

使用指南

網路管理卡 3

AP9640、AP9641、AP9643

內嵌網路管理卡3的UPS裝置，例如前置SRT的Smart-UPS裝置、前置SRTL的Smart-UPS Ultra 裝置或前置 SRYLF 的 Smart-UPS Modular Ultra 裝置。

990-91148L-038

2024 年 6 月

Schneider Electric 免責聲明

Schneider Electric 不保證本手冊所含的資訊具絕對的權威性、毫無錯誤或已經完整無缺。本文件並非是作為取代與特定地點相關之詳盡操作開發規劃書。因此，因使用本文件所造成之損害、違反法規規定、安裝不當、系統失效或任何其他問題，Schneider Electric 概不負任何責任。

本出版品所含的資訊係以原樣提供，而且是專門為了評估資料中心的設計與結構而製作。Schneider Electric 係以忠實的態度來編撰本文件，但不對當中所含資訊之完整性或正確性做出任何的明示或暗示的陳述或保證。

不論在任何情形下，Schneider Electric 或其母公司、分支機構、或其經理人員、董監事、員工，即使已被明確告知，對任何源自、起自、或關聯自本文件之使用或不使用，所導致之任何直接、間接、因果的、懲罰性的、特殊的、或偶然的損失（包括但不限於喪失業務、合約、營收、資料、資訊、或業務中斷導致的損害），概不負責。SCHNEIDER ELECTRIC 有權隨時變更或更新與此文件相關或其中的內容或格式，而無需事先通知。

相關內容之著作權、智慧財產權與任何其他專有權（包括，但不限於：軟體、影音、文字與照片）係 Schneider Electric 及其授權商所有。本公司有權保留所有未在本文明確授予之權利。本公司並未將任何形式的權利授權或指定，或以不同方式轉讓給任何存取本資訊之人員。

本文件之部分或所有內容均不得轉售。

目录

簡介 1

產品說明..... 1

功能	1
支援的裝置	2
IPv4 初始設定	2
IPv6 初始設定	3
其他應用的網路管理	3

內部管理功能..... 4

概觀	4
登入的優先順序	4
使用者帳號分類	4

如何在遺失密碼後重設..... 5

前面板 (AP9640)..... 6

前面板 (AP9641)..... 7

前面板 (AP9643)..... 8

LED 燈號說明..... 9

狀態 LED 指示燈	9
Link-RX/TX (10/100/1000) LED	9

監控功能..... 10

概觀	10
網路介面監控機制	10
重設網路計時器	10
自動登出	10

Web 使用者介面..... 11

簡介..... 11

概觀	11
支援的 Web 瀏覽器	11

登入的方法..... 11

概述	11
URL 位址格式	12
初次登入	13

首頁	13
概觀	13
圖示及連結	13
監控 UPS：狀態功能表.....	14
有關 UPS 的狀態功能表	14
狀態功能表的插座組	18
狀態功能表的電池系統	18
狀態功能表的通用 I/O	19
有關網路的狀態功能表	19
控制 UPS	20
有關 UPS 的控制功能表	20
控制功能表的插座組	22
有關控制功能表的安全	23
有關控制功能表的網路	24
配置設定值：1	25
配置功能表的插座組	25
插座組是什麼？	25
配置插座組	26
配置功能表的電源設定	27
配置功能表的關機設定	28
開始關機	28
關機期間	29
PowerChute 關機參數	29
UPS 一般頁面.....	31
自我測試排程頁面	32
關機排程.....	32
針對 UPS 及插座組選項	32

韌體更新畫面	33
使用 USB 隨身碟更新 UPS 韌體（僅限 AP9641、 AP9643 和內嵌 NMC 裝置）	34
使用 NMC 更新 UPS 韌體	34
用 FTP 更新 UPS 韌體	34
韌體更新設定配置頁面	35
PowerChute 網路關機用戶端	35
通用 I/O 頁面	35
溫濕度頁面	36
輸入接點頁面	36
輸出中繼頁面	36
液位感測器頁面	37
設定控制規範	37
安全功能表	38
連線期管理頁面	38
Ping 回應	38
本機使用者	38
遠端使用者驗證	39
LDAP 頁面	40
配置 LDAP 伺服器	43
配置 RADIUS 伺服器	43
TACACS+ 頁面	44
設定 TACACS+ 伺服器	45
防火牆頁面	45
802.1X 安全配置	47
SSL 憑證	48
配置設定值：2	49
配置功能表的網路	49
IPv4 的 TCP/IP 設定頁面	49
IPv6 的 TCP/IP 設定頁面	50
DHCP 回應選項	51
連接埠加速頁面	51
DNS 頁面	52
測試 DNS 頁面	52
Web 存取頁面	54
Web SSL 憑證頁面	54
控制台頁面	54
SNMP 頁面	55
Modbus 頁面	57
BACnet 頁面	58
FTP 伺服器頁面	61
Wi-Fi 畫面（僅限 AP9641、AP9643 和內嵌 NMC3 的裝置）	61

通知功能表	62
通知種類	62
配置事件動作	62
電子郵件通知頁面	64
SNMP Trap接收器頁面	66
SNMP Trap測試頁面	67
一般功能表	68
辨識頁面	68
日期/時間頁面	68
用配置檔案新建及匯入設定值	69
配置連結頁面	69
配置功能表的日誌	70
找出 Syslog 伺服器	70
Syslog 設定值	70
Syslog 測試及格式範例	71
「配置」選單上的 CEIP	71
測試功能表	72
測試及校準	72
設定 NMC LED 燈號閃爍	72
日誌及關於功能表	73
使用事件及資料日誌	73
事件日誌	73
資料日誌	74
用 SCP 或 FTP 取得日誌檔案的方法	75
UPS 日誌	77
能源用量	77
防火牆日誌	77
關於網路管理卡 3	78
關於 UPS 裝置	78
關於 NMC 及韌體模組	79
支援頁面	80

匯出配置設定值的方法..... 81

取得及匯出 .ini 檔案..... 81

程序彙整..... 81

.ini 檔案內容..... 81

詳細的步驟..... 81

上傳事件及錯誤訊息..... 83

事件及其錯誤訊息..... 83

config.ini 檔案中的訊息..... 83

覆蓋值產生的錯誤..... 83

NMC 韌體升級..... 84

升級韌體..... 84

韌體檔案傳輸方法..... 84

確認升級..... 84

上次的傳輸結果碼..... 84

確認所安裝韌體的版本號碼..... 84

變更使用者介面語言..... 84

信任根安全啟動..... 84

故障排除..... 88

網路管理卡存取問題..... 88

SNMP 相關問題..... 89

Modbus 問題..... 89

APC USB Wi-Fi Device (AP9834) 問題..... 90

LED 燈號說明..... 90

兩年原廠保固..... 91

保固條款..... 91

不可轉讓保固..... 91

例外條款..... 91

保固索賠..... 92

版權聲明..... 92

簡介

產品說明

功能

Schneider Electric UPS 網路管理卡（AP9640、AP9641 和 AP9643）及內嵌網路管理卡 3 的 UPS 裝置為 Web 式、IPv6 協定相符產品。安裝有 NMC 的裝置可利用下列多種開放式標準來管理：

SSL 上的 HTTP 協定 (HTTPS)	SSH 安全協定
安全複製 (SCP)	輕量級目錄存取通訊協定 (LDAP)
終端存取控制器存取控制系統升級版 (TACACS+)	區域網路可延伸的驗證通訊協定 (EAP) (全稱縮寫為 EAPoL)
建物自動化與控制網路協定 (BACnet)	Syslog
簡易網路管理通訊協定 V1、V2c、V3 版	Telnet
RADIUS	超文字傳輸協定 (HTTP)
Modbus	檔案傳輸協定 (FTP)

AP9640 網路管理卡：

- 提供 UPS 控制及自我測試排程功能。
- 提供資料及事件日誌。
- 可讓您透過事件日誌、電子郵件、Syslog 及 SNMP Trap 來設定通知。
- 提供 PowerChute® 網路關機支援。
- 支援以動態主機配置協定 (DHCP) 或 BOOTstrap 協定 (BOOTP) 伺服器提供 NMC 的網路 (TCP/IP) 值。
- 提供無需轉換成二進制檔案即可將已配置卡的使用者配置檔案 (.ini) 匯出到一或多個未配置卡的功能。
- 提供多種認證及加密的安全協定。
- 與 EcoStruxure™ IT 或資料中心專家通訊。
- 支援 Modbus TCP/IP。
- 支援 BACnet/IP。

AP9641 網路管理卡包括所有 AP9640 網路管理卡功能及下列：

- 提供兩個支援從 USB 隨身碟升級 NMC 以及 UPS 韌體的 USB 連接埠，以及選用的 APC USB Wi-Fi 裝置 (AP9834)。
- 兩組通用 I/O 連接埠，可供連接下列裝置：
 - 溫度感測器 (AP9335T) 或溫濕度感測器 (AP9335TH)
 - 支援兩組輸入接點及一組輸出中繼的中繼 I/O 連接器（需加裝選配的 AP9810 乾接點 I/O 配件）
 - 點液位感測器（NBES0301，選購配件）
- 支援 Modbus TCP/IP 及通用 I/O 連接埠 2 的 Modbus RTU。如需設定 Modbus RTU 的相關資訊，請參考 Modbus 文件附錄。

AP9643 網路管理卡包括所有 AP9640 網路管理卡功能及下列：

- 提供兩個支援從 USB 隨身碟升級 NMC 以及 UPS 韌體的 USB 連接埠，以及選用的 APC USB Wi-Fi 裝置 (AP9834)。
- 支援一組通用 I/O 連接埠，可供連接下列裝置：
 - 溫度感測器 (AP9335T) 或溫濕度感測器 (AP9335TH)
 - 繼電器輸入 / 輸出連接器，支持兩個輸入觸點和一個輸出繼電器（使用可選的附加組件 – AP9810 乾觸點 I/O 附件，這是一個可選的附件）
 - 點液位感測器（NBES0301，選購配件）
- 支援 Modbus TCP/IP，並通過序列 RS485 連接埠支援 Modbus RTU。如需設定 Modbus RTU 的相關資訊，請參考 Modbus 文件附錄。

前置 SRTL/SRYLF 且內嵌網路管理卡的 UPS 裝置含所有 AP9640 網路管理卡功能（但不支援 Modbus 和 BACnet），並且：

- 提供一或兩個 USB 連接埠，可支援以 USB 隨身碟升級 NMC 和 UPS 韌體，以及選配的 APC USB Wi-Fi 裝置 (AP9834)。
- 支援一組通用 I/O 連接埠，可供連接下列裝置：
 - 溫度感測器 (AP9335T) 或溫濕度感測器 (AP9335TH)
 - 支援兩組輸入接點及一組輸出繼電器的中繼 I/O 連接器（需加裝選配的 AP9810 乾接點 I/O 配件）
 - 點液位感測器（NBES0301，選購配件）

支援的裝置

網路管理卡 3 與下列裝置相容：

- 具有 SmartSlot 且前綴為 SMT、SMX、SRT 和 SURTD 的 Smart-UPS® 裝置，以及 2008 後製造的 SUA、SURTD、SRC 裝置*。
- 前綴為 SMV、SMVS、SRV 和 SRVS 和後綴帶有“C”的單相 Easy UPS 設備，例如：SMVS750CAI（仅限 AP9544）。



* 如需可安裝 NMC 3 之相容 UPS 的完整清單，請參閱知識庫文章 [FA237786](#)。

IPv4 初始設定

網路操作 NMC 前，請先定義下列 TCP/IP 設定值：

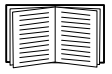
- NMC 的 IP 位址
- NMC 的子網路遮罩
- 預設閘道的 IP 位址（網段不同時才需要）

註：若預設閘道不可用，請使用與 NMC 位於同一子網路且通常一直在運作的電腦的 IP 位址。在網路流量很小時，NMC 會使用預設閘道測試網路。

註：網路管理卡 MAC 位址的前置為 00:C0:B7 或 28:29:86。若要確認 NMC 的 MAC 位址，前往「**支援頁面**」。您可以使用此 MAC 位址前置配置 DHCP 服務。



註：切勿將回送位址 (127.0.0.1) 設為預設閘道。此舉會使本卡停用。您之後必須以本機序列連接的方式，登入後將 TCP/IP 重設為預設值。



若要配置 TCP/IP 設定，請參閱紙本版網路管理卡 [安裝手冊](#)。

用 DHCP 伺服器配置 NMC 卡 TCP/IP 設定的方法，請參見「[DHCP 回應選項](#)」。

IPv6 初始設定

IPv6 網路配置可彈性適應您的需求。IPv6 適用於任何輸入至本介面的 IP 位址。您可手動或使用 DHCP 自動配置 IP 位址，詳細說明請參見「[IPv6 的 TCP/IP 設定頁面](#)」。

其他應用的網路管理

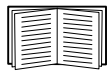
這些應用、公用程式及資源，可用於經 NMC 連上網路的 UPS。

- PowerChute 網路關機 — 提供將連接 UPS 裝置的電腦進行遠端無人關機的功能。
- APC PowerNet[®] MIB — 透過 SNMP 搜尋 UPS 裝置。
- EcoStruxure IT — 雲端式監控軟體，您可以使用此軟體透過 SNMP 及 Modbus TCP 監控 UPS 裝置。
- EcoStruxure[™] 資料中心專家 — 提供企業級電源管理，以及連網 UPS 和環境感測器等 SNMP 代理的管理。
- NMC 安全精靈 CLI — 協助建置或匯入 TLS 伺服器憑證及 SSH 主機密碼，保護與 NMC 通訊的完整性及機密性。

內部管理功能

概觀

請用 Web UI 或指令介面 (CLI) 查看 UPS 狀態以及管理 UPS 和 NMC。您亦可用 SNMP 監控 UPS 狀態。



如需 UI 的詳細資訊，請參閱 **Web 使用者介面**和**指令行介面 (CLI) 指南**。請參閱 **SNMP 頁面**，瞭解如何控制 SNMP 對 NMC 的存取。

登入的優先順序

您可設定多位使用者同時登入，各使用者的優先順序相同。相關詳細資訊，請參閱「**連線期管理頁面**」。

使用者帳號分類

NMC 具備多種使用權限等級 — 超級使用者、管理員、裝置使用者、唯讀使用者及網路使用者：

- **超級使用者**可使用 UI 的全部功能表，以及 CLI 的全部指令。超級使用者亦可定義其他使用者帳號，並設定其他不同的使用者。初次登入時，預設使用者名稱和密碼均為 `apc`。系統會在您登入後提示您輸入新密碼。

註：無法重命名或刪除超級使用者，但可以將其停用。建議在創建任何其他管理員帳號後停用超級使用者帳號。在停用超級使用者帳號之前，請確保至少啟用了一個管理員帳號。

- **管理員**可使用 UI 的全部功能表，以及 CLI 的全部指令。無預設名稱及密碼。
- **裝置使用者**可讀寫裝置相關的頁面和 Web UI 中的指令，但不能使用安全功能表下的連線期管理及網路區段的功能表和指令等管理員功能。

預設使用者名稱為 `device`，必須先設置密碼，才能啟用使用者帳戶。

- **唯讀使用者**擁有下列有限的使用權限：
 - 只能經 UI 使用。
 - 可使用與裝置使用者相同的功能表，但不能變更配置、控制裝置、刪除資料、使用檔案傳輸功能。配置選項可見但無法使用。（事件及資料日誌功能表無清除日誌的按鈕。）

預設使用者名稱是 `readonly`、密碼是 `apc`。

- **網路使用者**只能用 Web UI 及 CLI (Telnet/SSH，序列連接除外) 登入。無預設名稱及密碼。有關設定前三種帳號



管理員、裝置使用者、唯讀使用者和僅限網路使用者帳號預設為停用，在變更超級使用者預設密碼 (`apc`) 之後方可啟用。



如欲設定「管理員」、「裝置使用者」和「唯讀」帳戶類型的**使用者名稱**和**密碼**，請參見「**本機使用者**」。

如何在遺失密碼後重設



註: 重設 NMC 會將網路管理卡重設為預設配置。

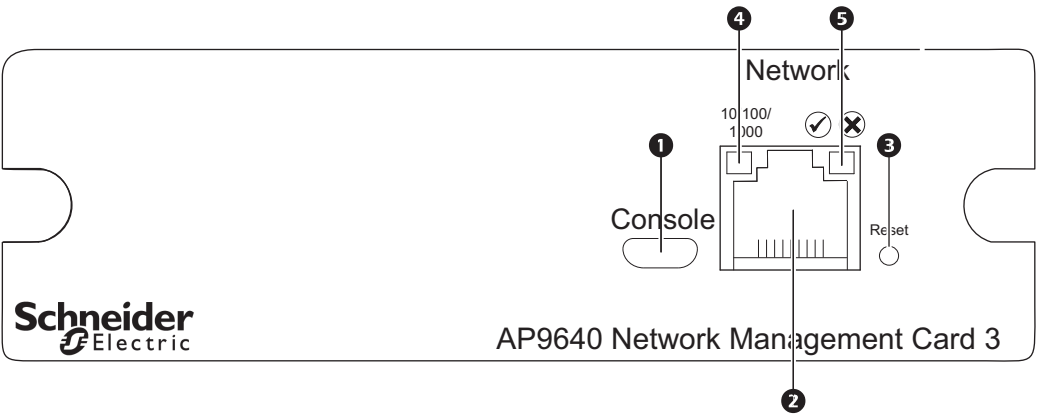
若您遺忘密碼，您必須使用 NMC 上的重設按鈕清除所有設定，包括密碼。按住重設按鈕 20-25 秒，確保狀態 LED 燈號閃爍綠色。當狀態 LED 燈號變為黃色或橘色時，放開重設按鈕，讓 NMC 完成重新啟動程序。

在 NMC 重新啟動後，您必須重新設定 NMC。相關詳細資訊，請參閱[安裝指南](#)或知識庫文章 [FA156064](#)。



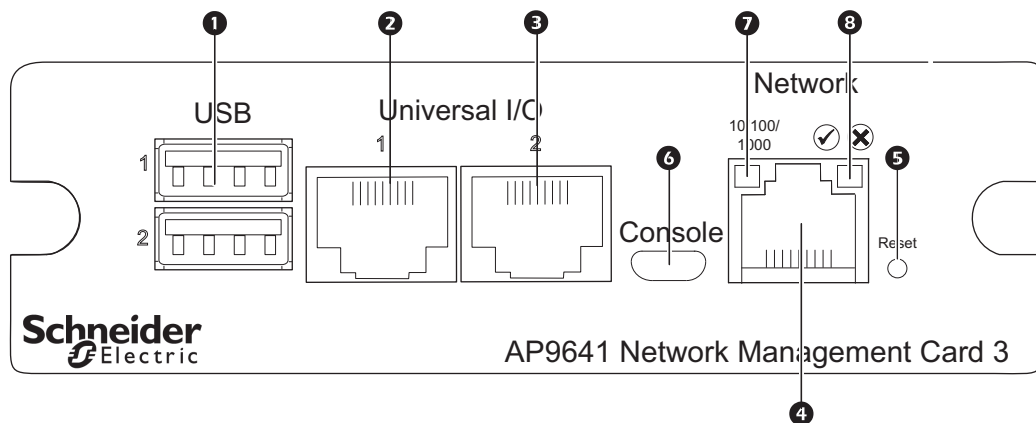
建議您在設定 NMC 之後匯出 .ini 檔案以防止在遺失密碼時遺失資料。相關詳細資訊，請參閱「[取得及匯出 .ini 檔案](#)」。

前面板 (AP9640)



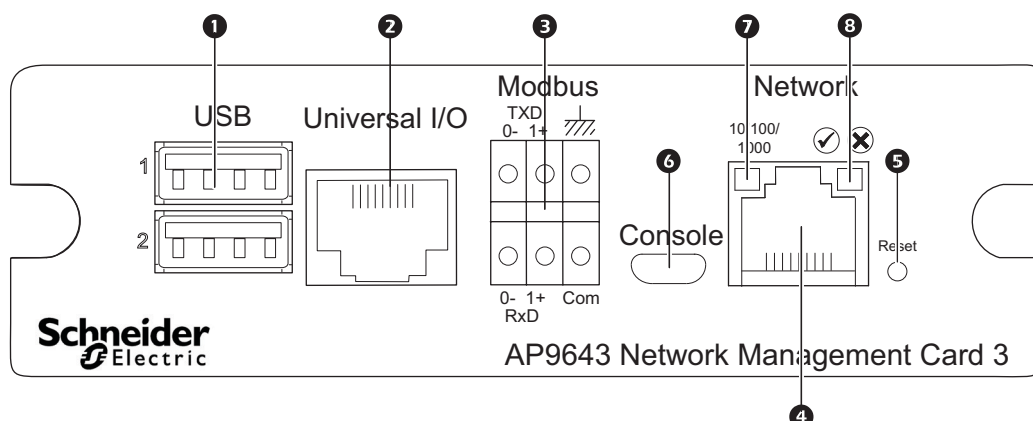
	項目	說明
1	USB 控制埠	使用 micro-USB 纜線 (APC 零件編號 960-0603) 將 NMC 連接至本機電腦，配置初始網路設定或存取指令介面 (CLI)。
2	10/100/1000 Base-T 連接器	將 NMC 連上乙太網路。
3	重設按鈕	重新啟動網路管理介面。注意：這不會影響 NMC 所在裝置的輸出電力。
4	Link-RX/TX (10/100/1000) LED	請參閱「Link-RX/TX (10/100/1000) LED」。
5	狀態 LED 指示燈	請參見「狀態 LED 指示燈」。

前面板 (AP9641)



	項目	說明
1	USB 埠	支援 NMC 以及 UPS 韌體升級和選用的 APC USB Wi-Fi 裝置 (AP9834)。請參閱「NMC 韌體升級」，「 使用 USB 隨身碟更新 UPS 韌體（僅限 AP9641、AP9643 和內嵌 NMC 裝置） 」和「 Wi-Fi 畫面（僅限 AP9641、AP9643 和內嵌 NMC3 的裝置） 」。
2 3	通用 I/O 連接埠	將溫度感測器、溫濕度感測器、繼電器輸入 / 輸出配件連接器和點液位感測器連接至 UIO 連接埠。繼電器 I/O 配件連接器有兩個輸入接點、一個輸出繼電器。
4	10/100/1000 Base-T 連接器	將 NMC 連上乙太網路。
5	重設按鈕	重新啟動網路管理介面。 注意： 這不會影響 NMC 所在裝置的輸出電力。
6	USB 控制埠	使用 micro-USB 纜線 (APC 零件編號 960-0603) 將 NMC 連接至本機電腦，配置初始網路設定或存取指令介面 (CLI)。
7	Link-RX/TX (10/100/1000) LED	請參閱「 Link-RX/TX (10/100/1000) LED 」。
8	狀態 LED 指示燈	LED 燈號。請參見「 狀態 LED 指示燈 」。

前面板 (AP9643)



項目	說明
1 USB 埠	支援 NMC 以及 UPS 韌體升級和選用的 APC USB Wi-Fi 裝置 (AP9834)。請參閱「NMC 韌體升級」，「 使用 USB 隨身碟更新 UPS 韌體（僅限 AP9641、AP9643 和內嵌 NMC 裝置） 」和「 Wi-Fi 畫面（僅限 AP9641、AP9643 和內嵌 NMC3 的裝置） 」。
2 通用 I/O 連接埠	將溫度感測器、溫濕度感測器、繼電器輸入/輸出配件連接器和點液位感測器連接至 UIO 連接埠。中繼 I/O 配件連接器有兩個輸入接點、一個輸出中繼。
3 Modbus 連接器	將 NMC 連上建物管理系統 (BMS) 隨附兩組端子台插頭連接器 (料號：730-0532)。如欲驗證 UPS 是否支援 Modbus，請參考 UPS 隨附的手冊。
4 10/100/1000 Base-T 連接器	將 NMC 連上乙太網路。
5 重設按鈕	重新啟動網路管理介面。 註： 這不會影響 NMC 所在裝置的輸出電力。
6 USB 控制埠	使用 micro-USB 纜線 (APC 零件編號 960-0603) 將 NMC 連接至本機電腦，配置初始網路設定或存取指令介面 (CLI)。
7 Link-RX/TX (10/100/1000) LED	請參閱「 Link-RX/TX (10/100/1000) LED 」。
8 狀態 LED 指示燈	LED 燈號。請參閱「 狀態 LED 指示燈 」。



關於 UPS 內的內嵌 NMC3 裝置，請參閱裝置隨附的《使用指南》，瞭解各種 NMC 連線的位置。

LED 燈號說明

狀態 LED 指示燈

本 LED 燈號顯示 NMC 的狀態。

狀態	說明
關閉	出現下列狀況： •NMC 無輸入電源。 •NMC 異常。可能需要修理或更換。請聯絡客戶支援。請參閱「APC 全球客戶支援」。
恆亮綠燈	NMC 的 TCP/IP 設定正確無誤。
恆亮橘燈	出現下列狀況之一： •NMC 發生硬體故障。請聯絡客戶支援。請參見「APC 全球客戶支援」。 •NMC 處於開機監控模式。NMC 處於開機監控模式。請參閱「關於 NMC 及韌體模組」。
閃綠燈	NMC 的 TCP/IP 設定有誤。 ¹
閃橘燈	NMC 正在請求 BOOTP。 ¹
交替閃綠及橘燈	LED 緩慢閃爍時，代表 NMC 正在請求 DHCP ² 。 ¹ LED 快速閃爍時，代表 NMC 正在啟動。
1. 若您不使用 BOOTP 或 DHCP 伺服器，請參閱紙本網路管理卡安裝手冊或 APC 網站提供的 PDF 來設定 NMC 的 TCP/IP 設定。 2. 使用 DHCP 伺服器的方法，請參見「DHCP 回應選項」。 註：如果在 NMC 開機時連接 micro-USB 纜線，NMC 可能需要等待 90 秒，讓系統有時間存取開機監控。在此延遲期間，不會有任何 LED 燈指示狀態。如果不需要本機存取 CLI，建議斷開 micro-USB 纜線。	

