Honeywell

ControlEdge PLC

ControlEdge RTU

Release 174.1

Network and Security Planning Guide

DISCLAIMER

This document contains Honeywell proprietary information. Information contained herein is to be used solely for the purpose submitted, and no part of this document or its contents shall be reproduced, published, or disclosed to a third party without the express permission of Honeywell International Sàrl.

While this information is presented in good faith and believed to be accurate, Honeywell disclaims the implied warranties of merchantability and fitness for a purpose and makes no express warranties except as may be stated in its written agreement with and for its customer.

In no event is Honeywell liable to anyone for any direct, special, or consequential damages. The information and specifications in this document are subject to change without notice.

CONTENTS

1 ABOUT THIS GUIDE

This document contains networking and security-related information. It provides information to assist you in planning, setting up, and maintaining a secure environment for your system.

Revision history

Revision	Date	Description
A	December 2022	Initial release of the document.

Introduction to ControlEdge Technology

Item	Description
ControlEdge PLC	ControlEdge 900 controllers running the eCLR (IEC 61131-3) execution environment with PLC software options configured with ControlEdge Builder.
ControlEdge RTU	ControlEdge 2020 controllers running the eCLR (IEC 61131-3) execution environment with RTU software options configured with ControlEdge Builder.
ControlEdge UOC	ControlEdge 900 controllers running the Honeywell control execution environment (CEE) configured with Experion Control Builder.

Special terms

The following table describes some commonly used industry-wide and Honeywell-specific terminology:

Terminology	Description
AES	Advanced Encryption Standard; AES is a symmetric block cipher chosen by the U.S. government to protect classified information.
AH	Authenticated Headers; AH is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service.

Terminology	Description
BITW	Bump-in-the-wire; a communications device which can be inserted into existing (legacy) systems to enhance the integrity, confidentiality, or reliability of communications across an existing logical link without altering the communications endpoints.
CMCC	Certificate Manager Configuration Console
CPM	Control Processor Module
CRL	Certificate revocation lists; A CRL is a list of digital certificates that have been revoked by the issuing CA before their scheduled expiration date and should no longer be trusted.
ECDH	Elliptic Curve Diffie Hellman; ECDH is an Elliptic Curve variant of the standard Diffie Hellman algorithm.
ECDSA	Ellipto-Curve Digital Signature Algorithm; ECDSA offers a variant of the Digital Signature Algorithm (DSA) which uses elliptic curve cryptography.
Engineering WorkStation	PC installed with ControlEdge Builder
EPM	Expansion Processor Module
ESP	Encapsulating Security Payload; ESP is used to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service (a form of partial sequence integrity), and limited traffic flow confidentiality.
Experion® PKS	Experion® Process Knowledge System
HMI	Human Machine Interface
HTTP	Hyper Text Transfer Protocol; HTTP is an application protocol for distributed, collaborative, and hypermedia information systems.
IKE	Internet Key Exchange; IKE is an IPsec (Internet Protocol Security) standard protocol used to ensure security for virtual private network (VPN) negotiation and remote host or network access.
IPsec	IPsec is an Internet Engineering Task Force (IETF)

Terminology	Description
	standard suite of protocols that provides data authentication, integrity, and confidentiality as data is transferred between communication points across IP networks.
Modbus	Modbus is a communication protocol developed by Modicon systems. In simple terms, it is a method used for transmitting information over serial lines between electronic devices.
MQTT	Message Queuing Telemetry Transport, an open OASIS and ISO standard (ISO/IEC 20922) lightweight, publish-subscribe network protocol that transports messages between devices. The protocol runs over TCP/IP, or over other network protocols that provide ordered, lossless, bi-directional connections.
OPC UA	OPC Unified Architecture; OPC UA is a machine to machine communication protocol for industrial automation developed by the OPC Foundation.
PLC	Programmable Logic Controller; A PLC is an industrial computer control system that continuously monitors the state of input devices and makes decisions based upon a custom program to control the state of output devices.
SCADA	Supervisory Control and Data Acquisition
SCEP	Simple Certificate Enrolment protocol; SCEP is a protocol used for enrolment and other Public Key Infrastructure (PKI) operations.
SHA-256	Secure Hash Algorithm; SHA is a cryptographic hash function.
Simulator	Simulator can be deployed on a Virtual Machine, and enables the user to configure a controller without connecting a physical controller.
SNTP	Simple Network Time Protocol; SNTP is a simplified version of Network Time Protocol (NTP) that is used to synchronize computer clocks on a network .
TLS	Transport Layer Security; TLS is a cryptographic protocol that provide communications security over a computer network.

Terminology	Description
X.509	An X.509 certificate is a digital certificate that uses the widely accepted international X.509 public key infrastructure (PKI) standard to verify that a public key belongs to the user, computer or service identity contained within the certificate.

Related documents

The following list identifies publications that may contain information relevant to the information in this document.

- ControlEdge Builder Software Installation User's Guide

- ControlEdge Builder Software Change Notice

- ControlEdge PLC and ControlEdge RTU Getting started

- ControlEdge Builder User's Guide

- ControlEdge 900 Platform Hardware Planning and Installation Guide

- ControlEdge 2020 Platform Hardware Planning and Installation Guide

- ControlEdge Builder Function and Function Block Configuration Reference

- ControlEdge Builder Protocol Configuration Reference Guide

- ControlEdge EtherNet/IP User's Guide

- ControlEdge RTU and PLC DNP3 Device Profile

- ControlEdge Bulk Configuration User's Guide

- ControlEdge PLC PROFINET User's Guide

- ControlEdge RTU Electronic Flow Measurement User's Guide

- Firmware Manager User Guide

2 INTRODUCTION

This guide contains networking and security information applicable to ControlEdge™ PLC and ControlEdge™ RTU. It provides recommendations to assist you in planning, setting up, and maintaining a secure environment for your system.

> **NOTE:** It is recommended to upgrade all firmwares and software to the latest version to reduce the threats from known and unknown risks.

Assumptions and Prerequisites

This guide is primarily intended for engineers, system administrators, and other technical staff who are responsible for planning the configuration and maintenance of ControlEdge PLC and ControlEdge RTU system. Therefore, it is assumed that the user has technical knowledge and familiarity with the following:

- Microsoft Windows operating systems
- Networking systems and concepts
- Security issues and concepts

> **ATTENTION:** As you derive a security program for your process control system, you must be aware that detailed information, if not protected, can fall into the hands of organizations that could cause harm to your control system or process operations.

3

SECURITY CHECKLISTS

This chapter provides a number of checklists which help you analyze the security issues that must be considered for your site.

The checklists cover some of the main security risks that may exist on a process control network and the steps that can be used to mitigate against them.

Viruses and Other Malicious Software Agents

There is the potential risk for malicious software agents, such as spy ware (trojans) and worms to infiltrate the process control network.

The infiltration of the malicious software agents can result in the following:

- Performance degradation
- Loss of system availability
- The capture, modification, or deletion of data
- Loss of public confidence if the external access becomes public knowledge

Mitigation steps

- Ensure that your virus protection and Microsoft security hot fixes are up to date on all nodes in your process control network and the system connected to it.
- Ensure that there are no e-mail clients on any nodes in your process control network.
- Use a firewall for the business network to process control network interface.

Unauthorized External Access

This threat includes intrusion into the process control system from the business network and possibly from an intranet or the Internet.

Unauthorized external access can result in the following:

- Loss of system availability

- Incorrect execution of controls, causing damage to the plant, or theft or contamination of product

- Loss of public confidence if the external access becomes public knowledge

Mitigation steps:

- Use a firewall for the business network to process control network interface to restrict access from the business network to process control network.

- Set the minimum level of privilege for all accounts, and enforce a strong password policy.

Unauthorized Internal Access

This risk encompasses unauthorized access from systems within the process control network. This threat is the most difficult to counter since attackers may well have legitimate access to part of the system and they simply want to exceed their permitted access.

Unauthorized internal access can result in the following:

- Loss of system availability

- Incorrect execution of controls causing damage to the plant, or theft or contamination of product

- The capture, modification, or deletion of data

Mitigation steps

- Ensure Engineering Station security.

- Use physical security for process control network systems for ControlEdge 900 Platform and 2020 Platform.

- Do not allow the use of unauthorized removable media.

- Prevent the use of unauthorized laptops on the process control network.

- Use and enforce a strong password policy. Change passwords at an acceptable frequency to reduce the risk when a password is compromised.

Accidental System Change

This risk encompasses inadvertent changes to executables or configuration files.

Accidental system change can result in the following:

- Loss of system availability
- Loss of data

Mitigation steps

Set the minimum level of privilege for all accounts, and enforce a strong password policy.

Protecting ControlEdge System Components

The measures in this section list the steps you can take towards securing ControlEdge system.

PC installed with ControlEdge Builder

Protection measure

- Take steps to implement and enforce physical security.
- Set the minimum level of privilege for all accounts and enforce a strong password policy. Change passwords at an acceptable frequency to reduce the risk when a password is compromised.
- Ensure that your virus protection and Microsoft security hot fixes are up to date on all systems.

Network Components

Protection measure

- Take steps to implement and enforce physical security. For example, lock the network switch in the cabinet.
- Set the minimum level of privilege for all accounts and enforce a strong password policy.
- Set the security of the manger type network switches properly.

System Performance and Reliability

Protection measures

- Do not allow port scanning within the process control network.

- Do not automatically schedule full system antivirus scans on PC installed with ControlEdge Builder.

4 BACKUP AND RESTORE

This chapter describes planning considerations for backup and restore policies and the tools that are supported for backing up and restoring your ControlEdge system.

Formulating a Disaster Recovery Policy

As part of your security strategy, it is highly recommended that you define a comprehensive backup and restore policy for disaster recovery purposes.

Consider the following when formulating this policy.

- How frequently critical data and configurations are changing. This dictates the frequency and completeness of backups.

- The safe onsite and offsite storage of full and incremental backups.

- The safe storage of installation media, license keys, and configuration information.

- Who is responsible for backups, and the testing, storing, and restoring of backups?

Backup and Restore Configurations

Use ControlEdge Builder to backup and restore your project configuration.

For more information, see "Managing a project" in the *ControlEdge Builder User's Guide*.

17

CHAPTER

5

PHYSICAL AND ENVIRONMENTAL CONSIDERATIONS

The physical security of a process control network is particularly important. If the hardware is rendered inoperable, the entire system (and hence the plant) is rendered inoperable.

Protecting Against Unauthorized System Access

External media drives can enable anyone to bypass Windows security and gain access to your system.

If there is an easy access to a computer, and it has a floppy disk or CD drive, it can be booted from an alternative operating system. This can be used to circumvent file system security, and could be used to install damaging software, or even to reformat the hard disk.

It is therefore of critical importance in relation to the nodes in your process control network that you prevent the use of all unauthorized removable devices and media such as CDs, DVDs, floppy disks, and USB memory sticks.

There are several other steps that can be taken to reduce the risk of unauthorized access, including:

- Setting the BIOS to boot only from the C drive.
- Setting a BIOS password (check that this does not prevent automatic startup).
- Physically securing the computer (for example, in a locked room or cabinet) or fitting locks to the floppy and CD or DVD drives.
- Removing (in extreme cases) the floppy and CD or DVD drives from the computer.
- Disabling USB ports and other ports capable of being used for memory sticks and other portable storage devices.

Control Room Access

Providing physical security for the control room is essential to reduce the possibility of many threats. The area often contains the Engineering Workstation and ControlEdge system. Limiting those who can enter this area, using smart or magnetic identity cards, biometric readers and so on are essential. In extreme cases, it may be considered necessary to make the control room blast-proof, or to provide a second off-site emergency control room so that control can be maintained if the primary area becomes uninhabitable.

Network and Controller Access

ControlEdge 900 and 2020 controllers are intelligent programmable devices, with the ability to be manipulated through loader software running on a laptop or similar, directly connected computer. In order to prevent unauthorized tampering, the controllers and network equipment must be physically protected in locked cabinets, and logically protected with passwords or other authentication techniques. Network cables are also vulnerable to damage or unauthorized connection. For maximum protection, cabling must be duplicated and laid in separate hardened cable runs.

Once the controller is deployed and powered on, the controller access password of each user type must be changed immediately. See "User Privilege" in *ControlEdge Builder User's Guide* for how to change passwords.

