

nCare 物聯網管理系統(V2.1.0)

User Manual

nCare 物聯網管理系統操作手冊

版權聲明

商標

免責聲明

技術支援與聯絡資訊

目錄

1. nCare 概述	1
2. nCare 環境說明	2
2.1. 作業系統需求	2
2.1.1. 伺服器端	2
2.1.2. 用戶端	2
2.2. 電腦硬體需求	2
2.3. 管理設備	2
3. nCare 安裝說明	3
3.1. nCare 安裝說明	3
3.2. nCare 解除安裝	3
3.3. 啟動 nCare	4
4. nCare 登入介面說明	5
4.1. 登入操作程序	5
5. nCare 系統(System)介面說明	7
5.1. 使用者管理(Users)	7
5.1.1. 帳號管理說明	7
5.1.2. 帳號管理操作	7
5.2. 訊息管理(Message)	10
5.2.1. 訊息管理說明	10
5.2.2. 訊息管理操作	10
5.3. 資料庫管理(Database)	16
5.3.1. 事件日誌管理說明	16
5.3.2. 事件日誌管理操作	16
5.4. DHCP 管理(DHCP)	17
5.4.1. DHCP 管理說明	17
5.4.2. DHCP 管理操作	17
5.5. IP 掃描(Scan IP)	20
5.5.1. IP 掃描說明	20
5.5.2. IP 掃描操作	20
5.6. 關於(About)	21
5.6.1. 許可證說明	21
5.6.2. 許可證操作	21
6. nCare 網路設備(Network Device)介面說明	24
6.1. 管理設備功能(Manage)	24
6.1.1. 設備列表(Device List)說明	24
6.1.2. 設備列表(Device List)操作	24
6.1.3. 設定備份(Config Backup)說明	40
6.1.4. 設定備份(Config Backup)操作	40

6.1.5. 設定還原(Config Restore)說明	41
6.1.6. 設定還原(Config Restore)操作	41
6.1.7. 韌體更新(Fw Upgrade)說明	43
6.1.8. 韌體更新(Fw Upgrade)操作	43
6.1.9. 設備配置(Device Provision)說明	45
6.1.10. 設備配置(Device Provision)操作	45
6.1.11. Modbus 設定檔(Modbus Profile)說明	46
6.1.12. Modbus 設定檔(Modbus Profile)操作	46
6.2. 日誌管理(Log)	48
6.2.1. 事件紀錄(Event Log)說明	48
6.2.2. 事件紀錄(Event Log)操作	48
6.2.3. 系統紀錄(System Log)說明	51
6.2.4. 系統記錄(System Log)操作	51
6.2.5. 告警回播(Playback)說明	51
6.2.6. 告警回播(Playback)操作	51
6.3. 使用流量(Usage)	54
6.3.1. 使用流量說明	54
6.3.2. 使用流量操作	54
6.4. 嚴重度(Severity)	57
6.4.1. 嚴重度說明	57
6.4.2. 嚴重度操作	57
6.5. 區隔期間(Interval)	58
6.5.1. 區隔期間說明	58
6.5.2. 區隔期間操作	58
6.6. 群組(Group)	59
6.6.1. 拓樸群組說明	59
6.6.2. 拓樸群組操作	59
6.7. 非法設備(Rogue AP/Device)	60
6.7.1. 非法設備說明	60
6.7.2. 非法設備操作	60
7. nCare 設備拓樸(Topology)介面說明	67
7.1. 拓樸圖(View)	67
7.1.1. 拓樸圖功能說明	67
7.1.2. 拓樸圖功能操作	67
7.2. 探索設備(Discovery)	100
7.2.1. 探索設備說明	100
7.2.2. 探索設備操作	100
7.3. 設備狀態(Status)	103
7.3.1. 設備狀態功能說明	103
7.3.2. 設備狀態功能操作	103
8. IoT Studio 介面說明	110
9. nCare 維護與管理	111

9.1. 存取控制	111
9.1.1. 使用者	111
9.1.2. 設備管理者	111
9.1.3. 系統管理者	112
9.2. 設備異常狀態	113
9.2.1. 同 IP 判斷	113
9.2.2. 同 Mac 判斷	114
9.2.3. 設備誤接成 Loop	115
10. 附件一	117

表目錄

表 1 伺服器端設備	2
表 2 用戶端設備	2
表 3 硬體需求	2
表 4 管理設備	2

圖目錄

圖 1 nCare 桌面捷徑	3
圖 2 nCare 解除安裝	3
圖 3 nCare 使用情境	4
圖 4 nCare 登入畫面	5
圖 5 登入語言選擇	5
圖 6 登入錯誤訊息	6
圖 7 登出系統	7
圖 8 新增使用者	7
圖 9 使用者權限	8
圖 10 使用者存取群組	9
圖 11 新增使用者	9
圖 12 新增使用者	9
圖 13 電子郵件測試	10
圖 14 簡訊測試	11
圖 15 簡訊測試訊息	11
圖 16 微信設定	12
圖 17 微信發送帳密設定	12
圖 18 微信發送測試	13
圖 19 微信測試訊息	13
圖 20 輸入推特帳密	14
圖 21 發送推特測試訊息	14
圖 22 測試訊息成功發送	15
圖 23 選擇警報通知對象	15
圖 24 設定警報通知對象	16
圖 25 資料庫設定	17
圖 26 進入設備 Interfaces 網頁	17
圖 27 選擇 LAN 或 WAN 介面	18
圖 28 設定設備的 Protocol	18
圖 29 填寫設備的主機名稱	19
圖 30 啟動 DHCP	19
圖 31 用戶列表	20
圖 32 填寫 IP 掃描起始位址	20
圖 33 IP 掃描資訊	21
圖 34 正版許可證期限	22
圖 35 試用版許可證期限	22
圖 36 跳出使用期限提示	23
圖 37 跳出過期提示	23
圖 38 查閱設備	24
圖 39 顯示或隱藏非法設備標誌	25
圖 40 增加設備	25
圖 41 新增設備的資訊	26
圖 42 設備種類選項	26
圖 43 通訊協定設定	27

圖 44 Trap 設定	27
圖 45 拓樸群組設定	28
圖 46 設定設備組態	28
圖 47 設備網頁帳密	29
圖 48 設備網頁資料	29
圖 49 MIB 瀏覽器功能	30
圖 50 MIB 瀏覽器設定畫面	31
圖 51 重置設備	31
圖 52 修改設備資訊	32
圖 53 無線網設定	32
圖 54 加密協定設定	33
圖 55 創建虛擬網路	33
圖 56 選擇 Bridge	34
圖 57 新增 Bridge	34
圖 58 選擇虛擬網路介面	35
圖 59 修改 NIO51 設備之無線網參數	35
圖 60 修改 NIO51 設備之 Serial/Modbus 參數	36
圖 61 修改 NIO50 之 Device Server 參數	36
圖 62 修改 IWSN Gateway 之 WirelessHART 參數 1	37
圖 63 修改 IWSN Gateway 之 WirelessHART 參數 2	37
圖 64 修改 IWSN Gateway 之 ISA100 參數 1	38
圖 65 修改 IWSN Gateway 之 ISA100 參數 2	38
圖 66 IPC 設備修改設定	39
圖 67 刪除設備資訊	39
圖 68 搜尋需備份的設備	40
圖 69 編輯設備備份的排程	40
圖 70 檢查備份列表	41
圖 71 檢查備份狀態	41
圖 72 搜尋需還原的設備	42
圖 73 選擇組態還原檔案	42
圖 74 確定組態還原	42
圖 75 還原錯誤訊息	43
圖 76 選擇需韌體更新的設備	43
圖 77 設定韌體更新的排程	44
圖 78 檢查韌體更新排程列表	44
圖 79 韌體升級結果	45
圖 80 設備配置設定	45
圖 81 選擇需要配置的設備	46
圖 82 填入 Modbus 設備型號與圖示	46
圖 83 填入 Modbus 設備掃描參數	47
圖 84 填入 Modbus 設備暫存器表	47
圖 85 查閱或修改 Modbus 設備參數	47
圖 86 事件日誌尋找記錄	48
圖 87 事件日誌資訊	48

圖 88 清除事件紀錄	49
圖 89 事件紀錄快捷功能	49
圖 90 事件記錄快捷嚴重層級	50
圖 91 選擇嚴重層級	50
圖 92 事件重播快捷鍵	50
圖 93 事件重現	50
圖 94 搜尋系統記錄	51
圖 95 修改告警回播的設定	51
圖 96 事件重播	52
圖 97 事件搜尋	52
圖 98 事件重播拓樸圖	53
圖 99 選擇監控設備與參數	54
圖 100 選擇折線圖的形式	54
圖 101 導出 Eth 數據	55
圖 102 導出 Wlan 數據	55
圖 103 導出 CPU 使用數據	55
圖 104 導出記憶體使用數據	56
圖 105 導出 NIO200 設備之流量	56
圖 106 導出 NIO51 設備之流量	57
圖 107 嚴重度事件列表	57
圖 108 嚴重度修改	58
圖 109 間隔期間設定	58
圖 110 拓樸群組新增	59
圖 111 拓樸群組列表	59
圖 112 掃描非法設備	60
圖 113 非法設備的資訊	60
圖 114 事件記錄顯示非法設備	61
圖 115 設備列表非法設備的警告標誌	61
圖 116 拓樸圖非法設備的警告標誌	62
圖 117 將設備加入白名單	62
圖 118 白名單列表	62
圖 119 新增白名單	63
圖 120 掃描白名單設備	63
圖 121 勾選白名單下的非法設備	64
圖 122 設定白名單下的非法設備	64
圖 123 載入非法設備設定	65
圖 124 非法設備設定已載入	65
圖 125 手動新增非法設備	65
圖 126 設定非法設備掃描週期	66
圖 127 nCare 拓樸圖	67
圖 128 拓樸圖功能鍵	67
圖 129 選取設備	68
圖 130 選取連線	68
圖 131 圈選設備	68

圖 132 新增連線	69
圖 133 新增設備	69
圖 134 掃描設備	70
圖 135 掃描不到新設備	70
圖 136 成功新增設備	70
圖 137 圈選群組	71
圖 138 設定群組	71
圖 139 檢視群組內設備	72
圖 140 移出群組	72
圖 141 選取歸納的設備	72
圖 142 選擇 WiFi 網段	73
圖 143 移出 WiFi 群組	73
圖 144 返回拓樸圖層	74
圖 145 刪除設備	74
圖 146 地圖	75
圖 147 連線流量顯示	75
圖 148 流量大連線則粗	76
圖 149 點選流量監測	76
圖 150 設定監測閥值	76
圖 151 開始監測	77
圖 152 連線超過閥值	77
圖 153 取消流量監控	78
圖 154 同時進行兩種流量監控	78
圖 155 顯示非法設備的警告	78
圖 156 選擇 VLAN	79
圖 157 顯示 VLAN 拓樸	79
圖 158 更新所有 IWF AP	80
圖 159 找不到 IWF AP 設備	80
圖 160 NIO200-HAG 設備之帳號設定	81
圖 161 填寫 NIO200-HAG 設備的帳號密碼	81
圖 162 NIO200-HAG 設備的帳號設定成功	81
圖 163 更新 IWSN	82
圖 164 掃描 NIO200-HAG 設備	82
圖 165 掃出 NIO200-HAG 之群組設備	82
圖 166 查閱 NIO200-HAG 群組設備	83
圖 167 NIO200-HAG 群組設備斷線	83
圖 168 NIO200-IAG 設備之帳號設定	84
圖 169 掃出 NIO200-IAG 的 ISA100 群組設備	84
圖 170 查閱 ISA100 的設備資訊	84
圖 171 設定 NIO200 系列設備之時區	85
圖 173 儲存拓樸	86
圖 174 重新載入拓樸	86
圖 175 更新 NIO50 設備	87
圖 176 設定 Modbus 編號訊息	87

圖 177 設定 Modbus 編號	88
圖 178 設定 Modbus 編號快捷鍵	88
圖 179 掃描 NIO50 設備	88
圖 180 NIO50 歸入 WiFi 群組	89
圖 181 WiFi 群組內的設備	89
圖 182 PLC 群組內的設備	90
圖 183 NIO50 設備資訊更新	90
圖 184 設定 Modbus 排程	91
圖 185 設定排程時間與週期	91
圖 186 即時更新 PLC 資料	92
圖 187 NIO51 的 PLC 群組	92
圖 188 查閱 NIO51 之 PLC 設備資訊	93
圖 189 編輯 NIO51 的 PCL 設備	93
圖 190 設備顏色警訊	93
圖 191 數字警訊	94
圖 192 乙太網路連線	94
圖 193 深綠色粗實線	94
圖 194 乙太線埠彙聚端口資訊	94
圖 195 Mesh 無線網路連線	95
圖 196 WiFi 連線	95
圖 197 網段內的設備	95
圖 198 灰色備援虛線	96
圖 199 細的紫色線	96
圖 200 粗的紫色線	96
圖 201 Vlan 端口資訊	97
圖 202 綠色連線	97
圖 203 綠色粗線	97
圖 204 紅色連線	98
圖 205 橘色連線	98
圖 206 設備快捷鍵	98
圖 207 Ping 功能	99
圖 208 重啟功能	99
圖 209 遠端桌面	100
圖 210 探索設備	100
圖 211 IP 位址記憶欄位	101
圖 212 不定範圍 CAPWAP 探索設備	101
圖 213 設定範圍 CAPWAP 探索設備	102
圖 214 探索進度	102
圖 215 顯示探索出的設備	102
圖 216 IWF 系列設備狀態	103
圖 217 IPC 系列設備狀態	103
圖 218 IPC 系列設備 WMI 功能	104
圖 219 IPC 系列設備 WMI 頁面	104
圖 220 PLC 設備歷史狀態	104

圖 221 編輯暫存器列表	105
圖 222 新增暫存器列表	105
圖 223 寫入暫存器資訊	106
圖 224 匯出設備狀態	106
圖 225 NIO51 的 PLC 設備狀態	106
圖 226 NIO200-HAG 的設備狀態	107
圖 227 NIO200-HAG 設備的 Run Command	107
圖 228 NIO200-IAG 的設備狀態	108
圖 229 NIO200-IAG 設備的 Run Command	108
圖 230 ISA100 Trouble Shooting 頁面	109
圖 231 IoT Studio 操作畫面	110
圖 232 系統使用者權限	111
圖 233 設備管理者權限	112
圖 234 系統管理者權限	112
圖 235 設備同 IP 的掃圖結果	113
圖 236 設備同 IP 的事件日誌	113
圖 237 設備同 Mac 的掃圖結果	114
圖 238 設備同 Mac 的事件日誌	114
圖 239 IP 掃描功能警告設備同 Mac	115
圖 240 設備誤接成 Loop 之警報	115
圖 241 設備誤接成 Loop 之事件日誌	116
圖 242 登入推特 Apps	117
圖 243 建立新程式	117
圖 244 填寫應用程式資訊	118
圖 245 取得應用程式資料	118
圖 246 選擇權限	119
圖 247 開通權限	119
圖 248 輸入 nCare 的推特帳密	120
圖 249 推特授權畫面	120
圖 250 授權 PIN 碼	121
圖 251 輸入 PIN 碼	121
圖 252 發送推特測試訊息	122
圖 253 測試訊息成功發送	122

1. nCare 概述

「nCare」是一套專門針對新漢股份有限公司無線網路及設備之關鍵應用而設計的網路管理系統，為使用者提供一個綜合性的管理平台，可以高效、即時、便利之形式監控、設置、維護重要的 IP 通訊網路，如工廠自動化系統。

「nCare」管理系統包含：設備管理、警示管理、效能管理、拓樸圖管理及系統管理，產品特點如下：

(1)自動探索與雲端管理功能

- 以 CAPWAP & LLDP & SNMP 管理 AP & CPE 層
- 並可以在系統中進行設備添加、編輯與刪除功能

(2)Visual Topology 視覺化拓樸圖功能

- 支援網狀網路和基礎結構拓樸圖

(3)AP 管理(AP Management)

- 配置與設定(Provisioning & configure)
- 組態備份與還原(Configuration backup & Restore)
- 回復原廠預設的值(Restore to factory default)
- 設備重置(Device Reset)
- 韌體更新(Firmware upgrade)
- 實用管理程序(Admin utility)

(4)系統報告與系統日誌

- 資產狀況管理(Asset Status)
- 匯出報告(Export)
- 系統日誌(System log)
- 使用量統計報告(Usage report)

(5)事件通知功能

- 觸發事件：可預先設定(Event trigger: Pre-defined)
- 外部警告通知(Outbound notice)

(6)使用者權限 (Administration)

- 通過用戶與密碼設置管理權限(Authority by username/password)
- 擴展權限(Scale up)

2. nCare 環境說明

2.1. 作業系統需求

2.1.1. 伺服器端

表 1 伺服器端設備

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

2.1.2. 用戶端

表 2 用戶端設備

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

2.2. 電腦硬體需求

表 3 硬體需求

設備	型式	規格
處理器	Intel(R) Atom(TM) CPU C2558	至少 2.40GHz
記憶體	DDR III	8GB
輸出入設備	Ethernet	1000Mbps
儲存設備	HDD	至少 75GB

2.3. 管理設備

表 4 管理設備

設備	型號
工業無線網路接取器	IWF300、IFW310
戶外無線網路接取器	IWF503、IWF504D、IWF6320、IWF6330
工業電腦	APPC1235、NISE105
Device Server	NIO50、NIO51
交換器	IGS-402SM-4PH24、IGS-402SM-8PH24、 IGS-1604SM
IWSN Gateway	NIO200(IAG、IDG、IDR、HAG、WMR)

3. nCare 安裝說明

3.1. nCare 安裝說明

- (1)請聯繫您的新漢銷售代理商，取得 nCare 軟體 CD 光碟或下載權限。取得 nCare 安裝包。確認您安裝 nCare 的伺服器需求，將軟體或光碟置入主機中。
- (2)請參考「nCare 物聯網管理系統快速安裝手冊」安裝 nCare。
- (3)安裝完成後，nCare 快捷鍵會被創立於桌面上。



圖 1 nCare 桌面捷徑

3.2. nCare 解除安裝

如果要刪除 nCare，請開啟「控制台」-「程式與功能」找到「nCare (remove only)」程式，點選「解除安裝/變更」，即可移除系統。

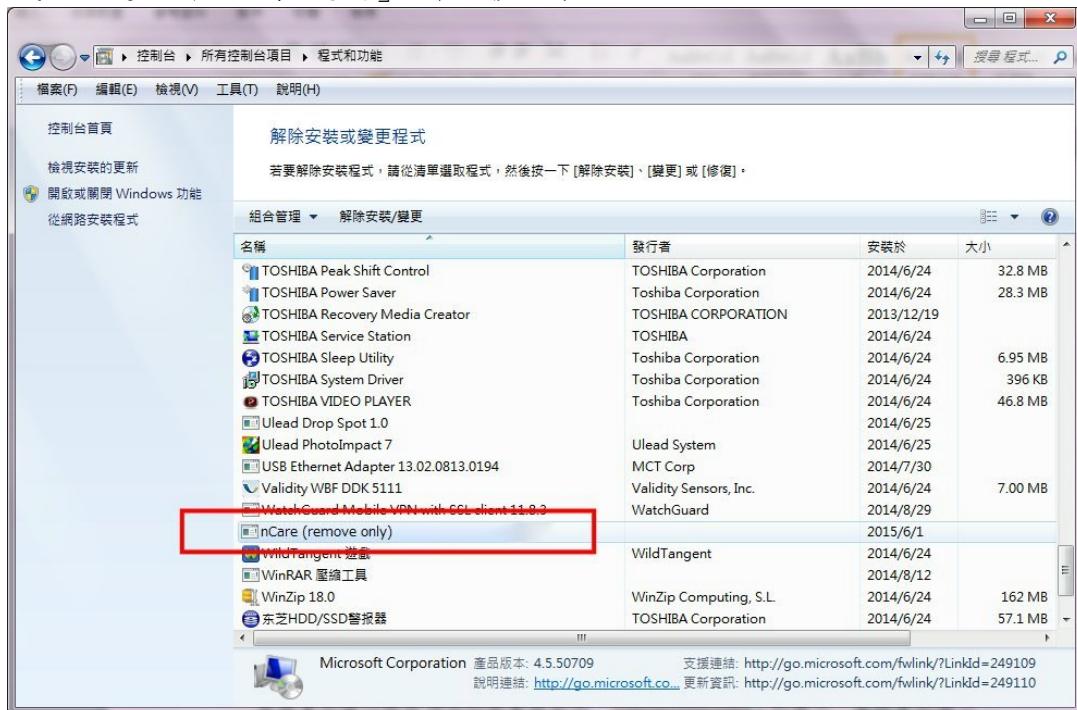


圖 2 nCare 解除安裝

3.3. 啟動 nCare

- (1)伺服器安裝 nCare 後，可使用 IE11、Firefox、Chrome 瀏覽器啟動。雙點擊 nCare 快捷圖示，進入系統登入頁面。
- (2)或是打開瀏覽器輸入網址：<https://localhost/>。即可進入登入頁面。
- (3)nCare 為 web-based 應用系統，一般使用者或系統管理員無須執行安裝程序，即可使用瀏覽器輸入網址:<https://x.x.x.x/>。「X.X.X.X」請填寫安裝系統的伺服器之 IP，透過有安裝 nCare 伺服器進入 nCare。
- (4)使用者若從新漢代理商取得含 nCare 系統之伺服器主機。系統預設 IP 為：「192.168.1.253」。subnet mask 為：「255.255.255.0」。網路線需接設備「lan0」。輸入以上資訊即可啟動 nCare，讓其他使用者以瀏覽器或 APP 連接使用。

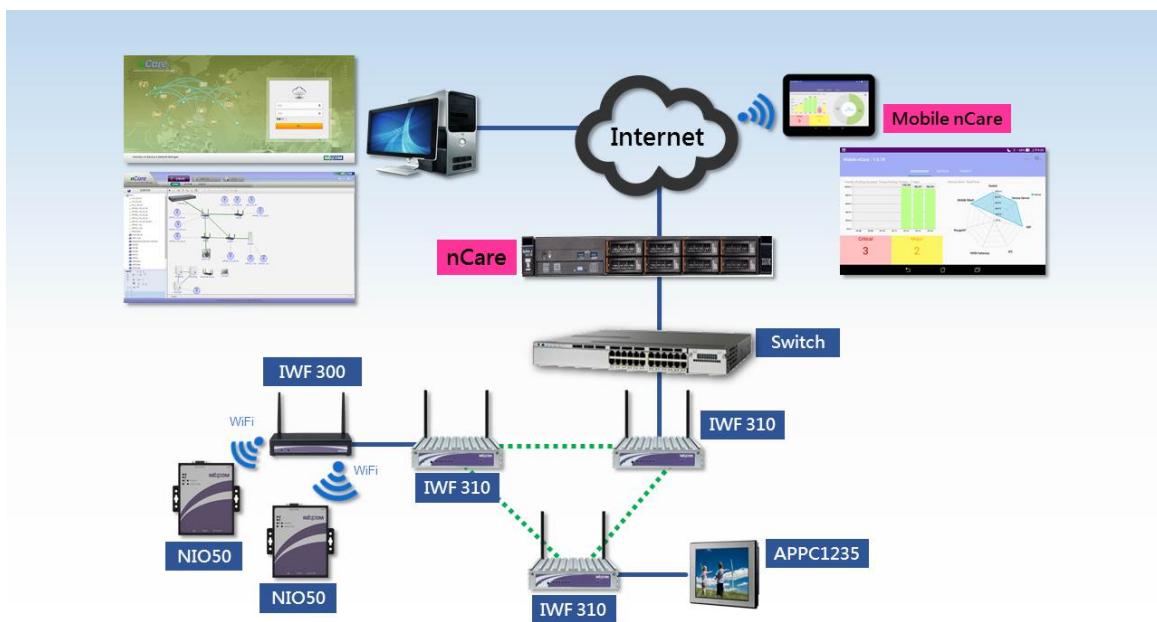


圖 3 nCare 使用情境

4. nCare 登入介面說明

4.1. 登入操作程序

(1)使用者透過網頁瀏覽器登入系統，如 IE11、Chrome、Firefox 登入系統。

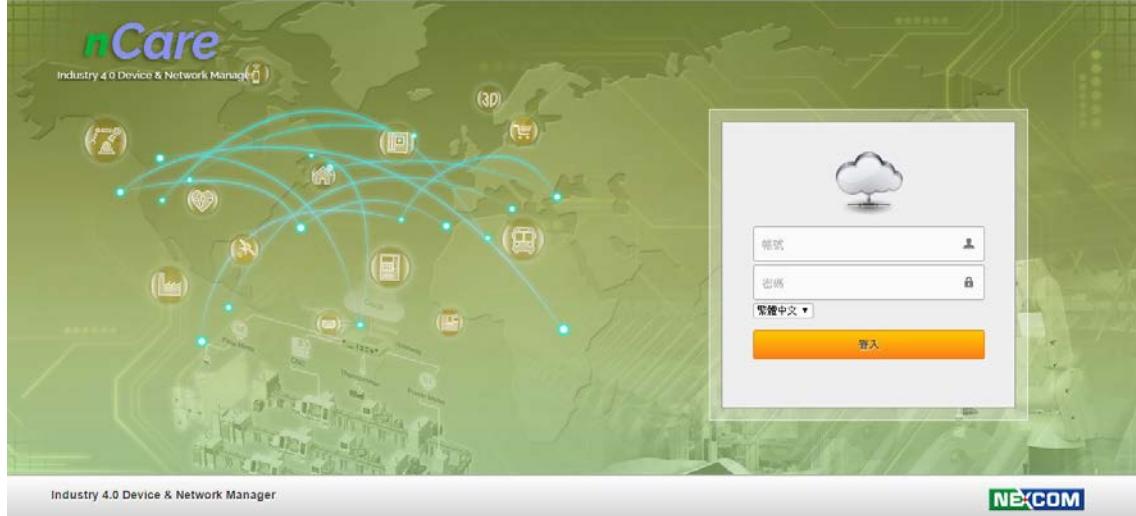


圖 4 nCare 登入畫面

(2)使用者可於「選擇語系」下拉選單中「英文」、「繁體中文」、「簡體中文」選擇適合之操作介面語系。



圖 5 登入語言選擇

(3)使用者輸入「帳號」、「密碼」，用戶帳號密碼設定請見 5.1 章節使用者管理。
第一次登入帳號、密碼皆為 admin。輸入錯誤時，系統以紅色驚嘆號提醒。

*當使用者密碼輸入錯誤超過三次，系統自動封鎖此帳號，需要聯繫系統管理員透過資料庫操作來解鎖。

命令如下：

- 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"



圖 6 登入錯誤訊息

(4)使用者登入後若閒置過久，將會自動登出系統。

(5)登入後可點選「登出」離開系統。

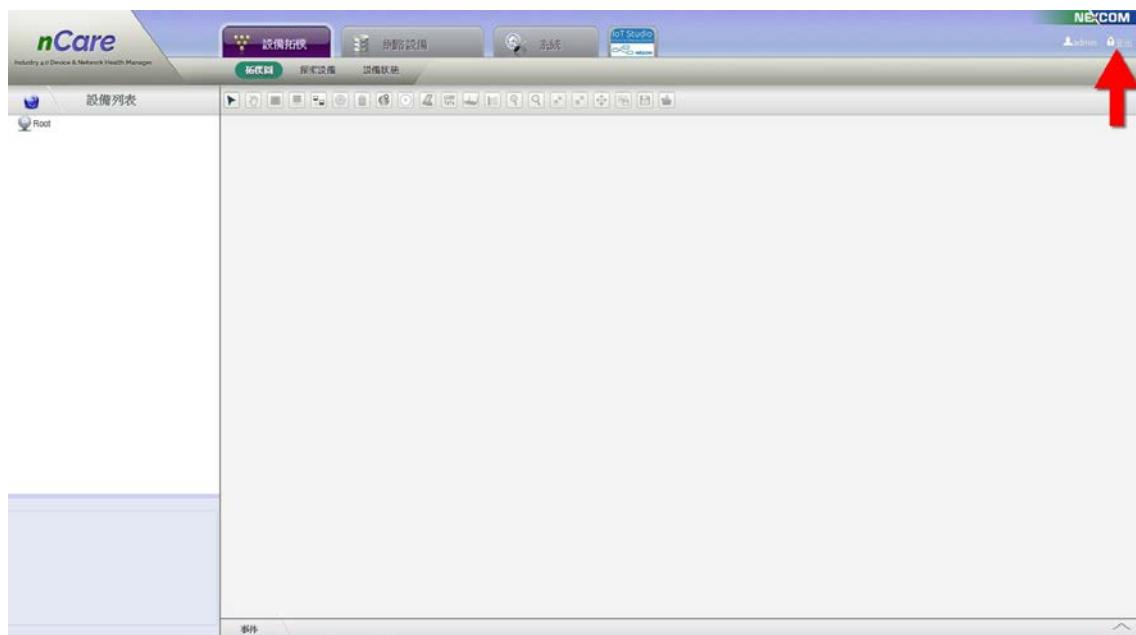


圖 7 登出系統

5. nCare 系統(System)介面說明

5.1. 使用者管理(Users)

5.1.1. 帳號管理說明

進入 nCare 主選單「系統」中之「使用者」頁面。管理者可管理登入系統的用戶，並設定其使用權限。

5.1.2. 帳號管理操作

(1)點選「帳號管理」頁面下方「新增」按鈕，跳出「建立使用者」視窗，即可填寫新增使用者的個人資料：名稱、密碼、確認密碼(可輸入數字、中英文字、不含特殊字元)、E-mail、手機號碼、存取層級、拓樸群組。

(2)填寫框格後方有紅色星號，表示必填資料。

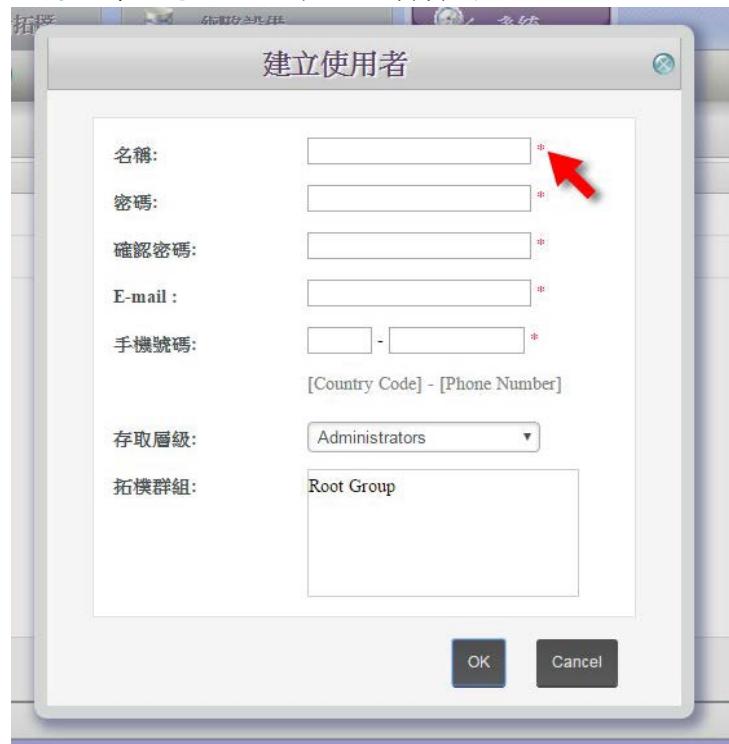


圖 8 新增使用者

(3)於「存取層級」下拉式選單中，選擇「Administrators」、「Managers」或「Users」之權限。

*系統管理者(Administrators)：系統管理者可存取系統的所有監控、設定、管理功能，並可建立或編輯使用者、重設使用者密碼等(詳細功能區分請參照 9.1.3 章節)。

*設備管理者(Managers)：設備管理者登入後除主選單「系統」之「使用者」：「帳號管理功能」無法使用之外，其餘皆與系統管理者的使用權限一致。(詳

細功能區分請參照 9.1.2 章節)。

*使用者(Users)：使用者僅可使用部分功能，如主選單無「系統」功能，主選單「網路設備」中，僅有「日誌」與「使用流量」功能。主選單「設備拓樸」中僅有「拓樸圖」、「設備狀態」，以及部分拓樸功能鍵可使用等。(詳細功能請參照 9.1.1 章節)。