Link-RX/TX (10/100/1000) LED

本 LED 燈號顯示 NMC 的網路狀態。

狀態	說明
關閉	出現下列狀況： •NMC 無輸入電源。 •連接 NMC 到網路的信號線斷開或故障。 •連接 NMC 到網路的裝置關閉或故障。 •NMC 本身故障。可能需要修理或更換。請聯絡客戶支援。請參閱「APC 全球客戶支援」
恆亮黃燈	NMC 已連上速度 10-100 Mbps 的網路。
恆亮綠燈	NMC 已連上速度 1000 Mbps 的網路。
閃爍黃燈	NMC 以 10-100 Mbps 的速度收發數據封包。
閃爍綠燈	NMC 以 1000 Mbps 的速度收發數據封包。

監控功能

概觀

為偵測內部故障並從非預期輸入復原，NMC 3 採用內建、全系統的監控機制。重新啟動以復原內部故障時，事件日誌會記錄一筆**系統：網路介面重新啟動**的事件。

網路介面監控機制

NMC 3 採用內部監控機制，以防無法從網路使用。例如：若 NMC 3 在 9.5 分鐘內未收到任何網路流量 (包括 SNMP 等直接流量或 ARP 請求等廣播流量)，即認定網路介面發生故障並重新啟動。

重設網路計時器

若要確保 NMC 3 不會在網路無動作 9.5 分鐘後重新啟動，NMC 3 會每 4.5 分鐘存取預設閘道一次。閘道如存在，會回應 NMC 3，同時重新啟動 9.5 分鐘計時器。您的應用如無需或沒有閘道，請指定同一網段上某個電腦的 IP 位址。該電腦的網路流量會以足夠的頻率重新啟動 9.5 分鐘計時器，以防 NMC 3 重新啟動。

自動登出

使用者預設在 3 分鐘無動作後，自動登出 NMC Web 及 CLI 介面。個別使用者的預設登出時間可用 Web 介面調整：

配 > 安全 > 本機使用者 > 管理。

- 點擊您要變更之帳號的使用者名稱超連結。
- 修改連線期逾時下的分鐘數。

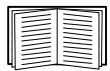
自動登出	期間 (分)
預設	3
最小	1
最高	60 (1 小時)

Web 使用者介面

簡介

概觀

您可利用 Web 使用者介面 (UI) 管理 UPS、網路管理卡 3 (NMC 3) 及查看 UPS 狀態。



有關如何選擇、啟用、停用控制 UI 存取的協定，以及定義協定所需 Web 伺服器連接埠的說明，請參見“**Web 存取頁面**”。

支援的 Web 瀏覽器

NMC Web UI 與下列軟體的最新版本相容：

- Microsoft Edge
- Firefox
- Google Chrome

其他常見的瀏覽器應該都可使用，但未經完整測試。

NMC 不能使用代理伺服器。使用瀏覽器存取 NMC 的 Web UI 前，請先完成下列作業：

- 將瀏覽器設為對 NMC 停用代理伺服器。
- 將代理伺服器設為不代理 NMC 的特定 IP 位址。

登入的方法

概述

您可將 DNS 名稱或 NMC 的系統 IP 位址用作 UI 的 URL。請用大小寫有別的使用者名稱及密碼登入。輸入密碼時將不會顯示密碼。如果登入不成功，將顯示無效的登入訊息。各種帳號的預設使用者名稱如下：

- 管理員或超級使用者為 `apc`
- `device`：裝置使用者
- `readonly`：唯讀使用者

另請參閱「**使用者帳號類型**」。

您可以在登入時從語言下拉框中選擇語言來設定 UI 語言。相關詳細資訊，請參閱「**變更使用者介面語言**」。



已啟用 HTTPS 時，NMC 會產生自己的憑證，用於確定與瀏覽器的加密方法。請參閱 **安全指南** 以了解詳細資訊。

URL 位址格式

在瀏覽器 URL 位址欄位輸入 NMC 的 DNS 名稱或 IP 位址後，按 ENTER 鍵。指定非 Internet Explorer 預設的 Web 伺服器連接埠時，請在 URL 前面加上 `http://` 或 `https://`。

註：HTTP 預設為停用，HTTPS 預設為啟用。

登入時常見的瀏覽器錯誤。

錯誤訊息	瀏覽器	原因
「本頁面無法顯示。」	Internet Explorer	Web 存取已停用或 URL 錯誤。
「無法連線。」	Firefox、Chrome	Web 存取已停用或 URL 錯誤。

URL 格式範例。另請參見“IPv6 的 TCP/IP 設定頁面”。

範例及存取模式	URL 格式
Web1 的 DNS 名稱	
HTTP	<code>http://Web1</code>
HTTPS	<code>https://Web1</code>
系統 IP 位址 139.225.6.133，以及一個預設的 Web 伺服器連接埠 (80)	
HTTP	<code>http://139.225.6.133</code>
HTTPS	<code>https://139.225.6.133</code>
系統 IP 位址 139.225.6.133，以及一個非預設的 Web 伺服器連接埠 (5000)	
HTTP	<code>http://139.225.6.133:5000</code>
HTTPS	<code>https://139.225.6.133:5000</code>
系統 IPv6 位址 2001:db8:1::2c0:b7ff:fe00:1100，以及一個非預設的 Web 伺服器連接埠 (5000)	
HTTP	<code>http://[2001:db8:1::2c0:b7ff:fe00:1100]:5000</code>

初次登入

當您初次登入 NMC 時，系統會提示您變更預設超級使用者帳號密碼 (apc)。登入 Web UI 後，系統將會詢問您是否想參與網路管理卡的客戶經驗改進計畫 (CEIP)。選擇您的偏好前將無法繼續使用。只要導覽至 Web UI 中的 **配置 > CEIP > 設定**，即可隨時選擇加入或退出 CEIP。如需更多資訊，請參閱「**配置**」選單上的 **CEIP**。您之後將重新導向至「配置摘要概覽」頁面。此頁面為所有系統通訊協定及其目前值（如已啟用/已停用）的概覽。稍後您可按照下列路徑隨時存取此頁面：**配置 > 網路 > 摘要**。

首頁

概觀

路徑：首頁

介面的**首頁**會顯示未處理的警報，以及事件日誌中最新的事件。

顯示 UPS 目前作業狀態的一或多個圖示及文字：

符號	說明
	無警報 ：目前無警報，UPS 及 NMC 作業正常。
	警告 ：出現需要注意且如未妥善處理可能損及資料或設備的警報狀況。
	嚴重 ：出現需要立即處理的嚴重警報。

每一頁面的左上角會出現報告 UPS 狀態的相同圖示。如有 **嚴重**或**警告**警報出現，未處理的警報筆數會一併顯示。

點擊**更多事件**，查看整個事件日誌。

圖示及連結

設定任何頁面為「首頁」（亦即登入後第一個顯示的頁面）的方法：進入該一頁面，點擊右上方的  圖示。

點擊 ，復原顯示登入首頁。

介面各頁面的左下角有三個可配置的網站連結。預設存取下列網頁的 URL：

- 連結 1：提供實用故障排除資訊的**知識庫**
- 連結 2：提供硬體背景資訊的**產品資訊**



配置連結的方法請參見“**配置連結頁面**”。

監控 UPS：狀態功能表

狀態功能表用於顯示 UPS 及網路目前的狀態。



您可使用配置功能表設定 UPS 及網路，詳細的說明請參見“配置設定值：1”及“配置設定值：2”。

請參見下列各節：

- “有關 UPS 的狀態功能表”
- “狀態功能表的插座組”
- “狀態功能表的電池系統”
- “狀態功能表的通用 I/O”
- “有關網路的狀態功能表”

有關 UPS 的狀態功能表

路徑：狀態 > UPS

本功能表顯示 UPS 負載、電池充電、電壓及其他有用資料。

欄位	說明
上次電池傳輸	上次切換為電池作業的原因。自我測試除外。
內部溫度	UPS 的內部溫度。
剩下的執行時間	UPS 可用電池電力支援目前負載的時間。
UPS 輸入	
輸入電壓	UPS 的輸入 AC 電壓 (VAC)。
旁路輸入電壓	UPS 為旁路模式時的 VAC。 某些 UPS 裝置可能無此選項。
UPS 輸出	
輸出電壓	指 UPS 供應其負載的 VAC。
負載電流	輸入電壓的電流安培數。
輸出負載	UPS 所連接設備的各相負載 kVA。
輸出百分比負載	UPS 所連接設備在無冗餘狀態下，對可用 kVA 的各相負載百分比。
輸出百分比電力	UPS 所連接設備對可用 kVA 的各相負載百分比。
輸出瓦數	UPS 對可用瓦數的負載百分比。
輸出 VA	UPS 對可用 VA 的負載百分比。
輸出效率	輸入電源直接輸出到負載的百分比。輸入電源未輸出到負載的部分即為 UPS 的耗用。
輸出電源用量	負載自上次重設後到預設點的電源用量。

欄位	說明
電池狀態	
電池容量	UPS 電池容量可用於支援所連接設備的百分比。
電池電壓	電池的 DC 電壓。
外接電池	除內建電池外，連上 UPS 的電池數。



部分 UPS 裝置可能無下列某些選項。

欄位	說明
額定電池電壓	UPS 電池的額定電壓；UPS 以電池為輸出電源時的額定 DC 電壓。
實際電池匯流排電壓	可用的 DC 電源。
外接電池櫃額定值	外接電池之電池櫃的額定（安培 - 小時）電力。
電池	UPS 擁有的內外接電池數。
不良電池	不良（需要更換）的電池數。
電池電流	電池的輸出電流
下一次電池更換日期	所安裝的 UPS 電池組中，最早的電池更換建議日期。
智慧模組	智慧模組相關資料尋求 APC 客服中心協助時，可能需要提供這些資料（韌體版本、製造日期、序號及硬體版本）。
輸入電壓	UPS 的輸入 AC 電壓 (VAC)。
旁路輸入電壓	UPS 為旁路模式時的 VAC。
輸入頻率	UPS 輸入電壓以赫茲 (Hz) 為單位表示的頻率。
頻率	輸出與輸入電壓以赫茲 (Hz) 為單位表示的頻率。
旁路頻率	UPS 旁路模式下之電壓以赫茲 (Hz) 為單位表示的頻率。
輸出電流	供應負載、以安培為單位表示的電流
輸出頻率	輸出電壓以赫茲 (Hz) 為單位表示的頻率。
負載電力	UPS 對可用瓦數的負載百分比。
明顯負載電力	UPS 對可用 VA 的負載百分比。
模組	有關 UPS 所安裝模組的資料。尋求 APC 客服中心協助時，可能需要提供這些資料（韌體版本、製造日期、序號及硬體版本）。
電源模組	有關 UPS 所安裝電源模組的資料。尋求 APC 客服中心協助時，可能需要提供這些資料。

路徑：狀態 > UPS > 量測值



下方選項只適用於前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置。

本功能表顯示剩下的 UPS 執行時間、電池充電、電壓及其他有用資訊。

欄位	說明
上次切換為電池供電之原因	上次切換為電池作業的原因。自我測試除外。
剩下的執行時間	UPS 可用電池電力支援目前負載的時間。
UPS 輸入	
輸入電壓	UPS 的輸入 AC 電壓 (VAC)。
頻率	UPS 輸入頻率，以赫茲 (Hz) 為單位。
UPS 輸出	
輸出電壓	指 UPS 為其負載供應的 VAC。
頻率	UPS 輸出頻率，以赫茲 (Hz) 為單位。
負載電流	輸入電壓的電流安培數。
輸出 VA	UPS 對可用 VA 的負載百分比。
輸出瓦數	UPS 對可用瓦數的負載百分比。
輸出電源用量	負載自上次重設後到預設點的電源用量。
功率係數	此值表示用電效益。理想值是 1，低於 1 的值一律表示電機系統出現耗損。
輸出效率	輸入電源直接輸出到負載的百分比。輸入電源未輸出到負載的部分即為 UPS 的耗用。
電池狀態	
充電狀態	UPS 電池容量可用於支援所連接設備的百分比。
電池電壓	電池的 DC 電壓。
健康狀況	包括任何電池系統故障，含個別電池架故障。故障會記錄為事件。
下一次電池更換日期	所安裝的 UPS 電池架中，最早的電池更換建議日期。

路徑：狀態 > UPS > 概觀



下方選項只適用於前置 SRYLF 且內嵌 NMC 的 UPS 裝置。

本頁面顯示 UPS 主電池架不同位置中的組件。例如：電源模組，電池模組，智慧模組，外接電池架。

路徑：狀態 > UPS > 電源



下方選項只適用於前置 SRYLF 且內嵌 NMC 的 UPS 裝置。

本頁面顯示目前的電源模組、模組位置以及每個模組的狀態。

路徑：狀態 > UPS > 電池



下方選項只適用於前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置。

這一項概述電池系統狀態與電池架狀態。

欄位	說明
電池系統狀態	
電池容量	UPS 電池容量可用於支援所連接設備的百分比。
剩下的執行時間	UPS 可用電池電力支援目前負載的時間。
額定電池電壓	UPS 電池的額定電壓；UPS 以電池為輸出電源時的額定 DC 電壓。
實際電池匯流排電壓	可用的 DC 電源。
所有模組的最高電池溫度	已安裝之所有模組的最高溫度。
所有模組的最低電池溫度	已安裝之所有模組的最低溫度。
最高電池電壓	已安裝之所有模組中，所有電池的最高電壓。
最低電池電壓	已安裝之所有模組中，所有電池的最低電壓。
電池架狀態	
狀態	電池架的狀態，包括個別電池架的狀態。狀態值除顯示正常的訊息外，還可顯示電池壽命將盡的訊息，或電池在組內的預期期限。故障會記錄為事件。
重大事件	若顯示大於 0 的值，表示發生了應立即解決的電池架問題。
警告	若顯示大於 0 的值，表示發生了可能需要解決的電池架問題。
正常	若顯示大於 0 的值，表示一切正常。
無電池	若顯示大於 0 的值，表示電池槽內未裝入任何電池模組。

點擊「主要」或「XRn/電池架 n」，進入 **電池狀態：主要電池架/電池狀態：電池架 n** 畫面。

欄位	說明
模組	電池模組與模組在電池架中的位置。
狀態	電池架的狀態。除「正常」以外，此值也可能表示電池使用壽命將盡，或者已經超出電池使用壽命。故障會記錄為事件。
健康狀況	包括任何電池系統故障。故障會記錄為事件。
上次電池更換	上次更換電池架的日期。

路徑：狀態 > UPS > 智慧模組



下方選項只適用於前置 SRYLF 且內嵌 NMC 的 UPS 裝置。

本頁面顯示目前的智慧模組、模組位置以及每個模組的狀態。

狀態功能表的插座組

路徑：插座組狀態 >

某些 UPS 裝置可能無此選項。本選項顯示 UPS 全部插座組的詳細資料。相關詳細資訊，請參閱“控制功能表的插座組”及“配置功能表的插座組”。

狀態功能表的電池系統

路徑：電池系統狀態 >



某些 UPS 裝置可能無此選項。

欄位	說明
電池系統狀態	
充電狀態	UPS 電池容量可用於支援所連接設備的百分比。
剩下的執行時間	UPS 可用電池電力支援目前負載的時間。
正極匯流排電壓	UPS 裝置 支援正極及負極電池電壓。
負極匯流排電壓	
更換電池匣 SKU	更換電池匣時應提供的料號。
電池組狀態	
電池組 1、2...	電池組的編號來自於內建的編號方法。
序號	電池組序號。
狀態	狀態指的是包括個別電池匣故障在內的電池組故障。故障會記錄為事件。
狀態	包括個別電池匣狀態在內的電池組狀態。 狀態值除顯示正常的訊息外，還可顯示電池壽期將盡的訊息，或電池在組內的預期壽限。故障會記錄為事件。

點擊電池組 1、2... 進入**電池組 n**的頁面。

欄位	說明
電池組 1、2... 或 內建組	
序號（若有）	電池組序號。
韌體修訂版本	電池組版本碼。
溫度	電池匣內感測器所示的溫度。

欄位	說明
電池組狀態	僅顯示電池組的故障，不含個別電池匣故障。故障會記錄為如下的事件： • 溫度超出範圍 • 一般故障 • 通訊故障 • 電池組框斷開 • 韌體與硬體不相容
電池匣 1 及（若有）電池匣 2	
狀態	狀態值除顯示正常訊息外，還可顯示電池壽命將盡、已盡或被測電池已近電池匣壽期的訊息。 故障會記錄為事件。
安裝日期	個別電池匣的安裝日。此一日期可修訂。
預估更換日期	UPS 可計算電池應更換的日期。 前述 狀態 欄為以此日期為基礎的估計值。
狀態	個別電池匣的狀態。關於一般電池組故障，請參見前述“電池組狀態”。故障會記錄為如下的事件： • 電池匣斷開 • 電池匣需更換 • 電池匣溫度過高：嚴重 • 電池匣溫度過高：警告。此通常（但不一定）會在前述嚴重狀態之前顯示。

狀態功能表的通用 I/O

路徑：通用 I/O 狀態 >



某些裝置可能無此選項。

溫濕度 顯示各感測器的名稱、警報狀態、溫度及濕度（如有支援）。點擊感測器名稱，編輯其名稱與位置，以及設定其閾值和滯後。相關詳細資訊，請參閱“**溫濕度頁面**”。

輸入接點 顯示各接點的名稱、警報狀態及開啟或關閉。裝有環境配件時，這些會自動取得並顯示。點擊輸入接點的名稱，查看詳細狀態或配置其值。已配置但停用的接點不會顯示。相關詳細資訊，請參閱“**輸入接點頁面**”。

輸出中繼 顯示各中繼的名稱及開啟或關閉。裝有環境配件時，這些會自動取得並顯示。點擊輸出繼電器的名稱，查看詳細狀態或配置其值。相關詳細資訊，請參閱“**輸出中繼頁面**”。

液位感測器 會顯示各個液位感測器的名稱、警報狀態和狀態（偵測到液位或無液位）。裝有環境配件時，這些會自動取得並顯示。點擊液位感測器的名稱，查看詳細狀態或配置其值。相關詳細資訊，請參閱**液位感測器頁面**。

近期環境事件 顯示與環境監控相關的事件，例如溫度超過閾值或是有關環境監控輸入接點的警告訊息。點擊更多事件的連結，查看全部的近期事件。

有關網路的狀態功能表

路徑：網路狀態 >

網路頁面顯示 IP 位址、網域名稱和乙太網路連接埠設定值。有關這些欄位的詳細背景資料請參見“**配置功能表的網路**”。

控制 UPS

控制功能表提供可立即影響 UPS 和其插座的選項，以及某些安全與網路功能。

請參見下列各節：

- “有關 UPS 的控制功能表”
- “控制功能表的插座組”
- “有關控制功能表的安全”
- “有關控制功能表的網路”

有關 UPS 的控制功能表

路徑：控制 > UPS

選擇某一選項鈕並點擊下一步後，另一用以彙整將發生之動作的頁面即會顯示出來；點擊套用，繼續執行這些動作。

這些動作依 UPS 裝置是否配備插座組而異。以下兩個表格分別加以說明。

- “配備插座組之裝置的 UPS 功能表操作”。
- “未配備插座組之裝置的 UPS 功能表操作”。

頁面正下方的這些勾選方塊，對兩個表格都適用。

勾選方塊	說明
Signal PowerChute 網路 關機用戶端	對於配有插座組的 UPS，如果未安裝 PowerChute 用戶端，本選項不能選取（請參見“PowerChute 網路關機用戶端”）。 選擇本選項以通知配置為 PowerChute 網路關機用戶端且與 UPS 通訊中的所有伺服器，以便根據 PowerChute 網路關機參數（請參見“配置功能表的關機設定”）的設定關機。 但此選項在執行任何旁路控制作業時不會通知伺服器。
略過插座關閉延遲	本選項僅適用於配有插座組的 UPS。立即關閉插座，略過設定的插座組延遲。 在緊急情況下或欲縮短執行時間時，可使用本選項。亦可用於負載裝置已被手動關機之時。



有關延遲及設定的詳細資訊，請參見「**配置功能表的關機設定**」、「**通用 I/O 頁面**」及「**控制功能表的插座組**」。

配備插座組之裝置的 UPS 功能表操作

行動	說明
重新啟動 UPS 插座組	套用「立即關機，AC 重新啟動」指令於整個插座組（請參見“控制功能表的插座組”）。點擊下一步，查看計時及延遲的個別細節資料。 關閉切換後插座組的輸出電源，再關閉主插座組（若有安裝）。套用此動作的任何插座組會等候其“重新啟動期間”及“開機延遲”設定的秒數。（插座組會在 AC 市電恢復時開啟，或一直等候到 AC 市電恢復為止，請參見“插座組是什麼？”。） UPS 會在 AC 市電恢復時開啟，或一直等到 AC 市電恢復為止。
開啟 UPS 插座組	開啟主插座組（若有安裝），再開啟全部切換後的插座組。本選項只在 UPS 目前為關閉狀態時顯示。點擊下一步，查看計時及延遲的個別細節資料。 UPS 和插座組隨即開啟。
關閉 UPS 插座組	關閉切換後插座組的輸出電源，再關閉主插座組（若有安裝）。套用本選項的任何插座組會一直關閉，直到被開啟為止。點擊下一步，查看計時及延遲的個別細節資料。
使 UPS 插座組進入睡眠狀態	UPS 輸出電源關閉達下列參數所指定的時間後，即會使 UPS 插座組進入睡眠狀態。點擊下一步，查看計時及延遲的個別細節資料。 • 插座組會在“關機延遲”所設定的時間後關閉其電源。 • 輸入電源恢復時，UPS 會在兩個設定期間後開啟輸出電源：“休眠時間”及“關機延遲”。 UPS 隨即關閉。經過「休眠時間」所設定的小時數後，UPS 會在 AC 市電恢復時開啟，或一直等候到 AC 市電恢復為止。
使 UPS 進入旁路模式 使 UPS 退出旁路模式	這些選項用於控制旁路模式的使用，以便在不關閉 UPS 電源的情形下，對 UPS 進行維護作業。 這些選項僅適用於 Symmetra UPS 與部分 Smart-UPS 裝置。



有關延遲及設定的詳細資訊，請參見「**配置功能表的關機設定**」及「**控制功能表的插座組**」。

未配備插座組之裝置的 UPS 功能表操作

行動	說明
重新啟動 UPS	透過下列動作重新啟動所連的設備。(點擊「下一步」，查看計時及延遲的個別細節資料。) - 關閉 UPS 電源。 - UPS 電池容量至少恢復到「最低電池容量」所設定的百分比之後(配置 – 關機 - 關機結束，請參見「受控的早期關機及關機末期」)，開啟 UPS 電源。
開啟 UPS	開啟 UPS 電源。此選項只在 UPS 關閉時顯示。 點擊「下一步」，查看計時及延遲的個別細節資料。
關閉 UPS	立即關閉 UPS 的輸出電源(無關機延遲)。UPS 將一直維持關閉，直至再次開啟。
使 UPS 進入睡眠狀態	關閉 UPS 的輸出電源達指定時間後，使 UPS 進入睡眠狀態。點擊「下一步」，查看計時及延遲的個別細節資料。 - UPS 在「關機延遲及 PowerChute 網路關機」所指定的時間後關閉輸出電源。 - 輸入電源恢復時，UPS 會在「休眠時間」所設定的時間後開啟輸出電源。
使 UPS 進入旁路及退出旁路模式	這些選項可控制旁路模式的使用，以便在不關閉 UPS 電源的情形下，對部分 Smart-UPS 裝置進行維護作業。 點擊「下一步」，查看計時及延遲的個別細節資料。 這些選項僅適用於 Symmetra UPS 與部分 Smart-UPS 裝置。

控制功能表的插座組

路徑：控制 > 插座組



某些 UPS 裝置可能無此選項。

您可用本選項開啟、關閉或重新啟動與 UPS 裝置獨立的個別插座組。(此頁面依名稱及狀態列出已透過**配置 - 插座組**選項配置的各 UPS 插座組，請參見「**插座組是什麼?**」)。

您可針對各插座組選擇(或不選擇)下列動作。這些都是一次性動作。

- 插座組狀態為**關閉**時：
 - 立即開啟**
 - 延遲後開啟**：等候**開啟延遲**所指定的秒數後開啟插座組。(請參見“**配置功能表的關機設定**”。)

- 插座組狀態為開啟時：
 - 立即關閉
 - 延遲後關閉：等候關閉延遲所指定的秒數後關閉插座組（請參見“配置功能表的關機設定”）。
 - 立即重新啟動：立即關閉群組，在重新啟動期間（請參見“配置功能表的關機設定”）及開啟延遲所指定的秒數後再將其開啟。
 - 延遲後重新啟動：在關閉延遲所指定的秒數後關閉插座組，之後於重新啟動期間及開啟延遲所指定的秒數後再將其開啟。
 - 立即關機，AC 重新啟動：立即關閉群組。在重新啟動期間及開啟延遲所指定的秒數後，檢查 AC 市電是否已恢復，且 UPS 可支援最小返回時間需求，然後開啟群組。
 - 延遲後關機，AC 重新啟動：等候關閉延遲所指定的秒數後關閉群組。在重新啟動期間及開啟延遲所指定的秒數後，檢查 AC 市電是否已恢復，且 UPS 可支援最小返回時間需求，然後開啟群組。

