.7.0_25
Flash Player	Flash Player 11 Active X Version

To ensure optimum performance, we recommend using the same version as stated above.

CHAPTER 2. WEM Interface

This chapter explains Graphic User Interface (GUI) of WEM and basic operating methods for WEM.

2.1 Connecting to WEM

This section explains WEM log-in and log-out procedures.

2.1.1 Log-in

Log-in procedure for WEM operation is explained below:

1) Open a Web browser (Microsoft Internet Explorer) to connect to WEM Server.

2) Enter Internet Protocol (IP) address of the WEM server in the address field and the log-in window appears.

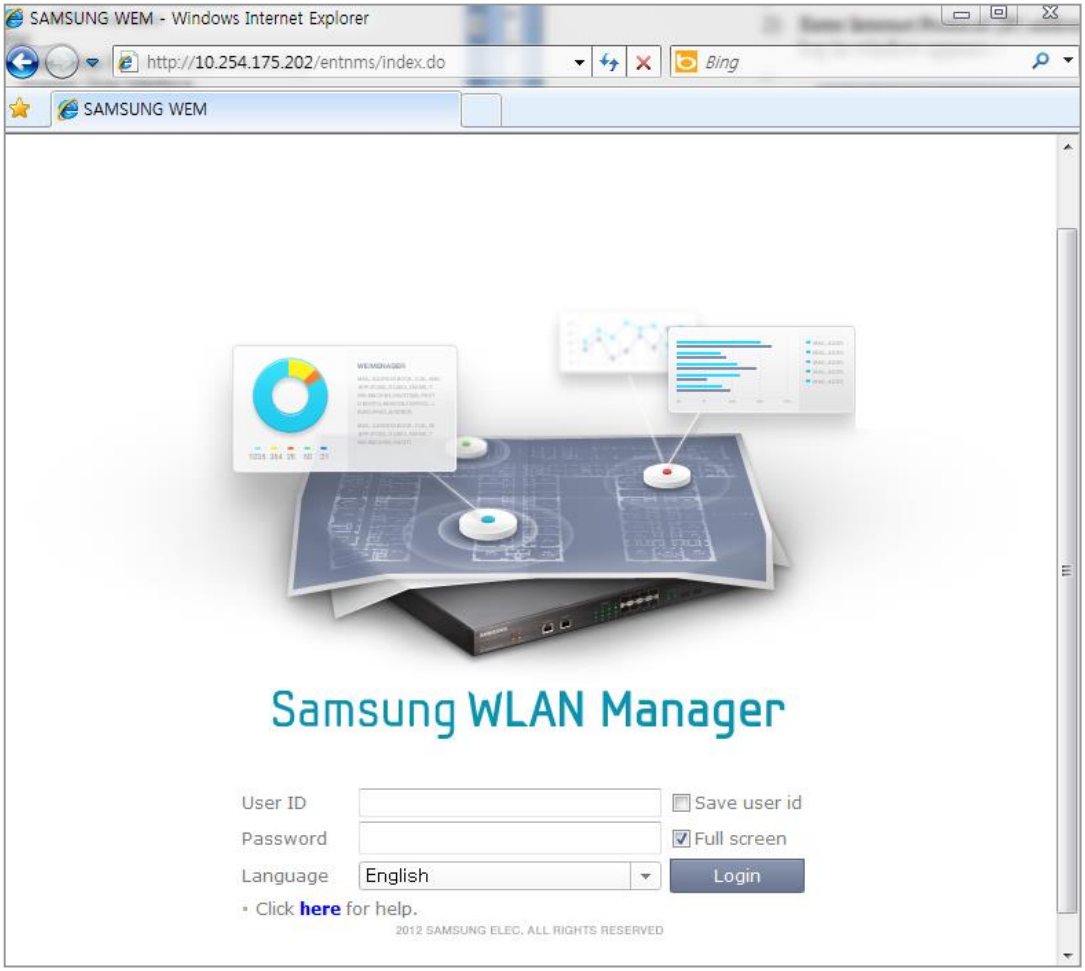


Figure 2. Log-in window

3) Enter the User ID and password in the corresponding fields and click ‘Login’ button.

4) Once the user information is verified, the WEM window appears.

2.1.2 Log-out

WEM log-out procedure is explained below:

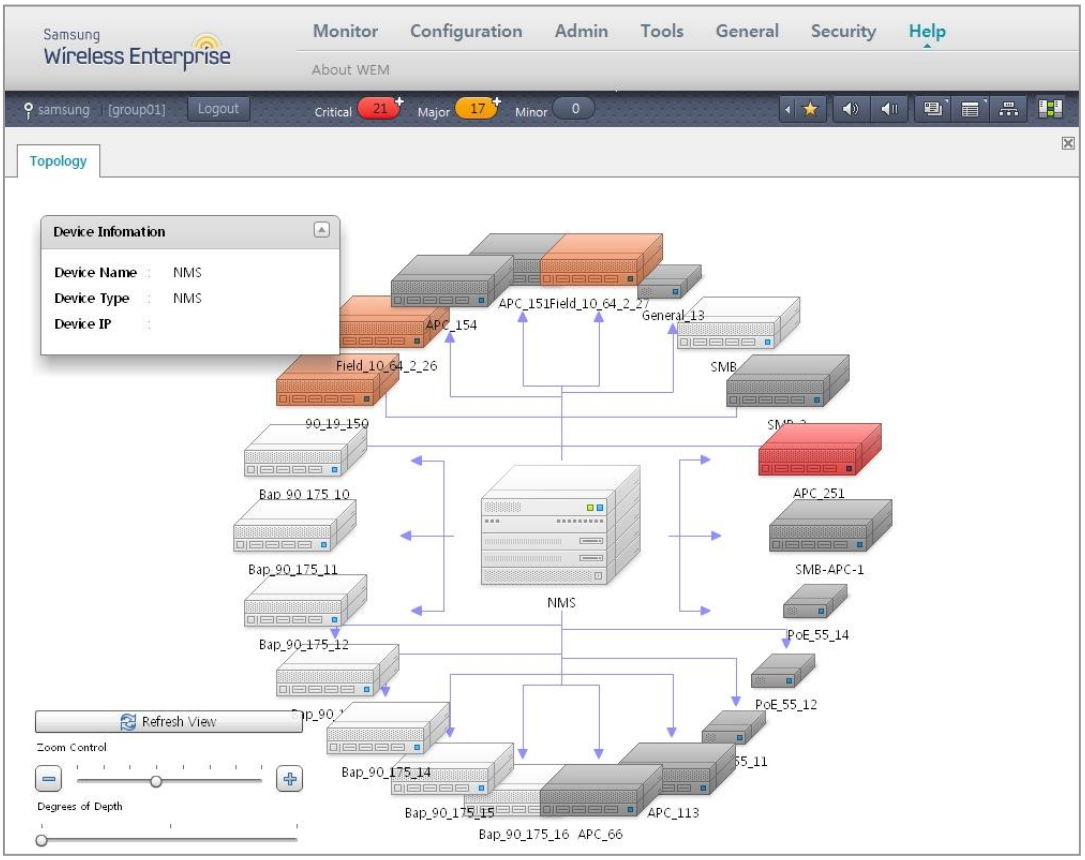


Figure 3. Log-out Button

1) Click the '**Logout**' button at the top left of the WEM window. A pop-up window will appear to confirm logout.
2) Click 'OK' button to log-out.

> **CHECK**
>
> **The Operation of WEM in Logout State**
>
> Even when you are logged out, the WEM System continues to perform certain functions, such as generating error messages and collecting the performance data's etc.

2.2 Interface Structure

The WEM window consists of the following three frames:

- Menu Frame
- Main Frame
- Tree Viewer Frame

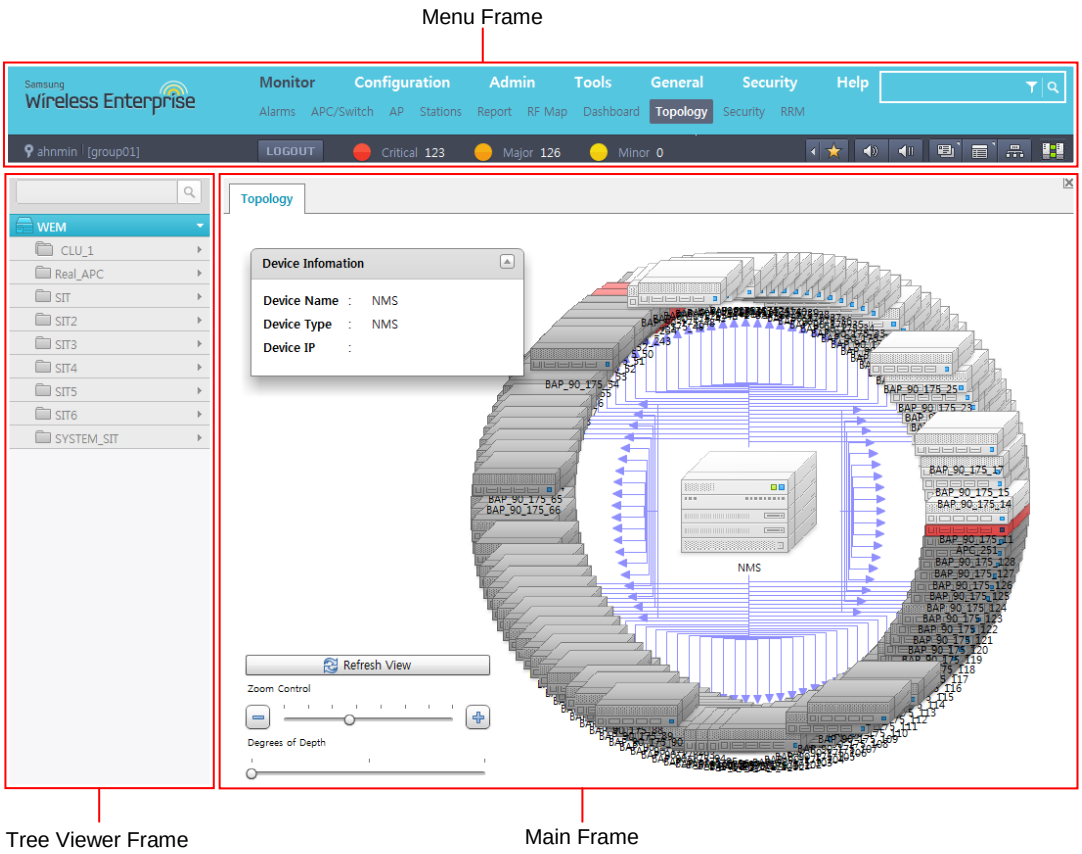


Figure 4. WEM Frame Structure

2.2.1 Menu Frame

These groups can be seen on the WEM menu frame and various commands from each management group can be executed.

The menu frame consists of the following elements: number order is reversed

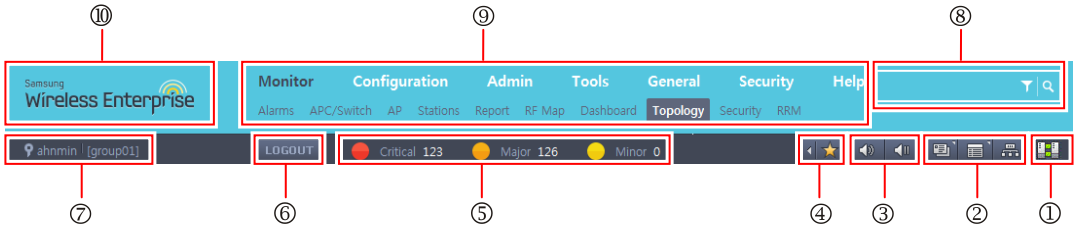


Figure 5. Menu Frame

Item	Description
①	WEM's logo and name
②	User menu consists of 7 management groups.
③	Network Element Search (Such as registered ACP, AP mobile station's)
④	User information (user ID and group)
⑤	Logout button
⑥	Displaying alarm count
⑦	Hides/Shows Quick Icon Bar.
⑧	- : On/Off the audible alarm - : Mute the audible alarm
⑨	- : Execute Dash Board - : Execute Event Viewer - : Hides/Shows Tree Viewer.
⑩	Displays connection status between the WEM server and client.

Description for Quick Icon Bar Button

Button	Description
	Execute Network Viewer function.
	Execute RF (Radio Frequency) MAP function.
	Execute spectrum analysis function
	Execute statistics function. No longer present?
	Display the summary information of the wireless terminal and its location move tracks.

2.2.2 Main Frame

Once a user executes a command in the menu frame, the main frame displays the corresponding function window.
By default the main frame displays the network viewer at the initial state.

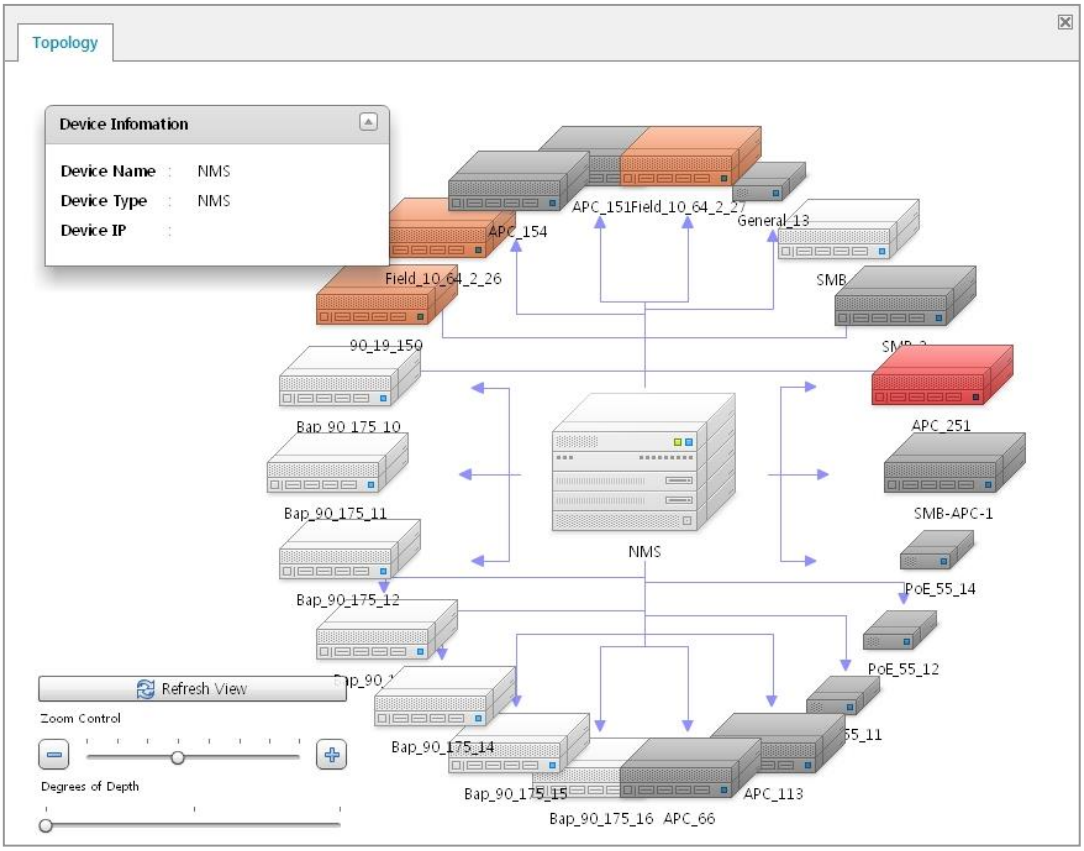


Figure 6. Main Frame

2.2.3 Tree Viewer Frame

Tree Viewer frame displays network elements in tree format. Tree Viewer frame displays the form of tree with the highest group, cluster, and controller order of this inferiority.

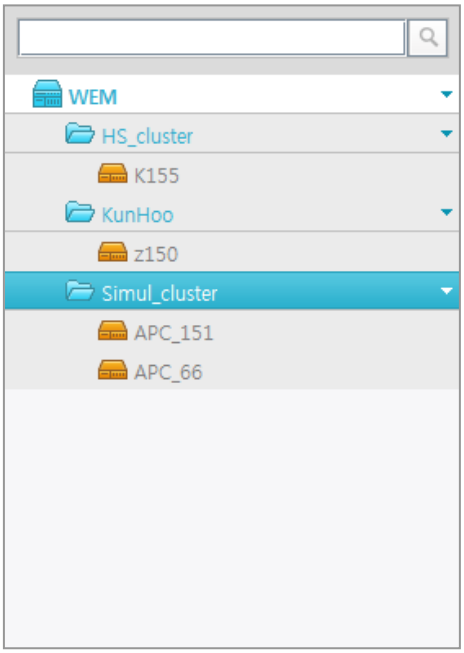


Figure 7. Tree Viewer Frame

Icons

The Tree Viewer has the icons shown in the figure below to identify the status of the network elements and alarm severity.
However, the WEM icon does not indicate an alarm status.

Network Element	Normal	Disabled	Critical (Red)	Major (Orange)	Minor (Yellow)
WEM		-	-	-	-
Controller					

Search Function

Each network elements are displayed in the Tree Viewer, user can search Network element in the search box at the top of the tree viewer.

2.3 Basic Operation

This section describes the basic elements for operating WEM.

2.3.1 Buttons

The command buttons used in WEM are designed to run the same functions in all windows. Command buttons commonly used in WEM are as listed below:

Button	Description
Active	Activates the job.
Clear	Deletes the data.
Deactive	Deactivates the job.
Execute	Executes command.
Get	Displays data that have already been configured or saved
Save	Saves the data.
Search	Searches data that have already been configured or saved
Set	Defines properties for the data or function
Test	Tests the job.

2.3.2 Basic Properties

Users shall generally set up a few elements while executing WEM functions.
Users may also need to set up search period for certain jobs

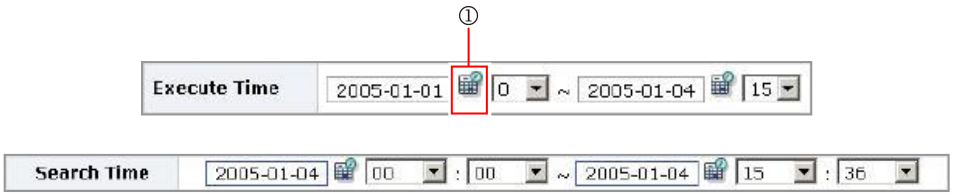


Figure 8. Example of Setting Period

The date can either be directly entered in the text box in the required format or can be selected in the calendar by clicking the calendar button (①).

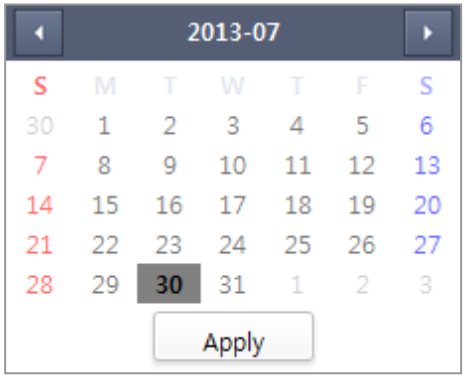


Figure 9. Calendar Window

Set the date using the ( ) ( ) button. Select a date to save the items for the selected dates to Main Frame.

2.4 Network Viewer

This section allows you to view Network Name, sub network, Network Element (NE) in hierarchal level and configured in tree shape for operators to easily understand the top to bottom structure of WEM Network Elements. Each network elements are called node.

Node	Description
WEM	A node used to indicate the top parent class (Root) in the Tree Viewer.
Group	A node used to manage controller by grouping.
Cluster	A node used to manage controller by cluster.
Controller	Group containing the controller node
Switch	Switch node which is controlled by WEM

The following picture is the sample screen of the tree viewer. The target content can be variously changed according to the group or the equipment organization.

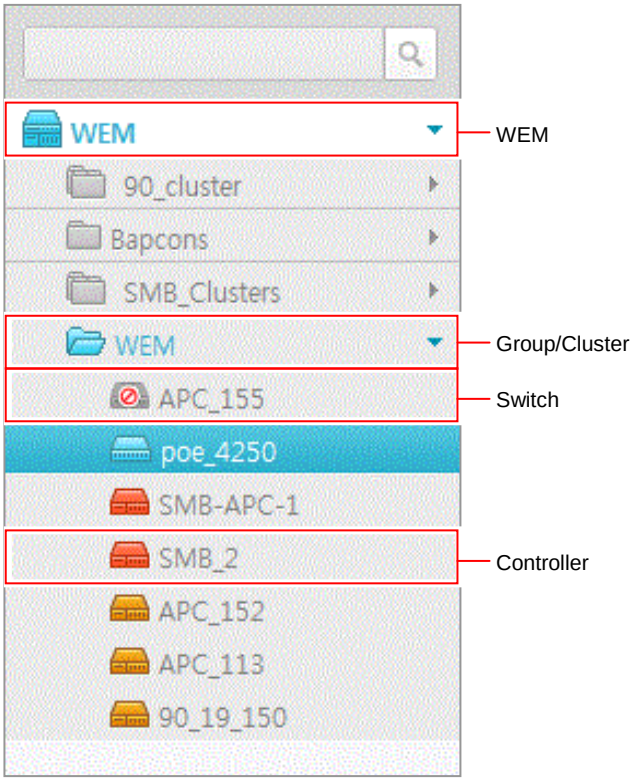


Figure 10. Tree Viewer (node structure)

Select a specific node in the Tree Viewer and right-click on it. A pop-up menu will appear to add, delete, view and modify the data of node.

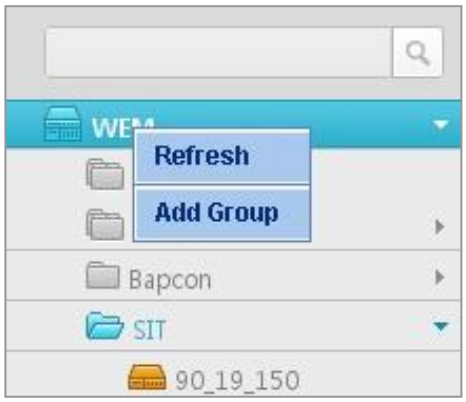


Figure 11. Tree Viewer (pop-up menu)

NOTE

Tree View

A controller must be registered before to add/modify/delete data in the list.

2.4.1 Group Node

Group Node is made by grouping the controller in devices, local, or cluster.

Creating a Group

1) Right-click on a WEM node in the Tree Viewer.

2) Click ‘Add Group’ in the pop-up menu.

3) Select the ‘Group Type’ and enter the ‘Group Name’ in the ‘Add Group Window’ displayed.

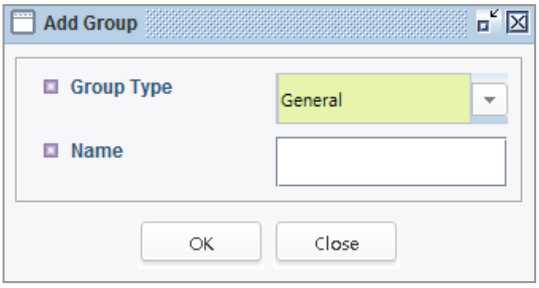


Figure 12. Adding a Group Window

4) Enter the group node name in ‘Name’ item, enter the ‘General’ or ‘Cluster’ in ‘Group Type’ item.

5) Click ‘OK’ button to add corresponding group in the Tree Viewer.

Deleting a Group

1) Select a group to delete in the Tree Viewer, and right-click on it.
2) Click ‘Delete Group’ in the pop-up menu.
3) A pop-up window appears to confirm, click ‘Yes’, to delete the selected group.

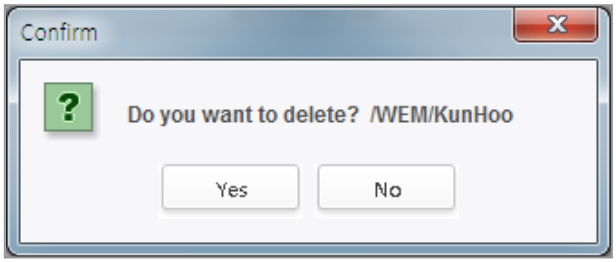


Figure 13. Deleting a Group Window

Modifying Group Information

1) Select a group to modify in the Tree Viewer, and right-click on it.
2) Click ‘Modify Group’ in the pop-up menu.
3) Select and change the data which you want to modify in the displayed window.
4) Click ‘OK’, to complete the modify the group information.

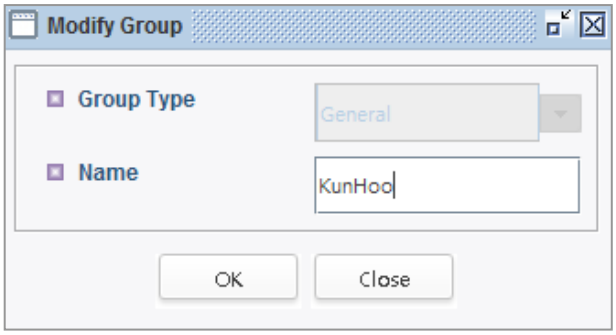


Figure 14. Change Group Window

2.4.2 Controller Node

Adding a Controller

1) Right-click on the group in the Tree Viewer.

2) Select ‘Add Controller’ in the pop-up menu.

3) The window is displayed to add Controller.

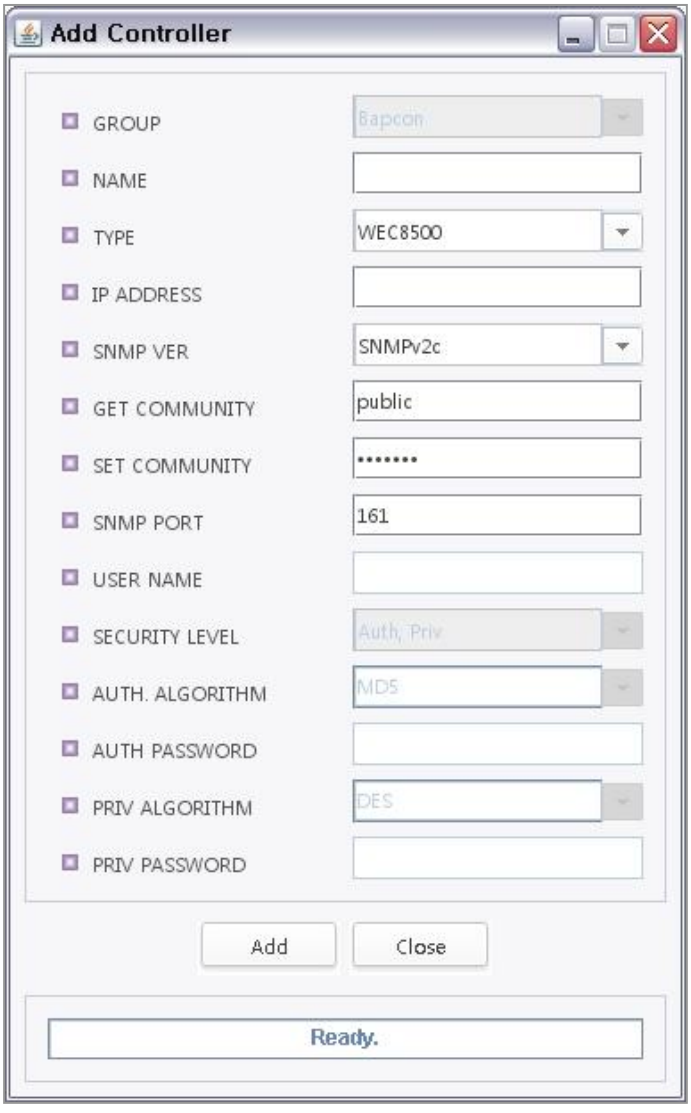


Figure 15. Adding Controller Window

4) Set the each field by input parameter. The operator can view processing status in the ‘Ready’ option at the bottom of window.

Parameter	Description
GROUP	Controller node group
NAME	Controller name
LOCATION	Controller's location
TYPE	Controller Type
IP ADDRESS	IP address of the controller
SNMP VER	SNMP version of the controller
GET COMMUNITY	Get the SNMP Community
SET COMMUNITY	Set the SNMP Community
SNMP PORT	SNMP port of the controller
USER NAME	SNMPv3parameter-set user name
SECURITY LEVEL	SNMPv3 parameter-set the security level
AUTH ALGORITHM	SNMPv3 parameter-authentication algorithm
AUTH PASSWORD	SNMPv3 parameter-authentication password
PRIV ALGORITHM	SNMPv3 parameter-each algorithm
PRIV PASSWORD	SNMPv3 parameter-each password

5) Click 'Add' button.

6) You can check the Controller added in the Tree Viewer.

Deleting a Controller

1) Select a Controller to delete in the Tree Viewer, and right-click on it.

2) Click 'Delete Controller' in the pop-up menu.

3) A pop-up window appears to confirm.

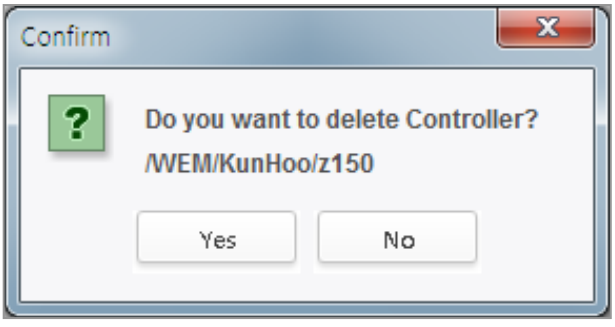


Figure 16. Controller Node Delete

4) Click 'Yes', to delete the selected Controller.

2.4.3 Cluster Auto Configuration

Cluster provides redundancy and easy network configuration for AP's Network. If one APC fails, other APC in that cluster will take over the failed APC's Network Load.
To configure cluster, Each Controllers must have cluster member information.
By using WEM, Operator can set cluster member information to each controllers automatically.
If using this function, Each Controllers will be lost previous cluster information.
So, operator should plan this activity because it will affect the current service

During the auto configuration, If SNMP error happened, WEM configure the setting continuously except for error items.
In this case, WEM will notify to user with error dialog window.

Setting

1) Go to 'Configuration' → 'Controller/Device' or 'Monitor' → 'Controller/Devices'.
2) I check the cluster which you'd like to comprise automatically in the Tree Viewer appeared in a left, and click the right of mouse in the concerned cluster group and select a menu.
3) Select 'Cluster AutoConfig' of the menu.
4) I confirm warning that the existing cluster creation is altogether deleted.
5) Select 'Yes' button.

2.4.4 Remove Cluster Auto Configuration

To release cluster, Each Controllers has to release cluster member information.
By using WEM, Operator can release cluster member information to each controllers automatically.
If using this function, each controller will be lost previous cluster information.
So, operator should plan this activity because it will affect the current service.
During the auto configuration, if SNMP error happened, WEM configure the setting continuously except for error items. In this case, WEM will notify to user with error dialog window.

Setting

1) Go to 'Configuration' → 'Controller' or 'Monitor' → 'Devices'.
2) I check the cluster which you'd like to lift automatically in the Tree Viewer appeared in a left, and click the right of mouse in the concerned cluster group and open a menu.
3) Select 'Cluster Auto Clear' of the menu.
4) Confirm warning that the existing clusters creation is altogether deleted.
5) Select 'Yes' button.

2.4.5 Switch Nodes

A switch belonging to a group node or cluster in the tree viewer can be directly configured.

Creating a Switch

1) Right-click in the tree viewer group.

2) Select ‘Switch Register’ in the popup menu.

3) The menu window where the switch can be created appears.

Figure 17. Switch Registration Menu Window

4) Set each field depending on entries. The registration process status in ‘Ready’ on the bottom of the window can be confirmed.

Item	Description
GROUP	Group to which a switch node belongs-Impossible to modify
NAME	Name of the switch
TYPE	Designate the type of a switch (iES4028FP, iES4226FP, iES4250GP, iES4028F, iES4224GP, iES4024GP, General)
IP ADDRESS	IP address of a switch
GET COMMUNITY	Designate SNMP community for viewing the switch.
SET COMMUNITY	Designate SNMP community for setting the switch.

Item	Description
SNMP PORT	SNMP port number of a controller
SNMP VER	Supported version of SNMP-Impossible to modify

5) Click the ‘Add’ button.

6) The switch added can be confirmed in the tree viewer.

Deleting a Switch

1) Select a switch to delete in the tree viewer and then right-click.
2) Select ‘Switch Deletion’ in the popup menu.
3) The window for asking the deletion of the switch appears.

Figure 18. Window for Confirming Switch Deletion

Automatic AP configuration

Automatic AP configuration is a function of automatically creating the information on the connection between the Ethernet port of the switch and the AP which is connected to the port by using the information on RFC1213 and bridge MIB (RFC1213). By using this function, the operator can easily create the information on the switch port and the AP connected therewith.

1) Select a switch to process the automatic AP configuration in the tree viewer and then right-click.

2) Select ‘Automatic AP Configuration’ in the popup menu.

3) The window for asking the automatic AP configuration appears.

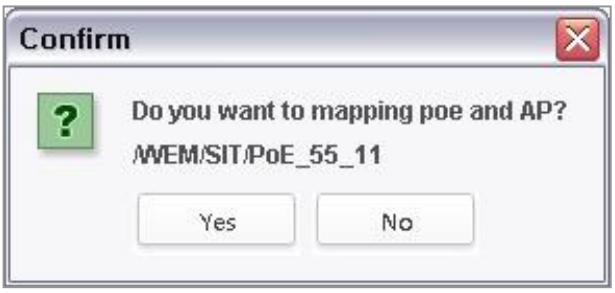


Figure 19. Window for Confirming Automatic AP Configuration

4) Click 'Yes' to perform the automatic AP configuration.

5) The result of the automatic AP configuration can be confirmed by viewing the concerned switch information in Configuration Management.

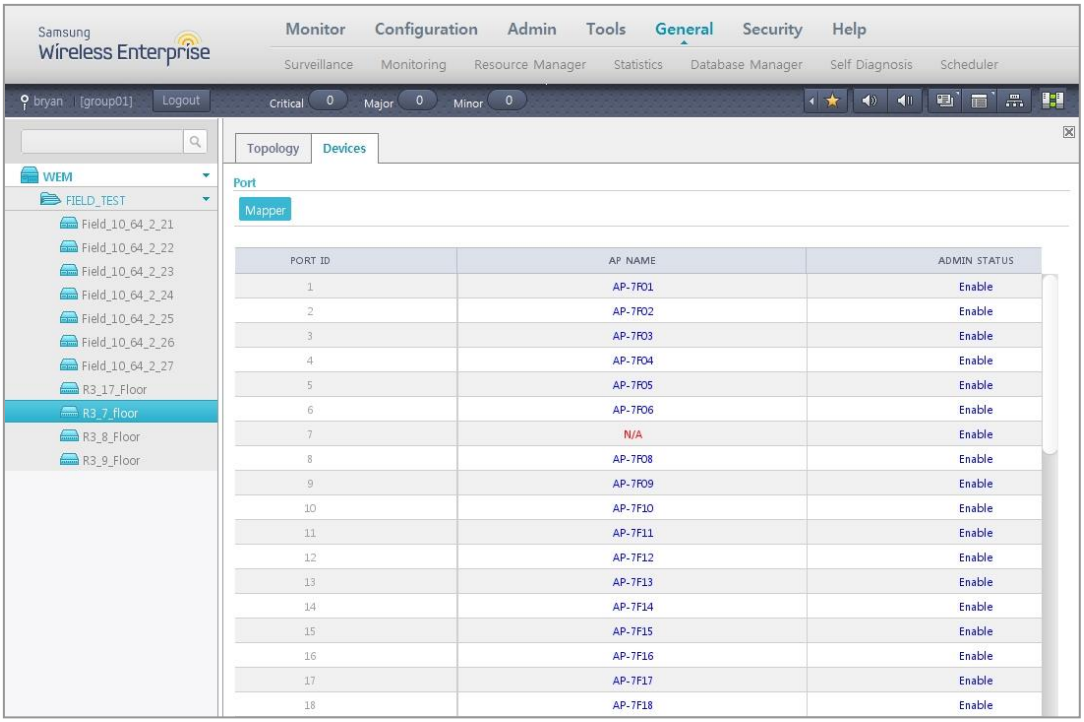


Figure 20. Screen for Information on Configuration between Switch and AP

CHAPTER 3. Monitor

This chapter describes how to use the monitoring function of the WEM.

The ‘Monitor’ menu can be distinguished as follows:

- Alarms
- Controller/Device
- AP
- Stations
- Report
- RF Map
- Dashboard
- Topology
- Security
- RRM
- WIPS
- DPI

3.1 Alarms

3.1.1 Current Alarms

The ‘Current Alarms’ displays on a ‘Event Viewer’ window where the real time events received through a server.

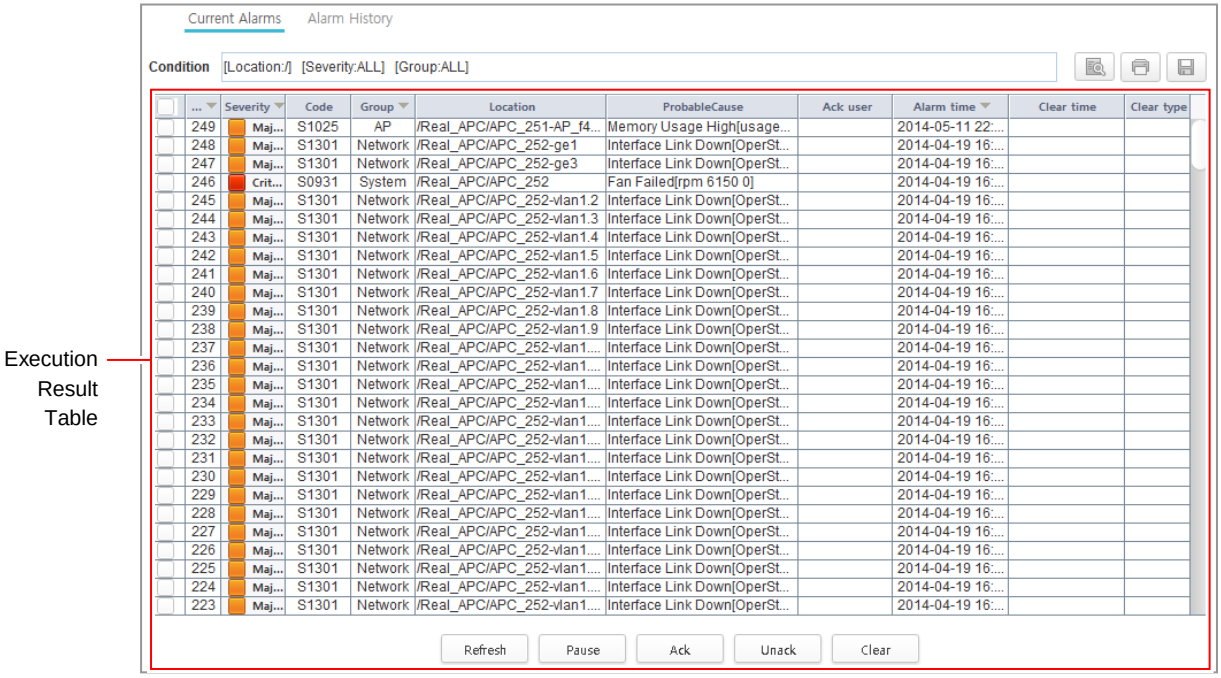


Figure 21. Current Alarm Window

The parameters for Current Alarm are as follows:

Parameter	Description
Severity	Alarm Grade - Critical: Critical Faults - Major: Major Faults - Minor: Minor Faults
Code	Displays the Alarm Code
Group	Alarm Group - system: The alarm that are generated in the APC. - ap: The alarm that are generated in the AP. - wifi: Alarm related Wi-Fi (Wireless Fidelity) - security: Alarm related security - network: Alarm related network - etc.: etc Environment?
Location	Displays the location where the alarm occurred.
Probable Cause	Displays the cause of the alarm.

Parameter	Description
Ack User	Displays which user acknowledge the Alarm.
Alarm Time	Displays the Alarm occurred time.
Clear Time	Displays the Alarm cleared time.
Clear Type	Displays how the Alarm was cleared(Auto/Manual).

Viewing and Setting Alarm Filter (Condition)

The system supports the setting to display only the specific events using alarm filtering. Click the 'Condition button ( )' at the top of the Current Alarm window to select the criteria of the event you wish to display.

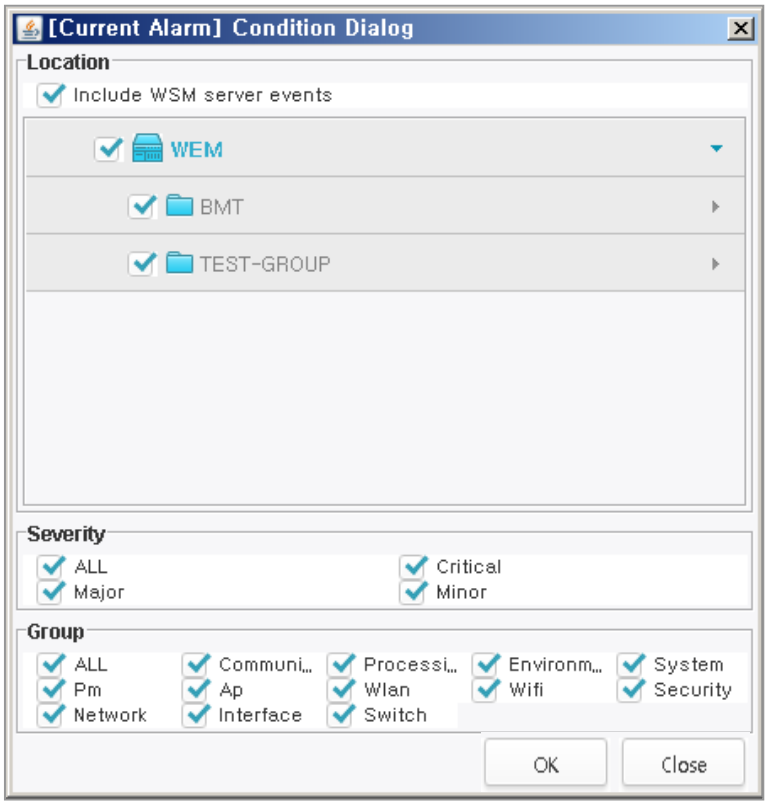


Figure 22. Current Alarm (Condition Dialog)

Viewing the Current Alarms

1) Select 'Monitor' → 'Alarm' → 'Current Alarms'.
2) Click 'Refresh' button to retrieve alarm information.
3) The search results will be displayed in the result table.
4) Click 'Save' button ( ) to save the results. Saves the alarm information in a window to an Excel file.
5) Click 'Print' button ( ) to print the results.

3.1.2 Alarm History

The ‘Alarm History’ menu allows viewing and modifying the fault information saved in the database.

The parameters of the alarm history are as follows:

Parameter	Description
Severity	Alarm Grade - Critical: Critical Faults - Major: Major Faults - Minor: Minor Faults
Clear Type	Displays how the Alarm was cleared. (Auto/Manual)
Code	Displays the Alarm Code
Group	Alarm Group - system: The alarm that are generated in the Controller. - ap: The alarm that are generated in the AP. - wifi: Alarm related Wi-Fi - security: Alarm related security - network: Alarm related network - etc.: etc
Location	Displays the Location where the alarm occurred.
Probable Cause	Displays the cause of the alarm.
Ack User	Displays which user acknowledge the alarm.
Alarm Time	Displays the alarm occurred time.
Clear Time	Displays the alarm cleared time.
Alarm Duration (Sec.)	The period of the total time from the time an alarm had occurred to the time it was cleared.
Additional text	The additional information of the alarm.

Retrieving the Alarm History (Event History)-Post Alarm History Window

1) Select ‘Monitor’ → ‘Alarm’ → ‘Alarm History’ menu.
2) On the Tree Viewer of the main window, select the NEs for which you want to view the Alarm history. The selected NEs are displayed in the Target field. If you select All, then all the errors of the system including EMS errors are displayed. If you want to view EMS errors only, then select the ‘EMS event only’ option.
3) Set the search conditions.
   - Select the search period in the ‘Period’ field, which allows user to search with in specific Date and Time.
   - User can select Alarm, Status, Fault or All in the ‘Event Type’ field. If you select Alarm, you can select a value in the ‘Severity’, ‘Group’, ‘Ack’, ‘Clear’, and ‘Code’ field to specify the searching conditions. If you select ‘Status’ or ‘Fault’, the ‘Severity’, ‘Group’, ‘Ack’, ‘Clear’, and ‘Code’ values are not used as the searching conditions. If you select all in the Event type field, all messages will be displayed.

- Select a type of alarm group in ‘Group’.
- Select an alarm code in ‘Code’.
- Select fault recognition and release in ‘Ack’ and ‘Clear’.

4) Click ‘Search’ button.
5) The search results will be displayed in the result table.
6) Click the ‘Save’ button to save the result.

Ack/Unack Alarms

1) After viewing the alarm history, select the alarms that you want to acknowledge in the results table
2) Click ‘Ack’ button.
3) Check whether the selected alarms have been acknowledged in the ‘No.’ column of the results table.
4) If you want to unacknowledged alarms, select them in the results table and click ‘Unack’.

Clear Alarm

1) After viewing the alarm history, select the alarm that you want to ack.
2) Click ‘Clear’ button.
3) Check whether the selected alarms have been cleared in the background color of the ‘Severity’ column and the ‘ClearTime’ column of the results table.

3.2 Controller/Device

3.2.1 Summarized Controller/Device Information

When WEM in the tree viewer is selected while 'Monitoring' → 'Controller/Device' has been selected, the summarized information on all controllers that the WEM now manages is provided in a form of table. If a specific cluster or controller group is selected instead of WEM, the summarized information on the controller belonging to the group can be viewed.

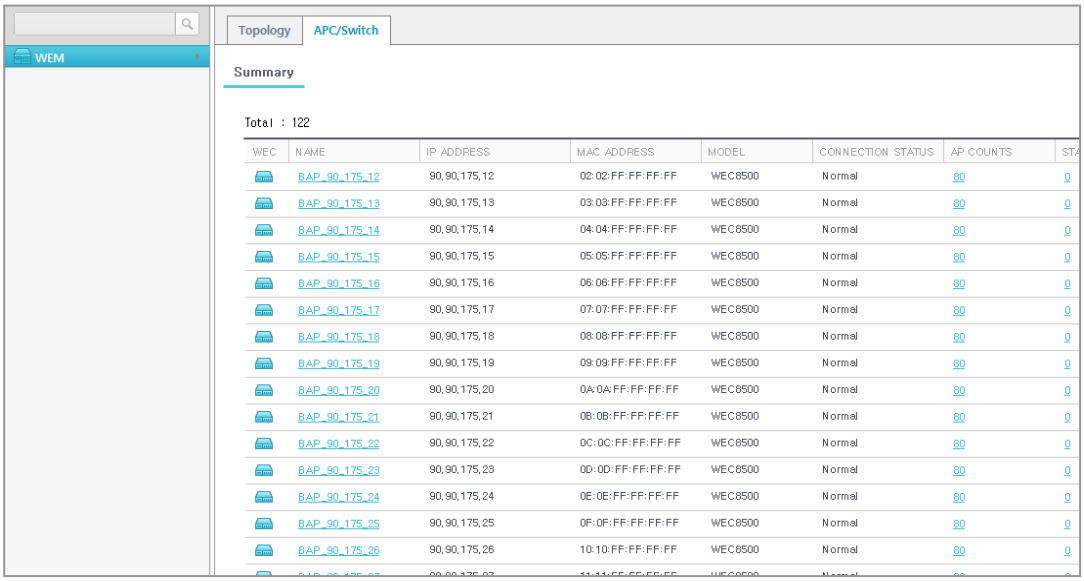


Figure 23. Summarized Controller Information Window

The description on the summarized controller information is as follows:

Item	Description
WEC	A link immediately accessing WEB GUI of the controller. Click the icon and then immediately move to the WEB GUI login screen of the controller.
Name	Name of the controller
IP Address	IP address of the controller
MAC Address	MAC address of the controller
Model	Controller Models - WEC8500 - WEC8050
Connection Status	Connection status between WEM and the controller - Normal - Abnormal
AP Counts	Total number of APs connected to the controller
Station Counts	Total number of stations connected to the controller * There may be any difference between the real time information and the recent 5-minute information stored in WEM DB.

3.2.2 Detailed Information on Controller

If you select a specific controller in the tree viewer while having selected 'Monitoring' → 'Controller/Device' in the menu or click the name of the specific controller in the table of the summarized controller information, you can view the following information on the controller:

- System
- DHCP
- Performance
- Security
- Radio

3.2.2.1 System

This shows the information on the system, software, resource, environment, etc. of the controller through tables and graphs.

System Configuration Information_WEC8500

This illustrates the configuration of the controller and the status of each interface in a form of figure.

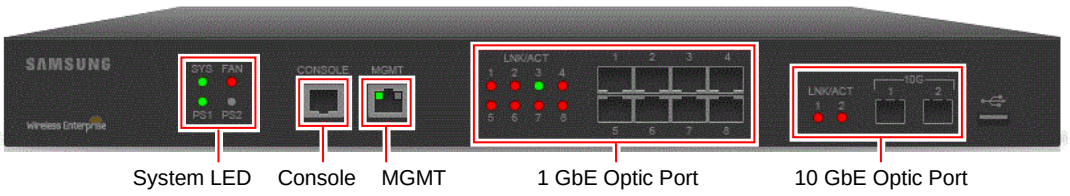


Figure 24. WEC8500 Configuration

LED for WEC8500 System

LED	Status	Description
SYS	Green	The system is normally operating.
	Red	The system is ready for booting.
FAN (Fan Module)	Green	The installed fan module is normally operating.
	Red	The fan module has a fault.
PS1 (Power Module 1)	Green	The installed power module 1 is normally operating
	Red	While the power module 1 is installed, the power is off or a fault occurs.
	Off	The power module 1 was not installed.
PS2 (Power Module 2)	Green	The installed power module 2 is normally operating

LED	Status	Description
	Red	While the power module 2 is installed, the power is off or a fault occurs.
	Off	The power module 2 was not installed.

WEC8500 Management Port

For management, WEC8500 provides 1 GbE/100 base-T UTP port (RJ-45) and it works in the 10/100 Mbps half or full duplex mode or in the 1000 Mbps full duplex mode. Besides, WEC8500 that supports the automatic MDI/MDI-X function can use the straight-through cable to all network connections for PC, server, another switch or network hub.

WEC8500 Optical Port

WEC8500 provides two 10 GbE optical ports and eight 1 GbE optical ports, each of which the status is displayed in LED.

Item	Port & LED	Description
10 GbE Port	LINK/ACT 1, LINK/ACT 2	Indicates the status of LINK/ACT of each port. - Green turns on when the link is normally connected. - Red turns on when the link has a fault. - Turned off when it is down by the setting.
	10G 1, 10G 2	10 GbE optical module connector
1 GbE Port	LINK/ACT 1~ LINK/ACT 8	Indicates the status of LINK/ACT of each port. - Green turns on when the link is normally connected. - Red turns on when the link has a fault. - Turned off when it is down by the setting.
	1G 1~1G 8	1 GbE optical module connector

System Configuration Information_WEC8050

This illustrates the configuration of the controller and the status of each interface in a form of figure.

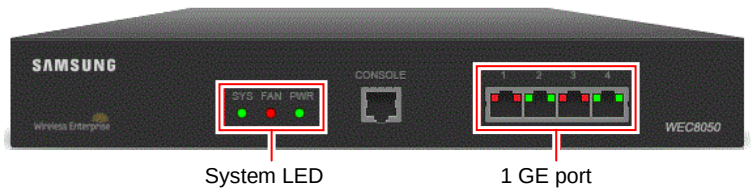


Figure 25. WEC8050 Configuration

LED for WEC8050 System

LED	Status	Description
SYS	Green	The system is normally operating.
	Red	The system is ready for booting.
FAN (Fan Module)	Green	The installed fan module is normally operating.
	Red	The fan module has a fault.
PWR (Power)	Green	The installed power module is normally operating.
	Red	While the power module is installed, the power is off or a fault occurs.

WEC8050 Optical Port

WEC8050 provides four 1 GbE optical ports, each of which the operating status is displayed in LED.

Item	Port & LED	Description
1 GE port	LINK/ACT 1~ LINK/ACT 4	Indicates the status of LINK/ACT of each port. - Green turns on when the link is normally connected. - Red turns on when the link has a fault. - Turned off when it is down by the setting.
	1G 1~1G 4	1 GbE optical module connector

Resource/Environment

Resource/environment information shows the information on the CPU load, memory usage, and disk usage history as shown in the figure below. When the general information screen is viewed for the first time, the information is not displayed. Execute the period setting icon on the right bottom of the graph and then and designate the period to display the information. By using the icon on the left bottom, it is possible to change in a form of table and it is also possible to store in a file (CSV format).

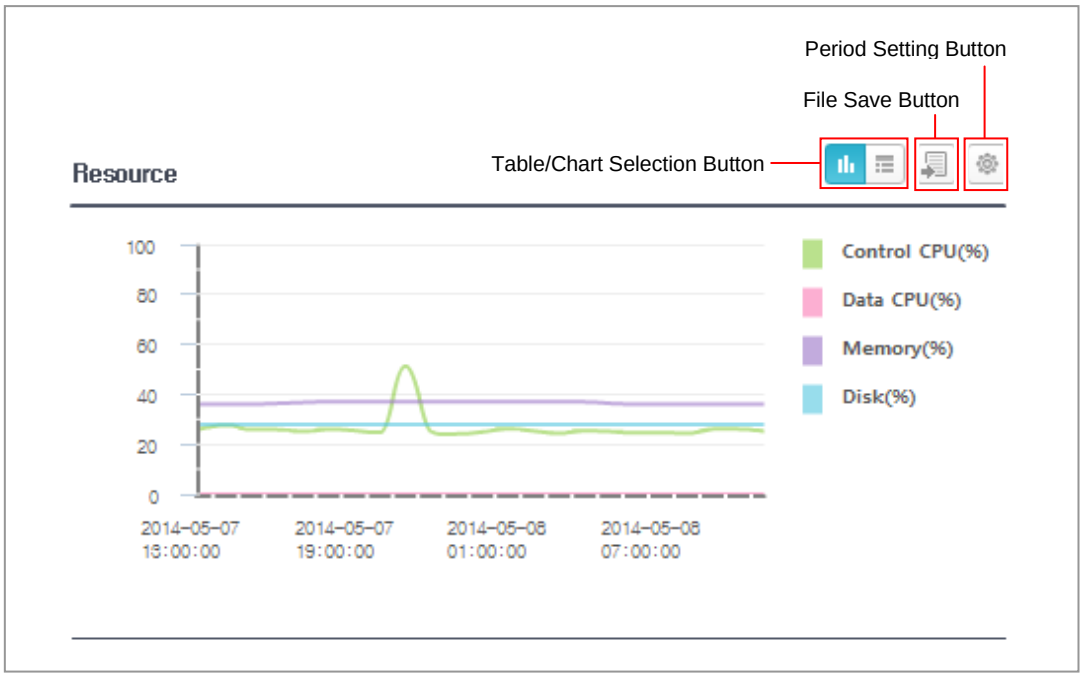


Figure 26. Resource/Environment Information

Temperature

The temperature information shows the real-time information on the temperature sensor installed on the CPU and board of the controller (only for WEC8500 model; No temperature information provided for WEC8050 model).

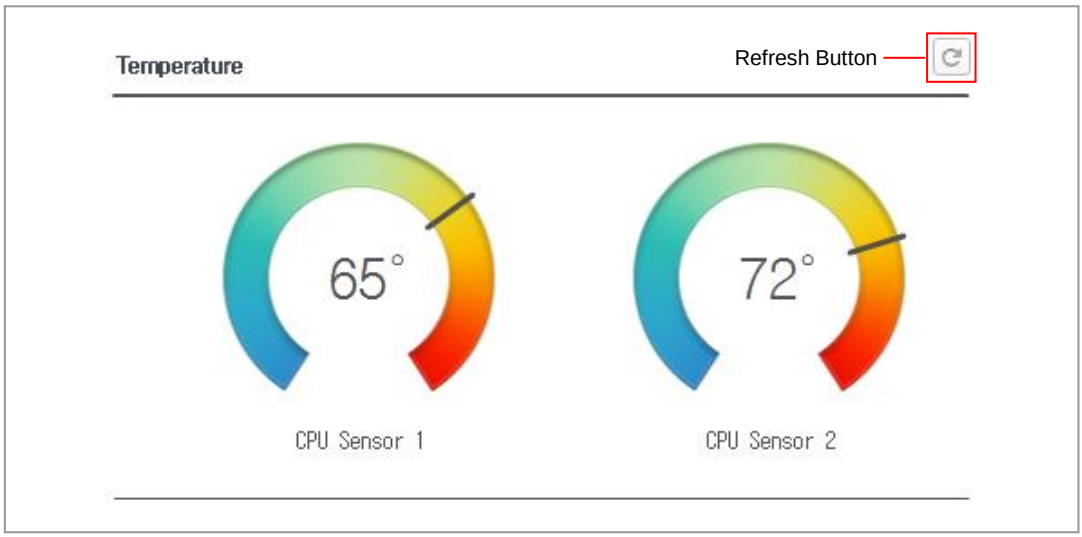


Figure 27. Controller Temperature Information

system information

Item	Description
The name of the system	Name of the controller
Location Information	Information on the location of equipment
The model name.	Equipment model name - WEC8500 - WEC8050
MAC address	MAC address of the controller
IP Address	IP address of the controller interface set to connect with WEM
Serial number	Unique manufacturing number of the controller
System Operating Time	The operating time elapsing after the system runs
System time	Current system time

Software

Item	Description
ACTIVE Version	Information on the firmware version of the controller now working
ACTIVE Date	Information on the firmware build time of the controller now working
STANDBY Version	Information on the backup firmware version of the controller
STANDBY Date	Information on the backup firmware build time of the controller

Alarm

Item	Description
CRITICAL	Number of critical alarms of the controller
MAJOR	Number of major alarms of the controller
MINOR	Number of minor alarms of the controller

APs

Item	Description
Total	Total number of APs connected to the controller
Activated	Number of activated APs connected to the controller. Click the link and then move immediately to the AP list information window.
Deactivated	Number of deactivated APs connected to the controller. Click the link and then move immediately to the AP list information window.

Unauthorized APs

Item	Description
Count	Total counts of unauthorized APs detected in the controller

Connected Terminals

Item	Description
Count	Total number of terminals connected to the controller. Click the link and then immediately move to the station information window.

Port

Provide the information on the setting and operating status of the optical ports and management ports embedded in the controller. Click the name of the linked port in blue to view the statistical information on the port.

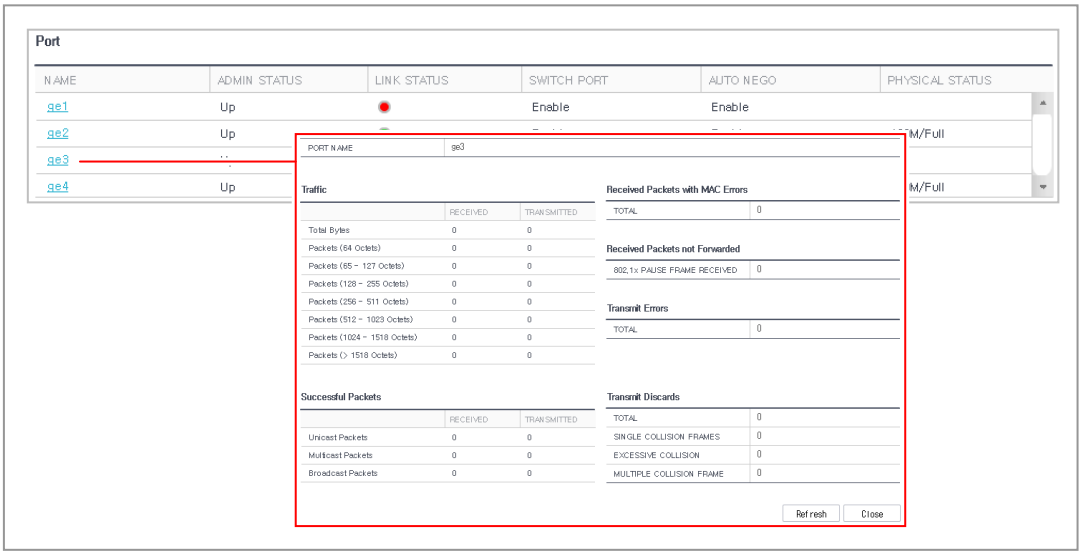


Figure 28. Port Information

Item	Description
NAME	Port name
ADMIN STATUS	The configuration status of the port by the operator (up or down)
LINK STATUS	Actual operating status of the port (Green: Up, Red: Down)
SWITCH PORT	Configuration status of switch function (enabled/disabled)
AUTO NEGO	Configuration status of auto negotiation mode (enabled/disabled)
PHYSICAL STATUS	Link connection status (Speed: 10M, 100M, 1G, 10G, Transmission Mode: Full Duplex, Half Duplex)

3.2.2.2 DHCP Information

3.2.2.2.1 Lists

Displays the DHCP information for wireless terminals.

The parameters of the DHCP List are as follows:

Parameter	Description
MAC ADDRESS	MAC address of wireless terminal for DHCP
STATION IP ADDRESS	IP address of wireless terminal for DHCP
Server IP ADDRESS	IP address for DHCP server
LEASE DURATION	Lease duration after DHCP connecting
LEASE TIME	DHCP lease time

Retrieve DHCP List

1) Select the AP Controller on the Tree Viewer which user wants to search.
2) Go to 'Monitor' → 'Controller/Device' → 'DHCP' → 'Lists' menu.
3) Displays DHCP information.

3.2.2.2.2 Statistics

User can view the DHCP statistics.

The parameters of the DHCP statistics are as follows:

Parameter	Description
BOOTP-REQUEST COUNTs	Request packet count for BOOTP protocol
BOOTP-INVALID COUNTs (Abnormal Format)	Invalid packet count of received BOOTP packet The number of invalid packet of which format is abnormal among received BOOTP packet.
BOOTP-RESPONSE COUNTs	Response packet count for BOOTP protocol
BOOTP-INVALID COUNTs (UNKNOWN STATIONs)	The number of invalid packet in which there is no assigned lease among received BOOTP request packet.
BOOTP-INVALID COUNTs (NOT SERVING SUBNET)	The number of invalid packet which is the band in which the IP assign is not provided among the received BOOTP request packet.
DHCP v4 DISCOVERS	Received DHCPv4 DISCOVER packet count
DHCP v4 INVALIDs (Abnormal Format)	Invalid packet count which is wrong format
DHCP v4 INVALIDs (UNKNOWN STATIONs)	The number of invalid packet in which there is no assigned lease among received DHCPv4 request packet.
DHCP v4 OFFERs	DHCPv4 [OFFER] packet count

Parameter	Description
DHCP v4 REQUEST COUNTs	DHCPv4 [REQUEST] packet count
DHCP v4 DECLINEs	DHCPv4 [DECLINE] packet count
DHCP v4 ACKs	DHCPv4 [ACK] packet count
DHCP v4 NAKs	DHCPv4 [NACK] packet count
DHCP v4 RELEASE	DHCPv4 [RELEASE] packet count
DHCP v4 INFORMs	DHCPv4 [INFORM] packet count
DHCP v4 INVALIDs (NOT SERVING SUBNET)	The number of invalid packet which is the band in which the IP assign is not provided among the received DHCPv4 request packet.

3.2.2.3 Performance

'Performance' Management manages items that are related to the performance of controller.

The performance management refers to managing the items related to the performance of AP Controller. It provides the function to display the data of the performance for the controller in real time on the screen. It provides the function to save and print.

3.2.2.3.1 CPU Utilization

WEM System monitors and retrieves CPU and Fan performance and Temperature in real time, user can view the result in graph/table format.

Retrieve CPU Performance

1) Select the AP Controller on the Tree Viewer which user wants to check.
2) Go to 'Monitor' → 'Controller/Device' → 'Performance' → 'CPU' menu.
3) Select 'CPU ID' on left of the window.
4) Select checkbox of 'CPU Usage' item.
5) User can set the interval 'Period' in seconds [10, 20, 30 & 60] at the 'Period' field.
6) Click 'Start' button to start monitoring. Click 'Stop' button, to stop the real timer monitoring.
7) User has an option to change output display format by clicking 'Graph' or 'Table' tab button in the down-right window.
8) Click 'Export' button to save the output graph and table in a file.

