# Altivar dPAC Module VW3A3530D

## User Guide

**NNZ13577.08**
**06/2023**


www.se.com

# Legal Information

# Table of Contents

# 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

Only appropriately trained persons who are familiar with and understand the contents of this manual and all other pertinent product documentation are authorized to work on and with this product. In addition, these persons must have received safety training to recognize and avoid hazards involved. These persons must have sufficient technical training, knowledge and experience and be able to foresee and detect potential hazards that may be caused by using the product, by changing the settings and by the mechanical, electrical and electronic equipment of the entire system in which the product is used. All persons working on and with the product must be fully familiar with all applicable standards, directives, and accident prevention regulations when performing such work.

# Intended Use

This product is a drive for three-phase synchronous and asynchronous motors and intended for industrial use according to this manual. The product may only be used in compliance with all applicable safety regulations and directives, the specified requirements and the technical data. Prior to using the product, you must perform a risk assessment in view of the planned application. Based on the results, the appropriate safety measures must be implemented. Since the product is used as a component in an entire system, you must ensure the safety of persons by means of the design of this entire system (for example, machine design). Any use other than the use explicitly permitted is prohibited and can result in hazards. Electrical equipment should be installed, operated, serviced, and maintained only by qualified personnel.

# 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 be 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.

# Cybersecurity Generalities

## Overview

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 the elements that help you configure a system that is less susceptible to cyber-attacks.

Network administrators, system integrators and personnel that commission, maintain or dispose of a device should:

- Apply and maintain the device's security capabilities. See Device Security Capabilities sub-chapter for details
- Review assumptions about protected environments. See Protected Environment Assumptions sub-chapter for details
- Address potential risks and mitigation strategies. See Product Defense-in-Depth sub-chapter for details
- Follow recommendations to optimize cybersecurity

For detailed information on the system defense-in-depth approach, refer to the following TVDAs:

- How Can I Reduce Vulnerability to Cyber Attacks in the Control Room (STN V2) on se.com.
- How can I Design and build a robust cybersecurity system for EcoStruxure Automation Expert systems.

  **NOTE:** This TVDA is available through your local Schneider Electric Services contact or Customer Care Center on (www.se.com/CCC).

To submit a Cybersecurity question, report security issues, or get the latest news from Schneider Electric, visit the Schneider Electric website.

**⚠WARNING**

**POTENTIAL COMPROMISE OF SYSTEM AVAILABILITY, INTEGRITY, AND CONFIDENTIALITY**

- Configure the security of the ATV dPAC to help prevent unauthorized access to device settings and information.
- Disable unused ports/services and default accounts, where possible, to minimize pathways for malicious attacks.
- Place networked devices behind multiple layers of cyber defenses (such as firewalls, network segmentation, and network intrusion detection and protection).
- Use cybersecurity best practices (for example: least rights, separation of duties) to help prevent unauthorized exposure, loss or modification of data and logs, interruption of services, or unintended operation.

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

Use the getting started with ATV dPAC manual to get more information on configuring ATV dPAC security.

## Protected Environment Assumption

Machines, controllers, and related equipment are usually integrated into networks. Unauthorized persons and malware may gain access to the machine as well as to other devices on the network/fieldbus of the machine and connected networks via insufficiently secure access to software and networks.

**⚠WARNING**

**UNAUTHORIZED ACCESS TO THE MACHINE VIA SOFTWARE AND NETWORKS**

- In your hazard and risk analysis, consider all hazards that result from access to and operation on the network/fieldbus and develop an appropriate cybersecurity concept.
- Verify that the hardware infrastructure and the software infrastructure into which the machine is integrated as well as all organizational measures and rules covering access to this infrastructure consider the results of the hazard and risk analysis and are implemented according to best practices and standards covering IT security and cybersecurity (such as: ISO/IEC 27000 series, Common Criteria for Information Technology Security Evaluation, ISO/ IEC 15408, IEC 62351, ISA/IEC 62443, NIST Cybersecurity Framework, Information Security Forum - Standard of Good Practice for Information Security, SE recommended Cybersecurity Best Practices*).
- Verify the effectiveness of your IT security and cybersecurity systems using appropriate, proven methods.

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

(*) : SE Recommended Cybersecurity Best Practices can be downloaded on SE.com.

Before considering cybersecurity practices on the device, please pay attention to following points:

- Cybersecurity governance – available and up-to-date guidance on governing the use of information and technology assets in your company.
- Perimeter security – installed devices, and devices that are not in service, are in an access-controlled or monitored location.

- Emergency power – the control system provides the capability to switch to and from an emergency power supply without affecting the existing security state or a documented degraded mode.
- Firmware upgrades – the ATV dPAC firmware upgrades can be found in the EcoStruxure Automation Expert software installer archive folder.
- Controls against malware – detection, prevention, and recovery controls to help protect against malware are implemented and combined with appropriate user awareness.
- Physical network segmentation – the control system provides the capability to:
  - Physically segment control system networks from non-control system networks.
  - Physically segment critical control system networks from non- critical control system networks.
- Logical isolation of critical networks – the control system provides the capability to logically and physically isolate critical control system networks from non-critical control system networks. For example, using VLANs.
- Independence from non-control system networks – the control system provides network services to control system networks, critical or non-critical, without a connection to non-control system networks.
- Excluding TLS based protocols, Encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.
- Zone boundary protection – the control system provides the capability to:
  - Manage connections through managed interfaces consisting of appropriate boundary protection devices, such as: proxies, gateways, routers, firewalls, and encrypted tunnels.
  - Use an effective architecture, for example, firewalls protecting application gateways residing in a DMZ.
  - Control system boundary protections at any designated alternate processing sites should provide the same levels of protection as that of the primary site, for example, data centers.
- No public internet connectivity – access from the control system to the internet is not recommended. If a remote site connection is needed, for example, encrypt protocol transmissions.
- Resource availability and redundancy – ability to break the connections between different network segments or use duplicate devices in response to an incident.
- Manage communication loads – the control system provides the capability to manage communication loads to mitigate the effects of information flooding types of DoS (Denial of Service) events.
- Control system backup – available and up-to-date backups for recovery from a control system failure.

# Security Policy

**⚠WARNING**

**ACCESSIBILITY LOSS**

- Setup a security policy to your device and ensure that you're following the backup policy with EcoStruxure Automation Expert to restore your device in case of accessibility loss.
- Define and regularly review the password policy.
- Periodic change of the passwords, Schneider Electric recommends a modification of the password each 90 days.

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

Cybersecurity helps to provide:

- Confidentiality (to help prevent unauthorized access)
- Integrity (to help prevent unauthorized modification)
- Availability/authentication (preventing the denial of service and assuring authorized access)
- Non-repudiation (preventing the denial of an action that took place)
- Traceability/detection (logging and monitoring)

Norm IEC 62443 is the worldwide standard for security of industrial control system (ICS) networks.

From the norm definition, ATV dPAC is considered as Embedded Device of the ICS network, and has been designed following the norm IEC 62443-4-1 and the technical security requirements are defined in compliance with norm IEC 62443-4-2.

ATV dPAC security features prevent the unauthorized disclosure of information via eavesdropping or casual exposure.

For an efficient security, the instructions and procedures should structure the roles and responsibilities in terms of security within the organization; in other words, who is authorized to perform what and when. These should be known by the users.

The anti-intrusion and anti-physical access to any sensitive installation should be set up.

All the security rules implemented in the ATV dPAC are in complement of the points above.

The device does not have the capability to transmit data encrypted using the CIP Safety protocol following protocols: HTTP, Modbus over serial, Modbus over Ethernet, EtherNet/IP, SNMP, SNTP. If other users gained access to your network, transmitted information can be disclosed or subject to tampering.

**⚠WARNING**

**CYBERSECURITY HAZARD**

- For transmitting data over an internal network, physically or logically segment the network, the access to the internal network needs to be restricted by using standard controls such as firewalls.
- For transmitting data over an external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.

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

Any computer using EcoStruxure Automation Expert, EcoStruxure Automation Device Maintenance, SoMove, DTM or Webserver should have an updated anti-virus, anti-malware, anti-ransomware application activated during the use.

## Product Defense-in-Depth

Use a layered network approach with multiple security and defense controls in your IT and control system to minimize data protection gaps, reduce single-points of failure and create a strong cybersecurity posture. The more layers of security in your network, the harder it is to breach defenses, take digital assets or cause disruption.

## Device Security Capabilities

ATV dPAC offers the following security features:

| Threats | Desired security property on Embedded Device | ATV dPAC security features |
|---|---|---|
| Information disclosure | confidentiality | Password encrypted in a non-reversible way |
| | | User access control |
| | | TLS based protocol to secure communication integrity |
| Tampering | Device integrity | Cryptographic signature of firmware package |
| Denial of Service | Availability | Device backup/restore |
| Spoofing/Elevation of privilege | User Authenticity / Authorization | Strong password policy |
| | | Access control commissioning through EcoStruxure Automation Expert, EcoStruxure Automation Device Maintenance, OPC UA, Webserver |
| | | Access control local using the Graphic Display Terminal (VW3A1111) |
| | | Access control commissioning tools Modbus TCP |
| | | Access control commissioning tools WebServer |

### Confidentiality

Information confidentiality capacity prevents unauthorized access to the device and information disclosure.

- The user access control helps on managing users that are authorized to access the device. Protect user credential at usage.
- The user’s passwords are encrypted in non-reversible way at rest
- The TLS security capabilities help protect the confidentiality of information through secure protocols that employ cryptographic algorithms, key sizes and mechanisms used to help prevent unauthorized users from reading information in transit, (ie: SSH, SFTP and HTTPS)

Information affecting the security policy of the device is encrypted in transit.

### Device Integrity Protection

The device integrity protection prevents unauthorized modification of the device with tampered or spoofed information.

This security capability helps protect the authenticity and integrity of the firmware running on the ATV dPAC and facilitates protected file transfer: digitally signed firmware is used to help protect the authenticity of the firmware running on the ATV dPAC and only allows firmware generated and signed by Schneider Electric.

Cryptographic signature of the firmware package executed at the firmware update

### Availability

The control system backup is essential for recovery from a control system failure and/or misconfiguration and participate on preventing denial of service. It also helps ensure global availability of the device by reducing operator overhead on security application/deployment.

These security capabilities help manage control system backup with the device:

- Independent security policy import/export for local secure backup and security policy sharing with other devices.
- Complete device backup/restore available on local HMI, DTM and FDR.

### User Authenticity and Authorization

The user authentication helps prevent the repudiation issue by managing user identification and prevents information disclosure and device integrity issues by unauthorized users.

These security capabilities help enforce authorizations assigned to users, segregation of duties and least rights:

- User authentication is used to identify and authenticate software processes and devices managing accounts
- Device Password policy and password strength configurable using SoMove, DTM or Webserver
- Authorization managed according to channels

In line with user authentication and authorization, the device has access control cryptographic features to check user credential before access is granted to the system.

In the ATV dPAC, the control of accessibility to the settings, parameters, configuration, and logging database is done with a user authentication after "Log in", with a name and password.

The ATV dPAC controls the access through:

- SoMove DTM (Serial and Ethernet connection)
- The webserver
- EcoStruxure Automation Expert
- EcoStruxure Automation Device Maintenance

# Potential Risks and Compensating Controls

Address potential risks using these compensating controls:

| Area | Issue | Risk | Compensating controls |
|---|---|---|---|
| User accounts. | Default account settings are often the source of unauthorized access by malicious users. | If you do not change default password or disable the user access control, unauthorized access can occur. | Ensure User access control is enabled on all the communication ports and change the default passwords to help reduce unauthorized access to your device. |
| Secure protocols. | Modbus serial, Modbus TCP, EtherNet/IP, SNMP, SNTP, HTTP protocols are insecure.<br><br>The device does not have the capability to transmit data encrypted using these protocols. | If a malicious user gained access to your network, they could intercept communication. | For transmitting data over internal network, physically or logically segment your network.<br><br>For transmitting data over external network, encrypt protocol transmissions over all external connections using an encrypted tunnel, TLS wrapper or a similar solution.<br><br>See Protected Environment Assumptions. |
| Physical access to the device | The device does not have the capability to restrict the access to the local HMI | If a malicious user physically gains access to your device, they can take unauthenticated control of the process and configuration of your device. (ie: they can reset the password and the security) | Ensure your device and its local HMI are in a secure area with restricted access |

# Product Related Information

## ⚠WARNING

**LOSS OF CONTROL**

- The designer of any control scheme must consider the potential failure modes of control paths and, for 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, 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 the product 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 USA: 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.

# About the Book

## Document Scope

The purpose of this document is to:

- Guide you to set up the drive.
- Show you how to program the drive.
- Visualize different menus, modes, and parameters.
- Help you in maintenance and diagnostics.

## Validity Note

This documentation is valid for the Altivar drives.

The technical characteristics of the devices described in the present document also appear online. To access the information online:

| Step | Action |
|---|---|
| 1 | Go to the Schneider Electric home page www.se.com. |
| 2 | In the **Search** box type the reference of a product or the name of a product range.<br>• Do not include blank spaces in the reference or product range.<br>• To get information on grouping similar modules, use asterisks (*). |
| 3 | If you entered a reference, go to the **Product Datasheets** search results and click on the reference that interests you.<br>If you entered the name of a product range, go to the **Product Ranges** search results and click on the product range that interests you. |
| 4 | If more than one reference appears in the **Products** search results, click on the reference that interests you. |
| 5 | Depending on the size of your screen, you may need to scroll down to see the datasheet. |
| 6 | To save or print a datasheet as a .pdf file, click **Download XXX product datasheet**. |

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

Use your tablet or your PC to quickly access detailed and comprehensive information on all our products on www.se.com.

The website provides the information you need for products and solutions:

- The whole catalog for detailed characteristics and selection guides.
- The CAD files to help design your installation, available in over 20 different file formats.
- All software and firmware to maintain your installation up to date,
- A large quantity of White Papers, Environment documents, Application solutions, Specifications to gain a better understanding of our electrical systems and equipment or automation.
- All the User Guides related to your drive are listed below:

| Title of Documentation | Reference Number |
|---|---|
| Discover catalog for EcoStruxure Automation Expert | DIA3ED2201101 (English), DIA3ED2201101 (French) |
| Modicon M251/M580 Distributed PACs and Altivar Drives with EcoStruxure™ Automation Expert Hardware Reference Guide | EIO0000004217 (English) |
| EcoStruxure Automation Expert Applications Design Guidelines - Reference Manual | EIO0000004686 (English) |
| Altivar Lexium - Instruction Sheet - Option Modules | S1A45591 (English) |
| Altivar Option Modules - Instruction sheets | VW3A3420 (digital encoder interface module) NHA80730.01 (digital encoder interface module - Instruction Sheet) , VW3A3422 (analog encoder interface module) — NVE19304.01 (analog encoder interface module - Instruction Sheet), VW3A3203 (extended I/O module - discrete 6I/2O - analog 2I) — EAV76404.01 (Extension module of Digital and Analog I/O - Instruction Sheet), VW3A3204 (extended relay module - 3 relays) — EAV76405.02 (Extension module of Output relays - Instruction Sheet), VW3A3424 (HTL encoder interface module) — QGH1764000 (HTL encoder interface module 12/15/24 Vdc - Instruction Sheet), VW3A3423 (resolver interface module) — NVE19307.01 (resolver interface module - Instruction Sheet) |
| ATV dPAC user guide | NNZ13577 (English), NNZ13578 (French), NNZ13579 (German), NNZ13580 (Spanish), NNZ13581 (Italian), NNZ13582 (Chinese), NNZ13583 (Portuguese) |
| ATV dPAC VW3A3530D Product data sheet | English |
| How to Configure ATV dPAC VW3A3530D in EcoStruxure Automation Expert - Video | How to Configure ATV dPAC in EAE v21.1 |
| EcoStruxure Automation Expert - How to Videos | Youtube Playlist: EcoStruxure Automation Expert How-to Videos |
| Getting Started with ATV dPAC VW3A3530D | JYT50503 (English), JYT50505 (French), JYT50511 (German), JYT50507 (Spanish), JYT50508 (Italian), JYT50513 (Chinese), JYT50517 (Portuguese) |
| EcoStruxure Automation Device Maintenance Altivar User Manual | JYT50472 (English) |
| EcoStruxure Automation Device Maintenance - Software | • V2.0: EADM (Chinese, English, French, German, Italian, Spanish)<br>• V2.1: EADM_V2.1 ( English)<br>• V3.0: EADM_V3.0 (English)<br>• V3.1: EADM_V3.1 (English) |
| SoMove - FDT | SoMove_FDT (Chinese, English, French, German, Italian, Portuguese, Spanish, Turkish) |
| ATV340 Getting Started - Video | FAQ FA367923 (English) |
| ATV340 Getting Started | NVE37643 (English), NVE37642 (French), NVE37644 (German), NVE37646 (Spanish), NVE37647 (Italian), NVE37648 (Chinese), NVE37643PT (Portuguese), NVE37643TR (Turkish) |
| ATV340 Installation Manual | NVE61069 (English), NVE61071 (French), NVE61074 (German), NVE61075 (Spanish), NVE61078 (Italian), NVE61079 (Chinese), NVE61069PT (Portuguese), NVE61069TR (Turkish) |
| ATV340 Programming Manual | NVE61643 (English), NVE61644 (French), NVE61645 (German), NVE61647 (Spanish), NVE61648 (Italian), NVE61649 (Chinese), NVE61643PT (Portuguese), NVE61643TR (Turkish) |
| ATV340 – DTM | ATV340_DTM_Library_EN (English), ATV340_DTM_Lang_FR (French), ATV340_DTM_Lang_DE (German), ATV340_DTM_Lang_SP (Spanish), ATV340_DTM_Lang_IT (Italian), ATV340_DTM_Lang_CN (Chinese) |
| ATV600 Getting Started | EAV63253 (English), EAV63254 (French), EAV63255 (German), EAV63256 (Spanish), EAV63257 (Italian), EAV64298 (Chinese), EAV63253PT (Portuguese), EAV63253TR (Turkish) |
| ATV630, ATV650 Installation Manual | EAV64301 (English), EAV64302 (French), EAV64306 (German), EAV64307 (Spanish), EAV64310 (Italian), EAV64317 (Chinese), EAV64301PT (Portuguese), EAV64301TR (Turkish) |
| ATV600 Programming Manual | EAV64318 (English), EAV64320 (French), EAV64321 (German), EAV64322 (Spanish), EAV64323 (Italian), EAV64324 (Chinese), EAV64318PT (Portuguese), EAV64318TR (Turkish) |
| ATV600 – DTM | ATV6xx_DTM_Library_EN (English - to be installed first), ATV6xx_DTM_Lang_FR (French), ATV6xx_DTM_Lang_DE(German), ATV6xx_DTM_Lang_SP (Spanish), ATV6xx_DTM_Lang_IT (Italian), ATV6xx_DTM_Lang_CN (Chinese) |
| ATV900 Getting Started | NHA61578 (English), NHA61579 (French), NHA61580 (German), NHA61581 (Spanish), NHA61724 (Italian), NHA61582 (Chinese), NHA61578PT (Portuguese), NHA61578TR (Turkish) |
| ATV930, ATV950 Installation manual | NHA80932 (English), NHA80933 (French), NHA80934 (German), NHA80935 (Spanish), NHA80936 (Italian), NHA80937 (Chinese), NHA80932PT (Portuguese), NHA80932TR (Turkish) |

| Title of Documentation | Reference Number |
|---|---|
| ATV900 Programming manual | NHA80757 (English), NHA80758 (French), NHA80759 (German), NHA80760 (Spanish), NHA80761 (Italian), NHA80762 (Chinese), NHA80757PT (Portuguese), NHA80757TR (Turkish) |
| ATV900 – DTM | ATV9xx_DTM_Library_EN(English - to be installed first), ATV9xx_DTM_Lang_FR (French), ATV9xx_DTM_Lang_DE (German), ATV9xx_DTM_Lang_SP (Spanish), ATV9xx_DTM_Lang_IT (Italian), ATV9xx_DTM_Lang_CN (Chinese) |
| Recommended Cybersecurity Best Practices | CS-Best-Practices-2019-340 (English) |

You can download these technical publications and other technical information from our website at www.se.com/en/download

## Terminology

The technical terms, terminology, and the corresponding descriptions in this manual normally use the terms or definitions in the relevant standards.