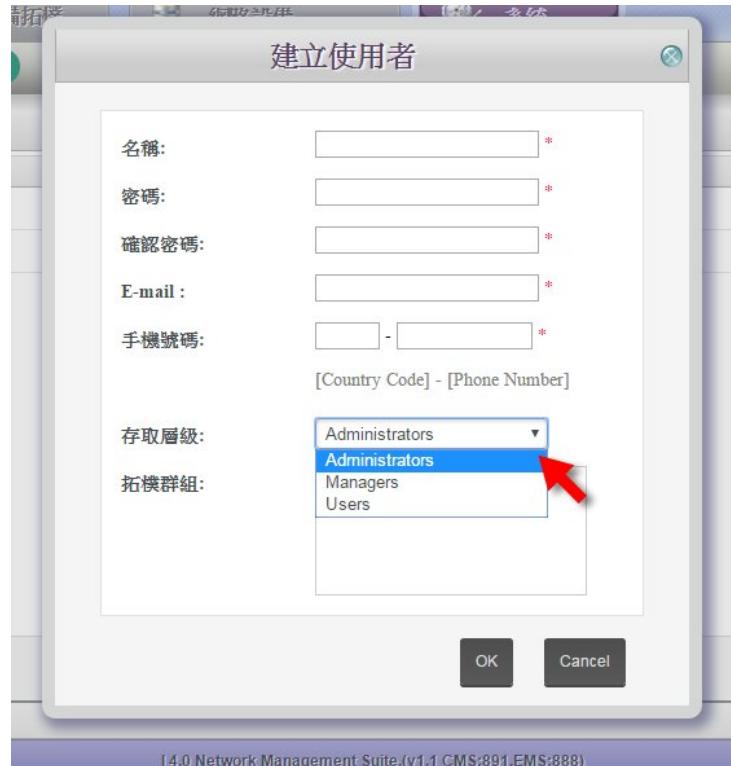


圖 9 使用者權限

(4)若設定「使用者(Users)」，可以進一步選擇要開放給他們管理或查閱的「拓樸群組」(群組設定請見 6.6 章節)。



圖 10 使用者存取群組

(5)點選「ok」，即彈出「新增成功」訊息，或以驚嘆號顯示錯誤項目，以滑鼠移至驚嘆號標誌上方，會說明錯誤資訊。

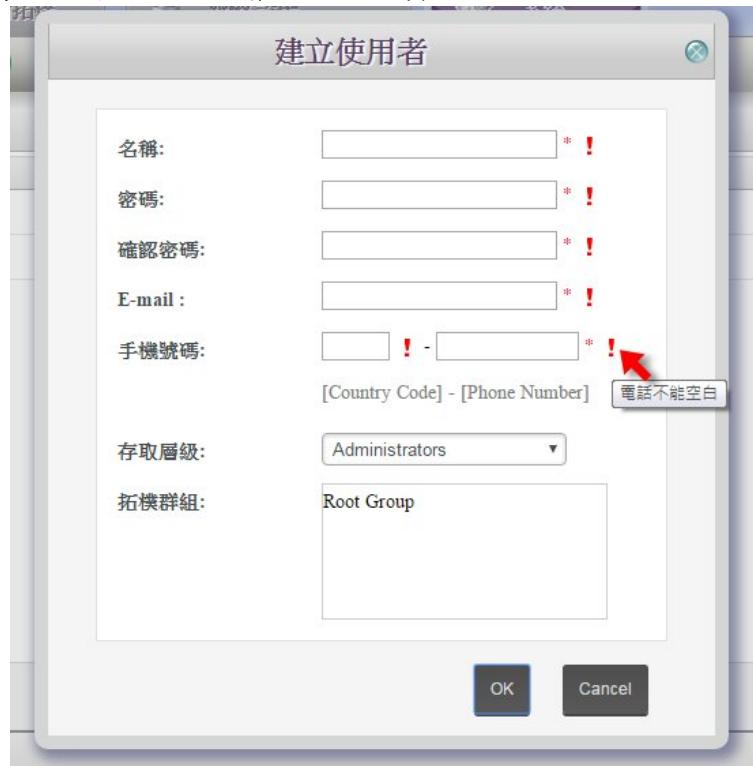


圖 11 新增使用者

(6)設定好之帳號顯示於頁面上，並可「修改」或「刪除」。

名稱	E-mail	手機號碼	存取層級	拓樸群組	修改	刪除
admin	account@	000-000000	Administrators	Root		
manager	manager@ii.org.tw	000-0000000000	Managers	Root		
user	user@ii.org.tw	000-0000000000	Users	Root		

圖 12 新增使用者

5.2. 訊息管理(Message)

5.2.1. 訊息管理說明

nCare 可於設備發出警報或連線流量超出閥值時，以「電子郵件/簡訊/社群媒體/通報使用者」發送警告訊息。也可針對嚴重警報與重要警報設定發送對象；連線流量的警報可選擇發送對象，詳細設定方式請見拓樸圖於 7.1.2.2 章節。

「訊息」功能頁面，可針對「電子郵件/簡訊/社群媒體」進行測試，讓管理者確認網管系統的警報功能是否能正常運作。

5.2.2. 訊息管理操作

5.2.2.1. 電子郵件

測試警告郵件是否正常，測試郵件將由有提供轉送服務公司或企業的郵件伺服器進行轉發，以下拉式選單選擇「服務提供」，再設定包含「SMTP 伺服器」、「SMTP 伺服器埠」、郵件伺服器的「郵件帳號」、「郵件密碼」欄位，填妥後點擊「修改設定」。並在「寄送目標」欄位中填寫測試者的郵件地址，點選「發送測試」按鍵，即可發送郵件信息至測試者的電子信箱中，已確認系統是否可正常發送郵件訊息給負責人。

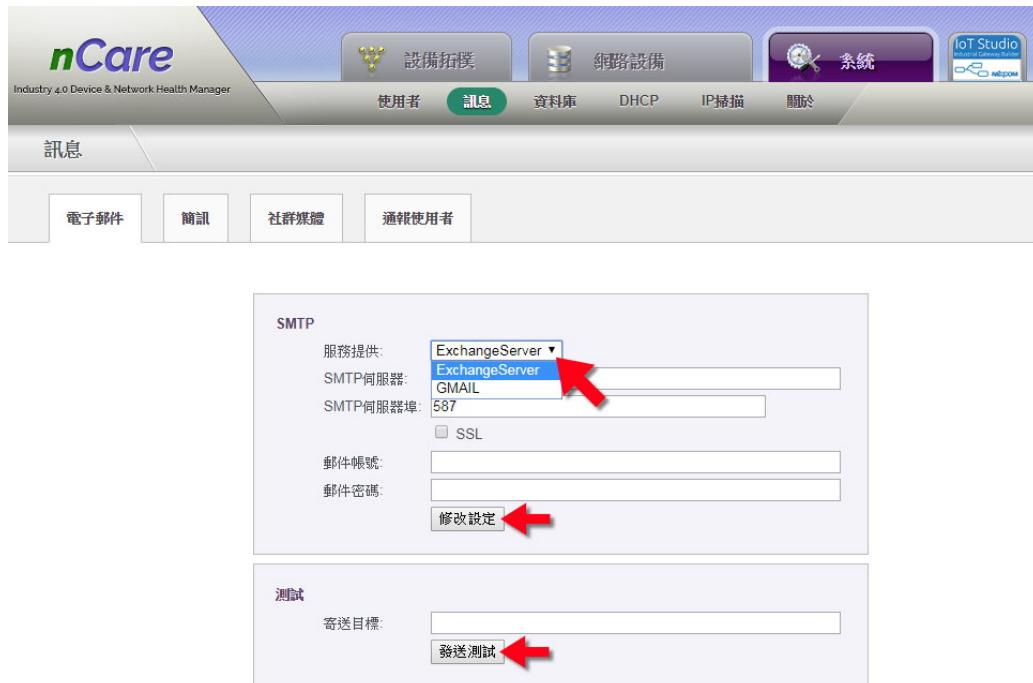


圖 13 電子郵件測試

5.2.2.2. 簡訊

(1)針對「簡訊功能」進行測試。系統測試者需事先取得企業內部簡訊發送系統的「服務提供」、「API ID」、「使用者」名稱、「密碼」，點擊「修改設定」。



圖 14 簡訊測試

(2) 設定完成後，填寫「國碼」、「手機號碼」欄位，點選「發送測試」，系統將發送訊息至手機中，即可確認系統是否可正常發送短訊給設備負責人。

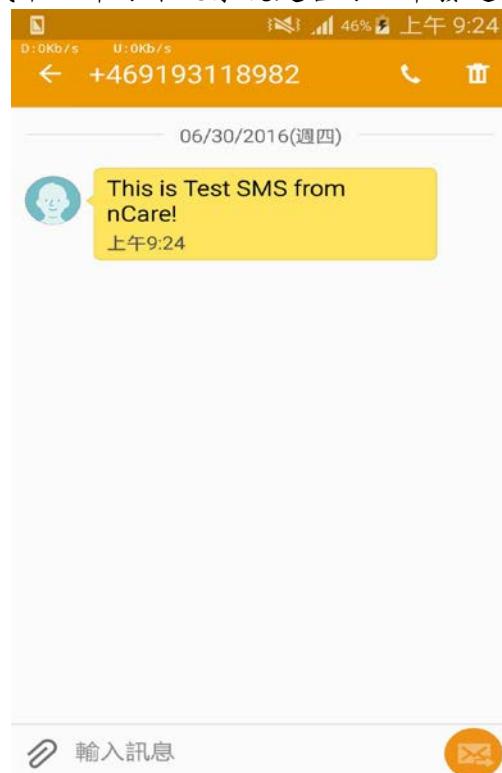


圖 15 簡訊測試訊息

5.2.2.3. 社群媒體

nCare 可針對社群媒體「微信」、「推特」、發送警報訊息，以下為設定說明。

(1)微信：

- a.申請個人微信帳號。
- b.關注「上海統漢信息科技」，關注後，將會產生「nCare」和「企業小助手」兩個關注目標。

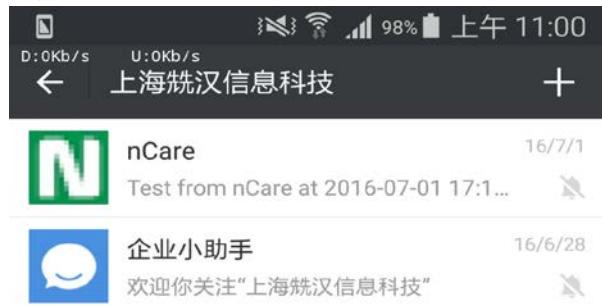


圖 16 微信設定

- c.向「上海統漢信息科技」申請發訊息的「應用程式編號」、「管理編號」和「管理密鑰」。填入後點選「登入」。



圖 17 微信發送帳密設定

- d.登入後系統產生 nCare 的 logo。點選「測試」發送訊息給微信帳號。



圖 18 微信發送測試

e. 發送後，微信 app 中的 nCare 關注目標，出現新訊息的紅點。點開後可看見測試訊息。

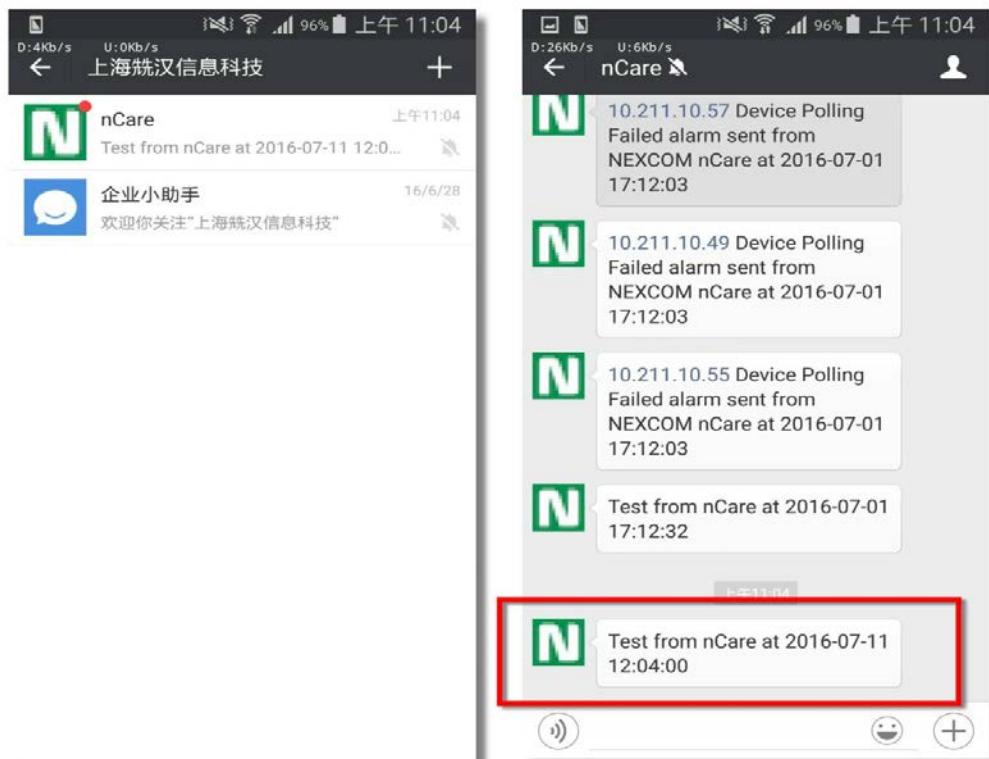


圖 19 微信測試訊息

(2)推特：

- a.申請個人推特帳號。
- b.進入Twitter Apps中建立新程式「Create New App」，取得應用程式編號「Consumer Key」與應用程式密鑰「Consumer Secret」，並輸入nCare欄位中(詳細申請方式請見附件一)。



圖 20 輸入推特帳密

c.點擊登入後，需再填入授權碼，完成登入動作。

d.點擊「測試」，發送測試訊息至推特中。



圖 21 發送推特測試訊息

d. 測試訊息成功發送至推特中。

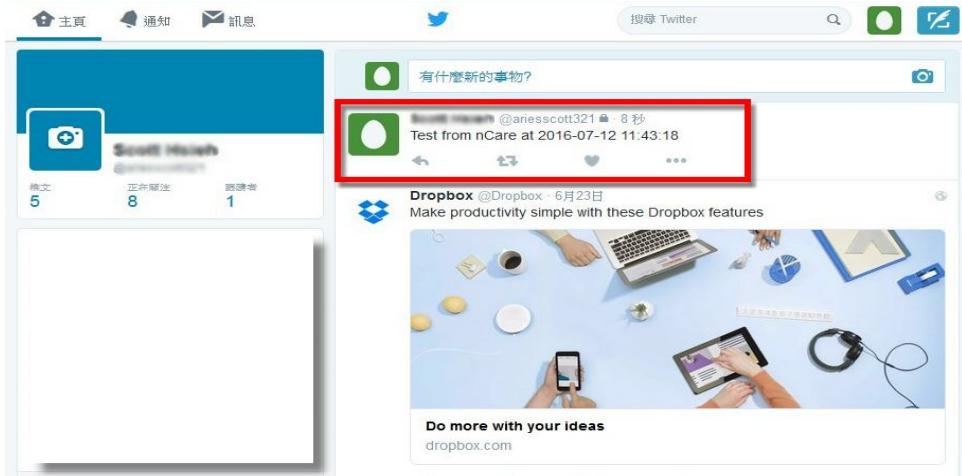


圖 22 測試訊息成功發送

5.2.2.4. 通報使用者

nCare 可指定「嚴重警報(Critical)」與「重要警報(Major)」的電子信箱(Email)或簡訊(SMS)訊息要發送的對象。

(1) 以下拉式選單選擇警報的嚴重度(Critical、Major)，以及通報類型(Email、SMS)，再勾選要「通報的使用者」(可複選)。



圖 23 選擇警報通知對象

(2)點選「修改設定」，即可完成設定。



圖 24 設定警報通知對象

5.3. 資料庫管理(Database)

5.3.1. 事件日誌管理說明

nCare 的資料庫可記錄設備如輪詢失敗、斷線之異常事件，並可指定事件紀錄在資料庫中保留的週期或數量上限，也可以手動清除所有的紀錄。

5.3.2. 事件日誌管理操作操作

- (1)勾選「最大保留事件週期」，填寫介於 1~365 之數字，點擊「修改設定」完成。如填選 180，則系統將每 180 天刪除舊的事件紀錄。
- (2)勾選「最大事件數量」，填寫 10000~1000000 之整數數字，點擊「修改設定」完成。如填寫 1000000，系統將每累積至 1000000 筆，即刪除舊的事件紀錄。
- (3)可複選，或兩項都不勾選，兩項皆不勾選則系統會持續累積事件紀錄。
- (4)點擊「刪除所有事件」，則儲存之所有事件紀錄都會被刪除。



圖 25 資料庫設定

5.4. DHCP 管理(DHCP)

5.4.1. DHCP 管理說明

由 nCare 內建之 DHCP 功能，自動為用戶端設備分配 IP 位址，使管理者大量部署設備至系統中，省去設備逐一設定 IP 位址、子網路遮罩及閘道器等資訊。

5.4.2. DHCP 管理操作

5.4.2.1. DHCP 設定

(1)取得設備後，先將設備連接上 nCare，並進入設備網頁進行 IP 設定。點擊設備網頁主選單的 Network，進入 Interfaces 頁面中。

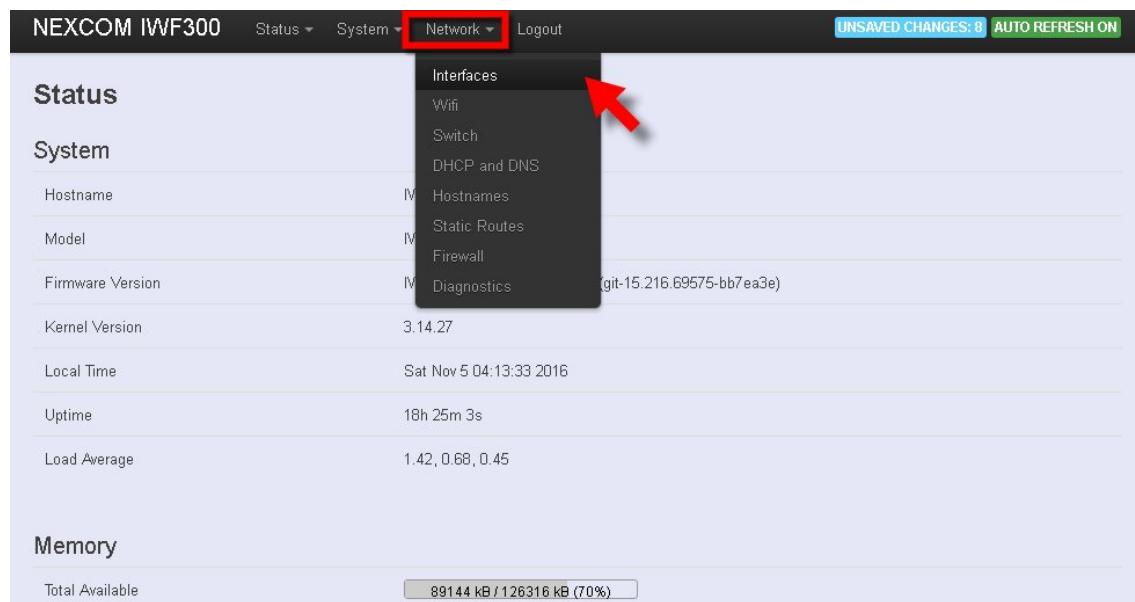


圖 26 進入設備 Interfaces 網頁

(2)依照需求選擇將設備設定為 LAN 或 WAN 的網路介面，再點擊「Edit」進入設定。

Interfaces

Interface Overview

Network	Status	Actions
LAN	Uptime: 20h 32m 10s MAC-Address: 00:10:F3:30:8B: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: 00:00:00:00:00:00 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 options

IPv6 ULA-Prefix: fdb2:26bc:7614::/48

圖 27 選擇 LAN 或 WAN 介面

(3)下拉式選單設定設備的 Protocol 為 DHCP client。

br-lan

Status	Uptime: 20h 38m 14s MAC-Address: 00:10:F3:30:8B:6F RX: 11.30 MB (174761 Pkts.) TX: 8.38 MB (73345 Pkts.) IPv4: 10.211.10.72/24
Protocol	Static address Static address DHCP client (highlighted) Unmanaged PPP PPTP PPPoE PPPoATM UMTS/GPRS/EV-DO L2TP
IPv4 address	<input type="text"/>
IPv4 netmask	<input type="text"/>
IPv4 gateway	<input type="text"/>
IPv4 broadcast	<input type="text"/>
Use custom DNS servers	<input type="text"/>
IPv6 assignment length	disabled <small>Assign a part of given length of every public IPv6-prefix to this interface</small>
IPv6 address	<input type="text"/>

圖 28 設定設備的 Protocol

(4)在「Common Configuration」頁面，填寫「Hostname to send when requesting DHCP」名稱。最後點擊「Save & Apply」完成設定。

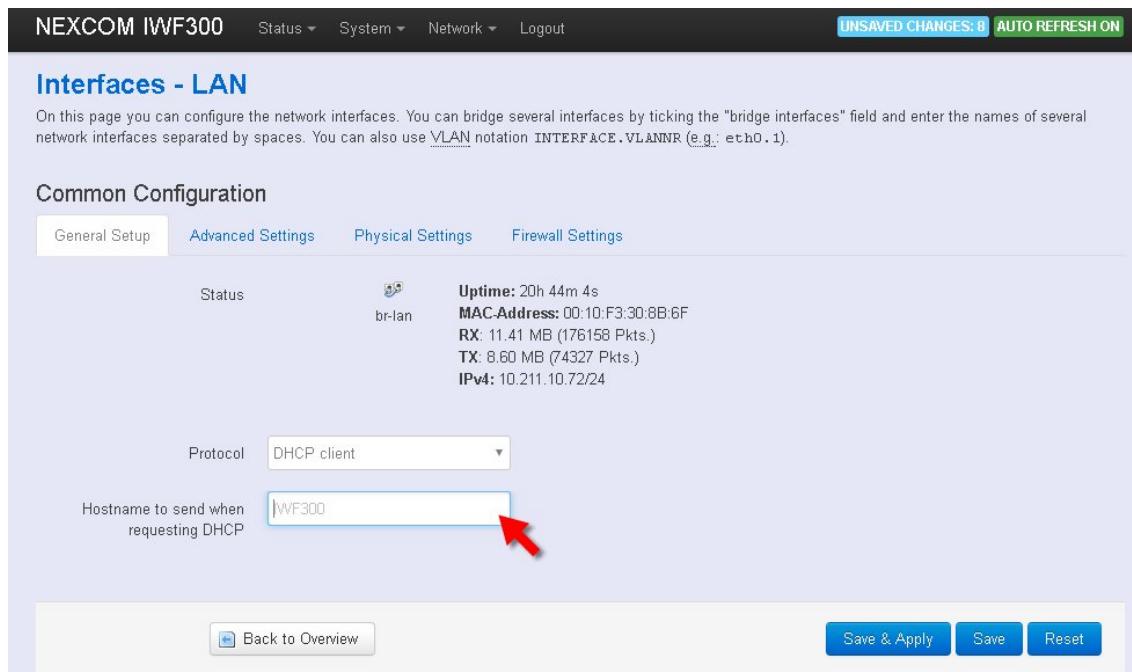


圖 29 填寫設備的主機名稱

(5)每一台要使用 DHCP 設定的設備，都以上述步驟設定完成後，打開 nCare 進入 DHCP 的「設定」畫面，勾選「啟動」，並填寫相關資訊，點擊「修改設定」，亦可新增實體位址(MAC)，綁定用戶 IP。



圖 30 啟動 DHCP

5.4.2.2. DHCP 用 戶 列 表

前一個步驟設定好後，在「用 戶 列 表」頁面即可搜尋到 DHCP 主動為設備配置好 IP 位址。

伺服器IP	實體位址	名稱	自動配置日期	到期日
192.168.1.10	00:10:F3:30:8B:6F	IWF300	2016-11-09 17:39:35	2016-11-09 18:00:16

圖 31 用 戶 列 表

5.5. IP 掃描(Scan IP)

5.5.1. IP 掃描說明

nCare 之 IP 掃描功能可快速判斷 IP 位址是否有設備正在使用。讓管理者查閱設備部屬的情形。

5.5.2. IP 掃描操作

(1)填寫要 nCare 掃描的「起始 IP 位址」與「結束 IP 位址」，並點選「掃描」。

圖 32 填寫 IP 掃描起始位址

(2)nCare 掃描後，即呈現前述填寫 IP 範圍內，有被使用的 IP 位址，及其 MAC 位址資訊。

IP位址	MAC位址
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
10.211.10.47	00:10:f3:36:f1:c3
10.211.10.50	00:10:f3:36:f1:45

圖 33 IP 掃描資訊

5.6. 關於(About)

5.6.1. 許可證說明

進入 nCare 主選單「系統」中「關於」頁面，可查閱安裝之 nCare 型號、版本、被授權使用之期限、可納管的設備數量與目前已經納管的設備數量。

(1)nCare 之試用版許可證會自動判斷使用者使用 nCare 的時間，而非“安裝”nCare 的時間。

(2)使用試用版的許可證操作 nCare，操作滿 24 小時即扣掉一天的權限。

5.6.2. 許可證操作

(1)許可證區分為試用版(試用 30 天)與正版(永久使用)。



圖 34 正版許可證期限

(2)試用版的許可證，會於此頁面的狀態中顯示可使用的天數。



圖 35 試用版許可證期限

(3) 許可證剩三天期限時，系統會主動在使用者登入時，跳出提示。

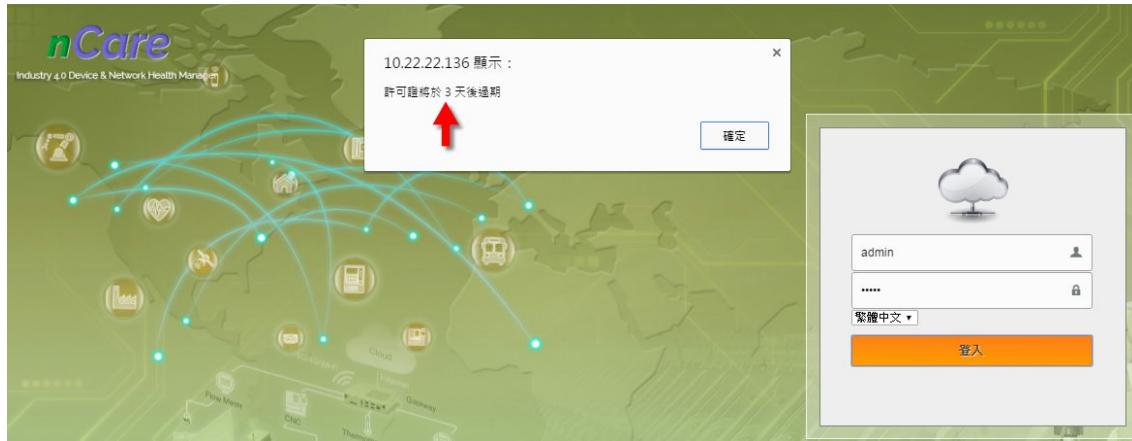


圖 36 跳出使用期限提示

(4) 許可證過期後，使用者將無法登入，且系統會跳出提示視窗。



圖 37 跳出過期提示

6. nCare 網路設備(Network Device)介面說明

6.1. 管理設備功能(Manage)

「管理設備」功能包含「設備列表(Device List)」、「設定備份(Config Backup)」、「設定還原(Config Restore)」、「韌體更新(Fw Upgrade)」、「設備配置(Device Provision)」與「Modbus 設定檔(Modbus Profile)」功能。可管理設備相關資訊、進行設備的設定備份與還原管理、設備韌體更新、為大量的設備部署相同配置設定值、建立 Modbus 檔案資訊等功能。

6.1.1. 設備列表(Device List)說明

設備列表頁面可新增、修改、刪除納管之設備。頁面中可根據設備類型顯示「設備名稱」、「IP 位址」、「設備種類」、「SSID」、「加密協定」、「經緯度」等資料，並可進入設備設定頁面進行相關操作設定或重啟設備。

6.1.2. 設備列表(Device List)操作

6.1.2.1. 查閱設備

(1)頁面左方點選「設備種類」如「IWF」、「Mobile Mesh」、「Device Server」、「IWSN Gateway」、「IPC」、「3rd-party AP」、「Switch」或「Others」查閱設備資料。

設備種類	編號	設備名稱	IP位址	設備種類	SSID	模式	加密協定	頻道	訊度	經度	網真	Mibrowser	重啟	修改	刪除
IWF	00:0e:8e:67:5b:ad	IWF300-83	10.211.10.63	IWF	IWF300_11N_2G_83	ap	psk2	6	0	0					
	00:10:03:5e:28:57	IWF310-44	10.211.10.44	IWF	IWF310_11N_2G_44	ap	psk2	11	0	0					
Mobile Mesh	00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	IWF	IWF300_11N_2G_46	ap	psk2	11	0	0					
Device Server	00:0e:8e:67:5f:a5	IWF300-64	10.211.10.64	IWF	IWF300_11N_2G_64	ap	psk2	11	0	0					
IWSN Gateway	10.211.10.43	IWF300-43	10.211.10.43	IWF	IWF300_11N_2G_43	ap	psk2	11	0	0					
					IWF300_11A_5G_43	ap	psk2	36	0	0					

圖 38 查閱設備

(2)可勾選「顯示/隱藏非法設備」，勾選顯示標記後，若設備為非法設備，則設備列表的編號旁上會出現驚嘆號⚠的警告圖示(非法設備設定與排除請見 6.7 章節)。



圖 39 顯示或隱藏非法設備標誌

6.1.2.2. 新增設備

(1)點擊頁面下方「新增」增加設備。



圖 40 增加設備

(2)跳出子視窗，可填寫設備資訊。包含「設備種類」、「通訊協定」、「Trap 設定」、「Syslog」、「設備名稱」、「IP 位址」、「讀取共同碼」、「寫入共同碼」、「拓樸群組」、「緯度」、「經度」。欄位後方有紅色星號者，為必填資料。



圖 41 新增設備的資訊

(3)新增設備時，「設備種類」可選擇「IWF」、「Mobile Mesh」、「IWSN Gateway」、「Device Server」、「IPC」、「3rd-party AP」、「Switch」或「Others」。

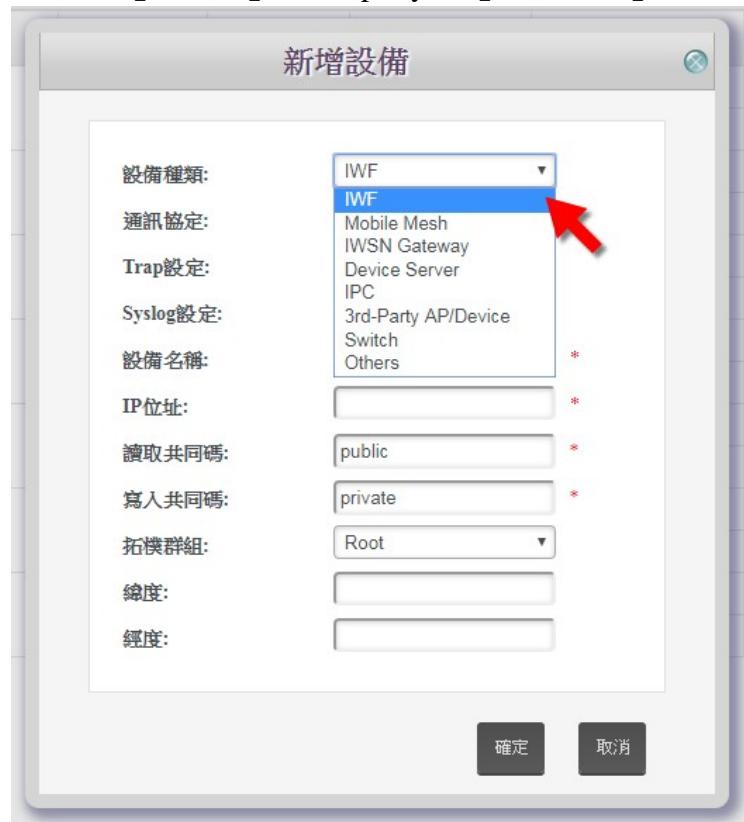


圖 42 設備種類選項

(4) 系統會根據設備類型選擇通訊協定，若無法判讀則以下拉式選單選擇「SNMP」、「Modbus」、「Python」協議。

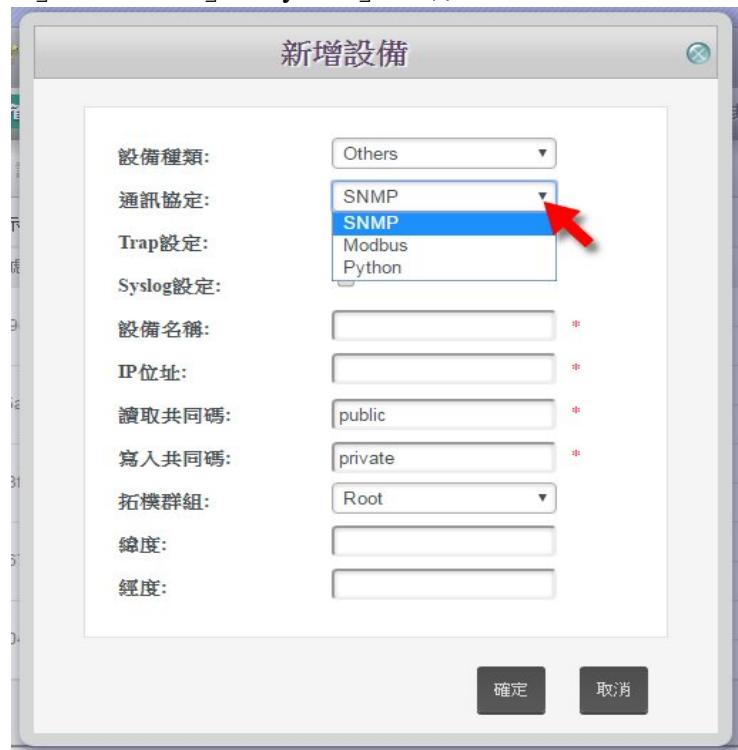


圖 43 通訊協定設定

(5) 勾選「Trap 設定」、「Syslog 設定」讓系統可自動幫新增的設備設定相關的數值，讓設備可主動發送 Trap 或變動狀態給系統。



圖 44 Trap 設定

(6) 「拓樸群組」可選擇此設備所屬的拓樸群組。拓樸群組名稱建立請見第 6.6 章節。

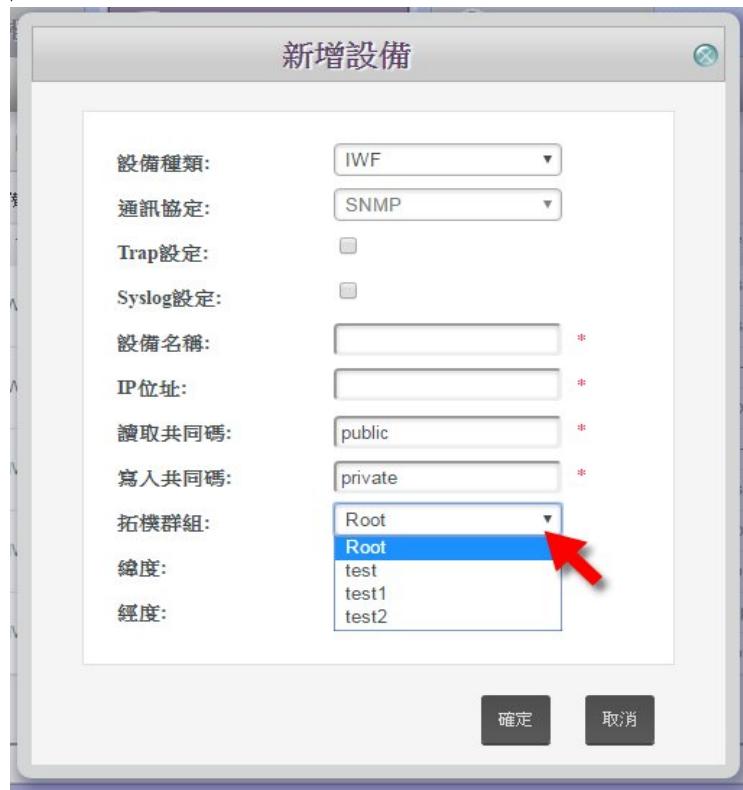


圖 45 拓樸群組設定

6.1.2.3. 設定設備組態

(1) 設備類型為「IWF」、「Mobile Mesh」、「Device Server」、「IWSN Gateway」、和「Switch」者，可點選欄位  可進入該設備的設定網頁，進行組態設定。

編號	設備名稱	IP位址	設備種類	SSID	模式	加密協定	頻道	強度	網真	Mibrowser	重啟	修改	刪除
00:0e:8e:67:5b:ad	IWF300-63	10.211.10.63	IWF	IWF300_11N_2G_63	ap	psk2	6	0	0				
00:10:13:5e:28:57	IWF310-44	10.211.10.44	IWF	IWF310_11N_2G_44	ap	psk2	11	0	0				
00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	IWF	IWF300_11A_5G_mesh	mesh	none	36	0	0				
00:0e:8e:67:5f:a5	IWF300-84	10.211.10.64	IWF	IWF300_11N_2G_64	ap	psk2	11	0	0				
10.211.10.43	IWF300-43	10.211.10.43	IWF	IWF300_11A_5G_04	ap	wpa	48	0	0				
				IWF300_11N_2G_43	ap	psk2	11	0	0				
				IWF300_11A_5G_43	ap	psk2	36	0	0				

圖 46 設定設備組態

(2)組態設定：進入設備網頁需輸入帳號、密碼，填寫後點擊登入(Login)。

NEXCOM IWF300

Authorization Required

Please enter your username and password.

