nCare IoT Management System

User's Manual

Content

1	Outline for nCare1			
2	In	trodu	ction for nCare Environment	
	2.12.22.3	2.1.1 2.1.2 Harc	Requirement Server-End Client-End dware Requirement ice Management	3 3 3
3	In	trodu	ction for nCare Installation	5
	3.13.23.3	Unir	allation for nCare nstallation for nCare re Activation	5
4	In	struct	tion for nCare Login	7
	4.1	Proc	edures for Logging in	7
5	In	terfac	e Illustration for nCare System	
	5.1	User	rs Management	
		5.1.1	Introduction for Account Management	
		5.1.2	Operation for Account Management	
	5.2		sage Management	
		5.2.1	Introduction for Message Management Operation for Message Management	
	5.3		abase Management	
		5.3.1	Introduction for Database Management	
		5.3.2	Operation for Database Management	
	5.4	DHC	P Management	20
		5.4.1	Introduction for DHCP Management	20
		5.4.2	Operation for DHCP Management	21
	5.5	Scar	ו IP	
		5.5.1	Introduction for Scan IP	24

		5.5.2	Operation for Scan IP	24
	5.6	Abou	ıt	25
		5.6.1	Introduction for License	25
		5.6.2	Operation for License	25
6	Int	trodu	ction for nCare Network Device Setting Interface	28
	6.1	Func	tions 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 N	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	
		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	Seve	rity	67
		6.4.1	Introduction for Severity	67
		6.4.2	Operation for Severity	
	6.5	Inter	val	68

		6.5.1	Introduction for Interval	68
		6.5.2	Operation for Interval	68
	6.6	Торо	ology Group	69
		6.6.1	Introduction for the Topology Group	69
		6.6.2	Operation for Topology Group	69
	6.7	Rogu	Je AP/Device	70
		6.7.1	Introduction for the Rogue AP/Device	70
		6.7.2	Operation for Rogue AP/Device	70
7	Int	trodu	ction for the Topology Interface of nCare	78
	7.1	Торо	ology View	
		7.1.1	Introduction for Topology View	78
		7.1.2	Operation for Topology View	78
	7.2	Devi	ce Discovery	118
		7.2.1	Introduction for Device Discovery	
		7.2.2	Operation for Device Discovery	118
	7.3	Devi	ce Status	
		7.3.1	Introduction for Device Status	
		7.3.2	Operation for Device Status	121
8	In	trodu	ction for IoT Studio	130
9	nC	Care N	laintenance and Management	131
	9.1	Acce	ss Control	131
		9.1.1	System User	131
		9.1.2	Device Manager	
		9.1.3	System Administrator	
	9.2	Devi	ce Aberrant Status	134
		9.2.1	Same IP	134
		9.2.2	Same MAC	
		9.2.3	Set as Loop with Mistake	
10	Ap	ppend	lix 1	138

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	
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 APP ID and APP Secret	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 Wireless Security 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 Dev	vice
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	
Figure 165 Check for NIO200-HAG Group Devices	
Figure 166 NIO200-HAG Group Devices Disconnected	
Figure 167 Account Setting Window for NIO200-IAG	
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	
Figure 179 Adding NIO50 Device to Topology Group	
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 Subnet112
Figure 198 Purple Line113
Figure 199 Purple Bold Line113
Figure 200 VLAN Status
Figure 201 Normal Link114
Figure 202 High Traffic Link114
Figure 203 Disconnected Link115
Figure 204 Link Over the Threshold115
Figure 205 Shortcut Key116
Figure 206 Ping Function117
Figure 207 Reboot Function117
Figure 208 Remote Desktop
Figure 209 Device Discovery119
Figure 210 Recent Searching Records of IP Range119
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
Figure 218 WMI Page for IPC Device
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 Studio130
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 MAC136
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 Program138
Figure 243 Create an application page 139
Figure 244 Obtain Application Data 139
Figure 245 Permission Selection140
Figure 246 Permission Opening141
Figure 247 Enter APP ID and APP Secret141
Figure 248 Twitter Authorization Page142
Figure 249 Twitter PIN Code142
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

2.1.1Server-End

Ta	able 1 Device of Server-End
Operation System	Window 7
Web Server	Tomcat 7.0
Database Server	MySQL (free)

2.1.2Client-End

Ta	able 2 Device for Client-End
PC Browser	Firefox, IE11, Chrome

2.2 Hardware Requirement

	Table 3 Hardware Requiremer	nt
Device	Туре	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

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

Table 4 Device Management

Device Server	NIO50 · NIO51
Switch	IGS-402SM-4PH24 \ IGS-402SM-8PH24 \
SWILCH	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.

Control Panel Home	Uninstall or change a program				
View installed updates	To uninstall a program, select it from the list and th	en click Uninstall, Change, or Rep	pair.		
Turn Windows features on or off					
	Organize 🔻				
		Publisher	▼ Install ▼ Sia		Version +
	Valle - V 27-Zip 16.02 (x64)	I gor Pavlov	2016/8/3	4.75 MB	
	Apache Tomcat 7.0 Tomcat7 (remove only)	Igor Paviov	2016/8/3	4.75 MD	7.0.56
	Google Chrome	Google Inc.	2016/7/15		52.0.2743.116
	Slobyle Chrome Sava 7 Update 71 (64-bit)	Oracle	2016/7/15	110 MD	7.0.710
	Sava 7 Update 71 (64-bit)	Oracle Oracle Corporation	2016/7/14 2016/8/3	106 MB	8.0.1010.13
	🚔 Java SE Development Kit 7 Update 71 (64-bit)	Oracle Oracle	2016/7/14		1.7.0.710
	Sava SE Development Kit 8 Update 101 (64-bit)	Oracle Corporation	2016/8/3	100000000000000000000000000000000000000	8.0.1010.13
	ManageEngine MibBrowser 5	ZOHO Corp.	2016/8/4	320 MD	5.2
	Managechgine Mobrowser 5	Microsoft Corporation	2016/7/14	00.0 MD	4.0.30319
	Microsoft .NET Framework 4 Extended	Microsoft Corporation	2016/7/14		4.0.30319
	Microsoft Visual C++ 2008 Redistributable - x86 9		2016/7/14		9.0.21022
	Microsoft Visual C++ 2012 Redistributable (x64)		2016/7/14		11.0.61030.0
	Microsoft Visual C++ 2012 Redistributable (x64)		2016/8/4		12.0.30501.0
	Microsoft Visual C++ 2013 Redistributable (x84)		2016/8/3		12.0.30501.0
	Microsoft Visual C++ 2013 Redistributable (x86)	Microsoft Corporation Microsoft Corporation	2016/8/3		14.0.23026.0
	MySOL Installer - Community	Oracle Corporation	2016/7/14		1.4.2.0
	MySQL Installer - Community MySQL Server 5.6	Oracle Corporation	2016/7/14	300 MB	
	MySQL Server 5.6	Oracle Corporation		139 MB	
	Care (remove only)	Oracle Corporation	2016/7/18 2016/8/9	139 MD	0.5.7
		TeamViewer	2016/7/20		11.0.63017
	Tftpd64 Service Edition (remove only)	Teamviewer			11.0.63017
	WinPcap 4.1.3	Directory Technology, Tech	2016/8/3		4.1.0.0000
		Riverbed Technology, Inc.	2016/8/4	1/1 100	4.1.0.2980
	Wireshark 2.0.5 (64-bit)	The Wireshark developer com	. 2016/8/4	161 MB	2.0.5

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 lan0.

(5) Enter the information above to activate nCare. And other users can use the system on browser or APP then.

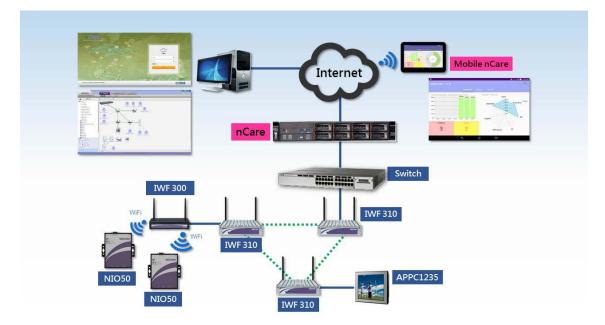


Figure 3 nCare User Scenario

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*.

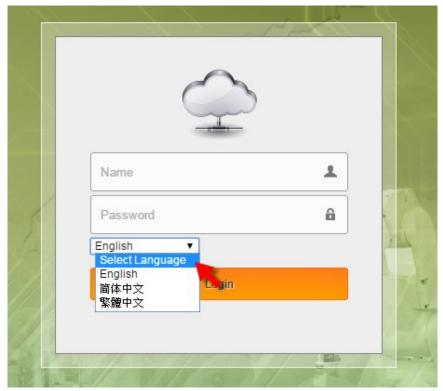


Figure 5 Interface Language Selection

- (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"

	\sim		1/1 -
	G.	5	
	Name	Ŧ	1
1	Password	â	Name is not entered
14	English V		
	Login		7.
			1 strok

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.

Login

nCare

nCcire Insuitry « Blaves & Network Headth Manager	Topology Image: Network Device System Image: System View Discovery Status	NÈ(COM Ladren Blagad
Device List		
3 X KOA		
1		
	Event	~

Figure 7 Logout from the System

5 Interface Illustration for nCare System

5.1 Users Management

5.1.1Introduction for Account Management

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

5.1.20peration for Account Management

- 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.

User Name:		*	
Password:		*	
Confirm Password:		40	
Email :		:1:	
Mobile Phone:	-	10	
	[Country Code] - [Phone	Number]	
Access Level:	Administrators	Y	
TopologyGroup:	Root Group		

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)

User Name:		-11
Password:		11:
Confirm Password:		38
Email :		:1:
Mobile Phone:	-	4
	[Country Code] - [Pho	ne Number]
Access Level:	Administrators	T
TopologyGroup:	Administrators Managers Users	

Figure 9 Access Level

(4) If <u>Users</u> 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)

User Name:	*	
User Name:		
Password:	di.	
Confirm Password:	*	
Email :	*	
Mobile Phone:	*	
	[Country Code] - [Phone Number]	
Access Level:	Users	
TopologyGroup:	Emer Root Group	

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.

User Name:		at 🚺	
Password:		* !	
Confirm Password:		* Password	is not enter
Email :		* !	
Mobile Phone:	<u>!</u>	ate _ 1	
	[Country Code] - [Ph	one Number]	
Access Level:	Administrators	•	
TopologyGroup:	Root Group		

Figure 11 Error Message for Create User Account

Delet

Root

Root

manager

Event

nCare		W Topology	Network Device	🔍 System	NOT Studio
dustry a 0 Device & Network He	alth Manager	Users Message	Database DHCP	Scan IP About	

000-0000000

000-00000000

000-0000000

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

Figure 12 User List with Modify and Delete icons.

Managers

5.2 Message Management

accountia

manager@gmail.con

r@gmail.co

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

- 5.2.2.1E-mail
- (1) To test this function, test mail should be linked by mail server of the corporation. Select <u>ExchangeServer</u> 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.

nCare Industry 40 Device & Network Health Manager	Users	ppology Message	Database	k Device DHCP	Scan IP	System About	IoT Studio Prome Convey Bude Conversion
Message							
E-mail SMS	Social Media Not	ification Users					
	SMTP Service By: SMTP Host: SMTP Port: Account: Password:	ExchangeServe ExchangeServe GMAIL 587 SSL Apply					
	Test E-Mail to:	Test					

Figure 13 E-mail Test

5.2.2.2SMS

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

nCare	🐺 Topology	Network Device	System
Message	Users Message	Database DHCP	Scan IP About
E-mail SMS	Social Media Notification Users		
1			
	Service By: Clickatell ▼ API ID:		
	User:		
	Apply	-	
	Test		
	Mobile Phone: Country Code	- Mobile Phone Number	
	Test		

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.

D:0Kb/s	ی:«א: און 469 u:oкb/s +469193118982	•■ 上午 く	9:24
	06/30/2016(週四)		
	This is Test SMS from nCare! 上午9:24		
② 輔	入訊息		

Figure 15 SMS Test Message

5.2.2.3Social Media

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

(1) WeChat

- a. Apply personal WeChat account
- b. Follow 上海兟汉信息科技
- 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 上海兟汉信息科技
- e. Enter the information on nCare, then click Login.

,	ork Health Manage	n.	Users Message	Database	DHCP	Scan IP	About
Message							
E-mail	SMS	Social Media	Notification Users				
							_
		WeChat					
		APP ID:					
		Corp ID:					

Figure 17 WeChat Setting Information

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

Message							
E-mail	SMS	Social Media	Notifi	cation Users			
		WeChat		20			
				nCare Network Mana	gement System		

Figure 18 WeChat Message Test

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

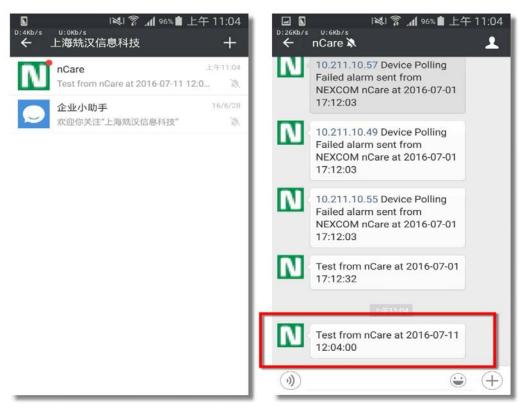


Figure 19 Test Message List of WeChat Target

- (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)

0 Device & Netwo	ork Health Manage	r	Users Message	Database	DHCP	Scan IP	About
essage							
E-mail	SMS	Social Media	Notification Users				
							_
		Twitter					
		APP ID: APP Sec	-				

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

Device & Network Health Manage		Topology	Netwo	ork Device		Systen
essage	U	sers Message	Database	DHCP	Scan IP	About
E-mail SMS	Social Media	Notification Users				
	WeChat					
	APP ID: Corp ID: Corp Secret:					
		Login				
	Twitter	Scott Hsieh				
		Logout	est 🛑			

Figure 21 Sending Test Message to Twitter

f. The test message will be shown on Twitter.

1 ij	〔 4 通知	11.10.	y 担礎 Twitter	۷ 🚺 💋
			有什麼新的事物?	Ø
Ø	Scott Hai	uh -	@ariesscott321	
推文 5	正在關注 <mark>8</mark>	認請者 1	Dropbox @Dropbox - 6月23日 Make productivity simple with these Dropbox features	6
			Do more with your ideas dropbox.com	vç

Figure 22 Twitter Test Message Successfully Sent

5.2.2.4Notification 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.

			Users	Message Databa	ise DHCP	Scan IP	Abo
Message							
E-mail	SMS	Social Med	a Notifica	ation Users			
	Sev	erity: Critical 🔹	Notification Type	Email •			
	Not	ification Users:		Email SMS			
		User Name	Access Level	Email	Mobile Phone	TopologyGroup	4
_		admin	Administrators	account@	000-0000000	Root	
		manager	Managers	manager@gmail.com	000-00000000	Root	
	œ			user@gmail.com	000-00000000	Root	
		user	Users	user@gmail.com	000 0000000		

Figure 23 Severity, Notification Type and Receiver Setting

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

Message							
E-mail	SMS	Social Media	Notificat	tion Users			
	Noti	fication Users: User Name	Access Level	Email	Mobile Phone	TopologyGroup	
		admin	Administrators	account@	000-0000000	Root	
	۲						
	۲	manager	Managers	manager@gmail.com	000-00000000	Root	
	1.000.0			manager@gmail.com user@gmail.com	000-00000000	Root Root	

Figure 24 Notification Users Setting

5.3 Database Management

5.3.1Introduction 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.

5.3.2Operation for Database Management

- 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.

nCare	🐺 Topology	Netwo	ork Device		System
stry 40 Device & Network Health Manager	Users Message	Database	DHCP	Scan IP	About
Database Event Log Mgmt					
Recycling Event					
Maximum reserved event period	l: 30 days (1-365)				
Maximum number of events: 100	ooo events (10,000-1,00	00,000)			

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.

5.4.2Operation for DHCP Management

- 5.4.2.1DHCP Setting
- (1) Connect the device with nCare for IP setting.
- (2) Enter the webpage of device and go to *Network>Interfaces*.

NEXCOM IWF300 Status -	System - Network - Logout	UNSAVED CHANGES: 8 AUTO REFRESH ON
Status	Interfaces Wiffi	
System	Switch DHCP and DNS	
Hostname	IV Hostnames	
Model	V Static Routes	
Firmware Version	IV Diagnostics (git-15.216.69575-t	bb7ea3e)
Kernel Version	3.14.27	
Local Time	Sat Nov 5 04:13:33 2016	
Uptime	18h 25m 3s	
Load Average	1.42, 0.68, 0.45	
Memory		
Total Available	89144 kB / 126316 kB (70%)	

Figure 26 Device Setting Webpage

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

NEXCOM IWF300	EXCOM IWF300 Status - System - Network - Logout UNSAVED CHANGES: 8 AUTO REFRESH ON		
Interfaces Interface Overview			
Network	Status	Actions	
LAN 5 ^g (<u>TTTTT & C</u>) br-lan	Uptime: 20h 32m 10s MAC-Address: 00:10:F3:30:88:6F RX: 11.17 MB (173208 Pkts.) TX: 7.98 MB (72111 Pkts.) IPv4: 10.211.10.72/24	🖉 Connect 🐵 Stop 🗹 Edit 💌 Delete	
WAN	Uptime: 21h 33m 20s MAC-Address: 00:00:00:00:00 RX: 137.52 KB (1829 Pkts.) TX: 398.43 KB (2662 Pkts.) IPv4: 192.168.0.1/24	🖉 Connect 🥥 Stop 🛛 Edit 💌 Delete	
Add new interface Global network option	15 fdb2:26bc:7614::/48		

Figure 27 WAN or LAN Setting Page Selection

(4) Enter the setting page, choose <u>DHCP client</u> as Protocol from the pull-down menu.

NEXCOM IWF300	Status - System - Netwo	ork 🗝 Logout	UNSAVED CHANGES: 8 AUTO REFRESH ON
Status	br-lan F F T	Jptime: 20h 38m 14s 4AC.Address: 00:10:F3:30:88:6F 4X: 11.30 MB (174761 Pkts.) FX: 8.38 MB (73345 Pkts.) Pv4: 10.211.10.72/24	
Protocol	Static address Static address	•	
IPv4 address	DHCP client Unmanaged PPP	×	
IPv4 netmask	PPtP PPPoE PPPoATM		
IPv4 gateway	UMTS/GPRS/EV-DO L2TP		
IPv4 broadcast			
Use custom DNS servers		1	
IPv6 assignment length	disabled ② Assign a part of given leng	th of every public IPv6-prefix to this	nterface
IPv6 address			

Figure 28 WAN or LAN Setting Page Selection

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

NEXCOM IWF300 Status	- System - Network	< ← Logout	UNSAVED CHANGES: 8 AUTO REFRESH ON
Interfaces - LAN On this page you can configure the networ network interfaces separated by spaces. Common Configuration			"bridge interfaces" field and enter the names of several eth0.1).
General Setup Advanced Settings	Physical Settings	Firewall Settings	
Status	br-lan MA RX TX:	time: 20h 44m 4s (C.Address: 00:10:F3:30:8B:6F : 11.41 MB (176158 Pkts.) : 8.60 MB (74327 Pkts.) 4: 10.211.10.72/24	
Protocol DHCF	? client		
Hostname to send when requesting DHCP	00	•	
🖷 Back to O	verview		Save & Apply Save Reset

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

nCa	re	🦞 Тор	ology	Netwo	ork Device		System
Industry 4.0 Device & Net	work Health Manager	Users	Message	Database	DHCP	Scan IP	About
DHCP							
Setting	Client List						

Enable:	
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:	
Lease Time (s):	* 60s ~ 2592000s (30 days)
	Apply

Figure 30 DHCP Enabling

5.4.2.2DHCP Client List

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

nCare		Topology Users Me		Network Device	Scan IP Abo	stem	T Studio
DHCP	Client List						
	Server IP 192.168.1.10	MAC Address 00:10:F3:30:8B:6F	Name IWF300	Auto Config Date 2016-11-09 17:39:35	Lease 2016-11-09		

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" .

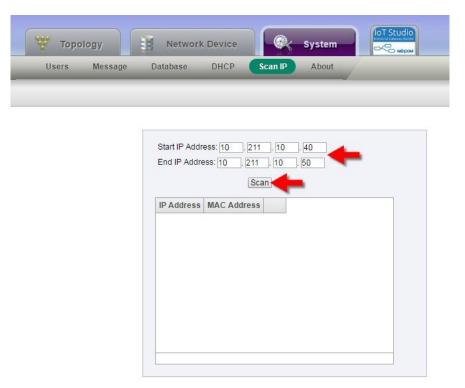


Figure 32 Enter IP Range

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

Topology	Network Device	System	
Users Message	Database DHCP	Scan IP About	
	Start IP Address: 10 . 21	1 . 10 . 40	
	End IP Address: 10 . 21	I . 10 . 50	
	S	can	
	IP Address	MAC Address	
	10.211.10.41	00:10:f3:32:7c:aa	
	10.211.10.42	00:10:f3:3f:66:02	
	10.211.10.43	00:10:f3:30:8b:a7	
	10.211.10.44	00:10:f3:30:8b:f3	
	10.211.10.46	00:10:f3:30:8b:a3	
	10.211.10.40		
	10.211.10.47	00:10:f3:36:f1:c3	

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.

5.6.20peration for License

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

nCare	Topology Network Device System
Industry 4.0 Device & Network Health Manager	Users Message Database DHCP Scan IP About
About License	
	License Model: IWF800 nCare Status: Perpetual Maximum Number of Devices: 1000 Current Number of Devices: 39 Version: v1.3.1 CMS:2506,EMS:2504

Figure 34 Status for Perpetual Version

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

nCare	🕎 Topology	Network Device
ustry 40 Device & Network Health Manager	Users Messa	age Database DHCP Scan IP About
About License		
		License
		Model: nCare (Trial Version)
		Status: The license will expire after 29 days
		Maximum Number of Devices: 1000 Current Number of Devices: 39
		Version: v1.3.1 CMS:2506,EMS:2504

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.

n Corre Industry 4 0 Device & Network Health Man(1)	10.22.22.136 顯示: The license will expire after 3 days	×		
		補定	Ŷ	,
		the state	admin English •	± 6
		TUNIN.	Login	

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.

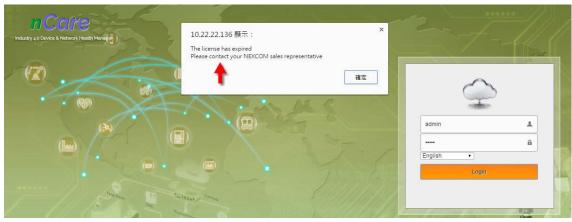


Figure 37 License Expired Inform

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.

6.1.20peration for Device List

- 6.1.2.1Device Check
- (1) Different kinds of Device Type are list at the left. Click on the Type to check for the related information of devices.

