用户指南

UPS 网络管理卡 3

AP9640、 AP9641、AP9643

带有嵌入式网络管理卡 3 且前缀为 SRTL/SRYLF 的 UPS 设备
包括 SRTL5KRM2UI、 SRTL5KRM2UT、 SRTL5KRM2UJ 和 SRYLF15KRMT

990-91148G-037
2022 年 11 月

Schneider Electric

施耐德电气法律免责声明

施耐德电气不保证本手册所提供信息的权威性、正确性或完整性。本出版物并不是要代替详细说明操作步骤的、特定地点专用的开发计划。因此，对于因使用本出版物而导致的损坏、违规、错误安装、系统故障或任何其他问题，施耐德电气不承担任何责任。

本出版物中所包含的信息是按原样提供的，整理这些信息仅用于评估数据中心的设计与结构之目的。本出版物由施耐德电气依照诚信原则编制。然而，本出版物所包含的信息的完整性或准确性未得到任何明示或暗示的说明或担保。

对于因使用或无能力使用本出版物或内容而导致、引发或相关的任何直接、间接、后果性、惩罚性、特殊或连带的损害赔偿（ 包括但不限于业务、合同、收入、数据、信息损失或业务中断带来的损害赔偿），即使施耐德电气已明确被告知出现此类损害赔偿的可能性，施耐德电气或其任何母公司、子公司或附属公司以及其各自的高管、董事或员工对此不承担任何责任。施耐德电气保留随时更改或更新本出版物内容或其格式的权利，恕不另行通知。

目录

简介

产品说明

特点

Schneider Electric UPS 网络管理卡（AP9640、AP9641、AP9643）以及带有嵌入式网络管理卡 3 且前缀为 SRTL/SRYLF 的 UPS 设备（SRTL5KRM2UI、SRTL5KRM2UT、SRTL5KRM2UJ 和 SRYLF15KRMT）可以使用如下多种开放标准管理安装有网络管理卡的设备：

安全超文本传输协议 (HTTPS)	安全接壳 (SSH)
安全拷贝 (SCP)	Secure Boot with Root of Trust for enhanced security
RADIUS	基于局域网的扩展认证协议 (EAPoL)
楼宇自动化和控制网络协议 (BACnet)	简单网络管理协议版本 1、2c 和 3 (SNMP v1、v2c、v3)
系统日志	Telnet
Modbus	超文本传输协议 (HTTP)
Hypertext Transfer Protocol (HTTP)	

AP9640 网络管理卡：

- 提供 UPS 控制和定期自检功能。
- 提供数据和事件日志。
- 使您能够通过事件记录、电子邮件、系统日志和 SNMP 陷阱设置通知。
- 提供对 PowerChute® Network Shutdown 的支持。
- 支持使用动态主机配置协议 (DHCP) 或引导协议 (BOOTP) 服务器提供 NMC 的网络 (TCP/IP) 值。
- 能够将用户配置 (.ini) 文件从已配置的管理卡导出到一个或多个未配置的管理卡，而不必将文件转换为二进制文件。
- 提供用于认证和加密的安全协议选择。
- 可与 StruxureWare Data Center Expert、 StruxureWare Operations 或 EcoStruxure™ IT 通信。
- 支持 Modbus TCP/IP。
- 支持 BACnet/IP

AP9641 网络管理卡包含 AP9640 网络管理卡的所有功能，并具有以下特性：

- 提供两个支持从 USB 闪存驱动器升级网络管理卡和 UPS 固件的 USB 端口，以及可选 APC USB Wi-Fi 设备 (AP9834)。
- 支持两个通用输入 / 输出端口，您可以连接：
  - 温度传感器 (AP9335T) 或温度 / 湿度传感器 (AP9335TH)
  - 支持两个输入触点和一个输出继电器 （使用可选的附加组件 — AP9810 干触点 I/O 附件）的继电器输入 / 输出接口
- 除了 Modbus TCP/IP 之外，还通过通用 I/O 端口 2 支持 Modbus RTU。有关如何配置 Modbus RTU 的信息，请参阅 《Modbus 文档附录》。

AP9643 网络管理卡包含 AP9640 网络管理卡的所有功能，并具有以下特性：

- 提供两个支持从 USB 闪存驱动器升级网络管理卡和 UPS 固件的 USB 端口，以及可选 APC USB Wi-Fi 设备 (AP9834)。
- 支持一个通用输入 / 输出端口，您可以连接：
  - 温度传感器 (AP9335T) 或温湿度传感器 (AP9335TH)
  - 支持两个输入触点和一个输出继电器 （使用可选的附加组件 AP9810 干触点 I/O 附件）的继电器输入 / 输出接口
- 除了 Modbus TCP/IP 之外，还通过序列 RS485 端口支持 Modbus RTU。有关如何配置 Modbus RTU 的信息，请参阅 《Modbus 文档附录》。

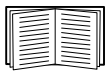
带有嵌入式网络管理卡且前缀为 SRTL/SRYLF 的 UPS 设备具备所有 AP9640 网络管理卡功能（Modbus 和 BACnet 支持除外），而且：

- 提供一个支持从 USB 闪存驱动器升级 NMC 和 UPS 固件的 USB 端口，以及可选的 APC USB Wi-Fi 设备 (AP9834)。

支持的设备

网络管理卡 3 与以下设备兼容：

- 带有 SmartSlot 且前缀为 SMT、 SMX、 SRT 和 SURTD 的 Smart-UPS® 设备，以及 2008 年后制造的 SUA, SURT, SRC 设备 *。
- 单相 Symmetra® UPS 设备。



* 要查看 NMC 3 可安装到的兼容 UPS 的完整列表，请参阅 **APC 网站**上的知识库文章 **FA237786**。

IPv4 初始设置

您必须先为 NMC 定义下列 TCP/IP 设置，然后它才可以在网络上运行：

- NMC 的 IP 地址
- NMC 的子网掩码
- 默认网关的 IP 地址 （只有在您打算退出网段时需要）

注：如果默认网关不可用，则使用与 NMC 处于相同子网且正在正常运行的计算机的 IP 地址。通信量很小时， NMC 使用默认网关测试网络。

注：网络管理卡的 MAC 地址前缀为 00:C0:B7 或 28:29:86。要检查 NMC 的 MAC 地址，请转至关于 > 网络。您可以使用此 MAC 地址前缀来配置 DHCP 服务。

注：请勿使用回送地址 (127.0.0.1) 作为默认网关。否则，将禁用管理卡。之后，您必须使用串行连接登录，并将 TCP/IP 设置重置为默认值。

若要配置 TCP/IP 设置，请参阅网络管理卡 *《安装手册》*，该手册可在 **APC 网站**上找到，并提供印刷版本。

有关如何在 NMC 上使用 DHCP 服务器配置 TCP/IP 设置的详细信息，请参阅 “DHCP 响应选项 ”。

IPv6 初始设置

IPv6 网络配置能够灵活满足您的要求。 IPv6 可在此界面输入 IP 地址的任何地方使用。您可以手动、自动或使用 DHCP 配置，请参阅 “IPv6 屏幕的 TCP/IP 设置 ”。

使用其他应用程序进行网络管理

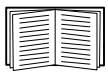
这些应用程序、实用程序和资源与通过 NMC 连接至网络的 UPS 一起工作。

- PowerChute Network Shutdown — 为连接至 UPS 设备的计算机提供无人值守的远程安全关机功能。
- APC PowerNet® MIB — 发现如何通过 SNMP 访问 UPS 设备。
- StruxureWare Data Center Expert — 提供企业级电源管理，并管理 SNMP 代理 （如联网 UPS 设备和环境传感器）。
- EcoStruxure IT — 基于云的监控软件，您可以使用该软件通过 SNMP 和 Modbus 监控您的 UPS 设备。
- 设备 IP 配置向导 — 通过网络配置一个或多个 NMC 的基本设置，请参阅 “ 设备 IP 配置向导 ”。
- 安全向导 — 帮助创建或导入传输层安全 (TLS) 服务器证书和安全接壳 (SSH) 主机密钥，以便保护与 NMC 通信的完整性和机密性。

内部管理功能

概述

使用 Web 用户界面 (UI) 或者命令行界面 (CLI) 查看 UPS 的状态和管理 UPS 及 NMC。您也可以使用 SNMP 监控 UPS 的状态。



有关 UI 的更多信息，请参阅 “Web 用户界面 ” 和 APC 网站上提供的命令行界面 (CLI) 指南。有关如何控制对 NMC 进行 SNMP 访问的信息，请参阅 “SNMP 屏幕 ”。

登录访问优先级

您可以让多个用户同时登录，其中每个用户都具有相同的访问权限。请参阅 “ 会话管理屏幕 ”。

用户帐户类型

NMC 具有不同的访问权限 — 超级用户、管理员、设备用户、只读用户和仅网络用户：

- **超级用户**可以使用 UI 中的所有菜单和命令行界面中的所有命令。超级用户也可以定义附加用户帐户，并为附加用户设置变量。首次登录时默认的用户名和密码均为 apc。登录后系统将提示您输入新密码。
  注：超级用户无法重命名或者删除，但是可以禁用。如果创建附加管理员账户，建议禁用超级用户账户。确保禁用超级用户账户之前，启用至少一个管理员账户。

  管理员可以使用 UI 中的所有菜单和命令行界面中的所有命令。默认用户名为 apc，必须先设置密码，才可启用用户帐户。
- **设备用户**具有对与设备相关的屏幕的读写权限。管理功能 （如 “ 安全 ” 菜单下的会话管理和 “ 日志 ” 下的防火墙）会变为灰色。

  默认的用户名为 `device`，必须先设置密码，才可启用用户帐户。
- **只读用户**具有以下受限的访问权限：
  - 仅通过 UI 访问。
  - 与上述 “ 设备用户 ” 具有相同的菜单访问权限，但是不能修改配置、控制设备、删除数据，或者使用文件传输选项。可以看到配置选项的链接，但无法使用。（事件和数据日志不会对此用户显示任何用于清除日志的按钮）。

  默认的用户名为 `readonly`，必须先设置密码，才可启用用户帐户。
- **仅网络用户**只能通过 Web 用户界面 (UI) 和 CLI （Telnet/SSH 而非串口）登录。无默认名称和密码。

默认情况下，管理员、设备用户、只读用户和仅网络用户帐户为禁用状态，并且在更改超级用户默认密码 (`apc`) 之前无法启用。

若要为管理员、设备用户和只读帐户类型设置用户名和密码值，请参阅 “ 本地用户 ”。

如何重置丢失的密码

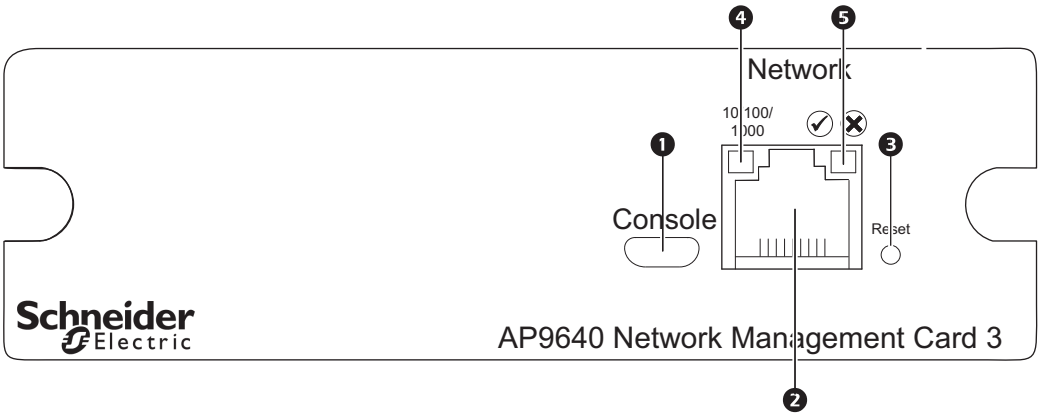
注意：重置 NMC 会将卡重置为默认配置。

如果忘记密码，必须使用 NMC 上的**重置**按钮清除包括密码在内的所有配置。按住**重置**按钮 20-25 秒，确保状态指示灯在此期间闪烁绿色。当状态指示灯变为黄色或橙色时，松开**重置**按钮，允许 NMC 完成其重启过程。

NMC 重新启动后，必须重新配置 NMC。有关详细信息，请参阅 **APC 网站**上提供的 ***《NMC 安装指南》*** 或知识库文章 **FA156064**。

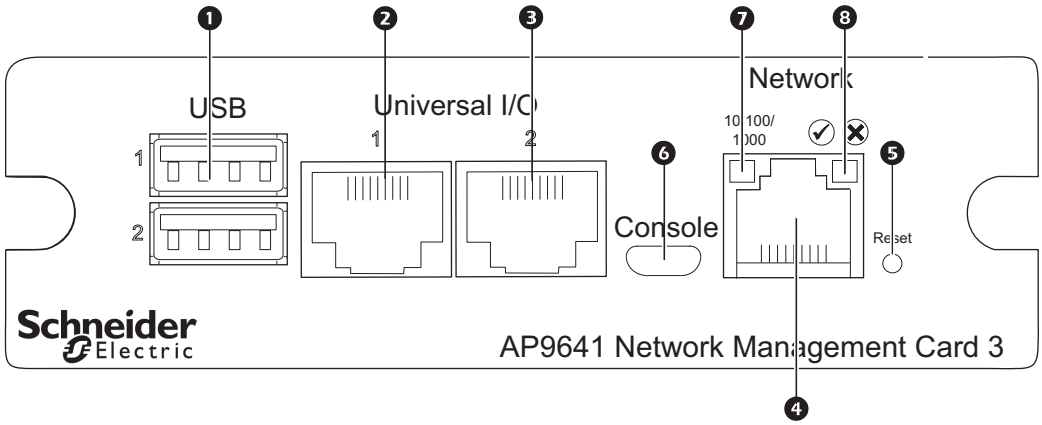
建议您在配置 NMC 后导出 .ini 文件，以防止在丢失密码时丢失数据。请参阅 “ 检索和导出 .ini 文件 ”。

前面板 (AP9640)



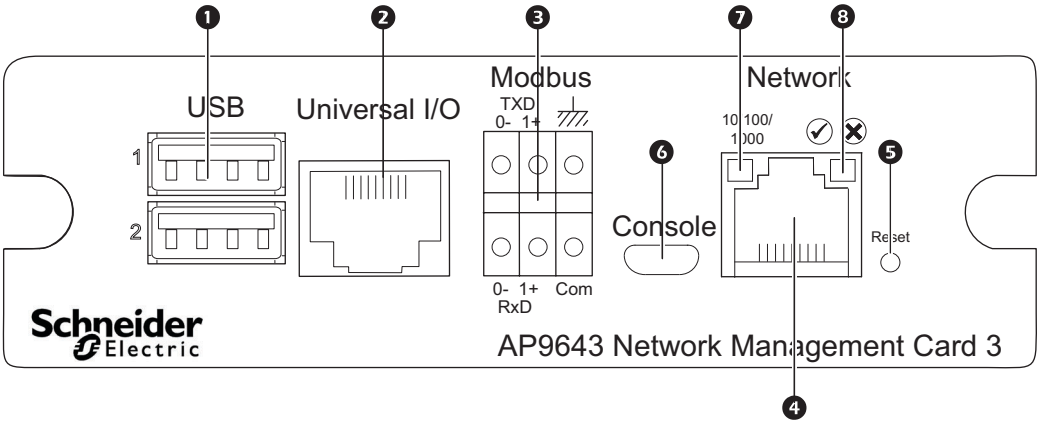
	项目	说明
1	USB 控制台端口	通过 micro-USB 线缆 （APC 部件号 960-0603）将 NMC 连接到本地计算机，以配置初始网络设置或访问命令行界面 (CLI)。
2	10/100/1000 Base-T 接口	将 NMC 连接到以太网。
3	“ 重置 ” 按钮	重新启动网络管理界面。**注：**这不会影响安装 NMC 的设备的输出电源。
4	Link-RX/TX (10/100/1000) 指示灯	请参阅 “Link-RX/TX (10/100/1000) 指示灯 ”。
5	状态指示灯	请参阅 “ 状态指示灯 ”。

前面板 (AP9641)



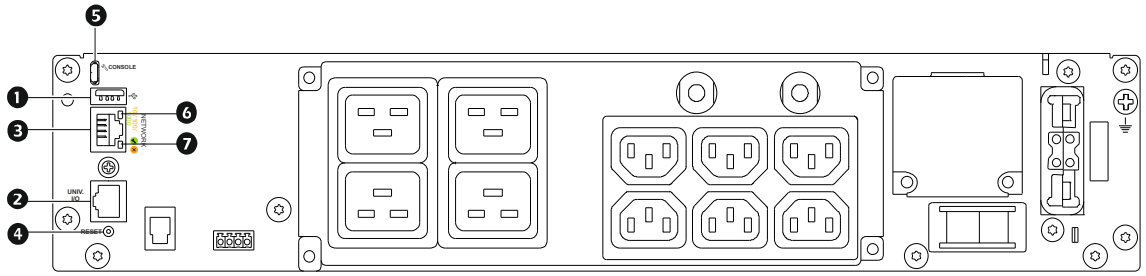
	项目	说明
1	USB 端口	支持网络管理卡和 UPS 固件更新和可选 APC USB Wi-Fi 设备 (AP9834)。请参阅 “ 文件传输 ”、“ 通过 USB 驱动器更新 UPS 固件 （仅限 AP9641、 AP9643 和 SRTL/SRYLF 设备） ” 和 “Wi-Fi 屏幕 （仅限 AP9641、 AP9643 和 SRTL 设备） ”。
2 **3**	通用 I/O 端口	连接温度传感器、温度 / 湿度传感器和继电器输入 / 输出附件接口至 UIO 端口。继电器输入 / 输出附件具有两个输入触点和一个输出继电器。
4	10/100/1000 Base-T 接口	将 NMC 连接到以太网。
5	“ 重置 ” 按钮	重新启动网络管理界面。**注：**这不会影响安装 NMC 的设备的输出电源。
6	USB 控制台端口	通过 micro-USB 线缆 （APC 部件号 960-0603）将 NMC 连接到本地计算机，以配置初始网络设置或访问命令行界面 (CLI)。
7	Link-RX/TX (10/100/1000) 指示灯	请参阅 “Link-RX/TX (10/100/1000) 指示灯 ”。
8	状态指示灯	指示灯 （发光二级管）为光源。请参阅 “ 状态指示灯 ”。

前面板 (AP9643)



	项目	说明
1	USB 端口	支持网络管理卡和 UPS 固件更新和可选 APC USB Wi-Fi 设备 (AP9834)。请参阅 “ 文件传输 ”、 “ 通过 USB 驱动器更新 UPS 固件（仅限 AP9641、 AP9643 和 SRTL/SRYLF 设备） ” 和 “Wi-Fi 屏幕（仅限 AP9641、 AP9643 和 SRTL 设备） ”。
2	通用 I/O 端口	连接温度传感器、温度/湿度传感器和继电器输入/输出附件接口至 UIO 端口。继电器输入/输出附件具有两个输入触点和一个输出继电器。
3	Modbus端口	将 NMC 连接到楼宇管理系统 (BMS)。包含两个接线盒插头（部件号 730-0532）。若要验证您的 UPS 是否支持 Modbus，请参阅您的 UPS 文档。
4	10/100/1000 Base-T 接口	将 NMC 连接到以太网。
5	重置按钮	重新启动网络管理界面。**注意**：这不会影响安装 NMC 的设备的输出电源。
6	USB 控制台端口	通过 micro-USB 线缆（APC 部件号 960-0603）将 NMC 连接到本地计算机，以配置初始网络设置或访问命令行界面 (CLI)。
7	Link-RX/TX (10/100/1000) 指示灯	请参阅 “Link-RX/TX (10/100/1000) 指示灯”.
8	状态指示灯	指示灯（发光二级管）为光源。请参阅 “状态指示灯”。

SRTL UPS 设备后面板 （SRTL5KRM2UI、SRTL5KRM2UT、 SRTL5KRM2UJ）



注意：上图描述内容关于 SRTL5KRM2UI。 .

	项目	说明
1	USB 端口	支持 NMC 固件更新和可选 APC USB Wi-Fi 设备 (AP9834)。请参阅 “ 文件传输 ” 和 “Wi-Fi 屏幕 （仅限 AP9641、 AP9643 和 SRTL 设备） ”。
2	通用 I/O 端口	将温度传感器、温度 / 湿度传感器和继电器输入 / 输出附件接头连接至 UIO 端口。继电器输入 / 输出附件具有两个输入触点和一个输出继电器。
3	10/100/1000 Base-T 接口	将 NMC 连接到以太网。
4	重置按钮	重新启动网络管理界面。**注意：**这不会影响安装 NMC 的设备的输出电源。
5	USB 控制台端口	通过 micro-USB 线缆 （APC 部件号 960-0603）将 NMC 连接到本地计算机，以配置初始网络设置或访问命令行界面 (CLI)。
6	Link-RX/TX (10/100/1000) 指示灯	请参阅 “Link-RX/TX (10/100/1000) 指示灯 ” 。
7	状态指示灯	指示灯 （发光二级管）为光源。请参阅 “ 状态指示灯 ”。

指示灯说明

状态指示灯

该指示灯 （发光二极管）显示 NMC 的状态。

状态	说明
关闭	存在以下情况之一： • NMC 并未接通输入电源。 • NMC 运行不正常。它可能需要修理或更换。联系客户支持。请参阅 “Schneider Electric 全球客户支持 ”。
稳定绿色	NMC 的 TCP/IP 设置有效。
稳定橙色	存在以下情况之一： • 在 NMC 中检测到硬件故障。联系客户支持。请参阅“Schneider Electric 全球客户支持”。 • NMC 处于 Bootmonitor 模式下。请参阅“关于 NMC 和固件模块”。
闪烁绿色	NMC 的 TCP/IP 设置无效。 [1]
闪烁橙色	NMC 正在发出 BOOTP 请求。 [1]
交替闪烁绿色和橙色	如果指示灯缓慢闪烁，表明 NMC 正在发出 DHCP[2] 请求。 [1] 如果指示灯快速闪烁，表明 NMC 正在启动。

1. 如果您没有使用 BOOTP 或 DHCP 服务器，请参阅印刷版和 APC 网站上提供的 PDF 格式的网络管理卡《安装手册》，以便配置 NMC 的 TCP/IP 设置。
2. 若要使用 DHCP 服务器，请参阅 “DHCP 响应选项 ”。

注意：如果在 NMC 启动时连接了 micro-USB 线缆，NMC 将等待 90 秒，以留出时间访问 Boot Monitor。请参阅“使用 XMODEM 升级一个 NMC”。在此延迟期间，没有 LED 处于活动状态。如果不需要在本地访问 CLI，建议断开 micro-USB 线缆。

Link-RX/TX (10/100/1000) 指示灯

该指示灯显示 NMC 的网络状态。

状态	说明
关闭	存在以下一种或多种情况： • NMC 并未接通输入电源。 • 将 NMC 连接至网络的缆线已断开或出现故障。 • 将 NMC 连接至网络的设备已关闭或运行不正常。 • NMC 本身运行不正常。它可能需要修理或更换。联系客户支持。请参阅 “Schneider Electric 全球客户支持 ”
稳定黄色	NMC 连接到通信速度为每秒 10-100 兆 (Mbps) 的网络。
稳定绿色	NMC 连接到通信速度为 1000 Mbps 的网络。
闪烁黄色	NMC 以 10-100 Mbps 的通信速度接收或传送数据包。
闪烁绿色	NMC 以 1000 Mbps 的通信速度接收或传送数据包。

Watchdog 功能

概述

NMC 3 使用内置的全系统 watchdog 机制检测内部问题并从意外输入复原。在其重新启动以从内部问题中复原后，事件日志中将记录**系统：已重新启动网卡**事件。

网卡 watchdog 机制

NMC 3 实施内置的 watchdog 机制，防止自身无法通过网络进行访问。例如，如果 NMC 3 在 9.5 分钟内没有接收到任何网络流量 （直接流量，例如 SNMP，或广播流量，例如地址解析协议 [ARP] 请求），则可以认为网卡有问题，并重新启动。

重置网络定时器

如果网络闲置 9.5 分钟，为了确保 NMC 3 不重新启动，它将尝试每 4.5 分钟与默认网关进行联络。如果网关存在，它会向 NMC 3 做出响应，并且该响应会重新启动 9.5 分钟定时器。如果您的应用程序不需要或者没有网关，请指定在网络上运行且位于同一子网的计算机的 IP 地址。该计算机的网络流量将尽量频繁地重新启动 9.5 分钟定时器，以防止 NMC 3 重启。

自动注销

默认情况下，用户将在 3 分钟不活动后自动从 NMC Web 和 CLI 界面注销。每个用户的默认注销时间可以通过 Web 界面进行调整：

配置 > 安全 > 本地用户 > 管理。

- 单击要更改的帐户用户名的超链接。
- 在 “ 会话超时 ” 下，修改分钟数。

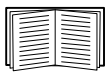
自动注销	持续时间 （分钟）
默认设置	3
最小值	1
最大值	60 （1 小时）

Web 用户界面

简介

概述

通过 Web 用户界面 (UI) 上的选项可以管理 UPS 和 UPS 网络管理卡 3 (NMC 3) 以及查看 UPS 的状态。



有关如何选择、启用和禁用控制访问 UI 的协议以及针对这些协议定义 Web 服务器端口的信息，请参阅 “Web 访问屏幕 ”。

支持的 Web 浏览器

NMC 3 Web UI 与以下操作系统兼容：

- Windows® 操作系统：
  - 已打开兼容性视图的 Microsoft® Internet Explorer® (IE) 8.x 或更高版本
  - 最新版本的 Microsoft® Edge®