Invalid username and/or password! Please try again.

Username

Password

Powered by LuCI (git-16.060.65840-1d56267) / OpenWrt (EU) v0.1.2

圖 47 設備網頁帳密

(3)進入設備網頁可查閱設備狀態，並進行相關設定。

NEXCOM IWF300 Status System Network Logout

Status

System

Hostname	IWF300
Model	Atheros DB120 reference board
Firmware Version	OpenWrt (EU) v0.1.2 / LuCI (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%)

圖 48 設備網頁資料

6.1.2.4. 由 Mibbrowser 設定設備

- (1)點選欄位  「MIB 瀏覽器」即跳出 MIB 瀏覽視窗，可查閱設備 MIB 資訊或進行參數設定。



圖 49 MIB 瀏覽器功能

- (2)MIB 瀏覽器主功能為：

-  「載入 MIB 檔案」：可由使用者端載入 MIB 檔案。
-  「Get」：由左方點選節點，再點擊 Get，可呈現設備節點資料。
-  「Set」：由左方點選節點，再點擊 Set，可設定設備節點參數。
-  「Get Next」：點擊 Get Next，可主動跳至下一個節點，並呈現資訊。
-  「Walk」：點擊群組的第一個節點，再點擊 Walk，會依序呈現整個群組節點的資訊。
-  「Table」：點擊節點後，再點擊 Table，可跳出設備「SNMP Table」視窗供管理者查閱。
-  「Clear」：點擊 Clear 可清除 Query Result。

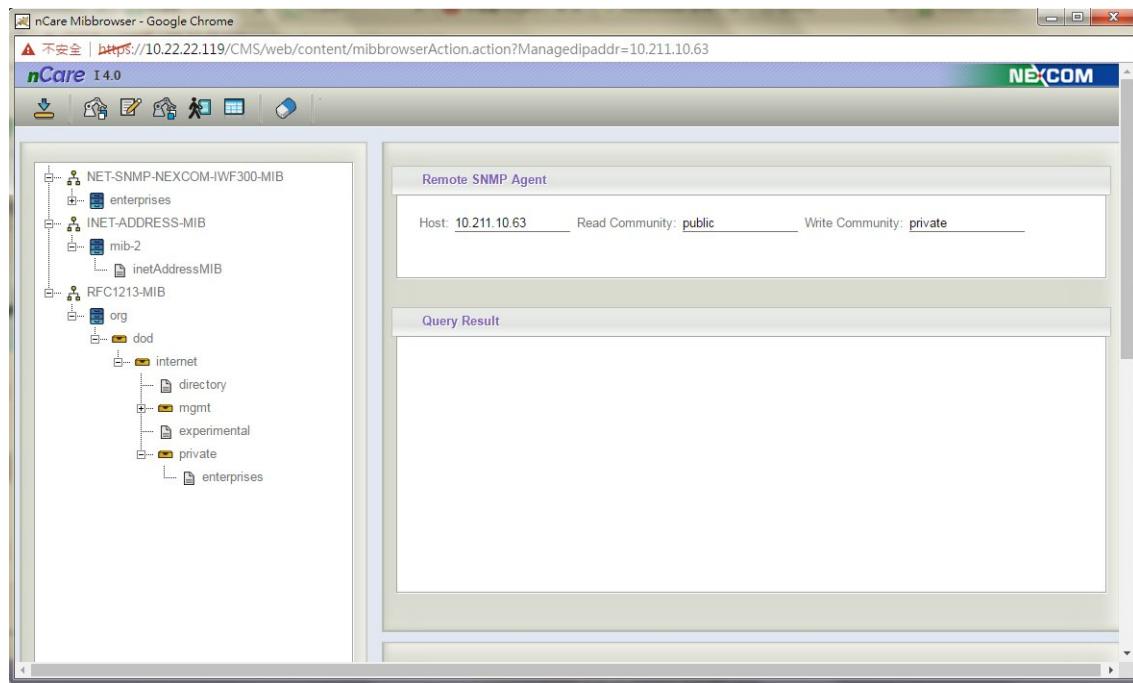


圖 50 MIB 瀏覽器設定畫面

6.1.2.5. 重置設備設定

(1) 點選欄位「重啟」可將設備重新開機。



圖 51 重置設備

6.1.2.6. 修改設備資訊

(1) 點選欄位「修改」可修改設備於列表上的資訊(Mobile Mesh 類型的設備無法使用此功能鍵，有修改需求請由「網頁」進入設備網頁修改)。



圖 52 修改設備資訊

(2)IWF 系列設備，點擊修改設備資訊，除了一般資料的頁籤外，還有「無線網」和「虛擬區域網路」頁籤可以修改設定。「無線網」頁籤包含「無線頻道」、「工作頻率」、「無線加密」等設定。



圖 53 無線網設定

(3) IWF 系列設備的「無線網」頁籤中「無線加密」設定，包含「WPA-EAP」、「WPA2-EAP」等加密協定設定。



圖 54 加密協定設定

(4) 「虛擬區域網路」可對不同的實體區域網路中的裝置進行邏輯分群管理，也就是可協助設備分割 Lan，根據需求進行 Vlan 劃分，以下為操作方式。

a. 首先，先從乙太網路創建虛擬網路的辨識碼(VLAN ID)，方便訊號辨認虛擬網路。輸入或以下拉式選單選擇「VLAN ID」、「VLAN Name」，以及選擇要開通的連接埠(Port)，點擊「新增 Vlan」則可創建。或刪除已經創建好的虛擬網路。



圖 55 創建虛擬網路

b. 設定設備的虛擬橋接網路(Bridge)，以下拉式選單選擇橋接網路，讓橋接器知道此設備為此虛擬網域的成員。

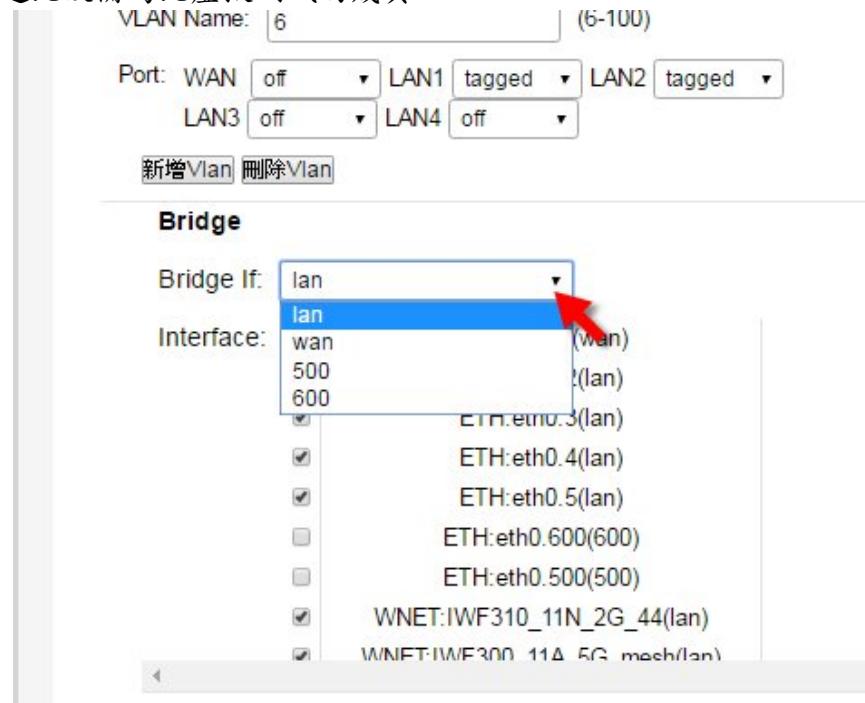


圖 56 選擇 Bridge

c. 或是點擊創建橋接網路「新增 Bridge(網頁)」nCare 將引導使用者進入設備的 web 介面進行橋接網路的創建，創建後再點擊「重新整理」，即可於 Bridge If 下拉式選單中找到新創建的橋接名稱。點擊「刪除 Bridge」則是可刪除已經創建好的橋接網段。



圖 57 新增 Bridge

d. 設定設備的網路介面(LAN Interface)。根據上一個步驟，會顯示不同的虛擬網路介面名稱，以勾選的方式，選擇設備訊號要通過的介面，再點「套用」提交設定。



圖 58 選擇虛擬網路介面

(5) Device Server 系列設備之 NIO51 模組的修改頁面，除了一般資料設定外，還有「無線網」及「Serial/Modbus」頁籤。

a. 「無線網」頁籤可設定如「無線頻道」、「工作頻率」或「無線加密」參數。



圖 59 修改 NIO51 設備之無線網參數

b. 「Serial/Modbus」頁籤則可針對「串列埠配置」和「TCP」做設定。



圖 60 修改 NIO51 設備之 Serial/Modbus 參數

(6)Device Server 系列之 NIO50 設備的修改頁面，除了一般資料設定外，則會有「Device Server」頁籤，可針對「WiFi AP Configuration」、「Serial Port Configuration」、「Data Flow Configuration」做設定。

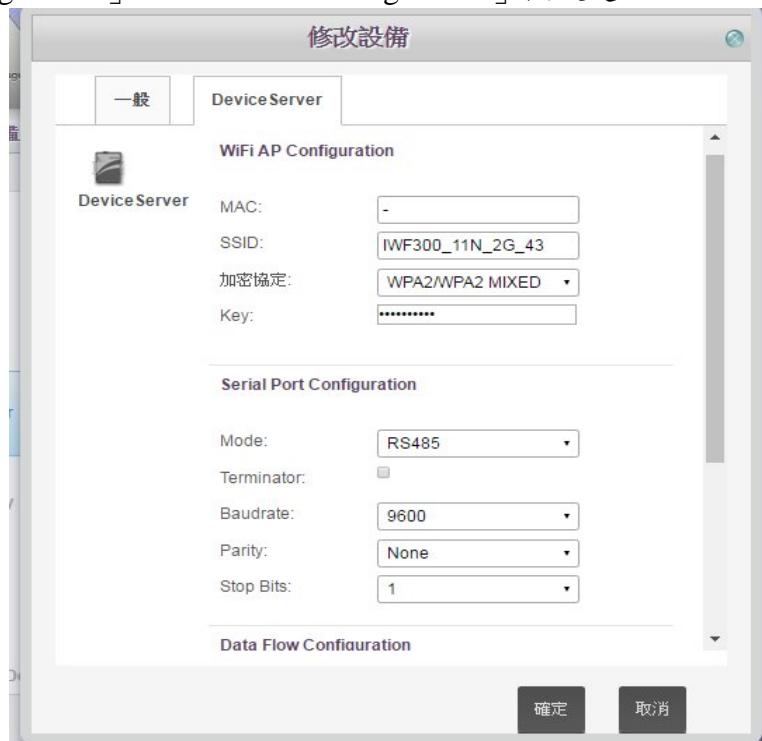


圖 61 修改 NIO50 之 Device Server 參數

(7) IWSN Gateway 系列的「NIO200-HAG」設備修改設備資訊，除了「一般資料」及「無線網」頁籤可設定之外，還有「WirelessHART」頁籤可以設定。

a.「WirelessHART」頁籤可設定「Access Point」、「Gateway」、「Network Manager」參數，填入參數後按「儲存」，並點擊「重新啟用」使新的設定生效。

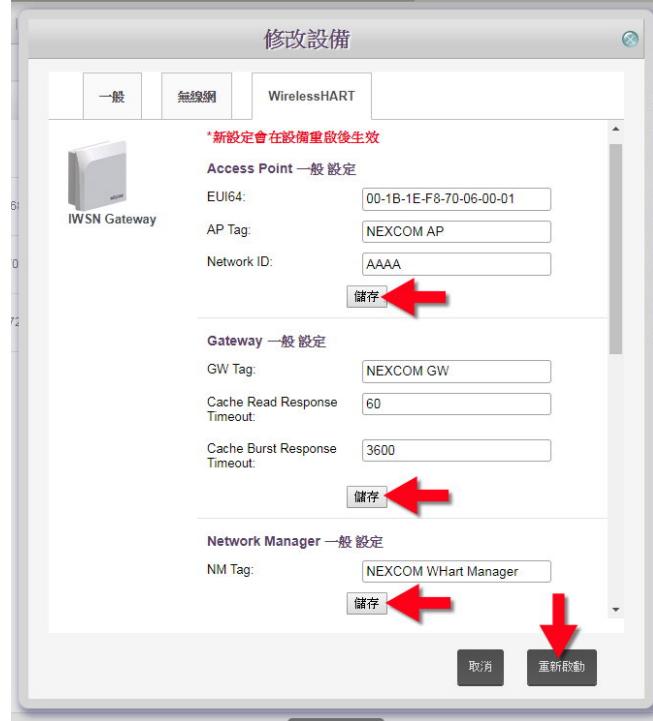


圖 62 修改 IWSN Gateway 之 WirelessHART 參數 1

b.「WirelessHART」頁籤往下拉，可進一步設定「Device Management」的「Access Points」、「Gateways」、「Devices」參數，以及在「Device List」新增與啟用設備。



圖 63 修改 IWSN Gateway 之 WirelessHART 參數 2

(8) IWSN Gateway 系列的「NIO200-IAG」設備修改設備資訊，除了「一般資料」及「無線網」頁籤可設定之外，還有「ISA100」頁籤可以設定。

a.「ISA100」頁籤可設定「Backbone Router」、「Gateway」、「System Manager」參數，填入參數後按「儲存」，並點擊「重新啟用」使新的設定生效。

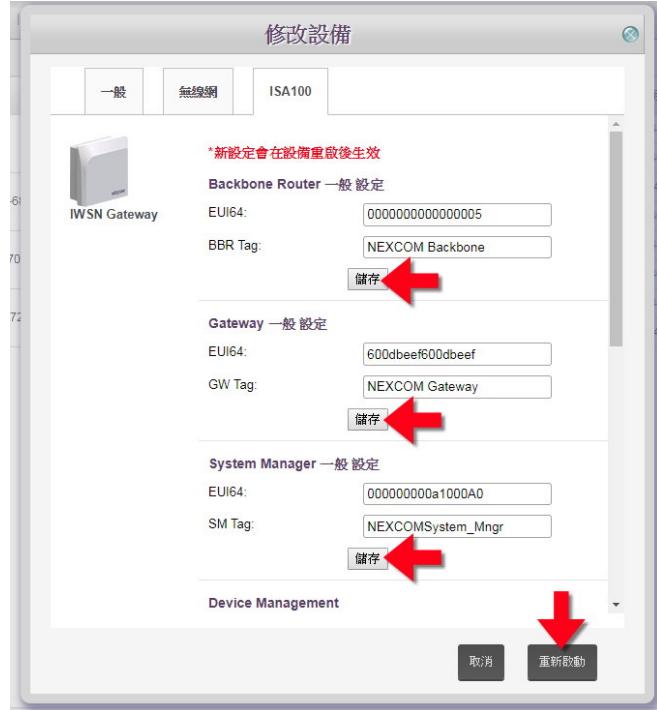


圖 64 修改 IWSN Gateway 之 ISA100 參數 1

b.「ISA100」頁籤往下拉，可進一步設定「Device Management」的「Backbones」、「Gateways」、「Devices」參數，以及在「Device List」新增與啟用設備。



圖 65 修改 IWSN Gateway 之 ISA100 參數 2

(9)IPC 系列設備修改設備資訊，除了一般資料之外，還有「警戒值」頁籤可做設定。點選啟動，並選擇警報接收對象後，點擊「確認」設定。



圖 66 IPC 設備修改設定

6.1.2.7. 刪除設備資訊

(1)點選欄位 ，可刪除設備的資訊。



設備種類	顯示種類非法設備													
	編號	設備名稱	IP位址	設備種類	SSID	模式	加密協定	頻道	強度	網真	Mibrowser	重啟	修改	刪除
IWF	00:0e:0e:67:5b:ad	IWF300-63	10.211.10.63	IWF	IWF300_11N_2G_63	ap	psk2	6	0					
Mobile Mesh	00:10:03:5e:28:57	IWF310-44	10.211.10.44	IWF	IWF310_11N_2G_44	ap	psk2	11	0					
Device Server	00:0e:0e:67:5a:90	IWF300-46	10.211.10.46	IWF	IWF300_11N_2G_46	ap	psk2	11	0					
IWSN Gateway	10.211.10.43	IWF300-43	10.211.10.43	IWF	IWF300_11N_2G_43	ap	psk2	11	0					
					IWF300_11A_5G_43	ap	psk2	36	0					

圖 67 刪除設備資訊

6.1.3. 設定備份(Config Backup)說明

nCare 可為設備進行設定備份，並可安排備份的期程，或是立即以手動執行備份作業。

6.1.4. 設定備份(Config Backup)操作

(1)勾選擬以「設備型號」或「設備 IP 位址」搜尋需要備份的設備，點選  進行搜尋。



圖 68 搜尋需備份的設備

(2)跳出設備列表，勾選擬需要備份的設備(可複選)，選擇「立即備份」，立即備份。或設定「排程名稱」、「開始時間」及備份「重複」的週期(無、每週、每個月)，按「新增排程」即可設定排程。



圖 69 編輯設備備份的排程

(3)成功設定更新排程後，主畫面左方即顯示此備份的工作名稱，點選工作名稱，可進一步執行修改、立即備份或刪除備份的工作。



圖 70 檢查備份列表

(4)點選備份工作名稱的「結果」，可跳出「備份檔案結果」視窗。顯示「設備名稱」、「IP 位址」、組態備份的「狀態」及「時間」。狀態若顯示成功(Success)，則表示備份檔案已儲存於系統內，點擊旁邊下載圖示 ，可將備份檔案下載至電腦中存放。

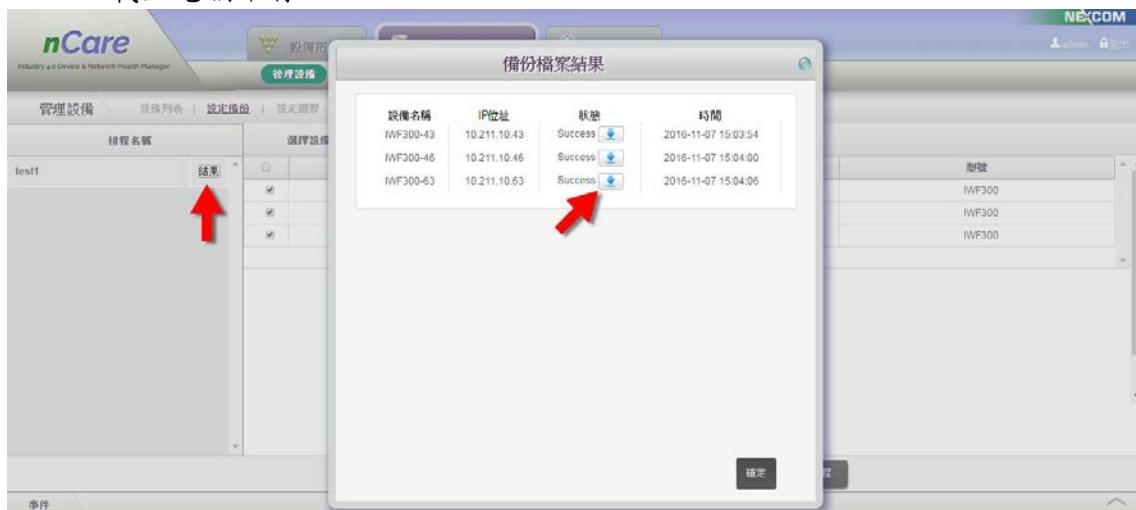


圖 71 檢查備份狀態

6.1.5. 設定還原(Config Restore)說明

nCare 可為設備進行設定還原，需先為設備進行設定備份(請參閱 6.1.4 章節)，利用既有的備份檔案來還原。

6.1.6. 設定還原(Config Restore)操作

(1)勾選以「設備型號」或「設備 IP 位址」點選  搜尋設備，並選擇需要還原的設備。



圖 72 搜尋需還原的設備

(2)點選資料夾圖示，跳出「設定還原」視窗，選擇前一個章節下載備份的組態檔案。

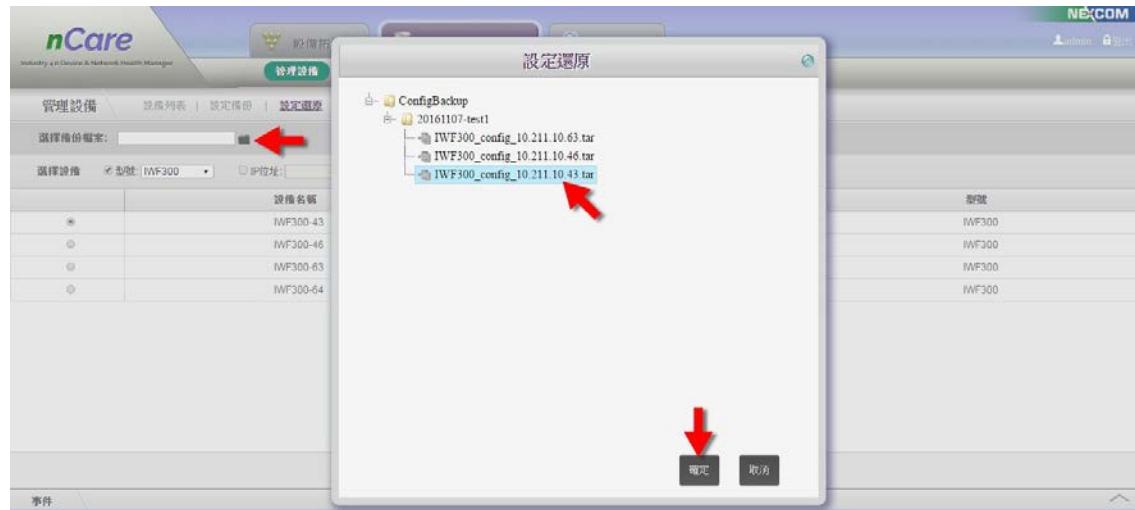


圖 73 選擇組態還原檔案

(3)載入檔案後，點擊「還原」及「確認」鍵後，即可進行設備設定還原。

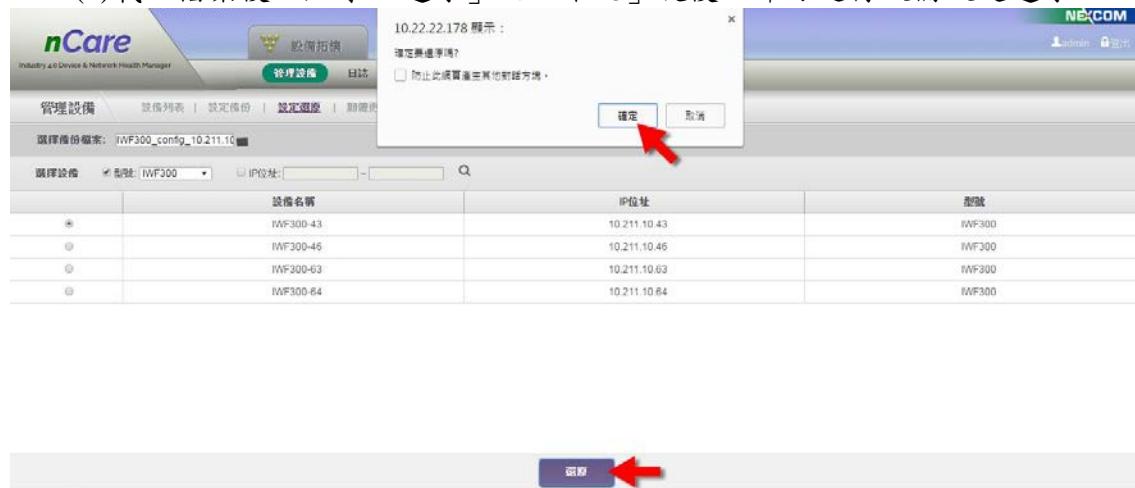


圖 74 確定組態還原

(4)若挑選到錯誤的還原檔案，系統將顯示錯誤訊息。

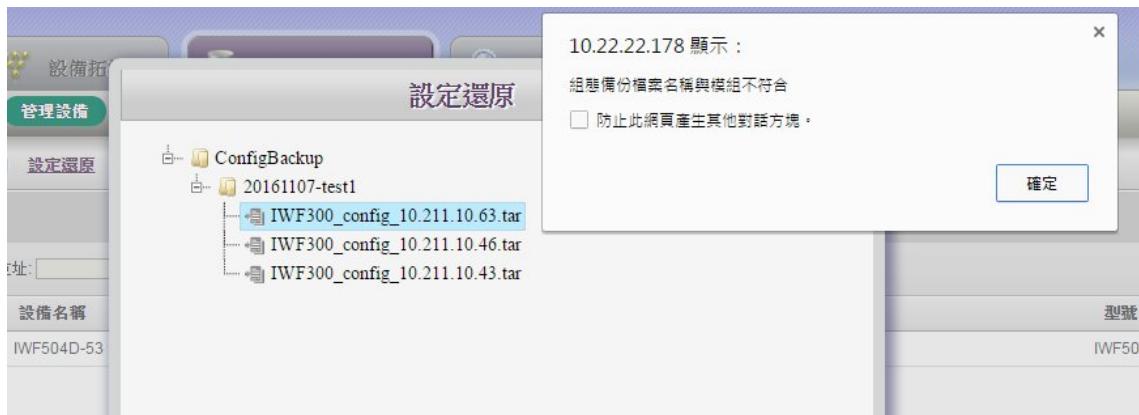


圖 75 還原錯誤訊息

6.1.7. 勅體更新(Fw Upgrade)說明

nCare 可為設備進行勅體更新，並可安排備份的期程，或是以手動進行立即的勅體更新作業。

*更新前，請確認 FW 檔案格式:[設備種類]-[版本號]，例如 IWF300-v2.0.bin

6.1.8. 勅體更新(Fw Upgrade)操作

(1)搜尋設備：勾選以「設備型號」或「設備 IP 位址」，點選 搜尋設備，再選擇需要還原的設備。



圖 76 選擇需勅體更新的設備

(2)勾選需要更新勅體的設備(可複選)。填寫「排程名稱」、「開始時間」，並點選資料夾圖示 尋找與設備對應的驅動程式(最新版的驅動程式請聯繫新漢服務人員，取得之勅體檔案，請勿更改檔名)，再點擊「新增排程」按下「確認」鍵即設定排程；或填寫「排程名稱」、點選資料夾載入勅體檔案後，直接點選「立即勅體更新」和「確認」鍵，使系統更新設備勅體。



圖 77 設定韌體更新的排程

(3)成功設定排程後，主畫面左方即顯示此備份的工作名稱，點選工作名稱，可進一步執行修改、立即更新或刪除排程的工作。



圖 78 檢查韌體更新排程列表

(4)點選工作名稱的「結果」，可跳出「韌體升級結果」視窗。顯示「設備名稱」、「IP 位址」、組態備份的「狀態」及「時間」。狀態若顯示成功(Success)，則表示設備已經成功進行韌體更新完畢；若顯示(Onging)表示正在更新中；若顯示(Failed)則為失敗，請聯繫新漢客服人員。



圖 79 韌體升級結果

6.1.9. 設備配置(Device Provision)說明

nCare 可讓管理者大量部署新設備，數個設備連結 nCare 的伺服器後，使用 DHCP 功能分配好 IP 位址(請見 5.4 章節 DHCP 管理)，再利用「設備配置」功能將部屬的新設備批次設定好 ESSID/Mesh ID、模式、加密協定等相關參數。

6.1.10. 設備配置(Device Provision)操作

(1) 選擇要大量配置的「設備種類」及「型號名稱」，填寫「一般設定」、「界面」、「工作頻率」等參數資料後，點擊「儲存」。

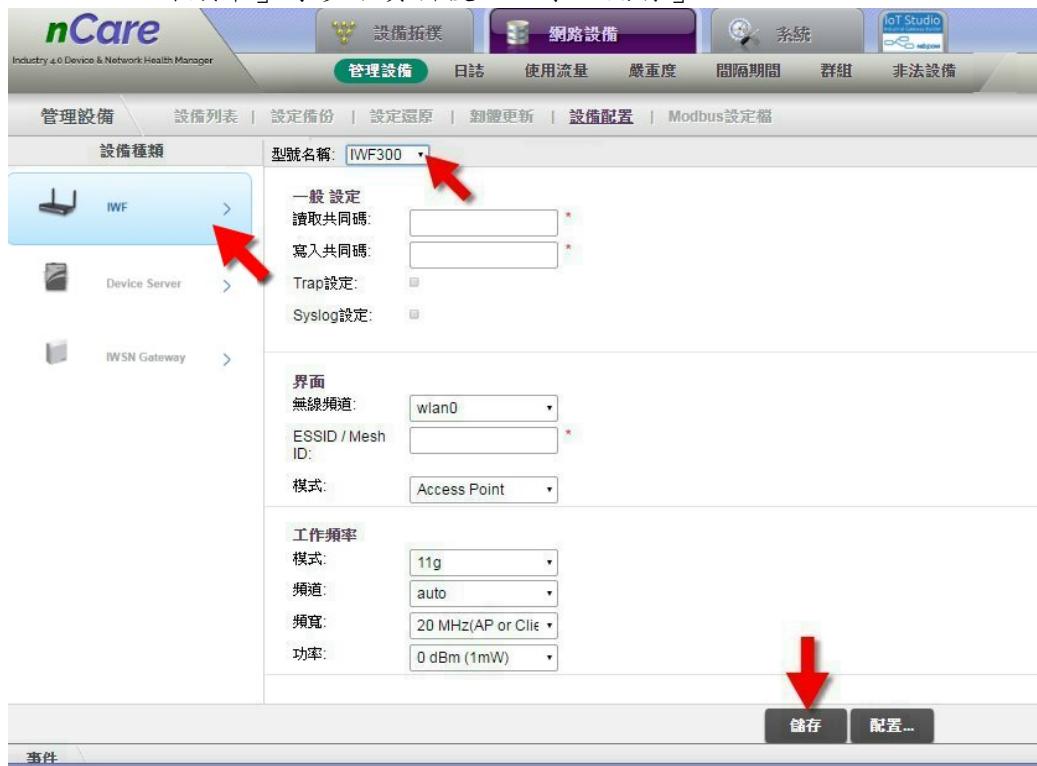


圖 80 設備配置設定

(2)點擊「配置」，跳出「設備列表」，勾選需要配置的設備(可複選)，再點擊「確定」，設備參數即一次性大量載入設備中。步驟完成後，前往「設備列表」(6.1.1 章節)及「拓樸圖」(需重新探索)，即可看見設備資料更新了。



圖 81 選擇需要配置的設備

6.1.11. Modbus 設定檔(Modbus Profile)說明

Modbus 設定檔功能可讓管理者事先於 nCare 中，建立 IPC 或 PLC 等支援 Modbus 的設備資料，管理者未來若要增加這些設備，只要將設備連上 nCare，即可於探索後顯示這些設備的資訊與圖示。

6.1.12. Modbus 設定檔(Modbus Profile)操作

(1)填寫設備型號，上傳設備圖示。



圖 82 填入 Modbus 設備型號與圖示

(2) 填寫「掃描參數」的資料，如「暫存器值」、「功能碼」、「點位偏移」、「字數」，以下拉式選單選擇「屬性」類別。(點位值請參考設備的手冊)



圖 83 填入 Modbus 設備掃描參數

(3) 再填寫「暫存器表」資料，點選「Add Register」、「Delete Register」可新增或刪除欄位，填寫「單位」、「點位偏移」、「字數」，以下拉式選單選擇「功能碼」和「屬性」最後點擊「新增」。(點位值請參考設備的手冊)

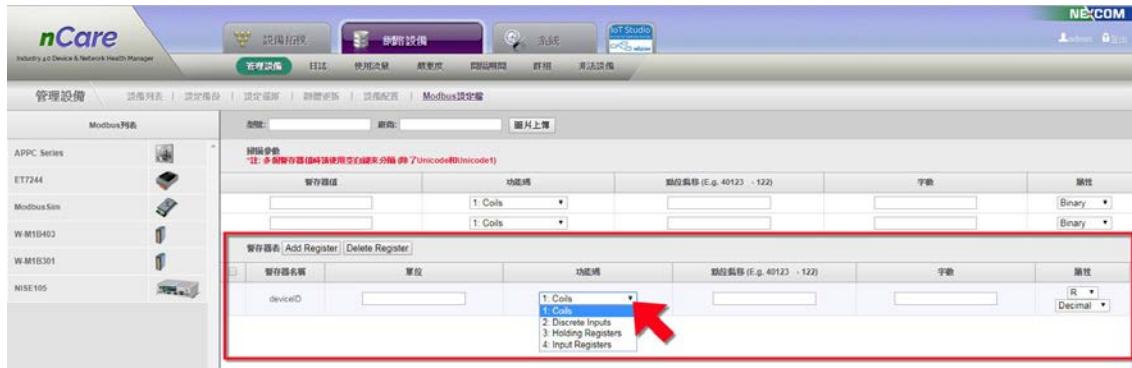


圖 84 填入 Modbus 設備暫存器表

(4) 新增之設備資料列於左側，並可進一步查詢、修改或刪除。



圖 85 查閱或修改 Modbus 設備參數

6.2. 日誌管理(Log)