Physical Access to Critical Devices

The malicious operation of critical ControlEdge 900 and 2020 modules will result in system shutdown, unexpected system start up or restart, or otherwise impact process control. The critical ControlEdge 900 modules include Expansion Processor Module (EPM), Control Processor Module (CPM), network switches for I/O network and host communication network, I/O Modules, power supply modules, and simulator. Critical ControlEdge 2020 modules include: Control Processor Module (CPM), network switches for I/O network and control network, Expansion IOM, and simulator. For maximum security, the ControlEdge PLC system must be placed in a cabinet or locked closet to protect against unauthorized access to the critical modules.

6

SECURITY UPDATES

Microsoft Security Updates and Service packs

Microsoft releases a range of security updates and other operating systems and software updates. Note that only Honeywell-qualified Microsoft updates are supported. Therefore, you must wait until Honeywell has validated Microsoft updates before installing them. It is also recommended that you implement a controlled system for the distribution of all updates.

Timely information on security updates can be obtained by subscribing to the Microsoft Security Bulletins at http://www.microsoft.com/technet/security/current.aspx

Virus Protection

Protection measure

- Choose supported antivirus software
- Installing antivirus software on Engineering Workstation
- Configure active scanning
- Tune the virus scanning for system performance
- Ensure frequent updates to antivirus signature files

NETWORK AND SECURITY

ControlEdge PLC or ControlEdge RTU can be configured as a redundant controller system or non-redundant controller system. It includes provisions for communication via Ethernet with host systems and the Ethernet ports provide a layer of protection against cyber-attacks. It is recommended to use Solarwinds and/or Honeywell Risk Manager to detect unintended and excess network traffic.

Architecture

ControlEdge system has two network levels, while level 1 network is used for internal I/O communication between CPM and related IOMs, and level 2 is aimed for the communication with the third party devices, HMI, SCADA or Engineering Workstation. The following diagram shows an example system architecture.

Figure 7-1: System architecture of ControlEdge PLC
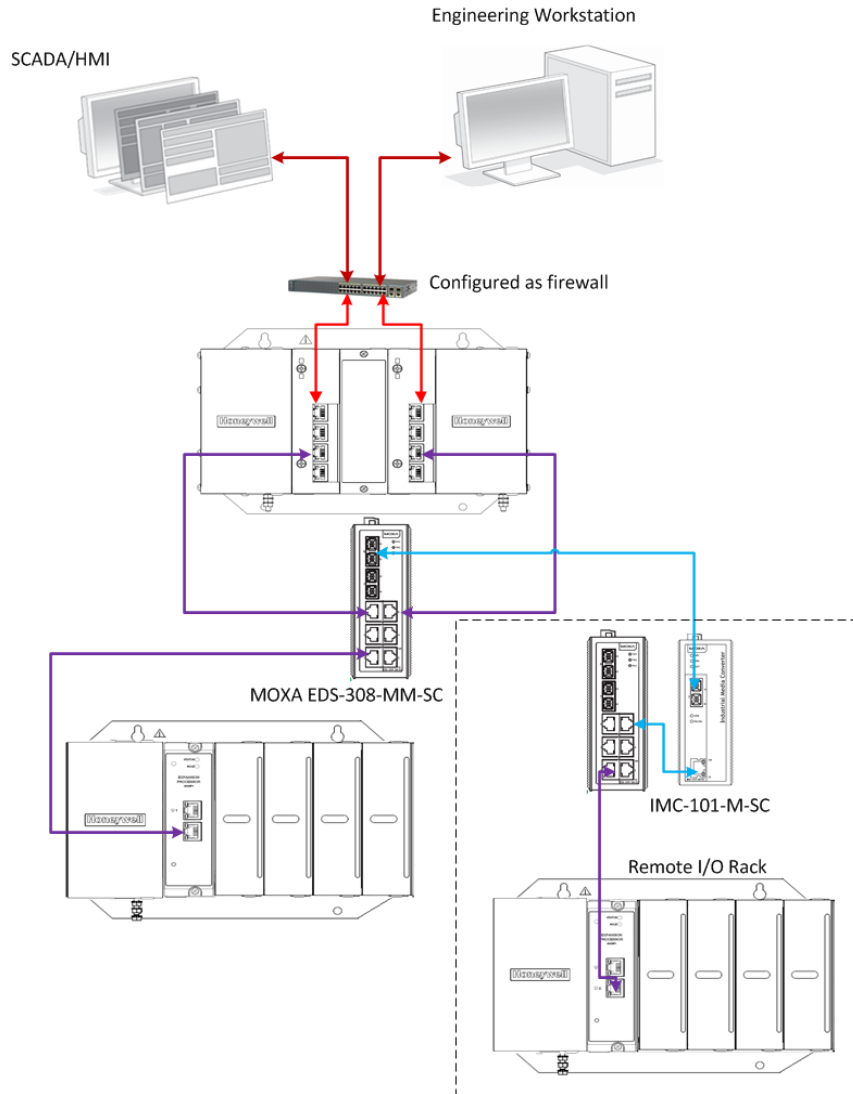
On the level 1 network, CPMs and EPMs connect to a switch, this network is the most critical network in the system as a failure or loss of service on this network can result in loss of control. On the level 2 network, the Engineering Workstation, third party devices, HMI, and SCADA connect to the switch at this level. A failure of this level network may result in a loss of view of the process if HMI or SCADA is employed. The two network levels must be isolated with each other.

ETH1/ETH2 ports of the CPM are required to be protected using a firewall device configured to prevent uncontrolled messages into the controller.

Built-in firewall is supported on CPM of ControlEdge PLC. See Built-in Firewall for more information.

ControlEdge 2020 system has two networks, I/O network is used for internal I/O communication between CPM and Expansion IOMs, control network is aimed for the communication with the third party devices, HMI, SCADA or Engineering Workstation, take the following diagram as an example of system architecture.

Figure 7-2: System architecture of ControlEdge RTU
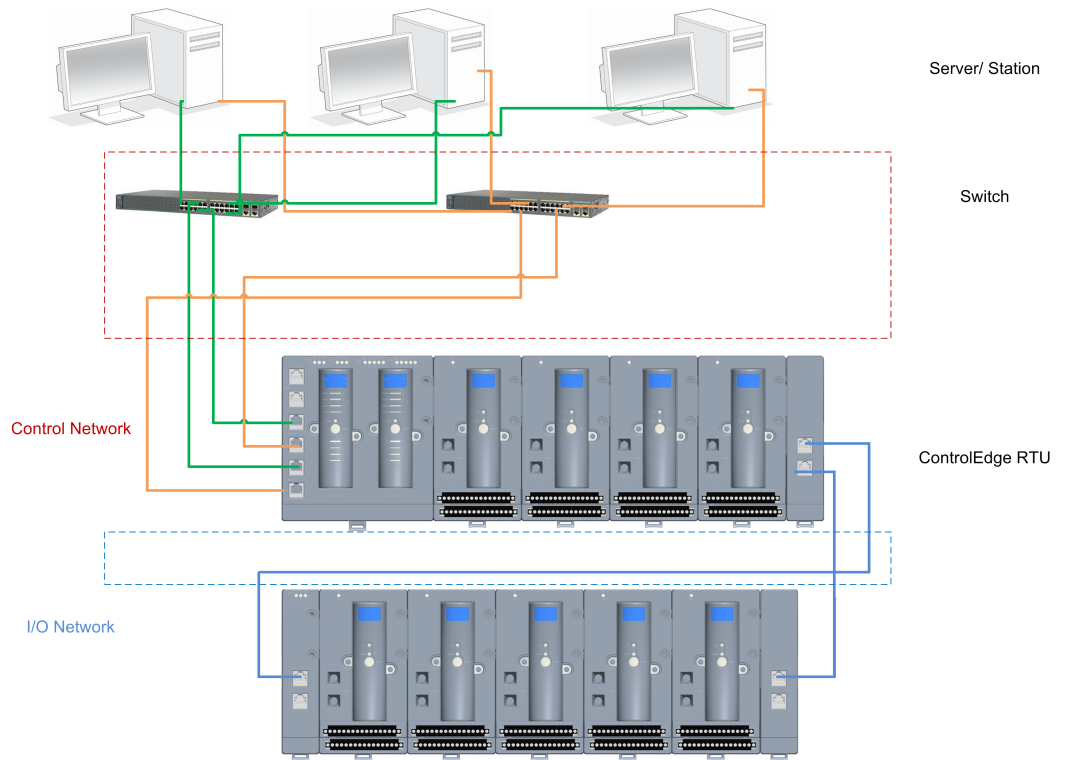
I/O network is the most critical network in the system as a failure or loss of service on this network can result in loss of control.

At control network, Engineering Workstation, third party devices, HMI, and SCADA connect to the switches. A failure of this level network may result in a loss of view for operator of the process if HMI or SCADA is employed.

The two networks must be isolated from each other.

The recommended firewall settings include:

- Close all Ethernet ports into controller except:
    - Modbus TCP Server (port 502 by default)
    - DNP3 Outstation (port 20000 by default) for ControlEdge RTU

- HART IP (port 5094 by default)

- OPC UA (port 4840 by default) only for ControlEdge PLC

- ControlEdge Builder Controller Configuration protocol (port 41103)

- ControlEdge PLC\RTU privacy protocol (port 9050)

- SNTP (port 123 ONLY if NTP server is enabled)

- Destination DHCP for uplink (port 68)

- Modbus Client and OPC UA Client that are configured in the relative function blocks

- EtherNet/IP (port 44818 and 2222)

- Profinet (port 34962, 34964, 49152, 49153 and 49154)

- MQTT (port 8883 by default)

- IEC60870-5-104 (port 2404 by default)

- Other ports. See Built-in Firewall for more information.

- Rate Limiting

  In general, one host should not be allowed to occupy unlimited bandwidth. For example, "broadcast storms" could be caused by an incorrectly configured topology or a malfunctioning device. Firewalls can prevent storms seen by ETH1/ETH2 ports. Limit rate of all traffic (Ingress/egress) to ETH1/ETH2 to <= 3000 packets per second.

Firewall device(s) should be introduced above the network at the control network level prior to the supervisory control network level. See Architecture for more information.

Planning for network topology

ControlEdge RTU collects data from field devices or drives field devices. It communicates with the supervisory server through a variety of means such as satellite, radio, mobile networks, Ethernet, RS232, and RS485.

Figure 7-3: ControlEdge RTU Network Topology
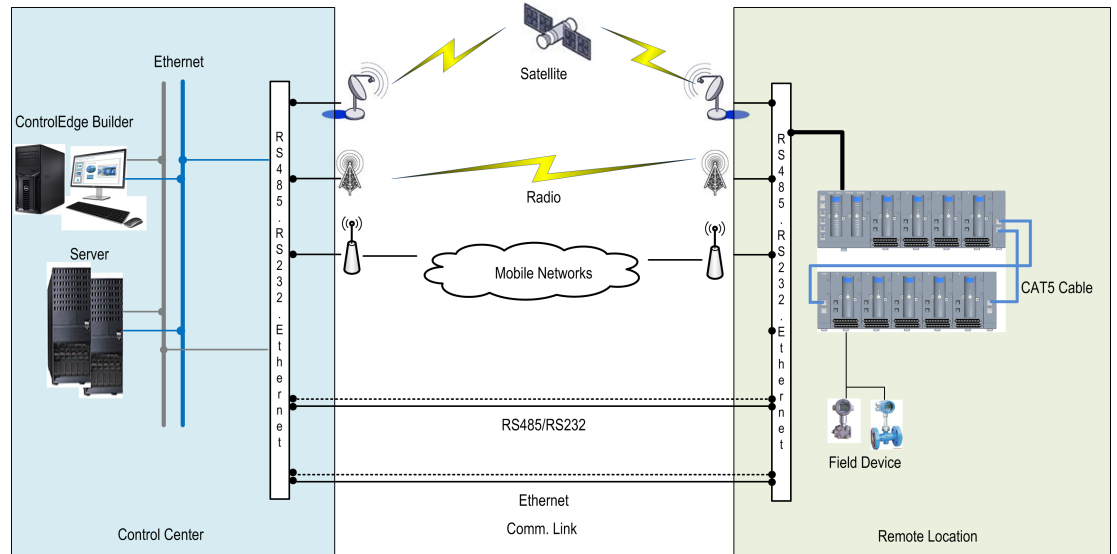
Control center includes engineering station, SCADA server and FDM server.

Honeywell ControlEdge Builder installed on the engineering station performs the system configuration, programming, maintenance, and trouble shooting.

This SCADA system monitors and controls ControlEdge 2020 Controllers deployed at remote locations.

Field Device Manager (FDM) application is an asset management system.

The application provides an environment to configure, commission, and maintain smart field devices. FDM server maintains the record of all the users and device information such as device type, device manufacture's information, device history, offline configuration information and so on. ControlEdge 2020 Controller communicates with FDM Server through HART-IP.