Retrieving Fan Performance

1) Select the AP Controller on the Tree Viewer which user want to check.
2) Go to 'Monitor' → 'Controller/Device' → 'Performance' → 'FAN' menu.
3) Select 'FAN ID' in the left window.
4) Select the checkbox of 'Fan RPM Level' Performance Maintenance.
5) User can set interval period in Seconds [10, 20, 30 & 60] at the 'Period' field.

6) Click ‘Start’ button to start monitoring. Click ‘Stop’ button, to stop the real-time monitoring.
7) User has an option to change output display format by clicking as ‘Graph’ or, ‘Table’ tab button in the down-right window.
8) Click ‘Export’ button to save the output graph and table in a file.

Retrieving Temperature

1) Select the AP Controller on the Tree Viewer which user want to check.
2) Go to ‘Monitor’ → ‘Controller/Device’ → ‘Performance’ → ‘Temp’.
3) Select ‘Temp Sensor ID’ in the left window.
4) Select the checkbox of ‘Temperature’ performance metrics.
5) User can set interval period in Seconds [10, 20, 30 & 60] at the ‘Period’ field.
6) Click ‘Start’ button to start monitoring. Click ‘Stop’ button, to stop the real-time monitoring.
7) User has an option to change output display format by clicking as ‘Graph’ or ‘Table’ tab button in the down-right window.
8) Click ‘Export’ button to save the output graph and table in a file.

3.2.2.3.2 Memory Usage

WEM System monitors and provides Memory usage in real time, user can view the result in graph/table format

Retrieve Memory Usage Performance

1) Select the AP Controller on the Tree Viewer which user wants to check.
2) Go to ‘Monitor’ → ‘Controller/Device’ → ‘Performance’ → ‘Memory’ menu.
3) Select the checkbox items which user wants to measure the performance in the left side of the window. Each performance measure are as follows.
   - Memory Total Size (GB): Total memory size
   - Memory Used Size (GB): Used memory size
   - Memory Usage (%): Memory usage in percentage
4) User can set the interval ‘Period in Seconds [10, 20, 30 & 60] at the ‘Period’ field.
5) Click ‘Start’ button to start monitoring. Click ‘Stop’ button, to stop the current real time monitoring.
6) User has an option to change output display format by clicking ‘Graph’ or ‘Table’ tab button in the down-right window
7) Click ‘Export’ button to save the output graph and table in a file.

3.2.2.3.3 Disk Usage

WEM system monitors and provides disk usage in real time; user can view the result in graph/table format.

Retrieve Disk Performance

1) Select the AP Controller on the Tree Viewer which user want to check.
2) Go to 'Monitor' → 'Controller/Device' → 'Performance' → 'Disk' menu.
3) Select the checkbox items which user wants to measure the performance in the left side of the window. Each performance measure is as follows.
   - Disk Total Size (GB): total memory size
   - Disk Used Size (GB): used memory size
   - Disk Free Size (GB): free memory size
   - Disk Usage (%): memory usage in percentage
4) User can set interval period in Seconds [10, 20, 30 & 60] at the 'Period' field.
5) Click 'Start' button to start monitoring. Click 'Stop' button, to stop the real-time monitoring.
6) User has an option to change output display format by clicking as 'Graph' or, 'Table' tab button in the down-right window.
7) Click 'Export' button to save the output graph and table in a file.

3.2.2.3.4 Interface

WEM System monitors and provides interface status of APC in real time, user can view the result in graph/table format.

Retrieving Interface Performance

1) Select the AP Controller on the Tree Viewer which user wants to check.
2) Go to 'Monitor' → 'Controller/Device' → 'Performance' → 'Interface' menu.
3) Select 'INTERFACE Name' to the left of the window.
4) Select the checkbox items which user wants to measure the performance in the left side of the window. Each performance measure is as follows.
   - In Octets (Kbps): Received data octets count
   - In UcastPkts (Kbps): Received unicast packet count
   - In Discards (Kbps): Discarded packets count in received data.
   - In Errors (Kbps): Error packets count in the received data
   - In UnknownProtos (Kbps): Unknown packet count of the received data
   - Out Octets (Kbps): Transmitted data octets count.
   - Out UcastPkts (Kbps): Transmitted unicast packets count
   - Out Discards (Kbps): Discarded packets counts in transmitted data
   - Out Errors (Kbps): Error packets count in the transmitted data
5) User can set interval period in seconds [10, 20, 30 & 60] at the 'Period' field.
6) Click 'Start' button to start monitoring. Click 'Stop' button, to stop the real time monitoring.
7) User has an option to change output display format by clicking 'Graph' or 'Table' tab button in the down-right window.
8) Click 'Export' button to save the output graph and table in a file.

3.2.2.4 Security

3.2.2.4.1 Guest User

Displays the security information of the Guest User registered in a controller on the screen.

Parameter	Description
NAME	Guest User Name
START TIME	Start Time for Guest User
END TIME	End Time for Guest User
FULL NAME	User Name for Guest User
STATUS	Status for Guest User (Enable, Disable)
SPONSOR	An Employee of the Organization
GRANTOR	Name of the Person who registered Guest User

Retrieve Security Information

1) Select the AC Controller on the Tree Viewer which user wants to search.
2) Go to 'Monitor' → 'Controller/Device' → 'Security' → 'Guest User' menu.
3) Displays 'Guest User' security information.

3.2.2.4.2 RADIUS

Displays the RADIUS information for selected APC.

Parameter	Description
ID	ID for RADIUS server
TYPE	RADIUS Server type Authentication Accounting Authentication/Accounting
IP ADDRESS	RADIUS server IP address
PORT	RADIUS support port

Retrieving

1) Select the AC Controller on the Tree Viewer which user wants to search.
2) Go to 'Monitor' → 'Controller/Device' → 'Security' → 'RADIUS' menu.
3) Displays the 'RADIUS' information.

3.2.2.4.3 TACACS+

Displays the TACACS+ information for selected APC.

Parameter	Description
ID	TACACS+ server ID
IP address	TACACS+ server IP
Shared Key	TACACS+ server shared key
Port	TACACS+ server port number (range: 1-65535, default: 49)
Source IP address	Source IP address of the TACACS+ message This must be one of the IP addresses configured in the W-EP WLAN system.
Status	Status of packet transmission to TACACS+ server (default: enable)

Retrieving

1) Select the AC Controller on the Tree Viewer which user wants to search.
2) Go to 'Monitor' → 'Controller/Device' → 'Security' → 'TACACS+' menu.
3) Displays the 'TACACS+' information.

3.2.2.5 Radio

The controller settings for wireless standards IEEE 802.11a/n/ac and IEEE 802.11b/g/n can be retrieved in this section.

Select the AP Controller on the Tree Viewer which user wants to check 802.11 information. Select 'Monitor' → 'Controller/Device' → 'Radio' → '802.11a/n/ac' or '802.11b/g/n'.

The parameters for IEEE 802.11a/n/ac and IEEE 802.11b/g/n are as follows:

IEEE 802.11a/n/ac

[Parameter]

Parameter	Description
RTS THRESHOLD	RTS (Request To Send) threshold
SHORT RETRY	Short retry limit to the number of times
LONG RETRY	Long retry limit to the number of times
FRAGMENTATION THRESHOLD	Fragmentation threshold
TX MSDU LIFE TIME	Tx MSDU (MAC Service Data Unit) valid time
RX MSDU LIFE TIME	Rx MSDU valid time

[802.11h]

Parameter	Description
POWER CONSTRAINT	Tx Power Limit
CHANNEL SWITCH ENABLE	Channel switch availability
CHANNEL SWITCH MODE	Channel switch mode
CHANNEL SWITCH COUNTS	The number of channel switches

IEEE 802.11b/g/n

[Parameter]

Parameter	Description
RTS THRESHOLD	RTS threshold
SHORT RETRY	Short retry limit to the number of times
LONG RETRY	Long retry limit to the number of times
FRAGMENTATION THRESHOLD	Fragmentation threshold
TX MSDU LIFE TIME	Tx MSDU (MAC Service Data Unit) valid time
RX MSDU LIFE TIME	Rx MSDU valid time

3.3 AP

3.3.1 Summarized AP Information

From the Summarized AP Information menu, the list of all APs registered now in the WEM and the summarized information by AP can be viewed. The summarized AP information screen is as shown below.

Figure 29. Summarized Information Screen

Each item on the summarized AP information screen is as shown below.

Item	Description
Link Test	Provide a function of testing whether the physical link between the AP and the controller works normally. Click the hyperlink and then the ping test for the selected AP is conducted by the controller and the test result is displayed on the pop-up screen in the WEM.
Name	Provide a hyperlink function to the detailed information window for a specific AP as the information on the name of the AP.
IP Address	IP address of the AP WAN interface
MAC Address	Physical address of the AP WAN interface
Controller	A controller to which an AP is registered
Location Info	As hyperlink information for the location on the RF map of the AP. Click the link to immediately move to the concerned RF map.
Mode	AP operation mode - General AP: Basic AP mode for user services - Root AP: A backbone AP for the repeater service. The wireless terminal is connected to the repeater AP and then the wired network via the root AP. - Repeater AP: As an edge AP for repeater service, the AP actually

Item	Description
	connected by the wireless terminal. - Sniffer AP: An AP which does not provide a user service but provides a function of capturing a packet in an air section packet (If the AP mode is a sniffer AP, establish the client IP address.) - Relay AP: An AP connecting the repeater AP with the root AP wirelessly
Admin Status	Information on the operator configuration status for the operation of the AP (Up, Down)
Operating Status	Information on actual operating status of the AP (Up, Down)
Ethernet Speed (MBPS)	Current speed of the AP
Ethernet Duplex	Duplex info of the AP
5 GHz channel	Information on 5 GHz channel in use by the AP
2.4 GHz channel	Information on 2.4 GHz channel in use by the AP
Radio Base MAC	Information on the base MAC address allocated to the WLAN interface
Model	AP model name
No. of Connected Terminals	The number of wireless terminals connected to the AP. Provide hyperlink and move to the screen on the list of the concerned terminal information when the information is clicked.
Spectrum Analysis	As a hyperlink to operate the spectrum analysis function for the wireless environment near the AP. Click the link and then move to 'Tool' → 'Spectrum Analysis' screen.

Viewing

1) Go to 'Monitoring' → 'AP' menu.
2) The list of registered APs is displayed on the screen.

Information on Number of APs

Information on the number of APs is provided on the left upper position of the Summarized AP Information screen.
If the condition to be viewed is changed by the setting of the condition for viewing, the information on the number of APs is changed.

Setting Number of List Lines of APs per Page

Use the Setting Number of APs per Page button on the right upper position of the Summarized AP Information screen to set the number of APs to be displayed per one page. The range is adjustable between 10 and 100.

Figure 30. Screen of Setting Number of List Lines of APs per Page

Specifying Search Conditions

Click the Specifying Search Conditions button ( ) on the Summarized AP Information screen to view information on only APs you want. The search conditions below can be set.

- Name of the controller
- AP mode
- Configuration status
- Operating status
- Ethernet Speed(MBPS)
- Ethernet Duplex

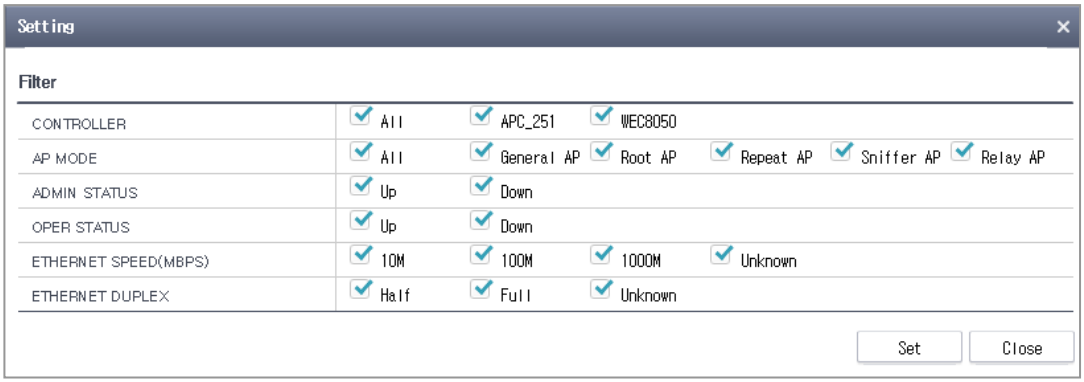


Figure 31. Screen on Specifying Search Conditions

Storing Summarized Information

When you click the ‘Save’ button ( ) on the right top in the screen on Summarized AP Information, you can store the summarized information on the currently searched APs in a CSV file.

Link Test

When you click the hyperlink on the link test items of the screen on Summarized AP Information, you can conduct the link test for the AP.

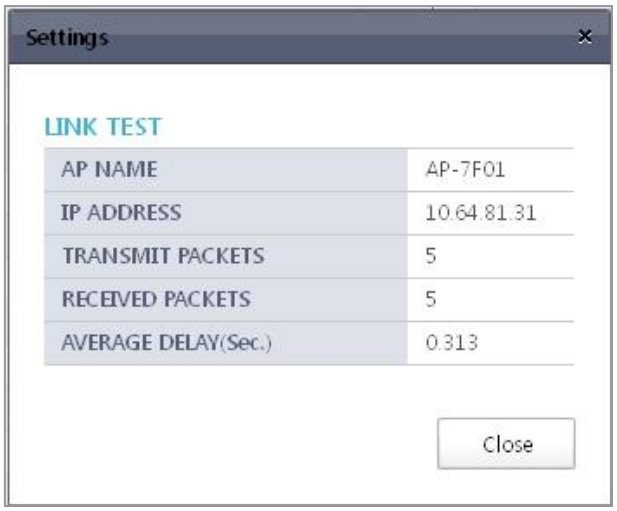


Figure 32. Link Test Screen

Map Location Information

It provides the hyperlink that can switch the list of APs on the screen on Summarized AP Information to the RF Map screen of the AP. For more information on the function, refer to the ‘RF Map’ in Chapter 3.

Spectrum Analysis

In the list of APs on the screen on Summarized AP Information, the hyperlink to execute the AP spectrum analysis immediately is provided. For more information on the function, refer to the ‘Spectrum Analysis’ in Chapter 6.

3.3.2 Detailed Information on AP

The detailed information on AP provides information on the configuration of the AP, software, operation, radio, and performance in details.

3.3.2.1 System

Viewing

1) Go to 'Monitoring' → 'AP' menu.
2) The list of registered APs is displayed on the screen.
3) Click the hyperlink in the 'Name' column of the AP you want to view in the list of APs.
4) The detailed information on the selected AP is displayed on the screen.

[Traffic]

The information on the history of AP traffic means the information on the data traffic sent and received through the WAN interface of the AP. History information is shown through the graphic or table and the history of the traffic history of the period you want by providing the setting of the viewing period may be viewed. In addition, if the file is required to be stored, it is possible to click the Save button to store the history of the viewed traffic in the file format of CSV.

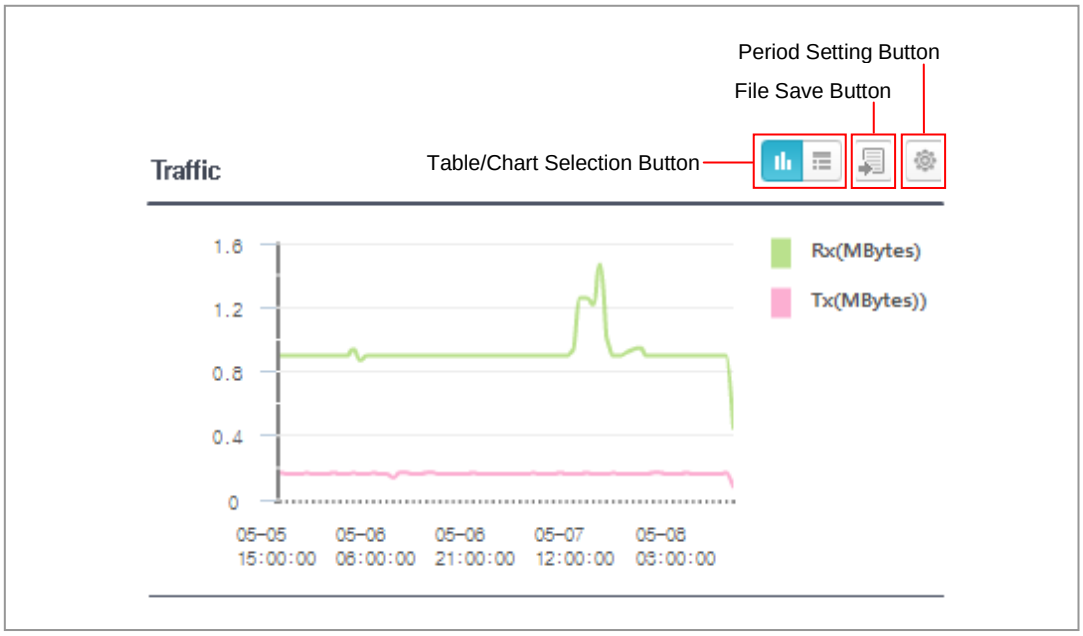


Figure 33. Traffic History Information

[CPU]

The information on the history of CPU of the AP shows the history of the CPU load of the AP by using the graph and the table. It is possible to view the history of the CPU load in the period you want to view by providing the setting of the viewing period, and if it is necessary to save the file, click the Save button and then the viewed history of the CPU load may be stored in a file format of CSV.

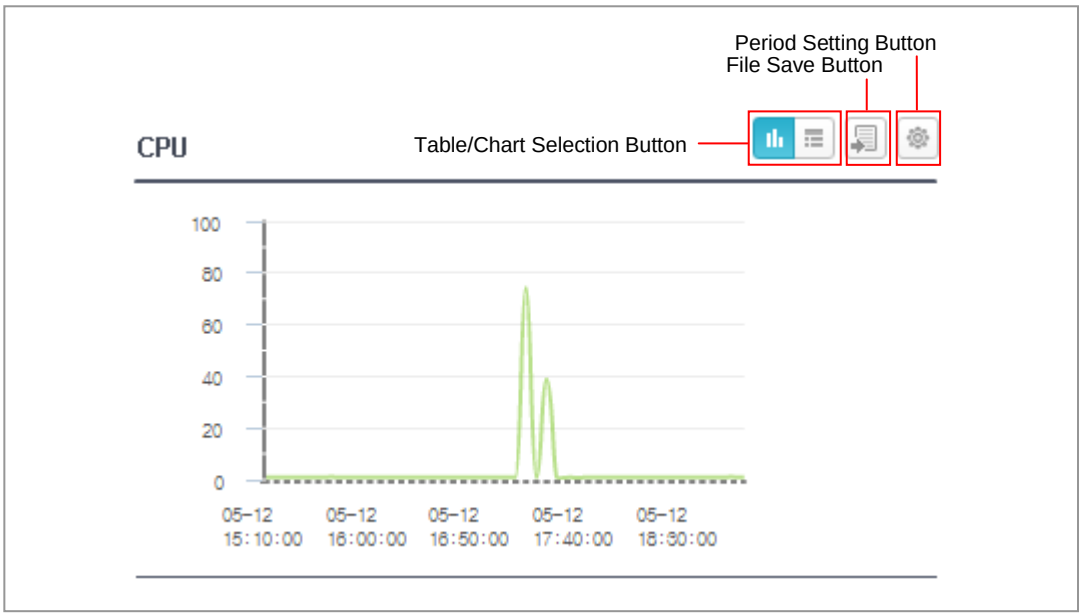


Figure 34. CPU Load History Information

[Map Location]

If the AP is registered on the RF MAP, the location of the AP is indicated on the RF MAP.

Figure 35. Map Location

[Configuration]

Item	Description
Name of AP	Name of AP (Possible to change in Configuration Management)
Group Name	The name of AP group where the AP is included
AP Mode	AP operation mode - General: Basic AP mode for user services - Root AP: A backbone AP for the repeater service. The wireless terminal is connected to the repeater AP and then the wired network via the root AP. - Repeater AP: As an edge AP for repeater service, the AP actually connected by the wireless terminal. - Sniffer AP: An AP which does not provide a user service but provides a function of capturing a packet in an air section packet (If the AP mode is a sniffer AP, establish the client IP address.) - Relay AP: An AP connecting the repeater AP with the root AP wirelessly
MAC Address	Physical address of the AP WAN interface
Map Location	As hyperlink information for the location on the RF map of the AP. Click the link to immediately move to the concerned RF map.
Location	Necessary to explain the location of the equipment and to be configured by the operator
Country	The configuration status of the country where the equipment is made
APC-AP Country Setting	Country setting agreement between the AP and the controller (Matched, Mismatched)
Environment	Equipment installation environment - Both - Outdoor - Indoor - Non-country
Echo Interval (sec.)	The keep-alive interval of the CAPWAP session between AP and controller
Maximum Discovery Interval (sec.)	The maximum waiting time before AP starts controller discovery
Reporting Interval (sec.)	Interval at which the statistical information on WiFi decryption error is reported
Statistical Interval (sec.)	Interval at which the WiFi statistical information is reported
Retransmission interval (sec)	The first retransmission interval of the CAPWAP control packet
Maximum Retransmission	Maximum retransmission count of the CAPWAP control packet
Echo Retransmission Interval (sec.)	The retransmission interval of the CAPWAP keep-alive packet

Item	Description
Maximum Echo Retransmission	Maximum retransmission count of the CAPWAP keep-alive packet
Configuration Status	Information on the operator configuration status for the operation of the AP (Up, Down)
Telnet	Use of Telnet (Enabled, Disabled)
SSH	Use of SSH (Secure Shell) (Enabled, Disabled)
VLAN Supported	VLAN (Virtual Local Area Network) supported (Enabled, Disabled)
NATIVE VLAN ID	Native VLAN ID information
Name of the First Controller	Name of the first controller where the AP is registered
Name of the Second Controller	Name of the second controller where the AP is registered
Name of the Third Controller	Name of the third controller where the AP is registered

[Software]

Item	Description
Active Software Version	The activated software package version
Boost Version	System boot image version

[Information]

Item	Description
Model	Model number
Serial Number	Serial manufacturing number of AP
AP local IP Address	IP address of the AP WAN interface
Operating Status	Information on actual operating status of the AP (Up, Down)
CAPWAP Status	Operating Status of CAPWAP link - IDLE: CAPWAP session is disconnected - DTLS: DTLS connection is made between AP and the controller - JOIN: A step of the AP starting the access to the controller - CONFIG: A step of the AP bringing the configuration information from the controller - DATA CHECK: A step of confirming the connection status of the CAPWAP data channel between AP and the controller - RUN: CAPWAP connection has been completed. - IMAGE: During the access of the AP to the controller, AP is being upgraded.
Radio Status 5 GHz	Information on the status of the 5 GHz radio (Up, Down)
Radio Status 2.4 GHz	Information on the status of the 2.4 GHz radio (Up, Down)

Item	Description
Up Time	The elapsed time after the AP has been booted
CAPWAP Up Time	The elapsed time after CAPWAP link is connected
RADIO Limited Number	Limited number of available radio
Number of Radio in Use	Number of radio in use
Discovery Type	Discovery type
Management IP Address	IP address used for management
Cause of Reboot	Reason for AP rebooted latest
Last Connection Time	Last connection time of AP
Spectrum Analysis	Hyperlink with spectrum analysis
Link Test	AP link test hyperlink

3.3.2.2 Radio

Viewing

1) Go to 'Monitoring' → 'AP' menu.
2) The list of registered APs is displayed on the screen.
3) Click the hyperlink in the 'Name' column of the AP you want to view in the list of APs.
4) The detailed information on the selected AP is displayed on the screen.
5) Select the Radio menu in the Detailed AP Information screen.
6) The radio information on the AP is displayed on the screen.

Real-time Channel Usage-802.11a/n/ac, 802.11b/g/n

This shows the usage of all channels, not of the radio channel now in use, in real time by using the graph. The real time information is not automatically updated and if you want to update, click the Update button on the right bottom of the graph to view the real time information again.

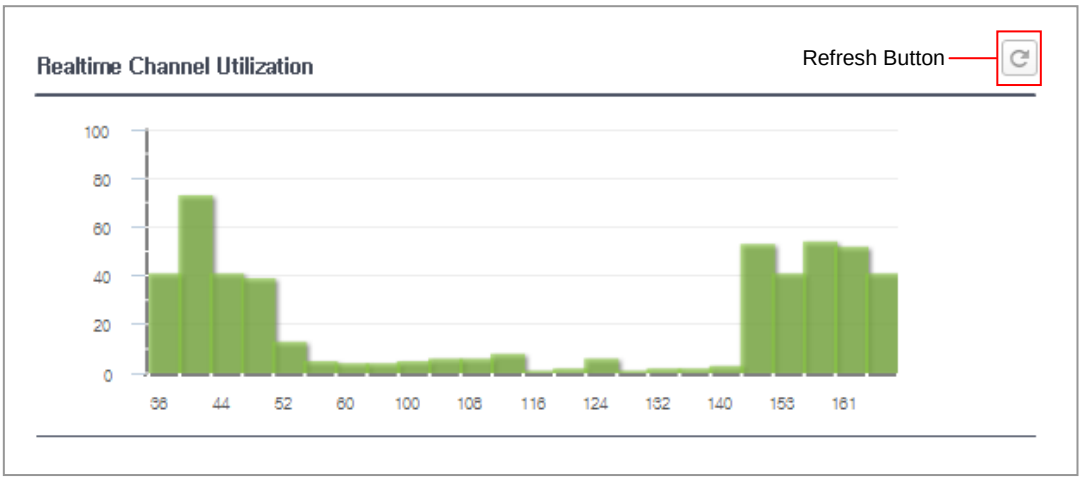


Figure 36. Real Time Channel Usage

Real-time Air Quality-802.11a/n/ac, 802.11b/g/n

This shows the air quality of all channels, not of the radio channel now in use, in real time by using the graph. The real time information is not automatically updated and if you want to update, click the Update button on the right bottom of the graph to view the real time information again.

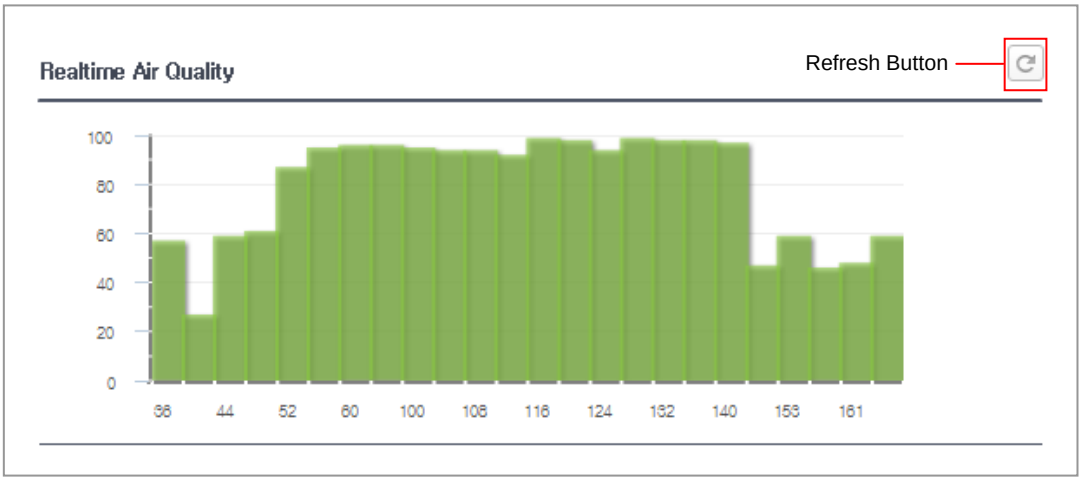


Figure 37. Real Time Air Quality

Channel Usage-802.11a/n/ac, 802.11b/g/n

This shows the history of the usage of the channel used in the AP through the graph and the table. The section of the history information may be configured by clicking the Setting of the Viewing Period on the right bottom of the graph.

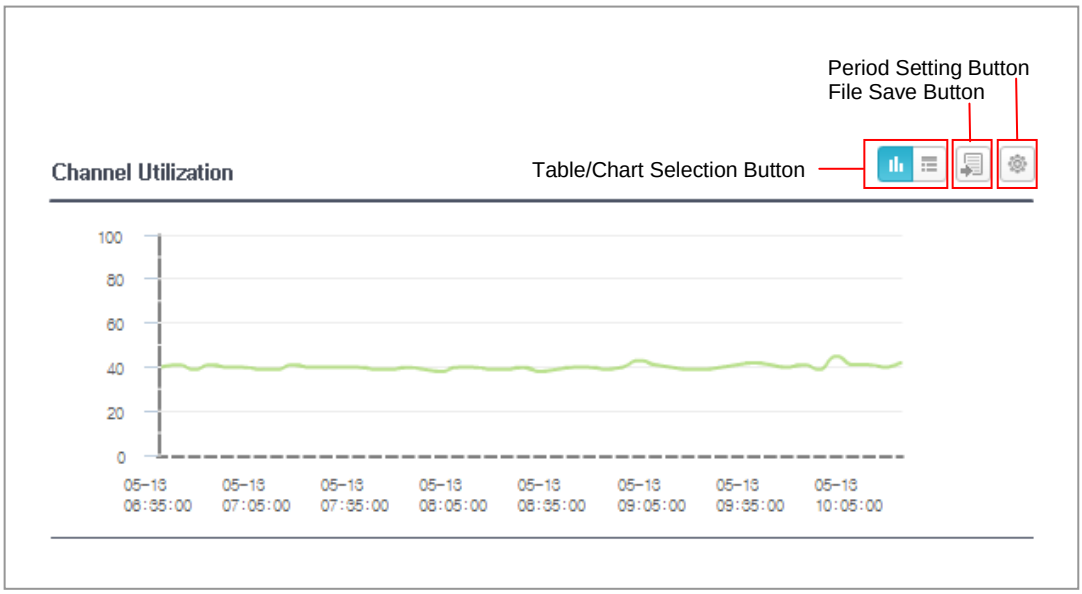


Figure 38. History of Channel Usage

Air Quality-802.11a/n/ac, 802.11b/g/n

This shows the history of the air quality of the channel used in the AP through the graph and the table. The section of the history information may be configured by clicking the Setting of the Viewing Period on the right bottom of the graph.

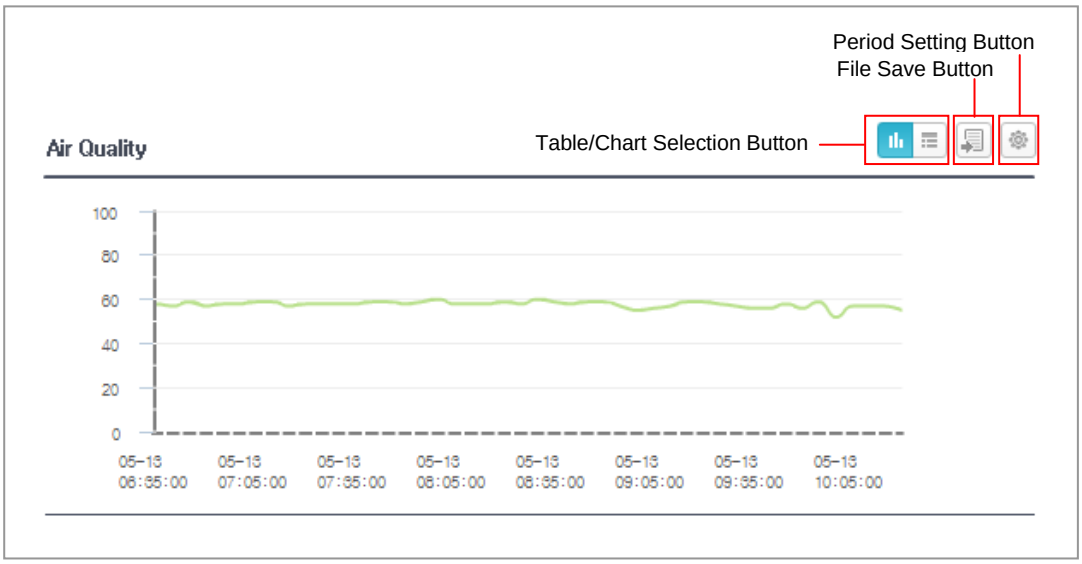


Figure 39. History of Air Quality

Traffic-802.11a/n/ac, 802.11b/g/n

The information on the history of AP radio traffic means the information on the history of data traffic sent and received through the radio interface of the AP. History information is shown through the graphic or table and the history of the traffic history of the period you want by providing the setting of the viewing period may be viewed. In addition, if the file is required to be stored, it is possible to click the Save button to store the history of the viewed traffic in the file format of CSV.

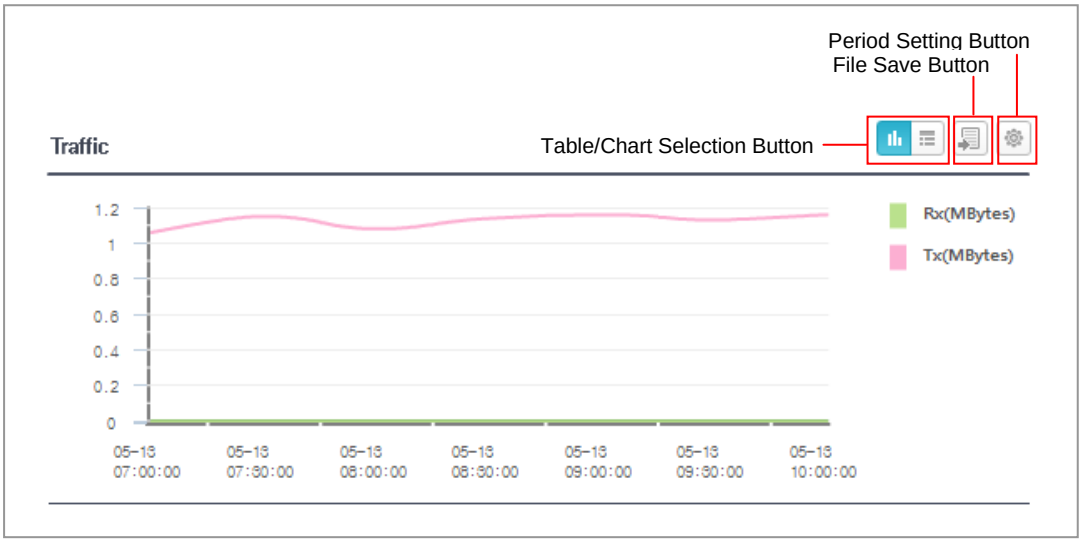


Figure 40. History of Radio Traffic

Radio Information-802.11a/n/ac

Item	Description
5 GHz Channel	Real-time channel information of 5 GHz radio
5 GHz Transmission Power	Real-time transmission power of 5 GHz radio
5 GHz Channel Usage (%)	Real-time channel usage of 5 GHz radio
5 GHz Air Quality (%)	Real-time air quality of 5 GHz radio

Radio Information-802.11b/g/n

Item	Description
2.4 GHz Channel	Real-time channel information of 2.4 GHz radio
2.4 GHz Transmission Power	Real-time transmission power of 2.4 GHz radio
2.4 GHz Channel Usage (%)	Real-time usage of the channel of 2.4 GHz radio now in use
2.4 GHz Air Quality (%)	Real-time air quality of 2.4 GHz radio now in use

List of Neighboring APs-802.11a/n/ac, 802.11b/g/n

Item	Description
Name of Neighboring AP	The name of the neighboring AP detected by the AP viewed
MAC Address	The MAC address of the neighboring AP
Radio MAC Address	The radio base MAC address of the neighboring AP
Channel	The radio channel in use by the neighboring AP
Transmission Power	The transmission power value of neighboring AP
RSSI (dBm)	The transmission power value of the neighboring AP detected by the AP being viewed

3.3.2.3 Performance

It shows the performance information of the WAN and WLAN interface of the AP in real time in a form of graph or table.

Viewing Interface Performance

1) Go to ‘Monitoring’ → ‘AP’ menu.
2) The list of registered APs is displayed on the screen.
3) Click the hyperlink in the ‘Name’ column of the AP you want to view in the list of APs.
4) The detailed information on the selected AP is displayed on the screen.
5) Select the performance menu in the Detailed AP Information screen.
6) The performance information on the AP is displayed on the screen.
7) Select ‘Interface Name; you want to see the performance information in the left of the window displayed.
8) Select the item you want to display among the performance measuring items in a

checkbox. Each performance measuring item is as follows:

- In Discards: Discarded packets among received ones
- In Errors: Error packets among received ones
- In NUcastPkts: Non-unicast packets received
- In Octets (Bytes): Data octet received
- In UcastPkts: Unicast packets received
- In Unknown Protos: Packets that do not know protocols among received ones
- Out Discards: Discarded packets among sent ones
- Out Errors (Kbps): Error packets among sent ones
- Out NUcastPkts: Non-Unicast packets sent
- Out Octets (Bytes): Data octet sent
- Out UcastPkts: Unicast packets sent

9) Select the viewing interval in the ‘Interval’.
10) To start monitoring, click the ‘Start’ button. If it has been already worked, click the ‘Stop’ button to stop the real time display.
11) Select the tab button on the ‘Graph’ and ‘Table’ on the left bottom of the window to change the screen display form.
12) Click the ‘Save’ button to store the displayed graph or table in a file.

3.4 Station

The information on the wireless terminal (station) managed by the WEM is displayed.
The summarized screen illustrates the list of all stations that are possible to view.
The detailed information by station may be viewed by clicking the hyperlink in the MAC address.

3.4.1 Summarized Station Information

The information on all wireless terminals possible to view in the WEM can be viewed.

Figure 41. Summarized Station Information Screen

Viewing

1) Go to 'Monitoring' → 'Station' menu.
2) The summarized station information screen is displayed.

Information on Number of Stations

Information on the number of stations is provided on the left upper position of the Summarized Station Information screen.
If the condition to be viewed is changed by the setting of the condition for viewing, the information on the number of stations is changed.

Setting Number of List Lines of Stations per Page

Use the Setting Number of stations per Page button on the right upper position of the Summarized Station Information screen to set the number of stations to be displayed per one page. The range is adjustable between 10 and 100.

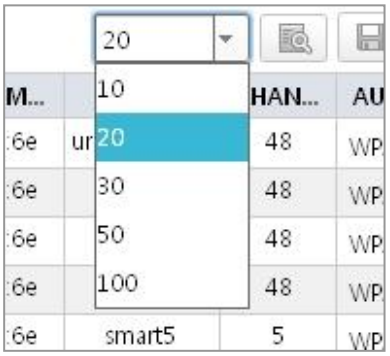


Figure 42. Screen on Setting Number of List Lines of Stations per Page

Specifying Search Conditions

Click the Specifying Search Conditions button ( ) on the Summarized Station Information screen to view information on only stations you want. The search conditions below can be set.

- Name of the controller
- Name of AP
- AP MAC address
- User name.
- SSID
- Station MAC address
- Station OS type
- Connection status

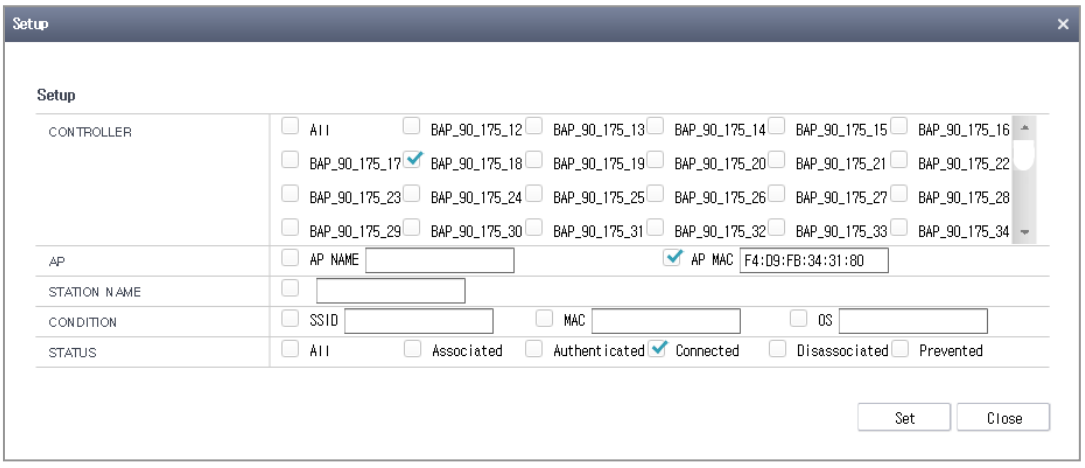


Figure 43. Screen on Specifying Search Conditions

Storing

When you click the 'Save' button ( ) on the right top in the screen on Summarized Station Information, you can store the list of the currently searched stations in a CSV file.

List of Stations

The list of stations is displayed on the top of the screen on Summarized Station Information and the description is as follows:

Item	Description
Trouble Shooting	Hyperlink to take the status test of the station
MAC Address	Station MAC address
User Name	Name of the station user
IP Address	Connected IP address used by a station
Name of AP	Name of AP to which the station now connects or last connected
AP MAC	MAC name of AP to which the station now connects or last connected
Name of Controller	Name of the controller connected to the AP to which the station now connects or last connected
MAC of Controller	Name of the MAC of the controller connected to the AP to which the station now connects or last connected
SSID	Name of SSID to which the station now connects or last connected
Channel	Radio channel used when the station is connected
Authentication	The method for authentication used when the station is connected
Encryption	The method for encryption used when the station is connected
VLAN	VLAN ID to which the station is connected
Protocol	Radio protocol used when the station is connected (2.4 GHz/5 GHz)
Status	Connection status of station
Recent Connection Time	Time when the station is connected last
Term	Time when the station is kept connected last
Map Location	Hyperlink on the location of the station on RF Map. Click it to immediately move to the map to display the location of the station.
Operating System	Operating system of the station (Android, iOS, etc.)
Transmission Rate	Data rate while the station is last connected

Traffic

The traffic information on the Summarized Station Information screen is the information on the history of total amount of traffic used by the selected stations under the conditions in the list of stations on the top. It is provided in a form of graph or table and the information on the history of station traffic during the period you want to view according to the setting of the viewing period can be viewed.

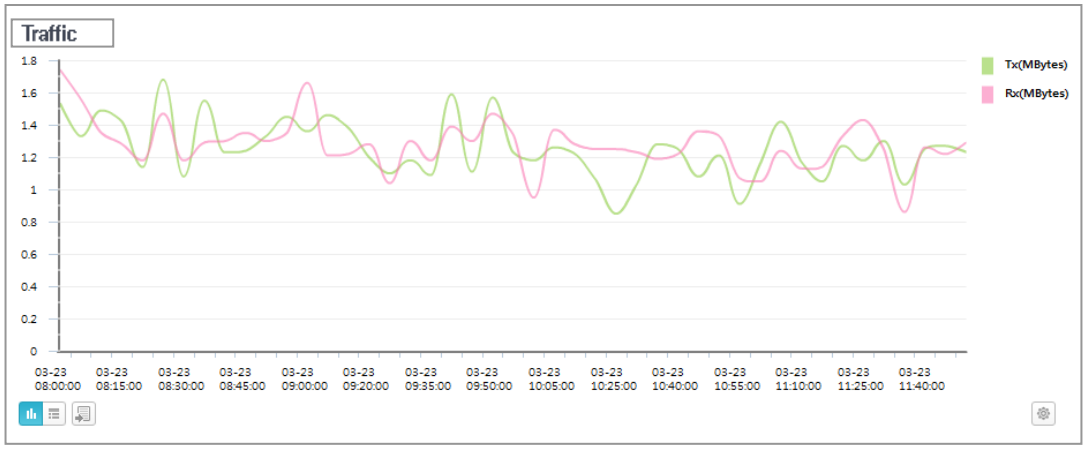


Figure 44. Total Amount of Station Traffic

Data Transmission Rate

The disconnection distribution of the stations by data transmission rate is displayed.

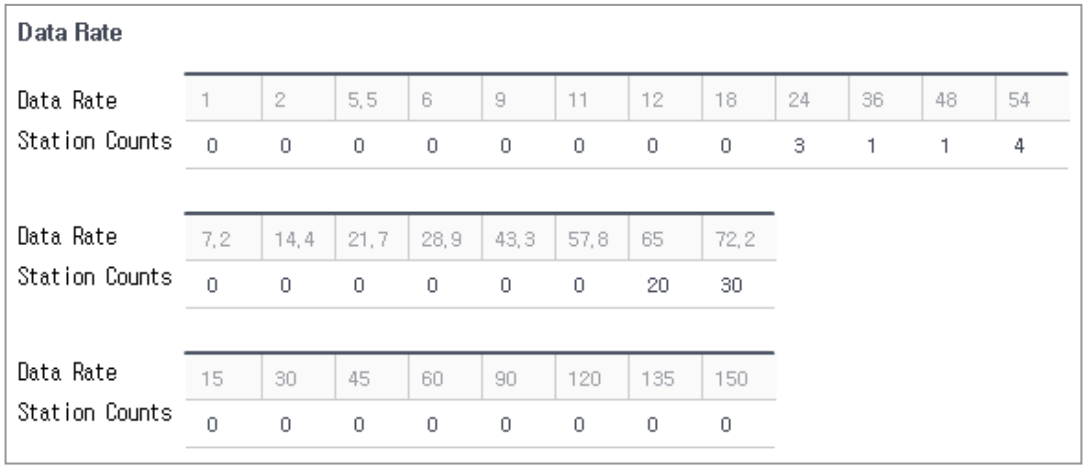


Figure 45. Station Distribution by Data Transmission Rate

3.4.2 Detailed Station Information

Viewing

1) Go to 'Monitoring' → 'Station' menu.
2) The summarized station information screen is displayed.
3) Click the hyperlink of the MAC address of the station you want to view in the list of stations on the screen for summarized station information.
4) The detailed station information screen is displayed.
5) To return to the Summarized Station Information screen, click the 'Back' button on the right top.

Station Information

Item	Description
MAC Address	Station MAC address
User Name	Name of the station user
IP Address	Connected IP address used by a station
VLAN ID	VLAN ID to which the station is connected
Dynamic VLAN	Status of configuring dynamic VLAN (Yes or No)
Data Transmission Rate Supported	Data transmission rate supportable by the station
Guest	Existence of a guest (Yes or No)
SSID	Name of SSID to which the station now connects or lastly connected
Protocol	Radio protocol used when the station is connected (2.4 GHz/ 5 GHz)
Channel	Radio channel used when the station is connected
RSSI (dBm)	Real time RSSI value of the station
SNR	SNR value of Station
Data Transmission Rate	Data transmission rate now connected
NCHO Mode	Type of service mode of AirMove (APP/STATION)
Handover Type	Type of handover: 802.11 HO (Station Controlled), AirMove (Network Controlled)
Reason for Handover	Reason for handover (Assoc, Reassoc, etc.)
Cluster Roll	Station roll upon the handover of Intercontroller L3
Cluster Anchor IP Address	IP address of the anchor roll controller upon the handover of Intercontroller L3
Cluster Foreign IP Address	IP address of the foreign roll controller upon the handover of Intercontroller L3
Connection Time	Time when the station is connected last
Status	Various status of the station
Performance	Performance of the station

Controller/AP Information

Item	Description
Name of Controller	Name of the controller connected to the AP to which the station now connects or lastly connected
IP Address of Controller	IP address of the controller connected to the AP to which the station now connects or lastly connected
Name of AP	Name of AP to which the station now connects or lastly connected
AP IP Address	IP address of the AP connected by the station
AP MAC Address	MAC address of AP to which the station now connects or lastly connected
AP Mode	Mode of AP to which the station now connects or lastly connected
AP Operating Status	Currently operating status of AP to which the station now connects or lastly connected (Up/Down)
AP Map Location	The location of the AP to which the station now connects or lastly connected on RF map
Branch Local Authentication	Support of branch local authentication (Yes or No)
WLAN ID	WLAN ID
BSSID	WLAN service IP in a specific AP
QoS Allocation	QoS allocation

Security information

Item	Description
Authentication Mode	The method for authentication used when the station is connected
Encryption Algorithm	The method for encryption used when the station is connected
EAP Type	Type of EAP
ACL Application Status	Application of access control to station (Yes or No)
ACL Name	Name of the access control applied to the station
AAA ACL Application Status	Application of AAA ACL
AAA ACL Name	Name of the applied AAA ACL
Guest ACL Name	Name of the applied guest ACL
HTTP Redirect URL	HTTP redirect URL (guest service)
HTTP Redirect	HTTP redirect on
Radius Authentication Server IP Address	Radius authentication server IP address
Radius Accounting Server IP Address	Radius accounting server IP address

Traffic Usage

The station provides the information on the history of used traffic in a graph or table. The viewing period is set by clicking the period setting icon on the right bottom of the graph.

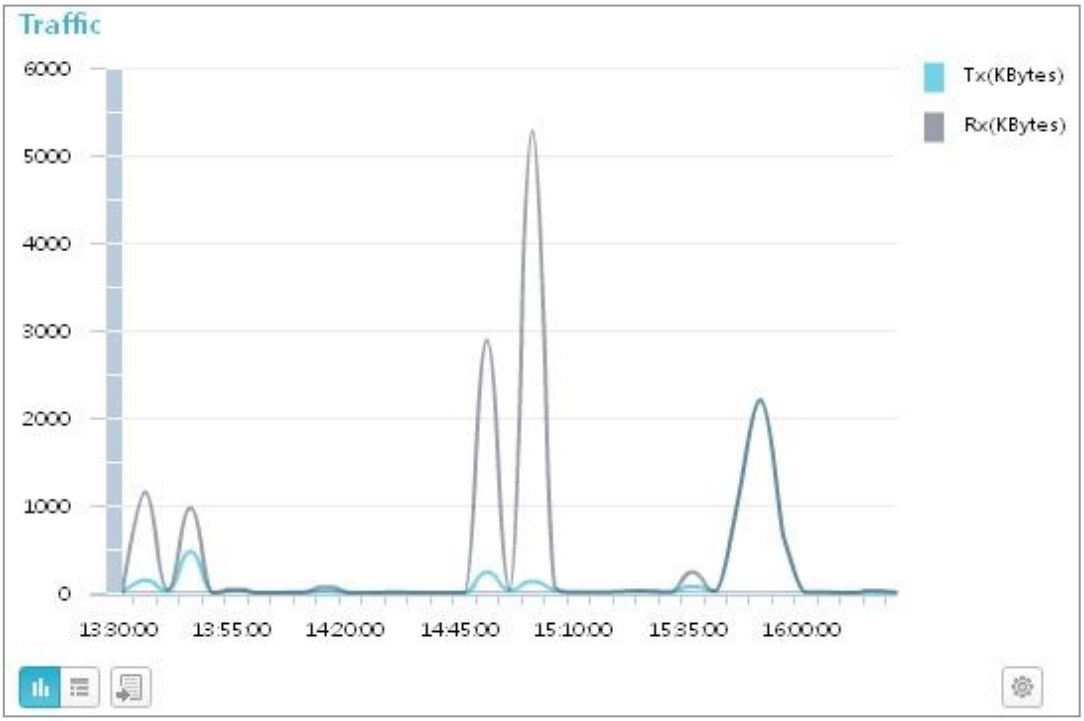


Figure 46. Station Traffic Usage

RSSI/SNR

The RSSI and SNR station history is shown in a graph and a table. The retrieval period is set by clicking on the period setup icon at the bottom right of the graph.

Figure 47. Stattion Traffic Usage and Station RSSI/SNR

History of Connection of Station

The function of viewing the history of the connection of the station is provided. You can click the period setting icon on the top of the screen on the list of connection history to set the period of viewing the connection history.

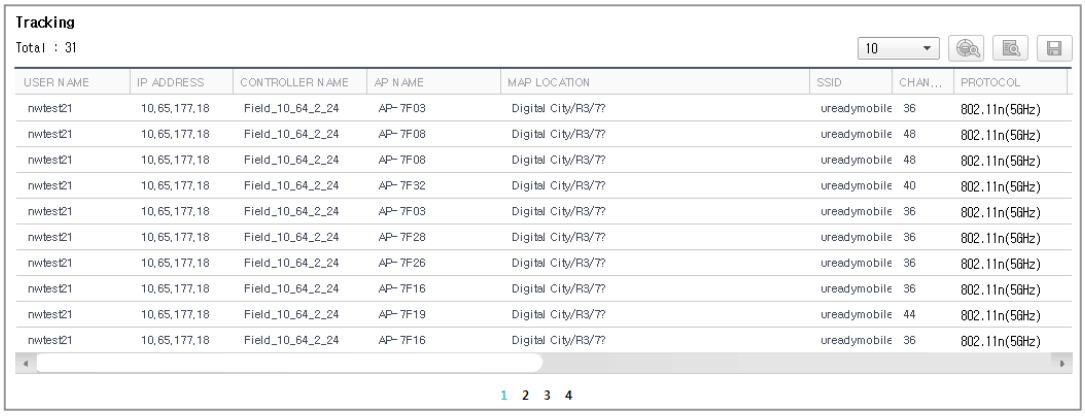


Figure 48. History of Connection of Station

Item	Description
User Name	Name of the station user
IP Address	Connected IP address used by the station
Controller Name	Name of the controller connected to the AP to which the station is connected
AP Name	Name of the AP to which the station was connected
Map Location	Location where the station was placed on the map
SSID	SSID with which the station was connected
Channel	Channel number used when the station was connected
Protocol	Connected protocol used when the station was connected (2.4 GHz, 5 GHz)
Connection Time	Time when the station was connected
Connection Ending Time	Time when the station released the connection
Term (sec.)	Time when the station is kept connected
Traffic (Byte)	Total traffic used during the time when the station is connected
Reason for Handover	Cause for the station performing handover
Authentication Time	Time when the station received authentication
IP Allocation Time	Time when the IP was allocated if the station was connected
RSSI (dBm)	RSSI value just before the station released the connection
SNR	SNR value just before the station ends the connection

Using Trouble Shooting

1) Select a station to which you want for troubleshooting in the list of stations and click the hyperlink on the troubleshooting column of the station.
2) Request the WEM to perform troubleshooting for the station.
3) The controller performs troubleshooting and delivers the result to the WEM.
4) Display the result of performing the troubleshooting in the WEM.

[Station Status]

Item	Description
Connection	The status on which the wireless terminal is connected to the AP (OK, NOK)
Authentication	The status on which the wireless terminal is authenticated to the AP (OK, NOK)
IP Allocation	IP allocation information for the wireless terminal to be connected with AP
PING	Check the communication with the wireless terminal (ping).

[AP Status]

Item	Description
Name of AP	Name of the AP to which the station is connected at the time that the station troubleshooting is performed
MAC Address	Radio MAC address of the AP to which the station is connected at the time that the station troubleshooting is performed
Radio Status	2.4 GHz or 5 GHz operating status AP operation status CAPWAP status (Run, Down, Idle)

[Station Event]

The history of events occurring in relation to the station is displayed. It is useful only when the controller turns on the station event notification option.

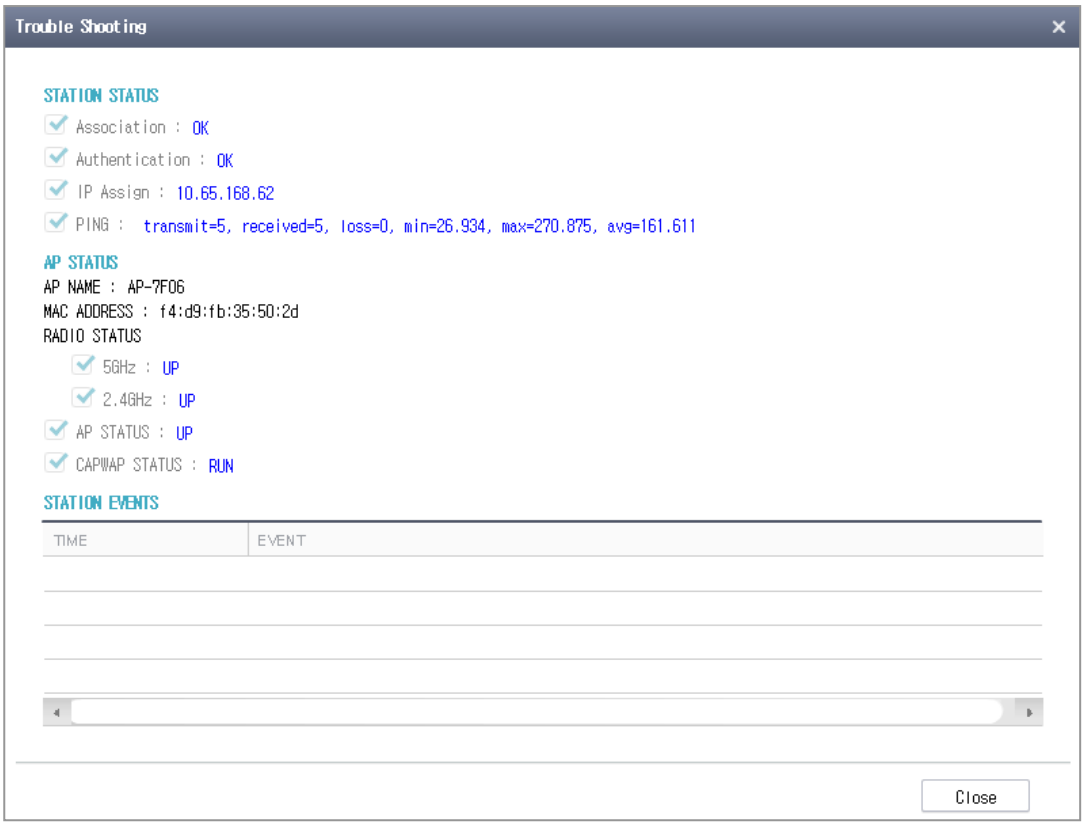


Figure 49. Station Troubleshooting

3.5 Report

WEM system allows user to generate statistics reports from the database.
The following reports can be gathered from WEM.

- Alarm
- Station
- Controller
- AP
- Security
- Network Quality
- Guest User

Output results will be saved in PDF (Portable Document Format) or CSV (Comma Separated Values) format.

The parameters for the statistics are as follows:

Parameter	Description
REPORT TITLE	Report title
REPORT TYPE	Report type
SCHEDULED	The schedule application condition
NEXT SCHEDULED RUN	The next statistics report fulfillment time
LAST RUN	The time when the statistical report is performed lastly
STATUS	The available condition
HISTORY	I output the career putting the statistical report into practice.
RUN NOW	I put the selected statistical report into practice and output to a screen in the form of PDF/CSV.

3.5.1 Alarm

Using the alarm information collected in the WEM, alarm-related statistical data are outputted in the form of a file.

Generating Alarm Statistics

1) Select the 'Monitoring' → 'Reports' → 'Alarms' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) Select a controller for which to generate a report.

6) Specify the alarm conditions-severity of alarms, events, replies, cleared, etc.-to include in the report.

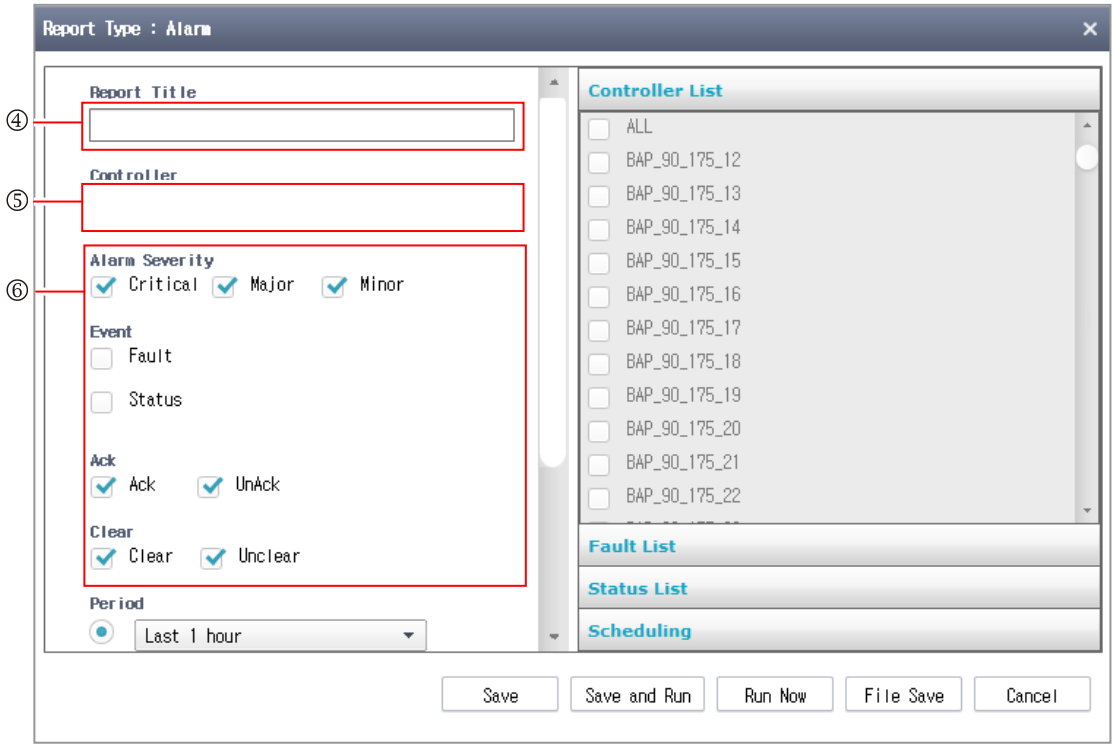


Figure 50. Speicify the Alarm Conditions

7) Specify an alarm period to include in the report.

8) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

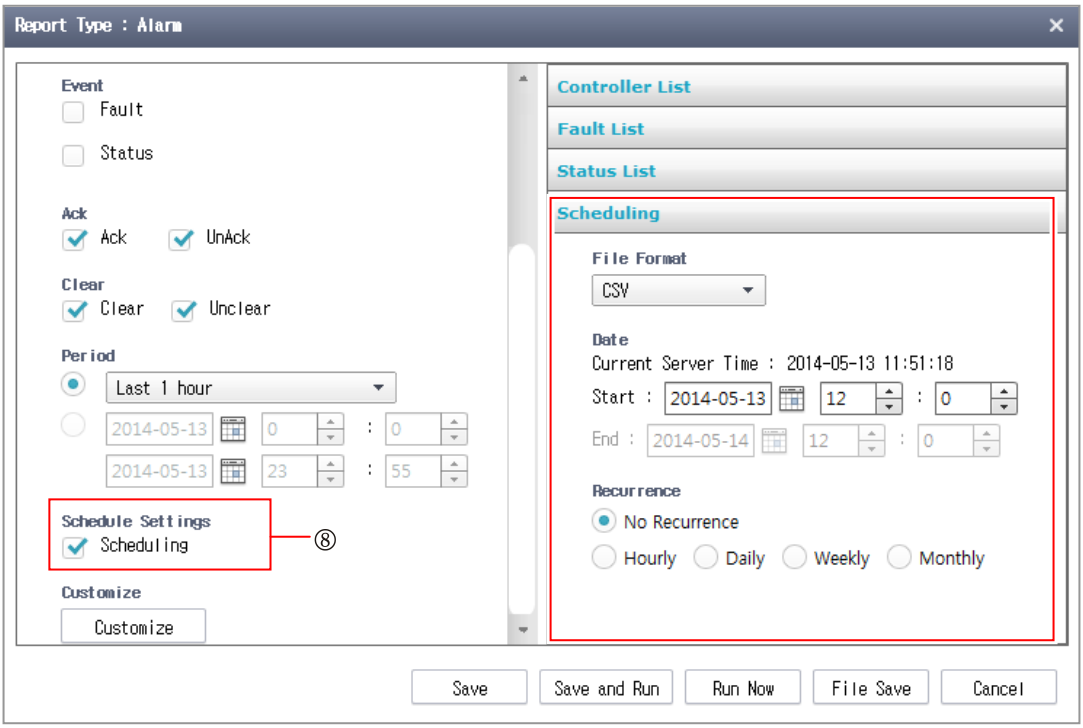


Figure 51. Specify the Report Schedule

9) Configure custom settings as required.

10) Select a Run option to start generating a report.

[Report Setting field]

Parameter	Description
Title	Report title
Controller	Target devices (controller)
Alarm Severity	Select this check box if you want to collect statistics (critical, major, minor)
Event Fault and Status	Select this check box if you want to collect statistics
Ack/Unack	Select this check box if you want to collect statistics
Clear/Unclear	Select this check box if you want to collect statistics
Period	Period Setting
Customize	Change of the output field.

