Modicon M580

BMENUA0100 OPC UA Embedded Module

Installation and Configuration Guide

Original instructions

06/2024

PHA83350.05

www.se.com

Legal Information

The information provided in this document contains general descriptions, technical characteristics and/or recommendations related to products/solutions.

This document is not intended as a substitute for a detailed study or operational and site-specific development or schematic plan. It is not to be used for determining suitability or reliability of the products/solutions for specific user applications. It is the duty of any such user to perform or have any professional expert of its choice (integrator, specifier or the like) perform the appropriate and comprehensive risk analysis, evaluation and testing of the products/solutions with respect to the relevant specific application or use thereof.

Schneider Electric reserves the right to make changes or updates with respect to or in the content of this document or the format thereof, at any time without notice.

To the extent permitted by applicable law, no responsibility or liability is assumed by Schneider Electric and its subsidiaries for any errors or omissions in the informational content of this document, as well as any non-intended use or misuse of the content thereof.

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.

Before You Begin

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

⚠WARNING

UNGUARDED EQUIPMENT

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

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

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

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

In some applications, such as packaging machinery, additional operator protection such as point-of-operation guarding must be provided. This is necessary if the operator's hands and

other parts of the body are free to enter the pinch points or other hazardous areas and serious injury can occur. Software products alone cannot protect an operator from injury. For this reason the software cannot be substituted for or take the place of point-of-operation protection.

Ensure that appropriate safeties and mechanical/electrical interlocks related to point-of-operation protection have been installed and are operational before placing the equipment into service. All interlocks and safeties related to point-of-operation protection must be coordinated with the related automation equipment and software programming.

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

Start-up and Test

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

⚠WARNING

EQUIPMENT OPERATION HAZARD

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

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

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

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

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

Before energizing equipment:

- Remove tools, meters, and debris from equipment.

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

Operation and Adjustments

The following precautions are from the NEMA Standards Publication ICS 7.1-1995:

(In case of divergence or contradiction between any translation and the English original, the original text in the English language will prevail.)

- 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 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

Document Scope

This manual describes the features and use of the M580 BMENUA0100 Ethernet communication module with embedded OPC UA server.

NOTE: The specific configuration settings contained in this guide are intended to be used for instructional purposes only. The settings required for your specific configuration may differ from the examples presented in this guide.

Validity Note

This document is valid for an M580 system when used with EcoStruxure™ Control Expert version 16.0 or any subsequent supporting version(s).

The characteristics of the products described in this document are intended to match the characteristics that are available on www.se.com. As part of our corporate strategy for constant improvement, we may revise the content over time to enhance clarity and accuracy. If you see a difference between the characteristics in this document and the characteristics on www.se.com, consider www.se.com to contain the latest information.

Related Documents

Title of documentation	Reference number
Modicon M580 Standalone, System Planning Guide for Frequently Used Architectures	HRB62666 (English), HRB65318 (French), HRB65319 (German), HRB65320 (Italian), HRB65321 (Spanish), HRB65322 (Chinese)
Modicon M580, System Planning Guide for Complex Topologies	NHA58892 (English), NHA58893 (French), NHA58894 (German), NHA58895 (Italian), NHA58896 (Spanish), NHA58897 (Chjnese)
Modicon M580 Hot Standby, System Planning Guide for Frequently Used Architectures	NHA58880 (English), NHA58881 (French), NHA58882 (German), NHA58883 (Italian), NHA58884 (Spanish), NHA58885 (Chinese)
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	EIO0000002726 (English), EIO0000002727 (French), EIO0000002728 (German), EIO0000002730 (Italian), EIO0000002729 (Spanish), EIO0000002731 (Chinese)

Title of documentation	Reference number
M580 BMENOS0300, Network Option Switch, Installation and Configuration Guide	NHA89117 (ENG) NHA89119 (FRE) NHA89120 (GER) NHA89121 (ITA) NHA89122 (SPA) NHA89123 (CHS)
Modicon M580, Hardware, Reference Manual	EIO0000001578 (English), EIO0000001579 (French), EIO0000001580 (German), EIO0000001582 (Italian), EIO0000001581 (Spanish), EIO0000001583 (Chinese)
Modicon M580, RIO Modules, Installation and Configuration Guide	EIO0000001584 (English), EIO0000001585 (French), EIO0000001586 (German), EIO0000001587 (Italian), EIO0000001588 (Spanish), EIO0000001589 (Chinese),
Modicon M580, Change Configuration on the Fly, User Guide	EIO0000001590 (English), EIO0000001591 (French), EIO0000001592 (German), EIO0000001594 (Italian), EIO0000001593 (Spanish), EIO0000001595 (Chinese)
Modicon X80, Discrete Input/Output Modules, User Manual	35012474 (English), 35012475 (German), 35012476 (French), 35012477 (Spanish), 35012478 (Italian), 35012479 (Chinese)
Modicon X80, BMXEHC0200 Counting Module, User Manual	35013355 (English), 35013356 (German), 35013357 (French), 35013358 (Spanish), 35013359 (Italian), 35013360 (Chinese)
Grounding and Electromagnetic Compatibility of PLC Systems, Basic Principles and Measures, User Manual	33002439 (ENG) 33002440 (FRE) 33002441 (GER) 33002442 (SPA) 33003702 (ITA) 33003703 (CHS)
EcoStruxure™ Control Expert, Program Languages and Structure, Reference Manual	35006144 (English), 35006145 (French), 35006146 (German), 35013361 (Italian), 35006147 (Spanish), 35013362 (Chinese)
EcoStruxure™ Control Expert, System Bits and Words, Reference Manual	EIO0000002135 (English), EIO0000002136 (French), EIO0000002137 (German), EIO0000002138 (Italian), EIO0000002139 (Spanish), EIO0000002140 (Chinese)
EcoStruxure™ Control Expert, Operating Modes	33003101 (English), 33003102 (French), 33003103 (German), 33003104 (Spanish), 33003696 (Italian), 33003697 (Chinese)
EcoStruxure™ Control Expert, Installation Manual	35014792 (English), 35014793 (French), 35014794 (German), 35014795 (Spanish), 35014796 (Italian), 35012191 (Chinese)

Title of documentation	Reference number
Web Designer for FactoryCast User Manual	35016149 (English), 35016150 (French), 35016151 (German), 35016152 (Italian), 35016153 (Spanish), 35016154 (Chinese)
Modicon Controllers Platform Cyber Security, Reference Manual	EIO0000001999 (ENG) EIO0000002001 (FRE) EIO0000002000 (GER) EIO0000002003 (SPA) EIO0000002002 (ITA) EIO0000002004 (CHS)

To find documents online, visit the Schneider Electric download center (www.se.com/ww/en/download/).

Product Related Information

⚠ 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

- Perform a Failure Mode and Effects Analysis (FMEA), or equivalent risk analysis, of your application, and apply preventive and detective controls before implementation.
- Provide a fallback state for undesired control events or sequences.
- Provide separate or redundant control paths wherever required.
- Supply appropriate parameters, particularly for limits.
- Review the implications of transmission delays and take actions to mitigate them.
- Review the implications of communication link interruptions and take actions to mitigate them.
- Provide independent paths for control functions (for example, emergency stop, over-limit conditions, and error conditions) according to your risk assessment, and applicable codes and regulations.
- Apply local accident prevention and safety regulations and guidelines.
- Test each implementation of a system for proper operation before placing it into service.

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

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

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

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

Terminology Derived from Standards

The technical terms, terminology, symbols and the corresponding descriptions in the information contained herein, 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 13849-1:2023	Safety of machinery: Safety related parts of control systems. General principles for design.
EN 61496-1:2020	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 62061:2021	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 61784-3:2021	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.

Trademarks

Windows is a registered trademark of Microsoft Corporation.

Information on Non-Inclusive or Insensitive Terminology

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

BMENUA0100 Module Characteristics

Introduction

This chapter describes the BMENUA0100 Ethernet communications module with embedded OPC UA server.

Module Features

Introduction

The Modicon BMENUA0100 OPC UA server module brings high performance OPC UA capabilities to Modicon M580 controller systems.

OPC UA is a secure and open communications platform for industrial communications, designed to be flexible and scalable from resource constrained IoT sensors in the field through to enterprise grade servers hosted in the data center or the cloud. Beyond connecting and moving data around, OPC UA defines a comprehensive information model for publishing and managing meta-information and system context to help simplify automation engineering and systems integration.

In realizing a communications standard for modern, connected industrial operations, OPC UA provides a common link between connected products in the field controllers, and enterprise applications and analytics. It is designed to be compatible with IT and security infrastructure such as firewalls, VPNs and proxies. OPC UA scales for both functional requirements and bandwidth.

Features

The BMENUA0100 module includes an OPC UA server and an embedded Ethernet switch. It is included in the Control Expert **Hardware Catalog** in the **Communication** module group.

The BMENUA0100 brings the following features to the Modicon M580 platform:

General:

- Direct and optimized access to Control Expert data dictionary for mapping between Control Expert and OPC UA variables, page 47.
- Support for Hot Standby configurations via OPC UA Redundancy, page 51.

- Compatibility with M580 Safety-related systems as a type 1 non-interfering module as defined by TÜV Rheinland.
- Seamless Ethernet backplane communications.
- DHCP/FDR client for downloading stored (non-cybersecurity) configuration settings.
- NTP time server, page 124 and client synchronization.
- Multiple diagnostic methods, including LEDs, page 131, DDT, page 135, OPC_UA variables and data items, page 147, Syslog, page 151, Modbus, page 155, SNMP, page 156, and secure web pages, page 157.
- Firmware Upgrade via the EcoStruxure™ Automation Device Maintenance Tool, page 166.
- Firmware integrity checking.
- Hardware secured storage.

Cybersecurity:

- Secure communications via HTTPS, OPC UA (optional), and IPsec (optional).
- Module-level OPC UA security, page 92 configurable via HTTPS.
- The ability to control inbound and outbound communication flow by enabling and disabling communication services, page 94.
- IPsec, page 99 based on a pre-shared key (PSK) for securing services such as SNMPv1, Modbus/TCP, Syslog, and NTPv4.

  NOTE: The BMENUA0100 supports main mode IPsec. An IPsec channel can be opened by either the BMENUA0100 server or a remote OPC UA client. On a PC client, IPsec is supported and validated on Windows 7, 10 and Windows server 2016 systems.

Authentication management:

- Role based access control (RBAC) and user authentication, page 111 for HTTPS and OPC UA clients.
- Certificates, page 103 for OPC UA client application entities.

M580 communication module features include:

- Ethernet backplane port for Ethernet communication over the local main Ethernet rack.
- X Bus backplane port for 24 Vdc power and rack addressing.
- NTP time server, page 124 and client synchronization.

Module Description

Introduction

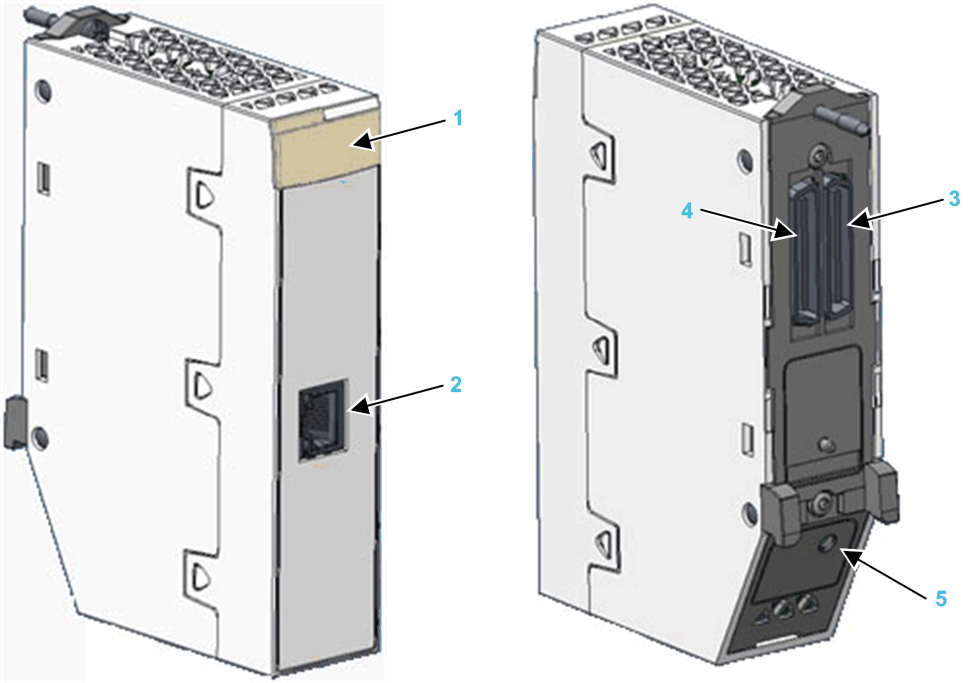
Schneider Electric offers two Ethernet communication modules with an embedded OPC UA server for communication with OPC UA clients, including SCADA:

- BMENUA0100 module for standard environments.
- BMENUA0100H module for harsh environments.

The module can be installed only in an Ethernet slot, on a main, local Ethernet rack. Refer to the topic *Supported BMENUA0100 Module Configurations*, page 59 for a description of supported module placements, including the maximum number of BMENUA0100 modules that can be placed into a rack.

Physical Description

This figure shows the external features of the BMENUA0100 module:



1 LED array

2 Control port with Ethernet link and activity LEDs

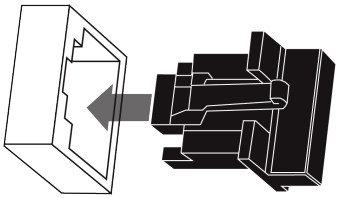
3 Ethernet backplane port

4 X Bus backplane port

5 Cybersecurity operating mode rotary selector switch

Refer to the topic LED Diagnostics, page 131 for information on reading module LEDs.

If the Ethernet control port is not enabled, use the stopper that ships with each module to help prevent debris from entering the control port:



External Ports

The BMENUA0100 module includes the following external ports:

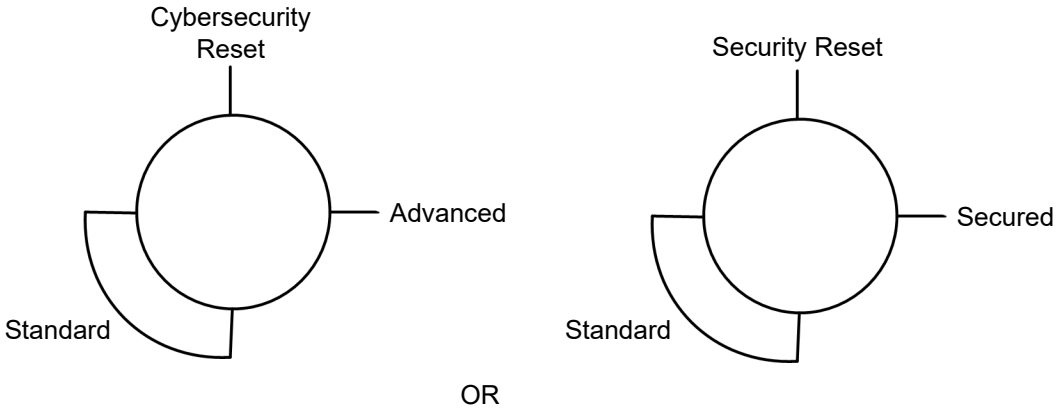
Port	Description
Control port	The control port is the single port located on the front of the BMENUA0100 module. Its features include: • When the control port is enabled, it is the exclusive interface for OPC UA communications, except when IPv6 is configured. ◦ When IPv6 is configured, both the backplane port and the control port can be used for OPC UA communications. ◦ When IPv6 is not configured, you can connect OPC UA clients located on the backplane network via the BMENUA0100 control port if a route has been defined/declared on the computer that hosts the OPC UA client. • Operating speed up to 1 Gb/s. When operating at the speed of: ◦ 1 Gb/s, use only CAT6 copper shielded twisted four-pair cables. ◦ 10/100 Mb/s, use CAT5e or CAT6 copper shielded twisted four-pair cables. • Dual IP stack that supports both IPv4 (32–bit) and IPv6 (128–bit) IP addressing: ◦ Both IPv4 and IPv6 are configured for the module. ◦ IPv6 configuration can be static or dynamic (via SLAAC). ◦ IPv4 default setting, page 115 is auto-assigned based on the module MAC address, if an IP address is not configured. • Secure access to the OPC UA server via both IPv4 and IPv6 protocols. • HTTPS secure protocol (over IPv4) for firmware upgrade, page 166 and cybersecurity configuration, page 84. • NTPv4 secure protocol support. • IPsec-provided security for non-secure services, including SNMPv1, Modbus TCP, and Syslog.
Ethernet backplane port	The BMENUA0100 Ethernet backplane port supports the IPv4 (32 bit) protocol. When the control port is disabled, the backplane port can support OPC UA communications. the backplane port includes the following features: • Operating speed up to 100 Mb/s. • Modbus TCP IPv4 Ethernet connectivity to the controller: ◦ The Ethernet backplane port is the exclusive port for Modbus diagnostics. • Exclusive port for non-cybersecurity configuration (IP, NTPv4, SNMPv1), by: ◦ Control Expert v14.1 and any subsequent supporting version(s) ◦ FDR/DHCP server • If the control port is disabled, the Ethernet backplane port provides secure access to the OPC UA server via the IPv4 protocol, and supports the following services: ◦ HTTPS secure protocol for firmware upgrade, page 166 and cybersecurity configuration, page 84. ◦ NTPv4, SNMPv1/v3 and Syslog.
X Bus backplane port	The BMENUA0100 module uses X Bus backplane communication to: • Receive 24 Vdc power. • Discover the rack and slot address of the BMENUA0100 module. **NOTE:** No other communication is performed via the X Bus backplane port of the BMENUA0100 module.

Rotary Switch

A four position rotary switch is located on the back of the module. Set this rotary switch to configure a mode for the controller

NOTE: A plastic screwdriver is provided for your convenience; use it, or an equivalent, to change the position of the rotary switch. Avoid using metal screwdrivers

Depending on your version of the module, the positions on the rotary switch are:



The settings are:

- Advanced (RL 6 and later) or Secured (earlier than RL 6) mode, page 30
- Standard mode, page 30
- Cybersecurity Reset (RL 6 and later) or Security Reset (earlier than RL 6), page 30

NOTE:

- The rotary switch is not accessible when the module is placed on the rack.
- In a Hot Standby system, verify that the BMENUA0100 module rotary switch positions – in both the primary and the standby local main racks – are the same. The system does not automatically perform this verification for you.

Refer to the description of cybersecurity operating modes, page 28 for information on each rotary switch position setting.

Module LEDs

LED Display

A 7-LED display panel is located on the front of the BMENUA0100 module:

The LEDs display information about the module as follows:

LED	Describes the state of the module
RUN	Operating condition.
ERR	Detected errors.
UACNX	OPC UA connections.
BS	Backplane port.
NS	Control port.
SEC	Cybersecurity condition.
BUSY	Data dictionary status

Refer to the LED Diagnostics topic, page 131 for information on how to use these LEDs to diagnose the state of the BMENUA0100 module.

Control Port LEDs

The control port, on the front of the module, presents two LEDs describing the state of the Ethernet link over the port:

- The ACT LED indicates the presence of Ethernet activity on the port.
- The LNK LED indicates the existence of an Ethernet link and the link speed.

Refer to the LED Diagnostics topic, page 135 for information on how to use the control port LEDs to diagnose the state of the BMENUA0100 module control port.

Standards and Certifications

Overview

This chapter describes the standards and certifications that apply to the BMENUA0100 Ethernet communications module with embedded OPC UA server.

Standards and Certifications

Download

Click the link that corresponds to your preferred language to download standards and certifications (PDF format) that apply to the modules in this product line:

Title	Languages
Modicon M580, M340, and X80 I/O Platforms, Standards and Certifications	• English: EIO0000002726 • French: EIO0000002727 • German: EIO0000002728 • Italian: EIO0000002730 • Spanish: EIO0000002729 • Chinese: EIO0000002731

BMENUA0100 Module Standard

Agency Requirements

The BMENUA0100 OPC UA embedded Ethernet communication module conforms to the following agency standard:

Marking	Requirement
OPC Unified Architecture	OPC UA V1.03: OPC Unified Architecture machine to machine communication protocol.

BMENUA0100 Firmware Compatibility with EcoStruxure™ Control Expert

Compatibility

Applications created with EcoStruxure™ Control Expert software are compatible with BMENUA0100 module firmware as follows:

BMENUA0100 Firmware Version	EcoStruxure™ Control Expert Software Version	
	14.0	15.0 or later
1.01	Fully compatible	Only legacy features of firmware version 1.01 are supported by software[1, 2, 3]
1.10	Fully compatible	Fully compatible

1. If a BMENUA0100 module with firmware version 1.01 receives an application generated with EcoStruxure™ Control Expert V15 where:
   - **Fast sampling rate** is **Activated** (in the IPConfig tab, page 116), this setting will not be implemented.
   - IPv4 is de-activated for the control port, the module control port will be configured with the IPv4 address that appears grayed-out in the **IPConfig** tab for the module.

     NOTE: The grayed-out IPv4 address can be the most recently user-input IPv4 address, or the IPv4 address automatically input by the EcoStruxure™ Control Expert software (172.16.12.1) if no IPv4 address was previously entered.
   - NTP, page 126 has been configured with an IPv6 address, the module web pages mistakenly indicate NTP is operational when the NTP service actually is not operational.

2. If two BMENUA0100 modules with firmware version 1.01 are configured in a Hot Standby rack with EcoStruxure™ Control Expert V15, the limitations described in the preceding items also apply to these modules.

3. If SNMP is enabled in Control Expert, include the IPv4 address of the SNMP manager in the SNMP tab for the BMENUA0100 module, page 127 so that the SNMP manager can access the SNMP MIB.

NOTE: The web pages displayed for the BMENUA0100 module depend on the module firmware version (for example version 1.01, 1.10 or 2.01).

BMENUA0100 Functional Description

Introduction

This chapter describes the supported functions of the BMENUA0100 Ethernet communications module with embedded OPC UA server.

Cybersecurity Operating Mode Settings

Introduction

The BMENUA0100 module can be configured to operate in either Advanced (or Secured) or Standard mode. The 4-position rotary selector switch on the back of the module determines the operating mode.

The three rotary switch positions are:

- Advanced (or Secured) mode
- Standard mode
- Cybersecurity (or Security) Reset

NOTE:

- The module default, out-of-the-box configuration, is the Advanced (or Secured) mode.
- You can view the position of the rotary switch in the Home page, page 89 of the module web pages.

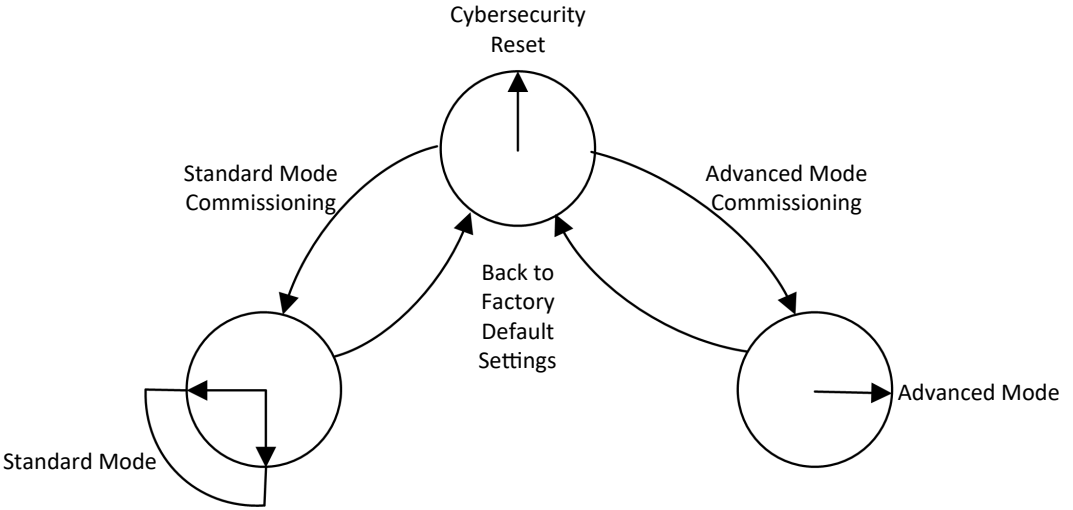
Because the rotary selector switch is not accessible while the module is on the rack, the switch position can be changed only when the module is powered off and removed from the rack. After a new switch position is selected, the module can be re-inserted into the rack and power applied.

NOTE: Use only the small, plastic screwdriver that ships with the module, page 23 to change the switch position and configure a cybersecurity operating mode.

Changing Operating Mode

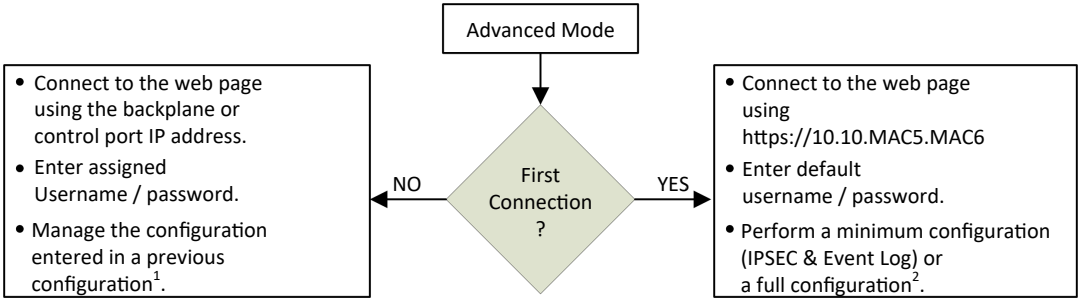
Each time you switch the cybersecurity operating mode from Advanced (or Secured) mode to Standard mode, or from Standard mode to Advanced (or Secured) mode, perform a Cybersecurity (or Security) Reset operation, page 80 before configuring the new mode.

The position of the rotary switch determines the operating state of the module, as follows:



A new (out-of-the-box factory default) module, or a module for which a **Cybersecurity (or Security) Reset** has been performed, can be commissioned for either Standard mode, page 80 or Advanced (or Secured) mode, page 78 operations.

The process for configuring the module for Advanced (or Secured) mode operations varies, depending on whether you are connecting to the module configuration settings for the first time after performing a Cybersecurity (or Security) Reset:



1 For information about managing the configuration, refer to the configuration chapter, page 84.

2 For information on performing a configuration on first connection, refer to the topic Advanced (or Secured) Mode Commissioning, page 78.

Advanced (or Secured) Mode

When operating in Advanced (or Secured) mode, the module will not engage in process communications – over either the control port or the backplane port – until valid cybersecurity settings have been configured. After Advanced (or Secured) mode has been configured, you can configure cybersecurity settings using the module web pages, page 84, which can be accessed via the HTTPS protocol over either the backplane or control ports. In Advanced (or Secured) mode, the module supports the level of cybersecurity that is specified in the cybersecurity configuration. Only after cybersecurity settings have been configured, can IP address, NTP client, and SNMP agent settings, page 114 be configured using the Control Expert configuration software.

Standard Mode

When operating in Standard mode, module communications can begin without the need for cybersecurity configuration. Cybersecurity settings are not required and cannot be configured. Only the IP address and other settings available in Control Expert can be configured.

Cybersecurity (or Security) Reset

The **Cybersecurity (or Security) Reset** command restores the out-of-the-box factory default configuration settings. It deletes any existing cybersecurity configuration, white lists, certificates, and role based access control settings. To complete the Cybersecurity (or Security) Reset, either cycle power (off, then on) to the BMENUA0100 module, or physically remove the module from the rack (which turns off power) then re-insert the module into the rack (which turns power back on). While the process of restoring factory default settings is ongoing, the **RUN** LED flashes green. After completion of process, the **RUN** LED turns to solid green, and the services are disabled.

This setting can be made using either the rotary switch or the web pages (when operating in Advanced (or Secured) mode):

- If set via rotary switch: the module ceases to be functional until the module is removed from the rack, the rotary switch is re-set to either the Advanced (or Secured) or Standard position, and the module is again placed on the rack. The necessary configuration(s) will need to be applied.
- If set via the web pages: upon completion of the process cycle power (off / on) to – or hot swap – the module in Standard or in Advanced (or Secured) mode. Both the cybersecurity and IP address settings need to be configured.

NOTE: After a Cybersecurity (or Security) Reset of the BMENUA0100 module, the following conditions apply to the module:

- No device certificates are preserved.
- All services are disabled except for HTTPS, which is used to create the cybersecurity configuration via the control port.
- Factory default settings are applied, including:
  - Username / Password default settings, page 31.
  - IP address default setting of 10.10.MAC5.MAC6, page 115.

NOTE: When the last two octets of the MAC address (*MAC5.MAC6*) correspond to *0.0* in the default address, make a point-to-point cable connection between your computer and the controller, communication module, or other module.

Default Username / Password Combination

The default username / password combination depends on the cybersecurity operating mode setting:

- Advanced (or Secured) mode: admin / password
- Standard mode: installer / Inst@ller1

NOTE: You will be asked to modify the password upon first use in Advanced (or Secured) mode. Verify your local laws and regulations whether this is a requirement.

Functions Supported by Advanced (or Secured) and Standard Operating Modes

The following functions are supported by the BMENUA0100 module in Advanced (or Secured) and Standard modes:

Mode	**Standard mode**			**Advanced (or Secured) mode**		
Control port	**Disable**	**Enable**		**Disable**	**Enable**	
Ethernet port	**Backplane**	**Backplane**	**Control port**	**Backplane**	**Backplane**	**Control port**
OPC UA Comm	Yes	No	Yes	Yes	No	Yes
Security Settings (4)	None	–	None	None, Sign, Sign&Encrypt (default value)	–	None, Sign, Sign&Encrypt (default value)
User authentication	No	–	No authentication (anonymous)	Operator, Engineer, No	–	Operator, Engineer, No

Mode	**Standard mode**			**Advanced (or Secured) mode**		
Control port	**Disable**	**Enable**		**Disable**	**Enable**	
Ethernet port	**Backplane**	**Backplane**	**Control port**	**Backplane**	**Backplane**	**Control port**
User authentication	authentication (anonymous)			authentication (anonymous)		authentication (anonymous)
SNMP V1	Yes (1, 2)	Yes (1, 2)	Yes (1, 2)	Yes (1)	Yes (1)	Yes (1)
SNMP V3	Yes (1, 2)	Yes (1, 2)	Yes (1, 2)	Yes (1)	Yes (1)	Yes (1)
NTP V4	Client only (1)	Client (1), Server	Yes, Client only (1)	Client only (1)	Client (1), Server	Yes, Client only (1)
Event Log	No	No	No	Yes	Yes	Yes
IPsec	No	No	No	No	No	Yes for Modbus, SNMP V1/V3, NTP V4 (3) and Syslog (IPsec enabled by default)
Web CS Config change (HTTPS)	No	No	No	Yes	Yes	Yes
User authentication	–	–	–	Admin	Admin	Admin
Network Services Comm server Enable/ Disable	If supported, always enabled (refer above)	If supported, always enabled (refer above)	If supported, always enabled (refer above)	All services are configurable (disabled by default)	All services are configura-ble (disabled by default)	All services are configurable (disabled by default)
Web Diagnostic (Home and Diagnostic pages only)	Yes	Yes	Yes	Yes	Yes	Yes
User authentication	Installer (default credentials)	Installer (default creden-tials)	Installer (default credentials)	Admin, Operator, Engineer, Installer	Admin, Operator, Engineer, Installer	Admin, Operator, Engineer, Installer
Firmware upgrade (HTTPS)	Yes	Yes	Yes	Yes	Yes	Yes, if HTTPS enabled
User authentication	Installer (default credentials)	Installer (default creden-tials)	Installer (default credentials)	Installer	Installer	Installer

Mode	Standard mode			Advanced (or Secured) mode		
Control port	**Disable**	**Enable**		**Disable**	**Enable**	
Ethernet port	**Backplane**	**Backplane**	**Control port**	**Backplane**	**Backplane**	**Control port**
Filtering: Forward All	–	–	(always enabled)	–	–	Forward all protocols
Filtering: Configured Forward Protocol	–	–	–	–	–	Forward of configured protocols
Filtering: Control Expert Data Flows to Device Network (including controller) (FTP, EIP, Explicit, Modbus, Ping) via IPv4 only[5]	–	–	Forward of Control Expert data flows from Control Network to Device Network (always enabled)	–	–	Forward of Control Expert data flows from Control Network to Device Network (disabled by default)

1. Configurable with Control Expert.
2. In standard mode, the SNMP version of the BMENUA0100 module is set in Control Expert. If SNMP is set to V3, and the module is configured with:
   - Firmware version 2 (BMENUA0100.2), it uses SNMP V3 with NoAuthNoPriv security level.
   - Firmware earlier than version 2 (BMENUA0100), it uses SNMP V1.

   For more information, refer to the topic SNMP Agent Configuration in Control Expert and the Web Pages, page 128.
3. NTP V4 can be configured to be transported outside IPsec tunnel.
4. For both Standard and Advanced (or Secured) cybersecurity operating modes, if Security Settings is set to *None*, there is no user authentication (i.e. the **User Identifier token types** OPC UA setting, page 101 is set to *Anonymous.*)
5. To provide Control Expert with online access to the controller or Device Network, configure the PC (on which Control Expert is installed) with an IP address on the same subnet as the BMENUA0100 module control port, and use the BMENUA0100 module control port IP address as the PC gateway IP address. In this case, no IP address of the PC can be on the same subnet as the BMENUA0100 module backplane port.

OPC UA Services

Introduction

This section describes the services supported by the OPC UA server embedded in the BMENUA0100 module.

BMENUA0100 OPC UA Server Operating Characteristics

Limitations

The maximum:

- Number of nodes that can be published in the BMENUA0100 OPC UA Server data access Address space is 100000 nodes.
- Memory amount that can be allocated to the BMENUA0100 OPC UA Server is 192 MB.

  NOTE: If either limit is exceeded, the server Address Space state enters into a *LimitsExceeded* state.

  NOTE: The time needed to establish time subscription may significantly depend on the number of items and the number of connected clients.

Other limitations, the context in which they occur, and their consequences if exceeded are set forth below:

Limit	Value	OPCUA Service	Service Parameter	Effects
Cumulative Session Count	10	*CreateSession*	(Not Applicable)	*Bad_TooManySessions* service result code
Minimum Session Timeout	30 s	*CreateSession*	Requested SessionTimeout	revisedSession Timeout
Cumulative Session timeout	3600 s	*CreateSubscription*	Requested SessionTimeout	revisedSession Timeout
Maximum Cumulative Subscription Count	40	*CreateSubscription*	(Not Applicable)	*Bad_TooManySubscriptions* service result code
Minimum Publishing Interval	250 ms[1] 20 ms[2]	*CreateSubscription*	Requested Publishing Interval	revisedPublishingInterval
Maximum Publishing Interval	10 s	*CreateSubscription*	Requested Publishing Interval	revisedPublishingInterval
Maximum Subscription Lifetime	300 s	*CreateSubscription*	Min(Requested Publishing Interval, 3600000) * Requested LifetimeCount	revisedLifetimeCount
Maximum Notifications Per Publish	12500	*CreateSubscription*	maxNotificationsPerPublish	Notifications maximum capacity is thus (1000/ revisedPublishingInterval) * 1000 notifications per second.

Limit	Value	OPCUA Service	Service Parameter	Effects
Minimum Sampling Interval	125 ms[1] 20 ms[2]	*CreateMonitoredtems*	MonitoringParameters. SamplingInterval	revisedSampling Interval
Maximum Message Queue Size	100	*CreateMonitoredtems*	MonitoringParameters. QueueSize	revisedQueueSize
Maximum Cumulative Monitored Items Count	50010 or 35010[3, 4] 2010[2]	*CreateMonitoredtems*	(Not Applicable)	*Bad_TooManyMonitoredItems* service result code
Maximum Subscriptions Per Session	4	–	–	–
Maximum Monitored Items Count Per Subscription	25000	–	–	–

1. If Fast Sampling is disabled.

2. If Fast Sampling is enabled.

3. If Fast Sampling is disabled, and the server is configured with:

- a sampling interval of at least 1 second, and
- a publishing interval of at least 1 second.

4. If Source Timestamping is enabled and activated, page 119, the maximum is 35010. If it is not activated, the maximum is 50010.

OPC UA Server

Introduction

The primary purpose of the BMENUA0100 Ethernet communication module is to provide an OPC UA communication channel over Ethernet between M580 controllers and OPC UA clients. The data of the M580 controller is mapped to variables in the BMENUA0100 module, and made available to OPC UA clients via an OPC UA server communication stack embedded in the BMENUA0100 module. OPC UA clients connect to the embedded OPC UA server stack using IP address of the BMENUA0100 module control port or backplane port, thereby establishing a client server connection. The BMENUA0100 module is able to handle a maximum of ten (10) simultaneous OPC UA client connections for firmware version 1.1 (or three (3) simultaneous OPC UA client connections for firmware version 1.0).

NOTE: The terms of each connection between an OPC UA client and the OPC UA server embedded in the BMENUA0100 module are determined by the client, which sets the attributes of the connection between the client and server.

The OPC UA server stack embedded in the BMENUA0100 module consists of functionalities defined by the following terms:

- Profile: a definition of functionality that comprises other profiles, facets, conformance groups, and conformance units.
- Facet: defines a partial functionality.
- Conformance Group: a collection of conformance units.
- Conformance Unit: a specific service, for example, read, write, and so forth.

BMENUA0100 Supported Profile

The BMENUA0100 module supports the **Embedded 2017 UA Server Profile**. As stated in the OPC Foundation web site, this profile “is a FullFeatured Profile that is intended for devices with more than 50 MBs of memory and a more powerful processor. This Profile builds upon the Micro Embedded Device Server Profile. The most important additions are: support for security via the Security Policies and support for the Standard DataChange Subscription Server Facet. This Profile also requires that Servers expose all OPC-UA types that are used by the Server including their components and their super-types."

For more information, refer to the OPC Foundation website at: http://opcfoundation.org/UA-Profile/Server/EmbeddedUA2017.

BMENUA0100 Supported Facets

The BMENUA0100 module supports the following facets:

- **Server Category > Facets > Core Characteristics**:
  - **Core 2017 Server Facet** (http://opcfoundation.org/UA-Profile/Server/Core2017Facet)
- **Server Category > Facets > Data Access**:
  - **ComplexType 2017 Server Facet** (http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017)
  - **Data Access Server Facet** (http://opcfoundation.org/UA-Profile/Server/DataAccess)
  - **Embedded DataChange Subscription Server Facet** (http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription)
- **Server Category > Facets > Generic Features**:
  - **Method Server Facet** (http://opcfoundation.org/UA-Profile/Server/Methods)

- **Security Category > Facets > Security Policy**:
  - **Basic128RSA15** (http://opcfoundation.org/UA/SecurityPolicy#Basic128Rsa15)
  - **Basic256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256)
  - **Basic256Sha256** (http://opcfoundation.org/UA/SecurityPolicy#Basic256Sha256)
- **Transport Category > Facets > Client-Server**:
  - **UA-TCP- UA-SC UA-Binary** (http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary)

The following topics discuss the services, related to the above-referenced facets, that are supported by the BMENUA0100 module.

BMENUA0100 OPC UA Server Stack Services

Supported OPC UA Services

The BMENUA0100 module OPC UA server stack supports the following service sets and services:

Service Set	Services
Attribute	• Read • Write
Discovery	• FindServers • GetEndpoints
MonitoredItem	• CreateMonitoredItems • ModifyMonitoredItems • DeleteMonitoredItems • SetMonitoringMode
SecureChannel	• OpenSecureChannel • CloseSecurechannel
Session	• CreateSession • ActivateSession • CloseSession

Service Set	Services
Subscription	• CreateSubscription • ModifySubscription • DeleteSubscription • SetPublishingMode • SetMonitoringMode • Publish • Republish
View	• Browse • BrowseNext • TranslateBrowsePathToNodeIds • RegisterNodes • UnregisterNodes

NOTE: For a description of these service sets and services, refer to the document *OPC Unified Architecture Specification Part 4: Services (Release 1.04)*.

BMENUA0100 OPC UA Server Stack Data Access Services

Supported Data Access Services

Data access by the BMENUA0100 module embedded OPC UA server stack is enabled by its support of the following facets and related services:

- Data Access Server Facet
- ComplexType 2017 Server Facet
- Core 2017 Server Facet

NOTE: In the following facet descriptions, italicized text indicates a direct quote of the OPC Foundation source material. Click on the links below and use the *OPC Foundation Unified Architecture Profile Reporting Visualization Tool* to access a description of each facet.

Core 2017 Server Facet

As stated in the OPC Foundation web site, the Core 2017 Server Facet “defines the core functionality required for any UA Server implementation. The core functionality includes the ability to discover endpoints, establish secure communication channels, create Sessions, browse the AddressSpace and read and/or write to Attributes of Nodes. The key

requirements are: support for a single Session, support for the Server and Server Capabilities Object, all mandatory Attributes for Nodes in the AddressSpace, and authentication with UserName and Password. For broad applicability, it is recommended that Servers support multiple transport and security Profiles."

For a full description of this facet, refer to http://opcfoundation.org/UA-Profile/Server/Core2017Facet.

The BMENUA0100 module embedded OPC UA server stack supports the following conformance units in the Core 2017 Server Facet:

- View Service Set, includes the following groups and services:
  - View Basic: includes the Browse and the BrowseNext services.
  - View TranslateBrowsePath: includes the TranslateBrowsePathsToNodeIds service.
  - View Register Nodes: includes the RegisterNodes and UnregisterNodes services as a way to optimize access to repeatedly used Nodes in the Servers OPC UA AddressSpace.
- Attribute Service Set, includes the following groups and services:
  - Attribute read: includes the Read service, which supports reading one or more attributes of one or more Nodes, including support of the IndexRange parameter to read a single element or a range of elements when the Attribute value is an array.
  - Attribute Write values: includes the Write Value service, which supports writing one or more values to one or more Attributes of one or more Nodes.
  - Attribute Write Index: includes the Write Index service, which supports the IndexRange for writing to a single element or a range of elements when the Attribute value is an array and partial updates is allowed for this array.