The following sections explain some of the typical topologies supported by ControlEdge 2020 Controller. Combinations of different connection media could be selected according to specific conditions at the customer site.

In the following two topologies, redundant and non- redundant ControlEdge RTU are connected to the server through Ethernet ports.

Redundant uplink communication is enabled by the two Ethernet ports. Modbus devices and subsystem over Modbus ASCII and ControlEdge RTU protocol are connected to the serial ports.

ST103A can be added into the system via RS485 ports over Modbus.

For wireless I\O communication, a Honeywell FDAP via wireless and FDAP is needed in the Ethernet.

Terminal server, wireless, radio, Modbus Slave, Modbus Master, wireless I/O devices and HART devices can be added into the system to build a more complicated architecture.

Figure 7-4: Redundant Ethernet Communication between Non-redundant ControlEdge RTU and server
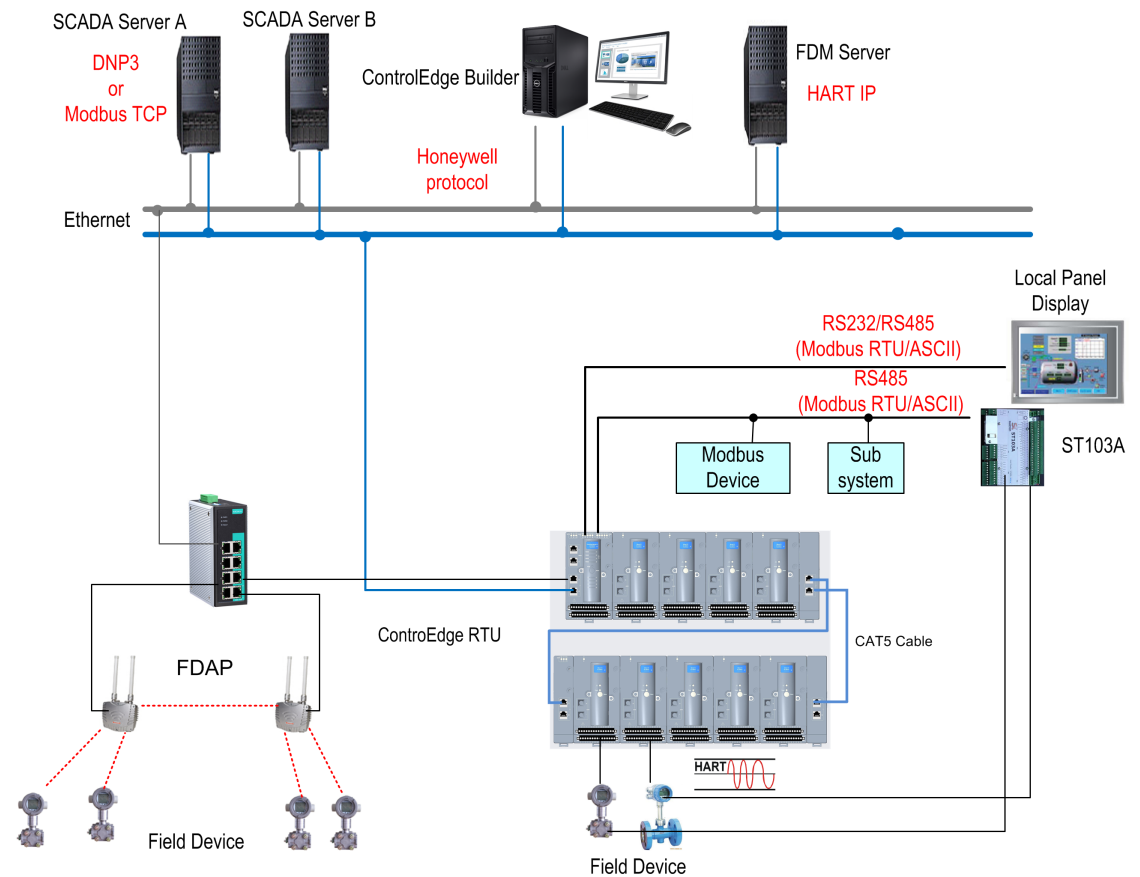
Figure 7-5: Redundant Ethernet Communication between Redundant ControlEdge RTU and server
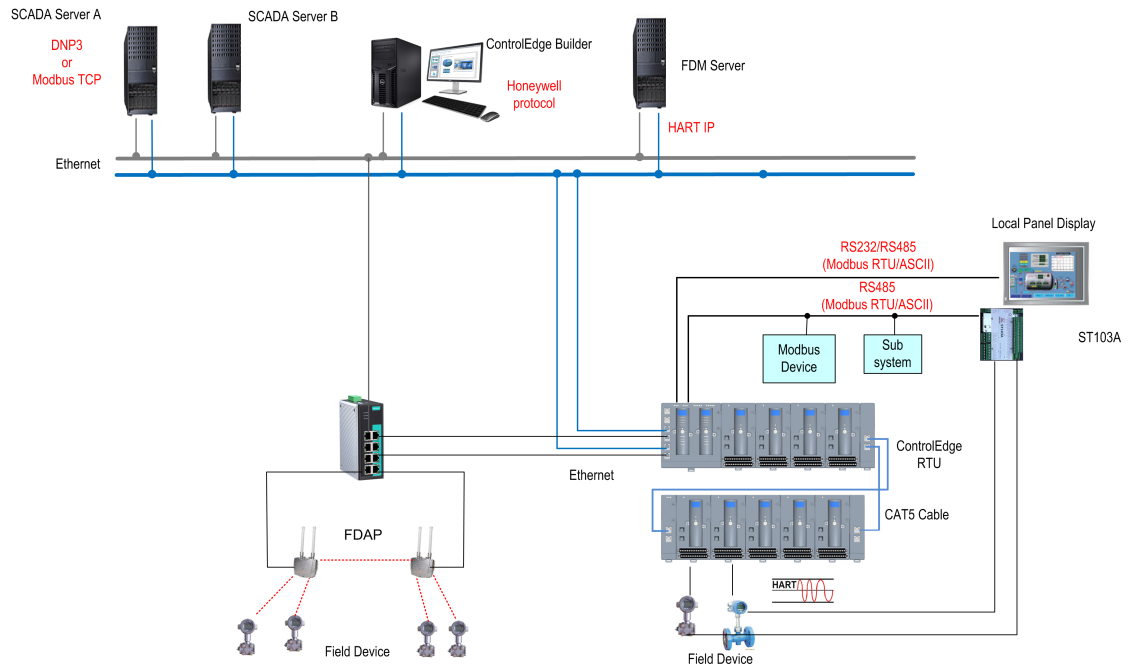
Supported Topologies

ControlEdge PLC supports Star, High Speed Ring (HSR), and Device Level Ring (DLR) I/O topologies for I/O communication;

ControlEdge RTU supports ring I/O topology for I/O communication.

Star Topology

ControlEdge PLC supports star I/O topology for I/O communication. The following diagram shows an example of the topology.

A switch is required for this topology. For more information, see "Planning for network topology" in the *ControlEdge 900 Controller Hardware Planning and Installation Guide*.

Figure 7-6: Single star topology

Ethernet Star
network
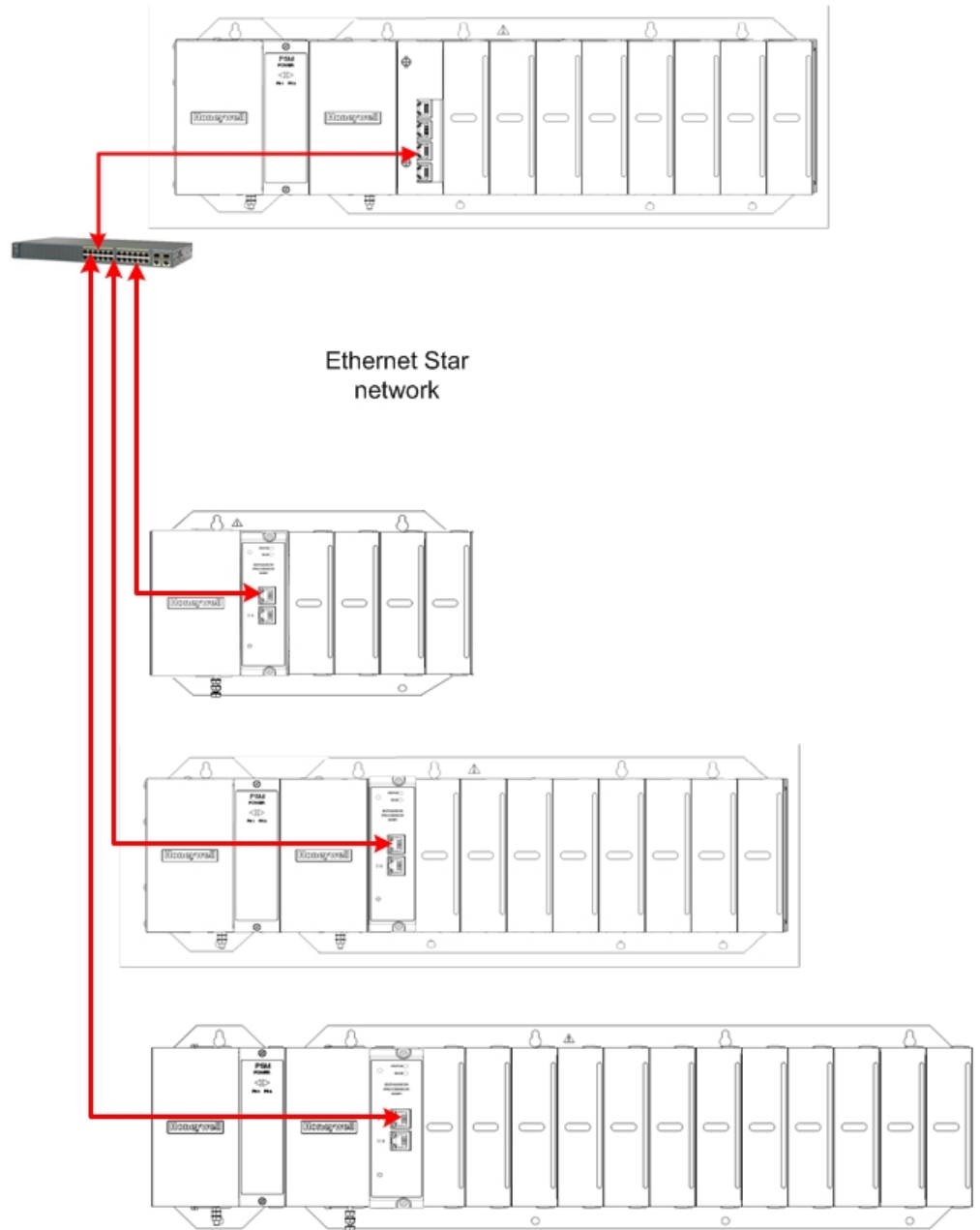
Figure 7-7: Redundant Star topology