「日誌頁面」包含「事件紀錄(Event Log)」、「系統紀錄(System Log)」和「告警回播(Playback)」。可將設備發生之異常事件記錄於列表中或記錄成檔案，提供管理者查閱回播。

6.2.1. 事件紀錄(Event Log)說明

nCare 會將設備異常之狀況紀錄於事件紀錄中，管理者可以設定搜尋條件，尋找設備過去的警示紀錄。

6.2.2. 事件紀錄(Event Log)操作

- (1)事件紀錄功能預設顯示一個月的所有警示紀錄。可單選或複選搜尋條件，如「起迄日期」、「IP 位址」、「嚴重程度」、「設備名稱」或先前已「清除」的紀錄來搜尋。

條號	IP位址	設備名稱	嚴重程度	事件	時間
1	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:27:37
2	10.211.10.65	NIO50-65	Major	Network Unstable	2017-04-21 18:24:03
3	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:22:52
4	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:22:52
5	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:21:40
6	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:21:40
7	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:21:40
8	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:21:40
9	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:20:29
10	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:20:29
11	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:18:07
12	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:16:07
13	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:16:07
14	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:16:54
15	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:15:43

圖 86 事件日誌尋找記錄

- (2)事件紀錄以紅、黃、綠顏色區分事件的嚴重程級(請見 6.4 章節嚴重度)，並顯示發生此事件之設備的「IP 位址」、「設備名稱」、「嚴重程度」、「事件名稱」及「發生時間」。

條號	IP位址	設備名稱	嚴重程度	事件	時間
1	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:27:37
2	10.211.10.65	NIO50-65	Major	Network Unstable	2017-04-21 18:24:03
3	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:22:52
4	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:22:52
5	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:21:40
6	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:21:40
7	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:21:40
8	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:21:40
9	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:20:29
10	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:20:29
11	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:18:07
12	10.211.10.66	NIO50-65	Normal	Polling Success	2017-04-21 18:16:07
13	10.211.10.66	NIO50-65	Critical	Polling Failed	2017-04-21 18:16:07
14	10.211.10.66	NIO50-65	Major	Network Unstable	2017-04-21 18:16:54
15	10.211.10.49	NIO50-49No	Critical	Polling Failed	2017-04-21 18:15:43

圖 87 事件日誌資訊

(3)每項事件紀錄前方可勾選「清除」(可複選)，勾選後再點擊上方的「清除」按鈕，即跳出「刪除成功」的子視窗，點擊確定後，勾選記號即會顯示於紀錄前方，但並不會清除此項紀錄。

*紅色(嚴重層級)警報，會因設備端恢復正常後，自動勾選清除鍵。黃色(重要層級)警報，設備端恢復後，使用者需手動勾選警報記錄來清除警報通知。

圖 88 清除事件紀錄

(4)事件記錄快捷功能：nCare 除了在「事件紀錄」頁面中有完整的警告紀錄。每一個主選單功能頁面下方皆有「事件紀錄」快捷功能。可點選右下方 或 收起即時事件視窗。

圖 89 事件紀錄快捷功能

(5)事件紀錄快捷功能僅顯示紅(嚴重)、黃(重要)的警訊。

編號	IP位址	設備名稱	事件名稱	時間
1	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:33:00
2	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:31:49
3	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:30:38
4	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:20:15
5	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:27:03

圖 90 事件記錄快捷嚴重層級

(6)左上方可勾選嚴重性，使系統顯示一項或兩項警告層級，也可完全不顯示。

編號	IP位址	設備名稱	事件名稱	時間
1	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:27:00
5	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:27:03
7	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:21:07
12	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:15:10
15	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:09:14

圖 91 選擇嚴重層級

(7)點擊「事件重播」會跳至「告警回播」頁面，詳請 6.2.5 章節。

編號	IP位址	設備名稱	事件名稱	時間
1	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:33:00
5	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:27:03
7	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:21:07
12	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:15:10
15	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:09:14

圖 92 事件重播快捷鍵

(8)點選拓樸下方的事件記錄快捷列表，選擇需要重現的事件，可於拓樸上顯示當下的靜態畫面。

編號	IP位址	設備名稱	事件名稱	時間
1	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:30:08
2	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:30:57
3	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:28:37
4	10.211.10.49	NIO50-49No	Polling Failed	2017-04-21 19:33:00
5	10.211.10.66	NIO50-65	Network Unstable	2017-04-21 19:31:49

圖 93 事件重現

6.2.3. 系統紀錄(System Log)說明

系統紀錄可紀錄使用者針對設備執行的各種變更或設備自動發出的警訊，如設備進行網頁或 MIB Browser 設定、更新韌體、設定備份等，皆會呈現於系統紀錄列表中。使用者可以通過查看系統紀錄，隨時掌握設備狀況。

6.2.4. 系統記錄(System Log)操作

(1) 系統紀錄預設顯示一個月內的所有紀錄。使用者可單選或複選搜尋條件，如「起迄日期」、「IP 位址」、「嚴重程度」、「設備名稱」來搜尋紀錄。

編號	IP位址	設備名稱	嚴重度	設備	時間	訊息
1	10.211.10.57	3310	Informational	Syslogd	2016-11-07 19:12:56	-- MARK--
2	10.211.10.57	3310	Informational	Syslogd	2016-11-07 19:02:55	-- MARK--
3	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:52:55	-- MARK--
4	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:42:54	-- MARK--
5	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:32:54	-- MARK--
6	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:22:53	-- MARK--
7	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:12:53	-- MARK--
8	10.211.10.57	3310	Informational	Syslogd	2016-11-07 18:02:52	-- MARK--
9	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:52:52	-- MARK--
10	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:42:51	-- MARK--
11	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:32:51	-- MARK--
12	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:22:50	-- MARK--
13	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:12:50	-- MARK--
14	10.211.10.57	3310	Informational	Syslogd	2016-11-07 17:02:49	-- MARK--

圖 94 搜尋系統記錄

6.2.5. 告警回播(Playback)說明

nCare 蔽集之警報事件，具有回播功能，可設定回播時間、搜尋事件，並以拓樸圖畫面重現設備發生異常的過程。

6.2.6. 告警回播(Playback)操作

(1) 系統預設「啟動」錄製告警事件，並以三分鐘記錄一次拓樸的異常狀況，每 30 天系統會清除所有紀錄重新錄製，每儲存滿 1024MB 的紀錄後，系統也會清除先前的紀錄。管理者可再針對「記錄週期」、「天數」、「記錄容量上限」修改設定。

啟動:	<input checked="" type="checkbox"/>
紀錄週期:	3 ▾ 分鐘
天數:	30 ▾ 天數
紀錄容量上限:	1024 ▾ MB
<input type="button" value="修改設定"/> <input type="button" value="事件重播"/>	

圖 95 修改告警回播的設定

(2)管理者欲查看先前的紀錄，可點擊「事件重播」，跳出事件重播分頁。

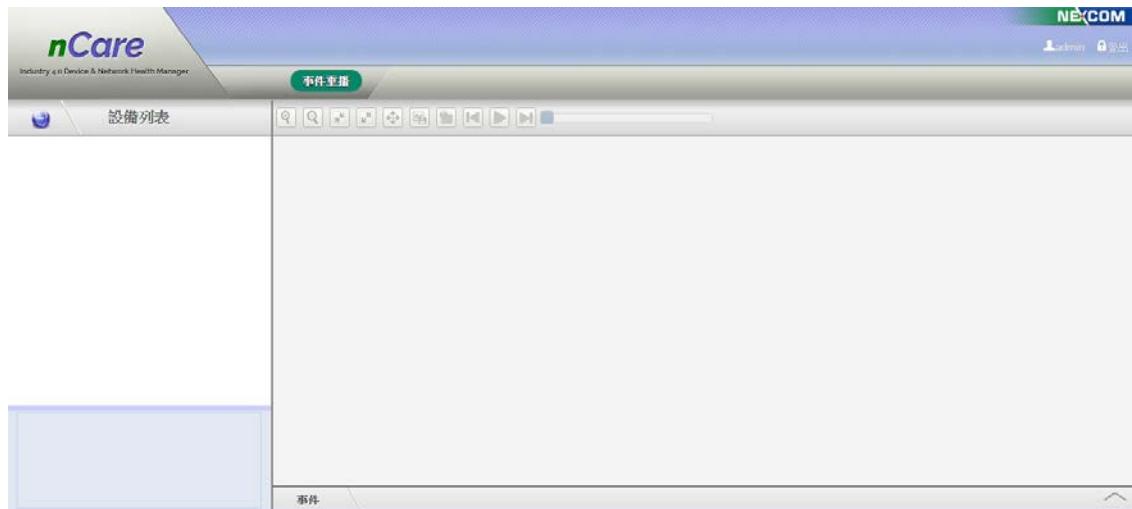


圖 96 事件重播

(3)告警記錄可藉由搜尋取得，點擊「尋找」圖示，跳出子視窗，可選擇搜尋起迄日，再點擊「確定」。

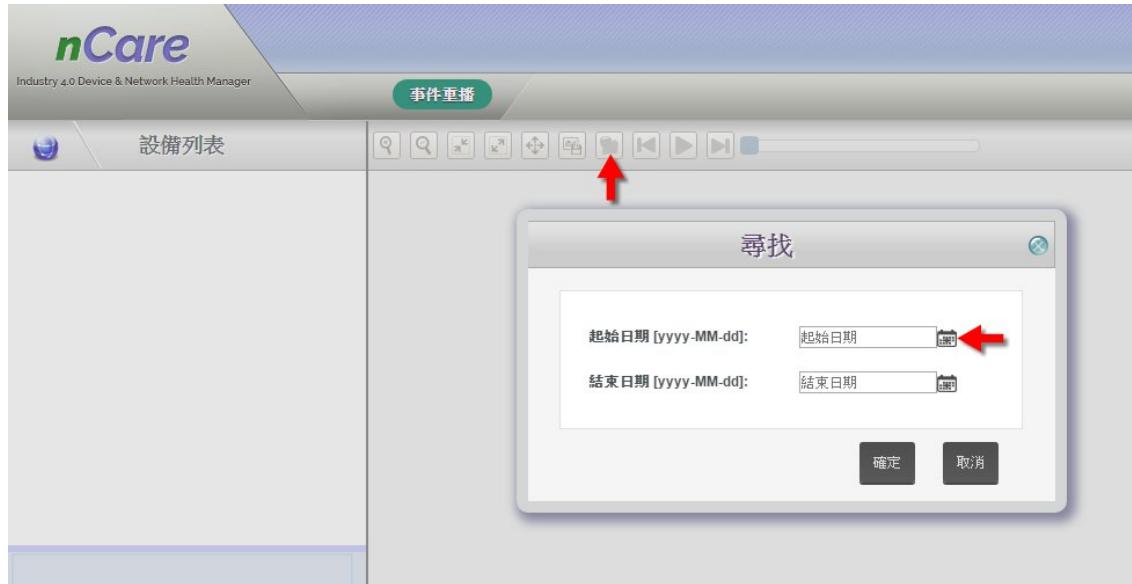


圖 97 事件搜尋

(4)搜尋後即顯示範圍內之所有告警紀錄，以利用上方功能鍵進行播放，重現事件發生之紀錄。

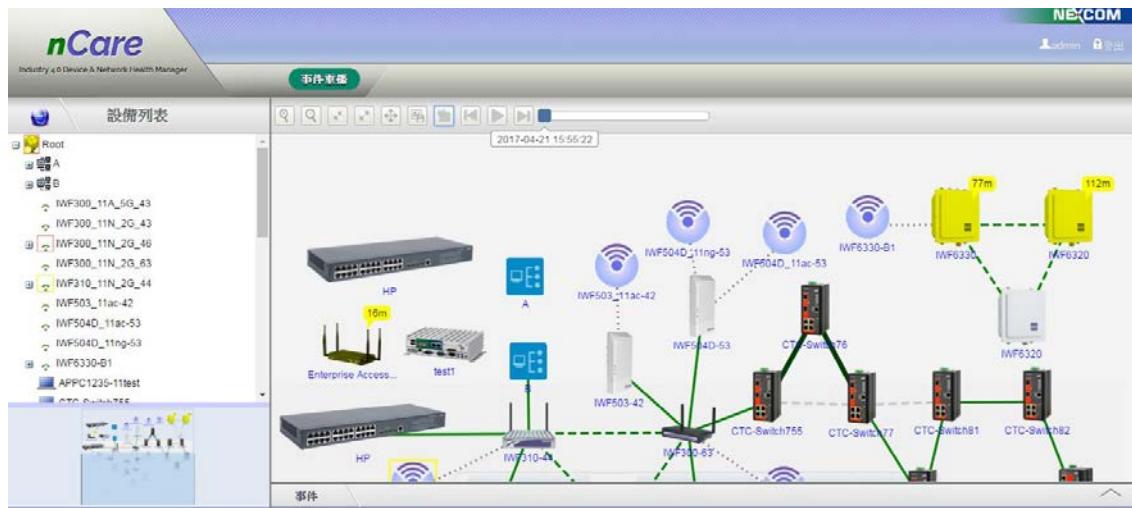


圖 98 事件重播拓樸圖

(5)事件重播上方之功能鍵功能如下：



- 放大：可放大事件重播拓樸畫面。
- 縮小：可縮小事件重播拓樸畫面。
- 全覽：顯示整個事件重播的拓樸畫面。
- 原始大小：顯示原始大小的事件重播拓樸畫面。
- 全螢幕：以全螢幕操作事件重播拓樸畫面，可按「ESC」或 跳回主畫面。
- 汇出成圖檔：可複製拓樸全覽圖。點擊後跳出分頁，再以右鍵下載 png 格式之圖檔。
- 尋找：依據搜尋的日期，顯示範圍內所有的告警紀錄。
- 上一個：播放上一個告警記錄時間點。
- 播放：播放告警紀錄。
- 下一個：播放下一個告警記錄時間點。

6.3. 使用流量(Usage)

6.3.1. 使用流量說明

nCare 可偵測設備的乙太網(Eth)、無線網(Wlan)、處理器(CPU)、記憶體(Memory)之流量或使用率，並可將數據導出成為折線圖。

6.3.2. 使用流量操作

(1)頁面左方選擇要監看的設備種類、頁面上方選擇要監看的參數，如乙太網、無線網、處理器、記憶體，系統將依據選擇顯示相關的資料數據。

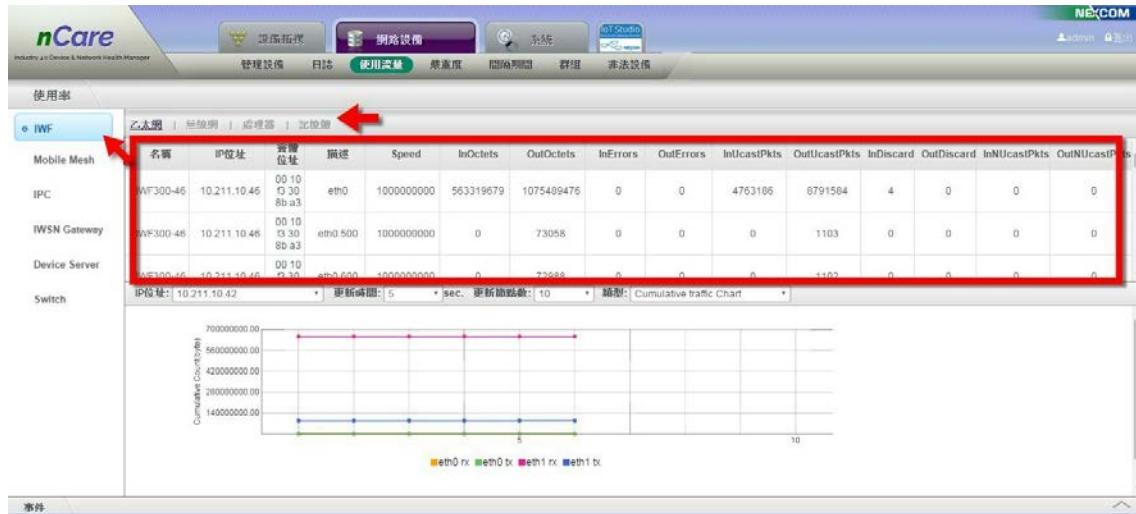


圖 99 選擇監控設備與參數

(2)下拉式選單「IP 位址」選擇監控的設備；「更新時間」選擇 5-30 秒更新一次折線圖的節點；「更新節點數」選擇每 10-100 個節點更新一次折線圖；若選擇輸出「乙太網」和「無線網」折線圖，還可選擇顯示「throughput chart」網路封包流量線圖或「cumulative traffic chart」累積封包量線圖。

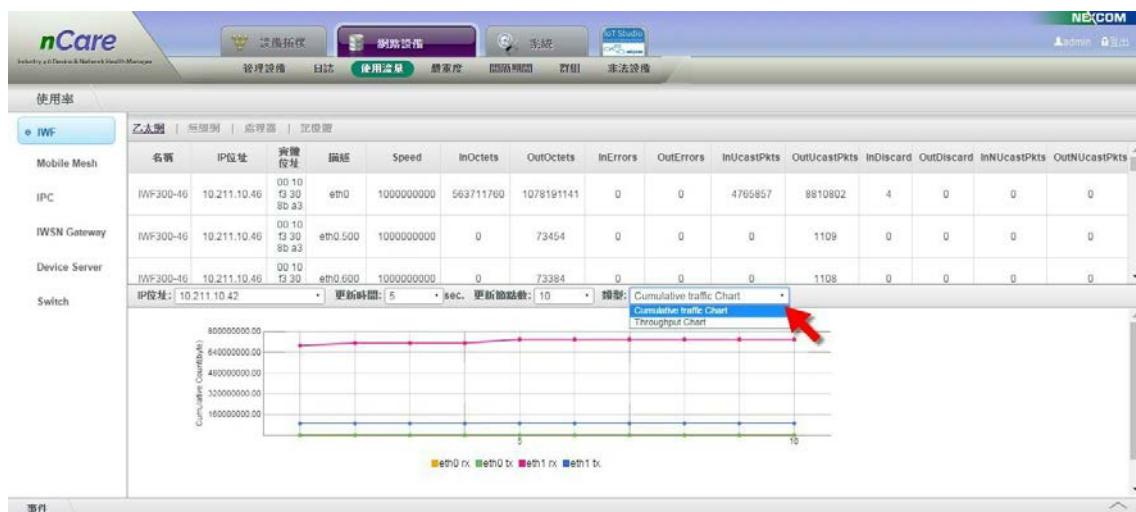


圖 100 選擇折線圖的形式

(3)選擇後系統開始導出折線圖數據，如「乙太網」可顯示設備的乙太網路輸出與輸入流量。

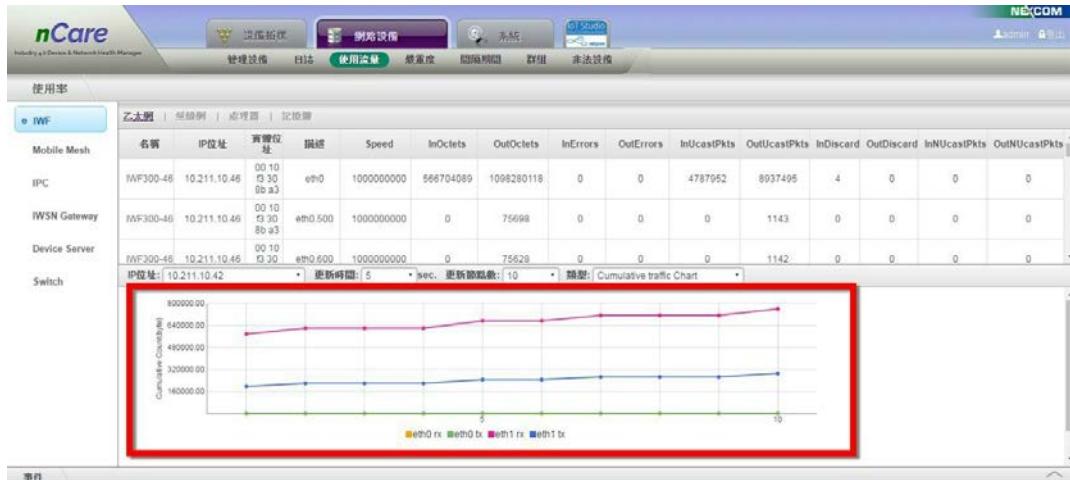


圖 101 導出 Eth 數據

(4)在「無線網」頁面，可導出設備 WiFi 網路的流量數據(throughput or cumulative traffic chart)與使用人次(Client count)之折線圖。



圖 102 導出 Wlan 數據

(5)在「處理器」頁面，可顯示 CPU 使用流量(CPU Usage)數據折線圖。



圖 103 導出 CPU 使用數據

(6)在「記憶體」頁面，可顯示記憶體使用率(Memory)折線圖。

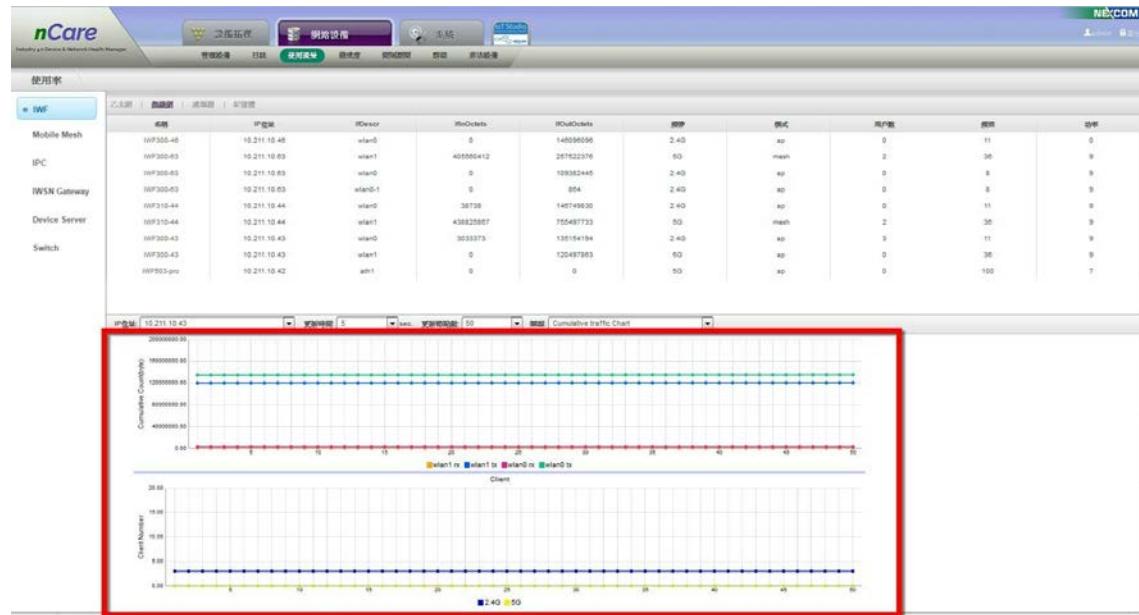


圖 104 導出記憶體使用數據

(7)左欄設備種類選擇「IWSN Gateway」，可針對「NIO200-IAG」、「NIO200-WMR」及「NIO200-HAG」設備產生各項流量折線圖。

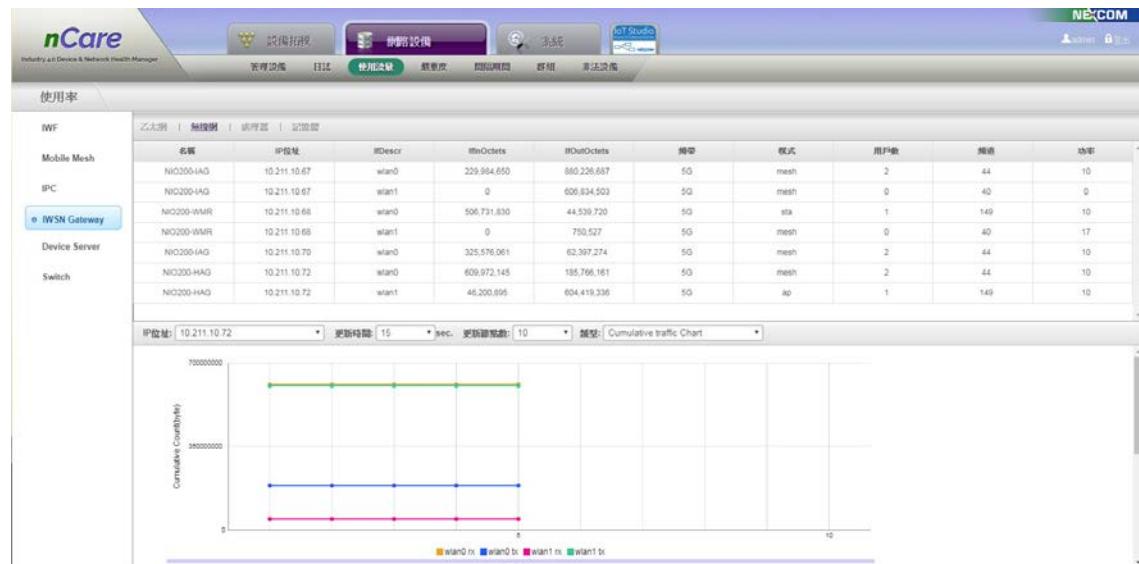


圖 105 導出 NIO200 設備之流量

(8)左欄設備種類選「Device Server」，可針對 NIO51 設備產生各項流量折線圖。

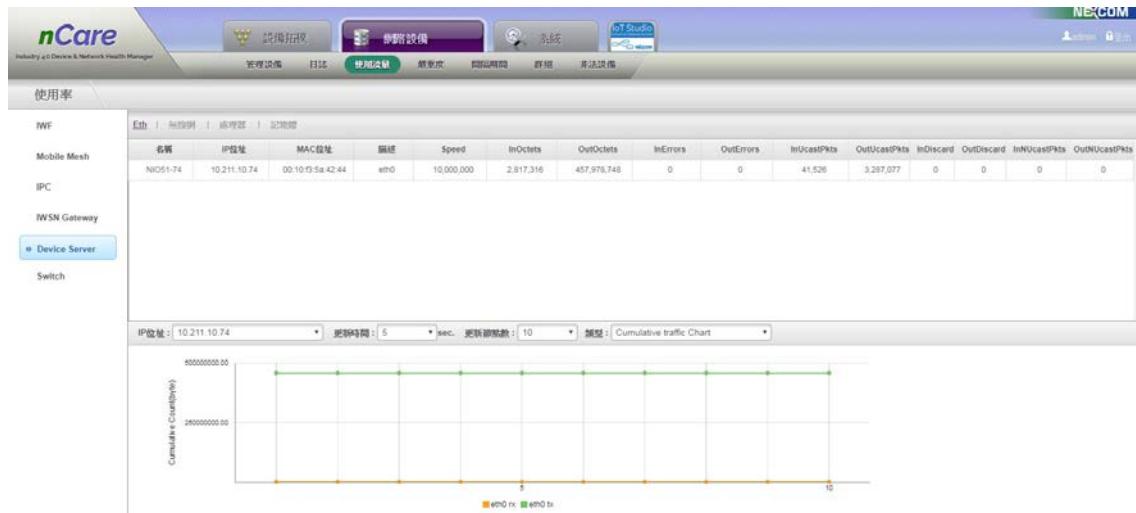


圖 106 導出 NIO51 設備之流量

6.4. 嚴重度(Severity)

6.4.1. 嚴重度說明

「嚴重程度」頁面功能可為「事件(Event)」設定不同的警報層級。嚴重警訊(Critical)標示為「紅色」，重要警訊(Major)標示為「黃色」，正常訊息(Normal)以「綠色」顯示。

6.4.2. 嚴重度操作

nCare 內建「Polling failed」(輪詢失敗)、「Link down」(斷線)、「Warm start」(暖啟動)、「Cold start」(冷啟動)、「Authentication failed」(驗證失敗)、「Polling success」(輪詢成功)、「Link up」(連線)、「IPC Temp Alarm」(IPC 溫度警報)、「IPC Storage Alarm」(IPC 儲存警報)、「Network Unstable」(網路不穩定)、「Rogue AP/Device Alarm」(非法 AP/設備警報)、「Ring Failure」(環狀鏈路斷線)、「Ring LinkUp」(環狀鏈路連線)訊息。

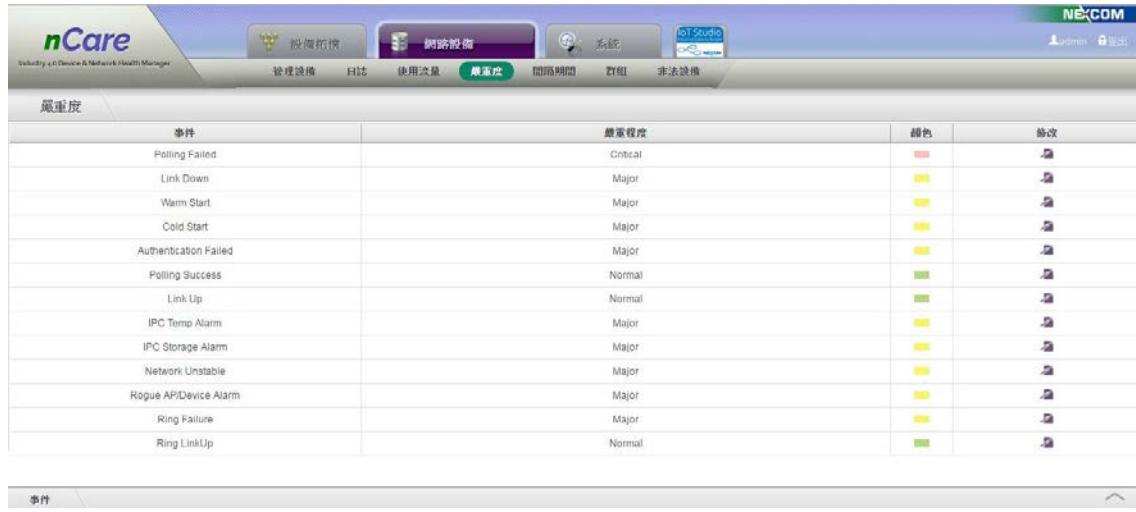


圖 107 嚴重度事件列表

(2)可點選事件列表右方的「修改」進行設定。彈出修改子視窗後，以下拉式選單為事件設定嚴重程度，修改後警示顏色將依嚴重度改變。



圖 108 嚴重度修改

6.5. 區隔期間(Interval)

6.5.1. 區隔期間說明

nCare 可以設定系統輪詢設備的週期，以及設備幾分鐘內發出的同樣的 Trap 可以合併顯示於事件日誌中。

6.5.2. 區隔期間操作

以拉下式選單選擇「輪詢設備間隔時間」或「重複事件合併期間」的分鐘數後，點擊「修改設定」即可設定。如圖每 1 分鐘輪詢設備一次，以及每 5 分鐘內，相同設備發出相同之警報事件可以合併顯示。



圖 109 間隔期間設定

6.6. 群組(Group)

6.6.1. 拓樸群組說明

此功能可事先規劃拓樸群組的名稱與資訊，以便歸納鄰近的設備群，或指定群組的管理權限給部分的使用者。

6.6.2. 拓樸群組操作

- (1)點選頁面下方「Add」，跳出「拓樸群組新增」子視窗新增群組資訊。設定拓樸群組之「名稱」、「地圖圖像(1MB 以下之 png、jpg、bmp 檔案)」、「地理位置經緯度」。



圖 110 拓樸群組新增

- (2)新增拓樸群組後，可點選「修改」、「刪除」重新設定。新增群組資料後續操作應用，參見 7.1.2.2 章節主選單「設備拓樸」→「拓樸圖」功能鍵「群組」。

群組	拓樸群組	名稱	地圖圖像	緯度	經度	修改	刪除
		Root	floor.jpg	0	0		
		host1		0	0		
		test2		0	0		
		host3		0	0		

圖 111 拓樸群組列表

6.7. 非法設備(Rogue AP/Device)

6.7.1. 非法設備說明

nCare 可偵測和設定未經授權的設備為非法設備，並給予標記與警報提醒使用者，以達到資安防護的作用。也可將合法的設備納入「白名單」中，讓系統偵測後辨別為合法設備。

6.7.2. 非法設備操作

6.7.2.1. 偵測(Detection)

(1)點選「掃描」偵測系統中是否有非法設備。



圖 112 掃描非法設備

(2)掃描後，系統會呈現非法的設備列表。內含「IP 位址」、「MAC 位址」、「名稱」、「型號」、「無線相連設備」及「有線相連設備」的資訊。

加入白名單	IP位址	MAC位址	名稱	型號	無線相連設備	有線相連設備
[+]	10.211.10.79	00:10:13:00:00:16	IWF504D-79	IWF504D	-	-
[+]	10.211.10.78	00:10:03:5a:42:06	IWF504D-78	IWF504D	-	-
[+]	10.211.10.77	00:10:03:4a:f1:0c	IWF503-77	IWF503	-	-
[+]	10.211.10.76	00:03:7f:00:00:55	IWF503-76	IWF503	-	-
[+]	10.211.10.74	00:10:03:5a:42:44	NIO51-74	NIO51	-	-
[+]	10.211.10.72	00:10:13:35:26:3a	NIO200-HAG-72	NIO200-HAG	-	-
[+]	10.211.10.70	00:10:03:62:38:5b	NIO200-IAG-70	NIO200-IAG	-	-
[+]	10.211.10.69	00:10:03:62:38:0d	NIO200-WMR-69	NIO200-WMR	-	-
[+]	10.211.10.67	00:10:03:5e:28:43	NIO200	NIO200-IAG	-	-
[+]	10.211.10.63	00:0e:8e:67:5b:ed	IWF300-63	IWF300	-	-
[+]	10.211.10.58	10.211.10.58_1	Unknown	Unknown device	-	-