7 20 000	ice & Network Health Manag	"	Manage	Log	Usage	Severit	y Interval Gro	sup	Rogue AP/De	vice							
Mana	ige <u>Devic</u>	ce_List	Config Backup	Config Restor	e Fw Up	grade	Device Provision	Modbus	Profile								
	Device Type		Show/Hide	Rogue Devices	6												
			л́ ID	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	De
-	IWF	>	00 0e 8e 67 5b ad	IWF300-63	10 211 10 63	IWE	IWF300_11N_2G_63	ap	psk2	6	0	0	h	ff	C		1
			00.00.80.67.50.40	IWP300-63	10.211.10.63	IWF	WF300_11A_5G_mesh	mesh	none	36	0	0	4	12	0		1
J.			00:10:13:5e:28:57	IWF310-44	10.211.10.44	IWE	IWF310_11N_2G_44	ар	psk2	11	0	0	n	er E	0	-	1
Ú.	Mobile Mesh	>	00.10.33.56.26.57	IMP310-14	10.211.10.44	TOP:	WF300_11A_5G_mesh	mesh	none	36	0	U	4	13	0	-48	1
			00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	IWE	IWF300_11N_2G_46	ap	psk2	11	0	0	n	132	O		1
	Device Server	~	00.08.08.07.58.90	141-200-40	10.211,10.40	TAAL	IWF300_11A_5G_mesh	mesh	none	36		0	4	12	0		1
	Device Server	>	00.0e 8e 67 5fa5	IWF300-64	10 2 11 10 64	IWE	IWF300_11N_2G_64	ар	psk2	11	0	0	h	F	C		
			00.00.00.07.5645	MF300-04	10.211.10.04	IVIE	IWF300_11A_5G_64	ap	wpa	48		0	"	12	0		I
	IWSN Gateway	>	00:0e:8e:67:57:87	IWF300-43	10.211.10.43	IWE	IWF300_11N_2G_43	ap	psk2	11	0	0	n	管	0		1
		6	A 00.00.00.01.01.01	1018-300-43	10.211.10.43	INT	IWF300_11A_5G_43	ap	psk2	36		U	"	13	U	-	Ō

Figure 38 Device List that Sorting by Device Type

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

Mana	no Deul		Conflig Backup Cor			everity	Interval Group		ue AP/Devic		-	-	-	-	-	-	-
Mana	Device Type	ce List	Show/Hide Rog		1 Yw Opgrac	ie i r	evice i rovision m	00003110	me								
			1 0	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowse	erReboo	tModif	yDe
-	IWF	>	1				IWF300_11N_2G_63	ap	psk2	6	1.2	125	2				
			00 De 8e 67 5b ad	IWF300-63	10.211.10.63	IWF	IWF300_11A_5G_mesh	mesh	none	36	0	0	ħ	T	O	2	1
1				IWF310-44	10 211 10 44		IWF310_11N_2G_44	ap	psk2	11	0	0	h	管	~		
	Mobile Mesh	>	00:10:13:5e:28:57	WVF310-44	10.211,10,44	IWF	IWF300_11A_5G_mesh	mesh	none	36	0	0	"	13	C	-18	1
				IWF300-46	10.211.10.46	IWF	IWF300_11N_2G_46	ар	psk2	11	0 0	D	11	100	C		1
1	Device Server		00:0e:8e:67:5a:90	WVF300-46	10.211.10.46	IWF	IWF300_11A_5G_mesh	mesh	none	36	U	U	4	12	0		
	Device Server	>	•	IWF300-64	10.211.10.64	IWE	IWF300_11N_2G_64	ap	psk2	11	0	0	11	F	o		
			00.0e.8e.67.5f.a5	WF 300-04	10.211.10.04	TWI-	IWF300_11A_5G_64	ар	wpa	48	0	0	11	13	0	-148	1
	IWSN Gateway	>		IWF300-43	10.211.10.43	IWE	IWF300_11N_2G_43	ap	psk2	11	0	0	11	晋	C		
		1	- 00:0e:8e:67:57:87	WP-300-#3	10.211.10.43	IMP	IWF300_11A_5G_43	ap	psk2	36	U	U	"	13	0	~**	1



- 6.1.2.2Add Device
- (1) Click Add icon to create new device.

1 20 000	ce & Network Health Manag		Manage	Log	Usage	Severit	y Interval Gr	oup	Rogue AP/De	vice							
Mana	ge <u>Devi</u>	ce List	Config Backup	Config Restor	e Fw Upj	grade	Device Provision	Modbus	Profile								
	Device Type		Show/Hide	Rogue Devices													
1.1			î ID	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	y Di
-	IWF	>	00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWE	IWF300_11N_2G_63	ар	psk2	6	0	0	n	÷	0		
			00.08.68.07.50.30	IVIF300-03	10.211.10.03	100P	IWF300_11A_5G_mosh	mesh	none	36	U	0	"	1	0	-10	
d.	Mobile Mesh		00:10:13:5e:28:57	IWF310-44	10.211.10.44	INF	IWF310_11N_2G_44	ар	psk2	11	0	0	n	ing .	C		
U.	MODILE MEST	>	00.10.00.00.00.01	111 212 44	10211.10.44		IWF300_11A_5G_mesh	mesh	none	36			~	14	0		
			00 0c 8c 67 5a 90	IWF300-46	10 211 10 46	IWF	IWF300_11N_2G_46	ар	psk2	11	0	0	11	.mr	0		
2	Device Server	>					IWF300_11A_5G_mesh	mesb	none	36			~	14	0	~	
_		1	00:0e:8e:67:5ta5	IWF300-64	10.211.10.64	INF	IWF300_11N_2G_64	ab	psk2	11	0	0	4	177	C		
					10001010001		IMF300_11A_5G_64	ap	wpa	48		×	~	H	0	-	
	IWSN Gateway	>	00 0e 8e 67 57 87	IWF300-43	10.211.10.43	IWE	IWF300_11N_2G_43	ap	psk2	11	0	0	11	100	C		
			*		0.0000000000000000000000000000000000000		IWF300_11A_5G_43	ap	psk2	36	1972	12	1	14	~	1000	

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.

Device Type:	IWF	Ŧ
Protocol:	SNMP	T
Trap Configuration:		
Syslog Configuration:		
Device Name:		4
IP Address:		*
Read Community:	public	18
Write Community:	private	40
Topology Group:	Root	*
Latitude:		
Longitude:		

Figure 41 Information for Creating a new Device

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

Topolo	Creat	e Device	0	E:DOM
lanage				ce
p Cont w/Hide Rogi Dev	Device Type: Protocol:	IWF IWF Mobile Mesh IWSN Gateway	K	Channel
:5b:ad IW	Trap Configuration: Syslog Configuration: Device Name:	Device Server IPC 3rd-Party AP/Device Switch Others	*	11 36
:28:57 IW	IP Address: Read Community:	public	*	11 36 11
:8b:a5 IWF:	Write Community: Topology Group:	private Root	*	36
:8b:71 IW	Latitude:			36
:00:55 IW	Longitude:			- 100
		ОК	Cancel	

Figure 42 Device Type Selection

(6) Choose the *Scan Protocol* with <u>SNMP</u>, <u>Modbus or Python</u>.

Device Type:	Others	•
rotocol:	SNMP	•
Trap Configuration:	SNMP Modbus Python	
yslog Configuration: Device Name:		
Address:		
ead Community:	public	
Vrite Community:	private	
lopology Group:	Root	•
Latitude:		
Longitude:		

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.

Device Type:	IWF	•
Protocol:	SNMP	•
Trap Configuration:		
Syslog Configuration	. 🖉 🔨	
Device Name:		*
IP Address:		
Read Community:	public	*
Write Community:	private	*
Topology Group:	Root	T
Latitude:		
Longitude:		

Figure 44 Scan Protocol Selection

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

Device Type:	IWF	¥
Protocol:	SNMP	v
Trap Configuration:		
Syslog Configuration:		
Device Name:		4
IP Address:		*
Read Community:	public	*
Write Community:	private	4
Topology Group:	Root	T
Latitude:	Root test	
Longitude:	test1 test2 test3	

Figure 45 Topology Group Selection

- 6.1.2.3 Configuration Setting for Device
- 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.

ry 40 Devi	ice & Network Hoalth Manag	ior /	Manage	Log	Usage	Severit	Device	oup	Rogue AP/De	dice.							
Mana		and the d					Device Provision				-	-	-	-	-		
Mana	Device Type	ce List		Rogue Devices		grade j	Device Provision 1	modbus	rrome								
1.1			л ID	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	y De
-	IWF	>	00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWE	IWF300_11N_2G_63	ap	psk2	6	0	0		F	Ó		
			00.06.86.67.50.86	IVVP-300-03	10.211.10.03	ivar-	IWF300_11A_5G_mesh	mesh	none	36	U	U	á.	13	0	-98	
d.			00 10 13 5e 28 57	IWF310-44	10 211 10 44	INF	IWF310_11N_2G_44	ар	psk2	11	0	0	W	eb er	C		
1 1	Mobile Mesh	>	00.1013.36.26.37	MIP310-44	10.211,10.44	TAL.	IWF300_11A_5G_mesh	mesh	none	36		U.	1	14	0	-	
			00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	IVE	IWF300_11N_2G_46	ар	psk2	11	0	0	2		o		
1	Device Server	>	00.00.00.01.00.00	111-200-10	10.211.10.40	m	IWF300_11A_5G_mesh	mesh	none	36		*	"	He.	0	-38	
	period series	1	00:0e:8e:67:5f:a5	IWF300-64	10.211.10.64	INF	IWF300_11N_2G_64	ap	psk2	11	0	0	"	F	Ó	-	
			00.00.00.01.01.85	1111 300-04	10.211.10.04	mit	IWF300_11A_6G_64	ар	wpa	48		0		14	0	-	
	IWSN Gateway	>	00:0e 8e 67 57 87	IWF300-43	10,211,10,43	IWE	IWF300_11N_2G_43	ap	psk2	11	0	0	n	晋	C		
			•	1111 2010 40	10.611.10.40		IWF300_11A_5G_43	ap	psk2	36			~	Ha	0	-	

Figure 46 Device Configuration Setting Page Icon

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

Authorizat	tion Red	quired		
Please enter your u Invalid username ar			again.	
		•		
	Username			
	Password			
🔲 Login 🔞 F	Reset			

Figure 47 Configuration Setting Login Page

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

NEXCOM IWF300	Status - System - Network - Logout
Status	
System	
Hostname	IWF300
Model	Atheros DB120 reference board
Firmware Version	OpenWrt (EU) v0.1.2 / LuCl (git-16.060.65840-1d56267)
Kernel Version	3.14.27
Local Time	Fri Mar 11 17:59:38 2016
Uptime	2d 1h 30m 51s
Load Average	0.39, 0.19, 0.16
Memory	
Total Available	86912 kB / 126316 kB (68%)
Free	83008 kB / 126316 kB (65%)
Buffered	3904 kB / 126316 kB (3%)

Figure 48 Status of Device on Device Configuration Page

6.1.2.4 Device Setting by Mibbrowser

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

ry 40 Deni	ice & Network Health Manag	ин /	Manage	Log	Usage	Severit	/ Interval Gro	oup	Rogue AP/De	vice							
Mana	ige <u>Devi</u>	ce List	Config Backup	Config Restor	e Fw Up	grade	Device Provision	Modbus	Profile		_	_		_	_		Ĩ
	Device Type		Show/Hide	Rogue Devices	£												
1.1			10	Device Name	IP Address	Device Type	8810	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	10
-	IWF	>	00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	INE	IWF300_11N_2G_63	ap	psk2	6	0	0	p	192	0		
			00.09.69.07.50.80	100-03	10.211.10.03	100P	TWF300_11A_5G_mesh	mesh	none	36	0		"		0	-18	
4	Mobile Mesh		00.10.f3.5e.28.57	IWF310-44	10.211.10.44	INF	IWF310_11N_2G_44	ap	psk2	11	0	0	1	MI	Browser	1.	
ų.	Mobile Mesh	>		111 212 44	10.211.10.44	1010	IWF300_11A_5G_mesh	mesh	none	36			1		0	- 148	
			00:0e:8e:67:5a:90	IWF300+46	10.211.10.46	INF	IWF300_11N_2G_46	ар	psk2	11	0	0	2	먣	0		
6	Device Server	>	00.00.00.01.00.00	111 999 19		int.	INF300_11A_5G_mesh	mesh	none	36			"	L.	0	-10	
_		1	00:0e:8e:67:5f:a5	IWF300-64	10.211.10.64	IWE	IWF300_11N_2G_64	ар	psk2	11	0	0	11	T ^{er}	0		
							IWF300_11A_5G_64	ap	wpa	48			4		0		
	IWSN Gateway	>	00:0e:8e:67:57:87	IWF300-43	10.211.10.43	IWF	IWF300_11N_2G_43	ар	psk2	11	0	0	2	E.	0		
			*	1111 000 10	10.211.10.10		IWF300_11A_5G_43	ap	psk2	36			1	1-a	0	- 200	

Figure 49 MIB Browser Icon

(2) Main functions of MIB Browser includes:

Limport 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**, <u>SNMP Table</u> can be shown then.



Clear: Used for clear Query Result.

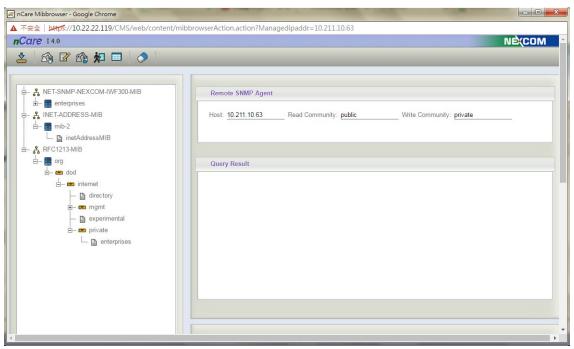


Figure 50 MIB Browser Setting Page

6.1.2.5Device Reboot

	Care Ice & Network Health Marag	a /	W Top Manage	ology Log	E Ne Usage	rtwork (Severit		System	and and a second se	itudio b elecentri vice							
Mana	IGE Devie	ce List 👘		Config Restor		grøde	Device Provision 1	Modbus	Profile								
	Derive type		iD showinde	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Report	Modify	Del
-	IWF	>					IWF300_11N_2G_63	ар	psk2	6				-72			
			00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWF	IWF300_11A_6G_mesh	mesh	none	36	0	0	ħ	f	Ä	-38	1
4			00:10:13:5e:28:57	IWF310-44	10.211.10.44	IWE	IWF310_11N_2G_44	ap	psk2	11	0	0	1	f	Re	boot	
Ψ.	Mobile Mesh	>	00.1033.36.20.57	1011-310-44	10.211,10.44	tore	IWF300_11A_5G_mesh	mesh	none	36	0	v	"	13	0		Ľ
			00 De 8e 67 5a 90	IWF300-46	10,211,10,46	IWE	IWF300_11N_2G_46	ap	psk2	11	0	0	n	F	C		1
1	Device Server	~	00.00.00.01.04.00	ME300-40	10.211.10.40	me	IWF300_11A_5G_mesh	mesh	none	36		U	"	Fil	0		ľ
	Device Server	>	00:0e:8e:67:5ta5	IWF300-64	10.211.10.64	IWE	IWF300_11N_2G_64	ар	psk2	11	0	0	11	귵	o	-	
			00.0e.8e.67,5t.a5	IWI-300-04	10.211,10.04	IVIP	IWF300_11A_5G_64	ap	wpa	48	U	U	4	G	0	-10	ř
	IWSN Gateway	>	00:0e:8e:67:57:87	IWF300-43		IWE	fWF300_11N_2G_43	ap	psk2	11				f	0	-	
		1	- 00:0e:8e:67:57:87	IVII-300-43	10.211.10.43	INF	IWF300_11A_5G_43	ap	psk2	36	0	0	h	14	C	-48	

Figure 51 Device Reboot Icon

- 6.1.2.6Device Modification
- Click a 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.)

ry 4.0 Devi	ste & Notiecrk Health Manag	"	Manage	Log	Usage	Severit	y Interval Gro	oup	Rogue AP/De	vice	8	_	_				
Mana	ige <u>Devi</u>	ce List	Config Backup	Conlig Restor	e Fw Up	grade	Device Provision	Modbus	Profile								
	Device Type		Show/Hide	Rogue Devices	5												
1.1			î ID	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	De
-	IWF	>	00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWF	IWF300_11N_2G_63	ap	psk2	6	0	0	n	19°	~		1
			00.0e.0e.07.50.80	TWP-300-03	10.211.10.03	INAL-	IWF300_11A_5G_mesh	mesh	none	36	0	v	4		0	Á	
4			00 10 /3 5e 28 57	IWF310-44	10 2 11 10 44	IWF	IWF310_11N_2G_44	ар	psk2	11	0	0	ħ	100	C	Me	bd
	Mobile Mesh	>	00.10.15.50.28.57	IME310-44	10.211.10.44	une.	IWF300_11A_5G_mesh	mesh	none	36	U.	0	4	Fi	0	-	
			00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	INF	IWF300_11N_2G_46	ар	psk2	11	0	0	11	- Car	0		
1	Device Server	>	00.00.00.01.08.00	1111 200-10	10,211,10,10	in	IWF300_11A_5G_mesh	mesh	none	36			80	4	U	-	
_	Series series	1	00:0e:8e:67:5fa5	IWF300-64	10.211.10.64	INF	IWF300_11N_2G_64	ap	psk2	11	0	0	11	Los .	O		
			00.00.00.01.01.00	111 300-04	10.2 11.10.04	int	IWF300_11A_5G_64	ар	wpa	48		×	~	14	U	-	
	IWSN Gateway	>	00.0e 8e 67 57.87	IWF300-43	10.211.10.43	INF	IWF300_11N_2G_43	ар	psk2	11	0	0	17	먬	C		
		1		WP300 43	10.211.10.43	INVP.	IWF300_11A_5G_43	ap	psk2	36		°	1	13	0	-98	

Figure 52 Device Modification Icon

(2) With **IWF Device** Type, click ² 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.

General	Wian Via	an	
	WifiRadio:	wlan0	•
IWF	ESSID / Mesh ID:	300_wlan0111	
	Mode:	Access Point	•
	Operating Frequer	су	
	Mode:	11n	•
	Channel:	8 (2.447 GHz)	•
	Width:	20 MHz(AP or Client n	•
	TxPower:	9 dBm (7mW)	•
	Wireless Security		
	Encryption:	WPA2-EAP	•]
	Cipher:	auto	•
	Radius-Authenticat Server	ion- 10.211.10.12	
	Radius-Authenticat Port	ion- 1812	

Figure 53 IWF Device Setting Page

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

hannel:			
	8 (2.44	47 GHz)	•
/idth:	_		•
xPower:	9 dBm	ı (7mW)	•
/ireless Security			_
	WPA2	-EAP	•
ipher:	auto		•
adius-Authentication	-Server	10.211.10.12	
adius-Authentication	-Port	1812	
adius-Authentication	-Secret	•••••	
adius-Accounting-Se	erver	10.211.10.12	
adius-Accounting-Po	ort	1813	
adius-Accounting-Se	ecret		
AS ID:		default	
It will take few sec	onds to	modify.	
	Power: ireless Security noryption: pher: adius-Authentication adius-Authentication adius-Accounting-Se adius-Accounting-Po adius-Accounting-Se adius-Accounting-Se	Power: 9 dBm ireless Security noryption: WPA2 pher: auto adius-Authentication-Server adius-Authentication-Port adius-Accounting-Server adius-Accounting-Port adius-Accounting-Secret AS ID:	Power: 9 dBm (7mW) ireless Security http://www.interpotential adius-Authentication-Server 10.211.10.12 adius-Authentication-Server 10.211.10.12 adius-Accounting-Server 10.211.10.12 adius-Accounting-Port 1813 adius-Accounting-Secret

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.

	M	lodify	y De	vice	9			
General	Wlan		Vlan					
Eth								
VLAN ID:			• (6	5-4094	4)			
VLAN Name:					(6-100)			
12	off 🔹	LAN1	off	•	LAN2	off		
Port: WAN								

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.

Bridge Bridge If	G .	_			7	1	
Bridge If:	lar	ו			•		
Interface:						l(wan)	
	8			ETH:	eth0.	2(lan)	
	8			ETH:	eth0.	3(lan)	
				ETH:	eth0.4	4(lan)	
	1			ETH:	eth0.	5(lan)	
		WNE	T:IWF3	10_11	N_20	3_44_w0-1(N	ULL
Creat B	ridge	e(Web) Refr	esh Ap	ply	Delete Bridge	

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**.

	IVI	odify Device	
General	Wian	Vlan	
Eth			
VLAN ID:		(6-4094)	
VLAN Name:		(6-100)	
Port: WAN o	f •	LAN1 off V LAN2 off V	
LAN3 of		LAN4 off •	
Create Vlan	Delete Vlar		
Bridge			
Bridge If:	lan		
Interface:		ETH:eth0.1(wan)	
interface.		ETH:eth0.2(lan)	
		ETH:eth0.3(lan)	
		ETH:eth0.4(lan)	
		ETH:eth0.5(lan)	
		ET:IWF300_11N_2G_63(lan)	
		T:IWF300_11A_5G_mesh(lan)	
Create Br	idge(Web)	Refresh Apply Delete Bridge	
- T		T	+
		OK Cancel Res	set to Default

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**.

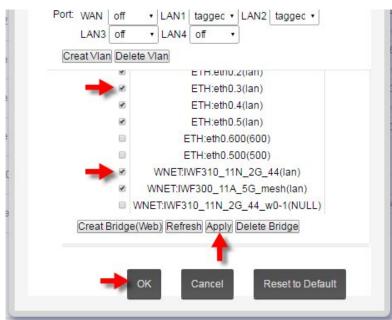


Figure 58 VLAN Interface Selection

(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 <u>Modify Device</u> page for NIO51 module of Device Server series.
 - a. *WifiRadio*, *Operating Frequency* and *Wireless Security* can be set on "Wlan" label.

General	Wlan	Serial/Mo	dhaan		
General	Widii	Senai/wo	ubus		
	WifiRadi	0:	wlan0	•	
Device Server	ESSID /	Mesh ID:	NIO51_11N_2G		
	Mode:		Mesh,802.11s	•	
		ng Frequei	ncy		
	Mode:		2.4G	•	
	Channel		11 (2.462 GHz)		
	Width:		40 minus MHz	•	
	TxPower	1 00 -	10 dBm (10mW)	•	
	Wireles	s Security			
	Encryptic	on:	No Encryption	V	
			It will take few seco	nds to modify.	

Figure 59 Wlan Setting Page for NIO51 Devices

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

	Modify Dev	ice		(
General	Vlan Serial/Modbus			
-	Serial Port Configu	uration		•
Device Server	Mode:	RS232	•	- 1
DeviceServer	Protocol:	Transparent	•	- 1
	Baud Rate:	115200	•	- 1
	Parity:	None	•	- 1
	Data Bits:	8	•	- 1
	Stop Bits:	1	Ŧ	- 1
	Flow Ctl:	None	¥	- 1
	Timeout(ms):	0		- 1
	Terminator:			
	TCP			- 1
	Mode:	Server	•	
	Listen Port:	502		
	Timeout(ms):	180		
			ок Са	ncel

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.

General	Device Server			
	Wi-Fi AP Configur	ation		
Device Server	MAC:	94:A1:A2:87:6E:ED		
	SSID:	WF300_11N_2G_43		
	Encryption:	WPA2/WPA2 MIXED	•	
	Key:	•••••		
	Mode:	RS485	•	
		RS485	•	
	Terminator:			
	Baud Rate:	9600	•	
	Parity:	None	•	
	Stop Bits:	1	•	

Figure 61 Parameters Modification for NIO51 of Device Server

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

General	Wlan WirelessHA	ART	
	*The new setting will t	take effect after device restart	
-	Access Point General	Setting	
WSN Gateway	EUI64:	00-1B-1E-F8-70-06-00-01	
	AP Tag:	NEXCOM AP	
	Network ID:	AAAA	
		Save	
	Gateway General Sett	ing	
	GW Tag:	NEXCOM GW	
	Cache Read Response Timeout:	60	
	Cache Burst Response Timeout:	3600	
		Save	
	Network Manager Ger	neral Setting	
	NM Tag:	NEXCOM WHart Manager	
	1	Save	L

Figure 62 Parameters Modification for WirelessHART of IWSN Gateway

- d. Scroll down Modify Device page.
- e. Paremwters 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.