Ethernet Star
network
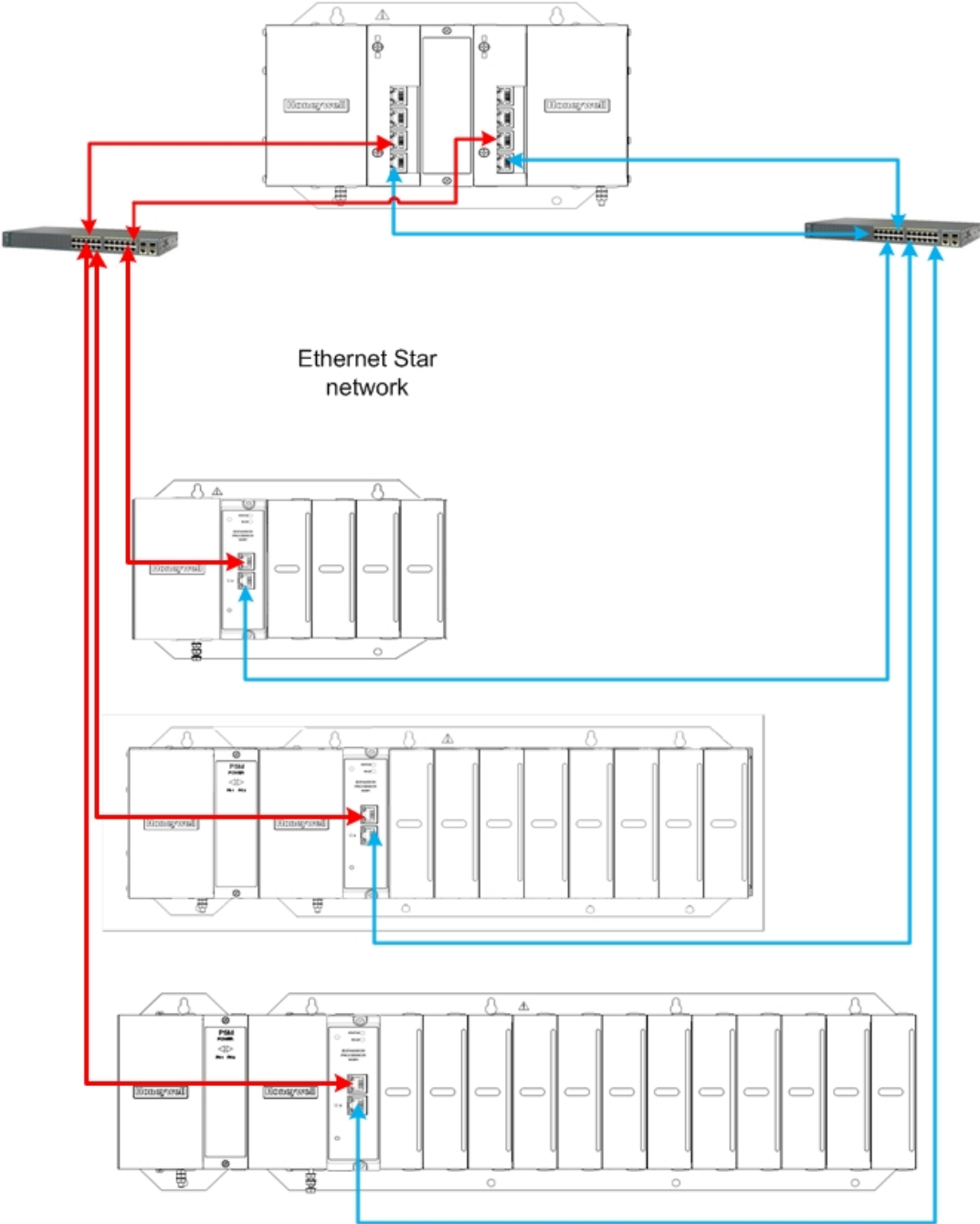
> **CAUTION:** ControlEdge PLC-I/O network is a private network, and the switch used for the interconnection of CPM and EPM must not be connected to any other LAN or WAN. Likewise, no devices or communication traffic other than the ControlEdge PLC components should be connected to the I/O network switch. Failure to comply will cause communication failures on the I/O network causing I/O modules to go in and out of their failsafe settings.

Ring Topology

- ControlEdge PLC supports ring (HSR or DLR) I/O topoloy for I/O communication. The following diagram shows an example of the topology.
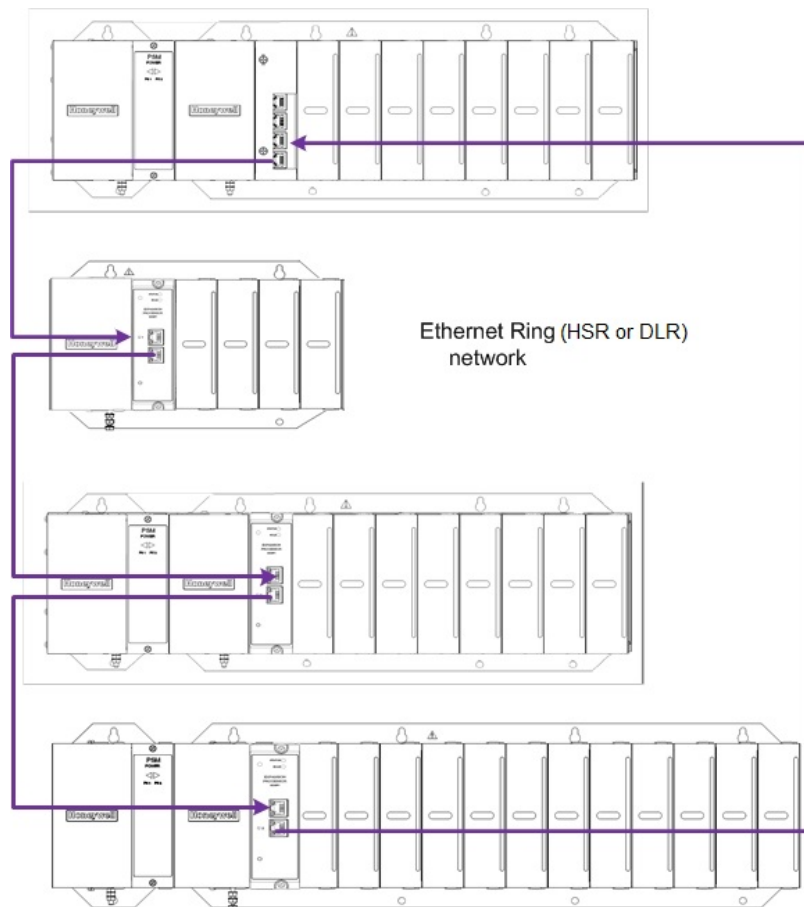
- CPM port 3 (ETH3) must be connected to CPM port 4 (ETH4) or EPM port 2 (ETH2).

- CPM port 4 (ETH4) must be connected to CPM port 3 (ETH3) or EPM port 1 (ETH1).

- EPM port 1 (ETH1) must be connected to EPM port 2 (ETH2) or CPM port 4 (EHT4).

- EPM port 2 (ETH2) must be connected to EPM port 1 (ETH1) or CPM port 3 (EHT3).

For more information, see "I/O Network Topology" in the *ControlEdge 900 Controller Hardware Planning and Installation Guide*.

- ControlEdge RTU supports ring I/O topology for I/O communication. The following diagram shows an example of the topology.

CAT5 Cable

For more information, see "Planning for network topology" in the *ControlEdge 2020 Controller Hardware Planning and Installation Guide*.

Network Security

> **ATTENTION:** Without Secured Communication, the system has a higher security risk between ControlEdge Builder and ControlEdge 2020/900 controller.

Three methods are provided to secure network communication, IPsec, VPN and TLS.

Figure 7–8: Network architecture secured by IPsec

Engineering Workstation

IP address: 10.1.0.30
Subnet Mask: 255.255.255.0

IPsec

ControlEdge Controller

IP address: 10.1.0.10
Subnet Mask: 255.255.255.0

Expansion I/O Modules
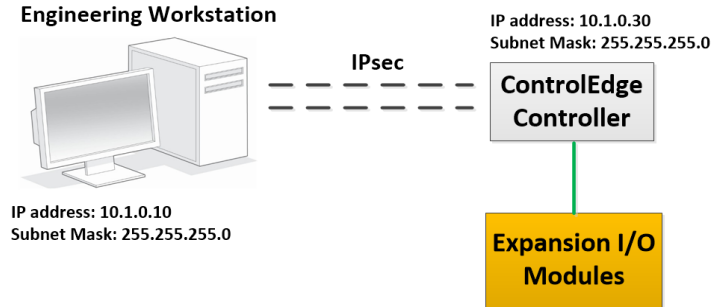
Figure 7–9: Network architecture secured by VPN

Engineering Workstation

Router

VPN

Router

IP address: 10.1.0.30
Subnet Mask: 255.255.255.0

ControlEdge Controller

IP address: 192.167.1.10
Subnet Mask: 255.255.255.0

Expansion I/O Modules
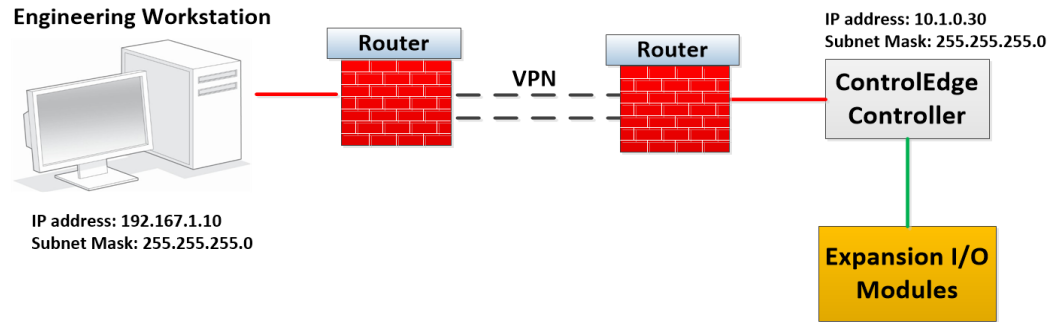
Figure 7–10: Network architecture secured by TLS

Engineering Workstation

Broker (Server)

TLS

IP address: 10.1.0.30
Subnet Mask: 255.255.255.0

ControlEdge Controller

IP address: 192.167.1.10
Subnet Mask: 255.255.255.0

Expansion I/O Modules
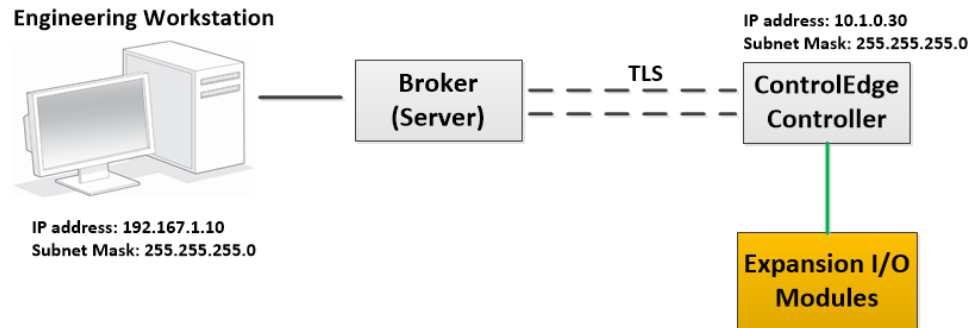
It is highly recommended to configure IPsec to secure network communication. For how to configure, see the "Configuring a secure connection" chapter.

However, ControlEdge 2020/900 controller configured with IPsec cannot communicate with other nodes which are not on the same network segment. In this case, instead of configuring IPsec on the controller, you need to configure a VPN on routers to secure the network communication.

> **ATTENTION:** The location of the routers need to be as close as possible to either end.

ControlEdge 2020/900 controller can communicate with other nodes through MQTT. In this case, instead of configuring IPsec on the controller, you need to configure TLS to secure the network communication.

Remote Location Related

ControlEdge PLC is in a private network and if the network has any failure, the I/O module will go in and out of failsafe settings. It is recommended to provide Bump-in-the-wire (BITW) to enhance the integrity, confidentiality, or reliability of communications with any other LAN or WAN; for example, the third party SCADA or HMI as shown in the following figure.

Figure 7-11: Remote location related
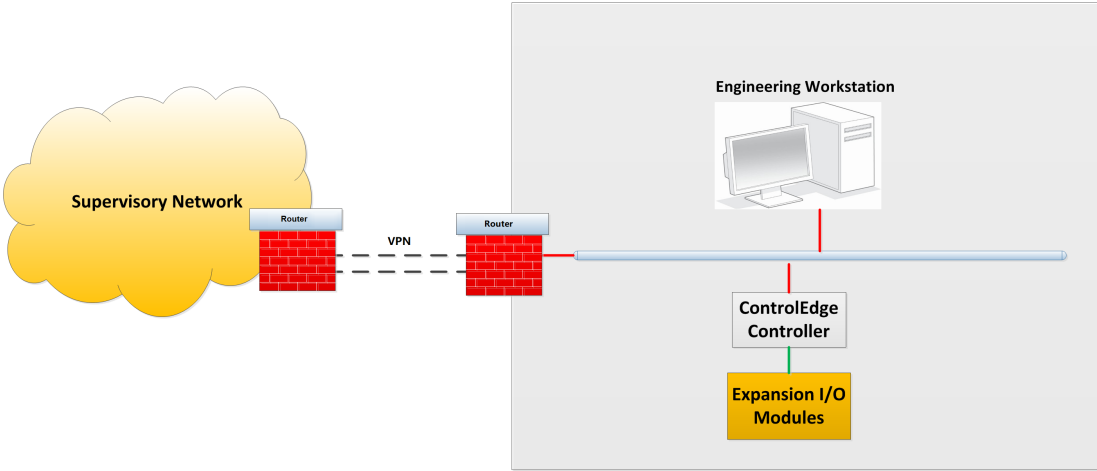
It is not recommended to connect a ControlEdge 2020 controller installed in a remote location to the public network. The communication to ControlEdge 2020 controller installed in a remote location is recommended to be on a private leased line or secured by setting up VPN device external to the ControlEdge RTU.

