

EcoStruxure Automation Device Maintenance

Firmware Upgrade Tool

Online Help

EIO0000004033.04
11/2022

Legal Information

The Schneider Electric brand and any trademarks of Schneider Electric SE and its subsidiaries referred to in this guide are the property of Schneider Electric SE or its subsidiaries. All other brands may be trademarks of their respective owners.

This guide and its content are protected under applicable copyright laws and furnished for informational use only. No part of this guide may be reproduced or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), for any purpose, without the prior written permission of Schneider Electric.

Schneider Electric does not grant any right or license for commercial use of the guide or its content, except for a non-exclusive and personal license to consult it on an "as is" basis. Schneider Electric products and equipment should be installed, operated, serviced, and maintained only by qualified personnel.

As standards, specifications, and designs change from time to time, information contained in this guide may be subject to change without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this material or consequences arising out of or resulting from the use of the information contained herein.

As part of a group of responsible, inclusive companies, we are updating our communications that contain non-inclusive terminology. Until we complete this process, however, our content may still contain standardized industry terms that may be deemed inappropriate by our customers.

© 2022 – Schneider Electric. All rights reserved.

Table of Contents

Safety Information.....	5
Qualification of Personnel	5
Proper Use.....	6
Before You Begin.....	6
Start-up and Test	7
Operation and Adjustments	7
Safety Precautions	8
About the Book.....	9
Introduction	14
Overview	14
System Requirements.....	15
Installation	16
Getting Started	17
Welcome Screen	17
EcoStruxure Automation Device Maintenance User	
Interface	19
Data Package	19
Device/Loading	20
Add Device	22
Configuring Settings	24
Error and Warning Window.....	25
Creating a New EcoStruxure Automation Device Maintenance	
Project.....	26
Saving the Project	27
Opening the Project.....	28
Configuring EcoStruxure Automation Device Maintenance	
Tool.....	31
Configuring Device Discovery Mode.....	31
Configuring Modbus TCP Scanner.....	33
Configuring DPWS Scanner	35
Configuring Communication Settings	36
Configuring Package Locations	36
Viewing the Log Files	37
Configuring Language.....	39
Resetting Application Settings	39
Configuring Security Features	40
Security Features	40
Managing Certificates	42
Managing the Public Key Infrastructure (PKI).....	47
Activating Syslog Message Logging	48
Data Package	50
Data Package Tab	50
Device/Loading	54
Device/Loading Tab	54
Grouping Devices in the DEVICE LIST	55
Removing Device	56

Managing User Credentials	60
Accessing Extensions	62
Monitoring the Device Discovery Status	64
Viewing / Confirming Messages	65
Viewing Logs.....	66
Update Center	66
Updating Firmware	67
Updating the Security Configuration File.....	69
Cybersecurity	72
What is Cybersecurity?	72
Schneider Electric Guidelines	74
Digital Signature Verification	76
Files Requiring Manual Deinstallation.....	77
Components Used by EcoStruxure Automation Device Maintenance.....	78
Glossary	81
Index	83

Safety Information

Important Information

Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, service, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.



The addition of this symbol to a “Danger” or “Warning” safety label indicates that an electrical hazard exists which will result in personal injury if the instructions are not followed.



This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

DANGER

DANGER indicates a hazardous situation which, if not avoided, **will result in** death or serious injury.

WARNING

WARNING indicates a hazardous situation which, if not avoided, **could result in** death or serious injury.

CAUTION

CAUTION indicates a hazardous situation which, if not avoided, **could result in** minor or moderate injury.

NOTICE

NOTICE is used to address practices not related to physical injury.

Please Note

Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel. No responsibility is assumed by Schneider Electric for any consequences arising out of the use of this material.

A qualified person is one who has skills and knowledge related to the construction and operation of electrical equipment and its installation, and has received safety training to recognize and avoid the hazards involved.

Qualification of Personnel

A qualified person is one who has the following qualifications:

- Skills and knowledge related to the construction and operation of electrical equipment and the installation.
- Knowledge and experience in industrial control programming.
- Received safety-related training to recognize and avoid the hazards involved.

The qualified person must be able to detect possible hazards that may arise from parameterization, modifying parameter values and generally from mechanical,

electrical, or electronic equipment. The qualified person must be familiar with the standards, provisions, and regulations for the prevention of industrial accidents, which they must observe when designing and implementing the system.

Proper Use

This product is a library to be used together with the control systems and long stator motor segments intended solely for the purposes as described in the present documentation as applied in the industrial sector.

Always observe the applicable safety-related instructions, the specified conditions, and the technical data.

Perform a risk evaluation concerning the specific use before using the product. Take protective measures according to the result.

Since the product is used as a part of an overall system, you must ensure the safety of the personnel by means of the design of this overall system (for example, machine design).

Any other use is not intended and may be hazardous.

Before You Begin

Do not use this product on machinery lacking effective point-of-operation guarding. Lack of effective point-of-operation guarding on a machine can result in serious injury to the operator of that machine.

WARNING

UNGUARDED EQUIPMENT

- Do not use this software and related automation equipment on equipment which does not have point-of-operation protection.
- Do not reach into machinery during operation.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

This automation equipment and related software is used to control a variety of industrial processes. The type or model of automation equipment suitable for each application will vary depending on factors such as the control function required, degree of protection required, production methods, unusual conditions, government regulations, etc. In some applications, more than one processor may be required, as when backup redundancy is needed.

Only you, the user, machine builder or system integrator can be aware of all the conditions and factors present during setup, operation, and maintenance of the machine and, therefore, can determine the automation equipment and the related safeties and interlocks which can be properly used. When selecting automation and control equipment and related software for a particular application, you should refer to the applicable local and national standards and regulations. The National Safety Council's Accident Prevention Manual (nationally recognized in the United States of America) also provides much useful information.

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before

placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

NOTE: Coordination of safeties and mechanical/electrical interlocks for point-of-operation protection is outside the scope of the Function Block Library, System User Guide, or other implementation referenced in this documentation.

Start-up and Test

Before using electrical control and automation equipment for regular operation after installation, the system should be given a start-up test by qualified personnel to verify correct operation of the equipment. It is important that arrangements for such a check are made and that enough time is allowed to perform complete and satisfactory testing.

⚠ WARNING

EQUIPMENT OPERATION HAZARD

- Verify that all installation and set up procedures have been completed.
- Before operational tests are performed, remove all blocks or other temporary holding means used for shipment from all component devices.
- Remove tools, meters, and debris from equipment.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Follow all start-up tests recommended in the equipment documentation. Store all equipment documentation for future references.

Software testing must be done in both simulated and real environments.

Verify that the completed system is free from all short circuits and temporary grounds that are not installed according to local regulations (according to the National Electrical Code in the U.S.A, for instance). If high-potential voltage testing is necessary, follow recommendations in equipment documentation to prevent accidental equipment damage.

Before energizing equipment:

- Remove tools, meters, and debris from equipment.
- Close the equipment enclosure door.
- Remove all temporary grounds from incoming power lines.
- Perform all start-up tests recommended by the manufacturer.

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995 (English version prevails):

- Regardless of the care exercised in the design and manufacture of equipment or in the selection and ratings of components, there are hazards that can be encountered if such equipment is improperly operated.
- It is sometimes possible to misadjust the equipment and thus produce unsatisfactory or unsafe operation. Always use the manufacturer's instructions as a guide for functional adjustments. Personnel who have access to these adjustments should be familiar with the equipment manufacturer's instructions and the machinery used with the electrical equipment.

- Only those operational adjustments actually required by the operator should be accessible to the operator. Access to other controls should be restricted to prevent unauthorized changes in operating characteristics.

Safety Precautions

During installation or use of this software, pay attention to the safety messages that occur in the software and that are included in the documentation. The following safety messages apply to this software in its entirety.

⚠ WARNING

RISK OF UNINTENDED EQUIPMENT OPERATION

- Do not use the software for critical control or protection applications where human or equipment safety relies on the operation of the control action.
- Do not use the software to control time-critical functions. The communication delays can occur between the time a control is initiated and when that action is applied.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

RISK OF INACCURATE DATA RESULTS

- Configure the software correctly to get accurate reports and/or data results.
- Do not base your maintenance or service actions solely on messages and information displayed by the software.
- Do not rely solely on software messages and reports to determine if the system is functioning correctly or meeting the applicable standards and requirements.
- Consider the implications of unintended transmission delays or failures of communications links.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: For detailed information on cybersecurity refer to the chapter Cybersecurity, page 72.

About the Book

Document Scope

This document describes the EcoStruxure Automation Device Maintenance tool. EcoStruxure Automation Device Maintenance can transfer firmware from a PC to supported Schneider Electric devices. The tool supports to discover relevant devices in the network and also allows to manually identify such devices if device discovery is not possible.

Validity Note

This document has been updated for EcoStruxure Automation Device Maintenance version 3.1.

The characteristics that are described in the present document, as well as those described in the documents included in the Related Documents section below, can be found online. To access the information online, go to the Schneider Electric home page www.se.com/ww/en/download/. For EcoStruxure Automation Device Maintenance documentation, type *EcoStruxure Automation Device Maintenance* in the search text box and press the **Enter** key.

The characteristics that are described in the present document should be the same as those characteristics that appear online. In line with our policy of constant improvement, we may revise content over time to improve clarity and accuracy. If you see a difference between the document and online information, use the online information as your reference.

Related Documents

Title of documentation	Reference number
Firmware Compatibility Rules, Modicon M580, Modicon Momentum, and Modicon X80 I/O Modules	EIO0000002634 (English)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (English) EIO0000002001 (French) EIO0000002000 (German) EIO0000002003 (Spanish) EIO0000002002 (Italian) EIO0000002004 (Chinese)
Modbus Specifications and Implementation Guides, Reference Manual	Modbus Application Protocol Specification
Devices Profile for Web Services, Reference Manual	WSDD-DPWS

Title of documentation	Reference number
EcoStruxure™ Control Expert, Operating Modes	33003101 (English) 33003102 (French) 33003103 (German) 33003104 (Spanish) 33003696 (Italian) 33003697 (Chinese)
EcoStruxure Automation Device Maintenance Altivar User Manual	JYT50472 (English) JYT50474 (French) JYT50482 (German) JYT50476 (Spanish) JYT50478 (Italian) JYT50483 (Chinese) JYT50484 (Turkish) JYT50485 (Portuguese)

Product Related Information

WARNING

LOSS OF CONTROL

- The designer of any control scheme must consider the potential failure modes of control paths and, for certain critical control functions, provide a means to achieve a safe state during and after a path failure. Examples of critical control functions are emergency stop and overtravel stop, power outage and restart.
- Separate or redundant control paths must be provided for critical control functions.
- System control paths may include communication links. Consideration must be given to the implications of unanticipated transmission delays or failures of the link.
- Observe all accident prevention regulations and local safety guidelines.¹
- Each implementation of this equipment must be individually and thoroughly tested for proper operation before being placed into service.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

¹ For additional information, refer to NEMA ICS 1.1 (latest edition), "Safety Guidelines for the Application, Installation, and Maintenance of Solid State Control" and to NEMA ICS 7.1 (latest edition), "Safety Standards for Construction and Guide for Selection, Installation and Operation of Adjustable-Speed Drive Systems" or their equivalent governing your particular location.

Before you attempt to provide a solution (machine or process) for a specific application using the POUs found in the library, you must consider, conduct and complete best practices. These practices include, but are not limited to, risk analysis, functional safety, component compatibility, testing and system validation as they relate to this library.

⚠ WARNING

IMPROPER USE OF PROGRAM ORGANIZATION UNITS

- Perform a safety-related analysis for the application and the devices installed.
- Ensure that the Program Organization Units (POUs) are compatible with the devices in the system and have no unintended effects on the proper functioning of the system.
- Use appropriate parameters, especially limit values, and observe machine wear and stop behavior.
- Verify that the sensors and actuators are compatible with the selected POUs.
- Thoroughly test all functions during verification and commissioning in all operation modes.
- Provide independent methods for critical control functions (emergency stop, conditions for limit values being exceeded, etc.) according to a safety-related analysis, respective rules, and regulations.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Only use software approved by Schneider Electric for use with this equipment.
- Update your application program every time you change the physical hardware configuration.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Incomplete file transfers, such as data files, application files and/or firmware files, may have serious consequences for your machine or controller. If you remove power, or if there is a power outage or communication interruption during a file transfer, your machine may become inoperative, or your application may attempt to operate on a corrupted data file. If an interruption occurs, reattempt the transfer. Be sure to include in your risk analysis the impact of corrupted data files.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION, DATA LOSS, OR FILE CORRUPTION

- Do not interrupt an ongoing data transfer.
- If the transfer is interrupted for any reason, re-initiate the transfer.
- Do not place your machine into service until the file transfer has completed successfully, unless you have accounted for corrupted files in your risk analysis and have taken appropriate steps to prevent any potentially serious consequences due to unsuccessful file transfers.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Care must be taken and provisions made for use of this library for machine control to avoid inadvertent consequences of commanded machine operation, state changes, or alteration of data memory or machine operating elements.

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

- Place operator devices of the control system near the machine or in a place where you have full view of the machine.
- Protect operator commands against unauthorized access.
- If remote control is a necessary design aspect of the application, ensure that there is a local, competent, and qualified observer present when operating from a remote location.
- Configure and install the Run/Stop input, if so equipped, or, other external means within the application, so that local control over the starting or stopping of the device can be maintained regardless of the remote commands sent to it.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in this manual, or that appear in or on the products themselves, are generally derived from the terms or definitions of international standards.

In the area of functional safety systems, drives and general automation, this may include, but is not limited to, terms such as *safety*, *safety function*, *safe state*, *fault*, *fault reset*, *malfunction*, *failure*, *error*, *error message*, *dangerous*, etc.

Among others, these standards include:

Standard	Description
IEC 61131-2:2007	Programmable controllers, part 2: Equipment requirements and tests.
ISO 13849-1:2015	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2013	Safety of machinery: Electro-sensitive protective equipment. Part 1: General requirements and tests.
ISO 12100:2010	Safety of machinery - General principles for design - Risk assessment and risk reduction
EN 60204-1:2006	Safety of machinery - Electrical equipment of machines - Part 1: General requirements
ISO 14119:2013	Safety of machinery - Interlocking devices associated with guards - Principles for design and selection
ISO 13850:2015	Safety of machinery - Emergency stop - Principles for design
IEC 62061:2015	Safety of machinery - Functional safety of safety-related electrical, electronic, and electronic programmable control systems
IEC 61508-1:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: General requirements.
IEC 61508-2:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Requirements for electrical/electronic/programmable electronic safety-related systems.
IEC 61508-3:2010	Functional safety of electrical/electronic/programmable electronic safety-related systems: Software requirements.
IEC 61784-3:2016	Industrial communication networks - Profiles - Part 3: Functional safety fieldbuses - General rules and profile definitions.
2006/42/EC	Machinery Directive
2014/30/EU	Electromagnetic Compatibility Directive
2014/35/EU	Low Voltage Directive

In addition, terms used in the present document may tangentially be used as they are derived from other standards such as:

Standard	Description
IEC 60034 series	Rotating electrical machines
IEC 61800 series	Adjustable speed electrical power drive systems
IEC 61158 series	Digital data communications for measurement and control – Fieldbus for use in industrial control systems

Finally, the term *zone of operation* may be used in conjunction with the description of specific hazards, and is defined as it is for a *hazard zone* or *danger zone* in the *Machinery Directive (2006/42/EC)* and *ISO 12100:2010*.

NOTE: The aforementioned standards may or may not apply to the specific products cited in the present documentation. For more information concerning the individual standards applicable to the products described herein, see the characteristics tables for those product references.

Introduction

Overview

Introduction

The EcoStruxure Automation Device Maintenance allows you to upgrade the firmware packages on multiple devices simultaneously. The devices can be discovered automatically or you can add the device manually, if automatic device discovery is not supported or switched off in the device.

The supported device discovery methods are:

- Modbus function code 43 (Read Device Identification)
- DPWS (Device Profile for Web Services)

Features

The EcoStruxure Automation Device Maintenance supports the following features:

- Automatic device discovery
- Manual device identification
- Security features
- Firmware update for multiple devices simultaneously
- IP address management

Supported Schneider Electric Devices

Modicon devices:

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

Altivar devices:

- Altivar product families
 - Altivar Process ATV6•• drives
 - Altivar Process ATV9•• drives
 - Altivar Machine ATV340 drives
- Altivar option modules:
 - VW3A3720 Ethernet
 - VW3A3721 MultiDrive-Link
 - VW3A3530D ATV dPAC
- Altivar soft starters:
 - Altivar Soft Starter ATS480

System Requirements

Hardware Requirements

Component	Minimum Requirement
CPU	Intel® Core i3 or later version is supported
RAM	Minimum 4 GB, recommended 8 GB or more
Hard disk space	500 MB of available disk space

Software Requirements

- Microsoft Windows® 10 Professional 32-bit/64-bit or later variant
- Microsoft Windows Server 2016 standard 64-bit
- Microsoft Windows Server 2019 standard 64-bit

Communication Protocols

The tool supports following protocols:

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

Screen Resolution

To view the software with best screen resolution, use 1920 x 1080 pixels screen resolution. As a minimum, 1280 x 1024 pixels screen resolution is required.

Cybersecurity

The following ports are used by the software:

- DPWS (via port 3702)
- FTP (via ports 20, 21)
- HTTP (via port 80) / HTTPs (via ports 443 and 8080)
- Modbus (via port 502)
- OPC UA (via port 4840)

⚠ WARNING

POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY

Use cybersecurity best practices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

NOTE: For detailed information on cybersecurity refer to the chapter [Cybersecurity](#), page 72.

Installation

Procedure

You can install the software by downloading the installation files from the [Schneider Electric website](#).

NOTE: Before you double-click the AutomationDeviceMaintenance.exe file, verify the integrity of the file as described in the chapter [Digital Signature Verification](#), page 76.

NOTE: You must have administrator rights to install the software.