圖 113 非法設備的資訊

(3)點選「掃描」被系統偵測為非法的設備後，「事件日誌(請見 6.2.1 章節)」也會同時記錄系統發現非法設備，點擊「事件日誌快捷鍵」可檢視紀錄。

編號	IP位址	設備名稱	事件名稱	時間
1	10.211.10.43	IWF300-43	Polling Failed	2018-05-03 19:07:53
2	10.211.10.11	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10)	2018-05-03 19:07:30
3	10.211.10.11	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10)	2018-05-03 19:07:30
4	10.211.10.11	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10)	2018-05-03 19:07:30
5	10.211.10.11	nCare	Rogue AP/Device Alarm (Found rogue device 10.211.10)	2018-05-03 19:07:30

圖 114 事件記錄顯示非法設備

(4)被偵測為非法的設備，在設備列表中(請見章節 6.1 查閱設備)，也會被標示驚嘆號提醒使用者。

設備種類	編號	設備名稱	IP位址	設備種類	SSID	模式	加密協定	頻道	強度	網頁	Mibrowser	重設	修改	刪除
IWF	00:0e:8e:67:5b:ad	IWF300-63	10.211.10.03	IWF	IWF300_11N_2G_63	ap	psk2	6	0	⋮	⋮	○	●	■
Mobile Mesh	00:10:03:5e:29:57	IWF310-44	10.211.10.44	IWF	IWF310_11N_2G_44	ap	psk2	11	0	⋮	⋮	○	●	■
Device Server	00:0e:8e:67:5a:90	IWF300-46	10.211.10.46	IWF	IWF300_11A_5G_46	ap	psk2	11	0	⋮	⋮	○	●	■
IWSN Gateway	00:0e:8e:67:5f:a5	IWF300-64	10.211.10.64	IWF	IWF300_11N_2G_64	ap	psk2	11	0	⋮	⋮	○	●	■
	10.211.10.43	IWF300-43	10.211.10.43	IWF	IWF300_11N_2G_43	ap	psk2	11	0	⋮	⋮	○	●	■
IPC	00:10:03:5a:42:01	IWF504D-69	10.211.10.69	IWF	IWF504D_11ng_69	ap	psk2	auto	0	⋮	⋮	○	●	■

圖 115 設備列表非法設備的警告標誌

(5)非偵測為非法設備，拓樸圖(請見 7.1.2.2 拓樸圖-功能按鍵)中也會被標記驚嘆號提醒使用者。

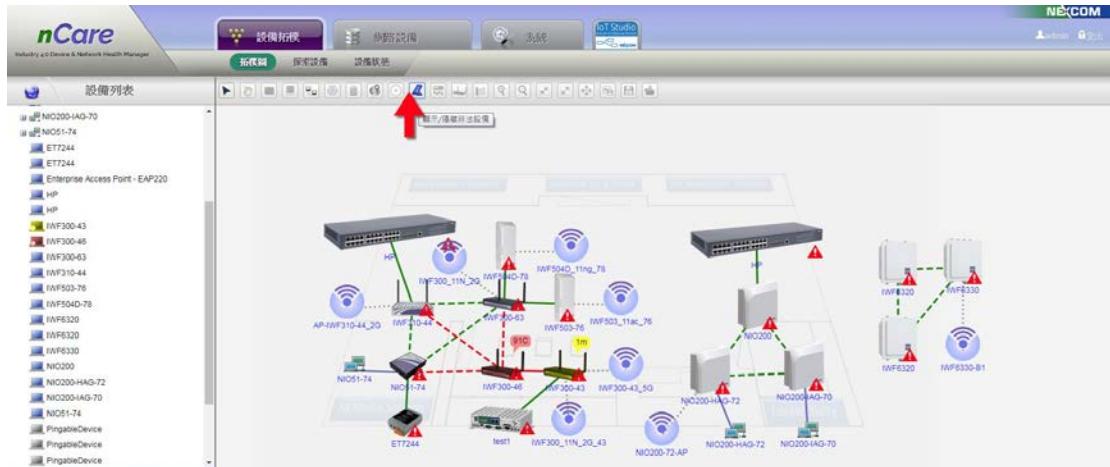


圖 116 拓樸圖非法設備的警告標誌

(6)點擊列表前方「+」號，可將此設備加入「白名單」中，歸納為合法設備。或是點擊「全部加入」，將偵測到的所有非法設備都轉為白名單。

加入白名單	IP位址	MAC位址	名稱	型號	危險相應設備	危險相應設備
[+]	10.211.10.79	00:10:f3:5a:42:0b	IWF504D-79	IWF504D	-	-
[+]	10.211.10.78	00:10:f3:5a:42:0b	IWF504D-78	IWF504D	-	-
[+]	10.211.10.77	00:10:f3:4a:fc:9c	IWF503-77	IWF503	-	-
[+]	10.211.10.76	00:03:7f:50:00:55	IWF503-76	IWF503	-	-
[+]	10.211.10.74	00:10:f3:5a:42:44	NIO51-74	NIO51	-	-
[+]	10.211.10.72	00:10:f3:35:26:3a	NIO200-HAG-72	NIO200-HAG	-	-
✓	10.211.10.70	00:10:f3:62:38:5b	NIO200-IAG-70	NIO200-IAG	-	-
[+]	10.211.10.68	00:10:f3:62:38:8d	NIO200-WMR-68	NIO200-WMR	-	-
[+]	10.211.10.67	00:10:f3:5e:20:43	NIO200	NIO200-IAG	-	-
[+]	10.211.10.63	00:0e:8e:67:5b:ad	IWF300-63	IWF300	-	-
[+]	10.211.10.68	10.211.10.68_1	Unknown	Unknown device	-	-

圖 117 將設備加入白名單

6.7.2.2. 白名單(White List)

(1)在偵測頁面中，被加入白名單的設備，資料會顯示在此「白名單」分頁中。並可對設備進行「修改」和「刪除」，也可整批匯入或匯出自名單(csv 格式)。

IP位址	MAC位址	備註	修改	刪除
10.211.10.70	00:10:f3:62:38:5b	NIO200-IAG-70		

圖 118 白名單列表

(2) 系統尚未納管的設備，也可以先以手動方式新增白名單。點擊下方「新增」，跳出「新增白名單」視窗，填寫設備資料後，點擊「確定」即可新增。



圖 119 新增白名單

6.7.2.3. 阻擋設備清單(Deny List)

此功能可手動新增非法設備的名單，也能針對白名單底下串接的設備，去設定是否為非法設備。

(1) 首先，需事先設定好白名單的設備(請見 6.7.2.2 章節)，再點擊「Add from Rogue Device」，nCare 將掃描出掛在白名單設備底下的所有設備。

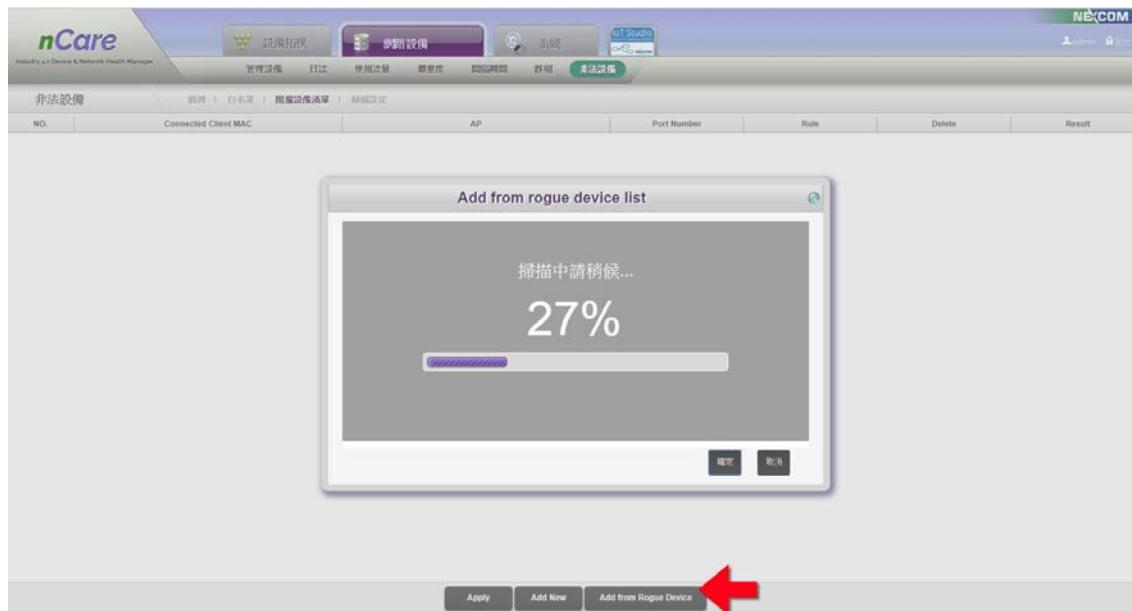


圖 120 掃描白名單設備

(2) 系統掃出掛在白名單底下的設備，列於「Add from rogue device list」視窗中，再勾選欲設定為非法設備的項目(可複選)，按「確定」。

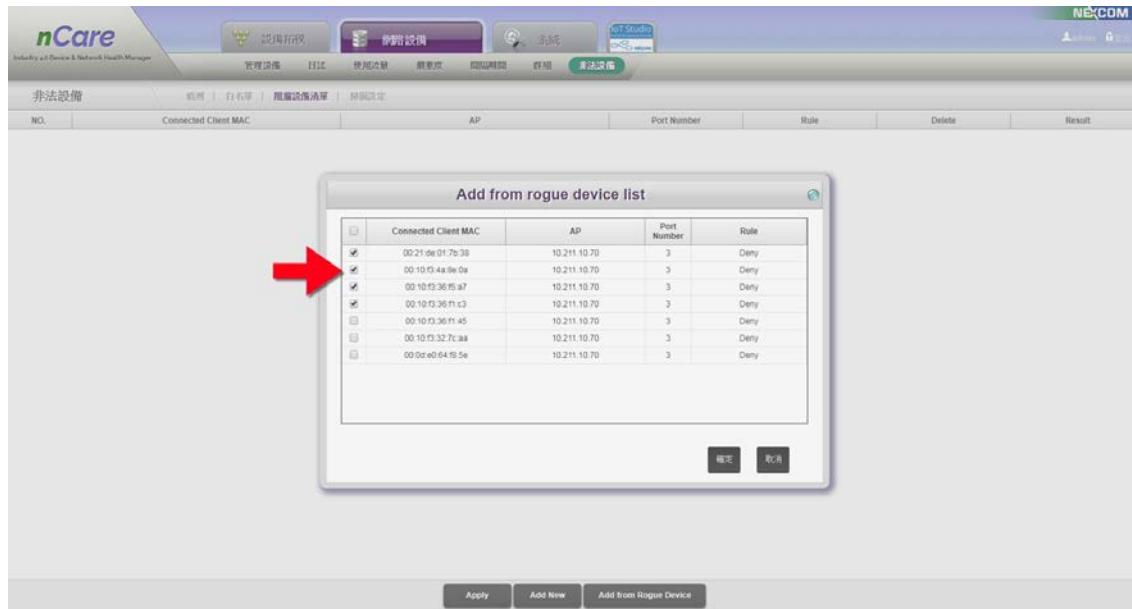


圖 121 勾選白名單下的非法設備

(3) 系統設定好欲拒絕的設備後，在「Result」欄位中仍會顯示「？」問號，表示系統已經設定完畢，但設定資料尚未載入設備中。



圖 122 設定白名單下的非法設備

(4) 點擊「Apply」，跳出「setting complete」訊息視窗，再點擊「確定」。



圖 123 載入非法設備設定

(5) 設定後，「Result」欄位即顯示為「√」勾號，表示非法設備的設定已經載入設備。

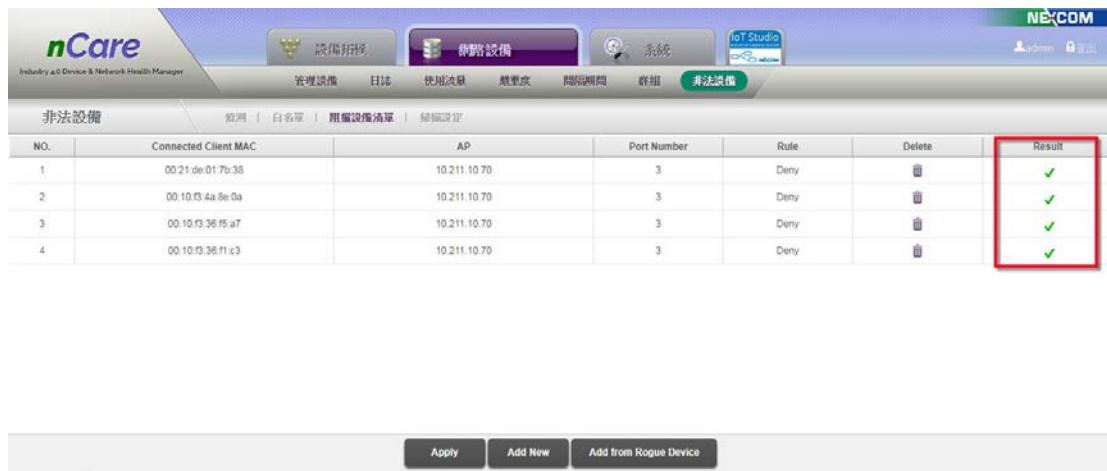


圖 124 非法設備設定已載入

(6)nCare 也可以手動新增非法設備，點擊「Add New」，跳出視窗，填寫「Connected Client MAC」、「AP」等資訊，再點擊「確定」完成設定。



圖 125 手動新增非法設備

6.7.2.4. 掃描設定(Scan Setting)

nCare 可自動掃描管設備中是否有非法設備，此功能則可設定 nCare 自動掃描的週期。輸入掃描週期(分鐘)，點擊「修改設定」即可完成設定。nCare 發現非法設備後，即可顯示警告於事件記錄中。



圖 126 設定非法設備掃描週期

7. nCare 設備拓樸(Topology)介面說明

nCare 介面包含左方「設備列表」，及右方拓樸圖之子功能「拓樸圖」、「探索設備」、「設備狀態」頁面。可探索設備、顯示納管之設備資訊、設備配置方式、連線狀態、硬體監控等效能顯示。

7.1. 拓樸圖(View)

7.1.1. 拓樸圖功能說明

nCare 拓樸頁面可以線條類型，顯示設備之間的連線關係，並以顏色警告管理者異常狀況。透過工具列與圖示快捷鍵可直接於拓樸圖上查閱設備資訊，管理設定設備與新增連線。

7.1.2. 拓樸圖功能操作

7.1.2.1. 拓樸圖繪製

點選主選單「設備拓樸」，可顯示系統納管之所有設備的拓樸圖(第一次使用請先進行 7.2 章節「探索設備」)。

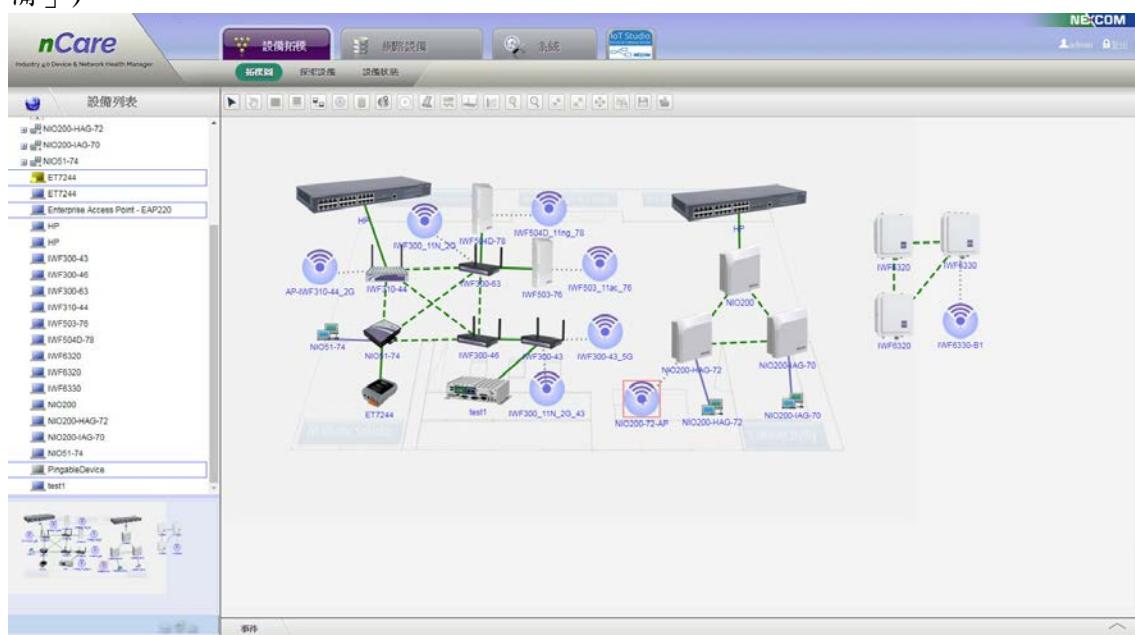


圖 127 nCare 拓樸圖

7.1.2.2. 拓樸圖功能按鍵

拓樸圖頁面上面按鍵功能如下：



圖 128 拓樸圖功能鍵



選取：系統預設進入拓樸圖中，即有「選取」功能。

(1)按住左鍵可選取、拖曳設備與連線，鬆開左鍵設備就會停留在該位置。滑鼠左鍵點擊設備或連線後，設備或線路下方會顯示陰影，表示已被選取。



圖 129 選取設備

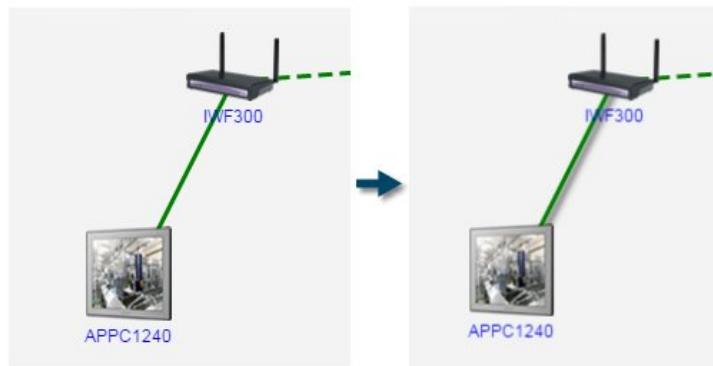


圖 130 選取連線

(2)Ctrl+滑鼠左鍵點選設備，或是按住滑鼠左鍵圈選，可一次圈選多個設備與連線。

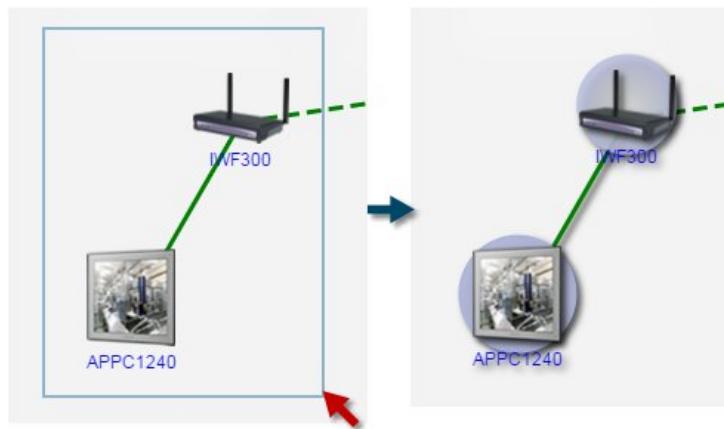


圖 131 圈選設備



移動：點選此功能可上下左右拖曳拓樸圖。



新增連線：在設備與設備之間建立新的連線。

(1)以滑鼠於 A 設備上點擊左鍵，拖曳連線至 B 設備再點擊左鍵一次，即可建立新連線。



圖 132 新增連線



新增設備：可為拓樸圖增加新的設備。

(1)選擇此功能後，點擊拓樸圖空白處，即可跳出「新增設備」視窗，選擇設備類型、通訊協定、Trap 設定、Syslog 設定、設備名稱、IP 位址...等資訊(紅色星號為必填)。

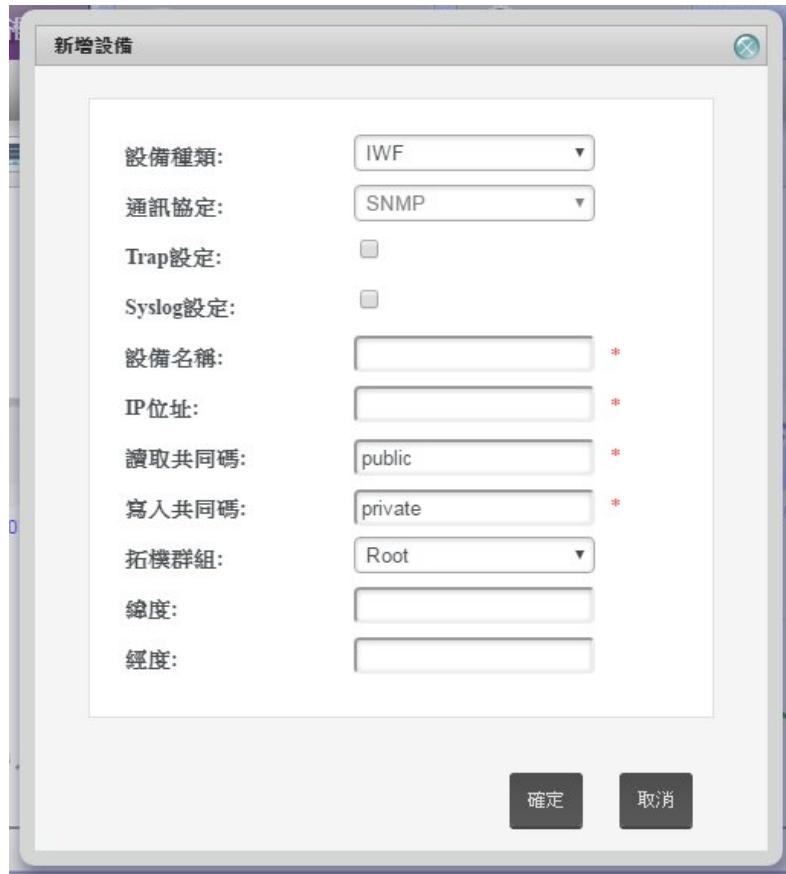


圖 133 新增設備

(2)點擊 OK，開始掃描。



圖 134 掃描設備

(3)若無此設備，則顯示「找不到新設備」的提示訊息。



圖 135 掃描不到新設備

(4)找到新設備，則顯示於拓樸頁面中。

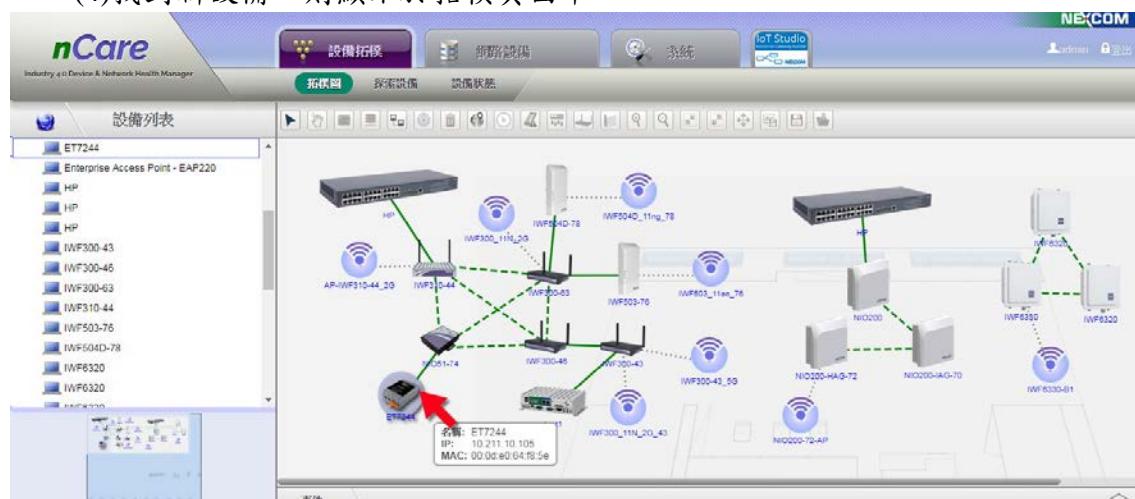


圖 136 成功新增設備



群組：可將設備歸類於同一群組。



(1)先以 **選取** 選取兩個以上的設備，再點擊「群組」圖示。

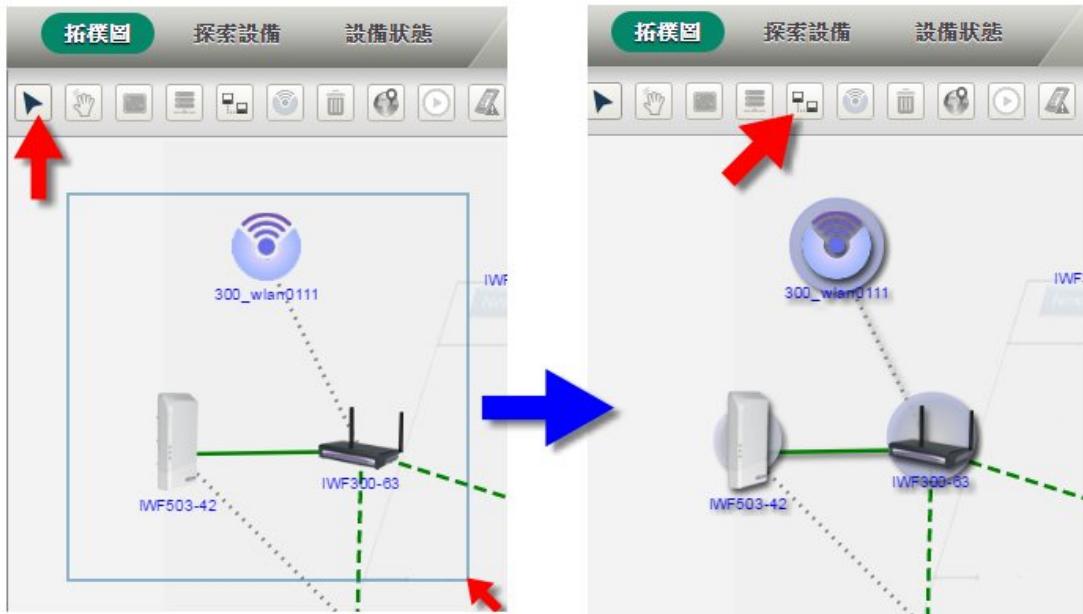


圖 137 圈選群組

(2)跳出群組視窗，設定的群組名稱(拓樸群組名稱設定請見 6.6 章節)，點擊 **OK**，即可將圈選的設備設為同一個群組。

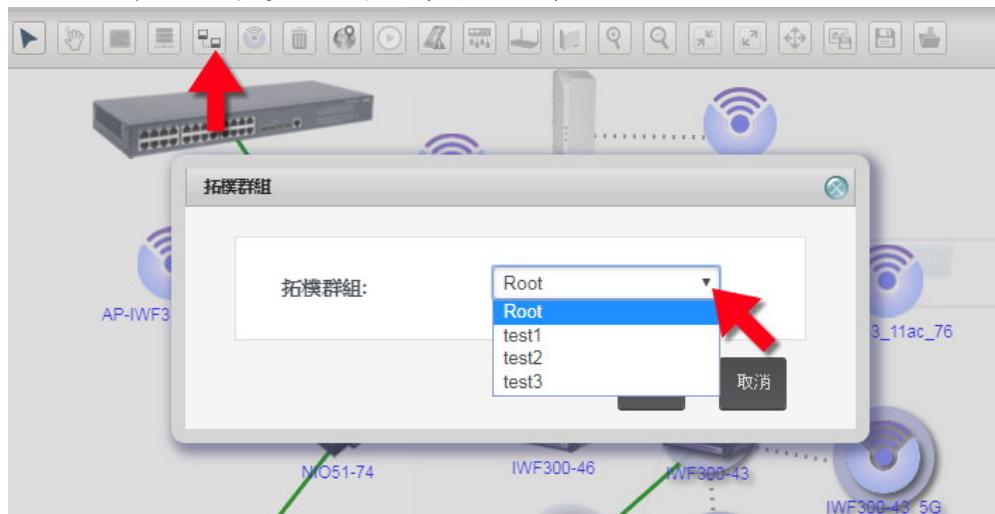


圖 138 設定群組



(3)群組成功產生後，需點擊「儲存拓樸」將群組設定儲存。點擊進入群組內，可以看見群組內的設備。



圖 139 檢視群組內設備

(4)若需取消或修改拓樸群組內之設備，可進入拓樸群組中，選取要移出的設備，再次點擊群組圖示跳出選擇子視窗，選擇「Root」，即可將設備移出。

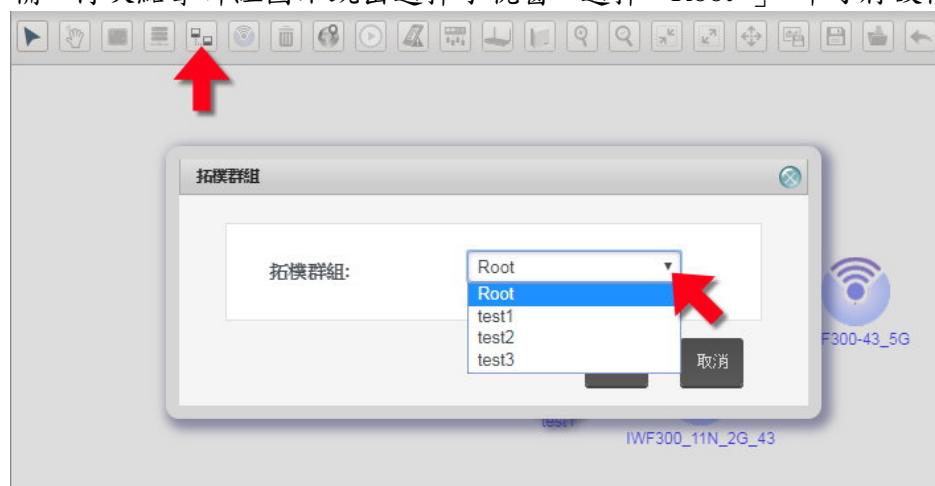


圖 140 移出群組

Wi-Fi 羣組：可將實體設備(如 IWF300、IWF310、IWF503、IWF504D、NIO51、NIO200 設備)納入 WiFi 羣組中。

(1)先選取設備，再點擊 WiFi 羣組圖示。

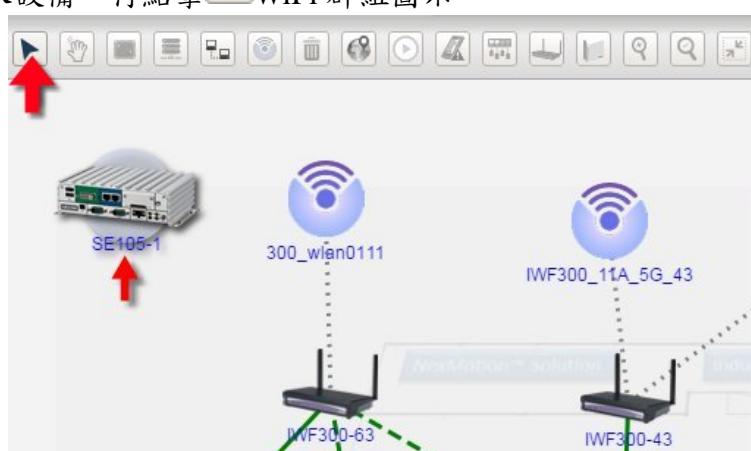


圖 141 選取歸納的設備

(2)跳出 WiFi 群組清單，選擇要歸入的 WiFi 網段，點擊 OK 確認，設備圖示就會進入網段圖示  中。

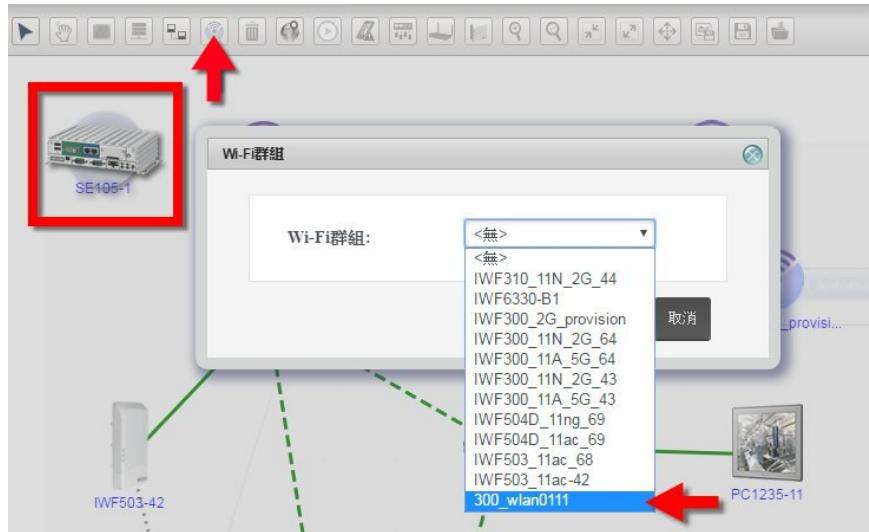


圖 142 選擇 WiFi 網段

(3)若需要將設備移出 WiFi 群組，則進入  中，選取設備，再點擊 WiFi 群組圖示，選擇網段「無」，則設備退出此 WiFi 網段。



圖 143 移出 WiFi 群組

(4)使用者點入 WiFi 群組後，功能列會多一個「返回」 圖示，若想回到上一層拓樸圖，可點擊之。



圖 144 返回拓樸圖層

刪除：刪除設備或連線，可使用 選取設備或連線，再點擊 刪除。系統刪除設備或連線前，會有警視窗，點擊「確認」後才會刪除。



圖 145 刪除設備

地圖：點選圖示選擇以 google 地圖或 百度地圖呈現拓樸。以地圖顯示拓樸群組與設備的位置。以滑鼠滾輪放大縮小地圖比例，縮小時系統以數字顯示該地區拓樸群組及設備的數量。

- (1)需事先於 6.1.2 設備列表章節或 6.6 拓樸群組設定經緯度，才能在地圖上顯示設備或群組的位置。
- (2)系統需連上網路，才能顯示地圖，點擊設備，可顯示設備名稱與經緯度，點擊「返回」可回到拓樸頁面。



