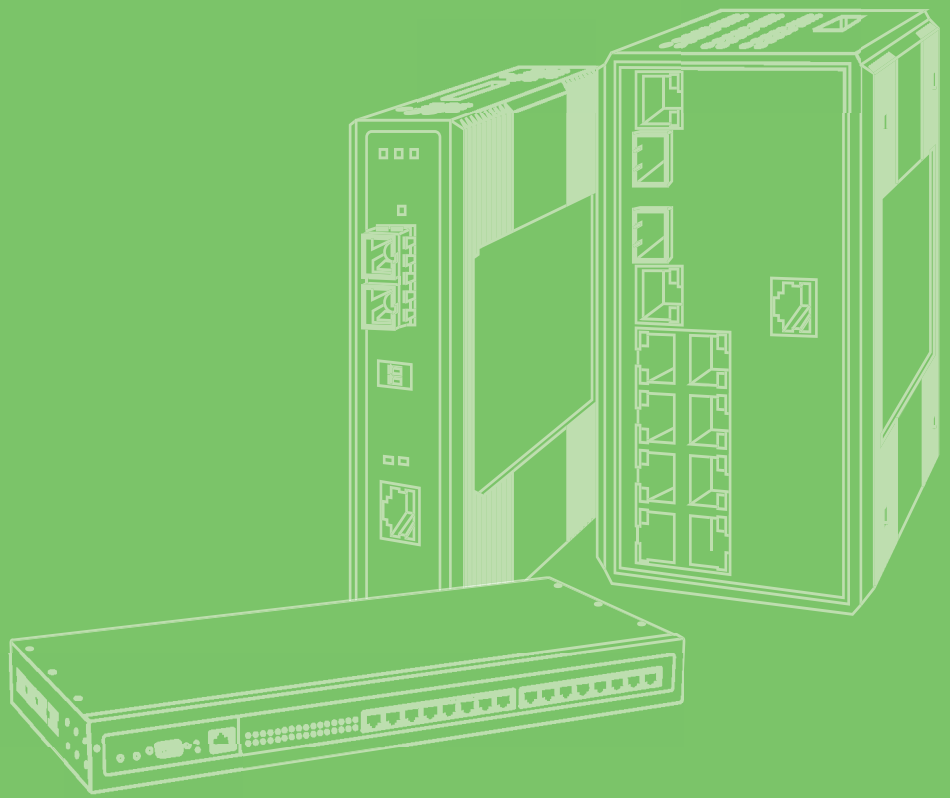


User Manual



## WebAccess/NMS

**ADVANTECH**

*Enabling an Intelligent Planet*

---

## Copyright

The documentation and the software included with this product are copyrighted 2022 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

## Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

## Technical Support and Assistance

1. Visit the Advantech web site at [www.advantech.com/support](http://www.advantech.com/support) where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
  - Product name and serial number
  - Description of your peripheral attachments
  - Description of your software (operating system, version, application software, etc.)
  - A complete description of the problem
  - The exact wording of any error messages

## Warnings, Cautions and Notes

**Warning!** *Warnings indicate conditions, which if not observed, can cause personal injury!*



**Caution!** *Cautions are included to help you avoid damaging hardware or losing data. e.g.*



*There is a danger of a new battery exploding if it is incorrectly installed. Do not attempt to recharge, force open, or heat the battery. Replace the battery only with the same or equivalent type recommended by the manufacturer. Discard used batteries according to the manufacturer's instructions.*

**Note!** *Notes provide optional additional information.*



## Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to:  
ICG.Support@advantech.com.tw

## About This Manual

This user manual is intended to guide professional installers in installing and configuring the WebAccess/NMS. It includes technical specifications, software utility introduction, as well as procedures for the use of the software utility to self-manage the devices.

At time of printing, the contents of this document were based on NMS version 3.0.3.

---

# Contents

<b>Chapter 1</b>	<b>Scope .....</b>	<b>1</b>
1.1	Document Name .....	2
1.2	System Outline.....	2
1.3	Document Outline .....	2
<b>Chapter 2</b>	<b>Technical Terms and Explanations ...</b>	<b>3</b>
2.1	Technical Terms and Explanations.....	4
<b>Chapter 3</b>	<b>Outline for WebAccess/NMS.....</b>	<b>5</b>
3.1	Outline for WebAccess/NMS .....	6
<b>Chapter 4</b>	<b>Getting Started .....</b>	<b>7</b>
4.1	OS Requirement .....	8
4.1.1	Device Management.....	8
4.1.2	Server .....	8
4.1.3	User .....	8
4.2	Hardware Requirement.....	8
<b>Chapter 5</b>	<b>WebAccess / NMS Installation .....</b>	<b>9</b>
5.1	WebAccess / NMS Installer .....	10
5.2	WebAccess / NMS Installation .....	10
5.3	WebAccess/NMS Uninstallation .....	14
5.4	EMS of WebAccess / NMS Installation Procedures.....	15
5.5	Run WebAccess / NMS .....	15
<b>Chapter 6</b>	<b>WebAccess / NMS Login .....</b>	<b>16</b>
6.1	Procedures for Logging in the first time .....	17
6.2	Login Functions.....	18
<b>Chapter 7</b>	<b>WebAccess / NMS Management Interface</b>	<b>20</b>
7.1	License Key .....	21
7.1.1	License Key .....	21
7.2	User Management .....	22
7.2.1	Users Settings Page .....	22
7.2.2	Adding Users .....	23
7.2.3	Modify and Delete Users .....	24
7.3	Database Management.....	25
7.3.1	Introduction for Database Management .....	25
7.3.2	Database Backup .....	25
7.3.3	Database Restore.....	26
7.3.4	Event Log Management.....	27

7.4	Access Log.....	29
7.4.1	Introduction for Access Log .....	29

## **Chapter 8 WebAccess / NMS Setting Interface 31**

8.1	Device Data.....	32
8.1.1	Introduction for Device Data .....	32
8.1.2	EMS Group .....	32
8.1.3	Modify and Delete EMS Groups .....	33
8.1.4	Topology Group .....	33
8.1.5	Modify and Delete Topology Groups .....	34
8.1.6	Managed Device .....	35
8.1.7	Modify and Delete Managed Devices .....	38
8.1.8	Configure Managed Devices.....	39
8.1.9	Supported Device .....	41
8.2	Severity .....	43
8.2.1	Introduction for Severity .....	43
8.2.2	Severity Operational Procedures .....	44
8.3	Message.....	45
8.3.1	Introduction for the Message .....	45
8.3.2	Message Operational Procedures .....	46
8.4	Maintenance.....	55
8.4.1	Introduction for Maintenance .....	55
8.4.2	Maintenance Operational Procedures .....	55

## **Chapter 9 WebAccess / NMS Monitoring Interface 62**

9.1	Topology .....	63
9.1.1	Introduction for Topology .....	63
9.1.2	Topology Functions.....	63
9.2	Dashboard.....	89
9.2.1	Device Status.....	89
9.2.2	Surveillance .....	89
9.2.3	Alarm Status .....	90
9.2.4	Top 10 Traffic Flow .....	90
9.3	Performance.....	91
9.3.1	Introduction for Performance .....	91
9.3.2	Performance Functions.....	91
9.4	Event Log .....	93
9.4.1	Introduction for Event Log.....	93
9.4.2	Event Log Functions .....	93
9.4.3	Shortcut Key for Event Log .....	95
9.4.4	Event Playback .....	97
9.5	System Log .....	100
9.5.1	Functions for Syslog .....	100

## **Chapter 10 WebAccess / NMS Troubleshooting .... 101**

10.1	FAQ.....	102
------	----------	-----

## **Chapter 11 WebAccess/NMS Maintenance and Management 104**

---

11.1	Access Control .....	105
	11.1.1 System User .....	105
	11.1.2 System Administrator .....	106
	11.1.3 Database Manager .....	106
11.2	Backup .....	107
11.3	Recovery from Error .....	107

## **Chapter 12 Reference ..... 108**

12.1	Reference .....	109
------	-----------------	-----

# Chapter 1

Scope

---

## 1.1 Document Name

This Operation and Maintenance Manual is for the setting, operation and maintenance for WebAccess/NMS. It includes the introduction for system, interface and functions. The version, serial number and revise history can be seen on both sides of the cover.

## 1.2 System Outline

The attributes of the system are list as follows:

---

Introduction of the system	This management system is called WebAccess/NMS, which is designed based on SNMP and ICMP standard, to manage all devices of Advantech or the devices from third-parties.
Target	IT technician may use the software such as WebAccess, IAG, even cloud application program to access the web-based WebAccess/NMS.

---

## 1.3 Document Outline

This document includes operation and functions of system, troubleshooting, and system maintenance. Please notice the information security and do not copy this document to people unrelated.



# Chapter 2

Technical Terms and  
Explanations

---

## 2.1 Technical Terms and Explanations

MIB	Management Information Base
SNMP	Simple Network Management Protocol
NMS	Network Management System
ICMP	Internet Control Message Protocol
GUI	Graphical User Interface

# Chapter 3

Outline for  
WebAccess/NMS

---

## 3.1 Outline for WebAccess/NMS

WebAccess/NMS is a management system used for managing devices for Advantech. A synthetic platform developed for monitoring, setting and maintaining devices via IP-based network.

WebAccess/NMS includes Device Management, Alarm Management, Efficiency Management, Topology Management and System Management. The distinctive features are listed as follows:

- If an error occurs, a warning message will be sent to administrator, and is easy to be accessed by smart phone or personal computer.
- If an error occurs, user may find the problem from Topology.
- Trap alert/alarm can be sent by WebAccess/NMS

# Chapter 4

Getting Started

## 4.1 OS Requirement

### 4.1.1 Device Management

Group 1	Platform
Group 2	Switch, Device Server, Wireless
Group 3	IO

### 4.1.2 Server

Operation System	Window 7, 8, 10 / Window server 2008, 2012
Web Server	Tomcat 7

### 4.1.3 User

PC Browser	Firefox, IE11, Chrome, Edge
Mobile Device Browser	Chrome, Safari
Resolution	PC, NB:1366×768 pixels Tablet:1280×720 pixels

## 4.2 Hardware Requirement

Device	Type	Specification
Processor	Intel Celeron CPU847E	1.10GHz
Memory	DDR3	4GB
I/O	Ethernet	1000Mbps
Storage	HDD	75GB

# Chapter 5

WebAccess / NMS  
Installation

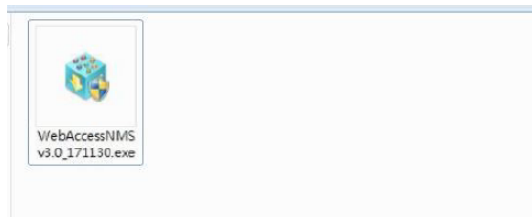
## 5.1 WebAccess / NMS Installer

WebAccess/NMS installer includes the following software:

Item	Software
1.	Microsoft Visual C++ Redistributable
2.	Microsoft .NET Framework 4.6.2. Extended
3.	MySQL Server 5.7
4.	Apache Server 2.4
5.	Java SE Development Kit
6.	Java Update 71.
7.	TFTP64 (32) Service
8.	Apache Tomcat7.0
9.	WebAccess/NMS

## 5.2 WebAccess / NMS Installation

1. Connect the WebAccess/NMS server to Internet.
2. Open the DISC folder, double-click "WebAccessNMS.exe" file.



WebAccess/NMS installer will start to install all the software listed on Chapter 5.1. The installation percentage is shown as "Please wait while Setup is loading?Verifying installer?\_\_%"

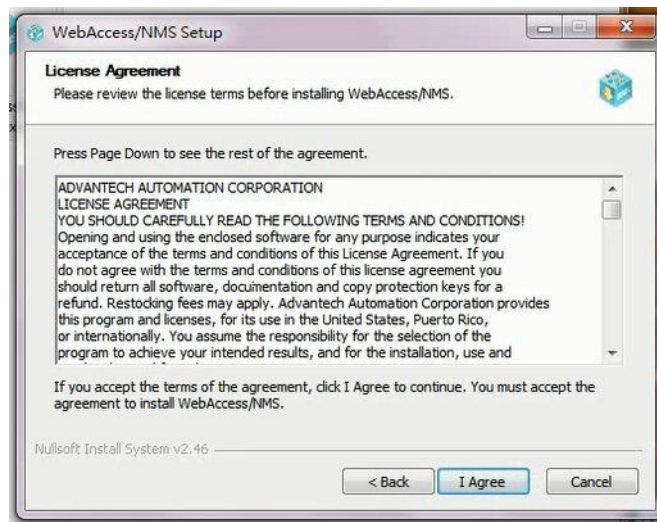




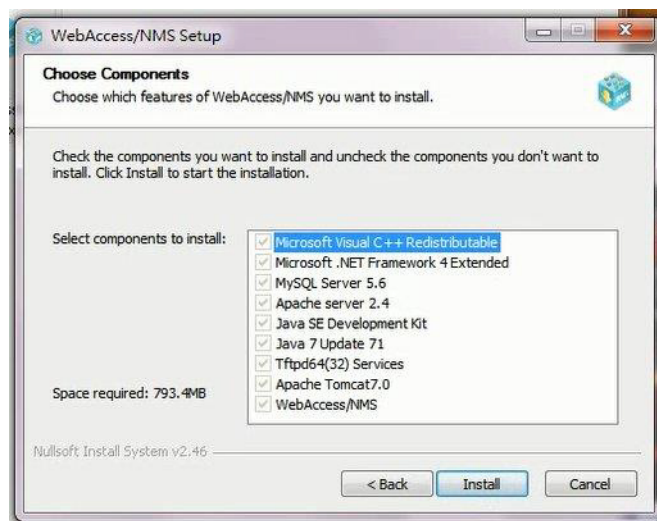
3. Click **Next** for the following step.



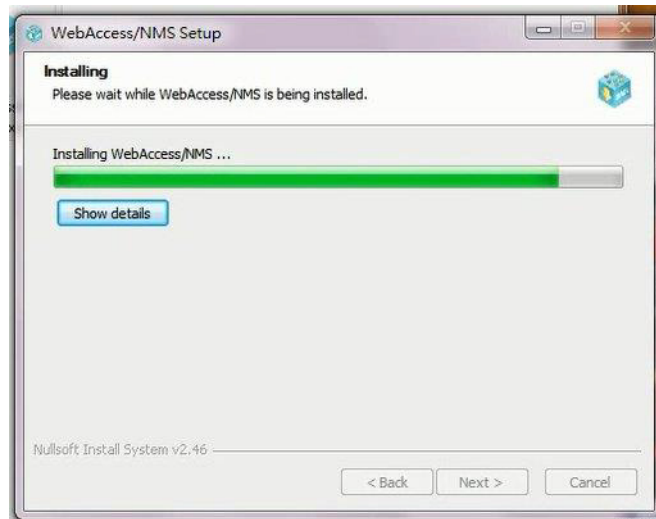
4. Read the license agreement of WebAccess/NMS, then click **I Agree** to the next step.



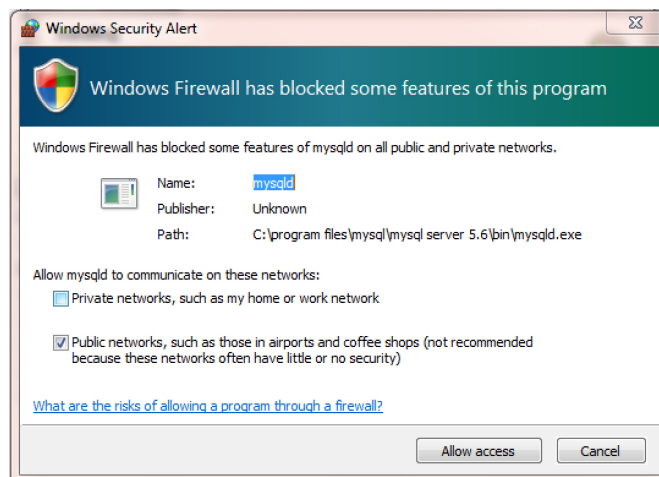
5. Click **Install** to continue.



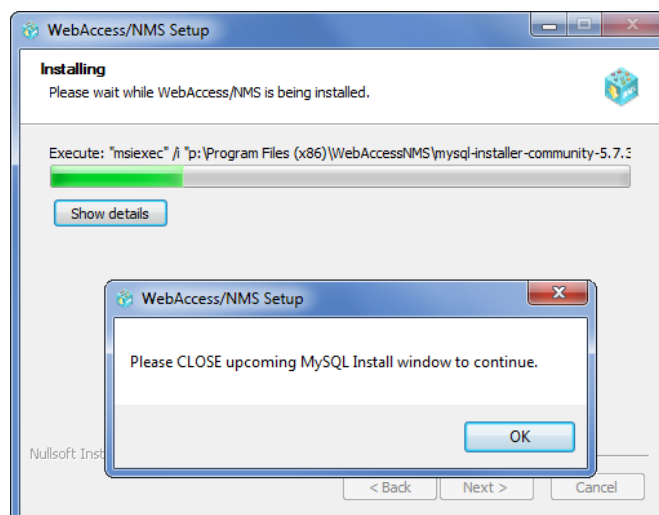
WebAccess/NMS is then installing.



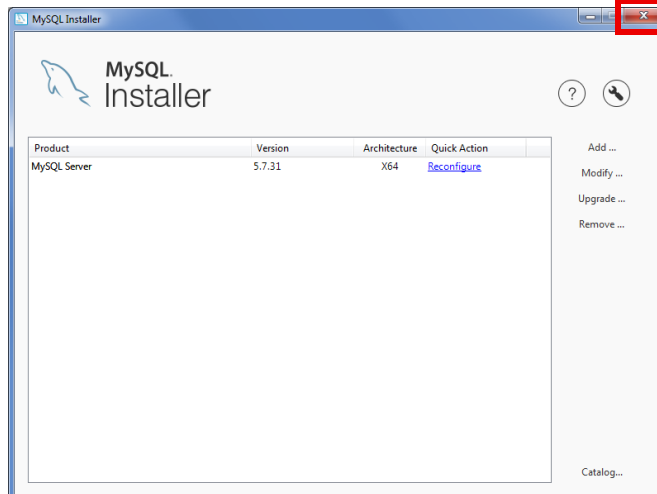
6. Click **Allow access** if Windows Security Alert pop-out.



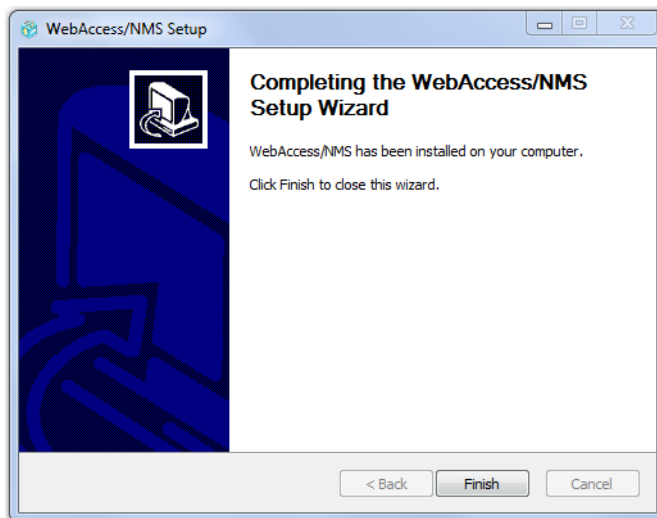
7. A Please close upcoming MySQL window to continue pop-up to inform user to close the MySQL window as shown in the following figure.



8. Click the **Close** button to continue.



9. WebAccess/NMS has successfully installed. Click **Finish** to close the installer.



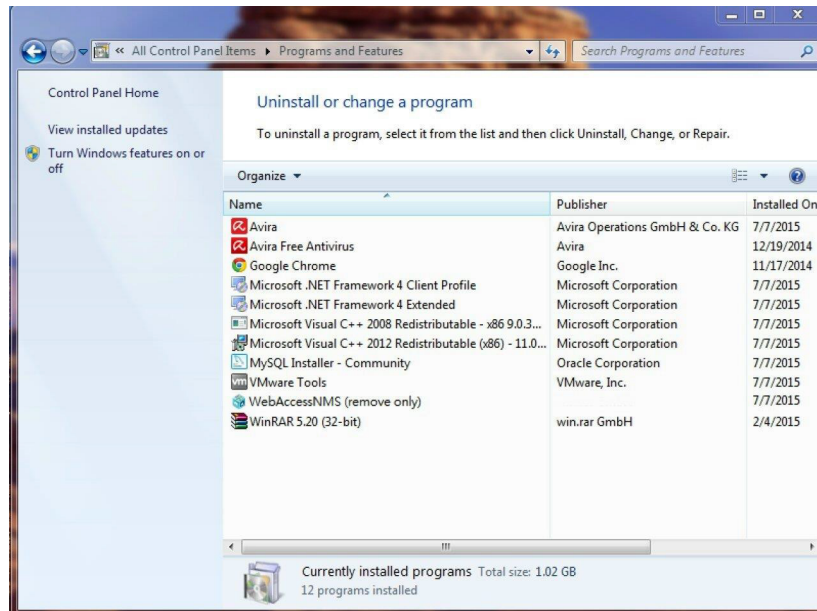
\* If *Microsoft.NET Framework4.5* is not yet installed in the system, the installer pops-up with a system reboot message. After the system boot up, the Microsoft.NET Framework4.5. installation process begins. Once completed, the system starts up normally.

10. Restart the computer for normal operation of the WebAccess/NMS.

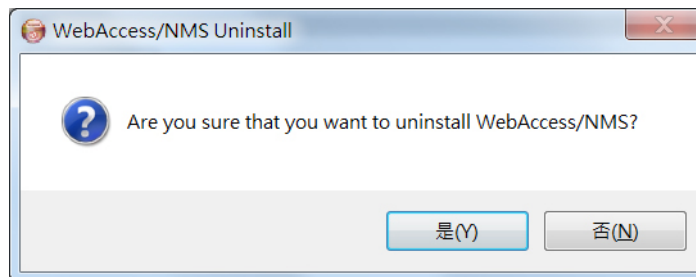
## 5.3 WebAccess/NMS Uninstallation

To uninstall the WebAccess application, use the following instructions:

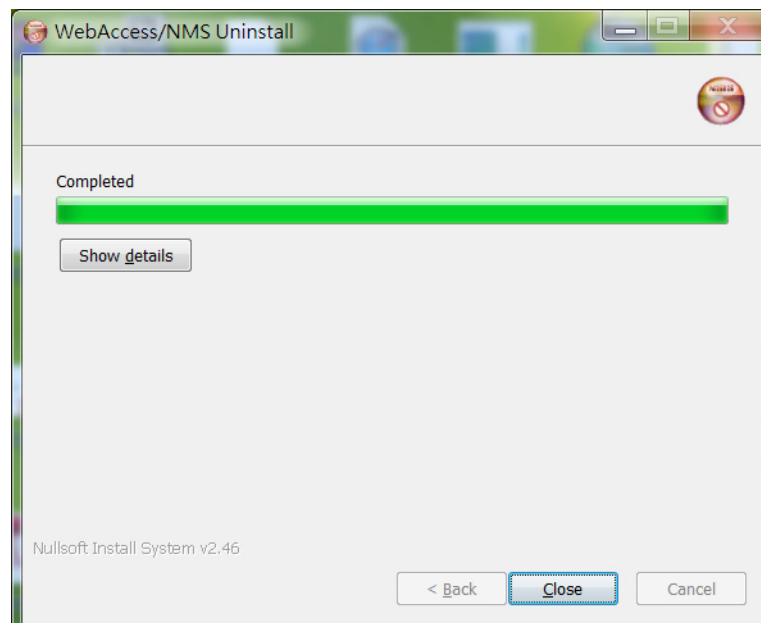
1. From the Start menu, open the Control Panel > Programs and Features to locate WebAccess/NMS (remove only) from the program list.
2. Select the application and click **Uninstall** to start.



3. A configuration pop-up displays. Click **Yes** to confirm the process.



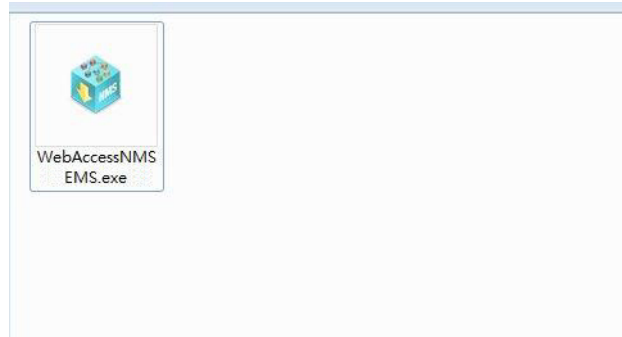
4. WebAccess/NMS is uninstalled from the system. Click **Close** to finish the process.



## 5.4 EMS of WebAccess / NMS Installation Procedures

If only EMS is required for installation to easily manage more devices for NMS, the installation procedure is as follows:

1. Click the WebAccessNMSEMS.exe icon.



To continue the process follow the instructions in the WebAccess/NMS Installation Procedures, see the following “WebAccess / NMS Installation” on page 10.

## 5.5 Run WebAccess / NMS

1. WebAccess/NMS can be opened on the following browsers:
  - IE
  - Firefox
  - Chrome
  - Safari

A WebAccessNMS shortcut displays on desktop after the installation is completed.

2. Double-click the icon to open the login page.



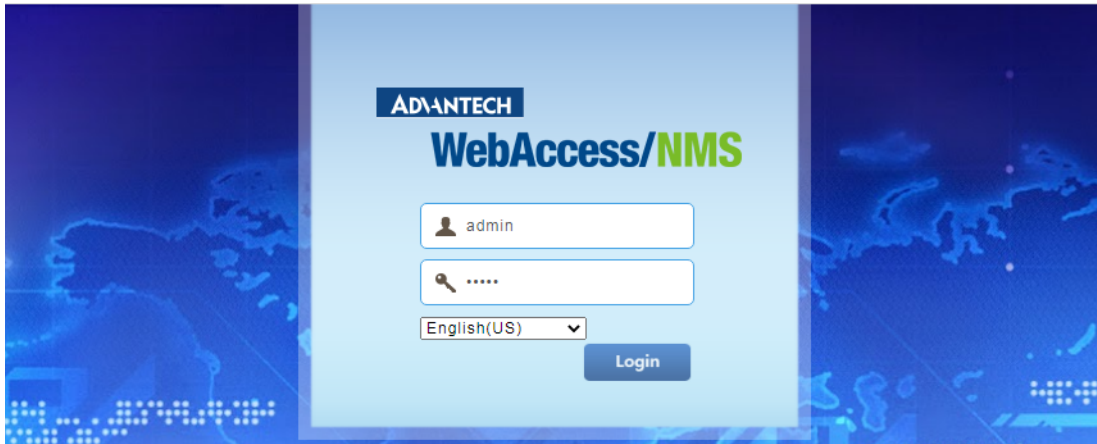
3. Or in the address field, enter `https://localhost/` to enter WebAccess/NMS login page.
  - \* After the Administrator profile installs the application, general users may type in the web as: `https://x.x.x.x/`, whereas x.x.x indicates the IP of the server where the system is installed. User may enter WebAccess/NMS through the system server directly without another installation procedure.

# Chapter 6

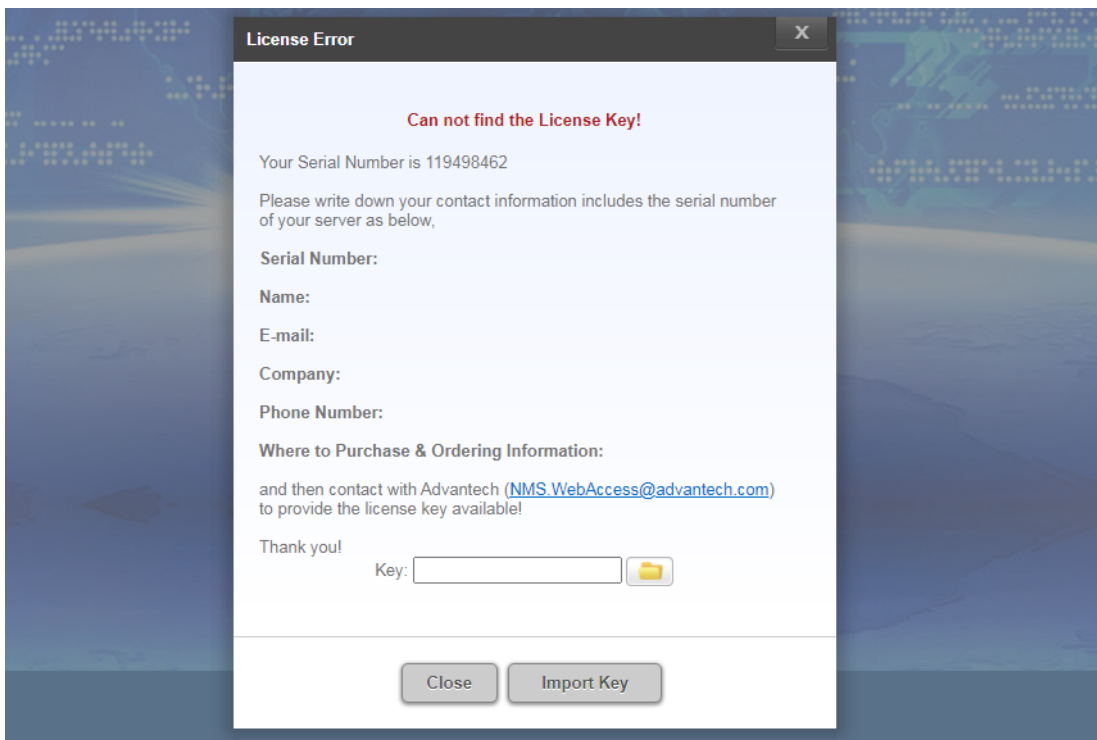
WebAccess / NMS  
Login

## 6.1 Procedures for Logging in the first time

1. Open a browser and enter `https://localhost/` to in the browser's address field to enter the WebAccess/NMS interface.
2. While logging in the first time, click the **Login** button to continue.

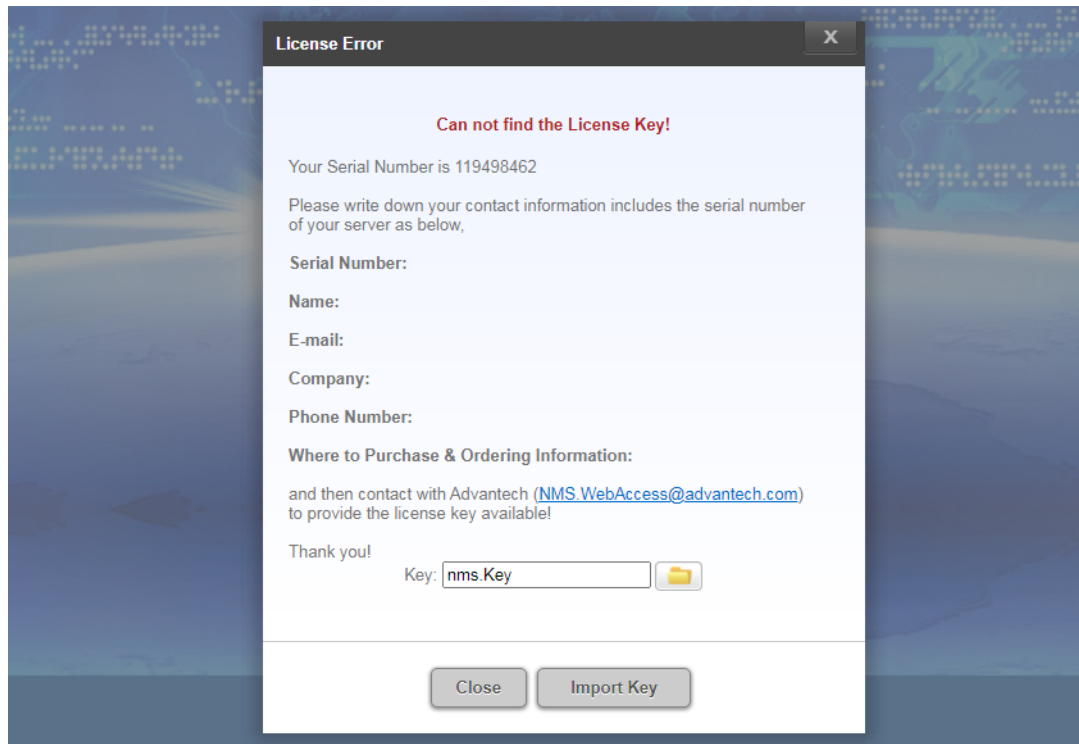


The License Error window displays.



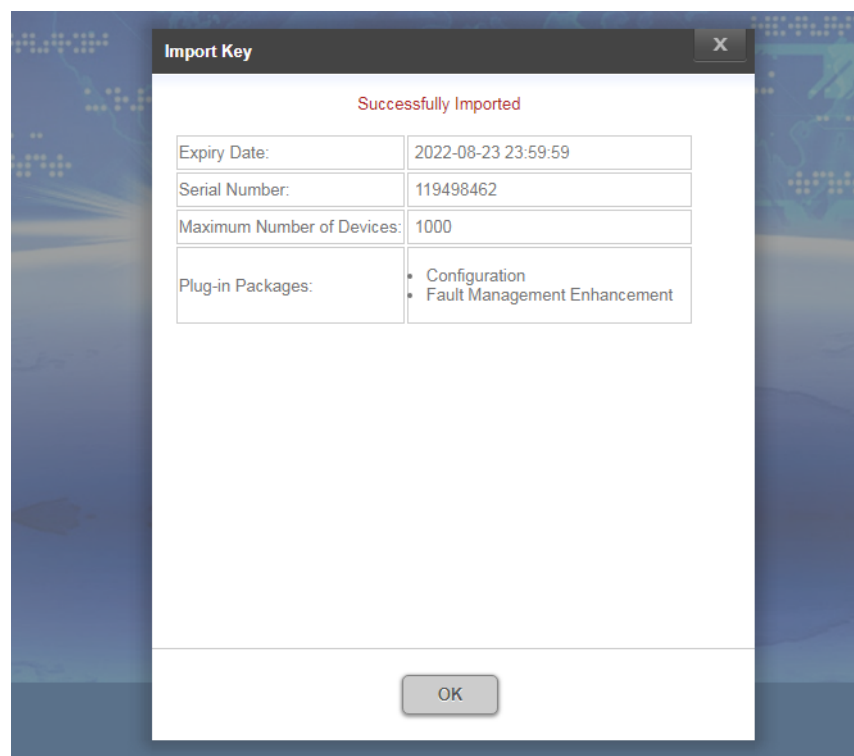
3. Once the license key from Advantech is obtained, click the **Browse** button to select the obtained license key as a file.

4. After selecting the license key file, click **Import Key** to continue.



The Import Key window displays. A list of the Expiry Date, Serial Number, Maximum Number of Devices and Plug-in Packages referencing the components of the key displays.

5. Click **OK** to return to the login page.



## 6.2 Login Functions

The application can be accessed through a browser such as Google Chrome, Firefox, Internet Explorer or Safari on a personal computer, smart phone or Tablet.



The application provides an interface in multiple languages: English, Traditional Chinese, Simplified Chinese. The default language is derived from the user's server configuration.

