How To Manage Certificates on the Controller

User Guide

06/2019

EIO0000003897.00

www.schneider-electric.com

Schneider Electric

The information provided in this documentation contains general descriptions and/or technical characteristics of the performance of the products contained herein. This documentation is not intended as a substitute for and is not to be used for determining suitability or reliability of these products for specific user applications. It is the duty of any such user or integrator to perform the appropriate and complete risk analysis, evaluation and testing of the products with respect to the relevant specific application or use thereof. Neither Schneider Electric nor any of its affiliates or subsidiaries shall be responsible or liable for misuse of the information contained herein. If you have any suggestions for improvements or amendments or have found errors in this publication, please notify us.

You agree not to reproduce, other than for your own personal, noncommercial use, all or part of this document on any medium whatsoever without permission of Schneider Electric, given in writing. You also agree not to establish any hypertext links to this document or its content. Schneider Electric does not grant any right or license for the personal and noncommercial use of the document or its content, except for a non-exclusive license to consult it on an "as is" basis, at your own risk. All other rights are reserved.

All pertinent state, regional, and local safety regulations must be observed when installing and using this product. For reasons of safety and to help ensure compliance with documented system data, only the manufacturer should perform repairs to components.

When devices are used for applications with technical safety requirements, the relevant instructions must be followed.

Failure to use Schneider Electric software or approved software with our hardware products may result in injury, harm, or improper operating results.

Failure to observe this information can result in injury or equipment damage.

Table of Contents

Safety Information

Important Information

NOTICE

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.

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.

About the Book

At a Glance

Document Scope

This document describes the steps for managing certificates which should be used for secured TCP communication at application level.

Validity Note

This document has been updated for the release of EcoStruxure™ Machine Expert V1.1.

Related Documents

Document title	Reference
Modicon M262 Logic/Motion Controller Hardware Guide	*EIO0000003659 (ENG)*; *EIO0000003660 (FRE)*; *EIO0000003661 (GER)*; *EIO0000003662 (SPA)*; *EIO0000003663 (ITA)*; *EIO0000003664 (CHS)*
EcoStruxure Machine Expert Programming Guide	*EIO0000002854 (ENG)*; *EIO0000002855 (FRE)*; *EIO0000002856 (GER)*; *EIO0000002858 (SPA)*; *EIO0000002857 (ITA)*; *EIO0000002859 (CHS)*

Product Related Information

⚠ WARNING

LOSS OF CONTROL

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

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

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

⚠ WARNING

UNINTENDED EQUIPMENT OPERATION

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

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

Terminology Derived from Standards

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

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

Among others, these standards include:

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

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

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

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

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

Applications Implementing Secured TCP Communication

Communication Libraries

EcoStruxure Machine Expert provides libraries that support secured communication using TLS (Transport Layer Security). They provide client and/or server functionality as indicated in the following table:

Library	Providing the functionality of:
TcpUdpCommunication	• TCP client • TCP server
HttpHandling	HTTP/HTTPS client
MqttHandling	MQTT / secured MQTT client
EmailHandling	• SMTP/SMTPS client • POP3/POP3S client

The clients or server can be configured to use TLS for encrypted communication.

Whether a connection using TLS is supported depends on the controller where the corresponding function block is used. Refer to the specific manual of your controller to verify if TCP communication using TLS is supported.

Certificates

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

Verification of Certificates

The EcoStruxure Machine Expert libraries that support secured connection using TLS provide the parameter `etCertVerifyMode` for selecting the mode of verification of the certificate which is sent by the communication partner during the TLS handshake.

The following modes are supported:

`etCertVerifyMode` Mode	Description
`TrustedOnly`	A certificate from the communication partner is required. The certificate must be classified as trusted.
`AllCertificates`	A certificate from the communication partner is required. Further verification on the certificate is not performed.
`NotVerified`	No certificate from the communication partner is required.

If the client or server is configured to verify the server certificate in mode `TrustedOnly`, it is required to manage the certificates on your controller in a manual manner. This can be performed using the editor **Security Screen** in EcoStruxure Machine Expert Logic Builder. The required steps are described in the following section.

NOTE: `TrustedOnly` is the only way to authenticate the communication partner.