8
SECURITY FEATURES

See the following security features for the application of ControlEdge 900 controller and ControlEdge 2020 controllers:

Item	Non Redundant ControlEdge 2020 controller		Redundant ControlEdge 2020 controller	ControlEdge 900 controller
	SC-UCMX01	SC-UCMX02	SC-UCNN11	900CP1-0200
Secure Boot	N/A	Yes	Yes	Yes
Mode Switch	N/A	N/A	N/A	Yes
Configurable Ports	Yes	Yes	Yes	Yes
Enable/Disable Protocol	Yes	Yes	Yes	Yes
Logon	Yes	Yes	Yes	Yes
Secured Communication	N/A	Yes	Yes	Yes
Genuine Device Assurance	N/A	Yes	Yes	Yes
Built-in Firewall	N/A	Yes	Yes	Yes

Secure Boot

This feature only applies to ControlEdge 900 controller (900CP1-0200), redundant ControlEdge 2020 controller (SC-UCNN11) and non-redundant ControlEdge 2020 controller (SC-UCMX02 only).

A secure boot feature in CPM and EPM (only apply to ControlEdge PLC) ensures that only a Honeywell released firmware can be loaded and run on them. This feature prevents any unauthorized tampering of firmware.

Honeywell code signing public key is burnt into a metal eFuse inside the processor in all ControlEdge 900 and 2020 controller nodes. This burning step is done in the factory and helps establish a hardware root of trust for verifying signed firmware during start-up.

Secure Boot is a rapidly emerging response to increasingly sophisticated operating systems and root kit attacks. Some of the benefits include:

- Addresses threats that have breached firewalls and reached the core
- Employs hardware and software architectures that insure survival of operating systems
- Used in conjunction with layered defense and detection
- Allows unit to self-reboot (or via command) to an unaltered and clean copy of operating systems upon verification failure.
- Bitstreams are qualified prior to load and execution.

Mode Switch

This feature only applies to ControlEdge 900 controller (900CP1-0200).

The Mode Switch on the front panel of CPM provides a method to restrict certain operations on ControlEdge 900 controller. It is recommended to switch the Mode Switch to RUN position after commissioning to prevent unauthorized operations like firmware upgrade, and configuration download to the running CPM.

For more information, see "CPM Mode Switch" in the *ControlEdge 900 Platform Hardware Planning and Installation Guide*.

Configurable Ports

The ports of Modbus TCP Master, Modbus TCP Slave and HART-IP server are configurable for ControlEdge 2020 controllers (SC-UCMX01, SC-UCMX02 and SC-UCNN11) and ControlEdge 900 controller (900CP1-0200).

For ControlEdge 900 controller specifically, the ports of OPC UA server, OPC UA Client, CDA Responder and DNP3 Outstation are configurable.

For ControlEdge 2020 controllers specifically, the ports of Enron Modbus Slave and DNP3 Outstation are configurable.

Change the default ports of the communication to prevent from external malicious attacks.

Protocols which are required can be enabled to reduce the attack.

Enable/Disable protocol

Disable any protocol that is not in use to avoid malicious attacks.

See section "Configuring ETH1 and ETH2" in *ControlEdge Builder User Guide* for how to bind the protocols.

See section "Configuring Protocols" in *ControlEdge Builder User Guide* for how to configure the protocols.

Logon

To prevent unauthorized access to a running system, ControlEdge Builder supports three user types including Operator, Engineer and Administrator, and this user management controls the operating privileges. A password is required when operating as a specific user type connecting to a running controller. For more information, see "User Privileges" in the *ControlEdge Builder User's Guide*.

It is recommended to change the passwords periodically. It is also recommended to share the passwords with only the minimum required people, who need to perform configuration operations on ControlEdge 900 controller and ControlEdge 2020 controllers. Unauthorized accesses are logged in ControlEdge 900 controller and ControlEdge 2020 controllers. It is recommended to periodically monitor the logs for unauthorized accesses.

The ControlEdge builder shows the login information with Date/Time, IP Address, User Role and Result (Success or Failed) on every login attempt, and the admin user can also see the ten most recent logins in the diagnostic.

If an unauthorized user attempts to access the controller and enters the incorrect password continuously five times, the controller will be locked for 1 minute. After one minute, if the user enters the incorrect password five times, the controller will be locked for 5 minutes. If the user keeps doing the same, the controller lock time goes up by 15 minutes, 30 minutes, and 1 hour. After 25 failed attempts, the controller locks for one hour for every five failed attempts.

The ControlEdge builder allows a maximum of 10 users to access the each controller.

Secured Communication Protocol

This feature only applies to ControlEdge 900 controller (900CP1-0200), redundant ControlEdge 2020 controller (SC-UCNN11) and non-redundant ControlEdge 2020 controller (SC-UCMX02 only).

Internet Protocol Security (IPsec) is used for communication between ControlEdge 900/2020 controller and Experion. It is highly recommended to configure IPsec to secure the communication.

For detailed information on how to configure the IPsec, see Configuring a Secure Connection for more information.

Genuine Device Assurance

This feature only applies to ControlEdge 900 controller (900CP1-0200), redundant ControlEdge 2020 controller (SC-UCNN11) and non-redundant ControlEdge 2020 controller (SC-UCMX02 only).

Genuine Device Assurance ensures that Honeywell released firmware can only be run on the Honeywell released hardware.

Built-in Firewall

This feature only applies to ControlEdge 900 controller (900CP1-0200), redundant ControlEdge 2020 controller (SC-UCNN11) and non-redundant ControlEdge 2020 controller (SC-UCMX02 only).

Firewall is default to be enabled. The user can not turn off the Firewall or can not reconfigure it. Only two uplink Ethernet ports are supported by the Firewall function of the CPM. Any Ethernet Rx data with port number that aren't in the following tables will be filtered out and cannot enter the system. Build-in firewall provides port filtering capability to filter the received data based on the port number.

> **NOTE:** Not all controllers (900CP1-0200, SC-UCNN11, SC-UCMX02) support all protocols listed in the following tables.

- The received data is able to be identified and passed into the system if the port number information embedded is the same as the fixed port number defined in the controller:

Port number	Port number type	Description
41103	Fixed destination port	Builder protocol

Port number	Port number type	Description
24558	Fixed destination port	Discovery protocol
9050	Fixed source port	Discovery protocol
123	Fixed source port	SNTP protocol
123	Fixed destination port	SNTP protocol
68	Fixed destination port	DHCP Client for uplink
67	Fixed source port	DHCP Server for uplink
500	Fixed destination/source port	IPSec for uplink (IKE ports)
4500	Fixed source port	IPSec for uplink(IKE ports)
55601	Fixed destination port	IPSec for uplink (CertMngr cleartext)
55602	Fixed destination port	IPSec for uplink (CertMngr encryption)
80	Fixed source port	IPSec for uplink (SCEP)
20091	Fixed destination/source port	Communication with Wireless I/O
20092	Fixed destination/source port	Communication with Wireless I/O
4091	Fixed destination/source port	Communication with Wireless I/O
44818 (TCP)	Fixed destination/source port	Communication with EtherNet/IP
44818 & 2222 (UDP)	Fixed destination/source port	Communication with EtherNet/IP
34962, 34964, 49152, 49153 and 49154	Fixed destination port	Communication with Profinet

Port number	Port number type	Description
(UDP)		

- The following dynamic ports will be set into configurable registers of the Firewall FPGA Logic module by the Firewall. The Firewall FPGA logic module provides a total of 32 configurable registers with 16 source ports and 16 destination ports.

Port number	Port number type	Description
Based on configuration	Dynamic source port	Modbus TCP Master
Based on configuration	Dynamic destination port	Modbus Slave
Based on configuration	Dynamic source port	OPC UA Client
Based on configuration	Dynamic destination port	OPC UA Server
Based on configuration	Dynamic destination port	HART-IP Server
Based on configuration	Dynamic destination port	Enron Modbus Slave
Based on configuration	Dynamic destination port	DNP Outstation
Based on configuration	Dynamic destination port	CDA Responder
Based on configuration	Dynamic destination port	User Defined Protocol
Based on configuration	Dynamic destination port	MQTT
Based on configuration	Dynamic destination port	IEC60870-5-104 Outstation

See Close all Ethernet ports into controller except: for more information.

- PING or other internet accesses are blocked.

> **ATTENTION:** If Wireless I/O is enabled on a controller, PING is automatically enabled.

- ARP rate limit is fixed at 1Mbit ARP rate.

9

CONFIGURING A SECURE CONNECTION

To support secure communications, network layer security provided by IPsec policies will be employed. To achieve this, all the nodes need a certificate issued by a certification authority (CA) trusted by all.

This chapter explains how to create a standalone root CA which can be used to issue certificates for Experion HS Servers as an example and other Windows nodes, as well as for ControlEdge 900 controller (900CP1-0200), redundant ControlEdge 2020 controller (SC-UCNN11) and non-redundant ControlEdge 2020 controller (SC-UCMX02 only). It also explains how to request certificates from this CA for three different purposes:

- IPsec – for use with secure communications between Experion, and any other Windows nodes that communicate with ControlEdge 900/2020 controllers.
- Certificate Manager Configuration Console (CMCC) – to facilitate a secure connection when configuring ControlEdge 900/2020 controllers.

> **NOTE:** CMCC is suggested to be operated on Windows 10 or Windows Server 2016.

- TLS – for use by the CA Server to ensure its HTTPS connection is secure for handling certificate enrolment for ControlEdge 900/2020 controllers.

In addition, this chapter will explain how to install the certificate on each Experion node and then how to enable IPsec policy to secure communications between Experion and the ControlEdge 900/2020 controllers.

About this chapter

You need a single CA Server for your system (this CA Server can be shared by multiple systems), so you need to install and configure

your CA Server only once for each system (or only once for multiple systems). After that you need to use CMCC to configure your ControlEdge PLC/RTUs, and then configure IPsec on the Windows nodes, this will generate the required certificates. A rough workflow through this chapter then would be:

Topics	Description	Reference
Planning deployment of IPsec	Overview of secured communications planning and topology	See Overview of an IPsec deployment for more information.
Configuring CA Server	Instructions on setting up CA Server	See Creating the Certificate Authority for more information.
Creating a certificate	Instructions to create and install a certificate. **TIP:** This section is used indirectly via directions from the "Install and Configure CMCC" and "Configuring and enable Windows node with IPsec" sections.	See Creating a certificate for a Windows node for more information.
Install and Configure CMCC	Steps to setup the Certificate Manager Configuration Console for PLC/RTU	See Installing Certificate Manager Configuration Console for more information.
Configuring PLC with IPsec	Instructions on using CMCC to configure IPsec on PLC	See Setup certificates and IPsec policy in PLC/RTU for more information.
Configuring and enable Windows node with IPsec	Instructions on using CMCC to configure IPsec on Windows node	See Enable IPsec policy on PCs for more information.
Enable IPsec on PLC	Steps to enable IPsec on PLC	SeeEnable IPsec policy rules in the PLC/RTU for more information.
Disable IPsec on Windows nodes	Instructions to turn off IPsec on any Windows node	See Disable IPsec policy on PCs for more

Topics	Description	Reference
		information.
Disable IPsec on PLC	Instructions to turn off IPsec on PLC	See Disable IPsec policy rules in the PLC/RTU for more information.
Backup and restore of CA	Details on backup and restore the CA node	See Backup and Restore of CA for more information.
Renewal of certificates	Details to renew the certificates once it is expired.	See Renewal and revocation of certificates for more information.
Troubleshooting		See Troubleshooting for more information.

This chapter takes Microsoft Windows 10 OS as example. When configuring Windows Server 2016 or previous Windows OS systems, the user interface may be different.

Security Communication Planning

Secure communications is required when two entities are communicating and do not want a third party to listen in (i.e. avoid man in the middle attacks). For that they need to communicate in a way not susceptible to eavesdropping or interception. Honeywell ControlEdge PLC/RTU secures its communications using IPsec and X.509 standards compliant certificates.

This chapter is the first user assistance that all customers, system integrators and planners need to read before installation, configuration and setup of Secure Communications for a ControlEdge PLC/RTU or a system including a ControlEdge PLC/RTU to deploy Honeywell secure communications.

Secure Communications Planning

As a first step to using Honeywell secure communications, is to define the nodes involved and the level of secure communications desired. The output of this planning session is a systems communication diagram. The figure below is an illustrative example of a systems communication diagram for ControlEdge PLC and ControlEdge RTU.