In the area of drive systems this includes, but is not limited to, terms such as **error, error message, failure, fault, fault reset, protection, safe state, safety function, warning, warning message**, and so on.

Among others, these standards include:

- IEC 61800 series: Adjustable speed electrical power drive systems
- IEC 61508 Ed.2 series: Functional safety of electrical/electronic/ programmable electronic safety-related
- EN 954-1 Safety of machinery - Safety related parts of control systems
- EN ISO 13849-1 & 2 Safety of machinery - Safety related parts of control systems.
- IEC 61158 series: Industrial communication networks - Fieldbus specifications
- IEC 61784 series: Industrial communication networks - Profiles
- IEC 60204-1: Safety of machinery - Electrical equipment of machines – Part 1: General requirements

In addition, the term **zone of operation** is used in conjunction with the description of specific hazards, and is defined as it is for a **hazard zone** or **danger zone** in the EC Machinery Directive (2006/42/EC) and in ISO 12100-1.

## Contact Us

Select your country on:

www.se.com/contact

**Schneider Electric Industries SAS**

Head Office

35, rue Joseph Monier

92500 Rueil-Malmaison

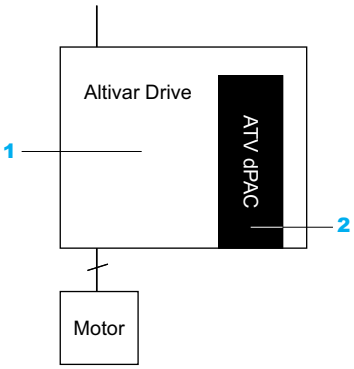
France

# ATV dPAC General Hardware Overview

## ATV dPAC Description

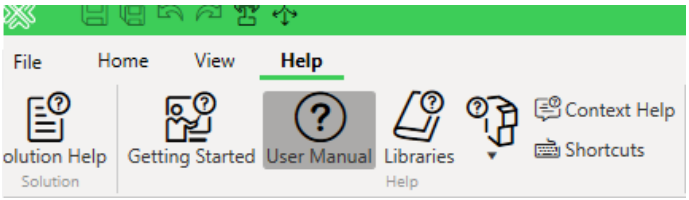
### Overview

The ATV dPAC (for Altivar distributed Process Automation Controller) is an option module (2) for Altivar variable speed drives (1). The catalog number of this option module is VW3A3530D.




This option module is a controller being part of EcoStruxure Automation Expert controller offer. ATV dPAC has various powerful features, can service a wide range of applications and adapts the Altivar drives to specific applications by integrating control system functions.

Software configuration, programming, and commissioning are achieved with the EcoStruxure Automation Expert software described in the *EcoStruxure Automation Expert User Manual*, accessible from the software help tab.




### Power Supply

The power supply of ATV dPAC is provided by the host Altivar Drive (See Electrical Requirements, page 36).

### Run/Stop

The ATV dPAC can be operated externally by an EcoStruxure Automation Expert software command.

### Memory

This table describes the different types of memory embedded to the ATV dPAC:

| Memory Type | Size | Used |
|---|---|---|
| RAM | 16 Mbytes of which 12 Mbytes available for the application and communication services | To execute the application. |
| Flash | 16 Mbytes | To save the program (and data in case of a power interruption). |

## Communication Features

The ATV dPAC communication ports include Ethernet (See Ethernet Port, page 41).

## Altivar Drive Features

The ATV dPAC can control or use the information coming from the following drives interfaces:

- Variable Speed Drive interface (part controlling the motor),
- Inputs and outputs embedded to the drive (such as digital inputs, analog inputs, analog outputs and relays).

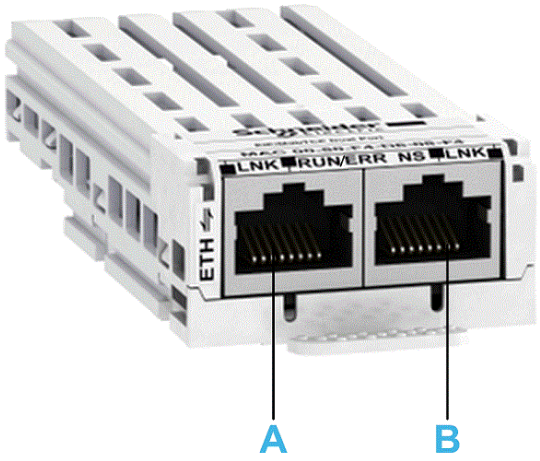
  **NOTE:** The following are supported from ATV dPAC software version **V3.1IE03**:

  - ATV340 embedded encoder (available on drives with power equal to or lower than 22 kW),
  - VW3A3420, VW3A3422, VW3A3423 and VW3A3424 option encoder interface modules (digital, analog, resolver and HTL),
  - VW3A3203 extended I/O module,
  - VW3A3204 extended relay module.

# ATV dPAC Hardware Presentation

## Overview

The following figure shows the VW3A3530D ATV dPAC module with one dual port Ethernet switch:



| Item | Description | Comment |
|---|---|---|
| A | Port A | RJ45 connector - Ethernet port |
| B | Port B | RJ45 connector - Ethernet port |

# Firmware Version Compatibility

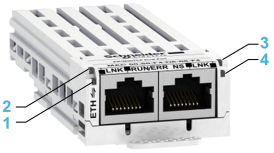
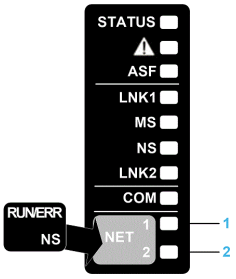
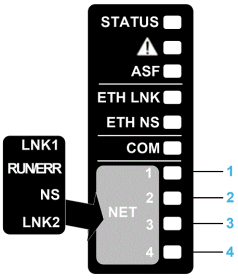
The ATV dPAC is compatible with:

- ATV340 drives with, at least, V1.8IE94 software version.
- Altivar Process ATV600 (ATV630, ATV650) drives with, at least, V2.6IE94 software version
- Altivar Process ATV900 (ATV930, ATV950) drives with, at least, V2.3IE94 software version.

In case of incompatible version between the drive and the ATV dPAC, **[Internal Error 6]** $\mathit{inF6}$ is triggered. A firmware update can be performed using EcoStruxure Automation Device Maintenance. For more information contact your local Schneider Electric Services.

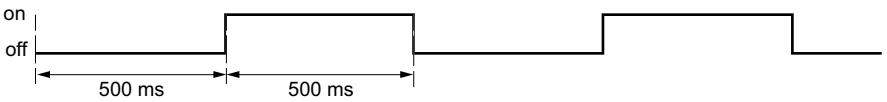
# Status LEDs

The following figures shows the LED indicators depending on the host Altivar drive:

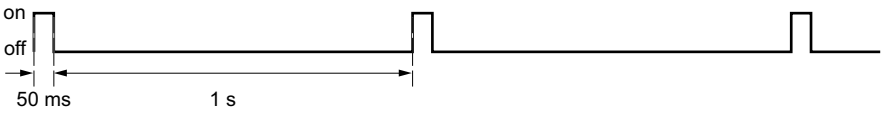
| **ATV340 (power ≤ 22 kW)** | **ATV340 (power > 22 kW)**<br>**ATV900** | **ATV600** |
|---|---|---|
| Display on ATV dPAC | Display on the control block of the host drive | Display on the control block of the host drive |
|  |  |  |
| Legend:<br>**1** LNK1 – **2** RUN/ERR<br>**3** NS – **4** LNK2 | **1** RUN/ERR – **2** NS | **1** LNK1 – **2** RUN/ERR<br>**3** NS – **4** LNK2 |

This figure shows the difference between the fast flash and the slow flash:

### Blinking




### Single Flash



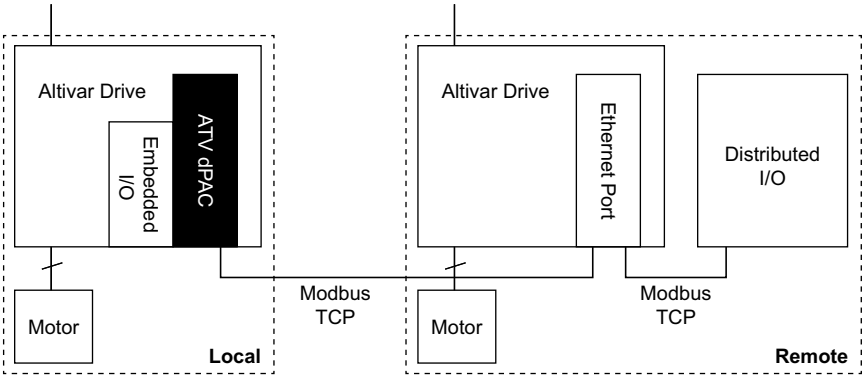
# Maximum Hardware Configuration

## Introduction

The ATV dPAC is a control system that offers a scalable solution with optimized configurations and an expandable architecture.

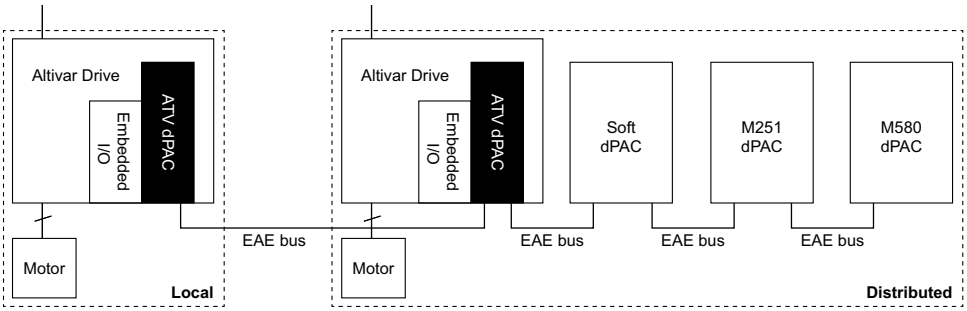
## Local and Remote Configuration Principle

The following figure defines the local and remote configurations:




## Local and Distributed Configuration Principle

The following figure defines the local and distributed configurations:




## Local Configuration Architecture

Optimized local configuration and flexibility are provided by the association of the following:

- ATV dPAC,
- Variable Speed Drive (part controlling the motor),
- Inputs and outputs embedded to the drive.

  **NOTE:** The following are supported from ATV dPAC software version **V3.1IE03**:

  - ATV340 embedded encoder (available on drives with power equal to or lower than 22 kW),
  - VW3A3420, VW3A3422, VW3A3423 and VW3A3424 option encoder interface modules (digital, analog, resolver and HTL),
  - VW3A3203 extended I/O module,
  - VW3A3204 extended relay module.

Application requirements determine the architecture of your ATV dPAC configuration.

## Remote Configuration Architecture

Optimized remote configuration and flexibility are provided, through Modbus TCP connection by the association of the following:

- ATV dPAC (acting as client over Modbus TCP),
- Other Altivar drives via Ethernet port (acting as Modbus TCP server)
- Distributed I/O such as Advantys STB Digital I/O modules or TM3 Bus Coupler for I/O modules. They are managed by ATV dPAC
- Modbus TCP Server
- OPC Unified Architecture Server (OPC UA Server) to be interfaced with SCADA Systems
- Other Modbus TCP server devices.

Application requirements determine the architecture of your ATV dPAC configuration.

## Distributed Configuration Architecture

Optimized distributed configuration and flexibility are provided, through EcoStruxure Automation Expert bus connection, by the association of the following:

- ATV dPAC
- M251 dPAC
- M580 dPAC
- Soft dPAC (for example running on server).

Application requirements determine the architecture of your ATV dPAC configuration.

## Maximum Number of Modules

The maximum configuration supported is:

- **Local**: the part of the drive controlling the motor and all embedded inputs/outputs of the drive,
- **Remote**: up to 13 Modbus TCP server devices,
- **Distributed**: up to 16 (ATV dPAC, M251 dPAC, M580 dPAC or soft dPAC).

  **NOTE:** The following are supported from ATV dPAC software version **V3.1IE03**:

  - ATV340 embedded encoder (available on drives with power equal to or lower than 22 kW),
  - VW3A3420, VW3A3422, VW3A3423 and VW3A3424 option encoder interface modules (digital, analog, resolver and HTL),
  - VW3A3203 extended I/O module,
  - VW3A3204 extended relay module.

  **NOTE:** Maximum configuration is based on activation of OPC UA services and varies with Bus Cycle Time, usage of EcoStruxure Automation Expert libraries, and other services. Use the light Hardware CAT for designing maximum configuration.

**NOTE:** The configuration with Altivar drives in remote architecture is done with SoMove using pre-configured .psx files (one for each drive family). For more information refer to SE.FieldDevice online help.

**NOTE:** In some environments, the maximum configuration populated by high consumption modules, coupled with the maximum distance allowable between the devices, may present bus communication errors although the EcoStruxure Automation Expert software allows for the configuration. In such a case you will need to analyze the power consumption of the modules chosen for your configuration, as well as the minimum cable distance required by your application, and possibly seek to optimize your choices.

# Accessories

## Overview

This section describes the accessories and cables.

## Accessories

| Reference | Description | Use | Quantity |
|---|---|---|---|
| VW3A1111 | Graphic Display Terminal (VW3A1111) | Includes a battery to monitor time when power is off.<br>**NOTE:** Graphic Display Terminal (VW3A1111) is not delivered with ATV340 and cabinet integration products (ATV600●●●●●Z, ATV900●●●●●Z). | 1 |
| VW3A1112 | Remote Mounting Kit | To mount the Graphic Display Terminal (VW3A1111) on enclosure door.<br>It requires a remote-mounting cord set. | 1 |
| VW3A1104R10<br>VW3A1104R30<br>VW3A1104R50<br>VW3A1104R100 | Remote-mounting cord set (1 m, 3 m, 5 m, 10 m) | To wire the drive to the remote-mounting kit.It is equipped with 2 RJ45 connectors. | 1 |
| ZB5AZ905 | Tightening tool | For remote mounting kit | 1 |

For more information refer to the Altivar drive catalogs.

## Cables

| Reference | Description | Details | Length |
|---|---|---|---|
| 490NTW000•• | Ethernet shielded cable for DTE connections | Standard cable, equipped with RJ45 connectors at each end for DTE.<br>CE compliant. | 2, 5, 12, 40, or 80 m<br>(6.56, 16.4, 39.37, 131.23 or 262.5 ft) |
| 490NTW000••U | | Standard cable, equipped with RJ45 connectors at each end for DTE.<br>UL compliant. | 2, 5, 12, 40, or 80 m<br>(6.56, 16.4, 39.37, 131.23, or 262.5 ft) |
| TCSECE3M3M••S4 | | Cable for harsh environment, equipped with RJ45 connectors at each end.<br>CE compliant. | 1, 2, 3, 5, or 10 m<br>(3.28, 6.56, 9.84, 16.4, 32.81 ft) |
| TCSECU3M3M••S4 | | Cable for harsh environment, equipped with RJ45 connectors at each end.<br>UL compliant. | 1, 2, 3, 5, or 10 m<br>(3.28, 6.56, 9.84, 16.4, 32.81 ft) |

# ATV dPAC Features

## Real Time Clock (RTC)

The ATV dPAC includes an RTC to provide system date and time information, and to support related functions requiring a real-time clock. To continue to monitor time when power is off, a non-rechargeable battery is required (see reference below).

This table shows how RTC drift is managed:

| RTC Characteristics | Description |
|---|---|
| RTC drift | Less than 60 seconds per month without any user calibration at 25 °C (77 °F) |

**NOTE:** It's mandatory to have a Graphic Display Terminal (VW3A1111) for ATV 340 to monitor the RTC when the power is off.