Follow the procedure to install the software:

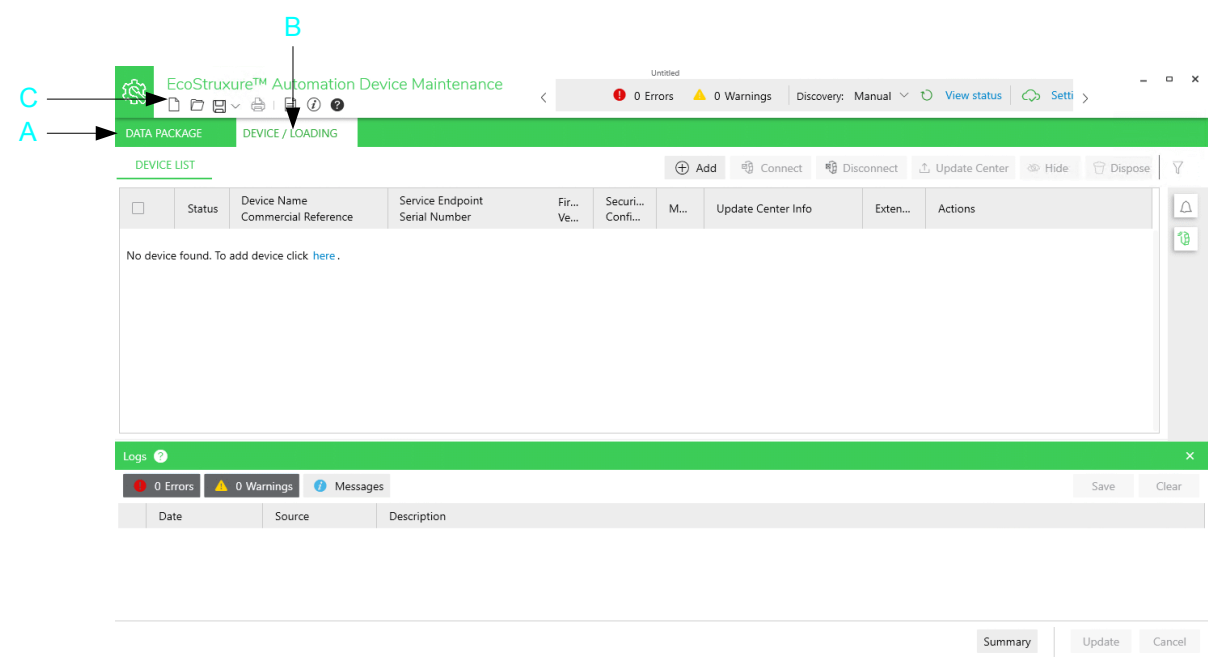
Step	Action
1	Locate the installation files using Windows Explorer after downloading the files.
2	Double click the EcoStruxure Automation Device Maintenance setup file. InstallShield Wizard is displayed.
3	Follow the instructions in the InstallShield Wizard to complete installation.

Getting Started

Welcome Screen

Overview











After initial start-up, EcoStruxure Automation Device Maintenance displays the following screen to upgrade firmware packages on multiple devices. When you close the tool, the present state of the user interface is saved. Thus, EcoStruxure Automation Device Maintenance will display the view that was present when you last closed the tool when you start it again.



Legend	Name	Function
A	Data Package	Displays the content of data package repository.
B	Device/Loading	Displays the details of discovered or manually identified devices.
C	Toolbar	Displays the set of icons to perform functions.

Toolbar

The toolbar allows to access the EcoStruxure Automation Device Maintenance general functions.

Element	Name	Description
	New Project	Allows you to create a new EcoStruxure Automation Device Maintenance project, page 26.
	Open	Allows to open an existing project, page 28.
	Save	Allows to save the project settings, page 27.
	Print	Feature is not available in this version.
	Logs	Allows you to view the log information.
	About	Allows to access the: <ul style="list-style-type: none"> EcoStruxure Automation Device Maintenance information Copy Details License Agreement Component Information System Information
	Help	Allows to access the Online help.
	Error	Allows to view the detected errors , page 25.
	Warning	Allows to view the detected warnings , page 25.
	Discovery	Allows to trigger device discovery when the device discovery mode is set to Manual .
–	Manual / Automatic	Select the device discovery mode Manual or Automatic from the list. For further information, refer to the <i>Configuring Device Discovery Mode</i> chapter, page 31.
–	Settings	Allows to configure Settings .

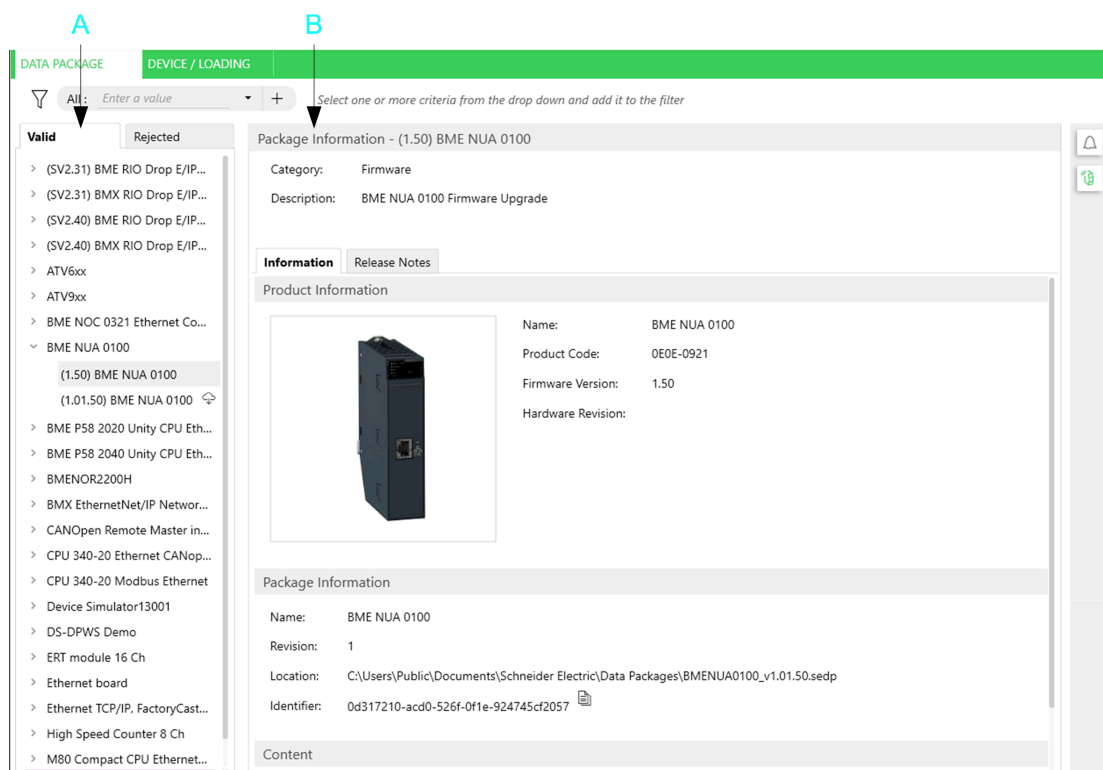
Buttons

Button	Description
Summary	After you have performed an update, click the Summary button to retrieve information on updated devices.
Update	After you have made settings for updating the firmware, page 67 or updating the security configuration file, page 69, click the Update button to start the update process as configured.
Cancel	The Cancel button allows you to cancel an update operation.

EcoStruxure Automation Device Maintenance User Interface

Data Package

Data Package feature contains package repository and displays the firmware packages available in the tool.




Legend	Name	Description
A	DATA PACKAGE list with tabs Valid and Rejected	Displays the list of locally available firmware packages. Packages available in the network are displayed if the required Add-On is installed. For further information, refer to the <i>Data Package Tab</i> chapter, page 50.
B	Package Information	Displays the description and content of the selected data package with static information in the upper part indicating the Category and the Description and with the two tabs Information and Release Notes in the lower part. For further information, refer to the <i>Data Package Tab</i> chapter, page 50.

Device/Loading


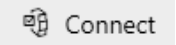
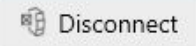
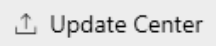




Overview

The **Device/Loading** tab displays the details of the devices known to the tool.

NOTE: Information displayed in this tab is only updated automatically if the discovery mode is set to **Automatic**. Click the  icon from the toolbar to display the latest values.











DATA PACKAGE		DEVICE / LOADING							
DEVICE LIST		⊕ Add 🔌 Connect 🔌 Disconnect 📶 Update Center 👁 Hide 🗑 Dispose 🔔							
<input type="checkbox"/>	Status	Device Name Commercial Reference	Service Endpoint Serial Number	Firmw... Version	Security Configurat...	Mode	Update Center Info	Extensions	Actions
<input type="checkbox"/>		Device Default Group (7)							
<input type="checkbox"/>	●	ATV630U07M3_dda1fa CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B01	-	-	-	-	🔌 🔌 📶 🔔 🗑 ⋮
<input type="checkbox"/>	●	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	-	-	🔌 🔌 📶 🔔 🗑 ⋮
<input checked="" type="checkbox"/>	●	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44716401Y	2.6IE94B13	-	-	-	-	🔌 🔌 📶 🔔 🗑 ⋮

Buttons of the tab:

Button	Description
	Click the Add button to add a new device. For further information, refer to Add Device , page 22.
	Click the Connect button to establish a connection to the selected device or devices.
	Click the Disconnect button to terminate the connection to the selected device or devices.
	Click the Update Center button to open the Update Center dialog box. It allows you to configure settings for performing a firmware update or an update of the security configuration file for the selected device or devices. For further information, refer to Update Center , page 66.
	Click the Hide button to hide the discovered device or devices. For further information, refer Device/Loading View , page 54.
	Click the Dispose button to dispose the discovered device or devices. For further information, refer Device/Loading View , page 54.
	Click the Notification Area button to view the notification area on the right-hand side of the Device/Loading tab. For further information, refer to Viewing / Confirming Messages , page 65.
	Click the Device Discovery Status button to view the Device Discovery Status view on the right-hand side of the Device/Loading tab. For further information, refer to Monitoring the Device Discovery Status , page 64.


Elements of the table:

Element	Description
Group	<p>You can assign the devices displayed in the DEVICE LIST to different groups as described in the chapter Grouping Devices in the DEVICE LIST, page 55.</p> <p>To select all devices that belong to a Group, select the check box of the Group.</p>
Check boxes	Select several check boxes on the left-hand side to perform the same operation on multiple devices simultaneously, such as Connect / Disconnect or updating operations.
Status	<p>Displays the status of the device:</p> <ul style="list-style-type: none"> Grey: The device is disconnected from the network. Yellow: The device is connected to the network but valid credentials have not been entered. Green: Valid credentials have been entered. Blue: The tool is loading content to the device. Red. The device is rebooting after firmware download to complete the installation.

Element	Description
Device Name Commercial Reference	Displays the name and the commercial reference (CR) of the device. NOTE: If you assigned a Friendly Name to your device, this user-defined name is only displayed if the communication protocol supports this parameter. Modbus TCP, for example, does not support it.
Service Endpoint Serial Number	Displays the service endpoint address as URI (Uniform Resource Identifier) and the serial number (SN) of the device.
Firmware Version	Displays the current firmware version of the device.
Mode	Only available after login: Indicates the mode of the device: RUN, STOP, BUSY, NOCONF, RESERVED, ENTERED, LOADING, COMPLETED, REQUIRERESTART, ERROR . The content of this cell is periodically refreshed. NOTE: Depending on the number of devices you are connected to, this mode monitoring can have an impact on your network bandwidth.
Update Center Info	Displays the update settings that have been configured in the Update Center dialog box: Firmware selected, Security configuration selected, Firmware update was successful, Firmware update was canceled, Firmware update was not successful . For further information, refer to Update Center , page 66.
Extensions	Modular devices provide a link (Extensions) that allows you to access the individual extensions of the device. For further information, refer to Accessing Extensions , page 62.
Actions	Icons are provided for each device to perform different device-specific operations:
	Click the Set credentials icon and enter the credentials to connect to the device in the Set credentials dialog box. The black icon indicates that no credentials are stored for the device. The yellow icon indicates that credentials have been stored but no login to the device has been performed. Alternatively, you can configure global credentials for the project via Settings > Project > User Credential Settings . For more information, refer to Managing User Credentials , page 60.
	The green Set credentials icon indicates that the credentials for the device have been validated and that the login has been performed successfully.
	The red Set credentials icon indicates that the attempt to log in to the device was unsuccessful. Perform the login procedure again and make sure to use the correct credentials.
	Click the Connect / Disconnect icon to establish or terminate a connection to the device.
	Click the Update Center icon to open the Update Center dialog box. It allows you to configure settings for performing a firmware update or an update of the security configuration file for the device. For further information, refer to Update Center , page 66.
	Click the Device log icon to view the log information.
	Click the Start device icon to start the device. NOTE: Perform a start-up test before using electrical control and automation equipment for regular operation after installation or update. For further information, refer to Start-up and Test , page 7.
	Displays the certificate status. <ul style="list-style-type: none"> Grey: Trusted certificate Red: Untrusted certificate Click the Device certificate icon to open the Certificate Information dialog box. For further information, refer to Managing the Trust Status of Certificates in the Device/Loading Tab , page 46.
	Indicates that the device is equipped with an SD memory card. Click this icon to download software directly to the SD memory card.
	Click the Additional device options icon for a list of commands available for devices after successful login. For further information, refer to <i>Details Available After Login</i> , page 55.
Progress	Displays the firmware update progress status.

Add Device

Overview

The **Add Device** dialog box opens by clicking the  **Add** button in the **Device/Loading** tab or by clicking the **No device found. To add device click here** link that is displayed when the device list is empty, for example, if you create a new project.

Add Device

Search Commercial Reference

Search...

Commercial Reference:*

0E0E-0521

0E0E-0921

140***

140*** (modernized)

171***

171*** (modernized)

ATS***

ATS*** (modernized)

Note: Modernized = commercialized after 2019.

For more information, refer to the [Schneider Electric Product Catalog](#)

Connection:*

HTTP/HTTPS

Secure

IP Address:*

172.10.15.25

443

Add Device

Cancel

It allows you to add devices manually if they cannot be discovered automatically by EcoStruxure Automation Device Maintenance because either the device does not support discovery or the device discovery feature is switched off. To achieve this, select the commercial reference.

By default, the list of **Commercial References** only contains templates of commercial references (such as **BME*****, **BMX***** or **Any device**). In this case, you have two options:

- Select the template that matches your product: For example, for BMEP582020, select **BME***** from the list.

NOTE: Two variants are provided for each template that cover the legacy (for example, **BME*****) and the recent version (for example, **BME*** (modernized)**). They differ in the supported protocols. Thus, if you do not find the protocol of your choice in the **Connection** list, select the second option provided for your product.
- To populate the list with commercial references of the devices you are using, copy the corresponding data packages to the folder you configured as **Local Repository** in the **Settings > Package Settings** dialog box. (For further information, refer to the chapter [Configuring Package Locations](#), page 36.) The table will then display specific references (such as **BMEP582020** or **BMXNOR0200**).

Component	Description
Commercial Reference	Select the Commercial Reference number of your device from the list and enter the device information according to the protocol selected from the Connection list on the right-hand side.
Connection	<p>Select the protocol that is used for communication from the list:</p> <ul style="list-style-type: none"> • HTTP/HTTPS • MODBUS (SL) • MODBUS (TCP) • OPC UA • FTP • USB <p>Depending on the selected protocol, the parameters are adapted.</p>
Secure	<p>This option is only available for HTTP/HTTPS communication:</p> <p>Select the option if the device is connected via a secured connection (HTTPS).</p>
IP Address	Enter the IP address of the device being added and the port that is used for communication.
Unit-ID	<p>This option is only available for MODBUS (TCP) communication:</p> <p>Enter the unit identification node for Modbus TCP communication.</p> <p>For more information on Modbus specifications, refer to Modbus Specifications and Implementation Guides.</p>

NOTE: EcoStruxure Automation Device Maintenance V3.1 and later versions support adding devices by the commercial reference. If you attempt to open project files that were created with EcoStruxure Automation Device Maintenance V3.0 and earlier versions which contain devices without commercial reference, you will be prompted to select a commercial reference for each unknown device.

Also refer to [Opening the Project](#), page 28.


Configuring Settings

Overview

The **Settings** page allows you to configure general settings.

Components	Description
Discovery	Select to configure the discovery mode. For more information, refer to Configuring Device Discovery Mode , page 31.
DPWS	Select to configure the details of DPWS scanner. For more information, refer to Configuring DPWS Scanner , page 35.
Modbus TCP	Select to configure the details of Modbus scanner. For more information, refer to Configuring Modbus TCP Scanner , page 33.
Communication	Select to configure the communication settings. For more information, refer to Configuring Communication Settings , page 36.
Package Setting	Select to configure the package settings. For more information, refer to Configuring Package Locations , page 36.
Security	Select the option to activate protection mode and to display notifications concerning security features such as encrypted communication using certificates, secured packages or syslog support. For more information, refer to Security Features , page 40.
Certificate Management	Select to enroll the application certificate for EcoStruxure Automation Device Maintenance and to manage the trust status of digital certificates of communication partners. For more information, refer to Managing Certificates , page 42.
PKI	Select to configure the Public Key Infrastructure (PKI). For more information, refer to Managing the Public Key Infrastructure (PKI) , page 47.
Logs	Select to view the EcoStruxure Automation Device Maintenance Log files and configure the log settings. For more information, refer to Viewing the Log Files , page 37.
Language	Select to configure the desired language. For more information, refer to Configuring Language , page 39.
Group	Select to group devices displayed in the DEVICE LIST . For more information, refer to Grouping Devices in the DEVICE LIST , page 55.
Project > User Credential Settings	Select to enter global credentials for the devices of the project. For more information, refer to Managing User Credentials , page 60.

Applying Modifications

Whenever you modify settings in a tab of the **Settings** page, this tab is marked by the refresh  icon indicating that there are modifications on this page that have not yet been applied.

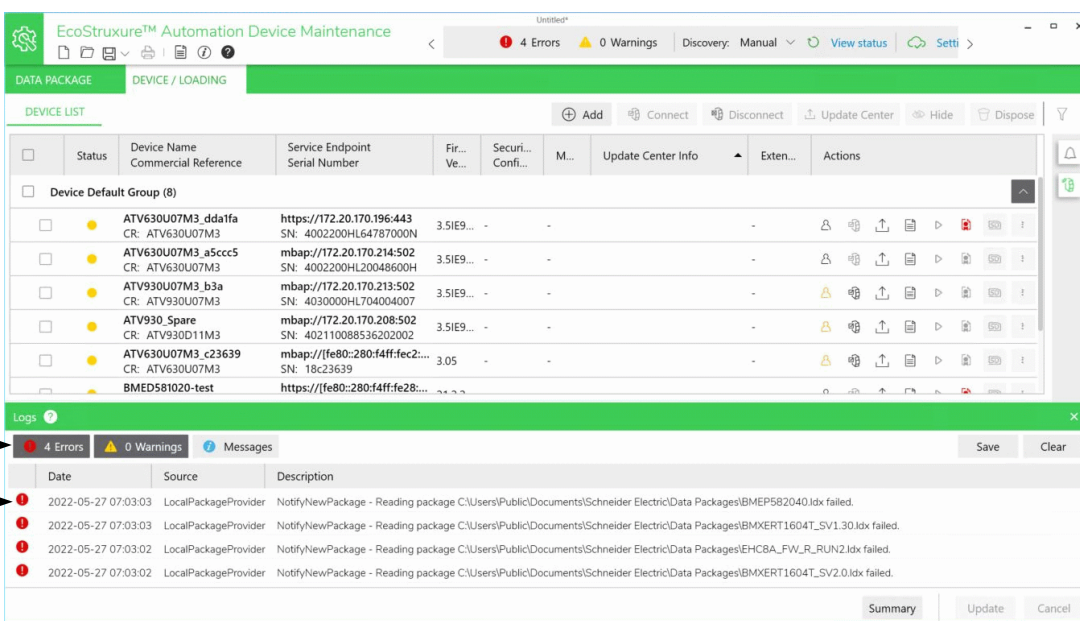
To apply the modifications to this page, click the **Apply** button.

To apply the modifications you performed in all tabs and to close the **Settings** page, click the **Ok** button.

Error and Warning Window

Overview

You can view details of the detected errors in the tool in a cumulative log window. The errors log provides the details to rectify the detected error related to the selected device. You cannot proceed with updating the firmware for the selected device unless the detected errors are resolved.