Figure 9-1: System Communication Diagram
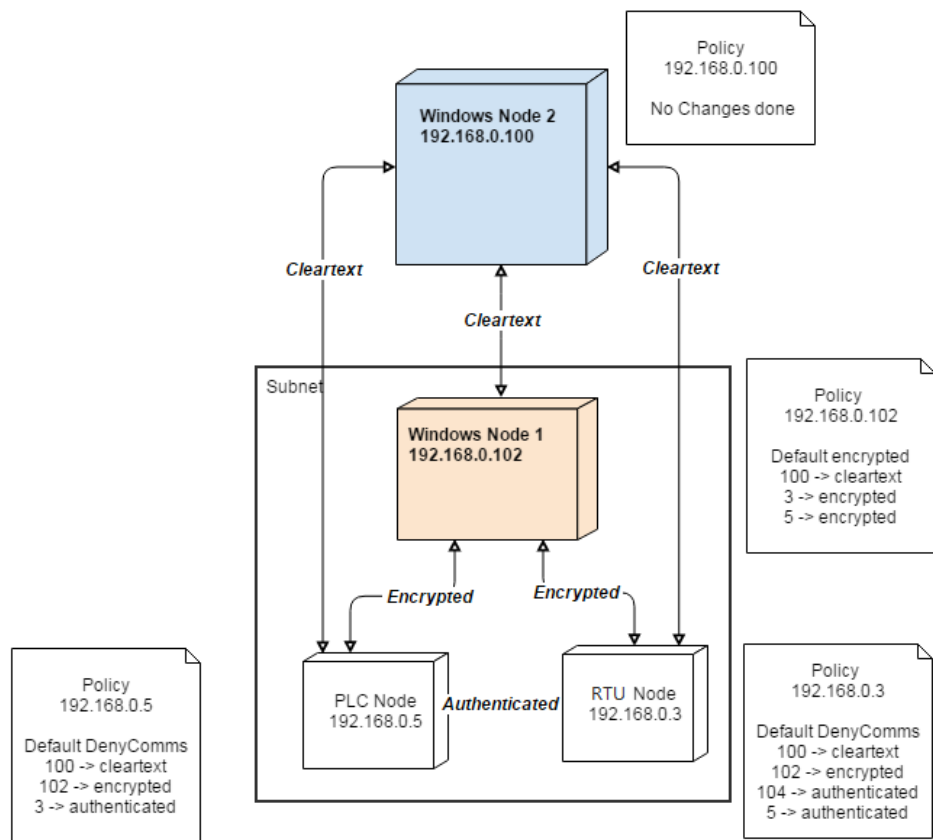
There are two windows nodes, one ControlEdge PLC and one ControlEdge RTU deployed at this site. Windows node 1 is participating with the ControlEdge PLC and ControlEdge RTU (at 192.168.0.3 and 192.168.0.5) in Secure Communications. Windows node 2 is excluded due to its network placement or interoperability

reasons from this setup. In Addition, the diagram depicts the level of secure communication expected (annotated as Cleartext, Authenticated and Encrypted). See the following chapters for further technical information on implementation of Honeywell secure communications solution.

Configuration and Setup Steps

After completion of a systems communication diagram, the next step is to complete installation of Secure Communications components.

To configure and enable the Secure Communications :

1. Install and configure a Certificate Authority (one time operation for an install) – See Creating the Certificate Authority for more information.

2. Install IPSEC configuration application and prepare it for use with PLC/RTU - See Installing Certificate Manager Configuration Console for more information.

3. Prepare the Windows node and PLC/RTU for IPsec configuration – See Setup certificates and IPsec policy in PLC/RTU for more information.

4. Configure IPsec policies (access control based on IP addresses) – See Setup certificates and IPsec policy in PLC/RTU for more information.

5. Configure Windows IPSEC (access control based on IP addresses) – See Enable IPsec policy on PCs for more information.

6. Enable IPsec on PLC/RTU and Windows nodes – See Enable IPsec policy rules in the PLC/RTU for more information.

Advanced Technical Information

This section will provide advanced technical information about the underlying technology to ensure Secure Communications for ControlEdge PLC/RTU.

Secure communication protocols provide a way to authenticate clients and servers and protect the integrity and confidentiality of communication between clients and servers. The table below lists the secure communication technologies for different protocols on different platforms.

Table 9-1: Securing Protocol Communication between nodes

Protocol	Secure Communications Technology
OPC UA Client/Server (Windows)	IPsec
ModBus Client/Server (Windows)	IPsec
Builder Communication	IPsec
HART-IP	IPsec
DNP3 Master/Outstation (Windows)	IPsec
SNTP	No secure Communication
Certificate Authority	HTTP
IPSEC Configuration App	TLS
MQTT	TLS
IEC60870-5-104	TLS
OPC UA Client/Server (Non-Windows)	See *Secure Communications with Non-Windows Nodes* section for more information
Modbus Client/Server (Non-Windows)	See *Secure Communications with Non-Windows Nodes* section for more information
DNP3 Master/Outstation (Non-Windows)	See *Secure Communications with Non-Windows Nodes* section for more information

Certificate Management

Trust is established between nodes by presenting and verifying X.509 (v3) certificates. Below are the characteristics of these certificates as they are distributed:

- ■ ECDSA P-256 signatures
- ■ Use of standard protocol SCEP (Simple Certificate Enrollment Protocol) for distribution, renewal and CRL retrieval capabilities

Secure Communications using IPsec

IPsec is the selected method for communication between nodes within the same subnet. And IKE protocol defined under IPsec, is used during initial negotiation to authenticate a partner endpoint and agree upon algorithms for subsequent attempts to secure communication. Below are the default security constructs and algorithms for all nodes using IPsec:

- Use of main mode IKEv1 and IKEv2 when supported by peer
- SHA-256 message authentication
- AES-CBC 128-bit encryption
- ECDH P-256 Key algorithm

Subsequent to establishing trust, IPsec security constructs selected for securing communication are :

- Deny all communication unless explicitly granted
- ESP mode only, no AH AES-GCM 128 bit message authentication, NULL encryption
- AES-GCM 128 bit message authentication and encryption

The above security constructs apply to a "security area", a structural grouping of nodes to establish Secure Communications. The policies below are options for all nodes that form a security area:

- No Communication: to prevent explicit communication
- Cleartext Communication: no security measures intended for interoperability scenarios
- Authentication (Message Integrity) only: for intra-zone node communication where confidentiality is not a concern
- Authentication and Encryption (Message Integrity and Data Confidentiality): Full encryption that helps preserve confidentiality

Secure Commuincations Using TLS

TLS is to secure communications for the IPsec configuration tool. In this scenario, version 1.2 or higher is primarily selected with the security constructs and characteristics below:

- SHA256/SHA384 hashing
- ECDHE (Forward secrecy, Ephemeral DH keys)

- ■ AES-GCM 128 bit encryption

TLS is also used to secure MQTT communication. It is strongly recommended to enable TLS security for MQTT connections.

TLS is also self downgrade compatibility with the previous version.

Further more, the CA certificate of external devices, which will be used to authenticate the access from particular external device should be configured in "Trust Chain". You should get the CA certificate from your vendor first, and then download this certificate file into the controller.

To enable TLS and download CA certificate to the controller:

1. Under **I/O and Communications** tab, click **Configure Protocols** > **MQTT**.
2. Select the connection from the left panel or click **Add Connection** to add a new connection.
3. Check **Enable TLS** and finish other configurations.
4. Click **Save**.
5. Under **I/O and Communications** tab, click **Configure Certificate** > **Trust Chain**.
6. Click **Browse** icon in Trust Chain field.
7. Select the certificate you want to download, and click **Open**.
8. Click **Download** to download the certificate of CA for external device/node to the controller.
9. Click **Save**.

> **NOTE:** For configuring MQTT and certificates, see *ControlEdge Builder User's Guide*.

Secure Communications with Non-Windows Nodes

Currently, if the Non-Windows node supports the security algorithm described in above Section Secure Communications using IPsec, the node can apply to Honeywell defined Secure Communications. For nodes that do not support the above security algorithms, a cleartext interoperability compliant policy needs to be defined.

Obtaining and installing the software

The **Secured Communications for ControlEdge PLC and Experion HS** package must be downloaded and installed.

To download the package

1. In a web browser, type the following URL.

   https://process.honeywell.com.

2. Click **Sign In** in the top-right corner of the page. Sign in options appears.

3. If you are a new user, create a new account at this website. Click **Create an Account**, and follow the on-screen instructions.

4. If you are an existing user, Click **SIGN IN TO MYHPS** and type your **user name** and **password**, and click **SIGN IN**.

   After successful sign in, your account name appears in the top-right of the page.

5. Click **Support>Product Documents & Downloads**, product documents & downloads page appears.

6. In the Search box, enter **Secured Communications for ControlEdge PLC and Experion HS**, and click the Search icon. The search results page appears with all the search results.

7. In the left pane, use the **Search Result Filters** to further filter the document, security update, or antivirus notification. For example, if you are locating a Software.

   a. Under **DOCUMENT TYPE**, click **Software Download.**

   b. Under **PRODUCT**, click **Experion HS**.

8. Click to download the **Secured Communications for ControlEdge PLC and Experion HS** document.

9. Open the document, and click the **Download Software** link to download the package.

   Secured Communications for ControlEdge PLC and Experion HS.zip file downloaded.

To install the package

1. Extract the package.

2. Run the file "Secured Communications for ControlEdge PLC and Experion HS.msi" with default settings to install the necessary files.

   The files are installed to `Software Files\Honeywell\Experion PKS\CertAuth`, where `Software Files` is potentially a custom install path (CIP) for Experion programs.

   Default location is `C:\Program Files (x86)\Honeywell\Experion PKS\CertAuth\`. For the rest of this document, `C:\Program Files (x86)` location should be substituted with the correct CIP path location, if a CIP install was performed.

Overview of an IPsec deployment

Before starting to configure IPsec, you should identify the IP addresses of all NICs in PCs (especially those to communicate to ControlEdge 900/2020 controllers and other devices) as well as the IP addresses of all Ethernet ports on the ControlEdge 900/2020 controllers and other devices used to communicate with PCs. Keep a list of all these IP addresses for reference.

As some nodes will require different IPsec policies, sort your IP addresses and nodes list into four sections:

- PCs not to use IPsec (e.g. the CA server, RDP Clients)
- PCs to use IPsec to communicate with the ControlEdge PLC/RTU and other PCs using IPsec
- Devices to use IPsec (e.g. ControlEdge PLCs/RTUs)
- Devices not to use IPsec (e.g. third party PLCs)

Assume a sample system below:

Figure 9-2: A sample system
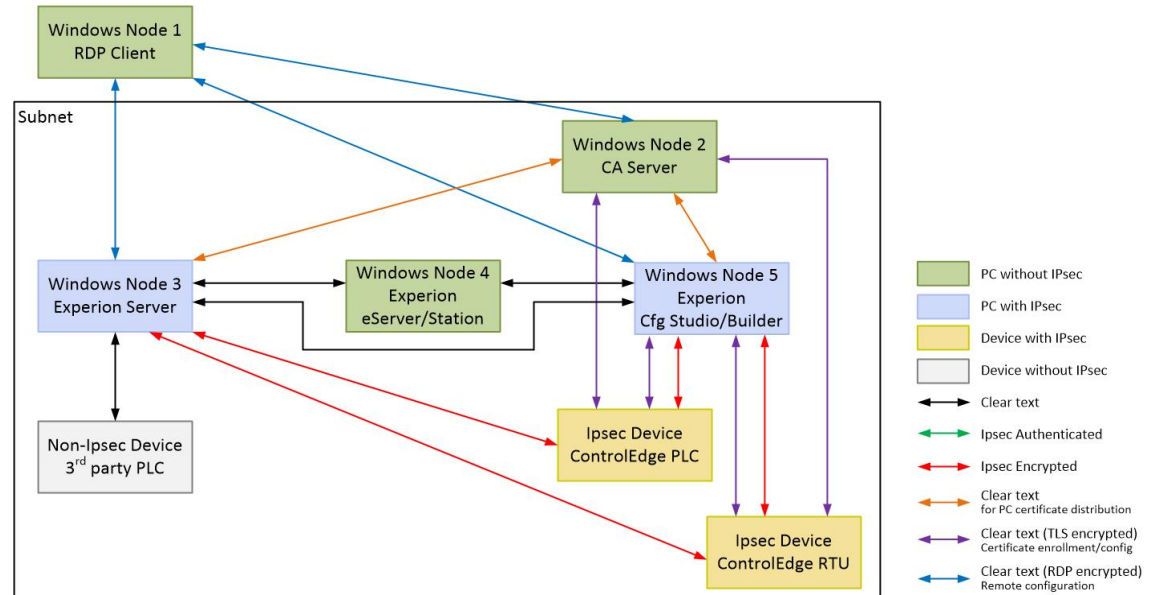
From this diagram, IPsec encryption is only used between Windows nodes and ControlEdge 900/2020 controllers.

