

# nCare IoT Management System

User's Manual

# Content

<b>1</b>	<b>Outline for nCare.....</b>	<b>1</b>
<b>2</b>	<b>Introduction for nCare Environment.....</b>	<b>3</b>
2.1	OS Requirement .....	3
2.1.1	Server-End.....	3
2.1.2	Client-End.....	3
2.2	Hardware Requirement.....	3
2.3	Device Management .....	3
<b>3</b>	<b>Introduction for nCare Installation .....</b>	<b>5</b>
3.1	Installation for nCare .....	5
3.2	Uninstallation for nCare.....	5
3.3	nCare Activation .....	6
<b>4</b>	<b>Instruction for nCare Login .....</b>	<b>7</b>
4.1	Procedures for Logging in.....	7
<b>5</b>	<b>Interface Illustration for nCare System.....</b>	<b>10</b>
5.1	Users Management .....	10
5.1.1	Introduction for Account Management .....	10
5.1.2	Operation for Account Management.....	10
5.2	Message Management .....	13
5.2.1	Introduction for Message Management .....	13
5.2.2	Operation for Message Management.....	13
5.3	Database Management .....	20
5.3.1	Introduction for Database Management .....	20
5.3.2	Operation for Database Management.....	20
5.4	DHCP Management.....	20
5.4.1	Introduction for DHCP Management.....	20
5.4.2	Operation for DHCP Management .....	21
5.5	Scan IP.....	24
5.5.1	Introduction for Scan IP .....	24

5.5.2	Operation for Scan IP .....	24
5.6	About .....	25
5.6.1	Introduction for License.....	25
5.6.2	Operation for License.....	25
<b>6</b>	<b>Introduction for nCare Network Device Setting Interface</b>	<b>28</b>
6.1	Functions for Network Device Management .....	28
6.1.1	Introduction for Device List .....	28
6.1.2	Operation for Device List.....	28
6.1.3	Introduction for Configuration Backup.....	47
6.1.4	Operation for Configuration Backup.....	47
6.1.5	Introduction for Configuration Restore .....	49
6.1.6	Operation for Configuration Restore .....	49
6.1.7	Introduction for Firmware Upgrade.....	51
6.1.8	Operation for Firmware Upgrade.....	51
6.1.9	Introduction for Device Provision .....	53
6.1.10	Operation for Device Provision.....	53
6.1.11	Introduction for Modbus Profile.....	55
6.1.12	Operation for Modbus Profile .....	55
6.2	Log Management.....	57
6.2.1	Introduction for Event Log .....	57
6.2.2	Operation for Event Log .....	57
6.2.3	Introduction for System Log.....	59
6.2.4	Operation for System Log .....	60
6.2.5	Introduction for Playback.....	60
6.2.6	Operation for Playback.....	60
6.3	Flow Usage.....	63
6.3.1	Introduction for Flow Usage.....	63
6.3.2	Operation for Flow Usage .....	63
6.4	Severity .....	67
6.4.1	Introduction for Severity .....	67
6.4.2	Operation for Severity.....	67
6.5	Interval .....	68

6.5.1	Introduction for Interval .....	68
6.5.2	Operation for Interval .....	68
6.6	Topology Group.....	69
6.6.1	Introduction for the Topology Group.....	69
6.6.2	Operation for Topology Group .....	69
6.7	Rogue AP/Device .....	70
6.7.1	Introduction for the Rogue AP/Device.....	70
6.7.2	Operation for Rogue AP/Device .....	70
<b>7</b>	<b>Introduction for the Topology Interface of nCare.....</b>	<b>78</b>
7.1	Topology View.....	78
7.1.1	Introduction for Topology View.....	78
7.1.2	Operation for Topology View .....	78
7.2	Device Discovery .....	118
7.2.1	Introduction for Device Discovery .....	118
7.2.2	Operation for Device Discovery.....	118
7.3	Device Status .....	121
7.3.1	Introduction for Device Status .....	121
7.3.2	Operation for Device Status .....	121
<b>8</b>	<b>Introduction for IoT Studio .....</b>	<b>130</b>
<b>9</b>	<b>nCare Maintenance and Management.....</b>	<b>131</b>
9.1	Access Control .....	131
9.1.1	System User .....	131
9.1.2	Device Manager.....	132
9.1.3	System Administrator.....	133
9.2	Device Aberrant Status .....	134
9.2.1	Same IP .....	134
9.2.2	Same MAC .....	135
9.2.3	Set as Loop with Mistake.....	136
<b>10</b>	<b>Appendix 1.....</b>	<b>138</b>



## Table Content

Table 1 Device of Server-End .....	3
Table 2 Device for Client-End.....	3
Table 3 Hardware Requirement.....	3
Table 4 Device Management .....	3

## Figure Content

Figure 1 nCare Shortcut on the Desktop .....	5
Figure 2 nCare Uninstallation on Control Panel.....	5
Figure 3 nCare User Scenario .....	6
Figure 4 nCare Login Page .....	7
Figure 5 Interface Language Selection.....	7
Figure 6 Error Message Notification.....	8
Figure 7 Logout from the System .....	9
Figure 8 Create User Account.....	10
Figure 9 Access Level.....	11
Figure 10 Topology Group Selections for Different Access Level .....	12
Figure 11 Error Message for Create User Account .....	12
Figure 12 User List with Modify and Delete icons. ....	13
Figure 13 E-mail Test.....	14
Figure 14 SMS Test .....	14
Figure 15 SMS Test Message .....	15
Figure 16 WeChat Page.....	15
Figure 17 WeChat Setting Information .....	16
Figure 18 WeChat Message Test.....	16
Figure 19 Test Message List of WeChat Target.....	17
Figure 20 Enter Twitter <i>APP ID</i> and <i>APP Secret</i> .....	17
Figure 21 Sending Test Message to Twitter .....	18
Figure 22 Twitter Test Message Successfully Sent.....	18
Figure 23 Severity, Notification Type and Receiver Setting.....	19
Figure 24 Notification Users Setting.....	19
Figure 25 Database Setting.....	20
Figure 26 Device Setting Webpage.....	21
Figure 27 WAN or LAN Setting Page Selection.....	21
Figure 28 WAN or LAN Setting Page Selection.....	22
Figure 29 Blank for “Hostname to send when requesting DHCP” .....	22
Figure 30 DHCP Enabling .....	23
Figure 31 DHCP Client List .....	24
Figure 32 Enter IP Range .....	24

Figure 33 IP Address and MAC Address List .....	25
Figure 34 Status for Perpetual Version .....	26
Figure 35 Status for Trial Version .....	26
Figure 36 Pop-up Window for Informing Expiration Days .....	26
Figure 37 License Expired Inform .....	27
Figure 38 Device List that Sorting by Device Type .....	28
Figure 39 Show/Hide Rogue Devices .....	29
Figure 40 Add Device Icon .....	29
Figure 41 Information for Creating a new Device.....	30
Figure 42 Device Type Selection .....	30
Figure 43 Scan Protocol Selection.....	31
Figure 44 Scan Protocol Selection.....	31
Figure 45 Topology Group Selection .....	32
Figure 46 Device Configuration Setting Page Icon .....	32
Figure 47 Configuration Setting Login Page .....	33
Figure 48 Status of Device on Device Configuration Page .....	33
Figure 49 MIB Browser Icon .....	34
Figure 50 MIB Browser Setting Page .....	35
Figure 51 Device Reboot Icon .....	35
Figure 52 Device Modification Icon .....	36
Figure 53 IWF Device Setting Page .....	36
Figure 54 <i>Wireless Security</i> Setting Page .....	37
Figure 55 Create VLAN.....	38
Figure 56 Bridge Selection .....	38
Figure 57 VLAN Interface Creation .....	39
Figure 58 VLAN Interface Selection .....	39
Figure 59 Wlan Setting Page for NIO51 Devices .....	40
Figure 60 Serial/Modbus Setting Page for NIO51 Devices .....	41
Figure 61 Parameters Modification for NIO51 of Device Server.....	42
Figure 62 Parameters Modification for WirelessHART of IWSN Gateway.....	43
Figure 63 Parameters Modification for WirelessHART of IWSN Gateway.....	44
Figure 64 Parameters Modification for ISA100 of IWSN Gateway.....	45
Figure 65 Parameters Modification for ISA100 of IWSN Gateway.....	46

Figure 66 IPC Device Setting .....	46
Figure 67 Device Deletion Icon .....	47
Figure 68 Search for Device to Backup.....	47
Figure 69 Configuration Backup with Schedule.....	48
Figure 70 Configuration Backup Schedule List .....	48
Figure 71 Status of Scheduled Configuration Backup.....	49
Figure 72 Search for Device to Restore .....	49
Figure 73 Backup File Selection .....	50
Figure 74 Configuration Restore Confirmation.....	50
Figure 75 Error Message for Wrong Backup File .....	51
Figure 76 Selection for the Device to Upgrade the Firmware .....	51
Figure 77 Upgrade the Firmware with Schedule.....	52
Figure 78 Scheduled Task Modification .....	52
Figure 79 Firmware Upgrade Result .....	53
Figure 80 Device Provision Setting .....	54
Figure 81 Choose the Device to Provision.....	54
Figure 82 Enter Modbus Profiles .....	55
Figure 83 Enter Discovery Parameter .....	56
Figure 84 Enter Register Table Parameters.....	56
Figure 85 Modbus Device List.....	57
Figure 86 Searching Conditions for Event Log.....	57
Figure 87 Event Log Table.....	58
Figure 88 Clear Event Record.....	58
Figure 89 Event Shortcut Table and its Icon.....	59
Figure 90 Severity Level shown on Event Shortcut Table.....	59
Figure 91 Severity Selection.....	59
Figure 92 System Log Table .....	60
Figure 93 Playback Setting.....	61
Figure 94 Events Playback.....	61
Figure 95 Events Searching .....	62
Figure 96 Issues shown on Topology.....	62
Figure 97 Data Table of Flow Usage.....	63
Figure 98 Different Form for Line Chart.....	64

Figure 99 Eth Data chart .....	64
Figure 100 WLAN Data Chart .....	65
Figure 101 CPU Data Chart .....	65
Figure 102 Memory Usage Data Chart .....	66
Figure 103 NIO200 Device Data Flow Line Chart.....	66
Figure 104 NIO51 Device Data Flow Line Chart.....	67
Figure 105 Severity Table.....	67
Figure 106 Severity Modification.....	68
Figure 107 Interval Setting Page.....	68
Figure 108 Add Topology Group Window.....	69
Figure 109 Topology Group List and Modify/Delete Icons .....	70
Figure 110 Scan for Rogue AP/Device.....	70
Figure 111 Rogue AP/Device Table .....	71
Figure 112 Rogue AP/Device list on Event Log Table .....	71
Figure 113 Rogue AP/Device on Device List.....	72
Figure 114 Rogue AP/Device on Topology .....	72
Figure 115 Add Rogue AP/Device into White List.....	73
Figure 116 White List.....	73
Figure 117 Add to White List Procedure .....	74
Figure 118 Scanning for White List Devices.....	74
Figure 119 Selection for Rouge Devices that Concatenated under the Device on the White List.....	75
Figure 120 Rogue Device Setting on White List.....	75
Figure 121 Rogue Device Loading .....	76
Figure 122 Rogue Device Loading Success.....	76
Figure 123 Rogue Device Added Manually.....	77
Figure 124 Rogue Detection Interval.....	77
Figure 125 nCare Topology(.....	78
Figure 126 Tool Bar for Topology .....	78
Figure 127 Device Selection.....	79
Figure 128 Connection Selection .....	79
Figure 129 Multiple Devices Selection .....	79
Figure 130 Add Connection.....	80

Figure 131 Add New Device .....	80
Figure 132 Device Discovery .....	81
Figure 133 New Device Not Found Window .....	81
Figure 134 Add Device Successfully .....	82
Figure 135 Group Selection .....	82
Figure 136 Topology Group Setting.....	83
Figure 137 Group Generation.....	83
Figure 138 Remove Group .....	84
Figure 139 WiFi Group Icon .....	84
Figure 140 WiFi Group Selection .....	85
Figure 141 Remove from WiFi Group .....	85
Figure 142 Back to Topology Icon .....	86
Figure 143 Device Deletion.....	86
Figure 144 Topology on Google Map.....	87
Figure 145 Flow Rate Monitoring .....	87
Figure 146 High Traffic Connection .....	88
Figure 147 Traffic Monitoring .....	88
Figure 148 Traffic Monitoring Window .....	89
Figure 149 Traffic Monitoring Started .....	89
Figure 150 Traffic Over Threshold .....	90
Figure 151 Stop Traffic Monitoring .....	90
Figure 152 Two Traffic Monitoring Simultaneously.....	91
Figure 153 Show/Hide Rogue Devices Icon.....	91
Figure 154 VLAN Selection .....	92
Figure 155 VLAN Topology .....	92
Figure 156 IWF AP Update .....	93
Figure 157 IWF AP Not Found.....	93
Figure 158 IWF AP Update .....	94
Figure 159 Account Setting for NIO200-HAG Series Devices .....	94
Figure 160 Account Setting Window for NIO200-HAG .....	95
Figure 161 NIO200-HAG Account Setting Success.....	95
Figure 162 IWSN Update.....	96
Figure 163 Scanning for NIO200-HAG Devices .....	96

Figure 164 Scanned Device Group under NIO200-HAG Devices .....	97
Figure 165 Check for NIO200-HAG Group Devices .....	97
Figure 166 NIO200-HAG Group Devices Disconnected .....	98
Figure 167 Account Setting Window for NIO200-IAG .....	98
Figure 168 Scanned ISA100 Device Group of NIO200-IAG .....	99
Figure 169 Check for ISA100 Device Information.....	99
Figure 170 Time Zone Setting for NIO200 Series Devices.....	100
Figure 171 Time Zone Sync with Browser.....	100
Figure 172 Save Topology .....	101
Figure 173 Load Topology.....	101
Figure 174 Update NIO50 Device.....	102
Figure 175 Modbus ID Setting .....	102
Figure 176 Modbus ID Setting for NIO50 Device .....	103
Figure 177 Modbus ID Setting Window .....	103
Figure 178 NIO50 Device Updating.....	104
Figure 179 Adding NIO50 Device to Topology Group .....	104
Figure 180 Devices in Topology Group .....	105
Figure 181 Devices in PLC Group.....	105
Figure 182 Devices Status for PLC Device.....	106
Figure 183 Modbus Scheduling.....	106
Figure 184 Time and Repeat Cycle for Modbus Scheduling.....	107
Figure 185 PLC Information Update .....	107
Figure 186 PLC Group of NIO51.....	108
Figure 187 Devices Information of NIO51.....	108
Figure 188 Modification for PLC Device of NIO51.....	109
Figure 189 Color Indication of Devices .....	109
Figure 190 Letter Indication of Device .....	109
Figure 191 Internet Connection.....	110
Figure 192 Trunk Connection .....	110
Figure 193 Trunk Status.....	111
Figure 194 Mesh Network Connection .....	111
Figure 195 WiFi Connection .....	111
Figure 196 Devices in the Wifi Subnet.....	112

Figure 197 Devices in the Wifi Subnet.....	112
Figure 198 Purple Line.....	113
Figure 199 Purple Bold Line .....	113
Figure 200 VLAN Status .....	113
Figure 201 Normal Link.....	114
Figure 202 High Traffic Link.....	114
Figure 203 Disconnected Link .....	115
Figure 204 Link Over the Threshold .....	115
Figure 205 Shortcut Key.....	116
Figure 206 Ping Function.....	117
Figure 207 Reboot Function .....	117
Figure 208 Remote Desktop .....	118
Figure 209 Device Discovery .....	119
Figure 210 Recent Searching Records of IP Range.....	119
Figure 211 CAPWAP Device Search without Entering IP Range.....	120
Figure 212 Device Searching with CAPWAP .....	120
Figure 213 Scan Percentage .....	121
Figure 214 Discovered Devices .....	121
Figure 215 IWF Type Device Status .....	122
Figure 216 IPC Type Device Status .....	122
Figure 217 WMI Function for IPC Device.....	123
Figure 218 WMI Page for IPC Device .....	123
Figure 219 History Status of PLC Device .....	124
Figure 220 PLC Type Device Register Table.....	124
Figure 221 Register Table Modification .....	125
Figure 222 Register Value Modification.....	125
Figure 223 Status Exportation .....	126
Figure 224 PLC Status for NIO51 .....	126
Figure 225 Device Status for NIO200-HAG.....	127
Figure 226 Run Command for NIO200-HAG.....	127
Figure 227 Device Status for NIO200-IAG.....	128
Figure 228 Run Command for NIO200-IAG.....	129
Figure 229 Trouble Shooting Page for ISA100 .....	129



Figure 230 Operation Page for IoT Studio.....	130
Figure 231 Authorization for nCare User.....	131
Figure 232 Authorization for nCare Manager .....	132
Figure 233 Authorization for nCare Administrator .....	133
Figure 234 Discovery Result for the Same IP .....	134
Figure 235 Event Log List for the Same IP .....	134
Figure 236 Discovery Result for the Same MAC .....	135
Figure 237 Event Log List for the Same MAC .....	135
Figure 238 Scan IP List for the Same MAC .....	136
Figure 239 Event for Devices set as Loop with Mistake on Main Page.....	136
Figure 240 Event for Devices set as Loop with Mistake on Event List.....	137
Figure 241 Login to Twitter Apps.....	138
Figure 242 Build a New Program.....	138
Figure 243 Create an application page .....	139
Figure 244 Obtain Application Data .....	139
Figure 245 Permission Selection.....	140
Figure 246 Permission Opening.....	141
Figure 247 Enter APP ID and APP Secret .....	141
Figure 248 Twitter Authorization Page.....	142
Figure 249 Twitter PIN Code .....	142
Figure 250 Enter PIN Code .....	143
Figure 251 Send Twitter Test Message .....	143
Figure 252 Test Message Sent Successfully .....	144

## 1 Outline for nCare

nCare is a management system used for managing devices for Nexcom. A synthetic platform developed for monitoring, setting and maintaining devices via IP-based network with high efficiency, synchronicity and convenience.

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

(1) Auto-discovery and cloud management

- To manage AP and CPE with CAPWAP & LLDP & SNMP
- Device can be added, edited and deleted

(2) Visual Topology

- Mesh network and basic structure of topology are supported

(3) AP management

- Provisioning & configure
- Configuration backup & restore
- Restore to factory default
- Device Reset
- Firmware upgrade
- Admin utility

(4) System report and daily record

- Asset status
- Export report
- System log
- Usage report

(5) Event notification

- Event trigger: Pre-defined

- Outbound notice

(6) Administration

- Authority by username/password
- Scale up

## 2 Introduction for nCare Environment

### 2.1 OS Requirement

#### 2.1.1 Server-End

Table 1 Device of Server-End

Operation System	Window 7
Web Server	Tomcat 7.0
Database Server	MySQL (free)

#### 2.1.2 Client-End

Table 2 Device for Client-End

PC Browser	Firefox, IE11, Chrome
------------	-----------------------

### 2.2 Hardware Requirement

Table 3 Hardware Requirement

Device	Type	Specification
Processor	Intel(R) Atom(TM) CPU C2558	At least 2.40GHz
Memory	DDRⅢ	8GB
I/O	Ethernet	1000Mbps
Storage	HDD	At least 75GB

### 2.3 Device Management

Table 4 Device Management

Device	Model
Industrial wireless network access device	IWF300、IFW310、IWF3310
Outdoor wireless network access device	IWF503、IWF504D、IWF6320、IWF6330

Device Server	NIO50、NIO51
Switch	IGS-402SM-4PH24、IGS-402SM-8PH24、 IGS-1604SM
IWSN Gateway	NIO200(IAG、IDG、IDR、HAG、WMR)

### 3 Introduction for nCare Installation

#### 3.1 Installation for nCare

- (1) Contact local Nexcom agent to get the software CD or download authority for installation package.
- (2) Confirm the server requirement for nCare environment.
- (3) Please refer to **nCare Quick Installation Guide** for detail installation procedures.
- (4) There is a shortcut on the desktop after installation.



Figure 1 nCare Shortcut on the Desktop

#### 3.2 Uninstallation for nCare

Open *Control Panel>Programs and Features* to find **nCare(remove only)**, then click **Uninstall** to remove nCare from the system.

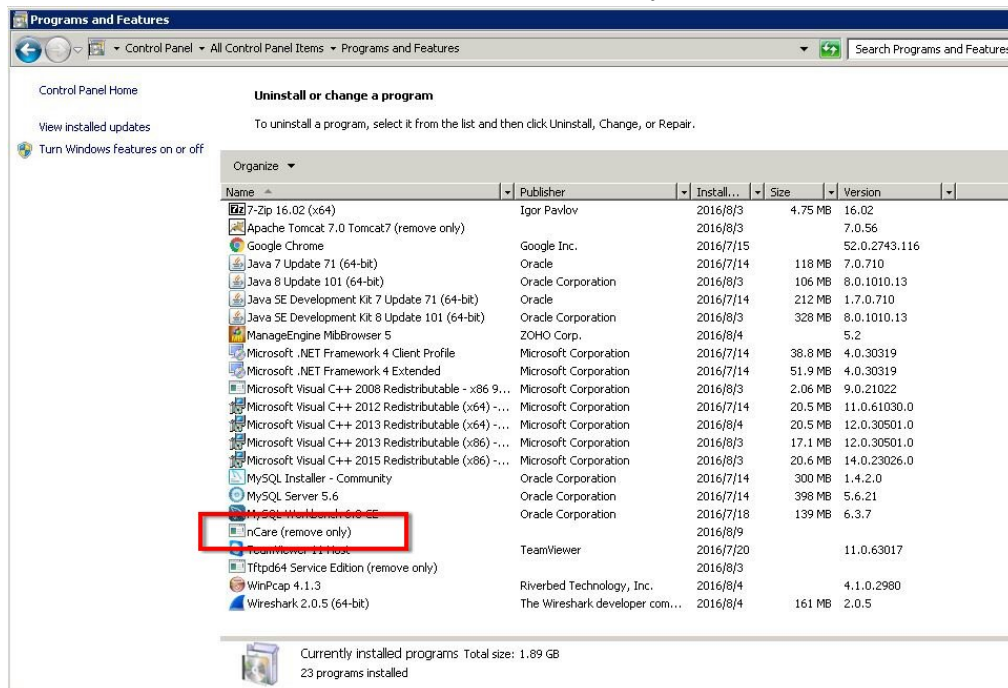


Figure 2 nCare Uninstallation on Control Panel

### 3.3 nCare Activation

- (1) nCare can be used on browsers such as IE 11, Chrome or Firefox. Double-click the shortcut icon to enter the login page directly.
- (2) Or type the web address: `https://localhost/` to enter login page.
- (3) nCare is a web-based application system. There is no need for installation procedures for normal user or administrator. Type `https://x.x.x.x/`, whrer `x.x.x.x` is the IP of nCare server.
- (4) If the nCare system is provided by Nexcom agent, the default information is  
IP:192.168.1.253  
Subnet Mask: 255.255.255.0  
An Ethernet cable should be connected with server and device **Ian0**.
- (5) Enter the information above to activate nCare. And other users can use the system on browser or APP then.

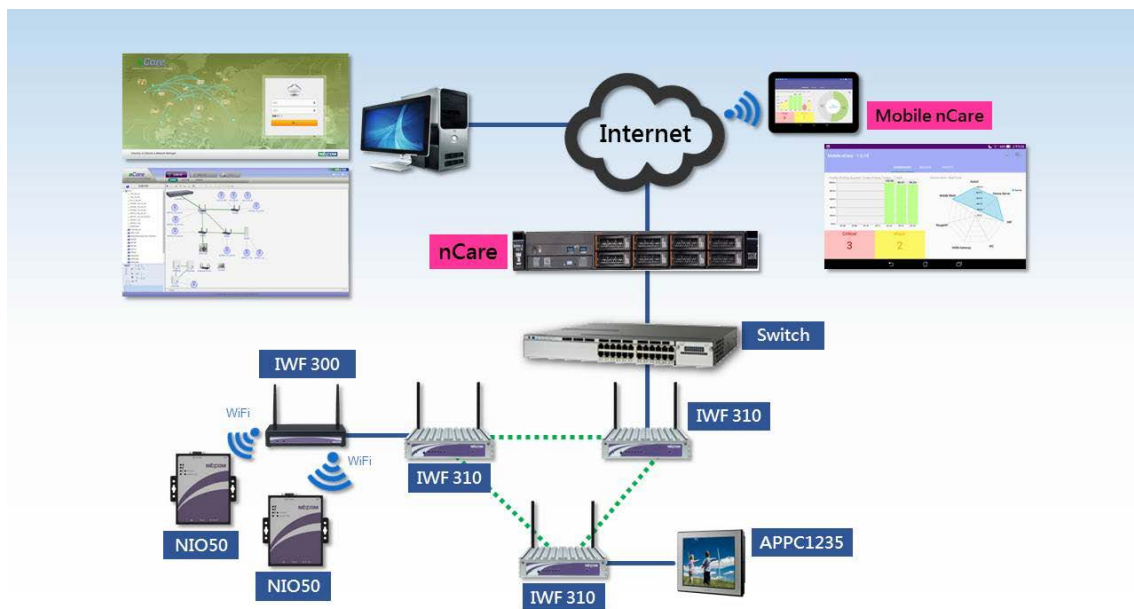


Figure 3 nCare User Scenario

## 4 Instruction for nCare Login

### 4.1 Procedures for Logging in

- (1) Log in the system browsers such as IE 11, Chrome or Firefox.



Figure 4 nCare Login Page

- (2) User may choose the interface language: *English, Simplified Chinese or Traditional Chinese.*

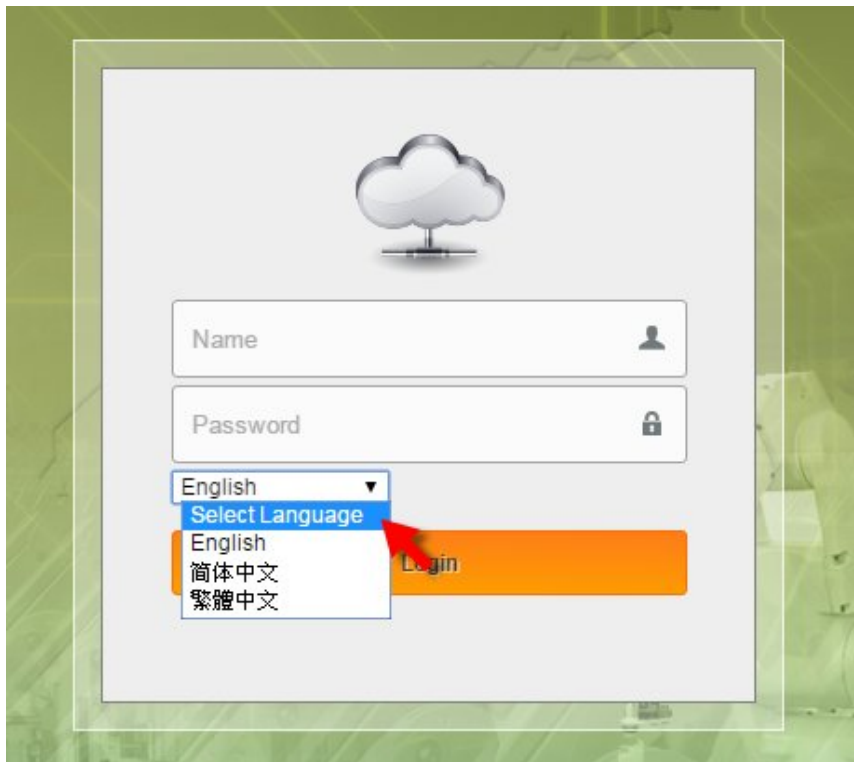


Figure 5 Interface Language Selection



- (3) Enter **Name** and **Password**. Please refer Chapter 5.1 User Management for setting procedures. Name and Password are both *admin* while logging in the first time. There will be an exclamation point appeared if the wrong information is entered.
- (4) When the user's password is entered incorrectly three times, the system automatically blocks this account. User needs to contact the system administrator to unlock it through the database operation.

The command is as follows:

- *Login to mysql server (default account/pass : root/admin)*
- *select cmsdb*
- *update userloginerror set valid=0*  
*or*  
*update userloginerror set valid=0 where username="admin"*

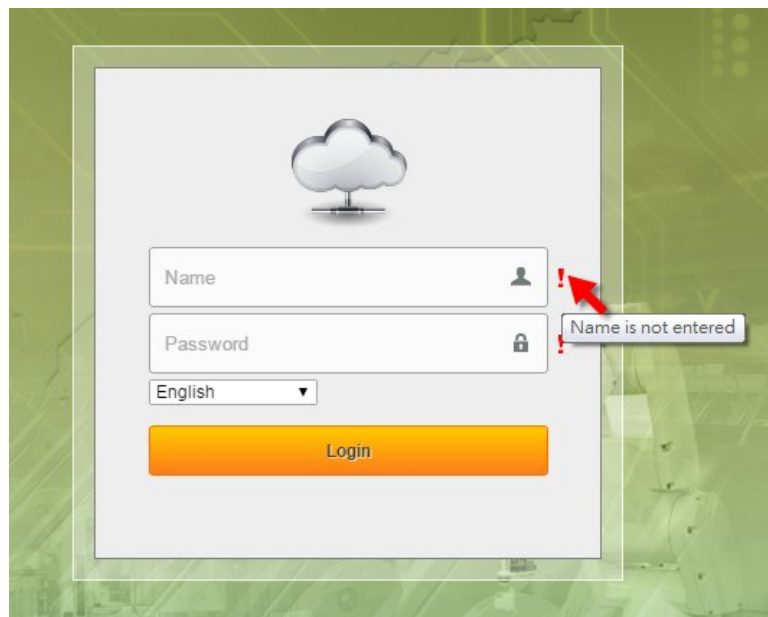


Figure 6 Error Message Notification

- (5) Click **Logout** to log out the system.

\* User may be automatically logged out if idling for a long time.

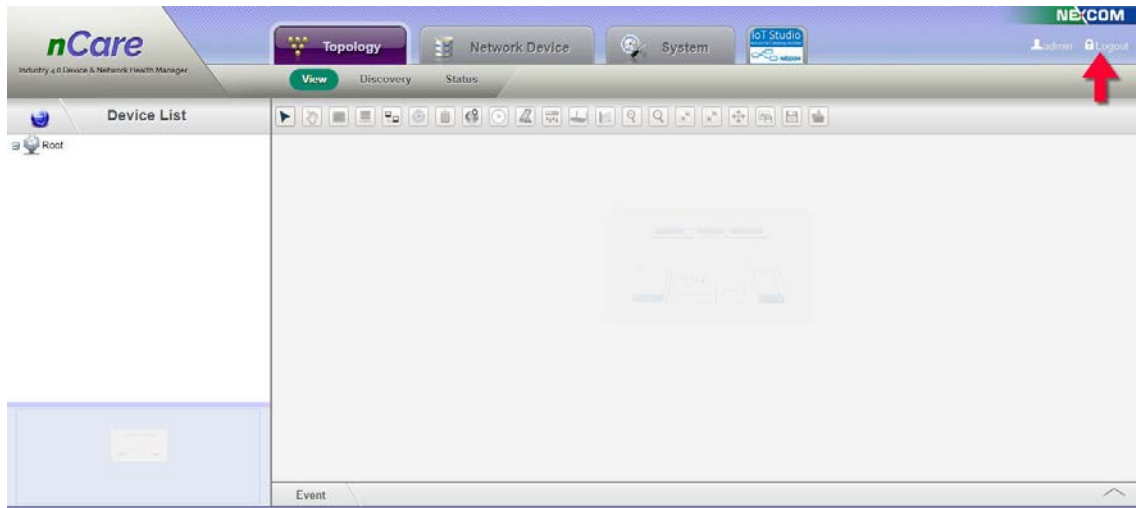


Figure 7 Logout from the System

## 5 Interface Illustration for nCare System

### 5.1 Users Management

#### 5.1.1 Introduction for Account Management

Enter the page of *System>Users* of nCare. Administrator may manage the users and set their authorities.

#### 5.1.2 Operation for Account Management

- (1) Click **Add** at the page of *Users>Account*, a **Create User Account** window will pop-up. Type in *User Name, Password, Confirm Password, Email, Mobile Phone number* and *Topology Group*.
- (2) The red star \* by the side of the frame indicates the information is required to enter.

Figure 8 Create User Account

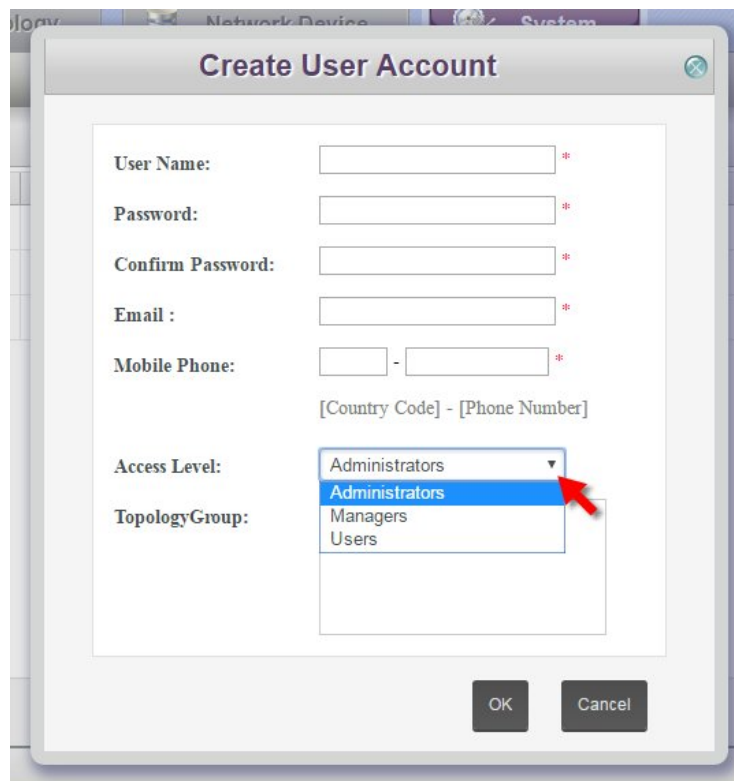
- (3) Choose Administrators, Managers or Users as its *Access Level*.

\* Administrators: Administrator may access all the monitoring, setting and managing functions, modifying user information and reset password.

(Please refer to Chapter 9.1.3 for more details)

\* **Managers:** Manager may have the same authority as Administrator besides the Account Management function. (Please refer to Chapter 0 for more details)

\* **Users:** User may only use partial functions. For example, there are no **System** function; only *Log* and *Usage* for **Network Device** function; only *View* and *Status* for **Topology** function with partial Topology icons. (Please refer to Chapter 9.1.1 for more details)



The image shows a 'Create User Account' dialog box with the following fields and options:

- User Name:  \*
- Password:  \*
- Confirm Password:  \*
- Email:  \*
- Mobile Phone:  -  \*  
[Country Code] - [Phone Number]
- Access Level:  (dropdown menu with options: Administrators, Managers, Users) \*
- TopologyGroup:

Buttons: OK, Cancel

Figure 9 Access Level

(4) If Users are selected as *Access Level*, please choose the Topology Group for them to view or manage. (Please refer to Chapter 6.6 for more details)

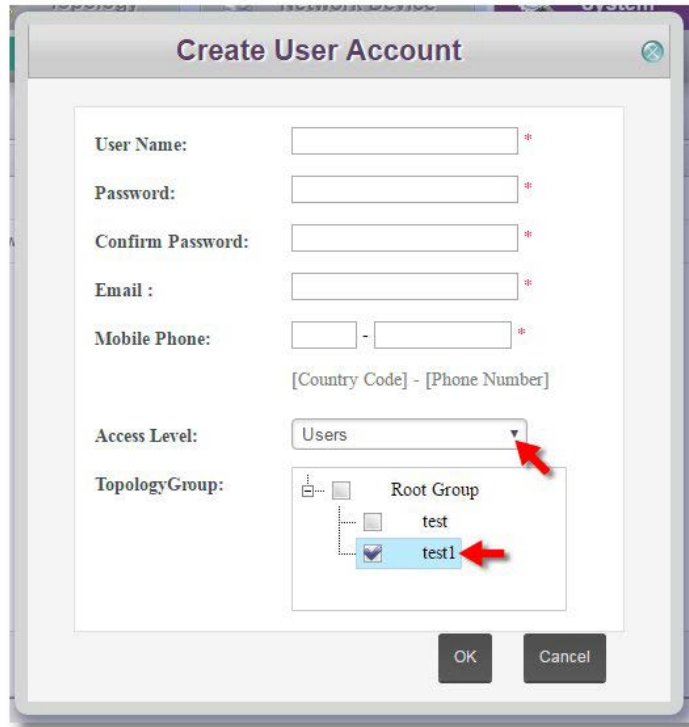


Figure 10 Topology Group Selections for Different Access Level

- (5) Click **OK** to add user account successfully. Or if there are invalid information entered, move the mouse to the exclamation point to see the error message.

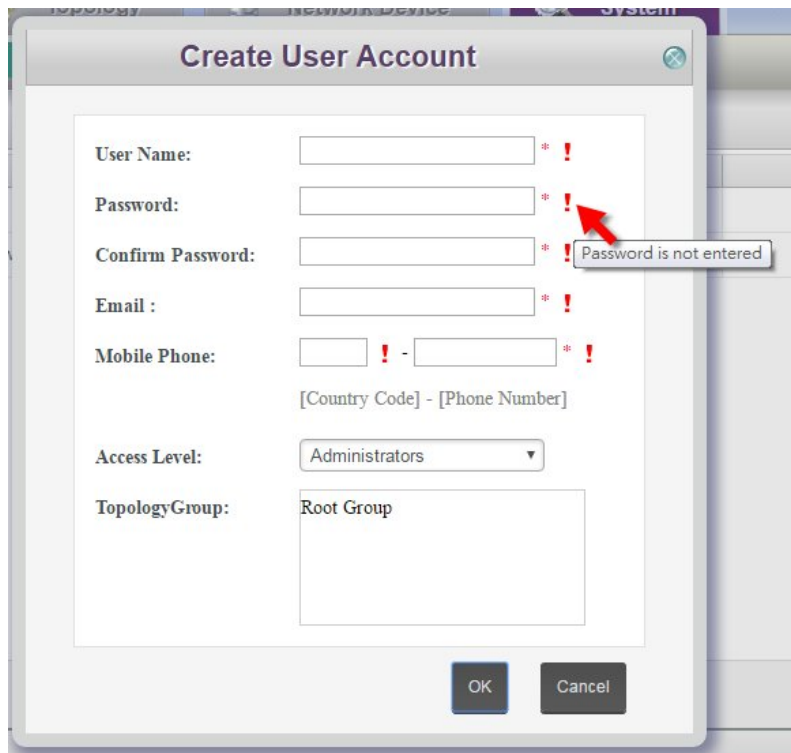


Figure 11 Error Message for Create User Account

(6) The added users can be Modified or Deleted.

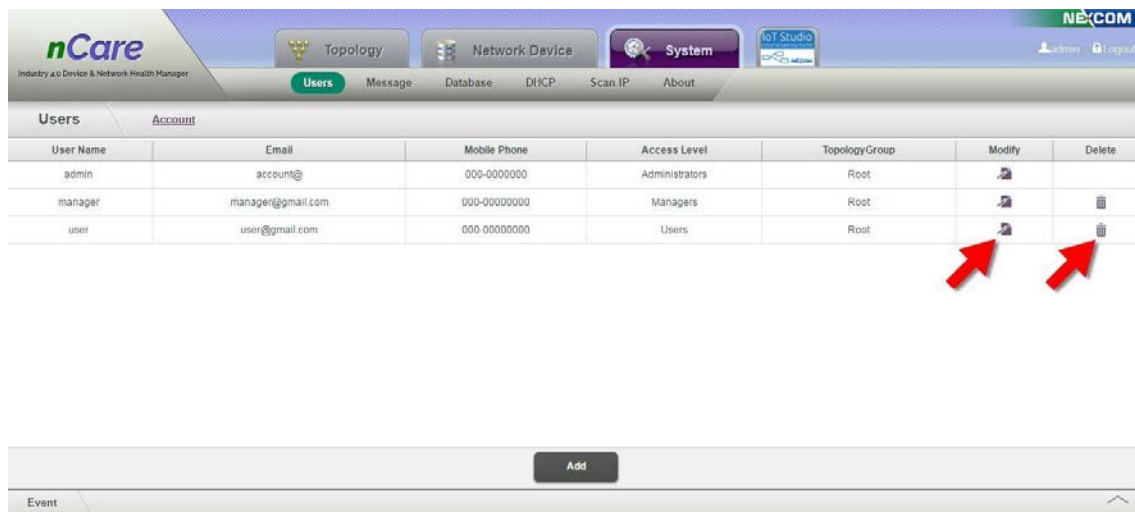


Figure 12 User List with Modify and Delete icons.

## 5.2 Message Management

### 5.2.1 Introduction for Message Management

If there are alarms of device or the data flow exceed certain number, an alarm message will be sent by *E-mail*, *SMS*, *Social Media* or *Inform User*. The Device alarm can be sent to default Administrator, and the receiver for Data Flow alarm can be chosen. (Please refer to Chapter 7.1.2.2 for more details)

The *E-mail*, *SMS* and *Social Media* functions can be test on **Message** page to make sure alarm functions are working normally.

### 5.2.2 Operation for Message Management

#### 5.2.2.1 E-mail

- (1) To test this function, test mail should be linked by mail server of the corporation. Select ExchangeServer from the pull-down menu, and *SMTP Host*, *SMTP Port*, *Account* and *Password* of mail server should be entered.
- (2) Click **Apply**.
- (3) Enter the e-mail address on *E-mail to* box, then click **Test**.

- (4) Go to the mail box to check if the test mail is received.

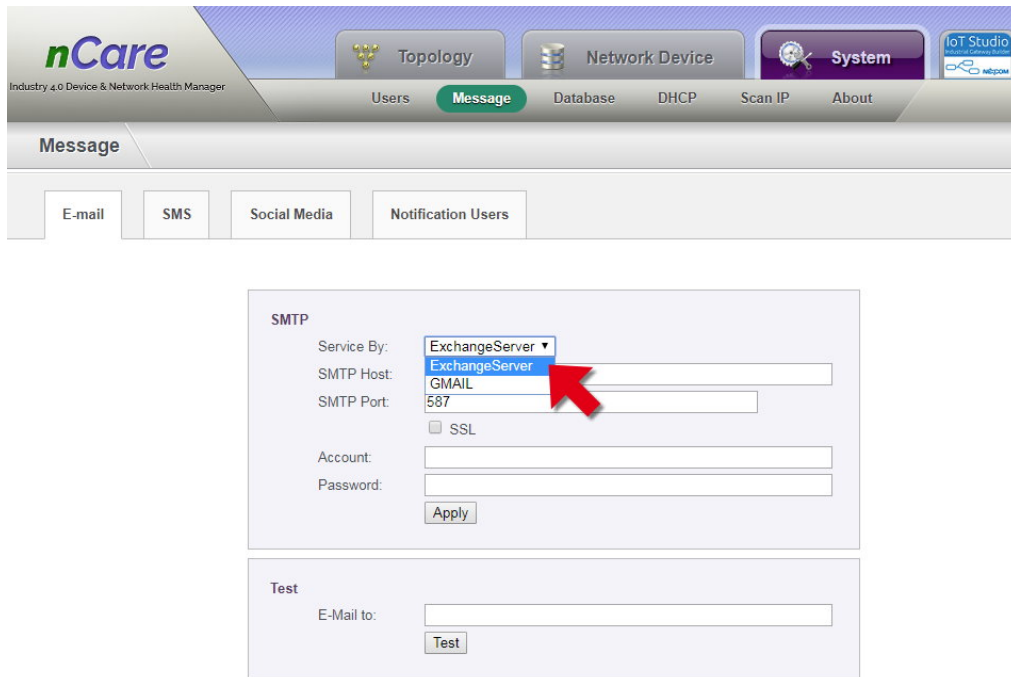


Figure 13 E-mail Test

### 5.2.2.2SMS

- (1) To test this function, internal information of corporation such as *Service by, API ID, Username* and *Password* should be entered.
- (2) Click **Apply**.

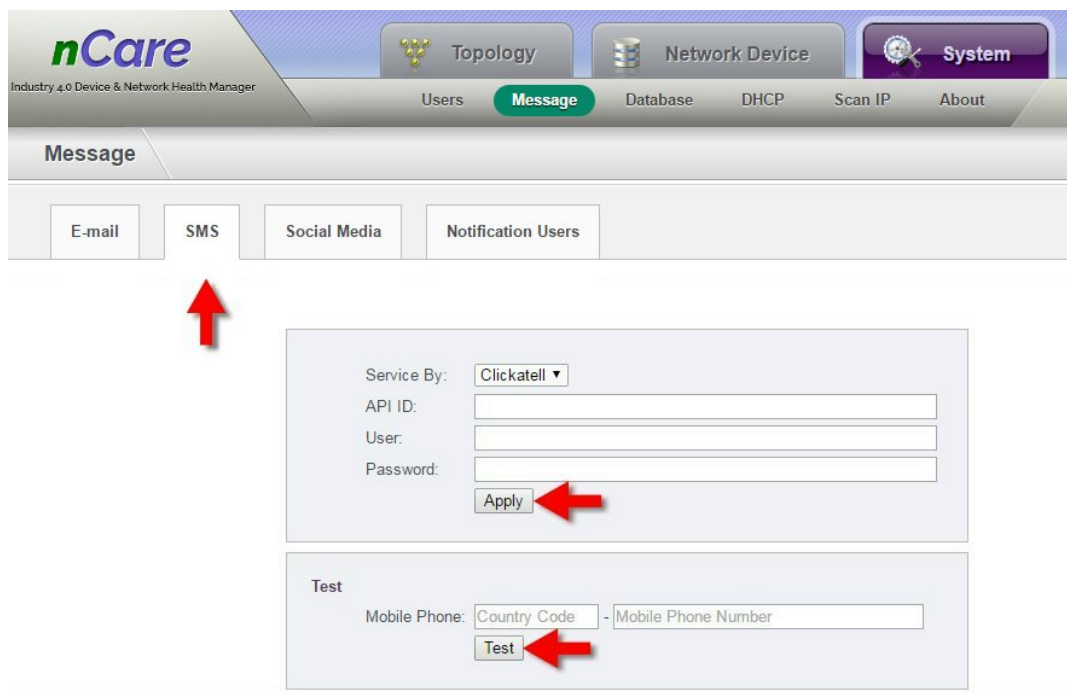


Figure 14 SMS Test

- (3) Enter *Country Code* and *Mobile Phone Number*, then click **Test**.
- (4) Check the mobile phone to see if the test SMS is received.

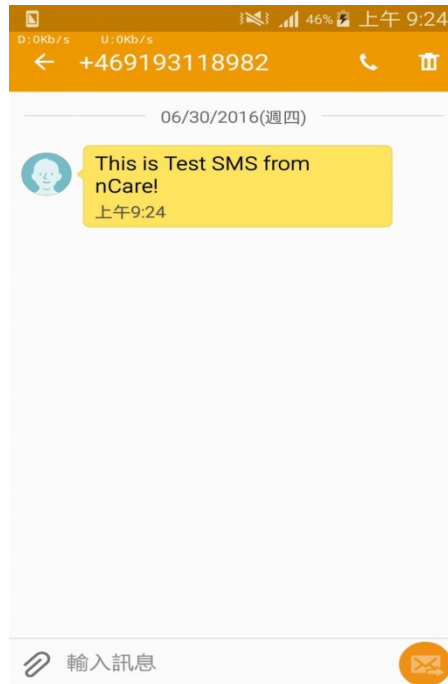


Figure 15 SMS Test Message

### 5.2.2.3 Social Media

The alarm message can also be sent to *WeChat* and *Twitter*. The setting procedures are list as follows:

#### (1) WeChat

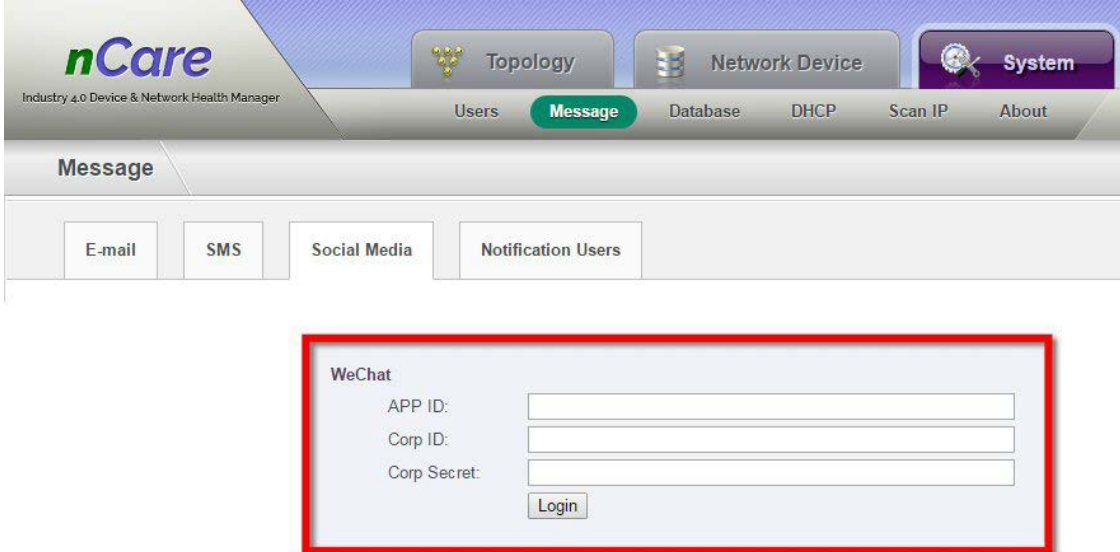
- a. Apply personal WeChat account
- b. Follow 上海兢汉信息科技
- c. Two targets, nCare and 企业小助手 will be shown.



Figure 16 WeChat Page



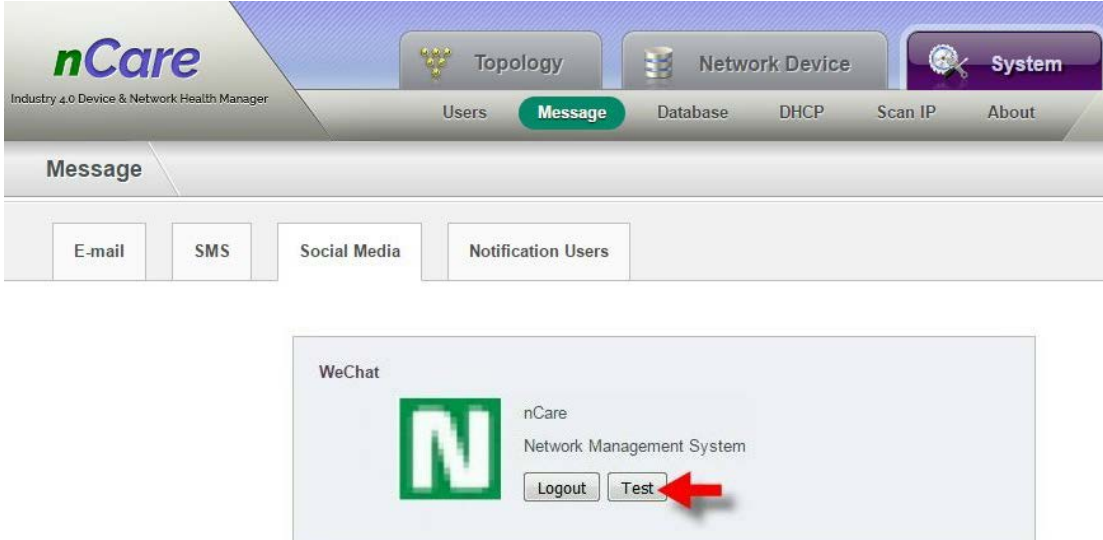
- d. Apply *APP ID*, *Corp ID* and *Corp Secret* from 上海兢汉信息科技
- e. Enter the information on nCare, then click **Login**.



The screenshot shows the nCare interface with the 'Message' tab selected. Under the 'Message' tab, there are four sub-tabs: 'E-mail', 'SMS', 'Social Media', and 'Notification Users'. The 'WeChat' section is highlighted with a red border. It contains three input fields for 'APP ID', 'Corp ID', and 'Corp Secret', and a 'Login' button.

Figure 17 WeChat Setting Information

- f. A nCare logo will be generated after login. Click **Test** for sending a message for the WeChat account.



The screenshot shows the nCare interface with the 'Message' tab selected. Under the 'Message' tab, there are four sub-tabs: 'E-mail', 'SMS', 'Social Media', and 'Notification Users'. The 'WeChat' section is highlighted with a red border. It contains a green 'N' logo, the text 'nCare Network Management System', and two buttons: 'Logout' and 'Test'. A red arrow points to the 'Test' button.

Figure 18 WeChat Message Test

- g. nCare is then being followed, indicated by a red dot. Click the icon for test message.

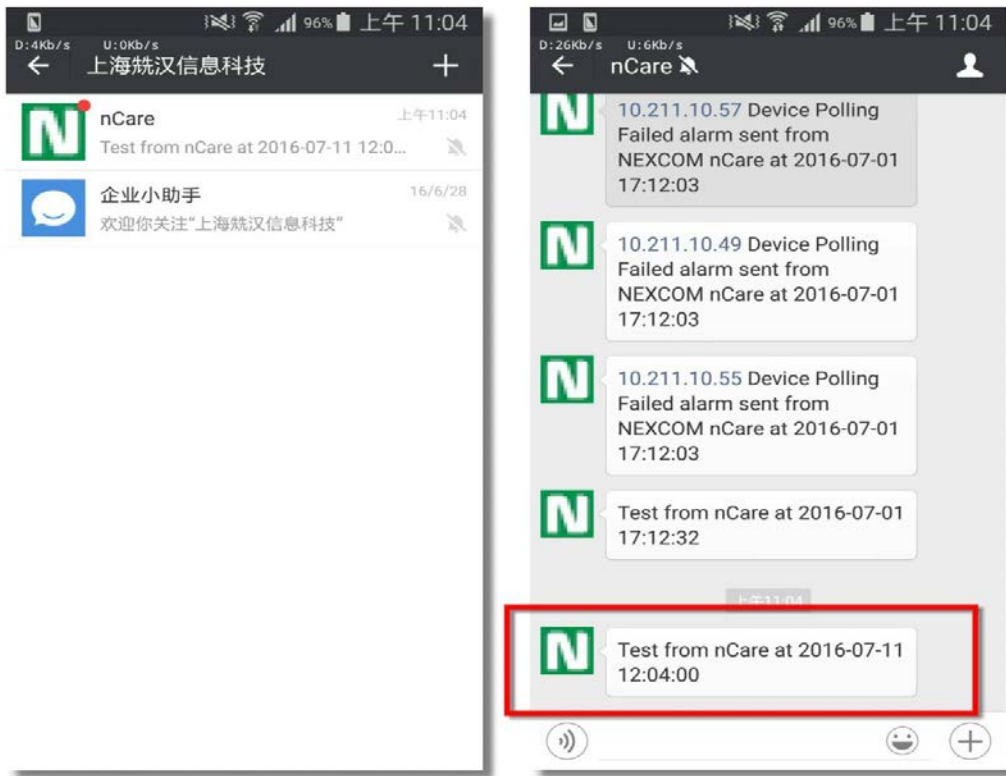


Figure 19 Test Message List of WeChat Target

(2) Twitter:

- a. Apply personal Twitter account.
- b. Create New App on Twitter Apps and get the **Consumer Key** and related **Consumer Secret**.
- c. Enter the information on nCare system page. (Please refer to the Appendix 1 for details)

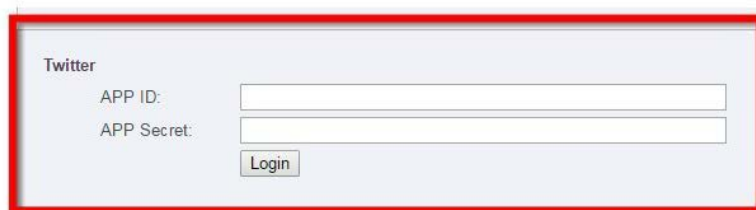
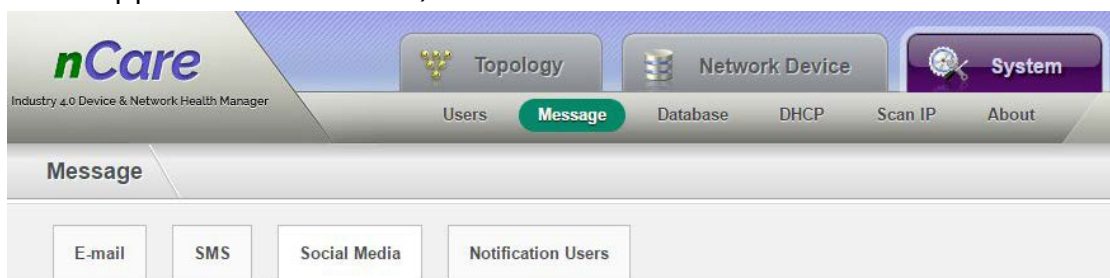


Figure 20 Enter Twitter APP ID and APP Secret

- d. Click **Login** and enter authorization code to complete login procedure.
- e. Click **Test** for sending test message to Twitter

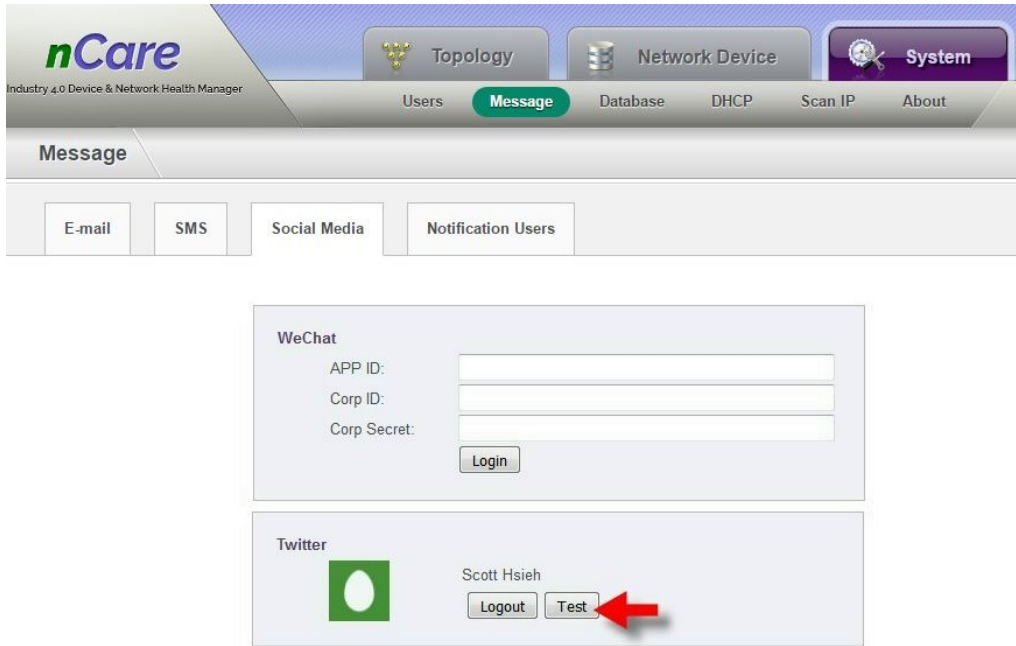


Figure 21 Sending Test Message to Twitter

- f. The test message will be shown on Twitter.