	Modify D)evice	(
General	Wlan Wirele	ssHART	
	Device Managem	ent	
	Access Points		
	00-1B-1E-F8-70-0	6-00-01, 00 00 12 34 00 00 00 00 0 🔻	
IWSN Gateway	<eui64>, <key>[,</key></eui64>	<eui64_redundancy>][, <netwo< td=""><td></td></netwo<></eui64_redundancy>	
		Save Delete	
	Gateways		
	00-1B-1E-F9-81-0	0-00-02, 00 00 12 34 00 00 00 00 C 🔻	
	<eui64>, <key></key></eui64>		- 1
		Save	- 1
	Devices		- 1
	Join Key is 🖲 uniqu	e per network O per device Active	
	00 00 12 34 00 00	00 00 00 00 00 00 00 00 00 00	- 1
	Device List		- 1
	Upload device list	Choose file Upload	- 1
	N 1 1 1 1 1		-
		Ormat 1	a hand
		Cancel F	Reboot

Figure 63 Parameters Modification for WirelessHART of IWSN Gateway

- (9) There are labels of "General," "Wlan" and "ISA100" on <u>Modify</u> <u>Device</u> 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	
	*The new setting will take effect	after device restart
	Backbone Router General Settin	g
IWSN Gateway	EUI64:	54
,	BBR Tag:	
	Save	-
	Gateway General Setting	
	EUI64:	
	GW Tag:	
	Save	
	System Manager General Setting	3
	EUI64:	
	SM Tag:	
	Save	
	Device Management	
	P 11	L '
		Canad
		Cancel Reboot

Figure 64 Parameters Modification for ISA100 of IWSN Gateway

- d. Scroll down Modify Device page.
- e. Paremwters 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.

		odify Device	(
General	Wlan	ISA100	
		lanagement	•
	Backbone	S	
IWSN Gateway		Ŧ	
in Sit Gateway	<eui64></eui64>	, <key>, <subnet></subnet></key>	
		Save Delete	
	Gateways		
		Υ.	- 1
	<eui64></eui64>	, <key>, <subnet></subnet></key>	- 1
		Save Delete	- 1
	Devices		- 1
		¥	- 1
	<eui64(-< td=""><td>EUI64)>, <key>, <subnet>[, <role>]</role></subnet></key></td><td>- 1</td></eui64(-<>	EUI64)>, <key>, <subnet>[, <role>]</role></subnet></key>	- 1
		Save Delete	
	Device Lis	st	_
		Cancel	eboot

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.

	Modify D	evice
General	Alert Threshold	
Active		
E-mail to: acco	unt@ ▼	
Temperature		
CPU Temp (Ma	ax: 100): <mark>30</mark> °C	□ SYS Temp (Max: 100): 30 °C
Usage		
HDD Running	Time(Min:100,000):1,000	hr
Storage		
-	n (Min: 100): 0 %	Storage Free Space (Min: 1,000): 0 MB
		OK Cancel
Fig	aure 66 IPC	Device Setting

6.1.2.7 Device Deletion

Click 🔲 icon to delete the chosen device.

	Care	~ -	Manage	Log	Usage	severit		System	Roque AP/Der	ice								
Mana	ige <u>Devi</u>	ce List	Config Backup	Config Restor		grade	Device Provision	Modbus	Profile		-	-		-	-		Ĩ	
	Device Type		Show/Hide	Rogue Device:														
			ÎD	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowser	Reboot	Modify	De	
-	IWF	>	00:0e 8e ti7 5b ad	IWF300-63	10,211,10,63	IWE	IWF300_11N_2G_63	ар	psk2	6	0	0	p	100	0			
			uu ue se or 56 ad		10.211-10.03	10.211.10.03	INVE	IWF300_11A_5G_mesh	mesh	none	36	0	U	4	R	0	-28	
4	11.1.1.1.11		00 10 13 5e 28 57	IWF310-44	10.211.10.44	INF	IWF310_11N_2G_44	ар	psk2	11	0	D	11	f	0		ļ	
1.1	Mobile Mesh	>	00.0010.0010.00	111 515 44	10211.10.44		IWF300_11A_5G_mesh	mesh	none	36	e.		"	14	0			
			00 0e 8e 67 5a 90	IWF300-46	10 211 10 48	INF	IWF300_11N_2G_46	ap	psk2	11	0	0	1	12	C	-		
2	Device Server	>	00 00 00 01 00 00	111 000 40	1021110.40		IWF300_11A_5G_mesh	mesh	none	36	1		4	14	0	-488		
-	CALIFIC SETTO	1	00.0e 8e 67 5t a5	IWF300-64	10,211,10.64	INF	IWF300_11N_2G_64	ар	psk2	11	0	0	4	- CEE	C			
			00.00.00.07.00.40	INF300-04	10,211,10.04	1147	IWF300_11A_5G_64	ap	wpa	48	, and a second s		4	Fi	0	~		
	IWSN Gateway	>	00 0e 8e 67 57 87	IWF300-43	10 211 10 43	INF	IWF300_11N_2G_43	ap	psk2	11	0	0	4	晋	C			
	100000000000000000000000000000000000000	-	• ULUE 80.07 57.87	WF300-43	10.211.10.43	TIVP	IWF300_11A_5G_43	ap	psk2	36	u	0	"	12	0	1		

Figure 67 Device Deletion Icon

6.1.3Introduction for Configuration Backup

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

6.1.4Operation for Configuration Backup

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

Select Device 😨 Model: [IWF300 🔹]	Address:	-
	Houress.	
UWF310	IP Add	dress Model
IWF6330M IWF6330H IWF3310XM IWF3310XH		
Schedule Name:		
	104/E03 104/E040 104/E03004 104/E03004 104/E03004 104/E03004 104/E03004 104/E03004	IWF503 IWF630 IWF6320M IWF6320M IWF6330M IWF6330M IWF3310XM IWF3310XH

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.

Schedule Name	Select Dev	vice 😿 Model: WF300 🔹 🗆 IP Addre	ss: Q	
*	0	Device Name	IP Address	Model
	2	1WF300-43	10.211.10.43	IWF300
	8	IWF300-46	10.211.10.46	IWF300
	8	IWF300-63	10.211.10.63	IWF300
	0	IWF300-64	10.211.10.64	IWF300
		Schedule Name:		

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.

Scher	dule Name	Select De	evice 🖉 Model: [IWF300 💽 🗆 IP Addr	nss: Q		
EST	Result	0	Device Name	IP Address	Model	-
		8	IWF300-43	10.211.10.43	IWF300	
		8	IWF300-46	10.211.10.46	IWF300	
	8	IWF300-63	10.211 10.63	IWF300		
			Schedule Name: [TEST Start Time: [2016/11/14 18:07] Repeat: None •			

Figure 70 Configuration Backup Schedule List

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

nCare	4	Config Ba	ckup Result		0		
Manage Device List <u>Config Ba</u> Schedule Name	Ck IVF300-43 IVF300-46 IVF300-46	IP Address 10.211.10.43 10.211.10.46 10.211.10.63	Success 😧 Success 😧 Success 👻	Time 2016-11-15 17:00:11 2016-11-15 17:00:17 2016-11-15 17:00:23		Model	
1	8 8 8		1			IWF300 IWF300 IWF300	
Event				ок			~

Figure 71 Status of Scheduled Configuration Backup

6.1.5Introduction for Configuration Restore

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

6.1.6Operation for Configuration Restore

Check device *Model* or *IP Address* for the searching condition. Click
 Q icon to search.

nCai		Network Device System	Ladmin 🚯
try ± 0 Device & Netwo	Manage Log Usage	Severity Interval Group Rogue AP/Device	
Manage	Device List Config Backup Config Restore Fw U	Ipgrade Device Provision Modbus Profile	
Choose Config fil	lo: 💼		
Select Device	Model: IWF300 • IP Address: -	a 🔶	
	Device Name	IP Address	Model
	IWF300-43	10.211.10.43	IWF300
1.	IWF300-46	10.211.10.46	IWF300
1 0	IWF300-40 IWF300-63	10,211,10,46	IWF300

Restore	
Event	^

Figure 72 Search for Device to Restore

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

	naper	Config Restore	0	
	<u> </u>	ConfigBackup 20161115-TEST	_	
Manage De	vice List Config Back	- + IWF300_config_10.211.10.63.tar		
Choose Config file:		TWF300_config_10.211.10.46.tar TWF300_config_10.211.10.43.tar		
ielect Device 🗵 Mode	e IWF300 • 0 1			
	Device N			Model
	IMF30			1WF300
0	IMF30			IWF300
0	IWF30			IWF300
0	IWF30			IWF300
rent		OK Car		~

Figure 73 Backup File Selection

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

nCai		System		
hy 20 Device & Netwo Manage Choose Config fil	Manago Log Device List Config Backup <u>Config Bestor</u> le: IWF300_config_10.211.	10.22.22.178 懸示: Are you sure you want to restore? Dh止此病算產生來他到該方機。 確定	× co	
Select Device	Model IWF300 V UP Address	· · · · · · · · · · · · · · · · · · ·	408	
Select Device	Model IWF300 IP Address. Device Name	IP Address	-50.9	Model
Select Device			To B	Model INF300
	Device Name	IP Address	- AG-M	
٠	Device Name INF300-43	IP Address 10.211.10.43		IWF300

	Restore	
Event		^
	Industry 4.0 Device & Network Heattin Manager	

Figure 74 Configuration Restore Confirmation

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

ser ce List Config Back	Config Restore	10.22.22.178 顯示: File name does not match with the model	X 確定
Device N IWF6:			Model IWF6330M
	Figure 75 Error Message for	r Wrong Backup File	

6.1.7Introduction 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

6.1.80peration for Firmware Upgrade

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

Schedule Name	Select Device 🕜 Model: IV/F300 🔹 🖂 IP Addr	ess:	-	
	Device Name	IP Address	Model	FW Version
	Schedule Name:			

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.

anage Device List Co	onfig Backup Cor	ofig Restore Ew Upgrade Device Provision	ion Modbus Profile		
Schedule Name	Select D	evice R Model. MF300 • P Addr	ess. Q		
	•	Device Name	IP Address	Model	FW Versio
-		IWF300-43	10.211 10.43	IWF300	0.1.3.1 EU
	0	IWF300-46	10.211.10.46	IWF300	0.1.3. EU
		IWF300-63	10.211.10.63	INF300	013
		Schedule Name: WF300 Start Time: 2016/11/15.0.00			

Figure 77 Upgrade the Firmware with Schedule

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

Schedule N	ime	Select De	ntig Restore <u>Ew Upgrade</u> Device Provisione evice			
F300-43	Result		Device Name	IP Address	Model	FW Version
4		×	IWF300-43	10.211.10.43	IWF300	0.1.3.11- EU
			Schedule Name: IWF300-43			

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**.

nCare		Topolo			-	(Instantina)				ALCOM
Housey 40 Divisio & Notwork Health Manager		Manage	F	irmware Up	grade Res	ult	0	_		
Manage Device	List Config	Васкир (Со	Device Name IWF300-43	IP Address 10.211.10.43	Status Success	Time 2016-11-15 18:45:38	1			
Schedule Nar	De	Select D	IWF300-43	10.211.10.43	Success	2010-11-15 18:45:38				
MF300	Repuil *					ακ		iodel	FW Version	¥
Event										~
			9	Industry 4.0 Device	& Network Heat	h Manager				

Figure 79 Firmware Upgrade Result

6.1.9Introduction 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). User the **Device Provision** function to batch process the parameter such as *ESSID/Mesh ID*, *Mode, Encryption*, etc.

6.1.10Operation for Device Provision

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

anag	je Device I	list Con	fig Backup Config Resto	re Fw Upgrade	Device Provis	ion Modbu	s Profile
	Device Type		Model Name: IWF300	-			
	IWF Device Server	> ×	General Setting Read Community: Write Community: Trap Configuration: Syslog Configuration.		 		
	IWSN Gateway >	Interface WifiRadio: ESSID / Mesh ID: Mode:	wian0 Access Point	•			
			Operating Frequ	11g	•		
			Channel: Width: TxPower:	US T auto 20 MHz 0 dBm (1mW)	•		

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.

			Devi	ce List			Ø	
a A	JI ID	Device Name	IP Address	SSID	Mode	Encryption	Channel	ł
	00:0e:8e:67:5b:ad	IWF300-	40.244.40.02	IWF300_11N_2G_63	ар	psk2	6	
	00.00.80.07.50.20	63	10.211.10.03	IWF300_11A_5G_mesh	mesh	none	36	
	00:0e:8e:67:5a:90	IWF300-	10 244 40 46	IWF300_11N_2G_46	ар	psk2	11	
	00.00.80.07.58.90	46	10.211.10.40	IWF300_11A_5G_mesh	mesh	none	36	
	00:0e:8e:67:5f:a5	IWF300-	10 211 10 64	IWF300_11N_2G_64	ар	psk2	11	
	00.0e.6e.07.51.a5	64	10.211.10.04	IWF300_11A_5G_64	ар	wpa	48	
	00:0e:8e:67:57:87	IWF300-	10 211 10 42	IWF300_11N_2G_43	ар	psk2	11	
Ĭ	00.00.00.01.01	43	10.211.10.43	IWF300_11A_5G_43	ар	psk2	36	
Ľ				Save Provis	or sion	< Ca	ncel	J

Figure 81 Choose the Device to Provision

6.1.11Introduction 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.

6.1.12Operation for Modbus Profile

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

Modbu	us List	Model:	Veni	dor:	1.	mage Upload	1		
APPC Series		Discovery Parame	iter white space to sepe	rate the regis	ter values when wo	rd count is a	arger than 1 (Except for Unicode & Unico	de1)	
ET7244	٠	Register Val	ue	Functio	n Code	Add	Iress Offset (E.g. 40123 → 122)	Word Count	Attribu
iodbus Sim	4			1: Coils	•				Binary
-M1B403	1	<u> </u>		1: Coils	•				Binary
-M1B301		Register Table Ad	d Register Delete R	Register					
	-circanau	Register Name	Unit		Function Co	ode	Address Offset (E.g. 40123 -> 122)	Word Count	Attribute
ISE105	Strain .	deviceID	C	1	1. Coils	۲	[]		R T Decimal

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)

	alth Manager	Manage Log	Usage Severity Inte	rval Group Rogue AP/Dev	ice		
Manage	Device List Cor	nfig Backup Config Re	store Fw Upgrade Device F	rovision Modbus Profile			
Modbu	s List	Model:	Vendor:	Image Upload			
C Series		Discovery Paramete "Note: Please use w	r hite space to seperate the register value	s when word count is larger than 1 (Exce	ot for Unicode & Unicode1)		
244	۲	Register	Value	Function Code	Address Offset (E.g. 40123 > 122)	Word Count	Attribute
ousSim	4		1: 0				Binary Binary
B403	1		1: C	ils 🔹			Decimal
	1	Register Table Add	Register Delete Register				Unicode Unicode1
8301				Function Code	Address Offset (E.g. 40123 > 122)	Word Count	Attribute

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)

nCare ndustry 40 Device & Network H		Manage Log	Usage Severity Interval	System			
Manage	Device List Confi	g Backup Config Restore	Fw Upgrade Device Provisio	n <u>Modbus Profile</u>			
Modb	us List	Model:	Vendor:	Image Upload			
PPC Series	Â.	Discovery Parameter "Note: Please use white s	pace to seperate the register values when	word count is larger than 1 (Except for	Unicode & Unicode1)		
7244	٠	Register Value	Functio	n Code	Address Offset (E.g. 40123 > 122)	Word Count	Attribute
dbusSim	4		1: Coils	T			Binary
W1B403	ſ		1: Coils	•			Binary
#1B301	-	Register Table Add Regi	ster Delete Register				
M1B301	ſ	Register Name	Unit	Function Code	Address Offset (E.g. 40123 > 122)	Word Count	Attribute
E105	Ster and	deviceID		1: Coils			R T Decimal T
				2: Discrete Inputs 3: Holding Registers 4: Input Registers			

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

	and the second se	-	Manage Log Usa	ge Severity In	terval Grou	up Rogue A	Pibevice	_		
Manage	Device List Co	ntig Be	ckup Config Restore	Fw Upgrade Device	Provision N	Aodbus Profile				
Modbe	zs List		Model: APPC Series	Vendor: NEXCOM		mage Upload				
APPC Series		*	Discovery Parameter "Note: Please use white spa	ce to seperate the registe	r values when we	ord count is large	r than 1 (Except for Un	icode & Unicode1)		
ET7244	۲		Register Value	Function	Code	Address	s Offset (E.g. 40123	122)	Word Count	Attribute
Modbus Sim	4		APPC Series	3: Holding Re	gisters 🔹	99			30	Unicode •
W-M1B403	i i	-	4339	3: Holding Re	gisters •	1			(1	Decimal •
			Register Table Add Register	Delete Register						
W-M1B301	1	0	Register Name	Unit	Func	tion Code	Address Offset (E.	a. 40123 → 122)	Word Count	Attribute
NISE105	Strain P		deviceID		1: Colls	•				RW •
		0	BIOSName		3: Holdin	g Registers 🔹	159		30	Hex •
		8	CPU_Usage		3: Holdin	g Registers •	18		1	R T Hex T
		10	HDDModelName		3: Holdin	g Registers •	299		30	R T

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.

6.2.20peration for Event Log

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

nCare		Topolog	y Si Netwo	rk Device System	C C atom		≜ idmin ≜La
obry 4 0 Device & Network Health Manager	Ma	mage 🤇	Log Usage Sev	erity Interval Group Ro	gue AP/Device		
Log EventLog	System Log	Playback	-				
		Clear					<<1 >
Begin Date: 2016-10-15		22	10 211 10 65	NI050	Normal	Polling Success	2016-11-15 18 31:30
		23	10.211.10.64	IWF300-64	Major	Cold Start	2016-11-15 18:29:58
End Date: 2016-11-15	8 1	24	10.211.10.64	IWF300-64	Major	Cold Start	2016-11-15 18:24:06
		25	10,211.10.49	NI050-49NonDHCP	Normal	Polling Buccess	2016-11-15 18:21:32
IP Address IP Address	0	26	10.211.10.43	IWF300-43	Major	Cold Start	2016-11-15 18:20:58
		27	10.211.10.49	NI050-49NonDHCP	Critical	Polling Failed	2016-11-15 18:17:37
Severity: Critical *		28	10.211.10.1	PingableDevice	Normal	Polling Success	2016-11-15 18:14:18
		29	10.211 10 10	PingableDevice	Normal	Polling Success	2016-11-15 18 14 18
Device Name: 3310	Y 2	30	10.211.10.60	NIO50	Normal	Polling Success	2016-11-15 18:14:18
		31	10.211.10.3	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
Clear	1	32	10.211.10.11	ModbusSim	Normal	Polling Success	2018-11-15 18:14:17
	10	33	10.211.10.65	NIO50	Normal	Polling Success	2016-11-15 18:14:17
Search		34	10.211.10.99	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		35	10 211 10 102	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
	-	36	10.211.10.116	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		37	10.211.10.130	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17

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.

nCare		Topolog	y Netwo	rk Device 💮 🚱 System	lo1 Studio		
ntry 4 0 Device & Network Health Manager	Ma	inage (Log Usage Sev	rerity Interval Group Ro	gue AP/Device		
Log Event Log	System Log	Playback					
		Clear					< < 1 >
Begin Date: 2016-10-15		22	10 211 10:85	NIGSO	Normal	Polling Soccess	2016-11-15 18 31 30
		23	10.211.10.64	IMF300-64	Major	Cold Start	2016-11-15 18:29:58
End Date. 2016-11-15	B v	24	10.211.10.64	IWF300-64	Major	Cold Start	2016-11-15 18:24:06
		25	10,211 10 49	NIO50-49NonDHCP	Normal	Polling Buccess	2016-11-15 18:21:32
IP Address IP Address	0	26	10.211.10.43	IWF300-43	Major	Cold Start	2016-11-15 18:20:58
		27	10.211.10.49	NIO50-49NonDHCP	Critical	Polling Failed	2016-11-15 18:17:37
Severity: Critical *		28	10.211.10.1	PingableDevice	Normal	Polling Success	2016-11-15 18:14:18
		29	10.211 10 10	PingableDevice	Normal	Polling Success	2018-11-15 18 14 18
Device Name: 3310	- ¥	30	10.211.10.60	NIO50	Normal	Polling Success	2016-11-15 18:14:18
		31	10.211.10.3	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
Clear	1 M 1	32	10.211.10.11	ModbusSim	Normal	Polling Success	2018-11-15 18 14:17
	10 C	33	10.211.10.65	NIO50	Normal	Polling Success	2016-11-15 18:14:17
Search		34	10.211.10.99	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
Contraction of the second second		35	10 211 10 102	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		36	10.211.10.116	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		37	10.211.10.130	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17

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.