選擇某個動作後，點擊下一步，查看各動作（包括任何延遲期間在內）的詳細說明。點擊套用開始動作。

有關控制功能表的安全

路徑：控制 > 安全 > 連線期間管理

本頁面顯示下列詳細資料：登入的使用者、所用的介面（例如 Web UI 或 CLI）、其 IP 位址，以及登入的時間長短。

如有足夠的權限，您還可點擊其名稱，查看驗證該使用者的方式。您亦可用**中斷連線期**按鈕將該使用者登出。

有關控制功能表的網路

路徑：控制 > 網路 > 重設 / 重新啟動

您可用這些選項重設各種網路管理卡選項以及 UI。

行動	說明
重新啟動管理介面	將自己登出，以重新啟動管理介面（例如 Web 使用者介面、CLI）。 UPS 及 NMC 裝置不會重新啟動。
重設全部 ¹	注意：此會將全部設定重設為預設值。 - 如果您未選取排除 TCP/IP，所有設定值與設定會重設為其預設值，包括決定此裝置獲取其 TCP/IP 設定值與 EAPoL 配置的必要方法的設定。TCP/IP 配置設定預設為 DHCP，而 EAPoL 存取預設為停用。 - 如果您選取了排除 TCP/IP，除了決定此裝置獲取其 TCP/IP 與 EAPoL 設定值的必要方法的設定以外，所有設定值與設定會重設為其預設值。
僅重設 ¹	TCP/IP : 僅重設決定此裝置取得 TCP/IP 設定值的必要方法的設定，包括已重設為停用的 EAPoL 配置。TCP/IP 配置設定預設為 DHCP，而 EAPoL 存取的預設為停用。
	事件配置 ：將事件重設為其預設配置。任何特殊配置的事件或群組也將會恢復到預設值。請參見「 通知功能表 」
	UPS 為預設值 ：僅將 UPS 設定（而非網路設定）重設為其預設值。
	喪失環境通訊警報 ：重設拔出連接至通用 I/O 連接埠的裝置時會觸發的喪失環境通訊警報。
	控制規範 ：重設用以定義 NMC 如何回應乾接點 I/O 配件所偵測到之警報的設定值。
¹ 重設可能需時一分鐘。您設定的 UPS 名稱不會被重設（請參見“ UPS 一般頁面 ”）。	

配置設定值：1

您可利用配置功能表選項來設定 UPS 及 NMC 的基本作業值。

請參見以下各節及「配置設定值：2」。

- 「配置功能表的插座組」
- 「配置功能表的電源設定」
- 「配置功能表的關機設定」
- 「UPS 一般頁面」
- 「自我測試排程頁面」
- 「關機排程」
- 「韌體更新畫面」
- 「PowerChute 網路關機用戶端」
- 「通用 I/O 頁面」
- 「安全功能表」



註：您可透過配置摘要頁面檢視部分配置設定 (配置 > 網路 > 摘要)。

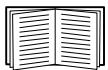
配置功能表的插座組

路徑：配置 > 插座組

某些 UPS 裝置可能無此選項。您可用本選項顯示並配置插座及後續延遲。

另請參見「狀態功能表的插座組」、「控制功能表的插座組」及「配置功能表的關機設定」。

插座組是什麼？



插座組僅見於某些 UPS 裝置。如欲判定 UPS 裝置是否支援插座組，請參考 UPS 隨附的手冊。

可用的設定視 UPS 裝置而異。

主要插座組 某些 UPS 裝置會提供 AC 市電給一組主要插座組。主要插座組可控制分配到 UPS 各切換插座組（如有）的電源。

- 主要插座組關閉時，切換插座組無法開啟。
- 關閉主要插座組前，UPS 會先關閉切換插座組。
- 開啟切換插座組前，UPS 需先開啟主要插座組。

切換插座組

- 各切換插座組可獨立作業。您可依序開啟或關閉這些插座，以及重新啟動連上這些插座的裝置。

配置插座組

插座組名稱及類型 **配置 - 插座組** 頁面會顯示您 UPS 插座組的名稱、類型及延遲。點擊**群組**下的插座組名稱，可變更包括順序延遲及負載減除選項在內的設定值。

順序設定 設定值隨 UPS 裝置而異。您可用順序選項來定義 UPS 回應使用者指令的方式。

欄位	說明
關機延遲	開啟的插座組會先等候幾秒關機延遲的時間，之後才關閉。藉由為插座設定不同的時間，您可排序其關閉，亦即指定其關閉的順序。
重新啟動期間	插座重新啟動的前置時間。
開機延遲	關閉的插座組收到開啟信號時，會先等候幾秒開機延遲的時間，之後才開啟。藉由為插座設定不同的時間，您可指定其開啟的順序。
最小返回執行時間	UPS 重新開啟前，必須能支援其負載的最短時間。

負載減除選項 您可用負載減除選項，指定用來使個別切換插座組減除電源的條件。



註：若使用「PowerChute 網路關機」管理 UPS，則不建議使用 NMC 負載減除選項，這可能會與 PowerChute 中所指定的插座組設定有衝突。

運用負載減除的例子：UPS 以電池供電或過載時，關閉顯示器等非關鍵性負載。這有助於保留電池電量以及必要負載的使用時間。另一實例：在過載後停用自動重新啟動，以便在重開插座組前查明過載的起因。

您可利用此選項，在符合下列條件的情況下關閉插座組：

- 電池開啟時間超過指定分鐘數。
- UPS 剩餘執行時間低於指定分鐘數。（執行時間指 UPS 可使用電池電力支援目前負載的時間長度。）
- UPS 過載指的是 UPS 所連接裝置的電力需求超過 UPS 可提供的程度。

您可啟動下列動作：

- **略過插座關閉延遲**。（立即關閉插座組，不等候**關閉延遲**所指定的秒數，本選項預設為停用。）
- **電源恢復後維持關閉**。（AC 市電恢復後維持關閉狀態。此選項預設為停用，且 UPS 會在**開啟延遲**所指定的秒數後開啟插座組。）

插座組事件及 Trap. 插座組狀態變更會產生事件 — **UPS：插座組基於資訊嚴重性開啟**，或 **UPS：插座組基於警告嚴重性關閉**。事件訊息的格式為「UPS：插座組 *group_number*、*group_name*、產生動作的原因」。例如：

UPS：插座組 1、Web 伺服器、已開啟。

UPS：插座組 3、印表機、已關閉。

事件預設為產生事件日誌記錄、電子郵件以及 Syslog 訊息。

如有針對事件配置 Trap 接收器，則在插座組開啟時會產生 Trap 298、插座組關閉會產生 Trap 299。事件訊息是 Trap 的自變數。嚴重程度預設為與事件相同。

配置功能表的電源設定

路徑：配置 > 電源設定



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 電源設定」。



可用的設定視 UPS 裝置而異。

額定輸出電壓是 UPS 以電池供電時，對負載所提供的 AC 電壓。您可配置下列個別裝置的項目類型：

- 高低**壓**設定可決定 UPS 自動調整電池對負載輸出的電壓範圍，以便保護負載。
超過電壓上限時，UPS 會使用其 AVR 削減功能；超過電壓下限時，UPS 會使用其 AVR 提高功能（或 UPS 無 AVR 提高功能時，則改用電池供電）。
- 啟用**綠色模式**可讓 UPS 以能源效率較高的旁路模式執行。但在綠色模式下，於需要時改以 UPS 電池供電的速度將會減緩。若您的環境需要有快速切換時間，您可停用綠色模式。
- UPS 會改以電池供電來因應輸入電源雜訊。**敏感性**設定會變更 UPS 對線路雜訊反應的時間。您可用**降低**及**低**選項，延長 UPS 在改為電池供電前，耐受線路輸入雜訊的時間。**低**選項用於輸入電源已知有大量線路雜訊時，例如輸入電源為發電機時。
- **額定輸出功率**：滿足負載裝置需求的最大額定功率
- **旁路**設定用於定義 UPS 切換為旁路模式的條件
- **警報閾值** 依可用的執行時間、冗餘電力及 UPS 負載而異。
- **輸出頻率範圍**：在此範圍內，UPS 會繼續正常運作，不需改用電池供電。
- **輸出頻率迴轉率**：UPS 取得輸入來源的鎖相時，輸出頻率在一段指定期間內能夠變化的最大量。以 Hz/s（赫茲 / 秒）表示。

配置功能表的關機設定

路徑：配置 > 關機



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 關機」。

您可用本頁面配置 UPS 關機的參數。請參見下表及「受控的早期關機及關機末期」。

開始關機

定義 UPS 關機所需的延遲及期間。

欄位	說明
低電池電力期間	對以電池供電的 UPS，此一選項定義剩餘執行時間的閾值，亦即 UPS 觸發電池電量過低警報的條件。舉例：低電池期間如設定為 10 分鐘，且 UPS 的估計剩餘執行時間已達 10 分鐘以下，系統即會觸發低電池警報。UPS 如未獲得輸入電源，就會在電池耗盡後關機。 低電池條件會對所有與 NMC 相關聯的 PowerChute 網路關機用戶端觸發關閉。
必要延遲上限	計算確保各 PowerChute 用戶端在 UPS 或 PowerChute 用戶端啟動正常關機後，各 PowerChute 用戶端可正常關機所需的延遲時間。 - 此一上限值是全部 PowerChute 網路關機用戶端伺服器所需的最大關機延遲。 - 每次 UPS 管理介面開啟或重設、或選擇且套用 強制協商 選項後，都會重新計算此值。 請參見「關機延遲及 PowerChute 網路關機」。

基本信號關機。

基本信號或「簡單信號」是 UPS 及伺服器、工作站或第三方系統間的簡單通訊方式。介面擴充器 2（AP9624）係一可提供簡單信號給 UPS 的智慧插槽配件。UPS 簡單信號可通知及執行正常系統關機，但不會提供進階或智慧信號所具有的持續高階監控功能。



注意：如有使用 PowerChute 網路關機，不建議您使用基本信號關機。對某些 UPS 型號，基本關機延遲等選項會影響 UPS 關機並取代低電池期間設定，後者被 PowerChute 用於計算所需的總關機時間。

欄位	說明
基本信號關機	如已用基本信號纜線將伺服器、工作站或第三方系統連接到 UPS，請啟用基本信號關機。UPS 不支援進階信號、或配置為以基本信號通訊時，請啟用基本信號關機。
基本低電池電力期間	對以電池供電的 UPS，此一選項定義剩餘執行時間的閾值，亦即 UPS 觸發電池電量過低警報的條件。接著，UPS 會： - 在 UPS 頁面顯示低電池通知。 - 透過低電池纜線傳送 UPS 的低電池通知給所連接的裝置。 UPS 如未獲得輸入電源，就會在電池耗盡後關機。此期間僅適用於 SMT、SMX、SRC、SURTD 及 SRT Smart-UPS 機型。
基本關機延遲	定義收到基本關機通知後，UPS 進行關機的前置時間。此一期間期滿後，UPS 即關機，不論電池剩餘執行時間多寡。 此延遲僅適用於某些 SMT、SMX、SRC、SURTD 及 SRT Smart-UPS 機型。

關機期間

指定 UPS 關機的時間長度。

欄位	說明
休眠時間	定義發出 UPS/ 插座組休眠指令後，UPS 輸出電源保持關閉的時間。UPS/ 插座組關閉後，會在此處所定義之休眠時間、加上插座組的返回時間或開啟延遲後再度開啟。若市電在此時點尚未恢復，UPS 會等到市電恢復後再開啟。請參見第 26 頁的「配置功能表的插座組」。 休眠指令可從 UPS 頁面、「有關 UPS 的控制功能表」、SNMP 指令或 PowerChute 企業版下達。

PowerChute 關機參數

指定 PowerChute 網路關機的關機參數。

欄位	說明
必須延遲上限 — 強制協商	啟用 強制協商 會重設必須延遲上限，以與低電池期間相符。NMC 會發送更新的狀態封包給所有已註冊的 PowerChute 代理。PowerChute 隨即比較封包內的低電池期間及所需的總關機時間，並相應提高必須延遲上限、或其註冊插座組的關機延遲。 PowerChute 每 30 秒進行一次執行時間剩餘查驗，方法是將 PowerChute 所需的總關機時間與 NMC 低電池期間比較。 選擇強制協商會重設全部插座組的關機延遲，使其與低電池期間的值相同。 強制協商可能耗時 10 分鐘，以計算 NMC 註冊 PowerChute 用戶端所需的設定值。詳細的說明請參見相關詳細資訊 30 請參閱關機延遲及 PowerChute 網路關機」。
電池供電時的關機動作	定義 UPS 關機後的動作： • 電源恢復時重新啟動 — 於市電恢復時重新啟動 UPS。 • 關閉且維持關閉狀態 — 即使市電恢復，UPS 繼續維持關閉。 • 忽略 PCNS 關機指令 - UPS 會關機並忽略任何已經設定的 PowerChute 關機指令。
使用者名稱	輸入要用於 PowerChute 的用戶名。
驗證詞	驗證詞用於 PowerChute 及 NMC 間的驗證。驗證詞預設為空白，您必須先設定才可啟用 PowerChute。
PCNS 通信協議	選擇與 PowerChute 通信的通信協議：HTTPS 或 HTTP。

受控的早期關機及關機末期。



部分 UPS 裝置可能無這些選項。這些選項**不能用於** SMT、SMX、SRC、SURTD 或 SRT Smart-UPS 機型。如要控制這些機型插座組的早期關機，請參見第 24 頁的「負載減除選項」。

您可利用受控的早期關機選項，在符合下列條件的情形下，關閉以電池供電的 UPS 裝置：

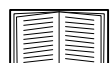
- 電池開啟時間超過指定分鐘數。
- UPS 剩餘執行時間低於指定分鐘數。（執行時間指 UPS 可使用電池電力支援目前負載的時間長度。）
- 電池電量低於設定的總容量百分比時。
- UPS 輸出的負載低於設定的百分比時。

您可用**電源恢復後仍然關閉**選項，指定 UPS 在 AC 市電恢復後要開啟或關閉。

關機結束選項可讓您設定 UPS 在 AC 市電恢復後重新開啟的條件及延遲時間。您可指定 UPS 再度開啟前的**電池容量下限**或**最小返回執行時間**，其值視 UPS 機型而異。

關機延遲及 PowerChute 網路關機

下節說明低電池期間、必須延遲上限及插座組關機延遲對 PowerChute 關機順序的影響。



有關 PowerChute 關機延遲順序的詳細說明，請參見 *PowerChute 網路關機使用手冊*。

對於兩種 UPS，不論有無插座組，關機時間都是由 NMC 與 PowerChute 網路關機互動協商而定，說明如下：

無插座組的 UPS 針對沒有插座組的 UPS，UPS 關機時間是**必須延遲上限**或 NMC **關機**頁面所訂**低電池期間**、加上非可配置的 2 分鐘延遲及 UPS 關機延遲後，兩者較大之值。



備註：

- 若為低電池條件所觸發的關機，低電池期間設定值效力高於必須延遲上限。
- 例外：型號為 SUM 開頭且配備插座組的 UPS，會用有插座組的方式計算 UPS 關機時間。

有插座組的 UPS

有插座組的 UPS，其關機時間是 NMC **插座組**頁面的**關機延遲**設定值，請參見「配置功能表的插座組」。(某些 UPS 裝置可能無此功能。)





備註：

有關 PowerChute 關機順序的詳細說明，請參見 [PowerChute 網路關機使用者手冊的「關機情境範例」](#)。

比較 PowerChute 所需關機時間及 NMC 所需延遲 / 插座組關閉延遲時，取兩者較大之值。
例如：PowerChute 用戶端指令如設定關機期間為 8 分鐘，而 UPS 的低電池期間為 10 分鐘，則 NMC 會以 10 分鐘為必須延遲上限。

強制協商時，NMC 會輪詢 PowerChute 用戶端所需的關機時間。因此，其會耗時 10 分鐘完成必須延遲上限 / 插座組關閉延遲的更新。

PowerChute 不會變更 NMC **低電池期間** 的值。

有插座組之 UPS 的 NMC 不會使用 PowerChute 網路關機 v3.x 及後續版本的**必須延遲上限**設定值。

UPS 一般頁面

路徑：配置 > UPS



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 一般」。



部分 UPS 裝置可能無此頁面。

某些下述選項可能不會顯示於某些 UPS 裝置。

欄位	說明
UPS 名稱	用於辨識 UPS 的名稱。
UPS 位置	UPS 的實體位置，機架或機塔。
警報聲	啟用或停用 UPS 的警報聲；可對某些 UPS 定義發出警報聲的條件。
LCD 語言偏好	指定 UPS 顯示所用的語言。
LCD 顯示	啟用或停用對 UPS 顯示介面的寫入 - 存取。 停用後，使用者仍能讀取 - 存取大部分的頁面，但控制及配置功能表的子畫面除外。
電池狀況警報警告時間	設定要在 UPS LCD 上顯示嚴重的電池更換警報之前的天數。設定為 -1，則不顯示通知警告。
電池狀況警報休眠時間	設定首次確認 UPS LCD 電池警報之後，該警報在顯示之前須進入休眠的天數。設定為 -1，則一旦首次確認警報後將不再顯示警報。
上次電池更換	輸入最近一次電池更換的年度及月份。
電池數目 或 外接電池	UPS 內建電池以外的電池數目。某些配備 16 個以上電池的 UPS 裝置，必須先以 16 為單位增加電池數目（例如 16、32、48，依此類推），然後再調整為正確值。
外接電池櫃	外接電池之電池櫃的額定（安培 - 小時）電力。

欄位	說明
電池充電速率	您可在此欄位變更 UPS 電池以百分比表示的充電速率。100% 代表廠商建議的充電速率。例如，設定為 200% 可使充電速率加倍。 例如，當電池充電速率設定為 100% 時： • 若電池總容量提高，UPS 電池充電器的電流會自動提高到滿足 100% 充電速率的程度 — 無需再調整充電速率。 • 若電池總容量減少，UPS 電池充電器的電流會自動降低到滿足 100% 充電速率的程度 — 無需再調整充電速率。 有關電池容量的詳細說明，請參見 UPS 使用者手冊。 注意：充電速率過高可能導致電解液沸騰及 / 或溢出，以及 / 或高氣壓。除非對此有充分的背景知識，否則請勿變更此設定值。
電池類型	係指電池類型，VRLA 代表閥控式鉛酸，排氣式單電池則為類似車用電池的濕式電池。
總電池容量	此設定可指定 UPS 電池的總容量，範圍在 7-200 安培小時（Ah）之間。此設定用於估計執行時間，以及決定電池充電所需的電流。UPS 如有總電池容量選項，每次增減電池數目後，請更新其值。有關電池容量的詳細說明，請參見 UPS 使用者手冊。

自我測試排程頁面

路徑：UPS > 配置 > 自我測試排程



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 自我測試排程」。

您可用本選項指定 UPS 執行自我測試的時間。

關機排程

路徑：配置 > 排程



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 排程功能」。



某些 UPS 裝置可能無此選項。所有 UPS 裝置的自我測試排程選項可能各不相同。



註：請勿設定相互重疊的關機排程。重疊的關機排程的範例如下：每週的關機時間設定為 8pm 至 9pm，而一次性的關機時間設定為 8.10pm 至 8.30pm。重疊的關機排程將會導致未知及未經測試的行為。

針對 UPS 及插座組選項

您可在 **UPS** 項下進行 UPS 裝置的關機排程，或在 **插座組** 項下進行切換插座組（若適用）的關機排程。

選擇 **UPS** 或 **插座組** 後，任何已配置的關機排程都會與啟用或停用等設定一起顯示在頁面上方。

編輯、啟用、停用或刪除關機排程。點擊 **UPS** 或**插座組**頁面上方排程清單內的排程名稱。此處顯示您編輯其參數的完整詳細資料。包括清除**停用**核選方塊以暫時停用，或是將其永久刪除。

建置 **UPS** 或切換插座組關機排程。

1. 在**排程**選項下，選擇 **UPS** 或**插座組**。
2. 用按鈕選擇關機排程類型：**一次性關機**、**每日關機**或**每週關機**，然後點擊**下一步**按鈕。
3. 如欲暫時停用排程，請取消勾選**啟用**核取方塊。
4. 指定名稱、排程日期及時間。
針對每週關機，用下拉清單指定頻率。
5. 指定裝置或插座組是否在關機後再度開啟：
開啟：指定 UPS 是否在指定的日期及時間開啟：**永不**（UPS 必須手動開啟），或 **立即**（UPS 將在等候 6 分鐘後開啟）

您可針對插座組選擇適當按鈕，指定要關閉的插座組。

Signal PowerChute 網路關機用戶端：指定是否通知 PowerChute 用戶端的詳細資訊，請參見「PowerChute 網路關機用戶端」。



此選項可讓您利用 PowerChute 網路關機公用程式，關閉 50 個網路上執行本公用程式用戶端軟體的伺服器。

韌體更新畫面

路徑：配置 > 韌體更新



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「配置 > UPS > 韌體更新 > 上傳」。



某些 UPS 裝置可能無此選項。

此處的更新指的是 **UPS 上的韌體**。請勿與 NMC 韌體升級混淆，請參見「NMC 韌體升級」。



請依照**韌體更新**畫面指示，決定是否需要在韌體更新前關閉 UPS 輸出。此操作取決於特定的 UPS 型號。



註：請用 Internet Explorer® V10 或後續版本查看**韌體更新**頁面（關閉相容檢視）。韌體更新頁面與 Edge® 瀏覽器不相容。

請按下列步驟更新韌體。（另請參閱「使用 USB 隨身碟更新 UPS 韌體（僅限 AP9641、AP9643 和內嵌 NMC 裝置）」以及「使用 FTP 更新 UPS 韌體」中的其他方法）。

1. 有關取得韌體更新檔案及後續操作指令的詳細說明，請參見 ID 為 **FA164737** 及 **FA170679** 的知識庫文件。
2. 選擇**配置 - 韌體更新**。
3. 點擊按鈕，找出下載到電腦上的更新檔案。
4. 點擊**更新 UPS** 按鈕，更新 UPS 韌體。
5. 更新完成後，檢查**上次更新結果**及**目前版本**項下或事件日誌下的狀態。

使用 USB 隨身碟更新 UPS 韌體（僅限 AP9641、AP9643 和內嵌 NMC 裝置）

在更新 UPS 韌體之前，請確保 USB 隨身碟支援 USB v1.1，且採用 FAT、FAT16 或 FAT32 格式。

1. 將 USB 隨身碟插入電腦的 USB 連接埠。
2. 請參考的知識庫文章 ID [FA164737](#) 和 [FA170679](#)，下載 UPS 的正確韌體更新檔案，並將檔案儲存至根資料夾中，或是 USB 隨身碟的 /upsw/ 目錄中。
3. 從電腦中退出含有韌體檔案的 USB 隨身碟，並將其插至 NMC 的 USB 連接埠。
4. 開啟 NMC Web 介面並前往「[配置](#)」>「[韌體更新](#)」。
5. 在「從 USB 隨身碟更新」窗格下，從下拉式清單中選取韌體檔案。
6. 點擊「[更新 UPS](#)」按鈕以更新 UPS 韌體。



註：韌體更新需要幾分鐘的時間。切勿在 UPS 韌體更新完成之前從 NMC 中移除 USB 隨身碟。如果在完成之前移除 USB 隨身碟，將無法成功更新韌體。

7. 更新完成後，檢查「[上次更新結果](#)」下或「事件日誌」中的狀態。

使用 NMC 更新 UPS 韌體

請按下列步驟更新韌體：

1. 有關取得韌體更新檔案及後續操作指令的詳細說明，請參見 ID 為 [FA164737](#) 及 [FA170679](#) 的知識庫文件。
2. 使用 SCP 或 FTP 將更新檔傳送到介面卡的 root 目錄。例如：`scp <firmware_file>.enc <nmc_username>@<nmc_ip_address>:<firmware_file>.enc`
3. 開啟 NMC Web 介面並前往「[配置](#) > [韌體更新](#)」。
4. 在「使用 NMC 更新」窗格下，從下拉式清單中選取韌體檔案。
5. 點擊「[更新 UPS](#)」按鈕，更新 UPS 韌體。
6. 更新完畢後，請至「[上次更新結果](#)」或「事件日誌」中查看狀態。

用 FTP 更新 UPS 韌體

您可用 FTP 快速地對多個 UPS 裝置進行更新。其更新步驟如下範例。這是從「[韌體更新畫面](#)」進行更新的另一種方法。



註：FTP 預設為停用，必須先啟用才可繼續進行。請參閱「[FTP 伺服器頁面](#)」。

1. 有關取得韌體更新檔案及後續操作指令的詳細說明，請參見 ID 為 [FA164737](#) 及 [FA170679](#) 的知識庫文件。
2. 將更新檔案 FTP 至該卡的 upsw 目錄，即可開始韌體更新步驟。

若更新檔案毀損或不適用於 UPS，FTP 韌體傳輸可能會中斷。

用 DOS FTP 指令載入更新檔案的範例如下：

```
$ ftp <NMC Network Address Here>
Connected to <NMC Network Address>.
220 AP9641 網路管理卡 AOS vX.Y.Z FTP 伺服器就緒。
User (<NMC Network Address>:(none)):apc
331 User name okay, need password.
```

```

password:
230 User logged in, proceed.
ftp> bin
200 TYPE Command okay.
ftp> hash
Hash mark printing On ftp:(2048 bytes/hash mark).
ftp> cd upsfw
250 CWD requested file action okay, completed.
ftp> put "<Path to UPS Firmware File>"
200 PORT Command okay.
150 File status okay; about to open data connection.
226 Closing data connection.
ftp:121984 bytes sent in 1.39Seconds 87.70Kbytes/sec.
ftp> quit
221 Goodbye.

