

EcoStruxure Automation Device Maintenance

固件升级工具

在线帮助

EIO0000004050.04
2022 年 11 月

法律声明

施耐德电气品牌以及本指南中涉及的施耐德电气及其附属公司的任何商标均是施耐德电气或其附属公司的财产。所有其他品牌均为其各自所有者的商标。本指南及其内容受适用版权法保护，并且仅供参考使用。未经施耐德电气事先书面许可，不得出于任何目的，以任何形式或方式（电子、机械、影印、录制或其他方式）复制或传播本指南的任何部分。

对于将本指南或其内容用作商业用途的行为，施耐德电气未授予任何权利或许可，但以“原样”为基础进行咨询的非独占个人许可除外。

施耐德电气的产品和设备应由合格人员进行安装、操作、保养和维护。

由于标准、规格和设计会不时更改，因此本指南中包含的信息可能会随时更改，恕不另行通知。

在适用法律允许的范围内，对于本资料信息内容中的任何错误或遗漏，或因使用此处包含的信息而导致或产生的后果，施耐德电气及其附属公司不会承担任何责任或义务。

作为负责任、具有包容性的企业中的一员，我们将更新包含非包容性术语的内容。然而，在我们完成更新流程之前，我们的内容可能仍然包含客户认为不恰当的标准化行业术语。

© 2022 – Schneider Electric.保留所有权利。

目录

安全信息	5
人员资质	5
正确用途	6
开始之前	6
启动与测试	6
操作与调节	7
安全注意事项	7
关于本书	9
简介	13
概述	13
系统要求	14
安装	15
快速入门	16
欢迎屏幕	16
EcoStruxure Automation Device Maintenance 用户界面	18
数据包	18
设备/加载	19
添加设备	21
配置设置	23
错误和警告窗口	24
创建新 EcoStruxure Automation Device Maintenance 项目	25
保存项目	26
打开项目	27
配置 EcoStruxure Automation Device Maintenance 工具	30
配置设备发现模式	30
配置 Modbus TCP 扫描器	32
配置 DPWS 扫描器	34
配置通讯设置	35
配置包位置	35
查看日志文件	36
配置语言	38
复位应用程序设置	38
配置安全功能	39
安全功能	39
管理证书	41
管理公钥基础设施 (PKI)	46
激活 Syslog 消息记录	47
数据包	49
“数据包”选项卡	49
设备/加载	53
设备/加载 选项卡	53
对设备列表中的设备分组	54
删除设备	55
管理用户凭据	57
访问扩展模块	59
监视设备发现状态	61

- 查看/确认消息62
- 查看日志63
- 更新中心**63
- 更新固件64
- 更新安全配置文件.....66
- 网络安全68
 - 什么是网络安全？68
 - Schneider Electric 指南70
 - 数字签名验证72
 - 需要手动卸载的文件72
 - EcoStruxure Automation Device Maintenance 使用的组件73
- 术语75
- 索引77

安全信息

重要信息

在试图安装、操作、维修或维护设备之前，请仔细阅读下述说明并通过查看来熟悉设备。下述特定信息可能会在本文其他地方或设备上出现，提示用户潜在的危险，或者提醒注意有关阐明或简化某一过程的信息。



在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。



这是提醒注意安全的符号。提醒用户可能存在人身伤害的危险。请遵守所有带此符号的安全注意事项，以避免可能的人身伤害甚至死亡。

⚠ 危险

危险表示若不加以避免,将会导致严重人身伤害甚至死亡的危险情况。

⚠ 警告

警告表示若不加以避免,可能会导致严重人身伤害甚至死亡的危险情况。

⚠ 小心

小心表示若不加以避免,可能会导致轻微或中度人身伤害的危险情况。

注意

注意用于表示与人身伤害无关的危害。

请注意

电气设备的安装、操作、维修和维护工作仅限于有资质的人员执行。施耐德电气不承担由于使用本资料所引起的任何后果。

有资质的人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

人员资质

具备资质的人员是指具有以下资质的人员：

- 拥有与电气设备和系统的构造和操作相关的技能和知识。
- 工业控制编程方面的知识和经验。
- 接受过安全相关培训，能够识别并避免相关风险。

具备资质的人员必须能够发现因设置参数和修改参数值所引起的、通常来自机械、电气或电子设备的可能危险。具备资质的人员必须熟悉旨在预防工业事故的各种标准、条例和规定，并且在设计和建造系统时必须加以遵守。

正确用途

此产品是结合控制系统和长定子电机段使用的库，仅用于本文档中描述的工业领域用途。

总是遵守适用的安全相关说明、指定条件和技术数据。

在使用本产品前，针对具体的用途执行风险评估。根据评估结果采取保护措施。

本产品是整个系统的组成部分，因此必须按照整个系统的设计（比如，机器设计）确保工作人员的安全。

不可用于任何其他用途，否则可能有危险。

开始之前

不得将本产品在没有有效作业点防护的机器上使用。如果机器上缺少有效的作业点防护，则有可能导致机器的操作人员严重受伤。

▲警告

未加以防护的设备

- 不得将此软件及相关自动化设备用在不具有作业点防护的设备上。
- 在操作期间，不得将手放入机器。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

此自动化设备及相关软件用于控制多种工业过程。根据所需控制功能、所需防护级别、生产方法、异常情况、政府法规等因素的不同，适用于各种应用的自动化设备的类型或型号会有所差异。在某些应用情况下，如果需要后备冗余，则可能需要一个以上的处理器。

只有用户、机器制造商或系统集成商才能清楚知道机器在安装、运行及维护过程中可能出现的各种情况和因素，因此，也只有他们才能确定可以正确使用的自动化设备和相关安全装置及互锁设备。在为特定应用选择自动化和控制设备以及相关软件时，您应参考适用的当地和国家标准及法规。National Safety Council's Accident Prevention Manual（美国全国公认）同样提供有非常有用的信息。

对于包装机等一些应用而言，必须提供作业点防护等额外的操作人员防护。如果操作人员的手部及其他身体部位能够自由进入夹点或其他危险区域内，并且可导致人员严重受伤，则必须提供这种防护。仅凭软件产品自身无法防止操作人员受伤。因此，软件无法被取代，也无法取代作业点防护。

在使用设备之前，确保与作业点防护相关的适当安全设备与机械/电气联锁装置已经安装并且运行。与作业点防护相关的所有联锁装置与安全设备必须与相关自动化设备及软件程序配合使用。

注: 关于协调用于作业点防护的安全设备与机械/电气联锁装置的内容不在本文档中功能块库、系统用户指南或者其他实施的范围之内。

启动与测试

安装之后，在使用电气控制与自动化设备进行常规操作之前，应当由合格的工作人员对系统进行一次启动测试，以验证设备正确运行。安排这种检测非常重要，而且应该提供足够长的时间来执行彻底并且令人满意的测试。

▲警告

设备操作危险

- 验证已经完成所有安装与设置步骤。
- 在执行运行测试之前，将所有元器件上用于运送的挡块或其他临时性支撑物拆下。
- 从设备上拆下工具、仪表以及去除碎片。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

执行设备文档中所建议的所有启动测试。保存所有设备文档以供日后参考使用。

必须同时在仿真与真实的网络境中进行软件测试。

按照地方法规（例如：依照美国 National Electrical Code ）验证所完成的系统无任何短路且未安装任何临时接地线。如果必须进行高电位电压测试，请遵循设备文档中的建议，防止设备意外损坏。

在对设备通电之前：

- 从设备上拆下工具、仪表以及去除碎片。
- 关闭设备柜门。
- 从输入电源线中拆除所有的临时接地线。
- 执行制造商建议的所有启动测试。

操作与调节

下列预防措施来自于 NEMA Standards Publication ICS 7.1-1995（以英文版本为准）：

- 无论在设计与制造设备或者在选择与评估部件时有多谨慎，如果对此类设备造作不当，将会导致危险出现。
- 有时会因为对设备调节不当而导致设备运行不令人满意或不安全。在进行功能调节时，始终以制造商的说明书为向导。进行此类调节的工作人员应当熟悉设备制造商的说明书以及与电气设备一同使用的机器。
- 操作人员应当只能进行操作人员实际所需的运行调整。应当限制访问其他控件，以免对运行特性进行擅自更改。

安全注意事项

在此软件的安装或使用期间，请注意软件中出现的以及本文档中所包含的安全消息。以下安全消息全部适用于此软件。

▲警告

设备失控风险

- 不要将此软件用于人身或设备安全依赖于控制操作的关键控制或保护应用场合。
- 不要将此软件用于控制注重时效的功能。在控制发起与操作实施之间可能发生通讯延迟。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

⚠ 警告

数据结果不准确的风险

- 正确配置此软件以便获得准确的报告和/或数据结果。
- 不得将维护或维修操作仅依赖于软件所显示的消息和信息。
- 不得仅依赖于软件消息和报告来判定系统是否在正确工作或者是否满足相应标准和要求。
- 考虑导致通讯链路意外传输延迟或故障的隐含因素。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

⚠ 警告

系统可用性、完整性和保密性的潜在危害

遵守网络安全最佳做法。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

注: 有关网络安全的详细信息，请参阅章节 [网络安全](#), 68 页。

关于本书

文档范围

本文档介绍 EcoStruxure Automation Device Maintenance 工具。EcoStruxure Automation Device Maintenance 能够将固件从 PC 传输到支持的 Schneider Electric 设备。此工具支持发现网络中的相关设备，并且还用于在无法执行设备发现时，手动识别这样的设备。

有效性说明

本文档已针对 EcoStruxure Automation Device Maintenance 3.1 进行了更新。

在本文档中以及在下面的“相关的文件”一节所提及的文档中介绍的特性可在线访问。如要在线访问信息，请访问 Schneider Electric 主页 www.se.com/ww/en/download/。对于 EcoStruxure Automation Device Maintenance 文档，请在搜索文本框中输入 *EcoStruxure Automation Device Maintenance*，然后按 **Enter** 键。

本文档中介绍的特性应该与网上显示的那些特性相同。依据我们的持续改进政策，我们将不断修订内容，使其更加清楚了，更加准确。如果您发现文档和在线信息之间存在差异，请以在线信息为准。

相关的文件

文件名称	参考编号
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Modicon 控制器平台网络安全，参考手册	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Modbus 规范和实施指南，参考手册	Modbus Application Protocol Specification
Web 服务设备配置文件，参考手册	WSDD-DPWS
EcoStruxure™ Control Expert 运行模式	33003101 (English) 33003102 (French) 33003103 (German) 33003104 (Spanish) 33003696 (Italian) 33003697 (Chinese)
EcoStruxure Automation Device Maintenance Altivar 用户手册	JYT50472 (English) JYT50474 (French) JYT50482 (German) JYT50476 (Spanish) JYT50478 (Italian) JYT50483 (Chinese) JYT50484 (Turkish) JYT50485 (Portuguese)

产品相关信息

<div>▲警告</div> <div><div>失去控制</div><div><ul style="list-style-type: none">设计师在设计任何控制方案时，都必须考虑控制路径的潜在失效模式，对于某些关键控制功能，应提供相应措施，以在路径失效期间和之后恢复安全状态。关键控制功能的示例有紧急停止、超程停止、断电和重启。为关键控制功能提供单独或冗余的控制路径。系统控制路径可包括通讯链路。必须对暗含的无法预料的传输延迟或链接失效问题加以考虑。遵守所有事故预防规定和当地的安全指南。¹为了保证正确运行，在投入使用前，必须对设备的每次执行情况分别进行全面测试。</div><div>未按说明操作可能导致人身伤亡或设备损坏等严重后果。</div></div>
<div><div>¹ 有关详细信息，请参阅 NEMA ICS 1.1（最新版）中的“安全指导原则 - 固态控制器的应用、安装和维护”以及 NEMA ICS 7.1（最新版）中的“结构安全标准及可调速驱动系统的选择、安装与操作指南”或您特定地区的类似规定。</div><div>在试图使用库中常见的 POU 为特定应用提供解决方案（机器或工艺）前，必须考虑、执行和完成最佳行为准则。这些行为准则包括但不限于与此库相关的风险分析、功能安全、组件兼容性、测试和系统验证。</div></div>
<div>▲警告</div> <div><div>程序组织单元使用不当</div><div><ul style="list-style-type: none">针对用途和安装的设备执行安全相关分析。确保程序组织单元 (POU) 兼容系统中的设备，不会对系统的正常功能产生意外影响。使用正确的参数特别是限值，并遵守机器磨损和停止行为。验证传感器和执行器与选定的 POU 兼容。在验证和试运行期间，充分测试所有功能在所有操作模式下的工作情况。根据安全相关分析、相关规则以及法律法规为关键控制功能（急停、值超限条件等）提供独立方法。</div><div>未按说明操作可能导致人身伤亡或设备损坏等严重后果。</div></div>
<div>▲警告</div> <div><div>意外的设备操作</div><div><ul style="list-style-type: none">本设备只能搭配经 Schneider Electric 认可的软件。每次更改物理硬件配置时，应更新应用程序。</div><div>未按说明操作可能导致人身伤亡或设备损坏等严重后果。</div></div>

数据文件、应用程序文件和/或固件文件等的不完全传输可对机器或控制器造成严重后果。如果在传输文件过程中断开电源，或者出现断电或通讯中断，则机器可能无法正常工作，或应用程序可能尝试运行数据损坏的文件。如果出现通讯中断，请再次尝试传输。一定要在您的风险分析中包括数据损坏文件的影响。

▲警告

意外的设备操作、数据损失或文件损坏

- 切勿中断正在进行的数据传输。
- 如传输因任何原因中断，则重新初始化传输。
- 除非您已在风险分析中考虑了文件损坏并且已采取相应措施来防止出现因文件传输不成功造成的任何潜在严重后果，否则，切勿在文件传输成功完成之前将机器投入运行。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

将此库用于机器控制时必须慎重，必须采取预防措施，避免指示的机器操作、状态改变或者数据存储或机器操作元素更改造成意外后果。

▲警告

意外的设备操作

- 将控制系统的操作设备安置在机器旁边或者安置在让您能够看到整台机器的地方。
- 保护操作命令，以防非法访问。
- 如果远程控制是应用程序必需的设计方面，请确保在从远程位置进行操作时，本地有胜任且具有相应资格的观察者在场。
- 为应用程序配置和安装运行/停止输入（如配备）或其他外部手段，以便在向它发送远程命令时，也能对装置的启动或停止保持本地控制。

未按说明操作可能导致人身伤亡或设备损坏等严重后果。

摘自标准的术语

本手册中的或者出现在产品自身中/上的技术术语、术语、符号和相应描述基本上均源自国际标准的条款或定义。

在功能安全系统、驱动器和一般自动化领域，这可能包括但不限于安全、安全功能、安全状态、故障、故障复位、失灵、失效、错误、错误消息、危险等词语。

这些标准包括：

标准	描述
IEC 61131-2:2007	编程控制器，第 2 部分：设备要求和测试。
ISO 13849-1:2015	机器安全：控制系统的安全相关部分。 设计通则。
EN 61496-1:2013	机械安全：电子感应式防护设备。 第 1 部分：一般要求和测试。
ISO 12100:2010	机械安全 - 设计的一般原则 - 风险评估和风险抑制
EN 60204-1:2006	机械安全 - 电气机械设备 - 第 1 部分：一般要求
ISO 14119:2013	机械安全 - 与防护设备关联的联锁设备 - 设计和选择原则
ISO 13850:2015	机械安全 - 紧急停止 - 设计原则
IEC 62061:2015	机械安全 - 安全相关的电气、电子和可编程电子控制系统的功能性安全
IEC 61508-1:2010	电气/电子/可编程电子安全相关系统的功能性安全：一般要求。
IEC 61508-2:2010	电气/电子/可编程电子安全相关系统的功能性安全：电气/电子/可编程电子安全相关系统的要求。
IEC 61508-3:2010	电气/电子/可编程电子安全相关系统的功能性安全：软件要求。
IEC 61784-3:2016	工业通信网络 - 配置 - 第 3 部分：功能安全现场总线 - 一般规则和配置定义
2006/42/EC	机械指令
2014/30/EU	电磁兼容性规程
2014/35/EU	低电压规程