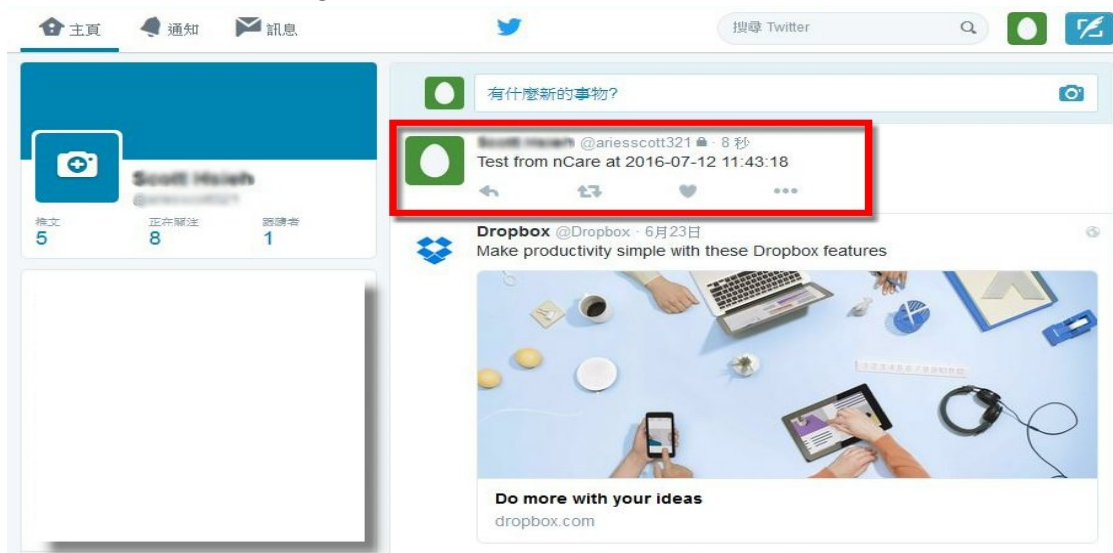


Figure 22 Twitter Test Message Successfully Sent

#### 5.2.2.4 Notification Users

The receiver of Email and SMS for Critical and Major alert can be set by nCare.

- (1) Choose the *Severity* and *Notification Type* from the pull-down menu.
- (2) Choose one or more users for receiving notification.

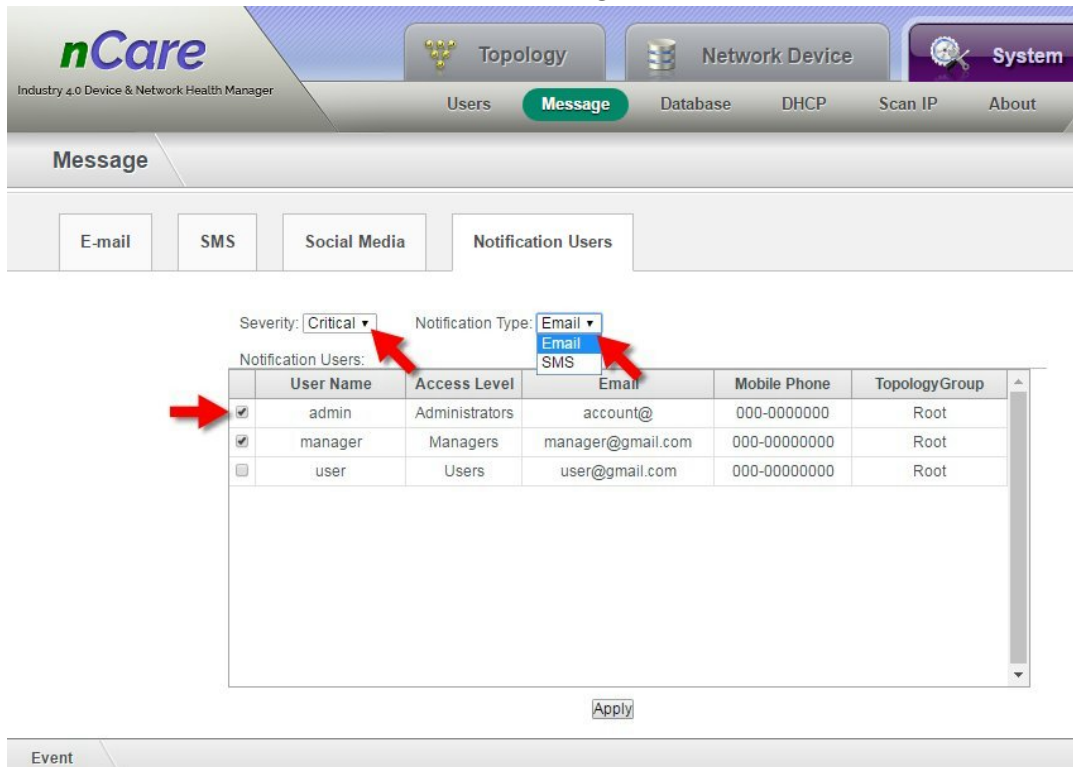


Figure 23 Severity, Notification Type and Receiver Setting

- (3) Click **Apply** to complete setting.

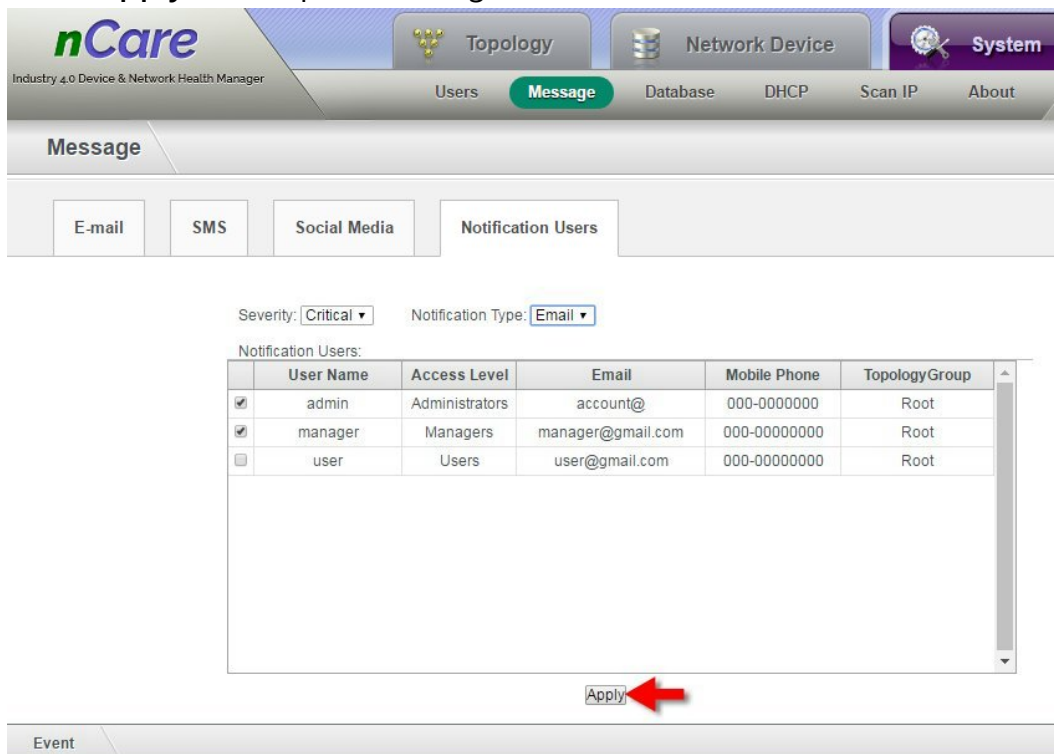


Figure 24 Notification Users Setting

## 5.3 Database Management

### 5.3.1 Introduction for Database Management

Abnormal event such as polling fail or disconnection can be recorded at nCare database. The storage cycle and maximum number of event can be set. All the records can be cleared.

### 5.3.2 Operation for Database Management

- (1) Check *Maximum reserved event period*. Enter number between 1~365 then click **Apply**. (If 180 is entered, all records stored for more than 180 days will be cleared.)
- (2) Check *Maximum number of events*. Enter number between 10000~1000000 then click **Apply**. (If 1000000 is entered, all old records that stored over 1000000 items will be cleared)
- (3) Either 2 boxes can be checked or not. If 2 boxes are both not checked, all event records will be saved continuously.
- (4) Click **Delete All Events** to clear all event records.

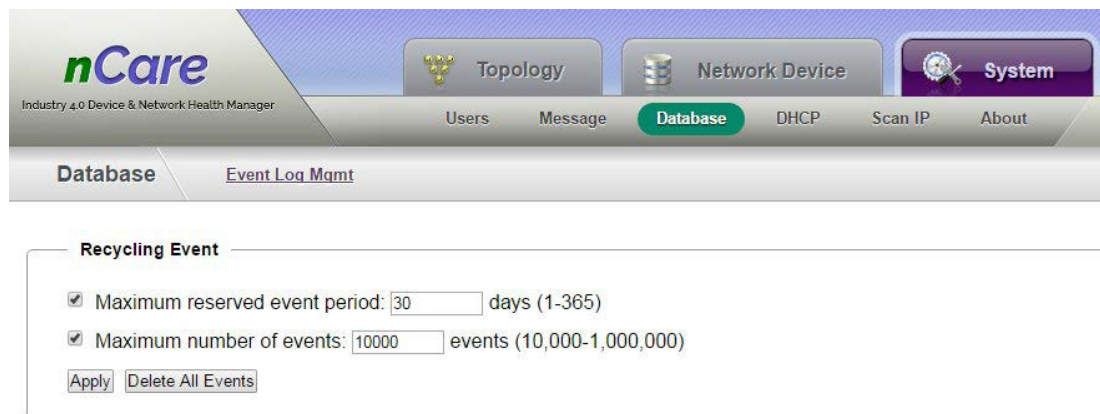


Figure 25 Database Setting

## 5.4 DHCP Management

### 5.4.1 Introduction for DHCP Management

The IP address of devices can be set by default built-in DHCP function. Manager may deploy multiple devices into system despite that setting IP address, subnet mask and gateway one-by-one.

### 5.4.2 Operation for DHCP Management

#### 5.4.2.1 DHCP Setting

- (1) Connect the device with nCare for IP setting.
- (2) Enter the webpage of device and go to *Network>Interfaces*.

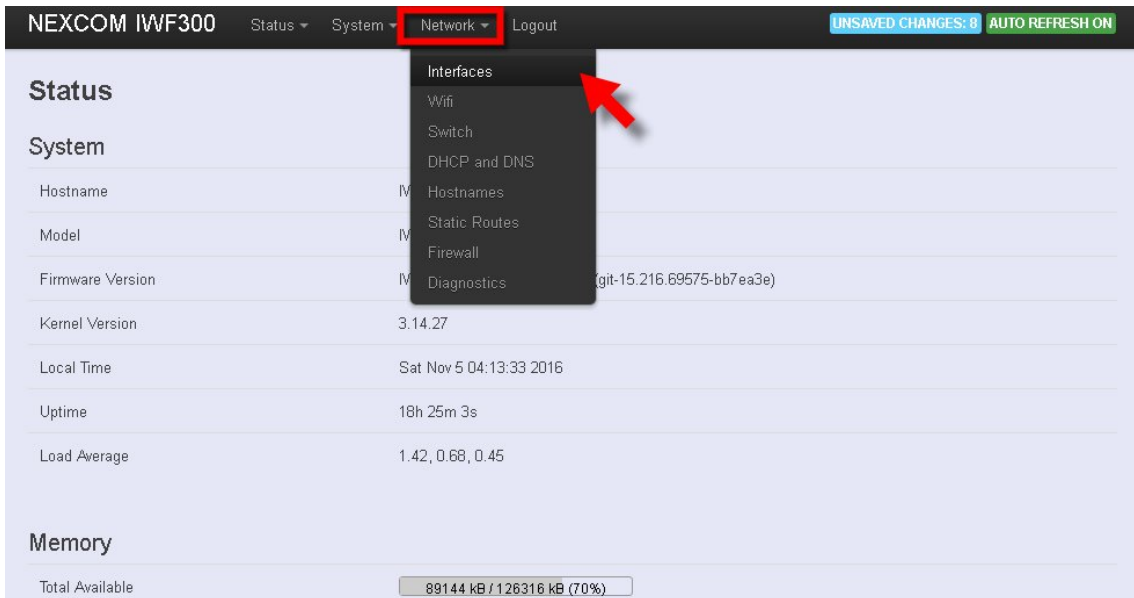


Figure 26 Device Setting Webpage

- (3) Click **Edit** of LAN or WAN to enter their setting page.

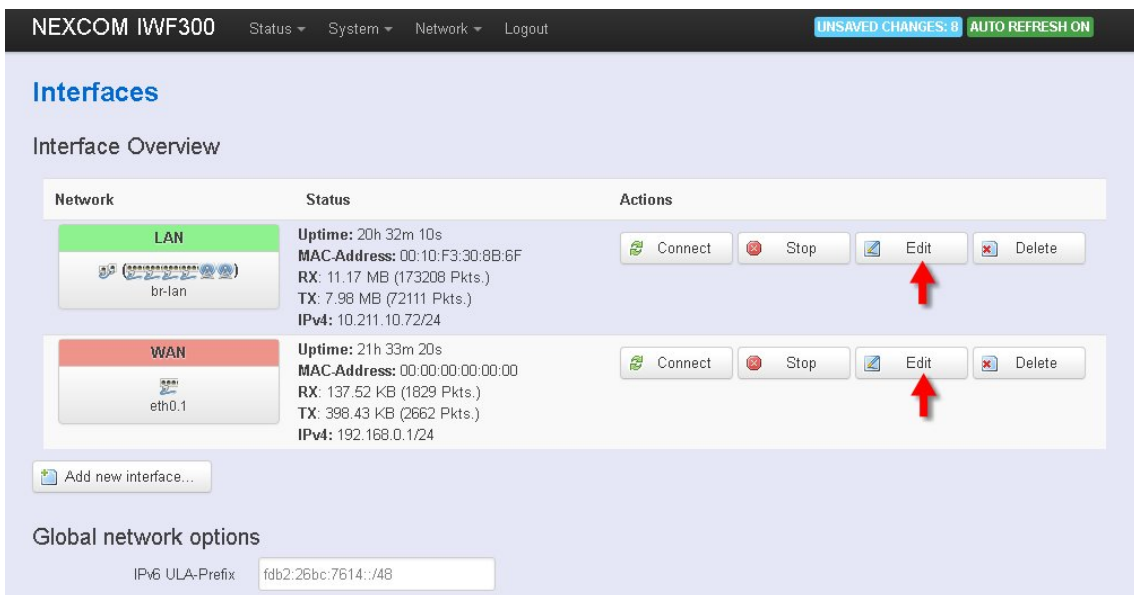


Figure 27 WAN or LAN Setting Page Selection



- Enter the setting page, choose DHCP client as Protocol from the pull-down menu.

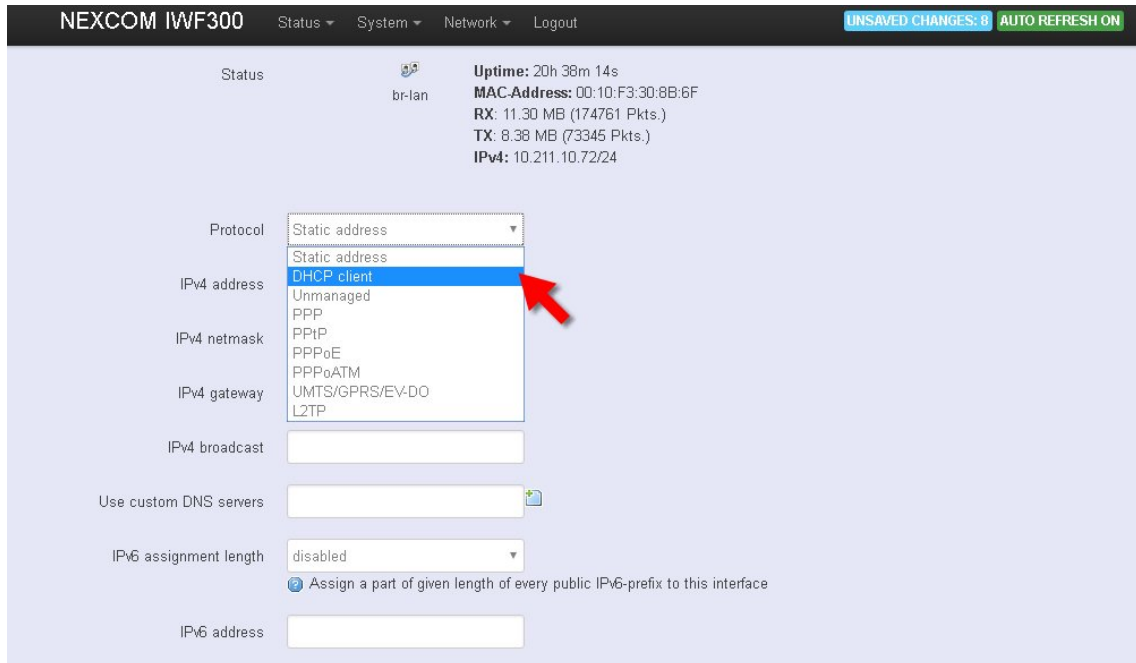


Figure 28 WAN or LAN Setting Page Selection

- Enter the name for *Hostname to send when requesting DHCP* at **Common Configuration** page.
- Click **Save & Apply** to complete setting.

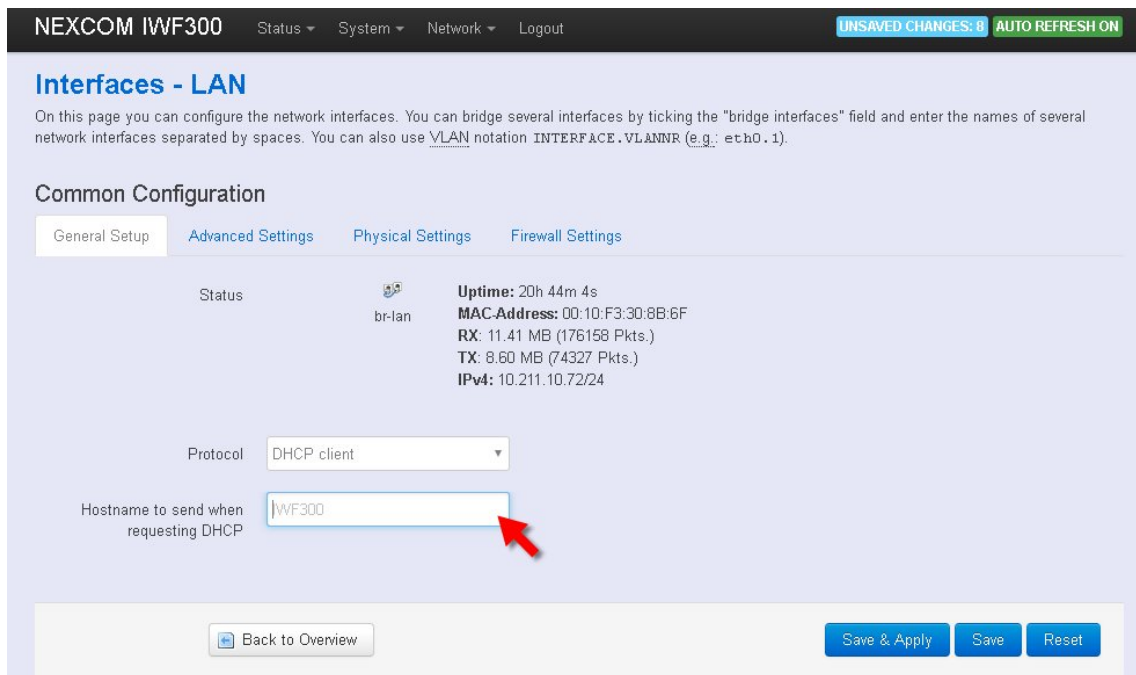


Figure 29 Blank for “Hostname to send when requesting DHCP”

- (7) DHCP devices should be set by going through all the procedures from (1) to (6).
- (8) Go to *System > DHCP > Setting* page of nCare.
- (9) Check "Enable."
- (10) Enter the related information.
- (11) Click **Apply** to complete DHCP setting.

\* The MAC Address can also be added with Client IP

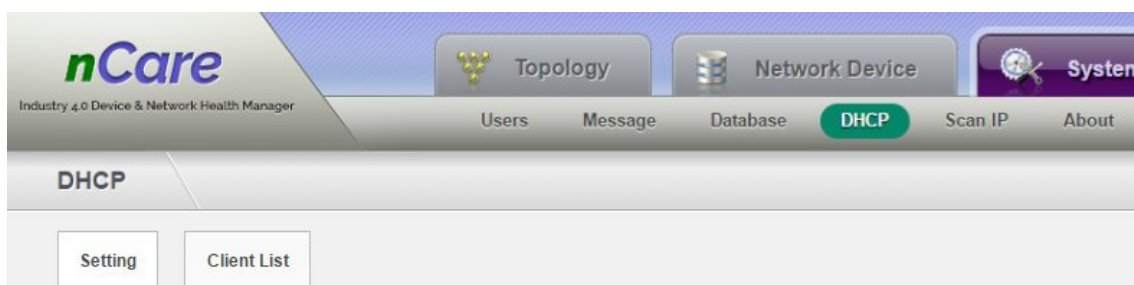
The screenshot shows the DHCP Setting form. The "Enable:" checkbox is checked, and a red arrow points to it. Below the checkbox are several input fields for network configuration: "IP Pool:" (10, 211, 10, 70, 80), "Subnet Mask:" (255, 255, 255, 0), "Default Gateway:" (10, 211, 10, 254), "DNS Server 1:" (168, 95, 1, 1), "DNS Server 2:" (empty), and "Lease Time (s):" (empty). An "Apply" button is located at the bottom of the form.

Figure 30 DHCP Enabling

#### 5.4.2.2 DHCP Client List

Go to *System > DHCP > Client List* page, a list of DHCP clients can all be shown.



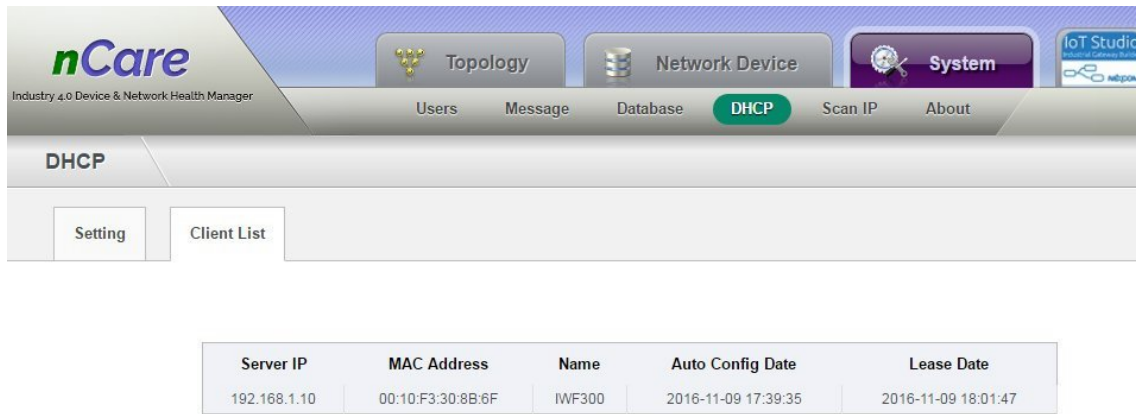


Figure 31 DHCP Client List

## 5.5 Scan IP

### 5.5.1 Introduction for Scan IP

Administrator may check if the IP address is available by **Scan IP** function.

### 5.5.2 Operation for Scan IP

- (1) Enter *Start IP Address* and *End IP Address*.
- (2) Click "Scan" .

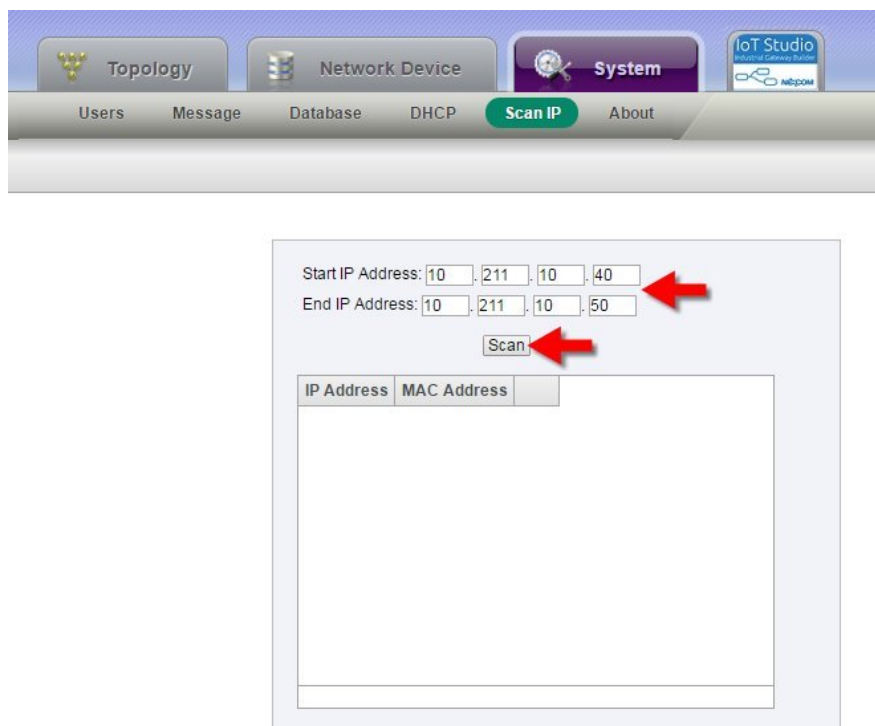


Figure 32 Enter IP Range

- (3) IP address and MAC address used can be shown on the list.

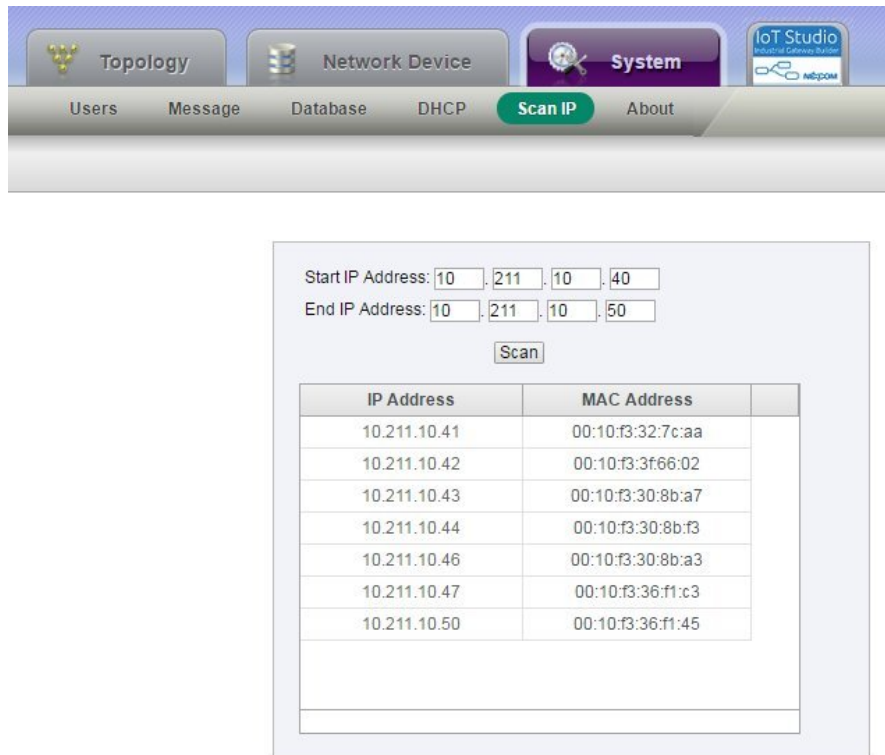


Figure 33 IP Address and MAC Address List

## 5.6 About

### 5.6.1 Introduction for License

Enter *System>About* page. The *Model, Status of Expiration Date, Maximum Number of Devices, Current Number of Device* and *Version* can be seen.

- (1) The license for trial version of nCare is determined by system instead of by installation time.
- (2) For running trail version of nCare, every 24 hours use implies one day authorization.

### 5.6.2 Operation for License

- (1) There are two Licenses, trial version (for 30 days) and perpetual version (permanent use).

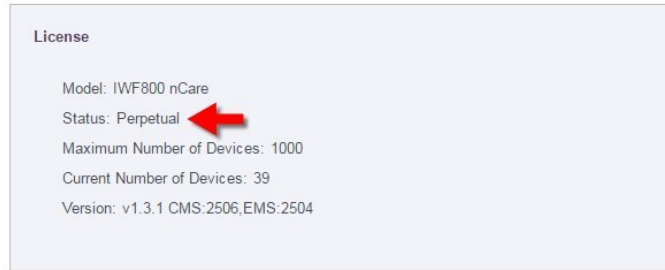
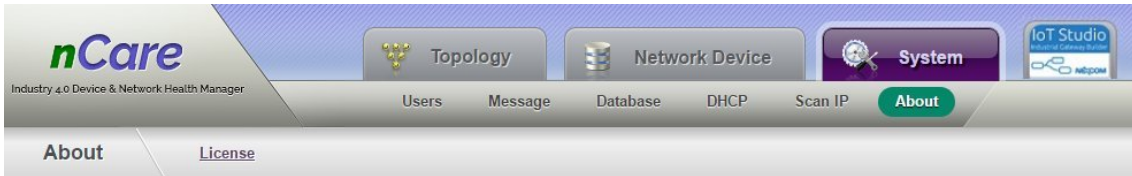


Figure 34 Status for Perpetual Version

(2) The expiration days for trial version will be shown on *Status*.

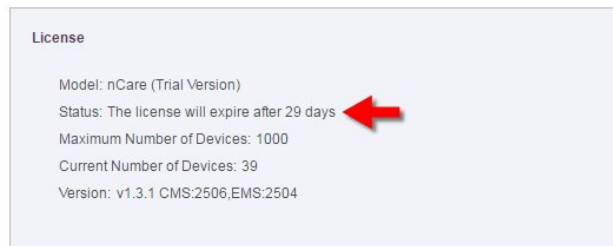
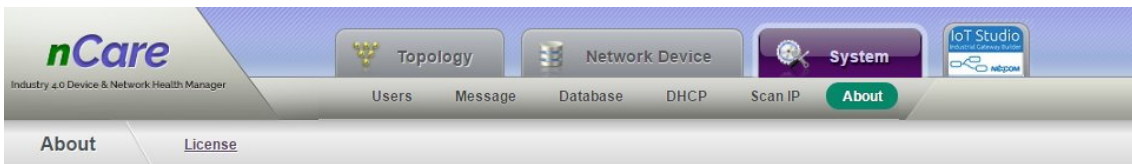


Figure 35 Status for Trial Version

(3) If the system will expire in 3 days, there is a pop-up window to inform user when logging-in.

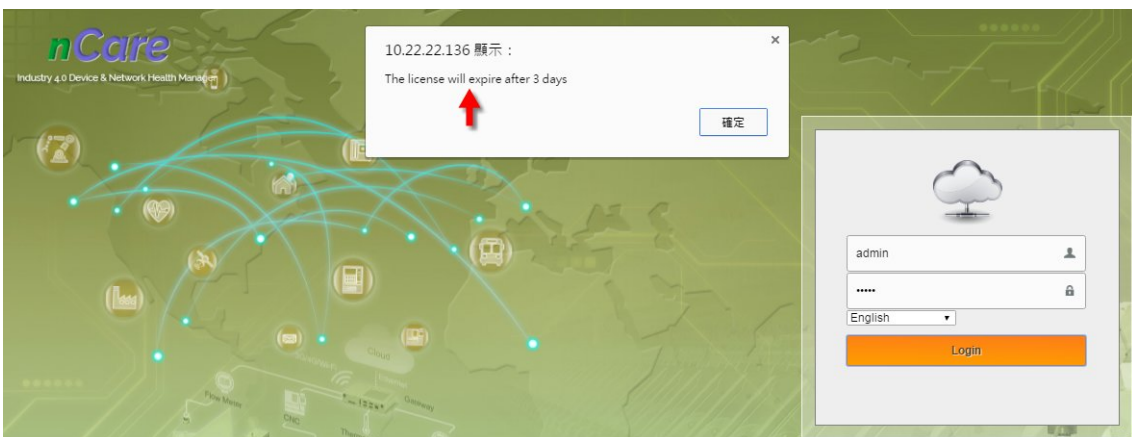


Figure 36 Pop-up Window for Informing Expiration Days

- (4) If the license is expired, user may not login. And there is a pop-up window to inform user.

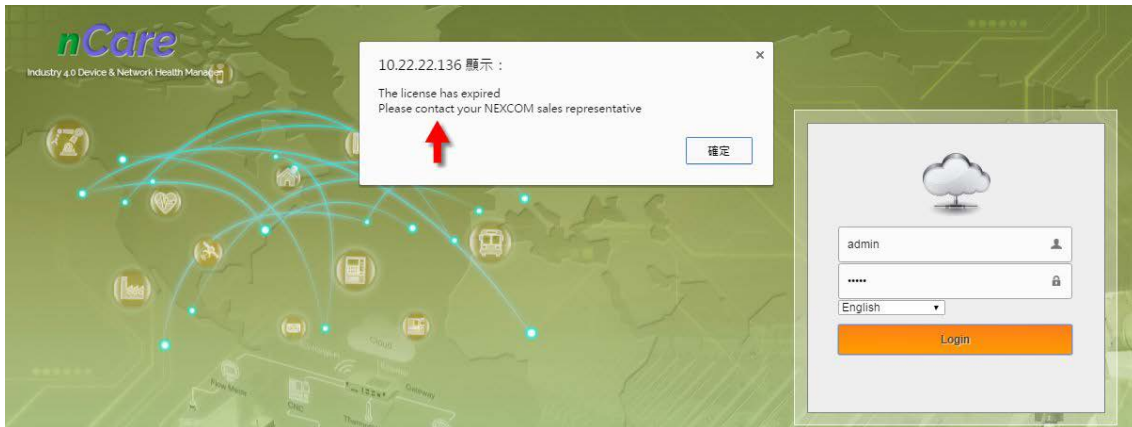


Figure 37 License Expired Inform

## 6 Introduction for nCare Network Device Setting Interface

### 6.1 Functions for Network Device Management

There are *Device List*, *Config Backup*, *Config Restore*, *Fw Upgrade* and *Device Provision* functions for Network Device Management.

#### 6.1.1 Introduction for Device List

The devices can be added, modified or deleted on *Device List* page. Information such as *Device Name*, *IP Address* and *SSID* are listed. User may also enter device setting page to change setting or reset the device.

#### 6.1.2 Operation for Device List

##### 6.1.2.1 Device Check

- (1) Different kinds of Device Type are list at the left. Click on the Type to check for the related information of devices.

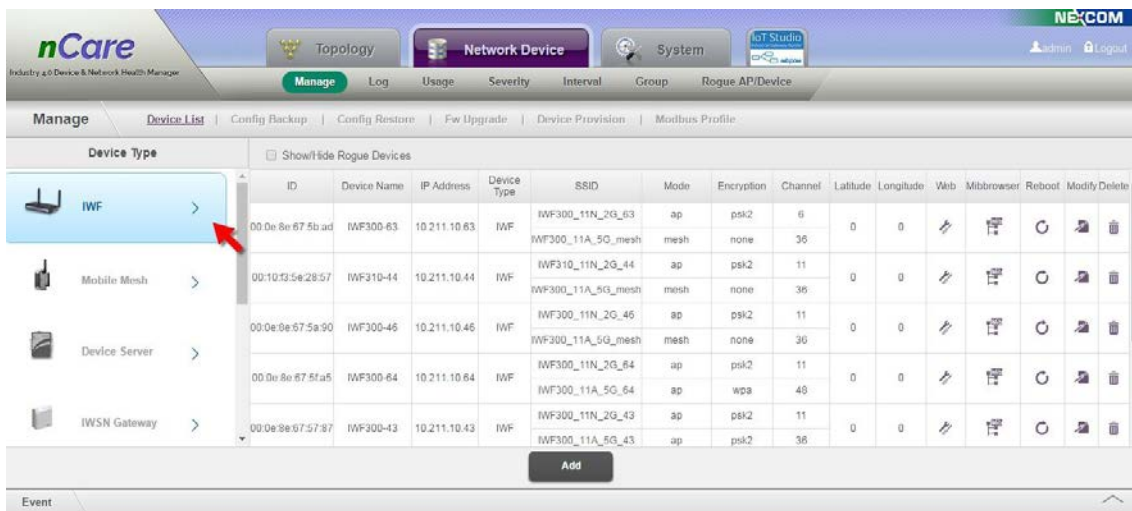



Figure 38 Device List that Sorting by Device Type

- (2) Check "Show/Hide Rogue Devices" and there will be a  icon appeared at the side of device ID for rogue device.

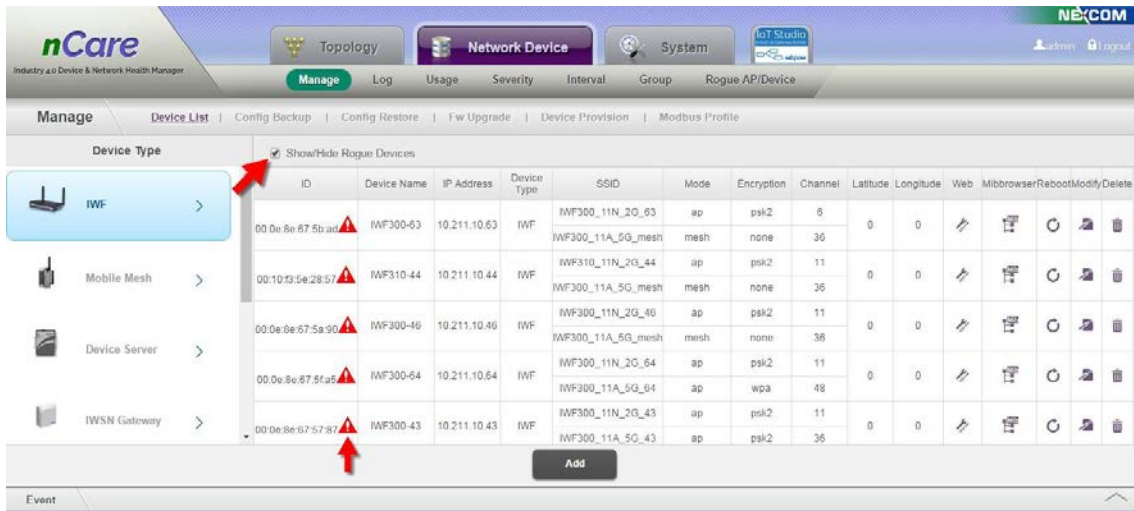


Figure 39 Show/Hide Rogue Devices

### 6.1.2.2 Add Device

- (1) Click **Add** icon to create new device.

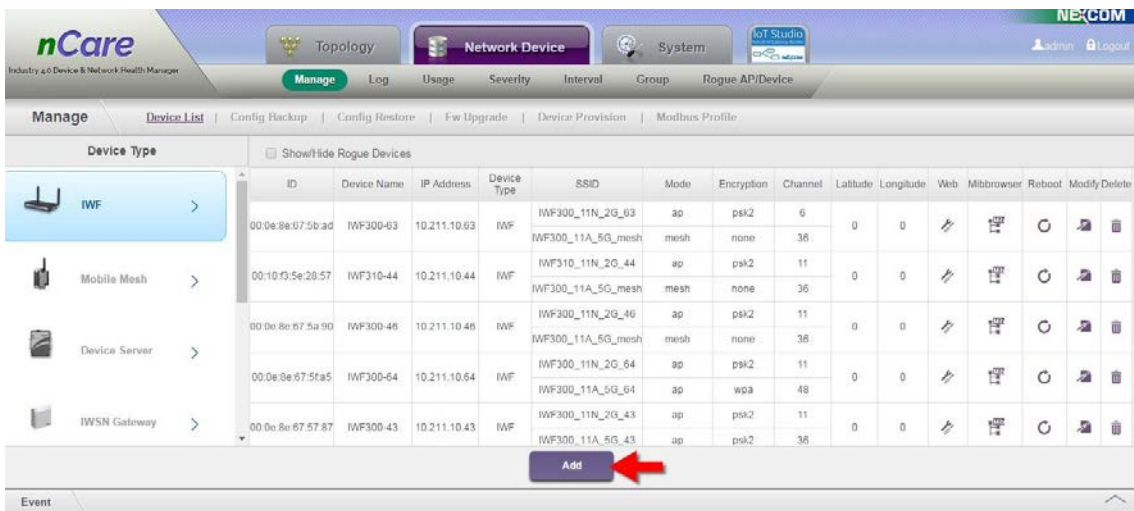


Figure 40 Add Device Icon

- (2) A **Create Device** window will pop-up. Enter the device information.
- (3) Default setting of *Read Community* and *Write Community* are public and private, respectively.
- (4) The red star \* by the side of the frame indicates the information is required to enter.

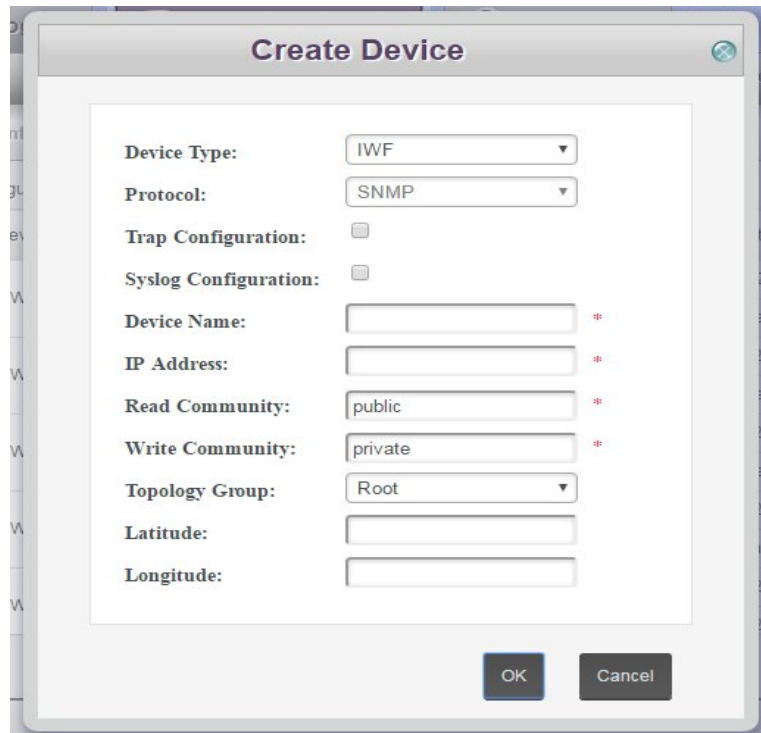


Figure 41 Information for Creating a new Device

(5) *Device Type* can be chosen from the pull-down menu.

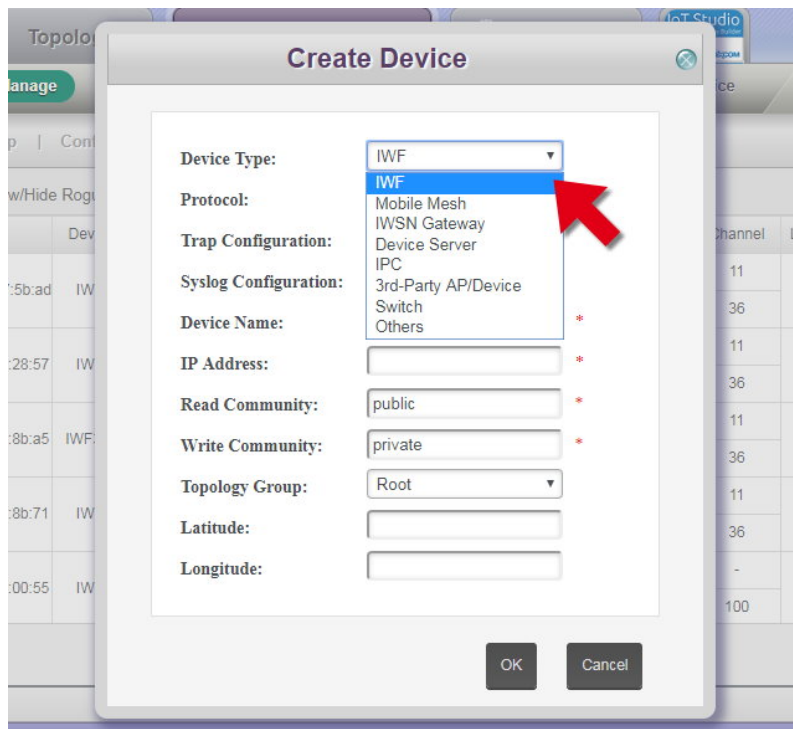
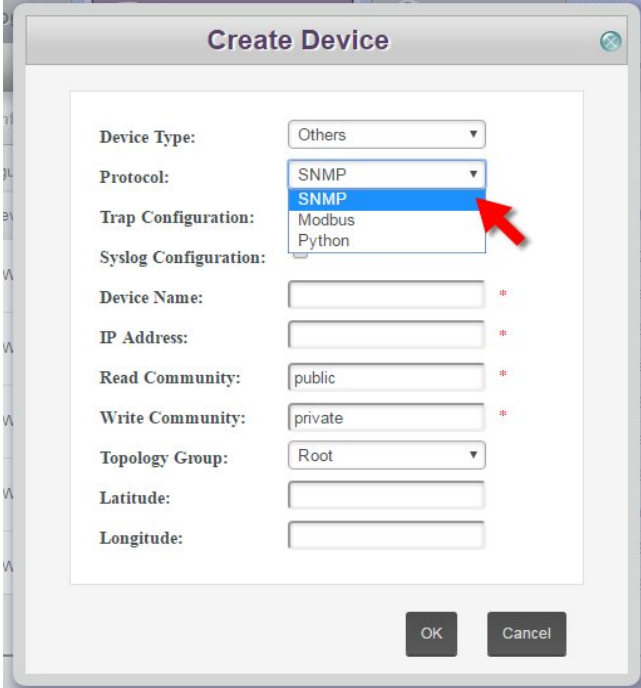


Figure 42 Device Type Selection



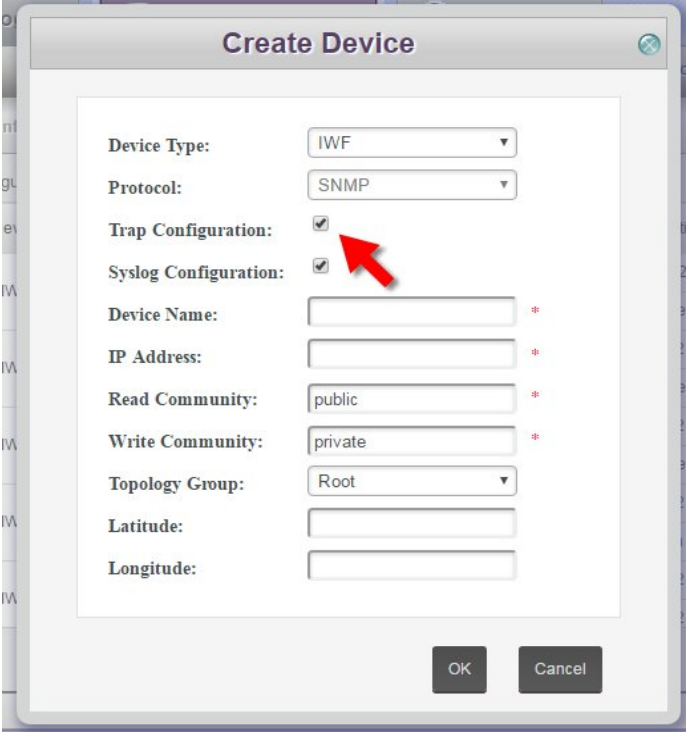
- (6) Choose the *Scan Protocol* with SNMP, Modbus or Python.



The screenshot shows the 'Create Device' dialog box. The 'Device Type' is set to 'Others'. The 'Protocol' dropdown menu is open, showing 'SNMP' selected and highlighted in blue. A red arrow points to the 'SNMP' option. Other fields include 'Trap Configuration' (empty), 'Syslog Configuration' (empty), 'Device Name' (empty), 'IP Address' (empty), 'Read Community' (public), 'Write Community' (private), 'Topology Group' (Root), 'Latitude' (empty), and 'Longitude' (empty). 'OK' and 'Cancel' buttons are at the bottom.

Figure 43 Scan Protocol Selection

- (7) Check "Trap Configuration" and "Syslog Configuration" to add related value for device. The device may send trap or variation to nCare.



The screenshot shows the 'Create Device' dialog box. The 'Device Type' is set to 'IWF'. The 'Protocol' is set to 'SNMP'. The 'Trap Configuration' and 'Syslog Configuration' checkboxes are checked. A red arrow points to the 'Syslog Configuration' checkbox. Other fields include 'Device Name' (empty), 'IP Address' (empty), 'Read Community' (public), 'Write Community' (private), 'Topology Group' (Root), 'Latitude' (empty), and 'Longitude' (empty). 'OK' and 'Cancel' buttons are at the bottom.

Figure 44 Scan Protocol Selection



- (8) Choose the Topology Group. Please refer to Chapter 6.6 for more detail.

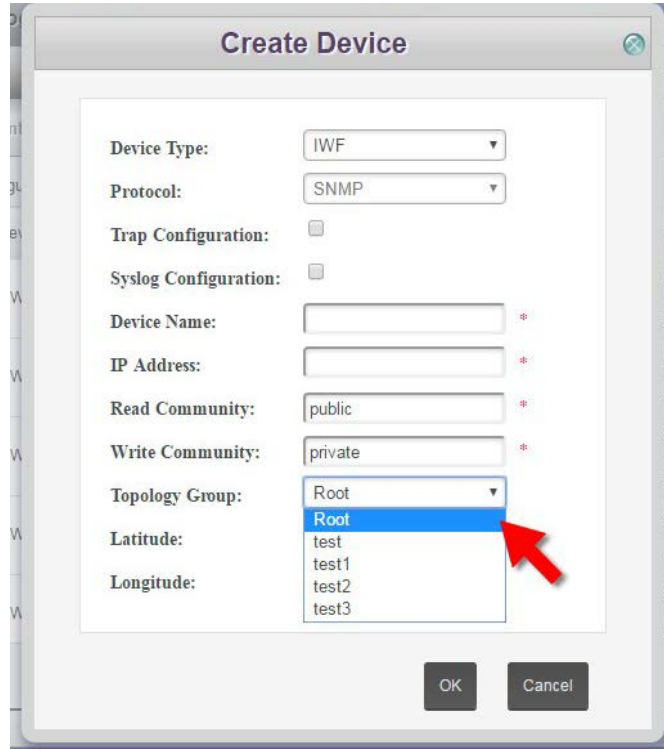



Figure 45 Topology Group Selection

### 6.1.2.3 Configuration Setting for Device

- (1) Configuration of device can be set with Device Type **IWF**, **Mobile Mesh**, **Device Server**, **IWSN Gateway** or **IWSN Gateway**.
- (2) Click  icon to enter device setting page.

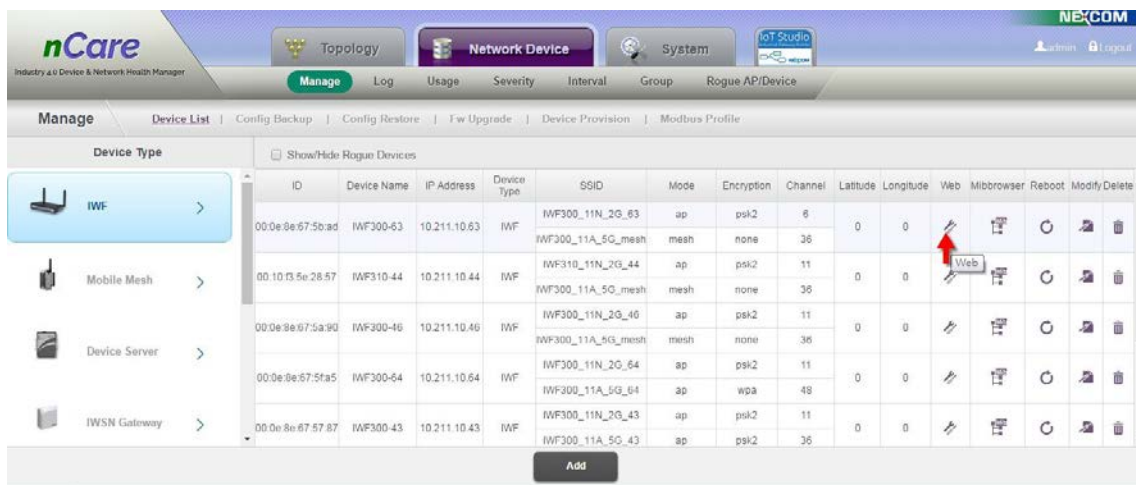


Figure 46 Device Configuration Setting Page Icon

(3) Configuration Setting: Enter *Username* and *Password* to login.

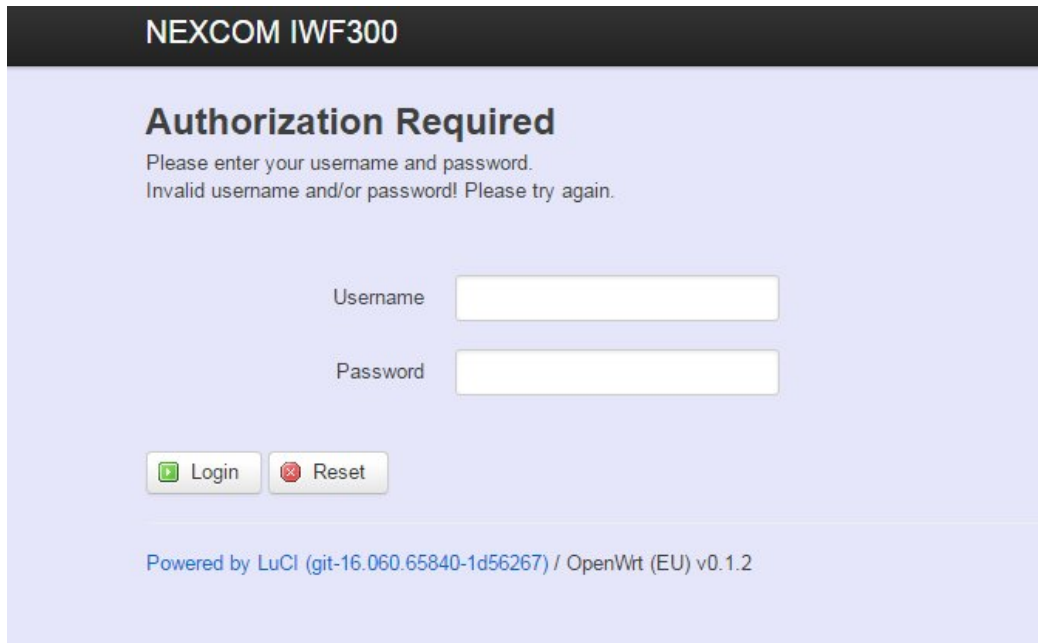



Figure 47 Configuration Setting Login Page

(4) Check the status of devices, and change configuration if needed.



Figure 48 Status of Device on Device Configuration Page

## 6.1.2.4 Device Setting by Mibbrowser

(1) Click MIB Browser icon  then a MIB Browser window will pop-out.

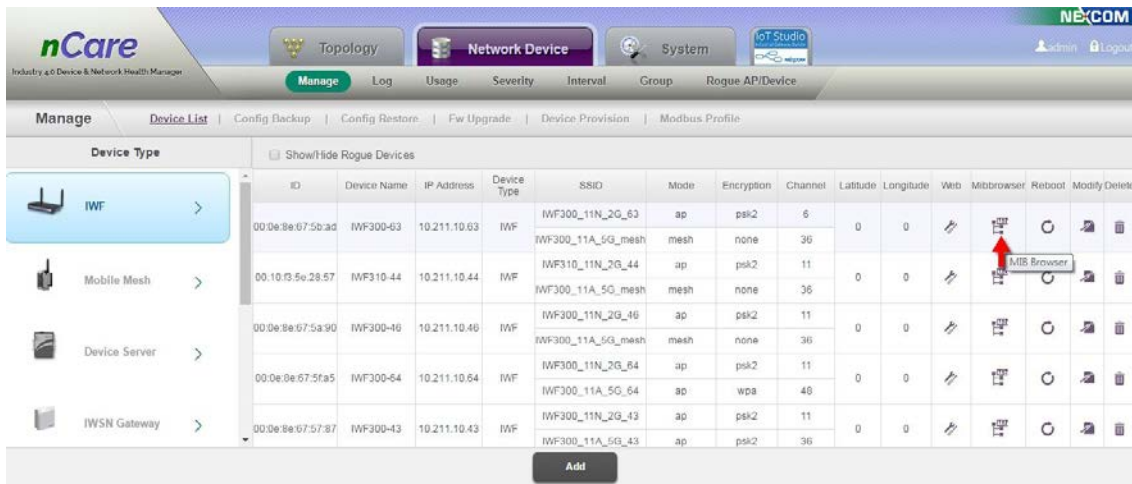


Figure 49 MIB Browser Icon

(2) Main functions of MIB Browser includes:



Import MIB File: User may import MIB file.



Get: Select node on the left then click **Get**, node information can be shown.



Set: Select node on the left then click **Set**, parameters of the node can be set.



Get Next: Click **Get Next** to jump to the next node.



Walk: Click the first node then click **Walk**, information of all nodes can be shown sequentially.



Table: Click the node then click **Table**, SNMP Table can be shown then.



Clear: Used for clear Query Result.