1. Open a browser and enter `https://localhost/` to in the browser's address field to enter WebAccess/NMS page.
2. Enter the Name and Password of a designated user. First time access, enter the default administrator account.  
Name (default): admin  
Password (default): admin

Refer to "User Management" on page 22 for further information.

3. Select a language by clicking the drop-down menu and selecting a language option.
4. Click Login to enter the interface.



Twenty concurrent users are supported by the WebAccess/NMS to perform search, monitoring, and manage accessed device functions.

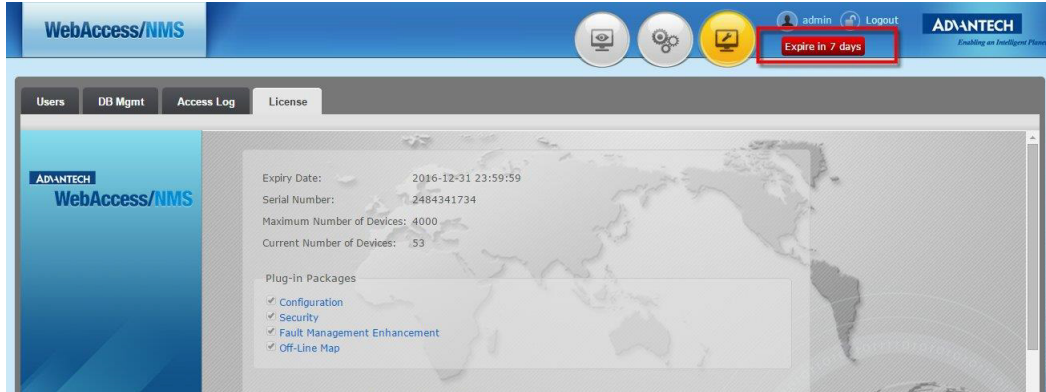
# Chapter 7

WebAccess / NMS  
Management Interface

## 7.1 License Key

### 7.1.1 License Key

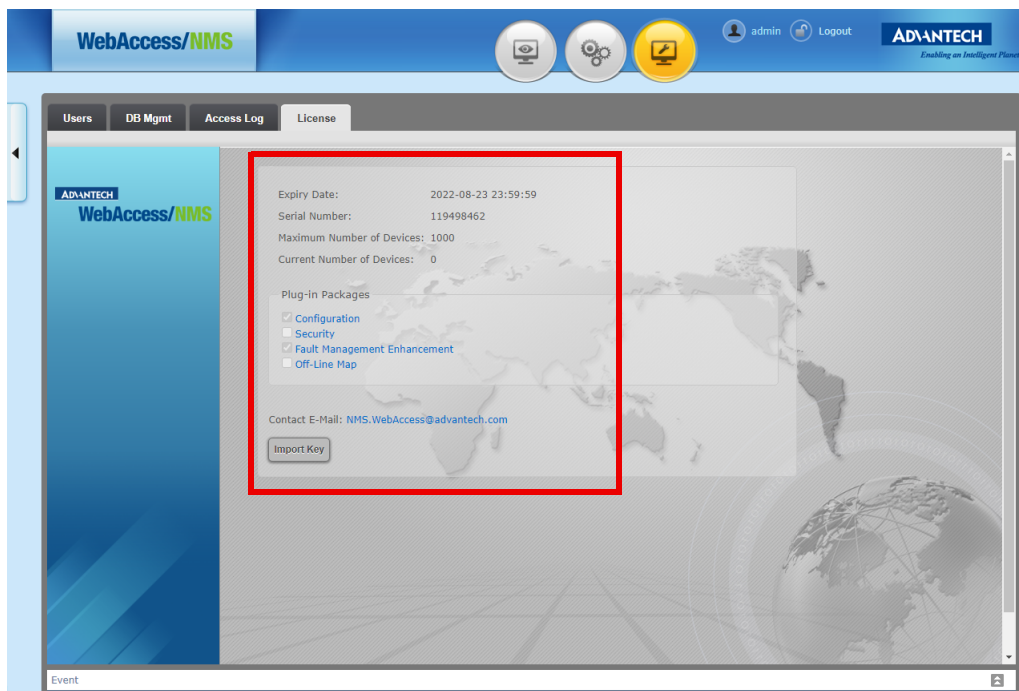
WebAccess/NMS can be leased for user to manage devices. If the license is set to expire within 60 days a notification displays on the interface with the remaining time clearly visible.



Users with administrative privileges can view the License page.

To open the License page:

1. From the tool bar menu click **Admin**.
2. The User management page displays. Click the **License** tab to open the License page.



From the License page, the Expiry Date, Serial Number, Maximum Number of Devices, Current Number of Devices, and the Plug-in Package are displayed.

\* Plug-in Packages corresponding to the license key are imported during initial licensing. If there are no corresponding plug-ins, the functions are not available after user log in.

Available plug-in package functions are listed as follows:

Item	Plug-in Package Name	Function
1	Configuration	<ul style="list-style-type: none"> <li>■ Remote VNC</li> <li>■ GUI MIB Browser</li> </ul>
2	Security (Will develop on v3.0)	<ul style="list-style-type: none"> <li>■ Configuration</li> <li>■ File Comparison</li> <li>■ Simple Virus Checking</li> <li>■ System Log analysis</li> </ul>
3	Fault Management Enhancement	<ul style="list-style-type: none"> <li>■ Alarm Playback</li> <li>■ Off-Line Playback</li> <li>■ Smart Alarm Actions(Will develop on v3.0)</li> </ul>
4	Off-Line Map plug-in	Off-Line Map plug-in

## 7.2 User Management

### 7.2.1 Users Settings Page

Users with administrative privileges can view the User management page.

To open the Users page:

1. From the tool bar menu click **Admin**.
2. The Users management page displays. By default the Users tab is displayed.



Default Group: *Administrator Group* and *User Group* are set for the Role Group to distinguish different authorities.

- Administrator Group: Administrator may access all monitoring setting and managing functions. Please refer to “System Administrator” on page 106 for detailed functions.
- User Group: User may only access partial functions. Please refer to “System User” on page 105 for detailed functions.

## 7.2.2 Adding Users

Once a User profile is created, it is displayed under the Users > User list. Available listings can be further modified or deleted from the list.

To modify or delete an entry:

1. From the Users page, click **Add** to begin the function. The Add User page displays.
2. Enter the following required information to identify the profile:
  - Name (Case-sensitive field)
  - Password (Case-sensitive field)
  - E-mail
  - Mobile Phone number.

**Note!** Name and Password fields are case-sensitive.



3. From the Role Group field, click the drop-down menu to identify the user as an Administrator or User.
4. Click **OK** to add the user. If an exclamation mark appears by the side of the frame, it indicates that the information should be corrected or completed.

5. The user can be designated as an administrator or user. Click the Role Group drop-down menu to select a role. Selecting administrators sets the Topology Group field as Root Group. Selecting User for the profile requires assigning the profile authorization to an already created group(s).
6. If the Role Group is assigned as Users, click the Root Group option to allow the profile to view the devices defined in the *Topology Groups*.

7. Click **OK** to create the profile or **Cancel** to return to the previous screen without saving.

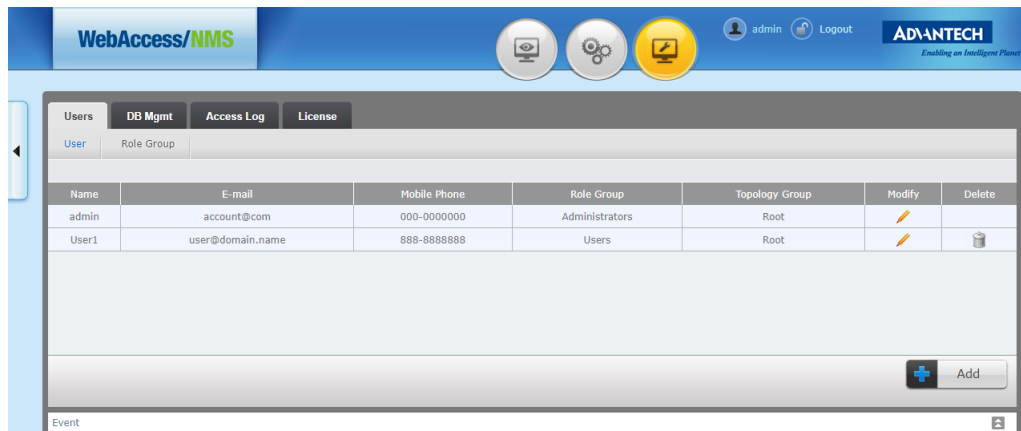
## 7.2.3 Modify and Delete Users

Once a User profile is created, it is displayed under the Users > User list.

Available listings can be further modified or deleted from the list.

To delete an entry:

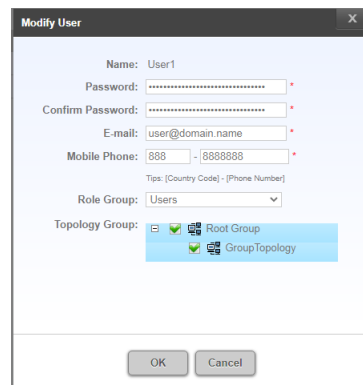
1. From the Users page, the list of available entries is displayed.



2. Select an entry and click the icon under Delete to remove the item.
3. A confirmation window displays, click **OK** to delete or **Cancel** to return to the previous menu.

Alternatively, to modify an entry:

4. Select an entry and click the icon under Modify to change the settings. The Modify User window displays.



The 'Modify User' dialog box is shown. It has fields for: Name (User1), Password (masked), Confirm Password (masked), E-mail (user@domain.name), Mobile Phone (888-8888888), Role Group (Users), and Topology Group (Root Group). There are 'OK' and 'Cancel' buttons at the bottom.

5. Change the following information to modify the profile:
  - Name (Case-sensitive field)
  - Password (Case-sensitive field)
  - E-mail
  - Mobile Phone number.

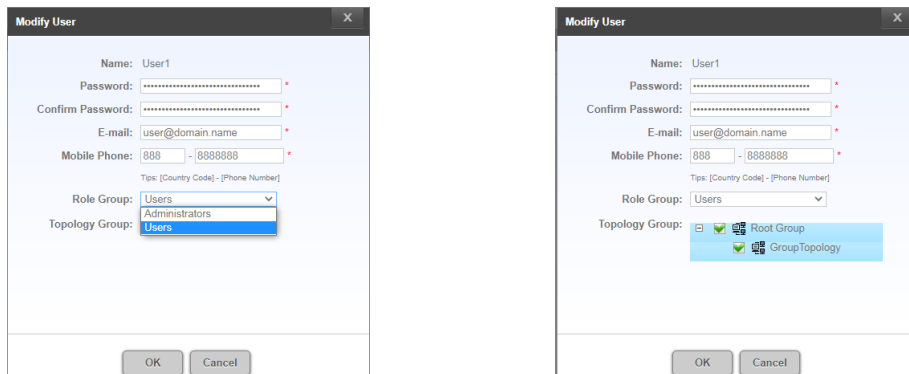
**Note!** Name and Password fields are case-sensitive.



6. From the Role Group field, click the drop-down menu to re-identify the user as an Administrator or User.
7. The user can be designated as an administrator or user. Click the Role Group drop-down menu to select a role. Selecting administrators sets the Topology Group field as Root Group. Selecting

User for the profile requires assigning the profile authorization to an already created group(s).

8. If the Role Group is assigned as Users, click the Root Group option to allow the profile to view the devices defined in the *Topology Groups*.



9. Click **OK** to modify the profile or **Cancel** to return to the previous screen without saving.

## 7.3 Database Management

### 7.3.1 Introduction for Database Management

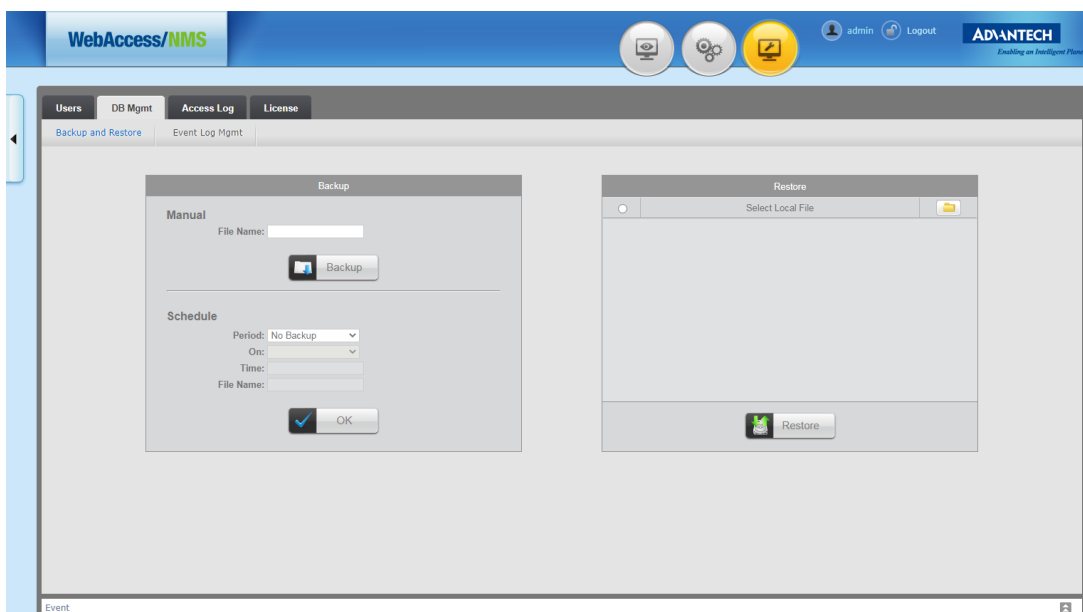
Regularly backup the database may lower the risk of data lost. Database backup, restoration and deletion are supported in this system. If there is error on the system, administrator can restore to particular time. If the history data is needed, administrator can also acquire from the system. This interface also includes the setting for the cycle, number of event log.

### 7.3.2 Database Backup

Users with administrative privileges can view the DB Mgmt page.


To open the DB Mgmt page:

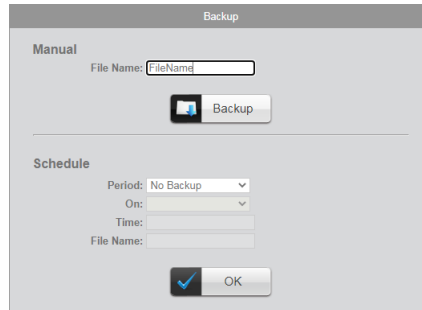
1. From the tool bar menu click **Admin**.  
The Users management page displays.
2. Click the **DB Mgmt** tab to view the Backup and Restore page.



Database backup can be configured as manual or scheduled function.

To perform a manual backup:

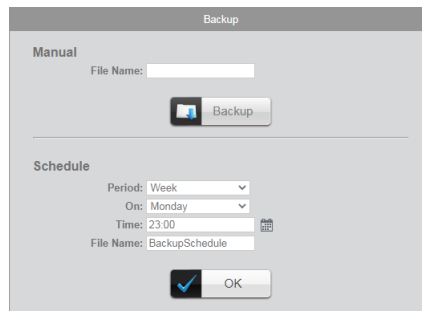
3. Enter the File Name to designate to the backup file.
4. Click **Backup**  to start the process.  
A window pops up and shows **Database Backup Setting Success** if the function was successful.



The screenshot shows a dialog box titled "Backup". It has two sections: "Manual" and "Schedule". In the "Manual" section, there is a "File Name:" label followed by a text input field containing "FileName" and a "Backup" button with a floppy disk icon. In the "Schedule" section, there is a "Period:" dropdown menu set to "No Backup", an "On:" dropdown menu, a "Time:" text input field, and a "File Name:" text input field. At the bottom of the "Schedule" section is an "OK" button with a checkmark icon.

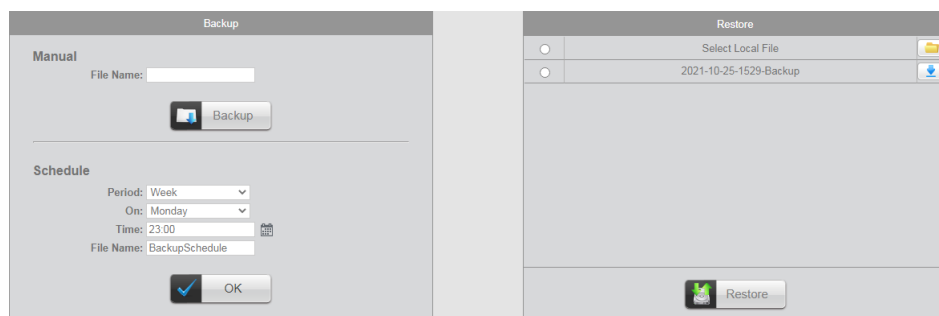
To schedule a backup:

5. Click the Period drop-down menu to select the schedule frequency, options include: No Backup (Default), Week, or Month.
6. Click the On drop-down menu to select the day of the week to start the function.
7. Enter a specific time in the Time field or click the calendar icon to select a time period for the start of the schedule.
8. In the File Name field, enter the name to designate to the backup file.
9. Click **OK** to create the scheduled event.



This screenshot shows the same "Backup" dialog box as above, but with the "Schedule" section selected. The "Period:" dropdown is set to "Week", the "On:" dropdown is set to "Monday", the "Time:" field is set to "23:00" with a calendar icon to its right, and the "File Name:" field is set to "BackupSchedule". The "OK" button is still present at the bottom.

All backup entries are listed in the Restore panel as shown in the following figure.



The screenshot shows two panels side-by-side. The left panel is the "Backup" dialog box with the "Schedule" section selected, showing "Period: Week", "On: Monday", "Time: 23:00", and "File Name: BackupSchedule". The right panel is the "Restore" panel, which has a "Select Local File" button and a list of backup entries. One entry is visible: "2021-10-25-1529-Backup" with a download icon. At the bottom of the "Restore" panel is a "Restore" button with a floppy disk icon.

### 7.3.3 Database Restore

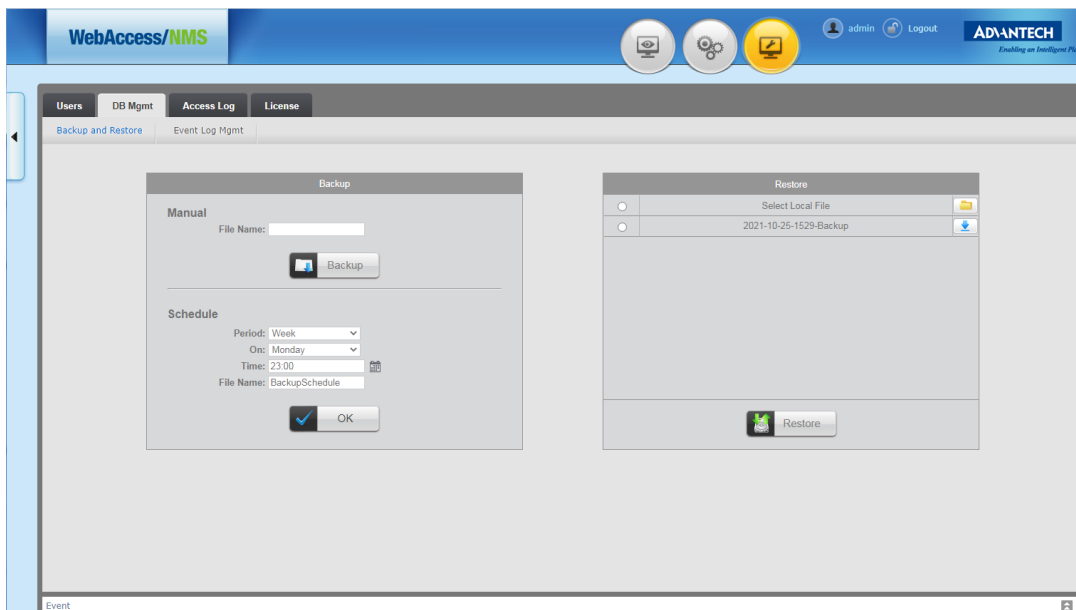
Users with administrative privileges can view the DB Mgmt page and restore a database.


To open the DB Mgmt page:

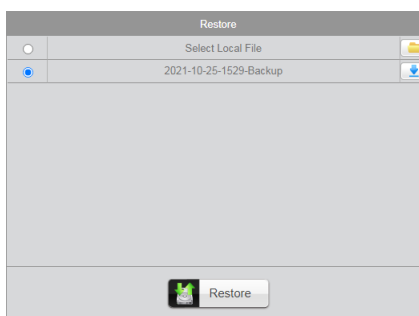
1. From the tool bar menu click **Admin**.  
The Users management page displays.





- Click the **DB Mgmt** tab to view the Backup and Restore page.



- Select an entry from the Restore list and click **Restore**  **Restore** to begin the process.



Alternatively, you can browse for a saved local file.

- Click the radio button to enable Select Local File.
- Click the icon  to open an explorer window.
- Select the local file and click **Open** to continue.
- Click **Restore**  **Restore** to begin the process.
- A pop up window displays **Are you sure you want to restore?** Click **Yes** to proceed or **Cancel** to return to the previous menu. The process completes and the database is restored.

### 7.3.4 Event Log Management

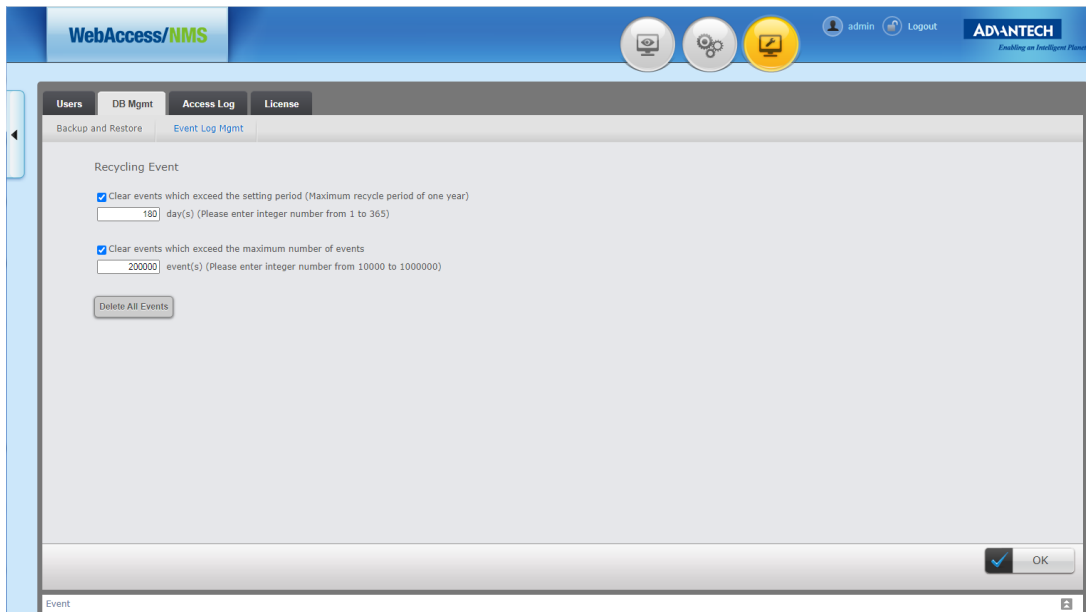
The database of WebAccess/NMS has recorded the status of devices, polling failure, link down and status change. The recycling time period and upper limit number of event can also be set. The record can be deleted by clicking **Delete All Events**.

Users with administrative privileges can view the DB Mgmt page.

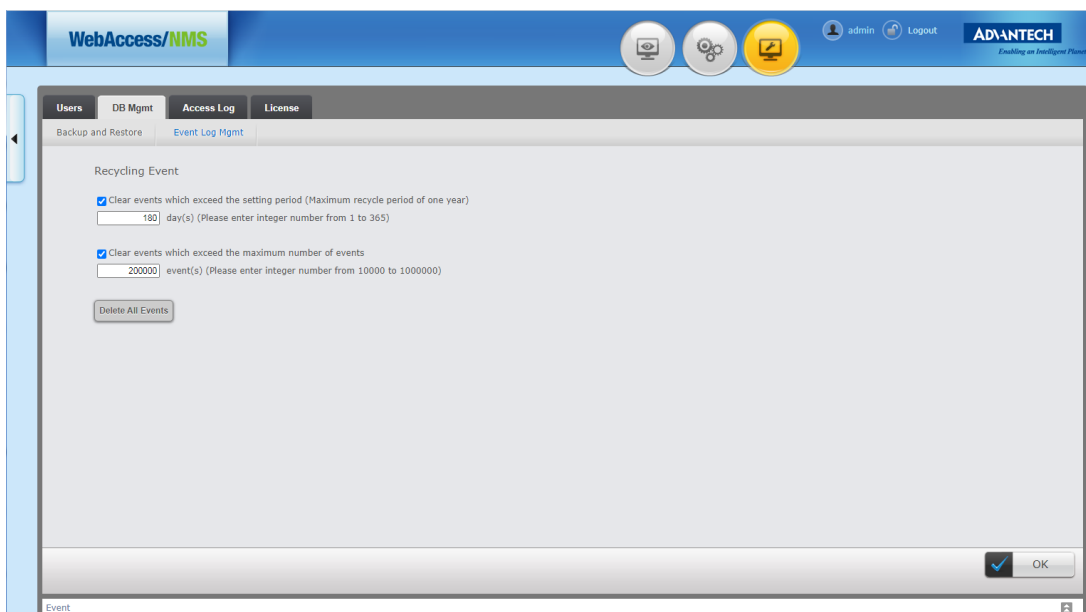
To open the DB Mgmt page:

- From the tool bar menu click **Admin**.  
The Users management page displays.

2. Click the **DB Mgmt** tab, then **Event Log Mgmt** to view the page.



3. Click **Delete All Events** to delete all event records.  
Alternatively, you can set automatic recycling event log function to delete events based on a time period or number threshold. Once either of the thresholds is reached, the recycling function is activated.
4. Click the day(s) field to disable or enable the setting period.
5. Enter a variable (1~365) to set the threshold in days to enable the delete events function.
6. Click the number of events field to disable or enable the maximum number of events policy.
7. Enter a variable (10000~1000000) to set the threshold in number of events to enable the delete events function.
8. Click OK to save the Event Log Mgmt settings.



If both settings are not checked, all events are saved.

## 7.4 Access Log

### 7.4.1 Introduction for Access Log

WebAccess/NMS can record system access logs such as: Log-in, Log-out, function operating procedure. The following access log categories are available:

- Add/Del/Edit device
- Add/Del line
- Add/Del/Edit EMS Group
- Add/Del/Edit Topology Group
- Add/Del/Edit Supported Device
- Add/Del/Edit FW Upgrade
- Add/Del/Edit Config Backup
- Add/Del/Edit Config Restore
- Add/Del/Edit User
- Apply Message Event
- Apply Message Correlation
- Apply DB Manual/Schedule/No Backup
- Apply SMS,Email, Trap
- Clear/Ack Event Log
- Change the Event Log Mgmt
- Configure device (set)
- Delete All Events
- Edit Severity
- Import License Key
- Operation for Access Log
- Open MIB Browser
- Open Web Browser
- Restore DB
- WebAccess/NMS Login/Logout

Log entries can be searched based on: Device Name, IP Address, Type (includes Configuration, Maintenance, SystemAdmin), Date, and User.

To search for a log entry:

1. From the tool bar menu click **Admin**.  
The Users management page displays.

- Click the **Access Log** tab, the Access Log page displays.

Index	Access Time	Device Name	IP Address	MAC Address	Type	User	Description
1	2021-10-25 15:29:16	NMS			SystemAdmin	admin	Database Manual Backup Backup
2	2021-10-25 14:37:36	NMS			SystemAdmin	admin	Modify user User1 success
3	2021-10-25 11:53:10	EMDevice	192.168.1.165	192.168.1.165	Configuration	admin	Add device EMDevice (192.168.1.165) successfully
4	2021-10-25 11:32:00	NMS			SystemAdmin	admin	Modify Topology Group GroupTopology
5	2021-10-25 11:14:58	NMS			SystemAdmin	admin	Add Topology Group GroupTopology
6	2021-10-25 11:14:36	NMS			SystemAdmin	admin	Modify EMS Group EMS001
7	2021-10-21 17:35:41	NMS			SystemAdmin	admin	Delete EMS Group EMSGroup
8	2021-10-21 17:35:30	NMS			SystemAdmin	admin	Add EMS Group EMSGroup
9	2021-10-20 17:34:02	NMS			SystemAdmin	admin	Login success
10	2021-10-20 17:33:34	NMS			SystemAdmin	admin	Logout success
11	2021-10-20 17:31:11	NMS			SystemAdmin	admin	Login success
12	2021-10-20 17:30:32	NMS			SystemAdmin	admin	Logout success
13	2021-10-20 17:30:26	NMS			SystemAdmin	admin	Modify user User1 success
14	2021-10-20 17:29:46	NMS			SystemAdmin	admin	Login success
15	2021-10-20 17:29:25	NMS			SystemAdmin	admin	Logout success
16	2021-10-20 17:29:16	NMS			SystemAdmin	admin	Add user User1 success
17	2021-10-20 17:27:43	NMS			SystemAdmin	admin	Login success
18	2021-10-20 17:27:26	NMS			SystemAdmin	admin	Logout success
19	2021-10-20 17:26:35	NMS			SystemAdmin	admin	Login success

- Click to access additional criteria to initiate a search of the entry log history list.

Index	Access Time	Device Name	IP Address	MAC Address	Type	User	Description
1	2021-10-25 15:29:16	NMS			SystemAdmin	admin	Database Manual Backup Backup
2	2021-10-25 14:37:36	NMS			SystemAdmin	admin	Modify user User1 success
3	2021-10-25 11:53:10	EMDevice	192.168.1.165	192.168.1.165	Configuration	admin	Add device EMDevice (192.168.1.165) successfully
4	2021-10-25 11:32:00	NMS			SystemAdmin	admin	Modify Topology Group GroupTopology
5	2021-10-25 11:14:58	NMS			SystemAdmin	admin	Add Topology Group GroupTopology
6	2021-10-25 11:14:36	NMS			SystemAdmin	admin	Modify EMS Group EMS001
7	2021-10-21 17:35:41	NMS			SystemAdmin	admin	Delete EMS Group EMSGroup
8	2021-10-21 17:35:30	NMS			SystemAdmin	admin	Add EMS Group EMSGroup
9	2021-10-20 17:34:02	NMS			SystemAdmin	admin	Login success
10	2021-10-20 17:33:34	NMS			SystemAdmin	admin	Logout success
11	2021-10-20 17:31:11	NMS			SystemAdmin	admin	Login success
12	2021-10-20 17:30:32	NMS			SystemAdmin	admin	Logout success
13	2021-10-20 17:30:26	NMS			SystemAdmin	admin	Modify user User1 success
14	2021-10-20 17:29:46	NMS			SystemAdmin	admin	Login success
15	2021-10-20 17:29:25	NMS			SystemAdmin	admin	Logout success
16	2021-10-20 17:29:16	NMS			SystemAdmin	admin	Add user User1 success
17	2021-10-20 17:27:43	NMS			SystemAdmin	admin	Login success
18	2021-10-20 17:27:26	NMS			SystemAdmin	admin	Logout success
19	2021-10-20 17:26:35	NMS			SystemAdmin	admin	Login success

# Chapter 8

WebAccess / NMS  
Setting Interface

## 8.1 Device Data

### 8.1.1 Introduction for Device Data

There are four functions under the Device Data menu:

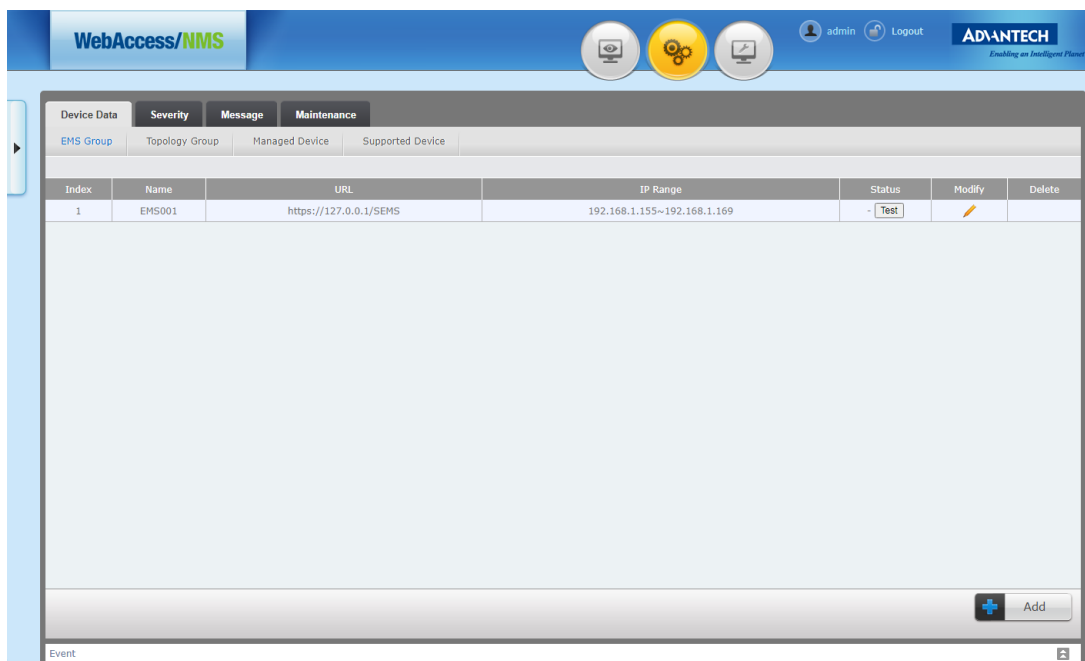
- EMS Group
- Topology Group
- Managed Device
- Supported Device

The function allows users to add/delete EMS group and Topology Group, and manage all information of the devices include *Device Model*, *Location* or *IP Address*. The device information can be set in advance for easier management.

### 8.1.2 EMS Group

To add an EMS group:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.



2. Click **Add** to open the Add EMS Group page.
3. Enter the required information as listed in the following:  
*EMS Group* page and the *Name*, *URL* and *IP range*.
4. Click **OK** to add the new EMS group entry or **Cancel** to return to the previous menu.

**Add EMS Group**

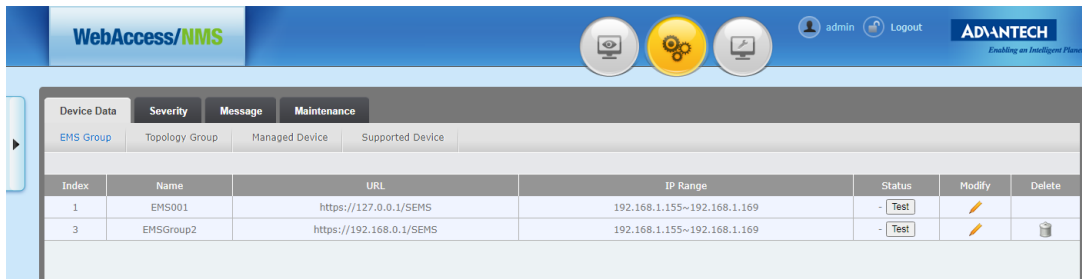
Name:  \*

URL: https://  /SEMS \*  
e.g., 192.168.0.1

IP Range:  \*  
e.g., 192.168.0.1~192.168.0.10

OK Cancel

- To view the status of the entry, click Test.  
An Active state describes a connected EMS group.  
An Unactive state describes issues with the EMS group and WebAccess/NMS connection.