注：若要通过 Internet Explorer® 查看 UPS 固件更新屏幕，请使用已打开兼容性视图的版本 10 或更高版本。UPS 固件更新屏幕不与 Edge® 浏览器兼容。请参阅第 33 页 “ 固件更新屏幕 ”。

- 所有操作系统：
  - 最新版本的 Mozilla® Firefox® 或 Google® Chrome®

其他常用的浏览器或许可以使用，但尚未经过全面测试。

NMC 无法与代理服务器一起工作。您必须执行以下操作之一，才能访问 NMC 的 UI：

- 配置 Web 浏览器，为 NMC 禁用代理服务器。
- 配置代理服务器，确保其不会代理 NMC 的特定 IP 地址。

如何登录

概述

您可以使用 NMC 的 DNS 名称或系统 IP 地址，作为 UI 的 URL 地址。使用您的用户名和密码登录（注意区分大小写）。默认的用户名视帐户类型而异：

- 管理员或超级用户为 `apc`
- 设备用户为 `device`
- 只读用户为 `readonly`

另请参阅 “ 用户帐户类型 ”。

登录后，可以从语言下拉框中选择自己的 UI 语言。请参阅 **“修改语言包”**。

启用 HTTPS 后， NMC 将生成自己的证书。该证书将与您的浏览器协商加密方法。有关更多详细信息，请参阅 **APC 网站**上的 《安全指南》。

URL 地址格式

在 Web 浏览器的 URL 地址字段键入 NMC 的 DNS 名称或者 IP 地址，并按下 ENTER。在 Internet Explorer 中指定非默认的 Web 服务器端口时， URL 必须包含 `http://` 或 `https://`。

注意：默认情况下， HTTP 为禁用状态， HTTPS 为启用状态。

登录时常见的浏览器错误消息。

错误消息	浏览器	错误原因
“ 该页面无法显示。 ”	Internet Explorer	Web 访问被禁用，或 URL 不正确。
“ 无法连接。 ”	Firefox、 Chrome	

URL 格式示例。另请参阅 “IPv6 屏幕的 TCP/IP 设置 ”。

示例和访问模式	URL 模式
`Web1` 的 DNS 名称	
HTTP	`http://Web1`
HTTPS	`https://Web1`
系统 IP 地址 `139.225.6.133` 和默认的 Web 服务器端口 (80)	
HTTP	`http://139.225.6.133`
HTTPS	`https://139.225.6.133`
系统 IP 地址 `139.225.6.133` 和非默认的 Web 服务器端口 (5000)	
HTTP	`http://139.225.6.133:5000`
HTTPS	`http://139.225.6.133:5000`
系统 IPv6 地址 `2001:db8:1:2c0:b7ff:fe00:1100` 和非默认的 Web 服务器端口 (5000)	
HTTP	`http://[2001:db8:1:2c0:b7ff:fe00:1100]:5000`

首次登录

首次登录 NMC 时，系统将提示您更改默认的超级用户帐户密码 (apc)。登录后，您将进入“ 配置摘要概述 ” 屏幕。该屏幕概述了所有系统协议及其当前值 （例如启用 / 禁用）。您可以随后通过以下路径随时访问此屏幕：**配置 > 网络 > 摘要**。

主页屏幕

概述

路径：主页

在界面的主页屏幕上，您可以查看活动警报和事件日志中最近记录的事件。

一个或多个图标以及附带的文本表示 UPS 目前的运行状态：

符号	说明
	**无警报**：没有警报， UPS 和 NMC 运行正常。
	**警告**：需要注意的警报情况，如果任其发展可能危害数据或设备。
	**严重**：存在严重警报，需要立即采取措施。

在每个屏幕的右上角，将使用相同的图标报告 UPS 状态。如果存在任何**严重**或**警告**警报，还会显示活动警报的数量。

若要查看完整的事件日志，请单击**更多事件**。

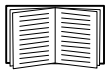
图标和链接

若要使任意屏幕成为“ 主页 ” 屏幕 （即您登录时显示的第一个屏幕），请转到该屏幕并单击右上角的  图标。

单击  返回以显示您登录时的“ 主页 ” 屏幕。

在界面每个屏幕的左下角，有三个连接至有用网站的可配置链接。默认情况下，通过该链接可以访问下列 Web 页面：

- 链接 1：www.apc.com 的 **Knowledge Base** （知识库）页面，包含有用的故障排除信息
- 链接 2：www.apc.com 的 **Product Information** （产品信息）页面，包含有关您的硬件的背景信息
- 链接 3：www.apc.com 的 **Downloads** （下载）页面，包含可用的固件和软件。

 若要重新配置这些链接，请参阅“ 配置链接屏幕 ”。

监控 UPS：状态菜单

“ 状态 ” 菜单选项可报告 UPS 和网络的当前状态。

您可以使用 “ 配置 ” 菜单选项配置 UPS 和网络，请参阅 “ 配置设置：1” 和 “ 配置设置：2”。

请参阅以下部分：

- “ 状态菜单上的 UPS”
- “ 状态菜单上的插座组 ”
- “ 状态菜单上的电池系统 ”
- “ 状态菜单上的通用 I/O”
- “ 状态菜单上的网络 ”

状态菜单上的 UPS

路径：状态 > UPS

此表显示了 UPS 负载、电池电量、电压和其他有用信息。

字段	说明
上次转电池模式原因	上一次转换为电池操作的原因。不包括自检。
内部温度	UPS 内部的温度。
剩余运行时间	UPS 可以使用电池电量支持其当前负载的时间长度。
UPS 输入	
输入电压	UPS 正在接收的交流电压 (VAC)。
旁路输入电压	UPS 处于旁路模式时使用的交流电压 (VAC)。 该选项并非适用于所有 UPS 设备。
UPS 输出	
输出电压	UPS 正在为其负载提供的交流电压 (VAC)。
负载电流	输入电压提供的电流，以安培为单位。
输出负载	连接的设备置于每相的负载，以 kVA 为单位。
输出负载百分比	连接的设备置于每相的负载，以没有冗余的可用 kVA 百分比的形式表示。
输出功率百分比	连接的设备置于每相的负载，以可用 kVA 百分比的形式表示。
输出功率 (W)	UPS 负载，以可用瓦特数百分比的形式表示。
输出功率 (VA)	UPS 负载，以可用 VA 百分比的形式表示。
输出效率	直接输出到负载的输入电源的百分比。 UPS 将消耗未输出到负载的输入电源。
输出能耗	负载使用的能量，从 UPS 上次重置为默认值时开始计算。

字段	说明
电池状态	
电池电量	可用于支持连接的设备的 UPS 电池电量的百分比。
电池电压	电池的直流电压。
外置式电池	连接至 UPS 的电池数量，不包括任何内置电池。

这些选项并非适用于所有 UPS 设备。

字段	说明
额定电池电压	UPS 电池电量额定电压； UPS 将其电池用作输出电源时电池提供的额定直流电压。
实际电池总线电压	可用的直流电源。
外置式电池柜额定值	外置式电池柜安培 - 小时额定值。
电池	UPS 所拥有的电池总数 （包括内置和外置）。
故障电池	“ 故障 ” 电池 （需要更换的电池）的数量。
电池电流	电池输出的电流。
下次电池更换日期	针对已安装 UPS 电池单元所建议的最早电池更换日期。
智能模块	有关智能模块的信息。当您向 APC 客户支持部门寻求帮助时，可能需要您提供此信息 （固件版本、生产日期、序列号和硬件版本）。
输入电压	UPS 正在接收的交流电压 (VAC)。
旁路输入电压	UPS 处于旁路模式时使用的交流电压 (VAC)。
输入频率	UPS 正在接收的电压的频率，以赫兹 (Hz) 为单位。
频率	输入电压和输出电压共享的频率，以赫兹 (Hz) 为单位。
旁路频率	当 UPS 处于旁路模式时使用的电压频率，以赫兹 (Hz) 为单位。
输出电流	向负载提供的电流，以安培为单位。
输出频率	输出电压的频率，以赫兹 (Hz) 为单位。
负载功率	UPS 负载，以可用瓦特数百分比的形式表示。
负载视在功率	UPS 负载，以可用 VA 百分比的形式表示。
模块	有关 UPS 中安装的模块的信息。当您向 APC 客户支持部门寻求帮助时，可能需要您提供此信息 （固件版本、生产日期、序列号和硬件版本）。
电源模块	有关 UPS 中安装的电源模块的信息。当您向 APC 客户支持部门寻求帮助时，可能需要您提供此信息。

路径：状态 > UPS > 测量值

以下选项仅适用于带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备。

此表显示了 UPS 剩余运行时间、电池电量、电压和其他有用信息。

字段	说明
上次转电池模式原因	上一次转换为电池操作的原因。不包括自检。
剩余运行时间	UPS 可以使用电池电量支持其当前负载的时长。
UPS 输入	
输入电压	UPS 正在接收的交流电压 (VAC)。
频率	UPS 正在接收的频率，以赫兹 (Hz) 为单位。
UPS 输出	
输出电压	UPS 正在为其负载提供的交流电压 (VAC)。
频率	UPS 正在发送的频率，以赫兹 (Hz) 为单位。
负载电流	输入电压提供的电流，以安培为单位。
输出功率 (VA)	UPS 负载，以可用 VA 百分比的形式表示。
输出功率 (W)	UPS 负载，以可用瓦特数百分比的形式表示。
输出能耗	负载使用的能量，从 UPS 上次重置为默认值时开始计算。
功率因数	该值表示所用电力的效率。理想值为 1，小于 1 表示电气系统存在损耗。
输出效率	直接输出到负载的输入电源的百分比。UPS 将消耗未输出到负载的输入电源。
电池状态	
充电状态	可用于支持所连接设备的 UPS 电池电量的百分比。
电池电压	电池的直流电压。
运行状况	此字段包括任何电池系统错误，含单个电池架的错误。错误记录为事件。
下次电池更换日期	针对已安装 UPS 电池架所建议的最早电池更换日期。

路径：状态 > UPS > 概述

以下选项仅适用于前缀为 SRTL/SRYLF 并配有嵌入式 NMC 的 UPS 设备。

本页显示 UPS 主机架中不同位置的组件。例如：功率模块、电池模块、智能模块、外部电池框架。

路径：状态 > UPS > 功率

以下选项仅适用于前缀为 SRTL/SRYLF 并配有嵌入式 NMC 的 UPS 设备。

本页显示现有功率模块、模块位置以及每个模块的状态。

路径：状态 > UPS > 电池

以下选项仅适用于带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备。

电池系统状态和电池架状态概述如下。

字段	说明
电池系统状态	
电池电量	可用于支持所连接设备的 UPS 电池电量的百分比。
剩余运行时间	UPS 可以使用电池电量支持其当前负载的时长。
额定电池电压	UPS 电池的额定电压容量；UPS 将其电池用作输出电源时电池提供的额定直流电压。
实际电池总线电压	可用的直流电源。
所有模块的最高电池温度	所有已安装模块的最高温度。
所有模块的最低电池温度	所有已安装模块的最低温度。
最高电池电压	所有已安装模块中所有电池的最高电压。
最低电池电压	所有已安装模块中所有电池的最低电压。
电池架状态	
状态	电池架的状态，包括单个电池架的状态。除正常之外，此处的值可以表示电池组的电池寿命即将终止或已超出电池寿命。错误记录为事件。
严重	如果显示的值大于 0，表示存在应该立即解决的电池架问题。
警告	如果显示的值大于 0，表示存在可能需要解决的电池架问题。
良好	如果显示的值大于 0，表示一切正常。
空位	如果显示的值大于 0，表示槽位未安装电池模块。

单击“主电池架”或“XRn/电池架 n”进入 **进入电池状态：主电池架/电池状态：电池状态 n** 屏幕。

字段	说明
模块	电池模块及其在电池架内的位置。
状态	电池架的状态。除正常之外，此处的值可以表示电池寿命即将终止或已超出电池寿命。错误记录为事件。
运行状况	这包括任何电池系统错误。错误记录为事件。
上次电池更换时间	上次更换电池的日期。

路径：状态 > UPS > 智能模块

以下选项仅适用于前缀为 SRTL/SRYLF 并配有嵌入式 NMC 的 UPS 设备。

本页显示当前智能模块、模块位置以及每个模块的状态。

状态菜单上的插座组

路径：状态 > 插座组

该选项并非适用于所有 UPS 设备。它显示了 UPS 上所有插座组的状态详细信息。另请参阅 “ 控制菜单上的插座组 ” 和 “ 配置菜单上的插座组 ”。

状态菜单上的电池系统

路径：状态 > 电池系统

该选项并非适用于所有 UPS 设备。

字段	说明
电池系统状态	
充电状态	可用于支持连接的设备的 UPS 电池电量的百分比。
剩余运行时间	UPS 可以使用电池电量支持其当前负载的时间长度。
正极母线电压	UPS 设备支持正负两极的电池电压。
负极母线电压：	
更换电池单元 SKU	应该引用的更换电池单元部件号。
电池组状态	
电池组 1、 2...	从内部编号方法所衍生的电池组号。
序列号	电池组的序列号。
运行状况	此字段包括任何电池组电池系统错误，含各单元的错误。错误记录为事件。
状态	电池组的状态，包括各单元的状态。 除正常之外，此处的值可以表示电池组的电池寿命即将终止或电池寿命已超出。错误记录为事件。

单击 “ 电池组 1、 2...” 进入**电池组 n** 屏幕页面。

字段	说明
电池组 1、 2... **或** **内部电池组**	
序列号 **（如果存在）**	电池组序列号。
固件版本	电池组修订号。
温度	电池盒中的传感器报告的温度。

字段	说明
组状态	仅限电池组错误，不包括各单元的错误。错误记录为事件，可能是： • 温度超出范围 • 常规错误 • 通信错误 • 电池组框架已断开连接 • 固件与硬件不兼容
电池单元 1 和 （如果存在）电池单元 2	
运行状况	此字段可表示单元的运行状况正常、电池寿命即将终止、电池寿命已超出或测量到电池的寿命即将终止。 错误记录为事件。
安装日期	各单元的安装日期。用户可编辑此日期。
预计更换日期	UPS 计算应更换电池的时间。 上述运行状况字段根据此日期得出值。
状态	单元的具体值。请参阅上文 “ 组状态 ” 了解一般的电池组错误。错误记录为事件，可能是： • 单元已断开连接 • 单元需要更换 • 单元温度过高：严重 • 单元温度过高：警告。通常在上述 “ 严重 ” 错误之前显示，但也存在例外情况。

状态菜单上的通用 I/O

路径：状态 > 通用 I/O

该选项并非适用于所有 UPS 设备。

温度和湿度显示每个传感器的名称、警报状态、温度和湿度 （如支持）。单击传感器的名称可编辑其名称和位置，还可配置其阈值和滞后值。请参阅 “ 温度和湿度屏幕 ” 了解更多详细信息。

输入触点显示每个触点的名称、警报状态和状态 （已打开或已关闭）。当您安装环境附件时，会自动查找并在此处显示这些内容。单击输入触点的名称，了解详细状态或配置其值。如果配置了触点而又将其禁用，则不会在此处显示。请参阅 “ 输入触点屏幕 ” 了解更多详细信息。

输出继电器显示每个继电器的名称和状态 （已打开或已关闭）。当您安装环境附件时，会自动查找并在此处显示这些内容。单击输入触点的名称，了解详细状态或配置其值。请参阅 “ 输出继电器屏幕 ” 了解更多详细信息。

最近的环境事件显示与环境监测相关的事件，例如，超出温度阈值或关于环境监测器输入触点的警告消息。单击 “ 更多事件 ” 链接查看最近事件的完整列表。

状态菜单上的网络

路径：状态 > 网络

“ 网络 ” 屏幕显示您的 IP、域名和以太网端口设置。有关这些字段的背景详细信息，请参阅 “ 配置菜单上的网络 ”。

控制 UPS

通过“控制”菜单选项，您可以立即采取影响 UPS 和插座的措施。这些选项同时还具有一些安全和网络功能。

请参阅以下部分：

- “控制菜单上的 UPS”
- “控制菜单上的插座组”
- “控制菜单上的安全”
- “控制菜单上的网络”

控制菜单上的 UPS

路径：控制 > UPS

当您选择单选按钮选项并单击“下一个”时，另一个屏幕将概括要进行的操作，单击此处的“应用”可继续进行操作。

操作将根据您是否拥有带插座组的 UPS 设备而有所不同。下面的两张表格分别涵盖了这些操作。

- “UPS 屏幕上的操作 （针对带插座组的设备）”。
- “UPS 屏幕上的操作 （针对不带插座组的设备）”。

正下方的这些屏幕复选框选项同时适用于两张表格。

复选框	说明
向 PowerChute Network Shutdown 客户端发信号	对于带插座组的 UPS，如果不存在 PowerChute 客户端，该选项将变为灰色 （请参阅“PowerChute Network Shutdown 客户端”）。 选择此选项可通知配置为与该 UPS 通信的 **PowerChute Network Shutdown 客户端**的所有服务器根据为 **PowerChute Network Shutdown 参数**配置的值关闭 （请参阅“配置菜单上的关闭”）。 但是，当执行任何旁路控制操作时，此选项将不会通知服务器。
跳过插座的关闭延迟时间	此选项仅适用于带插座组的 UPS。立即关闭插座，跳过配置的插座组延迟。 您可能需要在紧急情况下执行此操作或执行此操作以保留运行时间。或在负载设备的可能已被手动关闭的情况下执行此操作。

有关延迟和设置的更多信息，请参阅“**配置菜单上的关闭**”、“**UPS 通用屏幕**”和“**控制菜单上的插座组**”。

UPS 屏幕上的操作 （针对带插座组的设备）

操作	说明
重新启动 UPS 插座组	将“立即关闭，交流供电恢复时重新启动”命令应用于所有插座组 （请参阅“控制菜单上的插座组”）。单击“下一个”可查看关于计时和延迟的特定详细信息。 关闭开关插座组的输出电源，然后关闭主插座组 （如存在）。应用了操作的任何插座组将等待为其“重新启动持续时间”和“供电延迟”配置的秒数。（然后，如果交流市电电源可用，插座组将开启，或等到交流市电电源可用时再开启。请参阅“什么是插座组？ ”）。 如果交流市电电源可用， UPS 将开启，或等到交流市电电源可用时再开启。
启动 UPS 插座组	开启主插座组 （如存在），然后开启所有开关插座组。此选项仅在 UPS 当前关闭时显示。单击“下一个”可查看关于计时和延迟的特定详细信息。 然后， UPS 和插座组开启。
关闭 UPS 插座组	关闭开关插座组的输出电源，然后关闭主插座组 （如存在）。应用了操作的任何插座组将保持关闭状态，直到您再次开启其电源。单击“下一个”可查看关于计时和延迟的特定详细信息
将 UPS 插座组置于休眠模式	通过将 UPS 的输出电源关闭一段时间 （由以下参数定义），使 UPS 插座组进入休眠模式。单击“下一个”可查看关于计时和延迟的特定详细信息 • 关闭插座组的电源之前，插组将等待在其“关机延迟”中配置的时间。 • 输入电源恢复时， UPS 在配置的两个时间段过后将开启输出电源：“休眠时间”和“供电延迟”。 然后 UPS 关闭。经过配置为“休眠时间”的小时后，如果交流市电电源可用， UPS 将开启，或等到交流市电电源可用时再开启。
将 UPS 置于旁路模式 **将 UPS 从旁路转回**	这些选项用于控制旁路模式的使用。使用旁路模式可对 UPS 执行维护，而不必关闭 UPS 电源。 这些选项仅适用于 Symmetra UPS 和某些 Smart-UPS 设备。

有关延迟和设置的更多信息，请参阅“配置菜单上的关闭”、“第三方支持屏幕”和“控制菜单上的插座组”。

UPS 屏幕上的操作 （针对不带插座组的设备）

操作	说明
重新启动 UPS	通过下列方式，重新启动连接的装置：（单击 “ 下一个 ” 可查看关于计时和延迟的特定详细信息）。 • 关闭 UPS 电源。 • UPS 电池电量至少恢复为 “ 最低电池电量 ” （“ 配置 ” – “ 关闭 ” - “ 关闭结束时间 ”，请参阅阅 “ 受控的过早关闭和关闭结束时间 ”）中配置的百分比后，打开 UPS 的电源。
打开 UPS	打开 UPS 的电源。此选项仅在 UPS 关闭时显示。 单击 “ 下一个 ” 可查看关于计时和延迟的特定详细信息。
关闭 UPS	立即关闭 UPS 的输出电源，没有关机延迟。 UPS 将保持关闭状态，直到您再次将其打开。
将 UPS 置于休眠模式	通过在定义的时间内关闭输出电源，使 UPS 进入休眠模式。单击 “ 下一个 ” 可查看关于计时和延迟的特定详细信息。 • UPS 在等待 “ 关闭延迟 ” 中配置的时间过后，将关闭输出电源。 • 输入电源恢复时， UPS 在配置的 “ 休眠时间 ” 过后将打开输出电源。
将 UPS 置于旁路模式和使 UPS 退出旁路模式	这些选项用于控制旁路模式的使用。使用旁路模式可对某些 Smart-UPS 设备执行维护，而无需关闭 UPS 电源。 单击 “ 下一个 ” 可查看关于计时和延迟的特定详细信息。 这些选项仅适用于 Symmetra UPS 和某些 Smart-UPS 设备。

控制菜单上的插座组

路径：控制 > 插座组

该选项并非适用于所有 UPS 设备。

与 UPS 设备不同，使用此选项可开启、关闭或重新启动单个插座组。该选项可适用于单个 UPS 设备和同步控制组 （如启用，请参阅 “ 配置菜单上的插座组 ”）。

（此屏幕按名称和状态列出每个通过配置 — 插座组选项配置的 UPS 插座组，请参阅 “ 配置菜单上的插座组 ”）。

您可以为每个插座组选择下列任何操作 （或者无操作）。这些操作为一次性操作。

- 插座组的状态为关闭时：
  - 立即启动
  - 延迟启动：在供电延迟配置的秒数过后，开启插座组。（请参阅 “ 配置菜单上的关闭 ”）。

- 插座组的状态为开启时：
  - 立即关闭
  - 延迟关闭：在关机延迟配置的秒数过后，关闭插座组 （请参阅 “ 配置菜单上的关闭 ”）。
  - 立即重新启动：立即关闭插座组，然后在重新启动持续时间 （请参阅 “ 配置菜单上的关闭 ”）和供电延迟配置的秒数过后重新将其开启。
  - 延迟重新启动：在关机延迟配置的秒数过后关闭插座组，然后在重新启动持续时间和供电延迟配置的秒数过后重新将其开启。
  - 立即关闭，交流供电恢复时重新启动：立即关闭插座组。在重新启动持续时间和供电延迟配置的秒数过后，检查确定交流市电电源已恢复，且 UPS 能够支持最低恢复运行时间需求，然后再开启插座组。
  - 延迟关闭，交流供电恢复时重新启动：在关机延迟配置的秒数过后，关闭插座组。在重新启动持续时间和供电延迟配置的秒数过后，检查确定交流市电电源已恢复，且 UPS 能够支持最低恢复运行时间需求，然后再开启插座组。

选择一个操作后，单击 “ 下一个 ” 可查看该操作的详细说明，包括任何延迟的持续时间。单击 “ 应用 ” 可确认操作。

控制菜单上的安全

路径：控制 > 安全 > 会话管理

此屏幕提供关于登录用户、他们正在使用的界面 （例如 Web 用户界面、 CLI）、他们的 IP 地址和他们已登录时长的详细信息。

如果您有足够的权限，单击名称可查看使用了哪种身份验证方法来验证该用户。之后，您还可以使用终止会话按钮来注销用户。

控制菜单上的网络

路径：控制 > 网络 > 重置 / 重新启动

使用这些选项可重置不同的网络管理卡选项和 UI。

操作	说明
重新启动网卡界面	通过注销来重新启动网卡界面 （例如 Web 用户界面、 CLI）。 UPS 和 NMC 设备将不会重新启动。
全部重置 [1]	注意：这会将所有可配置值重置为其默认值。 • 如果没有选择**不包括 TCP/IP**，所有配置的值和设置会重置为其默认值，其中包括决定此设备须如何获得其 TCP/IP 配置值和 EAPoL 配置的设置。TCP/IP 配置设置的默认值为 DHCP，而 EAPoL 的访问权限默认为禁用。 • 如果选择了**不包括 TCP/IP**，除了决定此设备须如何获得其 TCP/IP 和 EAPoL 配置值的设置外，所有配置值和设置会重置为其默认值。
仅重置 [1]	**TCP/IP**：仅重置决定此设备须如何获得其 TCP/IP 配置值的设置，包括重置为禁用的 EAPoL 配置。TCP/IP 配置设置的默认值为 DHCP，而 EAPoL 的访问权限默认为禁用。
	事件配置：将事件重置为默认配置。任何专门配置的事件或组也将恢复为默认值。请参阅 “ 通知菜单 ” 了解详情
	将 UPS 设置为默认值：仅将 UPS 设置重置为其默认值，而不重置网络设置。
	环境监测通信中断警报：重置通用 I/O 端口设备拔出时触发的环境监测通信中断警报。
	控制策略：重置定义 NMC 如何对干触点 I/O 附件检测到的警报做出响应的设置。
[1] 重置最多可能需要一分钟的时间。将不会重置您配置的 UPS 名称 （请参阅 “UPS 通用屏幕 ”）。	