The screenshot shows the EcoStruxure Automation Device Maintenance application. The top toolbar includes buttons for Add, Connect, Disconnect, Update Center, Hide, and Dispose. Below the toolbar is the 'DEVICE LIST' table with columns: Status, Device Name, Commercial Reference, Service Endpoint, Serial Number, Fir... Ve..., Securi... Confi..., M..., Update Center Info, Exten..., and Actions. The table lists several devices, including ATN630U07M3 and BMED581020-test. Below the device list is the 'Logs' window, which has a status bar showing '4 Errors' and '0 Warnings'. The logs table has columns: Date, Source, and Description. It shows four error entries from 'LocalPackageProvider' dated 2022-05-27 07:03:03, 2022-05-27 07:03:03, 2022-05-27 07:03:02, and 2022-05-27 07:03:02. The logs window also has 'Summary', 'Update', and 'Cancel' buttons.

Legend	Name	Description
A	Error and warning status	Displays the number of detected errors and detected warnings.
B	Logs	Displays the number of detected errors and detected warnings with the description.

Viewing Errors and Warnings Log

Step	Action
1	Click the Errors or Warnings status in the toolbar. The Logs window displays the following information: <ul style="list-style-type: none"> Number of detected errors, detected warnings, and information. Description of the detected errors.
2	Select detected error, detected warning, and / or information messages of your choice.


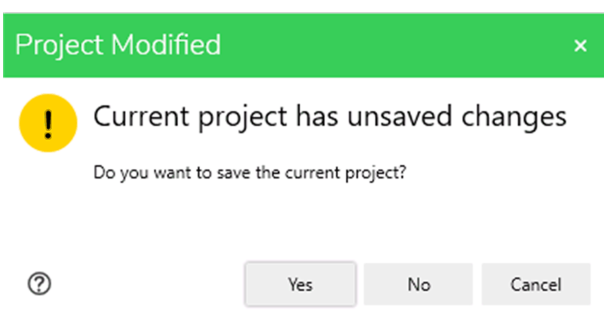
Step	Action
3	Click Save to save the selected detected error, detected warning, and information messages.
4	Click Clear to remove all the messages about detected errors and detected warnings from the log.

Creating a New EcoStruxure Automation Device Maintenance Project

Procedure

This feature allows you to create a new EcoStruxure Automation Device Maintenance project.

Follow these steps to create a project:

Step	Action
1	<p>Click the  icon.</p> <p>Result: The Project Modified dialog box is displayed if a project is open that has been modified and has not yet been saved.</p>
2	<p>In the Project Modified dialog box, click Yes to save the changes to the open project or No to close the project without saving.</p>  <p>Result: The open project is closed and a new project opens displaying the Device/Loading tab with the device list being empty.</p>


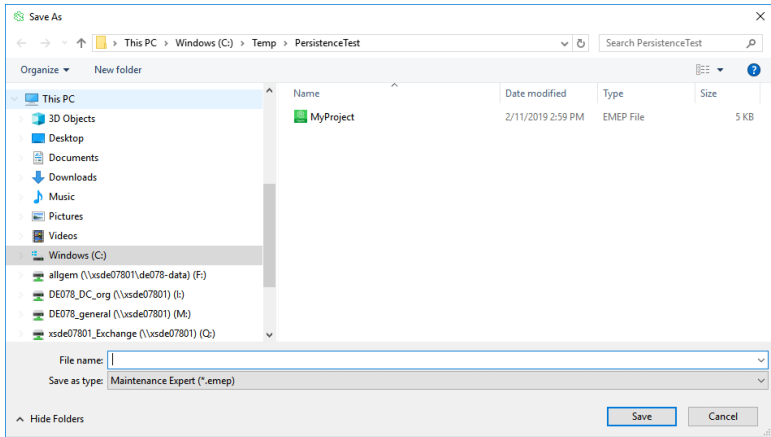
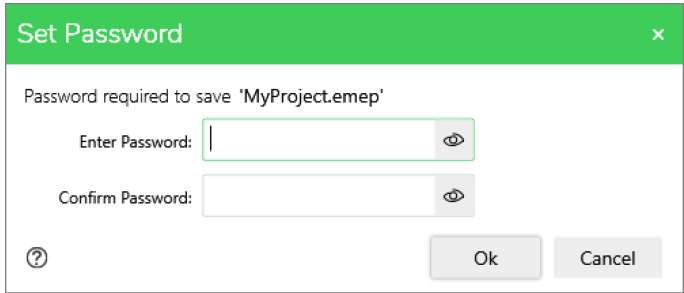
By creating a new project, the following tasks are automatically executed:

- The discovery mode is set to **Manual**.
- The log file entries are cleared.

Saving the Project

This feature allows you to save a copy of the current project with a different name or in a different location. The advantage is, the devices need not be added again and again when you open the EcoStruxure Automation Device Maintenance tool.


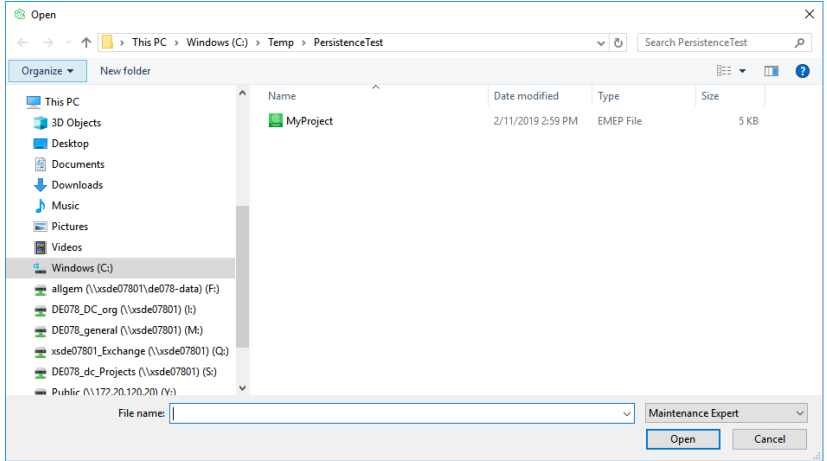
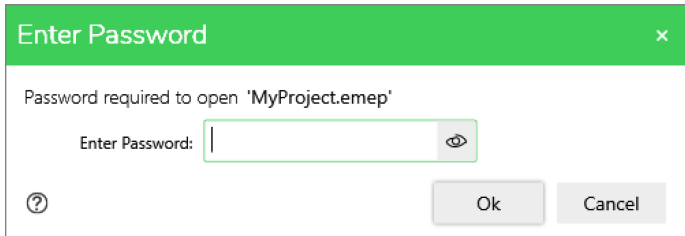
Follow these steps to save the project settings:

Step	Action
1	Click the  icon.
2	To save changes to the current project, click Save . To save a copy of the project, click Save As .
3	Select the folder you want to save the project to and enter the File name . 
4	Click Save and enter the same password in both fields of the Set Password dialog box. 
5	Click Ok to proceed.

Opening the Project

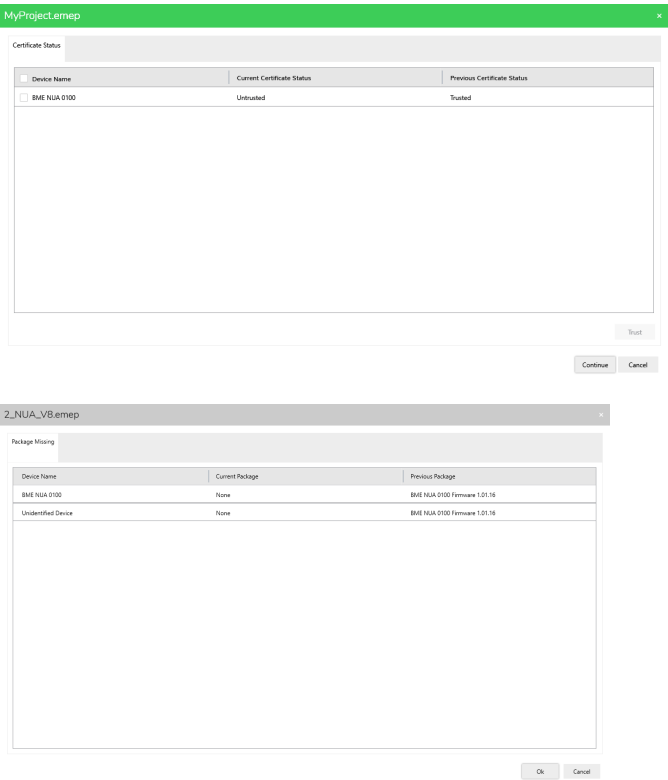
Opening a Project

Execute the following steps to open a project:

Step	Action
1	<p>Click the  icon.</p> 
2	<p>Select the folder and the project. Click Open and enter the password.</p> 
3	Click Ok to open the project.

Optional Steps for Project Files Created on Another Computer

If you attempt to open a project file which was created on another computer, the tool optionally indicates certificate trust status differences and package availability differences.



In this case, proceed as follows:

Step	Action
4	Select the devices you want to trust and click Trust .
5	Click Continue . <div></div>
6	Click OK to open the project with missing packages or click Cancel .

Optional Step for Project Files with Unidentified Devices

If you attempt to open project files that were created with EcoStruxure Automation Device Maintenance V3.0 and earlier versions which contain devices without commercial reference, a dialog box is displayed prompting you to select a commercial reference for each unknown device from the list:

UnIdentified_3.0.1.emep

The project contains devices with an unknown Commercial Reference.
Please verify the default selection below or select another Commercial Reference from the drop-down list!

The project was most likely created with an older version of EcoStruxure Automation Device Maintenance.
The option to manually add unidentified devices is not supported in this version anymore.

Service Endpoint	Commercial Reference
COM3/255	ATV***
mbap://145.0.0.1:502	ATV***
mbap://145.0.0.2:502	ATV***

Note: Modernized = commercialized after 2019.
For more information, refer to the [Schneider Electric Product Catalog](#)

Ok

Cancel

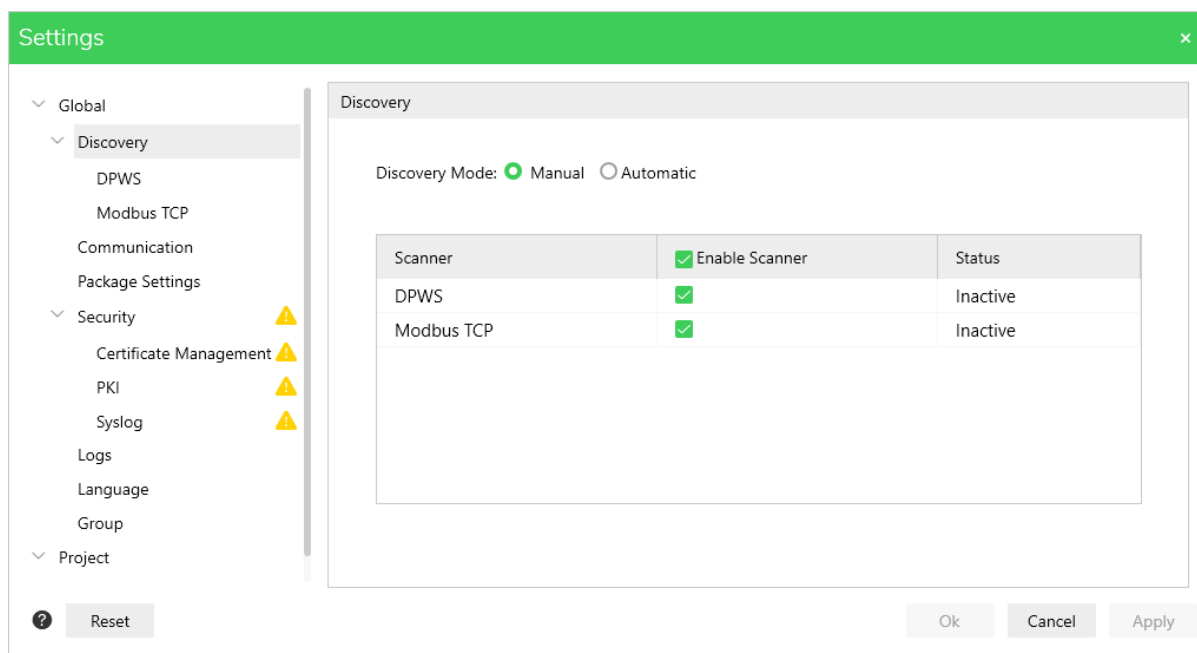
Select the commercial references of your choice and click **Ok** to open the project.

Configuring EcoStruxure Automation Device Maintenance Tool

Configuring Device Discovery Mode

Configuring Automatic Discovery Mode

You can select the device discovery mode as **Automatic** or **Manual**. In case of **Automatic** discovery, the tool will periodically send information over the network in the background and receive information from the responding devices.

Step	Action									
1	Click Settings menu at the top center of the Home page.									
2	Click Discovery option. <div><p>The screenshot shows the 'Settings' window with the 'Discovery' tab selected. On the left is a sidebar menu with categories: Global, Discovery (selected), DPWS, Modbus TCP, Communication, Package Settings, Security (with warning icons), Certificate Management, PKI, Syslog, Logs, Language, Group, and Project. The main area shows 'Discovery Mode' with 'Manual' selected (radio button) and 'Automatic' unselected. Below is a table:</p><table><thead><tr><th>Scanner</th><th>Enable Scanner</th><th>Status</th></tr></thead><tbody><tr><td>DPWS</td><td><input checked="" type="checkbox"/></td><td>Inactive</td></tr><tr><td>Modbus TCP</td><td><input checked="" type="checkbox"/></td><td>Inactive</td></tr></tbody></table><p>At the bottom of the window are buttons for 'Reset', 'Ok', 'Cancel', and 'Apply'.</p></div>	Scanner	Enable Scanner	Status	DPWS	<input checked="" type="checkbox"/>	Inactive	Modbus TCP	<input checked="" type="checkbox"/>	Inactive
Scanner	Enable Scanner	Status								
DPWS	<input checked="" type="checkbox"/>	Inactive								
Modbus TCP	<input checked="" type="checkbox"/>	Inactive								
3	Select Automatic mode.									
4	Select the scanners that will be taking part in discovery. Use this setting to help prevent scanning of any devices that you want to avoid.									
5	Click Apply and then, click OK .									

Configuring Manual Discovery Mode

You can select the device discovery mode as **Manual** to discover the devices connected in the network when required.

Step	Action									
1	Click Settings menu at the top center of the Home page.									
2	<div>Click Discovery option.</div> <div><div><div>Settings</div><div><div><div>Global</div><div>Discovery</div><div>DPWS</div><div>Modbus TCP</div><div>Communication</div><div>Package Settings</div><div>Security</div><div>Certificate Management</div><div>PKI</div><div>Syslog</div><div>Logs</div><div>Language</div><div>Group</div><div>Project</div></div><div><div>?</div><div>Reset</div></div></div><div><div>Discovery</div><div>Discovery Mode: <input checked="" type="radio"/> Manual <input type="radio"/> Automatic</div><table><tr><th>Scanner</th><th><input checked="" type="checkbox"/> Enable Scanner</th><th>Status</th></tr><tr><td>DPWS</td><td><input checked="" type="checkbox"/></td><td>Inactive</td></tr><tr><td>Modbus TCP</td><td><input checked="" type="checkbox"/></td><td>Inactive</td></tr></table><div><div>Ok</div><div>Cancel</div><div>Apply</div></div></div></div></div>	Scanner	<input checked="" type="checkbox"/> Enable Scanner	Status	DPWS	<input checked="" type="checkbox"/>	Inactive	Modbus TCP	<input checked="" type="checkbox"/>	Inactive
Scanner	<input checked="" type="checkbox"/> Enable Scanner	Status								
DPWS	<input checked="" type="checkbox"/>	Inactive								
Modbus TCP	<input checked="" type="checkbox"/>	Inactive								
3	Select Manual mode.									
4	Select the scanners that will be taking part in discovery. Use this setting to help prevent scanning of any devices that you want to avoid.									
5	Click Apply and then, click OK .									

Configuring Modbus TCP Scanner

Overview

The **Modbus TCP** scanner sends Modbus function code 43 requests to all IP addresses in a range that is defined by a **Start IP Address** and an **End IP Address**.

You can configure the following **Modbus TCP** parameters:

Element	Default value	Description
IP Address section:		
Range Name parameter	–	Optional name of the address range.
Start IP Address parameter	127.0.0.1	First address of the address scan range.
End IP Address parameter	127.0.0.1	Last address of the address scan range.
Import button	–	Click the Import button to import a configuration file that is available in .csv format (refer to the example of an import configuration file below, page 33). NOTE: This command overwrites the present configuration settings. Make sure to back up your settings beforehand. Result: A Windows File open dialog box opens and allows you to browse your network for the csv file. Click Open to import the configuration settings from the file. To apply the new settings, click Apply or Ok .
+ Add button	–	Click the + Add button to create a new address range. Result: A new line is added to the table with: Range Name = Default Start IP Address = 127.0.0.1 End IP Address = 127.0.0.1
Check box	–	Select / deselect a check box to include / exclude the selected range for the Modbus scan.
Trashbin button	–	Click the trashbin button to remove the selected range, i.e. line of the table.
Advanced Settings section:		
Start Port parameter	502	First port of the port scan range.
End Port parameter	502	Last port of the port scan range.
Timeout parameter	4000	Maximum wait time between sending a ping to device and receiving the reply.
Unit-ID parameter	255	Modbus unit ID used for accessing the device.

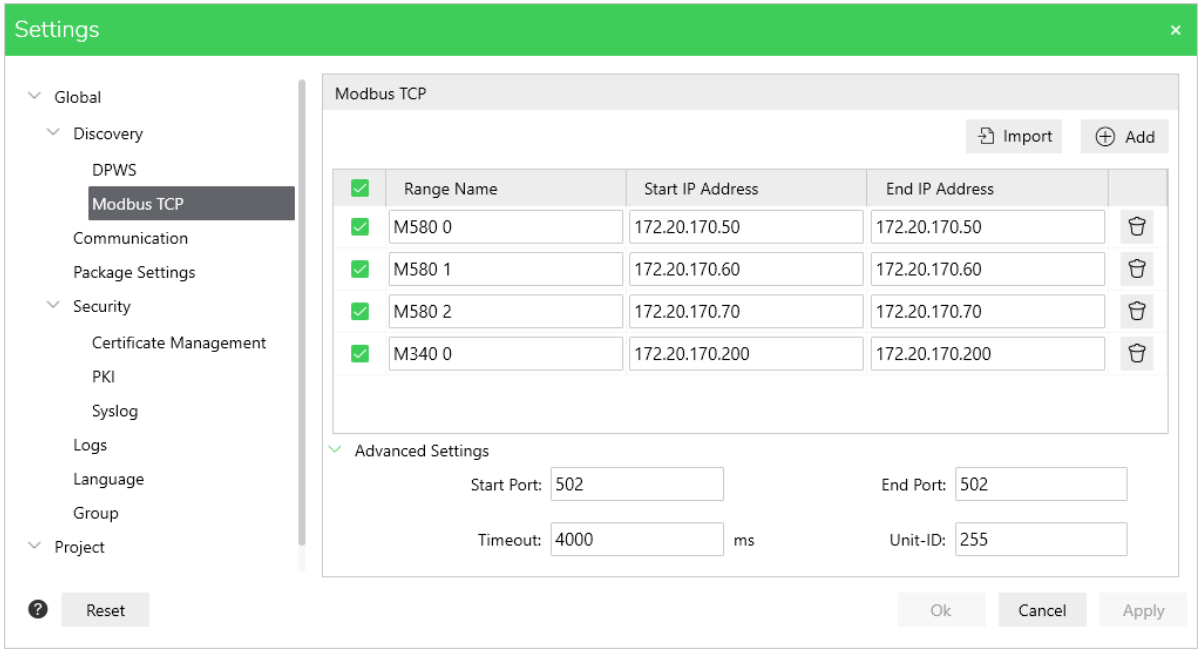
Example of an Import Configuration File

The format of the configuration file in .csv format should comply with the following example:

```
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
```

Configuring the Modbus TCP Scanner

Follow these steps to configure the **Modbus TCP** scanner:

Step	Action
1	Expand the Discovery menu on the Settings page.
2	Select the Modbus TCP node.
3	In the Modbus TCP view on the right-hand side, click the Add button to create a new address range.
4	<p>Click the Import button to import a configuration file or configure the following parameters:</p> <ul style="list-style-type: none"> • Range Name • Start IP Address • End IP Address • Start Port • End Port • Timeout • Unit-ID 
5	Click Apply to apply the Modbus TCP settings or Ok to apply all application settings modifications and to close the Settings dialog box.