此外，本文中所用的名词可能是被无意中使用的，因为它们是从其他标准中衍生出来的，如：

标准	描述
IEC 60034 系列	旋转电机
IEC 61800 系列	可调速电力驱动系统
IEC 61158 系列	用于测量和控制的数字数据通讯：用于工业控制系统的现场总线

最后，操作区一词可结合特定危险的描述一起使用，其定义相当于机器指令 (2006/42/EC) 和 ISO 12100:2010 中的风险区或危险区。

注：对于当前文档中引用的特定产品，上述标准可能适用，也可能不适用。若要了解与适用于此处所述产品的各项标准有关的更多信息，请参阅这些产品参考的特性表。

简介

概述

简介

EcoStruxure Automation Device Maintenance 让您能够同时升级多台设备上的固件包。设备可以被自动发现，或者如果设备不支持自动设备发现或者此功能已关闭，您可以手动添加设备。

支持的设备发现方法有：

- Modbus 功能代码 43 (读取设备标识)
- DPWS (Web 服务设备配置文件)

功能

EcoStruxure Automation Device Maintenance 支持以下功能：

- 自动设备发现
- 手动设备识别
- 安全功能
- 同时对多个设备执行固件更新
- IP 地址管理

支持的 Schneider Electric 设备

Modicon 设备：

- Modicon M340
- Modicon M580
- Modicon Momentum
- Modicon X80 I/O 模块

Altivar 设备：

- Altivar 产品系列
 - Altivar Process ATV6•• 驱动器
 - Altivar Process ATV9•• 驱动器
 - Altivar Machine ATV340 驱动器
- Altivar :
 - VW3A3720 Ethernet
 - VW3A3721 MultiDrive-Link
 - VW3A3530D ATV dPAC
- Altivar 软起动器：
 - Altivar ATS480 软起动器

系统要求

硬件要求

组件	最低要求
CPU	支持 Intel® Core i3 或更新的版本
RAM	最小 4 GB，建议 8 GB 或更大。
硬盘空间	500 MB 可用硬盘空间

软件要求

- Microsoft Windows® 10 Professional 32 位/64 位或更新的版本
- Microsoft Windows Server 2016 Standard 64 位
- Microsoft Windows Server 2019 Standard 64 位

通讯协议

工具支持以下协议：

- FTP
- HTTP / HTTPS
- Modbus SL
- Modbus TCP
- OPC UA
- TCP
- UDP
- USB


屏幕分辨率

如要以最佳的屏幕分辨率查看此软件，请使用 1920 x 1080 像素的屏幕分辨率。屏幕分辨率至少需要达到 1280 x 1024 像素。

网络安全

此软件使用以下端口：

- DPWS (藉由端口 3702)
- FTP (藉由端口 20、21)
- HTTP (藉由端口 80) / HTTPs (藉由端口 443 和 8080)
- Modbus (藉由端口 502)
- OPC UA (藉由端口 4840)

警告

系统可用性、完整性和保密性的潜在危害
遵守网络安全最佳做法。
未按说明操作可能导致人身伤亡或设备损坏等严重后果。

注: 有关网络安全的详细信息，请参阅章节 网络安全, 68 页。

安装
过程

您可以通过从 Schneider Electric 网站下载安装文件的方式，来安装软件。

注: 在双击 AutomationDeviceMaintenance.exe 文件之前，请先验证文件的完整性，如章节 数字签名验证, 72 页 所述。

注: 您必须拥有管理员权限，才能安装软件。

按照以下步骤安装软件：

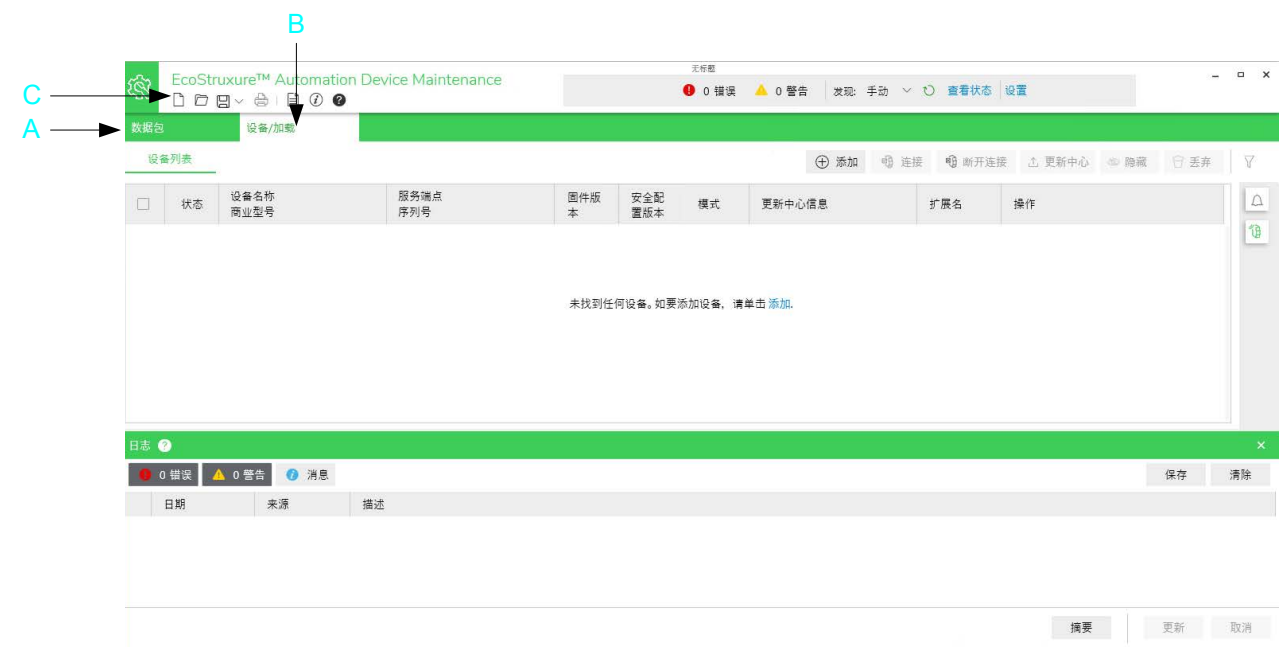
步骤	操作
1	在下载文件之后，通过 Windows 资源管理器定位安装文件。
2	双击 EcoStruxure Automation Device Maintenance 安装文件。 然后便会显示 InstallShield Wizard。
3	按照 InstallShield Wizard 中的说明，完成安装。

快速入门

欢迎屏幕

概述






首次启动后，EcoStruxure Automation Device Maintenance 显示以下屏幕以用于升级多台设备上的固件包。关闭此工具时，保存用户界面的当前状态。因此，重新启动时，EcoStruxure Automation Device Maintenance 将显示上次关闭工具时所显示的视图。



说明	名称	功能
A	数据包	显示数据包存储库的内容。
B	设备/加载	显示已发现或手动识别的设备的详细信息。
C	工具栏	显示用于执行功能的一系列图标。

工具栏

工具栏允许访问 EcoStruxure Automation Device Maintenance 常规功能。

元素	名称	描述
	新项目	让您能够创建新 EcoStruxure Automation Device Maintenance 项目, 25 页。
	打开	用于打开 existing project, 27 页。
	保存	用于保存 project settings, 26 页。
	打印	此版本中无此功能。
	日志	用于查看日志信息。
	关于	用于访问： <ul style="list-style-type: none">EcoStruxure Automation Device Maintenance 信息复制详情许可证协议组件信息系统信息
	帮助	用于访问在线帮助。
	错误	用于查看检测到的错误, 24 页。
	警告	用于查看检测到的警告, 24 页。
	发现	用于在设备发现模式设置为 手动 时触发设备发现。
–	手动 / 自动	从列表中选择 手动 或 自动 设备发现模式。 有关更多信息, 请参阅配置设备发现模式一章, 30 页。
–	设置	用于配置 设置 。

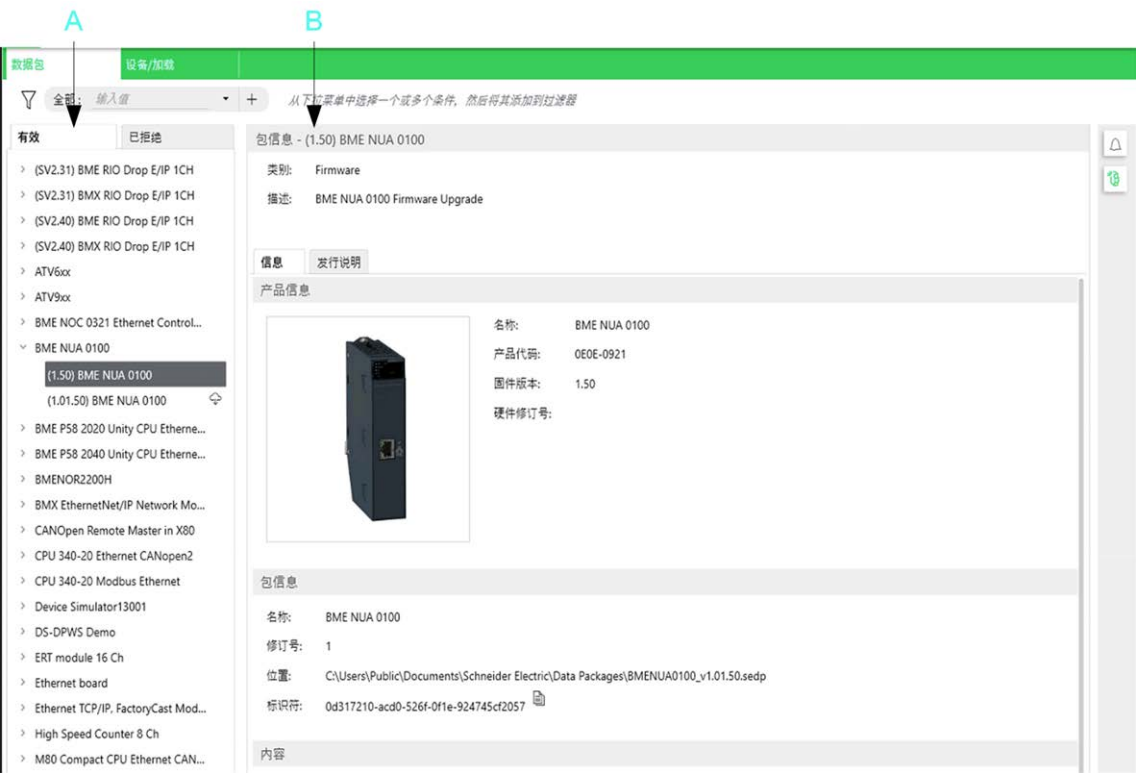
按钮

按钮	描述
总结	执行更新后, 单击 汇总 按钮, 获取与已更新的设备有关的信息。
更新	在对更新固件, 64 页或更新安全配置文件, 66 页进行了相关设置后, 单击 更新 按钮, 按配置的方式启动更新过程。
取消	取消 按钮让您能够取消更新操作。

EcoStruxure Automation Device Maintenance用户界面

数据包


数据包功能包含数据包存储库，并显示工具中可用的固件包。



说明	名称	描述
A	包含有效和已拒绝选项卡的数据包列表	显示本地可用固件包的列表。如果安装了所需的插件，便会显示网络中可用的包。 有关更多信息，请参阅“数据包”选项卡一章, 49 页。
B	包信息	显示所选数据包的描述和内容，上部的静态信息指示类别和描述，下部包含两个选项卡，即，信息和发行说明。 有关更多信息，请参阅“数据包”选项卡一章, 49 页。


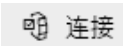

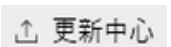




设备/加载

概述

设备/加载选项卡显示工具已知的设备的详细信息。
注: 只有在发现模式设置为**自动**时, 才会自动更新此选项卡中所显示的信息。
单击工具栏中的 图标, 即可显示最新值。



选项卡的按钮：

按钮	描述
	单击 添加 按钮, 添加新设备。有关更多信息, 请参阅 添加设备, 21 页。
	单击 连接 按钮, 建立到所选设备的连接。
	单击 断开连接 按钮, 终止与所选设备的连接。
	单击 更新中心 按钮, 打开 更新中心 对话框。它让您能够配置设置, 以便为所选设备执行固件更新或安全配置文件更新。有关更多信息, 请参阅 更新中心 , 63 页。
	单击 隐藏 按钮, 隐藏所发现的设备。有关更多信息, 请参阅“设备/加载”视图, 53 页。
	单击 Dispose (丢弃) 按钮, 丢弃所发现的设备。有关更多信息, 请参阅“设备/加载”视图, 53 页。
	单击 通知区域 按钮, 查看 设备/加载 选项卡右侧的通知区域。有关更多信息, 请参阅查看/确认消息, 62 页。
	单击 设备发现状态 按钮, 查看 设备/加载 选项卡右侧的 设备发现状态 视图。有关更多信息, 请参阅监控设备发现状态, 61 页。

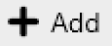
表格的元素：

元素	描述
组	您可以将 设备列表 中显示的设备分配给不同的组, 如章节对设备列表中的设备分组, 54 页所述。 如要选择属于某个 组 的所有设备, 请选中该 组 的复选框。
复选框	选中左侧的多个复选框, 可同时对多个设备执行相同操作, 如 连接/断开连接 或更新操作。
状态	显示设备的状态： <ul style="list-style-type: none">灰色：设备已断开网络连接。黄色：设备已连接到网络, 但尚未输入有效凭据。绿色：已输入有效凭据。蓝色：工具正将内容加载到设备。红色：固件下载后正重启设备, 以便完成安装。
设备名称 商业型号	显示设备的名称和商业型号 (CR)。 注: 如果为设备指定了 友好名称 , 则只有在通讯协议支持此参数时, 才会显示此用户定义名称。例如, Modbus TCP 就不支持此参数。