Index	Name	URL	IP Range	Status	Modify	Delete
1	EMS001	https://127.0.0.1/SEMS	192.168.1.155~192.168.1.169	- Test		
3	EMSGroup2	https://192.168.0.1/SEMS	192.168.1.155~192.168.1.169	- Test		

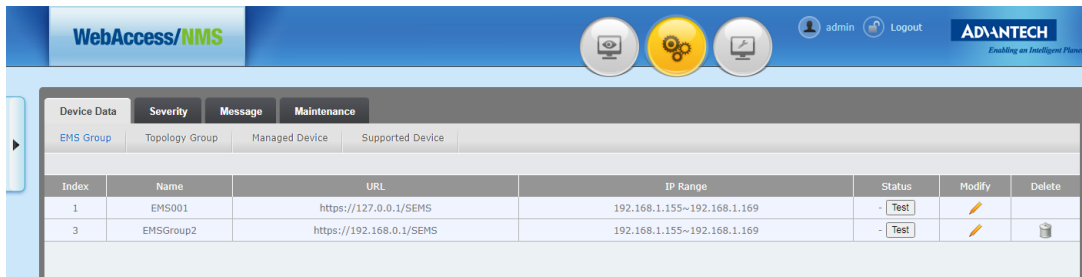
### 8.1.3 Modify and Delete EMS Groups

Once an EMS Group is created, it is displayed under the Service > Device Data > EMS Group list.

Available listings can be further modified or deleted from the list.

To delete an entry:

- From the EMS Group page, the list of available entries is displayed.

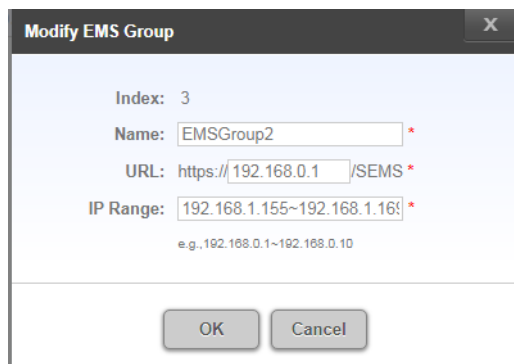


Index	Name	URL	IP Range	Status	Modify	Delete
1	EMS001	https://127.0.0.1/SEMS	192.168.1.155~192.168.1.169	- Test		
3	EMSGroup2	https://192.168.0.1/SEMS	192.168.1.155~192.168.1.169	- Test		

- Select an entry and click the icon under Delete to remove the item.
- A confirmation window displays, click **OK** to delete or **Cancel** to return to the previous menu.

Alternatively, to modify an entry:

- Select an entry and click the icon under Modify to change the settings.  
The Modify EMS window displays.



**Modify EMS Group**

Index: 3

Name:  \*

URL:  \*

IP Range:  \*

e.g., 192.168.0.1~192.168.0.10

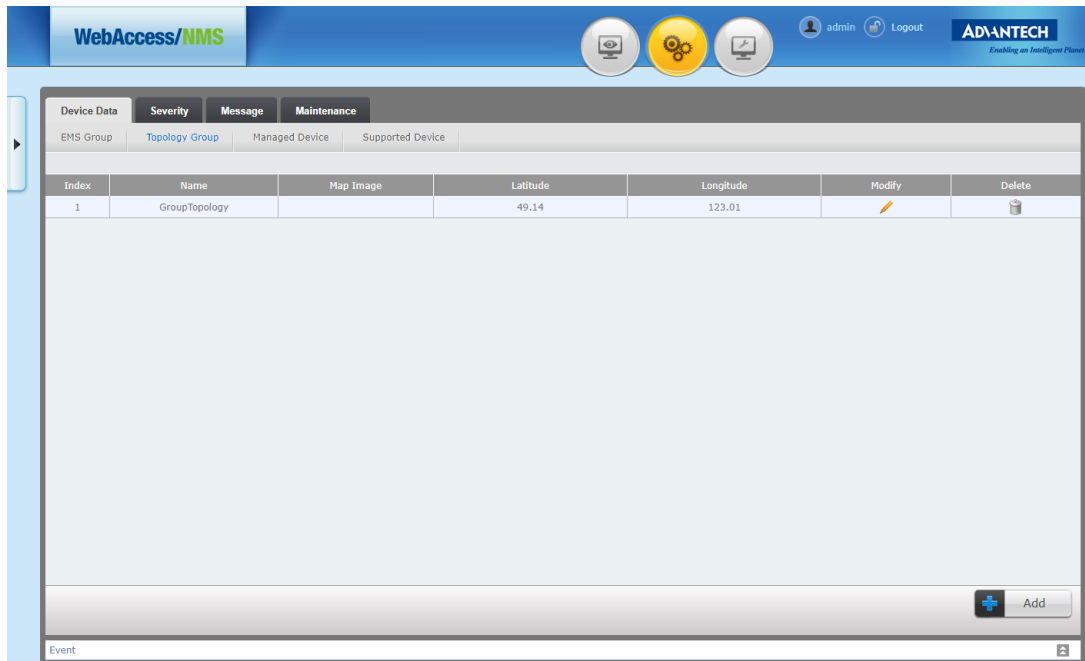
- Click **OK** to modify the EMS Group or **Cancel** to return to the previous screen without saving.


### 8.1.4 Topology Group

To add a Topology group:

- From the tool bar menu click **Setting**.  
The Device Data page displays.


2. Click the **Topology Group** tab, the Topology Group page displays.



3. Click **Add**  to open the Add Topology Group page.
4. Enter the required information as listed in the following:
  - Name
  - Map Image: Click the browse icon to select a local file.
  - Latitude
  - Longitude
5. Click **OK** to create the group or **Cancel** to return to the previous menu.

**Add Topology Group**

Name:  \*

Map Image:  

Latitude:

Longitude:

OK Cancel

### 8.1.5 Modify and Delete Topology Groups

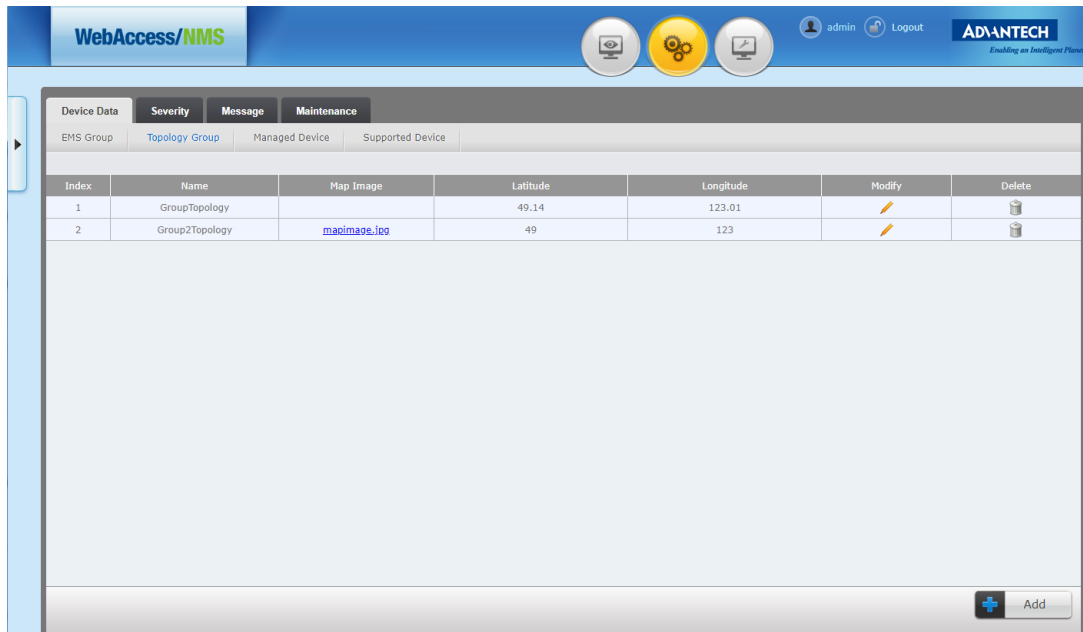
Once a Topology Group is created, it is displayed under the Service > Device Data > Topology Group list.

Available listings can be further modified or deleted from the list.

To delete an entry:



1. From the Topology Group page, the list of available entries is displayed.



2. Select an entry and click the icon under Delete to remove the item.
3. A confirmation window displays, click **OK** to delete or **Cancel** to return to the previous menu.  
Alternatively, to modify an entry:
4. Select an entry and click the icon under Modify to change the settings.  
The Modify Topology Group window displays.

5. Click **OK** to modify the Topology Group or **Cancel** to return to the previous screen without saving.

## 8.1.6 Managed Device

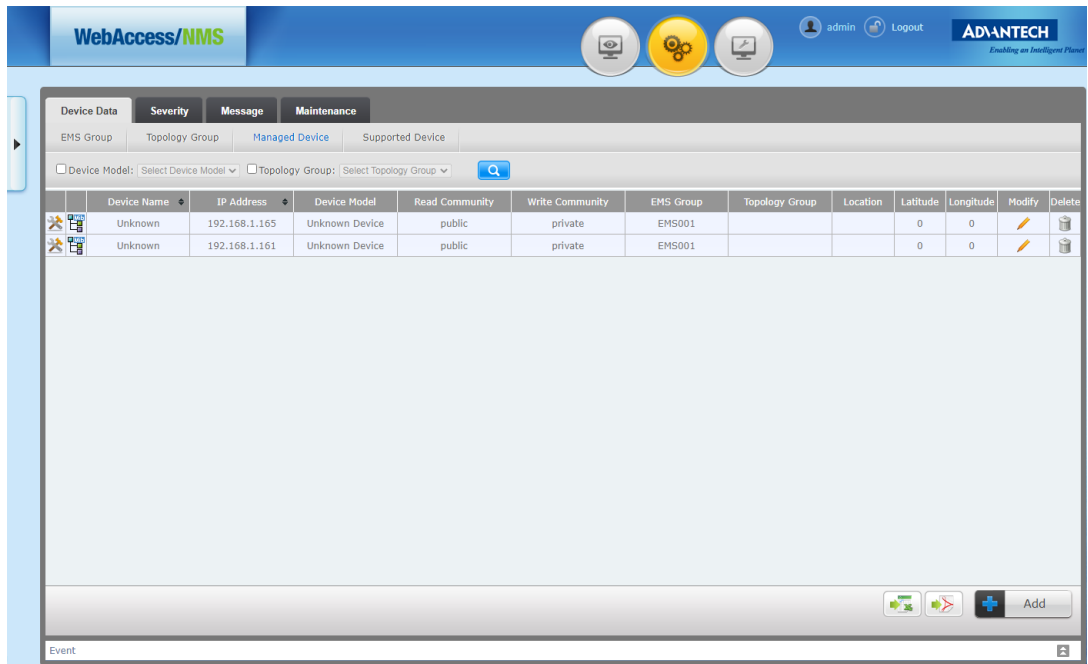
The information of managed devices are shown through the Managed Device function\*.


\* The number of *Managed Devices* is related to the number of selected *Device Discovery* of Monitoring for managing or inspecting.

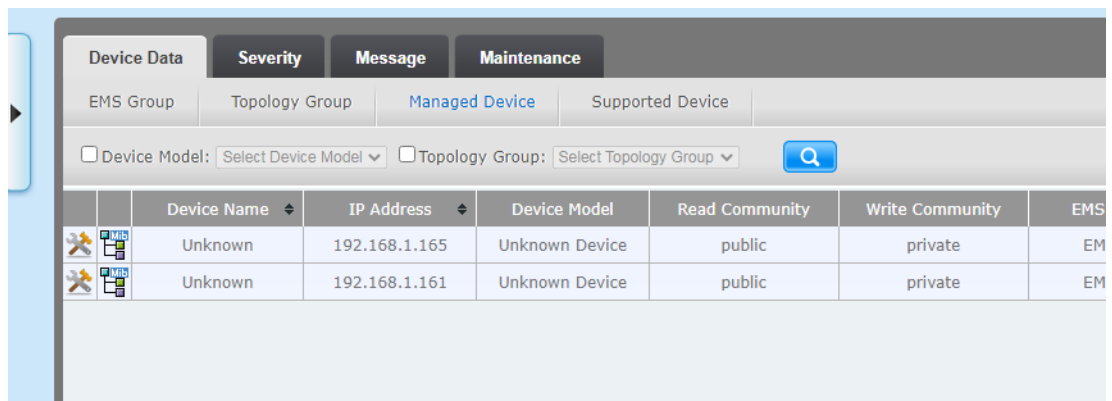
To add an EMS group:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.


- Click the **Managed Device** tab, the Managed Device page displays.

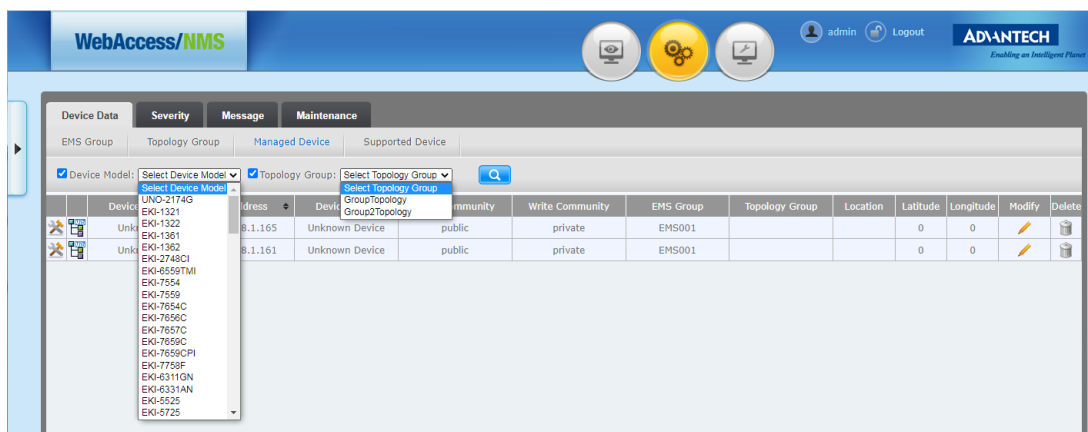


- Clicking on the  icon beside Device Name can change the listed sorting order.





To search for a device, the device model or topology group criteria is used to initiate the search function.

- Click on either the Device Model or Topology Group or both to enable the drop-down menu for options.
- Click the drop-down menu and select the search criteria.
- Click  to start the search.

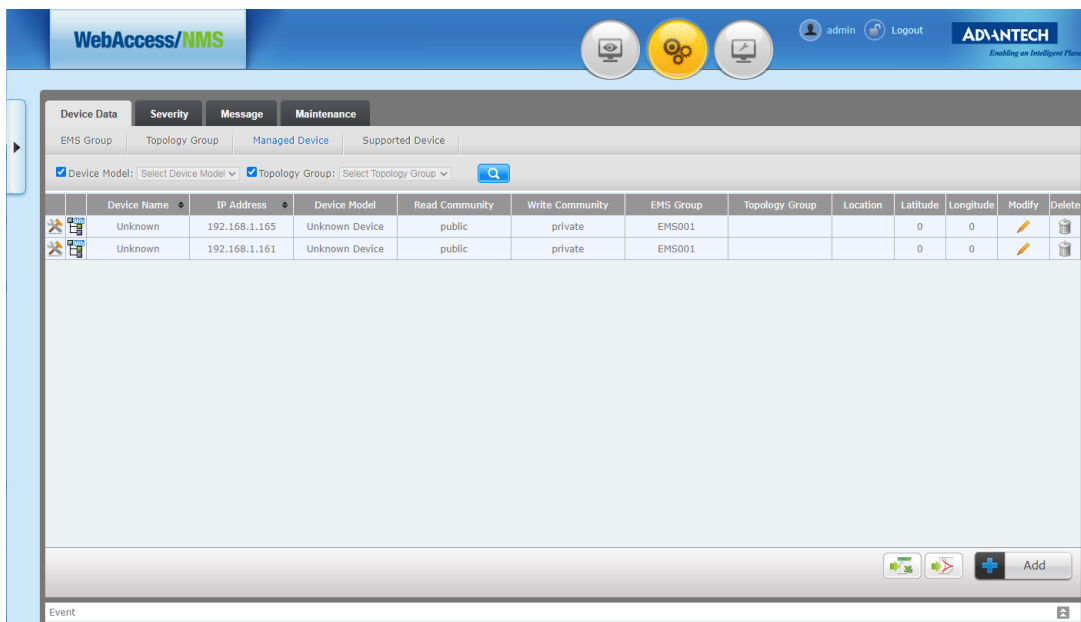


The displayed entry pool can be exported to an Excel or PDF file.

- To export the managed device list, click on either the Excel  or PDF  options.  
Once successfully exported, the Excel file is saved to the designated download folder.

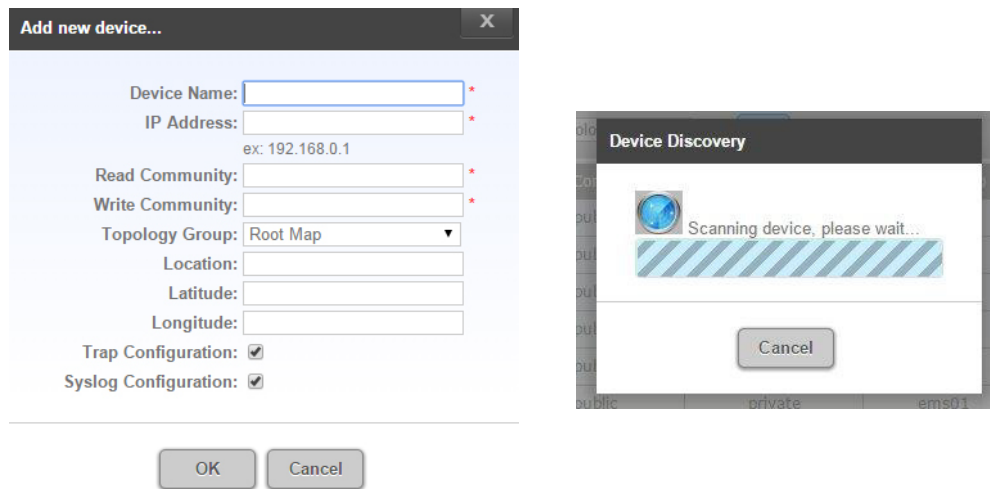
### 8.1.6.1 Adding New Devices

- From the tool bar menu click **Setting**.  
The Device Data page displays.
- Click the Managed Device tab. The Managed Device page displays.



- Click on **Add** to start the process. The **Add new device...** page displays.
- Enter the required information to define the entry.
  - Device Name
  - IP Address
  - Read Community (Default Setting: public)
  - Write Community (Default Setting: public)
  - Topology Group
  - Location
  - Latitude
  - Longitude
- By default the Trap Configuration and Syslog Configuration settings are enabled. Click to disable the options.
- Click **OK** to add the device or **Cancel** to return to the previous menu.  
The system adds the entry otherwise a notification displays with any errors.

\* If the *Trap Configuration* and *Syslog Configuration* are checked, the newly added device can be set automatically, and trap or variation can also be sent to the system.



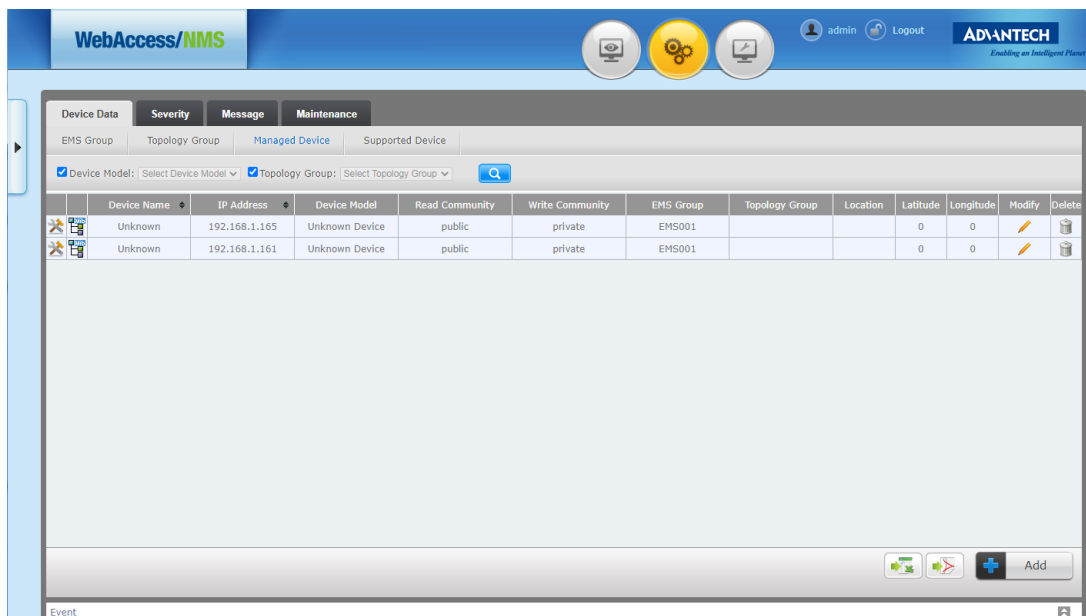
## 8.1.7 Modify and Delete Managed Devices

Once a device is added, it is displayed under the Service > Device Data > Managed Device list.

Available listings can be further modified or deleted from the list.


To delete an entry:


1. From the Managed Device page, the list of available entries is displayed.



2. Select an entry and click the icon under Delete to remove the item.
3. A confirmation window displays, click **OK** to delete or **Cancel** to return to the previous menu.

Alternatively, to modify an entry:

- Select an entry and click the icon  under Modify to change the settings. The Edit Device... window displays.



- After making the necessary changes, click **OK** to modify the Device entry or **Cancel** to return to the previous screen without saving.

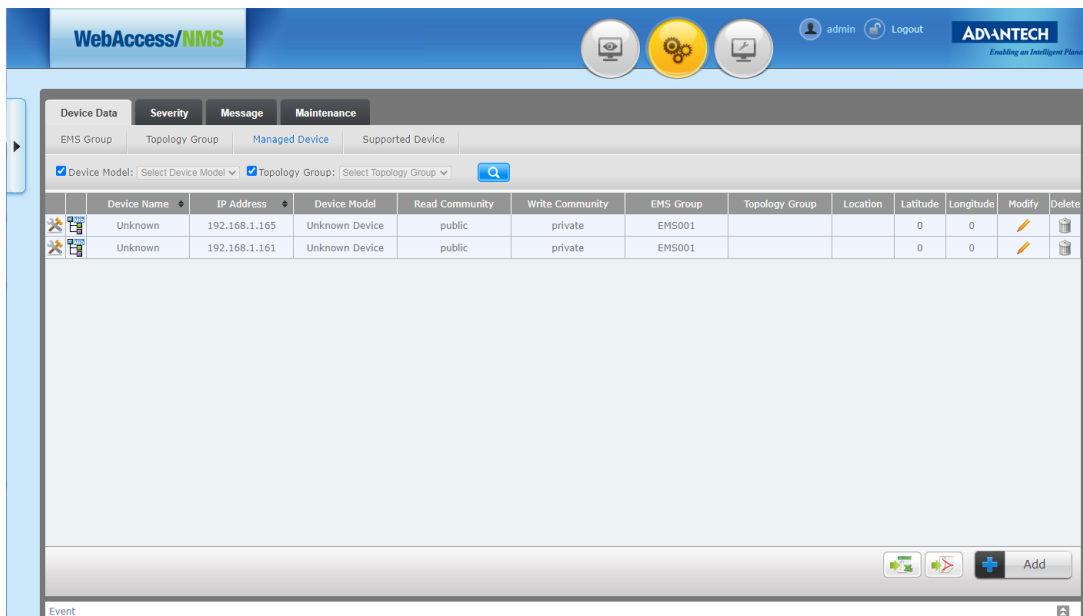
### 8.1.8 Configure Managed Devices

Once a device is added, it is displayed under the Service > Device Data > Managed Device list.


Available listings can be further configured.

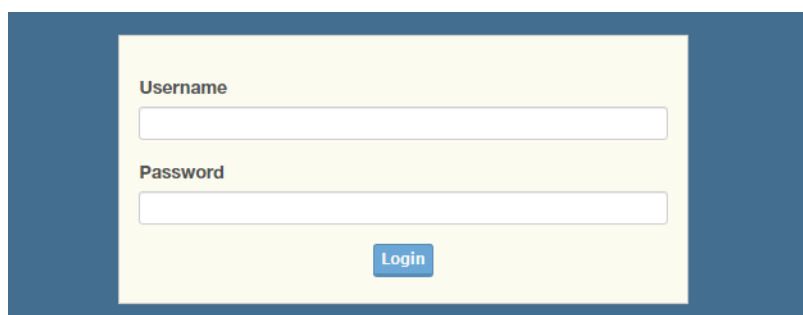
To configure an entry:

- From the Managed Device page, the list of available entries is displayed.



Device Name	IP Address	Device Model	Read Community	Write Community	EMS Group	Topology Group	Location	Latitude	Longitude	Modify	Delete
Unknown	192.168.1.165	Unknown Device	public	private	EMS001			0	0		
Unknown	192.168.1.161	Unknown Device	public	private	EMS001			0	0		

- Click  on the entry to configure. The device's login page displays on the default browser.

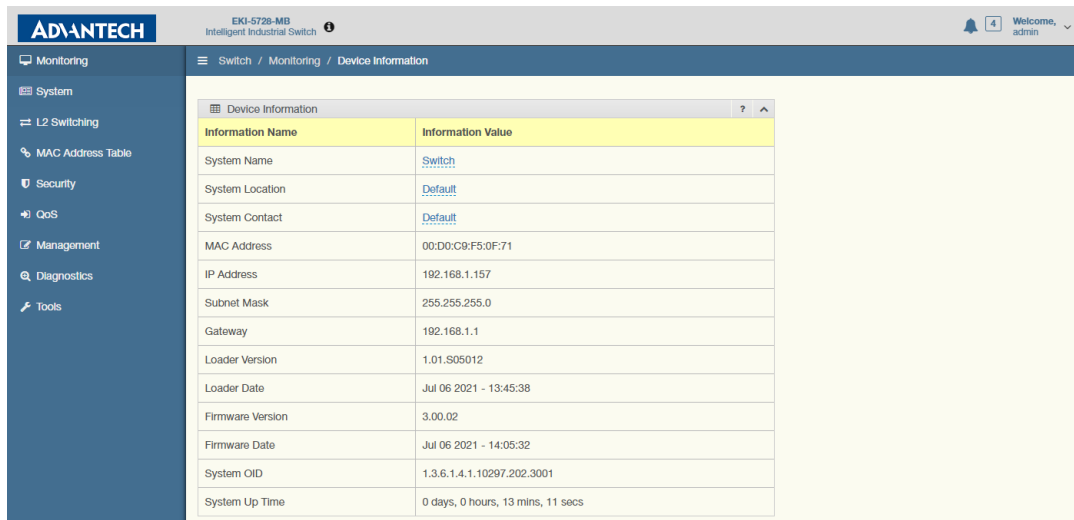


3. Enter the device username and password.  
(Default account: admin password: admin)  
The user interface offer access to the device's settings.

**Note!** There are no need for entering account and password for serial server.




The Device Information user interface displays. See the following figure.

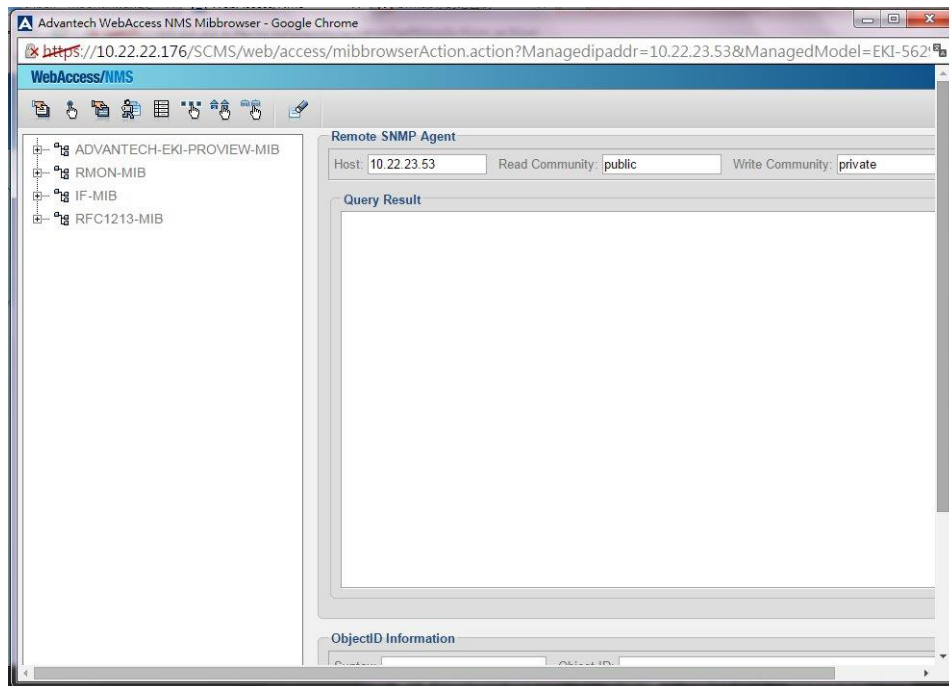


Device's can also be configured through the use of the MIB browser.

To access the MIB browser:

4. From the Managed Device page, click the  MIB browser icon.  
The WebAccess/NMS window displays.

\* If the license key does not support this function, the MIB file setting function is not accessible.

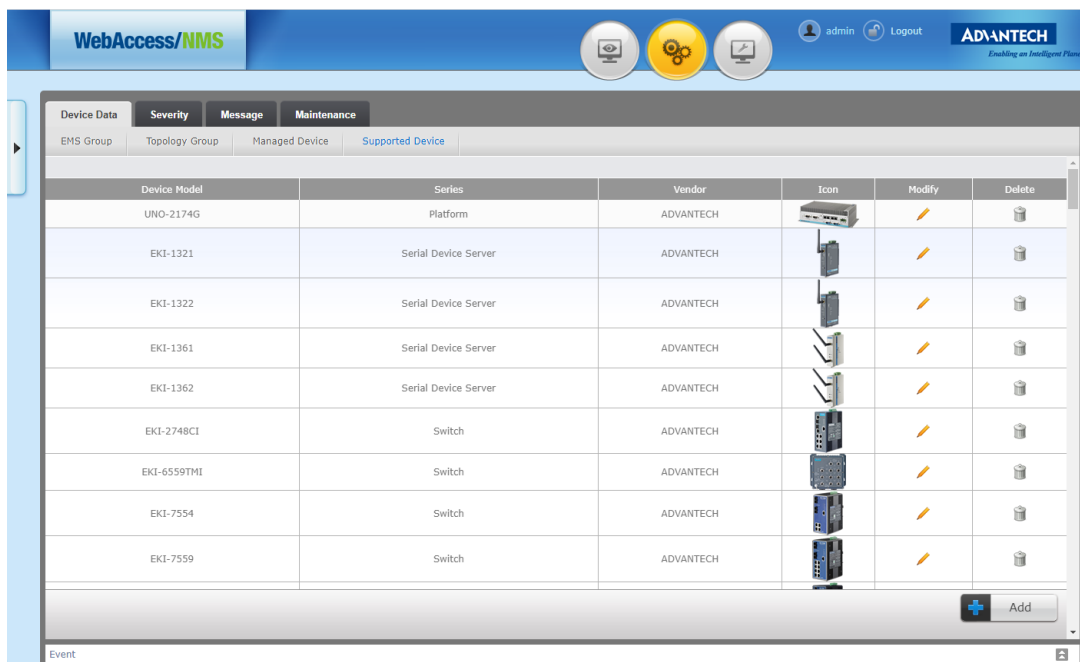


## 8.1.9 Supported Device

The Supported Device function displays the following device information: Device Model, Series, Vendor and device icon. The settings for the supported device can be configured.

To view supported devices:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.
2. Click the **Supported Device** tab, the Supported Device page displays.



To revise or delete a supported device:

3. Click to open the device page.

4. Modify the settings on the device page.
5. Click OK to continue or Cancel to return to the previous page.  
To delete a supported device:

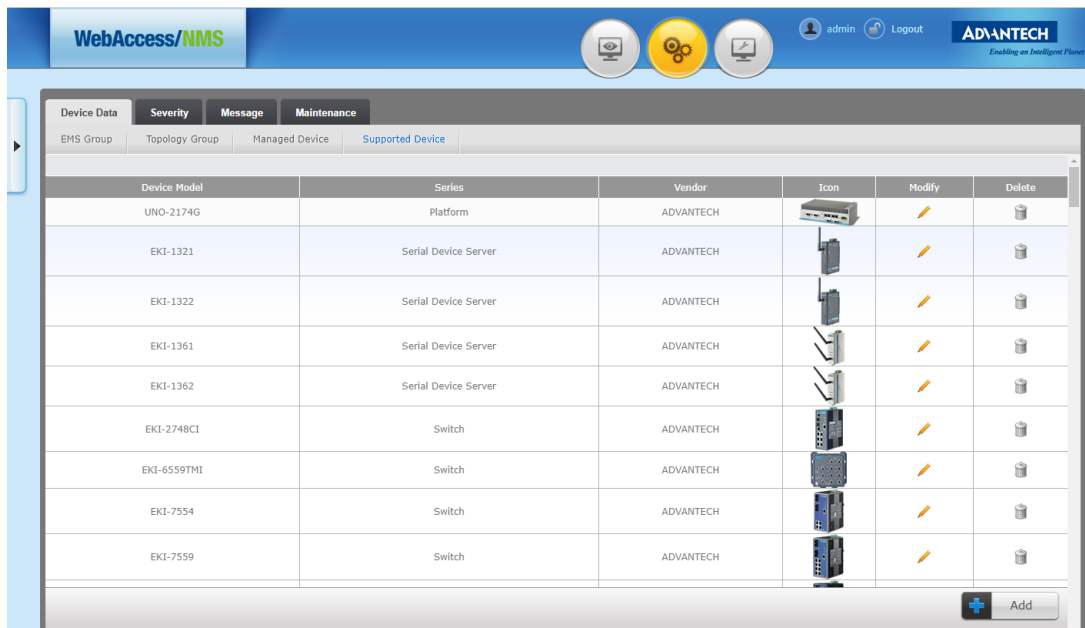
6. Click  to delete the supported device.

\* The icons of device are stored on the path:

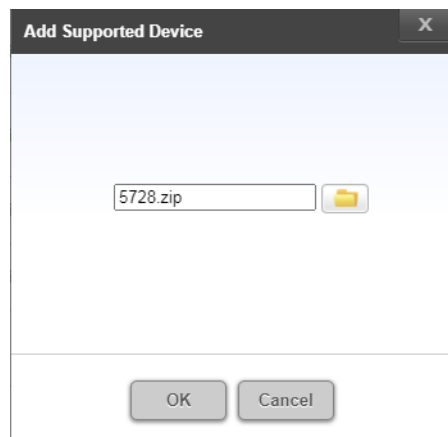
C:\ProgramFiles\ApacheSoftwareFoundation\Tomcat7.0\webapps\SCMS\web\access\img\topology\_device

### 8.1.9.1 Adding Supported Devices

1. From the tool bar menu click **Setting**.  
The Device Data page displays.
2. Click the Supported Device tab. The Supported Device page displays.