配置设置：1

通过“配置”菜单选项，您可以为 UPS 和 NMC 设置基本的操作值。

请参阅以下部分和配置设置：2。

- 配置菜单上的插座组
- 配置菜单上的电源设置
- 配置菜单上的关闭
- UPS 通用屏幕
- 自检计划屏幕
- 关机计划安排
- 固件更新屏幕
- PowerChute Network Shutdown 客户端
- 通用 I/O 屏幕
- 安全菜单

注意：您可以通过“配置摘要”屏幕查看某些配置设置 （**配置 > 网络 > 摘要**）。

配置菜单上的插座组

路径：配置 > 插座组

该选项并非适用于所有 UPS 设备。通过此选项，您可以显示和配置插座和顺序延迟。

另请参阅状态菜单上的插座组、控制菜单上的插座组和配置菜单上的关闭。

什么是插座组？

插座组仅在某些 UPS 设备上可用。若要确定您的 UPS 设备是否支持插座组，请参阅 UPS 文档。

可用的设置取决于不同的 UPS 设备。

主插座组。某些 UPS 设备向一个主插座组提供交流市电电源。主插座组控制 UPS 的所有开关插座组（如存在）的电源分配。

- 如果主插座组关闭，开关插座组将无法开启。
- 如果您关闭了主插座组， UPS 将先关闭开关插座组，之后再关闭主插座组。
- 若要打开开关插座组， UPS 必须先打开主插座组。

开关插座组。

- 每个开关插座都能独立地执行操作。您可以依次启动或停止这些插座，也可以重新启动插入这些插座的设备。

配置插座组

插座组名称和类型。在配置 - 插座组屏幕查看 UPS 插座的名称、类型和延迟。单击组下的插座组名称可更改其设置，包括顺序延迟和切断负载选项。

时间顺序设置。设置视不同的 UPS 设备而异。使用时间顺序选项定义 UPS 如何对用户签发的命令做出响应。

字段	说明
关机延迟	当插座组开启时，它会在关闭前等待此延迟时间 （以秒计）。通过在此处为插座设置不同的时间，您可以对其关闭时间进行排序，即您可以指定它们关闭的顺序。
重新启动持续时间	插座重新启动前将等待此时间。
供电延迟	当插座组关闭并接收到开启的信号时，它将在开启前等待此延迟时间 （以秒计）。通过在此处为插座设置不同的时间，您可以对其开启时间进行排序。
最短恢复运行时间	UPS 在能够再次开启前，必须支持其负载的最短时间长度。

切断负载选项。通过切断负载，您可以指定导致单个开关插座组丧失电源的情况。

注：如果通过 PowerChute Network Shutdown 管理 UPS，不建议使用 NMC 减载选项，否则将可能与 PowerChute 所指定的插座组设置冲突。

使用切断负载的一种情况是，当 UPS 在电池模式下运行或过载时关闭了非关键负载 （如监视器）。这样做可维持电池电量和关键负载的运行时间。另一种情况是在过载时禁用自动重新启动，以便在重新开启插座组前调查过载的原因。

使用这些选项，您可以在符合以下任意指定条件时关闭插座组：

- 使用电池的时间超出设置的分钟数时。
- UPS 的剩余运行时间小于设置的分钟数时。（运行时间是 UPS 可以使用电池电量支持其当前负载的时间长度）。
- UPS 过载 （与 UPS 相连的设备的所需电量超过 UPS 可以提供的电量）。

您也可以启用以下操作：

- 跳过插座的关闭延迟时间。（立即关闭插座组，而不等待关机延迟配置的秒数）。该选项默认为禁用。）
- 恢复供电后依然保持关闭。（交流市电电源恢复时，保持关闭。该选项默认为禁用，并且 UPS 将等待供电延迟配置的秒数，之后再开启插座组。）

插座组事件和陷阱。插座组状态的变化会生成事件 **UPS：插座组已开启**，或者 **UPS：插座组已关闭**（严重程度为 “ 警告 ”）。事件消息的格式为 “UPS：插座组*组号码，组名称，操作及原因*。例如：

```
UPS：插座组 1， Web 服务器，开启。

UPS：插座组 3，打印机，关闭。
```

默认情况下，事件将生成一个事件日志条目、一封电子邮件和一条系统日志消息。

如果您为事件配置了陷阱接收器，在插座组开启时，将生成陷阱 298 ；在插座组关闭时，将生成陷阱 299。事件消息为陷阱变量。默认的严重程度级别与事件相同。

配置菜单上的电源设置

路径：配置 > 电源设置

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备的路径为**配置 > UPS > 电源设置**。

可用的设置取决于不同的 UPS 设备。

当 UPS 使用电池模式时，额定输出电压是 UPS 为负载提供的交流电压。您可以配置下列设备特定的项目：

- 电压的上限和下限设置用于确定 UPS 自动调节对负载的电池输出的范围。这样可保护负载。

  当突破电压上限时， UPS 将使用其 AVR Trim 功能；当突破电压下限时， UPS 将使用其 AVR Boost 功能 （或如果 UPS 没有 AVR Boost 功能，将切换到电池模式）。
- 启用绿色模式将使 UPS 在旁路模式下运行，这样能更有效地使用能量。但是，在绿色模式下，必要时切换到 UPS 电池供电的速度较慢。如果您所在环境需要快速切换，则可以禁用绿色模式。
- UPS 通过使用电池模式对输入电源线噪声作出反应。灵敏度设置可更改 UPS 对线路噪声作出反应的时间。使用降低和低选项，以允许 UPS 在较长时间内接受有噪电源输入，之后再使用电池模式。如果已知输入电源在电话线上发出大量噪声 （例如，发电机提供的输入电源），则使用低。
- 输出瓦特功率：符合负载设备要求的最大额定功率。
- 旁路设置定义了 UPS 可以切换到旁路模式的条件。
- 警报阈值取决于可用的运行时间和冗余电源以及 UPS 负载。
- 输出频率范围：UPS 在不切换到电池状态下继续在线运行的范围。
- 输出频率转换速率：UPS 与输入源进行锁相时，输出频率在给定时间内的最大变化量。单位以赫兹/秒 (Hz/s) 表示。

配置菜单上的关闭

路径：配置 > 关闭

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备路径为**配置 > UPS > 关闭**。

使用此屏幕可配置 UPS 关闭的参数。请参阅下表和 “ 受控的过早关闭 ” 和 “ 关闭结束时间 ”。

关闭开始时间

定义在需要关闭 UPS 时应考虑的延迟和持续时间。

字段	说明
低电持续时间	对于在电池模式下运行的 UPS，此选项定义了剩余运行时间阈值，低于该阈值时，将在 UPS 上触发低电条件。例如，如果将 “ 低电持续时间 ” 设置为十分钟，且 UPS 预计剩余运行时间达到十分钟或更少时间，则将触发低电条件。如果 UPS 中的输入电源未恢复，它将在电池电量耗尽时关闭。 低电条件将在所有与 NMC 关联的 PowerChute Network Shutdown 客户端上触发关闭。
所需的最大延迟	计算当 UPS 或 PowerChute 客户端触发安全关闭时，确保每个 PowerChute 客户端有充足时间安全关闭所需的延迟。 • 这是列为 PowerChute Network Shutdown 客户端的任何服务器所需的最长关闭延迟。 • 每当开启或重置 UPS 的管理界面时，或选中 *强制协商* 选项并单击 “ 应用 ” 时，就会进行计算。 请参阅关闭延时和 PowerChute Network Shutdown。

简单信号关闭。

简单信号是 UPS 与服务器、工作站或第三方系统之间进行通信的一种简单方法。接口扩展器 2 (AP9624) 是一种可以为您的 UPS 提供简单信号的智能插槽附件。 UPS 简单信号可以提供通知和安全系统关闭，但不提供高级或智能信号提供的连续高级监控功能。

注：如果您正在使用 PowerChute Network Shutdown，则不建议使用 “ 简单信号关闭 ”。对于某些 UPS 型号，“ 简单关机延迟 ” 等选项可能会影响 UPS 关闭，并取代 PowerChute 用来计算所需总关闭时间的 “ 低电持续时间 ”。

字段	说明
简单信号关闭	如果您已经使用简单信号缆线将服务器、工作站或第三方系统连接到 UPS，请启用 “ 简单信号关闭 ”。如果您的 UPS 不支持高级信号或配置为用简单信号通信，请启用此选项。
简单信号低电持续时间	对于在电池模式下运行的 UPS，此选项定义了剩余运行时间阈值，低于该阈值时，将在 UPS 上触发低电条件。然后， UPS 将： • 在 UPS 显示上提供低电通知。 • 通过简单信号缆线将低电通知从 UPS 发送到所连接的设备。 如果 UPS 中的输入电源未恢复，它将在电池电量耗尽时关闭。此持续时间仅适用于 SMT、 SMX、 SRC、 SURTD 和 SRT Smart-UPS 型号。
简单关机延迟	定义 UPS 在收到简单关机通知后，关闭前等待的特定持续时间。此持续时间过后，UPS 将关闭，而不管剩余多少电池运行时间。 此延迟仅适用于某些 SMT、 SMX、 SRC、 SURTD 和 SRT Smart-UPS 型号。

关闭持续时间

指定 UPS 关机的时间长度。

字段	说明
休眠时间	定义在您发出 UPS/ 插座组休眠命令时， UPS 输出电源保持关闭状态的时间。当 UPS/ 插座组关闭时，它将在此处定义的 “ 休眠时间 ” 加上插座组的 “ 恢复时间 ” 或 “ 供电延迟 ” 后重新打开。如果市电电源在此时还未恢复， UPS 将等到其恢复后再重新打开。请参阅第 27 页上的 “ 配置菜单上的插座组 ”。 可以通过 UPS 显示 （即控制菜单上的 UPS）、 SNMP 命令或 PowerChute Business Edition 发出休眠命令。

PowerChute 关闭参数

指定 PowerChute Network Shutdown 使用的关闭参数。

字段	说明
所需的最大延迟 - 强制协商	启用*强制协商*可重置 “ 所需的最大延迟 ” 值，以使其与 “ 低电持续时间 ” 相匹配。更新后的状态数据包将由 NMC 发送给注册的所有 PowerChute 代理。然后， PowerChute 会将该数据包中发送的 “ 低电持续时间 ” 与它所需的总关闭时间进行比较，并相应地增加 “ 所需的最大延迟 ” 或其注册到的插座组的 “ 关机延迟 ”。 PowerChute 每 30 分钟执行一次剩余运行时间验证检查，以将所需的 PowerChute 总关闭时间与 NMC“ 低电持续时间 ” 进行比较。 选择 “ 强制协商 ” 会将所有插座组的 “ 关机延迟 ” 重置为与 “ 低电持续时间 ” 相同的值。 “ 强制协商 ” 最多可能需要十分钟来计算 NMC 上注册的所有 PowerChute 客户端所需的值。有关详细信息，请参阅第 33 页上的 “ 关闭延时和 PowerChute Network Shutdown”。
电池供电模式关闭行为	定义 UPS 关闭后的行为： • 电源恢复后重新启动 - 市电电源恢复后，重新启动 UPS。 • 关闭并保持关闭 - 市电电源恢复后， UPS 依然保持关闭。 • 忽略 PCNS 关闭命令 - UPS 将关闭并忽略已配置的 PowerChute 关闭命令。
用户名	输入配置于 PowerChute 的用户名。
身份验证短语	此短语用于在 PowerChute 和 NMC 之间进行身份验证。默认情况下，此短语为空，必须设置后才能启用 PowerChute。
PCNS 通信协议	选择通信协议用于和 PowerChute 通信：HTTPS 或 HTTP。

“ 受控的过早关闭 ” 和 “ 关闭结束时间 ”

这些选项并非适用于所有 UPS 设备。这些选项不适用于 SMT、 SMX、 SRC、 SURTD 或 SRT Smart-UPS 型号。若要针对这些型号控制插座组的过早关闭，请参阅第 28 页上的 “ 切断负载选项 ”。

通过 “ 受控的过早关闭 ” 选项，您可以在符合任何以下指定的条件时关闭使用电池供电的 UPS 设备：

- 使用电池的时间超出设置的分钟数时。
- UPS 的剩余运行时间小于设置的分钟数时。（运行时间是 UPS 可以使用电池电量支持其当前负载的时间长度）。
- 电池电量低于设置的总电量的百分比时。
- UPS 输出上的负载小于设置的百分比时。

通过**恢复供电后依然保持关闭**，您还可以决定在市电电源恢复后， UPS 是否恢复开启。

通过**关闭结束时间**选项，您可以设置市电电源恢复后 UPS 可恢复开启的条件和延迟时间。根据 UPS 型号，您可以指定 UPS 恢复开启前的**最低电池电量**或**最短恢复运行时间**。

关闭延时和 PowerChute Network Shutdown。

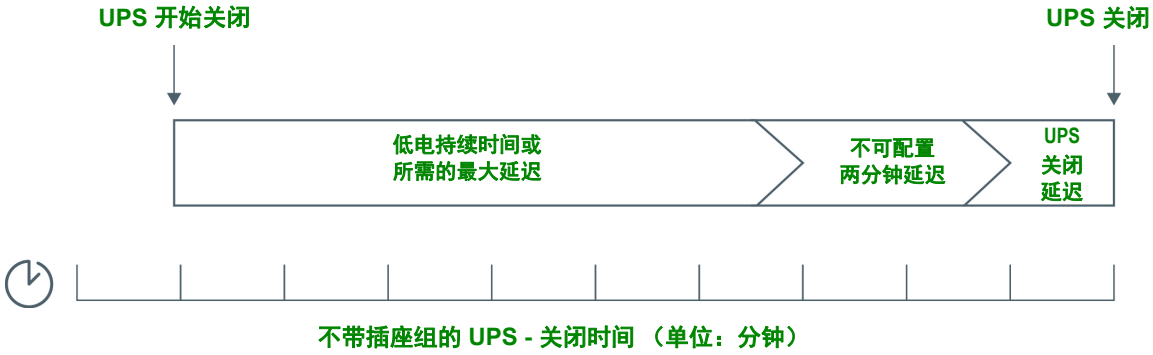
以下部分介绍了“低电持续时间”、“所需的最大延迟”和插座组的“关机延迟”如何影响 PowerChute 关闭序列。

有关 PowerChute 关闭序列的详细信息，请参阅 APC 网站上的《用户指南》。

对于带和不带插座组的这两种 UPS，关闭时间都通过 NMC 与 PowerChute Network Shutdown 进行互相作用来协商，如下所示：

不带插座组的 UPS

对于不带插座组的 UPS， UPS 关闭时间是 NMC 关闭屏幕上的所需的最大延迟值或低电持续时间值的较大者加上不可配置的 2 分钟延迟，再加上 UPS 的关闭延时。



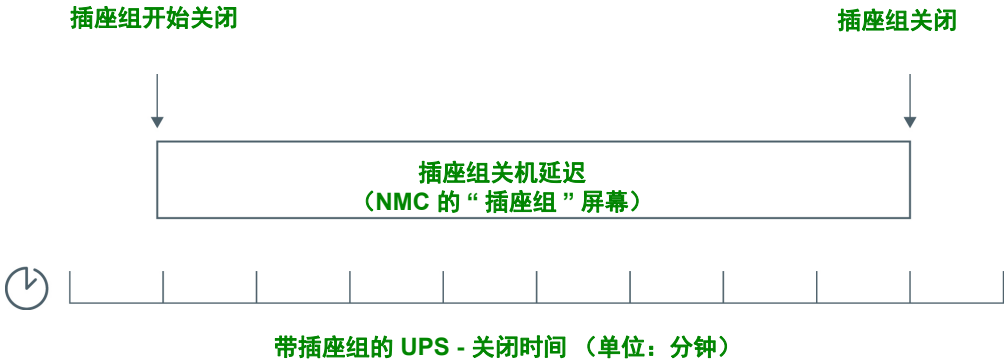
不带插座组的 UPS - 关闭时间 （单位：分钟）

注：

- 如果关闭已由低电条件触发，“低电持续时间”值将优先于“所需的最大延迟”值。
- 例外情况是，带插座组且前缀为 SUM 的 UPS 型号使用“不带插座组的 UPS”方法来计算 UPS 关闭时间。

带插座组的 UPS

对于带插座组的 UPS，关闭时间是 NMC 插座组屏幕上的关机延迟值，请参阅配置菜单上的插座组。（并非适用于所有 UPS 设备）。



带插座组的 UPS - 关闭时间 （单位：分钟）

注：

有关 PowerChute 关闭序列的详细信息，请参阅 APC 网站上 《PowerChute Network Shutdown 用户指南》中的 “ *关闭方案示例* ”。

在对 PowerChute 所需的关闭时间和 NMC“ 所需的最大延迟 ”/ 插座组的 “ 关机延迟 ” 进行比较的过程中，使用最大值。例如，如果 PowerChute 客户端命令行关闭持续时间设置为 8 分钟，但 UPS“ 低电持续时间 ” 为 10 分钟，NMC 将对 “ 所需的最大延迟 ” 使用较大值，即 10 分钟。

在 “ 强制协商 ” 中， NMC 会轮询 PowerChute 客户端以获取其所需的关闭时间。因此，更新 “ 所需的最大延迟 ”/ 插座组的 “ 关机延迟 ” 值最多可能需要十分钟。

PowerChute 决不会更改 NMC 低电持续时间字段的值。

使用 PowerChute Network Shutdown v3.x 或更高版本时， NMC 决不会将所需的最大延迟值用于带插座组的 UPS。

UPS 通用屏幕

路径：配置 > UPS

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备路径为配置 > UPS > 通用。

该屏幕并非适用于所有 UPS 设备。

某些 UPS 设备可能不会显示下面说明的某些选项。

字段	说明
UPS 名称	识别 UPS 的名称。
UPS 位置	机架式或塔式 UPS 的物理方位。
声音警报	启用或禁用 UPS 的声音警报。对于某些 UPS 设备，还可定义导致发出声音警报的状况。
LCD 语言首选项	指定您要使用的 UPS 显示语言。
LCD 显示	禁用或启用对 UPS 显示界面的写入权限。 禁用时，用户仍然具有大多数屏幕的读取权限，但不包括 “ 控制 ” 和 “ 配置 ” 菜单的子屏幕。
电池健康状态警报预警时间	设置 UPS LCD 显示更换电池严重警报之前的天数。设置天数为 -1 时，不显示预警通知。
电池健康状态警报休眠时间	设置 UPS LCD 电池警报从最初应答至最终显示应休眠的天数。设置天数为 -1 时，警报在最初应答后不再显示。
上次电池更换时间	输入最近一次更换 UPS 电池的年份和月份。

字段	说明
电池数量 或 **外置式电池**	电池数量，不含 UPS 上的内置电池。某些电池数量超过 16 的设备必须添加以 16 为倍数的电池数量（例如 16、32 和 48 等），但添加后可以调整为正确的值。
外置式电池柜	外置式电池柜安培 - 小时额定值。
电池充电率	通过此字段，您可以更改 UPS 电池充电的速度，以百分比表示。在此，100% 表示制造商建议的充电率。例如，若要将充电率提高一倍，可将此值设置为 200%。 例如，将 “ 电池充电率 ” 设置为 100% 时： • 如果总电池电量增加， UPS 电池充电器提供的电池充电电流将自动增加，以满足 100% 充电率 - 您无需更改充电率。 • 如果总电池电量降低， UPS 电池充电器提供的电池充电电流将自动降低，以满足 100% 充电率 - 您无需更改充电率。 有关电池电量的详细信息，请参阅 UPS 《用户指南》。 注意：充电率过高会导致电解液沸腾和 / 或排出和 / 或高气压。请勿更改此设置，除非您对该领域有丰富的背景知识。
电池类型	表示电池类型，其中 **VRLA** 是指阀控式密封铅酸蓄电池，**排气式电池**是指一种湿电池 （如用于汽车的电池）。
总电池电量	使用此设置可为您的 UPS 电池指定 7 到 200 安培小时 (Ah) 的总电量。可使用它来估计运行时间并确定为电池充电所需的电流。如果您的 UPS 具有可用的 “ 总电池电量 ” 选项，请在 UPS 中添加电池或移除电池时更新 “ 总电池电量 ” 的值。有关电池电量的详细信息，请参阅 UPS 《用户指南》。

自检计划屏幕

路径：UPS > 配置 > 自检计划

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备路径为**配置 > UPS > 自检计划**。

使用此选项可定义 UPS 进行自检的时间。

关机计划安排

路径：配置 > 计划安排

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备路径为**配置 > UPS > 计划安排**。

该选项并非适用于所有 UPS 设备。所有 UPS 设备的自检计划选项并非都相同。

注：请勿设置重合的关机计划时间。关机计划时间重合的一种情况是，设置每周关闭时间为 8pm 到 9pm，同时设置单次关闭时间为 8.10pm 至 8.30pm。关机计划时间重合将导致未知与未检的行为。

对于 UPS 和插座组选项

您可以为 **UPS** 下的 UPS 设备或**插座组**下的单个开关插座组 （如适用）计划安排关闭操作。

选择 **UPS** 或**插座组**时，任何已配置的关机计划安排及相关详细信息都将显示在屏幕顶部，包括其当前处于启用还是禁用状态。

编辑、启用、禁用或者删除计划关闭。单击 **UPS** 或**插座组**屏幕顶部的计划安排表中的计划名称，将显示完整的详细信息，您可以编辑其中的参数，包括取消勾选**启用**复选框来暂时将其禁用，或将其永久删除。

创建 UPS 或开关插座组关闭计划。

1. 在**计划安排**下，选择 **UPS** 或**插座组**。
2. 使用单选按钮选择要计划的关闭类型：**单次关闭**、**每日关闭**或**每周关闭**，然后单击**下一个**按钮。
3. 若要临时禁用计划，请清除**启用**复选框。
4. 指定名称、计划日期和时间。
   对于每周关闭，使用下拉框指定频率。
5. 指定关闭设备或插座组后是否要重新打开：

   重新打开：指定是否要在特定日期和时间开启 UPS，**从不** （UPS 必须手动开启），或**立即**（UPS 将在等待 6 分钟后开启）。

选择相应的按钮指定要关闭的插座组 （仅适用于插座组）。

向 PowerChute Network Shutdown 客户端发信号：指定是否通知 PowerChute 客户端，请参阅 PowerChute Network Shutdown 客户端。

利用该选项，您可以使用 PowerChute Network Shutdown 实用程序最多关闭使用该实用程序客户端版本的 50 台服务器。

固件更新屏幕

路径：UPS > 配置 > 固件更新

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备路径为**配置 > 固件更新 > 上传**。

该选项并非适用于所有 UPS 设备。

此处的更新请参考 *UPS 上的固件*。请勿将此项与 NMC 固件升级混淆 （请参阅文件传输）。

按照**固件更新**屏幕中的说明来确定是否需要在更新固件之前关闭 UPS 的输出。以上所述适用于特定的 UPS 型号。

注：若要通过 Internet Explorer® 查看**固件更新**屏幕，请使用已打开兼容性视图的版本 10 或更高版本。“ 固件更新 ” 屏幕不与 Edge® 浏览器兼容。

按照以下步骤更新固件。（另请参阅 “ 使用 FTP 更新 UPS 固件 ” 了解其他方法）。

1. 访问 APC 网站，阅读 ID 为 FA164737 和 FA170679 的知识库文章，了解有关获取固件更新文件和进一步说明的信息。
2. 选择**配置** - **固件更新**。
3. 单击该按钮，在计算机上找到已下载的更新文件。
4. 单击**更新 UPS** 按钮更新 UPS 固件。
5. 更新完成后，检查**上次更新结果**和**当前版 本**下或事件日志中的状 态。

通过 USB 驱动器更新 UPS 固件 （仅限 AP9641、 AP9643 和 SRTL/SRYLF 设备）

在更新 UPS 固件之前，请确保 USB 驱动器支持 USB v1.1，并且格式为 FAT、 FAT16 或 FAT32。

1. 将 USB 驱动器插入计算机上的 USB 端口。
2. 访问 APC 网站，阅读 ID 为 FA164737 和 FA170679 的知识库文章，下载正确的 UPS 固件更新文件，并将文件保存在 USB 驱动器的根目录或者 /upsfw/ 目录下。
3. 将包含固件文件的 USB 驱动器从计算机移除，并将其插入 NMC 的 USB 端口。
4. 打开 NMC 的 Web 界面，**进入配置 > 固件更新**。
5. 在“从 USB 驱动器更新”窗格的下拉列表中选择固件文件。
6. 单击“**更新 UPS**”按钮更新 UPS 固件。

   注意：固件更新可能需要几分钟时间。
   UPS 固件更新完成后，才可将 USB 驱动器从 NMC 中移除。如果在更新完成之前移除 USB 驱动器，固件更新将无法成功。
7. 更新完成后，检查“**上次更新结果**”下或“事件日志”中的状态。

通过 NMC 更新 UPS 固件

更新固件的步骤如下：

1. 有关如何获取固件更新文件和详细说明的信息，请参阅 **APC 网站**上的知识库文章 （ID **FA164737** 和 **FA170679**）。
2. 通过 SCP 或 FTP 将更新文件传输到管理卡的 root 目录。例如：`scp <firmware_file>.enc <nmc_username>@<nmc_ip_address>:<firmware_file>.enc`
3. 打开 NMC 网站界面，进入**配置 > 固件更新**。
4. 通过**从 NMC 更新**窗格下的下拉列表选中固件文件。
5. 单击**更新 UPS** 按钮更新 UPS 固件。
6. 更新完成时检查**上次更新结果**或事件日志下的状态。