> **ATTENTION:** If a controller uses a DNP3 master as a time source, only the cleartext communication is allowed between the controller and the DNP3 master.

Cleartext communications should be permitted:

1. Between RDP Client and all Windows nodes in the control system subnet for RDP connections only, as RDP traffic is already encrypted.

2. Between Experion and the 3rd party PLC as this device does not support any other forms of communications.

3. Between the CA Server and the ControlEdge 900/2020 controller, as this communication is via an HTTPS connection.

4. Between the ControlEdge Builder node with the CMCC tool to ControlEdge 900/2020 controller, as this connection utilises a TLS encrypted socket for the bulk of the communication.

5. Between the CA Server and the Windows nodes in the control system, as the PFX certificate files are password protected.

6. Between all Windows nodes in the control system subnet.

IPsec encrypted communications are:

1. Between the Windows node running Experion and ControlEdge 900/2020 controller.

2. Between the Windows node running the ControlEdge Builder and ControlEdge 900/2020 controller.

   From this system the nodes can be split as below:

   - PCs without IPsec

     ○ RDP Client (Windows Node 1)
     ○ CA Server (Windows Node 2)
     ○ Experion eServer or Station (Windows Node 4)
   - PCs with IPsec

     ○ Experion Server (Windows Node 3)
     ○ Experion Configuration Studio and ControlEdge Builder (Windows Node 5)
   - Device with IPsec

     ○ ControlEdge 900/2020 controller
   - Device without IPsec

     ○ 3rd party PLC

This chapter explains configuring a CA Server, issuing certificates for PCs, configuring IPsec on PCs and enrolling and configuring IPsec on ControlEdge 900/2020 controller.

Creating the Certificate Authority

The Certification Authority Server needs to be:

- Running Windows Server 2016 – Standard
- Able to receive traffic on port 80/tcp and port 443/tcp from the PLC/RTU without going through any Network Address Translation (NAT) layers. Access to the CA Server may work through NAT but it is not a supported topology.

> **CAUTION:** The Certificate Authority should be restricted from physical access within the network. Only authorized individuals should be allowed access for operations on this node.

This PC should not be used for any other purpose. Windows Server node running Windows Server 2016, and the screenshots and PowerShell scripts described in this chapter are taking Windows Server 2016 as an example.

These instructions create a standalone root Certificate Authority (CA) that can work in both a domain and workgroup environment. It will also configure the CA to support Network Device Enrolment Scheme (NDES) which is Microsoft's implementation of Simple Certificate Enrolment Protocol (SCEP) which allows network devices (such as the ControlEdge PLC/RTU) to enrol for a certificate.

This CA needs to be on the same network with the PLC/RTU and PC, and the CA Server needs to be always available, or at least it should be available for initial enrolment with IPsec for all PCs and PLCs/RTUs. If the CA Server is not available on an ongoing basis, it impacts on the ability for the PCs and PLCs/RTUs to receive updated Certificate Revocation Lists and for the PLC/RTU to auto-renew its certificate.

Take ControlEdge PLC as an example:

> **CAUTION:** Perform all installation and configuration instructions on the CA Server under the local Administrator account.

1. From the Experion HS R500 media, install the MSI file Secured Communications for ControlEdge PLC/RTU and Experion HS.msi and do not change the default setting.
2. From the Start menu, start an Administrative PowerShell command and open the Windows PowerShell folder then right-

click **Windows PowerShell** and select **Run as Administrator** .
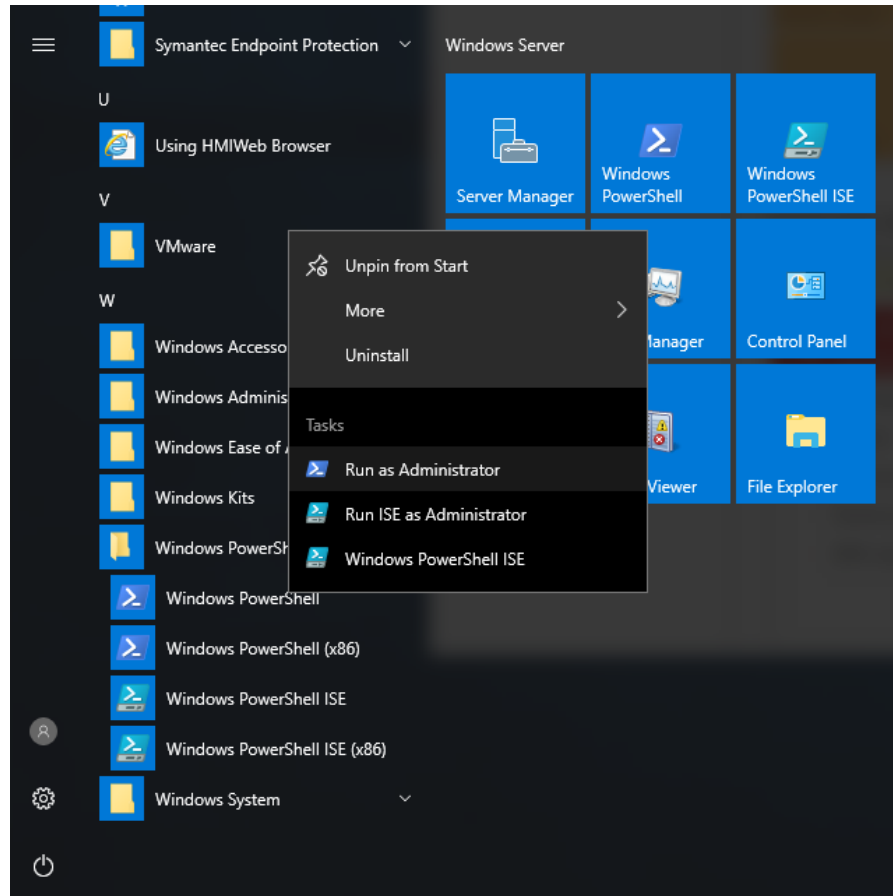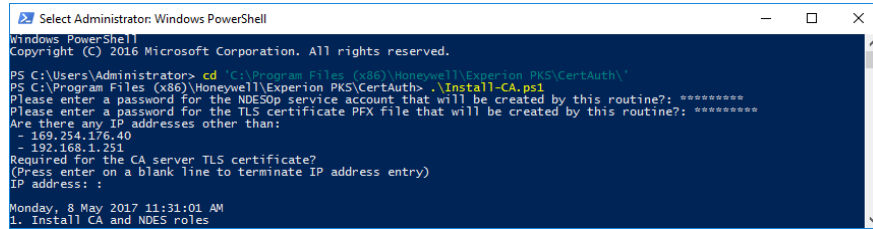
3. Navigate to `C:\Program Files (x86)\Honeywell\Experion PKS\CertAuth` folder with the following command:

    cd 'C:\Program Files (x86)\Honeywell\Experion PKS\CertAuth\'
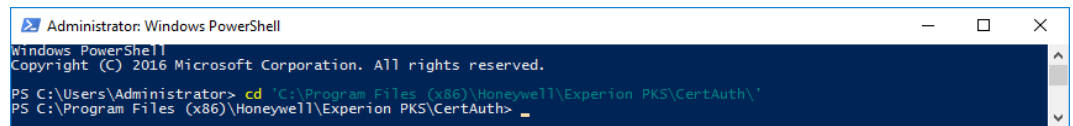
4. Run the following commands to installing and configuring the CA: `.\Install-CA.ps1`. When prompted,

    1. Enter a password for the NDESop account,
       The NDESop is a service account used to support generation of one time passwords (OTP) for enrollment of the PLC/RTU into IPsec.

    2. Enter a password to protect the TLS certificate generated by this script.

3. Enter the other IP addresses that the CA Server machine uses and not display. Press Enter on a blank entry when complete, or at first blank entry if no more to add.

All the Windows components will then be installed and configured, and it takes five to ten minutes.

The installation and configuration of the CA Server is complete.

Creating a certificate for a Windows node
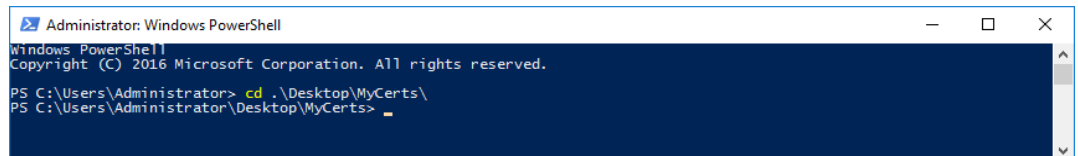
This section describes how to make different types of certificates. See Installing Certificate Manager Configuration Console and Enable IPsec policy on PCs for more information. You should follow the instructions to generate appropriate certificates.

To create a certificate, you need to generate a key pair, create a certificate signing request (CSR) and then make the CA sign the CSR. The key pair and CSR can be created either on the target Windows node machine or on the CA. For creating on the target machine, you need to manually transfer the CSR to the CA server. in this way, you can create the key pair and CSR on the CA air gapped from the target machines or in a different location.

> **TIP:** These instructions can be used to make the certificate for IPsec for Windows nodes that connect to the PLC/RTU, and to make the Certificate Manager Configuration Console (CMCC) and GetChallenge IIS web page TLS certificate. The TLS certificate for the CA GetChallenge web page is created automatically as part of the .\Install-CA.ps1 PowerShell script. See Creating the Certificate Authority for more information.
> The procedure for creating three certificate types (IPsec, CMCC & TLS) are almost the same, where they differ the steps below will clearly state this.

Creating a certificate

1. Make sure the PowerShell script `CACertificateRequest.ps1` is at C:\Program Files (x86)\Honeywell\Experion PKS\CertAuth (or the equivalent CIP location)

2. On the CA Server, start an Administrative PowerShell command prompt (See Creating the Certificate Authority for more information. See steps 1 and 2 for details.) or continue to use previously open prompt.

3. Navigate to a directory that you wish to store your certificates, for example `C:\Users\Administrator\Desktop\MyCerts`

```
Administrator: Windows PowerShell                                    —  □  ×

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> cd .\Desktop\MyCerts\
PS C:\Users\Administrator\Desktop\MyCerts> _
```

4. Run the PowerShell script as follows:
   ```
   & 'C:\Program Files (x86)\Honeywell\Experion
   PKS\CertAuth\CACertificateRequest.ps1'
   ```
   And answer the prompts as follows:
   CertificateType: the type of certificate and should be one of CMCC, TLS or IPsec
   Computer: the name of the computer the certificate will be installed on (for example the Experion HS Server...)
   Organization: the name of the company that owns this system.
   Country: the two letter country code where this system is installed.
   IPaddrs[n]: the IP address of the computer. If the computer has multiple IP addresses, type each and press Enter. Up to 10 IP addresses can be entered. Once complete, press Enter on a blank line.
   PFXPassword: the password to be used to protect the private key

in the output PFX file.

5. Once the script is complete, it displays the name and location of where it stores the output PFX file which contains the certificate and private key.

This file is copied to the target machine. The following section explains how to install the certificate at the target machine.

Importing certificate and private key on target machine

The process for importing certificates is almost the same for all three certificate types. However the store location and store do vary by certificate types.

Table 9-2: Store location for different certificate types

Certificate type	Store Location	Store	Reason	What nodes?
TLS	Local Machine	WebHosting (Web Hosting)	Used by IIS for the GetChallenge web page	CA Server
CMCC	Current User	My (Personal)	Used by the CMCC command line tool	Node used to setup IPsec on PLC/RTU typically an Experion Server
IPsec	Local Machine	My (Personal)	Used by Windows for IPsec	• Experion Servers connecting to PLC/RTU

Certificate type	Store Location	Store	Reason	What nodes?
				• Nodes using ControlEdge Builder to configure PLC/RTU

The instructions in this section explicitly explains what needs to be done for each certificate type as this information varies.