Log <u>Event Lon</u>	M. System Log	anage 🧲	10.22.22.178		× kevice		
	-	Clear					< < 1 >
Begin Date: 2016-10-15	8	22			Normal	Polling Success	2016-11-15 18:31:30
	2	23		-	Major	Cold Start	2016-11-15 18:20:58
End Date: 2016-11-15	1	24	10.211.10.64	IWF300-64	Major	Cold Start	2016-11-15 18:24:06
	1.	25	10.211.10.49	NI050-49NonDHCP	Normal	Polling Success	2016-11-15 18:21:32
IP Address: IP Address	1 R	26	10.211.10.43	IWF300-43	Major	Cold Start	2016-11-15 18:20:58
		27	10.211.10.49	NIO50-49NonDHCP	Critical	Polling Failed	2016-11-15 18:17:37
Severity: Critical *		28	10.211.10.1	PingableDevice	Normal	Polling Success	2016-11-15 18:14:18
		29	10.211.10.10	PingableDevice	Normal	Polling Success	2018-11-15 18 14 18
Device Name: 3310	1	30	10.211.10.60	NIO50	Normal	Polling Success	2016-11-15 18:14:18
		31	10.211.10.3	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
Clear	*	32	10 211,10 11	ModbusSim	Normal	Polling Success	2016-11-15 18 14 17
		33	10.211.10.65	NIO50	Normal	Polling Success	2016-11-15 18:14:17
Search		34	10.211.10,99	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		35	10.211.10.102	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		36	10.211.10.116	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17
		37	10.211.10.130	PingableDevice	Normal	Polling Success	2016-11-15 18:14:17

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.

	anager						Stern Sector		
			Manage	Log Us	age Severity Ir	nterval Group	Roque AP/Device		
Log	vent Log Syst	tern Log							
		-	Clear						< < 1 2 3 ≥
Begin Date 2016-10-08	(F)	-				Keltutan			2010-11-07 13 03.
Begin Liate: 2010-10-00	Page		312	10 211 10 121	Engable Device		Ponny Panna		
		9	373	10.211.10.115	PingableDevice	Critical	Polling Failed		2016-11-07 19:08:
End Date: 2016-11-08	₩.		374	10.211.10.49	NIO50	Normal	Polling Success		2016-11-07 19:08:
		A.	375	10 211 10 49	NI050	Critical	Polling Failed		2016-11-07 19:06
IP Address: IP Address		×.	376	10.211.10.116	PingableDevice	Critical	Polling Failed		2016-11-07 19:02:
		1	377	10.211.10.116	PingableDevice	Critical	Polling Failed		2016-11-07 18:57
Seventy Critical *		×.	378	10.22.22.178	ncare	Major	Rogue AP Alarm (Found rogue AP III,	8021x)	2016-11-07 18:53.3
			379	10.22.22.178	ncare	Major	Rogue AP Alarm (Found rogue AP III_e	mployee)	2016-11-07 18:53:
Device Name:			380	10.22.22.178	ncare	Major	Rogue AP Alarm (Found rogue AP ili)	guest)	2016-11-07 18:53
Event		-							
itical 🗭 Major									
ID	IP Address			C	Device Name		Event	Tin	ne 🔺
965	10.211.10.116			P	ngableDevice		Polling Failed	2016-11-0	19:13.16
66	10.211.10.121			PI	ngableDevice		Polling Failed	2016-11-07	19:09:22
567	10 211 10 116			P	ngableDevice		Polling Failed	2016-11-0	19.08.03
168	10.22.22.178				Root	Dogue AD Alex	m (Found roque device 10.211.10.105)	2016-11-0	
369	10.22.22.178				Root		m (Found roque device 10.211.10.253)	2016-11-0	

Figure 89 Event Shortcut Table and its Icon

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

Critical 🗹 Major	Replay			
ID	IP Address	Device Name	Event	Time
365	10.211.10.116	PingableDevice	Polling Falled	2016-11-07 19:13:16
366	10.211.10.121	PingableDevice	Polling Failed	2016-11-07 19:09:22
367	10.211.10.116	PingableDevice	Polling Failed	2016-11-07 19:08:03
368	10.22.22.178	Root	Rogue AP Alarm (Found rogue device 10.211 10.105)	2016-11-07 18 53 30
369	10.22.22.178	Root	Rogue AP Alarm (Found rogue device 10.211.10.253)	2016-11-07 18:53:30

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.

ritical 🔲 Major	Replay			
ID	IP Address	Device Name	Event	Time
4	10.211.10.45	NIOSO	Polling Failed	2016-07-26 18:10:28
3	10 211 10 45	NIO50	Polling Failed	2016-07-26 18 08-10
7	10.211.10.45	NIO50	Polling Failed	2016-07-26 18:05:52
0	10.211.10.45	NIO50	Polling Failed	2016-07-26 18:03:34
9	10.211.10.45	NIO50	Polling Failed	2016-07-26 18:01:16

Figure 91 Severity Selection

6.2.3Introduction for System Log

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

6.2.4Operation for System Log

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

nCare	1	Topology		ork Device	System		
		Manage Log	Usage S	everity Interva	l Group Rogu	e AP/Device	
Log EventLog (System Log	Playbock					
							« « 1 :
Begin Date: 2016-10-15	ID ID	IP Address	Device Name	Severity	Facility	Time	Message
10010-010 <u></u>	1	10.211.10.51	IWF6320	Informational	Syslogd	2016-11-15 18 52 31	MARK
End Date: 2016-11-15	2	10.211.10.47	IWF6330	Informational	System Deamons	2016-11-15 18:51:37	hostapd: ath16: STA 00:10:13:36
	3	10.211.10.57	3310	Informational	Syslogd	2016-11-15 18:51:06	MARK
P Address: IP Address	4	10.211 10.47	IMF6330	Informational	Syslogd	2016-11-15 18:43:54	- MARK -
124 ONE	5	10.211.10.50	IWF6320	Informational	Syslogd	2016-11-15 18:42:50	MARK
Seventy: Emergency	6	10.211.10.51	IWF6320	Informational	Syslogd	2016-11-15 18:42:30	MARK
	7	10.211.10.47	IWF6330	Informational	System Deamons	2016-11-15 18:41:37	hostapd: ath16: STA 00:10:f3:36
Device Name: 3310	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 -
Search	10	10.211.10.50	IWF6320	Informational	Syslogd	2016-11-15 18:32:49	MARK
	- 31	10.211.10.51	IWF6320	Informational	Syslogd	2016-11-15 18:32:30	MARK
	12	10.211.10.47	IWF8330	Informational	System Deamons	2016-11-15 18:31:37	hostapd_ath16_STA 00.10.13.36
	13	10.211.10.57	3310	Informational	Syslogd	2016-11-15 18:31:05	- MARK -
	14	10 211 10 64	IWF300-64	Emergency	System Deamons	2016-11-15 18 29:55	Nov 15 17 29 55 logread[5112]

Figure 92 System Log Table

6.2.5Introduction 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.

6.2.6Operation 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 <u>Playback</u> function.

Device Setting

nCare

Industry 4.0 Device & Network Health Manager	lanage Log				
	Log	Usage Severity	Interval	Group F	Rogue AP/Device
Log Event Log System Log	<u>Playback</u>				

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

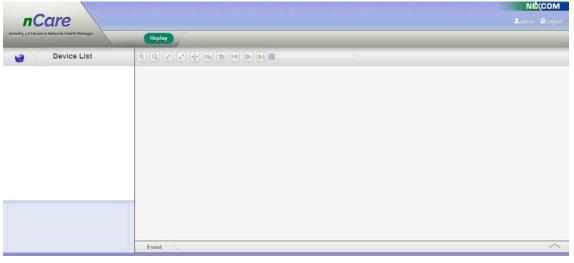


Figure 94 Events Playback

- (7) Click icon and a **Search** window will pop-out.
- (8) Select *Begin Date* and *End Date* then click "OK".

nCare Industry 4 0 Device & Network Health Manager	Replay	
Device List		
	Search (Begin Date [yyyy-MM-dd]: Begin Date [yyyy-MM-dd]:	
	End Date [yyyy-MM-dd]: End Date	

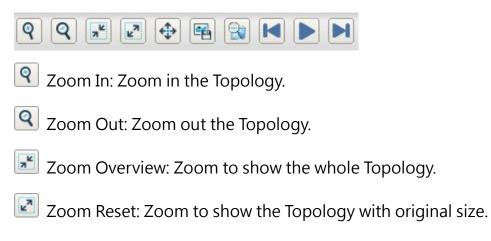
Figure 95 Events Searching

(9) Choose the issue for playback.

Device List		
	2017-05-05 16:24:13	
Root WF300_11A_5G_43		17m
WF300_11A_5G_64		
- IMF300_11N_2G_43		1
WF300_11N_2G_46	Im WF5040_11ng_60-	WF6330-B1 WF6330
. IWF300_11N_2G_63		TC-Switch78
- IWF300_11N_2G_64		
WF310_11N_2G_44	WF504D-69	
~ IWF504D_11ac_69	IMESOAD 11ac 69	CTO Switch82
_ IWF504D_11ng_69	IWF30-64	1m IV F6320
- IWF6330-B1	IWF310_11N_2G_44	
APPC1235-11test		
CTC-Switch75	CTC-SWI	theso CTO-Switch81
CTO CulmbTe	HP WENDLA NI050-61	
A	and the second sec	
		PingableDevice PingableDevice PingableDevice

Figure 96 Issues shown on Topology

(10) Playback icons are list as follows:



- 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 <u>png</u> 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

6.3.1Introduction 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.

6.3.2Operation for Flow Usage

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

y ±0 Device & Network Health	Manager		Manage	Lo	g Usage	Severi	ty Interv	al G	roup F	Rogue AP/Dev					
Usage	_	<u></u>		_								-	-	_	_
IWF	Eth ()	Wian CPU	I i Men	тогу 🧲	-										
Mobile Mesh	Name	IP Address	MAC Address	Descr	Speed	InOctets	OutOctets	InErrors	OutErrors	InUcastPkts	OutUcastPkts	InDiscard	OutDiscard	InNUcastPkts	OutNUcastPk
IPC	IWF300- 63	10.211.10.63	00 10 f3 30 8c 3b	eth0	1000000000	11048024	351749711	0	0	115196	2902086	16	0	Ō	0
	IWF300- 63	10.211.10.63	00 10 f3 30 8c 3b	eth0.2	1000000000	4519974	88463515	0	0	61407	754024	0	0	11328	0
IWSN Gateway	IWF300- 63	10.211.10.63	00 10 f3 30 8c 3b	eth0.3	1000000000	1480072	84981634	0	0	8587	726693	1463	0	4398	0
Device Server	IP Addre	ss: 10.211.10	.64	•	Refresh: 5	▼ sec.	Maxsize: 10	•	Type: Cum	ulative traffic C	hart 🔹				
Switch		6000000.00	-												
	(#1)									-	1				
	danado	36000000.00													
	Catho	24000000.00	-	-	-	•	-	-		_					
	Currat	12000000.00	-	_	-		1	4							

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 <u>Throughput Chart</u> and <u>Cumulative Traffic Chart</u> to choose for Ethernet and WLAN.

try 4.0 Device & Network Heal	th Manager	_	Manage	Lo		sage	Severi	ty Interv	al G	roup i	Rogue AP/Dev	ice				
Usage	_	<u></u>											-	-	_	_
e IWF	Eth I V	Vian CPU	I Merr	iory												
Mobile Mesh	Name	IP Address	MAC Address	Descr	Spee	d	InOctets	OutOctets	InErrors	OutErrors	InUcastPkts	OutUcastPkts	InDiscard	OutDiscard	InNUcastPkts	OutNUcastPk
IPC	IWF300- 63	10 211 10 63	00 10 13 30 8c 3b	eth0	1000000	000	11304468	356410079	0	0	117063	2941439	16	0	0	0
IWSN Gateway	IWF300+ 63	10.211.10.63	00 10 13 30 8c 3b	eth0.2	1000000	000	4568199	89582224	0	0	62071	764029	o	0	11458	D
TW3N Galeway	TWF300+ 63	10,211,10.63	00 10 f3 30 8c 3b	eth0.3	100000	1000	1563095	86146374	0	0	8947	736678	1481	0	4448	0
Device Server	IP Addre	ss: 10.211 10	64	*	Refresh:	5	v sec.	Maxsize: 10	•		ulative traffic 0					
Switch		7000000.00									ulative traffic 0 ughput Chart	Shart	-			
	(9)/4)/	56000000.00	-	-		-	-	•	-	+	-	-				
	ountit	42000000.00														
	atre C	28000000.00	-	-			-		-	-	-	-				
	Currut	14000000.00	-	_			-		-	-		-				

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.

Usage	_		_			_	_	_	_	_	_	_	_	_	_
e IWF	Eth 1 Wie	m CPU	Memory												
Mobile Mesh	Name	IP Address	MAC Address	Descr	Speed	InOctets	OutOctets	InErrors	OutErrors	InUcastPkts	OutUcastPkts	InDiscard	OutDiscard	InNUcastPkts	OutNUcastPk
IPC	IWF300-63	10.211.10.63	00 10 f3 30 8c 3b	eth0	1000000000	11396521	357438368	0	0	117617	2949842	16	U	o	D
IPG.	IWF300-63	10.211.10.63	00 10 f3 30 8c 3b	eth0.2	1000000000	4579590	89821460	0	0	62222	766127	0	0	11495	0
IWSN Gateway	IWF300-63	10.211.10.63	00 10 13 30 8c 3b	eth0.3	1000000000	1582303	86396938	0	0	9040	738800	1485	0	4460	0
Device Server	IP Address	: 10.211.10.42	00.10.13	• Re	fresh: 5	• sec. Max	size: 10	• Type:	Cumulative tra	flic Chart	•				
Switch	24 10 11 12					•]		

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.

0 Device & Network Healt	N	Manage Log Usage	Severity Interv	al Group Rogue A	P/Device					
sage										
WF	Eth Wian CPU	j Memory								
Aobile Mesh	Name	IP Address	lfDescr	IfinOctets	IfOutOctets	Band	Mode	Client	Channel	TxPower
	IWF300-46	10.211.10.46	wian0	0	146045078	2.4G	ap	0	11	0
PC	IWF300-63	10.211.10.63	wlan1	405356500	257280226	5G	mesh	2	36	9
WSN Gateway	IWF300-63	10.211.10.63	wlan0	0	109329291	2.4G	ар	0	8	9
in our may	IWF300-63	10.211.10.63	wlan0-1	0	864	2.4G	ар	0	8	9
Nevice Server	IWF310-44	10.211.10.44	wlan0	38738	146697388	2.4G	ар	0	11	9
witch	IWF310-44	10.211.10.44	wlan1	438509148	755087403	5G	mesh	2	36	9
	IWF300-43	10.211.10.43	wian0	3033077	135102793	2.4G	ар	3	11	9
	IWF300-43	10.211.10.43	wlan1	0	120448894	5G	ар	0	36	9
	IWF503-pro	10.211.10.42	ath1	0	0	5G	ap	0	100	7
	IP Address: 10.211.10	.44 •	Refresh: 5	•]sec. Maxsize:[50	Type: Cumulative t	traffic Chart	•	=		
	80000000.00		Refresh: 5	• jsec. Maxsize: 50	Type: Cumulative t	traffic Chart				
	00.00000008 ministry (10,0000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.000000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.00000008 00.0000008 00.0000008 00.00000008 00.0000008 00.0000008 00.0000008 00.0000008 00.0000008 00.0000008 00.0000008 00.000008 00.0000008 00.000008 00.000008 00.000008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.00008 00.0008 00.0008 00.00008 00.0008 00.0008 00.0008 00.0008 00.0008 00.0008 00.0008 00.0008 00.00008 00.0008 00.0008 00.00008 00.0008 00.0008 00.00008 00.0008 00.0008 00.00008 00.000		Refresh: 5	• jsec. Maxsize: 50	•] Type: Cumulative to	traffic Chart	•			
	80000000 00 (a) 64000000 00 (b) 148000000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 148000000 00 (c) 14800000000 00 (c) 1480000000 00 (c) 1480000000 00 (c) 148000000 00 (c) 148000000 00 (c) 1480000000 00 (c) 1480000000 00 (c) 148000000000000000000000000000000000000	,44 ··)		•)sec. Maxsize:[50	3 · · · · · · · · · · · · · · · · · · ·	raffic Chart	• • • •			
	80000000 00 (a) 64000000 00 (b) 148000000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 14800000 00 (c) 148000000 00 (c) 14800000000 00 (c) 1480000000 00 (c) 1480000000 00 (c) 148000000 00 (c) 148000000 00 (c) 1480000000 00 (c) 1480000000 00 (c) 148000000000000000000000000000000000000			30	3 · · · · · · · · · · · · · · · · · · ·	traffic Chart	•			

Figure 100 WLAN Data Chart

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

y ∉0 Devoce & Network Heal	Manage Log	Jsage Severity Interval Group Rogue AP/Device	
Jsage			
IWF	Eth Wian <u>CPU</u> Memory		
Mobile Mesh	Name	IP Address	CPU Usage(%)
	IWF300-63	10.211.10.63	15
IPC	IWF310-44	10.211.10.44	12
IWSN Gateway	IWF300-46	10.211.10.46	7
	IWF300-43	10.211.10.43	8
Device Server	IP Address: 10.211.10.42 Refresh	: 5 v sec. Maxsize: 10 v	
Switch	70.00 60.00 60.00 50.00 70.00 40.00 20.00 30.00 20.00 0.00		

Figure 101 CPU Data Chart

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

y a 0 Device & Network Hea	with Manage Log	Usage Severity Interval Group F	Rogue AP/Device	
Usage				
IWF	Eth Wan CPU Memory			
Mobile Mesh	Name	IP Address	Memory Usage(%)	Memory Size(k)
monue meen	IWF300-63	10,211,10,63	33	126316
IPC	IWF310-44	10.211.10.44	34	126316
	IWF300-46	10.211.10.46	35	126316
IWSN Gateway	IWF300-43	10.211.10.43	32	126316
Device Server	IWF504D-69	10,211,10,69	64	126364
Device Server	IP Address: 10.211.10.64 * Ref	resh: 5 + sec. Maxsize: 10 +		
Switch	0000 00000 0000 0000 0000 0000 0000 0000 0000 00000			

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.

Usage	-														
IWF	<u>Eth</u> Wlan	CPU M	lemory												
Mobile Mesh	Name	IP Address	MAC Address	Descr	Speed	InOctets	OutOctets	InErrors	OutErrors	InUcastPkts	OutUcastPkts	InDiscard	OutDiscard	InNUcastPkts	OutNUcastP
	NIO20D-IAG	10.211.10.67	00:10:f3:5e:28:43	eth1	1,000,000,000	3,310,287,350	192,229,678	D	0	20,246,534	1,839,177	63,885	0	0	D
IPC	NIO200-IAG	10.211.10.67	00:10:f3:5e:28:43	eth2	10,000,000	0	2,633,346,240	0	0	0	16,233,246	0	0	0	0
IWSN Gateway	NIO200-HAG	10.211.10.72	00:10:f3:5a:42:77	eth1	1,000,000,000	339,871,456	111,778,838	0	0	2,123,452	410,697	5,814	0	0	0
Device Server Switch	IP Address :		v) 1	Refresh : 5	v sec. M	laxsize : 10	• Type : Cum	ulative traffic CP	art ▼						
Device Server		10.211.10.72	•	Refresh : 5	▼]sec. M	laxsize : 10	• Type : Cum	ulative traffic CP	eart •						
			v I	Refresh : 5	• sec. M	laxsize : 10	• Type : Cum	ulative traffic Cł	art v						

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.

Usage															
IWF	Eth Wlar	n CPU Me	emory												
Mobile Mesh	Name	IP Address	MAC Address	Descr	Speed	InOctets	OutOctets	InErrors	OutErrors	InUcastPkts	OutUcastPkts	InDiscard	OutDiscard	InNUcastPkts	OutNUcastP
	NIO51	10.211.10.74	00:10:f3:5a:42:45	eth0	10,000,000	3,070,349,079	225,178,112	0	0	20,405,158	1,158,105	63,894	0	0	0
IPC															
WSN Gateway															
Device Server															
Switch															
Switch															
Switch															
Switch	IP Address	: 10.211.10.74	T	Refresh : 5	v sec. 1	Maxsize: 10	▼ Type: Cun	nulative traffic Cl	hart 🔻						
Switch		: 10.211.10.74	•	Refresh : 5	v sec. 1	Maxsize: 10	• Type : Cun	nulative traffic Cl	hart 🔻						
Switch			*	Refresh : 5	vjsec. I	Maxsize: 10	▼ Type: Cun	nulative traffic Cl	hart •						
Switch			•	Refresh : 5	v sec. I	Maxsize: 10	Type: Cun	ulative traffic Cl	hart •						
Switch			•	Refresh : 5	v sec. 1	Maxsize: 10	• Type : Cun	ulative traffic Cl	hart •						
Switch	e Count(byte)	400000000.00	•	Refresh : 5	Y sec. 1	Maxsize : 10	• Type : Cun	ulative traffic Cl	hart •						
Switch	e Count(byte)	400000000.00	•	Refresh : 5	۲)sec. ا	Maxsize : 10	▼ Type: Cun	nulative traffic Cl	hart •						
Switch		400000000.00	•	Refresh : 5	▼]sec. 1	Maxsize : 10	• Type: Cun	nulative traffic Cl	hart						

Figure 104 NIO51 Device Data Flow Line Chart

6.4 Severity

6.4.1Introduction for Severity

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

6.4.20peration for Severity

 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.

Care Topology	tk Device System		N
ide & Nerhook liesch Monoper Manage Log Usage	sevenity Intervat Group Rogue APiDevice		
Event	Severity	Color	Modify
Polling Failed	Critical		.9
Link Down	Major		.9
Warm Start	Major		
Cold Start	Major		.0
Authentication Failed	Major		.9
Polling Success	Normal	-	a
Link Up	Normal	-	.a
IPC Temp Alarm	Major		-9
IPC Storage Alarm	Major		a
Network Unstable	Major		.a
Rogue AP/Device Alarm	Major		-9
Ring Failure	Major		.a
Ring LinkUp	Normal		.9

Figure 105 Severity Table

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

Care Topology	System		
Nanage Log	Usage Severity Interval Group Rogue AP/Device		
erity			
Event	Seventy	Color	Modify
Polling Failed	Critical	-	2
Link Down	Major		
Warm Start	Maior.		
Cold Start	Modify Severity 📀		.a
Authentication Failed			.0
Polling Success	Trap. Polling Failed		.a
Link Up	Seventy: Critical	-	.a
IPG Temp Atarm			-9
IPC Storage Alarm	OK Cancel		a
Network Unstable			.0
Rogue AP/Device Alarm	(a)or :		-9
Ring Failure	anjor		a
Ring LinkUp	Normai		.0

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

Figure 106 Severity Modification

6.5 Interval

Event

6.5.1Introduction 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.

6.5.20peration 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' II be easier for managing the devices by the group with similar characteristics. The manage authority for a group can also be set.

6.6.2Operation 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.

Map Image	Latitude		Longitude
<u>floor.jpg</u>	Add Topolog	y Group	0
	Name: Map Image: Latitude: Longitude:	* (-85 ~ 85) (-180 ~ 180)	
		ок са	ancel

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

Care	Manage Log Us	age Severity Interval Grou	Rogue AP/Device		
roup Topology G					_
Name	Map Image	Latitude	Longitude	Modify	Delete
Root	floor.ipg	0	0	.0	
test1		0	0	.0	Û
tost2		0	0	.a	8
test3		0	0	.9	÷.

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.

6.7.20peration for Rogue AP/Device

- 6.7.2.1 Detection
- (1) Click Scan to detect for Rogue AP/Device.