```

3. 更新完成後，檢查 web 介面韌體更新頁面上**上次更新結果**項下或事件日誌下的狀態。

韌體更新設定配置頁面

路徑：配置 > UPS > 韌體更新 > 設定



下方選項只適用於前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置。

指定改用新 UPS 韌體的時間：僅在手動旁路或下載後輸出電源關閉時（並非所有 UPS 裝置/UPS 韌體版本皆支援）、僅在**下載後輸出電源關閉時**或**手動**。

PowerChute 網路關機用戶端

路徑：UPS > 配置 > PowerChute

PowerChute 網路關機用戶端可遠端將 UPS 裝置關機。

在網路上安裝 PowerChute 網路關機用戶端後，會自動加入此一清單。取消安裝 PowerChute 網路關機用戶端時，會自動從此清單刪除。

點擊 **新增用戶端**，輸入 PowerChute 網路關機用戶端的 IP 位址。刪除用戶端的方法：點擊清單中用戶端的 IP 位址，然後點擊**刪除用戶端**。本清單最多可包含 50 個用戶端的 IP 位址。

針對插座組，您還必須指定供電給 PowerChute 用戶端的插座組。



註：若 NMC 停用 HTTP，則 PowerChute 無法連接 NMC。請參閱「**Web 存取頁面**」以啟用 HTTP 或 HTTPS。

通用 I/O 頁面



通用 I/O 功能表適用於所安裝的溫濕度感測器 (AP9335T/ TH)、乾接點 I/O 配件 (AP9810) 或點液位感測器 (NBES0301)。這些通常被稱為環境監控。

溫濕度頁面

路徑：通用 I/O > 溫濕度

顯示各感測器的名稱、警報狀態、溫度及濕度（如有支援）。點擊感測器名稱，編輯其名稱與位置，以及設定其閾值和滯後。

閾值：您可設定各感測器的溫度閾值以及濕度閾值（如有支援）。達到閾值時，系統會發出警報信號。

高 及 **低** 為警告訊息。**最大** 及 **最小** 具關鍵性，必須處理。

滯後：您可用此值來避免因同一溫濕度閾值超過而導致的重複警報。

溫度或濕度如持續略高於或低於閾值，會重複觸發警報。設定較大的滯後值可防止此一現象發生。

滯後值不夠大時，測值上下起伏會導致閾值重複超過，亦即警報會觸發多次。請於了解下列說明後參考其後的範例。

- 針對最大及高閾值超過，警報的解除點是閾值 **減掉** 所輸入的滯後值。
- 對最小及低閾值超過，警報的解除點是閾值 **加上** 所輸入的滯後值。

起伏上升濕度的例子：假設 **最大** 濕度閾值為 65%，滯後值為 10%。濕度超過 65% 時，會觸發警報。接著其在 60-70% 的範圍內上下起伏，但 — 由於設定了 10% 滯後值 —，警報不會解除，故不會再發生新警報。要解除現有的警報，濕度必須降到 55% 以下（亦即 65% **減** 10%）。

起伏下降溫度的例子：假設 **最小** 溫度閾值為 12°C、溫度滯後值為 2°C。溫度低於 12°C 時發生警報。接著其在 13°C-11°C 的範圍內上下起伏，但 — 由於設定了 2°C 滯後值 —，警報不會解除，故不會再發生新警報。要解除現有的警報，溫度必須升到 14°C 以上（亦即 12°C **加** 2°C）。

輸入接點頁面

路徑：通用 I/O > 輸入接點

輸入接點顯示各接點的名稱、警報狀態及開啟或關閉。裝有環境配件時，這些會自動取得並顯示。

點擊輸入接點的名稱，查看詳細狀態或配置其值。停用後，接點即使在異常位置，也不會發生警報。其他欄位說明如下：

欄位	說明
警報狀態	正常 ：此輸入接點未發出警報，或此輸入接點發出警報時，指出警報的嚴重性。接點如未啟用，則顯示 停用 。
狀態	輸入接點的目前狀態： 關閉 或 開啟 。
Normal State (正常狀態)	輸入接點的正常（無警報）狀態： 關閉 或 開啟 。
嚴重程度	此輸入接點異常狀態警報的嚴重性訊息： 警告 或 重大 。

輸出中繼頁面

路徑：通用 I/O > 輸出中繼

輸出中繼顯示各中繼的名稱及開啟或關閉。裝有環境配件時，這些會自動取得並顯示。

點擊輸入接點的名稱，查看詳細狀態或配置其值。欄位說明如下：

欄位	說明
狀態	輸出中繼目前的狀態： 關閉 或 開啟 。
Normal State (正常狀態)	輸出中繼的正常（無警報）狀態： 關閉 或 開啟 。
Control (控制)	勾選此一核選方塊後點擊套用，即可變更輸出中繼的目前狀態。
延遲	警報狀態必須持續導致輸出中繼啟動的秒數。您可用此一設定，避免因短暫的瞬時條件觸發警報。 延遲開始後發生的其他相關警報不會使延遲重新開始，只會繼續倒數直到輸出中繼啟動為止。
保持	輸出中繼在警報發生後，保持啟動狀態的最小秒數。 即使觸發警報的狀況已排除，輸出中繼仍維持啟動狀態直到期滿為止。

液位感測器頁面

路徑：通用 I/O > 液位感測器

液位感測器會顯示各個感測器的名稱和狀態（偵測到液位或無液位）。裝有環境配件時，這些會自動取得並顯示。

點擊液位感測器的名稱，查看詳細狀態或配置其值。欄位說明如下：

欄位	說明
警報狀態	此液位感測器未發出警報時為 正常 ；此液位感測器發出警報時為 重大 。如果液位感測器未啟用此選項，則會顯示 停用 。
狀態	此感測器的狀態： 偵測到液位 或 無液位 。

設定控制規範

路徑：通用 I/O > 控制規範

對於連接乾接點 I/O 配件（AP9810）的 AP9641 或 AP9643 NMC，您可：

- 設定依 UPS 事件及輸入接點開啟或關閉的輸出中繼，請參見「按事件設定輸出回應」
- 設定依輸入接點動作的 UPS，請參見「設定 UPS 或輸出對某輸入警報的回應」



某些 UPS 裝置可能無法按輸入接點設定回應。

按事件設定輸出回應。

- 在**配置**功能表，選擇**通用 I/O** 及 **控制規範**。
- 點擊**新增規範**按鈕。
- 點擊類別或子類別名稱，查看相關的事件。
- 配置的方法如下：點擊事件名稱、選擇事件發生時要改變狀態之輸出中繼的核選方塊、點擊**儲存規範**。

設定 UPS 或輸出對某輸入警報的回應。

1. 在**配置**功能表，選擇**通用 I/O** 及**控制規範**。
2. 點擊**新增規範**按鈕。
3. 點擊**I/O 接點**子類別。
4. 選擇嚴重性相同的事件為輸入接點。例如：輸入接點的嚴重性為重大程度時，選擇重大事件。
NMC 可支援最多 4 個輸入。務必指定與此一事件相關聯的輸入。
5. 在**連接埠**下拉清單，選擇通用感測器**連接埠**編號 (1 或 2)，視有無安裝乾接點 I/O 配件而定。
6. 在**區域**下拉清單，選擇要安裝輸入的區域編碼 (A 或 B)。
7. 定義輸入狀態變更時 UPS 要執行的動作 (如有)。
8. 選擇要開啟或關閉的輸出 (如有)。
9. 點擊**儲存規範**。



所配置的動作會發生一次。

警報狀態解除前，若您將輸出恢復為其正常狀態，除非警報狀況解除後又再發生，否則輸出不會再開啟或關閉。

安全功能表

連線期管理頁面

路徑：配置 > 安全 > 連線期間管理

啟用**許可同步登入**：意即二或多名使用者可同時登入。每一使用者有相同的存取權限，且每一介面 (HTTP、FTP、telnet 控制台、序列控制台 (CLI) 等) 均視為登入的使用者。**許可同步登入**：允許同時有最多 8 名使用者登入 web 介面、5 位使用者登入 CLI，以及 1 位使用者登入序列控制台。

遠端驗證置換：NMC 支援多種遠端驗證通訊協定。啟動此一置換時，NMC 可讓本機使用者使用儲存在本機 NMC 的 NMC 密碼進行登入。另請參見「本機使用者」及「遠端使用者驗證」。

Ping 回應

路徑：配置 > 安全性 > Ping 回應

啟用**IPv4 Ping 回應**」核取方塊，允許網路管理卡 3 回應網路 ping。此對 IPv6 不適用。

本機使用者

您可用本功能表檢視、設定對 NMC 使用者介面的存取及個人偏好 (如日期格式)。此適用於以登入名稱定義的使用者。

路徑：配置 > 安全 > 本機使用者 > 管理

設定**使用者存取**。管理員及超級使用者可用本選項列示及配置可使用 UI 的使用者。點擊名稱連結可查看詳細資料，以及編輯或刪除使用者。

點擊**新增使用者**：加入使用者。您可在後續出現的**使用者配置**頁面，用解除**存取**核選方塊的方法，新增使用者並保留其存取。名稱及密碼最長可達 64 位元，多字節字元的長度較短。必須輸入密碼。



名稱及密碼長度如超過 64 位元，會被截短。
要變更超級使用者設定，您必須輸入目前的密碼。密碼不得超過 64 個 ASCII 字元。

請用**連線期逾時**配置此一 UI 登出使用者的前置時間（預設為 3 分鐘）。修改本設定後，必須登出才能套用新值。

序列遠端驗證置換：選擇此選項後，您可透過序列控制台 (CLI) 連接來略過遠端驗證通訊協定。此一頁面會啟用選定的使用者，但必須透過「連線期管理頁面」進行全域啟用，才能發揮作用。

相關詳細資訊，另請參見下述「配置 > 安全 > 本機使用者 > 預設值」。
帳號的背景資料請參見「使用者帳號分類」。

使用者偏好：勾選**事件日誌色碼**核選方塊，啟用事件日誌內警報文字的彩色編碼。（系統事件及配置變更項目的顏色不變。）

文字顏色	警報嚴重程度
紅色	Critical (重大事件) ：出現需要立即處理的嚴重警報。
橘色	警告 ：出現需要注意且如未妥善處理可能損及資料或設備的警報狀況。
綠色	警報解除 ：導致警報的狀況已改善。
黑色	正常 ：無警報。網路管理卡及連接的全部裝置正常作業中。
藍色	通知訊息 ：用以提供資訊的警報。網路管理卡及連接的全部裝置正常作業中。

匯出日誌格式：匯出的日誌檔案格式可為 CSV（逗點分隔）或定位點符號分隔。請參見「顯示事件日誌」。

請在此 UI 選擇測量的溫度尺度。**美國習慣**代表華氏、**公制**代表攝氏。

您可用**語言**欄位指定 UI 的預設語言。語言也可在登入時設定。



亦可指定不同的語言給電子郵件收件人及 SNMP Trap 接收者。關詳細資訊，請參閱「電子郵件收件人」及「Trap 接收器」。

路徑：配置 > 安全 > 本機使用者 > 預設值

預設值可加快新增使用者的速度。您可用本選項設定管理頁面許多選項的預設值，請參見前述「配置 > 安全 > 本機使用者 > 管理」。

遠端使用者驗證

路徑：配置 > 安全 > 遠端使用者 > 驗證



驗證。指定使用者登入時的驗證方法。

如需本機驗證的相關資訊（不使用 RADIUS 伺服器的集中式驗證），請參閱 [安全手冊](#)。

系統支援下列驗證及 LDAP（輕量級目錄存取通訊協定）、RADIUS（遠端驗證撥接使用者服務）和 TACACS+（終端存取控制器存取控制系統）授權功能：

- 使用者存取已啟用 RADIUS 或 TACACS+ 的 NMC 或其他啟用網路的裝置時，系統會發送驗證請求到伺服器，決定使用者的權限高低。
- LDAP、RADIUS 和 TACACS+ 使用者名稱在 NMC 以 64 個字元為限。

關於驗證方法，請參閱以下選項：

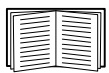
設定	說明
本機使用者驗證	指定是否以及何時檢查本機使用者資料庫： First：始終先檢查本機使用者資料庫。如果找到使用者名稱，則檢查密碼，登入結果為成功或失敗。如果找不到使用者名稱，則使用遠端驗證（如果已啟用）。 Last：如果連接遠端驗證伺服器時發生錯誤，則嘗試遠端驗證後將檢查本機使用者資料庫。當遠端驗證關閉時，其動作與 First 相同。 Off：永遠不檢查本機使用者資料庫。 註：不建議將此選項設定為 Off，因為如果遠端驗證伺服器故障或在 NMC 上配置錯誤，可能導致 NMC 遭永久鎖定。如果使用 Off，強烈建議為超級使用者或管理員啟用遠端驗證覆寫設定並設定序列遠端驗證覆寫選項。 註：如果本機和遠端使用者驗證設定都設為 Off，則本機使用者驗證將自動設定為 First。
遠端使用者驗證	指定使用哪個遠端驗證通訊協定（若有）： Off：不使用遠端使用者驗證，始終執行本機使用者驗證。 RADIUS：遠端使用者驗證將使用 RADIUS。 註：「未新增任何配置的 RADIUS 伺服器。」訊息表示您必須新增正確配置的 RADIUS 伺服器，以便進行 RADIUS 驗證。 TACACS+：遠端使用者驗證將使用 TACACS+。 註：「未新增任何配置的 TACACS+ 伺服器。」訊息表示您必須新增正確配置的 TACACS+ 伺服器，以便進行 TACACS+ 驗證。 LDAP：遠端使用者驗證將使用 LDAP。 註：「未新增任何配置的 LDAP 伺服器。」訊息表示您必須正確配置 LDAP，以便進行 LDAP 驗證。



如果 **本機驗證** 設定為 **Off**，且驗證伺服器無法使用、辨識錯誤或設定不當，所有使用者都無法使用遠端存取。要重新獲得存取權限，您必須用序列連接進入指令行介面，然後將 **存取** 設定變更為 **本機**、**radiusLocal** 或 **tacacs+Local**

例如，將存取設定變更為 **本機** 的指令是：

```
userauth -a local
```



若是 RADIUS 伺服器，另請參閱下述的「RADIUS 頁面」和「配置 RADIUS 伺服器」。

若是 TACACS+ 伺服器，請參閱下述的「TACACS+ 頁面」和「設定 TACACS+ 伺服器」。

若是 LDAP 伺服器，請參閱下述的 **LDAP 頁面** 和 **配置 LDAP 伺服器**。

LDAP 頁面

路徑：路徑：配置 > 安全 > 遠端使用者 > LDAP

您可以將裝置設定為使用 LDAP 伺服器來驗證遠端使用者。兩個常見的範例是 Microsoft Active Directory 和 OpenLDAP。驗證始終使用 TLS 連線上的簡單繫結要求來執行。請確定已安裝 LDAP 伺服器的 CA 憑證，以完成與 LDAP 伺服器的 TLS 連線。

LDAP 設定	說明
搜尋使用者 URI	代表最初繫結之使用者物件位置的 LDAP URI。此使用者物件必須擁有在 LDAP 資料庫中搜尋使用者的權限。使用者嘗試登入期間將連線至此 URI 中的 LDAP 伺服器，並使用「搜尋使用者密碼」中提供的密碼執行對 DN 的繫結。如果繫結成功，則會搜尋嘗試登入的使用者。 此 LDAP URI 必須包含 "ldap" 或 "ldaps" 架構。當使用 "ldaps" 時，TLS 連線為隱含式，TCP 連線預設使用連接埠 636。當使用 "ldap" 時，將傳送 StartTLS 要求來啟動 TLS 連線，且 TCP 連線預設使用連接埠 389。使用 "ldaps" 並非標準做法，不鼓勵使用。 此 LDAP URI 可能包括 LDAP 伺服器的位址以及連接埠編號（可選）。其後是搜尋使用者物件的 DN。如果搜尋使用者 DN 的結尾為 DC 元件，則會對此網域中的 LDAP 服務執行 SRV 記錄的 DNS 查詢。如果找到 SRV 記錄，將以之取代 URI 中指定的主機。如果找不到 SRV 記錄，將使用 URI 中指定的主機。如果已知存在 LDAP 的 SRV 記錄，則可以省略 URI 的主機元件。 如果省略 DN，則主機元件必須存在，並將執行匿名繫結。 範例： • "ldap://ldap.domain.com/CN=searchuser,OU=users,DC=domain,DC=com" 如果可取得 DNS，系統將對 domain.com 上的 LDAP 服務執行 SRV 記錄的 DNS 查詢。如果找到結果，則會連線至該結果。如果找不到，則會連線至連接埠 389 上的 "ldap.domain.com"。傳送 StartTLS 要求後，系統將建立 TLS，然後以「搜尋使用者密碼」中指定的密碼繫結至物件 "CN=searchuser,OU=users,DC=domain,DC=com"，並從這裡開始搜尋登入的使用者。 • "ldap:///CN=searchuser,OU=users,DC=domain,DC=com" 如果可取得 DNS，系統將對 domain.com 上的 LDAP 服務執行 SRV 記錄的 DNS 查詢。如果找到結果，則會連線至該結果。如果找不到，則不會建立連線，因為系統會略過 URI 的主機元件，且無法繼續進行 LDAP 驗證。如果連線成功，系統會以上述方式執行 StartTLS、繫結和搜尋。 • "ldaps://ldap.domain.com" 系統將連線至連接埠 636 的 "ldap.domain.com"，並在不傳送 StartTLS 要求的情況下立即執行 TLS 交握。如果成功，系統將執行匿名繫結，並從這裡開始搜尋登入的使用者。 • "ldap://ldap.domain.com:42/CN=searchuser,OU=users,DC=domain,DC=com" 此情況與第一個範例相同，但如果找不到 SRV 記錄，則會連線至連接埠 42 的 "ldap.domain.com"。
搜尋使用者密碼	如上所述，在搜尋使用者的初始繫結要求中使用的密碼。如果留白，系統將根據是否提供搜尋使用者 DN，執行匿名或無驗證的繫結。
回覆逾時	連線至 LDAP 伺服器並與之通訊時所使用的逾時時間（秒）。初始 TCP 連線必須在此期間內完成。如果確實在此期間內完成，則必須在每次發出 LDAP 要求過後的這段期間內收到來自伺服器的個別 LDAP 回應。由於單一 LDAP 驗證可能包含多個要求（如果追逐轉介，甚至可能包含多個伺服器），因此整體驗證時間最終可能遠大於這裡指定的逾時時間值。
使用者基礎 DN	這是基礎物件項目的 DN，所有登入的使用者都必須存在於其下。
群組基本 DN	這是基礎物件項目的 DN，以下設定中指定的使用者群組必須存在於其下。
管理員群組名稱	這是 NMC 管理員所屬的 LDAP 群組的通用名稱 (CN)。如果登入的使用者屬於該群組，則使用者將被授予管理員權限。
裝置使用者群組名稱	這是 NMC 裝置使用者所屬的 LDAP 群組的通用名稱 (CN)。如果登入的使用者屬於該群組，則使用者將被授予裝置使用者權限。
網路使用者群組名稱	這是 NMC 網路使用者所屬的 LDAP 群組的通用名稱 (CN)。如果登入的使用者屬於該群組，則使用者將被授予網路使用者權限。

LDAP 設定	說明
唯讀使用者群組名稱	這是 NMC 唯讀使用者所屬的 LDAP 群組的通用名稱 (CN)。如果登入的使用者屬於該群組，則使用者將被授予唯讀使用者權限。
Active Directory 架構	若啟用此選項，則將支援包含遵循標準 Active Directory 架構之 "User" 類別使用者和 "Group" 類別群組的 LDAP 目錄。
RFC2307 POSIX 架構	若啟用此選項，則將支援包含遵循 RFC 2307 定義架構之 "posixAccount" 類別使用者和 "posixGroup" 類別群組的 LDAP 目錄。
RFC4519 使用者架構	若啟用此選項，則將支援包含遵循 RFC 4519 定義架構之 "uidObject" 類別使用者和 "groupOfNames" 類別或 "groupOfUniqueNames" 類別群組的 LDAP 目錄。
RFC2798 inetOrgPerson	若啟用此選項，則將支援包含 RFC 2798 定義之 "inetOrgPerson" 類別使用者的 LDAP 目錄。
自訂使用者類別	若啟用此選項，則將支援任何包含不符合上述支援類別之類別使用者的 LDAP 目錄。啟用後必須提供 自訂使用者類別名稱 和 自訂使用者的使用者名稱屬性 設定，並可選擇提供 自訂使用者群組編號屬性 。
自訂群組類別	若啟用此選項，則將支援任何包含不符合上述支援類別之類別群組的 LDAP 目錄。啟用後必須提供 自訂群組類別名稱 和 自訂群組成員屬性 設定，並可選擇提供 自訂群組編號屬性 。另外，還必須正確設定 自訂群組成員類型 。
自訂使用者類別名稱	這是使用者項目所屬物件類別的名稱。只會在啟用 自訂使用者類別 時使用。
自訂使用者的使用者名稱屬性	屬性名稱，其包含 自訂使用者類別名稱 指定之物件類別的使用者名稱。只會在啟用 自訂使用者類別 時使用。
自訂使用者群組編號屬性	屬性名稱，其包含 自訂使用者類別名稱 指定之物件類別的使用者主要群組的群組編號。此為選填，只會在啟用 自訂使用者類別 時使用。使用方式與 "posixAccount" 類別中的 "gidNumber" 屬性相同。
自訂群組類別名稱	這是群組項目所屬物件類別的名稱。只會在啟用 自訂群組類別 時使用。
自訂群組成員屬性	屬性名稱，其包含 自訂群組類別名稱 指定之物件類別的群組成員。只會在啟用 自訂群組類別 時使用。當 自訂群組成員類型 設定為 "DN" 時，此屬性的值為 DN。當其設定為「使用者名稱」時，此屬性的值為使用者名稱。
自訂群組編號屬性	屬性名稱，其包含 自訂群組類別名稱 指定之物件類別的群組編號。此為選填，只會在啟用 自訂群組類別 時使用。使用方式與 "posixGroup" 類別中的 "gidNumber" 屬性相同。
自訂群組成員類型	指示 自訂群組類別名稱 指定之物件類別的群組成員的指定方式。其可設定為 "DN" 或「使用者名稱」。
測試設定	輸入伺服器上任何帳戶的使用者名稱和密碼，以在套用新配置的設定之前進行測試。如果使用者成功通過驗證，而且是至少一個指定群組的成員，則會套用該設定；否則不會套用。
略過測試及套用	直接套用設定，不先執行測試驗證。



另請參閱上文的**遠端使用者驗證**。

配置 LDAP 伺服器

OpenLDAP、Active Directory 或其他 LDAP 伺服器的配置不在本文件範圍內。如同上文設定說明中所述，預設設定為支援最常見的架構，包括 Active Directory 使用者和群組、RFC2307 中定義的 POSIX 架構、RFC4519 中定義的使用者架構，以及 RFC2798 中定義的 inetOrgPerson 使用者類別。如果配置新伺服器，建議選擇以上任一種架構。請務必為您希望支援的每個 NMC 使用者類型建立群組，並相應地將使用者新增至群組之中。

RADIUS 頁面

路徑：配置 > 安全 > 遠端使用者 > RADIUS

您可用 RADIUS 伺服器驗證遠端使用者。此選項的功能如下：

- 列示 NMC 可用的 RADIUS 伺服器（最多兩個），以及其逾時設定。
- 點擊 **RADIUS 伺服器** 連結，配置新的或已有的 RADIUS 伺服器驗證參數。

RADIUS 設定	說明
RADIUS 伺服器	主要或次要 RADIUS 伺服器的伺服器名稱或 IP 位址。
連接埠	主要或次要 RADIUS 伺服器的連接埠編號。 註：RADIUS 伺服器預設使用連接埠 1812 來進行使用者驗證。NMC 支援連接埠 1 - 65535。
密碼	RADIUS 伺服器及 NMC 間的共用密碼。
回覆逾時	NMC 等候 RADIUS 伺服器回應的秒數。
測試設定	輸入管理員使用者名稱及密碼，以測試所配置的 RADIUS 伺服器路徑。
略過測試及套用	不測試 RADIUS 伺服器路徑。



另請參見上述「遠端使用者驗證」及「配置 RADIUS 伺服器」。

配置 RADIUS 伺服器

配置程序彙整

您必須配置 RADIUS 伺服器，以與 NMC 搭配使用，請參見下列步驟。

如需具 VSA 的 RADIUS 使用者檔案範例，以及 RADIUS 伺服器上字典檔案條目的範例，請參閱 [安全手冊](#)。

1. 新增 NMC IP 位址到 RADIUS 伺服器用戶清單（檔案）。
2. 除非有定義 VSA，否則使用者必須配置服務型屬性。未配置服務型屬性時，使用者只有唯讀存取（限於 Web UI 上）。



有關 RADIUS 使用者檔案的說明，請參見 RADIUS 伺服器文件，以及 [安全手冊](#) 中的實例。

3. VSA 可取代 RADIUS 伺服器提供的服務型屬性。

VSA 需有字典條目及 RADIUS 使用者檔案。您可用字典檔案定義 ATTRIBUTE 及 VALUE 關鍵字的名稱，其數字值除外。變更數字值後，RADIUS 驗證及授權將無法使用。VSA 的優先順序高於標準 RADIUS 屬性。

在配備加密密碼的 UNIX® 系統配置 RADIUS 伺服器。

搭配使用 UNIX 加密密碼檔案 (/etc/passwd) 及 RADIUS 字典檔案時，可用下列兩種方法驗證使用者：

- 全部 UNIX 使用者都有管理員權限時，將下列資料加入 RADIUS “user” 檔案。僅允許裝置使用者時，將 APC-Service-Type 變更為 Device。

```
DEFAULT Auth-Type = System
APC-Service-Type = Admin
```