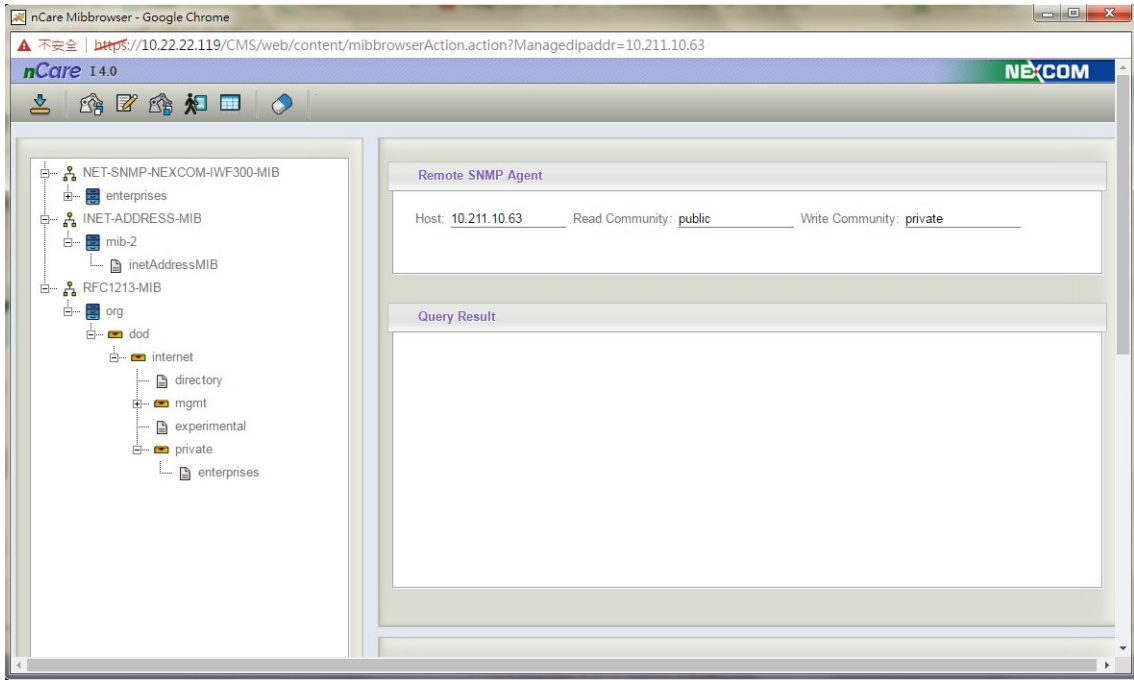



Figure 50 MIB Browser Setting Page

### 6.1.2.5 Device Reboot

Click  icon to reboot device.

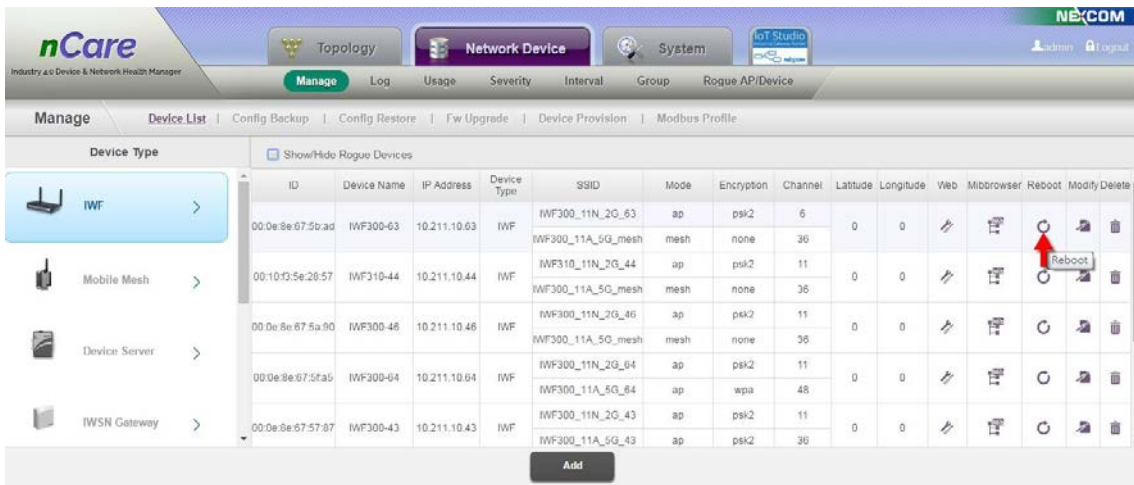




Figure 51 Device Reboot Icon

### 6.1.2.6 Device Modification

- (1) Click  icon to modify the information of device. (This icon cannot be used for **Mobile Mesh** type device, please click  icon to enter device webpage for modifying.)

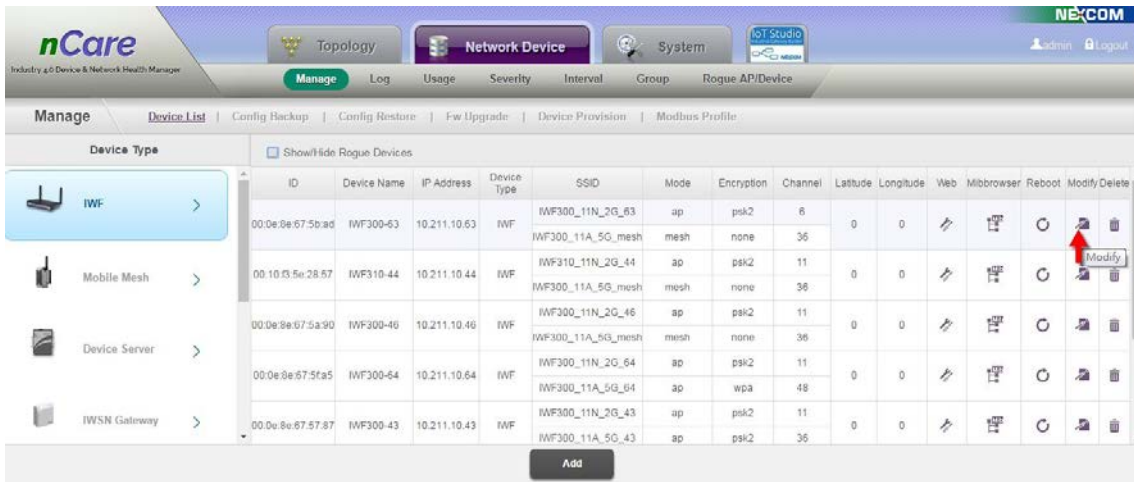



Figure 52 Device Modification Icon

- (2) With **IWF Device Type**, click  icon to modify the information of device. There are two extra labels, **Wlan** and **Vlan** for setting. There are information such as *WifiRadio*, *Operating Frequency* and *Wireless Security* can be filled.

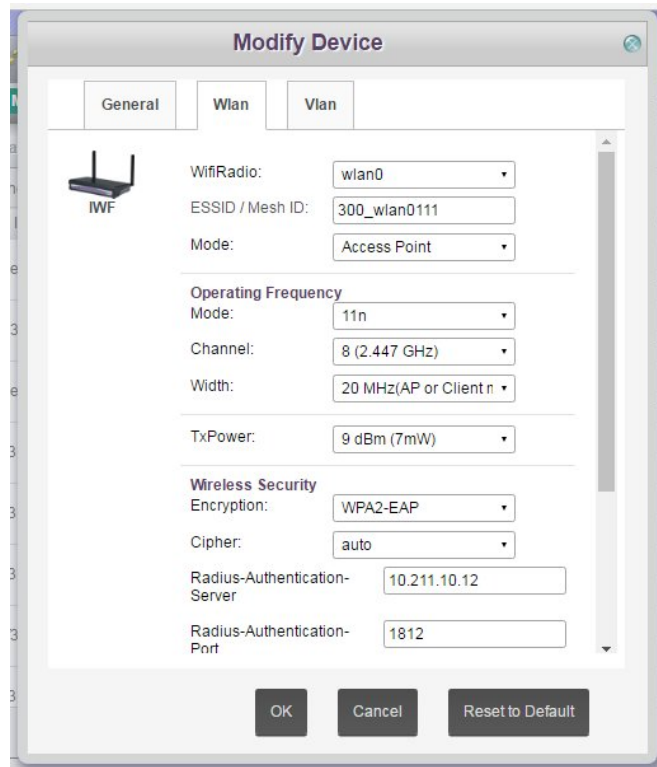


Figure 53 IWF Device Setting Page

(3) For the setting of *Wireless Security*, It will take few seconds to modify.

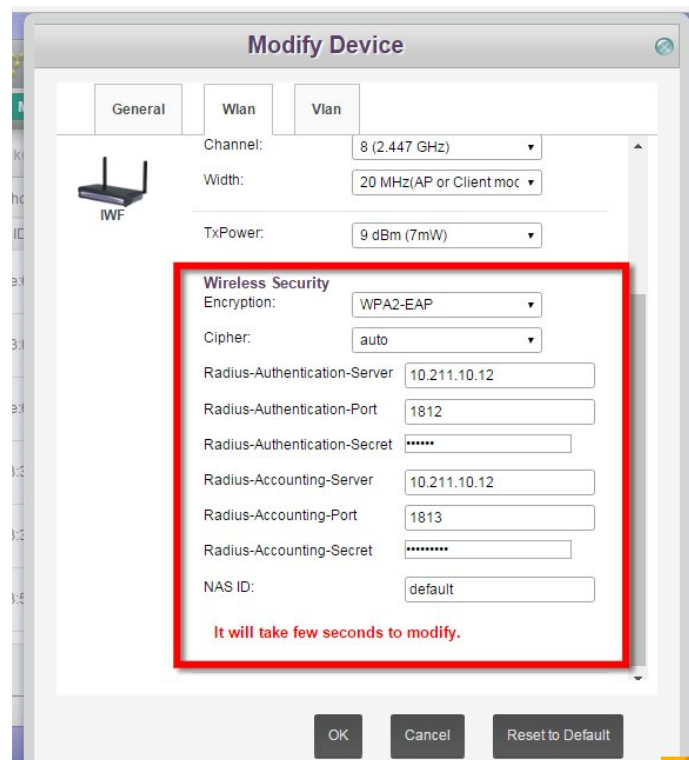


Figure 54 *Wireless Security* Setting Page

(4) Logical device grouping can be proceed with different physical network on **Vlan** label. That is, to cut LAN as desired VLAN. The procedures are list as follows:

- a. Create a *VLAN ID* on Ethernet.
- b. Choose *VLAN ID* from pull-down menu and enter *VLAN Name*.
- c. Choose the *Port* to open.
- d. Click **Create Vlan** to create a new VLAN, or click **Delete Vlan** to delete the VLAN.

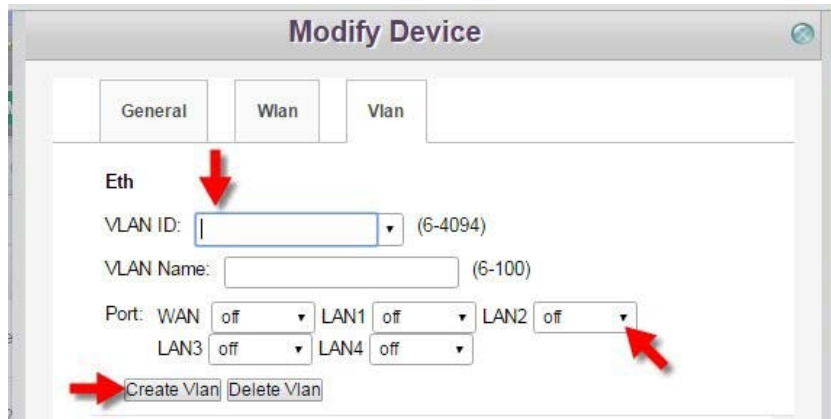


Figure 55 Create VLAN

- e. Choose the *Bridge If* from the pull-down menu to let the device been recognized by the bridge at this VLAN.

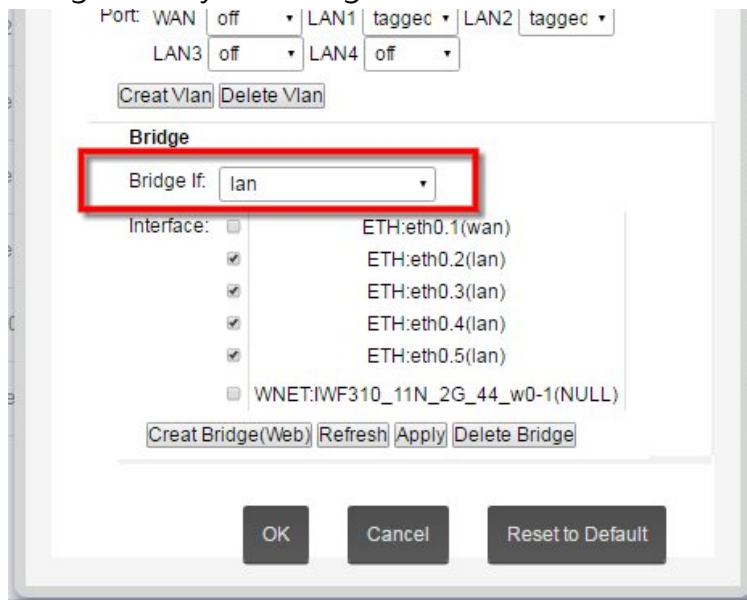


Figure 56 Bridge Selection

- f. Or click **Create Bridge(Web)** to guide the user to create bridge network on device web page, then click **Refresh**.
- g. The new-created bridge name can be found on the pull-down menu of *Bridge If*.
- h. The new-created bridge can be deleted by clicking **Delete Bridge**.



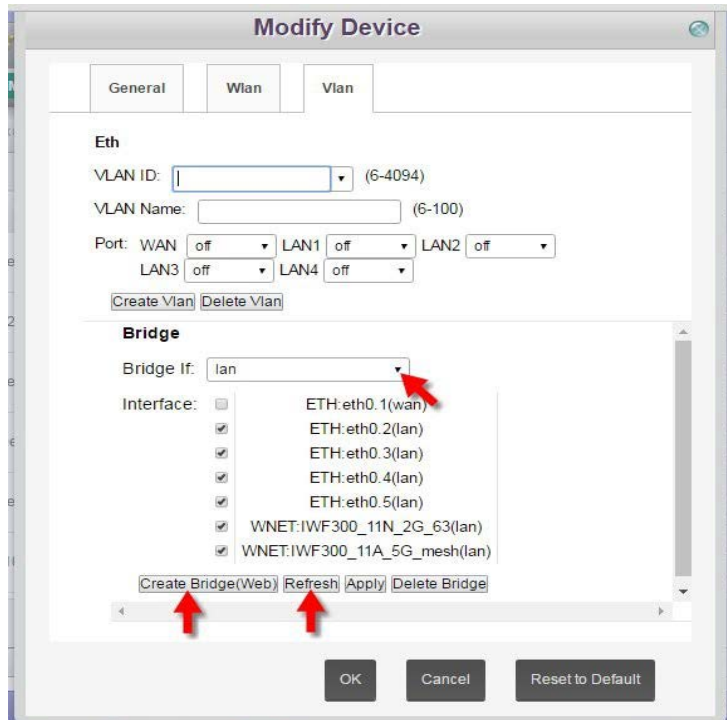


Figure 57 VLAN Interface Creation

- i. Set LAN Interface: Different VLAN name will be shown after proceed the previous procedures. Check the VLAN then click **Apply**.

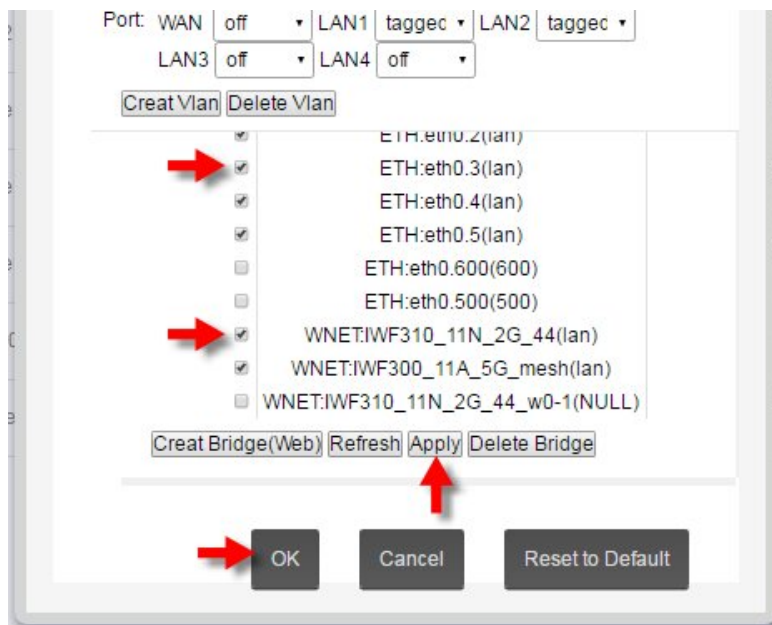


Figure 58 VLAN Interface Selection

- (5) Logical device grouping can be proceed with different physical network on **Vlan** label. That is, to cut LAN as desired VLAN. The



procedures are list as follows:

- a. Create a VLAN ID on Ethernet.
- b. Choose *VLAN ID* from pull-down menu and enter *VLAN Name*.

(6) There are labels of "Wlan" and "Serial/Modbus on Modify Device page for NIO51 module of Device Server series.

- a. *WifiRadio*, *Operating Frequency* and *Wireless Security* can be set on "Wlan" label.

The screenshot shows the 'Modify Device' window with the 'Wlan' tab selected. The configuration fields are as follows:

Field	Value
WifiRadio	wlan0
ESSID / Mesh ID	NIO51_11N_2G
Mode	Mesh,802.11s
<b>Operating Frequency</b>	
Mode	2.4G
Channel	11 (2.462 GHz)
Width	40 minus MHz
TxPower	10 dBm (10mW)
<b>Wireless Security</b>	
Encryption	No Encryption

It will take few seconds to modify.

Figure 59 Wlan Setting Page for NIO51 Devices

- b. *Serial Port Configuration* and *TCP* can be set on "Serial/Modbus" label.

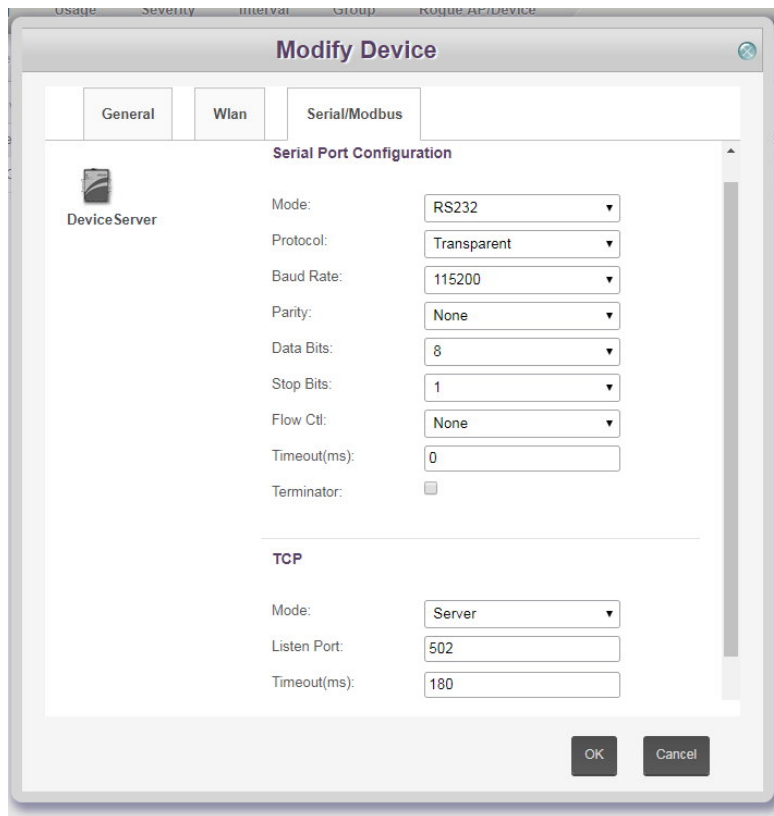


Figure 60 Serial/Modbus Setting Page for NIO51 Devices

- (7) Except normal setting for NIO51 series devices at Device Server label, there are *WiFi AP Configuration*, *Serial Port Configuration* and *Data Flow Configuration* setting options.

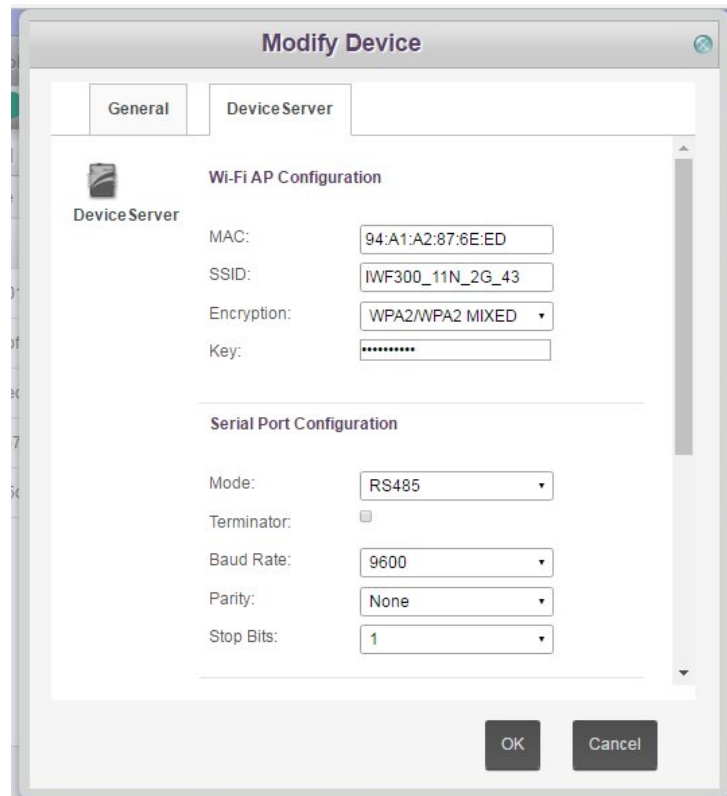


Figure 61 Parameters Modification for NIO51 of Device Server

- (8) There are labels of "General," "Wlan" and "WirelessHART" on Modify Device page for setting NIO200-HAG devices of IWSN Gateway series.
- Access Point, Gateway and Network Manager* can be set on "WirelessHART" label.
  - Enter parameters then click "Save."
  - Click **Reboot** for updating the setting.

**Modify Device**

General | Wlan | **WirelessHART**

IWSN Gateway

**\*The new setting will take effect after device restart**

**Access Point General Setting**

EUI64: 00-1B-1E-F8-70-06-00-01

AP Tag: NEXCOM AP

Network ID: AAAA

Save

**Gateway General Setting**

GW Tag: NEXCOM GW

Cache Read Response Timeout: 60

Cache Burst Response Timeout: 3600

Save

**Network Manager General Setting**

NM Tag: NEXCOM WHart Manager

Save

Cancel Reboot

Figure 62 Parameters Modification for WirelessHART of IWSN Gateway

- d. Scroll down Modify Device page.
- e. Parameters such as *Access Point*, *Gateway* and *Devices* for Device Management can be set on “WirelessHART” label.
- f. The device can be added or activated for Device List on this label as well.

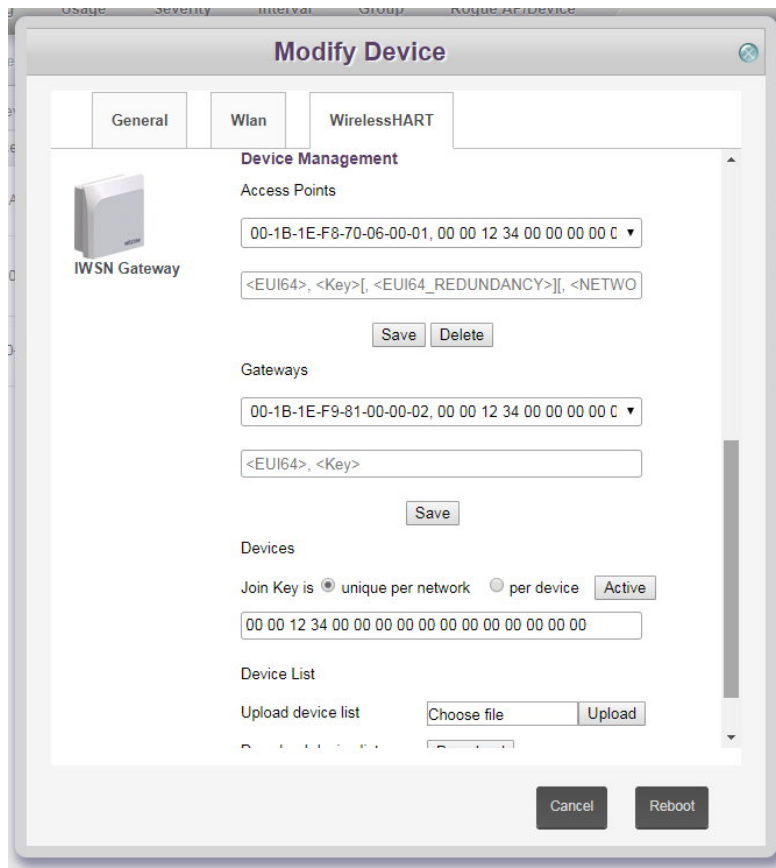


Figure 63 Parameters Modification for WirelessHART of IWSN Gateway

- (9) There are labels of "General," "Wlan" and "ISA100" on Modify Device page for setting NIO200-IAG devices of IWSN Gateway series.
- a. *Backbone Router, Gateway and Syetem Manager* can be set on "ISA100" label.
  - b. Enter parameters then click "Save."
  - c. Click **Reboot** for updating the setting.

**Modify Device**

General Wlan **ISA100**

IWSN Gateway

**\*The new setting will take effect after device restart**

**Backbone Router General Setting**

EUI64:

BBR Tag:

Save

**Gateway General Setting**

EUI64:

GW Tag:

Save

**System Manager General Setting**

EUI64:

SM Tag:

Save

**Device Management**

Cancel Reboot

Figure 64 Parameters Modification for ISA100 of IWSN Gateway

- d. Scroll down Modify Device page.
- e. Parameters such as *Backbones*, *Gateways* and *Devices* for Device Management can be set on "ISA100" label.
- f. The device can be added or activated for Device List on this label as well.

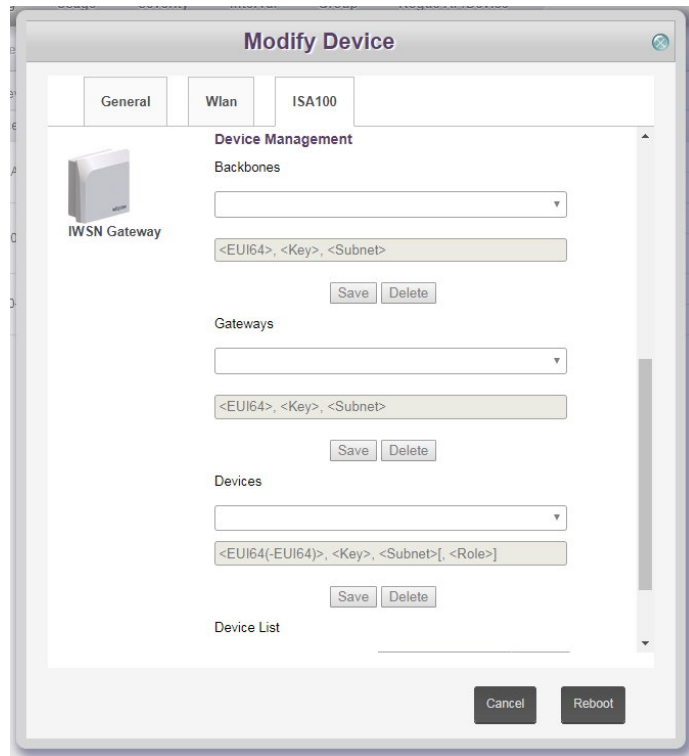


Figure 65 Parameters Modification for ISA100 of IWSN Gateway

(10) With **IPC Device** Type, there is another **Alert Threshold** for further setting except **General** page. Check the *Active* box and change the setting then click **OK** to save setting.

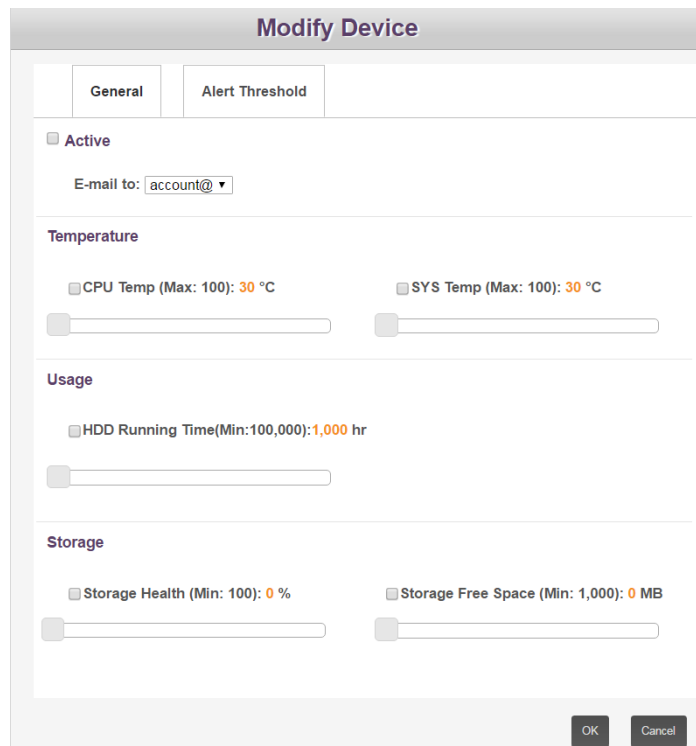


Figure 66 IPC Device Setting

### 6.1.2.7 Device Deletion

Click  icon to delete the chosen device.

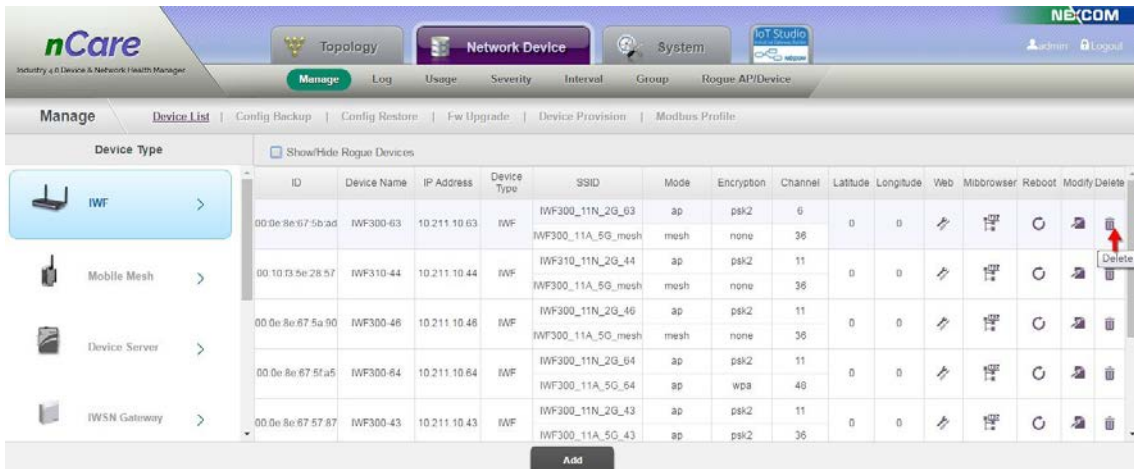



Figure 67 Device Deletion Icon

### 6.1.3 Introduction for Configuration Backup

The configuration of device can be backed-up manually or with schedule.

### 6.1.4 Operation for Configuration Backup

- (1) Check device *Model* or *IP Address* for the searching condition. Click  icon to search.

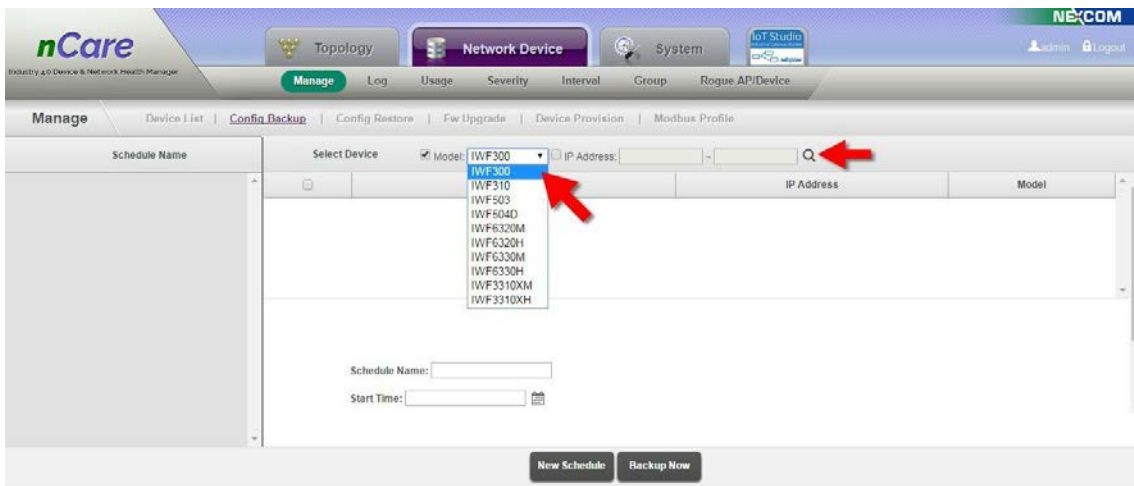


Figure 68 Search for Device to Backup

- (2) Multiple devices can be chosen for backing-up.
- (3) Click **Backup Now** to backup immediately.



- (4) Enter *Schedule Name*, *Start Time* and choose *Repeat* type from pull-down menu, then click **New Schedule** to setup backup scheduling.

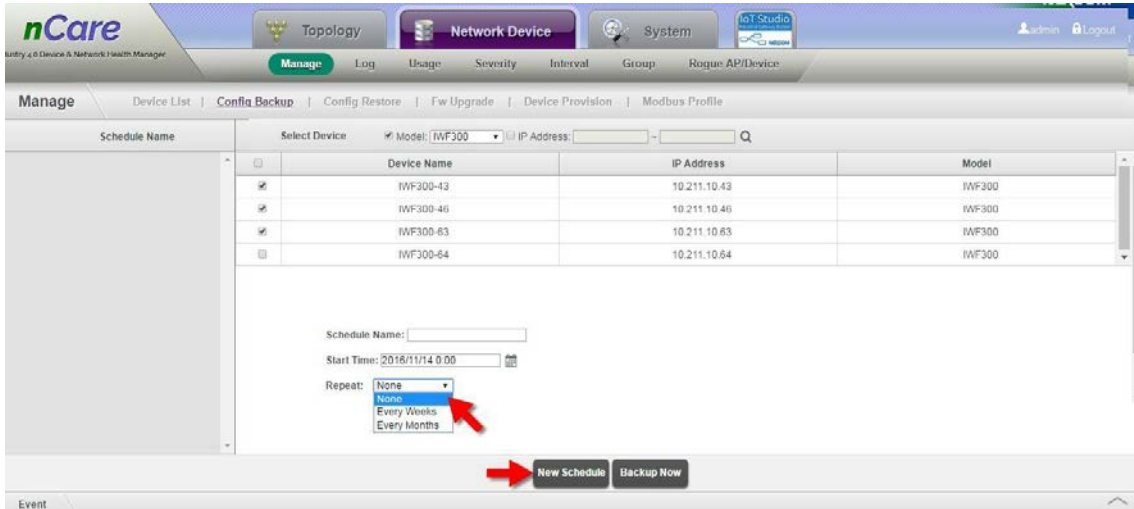


Figure 69 Configuration Backup with Schedule

- (5) The *Scheduled Name* of the configuration backup will be listed on the left. The schedule setting can be modified by clicking on the *Schedule Name*.
- (6) Click **Modify Schedule** to save the update.

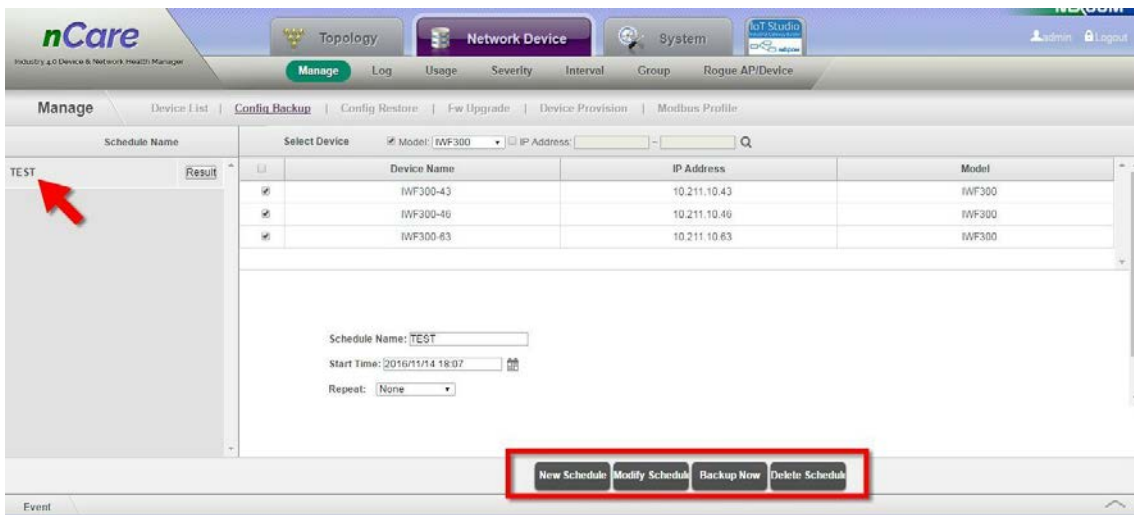



Figure 70 Configuration Backup Schedule List

- (7) Click on the **Result** to see the status of configuration backup. Click  icon to save the backup information.

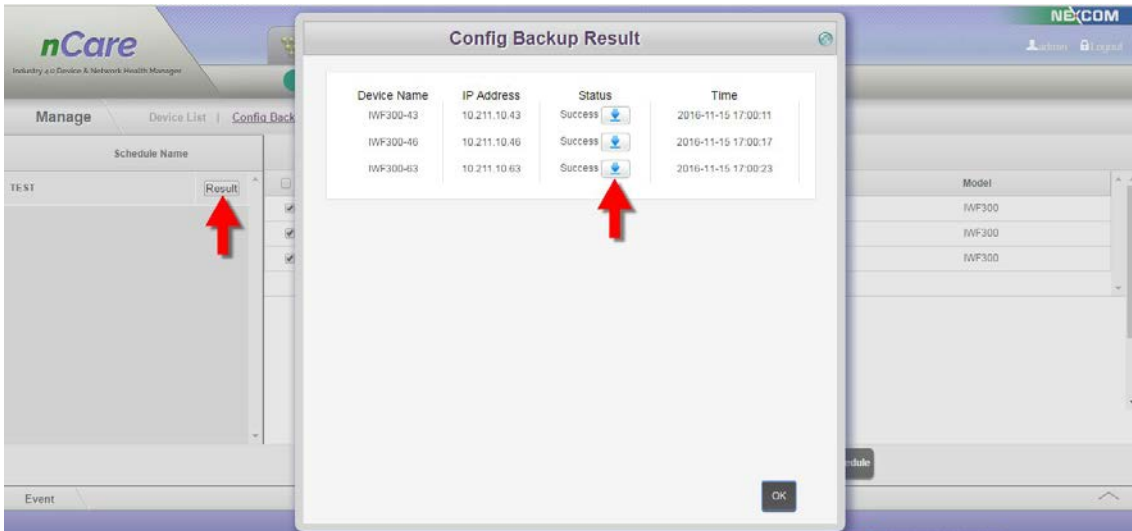



Figure 71 Status of Scheduled Configuration Backup

### 6.1.5 Introduction for Configuration Restore

After the configuration being backed-up, the device can also be restored by the saved configuration setting.

### 6.1.6 Operation for Configuration Restore

- (1) Check device *Model* or *IP Address* for the searching condition. Click  icon to search.

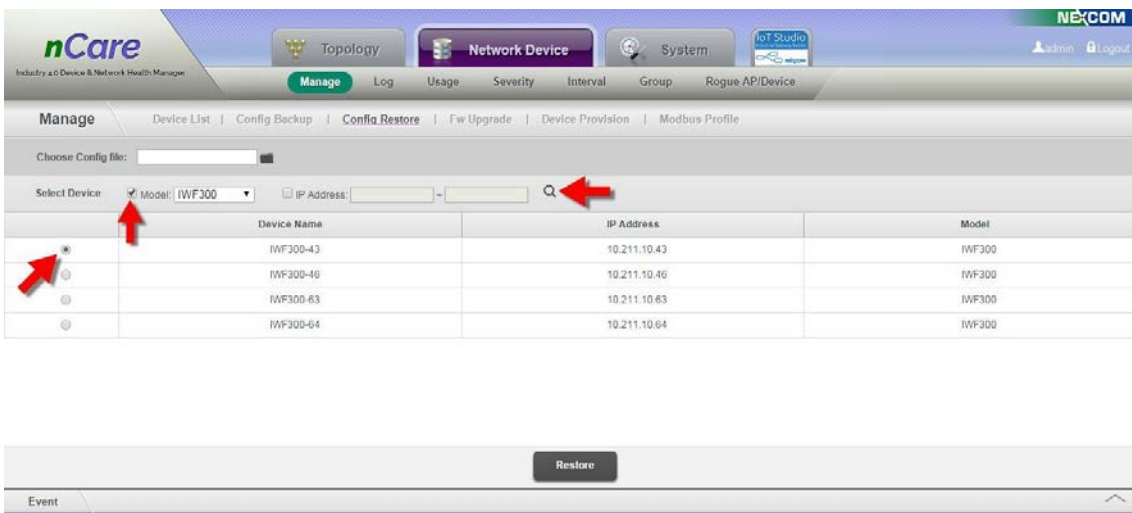



Figure 72 Search for Device to Restore

- (2) Click on the  icon to browse for backup file. Choose the desired one for device restoring.

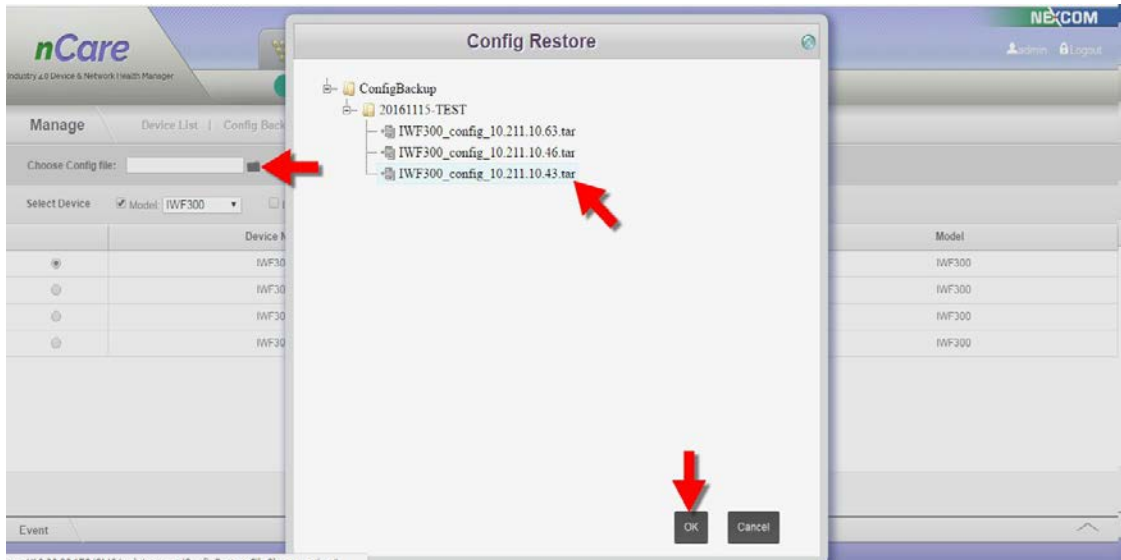


Figure 73 Backup File Selection

(3) Load the file, then click **Restore** and **Yes** to continue.

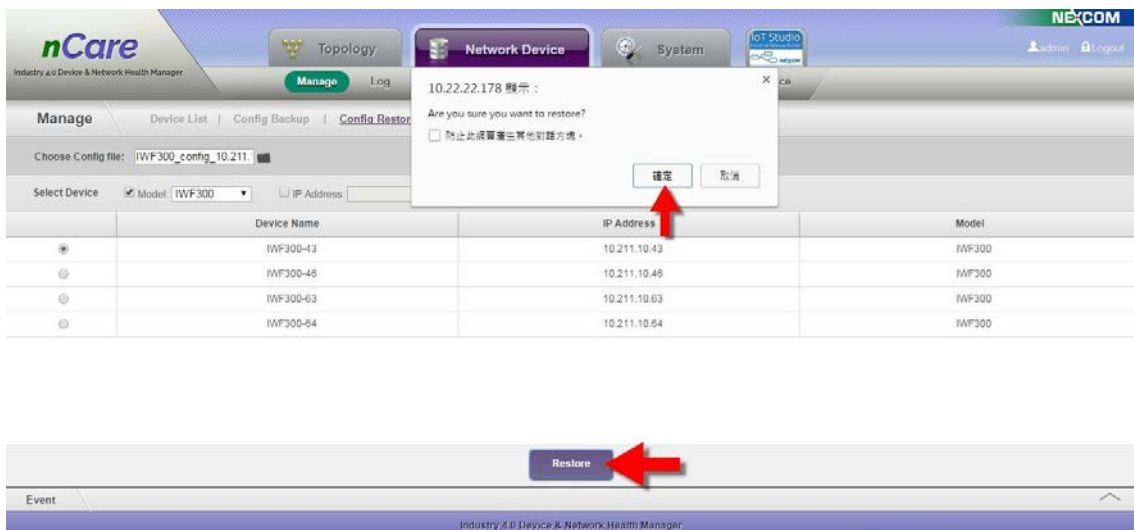


Figure 74 Configuration Restore Confirmation

(4) If the wrong backup file is chosen, an error message will pop-up.

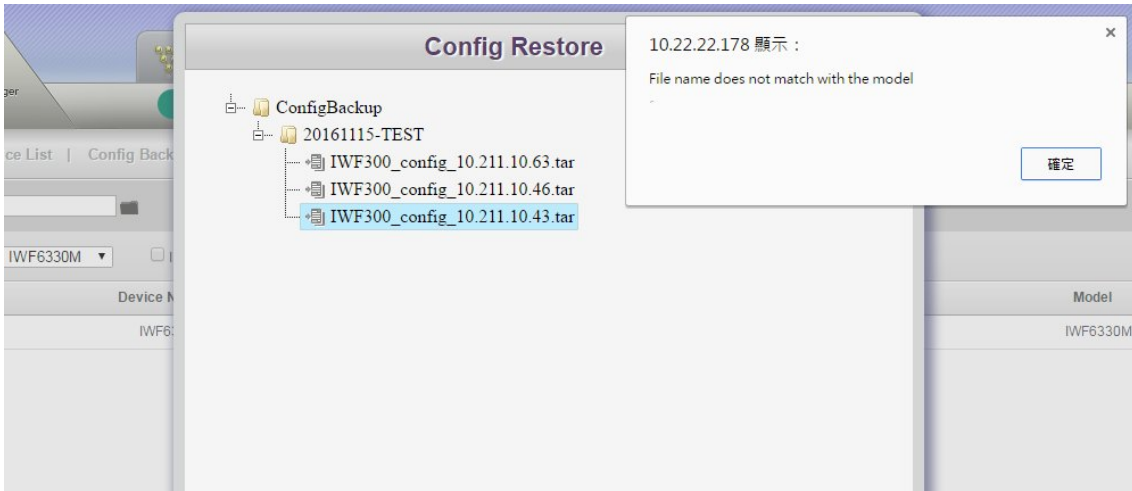



Figure 75 Error Message for Wrong Backup File

### 6.1.7 Introduction for Firmware Upgrade

nCare may upgrade the firmware for device manually or scheduled.

\* Please confirm the file type of firmware: [Device Type]-[Version]. For example: IWF300-v2.0.bin

### 6.1.8 Operation for Firmware Upgrade

(1) Select Device: Check "Model" or "IP Address" then click  to search for the device.

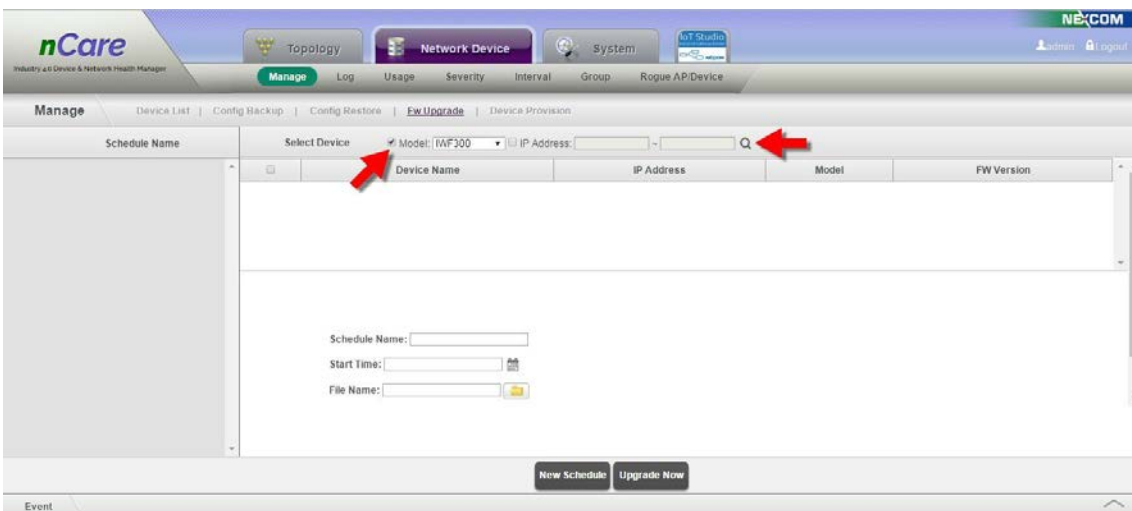


Figure 76 Selection for the Device to Upgrade the Firmware

(2) Check the device for upgrading the firmware. Fill Schedule Name, Start

Time, and choose file by clicking  to surf for related driver.

- (3) Click **New Schedule** and **Yes** to add a firmware upgrade task with schedule. Or click **Upgrade Now** to upgrade the firmware immediately.

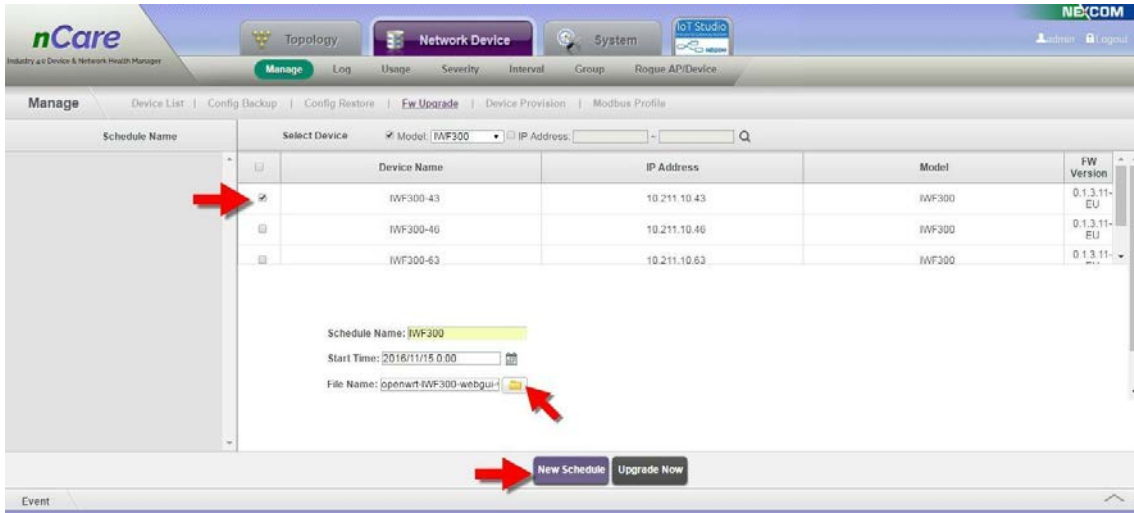


Figure 77 Upgrade the Firmware with Schedule

- (4) Click on the *Schedule Name* on the left to **Modify Schedule**, **Upgrade Now** or **Delete Schedule**.

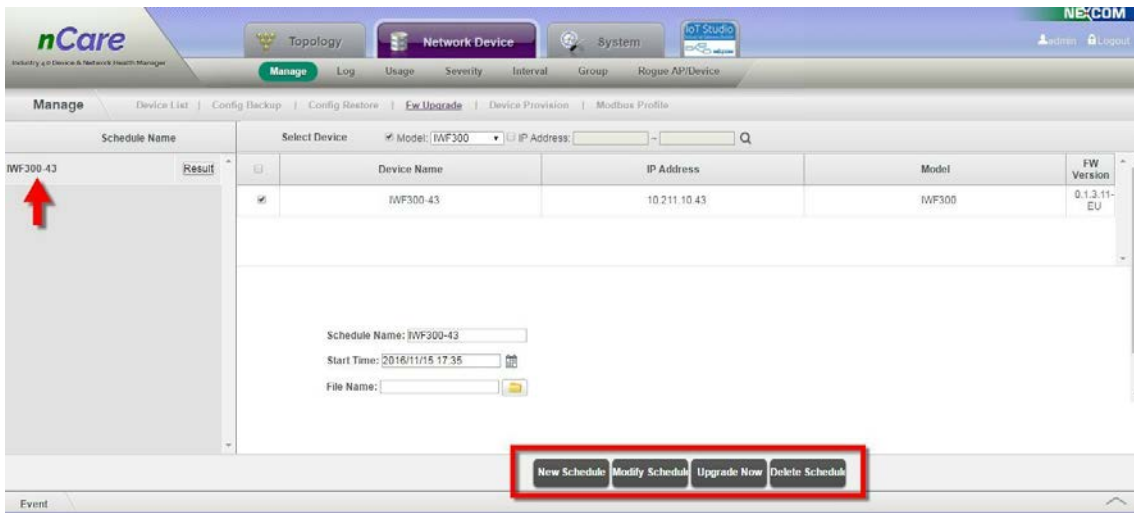


Figure 78 Scheduled Task Modification

- (5) Click on **Result**, and a "Firmware Upgrade Result" window will pop-out.
- (6) *Device Name, IP Address, Status and Time* will be shown.

Success: Firmware has upgraded successfully.

Ongoing: Device is upgrading.

Failed: Firmware has failed to upgrade, please contact the customer service of **Nexcom**.

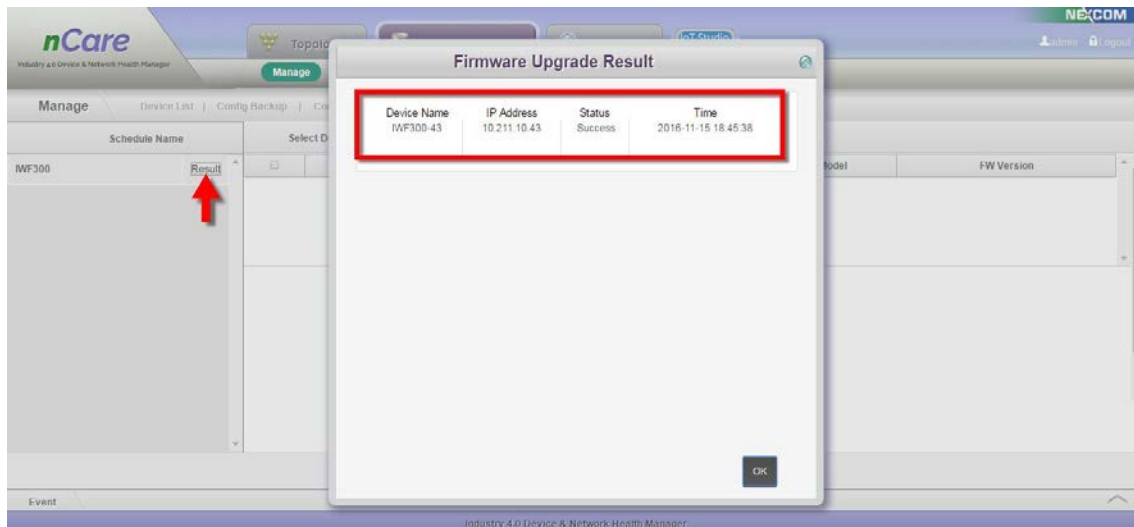


Figure 79 Firmware Upgrade Result

### 6.1.9 Introduction for Device Provision

Manager may deploy multiple new device by nCare. Connect all device to the server of nCar and set the IP address by the DHCP function(Chapter 5.4). Use the **Device Provision** function to batch process the parameter such as *ESSID/Mesh ID, Mode, Encryption, etc.*

### 6.1.10 Operation for Device Provision

- (1) Choose Device Type and Model Name.
- (2) Enter the information of *General Setting, Interface* and *Operation Frequency*.
- (3) Click **Save**.

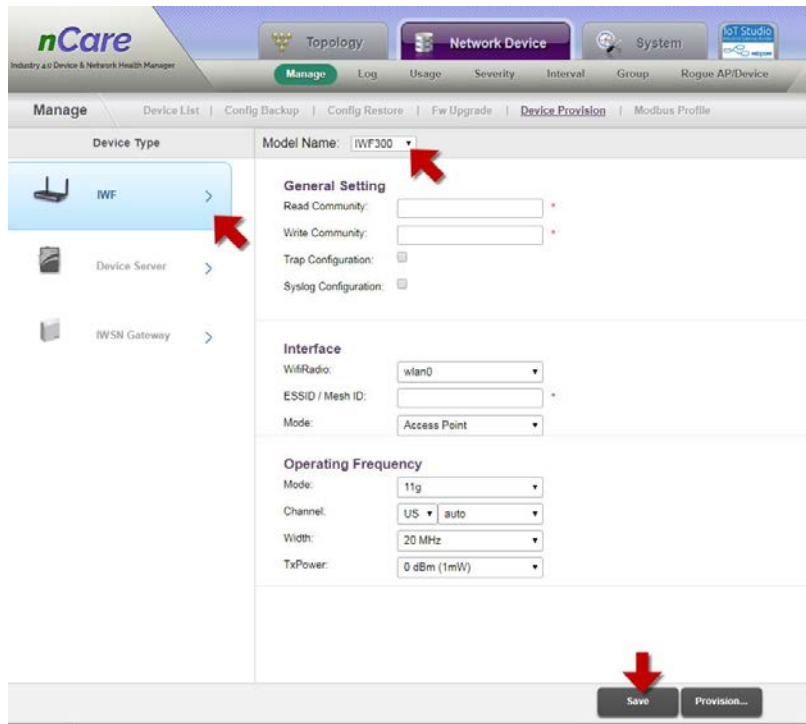


Figure 80 Device Provision Setting

- (4) Click **Provision**, and a *Device List* window will pop-out.
- (5) Choose the device to provision, then click **OK**.
- (6) Go to Device List (Chapter 6.1.1) and Topology (should be re-discovered), the device will be updated.