圖 146 地圖

 流量監測：系統可同時監測所有連線的流量，也可以針對某條連線設定閥值，啟用監控功能，當流量超過閥值時可警告管理者。設定方式如下：

(1)按下  流量監控圖示，即可同時監控拓樸圖中所有的連線(綠色虛線與綠色實線)。滑鼠移至任一連線上，可顯示連線送出與收到的流量。



圖 147 連線流量顯示

(2)連線的流量若超過 20MB 會變粗，超過 100MB 會變更粗。

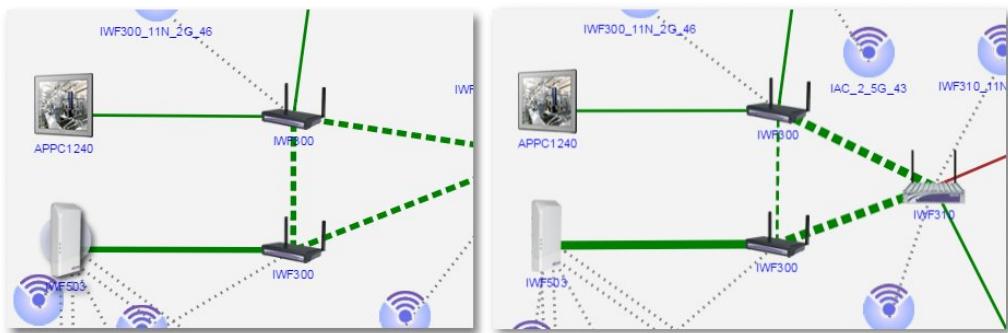


圖 148 流量大連線則粗

(3)另外，可針對單一連線啟用監控警報功能。先選取連線，右鍵點擊「流量監測」。



圖 149 點選流量監測

(4)跳出「流量監測」子視窗，啟用流量監測，設定「監測間隔秒數」與「監測警戒值」，並選擇超過警戒值時，發送電子郵件訊息的對象，點擊 OK 確認。



圖 150 設定監測閥值

(5)回到拓樸圖上，連線上方多了監控圖示，表示已經開始進行監測。

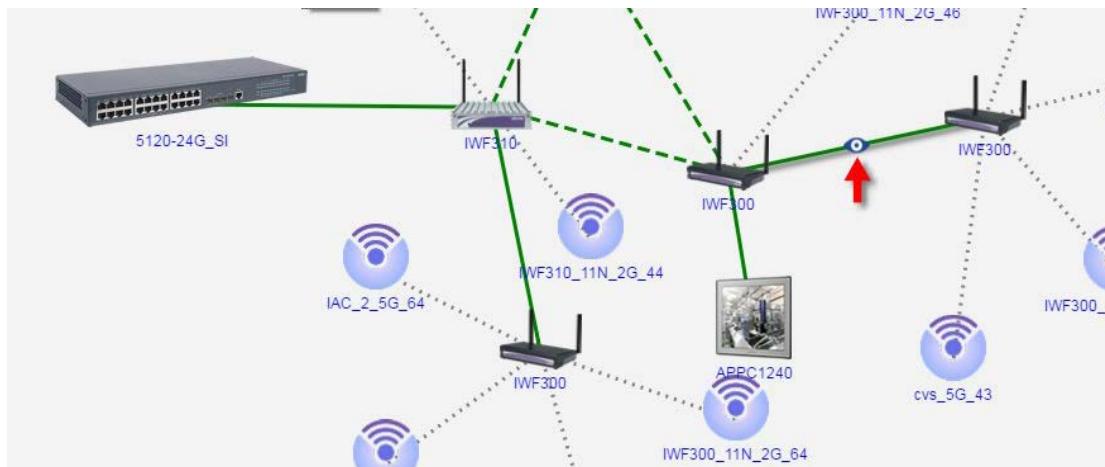


圖 151 開始監測

(6)當連線流量超過閥值，拓樸圖上連線變成橘色，並將發送訊息警告管理者。



圖 152 連線超過閥值

(7)需取消流量監測，可進入流量監測設定子視窗，取消勾選「啟用」，即可關閉監測。



圖 153 取消流量監控

(8)若開啟全拓樸圖的 連線流量監測，同時又針對單一連線進行流量警報設定，則超出閥值時，連線會變粗，且變成橘色，並發送警報訊息給管理者。

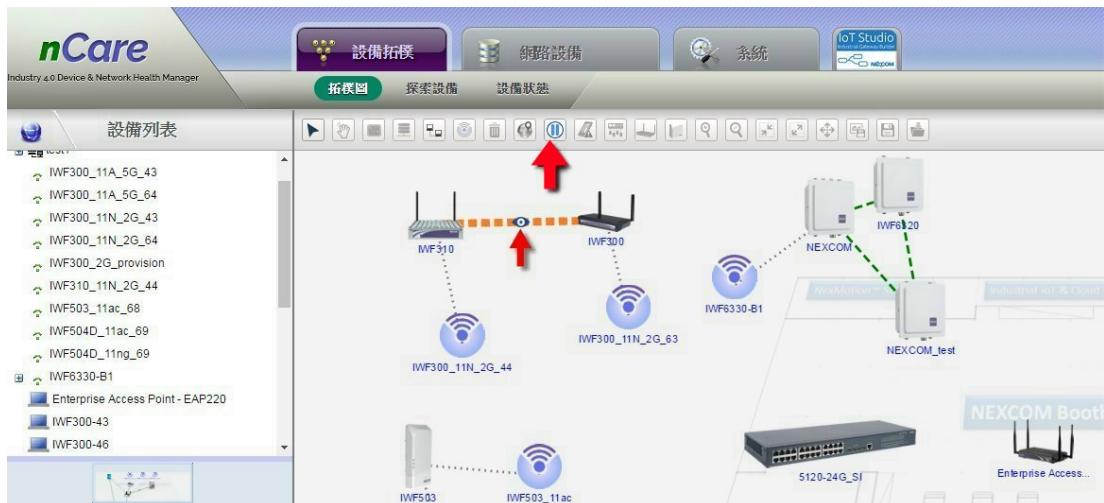


圖 154 同時進行兩種流量監控

顯示/隱藏非法設備：點擊顯示非法設備，則沒有列在白名單(白名單設定方式請見 6.7.2.2 章節)的設備旁，將有紅色驚嘆號提示。



圖 155 顯示非法設備的警告

 交換器虛擬區域網路：此功能可顯示主向位交換器設備的虛擬區域網路(VLAN)的網路拓樸線路圖。

(1)點選  圖示後，會跳出預先設定好的 VLAN 選單，提供管理者選擇。



圖 156 選擇 VLAN

(2)點選後，則以藍線顯示此 VLAN 內設備之邏輯配置概況。



圖 157 顯示 VLAN 拓樸

 更新 AP：可針對 IWF AP 設備進行更新。

(1)沒有圈選任何設備，點擊 ，即跳出「確定要更新所有 IWF AP 嗎？」、「警告：更新所有 IWF AP 可能會需要幾分鐘的時間」。點擊「確定」可開始更新。



圖 158 更新所有 IWF AP

(2)選擇了非 IWF AP 設備，再點擊 ，則會跳出「找不到 IWF AP」警告視窗。使用者需要選擇 IWF AP 設備才能啟動更新。



圖 159 找不到 IWF AP 設備

 **更新 IWSN：**可針對 NIO200 系統的設備進行掃描與更新。

(1)右鍵點擊「NIO200-HAG」設備，跳出快捷視窗，選擇「設定」-「帳號設定」。



圖 160 NIO200-HAG 設備之帳號設定

(2)跳出「帳號設定」視窗，填入帳號與密碼，選擇「確定」。



圖 161 填寫 NIO200-HAG 設備的帳號密碼

(3)跳出設備設定成功的訊息視窗，選擇「確定」。若顯示「設定失敗」，代表密碼可能已被他人修改，請確認新的密碼後，重新輸入帳密以做設定。



圖 162 NIO200-HAG 設備的帳號設定成功

(4)點擊拓樸圖功能鍵  「更新 IWSN 」。



圖 163 更新 IWSN

(5)開始掃描此台「NIO200-HAG」設備。



圖 164 掃描 NIO200-HAG 設備

(6)掃出「NIO200-HAG」設備底下以 WirelessHART 連線之群組設備。



圖 165 掃出 NIO200-HAG 之群組設備

(7)雙點擊群組設備圖示，可進入查看此 Sensor Group 之設備資訊，游標移至設備上方，可顯示設備資訊。

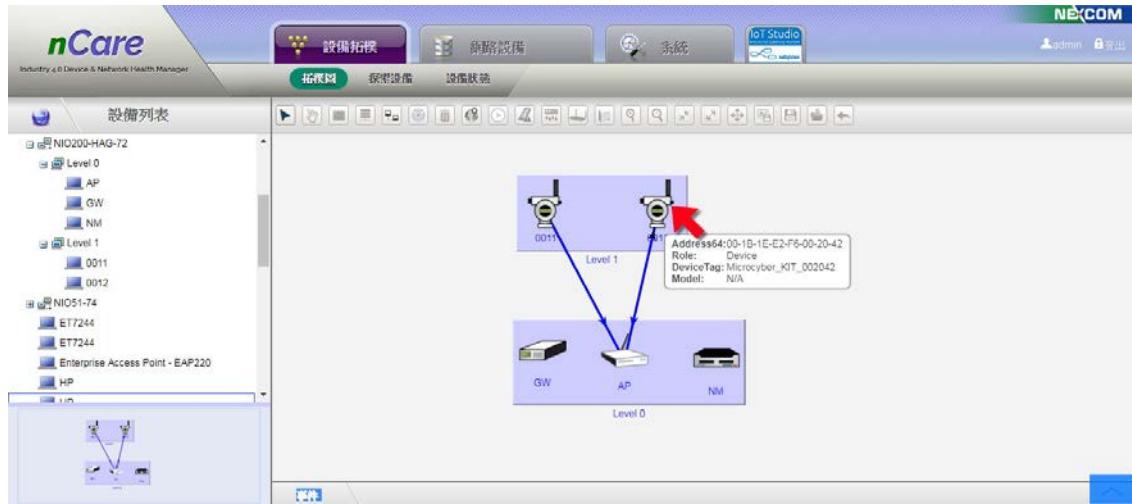


圖 166 查閱 NIO200-HAG 群組設備

(8)當 NIO200-HAG 之群組設備斷線時，系統線路顏色將顯示紅色作為警告。

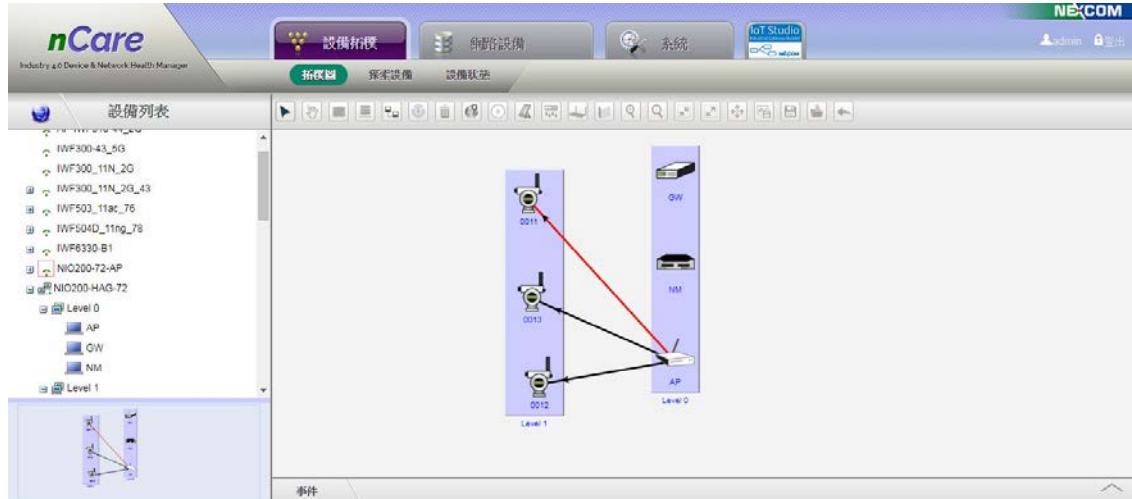


圖 167 NIO200-HAG 群組設備斷線

(9)設備為「NIO200-IAG」設備，點擊右鍵跳出快捷視窗，選擇「設定」-「I 帳號設定」。後續搜尋與查閱流程同「NIO200-HAG」設備，帳號密碼設定完畢後，點擊 「更新 IWSN」圖示。



圖 168 NIO200-IAG 設備之帳號設定

(10)更新後，即可掃出 NIO200-IAG 的 ISA100 群組設備。

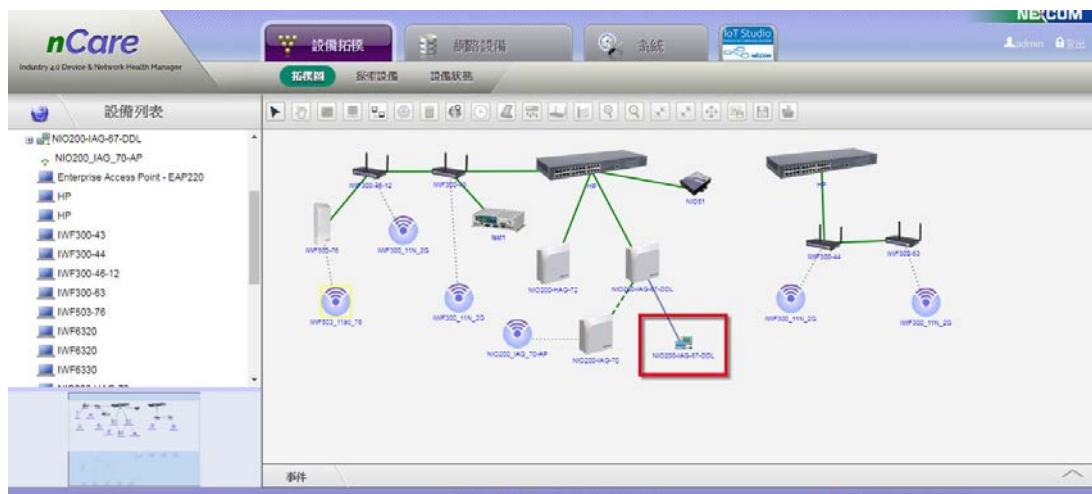


圖 169 掃出 NIO200-IAG 的 ISA100 群組設備

(11)點擊 ISA100 群組圖示，進入內容查閱設備資訊，當設備有斷線時，系統也會以顏色顯示警告。

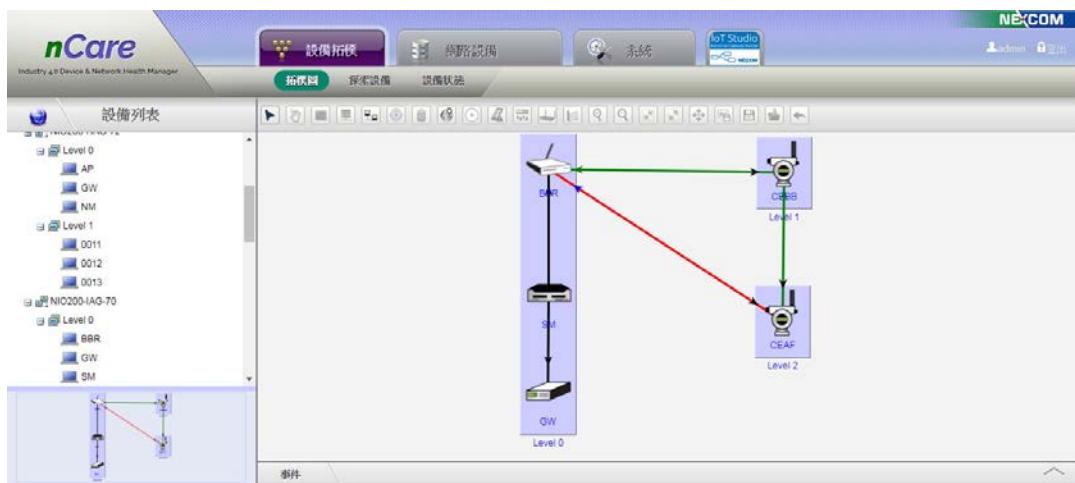


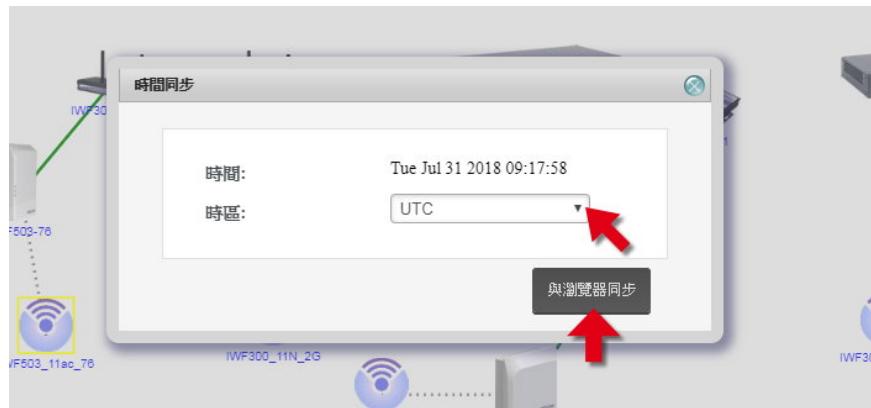
圖 170 查閱 ISA100 的設備資訊

(12)nCare 拓樸圖可設定「NIO200」設備之所屬時區。以右鍵點擊「NIO200」系列設備，跳出快捷視窗，選擇「設定」-「時間同步」。



圖 171 設定 NIO200 系列設備之時區

(13)跳出「時間同步」視窗，以下拉式選單選擇時區，再點擊「與瀏覽器同步」完成設定。



放大：可放大整個設備拓樸圖。

縮小：可縮小整個設備拓樸圖。

全覽：點選此功能後，可顯示拓樸圖中的所有設備。

原始大小：點選此功能後，即顯示原始大小之拓樸圖。

全螢幕：以全螢幕操作拓樸圖。再以「ESC」或 跳回系統主畫面。



匯出成圖檔：此功能可複製拓樸全覽圖。點選此功能後跳出分頁，再以右鍵下載 png 格式圖檔儲存。



儲存拓樸：系統可儲存記憶拓樸圖。點選此功能後，確認儲存拓樸圖。跳出「存檔成功」子視窗，即完成儲存。



圖 172 儲存拓樸



開啟拓樸：儲存拓樸後，若有對拓樸圖進行移動或修改，想回復原來的拓樸圖，可點擊「開啟拓樸」，確定重新載入拓樸，則拓樸圖會回復到未移動或修改的狀態。



圖 173 重新載入拓樸



更新 Device Server：點擊型號「NIO50」或「NIO51」設備，工具列會產生一個隱藏版的功能圖示。操作方式如下：

(1)選取 NIO50 或 NIO51 設備，再點擊功能列圖示。



圖 174 更新 NIO50 設備

(2)點擊後，系統跳出「請設定 Modbus 編號」提示訊息，需先設定此台 NIO50 設備要納管 PLC 設備之台數。



圖 175 設定 Modbus 編號訊息

(3)設定方式為，選取此設備並按右鍵，跳出快捷功能，點擊「Modbus 編號設定」。



圖 176 設定 Modbus 編號

(4)跳出「Modbus 編號設定」視窗，填寫「設備 ID」(僅能填寫 1~255 整數數字)後，點擊「新增」。若要刪除新增的設備 ID，則勾選後，點擊「刪除」。



圖 177 設定 Modbus 編號快捷鍵

(5)設定後，選取此台 NIO50 設備，並點擊 功能鍵，系統即針對此台設備掃描更新資訊。



圖 178 掃描 NIO50 設備

(6)掃描後，此台 NIO50 設備，會自動歸入所屬的 WiFi 網段群組中。



圖 179 NIO50 歸入 WiFi 羣組

(7)雙點擊 WiFi 羣組，進入可查看 NIO50 以及設定好的 PLC 設備群組。

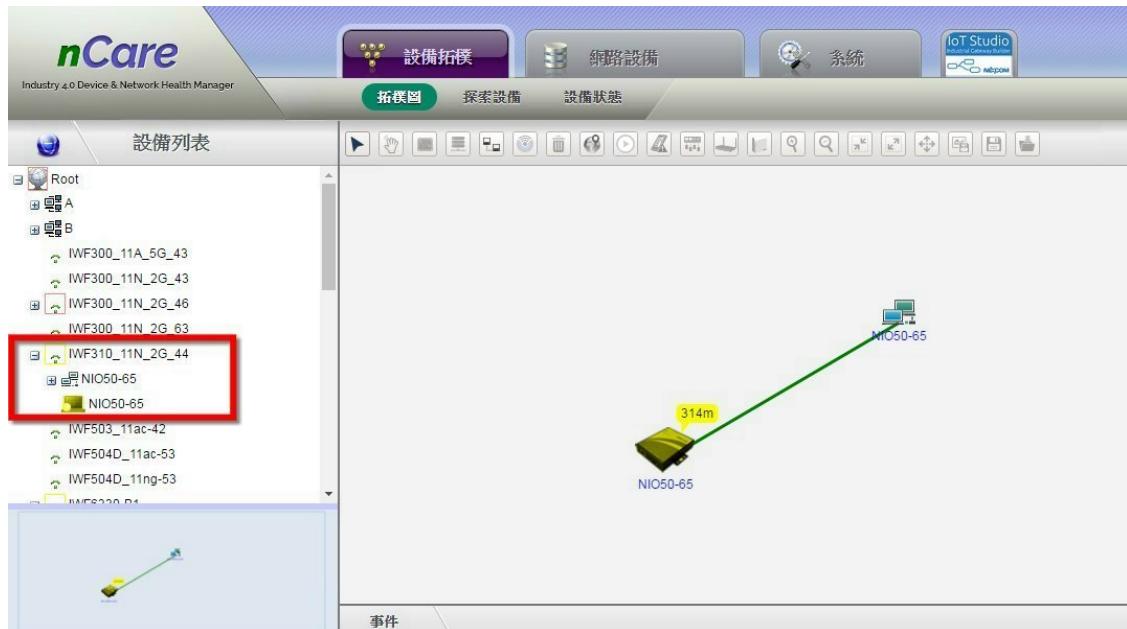


圖 180 WiFi 羣組內的設備

(8)雙點擊 PLC 羣組 ，可進入群組中查閱 PLC 設備。點擊「返回」  可回到上一層。



圖 181 PLC 群組內的設備

(9)點擊設備右鍵，選擇「狀態」，可看見系統已經更新設備資訊。

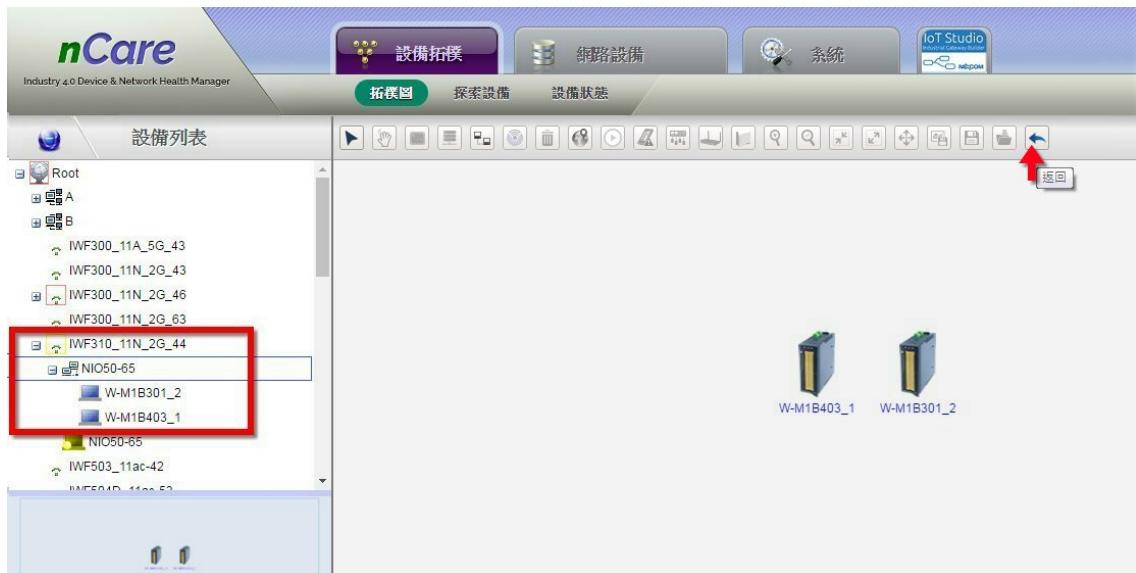


圖 182 NIO50 設備資訊更新

(10)此外，點擊 NIO50 設備右鍵，選擇「設定」-「Modbus 排程」，可設定排程自動抓取更新 PLC 的資料。



圖 183 設定 Modbus 排程

(11)跳出「Modbus Schedule」，選擇「開始時間」、「週期」，再點擊「Add to Schedule」。



圖 184 設定排程時間與週期

(12)也可以直接右鍵點擊 PLC 設備，進入「狀態」頁面，選擇「即時狀態」去更新 PLC 資訊。



圖 185 即時更新 PLC 資料

(13)NIO51 設備設定流程與 NIO50 相似，設定好 NIO51 的 PLC 設備群組後，雙點擊群組圖示 ，可進入群組中查閱 PLC 設備。



圖 186 NIO51 的 PLC 群組

(14)進入 NIO51 之 PLC 設備群組中，可查閱設備狀態，點擊「返回」可回到上一層。

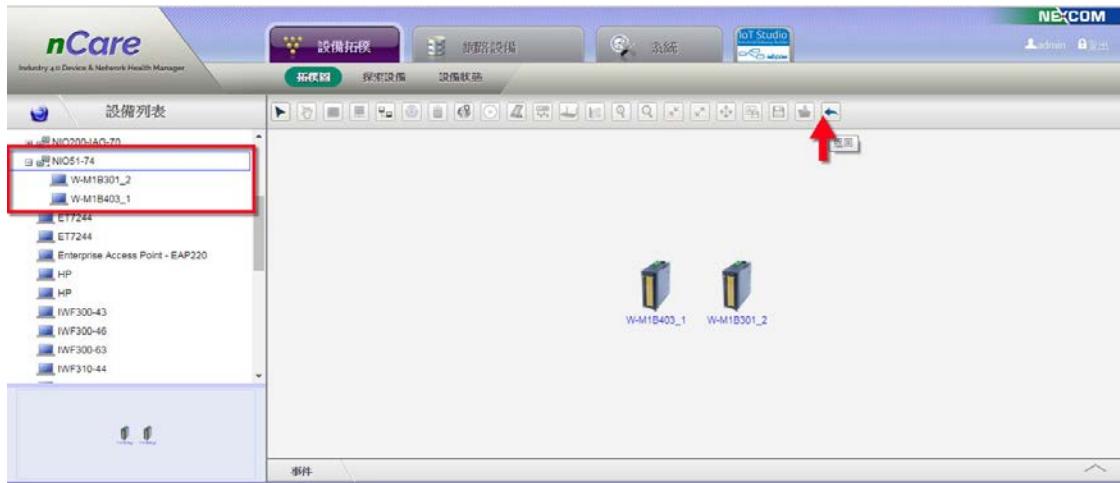


圖 187 查閱 NIO51 之 PLC 設備資訊

(15)右鍵點擊 PLC 設備右鍵，選擇「狀態」，可查閱 PLC 設備資訊，並可編輯設備的暫存器表。



圖 188 編輯 NIO51 的 PCL 設備

7.1.2.3. 拓樸圖警訊訊息

(1)顏色顯示：設備回傳異常狀況，並以顏色顯示警報的嚴重程度。設備圖示無訊息，表示正常；設備顯示黃色訊息，表示有重要警訊。紅色表示嚴重警訊。



圖 189 設備顏色警訊

(2)文字顯示：系統持續輪詢設備狀態，以數字顯示警告紀錄次數、以「c」表示嚴重警訊，「m」表示重度警訊。例如「1m」則表示有一個重度警訊，「2c+」表示有兩個嚴重警訊，「+」表示此設備除了兩個嚴重警訊，還有其他重度警訊。