[Schedule Setting field]

Parameter	Description
Scheduling	Scheduling tasks
File Format	Select the file format (CSV/PDF)
Start Date	Start Time
End Date	End Time
Recurrence	Generation interval

[Excute Setting field]

Parameter	Description
Save	Save the current configuration
Save and Run	Run statistics data collection and save data in CSV or PDF file format
Run Now	Run statistics data collection now
File Save	Save statistics data in CSV or PDF file format
Cancel	Cancel current configuration

3.5.2 Station

Using station-related information collected in the WEM, the statistical data of wireless devices are outputted in the forms of a file according to the period and conditions specified by the operator.

Generating Station Statistics

Follow the steps below to generate station-related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Stations' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) In the Type section, select a detailed report option.
   - Busiest Station: Generates a statistical report of the station with the most traffic according to the selected report setting option.
   - Station Counts: Generates a statistical report of station counts according to the selected report setting option.

- Station Traffic: Generates a statistical report of station traffic according to the selected report setting option.
- Station Sessions: Generates a statistical report of station session information according to the selected report setting option.
- Station Summary: Generates a station summary statistical report according to the selected report setting option.

6) In the Options section, select Controller or SSID.

7) In the Protocol section, select the protocols of stations to include in the report.

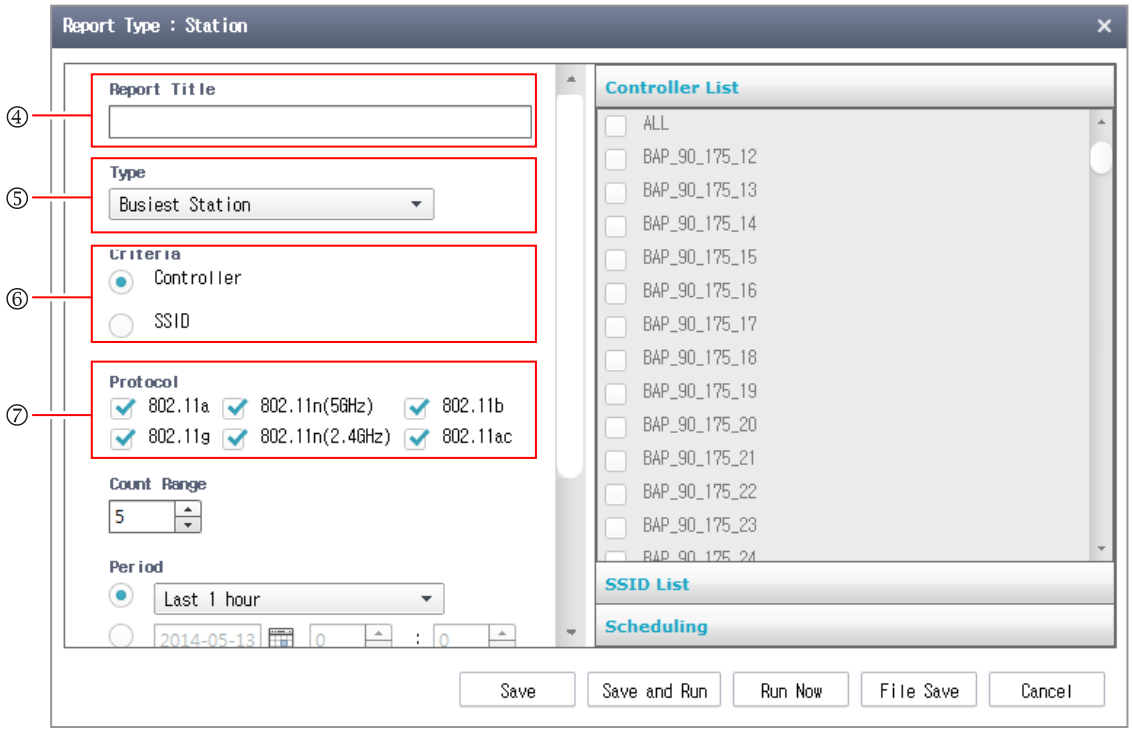


Figure 52. Generate the Station Report

8) In the Retrieval count section, specify the number of stations to retrieve.

9) In the Period section, specify a period to include in the report.

10) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

11) Configure custom settings as required.

12) Select a Run option to start generating a report.

[Report Setting field]

Parameter	Description
Title	Report title
Type	Report Type
Criteria	Controller/SSID
Protocol	IEEE 802.11a, IEEE 802.11n (5 GHz), IEEE 802.11b, IEEE 802.11g, IEEE 802.11n (2.4 GHz)
Retrieval Count	Specify a number of additional stations to retrieve (when Busiest Station is selected)
Period	Period Setting
Customize	Change of the output field.

3.5.3 Controller

Using controller-related information collected in the WEM, controller statistical data are outputted in the form of a file according to conditions specified by the operator.

Generating Controller Statistics

Follow the steps below to generate controller-related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Controller' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) In the Type section, select a detailed report option.
   - Controller Summary: Generates a controller summary statistical report according to the selected report setting option.
   - Controller Resource: Generates a statistical report of controller resources according to the selected report setting option.
   - Controller Interface: Generates a statistical report of controller interface according to the selected report setting option.

6) In the Options section, select a controller.

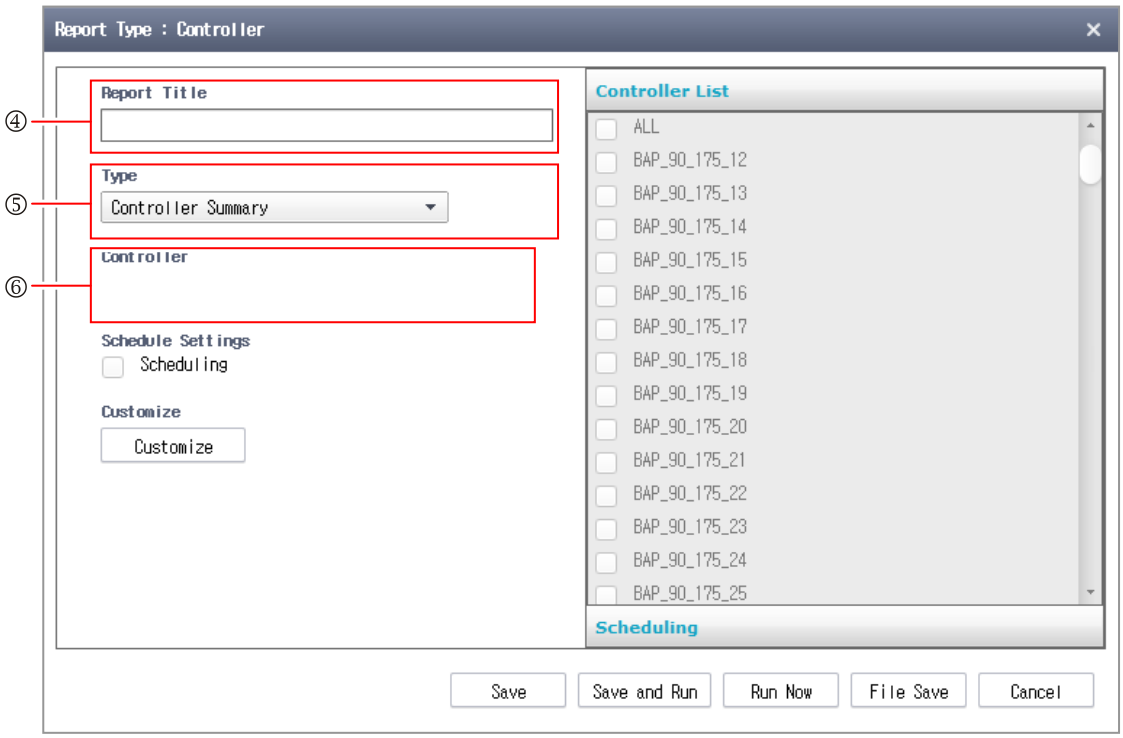


Figure 53. Generate the Controller Report

7) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

8) Configure custom settings as required.

9) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Type	Report type
Controller	Name of the specified controller
Schedule Setting	Enables scheduled generation of reports
Custom settings	Allows use of custom output fields in the report

3.5.4 AP

Using AP-related information collected in the WEM, AP statistical data are outputted in the form of a file according to conditions specified by the operator.

Generating AP Statistics

Follow the steps below to generate AP-related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'APs' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) In the Type section, select a detailed report option.
   - AP Summary: Generates an AP summary statistical report according to the selected report setting option.
   - AP Usage: Generates a statistical report of AP usage according to the selected report setting option.
   - Air Quality: Generates a statistical report of air quality according to the selected report setting option.
   - Channel Utilization: Generates a statistical report of AP channel utilization according to the selected report setting option.
   - AP Resource: Generates a statistical report of AP resource usage utilization according to the selected report setting option.
   - AP Interface: Generates a statistical report of AP interface performance according to the selected report setting option.
   - Busiest APs: Generates a statistical report of the APs with the most traffic according to the selected report setting option.
   - AP Uptime: Generates a statistical report of AP uptime according to the selected report setting option.

6) In the Options section, select Controller, SSID, or AP/radio.

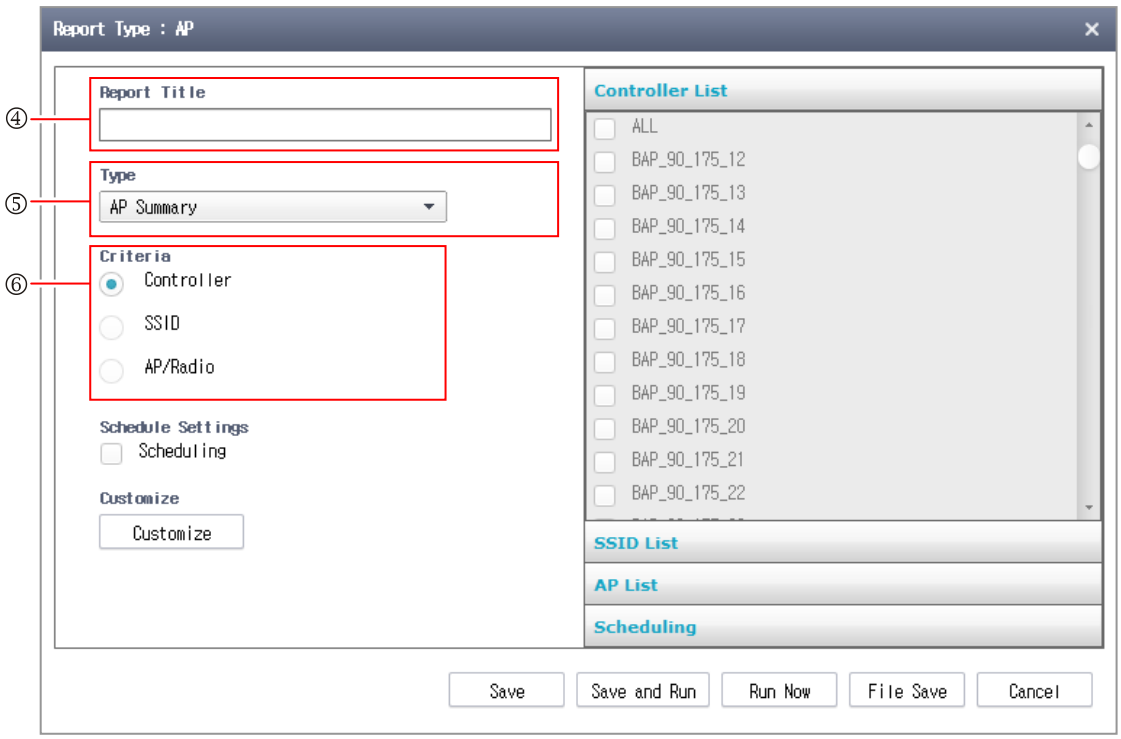


Figure 54. Generate AP Report

7) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

8) Configure custom settings as required.

9) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Type	Report type
Controller	Name of the specified controller, SSID or AP/radio
Retrieval Count	Specify a number of additional APs to retrieve (when Busiest APs is selected)
Period	Period for which to generate the report
Schedule Setting	Enables scheduled generation of reports
Custom settings	Allows use of custom output fields in the report

3.5.5 Security

Using rogue AP-related information and interferer-related information collected in the WEM, rogue AP statistical data and interferer statistical data are outputted in the form of a file according to conditions specified by the operator.

Generating Rogue AP Statistics

Follow the steps below to generate rogue AP-related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Security' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) In the Options section, select a controller.

6) Select 'Rogue APs' for Type.

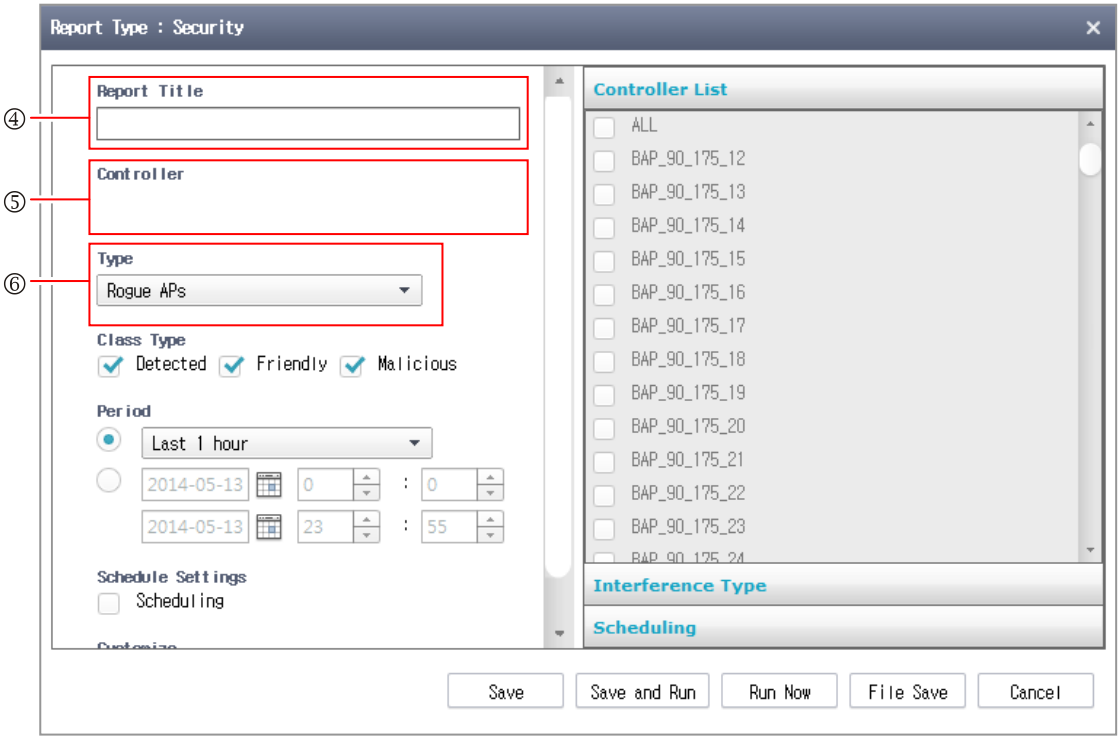


Figure 55. Generate Rogue AP Report

7) Select a Class Type.

8) In the Period section, specify a period to include in the report.

9) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

10) Configure custom settings as required.

11) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Controller	Name of the specified controller
Type	Type of report to generate (Rogue APs, Interferers)
Class Type	Type of rogue APs to include in the report - Unclassified - Non-malicious - Malicious
Period	Period for which to generate the report
Schedule Setting	Enables scheduled generation of reports
Custom settings	Allows use of custom output fields in the report

Generating Interferer Statistics

Follow the steps below to generate interferer-related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Security' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

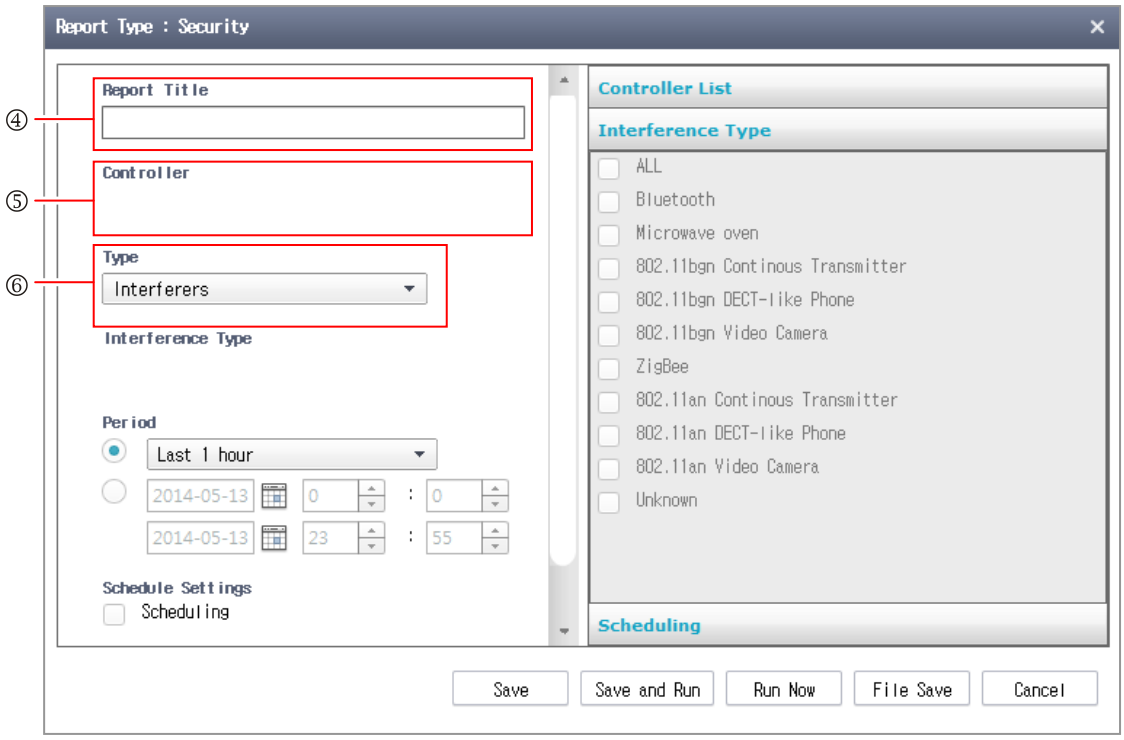


Figure 56. Generate Interferer Report

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

5) In the Options section, select a controller.

6) Select ‘Interferers’ for Type.

7) In the Options section, select an interferer type.

8) In the Period section, specify a period to include in the report.

9) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

10) Configure custom settings as required.

11) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Controller	Name of the specified controller
Type	Type of report to generate (Rogue APs, Interferers)
Interferer Type	Specifies a type of interferer
Period	Period for which to generate the report
Schedule Setting	Enables scheduled generation of reports
Custom settings	Allows use of custom output fields in the report

3.5.6 Network Quality

Using call-related information collected in the WEM, call statistical data are outputted in the form of a file according to conditions specified by the operator.

Generating Network Quality Statistics

Follow the steps below to generate network quality related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Network Quality' menu.

2) Click on Generate Report among the statistical menu items shown ( ).

3) The settings window appears, which allows you to add statistical items to include in the report.

4) Enter a title in the settings window.

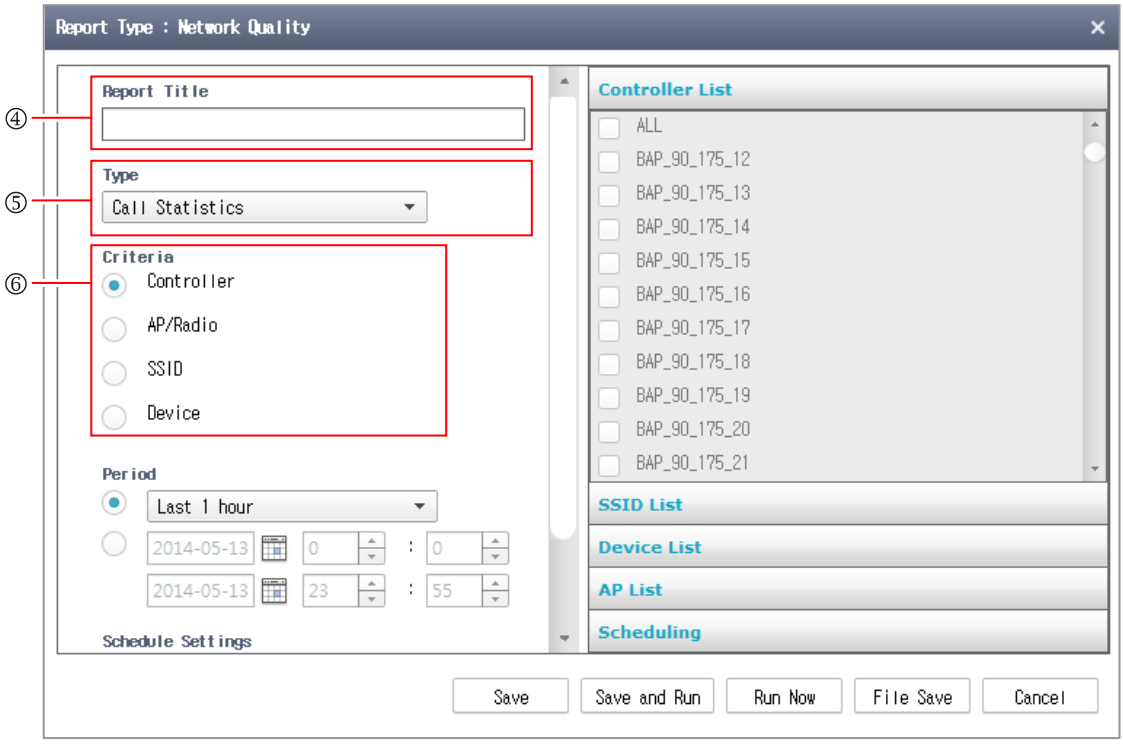


Figure 57. Generate Network Quality Report

5) Select a report type.
   - Call Statistic: Provides statistical data concerning call success rate, drop rate, etc.
   - Handover Latency: Provides statistical data concerning handover delay time
   - Handover Failure: Provides statistical data concerning handover failure
   - Association Latency: Provides statistical data concerning connection delay time
   - Association Failure: Provides statistical data concerning connection failure
   - Packet Loss: Provides statistical data concerning the packet loss rate

6) In the Options section, select Controller, AP/radio, SSID-a specific device type.

7) If selecting a specific device, the OS version of the device must also be selected.

8) In the Period section, specify a period to include in the report.

9) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.

10) Configure custom settings as required.

11) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Type	Specifies a type of report
Options	Generate statistics for the selected controller, AP/radio, SSID or device
OS Version	Specifies the OS version when a terminal has been selected and the statistics that are to be generated for a particular terminal
Period	Period for which to generate the report
Schedule Setting	Enables scheduled generation of reports
Custom Settings	Allows use of custom output fields in the report

3.5.7 Guest Users

Using guest user related information collected in the WEM, guest user statistical data are outputted in the form of a file according to conditions specified by the operator.

Generating Guest User Statistics

Follow the steps below to generate guest user related statistical data.

1) Select the 'Monitoring' → 'Reports' → 'Guest Users' menu.
2) Click on Generate Report among the statistical menu items shown ( ).
3) The settings window appears, which allows you to add statistical items to include in the report.
4) Enter a title in the settings window.
5) In the Options section, select a controller.
6) Select a report type.
   - Guest Summary
   - Guest Session
7) In the Period section, specify a period to include in the report.
8) If you want to use scheduled reporting, select Schedule setting and turn on the schedule.
9) Configure custom settings as required.
10) Select a Run option to start generating a report.

[Report Settings]

Item	Description
Title	Report title
Controller	Name of the specified controller
Type	Specifies a type of report

Item	Description
Period	Period for which to generate the report
Schedule Setting	Enables scheduled generation of reports
Custom Settings	Allows use of custom output fields in the report

3.5.8 Integrated Report

It reports the overview relating to the WEM, including the number of users, data usage, number of sessions, session time, present status by OS and device type, etc.

Creating Integrated Report

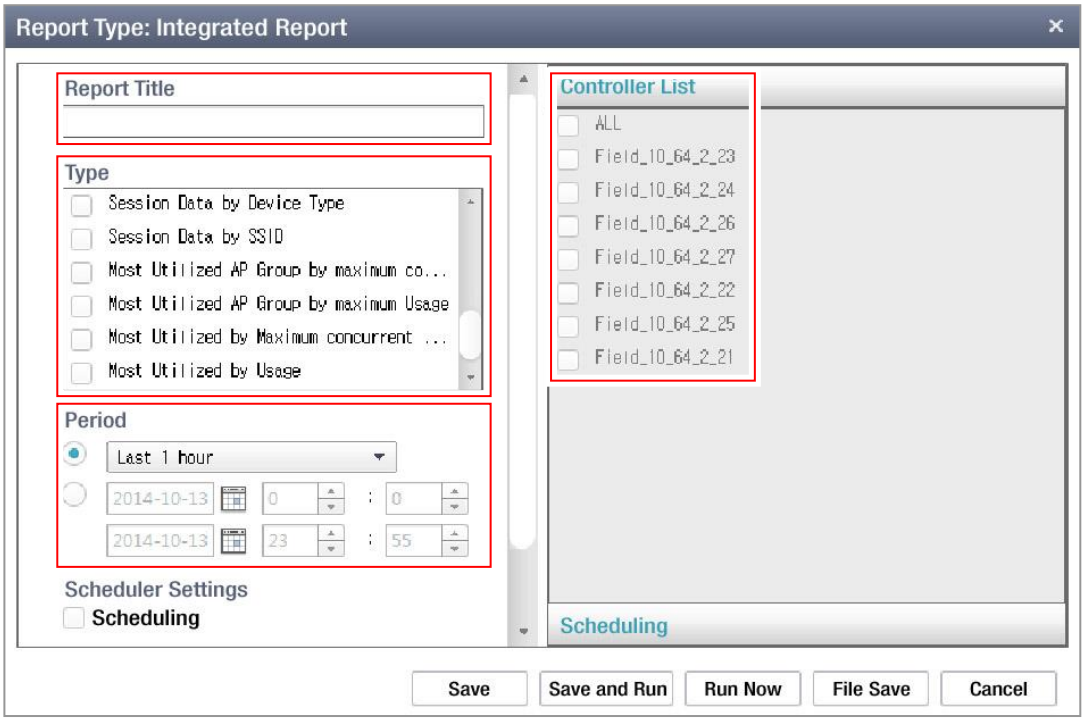
To create an integrated report, execute the following:

1) Select 'Monitoring' → 'Report' → 'Integrated Report' menu.

2) Click the Create Report ( ) in the statistical menu on the screen.

3) The setup window that may add statistical items appears.

4) Enter the title in the setup window.



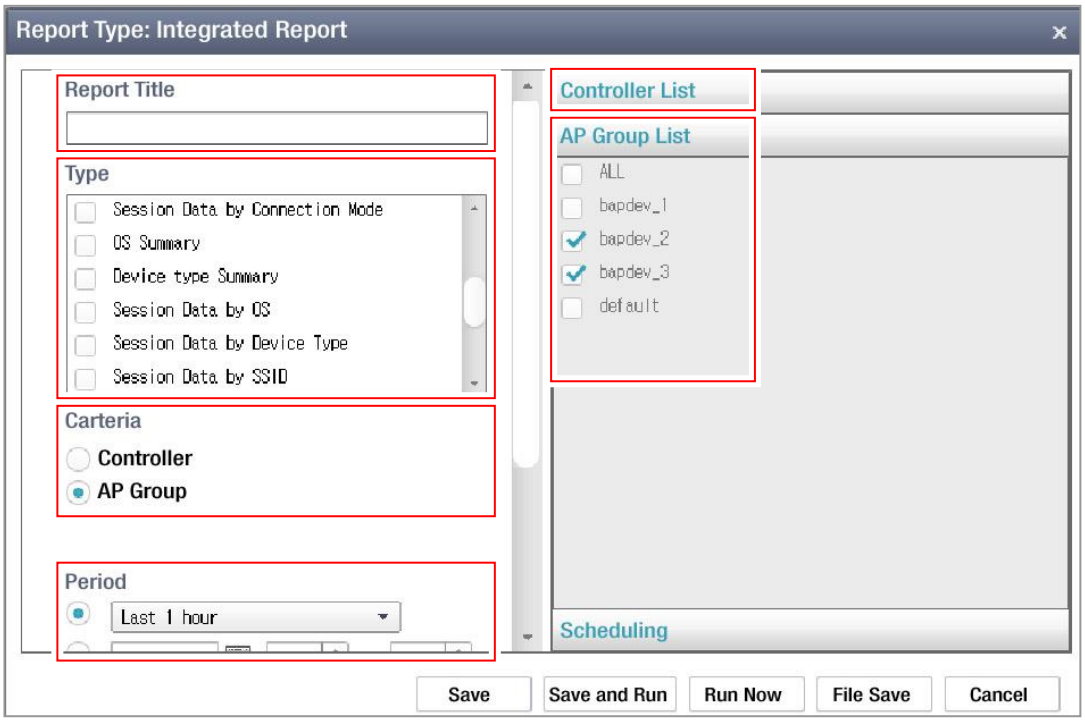


Figure 58. Creating Integrated Report

5) Select items to be included in the report.

- Client Count by SSID: Number of maximum concurrent users, average number of users, and graph of changes by time by SSID
- Client Usage by SSID: Maximum data usage and average data usage (at the interval of 5 min.), and graph of changes by time by SSID
- Client Count and Usage by AP Group: Number of maximum concurrent users, average number of users, maximum data usage, average data usage, and graph of changes by time by SSID of each AP group
- Client Session Summary: Information on total session count, client count and data usage
- Session Data by Connection Mode: Client count, data usage, total session time, and number of sessions by connection mode (radio)
- OS Summary: Number of users and data usage by OS
- Device Type Summary: Number of users by device type
- Session Data by OS: Number of users, data usage, total session time, and number of sessions by OS
- Session Data by Device Type: Number of users, data usage, total session time, and number of sessions by device type
- Session Data by SSID: Number of users, data usage, total session time, and number of sessions by SSID

- Most Utilized AP Group by Maximum Concurrent Count: Sorts based on the number of concurrent users in a unit of AP group. Displays the number of users and data usage.
- Most Utilized AP Group by Maximum Usage: Sorts based on data usage in a unit of AP group. Displays the number of users and data usage.
- Most Utilized by Maximum Concurrent Count: Sorts based on the number of concurrent users in a unit of AP. Displays the number of users and data usage.
- Most Utilized by Maximum Usage: Sorts based on data usage in a unit of AP. Displays the number of users and data usage.

6) Set the period to be included in the report in the period item.

7) If the reservation is required to be executed, select the schedule setting and set the schedule.

8) Select an APC or AP Group to be included in the report.

9) Selec the execution option and execute the report creation.

[Report Settings]

Item	Description
Title	Report title
Type	Selects items to be included in the report.
Carteria	Selects statistics for APC or AP Group
Period	Period for which a report is created
Controller List	Selects the APC to be included when a report is prepared.
Schedule Setting	Sets the report to operate fit for the reservation time.

3.6 RF Map

WEM provides a map overlay of operator entire network with real-time, visual network status indicators. Use the RF Map feature to place Wireless devices on a static map that are located in closed spaces such as buildings and offices. Use the built in map location tool to create a geographic view of your network and placement of your wireless devices and link status can quickly be determined to color coded icons.
User can plot current or historic information such as link SNR, traffic load and other metrics to evaluate network health and manage bottlenecks 'RF Map' view consists of the configuration view on the left, the right side of the tool bar and main view is classified.

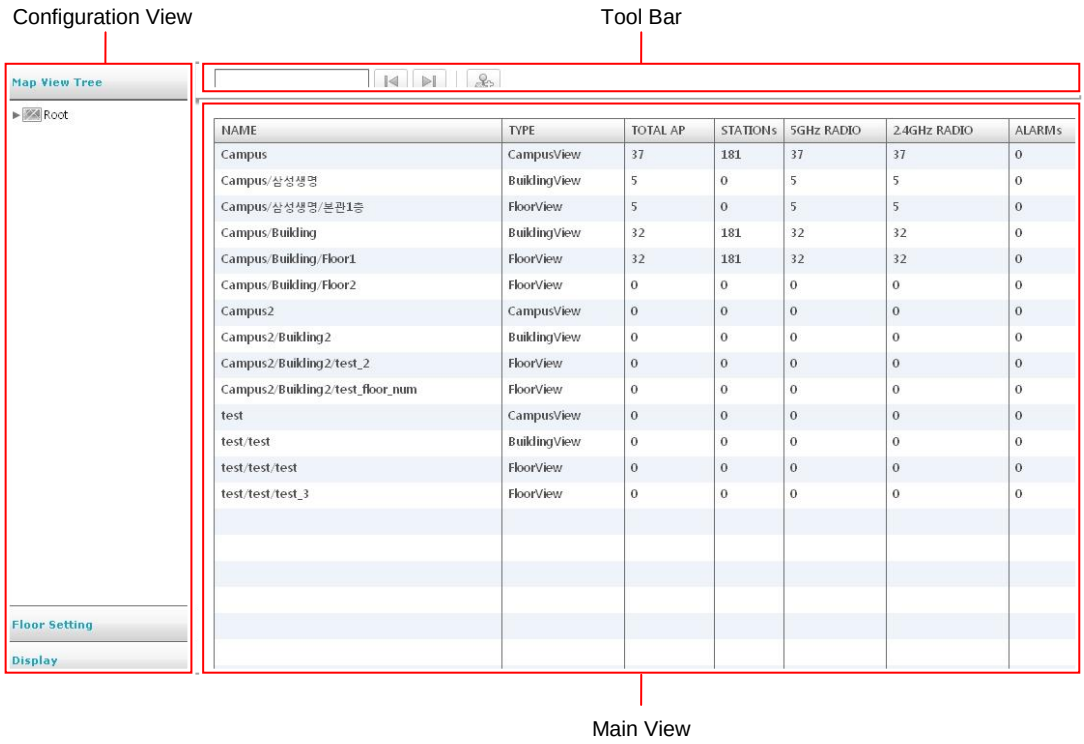


Figure 59. RF Map Window

Configuration View

The configuration view consists of 'Map Tree View', 'Floor Setting', and 'Display' menu.

- Map Tree View: It has Root View option which shows all the types of views in hierarchical structure. There are three types of Views i) Campus View ii) Building View iii) Floor View.
- Floor Setting: Consists of AP, AP Heat maps, Interferer, Station, Rogue AP & Rogue Station functions. Each option has different functions.
- Display: Consists of Name, MAC Address, IP Address, Tx Power, 'Channel', Channel Utilization, Air Quality Controller IP and Alarms options.

Tool Bar

Tool bar is used in accordance with the main view.

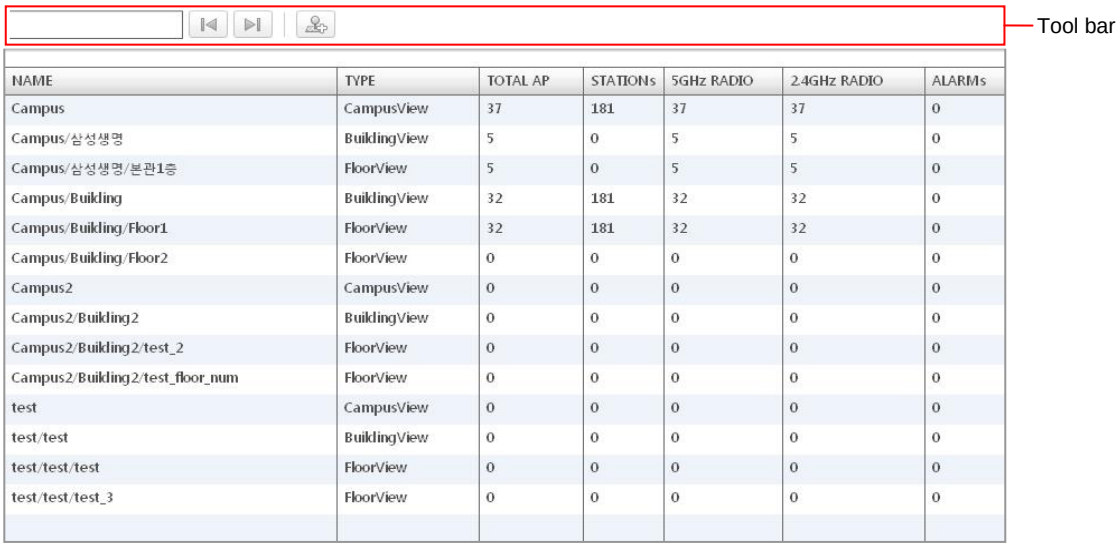
Main View

Main view window displays all the views in aligned manner, user can click on the each items in Map View Tree to get desired view.

> **NOTE**
>
> Order wise configuration to be followed, like Root → Campus view → Building view → floor view. In other words, user cannot create Campus or building from floor view.

3.6.1 Root View

The WEM provides to see all views type at a glance in the main window. All content comes under root option as a tree and links between each view. When user click root button, the system displays list of all view types with count of Total AP, Stations, Radio Types & Alarms information on each types.
A default output of the RF Map Layout is Root View.



NAME	TYPE	TOTAL AP	STATIONs	5GHz RADIO	2.4GHz RADIO	ALARMs
Campus	CampusView	37	181	37	37	0
Campus/삼성생명	BuildingView	5	0	5	5	0
Campus/삼성생명/본관1층	FloorView	5	0	5	5	0
Campus/Building	BuildingView	32	181	32	32	0
Campus/Building/Floor1	FloorView	32	181	32	32	0
Campus/Building/Floor2	FloorView	0	0	0	0	0
Campus2	CampusView	0	0	0	0	0
Campus2/Building2	BuildingView	0	0	0	0	0
Campus2/Building2/test_2	FloorView	0	0	0	0	0
Campus2/Building2/test_floor_num	FloorView	0	0	0	0	0
test	CampusView	0	0	0	0	0
test/test	BuildingView	0	0	0	0	0
test/test/test	FloorView	0	0	0	0	0
test/test/test_3	FloorView	0	0	0	0	0

Figure 60. Root View Window

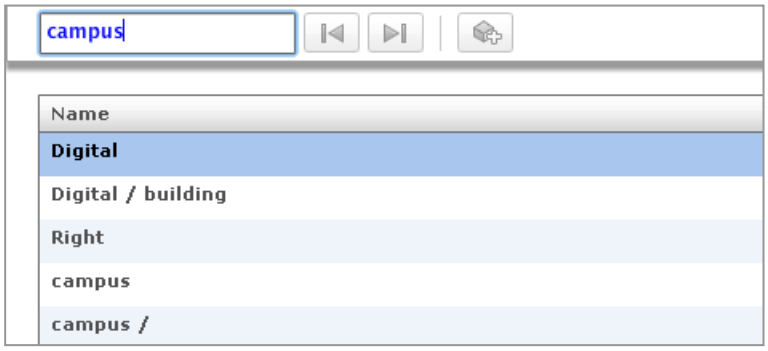
Root View provides the tool bar is as follows.

Button	Description
	Provides a search function.
	Add Campus

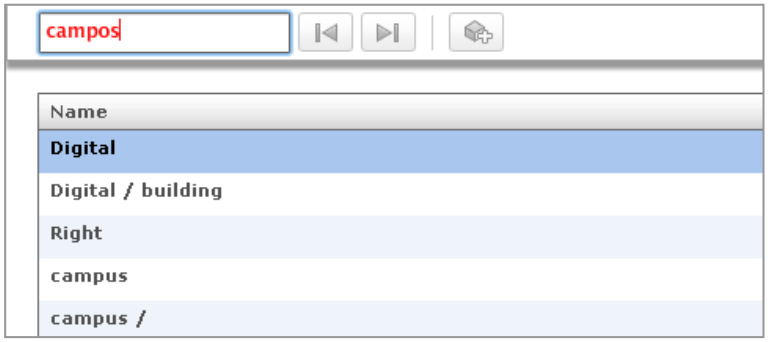
Searching

Search option allow user to search contents (name and view types) in the RF Map layout. Two buttons are available to support search contents to move forward and back [Previous' button ( ) and the 'Next' button ( )].When user type alphabet in the search field, the text color changes to RED or BLUE. Blue texts denote search item available in the list and Red texts denotes search item not available in the list.

[Blue: Search Item available in the list]



[Red: Search Item not available in the list]



The information provided in the main view is as follows:

Item	Description
Name	Name of campus, building and floor view
Category	Types of view - CampusView - BuildingView - FloorView
All APs	Number of APs existing in the view
Station	Number of stations existing in the view
5 GHz	Number of 5 GHz radio existing in the view
2.4 GHz	Number of 2.4 GHz radio existing in the view
Alarm	Number of active faults occurring in the view

3.6.2 Campus View

The ‘Campus View’ is the most basic step in the RF-MAP Viewer.
The screen output is as follows:

Figure 61. Campus View Window

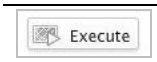
Add Campus

1) Select ‘Monitor’ → ‘RF Map’.
2) Click ‘Add Campus’ button ( ) in the main window.
3) Enter the campus name in the ‘Campus Name’ field, and enter a description in the ‘Description’ field, corresponding to campus.
4) Click OK button, A Pop up message displayed for successfully added Campus view.

> **NOTE**
> The screen must be manufactured in order of Root View → Campus View → Building View → Floor View. In short, while the campus or building view is not made, the floor cannot be immediately created.

> **NOTE**
> Move among all views is allowed only in the execution mode. While moving, you must check whether it is in the execution mode before clicking the required object button. In the edit mode, only the editing of the object is provided.

View from the campus to provide the tool bar, described as follows.

Button	Description
	Campus view of the screen zoom in and out
	Change mode ‘Execute/Modify’

‘Execute/Modify’ on the tool bar is a toggle button between two modes. When user click Modify button the following items appear on top of the window.

Button	Description
	Add building object
	Add background image/Change the background wallpaper of the current campus view
	Delete the currently visible screen of Campus view
	Save current output image screen
	Save all
	Refresh

To zoom in and out of campus view

Campus view screen supports zoom in and zoom out functions, which can be viewed by ‘%’ of unit. User can see ‘+’, ‘-’ button in the combo box and use the ‘%’ screen to zoom in and ‘%’ screen to zoom out Min % Zoom in is 50 % and Max % Zoom out is 400 %. (floor view supports the same features.)
When user saves Campus view screen in Zoom in or out mode, the result of saved image size will be normal as 100 % view.

Delete Campus

To delete the campus, all buildings registered on the screen must be deleted first. If you execute without deletion, a pop-up window of asking whether you will continue with the warning sentence that buildings exist now in the campus appears. At the time, if you select ‘OK’, the campus and buildings are all deleted.

1) Select ‘Monitor’ → ‘RF Map’.
2) Select Campus from Map View Tree on the left side of the screen.
3) Click the ‘Modify’ button, change the editing mode.
4) Click ‘Delete Campus’ button at the top of campus view.
5) Click ‘OK’ button to delete the campus object.

Create Building Object in Campus View

User has an option to add building in the campus. The building must be created as an object in the campus view.

1) Select ‘Monitor’ → ‘RF Map’.
2) Select a Campus view to create building object in the left side of the Map Tree View.
3) Click the ‘Modify’ button, to change the editing mode
4) Click ‘Add Building’ button ( ) at the top of campus view, the following window appears.
   Click the ‘Modify’ button, change the editing mode.
5) Enter Building Name in ‘Building Name’ Field, enter corresponding information in ‘Floors’ and ‘Basements’ fields.
6) Click ‘OK’ button to create building object.

After building object creation completed, user can see the building appears on the Campus View

Figure 62. Building on the campus view object is created the appearance

Modify building object

User can modify/delete the building object. Procedure is given below

1) Select ‘Monitor’ → ‘RF Map’.
2) On the left side of the ‘Map Tree View’, select the Campus view.
3) Select the building view object, which user want to delete from the campus view, press right click button on the building object.
4) A drop down menu appears.
5) Select ‘Change Information’ in the pop-up menu
6) The following modify window appears.
7) Enter the information to modify, click ‘OK’ button.

Delete Building Object

WEM system does not provide shortcut button to delete building object on the tool bar for prevent user to delete the building object mistakenly

1) Select 'Monitor' → 'RF Map'.
2) On the left side of the 'Map Tree View', select the Campus view.
3) Select the building view object, which user want to delete from the campus view, press right click button on the building object.
4) A drop down menu appears.
5) In the menu, select 'Delete Object'.
6) The following confirmation message window appears to confirm.
7) Click 'OK' button to delete the building object.

Add/Change Background Image in Campus View

User has an option to add/change background image for the campus view using shortcut button on the tool bar.

1) Select 'Monitor' → 'RF Map'.
2) Select Campus view from Map View Tree on the left side of the screen.
3) Click the 'Modify' button, change the editing mode.
4) Click 'Add Background Image' () button at the top of campus view.
5) As shown below, allowing you to select an image file in Windows.
6) When you click on the 'Open' button after you select an image file in local location, the background image is added/changed. Do not add/change a random image file, request user to change the proper background image data for WEM server to reflect in proper display.

Save Campus view screen

User can save the current output screen of the Campus view as an image.

1) Select 'Monitor' → 'RF Map'.
2) Select Campus view from Map View Tree on the left side of the screen.
3) Click the 'Modify' button, change the editing mode.
4) Click 'Save Image' () button at the top of campus view.
5) Specify the location and filename you want to save the image and click the 'Save' button. Click 'Save' button.

Screen image is saved as follows:

Figure 63. Current Window

Figure 64. Saved screen image

3.6.3 Building View

Building view is tied into one list to manage multiple floors (floor).
Therefore, when the first building view does not seem anything.

The tool bar provides from the building view are as follows:

Button	Description
	Add floor
	Show floor APs

Add a Floor

1) Select 'Monitor' → 'RF Map'.

2) Select building view to add floor object from Map View Tree on the left side of the screen.

3) Click 'Add Floor' () button at the top of campus view. The following window appears.

4) Enter each field, depending on the input parameters.

Parameter	Description
Floor Name	Floor name
Floors	Select the floor number which user want to add (Select Range: B2~6)
Description	Enter the current Description to create the floor from Building view.
Horizontal Span	Specifies the horizontal size of the actual corresponding layer. (Unit: cm)
Vertical Span	Specify the actual vertical size of the corresponding layer. (Unit: cm)

5) Click 'OK' button.

6) When the process is complete, go to view of the floor, as shown below, and double-click on the appropriate floor to register floor in the building view.

Figure 65. Floor View Resisted Window

Show AP on Floor Summary Window

User can identify the AP location on the Floor View instead of going in to each floor and waiting to load data, this probably saves time for user. If user wants to see full view & more AP information, then user can select on each floor and get the brief information.

1) Select Monitor → 'RF Map'.
2) Select Building view from Map View Tree on the left side screen
3) Click 'Show AP' ( )button at the top of building view.
4) AP position will be displayed on the floor image.

3.6.4 Floor View

Floor View shows the AP Location on the floor image, the output screen as shown below.

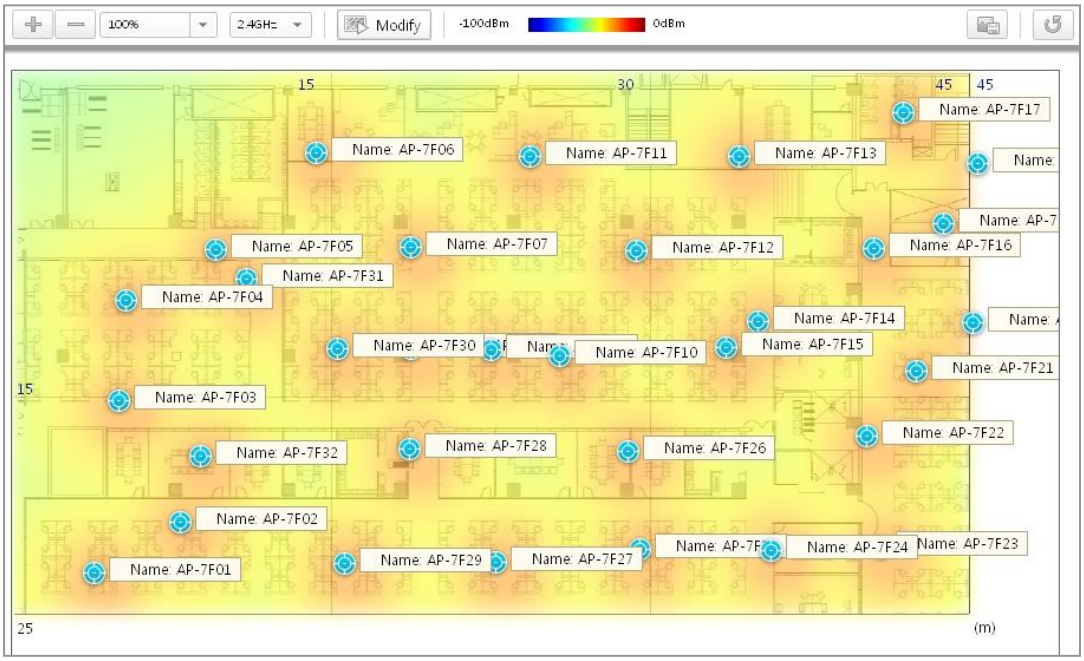


Figure 66. Floor View Window

The description of Tool bar are as follows:

Button	Description
100%	Floor View Zoom in and Zoom out
5GHz	Frequency bandwidth (2.4 GHz/5 GHz)
Modify Execute	Change mode ‘Execute/Modify’
-100dBm 0dBm	Signal Level Color reference
	Save current output image screen
	Refresh

‘Execute/Modify’ on the tool bar is a toggle button between two modes. When user click Modify button the following items appear on top of the window

Button	Description
	Modify Floor Information
	Add AP
	Add background image for current floor view

Button	Description
	Delete Floor
	The current screen is saved in a database server
	Planning mode
	Refresh

Floor View to Zoon In and Out

Floor view screen supports zoom in and zoom out functions, which can be viewed by '%' of unit. User can see '+', '-' button in the combo box and use the '%' screen to zoom in and '%' screen to zoom out. Min % Zoom in is 50 % and Max % Zoom out is 400 %.

Add AP

1) Select 'Monitor' → 'RF Map'.

2) Select Floor view from Map View Tree on the left side of the screen

3) Click the 'Modify' button, to change the editing mode.

4) Click 'Add AP' () button at the top of floor view. The window which is including the following information appears.

Item	Description
Select	Button for selecting an AP
AP Name	Name of the AP
MAC Address	MAC address of AP
IP Address	IP address of AP
AP Model	Model name of AP

5) Double-click the AP you want to register or select with the select button and click the 'OK' button.
The AP registered in the current floor view does not appear in the AP select screen. (APs cannot be registered at the same time in several floors.)

6) When AP registration is completed, the heat map area of the registered AP, AP object, and present status of station appear on the map.

Figure 67. AP Object completed registration

Item	Description
Heat Map	To display Signal Level in colors relative to the corresponding AP.
AP	Shows AP object. - Run Mode: When you select AP, it shows detail information of AP - Editing Mode: Support features such as drag-and-drop/delete of AP object
Station	Display the wireless terminals registered in the corresponding AP. Go to the Details screen when select the wireless terminal.

Deleting AP Object

WEM system does not provide shortcut button to delete AP object on the tool bar for prevent user to delete the object mistakenly Instead of that user may select the delete option in the drop down menu.

1) Select ‘Monitor’ → ‘RF Map’ menu.
2) Select Floor from Map View Tree on the left side of the screen.
3) Click the ‘Modify’ button, to change the editing mode.
4) Select the AP objects to delete from the Floor view, press right click button.
5) A Pop-up menu display. Select ‘Remove AP’ in the pop-up menu.
6) A pop up message window appears to confirm, Click ‘Ok’ button to delete AP object.
7) Click the ‘Save’ button to store the modification and click the Execute button to change the mode to the execution mode.

Retrieving AP Detailed Information

Display the detailed information for selected AP.

1) Select 'Monitor' → 'RF Map'.
2) Select floor view at the Map View Tree.
3) Select AP object at the Floor view, and right-click on it.
4) Select 'AP Detail Information' in the pop-up menu.
5) It goes to 'Monitor' → 'Devices' → 'System' → 'General' screen, it displays the detailed information.

Change Background image of Floor View

1) Select 'Monitor' → 'RF Map'.
2) Select floor at the Map View Tree.
3) Click the 'Modify' button, to change the editing mode.
4) Click 'Add Background Image' ( ) button at the top of floor view.
5) When you click on the 'Open' button after you select an image file in local location, the background image is changed. When the change on the background screen is requested, the image data will be reflected immediately to the server.
   Therefore, a person other than the operator shall not change the image file arbitrarily.

Deleting Floor

To delete the floor, all APs registered on the screen must be deleted first. If you execute without deletion, a pop-up window of asking whether you will continue with the warning sentence. At the time, if you select 'OK', the floors are all deleted.

1) Select 'Monitor' → 'RF Map'.
2) Select Floor view from Map View Tree on the left side of the screen.
3) Click the 'Modify' button, to change the editing mode.
4) Click on delete floor button on the tool bar. A warning message appears to confirm delete with AP objects
5) Click ok to delete

Floor View Screen Save

User can save the current output screen of the floor view as an image.

1) Select 'Monitor' → 'RF Map'.
2) Select Floor view from Map View Tree on the left side of the screen.
3) Click 'Save Image' ( ) button in the top of Floor view.
4) Specify the location and filename you want to save the image and click the 'Save' button.
5) Screen image saved does not take into the account of screen expanded/collapsed state of the saved screen image.

Setting Floor View

User can place objects and set parameters for AP on the floor view according to the needs, such as hide or show Floor Setting items and AP parameters.

- Floor Setting: AP, AP Heat Maps, Station, Interferer, Rogue AP & Rogue stations
- Display Parameter for AP: Name. Mac Address, IP Address, Tx Power, Channel, Channel Utilization, Air Quality, Controller IP and Alarms.

Display Parameter

User allows selecting display parameter items left side of the screen. If you choose the items, the information will display according to the parameters selected on the floor image.

Planning Mode

Planning Mode function helps user to predict signal coverage on different type of obstacles. You can place a virtual AP and select obstacle type to predict signal coverage in that.

Clicking ‘Planning Mode’ button in tool bar, the window is changed to the planning mode.

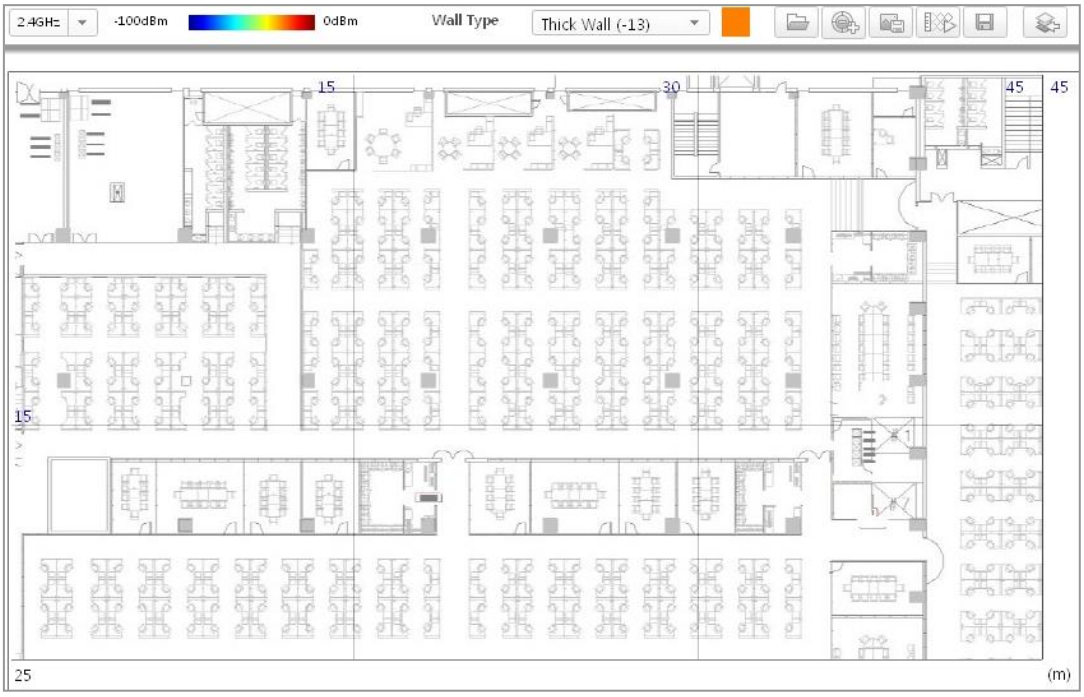
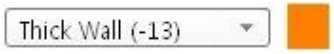
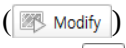


Figure 68. Planning Mode Window

The description of Tool bar are as follows:

Button	Description
	Wall Type - Thick Wall (-13) - Light Wall (-2) - Heavy Door (-15) - Light Door (-4) - Cubicle (-1) - Glass (-1.5)
	Load previous planning data
	Add Virtual AP
	The current screen is saved in database server
	Start planning
	Save planning data (AP, Wall location information)
	Go back to the floor view mode

1) Select ‘Monitor’ → ‘RF Map’ menu.
2) Select the floor in ‘Map View Tree’ at the left window.
3) Click the ‘Modify’ () button, to change the edit mode.
4) Click the ‘Planning Start ()’ button at the top of floor window

Add Virtual AP

1) Click ‘Add Virtual’ () button on tool bar to add virtual AP.
2) Click the left mouse button on Virtual AP to move AP location.
3) Right click on Virtual AP and Select ‘Setting’ in pop-up menu.
4) Enter the required fields, click ‘OK’ button.

Parameter	Description
Name	Virtual AP name
5 GHz Tx Power	Set the Tx Power of 5 GHz. (Unit: dBm)
2.4 GHz Tx Power	Set the Tx Power of 2.4 GHz. (Unit: dBm)

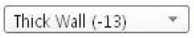
Remove Virtual AP

‘Remove Virtual AP’ provides in pop-up menu.

1) Select the Virtual AP to delete right-click on it.
2) Select the ‘Remove AP’ in the pop-up menu box.

Add Obstacle

To add obstacle, click the ‘Wall Type’ icon on the Tool bar at top of the planning window.

1) Select the Wall Type (

) in the drop down list and click on wall color to place obstacle in the floor image, to add obstacles.
2) Click right mouse button over the obstacles.
3) Select ‘Setting’ in the pop-up menu.
4) Enter required fields, click ‘OK’ button.

Parameter	Description
Width	Set the width of obstacles.
Height	Set the height of obstacles.
Angle	Set the angle of obstacles in MAP.

Remove Obstacle

‘Remove Obstacle’ provides in pop-up menu.

1) Select the obstacle to delete, Right click on it.
2) Select the ‘Remove Obstacle’ at the pop-up menu.

3.7 Dashboard

In addition to the reports available under Monitor, the WEM dashboard
Includes a dashboard view containing a number of dashboard reports by default.
You can also add dashboard reports to the WEM, providing custom report views you want to make available on your WEM dashboard. The following Wireless dashboard reports can be added.

Dashboard of the initial screen is organized as follows

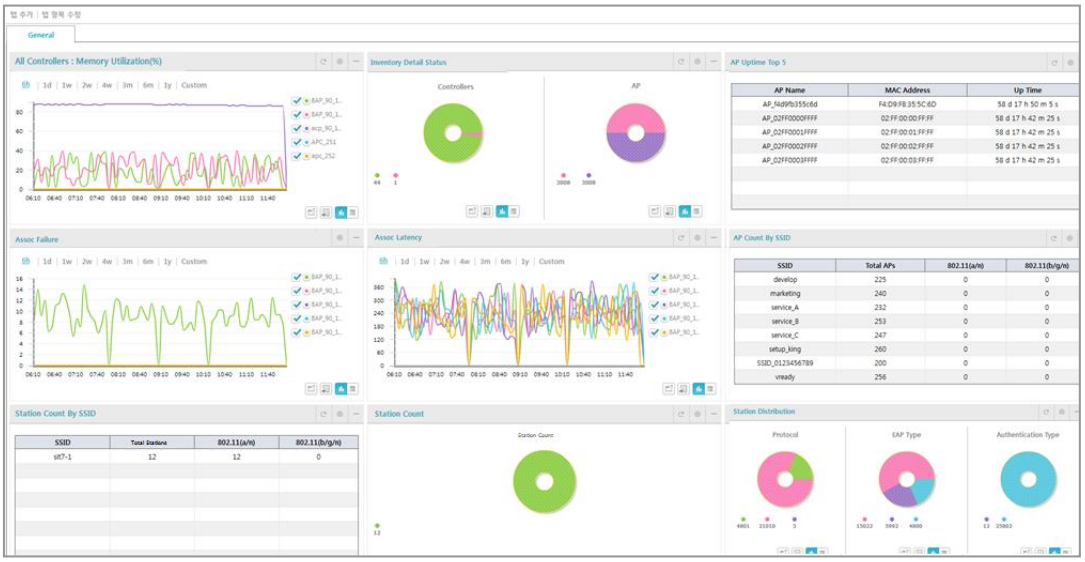


Figure 69. Dash Board Window

Dashboards provided by the content items are as follows.

Item	Description
AP Uptime Top 5	The oldest AP information, top 5.
All Controllers: CPU Utilization (%)	CPU usage of the controller
All Controllers: Memory Utilization (%)	Memory usage of the controller
Station Alarm Summary	The alarm summary that are generated in the Station
Station Count	The total number of wireless terminal
Station Distribution	Ratio of the entire wireless terminal 802.11an and 802.11bg.Displays Extensible Authentication Protocol (EAP) types at the same time.
Station Traffic Top 5	5 station information of which there are lots of traffic
Equipment Distribution	Information on the number of all APs, radios, station equipment managed in the WEM
Current Status of Equipment	Status information on controllers and APs managed by the WEM

Item	Description
Rogue AP Count	Rogue AP Count
Interferer Count	Interferer Count
Station Total Count	Station Total Count
Station Traffic	Traffic amount which occurs at the station.
AP Count By SSID	AP count by SSID
Station Count By SSID	Station count by SSID
Call Statistics	Information on the history of call number occurring by controller
Packet Loss	Information on the history of packet losses occurring by controller
Assoc Delay	Information on the history of station assoc delay statistics by controller
Assoc Failure Rate	Information on the history of station assoc failure rate by controller
Handover Delay	Information on the history of handover delay statistics by controller
Handover Failure Rate	Information on the history of handover failure rate by controller

Each content item screen are described as below:

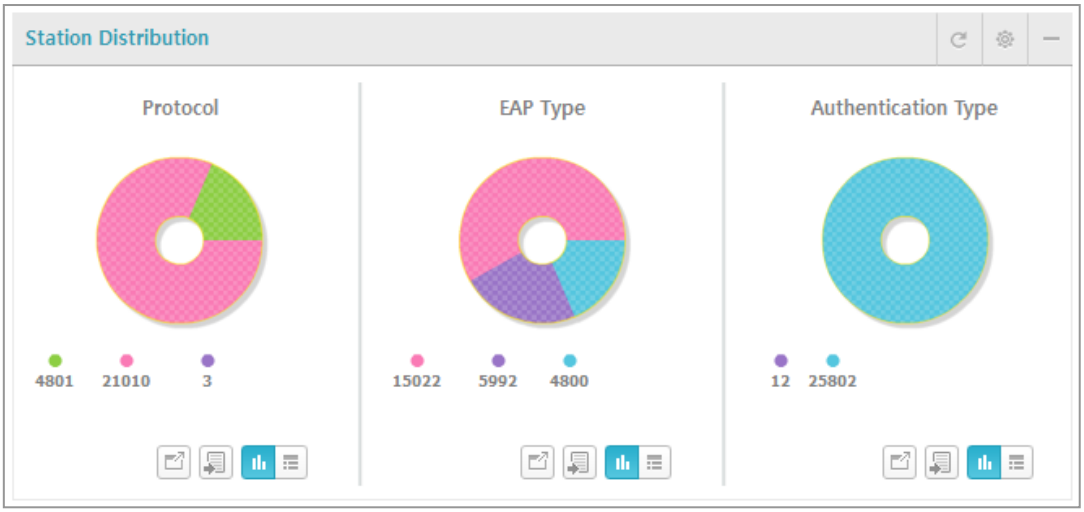


Figure 70. Contents Window

Button	Description
	Refresh button: Refresh the result
	Setting button: Set to perform functions of the content or the content of the refresh interval set

Button	Description
	Minimize button (-)/Maximize button (+): Content to minimize or maximize the output screen
	View Chart/View Table: Chart or table to switch the output screen
	Chart/Table Zoom out: Expanded to a full-screen chart or table output
	Data Output: Save the chart or table data displayed as CSV file.