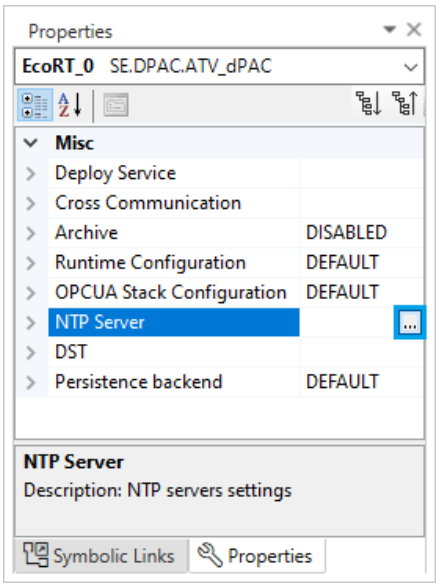
## NTP and DST configuration in EcoStruxure Automation Expert

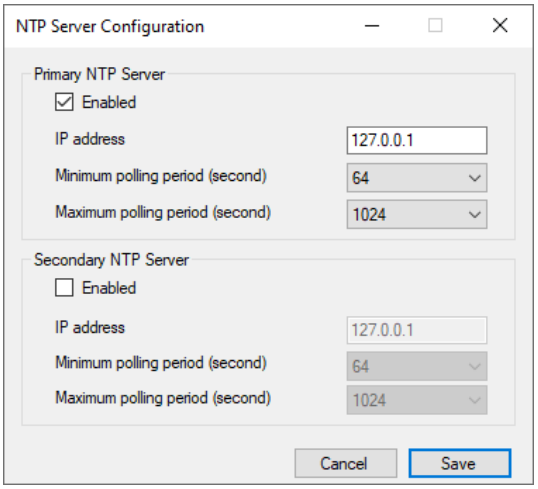
### Overview

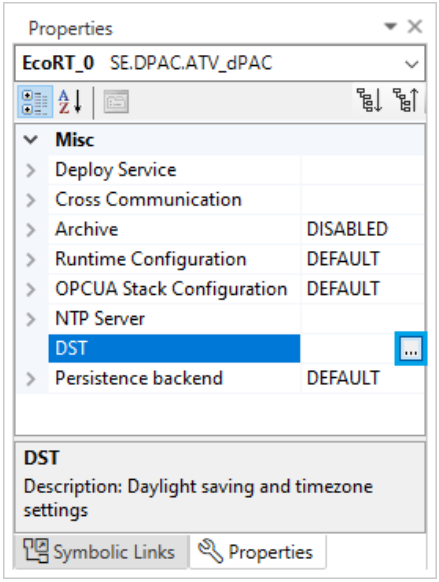
Use the **NTP** (Network Time Protocol) Server Configuration dialog to synchronize the clock of the selected device to a time value provided by an NTP server.

Use **DST** (Time zone and Daylight settings) to change the time zone of your device.

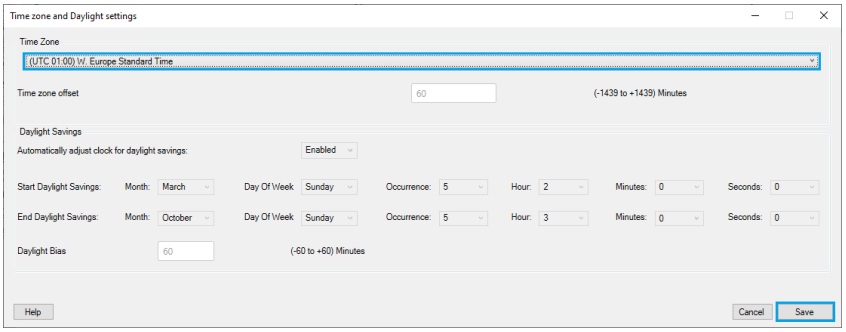
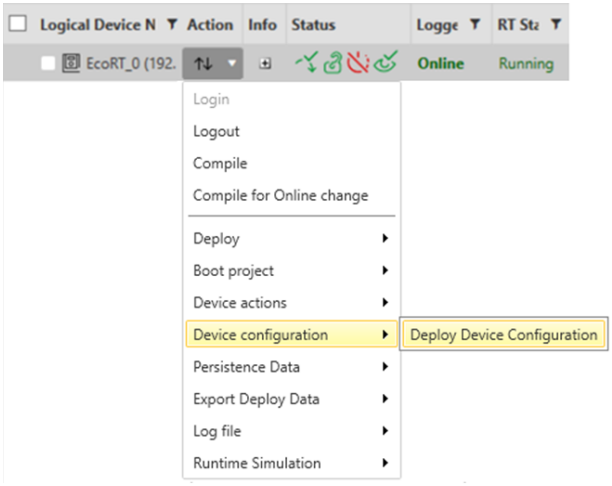
### Procedure

| Step | Action |
|---|---|
| 1 | Select a device in the Logical Devices editor in EcoStruxure Automation Expert. |
| 2 | In the Properties pad click the ellipsis for the NTP Server node.<br>  |
| 3 | **NTP Server Configuration** window opens allowing you to configure the following parameters:<br>• Primary NTP Server only<br>• Both, Primary NTP Server and Secondary NTP Server |

<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td></td><td>


<br>The table below explains these parameters:
<table>
<tr><th>Parameter</th><th>Description</th></tr>
<tr><td>Enabled</td><td>Activates polling by the NTP client of the device to the NTP server.</td></tr>
<tr><td>IP address</td><td>The IPv4 address.of the NTP server.</td></tr>
<tr><td>Minimum polling period</td><td>The minimum time, in seconds, the NTP client of the device waits to poll the NTP server.</td></tr>
<tr><td>Maximum polling period</td><td>The maximum time the NTP client of the device waits, in seconds, to poll the NTP server.</td></tr>
</table>
</td></tr>
<tr><td>4</td><td>
<ul>
<li>Set the IP address of your NTP server</li>
<li>Save the NTP server configuration</li>
</ul>
NOTE: The NTP server could be a PLC or a laptop, etc.
</td></tr>
<tr><td>5</td><td>
In the Properties pad click the ellipsis for the DST node.


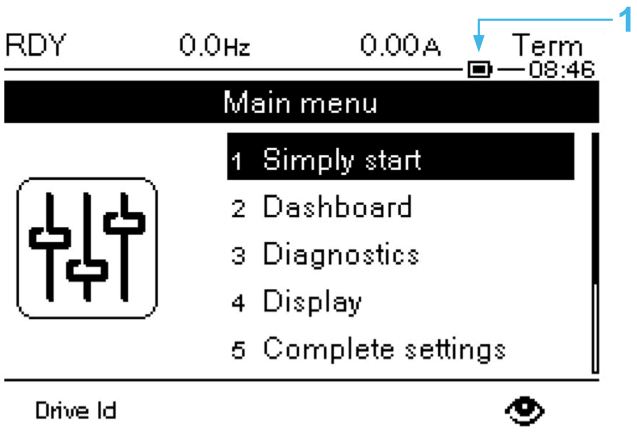
</td></tr>
<tr><td>6</td><td>Select your time zone from Time zone and Daylight settings window, then click Save.</td></tr>
</table>

| Step | Action |
|---|---|
| |  |
| 7 | • Open the deploy and diagnostic editor<br>• Compile<br>• Login to the device<br>• Deploy<br>• Run device actions<br>• Deploy device configuration<br>  |
| 8 | Restart the device to apply the changes. |

## Battery

ATV dPAC controller uses a battery located in the Graphic Display Terminal (VW3A1111): the Graphic Display Terminal (VW3A1111) must remain connected to the Altivar drive.

A battery icon on the Graphic Display Terminal (VW3A1111) indicates if the battery is depleted or absent.




Legend:

**1** Battery icon

The Graphic Display Terminal (VW3A1111) is not delivered with ATV340 drives and ATV600, ATV900 cabinet integration drives. It must be ordered separately.

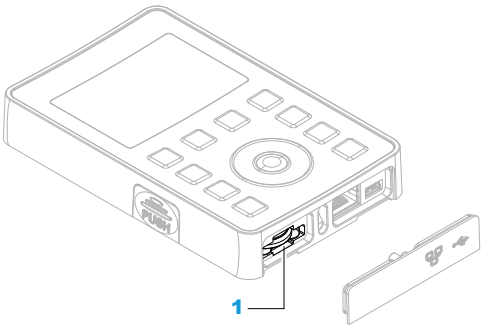
In the event of a power interruption, the backup battery maintains the RTC for the controller.

This table shows the characteristics of the battery:

| Characteristics | Description |
|---|---|
| **Use** | In the event of a transient power outage, the battery powers the RTC. |
| **Backup life** | At least 2 years at 25 °C maximum (77 °F). At higher temperatures, the time is reduced |
| **Battery monitoring** | Yes |
| **Replaceable** | Yes |
| **Controller battery type** | Lithium coin cell, type Panasonic CR2032 |

## Location of the Battery in the Graphic Display Terminal (VW3A1111)

The battery is located at the bottom of the Graphic Display Terminal (VW3A1111) (see 1 in the figure below):




## Installing or Replacing the Battery

While lithium batteries are preferred due to their slow discharge and long life, they can present hazards to personnel, equipment and the environment and must be handled properly.

**⚠DANGER**

**EXPLOSION, FIRE OR CHEMICAL BURNS**

- Replace with identical battery type
- Follow all the instructions of the battery manufacturer
- Remove all replaceable batteries before discarding unit
- Recycle or properly dispose of used batteries
- Protect battery from any potential short-circuit
- Do not recharge, disassemble, heat above 100 °C (212 °F), or incinerate
- Use your hands or insulated tools to remove or replace the battery
- Maintain proper polarity when inserting and connecting a new battery

**Failure to follow these instructions will result in death or serious injury.**

To install or replace the battery, follow these steps:

### Battery Installation

| Step | Action |
|---|---|
| 1 | Ensure that the power is off. |
| 2 | Remove the Graphic Display Terminal (VW3A1111) from the drive or the remove mounting kit. |
| 3 | Remove the strip at the bottom of the Graphic Display Terminal (VW3A1111) |
| 4 | Remove the battery from the battery holder |
| 5 | Insert the new battery into the battery holder in accordance with the polarity markings on the battery |
| 6 | Put back the strip at the bottom of the Graphic Display Terminal (VW3A1111) |
| 7 | Put back the Graphic Display Terminal (VW3A1111) at its previous location |
| 8 | Power on the drive (or at least the control part in case of separate supply mode). |
| 9 | Set the internal clock |

# ATV dPAC Installation

## ATV dPAC General Information

### Mechanical data

**ATV dPAC weight**: 0.15 kg

**ATV dPAC dimensions**: 41 x 109 x 23.25 mm (1.61 x 4.29 x 0.91 in)

### Environmental characteristics

Refer to Schneider Electric website and/or to the Installation Manual of Altivar drives, page 15

### Certifications and Standards

Refer to Schneider Electric website and/or to the Installation Manual of Altivar drives, page 15

## Installation and Maintenance Requirements

### Before Starting

Read and understand this chapter before beginning the installation of your system.

The use and application of the information contained herein require expertise in the design and programming of automated control systems. Only you, the user, machine builder or integrator, can be aware of all the conditions and factors present during installation and setup, operation, and maintenance of the machine or process, and can therefore determine the automation and associated equipment and the related safeties and interlocks which can be effectively and properly used. When selecting automation and control equipment, and any other related equipment or software, for a particular application, you must also consider any applicable local, regional or national standards and/or regulations.

Pay particular attention in conforming to any safety information, different electrical requirements, and normative standards that would apply to your machine or process in the use of this equipment.

# Disconnecting Power

Ensure that the power is off before installing or uninstalling any option modules.

**Read and understand these instructions before performing any procedure with this drive.**

**⚠⚠DANGER**

**HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH**

- Only appropriately trained persons who are familiar with and fully understand the contents of the present manual and all other pertinent product documentation and who have received all necessary training to recognize and avoid hazards involved are authorized to work on and with this drive system.
- Installation, adjustment, repair and maintenance must be performed by qualified personnel.
- Verify compliance with all local and national electrical code requirements as well as all other applicable regulations with respect to grounding of all equipment.
- Only use properly rated, electrically insulated tools and measuring equipment.
- Do not touch unshielded components or terminals with voltage present.
- Prior to performing any type of work on the drive system, block the motor shaft to prevent rotation.
- Insulate both ends of unused conductors of the motor cable.
- Do not short across the DC bus terminals or the DC bus capacitors or the braking resistor terminals.

**Failure to follow these instructions will result in death or serious injury.**

**⚠⚠DANGER**

**HAZARD OF ELECTRIC SHOCK, EXPLOSION, OR ARC FLASH**

Before performing work on the drive system:

- Disconnect all power, including external control power that may be present. Take into account that the circuit breaker or main switch does not de-energize all circuits.
- Place a “Do Not Turn On” label on all power switches related to the drive system.
- Lock all power switches in the open position.
- Wait 15 minutes to allow the DC bus capacitors to discharge.
- Verify the absence of voltage. (1)

Before applying voltage to the drive system:

- Verify that the work has been completed and that the entire installation cannot cause hazards.
- If the mains input terminals and the motor output terminals have been grounded and short-circuited, remove the ground and the short circuits on the mains input terminals and the motor output terminals.
- Verify proper grounding of all equipment.
- Verify that all protective equipment such as covers, doors, grids is installed and/or closed.

**Failure to follow these instructions will result in death or serious injury.**

Refer to the installation manual of the product. See Related Documents., page 15

## Programming Considerations

**⚠WARNING**

**UNANTICIPATED 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.**

## Operating Environment

In addition to the **Environmental Characteristics**, refer to **Product Related Information** in the beginning of the present document for important information regarding installation in hazardous locations for this specific equipment.

**⚠WARNING**

**UNANTICIPATED EQUIPMENT OPERATION**

Install and operate this equipment according to the conditions described in the Environmental Characteristics.

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

## Installation Considerations

**⚠WARNING**

**UNANTICIPATED EQUIPMENT OPERATION**

- Use appropriate safety interlocks where personnel and/or equipment hazards exist.
- Install and operate this equipment in an enclosure appropriately rated for its intended environment and secured by a keyed or tooled locking mechanism.
- Use the sensor and actuator power supplies only for supplying power to the sensors or actuators connected to the module.
- Power line and output circuits must be wired and fused in compliance with local and national regulatory requirements for the rated current and voltage of the particular equipment.
- Do not use this equipment in safety-critical machine functions unless the equipment is otherwise designated as functional safety equipment and conforming to applicable regulations and standards.
- Do not disassemble, repair, or modify this equipment
- Do not connect any wiring to reserved, unused connections, or to connections designated as No Connection (N.C.).

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

# Installation of the ATV dPAC

## Before Starting

Verify that the module catalog number marked on the label is the same as that on the delivery note corresponding to the purchase order.

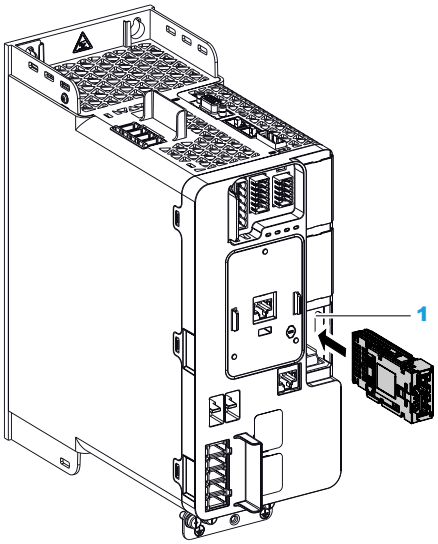
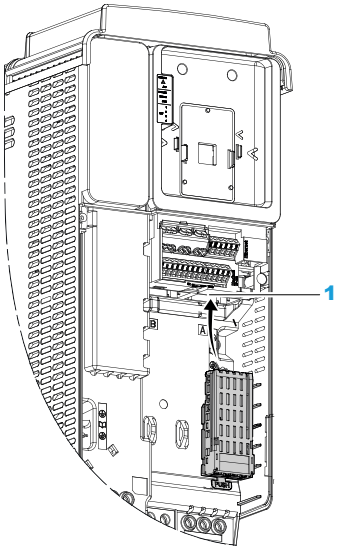
Remove the ATV dPAC module from its packaging and verify that it has not been damaged in transit.

Verify that the ATV dPAC is compatible with the drive firmware version. Refer to Firmware Version Compatibility, page 20.

## Insertion of the ATV dPAC

The table provides the procedure for insertion of the ATV dPAC in the drive:

| Step | Action |
|---|---|
| 1 | Ensure that the power is off. |
| 2 | Locate the module slot A on the bottom of the control part (or GP-FB on ATV340 with power equal to or lower than 22kW. |
| 3 | Insert the ATV dPAC in the corresponding slot. |
| 4 | Add the corresponding sticker on the LED front panel of the drive.<br>**NOTE:** There is not sticker for ATV340 with power equal to or lower than 22kW. In this case, the used LEDs are located on the module itself |
| 5 | Verify that the module is correctly inserted and locked mechanically in the drive. |

| **ATV340 (power ≤ 22 kW)** | **ATV340 (power > 22 kW), ATV600 and ATV900** |
|---|---|
|  |  |
| **1**: GP-FB Slot | **1**: Module slot A |

## Removal of the ATV dPAC

The table provides the procedure for removal of the ATV dPAC option module from the drive:

| Step | Action |
|---|---|
| 1 | Ensure that the power is off. |
| 2 | Press the strip. |
| 3 | Remove the module while maintaining the strip pressed, |

## Additional information

For more information on the installation refer to the Instruction Sheet S1A45591 provided with the ATV dPAC or on www.se.com

# Electrical requirements

## Wiring best practices

ATV dPAC is inserted inside Altivar drive. For the wiring related to the drive, refer to the section Drive Wiring available inside the installation of the drive (See Related Documents, page 15)

This paragraph describes the wiring guidelines and associated best practices to be respected when using the ATV dPAC system.

**⚠ DANGER**

**HAZARD OF ELECTRIC SHOCK, EXPLOSION OR ARC FLASH**

- Disconnect all power from all equipment including connected devices prior to removing any covers or doors, or installing or removing any accessories, hardware, cables, or wires except under the specific conditions specified in the appropriate hardware guide for this equipment.
- Always use a properly rated voltage sensing device to confirm the power is off where and when indicated.
- Replace and secure all covers, accessories, hardware, cables, and wires and confirm that a proper ground connection exists before applying power to the unit.
- Use only the specified voltage when operating this equipment and any associated products.

**Failure to follow these instructions will result in death or serious injury.**

## ⚠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.**

**NOTE:** 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.

These requirements must be applied when wiring an ATV dPAC system:

- Communication wiring must be kept separate from the power wiring. Route these 2 types of wiring in separate cable ducting.
- Verify that the operating conditions and environment are within the specification values.
- Use twisted pair, shielded cables for networks, and fieldbus.

Use shielded, properly grounded cables for all communication connections. If you do not use shielded cable for these connections, electromagnetic interference can cause signal degradation. Degraded signals can cause the controller or attached modules and equipment to perform in an unintended manner.

**⚠WARNING**

**UNANTICIPATED EQUIPMENT OPERATION**

- Use shielded cables for all communication signals.
- Ground cable shields for all communication signals at a single point.
- Route communication separately from power cables.

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

**NOTE:** Multipoint grounding is permissible if connections are made to an equipotential ground plane dimensioned to help avoid cable shield damage in the event of power system short-circuit currents.