Data Access Server Facet

As stated in the OPC Foundation web site, the Data Access Server Facet "specifies the support for an Information Model used to provide industrial automation data. This model defines standard structures for analog and discrete data items and their quality of service. This Facet extends the Core Server Facet which includes support of the basic AddressSpace behaviour."

For a full description of this facet, refer to http://opcfoundation.org/UA-Profile/Server/DataAccess.

ComplexType 2017 Server Facet

As stated in the OPC Foundation web site, the ComplexType 2017 Server Facet "extends the Core Server Facet to include Variables with structured data, i.e. data that are composed of multiple elements such as a structure and where the individual elements are exposed as

component variables. Support of this Facet requires the implementation of structured DataTypes and Variables that make use of these DataTypes. The Read, Write and Subscriptions service set shall support the encoding and decoding of these structured DataTypes. As an option the Server can also support alternate encodings, such as an XML encoding when the binary protocol is currently used and vice-versa."

For a full description of this facet, refer to http://opcfoundation.org/UA-Profile/Server/ComplexTypes2017.

BMENUA0100 OPC UA Server Stack Discovery and Security Services

Introduction

The BMENUA0100 module embedded OPC UA server stack supports both discovery and security services.

To connect to the OPC UA server in the BMENUA0100 module, an OPC UA client requires information describing the server, including its network address, protocol, and security settings. OPC UA defines a set of discovery features a client can use to obtain this information.

The information needed to establish a connection between an OPC UA client and an OPC UA server is stored in an endpoint. An OPC UA server can possess several endpoints, each containing:

- Endpoint URL (network address and protocol), for example:
  - For IPv4: opc.tcp://172.21.2.30:4840, where:

    - opc.tcp = protocols

    - 172.21.2.30 = IPv4 address

    - 4840 = opcua-tcp port number configured in Control Expert
  - For IPv6: opc.tcp://[2a01:cb05:431:f00:200:aff:fe02:a0a]:50000, where:

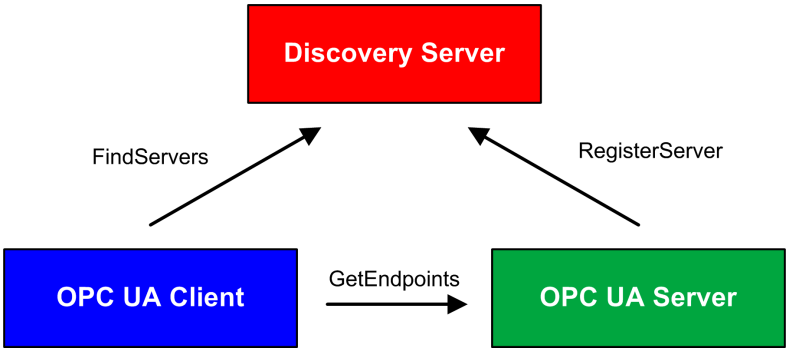
    - opc.tcp = protocols

    - [2a01:cb05:431:f00:200:aff:fe02:a0a] = IPv6 address

    - 50000 = opcua-tcp port number configured in Control Expert
- Security Policy (including a set of security algorithms and key length)
- Message Security Mode (security level for exchanged messages)
- User Token Type (server supported types of user authentication)

One or more OPC UA servers can exist. In the case of multiple servers, a discovery server can be used to provide information regarding each server. Individual servers can register

with the discovery server. Clients can request a list of some or all of the available servers from the discovery server and use the GetEndpoints service to acquire connection information from an individual server.



The BMENUA0100 module supports several discovery and security services, including:

- Discovery Service Set
- SecureChannel Service Set
- Session Service Set

The decision to enable or disable services depends on the cybersecurity policy you decide to implement for the server.

Discovery Service Set

The BMENUA0100 OPC UA server stack supports the Discovery Service Set, which is incorporated in the Core 2017 Server Facet, page 38. As implemented in the BMENUA0100 module, the supported services include:

- FindServers: As implemented in the BMENUA0100 module OPC UA server stack, this service finds the servers only on the local OPC UA server.
- GetEndpoints: Returns the Endpoints supported by a server and the configuration information required to establish a SecureChannel and a Session. Can provide a filtered Endpoints return list, based on profiles.

SecureChannel Service Set

The BMENUA0100 OPC UA server stack supports the SecureChannel Service Set, which includes the following services:

- OpenSecureChannel: Opens or renews a SecureChannel that provides confidentiality and integrity for the exchange of messages during a session. This Service requires the OPC UA server stack to apply the various security algorithms to the messages as they are sent and received.
- CloseSecureChannel: Terminates a SecureChannel.

Session Service Set

The BMENUA0100 OPC UA server stack supports the Session Service Set, which is incorporated in the Core 2017 Server Facet, page 38. As implemented in the BMENUA0100 module, the supported services include:

- CreateSession: After creating a SecureChannel with the OpenSecureChannel service, a client uses this service to create a session. The server returns two values which uniquely identify the session:
  - A sessionId, which is used to identify the session in the audit logs and in the server AddressSpace.
  - An authenticationToken, which is used to associate an incoming request with a session.
- ActivateSession: Used by the client to specify the identity of the user associated with the session. It cannot be used to change the session user.
- CloseSession: Terminates a session.

  NOTE: For the CreateSession and ActivateSession services, if the SecurityMode = None then:

  1. The Application Certificate and Nonce are optional.
  2. The signatures are null/empty.

BMENUA0100 OPC UA Server Stack Publish and Subscribe Services

Subscriptions

Instead of permanently reading information by polling, the OPC UA protocol includes the Subscription function. This function enables the OPC UA stack embedded in the BMENUA0100 module to provide publish/subscribe services, which are used when the module connects to remote devices.

An OPC UA client can subscribe to one or more selected nodes and let the server monitor these items. Upon the occurrence of a change event, for example a change in value, the server notifies the client of the change. This mechanism significantly reduces the quantity of

data that is transferred and therefore represents a significant reduction of bandwidth consumption.

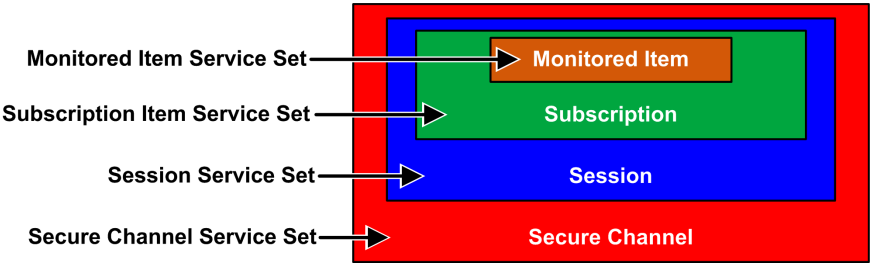
An OPC UA client can subscribe to the multiple types of information that an OPC UA server provides. The subscription groups together these varying types of data, called Monitored Items, to form a single collection of data called a Notification.

A subscription must:

- Consist of at least one Monitored Item.
- Be created within the context of a Session, which is created within the context of a Secure Channel.

NOTE: The subscription can be transferred to another session.

The service sets involved in a client subscription are described below:



Subscriptions and Overruns

In some cases, where there exists a large number of subcription requests, the OPC UA server attempts to obtain data from the controller in an amount greater than the controller or the BMENUA0100 module can handle in the specified publishing interval. In this case, the execution time for subscription requests will be automatically extended – and the next subscription execution postponed – until all requests can be completed.

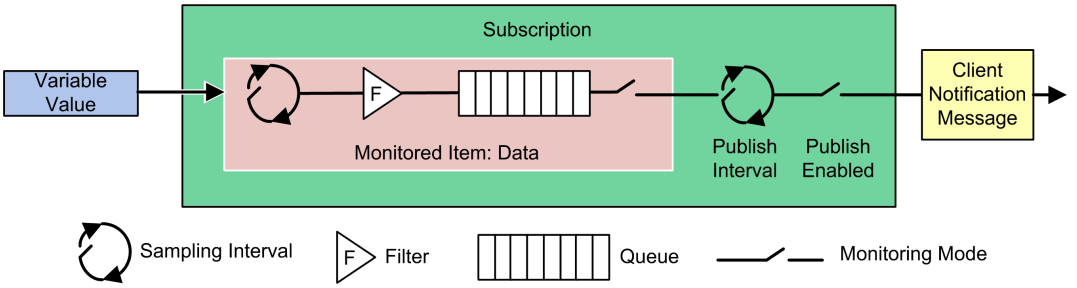
When setting a publishing interval, consider the number of clients and client requests the server needs to handle. When determining the number of client requests, confirm that all clients are operating online. In this regard, note that some clients can take 2 minutes or more to come online after startup.

NOTE: Set the publishing interval to at least twice the sampling interval to help avoid missing data changes.

Change Events

A client can subscribe to a data change event, which is triggered by a change to the value attribute of a variable, as a Monitored Item.

The configurable subscription settings, their sequence and roles, are described below:



The following three settings determine how Monitored Items are added to a subscription:

- Sampling Interval: the sampling time interval set for each Monitored Item in the subscription. This is the frequency by which the server verifies the data source for changes. For a single Variable item, the Sampling Interval can be smaller (i.e. faster) than the period between notifications to the client. In this case, the OPC UA Server may queue the samples and publish the complete queue. In extreme cases, the server will revise (i.e. slow) the Sampling Interval so that the data source will not experience excessive queuing load that may be caused by the sampling itself.

  NOTE: If OPC UA queuing of data samples is supported, the queue size (i.e., the maximum number of values which can be queued) can be configured for each monitored item. When the data is delivered (published) to the client, the queue is emptied. In case of a queue overflow, the oldest data is discarded and replaced by new data.

- Filter: a collection of several criteria used to identify which data changes or events are reported, and which are blocked.
- Monitoring Mode: used to enable or disable data sampling and reporting.

The following two settings apply to the Subscription itself:

- Publishing Interval: The period after which notifications collected in the queues are delivered to the client in a Notification Message (Publish Response). The OPC UA Client must confirm that the OPC UA server has received enough Publish Tokens (Publish Requests), so that whenever the Publish Interval elapsed and a notification is ready to send, the server uses such a token and sends the data within a Publish Response. In case that there is nothing to report (e.g. no values have changed) the server will send a KeepAlive notification to the Client, which is an empty Publish, to indicate that the server is still alive.
- Publish Enabled: Enables and disables the sending of the Notification Message.

Embedded DataChange Subscription Server Facet

As stated in the OPC Foundation web site, the Embedded DataChange Subscription Server Facet “specifies the minimum level of support for data change notifications within

subscriptions. It includes limits which minimize memory and processing overhead required to implement the Facet. This Facet includes functionality to create, modify and delete Subscriptions and to add, modify and remove Monitored Items. As a minimum for each Session, Servers shall support one Subscription with up to two items. In addition, support for two parallel Publish requests is required. This Facet is geared for a platform such as the one provided by the Micro Embedded Device Server Profile in which memory is limited and needs to be managed."

For a full description of this facet, refer to http://opcfoundation.org/UA-Profile/Server/EmbeddedDataChangeSubscription.

This facet supports the following services:

- Monitored Item Service Set
- Subscription Service Set

Monitored Item Service Set

The Monitored Item Service Set supports the following services:

NOTE: For a description of these service sets and services, refer to the document OPC *Unified Architecture Specification Part 4: Services (Release 1.04)*.

- CreateMonitoredItems: An asynchronous call used to create and add one or more MonitoredItems to a subscription.
- ModifyMonitoredItems: an asynchronous call to modify monitored items. This service is used to modify MonitoredItems of a subscription. Changes to the MonitoredItem settings are applied immediately by the server.
- DeleteMonitoredItems: an asynchronous call to delete monitored items. This service is used to remove one or more MonitoredItems of a subscription. When a MonitoredItem is deleted, its triggered item links are also deleted.
- SetMonitoringMode: an asynchronous call to set the monitoring mode for a list of MonitoredItems. This service is used to set the monitoring mode for one or more MonitoredItems of a subscription. Setting the mode to DISABLED causes all queued notifications to be deleted.

Subscription Service Set

The Subscription Service Set supports the following services:

NOTE: For a description of these service sets and services, refer to the document OPC *Unified Architecture Specification Part 4: Services (Release 1.04)*.

- CreateSubscription: an asynchronous call to create a subscription.
- ModifySubscription: an asynchronous call to modify a subscription. The server immediately applies changes to the subscription.

- DeleteSubscription: an asynchronous call to delete one or more subscriptions belonging to the client session. Successful completion of this service deletes all Monitored Items associated with the subscription.
- Publish: This Service is used for two purposes: to acknowledge the receipt of NotificationMessages for one or more subscriptions, and to request the server to return a NotificationMessage or a keep-alive message.
- Republish: an asynchronous republish call to get lost notifications. This service requests the subscription to republish a NotificationMessage from its retransmission queue. If the server does not have the requested message in its retransmission queue, it returns an error response.
- SetPublishingMode: an asynchronous call to enable sending of Notifications on one or more subscriptions.

BMENUA0100 OPC UA Server Stack Transport Services

Support for the UA-TCP UA-SC UA-Binary Facet

The BMENUA0100 module supports the UA-TCP UA-SC UA-Binary transport facet. (For additional information, refer to the online description at http://opcfoundation.org/UA-Profile/Transport/uatcp-uasc-uabinary.)

This transport facet defines a combination of network protocols, security protocols, and message encoding that is optimized for low resource consumption and high performance. It combines the simple TCP-based network protocol UA-TCP 1.0 with the binary security protocol UA-SecureConversation 1.0 and the binary message encoding UA-Binary 1.0.

Data that passes between an OPC UA client and the BMENUA0100 module embedded OPC UA server uses the TCP protocol, and is binary coded in accordance with the OPC UA Binary File Format.

NOTE: The OPC UA Binary File Format replaces the XML UA-Nodeset Schema from the OPC Foundation. It improves performance and memory consumption. It does not require an XML parser.

Discovering Controller Variables

Mapping Control Expert Controller Variables to OPC UA Data Logic Variables

Introduction

The OPC UA embedded server in the BMENUA0100 module uses Unified Messaging Application Services (UMAS) data dictionary requests to browse and discover M580 controller application variables. You will need to activate the data dictionary in the Control Expert project settings.

NOTE:

- The BMENUA0100 module can support a maximum data dictionary size of 100000 variables.
- The time required to load the data dictionary into the OPC UA server depends on the number of data dictionary items and the MAST period setting, page 162.

The collected variables are translated from the Control Expert data logic model view to the OPC UA data logic model view using the appropriate OPC UA stack services. An OPC UA client connected to the BMENUA0100 module–over its control port, or over its backplane port via the controller or a BMENOC0301 or BMENOC0311 communication module–can retrieve this collection of data using the services of the Data Access Server Facet, page 39 supported by the Embedded 2017 UA Server Profile, page 36.

Preloading the Data Dictionary to Avoid Communication Interruptions

An online application change made with Control Expert temporarily interrupts OPC UA server/client communication while the server acquires an updated data dictionary. This interruption is caused by inconsistent controller data mapping while the data dictionary is updated. During the period of communication interruption, the status of the monitored nodes, as indicated by UA Expert, is in error (**bad communication error** or **bad no communication** or **bad timeout**). To avoid this interruption of communications and its consequence, a synchronization mechanism can be set up between the BMENUA0100 module and the Control Expert configuration software, based on a preload of the updated data dictionary.

This feature is enabled in Control Expert in the **Tools > Project Settings...** window, in the **General > PLC embedded data** area, using the **Preload on build changes** and **Effective Build changes time-out** settings (see EcoStruxure™ Control Expert, Operating Modes). Refer to the Control Expert online help for information on how to configure this feature.

Activating the Data Dictionary

To activate the data dictionary in Control Expert:

Step	Action
1	In Control Expert, with the project open, select **Tools > Project Settings**.
2	In the **Project Settings** window, navigate to **General > PLC embedded data**, then select **Data dictionary**. **NOTE:** If the EcoStruxure™ Control Expert project includes a BMENUA0100 module and this setting is not selected, a detected error is generated during the application build.

Variable Data Type Conversion

The BMENUA0100 module can discover and convert to OPC UA data types the following basic variable types supported by the Control Expert data logic model:

Control Expert Elementary Data Type	OPC UA Data Type
BOOL	Boolean
EBOOL	Boolean
INT	Int16
DINT	Int32
UINT	UInt16
UDINT	UInt32
REAL	Float
BYTE	Byte
WORD	UInt16
DWORD	UInt32
DATE*	UInt32
TIME*	UInt32
TOD*	UInt32
DT*	Double
STRING	ByteString
* Refer to following table describing date-related data type conversion.	

For Control Expert data of types DATE, TIME, TOD, DT, the corresponding OPC UA data types are as follows:

Control Expert Elementary Data Type	Example value displayed in Control Expert	OPC UA Data Type	Corresponding value in OPC UA type
DATE	D#2017-05-17	UInt32	20170517 hex
TIME	T#07h44m01s100ms	UInt32	27841100
TOD	TOD#07:44:01	UInt32	07440100 hex
DT[1]	DT#2017-05-17-07:44:01	Double	4.29E-154
1. The returned data for Date and Time values is UATypeUInt64 which is the internal encoding of IEC 1131 DT in Control Expert - binary coded decimal (BCD) encoding.			

Discoverable Variables

For variables, the OPC UA client does not directly access a discovered controller data logic variable. Instead, the client accesses the discovered controller variable through an OPC UA data logic variable, which exists in the BMENUA0100 module and is mapped to the underlying controller variable. Because of the pass-through nature of data variable access, the acquisition request process is not optimized, and data dictionary acquisition performance is not representative of the controller performance.

NOTE: References, of the REF_TO type, to application variables in the OPC UA server are not accessible by the OPC UA client.

Examples of Control Expert controller variables discoverable by the OPC UA server in the BMENUA0100 module include:

- Structured variables with sub-fields: DDT and array variables.
- Program Unit variables are discoverable as follows:
  - Input/Output variables are accessible by the OPC UA client only for the BOOL type.
  - Input variables and Output variables are accessible by the OPC UA client, except for the types REF_TO, ARRAY, String, and Structure.

In addition, the following variables are discoverable by the OPC UA server by mapping them to application varables, then discovering the mapped application variables:

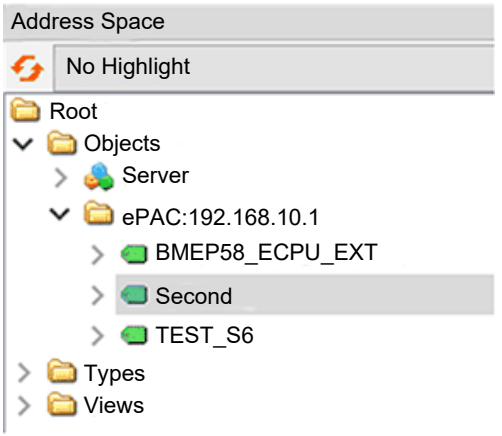
- Topological I/O variables:
  - Inputs: %I, %IW, %ID, %IF.
  - Outputs: %Q, %QW, %QD, %QF.
- Located variables: %M, %MW, %MD, %MF.
- System variables: %S, %SW, %SD.

NOTE: Variable discovery includes a variable (or symbol) for an extracted bit (for example, MyBoolVar located on %MW100.1).

Presentation of Discovered Variables in the OPC UA Client

The OPC UA server in the BMENUA0100 module can organize and graphically display discovered controller variables. An OPC UA client tool can connect to the BMENUA0100 module and view a node tree presentation of OPC UA server variables.

In the following example, an OPC UA client (in this example, the Unified Automation UaExpert client tool) connected to the BMENUA0100 module can view controller variables in its **Address Space** windows. The M580 controller IP address is represented by the node ePAC:192.168.10.1. Its child nodes represent Control Expert application variables:



In the example above, the first sub-node, BMEP58_ECPU_EXT, represents the device DDT for the M580 controller, which is automatically instantiated when the controller was added to the Control Expert application. The subsequent nodes represent other objects added to the application.

Using the OPC UA client tool, the node TEST_S6 was dragged and dropped into the **Data Access View** window, where the details of the variable are displayed:

Data Access View

#	Server	Node Id	Display Name	Value	Datatype	Source Timestamp	Server Timestamp	Statuscode
1	bmenua-server	NS2|String|0:Test_S6	TEST_S6	false	Boolean	10:43:54.830	10:43:54.830	Good
2	bmenua-server	NS0|Numeric|2258	CurrentTime	2019-08-12T08:43:54.733Z	DateTime	10:43:54.733	10:43:54.830	Good

In this case, the variable OPC UA data type is *Boolean* (indicating the underlying controller data type is BOOL) and its value is *false*.

NOTE: The **Server Timestamp** attribute of the OPC UA nodes is received from the BMENUA0100 OPC UA server in UTC (Universal Time Coordinated). It is displayed in local time.

Reading and Writing Discovered Variables in the OPC UA Client

An OPC UA tag in an OPC UA client (for example a SCADA) that refers to an array variable allows the client to read or write all elements of the array. For example the tag ‘MyArray’ declared as ARRAY[0...31] OF INT.

However, for the client to be able to read or write only a single element of an array, it is necessary to declare a specific tag that references the targeted single array element. For example ‘MyInt’ declared as INT referring to MyArray[2].

Hot Standby and Redundancy

OPC UA Server Redundancy

Two Types of Redundancy

The BMENUA0100 module supports the following types of redundancy:

- Hot Standby architecture, which describes redundant controllers.
- OPC UA server redundancy, which describes the use of redundant BMENUA0100 modules.

The redundancy of OPC UA servers, which is managed by the BMENUA0100 modules, follows the OPC UA standard “non-transparent server redundancy in warm failover mode” as defined by the OPC Foundation.

These two types of redundancy can be combined. The following designs are supported:

- A standalone controller, containing two BMENUA0100 modules.
- Two Hot Standby controllers, each containing one or two BMENUA0100 modules.

OPC UA Redundancy

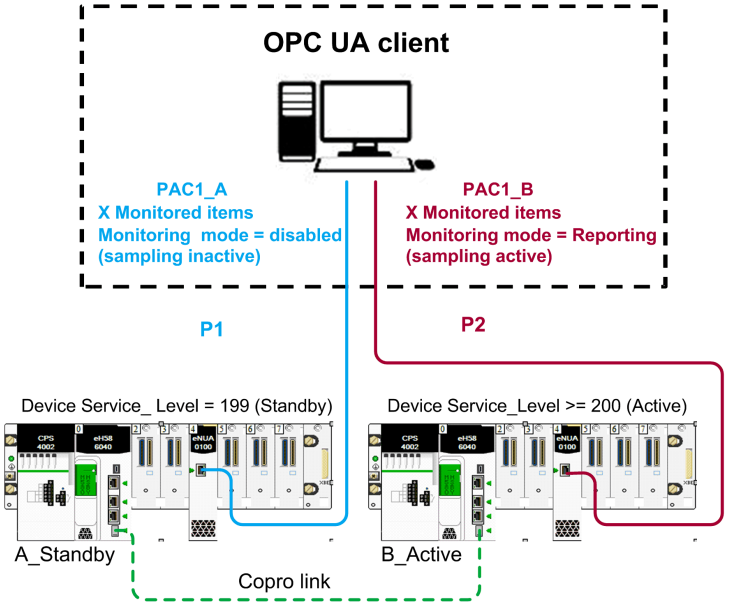
In an OPC UA non-transparent server redundant architecture in warm failover mode, the OPC UA client establishes sessions and manages communications with redundant servers. The sessions to be established include: an active session with the primary server and an inactive session with the secondary (or standby) server. The client must be configured for these two sessions to include the same monitored items.

The OPC UA client verifies the status of the two servers via the SERVICE_LEVEL variable, and switches the communication to the healthier server, depending on the value of this variable.

The OPC UA standard holds that the activation of communications is accomplished by adjusting the *Monitoring Mode* of the different sessions to the right value. The *Monitoring Mode* of the servers is controlled by the OPC UA client, and the procedure for adjusting it depends on the implementation of the client. For more information about adjusting *Monitoring Mode*, refer to the OPC UA client documentation.

This principle is a general principle, and applies to any architecture, including a Hot Standby architecture.

The following diagram depicts an OPC UA client connected to a pair of redundant OPC UA servers (each embedded in a BMENUA0100 module). The client has designated as the active server the one with the higher SERVICE_LEVEL value:



Hot Standby

In a Hot Standby configuration, a maximum of two BMENUA0100 modules can be installed in each Hot Standby main local rack. Each BMENUA0100 module is configured with a unique, static IP address. The BMENUA0100 modules retain their respective IP addresses, and do not exchange IP addresses on a Hot Standby switchover or swap.

NOTE: In a Hot Standby system, verify that the BMENUA0100 modules in the primary and the standby controllers:

- Are configured with identical cybersecurity settings, page 84, and
- Have their rotary selector switches, page 23 (located on the back of the module) set to the same position.
- Are installed in the same slot number, page 60 in their respective local main racks.

If these conditions do not exist, the module cannot retrieve its configuration set by Control Expert and stored in the controller and it would start in standalone mode. The system does not automatically perform these verifications.

The BMENUA0100 module DDT includes the SERVICE_LEVEL, page 147 variable, which provides information to the controller regarding the health of the OPC UA server in the BMENUA0100 module. The OPC UA client is informed of the status of the OPC UA server via the SERVICE_LEVEL variable, which is available as an OPC UA variable.

NOTE: Include the READ_DDT elementary function, for the purpose of updating the DDT of each BMENUA0100 module. In a Hot Standby configuration, add the READ_DDT to a code section that executes when the controller is in standby mode. This design returns BMENUA0100 diagnostic information that can be exchanged between the primary and standby controllers. The application can use this information to perform a consistency verification of the supported services and the cybersecurity configurations for the BMENUA0100 modules in the primary and standby controllers.

If the Hot Standby controller T_M_ECPU_HSBY DDT (see Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures) and its CMD_SWAP element are made available as HMI variables in a SCADA system, the SCADA application can trigger a swap by writing to the appropriate mapped OPC UA variable in the BMENUA0100.

In a Hot Standby system, the BMENUA0100 module that manages OPC UA communications with the SCADA may be the one located in the standby local rack. For this reason, you need to select the **Exchange on STBY** attribute for all scanned application variables to provide consistency of variable values between the primary and standby controllers.

In addition, to maintain consistency, the applications in the two Hot Standby controllers need to be synchronized.

In rare cases (primarily when the ECPU_HSBY_1.PLCX_ONLINE bit is set to FALSE either manually or programmatically), one of the controllers in a Hot Standby system may be in Wait mode. In this mode, this controller (the standby) is not synchronized with the primary controller and variables read from this controller are inaccurate. The state of a responding controller may be monitored via the following T_M_ECPU_HSBY DDT fields:

- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.WAIT
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_PRIMARY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.RUN_STANDBY
- T_M_ECPU_HSBY_1.LOCAL_HSBY_STS.STOP

Also, the Hot Standby system permits the two controllers to operate while running different applications. To provide for the consistency of variables between the primary and standby controllers, the data layout of the 2 controllers needs to be consistent, as shown by the T_M_ECPU_HSBY DDT field:

- T_M_ECPU_HSBY_1.DATA_LAYOUT_MISMATCH = FALSE

  NOTE: When OPC UA redundancy is configured, programmatically verify the module DDTs to confirm that the supported services and the cybersecurity configurations for the BMENUA0100 modules are consistent.

OPC UA Support for Redundant Servers, Clients, and Networks

As stated in the OPC Unified Architecture Specification Part 4: Services, Release 1.04, “OPC UA enables Servers, Clients and networks to be redundant. OPC UA provides the data structures and Services by which Redundancy may be achieved in a standardized manner.”

“Server Redundancy allows Clients to have multiple sources from which to obtain the same data. Server Redundancy can be achieved in multiple manners, some of which require Client interaction, others that require no interaction from a Client. Redundant Servers could exist in systems without redundant networks or Clients. Redundant Servers could also coexist in systems with network and Client Redundancy...”

“Client Redundancy allows identically configured Clients to behave as if they were single Clients, but not all Clients are obtaining data at a given time. Ideally there should be no loss of information when a Client Failover occurs. Redundant Clients could exist in systems without redundant networks or Servers. Redundant Clients could also coexist in systems with network and Server Redundancy...”

“Network Redundancy allows a Client and Server to have multiple communication paths to obtain the same data. Redundant networks could exist in systems without redundant Servers or Clients. Redundant networks could also coexist in systems with Client and Server Redundancy... OPC UA Part 4, section 6.6.1.”

Server Redundancy

As stated in the OPC Unified Architecture Specification Part 4: Services, Release 1.04, “There are two general modes of Server Redundancy, transparent and non-transparent.”

“In transparent Redundancy the Failover of Server responsibilities from one Server to another is transparent to the Client. The Client is unaware that a Failover has occurred and the Client has no control over the Failover behaviour. Furthermore, the Client does not need to perform any actions to continue to send or receive data.”

“In non-transparent Redundancy the Failover from one Server to another and actions to continue to send or receive data are performed by the Client. The Client must be aware of

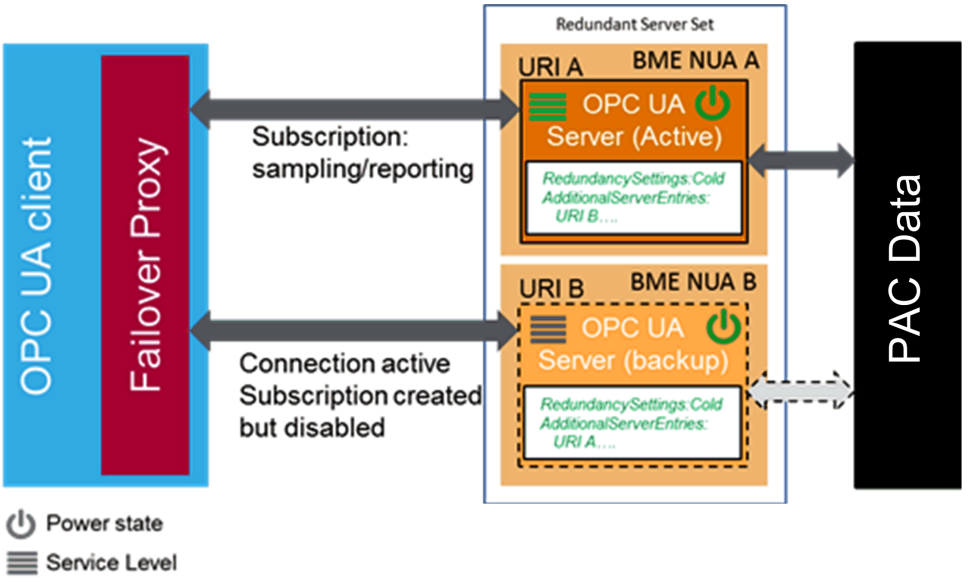
the Redundant Server Set and must perform the required actions to benefit from the Server Redundancy."

"The ServerRedundancy Object ... indicates the mode supported by the Server. The ServerRedundancyType ObjectType and its subtypes TransparentRedundancyType and NonTransparentRedundancyType ... specify information for the supported Redundancy mode. OPC UA Part 4, section 6.6.2"

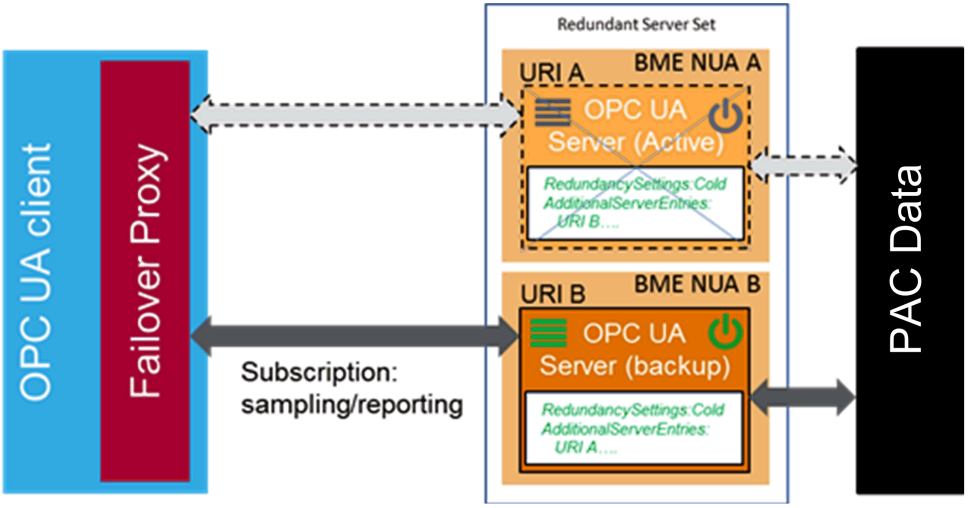
As noted above, the OPC UA server in the BMENUA0100 supports non-transparent server redundancy in warm failover mode.

OPC UA Server Warm Failover Mode

As stated in the OPC Unified Architecture Specification Part 4: Services, Release 1.04, warm failover mode "is where the backup Server(s) can be active, but cannot connect to actual data points." Therefore, only a single server will be able to consume data of the Control Expert application. "The ServiceLevel Variable ... indicates the ability of the Server to provide its data to the Client." OPC UA Part 4, section 6.6.2.4.4



When there is failover, action by the OPC UA client is needed; the OPC UA server embedded in BMENUA0100 becomes inactive:



Client Failover Behavior

As stated in the OPC Unified Architecture Specification Part 4: Services, Release 1.04, “Each Server maintains a list of ServerUris for all redundant Servers in the Redundant Server Set.”

NOTE: A Redundant Server Set is the collection of OPC UA servers in the Control Expert application that are configured to provide redundancy.

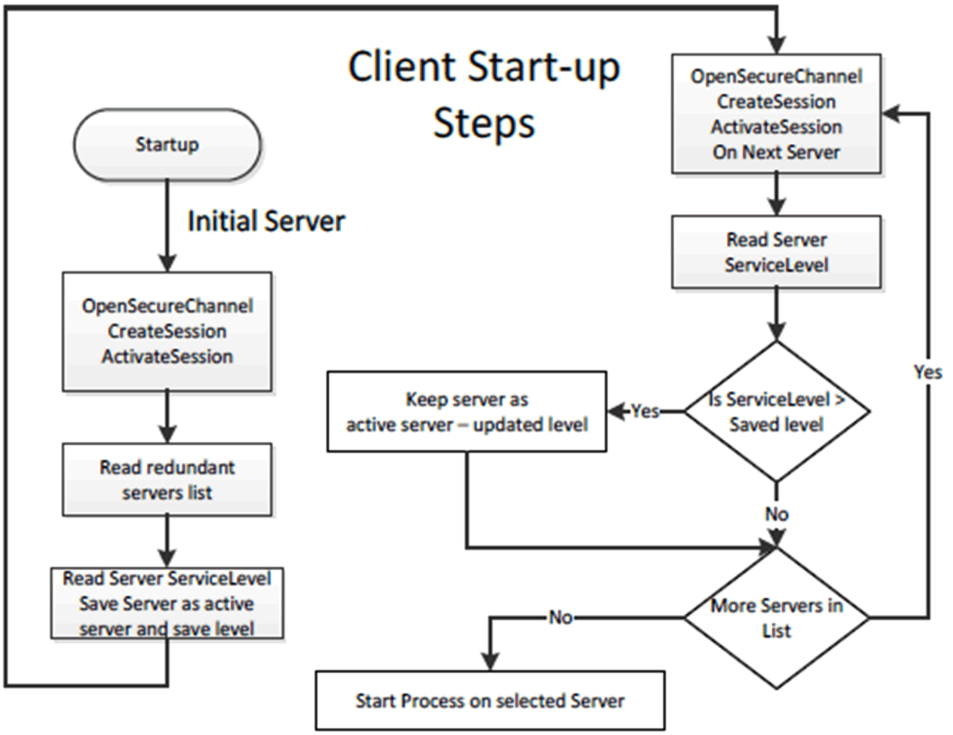
“The list is provided together with the Failover mode in the ServerRedundancy Object. To enable Clients to connect to all Servers in the list, each Server in the list shall provide the ApplicationDescription for all Servers in the Redundant Server Set through the FindServers Service. This information is needed by the Client to translate the ServerUri into information needed to connect to the other Servers in the Redundant Server Set. Therefore, a Client needs to connect to only one of the redundant Servers to find the other Servers based on the provided information. A Client should persist information about other Servers in the Redundant Server Set. OPC UA Part 4, section 6.6.2.4.5.1”

Client options in warm failover mode include:

- On initial connection, in addition to actions on Active Server:
  - Connect to more than one OPC UA Server.
  - Create Subscriptions and add monitored items.

- At failover:
  - Activate sampling on the subscriptions.
  - Activate publishing.

“Clients communicating with a non-transparent Redundant Server Set of Servers require some additional logic to be able to handle Server failures and to Failover to another Server in the Redundant Server Set. The following figure provides an overview of the steps a Client typically performs when it is first connecting to a Redundant Server Set.”



“The initial Server may be obtained via standard discovery or from a persisted list of Servers in the Redundant Server Set. But in any case the Client needs to check which Server in the Server set it should connect to. Individual actions will depend on the Server Failover mode the Server provides and the Failover mode the Client will make use.”

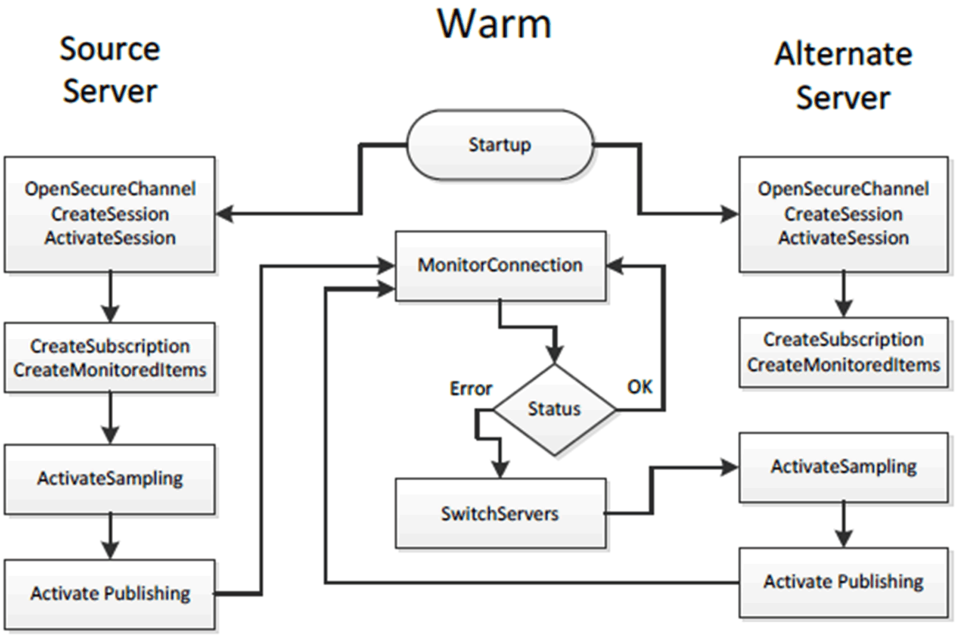
“Clients once connected to a redundant Server have to be aware of the modes of Failover supported by a Server since this support affects the available options related to Client behaviour. A Client may always treat a Server using a lesser Failover mode, i.e. for a Server that provide Hot Redundancy, a Client might connect and choose to treat it as if the Server was running in Warm Redundancy or Cold Redundancy. This choice is up to the client. In the case of Failover mode HotAndMirrored, the Client shall not use Failover mode Hot or

Warm as it would generate unnecessary load on the Servers. OPC UA Part 4, section 6.6.2.4.5.1”

OPC UA Client Warm Failover Mode

As stated in the OPC Unified Architecture Specification Part 4: Services, Release 1.04, in Warm Failover mode, “the Client should connect to one or more Servers in the Redundant Server Set primarily to monitor the ServiceLevel. A Client can connect and create Subscriptions and MonitoredItems on more than one Server, but sampling and publishing can only be active on one Server. However, the active Server will return actual data, whereas the other Servers in the Redundant Server Set will return an appropriate error for the MonitoredItems in the Publish response such as Bad_NoCommunication. The one Active Server can be found by reading the ServiceLevel Variable from all Servers.”

“The Server with the highest ServiceLevel is the Active Server. For Failover the Client activates sampling and publishing on the Server with the highest ServiceLevel. Figure 30 illustrates the steps a Client would perform when communicating with a Server using Warm Failover mode.”



OPC UA Part 4, section 6.6.2.4.5.3

Supported Architectures

Introduction

This chapter describes the topological architectures supported by the BMENUA0100 Ethernet communication module with embedded OPC UA server.

Supported BMENUA0100 Module Configurations

Placement of the BMENUA0100 Module

The BMENUA0100 module can be placed into an Ethernet slot on the local main rack (i.e. in the same rack as the controller) in the following configurations:

- an M580 standalone configuration.
- an M580 standalone Safety controller configuration.
- an M580 Hot Standby configuration.
- an M580 Hot Standby Safety controller configuration.

NOTE:

- The BMENUA0100 module can be used with all M580 controllers.
- In the event a network loop is created, the BMENUA0100 module goes into NOCONF (Not configured) state. To help prevent loops and related events, when you use the BMENUA0100 control port, split the control port network and the controller backplane network physically (via wiring splitting) and not only logically (via the subnet and subnet mask settings).

Connecting via the HTTPS Protocol

If your application experiences connection problems, consult your local IT support to confirm that your network configuration and security policies are consistent with HTTPS (port 443) access to the BMENUA0100 module IP address.

The BMENUA0100 module accepts the HTTPS connections with transport layer security (TLS) protocol v1.2 or later. For example, Windows 7 could require an update to enable TLS 1.2 to upgrade the firmware of the BMENUA0100 or access to its website.

Installation of the BMENUA0100 Module in a Flat Network

For multiple M580 racks connected on a single subnet (i.e., a flat network architecture) that include BMENUA0100 modules with the control port disabled, install each BMENUA0100 module in a different slot number in its respective rack (except for Hot Standby configurations, where the BMENUA0100 modules are installed in the same slot number). Alternatively, use a router to isolate the racks and thereby avoid potential address conflicts with the BMENUA0100 modules.