Configuring DPWS Scanner

Overview

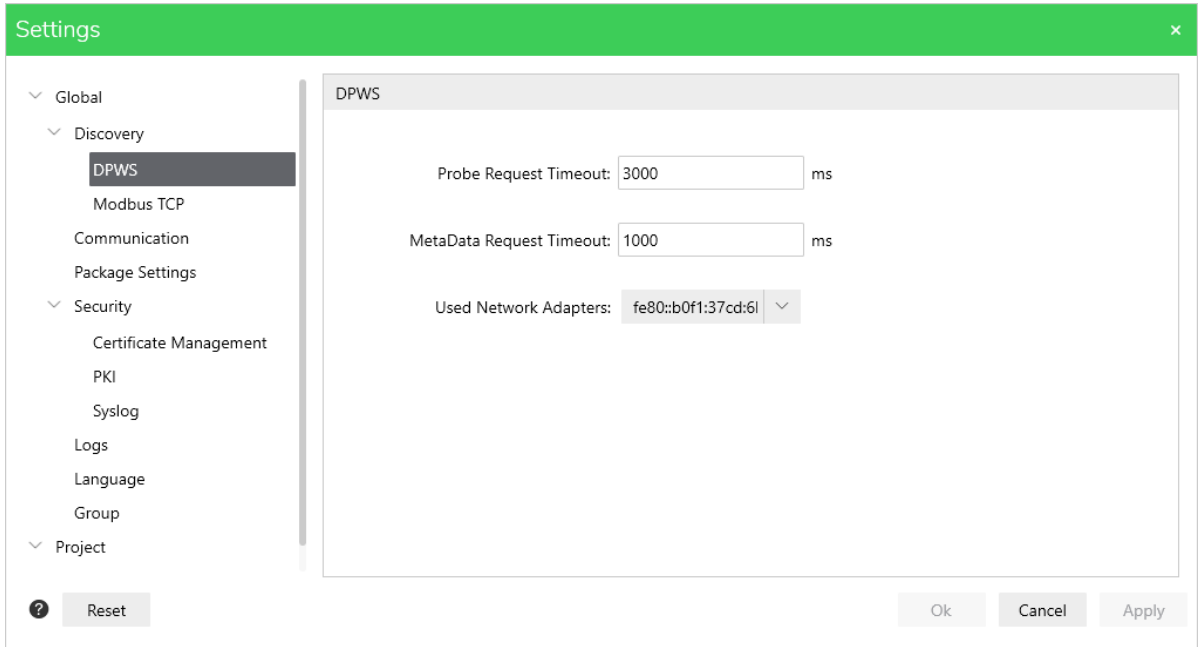
DPWS scanner is a client-side implementation of the **DPWS** standard which allows to discover DPWS-compliant devices.

For more information on DPWS Standards, refer to <http://docs.oasis-open.org/ws-dd/ns/dpws/2009/01>.

You can configure the following **DPWS** parameters:

Parameter	Default value	Description
Probe Request Timeout	3000 ms	Maximum wait time between sending a probe request and receiving the probe match responses from the devices.
Metadata Request Timeout	1000 ms	Maximum wait time between sending a metadata request and receiving the response from the device.
Used Network Adapters	–	List of network adapters to be used for sending the DPWS probe request.

Follow these steps to configure **DPWS** scanner:

Step	Action
1	Expand the Discovery menu on the Settings page.
2	<p>Select DPWS and enter the following details:</p> <ul style="list-style-type: none"> • Probe Request Timeout • Metadata Request Timeout • Used Network Adapters 
3	Click Apply and then, click Ok .

Configuring Communication Settings

Overview

The screenshot shows the 'Settings' dialog box with the 'Communication' tab selected. The left sidebar contains a tree view with the following structure:

- Global
 - Discovery
 - DPWS
 - Modbus TCP
 - Communication**
 - Package Settings
 - Security
 - Certificate Management
 - PKI
 - Syslog
 - Logs
 - Language
 - Group
 - Project

The main content area displays the 'Communication' settings:

- Timeout:** 6000 ms
- Automatic device status polling:**
 - Frequency (High priority): 3000 ms
 - Frequency (Low priority): 10000 ms

At the bottom of the dialog are buttons for 'Reset', 'Ok', 'Cancel', and 'Apply'.

You can configure the following communication settings for the communication between EcoStruxure Automation Device Maintenance and devices:


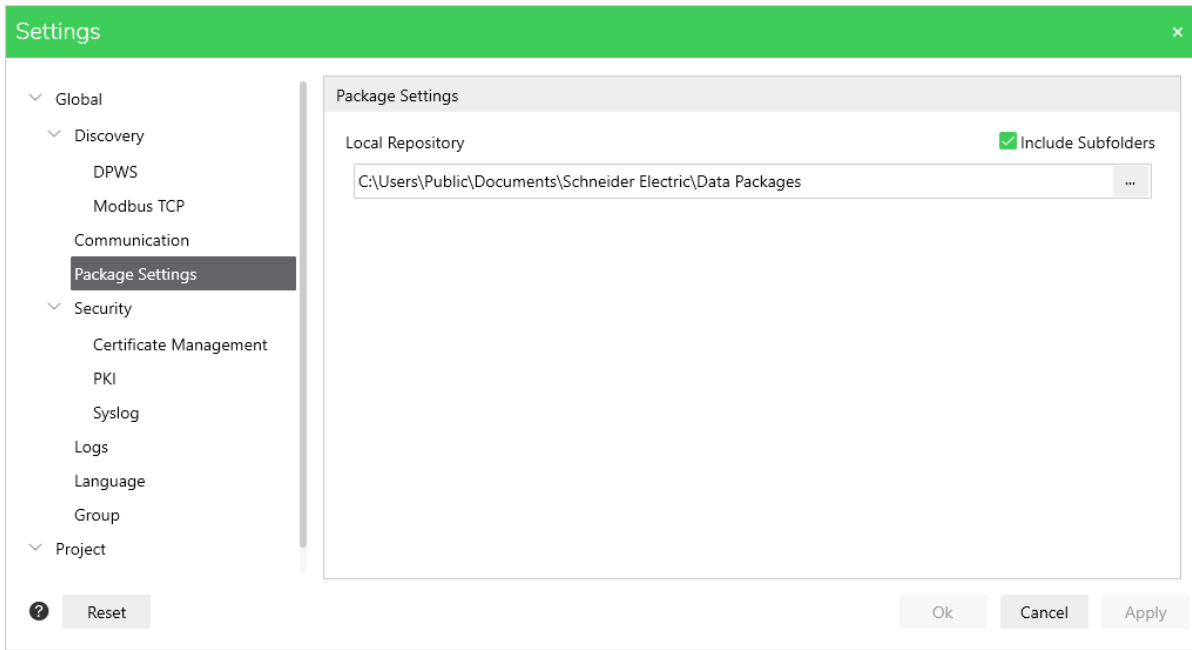
Parameter	Default value	Description
Timeout section:		
Timeout	6000 ms	Maximum wait time after requests / responses sent / received by EcoStruxure Automation Device Maintenance (for example, firmware updates, setting the IP configuration). For timeouts applying to discovery requests, refer to the Modbus TCP scanner, page 33 and DPWS scanner, page 35.
Automatic device status polling section: These parameters define the frequency of sending polling requests to detected devices in order to keep the device status, page 20 updated:		
Frequency (High priority):	3000 ms	High priority polling is used when firmware updates are performed. It allows to speed up detection of the device after it has been rebooted.
Frequency (Low priority):	10,000 ms	Low priority with less frequent polling cycles is used in normal operation.

Configuring Package Locations

You can configure the path of available firmware data packages in the tool. This allows for updating the device firmware versions. Furthermore, the specific commercial reference provided by each data package is added to the **Commercial Reference** list in the **Add Device** dialog box, page 22.

Changing Package Location

Follow these steps to change the package location:




Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Package Settings option.
3	Select the path to change the location of the Local Repository .
4	<p>Click the  icon and select the destination folder to change the path.</p>  <p>The screenshot shows the 'Settings' window with a sidebar on the left containing a tree view: Global, Discovery (with sub-items DPWS, Modbus TCP), Communication, Package Settings (highlighted), Security (with sub-items Certificate Management, PKI, Syslog), Logs, Language, Group, and Project. At the bottom of the sidebar are a help icon and a 'Reset' button. The main area is titled 'Package Settings' and contains a 'Local Repository' label, a text field with the path 'C:\Users\Public\Documents\Schneider Electric\Data Packages', and a folder selection icon. To the right of the text field is a checked checkbox labeled 'Include Subfolders'. At the bottom right of the window are 'Ok', 'Cancel', and 'Apply' buttons.</p>
5	Click Apply and then, click Ok .

Viewing the Log Files

You can view the stored logs and analyze it for any details for the selected device.

Follow these steps to view the logs:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select Logs option.
3	Set log creation to Active/Inactive .
4	Select the path to change the log file location.

Step	Action
5	<div><div></div><div>Click the icon and select the destination folder to change the path.</div></div> <div><div><div>Settings</div><div><div><div>Global</div><div>Discovery</div><div>DPWS</div><div>Modbus TCP</div><div>Communication</div><div>Package Settings</div><div>Security</div><div>Certificate Management</div><div>PKI</div><div>Syslog</div><div>Logs</div><div>Language</div><div>Group</div><div>Project</div></div><div><div>?</div>Reset</div></div><div><div>Logs</div><div><div><div>Active</div><div>Inactive</div></div><div>C:\Users\SESA395371\AppData\Local\Temp\AutomationDeviceMaintenance.log</div><div><div>...</div><div></div></div><div><div></div><div>The log file contains sensitive data. Delete the log file after use or store it in a safe place.</div></div></div><div><div>Ok</div><div>Cancel</div><div>Apply</div></div></div></div></div> <div><div>NOTE: For further information on the Cybersecurity notification, refer to Recommendation for Improved Cybersecurity, page 66.</div></div>
6	Click Apply and then, click OK .

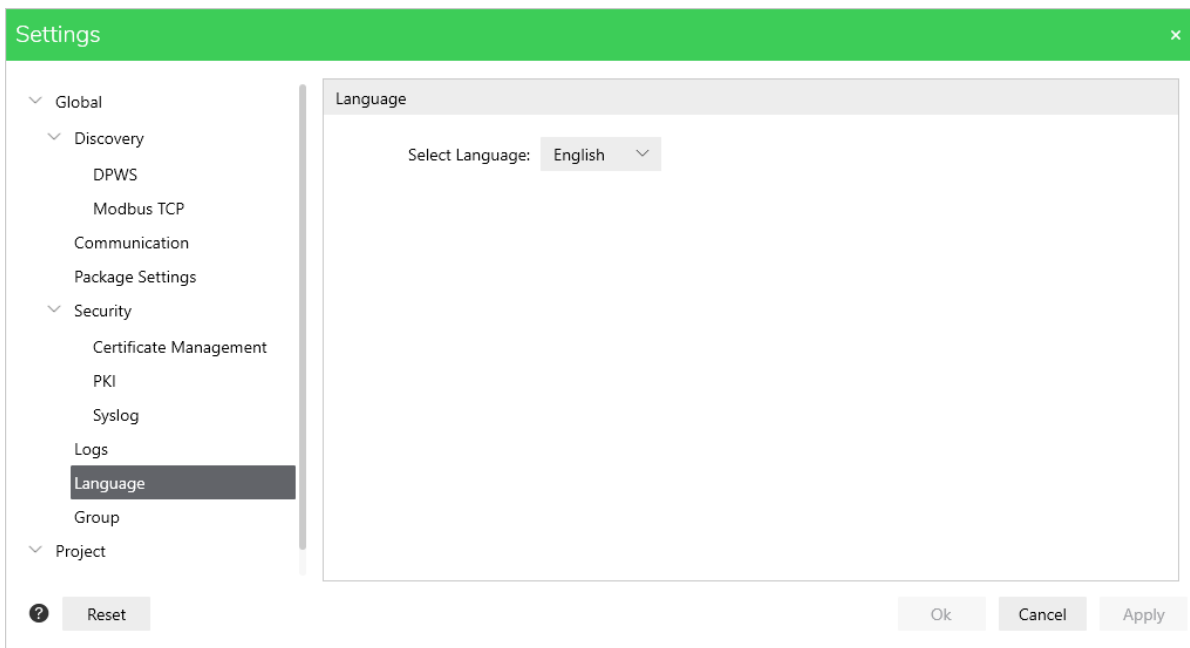
Configuring Language

You can select the language to view the EcoStruxure Automation Device Maintenance tool content in your preferred language.

The following languages are supported:

- English
- German
- French
- Spanish
- Italian
- Chinese

Follow these steps to set the language:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select Language option.
3	Click Select Language drop-down list to select the desired language. 
4	Click Apply and then, click OK . NOTE: Restart EcoStruxure Automation Device Maintenance to apply the language changes.

Resetting Application Settings

Overview

The dialog boxes of the **Settings** menu contain a **Reset** button in the lower left corner.

Click the **Reset** button to reset the values of all the application settings you configured via the **Settings** menu to their default values.

Configuring Security Features

Overview

Cybersecurity best practices and solutions are in constant evolution as a function of the latest information available. As a design criteria, Schneider Electric incorporates up-to-date knowledge and techniques to help make products more resilient to cyberattacks. The security by design approach results in the implementation of mechanisms to mitigate threats, reduce exploitable weaknesses, and defend against avoidable data breaches and cyberattacks.

NOTE:

To help keep your Schneider Electric products secure and protected, it is in your best interest that you implement the cybersecurity best practices as indicated in the *Cybersecurity Best Practices* document provided on the Schneider Electric website.

Due to the rapid rise of networking machines and plants, potential threats are also quickly rising. Therefore, carefully consider all possible security measures.

Security measures are necessary to help protect data and communication channels from unauthorized access.

NOTE: Before you configure security features consult your security administrator to help ensure that you are using the correct security settings.

Security Features

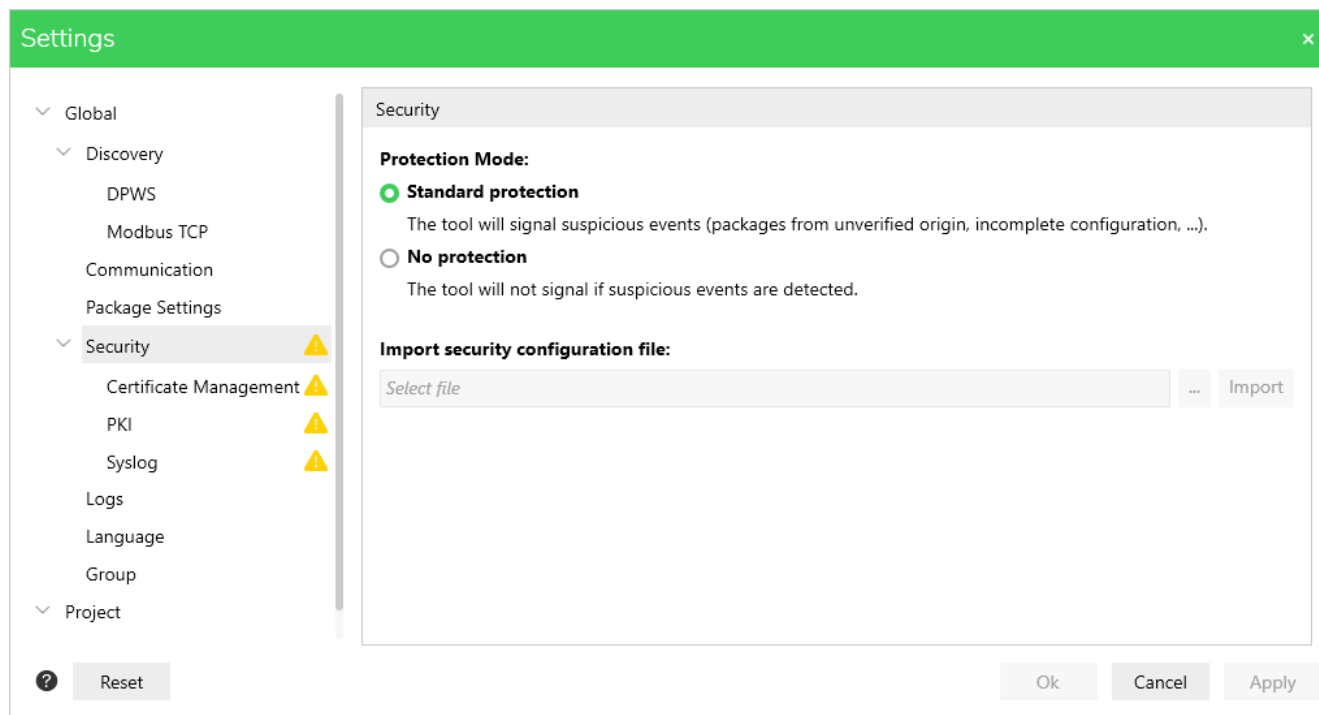
Overview

EcoStruxure Automation Device Maintenance supports the following security features:

- Encrypted communication using digital certificates in a Public Key Infrastructure (PKI).
- Handling of Schneider Electric Data Package Secure (SEDPS) digitally-signed packages.
- Syslog network protocol.

Activating / Deactivating Protection Mode

If you work within a protected network and you do not use security features, the notifications concerning security features (the yellow exclamation marks, for example) can be disabled via the **Security** option of the **Settings** page.



Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Security option.
3	Select the option to activate protection mode and to display notifications concerning security features.

Importing a Security Configuration File

EcoStruxure Automation Device Maintenance allows you to import security configuration settings that you have configured globally for your network within the EcoStruxure Cybersecurity Admin Expert application. If these settings are available as a file, import the file as follows:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Security option.
3	In the Import security configuration file section click the Import button to navigate to the security configuration file.
4	Click Open to import the security configuration settings from the file.

To update the security configuration file, use the **Update Center** as described in the chapter [Updating the Security Configuration File](#), page 69.

Managing Certificates

Overview

Digital certificates are required for secured communication via respective protocols (for example, HTTPS) in a Public Key Infrastructure (PKI).