使用 FTP 更新 UPS 固件

如果要在多台 UPS 设备上更新，使用 FTP 可以加快速度。操作步骤如下所示。这是从固件更新屏幕进行更新的另一种方法。

注意：默认情况下，FTP 为禁用状态，必须启用后才能继续。请参阅“FTP 服务器屏幕”。

1. 访问 APC 网站，阅读 ID 为 FA164737 和 FA170679 的知识库文章，了解有关获取固件更新文件和进一步说明的信息。
2. 使用 FTP 将更新文件放入管理卡 **upsfw** 目录，启动固件更新进程。

   如果更新文件损坏或与 UPS 不兼容，则 FTP 固件传输可能中断。

   以下是使用 DOS FTP 命令加载更新文件的示例：

```
$ ftp < 此处输入 NMC 网络地址 >
Connected to <NMC 网络地址 >.
220 AP9641 Network Management Card AOS vX.Y.Z FTP server ready.
User (<NMC 网络地址 >:(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 "<UPS 固件文件的路径 >"
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. 更新完成后，在事件日志中或 web 界面固件更新页面上次更新结果中，检查更新状态。

固件升级设置确认屏幕

路径：配置 > 固件更新 > 设置

以下选项仅适用于带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备。

指定切换到新 UPS 固件的时间：下载后输出电源关闭时或手动。

PowerChute Network Shutdown 客户端

路径：UPS > 配置 > PowerChute

PowerChute Network Shutdown 可远程关闭 UPS 设备。

在网络上安装 PowerChute Network Shutdown 客户端后，它将被自动添加到列表中。卸载 PowerChute Network Shutdown 客户端后，它将被自动删除。

单击添加客户端，输入新 PowerChute Network Shutdown 客户端的 IP 地址。若要删除某个客户端，请在列表中单击该客户端的 IP 地址，然后单击删除客户端。列表最多可包含 50 个客户端的 IP 地址。

带插座组时，您还需要指定使用哪个插座组为 PowerChute 客户端供电。

注意：如果在 NMC 上禁用 HTTP，则 PowerChute 无法连接到 NMC。请参阅“Web 访问屏幕”以启用 HTTP 或 HTTPS。

通用 I/O 屏幕

如果您安装了温度和湿度传感器 (AP9335T/TH) 或干触点 I/O 附件 (AP9810)，通用 I/O 菜单将发挥重要作用。使用这些功能的操作通常被称为环境监测。

温度和湿度屏幕

路径：通用 I/O > 温度和湿度

此屏幕将显示每个传感器的名称、警报状态、温度和湿度 （如支持）。单击传感器的名称可编辑其名称和位置，还可配置其阈值和滞后值。

阈值。对于每个传感器，您都可以为传感器测得的温度和湿度 （如支持）设置阈值。当达到阈值时，警报会发出信号。

高和低为警告警报。最大值和最小值为严重警报，必须对其进行处理。

滞后。使用滞后可避免因同一个超出温度或湿度阈值的情况而重复发出警报。

当超出阈值的温度或湿度轻微地上下波动时，会重复触发警报。较大的滞后值可防止出现这一情况。

如果滞后值不够大，波动首先会导致超出阈值，而后再清除，这意味着警报会被多次触发。请参阅以下示例，注意以下几点。

- 对于超出阈值最大值和上限的情况，警报的清除点是阈值*减去*您输入的滞后值。
- 对于超出阈值最小值和下限的情况，清除点是阈值*加上*滞后值。

湿度上升但上下浮动的示例：假设湿度阈值的*最大值*为 65%，湿度滞后值为 10%。那么，湿度升至 65% 以上将触发警报。然后它忽而降至 60% 又而升至 70%，但由于有 10% 的滞后值，警报未被清除，因此不会出现新警报。要清除现有警报，湿度需要降至 55% 以下 （65% *减去* 10%）。

温度降低但上下浮动的示例：假设温度阈值的*最小值*为 12°C，温度滞后值为 2°C，那么当温度降至 12°C 以下时会触发警报。然后它忽而升至 13°C 又忽而升至 11°C，但由于有 2°C 的滞后值，警报未被清除，因此不会出现新警报。要清除现有警报，温度需要升至 14°C 以上 （12°C *加上* 2°C）。

输入触点屏幕

路径：通用 I/O > 输入触点

输入触点显示每个触点的名称、警报状态和状态 （已打开或已关闭）。当您安装环境附件时，会自动查找并在此处显示这些内容。

单击输入触点的名称，了解详细状态或配置其值。禁用后，即使该触点处于异常位置，也不会生成警报。其他字段的说明如下：

字段	说明
警报状态	如果该输入触点没有报告警报，则为正常；如果该输入触点报告了警报，则显示警报严重程度。如果未对触点启用，则显示已禁用。
状态	该输入触点的当前状态：已关闭或已打开。
正常状态	该输入触点的正常 （非警报）状态：已关闭或已打开。
严重程度	该输入触点处于异常状态时，将生成以下警报严重程度： 警告或严重。

输出继电器屏幕

路径：通用 I/O > 输出继电器

输出继电器显示每个继电器的名称和状态 （已打开或已关闭）。当您安装环境附件时，会自动查找并在此处显示这些内容。

单击输入触点的名称，了解详细状态或配置其值。各个字段的说明如下：

字段	说明
状态	此输出继电器的当前状态：已关闭或已打开。
正常状态	此输出继电器的正常 （非警报）状态：已关闭或已打开。
控制	若要更改该输出继电器的当前状态，请选择此复选框并单击 “ 应用 ”。
延迟	在激活输出继电器前，所选警报状态必须存在的秒数。使用该设置可避免因短时瞬变情况而激活警报。 在延迟开始后，如果发生了额外映射的警报，延迟并不会重新开始，而是继续倒数计时，直到输出继电器被激活。
保持	警报发生后，输出继电器保持激活状态的最少秒数。 即使更正了激活的警报情况，输出继电器仍将保持激活状态，直至该时间结束。

配置控制策略

路径：通用 I/O > 控制策略

在连接了干触点 I/O 附件 (AP9810) 的 AP9641 或 AP9643 NMC 上，您可以：

- 根据 UPS 事件和输入触点，将输出继电器配置为打开或关闭，请参阅配置输出以对事件做出响应
- 根据输入触点配置 UPS 以执行操作，请参阅配置 UPS 或输出以对输入警报做出响应

并不是所有 UPS 设备都能配置为对输入触点做出响应。

配置输出以对事件做出响应。

1. 从**配置**菜单选择**通用 I/O** 和**控制策略**。
2. 单击**添加策略**按钮。
3. 单击类别或子类别名称，查看相应的事件。
4. 若要进行配置，单击事件名称，选择此事件发生时将更改状态的输出继电器的复选框，然后单击**保存策略**。

配置 UPS 或输出以对输入警报做出响应。

1. 从**配置**菜单选择**通用 I/O** 和**控制策略**。
2. 单击**添加策略**按钮。
3. 单击 **I/O 触点**子类别
4. 选择与输入触点具有相同严重程度的事件。例如，如果输入触点的严重程度为严重，那么请选择严重事件。

   NMC 最多支持四个输入。您必须指定与该事件相关的输入。
5. 在**端口**下拉列表中，选择安装干触点 I/O 附件的通用传感器的**端口**号 （1 或 2）。
6. 在**区域**下拉列表中，选择要安装输入的触点的区域字母 （A 或 B）。
7. 定义当输入更改状态时 UPS 将执行的操作 （如有）。
8. 选择将打开或关闭的输出 （如有）。
9. 单击**保存策略**。

您配置的操作将发生一次。

如果您在清除警报状况前，将输出恢复为正常状态，则输出将不会再次打开或关闭，除非清除了警报条件，而后其再次发生。

安全菜单

会话管理屏幕

路径：配置 > 安全 > 会话管理

启用允许并发登录意味着两个或以上用户可同时登录。每个用户都具有相同的访问权限，且每个界面（HTTP、 FTP、 Telnet 控制台、串行控制台 [CLI] 等）都视为一个登录用户。允许并发登录允许八个用户、五个用户和一个用户分别同时登录到 Web 界面、 CLI 和串行控制台。

远程身份验证覆盖：NMC 支持在服务器上进行 Radius 密码存储。但是，如果您启用了此覆盖选项，NMC 将允许本地用户使用存储于本地 NMC 上的密码登录。另请参阅本地用户和远程用户身份验证。

Ping 响应

路径：配置 > 安全 > Ping 响应

启用 **IPv4 Ping** 响应复选框可允许网络管理卡 3 响应网络 ping 命令。这并不适用于 IPv6。

本地用户

使用这些菜单选项可查看 NMC 用户界面，并设置对它的访问和单个首选项 （如显示的日期格式）。这适用于由用户登录名称定义的用户。

路径：配置 > 安全 > 本地用户 > 管理

设置用户权限。通过此选项，管理员或超级用户可列出并配置允许访问 UI 的用户。单击名称链接可查看详细信息，还可编辑或删除用户。

单击添加用户可添加用户。在随后出现的用户配置屏幕上，您可以添加用户，并通过取消选择访问权限复选框来拒绝访问。名称和密码的最大长度均为 64 字节，对于多字节字符长度更短。您需要输入密码。

“ 名称 ” 和 “ 密码 ” 中超过 64 字节的值可能被截断！
创建密码时，使用大小写字符、数字和特殊字符的组合。密码最多包含 64 个 ASCII 字符。

使用会话超时可配置此 UI 注销该用户前等待的时间 （默认为三分钟）。如果您更改该值，必须注销才能使更改生效。

串行远程身份验证覆盖：选择此选项后，您可以使用串行控制台 (CLI) 连接来绕过 RADIUS。此屏幕会为所选用户启用此选项，但必须通过会话管理屏幕进行全局启用后才能生效。

另请参阅下文的配置 > 安全 > 本地用户 > 默认设置。有关帐户的背景信息，请参阅用户帐户类型。

用户首选项选择**事件日志颜色编码**复选框，启用事件日志中记录的警报文本的颜色编码。（系统事件条目和配置更改条目不会改变颜色。）

文本颜色	警报严重程度
红色	**严重**：存在严重警报，需要立即采取措施。
橙色	**警告**：需要注意的警报情况，如果任其发展可能危害数据或设备。
绿色	**警报已清除**：导致警报的状况已得到改善。
黑色	**正常**：不存在警报。网络管理卡和所有相连的设备均正常工作。
蓝色	**提示**：用于提供信息的警报。网络管理卡和所有相连的设备均正常工作。

导出日志格式：可使用 CSV （逗号分隔型取值）或制表符来规定导出的日志文件的格式。请参阅显示事件日志。

在此 UI 中为测量值选择温度单位。**美国惯用**对应华氏度，**公制**对应摄氏度。

您可以通过**语言**字段指定 UI 的默认语言。您也可以在登录时设置。

您还可以为电子邮件收件人和 SNMP 陷阱接收器指定不同的语言。请参阅电子邮件收件人和陷阱接收器。

路径：配置 > 安全 > 本地用户 > 默认设置

设置默认值可更快速地添加用户。使用此选项可为 “ 管理 ” 屏幕中的多个选项设置默认值，请参阅上文的配置 > 安全 > 本地用户 > 管理。

远程用户身份验证

路径：配置 > 安全 > 远程用户 > 身份验证

身份验证。指定登录时您想使用的用户身份验证方法。

有关本地身份验证的信息 （不使用 RADIUS 服务器的集中身份验证），请参阅 APC 网站上提供的 *《安全手册》*。

支持以下 RADIUS （远程用户拨入认证服务）的身份验证和授权功能。

- 当用户访问启用了 RADIUS 的 NMC 或其他启用网络的设备时，会将身份验证请求发送到 RADIUS 服务器，以确定用户的权限级别。
- 与 NMC 一起使用的 RADIUS 用户名限制为 32 个字符。

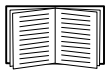
从下面选择一项：

- **仅本地身份验证**：RADIUS 已禁用。请参阅本地用户。
- **先 RADIUS 身份验证，后本地身份验证**：二者均已启用。首先从 RADIUS 服务器请求身份验证。如果 RADIUS 服务器没有响应，则使用本地身份验证。
- **仅限 RADIUS**：无本地身份验证。

如果选择了**仅限 RADIUS**，而 RADIUS 服务器不可用、识别不当，或者配置不当，则所有用户均无法使用远程访问。若要重新获得访问权限，您必须使用串行连接访问命令行界面，并将**访问权限**设置为**本地**或 **radiusLocal**。

例如，将访问权限设置更改为**本地**的命令为：