Adding Prefixes to Device (Role) Names in Flat Network Designs

When an architecture includes multiple BMENUA0100 modules, which communicate with other devices, such as M580 controllers that are configured on the same subnet, use prefixes for the device (or role) name of the devices, including M580 controllers. This naming convention makes it possible for BMENUA0100 modules to differentiate among the M580 controllers, and determine which controller is placed on which rack. This naming convention helps eliminate uncertainty relating to a flat network design. For example, without unique prefixes, a BMENUA0100 module cannot determine which M580 controller it should communicate with for retrieving its own configuration after an application download.

The device name prefix can be set in Control Expert in the tab **Tools > Project Settings > Configuration**.

Access to the BMENUA0100 embedded OPC UA Server

In the topological architectures described in this chapter, the BMENUA0100 communication module Ethernet backplane port and its control port can be used to provide access to the OPC UA server embedded in the module. For a description of when these ports can be used to access the embedded OPC UA server, refer to the descriptions of the Control port and the Ethernet backplane port in the topic External Ports, page 21.

Maximum Number of BMENUA0100 modules per Configuration

The maximum number of BMENUA0100 modules supported in an M580 configuration are:

M580 Configuration Type	Maximum Number of BMENUA0100 Modules
Standalone	Two in the local main rack for both standalone[1] and Hot Standby[1,2] standard and safety configurations.
Safety controller	
Hot Standby	
Hot Standby Safety controller	

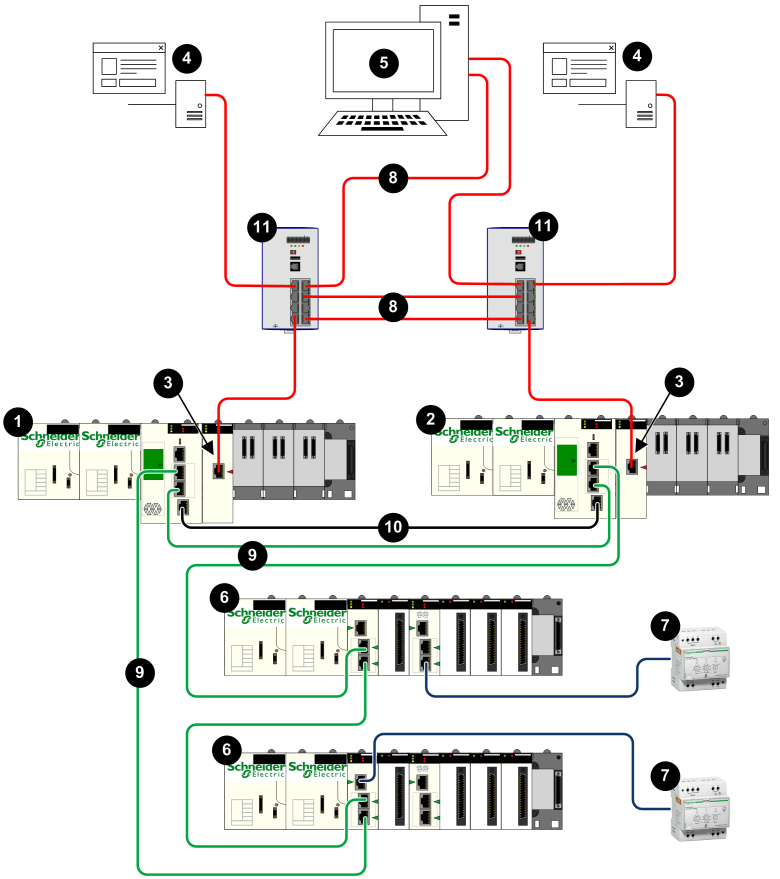
1. When two BMENUA0100 modules are used in a main rack:
   - Performance of each module will be slower than if a single module had been used.
   - Enable the control port in the configuration for both modules.
2. In Hot Standby configurations, place the BMENUA0100 module(s) in the same slot number(s) in the respective local main racks.

Change Configuration on the Fly (CCOTF)

The BMENUA0100 module does not support CCOTF.

Isolated Control Network with M580 Hot Standby Controllers

Architecture



1 Primary Hot Standby controller

2 Standby Hot Standby controller

3 BMENUA0100 Ethernet communications module with embedded OPC UA server

4 OPC UA client (SCADA system)

5 Engineering workstation with dual Ethernet connections

6 X80 Ethernet RIO drop

7 Distributed equipment

8 Control network

9 Ethernet RIO main ring

10 Hot Standby communication link

11 Dual ring switch (DRS)

Description

This architecture provides redundant connections to dual OPC UA clients (SCADA systems). Cybersecurity can be either enabled or disabled in this architecture. The control network (8) is logically isolated from both the Ethernet devices that reside in the Ethernet RIO main ring (9), including the controller, and the distributed Ethernet devices (7). This is accomplished at the Network layer of the OSI model via IP addressing.

The BMENUA0100 control port (3), with its dual IPv6/IPv4 stacks, allows upstream connectivity to the control network. When communicating via IPv6, it supports both stateless address auto-configuration (SLAAC) and static IP addressing.

The BMENUA0100 provides Modbus peer-to-peer communication between the two Hot Standby controllers. The controller ports provide downstream connectivity to the Ethernet devices on the Ethernet RIO main ring.

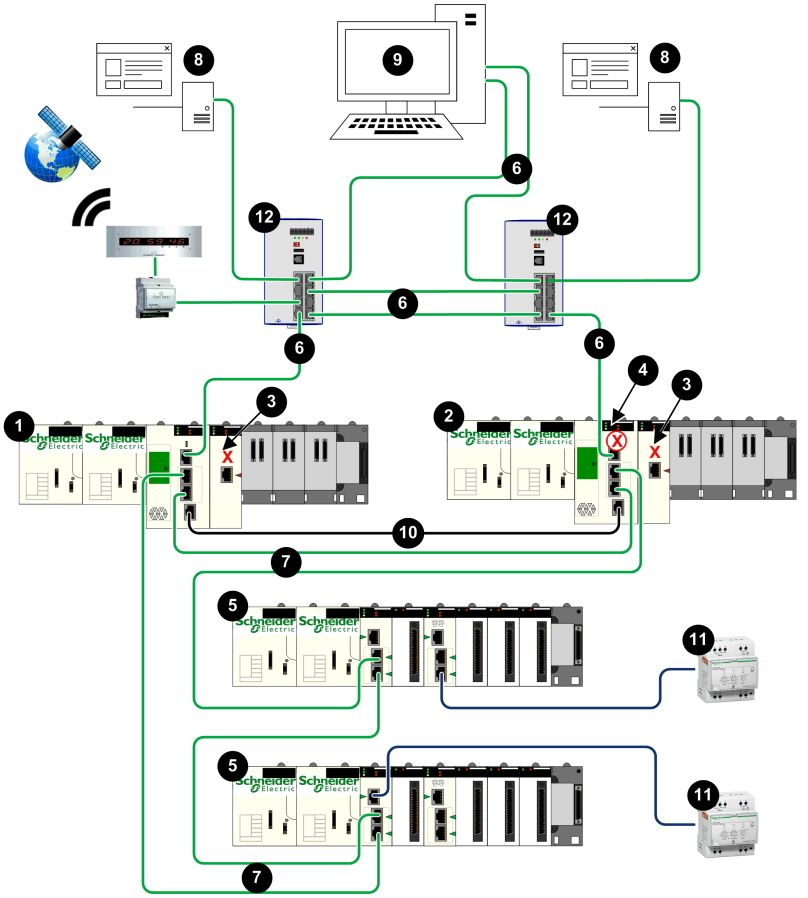
Each BMENUA0100 is a client of an NTP server that resides in the control network. The connection is made through the BMENUA0100 control port. The BMENUA0100 modules also serve as NTP servers for other devices in the Ethernet RIO main ring. In this Hot Standby design, the BMENUA0100 module configured as “A” acts is the primary NTP server, and the BMENUA0100 module configured as “B” acts is the standby NTP server. In this way, the controller time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the controller, which converts the raw record data and stores it in a

usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Non-Isolated Flat Network with M580 Hot Standby

Architecture



1 Primary Hot Standby controller

2 Standby Hot Standby controller

3 BMENUA0100 with control port disabled

4 Standby controller with automatic blocking of service port

5 X80 Ethernet RIO drop

6 Control network

7 Ethernet RIO main ring

8 OPC UA client (SCADA system)

9 Engineering workstation with dual Ethernet connections

10 Hot Standby communication link

11 Distributed equipment

12 Dual ring switch (DRS)

Description

This architecture provides redundant connections from M580 Hot Standby controllers to dual OPC UA clients (SCADA systems). Its primary purpose is to provide high availability to the Hot Standby controllers. For that reason, this architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port. Upstream communication from the Hot Standby controllers to the SCADA servers is accomplished via the primary controller service port. The controller ports provide downstream connectivity to the Ethernet devices on the Ethernet RIO main ring.

The standby controller service port (4) is disabled, which is accomplished by using the Control Expert configuration software to select **Automatic blocking of service port on Standby CPU** in the **ServicePort** tab of the configuration for both the primary and standby controllers.

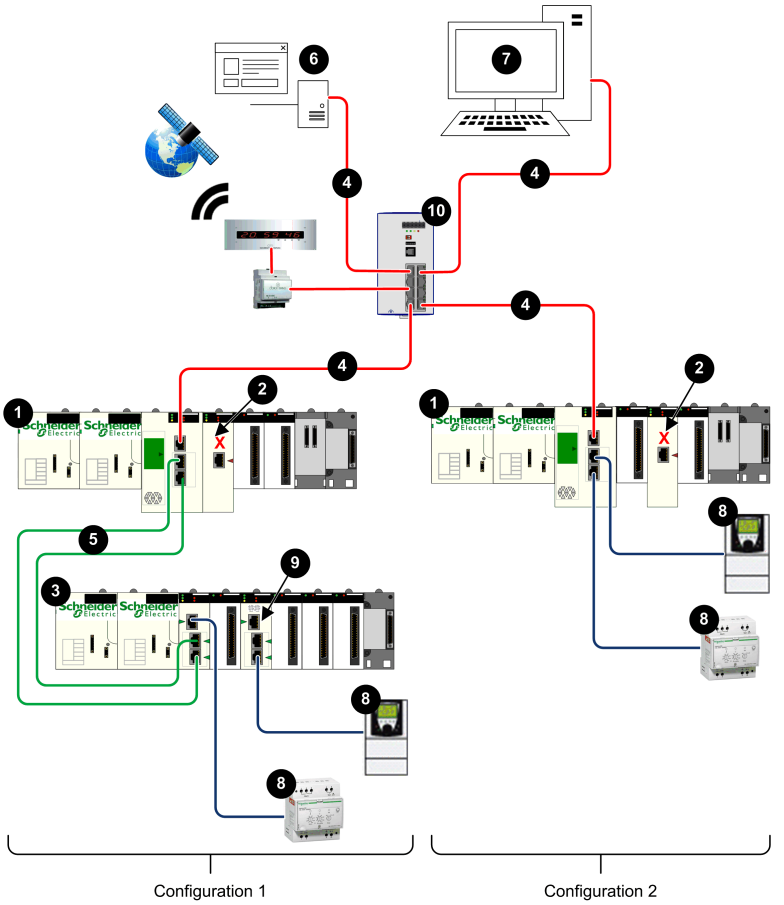
NOTE: The service port of the standby controller is disabled to help prevent the unintended creation of an Ethernet communications loop, where both the control network and the Ethernet RIO main ring are part of the same subnet. Refer to the *M580 Hot Standby System Planning Guide* and the topic Managing Flat Ethernet Networks with M580 Hot Standby (see *Modicon M580 Hot Standby, System Planning Guide for, Frequently Used Architectures*) for additional information.

In this flat network design, all devices, including the controller, BMECRA31310 modules, and the BMENUA0100 can be clients of the same NTP server that resides in the control network. Hence, controller time is synchronized with the BMENUA0100 module.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the controller, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with Multiple M580 Standalone Controllers and Single SCADA

Architecture



1 Standalone controller

2 BMENUA0100 with control port disabled

3 X80 Ethernet RIO drop

4 Control network

5 Ethernet RIO main ring

6 OPC UA client (SCADA system)

7 Engineering workstation with single Ethernet connection

8 Distributed equipment

9 BMENOS0300 switch

10 Dual ring switch (DRS)

Description

This architecture provides a connection to a single OPC UA client (a SCADA system) from multiple M580 standalone controllers. It is a cost-optimized architecture that does not require high availability. This architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled for each standalone controller. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port. Upstream communication from each controller to the single SCADA server is accomplished via the controller service port.

In configuration 1, downstream connectivity from the controller to the X80 Ethernet RIO drop (4) from the controller is provided by the controller dual device network ports. Further downstream connectivity is provided from the BMECRA31310 module service port and a BMENOS0300 switch (9) to distributed Ethernet equipment.

In configuration 2, downstream connectivity is provided by the dual device network ports to distributed Ethernet equipment.

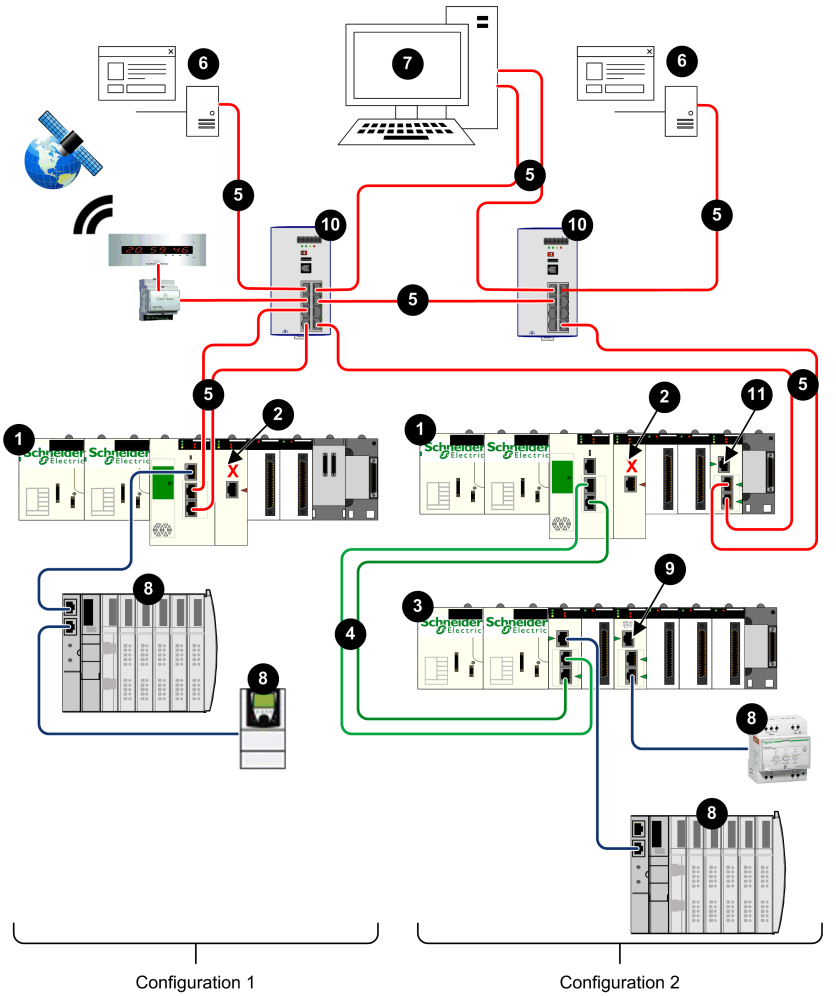
In this flat network design, all network devices – including the controller, BMECRA31310 modules and the BMENUA0100 – are NTP clients of an NTP server that resides in the control network. As a result, the controller time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the controller, which converts the raw record data and stores it in a

usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with Multiple M580 Standalone Controllers and Redundant SCADA

Architecture



1 Standalone controller

2 BMENUA0100 with control port disabled

3 X80 Ethernet RIO drop

4 Ethernet RIO main ring

5 Control network

6 OPC UA clients (SCADA systems)

7 Engineering workstation with dual Ethernet connections

8 Distributed equipment

9 BMENOS0300 switch

10 Dual ring switch (DRS)

11 BMENOS0300, BMENOC0301, or BMENOC0311 module

Description

This architecture provides high availability of the control network, via redundant connections between OPC UA clients (SCADA systems) and multiple M580 standalone controllers. This architecture presents a non-isolated flat network, joining together the control network and the Ethernet RIO main ring in a single subnet.

The BMENUA0100 control port is disabled for each standalone controller. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

In configuration 1, upstream communication to the SCADA servers is accomplished via the dual controller device network ports, using the RSTP redundancy protocol to assign roles to each port to avoid logical Ethernet loops. Downstream connectivity to the Ethernet distributed equipment is provided by the controller service port.

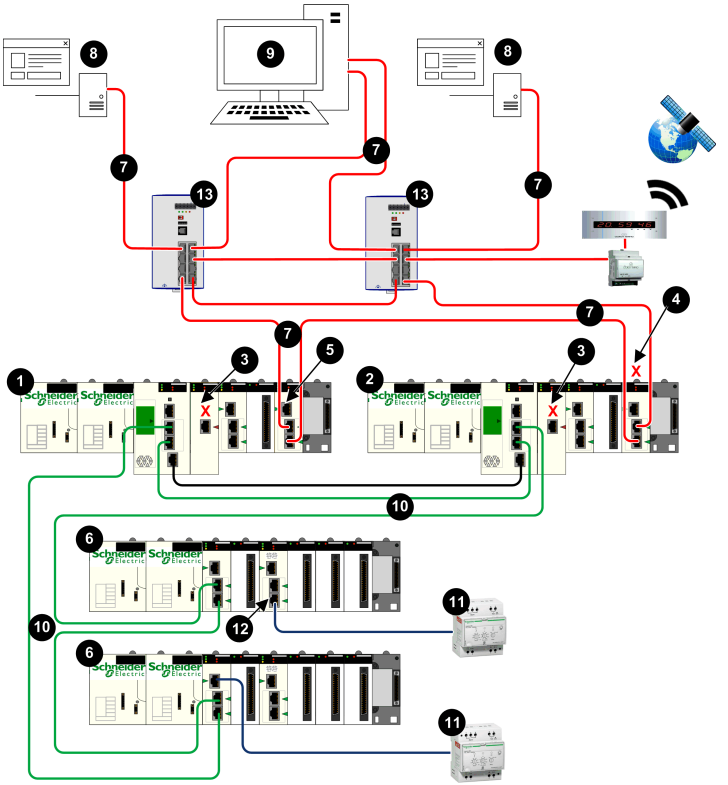
In configuration 2, upstream connectivity to the SCADA servers is provided by the device network ports of a BMENOS0300, BMENOC0301, or BMENOC0311 module. The RSTP redundancy protocol is used to assign roles to each port to avoid logical Ethernet loops. Downstream connectivity from the controller is provided from the controller device network ports to the X80 Ethernet remote I/O drop. Further downstream connectivity is provide by both the BMECRA31310 module service port and a BMENOS0300 switch (9) to distributed Ethernet equipment.

In this flat network design, all network devices – including the controller, BMECRA31310 modules and the BMENUA0100 – are NTP clients of an NTP server that resides in the control network. As a result, the controller time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the controller, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Flat Network with M580 Hot Standby Controllers and Redundant SCADA

Architecture



1 Primary Hot Standby controller

2 Standby Hot Standby controller

3 BMENUA0100 with control port disabled

4 BMENOS0300,BMENOC0301, or BMENOC0311 with backplane port disabled

5 BMENOS0300, BMENOC0301, or BMENOC0311 with backplane port enabled

6 X80 Ethernet RIO drop

7 Control network

8 OPC UA client (SCADA system)

9 Engineering workstation with dual Ethernet connections

10 Ethernet RIO main ring

11 Distributed equipment

12 BMENOS0300 switch

13 Dual ring switch (DRS)

Description

This architecture provides high availability with redundant connections linking redundant OPC UA clients (SCADA systems) to redundant Hot Standby controllers in a single subnet.

Each controller is connected to SCADA via either a BMENOS0300, BMENOC0301, or BMENOC0311 module. To help avoid Ethernet loops, the backplane port of one of the BMENOS0300, BMENOC0301, or BMENOC0311 modules is disabled. In this example, it is the module in the standby controller (4) has a disabled backplane port. Additionally, RSTP redundancy protocol is used to assign roles to each port to help avoid logical Ethernet loops.

The BMENUA0100 control port is disabled (3) for each standalone controller. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

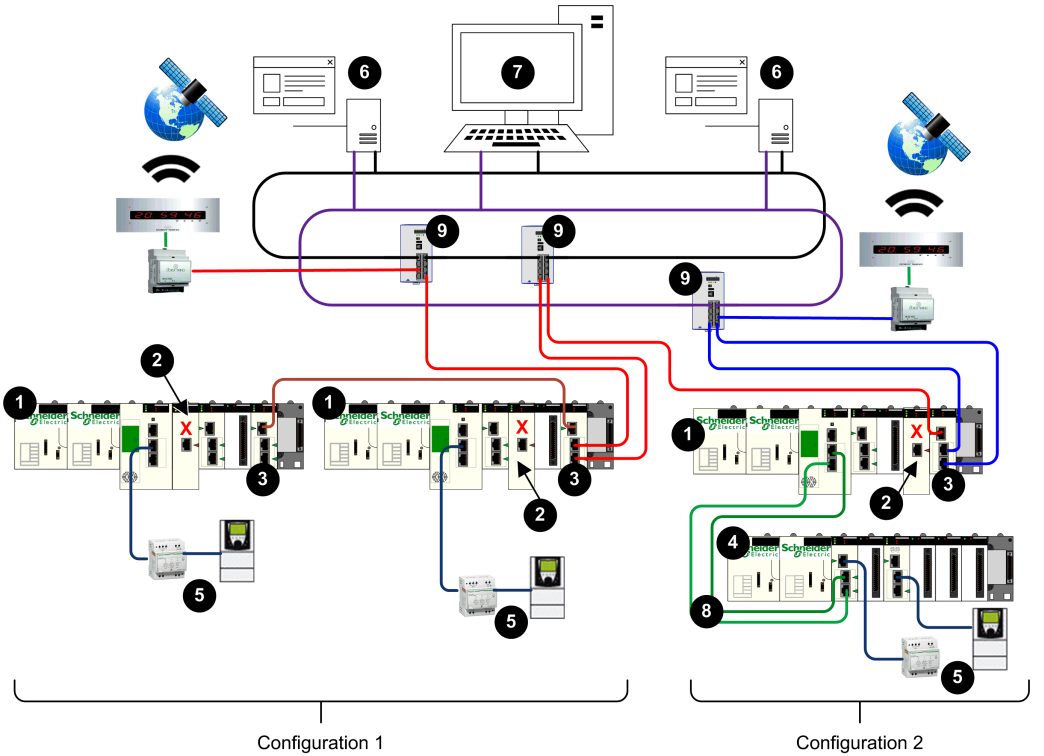
Downstream connectivity to the X80 Ethernet RIO drops is provided by the controller device network ports. Further downstream connectivity from the X80 Ethernet RIO drops is provided by both the CRA service port and a BMENOS0300 switch (12) to distributed Ethernet equipment.

In this flat network design, all network devices – including each Hot Standby controller and BMENUA0100 module – are NTP clients of an NTP server that resides in the control network. As a result, the controller time and the BMENUA0100 module time are synchronized.

The BMENUA0100 supports applicative time stamping. In this process, time stamping modules record events in their local buffer. These time stamped events are consumed by the application running in the controller, which converts the raw record data and stores it in a usable format. The formatted records can then be consumed by a supervisory application, such as a SCADA system.

Hierarchical Network featuring Multiple M580 Standalone Controller Connected to Control Network and Redundant SCADA

Architecture



1 Standalone controller

2 BMENUA0100 with control port disabled

3 BMENOC0321 Ethernet communications module

4 X80 Ethernet RIO drop

5 Distributed equipment

6 OPC UA client (SCADA system)

7 Engineering workstation with dual Ethernet connections

8 Ethernet RIO main ring

9 Dual ring switch (DRS)

Description

This architecture features a hierarchical network, which relies on BMENOC0321 communication modules to route network traffic between subnets. Upstream communication from the controllers to the OPC UA clients (SCADA systems) is accomplished via the dual device network ports of the BMENOC0321 module, using the RSTP redundancy protocol to avoid logical Ethernet loops.

NOTE: This architecture requires the configuration of static routes in the control network equipment to redirect the various subnets of the several controllers.

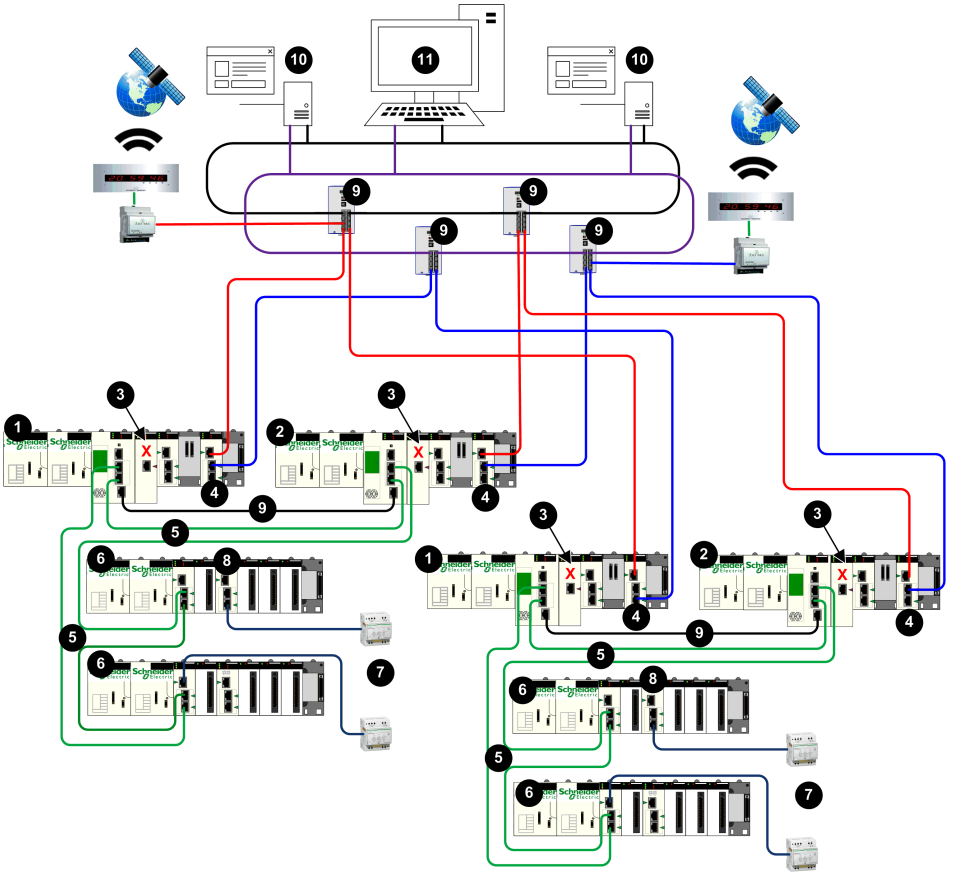
The BMENUA0100 control port (2) is disabled for each standalone controller. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

Configuration 1 includes two controllers that reside in the same subnet. This configuration employs the BMENOC0321 module to provide redundant upstream communications to the redundant SCADA servers. The BMENOC0321 module employs the RSTP redundancy protocol to avoid logical Ethernet loops. The dual device network ports of the two controllers provide downstream communication to the distributed Ethernet equipment.

Configuration 2 includes a single controller, with X80 Ethernet RIO drop. This controller uses the BMENOC0321 module for upstream communication to the redundant SCADA servers. The BMENOC0321 accomplishes this using two independent subnets. Downstream communication from the X80 Ethernet RIO drop is provided by both the BMECRA31310 module service port and a BMENOS0300 switch to distributed Ethernet equipment.

Hierarchical Network with Multiple M580 Hot Standby Controllers and Redundant SCADA Connections

Architecture



1 Primary Hot Standby controller

2 Standby Hot Standby controller

3 BMENUA0100 with control port disabled

4 BMENOC0321 Ethernet communications module

5 Ethernet RIO main ring

6 X80 Ethernet RIO drop

7 Distributed equipment

8 BMENOS0300 switch

9 Dual ring switch (DRS)

10 OPC UA client (SCADA system)

11 Engineering workstation with dual Ethernet connections

Description

This architecture features a hierarchical network, which relies on BMENOC0321 communication modules (4) to route network traffic between subnets. Upstream communication from the Hot Standby controllers to the OPC UA clients (SCADA systems) is accomplished via the dual device network ports of the BMENOC0321 modules, using the RSTP redundancy protocol to avoid logical Ethernet loops.

NOTE: This architecture requires the configuration of static routes in the control network equipment to redirect the various subnets of the several controllers.

The BMENUA0100 control port (3) is disabled for each controller. IPv4 Ethernet communication to the BMENUA0100 module is provided over the backplane port.

This configuration employs the BMENOC0321 module to provide redundant upstream communications via redundant connections to the redundant SCADA servers. The dual device network ports of the controllers provide downstream communication to the X80 Ethernet RIO drops. Farther downstream communication from the X80 Ethernet RIO drop to the distributed Ethernet equipment is provided by both the BMECRA31310 service port and a BMENOS0300 switch (8).

Commissioning and Installation

Introduction

This chapter describes how to select an operating mode and install the BMENUA0100 Ethernet communications module with embedded OPC UA server.

Commissioning Checklist for the BMENUA0100 Module

Commissioning Checklist

The following outline presents a sequence of tasks to follow when commissioning and installing a new BMENUA0100 module. This example configures the module to operate in Self-Signed & CA PKI mode with both IPV6 SLAAC and IPV4 addresses:

1. Configure the Control Expert application, page 114.
2. Configure the router / SLAAC server (for IPV6 in SLAAC mode).
3. Select Advanced (or Secured) mode operations for the module:

a.	Set rotary switch, page 23 on the back of the module to the Advanced (or Secured) Mode, page 30 position.
b.	Install the module, page 82 into an Ethernet slot on the rack.

4. Configure the cybersecurity settings using the module web pages, page 84:

a.	Create the cybersecurity configuration using the Settings web page, page 92.
b.	Set the **PKI mode** to Self-Signed & CA.
c.	For client devices that do not support PKI, create a **Trusted Clients Certificates** list, page 109.
d.	**Apply** the configuration file.

5. Perform manual certificate enrollment, page 108:

a.	Generate a certificate signing request (CSR).
b.	Push the CA certificate.
c.	Push the device certificate.

6. Add the CA certificate to OPC UA client devices.
7. Test communication between the OPC UA client and server.

Commissioning the BMENUA0100 Module

Introduction

The BMENUA0100 module with embedded OPC UA server appears in the Control Expert hardware catalog as a communications module. It consumes one I/O channel.

When a BMENUA0100 module comes from the factory, its cybersecurity operating mode is set to Advanced (or Secured) Mode by default. To configure the new module for Advanced (or Secured) Mode operations, follow the scenario for Advanced (or Secured) Mode Commissioning, page 30 set forth below.

To change the cybersecurity operating mode for a module that has previously been configured, including a new module you plan to configure for Standard mode operations, perform a Cybersecurity Reset (or Security Reset) operation, page 80 for the module. After the Cybersecurity Reset (or Security Reset) operation, you can follow the scenario for either Advanced (or Secured) Mode Commissioning, page 30 or Standard Mode Commissioning, page 30.

Advanced (or Secured) Mode Commissioning

Commissioning a BMENUA0100 module to operate in Advanced (or Secured) Mode, requires the completion of two configuration processes:

- Cybersecurity configuration, using the module web pages.
- IP address, NTP client, and SNMP agent configuration, using the Control Expert configuration tool.

Only a Security Administrator, using the Advanced (or Secured) Mode default username / password combination, page 31 can commission the module in Advanced (or Secured) Mode.

NOTE: Perform these configuration processes in following order:

- Use Control Expert to configure the control and backplane IP addresses.
- Use the module webpages to configure the cybersecurity settings.
- Use Control Expert to complete the NTP client and SNMP agent configurations.

NOTE: For commissioning in Advanced (or Secured) Mode with manual enrollment, refer to the topic Manual Enrollment, page 108.

The following procedure is intended for a new module that has not been previously configured. If you are using a module that has previously been configured, perform a Cybersecurity Reset (or Security Reset) operation, page 80 before proceeding with the following steps.

To commission the module in Advanced (or Secured) mode:

1. Configure IP address settings:

a.	Open the Control Expert configuration tool.
b.	In Control Expert, create a **New Project** add a BMENUA0100 module to the project from the **Hardware Catalog** then configure the IP address settings, page 114.

2. Configure cybersecurity settings:

a.	With the module detached from the rack, use the plastic screwdriver that ships with the module, page 23 to set the rotary switch to the **Advanced (or Secured)** position.
b.	Install, page 81 the module into an Ethernet slot on the local, main Ethernet rack and cycle power.
c.	Use your Internet browser to connect your configuration PC to the module, using either the control port or the backplane port, and navigate to the module web pages at the configured IP address.
d.	If your Internet browser displays a message, page 86 indicating a potential security risk, read the message, and if you agree, proceed to make the connection by clicking **Accept the Risk and Continue** (or similar, browser-specific language).
e.	In the user login page, enter the default username / password combination, page 31.
f.	Change and confirm the password. Refer to the User Management topic, page 111 for password requirements. The module **Home** page, page 89 is displayed.
g.	Starting from the **Home** page, navigate to the module web pages and configure its cybersecurity settings.

3. Configure NTP client, and SNMP agent settings:

a.	Open the Control Expert configuration tool.
b.	In Control Expert, configure the NTP client, and SNMP agent settings., page 114
c.	When the Control Expert project configuration is complete, connect to the controller and transfer the project to the controller.

NOTE: When the configuration is loaded in the BMENUA0100 module the module state changes from NOT CONFIGURED to CONFIGURED. The **SECURE** LED, page 134 indicates if the module is not configured or configured, and if the OPC UA server is connected to an OPC UA client.

Standard Mode Commissioning

In Standard mode, a cybersecurity configuration is not required. The IP address, NTP client, and SNMP agent settings are configured using the Control Expert configuration tool. In Standard mode, the module begins to communicate when it is placed on the rack, power is applied, and it receives a valid configuration from Control Expert.

Use the default username / password combination, page 31 to commission the module in Standard mode.

To commission the module in Standard mode:

1. With the module detached from the rack, use the plastic screwdriver that ships with the module, page 23 to set the rotary switch to the **Standard** position.
2. Place the module into an Ethernet slot on the local, main Ethernet rack and cycle power.
3. Open the Control Expert configuration tool.
4. In Control Expert, create a **New Project**, add a BMENUA0100 module to the project from the **Hardware Catalog**, then configure the IP address, page 115, NTP client, page 124, and SNMP agent, page 127 settings.
5. When the Control Expert project configuration is complete, connect to the controller and transfer the project to the controller.

NOTE: When operating in Standard mode, the **SECURE** LED is OFF.

Cybersecurity Reset (or Security Reset) Operation

For a module that has previously been configured, or for a new module you want to configure for mode cybersecurity operations, perform a Cybersecurity Reset (or Security Reset) operation before proceeding with cybersecurity configuration. A reset operation sets the cybersecurity settings to their factory default values. You can perform a reset by using the module web pages, or the rotary switch located on the back of the module.

Web pages: For a BMENUA0100 module that is presently configured for Advanced (or Secured) Mode operations:

1. Navigate to the **Configuration Management > RESET** web page.
2. Click **Reset**.

NOTE: The Cybersecurity Reset (or Security Reset) operation is complete when the **RUN** LED is solid green, and both the **NS** control port LED and **BS** backplane port LED are solid red.

3. Cycle power to the module in one of the following ways:
   - Turn off power to the module rack, then turn power back on.
   - Physically remove the module from the rack, then re-insert it.

   You can now proceed with Advanced (or Secured) Mode commissioning.

Rotary Switch: For any BMENUA0100 module:

1. With the module detached from the rack, use the plastic screwdriver that ships with the module, page 23 to set the rotary switch to the **Cybersecurity Reset** position.
2. Install, page 81 the module into an Ethernet slot on the local, main Ethernet rack, and cycle power.

   NOTE: This restores the factory default settings to the module, including the control port default IP address, page 115 of 10.10.MAC5.MAC6. When the last two octets of the MAC address (*MAC5.MAC6*) correspond to *0.0* in the default address, make a point-to-point cable connection between your computer and the controller, communication module, or other module.

   Upon completion, the **RUN** LED is solid green, and both the **NS** control port LED and **BS** backplane port LED are solid red. You can turn off power, remove the module from the rack, and proceed with either Advanced (or Secured) Mode Commissioning, page 30 or Standard Mode Commissioning, page 30.

Installing the BMENUA0100

Introduction

You can install the BMENUA0100 module only into a local, Ethernet main rack by placing it into any Ethernet slot not reserved for the power supply or controller.

NOTE: If your application is based on EcoStruxure Control Expert version less than 15.3 and if your application includes multiple controllers (that are not Hot Standby controllers) each with a BMENUA0100 module, install the modules so that the slot number of each BMENUA0100 module is unique. For example, for an application that includes two controllers, if a BMENUA0100 module in the rack of controller 1 is placed into slot 4, place a BMENUA0100 module in the rack of controller 2 into a slot other than slot 4.

Grounding Precautions

Follow all local and national safety codes and standards.

⚠⚠DANGER

ELECTRIC SHOCK

Wear personal protective equipment (PPE) when working with shielded cables.

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

The backplane for your module is common with the functional ground (FE) plane and must be mounted and connected to a grounded, conductive backplane.

⚠WARNING

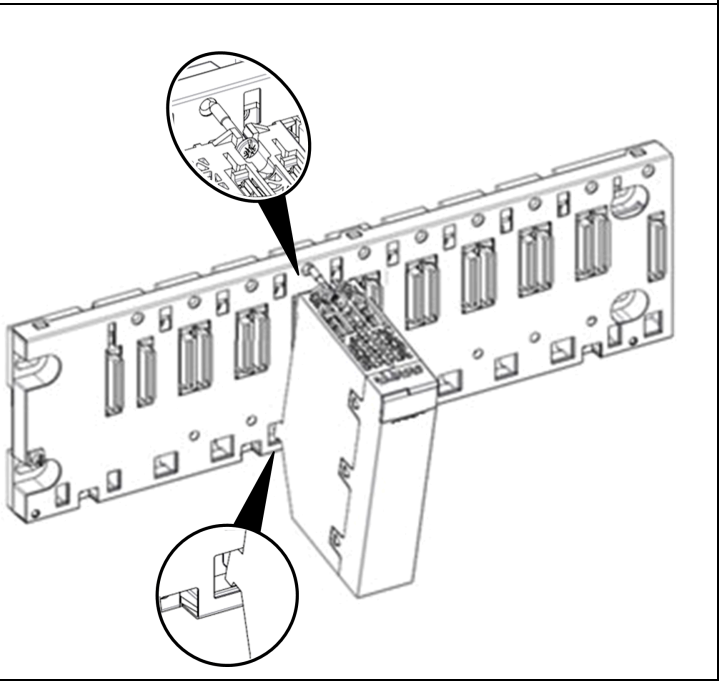
UNINTENDED EQUIPMENT OPERATION

Connect the backplane to the functional ground (FE) of your installation.

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

Installing a BMENUA0100 Module in the Rack

A BMENUA0100 module requires a single rack Ethernet slot. You can install the module into any Ethernet slot not reserved for the power supply or controller. Follow these steps to install a BMENUA0100 module in a rack:

Step	Action	
1	Position the locating pins situated at the bottom rear of the module in the corresponding slots on the rack.	
2	Swivel the module towards the top of the rack so that the module sits flush with the back of the rack. The module is now set in position.	
3	Tighten the single screw on top of the module to maintain the module in place on the rack. Tightening torque: 0.4...1.5 N•m (0.30...1.10 lbf-ft).	

Grounding the I/O Modules

For information on grounding, refer to the topic *Grounding the Rack and Power Supply Module* in the document *Modicon X80 Racks and Power Supplies Hardware Reference Manual*.

Configuration

Introduction

This chapter describes how to configure the BMENUA0100 Ethernet communications module with embedded OPC UA server.

Configuring the BMENUA0100 Cybersecurity Settings

Introduction

This section describes how to use the web pages of the BMENUA0100 Ethernet communication module with OPC UA server. Use the web pages to create a cybersecurity configuration for the module, and to view diagnostic data.

Introducing the BMENUA0100 Web Pages

Introduction

Use the BMENUA0100 web pages to create, manage and diagnose a cybersecurity configuration for the module, and to view event and OPC UA diagnostic data.

NOTE:

- The BMENUA0100 module web pages support HTTPS communication over IPv4 and IPv6 protocols, page 116.
- Use only recent versions of Internet browsers to access the web pages. Some older browsers, for example Internet Explorer v7 and earlier, are not supported.

  NOTE: The Chrome Internet Browser, version 123.0.6312.123 (build official) (64 bits) has been tested with the BMENUA0100 web pages.

For the BMENUA0100 module to operate in Advanced (or Secured) Mode, a cybersecurity configuration is required and must be performed before its IP address, NTP client, and SNMP settings can be configured using Control Expert, page 114. A cybersecurity configuration can be configured only locally for each BMENUA0100 module by connecting a configuration PC, running an HTTPS browser, to the BMENUA0100 module:

- Control port, if the control port is enabled.

- Backplane port (via a BMENOC0301or BMENOC0311 module or the controller), if the control port is disabled.

  NOTE: Before the BMENUA0100 module verifies the validity of the cybersecurity settings entered in the web pages, it first sets the IP address settings for both the control port and the backplane port that are configured in Control Expert, page 115.

For the BMENUA0100 module to operate in Standard mode, cybersecurity settings are not required and cannot be configured.

NOTE:

- When using a self-signed certificate, some browsers may report the connection between the PC and the module as “Unsecured”.
- For BMENUA0100 modules operating in Advanced (or Secured) Mode in a Hot Standby system, verify that the cybersecurity settings for the BMENUA0100 module in the primary controller are the same as the cybersecurity settings for the BMENUA0100 module in the standby controller. The system will not automatically perform this verification for you.