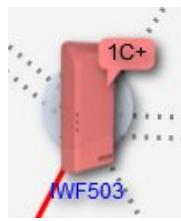


圖 190 數字警訊

7.1.2.4. 拓樸圖網路連線

(1)綠色實線：設備以一條乙太網路線連結，以綠色實線表示。

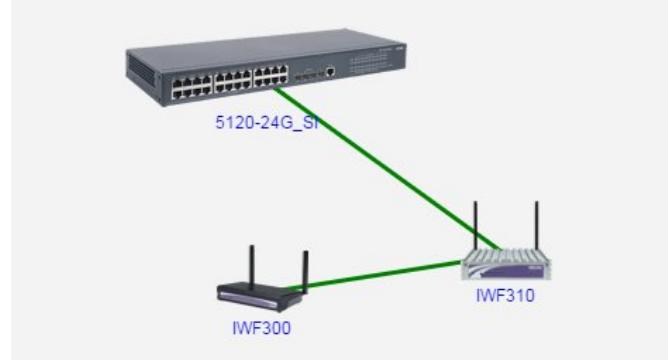


圖 191 乙太網路連線

(2)深綠色粗實線：粗線表示「埠彙聚/端口匯聚(Trunk)」，若為兩條以上乙太線之埠彙聚，則顯示粗的綠色實線。

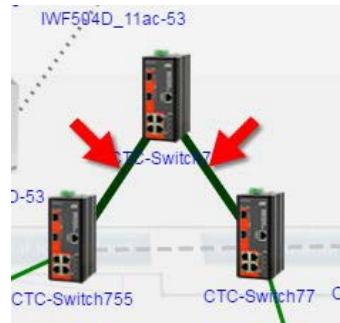


圖 192 深綠色粗實線

(3)當滑鼠移至乙太線的匯聚線路上方，可顯示Trunk端口的資訊。

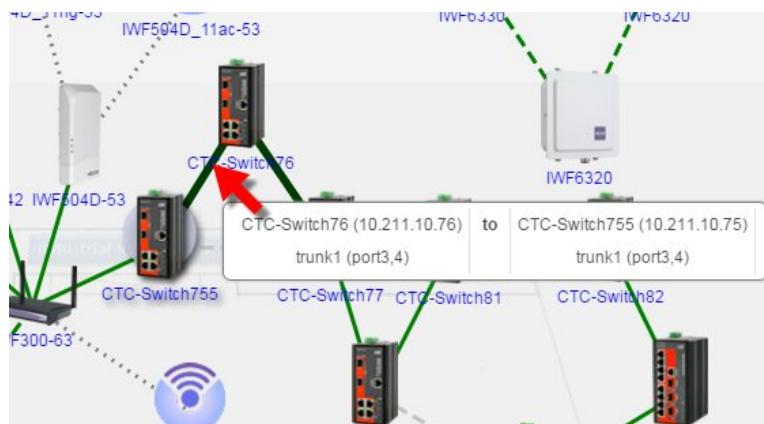


圖 193 乙太線埠彙聚端口資訊

(4)綠色虛線：若設備為 Mesh 無線網路連線，則以綠色虛線顯示。

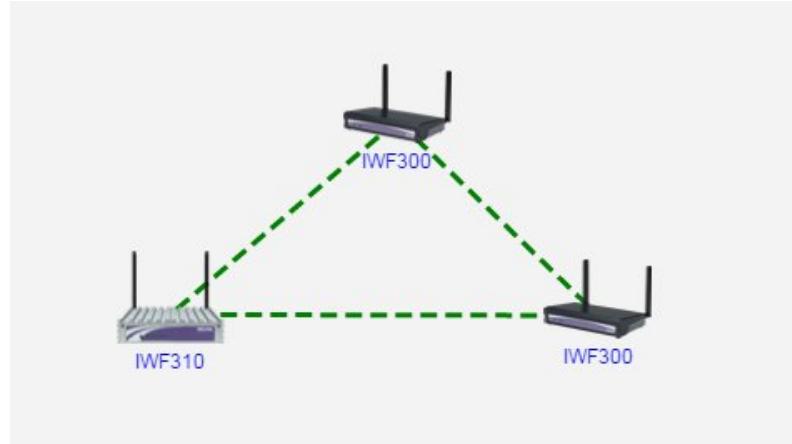


圖 194 Mesh 無線網路連線

(5)灰色點線：以灰色點線顯示 WiFi 連線，以  圖示顯示不同網域介面的名稱，如 CVS_2G_64。



圖 195 WiFi 連線

(6)點擊圖示可進入該 WiFi 網段，查看網段內有連線的設備。



圖 196 網段內的設備

(7)灰色虛線：表示設備雖有乙太線路連接，但為關閉(block)的狀態。若設備

偵測到乙太網路線路故障，會自動啟用灰色虛線的備援路徑。

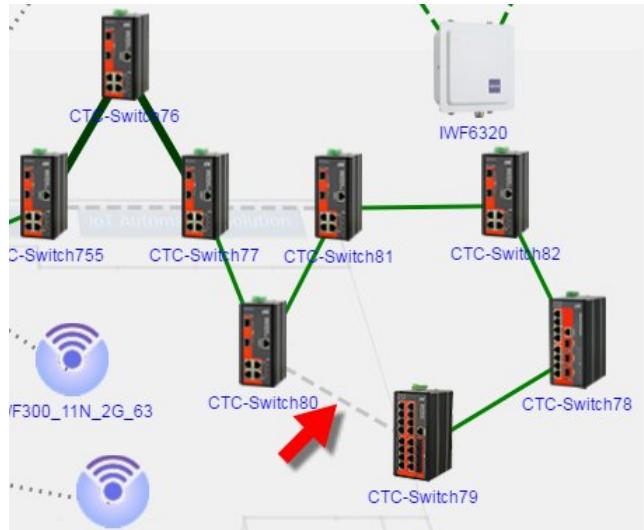


圖 197 灰色備援虛線

(8)紫色細線：若設備有一條乙太線，及兩條以上之 Vlan，則顯示為細的紫色線。

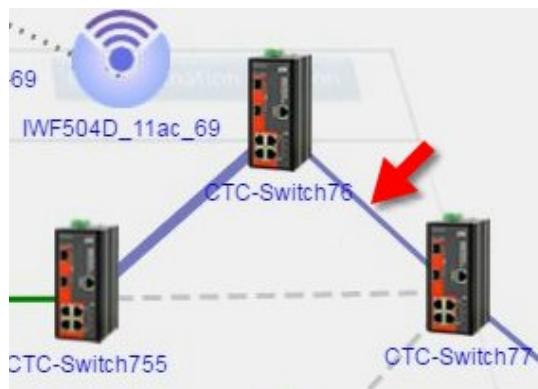


圖 198 細的紫色線

(9)粗的紫色線：若設備有兩條以上乙太線，及兩條以上之 Vlan，則顯示為粗的紫色線。

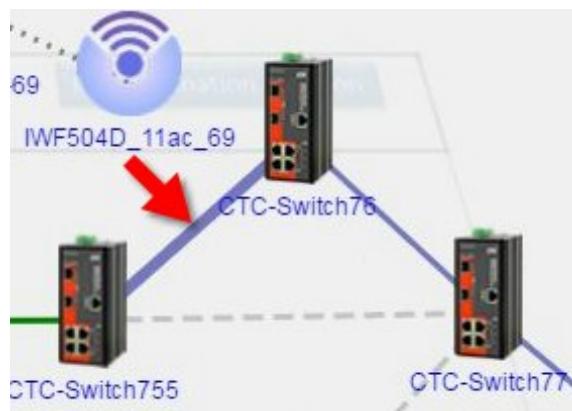


圖 199 粗的紫色線

(10)當滑鼠移至紫色 Vlan 線路上方，顯示 Vlan 端口的資訊。

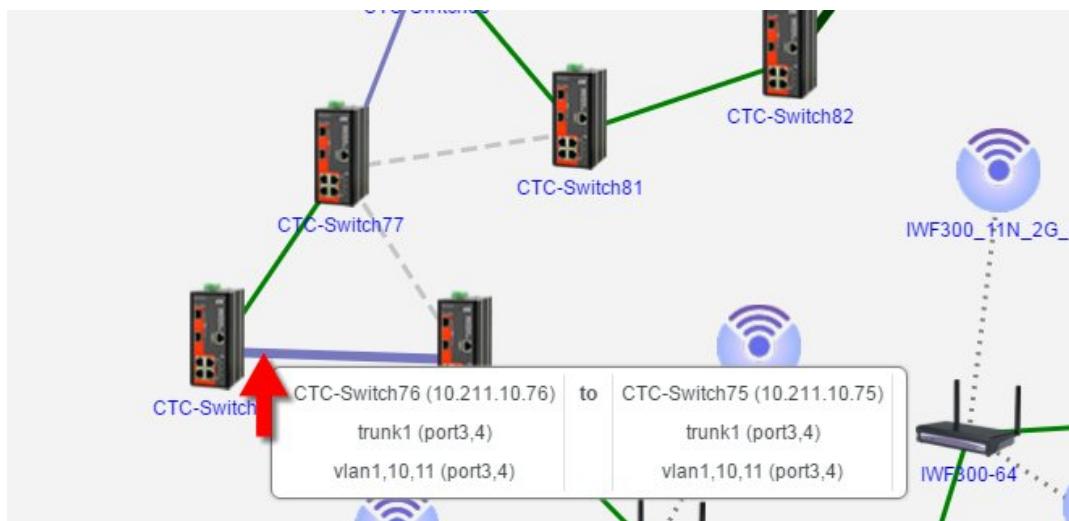


圖 200 VLAN 端口資訊

7.1.2.5. 拓樸圖鏈路狀態

(1)綠色細線：表示設備網路連線正常。



圖 201 綠色連線

(2)綠色粗線：比細線略粗的連線，表示流量超過 20MB；更粗的連線，表示連線流量超過 100MB。

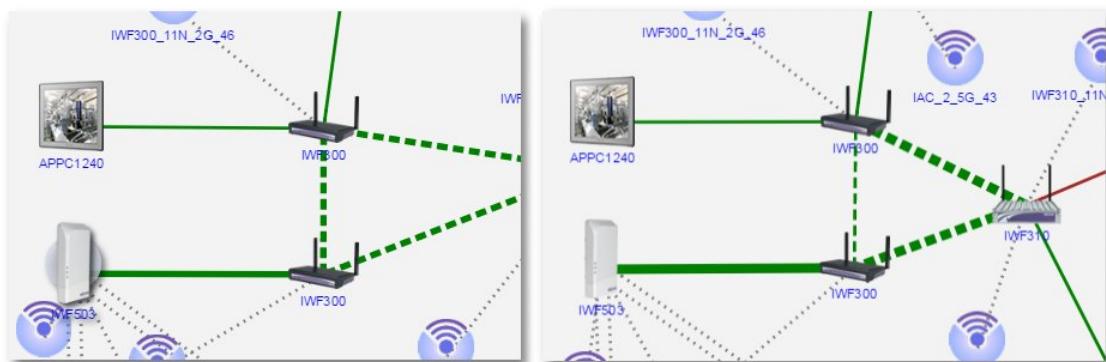


圖 202 綠色粗線

(3)紅色線：表示設備網路斷線。



圖 203 紅色連線

(4)橘色線：表示連線的流量超過使用者設定的閥值。



圖 204 橘色連線

7.1.2.6. 拓樸圖快捷鍵

設備上以滑鼠按右鍵，可顯示快捷功能鍵。依據設備類型，快捷鍵可直接跳至此設備之狀態、使用率、事件記錄頁面，或進行網頁設定、Ping 或重啟等功能。



圖 205 設備快捷鍵

- (1) 狀態：可直接跳至此設備的「設備狀態」頁面。
- (2) 使用率：可直接跳至此設備的「使用流量」頁面。
- (3) 事件紀錄：可直接跳至此設備的「日誌」頁面。
- (4) 設定：點此功能則可進入此設備的設定網頁，或可直接進行資訊修改、設備組態備份、組態還原、韌體更新等功能。
- (5) Ping：點此功能可主動偵測此設備網路是否連通，由設備回應的時間得知封包傳送的順暢度。點選下方的「Ping」可以再次偵測設備數值，點選「取消」則回到拓樸圖頁面。



圖 206 Ping 功能

- (6) 重啟：可直接針對此設備執行重新開機。

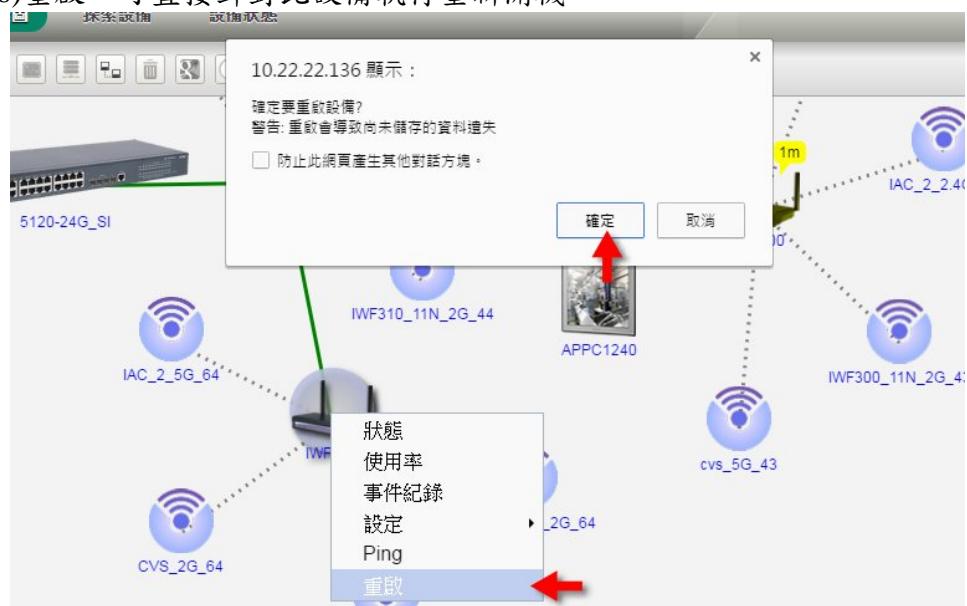


圖 207 重啟功能

7.1.2.7. 遠端桌面

設備若為 IPC 設備，點擊右鍵快捷選單，「設定」-「遠端桌面」，可遠端進入 IPC 設備之桌面進行操控(請先與新漢公司索取遠端桌面安裝包，安裝啟用後即可由 nCare 進入)。



圖 208 遠端桌面

7.2. 探索設備(Discovery)

7.2.1. 探索設備說明

nCare 可設定設備的 IP 範圍或使用的溝通協議，由系統自動探索出條件內所納管的設備，並於拓樸展示頁面中，將設備連接關係繪出。

*每台設備的 device name 必須包含 device series 字眼。

7.2.2. 探索設備操作

(1)輸入欲探索之設備的「IP 區段」，勾選通訊協議「全選」、「CAPWAP」、「SNMP」或「Modbus」，若有使用 SNMP，則可以選擇協議版本。並填入「讀取共同碼(預設為 public)」、「寫入共同碼(預設為 private)」，最後點擊下方「Scan」開始探索。



圖 209 探索設備

(2)探索功能可記錄最近四筆輸入的 IP 位址。

起始IP位址: . . .

結束IP位址: . . .

通訊協定: 全選 CAPWAP SNMP

Trap設定:

Syslog設定:

SNMP版本: V1/V2C

讀取共同碼: public

寫入共同碼: private

掃描

圖 210 IP 位址記憶欄位

(3)僅勾選 CAPWAP 通訊協定時，若不填寫設備 IP 範圍，則可搜尋與主機伺服器同區域網段，且支援 CAPWAP 通訊協定的設備，如有跨網段搜尋設備之需求，可勾選 SNMP 來達成。

起始IP位址: . . .

結束IP位址: . . .

通訊協定: 全選 CAPWAP SNMP Modbus

Trap設定:

Syslog設定:

SNMP版本: V1/V2C

讀取共同碼: public

寫入共同碼: private

掃描

圖 211 不定範圍 CAPWAP 探索設備

(4)僅勾選 CAPWAP 通訊協定，且設定 IP 範圍時，nCare 僅能探索與主機伺服器同區域網域內，且支援 CAPWAP 的設備。如下圖，nCare 安裝於 10.211.10.0 之 Class C 網段，nCare 僅能搜尋到的設備位址為 10.211.10.1~254，而 10.211.11.X 之設備則無法搜尋。



圖 212 設定範圍 CAPWAP 探索設備

(5)按下「掃描」後，即顯示搜尋的百分比。



圖 213 探索進度

(6)完成 100%後，拓樸圖頁面與設備列表，皆可顯示探索出的設備。



圖 214 顯示探索出的設備

7.3. 設備狀態(Status)

7.3.1. 設備狀態功能說明

nCare 可監測納管設備之核心資訊，包含基本資訊、參數(如 RSSI、Cost 等)與設備設定值，用以瞭解設備運作狀態。

7.3.2. 設備狀態功能操作

- (1)由左方設備列表，選擇需要查看的設備，依據不同的設備產生不同的資訊欄位，如 IWF 設備狀態，可呈現 IP 位址、經緯度基本資訊，或是介面、用戶清單、基地台掃描等資訊。

名稱	種類	MAC	頻道	Tx Kbps	Rx Kbps	AssocClient
lo	loopback	-	-	3141	3141	0
eth0	ethernet	00:10:03:30:8b:03	-	5887360	437454636	0
br-lan	ethernet	00:10:03:30:8b:03	-	844278	1322308	0
eth0.2	ethernet	00:10:03:30:8b:03	-	2144279	431183065	0
eth0.3	ethernet	00:10:03:30:8b:03	-	1343889	798775	0
eth0.4	ethernet	00:10:03:30:8b:03	-	1131594	0	0
eth0.5	ethernet	00:10:03:30:8b:03	-	1131594	0	0
eth0.1	ethernet	00:10:03:30:8b:03	-	808	0	0
wlan0	wireless	00:10:03:30:8b:05	11	1245366	0	0
wlan1	wireless	00:02:03:04:05:06	36	447821576	690938	0

MAC	IF	訊號強度	Tx	Rx
2g64_2	11	-54	80%	06:10:F3:30:8B:71

圖 215 IWF 系列設備狀態

- (2)IPC 系列設備，則可顯示由 Modbus 獲取的相關資訊如：設備資訊、硬體監控、GPIO 資訊。

設備資訊

Modbus | WMI

APP1235-11test

平臺

設備ID: 00:10:03:4a:8e:0a
設備名稱: APP1235-11test
型號: APPC Series
BIOS名稱: AD27
CPU類型: i46 Family 6 Model 54 Stepping 1/GenuineIntel
記憶體容量: 4.095MB

儲存設備

型號名稱: Hitachi_HTE543232A7A3
總軌數: 0
儲存空間: 305,243.33MB
已使用空間: 31,482.04MB

圖 216 IPC 系列設備狀態

- (3)IPC 設備還可由 WMI(Windows Management Instrumentation)進入，監控查閱其資源。點擊 WMI 後跳出「WMI Verification」視窗，輸入此台 IPC 設備之帳號密碼，再點擊「Submit」。



圖 217 IPC 系列設備 WMI 功能

(4)進入 WMI 頁面後即可查閱此設備之 MAC、種類、BASEBOARD、BIOS、CPU...等資源參數。

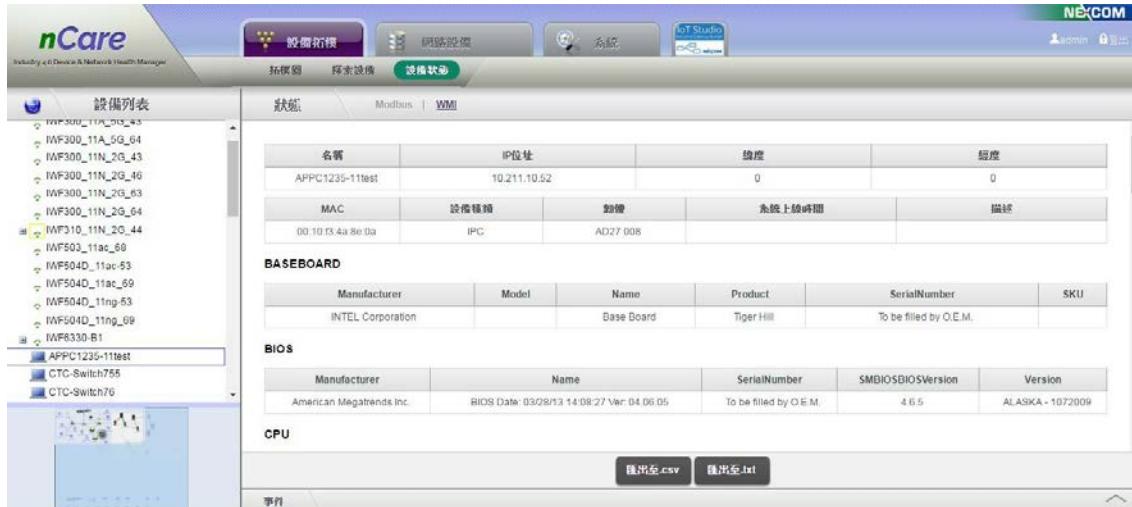


圖 218 IPC 系列設備 WMI 頁面

(5)若為 NIO50 底下的 PLC 設備，其設備狀態分為「歷史狀態」與「即時狀態」，可查閱設備名稱、IP 位址及經緯度與暫存器表。



圖 219 PLC 設備歷史狀態

(6)PLC 設備由「即時狀態」頁面進入，可對「暫存器表」作編輯。點擊「編輯」，進入修改列表。

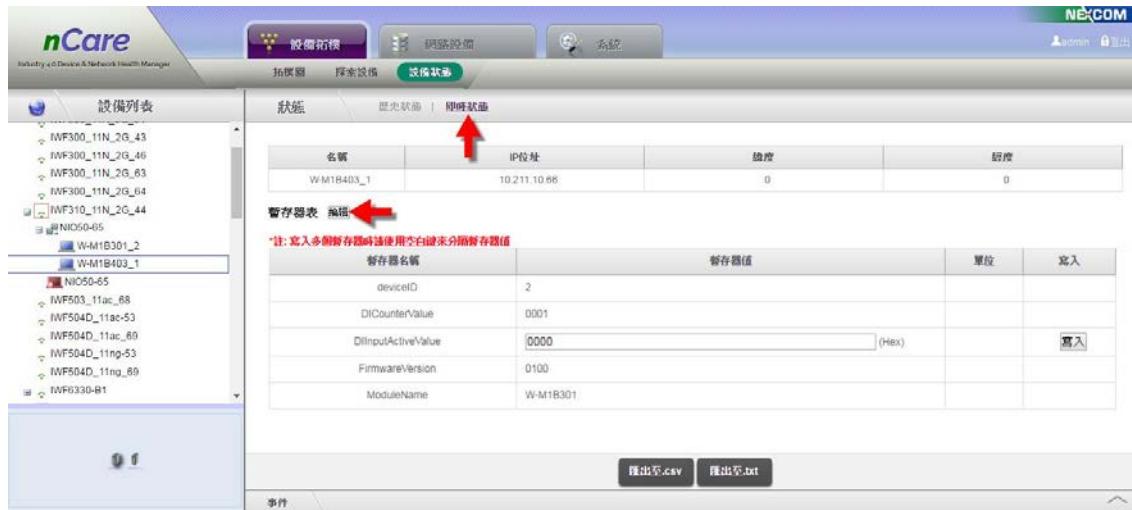


圖 220 編輯暫存器列表

(7)可「新增」與「刪除」暫存器列表。點擊「新增」後，填寫「暫存器名稱(限英文開頭)」、「單位」、「功能碼」、「點位偏移」及「字數」，「屬性」欄位可選擇欄位僅可讀(R)/欄位可編輯(W)/欄位可讀取資訊也可編輯(RW)，以及選擇「W」者，可再進一步設定「暫存器值」，最後再點擊「儲存」完成設定。



圖 221 新增暫存器列表

(8)完成暫存器列表新增後，自動回到前一頁，即可看見新增的暫存器資訊顯示於列表中。可編輯的「暫存器名稱」後方即有「暫存器值」的欄位可以直接填入資料，並點擊「寫入」編輯資訊。

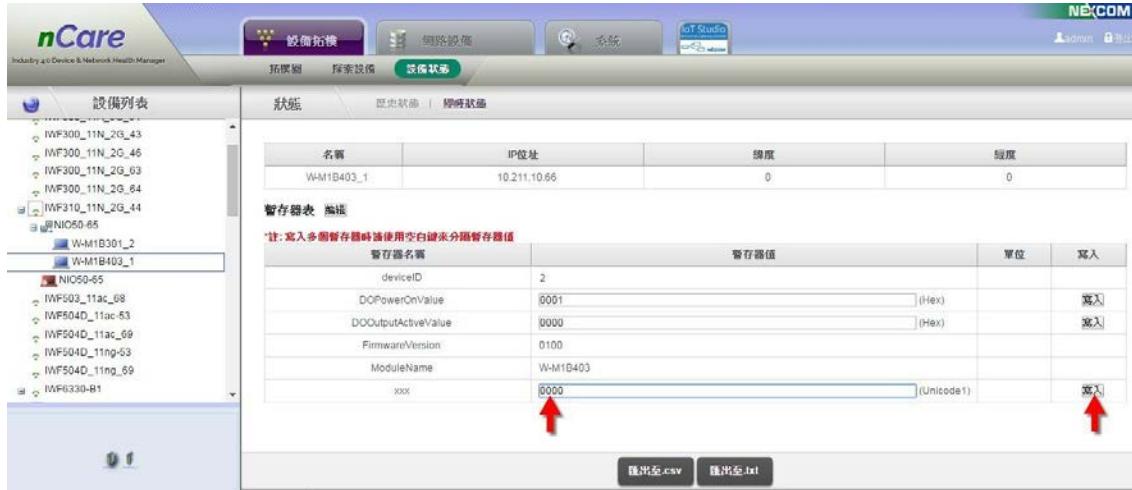


圖 222 寫入暫存器資訊

(9)「設備狀態」頁面，不管是 IWF 或 PLC 設備，若需要匯出檔案，點選下方「匯出至 CSV」或「匯出至 txt」即可匯出附檔名為.csv 或.txt 之資訊列表。



圖 223 匯出設備狀態

(10)若為 NIO51 底下的 PLC 設備，其設備狀態可查閱設備名稱、IP 位址及經緯度，並可編輯暫存器表。



圖 224 NIO51 的 PLC 設備狀態

(11)若為 NIO200-HAG 設備，其設備狀態的「Devices List」分頁可查閱設備基本資訊、界面、用戶清單、基地台掃描外，還可設定與更新「Wireless HART Devices List」和「Wireless HART Command Logs」的資訊。

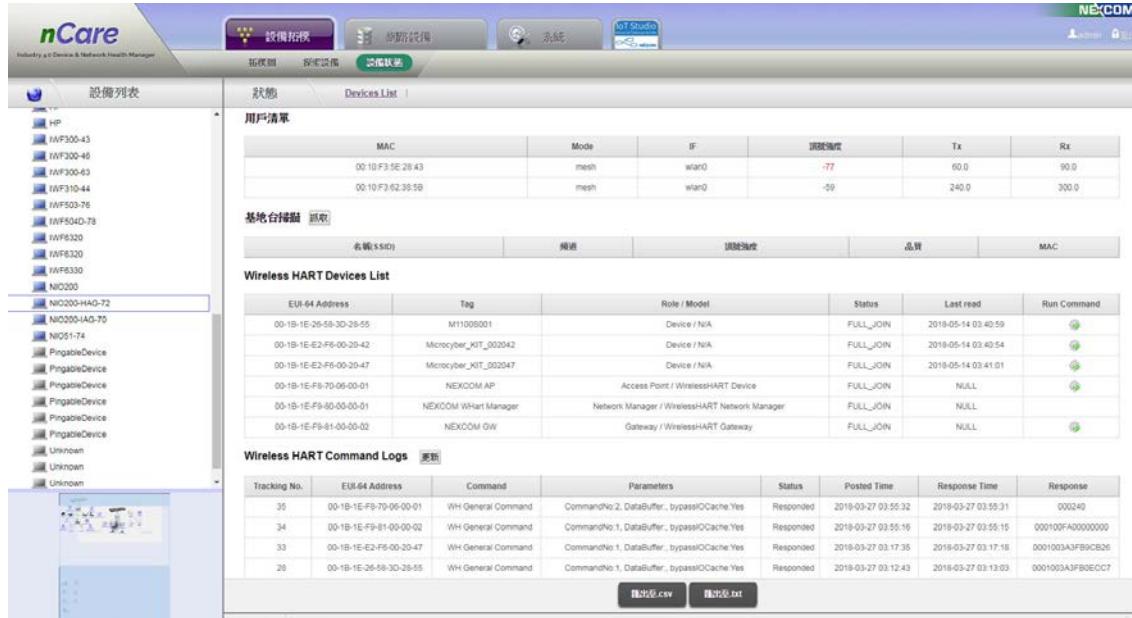


圖 225 NIO200-HAG 的設備狀態

(12)「Wireless HART Devices List」中除顯示「EUI-64 Address」、「Role / Model」、「Status」等資訊外，還可對設備「Run Command」進行設定。

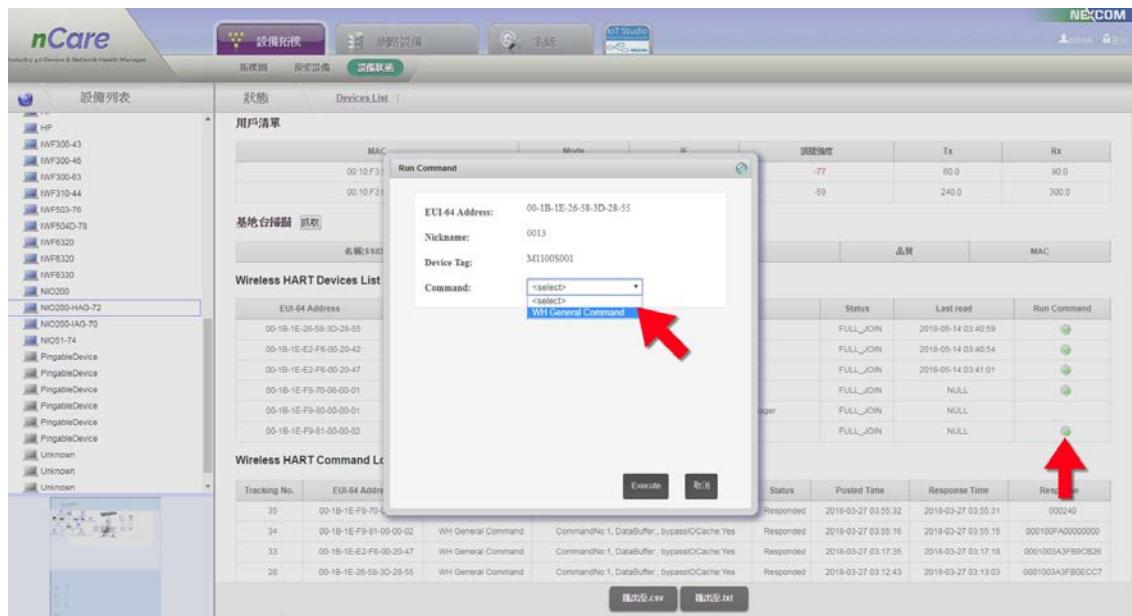


圖 226 NIO200-HAG 設備的 Run Command

(13)若為 NIO200-IAG 設備，其設備狀態有「Devices List」和「Trouble Shooting」分頁，「Devices List」可查閱設備基本資訊、界面、用戶清單、基地台掃描外，還可設定與更新「ISA100 Devices List」和「ISA100 Command Logs」的資訊。

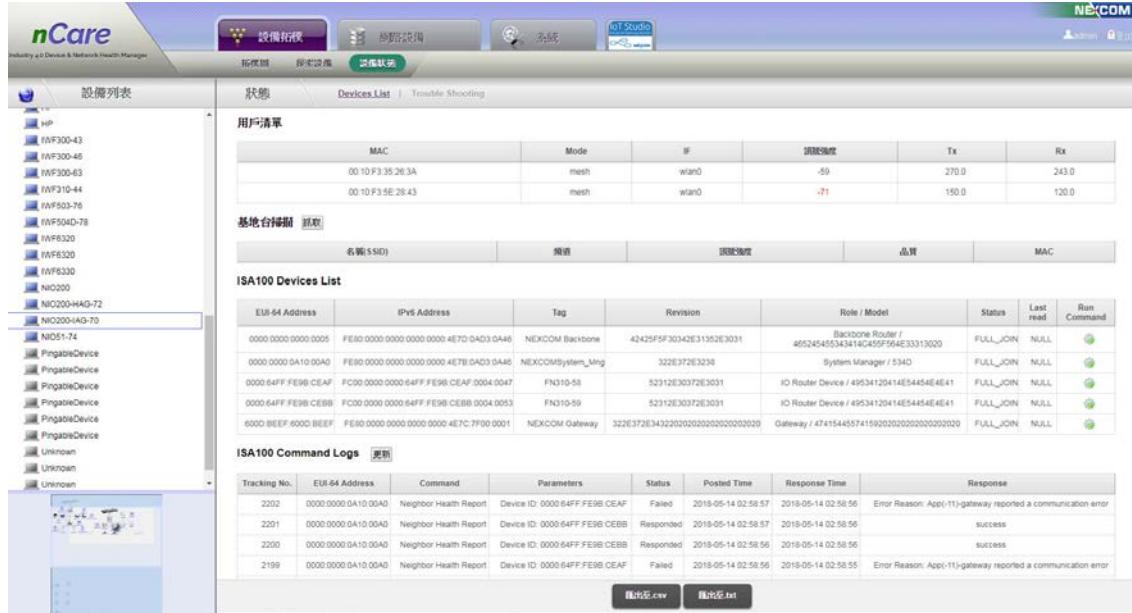


圖 227 NIO200-IAG 的設備狀態

(14)「Devices List」分頁中除顯示「EUI-64 Address」、「Role / Model」、「Status」等資訊外，還可對設備「Run Command」進行設定。

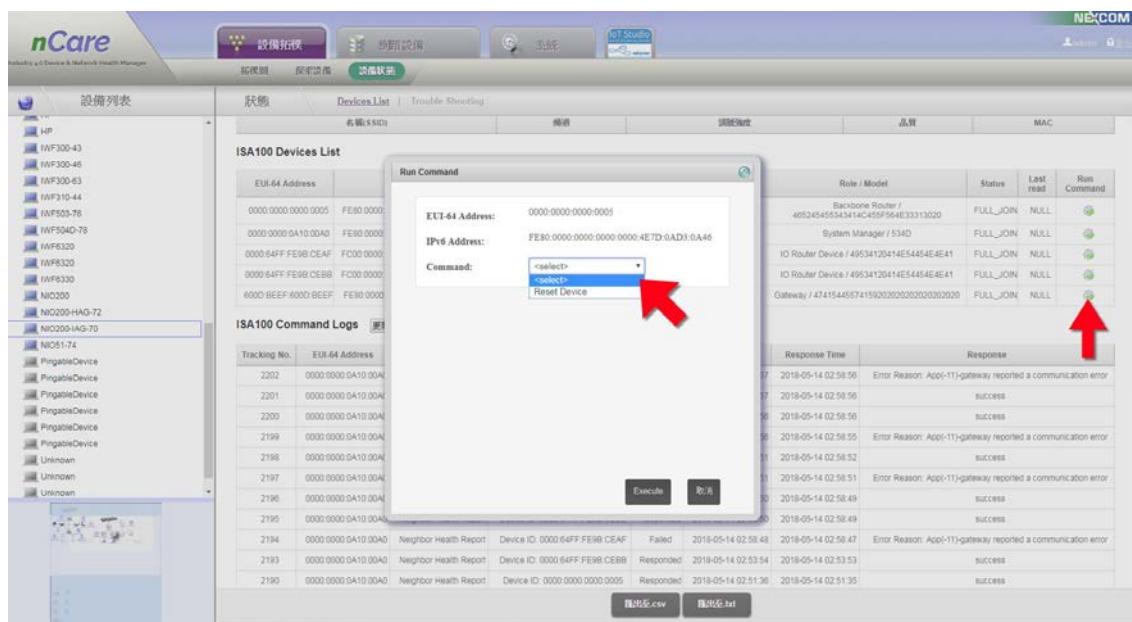
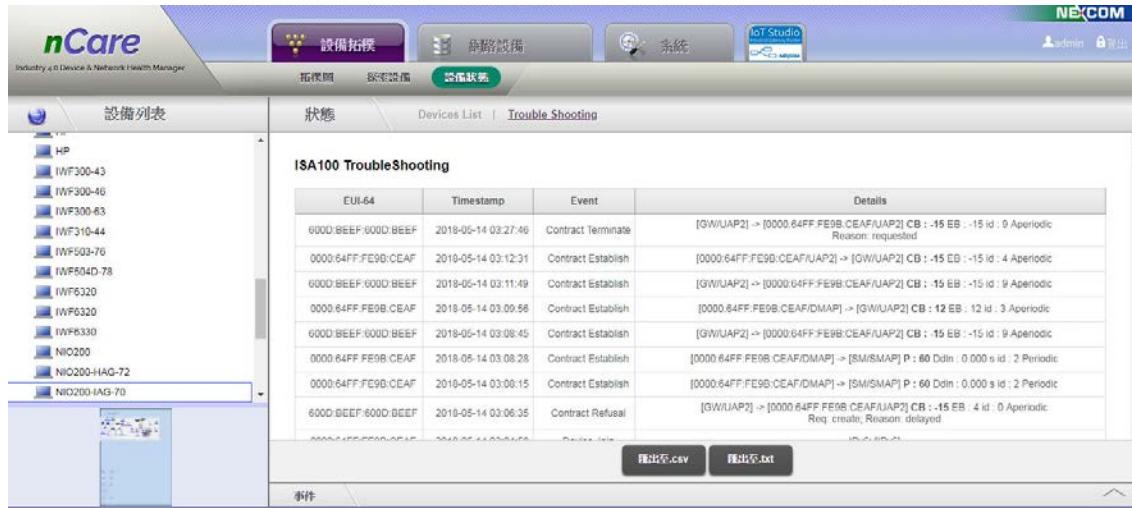


圖 228 NIO200-IAG 設備的 Run Command

(15)NIO200-IAG 設備狀態的「ISA100 Trouble Shooting」分頁，則可顯示「EUI-64」、「Timestamp」、「Event」和「Details」等資訊。



EUI-64	Timestamp	Event	Details
6000:BEFF:0000:BEFF	2018-05-14 03:27:46	Contract Terminate	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 0 Aperiodic Reason: requested
0000:64FF:FE9B:CEAF	2018-05-14 03:12:31	Contract Establish	[0000:64FF:FE9B:CEAF/UAP2] -> [GW/UAP2] CB : -15 EB : -15 id : 4 Aperiodic
6000:BEFF:0000:BEFF	2018-05-14 03:11:49	Contract Establish	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 9 Aperiodic
0000:64FF:FE9B:CEAF	2018-05-14 03:09:58	Contract Establish	[0000:64FF:FE9B:CEAF/DMAP] -> [GW/UAP2] CB : 12 EB : -12 id : 3 Aperiodic
6000:BEFF:0000:BEFF	2018-05-14 03:08:45	Contract Establish	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -15 id : 9 Aperiodic
0000:64FF:FE9B:CEAF	2018-05-14 03:08:28	Contract Establish	[0000:64FF:FE9B:CEAF/DMAP] -> [SM/SMAP] P : 60 DdIn : 0.000 s id : 2 Periodic
0000:64FF:FE9B:CEAF	2018-05-14 03:08:15	Contract Establish	[0000:64FF:FE9B:CEAF/DMAP] -> [SM/SMAP] P : 60 DdIn : 0.000 s id : 2 Periodic
6000:BEFF:0000:BEFF	2018-05-14 03:06:35	Contract Refusal	[GW/UAP2] -> [0000:64FF:FE9B:CEAF/UAP2] CB : -15 EB : -4 id : 0 Aperiodic Req create, Reason: delayed

圖 229 ISA100 Trouble Shooting 頁面

8. IoT Studio 介面說明

本功能可至新漢官網聯繫業務訂購安裝套件，網址如下：

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

安裝後，點擊 nCare 主選單「IoT Studio」，可超連結至 NEXCOM 的 IoT Studio NodeRed 操作頁面，如下圖(若無安裝，則無法使用此功能)：