3. Click on **Add** to start the process. The **Add Supported Device** page displays.
4. Click the browse icon to select a device file.
5. After selecting a file, click **OK** to create a new entry or **Cancel** to return to the previous menu.





6. Choose the *Device Model* and click **OK**. The device entry is added to the list on the Supported Device.



## 8.2 Severity

### 8.2.1 Introduction for Severity

The Severity function provides the following information: Trap and Ping. Administrator can setup trap message (Trap) and system polling (Ping). Colors indicate different alarm levels, as described in the following:

- Critical situations are marked as RED
- Major situations are marked as ORANGE
- Minor situations are marked as YELLOW
- Normal situations are marked as GREEN.

Alarm message are displayed in Message and Topology. If an alarm is activated, the administrator is notified through the configured method: SMS, E-mail or Trap.

---

## 8.2.2 Severity Operational Procedures

### 8.2.2.1 Trap

There are pre-defined default trap events listed on the Trap page such as the following:


- Polling Failed
- Slow Response
- Link Down
- Warm Start
- Cold Start
- Authentication Failed
- Polling Success
- Link Up
- Temperature Alarm
- Voltage Alarm
- Temperature Alarm Cleared
- Voltage Alarm Cleared
- Removable Device Alarm
- XRing Master Change
- WLAN Roaming
- Configuration changed
- Monitor process disappear
- Power 1 Transition
- Power 2 Transition
- Config Change
- Login Fail
- Port Looping

To view modify the severity of a trap:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Severity** tab to view the Trap page.

Trap	Severity	Color	Modify
Polling Failed	Critical	Red	✏️
Slow Response	Minor	Yellow	✏️
Link Down	Major	Orange	✏️
Warm Start	Major	Orange	✏️
Cold Start	Major	Orange	✏️
Authentication Failed	Minor	Yellow	✏️
Polling Success	Normal	Green	✏️
Link Up	Normal	Green	✏️
Temperature Alarm	Critical	Red	✏️
Voltage Alarm	Critical	Red	✏️
Temperature Alarm Cleared	Normal	Green	✏️
Voltage Alarm Cleared	Normal	Green	✏️
Removable Device Alarm	Minor	Yellow	✏️
XRing Master Change	Minor	Yellow	✏️
WLAN Roaming	Minor	Yellow	✏️
Configuration changed	Major	Orange	✏️
Monitor process disappear	Major	Orange	✏️
Power 1 Transition	Minor	Yellow	✏️
Power 2 Transition	Minor	Yellow	✏️
Config Change	Minor	Yellow	✏️

3. Administrator can modify severity by clicking on  icon.
4. Click the drop-down menu to select and designate a severity setting for the trap.

## 8.3 Message

### 8.3.1 Introduction for the Message

The Message menu provides access to the following functions:

- Notification for *SMS/E-mail/Trap/Sound/External Program*
- Event
- Correlation
- Throughput Monitor
- Playback

Administrator can test the functionality through WebAccess/NMS and confirm normal status. Alarm notifications can be delivered to via various methods to assigned profiles.

The alarm message can be sent by SMS, E-mail or Trap to the person in charge.

## 8.3.2 Message Operational Procedures

### 8.3.2.1 Notification

User may test the following functions: SMS, E-mail, Trap, or Sound.

To configure a setting:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.
2. Click the **Message** tab to view the Notification page.

The screenshot shows the WebAccess/NMS interface. At the top, there is a navigation bar with 'WebAccess/NMS' on the left and user information (admin, Logout) and the ADVANTECH logo on the right. Below the navigation bar, there are several tabs: 'Device Data', 'Severity', 'Message', and 'Maintenance'. The 'Message' tab is selected, and it contains sub-tabs: 'Notification', 'Event', 'Correlation', 'Playback', 'Advanced', and 'Process Monitor'. The 'SMS' section is active, showing two radio button options: 'OLD API' (selected) and 'NEW API'. Under 'OLD API', there are input fields for 'API ID', 'User', and 'Password'. Under 'NEW API', there is an input field for 'API Key'. Below these, there is a 'Mobile Phone' section with 'Country Code' and 'Mobile Phone Number' input fields, and 'Test' and 'Apply' buttons. The 'E-mail' section is also visible, showing 'SMTP Setting' with fields for 'SMTP Host' (smtp.gmail.com), 'SMTP Port' (587), and a 'From' section with 'Account' and 'Password' fields. There is also a 'Mail List' section with an 'E-Mail Key' field.

To test the SMS function:

3. In the SMS Setting panel, click to select an Old API or New API type entry.
4. In the respective field, enter the following information:

Old API:

- Enter the API ID
- User Name
- Password of the enterprise internal SMS settings

Or

Old API:

- Enter the API Key

This screenshot is a close-up of the SMS configuration panel from the previous image. It shows the 'Mobile Phone' section with two input fields: 'Country Code' and 'Mobile Phone Number'. Below these fields are 'Test' and 'Apply' buttons. The 'OLD API' radio button is selected.

5. In the Mobile Phone field enter the country code and mobile phone number to define the recipient of the notification.
6. Click **Test** to confirm the setting. If the settings are not accepted, an error displays, otherwise continue with the configuration.

7. Click **Apply** to create a notification option.

To test the E-mail function:

8. In the E-mail panel, enter the following information to complete the configuration and connect the notification feature to the enterprise's mail server:
  - SMTP Host
  - SMTP Port
  - Sender's E-mail account and password
  - E-mail to (used to test the settings)
9. Click **Test** to send a test E-mail to the E-mail to test account. If the settings are not accepted, an error displays, otherwise continue with the configuration.
10. Click **Apply** to create a notification option.

The screenshot shows the WebAccess/NMS configuration interface. The top navigation bar includes 'WebAccess/NMS', user 'admin', and a 'Logout' button. The main content area is divided into several sections: 'NEW API' with fields for 'API Key' and 'Mobile Phone' (509-1234567); 'E-mail' settings including 'SMTP Setting' (Host: smtp.gmail.com, Port: 587, TLS), 'From' (Account and Password), and 'Mail List' (E-Mail to); and 'Trap' settings (Trap Server IP, Trap Community: public, Trap Version: V2). Each section has 'Test' and 'Apply' buttons.

To test the Trap function:

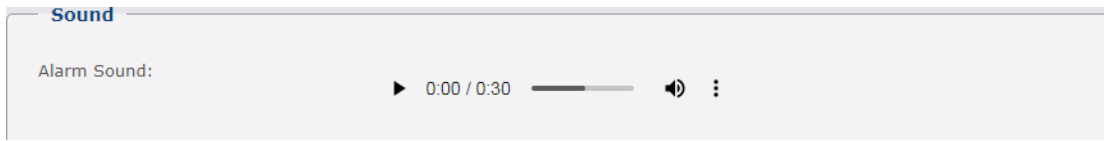
11. In the Trap panel, enter the following information to complete the configuration:
  - Trap Server IP
  - Trap Community
  - Trap Version (default: public)
12. Click **Test** to validate the settings. If the trap server obtains the sender test record, the settings are validated. Otherwise review the settings to determine the error.
13. Click **Apply** to create a trap notification.

This is a close-up of the 'Trap' configuration panel. It contains three input fields: 'Trap Server IP' (empty), 'Trap Community' (filled with 'public'), and 'Trap Version' (a dropdown menu set to 'V2'). Below the fields are 'Test' and 'Apply' buttons.

To test the Sound alert:

14. In the Sound panel, click the Play icon to test the alarm notification.
15. Slide the level bar left to right to adjust the volume of the alarm.
16. Click the Mute function to turn off the audio levels.
17. Click the settings icon to view the Download and Playback Speed options.

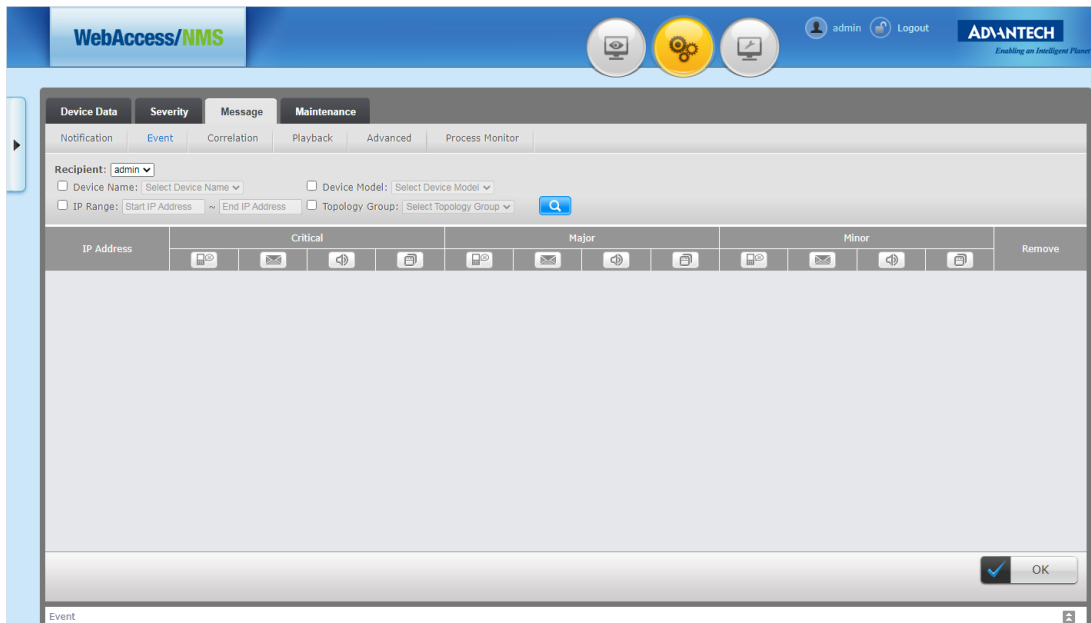
- Download allows you to download the audio file in an MP3 format.
- Playback Speed allows you to select the speed of the audio file, options: x0.5, x0.75, Normal (default), x1.25, x1.5, x1.75, x2)




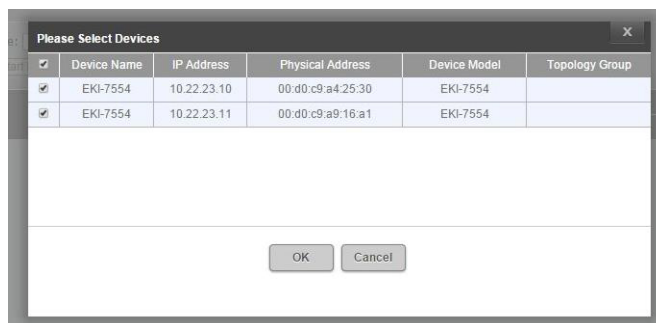
### 8.3.2.2 Event

The Event function allows you to search for devices enabling events.






1. From the tool bar menu click **Setting**.  
The Device Data page displays.
2. Click the **Message** tab and click **Event** to view the Event page.

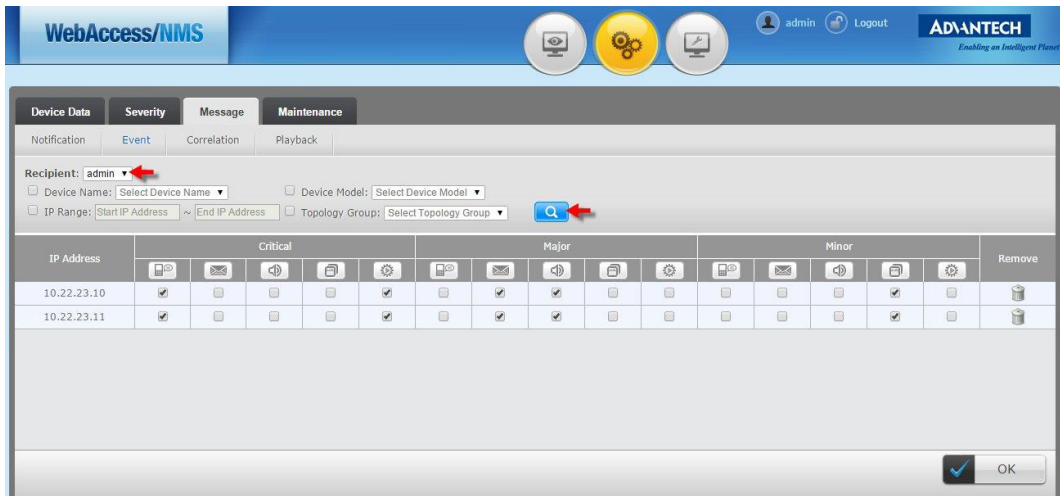


3. Click the drop-down menu to select the recipient of the event.
4. Choose Device Name, Device Model, IP Range or Topology Group
5. After selecting the required criteria, click  to search for the devices.
6. Select the device(s) from the search results to send an event notification.
7. Click OK to initiate the function or **Cancel** to return to the previous menu.



8. Select the method to initiate the event, options: SMS or E-mail, to send to the designated recipient.

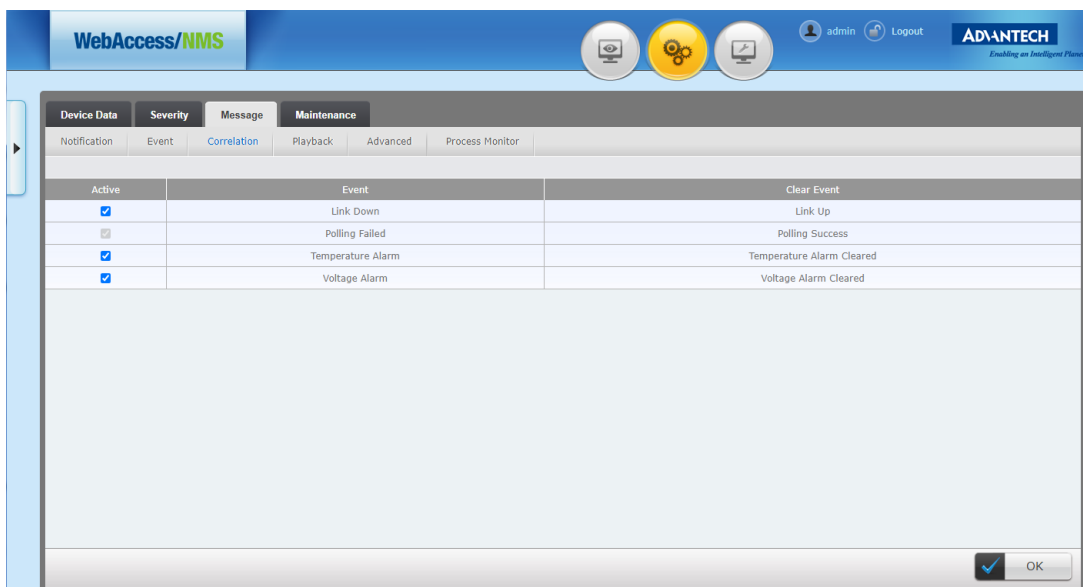
- Click      to select all or clear all check box, respectively. The event message (SMS, E-mail, Alarm Sound, or Pop-up Message) can be categorized as a different severity to be sent to the manager.



- Click **OK** to save Event setting.

### 8.3.2.3 Event Correlation

WebAccess/NMS may automatically clear unusual Event Record. In the following example, the Link Down event in the first row shows that the event is cleared and now its status is Link Up. For further details see “Event Log” on page 93.



### 8.3.2.4 Playback

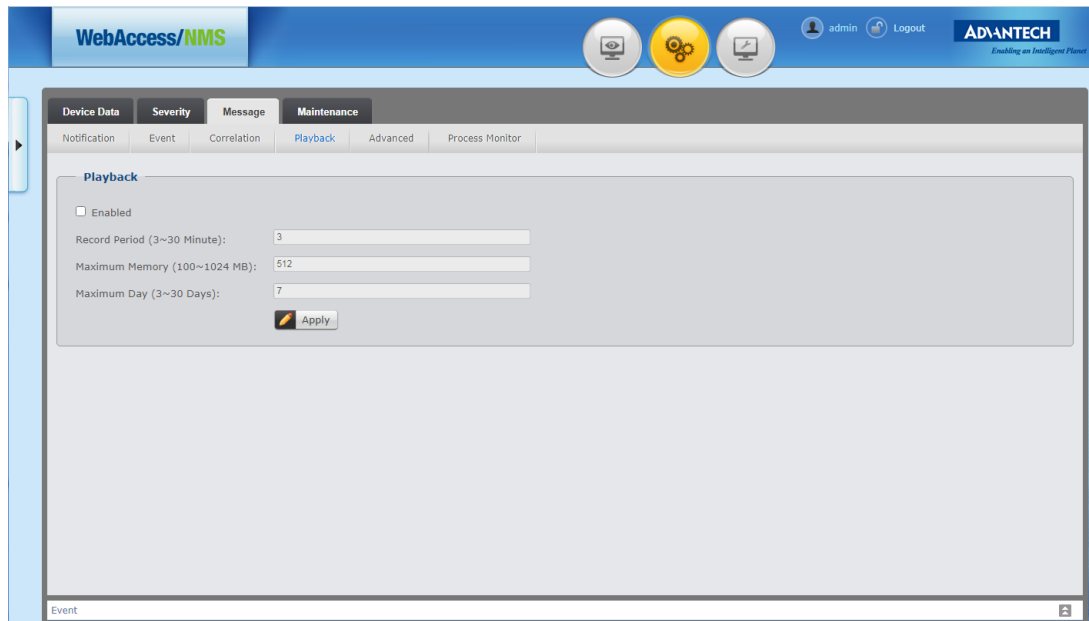
WebAccess/NMS is designed with an alarm playback function\* and can be configured based on record period, maximum memory, and maximum number of days.

\* Playback can only be used with plug-in package *Fault Management Enhancement* included of the license key.

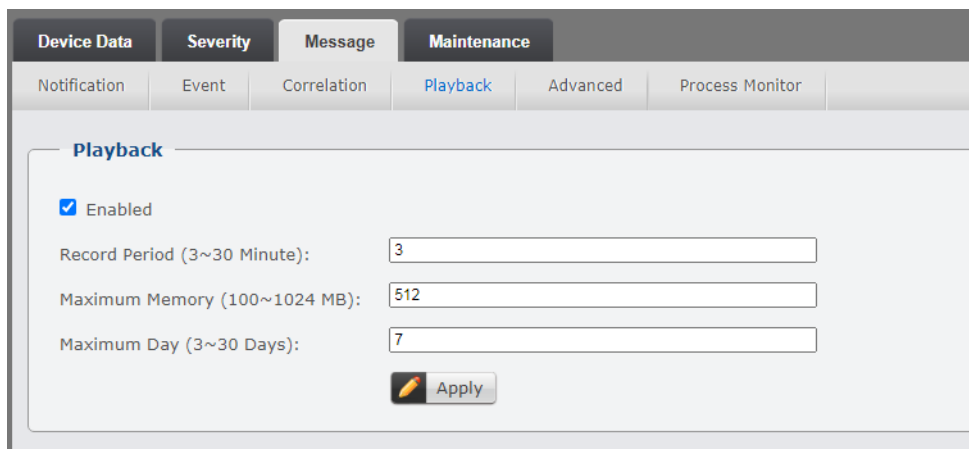
To configure playback:

- From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Message** tab and click **Playback** to view the Playback page.



3. Click **Enabled** to activate the function.
4. Enter the following information to complete the settings:
  - Record Period (3 ~ 30 minutes)
  - Maximum Memory (100 ~ 1024 MB)
  - Maximum Day (3 ~ 30 days)
5. Click **Apply** to complete setting and save the entry.



### 8.3.2.5 Throughput Monitor

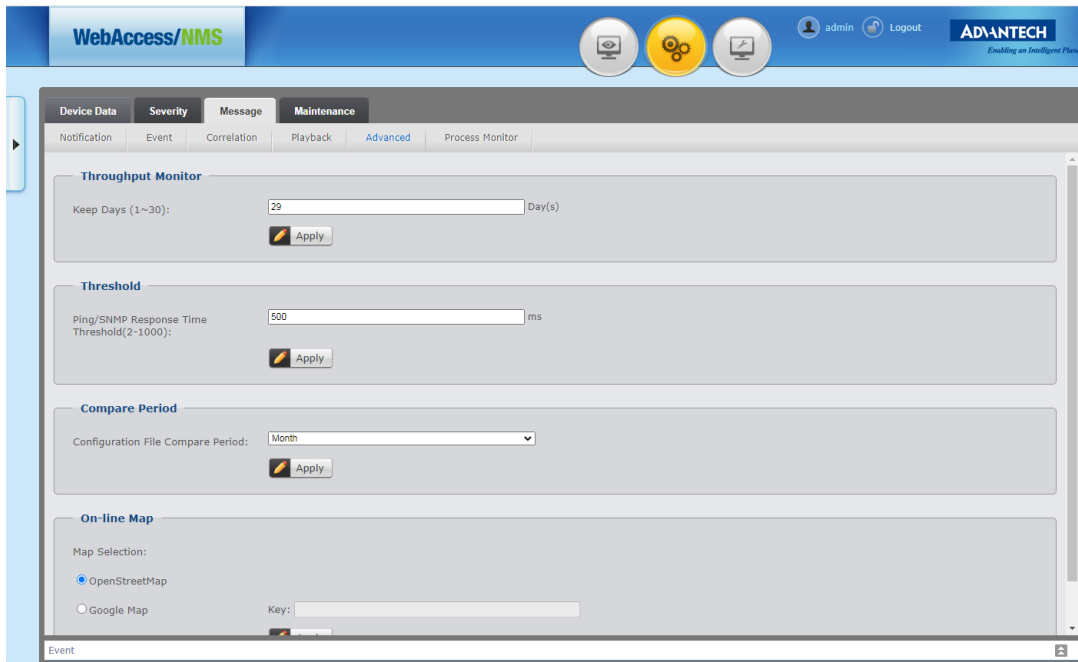
WebAccess/NMS is designed with a function to monitor the throughput between devices. The record span can be set between 1~30 days.

To configure throughput monitor:

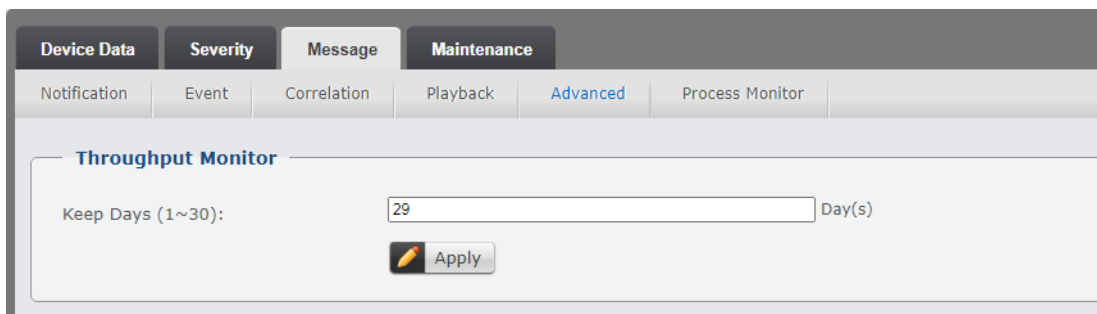
1. From the tool bar menu click **Setting**.  
The Device Data page displays.



2. Click the **Message** tab and click **Advanced** to view the Advanced page.



3. In the Throughput Monitor panel, enter the number of days to designate the period of time in days to keep the monitored record.
4. Click **Apply** to complete setting and save the entry.



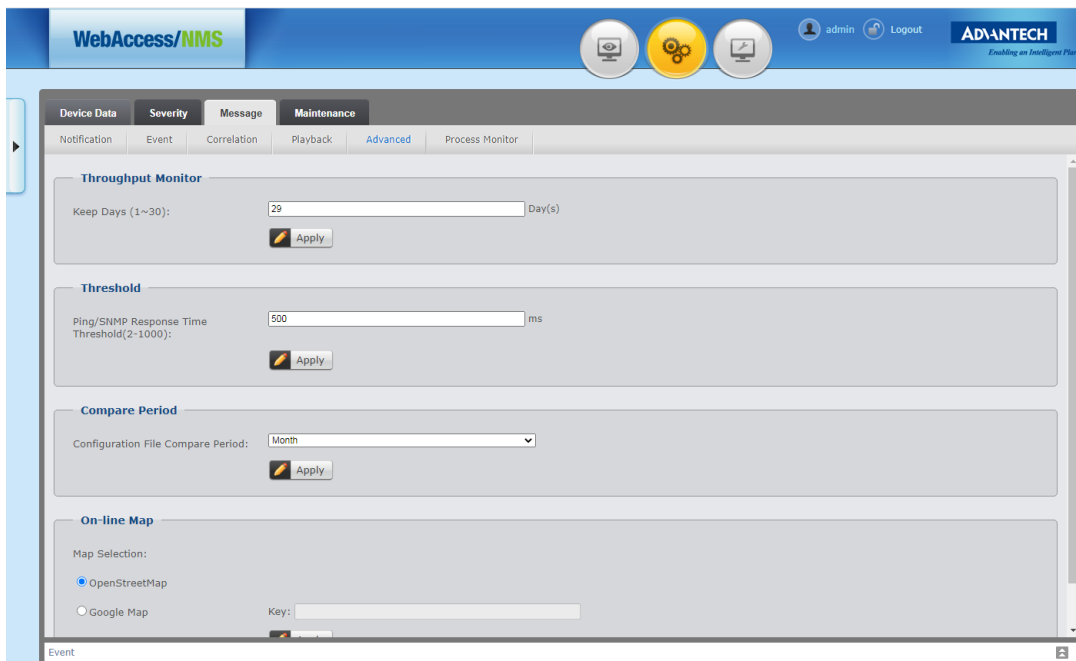
### 8.3.2.6 Threshold

WebAccess/NMS is designed with a function to monitor the threshold limits and enable a notification by setting the polling response time.

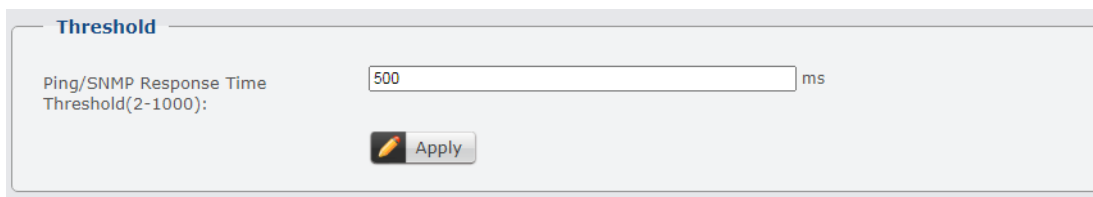
To configure threshold:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Message** tab and click **Advanced** to view the Advanced page.



3. In the Threshold panel, enter the variable to designate the polling response time in milliseconds using SNMP.
4. Click **Apply** to complete setting and save the entry.



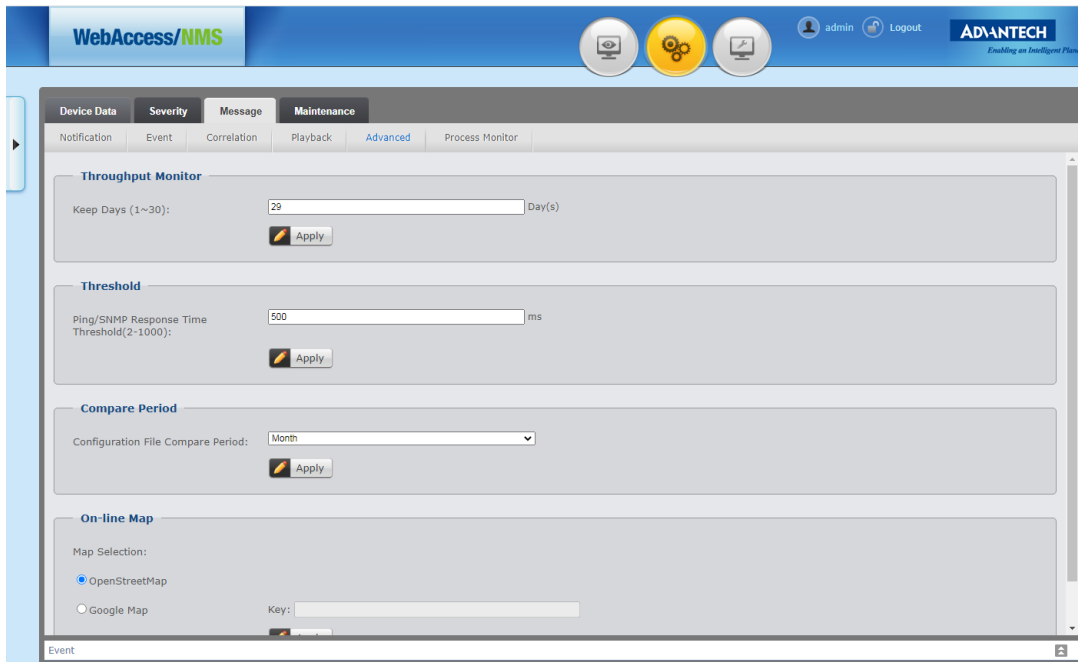
### 8.3.2.7 Compare Period

WebAccess/NMS is designed with a function automatically compare configurations, to find differences and fix network issues.

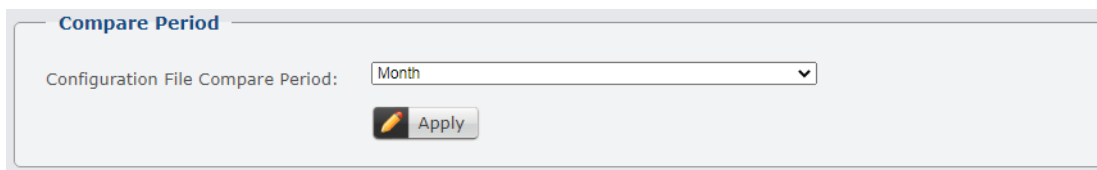
To configure compare period:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Message** tab and click **Advanced** to view the Advanced page.



3. In the Compare Period panel, click the drop-down menu to select the frequency of the compare function, option: Day, Week, Month (default).
4. Click **Apply** to complete setting and save the entry.



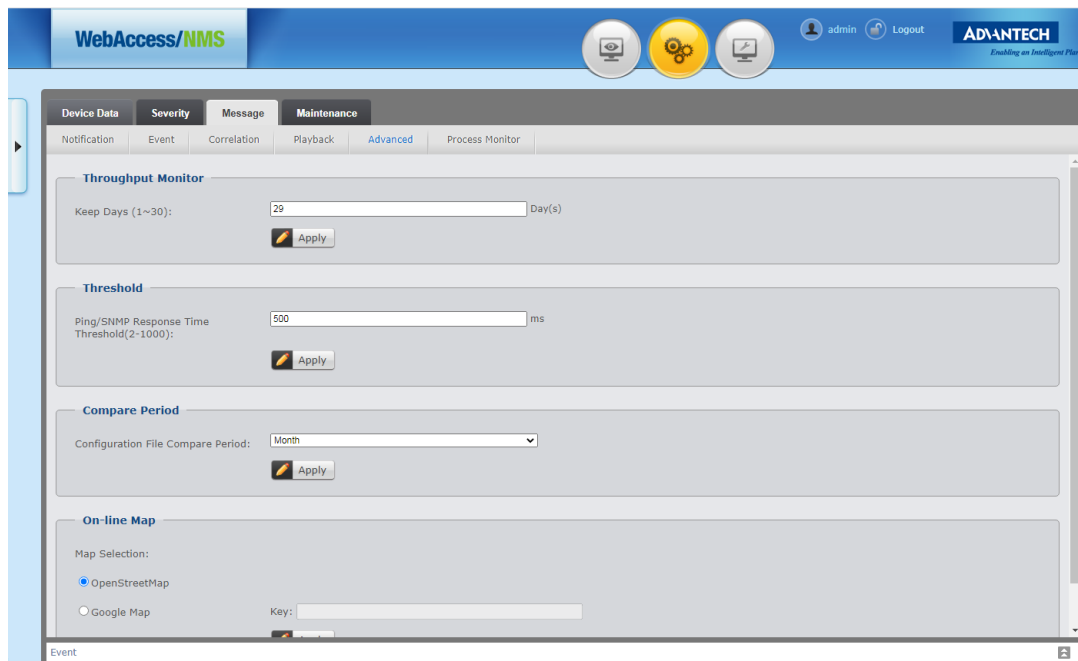
### 8.3.2.8 On-Line Map

WebAccess/NMS is designed with a function to designate the source of the on-line map display.

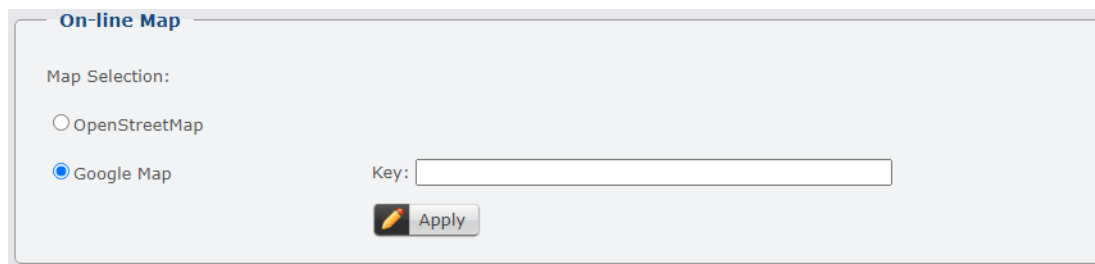
To set the on-line map reference:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Message** tab and click **Advanced** to view the Advanced page.



3. In the On-line Map panel, click to select between OpenStreetMap or Google Map.
4. If Google Map is selected, enter the authorized API key.
5. Click **Apply** to complete setting and save the entry.



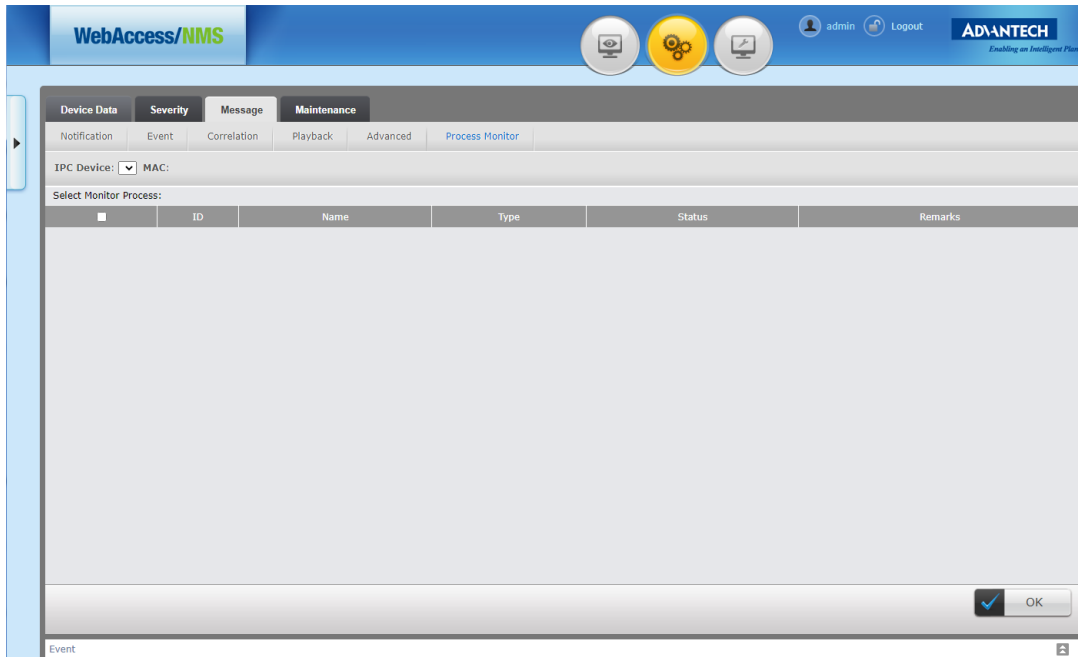
### 8.3.2.9 Process Monitor

WebAccess/NMS is designed with an advanced monitoring tool that displays real-time system activity.