The accessibility of web pages depends on the cybersecurity operating mode:

Web Page or Group	Advanced (or Secured) Mode	Standard Mode
Home, page 89	✓	✓
Settings (device security), page 92	✓	–
Certificates Management, page 103	✓	–
Access Control, page 111	✓	–
Configuration Management, page 113	✓	–
Diagnostic, page 157	✓	✓
✓ : web pages are accessible. – : web pages are not accessible.		

Initial Configuration of Cybersecurity Settings

You can configure initial cybersecurity settings for a BMENUA0100 module that has:

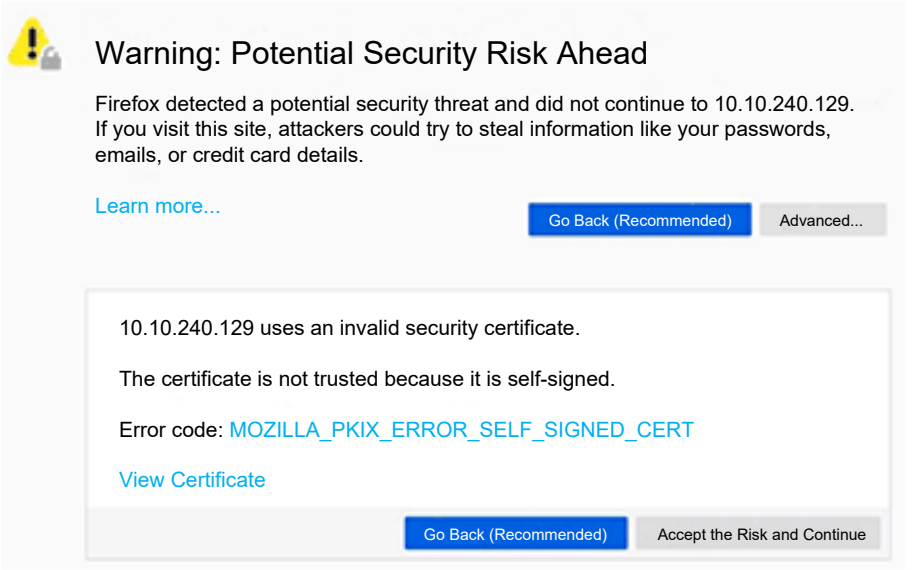
- Never been configured, and retains its initial factory default configuration.
- Previously been configured, but had its factory default configuration restored by executing the Cybersecurity (or Security) Reset command, page 30.

After a module has been configured with cybersecurity settings, and is operating in Advanced (or Secured) Mode, you can also modify the cybersecurity settings using the web pages.

Refer to the commissioning topic, page 78 for instructions on how to apply an initial configuration to the module.

First Login to the Web Pages

When you login to an unconfigured BMENUA0100 module, the following screen (or a like screen depending on the browser you are using) displays:



Despite the terms used in the message, the connection is secured via HTTPS. Read the message, and if you agree, proceed with the initial login by clicking **[Accept the Risk and Continue]** (or other similar browser-specific message).

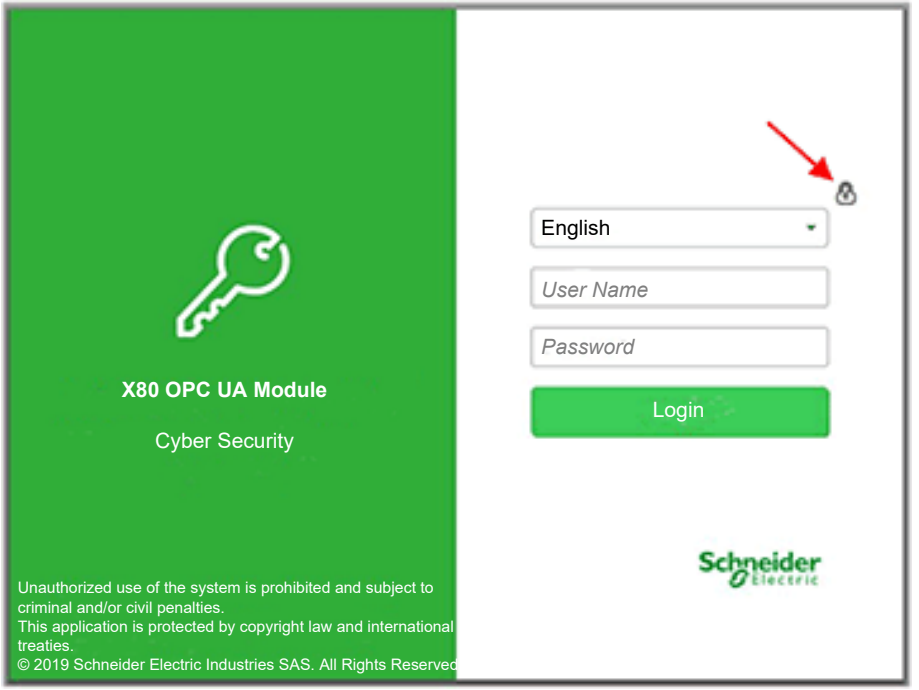
NOTE: The above message appears because the module does not yet have a valid configuration and is using a self-signed certificate.

Logging into the Web Pages

On the first login, the security administrator enters the default User Name and Password combination, page 31. Immediately thereafter, the administrator is required to change the default password.

You need to login each time you open the web pages for the BMENUA0100 module. Only persons that have been assigned a valid user account – with a valid username and password combination created by a security administrator in the **Access Control > User Management** web page, page 111 – can access the module web pages.

In the login page, select a language from the drop-down list, then enter your **User Name** and **Password**.

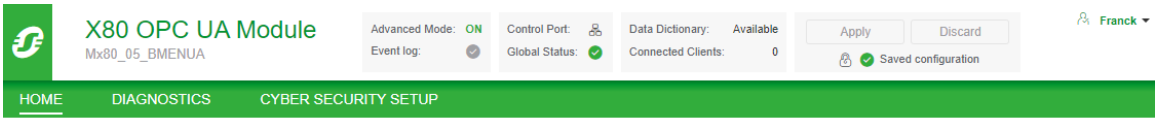


NOTE: The module cybersecurity operating mode is displayed by the lock icon in the upper-right part of the dialog box (indicated by the red arrow, above). If the lock is:

- Closed (as shown above): the module is operating in Advanced (or Secured) Mode, page 30.
- Open: the module is operating in Standard mode, page 30.

Web Page Banner

Every web page presents a banner at the top of the page:



The banner presents the following information about the BMENUA0100 module:

- Advanced (or Secured) Mode:
  - ON: the module is operating in Advanced (or Secured) Mode, page 30.
  - OFF: the module is operating in Standard mode, page 30.
- Event log:
  -  The Event log service is disabled.
  -  The Event log service is enabled; the log server is reachable.
  -  The Event log service is enabled, but the log server is not reachable.
  -  The Event log service is enabled, but an error has been detected.
- Control Port:
  -  The control port is enabled.
  -  The control port is disabled.
- Global Status:
  -  All services are operational.
  -  At least one service is not operational.
- Data dictionary:
  - Available: the data dictionary functionality is available.
  - Not Available: the data dictionary functionality is not available or is not enabled.
- Connected Clients: the number of connected OPC UA clients.
- Apply/Discard Configuration: Indicates the state of the module cybersecurity web page configuration:
  -  Unchanged configuration: The cybersecurity configuration contains no pending or invalid edits. The **Apply** and **Discard** buttons are disabled.
  -  Pending configuration: One or more changes to the cybersecurity configuration has not yet been applied. Both the **Apply** and the **Discard** buttons are enabled.
  -  Invalid configuration: The cybersecurity configuration is incomplete or incorrect. The **Apply** button is disabled; the **Discard** button is enabled. In this state, the web page displays, next to each affected menu item, a red circle that contains the number of invalid configuration settings reachable via that menu path. When you navigate to a page with an invalid configuration setting, the page displays the invalid configuration setting.

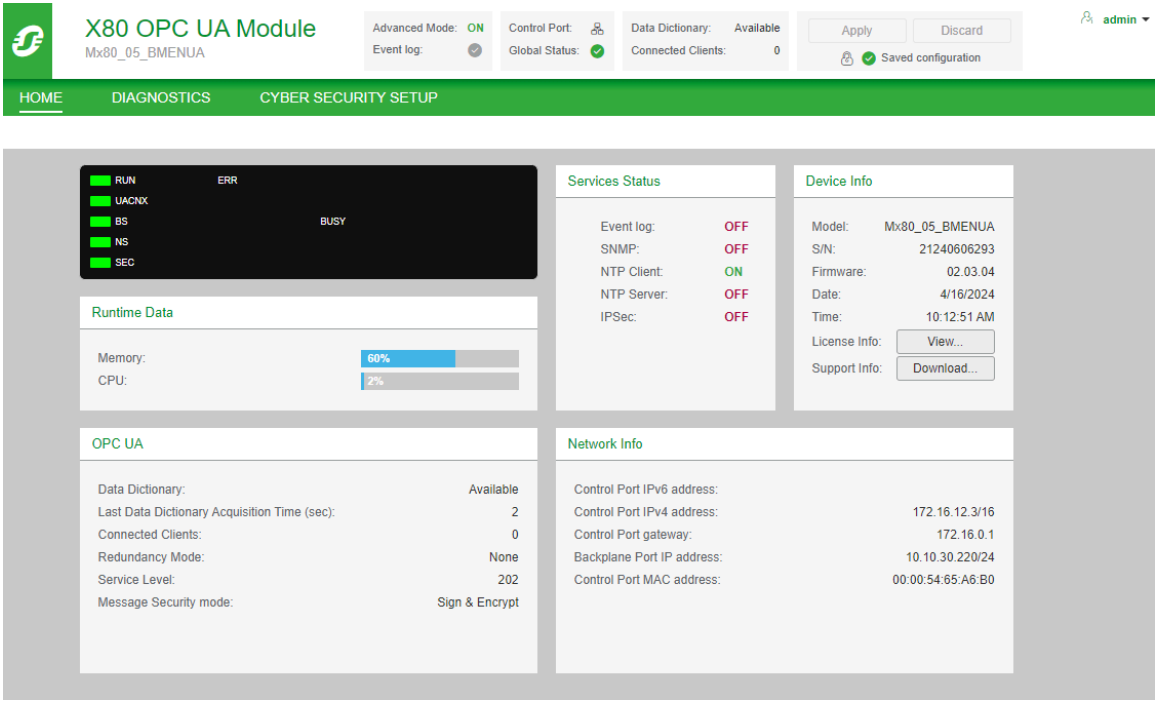
Web Page Help

Many Web pages offer parameter-level context sensitive help. To get help for a specific parameter, or field, place your cursor pointer over the icon.

Home Page

Introducing the Home Page

When you log into the BMENUA0100 web pages, the **Home** page opens by default. If the module has a valid configuration, the following page appears:



Use the **Home** page to:

- Access the navigation tree, which contains links to the BMENUA0100 module web pages. When the module is operating in:
  - Advanced (or Secured) Mode, page 30, both the DIAGNOSTICS and CYBER SECURITY SETUP menus are displayed and accessible to the security administrator.
  - Standard mode, page 30, only the DIAGNOSTICS menu is accessible.
- Display the state, page 131 of the module LEDs, page 24.
- Display collections of data for the module, including:
  - Runtime Data, page 90
  - OPC UA, page 90
  - Services Status, page 91
  - Network Info, page 91
  - Device Info, page 91

NOTE: When the rotary switch on the back of the module is set to the Cybersecurity (or Security) Reset, page 30 position, there is no communication with the module. Hence, the web pages – including the **Home** page – are not accessible.

Runtime Data

The **OPC UA** area displays:

- **Memory**: The percentage of internal RAM used by the OPC UA server (MEM_USED_PERCENT).
- **CPU**: The percentage of currently used CPU processing capacity (CPU_USED_PERCENT).

NOTE: The items described above are based on elements in the T_BMENUA0100 DDT, page 136.

OPC UA

The **Runtime Data** area displays:

- **Data dictionary**: The availability state of the data dictionary (DATA_DICT).
- **Last Data Dictionary Acquisition Time (sec)**: The duration of the last data dictionary acquisition (DATA_DICT_ACQ_DURATION).
- **Connected clients**: The number of connected OPC UA clients (CONNECTED_CLIENTS).
- **Redundancy mode**: The failover mode supported for a Hot Standby system (REDUNDANCY_MODE).

- **Service Level**: The OPC UA server health, based on data and service quality (SERVICE_LEVEL).

  NOTE: The five items described above are based on elements in the T_BMENUA0100 DDT, page 136.

- **Message Security mode**: The setting configured in the OPC UA web page, page 101: None, Sign, or Sign&Encrypt.

Services Status

The **Service Status** area displays the status – enabled (ON) or disabled (OFF) – of the following services as reported in the T_BMENUA0100 DDT, page 136:

- **Event log** (EVENT_LOG_SERVICE)
- **SNMP** (SNMP_SERVICE)
- **NTP Client** (NTP_CLIENT_SERVICE)
- **NTP Server** (NTP_SERVER_SERVICE)
- **IPSec** (IPSEC)

For modules earlier than version BMENUA0100.2.

- **Control Expert Data Flows** (CONTROIL_EXPERT_IP_FORWARDING)
- **CPU to CPU Data Flows** (CPU_TO_CPU_IP_FORWARDING)

Network Info

This area displays configuration settings for the BMENUA0100 module entered in Control Expert, page 115, and reported in the T_BMENUA0100 DDT, page 136, including:

- control port (CONTROL_PORT_IPV6, CONTROL_PORT_IPV4, and CONTROL_PORT_GTW)
- backplane port (ETH_BKP_PORT_IPV4)
- module MAC address, a unique hexadecimal value assigned to each module at the factory.

Device Info

This area displays the reference, serial number, and firmware version (FW_VERSION in the T_BMENUA0100 DDT, page 136), date, and time for the BMENUA0100 module.

Click **View...** to display licensing information.

Click **Download...** to display the **Download Support Info** dialog box. Refer to the topic Access Control, page 111 for more information.

Settings

In the BMENUA0100 module web pages, starting in the **Home** page, select **Settings** to display links to the following configuration pages, where you can enter settings for device security:

- User Account Policy, page 93
- Event Logs, page 93
- Network Services, page 94
- Service Forwarding, page 96
- IPsec, page 99
- SNMP, page 100
- OPC UA, page 101
- Security Banner, page 103

The configurable parameters for each node are described below.

Use these settings to configure device security for the BMENUA0100 module. After changing settings, select **Submit** or **Cancel**.

User Account Policy

Use these settings to configure user account policy:

Parameter	Description
Session maximum inactivity (minutes)	The idle session timeout period for HTTPS connections. If a connection is inactive for this period, the user session is automatically closed. Default = 15 minutes. **NOTE:** There exists no inactivity period timeout for OPC UA connections.
Maximum login attempts	The number of allowable unsuccessful login attemps. Default = 5 attempts. When the configured maximum is reached, the user account is locked.
Login attempt timer (minutes)	The maximum time period to login. Default = 3 minutes.
Account locking duration (minutes)	Time period during which no additional logins may be attempted after the maximum login attempts is reached. Upon the expiration of this period, a locked user account is automatically unlocked. Default = 4 minutes.

NOTE: These user account policy settings apply to OPC UA clients, page 164 that have been assigned a username.

Event Logs

Use these settings to configure the syslog client that resides in the BMENUA0100 module. The logs are stored locally in the module and exchanged with a remote syslog server, page 151 :

Parameter	Description
Service activation	Turns ON and OFF the syslog client service. Default = OFF.
Syslog server IP address	IPv4 or IPv6 address of the remote syslog server. **NOTE:** IPv6 is available for firmware version 1.10 and later of the BMENUA0100 module.
Syslog server port	The port number used by the syslog client service. Default = 601.

Network Services Activation

These services together constitute a firewall that permits or denies the passage of communications through the BMENUA0100 module. Use these settings to enable or disable the following services:

GLOBAL POLICY:

Service	Description
Enforce Security	Disables the network services except IPsec.
Unlock Security	Enables the network services except IPsec.

NETWORK SERVICES ACTIVATION: The default setting for the following services depends on the cybersecurity operating mode (CS Op Mode), as follows:

Service	Description	CS Op Mode default	
		Standard	Advanced (or Secured)
SNMP Agent	Enables and disables SNMP Agent communications.	Enabled	Disabled
NTP Server	Enables and disables NTP server communications.	Enabled	Disabled
IPsec	Enables and disables IPsec communications.	Disabled	Enabled[1]
Controller to Controller Data Flows[2, 3]	Enables and disables Modbus communications, passing through the BMENUA0100 module, between M580 controllers. Refer to *Configuring Communication for Controller to Controller Data Flows*, page 96.	Enabled	Disabled
Control Expert Data Flows to Controller only[2, 3]	Enables and disables Modbus, EtherNet/IP, Ping, explicit messaging, and FTP communications, passing through the BMENUA0100 module, between Control Expert configuration software and the controller only. Refer to *Configuring Communication for Control Expert Data Flow*, page 95.	Enabled	Disabled
Control Expert Data Flows to Device Network[2, 3]	Enables and disables Modbus, EtherNet/IP, Ping, explicit messaging, and FTP communications, passing through the BMENUA0100 module, between Control Expert configuration software and network devices, including the controller. Refer to *Configuring Communication for Control Expert Data Flow*, page 95.	Enabled	Disabled

Service	Description	CS Op Mode default	
		Standard	Advanced (or Secured)
HTTPS on control port	Enables and disables HTTPS communications over the control port. **NOTE:** If HTTPS is disabled, and the change applied, the web pages cannot be accessed via the control port. To regain access to the web pages from the control port, you can reset the cybersecurity configuration.	Disabled	Enabled
1. IPsec is enabled with no rules defined. The service needs to be configured. 2. Refer to the troubleshooting topic Activating Network Services Using Only an IPv6 Connection, page 164 for information regarding that configuration design. 3. Supported only by modules earlier than version BMENUA0100.2, as indicated in EcoStruxure Control Expert.			

NOTE: SNMP, NTP, Syslog and Modbus services are not inherently secure protocols. They are rendered secure when encapsulated within IPsec. Do not disable IPsec if any one of the SNMP, NTP, Modbus, or Syslog services is enabled.

Configuring Communication for Remote Software Running on PCs (Not Using NAT Forwarding)

The software addresses the target device (e.g., the M580 controller) using the IP address of the target device. To support this communication, set up two default gateways, as follows:

- On the host PC running the software, using IPv4, set up a PC default gateway to the BMENUA0100 module control port IP address.
- On the target device (e.g. the M580 controller), using IPv4, set up a device default gateway to the BMENUA0100 module control port IP address.
- On the host PC, add a route with the following command:

```
route ADD <<destination=subnet of the target device>> MASK <<subnet mask of the target device>> <<gateway=BMENUA0100 module backplane port IP address>>
```

For IPv4 in all firmware versions, and for IPv6 in firmware versions 1.10 and later, Modbus communications from Control Expert Connect screen address the BMENUA0100 control port IP address. Gateways are not needed for this communication.

Configuring Communication for Controller to Controller Data Flows

Modbus TCP/IP communications from controller to controller through the BMENUA0100 module will use the BMENUA0100 module IPv4 control port address, and not the address of the target controller.

NOTE:

- For BMENUA0100, the controller to controller forwarding is limited to Modbus TCP/IP protocol.
- Modbus protocol is the only protocol that supports device to device communication.
- Only IPv4 – and not IPv6 – addressing supports Modbus TCP/IP controller to controller data flows.

Service Forwarding (IP Forwarding)

A BMENUA0100 module with firmware version 2.01 or later includes this web page. Use it to configure the forwarding of unicast data flows that pass through the module between the control network and device network. In this web page you can create, edit, or remove a list of IP forwarding rules for the module.

NOTE: The Service Forwarding (IP Forwarding) feature does not support the following features

- Multicast data flows.
- EtherNet/IP implicit messaging.

As a result, this service the following tasks are not supported:

- Device discovery by the EcoStruxure Automation Device Maintenance (EADM) tool operating in automatic discovery mode. EADM device discovery using the manual discovery mode is supported. (multicast).
- Message forwarding to the controller local EtherNet/IP communication modules (EtherNet/IP implicit messaging).

Features:

The main features of the Service/IP forwarding function are:

- Capability to forward all data flows (“Forward All”).
- IP forwarding of the most common protocols used in the architecture through predefined templates (e.g.: Modbus, HTTPS, SNMP, …)
- Creation and application of of custom IP forwarding templates.

- NAT (Network Address Translation) forwarding of some protocols to local controller if @remote IP address is the BMENUA0100 IP V4 Control port

  NOTE: NAT forwarding applies to the following protocols: Modbus, Modbus over TLS, EIP explicit, EIP explicit over TLS, EIP implicit, OPC UA Client.

- The option to use, or not use, IPsec for protocols forwarded by NAT. Refer to the guidelines set forth in the notes at the end of the IPsec section, below, page 99.

NOTE:

- If several BMENUA0100 modules are placed in the same rack, configure only one BMENUA0100 module with the forwarding function.
- Multicast data flows are not forwarded.
- An online update of IP Forwarding rules may cause some ongoing communications to stop.
- For Service Forwarding (IP Forwarding) to succeed, the destination IP network needs to be different from the source IP network. For example, it is not possible to execute IP Forwarding between:
  - Source IP network 192.168.x.x (Mask 255.255.0.0) and
  - Destination IP network 192.168.x.x (Mask 255.255.0.0).
- The value of OPC UA Listening port needs to be the same for all BMENUA0100 modules communicating together (for example, in the case of OPC UA NAT forwarding between several BMENUA0100 modules.
- Activating the FTP protocol opens a range of TCP ports, from 1024 to 65535. As a result, other protocols with TCP ports in this range may also be forwarded. Enable forwarding of the FTP protocol only temporarily and when it is required.
  - Activating the TFTP protocol as a custom rule causes the same result as activating the FTP protocol. Enable forwarding of the TFTP protocol only temporarily and when it is required.

Refer to the following topics for more information about Service (IP) Forwarding architectures:

- Service (IP) Forwarding Supported Architectures, page 169
- Service (IP) Forwarding Non-Supported Architectures, page 172

IP Forwarding and OPC UA Communication

Both IP Forwarding and OPC UA compete for the BMENUA0100 module available communication bandwidth. For performance test results describing the impact of IP Forwarding, OPC UA communications, confidentiality settings, and custom rules on bandwidth, refer to the chapter IP Forwarding and OPC UA Communication, page 173.

Creating Rules:

- To document both predefined rules and custom rules, click **New Forwarding**, and complete the settings that define that rule.

  NOTE: When you select a service name, the port number and protocol are automatically assigned their default settings. These can be edited as required.
- To edit an existing rule, click the pencil icon, and edit its settings.
- To remove an existing rule, click the trash container icon.

Set **Forward All** to **OFF** to apply the listed rules. If you set **Forward All** to **ON**:

- The rules are suspended and the module forwards all protocols;
- You cannot configure forwarding for individual services, and
- All services will be forwarded over IPsec if IPsec is enabled.

Each rule is defined by the following fields:

Setting	Description
Service name	The following services are pre-defined: • Modbus • FTP • EIP explicit • ICMP • NTP / SNTP • SNMP • SNMP trap • HTTPS • Modbus over TLS • EIP explicit over TLS • LDAP Start TLS • Syslog • HTTP • DPWS meta data • OPC UA (for OPC UA client) • DNP3 • DNP3 over TLS • IEC 60870 • IEC 60870 over TLS • EIP Implicit **NOTE:** For OPC UA, the port number is the OPC UA port set in Control Expert for the BMENUA0100 module.
Port Number[1]	The port associated with the service.
Protocol[1]	The protocol associated with the service.

Setting	Description
IPsec use	• **TRUE** : the protocol is carried over IPsec. • **FALSE**: the protocol is not carried over IPsec, even if IPsec is activated in the configuration. This selection is available only when IPsec is enabled. **NOTE:** • **Do not use** IPsec for natively secured protocols (e.g. Modbus over TLS, EIP explicit over TLS, DNP3 over TLS, EIP 60870 over TLS) • **Do use** IPsec for non-natively secured protocols (e.g. Modbus , EIP explicit, OPC UA client, EIP IO)
Inbound Interface	• **Control Port**: if the remote Client request is received on Control Port (e.g.: Modbus TCP/IP request from Control Expert). • **Backplane Port**: if the remote Client request is received on Backplane Port (e.g., Modbus TCP Request from a controller Function block). • **Both**: if the remote Client request can be received on both Control and Backplane Port (e.g.: Modbus TCP/IP request from Control Expert and Modbus TCP Request from a controller Function block).
1. Auto-filled, but editable, for a predefined service name.	

IPsec

Use IPsec to help secure IPv4 Ethernet communication.

NOTE: IPsec does not support IPv6 addressing.

Use these settings to configure a maximum of 8 IKE / IPsec channels over IPv4 for the BMENUA0100 module. If more than 4 IPsec links are configured, the automatic connection to the controller after transfer through the BMENUA0100 may not succeed. In that case, connect to the controller manually.

Parameter	Description
IPsec SERVICE	• ON: Enables IPsec service. **NOTE:** As a precondition to enabling the IPsec service, you also need to enable the Control Port in the IPConfig settings, page 116. • OFF: Disables IPsec service.
NTP authorized outside IPsec	• De-selected (disabled): NTP is exchanged only through IPsec. • Selected (enabled): NTP is exchanged through IPsec if IPsec channel is opened, and outside IPsec if IPsec channel is not opened.
New link	Creates a new IKE / IPsec channel and adds it to the list for editing. **NOTE:** A maximum of 8 IKE / IPsec channels are supported.
For each IKE / IPsec channel, configure the following settings:	

Parameter	Description
Remote IP address	IPv4 address of the remote IPsec endpoint. **NOTE:** The remote device needs to be accessible from the BMENUA0100 Control Port (and not from the BMENUA0100 Backplane Port).
Confidentiality	• Selected: Communication will be encrypted. • De-selected: No encryption. **NOTE:** Confidentiality is disabled if *NTP without IPsec* is enabled.
Client type	Type of the remote IPsec endpoint: Windows or Device. **NOTE:** Default is Windows. Verify that the configured endpoint type matches the client.
PSK	A pre-shared key that is 32 hexadecimal characters long, the result of a random number generated by the BMENUA0100 module. It can be copied and edited in this web page. **NOTE:** PSK is disabled if *NTP without IPsec* is enabled.

NOTE: Configure Windows firewall settings, page 175 by downloading the "Windows script" from BMENUA0100 using the **Download script** command for each remote IP address. If the **IPsec use** setting is changed for some protocols, the Windows script needs to be downloaded again from the BMENUA0100 module and executed on Windows. For an example of Windows script, refer to the topic IPsec Windows Scripts, page 175.

NOTE: If 8 IPsec tunnels are configured, it may not be possible to automatically reconnect to the controller after download of an application. In this case, reconnect manually to the controller after the download.

NOTE: If IPsec service is activated (i.e. set to ON):

- Local HTTPS server Data Flow goes outside IPsec.
- Local OPC UA data flow is carried by default inside IPsec. In order to carry local OPC UA data flow outside IPsec, an OPC UA forwarding rule with “IPsec use = FALSE” needs to be set, even if there is no need to forward OPC UA data flow.

SNMP

Use these settings to configure the SNMP version and related settings.

NOTE: In Advanced (or Secured) Mode, the SNMP version needs to be configured the same in both Control Expert, page 128 and in the SNMP web page. If these settings are not the same, the SNMP service does not start.

Parameter	Description
SNMP Version	• v1 • v3
Security Level	For SNMP v1 and v3: • NoAuthNoPriv: Communication without authentication or privacy. **NOTE:** For SNMP v1, this is the only available setting. For SNMP v3 only: • AuthNoPriv: Communication with authentication but without privacy. The authentication protocol is SHA (Secure Hash Algorithm). • AuthPriv: Communication with both authentication and privacy. The protocols used are: ◦ Authentication: SHA. ◦ Privacy: AES (Advanced Encryption Standard).
Authentication Password	If authentication is enabled, enter a case-sensitive authentication password. It can contain from 8 to 12 characters, and can include alphanumeric characters (uppercase letters, lowercase letters, and numbers) as indicated by the web page tool tip.
Privacy Password	If privacy is enabled, enter a case-sensitive privacy password. It must contain 8 characters, and can and include alphanumeric characters (uppercase letters, lowercase letters, and numbers) as indicated by the web page tool tip.

OPC UA

Use these settings to configure the connection for the OPC UA server embedded in the BMENUA0100 module:

Parameter	Description
Message Security mode	• Sign&Encrypt (default): Each message is given a signature and is encrypted. • Sign: A signature is applied to each message. • None: No security policy is applied. In this case, the following two fields are disabled. **NOTE:** When **None** is selected, the **User Identifier token type** in the BMENUA0100 module is defined as **Anonymous**. In this case, you also need to configure the user identifier token type in the OPC UA client to **Anonymous**.
Security Policy	• Basic256Sha256 (default): It defines a security policy for configurations with valid cipher suite. • Basic256: It defines a security policy for configurations with deprecated cipher suite. **NOTE:** This selection is not used unless needed for interoperability with remote client. • Basic128Rsa15: It defines a security policy for configurations with deprecated cipher suite. **NOTE:** This selection is not used unless needed for interoperability with remote client.
User Identifier token types	• Anonymous: No user information is available. • User Name (default): User is identified by username and password.

NOTE: Cybersecurity configuration changes to the OPC UA server settings cause the server to restart and apply the new settings. As a result, if one or more OPC UA sessions exist when configuration changes are made, these sessions are suspended. When the *SessionTimeout* period expires, these sessions are closed. The *SessionTimeout* is part of the OPC UA SCADA client configuration.

NOTE: When the OPC UA server **Message Security Mode** setting is initially configured for **Sign&Encrypt** or **Sign** and an OPC UA client establishes a connection, if you subsequently set the OPC UA server **Message Security Mode** setting to **None**, an OPC UA Client (with its **Message Security Mode** setting also set to **None**) cannot establish a connection to the server.

To re-establish a connection:

1. Disconnect your OPC UA clients.
2. Change the OPC UA configuration in BMENUA0100 web page.
3. Wait while the **BUSY** LED is ON (yellow) until it turns OFF (not illuminated).
4. For the OPC UA clients, change their configuration (**Message Security Mode**) to the same setting used for the OPC UA server.
5. Reconnect the OPC UA clients to the server.

Security Banner

This page contains editable text that is displayed when a user accesses the BMENUA0100 module web pages:

Parameter	Description
Banner text	A string of up to 128 characters that is displayed to a user on the login page. The following editable text is displayed by default: “Unauthorized use of the system is prohibited and subject to criminal and/or civil penalties.”

Certificates Management

Certificates Management With and Without PKI

The BMENUA0100 module relies upon certificates for authentication. To provide cybersecurity, each entity (including OPC UA clients and the OPC UA server embedded in the BMENUA0100) needs to manage a trust list of all certificates of devices/applications that communicate with it.

The method of certificate management depends on your system design, which may - or may not - apply a public key infrastructure (PKI) with a certificate authority (CA).

Certificate Management without PKI:

Use this certificate management method if your system does not include a CA. This management method is supported by BMENUA0100 modules with firmware v1.0 and later. Manage certificates in the **Certificates Management** web pages as follows:

- Set **PKI mode** to **Self-Signed only**.
- Manage the **Certificate Trust List** using the **Add** and **Delete** functions to create a list for OPC UA clients that are authorized to communicate with the BMENUA0100 module.
- Export the BMENUA0100 module certificate to OPC UA client devices using the **Download** command in the **PKI Configuration > Device Certificate** page.

Certificate Management with PKI:

Use this certificate management method if your system includes a CA. This management method is supported by BMENUA0100 modules with firmware v1.1 and later. Manage certificates in the **Certificates Management** web pages as follows:

- Set **PKI mode** to either:
  - **CA only**: if all installed OPC UA client devices support PKI.
  - **Self-Signed & CA**: if some of the installed OPC UA client devices do not support PKI.

- If **PKI mode** is set to **CA only**:
  - Manually enroll, page 108 each BMENUA0100 module with the CA.
- If **PKI mode** is set to **Self-Signed & CA**:
  - Manually enroll, page 108 each BMENUA0100 module with the CA.
  - Manage the **Certificate Trust List** using the **Add** and **Delete** functions to create a list for OPC UA clients that are authorized to communicate with the BMENUA0100 module.

Updating the Certificate Trust List

After the first installation of BMENUA0100 firmware version 2.0 (BMENUA0100.2) or later, you need to remove the user added certificates from the **Certificate Trust List** in the **Certificates Management** web page. You can do this by:

- Manually removing these certificates using the **Delete** command, or
- Setting the cybersecurity rotary switch to the **Cybersecurity Reset** position.

After the **Certificate Trust List** is cleared, you can re-populate it with self-signed or CA issued certificates.

This task needs to be performed only on the first installation of firmware version 2.0 or later. You do not need to repeat the procedure on subsequent installations of later firmware versions.

NOTE: If you do not clear the **Certificate Trust List**, as described above, connections with OPC UA clients cannot be established or, if established, will be discarded.

Authentication Overview

An OPC UA client or a BMENUA0100 module can be authenticated in three ways:

- For firmware version 1.0 and later:
  - Self-signed certificate (only)
- For firmware version 1.10 and later:
  - PKI certificate issued by a third-party Certificate Authority (CA) only
  - PKI certificate issued by a CA and a self-signed certificate

To provide the required level of cybersecurity, each entity (OPC UA client, BMENUA0100) needs to manage a trust list of all certificates of devices/applications that communicate with it.

For firmware version 1.10 and later, the BMENUA0100 module creates a self-signed certificate for:

- Configuration of the cybersecurity settings via the module web pages
- Diagnostic of the module via its web pages
- Firmware upgrade
- OPC UA application instance certificates to permit OPC UA clients to access the embedded OPC UA server in the BMENUA0100 module.

For firmware version 1.0 the module creates two certificates: one HTTPS certificate and one OPC UA certificate.

NOTE:

- The expiration dates of the trusted certificates are made by reference to the internal Date and Time settings of the BMENUA0100 module. To avoid inconsistency, use the NTP service to update the Date and Time settings of the BMENUA0100 module, and verify that the NTP server is accessible and has an updated Time and Date settings.
- If you receive a *BadCertificateHostnameInvalid* detected error when attempting to connect your OPC UA client to the BMENUA0100 server in IPv6, it may be caused by a compressed IPv6 address (i.e., shortened IPv6 address). In this case verify the IPv6 address that was used and, if necessary, replace it using an uncompressed format.
- The BMENUA0100 module does not automatically manage the expiration dates of certificates. You need to manually manage certificate expiration dates.

Managing Certificates

In the BMENUA0100 module web pages, starting in the **Home** page, select **Certificates Management** to display links to the following application instance certificate management pages:

- PKI Configuration, page 107
- Client Trust List Management, page 109
- Device Certificates Export, page 110
- Manual Enrollment, page 108
- CA Certificates, page 110

Refer to the topics *Using GPOs/LGPOs*, page 163 and *Applying MMC Group Policy Management*, page 164 for information regarding the Windows™ tools you can use to help manage certificates.

Certificate Extensions

To support communication with the BMENUA0100 module, self-signed and CA certificates need to include specific extensions, as follows:

Self-Signed Certificates:

- KeyUsage (marked as critical):
  - DigitalSignature
  - KeyEncipherment (No usage for TLS suite based on ephemeral keys such as TLS_ECDHE_xxxx; usage for TLS_RSA_xxxx)
  - KeyCertSign: when the subject public key is used for verifying signatures on public key certificates (Value TRUE)
  - nonRepudiation (required by OPC UA standard)
  - dataEncipherment (required by OPC UA standard)
- Subject Alt Name: In the SAN field the following values can be specified: IPAddress V4/V6, URI
- Basic Constraints:
  - cA field: whether the certified public key may be used to verify certificate signatures (Value TRUE) and pathLenConstraint=0
- Subject Key Identifier:
  - means of identifying certificates that contain a particular public 160-bit SHA-1 hash of the value of the BIT STRING subjectPublicKey (excluding the tag, length, and number of unused bits).
- Extended Key Usage extension:
  - id-kp-serverAuth if TLS Web server authentication
  - id-kp-clientAuth if TLS Web client authentication

CA Certificates:

- KeyUsage (marked as critical):
  - DigitalSignature
  - KeyEncipherment (No usage for TLS suite based on ephemeral keys such as TLS_ECDHE_xxxx; usage for TLS_RSA_xxxx)
  - KeyCertSign: when the subject public key is used for verifying signatures on public key certificates (value FALSE)
  - nonRepudiation (required by OPC UA standard)
  - dataEncipherment (required by OPC UA standard)
- Subject Alt Name: In the SAN field the following values can be specified: IPAddress V4/V6, URI

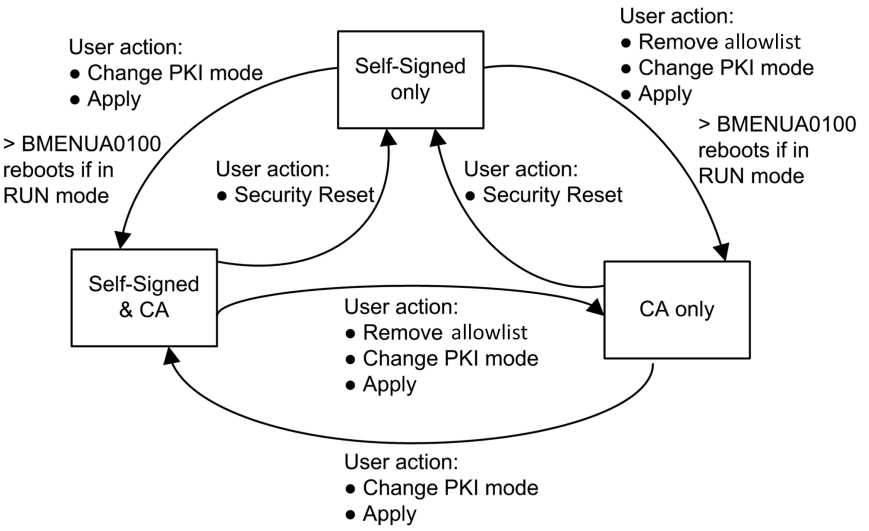
- Basic Constraints:
  - cA field: whether the certified public key may be used to verify certificate signatures (value FALSE)
- Extended Key Usage extension:
  - id-kp-serverAuth if TLS Web server authentication
  - id-kp-clientAuth if TLS Web client authentication
- CRL Distribution points
- Authority Key Identifier:
  - Identification of the public key corresponding to the private key used to sign a certificate.

PKI Configuration

Use the **PKI Configuration** page to specify the types of certificates accepted by the OPC UA server embedded in the module, including:

PKI Mode	Description
Self-Signed only	Only certificates in the **Trusted Client Certificate** list need to be managed.
CA only	All system devices need certificates signed by a CA.
Self-Signed and CA	Certificates are managed as follows: • The certificate for the BMENUA0100 module with firmware version 1.10 and later is issued by a CA. • Certificates for client devices that support PKI are issued by a CA. • Certificates for client devices that do not support PKI are self-signed.

The following diagram illustrates the user actions and events related to changing the PKI mode setting:



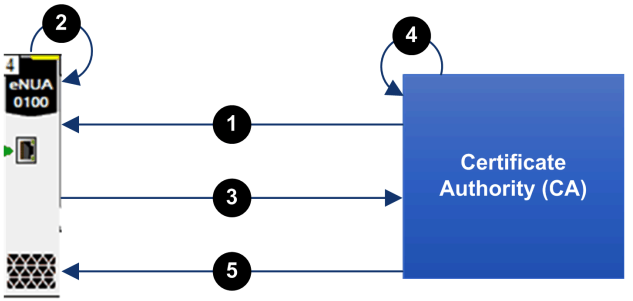
Manual Enrollment

After configuring the BMENUA0100 module in Control Expert, you can use the **Manual Enrollment** page to **Get** a CSR file to be submitted to a CA. After submitting the CSR file, you can then extract the correspondent CA certificate. Thereafter, you can **Push** this CA Certificate into the BMENUA0100 module. The combined **Get** and **Push** operations manually enroll a certificate issued by a third-party CA. After the certificate is pushed, the OPC UA server applies this certificate for the purpose of signing and encrypting its communication with the OPC UA client.

NOTE: As a pre-condition to performing manual enrollment:

- Confirm that the NTP client is enabled, page 124.
- Verify that the time setting for the BMENUA0100 module is correct.

The following is an overview of the manual certificate enrollment process:



1 BMENUA0100 imports a CA certificate from the certificate authority (CA)

2 BMENUA0100 generates a certificate signing request (CSR)

3 BMENUA0100 exports the CSR to the CA

4 The CA executes the CSR and generates a certificate

5 BMENUA0100 imports the certificate from the CA

Refer to the Schneider Electric video “How to work with PKI mode “Self-Signed & CA” on BMENUA0100 module?” at https://www.se.com/us/en/faqs/FAQ000191153/.

Client Trust List Management

Only OPC UA clients that have provided the BMENUA0100 module with an application instance certificate can communicate with the OPC UA server embedded in the module. The module implements local (module-based) management of OPC UA application instance certificates, which are stored in a trust list. Use the commands on the **Certificates Management** web pages to **Add**, **Download**, or **Delete** a certificate.

NOTE: OPC UA application instance trust list certificates are encoded in ANSI CRT.

To add a certificate to the list:

Step	Action
1	In the trust list management menu, click **Add**.
2	Click **Browse**, then navigate to and select the certificate you want to add to the list.
3	Click **Submit** to add the certificate.
4	Click **Apply** to save the change to the configuration.

To remove a certificate from the list:

Step	Action
1	In the trust list, click the certificate you want to remove
2	Select **Delete**.
3	Click **Yes** to remove the certificate from the list.
4	Click **Apply** to save the change to the configuration.

Device Certificates Export

You can export the BMENUA0100 module certificate for both HTTPS and OPC UA in the **CERTIFICATES MANAGEMENT > PKI CONFIGURATION** page by clicking on the **Download** button

CA Certificates

The CA certificate is a public key certificate that identifies the certificate authority (CA) in a public key infrastructure (PKI). Use the **CA Certificates** page to add the CA certificate(s) in the device.