```
radius -a local
```



另请参阅下方的 RADIUS 屏幕和配置 RADIUS 服务器。

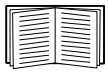
RADIUS 屏幕

路径：配置 > 安全 > 远程用户 > RADIUS

您可以使用 RADIUS 服务器对远程用户进行身份验证。使用此选项可执行以下操作：

- 列出 NMC 可用的 RADIUS 服务器 （最多两台）和每台服务器的超时时间。
- 单击 **Radius 服务器**链接可配置新的或现有 RADIUS 服务器的身份验证参数。

RADIUS 设置	说明
RADIUS 服务器	服务器名称或 IP 地址 （IPv4 或 IPv6）。 **注：**默认情况下， RADIUS 服务器使用端口 1812 对用户进行身份验证。若要使用不同的端口，在 RADIUS 服务器名称或 IP 地址末尾添加一个冒号再加上新的端口号。 NMC 支持端口 1812、 5000 - 32768。
保密	RADIUS 服务器与 NMC 之间的秘密共享。
回复超时	NMC 等待 RADIUS 服务器响应的时间 （以秒计）。
测试设置	输入管理员用户名和密码，以测试您配置的 RADIUS 服务器路径。
跳过测试并应用	不测试 RADIUS 服务器路径。

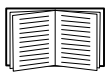


另请参阅上文的远程用户身份验证和下文的配置 RADIUS 服务器。

配置 RADIUS 服务器

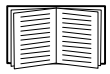
配置步骤摘要。

您必须配置 RADIUS 服务器，以与 NMC 一起工作，请参阅以下步骤。



有关具有供应商特定属性 (VSA) 的 RADIUS 用户文件示例和 RADIUS 服务器上字典文件中的条目示例，请参阅 **APC 网站**上提供的 *《安全手册》*。

1. 将 NMC 的 IP 地址添加到 RADIUS 服务器客户端列表 （文件）。
2. 除非定义了供应商特定属性 (VSA)，否则必须为用户配置 Service-Type 属性。如果没有配置 Service-Type 属性，用户将具有只读权限 （仅在 UI 上）。



请参阅 RADIUS 服务器文档，了解有关 RADIUS 用户文件的信息，并参阅 *《安全手册》* 了解相关示例。

3. 可以使用 VSA 代替 RADIUS 服务器提供的 Service-Type 属性。
   VSA 需要字典条目和 RADIUS 用户文件。在字典文件中，定义 ATTRIBUTE 和 VALUE 关键字的名称，但不定义数值。如果您更改了数值，RADIUS 身份验证和授权将会失败。VSA 优先于标准的 RADIUS 属性。

在 UNIX® 上配置 RADIUS 服务器使用隐蔽密码。

如果 UNIX 隐蔽密码文件 (/etc/passwd) 与 RADIUS 字典文件一起使用，则可以使用以下两种方法对用户进行身份验证：

- 如果所有的 UNIX 用户都具有管理权限，则将在 RADIUS “user” 文件中添加下列内容。若要只允许 “ 设备用户 ”，请将 APC-Service-Type 修改为 `Device`。

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

- 在 RADIUS “user” 文件中添加用户名和属性，并使用 /etc/passwd 验证密码。以用户 `bconners` 和 `thawk` 为例的说明如下：

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

支持的 RADIUS 服务器。

支持 FreeRADIUS v1.x 和 v2.x 以及 Microsoft Server 2008 和 2012 网络策略服务器 (NPS)。其他常用的 RADIUS 应用程序可能可以使用，但尚未经过全面测试。

防火墙界面

路径：配置 > 安全 > 防火墙 > 配置

启用或禁用防火墙功能。默认情况下，列出了配置的策略。选择启用复选框，启用防火墙。默认情况下，该复选框未予勾选。

- 单击应用，确认选择启用的防火墙策略。将打开防火墙确认页。
  - “ 确认 ” 页面包含关于在启用之前测试防火墙的建议。这不是强制性的。
  - 第一个超链接转到 “ 防火墙策略 ” 页。
  - 第二个超链接转到 “ 防火墙测试 ” 页。
  - 单击应用，启用防火墙并返回 “ 确认 ” 页。
  - 单击取消，返回 “ 配置 ” 页而不启用防火墙。
- 单击取消：不会启用新的选择项。停留在 “ 配置 ” 页。

路径：配置 > 安全 > 防火墙 > 活动策略

从 “ 可用策略 ” 下拉列表中选择一个活动策略，并查看该策略的有效性。默认情况下，显示当前的活动策略；您可以从列表中选择另一个。

- 单击**应用**，启用更改。如果选择并启用了不同的防火墙，则更改立即生效。如果选择了新配置的防火墙策略，则建议在启用前测试新防火墙。（请参阅上文的 “ 配置 ”。）
- 单击**取消**，恢复原始活动策略并停留在 “ 活动策略 ” 页。

路径：配置 > 安全 > 防火墙 > 活动规则

当启用防火墙时，该只读页会列出当前活动策略正强制执行的单个规则。请参阅**创建 / 编辑策略**部分，了解字段的说明 （优先级、目标、源、协议、活动和日志）。

路径：配置 > 安全 > 防火墙 > 创建 / 编辑策略

创建新策略；删除或编辑现有策略：

注：无法删除启用的活动防火墙策略，可以编辑正在运行的策略，但不建议采用此做法，因为会立即应用更改。相反，请禁用防火墙、编辑策略、进行测试，然后重新启用该策略。

创建新策略：单击**添加策略**，然后键入新防火墙文件的文件名。文件名应该包含 .fwl 文件扩展名。如果没有文件扩展名， .fwl 将会自动附加到名称上。

- 单击**应用**：如果文件名合法，则会创建空文件防火墙策略文件。它将位于系统上其他策略的 /fwl 文件夹中。
- 单击**取消**，返回之前的页面而不创建新的防火墙文件。

编辑现有策略：

选择**编辑策略**，进入编辑页面。您可以编辑不活动的防火墙策略。

警告页：如果尝试编辑启用的活动策略，将会打开一个警告页：
“ 编辑活动防火墙策略将导致立即应用做出的所有更改。建议在启用防火墙之前先禁用防火墙并测试策略。 ”

- 单击**应用**，离开 “ 警告 ” 页并返回 “ 编辑策略 ” 页。
- 单击**取消**，离开 “ 警告 ” 页并返回 “ 创建 / 编辑策略 ” 页。

1. 从**策略名称**下拉列表中选择要编辑的策略，然后单击**编辑策略**。
2. 单击**添加规则**或选择现有规则的**优先级**以转至**编辑规则**页。可通过本页面修改规则设置或删除选中的规则。

设置	说明
优先级	如果 2 个规则产生冲突，优先级较高的规则将决定执行的操作。最高优先级是 1 ；最低优先级是 250。
键入	**主机：**在 “IP/ 任何 ” 字段中，您将输入一个 IP 地址。 **子网：**在 “IP/ 任何 ” 字段中，您将输入一个子网地址。 **范围：**在 “IP/ 任何 ” 字段中，您将输入一个 IP 地址范围。
IP/ 任何	指定此规则适用的 IP 地址或地址范围，或选择下列之一： • **任何：**该规则适用于任何 IP 地址。 • **anyipv4：**该规则适用于任何 IPv4 地址。 • **anyipv6：**该规则适用于任何 IPv6 地址。
端口	指定规则将应用的端口。 • **无：**规则将适用于任何端口。 • **通用配置端口：**选择标准端口。 • **其他：**指定非标准端口编号。

设置	说明
协议	指定规则将应用的协议。 • **任何**：任何协议。 • **tcp**：用于应用之间的可靠信息传输。 • **udp**：TCP 的替代方案，用于更快速、更低的宽带信息 传输。虽然延迟较少，但 UDP 的可靠性不及 TCP。 • **icmp**：用于报告错误，进行故障排除。 • **icmpv6**：用于报告错误，在使用 IPv6 的应用程序上进行故障排除。
操作	**允许**：允许符合此规则的数据包。 **放弃**：放弃符合此规则的数据包。
日志	如果将此规则应用于数据包，则无论是阻止还是允许数据包，都会将条目添加到防火墙日志中。请参阅第第 74 页上的“ 防火墙日志 ”。

建议您在防火墙策略中添加以下一项作为最低优先级规则：

- 要将防火墙用作白名单，请添加
  `250 Dest any / Source any / protocol any / discard`
- 要将防火墙用作黑名单，请添加
  `250 Dest any / Source any / protocol any / allow`

删除策略：

选择删除策略，打开“ 确认删除 ”页。

单击应用进行确认，并从文件系统中删除选定的防火墙文件。

路径：配置 > 安全 > 防火墙 > 加载策略

将外部来源的策略 （带 .fwl 后缀）加载到此设备。

路径：配置 > 安全 > 防火墙 > 测试

暂时强制执行所选策略的规则，时长为您指定的时间。

802.1X 安全配置

路径 : 配置 > 安全 > 802.1X 安全

基于 IEEE 802.1X 端口的网络访问控制使用的 EAPoL （基于局域网的扩展认证协议）架构中， NMC 起到请求者的作用。 NMC 支持 EAP-TLS 身份验证方法，该方法需要您上传 3 个客户端证书。私钥以加密格式存储。您需要提供有效的密码才能启用 802.1X 安全访问权限。

注：NMC 仅支持 EAP-TLS 身份验证方法。

Web UI 为 EAPoL 配置提供以下选项：

设置	说明
EAPoL 访问权限	用于启用或禁用 802.1X 安全访问权限。 **注 :** 默认情况下禁用 802.1X 安全访问权限。您仅能在提供有效证书和私钥的有效密码后才能启用访问权限。
请求者标识符	允许您设置自己的请求者标识符 （包括空格在内最多 32 个字符）。 **注 :** 默认情况下，请求者标识符设置为 “NMC-Supplicantxx:xx:xx:xx:xx:xx”，其中六个八字节 “xx” 是 NMC 的 MAC ID。
CA 证书	上传 / 替换或移除 CA 根证书。支持的文件格式为 PEM （隐私增强邮件）或 DER （可辨别编码规则）格式，允许的文件扩展名为 .pem、 .PEM、 .der 或 .DER。
私钥证书	上传 / 替换或移除加密私钥。支持的文件格式为 PEM （隐私增强邮件）或 DER （可辨别编码规则）格式，允许的文件扩展名为 .key 或 .KEY。 **注 :** 不接受未加密的私钥。
私钥密码	提供密码对加密的私钥进行解密。包括空格在内，最多允许 64 个字符。
用户 / 公用证书	上传 / 替换或移除用户 / 公用证书。支持的文件格式为 PEM （隐私增强邮件）或 DER （可辨别编码规则）格式，允许的文件扩展名为 .pem、 .PEM、 .der 或 .DER。

配置设置：2

通过 “ 配置 ” 菜单选项，您可以为 UPS 和 NMC 设置基本的操作值。

请参阅以下部分和 “ 配置设置：1”。

- “ 配置菜单上的网络 ”
- “ 通知菜单 ”
- “ 常规菜单 ”
- “ 配置菜单上的日志 ”

注意：您可以通过 “ 配置摘要 ” 屏幕查看某些配置设置 （**配置 > 网络 > 摘要**）。

配置菜单上的网络

IPv4 屏幕的 TCP/IP 设置

路径：配置 > 网络 > TCP/IP > IPv4 设置

此选项显示 UPS 网络管理卡 3 (NMC) 当前所有的 IPv4 地址、子网掩码、默认网关、 MAC 地址和启动模式。使用屏幕下面部分可配置这些设置，包括禁用 IPv4。

有关 DHCP 和 DHCP 选项的信息，请参阅 RFC2131 和 RFC2132。

选项	说明
手动	在此指定 IPv4 地址、子网掩码和默认网关。
BOOTP*	每隔 32 秒，设备就会请求来自任何 BOOTP 服务器的网络分配： • 如果设备接收到有效的响应，它会启动网络服务。 • 如果存在之前配置的网络设置，且没有收到对五个请求 （最初的一次和四次重试）的有效响应，就会默认使用之前配置的设置。这样可确保 BOOTP 服务器不再可用时，设备仍保持可访问状态。 • 如果设备找到了一台 BOOTP 服务器，但发送至该服务器的请求失败或超时，它就会停止请求网络设置，直至重新启动。
DHCP*	每隔 32 秒，设备就会请求来自任何 DHCP 服务器的网络分配： • 如果找到了一台 DHCP 服务器，但发送至该服务器的请求失败或超时，它就会停止请求网络设置，直至重新启动。 • 当然，您也可以使用**需要供应商特定的 Cookie 才能接受 DHCP 地址**来设置设备，以接受租用并启动网络服务。 请参阅 “DHCP 响应选项 ”。 *

供应商类别：APC
客户端 ID：设备的 MAC 地址。如果您更改该值，新值在局域网中必须是唯一的。
用户类别：应用程序固件模块的名称，请参阅 “ 文件传输 ”。

IPv6 屏幕的 TCP/IP 设置

路径：配置 > 网络 > TCP/IP > IPv6 设置

此选项显示 UPS 网络管理卡 3 (NMC) 当前所有的 IPv6 设置。使用屏幕下面部分可配置这些设置，包括禁用 IPv6。

您可以选择使用手动或自动 IP 寻址，也可同时使用这两种方法。对于**手动**，选择复选框并输入**系统 IP**v6 地址及**默认网关**。

选择**自动配置**复选框可启用系统，以从路由器 （如可用）获得寻址前缀。 它将使用这些前缀，自动配置 IPv6 地址。

IPv6 可用格式	说明
fe80:0000:0000:0000:0204:61ff:fe9d:f156	IPv6 的完整形式
fe80:0:0:0:204:61ff:fe9d:f156	省略前面的 0
fe80:204:61ff:fe9d:f156	在 IPv6 地址中将多个 0 合并为 ::
fe80:0000:0000:0000:0204:61ff:254.157.241.86	末尾为 IPv4 点地址
fe80:0:0:0:0204:61ff:254.157.241.86	省略前面的 0，末尾为 IPv4 点地址
fe80:204:61ff:254.157.241.86	末尾为点地址，合并多个 0
:1	本地主机
fe80:	本地链接前缀
2001:	全局单播前缀

有关 **DHCPv6 模式**的信息，请参阅下表。

IPv6 配置的 DHCPv6 模式	
选项	**说明**
由路由器控制	选择此单选框后， DHCPv6 将由在 IPv6 路由器公告中接收到的 **M** （被管理地址配置标志位）和 **O** （其他配置标志位）标志位控制。 当接收到路由器公告时， NMC 将检查是否设置了 M 和 O 标志位。 NMC 对其解析如下： • **均未设置**：表示本地网络没有 DHCPv6 基础架构。 NMC 使用路由器公告和手动配置来获取并非本地链接的地址和其他设置。 • **设置 M，或 M 和 O**：在这种情况下，将出现完整的 DHCPv6 地址配置。 DHCPv6 用于获取地址和其他配置设置。这称作 “DHCPv6 stateful”。 如果已接收了 M 标志位，即使接收到没有设置 M 标志位的后续路由器公告数据包，DHCPv6 地址配置仍将保持有效，直到相关接口被关闭。 如果首先接收到 O 标志位，之后接收到 M 标志位， NMC 在接收到 M 标志位后，会执行完整地址配置。 • **只设置 O**：在这种情况下， NMC 将发送一个 DHCPv6 信息请求包。 DHCPv6 用于配置 “ 其他 ” 设置 （例如， DNS 服务器位置），但不提供地址。这称作 “DHCPv6 stateless”。
地址及其他信息	DHCPv6 用于获取地址和其他配置设置。这称作 “DHCPv6 stateful”。
仅限非地址信息	DHCPv6 用于配置 “ 其他 ” 设置 （例如， DNS 服务器位置），但不提供地址。这称作 “DHCPv6 stateless”。
从不	DHCPv6 不用于任何配置设置。

DHCP 响应选项

每个有效的 DHCP 响应都包含提供 NMC 在网络中运行所需的 TCP/IP 设置的选项。每个响应也同时具有影响 NMC 运行的其他信息。另请参阅知识库文章 FA156110。

供应商特定信息 （选项 43）

NMC 在 DHCP 响应中使用该选项，以确定 DHCP 响应是否有效。该选项包含一个 TAG/LEN/DATA 格式的选项，称作 APC Cookie。该选项默认为禁用。

- **APC Cookie. Tag 1, Len 4, Data“1APC”**

  选项 43 通知 NMC，已将一台 DHCP 服务器配置为为设备提供服务。

  以下示例显示了包含 APC cookie 的供应商特定信息选项 （十六进制格式）：

  选项 `43 = 0x01 0x04 0x31 0x41 0x50 0x43`

TCP/IP 选项。 NMC 在有效的 DHCP 响应中使用下列选项，定义其 TCP/IP 设置。在 RFC2132 中对所有这些选项 （第一个除外）进行了说明。

- **IP 地址** （来自 DHCP 响应的 **yiaddr** 字段，在 RFC2131) 中说明）：DHCP 服务器租借给 NMC 的 IP 地址。
- **子网掩码** （选项 1）：NMC 在网络上运行所需的子网掩码值。
- **路由器**，即默认网关 （选项 3）：NMC 在网络上运行所需的默认网关地址。
- **IP 地址租用时间** （选项 51）：NMC 租用 IP 地址的持续时间。
- **续租时间， T1** （选项 58）：在分配了 IP 地址租用后， NMC 在请求续租前必须等待的时间。
- **重新租用时间， T2** （选项 59）：在分配了 IP 地址租用后， NMC 在寻求重新租用前必须等待的时间。

其他选项。 NMC 在有效的 DHCP 响应中也使用这些选项。所有这些选项 （最后两个除外）都在 RFC2132 中进行了说明。

- **网络时间协议服务器** （选项 42）：NMC 最多可使用的两台 NTP 服务器 （主服务器与次服务器）。
- **时间偏移** （选项 2）：NMC 的子网相对于世界标准时间 (UTC) 的偏移量，单位：秒。
- **域名服务器** （选项 6）：NMC 最多可使用的两台域名 (DNS) 服务器 （主服务器与次服务器）。
- **主机名** （选项 12）：NMC 将使用的主机名 （最多 32 个字符）。
- **域名** （选项 15）：NMC 将使用的域名 （最多 64 个字符）。
- **启动文件名称** （来自 DHCP 响应的**文件**字段，在 RFC2131 中说明）：下载用户配置文件 （.ini 文件）的完整、有效的目录路径。DHCP 响应的 **siaddr** 字段指定 NMC 下载 .ini 文件的服务器的 IP 地址。下载后， NMC 使用 .ini 文件作为重新配置其设置的启动文件。
- **完全合格的域名** （FQDN，选项 81）：NMC 的完全合格的域名。

端口速度屏幕

路径：配置 > 网络 > 端口速度

“ 端口速度 ” 设置定义了以太网网络端口的通信速度。您的当前设置将在**当前速度**中显示。

您可以通过选择**端口速度**下的单选按钮来更改设置：

- 对于**自动协商** （默认），网络设备会进行协商，尽量以最高速度传输，但是如果两台设备支持的速度不匹配，就会使用较慢的速度。
- 另外，您可以选择 **10** Mbps 或 **100** Mbps，每个速度都有以下选项：
  - **半双工** （一次只在一个方向上通信）或
  - **全双工** （在同一个通道中同时在两个方向上通信）。

注意：您仅可通过选择**自动协商**单选按钮，将端口速度更改为 1000 Mbps。

DNS 屏幕

路径：配置 > 网络 > DNS > 配置

域名系统状态下的值列出了您当前的状态和设置。

使用**手动域名系统设置**下的选项可配置域名系统 (DNS)：

- 启用**屏蔽手动 DNS 设置**意味着其他来源 （如 DHCP）的配置数据优先于此处的手动配置。
- 指定**主 DNS 服务器**，或者具有 IPv4 或 IPv6 地址的**次 DNS 服务器**。对于发送电子邮件的 NMC，您必须至少定义主 DNS 服务器的 IP 地址。
  - 对于来自于主 DNS 服务器或次 DNS 服务器的响应， NMC 最多等待 15 秒。如果 NMC 在该时间内没有收到响应，将无法发送电子邮件。使用与 NMC 处于相同网段或附近网段，但不通过广域网 (WAN) 的 DNS 服务器。
  - 定义 DNS 服务器的 IP 地址后，对其进行测试，请参阅 “ 测试 DNS 屏幕 ”。
- **系统名称同步**：启用此选项可使 DNS 主机名与 NMC 系统名称同步。单击 “ 系统名称 ” 链接可对其进行定义。

  如果 DNS 主机名和 NMC 系统名称同步，则会根据 DNS RFC 将系统名称限制为特定字符数。如果不同步，则会将系统名称限制为 255 字符。
- **主机名**：您在此处配置了主机名称并在**域名**字段配置了域名后，用户可以在接受域名的 NMC 界面 （电子邮件地址除外）中的任何字段输入主机名。
- **域名 (IPv4/IPv6)**：对于 NMC 界面，您只需在此处配置域名。在此接受域名 （电子邮件地址除外）的 UI 中的所有其他字段中，只有输入主机名后， NMC 才会默认添加该域名。
  - 若要屏蔽添加域名指定的主机名的扩展名，请将域名字段设置为默认值 `somedomain.com` 或 `0.0.0.0`。
  - 若要屏蔽 *特定*主机名条目的扩展名 （例如，在定义陷阱接收器时），请在后面添加一个圆点。 NMC 会识别带圆点的主机名 （例如 `mySnmpServer.`），就好像它是完全合格的域名，并且不会附加域名。
- **域名 (IPv6)**：在此处指定 IPv6 域名。

测试 DNS 屏幕

路径：配置 > 网络 > DNS > 测试

使用此选项可发送通过查找 IP 地址测试 DNS 服务器设置的 DNS 查询。有关如何设置服务器的信息，请参阅上文的 “DNS 屏幕 ”。

查看**上次查询响应**结果字段中的测试结果。

- 根据**查询类型**，选择 DNS 查询使用的方法，请参阅下表。
- 根据**查询问题**，指定将用于所选查询类型的值，请参阅下表说明。

所选查询类型	要使用的查询问题
按主机	主机名、 URL
按 FQDN	完全合格的域名， `my_server.my_domain.com`
按 IP	服务器的 IP 地址。
按 MX	Mail Exchange 地址。

Web 访问屏幕

路径：配置 > 网络 > Web > 访问权限

使用此选项可配置 Web 界面的访问方式。（为激活此处的任何更改，您必须重新启动 NMC。请参阅第 23 页上 “ 控制菜单上的网络 ”）。

您可以使用 “ 启用 ” 复选框，通过 **HTTP** 或 **HTTPS** 或二者同时来启用对此 UI 的访问。默认情况下，HTTP 为禁用状态， HTTPS 为启用状态。 HTTPS 会在传输过程中对用户名、密码和数据加密，而 HTTP 不会。

HTTPS 还会通过数字证书对 NMC 进行身份验证。有关数字证书的使用方法，请参阅 **APC 网站**上提供的 *《安全手册》* 中的 “ 创建和安装数字证书 ”。

对于**端口**，您可以将设置更改为任何未使用的端口以提高安全性，范围为 5000 到 32768。然后，您必须在浏览器的地址字段中使用冒号 (:) 来指定端口号。例如，对于端口号 5000 和 IP 地址 152.214.12.114，请键入：

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

指定用于保护浏览器和 NMC 之间通信的最低协议：TLS v1.1 或 TLS v1.2。

通过要求启用验证 Cookie 复选框，可以在浏览器中启用会话 cookie 进行身份验证跟踪。**注意**：会话结束后会删除 cookie。

通过有限状态访问复选框，选择是否显示含基本设备状态的只读公共网页。默认禁用此功能，可以通过用作默认页面选项进行设置，用户仅使用 IP/ 主机名访问设备时显示默认登录页面。

Web SSL 证书屏幕

路径：配置 > 网络 > Web > SSL 证书

添加、替换或移除安全证书。 SSL （安全套接层）是一种协议，用于加密浏览器与 web 服务器之间的数据。

状态包括：

- **证书有效**：NMC 安装或生成了一份有效的证书。点击该链接，查看证书的内容。
- **未安装证书**：没有安装证书，或 FTP 或 SCP 没有将证书安装到正确的位置。使用**添加或替换证书文件**将证书安装到 NMC 上的正确位置：**/ssl**。
- **正在生成**：由于没有找到有效证书， NMC 正在生成一个证书。
- **正在加载**：正在激活 NMC 上的证书。

*启用 SSL 后，如果您安装的证书无效，或没有加载证书，则 NMC 会生成一份默认的证书，该过程最多会将对界面的访问延迟一分钟。*您可以使用默认的证书，实现基于基本加密的安全性，但是每当您登录时，都会显示一个安全警报消息。

添加或替换证书文件：浏览至使用安全向导创建的证书文件。有关 通过安全向导创建或 NMC 生成的数字证书的使用方法，请参阅 **APC 网站**上的 *《安全手册》* 中的 “ 创建和安装数字证书 ”。

移除：删除证书。另请参阅屏幕文字。

控制台屏幕

路径：配置 > 网络 > 控制台 > 访问权限

路径：配置 > 网络 > 控制台 > SSH 主机密钥

控制台访问

您需要启用控制台访问，才能更新 UPS 固件，请参阅 “ 固件更新屏幕 ”。控制台访问可启用命令行界面 (CLI)。

您可以使用 “ 启用 ” 复选框，通过 **Telnet** 或 **SSH** 或二者同时来启用对 CLI 的访问。默认情况下，Telnet 为禁用状态， SSH 为启用状态。 Telnet 在传输过程中不会对用户名、密码和数据加密，而 SSH 会。

注：如果您启用 SSH，则也会启用 SCP （安全拷贝），以用于安全文件传输。有关使用 SCP 的详细信息，请参阅 “ 文件传输 ”。

对于用于与 NMC 通信的端口，您可以将设置更改为任何未使用的端口以提高安全性，范围为 5000 到 32768。

- **Telnet 端口**：默认为 23。然后，您必须根据 Telnet 客户端程序的要求，使用冒号 (:) 或空格指定非默认的端口。

  例如，对于端口 5000 和 IP 地址 152.214.12.114，您的 Telnet 客户端需要以下命令之一：

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

- **SSH 端口**：默认为 22。有关指定非默认端口所需的命令行格式，请参阅 SSH 客户端的文档。另请参阅下文的 “SSH 主机密钥。 ”。

SSH 主机密钥。

如果您正在使用 SSH （安全接壳协议）进行控制台 (CLI) 访问，您可以在 “SSL 主机密钥 ” 屏幕中添加、替换或移除主机密钥。

状态显示主机密钥 （私有密钥）是否有效。 “ 状态 ” 包括：

- **SSL 已禁用**：当前未使用任何主机密钥。
- **正在生成**：由于没有找到有效的主机密钥， NMC 正在创建一个主机密钥。
- **正在加载**：正在激活 NMC 上主机密钥。
- **有效**：下列有效主机密钥之一包含在 **/ssh** 目录 （网络管理卡上的所需位置）中：
  - 安全向导创建的 1024 位或 2048 位主机密钥
  - 网络管理卡生成的 2048 位 RSA 主机密钥

添加或替换主机密钥：上载安全向导创建的主机密钥文件。若要使用安全向导，请参阅 **APC 网站**上的 *《安全手册》*。若要使用外部创建的主机密钥，请在启用 SSH 前加载主机密钥 （参阅上文的 “ 控制台访问 ”）

注：为了减少启用 SSH 所需的时间，请提前创建和上载主机密钥。*如果您启用 SSH，但没有加载主机密钥，则 NMC 最多需要一分钟的时间来创建主机密钥，在此期间， SSH 服务器将无法访问。*

移除：删除主机密钥。另请参阅屏幕文字。

若要使用 SSH，您必须安装 SSH 客户端。大多数 Linux 和其它 UNIX 平台都包含 SSH 客户端，但微软 Windows 操作系统没有 （Windows 10 除外）。可以从各个供应商处获得适用于 Windows 的客户端，例如，可以从 www.putty.org 获得 PuTTY。

SNMP 屏幕

SNMP 的所有用户名、密码和团体名称都会以纯文本的格式通过网络传输。如果您的网络要求高安全性加密，请禁用 SNMP 访问或将每个团体的访问权限设置为读取。（具有读取权限的团体可以接收状态信息和使用 SNMP 陷阱。）

当使用 **StruxureWare Data Center Expert** 管理 StruxureWare 系统公共网络上的 UPS 时，您*必须*在 NMC 界面中启用 SNMPv1 或 SNMPv3 （默认启用 SNMPv1）。读取访问权限将允许 StruxureWare 设备从 NMC 接收陷阱，但是在您使用 NMC 用户界面将 StruxureWare 设备设置为陷阱接收器时，需具有写入访问权限。

有关增强和管理系统安全的详细信息，请参阅 **APC 网站**上提供的 *《安全手册》*。

SNMPv1。

路径：配置 > 网络 > SNMPv1 > 访问权限和访问控制

使用 **访问权限**可启用或禁用 SNMP 版本 1 作为与 NMC 通信的方法。

默认情况下， SNMPv1 为禁用状态。必须设置**团体名称**，才能建立 SNMPv1 通信。

SNMPv1 选项支持使用 SNMPv2c。

访问控制

您最多可配置四个访问控制条目，指定对 NMC 具有访问权限的网络管理系统 (NMS)。
若要进行编辑，请单击团体名称。

默认情况下，将为四个可用 SNMPv1 团体中的每一个团体分配一个条目。您可以编辑这些设置，*对任何一个团体应用多个条目*，以将访问权限授予多个特定的 IPv4 和 IPv6 地址、主机名或 IP 地址掩码。

- 默认情况下，团体具有对网络中任何位置的 NMC 的访问权限。
- 如果您为任何一个团体名称配置多个访问控制条目，这意味着一个或多个其他团体将不具有对设备的访问权限。

团体名称：网络管理站 (NMS) 访问团体必须使用的名称。最大长度为 16 个 ASCII 字符。

NMS IP/ 主机名称：控制 NMS 的访问权限的 IPv4 或 IPv6 地址、 IP 地址掩码，或者主机名称。一个主机名或一个特定的 IP 地址 （例如， 149.225.12.1）只允许 NMS 在该位置进行访问。包含 255 的 IP 地址的访问权限限制如下：

- 149.225.12.**255**：仅 149.225.12 网段上的 NMS 才能访问。
- 149.225.**255.255**：仅 149.225 网段上的 NMS 才能访问。
- 149.**255.255.255**：仅 149 网段上的 NMS 才能访问。
- 0.0.0.0 （默认设置）也可以写作 255.255.255.255：任何网段上的任何 NMS 均可访问。

访问权限类型：NMS 通过团体可执行的操作。

- 读：任何时候都只能执行 GET
- 写：在任何时候都可以执行 GET，在没有用户登录 UI 或者命令行界面时，还可以执行 SET。
- 写 +：任何时候都可执行 GET 和 SET。
- 禁用：任何时候都不能执行 GET 或 SET。

SNMPv3。

路径：配置 > 网络 > SNMPv3 > 访问权限、用户配置文件和访问控制

对于 GET、 SET 和陷阱接收器， SNMPv3 使用用户配置文件系统来识别用户。 SNMPv3 用户在 MIB 软件程序中必须分配有用户配置文件，才能执行 GET 和 SET、浏览 MIB 并接收陷阱。

默认情况下， SNMPv3 为禁用状态。必须使用密码 （身份验证密码、隐私密码）启用有效的用户配置文件，才能建立 SNMPv3 通信。

若要使用 SNMPv3，您必须安装可支持 SNMPv3 的 MIB 程序。

NMC 支持 SHA 或 MD5 身份验证和 AES 或 DES 加密。

“ 访问权限 ” 下的**启用 SNMPv3 访问**可启用这一方法与该设备进行通信。

用户配置文件

默认情况下，将列出四个使用用户名 **apc snmp profile1** 至 **apc snmp profile4** 配置的用户配置文件的设置，且无身份验证、无隐私 （不加密）。若要编辑用户配置文件的以下设置，请单击列表中的用户名。

- 用户名：用户配置文件的识别符。 SNMP 版本 3 通过将配置文件的用户名与正在传输的数据包中的用户名相匹配，将 GET、 SET 和陷阱映射至用户配置文件。一个用户名最多包含 32 个 ASCII 字符。
- 身份验证密码：一个 15 到 32 个 ASCII 字符的短语，可验证通过 SNMPv3 与该设备通信的 NMS 为其承认的 NMS ；还可验证在传输过程中消息没有被更改，并且消息以及时的方式通信，表明没有出现延迟，没有被复制，并且之后没有在不适当的时间被重新发送。
- 隐私密码：一个 15 至 32 个 ASCII 字符的短语，通过使用加密确保对 NMS 传送至该设备或通过 SNMPv3 从该设备接收到的数据保密。
- 身份验证协议：采用 SNMPv3 支持 SHA 和 MD5 身份验证。必须选择其一。
- 隐私协议：采用 SNMPv3 支持将 AES 和 DES 作为加密和解密数据的协议。您必须同时使用隐私协议和隐私密码，否则就不会对 SNMP 请求加密。

  反过来说，如果没有选择身份验证协议，您就无法选择隐私协议。

访问控制。您最多可配置四个访问控制条目，指定对 NMC 具有访问权限的网络管理系统 (NMS)。若要进行编辑，请单击用户名。

默认情况下，将为四个用户配置文件中的每一个分配一个条目。您可以编辑这些设置，*对任何一个用户配置文件应用多个条目*，以将访问权限授予多个特定的 IP 地址、主机名或 IP 地址掩码。

- 默认情况下，所有使用该配置文件的 NMS 都具有对此设备的访问权限。
- 如果您为某个用户配置文件配置多个访问控制条目，这意味着一个或多个其他用户配置文件将不具有对此设备的访问权限。

用户名：从下拉列表中，选择该访问控制条目将应用的用户配置文件。可用选择为您通过 “ 用户配置文件 ” 选项配置的四个用户名。

NMS IP/ 主机名称：控制 NMS 的访问权限的 IP 地址、 IP 地址掩码或主机名称。一个主机名或一个特定的 IP 地址 （例如， 149.225.12.1）只允许 NMS 在该位置进行访问。包含 255 的 IP 地址的访问权限限制如下：

- 149.225.12.**255**：仅 149.225.12 网段上的 NMS 才能访问。
- 149.225.**255.255**：仅 149.225 网段上的 NMS 才能访问。
- 149.**255.255.255**：仅 149 网段上的 NMS 才能访问。
- 0.0.0.0 （默认设置）也可以写作 255.255.255.255：任何网段上的任何 NMS 均可访问。

Modbus 屏幕

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备不支持 Modbus。

通过 Modbus 选项将 NMC 配置为使用 Modbus 协议连接到楼宇管理系统 (BMS)。AP9640 NMC 卡支援 Modbus TCP， AP9641 和 AP9643 NMC 卡除了支援 Modbus TCP 外也支援 Modbus 序列。

有关在 UPS 上实施 Modbus 的详细信息，请参阅 **APC 网站**上提供的 *《Modbus 文档附录》* 和 *《Modbus 寄存器映射》*。

有关针对具有前缀 SMT、 SMX、 SURTD、 SRC 和 SRT 的 Smart-UPS 型号使用 Modbus 进行开关插座组管理的详细信息，请参阅 APC 网站 www.apc.com 上的应用注释 # 177。

注意：连接到 AP9641 和 AP9643 NMC 的 UIO 端口的温度和湿度传感器不通过 Modbus 受支持。

Modbus 串行 （仅限 AP9641 或 AP9643）

路径：配置 > 网络 > Modbus > 串行

1. 使用**访问权限**可启用或禁用 Modbus 串行作为与 NMC 通信的方法。
2. 为 Modbus 串行连接设置连接参数：
   - **波特率**是以比特 / 秒为单位的数据速率。它可以设置为 9600 （默认）或 19200。
   - **奇偶校验位**是校验位，可以设置为偶、奇或无。
   - **目标唯一 ID** 是目标设备的唯一 ID。它可以设置为 1 到 247 之间的值。
3. 单击 “ 应用 ” 保存所作的更改。

Modbus TCP。

路径：配置 > 网络 > Modbus > TCP

1. 使用**访问权限**可启用或禁用 Modbus TCP 作为与 NMC 通信的方法。
2. 为 TCP 连接设置**端口**号。它可以设置为 502 （默认）或 5000 到 32768 之间的值。
3. 单击 “ 应用 ” 保存所作的更改。

BACnet 屏幕

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备不支持 BACnet。

通过 BACnet 选项将 NMC 配置为使用 BACnet 协议，并使 UPS 数据可用于楼宇自动化和控制网络。

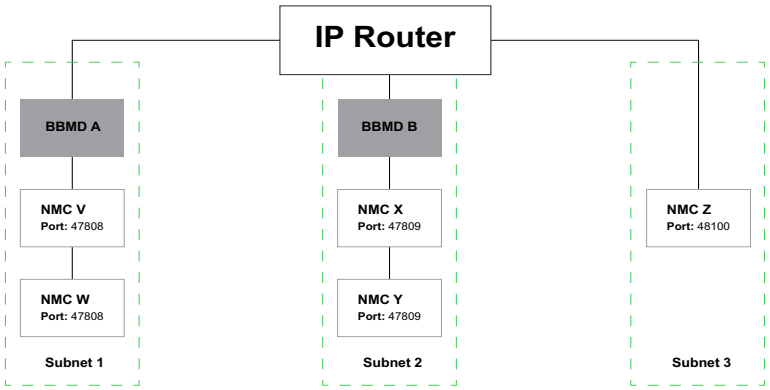
有关通过 BACnet 提供 UPS 数据点的更多信息，请参阅 APC 网站 www.apc.com 上提供的《BACnet 应用映射》。

BACnet 配置

选项	说明
访问权限	选中此复选框启用 BACnet。如果未启用，则 NMC 无法通过 BACnet 访问。默认情况下， BACnet 为禁用状态。 **注意：**在设置**设备通信控制密码**之前，无法启用 BACnet。
设备 ID	此 BACnet 设备的唯一标识符，用于寻址设备。可接受范围：0 – 4194303。
设备名称	此 BACnet 设备的名称，在 BACnet 网络上必须是唯一的。默认设备名称是 “BACn”+ NMC MAC 地址的最后八位数字。最小长度为 1 个字符，最大长度为 150 个字符，允许使用特殊字符。
网络协议	选择要使用的网络协议： • BACnet/IP
APDU 超时	NMC 将等待 BACnet 请求响应的毫秒数。可接受范围：1000 - 30000。缺省值是 6000。
APDU 重试	在中止请求之前， NMC 将做出的 BACnet 请求尝试的数量。可接受范围：1 – 10。缺省值是 3。
设备 通信 控制密码	BACnet 客户端使用设备通信控制服务来命令远程设备 （例如，启用了 BACnet 的 NMC）停止发起或停止响应指定持续时间内的所有 APDU （设备通信控制服务除外）。该服务可用于诊断目的。 指定设备通信控制密码，以确保 BACnet 客户端无法控制 NMC 的 BACnet 通信，而无需先提供此处设置的密码。密码必须在 8 到 20 个字符之间，并且必须包含： • 数字。 • 大写字符。 • 小写字符。 • 特殊字符。 建议在首次启用 BACnet 时更新密码。无需知道当前密码即可更新密码。

BACnet/IP

选项	说明
本地端口	NMC 用来发送和接收 BACnet/IP 消息的 UDP/IP 端口。 可接受范围：5000 – 65535。缺省值：47808。 **注：**启用了 BACnet/IP 的 NMC 地址被定义为 NMC 和本地端口的 IP 地址。

选项	说明
启用外部设备注册	选择复选框以使用 BACnet 广播管理设备 (BBMD) 注册 NMC。 **注：**如果 NMC 的子网上当前没有 BBMD，或者 NMC 使用不同的本地端口连接到 BBMD，则需要将 NMC 注册为具有 BBMD 的外部设备。  上面的范例中： • BBMD A 管理 NMC V 和 W 的广播消息。 • BBMD B 管理 NMC X 和 Y 的广播消息。 • 只有 NMC Z 需要将 BBMD A 或 B 注册为外部设备，因为其子网上不存在 BBMD。 • 注册后， NMC Z 可以从注册的 BBMD 接收广播消息，并且可以将消息发送到 BBMD，BBMD 将其广播到其子网中的所有设备，并通过 IP 路由器广播到网络上的其他 BBMD。
状态	外部设备注册状态 (FDR)： • **外部设备注册不活动** 以下情况， FDR 将不活动： – FDR 启用， BACnet 禁用 – FDR 禁用， BACnet 启用 – FDR 禁用， BACnet 禁用 • **注册成功** FDR 成功完成。 • **注册拒绝** FDR 未成功完成。NMC 将自动重试注册，但也可以使用**启用外部设备注册**复选框来提示 NMC 重新注册。 • **注册发送** FDR 请求已发送，但尚未完成。
BACnet/IP 广播管理设备	BACnet 广播管理设备的 IP 地址或完全限定域名 (FQDN)， NMC 卡将在此注册。
端口	BBMD 端口， NMC 卡将在此注册。
TTL	BBMD 将 NMC 保留为注册设备的秒数 （生存时间）。如果 NMC 在此时间之前没有重新注册，则 BBMD 将从其外部设备表中删除， NMC 将不再能够通过 BBMD 发送和接收广播消息。TTL 控制 NMC 向 BBMD 注册的频率，因为 NMC 将在这段时间到期之前尝试重新注册。

FTP 服务器屏幕

路径：管理 > 网络 > FTP 服务器

使用此屏幕可启用对 FTP 服务器访问权限并指定端口。

选项	说明
访问权限	FTP 传输文件时不会对文件加密。默认情况下， FTP 为禁用状态。 对于加密的文件传输，请使用安全拷贝 (SCP)。默认情况下， SCP （通过 SSH）为启用状态。但是，在更改超级用户默认密码 (apc) 之前，不允许文件传输。 **注意：**如果您希望随时可以访问设备，以便通过 StruxureWare Data Center Expert 或操作进行管理，则必须在该 UPS 的网络管理卡界面上启用 FTP 服务器。 有关增强和管理系统安全的详细信息，请参阅 APC 网站上提供的 *《安全手册》*。
端口	FTP 服务器的 TCP/IP 端口 （默认为 21）。 FTP 服务器使用指定端口和比指定端口小一个号码的端口。屏幕上会显示允许的非默认端口号：21 和 5001–32768。 **注：**通过让用户在 FTP 命令行中为 IP 地址附加端口名称，将 FTP 服务器配置为使用非默认的端口可提高安全性。根据所使用的 FTP 客户端，必须在附加的端口名称前面添加一个空格或冒号。

Wi-Fi 屏幕 （仅限 AP9641、 AP9643 和 SRTL 设备）

路径：配置 > 网络 > Wi-Fi

注意：当可选的 APC USB Wi-Fi 设备 (AP9834) 插入 AP9641/AP9643 卡的 USB 端口或插入带有嵌入式 NMC 且前缀为 SRTL 的 UPS 设备时，此屏幕会显示。

注意：建议您不要从有线连接的设备下载 config.ini 文件并上传整个文件到已启用 Wi-Fi 的设备，也不建议您从已启用 Wi-Fi 的设备下载 config.ini 文件并把整个文件上传到有线连接的设备，除非 `[NetworkWiFi]` 部分已被移除或所有设置命令前加分号改为注释（例如 `;WiFi = enabled`）。
`[NetworkWiFi]` 部分包含 ounce 用于 Wi-Fi 的设备设置信息，这些设置信息不能被上传到有线连接的设备。

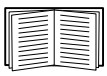
使用此屏幕可查看 Wi-Fi 网络的当前状态、启用/禁用 Wi-Fi，以及配置 Wi-Fi 网络的设置。

注意：启用/禁用 Wi-Fi 将禁用/启用有线局域网连接。配置 Wi-Fi 设置后，NMC 3 将重启。重启后，有线网络将被禁用，并且 NMC 3 会尝试连接到给定的网络名称 (SSID).

网络名称 (SSID)：指定 Wi-Fi 网络的网络名称 (SSID)。最大长度为 32 个字符。

安全类型：指定 Wi-Fi 网络的安全类型，并提供身份验证详细信息:

选项	说明
WPA	**Wi-Fi 密码：**为 Wi-Fi 网络指定密码。最大长度为 64 个字符。
WPA2-AES	
WPA2-Mixed	
WPA2-TKIP	
WPA2-Enterprise	• **用户名：**WPA2-Enterprise 身份验证的用户名。最大长度为 32 个字符。 • **密码：**WPA2-Enterprise 身份验证的密码。最大长度为 32 个字符。 • **外部标识：**指定 WPA-2-Enterprise 外部标识。这是 WPA-2-Enterprise 服务器使用的可选未加密标识。例如：user@example.com 或匿名。最大长度为 32 个字符。



有关如何升级 APC USB Wi-Fi 设备 (AP9834) 固件的信息，请参阅《NMC 3 CLI 指南》中的 wifi 命令。

若要对与 APC USB Wi-Fi 设备 (AP9834) 的连接以及设备的指示灯说明进行故障排除，请参阅 “APC USB Wi-Fi 硬件保护装置 (AP9834) 问题”。

通知菜单

请参阅以下部分：

- “ 通知类型 ”
- “ 配置事件操作 ”
- “ 电子邮件通知屏幕 ”
- “ 常规菜单 ”
- “SNMP 陷阱接收器屏幕 ”

通知类型