To view the process monitor activity information:

1. From the tool bar menu click **Setting**.  
The Device Data page displays.

2. Click the **Message** tab and click **Process Monitor** to view the Process Monitor page.



3. Click to select an entry to view it.
4. Click **OK** to complete setting and save the entry.

## 8.4 Maintenance

### 8.4.1 Introduction for Maintenance

At the maintenance page, WebAccess/NMS has 3 functions: *Firmware Upgrade*, *Configuration Backup* and *Configuration Restore*. User may run these functions periodically or manually.

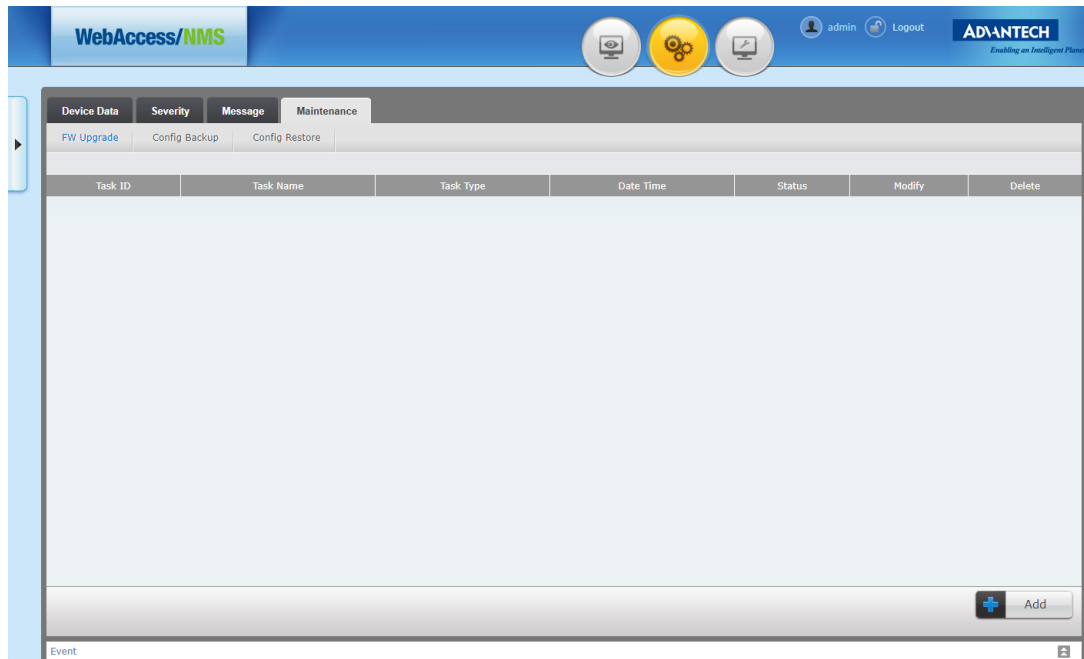
### 8.4.2 Maintenance Operational Procedures

#### 8.4.2.1 Firmware Upgrade

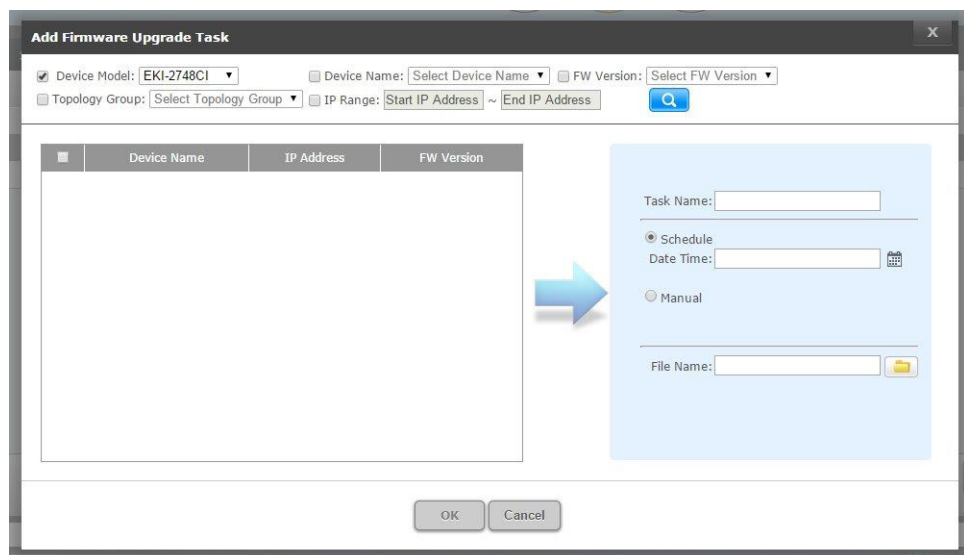
To update the firmware:


1. From the tool bar menu click **Setting**.  
The Device Data page displays.

- Click the **Maintenance** tab view the FW Upgrade page.




- Click **Add** to view the **Add Firmware Upgrade Task** page.



- Search and select the target device: User may search the device by Device Model, Device Name, FW Version, Topology Group or IP Range. Press  icon to start searching.



- Check the device to select for upgrading
- Enter Task Name.
- Select the Date Time for upgrading, options include: Schedule or manual to upgrade immediately.
- Click  icon to browse and select a specific driver file (Drivers can be downloaded on Advantech website).
- Click on **OK** to finish adding a Firmware Upgrade task.

\* The firmware upgrade files are stored on the path: C:\Program Files\Apache Software Foundation\Tomcat7.0\webapps\SCMS\DBBackup

Device Name	IP Address	FW Version
EKI-7554	10.22.23.10	v1.00 k5.03.19
EKI-7554	10.22.23.11	v1.00 k5.03.19

- After adding a new firmware upgrade task, the entry is displayed on the page as follows.
- Click or to modify or delete, respectively.

Task ID	Task Name	Task Type	Date Time	Status	Modify	Del
1	f	Manual	2014/10/24,11:53	Result		

- To view the result status, click **Result** to view the upgrade information. There are three status conditions: Success, Failure and Pending.

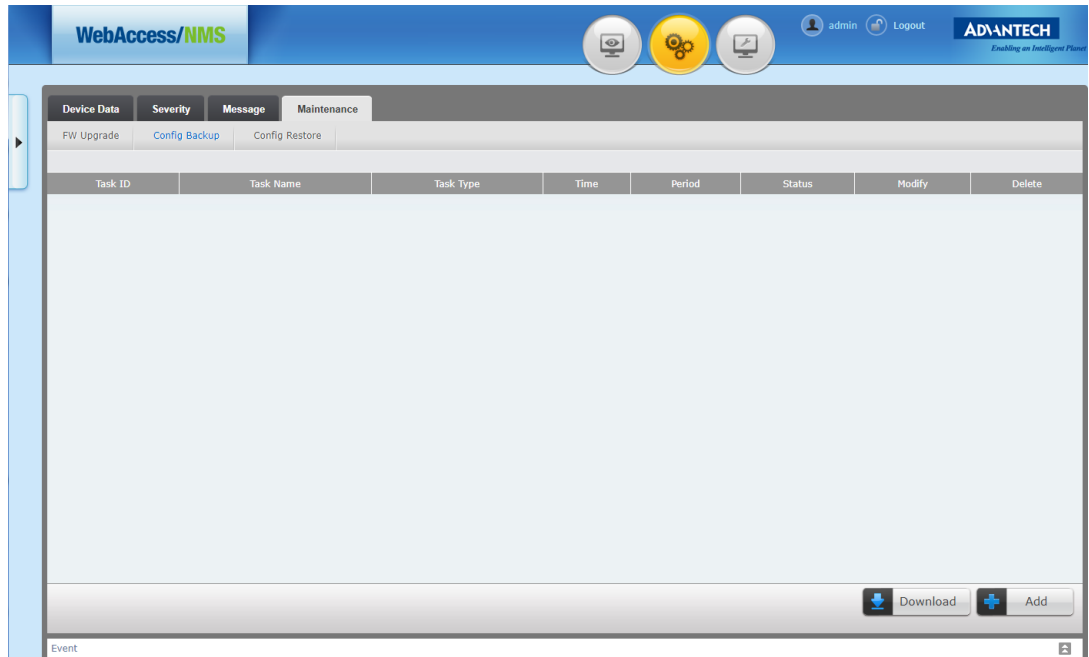
Device Name	IP Address	Status	Time
EKI-7659C	10.22.23.25	Pending	
EKI-7659C	10.22.23.26	Pending	

### 8.4.2.2 Configuration Backup

To backup the configuration:


- From the tool bar menu click **Setting**.  
The Device Data page displays.

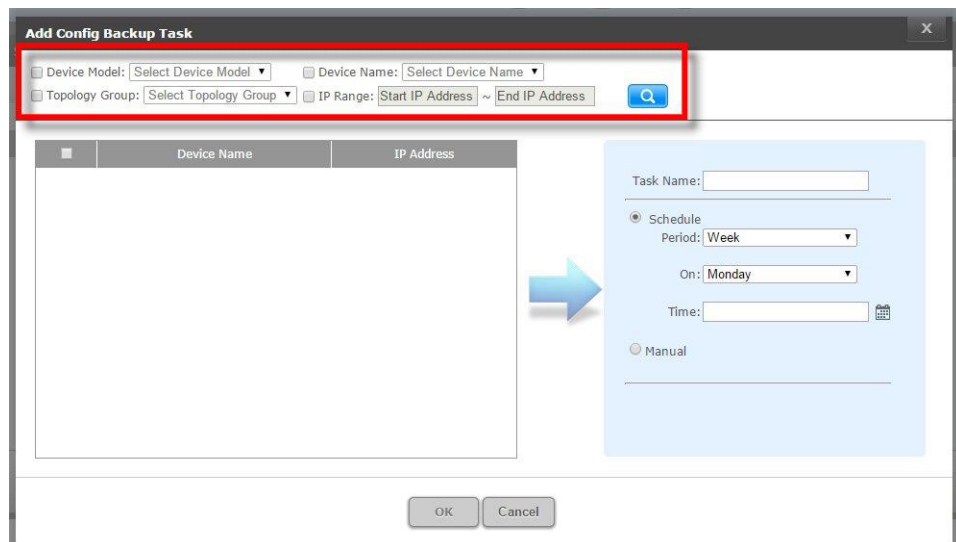
- Click the **Maintenance** tab and select Config Backup to view the Config Backup page.



There are two functions available for the maintenance of the system configuration, Download and Add.

To add a configuration backup event:



- Click **Add** on the bottom-right corner of the page to view the Add Config Backup Task window.
- Search and select the target device(s): User may search the device by Device Model, Device Name, Topology Group or IP Range. Press  icon to start searching.



- Check the device to select it for backup.
- Enter the Task Name.
- Select the Time Period for upgrading, options include: Schedule or manual to upgrade immediately.
- Click on **OK** to finish adding a Configuration Backup task.




\*The task name is limited to characters from the English alphabet, excluding special symbols.

9. After adding a new configuration backup task, the entry is listed in the page.
10. Click  or  to modify or delete, respectively.

Task ID	Task Name	Task Type	Time	Period	Status	Modify	Delete
2	f	Manual	2014/10/27,17:00	-	Result		
3	10.22.23.10	Manual	2014/10/27,17:10	-	Result		
4	10.22.23.11	Manual	2014/10/27,17:12	-	Result		
5	10.22.23.13	Manual	2014/10/27,17:15	-	Result		

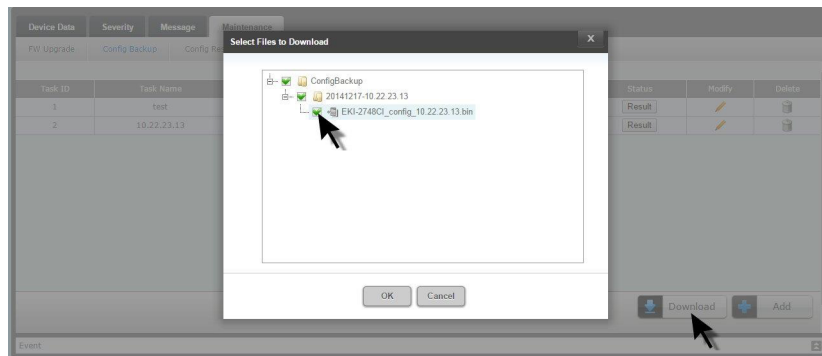
11. Click **Result** to see the status of configuration backup. There are three status conditions: Success, Failure and Pending.

12. If the status displays success, click the icon  to simultaneously save the result in the administrator's computer and enterprise server.

To download a configuration file:

13. From the Config Backup page, click  **Download** to view the Select Files to Download page.

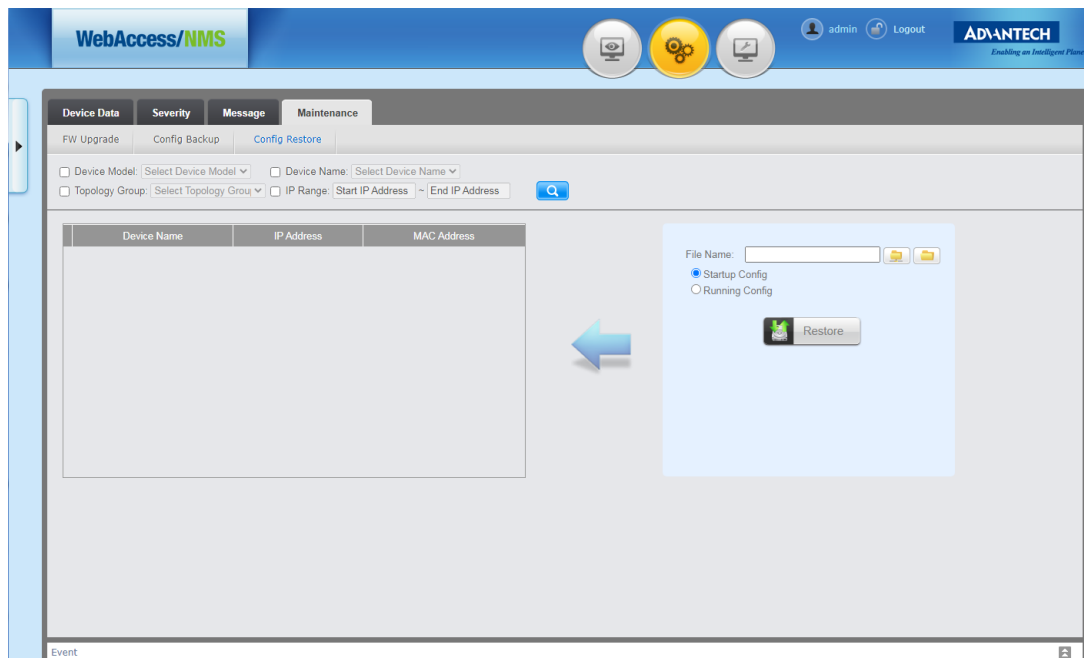
- Browse to select the backup file then click **OK** to download.




### 8.4.2.3 Configuration Restore

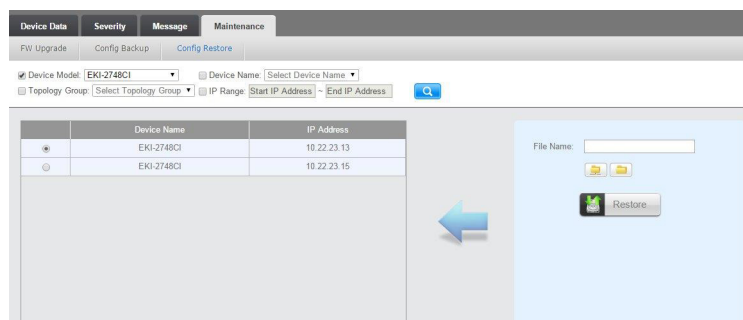
To restore configuration settings:



- From the tool bar menu click **Setting**.  
The Device Data page displays.
- Click the **Maintenance** tab and select Config Restore to view the Config Restore page.

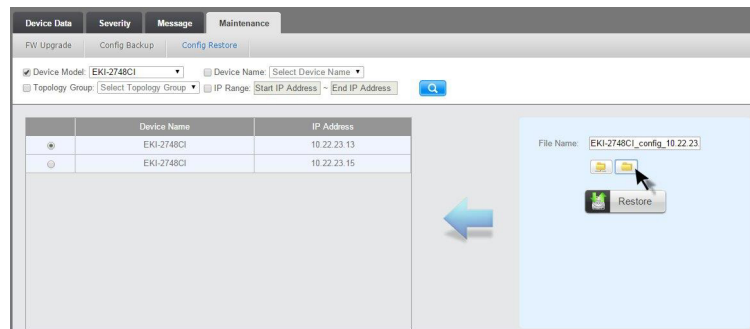
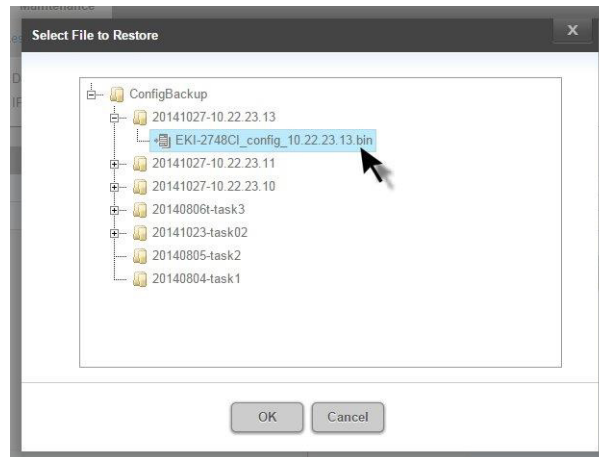


A configuration backup should be done first (refer to “Configuration Backup” on page 57) before proceeding with a firmware configuration restore.

- Select a target device(s). You can select Device Model, Device Name, Topology Group or IP Range to specify the device(2).
- Click  to search for the specified device(s).



5. Click  or  icon for browsing related configuration backup files from server or local devices, respectively. Then click **OK** to proceed.
6. Click **Restore** to start configuration restore. For example, restoring device EKI-2748 should choose the corresponding backup file:  
*EKI-2748CI\_config\_10.22.23.13.bin*.



7. If an incorrect backup file is selected, an error message displays.

# Chapter 9

WebAccess / NMS  
Monitoring Interface

The Monitoring menu page for WebAccess/NMS provides access to Device List and Device Properties, Topology View, Dashboard, Performance, Event Log, Syslog and Report functions. The device information, device deployment, connection status, efficiency of memory and CPU can be shown on this page. The device polling record and warning message can be stored.

## 9.1 Topology

### 9.1.1 Introduction for Topology

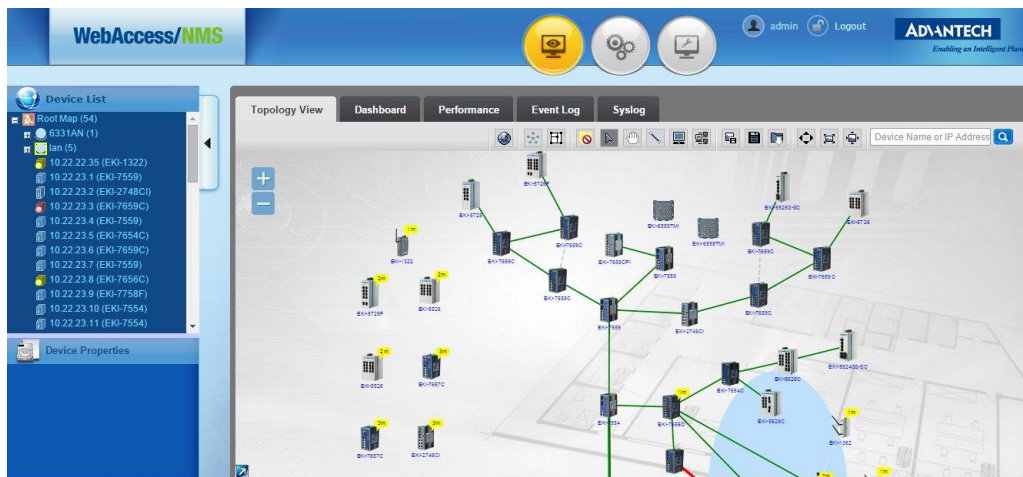
The topology of WebAccess/NMS composes of wired/wireless devices shown by different line and icons. The colors of line indicate different severity. WebAccess/NMS is able to generate topology only with selected devices and the devices can be shown on its locations of Map.

### 9.1.2 Topology Functions

#### 9.1.2.1 Topology View

To access the topology view:

1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.







The available menus for the Monitoring function are displayed.

#### 9.1.2.2 Topology Icons

The Topology icons are listed as follows:



Icon	Item	Icon	Item
	Device Discovery		Add to Topology Group
	Topology View		VLAN Setting

Icon	Item	Icon	Item
	Map		Export to Image
	VLAN Mode		Save Topology
	VCOM Mode		Load Topology
	USDG Mode		Full Screen
	Background Image		Zoom Reset
	Show / Hide Minor Alarm		Zoom Overview
	All Traffic Monitor		
	Select		
	Move		
	Create Link		
	Create Device		


### 9.1.2.3 Device Discovery

- From the tool bar menu click **Monitoring** to view the options. The Topology View page displays.



- From the panel tool bar, click **Device Discovery** : This function can be used to show the devices with selected IP range.



3. Click  icon, a Device Discovery window will pop-out.
4. Enter the following information to complete the configuration:
  - EMS Group
  - Start/End IP Address
  - Protocol (select ICMP+SNMP)
  - Read Community (select public)
  - Write Community (select private)

By default Trap Configuration is enabled. It allows the system to connect with the devices and setup parameters for receiving trap logs automatically.

The following figure displays an example of the settings:

IP range is entered as 10.22.24.1~10.22.24.50.

5. Click **OK** to start the search event.


The status of the device discovery process in percentage displays on the tool bar, see the following figure.

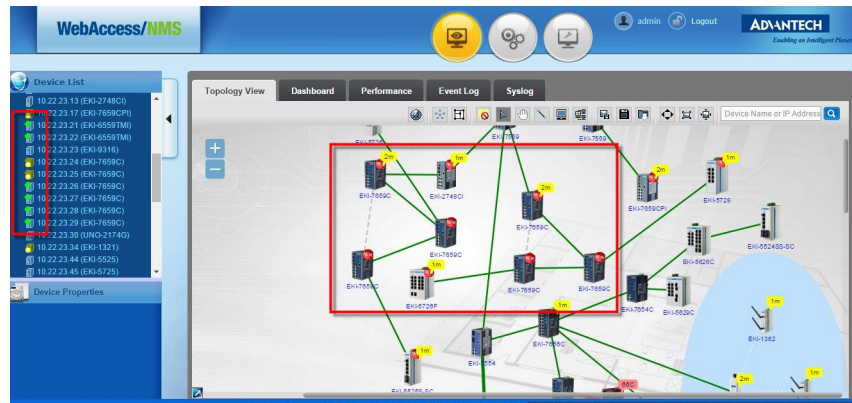



After Discovery is completed, a popup window displays the results. There are 7 categories: Success, Trap server is full, LLDP is disabled, SNMP set failed, Syslog server is full, Trap server set failed and Syslog server set failed.

Discovery Result		
IP Address	Device Model	Result
192.168.1.155	EKI-5728	LLDP is Disabled SNMP set failed Trap server set failed
192.168.1.166	PingableDevice	Success

6. Click **OK**. The devices with the IP range entered previously can be added on the system.

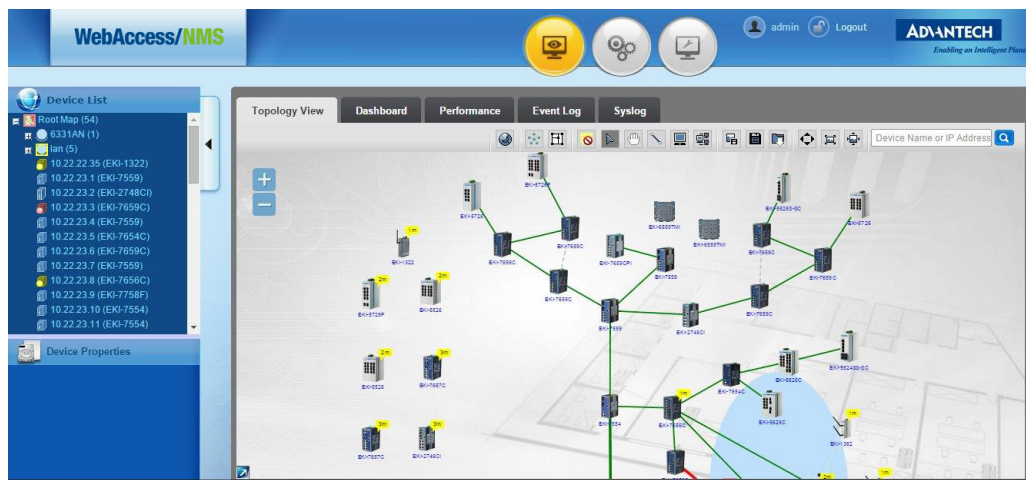
The new discovered devices will have an indicator  on the device icon and green + icon on the Device List (the indicators are disabled after the page is reloaded).





**Note!**  Device Discovery correlates to Setting function. For example, there are 10 devices for the topology discovery, the Managed Device, FW Upgrade, Config Backup and Config Restore will only search for these 10 devices. If users want to search or set for other devices, the devices should be re-discovered.

#### 9.1.2.4 Topology View

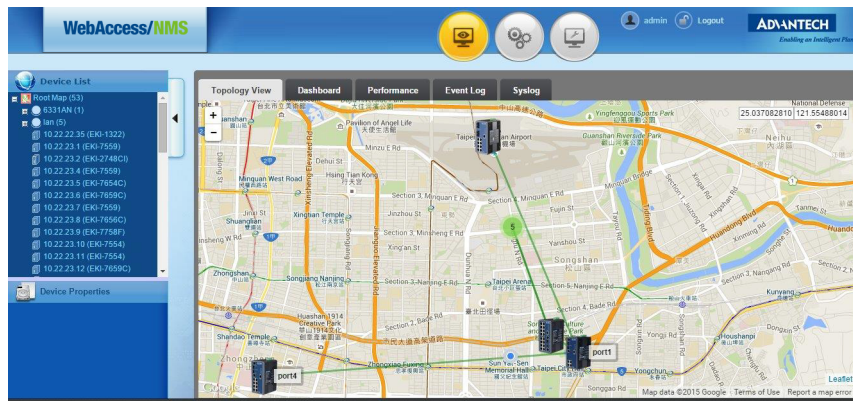
1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.



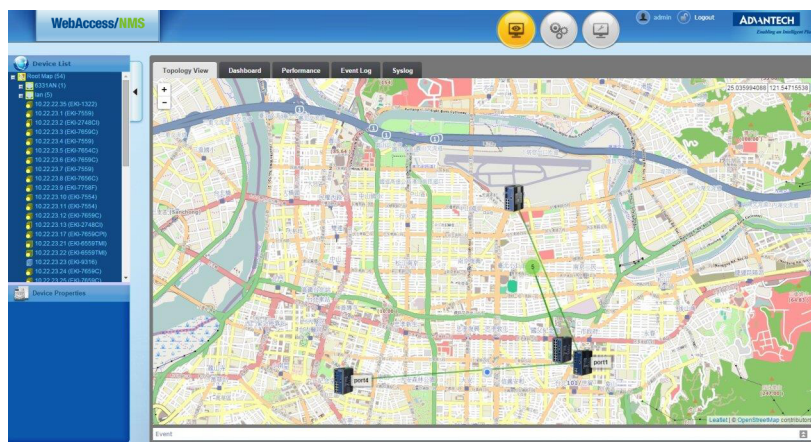
2. From the panel tool bar, click Topology View  to access VLAN, IGMP, VCOM and USDG mode to Topology View.
3. Click Map  to view the location of Topology Group and Devices, linkage of devices can be shown on the Map. The map can be scaled with different size. The number of device in a topology group would be shown with smaller scale map. The Latitude and Longitude should be set for the device to correspond to the map location.





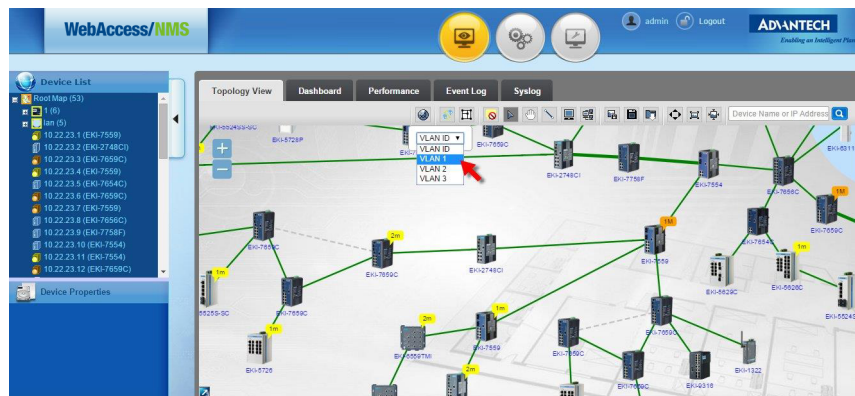
The map displays once connected to the map application such as Google Maps.



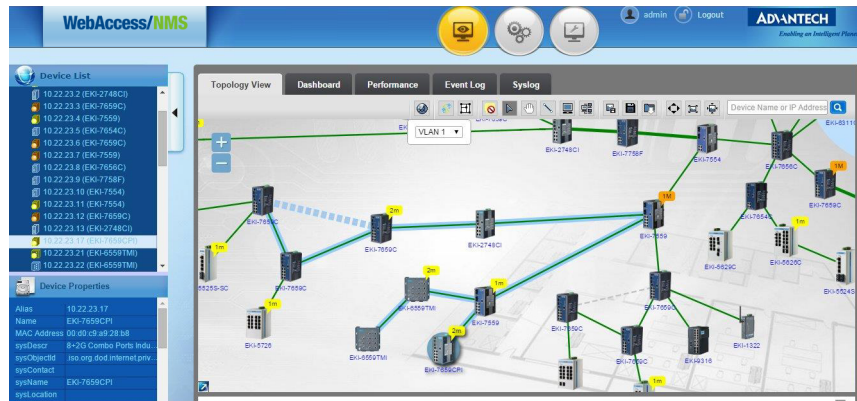
If the system does not have access to the Internet, users can purchase the Offline Map plug-in package from Advantech.




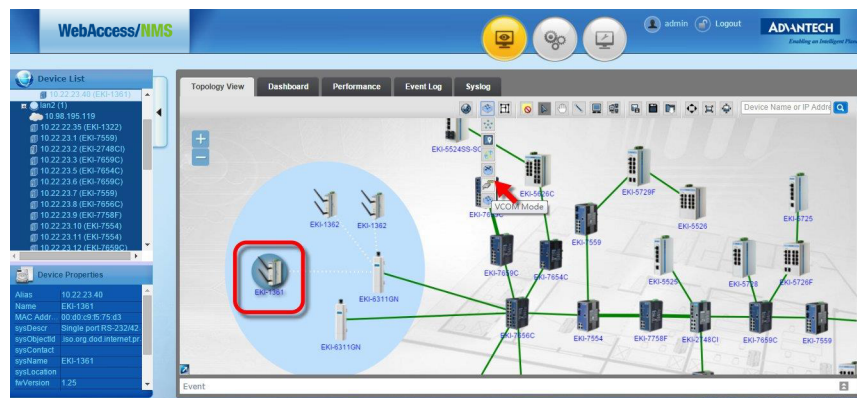
4. Click Map VLAN Mode  to view the VLAN topology map.
5. Click  the pre-set VLAN modes can be shown on the pull-down menu.



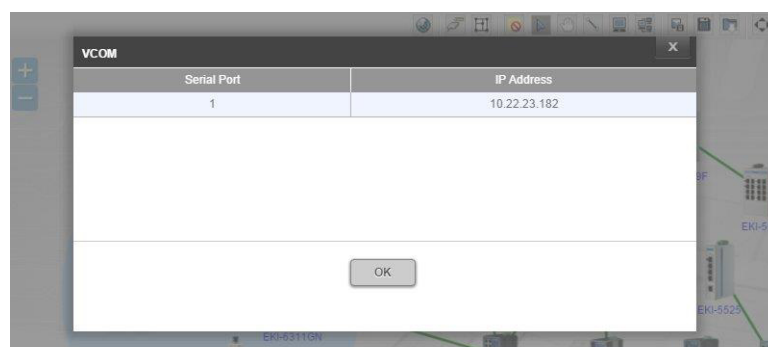
After choosing the mode, the logical deployment of the chosen VLAN can be shown in blue line.




6. Click VCOM Mode  to refer to the devices supporting VCOM and the overview of the data transmission. Advantech device server such as EKI-1361 and EKI-1321 can transfer an RS-232 signal to Ethernet signal to connect to the devices that are not connected through the NMS system.
7. Click on VCOM and select the VCOM supported devices such as EKI-1361.

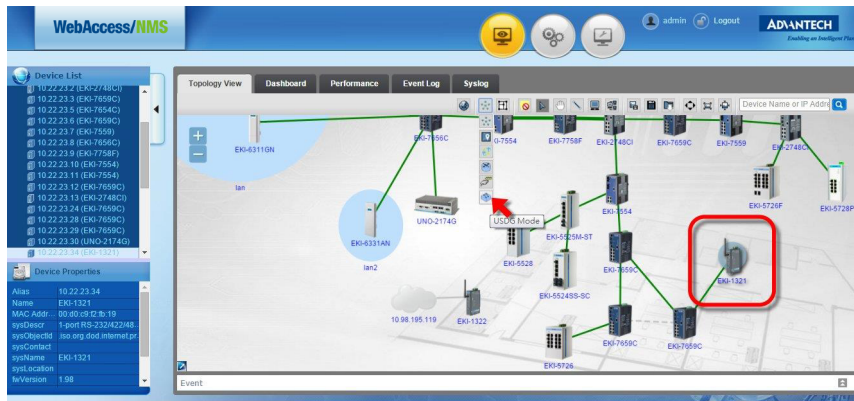


The pop-up window displays the Serial Port and IP Address of the selected device. The following figure displays EKI-1361 is transmitting data on port 1 with the IP 10.22.22.182.