To add a certificate from the CA to the CA Certificates list:

Step	Action
1	Open the web pages for the module, and in the **Login** dialog box, enter: • username • password Click **Login**.
2	Navigate to **CYBER SECURITY SETUP > CERTIFICATES MANAGEMENT** to access the certificates management tab, then select **CA Certificates**.
3	In the **TRUSTED CERTIFICATES** list, click **ADD** to add the CA certificate to the list.
4	Apply the changes to the cybersecurity configuration.

NOTE: A maximum of ten CA certificates can be added.

Access Control

Introduction

The BMENUA0100 module supports local authentication of users based on the use of username/password combinations for:

- Configuration of the module cybersecurity settings via HTTPS
- Firmware download via HTTPS
- Module web page diagnostics via HTTPS

NOTE: Only a user with the role of Security Administrator can create, edit, or delete user accounts.

The BMENUA0100 web pages provide tools for the management of user accounts. Starting in the **Home** page, click on **Access Control** to display a list of existing OPC UA user accounts, including their roles and permissions. In this page you can:

- Create a user account, page 112.
- Update the profile, page 112 of an existing user account.
- Delete, page 112 a user account.

User Management

The BMENUA0100 module provides role based access control (RBAC). All user accounts are assigned a role and can perform only those tasks associated with that role.

The following roles and permissions are supported:

Role	Permissions			
	Cybersecurity Configuration	Firmware Upgrade	Diagnostic Web Page Access	OPC UA Protocol Access
SECADM	Update, Read, Delete	–	Read	–
OPERATOR	–	–	Read	Connect
ENGINEER	–	–	Read	Connect
INSTALLER	–	Update	Read	–

Each BMENUA0100 module supports a maximum of 15 simultaneous users.

No custom roles or custom permission sets can be configured. No IP address-based access control allowlist can be configured.

Create a User Account

A Security Administrator can click **New User** then complete the following parameters to create a new user account:

Parameter	Description
User name	The user ID. The user will enter this along with the password to gain access to the permitted functions.
Password Confirm Password	The user password. The password is not displayed in clear text. Enter this value twice to confirm its accuracy. **NOTE:** Each password must be at least 8 characters long, and must contain at least one of the following characters: • an upper-case alpha character (A...Z) • a lower-case alpha character (a...z) • a base–10 digit (0...9) • a special character ~ ! @ $ % ^ & * _ + - = ` | \ ( ) [ ] : " ' < >
Roles	Select the role, which will define the permissions granted to the user: • Security Administrator • Operator • Engineer • Installer

Click **Apply Changes** after these parameters are configured to create the user account.

Update a User Account

To edit the settings of a user account, a Security Administrator can click on the edit icon (pencil) for the profile you want to edit. Click **Apply Changes** to save your edits. The same dialog box used to create a user account opens, letting you update some or all of the selected user account parameters,

Delete a User Account

To delete an existing user account, a Security Administrator can right click on the user account in the list, and under **Delete User** click **OK**.

Configuration Management

Introduction

To facilitate system configuration, you can export the cybersecurity settings of a configured BMENUA0100 module, and import that configuration into another module. In the BMENUA0100 module web pages, starting in the **Home** page, select **Configuration Management** to display links to the following cybersecurity configuration management pages:

- EXPORT, page 113
- IMPORT, page 113
- RESET, page 114

NOTE: Only a security administrator, with the role SECADM, can perform the configuration management tasks described in this topic.

Export a Configuration

Use the **EXPORT** page to export the cybersecurity configuration file of the local BMENUA0100 module. The exported configuration file is encrypted with the password assigned in this page. An exported configuration file can be stored and re-used.

To export the cybersecurity configuration file of the local BMENUA0100 module:

Step	Description
1	In the **EXPORT** page, assign the configuration file a **Password**. **NOTE:** The password needs to be a minimum of 16 characters, and applies the same rules that are used in the creation of user passwords, page 112.
2	Re-enter the assigned password in the **Confirm password** field.
3	Click **Download**.

NOTE: The configuration file is produced with the name: Mx80_xx_BMENUA.cfg, where “xx” indicates the slot number occupied by the module in the rack.

Import a Configuration

Use the **IMPORT** page to import a cybersecurity configuration file and apply it to the local BMENUA0100 module. The cybersecurity settings applied using this command overwrite the module existing cybersecurity settings.

To import a cybersecurity configuration file and apply it to the local BMENUA0100 module:

Step	Description
1	In the **IMPORT** page, click the file icon to open a window where you can select a **Configuration archive**.
2	Navigate to and select the configuration file you want to import, and click **OK**.
3	In the **IMPORT** page, enter the configuration file **Password** that was assigned to the file when the file was exported. **NOTE:** Optionally, you can select **Save** to automatically apply the imported configuration immediately after it is uploaded.
4	Click **Upload**. A dialog box opens informing you that your session has been closed. The configuration has been uploaded to the server.
5	Click **Reconnect** to close the dialog box and open the login screen, page 86.
6	Enter your security administrator username and password and click **Login**. The Home page opens. If **Save** was not selected in step 3, the banner indicates a pending configuration exists.
7	In the banner, click **Apply**, then click **Yes** to confirm that you want to apply the pending configuration. The new configuration is applied. **NOTE:** If you previously selected **Save** in the **IMPORT** page (as indicated in step 3, above) the configuration is automatically applied, and this step 7 is automatically performed.

Reset a Configuration

Click **Reset** in the **RESET** page to restore the “out of the box” factory default cybersecurity settings to the local BMENUA0100 module. This action has the same effect as setting the rotary selector switch to the Cybersecurity (or Security) Reset, page 30 position. After completing the reset, you need to execute a module reboot.

Configuring the BMENUA0100 in Control Expert

Introduction

This section describes how to configure IP address settings, the NTPv4 client, and the SNMPv1 agent for the BMENUA0100 Ethernet communication module with embedded OPC UA server.

Configuring IP Address Settings

Introduction

The BMENUA0100 Ethernet communications module with embedded OPC UA server includes two Ethernet ports:

- the control port located on the front of the module.
- a backplane port connecting the module to the local main rack Ethernet backplane.

The control port can be enabled or disabled, and is disabled by default. The backplane port is always enabled.

Static IP address settings for both the control port and the backplane port can be configured in the **IPConfig** tab of the BMENUA0100 configuration dialog box. In addition, IP address settings can be dynamically assigned to the control port via the Stateless Address Auto-configuration (SLAAC) method of DHCP.

When the BMENUA0100 module is used with a standalone controller, IP address settings are configured for one module. When two instances of the BMENUA0100 module are used in a Hot Standby controller architecture (one BMENUA0100 module in each controller), the Control Expert **IPConfig** configuration tab includes settings for two modules (A and B). In a Hot Standby controller architecture, the IP address for each module can be in different subnets.

IPv4 and IPv6 Stack Support

The control port can be configured to support IP stacks (each of which consists of a collection of Internet-enabling protocols) as follows:

- IPv4 stack: Supports only 32-bit addressing. An example of an IPv4 IP address is: 192.168.1.2.
- IPv4/IPv6 dual stack: Supports both 32-bit and 128-bit addressing. When both the IPv4 and IPv6 stacks are configured, the control port can receive and handle both IPv4 and IPv6 Ethernet packets An example of an IPv6 128-bit IP address is: 2001:0578:0123:4567:89AB:CDEF:0123:4567.

NOTE:

On initial power up (or after the module rotary switch has been set to **Cybersecurity (or Security) Reset**, powered up, then re-set to **Advanced (or Secured) Mode**, and then powered up again), the control port is assigned a default IPv4 address of 10.10.MAC5.MAC6, where MAC5 is the decimal value of the 5th octet of the module MAC address, and MAC6 is the decimal value of the 6th octet.

When the last two octets of the MAC address (*MAC5.MAC6*) correspond to *0.0* in the default address, make a point-to-point cable connection between your computer and the controller, communication module, or other module.

The MAC address of the module appears on its front face.

IPv6 via the Control Port

IPv6 communication is supported only via the control port.

NOTE: Control Expert flow can be configured to be routed to an M580 controller. Control Expert V15 and later can be connected to an M580 controller via the BMENUA0100 IPv6 address.

Configuring IP Addresses

Configure IP addressing in Control Expert, as follows:

Step	Action
1	In the **Project Browser** expand the **PLC Bus** node and open the BMENUA0100 module configuration dialog box.
2	Click on the **IPConfig** tab.
3	Enter changes in the appropriate fields on the **IPConfig** configuration page. (The following table describes the configuration page parameters.)

Configurable Parameters

Configure these IP address parameters for each BMENUA0100 communications module in your project:

Parameter		Description
Control Port		Enables/disables the control port of the BMENUA0100 module. When set to: • Enabled: the control port is the exclusive interface for IPv4 or IPv6 communication to the embedded OPC UA server. • Disabled (default): the Ethernet backplane port can support IPv4 communication to the OPC UA server.
IPv6 Control Port configuration		
	IPv6	Enables/disables IPv6 IP addressing for the control port when the control port is enabled. Default = disabled.
	Mode	Identifies the source of the IPv6 address: • SLAAC: Indicates the IPv6 IP address will be served to the control port from a DHCP server using the SLAAC method. • Static (default): Enables the IPv6@ field for inputting a static IPv6 IP address.
	IPv6 @	If **Static** is selected as the **Mode**, above, enter a valid IPv6 address for the control port. **NOTE:** • The BMENUA0100 cannot detect duplicate IPv6 addresses. Verify with your network administrator to ensure there are no duplicate IPv6 addresses within the same network segment. • The BMENUA0100 will accept, but cannot utilize, incorrect IPv6 addresses.
	Subnet prefix length	Automatically set for static IPv6 address, representing the number of bits of the SLAAC assigned IPv6 address that define the subnet network prefix. (default = 64).
IPv4 control port configuration		

Parameter		Description
	IPv4	Enables/disables IPv4 IP addressing for the control port, when the control port is enabled. Default = enabled.
	Mode	Identifies the source of the IPv4 address: • Default: An IP address is automatically assigned by the software. • Static (default): Enables the **IPv4 @**, **Subnet mask**, and **Default gateway** fields for inputting a static IPv4 IP address for the control port.
	IPv4 @	If the selected mode is: • **Default**: The IP address is automatically assigned; the **IPv4 @**, **Subnet mask**, and **Default gateway** fields are disabled. • **Static**: Enter a valid IPv4 address for the control port.
	Subnet mask	If **Static** is selected as the **Mode**, above, enter a valid IPv4 subnet mask for the control port, which determines the network portion of the IPv4 address.
	Default gateway	If **Static** is selected as the **Mode**, above, enter a valid IPv4 address for the default gateway.
Backplane port		
	IPv4 @	Enter a valid IPv4 address for the backplane port.
Source Timestamping		Refer to the topic Configuring Source Time Stamping, page 119.
Fast sampling rate		When selected, you can configure the OPC UA client with a minimum sampling interval of 20 ms, which permits monitoring of 2,000 items. De-selected by default, the default sampling period is 250 ms, permitting monitoring of the equivalent of 20,000 INT type items. **NOTE:** A change in this setting is effective only after a full download of the application.
OPCUA TCP Listening Port		The TCP port for OPCUA communication, either: • By default: pre-set to port 4840 • Other value: user-specified **NOTE:** The value of this port needs to be the same for all BMENUA0100 modules communicating together (for example, in the case of OPC UA NAT forwarding between several BMENUA0100 modules)

NOTE: When configuring your application in Control Expert:

- The **Ethernet Network** window (opened via **Tools > Ethernet Network Manager...**) displays settings for both the backplane port and the control port for the BMENUA0100 module, including information for the NTP server, SNMP manager, and - for a Hot Standby system - the standby BMENUA0100 module (B).
- The **Address Server** page of the controller (opened in the **DTM Browser** by double-clicking on the controller, then selecting **Services > Address Server**) displays the backplane port IP address of the BMENUA0100 module. In a Hot Standby configuration, the **Address Server** page of the controller displays the backplane port IP address for both BMENUA0100 modules.

Configuring Source Time Stamping

Source time stamping is supported by firmware version 2.01 (and later) of the BMENUA0100 module (BMENUA0100.2) in Control Expert.

To use source time stamping in an application, you need to enable then activate it.

After source time stamping is both enabled and activated, the BMENUA0100 module begins polling devices when there is at least one monitored item with **Monitoring mode** set to **Sampling** or **Reporting** in OPC UA client.

NOTE: Values are retrieved from an at-source-time-stamping device only for BOOL and EBOOL variables that are:

- configured as at-source-time-stamped (ASTS) in Control Expert.
- monitored by an OPC UA client as part of OPC UA subscription.

If the OPC UA node has not been added to – and monitored as part of – a subscription, the OPC UA synchronous read service will detect and report an error.

Enabling Source Time Stamping

Source time stamping is enabled in the Project Settings window. Navigate to **General > Time > Time Stamping Mode** then select **System**.

NOTE: The default **Time Stamping Mode** setting is **Applicative**. If you do not change the default setting to **System**, then a detected error is displayed when the application is built.

Activating Source Time Stamping

Use the **IPConfig** tab of the BMENUA0100 configuration dialog box to activate and configure time stamping.

In the **Source Timestamping** section, configure the following settings:

Setting	Description
Activated	Activates source time stamping for the application.
Polling of buffer (ms)	The polling rate for event read requests handled by the BMENUA0100. The valid settings range is from 250 ms minimum to 5000 ms maximum in increments of 250 ms. **NOTE:** The maximum number of source time stamped variables in Control Expert is 5000.

NOTE: If the M580 local rack includes two BMENUA0100 modules, source time stamping can be used by only one module. Refer to the topic Specifying the BMENUA0100 to Manage Timestamped Variables, page 122.

Managing At-Source-Time-Stamped Variables

Using `#TSEventItemsReady` and `#TSEventSynchro` OPC UA Dataitems

You can use the OPC UA-specific data items `#TSEventItemsReady` and `#TSEventSynchro` to browse and set, respectively, the state of at-source-time-stamped variables.

NOTE: Both data items are meaningful only when time-stamping is enabled in Control Expert and activated for the specific BMENUA0100 module.

The BMENUA0100 treats the `#TSEventSynchro` dataitem as a Boolean OPC UA node.

Setting the `#TSEventSynchro` item sends a synchronize command to all at-source-time-stamped devices of the M580 controller. The values returned to the OPC UA client by the devices initialize the at source timestamped variables to their present values.

The BMENUA0100 responds to the client setting the `#TSEventSynchro` item with one of the following messages:

- `UA_EGOOD`: The synchronization request was correctly sent to all timestamping devices.
- `UA_EBAD`: The synchronization request did not succeed because timestamping is disabled in the Control Expert project.
- `UA_EBADINVALIDSTATE`: The synchronization request did not succeed because timestamping was turned OFF for the BMENUA0100 module by the %MW400 feature, page 122.
- `UA_EBADINUSE`: The synchronization request did not succeed because the BMENUA0100 module could not reserve timestamping buffer.

- `UA_EBADDISCONNECT`: The synchronization request timed out and could not write the values in the specified time frame.

To perform this initialization, use an OPC UA client - for example UaExpert - to perform the following sequence of tasks:

1. Monitor the `#TSEventItemsReady` item which indicates the BMENUA0100 module is ready to manage timestamped variables of the controller buffers (including the M580 controller, BMECRA31310, BMXERT1604), and then wait for its value to change to 1 (TRUE).
2. Add monitored data items configured as at-source-time-stamped variables to one or more subscriptions.
3. Set the `#TSEventSynchro` write command to update the value and at-source-time-stamp of each item.

NOTE:

- The BMENUA0100 reads all configured timestamped variables in the controller. If an event (item state change) occurs on a timestamped monitored item, that item is updated. If an item is not monitored, it is discarded.
- Set the data change filter to **Status/Value/Timestamp**. Otherwise, it is possible that different OPC UA clients - for example clients that update values only on Status/Value changes - will display a different status and value for the same variable.
- Because the BMENUA0100 updates values periodically, it is possible that multiple events could occur since the previous update. In that case, the BMENUA0100 displays only the most recent value.
- Because `#TSEventSynchro` is sent to multiple timestamping devices, if any single device does not respond within the expected time frame, the `#TSEventSynchro` setting returns the response `UA_EBADDISCONNECT` indicating the command timed out and did not succeed. This is true even if other devices successfully respond.
- If the subscription is edited to contain, for example, only one variable for one device, executing `#TSEventSynchro` causes the loss of previously returned values for previously subscribed devices and variables.

Determining the M580 Controller Channels Dedicated to Timestamping

For communication between the BMENUA0100 and an M580 controller, where timestamping is enabled in Control Expert, 25% of the controller channels are dedicated to support the timestamp feature. A maximum of 75% of the controller channels remain available to carry other communication requests.

For example, for the BMEP584040 controller:

- Maximum number of channels: 13
- Channels used for timestamping: 3

- Channels used for non-timestamping: 10

Determining the Capacity of the BMENUA0100 to Read Timestamped Variables

The number of timestamped variables the BMENUA0100 can read per cycle depends on:

- The **Polling of buffer** setting in the **IP Config** tab of the module, and
- The capacity of the at source device, including:
  - The maximum number of TCP connections, and
  - The maximum number of supported at-source-time-stamped variables.

The formula for determining the maximum number of at-source-time-stamped variables for a device is:

((Max number of TCP connections) / (Number of channels)) x (Max number of timestamped variables per cycle)

For example:

- BMEP586040(C): 16 max connections, 4 channels, 82 max variables:

  ((16 / 4) x 82 = 328 total variables

  If **Polling of buffer** = 500 ms: 656 variables per second.
- BMECRA31310: 1 connection, 1 channel, 82 max variables:

  1 x 82 = 82 total variables

  If **Polling of buffer** = 500 ms: 164 variables per second.
- BMXERT1604: 1 connection, 1 channel, 20 max variables:

  1 x 20 = 20 total variables

  If **Polling of buffer** = 500 ms: 40 variables per second.

Specifying the BMENUA0100 to Manage Timestamped Variables

An M580 main rack can contain two BMENUA0100 modules. However, timestamped variables in the M580 controllers, BMECRA31310, and BMXERT1604 modules can be read and managed by only one BMENUA0100 module at a time. On startup, each BMENUA0100 by default attempts to reserve and lock access to timestamped variables.

In a rack with two BMENUA0100 modules, you need to specify the one that will read and manage timestamped variables. To specify the BMENUA0100 that will read and manage variables, do the following:

1. In the **IPConfig** tab for the two BMENUA0100 modules you want to have timestamping, select **Activated**.
2. For the BMENUA0100 module that you want to reserve the timestamping buffer, use the `WRITE_VAR` block to set the %MW400 word to 2, which turns ON reading and managing timestamped variables for this module.

   NOTE: Setting %MW400 = 2 identifies the BMENUA0100 module that will read and manage variables when two BMENUA0100 modules have the **Activated** setting selected.
3. For the other BMENUA0100 module that you do not want to reserve the timestamping buffer, use the `WRITE_VAR` block to set the %MW400 word to 1, which turns OFF reading and managing timestamped variables for these modules.

NOTE: You need to perform these steps after each change in operating mode, including cycling power ON, or loading the application, or performing an initialization.

The BMENUA0100 you specify retains control of reading and managing timestamped variables so long as both of the following conditions continue to exist:

- At least one timestamped variable is monitored.
- The BMENUA0100 **Monitoring mode** is set to either **Reporting** or **Sampling**.

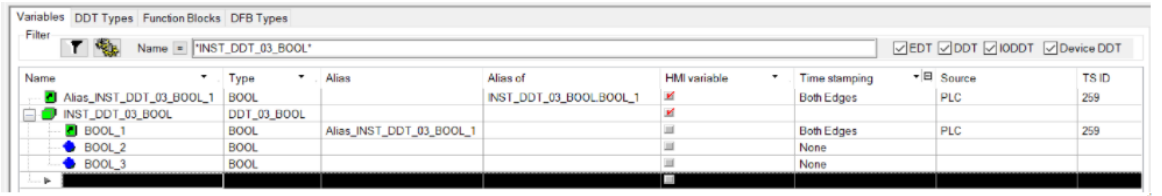
NOTE:

When the **Activated** setting is de-selected, variables values read by the BMENUA0100 are the values in controller memory.

When the **Activated** setting is selected and %MW400 has been set to 1, variable values read by the BMENUA0100 retain the last value read when the timestamping buffer was reserved.

Monitoring Timestamped Alias Variables

The BMENUA0100 recognizes time stamped BOOL or EBOOL **Alias** variables created in Control Expert, but will not similarly recognize any corresponding **Alias of** variables. An example of **Alias** and **Alias of** variables is shown below:



To be recognized by the BMENUA0100, the **Alias** variables need to be embedded in the data dictionary.

BOOL or EBOOL **Alias** variables and their corresponding **Alias of** variables share both the same logical address inside M580 memory and the same EventID in the M580 timestamping buffer. Source timestamping is managed only on the **Alias** and not on **Alias of** variable. In other words, you need to subscribe the **Alias** variable (OPC UA node) in the OPC UA client to be able to receive the source timestamping from the device instead of from the BMENUA0100 module.

Because neither the BOOL or EBOOL **Alias of** variable is seen as being at-source-time-stamped by the BMENUA0100 firmware, the **Alias** must be embedded in data dictionary. In that case, you need to add the **Alias** variable as a monitored item in an OPC UA subscription, in order to achieve source timestamping set by the device.

Configuring the Network Time Service

Introduction

The BMENUA0100 Ethernet communications module with embedded OPC UA server supports version 4 of the network time protocol (NTP). The NTP service synchronizes the clock in the BMENUA0100 module with the clock of a time server. The synchronized value is used to update the clock in the module.

Both IPv4 and IPv6 protocols are supported.

NOTE:

- If the NTP server resides in the controller, the BMENUA0100 module can update its time settings without introducing delay.
- When a new NTP server is reached or if there is a time offset on an NTP server, it can take up to 5 minutes to update the BMENUA0100. The **ERR** LED, page 131 remains ON until the BMENUA0100 time is synchronized with the NTP server.
- Manually configuring a time change, by inputting a future time, may disconnect the existing OPC UA channels. If the OPC UA client performs an automatic reconnection to the OPC UA server, new channels will be created and the re-connection performed.

Enabling and Disabling the NTP Client and the NTP Server

The BMENUA0100 module includes both an NTP server and an NTP client.

NTP Client:

If either the primary or secondary NTP server IP address is set to a value other than 0.0.0.0, the NTP client is enabled. If both the primary and secondary NTP server IP address settings are empty, or are set to 0.0.0.0 (IPv4) or 0000:0000:0000:0000:0000:0000:0000:0000 (IPv6), the NTP client is disabled.

NOTE: When both **Primary NTP Server** and **Secondary NTP Server** IP address settings are set to 0.0.0.0, the BMENUA0100 module cannot operate as either NTP client or NTP server.

NTP Server:

The NTP server is enabled, depending on the cybersecurity operating mode:

- In Advanced (or Secured) Mode, the NTP server is enabled if:
  - Either the primary or secondary NTP server IP address setting is set to a non-null value (i.e., set to a value other than 0.0.0.0); and
  - The NTP Server is set to enabled, in the **Network Services** web page, page 94 configuration settings.
- In Standard mode, the NTP server is enabled if either the **Primary NTP Server** or **Secondary NTP Server** IP address setting is set to a non-null value (i.e., set to a value other than 0.0.0.0).

  NOTE: If the BMENUA0100 is configured as NTP client on the backplane network (**Primary NTP Server** or **Secondary NTP Server**), the BMENUA0100 NTP server cannot be enabled for another device.

When both the NTP server and NTP client are enabled in the BMENUA0100 module, the module NTP client receives time settings over its control port from a remote NTP server. The module NTP server forwards these time settings over its backplane port to NTP clients.

NOTE: The BMENUA0100 module cannot operate as NTP server over its control port.

NTP Polling

The BMENUA0100 module optimally and dynamically manages the NTP polling period with the NTP server. No configuration is necessary.

Power Up

To establish the accurate Ethernet system network time, the system performs these tasks at power up:

- The BMENUA0100 communications module powers up.
- The BMENUA0100 communications module obtains the time from the NTP server.
- The service requires the requests to be sent periodically to obtain and maintain accurate time. Your **Polling Period** configuration impacts the accuracy of the time.

After an accurate time is received, the service sets the status in the associated time service diagnostic.

NOTE: The BMENUA0100 communications module does not maintain the time. Upon power up or power cycle, the clock value of the module is 0, which is equivalent to January 1 1980 00:00:00:00.

Configuring the Service

Configure the network time synchronization service in Control Expert, as follows:

Step	Action
1	In the **Project Browser** expand the **PLC Bus** node and open the BMENUA0100 module configuration dialog box.
2	Click on the **NTP** tab.
3	Enter changes in the appropriate fields on the **Network Time Service** configuration page. (The following table describes the configuration page parameters.)

Configurable Parameters

Configure these time synchronization parameters for each BMENUA0100 communications module in your project:

Parameter		Description
IPv4 NTP server configuration		
	Primary NTP Server (see Note)	Enter a valid IPv4 or IPv6 address for the primary NTPv4 server. **NOTE:** Set to the controller main IP address by default.
	Secondary NTP Server (see Note)	Enter a valid IPv4 or IPv6 address for the secondary NTPv4 server.
NOTE: • Configure NTP server address that can be reached by the BMENUA0100 module. If the control port is disabled, enter NTP server IP addresses that are in the same subnet as the backplane port. • You can configure an IPV4 address for the Primary NTP Server and an IPV6 address for the Secondary NTP Server (and vice versa), if both addresses are in the same domain. • For Hot Standby configurations, the NTP serve addresses for **NUA(A)** and **NUA(B)** need to be in the same network, for example, the network accessible via the backplane port, or the network accessible via the control port.		

NOTE: When operating in Advanced (or Secured) Mode, verify that the NTP service is enabled in the Network Services Activation, page 94 section of the **Settings** web page.

SNMP Agent Configuration

About SNMP

All firmware versions of the BMENUA0100 module support the version 1 (V1) SNMP agent. Firmware version 2 (and later) of the module (BMENUA0100.2) also supports version 3 (V3) of the SNMP agent.

NOTE: Both SNMP versions, V1 and V3, are not simultaneously supported.

An SNMP agent is a software component of the SNMP service that runs on the BMENUA0100 module and provides access to diagnostic and management information for the module. You can use SNMP browsers, network management software, and other tools to access this data.

In addition, the SNMP agent can be configured with the IP addresses of 1 or 2 devices (typically PCs that run network management software) to be the targets of event-driven trap messages. Such messages inform the management device of events like cold starts and the inability to authenticate a device.

NOTE: Communication to the SNMP agent running on the BMENUA0100 module can be performed using either IPv4 or IPv6 addressing.

Termination of SNMP Service

The SNMP service running on the BMENUA0100 module is terminated if:

- the module is in the ERROR state.
- the SNMP service is in the FAULT state.

Access the SNMP Tab

Double-click the BMENUA0100 module in the Control Expert configuration to access the **SNMP** tab.

The SNMP agent can connect to and communicate with 1 or 2 SNMP managers. The SNMP service includes:

- authentication checking by the BMENUA0100 module of any SNMP manager that sends SNMP requests.
- management of events or traps.

SNMP Agent Configuration in Control Expert and the Web Pages

Common SNMP parameters are configured in Control Expert. Cybersecurity related SNMP parameters are configured in module web pages.

If the cybersecurity rotary selector switch is set to:

- Advanced (or Secured) mode: you can configure the SNMP agent in both Control Expert and the BMENUA0100 module's web pages.

  NOTE: In Advanced (or Secured) mode, the SNMP version needs to be configured the same in both Control Expert, and in the SNMP web page, page 100. If these settings are not the same, the SNMP service does not start.

- Standard mode: you can configure the SNMP agent only in Control Expert.

  NOTE: If the module is configured for SNMP V3 in Control Expert:

  - The BMENUA0100.2 module, equipped with firmware version 2 or later, operates SNMP V3 with NoAuthNoPriv security level.
  - The BMENUA0100 module, with firmware earlier than version 2, operates SNMP V1.

SNMP Parameters

The Control Expert **SNMP** tab includes the following parameters. Unless otherwise indicated, parameters apply to both SNMP V1 and V3.

NOTE: In Advanced (or Secured) mode, the SNMP version needs to be configured the same in both Control Expert, and in the SNMP web page, page 100. If these settings are not the same, the SNMP service does not start.

Field	Parameter	Description	Value
SNMP Version	SNMP V1	Select this to use SNMP V1	selected/cleared
	SNMP V3	Select this to use SNMP V3	
IP Address managers	IP Address manager 1	The IPv4 address of the first SNMP manager to which the SNMP agent sends notices of traps.	Protocol (IPv4) dependent
	IP Address manager 2	The IPv4 address of the second SNMP manager to which the SNMP agent sends messages of traps.	

Field	Parameter	Description	Value
Agent	Location (SysLocation)	device location	31 characters (maximum)
	Contact (SysContact)	information about the person to contact for device maintenance	
	Enable SNMP manager	*cleared* (default): You can edit the **Location** and **Contact** parameters. *selected*: You cannot edit the **Location** and **Contact** parameters.	selected/cleared
Community names (SNMP V1 only)	Set	password that the SNMP agent requires to read commands from an SNMP manager **NOTE:** There is no default setting. If an SNMP manager is used, input the same community name used by the SNMP manager.	15 characters (maximum)
	Get		
	Trap		
Security (SNMP V1 only)	Enable **Authentication failure** trap	*cleared* (default): not enabled. *selected*: Enabled. The SNMP agent sends a trap message to the SNMP manager if an unauthorized manager sends a **Get** or **Set** command to the agent.	selected/cleared
SNMP User Name (SNMP V3 only)		The user name recognized by the SNMP server.	string of 32 characters max ASCII / UTF8 in the encoding range [33-122]

Supported Traps

By default, the BMENUA0100 module SNMP V1 agent supports the following traps:

- Linkup
- Linkdown

The **Authentication failure** trap is also supported, if enabled.

SNMP MIB-II Object Identifiers

Under the **Vendor Name** Schneider Electric, the BMENUA0100 module presents the following object identifier (OID) values:

Object Name	OID	Value
SysDesc	1.3.6.1.2.1.1.1	Product: BMENUA0100 - OPC UA communication module. Firmware ID: xx.yy
SysObjectID	1.3.6.1.2.1.1.2	1.3.6.1.4.1.3833.1.7.255.53
SysName	1.3.6.1.2.1.1.5	BMENUA0100
SysServices	1.3.6.1.2.1.1.7	74, representing the sum of (2_{7-1} + $_{24-1}$ + 2_{2-1}) and indicating support of protocols in the following OSI layers: • 7: application layer • 4: transport layer • 2: data-link layer
ifDesc	1.3.6.1.2.1.2.2.1.2	This OID contains information describing the interface, including the product name, and port name.

Configuring M580 Controller Settings for OPC UA Client - Server Connections

Introduction

This section describes settings made to the M580 controller configuration to support connections between the OPC UA server in the BMENUA0100 module and an OPC UA client.

Configuring M580 Controller Security Settings

Configuring Controller Services

To support communications between the OPC UA server in the BMENUA0100 module and an OPC UA client, enable the following settings in the Security tab of the M580 controller:

- **TFTP**
- **DHCP / BOOTP**

If both of these services are not enabled in the controller, OPC UA communications do not operate properly.

Diagnostics

Overview

This chapter describes the diagnostic tools available for the BMENUA0100 Ethernet communication module with embedded OPC UA server.

LED Diagnostics

Display Panel LED Diagnostics

The state of the BMENUA0100 module display panel LEDs, page 24 are presented, below, for the several operating states of the module.

NOTE: The state of the **SECURE** LED for the configured and non-configured state of the module are separately presented, below, following the initial presentation.

Operating State		LEDs						
		RUN (Green)	**UACNX (Green/ Red)**	**ERR (Red)**	**BS (Green/ Red)**	**NS LED (Green/ Red)**	**BUSY (Yellow)**	**SEC (Green/ Red)**
Power on sequence	1	OFF	ON	ON	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red ON
	2 (All LEDs ON)	ON	ON	ON	Green ON Red ON	Green ON Red ON	ON	Green ON Red ON
	3 (All LEDs OFF)	OFF	OFF	OFF	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
	4	ON	OFF	ON	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
	5 (Autotest[1])	Flashing	Flashing	Flashing	Green Flashing Red OFF	Green Flashing Red OFF	Flashing	Green Flashing Red OFF
Not configured		OFF	OFF	Flashing	Red flashing if not connected to an Ethernet Backplane port. Flashing green otherwise.	OFF if not cable plugged and connected to another powered device. Flashing green otherwise.	OFF	Refer to cyber-security LEDs, below, page 134.

Operating State		LEDs						
		RUN (Green)	**UACNX (Green/Red)**	**ERR (Red)**	**BS (Green/Red)**	**NS LED (Green/Red)**	**BUSY (Yellow)**	**SEC (Green/Red)**
Configured	After detecting a duplicated IPv4 address on backplane port	Flashing	Refer to description of **UACNX** LED, below, page 134	/	Green OFF Red ON	/	/	Refer to description of Secure Communication Status LED, below, page 134.
	After detecting a duplicated IPv4 address on Control Port	Flashing		/	/	Green OFF Red ON	/	
	RUN State	ON		OFF	Green ON Red OFF	Steady green if connected; Off if disconnected.	ON if data-dictionary acquisition in progress; Flashing if data dictionary overflow; otherwise OFF	
Power Off		OFF	OFF	OFF	Green OFF Red OFF	Green OFF Red OFF	OFF	Green OFF Red OFF
Recoverable Detected Error or Inconsistent Configuration[2]		/	/	ON	/	/	/	/
Non-recoverable Detected Error (Module will reboot)		OFF	OFF	ON	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red ON
Cybersecurity (or Security) Reset	In progress	Flashing	OFF	OFF	Green OFF Red ON	Green OFF Red ON	ON	Green OFF Red OFF
	Complete	ON	OFF	OFF	Green OFF Red ON	Green OFF Red ON	OFF	Green OFF Red OFF
Missing Cybersecurity (or Security) Reset[3]		OFF	OFF	ON	Green OFF Red ON	Green OFF Red ON	OFF	Flashing Red

Operating State	LEDs						
	RUN (Green)	**UACNX (Green/Red)**	**ERR (Red)**	**BS (Green/Red)**	**NS LED (Green/Red)**	**BUSY (Yellow)**	**SEC (Green/Red)**
OS Update	Flashing	OFF	OFF	Green OFF Red ON	Green OFF Red ON	ON	Green OFF Red OFF

1. The autotest is performed quickly and LED flashing cannot be visually detected.

NOTE: If the module remains in Autotest state, verify the rotary switch to confirm that it is in a valid position.

2. Refer to SERVICES_STATUS detected error codes in the T_BMENUA0100 DDT, page 136.

3. This state results from changing the rotary switch from Standard to Advanced (or Secured) mode, or from Advanced (or Secured) to Standard mode without performing a Cybersecurity (or Security) Reset, page 28 as an intermediate step.

NOTE: In this table, "/" indicates any state.

UACNX LED When the Module is in Configured State

The color (red or green) and state (flashing or steady) describe the state of the OPC UA connections:

Data Dictionary State	OPC UA Client Connection State	
	No OPC UA Client Connected	**At Least 1 OPC UA Client Connected**
Data Dictionary Unavailable	Flashing Red	Steady Red
Data Dictionary Available	Flashing Green	Steady Green

Secure Communications Status LED When the Module is Configured/Not Configured State

The states of the **SECURE** LED, when the module is in the configured or not configured state, are described below:

LED State	Description
OFF	The module is not operating in secure operating mode (i.e., the rotary switch is not set to the secure position).
RED	A secure communications critical error is detected. For example, no security configuration is present, a certificate is invalid, a certificate has expired and communications have stopped, and so forth.

LED State	Description
GREEN	Secure communications are enabled and running without detected error. A client is connected to the module and the module has received a valid cybersecurity configuration. The session is opened and the module is ready to respond to client requests.
FLASHING RED	Secure communications are enabled and running, but an error has been detected. For example, a certificate has expired but the configuration authorizes communications to continue.
FLASHING GREEN	The module has received a valid cybersecurity configuration and is ready to communicate with a client which will initiate a communication.

Control Port LED Diagnostics

The control port LEDs, page 25 can be used to diagnose the state of Ethernet communications over the control port:

LED	State	Description
ACT	Off	No link established.
	Green	Link established, no activity.
	Flashing Green	Link established, activity detected.
LNK	Off	No link established.
	Yellow	Link established at speed less than module maximum capability (10/100Mbps).
	Green	Link established at speed equal to module maximum capability (1000Mbps).

BMENUA0100 Derived Data Type (DDT)

Introduction

Each BMENUA0100 Ethernet communication module with embedded OPC UA server that you add to your application instantiates a common collection of data elements. You can use the tools presented in the Control Expert software to access these data elements and diagnose the module.

NOTE:

- DDT data returned in response to a Modbus request cannot exceed 256 bytes in length.
- Given the organization of the Control Expert data dictionary, requests for data stored in bits of words need to be extracted by the requesting client.

The contents of the DDT can be accessed using the READ_DDT, page 141 elementary function (EF) in Control Expert software.
s

NOTE: If the module DDT cannot be read for any reason – for example if the backplane IP address is not properly configured – you can perform module diagnostics via the module LEDs, page 131.

T_BMENUA0100 DDT Structure

The BMENUA0100 DDT includes the following elements:

Element	Type	Address	Description
DEVICE_NAME	STRING [16]	MW1...8	The module name.
CONTROL_PORT_IPV6	STRING [44]	MW9...30	Control Port IPv6 / subnet prefix length.
CONTROL_PORT_IPV4	STRING [18]	MW31...39	Control Port IPv4 / subnet prefix length.
CONTROL_PORT_GTW	STRING [16]	MW40...47	Control Port default gateway.
ETH_BKP_PORT_IPV4	STRING [18]	MW48...56	Backplane Port IPv4 / subnet prefix length.
ETH_STATUS	WORD	MW57	–
PORT_CONTROL_LINK	BOOL	MW57.0	• 0: Control port link is not operational. • 1: Control port link is operational.
ETH_BKP_PORT_LINK	BOOL	MW57.1	• 0: Backplane port link is not operational. • 1: Backplane port link is operational.
GLOBAL_STATUS	BOOL	MW57.2	• 0: Module is not operational. • 1: Module is operational.
NETWORK_HEALTH	BOOL	MW57.3	• 0: Network overload condition is detected. • 1: Network is operating normally.
Reserved	–	MW57.4...15	–

Element	Type	Address	Description
OPCUA_STATUS	T_OPCUA_STATUS	MW58...61	See details below.
DATA_DICT	BYTE	MW58[0]	• 1: Not available. Possible causes: ◦ The data dictionary functionality is not available or enabled in the Control Expert application and cannot be embedded in the controller. ◦ The loading/browsing of the data dictionary is in progress in OPC UA Server. • 2: Available, for example: ◦ The loading/browsing of the data dictionary by the OPC UA server completed with success. ◦ A pre-loading (in accordance with Control Expert data dictionary project settings) can be in progress. • 4: Busy. • 8: Data dictionary overflow.
DATA_DICT_ACQ_DURATION	BYTE	MW58[1]	Duration of last acquisition (0...255 seconds). **NOTE:** A value of 255 indicates a duration time equal to or greater than 255 seconds.
CONNECTED_CLIENTS	BYTE	MW59[0]	Number of connected OPC UA clients.
DATA_DICT_PRELOAD_DURATION	BYTE	MW59[1]	Duration of last data dictionary pre-load (0...255 seconds). **NOTE:** You can use the information contained in this element to adjust and optimize the **Effective Build changes time-out** setting in the **Tools > Project Settings > General > PLC embedded data** configuration window. Refer to Control Expert online help for information on how to configure this setting.
REDUNDANCY_MODE	BYTE	MW60[0]	• 0: None • 2: Non-transparent (“Hot”) redundancy mode.
SERVICE_LEVEL	BYTE	MW60[1]	OPC UA server health, page 147, depending on the data and service quality.
Reserved	WORD	MW61	–
SERVICES_STATUS	T_SERVICES_STATUS	MW62...68	See details below.