- 新增使用者名稱及屬性到 RADIUS “user” 檔案，並用 /etc/passwd 確認密碼。下列實例的使用者為 bconners 及 thawk：

```
bconners Auth-Type = System
APC-Service-Type = Admin
thawk Auth-Type = System
APC-Service-Type = Device
```

支援的 RADIUS 伺服器。

支援 FreeRADIUS v1.x 與 v2.x，以及 Microsoft Server 2008 與 2012 網路規範伺服器 (NPS)。其他常見的 RADIUS 應用程式應該都可使用，但可能未經完整測試。

TACACS+ 頁面

路徑: 配置 > 安全 > 遠端使用者 > TACACS+

您可以使用 TACACS+ 伺服器驗證遠端使用者。使用此選項執行以下操作：

- 列出 NMC 可用的 TACACS+ 伺服器（最多兩個），以及其逾時設定。
- 點擊 **TACACS+ 伺服器** 連結，設定新的或已有的 TACACS+ 伺服器驗證參數。

TACACS+ 設定	說明
TACACS+ 伺服器	主要或次要 TACACS+ 伺服器的伺服器名稱或 IP 位址
連接埠	主要或次要 TACACS+ 伺服器的連接埠編號。 註：TACACS+ 伺服器預設使用連接埠 49 來驗證使用者。NMC 支援連接埠 1 - 65535。
密碼	TACACS+ 伺服器與 NMC 之間的共用密碼。
回覆逾時	NMC 等候 TACACS+ 伺服器回應的秒數。
測試設定	輸入管理員使用者名稱及密碼，以測試所配置的 TACACS+ 伺服器路徑。
略過測試並套用	不測試 TACACS+ 伺服器路徑。



請參閱上述「遠端使用者驗證」及下述的「設定 TACACS+ 伺服器」。

有兩個適用於所有伺服器的全域 TACACS+ 選項：

TACACS+ 設定	說明
唯讀使用者權限等級	指定一個介於 0 和 15 之間的值。如果授權使用者的權限等級（priv-lvl 授權引數）大於或等於指定值，且小於 管理員權限等級 ，則該使用者將獲得唯讀存取權限。此值必須小於 管理員權限等級 。
管理員權限等級	指定一個介於 0 和 15 之間的值。如果授權使用者的權限等級（priv-lvl 授權參數）大於或等於此值，則該使用者將獲得管理員存取權限。此值必須大於 唯讀使用者權限等級 。

設定 TACACS+ 伺服器

設定程序摘要。

您必須設定 TACACS+ 伺服器，才能與 NMC 搭配使用。



有關設定 TACACS+ 伺服器的詳細資訊，請參閱[安全手冊](#)。

防火牆頁面

路徑：配置 > 安全 > 防火牆 > 配置

啟用或停用防火牆功能。預設會列出已配置的規範。勾選**啟用**核取方塊可啟用防火牆。預設會取消勾選核取方塊。

- 點擊**套用**可確認您已選擇啟用的防火牆規範。**防火牆確認**頁將會開啟。
 - 「確認」頁包含啟用前先測試防火牆的建議，但不強制進行測試。
 - 第一個超連結可前往「防火牆規範」頁。
 - 第二個超連結可前往「防火牆測試」頁。
 - 點擊**套用**可啟用防火牆並返回「確認」頁。
 - 點擊**取消**可不啟用防火牆直接返回「確認」頁。
- 點擊**取消**：不會啟用新的選擇項目。您會繼續留在「配置」頁。

路徑：配置 > 安全 > 防火牆 > 有效的規範

從可用規範下拉式清單中選擇有效的規範，並檢視規範的有效性。預設會顯示目前有效的規範；您可以從清單中選取其他規範。

- 點擊**套用**可啟用您的變更。如果選取並啟用不同的防火牆，變更會立即生效。如果選取新配置的防火牆規範，建議您啟用前先測試新防火牆。（參閱前述的「配置」）。
- 點擊**取消**可恢復原本有效的規範，並繼續留在「有效的規範」頁。

路徑：配置 > 安全 > 防火牆 > 有效的規則

防火牆啟用後，此唯讀頁會列出被目前有效的規範使用的個別規則。請參閱[建立 / 編輯規範](#)區段瞭解欄位說明（優先程度、目的地、來源、協定、動作與日誌）。

路徑：配置 > 安全 > 防火牆 > 建立 / 編輯規範

新增規範；刪除或編輯現有的規範：

註：無法刪除有效且已啟用的防火牆規範，僅可編輯執行中的規範，但不建議此做法，因為會立即套用變更。適當的做法是停用防火牆、編輯規範、進行測試，然後再重新啟用規範。

新增規範：點擊**新規範**，然後鍵入新防火牆檔案的檔名。該檔案的副檔名應是 .fwl。如果未輸入副檔名，名稱後方會自動補上 .fwl。

- 點擊**套用**：如果檔名符合規定，就會建立空的防火牆規範檔。檔案會與系統上的其他規範一起存放於 /fwl 資料夾內。
- 點擊**取消**可返回上一頁，且不新建防火牆檔案。

編輯現有規範：

選擇**編輯規範**可前往編輯頁。您可以編輯非有效的防火牆規範。

「警告」頁：如果您嘗試編輯有效且已啟用的規範，警告頁就會開啟：

「編輯有效的防火牆規範，會立即套用所有變更。建議您先停用防火牆、測試規範，然後再啟用。」

- 點擊**套用**可退出「警告」頁並返回「編輯規範」頁。
- 點擊**取消**可退出「警告」頁並返回「建立 / 編輯規範」頁。

1. 從規範名稱下拉式清單中選擇您想要編輯的規範，然後點擊**編輯規範**。
2. 點擊**新增規則**或選擇現有規則的**優先程度**，可前往**編輯規則**頁。從此頁面中，您可以變更規則設定或刪除已選取的規則。

設定	說明
優先程度	如果 2 項規則有衝突，較高優先程度的規則會決定後續動作。 最高優先程度為 1，最低為 250。
鍵入	主機：在「IP/ 任何」欄位中，可輸入單一 IP 位址。 子網路：在「IP/ 任何」欄位中，可輸入子網路位址。 範圍：在「IP/ 任何」欄位中，可輸入 IP 位址範圍。
IP/ 任何	指定套用此規則的 IP 位址或位址範圍，或選擇下列其中之一： • 任何：無論 IP 位址為何皆套用此規則。 • anyipv4：此規則套用至任何 IPv4 位址。 • anyipv6：此規則套用至任何 IPv6 位址。
連接埠	指定要套定此規則的連接埠。 • 無：此規則會套用至任何連接埠。 • 通用配置連接埠：選擇標準連接埠。 • 其他：指定非標準連接埠編號。
協定	指定要套定此規則的協定。 • 任何：任何協定。 • tcp：用於應用程式間的可靠資訊傳輸。 • udp：替代 TCP，用於較快速、較低頻寬的資訊傳輸。雖然較少延遲，但 UDP 的可靠性不及 TCP。 • icmp：用於報告錯誤以進行疑難排解。 • icmpv6：用於報告錯誤，針對使用 IPv6 的應用程式進行疑難排解。
行動	允許：允許符合此規則的封包。 捨棄：捨棄符合此規則的封包。

設定	說明
日誌	如果此規則套用至封包，無論封鎖或允許該封包，都會在防火牆日誌中新增記錄項目。相關詳細資訊，請參閱「 防火牆日誌 」。

建議您在防火牆規範中，將下列項目之一新增為最低優先程度規則：

- 若要將防火牆當作允許清單，請新增
priority 250, destination host any, source host any, protocol any, action discard
- 若要將防火牆當作封鎖清單，請新增
priority 250, destination host any, source host any, protocol any, action allow

刪除規範：

選擇**刪除規範**可開啟「確認刪除」頁。

點擊**套用**可確認，且選取的防火牆檔案會從檔案系統中移除。

路徑：配置 > 安全 > 防火牆 > 載入規範

從裝置外部來源上傳規範（後置為 .fwl）。

路徑：配置 > 安全 > 防火牆 > 測試

暫時執行所選規範的規則達您所指定的時間。

802.1X 安全配置

路徑：配置 > 安全 > 802.1X 安全

在以 IEEE 802.1X 連接埠為基礎的網路存取控制中使用的 EAPoL（區域網路可延伸的驗證通訊協定）架構中，NMC 支援 EAP-TLS 驗證方法。

EAP-TLS 在 TLS 握手中執行雙向驗證，這樣網路可對 NMC 進行驗證，NMC 也可對網路進行驗證。NMC 必須先安裝終端實體憑證及其關聯的私密金鑰。此憑證在握手期間會傳遞給驗證器。驗證器的憑證在握手期間也會傳遞給 NMC。為了使 NMC 驗證此憑證，它還必須為簽署此憑證的 CA（如果使用信任串鍊，則為根 CA）安裝憑證。這些憑證必須使用憑證載入器安裝至 NMC 的憑證存放區。請參閱「SSL 憑證」。

Web UI 提供以下選項用於 EAPoL 配置：

設定	說明
EAPoL 存取	使用 EAP-TLS 驗證方法啟用 IEEE 802.1X 驗證 (EAPoL)。 註：802.1X 安全存取預設為停用。只有在提供有效憑證及私密金鑰的有效複雜密碼時，您才可以啟用存取。請參閱「 SSL 憑證 」。
要求者識別碼	要傳送給驗證器的 EAP 要求者身分（含空格最多 32 個字元）。 註：要求者識別碼預設設定為「NMC-Suplicantxx:xx:xx:xx:xx:xx」，其中六個「xx」八位元字節是 NMC 的 MAC ID。
用戶端憑證	要在 EAP-TLS 驗證握手中使用的 NMC 的用戶端憑證。系統會提供已安裝的終端實體憑證的清單，並且必須從中選擇一個。可於「SSL 憑證」頁面上安裝用戶端憑證。

SSL 憑證

路徑：配置 > 安全 > SSL 憑證

NMC 支援 TLS（傳輸層安全性）與 SSL（安全通訊端層），透過為連線新增驗證與加密，在 TCP 之上提供一個安全層。為支援 TLS/SSL 連線，NMC 提供可以上傳 X.509 憑證與私密金鑰的憑證存放區。CA（憑證授權單位）憑證與終端實體憑證皆可上傳。

此頁面顯示包含所有已安裝憑證的清單。請按一下憑證的一般名稱，以導覽至憑證詳情頁面。詳情頁面提供憑證相關的其他資訊，並允許解除安裝包含該憑證的檔案。

上傳 CA 憑證	
設定	說明
憑證檔案	提供 CA 憑證。支援的檔案格式為 PEM 與 DER 編碼的 X.509。副檔名應為 .crt、.cer、.pem 或 .der。 PEM 檔案可能包含任何數量 CA 憑證的清單。

上傳本機裝置憑證	
設定	說明
憑證檔案	提供終端實體憑證。支援的檔案格式為 PEM 與 DER 編碼的 X.509。副檔名應為 .crt、.cer、.pem 或 .der。PEM 檔案可能包含首個憑證為終端實體憑證的憑證鏈。之後的憑證必須為中介 CA，讓各憑證驗證之前的憑證。
私密金鑰檔案	為終端實體憑證提供私密金鑰。檔案可加密或未加密，且必須為 PEM 或 DER 編碼，並使用 PKCS#8 格式。副檔名必須為 .p8、.key、.pem 或 .der。註：所有私密金鑰在儲存前皆由 NMC 加密。
私密金鑰複雜密碼	提供複雜密碼用於解密已加密的私密金鑰。包括空格最多 64 個字元。若私密金鑰檔案未加密，此欄位必須留白。

配置設定值：2

您可利用配置功能表選項來設定 UPS 及 NMC 的基本作業值。

請參見以下各節及「配置設定值：1」。

- 「配置功能表的網路」
- 「通知功能表」
- 「一般功能表」
- 「配置功能表的日誌」



註：您可透過配置摘要頁面檢視部分配置設定 (配置 > 網路 > 摘要)。

配置功能表的網路

IPv4 的 TCP/IP 設定頁面

路徑：配置 > 網路 > TCP/IP > IPv4 設定

本選項顯示 網路管理卡 3 (NMC) 的任何目前 IPv6 設定值。您可在頁面下方配置這些設定值，包括停用 IPv6。



有關 DHCP 及 DHCP 選項的說明，請參見 [RFC2131](#) 及 [RFC2132](#)。

選項	說明
手動	於此指定 IPv4 位址、子網路遮罩、預設閘道。
BOOTP*	裝置會每隔 32 秒向任何 BOOTP 伺服器請求網路指定： • 收到有效的回應後，即開始網路服務。 • 如已有先前配置的網路設定值，且在 5 次請求（第一次請求後再加四次）後仍未收到有效的回應，系統會依預設使用先前的設定值。此可確保在無 BOOTP 伺服器可用時仍可存取。 • 若有找到 BOOTP 伺服器，但提出的請求無效或逾時，則裝置在重新啟動前會停止請求網路設定值。
DHCP*	裝置會每隔 32 秒向任何 DHCP 伺服器請求網路指定： • 若有找到 DHCP 伺服器，但提出的請求無效或逾時，則裝置在重新啟動前會停止請求網路設定值。 • 您亦可將裝置設為須有廠商的特定 cookie 才接受 DHCP 位址，以便接受指定開始網路服務。 請參見「DHCP 回應選項」。

* 廠商等級：APC

用戶 ID：裝置的 MAC 位址。修改後的新 MAC 值在 LAN 上必須為唯一。

使用者等級：應用韌體模組的名稱，請參見「NMC 韌體升級」。

IPv6 的 TCP/IP 設定頁面

路徑：配置 > 網路 > TCP/IP > IPv6 設定

本選項顯示 網路管理卡 3（NMC）的任何目前 IPv6 設定值。您可在頁面下方配置這些設定值，包括停用 IPv6。

您可選擇手動或自動 IP 定址。兩者可同時使用。**手動配置**：勾選其核選方塊，輸入**系統 IP v6** 位址及**預設閘道**。

勾選**自動配置**核選方塊啟用系統，從路由器獲得定址前綴（如有）。系統會用這些前綴自動配置 IPv6 位址。

IPv6 可能的格式	說明
fe80:0000:0000:0000:0204:61ff:fe9d:f156	IPv6 的完整格式
fe80:0:0:0:204:61ff:fe9d:f156	省略前置 0
fe80::204:61ff:fe9d:f156	縮減 IPv6 位址內的多個 0 為 ::
fe80:0000:0000:0000:0204:61ff:254.157.241.86	IPv4 格式的位址在末端
fe80:0:0:0:0204:61ff:254.157.241.86	省略前置 0，IPv4 格式的位址在末端
fe80::204:61ff:254.157.241.86	IPv4 格式的位址在末端，多個 0 縮減
::1	localhost
fe80::	link-local 首碼
2001::	global unicast 首碼

有關 **DHCPv6 模式**，請參見下表。

DHCPv6 模式的 IPv6 配置	
選項	說明
被路由器控制的	選擇此按鈕方塊後，DHCPv6 會受從 IPv6 路由器廣播收到的旗標 M（被管理的位址配置旗標）及 O（其他狀態式配置旗標）之控制。 收到路由器廣播後，NMC 會檢查 M 及 O 旗標是否設定。NMC 對兩者的解釋如下： • 兩者均未設定：代表區域網路非屬 DHCPv6 架構。NMC 會使用路由器廣播及手動配置來取得非連結區域位址及其他設定。 • M 或 M 及 O 被設定：代表區域網路使用完整的 DHCPv6 位址配置。DHCPv6 被用來取得位址及其他設定值。此稱為「DHCPv6 狀態式」。 M 旗標收到後，DHCPv6 位址配置在相關介面被關閉前一直有效，即使後續路由器廣播封包內未設定 M 旗標亦然。 如先接到的是 O 旗標再接到 M 旗標，NMC 會在收到 M 旗標後進行完整的位址配置。 • 只設定 O：此時 NMC 會發送 DHCPv6 資訊請求封包。DHCPv6 用於配置「其他」設定（如 DNS 伺服器位置），但不提供位址。此稱為「DHCPv6 無狀態式」。
位址及其他資料	DHCPv6 被用來取得位址及其他設定值。此稱為「DHCPv6 狀態式」。
僅限非位址資訊	DHCPv6 用於配置「其他」設定（如 DNS 伺服器位置），但不提供位址。此稱為「DHCPv6 無狀態式」。
永不	DHCPv6 不使用於任何配置設定。

DHCP 回應選項

各有效 DHCP 回應皆含有 NMC 在網路上作業所需的 TCP/IP 設定值。各回應中亦包含其他可影響 NMC 作業的資訊。另請參閱知識庫文章 [FA156110](#)。

廠商特定資訊（選項 43）。NMC 會使用 DHCP 回應中的此一選項來決定 DHCP 回應是否有效。本選項內含 TAG/LEN/DATA 格式、稱作 APC Cookie 的選項。本選項預設為停用。

- **APC Cookie. 標籤 1、長度 4、資料 “1APC”**

選項 43 會通知 NMC 有某個 DHCP 伺服器被配置為服務裝置。

以下為內有 APC cookie 之廠商特定資料的 16 進位範例：

Option 43 = 0x01 0x04 0x31 0x41 0x50 0x43

TCP/IP 選項。NMC 會使用有效 DHCP 回應中的下列選項來定義其 TCP/IP 設定值。除第一個選項外，這些選項的說明請參見 [RFC2132](#)。

- **IP 位址** (DHCP 回應的 yiaddr 欄位，說明如 [RFC2131](#))：DHCP 伺服器指定給 NMC 的 IP 位址。
- **子網路遮罩** (選項 1)：NMC 在網絡上操作所需的子網路遮罩。
- **路由器亦即預設閘道** (選項 3)：NMC 在網絡上操作所需的閘道。
- **IP 位址租期** (選項 51)：NMC IP 位址租期的時間。
- **更新時間，T1** (選項 58)：NMC 獲得 IP 位址租期指定後，再申請租期更新前必須等候的時間。
- **重新綁定時間，T2** (選項 59)：NMC 獲得 IP 位址租期指定後，申請重新綁定該一租期前必須等候的時間。

其他選項。NMC 可使用有效 DHCP 回應中的上述選項。除最後兩個選項外，這些選項的說明請參見 [RFC2132](#)。

- **網路時間協定伺服器** (選項 42)：NMC 可使用的兩個 NTP 伺服器（主要及輔助）。
- **時間偏移** (選項 2)：NMC 子網路以 UTC 為基準的偏移秒數。
- **網域名稱伺服器** (選項 6)：NMC 可使用的兩個 DNS 伺服器（主要及輔助）。
- **主機名稱** (選項 12)：NMC 所要使用的主機名稱（長度最大 32 個字元）。
- **網域名稱** (選項 15)：NMC 所要使用的網域名稱（長度最大 64 個字元）。
- **開機檔案名稱** (DHCP 回應的 file 欄位，說明如 [RFC2131](#))：下載使用者配置檔（副檔名 .ini）的完整正確目錄 - 路徑。DHCP 回應中的 siaddr 欄位可指定 NMC 下載 .ini 檔案的伺服器 IP 位址。下載後，NMC 會以 .ini 檔作為配置設定的啟動檔案。
- **完整正確的域名** (FQDN, 選項 81)：NMC 完整正確的域名。

連接埠加速頁面

路徑：配置 > 網路 > 連接埠速率

連接埠速度設定值用於定義乙太網路連接埠的通訊速率。目前的設定值顯示於 [目前速率](#) 欄。

您可用 [連接埠速率](#) 下的按鈕，變更設定值：

- 對於預設的 [自動 - 協商](#) 設定，網路裝置會協商以盡可能高的速率傳輸。雙方所支援的速率不一致時，以較慢的速率為準。
- 您亦可選擇 **10 Mbps** 或 **100 Mbps**，其各具有下列選項：
 - **半-雙工**（一次只以一個方向通訊）或
 - **全雙工**（在同一頻道上同時以雙向通訊）。

註: 您僅可透過選擇**自動交涉**選項按鈕，將連接埠速度變更為 1000 Mbps。

DNS 頁面

路徑：配置 > 網路 > DNS > 配置

網域名稱系統狀態下的值係顯示目前的狀態及設定。

您可用**手動域名系統設定**來配置域名系統（DNS）：

- 啟用**覆蓋設定 DNS 設定**後，DHCP 等其他來源的配置設定會取代此處的手動設定。
- 指定**主 DNS 伺服器**及（如需要）**輔助 DNS 伺服器**的 IPv4 或 IPv6 位址。NMC 如要發送電子郵件，必須至少設定主 DNS 伺服器的 IP 位址。
 - NMC 等候主 DNS 伺服器回應最多 15 秒後，轉為等候輔助 DNS 伺服器回應。NMC 在回應時間內未收到回應時，無法發送電子郵件。您可用同一網段或相鄰網段的 DNS 伺服器作為 NMC，但不要跨廣域網路（WAN）。
 - 設定 DNS 伺服器的 IP 位址後，進行測試。請參見「測試 DNS 頁面」。
- **系統名稱同步化**：啟用此一選項，將 DNS 主機名稱及 NMC 系統名稱同步化。點擊系統名稱連結進行定義。



DNS 主機名稱及 NMC 系統名稱同步化後，系統名稱按 DNS RFC 限制為有限的字元。未同步化時，系統名稱限制為 255 個字元。

- **主機名稱**：在此配置主機名稱及**域名**欄位配置域名後，使用者可在接受域名的任何 NMC 介面欄位（電子郵件位址除外）輸入主機名稱。
- **域名 (IPv4/IPv6)**：對於 NMC 介面，只需要在此配置域名。在此介面接納域名的所有其他欄位（電子郵件位址除外），NMC 若只有一個主機名稱輸入，則會依預設新增此域名。
 - 避免因新增域名導致指定域名擴充的方法：域名欄位設定為預設值 `somedomain.com` 或 `0.0.0.0`。
 - 避免擴充**特定**主機名稱記錄（例如定義 Trap 接收器時）的方法：在域名結尾加句點。NMC 認定結尾有句點的主機名稱（例如 `mySnmpServer.`）為完整的正確名稱，且不再尾綴域名。
- **域名 (IPv6)**：在此指定 IPv6 域名。

測試 DNS 頁面

路徑：配置 > 網路 > DNS > 測試

您可用本選項發送測試 DNS 伺服器設定值的 DNS 查詢，後者會搜尋 IP 位址。設定伺服器的方法，請參見前述「DNS 頁面」。

在**上一次查詢回應**欄位查看測試結果。

- 在**查詢類型**欄，選擇使用 DNS 查詢的方法；請參見下表。
- 在**查詢類型**欄，按表格說明指定所選查詢類型的值。

選定的查詢類型	要使用的查詢問題
按主機	主機名稱，URL
按 FQDN	完整正確的域名， my_server.my_domain.com
按 IP	伺服器的 IP 位址。
按 MX	郵件交換位址。

Web 存取頁面

路徑：配置 > 網路 > Web > 存取

您可用本選項配置 Web 介面的存取方式。（套用此處所作的變更之前，需先將 NMC 重新啟動。請參見第 25 頁的「有關控制功能表的網路」。）

您可勾選啟用核選方塊，經 **HTTP** 或 **HTTPS** 或兩者，啟用對此 UI 的存取。HTTP 預設為停用，HTTPS 預設為啟用。HTTPS 在傳輸過程中會對使用者名稱、密碼及資料加密；HTTP 則否。

HTTPS 也會用數位憑證驗證 NMC。請參閱 [安全手冊](#) 中的「建立及安裝數位憑證」，以了解如何使用數位憑證。

您可將連接埠設為 5000–32768 間任何未使用的連接埠，以提高安全性。請在瀏覽器的位址欄位，以冒號（:）指定連接埠號碼。例如，連接埠編號為 5000、IP 位址為 152.214.12.114 時：

`http(s)://152.214.12.114:5000`

指定保護瀏覽器和 NMC 間通訊所使用的**最小通訊協定**：**TLS v1.1**、**TLS v1.2** 或 **TLS v1.3**。

您可以開放使用工作階段 Cookie 驗證瀏覽器追蹤功能，只要勾選「**啟用要求驗證 Cookie**」核取方塊即可。

註：工作階段結束時將會移除 Cookie。

使用「**受限制狀態存取**」核取方塊，選取是否要顯示一個註明基本裝置狀態的唯讀公開網頁。預設停用這項功能，但可透過「**當成預設網頁**」選項，使用者存取裝置時若只輸入 IP/主機名稱，就會顯示預設登錄頁面。

Web SSL 憑證頁面

路徑：配置 > 網路 > Web > SSL 憑證

新增、替換或移除安全憑證 SSL（安全插座層）是將瀏覽器及 web 伺服器間資料加密的協定。

狀態值可為：

- 有效的憑證**：NMC 已安裝或產生的有效憑證。點擊此一連結查看憑證內容。
- 未安裝的憑證**：憑證未安裝，或被 FTP 或 SCP 安裝到錯誤的位置。您可用**新增或取代憑證檔案**，將憑證安裝到正確的位置：**/ssl** 於 NMC：
- 產生**：未找到有效的憑證，NMC 正在產生憑證。
- 載入**：NMC 正在啟動憑證。



安裝了無效的憑證，或 SSL 啟用時為載入有效的憑證時，NMC 會耗時一分鐘產生預設憑證，導致介面存取延遲。您可用預設憑證進行基本的加密式安全，但每次登入時，系統會顯示安全警報訊息。

新增或取代憑證檔案：瀏覽用安全精靈產生的憑證。請參閱「建立及安裝數位憑證」（位於 [安全手冊](#) 內），以了解如何使用由安全精靈產生或由 NMC 產生的數位憑證。

移除：刪除憑證亦請參見頁面的說明文字。

控制台頁面

路徑：配置 > 網路 > 控制台 > 存取

路徑：配置 > 網路 > 控制台 > SSH 主機鍵

控制台存取 . 更新 UPS 韌體前，請先啟用控制台存取。請參見「韌體更新畫面」。控制台存取會啟動指令介面（CLI）的使用。

您可勾選啟用核選方塊，經 **Telnet** 或 **SSH** 或兩者，啟用對此一 CLI 的存取。Telnet 預設為停用，SSH 預設為啟用。Telnet 在資料傳輸中不會對使用者名稱、密碼及資料加密，SSH 則反之。

注意：啟用 SSH 時，SCP (SeCure CoPy) 會同時啟用，以便進行安全檔案傳輸。有關 SCP 的使用，詳情請見「**NMC 韌體升級**」

您可將與 NMC 通訊的連接埠變更為任何介於 5000-32768 間未使用的連接埠，以便提高安全性。

- **Telnet 連接埠：**預設為 23。您可用冒號 (:) 或空格，指定 Telnet 用戶端所需的非預設連接埠。

例如，您需用下列 Telnet 指令，指定編號 5000、IP 位址為 152.214.12.114 的連接埠：

```
telnet 152.214.12.114:5000 或 telnet 152.214.12.114 5000
```

- **SSH 連接埠：**預設為 22。指定非預設連接埠的指令格式，請參見 SSH 文件。另請參見下述「SSH 主機密鑰」。

SSH 主機密鑰：以 SSH 進行控制台 CLI 存取時，您可在 SSH 主機密鑰頁面新增、取代或移除主機密鑰。

狀態 顯示主機密鑰（私鑰）是否有效。狀態值可為：

- **SSH 已停用：**無主機密鑰使用中。
- **產生：**未找到有效的主機密鑰，NMC 正在產生主機密鑰。
- **載入：**NMC 正在啟動主機密鑰。
- **有效：**下列某個有效的主機密鑰位在 /ssh 目錄（網路管理卡所需的位置）：
 - 安全精靈所產生的 1024 或 2048 位元主機密鑰
 - 2048 位元 RSA 主機密鑰產生自網路管理卡

新增或取代主機密鑰：上傳安全精靈所產生的主機密鑰。上傳安全精靈所產生的主機密鑰。若要使用安全精靈，請參閱 [安全手冊](#)。使用外部產生的主機密鑰時，請在啟用 SSH 前（用前述的「控制台存取」）先加以載入。

注意：為縮短啟用 SSH 所需的時間，請預先新建及上傳主機密鑰。*未載入主機密鑰即啟用 SSH 時，NMC 會耗時 1 分鐘新建主機密鑰，這段時間內 SSH 伺服器將無法使用。*

移除：刪除主機密鑰亦請參見頁面的說明文字。



使用 SSH 前，請先安裝 SSH 用戶端。大多數 Linux 及其他 UNIX 平台都內建 SSH 用戶端，但 Microsoft Windows 作業系統則否 (Windows 10 除外)。有多家廠商皆提供 Windows 作業系統的用戶端，如 PuTTY，請見 www.putty.org 網站。

SNMP 頁面

SNMPv1 的使用者名稱、密碼及社群名稱都以明文在網路上傳輸。對於高加密安全性的網路。請停用 SNMPv1 存取或設定各社群的存取為讀取。（有讀取權限的社群可接收狀態資訊並使用 SNMPv1 Trap。）

使用 EcoStruxure™ IT 或資料中心專家來管理 EcoStruxure 系統公共網路上的 UPS 時，您必須在 NMC 介面中啟用 SNMPv1 或 SNMPv3。讀取存取可讓 EcoStruxure 裝置接收來自 NMC 的陷阱，但需有寫入存取才能用 NMC 使用者介面將 EcoStruxure 裝置設為陷阱接收器。



如需增強及管理系統安全的詳細資訊，請參閱 [安全手冊](#)。

SNMPv1.