When configuring single device Wireless dashboard reports, a single device must be selected.

Each dashboard report can be customized to fit your specific needs. From any dashboard report menu, click setting to open the configuration dialog.

Add Dashboard Tab

User can add items to monitor and manage in the dashboard window.

1) Select ‘Monitor’ → ‘Dashboard’.
2) Select ‘Add Tab’ menu at the top of the dashboard window.
3) Enter the tab name at the ‘Tab Name’ field.
4) ‘Select the contents you want to add in the Available Contents box, and then click the content where you want to move, using the ‘Left’ or ‘Right’ button.
5) Click the ‘Save’ button to save the setting.

Rename Dashboard Tab Name

1) Select ‘Monitor’ → ‘Dashboard’.
2) Dashboard window appears. Click the right mouse button at the top of the dashboard window, a pop-up menu appears on the screen.
3) Select the ‘rename tab’ item on the pop-up menu.
4) Enter the name to be changed in the ‘Tab Name’ item.
5) Clicking ‘Save’ button, save the settings.

Deleting Dashboard Tab

1) Select ‘Monitor’ → ‘Dashboard’ menu.
2) Dashboard window appears. Select the tap button and right click on it, a pop-up menu appears on the screen. (Or, select the delete icon on the tab.)
3) Select the ‘delete tab’ item on the pop-up menu. The confirmation window appears.
4) Click ‘Yes’ button to delete the selected tab.

Editing Content of the Dashboard Tab

user can modify the item existing configuration.

1) Select ‘Monitor’ → ‘Dashboard’ menu.
2) The dashboard window appears. Select ‘Edit Contents’ in the upper-left corner of the dashboard window.
3) Select the name of the tab you want to modify from the ‘Tab Name’.
4) To add an item, click the desired item from the ‘Available Contents’ after using the ‘Left’ or ‘Right’ button and specify the location where you want to add. To delete the existing item, select the item you want to delete in the ‘Left Contents’, and ‘Right Contents’ and then click on the ‘Remove’ button.
5) Click ‘Save’ button to save the settings.

3.8 Topology

'Topology' menu in WEM system belonging to the AP Controller device. it shows device information of APC also shows overview alarm status of the device. WEM allows user to arrange APC device in a graphical view in the main window.
In addition, user can retrieve APC information (Device Name, Type and IP)

To open Topology view Select 'Monitor' → 'Topology'.

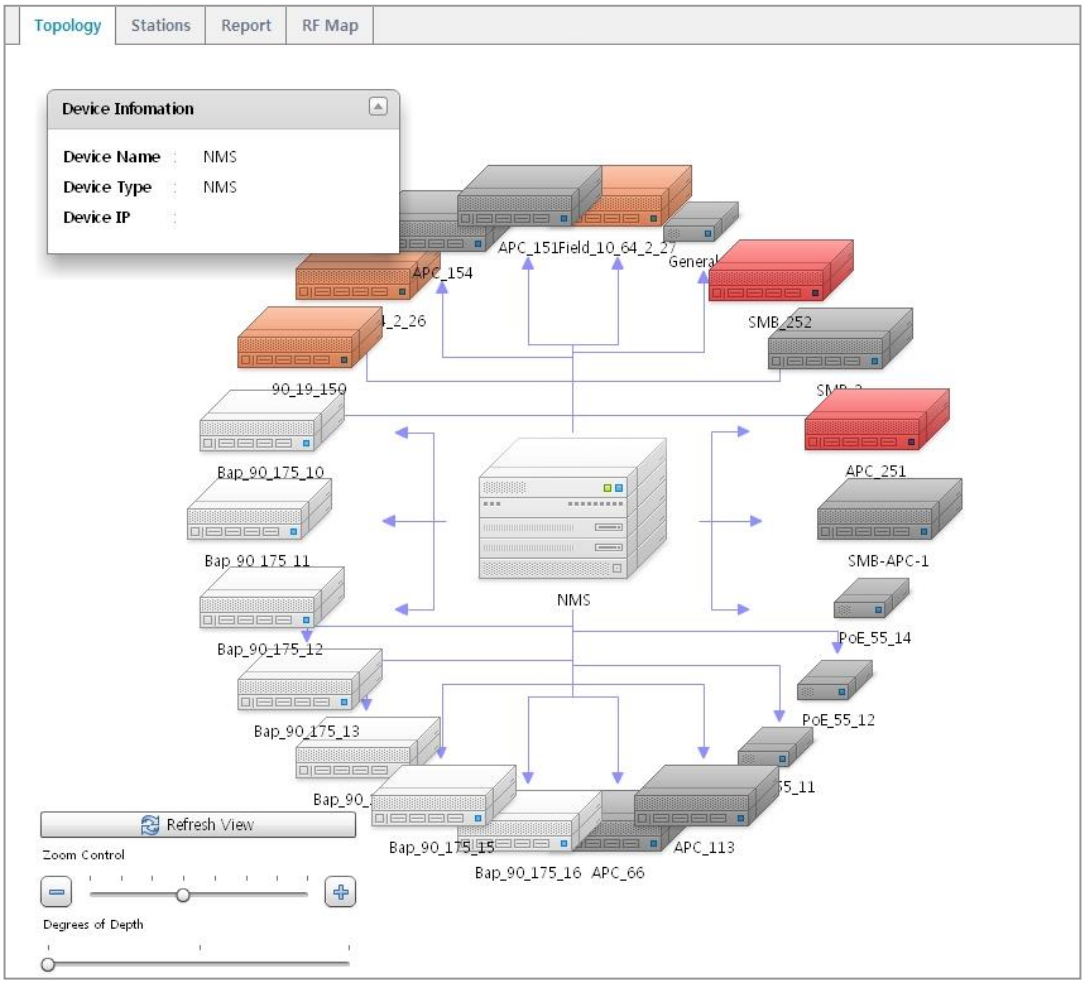


Figure 71. Topology Window

Icons

Topology view of main frame displays network elements types and an alarm status. Each network element with the following icon is displayed, the operator can see the color of the current alarm status.

Category	Normal (White)	Disable	Critical (Red)	Major (Orange)	Minor (Yellow)
Controller					
AP					
WEM					

Viewing Device Information

When you click the icon of the device displayed on the screen by using the mouse, the information on ‘Device Name’, ‘Device Type’ and ‘Device IP’ is displayed in the Device Information window on the right top of the screen.

Refreshing Screen

To refresh the information on the screen, click the Refresh View icon on the left bottom.

Zoom Control

To zoom in and out the screen, the ‘Zoom Control’ menu can be used. When you click the ‘-’ button, the screen becomes zoomed in and when you click the ‘+’ button, the screen becomes zoomed out.

Degrees of Depth

This is a function of deciding at how many steps the equipment could be displayed far from the currently selected equipment. When the depth is set to be the lowest, only the equipment directly connected with the currently selected equipment is displayed on the screen and when the depth increases at one more step, not only the equipment directly connected but also equipment connected through one equipment is displayed on the screen.


NOTE

Topology view is displayed WEM startup screen.

3.9 Security

3.9.1 Interferer

'Interferer' menu provides to view and set interference object for APC.

The parameters of the interferer are as follows:

Parameter	Description
AP NAME	AP name detecting interferer
MAC ADDRESS	AP MAC address detecting interferer
TIME	Detecting time
INTERFERER TYPE	Interferer Type - Bluetooth: Bluetooth interface device - Microwave oven: microwave - Continuous Transmitter: The same frequency generating device - Cordless Phone: Wireless telephone - Video Camera: Video camera - Zigbee: Zigbee interface device
RSSI (Received Signal Strength Indicator)	Received signal strength
MIN FREQUENCY	Minimum frequency
MAX FREQUENCY	Maximum frequency
Name of Controller	Name of the controller to which the AP detecting interference is connected
Name of Detected AP	Name of the AP detecting the interference source. Possible to move immediately to the AP information by using the hyperlink.
Map Location	Hyperlink that can immediately move to the location screen on the map of the interference source

Options are different

Below is the procedure to detect interference.

1) Select 'Monitor' → 'Security' → 'Interferer' menu.
2) Select the search device (Controller, Controller Group or WEM) on the Tree Viewer. Displays the selected device at the 'Target Node' field.
3) Select the interferer type at the 'INTERFERER TYPE' field.
4) Select the search period at 'RUN INTERVAL' field.
5) Clicking '**Run**' button, the result displays. Clicking '**Stop**' to stop interferer.

3.9.2 Rogue AP

The controller detects unauthorized APs and wireless terminals, and creates related alarms and logs.
WEM provides to view rogue APs information using the search conditions.

The detected Rogue APs are classified as follows

Type	Description
Detected AP	An unknown AP that does not match the user-defined friendly or malicious rules.
Friendly AP	AP that is allowed to be used by an administrator among the detected unauthorized APs - Configures the friendly AP classification policy. - An administrator can classify a specific AP as a friendly AP manually among the detected unauthorized APs.
Malicious AP	AP that is not allowed to be used by an administrator among the detected unauthorized APs and AP that can be used maliciously - Configures the malicious AP classification policy. - An administrator can classify a specific AP as a malicious AP manually among the detected unauthorized APs.

The parameters for the Rogue AP are as follows:

Parameter	Description
MAC ADDRESS	MAC address
TIME	Detecting time
CLASS TYPE	Rogue AP type (Friendly/Malicious/Unclassified)
SSID	SSID information
RAIDO	Wireless bandwidth (802.11an/802.11bgn)
CHANNEL	Channel
EVENT TYPE	Event type (Rogue AP/Illegal Channel)
CONTROLLER NAME	Controller which detected the rogue AP
DETECTED AP NAME	Name of the detected rogue AP
MAP LOCATION	Hyperlink of the rogue AP’s map location

Detecting Rogue AP

Below in the procedure to detect the unauthorized AP.

1) Select 'Monitor' → 'Security' → 'Rogue AP'.
2) Set the search conditions.
   - At the 'CONTROLLER' field, select the controller.
   - At the 'EVENT TYPE' field, select the event type.
   - At the 'CLASS TYPE' field, select the unauthorized/friendly/malicious AP type.
   - At the 'RADIO' field, select the radio property.
   - At the 'PERIOD' field, select the search period.
3) Click '**Search**' button.
4) The Rogue AP list is displayed in the result table.

3.9.3 Access Control List (ACL)

The access control function provides the function of viewing the information on the station that is limited to access from the controller system through the condition search.
Access Control List (ACL) information can be retrived from this section.

The access control function is classified depending on the classification policy as follows:

Classification Type	Description
ACL	A station limited by the ACL among the stations limited to access
Prevented by APC	A station prevented by APC
Prevented by AP	A station prevented by AP

The parameters for the access control are as follows:

Item	Description
LOCATION	Location where the access is denied
PREVENTED STATION	MAC address of the wireless terminal has been denied access to the network
TIME	Time when the access is denied
CAUSE	Reason why the access is denied

Retrieving Access Control List

1) Select 'Monitor' → 'Security' → 'ACL'.
2) Set the search conditions.
   - At the 'CONTROLLER' field, select the controller.
   - Select the access control type (ACL/Prevented Client) at the 'EVENT TYPE' items.
   - Select the search period in the 'PERIOD' items.
3) Click '**Search**' button.
4) The access control list will be displayed in the result table.

3.10 Remote Resource Management (RRM)

The radio resource management menu provides the screen where the radio resource management statistics information provided by the remote resource management (RRM) of the system can be viewed.

The parameters for the RRM are as follows:

[RADIO RESOURCE MANAGEMENT]

Item	Description
Statistics	Statistics (AP's at Maximum Power (a/n, b/g/n)
Value	RRM ratio
Statistics	Total channel change count/Total Tx Power change count
Last 24 Hours	Last 24 Hours statistics
Last 7 Days	Last 7 Days statistics

[TX POWER CHANGE]

Item	Description
CHANGE REASON	Change reason. (Coverage Hole Detected/Coverage Hole Recovery/ Neighbor RSSI/No Neighbor AP/User Change/Other)
802.11 (a/n)	Tx power changing count of Change Reason for 802.11 (a/n) protocol.
802.11 (b/g/n)	Tx power changing count of Change Reason for 802.11 (b/g/n) protocol.

[CHANNEL CHANGE]

Item	Description
CHANGE REASON	Change reason. (Channel Allocation/Channel Invalid/Duty Cycle/ Channel Utilization/Radar Detected/User Change/Other)
802.11 (a/n)	Channel changing count of Change Reason for 802.11 (a/n) protocol.
802.11 (b/g/n)	Channel changing count of Change Reason for 802.11 (b/g/n) protocol.

Retrieving RRM

1) Select 'Monitor' → 'RRM'.
2) RRM 'Tx power change' and 'channel change' is shown in the 'Last 24 Hours' and 'Last 7 Days' after a while.
3) You can select and see the graph indication one among the 'Last 24 Hours' or 'the Last 7 Days'.
4) User able to see statistics in table or graph format by clicking Table/Graph icon.

3.11 WIPS

The WIPS as wireless IPS is operated as a separate server. The WEM can register WIPS servers separately operated and receive events from such servers. All events are related to IPS and the statistics of the events can be briefly checked. The whole screen of the WIPS menu is as shown below.

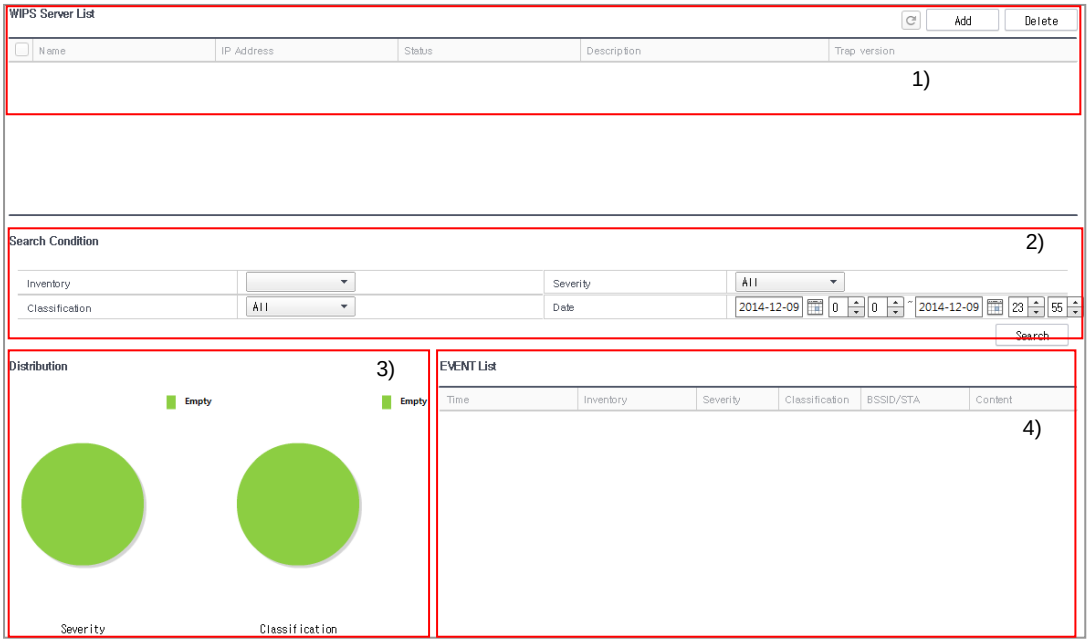


Figure 72. WIPS Screen

1) WIPS Server List: A list of WIPS servers registered in the WEM
2) Search Conditions: Event search conditions
3) Distribution: Event distribution (by significance and by category)
4) Event List

3.11.1 Registering WIPS Server

To receive an IPS event from the WIPS, WIPS servers to interoperate with the WEM must be registered and the WEM must be registered even to the WIPS to interoperate with. The WIPS can register only one WEM, and two or more WIPS servers can be registered in the WEM. Registration can be completed by configuring SNMPv3 TRAP between the WEM and the WIPS. If you want to delete servers in the WIPS server list, select the servers and then press the 'Delete' button.

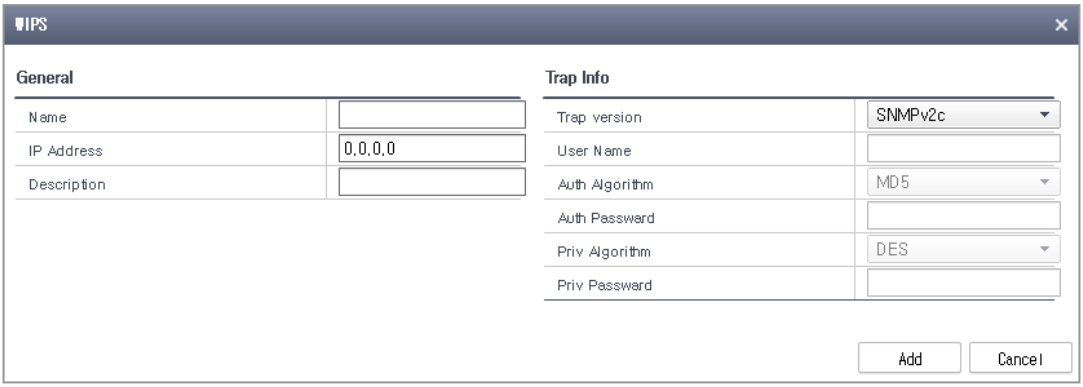


Figure 73. WIPS Server Addition

The items to enter upon registration are as follows:

Item	Description
Name	As the name of a WIPS server, a value to be distinguished by the operator
IP address	IP address of the WIPS server. Because a TRAP message is filtered based on the address, if two IP addresses are used for redundancy in the WIPS, it is necessary to check the IP address to be received by the WEM.
Description	As the explanation of a WIPS server, a value to be distinguished by the operator
Trap Version	SNMP version to be used by a TRAP message
User Name	As the name to be used upon the authentication of the TRAP message, it must be matched with the value set in the WIPS server.
Authentication Algorithm	As the authentication algorithm to be used upon the authentication of the TRAP message, it must be matched with the value set in the WIPS server.
The authentication password	As the authentication password to be used upon the authentication of the TRAP message, it must be matched with the value set in the WIPS server.
Individual Algorithm	As the algorithm to be used to encrypt the TRAP message, it must be matched with the value set in the WIPS server.

Item	Description
Development Password	As the password to be used to encrypt the TRAP message, it must be matched with the value set in the WIPS server.

3.11.2 Searching WIPS Event

You can search an event received from the WIPS in the WEM and check the statistical result.

The condition items for search are as follows:

Item	Description
Equipment	Possible to select one of registered WIPS server list or all WIPS servers.
Significance	Possible to select one of Critical, Major, and Minor events to search or search all severities.
Category	Possible to select one by event category and search all categories. The types of categories are as follows: - System - Unauthorized APs - Flooding attack - Terminal management - Peer-to-Peer - Man in the Middle - Air Attack Tool - MAC Spoofing - RF interference source
Date	Selects a time section to retrieve.

A pie chart which shows distribution is as follows:

Item	Description
Significance	Displays event distribution (%) depending on significance.
Category	Displays event distribution (%) depending on category.

The list of events shows following items:

Item	Description
Time	Event occurring time
Name of Equipment	Name of the equipment where an event occurs
Significance	Event significance (Critical, Major, Minor)
Category	Event category (same as the category of the event search conditions)

Item	Description
BSSID/STA	MAC address of a device which generates an event
Description	Event description

3.12 DPI

The DPI, as the abbreviation of deep packet inspection, shows the analysis of the application layer level of the data traffic. The DPI consists of five sub-menus: Summary, Wlans, Devices, Users, and Applications.

3.12.1 Summary

The Summary menu shows the present status of overall data traffic in center of the applications.
Below is the summary screen.

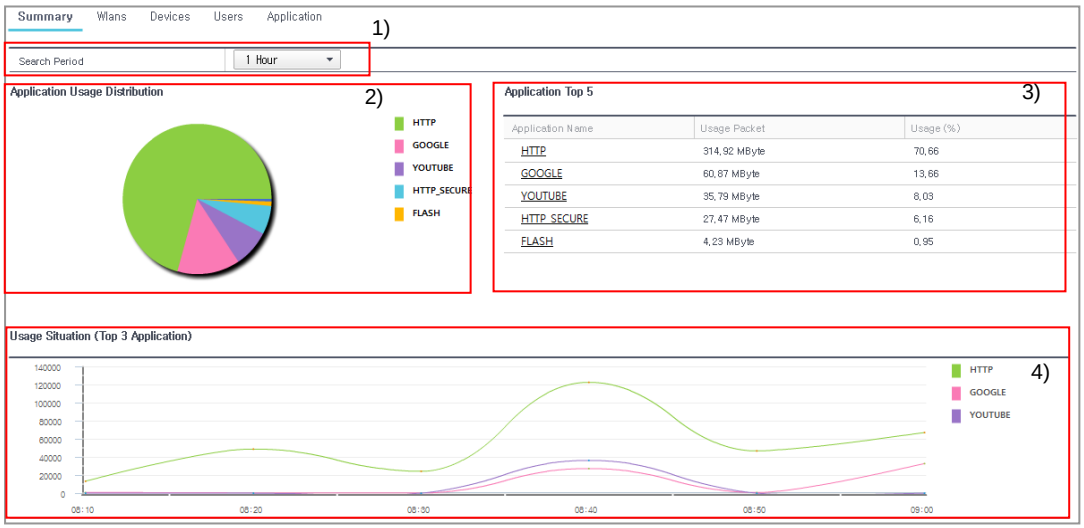


Figure 74. DPI-Summary1

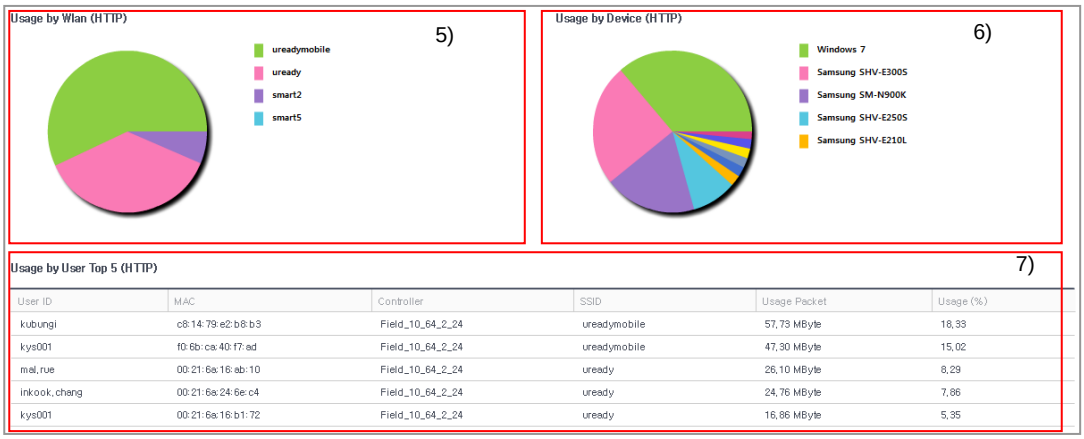


Figure 75. DPI-Summary2

Explanation on each number of the summary screen is as follows:

1) Statistics Time: Select a statistics time section.
2) Application Usage Distribution: Pie chart of all application usage distribution
3) Application Top 5: The table sorted in order of applications which are most frequently used ‘Usage by WLAN,’ ‘Usage by Device,’ and ‘Usage by User (Top 5)’ below are shown based on the applications most frequently used at first but if a specific application is selected in Application Top 5, they are changed to based on the application.
4) Usage Situation of Top 3: It shows the change of most frequently used top 3 applications by time in a graph.
5) Usage by WLAN: It shows the usage of a specific application by WLAN. At first, it illustrates the most frequently used application and if the operator selects another application in ‘Application Top 5’, it illustrates the application.
6) Usage by Device: It shows the usage of a specific application by device. At first, it illustrates the most frequently used application and if the operator selects another application in ‘Application Top 5’, it illustrates the application.
7) Usage by User (Top 5): It shows Top 5 users of a specific application. At first, it illustrates the most frequently used application and if the operator selects another application in ‘Application Top 5’, it illustrates the application.

The items of usage by user (Top 5) are as follows:

Item	Description
User ID	User ID of the station
MAC	MAC of the station
Controller	Name of the controller registered by the station
SSID	Name of SSID used by the station
USE KBYTE	Data usage
Usage Rate	Usage rate of the user among the whole usage of the application

3.12.2 Wlans

The Wlans menu shows the description of the applications used based on each Wlan. Below is the Wlans screen.

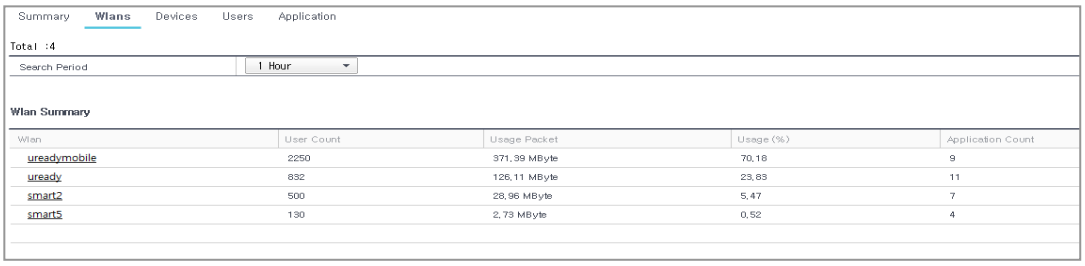


Figure 76. Main Screen of DPI-Wlans

In the usage by Wlan, Wlans are listed in order of usage and there are following items:

Item	Description
Wlan	Name of the Wlan
Number of users	Number of users by Wlan
Use BYTE	Data usage
Usage Rate	Usage rate by Wlan depending on whole data usage
Application Count	Number of applications used by each Wlan

If a specific Wlan is selected in the main screen of Wlans, you can see the detailed information on the use of applications of the Wlan. The screen is as shown below.

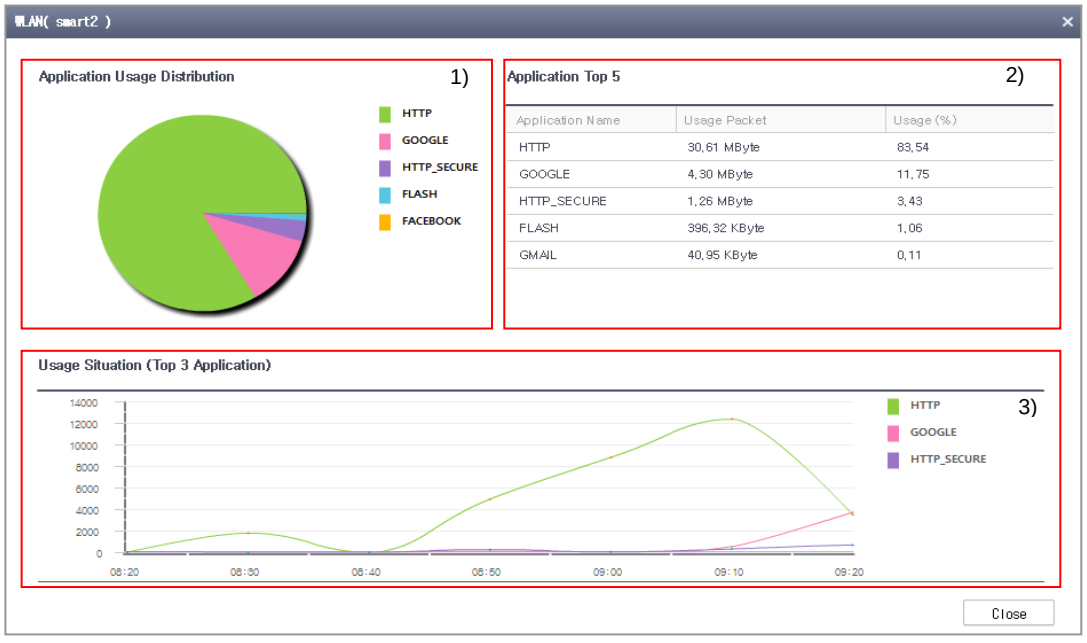


Figure 77. Detailed Screen of DPI-Wlans

Explanation on each number of the detailed screen of Wlan is as follows:

1) Application Usage Distribution: The distribution of usage of the Wlan by application
2) Application Top 5: Description on top 5 applications most frequently used in the Wlan
3) Usage Situation of Top 3: The changes of usage of top 3 applications most frequently used in the Wlan by time

3.12.3 Devices

The Devices menu shows the description of the applications used based on each device. Below is the screen of devices.

Figure 78. Main Screen of DPI-Devices

In the usage by device, devices are listed in order of usage and there are following items:

Item	Description
Device	Device name
Use BYTE	Data usage
Usage Rate	Usage rate by device depending on whole data usage
Application Count	Number of applications used by each device

If a specific device is selected in the main screen of devices, you can see the detailed information on the use of applications of the device. The screen is as shown below.

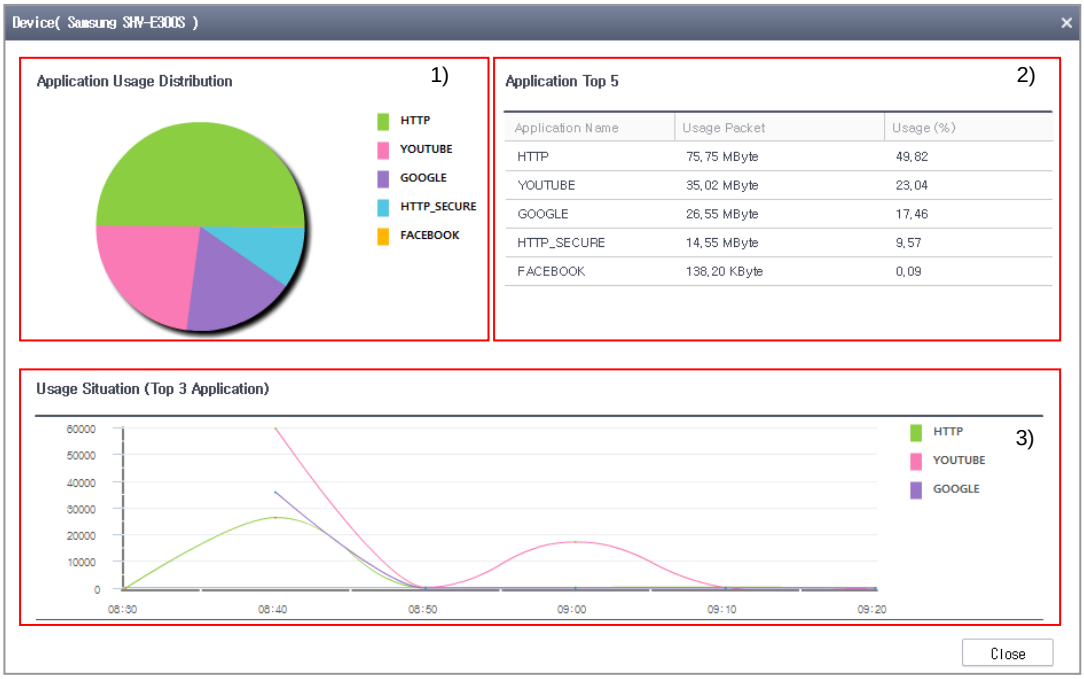


Figure 79. Detailed Screen of DPI-Devices

Explanation on each number of the detailed screen of devices is as follows:

1) Application Usage Distribution: The distribution of usage of the device by application
2) Application Top 5: Description on top 5 applications most frequently used in the device
3) Usage Situation of Top 3: The changes of usage of top 3 applications most frequently used in the device by time

3.12.4 Users

The Users menu shows the description of the applications used based on each user. Below is the screen of users.

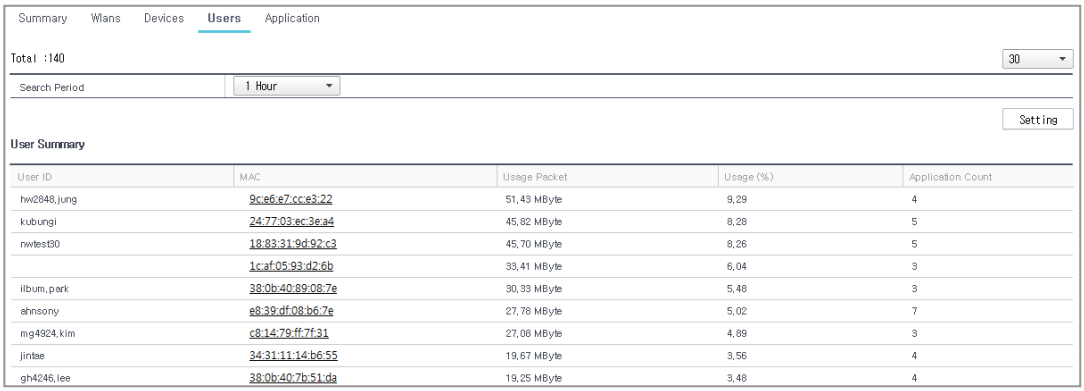


Figure 80. Main Screen of DPI-Users

In the usage by user, users are listed in order of usage and there are following items:

Item	Description
User ID	User ID
MAC	User Device MAC
Use Byte	Data usage used by each user
Usage Rate	Ratio of usage of the user to total usage
Application Count	Number of applications used by the user

If a specific user is selected in the main screen of users, you can see the detailed information on the use of applications of the user. The screen is as shown below.

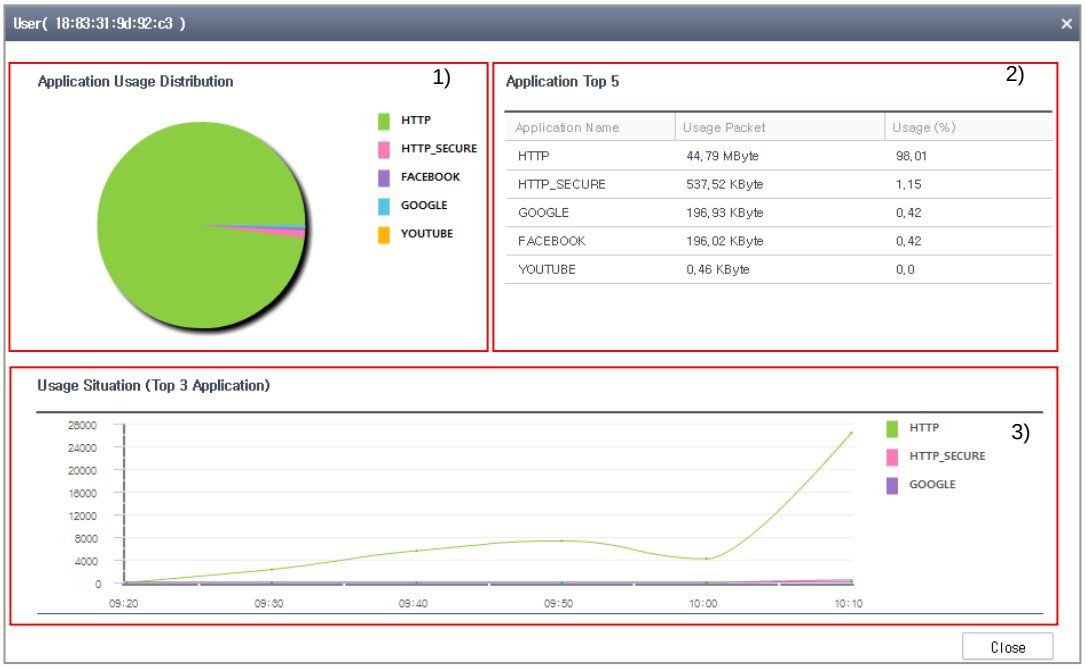


Figure 81. Detailed Screen of DPI-Users

Explanation on each number of the detailed screen of users is as follows:

1) Application Usage Distribution: The distribution of usage of the user by application
2) Application Top 5: Description on top 5 applications most frequently used by the user
3) Usage Situation of Top 3: The changes of usage of top 3 applications most frequently used by the user by time

3.12.5 Application

The Application menu shows the description on the usage of each application. Below is the screen of the Application.

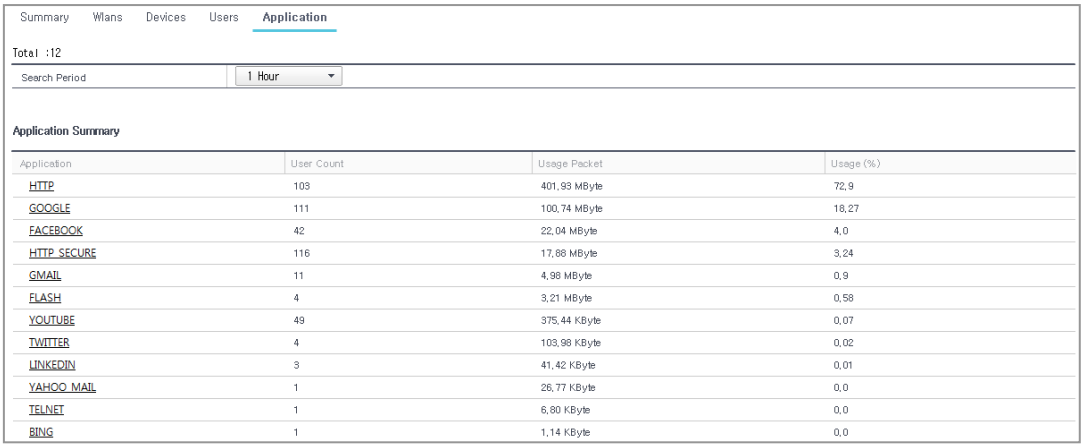


Figure 82. Main Screen of DPI-Application

In the usage by user, users are listed in order of usage and there are following items:

Item	Description
Application	Application name
Number of users	Number of users who use the application
Use Byte	Data usage used by each application
Usage Rate	Ratio of usage of the application to total usage

If a specific user is selected in the main screen of users, you can see the detailed information on the use of applications of the user. The screen is as shown below.

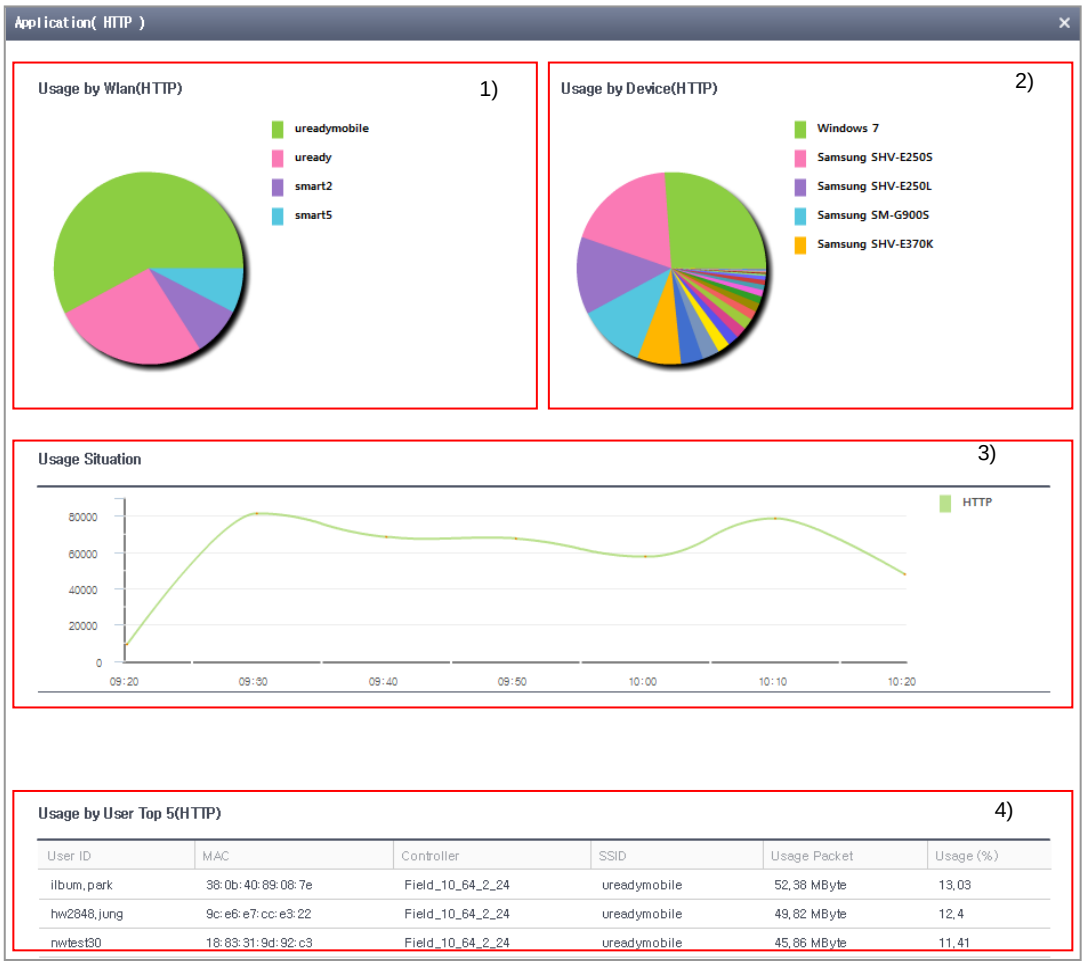


Figure 83. Detailed Screen of DPI-Application

Explanation on each number of the detailed screen of users is as follows:

1) Usage by WLAN: The distribution of usage by Wlan of the application
2) Usage by Device: The distribution of usage by device of the application
3) Usage Situation: Usage situation by time of the application
4) Usage by User (Top 5): Information on top 5 users in order of users who use the application most frequently

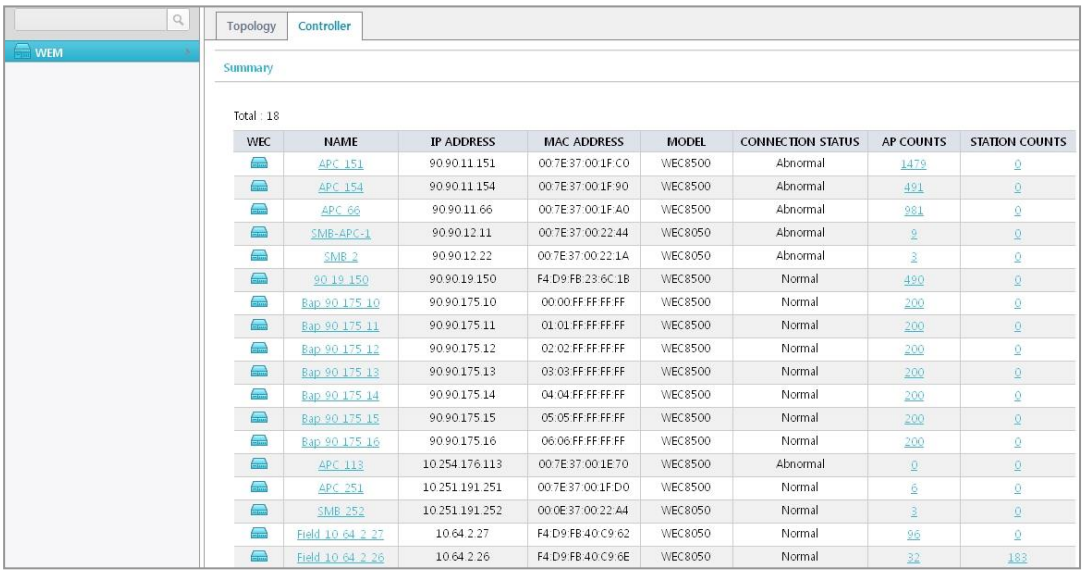
CHAPTER 4. Configuration

The configuration management is to view, change, add, and delete the information for each NE. By using the Configuration menu, you can view the current configuration and set up and control each NE
This menu is classified into following items:

- Controller/Device
- AP
- Mobility Group
- Controller Template
- AP Template
- Security

4.1 Controller/Device

While 'Configuration Management' → 'Controller' has been selected, when WEM in the tree viewer is selected, the summarized information on all controllers that the WEM now manages is provided in a form of table. If a specific cluster or controller group is selected instead of WEM, the summarized information on the controller belonging to the group can be viewed.



WEC	NAME	IP ADDRESS	MAC ADDRESS	MODEL	CONNECTION STATUS	AP COUNTS	STATION COUNTS
	APC_151	90.90.11.151	00:7E:37:00:1F:C0	WEC8500	Abnormal	1479	0
	APC_154	90.90.11.154	00:7E:37:00:1F:90	WEC8500	Abnormal	491	0
	APC_66	90.90.11.66	00:7E:37:00:1F:A0	WEC8500	Abnormal	981	0
	SMB-APC-1	90.90.12.11	00:7E:37:00:22:44	WEC8050	Abnormal	9	0
	SMB_2	90.90.12.22	00:7E:37:00:22:1A	WEC8050	Abnormal	3	0
	90_19_150	90.90.19.150	F4:D9:FB:23:6C:1B	WEC8500	Normal	490	0
	Bap_90_175_10	90.90.175.10	00:00:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_11	90.90.175.11	01:01:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_12	90.90.175.12	02:02:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_13	90.90.175.13	03:03:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_14	90.90.175.14	04:04:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_15	90.90.175.15	05:05:FF:FF:FF:FF	WEC8500	Normal	200	0
	Bap_90_175_16	90.90.175.16	06:06:FF:FF:FF:FF	WEC8500	Normal	200	0
	APC_113	10.254.176.113	00:7E:37:00:1E:70	WEC8500	Abnormal	0	0
	APC_251	10.251.191.251	00:7E:37:00:1F:D0	WEC8500	Normal	6	0
	SMB_252	10.251.191.252	00:0E:37:00:22:A4	WEC8050	Normal	3	0
	Field_10_64_2_27	10.64.2.27	F4:D9:FB:40:C9:62	WEC8050	Normal	96	0
	Field_10_64_2_26	10.64.2.26	F4:D9:FB:40:C9:6E	WEC8050	Normal	32	183

Figure 84. Summarized Controller Information Screen (consider changing)

The description on the summarized controller information is as follows:

Item	Description
WEC	A link immediately accessing WEB GUI of the controller. Click the icon and then immediately move to the WEB GUI login screen of the controller.
Name	Name of the controller
IP Address	IP address of the controller
MAC Address	MAC address of the controller
Model	Controller Models - WEC8500 - WEC8050
Connection status	Connection status between WEM and controller - Normal - Abnormal
Number of APs	Total number of APs connected to the controller
Number of Terminals	Total number of stations connected to the controller * There may be any difference between the real time information and the recent 5-minute information stored in WEM DB.

4.1.1 System

4.1.1.1 General

The ‘General’ menu allows the configuration of general settings in relation to the controller.

This menu allows configuration/retrieval of the following settings.

[AP Management Information]

Item	Description
IP address	IP address for AP management
Interface	Interface info for AP management (only for retrieval)

[Repeater Service]

Item	Description
Interface Group	Interface group to use for repeater service
Service	Enables/disables repeater service

[SIP ALG]

Item	Description
SIP ALG (VoIP AWARE)	Activates or deactives the SIP ALG (VoIP AWARE) service.
Sending CAC Limit Error Response Message	Activates or deactivates the error response function.
Detecting Long Time Call	Activates or deactivates the long time call detection function.
No Response Call-based Time (sec.)	Configures the reference time to process as no response call.
Long Time Connected Call-based Time (sec.)	Configures the reference time to determine as a long time connected call.
SIP Monitoring Port 1	Configures port 1 for monitoring SIP ALG.
SIP Monitoring Port 2	Configures port 2 for monitoring SIP ALG.
SIP Monitoring Port 3	Configures port 3 for monitoring SIP ALG.
SIP Monitoring Port 4	Configures port 4 for monitoring SIP ALG.
SIP Monitoring Port 5	Configures port 5 for monitoring SIP ALG.

[Voice Call Monitoring]

Item	Description
Voice Quality Monitoring	Enables/disables the system's voice quality monitoring function
Enhanced voice quality monitoring	Enables/disables the system's enhanced voice quality monitoring function

[Server Public Port]

Item	Description
FTP Public Port Number	Configures the FTP service public port.
SFTP Public Port Number	Configures the SFTP service public port.
HTTP Public Port Number	Configures the HTTP service public port.
HTTPS Public Port Number	Configures the HTTPS service public port.

Configuring Information

1) Select a controller to configure in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'System' → 'General' menu.
3) Configure the necessary settings.
4) Save the settings by clicking the 'Set' button.

4.1.1.2 Backup Controller

The ‘Backup Controller’ menu allows configuration of a backup controller for the selected controller. Information on controllers can be entered in the controller pool and then can be selected to be included in the backup controller list.

The backup controller configuration screen consists of the following settings.

[Fallback Configuration]

Item	Description
Service	Enables/disables the fallback function
Type	Specifies whether to run the service at all times or only for a specific period
Time	Specifies a specific period for which the service is set to run
Interval	Fallback test interval

[Controller Pool]

Item	Description
Controller Name	Controller name
Controller MAC Address	MAC address of the controller

[Backup Controller List]

Item	Description
Controller Name	Controller name
Controller MAC address	MAC address of the controller
IP address	IP address to use when connecting to the AP
Port	Port address to use when connecting to the AP
Public IP Address	Public IP address for connecting to the AP if the controller is in a NAT environment
Public Port	Port address for connecting to the AP if the controller is in a NAT environment

Setup

1) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘System’ → ‘Backup Controllers’ menu.
2) After configuring the fallback-related general settings, select the ‘Set’ button.
3) Click the ‘Add’ button in the Controller Pool to add a controller.

4) Select a type in the popup window. If entering manually, enter a controller name and its MAC address. If selecting from the controller list, select an item from the list.
5) Click the 'Add' button in the popup window to add a controller to the list.
6) Click the 'Add' button in the Backup Controller List to add a backup controller.
7) Enter all the information and click the 'Add' button in the popup window to add to the list.

4.1.1.3 mDNS Snooping General

The mDNS Snooping General menu provides functions for using the mDNS snooping service.

The configuration items of the mDNS setup screen are as follows.

[mDNS Snooping General]

Item	Description
mDNS Snooping Service	mDNS snooping function (enable/disable)

[Service Database List]

Item	Description
Service name	Name of services to use in mDNS (AirPrint, AirTunes, AppleTv, etc.)
Service string	Strings used in service names (ipp.tcp, raop.tcp, airplay.tcp, etc.)

Configuring

1) Select the 'Configure' → 'Controller/Device' → 'System' → 'mDNS Snooping General' menu.
2) Enable/disable the mDNS snooping service and click the 'Set' button.
3) Click the 'Add' button on the service database list to add the service to the service database list.
4) In the popup window, enter a service name and a service string.
5) Click the 'Set' button in the popup window to add the setting to the list.

Deleting

1) Select the 'Configure' → 'Controller/Device' → 'System' → 'mDNS Snooping General' menu.
2) Select a database to delete from the service database list and click the 'Delete' button to delete the database.

4.1.1.4 mDNS Snooping Profile

The mDNS Snooping Profile menu provides functions for using the services concerning mDNS snooping.

The configuration items of the mDNS profile screen are as follows.

[mDNS Snooping Profile]

Item	Description
Profile name	mDNS snooping profile name
Service count	Number of services registered in the profile

Configuring

1) Select the ‘Configure’ → ‘Controller/Device’ → ‘System’ → ‘mDNS Snooping Profile’ menu.
2) In mDNS Snooping Profile, click the 'Add' button.
3) Enter a profile name to use and click the 'Set' button.
4) Check that the specified profile is added to the mDNS snooping profile list.
5) Click on a snooping profile to use.
6) Select a service to configure from the popup menu.
5) Click the 'Add' button to add the setting to the list.

Deleting

1) Select the ‘Configure’ → ‘Controller/Device’ → ‘System’ → ‘mDNS Snooping Profile’ menu.
2) Select a profile to delete from the mDNS snooping profile list and click the 'Delete' button to delete the profile.

4.1.1.5 Configuration Synchronization

This function allows automatic synchronization of service settings between multiple controllers. When service settings are changed on the master controller, the settings are automatically applied to the connected slave devices.

The following settings can be checked.

[Configuration Synchronization]

Item	Description
Mode	Configuration Sync Mode (None/‘Active/Active’)

When in Active/Active mode, the following settings can be checked.

[Synced Controller]

Item	Description
ID	Controller index
Controller name	Name of the controller
IP address	IP address of the controller
Mode	Configuration sync mode of the controller
Role	Role mode of the controller
Connection status	Connection status of the controller

When in Active/Active mode, the following settings are available.

[Synchronization Role]

Item	Description
Mode	Synchronization role mode (Master/Slave/Standalone)

Configuring

1) Select a controller to configure in the tree viewer.
2) Select the 'Configure' → 'Controller/Device' → 'System' → 'Configuration Synchronization' menu.
3) If the configuration synchronization mode is Active/Active, select a synchronization role mode.
4) Click the 'Set' button to apply.

4.1.1.6 Country

The 'Country' menu allows configuration of a country code to be applied to the controller and transmission power editing for each country.

The following country settings are available.

[Preset Country Code]

Item	Description
Default Country Code	Specifies a country to apply to the controller
Default Environment	Specifies a controller operation environment (indoor, outdoor, both, non-country)
Country Code #1-3	Specifies a country

Item	Description
Environment #1-3	Specifies an environment
Preset General Channels and Maximum Transmission Level (5 GHz)	Maximum Tx power level at 5 GHz per channel
Preset General Channels and Maximum Transmission Level (2.4 GHz)	Maximum Tx power level at 2.4 GHz per channel
All Preset Channels (5 GHz)	All channels configured at 5 GHz
All Preset Channels (2.4 GHz)	All channels configured at 2.4 GHz

[Editing Country Code]

Item	Description
Country Code	Designates the country to be applied to the controller.
Maximum Transmission Power Level at 5 GHz	Configures Maximum Tx power level at 5 GHz per channel
Maximum Transmission Power Level at 2.4 GHz	Configures Maximum Tx power level at 2.4 GHz per channel

Setup

1) Select a controller to set up in Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'System' → 'Country' menu.
3) Set up the setup information items.
4) Click the 'Set' button to apply the country settings.

4.1.2 WLAN

4.1.2.1 Profile

This menu allows the retrieval and configuration of WLAN profiles of registered devices.

The setup items are shown below:

[Profile]

Item	Description
WLAN ID	WLAN ID
Name	Profile name
SSID	Service set identifier
Interface Group	Name of the interface group

Item	Description
Radio	Frequency band (2.4 GHz/5 GHz)
CAPWAP Tunnel Mode	Configures a CAPWAP tunnel mode.
SSID Hide	Configures SSID hide.
AAA Override	Activates or deactivates the AAA override function.
No. of Maximum UEs Connected	Configures number of maximum UEs connected.
AP Group List	List of AP groups to which the WLAN is added

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'WLAN' → 'Profile' menu.
3) WLAN profile list of the selected controller is displayed.
4) Click the 'Add'/'Delete' button at the bottom of the screen to add or delete WLAN profiles.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'WLAN' → 'Profile' menu.
3) WLAN profile list of the selected controller is displayed.
4) Click the 'Add' button.
5) Enter the WLAN profile settings.
6) Save the settings by clicking the 'Set' button.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'WLAN' → 'Profile' menu.
3) WLAN profile list of the selected controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.2.2 Security Layer 2

This menu provides a function of retrieving and configuring L2 security information set in the WLAN.

The items for configuring the security layer 2 are as follows:

[L2]

Item	Description
Profile Name	Profile name
Layer 2 Security Type	Basic Service Set (BSS) authentication type (NONE/Static WEP/802.1x (Dynamic WEP)/Static WEP + 802.1x (Dynamic WEP)/WPA + WPA2)
MAC Authentication	Configures the use of the MAC authentication.
MAC Filter	Configures a MAC filter.

[STATIC WEP]

Item	Description
WEP key format	Input format of the WEP encryption key (ASCII/HEX) - ASCII: ASCII string - HEX: Hexadecimal value
WEP key length	Key length (in bits) - 40 - 104
WEP key index	Key index (range: 1-4)
WEP key	WEP encryption key

[802.1x(DYNAMIC WEP)]

Item	Description
WEP key length (IEEE 1x)	Key length (in bits) - 40 - 104
EAPol re-authentication	EAP re-authentication interval (unit: seconds, range: 0-100,000)

[WPA+WPA2]

Item	Description
WPA	WPA Version 1

Item	Description
Encryption method (WPA)	Encryption method (TKIP/CCMP/BOTH) - TKIP: TKIP method - CCMP: AES-CCMP method - Both: TKIP and AES-CCMP methods
WPA2	WPA Version 2 (must be enabled at all times)
Encryption method (RSN)	Encryption type WPA2 only supports CCMP and cannot be changed.
Authentication key management (802.1x)	Authentication key algorithm (PSK/802.1x) - PSK: PSK (shared key) authentication method - 802.1x: 802.1x authentication method using a RADIUS server
Shared key format	Input format of the shared key (ASCII/HEX) - ASCII: ASCII string - HEX: Hexadecimal value
Shared key	Shared key
PMK validity (seconds)	PMK validity (unit: seconds, range: 0-1,000,000)
EAPoL re-authentication	EAP re-authentication interval (unit: seconds, range: 0-100,000)
Protected management frames (PMF)	Protected management frames (802.11w) function - Disabled: Disables the function - Optional: Enables the function and allows connection even by devices not using the function - Required: Enables the function but allows connection only by devices using the function

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘WLAN’ → ‘Security Layer 2’ menu.
3) The configuration status is displayed on the screen.
4) If the WLAN profile ('Profile Name') desired to configure is selected, the screen is converted to the screen of configuring security layer 2.
5) Configure the item for setting the selected profile.
6) Click the ‘Set’ button to save the settings.

4.1.2.3 Security Layer 3

This menu provides a function of retrieving and configuring L3 security information set in the WLAN.

The configuration items are as follows:

[Security Layer 3]

Item	Description
Profile Name	Profile name
Web Policy	Whether to use a web policy
Web Authentication	Web authentication
Upon Failure in MAC Authentication, Web Authentication	Upon failure in MAC authentication, uses web authentication.
Web Pass-Through	Moves to a specific address all the time when the user wants to use the web.
Conditional Web Transition	Conditional redirection
One-time Redirection	One-time redirection
Pre-authenticated ACL	ACL applied before the guest is authenticated
Web Page Type	Select Web Page Type (Downloaded/External)
URL	Activate when select External for Web Page Type. URL to which the guest is redirected

[Web Authentification]

Item	Description
Server Type	Authentification Server Type
1st~2nd RADIUS Server	RadiusServer for Authentification
Cache Period (DAYS)	Cache Period after authentificiation
Action after authentification	- Redirect: Excute redirect to defined URL - Request: Excute redirect to requested URL
Selected Profile name	Selected Profile name

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘WLAN’ → ‘Security Layer 3’ menu.
3) The configuration status of the security layer 3 is displayed on the screen.

4) If the WLAN profile (‘Profile Name’) desired to configure is selected, the screen is converted to the screen of configuring security layer 3.
5) Modify the item for setting the selected profile.
6) Click the ‘Set’ button to save the settings.

4.1.2.4 Security RADIUS

This menu provides a function of retrieving or configuring the information related to the security of the RADIUS server set in the WLAN.

The configuration items of security RADIUS are as follows:

Item	Description
Profile Name	WLAN profile
Fallback Interval	Configures the fallback period.
Charging Interval	Configures the charging period.
Authentication Server	Whether to perform the role as an authentication server
First to Third Authentication Servers	Configures an authentication server address.
Accounting Server	Whether to perform the role as an accounting server
First to Third Accounting Servers	Configures an accounting server address.
Selected Profile name	Selected Profile name

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘WLAN’ → ‘Security RADIUS’ menu.
3) The configuration status is displayed on the screen.
4) If the WLAN profile (‘Profile Name’) desired to configure is selected, the screen is converted to the screen of configuring security RADIUS.
5) Enter the settings.
6) Click the ‘Set’ button to save the settings.

4.1.2.5 802.11a/n/ac

This menu provides a function of retrieving or configuring the MCS information and data transmission rate of 802.11a/n/ac set in the WLAN.

The configuration items are as follows:

[Data Transmission Rate]
Configure whether to use each data rate (Disable/Supported/Basic).

Item	Description
6 Mbps	Whether to use 6 Mbps (Disable/Supported/Basic)
9 Mbps	Whether to use 9 Mbps (Disable/Supported/Basic)
12 Mbps	Whether to use 12 Mbps (Disable/Supported/Basic)
18 Mbps	Whether to use 18 Mbps (Disable/Supported/Basic)
24 Mbps	Whether to use 24 Mbps (Disable/Supported/Basic)
36 Mbps	Whether to use 36 Mbps (Disable/Supported/Basic)
48 Mbps	Whether to use 48 Mbps (Disable/Supported/Basic)
54 Mbps	Whether to use 54 Mbps (Disable/Supported/Basic)

[MCS Configuration]

Item	Description
Configuring HT(802.11n) Rx MCS	Configures HT(802.11n) Rx-related MCS.
Configuring VHT(802.11ac) MCS	Configures VHT(802.11ac)-related MCS.

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'WLAN' → '802.11a/n/ac' menu.
3) If the WLAN profile ('Profile Name') desired to configure is selected, the screen is converted to the setup screen.
4) Enter the settings.
5) Click the 'Set' button to save the settings.

4.1.2.6 802.11b/g/n

This menu provides a function of retrieving or configuring the MCS information and data transmission rate of 802.11b/g/n set in the WLAN.

The configuration items are as follows:

[Data Transmission Rate]
Configure whether to use each data rate (Disable/Supported/Basic).

Item	Description
1 Mbps	Whether to use 1 Mbps (Disable/Supported/Basic)
2 Mbps	Whether to use 2 Mbps (Disable/Supported/Basic)

Item	Description
5.5 Mbps	Whether to use 5.5 Mbps (Disable/Supported/Basic)
6 Mbps	Whether to use 6 Mbps (Disable/Supported/Basic)
9 Mbps	Whether to use 9 Mbps (Disable/Supported/Basic)
11 Mbps	Whether to use 11 Mbps (Disable/Supported/Basic)
12 Mbps	Whether to use 12 Mbps (Disable/Supported/Basic)
18 Mbps	Whether to use 18 Mbps (Disable/Supported/Basic)
24 Mbps	Whether to use 24 Mbps (Disable/Supported/Basic)
36 Mbps	Whether to use 36 Mbps (Disable/Supported/Basic)
48 Mbps	Whether to use 48 Mbps (Disable/Supported/Basic)
54 Mbps	Whether to use 54 Mbps (Disable/Supported/Basic)

[MCS Configuration]

Item	Description
Configuring HT(802.11n) Rx MCS	Configures HT(802.11n) Rx-related MCS.

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘WLAN’ → ‘802.11b/g/n’ menu.
3) If the WLAN profile (‘Profile Name’) desired to configure is selected, the screen is converted to the setup screen.
4) Enter the settings.
5) Click the ‘Set’ button to save the settings.

4.1.2.7 Advanced

This menu provides a function of retrieving and configuring the WLAN information set in the controller.

The configuration items are as follows:

[WLAN Advanced Options]

Item	Description
Profile Name	Profile Name
SSID	Service set identifier
ACL Rule	Name of the ACL rule
Non-permit of Static Address	Configures whether to receive the IP address by using the DHCP.

Item	Description
DHCP Override	Configures whether to use the DHCP override function.
DHCP Server	Enters the address of the DHCP server (Configures when the DHCP override is enabled).
WMM	Configures Wifi-MultiMedia (WMM) mode (Multimedia packet QoS preferred) (Enable/Disable).
Delivery Traffic Indication Message (DTIM)	Enters the Beacon DTIM period (1~255).
Terminal Timeout (sec.)	Time to make the UE time out if the UE is idle
AMPDU	Configures AMPDU (Enable/Disable).
VoIP Failure Detect	Whether to use the VoIP failure detection function (Enable/Disable)
Band Steering	Configures band steering (Disable/5.0GHz preferred/2.4 GHz preferred).
Load Balancing	Whether to use the load balancing function (Enable/Disable)
Threshold	Threshold
Maximum Denial Count	Enters the maximum denial count.
Multicast to Unicast	Whether to use the multicast function (Enable/Disable)
Discarding Multicast Packet	Whether to use the function of discarding a multicast packet (Enable/Disable)
REJECT PROBE Requesting Mode	Selects the requesting mode (RSSI, Time, Max. Allowed Stations).
802.11K	Configures 802.11K
RRM	- link-measurement - neighbor-report - beacon-passive-measurement - beacon-active-measurement - beacon-table-measurement - statistics-measurement - ap-channel-report
MDNS Snooping Profile	Configures mDNS Snooping Profile

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘WLAN’ → ‘Advanced’ menu.
3) The WLAN advanced configuration status is displayed on the screen.
4) If the WLAN profile (‘Profile Name’') desired to configure is selected, the screen is converted to the WLAN advanced configuration screen.
5) Enter the settings.
6) Click the ‘Set’ button to save the settings.