Element	Type	Address	Description
NTP_CLIENT_SERVICE	BYTE	MW62[0]	NTP client status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code: ◦ 1 = Invalid Time (Time never updated) ◦ 2 = Time catch up (Server time has increased or decreased by an offset of at least 1000 seconds. The BMENUA0100 module can take up to 5 minutes to be re-synchronized.) ◦ 4 = NTP server is still reachable, but does not synchronize client. When the NTP server resumes operations, the detected error will be resolved automatically. This may take up to 1024 seconds.
NTP_SERVER_SERVICE	BYTE	MW62[1]	NTP server status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code - Advanced (or Secured) Mode only: ◦ 1 = Control Port not configured ◦ 2 = NTP client of backplane and server enabled in web pages
SNMP_SERVICE	BYTE	MW63[0]	SNMP server status: • Bit 0: 0 = Inactive / 1 = Active • Bit 1 (SNMP V1): 0 = SNMP not configured / 1 = SNMP configured • Bits 1 & 2: (SNMP V3): 00 = SNMP not configured / 11 = SNMP configured • Bits 4...7: Detected error code: ◦ 1 = SNMP is enabled in Advanced (or Secured) Mode and no SNMP IP address is defined in Control Expert (0.0.0.0)
Reserved	BYTE	MW63[1]	–
WEB_SERVER	BYTE	MW64[0]	Web server status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code: ◦ 1 = Non-recoverable detected error
FW_UPGRADE	BYTE	MW64[1]	Firmware upgrade status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code: ◦ 1 = Invalid firmware package ◦ 2 = Last firmware update was not successful (managed as a non-recoverable detected error)

Element	Type	Address	Description
Reserved	BYTE	MW65[0]	–
Reserved	BYTE	MW65[1]	–
CONTROL_EXPERT_IP_ FORWARDING	BYTE	MW66[0]	Control Expert IP forwarding status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code (Advanced (or Secured) Mode only): ◦ 1 = Control port not configured **NOTE:** For modules with firmware version 2.01 and later, the value of this element is forced to 0.
CPU_TO_CPU_IP_ FORWARDING	BYTE	MW66[1]	Controller to controller forwarding status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code (Advanced (or Secured) Mode only): ◦ 1 = Control port not configured **NOTE:** For modules with firmware version 2.01 and later, the value of this element is forced to 0.
IPSEC	BYTE	MW67[0]	IPsec status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code (Advanced (or Secured) Mode only): ◦ 1 = Control port not configured
Reserved	BYTE	MW67[1]	–
EVENT_LOG_SERVICE	BYTE	MW68[0]	Event log service status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code (Advanced (or Secured) Mode only): ◦ 1 = Service event log detected error. ◦ 2 = Event log configuration detected error
LOG_SERVER_NOT_ REACHABLE	BYTE	MW68[1]	Log server status: • Bit 0: 0 = acknowledgement received from syslog server / 1 = No acknowledgement received from syslog server
FW_VERSION	T_FW_ VERSION	MW69...72	Module firmware version. See details below.
MAJOR_VERSION	WORD	MW69	Major firmware version.
MINOR_VERSION	WORD	MW70	Minor firmware version.
INTERNAL_REVISION	WORD	MW71	Firmware internal revision.
Reserved	WORD	MW72	–

Element	Type	Address	Description
CONTROL_PORT_STATUS	BYTE	MW73[0]	Control Port IPv4 status: • Bit 0: 0 = Inactive / 1 = Active • Bits 4...7: Detected error code (Advanced (or Secured) Mode only): ◦ 1 = Invalid IP ◦ 2 = Duplicate IP
Reserved	BYTE	MW73[1]	–
IN_PACKETS_RATE	UINT	MW74	Number of packets received per second on all Ethernet interfaces.
IN_ERROR_COUNT	UINT	MW75	Number of inbound packets with detected errors since last reset (modulo 65535).
OUT_PACKETS_RATE	UINT	MW76	Number of packets emitted per second on all Ethernet interfaces.
OUT_ERROR_COUNT	UINT	MW77	Number of outbound packets with detected errors since last reset (modulo 65535).
MEM_USED_PERCENT	BYTE	MW78[0]	Percentage of internal RAM used by OPC UA server.
CPU_USED_PERCENT	BYTE	MW78[1]	Percentage of internal processor used.
CYBERSECURITY_STATUS	T_CYBER SECURI-TY_ STATUS	MW79...80	Cybersecurity status. See details below.
SECURE_MODE	BYTE	MW79[0]	• 0: The module is operating in Standard mode. • 1: The module is operating in Advanced (or Secured) Mode.
CYBERSECURITY_STATE	BYTE	MW79[1]	Cybersecurity status: • 0: Advanced (or Secured) Mode OFF. (**SECURE** LED OFF) • 1: A secure communications enabled and running without detected error. (**SECURE** LED GREEN) • 2: Ready to communicate. (**SECURE** LED FLASHING GREEN) • 3: Secure communication running with minor detected errors. (**SECURE** LED FLASHING RED) • 4: Secure communications stopped because of critical detected error. (**SECURE** LED RED)
IPSEC_CHANNELS	BYTE	MW80[0]	The number of IPsec channels opened.
Reserved	BYTE	MW80[1]	–

Configuring the READ_DDT Elementary Function

Overview

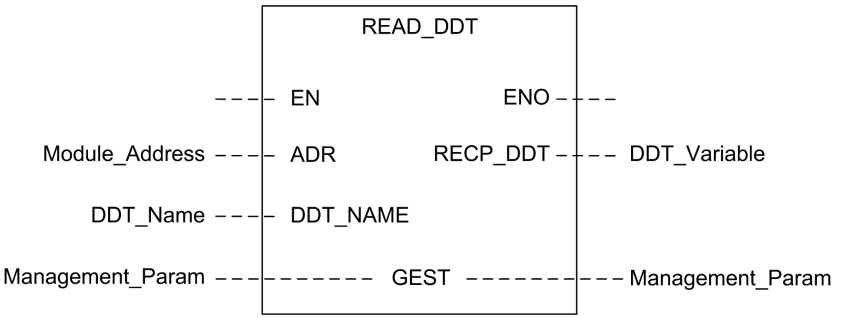
Use the READ_DDT function block to configure read messages for the BMENUA0100 communication module.

The ADR, the DDT_NAME, and the GEST parameters define the operation.

EN and ENO can be configured as additional parameters.

NOTE: For information about using this function block in a Hot Standby system, refer to the topic Asynchronous Communication Function Blocks (see *Modicon M580 Hot Standby Frequently Used Architectures System Guide*).

FBD Representation



Input Parameters

Parameter	Data type	Description
EN	BOOL	This parameter is optional. When this input is set to one, the block is activated and can solve the function blocks algorithm. When this input is set to zero, the block is deactivated and does not solve the function block algorithm.
ADR	Any Array of INT	Array containing the address of the destination entity of the exchange operation. The address is the result of the ADDMX function. (For example: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indicates the module at IP address 192.168.10.2, with UnitId 100 (local server of the module), connected to the embedded Ethernet port.
DDT_NAME	STRING	Name of DDT to read: T_BMENUA0100

Input/Output Parameters

The GEST array is local:

Parameter	Data type	Description		
GEST	Array [0...3] of INT	The management parameters, consisting of four words. Refer to the Control Expert help topic *Structure of the Management Parameters* (see *EcoStruxure™ Control Expert, Communication, Block Library*) for additional information regarding these parameters.		
		Word#	**Most Significant BYTE**	**Least Significant BYTE**
		0	Exchange number	Activity bit: rank 0 Cancel bit: rank 1 Immediate acknowledge bit: rank 2
		1	Operation report (see *EcoStruxure™ Control Expert, Communication, Block Library*)	Communication report (see *EcoStruxure™ Control Expert, Communication, Block Library*)
		2	Timeout (see *EcoStruxure™ Control Expert, Communication, Block Library*)	
		3	Length (see *EcoStruxure™ Control Expert, Communication, Block Library*)	

Output Parameters

Parameter	Data type	Description
ENO	BOOL	This parameter is optional. When you select this output you also get the EN input. ENO output is activated upon successful execution of the function block.
RECP_DDT	Any	Reception buffer. A DDT variable may be used. Refer to the T_BMENUA0100 DDT description, page 135 for the content of this DDT. The size of the data received (in bytes) is written automatically by the system in the fourth word of the management table.

Asynchronous Communication Function Block

In a Hot Standby application during a switchover event, the READ_DDT asynchronous communication function block does not automatically resume operation on the new Primary controller, unless specifically configured, as follows.

Use the following procedure to allow asynchronous communication EFBs to automatically resume operation after a switchover:

- Program your application so that all EFB instances are not exchanged with the Standby controller. To do this, de-select the **Exchange on STBY** attribute for the EFB instance.

Considerations when Configuring the Function

When using the READ_DDT EF, consider the following:

- If your application includes more than one BMENUA0100 in a rack, use separate instances of a WORD array for each GEST pin. Each block manages it own management WORD array.
- You do not need to specify a value for the length parameter in GEST[3], because there is no data to send. At the end of the operation (when the activity bit in GEST[0] is set to 0), the length is set with the length of the data copied into the RECP_DDT output parameter if no detected error is reported in GEST[1] or with an additional status code. Refer to the Control Expert help topic *Error Codes of EFBs with STATUS parameter* (see *EcoStruxure™ Control Expert, Communication, Block Library*) for a description of these additional status code values.
- A timeout value of 0 indicates no timeout. In this case, a communication delay or loss occurring during the exchange operation is not detected. The RECP_DDT parameter retains its previous value. To avoid this scenario, set the timeout to a non-zero value.
- In case of operation report 16#01 (Request not processed) or 16#02 (Incorrect response) in the GEST[1] word of the management table, an additional status code may be reported in the length parameter (GEST[3]). Status codes returned in this field correspond to a subrange of the possible STATUS parameter codes of communication EFBs. Possible values for the READ_DDT are 30ss hex and 4001 hex. Refer to the Control Expert help topic *Error Codes of EFBs with STATUS parameter* (see *EcoStruxure™ Control Expert, Communication, Block Library*) for a description of these additional status code values.
- Depending on the DDT specified in the DDT_NAME parameter, some consistency verifications are performed on the data received. If a mismatch is detected, code 16#02 (Incorrect response) is set in the operation report byte (the most significant byte of GEST[1]). Note that the block does not verify the data type validity of the variable configured as the reception buffer (RECP_DDT). Verify that the data type of the variable linked to the RECP_DDT parameter matches the type of data received.

⚠WARNING

UNINTENDED EQUIPMENT OPERATION

- Verify that the DDT-type variable associated to the RECP_DDT output parameter corresponds to the type of data written in the reception buffer.
- Verify that the address set in the ADR parameter corresponds to the correct module, especially when several identical modules are configured on the same network.

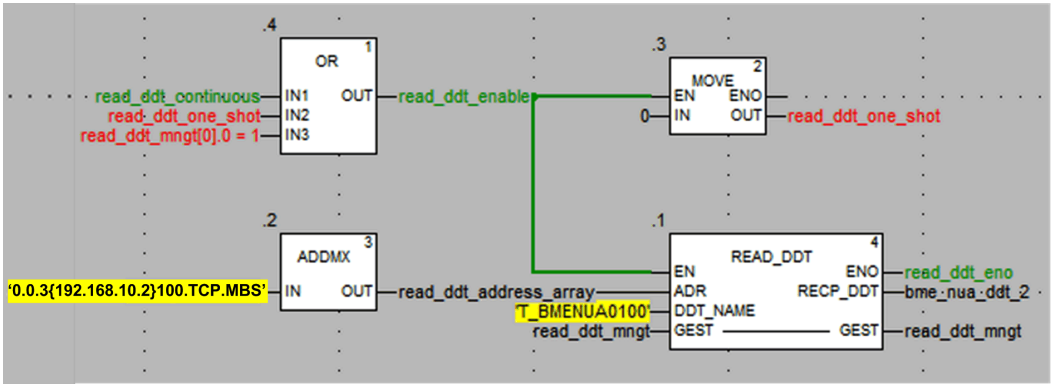
Failure to follow these instructions can result in death, serious injury, or equipment damage.

Configuring the READ_DDT Elementary Function

To configure the READ_DDT elementary function, follow these steps:

Step	Action
1	Set the address of the destination device in ADR (use an ADDM block to specify this address in an explicit string format).
2	Set DDT_NAME parameter with the name of the DDT to read.
3	Call the READ_DDT function to launch the communication (with EN input pin set to 1 if configured).
4	Monitor the activity bit (in the least significant byte of the GEST[0] parameter) until the communication is completed (the activity bit is set to 0 by the system when the communication has ended). Execute this function only once to avoid erasing the status values. For example, setting the EN pin to 0 during operation would cause the function to be called again.
5	View the report parameters in GEST[1]. If the report reads 16#0000, then RECP_DDT buffer has been filled with received data. Size of the data received (in bytes) is written in the fourth word (GEST[3]) of the management table.

READ_DDT EF Example



In this example, the READ_DDT EF may be started:

- Continuously by setting the read_ddt_continuous variable.

  NOTE: In the event of a detected error, report codes in the second word of the read_ddt_mngt variable cannot be read.

- Only one time, by setting the read_ddt_one_shot variable.

Configuring the READ_NUA_DDT Elementary Function

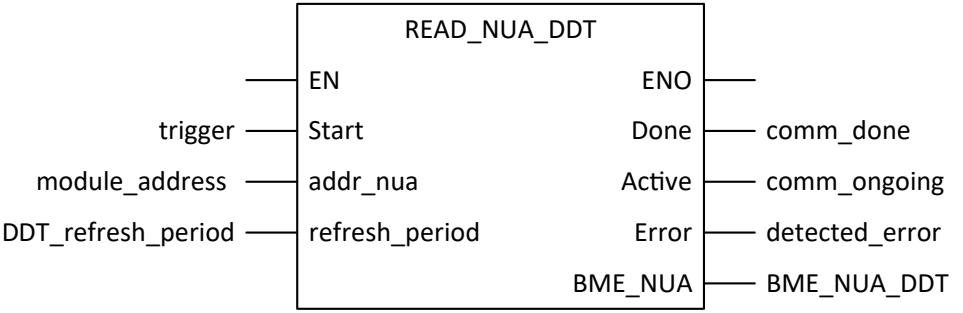
Use the `READ_NUA_DDT` function block to access diagnostic information of the BMENUA0100 module.

The `Start`, `addr_nua`, and `refresh_period` input parameters define the operation.

EN and ENO can be configured as additional parameters

NOTE: For information about using this function block in a Hot Standby system, refer to the topic Asynchronous Communication Function Blocks (see *Modicon M580 Hot Standby Frequently Used Architectures System Guide*).

FBD Representation



Input Parameters

Parameter	Data Type	Description
EN	BOOL	This parameter is optional. When this input is set to one, the block is activated and can solve the function blocks algorithm. When this input is set to zero, the block is deactivated and won't solve the function block algorithm.
Start	BOOL	The read of the BMENUA0100 DDT is continuous.
addr_nua	string[32]	Address of the BMENUA0100 module given to ADDMX() for read. Fixed length string containing the address of the destination BMENUA0100. The address is the result of the ADDMX function. (For example: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) indicates the module at IP address 192.168.10.2, with UnitId 100 (local server of the module), connected to the embedded Ethernet port.
refresh_period	TIME	Refresh period of the DDT.

Output Parameters

Parameter	Data Type	Description
ENO	BOOL	This parameter is optional. When you select this output you also get the EN input. ENO output is activated upon successful execution of the function block.
Done	BOOL	Communication is completed.
Active	BOOL	Communication is in progress.

Parameter	Data Type	Description
Error	BOOL	Detected error on communication function block.
BME_NUA	T_BMENUA0100	The BMENUA0100 DDT, page 135 that can be used as it is.

OPC UA Diagnostics

Introduction

The BMENUA0100 module presents both OPC UA server variables and Specific DataItems that can be used to identify the application running in the module, and to diagnose module operations.

OPC UA SERVICE_LEVEL Variable

The SERVICE_LEVEL variable provides information to a client regarding the status of the controller and the health of the OPC UA server. The SERVICE_LEVEL variable is directly accessible under the OPC UA server node tree. The SERVICE_LEVEL variable is also duplicated in the OPCUA_STATUS.SERVICE_LEVEL element of the BMENUA0100 module DDT, page 136, and can be programmatically accessed by executing the READ_ DDT, page 141 elementary function when the application is in the RUN state.

NOTE: In redundant architectures, the OPC UA client needs to monitor the SERVICE_ LEVEL variable in both the primary and the standby BMENUA0100 modules to manage the redundancy mechanism. When the client detects that the SERVICE_LEVEL value of the standby module is greater than the SERVICE_LEVEL value of the primary module, the client needs to trigger a switchover from the primary to the standby module.

The following service level variables apply to all firmware versions of the BMENUA0100 module, except as noted:

SERVICE_LEVEL Value	Status of the Controller / OPC UA Server	
	Firmware = V1.0	Firmware ≥ V1.1
0	BMENUA0100 is in boot phase. Controller is in NOCONF or ERROR state. Example of ERROR state: MAST task is in HALT state.	
1	OPC UA server has started. Data dictionary list browsing is ongoing.	
5	Data dictionary browsing is started.	
10	Data dictionary size overflow.	

SERVICE_LEVEL Value	Status of the Controller / OPC UA Server	
	Firmware = V1.0	**Firmware ≥ V1.1**
20	Data dictionary type browsing is ongoing.	
50	Data dictionary variable browsing is ongoing.	
100	Data dictionary browsing is complete. Reading of the controller status is ongoing. Address space will be updated with new data dictionary content.	
120[1]	Controller in STOP state.	Controller in STOP STANDBY or HALT STANDBY state (Hot Standby controller only).
150[1]	Controller in WAIT STANDBY state (Hot Standby controller only).	
199[1]	Controller in RUN STANDBY state (Hot Standby controller only).	
202[2]	<Not applicable>	Standalone_controller only: controller in STOP STANDALONE state. Hot Standby controller only: When both controllers are in STOP or HALT state, one BMENUA0100 is declared as master with service level = 202. Address space is OK and usable.
255	Controller in RUN (or RUN PRIMARY for Hot Standby controller). OPC UA server is fully operational	

1. This value does not need to be set before the server becomes operational.

2. This service level applies only to BMENUA0100 firmware V1.10 and later.

NOTE: The larger the size of the data dictionary, the longer the data dictionary acquisition time (i.e. the time required for the module to browse and load the data dictionary). During data dictionary acquisition, SERVICE_LEVEL remains at the value 100 until acquisition is completed. When a build change is performed in Control Expert generating a new data dictionary, the OPC UA server restarts the process of browsing the data dictionary browsing. During this process updates of the monitored items may be halted, with monitored item values frozen at their most recently updated value.

OPC UA Server Variables

You can view these variables online using an OPC UA client device, such as the UaExpert tool from Unified Automation. Navigate the OPC UA server node tree to **ServerStatus > BuildInfo** to display the following OPC UA server variables:

Variable	Description
BuildDate	The date the application in the controller was built.
BuildNumber	The number of the current controller application build.
ManufacturerName	“Schneider Electric”.
ProductName	“BMENUA0100”.
ProductUri	The unique Uniform Resource Identifier assigned to the module.
SoftwareVersion	The version of module firmware.

OPC UA Specific DataItems

The BMENUA0100 module supports the following Specific DataItems. These DataItems are accessible via the OPC UA server stack. While they are much like controller data items reachable via the Control Expert software, these Special DataItems are not linked to controller symbols and are not reachable via the Control Expert software:

DataItem	Data type	Default value	Description
#AddressSpaceState	INT16	0	The state of the address space, with its collection of objects and nodes. Possible values include: **0.** Empty **1.** Built **2.** Updating **3.** Partially built (no data dictionary exists in the application, or data dictionary overflow)
#ApplicationName	STRING	0	The controller application name.
#ApplicationVersion	STRING	0	The controller application version.
#CurrentDataDictionaryItemsCount	INT32	0	The number of items in the data dictionary that have been loaded into the server.
#CurrentMonitoredItemsCount	INT32	0	The number of items being monitored by the server.
#DeviceIdentity	STRING	0	The name of the controller reference.
#PLCDatadicReady	BYTE	1	Monitors the controller data dictionary loading status:

DataItem	Data type	Default value	Description
			1. The controller data dictionary is not available. Possible explanations include: • The data dictionary functionality is not available or enabled in the Control Expert application and cannot be embedded in the controller. • The loading/browsing of the data dictionary is in progress in OPC UA Server. 2. The controller data dictionary is available, for example: • The loading/browsing of the data dictionary by the OPC UA server completed with success. • A pre-loading (in accordance with Control Expert data dictionary project settings) can be in progress.
#PLCQualStatus	INT16	0	Monitors the communication status of a controller. Possible (hex) values include: • 00C0 hex: Communication with the controller is correct. • 0040 hex: No communication with the controller for a time less than the Device Timeout (5s). • 0 hex: controller is not identified.

DataItem	Data type	Default value	Description
#TSEventItemsReady	BOOL	0	A read-only item that indicates whether at-source-time-stamped variables and at-source-time-stamping devices have been browsed in the M580 econtroller application: • 0 = not browsed • 1 = browsed **NOTE:** This item is meaningful only when time stamping is enabled in Control Expert and activated for the specific BMENUA0100 module.
#TSEventSynchro	BOOL	0	A read-write item that, when activated, sends a synchronized value to the entire at-source-time-stamping devices attached to the M580 controller each time a write operation is performed. The purpose is to initialize all the timestamped monitored items to their values. • 0 = awaiting activation • 1 = activated **NOTE:** • The value of this item will appear as 0. A value of 1 will not be seen as it exists only momentarily and reverts again to the awaiting activation value of 0. • This item is meaningful only when time stamping is enabled in Control Expert and activated for the specific BMENUA0100 module.

Syslog

Introduction

The BMENUA0100 module logs events in a local diagnostic buffer, then sends a record of these events to a remote syslog server where they are stored and made available to syslog clients. To diagnose prior events, you can query the syslog server event records. For on-going module events, you can use the module web pages, page 154 to diagnose the state of the syslog service and to view specified events in the diagnostic buffer.

The local buffer operates as a circular buffer, with the most recent events overwriting and replacing the oldest events when the buffer is full.

The module stores events in volatile memory.

Logged events relate to either:

- Security/Authorization, page 153

  – or –

- Major changes in the system (log audit), page 154

The syslog service is configurable in the web pages, page 93 as part of the cybersecurity configuration and, therefore, can be active only when the module is operating in Advanced (or Secured) Mode. When the module is operating in Standard mode, the service is deactivated.

As implemented in the BMENUA0100 module, syslog is supported by IPv4 (firmware version 1.0 and later), and IPv6 (firmware version 1.10 and later).

NOTE: Syslog is not a natively secure protocol, but must be encapsulated within an IPsec, page 99 secure channel over the control port.

Syslog Message Structure

The syslog protocol – RFC 5424 – defines how events exchanged between the module and the remote server. The syslog message structure is set forth below:

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>PRI</td><td>Facility and severity information (description provided in following tables).</td></tr>
<tr><td>VERSION</td><td>Version of the syslog protocol specification (Version = 1 for RFC 5424.).</td></tr>
<tr><td>TIMESTAMP</td><td>Time stamp format is issued from RFC 3339 that uses the following ISO8601 Internet date and time format: YYY-MM-DDThh:mm:ss.nnnZ
NOTE: -, T, :, . , Z are mandatory characters and they are part or the time stamp field. T and Z need to be written in uppercase. Z specifies that the time is UTC.
Time field content description:
<table><tr><td>YYY</td><td>Year</td></tr><tr><td>MM</td><td>Month</td></tr><tr><td>DD</td><td>Day</td></tr><tr><td>hh</td><td>Hour</td></tr><tr><td>mm</td><td>Minute</td></tr><tr><td>ss</td><td>Second</td></tr><tr><td>nnn</td><td>Fraction of second in millisecond (0 if not available)</td></tr></table></td></tr>
<tr><td>HOSTNAME</td><td>Identifies the machine that originally sent the syslog message: fully qualified domain name (FQDN) or source static IP address if FQDN is not supported.</td></tr>
</table>

Field	Description
APP-NAME	Identifies the application that initiates the syslog message. It contains information that allows to identify the entity that sends the message (for example, subset of commercial reference).
PROCID	Identifies the process, or entity, or component that sends the event.
MSGID	Identifies the type of message on which the event is related to, for example HTTP, FTP, Modbus.
MESSAGE TEXT	This field contains several information: • Issuer address: IP address of the entity that generates the log. • Peer ID: Peer ID if a peer is involved in the operation (for example, user name for a logging operation). • Peer address: Peer IP address if a peer is involved in the operation. • Type: Unique number to identify a message (description provided in following tables). • Comment: String that describes the message (description provided in following tables).

Events Related to Security/Authorization

- Unsuccessful secure channel opening from OPC UA stack: for example, invalid certificate, expired certificate.
- Successful user sessions (Login/Password) from OPC UA stack (successful login)

  NOTE: In case of no login (Standard mode), the log is disabled so a record of the successful connection is not created.
- Unsuccessful user sessions (Login/Password) from OPC UA stack (unsuccessful login)

  NOTE: In case of no login (Standard mode), the log is disabled so a record of the unsuccessful connection is not created.
- Successful HTTPS connections to or from a tool (successful login): for example, a connection to the web server or a firmware download via HTTPS.
- Unsuccessful HTTPS login to or from a tool: for example, an unsuccessful connection to the web server or an unsuccessful firmware download via HTTPS.
- Successful user session disconnection (on demand logout) for HTTPS.
- Successful user session disconnection (on demand logout) for OPC UA.
- Automatic logout: for example, an inactivity timeout for either OPC UA or HTTPS.
- Integrity check error detected: for example, a digital signature detected error, or an integrity only (hash) detected error.
- Create a new certificate.

- Remove local certificates. This is accomplished by using the rotary selector switch to set the operating mode to the Cybersecurity (or Security) Reset position.
- Add a new client certificate from the allowlist into the device.
- Remove a client certificate from the allowlist into the device.

Events Related to Major Changes in the System (log audit)

- Application or cybersecurity configuration download into the device.
- Firmware download into the device.
- Mismatched signature for firmware that could not download into the device.

Syslog Web Page Diagnostics

Use the module web pages to diagnose the state of the syslog service running on the module, and to diagnose specified parts of the module syslog diagnostic buffer. You can also use the SERVICES_STATUS element of the module DDT, page 136 to view the syslog service status.

In the **Diagnostics > Event log diagnostic** menu, use the following commands to view the module syslog service status:

Parameter	Description
Status	• Operational: the module is operating in Advanced (or Secured) Mode and the syslog service is enabled. • Not operational: the module is operating in Advanced (or Secured) Mode but the syslog service is disabled.
Log server	• Reachable: a connection can be established to the remote syslog server. • Not reachable: a connection cannot be established to the remote syslog server.

In the **Diagnostics > Event log diagnostic** menu, in the **Diag Buffer to read** field, input the part of the diagnostic buffer to read.

Modbus Diagnostics

Introduction

You can use Modbus function code commands to perform diagnostics on the BMENUA0100 module. Modbus commands can reach the module only over its backplane port. Because Modbus is not an inherently secure protocol, you need to encapsulate Modbus commands within IPsec.

Only FC FC43/14 (Read Device Identification) and FC03 (read DDT MW%) requests are supported on the BMENUA0100 module.

Modbus Data Access and the Cybersecurity Operating Mode

The method you can use to access Modbus data depends on the cybersecurity operating mode. If the BMENUA0100 module is operating in:

- Standard mode: The BMENUA0100 module accepts the Modbus TCP/IP client data flow from any client that can access the backplane Ethernet network. Use standard Modbus communication methods, including DATA_EXCH, MBP_MSTR, READ_VAR and WRITE_VAR function blocks, and Control Expert commands.
- Advanced (or Secured) mode: The BMENUA0100 module accepts the Modbus TCP/IP client data flow only from the M580 controller. You can implement the DATA_EXCH block in the application.The READ_VAR and WRITE_VAR can also be used.

  NOTE: To address the Modbus server in the module, UnitID 100 needs to be used. Refer to your Modbus client documentation for information describing how to set this value. For example, when using the DATA_EXCH block, UnitId may be set with ADDMX as follows: ADDMX(0.0.3{192.168.10.2}100.TCP.MBS) where 192.168.168.10.2 is the backplane IP address of BMENUA0100 module.

43/14: Read Device Identification

The following device identification data can be returned using function code 43 / subcode 14:

Category	Object ID	Object Name	Type
Basic	00 hex	VendorName	ASCII string
	01 hex	ProductCode	ASCII string
	02 hex	MajorMinorRevision	ASCII string
Regular	03 hex	VendorUrl	ASCII string
	04 hex	ProductName	ASCII string
	05 hex	ModelName	ASCII string
	06 hex	UserApplicationName	ASCII string
	07 ...FF hex	Reserved	ASCII string

SNMP Diagnostics

Introduction

When the SNMP agent is configured, page 127, the BMENUA0100 module enables SNMP diagnostics in the TCP/IP-based Ethernet network by supporting the following MIBs:

- MIB-II
- Link Layer Discovery Protocol (LLDP) MIB

MIB-II

MIB-II provides an SNMP manager with a collection of device management variables. By reading these variables, an SNMP manager can diagnose the operation of a specific device, such as the BMENUA0100.

LLDP MIB

The LLDP MIB contains data collected by operation of the link layer discovery protocol relating to the identity, capabilities, and location on the Ethernet network. Using the LLDP MIB, an SNMP manager can discover the topology of the network and the capabilities of the network devices.

NOTE: SNMP communication of LLDP MIB data is made exclusively over the backplane port.

OPC UA Diagnostic Web Page

Use the **OPC UA Diagnostics** web page to view dynamic data describing the operation of the OPC UA server embedded in the BMENUA0100 module.

NOTE: The **OPC UA Diagnostic** web page is refreshed every 5 seconds.

Diagnostic Data

OPC UA Diagnostics web page displays the following read-only data. Note that all numeric values are in decimal format:

Field	Description
PLC Diagnostic	
EPAC	Controller IP address.
Device Identity	Controller part number.
Device Version	Controller firmware version.
Device Status	Connection status with controller: **Good**, **Bad**, **Uncertain**, **Unknown**, **Missing**.
Frame Time Out (in ms)	The maximum length of time the OPC UA server will wait for an answer from a device after sending a request. For example, 1000.
Maximum Channel number	Number of connections opened by OPC UA server on the controller.
Channels used for non-Timestamping	Number of connections that carry application data.
Channels used for Timestamping	Number of connections that carry timestamping data, page 121.
Request Length	Length of request for communication with controller.
Application Name (Device)	Control Expert project name.
Application Version (Device)	Application checksum and signatures.
Preload data dictionary	Available or Unavailable for application in controller.
Timestamping Status	Timestamping status is displayed: • Timestamping is enabled with access to Timestamped Variables in application. • Timestamping is not enabled, no access to Timestamped Variables.

Field	Description
List of devices with source time stamping configured	If timestamping is enabled, a list of devices is displayed indicating for each device: • Number of dedicated channels reserved for Timestamp Event Source polling. • Device type (BMECRA31310, controller, etc.). • IPv4 address. • Reservation of device timestamp buffer by the BMENUA0100 OPC UA embedded server: TRUE / FALSE.
OPC UA Diagnostic	
Endpoint url (IPV4)	OPC UA server IPv4 address, in the format: “opc.tcp://<IPv4 address>:<port number>”. For example: opc.tcp://192.168.2.142:4840
Fast Sampling Rate	Indicates if the Fast sampling rate setting is selected, page 116: • TRUE = selected • FALSE = not selected
Number of connected sessions	Total number of client sessions supported by the BMENUA0100 embedded OPC UA server.
Subscription(s) Information:	Information describing the variables monitored by the OPC UA server that are included in one or more subscriptions.
Number of monitored item(s) from internal Server node:	
Number of specific monitored item(s):	
Number of non specific monitored item (s):	
Number of TimeStamped monitored item (s) with monitoring mode not disabled:	
Total Number of monitored item(s):	
Current number of timers	The number of configured sampling intervals for the BMENUA0100 embedded OPC UA server.
Timer list	A list describing each sampling interval (i.e., timer) monitored by the BMENUA0100 embedded OPC UA server. Each item indicates: • The sampling interval in ms. • The number of monitored items. • The number of requests generated during the most recent execution.

Optimizing BMENUA0100 Performance

Optimizing BMENUA0100 Performance

Introduction

When optimizing performance of the BMENUA0100, consider the entire system. Pay particular attention to the overall communication efficiency and workload within the network architecture that includes the BMENUA0100 modules. It is in this context that OPC UA client performance optimizations also impact the OPC UA communication effectiveness.

Several settings, at different levels of the architecture, can enhance system performance or make your system more stable and robust during each of the operating mode phases (connections, browse, subscription, monitoring, and so forth).

NOTE:

- Add items in packets of a maximum size of 2000 items. The configured sampling interval is relevant only if greater than or equal to the MAST controller scan time.
- Set the CallTimeout to a value greater than or equal to 10 seconds in the OPC UA client.
- The General.SecureChannelLifetime setting for communication to an OPC UA client is set by default to 3,600,000 ms (1 hour). Use this default setting to avoid decreasing performance.
- The performance of the system depends strongly on the configuration (for example, the number of connected clients, the number of variables managed, and so forth).
- As an example, with 2000 monitored items, the refresh rate can be accomplished within 20ms only if the values of a maximum of 500 items change between two consecutive publishing iterations.

Performance Example

An OPC UA client can monitor up to 20 000 items in Standard cybersecurity mode.

Example based on:

- BMEP584040 with a MAST task cycle time at 20ms (CPU load less than 80%).
- BMENUA0100 in rotary switch position Standard (i.e. no secure communication, no IPsec channel).

- OPC UA client (UAExpert) initiates communication with Message Security mode set to **None** and monitors 20,000 items by reference to variables based on array of 'INT' type from a BMENUA0100 OPC UA server. This server is configured with Publishing Interval to 1 second, Sampling Interval to 1 second, session Timeout to 30 seconds.
- No other communication than OPC UA.

How to Adjust the Performance

Exchange data structure

The Data application memory of the controller is organized depending on the Data application definition in Control Expert. The more the variable declaration is structured, the more the BMENUA0100 Server generates optimized requests for access to the variables and to the Data Dictionary in Run time.

Thus, for the variables that are accessed by the OPC UA Client:

- Use Arrays or Data structure whenever possible.
- Enable the option **Only HMI variable** in **PLC embedded data** of the **Project Settings** and set only these variables with the attribute **HMI** to reduce the size of the Data Dictionary.
- In the Safety controller application, to reduce the data dictionary size, de-select the option **Usage of Process Namespace** (in **Project Settings > General > PLC embedded data > Data dictionary**.

Controller communication capabilities

The capability of the communication system depends on the M580 controller reference and some configuration setting. The controller reference determines:

- The system-wide controller processing performance capabilities.
- The number of requests per cycle that can be processed, even if configurable by System word %SW90.
- The maximum number of channels available to each BMENUA0100 for establishing connections to the M580 controller, page 168.

In addition, the less the MAST cycle time, the greater the number of communication requests that can be processed. Thus, the performance level is directly dependent to the MAST cycle time.

OPC UA client, configuration and usage

The number of monitored variables impacts the performance. The Sampling Rates and Publishing intervals configured for each OPC UA client determine the number of requests needed to animate the variables. Keep in mind that, when several OPC UA clients are connected to the same BMENUA0100 OPC UA server, when the Sampling Rates and

Publishing intervals are different in each OPC UA client sides, this configuration generates more requests.

All timeout values configurable from OPC UA client (Browse, Connect, Publish, Session, Watchdog…) need to be tuned to optimize and stabilize - to the extent possible - your overall system. As a side effect, these timeouts could impact the system performance.

Depending on the Message Security mode (None, Sign, Sign&Encrypt), the algorithm to compute the signature and the encryption takes additional time.

Controller to Controller and Control Expert to Controller communications

Each IPsec tunnel used to secure the communications other than OPC UA or HTTPS slows down the traffic, especially when the setting **Confidentiality** is enabled, thereby generating encryption and decryption.

How to Monitor the Performance

There are several ways to monitor performance.

Using Control Expert

Using Control Expert in connected mode, you can access the effective MAST cycle time and the M580 controller load for the system, for each task and for the total of all tasks by reading the system words %SW110 to %SW116. In addition, the M580 controller DDDT and the BMENUA0100 DDT can provide different diagnostic information linked to the system performance of the controller, such as:

- The Service Level of the OPC UA server.
- The number of connected OPC UA clients.
- The data dictionary status, acquisition time, preload duration.
- The Ethernet service status.
- The network health.
- The control port and the backplane port status.
- The number of Ethernet packets per second.
- The number of Ethernet packets that contain detected errors.
- The percentage of BMENUA0100 CPU load and used memory.
- The number of IPsec channels opened.

Using BMENUA0100 Web site

The Home page and the Diagnostic page of the BMENUA0100 Web site provide interesting information related to the performance of OPC UA servers. Some information comes from the BMENUA0100 DDT, and other information is given by the OPC UA server itself:

- Number of monitored items.
- Number of monitored specific items.
- The different sampling intervals currently in execution.
- The number of generated requests for the animations.
- Detected overruns.
- Number of connected clients.

Using OPC UA client

The OPC UA client can monitor directly some specific items under the OPC UA server, but also the ServiceLevel variable or some BMENUA0100 DDT subfields on demand through application variables.

Other services for diagnostic

In a more technical approach, the SNMP agent and the Syslog server of the BMENUA0100 module can help to get other diagnostic information linked to the performance of the OPC UA servers.

Troubleshooting the BMENUA0100 Module

Introduction

This topic describes tips you can use to better operate the BMENUA0100 module.

Impact of Using UaExpert as the OPC UA Client

If you are using UaExpert as the OPC UA client to read data values, note that UaExpert increments the *CurrentSubscriptionCount* by a value of 1 for each instance of UAExpert.

NOTE: The *CurrentSubscriptionCount* item is related to the server itself, and is not to be mistaken for the session-related item *CurrentSubscriptionsCount*.

Data Dictionary Acquisition Time and MAST Period

The time required to load the collection of variables in the data dictionary depends in on the number of data dictionary items and the configured MAST period. For an application that requires the OPC UA server in the BMENUA0100 module to monitor a number approaching the maximum of 100 000 items, the following results were observed and may be instructive.

For a non-safety-related application with 99 000 items:

MAST Period	Observed Data Dictionary Acquisition Time
20 ms	23 s
100 ms	46 s
200 ms	74 s

For a safety-related application with 99 000 items:

MAST Period	Observed Data Dictionary Acquisition Time
25 ms	15 s
200 ms	72 s

Configuring Subscriptions with More Than 30,000 Monitored Items

If you intend to create one or more subscriptions, which collectively include more than 30,000 monitored items, configure each subscription in the respective OPC UA client with a **Life Time Count** value of 300 seconds, which represents the Maximum Subscription Lifetime, page 34 value the OPC UA server in the BMENUA0100 module can support.

Using GPOs / LGPOs

Manage certificates on a host PC by means of one of the following tools available from the Windows™ operating system:

- Group Policy Objects (GPOs) to perform centralized management of user settings in a centralized Active Directory environment, or
- Local Group Policy Objects (LGPOs) for distributed management of user settings for individual PCs.

In either case, using GPOs or LGPOs can help prevent unauthorized access to your PC and its applications. Use of GPOs and LGPOs disables access to the Windows Microsoft Management Console (MMC), and supports implementation of only the approvelist configured by the software.

Applying MMC Group Policy Management

Manage certificates using the tools provided by Microsoft Windows™ to help prevent unauthorized certificates to be added to the PC, or modifying self-signed certificates of an OPC UA client. If left unmanaged, someone could include unauthorized certificates to the BMENUA0100 approvelist managed by the security administrator.

These tools include group policy management policies applied by the Group Policy Object (GPO), a plug-in of the Microsoft Management Console (MMC). Design your polices so that they disable access to the Windows MMC, and allow access only to entries in the approvelist configuration that are properly added by the software.

OPC UA Client Lock-Out

When connecting an OPC UA client that has an assigned user name to the OPC UA server embedded in the BMENUA0100 module, the user account policy settings, page 93 of the BMENUA0100 are applied. For example, if the number of **Maximum login attempts** is reached or exceeded, the OPC UA client cannot log in (**BadInternalError**) for the time set as the **Account locking duration**.

Activating Network Services Using Only an IPv6 Connection

The BMENUA0100 module supports the use of only IPv6 for IP addressing and communication. With only IPv6 activated, page 115, the **CPU to CPU Data Flows** and **Control Expert Data Flows to Device Network** network services are not be available. These services are supported only by IPv4.

However, it is still possible to enable these features in the **Settings > Network Services** web page. If these services are enabled when only IPv6 is activated, these services (**CPU to CPU** and **CE to Device Network**) appear as being ON in the **Home** page, but in fact they are not activated.

Only the **Control Expert Data Flows to CPU only** data flow filtering feature is supported by IPv6 communication. In this case, with only IPv6 communication activated, the **Home** page correctly shows **CE to CPU only** as being ON.

BOOLs Seen as BYTEs in Controller Data Structures

In BMENUA0100 OPC UA server, each element of the controller DDT is assigned to a byte in the controller, even if it is defined as a BOOL or an EBOOL in the BMENUA0100. Using

the OPC UA protocol, a client can globally read or write a BOOL or EBOOL member of a BMENUA0100 instance in the controller DDT, with a valid byte value other than 0 or 1 (for example, 255). Design your application to write or read BOOL or EBOOL values of only 0 or 1, as only these values are valid in the BMENUA0100.

Firmware Upgrade

EcoStruxure™ Automation Device Maintenance Tool

Introducing the EcoStruxure™ Automation Device Maintenance Tool

Use the EcoStruxure™ Automation Device Maintenance tool to upgrade the firmware of the BMENUA0100 module. EcoStruxure™ Automation Device Maintenance is a web-based tool that enables you to:

- Manually discover one or more BMENUA0100 modules in your project based on IP addresses.
- Upgrade the latest firmware version to BMENUA0100 modules over the web.

Before upgrading firmware, you need to:

- Connect to the BMENUA0100 in the role of installer.
- Disconnect the clients (web, OPC UA, other controllers) connected to the module.

For details on how to install and use the EcoStruxure™ Automation Device Maintenance tool, refer to the online help (see *EcoStruxure Automation Device Maintenance, Firmware Upgrade Tool, Online Help*).

NOTE: Schneider Electric's Unity Loader™ software tool is not usable for upgrading firmware for the BMENUA0100 module.

NOTE: After upgrading the BMENUA0100 module firmware from version 1.xx to version 2.xx when the BMENUA0100 is in Standard Mode, you need to perform a Security Reset operation, page 30 to restore the module factory default settings. Then select a Cybersecurity operating mode - Advanced (or Secured) Mode or Standard Mode - for the module.

Downgrading Firmware

It is possible to downgrade the firmware version of the BMENUA0100 module, for example from version 1.1 to version 1.0. To do this, after downgrading the software version using the EcoStruxure™ Automation Device Maintenance tool, perform a Cybersecurity (or Security) Reset operation, page 30 to restore the module factory default settings. Then select a cybersecurity operating mode – Advanced (or Secured) Mode or Standard Mode – for the module.