路徑：配置 > 網路 > SNMPv1 > 存取及存取控制

使用**存取**來啟用或停用 SNMPv1，作為與 NMC 通訊的方法之一。



SNMPv1 預設為停用。必須先設定**社群名稱**才可建立 SNMPv1 通訊。



使用 SNMPv2c 須有 SNMPv1 選項的支援。

存取控制：您可配置最多 4 個存取控制記錄來指定可存取 NMC 的網路管理系統（NMS）。點擊社群名稱可進行編輯。

四個可用的 SNMPv1 社群預設為每個都被指定一個記錄。您可編輯這些設定值，套用 *一筆以上的記錄到任一社群*、許多個 IPv4 及 IPv6 位址、主機名稱或 IP 位址遮罩的存取。

- 社群預設為可從網路任何位置存取 NMC。
- 配置多個存取控制記錄給任一社群名稱時，就會有一或多個其他社群無法存取該一裝置。

社群名稱：網路管理站 (NMS) 存取社群所用的名稱。長度上限為 16 個 ASCII 字元。

NMS IP/ 主機名稱：控制 NMS 存取的 IPv4 或 IPv6 位址、IP 位址遮罩或主機名稱。主機名稱或特定 IP 位址（例如 149.225.12.1），限制 NMS 只能在該一位置進行存取。可有 255 個限制存取的 IP 位址如下：

- 149.225.12.**255**：NMS 只能從 149.225.12 網段進行存取。
- 149.225.**255.255**：NMS 只能從 149.225 網段進行存取。
- 149.**255.255.255**：NMS 只能從 149 網段進行存取。
- 0.0.0.0（預設值）亦可表示為 255.255.255.255：NMS 可從任何網段進行存取。

存取類型：NMS 可經社群執行的動作。

- 讀取**：任何時候只能 GETS
- 寫入**：可於任何時候 GETS；無使用者登入 UI 或 CLI 時可 SETS。
- Write+**：任何時候都能 GETS 及 SETS。
- 停用**：任何時候都不能 GETS 及 SETS。

SNMPv3.

路徑：配置 > 網路 > SNMPv3 > 存取、使用者設定檔及存取控制

對 GET、SET 與 Trap 接收器，SNMPv3 會利用使用者設定檔系統來辨認使用者。SNMPv3 使用者必須具有 MIB 軟體程式指定的使用者設定檔，才能執行 GET 與 SET、瀏覽 MIB 與接收 Trap。



SNMPv3 預設為停用。有效的使用者設定檔必須先以複雜密碼啟用 (**驗證複雜密碼、隱私複雜密碼**)，才可建立 SNMPv3 通訊。



欲使用 SNMPv3，您必須擁有支援 SNMPv3 的 MIB 程式。

NMC 支援 SHA-256、SHA 或 MD5 驗證及 AES-256、AES 或 DES 加密。

啟用存取下的 SNMPv3 存取，可啟用與本裝置進行此一方式的通訊。

使用者設定檔：預設顯示其名稱為 **apc snmp profile1** 到 **apc snmp profile4**、無驗證及隱私（無加密）之 4 個使用者設定檔的設定值。點擊清單中的使用者名稱，編輯使用者設定檔的下列設定值。

- **使用者名稱**：使用者設定檔的編碼。SNMPv3 藉由匹配設定檔的使用者名稱及所傳輸之資料封包內的使用者名稱，將 GETs、SETs 及 Trap 對應到使用者設定檔。使用者名稱長度為 32 個 ASCII 字元以內。
- **驗證密碼**：驗證密碼是一個 8-32 個 ASCII 字元組成的密碼，用於驗證經 SNMPv3 與裝置通訊的 NMS 無誤。
也驗證訊息在傳輸中未遭篡改，且以即時的方式通訊。亦即，選項未因複製後於不當時間再次傳送而延遲。
- **隱私密碼**：隱私密碼是一個 8-32 個 ASCII 字元組成的密碼，用於確保 NMS 經 SNMPv3 收自或發到本裝置之資料的隱私（藉由加密）。
- **驗證協定**：SNMPv3 的建置支援 SHA-256、SHA 及 MD5 驗證。必須選擇下列某項。
- **隱私協定**：SNMPv3 的建置支援 AES-256、AES 及 DES 為資料加密與解密的協定。您必須使用隱私協定及隱私密碼，否則 SNMP 請求將不被加密。

亦即，如您未選擇任何驗證協定，就不能選擇隱私協定。

存取控制：您可配置最多 4 個存取控制記錄來指定可存取 NMC 的網路管理系統（NMS）。點擊使用者名稱可進行編輯。

四個使用者設定檔預設為每個都被指定一個記錄。您可編輯這些設定值，套用 **一筆以上的記錄到任一使用者設定檔**、許可多個特定 IP 位址、主機名稱或 IP 位址遮罩的存取。

- 使用該設定檔的所有 NMS 均預設為可存取本裝置。
- 配置多個存取控制記錄給單一使用者設定檔時，就會有一或多個其他使用者設定檔無法存取本裝置。

使用者名稱：選擇下拉清單中，存取控制記錄要配置的使用者設定檔。可用的選項為以「使用者設定檔」選項配置的四個使用者名稱。

NMS IP/ 主機名稱：控制 NMS 存取的 IP 位址、IP 位址遮罩或主機名稱。主機名稱或特定 IP 位址（例如 149.225.12.1），限制 NMS 只能在該一位置進行存取。可有 255 個限制存取的 IP 位址遮罩如下：

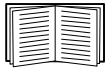
- 149.225.12.**255**：NMS 只能從 149.225.12 網段進行存取。
- 149.225.**255.255**：NMS 只能從 149.225 網段進行存取。
- 149.**255.255.255**：NMS 只能從 149 網段進行存取。
- 0.0.0.0（預設值）亦可表示為 255.255.255.255：NMS 可從任何網段進行存取。

Modbus 頁面



前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置不支援 Modbus。

您可用 Modbus 選項將 NMC 設為使用 Modbus 協定，以連接建物管理系統（BMS）。AP9640 NMC 卡支持 Modbus TCP，AP9641 和 AP9643 NMC 卡除了支持 Modbus TCP 之外还支持 Modbus 串行。



如需在 UPS 上安裝 Modbus 的詳細資訊，請參閱 [APC 網站](#) 上的 *Modbus 文件附錄及 Modbus 暫存器對應*。

有關 Smart-UPS（型號開頭為 SMT、SMX、SURTD、SRC 及 SRT）之 Modbus 切換插座組管理的詳細說明，請參見 [Application Note # 177](#)。



註：Modbus 不支援連上 AP9641 及 AP9643 NMC 之 UIO 連接埠的溫濕度感測器。

Modbus 序列（僅限 AP9641 或 AP9643）。

路徑：**Configuration > Network > Modbus > Serial**

1. 使用 **存取**來啟用或停用 Modbus 序列，作為與 NMC 通訊的方法之一。
2. 設定 Modbus 序列連接的連接參數如下：
 - **鮑率**支援 2400、9600（預設）、19200、38400、57600 或 115200。
 - **同位位元**是設定值可為偶數、奇數或無的檢查碼。
 - **目標唯一 ID**是目標裝置的唯一 ID 碼。其可設定為 1 至 247 間的任何值。
3. 點擊「套用」，儲存設定值。

Modbus TCP.

路徑：**配置 > 網路 > Modbus > TCP**

1. 使用 **存取**來啟用或停用 Modbus TCP，作為與 NMC 通訊的方法之一。
2. 設定 TCP 連接的**連接埠**號碼。連接埠可設定為 502（預設值）或 5000 至 32768 間的任何值。
3. 點擊「套用」，儲存設定值。

BACnet 頁面



前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置不支援 BACnet。

您可用 BACnet 選項將 NMC 設為使用 BACnet 協定，並讓 UPS 資料可提供建物自動化與控制網路使用。



有關透過 BACnet 提供 UPS 資料點的詳細說明，請參見 APC 網站 (www.apc.com) 上的 BACnet 應用程式對應。

BACnet 配置

選項	說明
存取	選擇核取方塊以啟用 BACnet。如果未啟用，無法透過 BACnet 存取 NMC。預設會停用 BACnet。 註：在設定 裝置通訊控制密碼 之後才可啟用 BACnet。
裝置識別碼	此 BACnet 裝置的唯一識別碼，用於辨別裝置的位址。 可接受的範圍：0 – 4194303。
裝置名稱	此 BACnet 裝置的名稱，必須是 BACnet 網路上唯一的名稱。預設裝置名稱為「BACn」+ NMC MAC 位址的後八位數字。最短長度為 1 個字元，最長為 150 個字元，且允許特殊字元。
網路協定	選擇要使用的協定： • BACnet/IP
APDU 逾時	NMC 等候 BACnet 要求回應的毫秒數。可接受的範圍：1000 - 30000。 預設值是 6000。
APDU 重試	NMC 在放棄要求之前嘗試的 BACnet 要求次數。可接受的範圍：1 – 10。 預設值是 3。
裝置通訊控制密碼	裝置通訊控制服務是 BACnet 用戶端所使用，可指示遠端裝置（如已啟用 BACnet 的 NMC）在指定的持續時間內停止初始化或停止回應所有 APDU（裝置通訊控制服務除外）。此服務可用於診斷目的。 指定裝置通訊控制密碼，以確保若未先提供此處設定的密碼，BACnet 用戶端將無法控制 NMC 的 BACnet 通訊。密碼必須介於 8 到 20 個字元之間。 建議在您首次啟用 BACnet 時更新密碼。您就算不知道目前的密碼亦可更新密碼。

BACnet/IP

選項	說明
本機連接埠	NMC 用來傳送與接收 BACnet/IP 訊息的 UDP/IP 連接埠。 可接受的範圍：5000 – 65535。預設：47808。 註：已啟用 BACnet/IP 的 NMC 位址的定義方式是 NMC 的 IP 位址及本機連接埠。

選項	說明
啟用外來裝置註冊	選擇此核取方塊，為 NMC 註冊 BACnet 廣播管理裝置 (BBMD)。 註：若 NMC 子網路上目前沒有 BBMD 或 NMC 與 BBMD 使用不同的本機連接埠，您就必須將 NMC 註冊為使用 BBMD 的外來裝置。 在前述範例中： • BBMD A 管理送往 NMC V 及 W 的廣播訊息。 • BBMD B 管理送往 NMC X 及 Y 的廣播訊息。 • 僅有 NMC Z 需要註冊為使用 BBMD A 或 B 的外來裝置，因為其子網路上不存在 BBMD。 • 註冊後，NMC Z 即可接收來自所註冊 BBMD 的廣播訊息，且可傳送訊息至 BBMD。BBMD 會再將訊息廣播至其子網路上的所有裝置，並透過 IP 路由器廣播至網路上的其他 BBMD。
狀態	外來裝置註冊 (FDR) 狀態： • 外來裝置註冊無效 以下情況時 FDR 無效： – FDR 啟用且 BACnet 停用 – FDR 停用且 BACnet 啟用 – FDR 停用且 BACnet 停用 • 註冊成功 FDR 已成功完成。 • 註冊遭拒 FDR 未成功完成。NMC 會自動重新嘗試註冊，但您也可以切換啟用外來裝置註冊核取方塊，提示 NMC 重新嘗試註冊。 • 註冊已送出 FDR 要求已送出，但尚未完成。
BACnet/IP 廣播管理裝置	NMC 卡將註冊 BACnet 廣播管理裝置的 IP 位址或完整網域名稱 (FQDN)。
連接埠	此 NMC 卡將註冊 BBMD 的連接埠。
TTL	BBMD 將 NMC 維持為已註冊裝置的秒數（存留時間）。若 NMC 在過期前並未重新註冊，BBMD 會從外來裝置表中將其刪除，且 NMC 無法再透過該 BBMD 傳送和接收廣播訊息。TTL 可控制 NMC 註冊該 BBMD 的頻率，因為 NMC 會在過期前嘗試重新註冊。

FTP 伺服器頁面

路徑：配置 > 網路 > FTP 伺服器

您可用本頁面啟用 FTP 伺服器存取並指定連接埠。

選項	說明
存取	FTP 的檔案傳輸不加密。FTP 預設為停用。 請使用 Secure CoPy (SCP) 進行加密檔案傳輸。SCP (透過 SSH) 預設為啟用。但是必須先變更超級使用者預設密碼 (apc) 才可進行檔案傳輸。 如需增強及管理系統安全的詳細資訊，請參閱 安全手冊 。
連接埠	FTP 伺服器的 TCP/IP 連接埠（預設為 21）。 FTP 伺服器使用指定的連接埠以及其下一個連接埠。頁面會顯示可用的非預設連接埠號碼：21 及 5001-32768。 注意：將 FTP 伺服器設為使用非預設連接埠可提高安全性，因為使用者必須在 FTP 指令行加註連接埠名稱到 IP 位址。加註連接埠名稱前，需前綴一個空格或冒號，視所用的 FTP 用戶端而定。

Wi-Fi 畫面（僅限 AP9641、AP9643 和內嵌 NMC3 的裝置）

路徑：配置 > 網路 > Wi-Fi



註：如果在 AP9641/AP9643 網路管理卡的 USB 連接埠或內嵌 NMC 的 UPS 裝置插入選用的 APC USB Wi-Fi 裝置 (AP9834)，則適用此頁面。

[NetworkWiFi] 部分包含特定於 Wi-Fi 使用的設備設定。這些設定不應上傳到有線設備。

您可在本畫面檢視目前的 Wi-Fi 網路狀態、啟用/停用 Wi-Fi 並配置 Wi-Fi 網路設定。

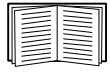


註：啟用/停用 Wi-Fi 將會停用/啟用有線的區域網路連線。Wi-Fi 設定配置完成後將重新啟動 NMC 3。重新啟動後將停用有線網路，且 NMC 3 會嘗試連線至指定 **網路名稱 (SSID)**。

網路名稱 (SSID)：指定 Wi-Fi 網路的網路名稱 (SSID)。長度上限為 32 個字元。

安全性類型：指定 Wi-Fi 網路的安全性類型，並提供驗證詳細資訊：

選項	說明
WPA	Wi-Fi 密碼 ：指定 Wi-Fi 網路的密碼。長度上限為 64 個字元。
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	使用者名稱：WPA2-Enterprise 驗證的使用者名稱。長度上限為 32 個字元。 密碼：WPA2-Enterprise 驗證的密碼。長度上限為 32 個字元。 外部身分：指定 WPA-2-Enterprise 的外部身分。此為 WPA-2-Enterprise 伺服器可選用的未加密身分。例如：user@example.com 或匿名。長度上限為 32 個字元。



如需升級 APC USB Wi-Fi 裝置 (AP9834) 韌體的相關資訊，請參閱 [NMC 3 CLI 指南](#) 中的 Wi-Fi 指令。
若要疑難排解 APC USB Wi-Fi 裝置 (AP9834) 的連線問題，以及瞭解裝置的 LED 燈號說明，請參閱「APC USB Wi-Fi Dongle (AP9834) 問題」。

通知功能表

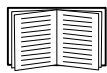
請參見以下各節：

- 「通知種類」
- 「配置事件動作」
- 「電子郵件通知頁面」
- 「SNMP Trap 測試頁面」
- 「SNMP Trap 接收器頁面」

通知種類

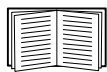
您可配置回應事件的通知動作。您可用下列方式通知事件給使用者：

- 主動、自動通知。指定的使用者或監控裝置直接被通知。
 - 電子郵件通知
 - SNMP Trap
 - Syslog 通知
- 間接通知
 - 事件日誌。未配置直接通知時，使用者藉由查看日誌來判定發生的事件



您亦可記錄系統效能供裝置監控之用。配置及使用此一資料記錄選項的說明，請參見「資料日誌」。

- 查詢（SNMP GET）



詳細的說明請參見「SNMP Trap 接收器頁面」及「SNMP Trap 測試頁面」。SNMP 會啟用 NMS 進行資料查詢。針對傳輸前不加密的 SNMPv1，配置限制最嚴的 READ SNMP 存取方式，以便進行資料查詢且無遠端配置變更的風險。

NMC 支援使用 [RFC1628 MIB](#)（管理資料庫）。設定 Trap 接收器的詳細說明，請參見「SNMP Trap 接收器頁面」。三個事件的 [1628 MIB](#) 群組限用於 MIB，不能用於 Powernet MIB。其可配置如任何事件（參見下述說明「配置事件動作」）。

配置事件動作

按事件配置

路徑：配置 > 通知 > 事件動作 > 按事件

系統預設全部事件均選擇記錄事件。定義個別事件的事件動作：

1. 選擇 [配置](#) 功能表，再選擇 [通知](#)、[事件動作](#) 及 [按事件](#)。
2. 搜尋事件的方法：點擊欄位標題，查看 [電源事件](#)、[環境事件](#) 或 [系統事件](#) 類別下的清單。

亦可點擊各欄位標題下的子類別，如**輸入線路狀態**或**溫度**。

3. 點擊事件名稱，查看或變更目前的配置，例如要透過電子郵件通知的收件人，或要由 SNMP 陷阱通知的 NMS。請參見“**通知參數**”。勾選**事件日誌**核選方塊，啟用或停用本事件的事件日誌記錄。



未配置 Syslog 伺服器時，Syslog 配置相關的項目不會顯示。



查看事件設定詳細資料時，您可啟用或停用事件日誌或 Syslog、停用對個別電子郵件收件人或陷阱接收器的通知，但不能新增或移除收件人或接收器。新增或移除收件人或接收器的說明如下：

- 「找出 Syslog 伺服器」
- 「電子郵件收件人」
- 「Trap 接收器」

按事件組進行配置

路徑：配置 > 通知 > 事件動作 > 按事件組

同時配置一組事件：

1. 選擇**配置**功能表，再選擇**通知**、**事件動作**及**按事件組**。
2. 選擇事件如何組成：
 - 選擇**按嚴重性分組**，然後選取一或多個嚴重性等級。事件嚴重性不能變更。
 - 選擇**按類別分組**，然後選擇一或多個預設組的全部事件。
3. 點擊下一步，執行各個頁面的動作：
 - a. 選擇事件組的事件動作。
 - 選擇預設之**記錄**以外的任何動作前，請先配置至少一個相關的收件人或接收器。
 - 選擇**記錄**且已配置 Syslog 伺服器時，在下一個頁面選擇**事件日誌**或 Syslog，或兩者全選。（請參見「配置功能表的日誌」。）
 - b. 選擇對此事件組啟用或停用新配置的事件動作。

請參見下述「通知參數」。

通知參數 這些配置欄位用於定義傳送事件通知的參數。請參見「按事件配置」及「按事件組進行配置」。

通常可藉由點擊收件人或接收器名稱來使用這些欄位。

欄位	說明
通知延遲	若事件持續指定時間長度（預設為 0），將會發送通知。該時間到期前狀況如已解除，就不會發送通知。
重複間隔	通知會按指定的間隔重複發送（預設為每 2 分鐘重複一次，直到狀況解除）。
初次通知後的通知次數	事件持續期間，通知重複的次數。
或	
持續通知直到狀況解除	通知持續發送，直到狀況解除或排除。

對於有相關解除事件的事件，還可設定下列參數。（有相關解除事件的事件範例為 UPS：與電池組通訊中斷 及 UPS：與電池組通訊恢復。）

電子郵件通知頁面

設定概覽 使用 SMTP，在事件發生時傳送電子郵件給四個收件人。

使用電子郵件功能前，請先配置下列設定值：

- 主要及（非必要的）輔助 DNS 伺服器的 IP 位址。（請參見「DNS 頁面」）
- SMTP 伺服器的 IP 位址或 DNS 名稱，以及至少一個電子郵件收件人的「伺服器」設為「本機」時的寄件人地址。請參閱下述的「SMTP 伺服器」和「電子郵件收件人」。
- 最多四個收件人的電子郵件位址。（請參見「電子郵件收件人」。）



您可用**收件人**選項的**收件位址**設定，將電子郵件-發送到文字型頁面。

SMTP 伺服器 .