In the context of TLS, certificates can be used to verify the identity of the communication partners. Certificates are sent during the establishing of a connection, the so-called TLS handshake. The sending of the certificate is optional for the client (in this case: the application certificate of EcoStruxure Automation Device Maintenance), unless the server requests the client certificate. The server is sending its certificate at every time. Only if the result of the verification of the certificate is positive a connection with the communication partner can be established.

EcoStruxure Automation Device Maintenance supports the following certificate trust modes:

- Manual trust mode: You can trust / untrust certificates of participants of secured communication manually. The trust status is managed in the **Trusted Certificates / Untrusted Certificates** tabs of the **Certificate Management** dialog box, page 45.
- Allowlist trust mode: You can import an allowlist with the security configuration file, page 41. EcoStruxure Automation Device Maintenance then trusts the certificates in this list automatically.
- Certificate Authority (CA) / enrollment trust mode: EcoStruxure Automation Device Maintenance automatically trusts the certificates that are enrolled with CA certificates that are available in the folder **Trusted Root Certification Authorities** of the Windows **Certificate Store**.

Considerations When Using Certificates

Consider the following when you use certificates for secured communications:

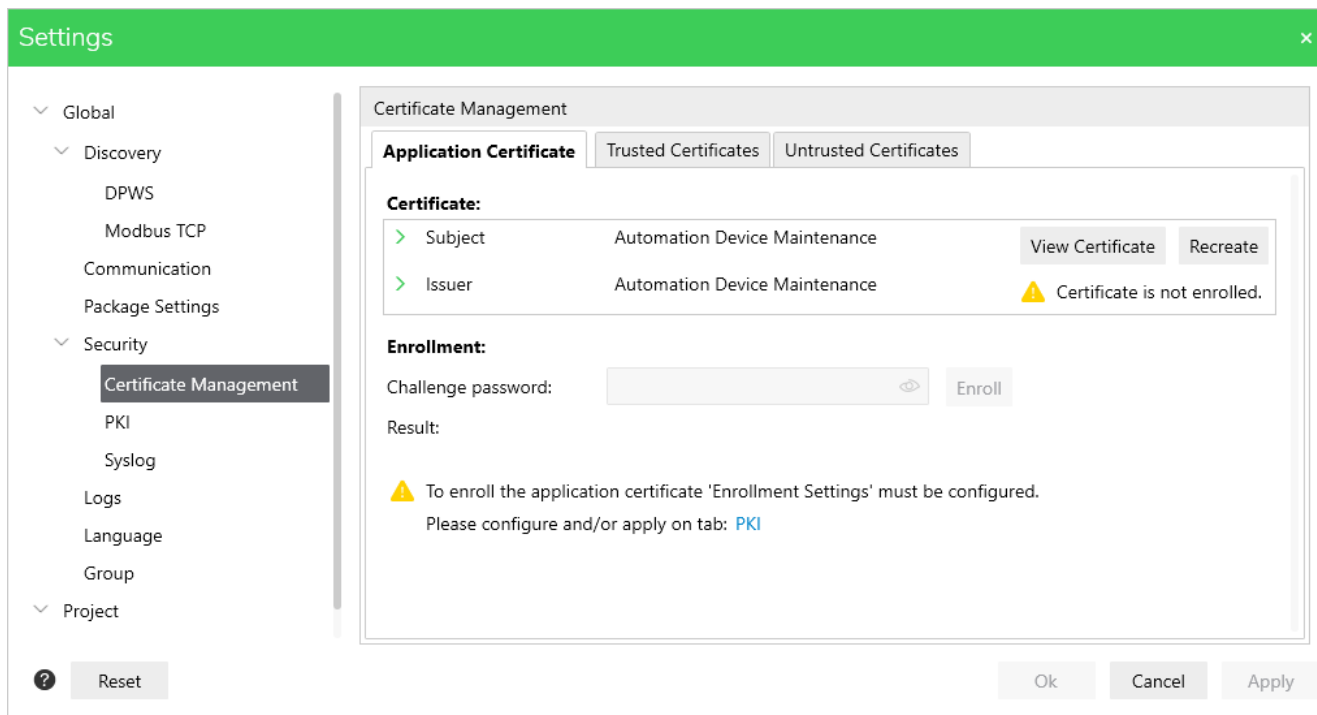
- Administration of certificates is required as they have a limited validity and therefore need to be updated in regular intervals. Consider this with respect to the life cycle of your machine or control.
- The data and time settings of your Windows PC are used to verify whether the certificate is still valid. Verify the settings in regular intervals via Windows **Start > Settings > Time & language > Date & Time**.
- If your PC running EcoStruxure Automation Device Maintenance is permanently offline, you have to update the **Certificate Revocation List** (CRL) manually in regular intervals. To achieve this, connect to your CRL Distribution Point, download the latest CRL and install it to your PC.
For the correct URL of the CRL Distribution Point, consult your security administrator.
- You can also declare certificates as untrusted in EcoStruxure Automation Device Maintenance, for example, via the **Certificate Management** dialog box, page 45.

Certificate Management Dialog Box

After initial installation, a default self-signed application certificate is available for EcoStruxure Automation Device Maintenance.

The **Certificate Management** dialog box provides the following options for the application certificate:

- Recreating the self-signed application certificate and assigning individual properties (see [Recreating the Self-Signed Application Certificate](#), page 43).
- Enrolling the application certificate to assign a digital signature of a Certificate Authority (CA) and to create a chain of trust (see [Enrolling the Application Certificate](#), page 44).
- Managing the trust status of digital certificates of communication partners (see [Managing the Trust Status of Certificates](#), page 45).



Recreating the Self-Signed Application Certificate

Follow these steps to recreate the default application certificate and to assign your individual properties:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Security > Certificate Management option.
3	In the Application Certificate tab, click the Recreate button. Result: The Create Certificate dialog box opens.
4	Enter the properties you want to assign to the certificate and click the Ok button. Result: The self-signed EcoStruxure Automation Device Maintenance certificate is presented to other participants of the communication with the properties you defined.

Enrolling the Application Certificate

To create a chain of trust, the EcoStruxure Automation Device Maintenance application certificate must be enrolled and digitally signed by a Certificate Authority (CA).

To enroll the certificate, first configure the **Enrollment Settings** as provided by the **Settings > Security > PKI** option, page 47.

Then, follow these steps to enroll the application certificate for EcoStruxure Automation Device Maintenance:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Security > Certificate Management option.
3	In the Application Certificate tab, verify that the application certificate is still self-signed and not yet enrolled: <ul style="list-style-type: none"> In the Certificate section, both Subject and Issuer display the same content: Automation Device Maintenance. The notification Certificate is not enrolled. is displayed in the Issuer line.
4	Enter your password for the CA in the Challenge password text box. This password is used for authorizing the enrollment request. For details, refer to your industrial network administrator.
5	Click Enroll . Result: EcoStruxure Automation Device Maintenance sends a certificate signing request from the application certificate together with the challenge password to the CA. If the password is not correct, an Enrollment not successful message will be returned. NOTE: This procedure replaces the default self-signed application certificate by a new signed certificate. The replacement cannot be undone.
6	Verify whether the process has been successfully completed: <ul style="list-style-type: none"> Result: Enrollment was successful is displayed in the Application Certificate tab. In the General tab of the Certificate Information dialog box, the Issuer entry has changed to the name of the CA, for example, <i>INT-DEV-SUB-CA</i>. The Certification Path tab of the Certificate Information dialog box indicates the root CA and the subordinate CAs in a hierarchical structure depending on your PKI configuration. The end entity certificate at the bottom of the hierarchical structure is the certificate of EcoStruxure Automation Device Maintenance with the following entries: <ul style="list-style-type: none"> CN (Common Name) = Automation Device Maintenance O (Organization) = Schneider Electric

Managing the Trust Status of Certificates

The tabs **Trusted Certificates** and **Untrusted Certificates** of the **Certificate Management** dialog box allow you to manage the trust status of certificates that are available in EcoStruxure Automation Device Maintenance.

In both tabs, each certificate is listed providing the following information:

Component	Description
Subject	Provides general information on the certificate: <ul style="list-style-type: none"> • CN = Common Name • OU = Organization Unit
Device Name	Provides the name of the device as it is displayed in the DEVICE LIST of the Device/Loading tab. If the certificate does not belong to a device, n/a is displayed.
Service Endpoint	The information on the service endpoint is provided for devices that are used in the present EcoStruxure Automation Device Maintenance session. If the certificate does not belong to a device, n/a is displayed.
Action	Allows you to open the Certificate Information dialog box via the View Certificate link.
Certificates Status	Indicates the status of the certificate: <ul style="list-style-type: none"> • Trusted • Untrusted

You can perform the following actions on certificates:

- To untrust certificates, select one or more certificates in the **Trusted Certificates** tab and click the **Untrust** button.
- To trust certificates, select one or more certificates in the **Untrusted Certificates** tab and click the **Trust** button. To trust the selected certificate/s temporarily, select the option **Trust this session**.
- To remove certificates, select one or more certificates in the **Trusted Certificates** or **Untrusted Certificates** tab and click the **Delete** button.


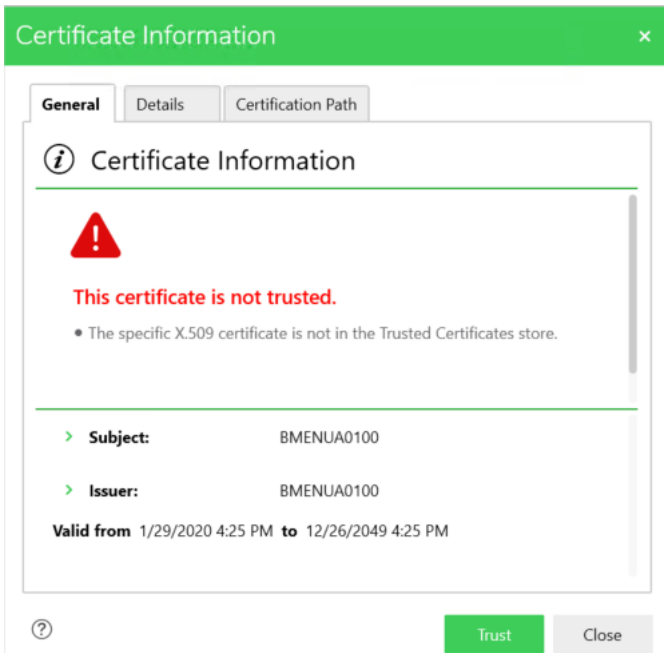
NOTE: Certificates of devices that are being used in the present EcoStruxure Automation Device Maintenance session cannot be deleted directly. The certificates are temporarily shifted to the list of **Untrusted Certificates** and will be removed when EcoStruxure Automation Device Maintenance is closed.

NOTE: Executing this command removes the selected certificates from the Windows PC. They will also be removed from the Windows **Certificate Store**.


Managing the Trust Status of Certificates in the Device/Loading Tab

You can also trust / untrust certificates of devices in the **Device/Loading** tab.

Follow these steps to trust the device certificate in the **Device/Loading** tab:

Step	Action
1	<p>Click the Device certificate icon  of the device.</p>  <p>NOTE: You can trust the server certificate temporarily.</p>
2	Select the check box to Trust the server certificate temporarily for the current session .
3	Click Trust Server Certificate .

Follow these steps to untrust the device certificate in the **Device/Loading** tab:

Step	Action
1	Click the Device certificate icon  of the device.
2	Click Untrust Server Certificate .

Managing the Public Key Infrastructure (PKI)

Settings for Enrolling the Application Certificate

If the **Security** option is enabled in the **Security** dialog box of the **Settings** page, the **PKI** dialog box allows you to configure the connection to the Certification Authority (CA) for enrolling the application certificate of EcoStruxure Automation Device Maintenance.

Settings

- Global
 - Discovery
 - DPWS
 - Modbus TCP
 - Communication
 - Package Settings
 - Security
 - Certificate Management
 - PKI**
 - Syslog
 - Logs
 - Language
 - Group
 - Project

PKI

Enrollment Settings:

Enrollment URL:

Issuer ID:

Timeout: ms

Verify Signature Only: ☐

Component	Description
Enrollment URL	Enter the Uniform Resource Locator (URL) of the Certification Authority (CA) that will issue the certificate.
Issuer ID	Enter the identifier of your certification authority issuer.
Timeout	Enter a timeout (in milliseconds) that corresponds to your Internet transfer rates. Default value: 10,000 ms
Verify Signature Only	If this option is not selected, the CA certificate must be available as trusted certificate in the Windows Certificate Store . To verify the digital signatures only, select this option.
Check connection button	Click the Check connection button to establish a connection to the website of the CA.
View Certificate button	After the connection to CA has been established successfully, the View Certificate button is displayed. Click the button to open the Certificate Information dialog box and verify the attributes of the certificate to help ensure that you are connected to the correct CA.

If the connection to the website of the CA has been successfully established, select the **Security > Certificate Management** option and proceed with the enrollment of the application certificate.

Activating Syslog Message Logging


Overview

The **Syslog** dialog box allows you to activate the syslog function and to configure EcoStruxure Automation Device Maintenance as a syslog client. EcoStruxure Automation Device Maintenance will then provide a subset of the log messages it generates to the corresponding syslog server by using the syslog settings configured in this dialog box.

The screenshot shows the 'Settings' application window with a green header bar. On the left is a sidebar menu with categories: Global, Discovery, Communication, Package Settings, Security, and Project. Under 'Security', 'Syslog' is selected and highlighted. The main area displays the 'Syslog' configuration dialog. At the top, it says 'Syslog:' followed by radio buttons for 'Enable' and 'Disable', with 'Disable' selected and a yellow warning triangle icon. Below this, there are input fields for 'Server Address' (containing '127.0.0.1') and 'Port' (containing '6514'). Under 'Network Protocol', there are radio buttons for 'UDP', 'TCP', and 'TLS', with 'TLS' selected. A 'Check connection' button is located below the protocol selection. At the bottom of the dialog are three buttons: 'Ok', 'Cancel', and 'Apply'. A 'Reset' button is also visible in the bottom left corner of the settings window.

Activating Syslog Message Logging

Follow these steps to activate the syslog function and to configure the connection to the syslog server:

Step	Action
1	Click Settings menu at the top center of the Home page.
2	Select the Security > Syslog option.
3	Select the option Enable to activate the syslog function.
4	In the Server Address text box, enter the IP address of your syslog server.
5	Enter the Port the server is monitoring for syslog messages from the clients.
6	Select the Network Protocol option: <ul style="list-style-type: none"> • UDP (User Datagram Protocol) • TCP (Transmission Control Protocol) • TLS (Transport Layer Security)
7	<p>For TCP or TLS connections, you can optionally click the Check connection button to verify the connection to the syslog server.</p> <p>Results:</p> <p>For TCP connections: A message is displayed indicating whether a connection to the server has been established.</p> <p>For TLS connections:</p> <ul style="list-style-type: none"> • A message is displayed indicating whether a connection to the server has been established. • An icon indicates whether the certificate of the syslog server is already declared as trusted. If the certificate is untrusted, click the  icon to open the Certificate Information dialog box that allows you to verify the certificate and to declare it as trusted. <p>NOTE: As UDP is based on a connectionless communication model, EcoStruxure Automation Device Maintenance cannot provide a solution to verify the connection. You must verify manually whether syslog messages are received on the server you specified.</p>

Data Package

Data Package Tab

Supported Data Package Types

The following file types are supported:

- *.fwp
- *.ldx
- *.sedp
- *.sedps

Secured Data Packages

EcoStruxure Automation Device Maintenance supports *.sedps (Schneider Electric Data Package Secure) data packages that are digitally signed: When protection mode is enabled, EcoStruxure Automation Device Maintenance verifies that this package comes from a verified origin and displays security notifications if the signature is not correct. For a general description of handling certificates, refer to the chapter [Managing Certificates](#), page 42.

If protection mode is activated, page 41, the following applies:

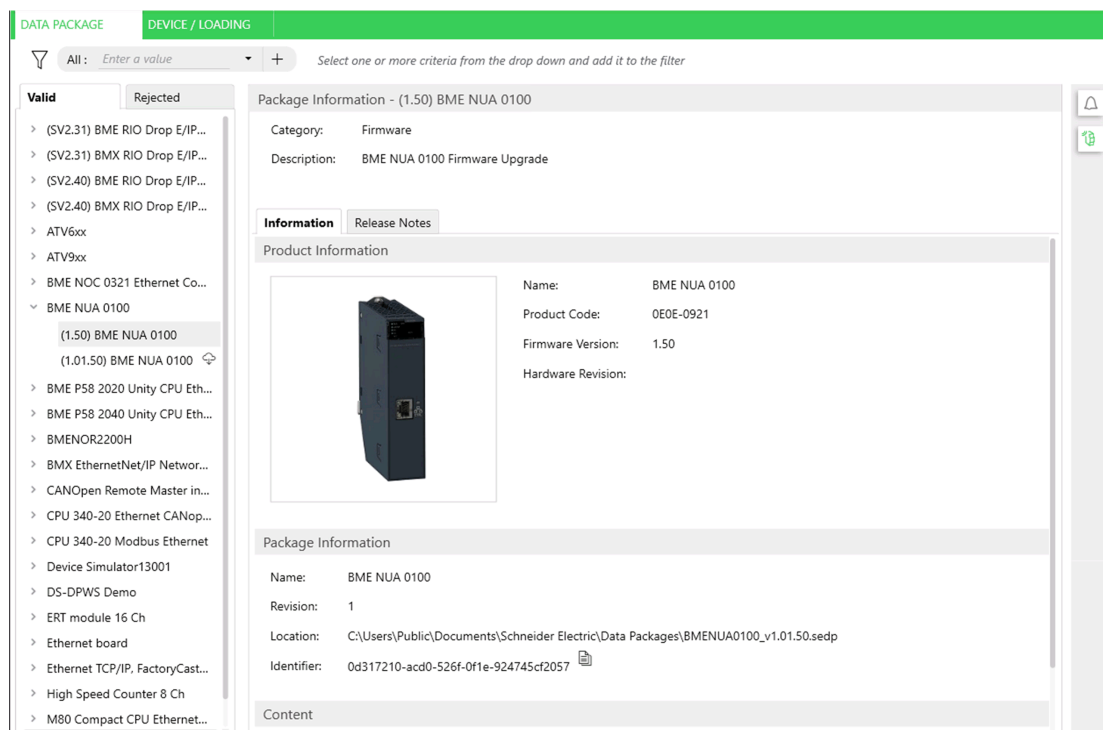
- The following package files are marked by the yellow notification icon in the list of packages of the **Data Package** tab and the message **Package is not from verified origin** is displayed on the right-hand side:
 - Unsigned package files.
 - Self-signed package files.
 - Package files that are using a root certificate that is not trusted.
- These packages are also marked in the **Device/Loading** tab by the yellow notification icon.
- If you attempt to perform an update firmware process with one of these data packages, the process is paused and the message **Trust chain of selected package cannot be verified. The download can harm the device. Do you want to continue?** is displayed in the [notification area](#), page 65. Carefully read the message and evaluate the risks. After you have confirmed the message, the process will continue.
- If you attempt to perform an update firmware process with one of these data packages, detected errors are displayed in the [Logs](#) window, page 66.

NOTICE
HARMED DEVICES Carefully verify if the data package originates from a trusted source because the download of a tampered data package can harm your device. Failure to follow these instructions can result in equipment damage.