元素	描述
服务端点 序列号	将服务端点地址显示为设备的 URI (统一资源标识符) 和序列号 (SN)。
固件版本	显示设备的当前固件版本。
模式	仅在登录后可用：指示设备的模式：RUN、STOP、BUSY、NOCONF、RESERVED、ENTERED、LOADING、COMPLETED、REQUIRERESTART、ERROR。此单元格的内容会定期刷新。 注： 根据所连接的设备的数量，此模式监控可能会影响网络带宽。
更新中心信息	显示在 更新中心 对话框中配置的更新设置： 已选择固件、已选择安全配置、固件更新成功、固件更新已取消、固件更新失败 。有关更多信息，请参阅 更新中心 , 63 页。
扩展模块	模块化设备提供让您能够对设备的具体扩展模块进行访问的链接 (扩展名)。有关更多信息，请参阅 访问扩展模块 , 59 页。
动作	为每个设备提供相关图标，以执行不同的设备特有操作：
	单击 设置凭据 图标，然后在 设置凭据 对话框中输入在连接到设备时需使用的凭据。黑色图标表示未存储设备的凭据。黄色图标表示已存储凭据，但未执行到设备的登录。 或者，您也可以通过 设置 > 项目 > 用户凭据设置 来配置项目的全局凭据。有关更多信息，请参阅 管理用户凭据 , 57 页。
	绿色 设置凭据 图标表示设备的凭据已被验证且登录已成功执行。
	红色的 设置凭据 图标表示设备登录失败。 重新执行登录程序，确保使用正确的凭据。
	单击 连接/断开连接 图标，建立或终止与设备的连接。
	单击 更新中心 图标以打开 更新中心 对话框。它让您能够配置设置，以便为设备执行固件更新或安全配置文件更新。有关更多信息，请参阅 更新中心 , 63 页。
	单击 设备日志 图标，查看日志信息。
	单击 启动设备 图标，启动设备。 注： 安装或更新后，在使用电气控制和自动化设备进行常规操作之前，应执行启动测试。有关更多信息，请参阅 启动与测试 , 6 页。
	显示证书状态。 <ul style="list-style-type: none">灰色：可信证书红色：不可信证书 单击 设备证书 图标，打开 证书信息 对话框。有关更多信息，请参阅 在设备/加载选项卡中管理证书的信任状态 , 45 页。
	指示设备配有 SD 存储卡。单击此图标，将软件直接下载到 SD 存储卡。
	在成功登录后，单击 其他设备选项 图标，查看设备可用的命令列表。有关更多信息，请参阅 登陆后可用的详细信息 , 53 页。
进度	显示固件更新进度状态。

添加设备

概述

添加设备对话框的打开方式是：单击设备/加载选项卡中的  Add 按钮，或者单击当设备列表为空（比如，如果要创建新项目）时显示的**未找到任何设备**。若要添加模块，请单击**此处**链接。



这样，如果由于设备不支持发现或者设备发现功能已关闭，导致 EcoStruxure Automation Device Maintenance 无法自动发现设备，那么便可以手动添加设备。为此，请选择商业型号。

缺省情况下，**商业型号**仅包含商业型号的模板（如 **BME*****、**BMX***** 或**任意设备**）。在这种情况下，有两个选项可供选择：

- 选择与您的产品匹配的模板：例如，对于 BMEP582020，从列表中选择 **BME*****。

注：为涵盖旧版本（例如，**BME*****）和最新版本（例如，**BME*** (升级版)**）的每个模板提供了两种变体。它们在支持的协议上有所不同。因此，如果在**连接**列表中找不到您选择的协议，请选择为您的产品提供的第二个选项。

- 如要将您正在使用的设备的商业型号填入列表，请将相应的数据包复制到在**设置 > 包设置**对话框中被配置为**本地存储库**的文件夹中。（有关更多信息，请参阅章节 **配置包位置**, 35 页。）然后，该表格将显示具体的型号（如 **BMEP582020** 或 **BMXNOR0200**）。

组成部分	描述
商业型号	从列表中选择设备的 商业型号 ，然后根据从右侧的 连接 列表中选择协议，输入设备信息。
连接	从列表中选择通讯协议： <ul style="list-style-type: none">• HTTP/HTTPS• MODBUS (SL)• MODBUS (TCP)• OPC UA• FTP• USB 参数会根据所选择的协议进行调整。
安全	此选项仅适用于 HTTP/HTTPS 通讯： 如果设备通过安全连接 (HTTPS) 进行连接，则选择此选项。
IP 地址	输入正添加的设备的 IP 地址以及用于通讯的端口。
设备 ID	此选项仅适用于 MODBUS (TCP) 通讯： 输入 Modbus TCP 通讯的设备标识节点。 有关 Modbus 规范的更多信息，请参阅 Modbus Specifications and Implementation Guides。

注: EcoStruxure Automation Device Maintenance V3.1 及更高版本支持按商业型号添加设备。如果您尝试打开使用 EcoStruxure Automation Device Maintenance V3.0 及更早版本创建的项目文件，且这些文件包含没有商业型号的设备，则系统会提示您为每个未知设备选择商业型号。

另请参阅 打开项目, 27 页。

配置设置


概述

设置页让您能够配置常规设置。



组成部分	描述
发现	用于配置发现模式。有关更多信息，请参阅 配置设备发现模式, 30 页。
DPWS	用于配置 DPWS 扫描器的详细信息。有关更多信息，请参阅 配置 DPWS 扫描器, 34 页。
Modbus TCP	用于配置 Modbus 扫描器的详细信息。有关更多信息，请参阅 配置 Modbus TCP 扫描器, 32 页。
通讯	用于配置通讯设置。有关更多信息，请参阅 配置通讯设置, 35 页。
包设置	用于配置包设置。有关更多信息，请参阅 配置包位置, 35 页。
安全	选择该选项可激活保护模式并显示与安全功能有关的通知，如使用证书进行的加密通讯、安全包或 syslog 支持。有关更多信息，请参阅 安全功能, 39 页。
证书管理	用于注册 EcoStruxure Automation Device Maintenance 的应用程序证书，并管理通讯合作伙伴数字证书的信任状态。有关更多信息，请参阅 管理证书, 41 页。
PKI	用于配置公钥基础设施 (PKI)。有关更多信息，请参阅 管理公钥基础设施 (PKI), 46 页。
日志	用于查看 EcoStruxure Automation Device Maintenance 日志文件并配置日志设置。有关更多信息，请参阅 查看日志文件, 36 页。
语言	用于配置所需语言。有关更多信息，请参阅 配置语言, 38 页。
组	用于对设备列表中显示的设备进行分组。有关更多信息，请参阅 对设备列表中的设备分组, 54 页。
项目 > 用户凭据设置	选择此选项，可输入项目设备的全局凭据。有关更多信息，请参阅 管理用户凭据, 57 页。

应用修改

每当修改了设置页中的设置时，此选项卡就会标有刷新图标 ，表示此页上有尚未应用的修改。

如要将修改应用到此页，请单击**应用**按钮。

如要应用所有选项卡中所执行的修改并关闭**设置**页，请单击**确定**按钮。

错误和警告窗口

概述

您可以在工具的累积日志窗口中查看检测到的错误的详细信息。错误日志提供了详细信息，可用于改正与所选设备相关的检测到的错误。除非已解决检测到的错误，否则无法继续更新所选设备的固件。



说明	名称	描述
A	错误和警告状态	显示检测到的错误和警告的数量。
B	日志	显示检测到的错误和警告的数量及其相关描述。

查看错误和警告日志



步骤	操作
1	单击工具栏中的 错误 或 警告 状态。 日志 窗口将显示以下信息： <ul style="list-style-type: none">检测到的错误的数量、检测到的警告以及信息。检测到的错误的描述。
2	选择检测到的错误、检测到的警告以及/或者所选择的信息消息。
3	单击 保存 ，保存所选择的检出错、检出警告和信息消息。
4	单击 清除 ，从日志中删除与检测到的错误和检测到的警告有关的所有消息。

创建新 EcoStruxure Automation Device Maintenance 项目

过程

此功能可用于创建新 EcoStruxure Automation Device Maintenance 项目。

按照以下步骤创建项目：

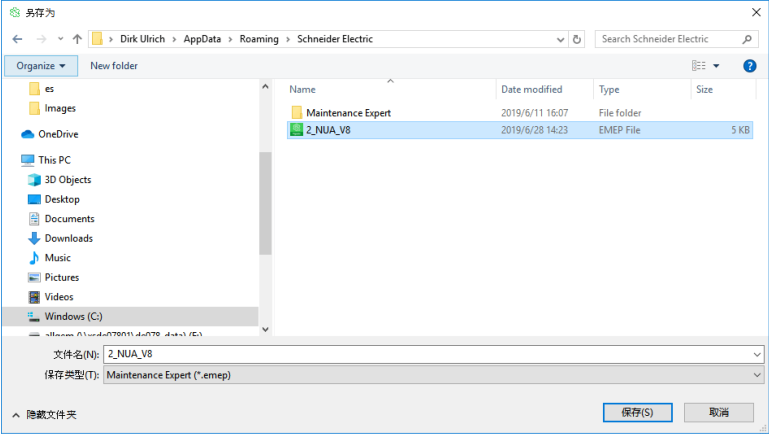

步骤	操作
1	<div>单击  图标。</div> <div>结果：如果打开的项目已修改但尚未保存，则会显示项目已修改对话框。</div>
2	<div>在项目已修改对话框中，单击是，保存对已打开项目的更改，或者单击否，在不保存的情况下关闭项目。</div> <div></div> <div>结果：关闭打开的项目，打开新项目，显示设备/加载选项卡，其中的设备列表为空。</div>

- 创建新项目时，会自动执行以下任务：
- 发现模式被设置为**手动**。
 - 清除日志文件条目。

保存项目

此功能让您能够以不同的名称或不同的保存位置来保存当前项目的副本。其优点在于，打开 EcoStruxure Automation Device Maintenance 工具时，不需要反复添加设备。


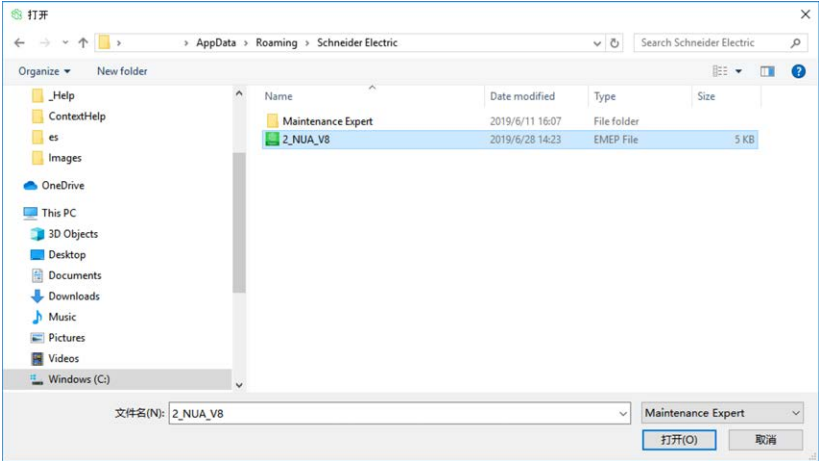

按照以下步骤保存项目设置：

步骤	操作
1	<div>单击  图标。</div>
2	<div>如要保存对当前项目的更改，请单击保存。 如要保存项目的副本，请单击另存为。</div>
3	<div>选择要用来保存项目的文件夹，然后输入文件名。</div> <div></div>
4	<div>单击保存，然后在设置密码对话框的两个字段中输入相同的密码。</div> <div></div>
5	<div>单击确定以继续。</div>

打开项目

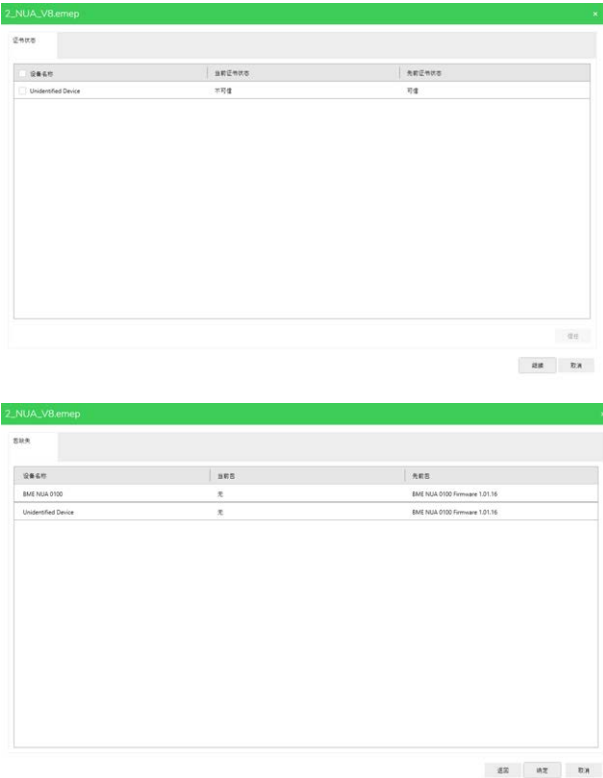
打开项目

如要打开项目，请执行以下步骤：


步骤	操作
1	<div>单击 图标。</div> <div></div>
2	<div>选择文件夹和项目。单击打开，然后输入密码。</div> <div></div>
3	单击 确定 ，打开项目。

适用于在其他计算机上创建的项目文件的可选步骤

如果试图打开的项目文件是在另一台计算机上创建的，工具会选择性地指示证书信任状态差异和包可用性差异。



在这种情况下，请执行以下操作：

步骤	操作
4	选择要信任的设备，然后单击 信任 。
5	单击 继续 。 <div></div>
6	单击 确定 ，打开有包缺失的项目，或者单击 取消 。

适用于涉及未识别设备的项目文件的可选步骤

如果您尝试打开使用 EcoStruxure Automation Device Maintenance V3.0 及更早版本创建的项目文件，且这些文件包含没有商业型号的设备，则会显示一个对话框，提示您从列表中为每个未知设备选择商业型号：



选择您选定的商业型号，然后单击**确定**以打开项目。

配置 EcoStruxure Automation Device Maintenance 工具

配置设备发现模式

配置自动发现模式

您可以将设备发现模式选择为**自动**或**手动**。如果是**自动**发现，工具将定期通过网络在后台发送信息，并接收来自响应设备的信息。

步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	单击 发现 选项。 <div></div>
3	选择 自动 模式。
4	选择将参与发现的扫描器。使用此设置可有助于防止扫描任何希望避免的设备。
5	单击 应用 ，然后单击 确定 。

配置手动发现模式

您可以将设备发现模式选择为**手动**，以在需要时发现网络中连接的设备。

步骤	操作									
1	单击 主页 顶部中心位置处的 设置 菜单。									
2	单击 发现 选项。 <div><div><div>设置</div><div><div><div>全局</div><div>发现</div><div>DPWS</div><div>Modbus TCP</div><div>通讯</div><div>包设置</div><div>安全</div><div>证书管理</div><div>PKI</div><div>Syslog</div><div>日志</div><div>语言</div><div>组</div><div>项目</div></div><div><div>发现</div><div>发现模式: <input checked="" type="radio"/> 手动 <input type="radio"/> 自动</div><table><thead><tr><th>扫描器</th><th><input checked="" type="checkbox"/> 启用扫描器</th><th>状态</th></tr></thead><tbody><tr><td>DPWS</td><td><input checked="" type="checkbox"/></td><td>非活动</td></tr><tr><td>Modbus TCP</td><td><input checked="" type="checkbox"/></td><td>非活动</td></tr></tbody></table></div><div><div>?</div><div>复位</div><div>确定</div><div>取消</div><div>应用</div></div></div></div></div>	扫描器	<input checked="" type="checkbox"/> 启用扫描器	状态	DPWS	<input checked="" type="checkbox"/>	非活动	Modbus TCP	<input checked="" type="checkbox"/>	非活动
扫描器	<input checked="" type="checkbox"/> 启用扫描器	状态								
DPWS	<input checked="" type="checkbox"/>	非活动								
Modbus TCP	<input checked="" type="checkbox"/>	非活动								
3	选择 手动 模式。									
4	选择将参与发现的扫描器。使用此设置可有助于防止扫描任何希望避免的设备。									
5	单击 应用 ，然后单击 确定 。									