For more details, refer to Grounding Shielded Cables, page 40.

**NOTE:** Surface temperatures may exceed 60 °C (140 °F).

To conform to IEC 61010 standards, route primary wiring (wires connected to power mains) separately and apart from secondary wiring (extra low voltage wiring coming from intervening power sources). If that is not possible, double insulation is required such as conduit or cable gains.

## DC Power supply characteristics & wiring

The power supply of the ATV dPAC is provided by the host Altivar drive. For the characteristics and wiring related to the power supply of the drive, refer to the installation manual of the drive (See Related Documents, page 15).

Depending on the drive wiring, there are two different modes to energize the ATV dPAC:

- With the drive powered by the power supply stage,
- With Separate Control Stage of the Drive. The control part and the power part of the drive are separated. The external control power supply must meet the requirements given in the installation manual of the drive.

**⚠⚠DANGER**

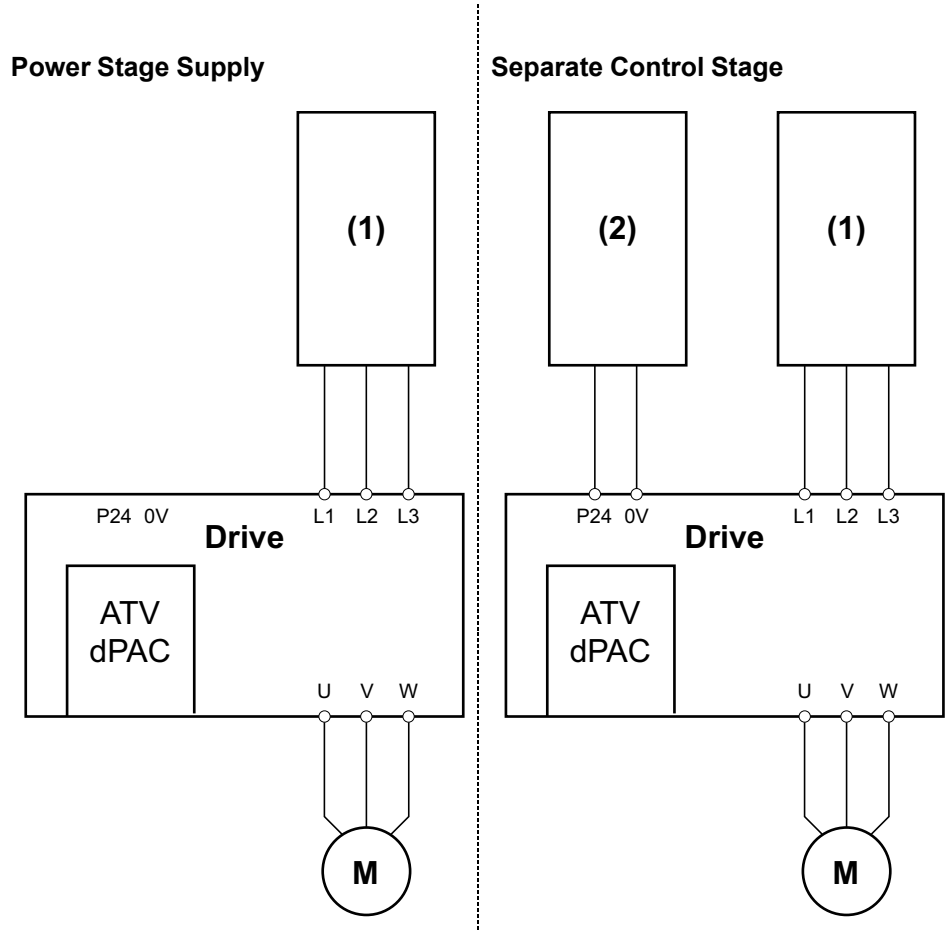
**ELECTRIC SHOCK CAUSED BY INCORRECT POWER SUPPLY UNIT**

The +24VDC supply voltage is connected with many exposed signal connections in the drive system.

- Use a power supply unit that meets the PELV (Protective Extra Low Voltage) requirements.

**Failure to follow these instructions will result in death or serious injury.**

**DC Power Supply Wiring**




Legend: **(1)** Power — **(2)** Control

**Power interruption**

With separate control stage, the duration of power interruptions where the ATV dPAC is able to continue normal operation varies depending upon the load on the outputs of the drive and the presence of option module, it can be shorter than 1 ms. With power stage supply, the duration of power interruptions where the ATV dPAC is able to continue normal operation varies but a minimum of 10 ms is maintained as specified by IEC standards. To sustain longer power interruption, it is advisable to use power stage supply.

When planning the management of the power supplied to the controller, you must consider the power interruption duration due to the fast cycle time of the controller.

There could potentially be many scans of the logic and consequential updates to the I/O image table during the power interruption, while there is no external power supplied to the inputs, the outputs or both depending on the power system architecture and power interruption circumstances.

**⚠WARNING**

**UNANTICIPATED EQUIPMENT OPERATION**

- Individually monitor each source of power used in the controller system including input power supplies, output power supplies and the power supply to the controller to allow appropriate system shutdown during power system interruptions.
- The inputs monitoring each of the power supply sources must be unfiltered inputs.

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

# Grounding the ATV dPAC system

ATV dPAC is inserted inside Altivar drive. For the grounding related to the drive, refer to the installation of the drive (See Related Documents, page 15).

Regarding the ATV dPAC, the following requirements must be applied.

**⚠WARNING**

**UNANTICIPATED EQUIPMENT OPERATION**

- Use shielded cables for all digital and analog I/O signals and communication signals.
- Ground cable shields at a single point.
- Route communication cables and I/O cables separately from power cables

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

1 Multi-point grounding is permissible if connections are made to an equi-potential ground plane dimensioned to help avoid cable shield damage in the event of power system short-circuit currents

# ATV dPAC Communication

## Ethernet Port

### Overview

The ATV dPAC is equipped with one dual Ethernet port switch.

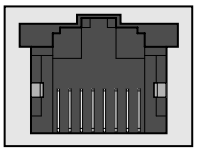
### Characteristics

This table describes the different Ethernet characteristics:

| Characteristic | Description |
|---|---|
| Function | Modbus TCP/IP protocol |
| Connector type | RJ45 |
| Auto negotiation | From 10 M half duplex to 100 M full duplex |
| Cable type | Shielded |
| Automatic cross-over detection | Yes |

### Pin assignment

This figure shows the RJ45 Ethernet connector pin assignment:



8 7 6 5 4 3 2 1

This table describes the RJ45 Ethernet connector pins:

| Pin N | Signal |
|---|---|
| 1 | TD+ |
| 2 | TD- |
| 3 | RD+ |
| 4 | NA |
| 5 | NA |
| 6 | RD- |
| 7 | NA |
| 8 | NA |

# Connecting the ATV dPAC to a PC

## Connecting the Controller to a PC

### Overview

To transfer, run, and monitor the applications, connect the ATV dPAC to a PC, that has EcoStruxure Automation Expert installed, using an Ethernet connection.

| *NOTICE* |
| --- |
| **INOPERABLE EQUIPMENT**<br>Always connect the communication cable to the PC before connecting it to the controller.<br>**Failure to follow these instructions can result in equipment damage.** |

The default IP address is 0.0.0.0 for both Ethernet ports.

The default mask is 0.0.0.0.

### Ethernet Port Connection

If there is a need for a firmware update, perform the following actions to connect the controller to the PC

| Step | Action |
| --- | --- |
| 1 | Connect the Ethernet cable to the PC. |
| 2 | Connect the Ethernet cable to either one of the Ethernet ports on the ATV dPAC. |
| 3 | Perform DPWS discovery (IPv6 connection) to connect from EcoStruxure Automation Device Maintenance. |
| 4 | Login and update the firmware, set the IPv4 address you need with EcoStruxure Automation Device Maintenance. |
| 5 | Use IPv4 address to connect from EcoStruxure Automation Expert. |

If the firmware is up to date, perform the following actions:

| Step | Action |
| --- | --- |
| 1 | Connect the Ethernet cable to the PC. |
| 2 | Connect the Ethernet cable to either one of the Ethernet ports on the ATV dPAC. |
| 3 | Add the ATV drive and ATV dPAC under Physical Topology in **EcoStruxure Automation Expert**, then configure the IP address using properties tab of ATV dPAC. |
| 4 | Start the system monitoring and configure security using default credentials.<br>Login - installer<br>Password - Inst@ller1<br>**NOTE:** Use the Graphic Display Terminal (VW3A1111) to enable security for the ATV drive and the ATV dPAC |
| 5 | Login and Deploy the EcoStruxure Automation Expert solution. |
| **NOTE:** It is also possible to set the IPv4 address with **EcoStruxure Automation Expert**. | |

# Firmware update with EcoStruxure Automation Device Maintenance

## Abstract

This chapter contains important information about the hardware, the firmware, and the software delivery of the product ATV dPAC. Read the chapter before using the product.

## Product information

The table below shows the contents of EcoStruxure Automation Expert installation package for different versions.

**ATV dPAC System Compatibility**

| EAE(1) version | SEDP archive | ATV dPAC VW3A3530-D firmware version | ATV340 firmware version | ATV6xx firmware version | ATV9xx firmware version | EADM(2) version | Labels of the Graphic Display Terminal (VW3A1111) | Date |
|---|---|---|---|---|---|---|---|---|
| **20.2.20318.-07** | SEDP_ATVD_20.2.321.01 | 3.1IE02_B05-20.2.321.01 | 3.1IE94_B12 | 2.6IE94_B12 | 3.1IE94_B12 | 20.2.310.1 | — | December 2020 |
| **21.1.21139.-10** | SEDP_ATVD_21.1.132.02 | 3.1IE04_B03-21.1.132.00 | 3.1IE94_B13 | 2.6IE94_B13 | 3.1IE94_B13 | 20.2.351.2 | — | July 2021 |
| **21.2.21346.-08** | SEDP_ATVD_21.2.21342.-00 | 3.1IE06_B04-21.2.21342.-00 | 3.4IE94_B02 | 3.5IE94_B02 | 3.5IE94_B02 | V3.0.191 | 1.24 | December 2021 |
| **22.0.22181.-16** | SEDP_ATVD_22.0.22179.-00 | 3.1IE07B06-22.0.22179.-00 | 3.4IE94_B04 | 3.5IE94_B04 | 3.5IE94_B04 | 3.0.203 | 1.38 | July 2022 |
| **22.1.23130.-00** | SEDP_ATVD_22.1.23130.-00 | 3.1IE10_B02-22.1.23130.-00 | V3.6IE94_B04 | 3.7IE94_B04 | 3.8IE94_B04 | 3.1.147 | 1.43 | June 2023 |
| **23.0** | SEDP_ATVD_23.0* | 3.1IE11B0*-23.0.* | 3.6IE94_B04 | 3.7IE94_B04 | 3.8IE94_B04 | 3.2.124 | 1.45 | July 2023 |

(1) EcoStruxure Automation Expert

(2) EcoStruxure Automation Device Maintenance

**NOTE:**

- To upgrade/downgrade any firmware versions between 21.2 and 23.0, it is recommended to use the latest version of EcoStruxure Automation Device Maintenance 3.2 (available in EcoStruxure Automation Expert 23.0 installation package).
- To upgrade/downgrade any firmware versions between 20.2 and 21.2, it is recommended to use the version of EcoStruxure Automation Device Maintenance which is compatible with the current firmware of the drive or the ATV dPAC, as well as the ATV Plugin (available in EcoStruxure Automation Expert installation package, to enable the firmware update).

The table below shows the Firmware upgrade/downgrade compatibility for the ATV dPAC module:

**ATV dPAC Firmware upgrade/downgrade Compatibility**

| From\ to | 20.2.20318.07<br>3.1IE02_B05 | 21.1.21139.10<br>3.1IE04_B03 | 21.2.21346.08<br>3.1IE06_B04 | 22.0.22181.16<br>3.1IE07_B06 | 22.1.23019.67<br>3.1IE09_B01 | 23.0 |
|---|---|---|---|---|---|---|
| **20.2.20318.07<br>3.1IE02_B05** | N/A | Yes(1) | No | No | No | No |
| **21.1.21139.10<br>3.1IE04_B03** | No | N/A | Yes(2) | No | No | No |
| **21.2.21346.08<br>3.1IE06_B04** | No | No | N/A | Yes(2) | Yes(2) | Yes(2) |
| **22.0.22181.16<br>3.1IE07_B06** | No | No | Yes(3) | N/A | Yes(2) | Yes(2) |
| **22.1.23019.67<br>3.1IE09_B01** | No | No | Yes(3) | Yes(3) | N/A | Yes(2) |
| **23.0** | No | No | Yes(3) | Yes(3) | Yes(3) | N/A |

(1) To update the firmware for this specific case only:

- Use EcoStruxure Automation Device Maintenance 20.2.351.2.
- Install Automation Device Maintenance - ATV Plugin 20.2.351.2 (available in EcoStruxure Automation Expert 21.1 installation package) to enable the firmware update, refer to the Readme file instructions for further information.

(2) To update the firmware use the latest version of EcoStruxure Automation Device Maintenance 3.2 (available in EcoStruxure Automation Expert 23.0 installation package).

(3) Downgrading is possible but not recommended, as new features will not be supported.

**NOTE:** After updating to firmware version 21.1 or later, you may notice a Security File Corrupt [SPFC] error, restart the drive to clear the error.

# ATV firmware update

## Overview

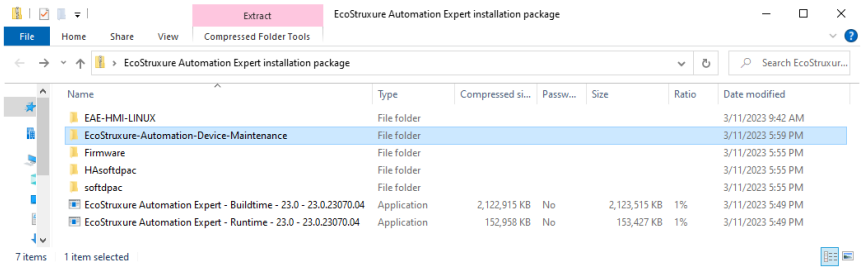
There are four main steps to update the firmware of the device:

1. Pre-configuration.
2. Update the ATV drive firmware.
3. Update the ATV dPAC firmware.
4. Update the labels and languages of the Graphic Display Terminal (VW3A1111).

## Step 1: Pre-configuration

Use the following instructions to setup the firmware with EcoStruxure Automation Device Maintenance.

| Step | Action |
|---|---|
| 1 | Download and install EcoStruxure Automation Device Maintenance (Available in EcoStruxure Automation Expert installation package) |




**NOTE:**

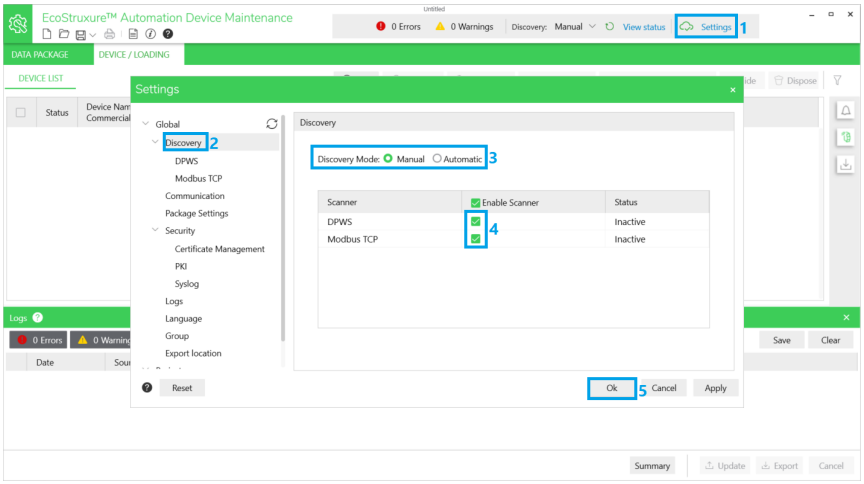
- To upgrade/downgrade any firmware versions between 21.2 and 23.0, it is recommended to use the latest version of EcoStruxure Automation Device Maintenance 3.2 (available in EcoStruxure Automation Expert 23.0 installation package).
- To upgrade/downgrade any firmware versions between 20.2 and 21.2, it is recommended to use the version of EcoStruxure Automation Device Maintenance which is compatible with the current firmware of the drive or the ATV dPAC, as well as the ATV Plugin (available in EcoStruxure Automation Expert installation package, to enable the firmware update).

2 Configure the discovery mode

**NOTE:** You can select the device discovery mode as **Automatic** or **Manual** discovery. In case of:

- **Automatic** discovery, the tool will periodically send information over the network in the background and receive information from the responding devices.
- **Manual** discovery, you can manually discover the devices connected in the network when required.

1. Click **Settings** menu.
2. Click **Discovery**.
3. Select the **Discovery mode** (**Automatic** or **Manual**)
4. Select the scanners that will be taking part in discovery (**DPWS**-IPv6 and **Modbus TCP**-IPv4). Use this setting to help prevent scanning of any devices that you want to avoid.
5. Click **OK**.



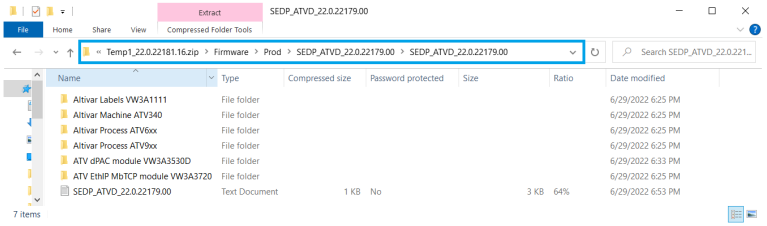

**NOTE:** For more information about how to configure the scanners (**DPWS** and **Modbus TCP**), refer to EcoStruxure Automation Device Maintenance online help.

3 Copy-paste the ATV Firmware packages (*.fwp files and *.sedp files), to the default EcoStruxure Automation Device Maintenance Data Packages folder: by default it is *C:\Users\Public\Documents\Schneider Electric\Data Packages*

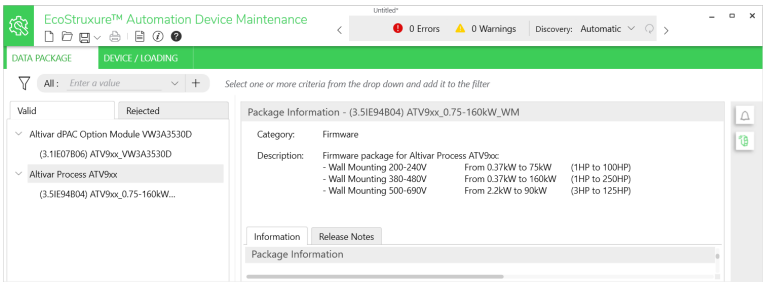
**NOTE:**

- Always update the firmware of the Altivar drive and the ATV dPAC to match the version of EcoStruxure Automation Expert, as mentioned in ATV dPAC system compatibility table.