4.1.3 Radio

This menu allows retrieval and configuration of various wireless-related settings.

Available menu items and settings vary according to the selected device type.
When a controller is selected, the following menu items are available.

- 802.11a/n/ac
- QoS (a/n)
- 802.11h (a/n)
- 802.11n/ac (a/n/ac)
- Radio resource management (a/n)
- 802.11b/g/n
- QoS (b/g/n)
- 802.11n (b/g/n)
- Radio resource management (b/g/n)

When an AP is selected, the following menu items are available.

- 802.11a/n/ac
- 802.11b/g/n

4.1.3.1 802.11a/n/ac

This menu allows retrieval and configuration of the following settings.

[Service]

Item	Description
Service	Enables/disables service

[General]

Item	Description
Bandwidth (MHz)	Specifies bandwidth
Beacon Interval (TUS)	Specifies beacon interval
RTS Threshold (Bytes)	RTS threshold value
Short Retry Limit Count	Short retry limit count
Long Retry Limit Count	Long retry limit count
Fragmentation Threshold (Bytes)	Fragmentation threshold value
Tx MSDU Lifecycle (TUS)	Valid Tx MSDU time
Rx MSDU Lifecycle (TUS)	Valid Rx MSDU time

Item	Description
Maximum Connection AP Count	Maximum allowed connection client count
Controlled Voice Optimization	Enables/disables controlled voice optimization
Multi-antenna Mode	Configures a multi-antenna mode (Dynamic/Static).

[Data Transfer Rate]

Configures usage option (Disable/Supported/Basic) for each data rate.

Item	Description
6 Mbps	6 Mbps usage option (Disable/Supported/Basic)
9 Mbps	9 Mbps usage option (Disable/Supported/Basic)
12 Mbps	12 Mbps usage option (Disable/Supported/Basic)
18 Mbps	18 Mbps usage option (Disable/Supported/Basic)
24 Mbps	24 Mbps usage option (Disable/Supported/Basic)
36 Mbps	36 Mbps usage option (Disable/Supported/Basic)
48 Mbps	48 Mbps usage option (Disable/Supported/Basic)
54 Mbps	54 Mbps usage option (Disable/Supported/Basic)

[Call Admission Settings]

The CAC function is provided to protect existing calls from the voice calls that are received by a wireless LAN. The controller does not allow any additional calls when the maximum number of allowed voice calls per radio is reached.

Item	Description
Voice Optimization	Enables/disables CAC
Maximum number of calls	Maximum number of calls
Number of reserved H/O calls	Number of reserved handover calls
Minor Alarm Threshold	Threshold to generate a minor level alarm
Major Alarm Threshold	Threshold to generate a major level alarm

[UE Admission Control]

Item	Description
UE Extraction Control	Whether to use extraction control of the UE which fails to connect consecutively
Reconnection Count Threshold	Number of maximum allowable reconnections of the UE which fails to connect consecutively

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → '802.11a/n/ac' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.2 QoS (a/n)

This menu allows retrieval and configuration of the following Qos (a/n) related settings.

[Wired QoS]

Item	Description
Profile	Selected profile
TAGGING Policy-802.1p	802.1p QoS marking setting (None/User Priority/Default Value)
TAGGING Policy-DSCP	DSCP QoS marking setting (Select Enable to activate.)
TAGGING Policy-External DSCP	DSCP marking setting in the CAPWAP header (InnerPacket/Default Value)
TAGGING Policy-Internal DSCP	DSCP marking setting of packets coming from the controller and wireless device (No marking/Default Value)
Protocol	QoS protocol (None/802.1p/DSCP)
Voice-802.1p	802.1p QoS value that will be used for a voice packet
Voice-DSCP	DSCP QoS value that will be used for a voice packet
Video-802.1p	802.1p QoS value that will be used for a video packet
Video-DSCP	DSCP QoS value that will be used for a video packet
BEST EFFORT-802.1p	802.1p QoS value that will be used for a best effort packet
BEST EFFORT-DSCP	DSCP QoS value that will be used for a best effort packet
Background-802.1p	802.1p QoS value that will be used for a background packet
Background-DSCP	DSCP QoS value that will be used for a background packet

[Wireless QoS]

Item	Description
Profile	Selected profile
Voice-802.1p	802.1p QoS value that will be used for a voice packet
Voice-DSCP	DSCP QoS value that will be used for a voice packet
Video-802.1p	802.1p QoS value that will be used for a video packet
Video-DSCP	DSCP QoS value that will be used for a video packet

Item	Description
BEST EFFORT-802.1p	802.1p QoS value that will be used for a best effort packet
BEST EFFORT-DSCP	DSCP QoS value that will be used for a best effort packet
Background-802.1p	802.1p QoS value that will be used for a background packet
Background-DSCP	DSCP QoS value that will be used for a background packet

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → 'QoS (a/n)' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.3 802.11h (a/n)

This menu allows retrieval and configuration of the following 802.11h (a/n) related settings.

Item	Description
Transmission Power Limit	Signal strength limit
Channel Switching Alarm	Enables/disables channel switching alarm
Limit Mode	Enables/disables limit mode
Channel Switching Times	Channel switching times

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → '802.11h (a/n)' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.4 802.11n/ac (a/n/ac)

This menu allows configuration of the controller 802.11n (a/n/ac) related information.

[Global MCS]

Item	Description
Supported	Specifies supported type
HT (802.11n) Rx MCS Setting	HT (802.11n) Rx related MCS Setting
VHT (802.11ac) MCS Setting	VHT (802.11ac) related MCS Setting

[Operation Type]

Item	Description
Guard Interval-20 MHz	Selects whether the guard Interval (20 MHz) is short or long.
Guard Interval-40 MHz	Selects whether the guard Interval (40 MHz) is short or long.
Guard Interval-80 MHz	Selects whether the guard Interval (50 MHz) is short or long.
Beamforming	Enables/disables beamforming

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → '802.11n (a/n/ac)' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.5 Radio Resource Management (a/n)

This menu allows configuration of the controller's radio resource management (a/n) related information.

[Radio Resource Management]

Item	Description
Status	Enables/disables radio resource management
RF Group Name	RF group name

[Dynamic Power Management]

Item	Description
Status	Enables/disables dynamic power management
RSSI Threshold (dBm)	RSSI threshold of dynamic power management
Scan Interval (sec)	Power status info retrieval interval
Minimum Transmission Power	Minimum transmission power reference
Maximum Transmission Power	Maximum transmission power reference

[Dynamic Channel Selection]

Item	Description
Status	Enables/disables dynamic channel selection

Item	Description
Scan Interval (sec)	Power status info retrieval interval
Channel Usage Threshold (%)	Channel usage threshold
Interferer Level Threshold (%)	Interferer level threshold
Delayed Channel Change	Enables/disables delayed channel change
Association Option	Association option (Voice/Traffic/Station association)
Anchor Start Time	Anchor start time
Anchor End Time	Anchor end time
DCS Channel	DCS channel selection

[Coverage Hole Detection Control]

Item	Description
Status	Enables/disables coverage hole detection
Collecting Statistics	Enables/disables statistical collection
Trap Warning Message Alert	Enables/disables trap warning message alert
Statistical Power Control Activation	Enables/disables statistical power control
Failed Client Count Ratio	Failed client count ratio
Minimum RSSI Threshold for Voice Traffic (DBM)	Minimum RSSI threshold for voice traffic
Minimum RSSI Threshold for Data Traffic (DBM)	Minimum RSSI threshold for data traffic
Failed Client Count	Failed client count
Time Interval	Time interval

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Radio’ → ‘Radio Resource Management (a/n)’ menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the ‘Set’ button.

4.1.3.6 802.11b/g/n

This menu allows configuration of the controller's 802.11b/g/n related information.

[Service]

Item	Description
Service	Enables/disables service

[General]

Item	Description
Beacon Interval (TUS)	Specifies beacon interval
RTS Threshold (Bytes)	RTS threshold value
Short Retry Limit Count	Short retry limit count
Long Retry Limit Count	Long retry limit count
Fragmentation Threshold (Bytes)	Fragmentation threshold value
Tx MSDU Lifecycle (TUS)	Valid Tx MSDU time
Rx MSDU Lifecycle (TUS)	Valid Rx MSDU time
Maximum Connection Count	Maximum allowed connection client count
Controlled Voice Optimization	Enables/disables controlled voice optimization
Multi-antenna Mode	Configures a multi-antenna mode (Dynamic/Static).

[Data Transfer Rate]

Configures usage option (Disable/Supported/Basic) for each data rate.

Item	Description
1 Mbps	1 Mbps usage option (Disable/Supported/Basic)
12 Mbps	12 Mbps usage option (Disable/Supported/Basic)
5.5 Mbps	5.5 Mbps usage option (Disable/Supported/Basic)
6 Mbps	6 Mbps usage option (Disable/Supported/Basic)
9 Mbps	9 Mbps usage option (Disable/Supported/Basic)
11 Mbps	11 Mbps usage option (Disable/Supported/Basic)
12 Mbps	12 Mbps usage option (Disable/Supported/Basic)
18 Mbps	18 Mbps usage option (Disable/Supported/Basic)
24 Mbps	24 Mbps usage option (Disable/Supported/Basic)
36 Mbps	36 Mbps usage option (Disable/Supported/Basic)
48 Mbps	48 Mbps usage option (Disable/Supported/Basic)
54 Mbps	54 Mbps usage option (Disable/Supported/Basic)

[Call Admission Settings]

The CAC function is provided to protect existing calls from the voice calls that are received by a wireless LAN. The controller does not allow any additional calls when the maximum number of allowed voice calls per radio is reached.

Item	Description
Voice Optimization	Enables/disables CAC
Maximum number of calls	Maximum number of calls
Number of reserved H/O calls	Number of reserved handover calls
Minor Alarm Threshold	Threshold to generate a minor level alarm
Major Alarm Threshold	Threshold to generate a major level alarm

[UE Admission Control]

Item	Description
UE Extraction Control	Whether to use extraction control of the UE which fails to connect consecutively
Reconnection Count Threshold	Number of maximum allowable reconnections of the UE which fails to connect consecutively

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → '802.11 (b/g/n)' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.7 QoS (b/g/n)

This menu allows retrieval and configuration of the following Qos (b/g/n) related settings.

[Wired QoS]

Item	Description
Profile	Selected profile
TAGGING Policy-802.1p	802.1p QoS marking setting (None/User Priority/Default Value)
TAGGING Policy-DSCP	DSCP QoS marking setting (Select Enable to activate.)
TAGGING Policy-External DSCP	DSCP marking setting in the CAPWAP header (InnerPacket/ Default Value)
TAGGING Policy-Internal	DSCP marking setting of packets coming from the controller and

Item	Description
DSCP	wireless device (No marking/Default Value)
Protocol	QoS protocol (None/802.1p/DSCP)
Voice-802.1p	802.1p QoS value that will be used for a voice packet
Voice-DSCP	DSCP QoS value that will be used for a voice packet
Video-802.1p	802.1p QoS value that will be used for a video packet
Video-DSCP	DSCP QoS value that will be used for a video packet
BEST EFFORT-802.1p	802.1p QoS value that will be used for a best effort packet
BEST EFFORT-DSCP	DSCP QoS value that will be used for a best effort packet
Background-802.1p	802.1p QoS value that will be used for a background packet
Background-DSCP	DSCP QoS value that will be used for a background packet

[Wireless QoS]

Item	Description
Profile	Selected profile
Voice-802.1p	802.1p QoS value that will be used for a voice packet
Voice-DSCP	DSCP QoS value that will be used for a voice packet
Video-802.1p	802.1p QoS value that will be used for a video packet
Video-DSCP	DSCP QoS value that will be used for a video packet
BEST EFFORT-802.1p	802.1p QoS value that will be used for a best effort packet
BEST EFFORT-DSCP	DSCP QoS value that will be used for a best effort packet
Background-802.1p	802.1p QoS value that will be used for a background packet
Background-DSCP	DSCP QoS value that will be used for a background packet

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Radio’ → ‘QoS (b/g/n)’ menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the ‘Set’ button.

4.1.3.8 802.11n (b/g/n)

This menu allows configuration of the controller's 802.11n (b/g/n) related information.

[Global MCS]

Item	Description
Supported	Selects a type that will be supported
HT (802.11n) Rx MCS Setting	HT (802.11n) Rx related MCS setting

[Operation Type]

Item	Description
Guard interval-20 MHz	Selects whether the guard Interval (20 MHz) is short or long.
Guard interval-40 MHz	Selects whether the guard Interval (40 MHz) is short or long.
Beamforming	Enables/disables beamforming

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Radio' → '802.11n (b/g/n)' menu.
3) The setup status is displayed.
4) Enter the settings.
5) Save the settings by clicking the 'Set' button.

4.1.3.9 Radio resource management (b/g/n)

This menu allows configuration of the controller's radio resource management (b/g/n) related information.

[Radio Resource Management]

Item	Description
Status	Enables/disables radio resource management
RF Group Name	RF group name

[Dynamic Power Management]

Item	Description
Status	Enables/disables dynamic channel selection
RSSI Threshold (dBm)	RSSI threshold

Item	Description
Scan Interval (sec)	Power status info retrieval interval
Minimum Transmission Power	Minimum Transmission Power
Maximum Transmission Power	Maximum Transmission Power

[Dynamic Channel Selection]

Item	Description
Status	Enables/disables dynamic channel selection
Scan Interval (sec)	Channel status info retrieval interval
Channel Usage Threshold (%)	Channel usage threshold
Interferer Level Threshold (%)	Interferer level threshold
Delayed Channel Change	Enables/disables delayed channel change
Association Option	Association option (Voice/Traffic/Station association)
Anchor Start Time	Anchor start time
Anchor End Time	Anchor end time
DCS Channel	DCS channel selection

[Coverage Hole Detection Control]

Item	Description
Status	Enables/disables coverage hole detection
Collecting Statistics	Enables/disables statistical collection
Trap Warning Message Alert	Enables/disables trap warning message alert
Statistical Power Control Activation	Enables/disables statistical power control
Failed Client Count Ratio	Failed client count ratio
Minimum RSSI Threshold for Voice Traffic (DBM)	Minimum RSSI threshold for voice traffic
Minimum RSSI Threshold for Data Traffic (DBM)	Minimum RSSI threshold for data traffic
Failed Client Count	Failed client count
Time Interval	Time interval

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Radio’ → ‘Wireless Resource Management (b/g/n)’ menu.
3) The setup status is displayed.

4) Enter the settings.
5) Save the settings by clicking the ‘Set’ button.

4.1.4 Interface

4.1.4.1 VLAN

VLAN is a function that performs switching by grouping similar wireless terminals into a work group regardless of their location. As this is a virtual LAN, only the corresponding group is separated and processed. The impact of the unnecessary broadcasting packet can be eliminated and the stable switching sub-net can be configured.
In the ‘VLAN’ menu, a list of configured VLANs is displayed and you can add or delete VLANs to and/or from it.

[VLAN]

Item	Description
Interface name	VLAN name
VLAN ID	VLAN ID value
VLAN description	Description of the VLAN
Setup status	Status that the administrator selected (up/down)

[Physical Port]

Item	Description
Port	Port name
Mode	Selects a hybrid mode (Not Used/Access/Trunk/Hybrid)
Hybrid egress tagging	VLAN Hybrid Egress tagging (Enable/Disable)

[IP address]

Item	Description
IP address	IP address
Netmask	Netmask value

[DHCP]

Item	Description
Global use	Enables/disables the DHCP service
Option 82 status	Enables/disables Option 82
Option 82 type	Type of Option 82 (AP-MAC/AP-MAC-SSID/AP-ETHMAC)

[Access Configuration List]

Item	Description
ACL name	ACL name to be applied
MDNS Snooping Profile	Configures mDNS Snooping Prifle

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Interface’ → ‘VLAN’ menu.
3) The VLAN-related configuration status is displayed on the screen. Modify the desired items.
4) Click the ‘Apply’ button to save and apply the settings.

Adding

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Interface’ → ‘VLAN’ menu.
3) The VLAN-related configuration status is displayed on the screen.
4) To Add a VLAN ID, click the ‘Add’ button.
5) The information input screen is displayed. Configures a VLAN name.
6) Enter the name of the VLAN ID you want to add.
7) Select between up or down for configuration status.
8) Click the ‘Set’ button to save the settings.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Interface’ → ‘VLAN’ menu.
3) The VLAN-related configuration status is displayed on the screen.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

4.1.4.2 Group

The controller groups the different interfaces into separate interface groups so that a common profile or code can be applied to each group. In this menu, you can search and configure the interface groups of a registered device.

[General]

Item	Description
Name	Interface group name

Item	Description
Description	Description

[A List of Selected Interfaces]

Item	Description
Name	Move the interface list you want to configure onto the item on the left by using the << and >> buttons.

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Interface' → 'Group' menu.
3) The selected controller's interface group list is displayed.
4) The operator can add or delete an interface group by clicking the 'Add'/'Delete' button at the bottom of the screen.

Adding

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Interface' → 'Group' menu.
3) The selected controller's interface group list is displayed.
4) Click the 'Add' button.
5) The information input screen is displayed.
6) Enter the information of an interface group.
   - Enter a group name in the 'Name' field.
   - Select the interfaces you want to add and decide whether to add each of them by using the arrow keys.
7) Click the 'Set' button to save the settings.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Interface' → 'Group' menu.
3) The selected controller's interface group list is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.4.3 Port

This menu allows retrieval and configuration of the port information configured in the controller.

[Port]

Item	Description
Name	Name of the physical port
Link status	Information about port operation status
Cable type	Information about the type of connected cable
Auto negotiation	Enables/disables auto negotiation
Connection status	Information about connection status
Link speed	Link speed
Duplexity	Enables/disables the full duplex method
Setup status	Whether to use the port (Up/Down)
Flow control	Enables/disables the flow control
MTU size	Configures the size of MTU

[Switch Port]

Item	Description
Status of the switch port	Enables/disables the switch port
IP address	IP address assigned to the port
Netmask	Netmask of the IP address assigned to the port
Bridge mode	Uses bridge groups or Link Aggregate Groups (LAGs) (uses one of the two, sa1 and sa2)
Storm control mode/level	If you have selected bridge groups, configure storm control (Disable, Multicast, Broadcast, Both). The level of storm control means the number of packets that are allowed per second. A threshold must be set for it.

Setup

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Interface’ → ‘Port’ menu.
3) The configuration status of the port configuration is displayed on the screen.
4) Select the port’s name (‘NAME’).The configuration screen related to port configuration will then appear.
5) Configure the port information.
6) Save the settings by clicking the ‘Set’ button.

4.1.5 Security

4.1.5.1 RADIUS

In the ‘RADIUS’ menu, you can configure the Remote Authentication Dial-In User Service (RADIUS) server for UE authentication.

The RADIUS configuration information items are as follows:

[Radius Server]

Item	Description
IP address	IP address of the authentication server
Type	Server type (authentication, accounting, and authentication & accounting)
Authentication port	Port number of the authentication server
Accounting port	Port number of the accounting port
Shared key	Information about the public key
Key type	Type of authentication key
Count of retransmissions	Number of times retransmission is performed when there is no response
Retransmission interval (sec)	Retransmission interval when there is no response
Number of times retransmission failover is performed	Number of times retransmission failover is performed
Change of Authorization (CoA)	Whether to use CoA

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Security’ → ‘RADIUS’ menu.
3) The configuration status of the controller’s RADIUS server is displayed.
4) Click the ‘Add’ button.
5) The input screen for the server configuration items is displayed.
6) Enter the RADIUS server configuration item information.
7) Click the ‘Set’ button to save the settings.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Security’ → ‘RADIUS’ menu.
3) The controller’s RADIUS server list is displayed.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

4.1.5.2 Subordinate Portal

This menu is used to retrieve and configure information related to the web authentication page that appears when a guest user, who has been configured in the controller, connects to an AP.

[Web Page]

The web page configuration items are as follows.

Item	Description
Web page type	Web authentication method - Internal: Default internal web pages - Downloaded: Downloading web pages to the system - Customized: Editing internal web pages Logo, Header, Body, Footer, etc. can be edited on internal web pages. After enabling the GUEST SELF REGISTRATION option, the user only needs to enter their name, email, etc. to access the Internet service.

[Web Service Address]

The web service address setting item is as follows:

Item	Description
Domain name	Domain name The domain name entered is displayed so that the IP address of the web page is not exposed in tunnel mode.
IP address	IP address setting Since domain names cannot be used in local bridge mode, the address entered in the IP address field is displayed.

[Web Service Port]

The web service port setting item is as follows:

Item	Description
1~8	Configures a port.

[Web Authentication Cache List]

Click the ‘Clear’ button to clear the web-authenticated user list.

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Web Authentication' menu.
3) The web authentication-related configuration value is displayed on the screen.
4) Enter settings.
5) Click the 'Set' button to save the settings.

4.1.5.3 Firewall General

Determines whether to use the controller's firewall function.

Item	Description
Firewall	Enables/disables the firewall

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall General' menu.
3) In the 'firewall' option, determine whether to use the firewall (Enable/Disable).
4) Save the settings by clicking the 'Set' button.

4.1.5.4 Firewall Policy

A firewall is a function that blocks the infiltration of unwanted traffic from external networks. To this end, functions such as access filtering, Demilitarized Zone (DMZ), and port forwarding are provided.

- Access filtering: This filtering prevents connections from unknown IP addresses. It is used not only to control access to resources that are not released externally, but also to control the external resources that members might access.
- DMZ function: This is used to allow connections from outside while performing the access control service using a firewall. For LAN networks, such as web servers and mail servers that are protected by firewalls but require unrestricted connections from outside, the DMZ function separates these networks from LAN networks which have not had firewall blocking applied to them and ensures their connection to separate subnets.
- Port forwarding: This is a similar function to DMZ, but instead ensures a connection to a specific network without using a separate detached DMZ port. Like the DMZ function, the extra network service that enables access to the office's intranet from outside via the Internet can be enabled.
  However, when using the extra network service, it is important to ensure intranet security.

In the ‘Firewall Policy’ menu, you can retrieve and manage the controller’s firewall configuration status.

The configuration items for the firewall policy are as follows:

Item	Description
Name	Name of the firewall policy
Operations	Operations that the policy is to perform - Permit: Permission - Deny: Prohibition
Protocol	Protocol that the policy will use - Any: All are managed according to the configuration of ACTION - IP: Only IP is operated depending on action configuration. - UDP: Only the UDP is managed according to the configuration of ACTION - TCP: Only the Transmission Control Protocol (TCP) is managed according to the configuration of ACTION - ICMP: Only the Internet Control Message Protocol (ICMP) is managed according to the configuration of ACTION.
Source IP address	Source IP address
Source netmask	Source netmask
Source port setup	Defines the action of the source port (Any, =, RANGE)
Destination IP address	Destination IP address
Destination netmask setup	Destination netmask
Destination port	Defines the action of the destination port (Any, =, RANGE)
ICMP Type	Configures the type of the ICMP message to be transmitted in the network.

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Security’ → ‘Firewall Policy’ menu.
3) The configuration status of the firewall policy will be displayed on the screen.
4) You can add/delete a firewall policy by clicking the ‘Add’/‘Delete’ button at the bottom of the screen.
   To modify a firewall policy, click on the name (the ‘NAME’ item) of the firewall policy you want to modify.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall Policy' menu.
3) The firewall's configuration status is displayed on the screen.
4) Click the 'Add' button.
5) Enter the information by referring to the configuration item.
6) Save the settings by clicking the 'Set' button.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall Policy' menu.
3) The firewall's configuration status is displayed on the screen.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.5.5 Firewall Interface

The Firewall Interface is used to retrieve or modify the configuration status of the controller's firewall interface and you can also add or delete a firewall interface to and/or from this menu.

The configuration items for the firewall interface are as follows:

Item	Description
Interface	Interface name
Policy rule	ACL name
Direction	Direction in which the firewall is applied - Ingress - Egress - Forward

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall Interface' menu.
3) The configuration status of the controller's firewall interface is displayed.
4) You can add/delete a firewall interface by clicking the 'Add'/'Delete' button at the bottom of the screen. To modify a firewall interface, click on the name (the 'Interface' item) of the interface you want to modify.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall Interface' menu.
3) The configuration status of the controller's firewall interface is displayed.
4) Click the 'Add' button.
5) Enter the information in the field of each configuration item.
6) Save the settings by clicking the 'Set' button.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Firewall Interface' menu.
3) The configuration status of the controller's firewall interface is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.5.6 NAT Pool

The NAT pool is used to retrieve, modify, add, or delete the configuration status of the controller's Network Address Translation (NAT) pool.

The configuration items for the NAT pool are as follows:

Item	Description
Name	Name of the NAT pool
Starting IP address	Start IP address of the NAT pool
Ending IP address	End IP address of the NAT pool
Subnet mask	IP subnet mask value

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Pool' menu.
3) The configuration status of the controller's NAT pool is displayed.
4) You can add/delete a NAT pool by clicking the 'Add'/'Delete' button at the bottom of the screen.
   To modify a NAT pool, click on the name (the 'NAME' item) of the NAT pool you want to modify.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Pool' menu.
3) The configuration status of the controller's NAT pool is displayed.
4) Click the 'Add' button.
5) Fill in the field of each NAT pool configuration item.
6) Save the settings by clicking the 'Set' button.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Pool' menu.
3) The configuration status of the controller's NAT pool is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.5.7 NAT Policy

The NAT policy is used to retrieve, modify, add, or delete the configuration status of the controller's NAT policy.

The configuration items for the NAT policy are as follows:

[NAT Translation Rule]

Item	Description
Type	Translation Type - Dynamic Network Address Translation (DNAT) - Static Network Address Translation (SNAT)
Direction	Direction (Inside/Outside)
Mode	Translation mode (Static/List)
Protocol type	Type of protocol (Any/TCP/UDP)
IP address	Original IP address
Port	Original input port
Translated IP address	Changed IP address
Translated port	Changed port
Firewall policy	Name of the firewall policy
NAT pool	Name of the NAT pool

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Policy' menu.
3) The configuration status of the controller's NAT translation is displayed.
4) You can add/delete a NAT translation by clicking the 'Add'/'Delete' button at the bottom of the screen.
   To modify a NAT translation, click on the type of NAT translation you want to modify.

Adding

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Policy' menu.
3) The configuration status of the controller's NAT translation is displayed.
4) Click the 'Add' button.
5) The input screen for the NAT translation information is displayed.

6) Enter the information in the field of each configuration item.

7) Click the 'Set' button to save the settings.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Nat Policy' menu.
3) The configuration status of the controller's NAT translation is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.5.8 NAT Interface

The NAT interface is used to retrieve, modify, add, or delete the configuration status of the controller's NAT interface.

The configuration items for the NAT interface are as follows:

Item	Description
Name	Name of the MAC filter
Policy	Policy to perform (Allow/Deny)
Registration Upon Failure in MAC Authentication	Configures access blocking if the UE fails to get MAC authentication.
Access Blocking Time (min)	Time to block the access
Registration upon Detection of Malicious UE	Configures access blocking if the malicious UE is detected.

Item	Description
Access Blocking Time (min)	Time to block the access
Registration of UE with Association and Handover Success Rate	Configures access blocking if the UE has low association and handover success rate.
Access Blocking Time (min)	Time to block the access

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'NAT Interface' menu.
3) The configuration status of the controller's NAT interface is displayed.
4) Click on the NAT interface whose configuration you want to modify.
5) Enter the information in the field of each NAT interface configuration item.
6) Save the settings by clicking the 'Set' button.

4.1.5.9 MAC Filter

The MAC filter is used to retrieve, modify, add, or delete the configuration status of the controller's MAC filter.

The configuration items for the MAC filter are as follows:

Item	Description
Name	Name of the MAC filter
Policy	Policy to be carried out (Allow/Deny)
Interval	Interval for MAC filtering
Count	Number of applied MAC addresses

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'MAC Filter' menu.
3) The configuration status of the controller's MAC filter is displayed.
4) Click on the name (the 'Number' item) of the MAC filter whose configuration you want to modify.
5) Enter the information in the field of each MAC filter configuration item.
6) Save the settings by clicking the 'Set' button.

4.1.5.10 TACACS+

The TACACS+(Terminal Access Controller Access Control System+) is used to retrieve, modify, add, or delete the configuration status of the controller's TACACS+.

The configuration items for TACACS+ are as follows.

Item	Description
ID	TACACS+ server ID
IP address	TACACS+ server IP
Shared key	TACACS+ server shared key
Port	TACACS+ server port number (range: 1-65535, default: 49)
Retransmission interval (sec)	Retransmission interval for a + message (range: 1-5, default value: 2, unit: seconds)
Retransmission times before failover	Maximum retransmission times of TACACS+ message before a TACACS server failover is attempted (range: 0-3, default value: 2)
Source IP address	Source IP address of the TACACS+ message This must be one of the IP addresses configured in the W-EP WLAN system.
Status	Status of packet transmission to TACACS+ server (default: enable)

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'TACACS+' menu.
3) The configuration status of the controller's TACACS+ is displayed.
4) Click on the name (the 'Number' item) of the TACACS+ whose configuration you want to modify.
5) Enter the information in the field of each TACACS+ configuration item.
6) Save the settings by clicking the 'Set' button.

Adding

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'TACACS+' menu.
3) The configuration status of the controller's TACACS+ is displayed.
4) Click the 'Add' button.
5) The input screen window for TACACS+ information is displayed.
6) Enter the information in the field of each configuration item.
7) Click the 'Set' button to save the settings.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'TACACS+' menu.
3) The configuration status of the controller's TACACS+ is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.5.11 External BYOD (Bring Your Own Device) Server

The function of configuring the external BYOD server is configured.

The configuration items of the operator are as follows:

Item	Description
Service	Whether to activate the external BYOD server interoperation function (Enable/Disable)
Server IP Address 1	BYOD Server IP Address Airfront IP upon the interoperation with AirCuve BYOD Suite.
Server IP Address 2	IP address of the Byfront IP upon the interoperation with AirCuve BYOD Suite
Requested URL	Upon the interoperation with AirCuve BYOD Suite, the HTTPS request URL necessary to update the list of all authentications

Item	Description
Sync. Status	Result value of updating the list of all authentications
Sync. Failure Reason	Reason of failure if the update of the list of all authentications fails - None: No failure - No response: When there is no response from the BYOD server - Invalid data format: When the BYOD server failed to send the data on the list of all authentications or in the invalid format

Viewing and Changing

1) Select the equipment (controller) to view in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'External BYOD Configuration' menu.
3) The configuration status of the operator's authentication method of the controller is displayed.
4) Enter the setting information.
5) Click the 'Set' button to save the settings.
6) Click the 'Force Sync' button to check the status of the sync with the external BYOD server.

4.1.5.12 Operator

The Operator menu is used to configure how the operator of the controller will be authenticated.

The operator's configuration items are as follows.

Item	Description
Authentication scheme	- Local: Uses the authentication information of the controller itself - TACACS+: Uses the authentication information of the TACACS+ server - Local/TACACS+: Uses the authentication information of the controller itself/TACACS+ server - TACACS+/Local: Uses the authentication information of the TACACS+ server/controller itself

Retrieving and Changing

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Security' → 'Operator' menu.
3) The configuration status of the controller's operator authentication type is displayed.
4) Click on the authentication type whose configuration you wish to modify.
5) Save the settings by clicking the 'Set' button.

4.1.6 ACL

The ACL allows different network access authority depending on the user. In addition, the ACL analyzes the packet information for network traffic control using many kinds of filtering methods, and provides a function that processes packets according to the method defined by the operator.

The key functions supported in relation to ACL are as follows.

- IPv4 address and MAC address filtering function.
- IP, TCP, UDP, and ICMP are supported.
- Destination IP address and port, and source IP address, port, and protocol are supported. An IP address can be entered in wildcard form and a port can be specified in a range of numbers.
- Admin ACL is supported, which enables packet control whose final destination is the controller.
- Various operators are supported.

4.1.6.1 Time Profile

The Time Profile menu is used to retrieve and configure the time profile of a registered device.

The configuration items for the time profile are as follows.

Item	Description
Name	Name of the time profile
Type	Information about the type of time profile (Absolute/Periodic)
Period	Period of time during which the time profile is applied (From now on/Range). This needs to be configured when the type is Periodic.
Start date	Information about the start date and time of ACL. This needs to be configured when the type is Absolute
End date	Information about the end date and time of ACL. This needs to be configured when the type is Absolute
Date	Date information that needs be configured when the type is Periodic and the period is Range
Time	Range of time in which ACL is applied. This needs to be configured when the type is Periodic.
Repetition type	How the ACL is applied repeatedly. This needs to be configured when the type is Periodic - Daily - Days of the Month - Days of the Week - Specific Days

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'Time Profile' menu.
3) The configuration status of the time profile is displayed.
4) You can add/delete a time profile by clicking the 'Add'/'Delete' button at the bottom of the screen.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'Time Profile' menu.
3) The configuration status of the time profile is displayed.
4) Click the 'Add' button.
5) Open the input screen for the time profile information.
6) Enter the information in the field of each configuration item.
7) Click the 'Set' button to save the settings.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'Time Profile' menu.
3) The configuration status of the time profile is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.6.2 IP ACL

The IP ACL menu is used to retrieve and configure the IP ACL rules items of a registered device.

The configuration items for IP ACL rules are as follows:

Item	Description
Name	Name
Sequence number	Serial number
Operations	Permit/Deny
Protocol	Protocol
Originating	Origination Information(Any/Address/URL)
Originating Port Number	If TCP/UDP is selected as protocol, port number should be defined.
Destination	Destination Information(Any/Address/URL)
Destination Port Number	If TCP/UDP is selected as protocol, port number should be defined.
TOS	ToS Type (Not Used/DSCP/Precedence) Tos Value should be defined if selected except Not Used.
OS AWARE	OS aware value

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'IP ACL' menu.
3) The configuration status of the selected controller's IP ACL is displayed on the screen.
4) You can add/delete an IP ACL rule by clicking the 'Add'/'Delete' button at the bottom of the screen.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'IP ACL' menu.
3) The configuration status of the selected controller's IP ACL rules is displayed on the screen.

4) Click the ‘Add’ button.
5) The information input screen window is displayed.
6) Enter the information in the field of each configuration item.
7) Click the ‘Set’ button to save the settings.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘ACL’ → ‘IP ACL’ menu.
3) The configuration status of the selected controller’s IP ACL rules is displayed on the screen.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

4.1.6.3 Access Group (Interface)

The Access Group menu is used to search and configure the access group of a registered device.

The configuration items for the access group are as follows.

Item	Description
Interface	Interface name
Direction	Direction of application (Ingress/Egress)
ACL Rule	Name of applied ACL rule

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘ACL’ → ‘Access Group (Interface)’ menu.
3) The access group setup status of the selected controller is displayed.
4) Operator can add or delete an access group by clicking ‘Add’/‘Delete’ button at the bottom of screen

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘ACL’ → ‘Access Group (Interface)’ menu.
3) The access group setup status of the selected controller is displayed.
4) Click the ‘Add’ button.
5) Fill in the field of each access group configuration item.
6) Save the settings by clicking the ‘Set’ button.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'Access Group (Interface)' menu.
3) The access group setup status of the selected controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.6.4 Access Group (System)

In this menu, you can retrieve and configure information about the access group (system) that is configured in the controller.

The setup items are shown below:

Item	Description
ACL rule	Name of the ALC rule

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'Access Group (System)' menu.
3) The access group setup status of the selected controller is displayed.
4) Modify the 'ACL rule' setup.
5) Save the settings by clicking the 'Set' button.

4.1.6.5 Access Group (Wireless)

This menu is used to retrieve or set up the access group (wireless) item configured in the controller. Set up the ACL rule to use in the WLAN profile in advance and apply it to the controller.

The setup items are shown below:

Item	Description
Instance ID	Instance ID
ACL rule	Name of applied ACL rule

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'ACL' → 'access group (wireless)' menu.

3) The access group (wireless) setup status of the selected controller is displayed.
4) Operator can add or delete an access group by clicking ‘Add’/‘Delete’ button at the bottom of screen

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘ACL’ → ‘access group (wireless)’ menu.
3) The access group setup status of the selected controller is displayed.
4) Click the ‘Add’ button.
5) Enter by referring to the access group (wireless) setup item.
6) Save the settings by clicking the ‘Set’ button.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘ACL’ → ‘access group (wireless)’ menu.
3) The setup status of the selected controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

4.1.7 DHCP

4.1.7.1 Proxy/Relay

The ‘Proxy/Relay’ menu is used to set up the controller-support Dynamic Host Configuration Protocol (DHCP) Proxy/Relay mode. The DHCP proxy mode enables a wireless terminal to connect to a server while hiding the location of the DHCP server from the wireless terminal. The DHCP relay mode directly connects the DHCP request of a wireless terminal to a sever.

The Proxy/Relay setup information items are shown below.

Item	Description
Mode	DHCP service mode (Proxy/Relay)
Timeout	DHCP service timeout
Existing DHCP server	First DHCP server IP address
Auxiliary DHCP server	Second DHCP server IP address

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'Proxy/Relay' menu.
3) The setup status is displayed.
4) Enter the Proxy/Relay setup information.
5) Save the settings by clicking the 'Set' button.

4.1.7.2 Internal DHCP

The internal DHCP menu is used to set up a DHCP server in a controller to provide DHCP service in an environment where an external DHCP server cannot be connected to.

The DHCP setup information items are shown below.

[DHCP Server]

Item	Description
Service Status	Enable/Disable of internal DHCP service

[Profile List]
This menu is used to set up all the DHCP-related services supported by the controller in a batch by using a single profile.

The information items available in the profile list table is shown below.

Item	Description
Name	Profile name
Network	Network bandwidth to apply
Netmask	Netmask to apply
allocation time (sec)	DHCP lease time

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'Internal DHCP' menu.
3) The internal DHCP information of the controller is displayed.
4) You can add or delete a profile by clicking the 'Add'/'Delete' button at the bottom of screen.

Adding

1) Select an equipment (controller) to set up in the Tree Viewer.

2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'Internal DHCP' menu.

3) The internal DHCP information of the controller is displayed.

4) Click the 'Add' button.

5) The screen switches to a profile setup screen.

6) Enter the profile list information detailed below and click 'Setup'.

Item	Description
Name	Profile name
Network	Network bandwidth to apply
Netmask	Netmask to apply
allocation time (sec)	DHCP lease time
Domain name	DHCP domain name
Default gateway	Default gateway
First-Third DNS mode	IP address of the Domain Name Service (DNS) server
First-Third NTP mode	IP address of the Network Time Protocol (NTP) server

7) Set up the range pool items by clicking the 'Add' button.
The setup items of the range pool are shown below.

Item	Description
Profile name	Profile name
Starting IP address	Starting IP address of the pool
Ending IP address	Ending IP address of the pool

8) Set up the fixed address pool items by clicking the 'Add' button.
The fixed address pool setup items are shown below.

Item	Description
Profile Name	Profile name
MAC address	MAC address of the device to which the profile will be applied
IPv4 address	IP address of the device to which the profile will be applied

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'Internal DHCP' menu.
3) The profile server list of the controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.7.3 OS Aware

The OS Aware menu is used to set up the information required for the system to recognize the OS of a terminal connected to the system.

The information displayed when selecting the menu is shown below.

[OS Aware]

Item	Description
OS Name	Sets the name of the operating system to be added.
OS Type	Configures an OS type (android, ios, windows, mac).
Rank	Configures OS Aware rank information.
DHCP Option	Configures the DHCP option number.
Fingerprint	Sets a fingerprint to be recognized.

Adding

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'OS Aware' menu.
3) The OS Aware list table of the controller is displayed.
4) Click the 'Add' button.
5) An additional OS Aware pop-up is displayed.
6) Enter OS Aware information item and click 'Setup'.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'DHCP' → 'OS Aware' menu.
3) The OS Aware list table of the controller is displayed.
4) Select the item you wish to delete in the list table.
5) Click the 'Delete' button.

4.1.8 QoS

4.1.8.1 Profile

You can retrieve or set up the Quality of Service (QoS) profile of a registered device.

The setup items of QoS profile are shown below.

Item	Description
Name	QoS profile name
Description	Description
Maximum Dot1p tag	QoS DOT1P priority tag
Downward bandwidth limit per user (Kbps)	Upward limit speed
Upward bandwidth limit per user (Kbps)	Downward limit speed
Voice-802.1p	802.1p QoS value that will be used for a voice packet
Voice-DSCP	DSCP QoS value that will be used for a voice packet
Video-802.1p	802.1p QoS value that will be used for a video packet
Video-DSCP	DSCP QoS value that will be used for a video packet
BEST EFFORT-802.1p	802.1p QoS value that will be used for a best effort packet
BEST EFFORT-DSCP	DSCP QoS value that will be used for a best effort packet
Background-802.1p	802.1p QoS value that will be used for a background packet
Background-DSCP	DSCP QoS value that will be used for a background packet

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘QoS’ → ‘Profile’ menu.
3) The QoS profile setup status of a controller is displayed.
4) You can add or delete a profile by clicking the ‘Add’/‘Delete’ button at the bottom of screen.

Adding

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘QoS’ → ‘Profile’ menu.
3) The QoS profile setup status of a controller is displayed.
4) Click the ‘Add’ button.
5) Enter a profile setup item.
6) Save the settings by clicking the ‘Set’ button.

Deleting

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘QoS’ → ‘Profile’ menu.
3) The QoS profile setup status of a controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

4.1.9 RBAC

4.1.9.1 Role Profile

It provides a function of viewing and configuring a role profile of Role Based Access Control (RBAC) of the registered equipment.

The configuration items of the role profile are as follows:

Item	Description
Name	Name of the role profile
ACL Rule	Name of the applied ACL rule
User QoS	Name of the applied QoS
Application QoS	Name of applied Application QoS
VLAN ID	Applied VLAN ID value
URL	Redirect URL

Viewing

1) Select the equipment (controller) to display in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Role Profile’ menu.
3) The configuration status of the role profile of the controller is displayed.
4) Click the 'Add' or 'Delete' button on the bottom of the screen to add or delete a profile.

Adding

1) Select the equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Role Profile’ menu.
3) The configuration status of the role profile of the controller is displayed.
4) Click the ‘Add’ button.
5) Enter the profile configuration item.
6) Click the ‘Set’ button to save the settings.

Deleting

1) Select the equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Role Profile’ menu.
3) The configuration status of the role profile of the controller is displayed.
4) Select the frontmost check box of the item to delete.
5) Click the ‘Delete’ button to delete the selected item.

4.1.9.2 Applicable Profile

The configuration items of the applicable profile are as follows:

Item	Description
Name	Name of the applicable profile
Priority	Priority to apply
The condition to be used.	Condition to be applied
Role Profile	Name of the applicable role profile

Viewing

1) Select the equipment (controller) to display in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Applicable Profile’ menu.
3) The configuration status of the applicable profile of the selected controller is displayed on the screen.
4) Click the ‘Add’ or 'Delete' button on the bottom of the screen to add or delete a profile.

Adding

1) Select the equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Applicable Profile’ menu.
3) The configuration status of the applicable profile of the selected controller is displayed on the screen.
4) Click the ‘Add’ button.
5) Display the information entry screen.
6) Refer to the configuration items to enter the value.
7) Click the ‘Set’ button to save the settings.

Deleting

1) Select the equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘RBAC’ → ‘Applicable Profile’ menu.

3) The configuration status of the applicable profile of the selected controller is displayed on the screen.
4) Select the frontmost check box of the item to delete.
5) Click the 'Delete' button to delete the selected item.

4.1.9.3 ACL Profile

This menu provides a function of retrieving and configuring the ACL profile set in the controller.

The information items in the ACL profile table are as follows:

Item	Description
Name	Name of the ACL profile
Number of ACLs	Number of ACLs included in the ACL profile
Number of All Rules	Number of rules set in the ACL profile

Viewing

1) Select the equipment (controller) to view in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'RBAC' → 'ACL Profile' menu.
3) The configuration status of the ACL profile of the selected controller is displayed on the screen.
4) Click the 'Add' or 'Delete' button on the bottom of the screen to add or delete a profile.

Adding

1) Select the equipment (controller) to view in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'RBAC' → 'ACL Profile' menu.
3) The configuration status of the ACL profile of the selected controller is displayed on the screen.
4) Click the 'Add' button.
5) The information entry screen is displayed.
6) Enter the ACL profile information by referring to the following entry items.

[Profile]

Item	Description
Name	Name of the ACL profile to configure
Number of ACLs	Number of ACLs configured

[ACL]

Item	Description
Name	Locates the ACL list to configure and the ACL list desired on the left by using the << and >> buttons.

Deleting

1) Select the equipment (controller) to view in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'RBAC' → 'ACL Profile' menu.
3) The configuration status of the ACL profile of the selected controller is displayed on the screen.
4) Select the frontmost check box of the item to delete.
5) Click the 'Delete' button to delete the selected item.

4.1.10 AP

4.1.10.1 Profile

The 'AP list' menu is used to retrieve or set up the list of APs included in the selected controller.
The setup screen is displayed when an operator selects an AP to set up in the list.

The setup items of AP list menu are as follows:

Item	Description
Name	A hyperlink leading to the screen for AP name or AP setup is provided.
IP address	Information of the IP address allocated to the AP
MAC address	MAC address of the AP
Controller	Name of the controller where the AP is connected
Mode	AP mode (General/Root/Repeater/Sniffer/Relay) In case of a remote AP, (r) is attached next to the mode.
Configuration Status	Up/down status by operator
Operating Status	Real time AP operation status (up/down)
Ethernet Speed (MBPS)	Link connection speed of AP
Ethernet Duplex	Link connection mode of AP
5 GHz channel	Information of the 5 GHz channel currently being used
2.4 GHz channel	Information of the 2.4 GHz channel currently being used
Radio base MAC	Radio base MAC address of the AP
Model	AP model

Deleting AP

You can delete a specific AP in the AP list table. Select an AP to delete and click the 'Delete' button at the top right corner.


NOTE

When an AP is deleted, it is deleted only in the selected controller and the setup information in other controllers is not deleted.

Rebooting AP

You can reboot a specific AP in the AP list table. Select an AP to reboot and click the 'Reboot' button at the top right corner.

4.1.11 AP group

4.1.11.1 Profile

This menu is used to retrieve or set up a profile for the AP group in the controller. An operator can manage each group flexibly by using the 'AP Group' menu.

The information contained in the AP group table is shown below:

Item	Description
Name	AP group name In case of a remote AP group, (r) is attached next to the name.
Number of APs	Number of APs in the AP group
Number of WLANs	Number of WLANs in the AP group

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Profile' menu.
3) The AP group list of the selected controller is displayed.
4) You can add or delete an AP Groups by clicking the 'Add'/'Delete' button at the bottom of the screen.

Adding

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Profile' menu.
3) The AP group list of the selected controller is displayed.

4) Click the ‘Add’ button.
5) The information input screen is displayed.
6) Enter AP group information.

Configuring

1) Select a device (controller) to configure in the tree viewer.
2) Select the ‘Configure’ → ‘Controller/Device’ → ‘AP Group’ → ‘Profile’ menu.
3) The selected controller and its AP group list are shown.
4) Click the hyperlink of a ‘Name’ to configure.
5) Enter the settings by referring to the input fields shown below.
   (‘AP Group’ settings of the default AP group only provides configuration for Name, AP count, WLAN count, Location, and Setting status.)
6) Click the 'Set' button to apply the settings.

[AP group]

Item	Description
Name	Name of the AP group profile to configure If it is set as a remote AP group, selects a check box.
Number of APs	Number of APs included in the AP group
Number of WLANs	Number of WLANs set in the AP group
AP application	Select to apply the settings below to all APs added to the group
AP mode	Sets the AP operation mode - General AP: Basic AP mode for user service - Root AP: Backbone AP for repeater service. The UE accesses the repeater AP and then connects to the wired network via the root AP. - Repeat AP: Edge AP for repeater service. This is the actual AP accessed by the UE.
Bridge service	Sets the bridge service function provided in repeater AP mode
UE service	Sets the UE service function provided in root AP mode
Map location	Hyperlinked information of the AP location on the RF map. Click to view the linked RF map.
IP mode	IP configuration mode - DHCP: IP allocation by DHCP - AP Priority: Using the method configured in the AP
Setting status	Administrator setting information (Up, Down) concerning AP operation
Discovery type	Discovery type setting of the controller (AP Followed/APC Referral)
First-third controller names	Shows the order of controllers to be accessed by the AP

[AP list]

Item	Description
Name	Position the AP list to set up at the left side by using the << or >> button.

[WLAN list]

Item	Description
Name	Position the WLAN list to set up at the left side by using the << or >> button.

Deleting

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Profile' menu.
3) The AP group list of the selected controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.11.2 Advanced

This menu is used to process batch setup for the AP groups in a controller.

[Advanced]

Item	Description
Name of AP Group	Name of the AP group
Application to AP	The following items are applied in all APs added in the group if being selected:
Echo Interval (sec.)	Keep-alive interval of the CAPWAP session between AP and controller
Maximum Discovery Interval (sec.)	Maximum waiting time before AP starts controller discovery
Reporting Interval (sec.)	Interval at which the statistical information on WiFi decryption error is reported
Statistical Timer (sec.)	Interval at which the WiFi statistical information is reported
Retransmission interval (sec.)	First retransmission interval of the CAPWAP control packet
Maximum retransmission count	Maximum retransmission count of the CAPWAP control packet
Echo Retransmission Interval (sec.)	Retransmission interval of the CAPWAP keep-alive packet

Item	Description
Maximum Echo Retransmission	Maximum retransmission count of the CAPWAP keep-alive packet

Item	Description
Telnet	Whether to use the Telnet service (Enable/Disable), a service port set
SSH	Whether to use the SSH service (Enable/Disable), a service port set
Console	Whether to use the console service (Enable/Disable)
DTLS	Configures Datagram Transmission Layer Security (DTLS) for data security (Disable/Control-Only/Enable).
LED	Sets the type of use of LED (On/Off/Off-Time). - If Off-Time is selected, necessary to set a time.
POE Type	Sets a POE type (802.3at/802.3af/Auto).

[VLAN]

Item	Description
VLAN Supported	Sets the VLAN of the AP supported (Enabled/Disabled).
NATIVE VLAN ID	Sets a NATIVE VLAN value (if the VLAN supported is enabled, enabled).

Item	Description
Country Code	Country code
Environment	Installation environment - Both - Outdoor - Indoor - Non-country

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘AP Group’ → ‘Advanced’ menu.
3) The AP group list of the selected controller is displayed.

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Advanced' menu.
3) The AP group list of the selected controller is displayed.
4) Click the hyperlink of a 'name' to set up.
5) Enter an advanced setup information item.
   (In case of Default AP Group, VLAN setup is not supported.)
6) Apply the settings by clicking the 'Set' button.

4.1.11.3 802.11a/n/ac

This menu is used to set up the 802.11a/n of a controller.

[802.11a/n/ac]

Item	Description
AP group name	AP group name
Service	Service enable setup (Enable/Disable)
Support	Support Type
Guard Interval -20 MHz	Guard Interval (20 MHz) short/long selection
Guard Interval -40 MHz	Guard Interval (40 MHz) short/long selection
Guard Interval -80 MHz	Guard Interval (50 MHz) short/long selection
Beamforming	Beamforming use of not use (Enable/Disable)
Channel	Set up a channel to use
Channel fix	Channel fix setup (Enable/Disable)
Transmission power	Transmission power setup
Power fix	Power fix setup (Enable/Disable)
Bandwidth (MHz)	Bandwidth
Max. connected APs	Max. connected APs
Multi-antenna Mode	Configures a multi-antenna mode (Dynamic/Static).

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP group' → '802.11a/n' menu.
3) The AP Group list of the selected controller is displayed.

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP group' → '802.11a/n' menu.
3) The AP Group list of the selected controller is displayed.
4) Click the hyperlink of a 'name' to set up.
5) Enter a setup information item.
6) Apply the settings by clicking the 'Set' button.

4.1.11.4 802.11b/g/n

This menu is used to set up the 802.11b/g/n of a controller.

[802.11 b/g/n]

Item	Description
AP group name	AP group name
Service	Service enable setup (Enable/Disable)
Support	Support Type
Guard Interval -20 MHz	Guard Interval (20 MHz) short/long selection
Guard Interval -40 MHz	Guard Interval (40 MHz) short/long selection
Beamforming	Beamforming use of not use (Enable/Disable)
Channel	Set up a channel to use
Channel fix	Channel fix setup (Enable/Disable)
Transmission power	Transmission power setup
Power fix	Power fix setup (Enable/Disable)
Max. connected APs	Max. connected APs
Multi-antenna Mode	Configures a multi-antenna mode (Dynamic/Static).

Retrieving

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP group' → '802.11b/g/n' menu.
3) The AP Group list of a selected controller is displayed.

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP group' → '802.11b/g/n' menu.
3) The AP Group list of a selected controller is displayed.
4) Click the hyperlink of a 'name' to set up.

5) Enter a setup information item.
6) Apply the settings by clicking the 'Set' button.

4.1.11.5 Remote AP group

If the APs are located in an area where the APC is not located, those APs must be classified into a separate group for service. The APC can manage the APs in another area by grouping them into a remote AP group.

In the menu, the operator can configure the below information and the APs in the remote AP group operate based on the same configuration.

[Advanced Options]

Item	Description
Backup RADIUS Server 1	First RADIUS server IP address or internal
Backup RADIUS Server 2	Second RADIUS server IP address or internal
Backup RADIUS Server 3	Third RADIUS server IP address or internal
Range	Operation range of the Send to APs button (All/ACL Profile Only)

Item	Description
ACL Profile Name	Name of the ACL profile to use
Application to AP	Selects the range to be applied to an AP added in the group.

[Tunnel Forwarding]

Item	Description
WLAN	WLAN ID to use
Split Tunnel ACL	Name of the ACL profile to use

[Local Bridging Forwarding]

Item	Description
WLAN	WLAN ID to use
VLAN ID	VLAN ID to use
ACL	Name of the ACL profile to use
Pre-Authentication ACL	Name of the pre-authentication ACL profile to use

Retrieving

1) Select the equipment (controller) to view in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Remote AP Group' menu.
3) The list of remote AP groups of the selected controller appears.

Setup

1) Select the equipment (controller) to set in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'AP Group' → 'Remote AP Group' menu.
3) The list of remote AP groups of the selected controller appears.
4) Click the hyperlink of the 'Name' to be set.
5) Enter the settings.
6) Click the 'Set' button to apply the settings.

4.1.12 Mobility

4.1.12.1 Cluster

An operator can modify the cluster related settings of a specific controller for a cluster group and enable/disable a service.

[Cluster Information]

Item	Description
Cluster name	Cluster name
Connection maintaining interval (sec)	Packet transmission interval for connection status check
Connection maintaining re-attempt times	Packet retransmission times for connection status check
Service Status	Service enable/disable status

[Cluster]

Item	Description
Cluster ID	Cluster ID
Controller name	Name of the controller in a cluster
MAC address	MAC address
Cluster IP address	Cluster IP address
Synchronization interval	Synchronization time interval
Connection status	Connection status

Setup

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Mobility' → 'Cluster' menu.
3) Set up an item to change on the screen.
4) Save the settings by clicking the 'Set' button.

4.1.13 Management

4.1.13.1 System Information

The System Information menu is used to retrieve or set up the basic information of a selected controller.

The modifiable information is shown below:

Item	Description
Name	Controller name
Location	Physical location of the controller
Contact	Name and contact info of the operator and responsible person
Operation time	Operation time recorded since initial system operation
Description	Brief description of the system

Configuring Information

1) Select a controller to retrieve in Tree Viewer or the controller list table.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'System Information' menu.
3) Modify the necessary items.
4) Save the settings by clicking the 'Set' button.

4.1.13.2 SNMP

The SNMP menu is used to retrieve or set up the SNMP related information of a device registered in WEM.

The SNMP setup information is shown below:

[Community]

Item	Description
Community	SNMP community name
Access type	Access type (Read Only/Read Write)

Item	Description
IP version	IP address version (IPv4/IPv6)
IPv4 address	IPv4 address
IPv6 address	IPv6 address
Netmask	Netmask

[User]

Item	Description
Name	User name for SNMP v3
Access type	Access type (Read Only/Read Write)
Authentication protocol	Protocol to be used for SNMP v3 authentication - Message-Digest algorithm 5 (MD5) - Secure Hash Algorithm (SHA)
Authentication key	Authentication key to be used for SNMP v3 authentication
Private protocol	Private protocol to be used for SNMP v3 authentication - NONE: Encryption protocol is not applied. - Data Encryption Standard (DES) - Advanced Encryption Standard (AES)
Private key	Private key to be used for SNMP v3 authentication

[Trap]

The trap menu is used to retrieve or set up the trap server registered in a controller device.

The trap setup information items are shown below:

Item	Description
Community name	SNMP community name
Trap version	SNMP trap version information
IP version	IP address version
IPv4 address	Manager IPv4 address
IPv6 address	Manager IPv6 address
Port	Port number

Retrieve community

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The community list of the controller is displayed.
4) You can add or delete a community by clicking the ‘Add’/‘Delete’ button at the bottom of the screen.

Add community

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The community list of the controller is displayed.
4) Click the ‘Add’ button.
5) Enter information into the community information input pop-up screen.
6) Save the settings by clicking the ‘Set’ button.

Delete community

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The community list of the controller is displayed.
4) Select the first checkbox of each item to delete.
5) Delete the item by clicking the ‘Delete’ button.

Retrieve user

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The user list of the controller is displayed.
4) You can add or delete a user by clicking the ‘Add’/‘Delete’ button at the bottom of screen.

Add user

1) Select an equipment (controller) to add in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The user list of the controller is displayed.
4) Click the ‘Add’ button.
5) Enter user information.
7) Save the settings by clicking the ‘Add’ button.

Delete user

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘SNMP’ menu.
3) The user list of the controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the ‘Delete’ button to delete the selected items.

Retrieve trap

1) Select an equipment (controller) to retrieve in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'SNMP' menu.
3) The trap list of the controller is displayed.
4) You can add or delete a trap by clicking the 'Add'/'Delete' button at the bottom of the screen.

Add trap

1) Select an equipment (controller) to add in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'SNMP' menu.
3) The trap list of the controller is displayed.
4) Click the 'Add' button.
5) Enter trap information.
7) Save the settings by clicking the 'Add' button.

Delete trap

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'SNMP' menu.
3) The trap list of the controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.13.3 DNS

The DNS menu is used to retrieve and set up the information related to the DNS server and relay service configured in a controller.

- Configuring DNS Client: Set up external DNS servers that a controller refers to
- Configuring DNS Relay: Set up a cache-containing relay that answers DNS requests from wireless terminals

The DNS setup items are shown below:

[Client]

Item	Description
Service	DNS service (Enable/Disable)
First DNS address	First DNS server IP address
Second DNS address	Second DNS server IP address
Third DNS address	Third DNS server IP address
Query Interval	DNS Query Interval of URL define at ACL

[Relay]

Item	Description
Cache size	Size of the cache to be used for DNS relay

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'DNS' menu.
3) The DNS server setup status of the controller is displayed.
4) Enter information by referring to a DNS setup item.
5) Save the settings by clicking the 'Set' button.

4.1.13.4 NTP

The NTP menu is used to retrieve and set local time synchronization related information.

[NTP Client]

The NTP client setup information is shown below:

Item	Description
Polling Service	NTP client service set up status
Polling Interval	Synchronization time interval of NTP client

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'NTP' menu.
3) The setup status is displayed.
4) Select enable/disable in 'Service'.
5) Set up the synchronization time interval of the NTP client in 'Interval'.
6) Save the settings by clicking the 'Set' button.
7) Set up the information of the NTP server where NTP clients will be connected by clicking the 'Add' button.
   The setup items of the NTP server are shown below:

항목	설명
Type	NTP server type(IP Address, Domain)
Server IP Address	IP address of NTP server (If the domain is selected)
Server Domain Name	Domain name of NTP server (If the IP adress is selected)

Delete NTP server

1) Select an equipment (controller) to delete in the tree viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'NTP' menu.
3) The NTP server list of the controller is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

[NTP Server]
This menu is used to set up the internal NTP server status (enable/disable) of a controller. The setup information items are shown below:

Item	Description
Service	NTP server service setup status (Enable/Disable)

[AP NTP]
The NTP client setup information relating to the AP are shown below:

Item	Description
Mode	Time setting mode of AP (TimeStamp/NTP Type)
Stamp Interval	Interval at which the APC transmits its time to the AP
NTP Polling Interval	Interval at which the AP receives time information from the NTP server

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'NTP' menu.
3) The setup status is displayed.
4) Set up the synchronization time interval of the NTP client in 'Interval'.
6) Save the settings by clicking the 'Set' button.
7) Set up the information of the NTP server where AP NTP clients will be connected by clicking the 'Add' button.
   The setup items of the NTP server are shown below:

Item	Description
No	Number
AP NTP server	URL address of the NTP server which will bring connection time information from the AP

Delete AP NTP server

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'NTP' menu.
3) The AP NTP server list is displayed.
4) Select the first checkbox of each item to delete.
5) Click the 'Delete' button to delete the selected items.

4.1.13.5 System Log

The 'System Log' menu is used to set up enable/disable of a system log and its level.

[System log mode]
The system log mode setup items are shown below:

Item	Description
Mode	System log (Enable/Disable)
Level	Log level of system log (Information/Notice/Warning/Minor/Major/Critical)

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'System' menu.
3) The setup status is displayed.
4) Enter the system log mode setup information.
5) Save the settings by clicking the 'Set' button.

[System log server]
The system log server setup is used to retrieve or set up the system log server of a controller.

The system log mode setup items are shown below:

Item	Description
System log server 1	First system log server IP address
Port 1	User Datagram Protocol (UDP) port number of the first system log server
System log server 2	Second system log server IP address
Port 2	User Datagram Protocol (UDP) port number of the second system log server

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'System' menu.
3) The system log server setup status of the controller is displayed. A maximum of two system log servers can be configured.
4) Click the IP address of the system log server you wish to change the settings of.
5) Enter information by referring to the setup items.
6) Save the settings by clicking the 'Set' button.

4.1.13.6 Service

[Telnet-SSH]
This menu is used to retrieve or set up the information related to the telnet server and SSH server configured in a controller.

The Telnet-SSH setup items are shown below:

Item	Description
Session timeout (sec)	Timeout time when a session is idle
Maximum number of sessions	Maximum number of sessions allowed to connect to a service
Telnet service	Telnet service setup status (Enable/Disable)
Port	Telnet port number
SSH service	SSH server service setup status (Enable/Disable)
Port	SSH port number

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Service' menu.
3) The setup status is displayed.
4) Enter information into the telnet setup item.
5) Save the settings by clicking the 'Set' button.

[FTP]
This menu is used to retrieve or set up the information related to the FTP server configured in a controller.

The setup items of FTP server are shown below:

Item	Description
Service	Service setup status
Port	Port number

Item	Description
ID	User ID
Password	User password

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Service' menu.
3) The setup status is displayed.
4) Enter information into the FTP setup item.
5) Save the settings by clicking the 'Set' button.

[Secure FTP]
This menu is used to retrieve or set up the information related to the secure FTP (secure File Transfer Protocol) server service configured in a controller.

The secure FTP setup items are shown below:

Item	Description
Service	Service setup status
ID	User ID
Password	User password

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Service' menu.
3) The setup status is displayed.
4) Enter information into the secure FTP server setup item.
5) Save the settings by clicking the 'Set' button.

[HTTP]
This menu is used to retrieve or set up the information related to the HTTP (Hypertext Transfer Protocol) server service configured in a controller.

The HTTP setup items are shown below:

Item	Description
Service	Service setup status (Enable/Disable)

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Service' menu.
3) The setup status is displayed.
4) Enter the HTTP server setup item information.
5) Save the settings by clicking the 'Set' button.

[HTTPs]

This menu is used to retrieve or set up the information related to the Hypertext Transfer Protocol over Secure Socket Layer (HTTPs) server service registered in a controller.

The HTTPs setup items are shown below:

Item	Description
Service	Service setup status (Enable/Disable)

Setup

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Service' menu.
3) The setup status is displayed.
4) Enter the HTTPs server setup item information.
5) Save the settings by clicking the 'Set' button.