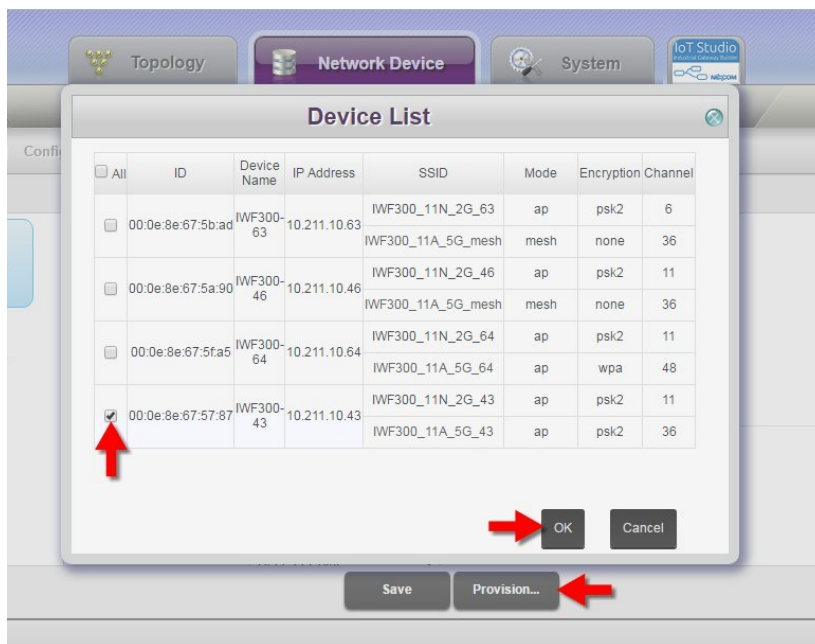


Figure 81 Choose the Device to Provision

### 6.1.11 Introduction for Modbus Profile

This function is used for create device that support Modbus such as IPC or PLC type of device. If this kind of devices are added, they can be discovered on nCare then.

### 6.1.12 Operation for Modbus Profile

- (1) Enter Device Model and upload the device icon.

The screenshot shows the nCare web interface for configuring a Modbus profile. The top navigation bar includes 'nCare', 'Topology', 'Network Device', 'System', and 'IoT Studio'. The main menu has 'Manage', 'Log', 'Usage', 'Severity', 'Interval', 'Group', and 'Rogue AP/Device'. The 'Modbus Profile' page is active, showing a 'Modbus List' on the left with items like 'APPC Series', 'ET7244', 'Modbus Sim', 'W-M1B403', 'W-M1B301', and 'NISE105'. The main area contains a 'Discovery Parameter' section with a note: '\*Note: Please use white space to separate the register values when word count is larger than 1 (Except for Unicode & Unicode1)'. Below this is a table for 'Register Table' with columns: Register Name, Unit, Function Code, Address Offset (E.g. 40123 -- 122), Word Count, and Attribute. The 'Model' and 'Vendor' fields are highlighted with a red box.

Figure 82 Enter Modbus Profiles

- (2) Enter the information of Modbus device on Discovery Parameter and Register Table area.
- (3) Enter Discovery Parameters such as *Register Value*, *Function Code*, *Address Offset* and *Word Count*.
- (4) Choose *Attribute* from the pull-down menu.(The value can be referred on device manual)



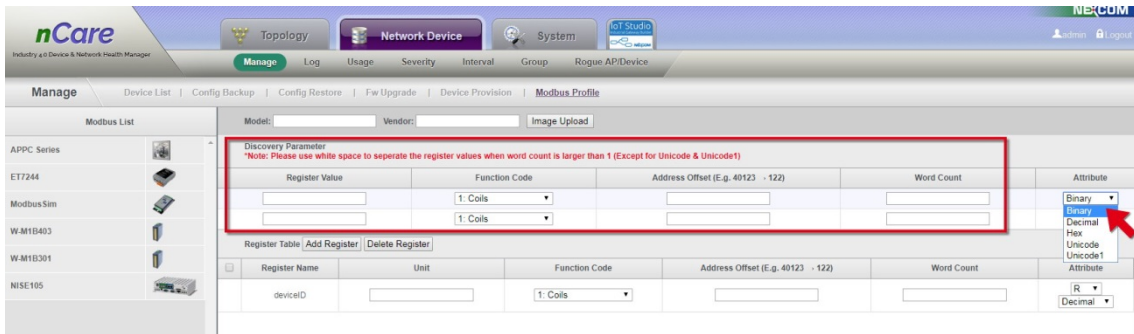


Figure 83 Enter Discovery Parameter

- (5) Click **Add Register** or **Delete Register** for adding or deleting field, respectively.
- (6) Enter Register Table such as *Register Name*, *Unit*, *Address Offset* and *Word Count*.
- (7) Choose *Function Code* and *Attribute* from the pull-down menu.(The value can be referred on device manual)

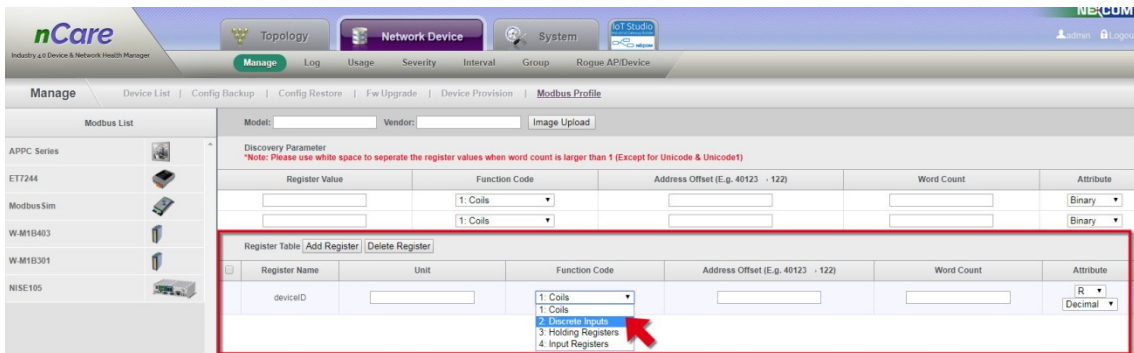


Figure 84 Enter Register Table Parameters

- (8) Modbus devices are listed on the left. Devices can be inquired, modified or deleted.
- (9) Click **Add** to complete device adding procedures

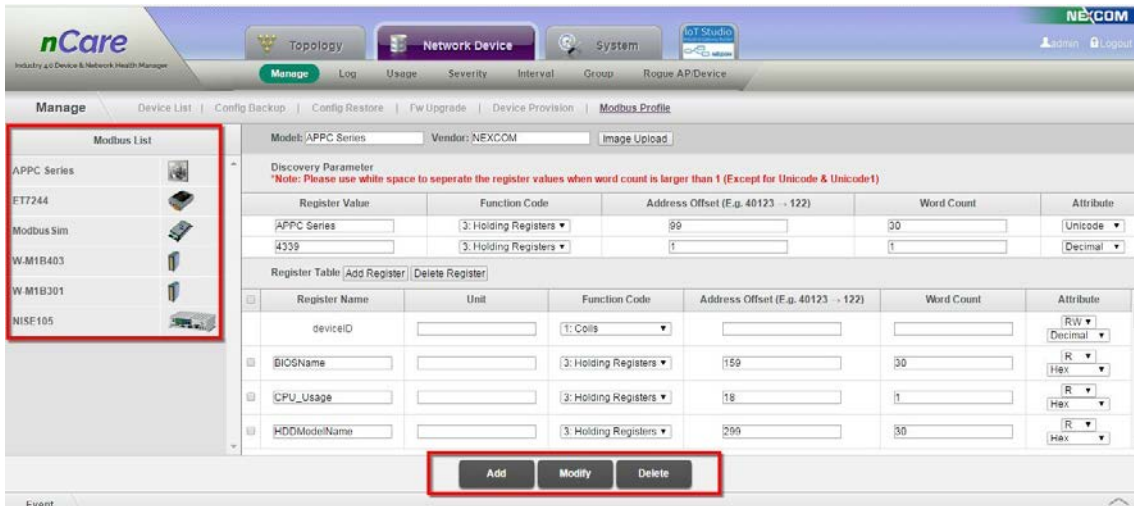


Figure 85 Modbus Device List

## 6.2 Log Management

Log page includes *Event Log*, *System Log* and *Playback*. Abnormal situations can be saved on the list and available for playback.

### 6.2.1 Introduction for Event Log

Abnormal situation will be saved on the record list. Administrator may search for the record with selected conditions.

### 6.2.2 Operation for Event Log

- (1) The *Event Log* function has event record within one month by default. Multiple searching conditions can be chosen.

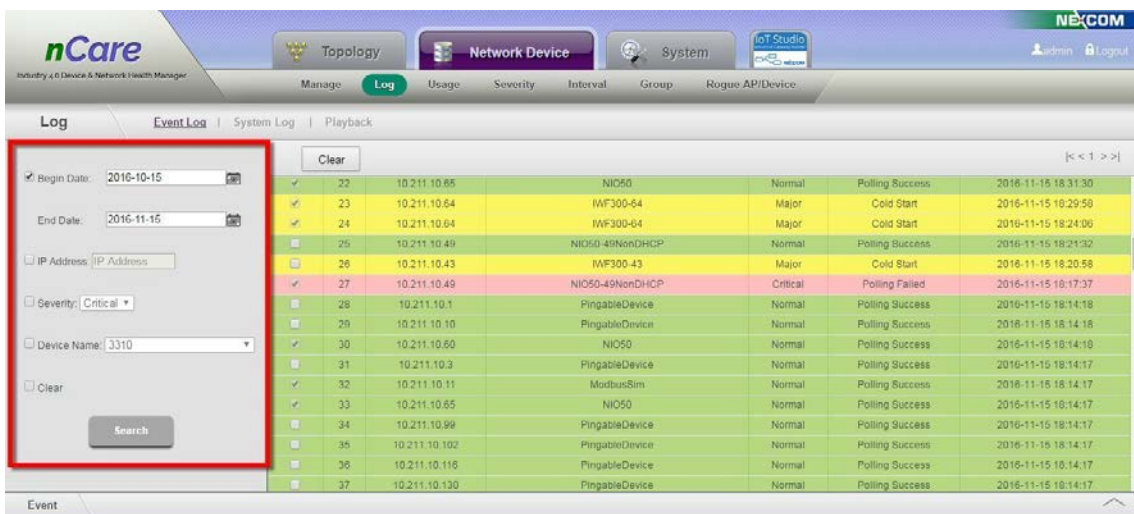


Figure 86 Searching Conditions for Event Log

(2) *Severity* of Event is marked with different colors. (Please refer to Chapter 6.4) The *IP Address*, *Device Name*, *Severity*, *Event Name* and *Time* will be shown.

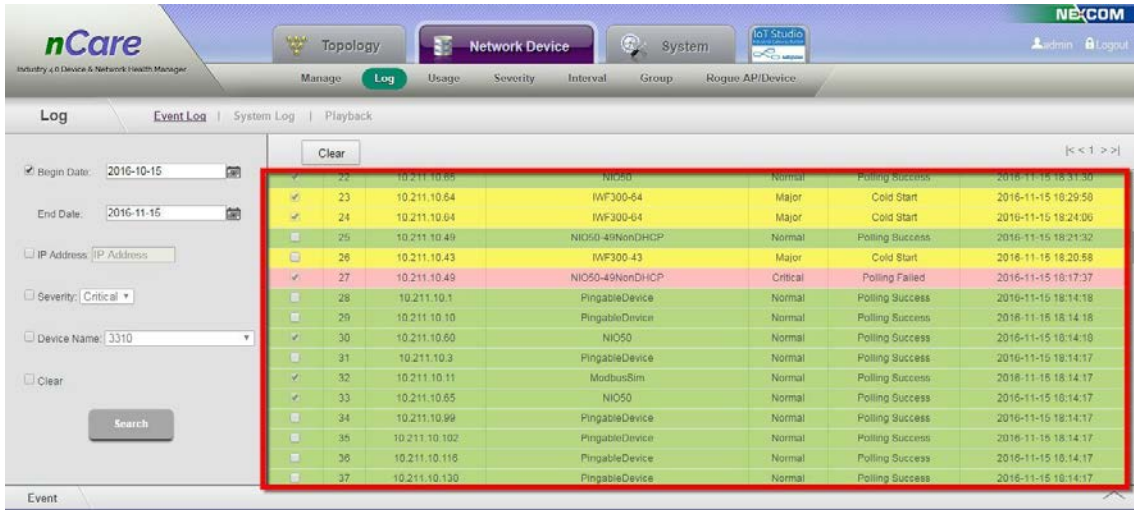


Figure 87 Event Log Table

(3) All records can be cleared by checking the box at its front, then click **Clear**.

(4) The deleted record will still show at the list but with fading check box.

\* Critical (RED) alert will be cleared automatically if the device is back to normal. Major (Yellow) alert should be cleared manually if the device is back to normal.

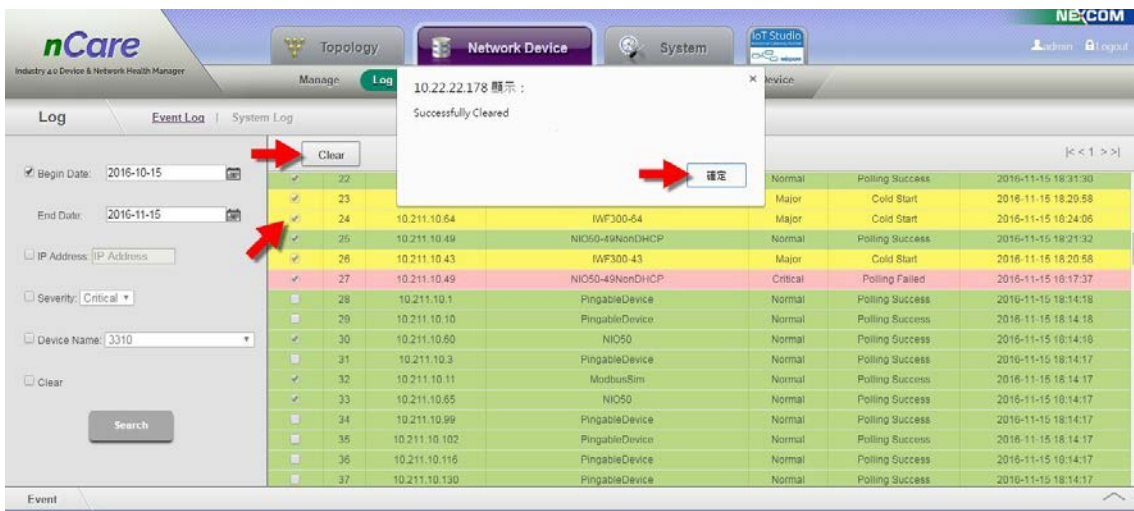


Figure 88 Clear Event Record



- (5) Event Shortcut Table: There is an icon below the main menu. Click  icon to open Event Shortcut Table, and click  to hide it.



Figure 89 Event Shortcut Table and its Icon

- a. Only RED (Critical) and YELLOW (Major) event will be shown on Event Shortcut Table.



Figure 90 Severity Level shown on Event Shortcut Table

- b. Severity level can be chosen by checking the box. And all kinds of events can be shown.



Figure 91 Severity Selection

### 6.2.3 Introduction for System Log

All the alert of execution and variation, such as MIB Browser setting, Firmware Upgrade, Device Backup, for the device will be recorded at **System Log** page. User may understand the status of device by checking **System Log** table.



### 6.2.4 Operation for System Log

**System Log** table is set to show the record within a month. User may search for the record with different searching conditions.

ID	IP Address	Device Name	Severity	Facility	Time	Message
1	10.211.10.51	IWF8320	Informational	Syslogd	2016-11-15 18:52:31	-- MARK --
2	10.211.10.47	IWF6330	Informational	System Daemons	2016-11-15 18:51:37	hostapd: ath16: STA 00:10:f3:36...
3	10.211.10.57	3310	Informational	Syslogd	2016-11-15 18:51:06	-- MARK --
4	10.211.10.47	IWF6330	Informational	Syslogd	2016-11-15 18:43:54	-- MARK --
5	10.211.10.50	IWF6320	Informational	Syslogd	2016-11-15 18:42:50	-- MARK --
6	10.211.10.51	IWF8320	Informational	Syslogd	2016-11-15 18:42:30	-- MARK --
7	10.211.10.47	IWF6330	Informational	System Daemons	2016-11-15 18:41:37	hostapd: ath16: STA 00:10:f3:36...
8	10.211.10.57	3310	Informational	Syslogd	2016-11-15 18:41:06	-- MARK --
9	10.211.10.47	IWF6330	Informational	Syslogd	2016-11-15 18:33:53	-- MARK --
10	10.211.10.50	IWF6320	Informational	Syslogd	2016-11-15 18:32:49	-- MARK --
11	10.211.10.51	IWF8320	Informational	Syslogd	2016-11-15 18:32:30	-- MARK --
12	10.211.10.47	IWF6330	Informational	System Daemons	2016-11-15 18:31:37	hostapd: ath16: STA 00:10:f3:36...
13	10.211.10.57	3310	Informational	Syslogd	2016-11-15 18:31:05	-- MARK --
14	10.211.10.64	IWF300-64	Emergency	System Daemons	2016-11-15 18:29:55	Nov 15 17:29:55 logread[5112]:

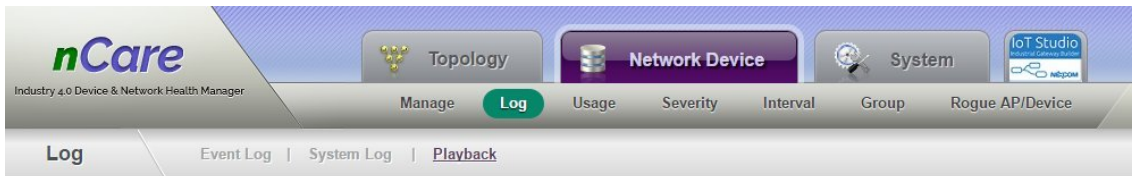
Figure 92 System Log Table

### 6.2.5 Introduction for Playback

Events can be playbacked with selected time or issue. The Topology at the selected time can also be shown for checking the issue.

### 6.2.6 Operation for Playback

- (1) Playback function is defaulted enabled.
- (2) Topology with issue is saved once in every 3 minutes.
- (3) The records will be cleared in 30 days.
- (4) Previous records will be cleared if the storage has reached 1024MB.
- (5) Administrator may set **Record Period**, **Days** and **Maximum Memory** for Playback function.



Enable:   
 Record Period: 3 minutes  
 days: 3 days  
 Maximum Memory: 128 MB

Figure 93 Playback Setting

(6) Click "Replay" for playing previous events.

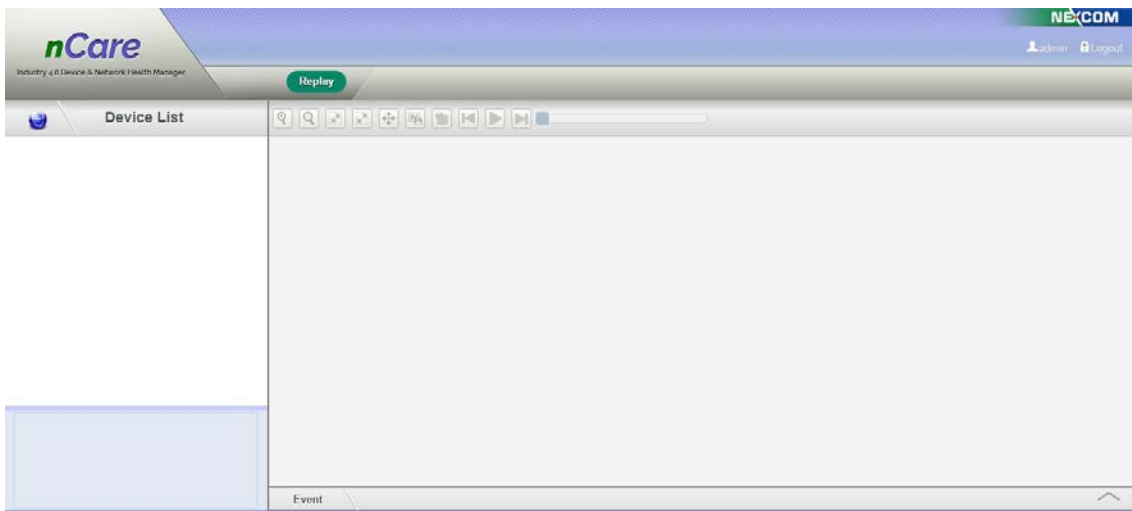



Figure 94 Events Playback

(7) Click  icon and a **Search** window will pop-out.

(8) Select *Begin Date* and *End Date* then click "OK" .

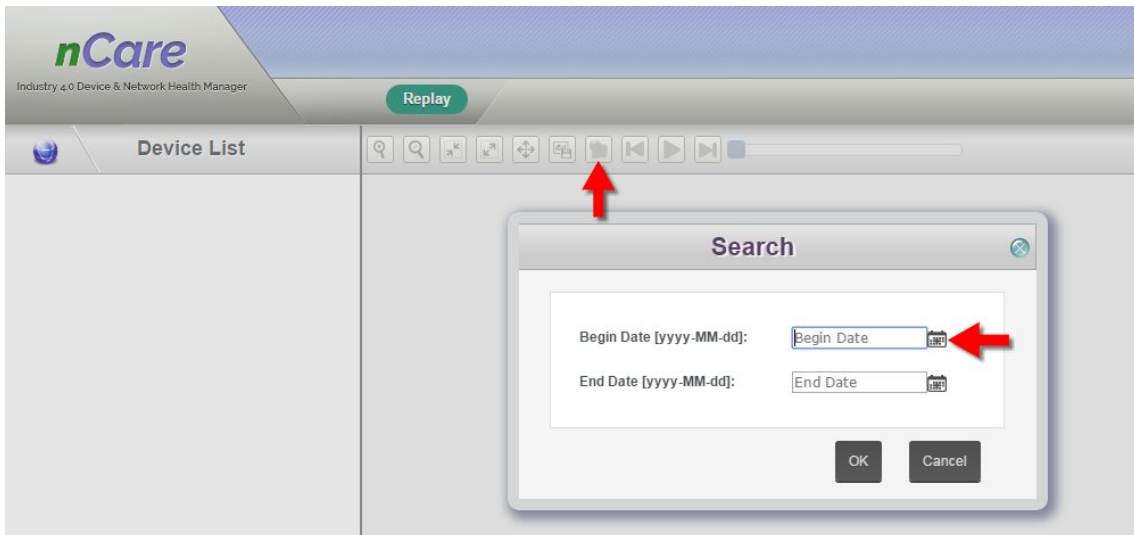


Figure 95 Events Searching

(9) Choose the issue for playback.

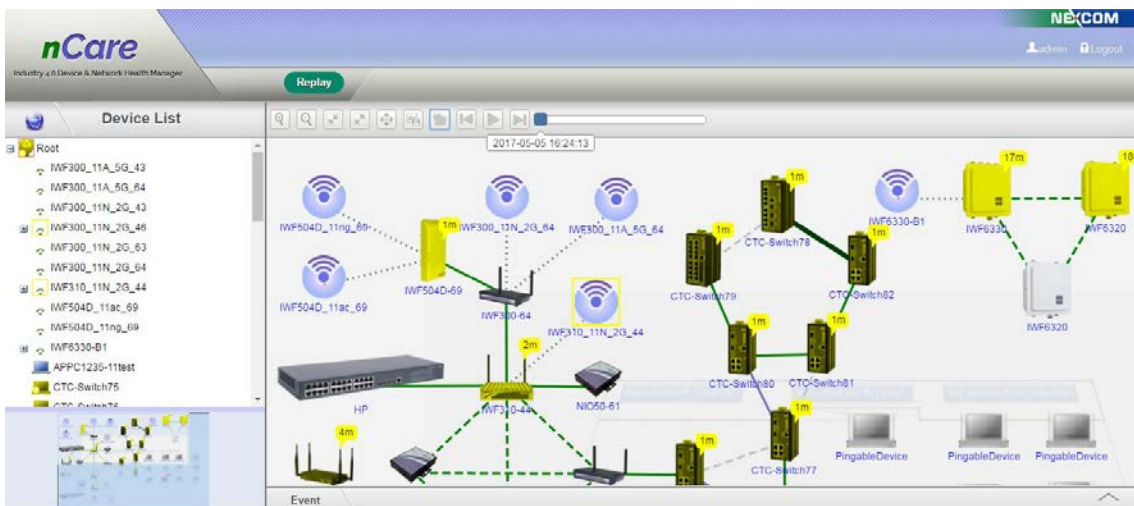
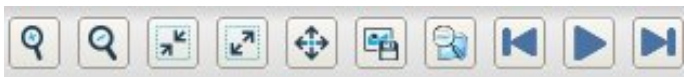





Figure 96 Issues shown on Topology


(10) Playback icons are list as follows:










 Zoom In: Zoom in the Topology.

 Zoom Out: Zoom out the Topology.

 Zoom Overview: Zoom to show the whole Topology.

 Zoom Reset: Zoom to show the Topology with original size.

-  Full Screen: Show Topology with full screen. Click "Esc" or  to back to main page.
-  Export to Image: Whole Topology can be saved. Click this icon and another page will pop-out, right-click to save as png image.
-  Search: Search for all the events with selected date range.
-  Previous: Play the event record from previous time point.
-  Play: Play the event record.
-  Next: Play the event record from the next time point.

## 6.3 Flow Usage

### 6.3.1 Introduction for Flow Usage

The flow usage of *Ethernet*, *WLAN*, *CPU* and *Memory* can be shown at this page. The data can be appeared as line chart.

### 6.3.2 Operation for Flow Usage

- (1) Choose the device to monitor with selected parameters, *Eth*, *Wlan*, *CPU* or *Memory*. The system will show the related data.

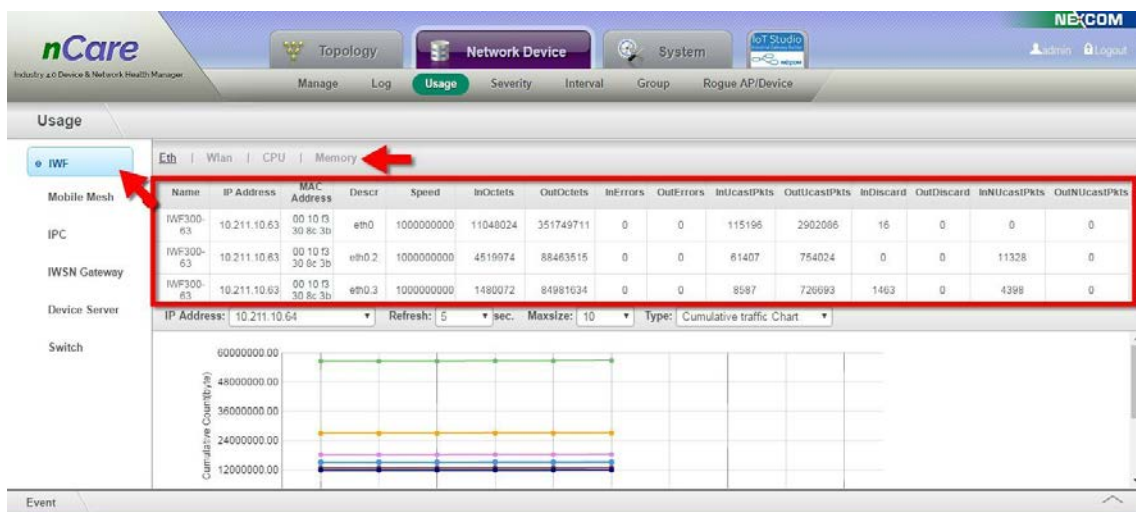


Figure 97 Data Table of Flow Usage

- (2) For the line chart, select the device from the pull-down menu of *IP*



Address with refresh time and maximum size node number. The line chart will be updated at the selected time and node number.

- (3) There are Throughput Chart and Cumulative Traffic Chart to choose for Ethernet and WLAN.

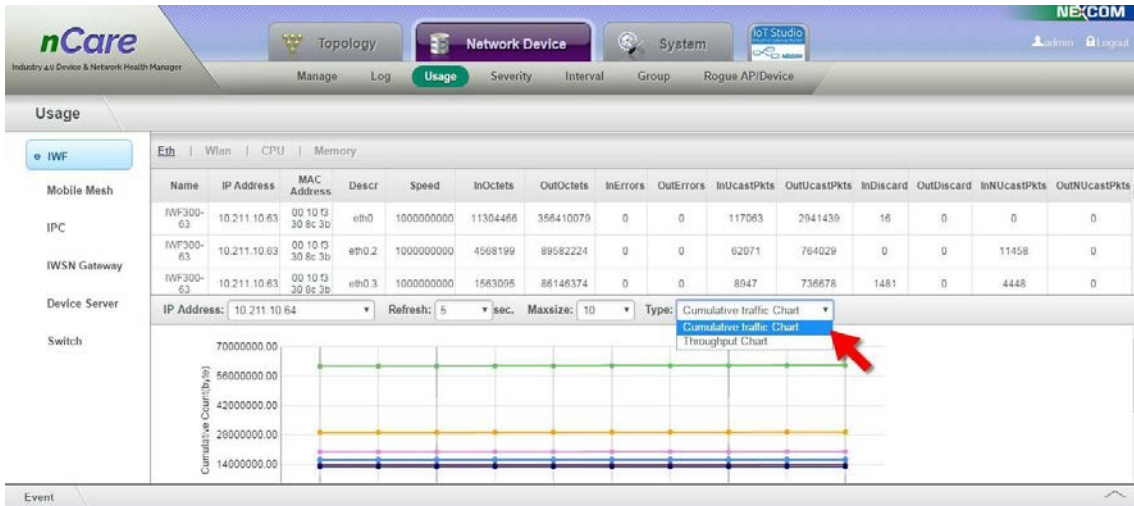


Figure 98 Different Form for Line Chart

- (4) The line chart will be drawn then. For example, the input and output flow of Ethernet will be shown.

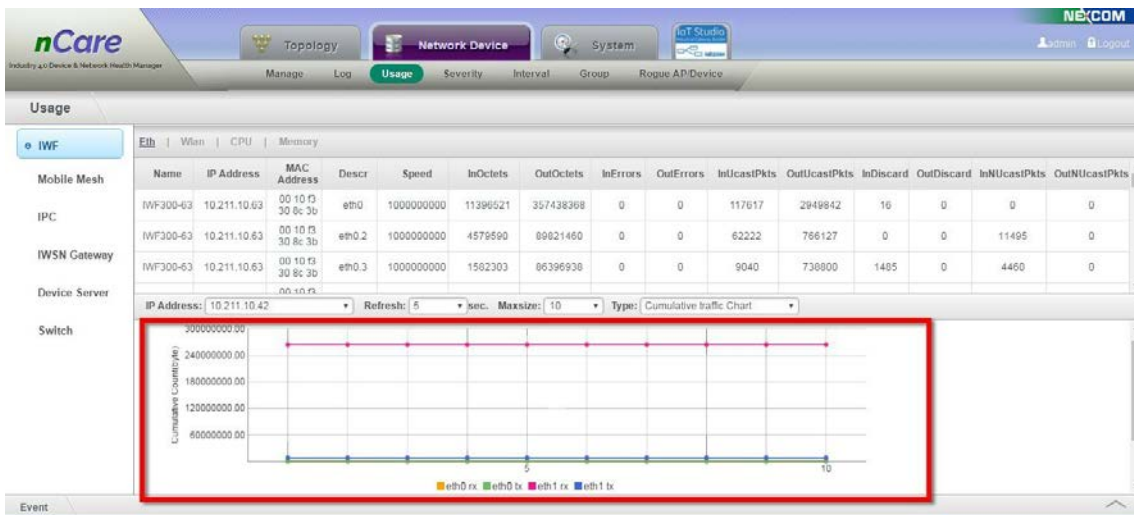


Figure 99 Eth Data chart

- (5) At the **Wlan** page, the line chart with throughput or cumulative traffic chart, and client number of WiFi Internet can be shown.

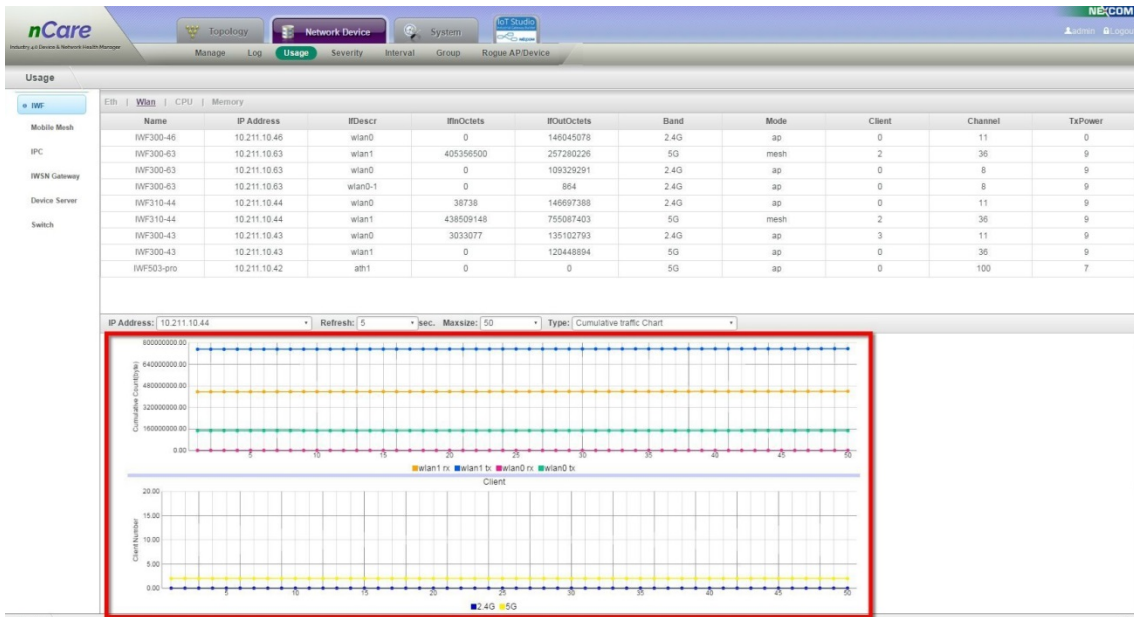


Figure 100 WLAN Data Chart

(6) At the CPU page, the line chart with CPU usage can be shown.

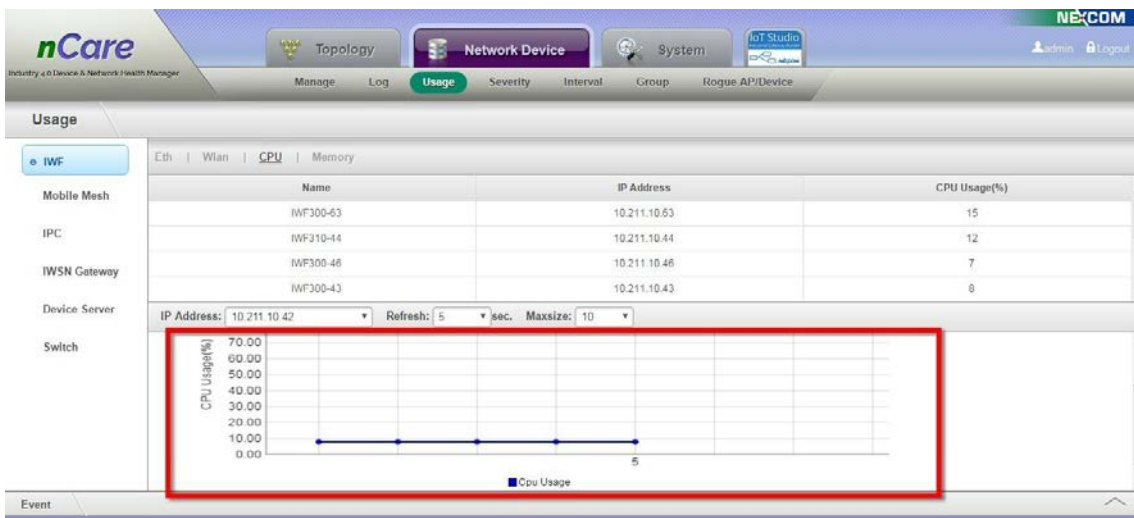


Figure 101 CPU Data Chart

(7) At the Memory page, the line chart with memory usage can be shown.

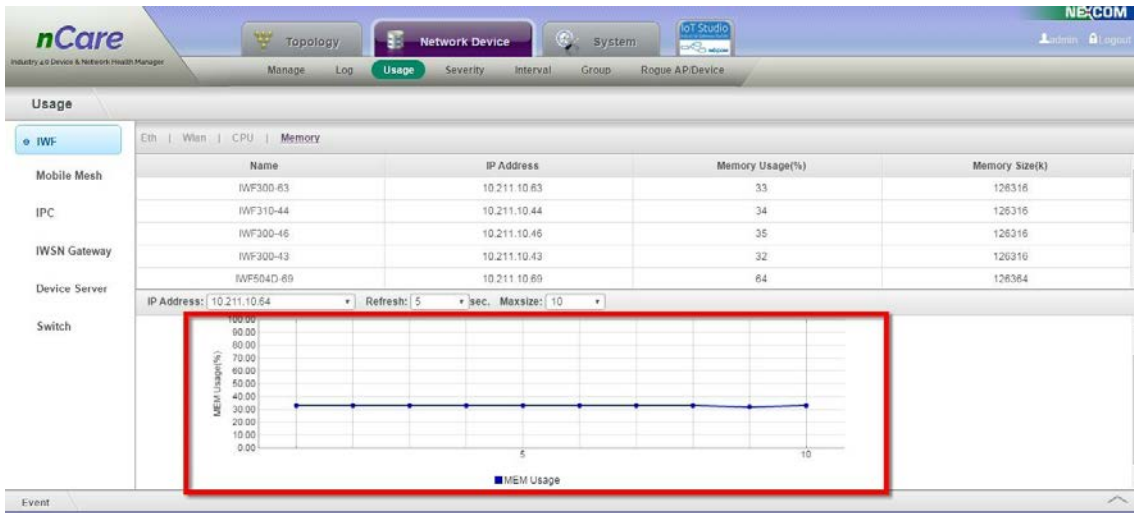


Figure 102 Memory Usage Data Chart

- (8) Choose the *IWSN Gateway* type device from the left column.
- (9) The data flow of NIO200-IAG, NIO200-WMR or NIO200-HAG can be shown as line chart.

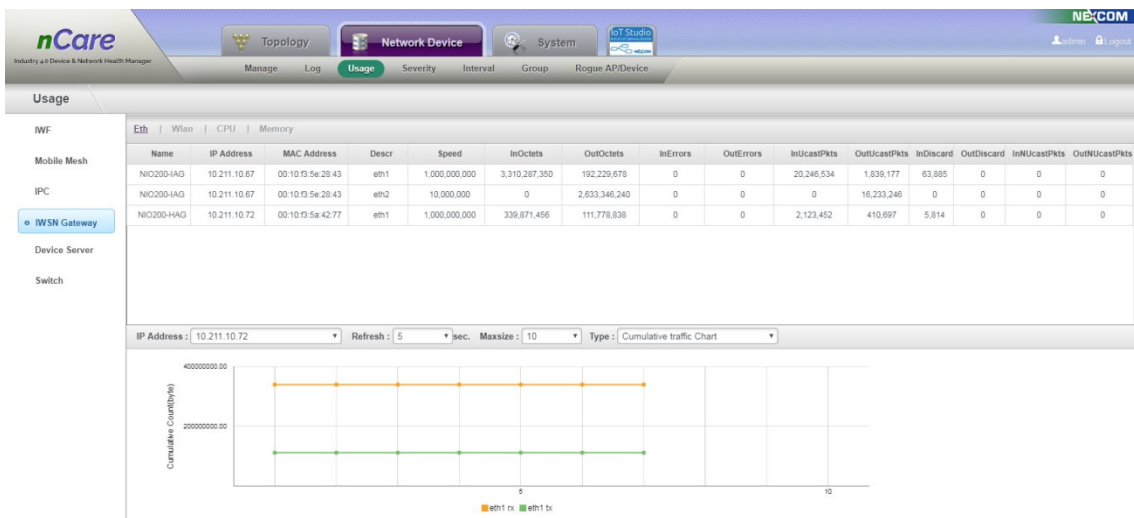


Figure 103 NIO200 Device Data Flow Line Chart

- (10) Choose the *Device Server* type device from the left column.
- (11) The data flow of NIO51 can be shown as line chart.

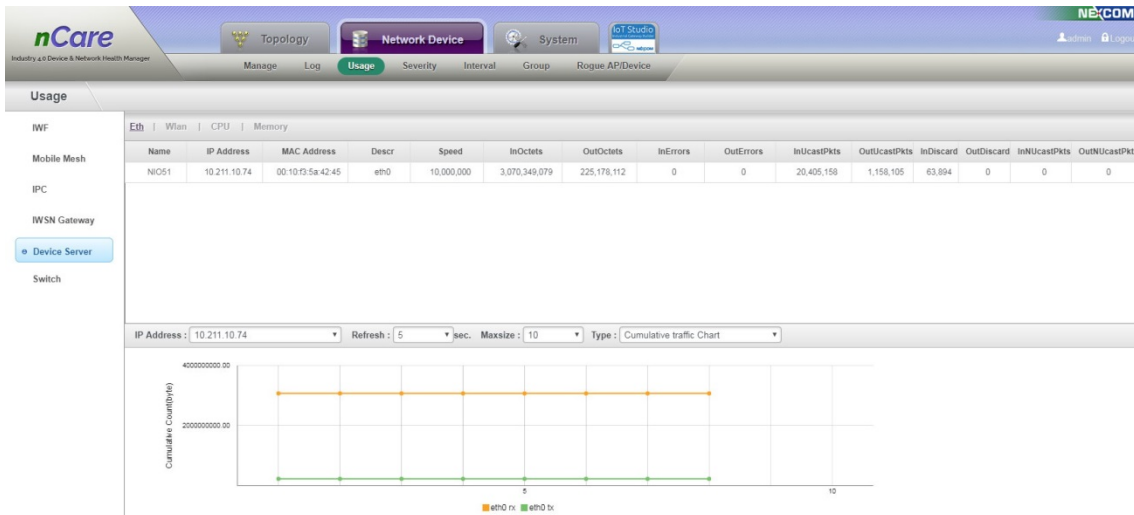


Figure 104 NIO51 Device Data Flow Line Chart

## 6.4 Severity

### 6.4.1 Introduction for Severity

The severity of Event is defined at this page. Critical situation marks as RED; Major situation marks as YELLOW; Normal situation marks as GREEN.

### 6.4.2 Operation for Severity

- (1) *Polling Failed, Link Down, Warm Start, Cold Start, Authentication Failed, Polling Success, Link Up, IPC Temp Alarm, IPC Storage Alarm and Rogue AP Alarm* with related *Severity* are all list at this page.

Event	Severity	Color	Modify
Polling Failed	Critical	Red	✎
Link Down	Major	Yellow	✎
Warm Start	Major	Yellow	✎
Cold Start	Major	Yellow	✎
Authentication Failed	Major	Yellow	✎
Polling Success	Normal	Green	✎
Link Up	Normal	Green	✎
IPC Temp Alarm	Major	Yellow	✎
IPC Storage Alarm	Major	Yellow	✎
Network Unstable	Major	Yellow	✎
Rogue AP/Device Alarm	Major	Yellow	✎
Ring Failure	Major	Yellow	✎
Ring LinkUp	Normal	Green	✎

Figure 105 Severity Table

- (2) This table may be modified. A **Modify Severity** window will pop-up when clicking on ✎ icon. Choose the *Severity* from the pull-down

menu then click **OK**. The color will change with its related severity.

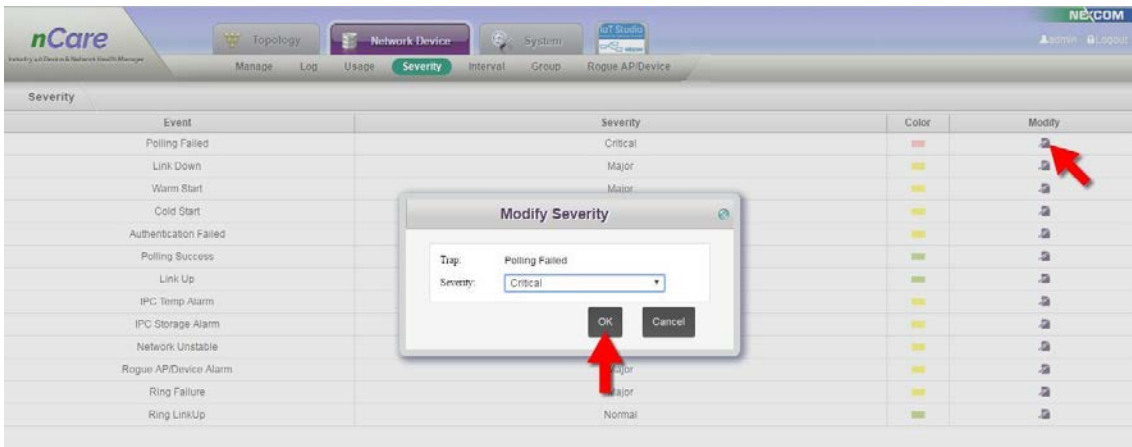


Figure 106 Severity Modification

## 6.5 Interval

### 6.5.1 Introduction for Interval

The cycle for polling device can be set. The trap sent by the same device within few minutes will be recorded at the Event Table.

### 6.5.2 Operation for Interval

Select *Polling Device Interval* and *Alarm Duplicate Period* then click **Apply**. Take the picture below for example, system will be polling device at every 60 seconds and duplicate the alarm at 300 seconds.

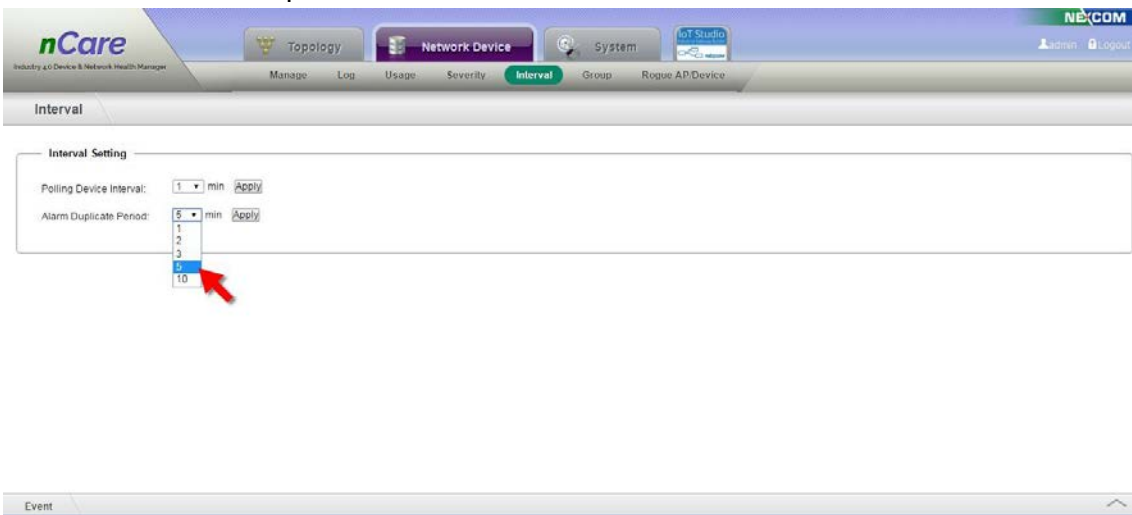


Figure 107 Interval Setting Page

## 6.6 Topology Group

### 6.6.1 Introduction for the Topology Group

This function is for classifying Topology Group. It'll be easier for managing the devices by the group with similar characteristics. The manage authority for a group can also be set.

### 6.6.2 Operation for Topology Group

- (1) Click on "Add" icon then an "Add Topology Group" window will pop-up. Enter Name, Latitude, Longitude, and choose for Map Image (with size smaller than 1MB and in png, jpg or bmp format).
- (2) Click "OK," then a new Topology Group will be added.

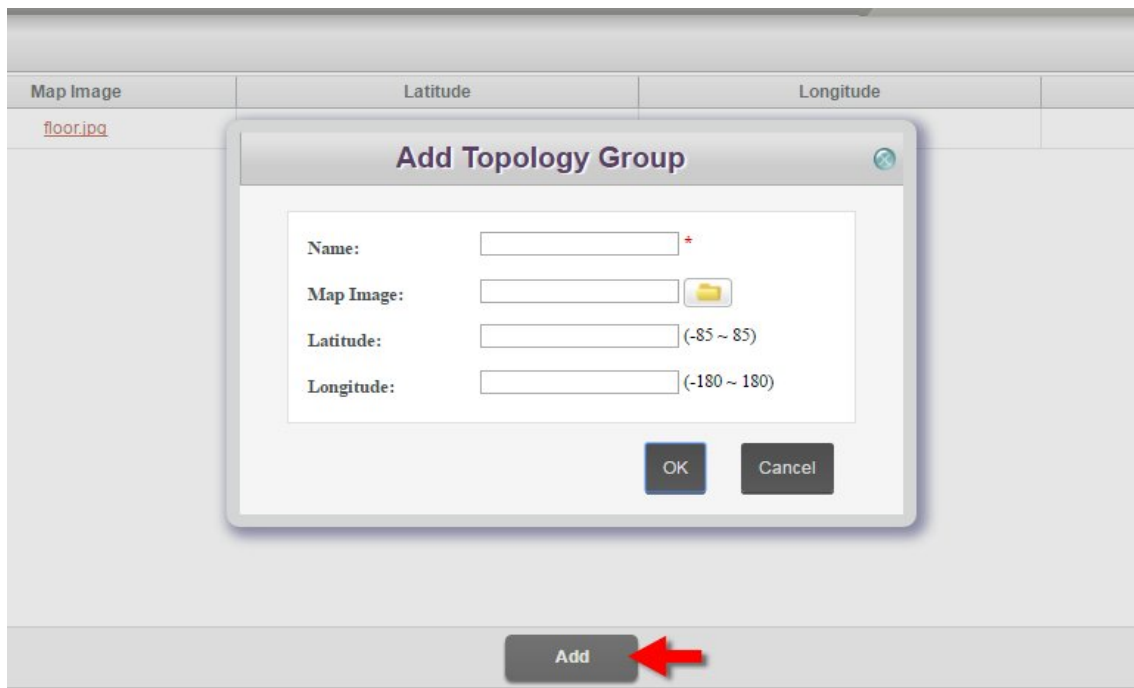


Figure 108 Add Topology Group Window

- (3) Topology Group can be modified or deleted. For further application of Topology Group, please refer to Chapter 7.1 Topology View\Group



Figure 109 Topology Group List and Modify/Delete Icons

## 6.7 Rogue AP/Device

### 6.7.1 Introduction for the Rogue AP/Device

Unauthorized Device can be detected and set by nCare. The device will be marked to inform users for security. However, the device can be incorporated into **White List**, to consider it as legal device.

### 6.7.2 Operation for Rogue AP/Device

#### 6.7.2.1 Detection

(1) Click **Scan** to detect for Rogue AP/Device.

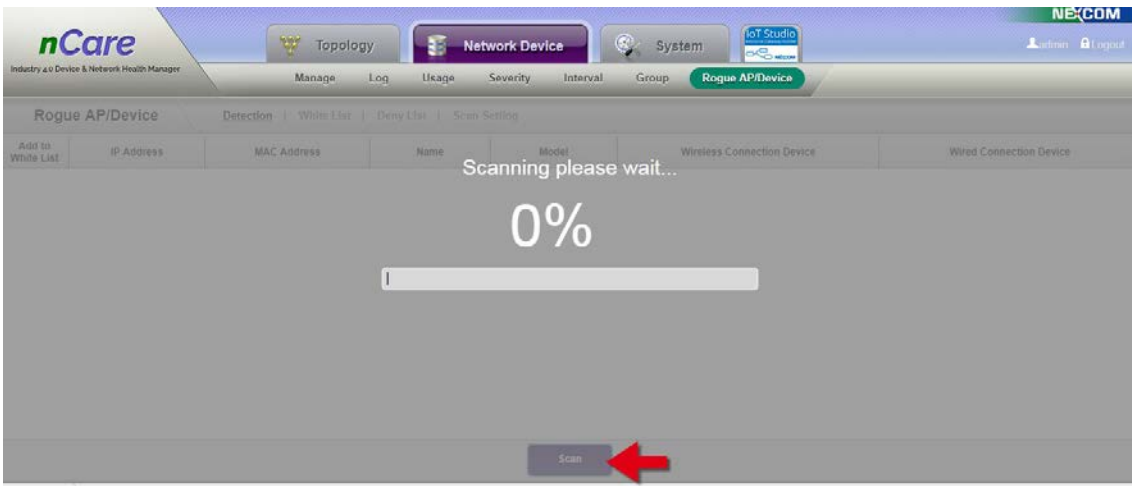


Figure 110 Scan for Rogue AP/Device

(2) There will be a list of rogue AP/device after scanned. The list includes information such as *IP Address*, *MAC Address*, *Name*, *Model*, *Wireless Connection Device* and *Wired Connection Device*.



Add to White List	IP Address	MAC Address	Name	Model	Wireless Connection Device	Wired Connection Device
<input type="checkbox"/>	10.211.10.79	de:aa:b9:08:29:2a	PingableDevice	Pingable device	-	-
<input type="checkbox"/>	10.211.10.78	00:10:f3:5a:42:01	PingableDevice	Pingable device	-	-
<input type="checkbox"/>	10.211.10.77	00:10:f3:4a:fc:8c	IWF503-77	IWF503	-	-
<input type="checkbox"/>	10.211.10.76	00:03:7f:50:00:55	IWF503-76	IWF503	-	-
<input type="checkbox"/>	10.211.10.74	00:10:f3:5a:42:45	NIO51	NIO51	-	-
<input type="checkbox"/>	10.211.10.72	00:10:f3:5a:42:77	NIO200-IAG-72	NIO200-IAG	-	-
<input type="checkbox"/>	10.211.10.70	00:10:f3:62:38:5b	NIO200-IAG-70	NIO200-IAG	-	-
<input type="checkbox"/>	10.211.10.67	00:10:f3:5e:28:43	NIO200-IAG-67-DDL	NIO200-IAG	-	-
<input type="checkbox"/>	10.211.10.63	00:0e:8e:67:5b:ad	IWF300-63	IWF300	-	-
<input type="checkbox"/>	10.211.10.58	cc:46:d6:86:d5:04	Unknown	Unknown device	-	-
<input type="checkbox"/>	10.211.10.57	00:10:f3:38:98:81	3310	IWF3310XH	-	-

Figure 111 Rogue AP/Device Table

(3) The information will also be recorded in **Event Log** table. (Please refer to chapter 6.2.1)

ID	IP Address	Device Name	Event	Time
1	10.211.10.77	IWF503-77	Poling Failed	2018-08-01 19:22:04
2	10.211.10.6	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12
3	10.211.10.6	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12
4	10.211.10.6	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12
5	10.211.10.6	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12

Figure 112 Rogue AP/Device list on Event Log Table

(4) The detected rogue AP/device will be marked with exclamation point on device list. (Please refer to chapter 6.1 )



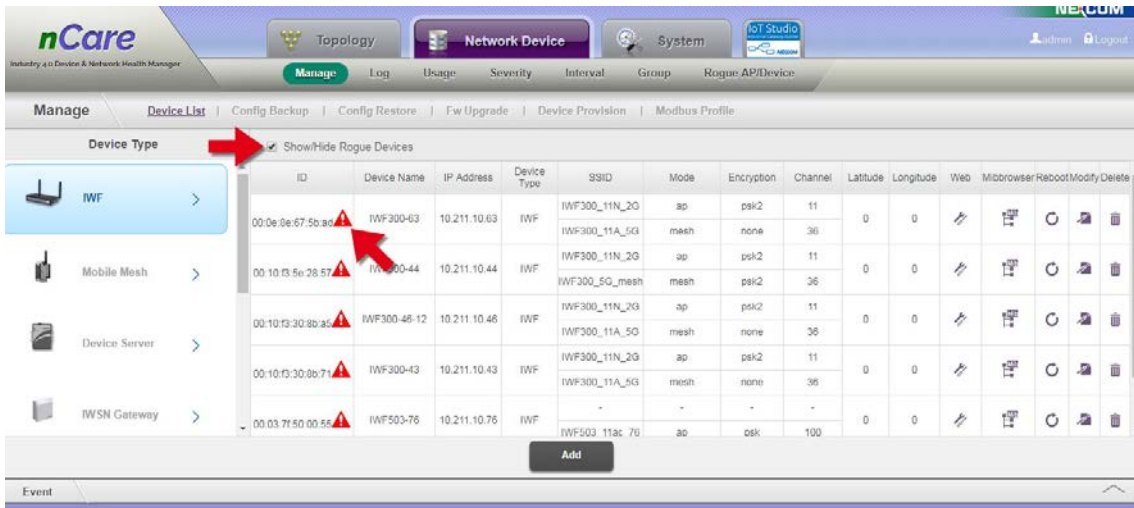


Figure 113 Rogue AP/Device on Device List

- (5) The detected rogue AP/device will be marked with exclamation point on topology as well. (Please refer to chapter 7.1.2.2)

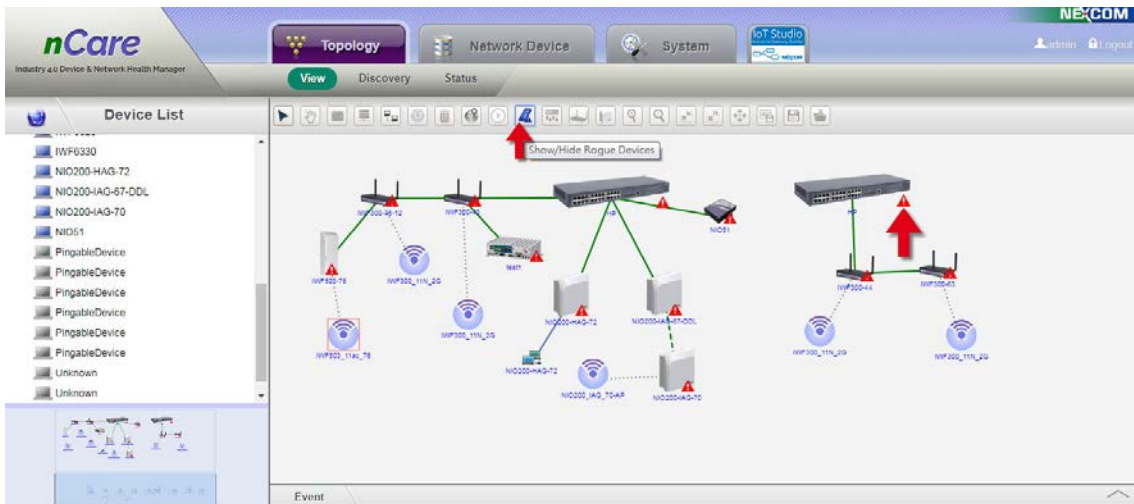


Figure 114 Rogue AP/Device on Topology

- (6) Click on the + mark to add the rogue AP/device into White List, or click **Add All** to add all rogue device into White List.