				NECOM
nCare	Topology	Network Device	System	
Industry 4.0 Device & Network Health Manager	Manage Log	Ukage Severity Inter		
Rogue AP/Device				
Add to White List IP Address	MAC Address	Nerre Scanning plea		Wired Connection Device
		Şcan	-	

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*.

ustry 4.0 Device	& Network Health Manager	Manage	Log Usage S	Severity Interval	Group Rogue AP/Device	
Rogue	AP/Device	Detection White L	ist Deny List Scan Si	etting		
Add to hite List	IP Address	MAC Address	Name	Model	Wireless Connection Device	Wired Connection Device
•	10.211.10.79	de:aa.b9.d6.29.2a	PingableDevice	Pingable device		
+	10.211.10.78	00:10:f3:5a:42:01	PingableDevice	Pingable device	200	
+	10.211.10.77	00.10.13.4a.fc.8c	IWF503-77	IWF503		
+	10.211.10.76	00:03:7f:50:00:55	IWF503-76	IWF503		
+	10.211.10.74	00:10:f3:5a:42:45	NIO61	NIO51		-
	10.211.10.72	00.10.13.5a.42.77	NI0280-HAG-72	NIO200-HAG		
+	10.211.10.70	00:10:13:62:38:5b	NI0200-IAG-70	NIO200-IAG	2.47	
+	10.211.10.67	00 10 f3 5c 28 43	NIO200-IAG-67-DDL	NIO200-IAG		
+	10.211.10.63	00:0e:8e:67:5b:ad	IWF300-63	IWF300	(1)	12
+	10.211.10.58	cc:46:d6:e6:d5:d4	Unknown	Unknown device	2.53	*
	10.211.10.57	00.10.13.36.16.51	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)

nC	are	торо	logy 💽 Net	work Device	System	Mice Liedman Alice
dustry a 0 Device	& Network Health Manager	Manage	Log Usage	Severity Interval		
Rogue	AP/Device	Detection White Lis	t Deny List Scan S	ietting		
Add to hite List	IP Address	MAC Address	Name	Model	Wireless Connection Device	Wired Connection Device
	10.211.10.79	de.aa.b9.d6.29.2a	PingableDevice	Pingable device		
+	10.211.10.78	00:10:13:5a:42:01	PingableDevice	Pingable device		t:
+	10.211.10.77	00:10:13:4a.fc.8c	IWF503-77	IWF503		
+	10.211.10.76	00:03:7f:50:00:55	IWF503-76	IWF503	•	-
+	10.211 10.74	00:10:13:5a:42:45	NIO51	NIO51		
				Scan A	IIA bb	
Event						
	ajor Replay					_
ID	IP Ad	dress	Device Nam	e	Event	Time
1	10.211	.10.77	IWF503-77		Polling Failed	2018-08-01 19:22:04
2	10.211	1.10.6	nCare		Rogue AP/Device Alarm (Found rogue device 10.211.10	2018-08-01 19 19 12
3	10.211	1.10.6	nCare		Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12
4	10.211	1.10.6	nCare		Rogue AP/Device Alarm (Found rogue device 10.211.10.	2018-08-01 19:19:12
5	10.211	1.10.6	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)

			Manage			verity			logue AP/Devi	SU	-		-		-	-					
Mana	Device Type	e List	Config Backup Co		I w Opgrad	e De	vice Provision	Modbus Pi	ofile												
			D	Device Name	IP Address	Device Type	SSID	Mode	Encryption	Channel	Latitude	Longitude	Web	Mibbrowse	r Rebool	Modify	Deli				
5	IWF	>					IWF300_11N_2G	ap	psk2	11					0			먐	~		
			00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWF	IWF300_11A_5G	mesh	none	36	0	0	11	1	0	-2	ũ				
4			A	100044	10.211.10.44	IWE	IWF300_11N_2G	ap	psk2	11	o	0	"	1 ²⁰⁰	O						
1 1	Mobile Mesh	>	00 10 f3 5e 28 57	111-000-44	10.211.10.44	INF	IWF300_5G_mesh	mesh	psk2	36		°.	"	12	0		.2 (
			•	IWF300-46-12	10.211.10.46	IWE	IWF300_11N_2G	ар	psk2	11	D	0	4	響	c.		1				
2	Device Server	>	00:10:13:30:86:85	HVP-300-40-12	10.211.10.40	INF	IWF300_11A_5G	mesh	none	36			4	F	C	1	1				
_		1		IWF300-43	10.211.10.43	IWE	IWF300_11N_2G	ар	psk2	11	0	0	11	먐	0		ī				
			00:10:13:30:86:71	110 000 10	19.2.11.10.10		IWF300_11A_5G	mesh	none	36			~	14	0	-100	1				
	IWSN Gateway	>	00 03 71 50 00 55	IWF503-76	10.211.10.76	IWF		10		3	0	0	11	评	C	a	1				
			00.03 7050 00.55		10.011.10.0		IWF503 11ac 70	ap	osk	100			4	14	~						

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)

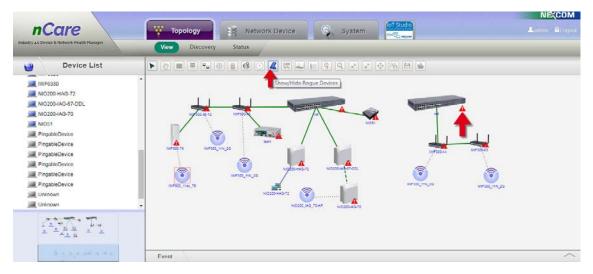


Figure 114 Rogue AP/Device on Topology

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

	& Network Health Manager	Manage	Log Usage S	Severity Interval	Group Rogue AP/Device						
Rogue AP/Device Detection White List Deny List Scen Setting											
Add to White List	IP Address	MAC Address	Name	Model	Wireless Connection Device	Wired Connection Device					
+	10.211.10.79	de aa b9 d6 29 2a	PingableDevice	Pingable device	(F						
+	10.211.10.78	00:10:13:58:42:01	PingableDevice	Pingable device	5 7	(*)					
+	10.211.10.77	00:10:13:4a.fc 8c	IWF503-77	IWF503							
1_	10.211.10.76	00:03:77:50:00:55	IWF503-76	IWF503		. * .					
	10 211 10 74	00,10 f3 5a 42 45	NIO51	NIO51							
	10.211.10.72	00:10:13:58:42:77	NIO200-HAG-72	NIO280-HAG							
+	10.211.10.70	00:10:13:62:38:56	NIO200-IAG-70	NIO200-IAG							
+	10.211.10.67	00:10:13:5e:28:43	NIO200-IAG-67-DDL	NIO200-IAG	<i>a</i>						
+	10.211.10.63	00:0e:8e:67:5b:ad	IWF300-63	IWF300		(4) (4)					
	10 211 10 58	cc 46 d6 e6 d5 d4	Unknown	Unknown device							
+	10.211.10.57	00:10:13:36:16:51	3310	IWF3310XH	3						

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 <u>.csv file</u>.

-				NE(C
nCare	🦉 Topology 💦 💽 Network Dev	Ice System	4	Ladmin 🔒
40 Device & Network Health Manager	Manage Log Usage Severity	Interval Group Rogue AP/Device		
togue AP/Device Detection	White List Deny List Scan Setting			
IP Address	MAC Address	Description	Modify	Dele
10.211.10.76	00:03:71:50:00:55	IWF503-76		
	Add	mport (.csv) Export (.csv)		

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.

			NE(COM
nCare Industry 40 Device & Network Health Manager	Manage Lo	System System	Autor Aleged
Rogue AP/Device Deter		Senviria and a setting	
IP Address	1 1 6		Modify Delete
10.211.10.76	•	Add WhiteList	.a û
		IP Address: MAC Address: Description:	
		Add Import (.csv) Export (.csv)	

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.

nCare Topology	System	Int Studio		Ladmin & Logout
Manage Log	Usage Severity Interval Group Rogue	AP/Device		
Rogue AP/Device Detection White List Deny Li	ist Scan Setting			
NO. Connected Client MAC	AP	Port Number Rule	Delete	Result
	Add from rogue devi Scanning pleas 33%	e wait 0		
		OK Cancel		
	Apply Add New A	udd from Rogue Device		

Figure 118 Scanning for White List Devices

Event

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

ogue AP/I	Device Detection White List	Deny List	Scan Setting					
).	Connected Client MAC		AP		Port Number	Rul	e Delete	Result
			Add fro	m rogue device	list	0		
			Connected Client MAC	AP	Port Number	Rule		
			78:48:59:d1:e5:7d	10.211.10.76	1	Deny		
		×	78:48:59:d1:e5:7d	10.211.10.74	1	Deny		
			78:48:59:d1:e5:7d	10.211.10.72	1	Deny		
			78:48:59:d1:e5:7d	10.211.10.70	4	Deny		
		۲	78:48:59:d1:e5:7d	10.211.10.67	1	Deny		
			20:4c:03:03:c7:50	10.211.10.76	1	Deny		
		0	20:4c:03:03:c7:50	10.211.10.74	1	Deny		
		0	20:4c:03:03:c7:50	10.211.10.72	1	Deny		
			20:4c:03:03:c7:50 20:4c:03:03:c7:50	10.211.10.70	4	Deny		
			20.4c.03.03.c7:50	10.211.10.67	1	Deny *		
						OK Cancel		
						Califier		

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

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

10.	Connected Client MAC	AP	Port Number	Rule	Delete	Result
1	78:48:59:d1:e5:7d	10.211.10.67	1	Deny	Û	?
2	20:4c:03:03:c7:50	10.211.10.67	1	Deny	Û	?
3	78:48:59:d1:e5:7d	10.211.10.70	4	Deny	ti -	?
4	20:4c:03:03:c7:50	10.211.10.70	4	Deny	Û	?
9	78:48:59:d1:e5:7d	10.211.10.72	1	Deny	Û	?
3	78:48:59:d1:e5.7d	10.211.10.74	1	Deny	Û	?
7	78.48.59.d1 e5.7d	10.211.10.76	1	Deny	Û	?

Figure 120 Rogue Device Setting on White List

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

Rogue Al	P/Device Induction While	Lind Deny List Senie Setting				
10.	Connected Client MAC	AP	Port Number	Rule	Delete	Result
	70:40:59:01:e5:70	Setting plea	se wait		0	?
		10.211.10.67		Deny	8	?
	78.48.80 d1 e5.7d	10.211.10.70	2 ÷		0	?
	20.4c:03:03:c7:50		4	Deny	8	?
	78:49:59:d1:45:7d			Dany		?
	70.40.59.d1 s5.7d	10.211.10.74			8	?
	78.48.59.d1.e5.7d			Deny	0	?

Figure 121 Rogue Device Loading

(9) A mark "✓" on the <u>Result</u> column indicates that the setting is done. A mark "×" on the <u>Result</u> 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.

	Manage	Log Usage Severity Int	terval Group Rogue /	P/Device		_
Rogue A	P/Device Detection White Lis	st Deny List Scan Setting				
NO.	Connected Client MAC	AP	Port Number	Rule	Delete	Result
1	78:48:59:d1:e5:7d	10.211.10.67	1	Deny	Û	×
2	20.4c.03.03.c7.50	10.211 10.67	ť	Deny	Û	1
3	78:48:59:d1:e5:7d	10.211.10.70	4	Deny	Û	1
4	20:4c:03:03:c7:50	10.211.10.70	4	Deny	Û	1
5	78:48:59:d1:e5:7d	10.211.10.72	1	Deny	Û	1
6	78:48:59:d1:e5:7d	10.211.10.74	-12	Deny	Û	
7	78.48.59.d1.e5.7d	10.211.10.76	1	Deny	Û	×

	Apply	Add New	Add from Rogue Device
Event			^

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.

NO.	Connected Client MAC	-(1		Rule	Delete	Result
1	78:48:59:d1:e5:7d	Add New	0	Deny	0	~
2	20 4c 03 03 c7 50			Deny	ů.	1
3	78:48:59:d1:e5:7d	Connected Client MAC:	•	Deny	Û	1
4	20-4c 03-03 c7.50	AP:		Deny	0	1
5	78:48:59:d1:e5:7d	Rule: Deny		Deny	8	1
6	78:48:59:d1:e5:7d			Deny	Û	~
7	78 48 59 d1 e5 7d			Deny	Û	×
		Apply Add New Add from	n Rogue Device	J		

Figure 123 Rogue Device Added Manually

6.7.2.4 Scan Setting

Rogue devices can be automatically detected by nCare. Enter the <u>Rogue</u> <u>Detection Interval</u> 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

7.1.1Introduction 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.

7.1.20peration for Topology View

7.1.2.1 Topology Drawing

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

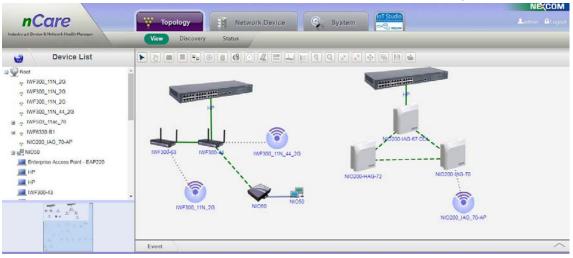


Figure 125 nCare Topology(

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

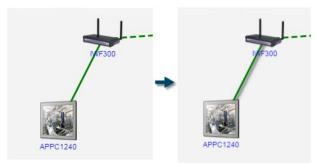


Figure 128 Connection Selection

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

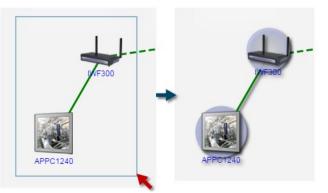


Figure 129 Multiple Devices Selection

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.

Device Type:	IWF	٣	
Protocol:	SNMP	Ŧ	
Trap Configuration:			
Syslog Configuration:			
Device Name:		*	
IP Address:		*	
Read Community:	public	*	
Write Community:	private	*	
Topology Group:	Root	•	
Latitude:			
Longitude:			

Figure 131 Add New Device

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

nCare

nCare	Topology Network Device System	NECOM
Industry 4.0 Device & Network Fealth Manager	Vew Discovery Status	
Device List TWF004D_11ng_09 TwF0330-B1 NF6330-B1 S120-24G_SI		
	Scanning please wait	
MF300-46 MF310-44 MF504D-53 MF504D-69 MF5020	MM200 2/9 pryster.	
NIC50 NIC50 NIC60-49NonDHCP		
	Entrypas access.	

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.

Device List		
- TMPOUAD_11ng_09 - TMPOUAD_11ng_09 5120-24G_SI 5120-24G_SI 240PC1235-11test ET7244	Scanning please wait.	
ET7244 Enterprise Access Point - EAP220 WF300-46 WF310-44		
 INF504D-53 INF504D-69 INF6320 	STIDS:/40_ST	
NIC50 NIC50-49NonDHCP		

Figure 133 New Device Not Found Window

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

nCare

nCare	Topology Network Device System	NÈCOM Loamin Al ogoit
Industry 20 Device & Network Health Manager	Ver Discovery Status	
Uevice List	▶ ? ■ = % 0 = @ 0 4 ₩ ↓ H ? ? ¥ 2 4 % H ★	
 TA-SUC_TA_SC_43 TMF300_TIN_2C_43 TMF300_G20_provision TMF310_TIN_2C_44 TMF504-53 TMF504-53 TMF504D_TI3c_53 TMF504D_TI3c_69 		
 IWF630-B1 IWF6330-B1 5120-24G_S1 5120-24G_S1 5120-24G_S1 APPC1235-11test 	MPSX40_1110_01 MMPSX40_111ac_88 MPSX40_510_210_510_210_510000 5120_240_51	
ET7244 ET7244 Enterprise Access Point - EAP220 INF300-43	NPC1235-11148 N0500_114_50_43 N0500_114_50_43 NARME: (N7200-43) IP: 10.2111.04.35 MAC: 60.1015.03.88.a9	
	test test MP300_t1N_20_43 M050.61	Convenient

Figure 134 Add Device Successfully

- Add to Topology Group: Classify the device with the same group.
- (1) Select two or more devices by \blacktriangleright , then click \blacksquare .

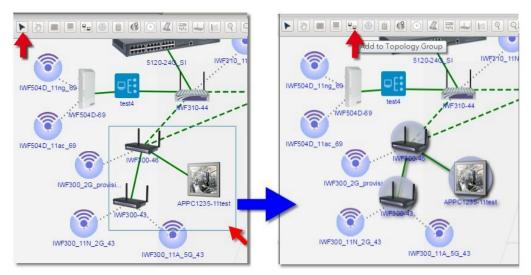


Figure 135 Group Selection

(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)

	*** **** ****	()		
		10_11N_2G_44		
	- <u> </u>		-	
	dd to Topology Group		8	
D-69				
0.00	Topology Group:	test5	Y	In succession of the
		Root test1		-
C		test2		
VF300_26		test3 test4	ancel	
		test5		

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 <u>Root</u> as group, then the device can be removed from the group.

ME	WFsper46		
Ad	ld to Topology Group		0
	Topology Group:	Root	-
P	Topology Group:	Root Root test1	
ŧ	Topology Group:	Root test1 test2	
P	Topology Group:	Root test1	ancel

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 \blacktriangleright , then click 1.

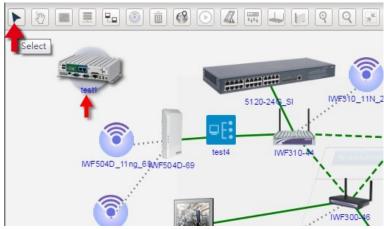


Figure 139 WiFi Group Icon

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

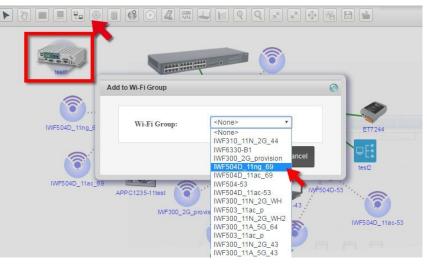


Figure 140 WiFi Group Selection

(3) If the devices need to be removed from the group, please select the device then click¹. Choose None as group, then the device can be removed from the group.

	Add to Wi-Fi Group	0
	Wi-Fi Group: <a>None>	-
Test	ок	Cancel

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 \blacktriangleright to select device or connection then click $\boxed{10}$. 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

O 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 (1) 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.

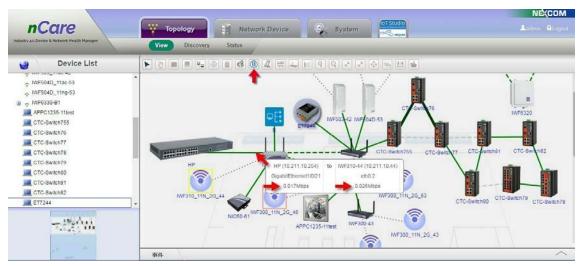


Figure 145 Flow Rate Monitoring

(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.

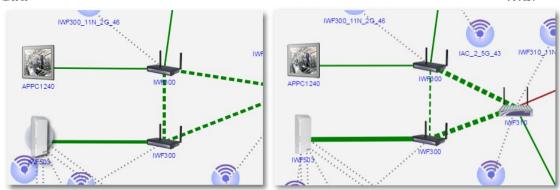


Figure 146 High Traffic Connection

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

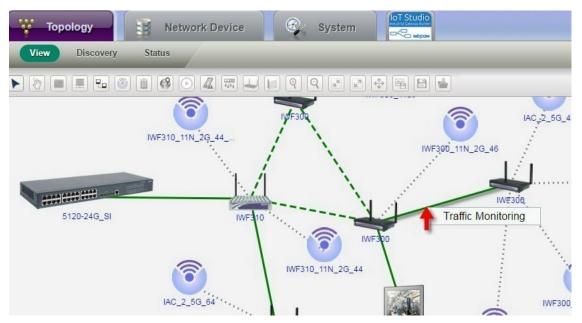


Figure 147 Traffic Monitoring

- (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.

- (8) Enter Interval, Threshold and E-mail for the receiver.
- (9) Click **OK** to complete setting.

		•
IWF504D_11ng_69	Traffic Monitoring Image: Constraint of the sector of	
IWF504D_11ac_69	OK Cancel	

Figure 148 Traffic Monitoring Window

(10) Back to Topology View. A little icon on the link indicates that the traffic monitoring has started.

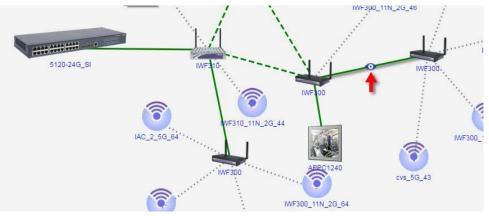
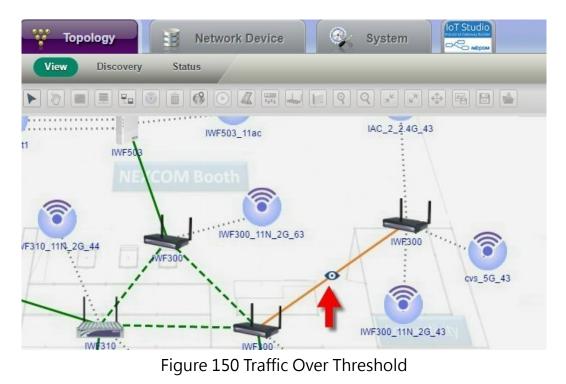


Figure 149 Traffic Monitoring Started

(11) The link will became ORANGE if the traffic is over the threshold. An E-mail will be sent to Administrator.



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

	Traffic Monitoring	IWF30
•••••• •	10.211.10.46(eth0.3) - 10.211.10.43(eth0.3) Active Interval 5 Sec (5 ~ 900) Threshold 1 Mbps (1 ~ 1024) E-mail to account@ *	
	OK Cancel	APPC1240

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.

nCare

nCcire Industry 40 Device & Network Health Manager	Topology Network Device System
Device List	View Discovery Status
u ∰test3	Traffic Monitoring
ge Witest4 NVF300_11A_5G_43 WVF300_21C_provision WVF300_2C_provision WVF300_2G_provision WVF300_2G_provision WVF500_2G_provision WVF500_D111x_2G_44 WVF504D_111a_53 WVF504D_111a_69 WVF504D_111a_69 WVF504D_111a_69 Stre530-B1 St20-24G_SI	
5120-24G_SI	NEXCOM Boot

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.

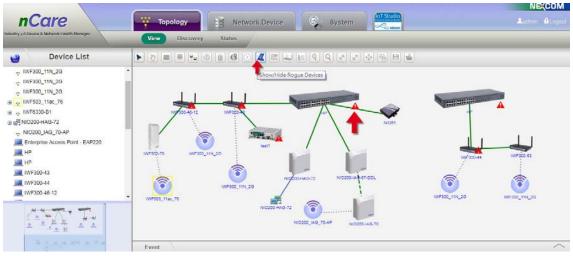


Figure 153 Show/Hide Rogue Devices Icon

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

nCare

PingabieDevice PingabieDevice	PringableDevice Pringa		Internal Length		
PingabinDavice PingabinDavice	PringabileDevice PringabileDevice		6 B 💼	N 7	🥹 Device List 🕨
PingabieDevice PingabieDevice	PingableDevice PingableDevice	5m			A 110
PingabieDevice VVAN 19 PingabieDevice PingabieDevice PingabieDevic	PingabieDevice VLAN 11 66- WF300_13N_20_64 WF300_11A_50_64 CTC-Switch78 CTC-Switch7				
PingabieDevice Pingab	PingabieDevice IMF300_T1N_2G_64 IMF300_T1N_2G_64 IMF300_T1A_5G_64 IMF3030-B1 IMF8330-B1 PingabieDevice IMF504D_11a_68 IMF504D_012 IMF504D_01	7	li (*)	VLAN 1	VL VL
PingableDevice PingableDevice	PingableDevice PingableDevice PingableDevice WF504D_69 WF504D_69 WF504D_69 WF504D_69 WF504D_6	-	IME6330-B1		PingabieDevice VL
PingableDevice PingableDevice PingableDevice PingableDevice PingableDevice PingableDevice PingableDevice PingableDevice PingableDevice	PingableDevice PingableDevice WF504D_011ac_69 WF504D_01000 WF504D_0100 WF504D_0100 WF504D_010	WF63	- 3m IWF633	Mrsvie_mmg_69* [WF300_13N_2G_64 [WE300_11A_50	
PingableDevice Pingable	ProgableDevice INF504D_59 CTC-Switch2 ProgableDevice INF504D_11ac_59 INF5040-64 CTC-Switch2	1 /			
PingableDevice Pingable	PingabieDevice INF504D_11ac_69 INF50454 CTC-SwithTr9 CUSSWitchs2		B		
Inspace Device Device Inspace Devic	Parabelerice WH5040_TTac_59 WH5040_TTac_59		CTQ-Switch82	IWF504D-69	
Pingable Device	PingableDevice		- 21m		
PinshiPavira	WP310_11N_20_44	IWF6320		IWE310_11N_2G_44	
CTC-Swith80 CTC-Swith81	PingabieDevice		the second secon		PingableDevice
- information	PingableDevice CTC-Switch80 CTC/Switch81		0 CTO-Switch81		PingableDevice
PingabieDevice + HP MISS 0-21 NI050-51 17m			- 17m		

Figure 154 VLAN Selection

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

Device List			9 - 2 - 5	-	
PingableDevice	* [VLAN 1 •]				10-
PingableDevice			and an a	(
PingableDevice	()	()			
PingableDevice	INF504D_11ng_69-	WF300_13N_2G_64 WE300_11A_50		IWF6330-B1	ash MFG
PingableDevice		In the second includes	CTC-Switch76		1554
PingableDevice	and the second				No. 1
PingableDevice	INF50			<u>p</u>	
PingableDevice	IWF504D_11ac_69		CTC-Switch79	CTC Switch82	=
PingableDevice		TWF310-64		21m	IWF6320
PingableDevice		WWWW0_THV_20_44			
PingableDevice				£	
PingableDevice			CTC-SWITCH80 CTC	Switch81	
PingableDevice	· HP	NIO50-61	- 17		

Figure 155 VLAN Topology

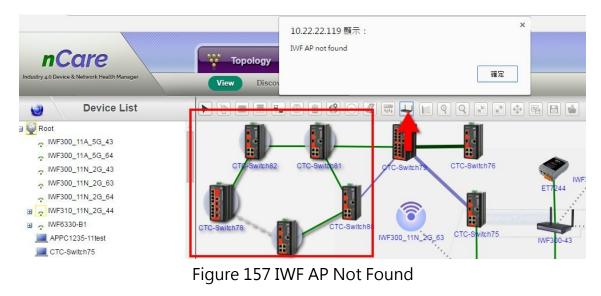
- Update AP: IWF AP can be updated by this function.
- (1) Click 🖳
- (2) If there is no AP selected, and an "Are you sure you want to update ALL IWF APs" window will pop-out. Click **OK** to proceed update.

nCare

-Corro	10.22.22.119 顯示:	×		TStudio	NECOM
neure		Device	System	So anticipa	🚣admin 🔒Logour
Industry 4 0 Device & Network Health N	Are you sure you want to update All IWF APs? Warning: Update All IWF APs may take a few minu			and the second	
	training, opcare with the Ars may take a lew mino	cr's			
Device		2 ka 🛛 🖏 📕	99**	1 B (*)	
- OTO OWIGHTER			Update AP		7m 11
Enterprise Access Point - E			0		
HP		<u></u>		ii 🔞	
HP			U	WE6330-B1	
IWF300-43	IWF5040_11ng_66-	IWF300_11N_2G_64 IWE	300_11A_6G_84	-Switch78	INF6330 MF6320
1WF300-46			Cit	-Switch78	
MF300-63	and the second s			10 A	61
IWF300-64		/F504D-69	СТС-5win 79	CTO Switch82	
IWF310-44	IWF504D_11ac_69	IWF300-54	•	1	
IWF504D-69		141122 2.20	11N_2G_44	21m	IWF6320
JMF6320				14	
T INF6320			<u> </u>	B	
T INF6330		amitin S	CTC-Switten	80 CTO Switch81	
III NIO50-61	HP	WESTO AN N	050-61	17m	
2.00.4987	in the second				and a second second
Tit. Maria		1 1 1	1		A CONTRACTOR OF A CONTRACTOR O
a strate		2 _		C-Switch77	PingableDevice PingableDevice
					Trees Income
11111	Enternaise Annaes NIO5 Event	1/3. 1 20.	2300,Ks	100000	
111111	Lven				
		Industry 4.0 Device & Ne	twork Health Manager		

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.