4.1.13.7 Time

The Time menu is used to set up the local time information that will be used for a controller.

The time information setup information items are shown below:

[Local Time]

Item	Description
Time	Specify time that will be used for the controller.
Time zone	Specify time zone that will be used for the controller.

Setup

1) Select a controller to set up in Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Time' menu.
3) Set up the setup information items.

4) Apply the time settings by clicking the ‘Set’ button.

4.1.13.8 Reboot

The ‘reboot’ menu is used to retrieve or set up the reboot information configured in a controller.

The setup information items are shown below:

[Reboot Setup]

Item	Description
Now	Rebooted immediately.
Elapsed time	Rebooted when a specific amount of time has elapsed
Specific time	Rebooted at a specific time
Schedule cancel	The saved rebooting settings are all cancelled.

Setup

1) Select a controller to reboot in Tree Viewer.
2) Select the ‘Configuration Management’ → ‘Controller/Device’ → ‘Management’ → ‘Reboot’ menu.
3) Set up the reboot items.
4) Execute or reserve reboot by clicking the ‘Set’ button.

4.1.13.9 Backup/Recovery

The ‘Backup/Recovery’ menu is used to back up the following information of a controller or apply the saved settings to the controller.

- Setup information
- Controller debugger file
- Controller log file

The backup/recovery information items are shown below:

[Backup/Recovery]

Item	Description
Backup/Recovery	Specify the item of a file to back up or recover. - Config File Backup - Config File Restore - APC Debug File Backup - APC Log File Backup
File name	Specify the name of a file to back up or recover.

Setup

1) Select a controller to set up in Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Backup/Recovery' menu.
3) Set up the setup information items.
4) Apply Backup/Recovery by clicking the 'Set' button.

4.1.13.10 Threshold

This is used to retrieve and set up the threshold of the CPU occupancy rate and memory usage configured in a controller.

[CPU Usage Rate]

Item	Description
Threshold	CPU usage rate threshold which will generate an alarm

[Memory Usage]

Item	Description
Threshold	Memory usage threshold which will generate an alarm

Configure threshold

1) Select an equipment (controller) to set up in the Tree Viewer.
2) Select the 'Configuration Management' → 'Controller/Device' → 'Management' → 'Threshold' menu.
3) The setup status is displayed.
4) Modify each threshold.
5) Save the settings by clicking the 'Set' button.

4.2 AP

4.2.1 AP summary information

The AP summary information menu is used to retrieve the list of all the APs registered in WEM and the summary information of each AP. The AP summary information screen is shown below.

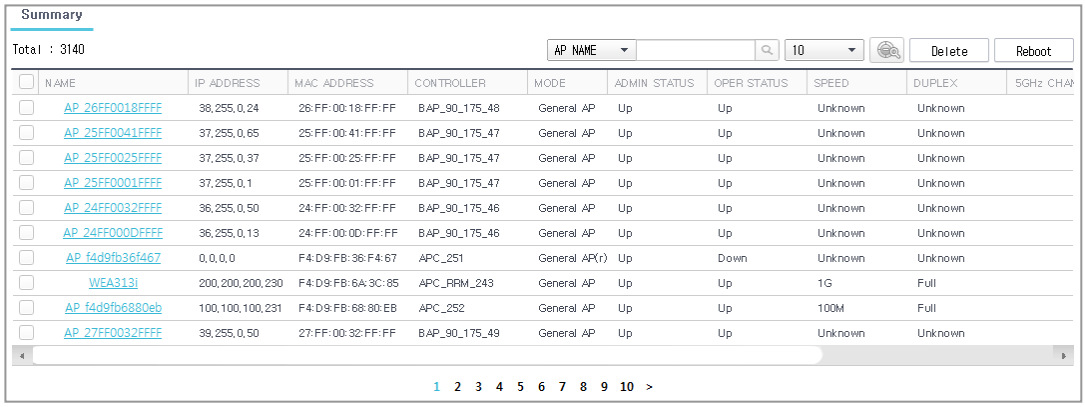


Figure 85. Summary information screen

Each item of the AP summary information screen is shown below.

Item	Description
Name	This is used to provide a hyperlink to the detailed information window of a specific AP by using the name information from an AP.
IP address	IP address of AP WAN interface
MAC address	Physical address of AP WAN interface
Controller	The controller name connceted with a specific AP.
Mode	AP operation mode - General AP: Basic AP mode for user services - Root AP: A backbone AP for the repeater service. The wireless terminal is connected to the repeater AP and then the wired network via the root AP. - Repeater AP: As an edge AP for repeater service, the AP actually connected by the wireless terminal. - Sniffer AP: An AP which does not provide a user service but provides a function of capturing a packet in an air section packet (If the AP mode is a sniffer AP, establish the client IP address.) - Relay AP: An AP connecting the repeater AP with the root AP wirelessly
Configuration Status	Information on the operator configuration status for the operation of the AP (Up, Down)
Operating Status	Information on actual operating status of the AP (Up, Down)
Ethernet Speed (MBPS)	Information on the status of the link connection speed

Item	Description
Ethernet Duplex	Information on the link connection mode of AP
5 GHz channel	Information on 5 GHz channel in use by the AP
2.4 GHz channel	Information on 2.4 GHz channel in use by the AP
Radio Base MAC	Information on the base MAC address allocated to the WLAN interface
Model	AP model name

Retrieving

1) Select the 'Configuration Management' → 'AP' menu.
2) The list of configurable APs is displayed on the screen.

Search condition setup

You can retrieve the information of a particular AP by clicking the search condition setup button ( ) on the AP summary information screen. The available search conditions are shown below.

- Controller name
- AP Mode
- Setup status
- Operation status
- Ethernet Speed (MBPS)
- Ethernet Duplex

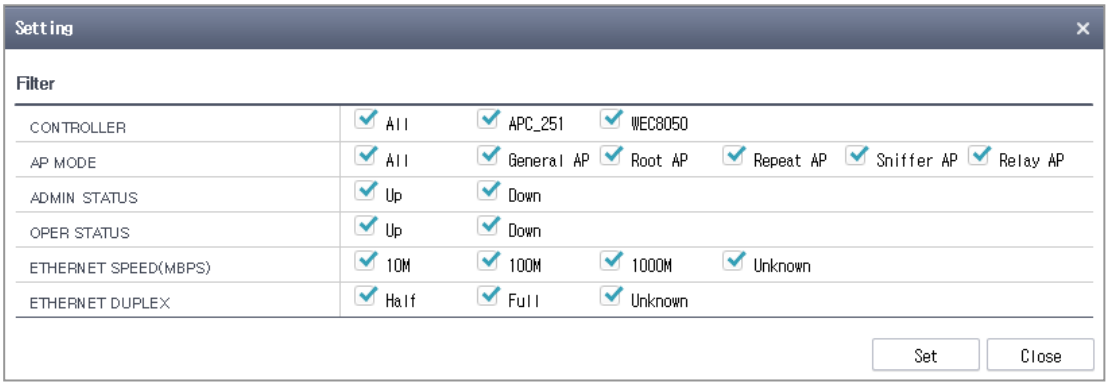


Figure 86. Search condition setup screen

Delete

You can delete a selected AP by clicking the 'Delete' icon in the top right-hand corner of the AP summary information screen.

Reboot

You can reboot a selected AP by clicking the 'Reboot' icon in the top right-hand corner of the AP summary information screen.

4.2.2 System

In the AP summary information screen that appears when you select an AP in Configuration Management, you can set up a specific AP by clicking the hyperlink of the AP.

4.2.2.1 General

You can retrieve or set up the following item when you select an AP.

Item	Description
AP name	Set up AP name.
Group name	Information of the group to which the AP belongs
AP Mode	Sets the AP operating mode. - General AP: Basic AP mode for user services - Root AP: A backbone AP for the repeater service. The wireless terminal is connected to the repeater AP and then the wired network via the root AP. - Repeater AP: As an edge AP for repeater service, the AP actually connected by the wireless terminal. - Sniffer AP: An AP which does not provide a user service but provides a function of capturing a packet in an air section packet - Relay AP: An AP connecting the repeater AP with the root AP wirelessly
Bridge service	Sets the bridge service function provided in repeater AP mode
UE service	Sets the UE service function provided in root AP mode
Client IP address	Client IP setting in Sniffer AP mode
MAC address	Physical address of the AP WAN interface
Map Location	As hyperlink information for the location on the RF map of the AP. Click the link to immediately move to the concerned RF map.
Location	Necessary to explain the location of the equipment and to be configured by the operator
IP Mode	IP Setting Mode - DHCP: IP is allocated to DHCP. - AP Priority: Under the method designated to the APs. - Static IP: Static IP used
Discovery Type	Sets the controller discovery type (AP Followed/APC Referral).
Configuration Status	Information on the operator configuration status for the operation

Item	Description
	of the AP (Up, Down)
Operating Status	Actual operating status of the AP (Up, Down)
Names of the First to Third Controllers	Shows the order of controllers to which the APs will be connected.

Setup

1) Go to 'Configuration Management' → 'AP' menu.
2) Click the hyperlink of the AP to be set in the list of APs on the Summarized AP Information displayed on the screen.
3) Select 'System' → 'General' in the display screen.
4) The item that can be set is displayed on the screen and the value of the field that can be changed is modified.
5) Click the 'Set' button to apply the settings.

4.2.2.2 Advanced

You can retrieve or set up the following item when you select an AP.

[Advanced]

Item	Description
AP name	AP name
Echo interval (sec)	CAPWAP session keep-alive interval between AP and controller
Maximum discovery interval (sec)	Maximum waiting time before an AP starts controller discovery
Report interval (sec)	Interval of reporting Wi-Fi decryption error statistical information
Statistics timer (sec)	Interval of reporting Wi-Fi statistical information
Retransmission interval (sec)	First retransmission interval of CAPWAP control packet
Maximum retransmission times	Maximum retransmission times of CAPWAP control packet
Echo retransmission interval (sec)	Retransmission interval of CAPWAP keep-alive packet
Maximum echo retransmission	Maximum retransmission times of CAPWAP keep-alive packet
Telnet	This is used to set up telnet service, usage and port information.
SSH	This is used to set up SSH service, usage and port information.
Console	Sets whether to use the console service.
DTLS	DTLS usage setup (Disable/Control-Only/Enable)
LED	Set up LED ON/OFF and OFF time.
POE Type	Sets a POE type (802.3at/802.3af/Auto).
VLAN support	Set up VLAN support (Enable/Disable).

Item	Description
NATIVE VLAN ID	Set up NATIVE VLAN ID
Country Code	Device country setup status
Environment	Device installation environment - Both - Outdoor - Indoor - Non-country
Edge AP	Edge AP setup (Enable/Disable)

[Time]

Item	Description
Time	Time zone setup per country/city

[Log Backup]

This provides the log backup hyperlink for an AP. When clicking the hyperlink, the log backup operation is immediately started.

Setup

1) Go to 'Configuration Management' → 'AP' menu.
2) Click the hyperlink of the AP to be set in the list of APs on the Summarized AP Information displayed on the screen.
3) Select 'System' → 'Advanced' in the display screen.
4) The item that can be set is displayed on the screen and the value of the field that can be changed is modified.
5) Click the 'Set' button to apply the settings.

4.2.3 Radio

In the AP summary information screen that appears when you select an AP in Configuration Management, you can set up radio for a specific AP by clicking the hyperlink of a specific AP name.

4.2.3.1 802.11a/n/ac

This menu is used to retrieve or set up 802.11a/n/ac related community.

[General]

Item	Description
AP name	AP name information
Service	Sets whether to activate the service.
Channel	Set up a radio channel to use.
Channel fix	Channel fix setup (Enable/Disable)
Transmission power	Set up transmission power level.
External antenna gain	Sets the gain value of the external antenna.
Power fix	Power fix setup (Enable/Disable)
Maximum allowed number of terminals	Set up maximum allowed number of terminals.
Multi-antenna mode	Configures a multi-antenna mode (Dynamic/Static).

[Operation Type]

Item	Description
Supported	802.11n/ac support enable/disable

Setup

1) Select the 'Configuration Management' → 'AP' menu.
2) In the AP list of the AP summary information displayed on a screen, click the AP hyperlink to set up.
3) In the output screen, select 'radio' → '802.11a/n/ac'.
4) The configurable items are displayed on a screen and then modify the value of a field that can be modified.
5) Save the settings by clicking the 'Set' button.

4.2.3.2 802.11b/g/n

This menu is used to retrieve or set up 802.11b/g/n related community.

[General]

Item	Description
AP name	AP name information
Service	Sets whether to activate the service.
Channel	Set up a radio channel to use.
Channel fix	Channel fix setup (Enable/Disable)
Transmission power	Set up transmission power level.
Power fix	Power fix setup (Enable/Disable)
External antenna gain	Sets the gain value of the external antenna.
Maximum allowed number of terminals	Set up maximum allowed number of terminals.
Multi-antenna mode	Configures a multi-antenna mode (Dynamic/Static).

[Operation Type]

Item	Description
Supported	802.11n support enable/disable

Setup

1) Select the ‘Configuration Management’ → ‘AP’ menu.
2) In the AP list of the AP summary information displayed on a screen, click the AP hyperlink to set up.
3) In the output screen, select ‘radio’ → ‘802.11b/g/n’.
4) The configurable items are displayed on a screen and then modify the value of a field that can be modified.
5) Save the settings by clicking the ‘Set’ button.

4.2.4 Remote AP

In the AP summary information screen that appears when you select an AP in Configuration Management, you can set up radio for a specific AP by clicking the hyperlink of a specific AP name.

4.2.4.1 General

This menu is used to retrieve or set up remote AP-related items.

[General]

Item	Description
Name of AP	Name of the AP now set
Group Name	Name of the group where APs are added
ACL Profile Name	Name of the ACL profile set
Range	Operation range of the Send to APs button (All/ACL Profile Only)

[Tunnel Forwarding]

Item	Description
WLAN	WLAN ID to use
Split Tunnel ACL	Split tunnel ACL to use

[Local Bridging Forwarding]

Item	Description
Number	Remote AP serial number
WLAN	WLAN ID to use
VLAN ID	VLAN ID to use
ACL	ACL profile name to use
Pre-authenticated ACL	Pre-authenticated ACL profile name to use

Retrieving

1) Go to ‘Configuration Management’ → ‘AP’ → ‘Select AP List’ → ‘Remote AP’ menu.
2) The remote AP configurable item is displayed on the screen.
3) Click the ‘Add’ or ‘Delete’ button on the bottom of the screen to add or delete the setting.

Setup

1) Go to ‘Configuration Management’ → ‘AP’ → ‘Select AP List’ → ‘Remote AP’ menu.
2) The remote AP configurable item is displayed on the screen.
3) Select the number and then the remote AP setup screen where the information can be changed appears.
4) Change the item.
5) Click the ‘Set’ button to save the settings.

Adding

1) Go to ‘Configuration Management’ → ‘AP’ → ‘Select AP List’ → ‘Remote AP’ menu.
2) The remote AP configurable item is displayed on the screen.
3) Click the ‘Add’ button.
4) Enter the information on the pop-up information entry screen.
5) Click the ‘Set’ button to save the settings.

Deleting

1) Select the ‘Configuration Management’ → ‘AP’ → ‘Select AP List’ → ‘Remote AP’ menu.
2) The list of remote APs is displayed on the screen.
3) Select the checkbox at the most front of the item to delete.
4) Delete an item by clicking the ‘Delete’ button.

4.3 Mobility Group

4.3.1 Cluster Lists

'Cluster Lists' menu provides to display the cluster group list. User can modify the information by selecting the Cluster list

The descriptions of Cluster List parameters are as follows:

Parameter	Description
CLUSTER NAME	Name of the Cluster List
KEEP ALIVE INTERVAL (sec)	Keep alive interval
KEEP ALIVE RETRY COUNTs	Keep alive retry counts

Modify Cluster List

1) Select the APC (controller) on the Tree Viewer.
2) Go to 'Configuration' → 'Mobility Group' to open Mobility Group Window.
3) Enter the required parameters to change the setting.
4) Click 'Set' button to save the settings.

4.4 Controller Template

4.4.1 Template

The controller template is a function of storing a set of specific settings in one file and selecting controllers to apply all the settings and applying them. It allows frequently used features to be stored and applied in a lump. This function can reduce a task of setting every controller by selecting several controllers at the same time and applying settings in a lump.

The controller template runs in the 'Configuration Management' → 'Controller Template' menu

Figure 87. Template List Screen

Adding

For all template items, the Add button is provided. When you click the Add button on the template list screen (Fig. 88), you can set and save a configuration group with a specific feature. Click the 'Save' button on the adding screen and then settings are saved under the template name as the required input element. Press the 'Close' button on the adding screen and then the screen returns to the template list screen.

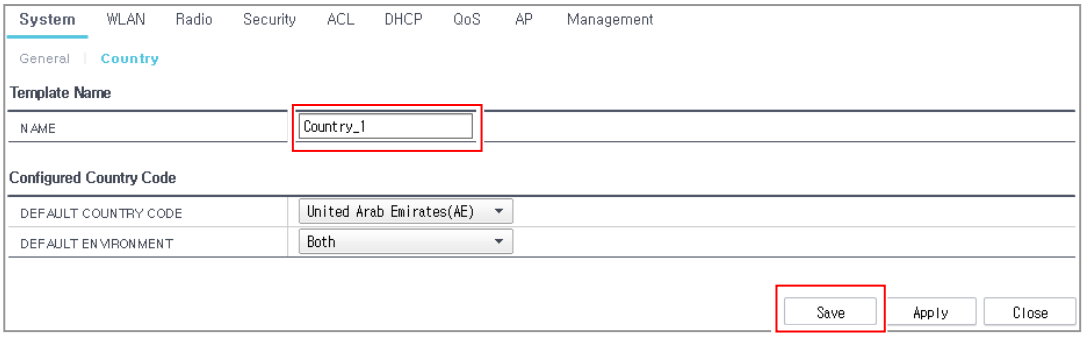


Figure 88. Template Adding Screen

Changing

To change a specific template item, click the name of the template you want to change on the template list screen. In the case, the screen same as the 'Adding' screen appears and you can check the pre-set value. Change the information and click the 'Save' button and then the information is changed to the template and then saved.

Deleting

Select the check box of the item you want to delete on the template list screen and click the 'Delete' button on the bottom.

Application

To apply a specific template, press the 'Apply' button. The 'Apply' button is on the template list screen and the 'Add' and 'Change' screens. To apply on the template list screen, select the check box of the item to apply in the list and press the 'Apply' button (Fig. 90).
To apply the 'Adding' or 'Changing' screen, click the name of the template in the template list and select the check box of the module in the screen you want to apply before pressing the 'Apply' button (Fig. 91). If there is no check box, all are applied.
Among them for ACL, OS Aware of DHCP, AP, Management Controller Account, SNMP, and NTP templates,
select the check box on the line you want to apply in the content added in the table and press the 'Apply' button (Fig. 92).
Press the 'Apply' button and a new window appears (Fig. 92). The left of the window is in a tree form and you can select several groups or controllers. Select the checkbox of the controller you want to apply and press the 'Apply' button at the bottom right to apply to each selected controller sequentially and then whether to succeed or fail in the application to each controller is displayed in the progress bar.

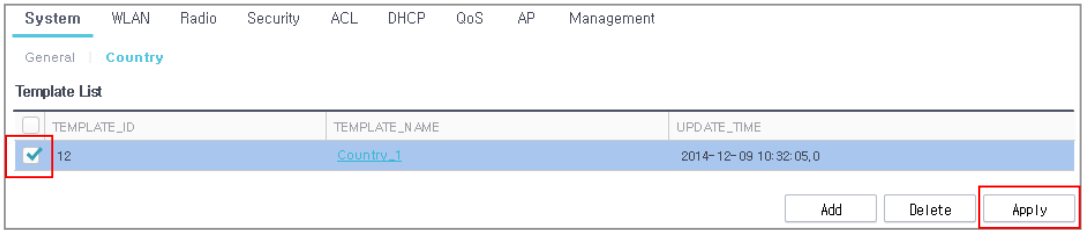


Figure 89. Application on Template List Screen

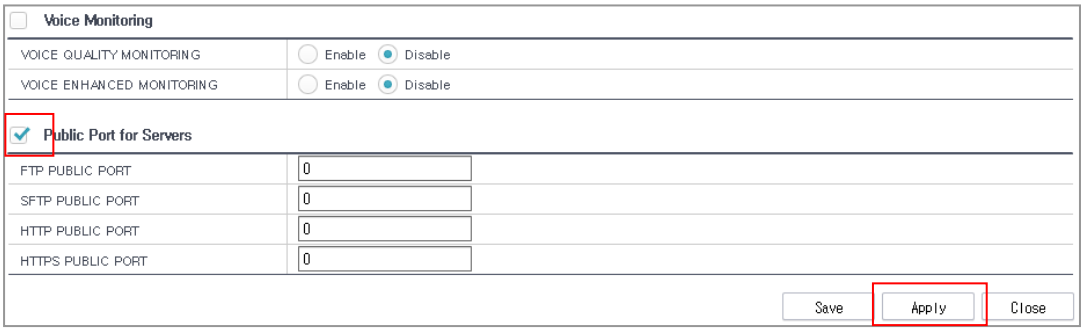


Figure 90. Application on Adding and Changing Screens

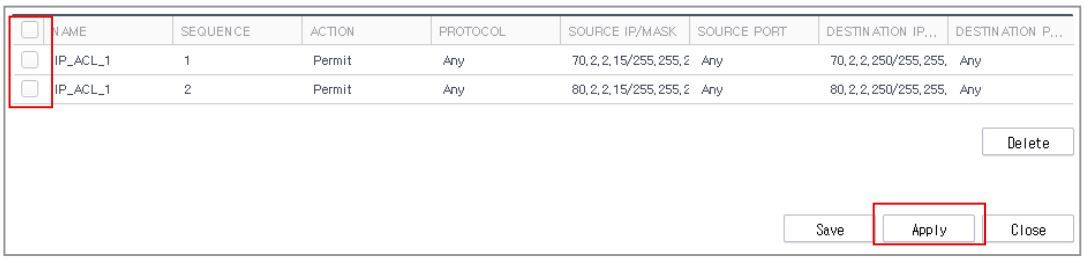


Figure 91. Application on Screens of Adding and Changing Templates with Table

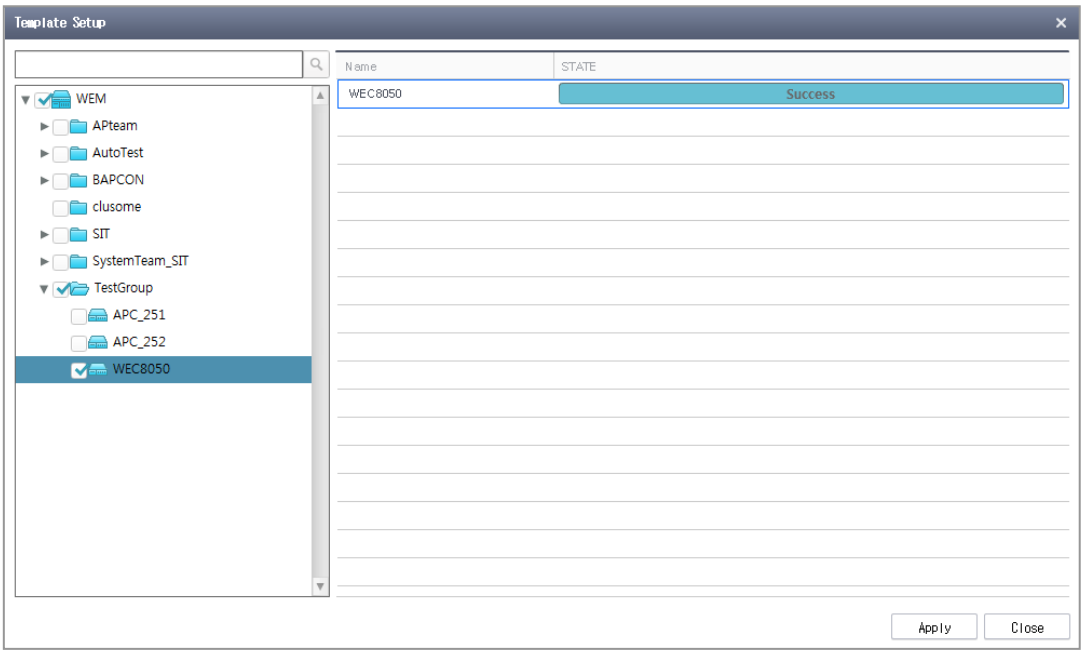


Figure 92. Controller Selection and Application

4.4.2 System

4.4.2.1 General

The 'System' → 'General' menu of the controller template provides a function of setting general information relating to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Repeater Service]

Item	Description
Service	Repeater service enabled or disabled

[SIP ALG]

Item	Description
SIP ALG (VoIP AWARE)	Activates or deactives the SIP ALG (VoIP AWARE) service.
Sending CAC Limit Error Response Message	Activates or deactivates the error response function.
Detecting Long Time Call	Activates or deactivates the long time call detection function.
No Response Call-based Time (sec.)	Configures the reference time to process as no response call.
Long Time Connected Call-based Time (sec.)	Configures the reference time to determine as a long time connected call.
SIP Monitoring Port 1	Configures port 1 for monitoring SIP ALG.
SIP Monitoring Port 2	Configures port 2 for monitoring SIP ALG.
SIP Monitoring Port 3	Configures port 3 for monitoring SIP ALG.
SIP Monitoring Port 4	Configures port 4 for monitoring SIP ALG.
SIP Monitoring Port 5	Configures port 5 for monitoring SIP ALG.

[Audio Call Monitoring]

Item	Description
Voice Quality Monitoring	Activates or deactivates a function of monitoring the voice quality of the system.

Item	Description
Improved Voice Quality Monitoring	Activates or deactivates a function of monitoring the improved voice quality of the system.
FTP Public Port Number	Sets FTP public port number.
SFTP Public Port Number	Sets SFTP public port number.
HTTP Public Port Number	Sets HTTP public port number.
HTTPS Public Port Number	Sets HTTPS public port number.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.2.2 Country

The 'System' → 'Country' menu of the controller template provides a function of setting a country code and an environment to be applied in the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Configured Country Code]

Item	Description
Basic Country Code	Designates the country to be applied to the controller.
Basic Environment	Designates a controller operating environment. (indoor, outdoor, both, non-country)

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.3 WLAN

4.4.3.1 Profile

The 'WLAN' → 'Profile' menu of the controller template provides a function of setting information relating to the WLAN to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Name	Profile Name
SSID	Service set identifier
Interface Group	Name of the interface group
Radio	Frequency band (2.4 GHz/5 GHz)
CAPWAP Tunnel Mode	Configures a CAPWAP tunnel mode.
SSID Hide	Configures SSID hide.
AAA Override	Activates or deactivates the AAA override function.
No. of Maximum UEs Connected	Configures number of maximum UEs connected.
Guest Service	Service support or not.

[Security Layer 2]

Item	Description
Layer 2 Security Type	Sets the Layer 2 security function type (NONE, Static WEP, 802.1x (Dynamic WEP), Static WEP+802.1x (Dynamic WEP), WPA+WPA2).
MAC Authentication	Configures the use of the MAC authentication.
MAC Filter	Configures a MAC filter.

[Security Layer 3]

Item	Description
Web Policy	Whether to use a web policy
Web authentication	Web authentication
Web Authentication upon Failure in MAC Authentication	Upon failure in MAC authentication, uses web authentication.
Web Pass-through	Moves to a specific address all the time when the user wants to use the web.
Conditional Web Redirection	Conditional redirection
One-time redirection	One-time redirection
Pre-authenticated ACL	ACL applied before the guest is authenticated
Overriding Redirect URL	Configures the overriding redirect URL status (enable/disable).
URL	URL to which the guest is redirected

[Security RADIUS]

Item	Description
Fallback Interval	Configures the fallback period.
Charging Interval	Configures the charging period.
Authentication Server	Whether to perform the role as an authentication server
First to Third Authentication Servers	Configures an authentication server address.
Accounting Server	Whether to perform the role as an accounting server
First to Third Accounting Servers	Configures an accounting server address.

[WLAN Advanced Options]

Item	Description
ACL Rule	Name of the ACL rule
Whether to Disallow Static Address	Configures whether to receive the IP address by using the DHCP.
DHCP Override	Configures whether to use the DHCP override function.
DHCP Server	Enters the address of the DHCP server (Configures when the DHCP override is enabled).
WMM	Sets the WMM mode.
DTIM	Beacon DTIM: 1~255 (default: 1)
Terminal Timeout (sec.)	Sets the idle timeout of the UE.
AMPDU	Sets AMPDU.

Item	Description
VoIP Failure Detect	Sets the detection of communication failure.
Band Steering	Sets band steering.
Load Balancing	Sets load balancing.
Threshold	Sets threshold setting.
Maximum Denial Count	Sets the maximum denial count.
Multicast to Unicast	Whether to use the multicast function (Enable/Disable)
Discarding Multicast Packet	Whether to use the function of discarding a multicast packet (Enable/Disable)
REJECT PROBE Requesting Mode	Selects the requesting mode (RSSI, Time, Max. Allowed Stations).

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4 Radio

4.4.4.1 802.11 a/n/ac

The ‘Radio’ → ‘802.11a/n/ac’ menu of the controller template provides a function of configuring information relating to 802.11a/n/ac to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Service]

Item	Description
Service	Sets whether to activate or deactivate the service.

[General]

Item	Description
Bandwidth (MHz)	Sets the bandwidth.
Beacon Interval (TUS)	Sets the Beacon interval.
Fragmentation Threashold (Byte)	Fragmentation threashold
Voice Control Optimization	Whether to use the voice control optimization function
Maximum Connected Client Count	Maximum number of connectible clients

[Data Transmission Rate]

Item	Description
6~54 Mbps	Whether to support data transmission rate each (Disable/Supported/Basic).

[Configuring Call Admission]

Item	Description
Voice Management Control Support	Whether to use CAC
Maximum Number of Calls	Maximum number of calls
Number of Reserved Handover Calls	Number of reserved H/O calls
MINOR Alarm Threshold	The minor level threshold at which an alarm occurs

Item	Description
MAJOR Alarm Threshold	The major level threshold at which an alarm occurs

[UE Admission Control]

Item	Description
UE Extraction Control	Whether to use the UE extraction control
Reconnection Count Threshold	Sets the reconnection count threshold.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.2 QoS(a/n)

The 'Radio' → 'QoS (a/n)' menu of the controller template provides a function of configuring information relating to QoS (a/n) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Wired QoS]

Item	Description
Profile	Selects a profile.
TAGGING Policy (802.1p)	Sets 802.1p QoS marking (None/User Priority/Default Value).
TAGGING Policy (DSCP)	Sets DSCP QoS marking (Activated with Enable).
TAGGING Policy (External DSCP)	Sets the DSCP item marking of the CAPWAP header (InnerPacket/(Default Value).
TAGGING Policy (Internal DSCP)	Sets the DSCP item marking of the packet coming from the controller and the wireless terminal (No marking/Default Value).
Protocol	QoS protocol (None/802.1p/DSCP)
Voice-802.1p	802.1p QoS value to be used in the voice packet
Voice-DSCP	DSCP QoS value to be used in the voice packet
Video-802.1p	802.1p QoS value to be used in the video packet
Video-DSCP	DSCP QoS value to be used in the video packet

Item	Description
BEST EFFORT-802.1p	802.1p QoS value to be used in the best effort packet
BEST EFFORT-DSCP	DSCP QoS value to be used in the best effort packet
Background-802.1p	802.1p QoS value to be used in the background packet
Background-DSCP	DSCP QoS value to be used in the background packet

[Wireless QoS]

Item	Description
Profile	Selects a profile.
Voice-802.1p	802.1p QoS value to be used in the voice packet
Voice-DSCP	DSCP QoS value to be used in the voice packet
Video-802.1p	802.1p QoS value to be used in the video packet
Video-DSCP	DSCP QoS value to be used in the video packet
BEST EFFORT-802.1p	802.1p QoS value to be used in the best effort packet
BEST EFFORT-DSCP	DSCP QoS value to be used in the best effort packet
Background-802.1p	802.1p QoS value to be used in the background packet
Background-DSCP	DSCP QoS value to be used in the background packet

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.3 802.11h(a/n)

The 'Radio' → '802.11h (a/n)' menu of the controller template provides a function of configuring information relating to 802.11h to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[802.11h]

Item	Description
Transmission Power Limitation	Sets the signal strength limitation value.
Channel Switching Notification	Activates or deactivates channel switching notification.
Limitation Mode	Whether to use a limitation mode

Item	Description
Number of Channel Switching	Sets the number of channel switching.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.4 802.11n (a/n/ac)

The 'Radio' → '802.11n (a/n/ac)' menu of the controller template provides a function of configuring information relating to 802.11n (a/n/ac) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Global MCS]

Item	Description
Supported	Selects a supported type.
Configuring HT (802.11n) Rx MCS	Configures HT (802.11n) Rx-related MCS.
Configuring VHT (802.11ac) MCS	Configures VHT (802.11ac)-related MCS.

[Operating Type]

Item	Description
Guard Interval-20 MHz	Selects whether the guard Interval (20 MHz) is short or long.
Guard Interval-40 MHz	Selects whether the guard Interval (40 MHz) is short or long.
Guard Interval-80 MHz	Selects whether the guard Interval (50 MHz) is short or long.
Beamforming	Whether to use beamforming

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.5 Radio Resource Management (a/n)

The 'Radio' → 'Radio Resource Management (a/n)' menu of the controller template provides a function of configuring information relating to RRM (a/n) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Radio Resource Management]

Item	Description
Status	Activates or deactivates the radio resource management function.
RF Group Name	Sets the name of RF group.

[Dynamic Power Management]

Item	Description
Status	Activates or deactivates the dynamic power management function.
RSSI Threshold (dBm)	Sets the RSSI threshold of the dynamic power management operation.
Scanning Interval (sec.)	Sets the interval of viewing the power status information.
Minimum Transmission Power	Sets the minimum transmission power standard.
Maximum Transmission Power	Sets the maximum transmission power standard.

[Selecting Dynamic Channel]

Item	Description
Status	Activates or deactivates the function of selecting a dynamic channel.
Scanning Interval (sec.)	Sets the interval of viewing the power status information.
Channel Usage Rate Threshold (%)	Sets the channel usage rate threshold and the internal usage rate threshold.
Interference Source Grade Threshold (%)	Sets the interference source grade threshold.

Item	Description
Delayed Channel Change	Whether to use the delayed channel change
Recognition Option	Sets whether to use the voice, traffic, and station recognition options and the number of stations.
Anchor Starting Time	Sets the start time of the anchor.
Anchor End Time	Sets the end time of the anchor.
Country	Not a real set value but an option to show the DSC channel on the bottom
DCS Channel	Sets the DCS channel.

[Coverage Hole Detection Control]

Item	Description
Status	Activates or deactivate the coverage hole detection function.
Collecting Statistics	Activates or deactivates the use of collecting statistics.
Trap Warning Message Notification	Activates or deactivates trap warning message notification.
Activating Statistics Power Control	Activates or deactivates statistics power control.
Percentage of Failed Client Count	Whether to use the percentage of failed client count
Minimum RSSI Threshold of Voice Traffic (DBM)	Sets minimum RSSI threshold of voice traffic.
Minimum RSSI Threshold of Data Traffic (DBM)	Sets minimum RSSI threshold of data traffic.
Failed Client Count	Sets failed client count.
Time Interval	Sets the time interval.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.6 802.11b/g/n

The ‘Radio’ → ‘802.11b/g/n’ menu of the controller template provides a function of configuring information relating to 802.11b/g/n to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Service]

Item	Description
Service	Sets whether to activate or deactivate the service.

[General]

Item	Description
Beacon Interval	Sets the Beacon interval.
Fragmentation Threashold (Byte)	Fragmentation threashold
Voice Control Optimization	Whether to use the voice control optimization function
Maximum Access Count	Number of stations allowed to be limited to access

[Data Transmission Rate]

Item	Description
1~54 Mbps	Whether to support data transmission rate each (Disable/Supported/Basic).

[Configuring Call Admission]

Item	Description
Voice Optimization	Whether to use CAC
Maximum Number of Calls	Maximum number of calls
Number of Reserved Handover Calls	Number of reserved H/O calls
MINOR Alarm Threshold	Minor level threshold at which an alarm occurs
MAJOR Alarm Threshold	Major level threshold at which an alarm occurs

[UE Admission Control]

Item	Description
UE Extraction Control	Whether to use the UE extraction control
Reconnection Count Threshold	Sets the reconnection count threshold.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.7 QoS (b/g/n)

The 'Radio' → 'QoS (b/g/n)' menu of the controller template provides a function of configuring information relating to QoS (b/g/n) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Wired QoS]

Item	Description
Profile	Selects a profile.
TAGGING Policy (802.1p)	Sets 802.1p QoS marking (None/User Priority/Default Value).
TAGGING Policy (DSCP)	Sets DSCP QoS marking (Activated with Enable).
TAGGING Policy (External DSCP)	Sets the DSCP item marking of the CAPWAP header (InnerPacket/Default Value).
TAGGING Policy (Internal DSCP)	Sets the DSCP item marking of the packet coming from the controller and the wireless terminal (No marking/Default Value).
Protocol	QoS protocol (None/802.1p/DSCP)
Voice-802.1p	802.1p QoS value to be used in the voice packet
Voice-DSCP	DSCP QoS value to be used in the voice packet
Video-802.1p	802.1p QoS value to be used in the video packet
Video-DSCP	DSCP QoS value to be used in the video packet
BEST EFFORT-802.1p	802.1p QoS value to be used in the best effort packet
BEST EFFORT-DSCP	DSCP QoS value to be used in the best effort packet
Background-802.1p	802.1p QoS value to be used in the background packet
Background-DSCP	DSCP QoS value to be used in the background packet

[Wireless QoS]

Item	Description
Profile	Selects a profile.
Voice-802.1p	802.1p QoS value to be used in the voice packet
Voice-DSCP	DSCP QoS value to be used in the voice packet
Video-802.1p	802.1p QoS value to be used in the video packet
Video-DSCP	DSCP QoS value to be used in the video packet

Item	Description
BEST EFFORT-802.1p	802.1p QoS value to be used in the best effort packet
BEST EFFORT-DSCP	DSCP QoS value to be used in the best effort packet
Background-802.1p	802.1p QoS value to be used in the background packet
Background-DSCP	DSCP QoS value to be used in the background packet

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.8 802.11n (b/g/n)

The 'Radio' → '802.11n (b/g/n)' menu of the controller template provides a function of configuring information relating to 802.11n (b/g/n) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Global MCS]

Item	Description
Supported	Selects the supported type.
Configuring HT (802.11n) Rx MCS	Configures HT (802.11n) Rx-related MCS.

[Operating Type]

Item	Description
Guard Interval-20 MHz	Selects whether the guard Interval (20 MHz) is short or long.
Guard Interval-40 MHz	Selects whether the guard Interval (40 MHz) is short or long.
Beamforming	Whether to use beamforming (Enable/Disable)

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.4.9 Radio Resource Management (b/g/n)

The 'Radio' → 'Radio Resource Management (b/g/n)' menu of the controller template provides a function of configuring information relating to RRM (b/g/n) to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Radio Resource Management]

Item	Description
Status	Sets whether to operate the radio resource management function.
RF Group Name	Sets the name of RF group.

[Dynamic Power Management]

Item	Description
Status	Sets whether to operate the dynamic power management function.
RSSI Threshold (dBm)	Sets the RSSI threshold of the dynamic power management operation.
Scanning Interval (sec.)	Sets the interval of viewing the power status information.
Minimum Transmission Power	Sets the minimum transmission power standard.
Maximum Transmission Power	Sets the maximum transmission power standard.

[Selecting Dynamic Channel]

Item	Description
Status	Sets whether to operate the function of selecting a dynamic channel.
Scanning Interval (sec.)	Sets the interval of viewing the power status information.
Channel Usage Rate Threshold (%)	Sets the channel usage rate threshold and the internal usage rate threshold.
Interference Source Grade Threshold (%)	Sets the interference source grade threshold.

Item	Description
Delayed Channel Change	Whether to use the delayed channel change
Recognition Option	Sets whether to use the voice, traffic, and station recognition options and the number of stations.
Anchor Starting Time	Sets the start time of the anchor.
Anchor End Time	Sets the end time of the anchor.
Country	Not a real set value but an option to show the DSC channel on the bottom
DCS Channel	Sets the DCS channel.

[Coverage Hole Detection Control]

Item	Description
Status	Sets whether to operate the coverage hole detection function.
Collecting Statistics	Whether to use collecting statistics
Trap Warning Message Notification	Whether to use trap warning message notification
Activating Statistics Power Control	Whether to use the activation of statistics power control
Percentage of Failed Client Count	Whether to use the percentage of failed client count
Minimum RSSI Threshold of Voice Traffic (DBM)	Sets minimum RSSI threshold of voice traffic.
Minimum RSSI Threshold of Data Traffic (DBM)	Sets minimum RSSI threshold of data traffic.
Failed Client Count	Sets failed client count.
Time Interval	Sets the time interval.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.5 Security

4.4.5.1 RADIUS

The ‘Security’ → ‘RADIUS’ menu of the controller template provides a function of setting information relating to the RADIUS to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[RADIUS Server]

Item	Description
Type	Selects a type of the RADIUS server.
IP address	Configures an IP address.
Authentication Port	Sets an authentication port.
Key Format	Selects a key format.
Shared Key	Sets a shared key.
Count of retransmissions	Sets retransmission count.
Retransmission interval (sec.)	Sets the retransmission interval.
Retransmission Failover Count	Sets retransmission failover count.
Change of Authorization (CoA)	Whether to use CoA

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.6 ACL

4.4.6.1 IP ACL

The 'ACL' → 'IP ACL' menu of the controller template provides a function of setting information relating to the ACL to the controllers in a lump.

[Template Name]

Item	Description
Template Name	Name of the template

[ACL]

Item	Description
Name	Sets a name.
Sequence Number	Sets sequence number.
Operation	Sets permit or denial.
Protocol	Sets a protocol (Any, ICMP, TCP, UDP).
The source IP address	Sets a source IP address value.
Source Net Mask	Sets a source mask value.
The destination IP address	Sets a target IP address value.
Destination Net Mask	Sets a target mask value.
TOS Type	ToS type (Not Used/DSCP/Precedence)
TOS Value	Configure the ToS value.
OS AWARE	OS Aware value

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.7 DHCP

4.4.7.1 Proxy/Relay

The ‘DHCP’ → ‘Proxy/Relay’ menu of the controller template provides a function of setting information relating to the Proxy/Relay of the controllers to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Proxy/Relay]

Item	Description
Mode	DHCP service mode (Proxy/Relay)
Timeout	Timeout of the DHCP service
Basic DHCP Server	The IP adress of the first DHCP server
Secondary DHCP Server	The IP adress of the second DHCP server

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.7.2 OS Aware

The ‘DHCP’ → ‘OS Aware’ menu of the controller template provides a function of setting information relating to OS Aware to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[OS Aware]

Item	Description
OS Name	Sets the name of the operating system to be added.

Item	Description
OS Type	Configures an OS type (android, ios, windows, mac).
Rank	Configures OS Aware rank information.
DHCP Option	Configures the DHCP option number.
Fingerprint	Sets a fingerprint to be recognized.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.8 QoS

4.4.8.1 Profile

The 'QoS' → 'Profile' menu of the controller template provides a function of setting QoS profile information to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Name	Sets the name of a profile.
Description	Sets explanation.
Maximum Dot1p Tag	Sets maximum Dot1p tag.
Limitation of Downstream Bandwidth by User (Kbps)	Sets the limitation of downstream bandwidth by user (Kbps).
Limitation of Upstream Bandwidth by User (Kbps)	Sets the limitation of upstream bandwidth by user (Kbps).
Voice-802.1p	Sets Voice-802.1p.
Voice-DSCP	Sets Voice-DSCP.
Video-802.1p	Sets Video-802.1p.
Video-DSCP	Sets Video-DSCP.
Best Effort-802.1p	Sets Best Effort-802.1p.
Best Effort-DSCP	Sets Best Effort-DSCP.
Background-802.1p	Sets Background-802.1p.
Background-DSCP	Sets Background-DSCP.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.9 AP

4.4.9.1 Profile

The ‘AP’ → ‘Profile’ menu of the controller template provides a function of setting the AP profile to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Name of AP	Sets the name of an AP.
MAC ADDRESS	Sets MAC ADDRESS.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.
You can import a file by using the ‘Import’ button.

4.4.10 Management

4.4.10.1 Controller Account

The ‘Management’ → ‘Controller Account’ menu of the controller template provides a function of setting the account information to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Level	Sets the connection level (Administrator/Operator/Monitor/Lobby Ambassador).
User	User Account
Password	User password
Checking Password	Enters the user password again.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.2 SNMP

The ‘Management’ → ‘SNMP’ menu of the controller template provides a function of setting SNMP to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Community]

Item	Description
Community	Name of SNMP community

Item	Description
Access Type	Access type (Read Only/Read Write)
IP version	IP address version (IPv4/IPv6)
IPV4 address	IPv4 address
IPV6 address	IPv6 address
Net Mask	Net mask

[User]

Item	Description
Name	The name of a user for SNMP v3
Access Type	Access type (Read Only/Read Write)
Authentication Protocol	Protocol to be used for SNMP v3 authentication - Message-Digest algorithm 5 (MD5) - Secure Hash Algorithm (SHA)
Authentication Key	Authentication key to be used for SNMP v3 authentication
Private Protocol	Private protocol to be used for SNMP v3 authentication - NONE: Encrypted protocol not applied. - Data Encryption Standard (DES) - Advanced Encryption Standard (AES)
Private Key	Private key to be used for SNMP v3 authentication

[Trap]

Item	Description
Community Name	Name of SNMP community
Trap Version	SNMP trap version information
IP version	IP address version
IPV4 address	Manager IPv4 address
IPV6 address	Manager IPv6 address
Port	Port number

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.3 DNS

The ‘Management’ → ‘DNS’ menu of the controller template provides a function of setting the information relating to DNS of the controllers to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

Item	Description
Service	Whether to use the DNS service
First DNS Address	The IP adress of the first DNS server
Second DNS Address	The IP adress of the second DNS server
Third DNS Address	The IP adress of the third DNS server

[Relay]

Item	Description
Cache Size	The cache size to be used in DNS relay

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.4 NTP

The ‘Management’ → ‘NTP’ menu of the controller template provides a function of setting information on the NTP client and the NTP server to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[NTP Client]

Item	Description
Polling	The configuration status of the NTP client service
Polling Interval	The synchronization time interval of the NTP client

Item	Description
Type	NTP server type (IP Address, Domain)
Server IP address	IP address of the NTP server (if Domain is selected as a type)
Server Domain Name	Name of the domain of the NTP server (if IP Address is selected as a type)

[NTP Server]

Item	Description
Service	Service configuration status of the NTP server (enabled/disabled)

[AP NTP]

Item	Description
Mode	Time Setting Mode of AP (TimeStamp/NTP Type)
Stamp Interval	Interval at which the APC transmits the time of the APC to the AP
NTP Polling Interval	Interval at which the AP receives time information from the NTP server
Server	URL address of the NTP server which will bring connection time information from the AP

Item	Description
Server	URL address of the NTP server which will bring connection time information from the AP

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.5 System Log

The 'Management' → 'System Log' menu of the controller template provides a function of setting the information relating to the sytem logs of the controller in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[System Log Mode]

Item	Description
Mode	Whether to create system log (Enable/Disable)
Severity	Log severity which will leave system logs (Information/Notice/Warning/Minor/Major/Critical)

[System Log Server]

Item	Description
System Log Server 1	The IP adress of the first system log server
Port 1	The port number of the user datagram protocol (UDP) of the first system log server
System Log Server 2	The IP adress of the second system log server
Port 2	The port number of the user datagram protocol (UDP) of the second system log server

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.6 Service

The 'Management' → 'Service' menu of the controller template provides a function of setting information on service activation and ports to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description

Template Name	Name of the template

[Telnet-SSH]

Item	Description
Session Timeout (sec.)	Sets the session timeout.
Maximum Session Number	Sets the maximum number of sessions.
Telnet Service	Whether to activate the Telnet service
Port	Set a Telnet port.
SSH Service	Whether to activate the SSH service
Port	Sets a SSH port.

[FTP]

Item	Description
Service	Whether to activate the FTP service
Port	Sets a FTP port.
ID	Sets a FTP ID.
Password	Sets a FTP password.

[Security FTP]

Item	Description
Service	Whether to activate the security FTP service
ID	Sets a security FTP ID.
Password	Sets a security FTP password.

[HTTP]

Item	Description
Service	Whether to activate the HTTP service

[HTTPs]

Item	Description
Service	Whether to activate the HTTPs service

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.7 Time

The ‘Management’ → ‘Time’ menu of the controller template provides a function of setting a local time to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Local Time]

Item	Description
Time	Designate the time to be applied to the controller.
Time Zone	Designate the time zone to be applied to the controller.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.8 Reboot

The ‘Management’ → ‘Reboot’ menu of the controller template provides a function of setting a reboot set in the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Reboot Settings]

Item	Description
Now	Rebooted immediately
Elapsed Time	Rebooted when a specific time has elapsed
Specific Time	Rebooted at a specific time
Schedule Cancellation	All reservations for reboots which have been set previously are canceled.

[Saving Settings]

Item	Description
Reboot after Saving	Rebooted after saving the settings
Reboot without Saving	Rebooted without saving the settings

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.4.10.9 Alarm Threshold

The 'Management' → 'Alarm Threshold' menu of the controller template provides a function of setting the information relating to the 'alarm threshold' of the controller in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[CPU Usage Rate]

Item	Description
Threshold	CPU usage rate threshold which will generate an alarm

[Memory Usage]

Item	Description
Threshold	Memory usage threshold which will generate an alarm

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5 AP Template

4.5.1 Template

The AP template is a function of storing a set of settings relating to APs under one name and selecting APs to which the settings will be applied in a lump and applying them to the APs. By doing so, it can store configuation sets with specific features which are frequently used. Therefore, the operator does not have to configure such frequently used configuration sets every time. In addition, it can reduce a task of setting every AP by selecting several controllers at the same time and applying settings in a lump.

The AP template runs in the ‘Configuration Management’ ‘AP Template’ menu.

Figure 93. Template List Screen

Adding

For all template items, the Add button is provided. When you click the Add button on the template list screen (Fig. 94), you can set and save a configuration group with a specific feature. Click the ‘Save’ button on the adding screen and then settings are saved under the template name as the required input element. Press the ‘Close’ button on the adding screen and then the screen returns to the template list screen.

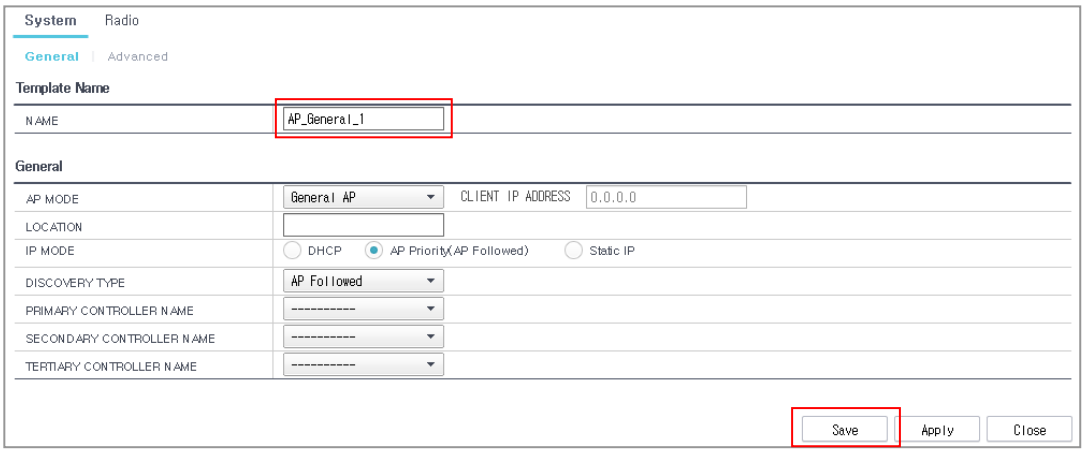


Figure 94. Template Adding Screen

Changing

To change a specific template item, click the name of the template you want to change on the template list screen. In the case, the screen same as the ‘Adding’ screen appears and you can check the pre-set value. Change the information and click the ‘Save’ button and then the information is changed to the template and then saved.

Delete

Select the check box of the item you want to delete on the template list screen and click the ‘Delete’ button on the bottom.

Application

To apply a specific template, press the ‘Apply’ button. The ‘Apply’ button is on the template list screen and the ‘Add’ and ‘Change’ screens. To apply on the template list screen, select the check box of the item to apply in the list and press the ‘Apply’ button (Fig. 96).
To apply the ‘Adding’ or ‘Changing’ screen, click the name of the template in the template list and select the check box of the module in the screen you want to apply before pressing the ‘Apply’ button (Fig. 97). If there is no check box, all are applied.
Press the ‘Apply’ button and then a new window appears (Fig. 98). The left of the window is in a tree form and you can select several APs or controllers here. Select the checkbox of the controller you want to apply and press the ‘Apply’ button at the bottom right to apply to each selected AP sequentially and then whether to succeed or fail in the application to each controller is displayed in the progress bar.

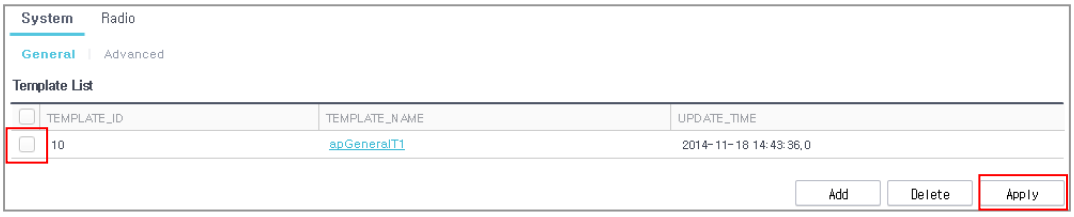


Figure 95. Application on Template List Screen

Figure 96. Application on Adding and Changing Screens

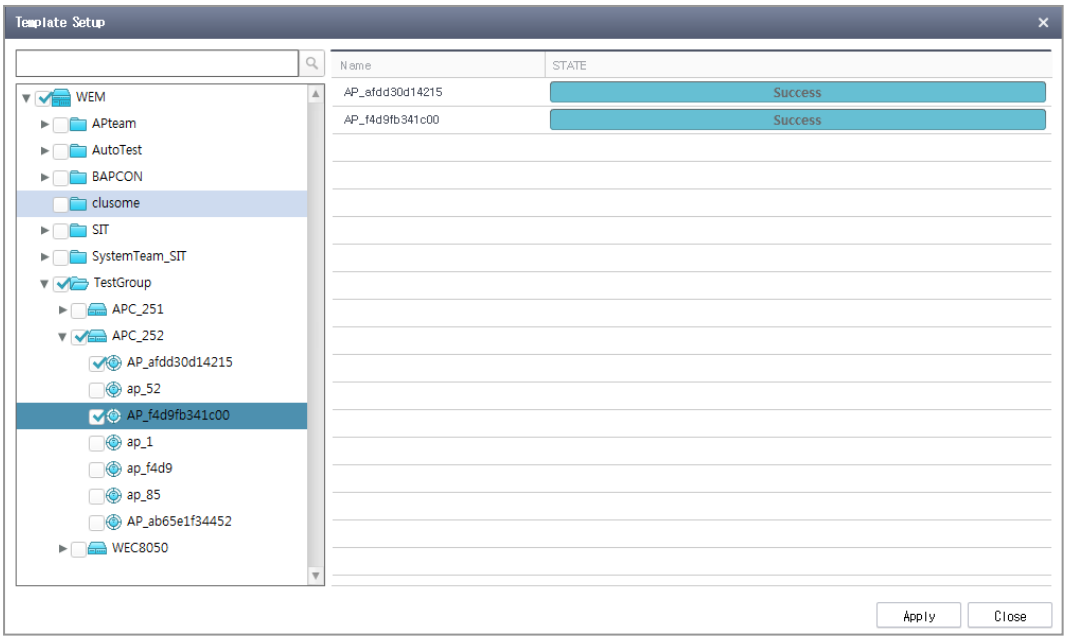


Figure 97. Controller Selection and Application

4.5.2 System

4.5.2.1 General

The 'System' → 'General' menu of the AP template provides a function of setting information to be set to the APs in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[General]

Item	Description
Name of AP	Sets the name of the AP.
AP Mode	AP operation mode - General: Basic AP mode for user services - Root AP: A backbone AP for the repeater service. The wireless terminal is connected to the repeater AP and then the wired network via the root AP. - Repeater AP: As an edge AP for repeater service, the AP actually connected by the wireless terminal.

Item	Description
	- Sniffer AP: An AP which does not provide a user service but provides a function of capturing a packet in an air section packet (If the AP mode is a sniffer AP, establish the client IP address.) - Relay AP: An AP connecting the repeater AP with the root AP wirelessly
Location	Location of the AP
IP Mode	IP Setting Mode - DHCP: IP is allocated to DHCP. - AP Priority: Under the method designated to the APs. - Static IP: Static IP used
Discovery Type	Sets the controller discovery type (AP Followed/APC Referral).
Names of First to Third Controllers	Shows the order of controllers to which the APs will be connected.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.5.1.

4.5.2.2 Advanced

The 'System' → 'Advanced' menu of the AP template provides a function of setting detailed items to be set to the APs in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Advanced Options]

Item	Description
Echo Interval (sec.)	Keep-alive interval of the CAPWAP session between AP and controller
Maximum Discovery Interval (sec.)	Maximum waiting time before AP starts controller discovery
Reporting Interval (sec.)	Interval at which the statistical information on WiFi decryption error is reported
Statistical Timer (sec.)	Interval at which the WiFi statistical information is reported
Retransmission interval (sec.)	First retransmission interval of the CAPWAP control packet

Item	Description
Maximum retransmission count	Maximum retransmission count of the CAPWAP control packet
Echo Retransmission Interval (sec.)	Retransmission interval of the CAPWAP keep-alive packet
Maximum Echo Retransmission	Maximum retransmission count of the CAPWAP keep-alive packet
Telnet	Sets whether to use Telnet and a port.
SSH	Sets whether to use Secure Shell (SSH) and a port.
Console	Whether to activate the AP console
DTLS	Sets whether to activate DTLS (Disabled/Control-Only/Enabled).
LED	Selects an LED option and sets the time.
POE Type	Selects a POE type.
VLAN Supported	Whether to support the Virtual Local Area Network (VLAN)
NATIVE VLAN ID	Sets a native VLAN ID.
Country	Configuration status of the country where the equipment is made
Environment	Equipment installation environment - Both - Outdoor - Indoor - Non-country
Edge AP	Sets an edge AP.

[Time]

Item	Description
Time	Sets time zone by country/city.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.5.1.

4.5.3 Radio

4.5.3.1 802.11a/n/ac

The 'Radio' → '802.11a/n/ac' menu of the AP template provides a function of setting information relating to the radio in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[General]

Item	Description
Service	Sets whether to activate the service.
Channel	Sets a radio channel to be used.
Fixed Channel	Sets whether to fix a channel (Enabled/Disabled).
Transmission Power	Sets the transmission power level.
Fixed Power	Sets whether to fix power (Enabled/Disabled).
Maximum Number of UEs Allowed to Be Connected	Maximum number of UEs allowed to be connected

[Operating Type]

Item	Description
Supported	Sets whether 802.11n/ac is supported.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.5.1.

4.5.3.2 802.11b/g/n

The 'Radio' → '802.11b/g/n' menu of the AP template provides a function of setting information relating to the radio in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[General]

Item	Description
Service	Sets whether to activate the service.
Channel	Sets a radio channel to be used.
Fixed Channel	Sets whether to fix a channel (Enabled/Disabled).
Transmission Power	Sets the transmission power level.
Fixed Power	Sets whether to fix power (Enabled/Disabled).
Maximum number of UEs allowed to be connected	Maximum number of UEs allowed to be connected

[Operating Type]

Item	Description
Supported	Sets whether 802.11n is supported.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.5.1.

4.5.4 Security

4.5.4.1 RADIUS

The ‘Security’ → ‘RADIUS’ menu of the controller template provides a function of setting information relating to the RADIUS to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[RADIUS Server]

Item	Description
Type	Selects a type of the RADIUS server.
IP address	Configures an IP address.
Authentication Port	Sets an authentication port.
Key Format	Selects a key format.
Shared Key	Sets a shared key.
Count of retransmissions	Sets retransmission count.
Retransmission interval (sec.)	Sets the retransmission interval.
Retransmission Failover Count	Sets retransmission failover count.
Change of Authorization (CoA)	Whether to use CoA

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.5 ACL

4.5.5.1 IP ACL

The ‘ACL’ → ‘IP ACL’ menu of the controller template provides a function of setting information relating to the ACL to the controllers in a lump.

[Template Name]

Item	Description
Template Name	Name of the template

[ACL]

Item	Description
Name	Sets a name.
Sequence Number	Sets sequence number.
Operation	Sets permit or denial.
Protocol	Sets a protocol (Any, ICMP, TCP, UDP).
The source IP address	Sets a source IP address value.
Source Net Mask	Sets a source mask value.
The destination IP address	Sets a target IP address value.
Destination Net Mask	Sets a target mask value.
TOS Type	ToS type (Not Used/DSCP/Precedence)
TOS Value	Configure the ToS value.
OS AWARE	OS Aware value

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.6 DHCP

4.5.6.1 Proxy/Relay

The ‘DHCP’ → ‘Proxy/Relay’ menu of the controller template provides a function of setting information relating to the Proxy/Relay of the controllers to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Proxy/Relay]

Item	Description
Mode	DHCP service mode (Proxy/Relay)
Timeout	Timeout of the DHCP service
Basic DHCP Server	The IP adress of the first DHCP server
Secondary DHCP Server	The IP adress of the second DHCP server

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.6.2 OS Aware

The ‘DHCP’ → ‘OS Aware’ menu of the controller template provides a function of setting information relating to OS Aware to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[OS Aware]

Item	Description
OS Name	Sets the name of the operating system to be added.

Item	Description
OS Type	Configures an OS type (android, ios, windows, mac).
Rank	Configures OS Aware rank information.
DHCP Option	Configures the DHCP option number.
Fingerprint	Sets a fingerprint to be recognized.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.7 QoS

4.5.7.1 Profile

The 'QoS' → 'Profile' menu of the controller template provides a function of setting QoS profile information to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Name	Sets the name of a profile.
Description	Sets explanation.
Maximum Dot1p Tag	Sets maximum Dot1p tag.
Limitation of Downstream Bandwidth by User (Kbps)	Sets the limitation of downstream bandwidth by user (Kbps).
Limitation of Upstream Bandwidth by User (Kbps)	Sets the limitation of upstream bandwidth by user (Kbps).
Voice-802.1p	Sets Voice-802.1p.
Voice-DSCP	Sets Voice-DSCP.
Video-802.1p	Sets Video-802.1p.
Video-DSCP	Sets Video-DSCP.
Best Effort-802.1p	Sets Best Effort-802.1p.
Best Effort-DSCP	Sets Best Effort-DSCP.
Background-802.1p	Sets Background-802.1p.
Background-DSCP	Sets Background-DSCP.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.8 AP

4.5.8.1 Profile

The ‘AP’ → ‘Profile’ menu of the controller template provides a function of setting the AP profile to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Name of AP	Sets the name of an AP.
MAC ADDRESS	Sets MAC ADDRESS.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.
You can import a file by using the ‘Import’ button.