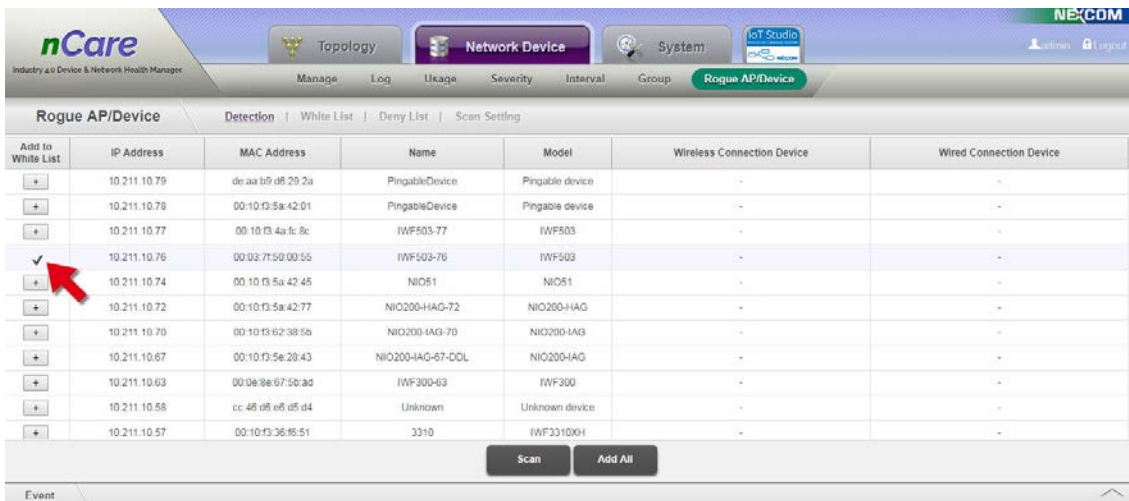


Figure 115 Add Rogue AP/Device into White List

### 6.7.2.2 White List

- (1) The detected rogue AP/device, which is considered as legal device, will be list on **White List**. The device can be modified and the list can be imported or exported as .csv file.

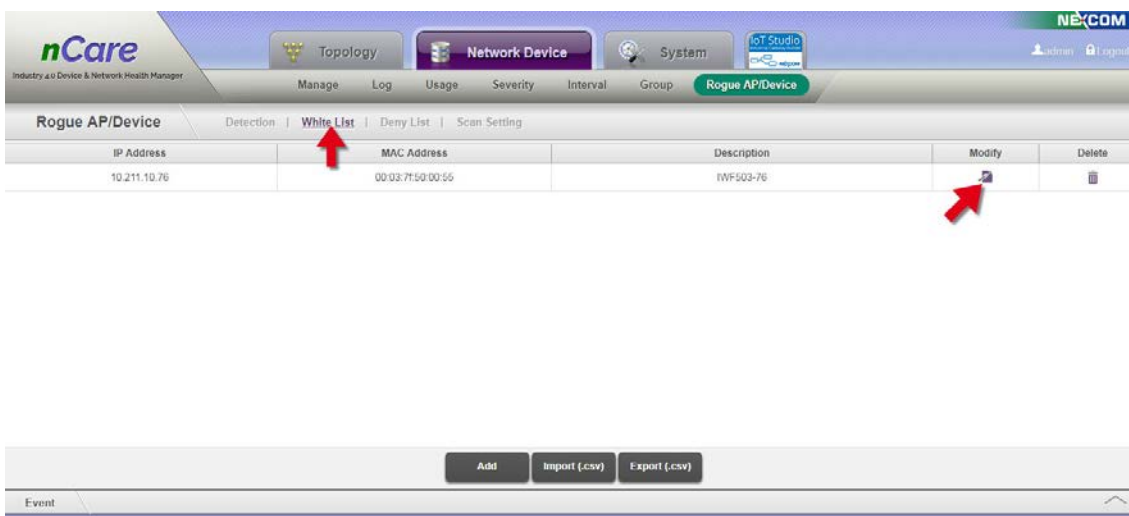


Figure 116 White List

- (2) Devices that have not be managed can also be added into White List.
- (3) Click Add and a Add **White List** window will pop-out.
- (4) Enter the related information the click **OK**. The device will be added successfully.

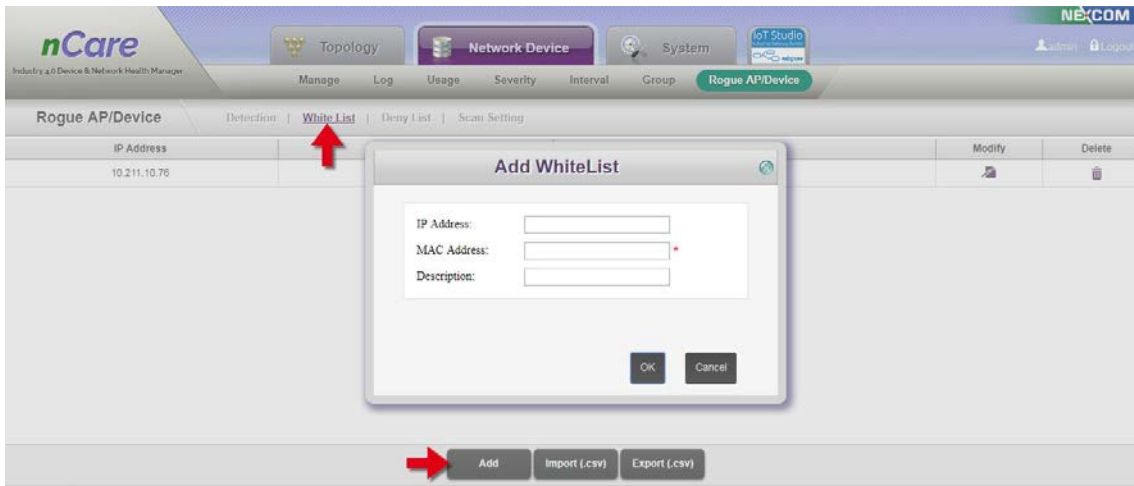


Figure 117 Add to White List Procedure

### 6.7.2.3 Deny List

Rogue device list can be set by this function. The device concatenated under the device on the white list can also be set as rogue device or not.

- (1) The device on white list should be set first. (Please refer to Chapter 6.7.2.2 for the white list)
- (2) Click Add from Rogue Device for searching all devices concatenated under the device on the white list.

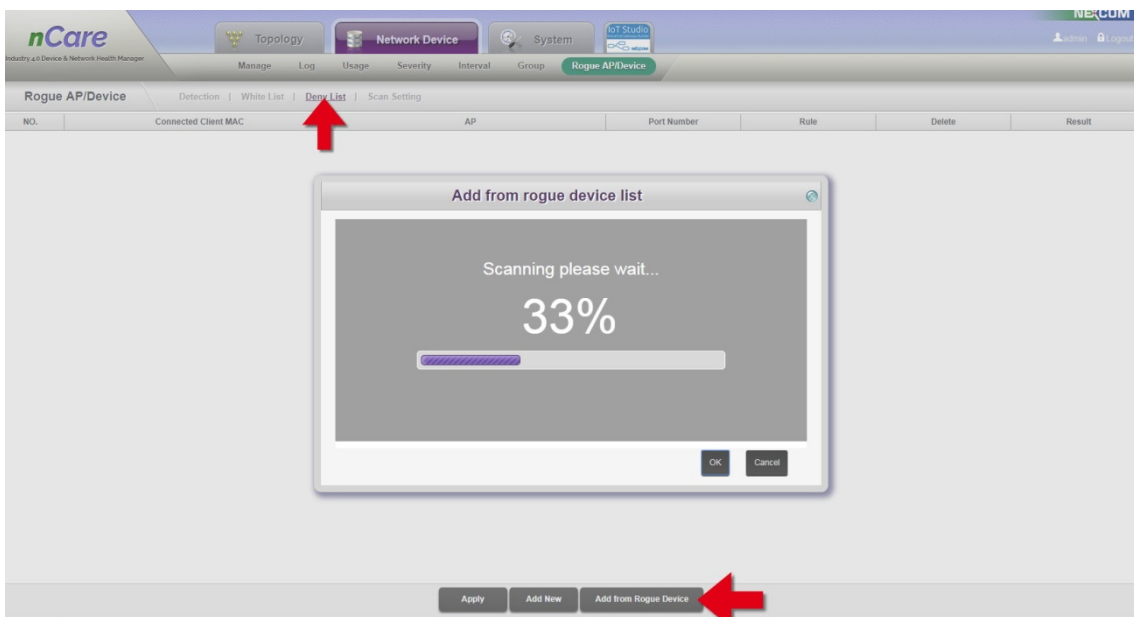


Figure 118 Scanning for White List Devices

- (3) All devices concatenated under the device on the white list will be listed on Add from rogue device list.
- (4) Check for the devices as rogue device.
- (5) Click **OK** to confirm.

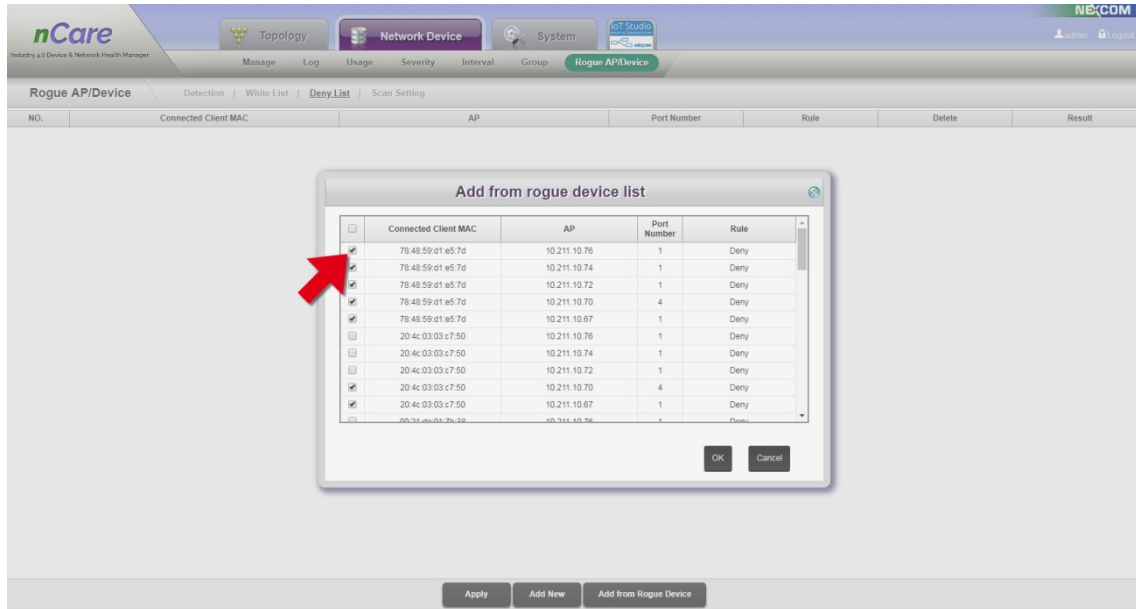


Figure 119 Selection for Rouge Devices that Concatenated under the Device on the White List

- (6) A question mark "?" on the Result column indicates that the setting is still loading to device.

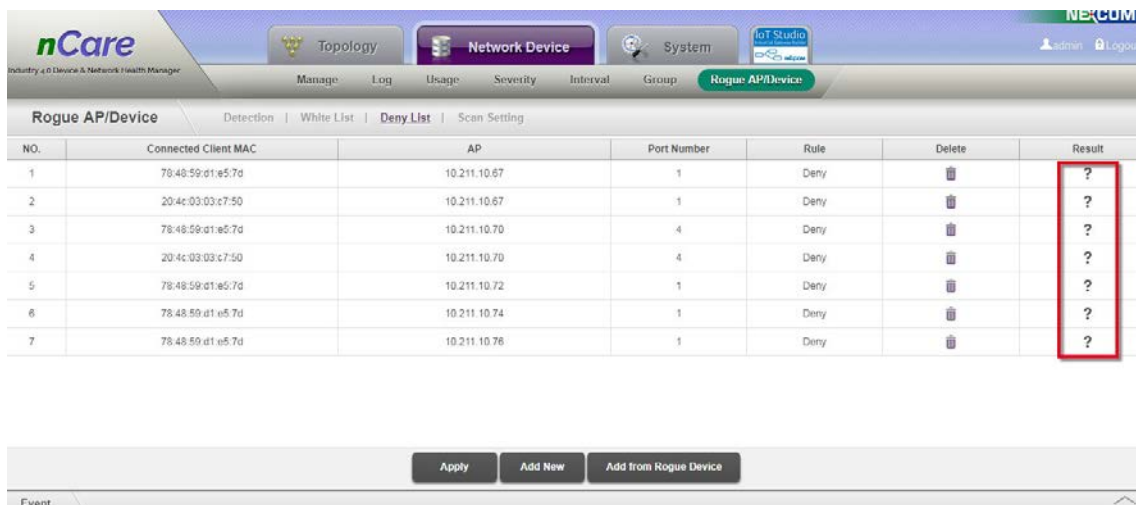


Figure 120 Rogue Device Setting on White List

(7) Click Apply then a "Setting complete" message will pop-out..

(8) Click OK.

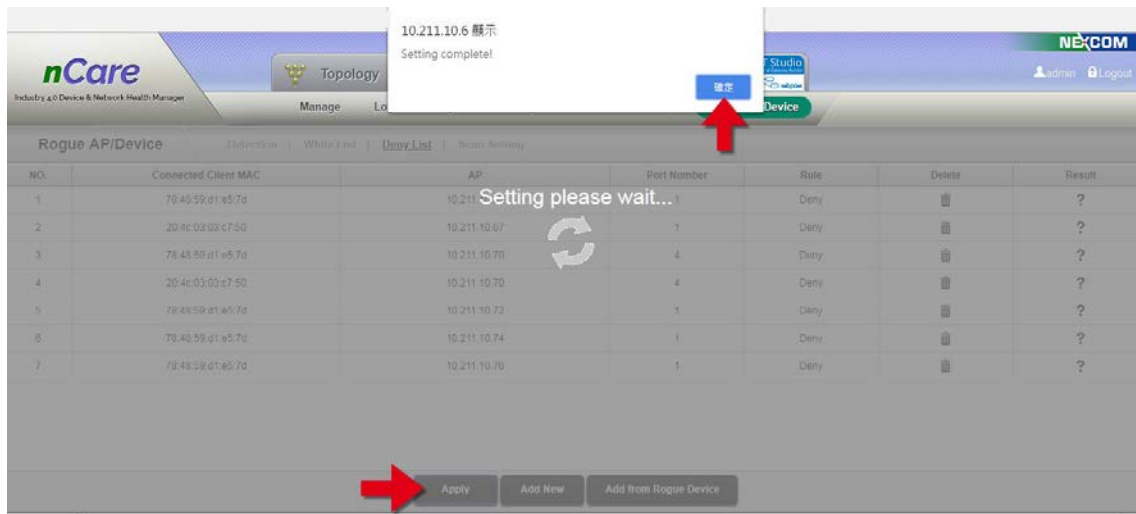


Figure 121 Rogue Device Loading

(9) A mark "✓" on the Result column indicates that the setting is done. A mark "✗" on the Result column indicates that the device is in the white list, it can't be set as rogue device as well. The setting procedure is terminated.

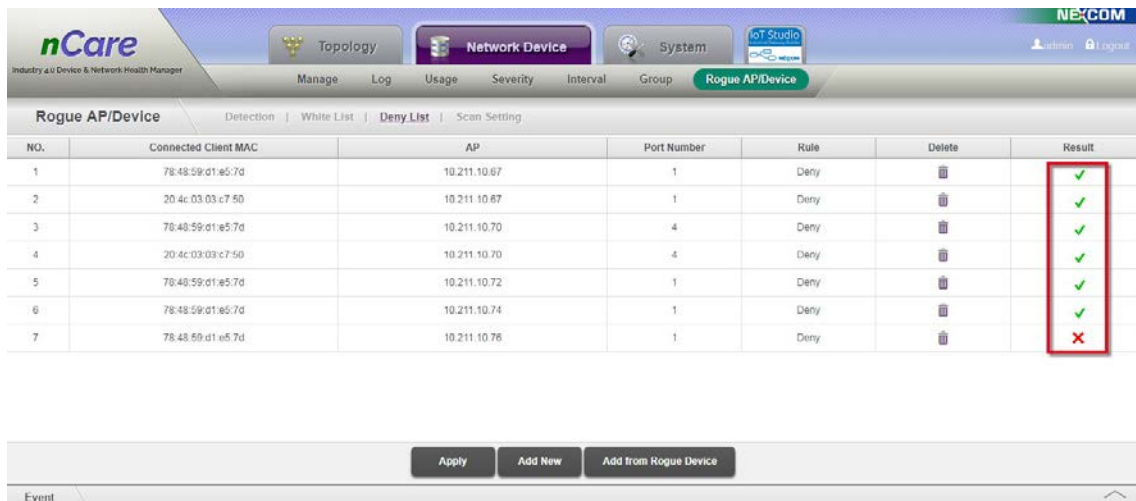


Figure 122 Rogue Device Loading Success

(10)Rogue Device can also be added manually.

(11)Click Add New.

(12) Enter *Connected Client MAC* and *AP*.

(13) Click **OK** to complete setting.

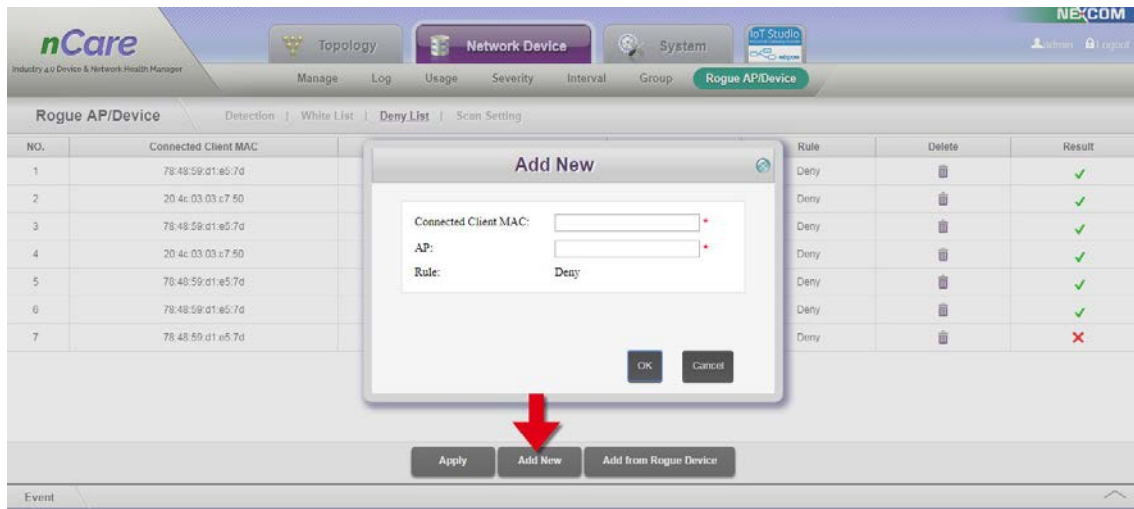


Figure 123 Rogue Device Added Manually

#### 6.7.2.4 Scan Setting

Rogue devices can be automatically detected by nCare. Enter the Rogue Detection Interval in minutes then click **Apply**, the rogue device found by nCare will be shown on Event Log.



Figure 124 Rogue Detection Interval



## 7 Introduction for the Topology Interface of nCare

Topology Interface includes: Device List on the left, View/Discovery/ Status main page on the middle.

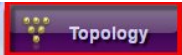
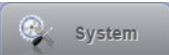
### 7.1 Topology View

#### 7.1.1 Introduction for Topology View

Lines between devices indicate the connection of devices. The colors of lines also imply certain situations. All devices can be surfed, managed and added by the toolbar and shortcut keys on the top.

#### 7.1.2 Operation for Topology View

##### 7.1.2.1 Topology Drawing

Click on    to see all managed devices. (Please refer to Chapter 7.2 for the first-time discovery)

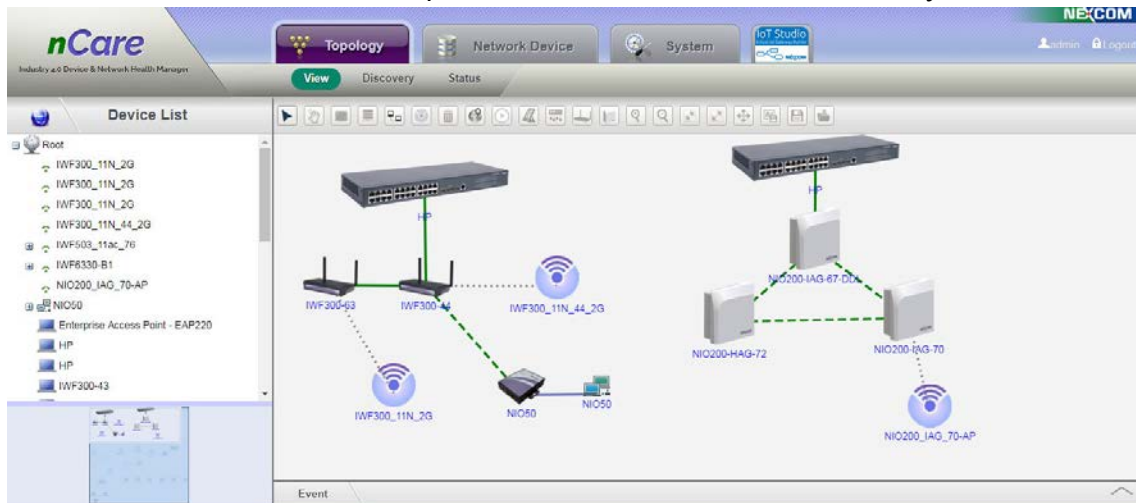


Figure 125 nCare Topology(

##### 7.1.2.2 Icons on Tool Bar for Topology

The functions of icons on Tool Bar are listed as follows:



Figure 126 Tool Bar for Topology

-  Select: This is the default function when entering the Topology.

- (1) The device can be selected or dragged by left-clicking the device icon. The device icon will stop at the last point while releasing the left mouse. Shadow of the device icon indicates that the device is selected.



Figure 127 Device Selection

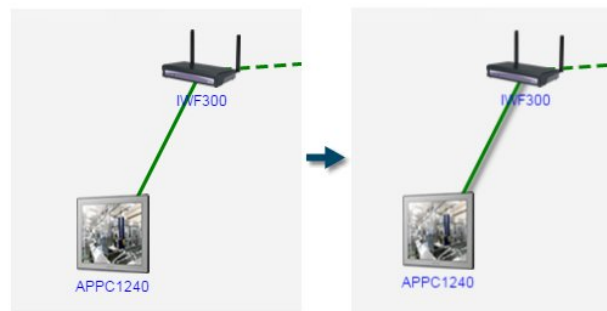


Figure 128 Connection Selection

- (2) Multiple devices can be selected by pressing the Ctrl on the keyboard with clicking the left mouse on those devices.

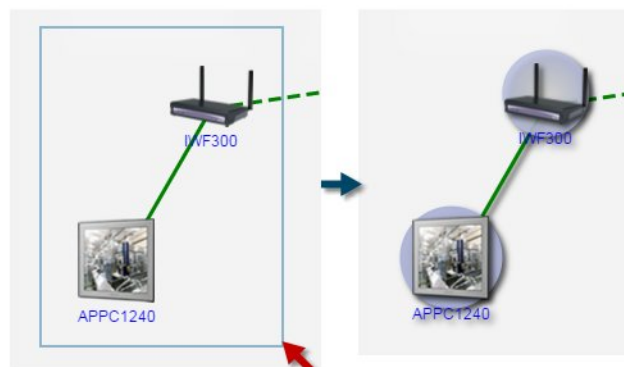


Figure 129 Multiple Devices Selection



Move: Use this function for dragging topology



Create Link: To create a new link between devices. Left-click device A then drag the line to device B. Left-click device B to successfully make a connection between device A and B.



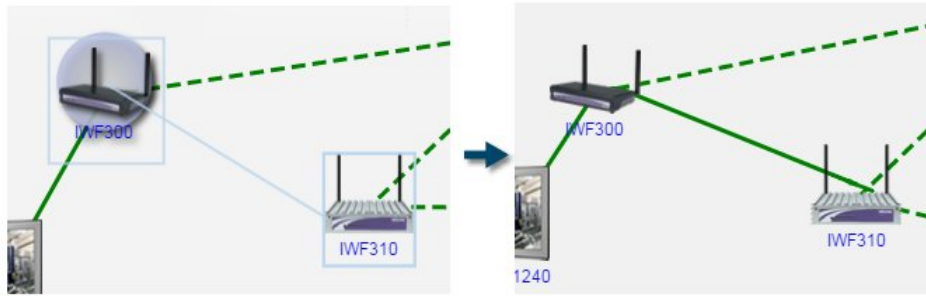


Figure 130 Add Connection



Create Device: To add new device on topology.

- (1) Clicking on the blank part of topology, a **Create Device** window will pop-up.
- (2) Enter and select the information.

Figure 131 Add New Device

- (3) Click **OK** to start discovering.

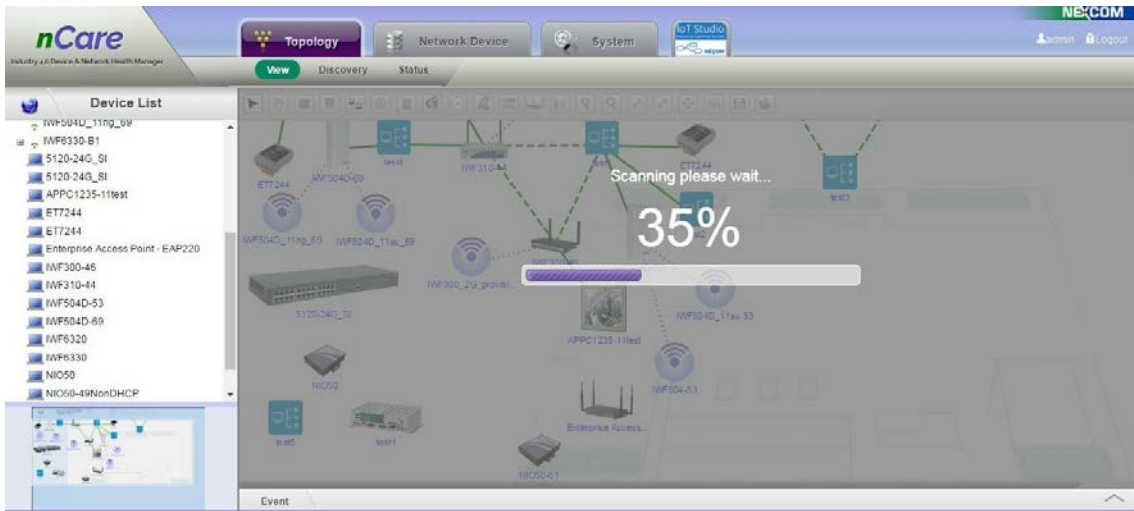


Figure 132 Device Discovery

- (4) If there is no device matched, a window with **New device not found** will pop-up to inform the user.

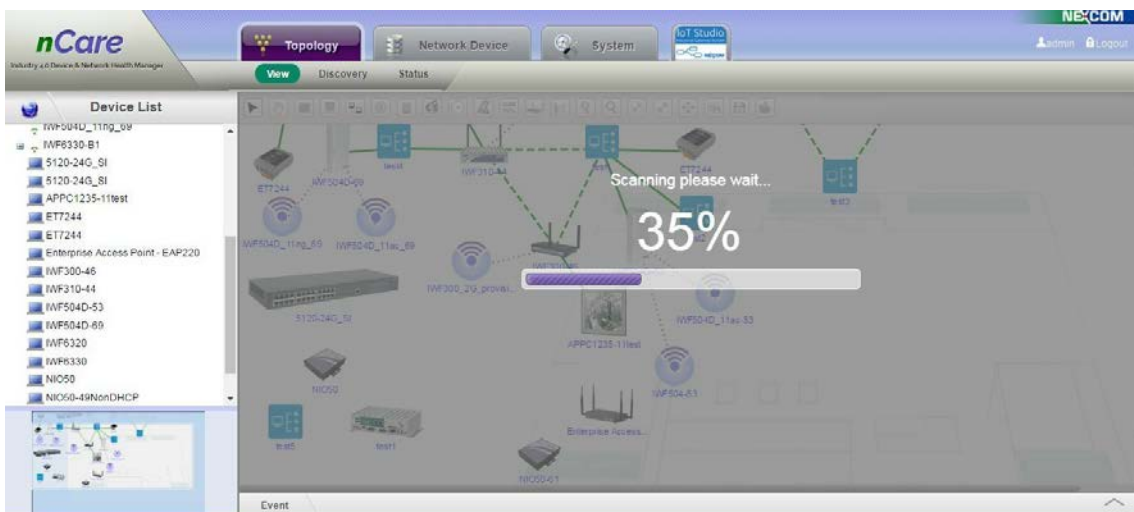


Figure 133 New Device Not Found Window

- (5) If the device can be found, it will show on Topology.

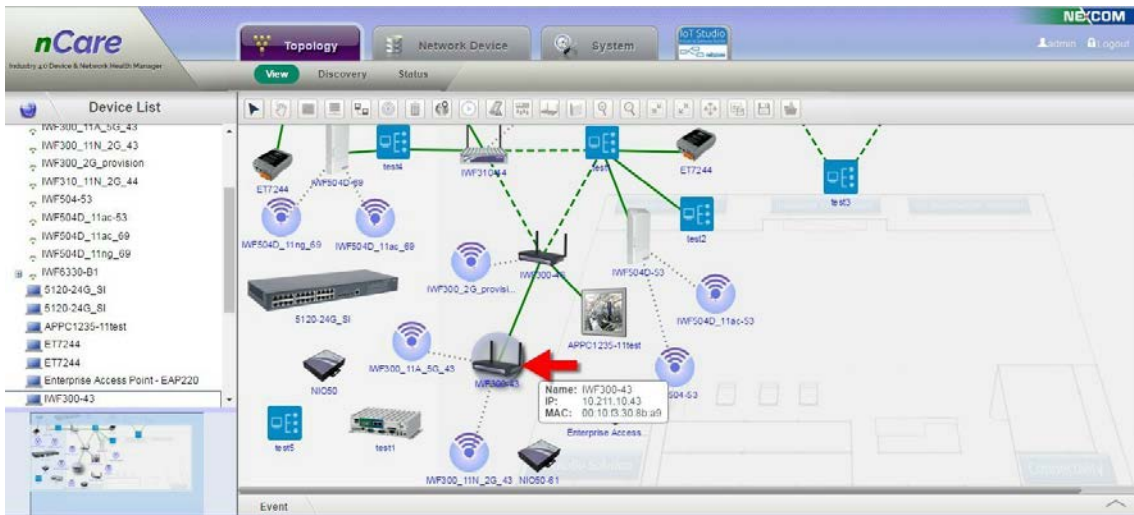


Figure 134 Add Device Successfully

 Add to Topology Group: Classify the device with the same group.

(1) Select two or more devices by , then click .

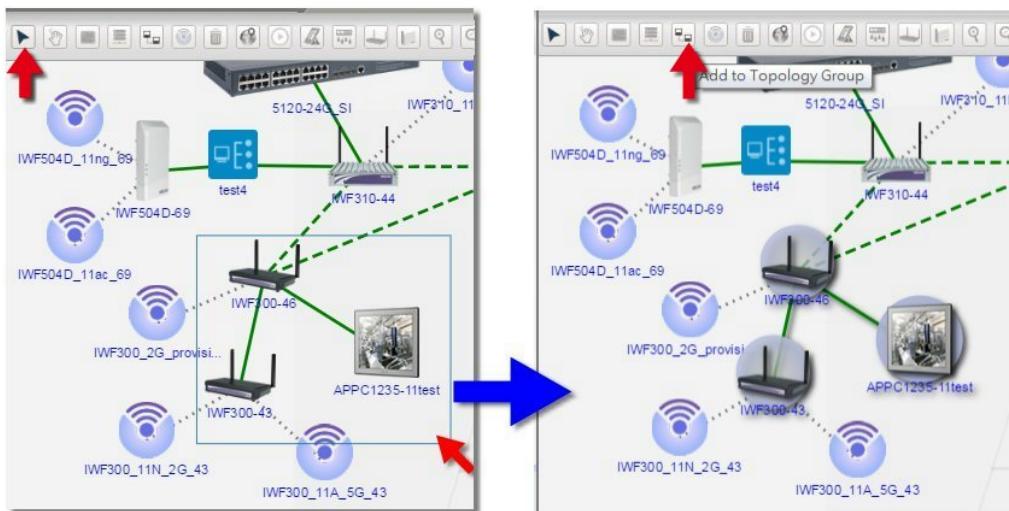


Figure 135 Group Selection

(2) An **Add to Topology Group** window will pop-up. Choose the Topology Group name then click **OK**. (Please refer to Chapter 6.6 for Topology Group setting)

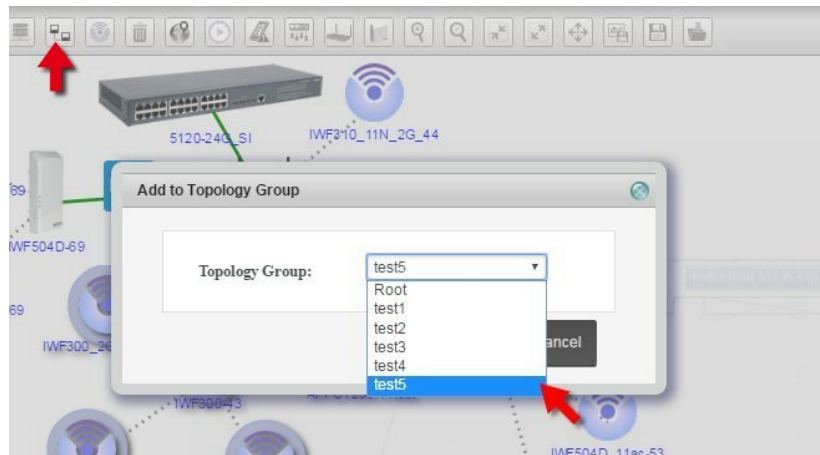



Figure 136 Topology Group Setting

- (3) After the group is successfully added, click  to save the change. Then all selected devices can be seen on this group.

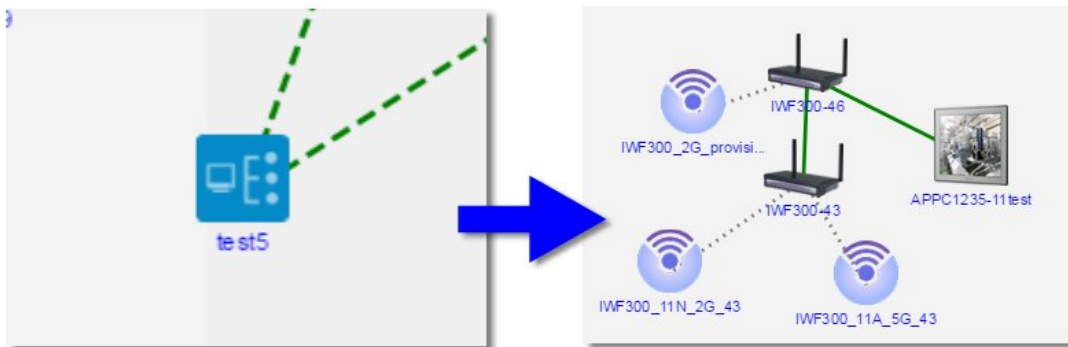



Figure 137 Group Generation

- (4) If the devices need to be removed from the group, please select the device then click . Choose Root as group, then the device can be removed from the group.

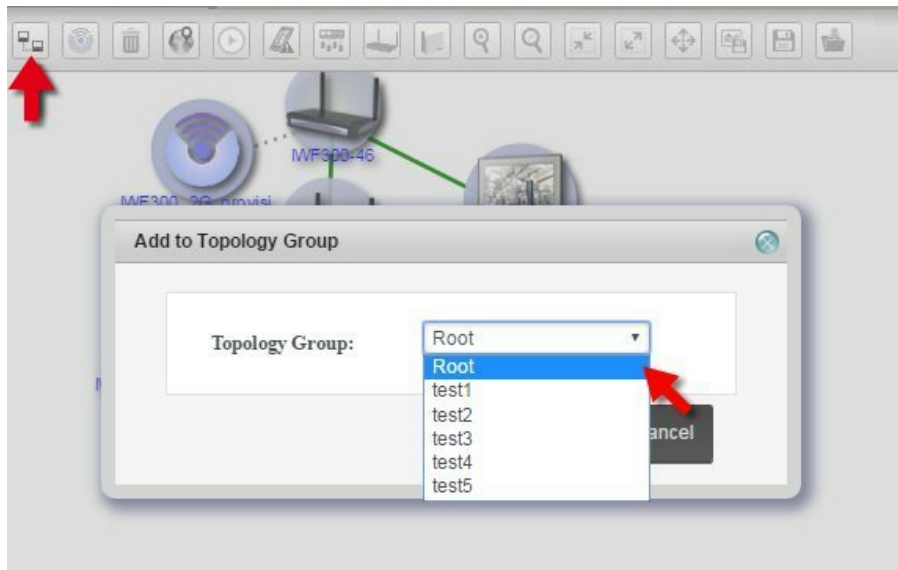




Figure 138 Remove Group

 Add to WiFi Group: Classify the device into WiFi group.

\* WiFi Group: Device such as IWF300, IWF310, IWF503, IWF504D, NIO51 and NIO200 can be added in WiFi Group.

(1) Select the device by , then click .

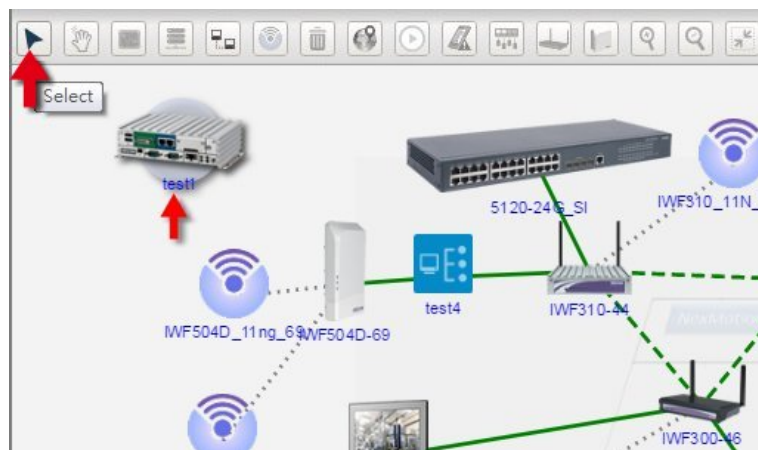



Figure 139 WiFi Group Icon

(2) An **Add to WiFi Group** window will pop-up. Choose the WiFi Group name then click OK. The device will be grouped at .

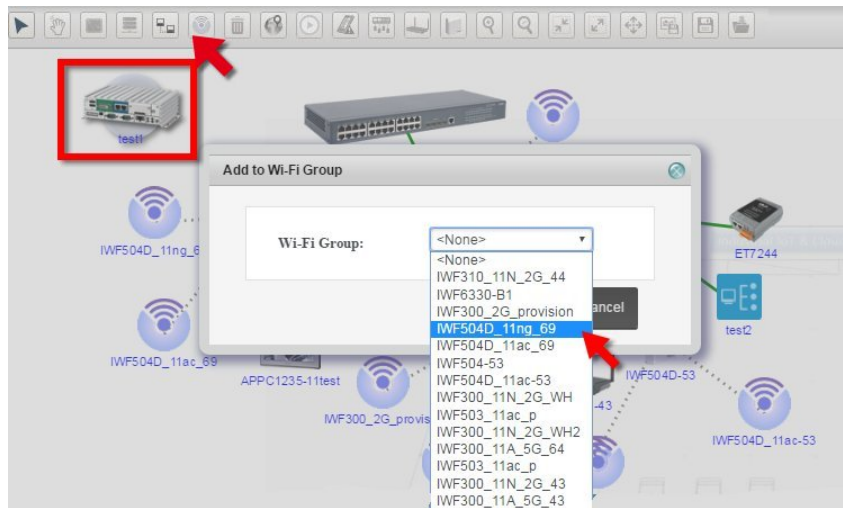


Figure 140 WiFi Group Selection



- (3) If the devices need to be removed from the group, please select the device then click . Choose None as group, then the device can be removed from the group.



Figure 141 Remove from WiFi Group

- (4) There is an icon  shown after entering the WiFi Group. Click this icon to go back to previous page.



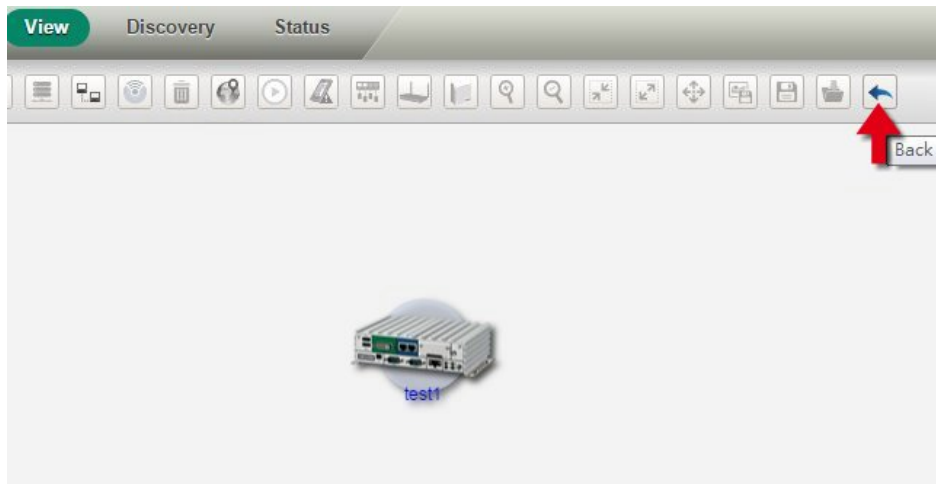





Figure 142 Back to Topology Icon

 Delete: Delete the device or connection. Click  to select device or connection then click . A window will pop-up to inform the user. Click Yes to delete device successfully.

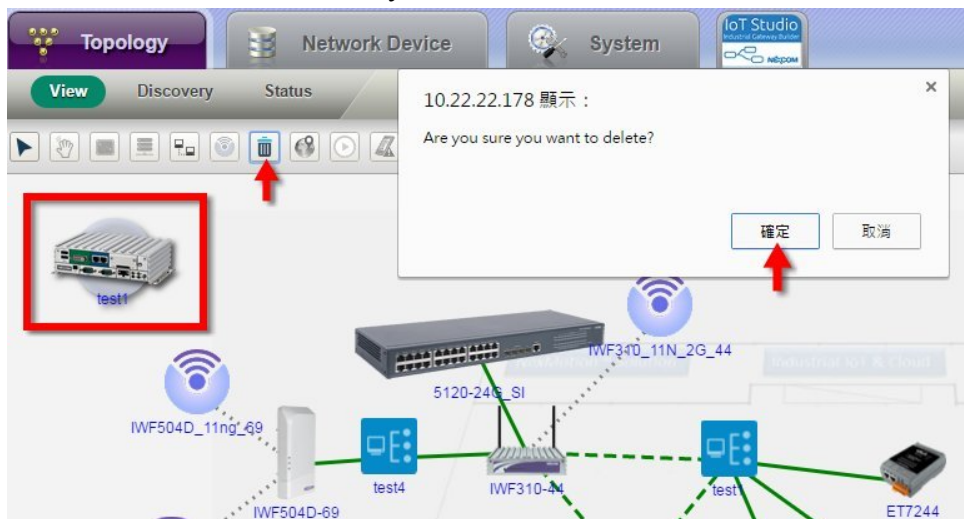





Figure 143 Device Deletion


 Map : Click  icon for Google Map or  icon for Baidu Map. The device can be shown on the map. Scroll up or down to enlarge or narrow the size of the map. If the devices are too close to distinguish, only number of the devices will be shown.


- (1) Please refer to Chapter 6.1.1 Device List and Chapter 6.6 Topology Group. Set the latitude and longitude of device and group first, then the device and group can be shown normally on the map.

- (2) The system should connect with the Internet to show the Google map. Move the mouse to the device icon then the *Device Name*, *Latitude* and *Longitude* can be shown. Click **Back** to original Topology page.



Figure 144 Topology on Google Map

 Traffic Monitoring: The system may monitor multiple traffic of connection. If one or more traffic flow is over the threshold, Administrator will be informed. The setting procedures are list as follows:

- (1) Click  icon and all the connections between all devices can be monitored (Green dash line and green solid line).
- (2) Move the mouse to one of the line, the flow rate can be shown then.

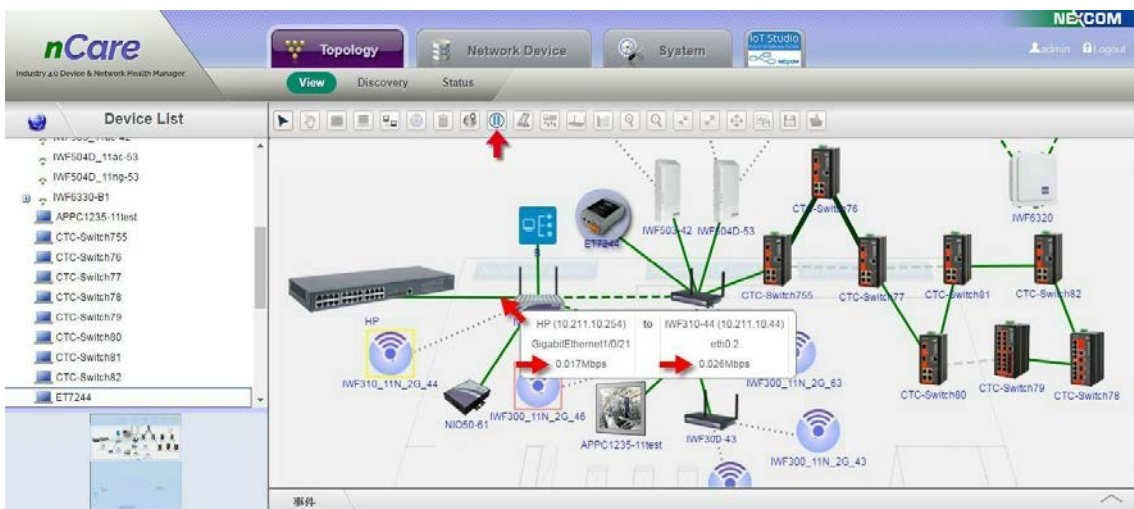


Figure 145 Flow Rate Monitoring



- (3) GREEN bold line indicates that the traffic flow of devices are over 20 MB. The bolder one indicates that the traffic flow of devices are over 100 MB.

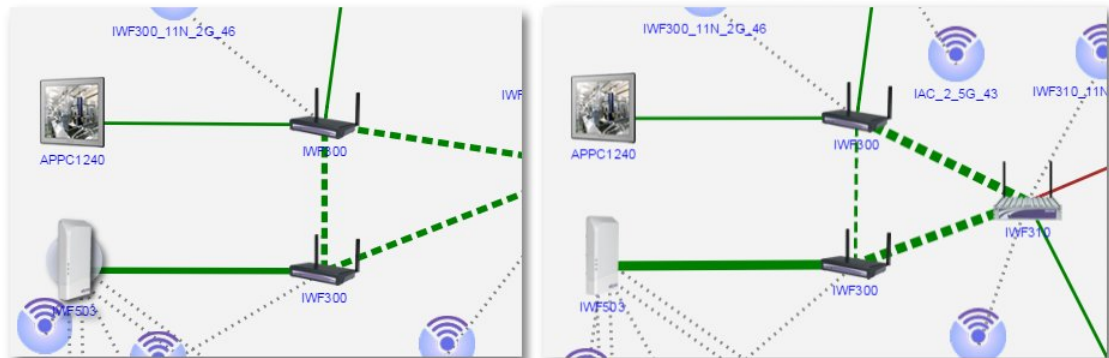


Figure 146 High Traffic Connection

- (4) The system also can set alarm for specific link monitoring to notify users.

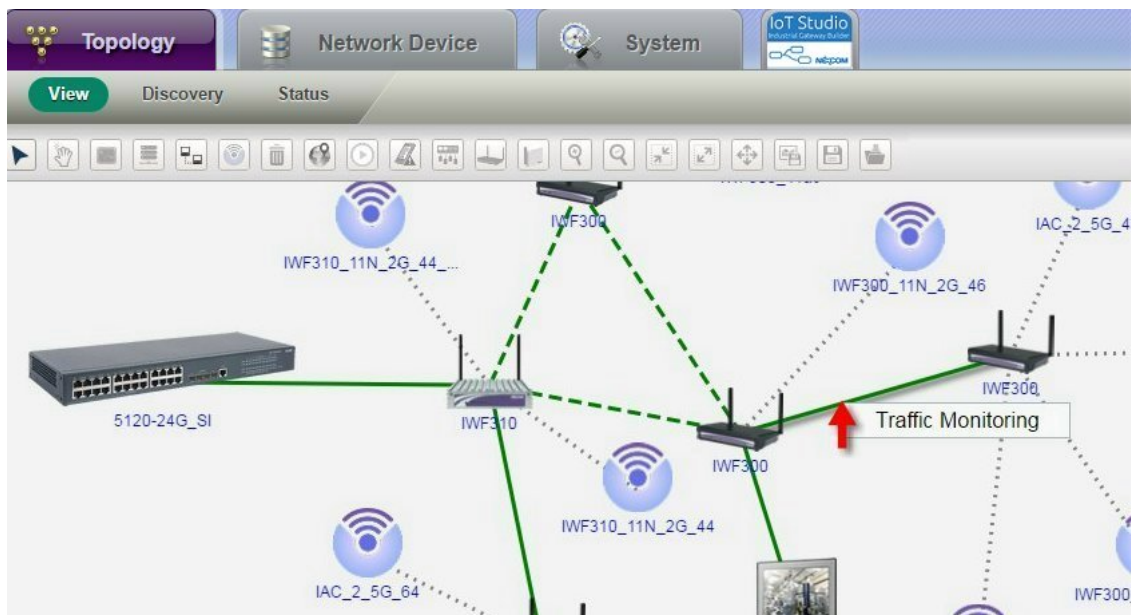


Figure 147 Traffic Monitoring

- (5) Right-click the link to open the pop-up menu and select **Traffic Monitoring**.
- (6) A Traffic Monitoring window will pop-up.
- (7) Check Active.



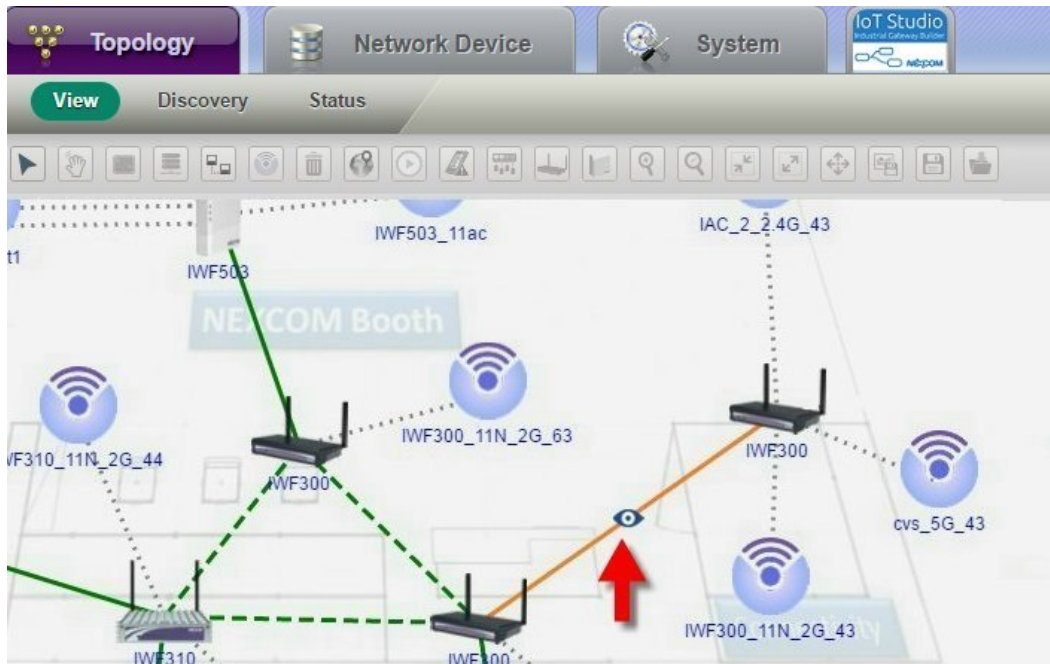


Figure 150 Traffic Over Threshold

- (12) If user want to stop traffic monitoring, uncheck the box of *Active* then click **OK** to cancel monitoring.

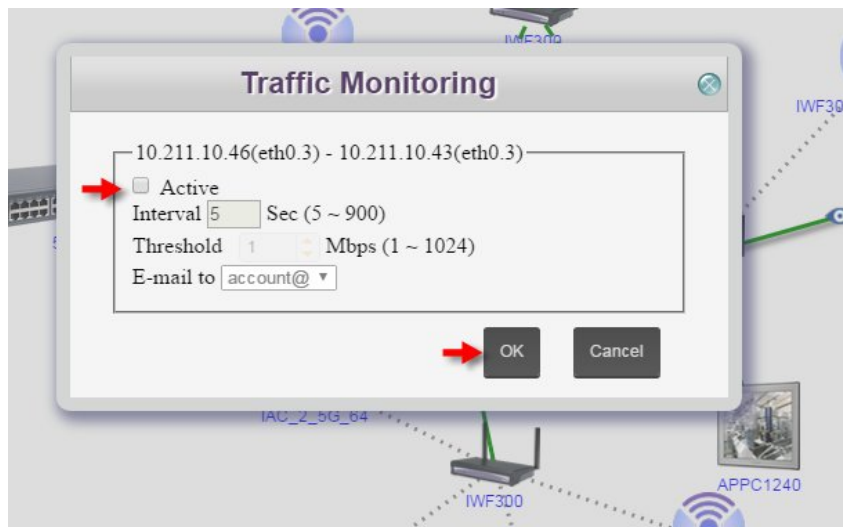



Figure 151 Stop Traffic Monitoring

- (13) Click  for traffic monitoring.
- (14) If the whole Topology traffic monitoring is running with one of the link has been set for traffic alarm, the link will become **ORANGE** bold line while the traffic flow is over the threshold. An alarm message will also be sent to manager.

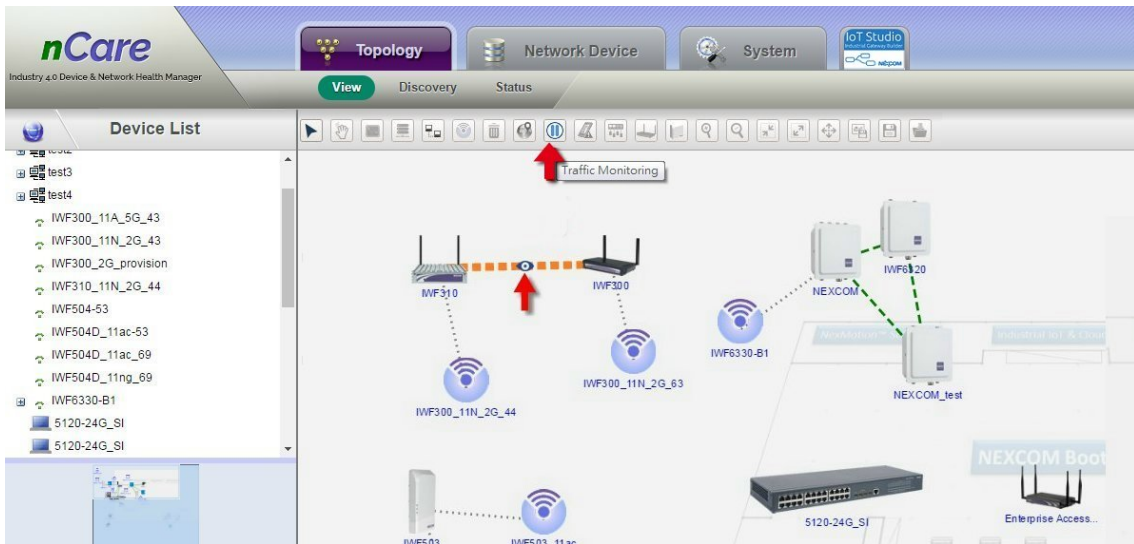



Figure 152 Two Traffic Monitoring Simultaneously

 Show/Hide Rogue Devices: Click to show/hide rogue devices not in the White list (Please refer to Chapter 6.7.2.2). There will be an exclamation mark at the side of the device icon.

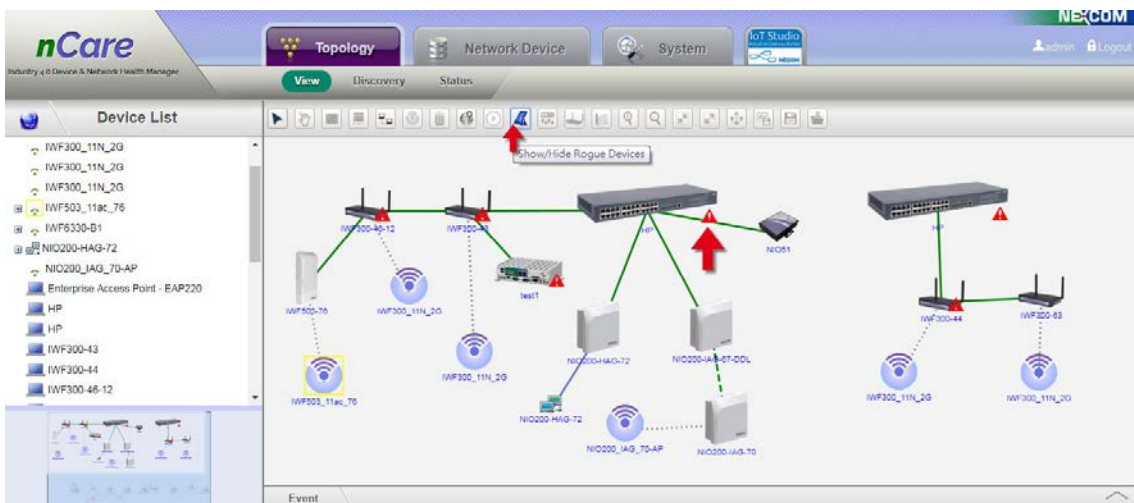



Figure 153 Show/Hide Rogue Devices Icon

 Switch VLAN: Click the icon and a VLAN list can be chosen. Choose one and the Topology will be shown with Switch VLAN.