配置 Modbus TCP 扫描器

概述

Modbus TCP 扫描器向通过**起始 IP 地址**和**结束 IP 地址**定义的范围内的所有 IP 地址发送 Modbus 功能代码 43 请求。

您可以配置以下 **Modbus TCP** 参数：

元素	缺省值	描述
IP 地址部分：		
范围名称参数	—	地址范围的可选名称。
起始 IP 地址参数	127.0.0.1	地址扫描范围的第一个地址。
结束 IP 地址参数	127.0.0.1	地址扫描范围的最后一个地址。
导入按钮	—	单击 导入 按钮，导入支持 .csv 格式的配置文件（请参阅下面的导入配置文件示例, 32 页）。 注: 此命令会覆盖当前配置设置。务必事先备份您的设置。 结果： 打开 Windows 文件打开 对话框，在网络上浏览 csv 文件。单击 打开 ，从文件导入配置设置。如要应用新设置，请单击 应用 或 确定 。
+ 添加按钮	—	单击 + 添加 按钮，创建新地址范围。 结果： 表中添加新行，其中： 范围名称 = 缺省 起始 IP 地址 = 127.0.0.1 结束 IP 地址 = 127.0.0.1
复选框	—	选中/取消选中复选框，以包含/排除 Modbus 扫描的选定范围。
垃圾桶按钮	—	单击垃圾桶按钮可删除选定范围，即，表格的行。
高级设置部分：		
起始端口参数	502	端口扫描范围的第一个端口。
结束端口参数	502	端口扫描范围的最后一个端口。
超时参数	4000	从向设备发送 ping 到接收答复之间的最大等待时间。
设备 ID 参数	255	用于设备寻址的 Modbus 设备 ID。

配置文件导入示例

.csv 格式的配置文件在格式上应与以下示例一致：

```
enabled;name;start;end
1;range 1;127.0.0.1;127.0.0.1
1;range 2;127.0.0.2;127.0.0.2
```


配置 Modbus TCP 扫描器

请按以下步骤配置 **Modbus TCP** 扫描器：

步骤	操作
1	展开设置页上的发现菜单。
2	选择 Modbus TCP 节点。
3	在右侧的 Modbus TCP 视图中，单击 添加 按钮，创建新地址范围。
4	<p>单击导入按钮，导入配置文件，或者配置以下参数：</p> <ul style="list-style-type: none"> 范围名称 起始 IP 地址 结束 IP 地址 起始端口 结束端口 超时 设备 ID 
5	单击 应用 ，应用 Modbus TCP 设置，或者单击 确定 ，应用所有应用程序设置修改并关闭 设置 对话框。

配置 DPWS 扫描器

概述

DPWS 扫描器是 DPWS 标准的一种客户端侧实现，它用于发现符合 DPWS 标准的设备。

有关 DPWS 标准的更多信息，请参阅 <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>。

您可以配置以下 DPWS 参数：

参数	缺省值	描述
探测器请求超时	3000 毫秒	从发送探测器请求到从设备接收到探测器匹配响应之间的最大等待时间。
元数据请求超时	1000 毫秒	从发送元数据请求到从设备接收到响应之间的最大等待时间。
使用的网络适配器	—	要用于发送 DPWS 探测器请求的网络适配器的列表。

请按以下步骤配置 DPWS 扫描器：

步骤	操作
1	展开设置页上的发现菜单。
2	<div>选择 DPWS，然后输入以下详细信息：</div> <ul style="list-style-type: none">• 探测器请求超时• 元数据请求超时• 使用的网络适配器 <div></div>

配置通讯设置

概述

设置

全局

发现

DPWS

Modbus TCP

通讯

包设置

安全

证书管理

PKI

Syslog

日志

语言

组

项目

?

复位

通讯

超时

超时: 6000 毫秒

自动设备状态轮询

频率 (高优先级): 3000 毫秒

频率 (低优先级): 10000 毫秒

确定

取消

应用

您可以为 EcoStruxure Automation Device Maintenance 和设备之间的通讯配置以下通讯设置：

参数	缺省值	描述
超时：		
超时	6000 毫秒	EcoStruxure Automation Device Maintenance 发送/接收了请求/响应（比如，固件更新、设置 IP 配置）之后的最长等待时间。 有关应用到发现请求的超时，请参阅 Modbus TCP 扫描器, 32 页和 DPWS 扫描器, 34 页。
自动设备状态轮询部分：这些参数定义向检测到的设备发送轮询请求以便保持设备状态, 19 页更新的频率：		
频率（高优先级）：	3000 毫秒	执行固件更新时，使用高优先级轮询。它用于在重启设备后加快设备检测速度。
频率（低优先级）：	10,000 毫秒	在正常操作中，使用轮询循环频率较低的低优先级。

配置包位置

您可以在工具中配置可用固件数据包的路径。这样就能够更新设备固件版本。此外，每个数据包所提供的特定商业型号将添加到添加设备对话框, 21 页的商业型号列表中。

更改包位置

按照以下步骤更改包位置：




步骤	操作
1	单击主页顶部中心位置处的 设置 菜单。
2	选择 包设置 选项。
3	选择更改 本地存储库 位置时所使用的路径。
4	<div>单击  图标，选择路径更改的目标文件夹。</div> <div></div>
5	单击 应用 ，然后单击 确定 。

查看日志文件

您可以查看存储的日志并对其进行分析以便获得所选设备的任何详细信息。

按照以下步骤查看日志：

步骤	操作
1	单击主顶部中心位置处的 设置 菜单。
2	选择 日志 选项。
3	将日志创建设置为 已激活/未激活 。
4	选择更改日志文件位置的路径。

步骤	操作
5	<div><div></div><div>单击  图标，选择路径更改的目标文件夹。</div></div> <div><div><div>设置</div><div><div>全局</div><div>发现</div><div>DPWS</div><div>Modbus TCP</div><div>通讯</div><div>包设置</div><div>安全</div><div>证书管理</div><div>PKI</div><div>Syslog</div><div>日志</div><div>语言</div><div>组</div><div>项目</div></div><div><div>日志</div><div><div>活动</div><div>非活动</div></div><div><div>C:\Users\AdminUser\AppData\Local\Temp\AutomationDeviceMaintenance.log</div><div>...</div><div></div></div><div><div></div><div>日志文件包含敏感数据。请在使用后删除该日志文件或将其保存在安全的地方。</div></div><div><div>?</div><div>复位</div><div>确定</div><div>取消</div><div>应用</div></div></div></div></div> <div>注: 有关网络安全通知的更多信息，请参阅 增强网络安全的建议, 63 页。</div>
6	单击应用，然后单击确定。

配置语言

您可以选择语言，从而以首选语言查看 EcoStruxure Automation Device Maintenance 工具的内容。

支持下列语言：

- 英语
- 德语
- 法语
- 西班牙语
- 意大利语
- 中文

按照以下步骤设置语言：

步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	选择 语言 选项。
3	<p>单击选择语言下拉列表，选择所需的语言。</p> 
4	<p>单击应用，然后单击确定。</p> <p>注：重新启动 EcoStruxure Automation Device Maintenance，以应用语言更改。</p>

复位应用程序设置

概述

设置菜单的对话框在左下角包含**复位**按钮。

单击**复位**按钮，可将通过**设置**菜单配置的所有应用程序设置值复位为缺省值。

配置安全功能

概述

我们根据可用的最新信息，不断改进网络安全最佳做法和解决方案。其中一个设计标准是，Schneider Electric 包含先进的指示和技术，以帮助提高产品抵御网络攻击的能力。通过设计途径实现的安全性实现了通过相应的机制部署，来降低威胁、降低可被利用的漏洞、并抵御不可避免的数据破坏和网络功能。

注:

为了有助于保持和保护 Schneider Electric 产品的安全，强烈建议您采取 Schneider Electric website 上提供的网络安全最佳做法中所述的网络安全最佳做法。

由于机器和设备联网量的飞速增加，潜在威胁也快速攀升。因此，请谨慎考虑一切可能的安全措施。

安全措施是必要的，有助于保护数据和腾讯通道免遭非法访问。

注: 在配置安全功能之前，请咨询安全管理员，以确保使用正确的安全设置。

安全功能

概述

EcoStruxure Automation Device Maintenance 支持以下安全功能：

- 在公钥基础设施 (PKI) 中使用数字证书的加密通讯。
- Schneider Electric Data Package Secure (SEDPS) 数字签名包的处理。
- Syslog 网络协议。

激活/禁用保护模式

如果您在受保护的网路中工作，但不使用安全功能，则可以通过**设置**页面的**安全**选项禁用与安全功能（例如，带有黄色感叹号）有关的通知。



步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	选择 安全 选项。
3	选择该选项以激活保护模式并显示与安全功能有关的通知。

导入安全配置文件

EcoStruxure Automation Device Maintenance 让您能够导入在 EcoStruxure Cybersecurity Admin Expert 应用程序中为网路全局配置的安全配置设置。如果这些设置可用作文件，则按如下方式导入文件：

步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	选择 安全 选项。
3	在 导入安全配置文件 部分，单击 导入 按钮，导航至安全配置文件。
4	单击 打开 ，从文件导入安全配置设置。

如要更新安全配置文件，请使用**更新中心**，如章节更新安全配置文件, 66 页所述。

管理证书

概述

在公钥基础设施 (PKI) 中，通过相应协议（例如 HTTPS）进行安全通讯时，需要使用数字证书。

在 TLS 的环境中，可以使用证书来验证通讯合作伙伴的身份。证书在连接建立期间发送，亦即所谓的 TLS 握手。除非服务器要求客户端证书，否则证书发送对于客户端是可选的（在这种情况下为 EcoStruxure Automation Device Maintenance 的应用程序证书）。服务器始终会发送其证书。只有在证书验证结果为肯定结果时，才能够建立与通讯合作伙伴的连接。

EcoStruxure Automation Device Maintenance 支持以下证书信任模式：

- 手动信任模式：您可以手动信任/取消信任安全通讯参与者的证书。信任状态在**证书管理**对话框的**可信证书/不可信证书**选项卡中进行管理, 44 页。
- 允许列表信任模式：您可以使用安全配置文件, 40 页导入允许列表。EcoStruxure Automation Device Maintenance 于是会自动信任此列表中的证书。
- Certificate Authority (CA) / 注册信任模式：EcoStruxure Automation Device Maintenance 自动信任已藉由 CA 证书注册的证书，这些 CA 证书位于 Windows **证书存储库的可信根证书授权**文件夹中。

证书使用时的注意事项

使用证书开展安全通讯时，应注意以下事项：

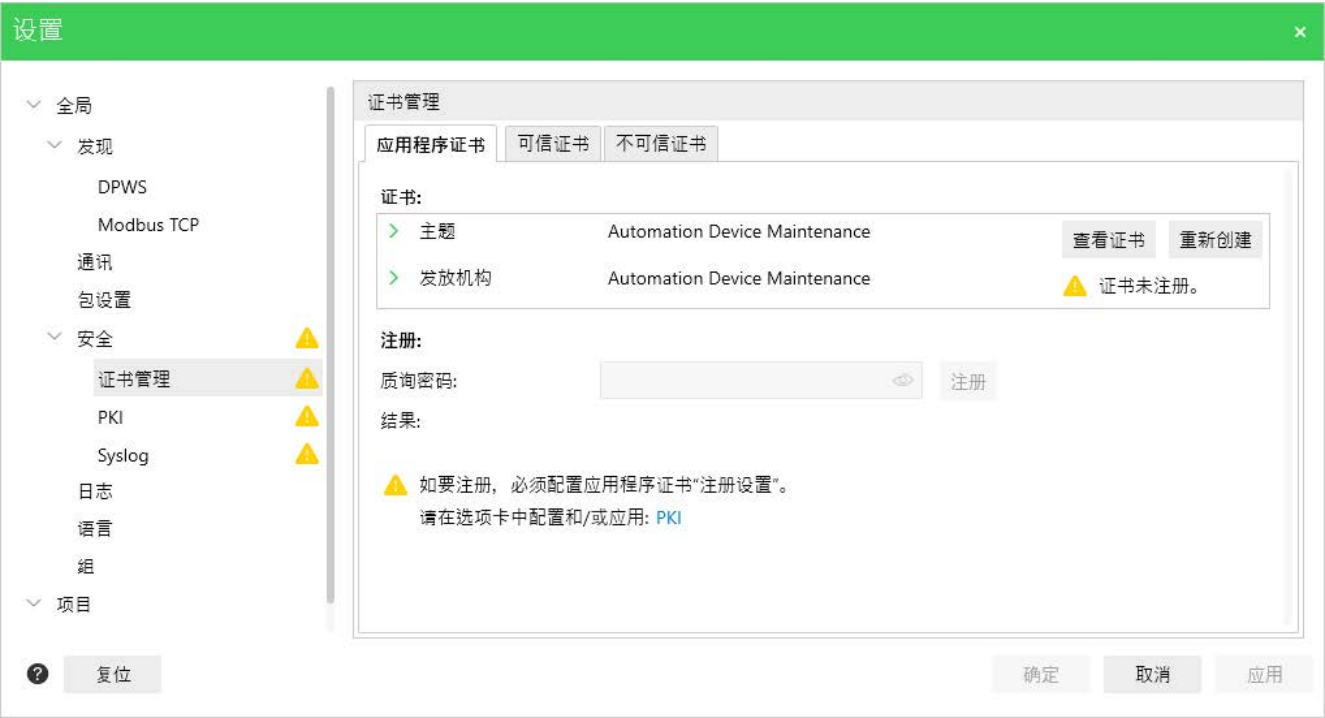
- 必须管理证书，因为它们的有效期有限，因此需要定期更新。在考虑机器寿命周期或控制时，需要注意这一点。
- 根据 Windows PC 的日期和时间来检查证书是否仍有效。通过 Windows **开始 > 设置 > 时间和语言 > 日期和时间**来定期检查设置。
- 如果运行 EcoStruxure Automation Device Maintenance 的 PC 永久脱机，则必须定期手动更新**证书撤销列表** (CRL)。为此，请连接到 CRL 分发点，下载最新 CRL，并将其安装到 PC。
有关 CRL 分发点的正确 URL，请咨询安全管理员。
- 您也可以在 EcoStruxure Automation Device Maintenance 中（例如，通过**证书管理**对话框, 44 页）将证书声明为不可信。

证书管理对话框

初始安装后，将为 EcoStruxure Automation Device Maintenance 提供缺省自签名应用程序证书。

证书管理对话框为应用程序证书提供以下选项：

- 重新创建自签名应用程序证书并指定具体属性（请参阅 重新创建自签名应用程序证书, 42 页）。
- 注册应用程序证书以分配 Certificate Authority (CA) 的数字签名并创建信任链（请参阅 注册应用程序证书, 43 页）。
- 管理通讯合作伙伴数字证书的信任状态（请参阅 管理证书的信任状态, 44 页）。



重新创建自签名应用程序证书

按照以下步骤，重新创建缺省应用程序证书，并指定具体属性：

步骤	操作
1	单击主页顶部中心位置处的设置菜单。
2	选择安全 > 证书管理选项。
3	在应用程序证书选项卡中，单击重新创建按钮。 结果：创建证书对话框随即打开。
4	输入要为证书指定的属性，然后单击确定。 结果：向其他通讯参与者提供包含预定义属性的自签名 EcoStruxure Automation Device Maintenance 证书。