您可以配置响应事件时的通知操作。您可以采用几种方式的任意一种向用户通知事件：

- 活动、自动通知。直接联系指定的用户或监测设备。
  - 电子邮件通知
  - SNMP 陷阱
  - 系统日志通知
- 间接通知
  - 事件日志。如果没有配置直接通知，用户必须检查日志，确定发生的事件。

您也可以记录系统性能数据，用于设备监测。有关如何配置和使用此数据记录选项，请参阅 “ 数据日志 ”。

– 查询 (SNMP GET)

有关更多信息，请参阅 “SNMP 陷阱接收器屏幕 ” 和 “ 常规菜单 ”。SNMP 启用 NMS 来执行信息查询。对于 SNMPv1，在传输前不对数据加密，通过配置最受限制的 SNMP 访问类型 (READ) 来启用信息查询，不存在远程配置被修改的风险。

NMC 支持使用 **RFC1628 MIB** （管理信息库）。有关设置陷阱接收器的信息，请参阅 “SNMP 陷阱接收器屏幕 ”。三个事件的 **1628 MIB** 组仅用于此 MIB，而非可选的 Powernet MIB。可以像配置其他事件那样配置它们 （请参阅后文的 “ 配置事件操作 ”）。

配置事件操作

按事件配置

路径：配置 > 通知 > 事件操作 > 按事件

默认情况下，将为所有事件选择日志记录操作。为每个事件定义事件操作：

1. 选择**配置**菜单，然后选择**通知**、**事件操作**和**按事件**。
2. 若要查找事件，请单击栏标题查看**电源事件**、**环境事件**或**系统事件**类别下的列表。

   或者，您可以单击这些标题下的子类别，如**输入线路状态**或**温度**。
3. 单击事件名称以查看或更改当前配置 （例如，通过电子邮件通知的收件人，或通过 SNMP 陷阱通知的网络管理系统 [NMS]）。请参阅 “ 通知参数 ”。单击**事件日志**复选框，以启用或禁用此事件的事件日志条目。

如果没有配置系统日志服务器，则与系统日志配置相关的项目将不会显示。

查看事件配置的详细信息时，您可以启用或禁用事件日志记录或系统记录，或者禁用特定电子邮件收件人或陷阱接收器的通知，但您不能添加或者删除收件人或接收器。若要添加或删除收件人或接收器，请参阅以下部分：

- “ 确定系统日志服务器 ”
- “ 电子邮件收件人 ”
- “ 陷阱接收器 ”

按事件组配置

路径：配置 > 通知 > 事件操作 > 按组

同时配置一组事件：

1. 选择**配置**菜单，然后选择**通知**、**事件操作**和**按组**。
2. 选择如何给事件分组以进行配置：
   - 选择**按严重程度分组**，然后选择一个或多个严重程度。您无法更改事件的严重程度。
   - 选择**按类别分组**，然后选择一个或多个预定义类别中的所有事件。
3. 单击“下一个”，在屏幕之间移动，执行下列操作：
   a. 为事件组选择事件操作。
      - 若要选择除**日志记录**（默认）以外的任何操作，您首先必须至少配置一个相关收件人或接收器。
      - 如果您选择**日志记录**，并且已配置系统日志服务器，请在下一屏幕上选择**事件日志**或系统日志（或两者）。（请参阅“配置菜单上的日志”）。

   b. 选择是否让该事件组保持启用新配置的事件操作，或禁用该操作。

   请参阅正下方的“通知参数”。

通知参数。这些配置字段定义了发送事件通知的参数。请参阅“按事件配置”和“按事件组配置”。.

通常通过单击接收器或收件人名称访问这些参数。

字段	说明
通知延迟	如果事件在指定时间内仍然存在，则发送通知。如果该状况在时间到期前清除，则不发送通知。
重复间隔	在指定的时间间隔（默认为每 2 分钟，直至状况清除）重复发送通知。
初次发送后的通知数	事件处于活动状态时，重复发送通知的次数。
或	
通知直至状况清除	重复发送通知，直至状况清除或得到解决。

对于具有相关清除事件的事件，您也可以设置这些参数。（具有其清除事件的事件示例为 UPS：与电池组的通信中断和
UPS：已恢复与电池组的通信）。

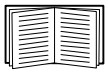
电子邮件通知屏幕

设置概况。使用简单邮件传输协议（SMTP），在发生事件时，将电子邮件最多发送给四个收件人。

若要使用电子邮件功能，您必须定义下列设置：

- 主域名系统 (DNS) 服务器和次域名系统 (DNS) 服务器（可选）的 IP 地址。（请参阅“DNS 屏幕”）

- **SMTP 服务器**的 IP 地址或 DNS 名称和**发件人地址**。（请参阅下文的 “SMTP 服务器 ”）
- 最多四个收件人的电子邮件地址。（请参阅 “ 电子邮件收件人 ”）



您可以使用**收件人**选项的**收件人地址**设置，向基于文字的屏幕发送电子邮件。

SMTP 服务器

路径：配置 > 通知 > 电子邮件 > 服务器

此屏幕列出了您的主次 DNS 服务器 （请参阅 “DNS 屏幕 ”）以及以下字段：

字段	说明
传出邮件配置	
发件人地址	NMC 发送的电子邮件消息中的**发件人**字段中的内容： • 格式为 *user@ [IP 地址]*（如果 IP 地址被指定为**本地 SMTP 服务器**） • 在电子邮件消息中的格式为 *user@ 域*（如果配置了 DNS，且 DNS 名称被配置为**本地 SMTP 服务器**）。 **注：**本地 SMTP 服务器可能要求您针对该设置使用服务器上的有效用户帐户。请参阅服务器的文档。
SMTP 服务器	本地 SMTP 服务器的 IPv4/IPv6 地址或 DNS 名称。 **注：**只有在 **SMTP 服务器**设置为**本地**时，才要求该定义。请参阅 “ 电子邮件收件人 ”。
身份验证	如果 SMTP 服务器需要进行身份验证，则启用此选项。
端口	SMTP 默认端口为 25。备选端口：465、 587、 2525、 5000 - 32768。
用户名 / 密码 / 确认密码	如果您的邮件服务器需要身份验证，请在此处键入您的用户名和密码。这只是执行简单的身份验证，而非 SSI 验证。
高级	
使用 SSL/TLS	• **从不**：SMTP 服务器不要求也不支持加密。 • **如果支持**：SMTP 服务器发出支持 STARTTLS 的公告，但 *不*要求加密连接。STARTTLS 命令在发出公告后发送。 • **始终**：SMTP 服务器要求 STARTTLS 命令在连接到它时发送。 • **隐式**：SMTP 服务器只接受已加密的连接。无 STARTTLS 消息发送至服务器。
需要 CA 根证书	此选项只应在您的组织的安全策略不允许 SSL 连接的隐式信任时启用。启用后，必须将有效的根 CA 证书加载到 NMC 才能发送加密电子邮件。
文件名	此字段取决于 NMC 上安装的根 CA 证书和是否需要根 CA 证书。

电子邮件收件人

路径：配置 > 通知 > 电子邮件 > 收件人-

最多指定四个电子邮件收件人。单击名称，配置设置。另请参阅上文的 “SMTP 服务器 ”。

字段	说明
电子邮件生成	启用 （默认）或禁用发送电子邮件给收件人。
收件人地址	用户和收件人的域名。若要使用电子邮件寻呼，请使用电子- 邮件地址，作为收件人寻呼机的网关帐号 （例如， `myacct100@skytel.com`）。寻呼机网关将发出寻呼。 若要绕过邮件服务器 IP 地址的 DNS 查找，请使用 IP 地址并加括号，而非电子邮件域名，例如，使用 jsmith@[xxx.xxx.x.xxx]，而不是 jsmith@company.com 。当 DNS 查找工作不正常时，这样很有用。 **注：**收件人的寻呼机必须能够使用基于文本的消息。
格式	长格式包含设备名称、位置、触点、 IP 地址、序列号、日期和时间、事件代码以及事件说明。短格式仅提供事件说明。
语言	从下拉列表中选择一种语言，所有邮件都将以该语言发送。可以针对不同用户使用不同语言。请参阅 “ 添加和修改语言包 ”。
服务器	选择以下电子邮件路由方法之一： • 本地：通过本地站点的 SMTP 服务器。此建议设置可确保使用本地站点的 SMTP 服务器发送电子邮件。选择此设置会限制延迟和网络中断，并在数小时内重试发送电子邮件。 当选择本地设置时，您必须同时启用在设备的 SMTP 服务器转发，并设置一个特殊的外部电子邮件帐户来接收转发的电子邮件。做出这些更改前，请咨询您的 SMTP 服务器管理员。 • 收件人：通过收件人的 SMTP 服务器。 NMC 对收件人电子邮件地址执行 MX 记录查找，并将该地址用作其 SMTP 服务器。电子邮件只发送一次，因此很容易丢失。 • 自定义：此设置可使每个电子邮件收件人都具有其独有的服务器设置。这些设置不受上文 “SMTP 服务器 ” 下的设置影响。

电子邮件 SSL 证书。

路径：配置 > 通知 > 电子- 邮件 > SSL 证书

在 NMC 上加载邮件 SSL 证书可提高安全性。文件的扩展名必须为 `.crt` 或 `.cer`。可在任何给定时间加载最多五个文件。

安装时，此处还会显示证书详细信息。无效证书的所有字段都将显示为 “n/a” （“ 文件名 ” 除外）。

证书可从此屏幕中删除。应手动修改任何使用证书的电子邮件收件人，以删除此证书的引用。

电子邮件测试。

路径：配置 > 通知 > 电子邮件 > 测试-

给已配置的收件人发送一条测试消息。

SNMP 陷阱接收器屏幕

陷阱接收器

路径：配置 > 通知 > SNMP 陷阱 > 陷阱接收器

通过简单网络管理协议 (SNMP) 陷阱，您可以自动获得重要 UPS 事件的通知。这些工具对监测网络上的设备十分有用。

陷阱接收器将按 **NMS IP/ 主机名**显示，其中 NMS 代表网络管理系统。您最多可以配置 6 个陷阱接收器。

若要配置新的陷阱接收器，请单击**添加陷阱接收器**。若要编辑 （或删除）接收器，请单击其 IP 地址 / 主机名。

如果您删除了一个陷阱接收器，在 “ 配置事件操作 ” 中为删除的陷阱接收器配置的所有通知设置都将设置为默认值。

选择 **SNMPv1** 或 **SNMPv3** 单选按钮可指定陷阱类型。对于同时接收*两种*陷阱类型的 NMS，您必须为该 NMS 分别配置两个陷阱接收器，每种陷阱类型一个接收器。

字段	说明
陷阱生成	启用 （默认）或禁用该陷阱接收器的陷阱生成。
Powernet MIB 陷阱生成 / RFC1628	对创建的每个陷阱，在这两个 MIB 陷阱生成类型之中选择。 Powernet 选项是为 Schneider Electric 定制的，包含与公司产品有关的许多附加变量。 RFC1628 是 UPS 设备通用的标准管理信息库 (MIB)。 如果您使用 RFC1628 MIB，也可以使用三个 RFC1628 事件通知 （请参阅 “ 配置事件操作 ”）。它们也可以用于避免在 NMC 环境之外配置通知事件的需要，请参阅 RFC1628 MIB。
NMS IP/ 主机名	该陷阱接收器的 IPv4/ IPv6 地址或主机名。默认为 0.0.0.0，表示陷阱接收器处于未定义状态。
语言	从下拉列表中选择一种语言。选择的语言可以不同于 UI 和其他陷阱接收器。
SNMPv1	团体名称：在将 SNMPv1 陷阱发送至陷阱接收器时用作标识符的名称。 身份验证陷阱：启用该选项时 （默认），通过 “NMS IP/ 主机名 ” 设置定义的 NMS 将接收到身份验证陷阱 （尝试登录该设备无效时产生的陷阱）。
SNMPv3	用户名：为该陷阱接收器的用户配置文件选择标识符。另请参阅 “SNMP 屏幕 ” 下的 “ 用户配置文件 ”。

SNMP 陷阱测试屏幕

路径：配置 > 通知 > SNMP 陷阱 > 测试

上次测试结果：最近的 SNMP 陷阱测试结果。成功的 SNMP 陷阱测试只会验证是否发送了陷阱；并不会验证所选陷阱接收器是否接收到陷阱。如果满足以下所有情况，则陷阱测试成功。

- 该设备已启用为所选陷阱接收器配置的 SNMP 版本 （SNMPv1 或 SNMPv3）。
- 陷阱接收器本身已启用。
- 如果为收件人地址选择了主机名，则该主机名即可映射到有效的 IP 地址。

收件人：选择测试 SNMP 陷阱被发送到的 IP 地址或主机名。如果没有配置陷阱接收器，将显示陷阱接收器配置屏幕的链接。请参阅上文的 “SNMP 陷阱接收器屏幕 ”。

常规菜单

此菜单处理其他配置项目，包括设备标识、日期和时间、导出和导入 NMC 配置选项、屏幕左下方的三个链接以及合并数据以进行故障排除。

标识屏幕

路径：配置 > 常规 > 标识

定义以下项目使用的名称 （NMC 系统名称，请参阅 “DNS 屏幕 ”）、位置 （物理位置）和联系人 （设备负责人）：

- NMC 的 SNMP 代理
- StruxureWare 数据中心专家

“ 名称 ” 字段专门由 NMC 的 SNMP 代理中的 **sysName**、 **sysContact** 和 **sysLocation** 对象标识符 (OID) 使用。有关 MIB-II OID 的更多信息，请参阅 *《PowerNet® SNMP Management Information Base (MIB) 参考指南》*，该指南可在 APC 网站上找到。

日期 / 时间屏幕

模式。

路径：配置 > 常规 > 日期 / 时间 > 模式

设置 NMC 使用的时间和日期。您可以手动更改当前设置，亦或通过网络时间协议 （NTP）服务器更改：

对于两者，您都要选择时区。这是您的本地时间与世界标准时间 (UTC) （也称为格林威治标准时间 [GMT]）的时差。

- 手动模式：执行以下操作之一：
  - 为 NMC 输入日期和时间，或
  - 勾选应用本地计算机时间复选框，读取您正在使用的计算机的日期和时间设置，并将其应用到此处。
- 与 NTP 服务器同步：使用 NTP （网络时间协议）服务器为 NMC 定义日期和时间。

默认情况下， StruxureWare Data Center Expert 专用网络上的任何 NMC 都通过使用 StruxureWare Data Center Expert 作为 NTP 服务器获取其时间设置。

字段	说明
屏蔽手动 NTP 设置	如果您选择此选项，其他来源 （通常是 DHCP）的数据将优先于您此处设置的 NTP 配置。
主 NTP 服务器	输入主 NTP 服务器的 IP 地址或域名。
次 NTP 服务器	在次服务器可用时，输入次 NTP 服务器的 IP 地址或域名。
更新间隔	定义 NMC 访问 NTP 服务器获取更新的频率，按小时计。*最小值*：1；*最大值*：8760 （1 年）。
立即使用 NTP 更新	立即通过 NTP 服务器更新日期和时间。

夏令时。

路径：配置 > 常规 > 日期 / 时间 > 夏令时

夏令时 (DST) 默认为禁用。您可以启用传统的美国 DST，或启用和配置自定义的夏令时，与您所在地区实施的夏令时相匹配。

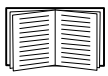
自定义 DST 时，如果到了您在开始下指定的时间和日期，系统将把时钟向前调整一小时；如果到了您在结束下指定的时间和日期，系统将把时钟往回调整一小时。

- 如果您当地的 DST 始终在一个月特定的*第四个*星期几开始或结束 （例如，第四个星期日），则选择**第四个 / 最后一个**。如果该月存在第五个星期日，您仍然应该选择**第四个 / 最后一个**。
- 如果您当地的 DST 始终在一个月特定的*最后一个*星期几开始或结束 （无论是第四个或第五个），则选择**第五个 / 最后一个**。

使用配置文件创建和导入设置

路径：配置 > 常规 > 用户配置文件

通过此选项，您可以重复使用现有的配置设置来简化并加速新设备的配置。使用上载可将配置数据传输到此界面，使用下载可从此界面传输数据 （然后使用文件配置其他界面）。文件的默认名称为 **config.ini**。



若要检索和自定义已配置的 NMC 的文件，请参阅 “ 如何导出配置设置 ”。

配置链接屏幕

路径：配置 > 常规 > 快速链接

使用此选项可查看和更改界面中每个屏幕左下角显示的 URL 链接。

若要重新配置链接，请单击名称栏中的链接名称。您可以通过单击重置为默认值，随时将链接重置为其默认值。

配置菜单上的日志

路径：配置 > 日志 > 系统日志 > *选项*

在发生事件时， NMC 最多可以向四个系统日志服务器发送消息。系统日志服务器在集中记录事件的日志中记录网络设备发生的事件。

该用户指南不对系统日志或其配置值进行详细说明。有关系统日志的详细信息，请参阅 RFC3164。

确定系统日志服务器

路径：配置 > 日志 > 系统日志 > 服务器

字段	说明
系统日志服务器	使用 IPv4/ IPv6 地址或主机名，定义接收 NMC 发送的系统日志消息的一至四个服务器。
端口	NMC 将用于发送系统日志消息的用户数据报协议 (UDP) 端口。默认为 514，即分配给系统日志的 UDP 端口。
语言	选择所有系统日志消息的语言。
协议	在 UDP 和 TCP 之间选择。

系统日志设置

路径：配置 > 日志 > 系统日志 > 设置

字段	说明
消息生成	为已将系统日志配置为通知方法的事件启用系统日志消息生成和日志记录。请参阅“配置事件操作”。
设备代码	选择分配给 NMC 的系统日志消息的设备代码（默认为用户）。 **注：**用户能够最好地定义 NMC 发送的系统日志消息。*请勿*更改该选项，除非系统日志网络或系统管理员建议这样做。
严重程度映射	向可用的系统日志优先级映射 NMC 或环境事件的每个严重程度。本地选项为“严重”、“警告”和“提示”。您应该不需要更改映射。 以下定义来自 RFC3164： • 紧急：系统不可用 • 警报：必须立即采取措施 • 严重：严重情况 • 错误：错误情况 • 警告：警告情况 • 通知：正常但重要的情况 • 提示：供参考的消息 • 调试：调试级消息 本地优先级设置的默认设置如下： • 严重映射为严重 • 警告映射为警告 • 提示映射为信息 **注：**若要禁用系统日志消息，请参阅“配置事件操作”。

系统日志测试和格式示例

路径：日志 > 系统日志 > 测试

将测试消息发送至系统日志服务器 （通过上述 “ 确定系统日志服务器 ” 选项配置）。结果将被发送到所有已配置的系统日志服务器。

选择分配给测试消息的严重程序，然后定义测试消息。消息的格式包含事件类型 （例如， APC、系统或设备），之后加有冒号、空格和事件文本。消息最多包含 50 个字符。

- 优先级 (PRI)：分配给消息事件的系统日志优先级和 NMC 发送的消息的设备代码。
- 标题：时间戳和 NMC 的 IP 地址。
- 消息 (MSG) 部分：
  - TAG （标签）字段，之后加有冒号和空格，定义事件类型。
  - CONTENT （内容）字段是事件文本，之后 （可选）加有空格和事件代码。

  示例：`APC: Test Syslog is valid`。

测试菜单

测试和校准

路径：测试 > UPS

该选项并非适用于所有 UPS 设备。

不支持对锂离子 UPS 设备（包括前缀为 SRTL/SRYLF 的 UPS 设备）运行校准。

对于某些 UPS 设备，您可以对其运行自检、警报测试或运行时间校准。**自检**和**校准**字段将显示最近测试和校准的结果。

运行时间校准会使 UPS 根据其当前负载重新计算可用的运行时间，以此来确保报告的运行时间更准确。由于校准操作会临时消耗 UPS 电池电量，只有电池电量为 100% 时，才可以执行校准。您的 UPS 的负载必须至少为 15% 且无波动，才能确保正常进行校准。

注意 — 运行时间校准会深度释放 UPS 电池电量，如果发生电源故障，会使 UPS 暂时无法支持其连接的负载。

经常校准会缩短电池寿命。

在明显增大 UPS 支持的负载时执行校准。

UPS 的警报测试视设备而定，可能不适用于您的 UPS。要启用警报，请参阅 “UPS 通用屏幕 ”。

- 当您选择 **UPS 警报测试**时， UPS 将发出蜂鸣并持续四秒，且指示灯亮起。
- 当您选择 **UPS 警报测试 - 持续**时， UPS 将发出蜂鸣，且指示灯亮起，直到您取消测试。此屏幕将单独显示一项：**取消持续警报测试**。若要取消测试，请选择此项并单击 “ 应用 ”。或者，您可以按 UPS 的指示灯显示界面上的任意键。此测试有助于查找 UPS。

将 NMC 指示灯设置为闪烁

路径：测试 > 网络 > LED Blink

如果您难以找到您的 UPS 设备，在 **LED Blink 持续时间**字段中输入分钟数并单击 “ 应用 ”， NMC 指示灯就会开始闪烁。这可以帮助您查找物理设备。

日志和关于菜单

使用事件和数据日志

事件日志记录单个事件。而数据日志通过定期记录值，为您提供系统快照。

事件日志

路径：日志 > 事件 > *可用选项*

默认情况下，日志将从最新事件开始，显示最近两天内记录的所有事件。请参阅“ 按事件配置 ”。

此外，日志记录：i) 任何发送 SNMP 陷阱的事件， SNMP 身份验证尝试失败除外。 ii) 异常的内部系统事件。

您可以通过“ 配置 ”菜单上的“ 本地用户 ”启用事件颜色编码。

显示事件日志。

路径：日志 > 事件 > 日志

默认情况下，事件日志首先显示最近的事件。若要查看 Web 页面上一起列出的事件，请单击**在新窗口中显示日志**按钮。要执行此操作，必须在浏览器中启用 JavaScript。

若要在文本文件中打开日志或将日志保存到磁盘，请单击与**事件日志**标题在同一行的软盘图标 。

您还可以使用安全拷贝 (SCP) 或 FTP 查看事件日志。请参阅“ 如何使用 SCP 或 FTP 检索日志文件 ”。

过滤事件日志。使用过滤功能来忽略您不想显示的信息。

按日期或时间过滤日志	使用**最近**或**从**单选按钮。（过滤器配置将会被保存，直到 NMC 重新启动）。
按事件严重程度或类别过滤日志	单击**过滤日志**。清除复选框以将其从视图中删除。单击**应用**后，事件日志页面左上角的文字将指示过滤器处于活动状态。过滤器将一直处于活动状态，直至您将其清除或 NMC 重新启动。若要删除活动的过滤器，请单击**过滤日志**，然后单击**清除过滤器 (全部显示)**。作为管理员，单击**另存为默认值**可将该过滤器另存为所有用户的新默认日志视图。

有关过滤的重要事项：

- 使用 OR 逻辑通过过滤器处理事件。如果您应用了一个过滤器，它将处于工作状态而不会考虑其他过滤器。
- 在**按严重程度过滤**列表中清除的事件决不会显示在过滤的事件日志中，即使您在**按类别过滤**列表中选择了该事件。
- 同样地，在**按类别过滤**列表中清除的事件也决不会显示在过滤的事件日志中。

删除事件日志。若要删除所有事件，请单击**清空日志**。删除的事件不可恢复。

若要根据指派的严重级别或者事件类别禁止记录事件，请参阅“ 按事件组配置 ”。

配置反向查找：

路径：日志 > 事件 > 反向查找

启用反向查找后，在发生与网络有关的事件时，与该事件有关的网络设备的 IP 地址*和*域名都会记录在事件日志中。如果设备没有域名条目，则与事件一起记录的只有 IP 地址。

由于域名的更改频率通常低于 IP 地址，因此启用反向查找可以提高识别导致事件的网络设备的地址的能力。

反向查找默认为禁用。如果您未配置 DNS 服务器，或由于网络流量大而使网络性能不佳，则不需要启用该功能。

调整事件日志大小

路径：日志 > 事件 > 大小

使用事件日志大小可指定日志条目的最大数量。

注意：当您调整事件日志的大小以指定最大数量时，*所有现有的日志条目都将被删除*。为避免丢失日志数据，请首先使用 SCP 或 FTP 检索日志 （参阅 “ 如何使用 SCP 或 FTP 检索日志文件 ”）。当日志随后到达最大数量时，较旧的条目将被删除。

数据日志

路径：日志 > 数据 > *选项*

使用数据日志可显示 UPS 测量值、 UPS 电源输入以及 UPS 和电池的环境温度。

显示数据日志及调整其大小的步骤与事件日志相同，唯一不同之处在于您使用数据而非事件下的菜单选项。请参阅 “ 显示事件日志 ” 和 “ 调整事件日志大小 ”。

若要按日期或时间过滤数据日志，请使用最近或从单选按钮。（过滤器配置将会被保存，直到 NMC 重新启动）。要删除数据日志中记录的所有数据，请单击清空数据日志。删除的数据不可恢复。

设置数据收集间隔 （日志 > 数据 > 间隔）：在日志间隔设置中定义在数据日志中搜索和存储数据的频率。单击 “ 应用 ” 后，将重新计算可能的存储天数，并在屏幕顶部显示。

日志装满后，将删除最旧的条目。若要避免自动删除较旧的数据，请直接参阅下面的 “ 配置数据日志转存 （日志 > 数据 > 转存）： ”。

注：由于间隔指定记录数据的频率，因此*间隔越小*，记录数据的次数越多，日志文件就越大。

配置数据日志转存 （日志 > 数据 > 转存）：转存会使数据日志的内容按名称和位置被附加到您指定的文件上，这意味着您可以在数据被删除前存储数据，请直接参阅后文的 “ 设置数据收集间隔 （日志 > 数据 > 间隔）： ”。

使用此选项可设置密码保护和其他参数。

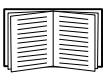
字段	说明
FTP 服务器	文件将驻留的服务器的 IP 地址或主机名。
用户名 **密码**	将数据发送到储存库文件所需的用户名和密码。还必须为该用户配置数据储存库文件和存储该文件的目录 （文件夹）的读写权限。
文件路径	储存库文件的路径。
文件名	储存库文件 （ASCII 文本文件）的名称，例如 `datalog.txt`。 任何新数据都将被附加到此文件，而不会将其覆盖。
唯一文件名	选择该复选框可将日志另存为 `mmddyyyy_<filename>.txt`，其中文件名是您在上面的**文件名**字段中指定的名称。 任何新数据都将被附加到文件，但每天都有其独有的文件。
上载间隔延迟 *n* 小时。	将数据上载到文件之间间隔的小时数 （最大 24 小时）。
失败后每隔 *n* 分钟尝试上载	上载失败后，尝试将数据上载到文件之间间隔的分钟数。
最多 *n* 次	初次失败后，尝试上载的最大次数。
直到上载成功	尝试上载文件，直到传输完成。

如何使用 SCP 或 FTP 检索日志文件

管理员或设备用户可以使用 SCP 或 FTP 检索以制表符分隔的事件日志文件 (*event.txt*) 或者数据日志文件 (*data.txt*)，并将其导入电子数据表中。二者都存在于 NMC 上。

- 该文件将报告自从上次删除日志以来记录的或因达到最大尺寸而被截断的所有事件或数据。
- 该文件包含事件日志或数据日志没有显示的信息。
  - NMC AOS 和应用程序版本
  - 检索文件的日期和时间
  - NMC 的**名称**、**联系人**和**位置**值以及 IP 地址
  - UPS 型号的名称 （仅限 *data.txt* 文件）
  - 记录的每个事件唯一的**事件代码** （仅限 *event.txt* 文件）
  - 对于日志条目， NMC 使用四位数年份。您可能需要在电子数据表应用程序中选择一个四位数日期格式，以显示所有四位数字。

如果您使用基于加密的安全协议，请参阅 “ 使用 SCP 检索文件 ”。如果您使用未加密的身份验证方法来保证安全，请参阅 “ 使用 FTP 检索文件 ”。



有关设置您所需安全类型的可用协议和方法的信息，请参阅 *《安全手册》*，该手册可在 **APC 网站**上找到。

使用 SCP 检索文件。在 NMC 上启用 SSH，请参阅 “ 控制台访问权限 ”。**注：**以下命令仅为示例。

若要检索 *event.txt* 文件，请使用下列命令

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

若要检索 *data.txt* 文件，请使用下列命令

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

使用 FTP 检索文件。若要使用 FTP 检索 *event.txt* 或 *data.txt* 文件：

1. 在命令提示符中，键入 `ftp` 和 NMC IP 地址，并按下 ENTER。

   如果 **FTP 服务器**选项 （请参阅 “FTP 服务器 ”）的**端口**设置已更改，不是其默认值 `21`，您必须在 FTP 命令中使用该非默认值。

   对于 Windows FTP 客户端，请使用下列命令 （包括空格）。（对于某些 FTP 客户端，您必须使用冒号代替 IP 地址和端口号之间的空格）。

   ```
   ftp>open ip_address port_number
   ```

   要设置非默认端口值以加强 FTP 服务器的安全性，请参阅 “FTP 服务器 ”。您可以指定 5001 至 32768 之间的任意端口。

2. 以管理员或设备用户身份登录时，请使用区分大小写的**用户名**和**密码**。对于管理员，默认用户名为 `apc`。对于设备用户，默认用户名为 `device`。
3. 若要将文件传输模式设置为二进制，键入：

   ```
   ftp>bin
   ```

   若要在文件传输期间显示进度条，键入：

   ```
   ftp>hash
   ```

4. 使用 `get` 命令将日志的文本传输到您的本地驱动器。

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

   或

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

5. 您可以使用 `del` 命令，清除每个日志的内容。

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

   或

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

   系统将不会提示您确认删除。

   – 如果您清除了数据日志，事件日志会记录删除日志的事件。
   – 如果您清除了事件日志，新的 *event.txt* 文件将记录事件。

6. 在 `ftp>` 提示符后面键入 `quit`，从 FTP 退出。

UPS 日志

路径：日志 > UPS

此菜单选项并非适用于所有 UPS 设备。

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备的路径为日志 > 电源事件。

此信息来自于 UPS 设备，并且是与 NMC 日志分开的。（它不与 NMC“ 事件日志 ” 直接相关或不是其子集）。

此信息可帮助技术支持团队解决问题。

UPS 转换日志列出 UPS 的转换事件，包括转换至电池和转换为旁路。

UPS 故障日志列出 UPS 的故障事件。

能耗

路径：日志 > 能耗

此菜单选项并非适用于所有 UPS 设备。

您的 UPS 设备的累计能量使用率数据显示在屏幕顶部，每周的故障则显示在屏幕底部的表中。

字段	说明
能耗	UPS 到目前为止消耗的能量，以千瓦时计。例如， UPS 为 350 W 的灯泡供电 1000 小时可消耗 350 kWh 的能量。
总成本	预计到目前为止使用的能量的总成本。例如，一个灯泡 1000 个小时消耗 350 kWh 的能量，而每 kWh 的价格为 0.10 美元，则这段时间的费用即为 35 美元。
CO_2 排放量	预计交流市电公司到目前为止为提供使用的能量而向环境释放的 CO_2 的数量。

成本和 CO_2 排放量根据能量来源和配电网的不同存在很大差异。您可以从**位置**下拉框中选择您所在的国家 / 地区获得粗略的估算值，或使用 “ **（编辑）** ” 链接输入您的成本和排放量数据。

编辑位置会创建一个自定义位置，而不会更改该位置的默认数据。例如，如果您从下拉列表选择 **IE-Ireland**，然后使用编辑来更改数据，那么在下拉列表顶部将创建一个名为 **Custom (IE-Ireland)** 的条目。

防火墙日志

路径：日志 > 防火墙

如果您创建了防火墙策略，则将在此处记录防火墙事件。有关实施策略的更多信息，请参阅 “ 防火墙界面 ”。

此信息可帮助技术支持团队解决问题。

日志条目包含有关流量和规则操作 （允许、放弃）的信息。如果在此处登录，这些事件将不会记录到主事件日志中。请参阅 “ 事件日志 ”。

防火墙日志最多可包含 50 个最近的事件，这些事件在 NMC 重新启动时将被清除。

关于网络管理卡 3

关于 UPS 设备

路径：关于 > UPS

带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备的路径为关于 > UPS > 通用。

UPS 下显示的信息视所用设备而异。

字段	说明
型号 / SKU/ 序列号	这些字段用于识别您的 UPS 设备。
生产日期	您的 UPS 的生产日期。
固件版本	UPS 上目前安装的固件模块的版本号。
固件版本 2	UPS 上目前安装的固件的第二个版本号，在多个处理器需要不同版本号时使用。
额定视在功率	UPS 的 VA 总功率。
额定有功功率	UPS 的总负载能力 （单位：W）。
额定视在功率 / 相	UPS 每个相位的 VA 功率。 从技术层面上来说，它是每个相位当前的视在功率，单位为伏安 (VA)。视在功率是 RMS （均方根）电压和 RMS 安培数的乘积。
额定有功 功率 / 相	UPS 的总负载能力 （单位：W）。 每个相位当前活动的旁路功率，单位为瓦 (W)。有功功率是电压和电流瞬时乘积的平均值。
关于 UPS 监控软件	包含关于软件直接串行监控 UPS 或通过 USB 进行监控的各种信息。
内部电池 SKU/ 外部电池 SKU	这些字段用于识别电池的部件号，在对问题进行故障排除时很有用。

路径：关于 > UPS > 功率

以下选项仅适用于前缀为 SRYLF 并配有嵌入式 NMC 的 UPS 设备。

字段	说明
序列号	功率模块的序列号。
SKU	功率模块的 SKU。
日期	功率模块的制造日期。
版本	功率模块的版本号。

路径：关于 > UPS > 电池

以下选项仅适用于带有嵌入式 NMC 且前缀为 SRTL/SRYLF 的 UPS 设备。

字段	说明
序列号	电池的序列号。
SKU	电池的 SKU。
日期	上次更换电池的日期。
版本	电池的版本号。

单击“主配线架”或“电池配线架 n”进入**主配线架/ 电池配线架 n** 屏幕查看更多电池信息。

路径：关于 > UPS > 智能模块

以下选项仅适用于前缀为 SRYLF 并配有嵌入式 NMC 的 UPS 设备。

字段	说明
序列号	智能模块的序列号。
SKU	智能模块的 SKU。
日期	智能模块的制造日期。
版本	智能模块的版本号。

关于 NMC 和固件模块

路径：关于 > 网络

硬件出厂设置：硬件信息有助于排除 NMC 设备问题，包括型号和序列号、硬件版本、制造日期、 MAC 地址和管理正常运行时间。

管理卡已运行时间指的是此管理卡连续运行的时间长度，即自 NMC 热启动或冷启动后的时间长度。

应用程序模块、 **APC 操作系统 (AOS)** 和 **Boot Monitor**：此信息有助于进行故障排除，以及确定 www.apc.com/shop/us/en/tools/software-firmware 上是否有更新的固件。

字段标记	说明
名称	固件模块的名称。 **应用程序模块**名称视 UPS 设备类型而异，例如 **sumx** 适用于 Smart-UPS 设备，**sy** 适用于 Symmetra 设备。 **“APC 操作系统 (AOS)” 模块**通常命名为 **aos**， **Boot Monitor 模块**通常命名为 boot。
版本	固件模块的版本号。模块的版本号可能有所不同，但兼容的模块会同时发布。切勿将不同版本的应用程序模块和 **AOS modules** 模块结合在一起。 请参阅 “ 升级固件 ”。
日期 / 时间	构建固件模块的日期和时间。

另请参阅 “ 验证所安装固件的版本号 ”。

支持屏幕

路径：关于 > 支持

通过此选项，您可以将此界面中的各种数据合并到单个压缩文件中，以便用于故障排除和客户支持。数据包括事件和数据日志、配置文件 （请参阅 “ 使用配置文件创建和导入设置 ”）和复杂的调试信息。

单击生成日志创建文件，然后单击下载。系统将询问您是否要查看或保存压缩文件。

设备 IP 配置向导

功能、要求和安装

设备 IP 配置向导可发现未分配 IP 地址的网络管理卡 (NMC)。发现后，您即可为这些卡配置 IP 地址设置。

您还可以输入 IP 范围定义搜索，以此搜索已联网的设备。该向导可以扫描定义范围中的 IP 地址并发现已通过 DHCP 分配 IP 地址的卡。

注意：

- 您无法使用IP范围搜索网络上已分配的设备，除非在NMC上启用SNMPv1并将团体名称设为“public”。有关详细信息，请参阅“SNMP 屏幕”。
- 配置完NMC IP地址后，您必须将URL从http更新为https，才能在浏览器中访问NMC Web UI。

有关此向导的详细信息，请参阅 APC 网站上的知识库文章 FA156064。

要使用 DHCP Option 12，请参阅知识库文章 FA156064。

系统要求

该向导在 Microsoft Windows 2000、Windows Server® 2012、Windows Server 2016、Windows Server 2019 以及 32 位和 64 位版本的 Windows 8.1 和 Windows 10 操作系统上均可运行。

该向导支持固件版本为 3.0.x 或更高的管理卡并且仅适用于 IPv4。

安装

要通过下载的可执行文件安装向导：

1. 访问 www.apc.com/shop/tools/software-firmware。
2. 通过软件/固件 > 向导和配置进行筛选。
3. 下载设备 IP 配置向导。
4. 运行下载文件的文件夹中的可执行文件。

安装后，即可通过 Windows 菜单选项找到该向导。

如何导出配置设置

检索和导出 .ini 文件

步骤摘要

管理员可以检索 UPS 网络管理卡 3 (NMC) 的 .ini 文件，并将其导出到其他 NMC 或多个 NMC。以下为操作步骤，有关详细信息请参阅后文。

1. 使用所需设置配置 NMC 并将其导出，请参阅 “ 使用配置文件创建和导入设置 ”。
2. 从该 NMC 检索 .ini 文件。
3. 自定义文件，至少更改 TCP/IP 设置。
4. 使用 NMC 支持的文件传输协议将副本传输到一个或多个其他 NMC。要传输到多个 NMC，请使用 FTP 或 SCP 脚本或 .ini 文件实用程序。

每个接收的 NMC 会使用该文件重新配置自己的设置，然后删除该文件。

.ini 文件的内容

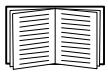
您从 NMC 检索的 config.ini 文件包含以下内容：

- *段落标题*和*关键字*（仅支持您检索文件的特定 UPS/ NMC 设备的段落标题和关键字）：**段落标题**为类别名称，包含在括号 ([ ]) 中。每个段落标题下的**关键字**为描述特定 NMC 设置的标签。每个关键字后面都带有一个等号和一个值 （默认值或者配置的值）。
- 关键字 `Override`：使用默认值时，该关键字会阻止导出一个或多个关键字及其设备特定的值。例如，在 `[NetworkTCP/IP]` 段落中， `Override` 的默认值 （NMC 的 MAC 地址）将阻止导出 `SystemIP`、 `SubnetMask`、 `DefaultGateway`，和 `BootMode` 值。

详细步骤

检索。要设置和检索要导出的 .ini 文件：

1. 如果可以，使用 NMC 界面配置其设置，以便导出。（直接编辑 .ini 文件具有引入错误的风险）。
2. 以下示例显示，如何使用 FTP 从使用命令提示符型客户端的已配置 NMC 中检索 config.ini 文件
   a. 使用 NMC 的 IP 地址打开连接：
      `ftp> ip_address`
   b. 使用管理员用户名和密码登录。
   c. 若要将文件传输模式设置为二进制，键入：
      `ftp> bin`
      若要在文件传输期间显示进度条，键入：
      `ftp> hash`
   d. 检索包含 NMC 设置的 config.ini 文件：
      `ftp> get config .ini`
      文件将被写入您启动 FTP 客户端的文件夹。



若要从多个 NMC 获取配置设置，并将其导出到其它 NMC，请参阅 APC 网站上提供的 *《发行说明：ini 文件实用程序》*。或者，请参阅 http://www.apc.com/support 上的知识库文章 FA156117。

1. 使用文本编辑器自定义文件。
   - 段落标题、关键字和预定义的值不区分大小写，但是您定义的字符串值区分大小写。
   - 使用相邻的引号表示没有值。例如， `LinkURL1=""` 表示故意没有定义 URL。
   - 含有前导或尾随空格或已经包含在引号中的任何值都应包含在引号中。
   - 若要导出排定的事件，请直接在 .ini 文件中配置值。
   - 如果接收的 NMC 可以访问网络时间协议服务器，则请将 `NTPEnable` 配置为 `enabled`，以导出最精确的系统时间：

     ```
     NTPEnable=enabled
     ```

     另外，也可以将 `[SystemDate/Time]` 段落作为单独的 .ini 文件导出，以减少传输时间。
   - 若要添加备注，请使用分号 (;) 作为每行备注的开头。

2. 将自定义的文件复制到相同的文件夹中，并使用其他文件名：
   - 文件名最多 64 个字符，且必须带有 .ini 后缀。
   - 保留原始的自定义文件，以备日后使用。*您保留的文件是您所作备注的唯一记录。*

将文件传输至单个 NMC。若要将 .ini 文件传输到其他网络管理卡，请采用以下任意方法：

- 从接收的 NMC 的用户界面选择**配置** — **常规** — **用户配置文件**。输入文件的完整路径，或使用您的本地 PC 上的**浏览**。
- 使用网络管理卡支持的任何文件传输协议，即 FTP、 FTP 客户端、 SCP 或 TFTP。以下示例使用的是 FTP：
  a. 在包含自定义的 .ini 文件副本的文件夹中，使用 FTP 登录到您要导出 .ini 文件的 NMC：
     ```
     ftp> open ip_address
     ```
  b. 若要将文件传输模式设置为二进制，键入：
     ```
     ftp> bin
     ```
     若要在文件传输期间显示进度条，键入：
     ```
     ftp> hash
     ```
  c. 将自定义的 .ini 文件的副本导出到接收的 NMC 的根目录：
     ```
     ftp> put filename .ini
     ```

将文件传输到多个 NMC。请遵循以下步骤：

- 使用 FTP 或 SCP，但编写一个脚本，包含并重复将文件导出到单个 NMC 使用的步骤。
- 使用批处理文件和 .ini 文件实用程序。

若要创建批处理文件并使用实用程序，请参阅 **APC** 网站上提供的 *《发行说明：ini 文件实用程序》*。或者，请参阅 http://www.apc.com/support 上的知识库文章 FA156117。

上传事件和错误消息

事件及其错误消息

在接收的网络管理卡使用 .ini 文件更新其设置操作完成后，将出现以下事件：

配置文件已上载完毕， *number* 个有效值

如果关键字、段落名称或值无效，接收的 NMC 也会上传成功，但其他事件文本会说明发生的错误。

事件文本	说明
配置文件警告：行 *number* 上的关键字无效。 配置文件警告：行 *number* 上的值无效。	忽略带无效关键字或值的行。
配置文件警告：行 *number* 中的段落无效。	如果段落名称无效，则忽略该段落中的所有关键字 / 值对。
配置文件警告：在行 *number* 的段落以外发现关键字。	忽略在文件开头 （即在任何段落标题之前）输入的关键字。
配置文件警告：配置文件超出最大尺寸。	如果文件太大，上载将无法完成。缩小文件尺寸，或将其分为两个文件，然后再次尝试上载。

config.ini 中的消息

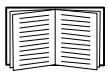
必须成功找到与您下载 config.ini 文件的 NMC 有关的设备，才能包含其配置。如果设备 （例如， UPS） 不存在或者没有找到， config.ini 文件在适当的段落标题下面包含一条消息，而不是关键字和值。例如：

`UPS` 未找到

如果您不打算将设备的配置导出作为 .ini 文件导入的一部分，可以忽略这些消息。

屏蔽值生成的错误

`Override` 关键字及其值阻止导出值时，将在事件日志中生成错误消息。



有关屏蔽值的信息，请参阅 “.ini 文件的内容 ”。

由于屏蔽值为设备特有的，且不适合导出到其他 NMC，因此可忽略这些错误消息。为了防止生成这些错误消息，请删除包含 `Override` 关键字的行和包含被屏蔽的值的行。请勿删除或修改包含段落标题的行。

相关主题

在 Windows 操作系统上，您可以使用 “ 设备 IP 配置向导 ” 更新网络 NMC 的基本 TCP/IP 设置，并通过用户界面配置其他设置，而不是传输 .ini 文件。

请参阅 “ 设备 IP 配置向导 ”。

文件传输

升级固件

升级 UPS 网络管理卡 3 (NMC) 上的固件后，您可获得最新功能、安全性和性能改善以及漏洞修复。请参阅 “ 固件更新屏幕 ”。

此处的升级仅指将 .nmc3 文件放到 NMC 上，就其本身而言并没有安装。定期查看 **www.apc.com/shop/tools/software-firmware** 了解有无任何新的升级。

.nmc3 文件名使用下列格式：