Appendices

What's in This Part

Controller Connections

What's in This Chapter

OPC UA Server to Controller Connections

Opened Connections

The number of connections the BMENUA0100 module can open to the M580 controller depends on the capacity of the controller. Thus, performance of the BMENUA0100 module depends on the time required to perform the MAST task and the selected controller. The maximum number of connections opened by each BMENUA0100 module to the M580 controller are as follows:

Controller Model	Maximum Number of Connections Opened by each BMENUA0100
BMEP581020(H)	9
BMEP5820•0	9
BMEP5830•0	12
BMEP5840•0	15
BMEP585040	15
BMEP586040(C)	18
BMEH582040	9
BMEH584040(C)	15
BMEH586040	18

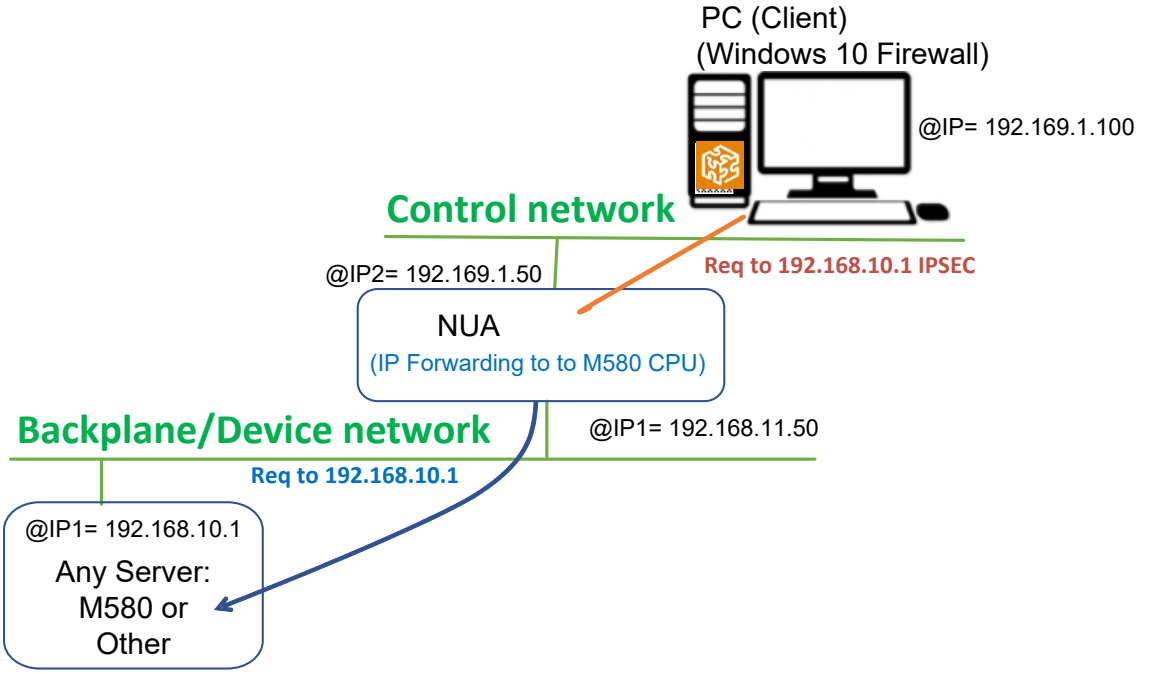
Service (IP) Forwarding Architectures

What's in This Chapter

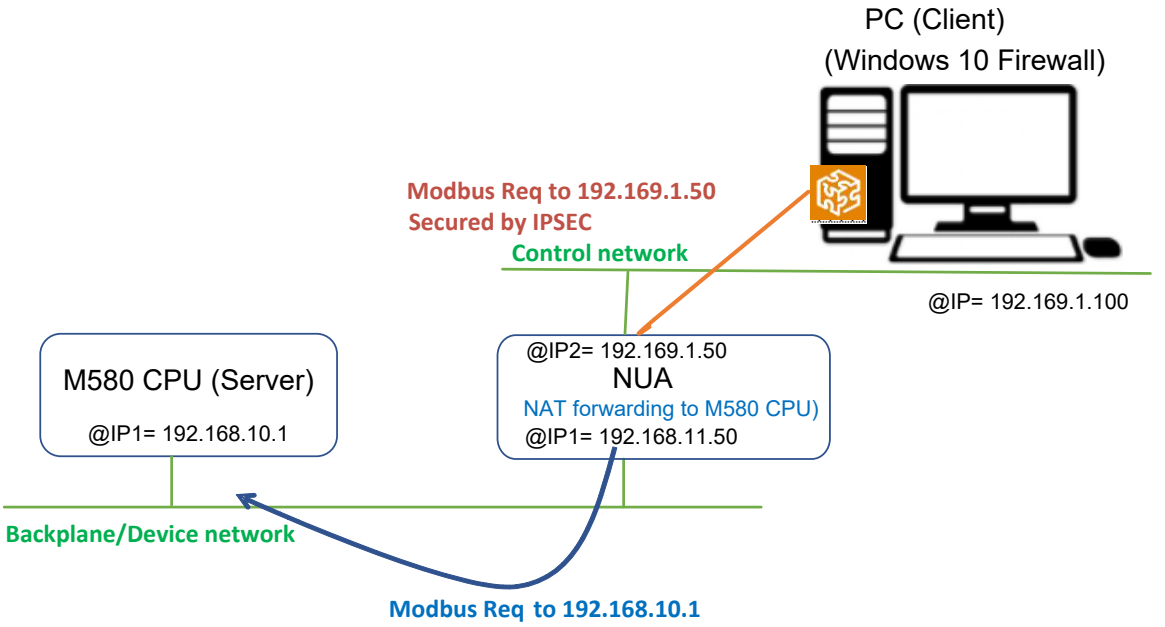
This chapter presents the architectures supported and not supported by the Service (IP) Forwarding feature of the BMENUA0100 module.

Service (IP) Forwarding Supported Architectures

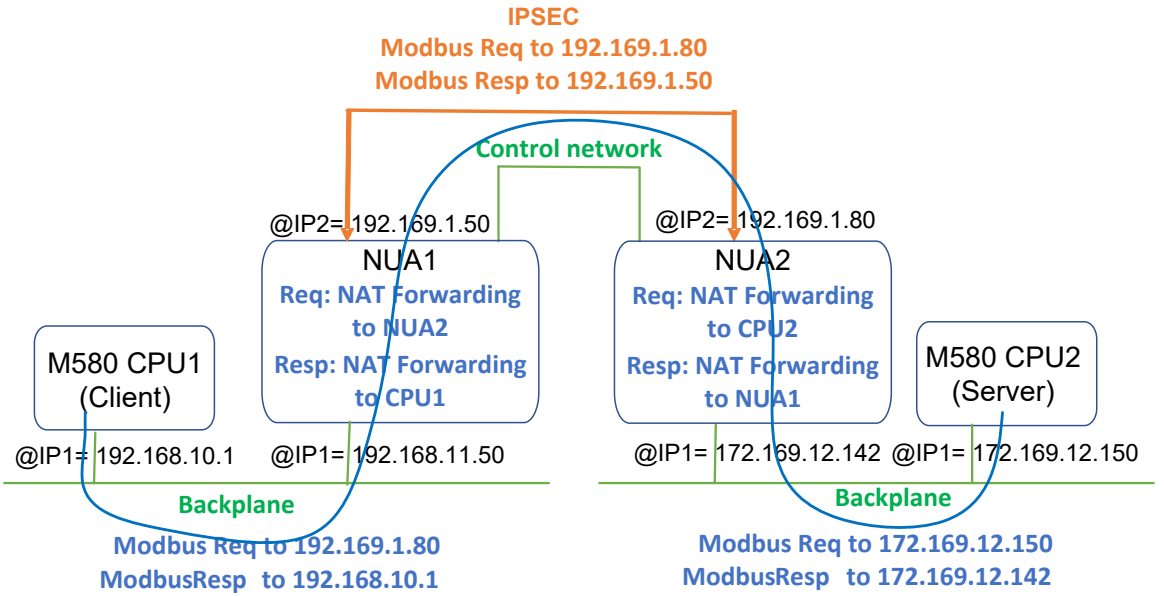
IP Forwarding from Windows Client (Control Network) to Any Client (Backplane/Device Network)



NAT Forwarding from Windows Client (Control Network) to M580 Controller (Backplane/Device Network)

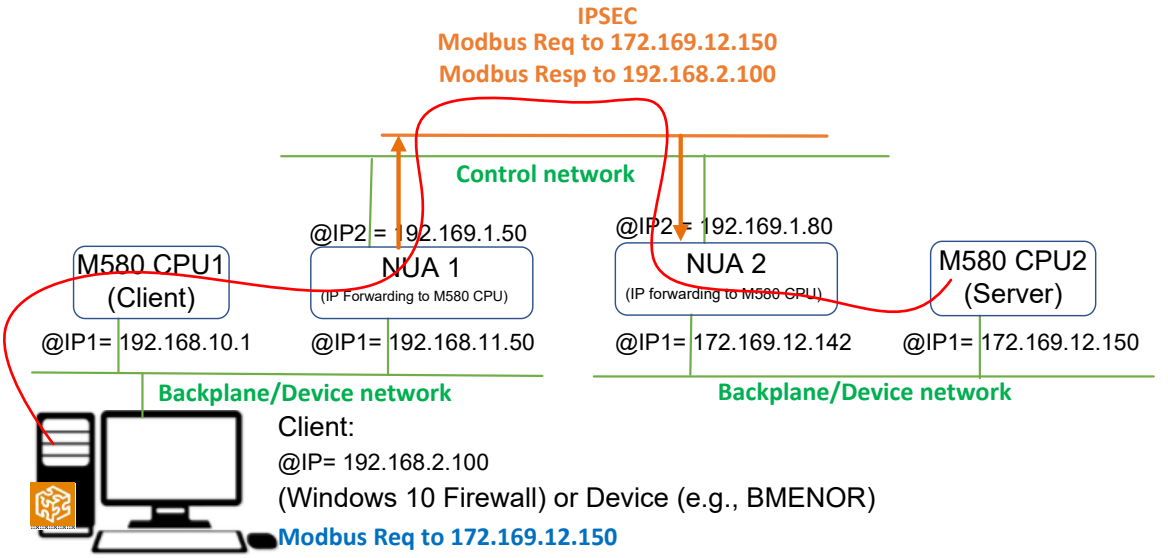


NAT Forwarding Between Backplanes for M580 Controller to M580 Controller Communication



Service (IP) Forwarding Non-Supported Architectures

IP Forwarding Between Backplanes/Device Networks



IP Forwarding and OPC UA Communication

What's in This Chapter

Both IP Forwarding and OPC UA compete for the BMENUA0100 module available communication bandwidth. This chapter contains the results of tests of module performance where only IP Forwarding is used and where both IP Forwarding and OPC UA communication are used.

IP Forwarding Impact on Performance

When only IP Forwarding — and not OPC UA communication — is activated, the impact on the BMENUA0100 module bandwidth is as follows:

IPsec	Confidentiality	Forward	Length frame (Bytes)	Bandwidth (Kbytes/sec)
No	N/A	Forward All	1000	8800
No	N/A	Custom rule	1000	10600
Yes	No	Forward All	1000	3400
Yes	No	Custom rule	1000	4000
Yes	Yes	Forward All	1000	2600
Yes	Yes	Custom rule	1000	2500

NOTE: These values are presented only as an example. Use them as an estimation of the impact of different parameters (IPsec, Confidentiality, etc.) on performance. Actual performance depends of your specific infrastructure.

The impact on bandwidth is displayed when:

- Only IP Forwarding communication flow is supported, and no OPC UA communication flow is included.
- IPsec is used (IPsec = Yes) and not used (IPsec = No).
- Frames are Signed (Confidentiality = No) versus when frames are both Signed & Encrypted (Confidentiality = Yes), and IPsec is used (in both cases).
- Custom rules for IP Forwarding are applied versus Forward All.

NOTE: The length of the frames has only a slight impact on global performance.

IP Forwarding and OPC UA Impact on Performance

When both IP Forwarding and OPC UA communication are activated, the impact on the BMENUA0100 module bandwidth is as follows:

Number of monitored OPC UA items per subscription	IPsec	Confidentiality	Forward	Bandwidth (Kbytes/ sec)
0	No	N/A	Custom rule	10600
0	Yes	No	Custom rule	4000
0	Yes	Yes	Custom rule	2500
20000	No	N/A	Custom rule	8800
20000	Yes	No	Custom rule	2900
20000	Yes	Yes	Custom rule	2000

NOTE: These values are presented only as an example. Use them as an estimation of the impact of different parameters (IPsec, Confidentiality, etc.) on performance. Actual performance depends of your specific infrastructure.

The impact on bandwidth is displayed when:

- All packet forwarding is performed via Custom rule (no Forward All).
- OPC UA communication flows are not included (Number of monitored OPC UA items = 0) and included (= 2000).

  NOTE: The number of OPC UA monitored items has little impact.

IPsec Windows Scripts

What's in This Chapter

IKE/IPsec Windows Firewall Configuration Scripts

To run IPsec on a PC that hosts either the Control Expert configuration software or an OPC UA client (e.g. SCADA), you need to add network configuration on the host firewall. For each IPsec rule configured on the webpages, an associated script (named IPSecWindowsConf.bat) can be downloaded using the gear wheel icon. Run this script to set the host firewall into the configuration.

- IKE/IPsec in **transport** mode for the data flows that are local to the BMENUA0100.
- IKE/IPsec in **tunnel** mode for the data flows that are forwarded to the Ethernet backplane.
- Passthrough rules for HTTPS, secured OPCUA and some other protocols for which **IPSEC use** = FALSE.

The following examples present Windows firewall configuration scripts with and without IPsec confidentiality.

In each script example, you need to provide values for the following variables:

- **`endpoint1`**: the remote IP address value in the IPsec configuration.
- **`endpoint2`**: the BMENUA0100 control port IP address.
- **`Auth1psk`**: the PSK setting in the IPsec configuration.

Windows Firewall Script With Confidentiality

NOTE: If confidentiality is enabled in the IPsec configuration, use `qmsecmethods=esp:sha256-aes128`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess

netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"
```

```
netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
aes128+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Windows Firewall Script Without Confidentiality

NOTE: If confidentiality is not enabled in the IPsec configuration, use `qmsecmethods=esp:sha256-None`

```
netsh advfirewall reset

netsh advfirewall set global mainmode mmkeylifetime 2879min,0sess

netsh advfirewall set global mainmode mmsecmethods dhgroup14:aes128-
sha256,dhgroup2:aes128-sha256

netsh advfirewall consec delete rule name="IPSECtunnel"

netsh advfirewall consec delete rule name="IPSECtransport"
```

```
netsh advfirewall consec delete rule name="IPSECpassthroughOPCUA"

netsh advfirewall consec delete rule name="IPSECpassthroughHTTPS"

netsh advfirewall consec add rule name="IPSECtransport" endpoint1=
192.169.1.100 endpoint2=192.169.1.50 action=requireinrequireout
description="IPSECtransport" mode=transport enable=yes profile=public
type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec add rule name="IPSECpassthroughOPCUA"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughOPCUA" mode=transport
enable=yes profile=public type=static protocol=tcp port2=4840

netsh advfirewall consec add rule name="IPSECpassthroughHTTPS"
endpoint1=192.169.1.100 endpoint2=192.169.1.50 action=
noauthentication description="IPSECpassthroughHTTPS" mode=transport
enable=yes profile=public type=static protocol=tcp port2=443

netsh advfirewall consec add rule name="IPSECtunnel" endpoint1=
192.169.0.0/16 endpoint2=192.168.0.0/16 localtunnelendpoint=
192.169.1.100 remotetunnelendpoint=192.169.1.50 action=
requireinrequireout description="IPSECtunnel" mode=tunnel enable=yes
profile=public type=static protocol=any auth1=computerpsk auth1psk=
b936789cb3626d83aaaf1e3ddb84984b qmpfs=none qmsecmethods=esp:sha256-
None+1440min

netsh advfirewall consec show rule name=all verbose

pause
```

Setting Up a Windows Certificate Authority

What's in This Chapter

This chapter describes how to set up a Microsoft Windows™ Certificate Authority to be used in an enterprise-wide user authentication and authorization system.

Preliminary Steps

The following describes the items you need and the preliminary steps you need to take before installing the certificate server.

Necessary Items

You will need the following items:

- Microsoft Windows™ Server Manager: This can be downloaded from the Microsoft website.
- Microsoft Windows Active Directory Certificate Server (ADCS): This commercial software is included as part of Windows Server. The BMENUA0100 module supports server versions 2016 and 2019.
- The file TemplatePackage.zip, which can be downloaded from Schneider Electric.

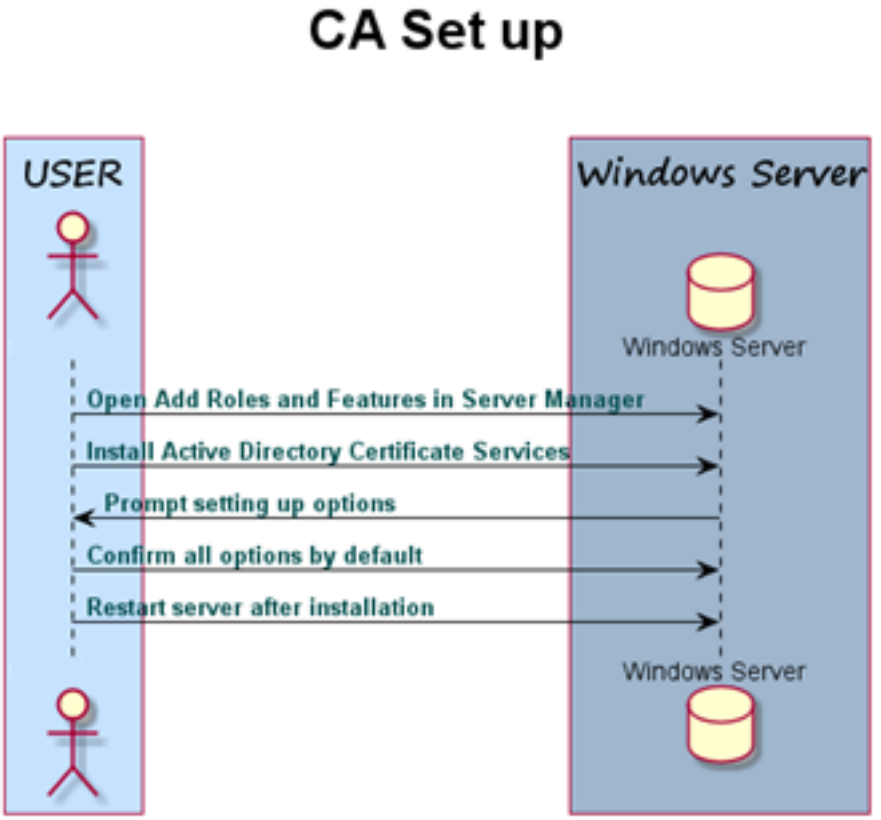
Preliminary Software Installations

Run the Active Directory Certificate Server installation file, then follow the several prompted steps to create a user account and password.

Server Manager should come pre-installed on your host PC. If not, it can be downloaded from the Microsoft web site.

Install Microsoft Windows Active Directory Certificate Server Overview

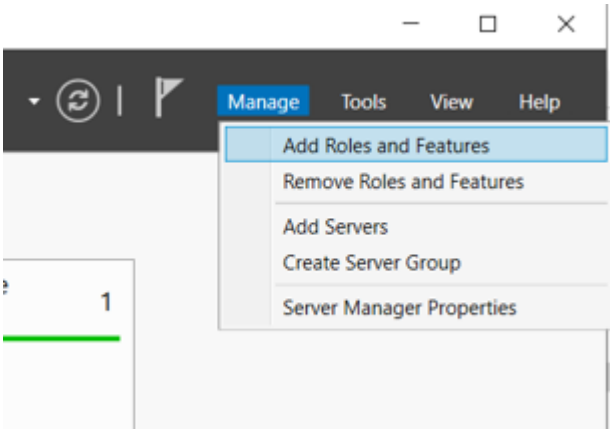
The following diagram presents an overview of the certificate authority (CA) setup process:



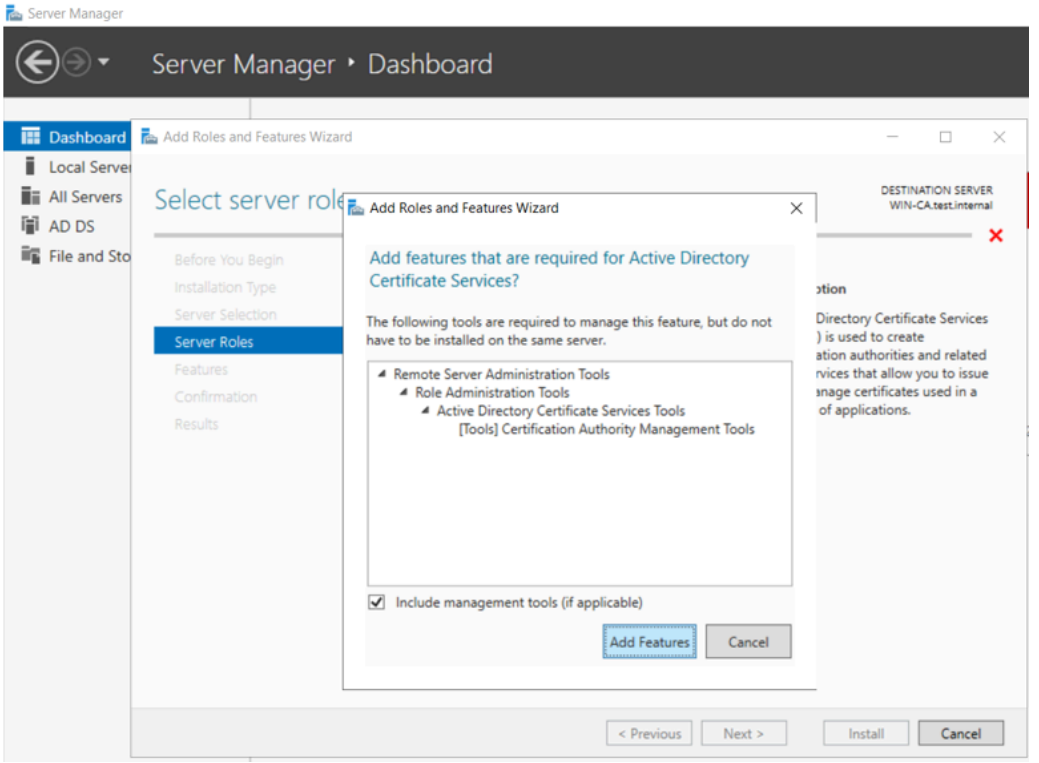
Install Active Directory Certificate Server (ADCS)

1. Start Microsoft Windows™ Server Manager and open its Dashboard.

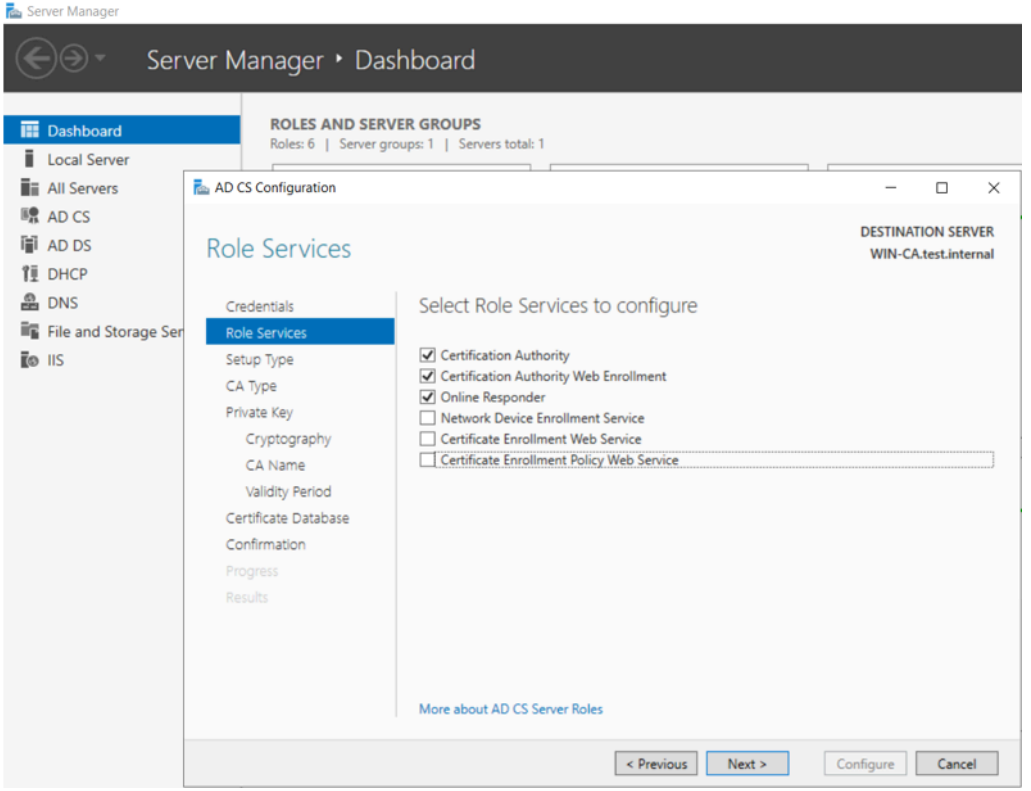
2. Select **Manage > Add Roles and Features**.



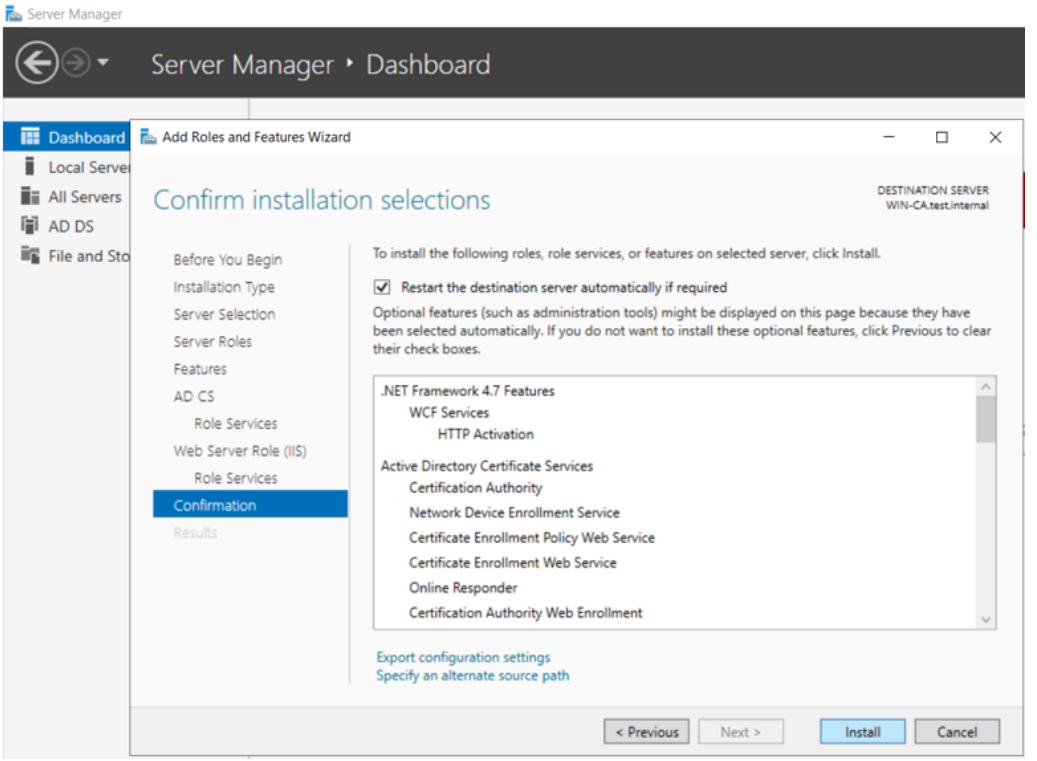
3. Add both the required roles and features and include the management tools:



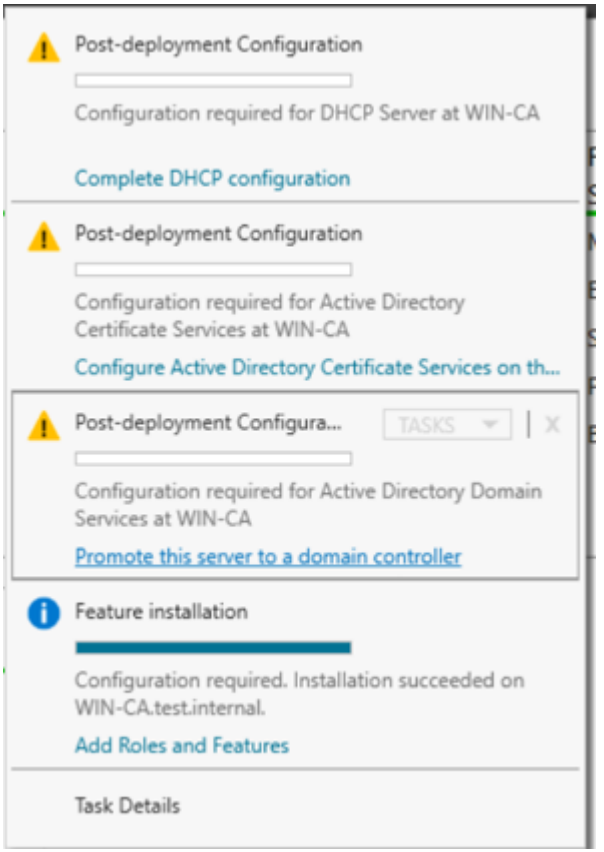
4. Select the Role Services to be configured:



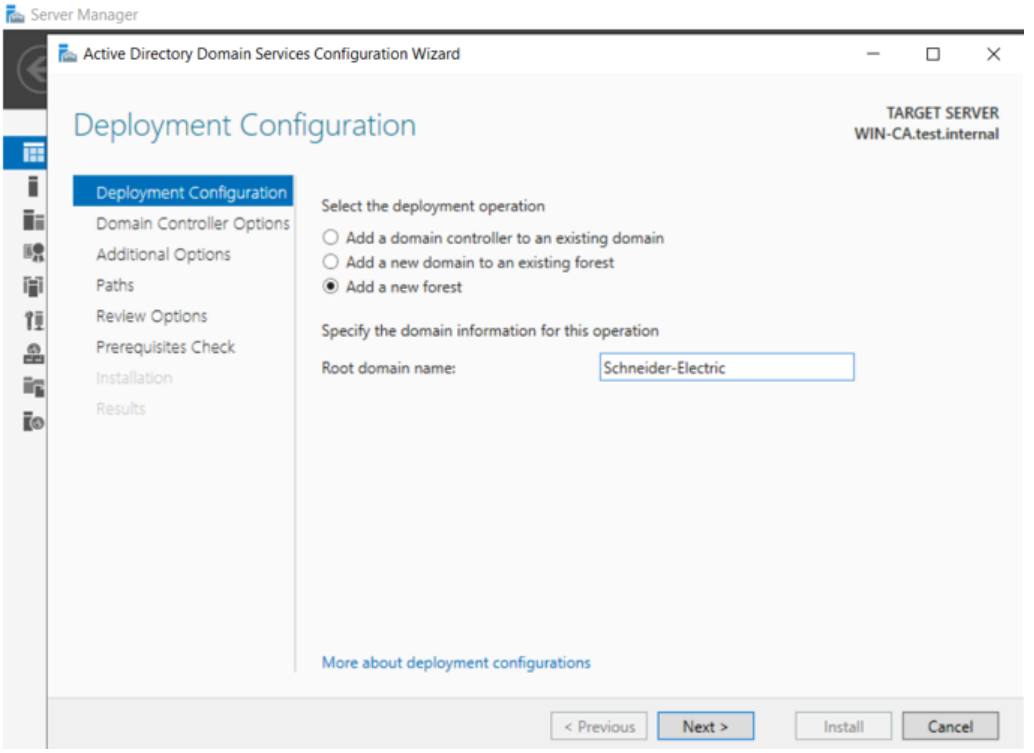
5. Confirm the installation selections:



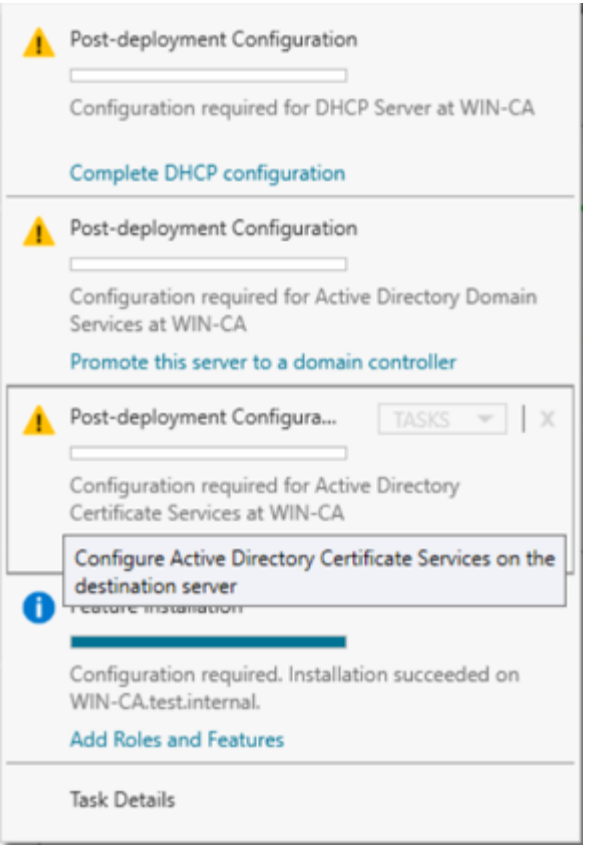
6. Click **Install**. Server Manager displays the installation progress:



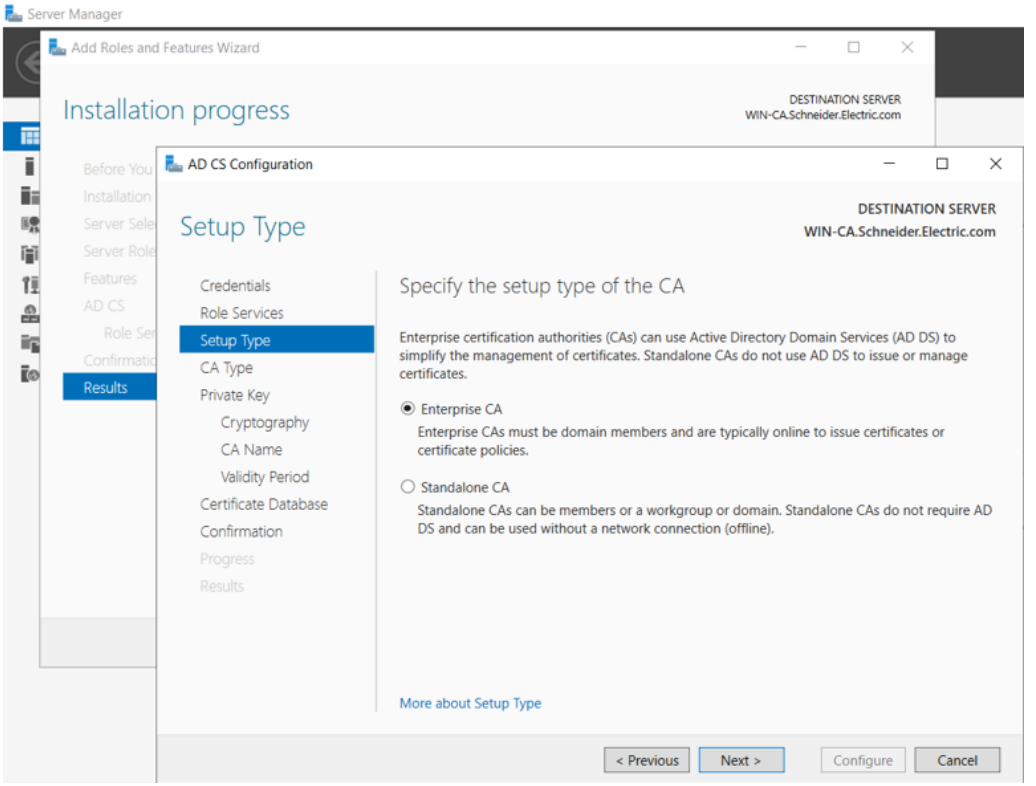
7. Select the deployment operation by creating a new forest or adding to an existing forest, and specify the domain :



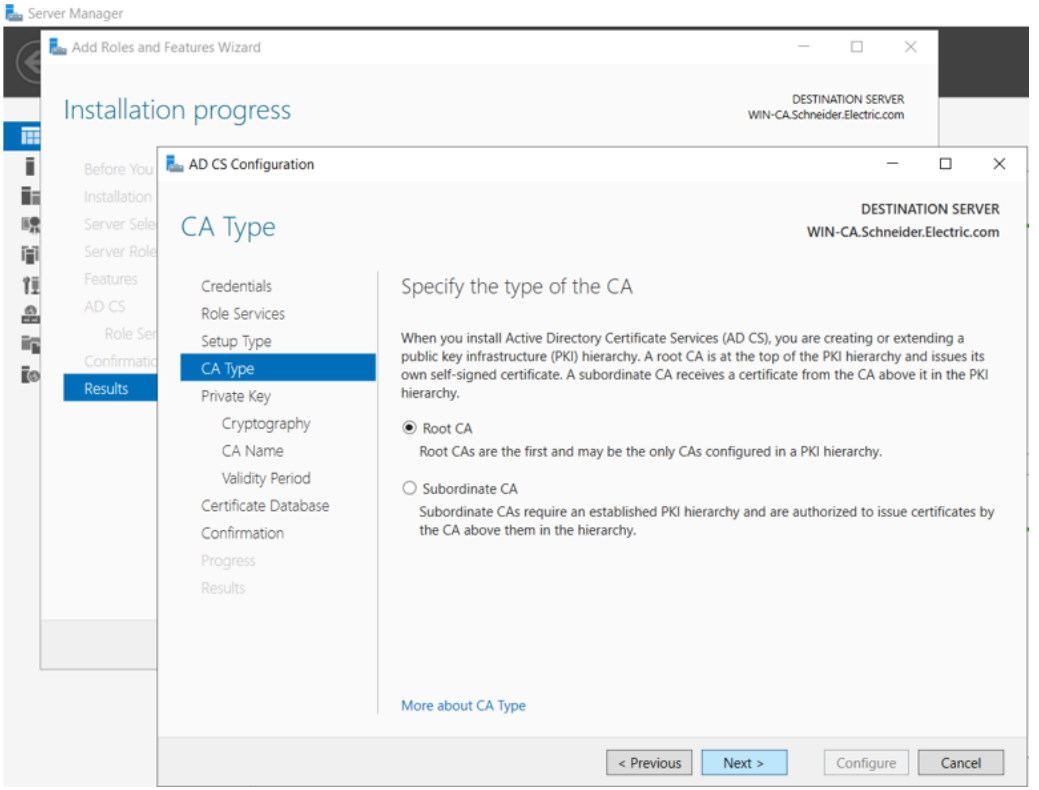
8. Server Manager displays configures the selections:



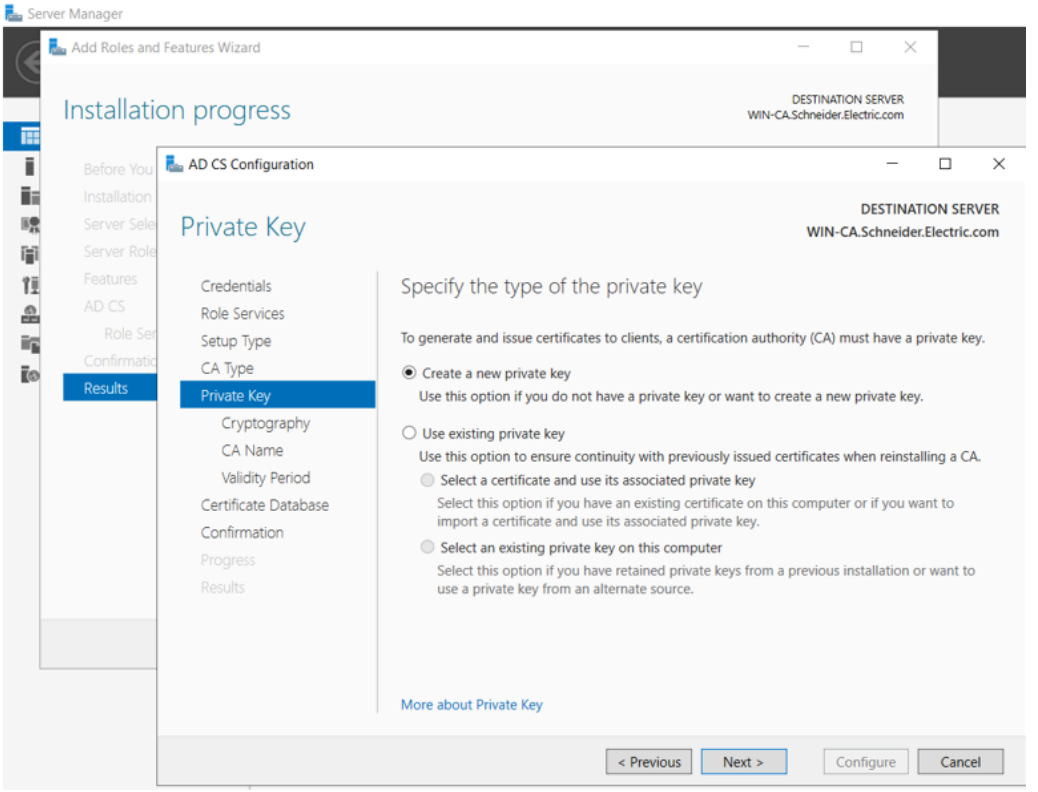
9. Specify the type of CA to setup:



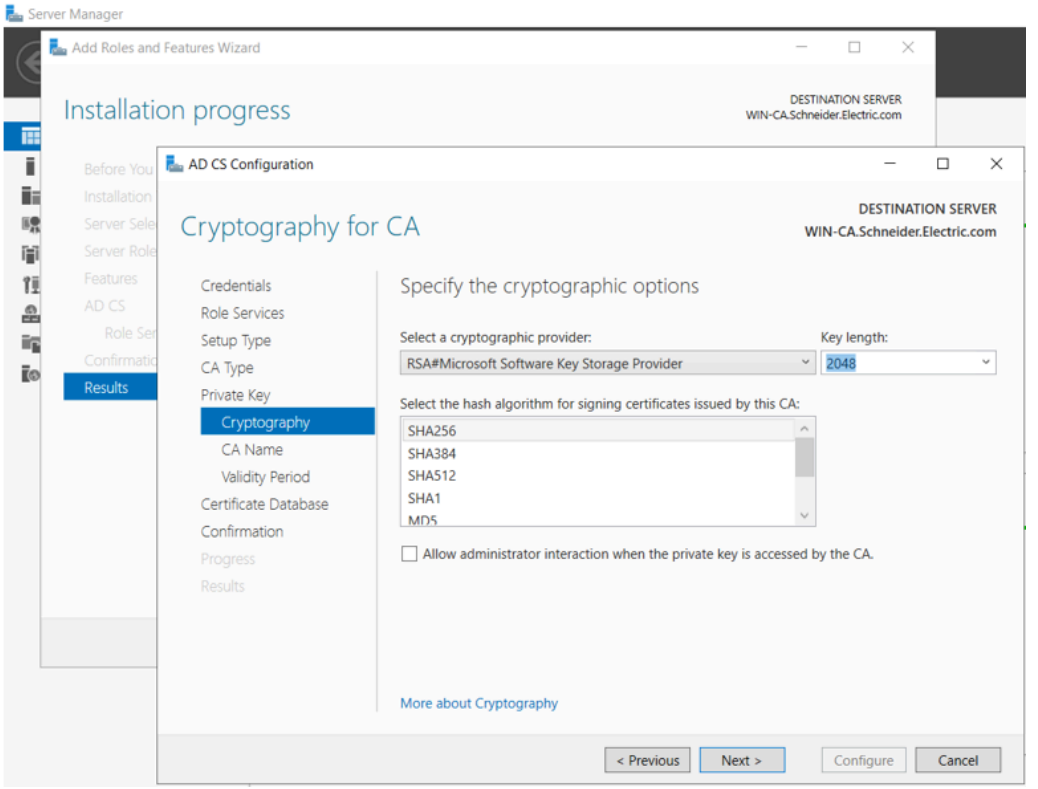
10. Specify the type of CA:



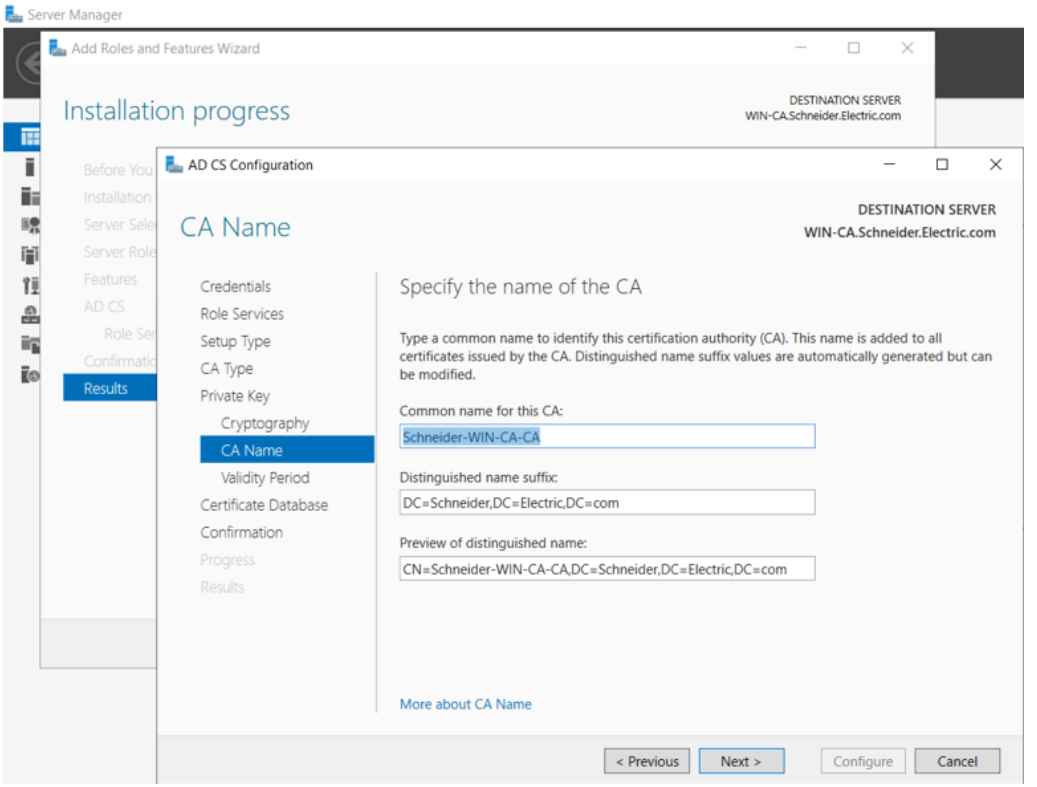
11. Specify the type of private key:



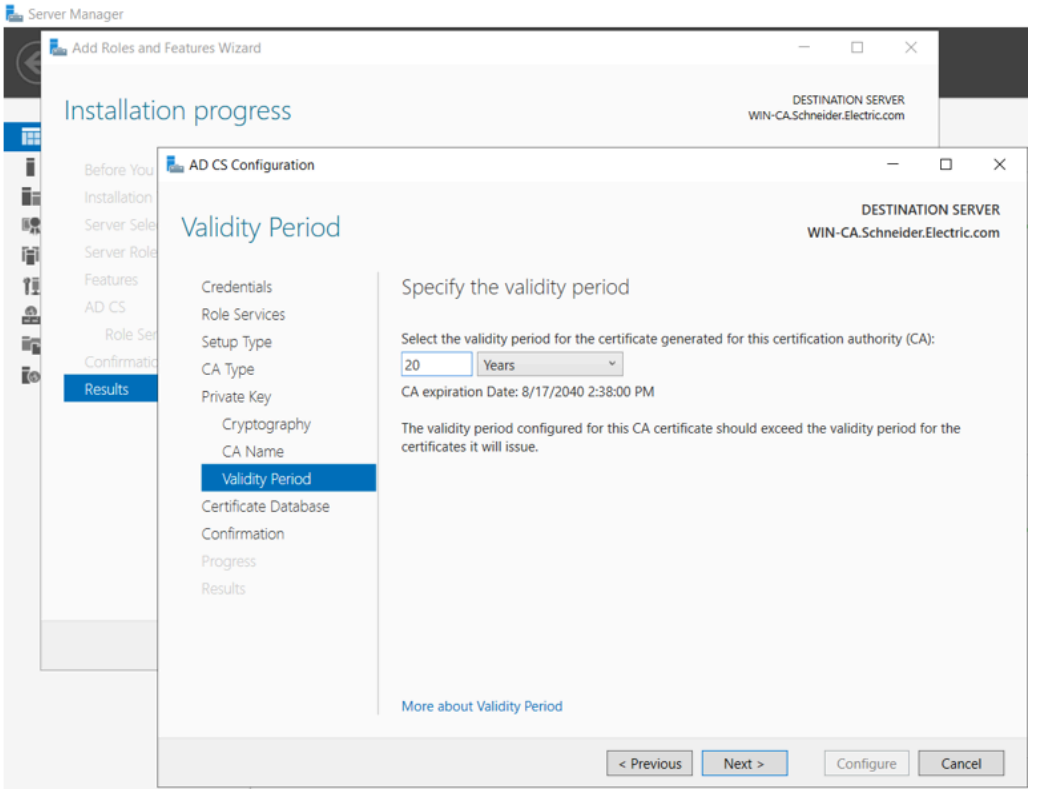
12. Specify the cryptographic selections:



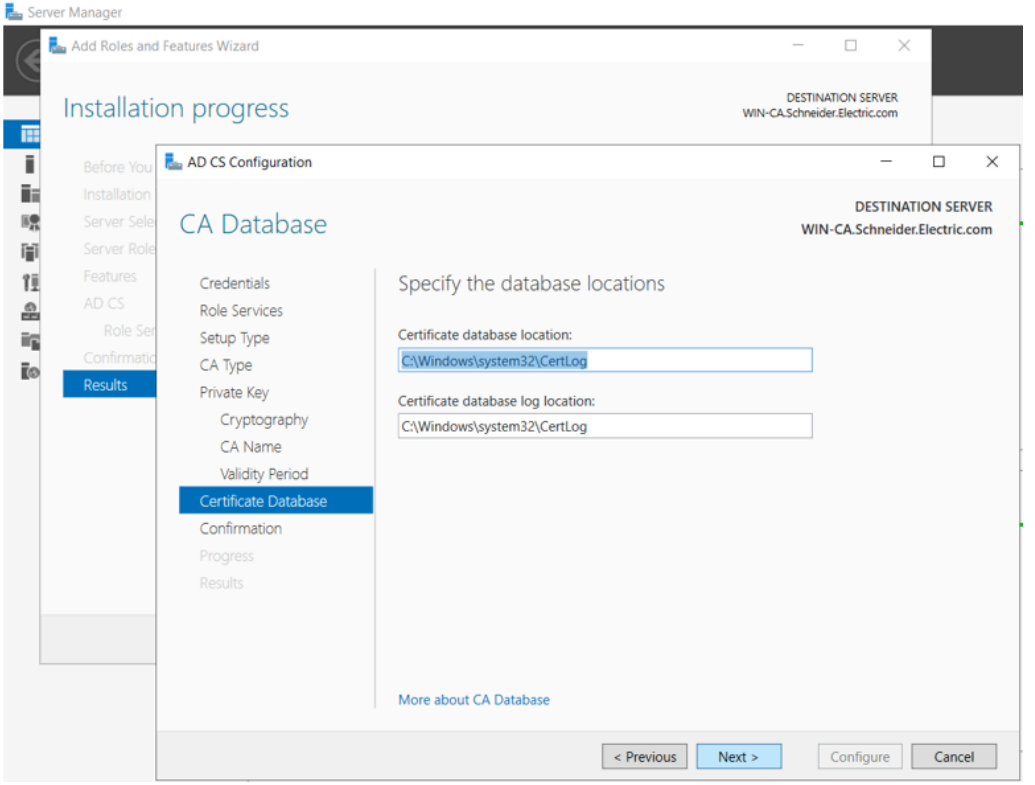
13. Specify the naming selections for the CA:



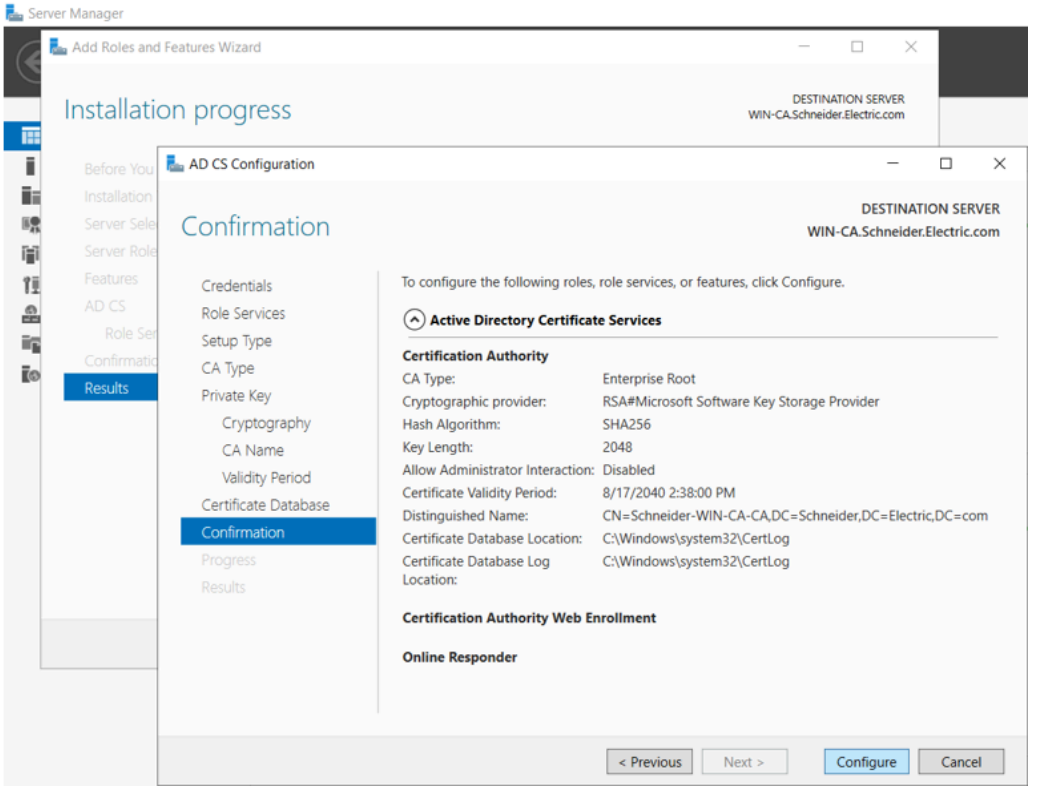
14. Specify the validity period. The typical validity period of a CA certificate is 5 years:



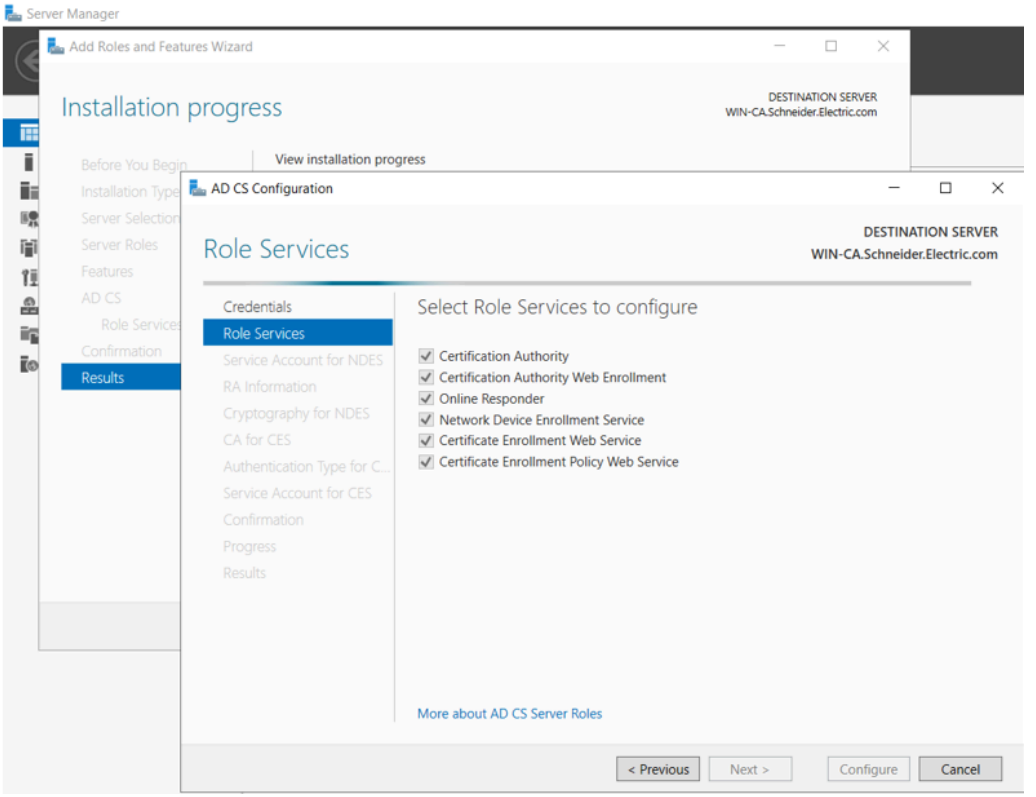
15. Specify the locations of the certificate database and the log:



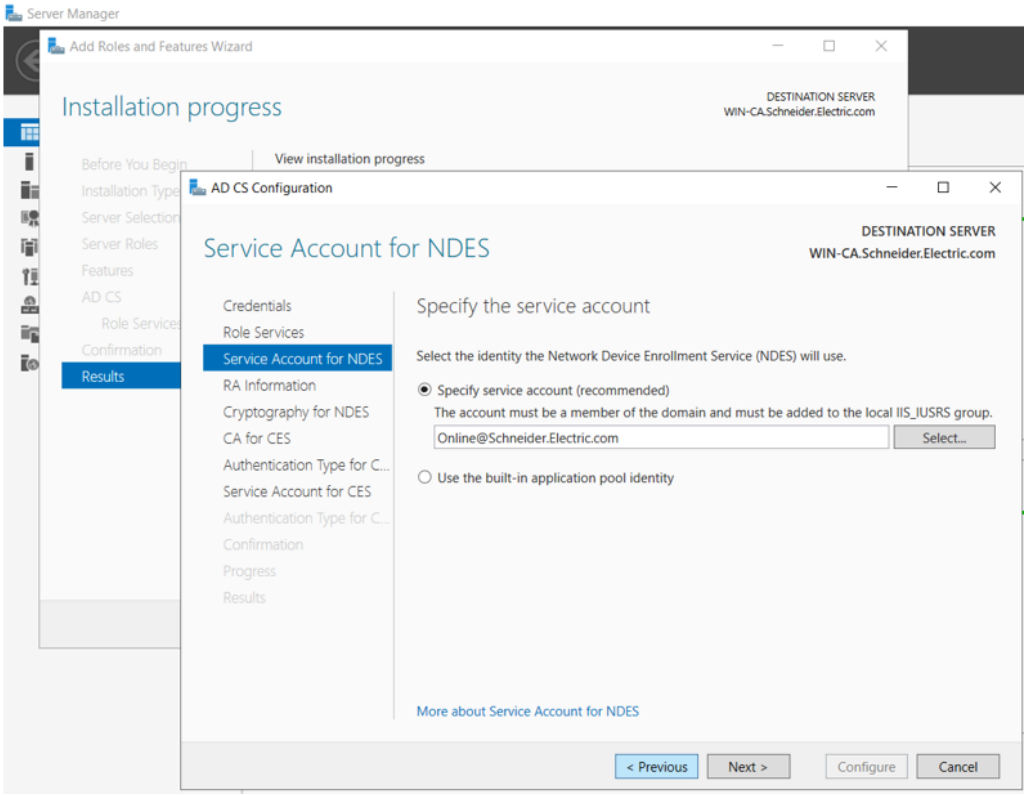
16. Confirm the selected Active Directory Certificate Services and, if correct, click **Configure**:



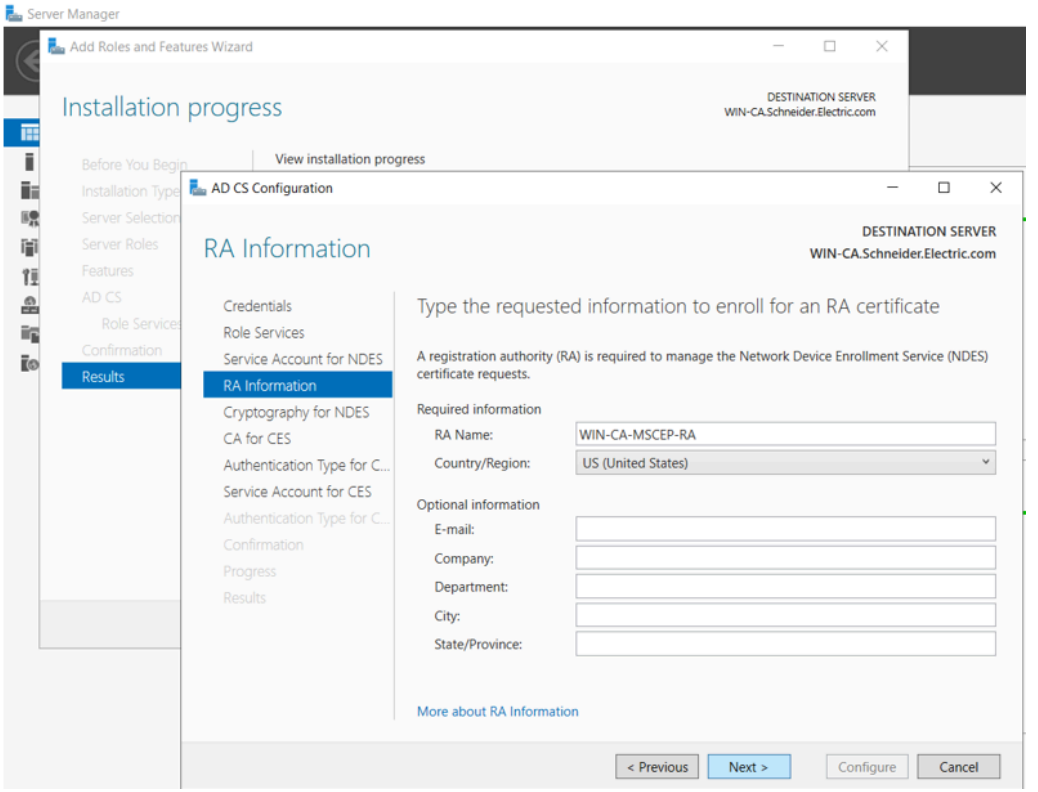
17. Select the role services to configure:



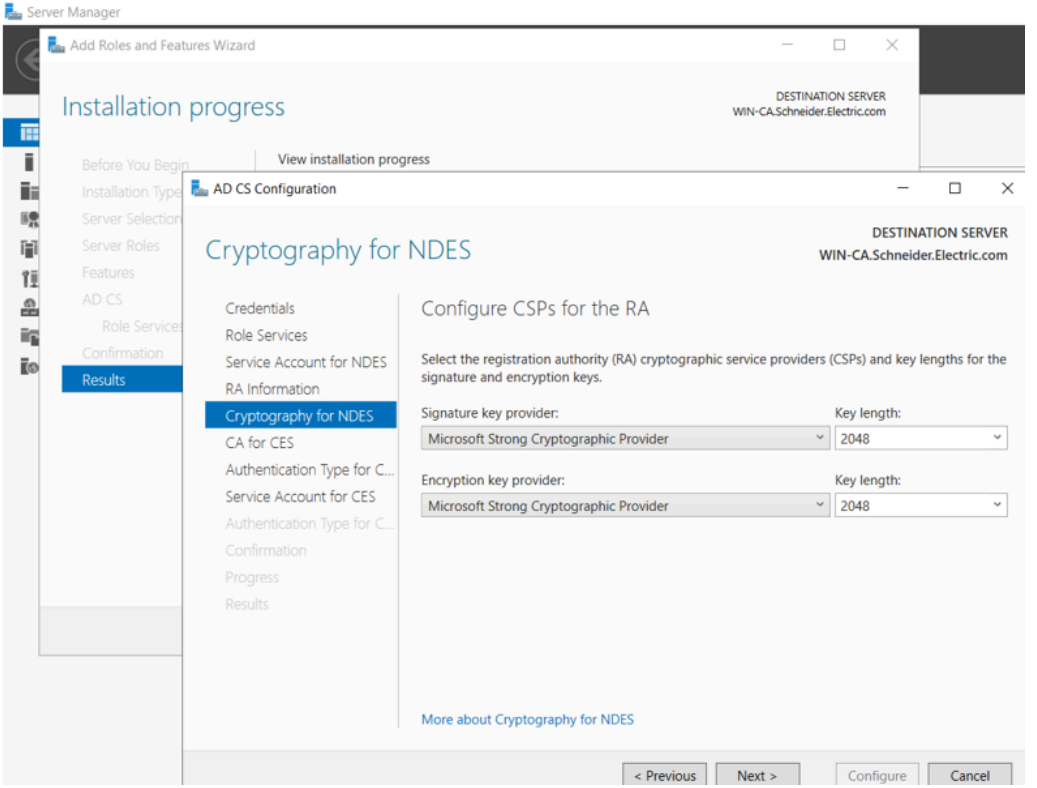
18. Specify the service account:



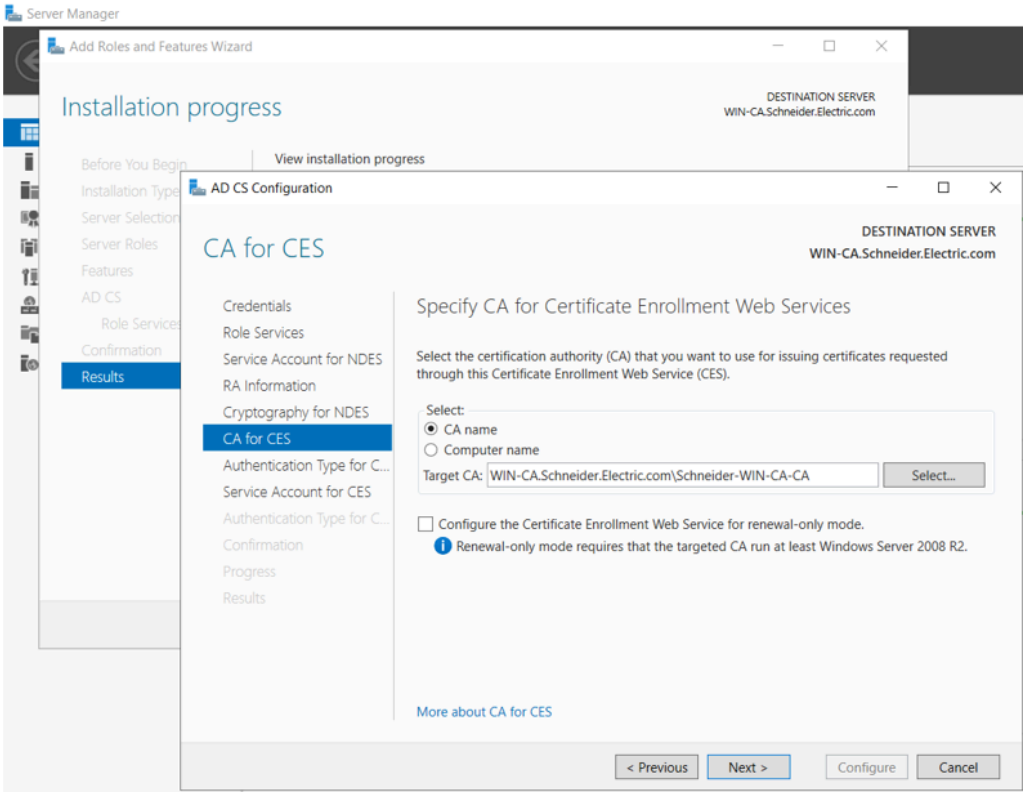
19. Input the information to enroll for a registration authority (RA) certificate:



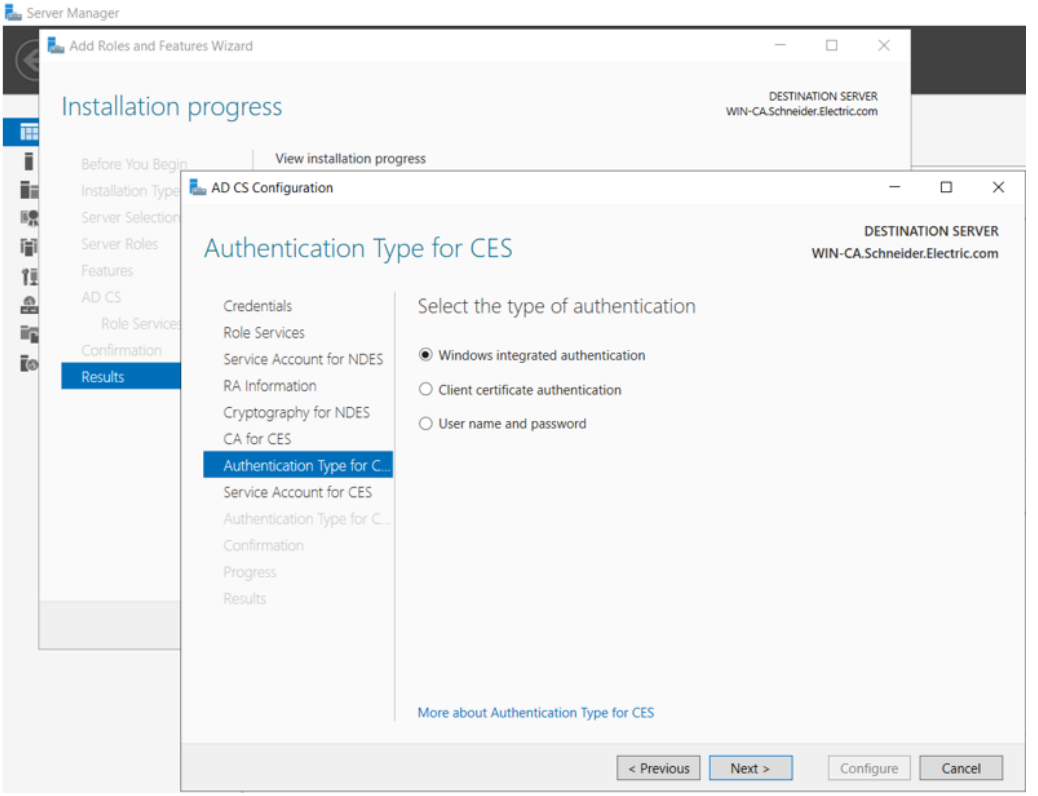
20. Select cryptography settings for the RA:



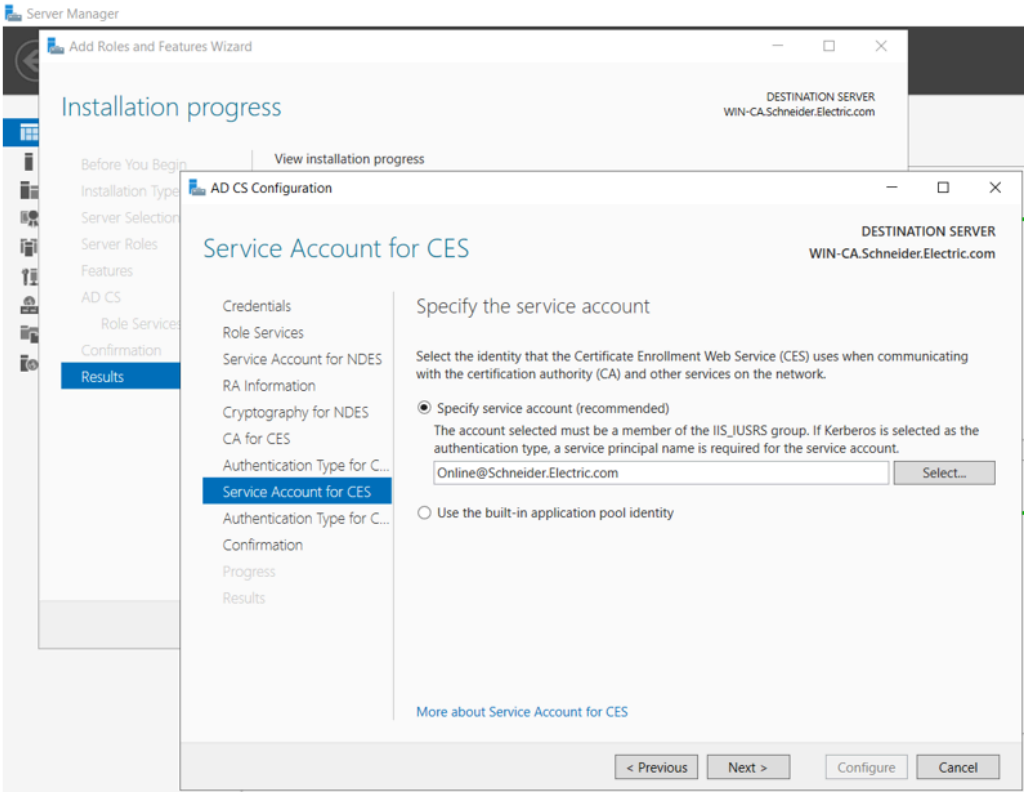
21. Specify the CA for certificate enrollment web services:



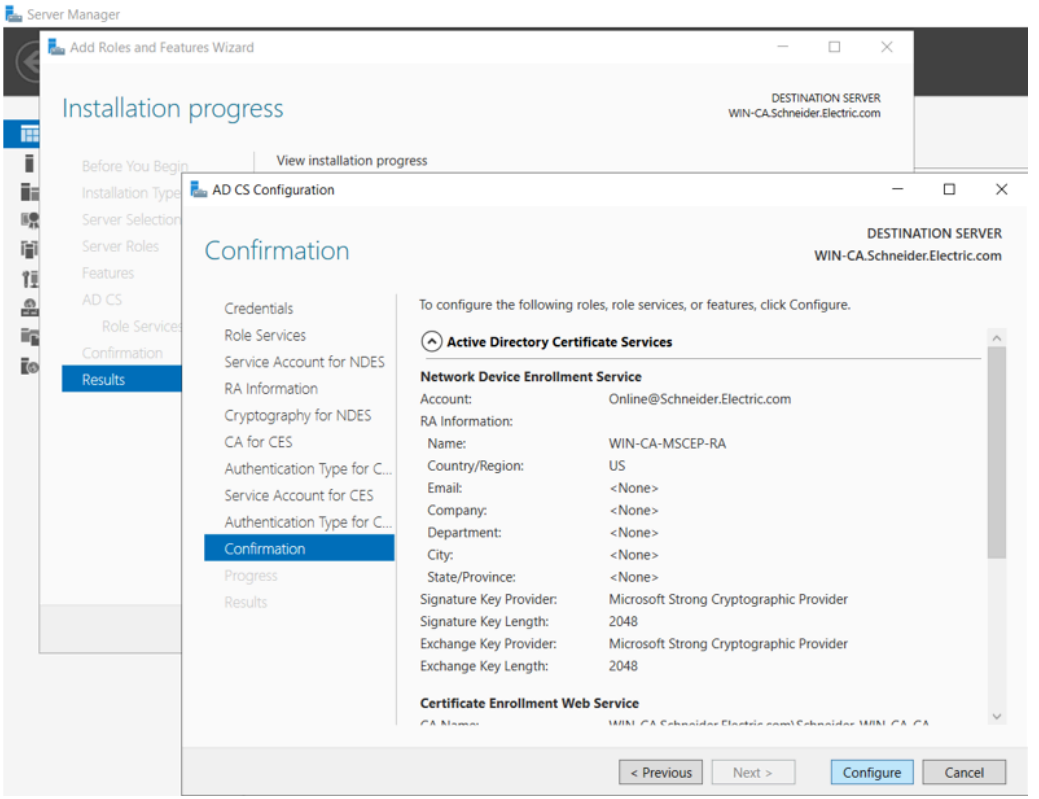
22. Select an authentication type:



23. Specify the service account:



24. Confirm the roles, services and features, then click **Configure**:



This completes the setup of Active Directory Certificate Server.

Applying the Certificate Authority Template

The last part of setting up a Microsoft Windows Certificate Authority is to apply the CA template provided by Schneider Electric.

The template and supporting items are contained in the file “TemplatePackage.zip” provided by Schneider Electric.

To apply the certificate, follow these steps:

1. Unzip the file “TemplatePackage.zip” and copy its contents (a folder named “TemplatePackage” to a location other than C:\Windows\System32...

   For example, you could copy this folder to “C:\Users\Administrator\Desktop\”
2. Start Microsoft Windows PowerShell (or another command tool) as administrator.

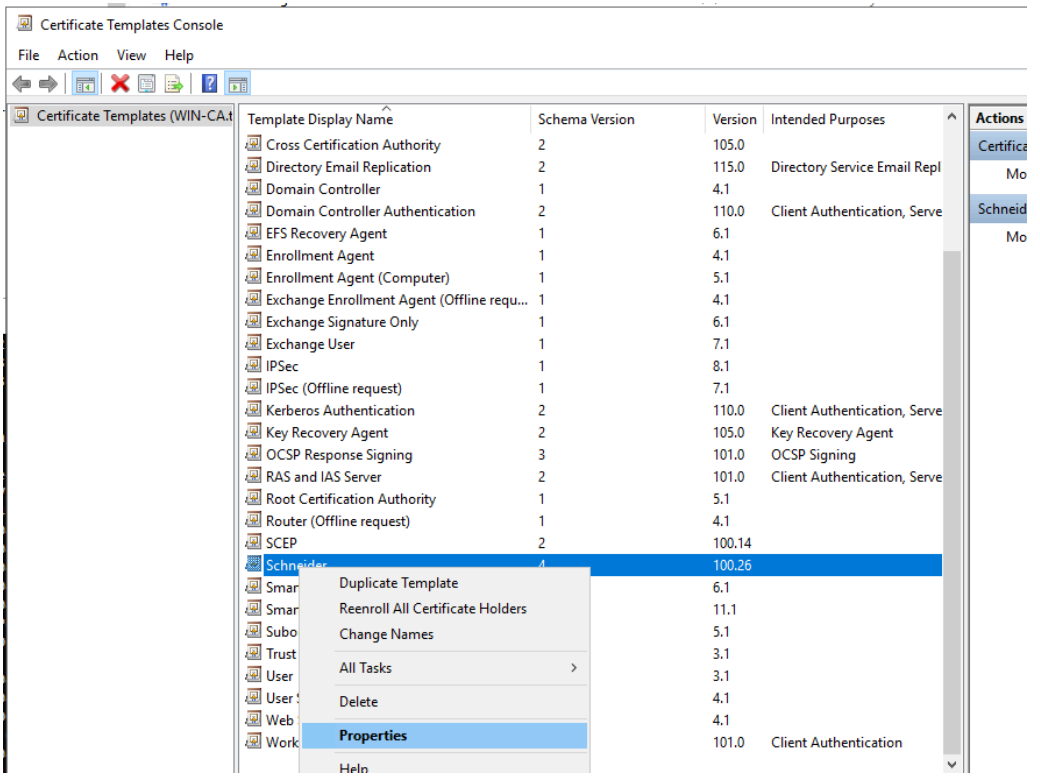
3. Navigate to the folder where you placed TemplatePackage, for example:

   ```
   > cd C:\Users\Administrator\Desktop\TemplatePackage
   ```

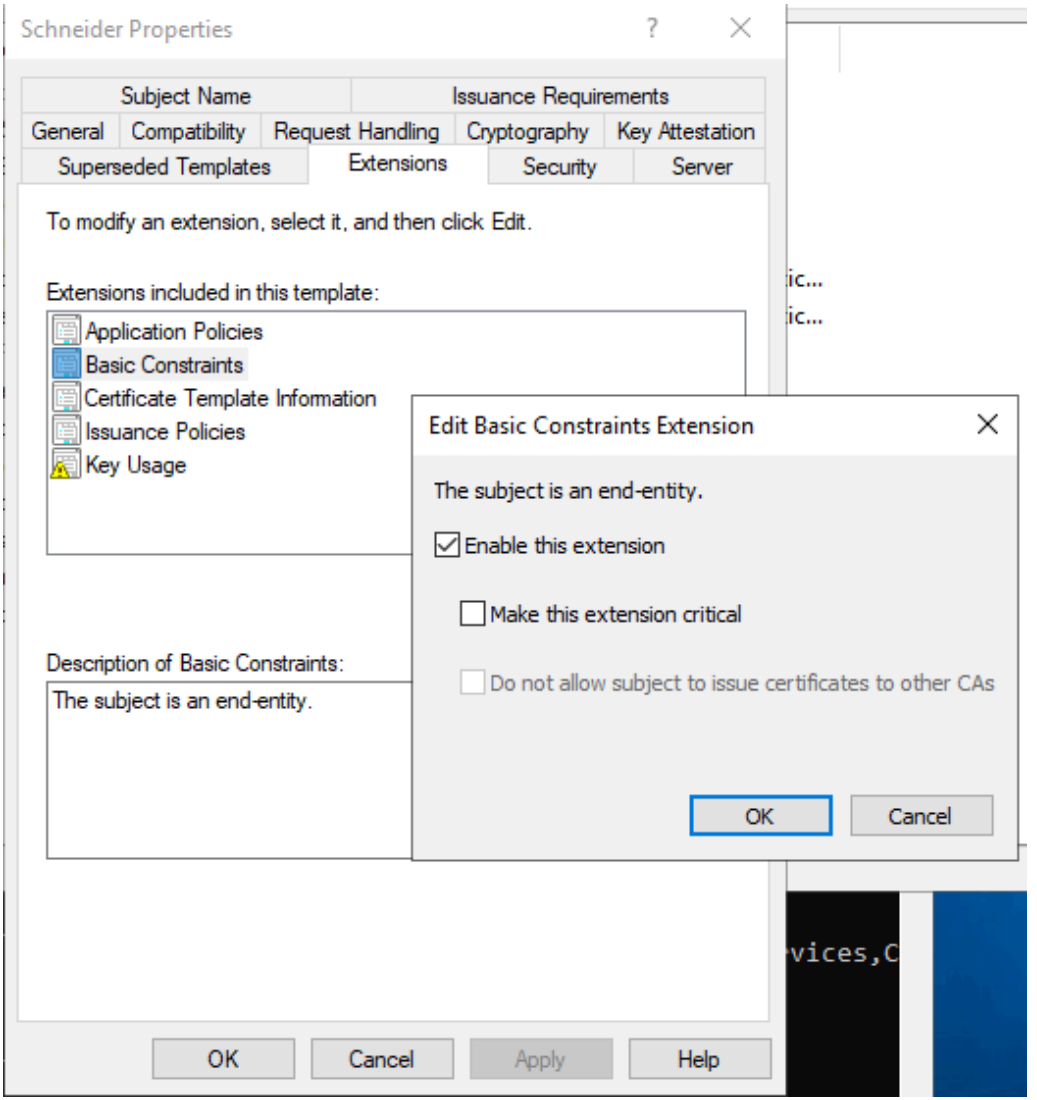
4. Run the template within the TemplatePackage folder, as follows:

   ```
   > .\ImportCertificateTemplate.ps1
   ```

5. On the host PC, open the Certificate Templates Console, right click on the Schneider certificate, then select **Properties**:



6. In the **Schneider Properties** window, open the **Extensions** tab, double-click **Basic Constraints**, and in the **Edit Basic Constraints** dialog box select **Enable this extension** and click **OK**:



Performing Manual Enrollment

Refer to the topic manual certificate enrollment, page 108 for information on how to perform this task.

Click on the link embedded in that topic to access a “How To” video presentation.

Glossary

H

harsh environment:

Resistance to hydrocarbons, industrial oils, detergents and solder chips. Relative humidity up to 100%, saline atmosphere, significant temperature variations, operating temperature between -10°C and + 70°C, or in mobile installations. For hardened (H) devices, the relative humidity is up to 95% and the operating temperature is between -25°C and + 70°C.

I

IP address:

The 32-bit identifier, consisting of both a network address and a host address assigned to a device connected to a TCP/IP network.

S

SNTP:

(*simple network time protocol*) See NTP.

T

trap:

A trap is an event directed by an SNMP agent that indicates one of these events:

- A change has occurred in the status of an agent.
- An unauthorized SNMP manager device has attempted to get data from (or change data on) an SNMP agent.

Index

T

W

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.

PHA83350.05