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

nCare

Device List	N 0 0 0 0	10111 10 014				
OTO OWNERDE	•					
Enterprise Access Point - EAP220		-	0	1000		
HP			Scanning	please wait		
WF300-43	WF504D 1100 69-				(MF6330-81	
IWF300-46	TWI-SO4D_TIND_OB/2	IWF300_13N_20_64	ME300 114 56 64	C GartenTD	EQ.	RE33D NVFI
WF300-63	0			10/2		Ser. 1
WF300-64	Contraction of the second					
WF310-64		NF504D-69	CITE-S	ewanter 70 G	TC Switch82	
	WE5040_11ac_69	THE PARTY OF	101101000		(
WF504D-69		145	310_11N_20_44			
IWF6320	and the second sec					
			0	CTO-SWITCHES CTO-SWITC		
WF6330 NIO50-61		Constant of		A CARE		
NICSU-61	- HP	- Consequences		170		
444 文学	am					
44.000		1				

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.

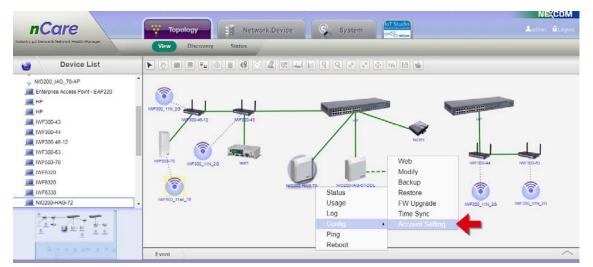


Figure 159 Account Setting for NIO200-HAG Series Devices

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

Device List	• 2 II I I I I			⊕ 16 18 18		
NIC200_IA0_70-AP Enterprise Access Point - EAP220 HP HP IVF300-43 WVF300-44	00000_110_20 100000_110_20 10000046-12	Account Setting			-	
INF300-46-12 INF300-63 INF603-76 INF6320 INF6320	WF005-70 WF300_11A	Password:	OK Cancel	NOS1		
INF6330 NIO200-HAG-72	WFSDLTIAL 28			NIO20014-0-70		0_11N_20

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.

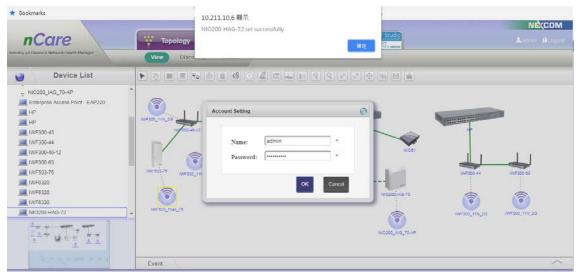


Figure 161 NIO200-HAG Account Setting Success

(8) Click 📃 icon for updating IWSN.

Topology

Device List		04849		6 8 4		
NIC200_IAG_70-AP			te IWSN			
Enterprise Access Point - EAP220						
HP		1 .	and the second sec			
HP	WF300_11N_20					
WF300-43	11/ 200-46-12 JM/F200	43	-/+		+	
WF300-44			/			
WF300-46-12				NI051		1.1
WF300-63	🛛 🚺 🛜 🚎					
WF503-76	INF503-78 INF300_11N_20 1est1		No.	Long Long	IWF300-44	IWF300-63
WF6320	A A A A A A A A A A A A A A A A A A A					
IWF6320	8	NI0200 HV/G-72	NI0200-IAG-67-DDL	NI0200 UAG-70	-	-
WF6330					(()
NIO200-HAG-72	TWF503_11ac_78			1	IWE200_11N_2G	INF300_11N_20
1				•		
				10200_14/3_70-AP		

Figure 162 IWSN Update

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

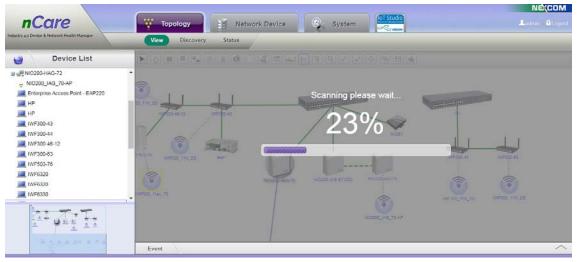


Figure 163 Scanning for NIO200-HAG Devices

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

nCare

Device List	4
NO200-HAG-72 NO200_HAG-70-AP Finiteprise Access Point - EAP220 HP HP HP WF300-43 WF300-43 WF500-63 WF500-63 WF500-63 WF500-63 WF500-63 WF500-63 WF500-63 WF500-63 WF500-64 WF500-6	WF300_11N_20 WF300_11N_20

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.

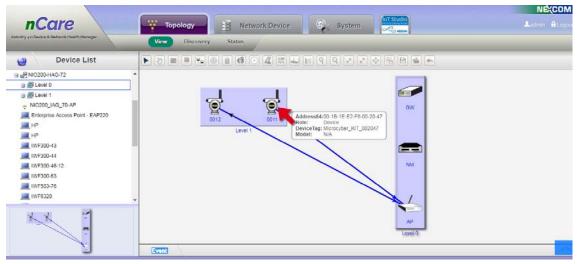


Figure 165 Check for NIO200-HAG Group Devices

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

nCare

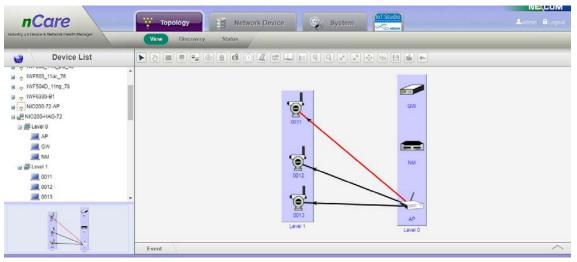


Figure 166 NIO200-HAG Group Devices Disconnected

(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.

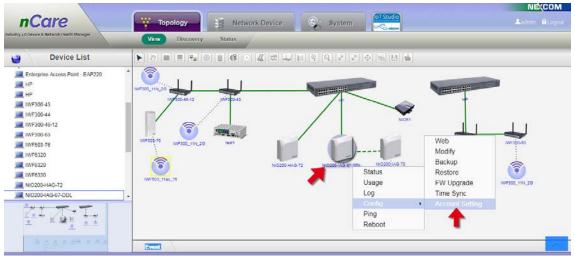


Figure 167 Account Setting Window for NIO200-IAG

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

nCare

😸 Device List	
	WF302_INL30

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.

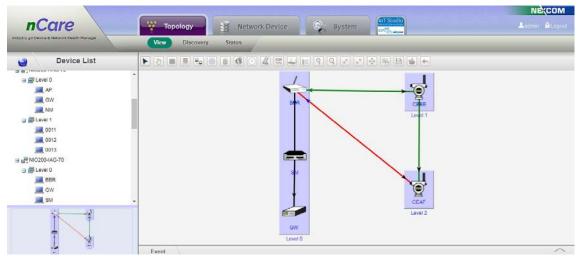


Figure 169 Check for ISA100 Device Information

(20) Time zone can be set for NIO200.

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

nCare

y 4 D Device & Notwerk Health Manager	Discovery Status				
Device List			0 % B		
NIC200_LAG_T0-AP Enimprise Access Point - EAP220 HP IVF300-43 IVF300-44-12 IVF500-76 IVF500-76 IVF500-112.0 IVF500-12.0 IVF500-12.0 IVF500-12.0 IVF500-12.0 IVF500-12.0 IVF500-12.0 IVF500-10.0		Status Usage	Web Modify Backup Restore FW Upgrade	NV500 44	MF500 53
NIO200-HAG-72		Log	Time Sync	W#300_11N_20	minado (milita
KI T.T.		Config > Ping	Account Setting	•	
A 19 19 19 1 1 1		Reboot			

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.

nCcire Industry 40 Device & Network Health Manager	Topology System	
Device List		
	The System Doorer The System D	11 11 11 12 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 12 14 14 14 14 14 14 14 14 14 14 14 14 14
- 8 g. a.	Event	^

Figure 171 Time Zone Sync with Browser

- **Q** Zoom In: Click to zoom in the Topology View.
- Soom 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 **e** icon and click **Yes** on the pop-up window. The topology will be recovered then.

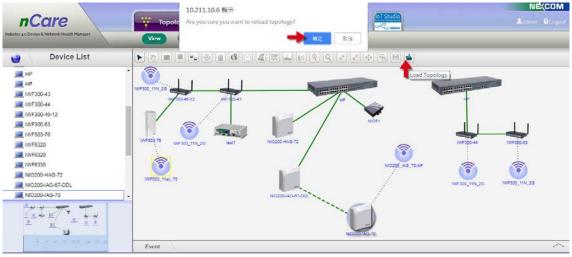


Figure 173 Load Topology

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.

nCare

) Device List			2 4 6 6 6	
 IWF300_11N_2G IWF6330-B1 Enterprise Access Point - EAP220 I+P I+P I+P IWF300-43 IWF300-44 IWF300-45 IWF300-45 IWF300-45 IWF300-45 IWF300-45 IWF300-45 IWF300-45 IWF300-45 IWF300 	WF300_11N_20	MF20-43 WF300_111(3	WF300 11N 20	er Server)
NI050	-		Nicase IW	F300-63 IWF300_11N_2G

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.

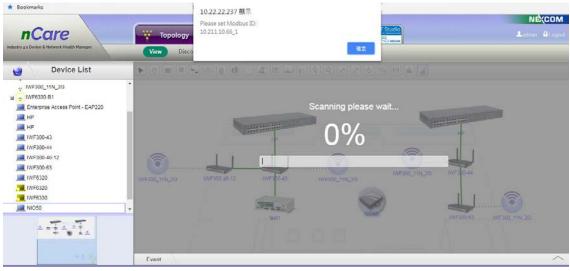


Figure 175 Modbus ID Setting

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

stry 4.0 Device & Network Health Manager	View Dise	covery Status	J.				
Device List		Po 🐵 🗉 🚱	0 4 5 4	99**			
WF030_11N_20 WF030_11N_20 WF030_11 = EAP220 HP HP WF030-43 WF030-44 WF030-43 WF030-43 WF030-43 WF030-4 WF030-4 WF030-4 WF030-4 WF030 WF030 WF030 NO50 T	WF300_11N_20	IWF300-40-12	IVFSD-43	INF300_11N_26	INFIDO_TIN_20	Web Modify Backup Restore FW Upgrade Modus ID Saltin Modus Scheduk	

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*.

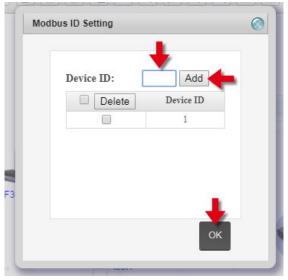


Figure 177 Modbus ID Setting Window

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

nCare

WF300_11N_20	
e Interprise Access Point - EAP220 Scanning please wait	
HP Contraction of the second	China -
	a state of the sta
HP WF300-13 11%	+
IVF300-44	
INF30046-12	
IWF300-63	
WF6320 INF300_11N_20 INF300-45-12 INF300-43 INF300_11N_20 IN	F300-44
■ (WF6320	
L MF6330	
NI050	

Figure 178 NIO50 Device Updating

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

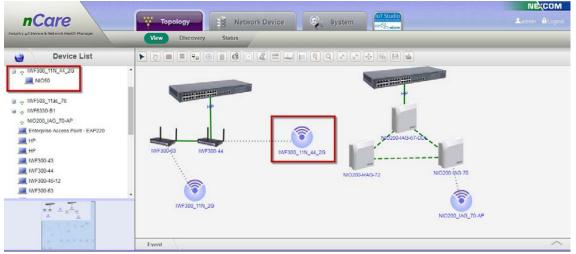


Figure 179 Adding NIO50 Device to Topology Group

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

nCare

		NE(COM
nCare	Topology 🔡 Network Device 🚭 System	
dustry 4.0 Device & Network Health Manager	View Discovery Status	
Barden Het		
Device List		
WF300_11N_44_2G	*	
田 副門 NIO50		
III NIO50		
 IWF503_11ac_76 		
- IWF6330-81		
NIO200_IAG_70-AP Enterprise Access Point - EAP220	NIOSO	
HP		
HP I		
IWF300-43		
IWF300-44		
IWF300-46-12		
s		
	Event	/

Figure 180 Devices in Topology Group

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

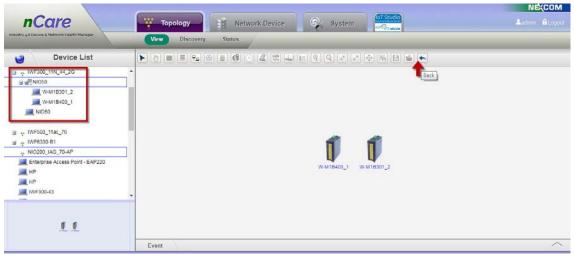


Figure 181 Devices in PLC Group

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

nCare

	View Discovery Status		
Device List	Status History Status	Current Status	
- IWF300_11N_44_2G 副型NIC50	Name	IP Address Latitude	Longitude
W-M1B301_2	W-M1B301_2	- 0	0
WF503_11ac_76 WF6330-B1 NIO200_IAG_70-AP	*Note: Please use white space to seper Register Name devicetD	ate the register values when write multiple registers Register Value 2	Unit Write
Enterprise Access Point - EAP220	DICounterValue	2 0001	
HP HP	DlinputActiveValue	0000 (Hex)	Write
IWF300-43	FirmwareVersion	0100	, taganan
-	ModuleName	W-M18301	
		Export to .csv Export to .txt	

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.

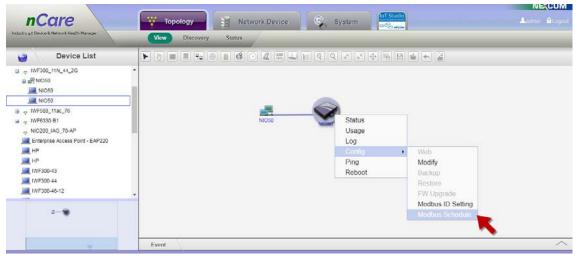


Figure 183 Modbus Scheduling

- (13) A "Modbus Schedule" window will pop-out.
- (14) Select *Start Time* and *Repeat*.
- (15) Click Add to Schedule to complete setting.

Mode	ous Schedule					0
	IP Address	:				
	Start Time:	:				
		None	•			
		Every Weeks Every Months				
			Add to s	Schedule	Cancel	

Figure 184 Time and Repeat Cycle for Modbus Scheduling

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

	View Discovery State	3			
Device List	Status History Sta	itus Current Status			
₩F300_11N_44_20	Name	IP Address	Latitude	Longitude	
W-M1B301_2	W-M1B301_2		0	0	
WF503_11ac_76 WF5030-B1	Register Table Edit "Note: Please use white space to sep Register Name	perate the register values when write mu	Itiple registers Register Value	Unit	Write
₩F503_11ac_76 ↓ WF50330-B1	"Note: Please use white space to sep	perate the register values when write mu		Unit	Write
 WF503_11ac_76 WF6330-B1 NIO200_IAG_70 AP Enterprise Access Point - EAP220 	"Note: Please use white space to sep Register Name			Unit	Write
WF503_11ac_76 WF503_61 WF5030_61 NI0200_JAG_70.AP Enterprise Access Point - EAP220 HP	"Note: Please use white space to seg Register Name device(D	2		(Hex)	Write
	*Note: Please use white space to seg Register Name deviceID DICcunterValue	2 0001			

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.

nCare

Device List	View Discovery	Status	Q	4	_
	Im NIGS1	MF200-44 MF200_11N_200	NI0200-HAG-72	-	

Figure 186 PLC Group of NIO51

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

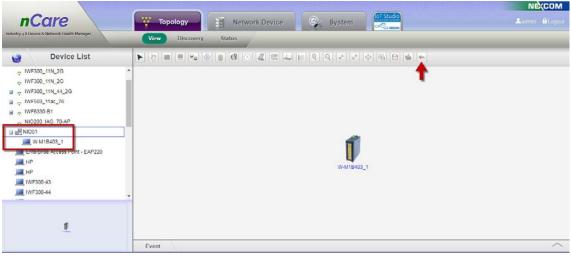


Figure 187 Devices Information of NIO51

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

nCare

Device List	Status					
	atatus					
 WF300_11N_2G WF300_11N_2G WF300_11N_2G WF300_11N_44_2G 	Name	Name IP Address Latitude			Longitude	
- IWF503_11ac_76	W-M18403_1	14	0			
► IWF6330-B1 ► NIO200_IAG_70-AP ■ NIO51 W-M18403_1	Register Table Edit Note: Please use while space to Register Nan	seperate the register values when write mu	Itiple registers Register Value		Unit	Write
Enterprise Access Point - EAP220	deviceID	1			20020	
E HP	DOPowerOnV	alue 0000	0000			Write
HP WF300-43	DOOutputActive	Value 0000	0000 (Hex)			Write
			0100			
WF300-44	FirmwareVers	ion 0100				

Figure 188 Modification for PLC Device of NIO51

- 7.1.2.3 Warning Message of Topology
- 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 <u>normal</u>. YELLOW message indicates <u>Major</u> issue. RED message indicates <u>Critical</u> issue.



Figure 189 Color Indication of Devices

- (2) Letter Indication: Letters indicates the numbers of alarms. **C** indicates <u>Critical</u> alarms. **M** indicates <u>Major</u> 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.

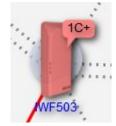


Figure 190 Letter Indication of Device

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

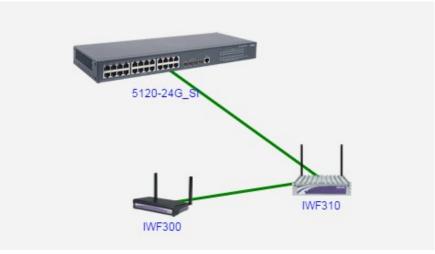


Figure 191 Internet Connection

- (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.

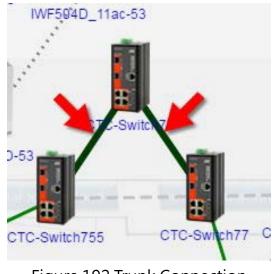


Figure 192 Trunk Connection

- +D_111g033
 IWF504D_11ac-53
 IWF6330
 IWF6320

 +2
 IWF604D-53
 IWF6320
 IWF6320

 +2
 IWF604D-53
 CTC-Switch76 (10.211.10.76)
 to
 CTC-Switch755 (10.211.10.75)

 CTC-Switch755
 CTC-Switch77
 CTC-Switch81
 CTC-Switch81

 F300-63*
 CTC-Switch755
 CTC-Switch81
 CTC-Switch81
- (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.

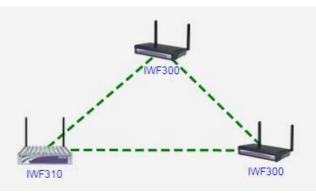


Figure 194 Mesh Network Connection

(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 \bigcirc icon to see the devices at this subnet. NE(COM **n**Care W Topology Network Device System View Discovery Status Device List 1 6 IWF300 11N 2G IWF300_11N_2G --------IWF300_11N_2G WF300 11N 2G 503_11ac_76 IWF503-77 E6330-81 NIC200_IAG_70-AP Enterprise Access Point - EAP220 HP HP WF300-43 1 1-11

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.

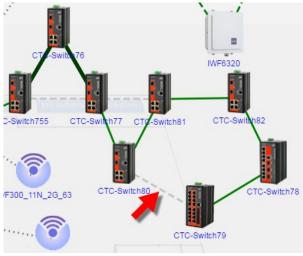


Figure 197 Devices in the Wifi Subnet

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

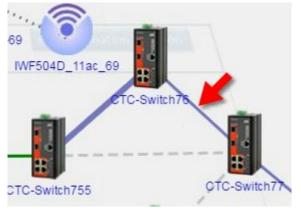


Figure 198 Purple Line

(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.