4.5.9 Management

4.5.9.1 Controller Account

The ‘Management’ → ‘Controller Account’ menu of the controller template provides a function of setting the account information to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Profile]

Item	Description
Level	Sets the connection level (Administrator/Operator/Monitor/Lobby Ambassador).
User	User Account
Password	User password
Checking Password	Enters the user password again.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.2 SNMP

The ‘Management’ → ‘SNMP’ menu of the controller template provides a function of setting SNMP to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Community]

Item	Description
Community	Name of SNMP community

Item	Description
Access Type	Access type (Read Only/Read Write)
IP version	IP address version (IPv4/IPv6)
IPV4 address	IPv4 address
IPV6 address	IPv6 address
Net Mask	Net mask

[User]

Item	Description
Name	The name of a user for SNMP v3
Access Type	Access type (Read Only/Read Write)
Authentication Protocol	Protocol to be used for SNMP v3 authentication - Message-Digest algorithm 5 (MD5) - Secure Hash Algorithm (SHA)
Authentication Key	Authentication key to be used for SNMP v3 authentication
Private Protocol	Private protocol to be used for SNMP v3 authentication - NONE: Encrypted protocol not applied. - Data Encryption Standard (DES) - Advanced Encryption Standard (AES)
Private Key	Private key to be used for SNMP v3 authentication

[Trap]

Item	Description
Community Name	Name of SNMP community
Trap Version	SNMP trap version information
IP version	IP address version
IPV4 address	Manager IPv4 address
IPV6 address	Manager IPv6 address
Port	Port number

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.3 DNS

The ‘Management’ → ‘DNS’ menu of the controller template provides a function of setting the information relating to DNS of the controllers to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

Item	Description
Service	Whether to use the DNS service
First DNS Address	IP adress of the first DNS server
Second DNS Address	IP adress of the second DNS server
Third DNS Address	IP adress of the third DNS server

[Relay]

Item	Description
Cache Size	Cache size to be used in DNS relay

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.4 NTP

The ‘Management’ → ‘NTP’ menu of the controller template provides a function of setting information on the NTP client and the NTP server to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[NTP Client]

Item	Description
Polling	Configuration status of the NTP client service
Polling Interval	Synchronization time interval of the NTP client

Item	Description
Type	NTP server type (IP Address, Domain)
Server IP address	IP address of the NTP server (if Domain is selected as a type)
Server Domain Name	Name of the domain of the NTP server (if IP Address is selected as a type)

[NTP Server]

Item	Description
Service	Service configuration status of the NTP server (enabled/disabled)

[AP NTP]

Item	Description
Mode	Time Setting Mode of AP (TimeStamp/NTP Type)
Stamp Interval	Interval at which the APC transmits the time of the APC to the AP
NTP Polling Interval	Interval at which the AP receives time information from the NTP server
Server	URL address of the NTP server which will bring connection time information from the AP

Item	Description
Server	URL address of the NTP server which will bring connection time information from the AP

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.5 System Log

The 'Management' → 'System Log' menu of the controller template provides a function of setting the information relating to the sytem logs of the controller in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[System Log Mode]

Item	Description
Mode	Whether to create system log (Enable/Disable)
Severity	Log severity which will leave system logs (Information/Notice/Warning/Minor/Major/Critical)

[System Log Server]

Item	Description
System Log Server 1	IP adress of the first system log server
Port 1	Port number of the user datagram protocol (UDP) of the first system log server
System Log Server 2	IP adress of the second system log server
Port 2	Port number of the user datagram protocol (UDP) of the second system log server

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.6 Service

The 'Management' → 'Service' menu of the controller template provides a function of setting information on service activation and ports to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description

Template Name	Name of the template

[Telnet-SSH]

Item	Description
Session Timeout (sec.)	Sets the session timeout.
Maximum Session Number	Sets the maximum number of sessions.
Telnet Service	Whether to activate the Telnet service
Port	Set a Telnet port.
SSH Service	Whether to activate the SSH service
Port	Sets a SSH port.

[FTP]

Item	Description
Service	Whether to activate the FTP service
Port	Sets a FTP port.
ID	Sets a FTP ID.
Password	Sets a FTP password.

[Security FTP]

Item	Description
Service	Whether to activate the security FTP service
ID	Sets a security FTP ID.
Password	Sets a security FTP password.

[HTTP]

Item	Description
Service	Whether to activate the HTTP service

[HTTPs]

Item	Description
Service	Whether to activate the HTTPs service

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.7 Time

The 'Management' → 'Time' menu of the controller template provides a function of setting a local time to be applied to the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Local Time]

Item	Description
Time	Designate the time to be applied to the controller.
Time Zone	Designate the time zone to be applied to the controller.

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.8 Reboot

The 'Management' → 'Reboot' menu of the controller template provides a function of setting reboot set in the controllers in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[Reboot Settings]

Item	Description
Now	Rebooted immediately
Elapsed Time	Rebooted when a specific time has elapsed
Specific Time	Rebooted at a specific time
Schedule Cancellation	All reservations for resetting which have been set previously are canceled.

[Saving Settings]

Item	Description
Reboot after Saving	Rebooted after saving the settings
Reboot without Saving	Rebooted without saving the settings

The procedures of adding, changing, deleting or applying a template are same. Refer to Section 4.4.1.

4.5.9.9 Alarm Threshold

The 'Management' → 'Alarm Threshold' menu of the controller template provides a function of setting the information relating to the 'alarm threshold' of the controller in a lump.

The items are given below.

[Template Name]

Item	Description
Template Name	Name of the template

[CPU Usage Rate]

Item	Description
Threshold	CPU usage rate threshold which will generate an alarm

[Memory Usage]

Item	Description
Threshold	Memory usage threshold which will generate an alarm


NOTE

Template Add/Modify/Delete/Apply

Add, Modify, Delete, Apply, method refer to Section 4.5.1.

4.6 Security

4.6.1 Interferer

This function provides to set source of WLAN interference for AP that can cause interference.

The parameters are as follows:

Parameter	Description
Interferer 2.4 GHz	Bluetooth device, microwave. Jammer, wireless telephone, video camera, zigbee device
Interferer 5 GHz	Jammer, wireless telephone, video camera

Setting Interferer

1) Select the AP controller on the Tree Viewer.
2) Go to 'Configuration' → 'Security' → 'Interferer'.
3) Change the information.
4) Click the '**Set**' button, save the data.

CHAPTER 5. Admin

This chapter describes the WEM admin window and features.

The ‘Admin’ menu can be distinguished as follows:

- Alarm
- Software
- Settings
- License

5.1 Alarm

5.1.1 Audible Alarm

The ‘Audible Alarm’ notifies an operator of a fault by generating a particular sound (audible sound).

Each item is shown below.

Item		Description
Mute		Whether to generate an audible sound.
By Grade	Play	- Repeat: Whether to generate an audible sound once or repeatedly - No Interception: If this item is checked, the first audible sound is played in its entirely and then other sounds are played after that.
	Level	Alarm level that will generate an audible sound - Critical/Major/Minor:
	Policy	Policy of generating audible sound - Representative alarm/Final alarm - List of audible sound exception code
Fault code-based	Play	Repeat: Whether to generate an audible sound once or repeatedly
	Sound source	Select a sound source for an audible sound.

Stop an audible sound being played

1) Select 'Operation Management' → 'Alarm' → 'Audible Alarm' menu.
2) Click the 'Pause' button at the bottom of the screen.

Setup

1) Select 'Operation Management' → 'Alarm' → 'Audible Alarm' menu.
2) The setup status of audible sound is displayed on the screen.
3) Select an item to change. If you select the 'Mute' checkbox, all other items become disabled.
4) To set up an audible alarm code, select the 'Final Alarm' of the 'Policy' (Policy of generating audible sound) and click the 'Add' button on the right-hand side.
5) The audible alarm code search screen is displayed.
6) After selecting 'NE type', 'NE Version', 'Event Type', click 'Search' button.
7) If the search result is displayed on the screen, select an alarm code and click the 'add' button.
8) Click the 'Set' button.

5.1.2 Ticketing group

When an alarm occurs, WEM transmits its details and location to the previously configured e-mail list. The 'E-mail Group' manages the e-mail list.

The e-mail group setup items are shown below.

Item	Description
E-mail address	E-mail address
Name	E-mail recipient's name
Description	Additional explanation

Retrieving

1) Select 'Operation Management' → 'Ticketing Group'.
2) The list of e-mails is shown in the results table.
3) When you click the 'Retrieve' button at the bottom of the screen, the list of e-mail groups is updated.
   You can add/delete an e-mail group by clicking 'Add/Delete'.

Adding

1) Select 'Operation Management' → 'Ticketing Group'.
2) The list of e-mails is shown in the results table.
3) To add an e-mail group, enter the 'e-mail address', 'Name', and 'Description' of the setup table, instead of entering the items from the results table.
4) Save the settings by clicking the 'Add' button.

Deleting

1) Select ‘Operation Management’ → ‘Ticketing Group’.
2) The list of e-mails is shown in the results table.
3) Select the checkbox in the most front of the item to delete.
4) Delete a selected e-mail item by clicking the ‘Delete’ button.

5.1.3 Ticketing setup

This is used to send a locational condition to a specified e-mail address when a specific alarm occurs.

The e-mail setup items are shown below.

Item	Description
TARGET	Target device to which an e-mail will be sent
Total alarm list/Selected alarm list	Total alarm list and selected alarm list
Total e-mail list/Selected e-mail list	Total e-mail list and selected e-mail list
Title	Title of an e-mail to send

Retrieving

1) Select ‘Operation Management’ → ‘Ticketing Setup’.
2) Select an equipment (controller) to retrieve in the Tree Viewer. The selected device is displayed in the ‘TARGET’ field.
3) Select the ‘Retrieve’ button.
4) The e-mail related setup information is displayed in the results table.

Adding

1) Select ‘Operation Management’ → ‘Ticketing Setup’.
2) Select an equipment (controller) to retrieve in the Tree Viewer. The selected device is displayed in the ‘TARGET’ field.
3) Select the ‘Retrieve’ button.
4) The e-mail related setup information is displayed in the results table.
5) Instead of selecting an item in the results table, select an alarm to add and an e-mail in the setup table and click the right arrow (‘>’) button.
6) Save the settings by clicking the ‘Add’ button.

Deleting

1) Select ‘Operation Management’ → ‘Ticketing Setup’.
2) Select an equipment (controller) to retrieve in the Tree Viewer. The selected device is displayed in the ‘TARGET’ field.
3) Select the ‘Retrieve’ button.
4) The e-mail related setup information is displayed in the results table.
5) Select the checkbox at the most front of the item to delete.
6) Delete a selected e-mail item by clicking the ‘Delete’ button.

5.1.4 Ticketing History

This is used to retrieve the history of e-mail transmission.

The e-mail history retrieving items are shown below.

Item	Description
TARGET	Target device whose e-mail transmission history will be retrieved
Alarm code	Alarm code to retrieve
E-mail address	E-mail address to retrieve
Result	Transmission result of an e-mail to retrieve (Total/Success/Failure)
Period	Period when e-mail transmission history will be retrieved

Retrieving

1) Select 'Operation Management' → 'Ticketing History' → 'E-mail History'.
2) Select an equipment (controller) to retrieve in the Tree Viewer. The selected device is displayed in the 'TARGET' field.
3) Enter search conditions.
4) Click the 'Retrieve' button.

5.1.5 Level/blocking control

You can check the alarm level information including alarm ID, name and group.

The alarm control items are shown below.

Item	Description
Alarm severity	Applied alarm severity (Critical, Major, Minor)
Whether an alarm is allowed	Whether an alarm is allowed (Allow, Inhibit)
Applied controller	Select a controller to apply.

[Alarm Severity Information]

Item	Description
Alarm number	Alarm ID
Alarm name	Alarm name
Group name	- system: Alarm occurred in a controller - ap: Alarm occurred in an AP - wifi: Wi-Fi related alarm - security: Security related alarm - network: Network related alarm - etc.: Others

Item	Description
Alarm severity	Alarm severity - Critical: Critical Faults - Major: Major Faults - Minor: Minor Faults
Allow Alarm	Allow Alarm (Allowed/Inhibit)

Retrieve alarm severity information

1) Select ‘Operation Management’ → ‘level/blocking control’ menu.
2) Select ‘Alarm Severity’ and ‘Allow Alarm’.
3) Select a controller to apply.
4) Click the ‘Save’ button.

5.1.6 Filter setup

An operator can receive alarms selectively by specifying the desired alarms.

The alarm filter items are shown below.

Item	Description
Alarm filter group	ALL/SYSTEM/PM/AP/WLAN/WIFI/SECURITY/NETWORK/ INTERFACE/SE
Alarm filter severity	Applied alarm severity (Critical, Major, Minor)

[Alarm Filter Information]

Item	Description
Controller name	Controller name
IP address	IP address of a controller
Filter group	Alarm filter group (ALL/SYSTEM/PM/AP/WLAN/WIFI/SECURITY/ NETWORK/INTERFACE/SE)
Filter severity	- Critical: Critical Faults - Major: Major Faults - Minor: Minor Faults
Remarks	Status information

Alarm filter setup

1) Select ‘Operation Management’ → ‘filter Set’ menu.
2) Select ‘Alarm Filter Group’ and ‘Alarm Filter Level’.
3) By using the checkbox on the left, select a controller to set up.
4) Click the ‘Save’ button.

5.1.7 User-defined Alarms

The operator can create alarms by combining alarms or events already defined in the system based on specific conditions.
The following user-defined alarm settings are available.

Item	Description
ID	ID of the user-defined alarm
Alarm name	Name of the user-defined alarm
Type	Type of the user-defined alarm. Available types include Count, Combine, Escalate, Threshold, and Compare.
Base alarm	System-defined alarm. These are combined to create user-defined alarms.
Level	Level of the defined alarm. Available levels include Critical, Major, and Minor.
Display name	Alarm name to display in the alarm display window.
Description	Description of the defined alarm
Transmission option	Specifies where the alarm should be transmitted. (Available options include Email and WEM.)

[Types]

Item	Description
Count	An alarm (APC down, AP down, Radio down) can be selected as a condition. The user-defined alarm is triggered if the alarm count exceeds a specified value within a specified period (days/hours/minutes). (Example: The user-defined alarm is triggered if ACP Down occurs 5 or more times in 1 day.)
Combine	Alarms (Channel Utilization, Noise Level, Rogue AP Detected, Interferer Detected) can be selected as conditions. The user-defined alarm is triggered if all of the specified alarms occur within a specified period (days/hours/minutes). (Example: The user-defined alarm is triggered if both the Channel Utilization and Noise Level alarms occur during 1 day.)
Escalate	An event (Call Quality, Noise Level, Packet Loss Rate, Packet Retry Rate, Channel Utilization, Rogue AP Detected, Interferer Detected) can be selected as a condition. The user-defined alarm is triggered if the specified event occurs. (Example: The user-defined alarm is triggered if the Rogue AP Detected event occurs.)
Threshold	An event (Call Quality, Noise Level, Packet Loss Rate, Packet Retry Rate, Channel Utilization, Rogue AP Detected, Interferer Detected) can be selected as a condition. The user-defined alarm is triggered if the specified event occurs and the value exceeds a specified value.

Item	Description
	(Example: The user-defined alarm is triggered if the Interferer Detected event occurs and the RSSI value exceeds the specified value.)
Compare	A string can be selected as a condition. The user-defined alarm is triggered if an event or an alarm containing the specified string occurs. (Example: The user-defined alarm is triggered if an event or an alarm containing 00:16:b7 occurs.)

Configuring User-defined Alarms

1) Select the 'Operation Management' → 'Alarms' → 'User-defined Alarms' menu.
2) Click the 'Register' button.
3) Specify a name and a type of the user-defined alarm.
4) Enter conditions according to the specified type.
5) Enter alarm information. Select Critical, Major, or Minor for Level according to the priority level of the alarm, and specify a name to display on the screen.
6) Specify the Email option if you wish to receive alarm notification by email.

Deleting User-defined Alarms

1) Select the 'Operation Management' → 'Alarms' → 'User-defined Alarms' menu.
2) Select a user-defined alarm to delete.
3) Click the 'Delete' button.

5.2 Software

5.2.1 Package management

The package management uploads or downloads the software package of a controller or an AP to/from the WEM server or controller.

The setup items are shown below:

[Device]

Item	Description
Device	Select a controller or an AP.

[Package List]

Item	Description
Name	Controller or AP package name saved in WEM
Size	Size of controller or AP package saved in WEM
Date	Time when controller or AP package saved in WEM is updated

[Controller List]

Item	Description
Name	Name of a controller that will download a package from WEM
Version	Package version of the current controller
300 Series AP Version	300 Series AP package version of the controller
400 Series AP Version	400 Series AP package version of the controller
Status	Package download status

Setup

1) Select ‘Operation Management’ → ‘software’ → ‘package Management’.
2) Select a controller or an AP in the Device.
3) Select a package from the package list to upload it to a device. If the file you want is not available, click the ‘Upload’ button and select a package you wish to upload to WEM.
4) Select a controller from which you want to download a package you selected.
5) When you click the ‘Download’ button, the package download is started and you can see the download progress in the Status bar.

5.2.2 Package upgrade

This is used to apply a downloaded software package to a controller or an AP.

Its items are shown below.

[Device]

Item	Description
Device	Selects a controller, an AP, or a remote AP group.

When you select an AP, the Option/Category is displayed separately.

[Option/Category]

Item	Description
Option	Total or individual. Total means that all the APs in a controller are selected and Individual means that a specific AP is selected.
Category	Select Default, fast upgrade or pre-download. - Default: A specific package is downloaded to a specific controller and upgrade is performed when an AP is rebooted. - Fast upgrade: Upgrade is started once download is complete. - Pre-download: An AP is rebooted with a pre-download option.
Forced upgrade	Option enabled when Individual is selected - Enable: Enable forced upgrade. - Disable: Disable forced upgrade.

When you select a controller, the following items are displayed in the controller list.

[Controller List]

Item	Description
Name	Name of a controller whose package will be changed
Version	Package version of the current controller
Status	Package download status

When you select an AP and then select Total from the option, the following items are displayed in the controller list.

Item	Description
Name	Name of a controller whose package will be changed

Item	Description
300 Series AP Version	Name of the package of 300 Series AP set
400 Series AP Version	Name of the package of 400 Series AP set
Category	Display AP upgrade method and a selected category.
Status	Upgrade progress status

[Package File]

Item	Description
300 Series	A package file of 300 Series AP to be upgraded
400 Series	A package file of 400 Series AP to be upgraded

When you select an AP and then select Individual from the option, the following items are displayed in the controller list.

Item	Description
Controller name	Name of a controller whose package will be changed
AP group	AP group name
AP name	Selected AP name
Operating Version	Operating software version
Backup Version	Software version backed up
Setup version	Version of configured software
Forced upgrade	Whether to use forced upgrade
Category	Display AP upgrade method and a selected category.
Status	Upgrade progress status

[Package File]

Item	Description
Package File	Package file to upgrade

[Saving Control]

Item	Description
Saving Control	Package upgrade after saving/Package upgrade without saving

[Recovery Control]

Item	Description
Recovery Control	Recovery of previous setup/No recovery of previous setup

Setup

1) Select ‘Operation Management’ → ‘Software’ → ‘Package Management’.
2) Select a controller or an AP in the Device.
3) When selecting an AP, select Total or Individual as Option/Category by referring to the item remark column.
4) Select a target controller to upgrade.
5) When you click the ‘Retrieve’ button of Package File, a dialog box is displayed from where you can select a specific package. Select the package you want.
6) When you click the ‘Upgrade’ button, upgrade to the package is performed.

5.3 Setup

5.3.1 Data server

Screen where you can set up the information required for data transmitting/receiving.

The information items are shown below.

Item	Description
Data transmission	Whether to use data transmission (Enable/Disable)
Data server	Data server setup (WEM/Other Server)

[Other Server Settings]

Item	Description
IP address	Server IP address
Directory	Directory where a file will be uploaded
Port	Server service port
Connection account	Server connection account
Password	Server connection password
Confirm Password	Server connection password (Confirm)

[Data Server Information]

Item	Description
Controller name	Controller name
Controller IP address	IP address of a controller
Status	FTP server enable/disable
Server directory	Upload path of a FTP server
Server IP address	IP address of a FTP server
Connection account	User ID of a FTP server
Port	Port number of a FTP server
Remarks	Status information

Setup

1) Select ‘Operation Management’ → ‘Set’ → ‘Data Server’ menu.
2) Enter ‘Data Transmission’ and ‘Data Server’ information.
   - Select whether to use ‘Data Transmission’.
   - Select WEM or Other Server in ‘Data Server’.

- If you select Other Server, enter upload IP address/path and port number into ‘IP address’, ‘Directory’, and ‘Port’.
- If you select Other Server, enter user account information into ‘Connection Account’ and ‘Password’.

3) By using the checkbox on the left, select a controller to set up.
4) Click the ‘Save’ button.

5.4 License

The WEM can provide license-based management for the allowed number of WE WLAN APs and firewalls, Voice Quality Monitor (VQM) service range, and WE WLAN AP.

The license items are shown below.

[Server License Information]

Item	Description
Number of accommodable APC/AP	Total number of controller/APs that can be managed after registration in WEM
Maximum number of users who can connect simultaneously	Number of clients who can connect to WEM simultaneously
Number of APCs being used	Number of registered controllers
Switch being used	Number of registered switches
Number of APs being used	Number of registered APs

Retrieving license

1) Select 'Operation Management' → 'License' menu.
2) Display license related information.

Change license

1) Select 'Operation Management' → 'License' menu.
2) Click the 'Change License' button.
3) Select a license file to change and click the 'Upload' button.
4) After rebooting the WEM server, the change is successfully applied.

[APC License Information]

Item	Description
APC name	Controller name
Number of APs	Number of APs that can be registered
VQM	Whether to use VQM
Firewall	Whether to use firewall
License list	Type, remaining period, installation times information

Retrieving license

1) Select 'Operation Management' → 'License' menu.
2) Display license related information.

Change license

1) Select ‘Operation Management’ → ‘License’ menu.
2) Click the ‘Change License’ button.
3) Enter a license key to change.
4) Click the ‘Apply’ button.

CHAPTER 6. Tools

This chapter describes external tools of WEM such as spectral analysis function, voice quality monitoring function, and packet capture function.

6.1 Spectrum Analyzer

Radio frequency (RF) interference is unpredictable and cause problem for WLAN performance. It can originate from neighboring Wi-Fi networks or non-Wi-Fi sources, such as 2.4-GHz cordless phones, microwave ovens, analog video cameras and wireless telemetry systems. Spectrum analyzer provides a critical layer of visibility into non-802.11 sources of RF interference and their effects on WLAN performance. The spectrum analyzer remotely identifies RF interference, classifies its source and provides real-time analysis at the point of the problem.

- Real time FFT: Wireless capture data converted into Fast Fourier Transform (FFT) and spectrum graph
- Duty Cycle: Channel utilization rate and spectrum graph

Real-time Spectrum Analyzer

1) Select ‘Tools’ → ‘Spectrum Analyzer’.
2) In the Tree Viewer, select AP to retrieve. Selected AP appears at the ‘Target Node’.
3) Click ‘Set’ button to open spectrum configuration window appears.
4) Set Wireless communication standards in the ‘Radio’ field.
5) Select ‘Real Time Configuration’ tab, and then set each item.
   - In the ‘Real-time Monitor Setup’ of ‘Real-time FFT’, select based on an average value or maximum value.
   - Select a spectrum type and spectrum search range in the ‘Spectrogram Monitor Setup’ of ‘Real-time FFT’.
   - Select a spectrum search range in the ‘Spectrogram Monitor Setup’ of ‘Channel Usage Rate’.
6) Click ‘Save’ button, save the settings.
7) If you click the ‘Run’ button in the main window of spectral analysis, the real-time monitoring is driven. Click the ‘Stop’ button to stop real time monitoring.

6.2 VQM

VQM as Voice Quality Monitor provides the voice-related information.
The operator may set the voice-related information of the controller system to the WEM server through the 'Control'. The description of the received files is stored in the database and statistical information by using the data through the 'Statistics' can be obtained.
In addition, VQM can obtain the data on the specific station now in use in real time in the 'Monitoring. In 'File History', the voice information files are normally dealt with from the controller system and it can be checked whether they are stored in the database.
The files received from the controller system cannot be properly handled for the reasons such as error in file format, and lack of data and the operator may check the history in the 'File History'.

6.2.1 Control

In the 'Control', the voice-related information of the controller system can be set to be transmitted to the WEM server and at the time file size, transmission interval, etc. can be set. In addition, ports and alarm occurring threshold values to be monitored can be set.

[General Items]

Item	Description
Operation	VQM enable/disable indicator
Description	Whether detailed matters are included in voice data
Maximum Session Number (1-2500)	Number of maximum media sessions to be monitored by VQM
Inspection Cycle (5-60)	The cycle at which the VQM brings media session information (Not the cycle at which the information file is transmitted from the controller to the WEM)
Session Deletion Waiting Time (15-60)	If there is no media data, the waiting time to delete the session

[Interface Items]

Item	Description
Port Area (1-65535)	The port area to be monitored by the VQM

[Alarm Items]

Item	Description
Burst (30-93)	Threshold value that generates alarm for burst
Delay (1-1000)	Threshold value that generates alarm for delay

Item	Description
MOS (1.0-5.0)	Threshold value that generates alarm for MOS
R-Factor (30-93)	Threshold value that generates alarm for R-Factor

[File Save]

Item	Description
Save Information	Whether to transmit the information collected by the VQM to the WEM
Storage Size (1024-102400)	The file size when the information file is transmitted to the WEM
File Name	Set the file prefix for classifying the controller.
Saving Interval	The interval at which the information file is transmitted to the WEM
Saving Method	The interval at which the information file is transmitted to the WEM
Server Address	The address of the server to transmit the information file (WEM address)
Saving Location	Directory to transmit the information file to
Account ID	Account ID to use when the information file is transmitted
Password	Password to use when the information file is transmitted

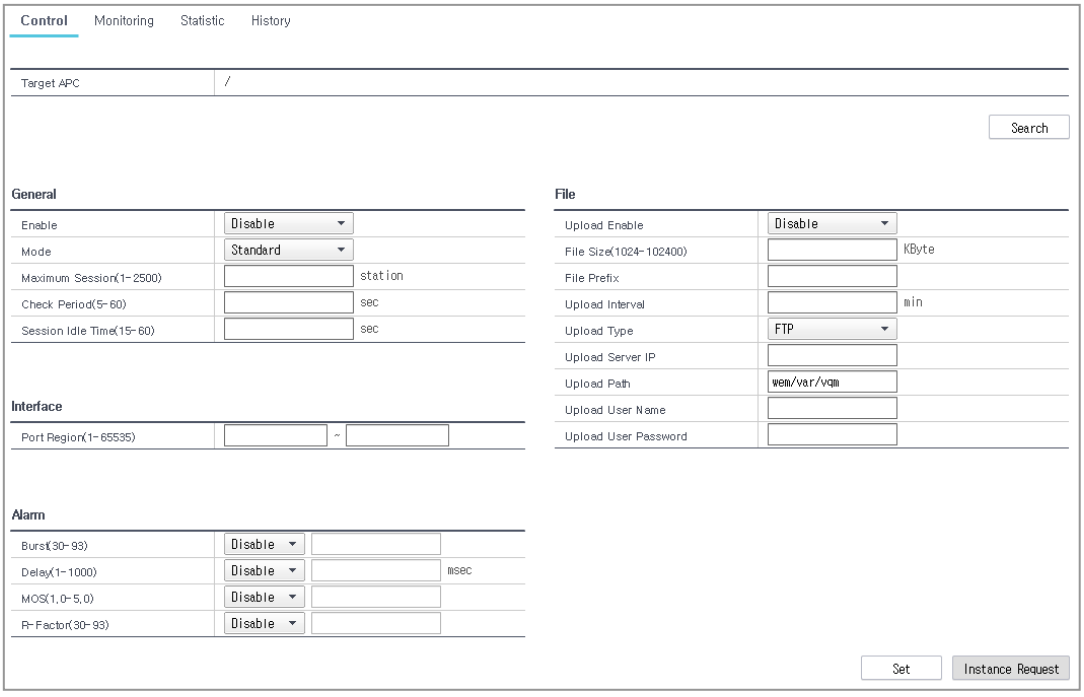


Figure 98. VQM Control

Viewing VQM Control

1) Select a controller in the tree.
2) Click the ‘Search’ button on the ‘Control’ screen.

Changing VQM Control

1) Change the item you want to change.
2) Click the ‘Set’ button on the ‘Control’ screen.

6.2.2 Monitoring

In ‘Monitoring’, the voice information on a specific station in use can be checked in real time. The methods for viewing include IP address, MAC, username (username at wireless connection), telephone, etc. In the result window on the right side, you can check the result in a form of graph or table. If the station you want to view is not in user, the controller system responds as Not-OK, and the WEM displays there is no subject to view.

Figure 99. VQM Monitoring

Starting Monitoring

1) Select a control system or group you want to view in the tree.
2) Select a method for viewing in ‘Condition’.
3) Enter a subject that meets ‘Condition’ in the ‘SubCondition’.
4) Check an item you want to view in ‘Item’.
5) Set the viewing interval in the ‘Period’.
6) Click the ‘Start’ button.

Stopping Monitoring

1) Click the ‘Stop’ button.
2) Click the ‘Set’ button on the ‘Control’ screen.

Saving or Printing

1) Click the ‘Save’ button and enter the file name before clicking the ‘OK’ button.
2) After clicking the ‘Print’ button, perform the printing command as indicated on the screen.

6.2.3 Statistics

In ‘Statistics’, the description on the voice-related statistics can be viewed based on the data received from the controller.

6.2.3.1 Call Summary

In the ‘Call Summary’ tab, you can check the overall status. Statistical subjects may be a controller system and a group. The conditions may be designated by SSID, WLAN, and BSSID, and a specific station may be designated by using IP address, Username, MAC, and telephone as secondary conditions. The period during which the statistical value is viewed can be set by using the target period or time setting.
In ‘MOS Status’ on the right top, the operator can set the threshold value to classify under the MOS and classify and indicate number of calls whose status is good and whose status is bad based on the threshold value.
‘Service Health’ on the bottom displays the number of calls by Mean Opinion Score (MOS) value in a bar graph and ‘Call Quality’ may show the progress of the MOS value depending on the time. ‘Problem Indicator’ shows the number of calls whose index is not good in a bar graph.

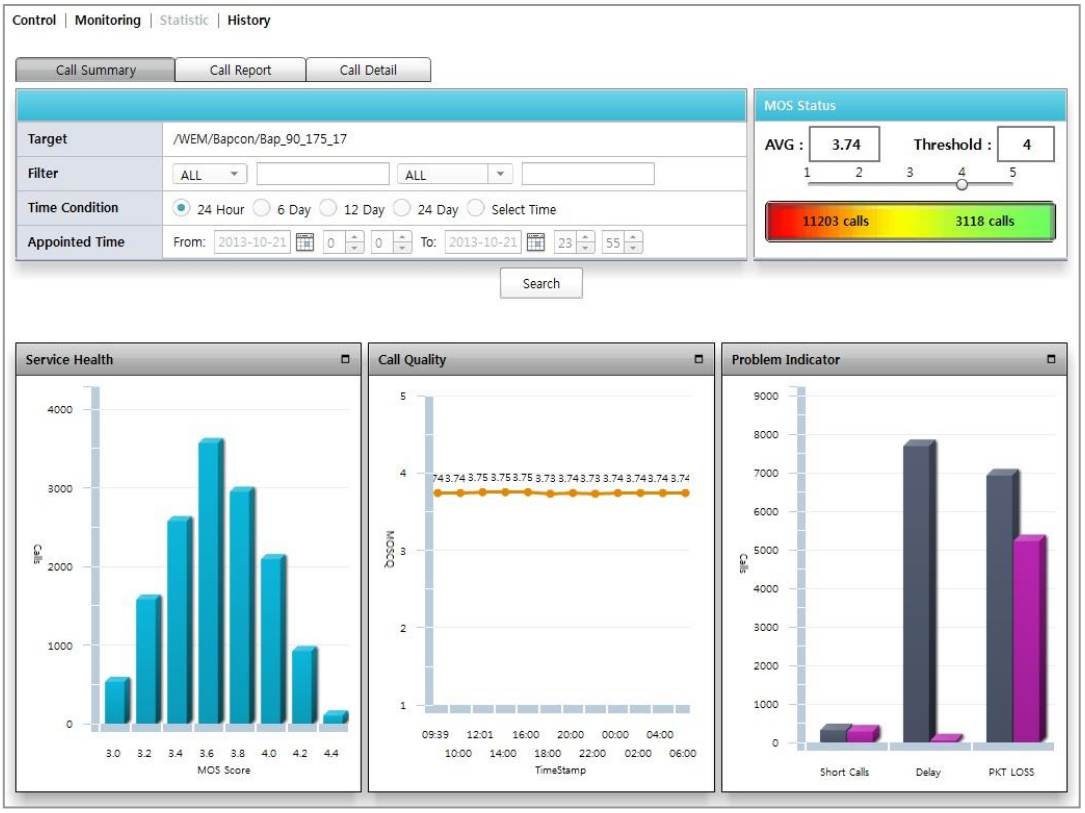


Figure 100. VQM Status Board

Viewing Statistical Value

1) Select the subject as a controller system or group in the tree.
2) Designate a subject as SSID, WLAN and BSSID in the ‘Conditions’ or a station with IP address, MAC, username, and telephone number.
3) Select the period to view in ‘Appointed Time’.
4) If you want to set a specific period, select ‘a designation date’ in the ‘Target Period’ and enter the time you want in the ‘Time Setting’.
5) Designate a threshold value with which calls whose status is good and bad are classified in ‘MOS Status’.
6) Click the ‘Search’ button.

6.2.3.2 Call Report

In the ‘Call Report’ tab, you can make a report on the statistics.

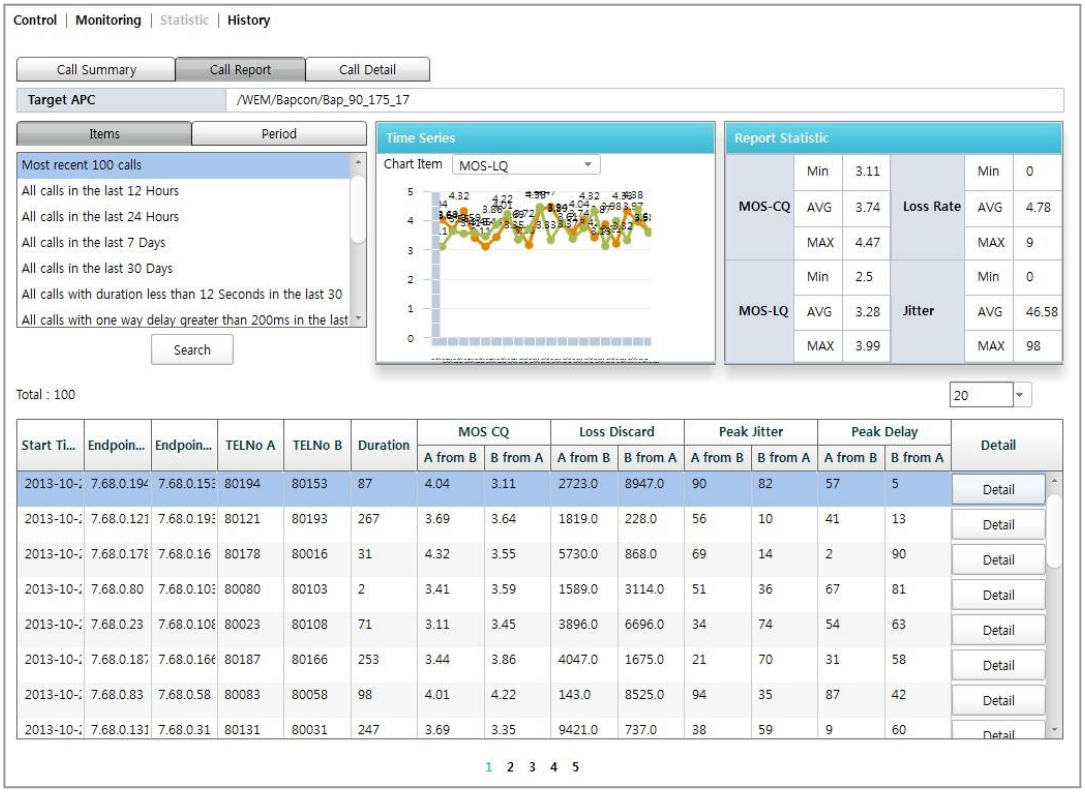


Figure 101. VQM Report

Creating Report

1) To make a report with specific items, select an item you want in the ‘Items’ tab.
2) To make a report with a specific period, select an item you want in the ‘Period’ tab.
3) Designate a specific item to view in ‘Time Series’.
4) Click the ‘Search’ button.

6.2.3.3 Call Detail

In the ‘Call Detail’ tab, the detailed information on a specific call can be viewed.
In the ‘Call Report’ tab, click ‘Call Detail’ button on the call you want to see more in the list of calls appearing on the screen, the screen is switched to ‘Call Detail’ and the detailed information appears. In the Details screen, you can see the status of sound sources such as delay, echo, and noise and the call occurring time, telephone number, IP address, etc. In the table as shown below, you can check each indicators relating to the voice of the call.

Figure 102. Detailed Information on VQM

Viewing Details

Click the ‘Call Detail’ button of the call you want to see in detail in the ‘Call Report’ screen.

6.2.4 History

In ‘History’, the result of the process of the voice-related information file received from the controller can be viewed. If it is impossible to extract information for any reasons such as wrong file format received from the controller, the WEM processes the file failed and keeps the record.

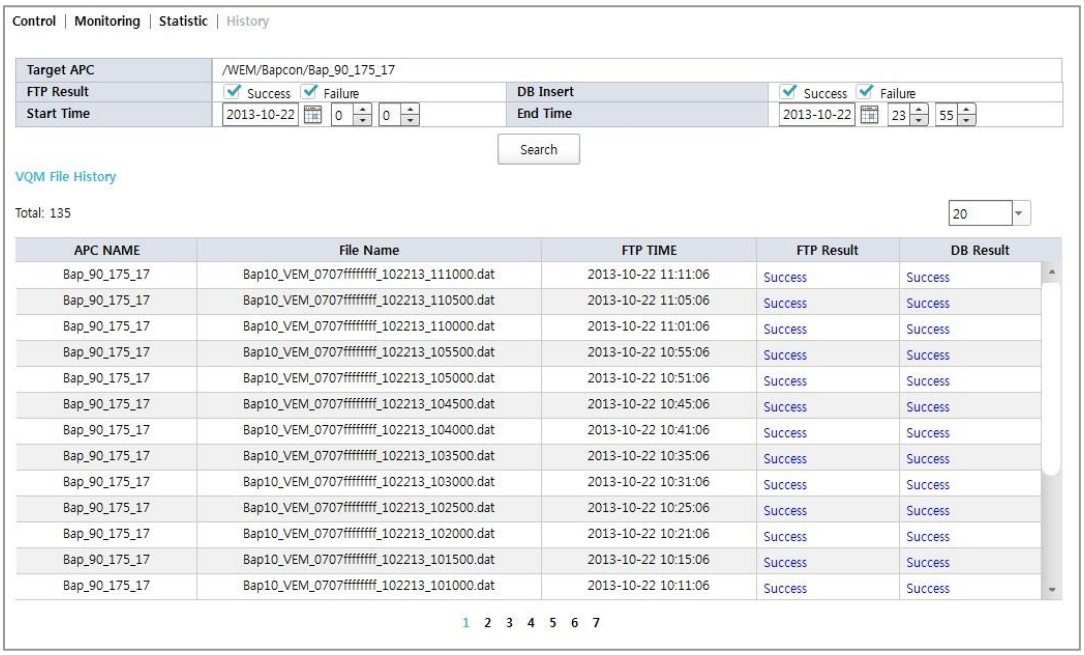


Figure 103. VQM File History

Viewing File History

1) Select a controller system or group you want to see the file history from in the tree.
2) Select whether you will see only success-related files, only failure-related files or both files in ‘FTP Result’.
3) Select whether you will see only DB processing success-related files, only failure-related files or both in the ‘DB Insert’.
4) Enter the time that you want to see the file processing result in the ‘Start Time’ and ‘End Time’.
5) Click the ‘Search’ button.

6.3 Packet Capture

6.3.1 APC Packet Capture

It provides a function of retrieving or configuring the packet capture information set in the controller.

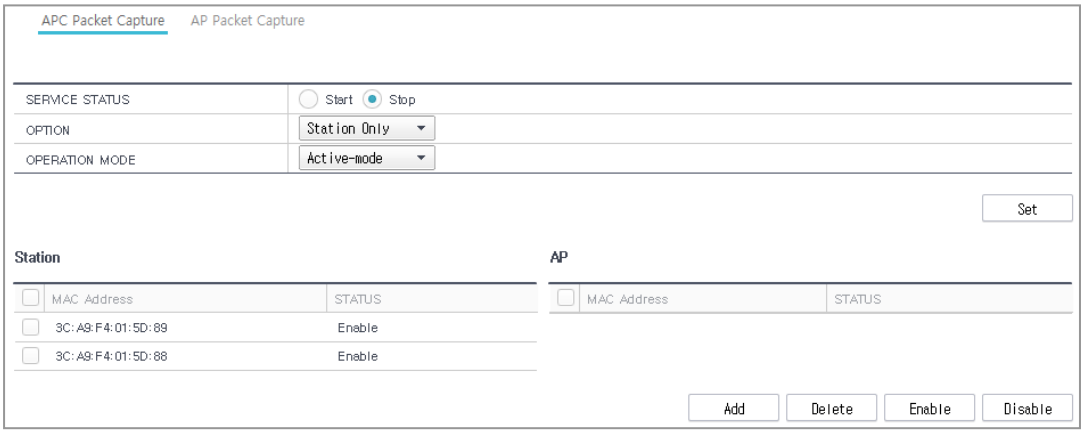


Figure 104. APC Packet Capture

'Packet Capture' menu provides a feature to retrieve and set the packet capture information on the APC.
Packet capture parameter are as follows:

Parameter	Description
SERVICE STATUS	Packet capture service status
OPTION	The target for packet capture (Station Only/AP Only/Station or AP/ Station and AP)
Operation mode	Packet capture operation mode. This must be set to remote-mode in order to access the packets of an APC from a remote PC.

[STATION]

Parameter	Description
MAC address	Set up the MAC address of a station where packet capture will be executed
Status	Packet capture service status

[AP]

Parameter	Description
MAC address	Set up the MAC address of an AP where packet capture will be executed
Status	Packet capture service status

Setting

1) Select ‘Tools’ → ‘Packet Capture’.
2) Packet capture settings appears on the screen.
3) Select the service that user want to use packet capture in ‘SERVICE STATUS’ item.
4) Select ‘Option’ in ‘OPTION’ item.
5) Click ‘Set’ button to save the settings.

Adding

1) Select ‘Tools’ → ‘Packet Capture’.
2) Packet capture settings appears on the screen.
3) Click ‘Set’ button and select STATION/AP and enter the MAC address of the device.
4) Click ‘Set’ button to save the settings.

Activating/Deactivating

1) Select ‘Tools’ → ‘Packet Capture’.
2) Packet capture settings appears on the screen.
3) Select the check box of the STATION/AP which you want activating/deactivating.
4) Click ‘Act/Deact’ button to save the settings.

General

The ‘**General**’ menu monitors and checks the operation status and its functions, and resources on the WEM server, and client side status, and also provides the various additional functions required to set up and control the operating environment.

The ‘General’ menu can be distinguished as follows:

- Surveillance
- Monitoring
- Resource Manager
- Statistics
- Database Manager
- Self Diagnosis
- Scheduler

6.3.2 AP Packet Capture

It provides a function of viewing or configuring the packet capture information set in the AP.

The packet capture items are as follows:

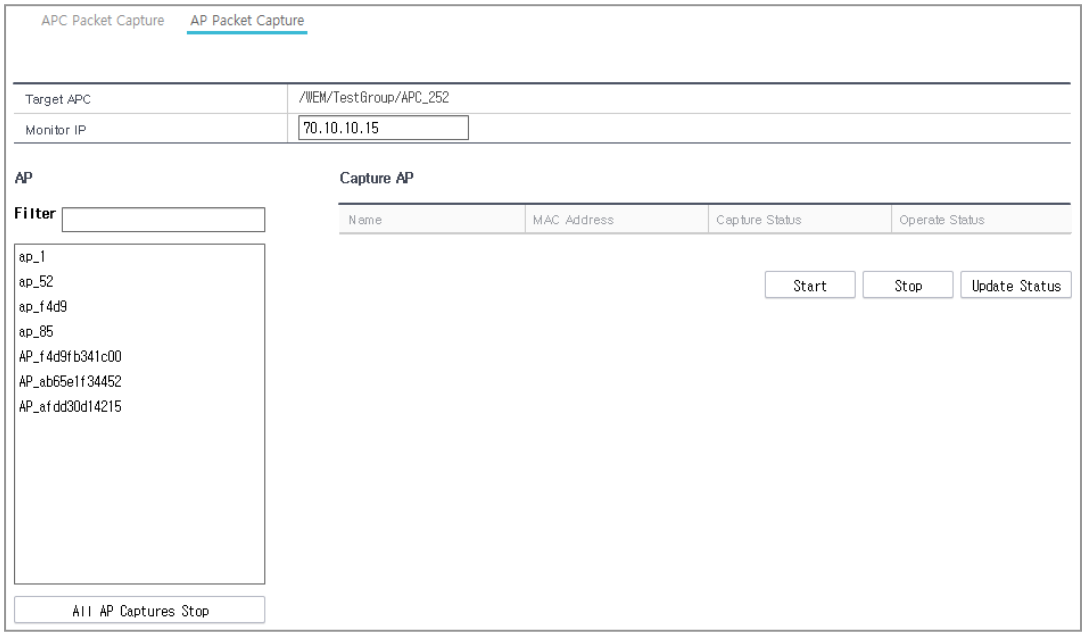


Figure 105. AP Packet Capture

Item	Description
Target APC	APC where an AP whose packet will be captured
Monitor IP	IP of the equipment which can receive the captured information from the wirelessly connected AP (PC or laptop)

[AP]

Item	Description
Filter	Enters a condition for filtering an AP to be retrieved. ex) If AB is entered, information on all APs whose name has AB is displayed.
Stopping Capture of All APs	Stops the captures of all APs which are set to be captured.

[Capture AP]

Item	Description
Name	Name of the AP to which packet capture will be performed

Item	Description
MAC Address	MAC address of the AP to which packet capture will be performed
Capture Status	Capture status of the selected AP
Operating Status	Operating status of the selected AP

Setup

1) Select the 'Tools' → 'Packet Capture' → 'AP' Packet Capture menu.
2) The packet capture-related configuration status is displayed on the screen.
3) Select the APC to use the packet capture service in 'Target APC'. To use the APC, you must select the desired APC by using the Tree menu.
4) Enter the condition of the AP you want to select in 'Filter'.
5) Select the AP to capture in the item and then it is automatically registered in the right capture AP.
6) Press the 'Start' button to start capturing.
7) Press the 'Stop' button to stop capturing.
8) Press the 'Refresh' button and then the present status is refreshed.
9) Press the 'Stop All AP Captures' button and then you can stop the captures of all APs belonging to the APC if the APs other than those currently selected are being captured.

Application to Release Capturing

1) Select the 'Tools' → 'Packet Capture' → 'AP' Packet Capture menu.
2) The packet capture-related configuration status is displayed on the screen.
3) Select the APC to use the packet capture service in 'Target APC'. To use the APC, you must select the desired APC by using the Tree Viewer. To see the TreeViewer, use the Show Tree Viewer button on the right top.
4) Check an AP you want to remove in 'Caputer AP'.
5) To release capturing, select the item of the AP in 'Capture AP' and then the item is removed.

6.3.3 Using Packet Capture Program

If the packet capture is used, the packet capture program must be used in the user's PC. To use Wireshark, follow the steps below:

Setup

1) Run Wireshark.
2) Open Capture Option in the program.
3) Set an interface of the option to monitor to be remote and set the IP of the APC for the APC packet capture and the IP of the AP for the AP packet capture.
4) Press the 'OK' button and then the 'Start' button.
5) The capture starts and the message is displayed.
6) To stop, press the 'Stop live capture' button.

CHAPTER 7. General

The '**General**' menu monitors and checks the operation status and its functions, and resources on the WEM server, and client side status, and also provides the various additional functions required to set up and control the operating environment.

The 'General' menu can be distinguished as follows:

- Surveillance
- Monitoring
- Resource Manager
- Database Manager
- Self Diagnosis
- Scheduler

7.1 Surveillance

7.1.1 Network Status

'Network Status' menu provides function to check network status of the nodes (AP, APC and Switch) periodically.

The parameters for the network status are as follows

Parameter	Description
NE INDEX	NE registered location
NE TYPE	Type of the NE (AP/APC/Switch)
LOCATION	NE Group Location
MASTER IP ADDRESS	The primary IP address of the NE
VICE IP ADDRESS	The vice IP address of the NE
PING STATUS	Using ICMP ping state
SNMP STATUS	SNMP agent state

Network State Retrieving

1) Select ‘General’ → ‘Surveillance’ → ‘Network Status’ to open Network status window.
2) Set the search conditions. ‘Target’ section, and then you want to look up the tree viewer from the main screen of the NE. Enter or select the ‘IP Address’ section you want to look up the IP address of the NE.
3) Click ‘Search’ button.
4) The search results will be displayed in the result table. it is depending on the search conditions set by user.
5) Real-time network status for specific Device displayed.
6) Click ‘Get’ button to update.
7) User can set interval in seconds (Min: 10 sec) to update the status periodically

7.1.2 Process Status

In this section provides information about WEM Process running status.
The Process Status function allows user to view the status of the processes running in the WEM server and stop or restart them. If a process is abnormal, user should stop and restart it. The WEM server maintains a process list. If a process is stopped in an abnormal way, the WEM sever restarts it automatically.

Process management parameters are as follows:

Parameter	Description
NAME	Displays Name of the Process
STATUS	Displays the status of the process (Running/Stop)
START TIME	Displays the start time of the process if it is running.
RESTART COUNTs	Displays number of times the process is restarted
PROCESS ID	Displays the ID of the process if it is running
CPU (%)	Displays percentage of CPU Utilization of the Running process
MEMORY USED/TOTAL (Mbyte)	Displays Total/Used Memory of the Running process
THREADs	Displays the number of Threads used for running process
DB CONNECTIONs USED/TOTAL	Displays DB Connections (Used/Total) summary of the Running process
LOG LEVEL	Displays at what level logs are created for the process.

Process Status

1) Select ‘General’ → ‘Surveillance’ → ‘Process Status’ menu to open running process window.
2) Click the ‘Search’ button to refresh the status of running process by recent information.

Stop and Restart the Process

1) Select ‘General’ → ‘Surveillance’ → ‘Process Status’ menu to open current running process window.
2) Select the process that user wants to stop or restart.
3) Click ‘Stop’ or ‘Restart’ button to perform the action.

Setting Log Level

The log level of the process are as follows, and higher log level log information is recorded in detail.

Log level: CONFIG > INFO > WARNING > SEVERE > OFF

- OFF: does not capture the log
- SEVERE: Information required to carry out the program
- WARNING: program to perform the low level of information
- INFO: The program to perform most of the information is displayed
- CONFIG: Not used

Perform the following steps to set the log level.

1) Select ‘General’ → ‘Surveillance’ → ‘Process Status’ to open current running process window.
2) Select the process that user wants to configure log level.
3) In the ‘Log level’ filed, Choose the desired log level in the drop down box.
4) Click ‘modify’ button to apply/save the settings.

7.2 Monitoring

'Monitoring' menu displays the CPU and Memory status of the Network, Network Interface of the state specific intervals.

Select 'General' → 'Monitoring'. The WEM resources of the state from the server periodically by measuring the state graph.

The parameters are as follows:

Item	Description
CPU Usage (%)	Current usage rate of database
CPU Usage History	CPU usage history after monitoring
Memory Usage (%)	Current memory usage rate
Memory Usage History	Memory usage history after monitoring
Network Usage History	Network usage history after monitoring

7.3 Resource Manager

The Resource Manager function monitors the status of the resources of the WEM server such as CPU, file system, memory, and database. user can set the alarm thresholds for each resource and the interval that the WEM server monitors each resource.

7.3.1 CPU

The CPU function allows user to view the usage of each CPU in the WEM server and set the alarm thresholds for CPU. If the server has more than one CPU, usage of each CPU is displayed. If the usage of a CPU of the WEM server exceeds a threshold, the corresponding alarm is generated.
The parameter of CPU are as follows:

Parameter	Description
RESOURCE	Displays the ID of the CPU.
USAGE (%)	Displays the current usage of the CPU.
USER (%)	Displays the CPU usage by user processes.
SYSTEM (%)	Displays the CPU usage by system processes.
WAIT IO (%)	Displays the CPU usage used for waiting for available IO resources.
IDLE (%)	Displays the ratio of idle state.

Retrieve CPU status

1) Select ‘General’ → ‘Resource Manager’ → ‘CPU’ to CPU status windows.
2) The CPU Status Results table is updated automatically (interval of 5 sec).
   Click Get button to refresh CPU status.
3) By clicking ‘Average’ button, the detailed information of each CPU ID is displayed.

Threshold Setting

1) Select ‘General’ → ‘Resource Manager’ → ‘CPU’.
2) Set the threshold value of CPU by each alarm level in ‘Threshold’ item.
3) Select whether to apply the alarm occurrence (Allow/Inhibit) in ‘InhibitFlag’ item, when the alarm is occurred more than threshold value.
4) Click ‘Set’ button to save the settings.

7.3.2 Memory

The Memory function allows user to view the usage of the memory in the WEM server and set the alarm thresholds for memory. Memory usage is the percentage of the currently used memory size to the total memory size. If the memory usage of the WEM server exceeds a threshold, the corresponding alarm is generated
The parameter of memory are as follows:

Parameter	Description
RESOURCE	Displays the type of the memory.
CURRENT STATUS (%)	Displays the current usage of the memory.
TOTAL SIZE (MBytes)	Displays the total size of the memory in units of MB.
USED SIZE (MBytes)	Displays the used size of the memory in units of MB.
FREE SIZE (MBytes)	Displays the unused size of the memory in units of MB.

Retrieve Memory Status

1) Select ‘General’ → ‘Resource Manager’ → ‘Memory’ to open Memory status window.
2) The Memory Status Results table is updated automatically (interval of 5 sec).
   Click ‘**Get’** button to refresh Memory status

Setting Threshold Value

1) Select ‘General’ → ‘Resource Manager’ → ‘Memory’ to open Memory status window.
2) Set the threshold value of memory by each alarm level in ‘Threshold’ item.
3) Select whether to apply the alarm occurrence (Allow/Inhibit) in ‘InhibitFlag’ item, when the alarm is occurred more than threshold value.
4) Click ‘**Set**’ button to save the setting.

7.3.3 File System

The File System function allows user to view the usage of the file systems in the WEM server and set the alarm thresholds for each file system. The usage information is displayed in detail for each file system. If the usage of a file system of the WEM server exceeds a threshold, the corresponding alarm is generated.
The parameter of file system are as follows:

Parameter	Description
RESOURCE	Displays the type of the file system.
CURRENT STATUS (%)	Displays the current usage of the file system.
TOTAL SIZE (MBytes)	Displays the total size of the file system in units of MB.
USED SIZE (MBytes)	Displays the used size of the file system in units of MB.
FREE SIZE (MBytes)	Displays the unused size of the file system in units of MB.

Retrieve File System State

1) Select ‘General’ → ‘Resource Manager’ → ‘File System’ to open File System status window.
2) The File System Status Results table is updated automatically (interval of 5 sec). Click Get button to refresh File system status.

Setting Threshold Value

1) Select ‘General’ → ‘Resource Manager’ → ‘File System’ to open File System status window.
2) Set the threshold value of File System by each alarm level in ‘Threshold’ item.
3) Select whether to apply the alarm occurrence (Allow/Inhibit) in ‘InhibitFlag’ item, when the alarm is occurred more than the threshold value.
4) Click ‘Set’ button to save the settings.

7.3.4 DB Usage

The Database function allows user to view the usage of the databases in the WEM server and set the alarm thresholds for each database. If the usage of a database of the WEM server exceeds a threshold, the corresponding alarm is generated.
Database parameters are as follows:

Parameter	Description
RESOURCE	Displays the type of the database
CURRENT STATUS (%)	Displays the current usage of the database
TOTAL SIZE (MBytes)	Displays the total size of the database in units of MB.
USED SIZE (MBytes)	Displays the used size of the database in units of MB.
FREE SIZE (MBytes)	Displays the unused size of the database in units of MB.

Retrieve Database State

1) Select ‘General’ → ‘Resource Manager’ → ‘DB Usage’ to open DB Usage status window.
2) The DB Usage Status Results table is updated automatically (interval of 5 sec). Click Get button to refresh File system status.

Setting Threshold Value

1) Select ‘General’ → ‘Resource Manager’ → ‘DB Usage’ menu.
2) Set the threshold value of DB usage by each alarm level in ‘Threshold’ item.
3) Select whether to apply the alarm occurrence (Allow/Inhibit) in ‘InhibitFlag’ item, when the alarm is occurred more than the threshold value.
4) Click ‘Set’ button to save the settings.

7.3.5 Network Interface

'Network Interface' menu provides to retrieve information on each network interface of WEM server.

The descriptions of the parameters are as follows:

Parameter	Description
RESOURCE	Network Interface type
IP ADDRESS	Interface IP address of WEM server
IN PACKET COUNTs (Bytes)	Size of packet received through the interface
IN ERROR	Count of error packet received through the interface
OUT PACKET COUNTs (Bytes)	Size of packet sent through the interface
OUT ERROR	Count of error packet sent through the interface
OUT COLLISION	Count of collision packet

Retrieve Network Interface State

1) Select 'General' → 'Resource Manager' → 'Network Interface' menu.
2) Displays the Network Interface's status.

7.4 Database Manager

7.4.1 Backup

The Backup function allows user to back up the database automatically or manually.
For manual backup, you can specify the backup range, backup device (location), and backup file name. For auto backup, you can register the daily, weekly, and monthly backup schedules.
The description of the output parameters are as follows:

Parameter	Description
Type	Backup range (Group/Table)
Execution	Backup execution mode (Auto/Manual)
Location	Backup device (Hard Disk)
Path	The path of the backup file
File Name	The name of the backup file
Schedule	Auto backup schedules - Type: Monthly/Weekly/Daily - DATE/DAY/HOUR/MINUTE
Total Tables	Total table lists (when the type is Table)
Selected Tables	Selected table lists (when the type is Table)

Manual Backup

1) Select ‘General’ → ‘Database Manager’ → ‘Backup’ menu.
2) Select any one of ‘Group’ or ‘Table’ option in the ‘Type’ field
3) In the ‘Execution’ field, select the ‘Manual’.
4) Enter the backup file name at the ‘File Name’ field.
5) If user choose ‘Table option in the backup type’, then select items in Total Table list and press arrow button to move the items to selected Tables’.
6) Click ‘Set’ button, to execute the manual backup.

Automatic backup

1) Select ‘General’ → ‘Database Manager’ → ‘Backup’.
2) Select any one of ‘Group’ or ‘Table’ option in the ‘Type’ field.
3) Select ‘Auto’ backup method in ‘Execution’ field.
4) Enter the backup file name in the ‘File Name’ item.
5) Select schedule type daily or weekly or monthly.
6) If user choose Table option in the backup type, then select items in Total Table list and press arrow button to move the items to selected tables.
7) Click ‘Set’ button, to save auto backup schedule.

7.4.2 Schedule

The Schedule function allows user to view the backup schedules and delete a registered backup schedule.
Schedule parameter are as follows:

Parameter	Description
Type	Backup range (Database, Group, Table)
Operator	The operator who registered the backup schedule
Period	Backup period type (Daily, Weekly, Monthly
Time	Backup start time
Information	Backup script
Register Time	The time that the backup schedule was registered

Backup Schedule View and Deleting

1) Select 'General' → 'Database Manager' → 'Schedule'.
2) Enter search condition in the search condition input table.
   - Select the backup rage (All, database, group, table) in 'Type'.
   - Select the backup period (All, Monthly, Weekly, Daily) in 'Period'.
3) Click 'Search' button.
4) Registered an automatic backup schedule results appears in the output table.
5) Delete Auto Backup, Select auto backup schedules that user want to delete in the Results table, then Click on Delete button.

7.4.3 Backup File

'Backup File' function allows user to view or delete the database backup information and restore a database using the corresponding backup information The descriptions of the result table parameters are as follows:

Parameter	Description
File Location	Location where the backup file is stored
File Name	Backup file name
Backup Time	Time when the backup file was created
Size	Size of the backup file

You can restore the database using the backup file, viewing detailed information, deletion as shown below:

1) Select 'General' → 'Database Manager' → 'Backup File'.
2) Select backup file type (All, Database, Group, Table) at 'Type' field.
3) Click 'Search' button.

4) The backup file information is displayed in the result table.
5) Select one of the backup files and select the desired button.
   - If you want to restore the database, click ‘Restore’ button.
   - If you want to check the detailed information, click ‘Detail’ button.
   - If you want to delete the backup file, click ‘Delete’ button.

7.4.4 History

The History function allows you to view the backup and restore histories.
The parameters of history are as follows:

Parameter	Description
Mode	Type of the history you want view (Backup/Restore)
Exec	Backup execution type (Auto/Manual)
File Location	Location where the backup file is stored
File Name	Backup file name
Execute Time	Start time of the backup/restore operation

Below is the procedure to display the backup/recovery history

1) Select ‘General’ → ‘Database Manager’ → ‘History’.
2) Enter the search conditions in the search input table.
   - Select the history command (Backup/Restore) in the ‘Command’ field.
   - Select the type (All, Database, Group, Table) in the ‘Type’ field.
   - Select the operator ID in the ‘Operator’ field.
   - Select the search period in the ‘Period’ field.
3) Select ‘Search’ button.
4) The backup/recovery history information displayed in the result table.

7.4.5 Storage Period

Storage Period function allows you to set the storage period for PM, FM, and SM raw data, and hourly, weekly, and monthly statistics data in the databases of the server.
Data is deleted automatically according to the periods configured.
The parameters for retention are as follows:

Parameter	Description
Raw Data Period	Raw data collected in the storage cycle
Hourly Data Period	Hourly Stats for data retention cycle
Daily Data Period	Daily Statistics data retention cycle
Monthly Data Period	Monthly statistical data retention cycle
Oper. Data Period	Operation log data retention cycle

Parameter	Description
Login Data Period	Login history data retention cycle

Must perform the following steps to view or set the storage period.

1) Select ‘General’ → ‘Database Manager’ → ‘Storage Period’.
2) Displays storage period information of each items.
   When you click the ‘Search’ button, retention time information is updated
3) To change the storage period for a type of data, select a storage period in the corresponding Period box and click Set button.

7.4.6 Diagnosis

The DB Status (Diagnosis) function diagnoses the current status of the database automatically. The diagnosis results can be Normal, Abnormal, or Fixed Diagnosis parameter are as follows:

[DB Status]

Parameter	Description
DB Test Name	DB diagnosis item
Result	DB diagnosis result (Normal, Fixed, Abnormal) - NORMAL: normal - FIXED: fixed problem - ABNORMAL: abnormal
Reason	Abnormal) Reason

Performing Diagnosis (DB) Status

1) Select ‘General’ → ‘Database Manager’ → ‘Diagnosis’.
2) The database self-diagnosis is performed and the results are displayed on the DB Status (Diagnosis) Window
3) By clicking Search button, the database self-diagnosis is performed again and the results are displayed.

7.5 Self Diagnosis

The Self Diagnosis function displays the RMI and DB connection status and event channel status of the processes running in the WEM server
Self Diagnosis parameters are as follows:

[IPC Status]

Parameter	Description
PROCESS NAME	Name of the Process
DB STATUS	The connection status between process and the database - Normal:  , Abnormal: 
RMI STATUS	The connection status between process and the RMI - Normal:  , Abnormal: 

[Event Channel Status]

Parameter	Description
PUBLISHER	The process that distributes events
LINK STATUS	The status of the link between processes. - Normal:  , Abnormal: 
SUBSCRIBER (ID)	The process that receives events.

Self Diagnosis Retrieving

1) Select ‘General’ → ‘Self Diagnosis’ menu.
2) IPC status and Event Channel status displayed in the output screen.
3) If you click Test on the Self Diagnosis window, the event channel status and IPC status are tested and the results are updated.

CHAPTER 8. Security

The security function allows you, as an administrator, to add, modify, search, and delete an operator so that only permitted operator can connect to the WEM system. You can also restrict the privilege and search various histories for an operator.
The ‘Security’ menu can be distinguished as follows:

- User Manager
- Change Password
- Group Manager
- IP Manager
- Login History
- Operation History

8.1 User Manager

8.1.1 User Manager

The User Manager function allows you to set, view, modify, and delete the operator ID, operator information, privilege, and command range for each operator.
The parameters for the user management are as follows:

Parameter	Description
User ID	Operator ID
Privilege	Operator Level (All/Administrator/Operator/Monitor/Guest/Lobby Ambassador)
Status	User’s status (All/Enable/Disable/Lockout/Password Initialized)
Group	Operator group. Each group has its own NE to manage. The operator of the highest level should select ‘Default group’.