- The firmware packages can be found in EcoStruxure Automation Expert installation package (**Example: EcoStruxure Automation Expert installation package > Firmware > Prod > SEDP_ATVD_*.zip**)

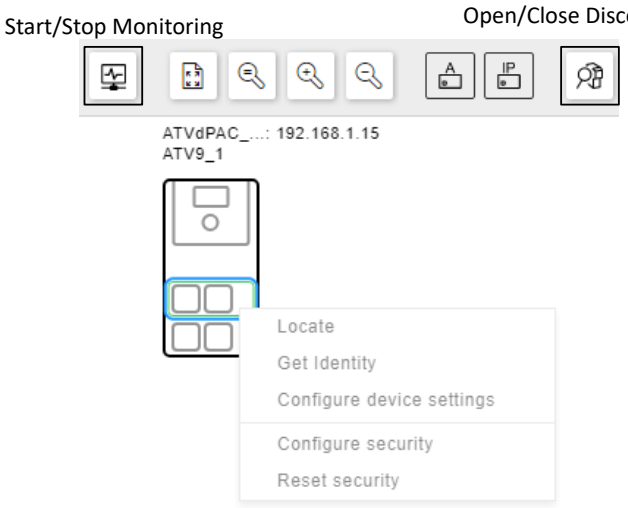



The copied and pasted packages will then be displayed in EcoStruxure Automation Device Maintenance in **DATA PACKAGE** tab.




4 Before updating the firmware:

- Confirm that EcoStruxure Automation Expert version supports the firmware version you are installing.
- Close EcoStruxure Automation Expert discovery view in the Topological View.
- Stop EcoStruxure Automation Expert monitoring in the Topological View is recommended.



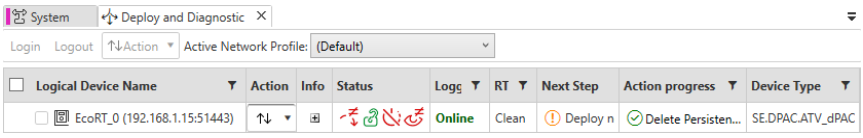
5

Before updating the firmware, confirm that the ATV dPAC runtime state is **CLEAN**, **READY**, or **STOPPED** as follows:

| ATV dPAC State | Upgrade Status |
|---|---|
| CLEAN | ALLOWED |
| READY | ALLOWED |
| STOPPED | ALLOWED |
| RUNNING | ALLOWED<br>**NOTE:** EcoStruxure Automation Device Maintenance stops the ATV dPAC if its in the run state before starting the firmware update. It's not mandatory to stop using EcoStruxure Automation Expert. |
| ONLINE CHANGE | REFUSED |
| ERRORHALT | REFUSED |

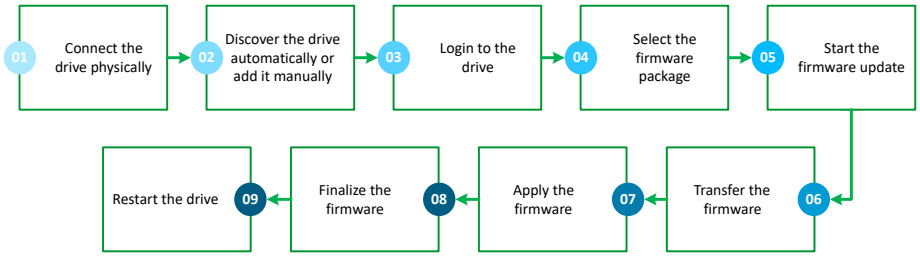
**NOTE:** When an ATV dPAC application is in Running state:

- https connection blocks changing the IP settings.
- mbap connection authorizes the connected device to change the IP settings but a reset will take place.




# Step 2: Update the ATV drive firmware

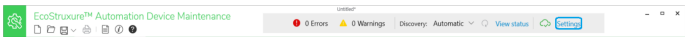
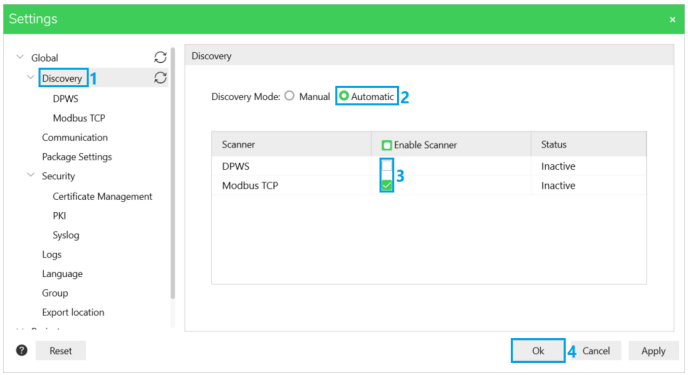
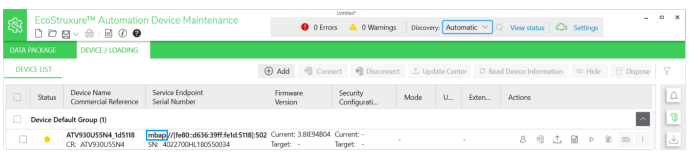
Use the following instructions to update the drive firmware with EcoStruxure Automation Device Maintenance.




**NOTE:** The steps 06, 07, 08 and 09 are done automatically by EcoStruxure Automation Device Maintenance, you only need to confirm the safety message related to the steps 06, 07 and 08.

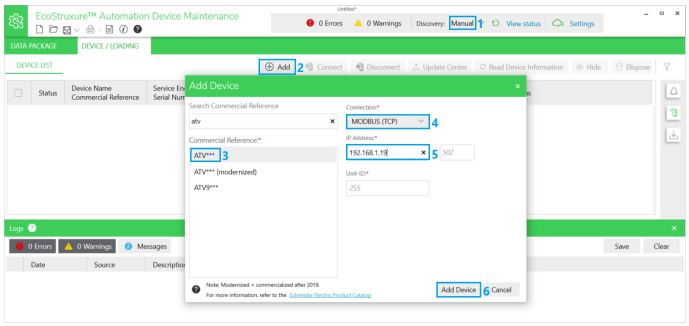
The following procedure is used with EcoStruxure Automation Device Maintenance 3.2, thus, it can be used to update any firmware version between 21.2 and 23.0

| step | Action |
|---|---|
| 01 | Connect the drive physically<br><br>For drives supporting Ethernet protocol, connect the Ethernet cable between the device embedded Ethernet port and the computer where EcoStruxure Automation Device Maintenance is running, then turn on the drive if it is not already on.<br><br>  <br><br>**NOTE:** The firmware update of ATV340 < 22kW (ATV340U07N4 to ATV340D22N4) cannot be done over embedded Ethernet port. To update it you can either connect your drive to Ethernet option module port, or to modbus serial line port using TCSMCNAM3M002P cable. |
| 02 | Discover the drive automatically or add it manually<br>• Discover the drive automatically |

| Step | Action |
|---|---|
| 1 | Select **Settings** from EcoStruxure Automation Device Maintenance toolbar.<br>  |
| 2 | Updating the settings<br>1. Select **Discovery**<br>2. Select **Automatic**<br>3. Deselect **DPWS** and Select **Modbus TCP**.<br>4. Click **Ok**.<br>  <br><br>**NOTE:** For ATV drive, firmware automatic discovery is always performed using the Modbus TCP scanner. |
| 3 | **Result:** The drive is added automatically using **Modbus TCP** scanner (**mbap**- IPv4) in **DEVICE / LOADING** tab.<br>  <br><br>**NOTE:** Some firewall software may block the discovery. If you are unable to discover the device, disable firewall or consult your system administrator. |

**NOTE:** If the automatic discovery is not working, then add the drive manually.

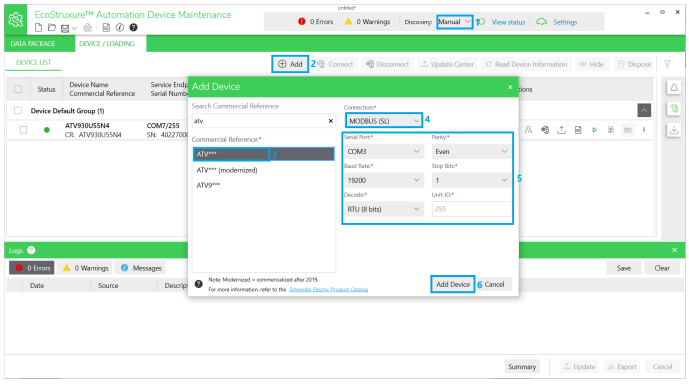
| step | Action |
|---|---|
| | • Add the drive manually using **Modbus TCP** scanner (**mbap**-IPv4) |

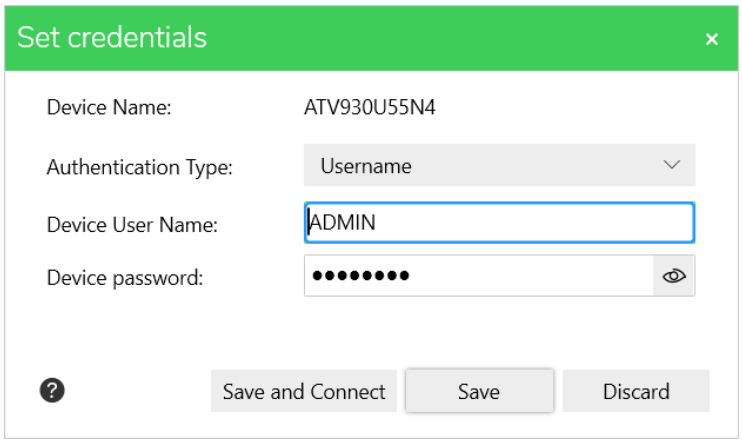
| Step | Action |
|---|---|
| 1 | Select **Manual** from **Discovery** drop-down menu (to prevent the cyclic data change effect between **DPWS** and **Modbus TCP** scanner. |
| 2 | Click **Add** ⊕ Add. |
| 3 | Select the **Commercial Reference** of your drive.<br>**NOTE:** To add the drive manually using **Modbus TCP** scanner (**mbap**-IPv4), select **ATV*****, not **ATV*** (modernized)**. |
| 4 | Select **MODBUS (TCP)** for **Connection**. |
| 5 | Type the **IP Address** of your drive. |
| 6 | Click **Add Device**.<br>The figure below shows all the steps:<br>  |

**NOTE:** if the drive manual add feature using **Modbus TCP** scanner is not working, then add it using **Modbus serial line** scanner.

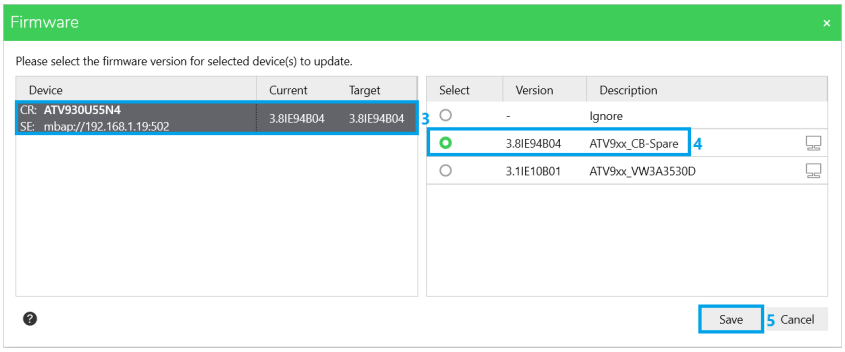
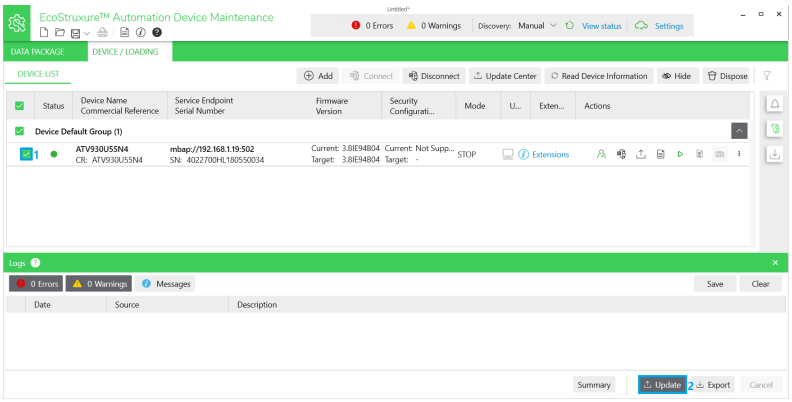
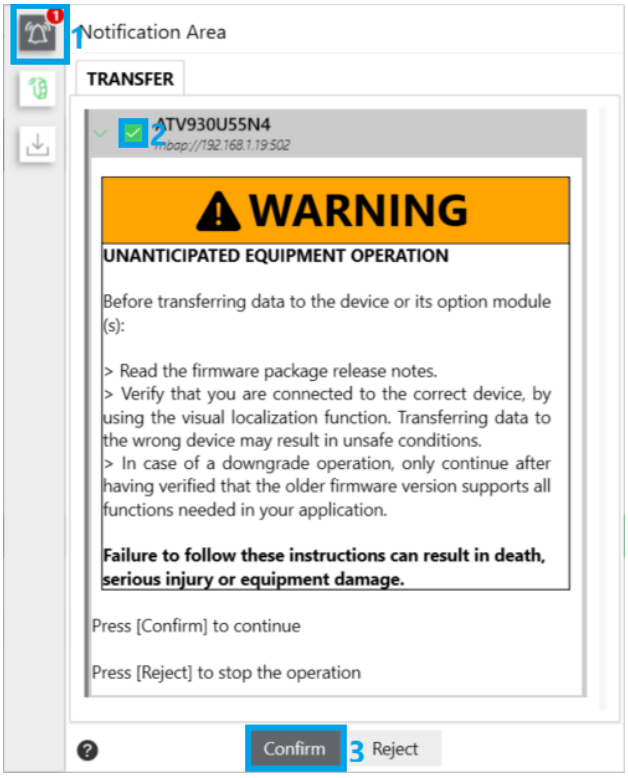
- Add the drive manually using **Modbus serial line** scanner for firmware update in case Ethernet protocol is not supported. To add a device.

  **NOTE:** For ATV drives, the physical connection can be done using TCSMCNAM3M002P cable.

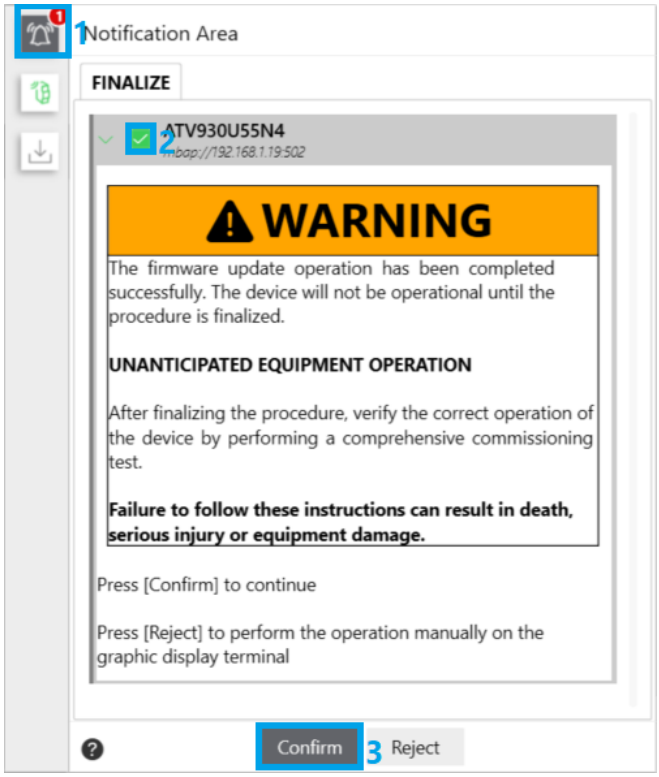
| Step | Action |
|---|---|
| 1 | Select **Manual** from **Discovery** drop-down menu (to prevent the cyclic data change effect between **DPWS** and **Modbus TCP** scanner. |
| 2 | Click **Add** ⊕ Add. |
| 3 | Select the **Commercial Reference** of your drive.<br>**NOTE:** Add the drive manually using **Modbus serial line** scanner, select **ATV*****, not **ATV*** (modernized)**. |
| 4 | Select **MODBUS (SL)** for **Connection**. |
| 5 | According to the laptop port you used to physically connect your drive, update the port settings (**Serial Port**, **Parity**, **Baud Rate**, **Stop Bits**, and **Decode**) |
| 6 | Click **Add Device**.<br>  |

<table>
<tr><th>step</th><th>Action</th></tr>
<tr><td></td><td>NOTE: Modbus SL connection offers limited information, compared to DPWS. Consequently, data such as the Serial Number and the Mode are not retrieved from the devices.</td></tr>
<tr><td>03</td><td>Login to the drive
<table>
<tr><th>Step</th><th>Action</th></tr>
<tr><td>1</td><td>Click Set credentials icon</td></tr>
<tr><td>2</td><td>Type the credentials
<ul>
<li>For Device User Name, type <code>ADMIN</code></li>
<li>For Device password, type the drive embedded Ethernet credentials.</li>
</ul>