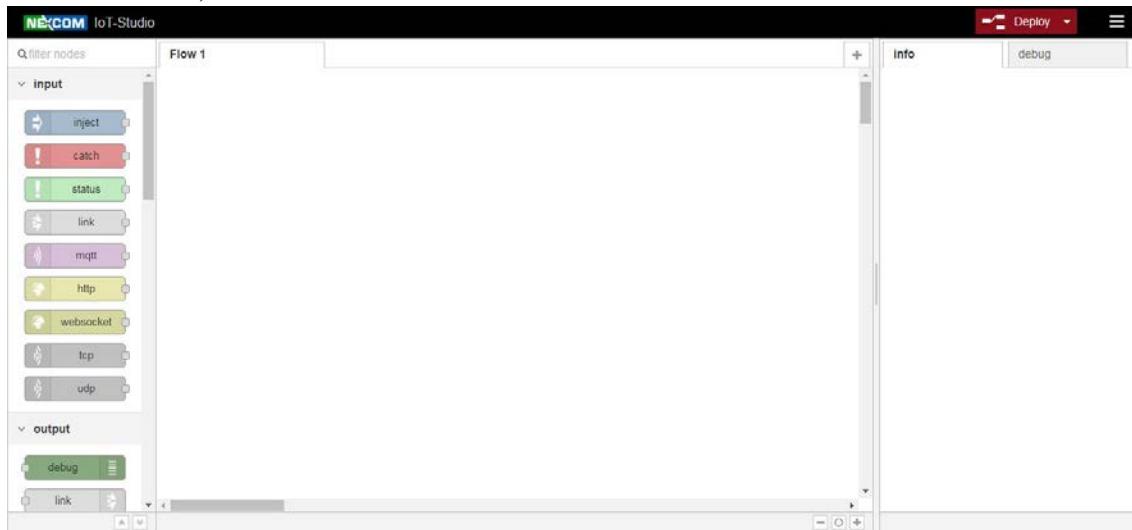


圖 230 IoT Studio 操作畫面

9. nCare 維護與管理

9.1. 存取控制

nCare 為了防止任何未經授權的系統存取、破壞或不當操作，而有存取權限保護之功能，對於系統資料存取、功能設定或更新排程，建立權限的分層管控，以確實管理系統之存取與配置。

9.1.1. 使用者

使用者可監控管理者開放給使用者的群組設備，針對開放給使用者監控的設備，可查閱設備異常事件記錄、使用率，並可操作拓樸頁面。nCare 存取權限如下：

主選單	設備拓樸 (僅限於開放給使用者查閱的設備)			網路設備 (僅限於開放給使用者查閱的設備)							
子選單	拓樸圖		設備狀態	日誌			使用流量				
次選單	功能鍵	快捷鍵	匯出報告	事件日誌	系統日誌	告警回播	乙太網	無線網	處理器	記憶體	溫度
存取權限	可操作： 1.選取 2.移動 3.流量監測 4.顯示/隱藏非法設備 5.交換器虛擬區域網路 6.更新AP 7.更新IWSN 8.放大 9.縮小 10.全覽 11.原始大小 12.全螢幕 13.匯出成圖檔	可操作： 1.狀態 2.使用率 3.事件記錄 4.Ping	可操作完整功能								

圖 231 系統使用者權限

9.1.2. 設備管理者

設備管理員除了系統使用者「帳號管理功能」之外，其餘操作功能皆與系統管理者相同，存取權限如下：

主選單	設備拓樸			網路設備								系統					IoT Studio				
子選單	拓樸圖	探索設備	設備狀態	管理設備			日誌		使用流量	嚴重程度	間隔時間	群組	非法設備		訊息	資料庫	DHCP		IP掃描	關於	
次選單	功能鍵	快捷鍵	探索	狀態	1.設備列表 2.設定備份 3.設定還原 4.副體更新 5.設備配置 6.Modus設定檔			事件日誌	系統日誌	告警回播	1.乙太網 2.無線網 3.處理器 4.記憶體 5.溫度	拓樸群組	1.偵測 2.白名單 3.阻擋設備清單 4.掃描設定		1.電子郵件 2.簡訊 3.社群媒體 4.通報使用者	資料庫紀錄管理	設定	用戶列表	IP掃描	許可證	需聯繫新漢公司取得安裝套件
存取功能	可操作所有功能。																				

圖 232 設備管理者權限

9.1.3. 系統管理者

系統管理者可監控系統納管的所有設備，擁有完整的系統操作功能權限，存取權限如下：

主選單	設備拓樸			網路設備								系統					IoT Studio					
子選單	拓樸圖	探索設備	設備狀態	管理設備			日誌		使用流量	嚴重程度	間隔時間	群組	非法設備		使用者	訊息	資料庫	DHCP		IP掃描	關於	
次選單	功能鍵	快捷鍵	探索	狀態	1.設備列表 2.設定備份 3.設定還原 4.副體更新 5.設備配置 6.Modus設定檔			事件日誌	系統日誌	告警回播	1.乙太網 2.無線網 3.處理器 4.記憶體 5.溫度	拓樸群組	1.偵測 2.白名單 3.阻擋設備清單 4.掃描設定		帳號管理	1.電子郵件 2.簡訊 3.社群媒體 4.通報使用者	資料庫紀錄管理	設定	用戶列表	IP掃描	許可證	需聯繫新漢公司取得安裝套件
存取功能	可操作系統納管的設備及系統所有功能。																					

圖 233 系統管理者權限

9.2. 設備異常狀態

9.2.1. 同 IP 判斷

當設備被設定為同一個 IP，並接受 nCare 納管時，nCare 執行探索設備(Discovery)會顯示錯誤資訊於掃圖結果中，並發出異常通報與警訊。

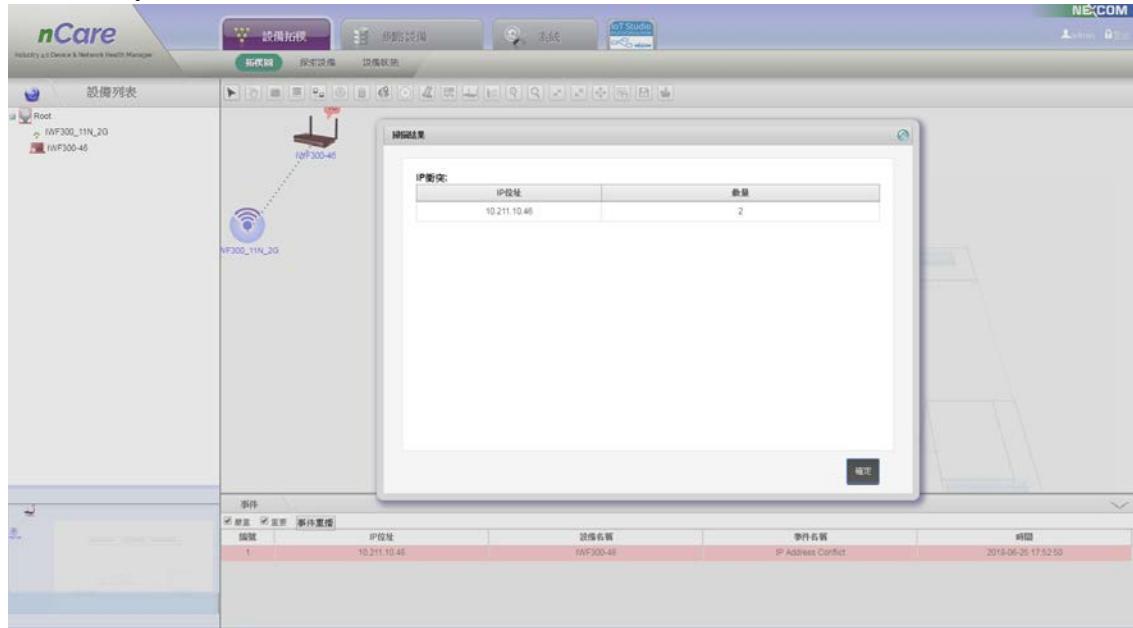


圖 234 設備同 IP 的掃圖結果

掃描拓樸圖後，發出相同 IP 的警報訊息，也會列於事件日誌中。

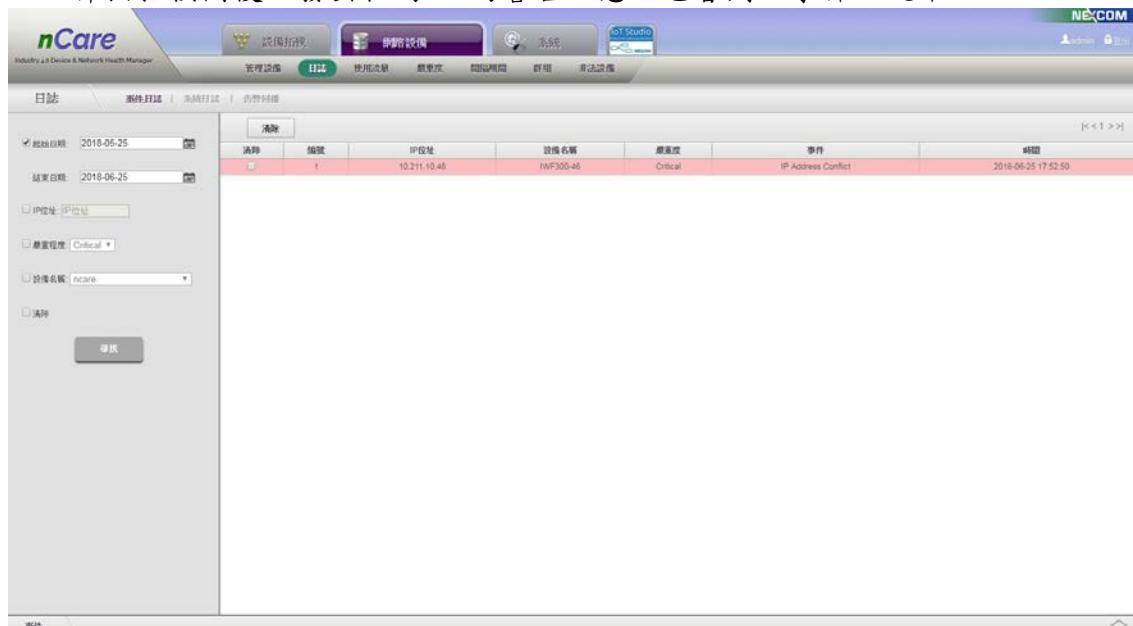


圖 235 設備同 IP 的事件日誌

9.2.2. 同 Mac 判斷

當設備被設定為同一個 Mac，並接受 nCare 納管時，nCare 執行探索設備(Discovery)會顯示錯誤資訊於掃圖結果中，並發出異常通報與警訊。

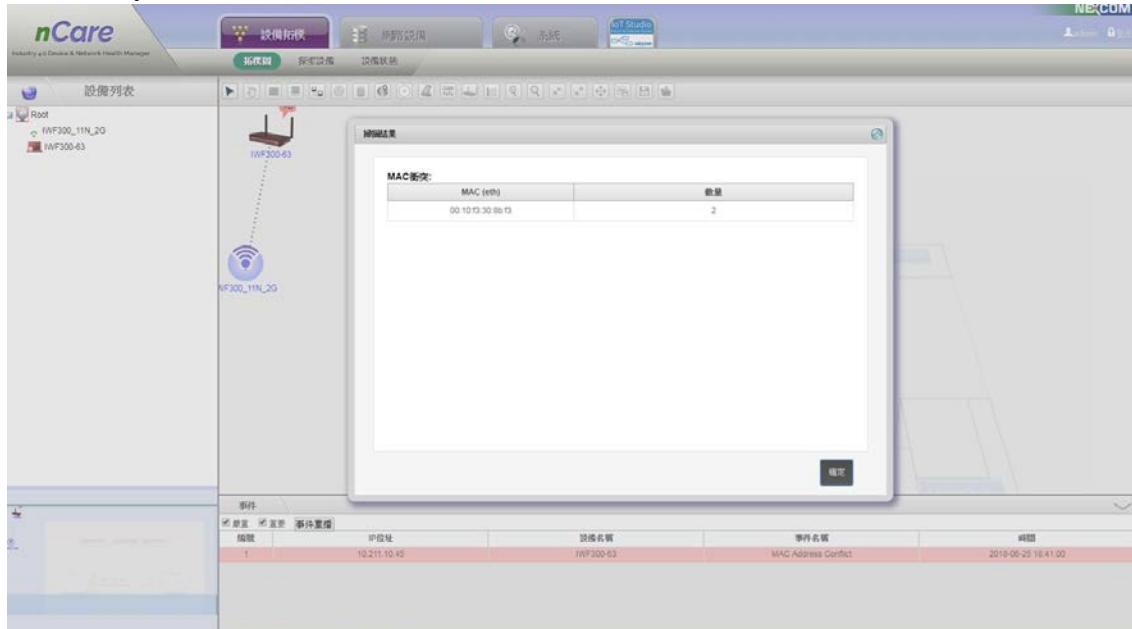


圖 236 設備同 Mac 的掃圖結果

掃描拓樸圖後，發出相同 Mac 的警告訊息，也會列於事件日誌中。

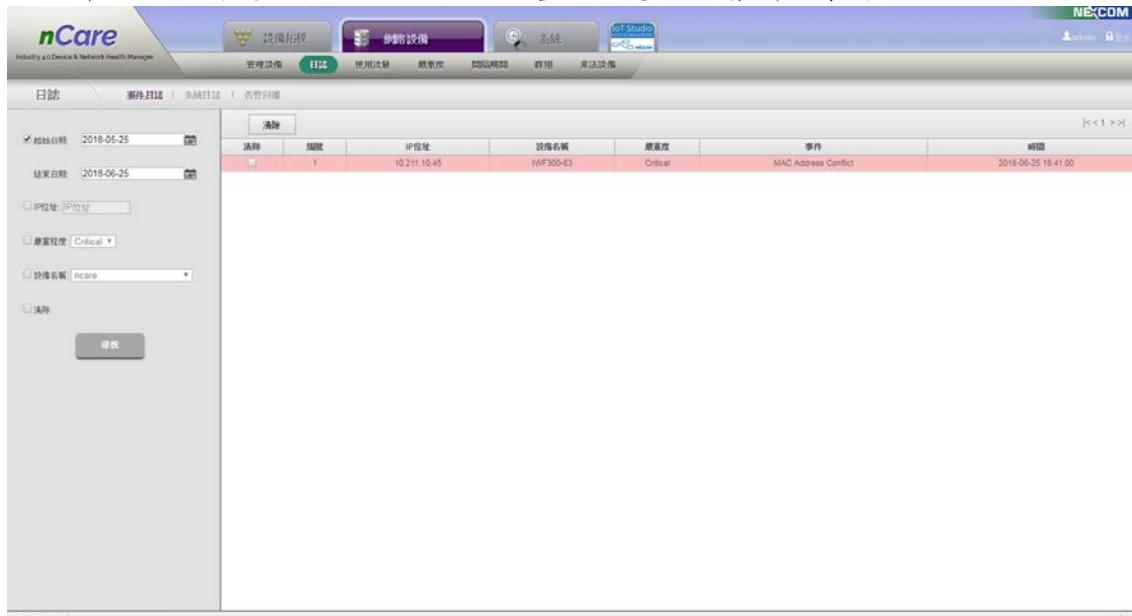


圖 237 設備同 Mac 的事件日誌

主選單「系統」-「IP 掃描」此項功能中，nCare 也會掃描出異常並顯示紅字提醒管理者。



圖 238 IP 掃描功能 警告設備同 Mac

9.2.3. 設備誤接成 Loop

當設備被 nCare 納管，但設備被誤接成迴圈(Loop)時，nCare 有檢測功能可收取設備發出之 syslog，並發出警報訊息，儲存異常訊息於事件日誌中。

*誤接為 Loop 的設備，需先將設備的 System Log Server 設定於 nCare 上。

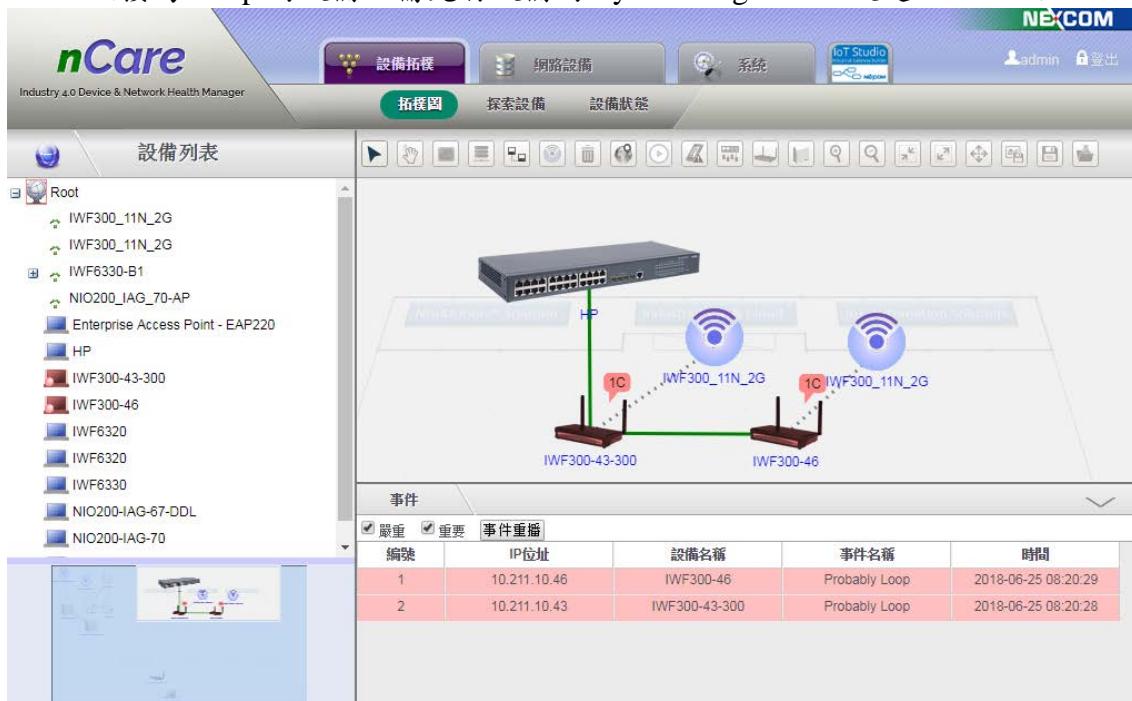


圖 239 設備誤接成 Loop 之警報

設備誤接成 Loop 後，顯示警告列於事件日誌中。

ID	Time	Device	Type	Level	Last Update
9	10.211.10.67	NIO200-IAG-7-DDL	Critical	Polling Failed	2018-06-25 17:29:56
10	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:29:56
11	10.211.10.41	Enterprise Access Point - EAP220	Critical	Polling Failed	2018-06-25 17:26:45
12	10.211.10.47	IWF6330	Critical	Polling Failed	2018-06-25 17:26:45
13	10.211.10.50	IWF6320	Critical	Polling Failed	2018-06-25 17:26:45
14	10.211.10.51	IWF6320	Critical	Polling Failed	2018-06-25 17:26:45
15	10.211.10.57	3310	Critical	Polling Failed	2018-06-25 17:26:45
16	10.211.10.41	Enterprise Access Point - EAP220	Critical	Polling Failed	2018-06-25 17:23:34
17	10.211.10.47	IWF6330	Critical	Polling Failed	2018-06-25 17:23:34
18	10.211.10.50	IWF6320	Critical	Polling Failed	2018-06-25 17:23:34
19	10.211.10.51	IWF6320	Critical	Polling Failed	2018-06-25 17:23:34
20	10.211.10.52	PingableDevice	Critical	Polling Failed	2018-06-25 17:23:34
21	10.211.10.70	NIO200-IAG-70	Critical	Polling Failed	2018-06-25 17:23:34
22	10.211.10.46	IWF300-46	Critical	Probably Loop	2018-06-25 08:23:54
23	10.211.10.43	IWF300-43-300	Critical	Probably Loop	2018-06-25 08:23:30
24	10.211.10.46	IWF300-46	Critical	Probably Loop	2018-06-25 08:20:29
25	10.211.10.43	IWF300-43-300	Critical	Probably Loop	2018-06-25 08:20:28

圖 240 設備誤接成 Loop 之事件日誌

10. 附件一

7.2.2.3 章節之(3)推特發送警報訊息的設定方式

(1)先申請推特的個人帳號。再由 Twitter Apps：<https://apps.twitter.com/> 登入。

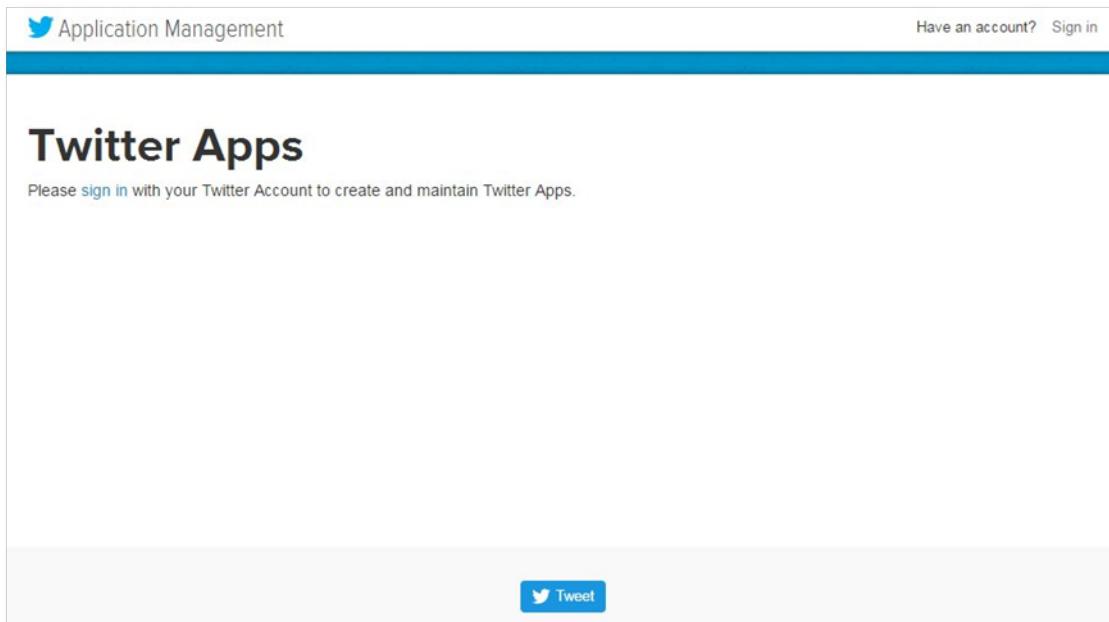


圖 241 登入推特 Apps

(2)登入 Twitter Apps 後，點擊「Create New App」建立新程式。



圖 242 建立新程式

(3)進入「Create an application」頁面，創建應用程式。輸入應用程式資訊

(Name、Description、Website 可任意填，Callback URL 請留白)。請詳讀開發協議「developer Agreement」，並選擇「Yes, I agree」。最後點擊創建你的推特應用程式「create your Twitter application」。

Create an application

Application Details

Name *

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

Description *

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

Website *

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

Callback URL

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

Developer Agreement

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

圖 243 填寫應用程式資訊

(4)完成設定後可取得此畫面。

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

Details **Settings** **Keys and Access Tokens** **Permissions** **Test OAuth**

 **Organization**

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

Organization	None
Organization website	None

Application Settings

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

Access level	Read and write (modify app permissions)
Consumer Key (API Key)	Gv7bjbCM8lwdr6aLTUaqXgJ6 (manage keys and access tokens)
Callback URL	None
Callback URL Locked	No
Sign in with Twitter	Yes
App-only authentication	https://api.twitter.com/oauth2/token
Request token URL	https://api.twitter.com/oauth/request_token
Authorize URL	https://api.twitter.com/oauth/authorize
Access token URL	https://api.twitter.com/oauth/access_token

圖 244 取得應用程式資料

(5) 選擇頁籤「權限(permissions)」，選擇可「Read and Write」之權限。再點擊更新設置「Update Settings」。

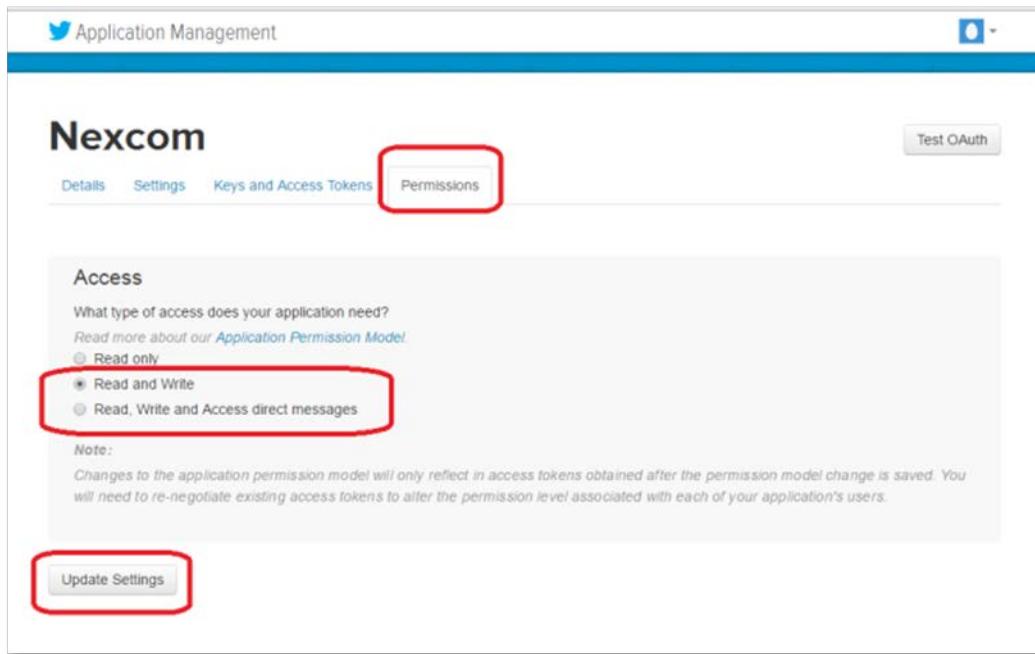


圖 245 選擇權限

(6) 回到頁籤「Keys and Access Token」並點選創建我的存取權限「Create my access token」，即可開通發訊息的權限。

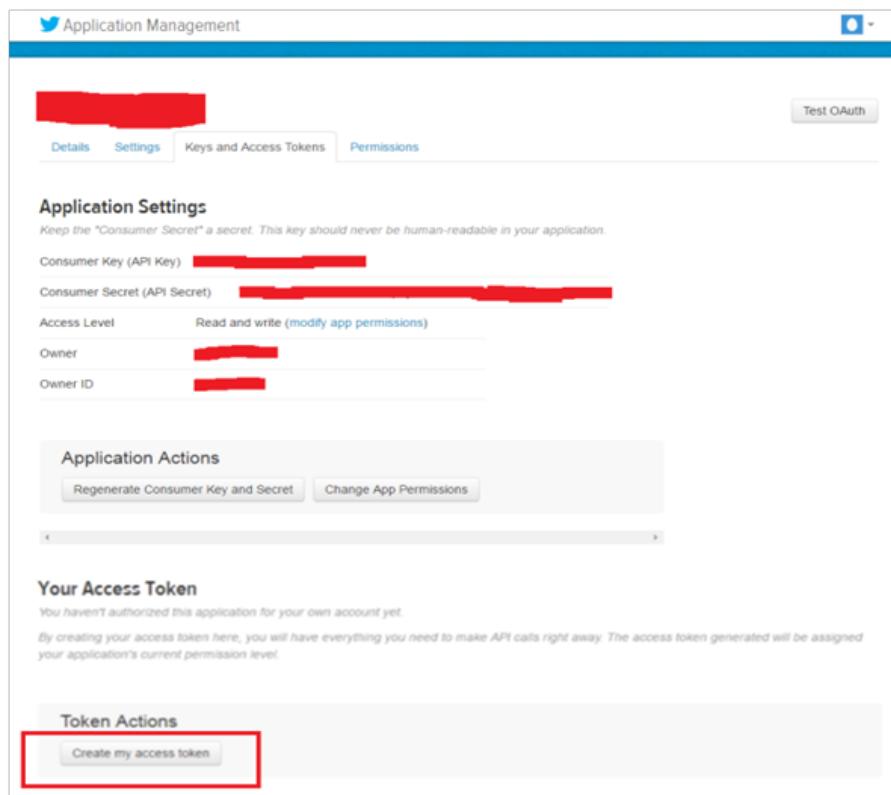


圖 246 開通權限

(7)再上一步驟 Twitter Apps 的頁面中，有應用程式編號「Consumer Key」與應用程式密鑰「Consumer Secret」，填入 nCare 之 Twitter 登入的對應帳號中，並選擇登入。



圖 247 輸入 nCare 的推特帳密

(8)登入後，即會跳出授權畫面，點擊「授權應用程式」。



圖 248 推特授權畫面

(9)點擊後，跳出授權 PIN 碼



圖 249 授權 PIN 碼

(10)將 PIN 碼輸入至 nCare 中。



圖 250 輸入 PIN 碼

(11)完成登入後，可點擊「測試」發送訊息至推特。

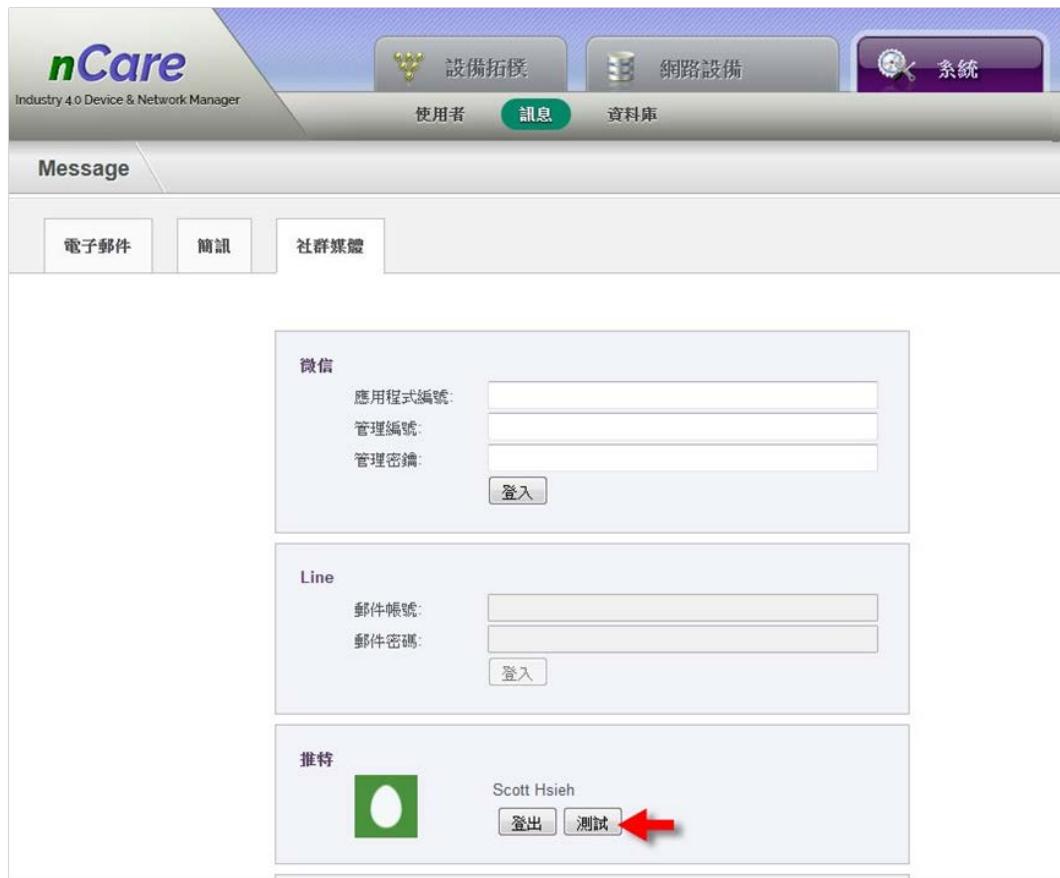


圖 251 發送推特測試訊息

(12)推特中出現測試訊息。

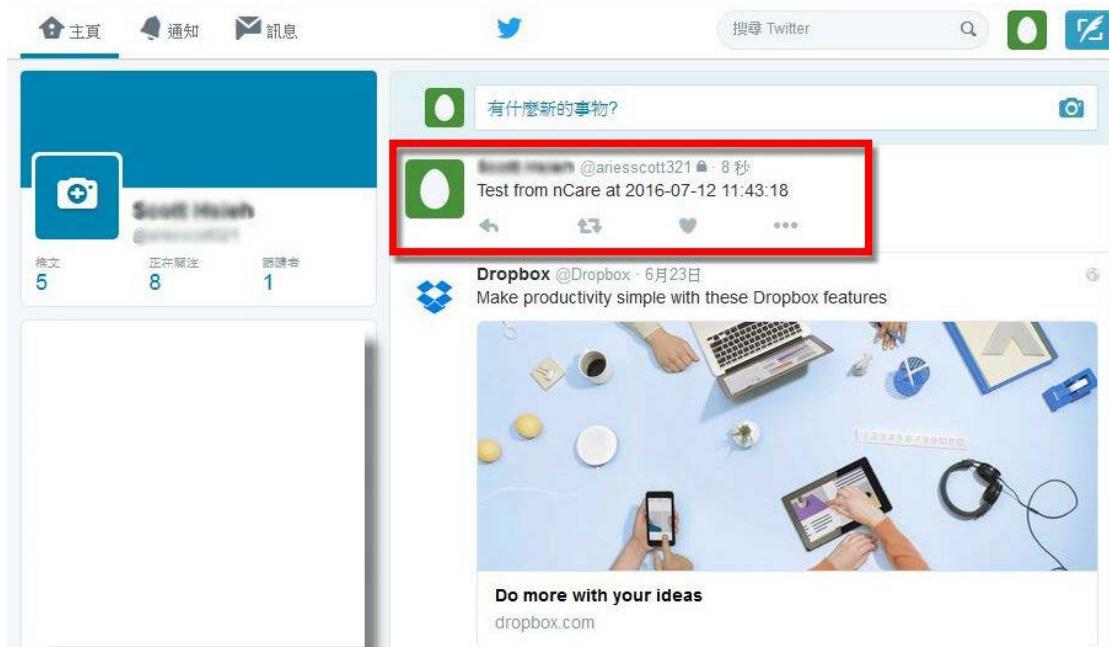


圖 252 測試訊息成功發送