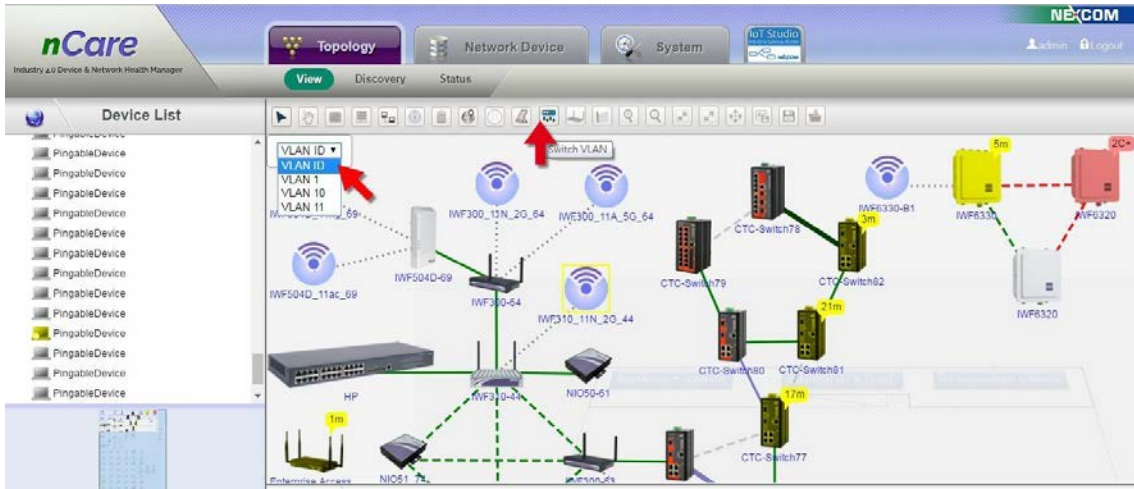


Figure 154 VLAN Selection

(1) BLUE line indicates the deployment of the selected VLAN.

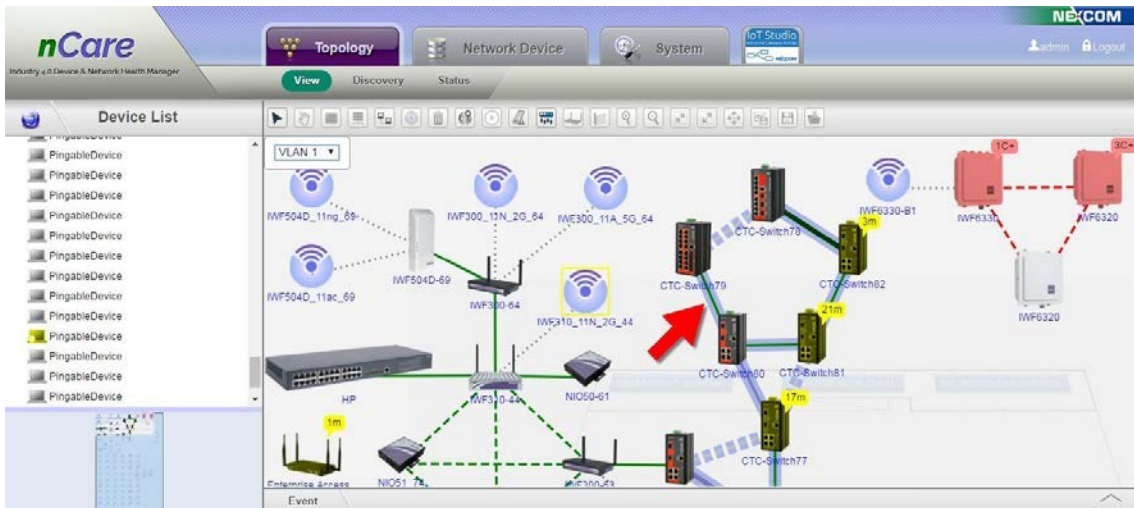



Figure 155 VLAN Topology

 Update AP: IWF AP can be updated by this function.

(1) Click .

(2) If there is no AP selected, and an “Are you sure you want to update ALL IWF APs” window will pop-out. Click **OK** to proceed update.




Figure 156 IWF AP Update

- (3) If non-IWF AP is selected, and an “IWF AP not found” window will pop-out. User should choose an IWF AP to start update.



Figure 157 IWF AP Not Found

- (4) Select one or more IWF AP and click .
- (5) The selected device(s) will be updated.

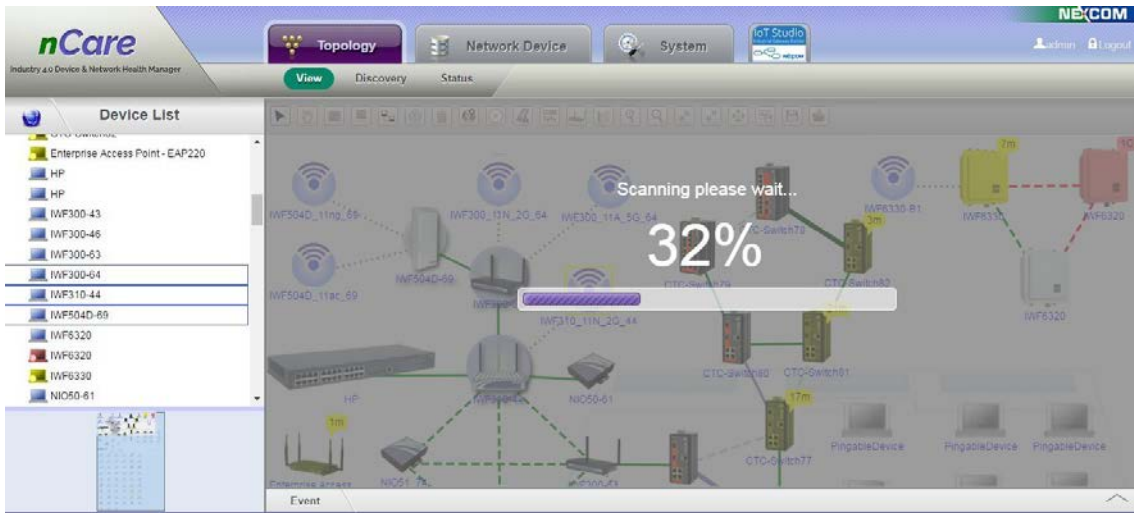



Figure 158 IWF AP Update

 Update IWSN: NIO200 series devices can be scanned and updated by this function.

- (1) Right-click NIO200-HAG device icon.
- (2) Choose Config > Account Setting.

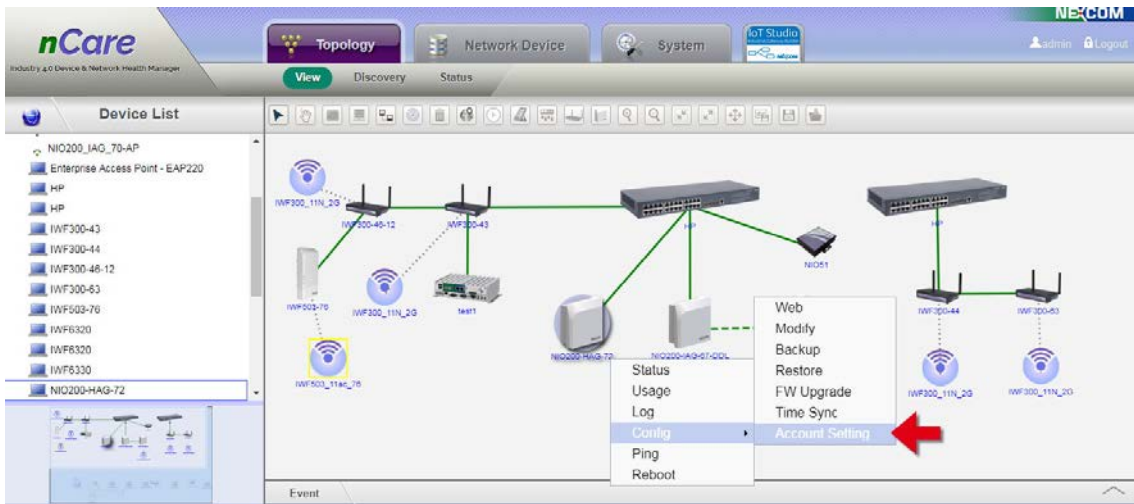


Figure 159 Account Setting for NIO200-HAG Series Devices

- (3) An Account Setting window will pop-out.
- (4) Enter *Name* and *Password*.
- (5) Click **OK** to complete setting.

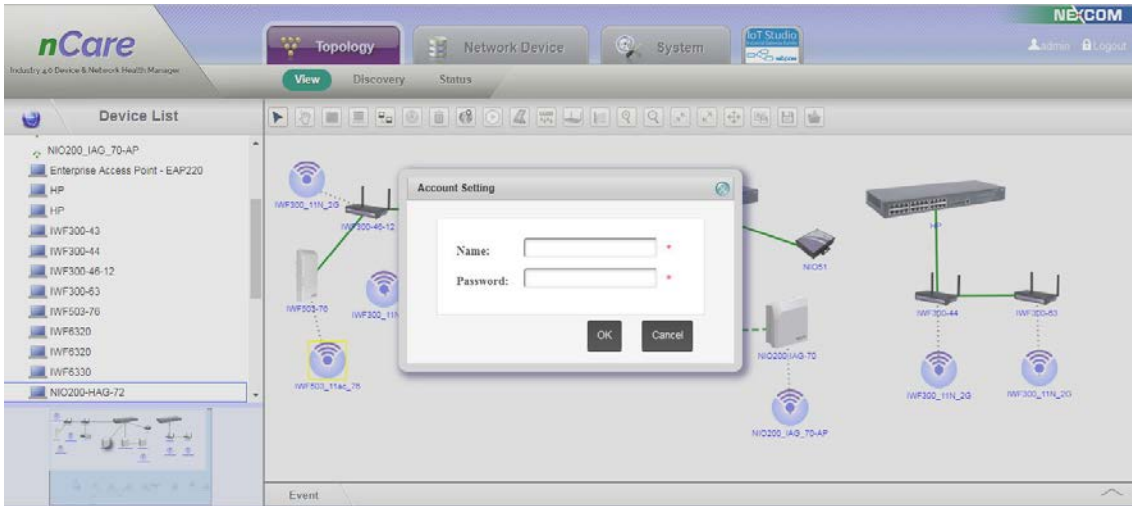


Figure 160 Account Setting Window for NIO200-HAG

- (6) A “Set Successfully” window pops-out indicates that nCare has already connected with NIO200-HAG device successfully.
- (7) However, a “Set Failure” window pops-out indicates that the account password is wrong. Please confirm the password and re-login again.

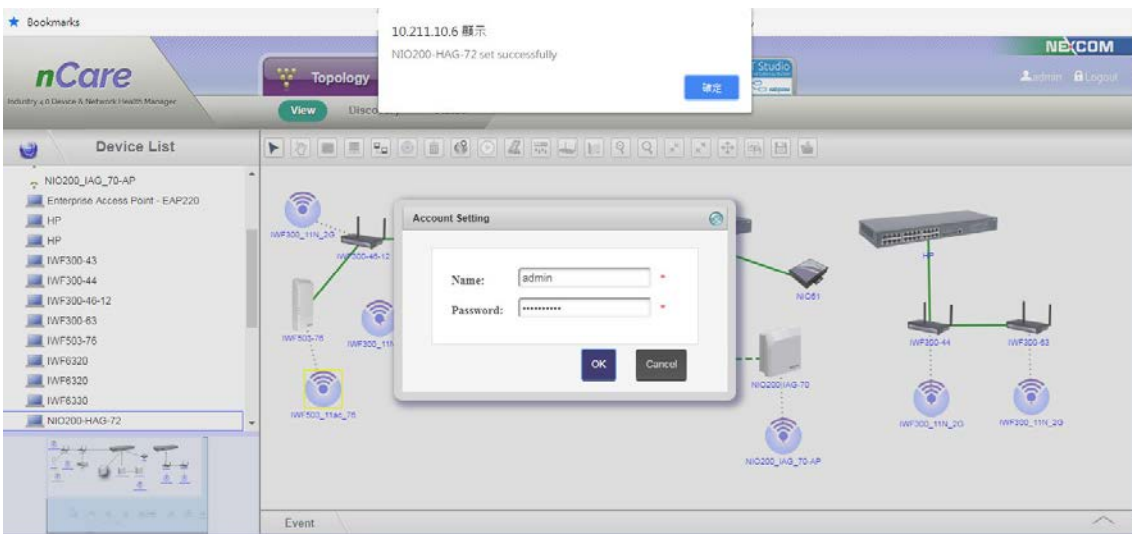



Figure 161 NIO200-HAG Account Setting Success

- (8) Click  icon for updating IWSN.



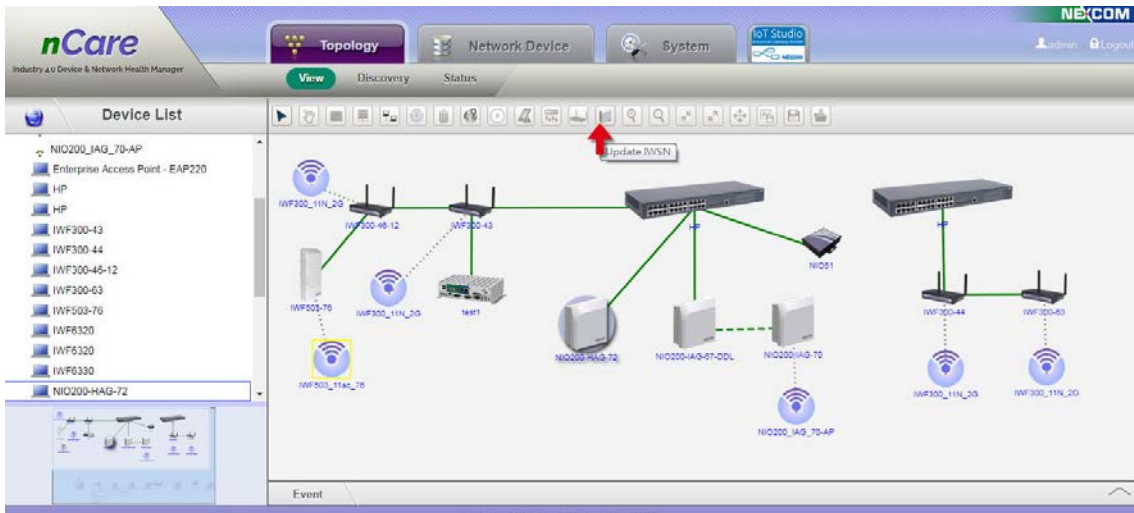


Figure 162 IWSN Update

(9) nCare is then scanning for NIO200-HAG devices.

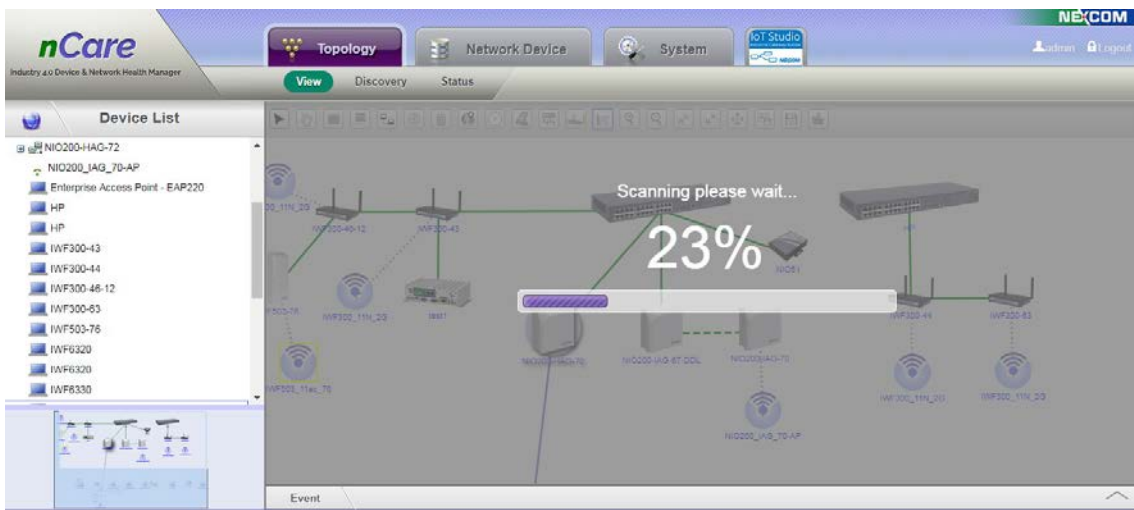


Figure 163 Scanning for NIO200-HAG Devices

(10) Device Group connected under NIO200-HAG devices with WirelessHART are scanned.

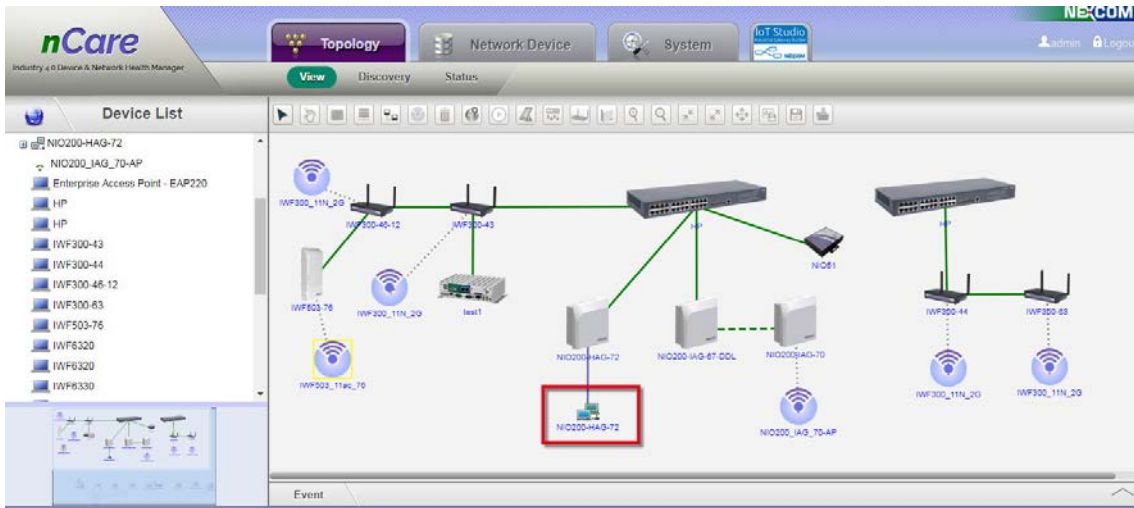


Figure 164 Scanned Device Group under NIO200-HAG Devices

(11) Double-click Device Group icon to see this Sensor Group.

(12) Move the cursor to the device icon, the device information will be shown.

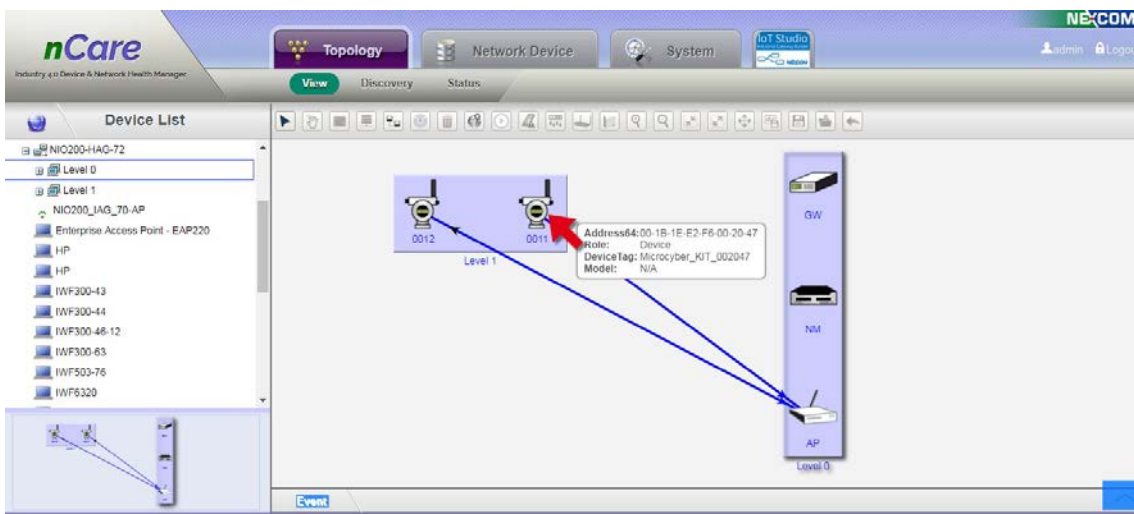


Figure 165 Check for NIO200-HAG Group Devices

(13) If the NIO200-HAG group device is disconnected, the line will become **RED** to inform user.

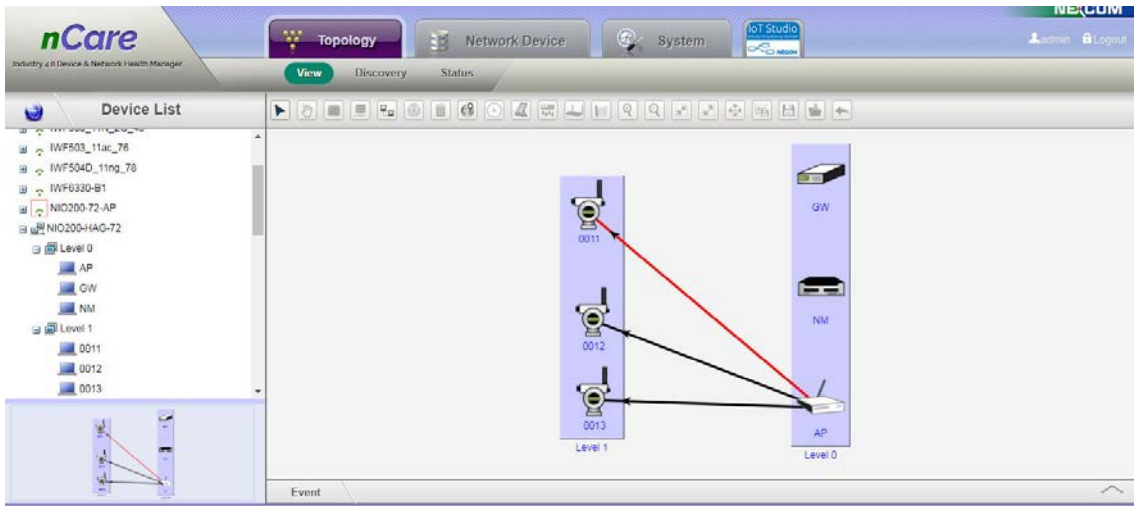


Figure 166 NIO200-HAG Group Devices Disconnected

(14) For NIO200-IAG series devices, the account setting procedure is the same as NIO200-HAG.

(15) After the account is set successfully, click  icon for update IWSN.

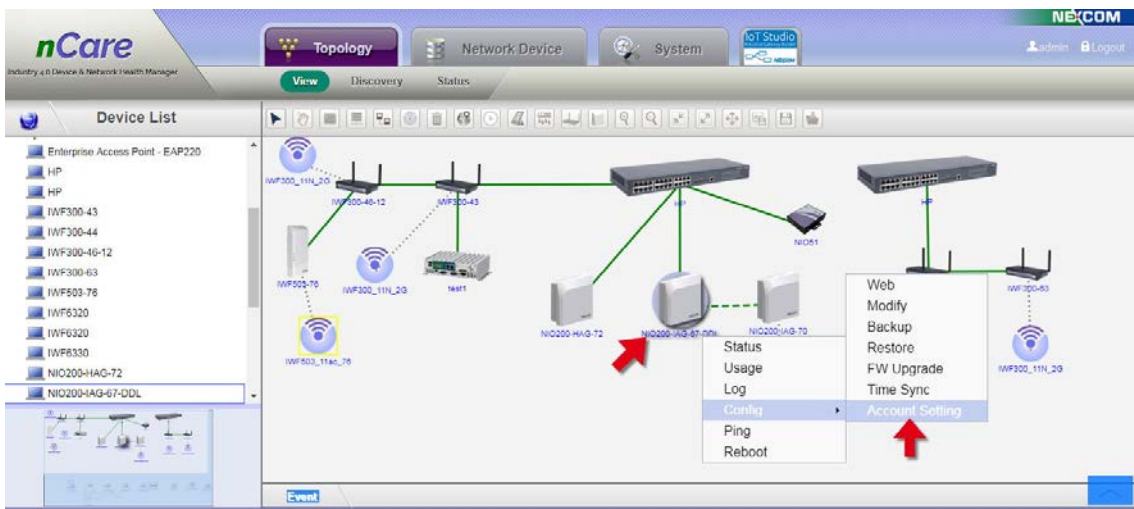


Figure 167 Account Setting Window for NIO200-IAG

(16) ISA100 group devices of NIO200-IAG will be scanned after updating IWSN.

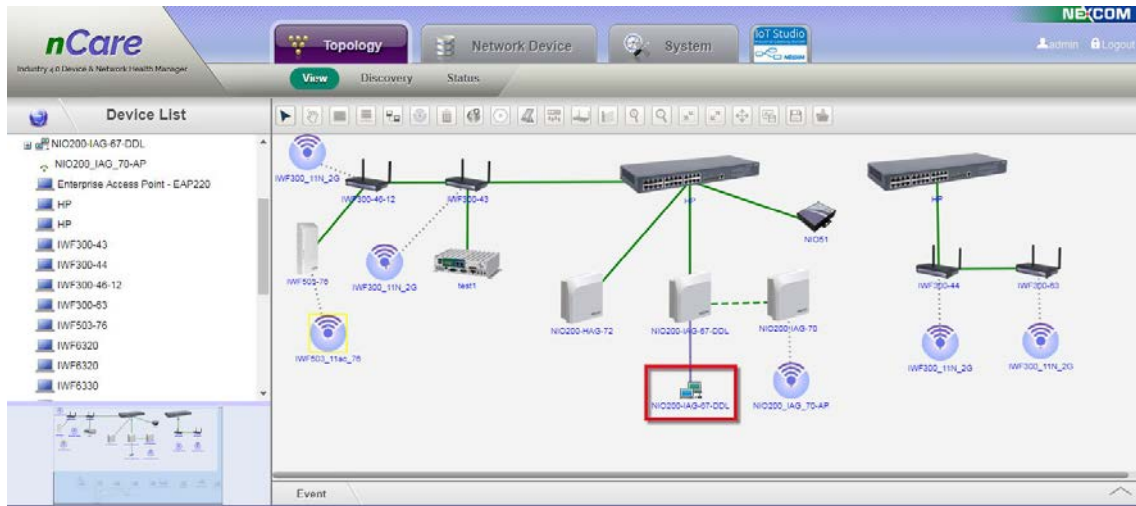


Figure 168 Scanned ISA100 Device Group of NIO200-IAG.

(17) Double-click ISA100 Device Group icon.

(18) Move the cursor to the device icon, the device information will be shown.

(19) If the group device is disconnected, the line will become RED to inform user.

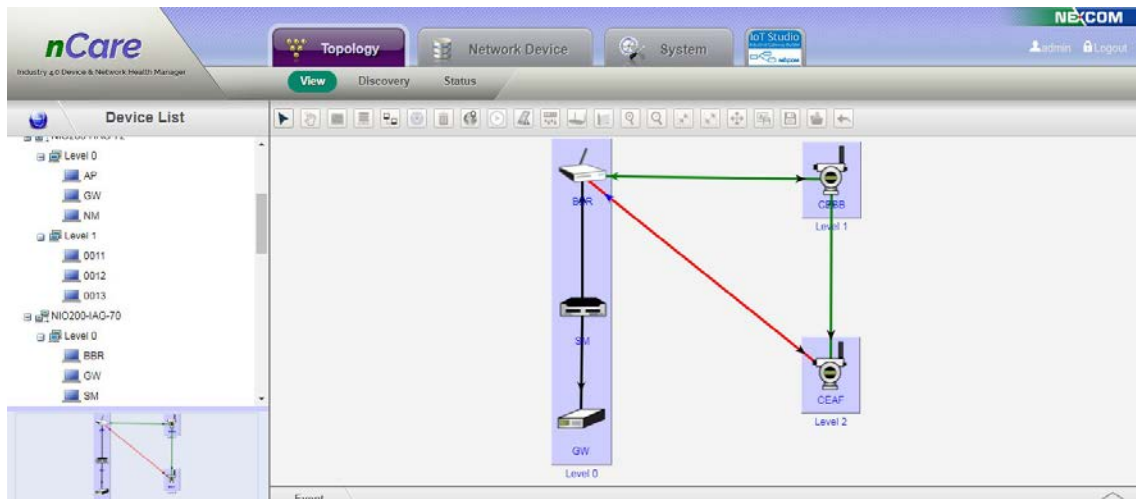


Figure 169 Check for ISA100 Device Information

(20) Time zone can be set for NIO200.

(21) Right-click NIO200 device icon, choose Config > Time Sync

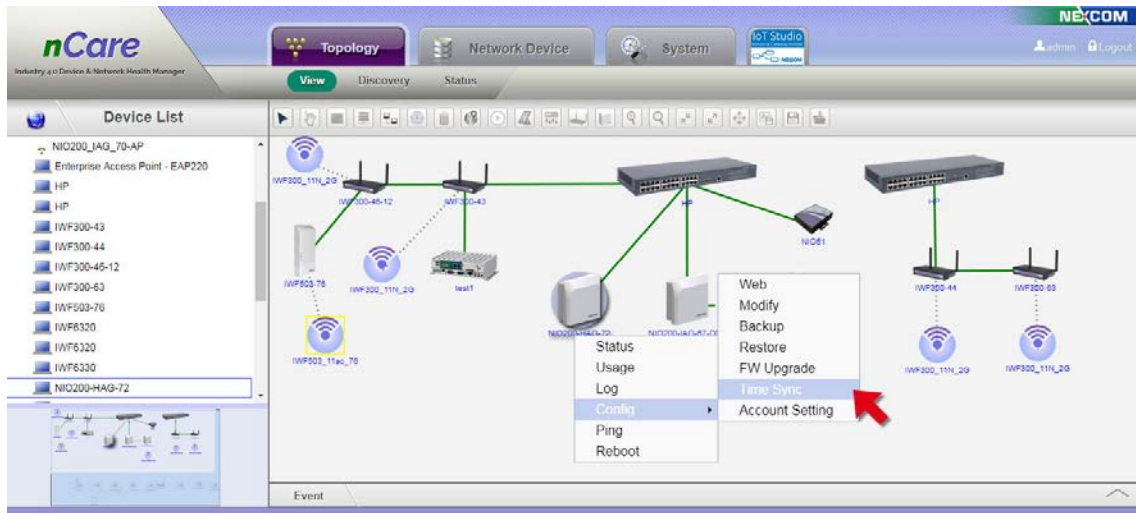


Figure 170 Time Zone Setting for NIO200 Series Devices

(22)A “Time Sync” window will pop-out.

(23)Scroll down to choose the time zone.

(24)Click **Sync with browser** to complete setting.

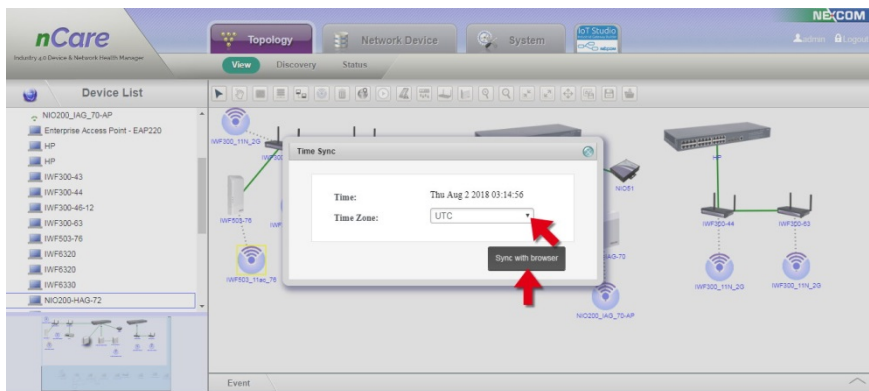










Figure 171 Time Zone Sync with Browser

-  Zoom In: Click to zoom in the Topology View.
-  Zoom Out: Click to zoom out the Topology View.
-  Zoom Overview: Click to see the whole topology.
-  Zoom Reset: Click to see the Topology with original size.
-  Full Screen: Topology will be shown in full screen. Click **ESC** or  to back to the main page of system.
-  Export to Image: This function can export topology map at a new



window. Right-click to save as a png format file.

 Save Topology: The Topology can be saved. Click this icon then click **OK** on the pop-up window to complete saving.

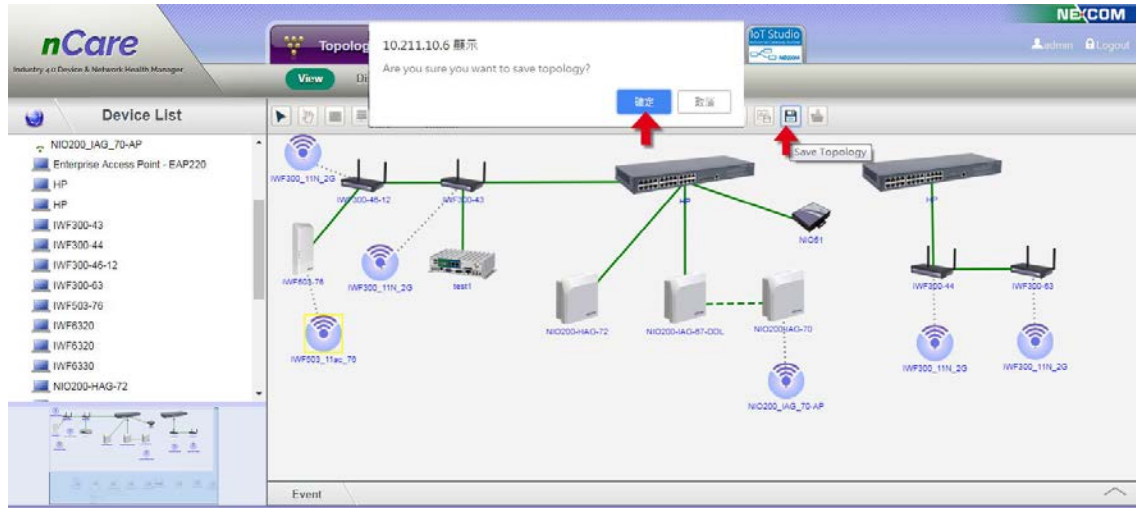




Figure 172 Save Topology

 Load Topology: If the user has revised the topology and want to recover from the previous status, just click  icon and click **Yes** on the pop-up window. The topology will be recovered then.

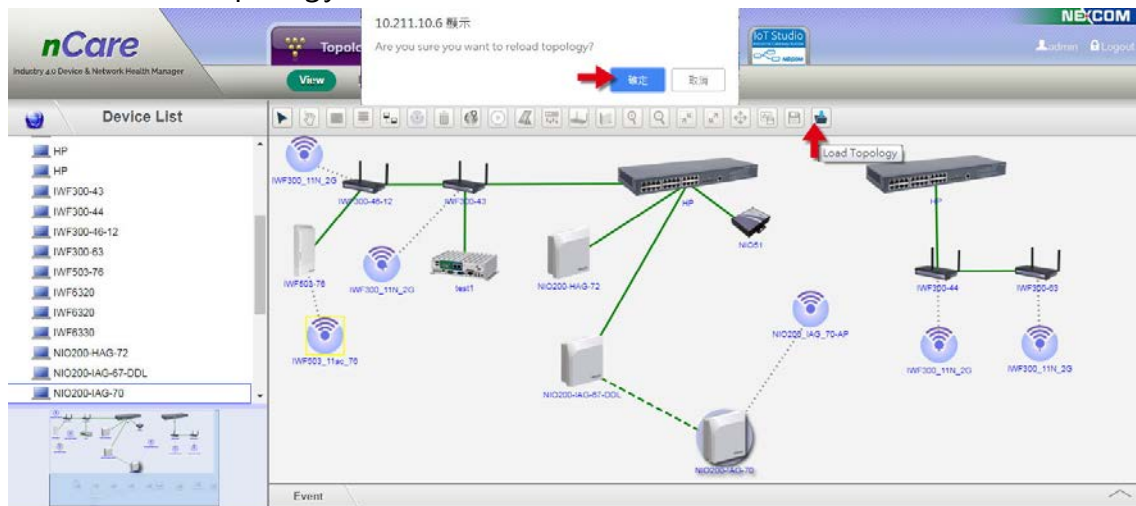



Figure 173 Load Topology

 Update Device Server: Click on device model **NIO50** and **NIO51**. A hidden icon will be shown. The operation procedures are list as follows:

- (1) Click on NIO50 or NIO51 device icon then click  icon.

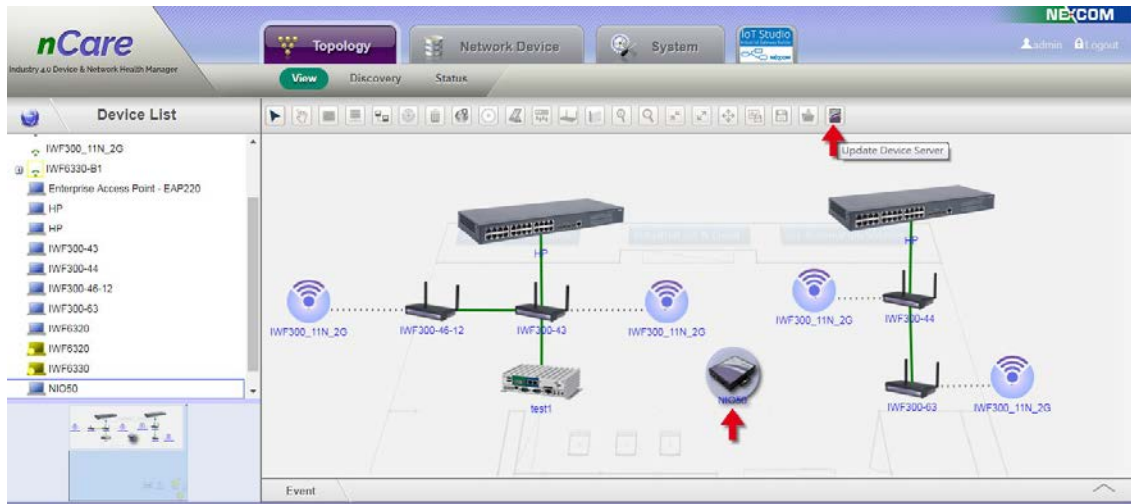


Figure 174 Update NIO50 Device

- (2) A "Please set Modbus ID" window will pop-out. The number of PLC devices deployed with NIO50 device should be set first.

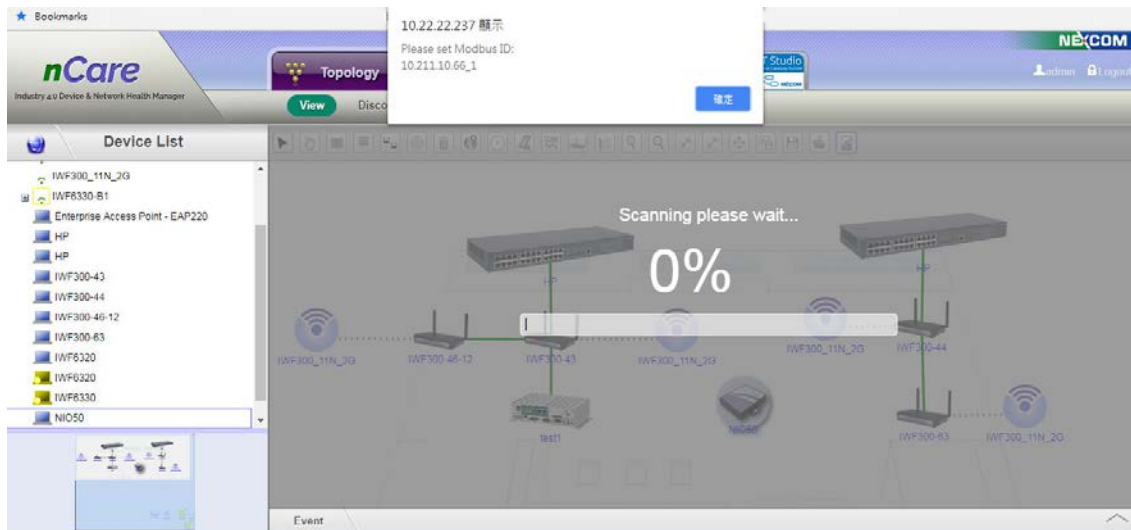


Figure 175 Modbus ID Setting

- (3) Right-click the NIO50 device icon to enter Modbus ID Setting.

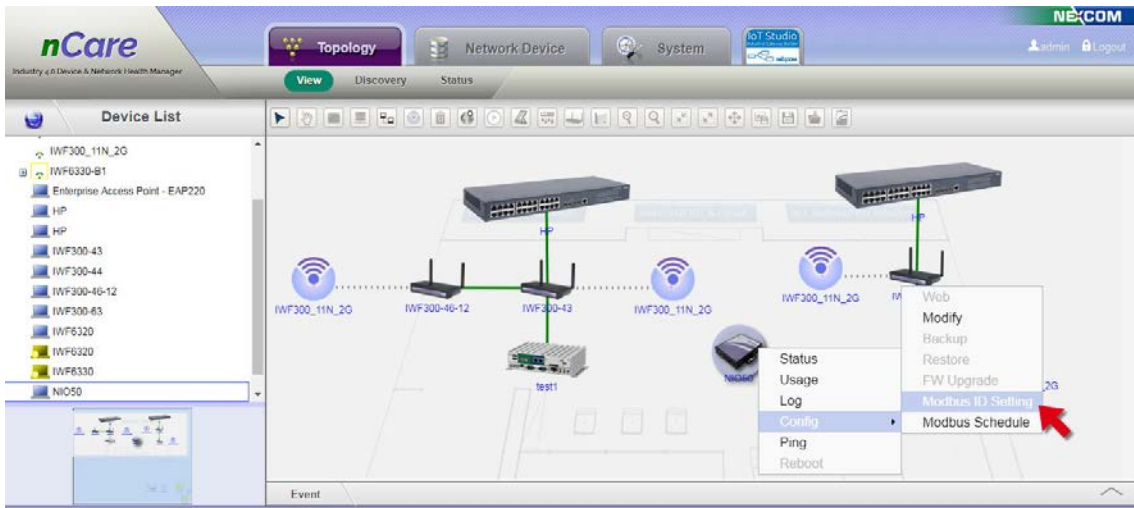


Figure 176 Modbus ID Setting for NIO50 Device

- (4) A “Modbus ID Setting” window will pop-out. Enter the *Device ID* (1~254) then click **OK**.
- (5) Check the Device ID then click **Delete** to delete the selected *Device ID*.

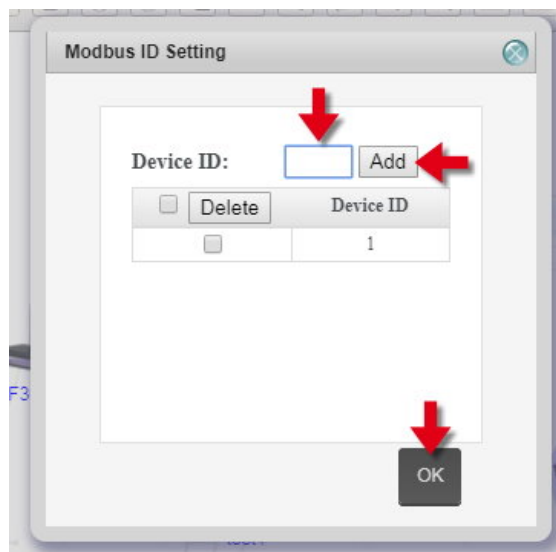


Figure 177 Modbus ID Setting Window

- (6) Select the NIO50 device then click  System will scan for updating.



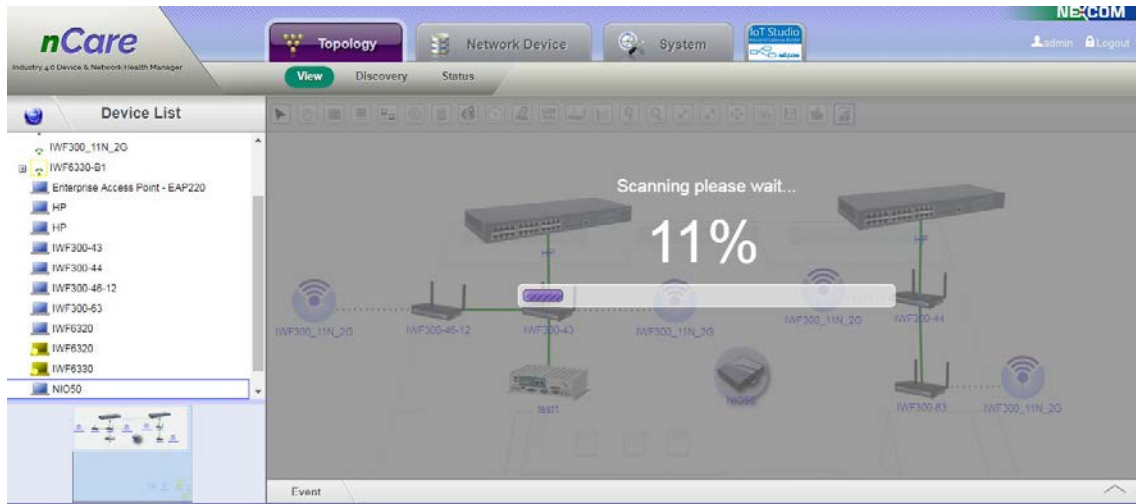


Figure 178 NIO50 Device Updating

(7) NIO50 device will be added into its WiFi Topology Group.

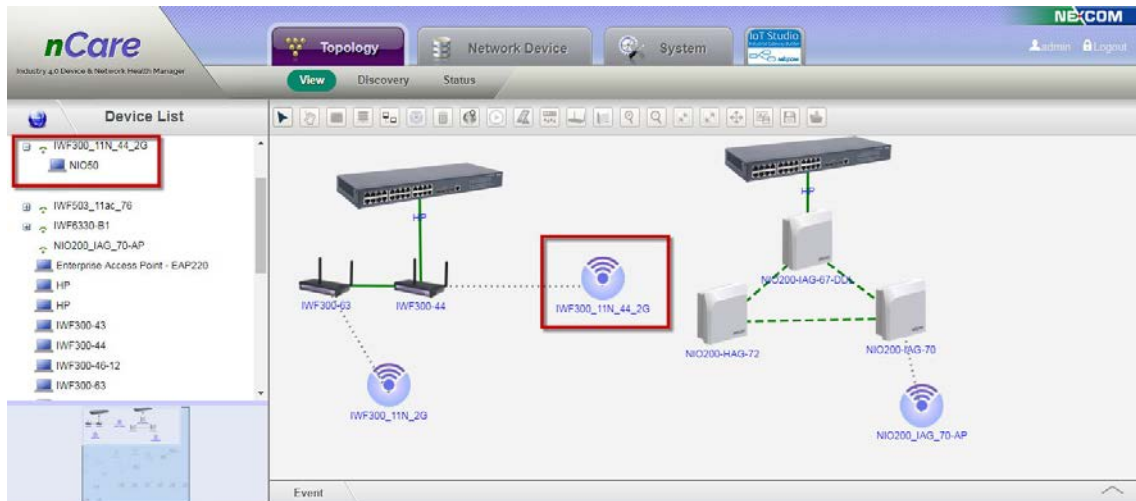


Figure 179 Adding NIO50 Device to Topology Group

(8) Double-click the group icon to check NIO50 device and the PLC device group.

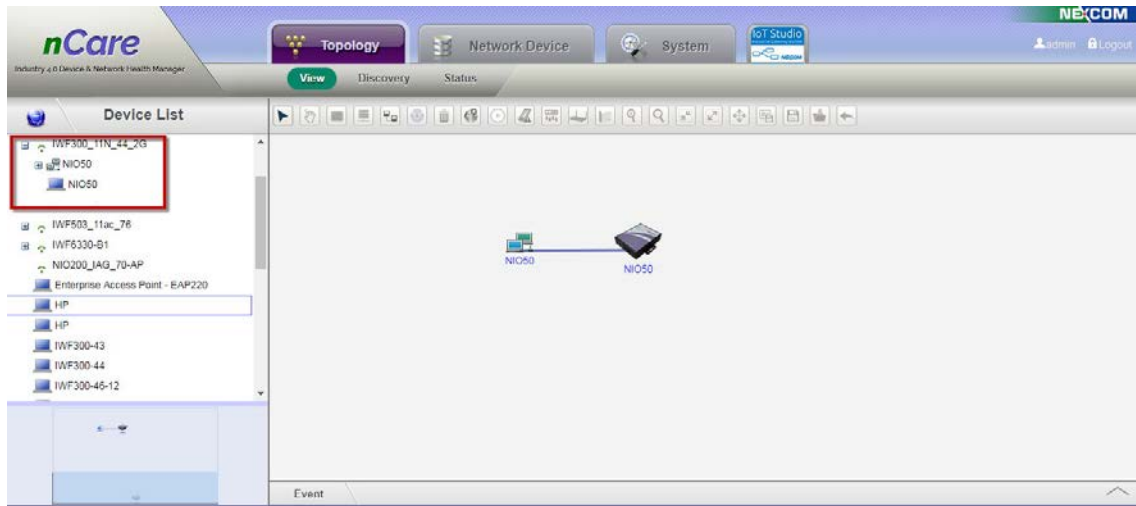



Figure 180 Devices in Topology Group

(9) Double-click the PLC group icon to check PLC devices. Click  to back to upper-layer.

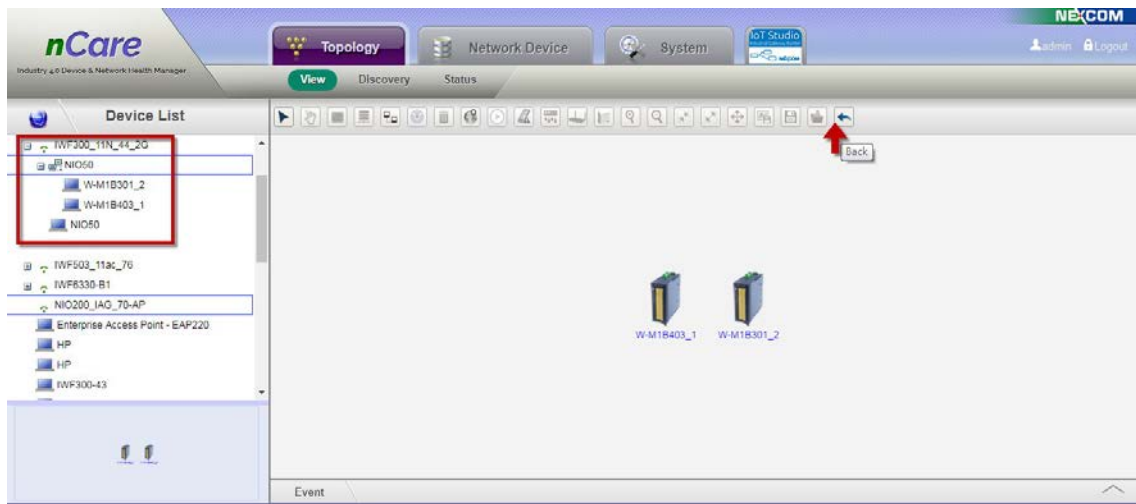


Figure 181 Devices in PLC Group

(10) Right-click the device icon then click **Status**. *Device Status* can be shown as table.

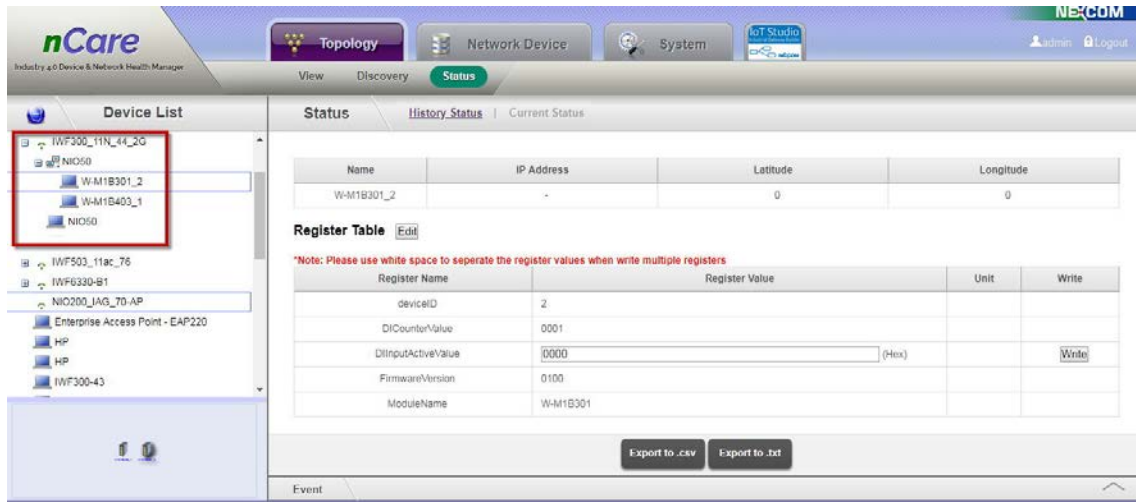


Figure 182 Devices Status for PLC Device

(11) Right-click the device icon and choose Config > Modbus Schedule.

(12) PLC data can be updated with schedule.

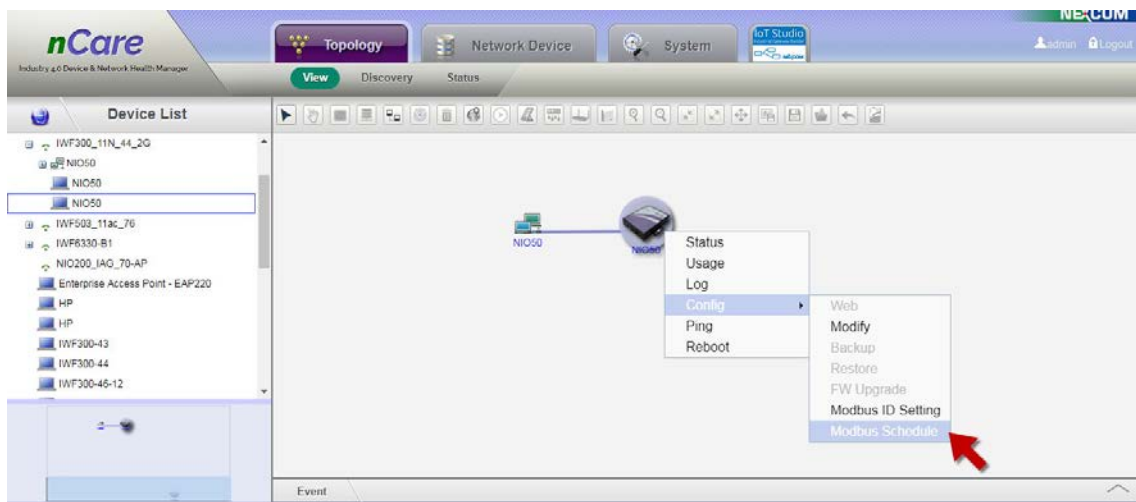


Figure 183 Modbus Scheduling

(13) A "Modbus Schedule" window will pop-out.

(14) Select *Start Time* and *Repeat*.

(15) Click **Add to Schedule** to complete setting.

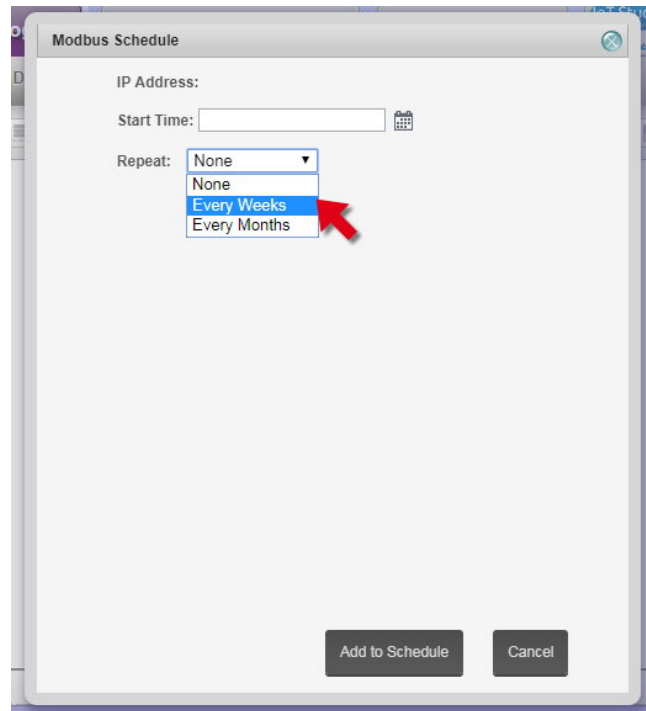


Figure 184 Time and Repeat Cycle for Modbus Scheduling

(16) Otherwise, right-click PLC device icon then enter Current Status page. The PLC information can be updated on this page.

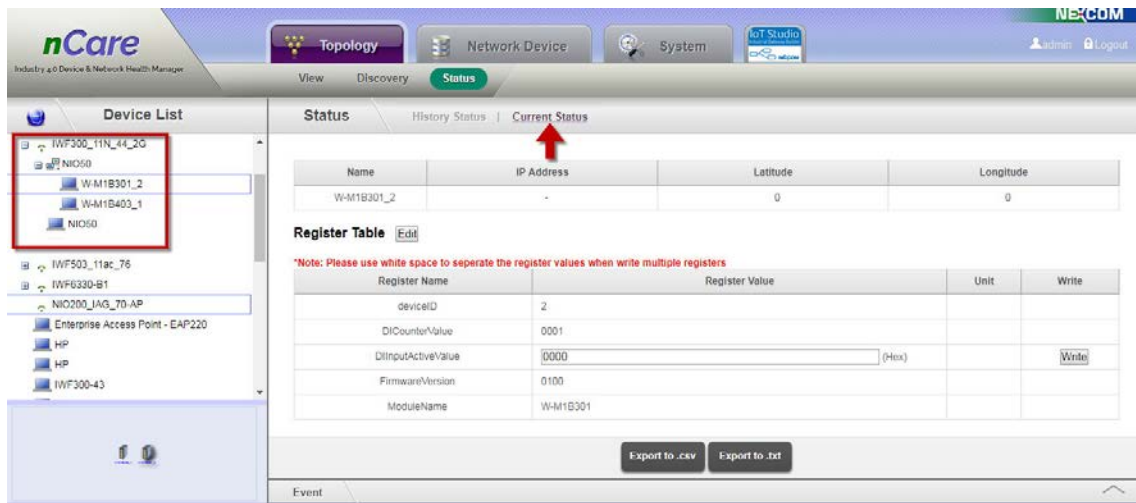



Figure 185 PLC Information Update

(17) The setting procedures for NIO51 are similar to NIO50.