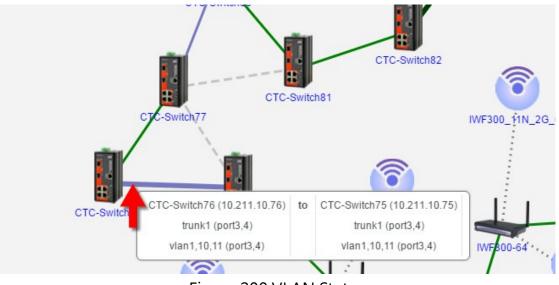


Figure 200 VLAN Status

- 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

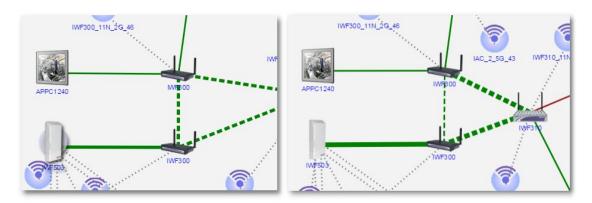


Figure 202 High Traffic Link

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

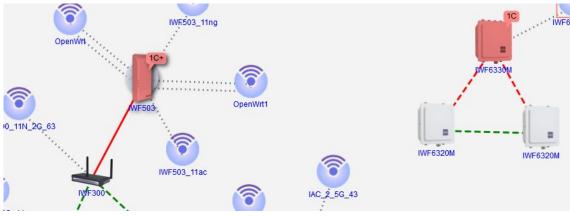


Figure 203 Disconnected Link

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

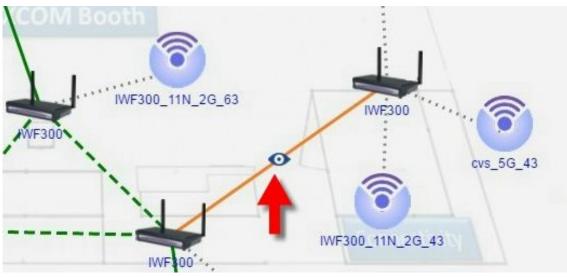


Figure 204 Link Over the Threshold

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*.

F300_11N_2G_46	cvs_5G_43	IWF300	CV5_5G_64
IWF300	Status		
	Usage Log		
IAC_2_2.4G_43	Config	Web	
	Ping	A Modify	
	Reboot	Backup	
IAC_2_5G_43		Restore FW Upgrade	

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.

Device IP:	10.211.10.63	Device Name:	IWF300	
EchoCount(1~4):	4	Size(8~5120):	32	(bytes)
		Timeout:	1000	(ms)
	Packets: 9 loss), Approximate re	cs for 10.211.10. Sent = 4, Receive Dund trip times i 1ms, Maximum = 1	d = 4, Lost n milli-sec	conds:

Figure 206 Ping Function

(6) Reboot: Reboot the device.

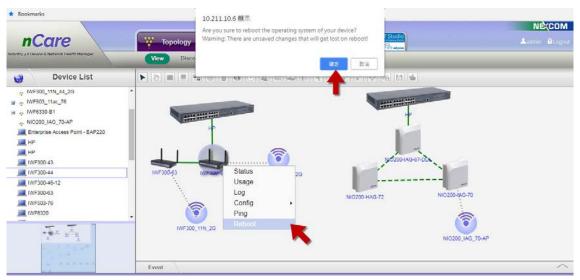


Figure 207 Reboot Function

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.

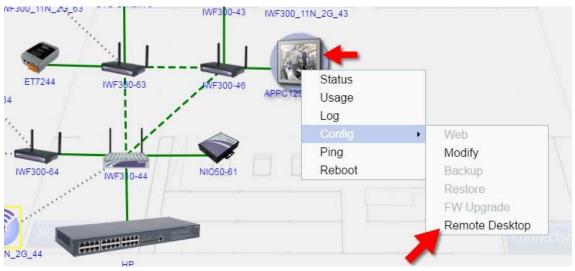


Figure 208 Remote Desktop

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.

7.2.20peration 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 <u>public</u> by default) and *Write Community*(set as <u>private</u> by default)

Topology

Device List	Discovery
Root WF300_11A_56_43 WF300_11A_56_64 WF300_11A_26_43 WF300_11N_20_43 WF300_11N_20_43 WF300_11N_20_64 WF500_11N_20_64 WF504D_11a_26_44 WF504D_11a_26_9 WF504D_11a_69 WF504D_11a_69	Start IP Address: End IP Address: Protocol: Trap Configuration: Systog Configuration: SNMP Version: (VI/V2C • Read Community: Write Community: private
	Scan

Figure 209 Device Discovery

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

Device List	Discovery	_
Root WF300_114_50_64 VMF300_114_50_64 WF300_1114_50_64 VMF300_1114_20_43 WF300_1114_20_43 WF300_1114_20_64 WF300_1114_20_64 WF300_1114_20_64 WF504D_1142_064 WF504D_1142_064 WF504D_1142_064 <tr< td=""><td>Start IP Address: End IP Address: Protocol: Trap Configuration: Systog Configuration: SNMP Version: VI/V2C • Read Community: Write Community: private</td><td></td></tr<>	Start IP Address: End IP Address: Protocol: Trap Configuration: Systog Configuration: SNMP Version: VI/V2C • Read Community: Write Community: private	
CTC-Switch75	- Scan	

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.

nCare

🥑 Device List	Discovery		
Root wWr300_11A_50_43 wWr300_11N_30_45 wWr300_11N_20_43 wWr300_11N_20_66 wWr300_11N_20_663 wWr300_11N_20_64 wWr500_11N_20_64 wWr500_11N_20_64 <th>Start IP Address: End IP Address: Protocol: Trap Configuration: Syslog Configuration: SNMP Version: <u>V1/V2C ▼</u> Read Community: Write Community:</th> <th>All CAPWAP SNMP Modbus</th> <th></th>	Start IP Address: End IP Address: Protocol: Trap Configuration: Syslog Configuration: SNMP Version: <u>V1/V2C ▼</u> Read Community: Write Community:	All CAPWAP SNMP Modbus	

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.

Device List	Discovery	
Root MF300_11A_56_43 MF300_11A_56_64 MF300_11N_26_43 MF300_11N_26_43 MF300_11N_26_43 MF300_11N_26_44 MF300_11N_26_44 MF5040_11a_69 MF	Start IP Address: End IP Address: I0, 211, 10, 1 Protocol: Trap Configuration: Syslog Configuration: SNMP Version: V1/V2C • Read Community: Write Community: private	

Figure 212 Device Searching with CAPWAP

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

y çı: Device & Network Health Manager	View Discovery Status	
Device List		
Root		
	Scanning please wait	
	10%	
	1070	
	the second se	

Figure 213 Scan Percentage

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

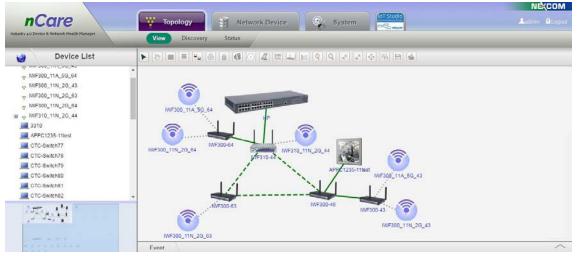


Figure 214 Discovered Devices

7.3 Device Status

7.3.1 Introduction for Device Status

The status of devices can be shown on this page.

7.3.2Operation 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.

nCare

Device List	Status	1		_		_		
	* Nam	ie	IP Address		Latitude	-	Longitude	
WIG50-66 v IWF300_11N_26 v IWF300_11N_26 v IWF300_11N_26 v IWF300_11N_26	IWF300	-46-12	10.211.10.46		0		0	
	MA	c	Device Type	Firmware	System up time	1	Description	
	00:10:13:	30:8b:a5	IWF (IWF300)	v1.1.9A-US	23 days/ 7 hours/ 29 minutes/ 2	23 seconds.	inux IWF300-46-12 3 14 27 #1 Tue Feb 13 12 20 07 CST 2018 mips	
WF6330-B1	Interface	Interface						
Enterprise Access Point - EAP220	Name	Туре	MAC	Channel	Tx bytes	Rx byb	es AssocClient	
HP.	10	loopback		19	447,828	447,8	28 0	
IWF300-43	ethD	ethernet	00:10:13:30:86:a3	100	463,913,838	3,389,57	0,414 0	
	br-lari	ethernet	00.10. 13.30.8 5.a3	1.2	434,173,735	2,674,28	1,149 0	
WF300-46-12 *	eth0.2	ethernet	00:10:13:30:8b:a3		476,405,622	2,952,99	7,614 0	
- FAT	8010.2							

Figure 215 IWF Type Device Status

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

Device List	Status Modbus WMI	
3310		_
APPC1235-11test		
CTC-Switch77	Device Information Hardware Monitoring GPIO	
CTC-Switch78		
CTC-Switch79		
CTC-Switch80	Platform	
CTC-Switch81	Device ID : 00:10:13:4a:0e:0a	
CTC-Switch82	Device Name : APPC1235-11test	
Enterprise Access Point - EAP220	Model : APPC Series	
HP	APPC1235-11test BIOS Name : AD27	
HP	CPU model : x86 Family 6 Model 54 Stepping 1/ GenuineIntel	
IWF300-43	DRAM Size : 4,095MB	
IWF300-46		
INF300-63		
に見る	Storage	
(24)분년	Model Name : Hitachi_HTE543232A7A3	

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**.

nCcire try 40 Device & Network Health Manager	View Disc	covery Status	rk Device 😪 System	
Device List	Status	Modbus <u>WMI</u>	+	
APPC1235-11test		WMI Verification		
CTC-Switch77				
CTC-Switch78				
CTC-Switch79		IP Address:	10.211.10.52	
CTC-Switch80		T. N.	*.	
CTC-Switch81		User Name:		
CTC-Switch82		Password:		
Enterprise Access Point - EAP220				
HP				_
HP				-
WF300-43			Submit Cance	el
WF300-46				-
IWE300-63	-			
·Zali				

Figure 217 WMI Function for IPC Device

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

	View Discovery	Status				
Device List	Status Mo	dbus <u>WMI</u>				
3310	*					
APPC1235-11test	Name	IP Address		Latitude	Long	ituda
CTC-Switch77						
CTC-Switch78	APPC1235-11test	10.211.10.5	2	0		0
CTC-Switch79	MAC	Device Type	Firmware	System up time	De	scription
CTC-Switch80		Construction Construction	1000000000	uj stem up sm		
CTC-Switch81	00:10:13:4a.8e.0a	IPC	AD27 008			
CTC-Switch82	BASEBOARD					
Enterprise Access Point - EAP220	DAVEDUARD					
HP	Manufacturer	Model	Name	Product	SerialNumber	SKU
HP	INTEL Corporatio	in	Base Board	Tiger Hill	To be filled by O E M.	
INF300-43					a to movely over	
N/F300-46	BIOS					
IWE300-63				0	0	
ATRA CI	Manufacturer		Name	SerialNumber	SMBIOSBIOSVersion	Version

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.

nCare

Device List	Status History	Status Current Status				
	*					
W-M1B301_2	Name	IP Address	Latitude		Longitude	
Enterprise Access Point - EAP220	W-M1B403_1		0		0	
HP HP IWF300-43		to seperate the register values when				
WF300-44	Register N	ame	Register Value		Unit	Write
IWF300-46-12	device	ID 1				
IWF300-63	DOPowerO	nValue 0000	0000			Write
WF503-76	DOOutputAct	iveValue 0000		(Hex)		Write
WF6320	FirmwareV	ersion 0100				

Figure 219 History Status of PLC Device

- (8) The <u>Registered Table</u> can be edited at **Current Status** page.
- (9) Click "Edit" to go to modify page.

Device List	Status	Status Current Status			
Root		+			
INF300_11A_5G_43	Name	IP Address	Latitude	Longitu	de
• IWF300_11A_5G_64	W-M1B403_1	10.211.10.66	0	0	
 №F300_11N_2G_64 №F310_11N_2G_44 ■NIC50-65 	Register Nan deviceID	27	Register Value	Unit	Write
		alue 0001	10	iex)	Write
W-M1B301_2	DOPowerOnV	0001			
W-M1B403_1	DOPtwerdny			Hex)	Write
		Value 0000		Hex)	

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 <u>Binary</u>, <u>Decimal</u> or <u>Hexadecimal</u>.

(14) Click "Save" to complete modification.

	View	Discovery Sta	dus				
Device List	Stat	tus History	Status Current S	tatus			
Root - IMF300_11A_5G_43 - IMF300_11A_5G_64	"Note: F	Participants of the second second second		lues when write multiple registe Function Code		Word Count	
- INF300_11N_2G_43	II All	Register Name	Unit	Function Code	Address Offset (E.g. 40123 -> 122)	word Count	Attribute
PingableDevice		deviceID		1: Coils •			Hex •
 IWF300_11N_2G_64 IWF310_11N_2G_44 		DOPowerOnValue		3. Holding Registers *	256	[1	RW •
■ INIO50-65 ■ W-M18301_2	.0	DOOutputActiveValue	1	3 Holding Registers *	384	1	RW • Hex •
W-M1B403_1		FirmwareVersion	16	3. Holding Registers *	4096	1	R T Hex T
NIC50-65 2 IWF8330-81 2 2240		ModuleName	I [3: Holding Registers •	4097	8	R T Unicode1 T
	-	XXX	I (1: Coils •	22	1	B R RW

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.

Name W4M18403_1	Status Current Status					
100000	IP Address	10.12.12.10				
1818440402 4		Latitude		Longitude		
About Charley "	10.211.10.66	0		0		
: Please use white space to		ter values when write multiple registers Register Value				
DOPowerOnVa	lue 0001		(Hex)		Write	
DOOutputActive)					Write	
FirmwareVers	on 0100		18.558		(COLUMN)	
ModuleNam	e W-M1B403					
xxx	0000000000		(Binary)		Write	
	Register Nam deviceID DOPowerOnVa DOOutputActiveV FirmwareVersi ModuleNam	e: Please use white space to separate the register values when write mult Register Name deviceID DOPowerOnValue DOOUtputActiveValue DOOUtputActiveValue FirmwareVorsion 0100 WoduleName WH41B403	e: Please use white space to separate the register values when write multiple registers Register Name Register Value deviceID 0001 DOPowerCnValue 0000 DOOutputActiveValue 0000 FirmwareVersion 0100 ModuleName VH/4118403	e: Please use whet space to separate the register values when write multiple registers Register Name Register Value deviceID 0001 DDOPowerChValue 0000 DDOoutputActiveValue 00000 FirmwareVersion 0100 ModuleName VH-H18403	Iterase use despace to separate the register values when write multiple registers Register Value Unit deviceID 6001 (Hex) 1 DDOPowerCmValue 0000 (Hex) 1 DDOOutputActiveValue 0000 (Hex) 1 FirmwareVersion 0100 (Hex) 1 ModuleName V-Vrit18403 1 1	

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.

nCare

atry 40 Device & Network Health Manager	View Di	scovery S	tatus						
Device List	Status								
Root	-								
* IWF300_11N_2G	Name		IP Address		Latitude	L	Longitude		
 IWF300_11N_2G IWF300_11N_2G 	IWF30	0-44	10.211.10.44		0		0		
v IWF300_11N_44_2G	мас		Device Type	Firmware	System up time		Description		
 IWF503_11ac_76 IWF5330-B1 	00,10.13.5	e 28.57	IWF (IWF 300)	v1.1.9A-US	28 days/ 9 hours/ 41 minutes/ 6 s		0-44 3.14.27 #1 Tue Feb 13 1:07 CST 2018 mips		
NIO200_IAG_70-AP Enterprise Access Point - EAP220	Interface								
HP	Name	Туре	MAC	Channel	Tx bytes	Rx bytes	AssocClient		
HP IWF300-43	lo	loopback	1 91		79,121	79,121	0		
WF300-44	eth0	ethernet	00:10:f3:30:8b	n -	1,226,416,945	442,834,614	0		
1	br-lan	ethernet	00:10:13:30:86	n -	11,251,183	36,738,746	0		
×	etto() 2	ethernet	00:10:13:30:86	n .	40.910.220	891 386	n		

Figure 223 Status Exportation

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

Device List	Charles .				
Device List	Status				
- NIO51 -	Name	IP Address	Latitude	Longitud	
W-M1B403_1 Enterprise Access Point - EAP220	W-M18403_1		0	0	
HP HP IWF300-43 IWF300-44	Register Table Edit *Note: Please use white space to s Register Name	eperate the register values when write mult	tiple registers Register Value	Unit	Write
IWF300-46-12	deviceID	1			
IWF300-63	DOPowerOnVa	lue 0000	(Hex	(Write
WF300-83 WF503-76	DOOutputActive	alue 0000	(Hex		Write
	DOOUTputActives		0100		
IWF503-76 IWF6320 IWF6320	FirmwareVersi	on 0100			

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.

40 Device & Network Health Manager	View Discove	ry Status								
Device List	Status	Devices Lis	đ l							
Enterprise Access Point - EAP220	Name	Туре		MAC		Channel	Tx by	tes	Rx bytes	AssocClient
HP	lo	loopba	:k			-	1,291	,625	1,291,625	0
HP	br-lan	ethern	et O	00:10:f3:5a:42:77			1,972	.024	6,601,917	0
IWF300-43	wian1	wireles	s 0	00:10:13:5e:28:6b		44	2.388	665	8.076.194	2
IWF300-44				10.10.00.20.00			2,000		0,010,104	-
IWF300-46-12	Client List									
IWF300-63	_					1				
IWF503-76			AC		Mode	IF		RSSI	Тх	Rx
IWF6320 IWF6320		00:10:F	3:62:38:58		mesh	wla	n1	-49	270.0	270.0
IWF6330		00:10:F	3:5E:28:43		mesh	wla	n1	-62	300.0	270.0
NIO200-HAG-72	AD 0447	AP Scan Get								
NIO200-IAG-67-DDL	AP Scan Get									
NIO200-IAG-70		Name(SSI)}		Channel		RSSI		Quality	MAC
NIO51										
PingableDevice	Wireless HART [Devices List								
PingableDevice	EUI-64 Add	iress	Tag			Role / Model		Status	Last read	Run Command
PingableDevice	00-1B-1E-E2-F			242		Device / N/A		FULL_JO		
PingableDevice			Microcyber_KIT_0020							
PingableDevice	00-1B-1E-E2-F	6-00-20-47	Microcyber_KIT_0020	047		Device / N/A		FULL_JO		-
PingableDevice Unknown	00-1B-1E-F8-7	0-06-00-01	NEXCOM AP		Access	Point / WirelessHAR	l' Device	FULL_JO	IN NULL	۲
Unknown	00-1B-1E-F9-8	0-00-00-01	NEXCOM WHart Mana	ager	Network Mana	ger / WirelessHART N	etwork Manager	FULL_JO	IN NULL	
	00-1B-1E-F9-8	1-00-00-02	NEXCOM GW		Gate	vay / WirelessHART G	ateway	FULL_JO	IN NULL	۵
	Wireless HART (Command Lo	gs Update							
0	Tracking No.		EUI-64 Address	Command	Dara	neters	Status	Posted Time	Response Time	Response

Figure 225 Device Status for NIO200-HAG

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

Device List	Status	Devices List								
Enterprise Access Point - EAP220	Name	Туре		MAC	Channel		Tx bytes	R	x bytes	AssocClient
HP	lo	loopback					1,291,625		1,291,625	0
HP	br-lan	etherni	Run Command			0	1,972,024	6	3,601,917	0
IWF300-43	wian1	wireles	Run Command			0	2.388.665		3.076.194	2
IWF300-44							2,000,000			
IWF300-46-12	Client List		EUI-64 Address:	00-1B-1E-E2-F6	i-00-20-42					
IWF300-63 IWF503-76		M	Nickname:	0011				SSI	Tx	Rx
WF6320					000010					
WF6320		00:10:F	Device Tag:	Microcyber_KII	_002042			-49	270.0	270.0
WF6330		00:10:F	Command:	<select></select>	*			-62	300.0	270.0
NIO200-HAG-72	AP Scan Get			<select></select>						
NIO200-IAG-67-DDL	AF Scall Ger			WH General C	ommand					
NIO200-IAG-70		Name(SSIL						(Quality	MAC
NI051										
PingableDevice	Wireless HART [Devices List								
PingableDevice	EUI-64 Add	iress						Status	Last read	Run Command
PingableDevice	00-18-1E-E2-F	8-00-20-42						FULL_JOIN	2018-08-03 04:23:04	
PingableDevice PingableDevice	00-18-1E-E2-F									
PingableDevice								FULL_JOIN	2018-08-03 04:23:01	
Unknown	00-1B-1E-F8-7	0-06-00-01						FULL_JOIN	NULL	
Unknown	▼ 00-1B-1E-F9-8	0-00-00-01			Execute Ca	incel	lager	FULL_JOIN	NULL	
	00-1B-1E-F9-8	1-00-00-02						FULL_JOIN	NULL	
to the	Wireless HART O		35 Update	Command	Parameters	Status	Posted	Time	Response Time	Response

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) <u>ISA100 Devices List</u> and <u>ISA100 Command Logs</u> can also be set and updated on this page.