Managing Certificates on the Controller

Overview

If the client or server is configured to verify the certificate of the communication partner in mode `TrustedOnly`, the corresponding certificate must be available on the controller and it must be declared as trusted. To achieve this, use the editor **Security Screen** in EcoStruxure Machine Expert Logic Builder to manage the certificates on your controller.

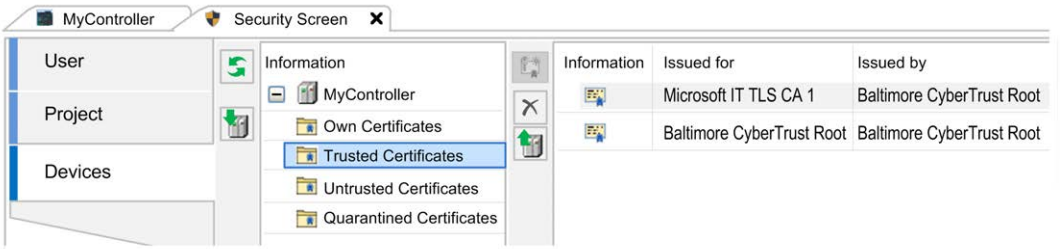
Security Screen Editor

The **Security Screen** editor is available in EcoStruxure Machine Expert Logic Builder via the **View → Security Screen** command. The **Devices** tab of the **Security Screen** editor provides access to the folders that are dedicated to managing certificates on the connected controller.

Click the  button to display the corresponding folders and their content for the certificate handling on the connected controller.

For example, the following categories are available for the Modicon M262 Logic/Motion Controller:

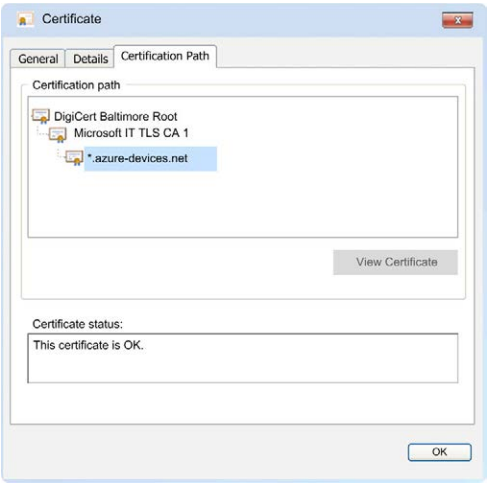
- **Own Certificates**: Certificates owned by the controller which are used for associated services it provides.
- **Trusted Certificates**: Certificates that have been created by a trusted certificate source.
- **Untrusted Certificates**: Certificates that you have declared as untrusted.
- **Quarantined Certificates**: Certificates that do not meet the criteria of the other categories.



Successful verification of a certificate in mode `TrustedOnly` is only possible if the corresponding certificate(s) are available in the folder **Trusted Certificates**.

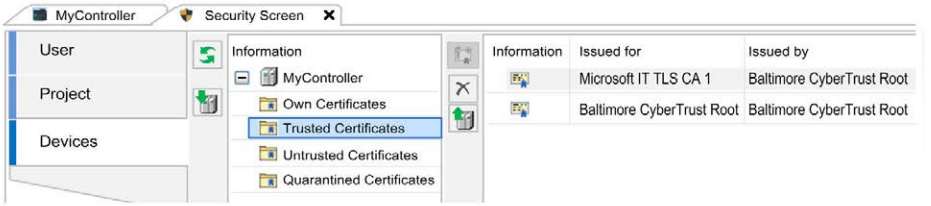
Declare a Certificate as Trusted

In order to declare certificates as trusted on your controller, perform the following steps:

Step	Action	Comment
1	Save the certificate of a device / software that you received from the manufacturer to your PC running EcoStruxure Machine Expert.	If you did not receive a certificate from the manufacturer of your device / software, you can obtain it by trying to establish a connection as described in the paragraph *Obtaining an Unknown Certificate* *(see page 17)*.
2	Double-click the certificate. **Result**: The **Certificate** dialog box opens.	–
3	Inspect the certificate carefully in the **General** tab and decide whether you want to declare it as trusted.	–
4	Select the **Certification Path** tab and verify whether there is only one entry. 	If there is only one entry in the **Certification Path** tab, then this is a self-signed certificate, as for example, for the Modicon M262 Logic/Motion Controller. You can skip the next two steps and proceed with step 7. If there is a tree structure in the **Certification Path** tab, then this certificate has been signed by a CA (Certificate Authority). In this case, perform the following steps for CA certificates.
5	If the certificate has been signed by a CA: Verify each certificate from the tree structure including the root CA certificate from the **Certification Path** tab.	–
6	For each CA certificate of the **Certification Path**, select the certificate and click the **View Certificate** button. **Result**: A new dialog box opens for the selected certificate.	–
7	Select the **Details** tab and click the **Copy to file...** button to save the certificate on the PC.	–
8	Download the saved certificate files to the **Trusted Certificates** folder of your controller.	Refer to the paragraph *Downloading Certificate(s) Declared as Trusted to the Controller* *(see page 16)*.