(18) Double-click  icon to check PLC device in the group.

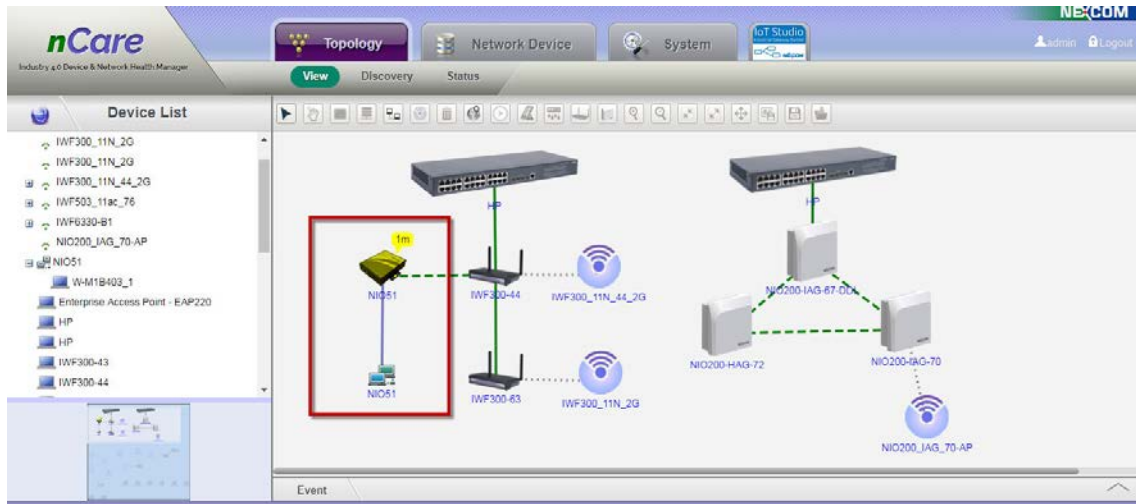



Figure 186 PLC Group of NIO51

(19) Double-click the NIO51 group icon to check PLC devices. Click  to back to upper-layer.

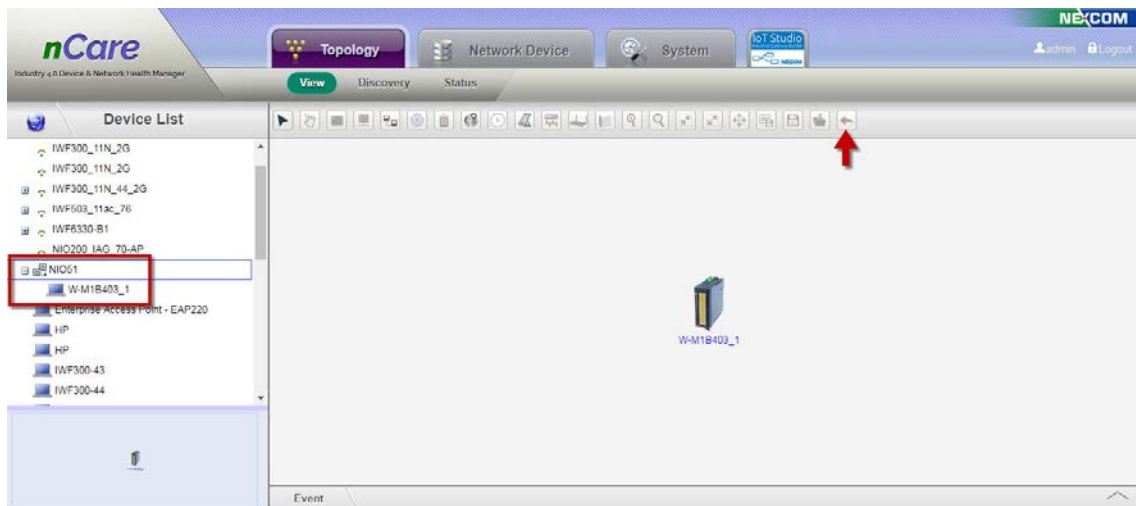


Figure 187 Devices Information of NIO51

(20) Right-click the NIO51 group icon then choose Status, Register Table can be modified on this page.

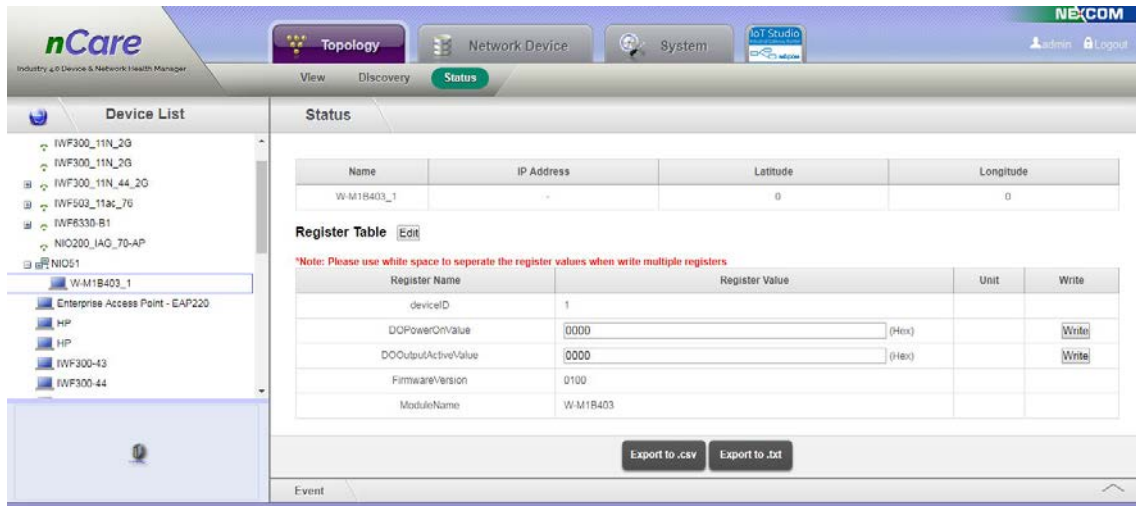


Figure 188 Modification for PLC Device of NIO51

7.1.2.3 Warning Message of Topology

- (1) Color Indication: Device will send trap when there is an issue. System will show different alarm levels on the device by colors. No message indicates the device is normal. YELLOW message indicates Major issue. RED message indicates Critical issue.



Figure 189 Color Indication of Devices

- (2) Letter Indication: Letters indicates the numbers of alarms. C indicates Critical alarms. M indicates Major alarms.
- (3) For example: **1M** indicates there are 1 Major alarms; **2C+** indicates there are 2 Critical alarms, where + indicates that there are other alarms besides these 2 Critical alarms.



Figure 190 Letter Indication of Device

## 7.1.2.4 Topology Link

- (1) GREEN line indicates that devices are connected with Internet via Ethernet.

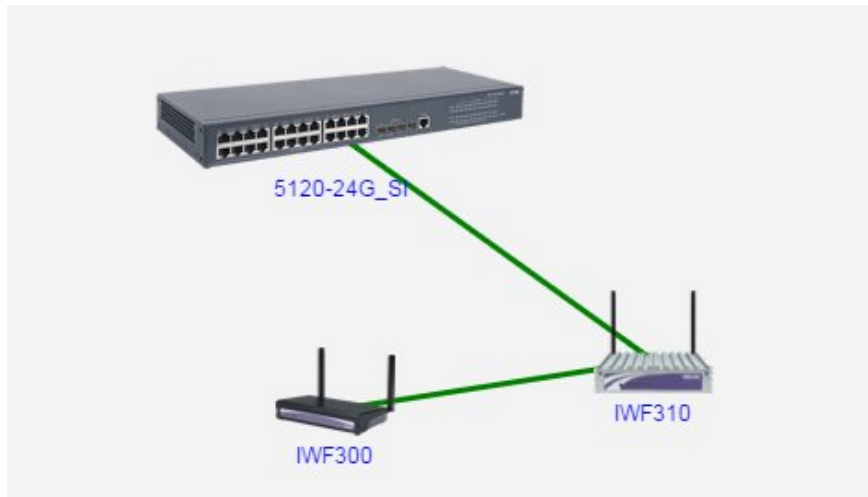


Figure 191 Internet Connection

- (2) BOLD line indicates that the connection between the two devices is Trunk.
- (3) GREEN BOLD line indicates that there are 2 or more Ethernet connected between the 2 devices.

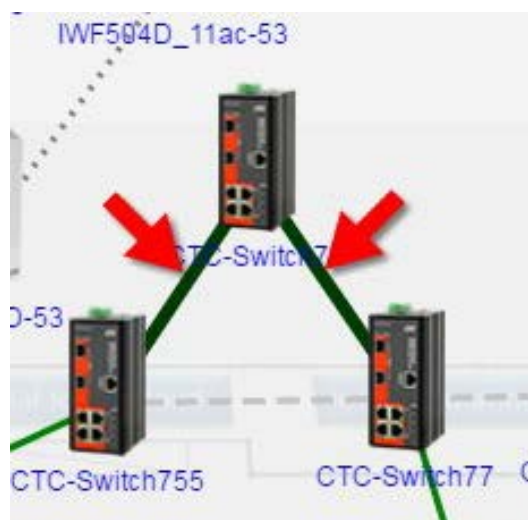


Figure 192 Trunk Connection



(4) Move the mouse to the line, port status of the Trunk can be shown.

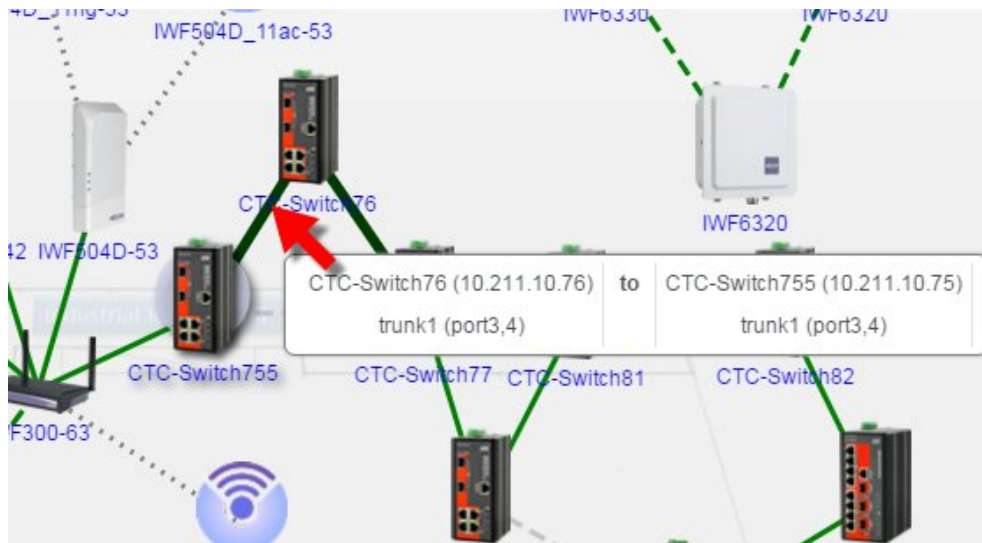


Figure 193 Trunk Status

(5) GREEN DASH line indicates that devices are connected to Mesh Network.

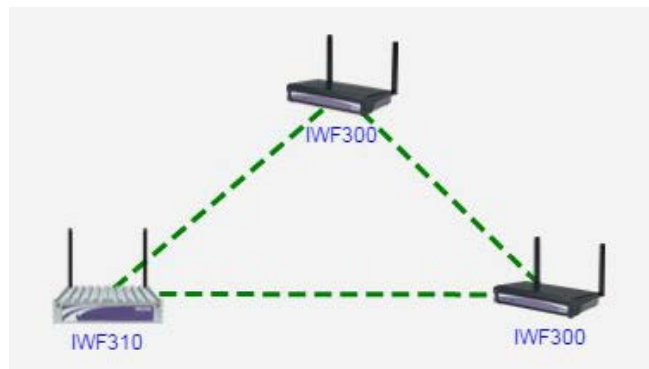



Figure 194 Mesh Network Connection

(6) GREY DOT line indicates that devices are connected to WiFi Network.

 icon shows the name of the subnet, for example: CVS\_2G\_64.

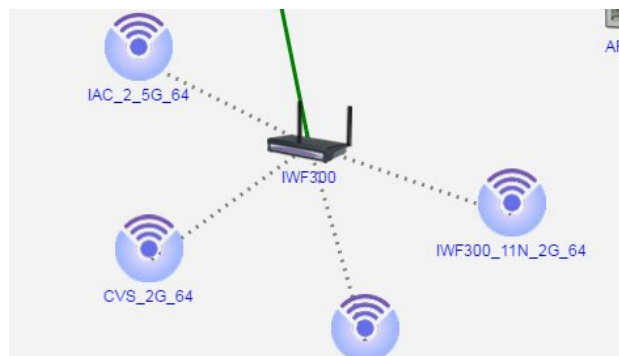



Figure 195 WiFi Connection



(7) Click  icon to see the devices at this subnet.

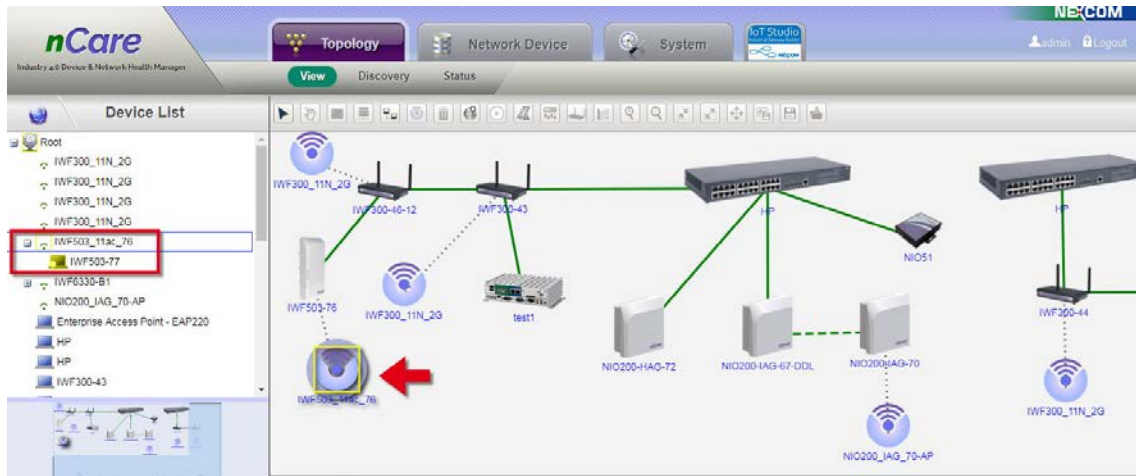


Figure 196 Devices in the Wifi Subnet

(8) GREY DASH line indicates that the device is connected with Ethernet line but is blocked. If the malfunction is detected of the Ethernet, GREY DSH line will be activated to show the backup path.

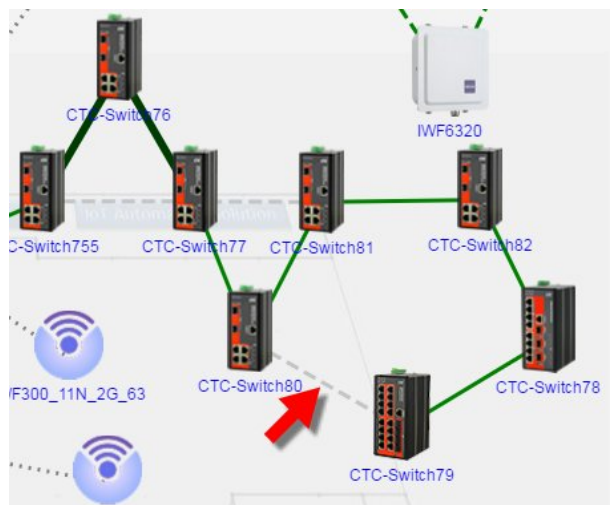


Figure 197 Devices in the Wifi Subnet

(9) PURPLE line indicates that there are one Ethernet and 2 or more VLAN connections.

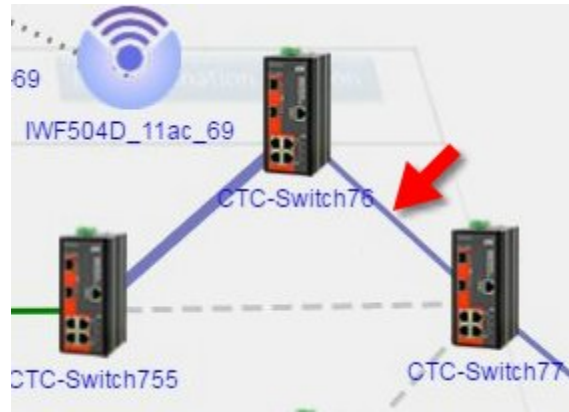


Figure 198 Purple Line

(10) PURPLE BOLD line indicates that there are 2 or more Ethernet and 2 or more VLAN connections.

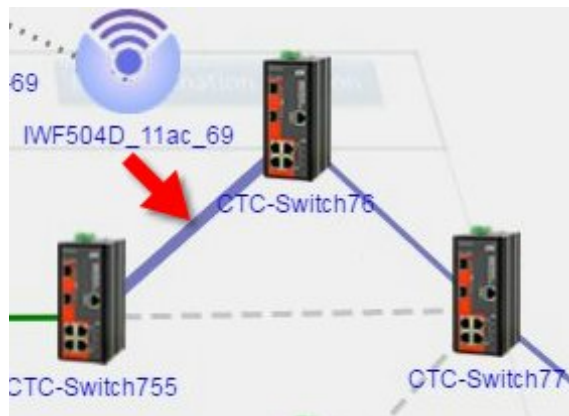


Figure 199 Purple Bold Line

(11) Move the mouse to the line, port status of the VLAN can be shown.

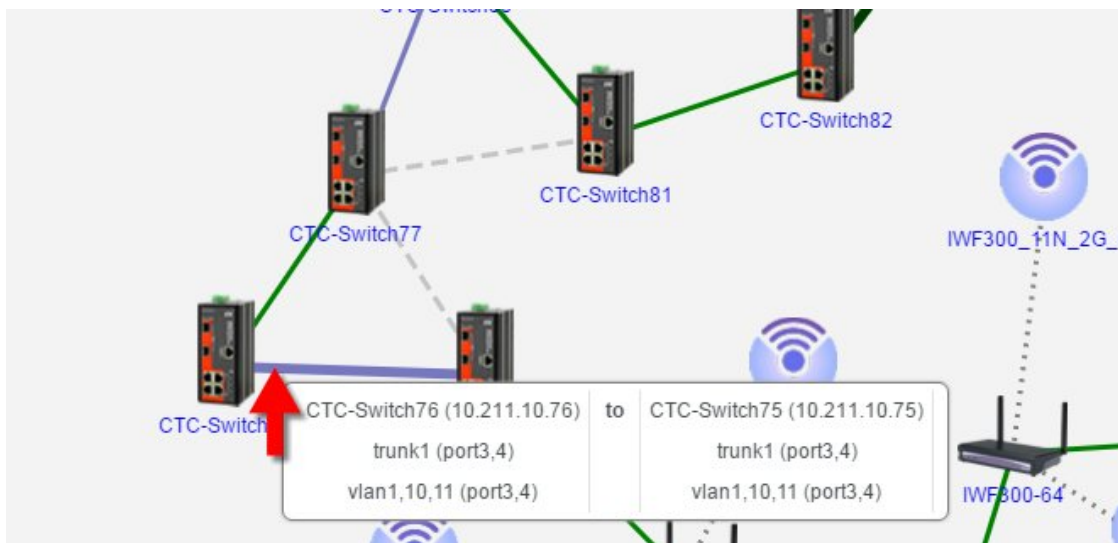


Figure 200 VLAN Status

## 7.1.2.5 Status of Topology Link

- (1) GREEN line indicates that connected of devices are normal.

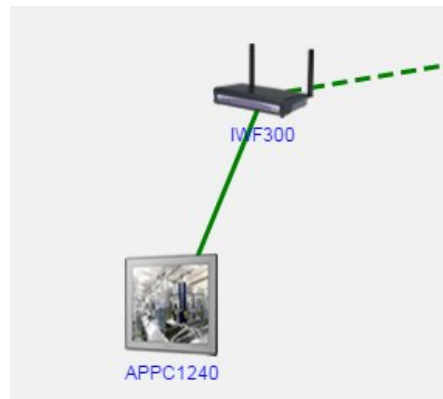


Figure 201 Normal Link

- (2) GREEN bold line indicates that the traffic flow of devices are more than 20 MB. The bolder one indicates that the traffic flow of devices are more than 100 MB

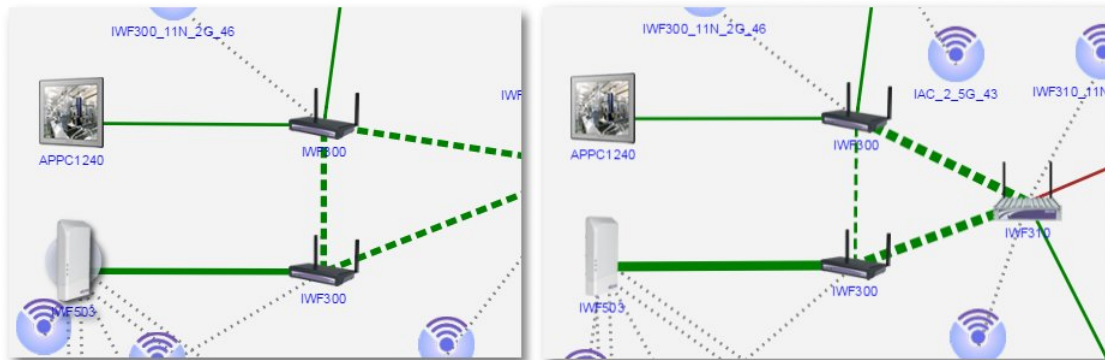


Figure 202 High Traffic Link

- (3) RED bold line indicates that devices are disconnected.

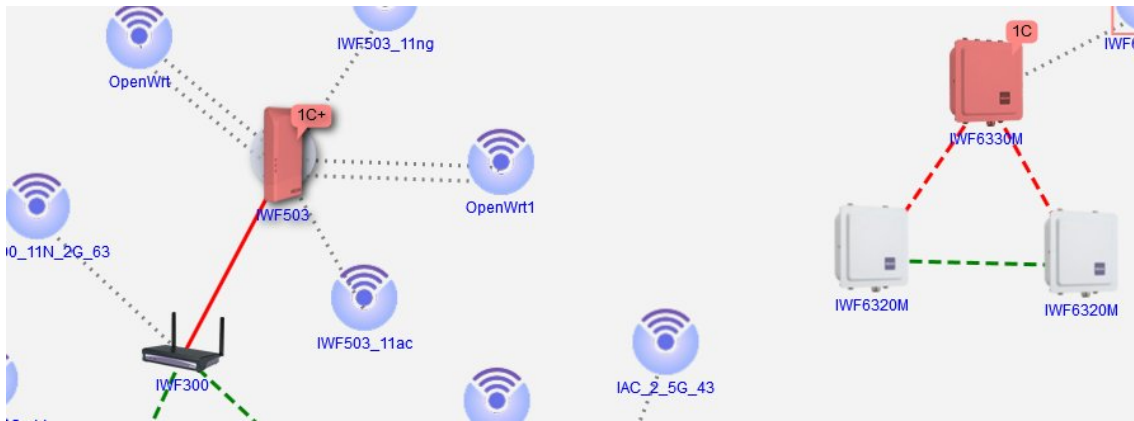


Figure 203 Disconnected Link

(4) ORANGE line indicates that the traffic flow is over the threshold.

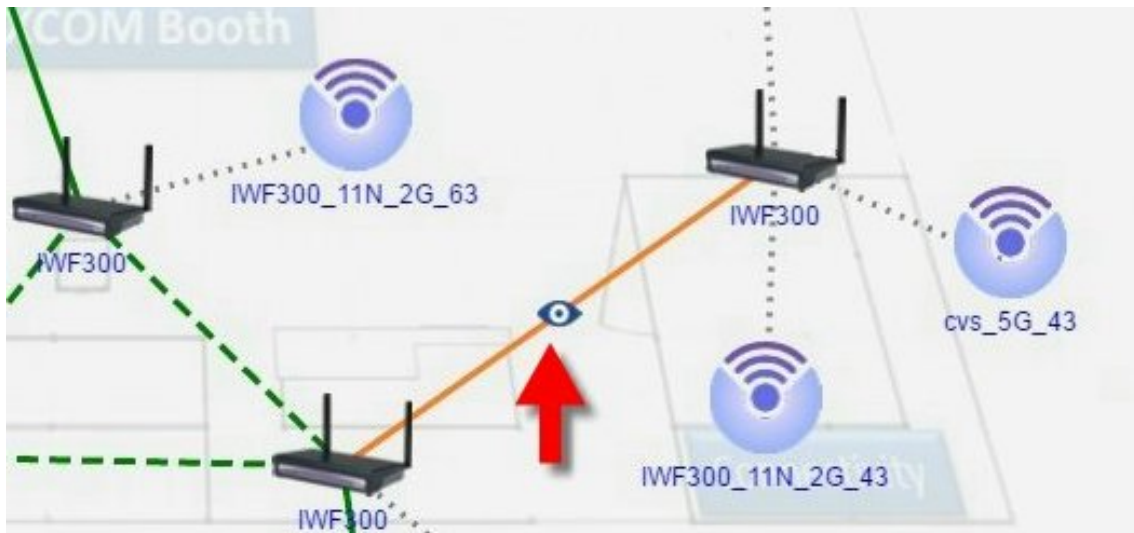


Figure 204 Link Over the Threshold

#### 7.1.2.6 Shortcut Key

Right-click on the device and a shortcut list will appear. Information includes *Status*, *Usage*, *Log*, *Config*, *Ping* and *Reboot*.

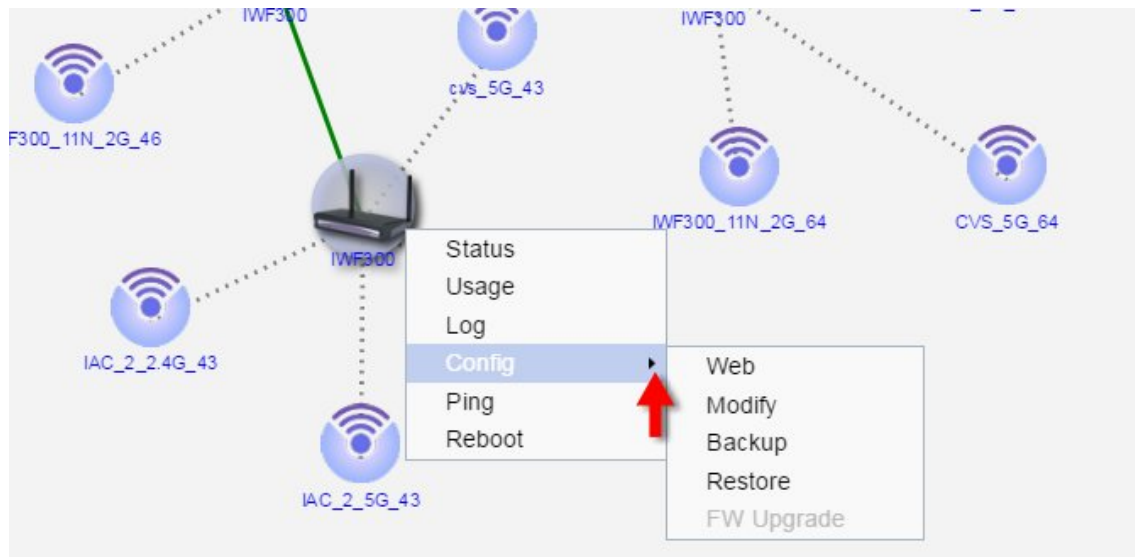


Figure 205 Shortcut Key

- (1) Status: Go to *Device Status* page.
- (2) Usage: Go to *Device Usage* page.
- (3) Log: Go to *Device Log* page.
- (4) Config: Go to *Device Setting* page. Or Modify, Backup, Restore or FW Upgrade for devices.
- (5) Ping: This function is for monitoring the network connection of device. Check the response time to confirm whether the packet is transferring smoothly or not. Click **Ping** to ping again or click **Cancel** to go back Topology View.

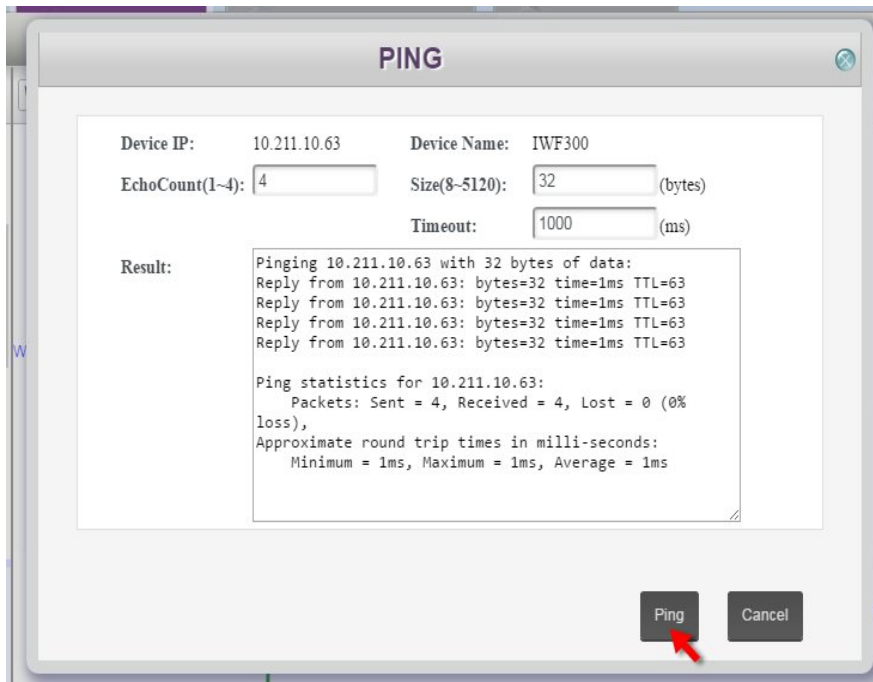


Figure 206 Ping Function

(6) Reboot: Reboot the device.

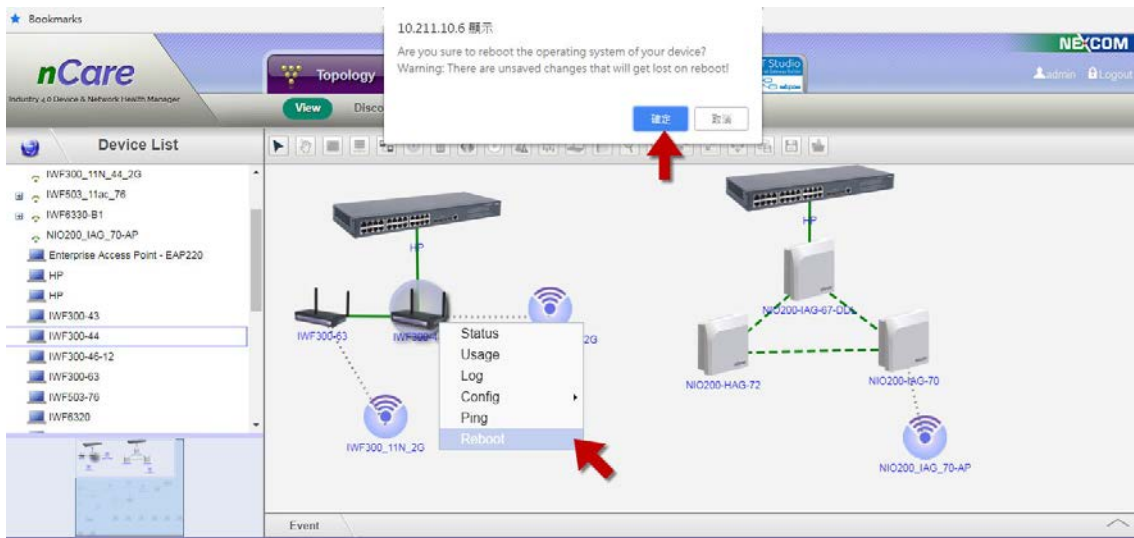


Figure 207 Reboot Function

### 7.1.2.7 Remote Desktop

If the IPC device is selected, right-click the menu, go to Config > Remote Desktop, to enter the desktop of IPC device

\* Remote Desktop Installer should be asked first from NEXCOM.



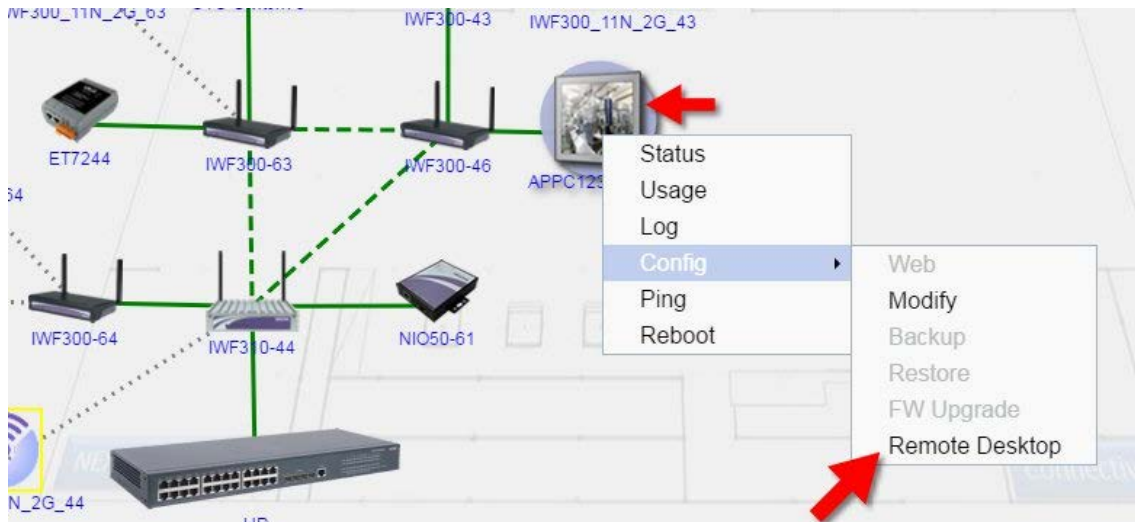


Figure 208 Remote Desktop

## 7.2 Device Discovery

### 7.2.1 Introduction for Device Discovery

Device IP and protocol can be set on this system. Devices will be shown on the page if they fit the discover condition. The connections of devices can also be drawn.

\* "Device Series" should be included on all device names.

### 7.2.2 Operation for Device Discovery

- (1) Enter the IP section to discover. Check *All*, *CAPWAP*, *SNMP* or *Modbus* for protocol.
- (2) If *SNMP* is selected, *SNMP* version can be chosen. Enter *Read Community* (set as public by default) and *Write Community* (set as private by default)



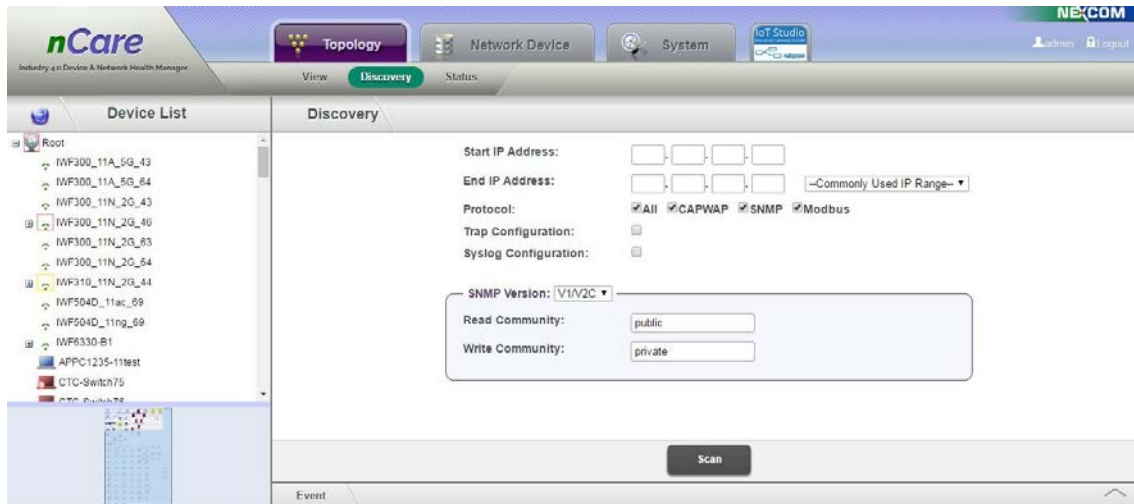


Figure 209 Device Discovery

(3) 4 recent searching records of IP ranges can be chosen for Discovery.



Figure 210 Recent Searching Records of IP Range

- (4) If **CAPWAP** is selected, system will search for the subnet the same as server without entering the IP range.
- (5) If cross-subnet search is required, please check **SNMP** before scan.

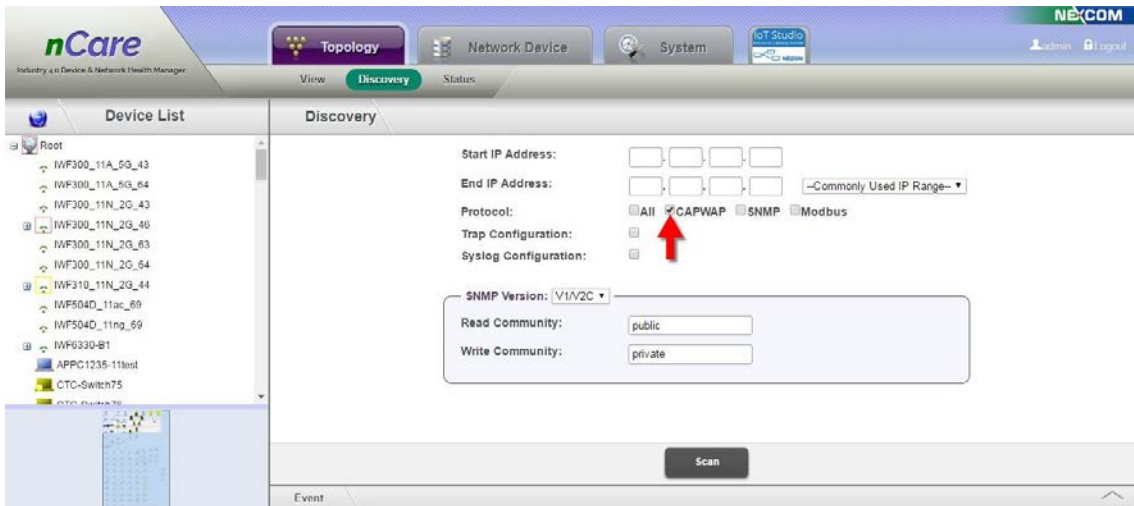


Figure 211 CAPWAP Device Search without Entering IP Range

- (6) Take the following figure for example. nCare is installed at 10.211.10.0 class C subnet, IP range 10.211.10.1~10.211.10.254 can only be searched. However, subnet IP range 10.211.11.X cannot be searched.

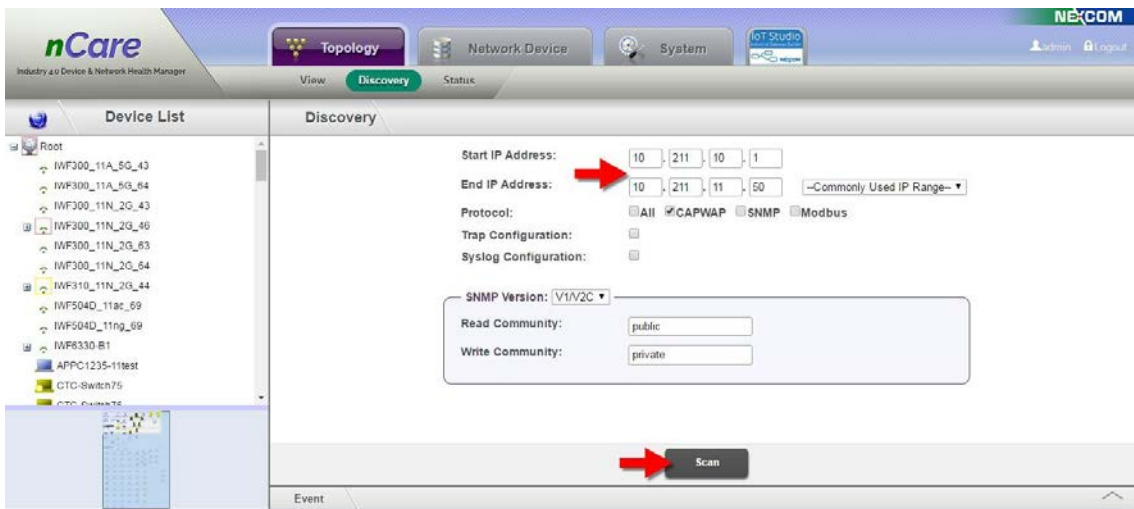


Figure 212 Device Searching with CAPWAP

- (7) Click **Scan** to start discovery. The scanning percentage will be shown on the page.

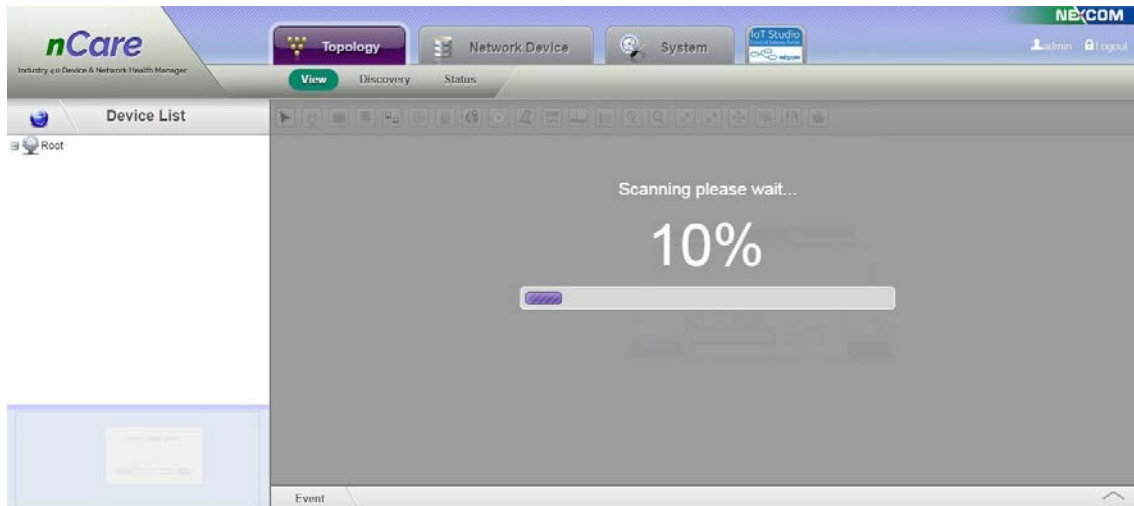


Figure 213 Scan Percentage

(8) All discovered devices can be shown on Topology then.

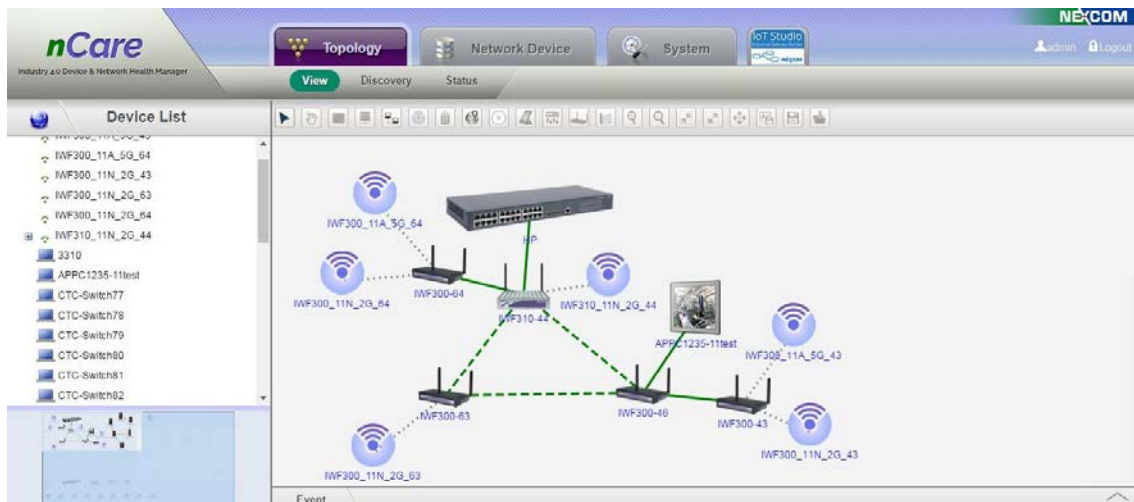


Figure 214 Discovered Devices

## 7.3 Device Status

### 7.3.1 Introduction for Device Status

The status of devices can be shown on this page.

### 7.3.2 Operation for Device Status

- (1) Select the device from the *Device List* on the left.
- (2) Device status such as *Name*, *Type*, *MAC*, *Channel*, *Tx Kbps*, *Rx Kbps* and *AssocClient* will be shown for IWF type device.

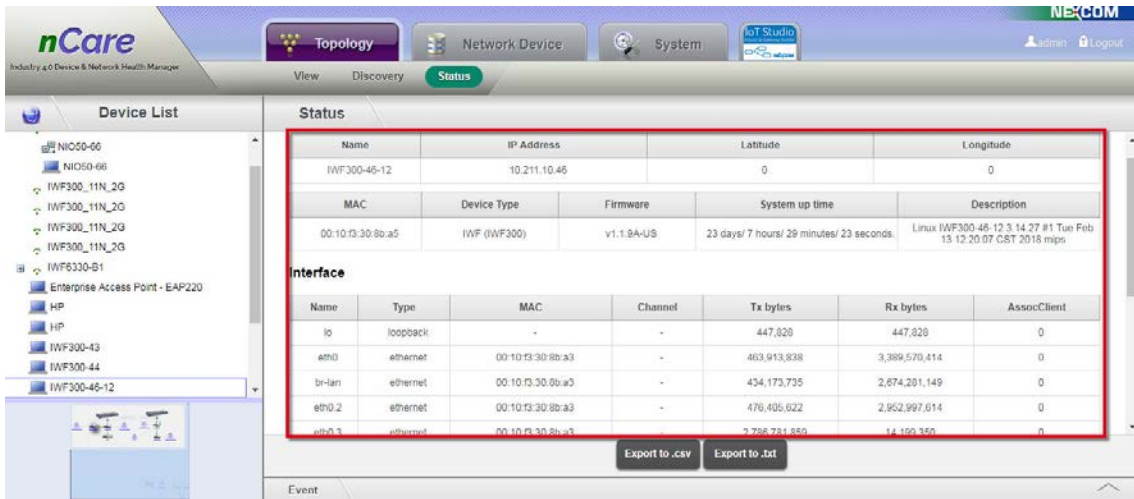


Figure 215 IWF Type Device Status

- (3) *Device Information, Hardware Monitoring and GPIO* can be shown at **Modbus** page for IPC type device.

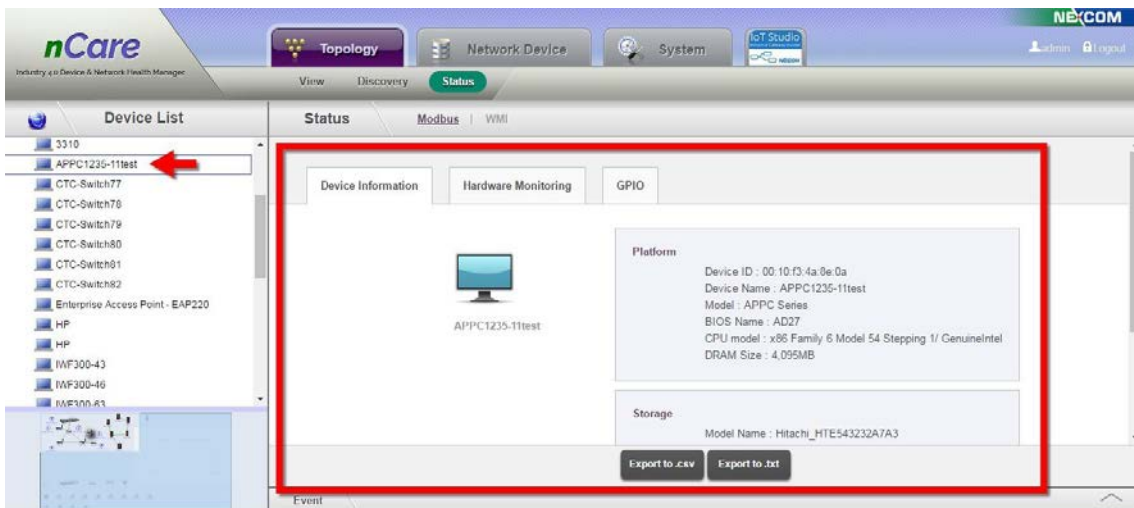


Figure 216 IPC Type Device Status

- (4) The resource of IPC device can be viewed at **WMI**(Windows Management Instrumentation) page.
- (5) Enter *User Name* and *Password* of the device then click **Submit**.

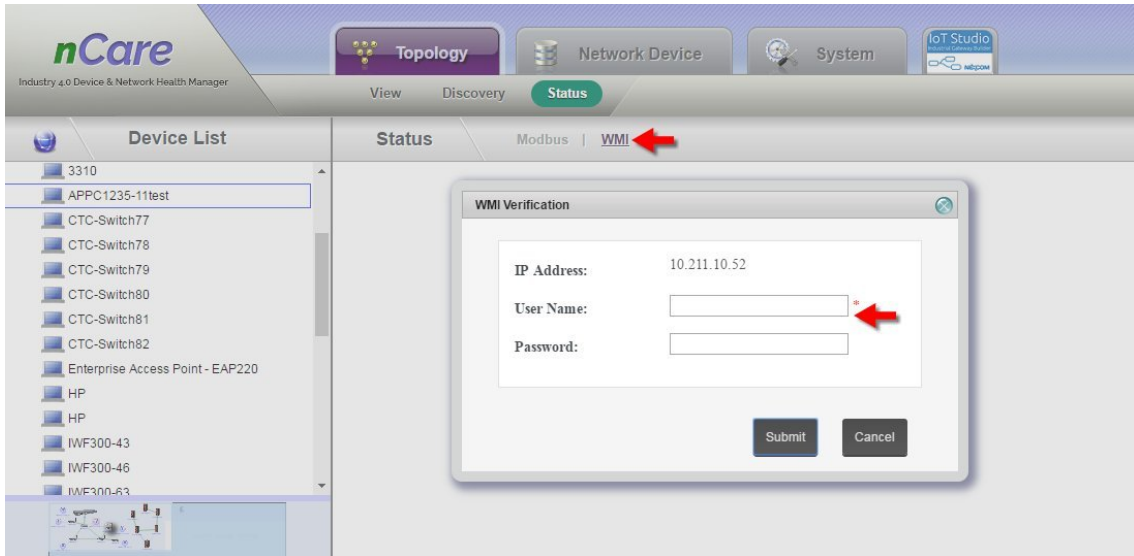


Figure 217 WMI Function for IPC Device

(6) *MAC, Device Type, Baseboard, BIOS* and *CPU* can be viewed on **WMI** page then.

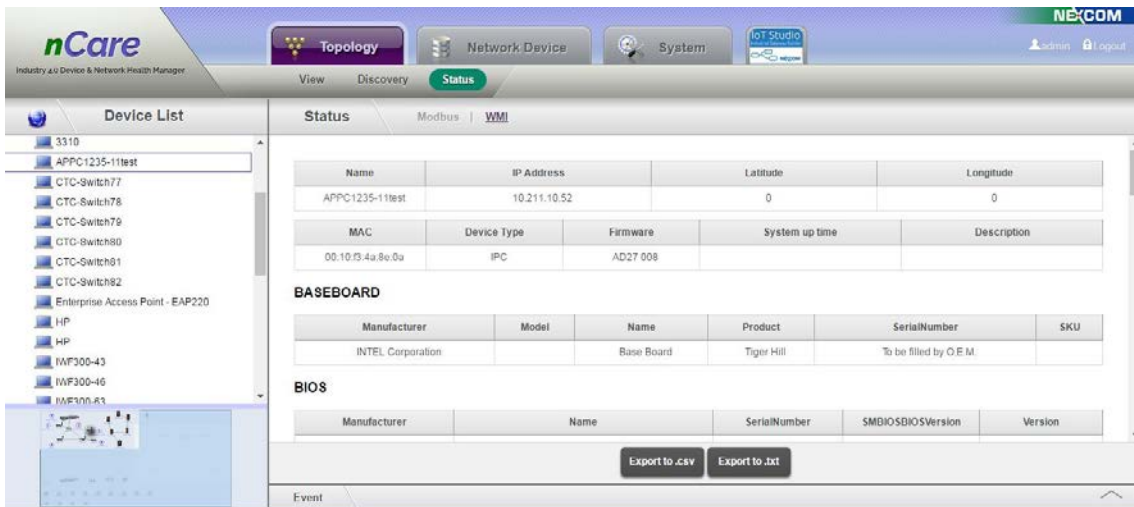


Figure 218 WMI Page for IPC Device

(7) If PLC device under NIO50 structure is selected, **History Status** and **Current Status** will be shown on the page. *Device Name, IP Address, Latitude* and *Longitude* can be viewed then.

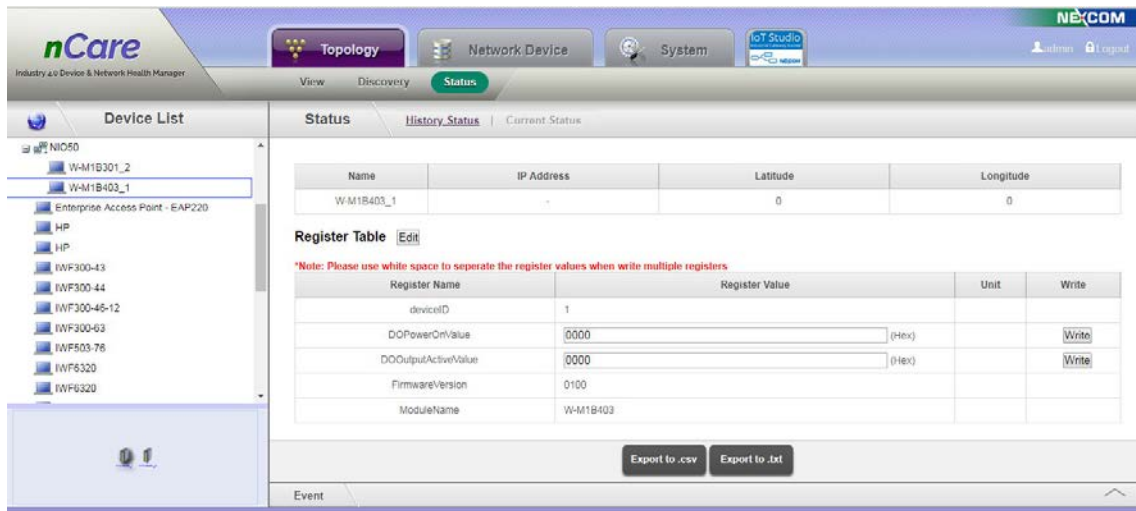


Figure 219 History Status of PLC Device

(8) The Registered Table can be edited at **Current Status** page.

(9) Click “Edit” to go to modify page.

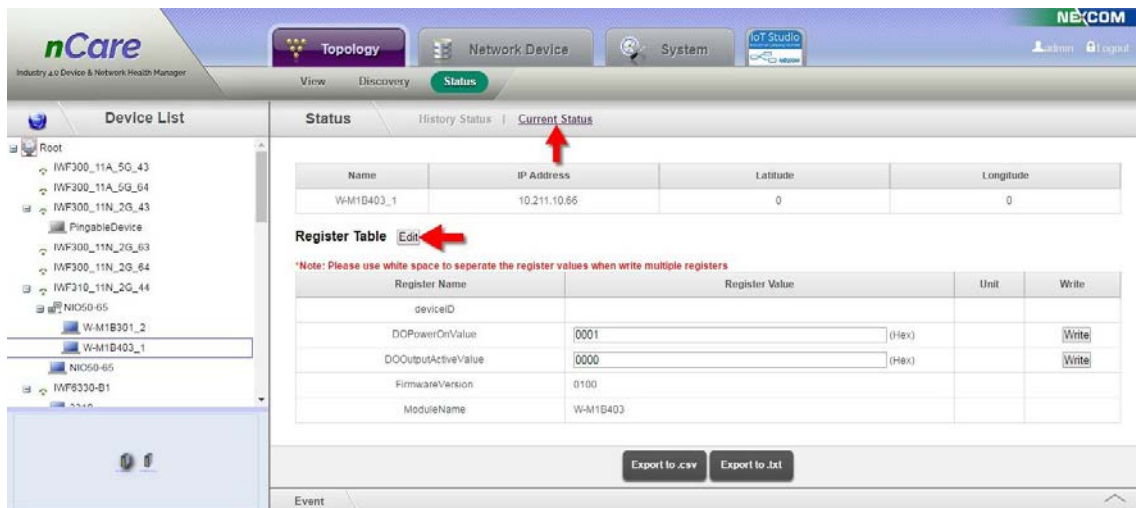


Figure 220 PLC Type Device Register Table

(10) Basic Information, such as *IP Address*, *Latitude* and *Longitude*, or Interface, Client List and AP Scan can be shown for IWF type device.

(11)The *Register Table* of **PLC device** can be edited.

(12)The *Register Table* of **PLC device** can be added or deleted.

(13) Enter *Register Name*, *Unit*, *Function Code*, *Address Offset*, *Word Count*. *Attribute* can be chosen as R (read)/W (write)/RW (read and write).



With *Attribute* selected as *W*, the attribute can also be chosen as Binary, Decimal or Hexadecimal.

(14) Click "Save" to complete modification.