注册应用程序证书

如要创建信任链，必须由 Certificate Authority (CA) 注册 EcoStruxure Automation Device Maintenance 应用程序证书并进行数字签名。

如要注册证书，请首先配置**设置 > 安全 > PKI** 选项, 46 页所提供的**注册设置**。

然后，按照以下步骤注册应用程序证书EcoStruxure Automation Device Maintenance：

步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	选择 安全 > 证书管理 选项。
3	在 应用程序证书 选项卡中，检查应用程序证书是否仍被自签名且尚未注册： <ul style="list-style-type: none">在证书部分，主题和发放机构都显示相同内容：Automation Device Maintenance。在发放机构行中显示有通知证书未注册。。
4	在 质询密码 文本框中输入 CA 密码。此密码用于授权注册请求。有关详细信息，请咨询您的工业网络管理员。
5	单击 注册 。 结果： EcoStruxure Automation Device Maintenance 将来自应用程序证书的证书签名请求连同质询密码发送到 CA。如果密码不正确，将返回消息 注册失败 。 注： 此过程将缺省自签名应用程序证书替换为新的签名证书。这种替换无法被撤消。
6	检查过程是否已成功完成： <ul style="list-style-type: none">结果：在应用程序证书选项卡中显示了注册成功。在证书信息对话框的常规选项卡中，发放机构 条目已更改为 CA 的名称，例如 <i>INT-DEV-SUB-CA</i>。证书路径 证书信息对话框的“证书路径”选项卡根据 PKI 配置，指示层级结构中的 根 CA和从属 CA。层级结构底部的终端实体证书是 EcoStruxure Automation Device Maintenance 的证书，其中包含以下条目：<ul style="list-style-type: none">CN (Common Name) = Automation Device MaintenanceO (Organization) = Schneider Electric

管理证书的信任状态

证书管理对话框的**可信证书**和**不可信证书**选项卡让您能够管理 EcoStruxure Automation Device Maintenance 中可用证书的信任状态。

在这两个选项卡中，列出了各证书，并提供了以下信息：

组成部分	描述
主题	提供证书概述： <ul style="list-style-type: none">• CN = 常用名• OU = 组织单位
设备名称	按 设备/加载 选项卡的 设备列表 中所示，提供设备名称。 如果证书不属于某个设备，则显示 不适用 。
服务端点	为当前 EcoStruxure Automation Device Maintenance 会话中所用的设备提供有关服务端点的信息。 如果证书不属于某个设备，则显示 不适用 。
操作	让您能够通过 查看证书 链接打开 证书信息 对话框。
证书状态	指示证书的状态： <ul style="list-style-type: none">• 可信• 不可信

您可以对证书执行以下操作：

- 如要取消信任证书，请在**可信证书**选项卡中选择一个或多个证书，然后单击**取消信任**按钮。
- 如要信任证书，请在**不可信证书**选项卡中选择一个或多个证书，然后单击**信任**按钮。如要临时信任所选证书，请选择**信任此会话**选项。
- 如要删除证书，请在**可信证书**或**不可信证书**选项卡中选择一个或多个证书，然后单击**删除**按钮。

注: 无法直接删除当前 EcoStruxure Automation Device Maintenance 会话中正在使用的设备证书。这些证书会临时移至**不可信证书**列表，并在 EcoStruxure Automation Device Maintenance 关闭后删除。

注: 执行此命令会从 Windows PC 中删除所选证书。此外，它们还将从 Windows **证书存储库**中删除。


在设备/加载选项卡中管理证书的信任状态

您还能够**在设备/加载选项卡中信任/取消信任设备证书。**

按照以下步骤，在**设备/加载**选项卡中信任设备证书：

步骤	操作
1	<p>单击设备的设备证书图标.</p>  <p>注: 您可以临时信任服务器证书。</p>
2	选中复选框 暂时信任当前会话的服务器证书 。
3	单击 信任服务器证书 。

按照以下步骤，在**设备/加载**选项卡中取消信任设备证书：

步骤	操作
1	单击设备的 设备证书 图标  。
2	单击 不信服务器证书 。

管理公钥基础设施 (PKI)

与应用程序证书注册相关的设置

如果在**设置**页的**安全**对话框中启用了**安全**选项，则 **PKI** 对话框会允许您配置到 Certification Authority (CA) 的连接，以便注册 EcoStruxure Automation Device Maintenance 的应用程序证书。

设置

全局

发现

DPWS

Modbus TCP

通讯

包设置

安全

证书管理

PKI

Syslog

日志

语言

组

项目

PKI

注册设置:

注册 URL:

发放机构 ID:

超时:

10000

毫秒

仅验证签名:

☐

检查连接

?

复位

确定

取消

应用

组成部分	描述
注册 URL	输入颁发证书的 Certification Authority (CA) 的统一资源定位符 (URL)。
发放机构 ID	输入证书发放机构的标识符。
超时	输入与您的互联网传输速率相对应的超时（毫秒）。 缺省值：10,000 毫秒
仅验证签名	如果未选择此选项，则 CA 证书必须是 Windows 证书存储库中的可信证书。 如要仅验证数字签名，请选择此选项。
检查连接按钮	单击检查连接按钮，可建立到 CA 网站的连接。
查看证书按钮	成功建立到 CA 的连接后，将显示查看证书按钮。 单击此按钮可打开证书信息对话框，并验证证书的属性，以帮助确保连接到正确的 CA。

如已成功建立到 CA 网站的连接，请选择**安全 > 证书管理**选项，然后注册应用程序证书。

激活 Syslog 消息记录

概述

Syslog 对话框让您能够激活 syslog 功能，并将 EcoStruxure Automation Device Maintenance 配置为 syslog 客户端。EcoStruxure Automation Device Maintenance 然后将使用在此对话框中配置的 syslog 设置，将其生成的部分日志消息提供到相应的 syslog 服务器。

设置

全局

发现

DPWS

Modbus TCP

通讯

包设置

安全

证书管理

PKI

Syslog


日志

语言

组


项目

Syslog

Syslog: ☐ 启用 ☒ 禁用 

服务器地址: 端口:

网络协议: ☐ UDP ☐ TCP ☒ TLS



激活 Syslog 消息记录

按照以下步骤激活 syslog 功能并配置到 syslog 服务器的连接：

步骤	操作
1	单击 主页 顶部中心位置处的 设置 菜单。
2	选择 安全 > Syslog 选项。
3	选择 启用 选项，激活 syslog 功能。
4	在 服务器地址 文本框中，输入 syslog 服务器的 IP 地址。
5	输入服务器为从客户端接收 syslog 消息而正在监视的 端口 。
6	选择 网络协议 选项： <ul style="list-style-type: none">• UDP（用户数据报协议）• TCP（传输控制协议）• TLS（传输层安全）
7	<p>对于 TCP 或 TLS 连接，您可以视需要单击检查连接按钮，以验证到 syslog 服务器的连接。</p> <p>结果：</p> <p>对于 TCP 连接：将显示一条消息，指示是否已建立到服务器的连接。</p> <p>对于 TLS 连接：</p> <ul style="list-style-type: none">• 将显示一条消息，指示是否已建立到服务器的连接。• 相应图标会指示 syslog 服务器的证书已被声明为可信。如果证书不可信，则单击 图标，打开证书信息对话框，此对话框可让您验证证书并将其声明为可信。 <p>注：由于 UDP 是基于无连接通讯模型的，因此 EcoStruxure Automation Device Maintenance 无法提供用于验证连接的解决方案。您必须手动验证是否在指定的服务器上接收了 syslog 消息。</p>

数据包

“数据包”选项卡

支持的数据包类型

支持以下文件类型：

- *.fwp
- *.idx
- *.sedp
- *.sedps

安全数据包

EcoStruxure Automation Device Maintenance 支持拥有数字签名的 *.sedps (Schneider Electric Data Package Secure) 数据包：启用保护模式后，EcoStruxure Automation Device Maintenance 将检查此包是否来自经验证的来源，并在签名不正确时显示安全通知。有关证书处理的概述，请参阅章节 [管理证书](#), 41 页。

如果激活了保护模式, 40 页，则适用以下规则：

- 以下包文件在**数据包**选项卡的包列表中标有黄色通知图标，右侧显示有消息**无法验证软件包信任链**：
 - 未签名的包文件。
 - 自签名包文件。
 - 正在使用不可信根证书的包文件。
- 这些包还在**设备/加载**选项卡中标有黄色通知图标。
- 如果尝试使用这些数据包中的某个数据包执行固件更新，则更新过程将暂停，并会在**通知区域**, 62 页中显示消息**无法验证所选软件包的信任链。如果下载，可能损坏设备。是否要继续？**。查看/确认消息, 62 页仔细阅读此消息，并评估风险。确认此消息后，该过程将继续。
- 如果尝试使用这些数据包执行固件更新，则在**日志窗口**, 63 页中会显示检测到的错误。

注意

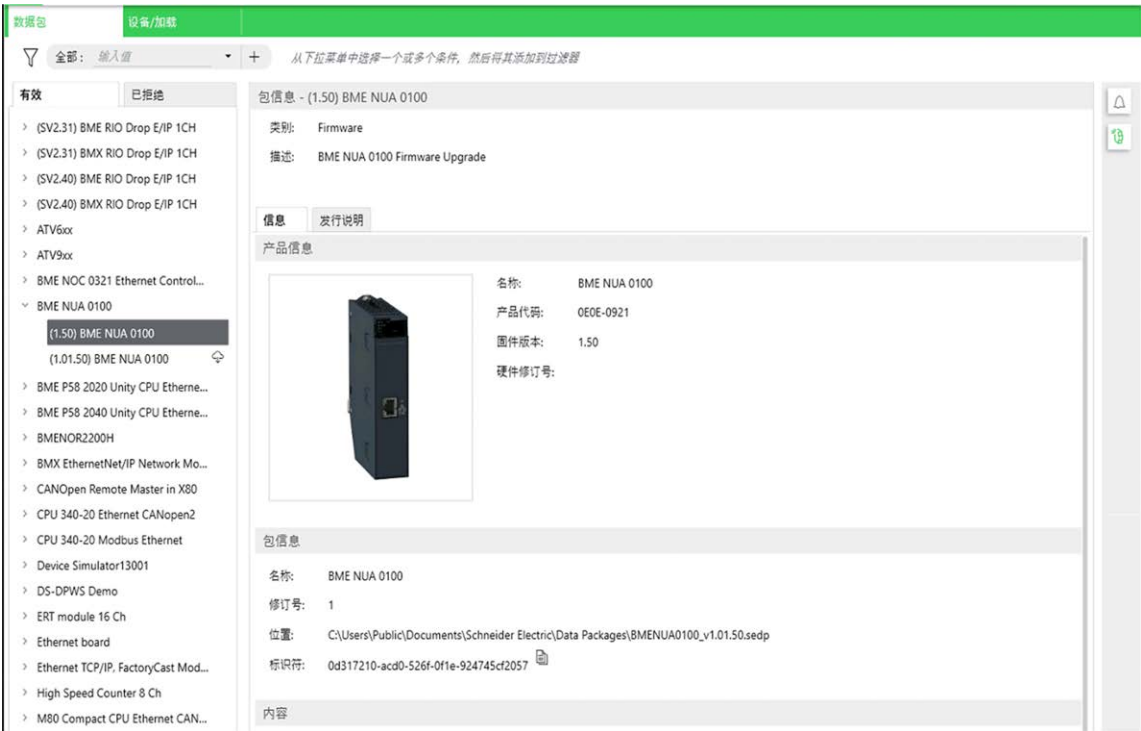
设备损坏

仔细检查数据包来源是否可信，否则下载被篡改的数据包可能会损坏您的设备。
不遵循上述说明可能导致设备损坏。

数据包选项卡概述

您可以查看数据包库的内容，找到具体数据包的详细信息及内容。

选项卡左侧以列表形式显示按设备系列分组的本地可用数据包。选项卡右侧显示所选数据包的详细信息。



数据包列表

左侧的数据包列表包含两个选项卡：

- **有效**选项卡列出了 PC 上按设备系列分组的本地可用数据包。
- **已拒绝**选项卡列出了已下载到 PC 但出于某种原因无法处理的数据包。由于数据包文件可能在下载过程中已受到破坏，它可以有助于再次执行下载。如果问题仍未解决，请联系 Schneider Electric 服务代表，获取更多帮助。

过滤数据包列表

为了减少列表中显示的数据包数量，可以应用搜索条件，具体如下：

步骤	操作
1	<p>在文本字段全部中输入一个字符串。如要基于特定数据包属性来限制搜索，可以选择性地打开列表，然后选择搜索条件。</p>
2	<p>单击搜索列表右侧的加号按钮，启动搜索。</p> <p>结果：数据包列表显示与所输入的搜索条件相符的条目。搜索框左侧显示一个黄色图标，指示过滤条件已应用并且列表条目由此缩减为符合搜索条件的那些数据包。</p>
3	<p>重复步骤 1 和 2，以定义另一个过滤条件。过滤条件通过“和”组合。</p> <p>结果：数据包列表显示同时符合这两个搜索条件的条目。</p>
4	<p>如要清除单个过滤条件，请单击此过滤条件的叉号按钮。</p> <p>或者，如要删除已定义的所有过滤条件，请单击清除所有过滤器链接。您将看到完整的数据包列表。</p>

包信息

左侧的**包信息**提供与数据包列表中选定的数据包有关的信息。

上部部分提供以下信息：

- **类别**
- **描述**

信息选项卡显示以下详细信息：

- **产品信息部分：**
 - 图片 - 如果数据包中提供
 - **名称**
 - **产品代码**
 - **固件版本**
 - **硬件版本**
- **包信息部分：**
 - **名称**
 - **版本**
 - **位置**
 - **标识符：** **复制到剪贴板**按钮让您能够将标识符字符串复制到 PC 的剪贴板。
- **内容部分：**提供列表中的数据包的内容。

如果数据包包含标示为 `ReleaseNotes` 的文档，则**发行说明**选项卡显示内容。如果数据包中不存在这类文档，此选项卡将为空。

设备/加载

设备/加载选项卡

概述

EcoStruxure Automation Device Maintenance 在**设备/加载**选项卡中显示一组特定设备属性（如设备名称、服务端点、固件版本）。

注: 只有在发现模式设置为**自动**时，才会自动更新此选项卡中所显示的信息。

单击工具栏中的  图标，即可显示最新值。



有关为设备显示的详细信息，请参阅章节 [设备/加载](#), 19 页。

登陆后可用的详细信息

在成功登录到设备且设备状态更改为绿色后，单击按钮，可访问每个设备的以下命令：

命令	描述
光信号	设备发出光信号，帮助您在支持此功能的设备的硬件机架中识别出该设备。
光信号和声音信号	设备发出光信号和声音信号，帮助您在支持此功能的设备的硬件机架中识别出该设备。
属性	<p>打开一个额外的属性对话框，其中以不同的选项卡提供了有关设备的其他信息：</p> <ul style="list-style-type: none"> • 设备信息选项卡提供有关设备的一般信息： <ul style="list-style-type: none"> ◦ 产品 ID ◦ 产品名称 ◦ 固件版本 ◦ 硬件版本 ◦ 硬件 ID ◦ MAC 地址 • 设备状态选项卡提供有关设备当前状态的信息。 • 配置选项卡提供有关设备配置设置的信息。如果设备支持，可在此选项卡中修改配置设置。 <p>注：修改配置设置后，可能需要重启设备，其作用可能相当于将控制器设置为“停止”状态。具体的效果由通知区域中显示的消息予以指示。仔细阅读每条消息，并在评估风险后确认。确认每条消息后，该过程将继续。</p> <p>所显示的属性信息取决于具体的设备。有关更多信息，请参阅您设备的用户文档。</p>