	1								_	-	_
Device List	Status	Devices Li	st Trouble Shooting								
Enterprise Access Point - EAP220	•		MAC	Mod	e	IF	RSSI	Тх		F	2x
HP		00:10:	F3:5E:28:43	me	sh	wian0	-63	180.0		2	40.0
HP		00:10	F3:5E:28:6B	me	sh	wian0	-42	243.0		2	70.0
IWF300-43											
IWF300-46-12	AP Scan G	iet									
IWF300-63		Name(SSI	D)	Channe	I	RSSI		Quality		MA	с
IWF503-76											
IWF6320	ISA100 Dev	ices List									
IWF6320	EUI-64 Add	Iress	IPv6 Address	Tag	Rev	ision	Role	Model	Status	Last	Run
IWF6330 NIO200-HAG-72								ne Router /		read	Comman
NIO200-HAG-72 NIO200-IAG-67-DDL	0000:0000:00	00:0005 FE80:0000	0000:0000:0000:4E7D:0AD3	0A46 NEXCOM Backbone	42425F5F303	42E31352E3031	465245455343414	C455F564E33313020	FULL_JOIN	NULL	۲
NIO200-IAG-70	0000.0000.04	10:00A0 FE80:0000	0000.0000.0000.4E7B.0AD3	000:4E7B.0AD3:0A46 NEXCOMSystem_Mng 322E372E3238 System Manager / 534D		FULL_JOIN	NULL	۲			
NIO51	0000:64FF:FE	9B:CEAF FC00:0000	0000:64FF:FE9B:CEAF:0004	:0047 FN310-58	52312E3	0372E3031	IO Router Device / 495	534120414E54454E4E41	FULL_JOIN	NULL	
PingableDevice	0000:64FF:FE	9B.CEBB FC00:0000	CEB8 FC00.0000.0000.64FF.FE98.CEB8.0004.0053		52312E3	0372E3031	IO Router Device / 49	534120414E54454E4E41	FULL_JOIN	NULL	٩
PingableDevice	600D:BEEF:60	OD BEEF FESO 000	0000.0000.0000.4E7C:7F00	0001 NEXCOM Gateway	322E372E3432202	0202020202020202020	Gateway / 4741544557	\$15920202020202020202020	FULL_JOIN	NULL	۲
PingableDevice PingableDevice											
PingableDevice	ISA100 Con	mand Logs	date								
PingableDevice	Tracking No.	EUI-64 Address	Command	Parameters	Status	Posted Time	Response Time		Response		
Unknown	2409	0000:0000:0A10:00A	0 Neighbor Health Report	Device ID: 0000:0000:0000:	0005 Responded	2018-08-03 20:27:33	2018-08-03 03:26:49		success		
Unknown	2408	0000:0000:0A10:00A	0 Neighbor Health Report	Device ID: 0000:64FF:FE9B:	CEBB Responded	2018-08-03 20:22:41	2018-08-03 03:21:55		success		
	2407	0000:0000:0A10:00A	0 Neighbor Health Report	Device ID: 0000:64FF:FE9B:	CEBB Responded	2018-08-03 20:22:37	2018-08-03 03:21:53		success		
1º Alt	2406	0000:0000:0A10:00A	0 Neighbor Health Report	Device ID: 0000:64FF:FE9B:	CEBB Responded	2018-08-03 20:22:29	2018-08-03 03:21:43		success		
<u>0</u>	2405	0000:0000:0A10:00A		Device ID: 600D:BEEF:600D:		2018-08-03 20:22:25		Error Reason: App(-11)-g		d a comm	unication erro
	2404	0000.0000.0A10.00A	-	Device ID: 600D:BEEF:600D		2018-08-03 20:22:23		Error Reason: App(-11)-g			

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.

nCare

	View Di	scovery	Status										
Device List	Status		Devices List										
Enterprise Access Point - EAP220	*		MA	AC		Mode		IF	RSSI	Tx			Rx
HP			00:10:F3	3:5E:28:43		mesh		wlan0	-63	180.0		2	240.0
HP			00:10:F	Run Command				0	-42	243.0		1	270.0
IWF300-43 IWF300-44													
WF300-46-12	AP Scan	iet			0000-0	000-0000-0005							
WF300-63			Name(SSI	EUI-64 Address	s:					Quality		MA	c
WF503-76				IPv6 Address:	FE80:	000:0000:0000:000	0:4E7D:0AD	3:0A46 -					
WF6320	ISA100 Dev	ices List		Command:	Rese	t Device	•						
WF6320	EUI-64 Add								Data	/ Model	Status	Last	Run
WF6330	EUI-04 Add	iress	_	Restart Type		select>	•				Status	read	Comman
NIO200-HAG-72	0000:0000:00	000:0005	FE80:0000		V	arm Restart		_	Backbo 465245455343414	one Router / 4C455F564E33313020	FULL_JOIN	NULL	9
NIO200-IAG-67-DDL	0000:0000:04	10:00A0	FE80:0000			estart as provisione eset to factory defau			System M	lanager / 534D	FULL JOIN	NULL	6
NIO200-IAG-70 NIO51	0000:64FF:FE	9B CEAF	FC00:0000:						IO Router Device / 49	534120414E54454E4E41	FULL_JOIN	NULL	6
PingableDevice	0000:64FF:FE									634120414E54454E4E41	FULL_JOIN		10
PingableDevice													
PingableDevice	600D:BEEF:60	JUD:BEEF	FE80.0000						Gateway / 4/4154455/	415920202020202020202020	FULL_JOIN	NULL	
PingableDevice	ISA100 Com	mand L	ogs Up										
PingableDevice													
PingableDevice	Tracking No.	EUI-64	Address						Response Time		Response		
Inknown Inknown	2409	000:000	0:0A10:00A(recute	Cancel	2018-08-03 03:26:49		success		
nknown	2408	0000:000	0:0A10:00A(E	lecule	Gancer	2018-08-03 03:21:55		success		
T. T.A.	2407	000:000	0:0A10:00A0	and the second statement of the second s					2018-08-03 03:21:53		success		
	2406	0000:000	0:0A10:00A0	Neighbor Health Report	Device ID: 000	0.64FF:FE9B:CEBB	Responded	2018-08-03 20:22:29	2018-08-03 03:21:43		success		
<u>a</u>	2405	0000:000	0:0A10:00A0	Neighbor Health Report	Device ID: 600	DIBEEF:600DIBEEF	Failed	2018-08-03 20:22:25	2018-08-03 03:21:41	Error Reason: App(-11)-g	ateway reporte	ed a comm	nunication err
	2404	0000.000	0.0A10.00A0	Neighbor Health Report	Device ID: 600	D.BEEF.600D.BEEF	Failed	2018-08-03 20:22:23	2018-08-03 03:21:37	Error Reason: App(-11)-g	ateway reporte	d a comm	nunication err

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.

nCare try 40 Device & Network Health Manager	View Discovery Status		System		
Device List	Status Devices Li	st Trouble Shooting			
Enterprise Access Point - EAP220	•	-			
HP I	ISA100 TroubleShooting				
HP		-			
IWF300-43	EUI-64	Timestamp	Event	Details	
IWF300-44	600D:BEEF:600D:BEEF	2018-08-03 02:43:03	Contract Modify	[GW/UAP2] -> [0000:64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 id : 5 Aperiodic	
IWF300-46-12	600D:BEEF:600D:BEEF	2018-08-03 02:42:53	Contract Modify	[GW/UAP2] -> [0000:64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 id : 5 Aperiodic	
IWF300-63	600D:BEEF:600D:BEEF	2018-08-03 02:37:53	Contract Modify	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 4 Aperiodic	
IWF503-76 IWF6320	600D:BEEF:600D:BEEF	2018-08-03 02:37:53	Contract Modify	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 4 Aperiodic	
IWF6320	600D BEEF 600D BEEF	2018-08-03 02:37:53	Contract Modify	[GW/UAP2] -> [0000.64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 4 Aperiodic	
WF6330	0000:64FF:FE9B:CEBB	2018-08-03 02:26:10	Contract Establish	[0000:64FF;FE9B;CEBB/UAP2] -> [GW/UAP2] CB : -15 EB : -15 id : 3 Aperiodic	
NIO200-HAG-72					
NIO200-IAG-67-DDL	600D:BEEF:600D:BEEF	2018-08-03 02:25:57	Contract Modify	[GW/UAP2] >> [0000:64FF;FE9B;CEBB/UAP2] CB : -8 EB : 4 id : 5 Aperiodic	
NIO200-IAG-70	600D:BEEF:600D:BEEF	2018-08-03 02:25:17	Contract Establish	[GW/UAP2] -> [0000:64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 Id : 5 Aperiodic	
NIO51	0000:64FF:FE9B:CEBB	2018-08-03 02:24:47	Contract Establish	[0000:64FF:FE9B:CEBB/DMAP] → [SM/SMAP] P : 60 Ddin : 0.000 s id : 2 Periodic	
PingableDevice	600D:BEEF:600D:BEEF	2018-08-03 02:24:27	Contract Refusal	[GW/UAP2] -> [0000.64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 id : 0 Aperiodic Reg: create; Reason: delayed	
PingableDevice	0000:64FF:FE9B:CEBB	2018-08-03 02:24:11	Contract Refusal	[0000:64FF:FE9B:CEBB/DMAP] → [GW/UAP2] CB: 12 EB: 12 id: 0 Aperiodic Reg. create; Reason: delayed	
PingableDevice PingableDevice	600D:BEEF:600D:BEEF	2018-08-03 02:23:57	Contract Refusal	[GW/UAP2] → [0000.64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 id : 0 Aperiodic Reg: create; Reason: delayed	
PingableDevice	600D:BEEF:600D:BEEF	2018-08-03 02:23:49	Contract Refusal	[GW/UAP2] → [0000:64FF:FE98.CE88/UAP2] CB: -15 EB: 4 id: 0 Aperiodic Reg: create; Reason: delayed	
Unknown		2018-08-03 02:23:27	Contract Refusal	[GW/UAP2] -> [0000.64FF:FE9B:CE8B/UAP2] CB : -15 EB : -15 id : 0 Aperiodic Reg: create; Reason: delayed	
To The	600D:BEEF:600D:BEEF	2018-08-03 02:22:57	Contract Refusal	[GW/UAP2] → [0000:64FF:FE9B:CEBB/UAP2] CB : -15 EB : -15 Id : 0 Aperiodic Reg: create; Reason: delayed	
	0000:64FF:FE9B:CEBB	2018-08-03 02:22:47	Device Join	IPv6; [IPv6]	
<u>.</u>	600D:BEEF:600D:BEEF	2018-08-03 02:22:26	Contract Modify	[GW/UAP2] → [0000:64FF:FE9B:CEAF/UAP2] CB : -8 EB : 4 id : 4 Aperiodic	
	0000:64FF:FE9B:CEAF	2018-08-03 02:22:16	Contract Establish	[0000:64FF:FE9B:CEAF/UAP2] -> [GW/UAP2] CB : -15 EB : -15 id : 3 Aperiodic	

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-s olutions/iot-studio/nexcom-industrial-iot-studio

After installation, click IoT Studio on the main page

Topology 🛐 Network Device 🙊 System

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.

9.1.1System 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 <u>nCare User</u> is shown as follows:

Main Menu	Sub menu L1	Sub Menu L2	Authorization
Topology	View	lcons	Opened functions: • Select • Move • Traffic Monitoring • Show/Hide Rogue Devices • Switch VLAN • Update AP • Update IWSN • Zoom In • Zoom Out • Zoom Out • Zoom Overview • Zoom Reset • Full Screen • Export to Image (For devices opened by Administrator) Opened functions:
		Shortcut	 Usage Log Config Ping (For devices opened by Administrator)
	Status	Export to Report	
Network Device	Log	Event Log	All functions are opened (For devices opened by Administrator)
		System Log	
	Usage	Eth	
		Wlan	
		CPU	
		Memory	

Figure 231 Authorization for nCare User

9.1.2Device Manager

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

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

Figure 232 Authorization for nCare Manager

9.1.3System Administrator

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

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

Figure 233 Authorization for nCare Administrator

9.2 Device Aberrant Status

9.2.1Same IP

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

					NECOM
nCare	Topology	Network Device	System		
Industry 4.0 Device & Network Health Manager	View Discovery	Status	- Citetan		
Device List					
Root	1	Discovery Result			0
MF300-46	VF300_11N_20	10			
		IP Conflic			
	INF300-		IP Address	Quantity	
			10.211.10.46	2	
				_	
				ок	
					and the second s
	Event				_ ~
<u>ب</u>	Critical Major Replay				
	ID	IP Address	Device Name	Event	Time
	1	10.211.10.46	IWF300-46	IP Address Conflict	2018-06-25 17:55:41
			Industry 4.0 Device & Network Health Manager		

Figure 234 Discovery Result for the Same IP

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

try 4.0 Device & Network Health Manager	Manage Log	Usage Severity In	iterval Group Rogue AP/	Device		
Log Event Log Sys	tem Log Playback					
	Clear					< < 1
Begin Date: 2018-05-25	Clear ID	IP Address	Device Name	Severity	Event	Time
nd Date: 2018-06-25	1	10.211.10.46	IWF300-46	Critical	IP Address Conflict	2018-06-25 17:57:20
Address: IP Address						
verity: Critical *						
wice Name: ncare 🔻	1					
bar						
Search						

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.

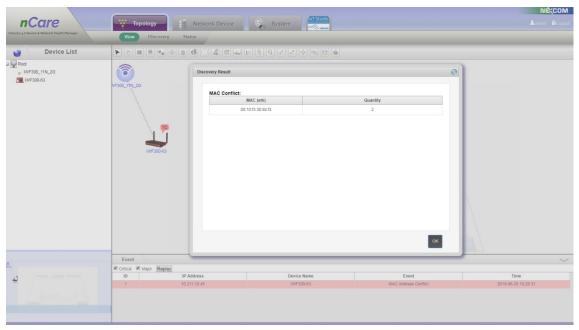


Figure 236 Discovery Result for the Same MAC

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

Andry a's Device & National Nanage Log Usage Severity Interval Group Rogue AP/Device Log EventLog Playback	nCare	Topology	Network Device System			NECON Ladmin Alog
Clear ID IP Address Device Name Sevently Event Time Bigin Date: 2018-06-25 ID 1 10.211.10.45 IVF300.63 Orncal MAC Address Contect 2018-06-25 18.21.31 End Date: 2018-06-25 ID 1 10.211.10.45 IVF300.63 Normal Moling Buckess 2018-06-25 18.27.58 IP Address IP Address IP Address IP Address IVF300.63 Normal Poling Buckess 2018-06-25 18.27.58 Barver, Circical * IP IP Address IVF300.63 Normal Poling Buckess 2018-06-25 18.27.58 Barver, Circical * IP						
Bagen Date: 2018-06-25 Image: Control of the state o	Log <u>Event Log</u> System	m Log Playback				
Like U IP-Address Davice Name Several Like Image 2018-06-25 1 10/21110/45 IVF00063 Ornical MACAdress Conflict 2018-06-25 18.27.38 3 Brokess 2 10/21110/45 IVF00063 Normal Poling Success 2018-06-25 18.27.58 3 Brokess - 2 10/21110.45 IVF00063 Normal Poling Success 2018-06-25 18.27.58 3 Brokess - 2 10/21110.45 IVF00063 Normal Poling Success 2018-06-25 18.27.58 3 Brokess - 2 10/21110.45 IVF00063 Normal Poling Success 2018-06-25 18.27.58 3 Brokess - - 2 10/21110.45 IVF00063 Normal Poling Success 2018-06-25 18.27.58 3 Brokess - - - - - - - - - 3 Douce Name rcare - - - - - - - - - 3 Douce Name rcare - - - - - - - - - - - 3 Douce Name rcare - - - - -		Clear				<<1>
End Date: 2018-06-25 Comman Posting Staccess 2019-06-25 18 27:58 IP Address IP Addres IP Addres IP Addre	Jegin Date: 2018-05-25	Clear ID	IP Address Device Name	Severity	Event	Time
IP Address IP Address Severity Critical * Clear		1	10.211.10.45 IWF300-63	Critical	MAC Address Conflict	2018-06-25 18:28:31
Severity: Critical * Desce Name: ncare Clear	and Date: 2018-06-25	2	10.211.10.45 IWF300-63	Normal	Polling Success	2018-06-25 18:27:58
Clear	Severity: Critical *					
	Search					

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.

o Device & Network Health Manager	Users Message	Database	DHCP Scan IP	About	
			Start IP Address: 10 . 21 End IP Address: 10 . 211		
			IP Address	MAC Address	
			10.211.10.44	00:10:f3:30:8b:f3	
			10.211.10.45	00:10:f3:30:8b:f3	

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.

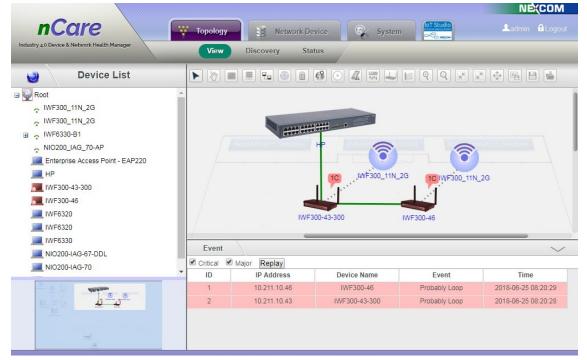


Figure 239 Event for Devices set as Loop with Mistake on Main Page

nCare	100	Торо	ology	S N	etwork Device 🤤 🎯 System	n 🥪		Ladmin 🔒 Logo
stry 4.0 Device & Network Health Manager	-	N	lanag	je Log	Usage Severity Inte	rval	Group Rog	ue AP/Device
Log Event Log	System	n Log	P	layback				
			Cle	ear				<<1>>
Begin Date: Begin Date		0	А	10.211.10.07	NIU200-IAG-07-DDL	Critical	Poliing Falled	2018-00-20 17.29.00
			10	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:29:56
End Date: End Date			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
IP Address: IP Address			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
Severity: Critical V			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
Device Name: ncare	v		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
Clear			19	10.211.10.51	IWF6320	Critical	Polling Failed	2018-06-25 17:23:34
Cieai			20	10.211.10.52	PingableDevice	Critical	Polling Failed	2018-06-25 17:23:34
		1	21	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:23:34
Search			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: <u>https://apps.twitter.com/</u>

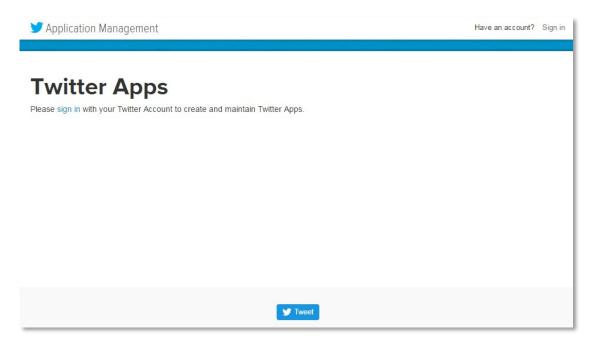


Figure 241 Login to Twitter Apps

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



Figure 242 Build a New Program

- (4) Enter <u>Create an application</u> 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.

Application Details	
Name *	
Your application name. This is used	I to attribute the source of a tweet and in user-facing authorization screens, 32 characters max.
Description *	
Your application description, which w	will be shown in user-facing authorization screens. Between 10 and 200 characters max.
Website *	
Your application's publicly accessible	ie 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.
source attribution for tweets created	
source attribution for tweets created (if you don't have a URL yet, just put	by your application and will be shown in user-facing authorization screens.
source attribution for tweets created i (if you don't have a URL yet, just put	by your application and will be shown in user-facing authorization screens.
source altribution for tweets created (If you don't have a URL yet, just put Caliback URL	by your application and will be shown in user-facing authorization screens.
source altribution for tweets created. (If you don't have a URL yet, just put Caliback URL Where should we return after succes	f by your application and will be shown in user-facing authorization acreens. I a placeholder here but remember to change it later.)
source altribution for tweets created. (If you don't have a URL yet, just put Caliback URL Where should we return after succes	I by your application and will be shown in user-facing authorization screens. I a placeholder here but remember to change it later.) sofully authenticating? Okum 1.0a applications should explicitly apecily their oauth_callback URL on the request token step, regardless of the value given
source attribution for tweets created. (If you don't have a URL yet, just put Callback URL Where should we return after succes	I by your application and will be shown in user-facing authorization screens. I a placeholder here but remember to change it later.) sofully authenticating? Okum 1.0a applications should explicitly apecily their oauth_callback URL on the request token step, regardless of the value given
source altribution for tweets created. (If you don't have a URL yet, just put Caliback URL Where should we return after succes	I by your application and will be shown in user-facing authorization screens. I a placeholder here but remember to change it later.) sofully authenticating? Okum 1.0a applications should explicitly apecily their oauth_callback URL on the request token step, regardless of the value given
source altribution for hweets created. (If you don't have a URL yet, just put Caliback URL Where should we return after succes	In y your application and will be shown in user-facing authorization screens. Is a placeholder here but remember to change if later.) sofully authenticating? O4un 1.0a applications should explicitly specify their oauth_callback URL on the request token step, regardless of the value given musing calibacks, leave this field blank.

Figure 243 Create an application page

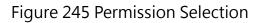
(7) You' II see the page shown below after complete setting.

		Test OAuth
Details Settings	Keys and Access Tokens Permissions	
A		
¥ -		
Organization		
Information about the org	panization of company associated with your application. This information is optional.	
Organization	None	
Organization website	None	
r		
Application Settin		
	ngs	
	IGS mer Key and Secret are used to authenticate requests to the Twitter Platform.	
	-	
Your application's Consu Access level	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions)	
Your application's Consul Access level Consumer Key (API Key)	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gy/TbjbCM8hvdn6al.TUaq0kgJ6 (manage keys and access	
Your application's Consu	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gv7bjbCM8lwdn6aLTUaq0kgJ6 (manage keys and access tokens)	
Your application's Consur Access level Consumer Key (API Key) Callback URL	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Øv7bjbCM8lwdn6aLTUaq0/gJ6 (manage keys and access tokens) None	
Your application's Consu Access level Consumer Key (API Key) Callback URL Callback URL Locked	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gv7bjbCM8hwdn6aLTUaq0kgJ6 (manage keys and access tokens) None No	
Your application's Consur Access level Consumer Key (API Key) Caliback URL Caliback URL Caliback URL Locked Sign in with Twitter App-only authentication	mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gv7bjbCM8lwdn6aLTUaq0kgJ6 (manage keys and access tokens) None No Yes	
Your application's Consur Access level Consumer Key (API Key) Caliback URL Caliback URL Caliback URL Locked Sign in with Twitter	Mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gv7bjbCM8lwdn6aLTUaq0kgJ6 (manage keys and access tokens) None No Yes https://apl.twitter.com/oauth2token	
Your application's Consur Access level Consumer Key (API Key) Callback URL Callback URL Callback URL Locked Sign in with Twitter App-only authentication Request token URL	Mer Key and Secret are used to authenticate requests to the Twitter Platform. Read and write (modify app permissions) Gv7bjbCM8lwdn6aLTUlaq0kgJ6 (manage keys and access tokens) None No Yes https://apl.twitter.com/loauth2/token https://apl.twitter.com/loauth2/token	

Figure 244 Obtain Application Data

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

Nexco		Test OAuth
Access		
What type of a	ccess does your application need?	
	ut our Application Permission Model	
Read only		
Read and V	and the second	
Read, Write	and Access direct messages	
Note:		
	application permission model will only reflect in access tokens obtained af negotiate existing access tokens to after the permission level associated wi	



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

nCare

		Test OAuth
Details Settings Ke	ys and Access Tokens	Permissions
Application Setting	s	
Keep the "Consumer Secret	" a secret. This key sh	ould never be human-readable in your application.
Consumer Key (API Key)		
Consumer Secret (API Secre	et)	and the second
Access Level	Read and write (modify	(app permissions)
Owner	and the second second	
Owner ID		
Application Actio		Change App Permissions
4		
Your Access Token		
You haven't authorized this a	application for your ow	n account yet.
By creating your access toke your application's current pe		everything you need to make API calls right away. The access token generated will be assigned
Token Actions		

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.

nCare	тор	pology	Network Device	• 🔍 – s	ystem
dustry 4.0 Device & Network Health Manager	Users	Message	Database		
Message					
E-mail SMS	Social Media				
					1
	Twitter APP ID:				
	APP Secret:				
		Login			

Figure 247 Enter APP ID and APP Secret

(15) Click Authorize Program.

要授權 使用你的帳戶嗎?
此應用程式將可以: • 從您的時間軸上續取推文。 • 增衍關注了結並歸注新用戶。 • 夏新您的個人檔案 · 為你發後推文。
· 河小被冲滩人。 將無法: · 浮取你的私人訊意。 · 查看您的 Twitter 密碼。
你她听可以说「谈定」页面的 應用程式標施 中,撤销任何應用程式的存取種。 如果按磁站未偏應用程式,你的任何操作仍得得掉 Twitter 的服音信款 撤使做行。尤其,部分使用读说将音能得至與
Twitter分享。如滞详细演讯,适步规量型的通机政策。

Figure 248 Twitter Authorization Page

(16) A PIN code will pop-up.



Figure 249 Twitter PIN Code

(17) Enter the PIN code on nCare.

Appendix

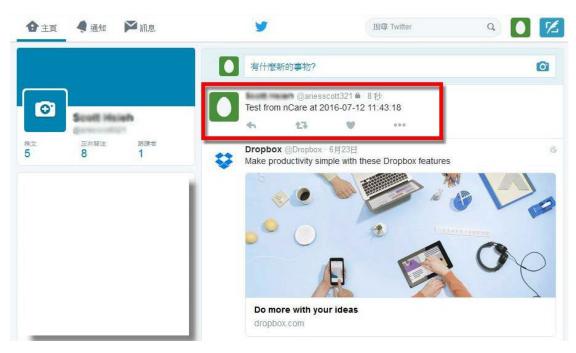
nCare

nCare Industry 40 Device & Network Manager	Topology Network Device Syste	m
Message	Users Message Database	
E-mail SMS	Social Media	
	Line Account: Password: Login	
	Twitter PIN Code Apply	
	Figure 250 Enter PIN Code	

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

sage		
mail SMS	Social Media	
	WeChat	
	APP ID: Corp ID:	
	Corp Secret:	
	Login	
	Line	
	Account:	
	Login	
	Twitter	
	Iwitter	

Figure 251 Send Twitter Test Message



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

Figure 252 Test Message Sent Successfully