Where to find the default password?<br>If the password has not been modified via SoMove or Webserver, the drive default embedded Ethernet credentials can be used, and is available from the Graphic Display Terminal (VW3A1111) :
<ul>
<li>If your drive is physically connected to the embedded Ethernet port: [Main Menu] > [Communication] COM > [Comm parameters] CMP > [Embd Eth Config] ETE > [User authentication] SECE > [Default Pwd Eth] WDPE.</li>
<li>If your drive is physically connected to the Ethernet option module port: [Main Menu] > [Communication] COM > [Comm parameters] CMP > [Opt Eth Config] ETO > [User authentication] SECO > [Default Pwd Eth Opt] WDPO.</li>
</ul>
How to reset the password?<br>If the password has been modified but you don’t know the new credentials, the drive default embedded Ethernet credentials can be reset from the Graphic Display Terminal (VW3A1111) :
<ul>
<li>If your drive is physically connected to the embedded Ethernet port: [Main Menu] > [Communication] COM > [Comm parameters] CMP > [Embd Eth Config] ETE > [User authentication] SECE > [Reset Eth Embd Pwd] RWPE > [Yes] Yes.</li>
<li>If your drive is physically connected to the Ethernet option module port: [Main Menu] > [Communication] COM > [Comm parameters] CMP > [Opt Eth Config] ETO > [User authentication] SECO > [Reset Eth Opt Pwd] RWPO > [Yes] Yes.<br>NOTE: if you add the drive manually using Modbus serial line scanner, you can login using Anonymous Authentification Type (Credentials are not needed).</li>
</ul>
</td></tr>
<tr><td>3</td><td>Click Save and Connect.</td></tr>
</table>
NOTE: If the security status is Disabled you can use the Anonymous Authentication Type to login.</td></tr>
<tr><td>04</td><td>Select the firmware package
<ol>
<li>Click Update Center icon .</li>
<li>Click Firmware.</li>
<li>Select the check boxes of the devices that you want to update.</li>
<li>Select the correct firmware package.</li>
<li>Click Save.</li>
</ol>
</td></tr>
</table>

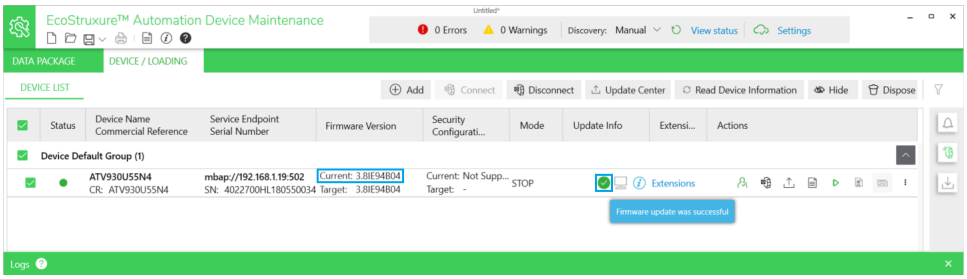
| step | Action |
|---|---|
| |  |
| 05 | Start the firmware update<br>1. Select the device that you want to update.<br>2. Click **Update**.<br>  <br>3. Click **Next** > **Next** > **Next** > **Confirm**. |
| 06 | Transfer the firmware<br>When the firmware update is started, you will receive a notification in the **Notification Area**.<br>1. Click  icon to open the **Notification Area**.<br>2. Select the message by activating the check box.<br>3. Click **Confirm**.<br>  |

| step | Action |
|---|---|
| 07 | Apply the firmware<br><br>When the firmware is transferred, you will receive a notification in the **Notification Area**.<br><br>1. Click icon to open the **Notification Area**.<br>2. Select the message by activating the check box.<br>3. Click **Confirm**.<br><br>  |
| 08 | Finalize the firmware<br><br>When the firmware is applied, you will receive a notification in the **Notification Area**.<br><br>1. Click icon to open the **Notification Area**.<br>2. Select the message by activating the check box.<br>3. Click **Confirm**. |

| step | Action |
|---|---|
| |  |
| 09 | When the firmware is finalized<br>1. Press **OK** on the Graphic Display Terminal (VW3A1111).<br>2. Restart the drive. |

**Result:**

When the firmware update is complete, the current firmware version is updated and the update info shows the icon ✔ indicating that the firmware update was successful.

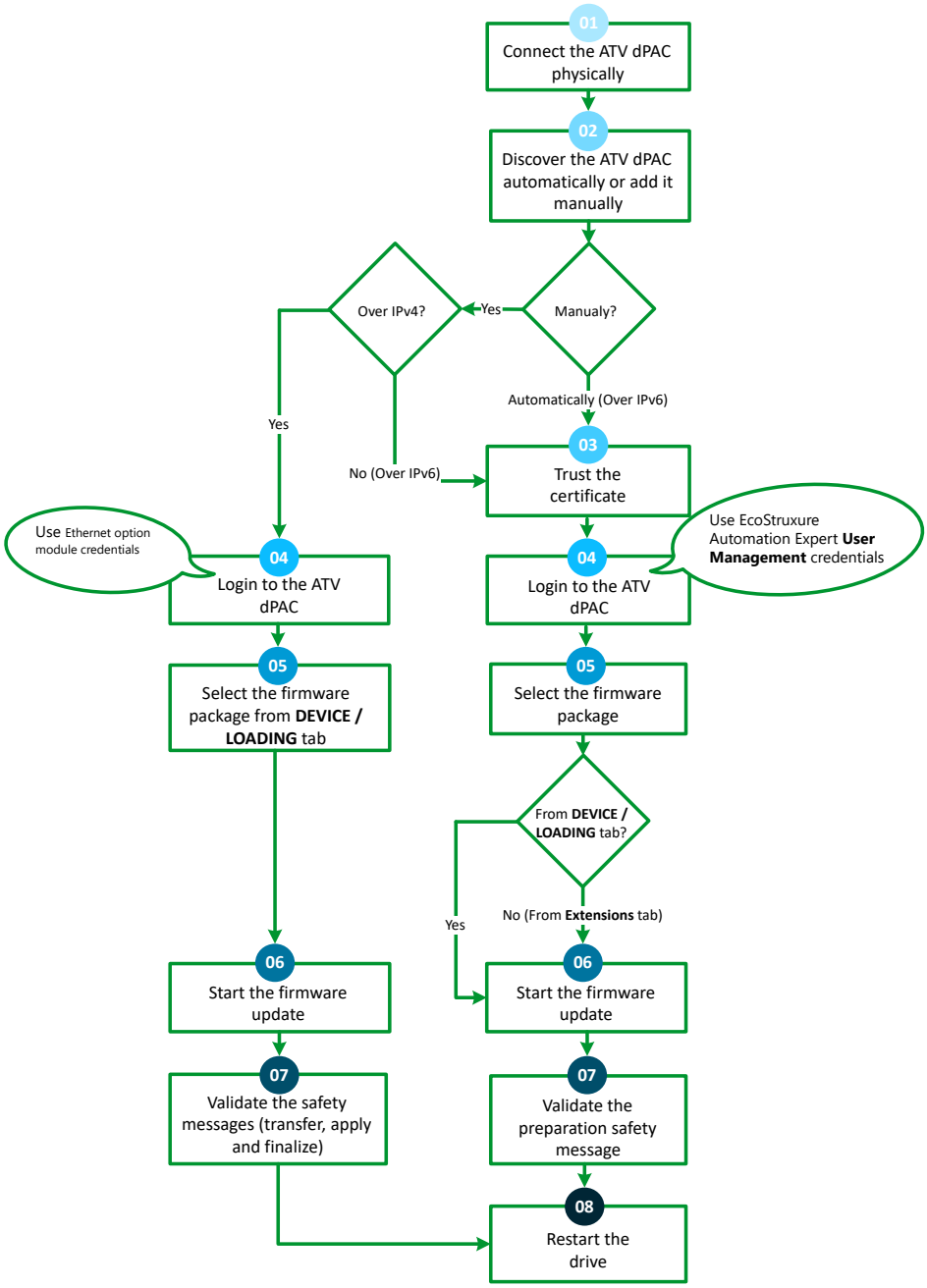



**NOTE:** Refer to the EcoStruxure Automation Device Maintenance User Manual (JYT50472) for more information.

**NOTE:** User access levels (with different authorizations) are defined for the application. User access level 3 is required in order to perform firmware updates.

## Step 3: Update the ATV dPAC firmware

Use the following instructions to update the drive firmware with EcoStruxure Automation Device Maintenance.


01
Connect the ATV dPAC physically
02
Discover the ATV dPAC automatically or add it manually
Manualy?
Yes
Over IPv4?
Yes
No (Over IPv6)
Automatically (Over IPv6)
03
Trust the certificate
Use Ethernet option module credentials
04
Login to the ATV dPAC
Use EcoStruxure Automation Expert **User Management** credentials
04
Login to the ATV dPAC
05
Select the firmware package from **DEVICE / LOADING** tab
05
Select the firmware package
From **DEVICE / LOADING** tab?
Yes
No (From **Extensions** tab)
06
Start the firmware update
06
Start the firmware update
07
Validate the safety messages (transfer, apply and finalize)
07
Validate the preparation safety message
08
Restart the drive

Refer to the following table to decide which scanner to use:

| Connection type | MODBUS (TCP) scanner (mbap protocol and *.fwp file) | DPWS scanner (https protocol and*.sedp file) | |
|---|---|---|---|
| | | From DEVICE/ LOADING tab (*_ATVhost.sedp file) | From EXTENSIONS tab (*_Extension. sedp file) |
| **From 20.2 to 21.1** | Yes | N/A(1) | N/A(2) |
| **From 21.1 to 21.2** | Yes | N/A(1) | N/A(2) |
| **From 21.2 to 22.0** | Yes | Yes(3) | N/A(2) |
| **From 21.2 to 22.1** | Yes | Yes(3) | Yes(3) |
| **From 21.2 to 23.0** | Yes | Yes(3) | Yes(3) |
| **From 22.0 to 21.2** | Yes | N/A(1) | N/A(2) |
| **From 22.0 to 22.1** | Yes | Yes(3) | Yes(3) |
| **From 22.0 to 23.0** | Yes | Yes(3) | Yes |
| **From 22.1 to 21.2** | Yes | N/A(1) | N/A(2) |
| **From 22.1 to 22.0** | Yes | Yes(3) | N/A(2) |
| **From 22.1 to 23.0** | Yes | Yes | Yes |
| **From 23.0 to 21.2** | Yes | N/A(1) | N/A(2) |
| **From 23.0 to 22.0** | Yes | Yes(3) | N/A(2) |
| **From 23.0 to 22.1** | Yes | Yes(3) | Yes(3) |

(1): *_ATVhost.sedp file does not exist for this version.

(2): *_Extension.sedp file does not exist for this version.

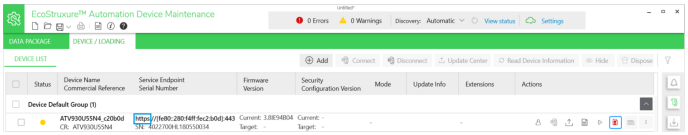
(3): An error may occur after the firmware update is complete, although, the firmware update is successful.

**NOTE:**

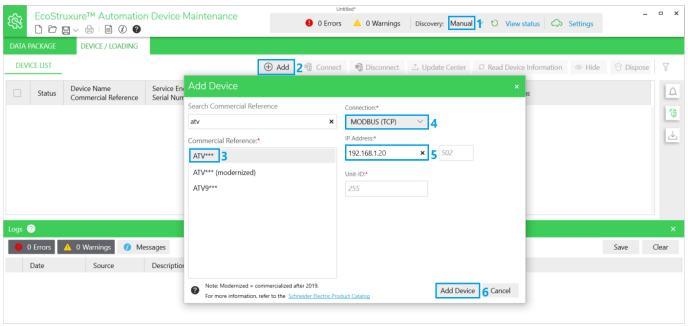
- You need to update the firmware of ATV dPAC after updating the firmware of the drive with the appropriate firmware version.
- The following procedure is used with EcoStruxure Automation Device Maintenance 3.2, thus, it can be used to update any firmware version between 21.2 and 23.0

| Step | Action |
|---|---|
| 01 | Connect the ATV dPAC physically<br><br>Connect the Ethernet cable between the ATV dPAC port and the computer where EcoStruxure Automation Device Maintenance is running, then turn on the drive if it is not already on.<br><br>  |
| 02 | Discover the ATV dPAC automatically or add it manually |

| Step | Action |
|---|---|
| | • Discover the drive automatically |

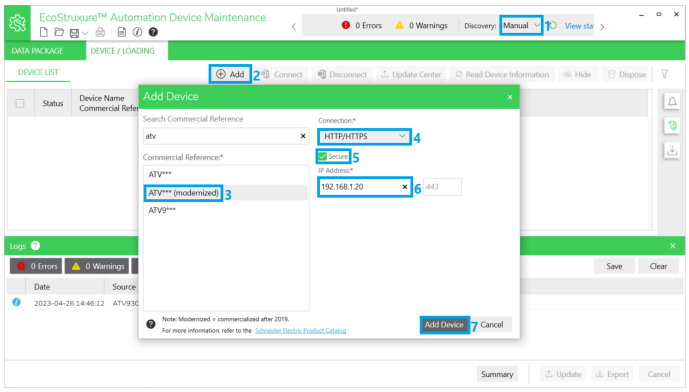
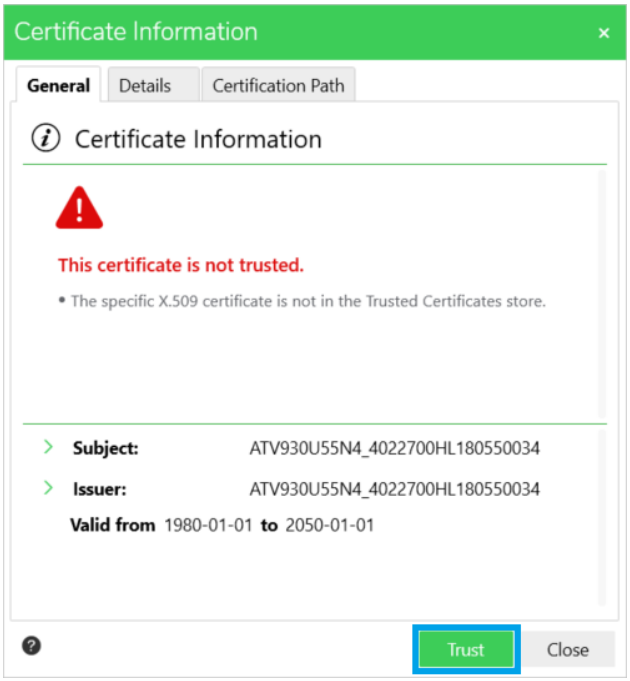
| Step | Action |
|---|---|
| 1 | Select Automatic from **Discovery** drop-down menu to perform automatic discovery.<br>  |
| 2 | **Result:** The ATV dPAC is added automatically using **DPWS** scanner (**https**-IPv6) in **DEVICE / LOADING** tab.<br>  <br>**NOTE:** Some firewall software may block the discovery. If you are unable to discover the device, disable firewall or consult your system administrator. |

• Add the ATV dPAC manually using **Modbus TCP** scanner (**mbap**-IPv4)

| Step | Action |
|---|---|
| 1 | Select **Manual** from **Discovery** drop-down menu. |
| 2 | Click **Add**  in the **DEVICE / LOADING** tab to add a new device. |
| 3 | Select the **Commercial Reference** of the drive hosting your ATV dPAC.<br>**NOTE:** To discover the ATV dPAC manually using **Modbus TCP** scanner (**mbap**-IPv4), select **ATV*****, not **ATV*** (modernized)**. |
| 4 | Select **MODBUS (TCP)** for **Connection**. |
| 5 | Type the **IP Address** of your ATV dPAC. |
| 6 | Click **Add Device**.<br>The figure below shows all the steps:<br>  |

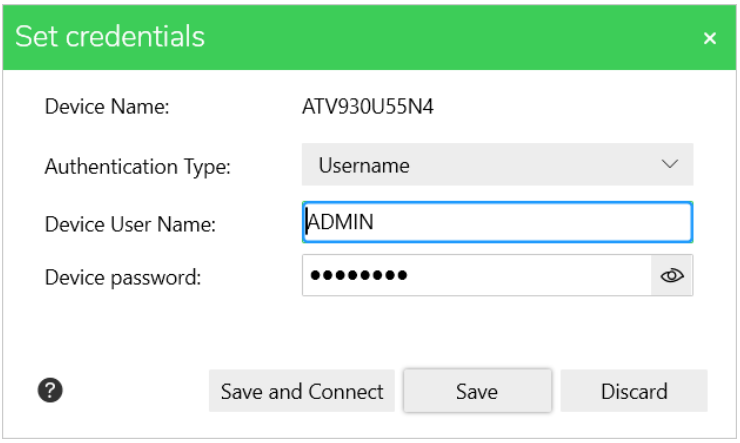
• Discover the ATV dPAC manually using **DPWS** scanner (**https**-IPv6)

| Step | Action |
|---|---|
| 1 | Select **Manual** from **Discovery** drop-down menu. |
| 2 | Click **Add**  in the **DEVICE / LOADING** tab to add a new device. |
| 3 | Select the **Commercial Reference** of the drive hosting your ATV dPAC.<br>**NOTE:** To discover the ATV dPAC manually using **DPWS** scanner (**https**-IPv6), select **ATV*** (modernized)**, not **ATV*****. |
| 4 | Select **HTTP/HTTPS** for **Connection**. |
| 5 | Activate the check box **Secure**. |
| 6 | Type the **IP Address** of your ATV dPAC. |
| 7 | Click **Add Device**. |

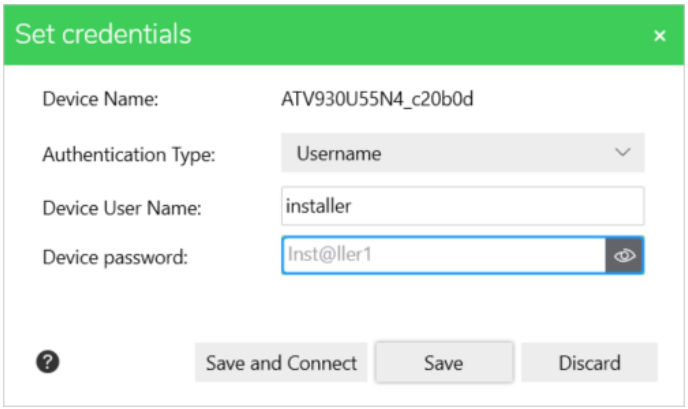
| Step | Action |
|---|---|
| | The figure below shows all the steps:<br>  |
| 03 | **NOTE:** Follow this step only if you discover your ATV dPAC using **DPWS** scanner (**https**-IPv6).<br>1. Click **Device certificate** icon.<br>2. Click **Trust**.<br>  |
| 04 | Login to the ATV dPAC |

| Step | Action |
|---|---|

## Login the ATV dPAC over Modbus TCP scanner (mbap-IPv4) discovery

| Step | Action |
|---|---|
| 1 | Click **Set credentials** icon |
| 2 | Type the credentials<br>For **Device User Name**, type `ADMIN`<br>For **Device password**, type the Ethernet option module credentials.<br>  <br>**NOTE:** :<br>• If the password is not modified via SoMove or Webserver, the default Ethernet option module credentials can be used, and are available from the Graphic Display Terminal (VW3A1111) in: **[Main Menu] > [Communication] COM > [Comm parameters] CMP > [Opt Eth Config] ETO > [User authentication] SECO > [Default Pwd Eth Opt] WDPO**<br>• If the password is modified but you don't know the new credentials, the drive Ethernet option module credentials can be reset from the Graphic Display Terminal (VW3A1111) in: **[Main Menu] > [Communication] COM > [Comm parameters] CMP > [Opt Eth Config] ETO > [User authentication] SECO > [Reset Eth Opt Pwd] RWPO > [Yes] Yes** |
| 3 | Click **Save and Connect**. |