对设备列表中的设备分组

概述

EcoStruxure Automation Device Maintenance 让您能够通过创建组来组织设备列表中显示的设备。

EcoStruxure Automation Device Maintenance V3.0 通过定义 IP 地址范围，支持根据设备的 IP 地址进行分组。较新的 EcoStruxure Automation Device Maintenance 版本中可能提供了其他分组条件。

注: 此分组功能不支持 IPv4 地址。EcoStruxure Automation Device Maintenance V3.0 不支持 IPv6 标准。

创建组

按照以下步骤对设备分组：

步骤	操作
1	在 设置 页上，选择 组 选项。
2	展开 分组规则 列表，选择 网络区域 选项。
3	单击 + 添加 按钮，创建新地址范围。 结果： 将显示一个包含空行的表。
4	在 组名 单元格中，输入设备组的名称。
5	在 起始 IP 地址 单元格中，输入设备组地址范围的第一个 IP 地址。
6	在 结束 IP 地址 单元格中，输入设备组地址范围的最后一个 IP 地址。 <div></div>
7	单击 + 添加 按钮，创建其他组。 或者 单击 应用 ，应用 组 设置。 或者 单击 确定 ，应用所有应用程序设置修改并关闭 设置 对话框。

删除设备

概述

您可以在**设备/加载**菜单中的**设备列表**选项卡中暂时隐藏或永久丢弃设备，以此来达到删除设备的目的。

可以通过执行以下操作来删除设备：

- 隐藏活动的设备
- 丢弃活动的设备
- 丢弃隐藏的设备




隐藏活动的设备

按照以下步骤隐藏活动的设备：

步骤	操作
1	单击 设备/加载 选项卡。 发现的活动设备列出在 设备列表 选项卡下。
2	在 设备/加载 中： <ul style="list-style-type: none">• 通过单击设备行中的单元格，选择单个设备。或者• 通过选中每行左侧的复选框或选择整个组，来选择多个设备。
3	所选设备的以下图标会激活： <div><div> Hide</div><div>•</div><div> Dispose</div><div>•</div></div>
4	单击  Hide 图标。 然后便会显示 隐藏设备 消息。 <div><div>隐藏设备</div><div>×</div><div>!</div><div>确定要将所选择的设备移动至“隐藏设备列表”吗？</div><div>如已隐藏，您可以从“隐藏设备列表”中重新激活设备。</div><div>?</div><div>是</div><div>否</div></div>
5	单击 是 以继续。 所选设备被移动到 隐藏设备列表 选项卡。 注： 您可以从 隐藏设备列表 重新激活隐藏的设备。

取消对隐藏设备的隐藏

按照以下步骤取消对隐藏设备的隐藏：

步骤	操作
1	单击 设备/加载 选项卡。 发现的活动设备列出在 隐藏设备列表 选项卡下。
2	<ul style="list-style-type: none">通过单击设备行中的单元格，选择单个设备。或者通过选中每行左侧的复选框或选择整个组，来选择多个设备。
3	所选设备的以下图标会激活： <div> Unhide</div> <ul style="list-style-type: none"> <div> Dispose</div> <ul style="list-style-type: none">
4	单击  Unhide 图标。 所选设备被移动到 设备列表 选项卡。






丢弃活动的设备

按照以下步骤丢弃活动的设备：

步骤	操作
1	单击 设备/加载 选项卡。 发现的活动设备列出在 设备列表 选项卡下。
2	<ul style="list-style-type: none">通过单击设备行中的单元格，选择单个设备。或者通过选中每行左侧的复选框或选择整个组，来选择多个设备。
3	所选设备的以下图标会激活： <div> Hide</div> <ul style="list-style-type: none"> <div> Dispose</div> <ul style="list-style-type: none">
4	单击  Dispose 图标。 然后便会显示 丢弃设备 消息。 <div><div>丢弃设备</div><div> 确定要永久删除所选择的设备吗？ 设备被丢弃后，无法恢复。如果选择了自动发现，且设备在网络中仍然可达，则可以重新发现丢弃的设备。</div><div> <div>是</div> <div>否</div></div></div>
5	单击 是 以继续。 注： 选择 是 将使设备从工具中永久丢弃，如要使设备重新回到工具中，必须对其重新执行发现或手动添加。

丢弃隐藏的设备

按照以下步骤丢弃隐藏的设备：

步骤	操作
1	单击 设备/加载 选项卡。 发现的活动设备列出在 隐藏设备列表 选项卡下。
2	<ul style="list-style-type: none">通过单击设备行中的单元格，选择单个设备。或者通过选中每行左侧的复选框或选择整个组，来选择多个设备。
3	所选设备的以下图标会激活： <div><div> Unhide</div><div> Dispose</div></div>
4	单击  图标。 然后便会显示 丢弃设备 消息。 <div><div>丢弃设备</div><div> 确定要永久删除所选择的设备吗？ 设备被丢弃后，无法恢复。如果选择了自动发现，且设备在网络中仍然可达，则可以重新发现丢弃的设备。</div><div> <div>是 否</div></div></div>
5	单击 是 以继续。 注： 选择 是 将使设备从工具中永久丢弃，且无法恢复。

管理用户凭据



概述

EcoStruxure Automation Device Maintenance 让您能够为项目全局输入设备授权访问所需的凭据，以及为每个设备单独输入这些凭据。


全局管理用户凭据

如要全局管理项目的用户凭据，请转到**设置**页，然后选择**项目 > 用户凭据设置**选项。





选择**身份验证类型 > 用户名**或**身份验证类型 > 自定义**，然后根据需要输入凭据。单击**确定**，保存凭据。因此，**设备/加载**页中适用设备的**设置凭据**图标将变为黄色，您可以单击**连接**图标  或按钮  **连接**，在无需重新输入凭据的情况下登录。

管理每个设备的用户凭据

如要单独管理每个设备的用户凭据，请打开**设备/加载**页，然后单击表格的设备行中的**设置凭据**图标 ：



您可以单击**保持并连接**，保存凭据并建立到设备的连接。成功登录后，**设置凭据**图标变为绿色。或者，您也可以单击**保存**，保存此设备的凭据以供日后登录之用。在这种情况下，**设置凭据**图标变为黄色，您可以单击**连接**图标  或按钮  **连接**，在无需重新输入凭据的情况下登录。

用户凭据参数

所显示的参数是设备特有的，应请求登录到特定设备所需的凭据。有关更多信息，请参阅您设备的用户文档。

如要登录到 Modicon M340、Modicon M580 或 Momentum 控制器，需要输入三个密码。有关应用程序保护密码、数据存储密码和固件保护密码的详细信息，请参阅 *EcoStruxure Control Expert Operating Modes* or the legacy *Unity Pro Operating Modes manual* 中的相应章节。本手册翻译版的下载链接见本在线帮助中的“相关文档” 9 页列表。

访问扩展模块

概述



设备/加载选项卡设备列表中的模块化设备提供了让您能够对设备的具体扩展模块进行访问的链接。

模块化设备示例：

数据名		设备/功能								
设备列表		网络设备列表								
<input type="checkbox"/>	状态	设备名称 原型型号	服务端点 序列号	固件版本	安全配置 版本	模式	更新中心信息		扩展名	操作
<input type="checkbox"/>	设备列表查看 (5)									
<input checked="" type="radio"/>		ATV630U07M3_441e60 CR: ATV630U07M3	https://T2.20.176.443 SN: 4002-2000H-L64787000N	3.5I594804	-	-			-	
<input checked="" type="radio"/>		ATV630EIP SN: 4002-2000G-L64787000N	mbsp://T2.20.170.209.502 SN: 4002-2000G-L64787000N	2.6I594813	-	STOP			扩展名	

如果设备支持，则**扩展链接** (**扩展名**) 会打开新的**扩展**选项卡，并提供按**扩展分**组的模块化设备。

数据名	设备/地址	扩展名				
ATV630EP						
ATV630EP	mbapp//172.20.170.209-562 CR: ATV630U07M3 SN: 4004000HL44715401Y 固件版本: 2.6IE94B13					更新中心
0						
状态	设备名称 商业型号	服务器点 序列号	固件版本	更新中心信息		操作
<input type="checkbox"/>	● EtherNet/IP ModbusTCP module CR: VW3A3721	1 SN:	1.8IE13B02			更新

通过这两个选项卡可以（通过**更新中心**图标  或**更新中心**按钮  **更新中心**）访问**更新中心**对话框，该对话框让您能够通过**固件**按钮选择固件数据包。

对于无法通过单击**扩展**链接按需加载扩展模块的设备，请按照下一节中所述的方式访问各个扩展模块。

手动访问扩展模块

对于无法通过单击**扩展**链接按需加载扩展模块的设备，请执行以下操作：

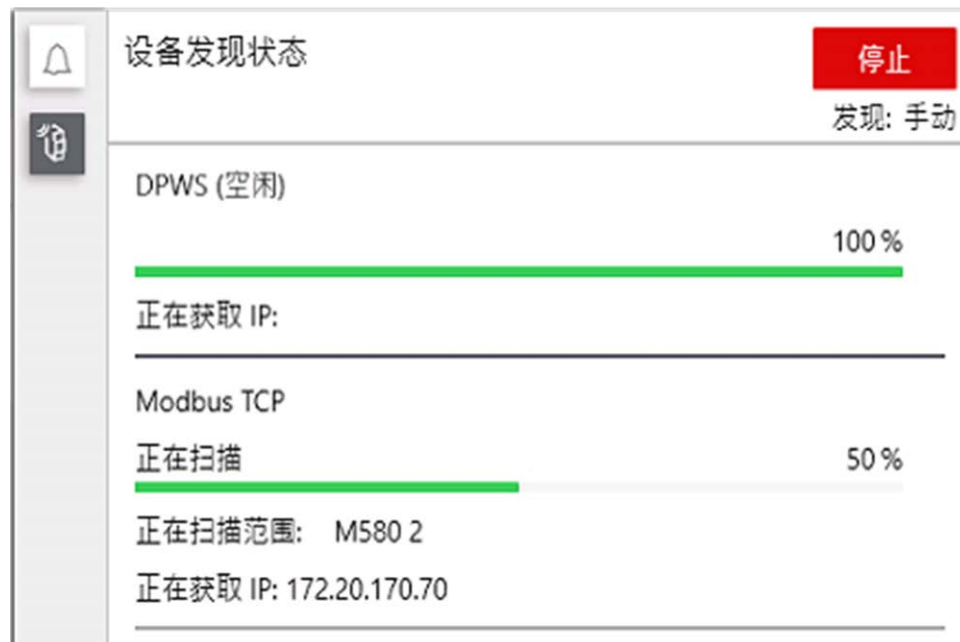
步骤	操作														
1	<p>单击模块化设备中的扩展链接。</p> <p>结果：扩展选项卡随即打开。如果设备无法通过单击扩展链接按需加载扩展模块，则会提供添加按钮。</p>														
2	<p>单击添加按钮或链接未找到模块。如要添加模块，请单击此处。</p> <p>结果：添加模块对话框随即打开。</p>														
3	<p>在添加模块对话框中，配置用于访问设备扩展模块的参数：</p> <ul style="list-style-type: none">• 机架编号• 插槽号														
4	<p>单击确定按钮，启动发现扫描。</p> <p>成功检测到扩展模块后，将显示扩展选项卡。</p> <div><div><div>数据总览</div><div>设备/加载</div><div>扩展名</div></div><div><div>ATV630EIP</div><div><div>ATV630EIP</div><div>mbap://172.20.170.209:502</div><div>CR: ATV630U07M3</div><div>SN: 4004000HL44718401Y</div><div>固件版本: 2.6IE94813</div><div>更新中心</div></div><div><div>0</div><table><thead><tr><th></th><th>状态</th><th>设备名称 商业型号</th><th>服务端点 序列号</th><th>固件版本</th><th>更新中心信息</th><th>操作</th></tr></thead><tbody><tr><td><input type="checkbox"/></td><td><div></div></td><td>EtherNet/IP, ModbusTCP module CR: VW3A3721</td><td>1 SN:</td><td>1.8IE13802</td><td></td><td><div>上传</div><div>下载</div></td></tr></tbody></table></div></div></div>		状态	设备名称 商业型号	服务端点 序列号	固件版本	更新中心信息	操作	<input type="checkbox"/>	<div></div>	EtherNet/IP, ModbusTCP module CR: VW3A3721	1 SN:	1.8IE13802		<div>上传</div> <div>下载</div>
	状态	设备名称 商业型号	服务端点 序列号	固件版本	更新中心信息	操作									
<input type="checkbox"/>	<div></div>	EtherNet/IP, ModbusTCP module CR: VW3A3721	1 SN:	1.8IE13802		<div>上传</div> <div>下载</div>									
5	<p>关闭扩展选项卡。</p>														

监视设备发现状态

概述

设备发现过程正在运行时，可以单击**设备/加载**选项卡中的按钮，获取此过程的状态。

在右侧会打开**设备发现状态**视图：



它显示以下信息：


- 为每个扫描器单独提供进度信息。
- 如果为扫描器配置了不同的范围，则为每个范围单独提供进度信息（比如，对于 Modbus TCP 扫描器, 32 页）。

启动/停止按钮让您能够启动手动设备发现，或者直接从该视图停止正在运行的设备发现过程。

查看/确认消息

概述

EcoStruxure Automation Device Maintenance 执行的某些过程需要用户交互。每当需要确认时，会暂停过程（如，更新固件），并在通知区域中显示相应消息。仔细阅读每条消息，并在评估风险后确认。确认每条消息后，该过程将继续。

如要打开通知区域，请单击设备/加载选项卡中的  按钮。

数据包

设备/加载

设备列表

⊕ 添加

🔌 连接

🔌 断开连接

🔄 更新中心

🔍 隐藏

🗑 丢弃

▼

<input type="checkbox"/>	状态	设备名称 商业型号	服务端点 序列号	固件版本	安全配置 版本	模式	更新中心信息
<input checked="" type="checkbox"/>		BME NOC0321 CR: BME NOC0321	ftp://172.20.170.62:21 SN:	01.06 IR 2	-	需要确认	已选择固件
<input type="checkbox"/>		140*** CR: 140***	https://172.20.170.72:443 SN:	-	-	-	
<input type="checkbox"/>		BMEP586040_21190100014 CR: BMEP586040	https://[fe80::280:f4ff:fe20:cde0]:443 SN: 21190100014	4.01.28	-	-	
<input type="checkbox"/>		ATV930U07M3_b3a CR: ATV930U07M3	mbap://172.20.170.213:502 SN: 4030000HL704004007	3.5IE94B01	-	-	
<input type="checkbox"/>		ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B04	-	-	
<input type="checkbox"/>		BMED581020-test CR: BMED581020	https://[fe80::280:f4ff:fe28:4142]:443 SN: 21212711508	22.0.22152	-	-	
<input type="checkbox"/>		BME P58 2020 CR: BME P58 2020	ftp://172.20.170.60:21 SN:	02.90 IR 5	-	-	
<input type="checkbox"/>		M251D CR: TM251MDESE	https://[fe80::280:f4ff:fe0b:5470]:443 SN: PROD0006115	22.0.2215...	-	-	
<input type="checkbox"/>		ATV630U07M3 CR: ATV630U07M3	mbap://[fe80::280:f4ff:fec2:3639%1... SN: 18c23639	3.5IE94B02	-	-	
<input type="checkbox"/>		ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	