```
apc_hardware-version_type_firmware-version.nmc3
```

- apc：表示上下文。
- hardware-version：hw0n 中的 n 表示您可以使用该文件的硬件版本。
- type：表示模块类型， su 表示 Smart-UPS 设备， sy 则表示 Symmetra 设备。
- version：文件的版本号。

固件文件传输方法

从 **www.apc.com/shop/tools/software-firmware** 获取免费的最新固件版本。若要升级一个或多个 NMC 的固件，请使用以下三种方法之一：

- 在 Windows 操作系统上，使用从 **APC 网站**下载的**固件升级实用程序**。请参阅 “ 使用 NMC 固件升级实用程序 ”。
- 在任何支持的操作系统上，您可以使用 **FTP 或 SCP** 传输 .nmc3 文件。请参阅 “ 使用 FTP 或 SCP 升级一个网络管理卡 ”。
- 对于不在网络上的网络管理卡，使用 **XMODEM**，通过 USB 虚拟通信端口，经由引导加载程序从计算机向 NMC 传输 .nmc3 文件。请参阅 “ 使用 XMODEM 升级一个 NMC”。
- 使用 **USB 驱动器**从你的电脑传输固件文件 （仅限 AP9641 和 AP9643）。请参阅 “ 使用 USB 驱动器传输和更新文件 （仅限 AP9641、 AP9643 和 SRTL/SRYLF 设备） ”。
- 有关升**级多个 NMC** 的方式，请参阅 “ 升级多个网络管理卡上的固件 ” 以及 “ 使用 NMC 固件升级实用程序在 Windows 上进行多项升级 ”。

使用 NMC 固件升级实用程序

此固件升级实用程序是 **APC 网站**上提供的固件升级包的一部分。（切勿使用某种产品专用的升级实用程序升级其他产品的固件）。

使用实用程序在 Windows 系统上进行升级。在任何支持的 Windows 操作系统上， NMC 固件升级实用程序会自动传输 .nmc3 文件。

将下载的固件升级文件解压，并双击 .exe 文件。在对话框字段中输入主机 IP 地址、用户名和密码。您还必须选择 FTP 或 SCP 及其关联端口。

注意：必须在 NMC 设备上启用所选协议，才能完成固件升级。另请参阅 “ 使用 NMC 固件升级实用程序在 Windows 上进行多项升级 ”。

使用 FTP 或 SCP 升级一个网络管理卡

FTP。使用 FTP 通过网络升级 NMC：

- NMC 必须联网，且必须配置其系统 IP、子网掩码和默认网关。
- 必须在 NMC 中启用 FTP 服务器，请参阅 “FTP 服务器 ”。

若要传输文件，请执行以下步骤：

1. 在一台联网的计算机上打开命令提示窗口。转到包含固件文件的目录，并列出文件：

   ```
   C:\>cd apc
   C:\apc>dir
   ```

   有关文件信息，请参阅 “ 关于 NMC 和固件模块 ”。

2. 打开 FTP 客户端会话：

   ```
   C:\apc>ftp
   ```

3. 输入 `open` 和 NMC 的 **IP 地址**，然后按下 ENTER。如果 FTP 服务器的**端口**设置已更改，不是其默认值 **21**，则您必须在 FTP 命令中使用该非默认值。

   - 对于 Windows FTP 客户端，使用空格分隔非默认的端口号和 IP 地址。例如（显示 21000 前的空格）：

     ```
     ftp> open 150.250.6.10 21000
     ```

   - 一些 FTP 客户端则要求在端口号前面使用冒号。

4. 以管理员身份登录。
5. 升级固件。

   ```
   ftp> bin
   ftp> put apc_hw05_aos_nnn.bin （其中 nnn 是固件版本号）
   ```

6. FTP 确认传输后，键入 `quit` 关闭会话。

SCP。若要使用 XMODEM 升级一个未联网的 NMC，则必须通过固件升级实用程序提取固件文件 （请参阅 “ 提取固件文件：”）。

1. 使用 SCP 命令行将 `.nmc3` 文件传输到 NMC。以下示例使用 `v-v-v-v` 代表应用模块的版本号：

   ```
   scp apc_hw21_su_v-v-v-v.nmc3 apc@158.205.6.185:apc_hw21_su_v-v-v-v.nmc3
   ```

注：若要使用 SCP，必须启用 SSH。请参阅 “ 控制台屏幕 ” 以启用 SSH。

使用 XMODEM 升级一个 NMC

若要使用 XMODEM 升级一个未联网的 NMC：

1. 将提供的 micro-USB 线缆 （部件号 960-0603）连接至 NMC 和本地计算机上的 USB 端口。
2. 按下 NMC 上的 “ **重置** ” 按钮。
3. 如果 NMC 在启动时检测到 USB 连接，它将等待 90 秒，以便操作系统有足够的时间识别和配置虚拟通信端口。虚拟通信端口准备就绪后，运行终端程序 （如 HyperTerminal 或 Tera Term）来选择虚拟通信端口。
4. 按 **Enter** 键两次，或等待 Boot Monitor 出现提示：BM>

   注意：如果在重新启动NMC后的90秒内未连接到BootMonitor，NMC将继续其正常启动过程。

5. 键入 XMODEM，然后按下 **Enter**。

6. 在终端程序的菜单上，选择 XMODEM，然后使用 XMODEM 选择要传输的 .nmc3 文件。XMODEM 传输完成后，Boot Monitor 提示符恢复。

   键入 **reset**，或按下**重置**按钮以重新启动 NMC。

注意：需要驱动程序才能通过 Windows 7 连接到 NMC 控制台。驱动程序可从 **APC 网站**上 AP9640/AP9641/AP9643 产品页面下载 “ **软件 / 固件** ” 部分中下载。 Windows 10 不需要驱动程序。

1. 当您通过 micro-USB 线缆连接 NMC 时，会在“其他设备”中发现一个名为“NMC3-CDC”的设备。

2. 右键单击此设备，然后选择“更新驱动程序软件...”

3. 选择“浏览计算机以查找驱动程序软件”选项，然后导航到驱动程序的下载位置 (usb_cdc_ser.inf)。

4. 接受未签名的驱动程序安全消息。

现在，Windows 可以识别 NMC 并为该设备分配 COM 端口。

使用 USB 驱动器传输和更新文件 （仅限 AP9641、 AP9643 和 SRTL/SRYLF 设备）

本功能在引导加载程序 v1.3.3.1 及更高版本可用，在开始传输前，确保 USB 驱动器的文件格式为 FAT、FAT16 或 FAT32。

1. 下载固件升级文件。
2. 在 USB 闪存驱动器上创建一个名为 **apcfirm** 的文件夹。
3. 把 .nmc3 文件放到 **apcfirm** 文件夹。
4. 使用文本编辑器创建一个名为 nmc3.rcf 的文件。（文件扩展名必须为 .rcf， 而不是 .txt 等）。
5. 在 nmc3.rcf 中增加一行用于待升级的固件包，
   例如，升级 Smart-UPS 应用程序 v2.x 版，型号：
   NMC3=apc_hw21_su_2-x.nmc3
6. 将 nmc3.rcf 放到闪存驱动器的 **apcfirm** 文件夹中。
7. 将闪存驱动器插入 NMC 上的 USB 端口，请参阅 “ 前面板 (AP9641)”、“ 前面板 (AP9643)” 和 “SRTL UPS 设备 （SRTL5KRM2UI、 SRTL5KRM2UT、 SRTL5KRM2UJ）的后面板 ”。
8. 重启网络管理卡并等待重启全部完成。
9. 使用 “ 验证升级 ” 中的步骤检查升级是否已成功完成。

升级多个网络管理卡上的固件

使用以下两种方法之一：

- **Windows 上的 NMC 固件升级实用程序**。请参阅 “ 使用 NMC 固件升级实用程序在 Windows 上进行多个升级 ”。
- **使用 FTP 或 SCP**。若要使用 FTP 客户端或 SCP 升级多个 NMC，则编写一个自动执行该步骤的脚本。
- **导出配置设置**。您可以创建批处理文件和使用实用程序从多个 NMC 获取配置设置，并将它们导出到其他 NMC。

请参阅知识库中的 *《发行说明：ini 文件实用程序》*，该文档可在 **http://www.apc.com/site/support/** 上找到。

使用 NMC 固件升级实用程序在 Windows 上进行多个升级。从 APC 网站的 NMC 下载页面下载升级实用程序后，双击 .exe 文件并解压缩内容。：

1. 使用实用程序在目录中查找 `devices.txt` 文件。使用文本编辑器打开并修改此文件，以便为要升级的每个 NMC 设备输入必要信息：
   - [Device]：如需升级每个 NMC，则必须包含此部分标头。
   - Host：设备的 IPv4 地址。
   - Protocol：SCP 或 FTP。
   - Port：SCP 或 FTP 的关联端口。
   - Username：NMC 上启用的管理员用户名。
   - Password：NMC 上启用的管理员密码。

   从 device.txt 中删除所有注释和分号，然后保存更改。

   例如：