NOTE

User ID and Input Password

A user ID can be 5 to 20 characters long and a password can be a combination of alphabets and numbers and must be 8 to 12 characters long.

NOTE

Restrictions for changing password

The password can be changed once a day, you cannot use recently used password.

Searching Users

1) Select ‘Security’ → ‘User Manager’ → ‘User Manager’ to open user manager menu window.
2) Currently registered users information are displayed in the result table.
3) Enter the search criteria to search for specific conditions. You can search by group, ID privileged, state-specific, etc.
4) Click ‘Search’ button.
5) The search results will be displayed in the result table.
6) Select an operator in the Results table, the detailed information for the selected operator is displayed on the User Profile window right to the Results table.

User Registration

1) Select ‘Security’ → ‘User Manager’ → ‘User Manager’ menu.
2) Click ‘Add’ button.
3) The operator registration window appears on the right side of the window.
4) Enter operator information.
   - Enter the operator user ID, password in the ‘User ID’, ‘Password’ and ‘Re-Password’ item.
   - Setting user level at the ‘Privilege’. Set NE Group ‘Group’ claim that user can be managed.
   - Enter the login session count single or multiple (Same User ID can be used simultaneously for different user login access if multiple login type selected).
5) By clicking ‘OK’ button, the result of registration will be shown in the result table.

Modifying User Information

1) Select ‘Security’ → ‘User Manager’ → ‘User Manager’.
2) Select a user to change from the results table.
3) Click ‘Modify’ button.
4) A window to modify the user information appears at the setting table on the right side of the window.
5) Change the user information.
   - Setting operator level at the ‘Privilege’.
   - Set ‘Group’ claim that can be managed by the operator in the NE group.
   - ‘Status’ claim to the operator state.
   - ‘Select the Login type (Single or Multiple)
   - Enter e-mail and phone number, etc.
6) By clicking ‘OK’ button, to modify the information and update in the result table.

Delete User Information

1) Select ‘Security’ → ‘User Manager’ → ‘User Manager’.
2) Select a user to delete from the result table.
3) Click ‘Delete’ button.
4) When the password input window appears, enter the user’s password.
5) By clicking ‘OK’ button, the changed information is reflected and displayed in the result table. At this time, a client who is logged in with the deleted user ID will be terminated forcefully.

8.1.2 Command Manager

The Command Manager function allows user to view a list of the commands that an WEM operator can perform and set the privilege to access to menu and command for each operator.

Restricting menu by user

1) Select ‘Security’ → ‘User Manager’ → ‘Command Manager’.
2) Select User ID and Click Search button 3.
3) Search results are displayed and user can view the commands allowed to selected User ID.
4) Operator can add/modify/remove commands for specific user ID.
5) Click Save button to save the settings.

8.2 Change Password

This function allows you to change the password of an user who is currently logged in.

Change Password

1) Selecting ‘Security’ → ‘Change Password’, to open the changing password window.
2) To change the password, enter the old password, new password, and new password again for confirmation in the Change Password window
3) Click ‘OK’ button to change password.


NOTE

Operator password

A user password can be a combination of alphabets and numbers and must be 8 to 12 characters long.


NOTE

Restrictions for changing password

The password can be changed once a day, you cannot use recently used password.

8.3 Group Manager

The Group Manager function allows you to make a grouping for network elements for efficient and easier management.
The parameters for the group management are as follows:

Parameter	Description
Group Name	The group name of the network
Configuration Info.	Configuration Information
User List	User list of registered group
Comment	Comment

Search Group

1) Select 'Security' → 'Group Manager'.
2) The information of the currently registered group is displayed in the result table.
3) Click 'Search' button to refresh the registered group information.
4) Select the Group to check the detailed information
5) The detailed information of the selected group is displayed on the right side of the window.

Add a Group

1) Select 'Security' → 'Group Manager'.
2) Click 'Add' button.
3) The Register Group window is displayed to the right of the Results table. Enter the group name and select the elements to include to the group.
   Click OK button on the Register Group window. Check whether the group you added is displayed in the Results table.

Modify Group Information

1) Select 'Security' → 'Group Manager'.
2) Select the group you want to modify in the Results table. However, you cannot modify the default group.
3) Check whether the detailed information for the selected group is displayed at the right to the Results table.
4) Click Modify button at the bottom of the Group Manager window. Change the elements to include to the selected group on the Change Group Information window.
5) Click OK button on the Change Group Information window.

Delete a Group

1) Select ‘Security’ → ‘Group Manager’.
2) Select the group you want to delete in the Results table. However, you cannot delete the default group.
3) Click Delete button at the bottom of the Group Manager window.
4) Click OK button in the confirm message box displayed.
5) The changed information is reflected and displayed in the result table.

8.4 IP Manager

The IP Manager function allows user to set whether to permit log-in for each client IP address and manage the number of sessions that can be opened at the same time.
The parameters for IP management are as follows:

Parameter	Description
IP Address	IP address of the wireless terminal
Login Allowance	Sets whether to permit log-in for the IP address. If set to Allow, the operator can log in to the system from that IP address. If set to Deny, the operator cannot log in from that IP address. - Allow: Login from the registered IP is allowed. - Deny: Login from the registered IP is not allowed.
Sessions	The maximum number of sessions that can be opened simultaneously from the IP address when Login Allowance is set to Allow.
Description	Description of the IP address

Searching the IP

1) Select ‘Security’ → ‘IP Manager’ menu.
2) This shows information about the IP addresses which are currently registered.
3) Enter the search conditions at ‘Login Allowance’ and ‘IP Address’ items.
4) Click ‘Search’ button.
5) The search results will be displayed in the result table.
6) Enter IP address at the ‘Select’ item to view detailed information.
7) The detailed IP information of the selected group is displayed on the right side of the window.

Registering an IP

1) Select ‘Security’ → ‘IP Manager’.
2) Click ‘Add’ button.
3) The IP registration window appears on the setting table of the right side.
4) Enter IP information.
   - Enter the IP address at the ‘IP Address’ field.
   - At ‘Login Allowance’ field, Choose Allow or Deny.
   - At ‘Session’ field, enter the number of sessions that can be logged in simultaneously.
5) By clicking ‘OK’ button, the registered IP information is displayed on the searching result table. However, if the ‘Login Allowance’ is set to ‘Deny’, the client that was being operated in the IP address is forced to terminate.

Modify the IP Address

1) Select ‘Security’ → ‘IP Manager’.
2) In ‘Select’ field, select IP address to change in the result table.
3) Click ‘Modify’ button.
4) The IP changing window appears.
5) Modify IP Information.
   - At ‘Login Allowance’ field, Choose Allow to Deny.
   - At ‘Session’ field, enter the number of sessions that can be logged in simultaneously.
6) By clicking ‘OK’ button, the registered IP information is displayed on the searching result table. However, if the ‘Login Allowance’ is set to ‘Deny’, the client that was being operated in the IP address is forced to terminate.

Deleting an IP

1) Select ‘Security’ → ‘IP Manager’.
2) At ‘Select’ field, select the IP address to delete in the result table.
3) Click ‘Delete’ button.
4) The deletion confirmation window appears, click ‘OK’ button.
5) The changed information is reflected and displayed in the result table. However, if any client is currently operated in the IP address being deleted, the client will be forced to terminate.

8.5 Login History

The Login History function allows user to search the database of WEM server for the operators who connected to and operated the system and the operators that are in a session currently.

8.5.1 Login History

The Login History function allows user to view the login and logout history of the users. You can view the history of all the login tries to the WEM for each user.
The parameters for the login history are as follows:

Parameter	Description
User ID	The ID of the logged-in user
IP Address	The IP address of the client
Login Time	The time that the user logged in
Logout Time	The time that the user logged out
Success/Fail	Displays whether the user logged in successfully or not.
Login Fail Reason	Displays the reason if the login failed.
Logout Status	Displays the logout status

Searching the Login History

1) Select ‘Security’ → ‘Login History’ → ‘Login History’.
2) Enter the search conditions in the search condition input table (The search conditions are user ID, IP address, login success/fail, and period.).
3) Click ‘Search’ button.
4) The login history search results are displayed in the result table.
5) Click the ‘Save’ button to save the searched data in an Excel file or text file.

8.5.2 Login Session

The Logon Session function allows user to search the information of for the users who are being logged in to the WEM server and close a specific session forcibly if necessary.
The parameters for the logon session are as follows:

Parameter	Description
User ID	The ID of the logged-in user.
Privilege	The level of the logged-in user
IP Address	The IP address of the client
Login Time	The time that the user logged in

Searching the Login Session

1) Select ‘Security’ → ‘Login History’ → ‘Login Session’.
2) The sessions that are currently logged in are displayed. Click the ‘Search’ button to search the logged in session information again.
3) Select the session that you want to close forcibly in the Results table.
   Click Delete button on the Logon Session window. The selected session is closed forcibly.
4) Check whether the session you closed forcibly is deleted from the Results table.

8.6 Operation History

The Operation History function allows user to search the database of the WEM server for various operation histories. The search conditions are User ID, Function, Message, Command, and Period.
The parameters for the operation log are as follows:

Parameter	Description
User ID	The ID of the Logged in user
Target	The target on which the command was executed
Function	The WEM block that used the command.
Message	The type of the command
Request/Response Time	The time that the command was requested/Executed
IP Address	The IP address of the client that executed the command
Command	The command that was executed.
Result	Command execution result
Fail Reason	The reason of the failed command
Additional Info	The parameters used when the command was executed.

Searching the Operation History

1) Select 'Security' → 'Operation History'.
2) Select the system for which you want to search the operation history in the Tree View. The selected system is displayed on the Target field in the input table.
3) Enter the search conditions you want, such as Period, User ID, Function, Message, Command, in the input table.
   - Enter a operator ID in the 'User ID' field.
   - Select the type in the 'Function' field.
   - Select the command type separator in the 'Message' field.
   - Enter the command in the 'Command' field.
   - Set the search period in the 'Period' field.
4) Click 'Search' button.
5) The operation log search results are displayed in the result table.
6) Click the '**Save**' button to save the searched data in an Excel file or a text file.

CHAPTER 9. Help

Help is used to view the following information of the WEM server. The server information shows package version and build date.

Figure 106. WEM Help Window

ANNEX A. Alarm List

Cross check all the description which are not clear.

Alarm Code	Alarm Name	Description
856	Software Down	A specific software block is abnormal.
863	CPU Load Alarm	This occurs if the CPU usage rate of the system is higher than the set threshold.
864	Memory Usage Alarm	This occurs if the memory usage rate of the system is higher than the set threshold.
865	Disk Usage Alarm	This occurs if the disk usage rate of the system is higher than the set threshold.
866	Fan RPM Alarm	This occurs if the fan level of the system is higher than the set threshold.
867	System Temperature Alarm	An alarm that occurs if the temperature of the system exceeds the set threshold.
868	System Thermal Runaway	An alarm that occurs if the temperature of the system normal operating the set threshold.
877	DHCP Sever Connect Failure	This alarm occurs when the communication between the DHCP server and the system.
878	DNS Server Connect Failure	This alarm occurs when the communication between the DNS server and the system.
879	NTP Server Connect Failure	This alarm occurs when the communication between the NTP server and the system.
931	Fan Fail alarm	This alarm occurs when the operation speed (rpm) out of range in the fan operation status.
936	Temperature Sensor Fail	It occurs when a temperature sensor increases abnormally.
937	Power Module Fail	It occurs when a power supply module increases abnormally.
945	DISK Full	This occurs if the disk usage is 99 % or higher.
946	DISK Rate High	This occurs if the disk usage rate of the system is higher than the set threshold. This alarm occurs when disk usage rate is more than 1 MBytes/sec and continue for more than 60 minutes.

Alarm Code	Alarm Name	Description
947	DISK Rate High (Shortterm)	This occurs if the disk usage rate of the system is higher than the set short term threshold. This alarm occurs when disk usage rate is more than 50 MBytes/sec and continue for more than 5 minutes.
1001	Duplicated IP	This alarm occurs when IP address conflict.
1002	No Radio	This alarm occurs when all BSS of the AP are deleted and the mobile service is impossible.
1013	AP BSS Down	This alarm occurs when the beacon of the specific BSS is not sensed for the predetermined time.
1016	AP Down	In case when AP and connection were cut off, or a shutdown made the AP connection link compulsorily, AP down message happened, and AP and connection were again recommenced, AP Down is lifted.
1023	AP CPU Load High	This occurs if the CPU load rate of the AP is higher than 90 % the set threshold.
1025	AP MEM Usage High	This occurs if the memory usage rate of the AP is higher than 70 % the set threshold.
1027	Monitor Device Fail	This alarm occurs if the system with RF monitor device has communication filature for the predetermined time.
1031	Radio (2.4G or 5G) TX failure	This alarm occurs in case the obstacle to the specification Radio (2.4 G or 5 G) happens and the relevant airwave Tx doesn’t accomplish.
1041	AP Disk usage high	This alarm occurs in case of exceeding 70 % in which the usage value of AP user disk (configs) is the Threshold value an alarm happens.
1103	CAC Minor Calls	This alarm occurs when I generate the minor alarm threshold which the Radio of AP sets particularly over during the call try and the bids falls into the threshold or less.
1104	CAC Major Calls	This alarm occurs when I generate the major alarm threshold which the Radio of AP sets particularly over during the call try and the bids falls into the threshold or less, the alarm this is lifted.
1175	CLUSTER APC Lost Connection	In case the connection with APC comprising CLUSTER with the happening alarm among CLUSTER operation is cut off, I happen.
1177	VCC Connection Down	This alarm occurs when SCME connection for the VCC (Voice Call Continuity) is failure.
1221	Radius Servers Failed	This alarm occurs when the all RADIUS server occur communication failure.
1301	NET Link Dn	This alarm occurs when interface link is down.
1485	NFM Restart	This alarm occurs when the forwarding engine is restart.

Alarm Code	Alarm Name	Description
2001	EMS Process Alarm [Server Process Down]	This alarm occurs when WEM server process goes down.
2002	EMS Resource Alarm [HDD]	This alarm occurs when hard disk usage rate exceeds the threshold.
2003	EMS Resource Alarm [DB]	This alarm occurs when database usage rate exceeds the threshold.
2004	EMS Resource Alarm [Memory]	This alarm occurs when memory usage rate exceeds the threshold.
2006	Protocol Status [Communication Fail: TL1/SNMP/…}	Communication fail: TL1/SNMP/….
2007	Protocol Status [Communication Fail: Ping]	Communication fail: ping fail.
2008	EMS Resource Alarm [CPU]	This alarm occurs when CPU usage rate exceeds the threshold.

ANNEX A. Open Source Announcement

Some software components of this product incorporate source code covered under the Mozilla Public License (MPL), the GNU Lesser General Public License (LGPL) and BSD License etc.

Acknowledgement:

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)

The software included in this product contains copyrighted software that is licensed under the LGPL. You may obtain the complete Corresponding Source code from us for a period of three years after our last shipment of this product by sending email to: oss.request@samsung.com

If you want to obtain the complete Corresponding Source code in the physical medium such as CD-ROM, the cost of physically performing source distribution may be charged. You may also find a copy of the source at http://opensource.samsung.com/

This offer is valid to anyone in receipt of this information.

Below is the list of components covered under GNU General Public License, the GNU Lesser General Public License and BSD License etc.

Component	License
Apache Jakarta Commons BeanUtils	Apache License 1.1
Apache Jakarta Commons Digester	Apache License 1.1
Apache Jakarta Commons Discovery	Apache License 1.1
Apache Jakarta Commons EL	Apache License 1.1
Apache Tomcat	Apache License 1.1
Apache Xerces Java XML Parser	Apache License 1.1
Apache Xerces Java XML Parser	Apache License 2.0
Apache Ant	Apache License 2.0

Component	License
Apache Axis2/Java	Apache License 2.0
Apache Commons Collections (for Apache Directory Studio)	Apache License 2.0
Apache Commons FileUpload	Apache License 2.0
Apache Commons Logging (for Apache Directory Studio)	Apache License 2.0
Apache Geronimo	Apache License 2.0
Apache Jakarta Commons Codec	Apache License 2.0
Apache Jakarta Commons Digester	Apache License 2.0
Apache Jakarta Commons Email	Apache License 2.0
Apache Jakarta Commons IO	Apache License 2.0
Apache Jakarta Commons Lang	Apache License 2.0
Apache Jakarta Commons Logging	Apache License 2.0
Apache Jakarta HTTP Client	Apache License 2.0
Apache Log4j	Apache License 2.0
Apache Neethi	Apache License 2.0
Apache POI	Apache License 2.0
Apache POI-org.apache.poi:poi-ooxml	Apache License 2.0
Apache POI-org.apache.poi:poi-ooxml-schemas	Apache License 2.0
Apache ServiceMix::Bundles::wsdl4j	Apache License 2.0
Apache ServiceMix OSGI Common Bundles: jaxb-api	Apache License 2.0
Apache ServiceMix OSGI Common Bundles: jaxb-impl	Apache License 2.0
Apache Struts	Apache License 2.0
Apache Velocity	Apache License 2.0
Apache Xerces Java 1 XML Parser	Apache License 2.0
Apache XML Security Java	Apache License 2.0
Apache XML Xalan-Java	Apache License 2.0
Apache XMLBeans	Apache License 2.0
Apache XML-Commons Resolver	Apache License 2.0
Apache-Ant	Apache License 2.0
Apache-Jakarta BeanUtils	Apache License 2.0
Apache-Jakarta Collections	Apache License 2.0
Apache-Jakarta Digester	Apache License 2.0
Apache-Jakarta Net	Apache License 2.0
Apache-Jakarta Pool	Apache License 2.0
buildr-jaxb-xjc	Apache License 2.0
catalina-ant	Apache License 2.0
Commons BeanUtils Bean Collections	Apache License 2.0
Commons Collections	Apache License 2.0

Component	License
Commons DBCP	Apache License 2.0
Commons Lang	Apache License 2.0
Commons Net	Apache License 2.0
dom4j (for Apache Directory Studio)	Apache License 2.0
jaas	Apache License 2.0
Jakarta Commons-Logging	Apache License 2.0
jasper-compiler	Apache License 2.0
jasper-runtime	Apache License 2.0
Java Image Filters	Apache License 2.0
jsp-api	Apache License 2.0
JTA 1.0.1B	Apache License 2.0
Log4j (for Apache Directory Studio)	Apache License 2.0
Quartz	Apache License 2.0
servlet-api	Apache License 2.0
SNMP4J	Apache License 2.0
SNMP4J Agent	Apache License 2.0
Spring Framework: Beans	Apache License 2.0
Spring Framework: Core	Apache License 2.0
struts	Apache License 2.0
Woodstox	Apache License 2.0
Xalan Java	Apache License 2.0
Xerces2 Java Parser	Apache License 2.0
Xerces2-j-xerces: xercesImpl	Apache License 2.0
XML Commons External Components XML APIs	Apache License 2.0
XML Commons External Components XML APIs Extensions	Apache License 2.0
XmlBeans	Apache License 2.0
jlayout	BSD License
MSV XML Schema Library	BSD License
relaxng-datatype (java)	BSD License
JAXB 2.0 Project	CDDL 1.0
Cryptix JCE	Cryptix General License
CyberNeko HTML Parser-(NekoHTML)	CyberNeko Software License 1.0
DOM4J-Flexible XML Framework for Java	dom4j License (BSD 2.0 +)
jaxen	Jaxen License
JDOM	Jdom License
DynamicReports-core	LGPL 2.1
iText, a JAVA-PDF library	LGPL 2.1

Component	License
JasperReports	LGPL 2.1
JFreeChart-1. JFreeChart	LGPL 2.1
JFreeChart-3. JCommon	LGPL 2.1
SwingX	LGPL 2.1
LIBSMI-Main	Libsmi License
AIRforiOSLoadExternalSWFTest	MIT License
FlexDock	MIT License
httpunit	MIT License
jmockit	MIT License
jQuery JavaScript Library	MIT License
jqueryclient	MIT License
jqueryui-module	MIT License
Simple AJAX Code-Kit-SACK	MIT License
SLF4J API Module	MIT License
SLF4J JDK14 Binding	MIT License
swfobject	MIT License
iText, a JAVA-PDF library	Mozilla Public License 1.1
Mozilla Rhino: JavaScript for Java	Mozilla Public License 1.1
JavaMail	Sun JavaMail 1.4 License

Apache 1.0 License

==========

Copyright(c) 1995-1999 The Apache Group. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
   “This product includes software developed by the Apache Group for use in the Apache HTTP server project
   (http://www.apache.org/).”
4. The names “Apache Server” and “Apache Group” must not be used to endorse or promote products derived from this software without prior written permission.
   For written permission, please contact apache@apache.org.

5. Products derived from this software may not be called “Apache” nor may “Apache” appear in their names without prior written permission of the Apache Group.
6. Redistributions of any form whatsoever must retain the following acknowledgment: “This product includes software developed by the Apache Group for use in the Apache HTTP server project (http://www.apache.org/).”

THIS SOFTWARE IS PROVIDED BY THE APACHE GROUP “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED.
IN NO EVENT SHALL THE APACHE GROUP OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

This software consists of voluntary contributions made by many individuals on behalf of the Apache Group and was originally based on public domain software written at the National Center for Supercomputing Applications, University of Illinois, Urbana-Champaign. For more information on the Apache Group and the Apache HTTP server project, please see {http://www.apache.org/}.

Apache License

Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

“License” shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

“Licensor” shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

“Legal Entity” shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity.
For the purposes of this definition, “control” means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50 %) or more of the outstanding shares, or (iii) beneficial ownership of such entity. “You” (or “Your”) shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear.

The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and provide additional or different license terms and conditions use, reproduction, or distribution of Your modifications, or any such Derivative Works as a whole, provided Your use, roduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]" replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

BSD 2.0 License

Copyright(c) <YEAR>, <OWNER>
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of the <ORGANIZATION> nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

COMMON DEVELOPMENT AND DISTRIBUTION LICENSE (CDDL) Version 1.0

1. Definitions.

1.1. “Contributor” means each individual or entity that creates or contributes to the creation of Modifications.

1.2. “Contributor Version” means the combination of the Original Software, prior Modifications used by a Contributor (if any), and the Modifications made by that particular Contributor.

1.3. “Covered Software” means (a) the Original Software, or (b) Modifications, or (c) the combination of files containing Original Software with files containing Modifications, in each case including portions thereof.

1.4. “Executable” means the Covered Software in any form other than Source Code.

1.5. “Initial Developer” means the individual or entity that first makes Original Software available under this License.

1.6. “Larger Work” means a work which combines Covered Software or portions thereof with code not governed by the terms of this License.

1.7. “License” means this document.

1.8. “Licensable” means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. “Modifications” means the Source Code and Executable form of any of the following:

A. Any file that results from an addition to, deletion from or modification of the contents of a file containing Original Software or previous Modifications;

B. Any new file that contains any part of the Original Software or previous Modification; or

C. Any new file that is contributed or otherwise made available under the terms of this License.

1.10. “Original Software” means the Source Code and Executable form of computer software code that is originally released under this License.

1.11. “Patent Claims” means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.12. “Source Code” means (a) the common form of computer software code in which modifications are made and (b) associated documentation included in or with such code.

1.13. “You” (or “Your”) means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License. For legal entities, “You” includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, “control” means (a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50 %) of the outstanding shares or beneficial ownership of such entity.

2. License Grants.

2.1. The Initial Developer Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, the Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer, to use, reproduce, modify, display, perform, sublicense and distribute the Original Software (or portions thereof), with or without Modifications, and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using or selling of Original Software, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Software (or portions thereof).

(c) The licenses granted in Sections 2.1 (a) and (b) are effective on the date Initial Developer first distributes or otherwise makes the Original Software available to a third party under the terms of this License.

(d) Notwithstanding Section 2.1 (b) above, no patent license is granted: (1) for code that You delete from the Original Software, or (2) for infringements caused by: (i) the modification of the Original Software, or (ii) the combination of the Original Software with other software or devices.

2.2. Contributor Grant.

Conditioned upon Your compliance with Section 3.1 below and subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license:

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof), either on an unmodified basis, with other Modifications, as Covered Software and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: (1) Modifications made by that Contributor (or portions thereof); and (2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) The licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first distributes or otherwise makes the Modifications available to a third party.

(d) Notwithstanding Section 2.2 (b) above, no patent license is granted: (1) for any code that Contributor has deleted from the Contributor Version; (2) for infringements caused by: (i) third party modifications of Contributor Version, or (ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or (3) under Patent Claims infringed by Covered Software in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Availability of Source Code.

Any Covered Software that You distribute or otherwise make available in Executable form must also be made available in Source Code form and that Source Code form must be distributed only under the terms of this License.

You must include a copy of this License with every copy of the Source Code form of the Covered Software You distribute or otherwise make available.

You must inform recipients of any such Covered Software in Executable form as to how they can obtain such Covered Software in Source Code form in a reasonable manner on or through a medium customarily used for software exchange.

3.2. Modifications.

The Modifications that You create or to which You contribute are governed by the terms of this License. You represent that You believe Your Modifications are Your original creation(s) and/or You have sufficient rights to grant the rights conveyed by this License.

3.3. Required Notices.

You must include a notice in each of Your Modifications that identifies You as the Contributor of the Modification. You may not remove or alter any copyright, patent or trademark notices contained within the Covered Software, or any notices of licensing or any descriptive text giving attribution to any Contributor or the Initial Developer.

3.4. Application of Additional Terms.

You may not offer or impose any terms on any Covered Software in Source Code form that alters or restricts the applicable version of this License or the recipients rights hereunder. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Software. However, you may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear that any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.5. Distribution of Executable Versions.

You may distribute the Executable form of the Covered Software under the terms of this License or under the terms of a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable form does not attempt to limit or alter the recipient’s rights in the Source Code form from the rights set forth in this License. If You distribute the Covered Software in Executable form under a different license, You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.6. Larger Works.

You may create a Larger Work by combining Covered Software with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Software.

4. Versions of the License.

4.1. New Versions.

Sun Microsystems, Inc. is the initial license steward and may publish revised and/or new versions of this License from time to time. Each version will be given a distinguishing version number. Except as provided in Section 4.3, no one other than the license steward has the right to modify this License.

4.2. Effect of New Versions.

You may always continue to use, distribute or otherwise make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. If the Initial Developer includes a notice in the Original Software prohibiting it from being distributed or otherwise made available under any subsequent version of the License, You must distribute and make the Covered Software available under the terms of the version of the License under which You originally received the Covered Software. Otherwise, You may also choose to use, distribute or otherwise make the Covered Software available under the terms of any subsequent version of the License published by the license steward.

4.3. Modified Versions.

When You are an Initial Developer and You want to create a new license for Your Original Software, You may create and use a modified version of this License if You: (a) rename the license and remove any references to the name of the license steward (except to note that the license differs from this License); and (b) otherwise make it clear that the license contains terms which differ from this License.

5. DISCLAIMER OF WARRANTY.

COVERED SOFTWARE IS PROVIDED UNDER THIS LICENSE ON AN “AS IS” BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED SOFTWARE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED SOFTWARE IS WITH YOU. SHOULD ANY COVERED SOFTWARE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED SOFTWARE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

6.TERMINATION.

6.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

6.2. If You assert a patent infringement claim (excluding declaratory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You assert such claim is referred to as "Participant") alleging that the Participant Software (meaning the Contributor Version where the Participant is a Contributor or the Original Software where the Participant is the Initial Developer) directly or indirectly infringes any patent, then any and all rights granted directly or indirectly to You by such Participant, the Initial Developer (if the Initial Developer is not the Participant) and all Contributors under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively and automatically at the expiration of such 60 day notice period, unless if within such 60 day period You withdraw Your claim with respect to the Participant Software against such Participant either unilaterally or pursuant to a written agreement with Participant.

6.3. In the event of termination under Sections 6.1 or 6.2 above, all end user licenses that have been validly granted by You or any distributor hereunder prior to termination (excluding licenses granted to You by any distributor) shall survive termination.

7. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED SOFTWARE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOST PROFITS, LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

8. U.S. GOVERNMENT END USERS.

The Covered Software is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" (as that term is defined at 48 C.F.R. 252.227-7014 (a)(1)) and "commercial computer software documentation" as such terms are used in 48 C.F.R. 12.212 (Sept. 1995).

Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Software with only those rights set forth herein. This U.S. Government Rights clause is in lieu of, and supersedes, any other FAR, DFAR, or other clause or provision that addresses Government rights in computer software under this License.

9. MISCELLANEOUS.
This License represents the complete agreement concerning subject matter hereof.
If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by the law of the jurisdiction specified in a notice contained within the Original Software (except to the extent applicable law, if any, provides otherwise), excluding such jurisdiction's conflict-of-law provisions. Any litigation relating to this License shall be subject to the jurisdiction of the courts located in the jurisdiction and venue specified in a notice contained within the Original Software, with the losing party responsible for costs, including, without limitation, court costs and reasonable attorneys' fees and expenses.
The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License. You agree that You alone are responsible for compliance with the United States export administration regulations (and the export control laws and regulation of any other countries) when You use, distribute or otherwise make available any Covered Software.

10. RESPONSIBILITY FOR CLAIMS.
As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

Cryptix General License

Copyright(c) 1995-2004 The Cryptix Foundation Limited. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE CRYPTIX FOUNDATION LIMITED AND CONTRIBUTORS “AS IS” AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE CRYPTIX FOUNDATION LIMITED OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The CyberNeko Software License, Version 1.0

(c) Copyright 2002, 2003, Andy Clark. All rights reserved.
Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The end-user documentation included with the redistribution, if any, must include the following acknowledgment: “This product includes software developed by Andy Clark.” Alternately, this acknowledgment may appear in the software itself, if and wherever such third-party acknowledgments normally appear.
4. The names “CyberNeko” and “NekoHTML” must not be used to endorse or promote products derived from this software without prior written permission.
   For written permission, please contact andy@cyberneko.net.
5. Products derived from this software may not be called “NekoHTML”, nor may “NekoHTML” appear in their name, without prior written permission of the author.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR OTHER CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
==========

This license is based on the Apache Software License, version 1.1.

dom4j License

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name “DOM4J” must not be used to endorse or promote products derived from this Software without prior written permission of MetaStuff, Ltd. For written permission, please contact dom4j-info@metastuff.com.
4. Products derived from this Software may not be called “DOM4J” nor may “DOM4J” appear in their names without prior written permission of MetaStuff, Ltd. DOM4J is a registered trademark of MetaStuff, Ltd.
5. Due credit should be given to the DOM4J Project-http://www.dom4j.org

THIS SOFTWARE IS PROVIDED BY METASTUFF, LTD. AND CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL METASTUFF, LTD. OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

jaxen License

Redistribution and use of this software and associated documentation (“Software”), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices. Redistributions must also contain a copy of this document.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The name “jaxen” must not be used to endorse or promote products derived from this Software without prior written permission of The Werken Company. For written permission, please contact bob@werken.com.
4. Products derived from this Software may not be called “jaxen” nor may “jaxen” appear in their names without prior written permission of The Werken Company. “jaxen” is a registered trademark of The Werken Company.
5. Due credit should be given to The Werken Company. (http://jaxen.werken.com/).

THIS SOFTWARE IS PROVIDED BY THE WERKEN COMPANY AND CONTRIBUTORS “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE WERKEN COMPANY OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

jdom License

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name “JDOM” must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact {request_AT_jdom_DOT_org}.
4. Products derived from this software may not be called “JDOM”, nor may “JDOM” appear in their name, without prior written permission from the JDOM Project Management {request_AT_jdom_DOT_org}.

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following:

“This product includes software developed by the JDOM Project (http://www.jdom.org/).”

Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED “AS IS” AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.
This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.
When we speak of free software, we are referring to freedom of use, not price.
Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.
To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.
For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.
To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author’s reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program.
We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.
Most GNU software, including some libraries, is covered by the ordinary GNU General Public License.
This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.
When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs.
These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.
For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard.
To achieve this, non-free programs must be allowed to use the library.
A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.
In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software.
For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.
The precise terms and conditions for copying, distribution and modification follow.
Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0) This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1) You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2) You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:
   a) The modified work must itself be a software library.
   b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.
   c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.
   d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful. (For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application.

Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.) These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works.

But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it. Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library. In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3) You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices. Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

   This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4) You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

   If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5) A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a “work that uses the Library”. Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

   However, linking a “work that uses the Library” with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a “work that uses the library”.

The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library.

The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6) As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

   You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

   a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

   b) Use a suitable shared library mechanism for linking with the Library.
   A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

   c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy. For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7) You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8) You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9) You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10) Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11) If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License.
If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library. If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.
It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice. This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.
12) If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.
13) The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.
Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and “any later version”, you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.
14) If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15) BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16) IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).
To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the library's name and an idea of what it does.
Copyright(c) year name of author

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.

See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.
You should also get your employer (if you work as a programmer) or your school, if any, to sign a “copyright disclaimer” for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library ‘Frob’ (a library for tweaking knobs) written by James Random Hacker.

Signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

libsmi license

Copyright(c) 1999-2002 Frank Strauss, Technical University of Braunschweig.
This software is copyrighted by Frank Strauss, the Technical University of Braunschweig, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files.

The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

THE AUTHORS **AND** DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN “AS IS” BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

The MIT License

Copyright(c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the “Software”), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

MOZILLA PUBLIC LICENSE Version 1.1

1. Definitions.

1.0.1. "**Commercial Use**" means distribution or otherwise making the Covered Code available to a third party.

1.1. "**Contributor**" means each entity that creates or contributes to the creation of Modifications.

1.2. "**Contributor Version**" means the combination of the Original Code, prior Modifications used by a Contributor, and the Modifications made by that particular Contributor.

1.3. "**Covered Code**" means the Original Code or Modifications or the combination of the Original Code and Modifications, in each case including portions thereof.

1.4. "**Electronic Distribution Mechanism**" means a mechanism generally accepted in the software development community for the electronic transfer of data.

1.5. "**Executable**" means Covered Code in any form other than Source Code.

1.6. "**Initial Developer**" means the individual or entity identified as the Initial Developer in the Source Code notice required by **Exhibit A**.

1.7. "**Larger Work**" means a work which combines Covered Code or portions thereof with code not governed by the terms of this License.

1.8. "**License**" means this document.

1.8.1. "**Licensable**" means having the right to grant, to the maximum extent possible, whether at the time of the initial grant or subsequently acquired, any and all of the rights conveyed herein.

1.9. "**Modifications**" means any addition to or deletion from the substance or structure of either the Original Code or any previous Modifications. When Covered Code is released as a series of files, a Modification is:

- **A.** Any addition to or deletion from the contents of a file containing Original Code or previous Modifications.
- **B.** Any new file that contains any part of the Original Code or previous Modifications.

1.10. "**Original Code**" means Source Code of computer software code which is described in the Source Code notice required by **Exhibit A** as Original Code, and which, at the time of its release under this License is not already Covered Code governed by this License.

1.10.1. "**Patent Claims**" means any patent claim(s), now owned or hereafter acquired, including without limitation, method, process, and apparatus claims, in any patent Licensable by grantor.

1.11. "**Source Code**" means the preferred form of the Covered Code for making modifications to it, including all modules it contains, plus any associated interface definition files, scripts used to control compilation and installation of an Executable, or source code differential comparisons against either the Original Code or another well known, available Covered Code of the Contributor's choice. The Source Code can be in a compressed or archival form, provided the appropriate decompression or de-archiving software is widely available for no charge.

1.12. "**You**" **(or** "**Your**"**)** means an individual or a legal entity exercising rights under, and complying with all of the terms of, this License or a future version of this License issued under Section 6.1. For legal entities, "You" includes any entity which controls, is controlled by, or is under common control with You. For purposes of this definition, "control" means(a) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (b) ownership of more than fifty percent (50 %) of the outstanding shares or beneficial ownership of such entity.

2. Source Code License.

2.1. The Initial Developer Grant. The Initial Developer hereby grants You a world-wide, royalty-free, non-exclusive license, subject to third party intellectual property claims:

(a) under intellectual property rights (other than patent or trademark) Licensable by Initial Developer to use, reproduce, modify, display, perform, sublicense and distribute the Original Code (or portions thereof) with or without Modifications, and/or as part of a Larger Work; and

(b) under Patents Claims infringed by the making, using or selling of Original Code, to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the Original Code (or portions thereof).

(c) the licenses granted in this Section 2.1 (a) and (b) are effective on the date Initial Developer first distributes Original Code under the terms of this License.

(d) Notwithstanding Section 2.1 (b) above, no patent license is granted: 1) for code that You delete from the Original Code; 2) separate from the Original Code; or 3) for infringements caused by: i) the modification of the Original Code or ii) the combination of the Original Code with other software or devices.

2.2. Contributor Grant. Subject to third party intellectual property claims, each Contributor hereby grants You a world-wide, royalty-free, non-exclusive license

(a) under intellectual property rights (other than patent or trademark) Licensable by Contributor, to use, reproduce, modify, display, perform, sublicense and distribute the Modifications created by such Contributor (or portions thereof) either on an unmodified basis, with other Modifications, as Covered Code and/or as part of a Larger Work; and

(b) under Patent Claims infringed by the making, using, or selling of Modifications made by that Contributor either alone and/or in combination with its Contributor Version (or portions of such combination), to make, use, sell, offer for sale, have made, and/or otherwise dispose of: 1) Modifications made by that Contributor (or portions thereof); and 2) the combination of Modifications made by that Contributor with its Contributor Version (or portions of such combination).

(c) the licenses granted in Sections 2.2 (a) and 2.2 (b) are effective on the date Contributor first makes Commercial Use of the Covered Code.

(d) Notwithstanding Section 2.2 (b) above, no patent license is granted: 1) for any code that Contributor has deleted from the Contributor Version; 2) separate from the Contributor Version; 3) for infringements caused by: i) third party modifications of Contributor Version or ii) the combination of Modifications made by that Contributor with other software (except as part of the Contributor Version) or other devices; or 4) under Patent Claims infringed by Covered Code in the absence of Modifications made by that Contributor.

3. Distribution Obligations.

3.1. Application of License. The Modifications which You create or to which You contribute are governed by the terms of this License, including without limitation Section2**.2**. The Source Code version of Covered Code may be distributed only under the terms of this License or a future version of this License released under Section **6.1**, and You must include a copy of this License with every copy of the Source Code You distribute. You may not offer or impose any terms on any Source Code version that alters or restricts the applicable version of this License or the recipients' rights hereunder. However, You may include an additional document offering the additional rights described in Section **3.5**.

3.2. Availability of Source Code. Any Modification which You create or to which You contribute must be made available in Source Code form under the terms of this License either on the same media as an Executable version or via an accepted Electronic Distribution Mechanism to anyone to whom you made an Executable version available; and if made available via Electronic Distribution Mechanism, must remain available for at least twelve (12) months after the date it initially became available, or at least six (6) months after a subsequent version of that particular Modification has been made available to such recipients. You are responsible for ensuring that the Source Code version remains available even if the Electronic Distribution Mechanism is maintained by a third party.

3.3. Description of Modifications. You must cause all Covered Code to which You contribute to contain a file documenting the changes You made to create that Covered Code and the date of any change. You must include a prominent statement that the Modification is derived, directly or indirectly, from Original Code provided by the Initial Developer and including the name of the Initial Developer in (a) the Source Code, and (b) in any notice in an Executable version or related documentation in which You describe the origin or ownership of the Covered Code.

3.4. Intellectual Property Matters

(a) Third Party Claims. If Contributor has knowledge that a license under a third party's intellectual property rights is required to exercise the rights granted by such Contributor under Sections 2.1 or 2.2, Contributor must include a text file with the Source Code distribution titled "LEGAL" which describes the claim and the party making the claim in sufficient detail that a recipient will know whom to contact. If Contributor obtains such knowledge after the Modification is made available as described in Section 3.2, Contributor shall promptly modify the LEGAL file in all copies Contributor makes available thereafter and shall take other steps (such as notifying appropriate mailing lists or newsgroups) reasonably calculated to inform those who received the Covered Code that new knowledge has been obtained.

(b) Contributor APIs. If Contributor's Modifications include an application programming interface and Contributor has knowledge of patent licenses which are reasonably necessary to implement that API, Contributor must also include this information in the LEGAL file.

(c) Representations. Contributor represents that, except as disclosed pursuant to Section 3.4 (a) above, Contributor believes that Contributor's Modifications are Contributor's original creation(s) and/or Contributor has sufficient rights to grant the rights conveyed by this License.

3.5. Required Notices. You must duplicate the notice in **Exhibit A** in each file of the Source Code. If it is not possible to put such notice in a particular Source Code file due to its structure, then You must include such notice in a location (such as a relevant directory) where a user would be likely to look for such a notice. If You created one or more Modification(s) You may add your name as a Contributor to the notice described in **Exhibit A**. You must also duplicate this License in any documentation for the Source Code where You describe recipients' rights or ownership rights relating to Covered Code. You may choose to offer, and to charge a fee for, warranty, support, indemnity or liability obligations to one or more recipients of Covered Code. However, You may do so only on Your own behalf, and not on behalf of the Initial Developer or any Contributor. You must make it absolutely clear than any such warranty, support, indemnity or liability obligation is offered by You alone, and You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of warranty, support, indemnity or liability terms You offer.

3.6. Distribution of Executable Versions. You may distribute Covered Code in Executable form only if the requirements of Section **3.1**-**3.5** have been met for that Covered Code, and if You include a notice stating that the Source Code version of the Covered Code is available under the terms of this License, including a description of how and where You have fulfilled the obligations of Section **3.2**. The notice must be conspicuously included in any notice in an Executable version, related documentation or collateral in which You describe recipients' rights relating to the Covered Code.

You may distribute the Executable version of Covered Code or ownership rights under a license of Your choice, which may contain terms different from this License, provided that You are in compliance with the terms of this License and that the license for the Executable version does not attempt to limit or alter the recipient's rights in the Source Code version from the rights set forth in this License. If You distribute the Executable version under a different license You must make it absolutely clear that any terms which differ from this License are offered by You alone, not by the Initial Developer or any Contributor. You hereby agree to indemnify the Initial Developer and every Contributor for any liability incurred by the Initial Developer or such Contributor as a result of any such terms You offer.

3.7. Larger Works. You may create a Larger Work by combining Covered Code with other code not governed by the terms of this License and distribute the Larger Work as a single product. In such a case, You must make sure the requirements of this License are fulfilled for the Covered Code.

4. Inability to Comply Due to Statute or Regulation.

If it is impossible for You to comply with any of the terms of this License with respect to some or all of the Covered Code due to statute, judicial order, or regulation then You must: (a) comply with the terms of this License to the maximum extent possible; and (b) describe the limitations and the code they affect. Such description must be included in the LEGAL file described in Section **3.4** and must be included with all distributions of the Source Code. Except to the extent prohibited by statute or regulation, such description must be sufficiently detailed for a recipient of ordinary skill to be able to understand it.

5. Application of this License.

This License applies to code to which the Initial Developer has attached the notice in **Exhibit A** and to related Covered Code.

6. Versions of the License.

6.1. New Versions. Netscape Communications Corporation ("Netscape") may publish revised and/or new versions of the License from time to time. Each version will be given a distinguishing version number.

6.2. Effect of New Versions. Once Covered Code has been published under a particular version of the License, You may always continue to use it under the terms of that version. You may also choose to use such Covered Code under the terms of any subsequent version of the License published by Netscape. No one other than Netscape has the right to modify the terms applicable to Covered Code created under this License.

6.3. Derivative Works. If You create or use a modified version of this License (which you may only do in order to apply it to code which is not already Covered Code governed by this License), You must (a) rename Your license so that the phrases "Mozilla", "MOZILLAPL", "MOZPL", "Netscape", "MPL", "NPL" or any confusingly similar phrase do not appear in your license (except to note that your license differs from this License) and (b) otherwise make it clear that Your version of the license contains terms which differ from the Mozilla Public License and Netscape Public License. (Filling in the name of the Initial Developer, Original Code or Contributor in the notice described in **Exhibit A** shall not of themselves be deemed to be modifications of this License.)

7. DISCLAIMER OF WARRANTY.

COVERED CODE IS PROVIDED UNDER THIS LICENSE ON AN "AS IS" BASIS, WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES THAT THE COVERED CODE IS FREE OF DEFECTS, MERCHANTABLE, FIT FOR A PARTICULAR PURPOSE OR NON-INFRINGING. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE COVERED CODE IS WITH YOU. SHOULD ANY COVERED CODE PROVE DEFECTIVE IN ANY RESPECT, YOU (NOT THE INITIAL DEVELOPER OR ANY OTHER CONTRIBUTOR) ASSUME THE COST OF ANY NECESSARY SERVICING, REPAIR OR CORRECTION. THIS DISCLAIMER OF WARRANTY CONSTITUTES AN ESSENTIAL PART OF THIS LICENSE. NO USE OF ANY COVERED CODE IS AUTHORIZED HEREUNDER EXCEPT UNDER THIS DISCLAIMER.

8. TERMINATION.

8.1. This License and the rights granted hereunder will terminate automatically if You fail to comply with terms herein and fail to cure such breach within 30 days of becoming aware of the breach. All sublicenses to the Covered Code which are properly granted shall survive any termination of this License. Provisions which, by their nature, must remain in effect beyond the termination of this License shall survive.

8.2. If You initiate litigation by asserting a patent infringement claim (excluding declatory judgment actions) against Initial Developer or a Contributor (the Initial Developer or Contributor against whom You file such action is referred to as "Participant") alleging that:

(a) such Participant's Contributor Version directly or indirectly infringes any patent, then any and all rights granted by such Participant to You under Sections 2.1 and/or 2.2 of this License shall, upon 60 days notice from Participant terminate prospectively, unless if within 60 days after receipt of notice You either: (i) agree in writing to pay Participant a mutually agreeable reasonable royalty for Your past and future use of Modifications made by such Participant, or (ii) withdraw Your litigation claim with respect to the Contributor Version against such Participant. If within 60 days of notice, a reasonable royalty and payment arrangement are not mutually agreed upon in writing by the parties or the litigation claim is not withdrawn, the rights granted by Participant to You under Sections 2.1 and/or 2.2 automatically terminate at the expiration of the 60 day notice period specified above.

(b) any software, hardware, or device, other than such Participant's Contributor Version, directly or indirectly infringes any patent, then any rights granted to You by such Participant under Sections 2.1 (b) and 2.2 (b) are revoked effective as of the date You first made, used, sold, distributed, or had made, Modifications made by that Participant.

8.3. If You assert a patent infringement claim against Participant alleging that such Participant's Contributor Version directly or indirectly infringes any patent where such claim is resolved (such as by license or settlement) prior to the initiation of patent infringement litigation, then the reasonable value of the licenses granted by such Participant under Sections 2.1 or 2.2 shall be taken into account in determining the amount or value of any payment or license.

8.4. In the event of termination under Sections 8.1 or 8.2 above, all end user license agreements (excluding distributors and resellers) which have been validly granted by You or any distributor hereunder prior to termination shall survive termination.

9. LIMITATION OF LIABILITY.

UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, WHETHER TORT (INCLUDING NEGLIGENCE), CONTRACT, OR OTHERWISE, SHALL YOU, THE INITIAL DEVELOPER, ANY OTHER CONTRIBUTOR, OR ANY DISTRIBUTOR OF COVERED CODE, OR ANY SUPPLIER OF ANY OF SUCH PARTIES, BE LIABLE TO ANY PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES, EVEN IF SUCH PARTY SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY RESULTING FROM SUCH PARTY'S NEGLIGENCE TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS EXCLUSION AND LIMITATION MAY NOT APPLY TO YOU.

10. U.S. GOVERNMENT END USERS.

The Covered Code is a "commercial item," as that term is defined in 48 C.F.R. 2.101 (Oct. 1995), consisting of "commercial computer software" and "commercial computer software documentation," as such terms are used in 48 C.F.R. 12.212 (Sept. 1995). Consistent with 48 C.F.R. 12.212 and 48 C.F.R. 227.7202-1 through 227.7202-4 (June 1995), all U.S. Government End Users acquire Covered Code with only those rights set forth herein.

11. MISCELLANEOUS.

This License represents the complete agreement concerning subject matter hereof. If any provision of this License is held to be unenforceable, such provision shall be reformed only to the extent necessary to make it enforceable. This License shall be governed by California law provisions (except to the extent applicable law, if any, provides otherwise), excluding its conflict-of-law provisions. With respect to disputes in which at least one party is a citizen of, or an entity chartered or registered to do business in the United States of America, any litigation relating to this License shall be subject to the jurisdiction of the Federal Courts of the Northern District of California, with venue lying in Santa Clara County, California, with the losing party responsible for costs, including without limitation, court costs and reasonable attorneys' fees and expenses. The application of the United Nations Convention on Contracts for the International Sale of Goods is expressly excluded. Any law or regulation which provides that the language of a contract shall be construed against the drafter shall not apply to this License.

12. RESPONSIBILITY FOR CLAIMS.

As between Initial Developer and the Contributors, each party is responsible for claims and damages arising, directly or indirectly, out of its utilization of rights under this License and You agree to work with Initial Developer and Contributors to distribute such responsibility on an equitable basis. Nothing herein is intended or shall be deemed to constitute any admission of liability.

13. MULTIPLE-LICENSED CODE.

Initial Developer may designate portions of the Covered Code as Multiple-Licensed. Multiple-Licensedmeans that the Initial Developer permits you to utilize portions of the Covered Code under Your choice of the MPL or the alternative licenses, if any, specified by the Initial Developer in the file described in Exhibit A.

EXHIBIT A-Mozilla Public License.

"The contents of this file are subject to the Mozilla Public License Version 1.1 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.mozilla.org/MPL/
Software distributed under the License is distributed on an "AS IS" basis, WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License for the specific language governing rights and limitations under the License.
The Original Code is _____.
The Initial Developer of the Original Code is _____.
Portions created by _____ are Copyright(c) _____
_____. All Rights Reserved.
Contributor(s): _____.
Alternatively, the contents of this file may be used under the terms of the _____ license (the [___] License), in which case the provisions of [_____] License are applicable instead of those above. If you wish to allow use of your version of this file only under the terms of the [____] License and not to allow others to use your version of this file under the MPL, indicate your decision by deleting the provisions above and replace them with the notice and other provisions required by the [___] License. If you do not delete the provisions above, a recipient may use your version of this file under either the MPL or the [___] License."

[NOTE: The text of this Exhibit A may differ slightly from the text of the notices in the Source Code files of the Original Code. You should use the text of this Exhibit A rather than the text found in the Original Code Source Code for Your Modifications.]

Sun JavaMail 1.4 License

A. Sun Microsystems, Inc. (“Sun”) ENTITLEMENT for SOFTWARE
Licensee/Company: Entity receiving Software.
Effective Date: Date of delivery of the Software to You.
Software: JavaMail 1.4.
License Term: Perpetual (subject to termination under the SLA).
Licensed Unit: Software Copy.
Licensed unit Count: Unlimited.
Permitted Uses:

1. You may reproduce and use the Software for Individual, Commercial, or Research and Instructional Use for the purposes of designing, developing, testing, and running Your applets and application (“Programs”).
2. Subject to the terms and conditions of this Agreement and restrictions and exceptions set forth in the Software’s documentation, You may reproduce and distribute portions of Software identified as a redistributable in the documentation (“Redistributable”), provided that:
   a. you distribute Redistributable complete and unmodified and only bundled as part of Your Programs,
   b. your Programs add significant and primary functionality to the Redistributable,
   c. you distribute Redistributable for the sole purpose of running your Programs,
   d. you do not distribute additional software intended to replace any component(s) of the Redistributable,
   e. you do not remove or alter any proprietary legends or notices contained in or on the Redistributable.
   f. you only distribute the Redistributable subject to a license agreement that protects Sun’s interests consistent with the terms contained in this Agreement, and
   g. you agree to defend and indemnify Sun and its licensors from and against any damages, costs, liabilities, settlement amounts and/or expenses (including attorneys’ fees) incurred in connection with any claim, lawsuit or action by any third party that arises or results from the use or distribution of any and all Programs and/or Redistributable.
3. Java Technology Restrictions. You may not create, modify, or change the behavior of, or authorize your licensees to create, modify, or change the behavior of, classes, interfaces, or subpackages that are in any way identified as “java”, “javax”, “sun” or similar convention as specified by Sun in any naming convention designation.

B. Sun Microsystems, Inc. (“Sun”) SOFTWARE LICENSE AGREEMENT
READ THE TERMS OF THIS AGREEMENT (“AGREEMENT”) CAREFULLY BEFORE OPENING SOFTWARE MEDIA PACKAGE. BY OPENING SOFTWARE MEDIA PACKAGE, YOU AGREE TO THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCESSING SOFTWARE ELECTRONICALLY, INDICATE YOUR ACCEPTANCE OF THESE TERMS BY SELECTING THE “ACCEPT” BUTTON AT THE END OF THIS AGREEMENT. IF YOU DO NOT AGREE TO ALL OF THE TERMS, PROMPTLY RETURN THE UNUSED SOFTWARE TO YOUR PLACE OF PURCHASE FOR A REFUND OR, IF SOFTWARE IS ACCESSED ELECTRONICALLY, SELECT THE “DECLINE” (OR “EXIT”) BUTTON AT THE END OF THIS AGREEMENT. IF YOU HAVE SEPARATELY AGREED TO LICENSE TERMS (“MASTER TERMS”) FOR YOUR LICENSE TO THIS SOFTWARE, THEN SECTIONS 1-5 OF THIS AGREEMENT (“SUPPLEMENTAL LICENSE TERMS”) SHALL SUPPLEMENT AND SUPERSEDE THE MASTER TERMS IN RELATION TO THIS SOFTWARE.

1. Definitions.
   a. “Entitlement” means the collective set of applicable documents authorized by Sun evidencing your obligation to pay associated fees (if any) for the license, associated Services, and the authorized scope of use of Software under this Agreement.
   b. “Licensed Unit” means the unit of measure by which your use of Software and/or Service is licensed, as described in your Entitlement.
   c. “Permitted Use” means the licensed Software use(s) authorized in this Agreement as specified in your Entitlement. The Permitted Use for any bundled Sun software not specified in your Entitlement will be evaluation use as provided in Section 3.
   d. “Service” means the service(s) that Sun or its delegate will provide, if any, as selected in your Entitlement and as further described in the applicable service listings at www.sun.com/service/servicelist.
   e. “Software” means the Sun software described in your Entitlement. Also, certain software may be included for evaluation use under Section 3.
   f. “You” and “Your” means the individual or legal entity specified in the Entitlement, or for evaluation purposes, the entity performing the evaluation.

2. License Grant and Entitlement.
   Subject to the terms of your Entitlement, Sun grants you a nonexclusive, nontransferable limited license to use Software for its Permitted Use for the license term.
   Your Entitlement will specify
   a. Software licensed,
   b. the Permitted Use,
   c. the license term, and
   d. the Licensed Units.

Additionally, if your Entitlement includes Services, then it will also specify the
e. Service and
f. service term.

If your rights to Software or Services are limited in duration and the date such rights begin is other than the purchase date, your Entitlement will provide that beginning date(s).
The Entitlement may be delivered to you in various ways depending on the manner in which you obtain Software and Services, for example, the Entitlement may be provided in your receipt, invoice or your contract with Sun or authorized Sun reseller. It may also be in electronic format if you download Software.

3. Permitted Use.
As selected in your Entitlement, one or more of the following Permitted Uses will apply to your use of Software. Unless you have an Entitlement that expressly permits it, you may not use Software for any of the other Permitted Uses. If you don't have an Entitlement, or if your Entitlement doesn't cover additional software delivered to you, then such software is for your Evaluation Use.
a. Evaluation Use. You may evaluate Software internally for a period of 90 days from your first use.
b. Research and Instructional Use. You may use Software internally to design, develop and test, and also to provide instruction on such uses.
c. Individual Use. You may use Software internally for personal, individual use.
d. Commercial Use. You may use Software internally for your own commercial purposes.
e. Service Provider Use. You may make Software functionality accessible (but not by providing Software itself or through outsourcing services) to your end users in an extranet deployment, but not to your affiliated companies or to government agencies.

Licensed Units.
Your Permitted Use is limited to the number of Licensed Units stated in your Entitlement. If you require additional Licensed Units, you will need additional Entitlement(s).

Restrictions.
(a) The copies of Software provided to you under this Agreement are licensed, not sold, to you by Sun. Sun reserves all rights not expressly granted.
(b) You may make a single archival copy of Software, but otherwise may not copy, modify, or distribute Software. However if the Sun documentation accompanying Software lists specific portions of Software, such as header files, class libraries, reference source code, and/or redistributable files, that may be handled differently, you may do so only as provided in the Sun documentation.
(c) You may not rent, lease, lend or encumber Software.

(d) Unless enforcement is prohibited by applicable law, you may not decompile, or reverse engineer Software.
(e) The terms and conditions of this Agreement will apply to any Software updates, provided to you at Sun's discretion, that replace and/or supplement the original Software, unless such update contains a separate license.
(f) You may not publish or provide the results of any benchmark or comparison tests run on Software to any third party without the prior written consent of Sun.
(g) Software is confidential and copyrighted.
(h) Unless otherwise specified, if Software is delivered with embedded or bundled software that enables functionality of Software, you may not use such software on a stand-alone basis or use any portion of such software to interoperate with any program(s) other than Software.
(i) Software may contain programs that perform automated collection of system data and/or automated software updating services. System data collected through such programs may be used by Sun, its subcontractors, and its service delivery partners for the purpose of providing you with remote system services and/or improving Sun's software and systems.
(j) Software is not designed, licensed or intended for use in the design, construction, operation or maintenance of any nuclear facility and Sun and its licensors disclaim any express or implied warranty of fitness for such uses.
(k) No right, title or interest in or to any trademark, service mark, logo or trade name of Sun or its licensors is granted under this Agreement.

Term and Termination.
The license and service term are set forth in your Entitlement(s). Your rights under this Agreement will terminate immediately without notice from Sun if you materially breach it or take any action in derogation of Sun's and/or its licensors' rights to Software. Sun may terminate this Agreement should any Software become, or in Sun's reasonable opinion likely to become, the subject of a claim of intellectual property infringement or trade secret misappropriation. Upon termination, you will cease use of, and destroy, Software and confirm compliance in writing to Sun. Sections 1, 5, 6, 7, and 9-15 will survive termination of the Agreement.

Java Compatibility and Open Source.
Software may contain Java technology. You may not create additional classes to, or modifications of, the Java technology, except under compatibility requirements available under a separate agreement available at www.java.net.
Sun supports and benefits from the global community of open source developers, and thanks the community for its important contributions and open standards-based technology, which Sun has adopted into many of its products.
Please note that portions of Software may be provided with notices and open source licenses from such communities and third parties that govern the use of those portions, and any licenses granted hereunder do not alter any rights and obligations you may have under such open source licenses, however, the disclaimer of warranty and limitation of liability provisions in this Agreement will apply to all Software in this distribution.

Limited Warranty.
Sun warrants to you that for a period of 90 days from the date of purchase, as evidenced by a copy of the receipt, the media on which Software is furnished (if any) will be free of defects in materials and workmanship under normal use. Except for the foregoing, Software is provided "AS IS". Your exclusive remedy and Sun's entire liability under this limited warranty will be at Sun's option to replace Software media or refund the fee paid for Software. Some states do not allow limitations on certain implied warranties, so the above may not apply to you. This limited warranty gives you specific legal rights. You may have others, which vary from state to state.

Disclaimer of Warranty.
UNLESS SPECIFIED IN THIS AGREEMENT, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT THESE DISCLAIMERS ARE HELD TO BE LEGALLY INVALID.

Limitation of Liability.
TO THE EXTENT NOT PROHIBITED BY LAW, IN NO EVENT WILL SUN OR ITS LICENSORS BE LIABLE FOR ANY LOST REVENUE, PROFIT OR DATA, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL OR PUNITIVE DAMAGES, HOWEVER CAUSED REGARDLESS OF THE THEORY OF LIABILITY, ARISING OUT OF OR RELATED TO THE USE OF OR INABILITY TO USE SOFTWARE, EVEN IF SUN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
In no event will Sun's liability to you, whether in contract, tort (including negligence), or otherwise, exceed the amount paid by you for Software under this Agreement.
The foregoing limitations will apply even if the above stated warranty fails of its essential purpose. Some states do not allow the exclusion of incidental or consequential damages, so some of the terms above may not be applicable to you.

Export Regulations.
All Software, documents, technical data, and any other materials delivered under this Agreement are subject to U.S. export control laws and may be subject to export or import regulations in other countries. You agree to comply strictly with these laws and regulations and acknowledge that you have the responsibility to obtain any licenses to export, re-export, or import as may be required after delivery to you.
U.S. Government Restricted Rights.
If Software is being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), then the Government's rights in Software and accompanying documentation will be only as set forth in this Agreement; this is in accordance with 48 CFR 227.7201 through 227.7202-4 (for Department of Defense (DOD) acquisitions) and with 48 CFR 2.101 and 12.212 (for non-DOD acquisitions).

Governing Law.
Any action related to this Agreement will be governed by California law and controlling U.S. federal law. No choice of law rules of any jurisdiction will apply.

Severability.
If any provision of this Agreement is held to be unenforceable, this Agreement will remain in effect with the provision omitted, unless omission would frustrate the intent of the parties, in which case this Agreement will immediately terminate.

Integration.
This Agreement, including any terms contained in your Entitlement, is the entire agreement between you and Sun relating to its subject matter. It supersedes all prior or contemporaneous oral or written communications, proposals, representations and warranties and prevails over any conflicting or additional terms of any quote, order, acknowledgment, or other communication between the parties relating to its subject matter during the term of this Agreement. No modification of this Agreement will be binding, unless in writing and signed by an authorized representative of each party.
Please contact Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, California 95054 if you have questions.

ABBREVIATION

A

ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
APC	Access Point Controller

B

BSS	Basic Service Set
BYOD	Bring Your Own Device

C

CAC	Call Admission Control
CAPWAP	Control And Provisioning Wireless Access Point
CCTV	Closed Circuit Television
CHDC	Coverage Hold Detection and Control
CLI	Command Line Interface
CPU	Central Processing Unit
CSV	Comma Separated Values

D

DB	Database
DCS	Data Coding Scheme
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone
DNAT	Dynamic Network Address Translation
DNS	Domain Name Service
DPC	Dynamic Power Control
DSCP	DiffServ Code Point
DTIM	Delivery Traffic Identification Maps
DTLS	Datagram Transmission Layer Security

E

EAP	Extensible Authentication Protocol
EDCA	Enhanced Distributed Channel Access

F

FTP	File Transfer Protocol
FFT	Fast Fourier Transform

G

GUI	Graphic User Interface

H

HO	Handover
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol

I

I/O	Input/Output
ICMP	Internet Control Message Protocol
ID	Identification
IRFM	Infrared Financial Management
IP	Internet Protocol
IPC	Inter Process Communication

J

JDBC	Java Database Connectivity
JSP	Java Server Page

M

MAC	Media Access Control
MCS	Modulation and Coding Scheme
MD5	Message-Digest algorithm 5
MDI	Medium Dependent Interface
MDI-X	Medium Dependent Interface-Crossover
MOS	Mean Opinion Score
MSDU	MAC Service Data Unit

N

NAT	Network Address Translation
NE	Network Element
NTP	Network Time Protocol

P

PEAP	Protected Extensible Authentication Protocol
PDF	Portable Document Format

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial-In User Service
RF	Radio Frequency
RMI	Remote Method Invocation
ROM	Read Only Memory
RPM	Revolution Per Minute
RRM	Radio Resource Management
RSSI	Received Signal Strength Indicator
RTS	Request To Send

S

SAS	Serial Attached SCSI
sFTP	secure File Transfer Protocol
SHA	Secure Hash Algorithm
SNAT	Static Network Address Translation
SNMP	Simple Network Management Protocol
SNR	Signal to Noise Ratio
SSH	Secure Shell
SSID	Service Set Identifier

T

TACACS	Terminal Access Controller Access Control System
TCP	Transmission Control Protocol
ToS	Type of Service

U

UDP	User Datagram Protocol

V

VLAN	Virtual Local Area Network
VQM	Voice Quality Manager

W

WEM	Wireless Enterprise Manager
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network

X

XML	Extensible Markup Language

WEM (Wireless Enterprise Manager)
Operation Manual