通知区域

安全提示

☒ BME NOC0321
ftp://172.20.170.62:21

在将数据传输到 PLC 之前，请确保连接到了正确的设备。方法是检验在“固件”选项卡上显示的 PLC 地址和 MAC 地址。如果将数据传输到不正确的设备，则可能导致与过程进行危险的交互。

要继续数据传输吗？

确认

拒绝

摘要

更新

取消

- 通知区域中可以显示两种不同类型的消息：
- 确认消息：通过激活复选框的方式选择消息，然后单击**确认**以确认消息并恢复运行过程，或者单击**拒绝**以停止过程。
 - 通知消息：通过激活复选框的方式选择消息，然后单击**确定**以确认消息并恢复运行过程。
- 不显示通知**选项让您能够禁用通知消息显示。如果选择了此选项，将假设消息已确认，在不需要为用户交互而中断的情况下，自动执行过程。
- 注:** 仅当您在维护模式下工作且操作员已验证机器或过程环境的安全状态时，才激活此选项。

查看日志


您可以查看存储的日志并对其进行分析以便获得所选设备的详细信息。


日志信息可以在以下部分中查看：

- 如需查看每个设备的日志信息，可在**设备/加载**页中查看
- 如需查看整个项目的日志信息，可在**日志**窗口中查看

注：在**日志**窗口中，在单个窗口中显示检测到的错误、检测到的警告以及信息消息。

如要查看选定设备专有的日志，请执行以下操作：

步骤	操作
1	访问 设备/加载 页。
2	单击设备的 设备日志 图标  。 结果： 在表格中设备行下方直接打开一个小的 日志信息 视图。如有必要，可使用右侧的滚动条查看所有日志条目。

如要隐藏设备的**日志信息**，请再次单击**设备日志**图标 。

增强网络安全的建议

日志文件通常包含敏感数据，例如


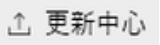
- 设备地址
- 设备名称
- 网络拓扑详细信息
- 网络配置详细信息

这些数据存储在您 PC 的硬盘上。如果不再需要日志文件，请尽快删除，或者将其存放在安全位置，仅允许经过授权的访问。

更新中心

概述

更新中心对话框让您能够为固件更新或安全配置文件更新配置相关设置。这些配置设置可同时应用于单一设备或不同设备。

- 如要对单一设备执行更新，请在**设备/加载**选项卡中，单击表格设备行中的**更新中心**图标 。
- 如要同时对项目的不同设备执行更新，请在**设备/加载**选项卡中选择设备，然后单击按钮栏中的**更新中心**按钮 。

更新中心对话框

这两个操作都会打开**更新中心**对话框，让您能够选择：

- **固件**：用于配置相关设置，以便为所选设备执行固件更新。有关更多信息，请参阅 [更新固件](#), 64 页。
- **安全**：用于配置相关设置，以便为所选设备执行安全配置文件更新。有关更多信息，请参阅 [更新安全配置文件](#), 66 页。
- **复位**：用于复位所选设备的更新设置。

如要确认设置并关闭**更新中心**对话框，请单击**保存**按钮。因此，在**设备/加载**选项卡, 19 页的设备**更新中心信息**单元格中会指示所做的配置。

如要按配置的方式执行更新过程，请单击**更新**按钮。

更新固件

概述

EcoStruxure Automation Device Maintenance 让您能够对**设备/加载**选项卡中显示的设备执行固件更新。


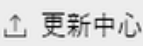


如要更新模块化设备的固件，可以按照章节 [访问扩展模块](#), 59 页 中所述那样，访问具体的扩展模块。

可以为多个扩展模块和/或机架模块选择数据包。EcoStruxure Automation Device Maintenance 将同时更新这些设备的固件。

注：如果同时更新控制器和模块，请确保在模块更新仍在运行时不重启控制器。请参见下面的重要风险说明。

更新固件

如要更新固件，请执行以下步骤：

步骤	操作
1	访问 设备/加载 页。
2a	如要对具体的设备执行更新，请单击设备行中的 更新中心 图标  。
2b	如要同时对项目的不同设备执行更新，请选中设备的复选框或选中整个 组 的复选框，然后单击按钮栏中的 更新中心 按钮  。
3	在 更新中心 对话框中，单击 固件 按钮。
4	在 固件 对话框中，为每个设备选择固件数据包。 <div></div>
5	单击 保存 ，保存固件更新配置并关闭 固件 对话框。 结果： 设备/加载 选项卡, 19 页中的 更新中心信息 单元格或者一个或多个设备的单元格显示文本 已选择固件 。
6	单击 设备/加载 选项卡中的 更新 按钮，启动更新过程。 结果： 显示 更新确认 对话框。 <div></div>
7	在 更新确认 对话框中，仔细查看选择用于更新的设备的列表，并验证您所做的设置。
8	单击 确认 按钮，启动更新过程。 结果： 更新固件过程启动。每当需要用户交互时，会暂停此过程，并在 通知区域 , 62 页中显示相应消息。仔细阅读每条消息，并在评估风险后确认。确认每条消息后，该过程将继续。
9	固件更新过程成功完成后，单击 EcoStruxure Automation Device Maintenance 底部的 汇总 按钮, 17 页，显示 Update Summary （更新汇总）对话框。它提供与每个设备的更新状态有关的信息，这些信息指示上一个版本和目标版本以及数据包/文件。

<div>注意</div> <div>设备损坏</div> <div>请勿关闭 PC 或应用程序，并确保在固件更新过程中 PC 不进入睡眠模式，否则该过程将中断，进而可能损坏设备。</div> <div>不遵循上述说明可能导致设备损坏。</div>
--

您可以视需要选中复选框**我确认，系统处于维护模式，且我希望禁用所有安全消息以便执行这个更新操作。**这有助于防止过程暂停。

注: 仅当您在维护模式下工作且操作员已验证机器或过程环境的安全状态时，才激活此选项。

固件更新过程成功完成后，对于控制器，可以视需要单击**设备/加载**选项卡, 19 页中的**启动设备**图标，以启动设备。

注: 安装或更新后，在使用电气控制和自动化设备进行常规操作之前，应执行启动测试。有关更多信息，请参阅 **启动与测试**, 6 页。

更新安全配置文件


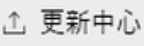
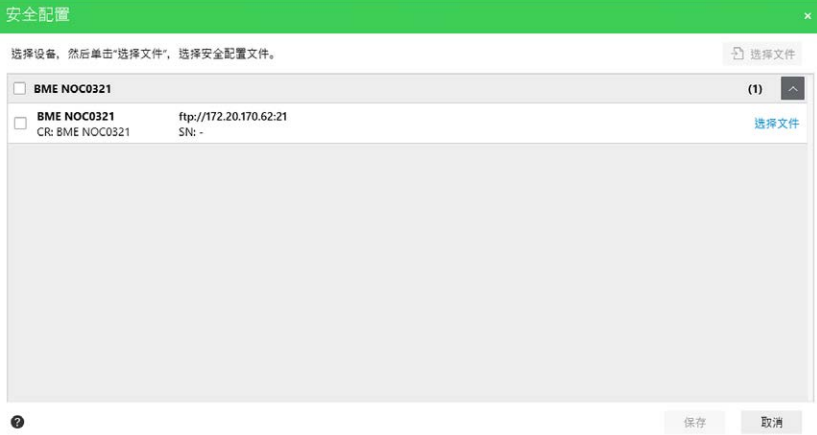
概述

EcoStruxure Automation Device Maintenance 让您能够更新安全配置文件，该文件包含在 EcoStruxure Cybersecurity Admin Expert 应用程序中为网络全局配置的安全配置设置。

注: 新安全配置文件可以为设备分配新凭据。将来登录时，将需要输入新凭据。

更新安全配置文件

如要更新安全配置文件，请执行以下步骤：

步骤	操作
1	访问设备/加载页。
2a	如要对具体的设备执行更新，请单击设备行中的 更新中心 图标  。
2b	如要同时对项目的不同设备执行更新，请选中设备的复选框或选中整个 组 的复选框，然后单击按钮栏中的 更新中心 按钮  。
3	在 更新中心 对话框中，单击 安全 按钮。
4	<p>在安全配置对话框中，选择具体的设备，然后单击此设备的选择文件链接或选择多个设备，然后单击对话框上部的选择文件按钮。</p>  <p>结果：显示 Windows 文件打开对话框，让您能够在网络上浏览安全配置文件。</p>
5	<p>选择安全配置文件，然后单击打开按钮。</p> <p>结果：安全配置对话框显示包含所选文件的设备。</p>
6	<p>单击保存按钮，保存配置并关闭安全配置对话框。</p> <p>结果：设备/加载选项卡, 19 页中的更新中心信息单元格或者一个或多个设备的单元格显示文本已选择安全配置。</p>
7	<p>单击设备/加载选项卡中的更新按钮，启动更新过程。</p> <p>结果：显示更新确认对话框。</p>
8	在 更新确认 对话框中，仔细查看选择用于更新的设备的列表，并验证您所做的设置。
9	<p>单击确认按钮，启动更新过程。</p> <p>结果：更新过程启动。每当需要用户交互时，会暂停此过程，并在通知区域, 62 页中显示相应消息。仔细阅读每条消息，并在评估风险后确认。确认每条消息后，该过程将继续。</p>

注意

设备损坏

请勿关闭 PC 或应用程序，并应确保在固件更新过程中 PC 不进入睡眠模式，否则该过程将中断，进而可能损坏设备。

不遵循上述说明可能导致设备损坏。

您可以视需要选中复选框**我确认，系统处于维护模式，且我希望禁用所有安全消息以便执行这个更新操作**。这有助于防止过程暂停。

注：仅当您在维护模式下工作且操作员已验证机器或过程环境的安全状态时，才激活此选项。

网络安全

简介

网络安全是一种网络管理分支，用于应对在计算机系统上或由计算机系统发起的攻击，这些攻击会通过计算机网络执行，可以导致意外或故意的破坏。网络安全的目的在于，帮助提升信息和物理资产的保护级别，以免遭受盗窃、破坏、滥用或发生事故，同时保证其预期用户的访问和使用。

没有哪一种网络安全方法能够单独满足需求。Schneider Electric 推荐采用深度防御方法。本方法由 National Security Agency (NSA) 提出，将网络分为安全功能、设备和流程三层。此方法的基本组成部分包括：

- 风险评估
- 基于风险评估结果而建立的安全计划
- 多阶段培训活动
- 使用控制区 (DMZ) 将工业网络从企业网络中进行物理分离，并使用防火墙和路由建立其他安全区域
- 系统访问控制
- 设备加强
- 网络监控和维护

本章定义有助于您配置不易受到网络攻击影响的系统的要素。有关深度防御方法的详细信息，请参阅系统技术说明：我如何...降低 Schneider Electric website 遭受的网络攻击风险。

什么是网络安全？

概述

网络威胁是指可破坏计算机系统和网络正常操作的蓄意行为或意外行为。这些行为可在物理设施内或从外部位置发起。控制环境的安全挑战包括：

- 各种物理和逻辑界限
- 多个站点和较大的地理范围
- 对流程可用性安全实施的负面影响
- 随着业务控制的通讯越来越开放，从业务系统到控制系统的迁移越来越容易接触蠕虫和病毒
- 通过 USB 设备、供应商和服务专员的笔记本电脑以及企业网络越来越多地接触恶意软件
- 控制系统对物理和机械系统的直接影响

网络攻击的来源

实施考虑网络攻击和意外的各种潜在来源的网络安全计划，包括：

源极	描述
内部	<ul style="list-style-type: none"> • 员工或合同工的行为不当 • 员工或合同工不满
外部机会（非指引）	<ul style="list-style-type: none"> • 脚本小子* • 消遣型黑客 • 病毒编写人员
外部故意（受引导）	<ul style="list-style-type: none"> • 犯罪团体 • 积极分子 • 恐怖分子 • 外国机构
意外	
*黑客的俗称，他们使用他人编写的恶意脚本，而不必全面理解脚本的运行方式及其对系统的潜在影响	

可能启动对控制系统的蓄意网络攻击，以实现大量的恶意结果，包括：

- 通过阻止或延迟信息流来破坏生产流程
- 损坏、禁用或关闭设备，对生产或设备产生负面影响
- 修改或禁用安全系统，导致刻意的损坏

攻击者如何获得访问权限

网络攻击者绕过周边防御，可获得对控制系统网络的访问权限。访问的共同点包括：

- 拨号接入远程终端 (RTU) 设备
- 供应商访问点（如技术支持访问点）
- IT 控制的网络产品
- 公司虚拟专用网络 (VPN)
- 数据库链接
- 防火墙配置不佳
- 对等实用工具

网络安全认证

Schneider Electric 基于以下建议制定了网络安全指南：

- Achilles
- ISA Secure

有关疑问、资讯或漏洞报告问题

如要提交网络安全问题，请获取 Schneider Electric 最新资讯，或者如要报告漏洞问题，请访问我们的 [website](#)。

Schneider Electric 指南

简介

您的 PC 系统可运行各种应用程序来增强您的控制环境中的安全性。系统具有出厂默认设置，要求重新配置以与 Schneider Electric 的深度防御方法的设备加强建议保持一致。

下面的指南介绍了 Windows 操作系统中的流程。这些仅作为示例提供。您的操作系统和应用程序可能有不同的要求或流程。

加强工程工作站

客户会选择各种商业 PC 系统，满足自己的工程工作站需求。关键的加强技术包括：

- 强大的密码管理。
- 用户帐户管理。
- 应用到应用程序和用户帐户的最低特权方法。
- 删除或禁用不需要的服务。
- 删除远程管理特权。
- 系统补丁管理。

禁用未使用的网络接口卡

验证是否禁用应用程序不需要的网络接口卡。例如，如果您的系统有 2 个网络卡，且应用程序只使用一个，则验证是否禁用另一个网络卡（本地连接 2）。

在 Windows 中禁用网卡：

步骤	操作
1	打开 控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置 。
2	右键单击未使用的连接。选择 禁用 。

配置局域连接

各种 Windows 网络设置可增强与 Schneider Electric 建议的深度防御方法一致的安全性。

在 Windows 系统中，通过打开**控制面板 > 网络和 Internet > 网络和共享中心 > 更改适配器设置 > 本地连接 (x)** 来访问这些设置。

以下列表是您可能在**本地连接属性**屏幕上对系统进行的配置更改的示例：

- 禁用各个网络卡上的所有 IPv6 堆栈。（本系统示例不要求 IPv6 地址范围，禁用 IPv6 堆栈可限制导致 IPv6 潜在安全风险的漏洞。
- 禁用**Microsoft 网络的文件和打印机共享**。