Overview of the Data Package Tab

You can view the content of the data package library to find details of the individual packages and the content.

The left-hand side of the tab displays the list of locally available data packages grouped by device family. The right-hand side of the tab displays the details of the selected package.



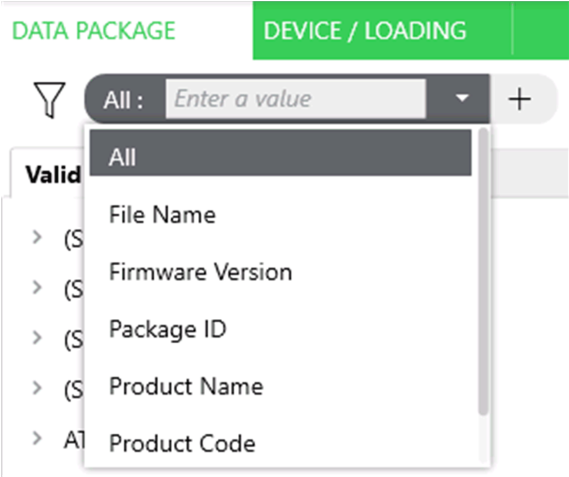
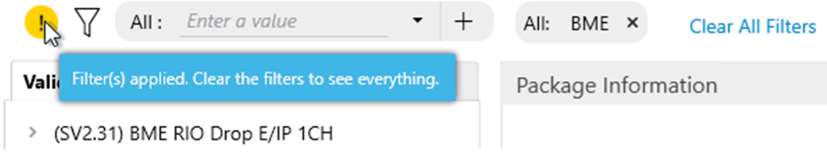
List of Data Packages

The list of data packages on the left-hand side consists of two tabs:

- The **Valid** tab lists the data packages that are locally available on your PC grouped by device family.
- The **Rejected** tab lists data packages that you downloaded to your PC but cannot be processed for any reason. As the data package file may have become corrupted during the download process, it may help to download it a second time. If this does not solve the issue, contact your Schneider Electric representative for further assistance.

Filtering the Data Packages List

To reduce the number of data packages displayed in the list, you can apply search criteria as follows:

Step	Action
1	<p>Enter a string in the text field All. To limit the search on a specific data package property, you can optionally open the list and select a search criterion.</p> 
2	<p>Click the plus button on the right-hand side of the search list to start the search.</p> <p>Result: The data package list displays entries that meet the search criterion you entered. A yellow icon is displayed left to the search box indicating that a filter is applied and that the list entries are therefore reduced to those data packages meeting the search criterion.</p> 
3	<p>Repeat steps 1 and 2 to define another filter. The filters are AND combined.</p> <p>Result: The data package list displays entries that meet both search criteria.</p>
4	<p>To clear a single filter, click the cross button of this filter.</p> <p>Alternatively, to remove all filters you defined, click the Clear all Filters link. You will see the complete list of data packages.</p>

Package Information

The **Package Information** on the right-hand side provides information on the data package that is selected in the list of data packages.

The upper part provides the following information:

- **Category**
- **Description**

The **Information** tab displays the following details:

- **Product Information** section:
 - Picture - if available in the data package
 - **Name**
 - **Product Code**
 - **Firmware Version**
 - **Hardware Revision**
- **Package Information** section:
 - **Name**
 - **Revision**
 - **Location**
 - **Identifier:** The **Copy to Clipboard** button allows you to copy the identifier string to the Clipboard of your PC.
- **Content** section: Provides the content of the data package in a list.


The **Release Notes** tab displays content if the data package contains a document labeled as `ReleaseNotes`. If no such document exists for the data package, the tab will be empty.

Device/Loading

Device/Loading Tab

Overview

EcoStruxure Automation Device Maintenance displays a certain set of device properties (such as device name, service endpoint, firmware version) in the **Device/Loading** tab.

NOTE: Information displayed in this tab is only updated automatically if the discovery mode is set to **Automatic**. Click the  icon from the toolbar to display the latest values.

DATA PACKAGE

DEVICE / LOADING

DEVICE LIST

⊕ Add

🔌 Connect

🔌 Disconnect

📶 Update Center

🔌 Hide


🗑 Dispose

🔍

<input type="checkbox"/>	Status	Device Name Commercial Reference	Service Endpoint Serial Number	Firmw... Version	Security Configurat...	Mode	Update Center Info	Extensions	Actions
<input type="checkbox"/>	Device Default Group (7)								
<input type="checkbox"/>	●	ATV630U07M3_dda1fa CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94B01	-	-	-	-	<div><div>👤</div><div>🔌</div><div>📶</div><div>📶</div><div>🗑</div><div>🔌</div><div>🔍</div></div>
<input type="checkbox"/>	●	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94B02	-	-	-	-	<div><div>👤</div><div>🔌</div><div>📶</div><div>📶</div><div>🗑</div><div>🔌</div><div>🔍</div></div>
<input checked="" type="checkbox"/>	●	ATV630EIP CR: ATV630U07M3	mbap://172.20.170.209:502 SN: 4004000HL44718401Y	2.6IE94B13	-	-	-	-	<div><div>👤</div><div>🔌</div><div>📶</div><div>📶</div><div>🗑</div><div>🔌</div><div>🔍</div></div>

For information on the details displayed for the devices, refer to the chapter [Device/Loading](#), page 20.

Details Available After Login

After you have successfully logged into a device and the device status has changed to green, click the  button to get access to the following commands for each device:

Command	Description
Optical	The device issues an optical signal to help you identifying it in a hardware rack for devices supporting the feature.
Optical and acoustical	The device issues an optical and an acoustical signal to help you identifying it in a hardware rack for devices supporting the feature.
Properties	<p>Opens an additional Properties dialog box that provides further information on the device in different tabs:</p> <ul style="list-style-type: none"> • Device Information tab provides general information on the device: <ul style="list-style-type: none"> ◦ Product Id ◦ Product Name ◦ Firmware Version ◦ Hardware Revision ◦ Hardware-ID ◦ MAC Address • Device status tab provides information on the present status of the device. • Configuration tab provides information on the configuration settings of the device. If supported by the device, configuration settings can be modified in this tab. <p>NOTE: Modifications of the configuration settings may require a restart of the device which may have the effect that the controller is set to STOP state. The effects are indicated by messages displayed in the notification area. Carefully read each message and confirm after you have evaluated the risks. After you have confirmed each message, the process will continue.</p> <p>The Properties information displayed depends on the respective device. For further information, refer to the user documentation of your device.</p>

Grouping Devices in the DEVICE LIST

Overview

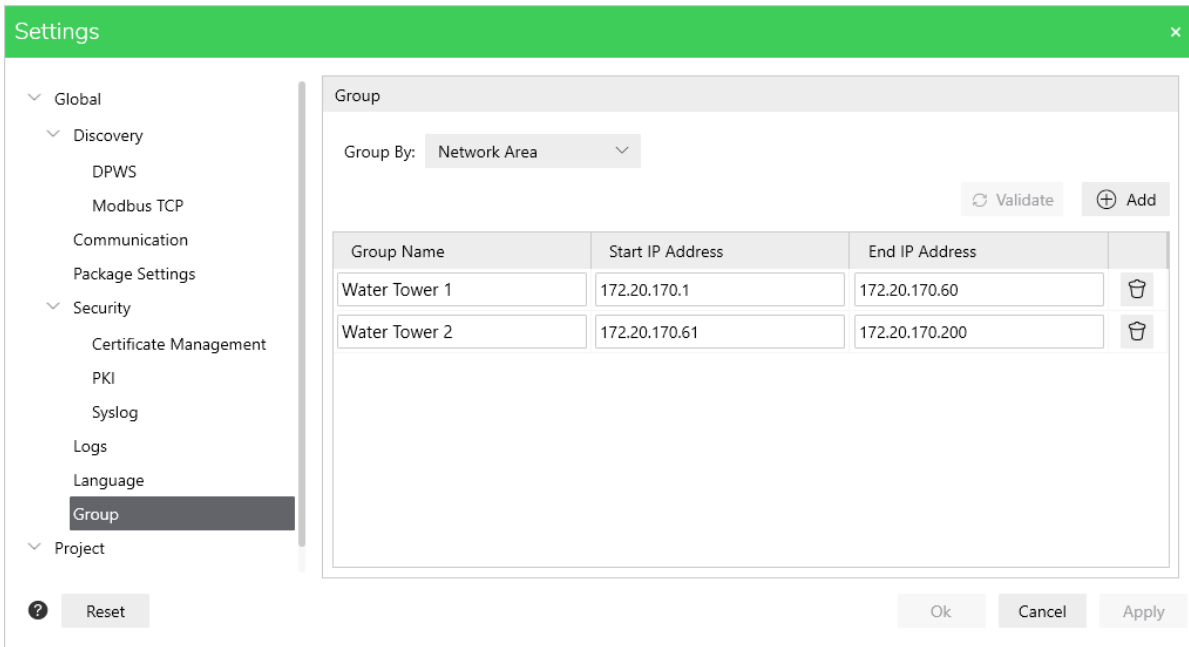
EcoStruxure Automation Device Maintenance allows you to structure the devices displayed in the **DEVICE LIST** by creating groups.

EcoStruxure Automation Device Maintenance V3.0 supports grouping according to the IP addresses of the devices by defining IP address ranges. Additional grouping criteria might be added with later EcoStruxure Automation Device Maintenance versions.

NOTE: This grouping function is exclusive to IPv4 addresses. The IPv6 standard is not supported by EcoStruxure Automation Device Maintenance V3.0.

Creating Groups

Follow these steps to group devices:

Step	Action
1	Select the Group option on the Settings page.
2	Expand the Group By list and select the option Network Area .
3	Click the + Add button to create a new address range. Result: A table with an empty line is displayed.
4	In the Group Name cell enter a name for your group of devices.
5	In the Start IP Address cell enter the first IP address of the address range for your group of devices.
6	In the End IP Address cell enter the last IP address of the address range for your group of devices. 
7	Click the + Add button to create another group. Or Click Apply to apply the Group settings. Or Click Ok to apply all application settings modifications and to close the Settings dialog box.

Removing Device

Overview






You can remove the devices by temporarily hiding or permanently disposing them from the **Device List** tab in the **Device/Loading** menu.

The device can be removed by performing the following activities:

- Hiding an active device
- Disposing an active device
- Disposing a hidden device




Hiding an Active Device

Follow these steps to hide an active device:

Step	Action
1	Click Device/Loading tab. Discovered active devices are listed under the Device List tab.
2	In the Device/Loading : <ul style="list-style-type: none"> Select a single device by clicking a cell in the row of the device. OR Select multiple devices by selecting the check boxes on the left-hand side of each row or by selecting the entire Group.
3	The following icons are activated for selected devices: <ul style="list-style-type: none">  Hide  Dispose
4	Click the  icon. The Hide Device message will be displayed. <div> <div>Hide Device ×</div> <div>  Are you sure you want to move the selected device(s) to HIDDEN DEVICE LIST? Once hidden, you can reactivate the device(s) from the HIDDEN DEVICE LIST. </div> <div>  <div>Yes No</div> </div> </div>
5	Click Yes to proceed. The selected device is moved to Hidden Device List tab. NOTE: You can reactivate the hidden devices from the Hidden Device List .




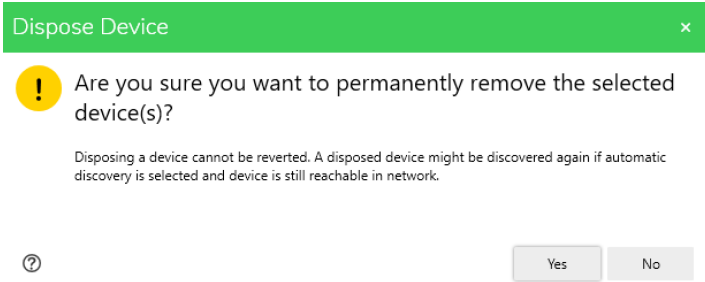
Unhiding a Hidden Device

Follow these steps to unhide a hidden device:

Step	Action
1	<p>Click Device/Loading tab.</p> <p>Hidden devices are listed under the Hidden Device List tab.</p>
2	<ul style="list-style-type: none">• Select a single device by clicking a cell in the row of the device.OR• Select multiple devices by selecting the check boxes on the left-hand side of each row or by selecting the entire Group.
3	<p>The following icons are activated for selected devices:</p> <ul style="list-style-type: none">•  Unhide•  Dispose
4	<p>Click the  Unhide icon.</p> <p>The selected device is moved to Device List tab.</p>




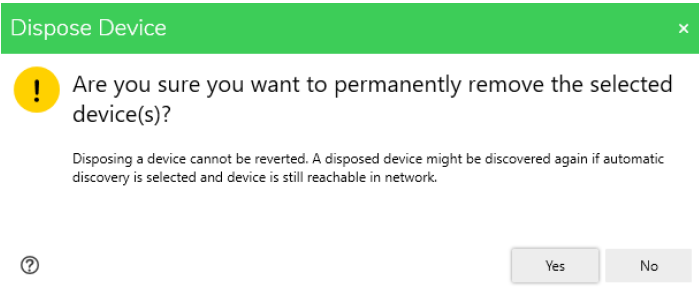
Disposing an Active Device

Follow these steps to dispose an active device:

Step	Action
1	Click Device/Loading tab. Discovered active devices are listed under the Device List tab.
2	<ul style="list-style-type: none"> Select a single device by clicking a cell in the row of the device. OR Select multiple devices by selecting the check boxes on the left-hand side of each row or by selecting the entire Group.
3	<p>The following icons are activated for selected devices:</p> <ul style="list-style-type: none">  Hide  Dispose
4	<p>Click the  Dispose icon.</p> <p>The Dispose Device message will be displayed.</p> 
5	<p>Click Yes to proceed.</p> <p>NOTE: Choosing Yes will dispose the device permanently from the tool and to get the device back into the tool it must either be discovered or manually added again.</p>

Disposing a Hidden Device

Follow these steps to dispose a hidden device:

Step	Action
1	Click Device/Loading tab. Hidden devices are listed under the Hidden Device List tab.
2	<ul style="list-style-type: none"> Select a single device by clicking a cell in the row of the device. OR Select multiple devices by selecting the check boxes on the left-hand side of each row or by selecting the entire Group.
3	<p>The following icons are activated for selected devices:</p> <ul style="list-style-type: none">  Unhide  Dispose
4	<p>Click the  icon.</p> <p>The Dispose Device message will be displayed.</p>  <p>The dialog box shows a green header "Dispose Device" with a close button. Below it is a yellow warning icon and the text: "Are you sure you want to permanently remove the selected device(s)?". A smaller note states: "Disposing a device cannot be reverted. A disposed device might be discovered again if automatic discovery is selected and device is still reachable in network." At the bottom are a help icon, "Yes", and "No" buttons.</p>
5	<p>Click Yes to proceed.</p> <p>NOTE: Choosing Yes will dispose the device permanently from the tool and it cannot be retrieved.</p>

Managing User Credentials



Overview

EcoStruxure Automation Device Maintenance allows you to enter credentials for authorized access to the devices globally for the project and individually for each device.


Managing User Credentials Globally

To manage user credentials globally for the project, go to the **Settings** page and select the option **Project > User Credential Settings**.


Select **Authentication Type > Username** or **Authentication Type > Custom** and enter the credentials as required. Click **Ok** to save the credentials. As a result, the **Set credentials** icon of the applicable devices in the **Device/Loading** page is set

to yellow and you can click the **Connect** icon  or button  for login without entering the credentials again.

Managing User Credentials per Device

To manage user credentials for each device individually, open the **Device/Loading** page and click the **Set credentials** icon  in the device row of the table:

You can click **Save and Connect** to save the credentials and establish a connection to the device. After successful login, the **Set credentials** icon turns green. As an alternative, you can click **Save** to save the credentials for this device for later login. In this case, the **Set credentials** icon turns yellow and you can click

the **Connect** icon  or button  for login without entering the credentials again.

User Credential Parameters

The parameters displayed are device-specific and request the credentials that are required for login to the specific device. For further information, refer to the user documentation of your device.














For login to Modicon M340, Modicon M580 or Momentum controllers, three passwords are required. For detailed information on the application protection password, the data storage password, and the firmware protection password, refer to the corresponding chapters in the *EcoStruxure Control Expert Operating Modes* or the legacy *Unity Pro Operating Modes* manual. The download links for translations of this manual are provided in the list of Related Documents in this online help, page 9.

Accessing Extensions





Overview


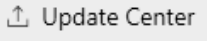
A modular device in the **DEVICE LIST** of the **Device/Loading** tab provides a link that allows you to access the individual extensions of the device.

Example of a modular device:

DATA PACKAGE									
DEVICE / LOADING									
DEVICE LIST									
<div>⊕ Add ⚙ Connect ⚙ Disconnect ↗ Update Center ⚙ Hide 🗑 Dispose</div>									
<input type="checkbox"/>	Status	Device Name Commercial Reference	Service Endpoint Serial Number	Fi... V...	Secu... Conf...	M...	Update Center Info	Exte...	Actions
Device Default Group (6)									
<input type="checkbox"/>	●	ATV930U07M3_b3aa7d CR: ATV930U07M3	mbap://172.20.170.213:502 SN: 4030000HL704004007	3.5IE9...	-	-	-	-	      
<input type="checkbox"/>	●	ATV630U07M3 CR: ATV630U07M3	mbap://fe80::280:f4ff:fec2:3639%17 SN: 18c23639	3.5IE9...	-	STOP	-	Extensions	     

If supported by the device, the **Extensions** link ([Extensions](#)) opens a new **Extensions** tab and provides the modular devices grouped by **Extension**.

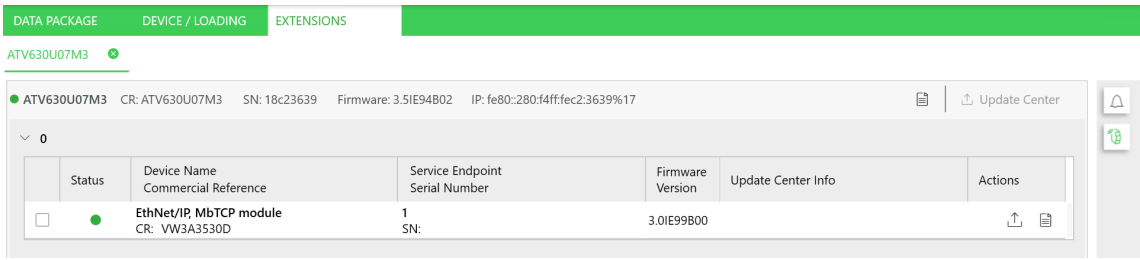
DATA PACKAGE									
DEVICE / LOADING									
EXTENSIONS									
ATV630U07M3 ●									
● ATV630U07M3 CR: ATV630U07M3 SN: 18c23639 Firmware: 3.5IE94B02 IP: fe80::280:f4ff:fec2:3639%17  									
▼ 0									
<input type="checkbox"/>	Status	Device Name Commercial Reference	Service Endpoint Serial Number	Firmware Version	Update Center Info	Actions			
<input type="checkbox"/>	●	EthNet/IP, Modbus module CR: VW3A3530D	1 SN:	3.0IE99800	-	 			

Both tabs provide access to the **Update Center** dialog box (via the **Update Center** icon  or the **Update Center** button ) that allows you to select the firmware data package via the **Firmware** button.