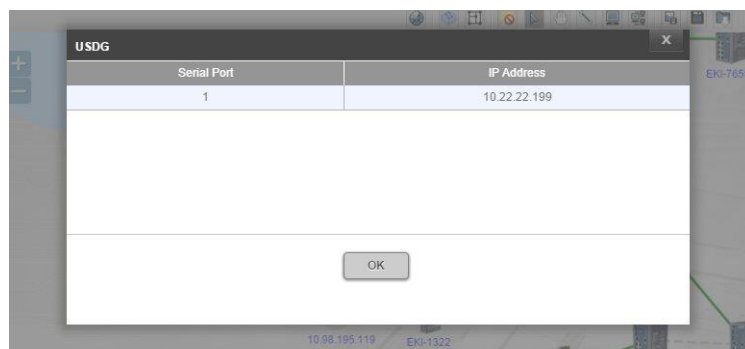


8. Click USDG Mode  to view devices supporting USDG and the overview of the data transmission. Advantech device server such as EKI-1321 and EKI-1322 can transfer the RS-232 signal to wireless WiFi signal to connect to the devices that are not connected to the NMS system.

- Click USDG to select the USDG supported devices such as the EKI-1321.

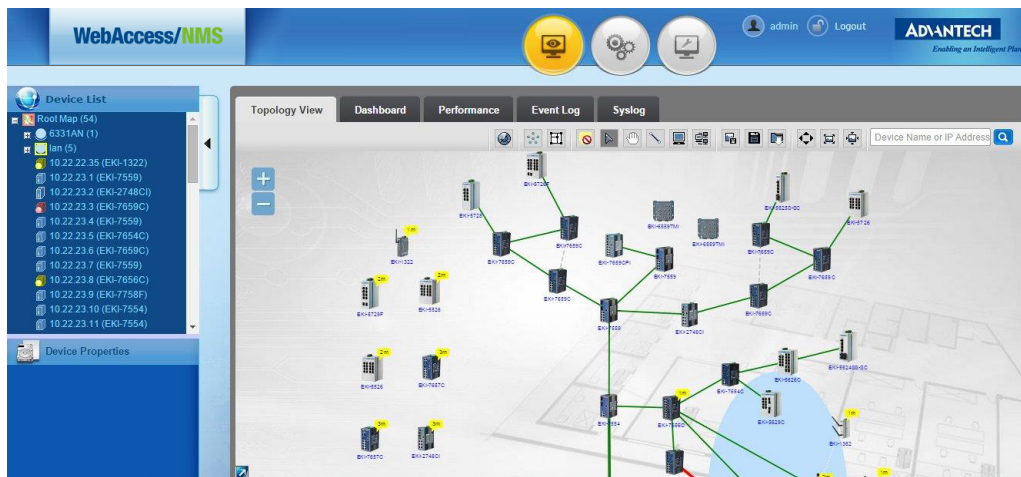



The pop-up window displays the Serial Port and IP Address of the selected device. Take the following picture displays that the EKI-1361 is transmitting data on port 1 with IP 10.22.22.199.



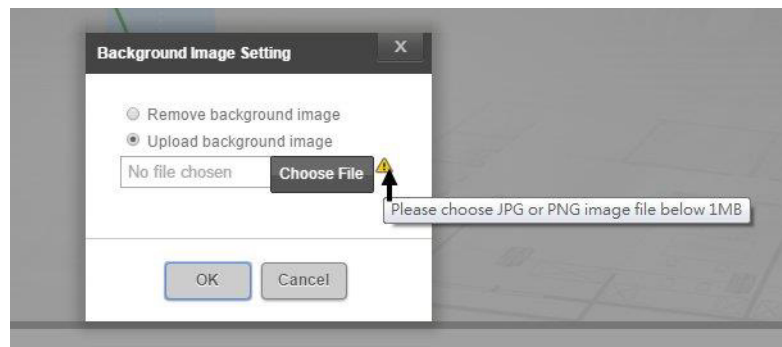
### 9.1.2.5 Background Image

- From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.



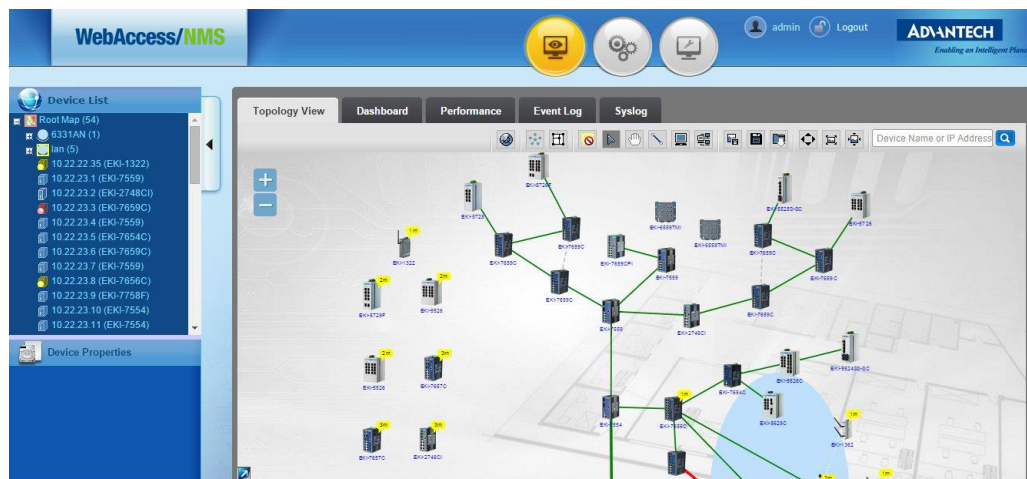
- Click Background Image  to view the background of the topology. A window pops up while to change the setting.

- Click Select File to choose image then click **OK** to upload. Only PNG and JPEG image formats under 1MB are supported. File names only support English alphabet characters.

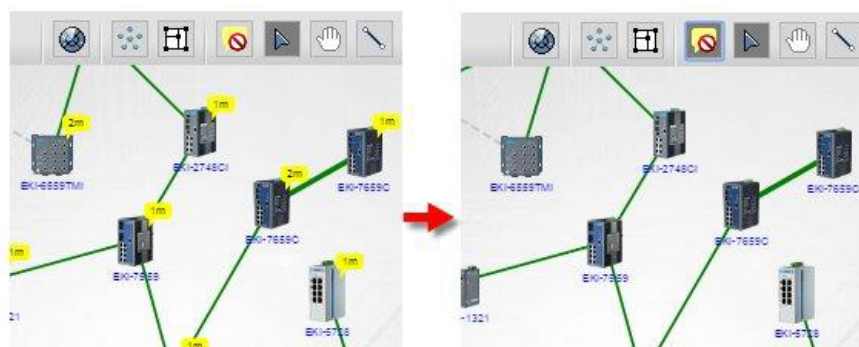


### 9.1.2.6 Show / Hide Minor Alarm

- From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.



- Click Show/Hide Minor Alarm  to view the show/hide on topology. Click on the icon then click on the device displaying minor alarm status, after which the yellow notification disappears.




### 9.1.2.7 All Traffic Monitor


- From the tool bar menu click **Monitoring**  to view the options.

The Topology View page displays.




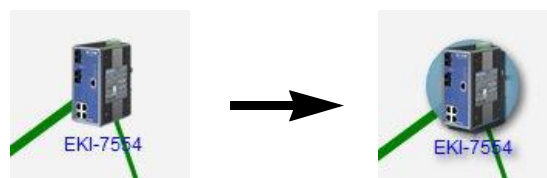
2. Show/Hide Minor Alarm : Minor Alarm can be chosen to show/hide on topology by this function.
3. Click on this icon then click on the device with minor alarm, the yellow symbol will disappear.

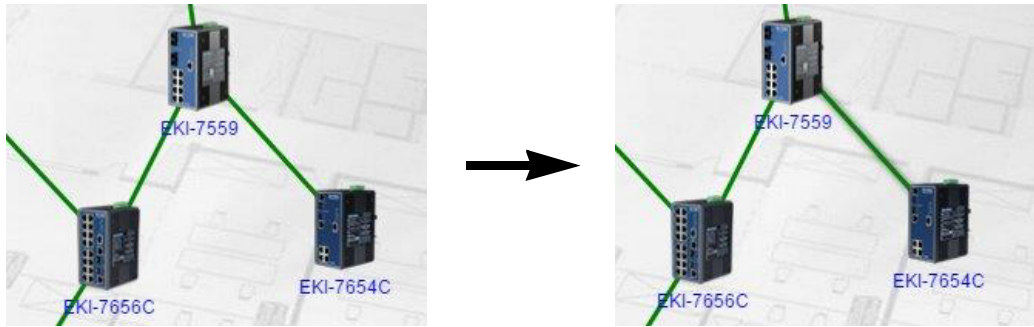
### 9.1.2.8 Select

1. From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.

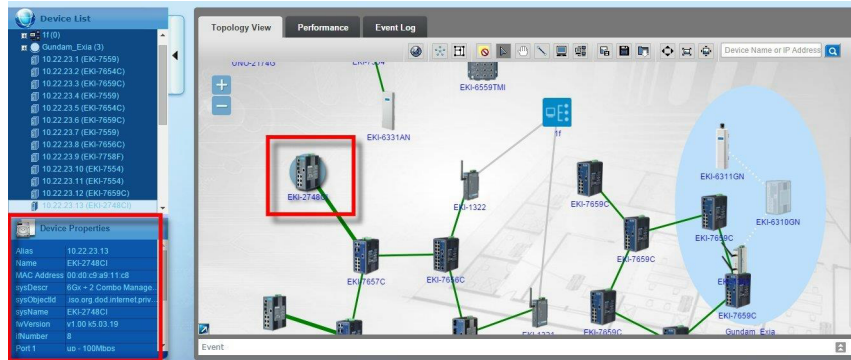


2. Click Select  to view This function is set with default while enter the Topology View. Keep left click the mouse to select/drag device and link to the desired position. A shadow will appear while successfully choosing a device or link.

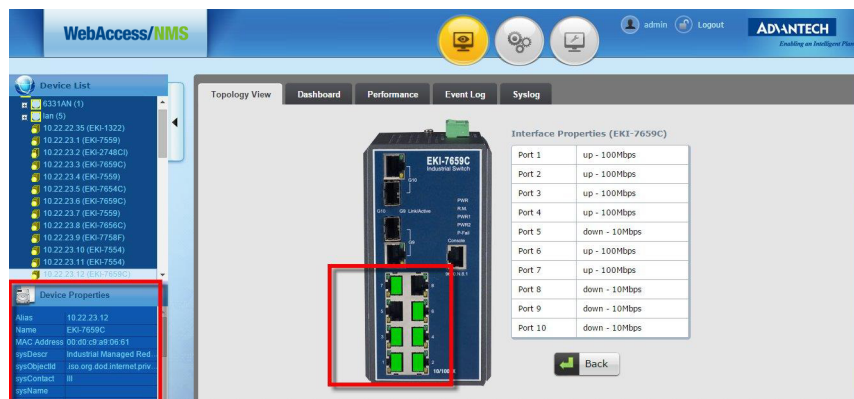




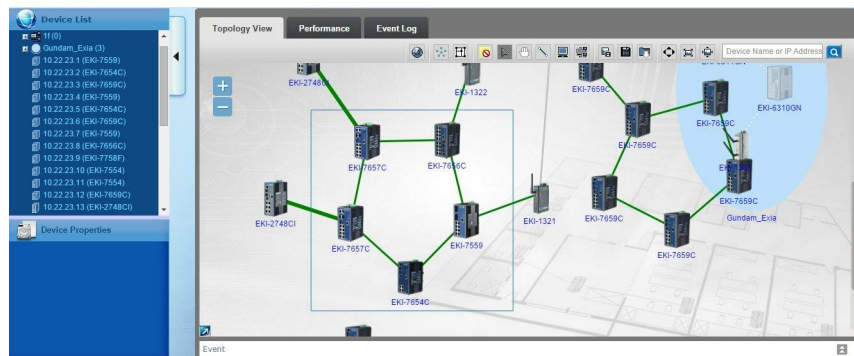
3. Left-click the mouse on the selected device to view the Device List and Device Properties.



4. Double click on the device to view the Interface Properties menu. A green status indicator means the port is connected.
5. Click **Back** to Topology View.

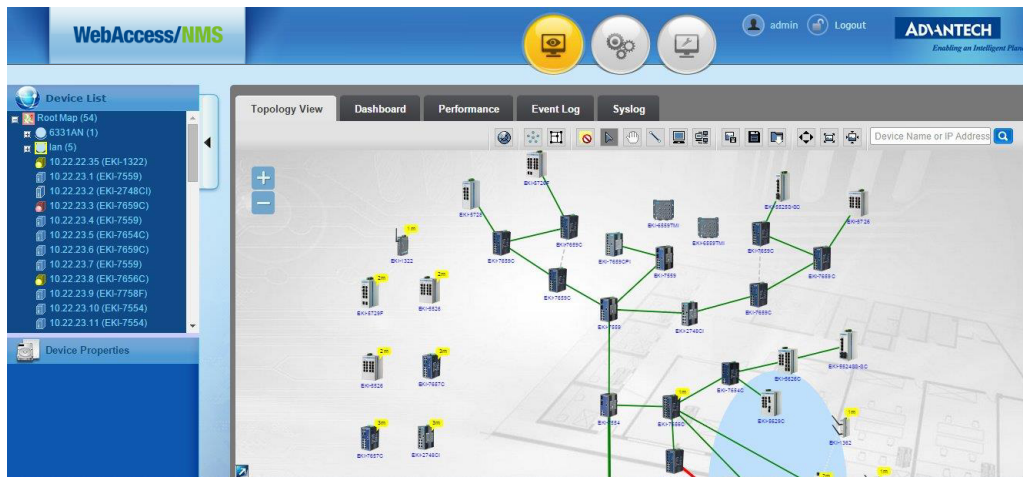





Multiple devices and links can be chosen by holding down the Ctrl key while selecting with the left mouse key.



### 9.1.2.9 Move Topologies

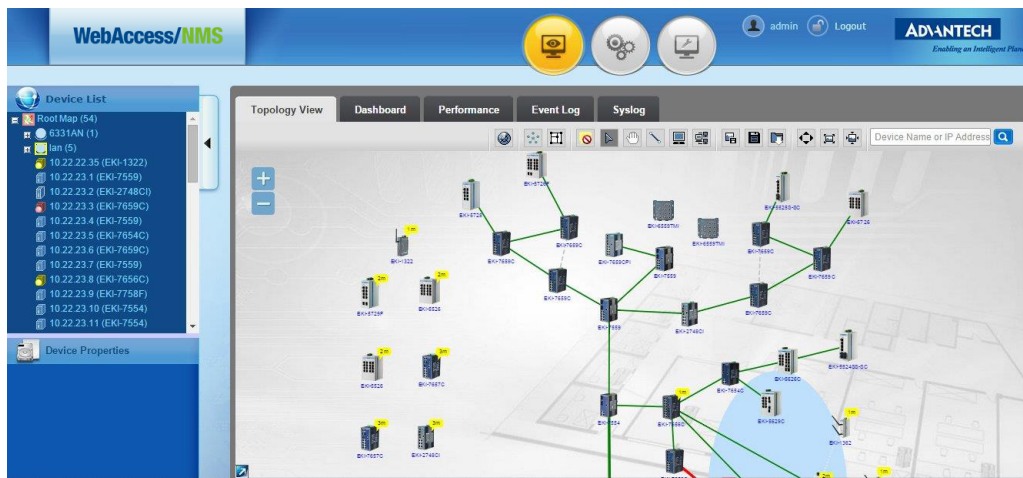
1. From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.






2. Click the Select  drop-down menu to view the move  icon.
3. Click Move  to drag a topology.

### 9.1.2.10 Create a Topology Link

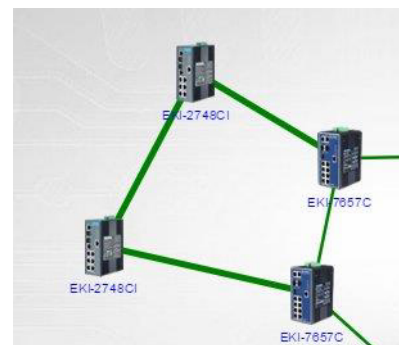
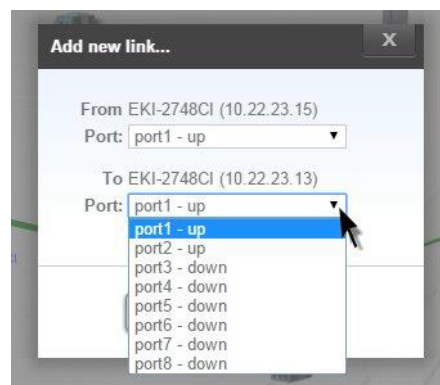
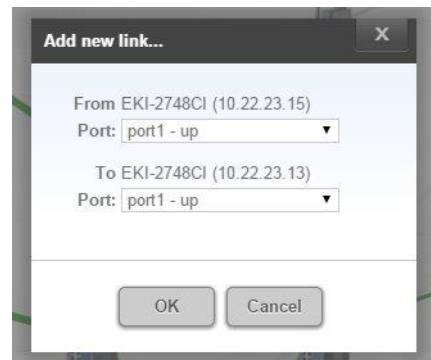
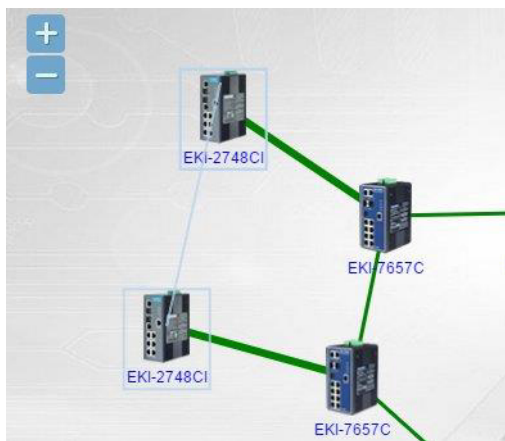
1. From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.



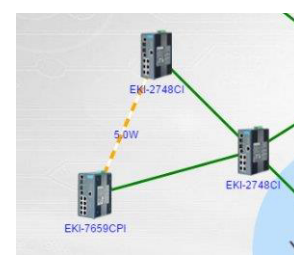
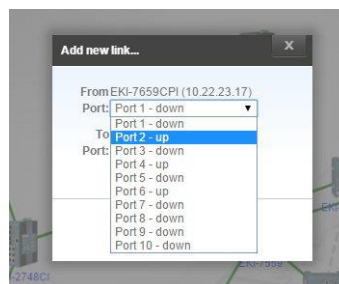
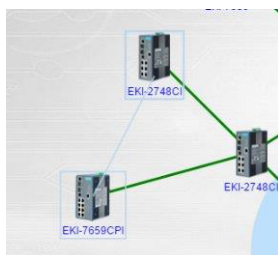
2. Click the Select  drop-down menu to view the link  icon.
3. Left-click on device A to select it.
4. Drag cursor to device B and left-click over the device B to establish the pathway.
5. Press **OK** on the pop-out window to create the link.

If user wants to remove the link, click icon  first to select the link, then press **Delete**.

\* If there is no link between real devices, topology displays a corrected correct status after the rediscover process of the devices.



\* The link between the device with power supply and normal device can be drawn manually (Automatic link creation is not supported at this time). For example, port 2 of EKI-7659CPI can supply power a link displaying the voltage can be created to state it.






### 9.1.2.11 Create a Device


1. From the tool bar menu click **Monitoring**    to view the options.

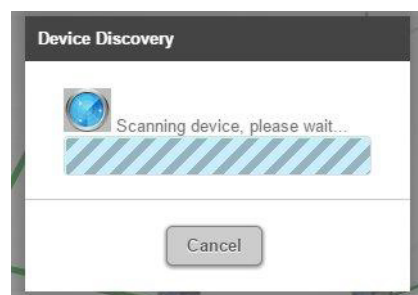


The Topology View page displays.



2. Click the Select  drop-down menu to view the Create Device  icon.
3. Click on the  icon.
4. Click on the Topology map to view the Add new device... window.
5. Click on the EMS Group drop-down menu to select the corresponding group for the device.
6. Enter the required information as follows:  
Device name, IP Address, Read Community, Write Community, Topology Group, Location, Latitude, Longitude, Trap Configuration, and Syslog Configuration.
7. Click **OK** to create a new device.

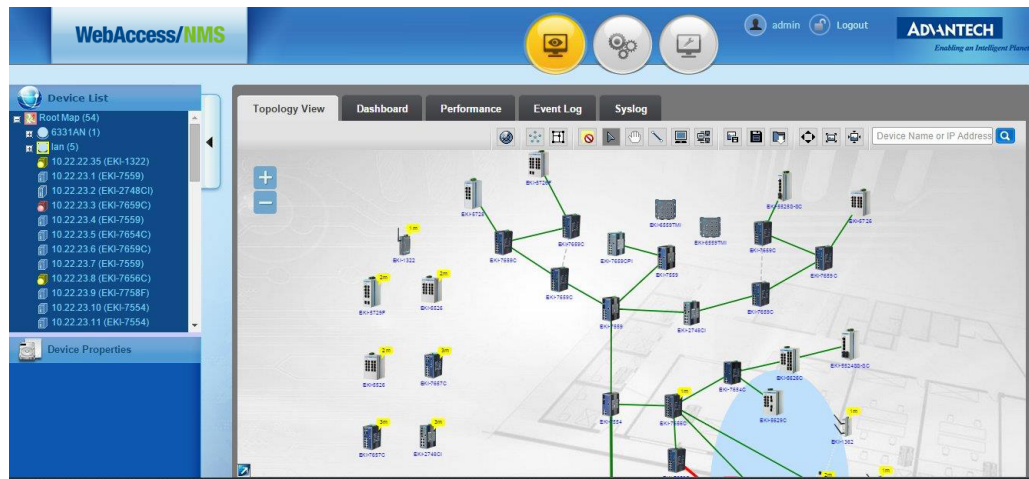
\* If user wants to remove the device, click icon  first to select the device, then press **Delete**.




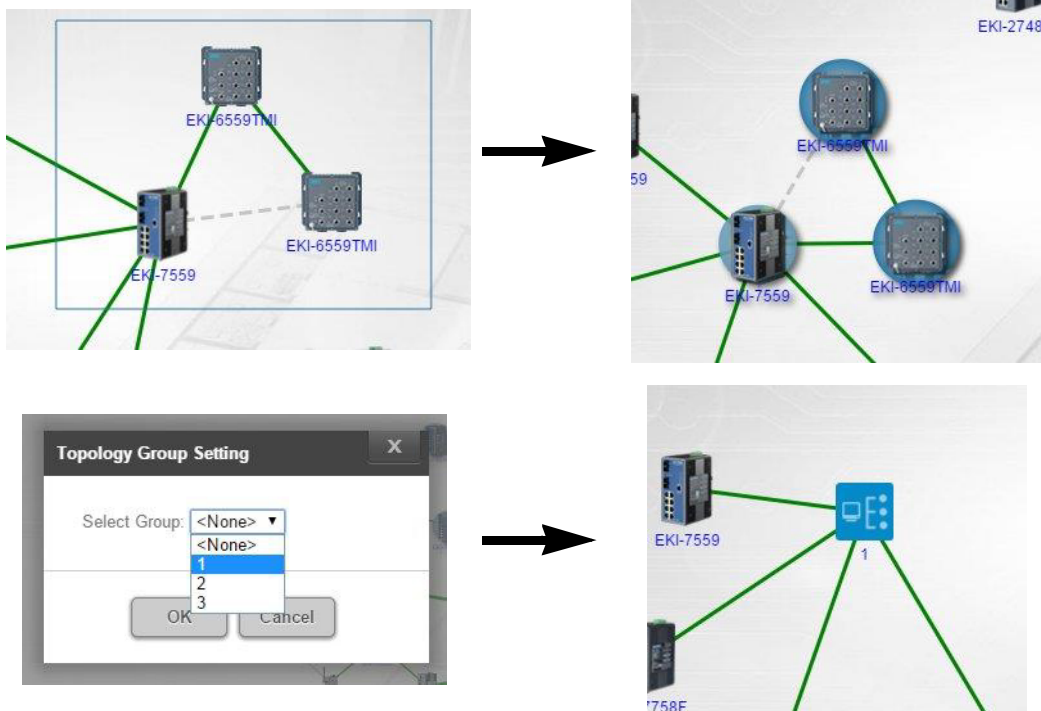
### 9.1.2.12 Add to a Topology Group

1. From the tool bar menu click **Monitoring**    to view the options.

The Topology View page displays.



2. From the Topology View window, select a device(s).
  3. Click the Add to Topology Group  icon to display the to view Topology Group Setting window.
  4. Click the Select Group drop-down menu to select the target group.
  5. Select the group then press **OK**.
- \* Group setting can be referred to “Topology Group” on page 33.




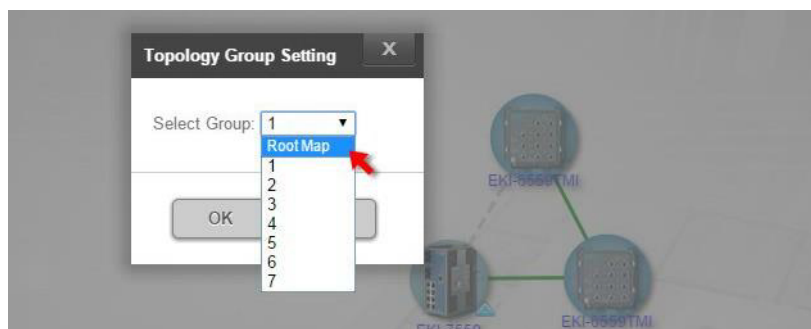
Topology groups will be shown on the Device List. Double click the group name then user may check the devices and link of this group. A blue triangular icon

next to the device indicates that this device is the Root of the whole group, and other devices are designated the Sub Tree.



To remove a device from the group”

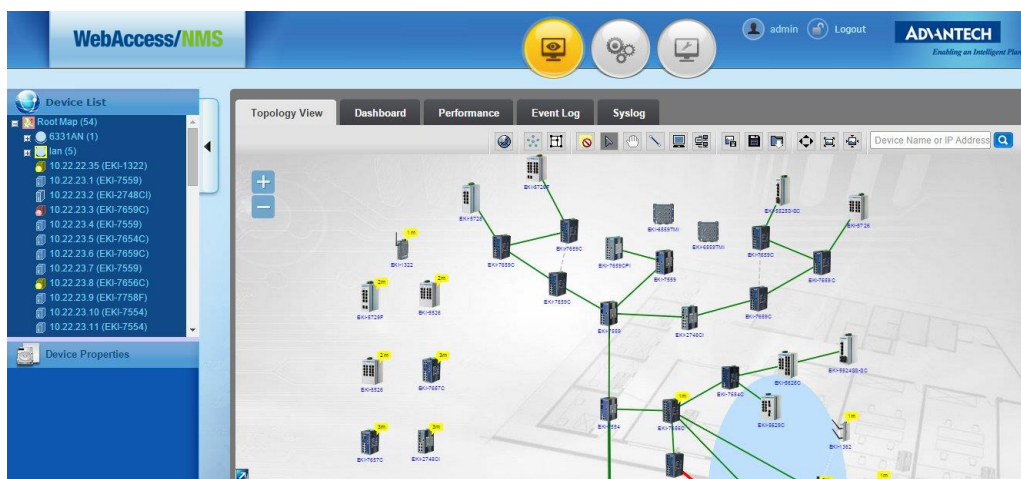
6. Double click the group icon, select device to remove then click .
7. From the drop-down menu select None. The the device is removed from the group.




### 9.1.2.13 Export Topology Map to Image

The Export to Image function allows you to export a topology map as PNG formatted file.

1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.



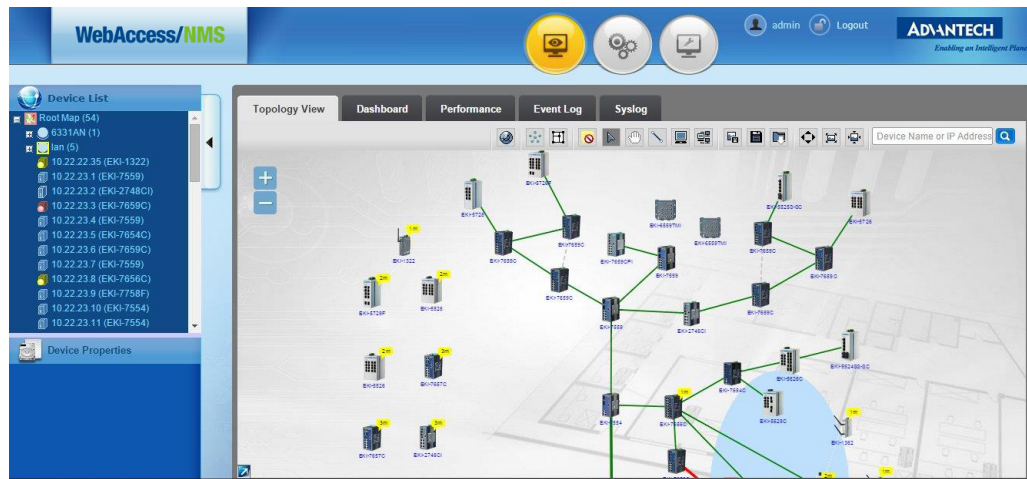
2. Click the Export to Image . A new window in the default browser open displaying the captured topology map.



### 9.1.2.14 Save Topology Map

The Save Topology function allows you to save a topology map to the local system default download folder\*.

\* Topology is saved by default on the server: C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\WEB-INF\topoFile

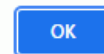
1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.



2. Click the Save Topology  icon to save the topology view. A  Save Successfully window displays when the save is successful.
3. Click **OK** to complete the process.

127.10.10.10 says

Save Successfully

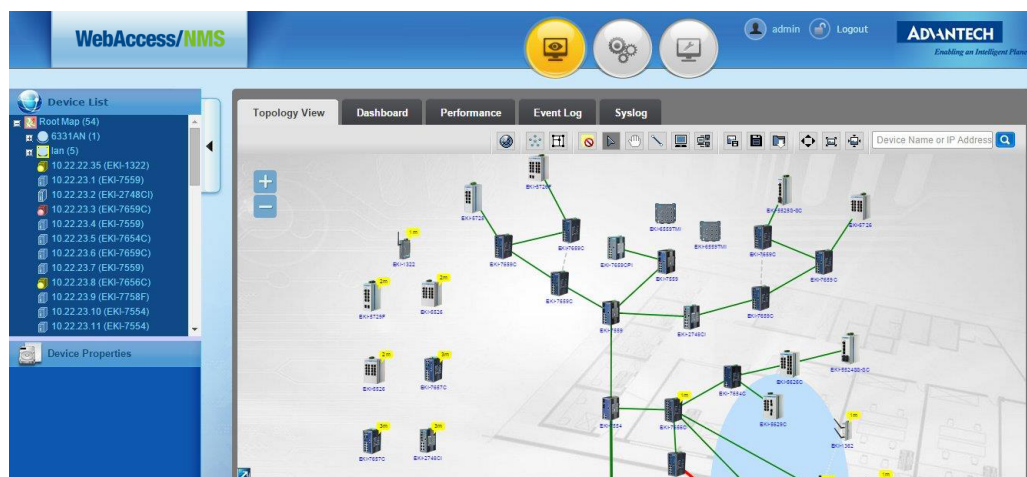


### 9.1.2.15 Load Topology Map

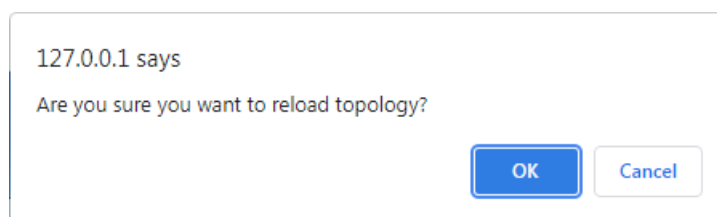
The Load Topology function allows you to recover a topology map from the local system\*.

\* Topology is saved by default on the server: C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\WEB-INF\topoFile

1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.



2. Click the Load Topology  icon to recover a saved topology.
3. Click **Yes** to complete the process.



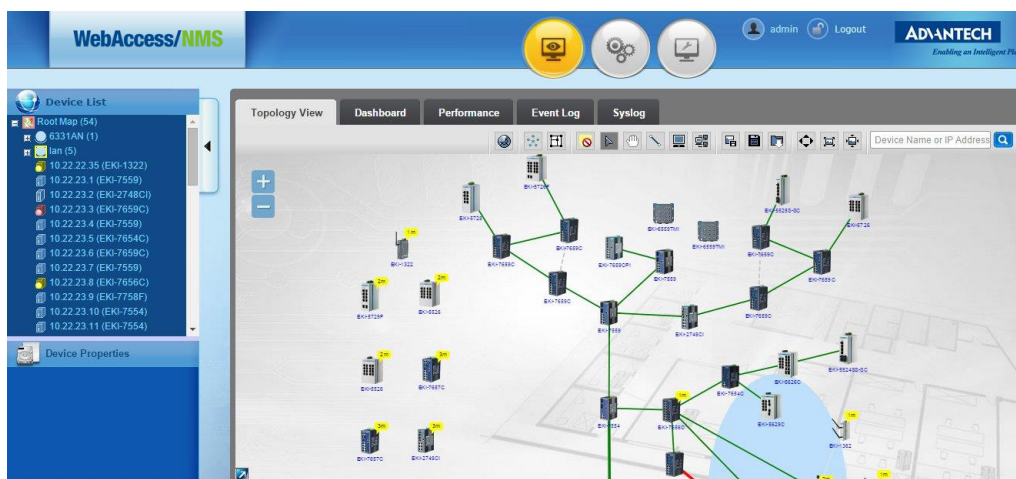
\* System may accommodate 20 users online simultaneously. If the topology is loading by a different user, an exclamation mark displays to notify that the topology has been recovered by a different user.





### 9.1.2.16 View Full Screen

The topology can be displayed on a full screen format.

1. From the tool bar menu click **Monitoring**  to view the options. The Topology View page displays.



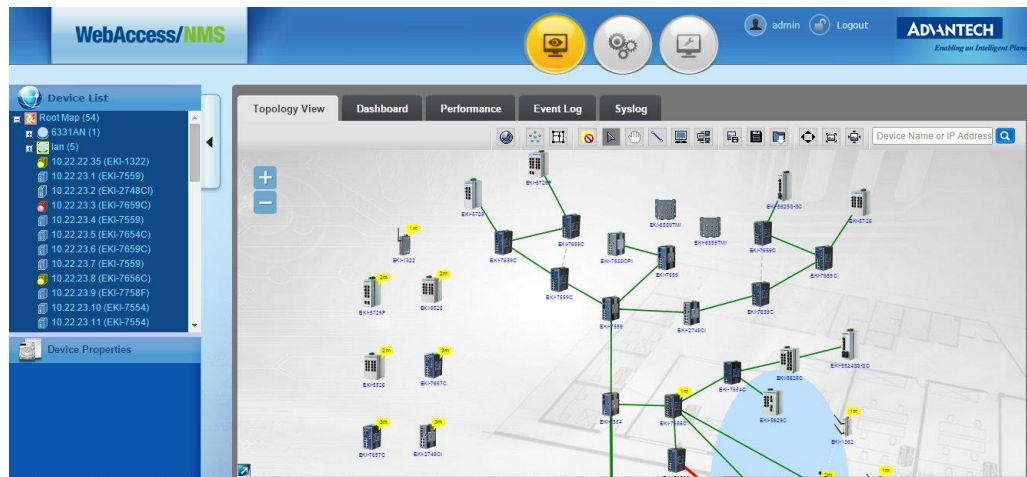
2. Click the Full Screen Topology  to display a full screen view of the current topology.
3. Click **ESC** or  to return to the previous page.