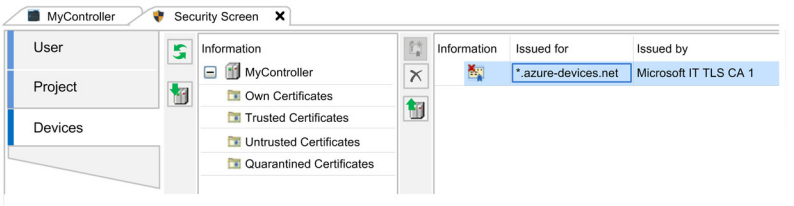
Downloading Certificate(s) to the Controller

To save certificates that you have declared as trusted to the folder **Trusted Certificates** on your controller, proceed as follows:

Step	Action
1	In EcoStruxure Machine Expert Logic Builder, execute the **Security Screen** editor from the **View** menu.
2	In the **Security Screen** editor, select the **Devices** tab.
3	Click the button **Refresh the list of available devices and their certificate stores**. **Result**: The display is updated according to the information received from the connected controller.
4	Select the folder **Trusted Certificates**, and click the **Download** button.
5	In the **Open** dialog box, navigate to the folder on your PC running EcoStruxure Machine Expert where you saved the certificate file(s).
6	Select the certificate file(s) and click the **Open** button. **Result**: The certificates are downloaded to the controller and are displayed on the right-hand side of the **Security Screen** editor as content of the folder **Trusted Certificates**. 

Obtaining an Unknown Certificate

If the certificate of a communication partner is not available and you cannot obtain it from the manufacturer or another source, proceed as follows:

Step	Action	Further information
1	Establish a secured connection with `etCertVerifyMod` set to `TrustedOnly` between the client and the server: ● If your application implements a client, connect to the server. ● If your application implements a server, open the server and accept the incoming connection from the client. **Results**: ● As the certificate that has been sent by the server or client is unknown, the connection cannot be established. ● The unknown certificate is stored in the folder **Quarantined Certificates** on your controller.	● If your controller application implements a client, the result `ConnectionFailed` may indicate that the certificate that has been received from the server is unknown. ● If your controller application implements a server, the result `TlsError` may indicate that the certificate that has been received from the client is unknown. **NOTE:** If the folder is empty, the communication partner may have not sent its certificate. Verify the configuration of the remote server or client in order to find out whether a certificate can be expected.
2	In EcoStruxure Machine Expert Logic Builder, open the **Security Screen** editor and click the button **Refresh the list of available devices and their certificate stores**.	–
3	Select the folder **Quarantined Certificates**.	–
4	Select the certificate from the list on the right-hand side of the **Security Screen** editor, and click the **Upload the selected certificate from the device and save it to your PC** button. 	
5	In the **Save as** dialog box, navigate to a folder on your PC running EcoStruxure Machine Expert where you want to save the certificate file(s) and click the **Save** button.	–
6	Verify the certificate(s) and decide if you want to declare them as trusted as described in the paragraph *How to Obtain Trusted Certificates (see page 15)*.	–
7	Download the certificate(s) declared as trusted to the controller *(see page 16)*.	–

Considerations When Using Certificates

Considerations

Consider the following when you use certificates for secured communications:

- Administration of certificates is required as they have a limited validity and therefore need to be updated in regular intervals. Consider this with respect to the life cycle of your machine or control.
- The controller clock is used to verify whether the certificate is still valid. Make sure that the controller clock is synchronized with UTC (Universal Time Coordinated) in regular intervals. To verify the controller clock, refer to the **Services** tab of your controller configuration.
- You can also declare certificates as untrusted by saving them to the folder **Untrusted Certificates** in the controller.