路徑：配置 > 通知 > 電子郵件 > 伺服器

本頁面顯示主要及輔助 DNS 伺服器（請參見「DNS 頁面」）及下列欄位：

欄位	說明
外送郵件配置	
寄件位址	NMC 所發送電子郵件的寄件人地址。
SMTP 伺服器	本機 SMTP 伺服器的 IPv4/IPv6 位址或 DNS 名稱。
驗證	若 SMTP 伺服器需要驗證，請啟用此選項。
連接埠	SMTP 連接埠編號，預設值為 25。未加密電子郵件的常用連接埠為 25，SSL/TLS 加密電子郵件的常用連接埠為 465 和 587。您可將連接埠設定變更為 1 - 65535 間的任何連接埠。
使用者名稱 / 密碼 / 確認密碼	若 SMTP 伺服器需要驗證，請於此鍵入您的使用者名稱及密碼。
進階	
使用 SSL/TLS	• 永不：SMTP 伺服器不需要/不支援加密 • 如支援：SMTP 伺服器會廣播對 STARTTLS 的支援，但無需對連接加密。STARTTLS 指令在廣播完成後發送。通常使用連接埠 25。 • 永遠：SMTP 伺服器需先發送 STARTTLS 指令後才能連接伺服器。通常使用連接埠 587。 • 隱含式：SMTP 伺服器只接受有加密的連接。無 STARTTLS 訊息發送到伺服器。通常使用連接埠 465。
需有 CA 根憑證	此項應在貴公司的安全規範不允許對 SSL/TLS 連接作隱含式信任時啟用。若啟用此選項，則必須使用憑證載入器將 SMTP 伺服器的有效 CA 憑證安裝至 NMC 的憑證存放區，以便 TLS 與 SMTP 伺服器成功連接。請參閱「SSL 憑證」頁面。

電子郵件收件人

路徑：配置 > 通知 > 電子郵件 > 收件人

最多可指定四個電子郵件收件人。點擊名稱後配置設定值。另請參見上述「SMTP 伺服器」。

欄位	說明
電子郵件產生	啟用（預設）或停用發送電子郵件給收件人。
收件人位址	收件人的使用者及網域名稱。使用電子郵件進行傳呼時，請用-電子郵件位址作為收件人的傳呼機閘道帳號（例如：myacct100@skytel.com）。傳呼機閘道會產生傳呼內容。 您可用括號中的 IP 位址取代電子郵件域名，以免 DNS 搜尋電子郵件伺服器的 IP 位址；例如用 jsmith@[xxx.xxx.x.xxx] 代替 jsmith@company.com。這可用於 DNS 搜尋異常時。 注意：收件人的傳呼機必須能夠使用文字型訊息。
格式	長格式包括名稱、位置、接點、IP 位址、裝置序號、日期及時間、事件碼以及事件說明。短格式僅有事件說明。
語言	選擇下拉清單中的語言，使任何電子郵件以該語言發送。不同的使用者可設定不同的語言。請參見“變更使用者介面語言”。
伺服器	選擇下列電子郵件路由方式： • 本機：透過本站的 SMTP 伺服器。此選項可確保電子郵件會用本站的 SMTP 伺服器發送。本設定可限制延遲、避免網路故障、長時間重試電子郵件發送。 選擇此一設定時，請啟用裝置 SMTP 伺服器的轉寄功能，並指定特殊的外部電子郵件帳號供轉寄電子郵件接收之用。進行此一變更前，請洽詢 SMTP 伺服器的管理員。 • 收件人：經由收件人的 SMTP 伺服器。NMC 會對收件人電子郵件位址進行 MX 記錄查詢，並以其結果作為 SMTP 伺服器。由於電子郵件只發送一次，因此極易丟失。 註：使用此設定時，寄件人地址會與收件人地址匹配，驗證和加密 (TLS) 將停用，並會使用連接埠 25。 • 自訂：本設定讓各電子郵件收件人有自己的伺服器設定值。選取後，將啟用後續的伺服器設定。這些設定與上述「SMTP 伺服器」中所述設定相同，並與那些設定無關。

SNMP Trap 接收器頁面

Trap 接收器

路徑：配置 > 通知 > SNMP Trap > Trap 接收器

您可藉由簡單網路管理協定（SNMP）Trap，自動接收重大 UPS 事件的通知。這對網路上裝置的監控相當有用。

Trap 接收器會按 **NMS IP/ 主機名稱** 顯示，其中，NMS 代表網路管理系統。您可配置最多 6 個 Trap 接收器。

配置新 Trap 接收器的方法：點擊**新增 Trap 接收器**。編輯或刪除接收器的方法：點擊其 IP 位址 / 主機名稱。

刪除某一 Trap 接收器後，配置於該 Trap 接收器「配置事件動作」下的通知設定全會恢復為預設值。

選擇 **SNMPv1** 或 **SNMPv3** 按鈕，指定 Trap 類型。對於接收**兩種**Trap 的 NMS，請分別配置該 NMS 的兩種 Trap 接收器類型。

欄位	說明
Trap 產生	啟用（預設）或停用此一 Trap 接收器的 Trap 產生。
Powernet MIB Trap 產生器 / RFC1628	對每一新建的 Trap，指定兩種 MIB Trap 之一。 Powernet 選項是針對 Schneider Electric 特製的，且具備與後者產品相關的大量其他變數。RFC1628 是 UPS 裝置的通用、標準 MIB。 使用 RFC1628 MIB 時，亦可使用 RFC1628 事件通知（請參見「配置事件動作」）。其可用於避免配置 NMC 環境外的事件通知，請參見 RFC1628 MIB 。
NMS IP/ 主機名稱：	本 Trap 接收器的 IPv4/ IPv6 位址或主機名稱。預設值 0.0.0.0 代表 Trap 接收器未定義。
語言	選擇下拉清單中的語言。此一語言可與 UI 及其他 Trap 接收器不同。
SNMPv1	社群名稱：SNMPv1 Trap 發送到本 Trap 接收器時用作識別碼的名稱。 驗證 Trap：本選項啟用（預設值）後，NMS IP/ 主機名稱設定所含的 NMS 會收到驗證 Trap（錯誤登入本裝置所產生的 Trap）。
SNMPv3	使用者名稱：選擇使用者設定檔的代號，以用於本 Trap 接收器。另請參見「SNMP 頁面」下的「使用者設定檔」。

SNMP Trap 測試頁面

路徑：配置 > 通知 > SNMP Trap > 測試

上一次的測試結果：最近 SNMP Trap 測試的結果。SNMP Trap 測試成功僅代表已發送 Trap，不代表 Trap 被所選的 Trap 接收器收到。若下列條件皆為真，代表 Trap 測試成功：

- 配置於所選 Trap 接收器的 SNMP 版本（SNMPv1 或 SNMPv3），已在本裝置啟用。
- Trap 接收器本身已啟用。
- **收件人**位址如有設定主機名稱，該一名稱可對應到有效的 IP 位址。

收件人：選擇測試 SNMP Trap 發送的 IP 位址或主機名稱。未配置 Trap 接收器時，頁面會顯示 **Trap 接收器**配置頁面的連結。請參見上述「SNMP Trap 接收器頁面」。

一般功能表

本功能表處理雜項配置，包括：裝置辨識、日期及時間、匯出或匯入 NMC 配置選項、頁面左下角的三個連結，以及彙整資料供進行故障排除。

辨識頁面

路徑：配置 > 一般 > 辨識

定義以下項目使用的**名稱**（NMC 系統名稱，請參閱「DNS 頁面」）、**位置**（物理位置）、**系統訊息**（登入時顯示的自定義訊息）和**聯繫人**（裝置負責人員）：

- NMC 的 SNMP 代理
- EcoStruxure™ IT 或資料中心專家



名稱欄位會被 NMC 之 SNMP 代理的下列物件 ID（OID）使用：sysName、sysContact 及 sysLocation。如需 MIB-II OID 的詳細資訊，請參閱 [APC 網站](#) 上的 *PowerNet® SNMP 管理資訊庫 (MIB) 參考指南*。

日期 / 時間頁面

Mode

路徑：配置 > 一般 > 日期 / 時間 > 模式

設定 NMC 所用的日期及時間。您可手動或經網路時間協定（NTP）伺服器變更目前的設定值：

兩者均選擇**時區**。這是您當地時間與世界標準時間（UTC）—亦稱格林威治標準時間（GMT）之間的差。

- **手動模式**：執行下列之一：
 - 輸入 NMC 的日期及時間，或
 - 勾選**套用本地電腦時間**，查看您所用電腦的日期及時間設定，並套用於此。
- **與 NTP 伺服器同步**：用 NTP 伺服器定義 NMC 的日期及時間。



EcoStruxure™ IT 或資料中心專家隱私側的 NMC，預設使用 EcoStruxure™ IT 或資料中心專家的 NTP 伺服器之時間設定值。

欄位	說明
覆蓋手動 NTP 設定值	選擇本選項後，來自其他來源（通常為 DHCP）的資料會優先於此處設定的 NTP 配置。
主 NTP 伺服器	輸入主要 NTP 伺服器的 IP 位址或域名。
輔助 NTP 伺服器	輸入輔助 NTP 伺服器（如有）的 IP 位址或域名。
更新間隔	定義 NMC 存取 NTP 伺服器以進行更新的間隔時數。 <i>最小</i> ：1； <i>最大</i> ：8760（1 年）。
立即用 NTP 更新	立即用 NTP 伺服器更新日期及時間。

日光節約

路徑：配置 > 一般 > 日期 / 時間 > 日光節約

日光節約時間（DST）預設為停用。您可啟用傳統的美國 DST，或啟用及配置符合當地日光節約時間規定的設定值。

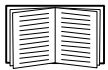
自訂 DST 時，系統會從您於**開始**選項所訂的日期及時間將時鐘提前一小時，以及從您於**結束**選項所訂的日期及時間將時鐘延後一小時。

- 本地 DST 如規定於特定月份的某一**第四**天開始及結束（例如第四個週日），請選擇**第四 / 最後**。即使該月份有五個週日，仍應選擇**第四 / 最後**。
- 本地 DST 如規定於某一月份特定週日的**最後**一次開始及結束（不論是第四或第五個），請選擇**第五 / 最後**。

用配置檔案新建及匯入設定值

路徑：配置 > 一般 > 使用者配置檔案

本選項可讓您用現有的配置設定值，加快及簡化新裝置的配置。您可用**上傳**將配置資料傳送到本介面，以及使用**下載**從本介面進行傳送（再將該檔用於配置其他介面）。檔案名稱預設為 **config.ini**。



取得、修改 NMC 配置檔案的說明，請參見「匯出配置設定值的方法」。

配置連結頁面

路徑：配置 > 一般 > 快速連結

您可用本選項查看並修改顯示於本介面各頁面左下角的 URL 連結。

重新配置連結的方法：點擊**名稱**欄內的名稱。您可點擊**恢復預設值**選項，將連結恢復為預設值。

配置功能表的日誌

路徑：配置 > 日誌 > Syslog > 選項

有事件發生時，NMC 可傳送訊息到最多四個 Syslog 伺服器。Syslog 伺服器會將網路裝置發生的事件集中存至一事件日誌。



本使用手冊未提供 Syslog 本身及其配置值的詳細說明。如需 Syslog 的詳細說明，請參見 RFC5424。

找出 Syslog 伺服器

路徑：配置 > 日誌 > Syslog > 伺服器

欄位	說明
Syslog 伺服器	您可用 IPv4/ IPv6 位址或主機名稱找出接收 NMC 所發 Syslog 訊息的四個伺服器之一。
連接埠	NMC 將用於傳送 Syslog 訊息的連接埠。預設連接埠為 6514，也是指定給安全 Syslog (TLS) 的連接埠。
語言	選擇 Syslog 訊息所用的語言。
協定	在 UDP、TCP 或 TLS 間選擇。
TLS 用戶端憑證	如果所選為 TLS 協定，選擇用戶端憑證將用於在 Syslog 伺服器進行相互驗證。預設選項「無」會停用相互驗證。可於 SSL 憑證 上安裝用戶端憑證。

Syslog 設定值

路徑：配置 > 日誌 > Syslog > 設定值

欄位	說明
訊息產生	啟用以 Syslog 為通知方式之事件 Syslog 訊息的產生及記錄。請參見「配置事件動作」。
設施碼	選擇指定給 NMC Syslog 訊息的設施碼（預設為 User ）。 注意： User 可良好定義 NMC 發送的 Syslog 訊息。除非有 Syslog 網路或系統管理員要求，否則切勿變更此一選擇。

欄位	說明
嚴重性對應	將 NMC 或環境事件的各個嚴重程度對應到可用的 Syslog 優先順序。本機選項為嚴重、警告、通知訊息。請勿修改對應方式。 下列定義取自 RFC5424： • Emergency（緊急）：系統無法使用 • Alert（警報）：必須立即採取行動 • Critical（重大事件）：狀況嚴重 • Error（異常）：狀況異常 • Warning（警告）：警告狀況 • Notice（告知）：正常但重大的狀況 • Informational（通知訊息）：通知訊息 • Debug（除錯）：除錯相關的訊息 本機設定值的預設值如下： • Severe（嚴重）對應到 Critical • Warning（警告）對應到 Warning • Informational（通知訊息）對應到 Info 注意：停用 Syslog 訊息的方法，請參見「配置事件動作」。

Syslog 測試及格式範例

路徑：日誌 > Syslog > 測試

傳送文字訊息到 Syslog 伺服器（以前述「找出 Syslog 伺服器」選項配置。）結果會傳送到所有已配置的 Syslog 伺服器。

選擇要指定到測試訊息的嚴重性後，定義測試訊息。訊息格式為事件類型（APC、系統或裝置等）後接冒號、空格及事件文字說明。訊息長度最大為 50 個字元。

- 優先順序（PRI）：指定給訊息事件的 Syslog 優先順序，以及 NMC 所發訊息的設施碼。
- 標題：時間戳及 NMC 的 IP 位址。
- 訊息（MSG）部分：
 - TAG 欄位，後接冒號加空格、事件類型辨識碼。
 - CONTENT（內容）欄位內含事件文字，後綴（非必要）空格及事件碼。

範例：APC:Syslog 測試正常。

「配置」選單上的 CEIP

路徑：配置 > CEIP > 設定

網路管理卡的客戶經驗改進計畫 (CEIP) 為我們提供資訊，讓我們能改善產品與服務，並協助我們建議您以最佳方式部署和配置 NMC。

若加入 CEIP，我們會收集您在自己環境中配置與使用網路管理卡方式的特定資訊。此資訊完全匿名，因此無法用於識別任何個人的身分。如需詳細資訊，請參閱 [CEIP 常見問題](#)。

測試功能表

測試及校準

路徑：測試 > UPS



某些 UPS 裝置可能無此選項。

不支援對鋰離子 UPS 設備（包括前置 SRTL/SRYLF 的 UPS 設備）執行校正。

某些 UPS 型號可讓您進行自我測試、警報測試或執行校準。**自我測試**及**校準**欄位會顯示最近一次的結果。

執行校準會使 UPS 重新計算目前負載下所餘容量的執行時間。此可確保提供更準確的執行時間資料。校準時，UPS 會暫時耗盡其電池，因此只能在電池容量滿載時進行測試。UPS 的負載必須至少為 15% 且無劇烈波動，以確保校準結果有效。



注意：執行校準會將 UPS 電池深度放電，以致發生停電時可能暫時無法支援其負載。

頻繁校準會減損電池壽命。

大幅提高 UPS 所支援的負載時，務請執行校準。

UPS 的警報測試隨裝置而異，您的 UPS 亦可能未提供此功能。啟用警報的方法，請參見“UPS 一般頁面”。

- 選擇 **UPS 警報測試**後，UPS 會連續發出嗶聲，且 LED 燈號閃亮 4 秒。
- 選擇 **UPS 警報測試 – 連續**後，UPS 會連續發出嗶聲且 LED 燈號閃亮，直到手動取消測試為止。螢幕會獨立顯示提示：**取消連續警報測試**。選擇此提示、點擊套用，即可取消測試。亦可按下 UPS 的 LED 顯示介面上任一鍵來取消測試。此測試可用於找出 UPS。

設定 NMC LED 燈號閃爍

路徑：測試 > 網路 > LED 燈號閃爍

找不到您的 UPS 裝置時，可在 **LED 閃爍期間**欄位輸入分鐘數並點擊套用，NMC 的 LED 燈號即會開始閃爍。此可協助找出實體裝置。

日誌及關於功能表

使用事件及資料日誌

事件日誌記錄個別發生的現象。資料日誌則以定期記錄特定值的方式，提供系統快照。每個事件都包含以下資訊：

事件	說明
日期	事件發生的日期。
時間	事件發生的時間。
使用者	發起操作的使用者。可能會顯示使用者名稱，若為內部服務的一部分則會顯示「系統」，若為連接裝置發起的操作則會顯示「裝置」。
事件	描述事件的文字。
編碼	事件識別碼。（並非所有使用者介面都提供。）

事件日誌

日誌預設顯示所有事件。請參閱「配置事件動作」。

事件日誌會記錄所有事件，包括存取控制、要求錯誤、系統事件、設定變更（包括透過 config.ini 檔案）和稽核事件。可設為存放 25 到 30,000 個事件，預設值為 1500。如果事件日誌已滿且發生新事件，則最早的事件會被覆寫。若要保留事件，則應設定將事件匯出到 Syslog 伺服器。

您可使用配置功能表的「本機使用者」來啟用事件顏色編碼。

註：事件日誌使用 AES-256 ESSIV 進行加密，並在使用前由 NMC 使用 HMAC-SHA256 進行加密驗證。

顯示事件日誌

路徑：日誌 > 事件 > 日誌

事件日誌預設顯示日期最近的事件。點擊**開新視窗顯示日誌**按鈕，將事件集中顯示於頁面。此一功能需先啟動 JavaScript。

以文字檔案開啟日誌或儲存日誌到磁碟的方式如下：點擊**事件日誌**標題欄內同一行的磁片圖示.



您也可用 Secure CoPy (SCP) 或 FTP 查看事件日誌。相關詳細資訊，請參閱「**用 SCP 或 FTP 取得日誌檔案的方法**」。

篩選事件日誌：您可用篩選器排除不想顯示的資料。

用日期或時間篩選日誌	按上一個 或 起自 按鈕 。（篩選器配置在 NMC 重新啟動前一直有效。）
按事件嚴重程度或類別篩選日誌	點擊篩選日誌。取消勾選，將其自頁面移除。點擊事件日誌頁面右上角的 套用 文字，篩選器即開始作用。篩選器被移除或 NMC 重新啟動前一直有效。取消篩選器的方式如下：點擊 篩選日誌 、點擊 取消篩選器（顯示全部） 。管理員可點擊 儲存為預設 ，將篩選器儲存為每一使用者的預設日誌顯示。

有關篩選的注意事項：

- 事件會按「或」邏輯進行篩選。套用某一篩選器後，其他篩選器即無效。
- 在**按嚴重性篩選**清單中已清除的事件，即使在**按類別篩選**清單中挑選，也不會顯示於被篩選的事件日誌上。
- 在**按類別篩選**清單中清除的事件亦然。

刪除事件日誌：點擊**清除日誌**會刪除全部事件。刪除的事件無法復原。



有關按指定嚴重程度或類別停止記錄事件的方法，請參見「按事件組進行配置」。

設定反向搜尋：

路徑：日誌 > 事件 > 反向搜尋

反向搜尋功能啟用後，若發生網路相關事件，網路所連裝置的 IP 位址及網域名稱都會記錄在事件日誌裡。裝置無網域名稱時，則僅記錄其 IP 位址。

由於網域名稱通常比 IP 位址較少變動，反向搜尋有助於找出導致事件發生的網路連接裝置位址。

反向搜尋預設為停用。未配置 DNS 伺服器或因流量過大導致網路效能不佳時，請勿啟用本功能。

重設事件日誌大小

路徑：日誌 > 事件 > 大小

您可使用事件日誌大小來指定事件日誌筆數上限。



注意：重設事件日誌大小到最大限度時，*現有的全部記錄都會刪除*。為避免資料遺失，請先用 SCP 或 FTP 取得日誌。請參閱「**用 SCP 或 FTP 取得日誌檔案的方法**」。日誌記錄達到上限時，較早的記錄會被刪除。

資料日誌

路徑：日誌 > 資料 > 選項

用資料日誌顯示 UPS 的測值：UPS 的電源輸入、UPS 及電池的環境溫度。

註：資料日誌使用 AES-256 ESSIV 進行加密，並在使用前由 NMC 使用 HMAC-SHA256 進行加密驗證。

顯示及重設資料日誌大小的步驟與事件日誌相同，只要改用**資料**而非**事件**下的選項即可。請參見「顯示事件日誌」及「重設事件日誌大小」。

您可用**上一次**或**起自**按鈕，依日期及時間篩選資料日誌。（篩選器配置在 NMC 重新啟動前一直有效）。點擊**清除資料日誌**會刪除資料日誌內的全部記錄。刪除的資料無法復原。

設定資料收集間隔（日誌 > 資料 > 間隔）：在**日誌間隔**設定選項，定義資料收集及儲存於資料日誌的頻率。點擊套用後，可用的儲存天數會重新計算，並顯示於頁面上方。

日誌空間存滿後，最早的記錄會被刪除。避免自動刪除早期資料的方法，請參見下列的「配置資料日誌循環（日誌 > 資料 > 循環）」。

注意：由於間隔設定會指定資料記錄的頻率，*間隔越小*，資料儲存的次數越多，日誌檔案就越大。

配置 資料日誌循環（日誌 > 資料 > 循環）：日誌循環可使資料日誌的內容附加到您依名稱及位置所指定的檔案。換言之，您可在資料刪除前就加以儲存，請參見前述的「設定資料收集間隔（日誌 > 資料 > 間隔）」。

請用此一選項設定密碼保護以及其他參數。

欄位	說明
FTP 伺服器	檔案儲存所在的伺服器 IP 位址或主機名稱。
使用者名稱 密碼	傳送資料到儲存檔案所需的使用者名稱及密碼。此一使用者必須具有讀寫資料儲存檔案及檔案所在目錄（資料夾）的權限。
檔案路徑	儲存檔案的路徑。
檔案名稱	儲存檔案的名稱（ASCII 文字檔），例如 <code>datalog.txt</code> 。 新資料會附加到此檔案，而非將其覆寫。
唯一的檔案名稱	選取此項目可將日誌儲存為 <code>mmddyyyy_<filename>.txt</code> 檔，其中的檔案名稱（filename）是您在前述 Filename 欄位中指定的。 新資料會附加至每日有所不同的檔案。
上傳前延遲 n 小時。	上傳資料到檔案前的小時數（最大 24 小時）。
上傳失敗時，每隔 n 分鐘再試傳。	上傳失敗後，再度試傳前的分鐘數。
最多 n 次	上傳失敗後，
再度試傳直到成功前的次數上限。	一直試傳直到成功為止。

用 SCP 或 FTP 取得日誌檔案的方法

管理員或裝置使用者可使用 SCP 或 FTP 取得以定位點符號分隔的事件日誌檔案 (*event.txt*) 或資料日誌檔案 (*data.txt*) 並將其匯入至試算表。兩者都存在 NMC 上。

- 檔案內含日誌上次刪除或因達到上限被截斷後所記錄的全部事件或資料。
- 檔案內含事件日誌或資料日誌不顯示的內容。
 - NMC AOS 及應用版本
 - 檔案取得的日期及時間
 - 名稱**、**接點**和**位置**的值，以及 NMC 的 IP 位址。
 - UPS 型號名稱（僅限 *data.txt* 檔案）
 - 被記錄事件的唯一**事件碼**（僅限 *event.txt* 檔案）
 - NMC 的日誌記錄採用四位數字年度。您必須在試算表應用程式中選擇四位數字年度的日期格式，才能顯示完整的年度數字。



使用加密式安全協定時，請參見「用 SCP 取得檔案」。使用非加密式安全驗證時，請參見「用 FTP 取得檔案」。



請參閱[安全手冊](#)，瞭解設定您所需安全類型的可用通訊協定和方法。

用 SCP 取得檔案。啟用 NMC 的 SSH，請參閱「控制台存取」。註：以下指令僅為範例。

請用下列指令取得 *event.txt* 檔案：

```
scp <username@hostname> 或 <ip_address>:event.txt ./event.txt
```

請用下列指令取得 *data.txt* 檔案：

```
scp <username@hostname> 或 <ip_address>:data.txt ./data.txt
```

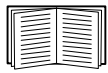
用 FTP 取得檔案 用 FTP 取得 *event.txt* 或 *data.txt* 檔案的方法：

1. 在指令提示下，輸入 `ftp` 及 NMC 的 IP 位址，然後按 ENTER 鍵。

FTP 伺服器 選項（請參見「FTP 伺服器」）的**連接埠**設定如非預設值 (21) 時，FTP 指令應作相對的改變。

在 Windows FTP 用戶端使用下列指令（包括空格）。(某些 FTP 用戶端需要在 IP 位址及連接埠號碼間以冒號取代空格。)

```
ftp>open ip_address port_number
```



使用非預設連接埠號碼加強 FTP 伺服器安全性的方法，請參見「FTP 伺服器」。您可使用 5001 到 32768 間的任何連接埠。

2. 請用大小寫有別的管理員或裝置使用者的**使用者名稱**及**密碼**登入。管理員的預設使用者名稱是 `apc`。裝置使用者的預設使用者名稱是 `device`。
3. 如要將檔案傳輸模式設為二進制，請輸入：

```
ftp >bin
```

若要在檔案傳輸時顯示進度，請輸入：

```
ftp>hash
```

4. 用 `get` 指令將日誌文字檔傳輸到本機磁碟。

```
ftp>get event.txt
```

或

```
ftp>get data.txt
```

5. 您可用 `del` 指令，刪除兩種日誌的內容。

```
ftp>del event.txt
```

或

```
ftp>del data.txt
```

刪除前系統不會提示確認訊息。

- 清除資料日誌時，事件日誌會記錄一筆日誌已刪除事件。
- 清除事件日誌時，新產生的 *event.txt* 檔案會記錄此一事件。

6. 在 `ftp>` 提示下，輸入 `quit` 指令，結束 FTP 程式。

UPS 日誌

路徑：日誌 > UPS



某些 UPS 裝置可能無此功能表選項。



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「日誌 > 電源事件」。

此資訊來自 UPS 裝置，與 NMC 日誌無關。（與 NMC 「事件日誌」非直接相關，亦非其子集。）

此資訊有助於技術支援團隊解決問題。

UPS 切換日誌 顯示 UPS 內的切換事件表，包括切換到電池及切換到旁路。

UPS 故障日誌 顯示 UPS 內的故障事件表。

能源用量

路徑：日誌 > 能源用量



某些 UPS 裝置可能無此功能表選項。

UPS 裝置的累計能源使用量顯示於頁面上方，按週細分的用量表顯示於頁面下方。

欄位	說明
能源用量	UPS 到目前為止，以瓩 - 小時為單位表示的能源用量。例如：供電給 350 W 燈泡 1000 小時的 UPS，其耗電量即為 350 kWh。
總成本	到目前為止所耗電能的總成本。例如：供電給 350 W 燈泡 1000 小時的 UPS，其耗電量為 350 kWh。電費每度 \$0.10 時，該期間的總成本即為 \$35。
CO ₂ 排放	電力公司為供電至目前為止所耗電能而釋出的 CO ₂ 排放量。

成本及 CO₂ 排放量會依能源種類及配電網路而大有不同。您可從**位置**下拉清單選擇所在的國家，獲得約略的估計值，或點擊**編輯**後，自行輸入成本及排放資料。