```
[Device]
Host=192.168.0.1
Protocol=SCP
Port=22
Username=apc
Password=apc


[Device]
Host=192.168.0.2
Protocol=SCP
Port=22
Username=apc
Password=apc
```

   如果 `devices.txt` 已存在，则您可使用该现有文件。
2. 打开固件升级实用程序。如果 `device.txt` 文件提供了正确的详细信息，则实用程序中将显示以下消息：

   检测到设备列表并已将其导入，因此下方事件窗口中列出的主机将用作活动主机。
3. 单击实用程序中的“开始更新”，以启动固件版本升级。

验证升级

最后的传输结果代码

可能的传输错误包括未找到 TFTP 或 FTP 服务器，或服务器拒绝访问、未找到服务器或未识别传输文件，或传输文件受损。

验证所安装固件的版本号

路径：关于 — 网络

使用 Web UI 验证已升级的固件模块的版本号。您也可以使用 SNMP GET 获取 MIB II **sysDescr** OID。在命令行界面，使用 **about** 命令。

更改 UI 语言

您可以通过从登录屏幕的语言下拉框中选择一种语言，以不同语言显示 NMC 用户界面 (UI)。

UI 包含九种可用的语言：法语、意大利语、德语、西班牙语、巴西葡萄牙语、俄语、韩语、日语和简体中文。

疑难解答

网络管理卡访问问题

有关常见问题的逐步疑难解答和实用解决方案，请访问 www.apc.com/support 上的知识库。若要联系客户支持，请参阅 “Schneider Electric 全球客户支持 ”。

问题	解决方案
无法 ping NMC	如果 NMC 的状态指示灯为绿色，尝试 ping 与 NMC 处于相同网段的其它节点。如果失败，则表明 NMC 没有问题。如果状态指示灯不是绿色，或 ping 测试成功，则执行以下检查： • 验证 NMC 是否适当安装在 UPS 中。 • 验证所有网络连接。 • 验证 NMC 和 NMS 的 IP 地址。 • 如果 NMS 与 NMC 在不同的物理网络 （或子网）上，则验证默认网关 （或路由器）的 IP 地址。 • 验证 NMC 子网掩码的子网位数。
无法通过终端程序分配通信端口	您必须先关闭使用通信端口的所有应用程序、服务或程序，才能使用终端程序配置 NMC。
无法通过串行连接访问命令行界面	确认您没有更改波特率。尝试 2400、9600、19200 或 38400。
无法远程访问命令行界面	• 确保您使用了正确的访问方法：Telnet 或安全外壳协议 (SSH)。管理员可以启用这些访问方法。默认情况下，Telnet 为禁用状态，SSH 为启用状态。可以单独启用 / 禁用 SSH 和 Telnet。 • 对于 SSH， NMC 可能会创建主机密钥。 NMC 最多需要一分钟的时间创建主机密钥，在这段时间内，将无法访问 SSH。
无法访问 用户界面 (UI)	• 验证是否已启用 HTTP 或 HTTPS 访问。 • 确认您指定了正确的 URL，该 URL 应与 NMC 使用的安全系统一致。SSL 要求 URL 以 https 而非 http 开头。 • 验证您可以 ping NMC。 • 验证您使用的 Web 浏览器支持 NMC。请参阅 “Schneider Electric 全球客户支持 ”。 • 如果 NMC 刚刚重新启动，并且正在建立 SSL 安全性，则 NMC 可能会生成一份服务器证书。 NMC 最多需要一分钟的时间创建该证书，在这段时间内， SSL 服务器不可用。

SNMP 问题

问题	解决方案
无法执行 GET	• 检查只读 (GET) 团体名称 (SNMPv1)，或用户配置文件配置 (SNMPv3)。 • 使用命令行界面或 UI 确保 NMS 具有访问权限。请参阅 “SNMP 屏幕 ”。
无法执行 SET	• 验证是否已启用 SNMP。默认情况下， SNMPv1 和 SNMPv3 为禁用状态。 • 验证读取 / 写入 (SET) 团体名称 (SNMPv1) 或用户配置文件配置 (SNMPv3)。 • 使用命令行界面或 UI 确保 NMS 具有写入 (SET) 访问权限 (SNMPv1)，或通过访问权限控制列表 (SNMPv3) 将访问权限授予目标 IP 地址。请参阅 “SNMP 屏幕 ”。

问题	解决方案
无法在 NMS 接收陷阱	• 确保为作为陷阱接收器的 NMS 正确配置了陷阱类型 （SNMPv1 或 SNMPv3）。 • 对于 SNMP v1，查询 **mconfigTrapReceiverTable** MIB OID，以确认正确列出了 NMS IP 地址，并且为该 NMS 定义的团体名称与表格中的团体名称相匹配。如果其中有一个不正确，请使用 SET 纠正 **mconfigTrapReceiverTable** OID，或使用命令行界面或 UI 纠正陷阱接收器的定义。 • 对于 SNMPv3，检查 NMS 的用户配置文件配置，并运行陷阱测试。 请参阅 “SNMP 屏幕 ”、 “ 陷阱接收器 ” 和 “ 常规菜单 ”。
无法识别 NMS 接收到的陷阱	请参阅您的 NMS 文档，以确认陷阱正确集成在警报 / 陷阱数据库中。

Modbus 问题

有关 AP9641 和 AP9643 卡的 Modbus 布线和串行配置的更多信息，请参阅网络管理卡*实用程序*光盘和 APC 网站上的 *《Modbus 文档附录》*。有关 Modbus 寄存器和位数说明的详细信息，请参阅 **APC 网站**上提供的 *《Modbus 寄存器映射》*。

APC USB Wi-Fi 硬件保护装置 (AP9834) 问题

问题	解决方案
无法连接到 wi-fi 网络	• 验证 APC USB Wi-Fi 设备是否正确插入 AP9641/AP9643 卡的 USB 端口。 • 验证 NMC Web UI 或 CLI 中是否提供了正确的 Wi-Fi 设置。 • 验证 NMC 的事件日志中没有与 Wi-Fi 相关的事件。如果 wifi 设置输入不正确或留空，NMC 会向事件日志记录一个错误。例如：“USB Wi-Fi 设备错误。Wi-Fi 设置”。 如果问题仍然存在，请联系网络管理员诊断连接问题。
无法解决设备指示灯的红色长亮状态	• 验证 NMC Web UI 或 CLI 中是否提供了正确的 Wi-Fi 设置。 • 解决 NMC 事件日志中任何与 wi-fi 相关的事件。例如：“USB Wi-Fi 设备错误。Wi-Fi 设置”。 • 通过其他方法重新启用有线连接并配置 Wi-Fi 设置： – Web UI (**配置 > 网络 > Wi-Fi**) – 命令行界面（wifi 命令） – config.ini 文件（NetworkWiFi 部分） 如果有线连接不再可用，请将 micro-USB 线缆 (960-0603) 连接到 NMC 的控制台端口以访问 CLI，并使用 xferINI 命令传输 config.ini 文件。有关详细信息，请参阅《NMC 3CLI 指南》。 如果问题仍然存在，请联系客户支持部门。请参阅“APC 全球客户支持”。

指示灯说明

状态	说明
熄灭	存在以下情况之一： • 设备未插入 AP9641/AP9643 NMC 上的 USB 端口。 • NMC 的固件不支持 Wi-Fi。固件版本 1.4 及更高版本提供 Wi-Fi 支持。请参阅第 81 页的“文件传输”。 • 设备运行不正常。可能需要进行修理或更换。请联系客户支持部门。请参阅“APC 全球客户支持”。
绿色长亮	设备已连接到接入点，但没有网络活动。
绿色闪烁	设备已连接到接入点，并且 Wi-Fi 网络处于活动状态。
红色长亮	存在以下情况之一： • 设备存在永久性错误。 • NMC Wi-Fi 设置存在永久性错误。 • 连接到接入点时出现无法解决的问题。
红色闪烁	设备正在与接入点建立 Wi-Fi 连接。

两年担保

本担保仅适用于购买后遵照手册进行使用的产品。

担保条款

APC 保证，自购买之日起两年内，其产品不会出现材料和工艺方面的问题。 APC 将对本担保范围内的故障产品提供修理或更换服务。本担保不适用于因偶然、疏忽或误用而损坏或以任何方式更改或改装过的设备。故障产品或部件的修理或更换并不会延长原担保期。根据本担保提供的任何部件可能是全新的，也可能是工厂翻新品。

不可转让担保

本担保只适用于正确进行过产品注册的原始购买者。产品可通过 APC 网站 www.apc.com 注册。

免责条款

若经 APC 测试和检测发现，购买者所声称的缺陷根本不存在或由购买者或任何第三方误用、疏忽、安装或测试不当引起，则 APC 不给予担保服务。如属下列情况， APC 亦不提供担保服务：未经授权擅自修理或改装、错误或不当的电压或连接、现场操作条件不当、腐蚀性环境、修理、安装、暴露于自然环境、天灾、火灾、失窃，或不依照 APC 建议或规范安装，或更改、涂污、去除 APC 序列号，或进行其他超出使用范围的操作。

对于根据本协议及其相关条款销售、维修或提供的产品， APC 不提供任何明示或暗示的基于法律或其他形式的担保。对于本产品用于特殊目的的适销性、满意度和适用性， APC 不提供任何形式的暗示的担保。 APC 提供与产品相关的技术或其他建议或服务并不会扩充、缩减或影响 APC 的明示担保，亦不会由此产生任何责任或义务。上述担保和补救措施具有排他性，并取代所有其他担保和补救措施。如果 APC 违反上述担保规定，则上述担保为 APC 的唯一责任，同时也是购买者的唯一救济。 APC 提供的担保仅授予本产品购买者，任何第三方不得享受本担保。

APC 及其高管、董事、子公司或员工不对使用、修理或安装产品过程中发生的任何间接的、特殊的、衍生性或惩罚性的损害赔偿负责，不论此类损害赔偿是来自于合同或民事侵权，不论是属于过错、疏忽或严格责任，或者 APC 是否已预先被告知损害的可能性。特别地， APC 对任何费用不承担责任，例如损失利润和收入、设备损坏、无法使用设备、软件损坏、丢失数据、替代物的成本、第三方索赔或其他方面的费用。

APC 的任何销售人员、员工或代理商无权对本担保进行任何增补或修改。如必要，仅可由 APC 高管和法律部门以书面形式签署对本担保条款的修改。

担保索赔

提出担保索赔的客户可以通过 APC 网站的支持页面 (www.apc.com/support) 访问 APC 客户支持网络。请从网页顶部的国家 / 地区选项下拉菜单中选择您所在的国家 / 地区。选择 “Support” （支持）选项卡以获取您所在地区的客户支持联系信息。

版权声明

Cryptlib Cryptology Library

Cryptlib 版权所有 © Digital Data Security New Zealand Ltd 1998。

Berkeley Database

版权所有 © 1991, 1993 The Regents of the University of California。保留所有权利。

如果满足下列条件，则不论是否已修改，都允许以源代码和二进制形式再分发和使用：

1. 源代码的再分发必须保留以上版权声明、此条件列表和以下免责声明。
2. 若以二进制形式再分发，必须在分发时提供的文档和/或其他材料中复制以上版权声明、此条件列表和以下免责声明。
3. 所有提及本软件功能或用途的广告材料必须显示以下确认声明：本产品包含由加州大学伯克利分校 (University of California, Berkeley) 及其贡献者开发的软件。
4. 未经事先书面许可，在本软件基础上开发的产品不得擅用大学名称或其贡献者名称作宣传或促销。

董事会和贡献者“按原样”提供本软件，并特此否认任何明示或暗示的保证，包括但不限于有关适销性和特定用途适用性的暗示保证。在任何情况下，董事会或贡献者对由于使用本软件而造成的任何直接、间接、偶然、特殊、惩罚性或后果性的损失（包括但不限于获得替代商品或服务、无法使用、数据丢失、利润损失或业务中断）不承担任何责任，无论由于什么原因、根据何种责任理由；也无论是否属于合同、严格责任或民事侵权范畴（因疏忽或其他原因），即使事先已被告知可能会造成这种损失，概不例外。

Lua

版权所有 © 1994–2021 Lua.org, PUC-Rio

特此免费许可任何获得本软件和相关文档文件（“软件”）副本的人士可以不受限制地处理软件，包括但不限于使用、复制、修改、合并、发布、分发、再许可和/或出售软件副本，并许可获得软件的人士享有上述同等权利，但须遵守以下条件：

所有软件副本或实质部分应纳入上述版权声明和以下许可声明。

本软件“按原样”提供，不含任何形式的明示或暗示保证，包括但不限于有关适销性、特定用途适用性和非侵权的保证。在任何情况下，作者或版权所有者对索赔、损害赔偿或其他责任概不负责，无论是否属于合同行为、侵权行为或其他行为，也无论是否由软件或软件使用或其他交易引起或与之相关。

射频干扰

未经责任方明确许可，用户不得对此单元进行更换和维修，否则将失去运行此设备的授权。

美国 — FCC

此设备经测试证明符合 FCC 规则第 15 部分中关于 A 类数字设备的限制规定。这些限制旨在为商业环境中运行的设备提供合理的保护，使之免受有害干扰。此设备会产生、使用并辐射射频能量，如果不按照本用户手册中的说明进行安装和使用，可能会对无线电通信产生有害干扰。在居民区操作此设备可能会导致不良的干扰。用户将独自承担排除此类干扰的责任。

加拿大 — ICES

此 A 类数字设备符合加拿大 ICES-003。

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

日本 — VCCI

这是基于日本非官方信息技术设备干扰控制委员会 (VCCI) 标准的 A 类产品。 在居住环境中，此产品可能会造成射电干扰，在这种情况下，可能需要用户采取适当的纠正措施。

この装置は、情報処理装置等電波障害自主規制協議会 （VCCI）の基準に基づくクラス A 情報技術装置です。この装置を家庭環境で使用すると、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に要求されることがあります

台湾 - BSMI

警告使用者：
這是甲類的資訊產品，在居住的
環境中使用時，可能會造成射頻
干擾，在這種情況下，使用者會
被要求採取某些適當的對策。

澳大利亚和新西兰

注意：本产品是 A 类产品。在居住环境中，此产品可能会造成射电干扰，在这种情况下，可能需要用户采取适当的措施。

欧盟

本产品符合欧盟理事会 2004/108/EC 指令的保护要求，该规范近似于各成员国有关电磁兼容性的法规。 对未经许可擅自改装产品而导致无法遵守保护要求的行为， APC 不承担相关责任。

本产品经过测试，符合 CISPR 22/ 欧洲标准 EN 55022 有关 A 类信息技术设备 (Class A Information Technology Equipment) 的限制。 A 类设备的限制旨在为商业与工业环境中获准运行的通信设备提供合理的保护，使之免受干扰。

注意：本产品是 A 类产品。 在居住环境中，此产品可能会造成射电干扰，在这种情况下，可能需要用户采取适当的措施。

韩国 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 .

Schneider Electric 全球客户支持

您可以通过以下任意方式免费获得本产品或其他任何产品的客户支持服务：

- 访问 Schneider Electric 网站，以查阅 Schneider Electric 知识库中的文档，以及提交客户支持请求。
  - **www.apc.com** （公司总部）
    连接到特定国家或地区的本地化 Schneider Electric 网站，每个站点均会提供客户支持信息。
  - **www.apc.com/support/**
    通过搜索 Schneider Electric 知识库和使用 e-support 获取全球支持。
- 通过电话或电子邮件联系 Schneider Electric 客户支持中心。
  - 国家 / 地区专属的当地支持中心：有关联系信息，请访问 **www.apc.com/support/contact**。

有关如何获取当地客户支持的信息，请与客户支持代表或其他向您出售产品的经销商联系。

990-91148G-037

2022 年 11 月