For devices that cannot load the extensions on demand by clicking the **Extensions** link, follow the process described in the next section to access individual extensions.


Accessing Extensions Manually

For devices that cannot load the extensions on demand by clicking the **Extensions** link, proceed as follows:

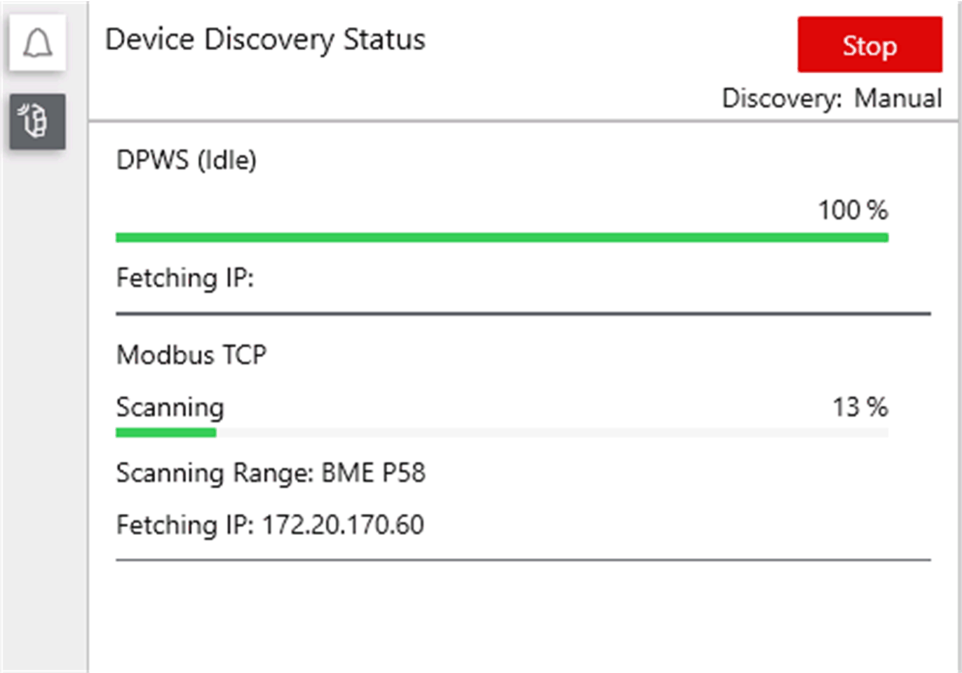
Step	Action
1	Click the link Extensions of the modular device. Result: The Extensions tab opens. If the device cannot load the extensions on demand by clicking the Extensions link, an Add button is provided.
2	Click the Add button or the link No module found. To add module click here . Result: The dialog box Add Module opens.
3	In the dialog box Add Module , configure the parameters for accessing the extensions of the device: <ul style="list-style-type: none"> Rack number Slot number
4	Click the OK button to start the discovery scan. When the extensions have been successfully detected, the Extensions tab is displayed. 
5	Close the Extensions tab.

Monitoring the Device Discovery Status

Overview

Whenever the device discovery process is running, you can retrieve the status on this process by clicking the  button in the **Device/Loading** tab.

The **Device Discovery Status** view opens on the right-hand side:



It displays the following information:


- Progress information is provided for each scanner individually.
- If different ranges are configured for a scanner, progress information is provided for each range individually (for example, for Modbus TCP scanner, page 33).

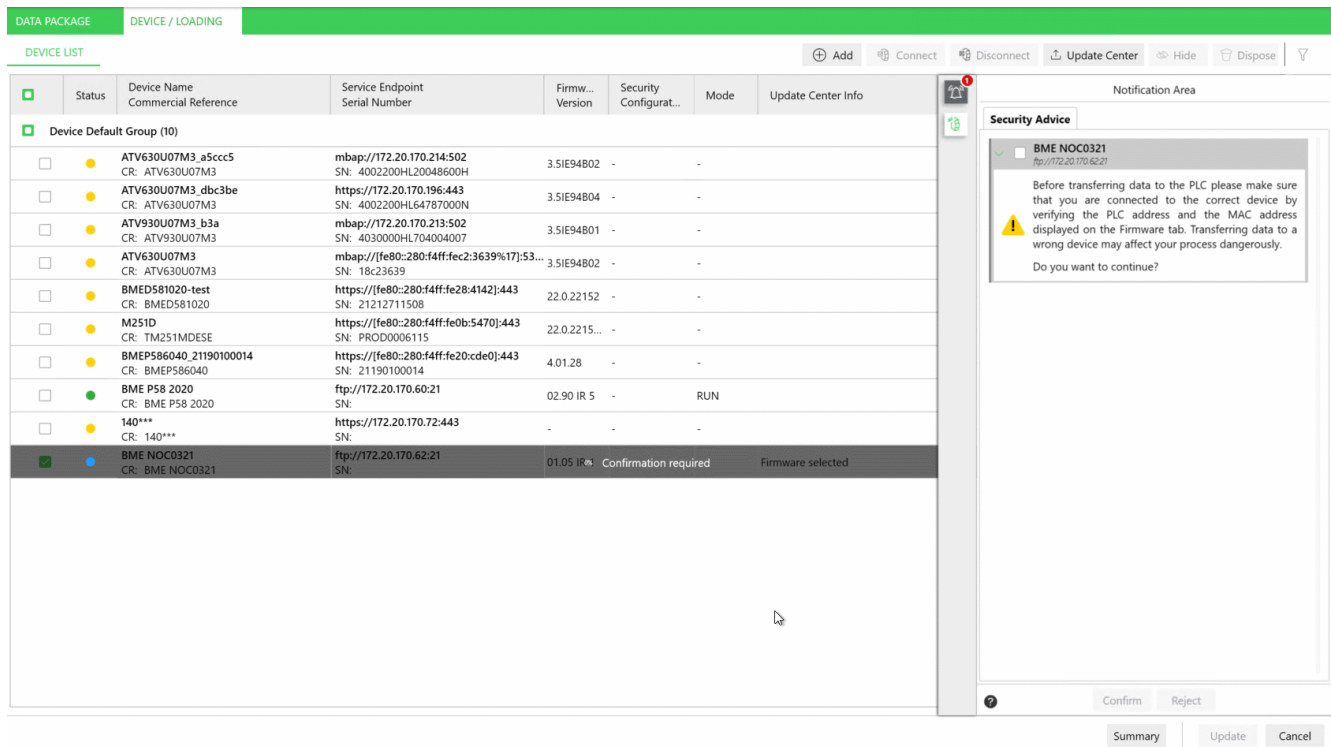
The **Start/Stop** button allows you to start a manual device discovery or to stop a running device discovery process directly from this view.

Viewing / Confirming Messages

Overview

Some of the processes that are executed by EcoStruxure Automation Device Maintenance require user interactions. Whenever confirmation is required, the process, such as updating the firmware, is paused and a message is displayed in the notification area. Carefully read each message and confirm after you have evaluated the risks. After you have confirmed each message, the process will continue.

To open the notification area, click the  button in the **Device/Loading** tab.



The screenshot shows the 'DEVICE / LOADING' tab in the EcoStruxure Automation Device Maintenance interface. The 'DEVICE LIST' table contains the following data:

Status	Device Name Commercial Reference	Service Endpoint Serial Number	Firmw... Version	Security Configurat...	Mode	Update Center Info
<input checked="" type="checkbox"/>	Device Default Group (10)					
<input type="checkbox"/>	ATV630U07M3_a5ccc5 CR: ATV630U07M3	mbap://172.20.170.214:502 SN: 4002200HL20048600H	3.5IE94802	-	-	
<input type="checkbox"/>	ATV630U07M3_dbc3be CR: ATV630U07M3	https://172.20.170.196:443 SN: 4002200HL64787000N	3.5IE94804	-	-	
<input type="checkbox"/>	ATV930U07M3_b3a CR: ATV930U07M3	mbap://172.20.170.213:502 SN: 4030000HL704004007	3.5IE94801	-	-	
<input type="checkbox"/>	ATV630U07M3 CR: ATV630U07M3	mbap://[fe80::280:f4ff:fe2:3639%17]:53... SN: 18c23639	3.5IE94802	-	-	
<input type="checkbox"/>	BMED581020-test CR: BMED581020	https://[fe80::280:f4ff:fe28:4142]:443 SN: 21212711508	22.0.22152	-	-	
<input type="checkbox"/>	M251D CR: TM251MDESE	https://[fe80::280:f4ff:fe0b:5470]:443 SN: PROD0006115	22.0.2215...	-	-	
<input type="checkbox"/>	BMPE586040_21190100014 CR: BMPE586040	https://[fe80::280:f4ff:fe20:cde0]:443 SN: 21190100014	4.01.28	-	-	
<input type="checkbox"/>	BME P58 2020 CR: BME P58 2020	ftp://172.20.170.60:21 SN:	02.90 IR 5	-	RUN	
<input type="checkbox"/>	140*** CR: 140***	https://172.20.170.72:443 SN:	-	-	-	
<input checked="" type="checkbox"/>	BME NOC0321 CR: BME NOC0321	ftp://172.20.170.62:21 SN:	01.05 IR 3	Confirmation required	Firmware selected	

The 'Notification Area' on the right displays a 'Security Advice' message for BME NOC0321. The message text is: 'Before transferring data to the PLC please make sure that you are connected to the correct device by verifying the PLC address and the MAC address displayed on the Firmware tab. Transferring data to a wrong device may affect your process dangerously. Do you want to continue?'. The message includes a warning icon and a checkbox. At the bottom of the notification area are buttons for 'Confirm', 'Reject', 'Summary', 'Update', and 'Cancel'.

Two different types of messages can be displayed in the notification area:

- Confirmation messages: Select the message by activating the check box, and click **Confirm** to confirm the message and to resume the running process or click **Reject** to stop the process.
- Notification messages: Select the message by activating the check box, and click **OK** to confirm the message and to resume the running process.

The **Don't show notifications** option allows you to disable displaying notification messages. If the option is selected, the processes will be executed automatically without interruptions for user interactions presuming that the messages are confirmed.

NOTE: Activate this option only if you are working in maintenance mode and the operator has verified the state of security of your machine or process environment.

Viewing Logs


You can view the stored logs and analyze it for details concerning the selected device.

The log information can be viewed in the following sections:

- For each device in the **Device/Loading** page
- For the entire project in the **Logs** window

NOTE: In the **Logs** window, detected errors, detected warnings, and information messages are displayed in a single window.

To view the logs exclusive to the selected device, proceed as follows:

Step	Action
1	Access the Device/Loading page.
2	<p>Click the Device log icon  of a device.</p> <p>Result: A small Log info view opens directly in the table below the device row. Use the scroll bar on the right-hand side to see all log entries, if necessary.</p>

To hide the **Log info** for a device, click the **Device log** icon  once again.

Recommendation for Improved Cybersecurity

The log file contains usually sensitive data such as


- Device addresses
- Device names
- Details of the network topology
- Details of the network configuration

It is stored on the hard disk of your PC. Delete the log file as soon as it is no longer needed or store it in a safe place, where unauthorized access is not possible.

Update Center

Overview

The **Update Center** dialog box allows you to configure the settings for performing a firmware update or an update of the security configuration file. These configuration settings can be applied to an individual device or to different devices simultaneously.

- To perform updates on an individual device, click the **Update Center** icon  in the device row of the table in the **Device/Loading** tab.
- To perform updates for different devices of the project simultaneously, select the devices in the **Device/Loading** tab, and click the **Update Center** button

 Update Center

from the button bar.

Update Center Dialog Box

Both operations open the **Update Center** dialog box that allows you to select:

- **Firmware:** For configuring settings for updating the firmware of the selected device or devices. For further information, refer to [Updating Firmware](#), page 67.
- **Security:** For configuring settings for updating the security configuration file of the selected device or devices. For further information, refer to [Updating the Security Configuration File](#), page 69.
- **Reset:** For resetting the update settings for the selected device or devices.

To confirm the settings and to close the **Update Center** dialog box, click the **Save** button. As a result, the configuration you made is indicated in the **Update Center Info** cells of the device or devices in the **Device/Loading** tab, page 20.

To execute the update process as configured, click the **Update** button.

Updating Firmware

Overview

EcoStruxure Automation Device Maintenance allows you to update the firmware of devices displayed in the **Device/Loading** tab.



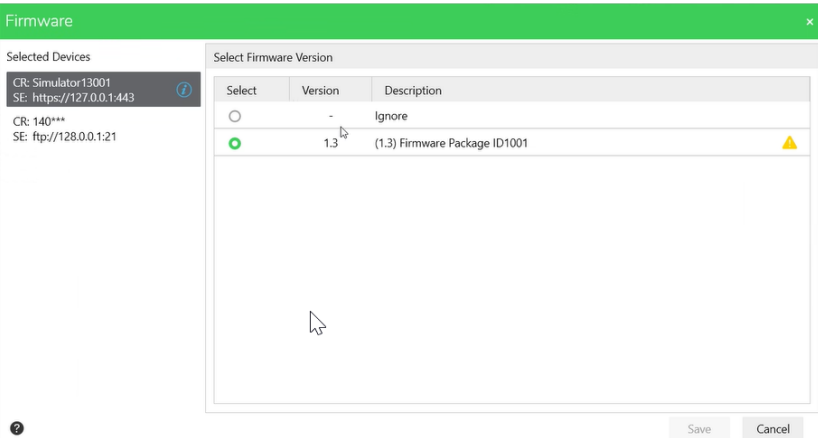
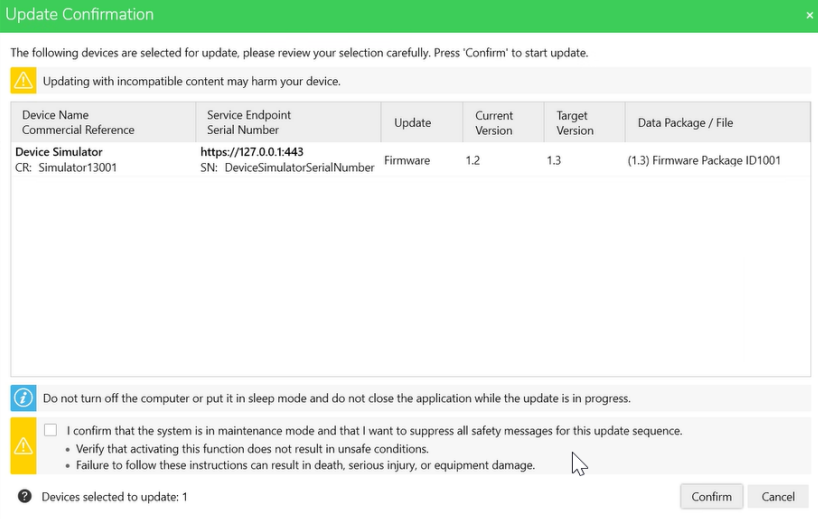
To update the firmware of modular devices, you can access the individual extensions as described in the chapter [Accessing Extensions](#), page 62.

You can select data packages for multiple extensions and / or rack modules. EcoStruxure Automation Device Maintenance will simultaneously update the firmware of those devices.

NOTE: If you perform a simultaneous update for the controller and the modules, ensure that you do not restart the controller while the update of the modules is still running. See important [hazard message](#) below.

Updating the Firmware

Execute the following steps to update the firmware:

Step	Action
1	Access the Device/Loading page.
2a	To perform updates on an individual device, click the Update Center icon  in the row of the device.
2b	To perform updates for different devices of the project simultaneously, select the check boxes of the devices or select the check box of the entire Group and click the Update Center button  from the button bar.
3	In the Update Center dialog box, click the Firmware button.
4	In the Firmware dialog box, select the firmware data package for each device. 
5	Click Save to save the firmware update configuration and to close the Firmware dialog box. Result: The Update Center Info cell or cells of the device or devices in the Device/Loading tab, page 20 display the text Firmware selected .
6	Click the Update button from the Device/Loading tab to start the update process. Result: The Update Confirmation dialog box is displayed. 
7	In the Update Confirmation dialog box, carefully review the list of devices selected for update and verify the settings you made.

Step	Action
8	Click the Confirm button to start the update process. Result: The update firmware process starts. Whenever a user interaction is required, the process is paused and a message is displayed in the notification area, page 65. Carefully read each message and confirm after you have evaluated the risks. After you have confirmed each message, the process will continue.
9	After the firmware process has been successfully completed, click the Summary button, page 18 from the bottom of the EcoStruxure Automation Device Maintenance to display the Update Summary dialog box. It provides information on the status of the update for each device indicating the previous and the target version as well as the data package / file.

NOTICE

DAMAGED DEVICES

Do not turn off the PC or close the application and make sure that the PC does not enter sleep mode while the update firmware process is running because the interruption of the process can damage the device.

Failure to follow these instructions can result in equipment damage.

You can optionally select the check box **I confirm that the system is in maintenance mode and that I want to suppress all safety messages for this update sequence..** This helps prevent the process from being paused.

NOTE: Activate this option only if you are working in maintenance mode and the operator has verified the state of security of your machine or process environment.

After the firmware process has been successfully completed, for controllers you can optionally click the **Start device** icon in the **Device/Loading** tab, page 20 to start the device.

NOTE: Perform a start-up test before using electrical control and automation equipment for regular operation after installation or update. For further information, refer to **Start-up and Test**, page 7.

Updating the Security Configuration File



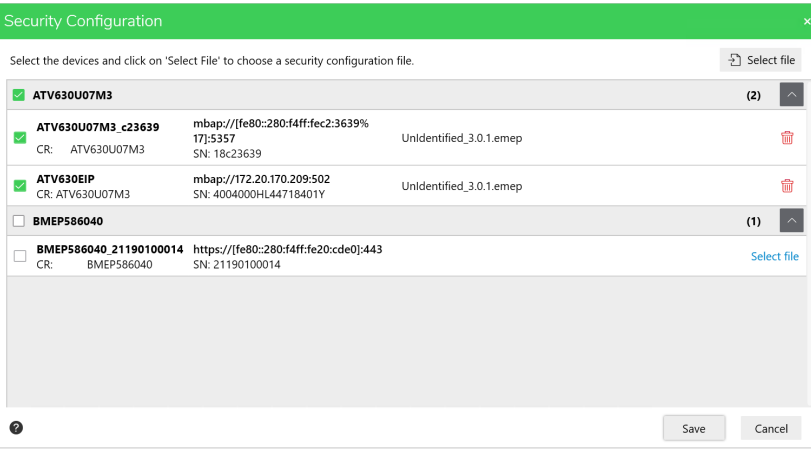
Overview

EcoStruxure Automation Device Maintenance allows you to update the security configuration file that contains security configuration settings that you have configured globally for your network within the EcoStruxure Cybersecurity Admin Expert application.

NOTE: The new security configuration file can assign new credentials to the device or devices. For future login, the new credentials will be required.