## Login the ATV dPAC over DPWS scanner (https-IPv6) discovery

| Step | Action |
|---|---|
| 1 | Click **Set credentials** icon |
| 2 | Type the credentials<br>• **Case 1:** The security is not Configured (New user credentials).<br>◦ For **Device User Name**, type `installer`.<br>◦ For **Device password**, type `Inst@ller1`.<br>  |

| Step | Action |
|---|---|
| | **Login the ATV dPAC over DPWS scanner (https-IPv6) discovery (Continued)** |

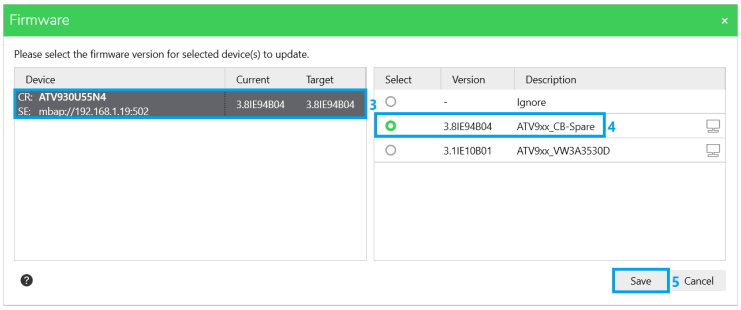
| Step | Action |
|---|---|
| | • **Case 2:** The security is configured: use EcoStruxure Automation Expert **User Management** credentials.<br>**NOTE:** If the security is configured but you don't know EcoStruxure Automation Expert **User Management** credentials, the **User Management** credentials can be reset, refer to the chapter Local reset of the ATV dPAC security, page 69 for more information.<br>**NOTE:** For firmware version 21.1 (3.1IE04_B03) or earlier, use EcoStruxure Automation Device Maintenance webserver credentials, available in the Graphic Display Terminal (VW3A1111) if the security is enabled, or Anonymous login if the security is disabled |
| 3 | Click **Save and Connect**. |

05

Select the firmware package

**Method 1:** From **DEVICE / LOADING** tab:

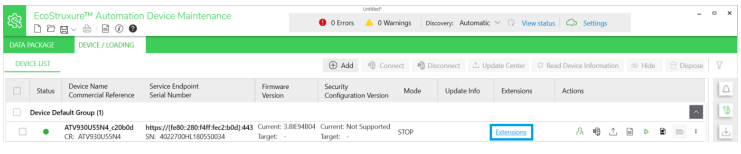
| Step | Action |
|---|---|
| 1 | Click **Update Center** icon . |
| 2 | Click **Firmware**. |
| 3 | Select the check boxes of the devices that you want to update. |
| 4 | Select the appropriate firmware package. |
| 5 | Click **Save**. |

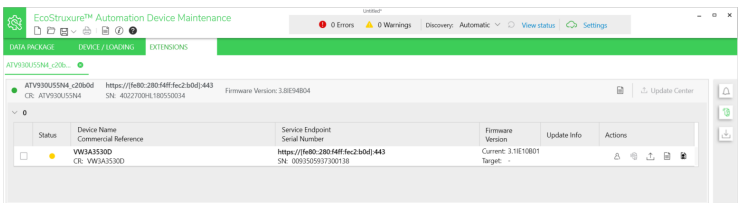



**Method 2:** From **EXTENSIONS** tab:

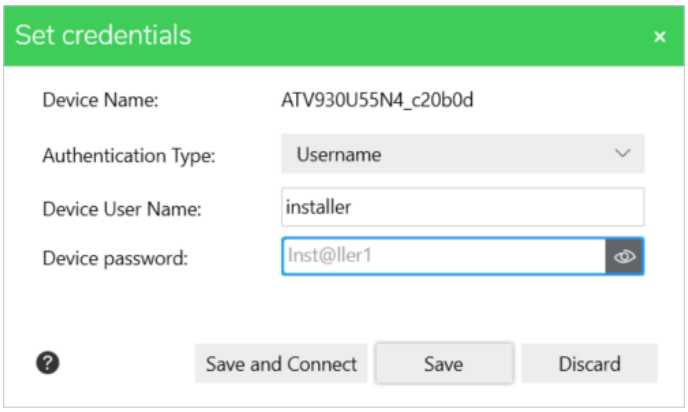
**NOTE:** This method can only be used if you are using **DPWS** scanner (https-IPv6).

| Step | Action |
|---|---|
| 1 | Click on **Extensions** from **DEVICE / LOADING** tab to open **EXTENSIONS** tab. |
| 2 | Click on chevron (angle bracket) symbol 0 to open the device.<br>**Result:** |
| 3 | Login to the ATV dPAC<br>1. Click **Set credentials** icon |



| Step | Action |
|---|---|
| | |

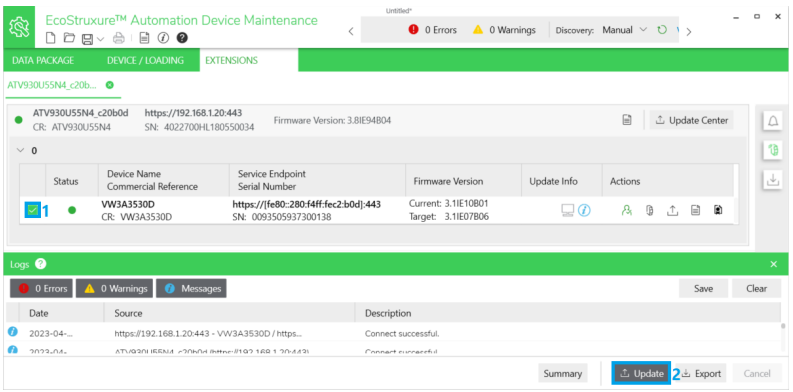
| Step | Action |
|---|---|
| | 2. Type the credentials<br>**Case 1:** The security is not Configured (New user credentials).<br>• For **Device User Name**, type `installer`.<br>• For **Device password**, type `Inst@ller1`.<br>  <br>**Case 2:** The security is configured: use EcoStruxure Automation Expert **User Management** credentials.<br>**NOTE:** If the security is configured but you don't know EcoStruxure Automation Expert **User Management** credentials, the **User Management** credentials can be reset, refer to the chapter Local reset of the ATV dPAC security for more information.<br>**NOTE:** For firmware version 21.1 (3.1IE04_B03) or earlier, use EcoStruxure Automation Device Maintenance webserver credentials, available in the Graphic Display Terminal (VW3A1111) if the security is enabled, or Anonymous login if the security is disabled<br>3. Click **Save and Connect**. |
| 4 | Click **Update Center** icon . |
| 5 | Click **Firmware**. |
| 6 | Select the check boxes of the devices that you want to update. |
| 7 | Select the appropriate firmware package. |
| 8 | Click **Save**. |

**06**

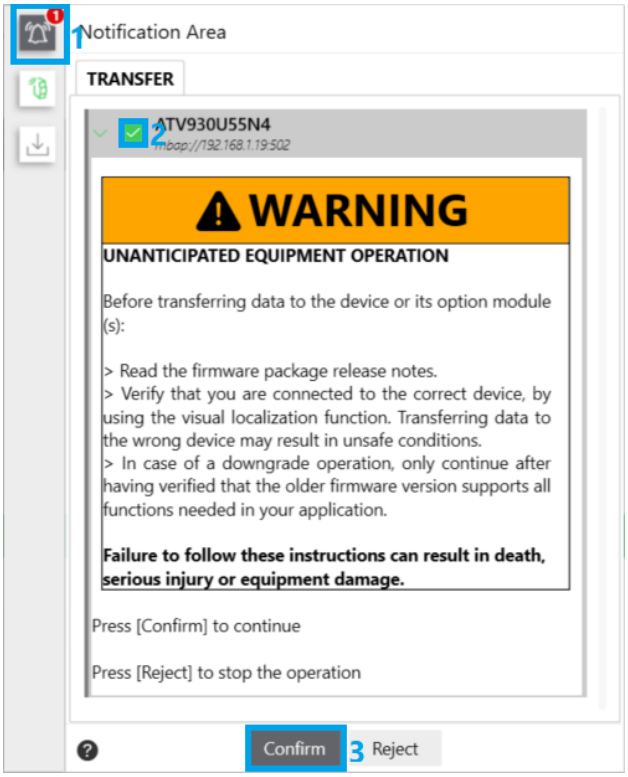
Start the firmware update

**NOTE:** Whether you selected the firmware package from **DEVICE / LOADING** tab or **EXTENSIONS** tab, follow these instructions:

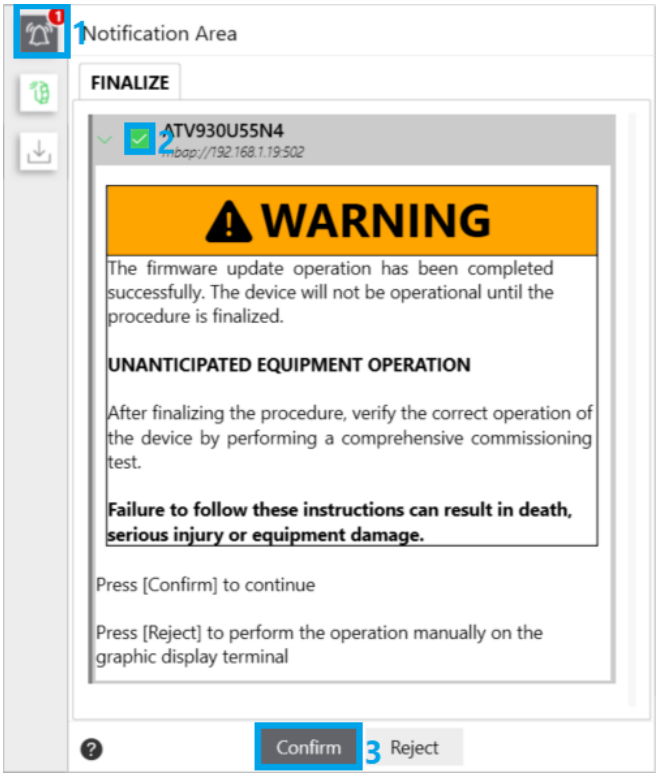
1. Select the device you want to update by checking the box.
2. Select update.

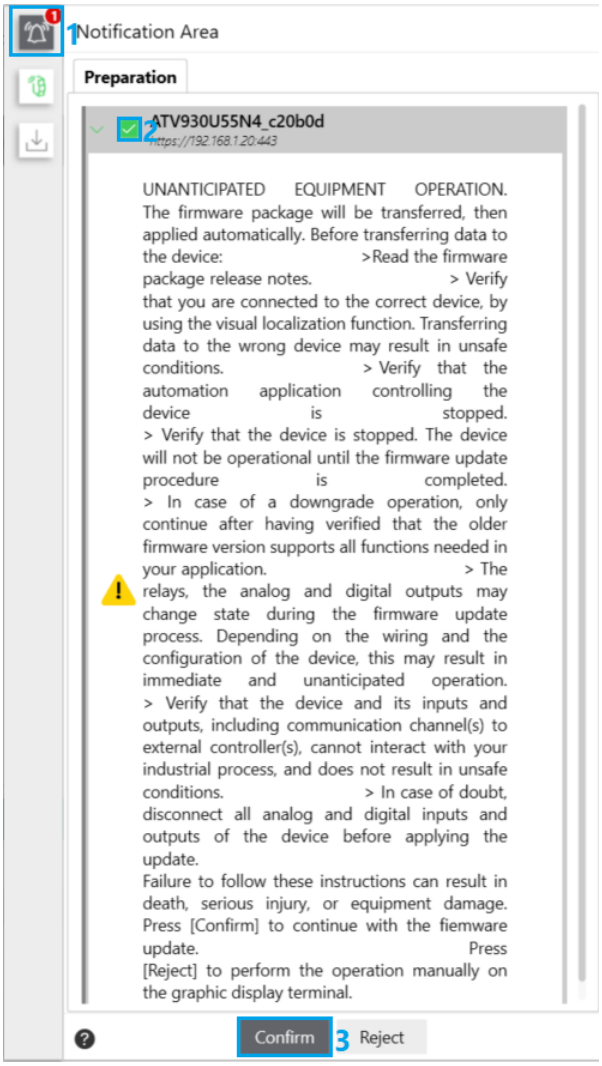



3. Click **Next > Next > Next > Confirm**.

| Step | Action |
|---|---|
| 07 | 1. Transfer the firmware<br>When the firmware update is started, you will receive a notification in the **Notification Area**.<br>a. Click icon to open the **Notification Area**.<br>b. Select the message by activating the check box.<br>c. Click **Confirm**.<br>  <br><br>2. Apply the firmware<br>When the firmware is transferred, you will receive a notification in the **Notification Area**.<br>a. Click icon to open the **Notification Area**.<br>b. Select the message by activating the check box.<br>c. Click **Confirm**. |

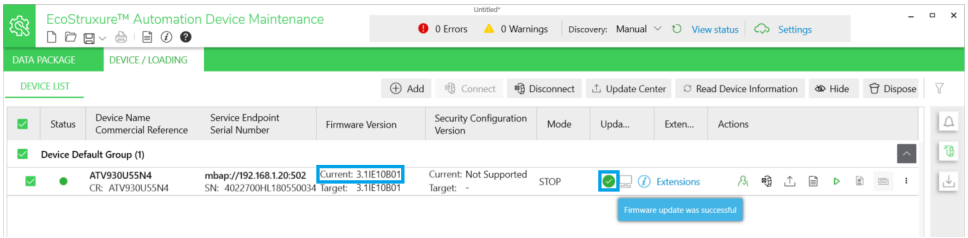
| Step | Action |
|---|---|
| |  <br>3. When the firmware is applied, you will receive a notification in the **Notification Area**.<br>a. Click icon to open the **Notification Area**.<br>b. Select the message by activating the check box.<br>c. Click **Confirm**. |

| Step | Action |
|---|---|
| |  <br>**NOTE:** If you update the firmware over **DPWS** scanner (https-IPv6), using sdep file you will receive only 1 notification (preparation) in the **Notification Area** instead of 3 notifications (Transfer, apply and finalize) if you updating over **Modbus TCP** scanner (mbap-IPv4) using mbap file. follow these instructions if you are updating over **DPWS** scanner: |

| Step | Action |
|---|---|
| | 1. Click icon to open the **Notification Area**.<br>2. Select the message by activating the check box.<br>3. Click **Confirm**.<br>  |
| 08 | When the firmware is finalized<br>1. Press **OK** on the Graphic Display Terminal (VW3A1111).<br>2. Restart the drive. |

**Result:**

When the firmware update is complete, the current firmware version is updated and the update info shows the icon ✔ indicating that the firmware update was successful.

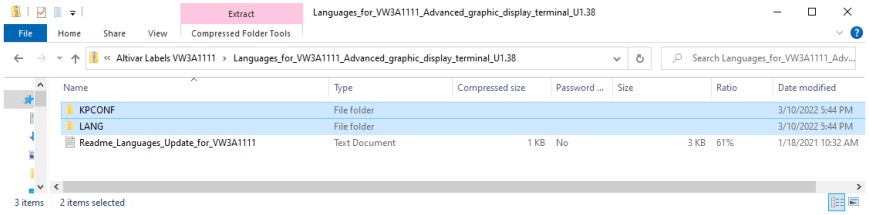


# Step 4: Update the labels and languages of the Graphic Display Terminal (VW3A1111)

The Graphic Display Terminal (VW3A1111) labels and languages can be updated

**NOTE:** Labels and languages :

- Can be found using the **EcoStruxure Automation Expert software installer archive** It exists on the following location: **EcoStruxure Automation Expert software installer archive > Firmware > Prod > SEDP_ATVD_*.zip > SEDP_ATVD_* > Altivar Labels VW3A1111 > Languages_for_VW3A1111_Advanced_graphic_display_terminal_*.zip**




- The latest version can be found here: Languages_for_VW3A1111_Advanced_graphic_display_terminal

The following table describe the procedure to update the labels and languages of the Graphic Display Terminal (VW3A1111) :

| Step | Action |
|---|---|
| 1 | Download the latest version of the labels and languages of the Graphic Display Terminal (VW3A1111) |
| 2 | Save the downloaded file on your computer |
| 3 | Unzip the file and follow the Readme file instructions |

**NOTE:** To transfer the labels and languages of the Graphic Display Terminal (VW3A1111), you need to connect the Graphic Display Terminal (VW3A1111) to your laptop using the following cables:

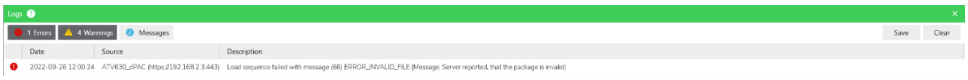
- Any USB plug-type A connector to USB plug-type mini B connector.
- BMXXCAUSBH018 cable.