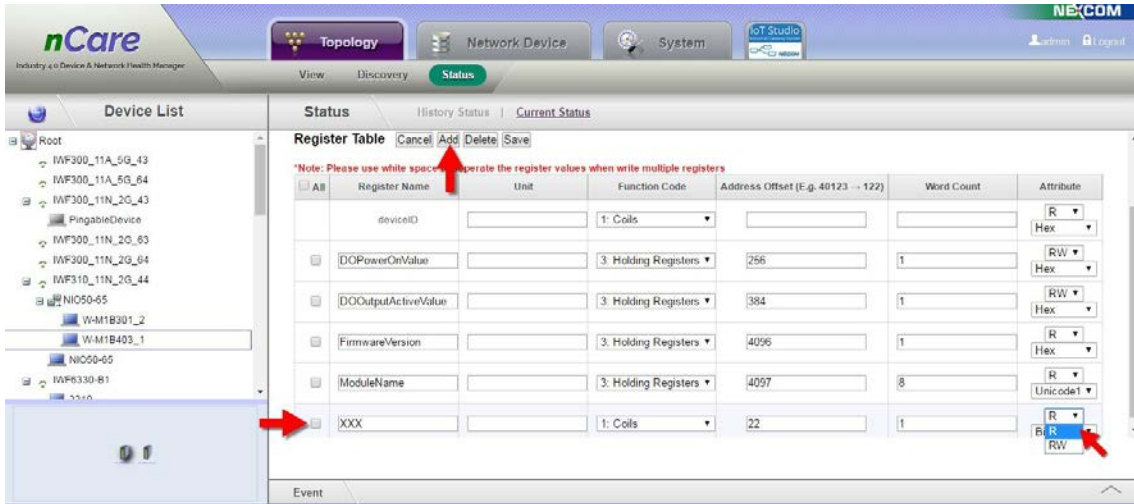


Figure 221 Register Table Modification

(15) After the table is updated, the *Register Value* can be added directly.

(16) Click **Write** to write in the information.

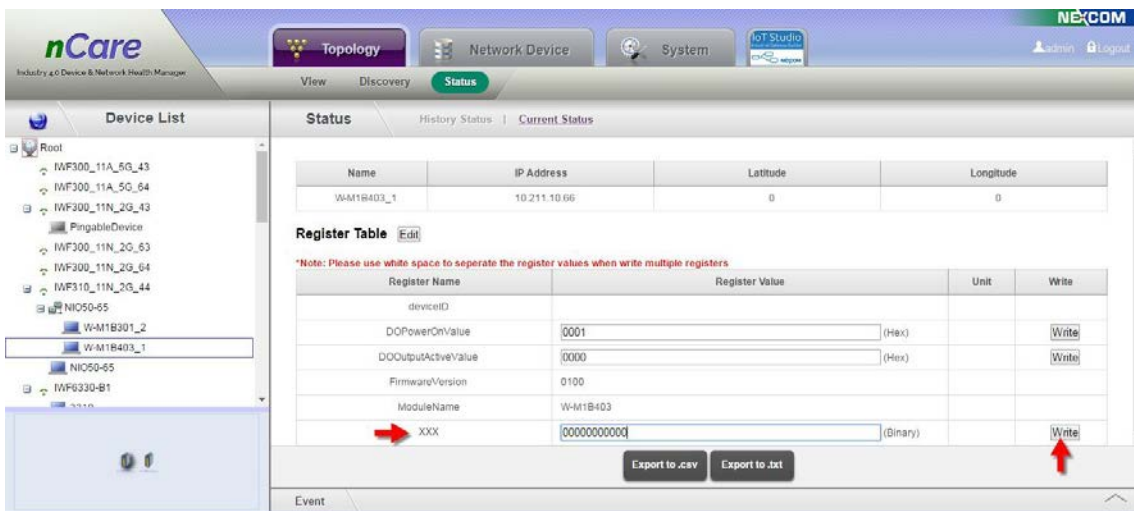


Figure 222 Register Value Modification

(17) Click **Export to .csv** or **Export to .txt** to export the status for IWF and PLC devices with desired file format at Status page.



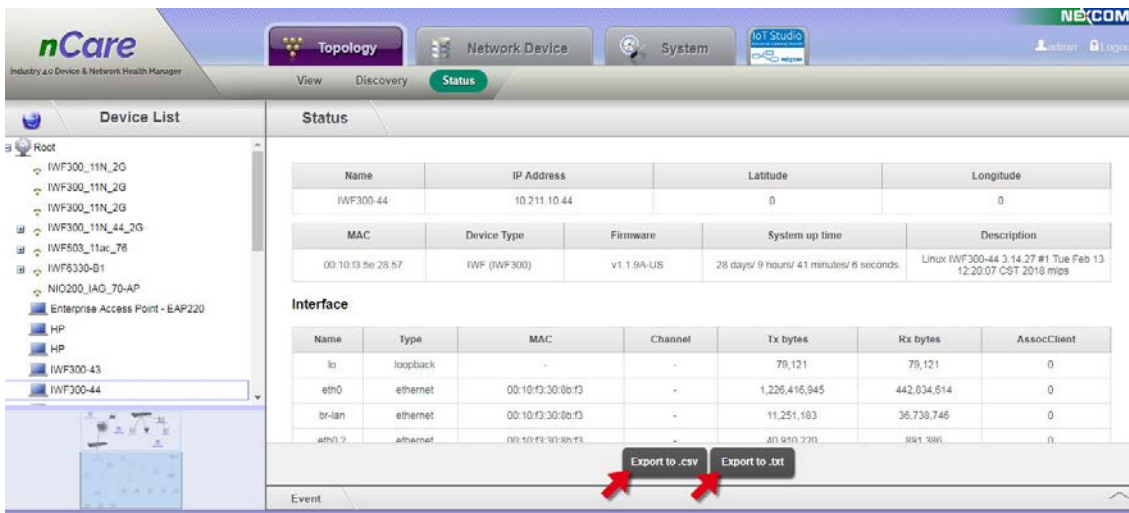


Figure 223 Status Exportation

(18) Status of PLC device under NIO51 such as *Name*, *IP Address*, *Latitude* and *Longitude* can be shown, and Register Table can also be modified on the page.

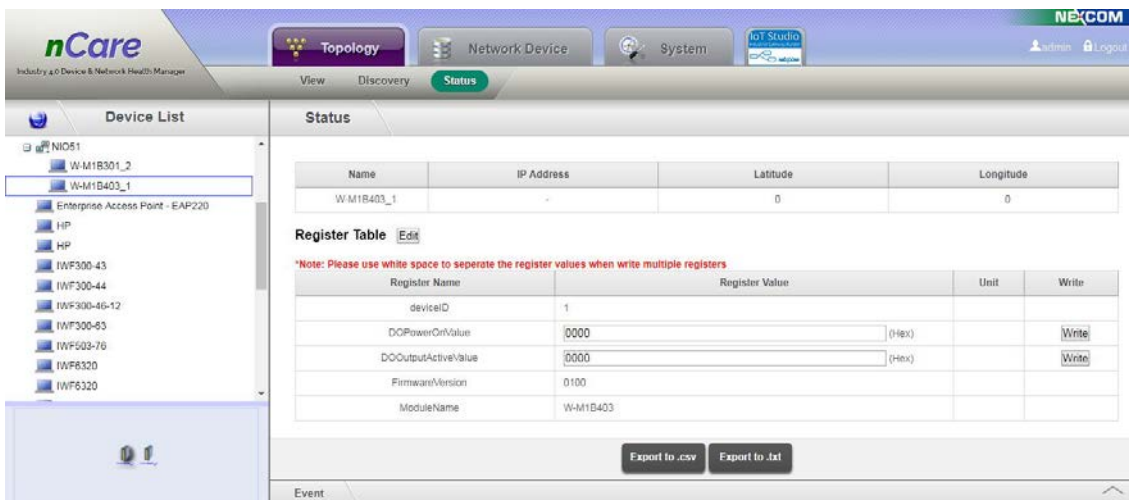


Figure 224 PLC Status for NIO51

(19) Status of NIO200-HAG device such as *Interface*, *Client List* and *AP Scan* can be shown on the page.

(20) All devices connected with WirelessHART under NIO200-HAG can be scanned.

(21) Wireless HART Devices List and Wireless HART Command Logs can

also be set and updated on this page.

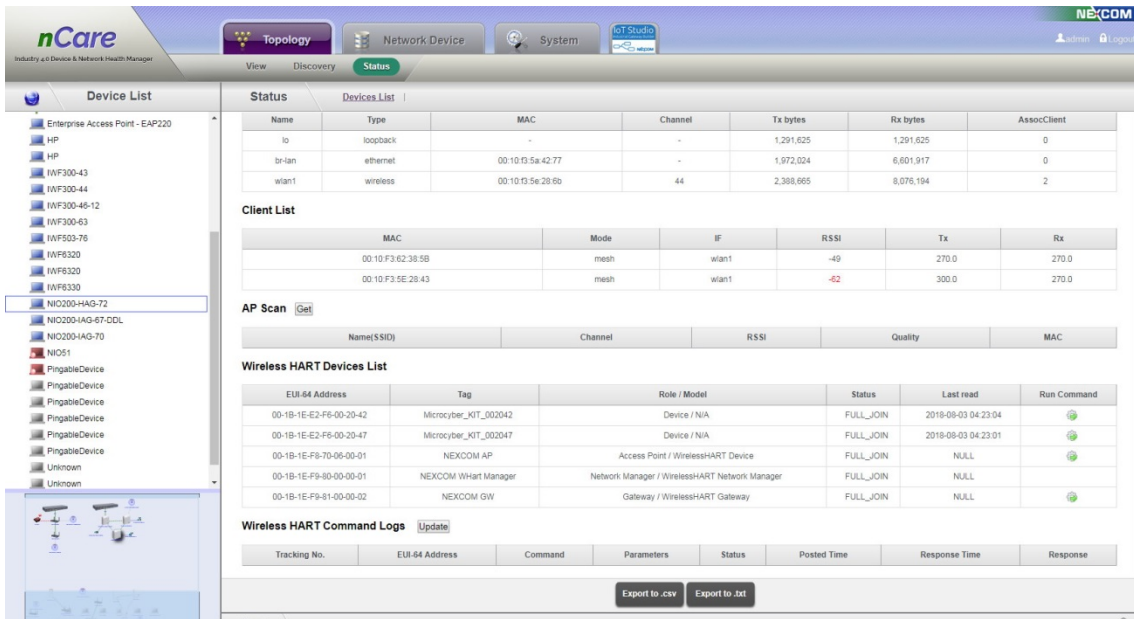


Figure 225 Device Status for NIO200-HAG

(22) EUI-64 Address, Role / Model and Status can be shown on Wireless HART Devices Scan List.

(23) "Run Command" can also be done here.

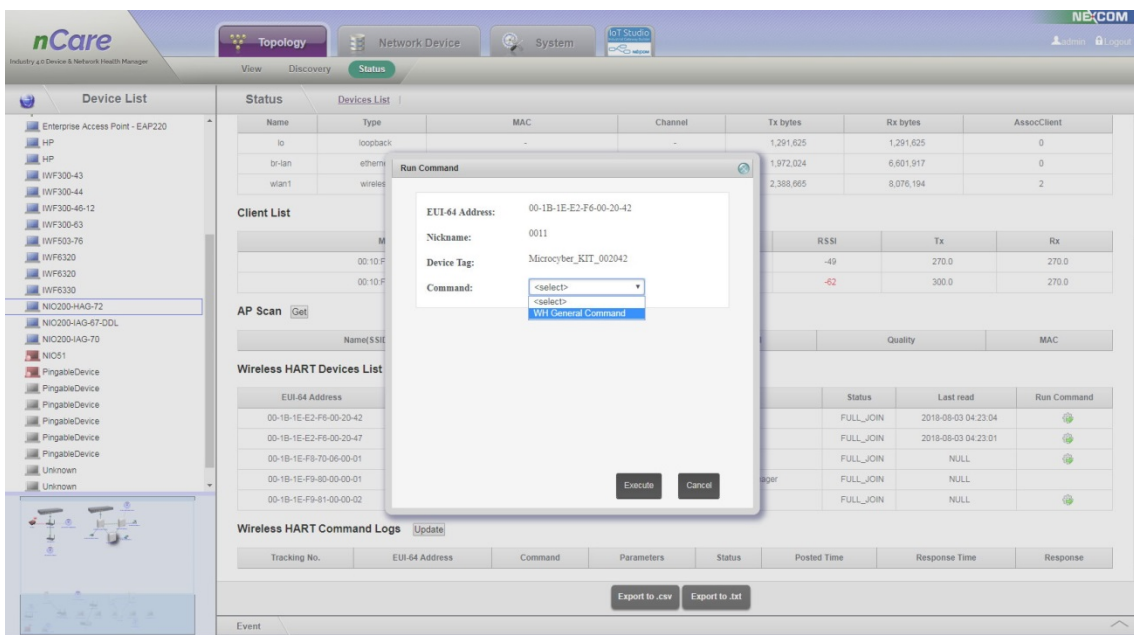


Figure 226 Run Command for NIO200-HAG

- (24) There are Devices List and Trouble Shooting for NIO200-IAG Status.
- (25) Status of NIO200-IAG device such as *Interface*, *Client List* and *AP Scan* can be shown on the page.
- (26) All devices connected with WirelessHART under NIO200-IAG can be scanned.
- (27) ISA100 Devices List and ISA100 Command Logs can also be set and updated on this page.

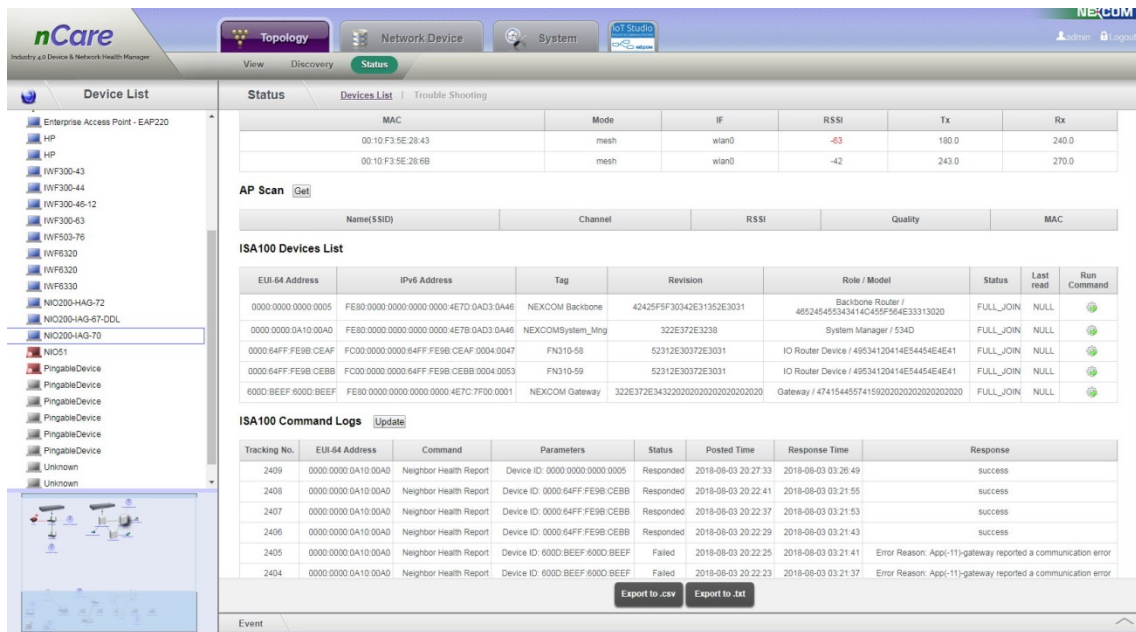


Figure 227 Device Status for NIO200-IAG

- (28) *EUI-64 Address*, *Role / Model* and *Status* can be shown on Devices List.
- (29) "Run Command" can also be done here.

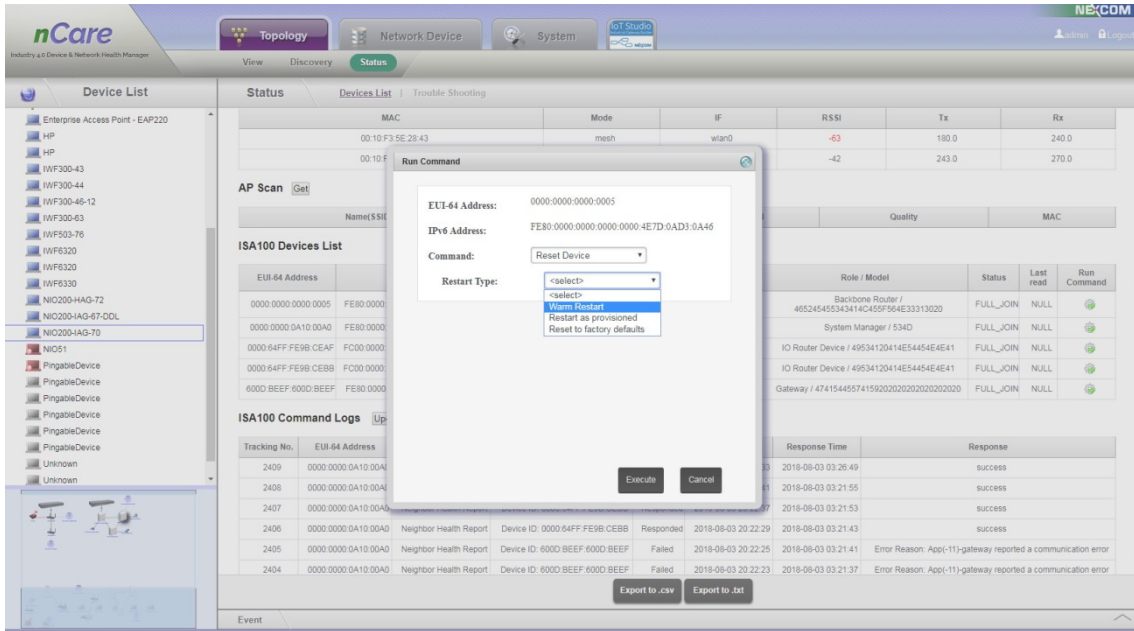


Figure 228 Run Command for NIO200-IAG

(30) EUI-64, Timestamp, Event and Details can be shown on ISA100 Trouble Shooting page under NIO200-IAG status.

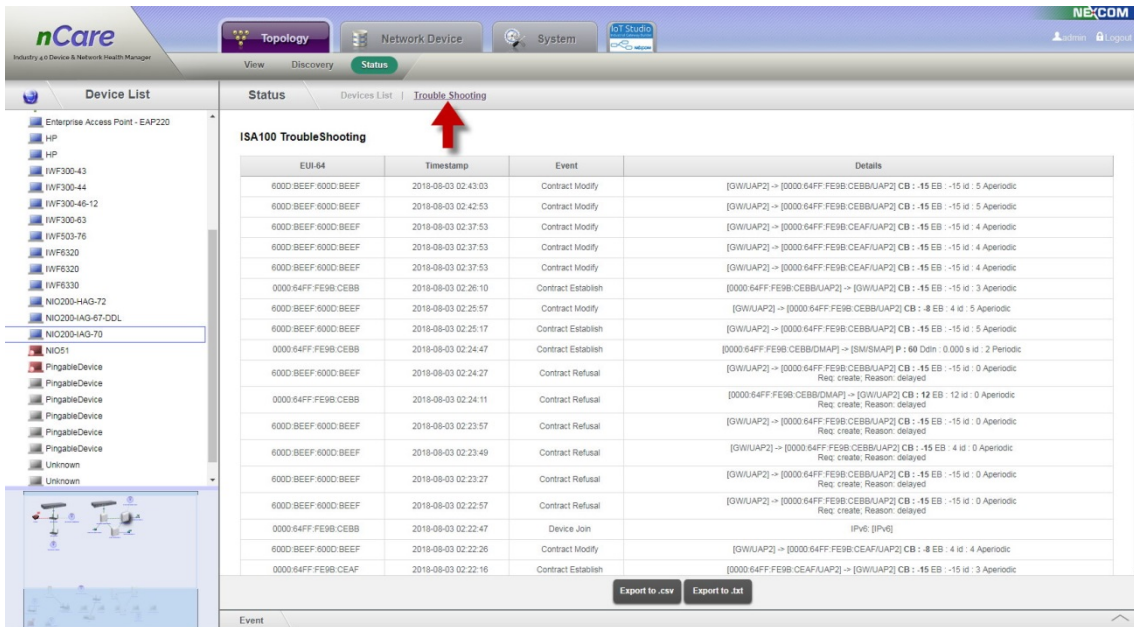


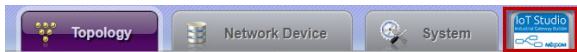
Figure 229 Trouble Shooting Page for ISA100

## 8 Introduction for IoT Studio

This function can be used by purchasing installation kit from salesperson of NEXCOM on the web page:

<http://www.nexcom.com.tw/Products/industrial-computing-solutions/iot-solutions/iot-studio/nexcom-industrial-iot-studio>

After installation, click IoT Studio on the main page



It can be hyperlinked to “IoT Studio NodeRed” page on NEXCOM as shown below. (This function is available after purchased)

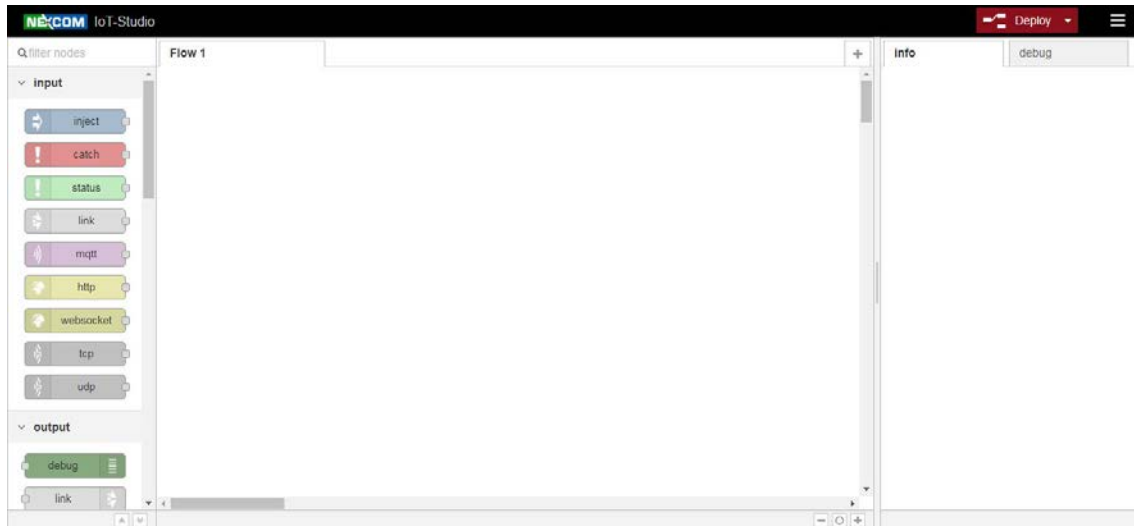


Figure 230 Operation Page for IoT Studio

## 9 nCare Maintenance and Management

### 9.1 Access Control

To avoid any unauthorized access, invade or improper operation, nCare has access control function. It includes data access, function setting and update scheduling, to make sure the function for system access and deployment.

#### 9.1.1 System User

User may only monitor for the group devices that is opened by Administrator. And for these devices, user may view the event and efficiency of alarms, use Topology view. The authorization for nCare User is shown as follows:

Main Menu	Sub menu L1	Sub Menu L2	Authorization
Topology	View	Icons	Opened functions: <ul style="list-style-type: none"> <li>• Select</li> <li>• Move</li> <li>• Traffic Monitoring</li> <li>• Show/Hide Rogue Devices</li> <li>• Switch VLAN</li> <li>• Update AP</li> <li>• Update IWSN</li> <li>• Zoom In</li> <li>• Zoom Out</li> <li>• Zoom Overview</li> <li>• Zoom Reset</li> <li>• Full Screen</li> <li>• Export to Image</li> </ul> (For devices opened by Administrator)
		Shortcut	Opened functions: <ul style="list-style-type: none"> <li>• Usage</li> <li>• Log</li> <li>• Config</li> <li>• Ping</li> </ul> (For devices opened by Administrator)
	Status	Export to Report	All functions are opened (For devices opened by Administrator)
Log	Event Log		
	System Log		
Usage	Eth		
	Wlan		
	CPU		
	Memory		

Figure 231 Authorization for nCare User



### 9.1.2 Device Manager

Manager may use all functions except *Account Management*. The authorization for nCare Manager is shown as follows:

Main Menu	Sub menu L1	Sub Menu L2	Authorization
Topology	View	Icons	All functions are opened
		Shortcut	
	Discovery	Discovery	
Network Device	Manage	Device List	
		Config Backup	
		Config Restore	
		Fw Upgrade	
		Device Provision	
		Modbus Profile	
	Log	Event Log	
		System Log	
		Playback	
	Usage	Eth	
		Wlan	
		CPU	
		Memory	
		Temperature	
	Severity		
	Interval		
	Group	Topology Group	
	Rogue AP/Device	Detection	
		White List	
Deny List			
Scan Setting			
System	Message	E-mail	
		SMS	
		Social Media	
		Notification Users	
	Database	Event Log Mgmt	
	DHCP	Setting	
		Client List	
	Scan IP	Scan IP	
About	License		
IoT Studio	Purchasing installation kit from salesperson of NEXCOM		

Figure 232 Authorization for nCare Manager



### 9.1.3 System Administrator

Administrator has complete system monitoring right. The authorization for nCare Administrator is shown as follows:

Main Menu	Sub menu L1	Sub Menu L2	Authorization
Topology	View	Icons	All functions are opened
		Shortcut	
	Discovery	Discovery	
	Device Status	Status	
Network Device	Manage	Device List	
		Config Backup	
		Config Restore	
		Fw Upgrade	
		Device Provision	
		Modbus Profile	
	Log	Event Log	
		System Log	
		Playback	
	Usage	Eth	
		Wlan	
		CPU	
		Memory	
		Temperature	
	Severity		
Interval			
Group	Topology Group		
Rogue AP/Device	Detection		
	White List		
System	Users	Account Management	
	Message	E-mail	
		SMS	
		Social Media	
		Notification Users	
	Database	Event Log Mgmt	
	DHCP	Setting	
		Client List	
Scan IP	Scan IP		
About	License		
IoT Studio	Purchasing installation kit from salesperson of NEXCOM		

Figure 233 Authorization for nCare Administrator

## 9.2 Device Aberrant Status

### 9.2.1 Same IP

If devices are set as the same IP, aberrant event and alarm will be shown after discovering.

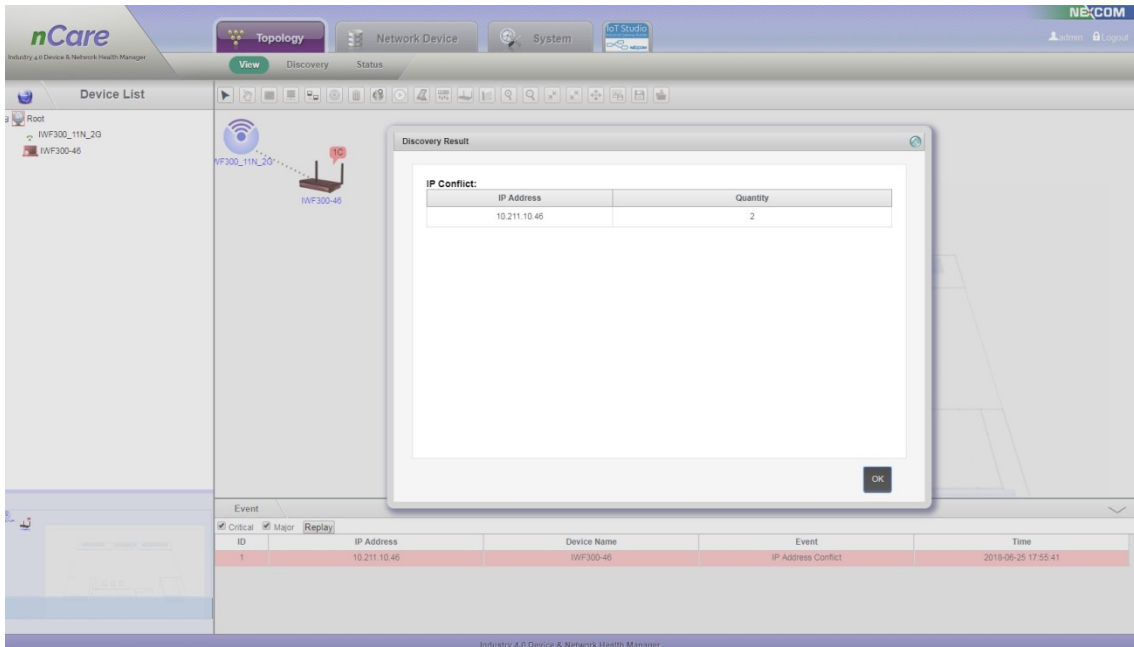


Figure 234 Discovery Result for the Same IP

Same IP alarms will be shown on Event Log as well.

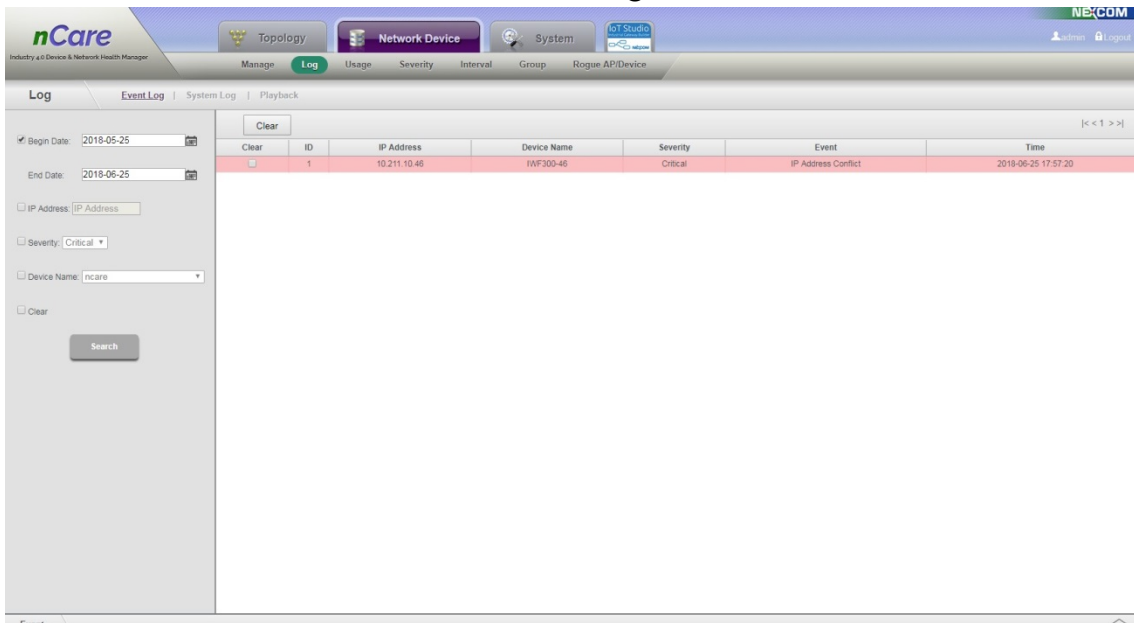


Figure 235 Event Log List for the Same IP

### 9.2.2 Same MAC

If devices are set as the same MAC, aberrant event and alarm will be shown after discovering.

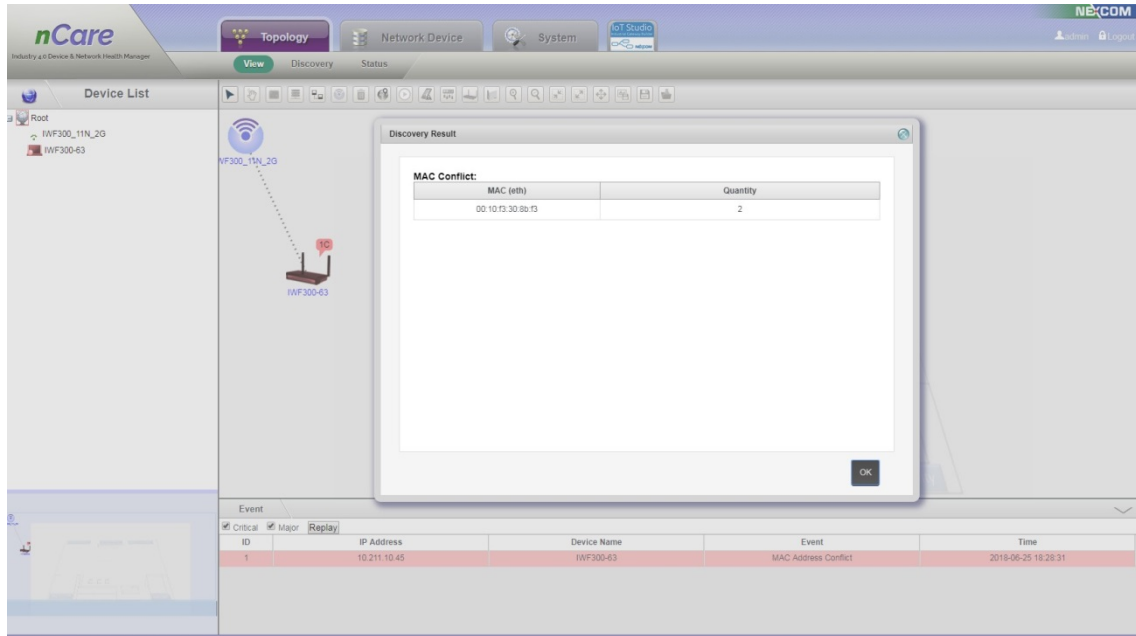


Figure 236 Discovery Result for the Same MAC

Same MAC alarms will be shown on Event Log as well.

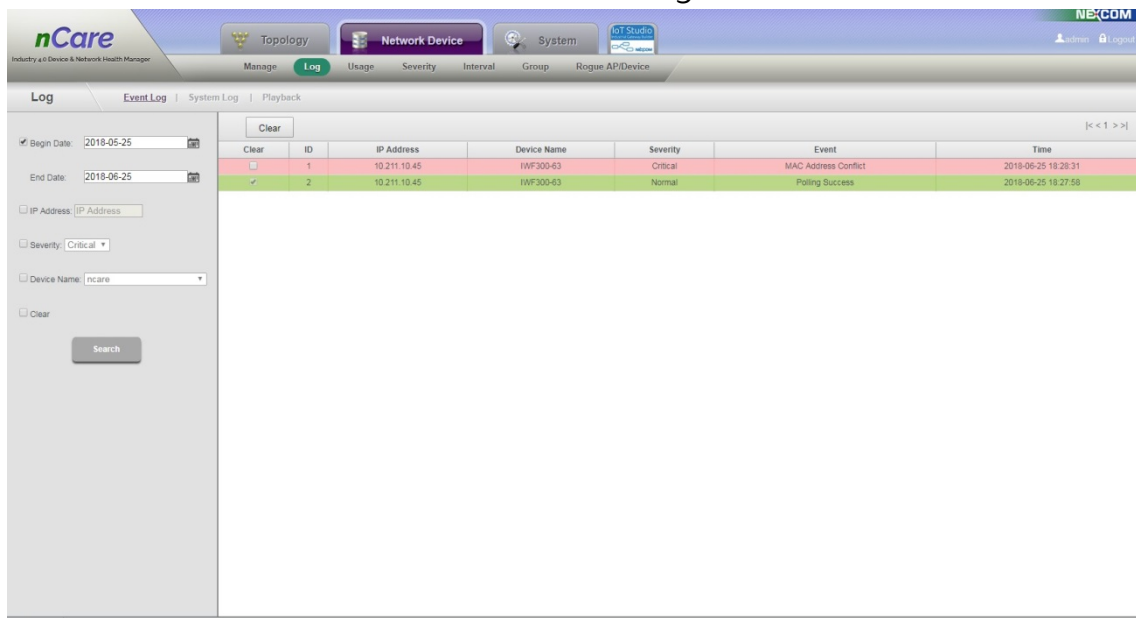


Figure 237 Event Log List for the Same MAC

The list will be marked as **RED** to inform administrator on main page: System > Scan IP.

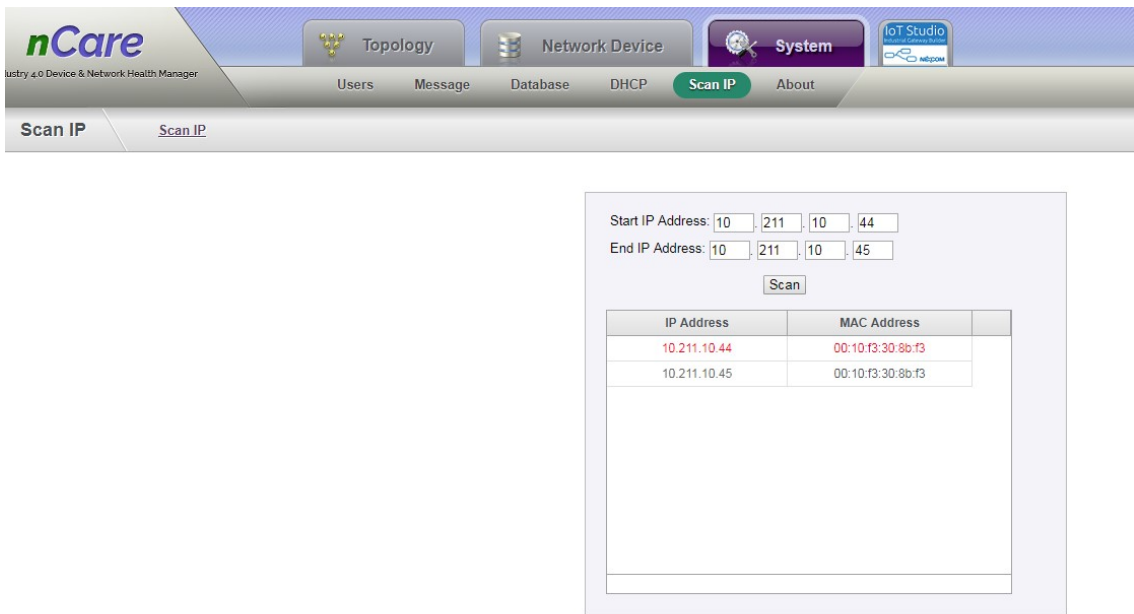


Figure 238 Scan IP List for the Same MAC

### 9.2.3 Set as Loop with Mistake

If devices are set as loop with mistake, an alarm will be sent and the aberrant message will be list as event under main page and on Event Log.

\* Devices' System Log Server should be set on nCare first for those that set as loop with mistake.

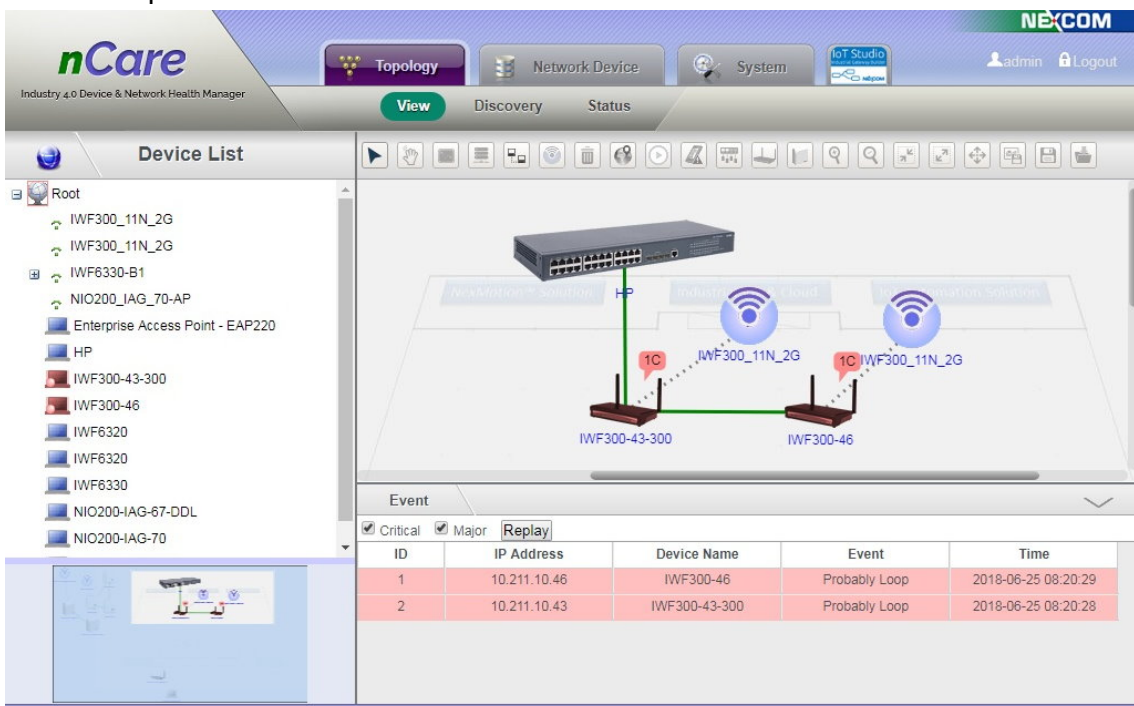


Figure 239 Event for Devices set as Loop with Mistake on Main Page

The screenshot shows the nCare web interface. At the top, there are navigation tabs: Topology, Network Device, System, and IoT Studio. Below these are sub-tabs: Manage, Log (selected), Usage, Severity, Interval, Group, and Rogue AP/Device. The main content area is titled 'Log' and includes sub-tabs for Event Log, System Log, and Playback. On the left, there is a search filter panel with the following options:

- Begin Date: [Begin Date]
- End Date: [End Date]
- IP Address: [IP Address]
- Severity:  Critical
- Device Name: ncare
- Clear
- Search button

The main table displays a list of events with the following columns: ID, IP Address, Device Name, Severity, Status, and Time. The table contains 17 rows of data, with rows 20, 21, and 25 highlighted in red. Row 20 is checked.

ID	IP Address	Device Name	Severity	Status	Time
9	10.211.10.67	NIO200-IAG-67-DDL	Critical	Polling Failed	2018-06-25 17:29:56
10	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:29:56
11	10.211.10.41	Enterprise Access Point - EAP220	Critical	Polling Failed	2018-06-25 17:26:45
12	10.211.10.47	IWF6330	Critical	Polling Failed	2018-06-25 17:26:45
13	10.211.10.50	IWF6320	Critical	Polling Failed	2018-06-25 17:26:45
14	10.211.10.51	IWF6320	Critical	Polling Failed	2018-06-25 17:26:45
15	10.211.10.57	3310	Critical	Polling Failed	2018-06-25 17:26:45
16	10.211.10.41	Enterprise Access Point - EAP220	Critical	Polling Failed	2018-06-25 17:23:34
17	10.211.10.47	IWF6330	Critical	Polling Failed	2018-06-25 17:23:34
18	10.211.10.50	IWF6320	Critical	Polling Failed	2018-06-25 17:23:34
19	10.211.10.51	IWF6320	Critical	Polling Failed	2018-06-25 17:23:34
20	10.211.10.52	PingableDevice	Critical	Polling Failed	2018-06-25 17:23:34
21	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:23:34
22	10.211.10.46	IWF300-46	Critical	Probably Loop	2018-06-25 08:23:54
23	10.211.10.43	IWF300-43-300	Critical	Probably Loop	2018-06-25 08:23:30
24	10.211.10.46	IWF300-46	Critical	Probably Loop	2018-06-25 08:20:29
25	10.211.10.43	IWF300-43-300	Critical	Probably Loop	2018-06-25 08:20:28

Figure 240 Event for Devices set as Loop with Mistake on Event List

## 10Appendix 1

The setting process of sending alarm message by twitter:

- (1) Register for a twitter account.
- (2) Login by twitter Apps: <https://apps.twitter.com/>

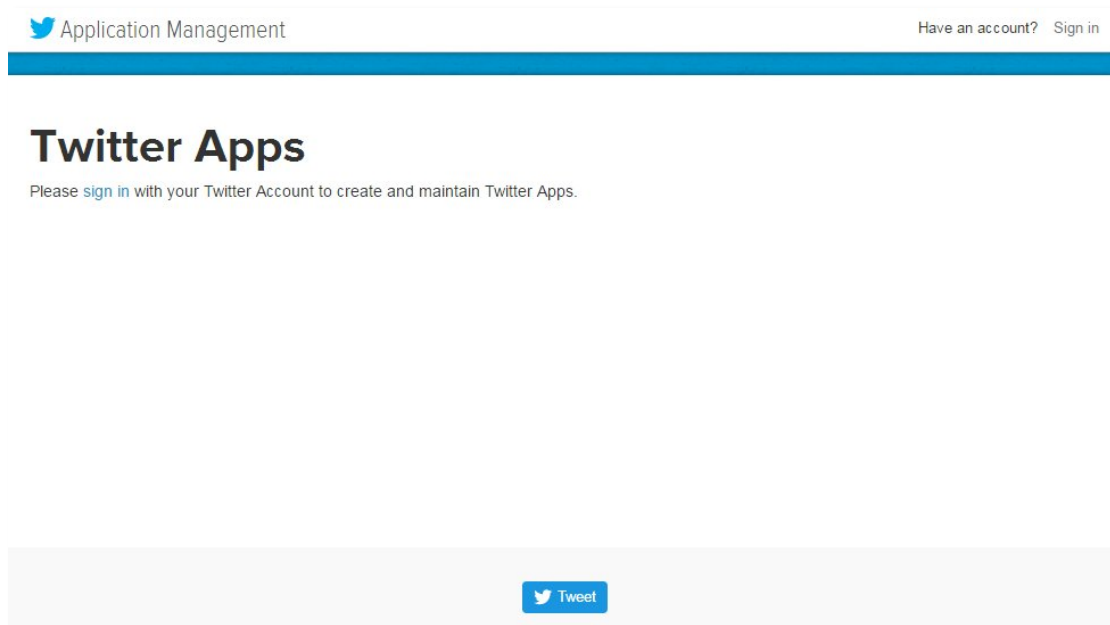


Figure 241 Login to Twitter Apps

- (3) Click **Create New App** to build a new program.



Figure 242 Build a New Program

- (4) Enter Create an application page then enter related information. (Please left blank for Callback URL)
- (5) Read **Developer Agreement** then click **Yes, I agree**.

(6) Click **create your Twitter application**.

**Create an application**

**Application Details**

**Name \***

Your application name. This is used to attribute the source of a tweet and in user-facing authorization screens. 32 characters max.

**Description \***

Your application description, which will be shown in user-facing authorization screens. Between 10 and 200 characters max.

**Website \***

Your application's publicly accessible home page, where users can go to download, make use of, or find out more information about your application. This fully-qualified URL is used in the source attribution for tweets created by your application and will be shown in user-facing authorization screens. (If you don't have a URL, yet, just put a placeholder here but remember to change it later.)

**Callback URL**

Where should we return after successfully authenticating? OAuth 1.0a applications should explicitly specify their oauth\_callback URL on the request token step, regardless of the value given here. To restrict your application from using callbacks, leave this field blank.

**Developer Agreement**

You may be given access to certain non-public information, software, and specifications relating to the Licensed Material ("Confidential Information"), which is confidential and proprietary to Twitter. You may use this Confidential Information only as necessary in exercising your rights granted in this Agreement. You may not disclose any of this Confidential Information to any third

Figure 243 Create an application page

(7) You' ll see the page shown below after complete setting.

Your application has been created. Please take a moment to review and adjust your application's settings.

Test OAuth

Details Settings Keys and Access Tokens Permissions

**Organization**

Information about the organization or company associated with your application. This information is optional.

Organization

Organization website

**Application Settings**

Your application's Consumer Key and Secret are used to authenticate requests to the Twitter Platform.

Access level

Consumer Key (API Key)

Callback URL

Callback URL Locked

Sign in with Twitter

App-only authentication

Request token URL

Authorize URL

Access token URL

Figure 244 Obtain Application Data



- (8) Go to Permissions page.
- (9) Choose *Read and Write* for Access.
- (10) Click **Update Settings**.

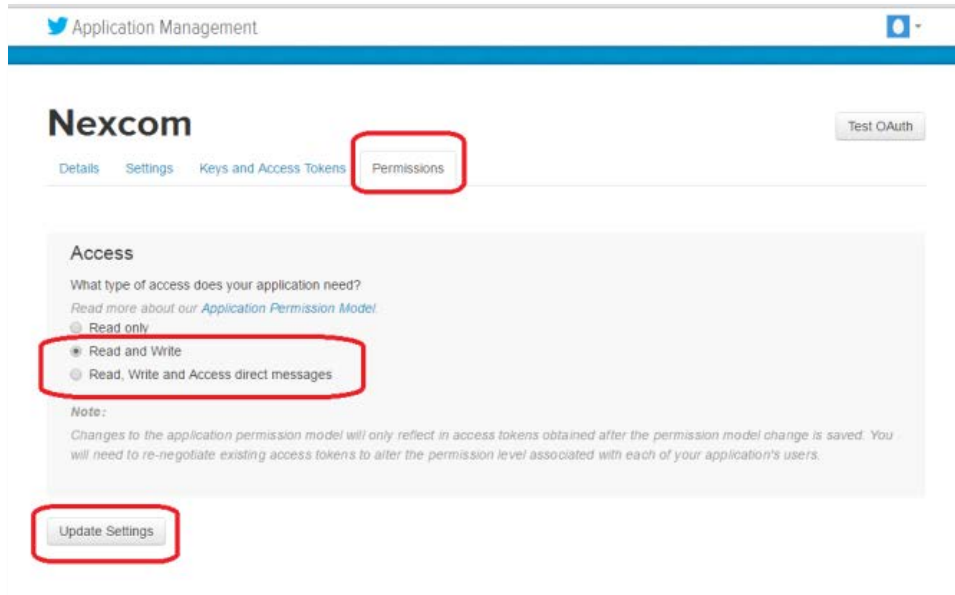


Figure 245 Permission Selection

- (11) Go to Keys and Access Token page.
- (12) Click **Create my access token** for your own authorization.

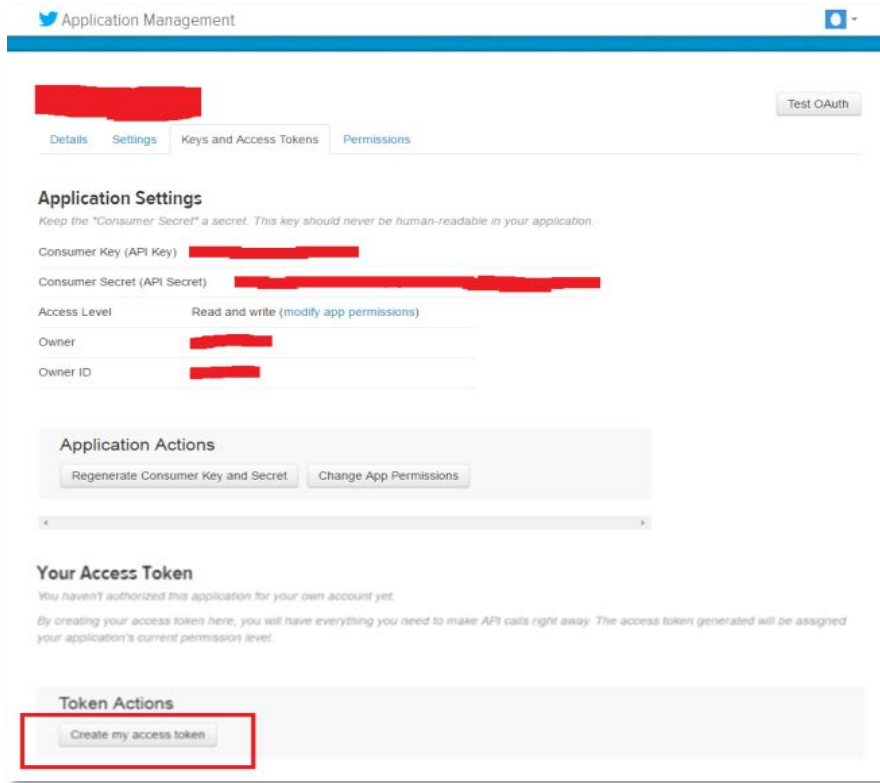


Figure 246 Permission Opening

(13) Back to Twitter Apps page. Enter the *Consumer Key* and *Consumer Secret* on this page into the related information area on nCare System>Message>Social Media>Twitter page.

(14) Click **Login**.

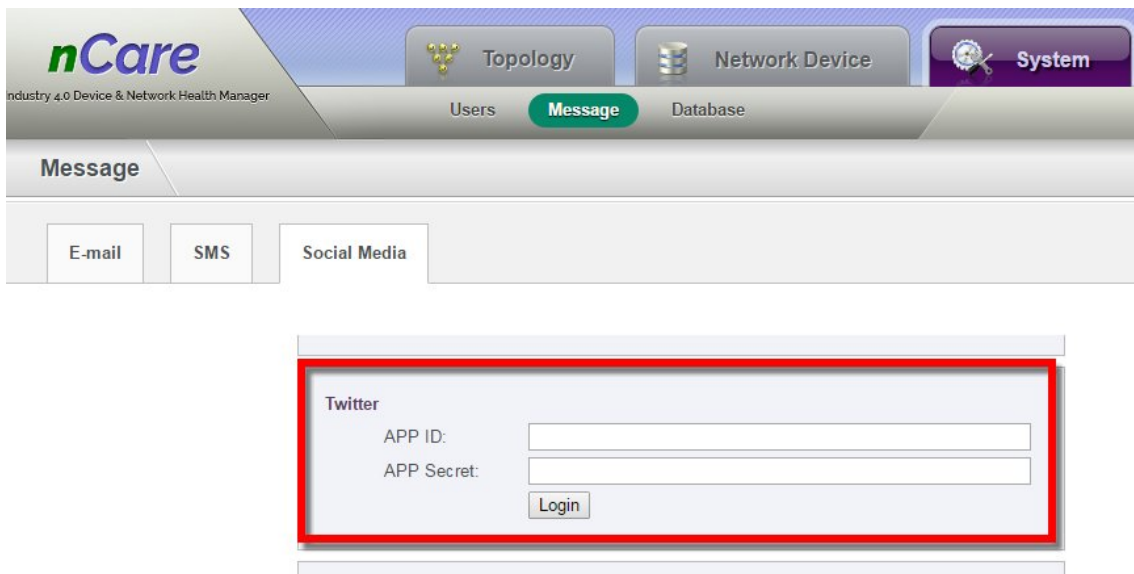


Figure 247 Enter APP ID and APP Secret

(15) Click **Authorize Program**.



Figure 248 Twitter Authorization Page

(16) A PIN code will pop-up.



Figure 249 Twitter PIN Code

(17) Enter the PIN code on nCare.

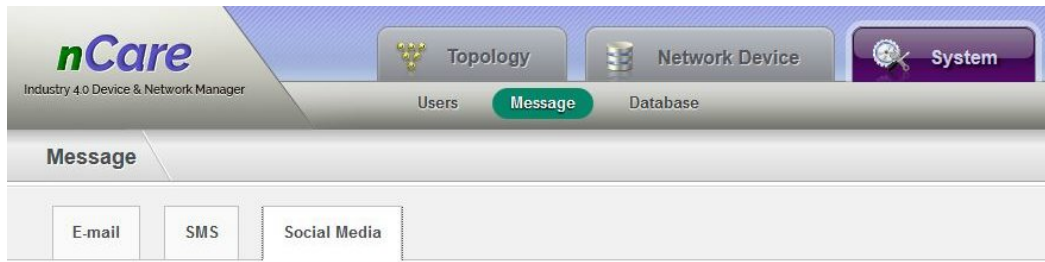
This is a configuration form for social media integration. It has two sections: 'Line' and 'Twitter'. The 'Line' section has fields for 'Account:' and 'Password:', followed by a 'Login' button. The 'Twitter' section has a 'PIN Code' field and an 'Apply' button. A red rectangular box highlights the 'PIN Code' field and the 'Apply' button.

Figure 250 Enter PIN Code

(18) After logging-in, click **Test** to send a test message to Twitter.

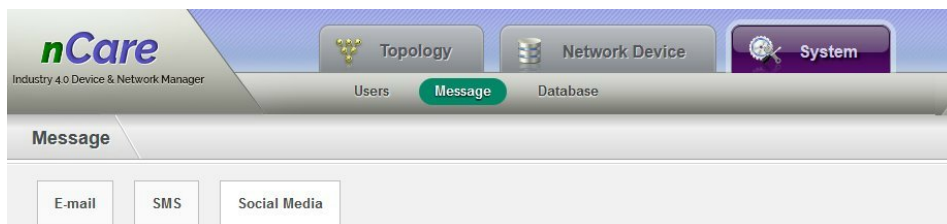
This screenshot shows the configuration form after logging in. It contains three sections: 'WeChat', 'Line', and 'Twitter'. The 'WeChat' section has fields for 'APP ID:', 'Corp ID:', and 'Corp Secret:', with a 'Login' button. The 'Line' section has fields for 'Account:' and 'Password:', with a 'Login' button. The 'Twitter' section shows a green profile picture icon, the name 'Scott Hsieh', and two buttons: 'Logout' and 'Test'. A red arrow points to the 'Test' button.

Figure 251 Send Twitter Test Message

(19) The test message will be shown on Twitter page.

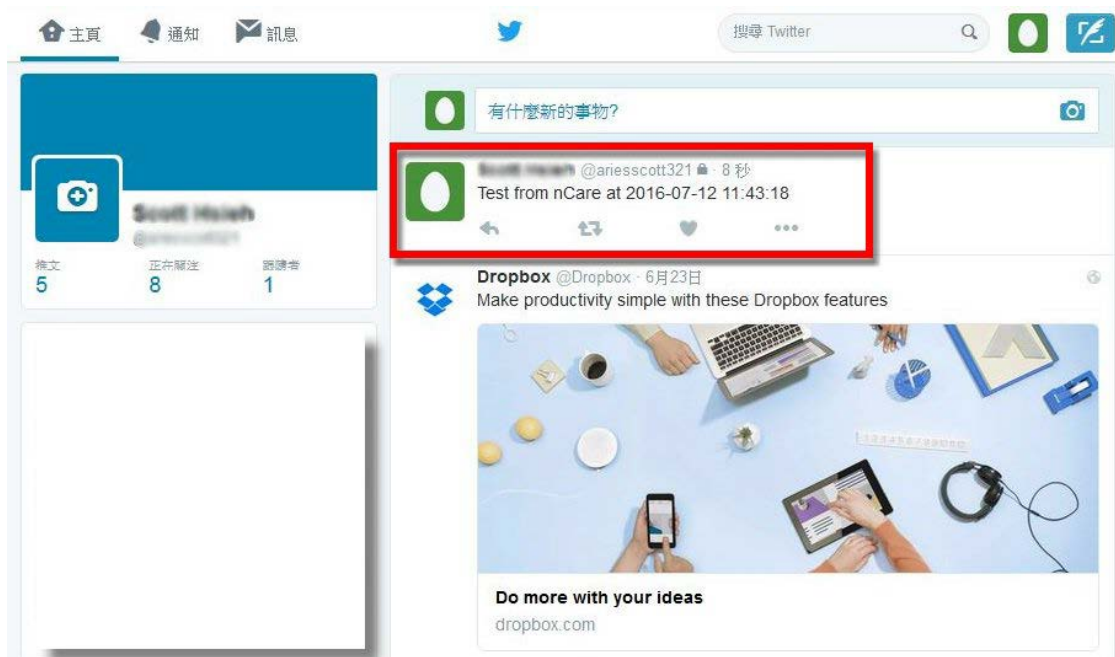


Figure 252 Test Message Sent Successfully