Updating the Security Configuration File

Execute the following steps to update the security configuration file:

Step	Action
1	Access the Device/Loading page.
2a	To perform updates on an individual device, click the Update Center icon  in the row of the device.
2b	To perform updates for different devices of the project simultaneously, select the check boxes of the devices or select the check box of the entire Group and click the Update Center button  from the button bar.
3	In the Update Center dialog box, click the Security button.
4	<p>In the Security Configuration dialog box, select an individual device and click the Select file link for this device or select several devices and click the Select file button from the upper part of the dialog box.</p>  <p>Result: A Windows file open dialog box is displayed and allows you to browse your network for the security configuration file.</p>
5	<p>Select the security configuration file and click the Open button.</p> <p>Result: The Security Configuration dialog box displays the devices with the selected files.</p>
6	<p>Click the Save button to save the configuration and to close the Security Configuration dialog box.</p> <p>Result: The Update Center Info cell or cells of the device or devices in the Device/Loading tab, page 20 display the text Security configuration selected.</p>
7	<p>Click the Update button from the Device/Loading tab to start the update process.</p> <p>Result: The Update Confirmation dialog box is displayed.</p>
8	In the Update Confirmation dialog box, carefully review the list of devices selected for update and verify the settings you made.
9	<p>Click the Confirm button to start the update process.</p> <p>Result: The update process starts. Whenever a user interaction is required, the process is paused and a message is displayed in the notification area, page 65. Carefully read each message and confirm after you have evaluated the risks. After you have confirmed each message, the process will continue.</p>

NOTICE

DAMAGED DEVICES

Do not turn off the PC or close the application and make sure that the PC does not enter sleep mode while the update firmware process is running because the interruption of the process can damage the device.

Failure to follow these instructions can result in equipment damage.

You can optionally select the check box **I confirm that the system is in maintenance mode and that I want to suppress all safety messages for this update sequence..** This helps prevent the process from being paused.

NOTE: Activate this option only if you are working in maintenance mode and the operator has verified the state of security of your machine or process environment.

Cybersecurity

Introduction

Cybersecurity is a branch of network administration that addresses attacks on or by computer systems and through computer networks that can result in accidental or intentional disruptions. The objective of cybersecurity is to help provide increased levels of protection for information and physical assets from theft, corruption, misuse, or accidents while maintaining access for their intended users.

No single cybersecurity approach is adequate. Schneider Electric recommends a defense-in-depth approach. Conceived by the National Security Agency (NSA), this approach layers the network with security features, appliances, and processes. The basic components of this approach are:

- risk assessment
- a security plan built on the results of the risk assessment
- a multi-phase training campaign
- physical separation of the industrial networks from enterprise networks using a demilitarized zone (DMZ) and the use of firewalls and routing to establish other security zones
- system access control
- device hardening
- network monitoring and maintenance

This chapter defines elements that help you configure a system that is less susceptible to cyber attacks. For detailed information on the defense-in-depth approach, refer to the *System Technical Note: How Can I... Reduce Vulnerability to Cyber Attacks* on the [Schneider Electric website](#).

What is Cybersecurity?

Overview

Cyber threats are deliberate actions or accidents that can disrupt the normal operations of computer systems and networks. These actions can be initiated from within the physical facility or from an external location. Security challenges for the control environment include:

- diverse physical and logical boundaries
- multiple sites and large geographic spans
- adverse effects of security implementation on process availability
- increased exposure to worms and viruses migrating from business systems to control systems as business-control communications become more open
- increased exposure to malicious software from USB devices, vendor and service technician laptops, and the enterprise network
- direct impact of control systems on physical and mechanical systems

Sources of Cyber Attacks

Implement a cybersecurity plan that accounts for various potential sources of cyber attacks and accidents, including:

Source	Description
internal	<ul style="list-style-type: none">• inappropriate employee or contractor behavior• disgruntled employee or contractor
external opportunistic (non-directed)	<ul style="list-style-type: none">• script kiddies*• recreational hackers• virus writers
external deliberate (directed)	<ul style="list-style-type: none">• criminal groups• activists• terrorists• agencies of foreign states
accidental	
* slang term for hackers who use malicious scripts written by others without necessarily possessing a comprehensive understanding of how the script works or its potential impact on a system	

A deliberate cyber attack on a control system may be launched to achieve a number of malicious results, including:

- disrupt the production process by blocking or delaying the flow of information
- damage, disable, or shut down equipment to negatively impact production or the environment
- modify or disable safety systems to cause intentional harm

How Attackers Gain Access

A cyber attacker bypasses the perimeter defenses to gain access to the control system network. Common points of access include:

- dial-up access to remote terminal unit (RTU) devices
- supplier access points (such as technical support access points)
- IT-controlled network products
- corporate virtual private network (VPN)
- database links
- poorly configured firewalls
- peer utilities

Cybersecurity Certifications

Schneider Electric developed cybersecurity guidelines based on the following recommendations:

- Achilles
- ISA Secure

For Questions, News or Reporting Vulnerability Issues

To submit a cybersecurity question, get the latest news from Schneider Electric, or report vulnerability issues, visit our [website](#).

Schneider Electric Guidelines

Introduction

Your PC system can run a variety of applications to enhance security in your control environment. The system has factory default settings that require reconfiguration to align with Schneider Electric's device hardening recommendations of the defense-in-depth approach.

The following guidelines describe procedures in a Windows operating system. They are provided as examples only. Your operating system and application may have different requirements or procedures.

Hardening Engineering Workstations

Customers may choose from various commercial PC systems for their engineering workstation needs. Key hardening techniques include:

- Strong password management.
- User account management.
- Methods of least privilege applied to applications and user accounts.
- Removal or disabling unneeded services.
- Removing remote management privileges.
- Systematic patch management.

Disabling Unused Network Interface Cards

Verify that network interface cards not required by the application are disabled. For example, if your system has 2 cards and the application uses only one, verify that the other network card (Local Area Connection 2) is disabled.

To disable a network card in Windows:

Step	Action
1	Open Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings .
2	Right-click the unused connection. Select Disable .

Configuring the Local Area Connection

Various Windows network settings provide enhanced security aligned with the defense-in-depth approach that Schneider Electric recommends.

In Windows systems, access these settings by opening **Control Panel > Network and Internet > Network and Sharing Center > Change Adapter Settings > Local Area Connection (x)**.

This list is an example of the configuration changes you might make to your system on the **Local Area Connection Properties** screen:

- Disable all IPv6 stacks on their respective network cards. (This system example does not require the IPv6 address range and disabling the IPv6 stacks limits vulnerability to potential IPv6 security risks.
- Disable **File and Print Sharing for Microsoft Network**.

Schneider Electric's defense-in-depth recommendations also include the following:

- Define only static IPv4 addresses, subnet masks, and gateways.
- Do not use DHCP or DNS in the control room.

Managing Windows Firewall

Schneider Electric's defense-in-depth approach recommendations include enabling the Windows host firewall on all system PCs. Enable the firewalls for any public or private profile listed.

It is recommended practice that users define firewall rules that refuse connections to or from any unknown/untrusted external host.

Disabling the Remote Desktop Protocol

Schneider Electric's defense-in-depth approach recommendations include disabling remote desktop protocol (RDP) unless your application requires the RDP.

Execute the following steps to disable the protocol for Windows 10 systems:

Step	Action
1	Right-click the Windows Start button and execute the command System .
2	From the Settings menu, execute the Remote Desktop command.
3	In the Remote Desktop view, turn off Enable Remote Desktop (toggle to Off).

For other Windows operating systems, execute equivalent procedures.

Updating Security Policies

Update the security policies on the PCs in your system by `gpupdate` in a command window. For more information, refer to the Microsoft documentation on `gpupdate`.

Disabling LANMAN and NTLM

The Microsoft LAN Manager protocol (LANMAN or LM) and its successor NT LAN Manager (NTLM) have vulnerabilities that make their use in control applications inadvisable.

The following steps describe how to disable LM and NTLM in a Windows system:

Step	Action
1	In a command window, execute <code>secpol.msc</code> to open the Local Security Policy window.
2	Open Security Settings > Local Policies > Security Options .
3	Select Send NTLMv2 response only. Refuse LM & NTLM in the Network Security: LAN Manger authentication level field.
4	Select the Network Security: Do not store LAN Manager hash value on next password change check box.
5	In a command window, enter <code>gpupdate</code> to commit the changed security policy.

Managing Updates

Before deployment, update all PC operating systems using the utilities on Microsoft's **Windows Update** Web page. To access this tool in Windows, select **Start > All Programs > Windows Update**.

Digital Signature Verification

Verifying the Integrity of EcoStruxure Automation Device Maintenance after Download

After you have downloaded the EcoStruxure Automation Device Maintenance executable file from the Schneider Electric website, verify the integrity of the file by executing the following steps:

Step	Action
1	Right-click the <code>AutomationDeviceMaintenance.exe</code> file and execute the command Properties from the contextual menu.
2	In the AutomationDeviceMaintenance.exe Properties dialog box, select the Digital Signatures tab.
3	From the Signature list select the entry Schneider Electric USA, INC. and click the Details button to see the Digital Signature Details .
4	In the Digital Signature Details dialog box, ensure that the information This digital signature is OK. is displayed.

You can now double-click the .exe file to start EcoStruxure Automation Device Maintenance.

Verification of Components during Start-up

When EcoStruxure Automation Device Maintenance is started, each loaded dynamic-link library (DLL) is scanned to verify whether or not it is trusted. This is a built-in security feature against cyberattacks and to increase the trust level.

What to do if Untrusted Components are Detected

If untrusted components are detected, the launch of EcoStruxure Automation Device Maintenance is aborted and a message is displayed indicating that an exception has been detected.

In this case, you have the following options:

- Reinstall EcoStruxure Automation Device Maintenance.
- If you have the slightest suspicion that this has been caused by a cyber attack, consult the [Schneider Electric Cybersecurity services portal](#) for further advice or assistance.

To find the component that causes the issue, you can use a debug tool, such as WinDbg: Start the debug tool, start EcoStruxure Automation Device Maintenance and observe the log file content for entries which indicate that the validity of the code signature of a DLL cannot be determined.

Files Requiring Manual Deinstallation

Overview

When you deinstall EcoStruxure Automation Device Maintenance from your PC, program files are automatically removed, but there are some user-specific files that you need to handle individually in order to help avoid cybersecurity issues.

EcoStruxure Automation Device Maintenance Settings File

The EcoStruxure Automation Device Maintenance settings file *AutomationDeviceMaintenanceSettings.emes* file is created by EcoStruxure Automation Device Maintenance to store the configuration you perform in the **Settings** dialog box (for example, Modbus TCP scan ranges or discovery settings). It is not removed from your PC with the deinstallation of EcoStruxure Automation Device Maintenance but needs to be removed manually.

Remove it from the folder *%APPDATA%\Schneider Electric\Automation Device Maintenance* using the Windows Explorer or other file system tools.

Certificates

The EcoStruxure Automation Device Maintenance certificate and the **Trusted Certificates** and **Untrusted Certificates** managed in the **Settings** dialog box under **Security > Certificate Management** (also refer to **Certificate Management Dialog Box**, page 43) are removed from the Windows PC with the deinstallation of EcoStruxure Automation Device Maintenance. They are also removed from the Windows Certificate Store.

Data Packages

Data packages, page 19 that have been saved locally are not removed from your PC with the deinstallation of EcoStruxure Automation Device Maintenance. By default, data packages are stored in the folder *%PUBLIC%\Public Documents\Schneider Electric\Data Packages*. You can configure your individual path in the **Settings > Package Settings** dialog box, page 36.

Remove either the default or the configured folder manually using the Windows Explorer or other file system tools.

EcoStruxure Automation Device Maintenance Project Files

EcoStruxure Automation Device Maintenance project files are not removed from your PC with the deinstallation of EcoStruxure Automation Device Maintenance. Search for files with file extension **.emep* and remove them manually or store them for later usage in a safe place where unauthorized access is not possible.

Log Files

The log files that have been locally saved to the path specified in the **Settings > Logs** dialog box, page 37 are not removed from your PC with the deinstallation of EcoStruxure Automation Device Maintenance. Remove the folder manually using the Windows Explorer or other file system tools or store the log files for later usage in a safe place where unauthorized access is not possible.


Components Used by EcoStruxure Automation Device Maintenance

Overview

EcoStruxure Automation Device Maintenance provides an overview of the components and the present versions. If an exception is detected, this list of components and versions can help finding the component that might be the cause.

Retrieving a List of Components

To retrieve a list of the components that are loaded by EcoStruxure Automation Device Maintenance, proceed as follows:

Step	Action																																	
1	<p>Click the About button  from the toolbar.</p> <p>Result: The About dialog box opens.</p>																																	
2	<p>Click the Component Information link.</p> <p>Result: The dialog box Component Information opens.</p> <div><div>About</div><div><div>Component Information</div><table><thead><tr><th>Component Name</th><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>AutomationDeviceMaintenance</td><td>3.0.140.0</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></tbody></table><div>Back to About Copy Details</div><div><div>Life Is On</div><div>Schneider Electric</div></div><div>OK</div></div></div>	Component Name	Version	Description	AutomationDeviceMaintenance	3.0.140.0	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
Component Name	Version	Description																																
AutomationDeviceMaintenance	3.0.140.0	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>Click the Copy Details link to copy the list of components and versions to the clipboard.</p> <p>You can now paste the content to a *.txt file that allows you convenient search operations for specific components and corresponding versions.</p>																																	

Glossary

D

Data Package, Firmware Package:

A data package is a file used for content exchange between tool and devices. It can be in SEDP format. A data package contains firmware package(s) but can also contain configuration, PLC applications, and so on.

Device Certificate:

An X.509 public key certificate used by tool and device to establish a secure communication channel (for example: HTTPs).

Device Discovery:

Automatic detection of devices and services those devices offer in a computer network.

Device Family:

A group of devices of similar types each device family is identified by a Product ID.

DHCP: Dynamic Host Configuration Protocol**DNS:** Domain Name System**DPWS:**

Device Profile for Web Services, standard for discovery and description of devices which support web services.

H

HTTP:

Hypertext Transfer Protocol

HTTPs:

Hypertext Transfer Protocol Secure also known as HTTP over TLS.

I

ICS: Industrial Control and Systems**IEC:**

(international electrotechnical commission) A non-profit and non-governmental international standards organization that prepares and publishes international standards for electrical, electronic, and related technologies.

IP address:

Address of a device according IP protocol standards. It can be in IPv4 or IPv6 address format.

IP:

Internet Protocol

ISO: International Organization for Standardization

N

NEMA:

(national electrical manufacturers association) The standard for the performance of various classes of electrical enclosures. The NEMA standards cover corrosion resistance, ability to help protect from rain, submersion, and so on. For IEC member countries, the IEC 60529 standard classifies the ingress protection rating for enclosures.

O

OPC UA:

OPC Unified Architecture: OPC UA is an interoperability standard for the secured and reliable exchange of data in the industrial automation space. It is a platform independent communication protocol using the server/client model. The connection between client and server is commonly based on the reliable transport layer protocol (TCP, Transmission Control Protocol).

For more information about the OPC especially OPC UA refer to the official webpage of the OPC Foundation at <https://opcfoundation.org>.

P

PLC:

(programmable logic controller) An industrial computer used to automate manufacturing, industrial, and other electromechanical processes. PLCs are different from common computers in that they are designed to have multiple input and output arrays and adhere to more robust specifications for shock, vibration, temperature, and electrical interference among other things.

POU:

(program organization unit) A variable declaration in source code and a corresponding instruction set. POU's facilitate the modular re-use of software programs, functions, and function blocks. Once declared, POU's are available to one another.

Product ID:

Product Identifier, identifies the product family a device belongs to.

S

SEDP:

Schneider Electric Data Package, standardized file format for content exchange between software tools and devices.

T

TCP:

Transmission Control Protocol

TLS:

Transport Layer Security

U

UDP: User Datagram Protocol

URL:

Uniform Resource Locator

Index

A

accessing extensions	62
add device	22
Application Certificate	42
Apply button	25
applying modifications	25
AutomationDeviceMaintenanceSettings.emes file	77

C

CA	42
certificate	
validate, trust, untrust, remove	42
Certificate Authority	42
Certificate Management	42
certificates	42
communication protocols	15
component information	78
components and versions	78
configuration file import	33
configure	
discovery	31
discovery, Modbus, package setting, language, certificate	24
configuring	
communication settings	36
DPWS scanner	35
language, change	39
Modbus TCP	33
package locations	36
confirmation messages	65
Copy to Clipboard button	53
copying the identifier	53
credentials	24, 60, 67
csv file for import	33
csv file import	33
cybersecurity	72
certifications	72
firewall	75
guidelines	74
introduction	72
LANMAN / NTLM	76
local area connection	75
network interface cards	74
remote desktop	75

D

data	
firmware, configuring	51
data package	50
package name, package information	19
deinstallation	77
delete certificate	42
device	
update, config options, credentials	60
device certificate	
trusted, untrusted	20
device discovery	
Modbus, DPWS (device profile for web services)	14
Device Discovery Status	64
Device login dialog box	60
device/loading	

device name, status, data package	20
Device/Loading tab	54
discovery	
automatic, manual	31
manual, automatic	24
DLL untrusted	76
DPWS scanner	
probe request, metadata request, network adapters	35

E

enroll application certificate	42
error	
error, warning	18
save, clear	25
exception	76
extensions	62
Extensions tab	62

F

firmware	
update, device/loading, data package	67
version, upgrade info, progress	20
Firmware dialog box	67
firmware package	
package information, package name	17
frequency of polling	36
fwp package files	50

G

Group option	55
grouping devices	55

H

hardware	
CPU, RAM, HDD	15
HTTP / HTTPS communication	22

I

identifier	
copy	53
Import security configuration file	40
importing a configuration file	33
information	
package, product	51
save, clear	25
installation	
procedure, installation wizard, install, license agreement	16

L

Idx package files	50
Local Repository	36
login dialog box	60
login for firmware update	67
logs	
view	66

M			
Modbus TCP			
unit ID, ping timeout, port	33		
Modbus TCP communication	22		
modifications in Settings page	25		
modular devices	62		
monitoring the device discovery status	64		
N			
new project	26		
notification area	65		
notification messages	65		
O			
Ok button	25		
P			
package location			
add	37		
passwords	60, 67		
PKI	47		
polling frequency	36		
project			
new	26		
open	28		
open, save	18		
save	27		
project files from another computer	29		
project files with unidentified devices	30		
Project Modified dialog box	26		
Public Key Infrastructure (PKI)	47		
R			
rack modules	62		
refresh icon	25		
Rejected data packages	51		
remove certificate	42		
removing files	77		
resetting application settings	39		
S			
SD memory card	20		
secured package files sedps	50		
security configuration file	40, 69		
security features	40		
sedp package files	50		
sedps package files	50		
software			
features, supported firmware packages	14		
supported devices	14		
syslog	48		
system requirements			
hardware, software, communication protocols,			
screen resolution, cybersecurity	15		
T			
TCP	48		
timeout			
communication settings	36		
		TLS	48
		toolbar	
		about, help, discovery	18
		trust certificate	42
U			
		UDP	48
		untrust certificate	42
		untrusted DLL	76
		Update Center	66
		Update Confirmation dialog box	67
		Update Summary dialog box	67
		updating firmware	67
		updating security configuration file	69
V			
		Valid data packages	51
		view	20
W			
		warning	
		save, clear	25
		welcome screen	
		data package, device/loading, toolbar	17

Schneider Electric
35 rue Joseph Monier
92500 Rueil Malmaison
France

+ 33 (0) 1 41 29 70 00

www.se.com

As standards, specifications, and design change from time to time,
please ask for confirmation of the information given in this publication.

© 2022 Schneider Electric. All rights reserved.

EIO0000004033.04