編輯產生的自訂位置不會影響該位置的預設值。例如：從下拉清單選擇 **IE-Ireland** 並用編輯功能修改其資料後，下拉清單上方會產生一個 **Custom (IE-Ireland)** 項目。

防火牆日誌

路徑：日誌 > 防火牆

有建置防火牆時，其事件將記錄於此。建置防火牆的詳細說明，請參見「防火牆頁面」。

此資訊有助於技術支援團隊解決問題。

記錄項目包括流量及規則動作（許可、拒絕）的資訊。記錄於此的事件不會再記錄於主事件日誌。請參見「事件日誌」。

防火牆日誌可記錄 50 條最近的事件。NMC 重新啟動後，防火牆日誌會被清除。

關於網路管理卡 3

關於 UPS 裝置

路徑：關於 > UPS



前置 SRTL/SRYLF 且內嵌 NMC 之 UPS 裝置的路徑是「關於 > UPS > 一般」。



UPS 項下顯示的資料內容會依所用的裝置而異。

欄位	說明
型號 / SKU/ 序號	描述您 UPS 裝置的欄位。
製造日期	UPS 的製造日期。
韌體修訂版本	目前安裝於 UPS 的韌體模組版本編號
韌體 Revision2	目前安裝於 UPS 的是韌體版本 2。此版本用於需要不同版本的多個處理器。
明顯的電源額定值	UPS 的總 VA 容量。
真實的電源額定值	UPS 的總負載容量（以瓦為單位）。
明顯的每相電源額定值	UPS 各相的 VA 容量。 深入而言，這是各相目前以 VA 為單位的明顯電源。明顯電源是伏特及安培 RMS（均方根）的積。
真實電源 每相額定	UPS 的總負載容量（以瓦為單位）。 各相目前以瓦為單位 (W) 的有效旁路電源。有效電源是電壓及電流瞬間乘積的時間平均值。
內建電池 SKU/ 外接電池 SKU	這些欄位顯示電池的料號。這可供故障排除或訂購替換零件時之用。

路徑：關於 > UPS > 電源



下方選項只適用於前置 SRYLF 且內嵌 NMC 的 UPS 裝置。

欄位	說明
序號	電源模組的序號。
SKU	電源模組的 SKU。
日期	電源模組的製造日期。
版本	電源模組的韌體版本。

點擊「主要」或「XRn/電池架 n」進入「[主要電池架 / 電池架 n](#)」畫面，深入瞭解電池資訊。

路徑：關於 > UPS > 電池



下方選項只適用於前置 SRTL/SRYLF 且內嵌 NMC 的 UPS 裝置。

欄位	說明
序號	電池架/模組序號。
SKU	電池架/模組的 SKU。
日期	電池架/模組的製造日期。
版本	電池架/模組的韌體版本。

路徑：關於 > UPS > 智慧模組



下方選項只適用於前置 SRYLF 且內嵌 NMC 的 UPS 裝置。

欄位	說明
序號	智慧模組的序號。
SKU	智慧模組的 SKU。
日期	智慧模組的製造日期。
版本	智慧模組的韌體版本。

關於 NMC 及韌體模組

路徑：關於 > 網路

硬體廠商：此項硬體資訊有助於疑難排解 NMC 裝置發生的問題，資訊內容包括機型和序號、硬體版本、製造日期、MAC 位址以及管理使用時間。

管理正常運行時間 指的是此一管理介面持續運行的時間；亦即 NMC 上一次冷或熱開機以來的時間。

應用模組、APC OS (AOS) 以及 開機監控：此資訊可供故障排除以及查看是否有更新版韌體可用，網址：<https://www.apc.com/shop/us/en/tools/software-firmware/>。

現場標籤	說明
Name (名稱)	韌體模組的名稱。 應用模組名稱會依 UPS 裝置類型而異。例如，su 適用於 Smart-UPS 裝置，sy 適用於 Symmetra 裝置。 APC AOS 模組一律命名為 aos，開機監控模組一律命名為 boot。
版本	韌體模組版本編號模組版本編號可能會有不同，但相容的模組會一起發布。切勿混用不同版本的應用模組及 AOS 模組。 請參見「升級韌體」。
Date/Time (日期 / 時間)	建立韌體模組的日期與時間。

另請參見「確認所安裝韌體的版本號碼」。

支援頁面

路徑：前往支援頁面

您可利用本選項將此介面的各種資料彙整為單一壓縮檔案，以便供故障排除及客戶支援之用。資料內容涵蓋事件及資料日誌、配置檔案（請參見「用配置檔案新建及匯入設定值」）及複雜的除錯資料。

點擊**產生日誌**選項，生成檔案後**下載**。系統會詢問您要檢視或是儲存壓縮檔案。

匯出配置設定值的方法

取得及匯出 .ini 檔案

程序彙整

管理員可取得 網路管理卡 3 (NMC) 的 .ini 檔案，並匯出給一或多個 NMC。

1. 關於配置 NMC 設定值及匯出的方法，請參見“用配置檔案新建及匯入設定值”。
2. 從 NMC 取出 .ini 檔案。
3. 至少修改檔案內的 TCP/IP 設定值。
4. 請用 NMC 支援的 FTP 傳送檔案副本到一或多個 NMC。傳送多個 NMC 時，請使用 FTP 或 SCP 腳本或 .ini 檔案公用程式。

每個取出的 NMC 皆使用此檔案來重新配置其設定值，之後再將其刪除。

.ini 檔案內容

從 NMC 取得的 config.ini 檔案內容如下：

- **段落標題及關鍵字**（僅限取得檔案之特定 UPS/NMC 裝置支援者）：段落標題為括號 ([]) 內的類別名稱。關鍵字：位於段落標題之下，用於說明個別 NMC 設定值的標籤。各關鍵字後綴一個等號及（預設或配置的）數值。
- **Override 關鍵字**：此關鍵字是透過其預設值來防止匯出一或多個關鍵字及其依裝置而異的設定值。例如：[NetworkTCP/IP] 段落中，Override 的預設值（NMC 的 MAC 位址）會阻止匯出 SystemIP、SubnetMask、DefaultGateway、BootMode 的設定值。

詳細的步驟

取得設定及取得 .ini 檔案以便匯出：

1. 可能的話，用 NMC 的介面來配置匯出所要的設定值。（直接編輯 .ini 檔案極易出錯。）
2. 以下範例顯示如何使用 FTP，利用命令提示字元型用戶端從已設定的 NMC 取得 config.ini：
 - a. 用 IP 位址開啟與 NMC 的连接：

```
ftp> ip_address
```
 - b. 用管理員使用者名稱及密碼登入。
 - c. 如要將檔案傳輸模式設為二進制，請輸入：

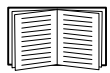
```
ftp >bin
```

若要在檔案傳輸時顯示進度，請輸入：

```
ftp>hash
```
 - d. 取得內含 NMC 設定值的 config.ini 檔案：

```
ftp> get config.ini
```

檔案寫入從該處啟動 FTP 用戶端的資料夾。



若要取得多個 NMC 的配置設定並匯出至其他 NMC，請參閱 [APC 網站](#) 上的 *版本資訊：ini 檔案公用程式*。或者，請參閱知識庫文章 [FA156117](#)。

自訂 . 檔案傳送到其他 NMC 前，請先加以修訂。

1. 您可用文字編輯程式修訂此一檔案。

- 段落標題、關鍵字及預設值不分大小寫，但所定義的字串則需區分。
- 請用相連的引號代表空值。例如：LinkURL1="" 代表 URL 未定義。
- 任何前後有空格或本身已有引號的設定值，均應前後加引號。
- 匯出排程事件的方法：直接在 .ini 檔案中配置其值。
- 匯出最精確系統時間的方法：若接收端 NMC 可使用 NTP 伺服器，請將 NTPEnable 設為 enabled：

```
NTPEnable=enabled
```

亦可將 [SystemDate/Time] 段落匯出為獨立的 .ini 檔案，以減少傳輸時間。

- 新增附註的方法：於各附註行前綴分號 (;)。

2. 將修訂後的檔案複製為同一資料夾內不同名稱的檔案：

- 檔案名稱長度可達 64 個字元，副檔名必須為 .ini。
- 保留原始的修改後檔案供日後使用。*所保留的檔案是您所作附註的僅有紀錄。*

傳送檔案到單一 NMC. 用下列任一方法將 .ini 檔案傳送到另一網路管理卡。

- 在接收端的 NMC 使用者介面，選擇 **配置 - 一般 - 使用者配置檔**。輸入檔案的完整路徑，或使用本機電腦的檔案總管。
- 使用網路管理卡支援的任何檔案傳輸協定，例如 FTP、FTP 用戶端、SCP 或 TFTP。下列範例使用 FTP：
 - a. 在修訂後複製 .ini 檔案儲存的資料夾中，用 FTP 登入您 .ini 檔案匯出之目標的 NMC：


```
ftp> open ip_address
```
 - b. 如要將檔案傳輸模式設為二進制，請輸入：


```
ftp >bin
```

 若要在檔案傳輸時顯示進度，請輸入：


```
ftp>hash
```
 - c. 將複製的修訂後 .ini 檔案匯出到接收端 NMC 的根目錄：


```
ftp> put filename.ini
```

傳送檔案到多個 NMC：請遵循以下步驟：

- 用 FTP 或 SCP 寫一含有將檔案匯到單一 NMC 之重複步驟的腳本。
- 使用批次處理檔案及 .ini 檔案公用程式。



若要建立批次檔並使用公用程式，請參閱 [APC 網站](#) 上的 *版本資訊：ini 檔案公用程式*。或者，請參閱知識庫文章 [FA156117](#)。

上傳事件及錯誤訊息

事件及其錯誤訊息

接收端網路管理卡完成用 .ini 檔案更新設定後，會發生下列事件。

Configuration file upload complete, with *number* valid values

若關鍵字、段落名稱或設定值無效，但接收端 NMC 成功，會另有事件文字說明錯誤。

事件文字	說明
配置檔案警告：第 <i>number</i> 行有無效的關鍵字。 配置檔案警告：第 <i>number</i> 行有無效的值。	有無效關鍵字或值的行會被忽略。
配置檔案警告：第 <i>number</i> 行有無效的段落。	若段落名稱無效，段落內的所有關鍵字 / 值對都會被忽略。
配置檔案警告：第 <i>number</i> 行的關鍵字超出段落。	檔案前端輸入的關鍵字（亦即任何段落標題之前）會被忽略。
配置檔案警告：配置檔案過大。	檔案過大時，上傳會不完整。請縮小檔案或分為兩個檔案後再試。

config.ini 檔案中的訊息

與 NMC config.ini 檔案下載相關的裝置必須被找到，以便納入其配置。裝置（例如 UPS）如不存在或找不到，config.ini 檔案會在相關段落名稱下顯示訊息，而不是在關鍵字及設定值。例如：

UPS not discovered

若不要將裝置配置匯出為 .ini 檔案匯入，可忽略這些訊息。

覆蓋值產生的錯誤

Override 關鍵字及其設定值會於阻擋匯出設定值時，在事件日誌產生錯誤訊息。



有關哪些資料會被覆蓋的詳細說明，請參見「.ini 檔案內容」。

由於被覆蓋的值依裝置而異，且不宜匯出給其他 NMC，請忽略這些錯誤訊息。您可刪除內有 Override（覆蓋）關鍵字及所覆蓋設定值的行，以預防這些錯誤訊息。切勿刪除或變更含有段落標題的行。

NMC 韌體升級

升級韌體

若未訂閱安全 NMC 系統，則可用的最新 NMC3 韌體版本為 2.5.x。安全 NMC 系統 (SNS) 可讓您的連接裝置避開未知的威脅 (IEC 62443-4-2)、符合不斷變動的法規，並在硬體的整個生命週期內保持靈活度，藉以保護您的業務。要瞭解更多資訊，請造訪 www.apc.com/secure-nmc。



Symmetra 裝置目前不需訂閱安全 NMC 系統。

韌體檔案傳輸方法

若要升級一或多個 NMC 的韌體，請從 APC 網站下載適用於應用程式的安全 NMC 系統工具。如需有關如何使用安全 NMC 系統工具的詳細資訊，請參閱 [使用指南](#)。

註：使用安全 NMC 系統工具升級到韌體版本 3.x 需要有效的安全 NMC 系統訂閱方案。

確認升級

上次的傳輸結果碼

可能的傳輸錯誤包括 TFTP 或 FTP 伺服器找不到，或伺服器無法存取、伺服器找不到或無法辨認傳輸檔案，或傳輸檔案毀損。

確認所安裝韌體的版本號碼

路徑：關於 - 網路

請用 Web UI 確認升級後韌體模組的版本。亦可使用 SNMP GET 於 MIB II **sysDescr** OID。在指令介面使用 **about** 指令。

變更使用者介面語言

您可以從登入頁面的「**語言**」下拉式方塊中選取語言，以不同語言顯示 NMC 使用者介面 (UI)。

UI 有九種語言可用：法文、義大利文、德文、西班牙文、巴西葡萄牙文、俄文、韓文、日文和簡體中文。

信任根安全啟動

信任根安全啟動可在 NMC 硬體層面提供增強的安全性。NMC 的處理器會使用 ECDSA，透過使用已知的公開金鑰驗證系統啟動加載器的簽名。系統啟動加載器也會使用 ECDSA，透過使用存放於系統啟動加載器中的 Schneider Electric 韌體簽名 CA 公開金鑰來驗證韌體簽名。

故障排除

網路管理卡存取問題

故障排除的詳細步驟請參見 www.apc.com/support 的知識庫，以及對常見問題的解決方案。如欲聯繫客戶支援，請參見“[APC 全球客戶支援](#)”。

問題	解決方法
Ping 不到 NMC	NMC 的狀態 LED 燈號如為綠色，請嘗試 ping NMC 同一網段的其他節點。如果一樣 ping 不到，代表 NMC 沒有故障。如果狀態 LED 燈號如不是綠色、或 ping 測試成功，請執行下列步驟： • 檢查 NMC 正確裝設於 UPS。 • 檢查各網路連接。 • 檢查 NMC 和 NMS 的 IP 位址。 • 如 NMS 與 NMC 位於不同的實體網路 (或子網路)，請檢查預設閘道 (或路由器) 的 IP 位址。 • 檢查 NMC 子網路遮罩的子網位元數。
無法用終端程式分配通訊埠	用終端程式配置 NMC 前，需先關閉任何使用該連接埠的應用、服務或程式。
無法藉由序列連接來存取指令介面	檢查是否變更鮑率。請嘗試 2400、9600、19200、38400、57600、或 115200。
無法遠端存取指令介面	• 檢查是否使用正確的存取方式：Telnet 或 Secure SHell (SSH)。管理員可啟用這些存取方式。Telnet 預設為停用，SSH 預設為啟用。SSH 和 Telnet 可以分別啟用 / 停用。 • 若使用 SSH，NMC 可能會新建主機密鑰。NMC 新建主機密鑰需時 1 分鐘，這段期間 SSH 無法使用。
無法存取使用者介面 (UI)	• 檢查 HTTP 或 HTTPS 存取是否啟用。 • 請確認所指定的 URL 是否正確 -- 應與 NMC 所用的安全系統一致。SSL 的 URL 應前綴 https 而非 http。 • 檢查是否可 ping NMC。 • 檢查是否使用 NMC 支援的 Web 瀏覽器。請參見“APC 全球客戶支援”。 • 若 NMC 剛重新啟動且系統正在設定 SSL 安全性，NMC 可能正在產生伺服器憑證。NMC 新建此憑證需時 1 分鐘，這段期間 SSL 伺服器無法使用。

SNMP 相關問題

問題	解決方法
無法執行 GET 指令	• 檢查讀取 (GET) 社群名稱 (SNMPv1) 或使用使用者設定檔配置 (SNMPv3)。 • 用指令介面或 UI 檢查 NMC 是否有存取。請參見“SNMP 頁面”。
無法執行 SET 指令	• 檢查 SNMP 是否已啟用。SNMPv1 及 SNMPv3 預設為停用。 • 檢查讀取 / 寫入 (SET) 社群名稱 (SNMPv1) 或使用使用者設定檔配置 (SNMPv3)。 • 用指令介面或 UI 確認 NMS 有寫入 (SET) 存取 (SNMPv1)，或已獲准藉由存取控制清單 (SNMPv3) 存取目標 IP 位址。請參見“SNMP 頁面”。
無法取得 NMS 的 Trap	• 檢查 NMS 的 Trap 接收器是否配置正確的 Trap 類型 (SNMPv1 或 SNMPv3)。 • 針對 SNMP v1，請查詢 <code>mconfigTrapReceiverTable</code> MIB OID，確認 NMS IP 位址顯示正確，且 NMS 的社群名稱與表列社群名稱相符。如有其中一個不正確，請用 SETs 到 <code>mconfigTrapReceiverTable</code> OIDs，或用指令介面或 UI 修改正確的 Trap 接收器定義。 • 針對 SNMPv3，檢查 NMS 的使用者設定檔配置，並執行 Trap 測試。 請參見“SNMP 頁面”、“Trap 接收器”及“SNMP Trap 測試頁面”。
在 NMS 收到的 Trap 無法辨識	請參見 NMS 文件，確認該 Trap 是否納入警報 / TrapTrap 資料庫。

Modbus 問題



有關 AP9641 和 AP9643 卡的 Modbus 配線及序列配置的詳細說明，請參閱 [Modbus 文件附錄](#)。如需 Modbus 暫存器和位元資料的詳細說明，請參閱 [APC 網站](#)上的 [Modbus 暫存器對應](#)。

APC USB Wi-Fi Device (AP9834) 問題

問題	解決方法
無法連線到 Wi-Fi 網路	• 確認 APC USB Wi-Fi 裝置是否已正確插入 AP9641/AP9643 網路管理卡的 USB 連接埠。 • 確認已在 NMC Web UI 或 CLI 中提供正確的 Wi-Fi 設定。 • 確認 NMC 事件記錄中沒有 Wi-Fi 相關事件。如果您輸入的 Wi-Fi 設定錯誤或空白，NMC 就會在事件記錄中留下錯誤記錄。例如：「USB Wi-Fi 裝置錯誤。Wi-Fi 設定。」 若問題仍無法解決，請聯絡網路管理員診斷連線問題。
無法解除裝置上的紅色 LED 燈號恆亮狀態	• 確認已在 NMC Web UI 或 CLI 中提供正確的 Wi-Fi 設定。 • 解決 NMC 事件日誌中任何與 Wi-Fi 相關的事件。例如：「USB Wi-Fi 裝置錯誤。Wi-Fi 設定。」 • 透過其他方法重新啟用有線連線並配置 Wi-Fi 設定： – Web UI (配置 > 網路 > Wi-Fi) – 指令介面 (Wi-Fi 指令) – config.ini 檔案 (NetworkWiFi 部分) 若無法再使用有線連線，請將 micro-USB 連接線 (960-0603) 連接至 NMC 的主機連接埠以存取 CLI，再使用 xferINI 指令傳輸 config.ini 檔案。如需更多資訊，請參閱 NMC 3 CLI 指南。 若問題仍無法解決，請聯絡客戶支援。請參閱「APC 全球客戶支援」。

LED 燈號說明

狀態	說明
熄滅	出現下列狀況之一： • 裝置未插入 AP9641/AP9643 NMC 的 USB 連接埠。 • NMC 的韌體不支援 Wi-Fi。僅 1.4 及以上版本的韌體支援 Wi-Fi。請參閱第 85 頁的「NMC 韌體升級」。 • 裝置無法正常運作。可能需要修理或更換。請聯絡客戶支援。請參閱「APC 全球客戶支援」。
恆亮綠燈	裝置已連線至存取點，但沒有網路活動。
閃綠燈	裝置已連線至存取點，且 Wi-Fi 網路已啟用。
恆亮紅燈	出現下列狀況之一： • 裝置存在永久性錯誤。 • NMC Wi-Fi 設定存在永久性錯誤。 • 連線至存取點時發生無法解決的問題。
閃紅燈	裝置正透過 Wi-Fi 連線至存取點。

兩年原廠保固

此保固僅適用於購買後遵照手冊進行使用的產品。

保固條款

APC 保證其產品自購買之日起的兩年內不會出現材料和工藝方面的缺陷。APC 將對本保固適用的缺陷產品提供維修或更換服務。本保固不適用於因偶然、疏忽或誤用所造成的損壞或以任何方式更改或修改過的產品。缺陷產品或部件的維修或更換並不會延長原始保固期。本保固所提供的任何部件可能是新品，也可能是工廠再製品。

不可轉讓保固

本保固僅適用於正確註冊了產品的原始購買者。產品可透過 APC 網站 www.apc.com 進行註冊。

例外條款

若經 APC 測試和檢測發現，使用者所聲稱的缺陷根本不存在或由使用者或任何第三方誤用、疏忽、安裝或測試不當所致，則 APC 不給予保固服務。若屬下列情況，APC 亦不提供保固服務：未經授權擅自修理或改裝、錯誤或不當的電壓或連接、現場操作條件不當、腐蝕性環境、修理、安裝、暴露於自然環境中、自然因素、火災、失竊、或不按 APC 建議或規格進行安裝、或更改、損壞、移除 APC 序號的任何情形，或者進行其他超出預期使用範圍的操作。

對於根據本協議及其相關條款銷售、維修或提供的產品，APC 在法律或相關法規允許的範圍內不提供任何明示或暗示的擔保。對於本產品的適銷性、滿意度和用於特殊目的適用性，APC 不提供任何形式的暗示擔保。APC 提供與產品相關的技術或其他建議或服務並不會擴大、縮減或影響 APC 的明示擔保，亦不會由此產生任何責任或義務。上述保固和補救措施是排他的，並取代所有其他保固和補救措施。上述保固規定構成 APC 的單方責任，若 APC 違反此類保固規定，則應獨自給予購買者賠償。APC 提供的保固僅授予本產品購買者，任何第三方不得享受本保固。

APC 及其管理人員、主管、子公司或員工對由於使用、維修或安裝產品而產生的任何間接、特殊、後果性或懲罰性的損害賠償概不負責，不論此類損害賠償是源於合同還是民事侵權，是屬於過錯、疏忽還是嚴格責任，或者 APC 是否已被預先告知此類損害賠償發生的可能性，皆不例外。具體而言，APC 對任何費用不承擔責任，例如利潤或收入損失、設備損失、使用設備造成的損失、軟體損失、資料遺失、替代物的成本、第三方索賠或其他方面的費用。

APC 的任何銷售人員、員工或代理商無權對本保固的條款進行任何增補或修改。若有必要，僅可由 APC 管理人員和法律部門以書面形式簽署對本保固條款的修改。

保固索賠

提出保固索賠的客戶，可以透過 APC 網站的支援頁面 (www.apc.com/support) 存取 APC 客戶支援網路。請從網頁頂部的國家 / 地區選項下拉功能表中選擇您所在的國家 / 地區。選擇「Support」（支援）標籤以獲取您所在地區的客戶支援聯絡資訊。

版權聲明

若要檢視網路管理卡 3 版權聲明，請參閱[此處](#)。

無線電頻率干擾



未經保證產品符合規範的一方明確許可而變更或改裝設備將廢止使用者操作該設備之授權。

美國—FCC

本設備經測試符合 A 類數位裝置的限制（符合 FCC 規則第 15 章的要求）。這些限制是為了確保在商業環境中使用本設備時，可提供防止有害干擾的合理保護。此設備會產生、使用和放射無線電頻率能量，若不按照本使用手冊安裝和使用，可能會對無線電通訊產生有害的干擾。在住宅區使用此裝置可能會導致有害干擾。在此情況下使用者可能需要自行承擔消除此干擾的責任。

加拿大 — ICES

Class A 數位設備滿足加拿大的 ICES-003 法規的要求。

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

日本—VCCI

この装置は、クラス A 機器です。この装置を住宅環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

台灣—BSMI

本產品是在第 2 類環境中供商業和工業使用，為避免擾動產生，可能需要一些安裝限制或額外的措施。

澳洲和紐西蘭

注意：本產品屬於 A 類產品。本產品若用於家居環境中可能會產生無線電干擾，若出現此情況，使用者需自行採取適當的措施。

歐盟

本產品符合 EU Council Directive 2004/108/EC 對會員國有關電磁相容性一致性的保護要求。APC 因本產品任何未經許可所為之修改，所導致之電磁相容性不符要求，概不負責。

本產品已按 CISPR 22/European Standard EN 55022 測試符合 Class A Information Technology Equipment 的限制。Class A 設備的限制是在商業及工業環境下，為登記有案之通訊設備提供合理的保護。

注意：本產品屬於 A 類產品。本產品若用於家居環境中可能會產生無線電干擾，若出現此情況，使用者需自行採取適當的措施。

韓國 한국

A 급 기기 (업무용 방송통신기기)

이 기기는 업무용 (A 급) 으로 전자파적합등록을 한 기기이오니판매자 또는 사용자는 이 점을 주의하시기 바라며 , 가정외의지역에서 사용하는 것을 목적으로 합니다 .

APC by Schneider Electric

全球客戶支援

存取客戶支援條款的途徑可能因產品而異。您可透過以下方式獲得客戶支援：

- 造訪 Schneider Electric 網站，以存取 Schneider Electric 知識庫裡的文件並提交客戶支援請求。
 - **www.apc.com**（公司總部）
連接到已針對特定國家 / 地區進行本地化的 Schneider Electric 網站，各個網站均提供客戶支援資訊。
 - **www.apc.com/support/**
透過搜尋 Schneider Electric 知識庫和使用電子支援形式獲取全球-支援。
- 致電或傳送電子郵件聯絡 Schneider Electric 客戶支援中心。
 - 國家當地的支援中心：請前往 **www.apc.com/support/contact** 查看聯絡資訊。

有關如何獲取當地客戶支援的資訊，請與代表或其他向您出售產品的分銷商聯絡。