Schneider Electric 的深度防御建议还包括以下内容：

- 仅定义静态 IPv4 地址、子网掩码和网关。
- 在控制室内不要使用 DHCP 或 DNS。

管理 Windows 防火墙

Schneider Electric 的深度防御方法建议包括在所有系统电脑上启用 Windows 主机防火墙。为列出的任何公共或私有配置文件启用防火墙。

建议的做法是用户定义防火墙，拒绝连接到未知/不受信任的外部主机或拒绝来自这类主机的连接。

禁用远程桌面协议

Schneider Electric 的深度防御方法建议包括禁用远程桌面协议 (RDP)，除非您的应用程序需要 RDP。

如要禁用 Windows 10 系统的协议，请执行以下操作：

步骤	操作
1	右键单击 Windows 开始 按钮，然后执行 系统 命令。
2	从 设置 菜单，执行 远程桌面 命令。
3	在 远程桌面 视图中，关闭 启用远程桌面 （切换到 关 ）。

对于其他 Windows 操作系统，请执行与之相当的操作。

更新安全策略

通过命令窗口中的 `gpupdate` 更新您系统中与 PC 相关的安全策略。有关详细信息，请参考与 Microsoft 相关的 `gpupdate` 文档。

禁用 LANMAN 和 NTLM

Microsoft LAN Manager 协议（LANMAN 或 LM）及其后续 NT LAN Manager (NTLM) 具有使其在控制应用程序中的使用不合适的漏洞。

以下步骤介绍了如何在 Windows 系统中禁用 LM 和 NTLM：

步骤	操作
1	在命令窗口中，执行 <code>secpol.msc</code> 以打开 本地安全策略 窗口。
2	打开 安全设置 > 本地策略 > 安全选项 。
3	选择 仅发送 NTLMv2 响应 。在 网络安全 中 拒绝 LM 和 NTLM：LAN Manger 验证级别 字段。
4	选择 网络安全：不要在下次更改密码时存储 LAN Manager 的哈希值 复选框。
5	在命令窗口中，输入 <code>gpupdate</code> 以提交更改的安全策略。

管理更新

部署前，使用 Microsoft **Windows 更新** Web 页面上的实用程序更新所有 PC 的操作系统。要在 Windows 中访问此工具，请选择**开始 > 所有程序 > Windows 更新**。

数字签名验证

检查下载后的 EcoStruxure Automation Device Maintenance 完整性

从 Schneider Electric 网站下载 EcoStruxure Automation Device Maintenance 可执行文件后，通过执行以下步骤验证文件的完整性：

步骤	操作
1	右键单击 AutomationDeviceMaintenance.exe 文件，从上下文菜单执行 属性 命令。
2	在 AutomationDeviceMaintenance.exe Properties 对话框中，选择 数字签名 选项卡。
3	从 签名列表 中选择 Schneider Electric USA, INC. 条目，然后单击 详细信息 按钮，查看 数字签名详细信息 。
4	在 数字签名详细信息 对话框中，确保显示信息 此数字签名正常 。。

现在，您可以双击 .exe 文件已启动 EcoStruxure Automation Device Maintenance。

在启动期间验证组件

启动 EcoStruxure Automation Device Maintenance 时，会扫描每个已加载的动态链接库 (DLL)，以检查它是否可信。这是抵御网络攻击和提高信任级别的内置安全功能。

检测到不可信组件时怎么办

如果检测到不可信组件，则会中止启动 EcoStruxure Automation Device Maintenance，并显示一条消息，指示检测到异常。

在这种情况下，您有以下选择：

- 重新安装 EcoStruxure Automation Device Maintenance。
- 如果您认为此异常不大可能由网络攻击造成，请查阅 Schneider Electric Cybersecurity services portal，获取更多建议或帮助。

如要查找导致问题的组件，可以使用调试工具，如 WinDbg：启动调试工具，启动 EcoStruxure Automation Device Maintenance，并观察日志文件内容中是否有条目指示无法确定 DLL 的代码签名的有效性。

需要手动卸载的文件

概述

卸载 PC 上的 EcoStruxure Automation Device Maintenance 时，程序文件会自动删除，但是需要单独处理一些用户特有文件，以避免网络安全问题。

EcoStruxure Automation Device Maintenance 设置文件

EcoStruxure Automation Device Maintenance 设置文件 *AutomationDeviceMaintenanceSettings.emes* 由 EcoStruxure Automation Device Maintenance 创建，用于存储在**设置**对话框中执行的配置（例如，Modbus TCP 扫描范围或发现设置）。卸载 EcoStruxure Automation Device Maintenance 时，它不会从 PC 中删除，而是需要手动删除。

使用 Windows 资源管理器或其他文件系统工具，将其从文件夹 %APPDATA%\Schneider Electric\Automation Device Maintenance\ 中删除。

证书

卸载 EcoStruxure Automation Device Maintenance 时，将从 Windows PC 中删除 EcoStruxure Automation Device Maintenance 证书以及在**安全 > 证书管理**（另请参阅 **证书管理**对话框, 42 页）下方的**设置**对话框中管理的**可信证书**和**不可信证书**。此外，它们还将从 Windows 证书存储库中删除。

数据包

在卸载 EcoStruxure Automation Device Maintenance 时，不会从 PC 中删除本地保存的数据包, 18 页。数据包缺省存储在文件夹 %PUBLIC%\Public Documents\Schneider Electric\Data Packages 中。您可以在**设置 > 包设置**对话框, 35 页中配置具体的路径。

使用 Windows 资源管理器或其他文件系统工具，手动删除缺省文件夹或所配置的文件夹。

EcoStruxure Automation Device Maintenance 项目文件

卸载 EcoStruxure Automation Device Maintenance 时，不会从 PC 中删除 EcoStruxure Automation Device Maintenance 项目文件。搜索文件扩展名为 *.emep 的文件，并手动将其删除，或将其存储在安全位置以备日后使用，在这个安全位置，未经授权，无法访问这些文件。

日志文件

卸载 EcoStruxure Automation Device Maintenance 时，不会从 PC 中删除已本地保存到**设置 > 日志**对话框, 36 页中指定的路径的日志文件。使用 Windows 资源管理器或其他文件系统工具，手动删除文件夹，或者将日志文件存储在安全位置以备日后使用，在这个安全位置，未经授权，无法访问这些文件。

EcoStruxure Automation Device Maintenance 使用的组件

概述

EcoStruxure Automation Device Maintenance 提供了组件和当前版本的概览。如果检测到异常，则此组件和版本列表可有助于查找可能造成此异常的组件。

检索组件列表

如要检索由 EcoStruxure Automation Device Maintenance 加载的组件列表，请执行以下操作：

步骤	操作																																	
1	<p>单击工具栏上的关于按钮。</p> <p>结果：关于对话框随即打开。</p>																																	
2	<p>单击组件信息链接。</p> <p>结果：组件信息对话框随即打开。</p> <div><div>关于</div><div><div>组件信息</div><table><tr><th>组件名称</th><th>版本</th><th>描述</th></tr><tr><td>AutomationDeviceMaintenance</td><td>3.0.154.0</td><td>General</td></tr><tr><td>BrandIdentity</td><td>4.19.0.2175</td><td>General</td></tr><tr><td>ServiceCommon</td><td>3.1.3.0</td><td>General</td></tr><tr><td>log4net</td><td>2.0.11.0</td><td>General</td></tr><tr><td>PackageCommon</td><td>3.0.4.0</td><td>General</td></tr><tr><td>Org.Schneider.FWChecker</td><td>2.5.2.0</td><td>General</td></tr><tr><td>Org.Schneider.Crypto</td><td>2.5.2.0</td><td>General</td></tr><tr><td>Asn1Parser</td><td>2.5.2.0</td><td>General</td></tr><tr><td>SE.CS.PKI.Common</td><td>1.0.6.0</td><td>General</td></tr><tr><td>PackageDescriptionLibrary</td><td>3.1.1.0</td><td>General</td></tr></table><div>返回到关于页面 复制详情</div><div>Life Is On </div><div>确定</div></div></div>	组件名称	版本	描述	AutomationDeviceMaintenance	3.0.154.0	General	BrandIdentity	4.19.0.2175	General	ServiceCommon	3.1.3.0	General	log4net	2.0.11.0	General	PackageCommon	3.0.4.0	General	Org.Schneider.FWChecker	2.5.2.0	General	Org.Schneider.Crypto	2.5.2.0	General	Asn1Parser	2.5.2.0	General	SE.CS.PKI.Common	1.0.6.0	General	PackageDescriptionLibrary	3.1.1.0	General
组件名称	版本	描述																																
AutomationDeviceMaintenance	3.0.154.0	General																																
BrandIdentity	4.19.0.2175	General																																
ServiceCommon	3.1.3.0	General																																
log4net	2.0.11.0	General																																
PackageCommon	3.0.4.0	General																																
Org.Schneider.FWChecker	2.5.2.0	General																																
Org.Schneider.Crypto	2.5.2.0	General																																
Asn1Parser	2.5.2.0	General																																
SE.CS.PKI.Common	1.0.6.0	General																																
PackageDescriptionLibrary	3.1.1.0	General																																
3	<p>单击复制详细信息链接，将组件和版本列表复制到剪贴板。</p> <p>现在，您可以将内容粘贴到 *.txt 文件，以便对特定组件和相应版本执行搜索操作。</p>																																	

术语

产品 ID:

产品标识符，用于识别设备所属的产品系列。

数据包，固件包:

数据包是用于在工具与设备之间交换内容的文件。它可以是 SEDP 格式。数据包包含固件包，但还可以包含配置、PLC 应用程序等。

设备发现:

自动检测设备以及这些设备在计算机网络中提供的服务。

设备系列:

一系列类型相似的设备，每个设备系列由产品 ID 来识别。

设备证书:

一种 X.509 公共密钥证书，被工具和设备用来建立安全通讯通道（如：HTTPs）。

D

DHCP: 动态主机配置协议

DNS: 域名系统

DPWS:

Web 服务设备配置文件，是用于发现和描述支持 Web 服务的设备的标准。

H

HTTP:

超文本传输协议

HTTPs:

安全超文本传输协议，又称为基于 TLS 的 HTTP。

I

ICS: 工业控制和系统

IEC:

（国际电工委员会）负责为所有电器、电子和相关技术制定和发布国际标准的非盈利性和非政府性的国际标准组织。

IP 地址:

根据 IP 协议标准的设备地址。它可为 IPv4 或 IPv6 地址格式。

IP:

互联网协议

ISO: 国际标准化组织

N

NEMA:

（美国国家电气制造商协会）负责制定各种类型的电气机箱的性能标准。NEMA 标准涉及防腐蚀、防雨淋和防淹没等性能。对于 IEC 成员国家，IEC 60529 标准还对机箱的入口防护等级进行了分类。

O

OPC UA:

OPC 统一架构：OPC UA 是工业自动化领域安全可靠数据交换的互操作性标准。它是一种平台中立的通讯协议，采用客户端/服务器模型。客户端与服务器之间的连接普遍基于可靠的传输层协议（TCP，传输控制协议）。

有关 OPC（尤其是 OPC UA）的更多信息，请参阅 OPC Foundation 官网 <https://opcfoundation.org>。

P

PLC:

（可编程可编程控制器）用于自动化制造、工业和其他机电进程的工业计算机。此外，PLCs 与普通计算机不同，因为这些计算机拥有多个输入和输出数组，并且符合冲击、振动、温度和电气干扰的更强大的规范。

POU:

（程序组织单元）源代码的变量声明和相应的指令集。POUs 有助于简化软件程序、功能和功能块的模块化重用。经过声明后，POUs 便可相互使用。

S

SEDP:

Schneider Electric 数据包，用于在软件工具与设备之间交换内容的标准化文件格式。

T

TCP:

传输控制协议

TLS:

传输层安全

U

UDP: 用户数据报协议

URL:

统一资源定位符

索引

不可信 DLL	72	注册应用程序证书	41
信任证书	41	涉及未识别设备的项目文件	29
信息		添加设备	21
保存, 清除	24	登录以执行固件更新	64
包, 产品	50	登录对话框	57
公钥基础设施 (PKI)	46	监视设备发现状态	61
凭据	23, 57, 64	硬件	
分组设备	54	CPU, RAM, HDD	14
删除文件	72	确定 按钮	23
删除证书	41	确认消息	62
刷新图标	23	视图	19
包位置		系统要求	
添加	36	硬件, 软件, 通讯协议, 屏幕分辨率, 网络安全	14
卸载	72	组件信息	73
发现		组件和版本	73
手动, 自动	23	组 选项	54
自动, 手动	30	网络安全	68
取消信任证书	41	LANMAN / NTLM	71
固件		局域连接	70
更新, 设备/加载, 数据包	64	指南	70
版本, 升级信息, 进度	19	简介	68
固件包		网络接口卡	70
包信息, 包名称	16	认证	68
固件 对话框	64	远程桌面	71
复位应用程序设置	38	防火墙	71
复制到剪贴板 按钮	52	要导入的 csv 文件	32
复制标识符	52	警告	
安全功能	39	保存, 清除	24
安全包文件 sedps	49	设备	
安全配置文件	39, 66	更新, 配置选项, 凭据	57
安装		设备/加载	
过程, 安装向导, 安装, 许可证协议	15	设备名称, 状态, 数据包	19
密码	57, 64	设备/加载 选项卡	53
导入安全配置文件	39	设备发现	
导入配置文件	32	Modbus, DPWS (Web 服务设备配置文件)	13
工具栏		设备发现状态	61
关于, 帮助, 发现	17	设备登录 对话框	57
已拒绝 的数据包	50	设备证书	
应用修改	23	可信, 不可信	19
应用 按钮	23	设置 页中的修改	23
应用程序证书	41	访问扩展模块	59
异常	72	证书	41
扩展模块	59	验证, 信任, 取消信任, 删除	41
扩展 选项卡	59	证书管理	41
支持的设备	13	超时	
数据		通讯设置	35
固件, 配置	50	轮询频率	35
数据包	49	软件	
包名称, 包信息	18	功能, 支持的固件包	13
新项目	25	通知区域	62
日志		通知消息	62
查看	63	通讯协议	14
更新中心	63	配置	
更新固件	64	DPWS 扫描器	34
更新安全配置文件	66	Modbus TCP	32
更新摘要 对话框	64	包位置	35
更新确认 对话框	64	发现	30
有效 数据包	50	发现, Modbus, 包设置, 语言, 证书	23
本地存储库	35	语言, 更改	38
机架模块	59	通讯设置	35
来自其他计算机的项目文件	28	配置文件导入	32
标识符		错误	
复制	52	保存, 清除	24
模块化设备	59	错误, 警告	17
欢迎屏幕		项目	
数据包, 设备/加载, 工具栏	16	保存	26
		打开	27
		打开, 保存	17
		新建	25

项目已修改对话框	25
----------------	----

A

AutomationDeviceMaintenanceSettings.emes 文件	72
---	----

C

CA	41
Certificate Authority	41
csv 文件导入	32

D

DLL 不可信	72
DPWS 扫描器 探测器请求，元数据请求，网络适配器	34

F

fwp 包文件	49
---------------	----

H

HTTP/HTTPS 通讯	21
---------------------	----

L

Idx 包文件	49
---------------	----

M

Modbus TCP 设备 ID，ping 超时，端口	32
Modbus TCP 通讯	21

P

PKI	46
-----------	----

S

SD 内存卡	19
sedp 包文件	49
sedps 包文件	49
syslog	47

T

TCP	47
TLS	47

U

UDP	47
-----------	----

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

由于各种标准、规范和设计不时变更，请索取对本出版物中给出的信息的确认。

© 2022 Schneider Electric. 版权所有

EIO0000004050.04