### 9.1.2.17 View Full Screen

The topology can be displayed on a full screen format.

1. From the tool bar menu click **Monitoring**  to view the options.

The Topology View page displays.



2. Click the Zoom Reset  to display the topology in the default view size.

### 9.1.2.18 View Zoom Overview

The full topology view can be displayed by using the Zoom Overview function.

1. From the tool bar menu click **Monitoring**    to view the options. The Topology View page displays.



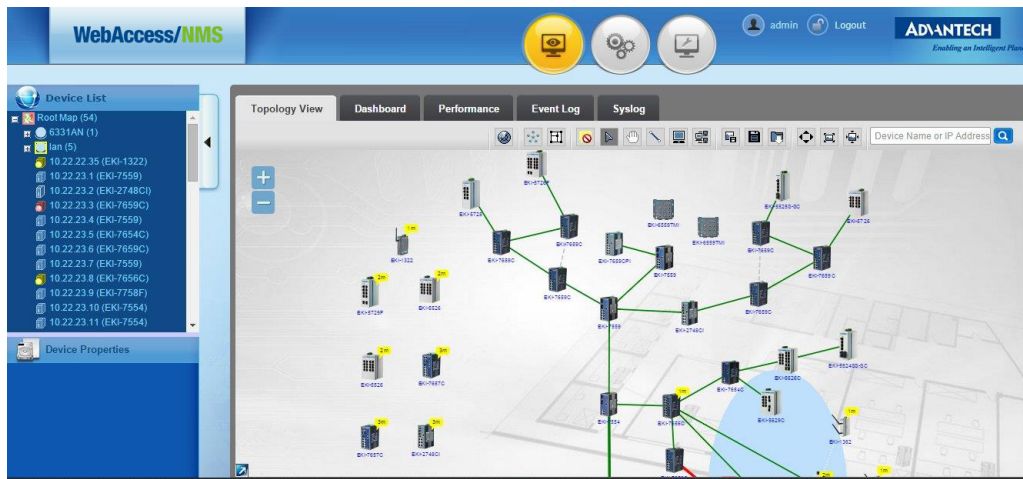
2. Click Zoom Overview  to display the entire topology view on the screen.

### 9.1.2.19 Search for a Device

The full topology view can be displayed by using the Zoom Overview function.

1. From the tool bar menu click **Monitoring**    to view the options.

The Topology View page displays.



2. In the search field  , enter the device name or corresponding IP address.
3. Click Search  : to begin the process.



Discovered devices are highlighted on the topology map.

### 9.1.2.20 Topology Alarm Message

Devices trap notifications are enabled when an issue is detected. If system is operating normally no indications are provided.

There are different alarm states as follow:

- No messages indicate the device is operating normally.
- YELLOW messages indicate a Minor issue.
- ORANGE messages indicate a Major issue.
- RED messages indicate a Critical issue.



Double click on the device to view the Interface Properties menu.

When a device is updating and the Device Properties column displays blank, the device is offline. See the following figure for more information



Events are categorized as follows:

- C indicates a Critical alarms
- M indicates a Major alarm
- m indicates a Minor alarm.

As an example: 2M+ indicates there are 2 Major alarms and other minor alarms.

### 9.1.2.21 Topology Link

Devices are connected to the Internet via Ethernet as indicated by Green link.



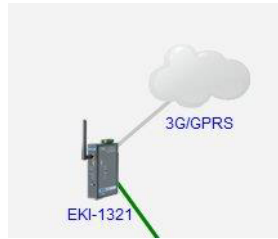
Devices connected to the Internet via WiFi are indicated by a Blue circle. See the following figure for further details.

In the following example, the EKI-6311GN is a wireless AP and all subsequent devices connected to it are encircled in blue. If there is another wireless AP device, it is identified by a different circle.





Devices, such as EKI-1321 and EKI-1322, are able to connect with Internet via 3G/GPRS. The SIM card can be set for their 3G/GPRS setting. 3G/GPRS is indicated by CLOUD icon.

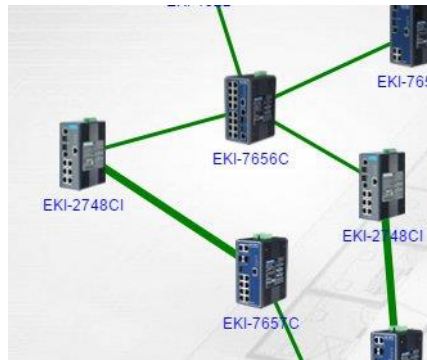


### 9.1.2.22 Status of Topology Link

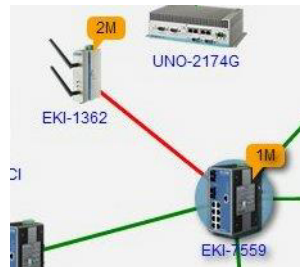
The Topology displays the link status between devices.

Green Solid Line: Indicates devices are connected via Ethernet.

Green Bold Line: Indicates devices are connected via multiple Ethernet links. (trunking)



Red Solid Line: Indicates the connection is offline.

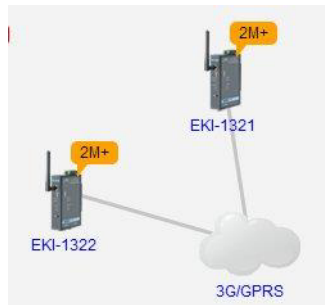


Gray Dashed Line: Indicates the devices are connected by Ethernet but link is blocked.

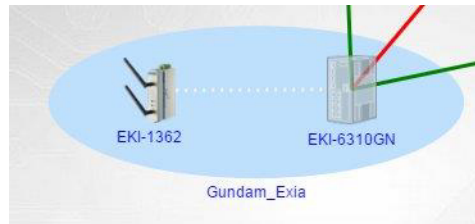
\* Devices, such as EKI-7659C and EKI-7559, can be connected as X-Ring. The spare route for disconnection and re-connection can be shown on the Discovery page. If the system detects the connection failed, the spare route can be run. The situation will be shown graphically and the alarm will be sent.



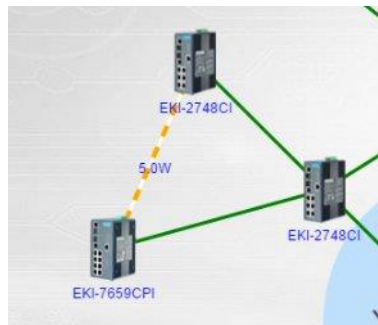
Gray Solid Line: Indicates the devices are connected to 3G/GPRS.



White Dot Line: Indicates the devices are connected via WiFi.



Orange/White dynamic line: Indicates the device has power supply.

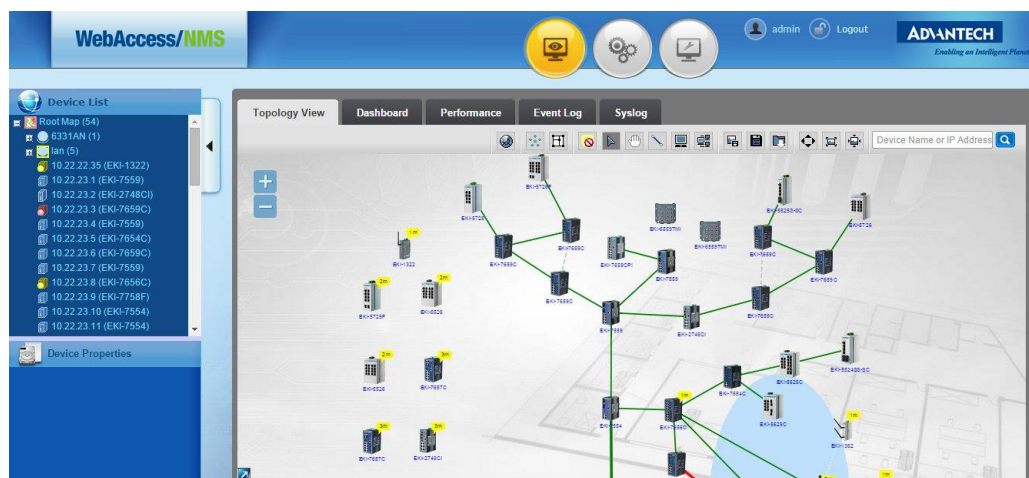


### 9.1.2.23 Traffic Monitoring

The Ethernet traffic between all devices can be monitored through the WebAccess/NMS.

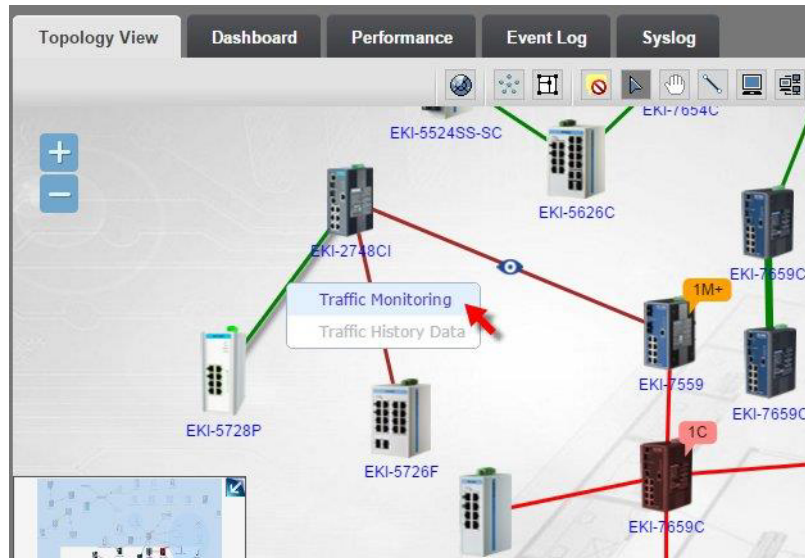
1. From the tool bar menu click **Monitoring**.

The Topology View page displays.

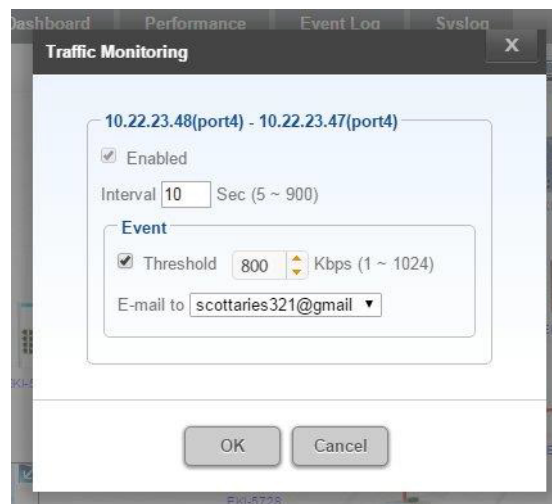



2. Right-click the connection between the devices and click **Traffic Monitoring**.

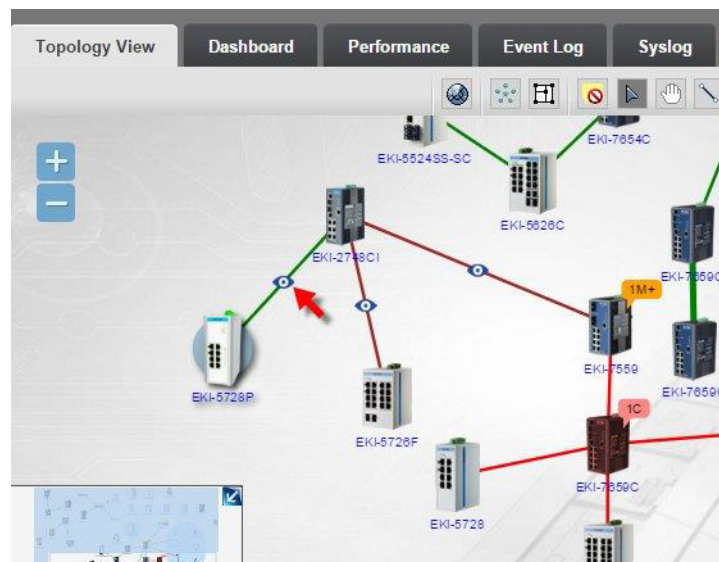
\* This function is only available to Administrator profiles.



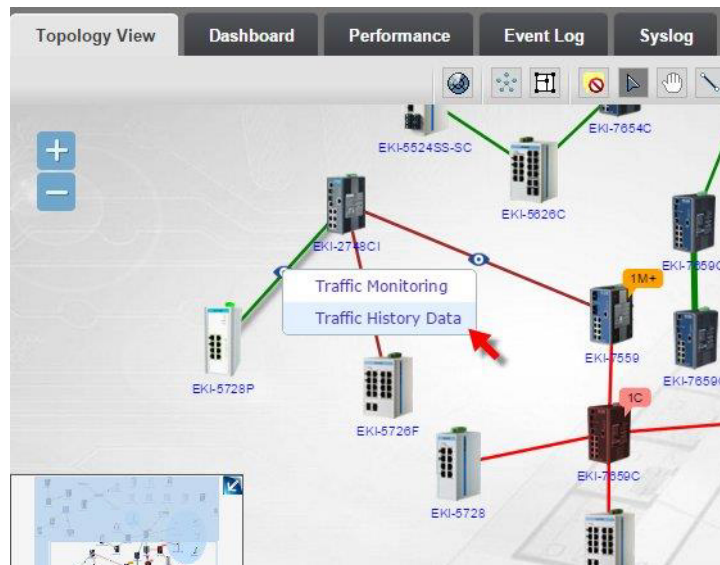
3. The Traffic Monitoring function can be enabled through the pop-up window. The time interval of traffic/the event e-mail list can be set. Click **OK** to finish the setting.



The connected devices set for monitoring are identified through the following icon: .



- Right-click the connection to view the Traffic History Data.



- Click **Traffic History Data** to view the date and Throughput chart. The data can be saved as a CSV file while the chart can be saved as a PNG file.



#### 9.1.2.24 Shortcut Keys

Right-click on the device and a shortcut list will appear. The following Information displays:

Configuration, Performance, Event Log, Edit and Update Device

Update Device can be used to monitor and update the status of device and connection individually.

The Ethernet traffic between all devices can be monitored through the WebAccess/NMS.

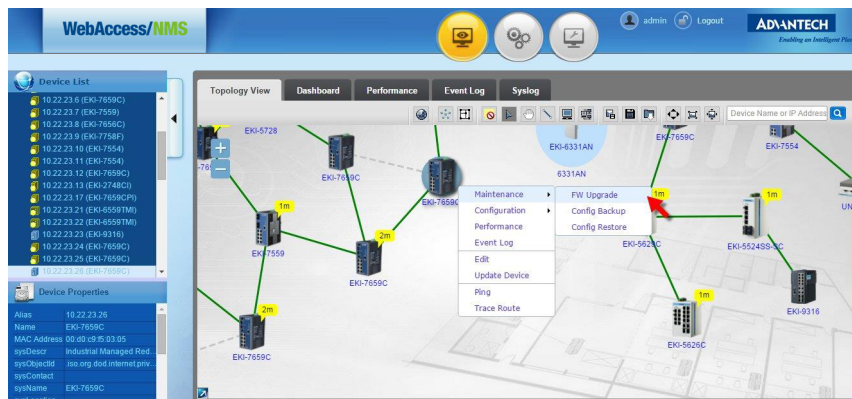
- From the tool bar menu click **Monitoring**.

The Topology View page displays.



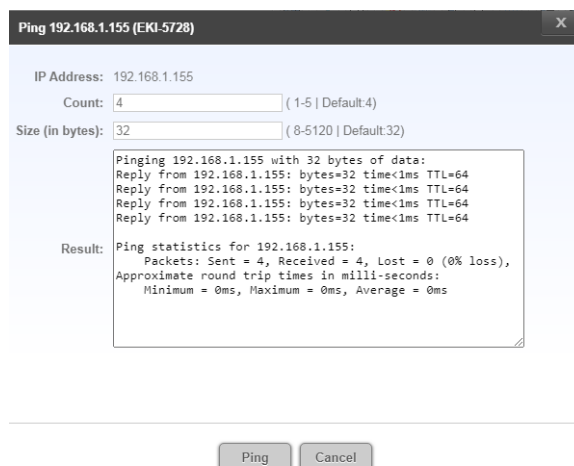
2. Select a device from the topology map and right-click on it to display the short-cut menu.

\* Web Configuration and MIB Browser can only be used with the plug-in package Configuration which is included in the licensed (key) version.



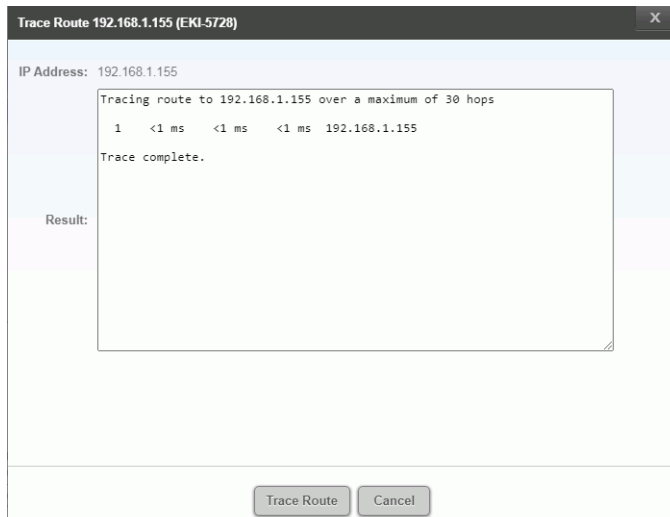
**Ping:** User may monitor if the device is connected by clicking on **Ping**. The result will be shown on the box.

3. Click **Ping** to ping again or click **Cancel** to return to the Topology View.



**Trace Route:** User may trace the route and device hops through the Trace Route function to search issues during transmission.

- Click **Trace Route** to trace again or click **Cancel** to return to the Topology View.

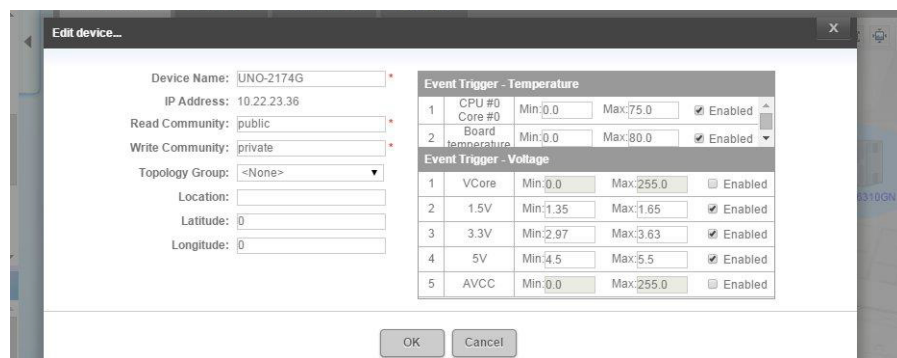


**Update Device:** This function offers the ability to re-discover the status of connection. If the connection of certain device is deleted and would like to recover to previous status of connection.

- Click on **Update Device** without updating the whole topology.

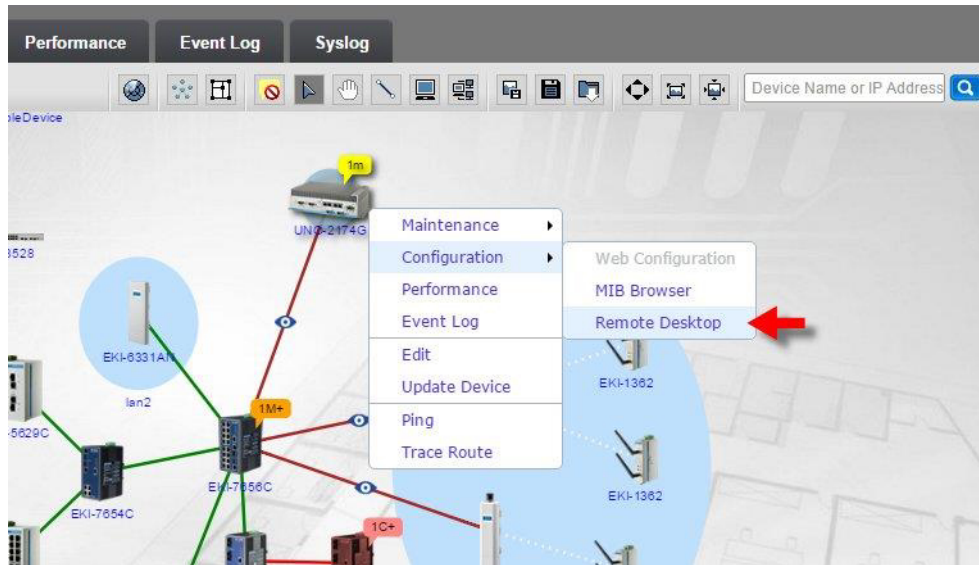


\* For UNO series models, right-click the device then click **Edit**, the detail of device can be edited, and the threshold for temperature and voltage can be set as well.



For UNO series models, right-click the device then click **Configuration - Remote Desktop** to enter the UNO server for configuration.

\* Remote Desktop can only be used with the plug-in package Configuration which is included in the licensed (key) version.



## 9.2 Dashboard

The status of all monitored devices on the system can be referred on the dashboard of WebAccess/NMS. User may also detect and monitor on certain devices.

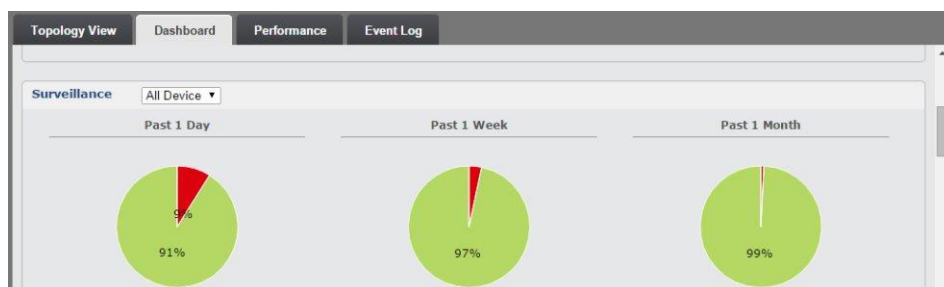
### 9.2.1 Device Status

The percentage of severities (Critical, Major, Minor and Normal) is shown as pie chart. The device status of the Whole System, Switch, Wireless, Device Server, and Platform are shown from left to right, respectively, as the picture below.



### 9.2.2 Surveillance

This function can monitor and check the percentage of device Polling Failed within a certain time interval (Past 1 Day, Past 1 Week and Past 1 Month).

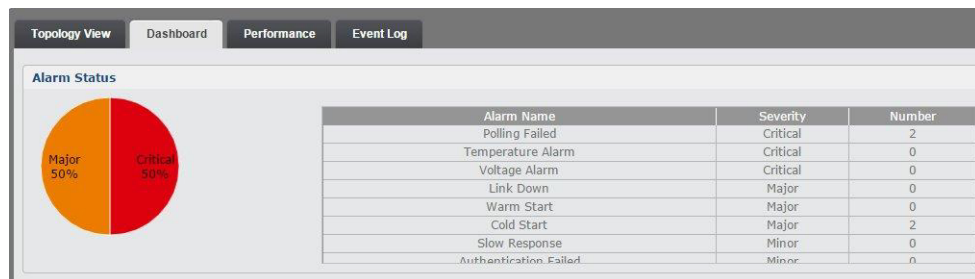


The function can also monitor the percentage of device Polling Success/Failed for certain group. (Group Setting can be referred on “Topology Group” on page 33 and (9) at “Topology Icons” on page 63)



### 9.2.3 Alarm Status

This function can summarize the alarms of Critical, Major and Minor situations. The percentage of Alarm Status is shown as pie chart at left. User may read how many alarms they have to solve from the information.



### 9.2.4 Top 10 Traffic Flow

Dashboard also shows devices with Top 10 traffic flow. Choose the items from the pull-down menu: In/Out Traffic, In/Out Error Traffic, Wireless Traffic or Serial Port Traffic, the system may show the Top 10 list below.





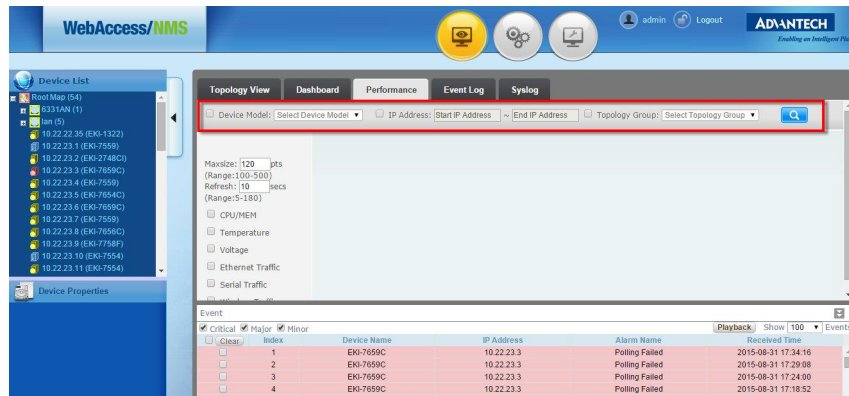
## 9.3 Performance

### 9.3.1 Introduction for Performance

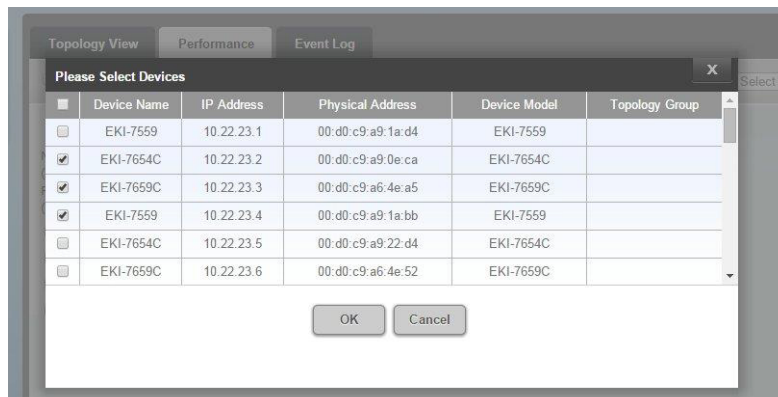
Ethernet Traffic, CPU/Memory rate, Network efficiency, Resource of Server (includes CPU, memory, virtual memory) can be detected by WebAccess/NMS. The data can be shown as line graph.

### 9.3.2 Performance Functions

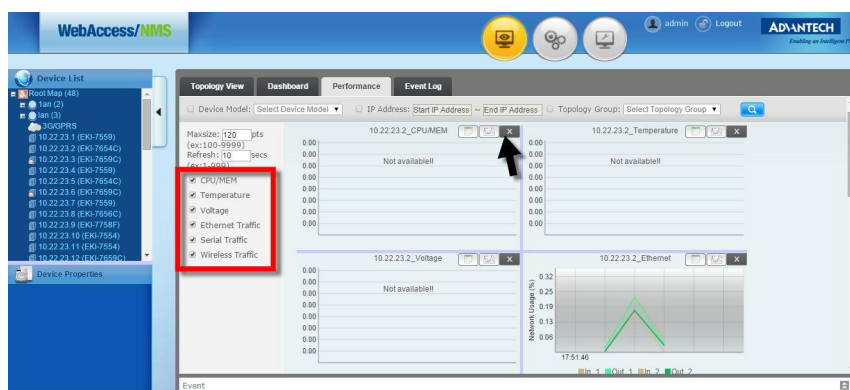
1. Check and select Device Model, IP Address and Topology Group to search.



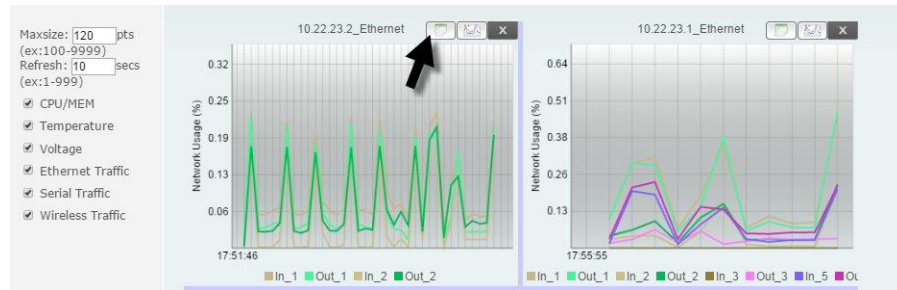
2. Device Name, IP Address, Physical Address, Device Model and Topology Group are shown on the pop up window. Check to select the device (no more than 5) then click **OK**. A window displays Please choose at least one type of data to monitor (30 device performance data diagram maximum)




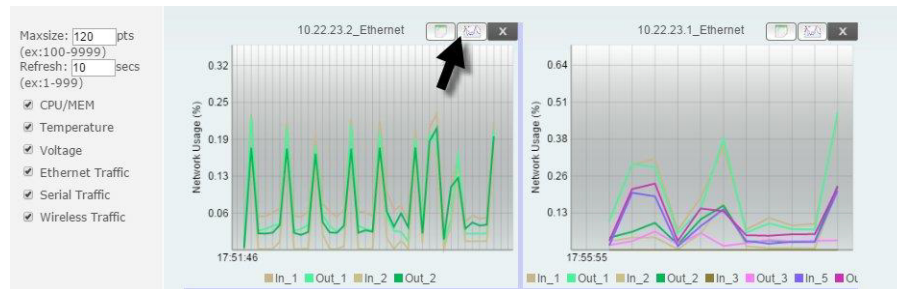
3. Check CPU/MEM, Temperature, Voltage Ethernet Traffic, Serial Traffic and Wireless Traffic for related line graph. If the functions are not supported by the devices, window displays Not available!! on the graph. Click Close (X) to remove the graph from the page.



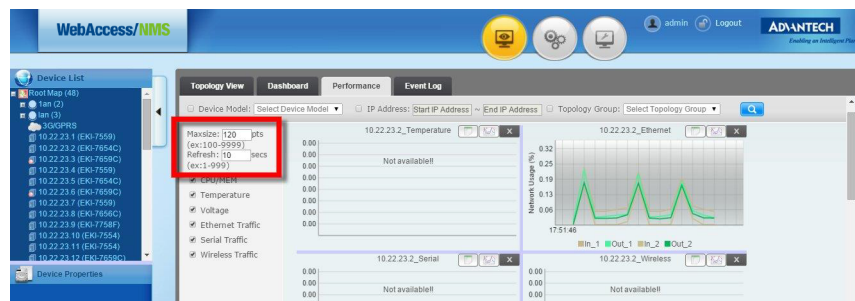
- Click on the  icon, the graphs can be exported as Excel file.



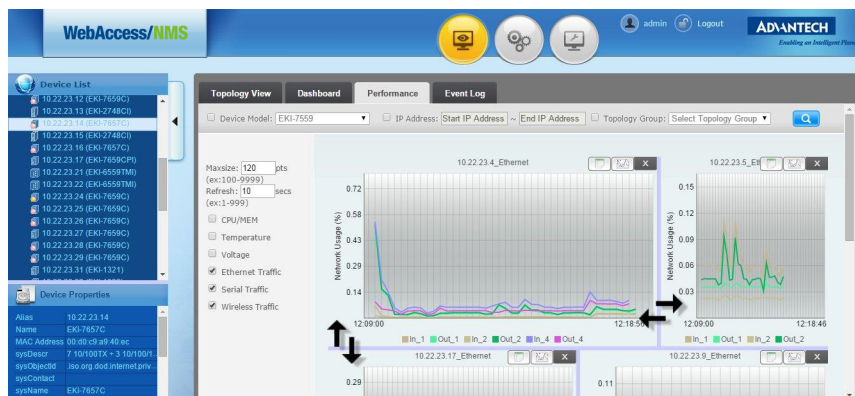
- Click on  icon, the graphs can be exported as PNG image.



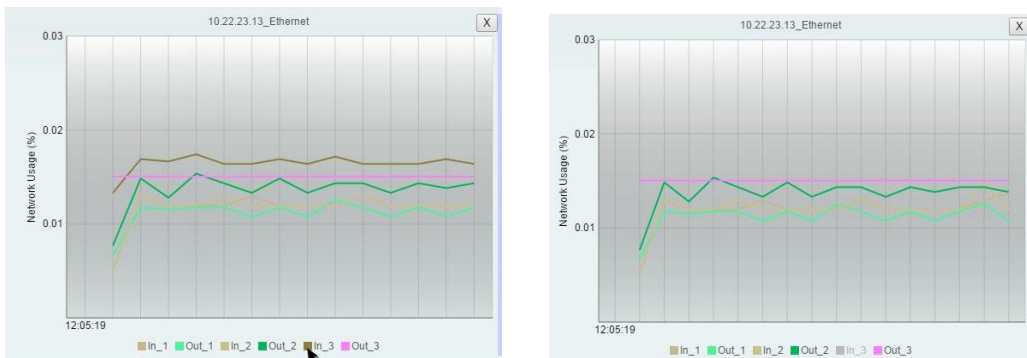
- The default number of points for a line graph is 120. If the number of point is over 120, system will delete the graph and draw a new one. User may set the number of points by themselves between 100~9999.
- The default time for update the status is 10 seconds. There will be a new point generated every 10 seconds. Use may change the update time by entering 1~999 as the time period.



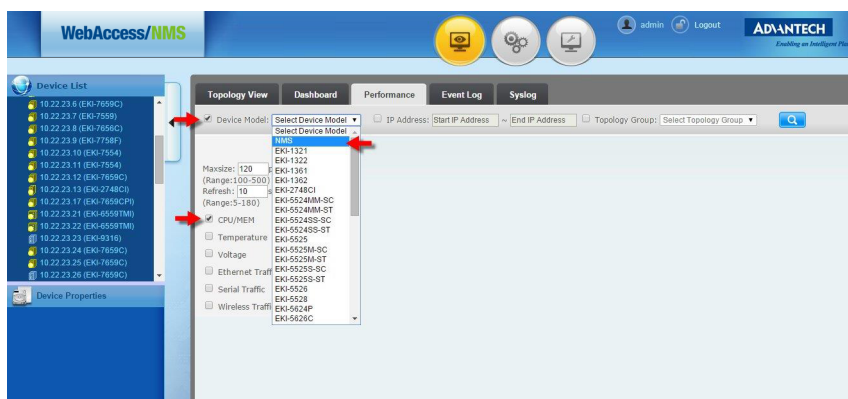
- Scroll the mouse to scale the graph. The graph can be scaled up or down with the mouse scrolled forward or backward.
- Click on the BLUE divide line on the page, the graphs can be disposed with user's convenience.



- Click the color identification below to show/hide the graph.



- For monitoring the server of WebAccess/NMS, click the box of CPU/MEM and choose "NMS" on pull-down menu of Device Model.



- The line chart will be shown after clicking on .