# Troubleshooting during the ATV dPAC Firmware Update

## Abstract

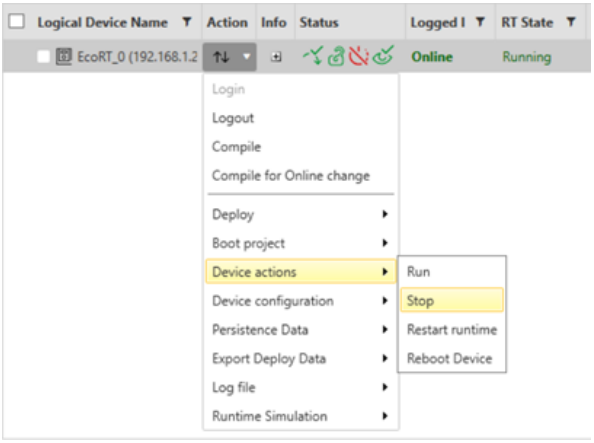
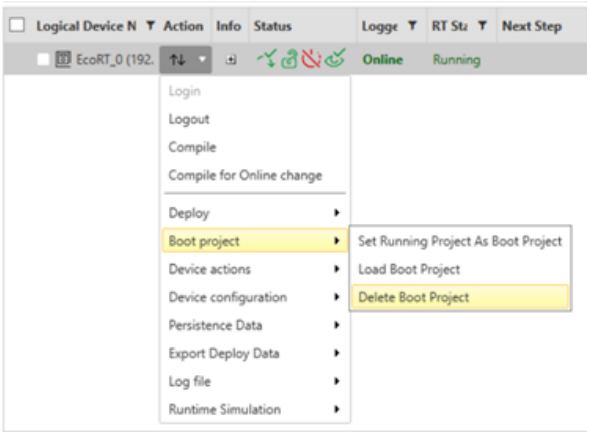
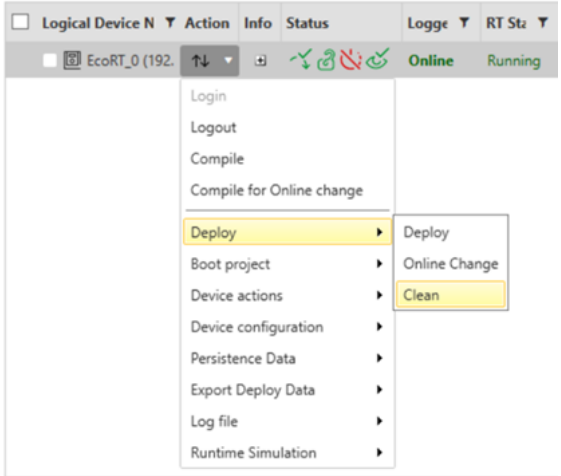
To allow a reliable firmware update procedure, stopping or cleaning the EcoRT application could be needed in the ATV dPAC, to free-up enough memory.

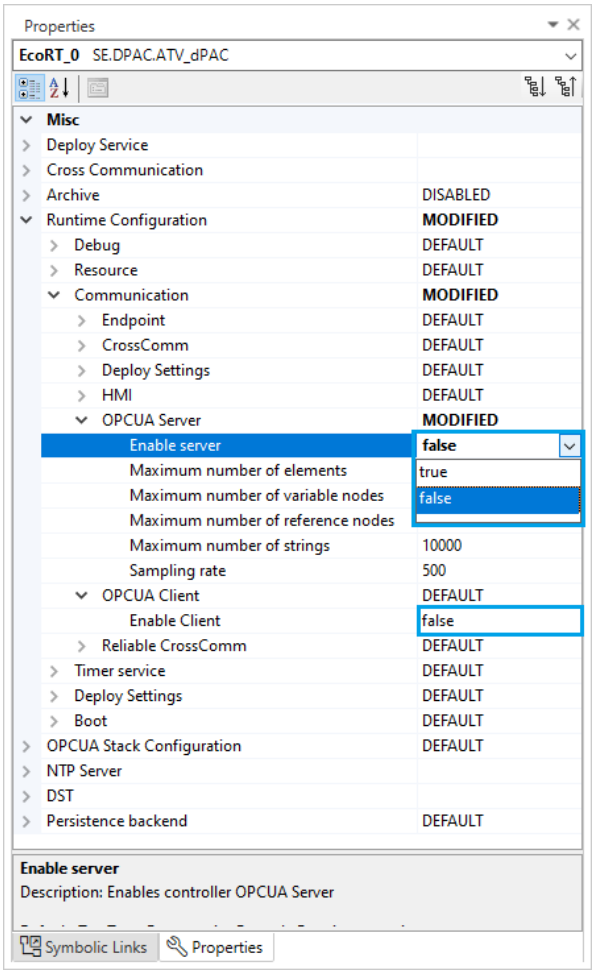
The image below illustrates the displayed error, when the firmware update can’t be achieved due to a lack of memory:

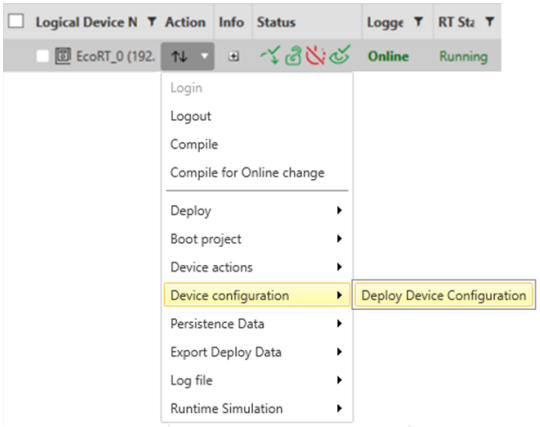
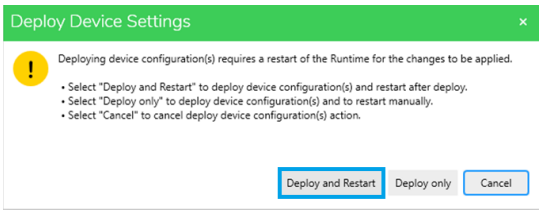



## Description

The following table describes the steps to solve the lack of memory error when updating the firmware of the ATV dPAC:

| Step | Description | Action |
|---|---|---|
| 1 | Stop the application<br>**NOTE:** The device should not operate until the firmware update is completed. | Open the Deploy and Diagnostic Editor in EcoStruxure Automation Expert → click on Action → select Device actions → select Stop<br>  |
| 2 | Delete the Boot Project | Open the Deploy and Diagnostic Editor in EcoStruxure Automation Expert → click on Action → select Boot project→ select Delete Boot Project<br>  |
| 3 | Clean the state of the ATV dPAC | Open the Deploy and Diagnostic Editor in EcoStruxure Automation Expert → click on Action → select Deploy → select Clean<br>  |
| 4 | Verify that:<br>• the device<br>• its inputs<br>• its outputs<br>• the communication channels to external controllers | **NOTE:** In case of doubt, disconnect all analog and digital inputs and outputs from the device before applying the firmware update. |

| Step | Description | Action |
|---|---|---|
| | cannot interfere with your industrial process, and does not result in unsafe conditions. | |
| 5 | Disable the OPC UA Server and Client, if the are already enbaled.: | Open the system tab in EcoStruxure Automation Expert → click on Logical Devices→ select the device to display its properties → display the Runtime Configuration options → Disable OPC UA server and Client if the are already enbaled, as mentioned in the following image:<br>  |

| Step | Description | Action |
|---|---|---|
| 6 | Deploy the Device configuration and Restart | Open the Deploy and Diagnostic Editor → click on Action → select Device actions → select Stop<br>1. Open the Deploy and Diagnostic Editor → click on Action → select Device configuration→ select Deploy Device Configuration<br>  <br><br>2. Select Deploy and Restart<br>  <br> |

# Local reset of the ATV dPAC security

## Overview

If the device password has been forgotten, the user can reset the security of the ATV dPAC, using the drive's Graphic Display Terminal (VW3A1111).

## Prerequisites

- Update the firmware package of:
  - The Drive (Refer to the firmware update with EcoStruxure Automation Device Maintenance chapter for more details on this step).
  - The ATV dPAC (Refer to the firmware update with EcoStruxure Automation Device Maintenance chapter for more details on this step).
- Update the labels and languages of the Graphic Display Terminal (VW3A1111) (Refer to the firmware update with EcoStruxure Automation Device Maintenance chapter for more details on this step).

  **NOTE:** The table below shows the firmware versions that allows this feature (Local reset of the ATV dPAC security).

| Device | ATV6xx | ATV9xx | ATV340 | ATV dPAC |
|---|---|---|---|---|
| Firmware Version greater than | V3.7IE94_B04 | V3.8IE94_B04 | V3.6IE94_B04 | V3.1IE09B01-22.1.23006.00 |

## Procedure

1. **Local reset the security on the Graphic Display Terminal (VW3A1111)** by following these steps: **[Main menu] > [Communication] > [Comm parameters] > [dPAC config] > set [dPAC Security Reset] to Yes > click the OK button to accept the warning message**

   **NOTE:** While the application keeps running security is not yet reset.

   **NOTE:** you need to take the appropriate steps to stop the application, and power-down the drive.

   **⚠WARNING**

   **UNAUTHENTICATED ACCESS AND PROCESS OPERATION**

   Setting this parameter to YES, default credentials will allow access to the ATV dPAC, at the next device power-up.

   Do not set this parameter to YES if your machine or process is accessible to unauthorized personnel either directly or via a network.

   Power-cycle the device, and re-configure security to run the application.

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

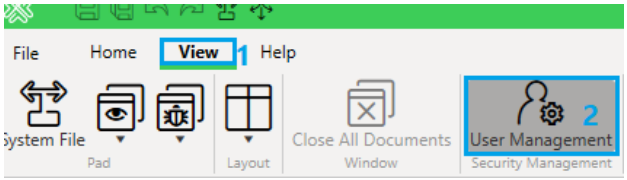
2. Restart the drive manually

3. **Reset the password of your existing solution in EcoStruxure Automation Expert:**

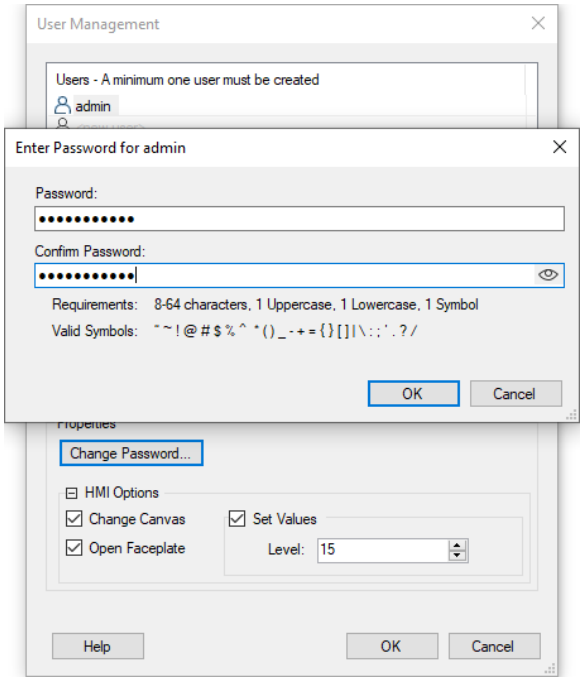
   **NOTE:** This step will only be needed if you have forgotten the password of your existing solution, if this is not the case create a new solution with your chosen credentials and skip this step.

   **NOTE:** The credentials of your solution will be the new credentials of your ATV dPAC module.

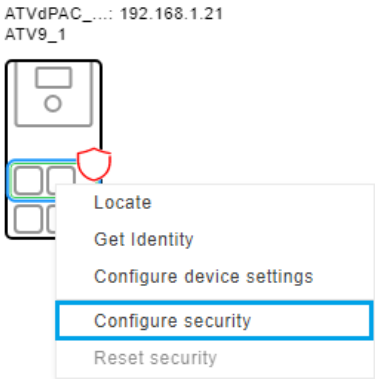
   a. **click on View window > click on User Management**




   b. **Click on the existing username > click on change password > set the new password of the solution**

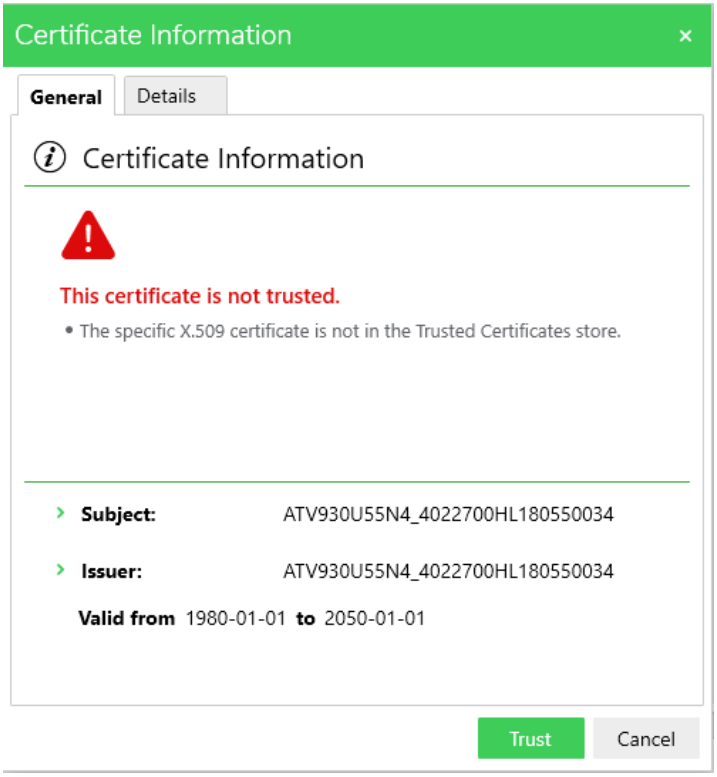


4. **Configure the security of your existing solution in EcoStruxure Automation Expert :**
   a. Open the system tab 
   b. **Select Physical devices > drag and drop your ATV Drive > Add an ATV dPAC communication card > set its IP Address**
   c. Start monitoring 
   d. Right click on the ATV dPAC device to configure the security

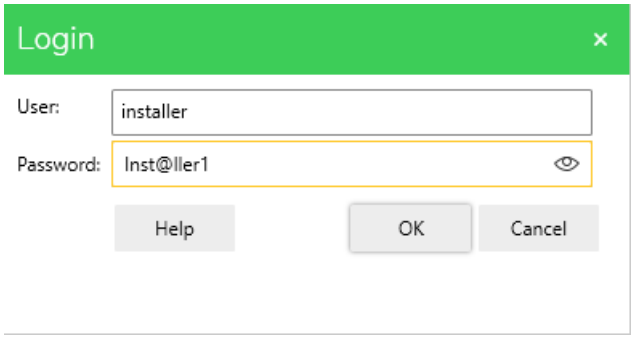



**NOTE:** Some firewall software may block device security configuration. If you are unable to configure the device, disable the firewall or consult your system administrator.

   e. Trust the certificate information.



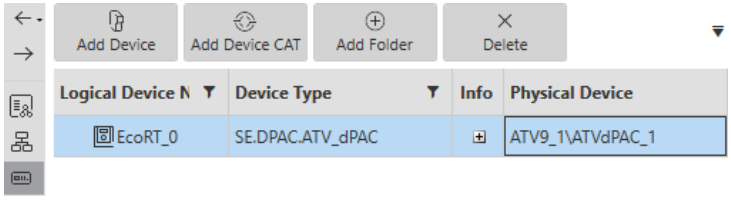

   f. Use the default credentials to login




**NOTE:** The default credentials are:

- User: `installer`
- Password: `Inst@ller1`

g. In logical devices, **Add a device that has SE.DPAC.ATV_dPAC as a type > Link it to your existing device**




5. Open the Deploy and Diagnostic editor, do the following:
   - Compile the solution
   - Login using the EcoStruxure Automation Expert user management credentials.
   - Deploy the solution
   - Run device actions

You can now start the local HMI using the EcoStruxure Automation Expert user management credentials.

**NOTE:** The credentials of your ATV dPAC module are the EcoStruxure Automation Expert user management credentials.

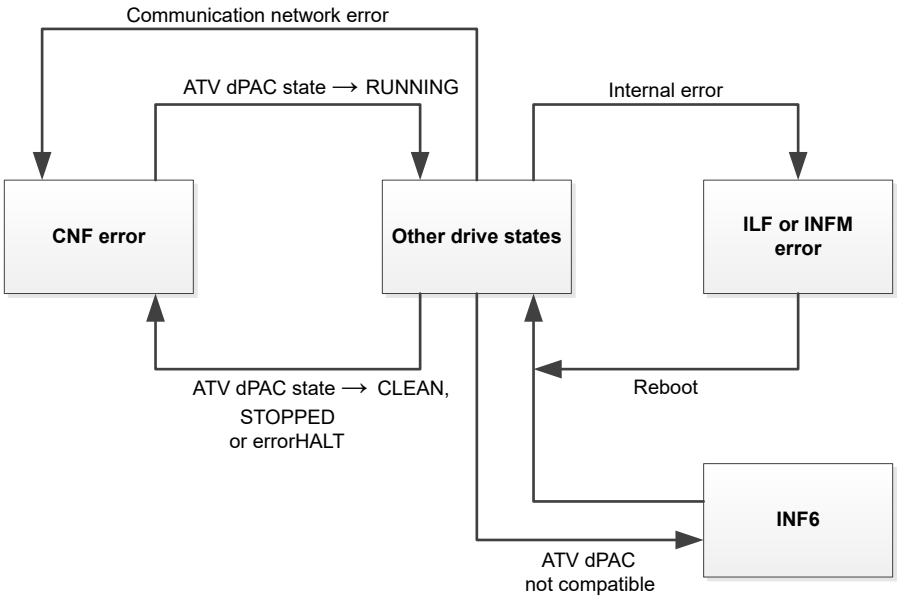
# Controller States and Behaviors

# ATV dPAC Specific Behavior

## Introduction

This chapter describes the specific behavior related to the ATV dPAC operating modes. The part common to EcoStruxure Automation Expert controller offer is described in the 'Operating Modes' chapter in the EcoStruxure™ Automation Expert Reference Guide.

## Operating States for ATV dPAC and Altivar Drives




The drive operating mode machine is different from the ATV dPAC operating mode machine. With ATV dPAC, the drive continues to follow its operating state machine.

- The drive remains in Operating State Fault **[Fieldbus Com Interrupt]** CnF if ATV dPAC is in the operating mode CLEAN, STOPPED or errorHALT. The drive switches from this state when ATV dPAC is in operating mode RUNNING.
- If a communication network error is detected by the ATV dPAC, ATV dPAC switches to errorHALT operating mode and **[Fieldbus Com Interrupt]** CnF is triggered by the drive.

  **NOTE:** The drive response to a **[Fieldbus Com Interrupt]** CnF error can be configured via the parameter **[Fieldbus Interrupt Resp]** CLL.
- If an internal error is detected, **[Internal Link Error]** ILF or **[Internal Error 22]** InF0is triggered by the drive depending on the error.
- In case of **[Internal Error 6]** InF6, the ATV dPAC is not supported by the firmware of the drive. Verify the version compatibility.

For more information on the drive errors, refer to the drive Programming Manual, page 15.

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.



NNZ13577.08