## 9.4 Event Log

### 9.4.1 Introduction for Event Log

WebAccess/NMS can save the polling record in Event Log and send notification to remind that while the hard disk is full. User may search the alarm message by selected conditions.

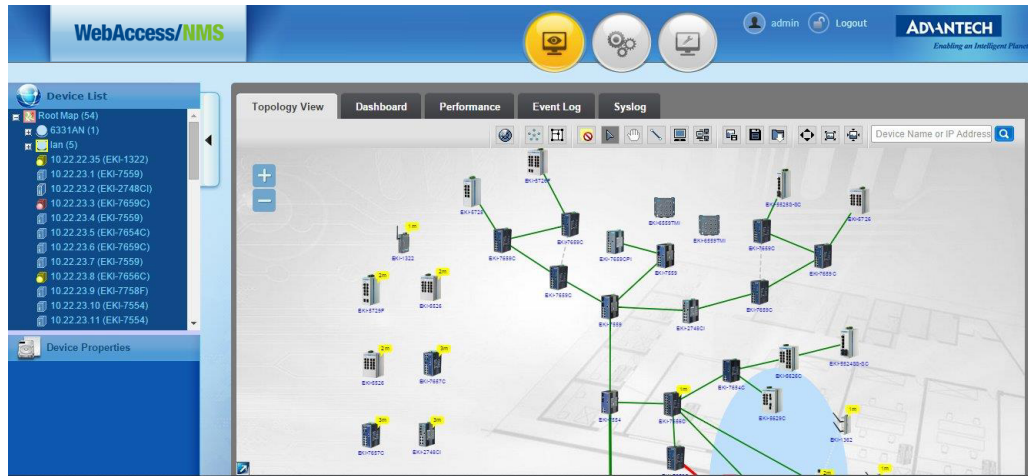
### 9.4.2 Event Log Functions

The page of *Event Log* shows all alarm messages with a default time period: a month. User may check *Device Name*, *IP Address*, *Date* or *Severity* for filtering the list to desired condition, or the previously cleared messages.

Index	Count	Received Time	Device Name	IP Address	Severity	Alarm Name
1	1	2015-06-24 16:32:23	EMS002	10.22.22.195	Critical	EMS is not reachable
2	6	2015-06-24 16:26:23	EMS002	10.22.22.195	Critical	EMS is not reachable
3	6	2015-06-24 16:20:23	EMS002	10.22.22.195	Critical	EMS is not reachable
4	1	2015-06-24 16:17:42	EKI-7657C	10.22.24.14	Normal	Polling Success
5	1	2015-06-24 16:17:42	EKI-2748CI	10.22.24.15	Normal	Polling Success
6	1	2015-06-24 16:17:42	EKI-7657C	10.22.24.16	Normal	Polling Success
7	1	2015-06-24 16:17:42	EKI-1321	10.22.24.34	Normal	Polling Success
8	1	2015-06-24 16:17:42	EKI-5729F	10.22.24.41	Normal	Polling Success
9	1	2015-06-24 16:17:42	EKI-5526	10.22.24.42	Normal	Polling Success
10	1	2015-06-24 16:17:42	EKI-5526	10.22.24.43	Normal	Polling Success
11	1	2015-06-24 16:15:41	EKI-5526	10.22.24.42	Normal	Polling Success
12	6	2015-06-24 16:14:23	EMS002	10.22.22.195	Critical	EMS is not reachable
13	2	2015-06-24 16:14:04	EKI-7657C	10.22.24.14	Minor	Syslog Server is Full

Alarm messages include *Index*, *Count* (Event happens within 5 minutes), *Received Time*, *Device Name*, *IP Address*, *Severity* and *Alarm Name*. The background color is related to their severity.

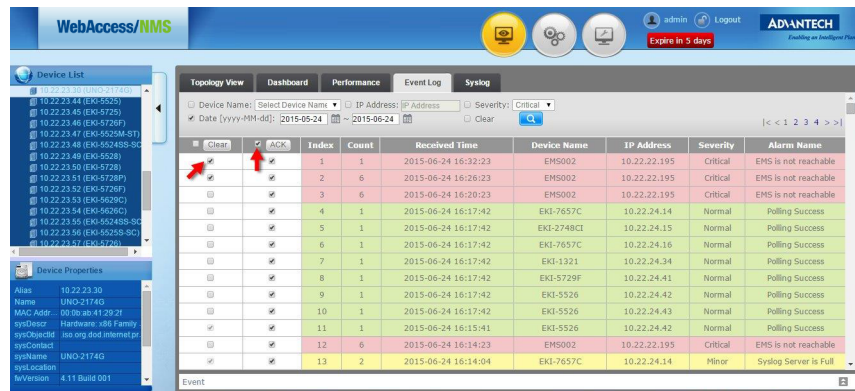
- From the tool bar menu click **Monitoring**.  
The Topology View page displays.



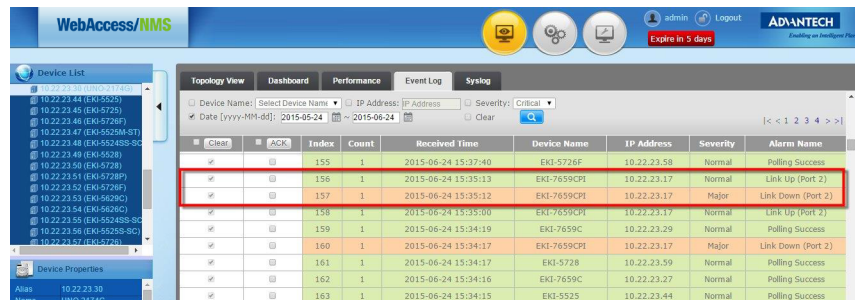
- Click the Event Log tab.
- Every message record can be cleared or marked as read.

Check  **Clear**  **ACK** to clear the log record.

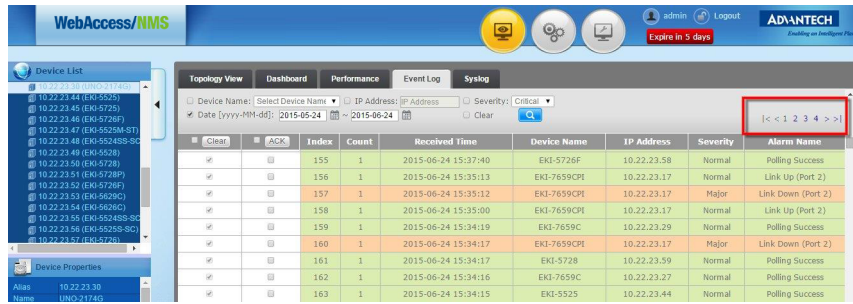
Once cleared a Successfully Deleted or Ack Successfully displays then the page is refreshed. The check symbol will be shown on the selected record, but will not be deleted.



The system may automatically check the Clear function (please refer to “Event Correlation” on page 49). In the following example, the EKI-2748CI status is changed from Link Down to Link Up. System automatically checks **Clear**.

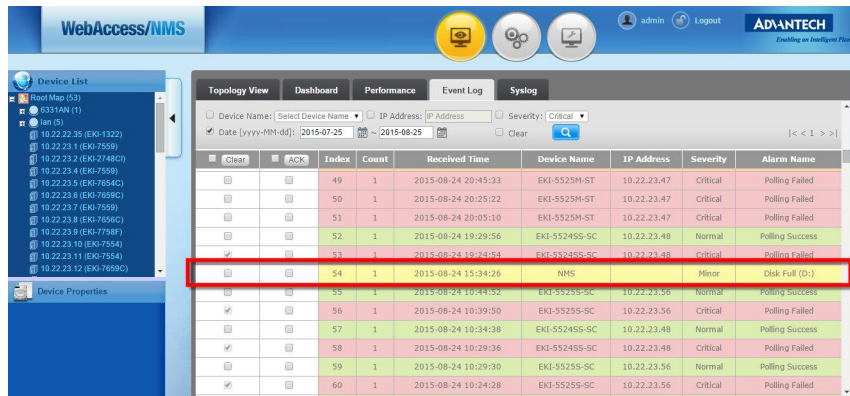


The Event Log displays 1,000 records per page.

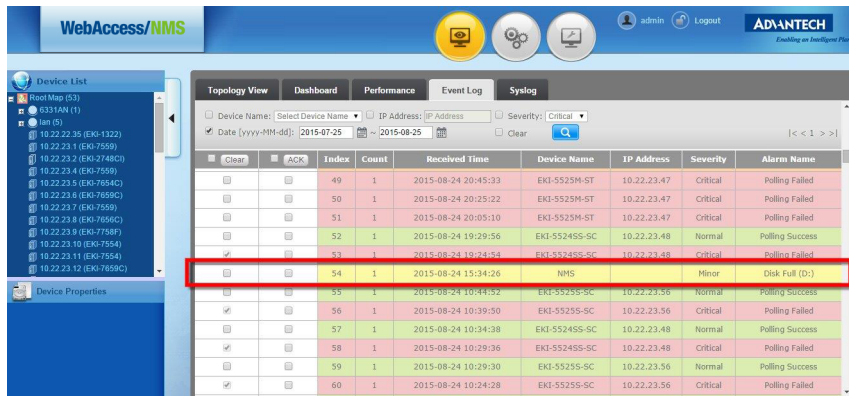


With regard to Alarm Name, The alarm is shown in the Event Log table according to the Severity (“Severity” on page 43). NMS Disk Full and UNO Warranty has been Expired is also specifically listed.

NMS Disk Full (Monitor once per 24 hours)



UNO warranty has been expired. (System will detect the warranty automatically after UNO is installed)



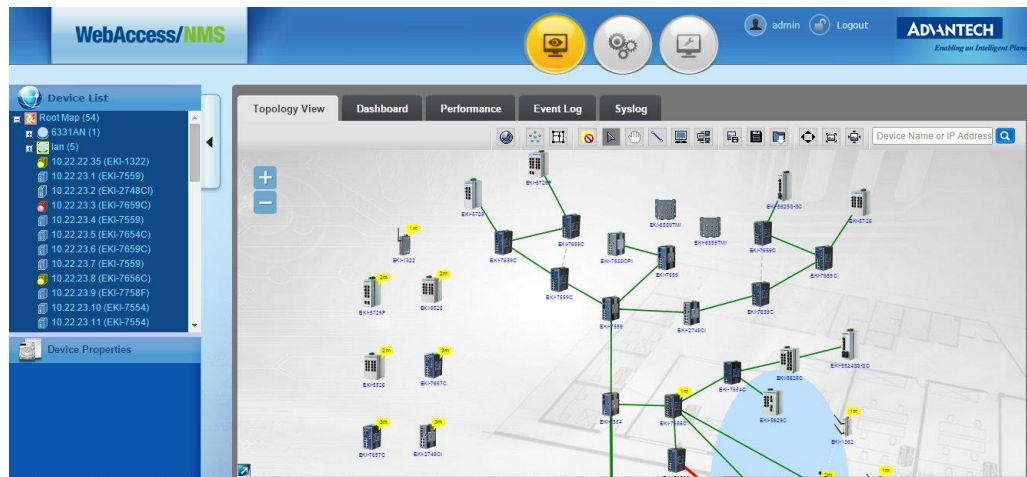
### 9.4.3 Shortcut Key for Event Log



WebAccess/NMS provides a complete alarm record log view.

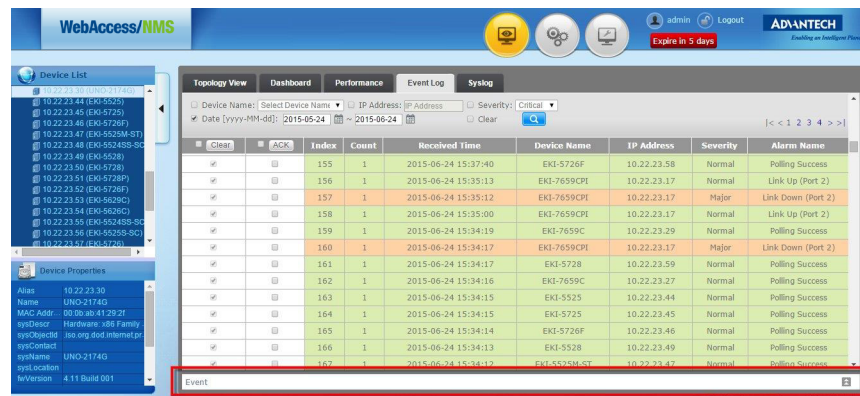
To view the Event shortcut:

1. From the tool bar menu click **Monitoring**.

The Topology View page displays.



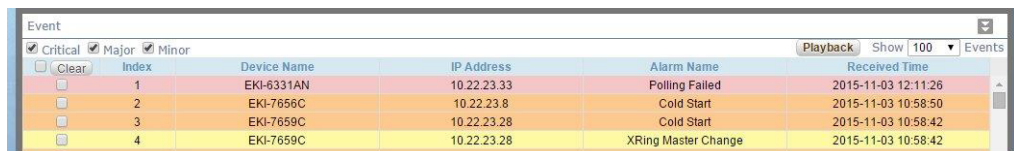
2. Click the Event Log to view the Event Log page.
3. Click  to pop-out or  to hide.



The Event shortcut log key records the following events:

Critical, Major and Minor alarm messages.

Critical situations are indicated in RED, Major situation are indicated in ORANGE, while Minor situations are indicated in YELLOW.



The severity can be chosen by checking the Critical, Major or Minor on the upper-left corner.



4. The Clear Log functions by selecting a log record by checking.
5. Click **Clear** to clear the record. If user wants to check the clearing record, please refer to "Event Log Functions" on page 93. If user has set the Event Cor-

relation (Please refer to “Event Correlation” on page 49), the shortcut event log will clear the record after the alarm is removed.

Index	Device Name	IP Address	Alarm Name	Received Time
1	EKI-6331AN	10.22.23.33	Polling Failed	2015-11-03 12:11:26
2	EKI-7656C	10.22.23.8	Cold Start	2015-11-03 10:58:50
3	EKI-7659C	10.22.23.28	Cold Start	2015-11-03 10:58:42
4	EKI-7659C	10.22.23.28	XRing Master Change	2015-11-03 10:58:42

The number of the events can be chosen by selecting the number from the upper-right pull-down box.

Index	Device Name	IP Address	Alarm Name	Received Time
1	EKI-6331AN	10.22.23.33	Polling Failed	2015-11-03 12:11:26
2	EKI-7656C	10.22.23.8	Cold Start	2015-11-03 10:58:50
3	EKI-7659C	10.22.23.28	Cold Start	2015-11-03 10:58:42
4	EKI-7659C	10.22.23.28	XRing Master Change	2015-11-03 10:58:42

### 9.4.4 Event Playback

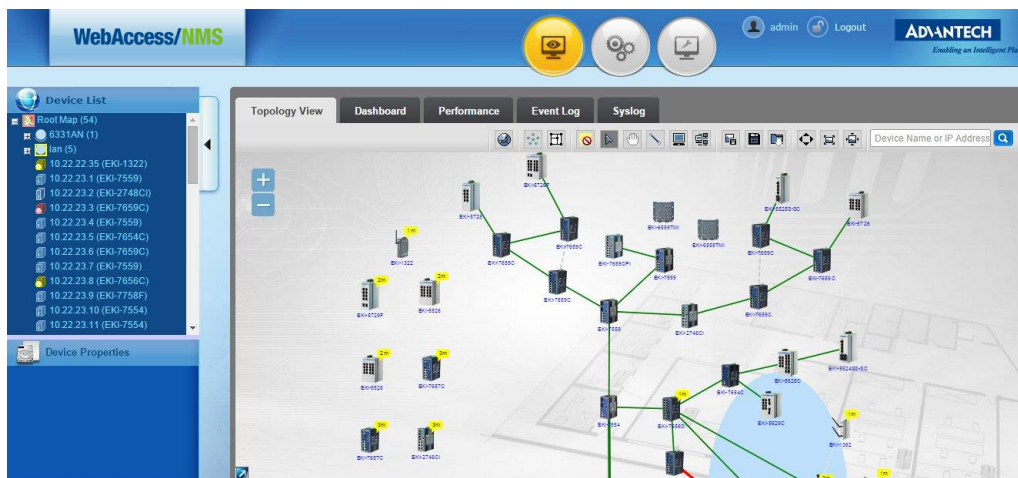
The number of the events can be chosen by selecting the number from the upper-right pull-down box.

The Alarm Event can be saved and for playback. The process can be shown on Topology View. The operation procedures are list as follows:

\* *Event Playback* can only be used with plug-in package "Fault Management Enhancement" included of the license key.

#### 9.4.4.1 Alarm Playback Function

- From the tool bar menu click **Monitoring**.  
The Topology View page displays.

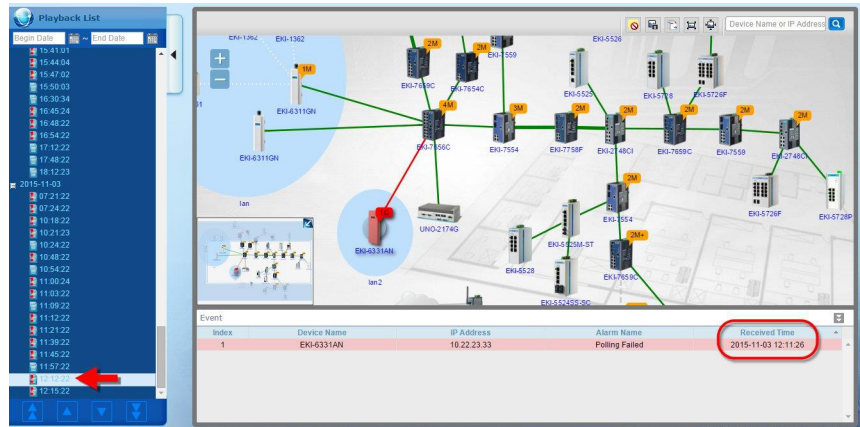


- From the Event frame, click playback to view the Playback List.



The Playback List displays.

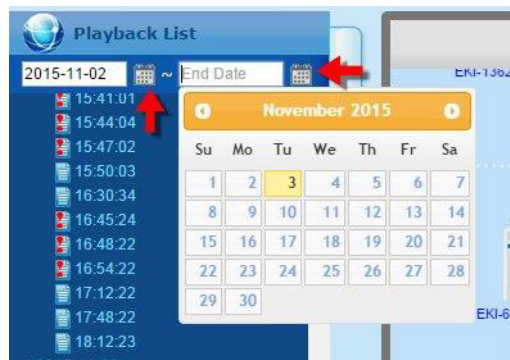
3. Click on the Alarm device to view the related information on the Event table.
4. Check the Event table and the corresponding time of Playback List. Click on the time slot for showing the Topology View at the chosen time.



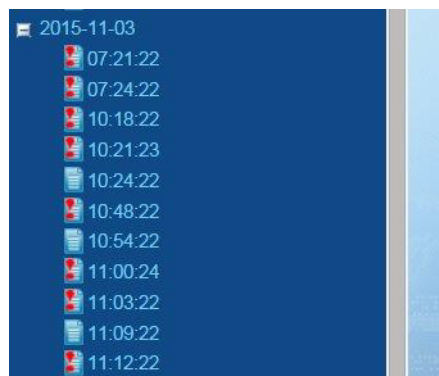
#### 9.4.4.2 Introduction of Playback Function

To activate the playback function:

1. From the Playback List, click on a calendar icon to enter the starting and ending dates to define the search criteria.



2. If there is a red exclamation mark "!" on the icon, it indicated that there is an alarm of the device on the topology. If there is not, it indicates that the devices had been modified or shifted. The processes can all be seen on the Playback function.




3. The Arrow icon can be chosen on the bottom of the Playback List. Click the Double Arrow icon to the Topology View that is with warning exclamation mark "!".

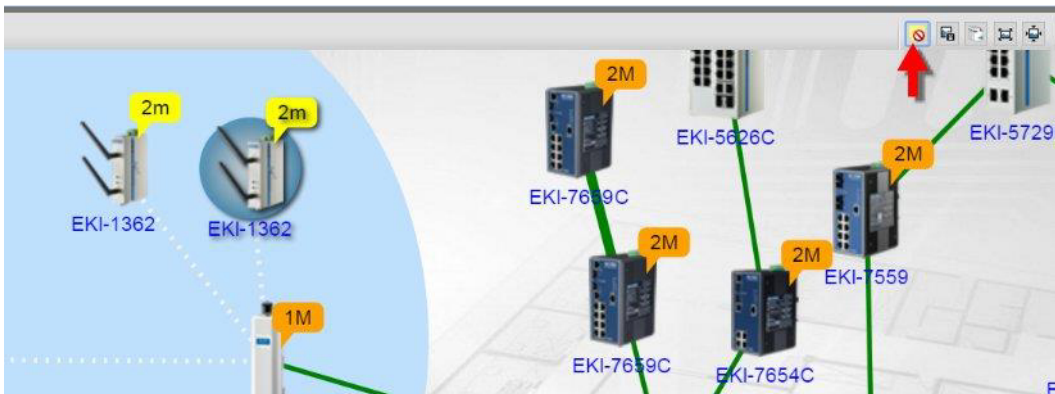






### 9.4.4.3 Playback Toolbar


The Show/Hide Minor Alarm  functions to show/hide the topology. Click the icon to display the corresponding devices identified with a minor alarm.

1. Show Minor Alarm.



2. Click the icon to hide Minor Alarm.  
To export to an image (PNG format):
3. Click  and browse the file folder to save.  
To export to a downloadable file. The XML file can be imported by an NMS application.




Export Playback File : The Playback file can be downloaded, and the .xml file can be imported to other NMS.

4. Click  to view the Export Playback File window.
5. Enter Date and Time, and click **OK** to download the archive file.



The unzip .xml file can be imported to other WebAccess/NMS. The default download path is C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\replay


To Zoom Rest, Zoom Overview, and Device Search:

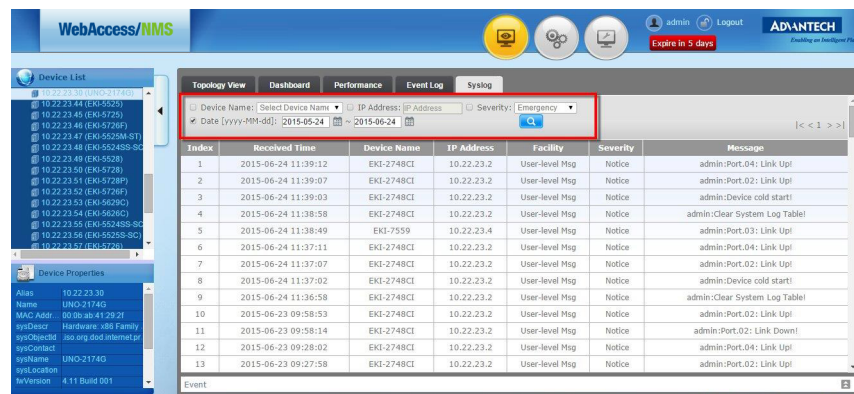
- Zoom Reset : Click to set the viewing size to default and display the Topology Playback.
- Zoom Overview : Click to view the entire Topology Playback on the screen.
- Device Search  : Enter the Device Name or IP Address in the field to perform a device search.

## 9.5 System Log

Syslog may record all events at any time. If the device has been set on webpage or MIB Browser, the firmware has been updated and the configuration has backup, will all be shown on the Syslog. Manager may control the device status by checking the Syslog.

### 9.5.1 Functions for Syslog

Syslog will show all the events within a month. User may check by *Device Name*, *IP Address*, *Severity* and *Date*, then click  to search for the syslog of selected device.



Index	Received Time	Device Name	IP Address	Facility	Severity	Message
1	2015-06-24 11:39:12	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.04: Link Up!
2	2015-06-24 11:39:07	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.02: Link Up!
3	2015-06-24 11:39:03	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Device cold start!
4	2015-06-24 11:38:58	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Clear System Log Table!
5	2015-06-24 11:38:49	EKI-7559	10.22.23.4	User-level Msg	Notice	admin:Port.03: Link Up!
6	2015-06-24 11:37:11	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.04: Link Up!
7	2015-06-24 11:37:07	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Device cold start!
8	2015-06-24 11:37:02	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Device cold start!
9	2015-06-24 11:36:58	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Clear System Log Table!
10	2015-06-23 09:58:53	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.02: Link Up!
11	2015-06-23 09:58:14	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.02: Link Down!
12	2015-06-23 09:28:02	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.04: Link Up!
13	2015-06-23 09:27:58	EKI-2748CI	10.22.23.2	User-level Msg	Notice	admin:Port.02: Link Up!

The Severity includes *Emergency*, *Alert*, *Critical*, *Error*, *Warning*, *Notice*, *Informational* and *Debug*.



Index	Received Time	Device Name	IP Address	Facility	Severity
1	2015-06-24 17:11:22	Unknown	10.22.23.23		Critical
2	2015-06-24 11:39:12	EKI-2748CI	10.22.23.2		Notice
3	2015-06-24 11:39:07	EKI-2748CI	10.22.23.2	User-level Msg	Notice

# Chapter 10

WebAccess / NMS  
Troubleshooting

## 10.1 FAQ

Q1: Internet is connected for sure, but the log-in page cannot be shown

A:

1. Check if the network domain is in the Intranet of computer facilities.
2. If the network domain is in the Intranet and the log-in page still cannot be shown, please contact administrator to reopen Tomcat.

Q2: The account name and password keep appear to be wrong on the log-in page.

A: If user enter wrong password 3 times, the account will be locked and cannot log-in. Please contact administrator to unlock the account.

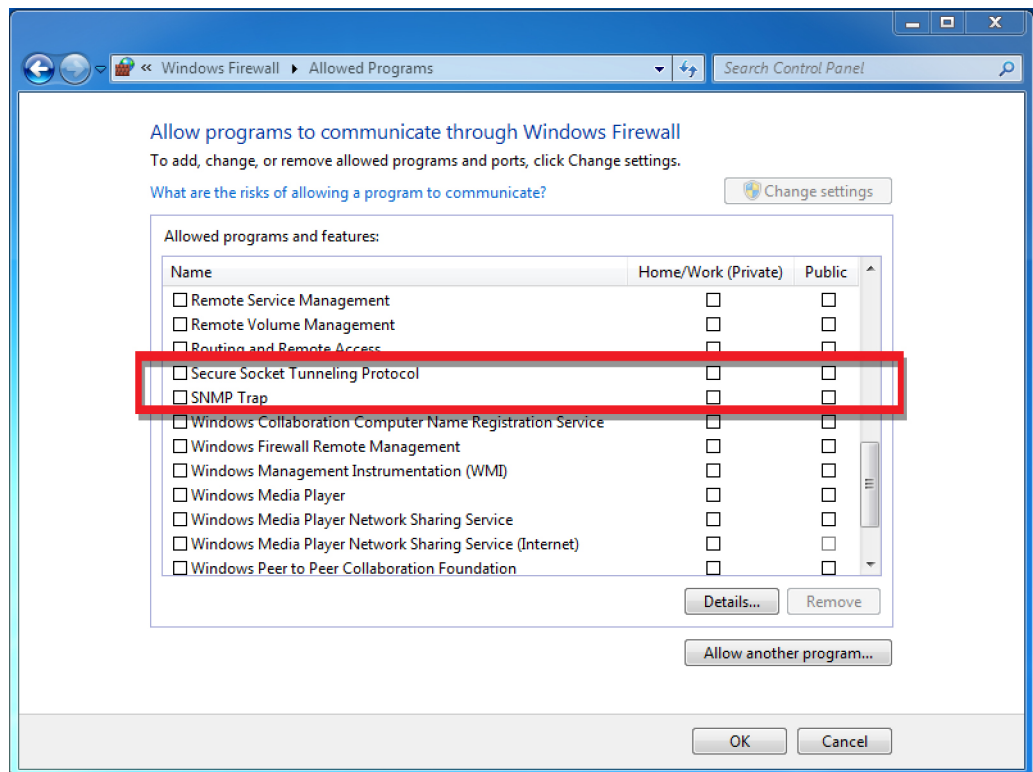
Q3: What should I do if the system is crashed.


A: Please contact administrator to reopen the system server.

Q4: Cannot receive Trap (System cannot receive message from devices)

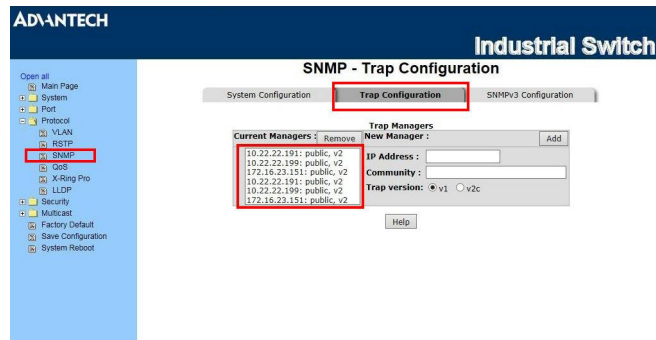
A:

1. Please check Start/Control Panel/Windows Firewall/Allow a program or feature through Windows Firewall. Click Change settings, then check all the boxed of SNMP Trap.



2. If the trap message still cannot be received, please go to the system setup page Setting/Device Data/Managed Device and click  to the device setting page. Check SNMP/Trap Configuration/Current Managers to see if the IP for system

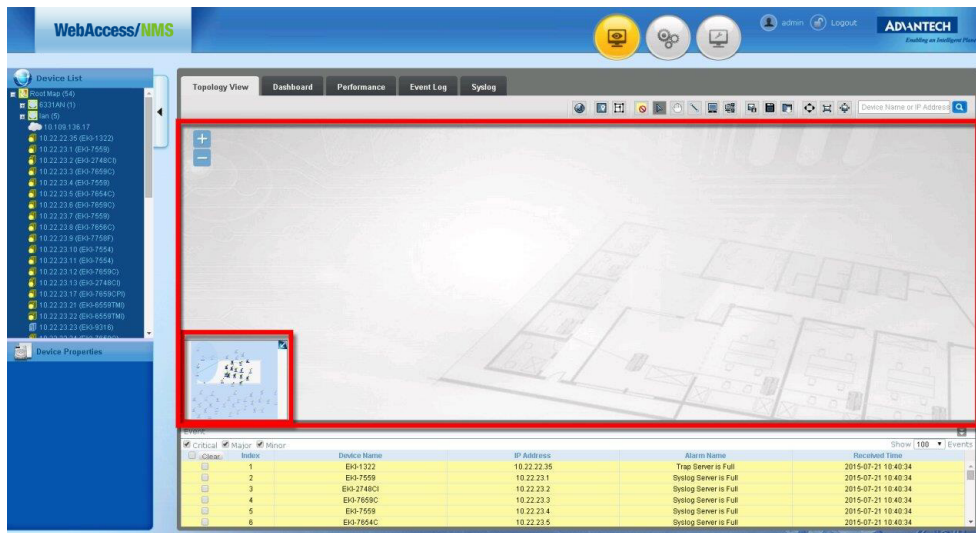
server is in the list. If it's not, please add the IP for the system server to successfully receive the trap message from server.



Q5: Is it possible to open 2 different limited systems, Administrator and User, at the same computer?

A: Yes. But it should be opened by different session. If the system is opened via IE, open the other limited system through File/Create New Session; If the system is opened via Google Chrome, open the other limited system through New incognito window; If the system is opened via FireFox, a CookiPie kit should be downloaded. Reopen FireFox and right-click on the new page, select "Pie" icon on the Toggle On/Off CookiPie, then the other limited system can be opened.

Q6: If the OS of the server is Windows 7 32-bit or Windows server 2008 R2-64bit, why the Topology View cannot show any devices by entering the system by the shortcut on desktop? (Refer to the picture below)



A: Please shut down the server and run as the instruction (2) of "Run WebAccess / NMS" on page 15. Open the Browser and type: <https://localhost/> to enter the Login page. Then the Device Discovery will be shown normally.

# Chapter 11

WebAccess/NMS  
Maintenance and  
Management

## 11.1 Access Control

To avoid any unauthorized access, invade or improper operation, WebAccess/NMS has access control function. For data access, function setting and update scheduling, create access control levels to manage system access and deployment.

### 11.1.1 System User

User may search EMS device group, generate topology, check status and information of devices, and receive device warning message. But authorization is only opened for checking the device data, operation status, event log and efficiency. Adding devices, setting/updating date is not opened. The authorization for WebAccess/NMS user is shown as follows:

System User can only view the history information of Traffic Monitoring and cannot do configuration.

Main Menu	Monitoring				
Sub menu L1	Topology	Dashboard	Performance	Event Log	Syslog
Sub menu L2	Icons				
Auth.	Opened functions: All functions are opened				
	<ul style="list-style-type: none"><li>■ Show/Hide Minor Alarm</li><li>■ Select</li><li>■ Move</li><li>■ Export as Image</li><li>■ Full Screen</li><li>■ Zoom Reset</li><li>■ Zoom Overview</li></ul>				

Main Menu	Settings		
Sub menu L1	Device Data		Severity
Sub menu L2	Managed Device	Supported Device	Trap
Auth.	Can only search devices, download device data, check device data and trap, ping message. No setting and adding functions are allowed.		

## 11.1.2 System Administrator

Administrator has most authorizations, includes creating user's account and password; system and device setting, backup and restore; create EMS group, Topology group; setting alarm message and so on. The authorization for WebAccess/NMS administrator is shown as follows:

Main Menu	Monitoring				
Sub menu L1	Topology	Dashboard	Performance	Event Log	Syslog
Sub menu L2	15 Icons				
Auth.	All functions are opened				

Main Menu	Setting Part 1				
Sub menu L1	Device Data				Severity
Sub menu L2	EMS Group	Topology Group	Managed Device	Supported Device	Trap
Auth.	Supported devices can be revised but can't be added. All functions are opened.				All functions are opened

Main Menu	Setting Part 2					
Sub menu L1	Message			Maintenance		
Sub menu L2	Notification	Event	Correlation	FW Upgrade	Config Backup	Config Restore
Sub menu L3	SMS/ E-mail/ Trap/Sound					
Auth.	All functions are opened					

## 11.1.3 Database Manager

Database manager has the authority not only for system setting, backup and update, but also entering MySQL database and Tomcat to setup CMS and EMS; device access; firmware and geographic information setting; unlock for users. The stored paths for WebAccess/NMS related data are list as follows:

Item	Path on the Server
Device - Backup	C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\ConfigBackup
Device - FW upgrade	C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\FirmwareUpgrade
Database - Backup	C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\DBbackup
Supported Device - Icons	C:\Program Files\Apache Software Foundation\Tomcat 7.0\webapps\SCMS\web\access\img\topology_device



## 11.2 Backup

System and device backup are supported on WebAccess/NMS. Creating the system and device backup is recommended at the first installation, and is good for system recovery if needed.

- System Backup please refer to “Database Backup” on page 25.
- Device Backup please refer to “Configuration Backup” on page 57.

## 11.3 Recovery from Error

System and restore backup are supported on WebAccess/NMS. Creating the system and device restore is recommended at the first installation, and is good for system recovery if needed.

- System Recovery please refer to “Database Restore” on page 26.
- Device Recovery please refer to “Configuration Restore” on page 60.

# Chapter 12

Reference

## 12.1 Reference

WebAccess/NMS Spec\_v3.0.3 Build-in:6299

# ADVANTECH

*Enabling an Intelligent Planet*

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

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© 2022 Advantech Co., Ltd.