1. Locate the certificate PFX file in Windows Explorer (it should have been copied to this node at the end of last section) and double-click it.
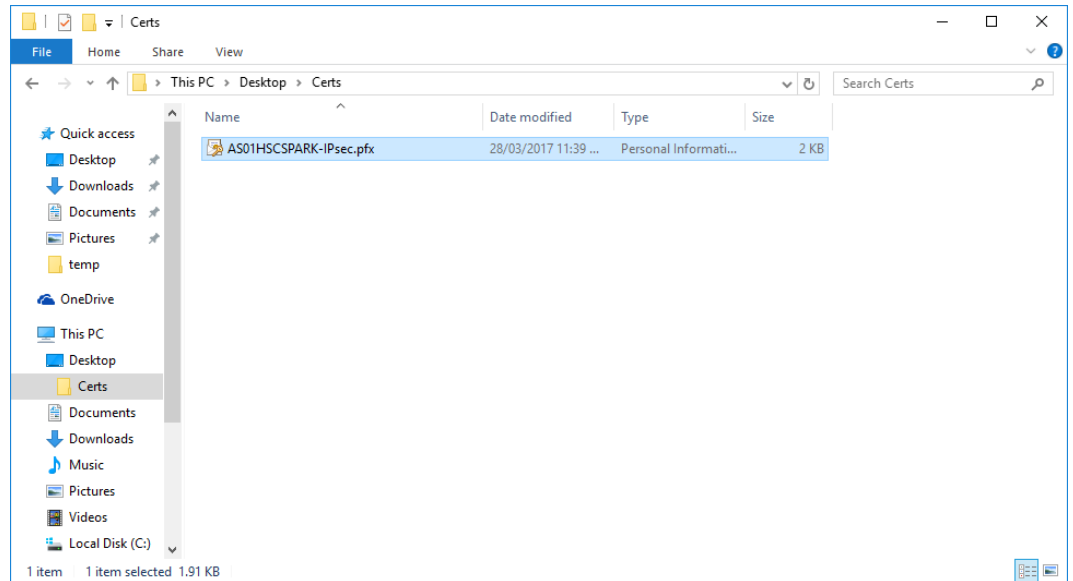
2. Select the certificate store location. This varies by certificate types.

    • For IPsec and TLS certificates only:

    At the **Welcome to the Certificate Import Wizard**, under **Store Location** select **Local Machine** and click **Next**.
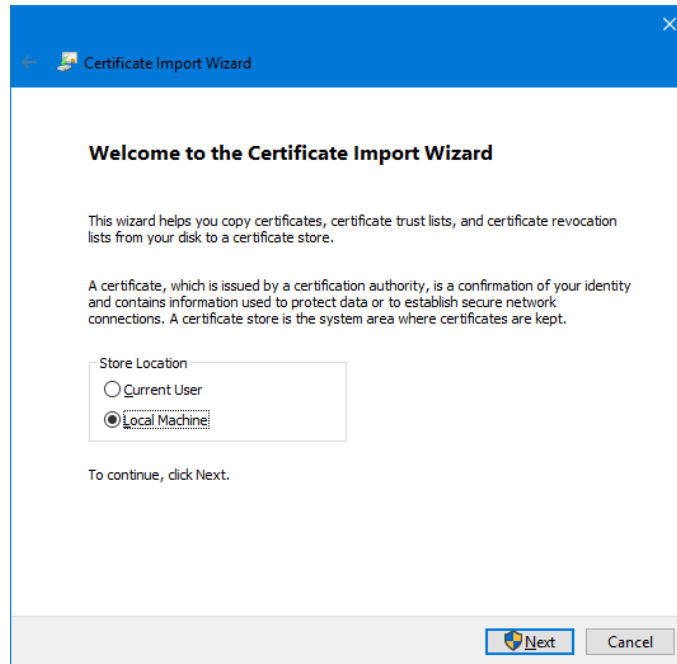
- For CMCC certificate types only:

  At the **Welcome to the Certificate Import Wizard** , under **Store Location** select **Current User** and click **Next**.
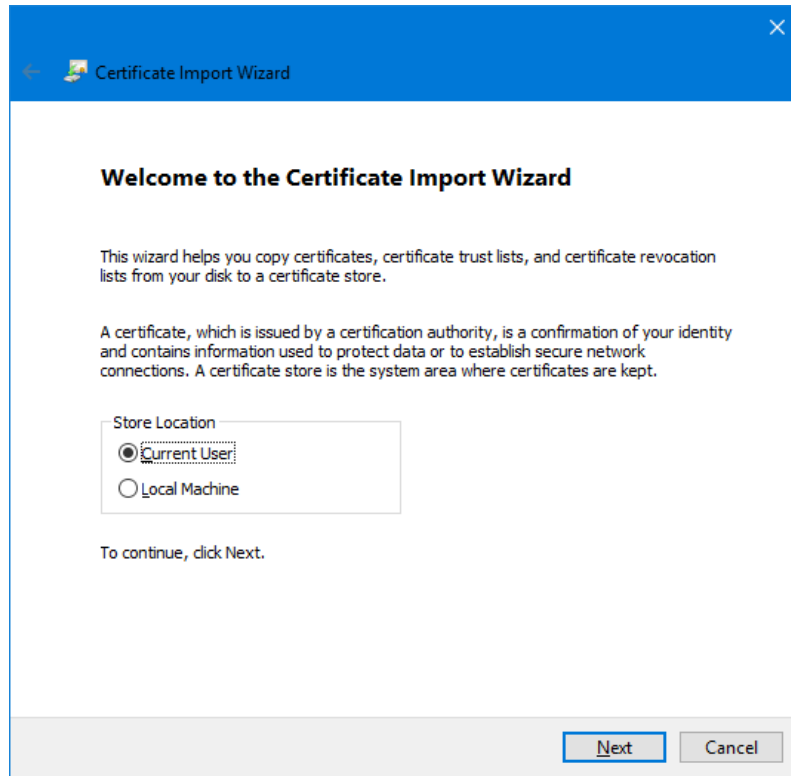
3. If the **User Account Control** dialoge displays, click **Yes** or provide the credentials.
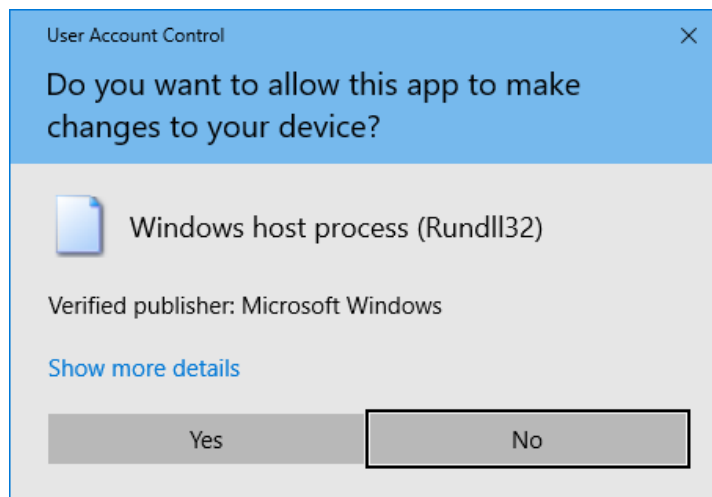
4. Under **File to Import**, specify the file in **File name** and click **Next**.
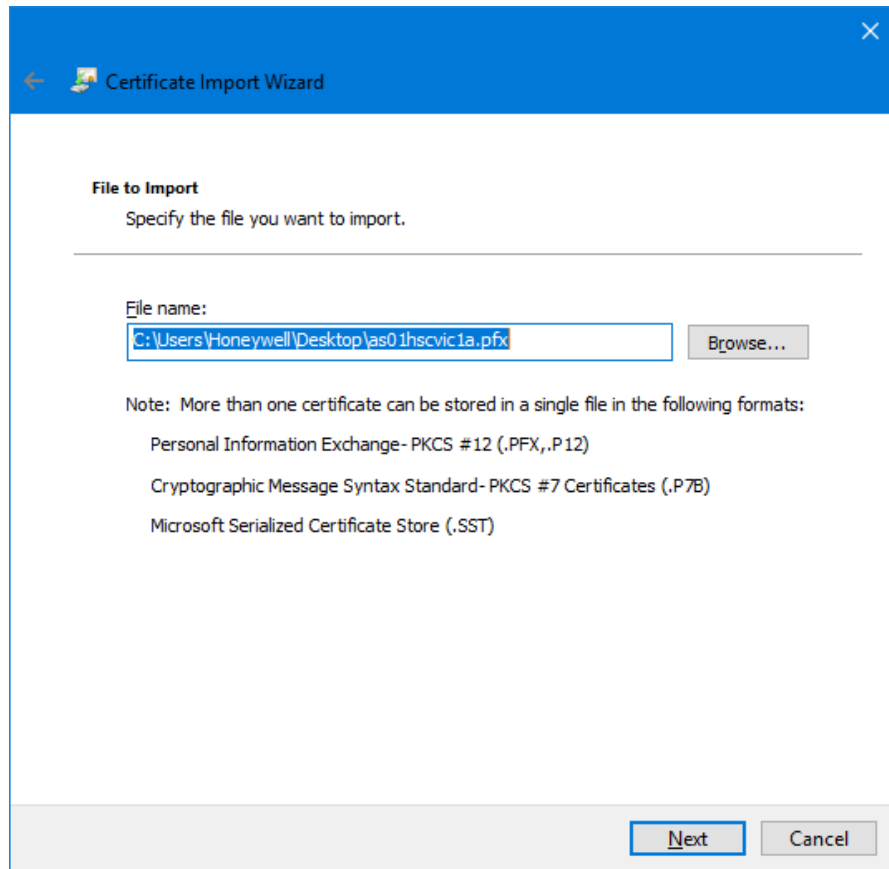
5. Under **Private key protection**, enter the password you set when exporting the certificate. Ensure **Mark the key as exportable** option is de-selected and **Include all extended properties** is selected and

click **Next**.
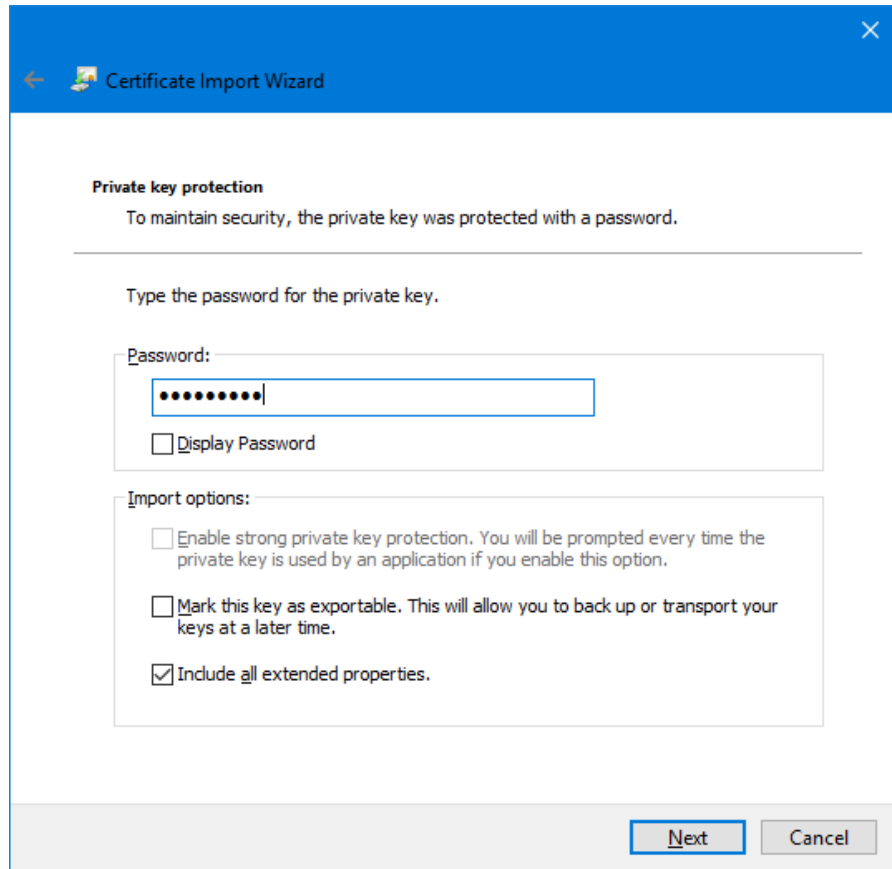
6. The correct Certificate Store needs to be chosen for the certificate type. This varies based on Certificate Type:

- For IPsec or CMCC certificate types only:

  Under **Certificate Store**, select **Automatically select the certificate store based on the type of certificate** and click **Next**.
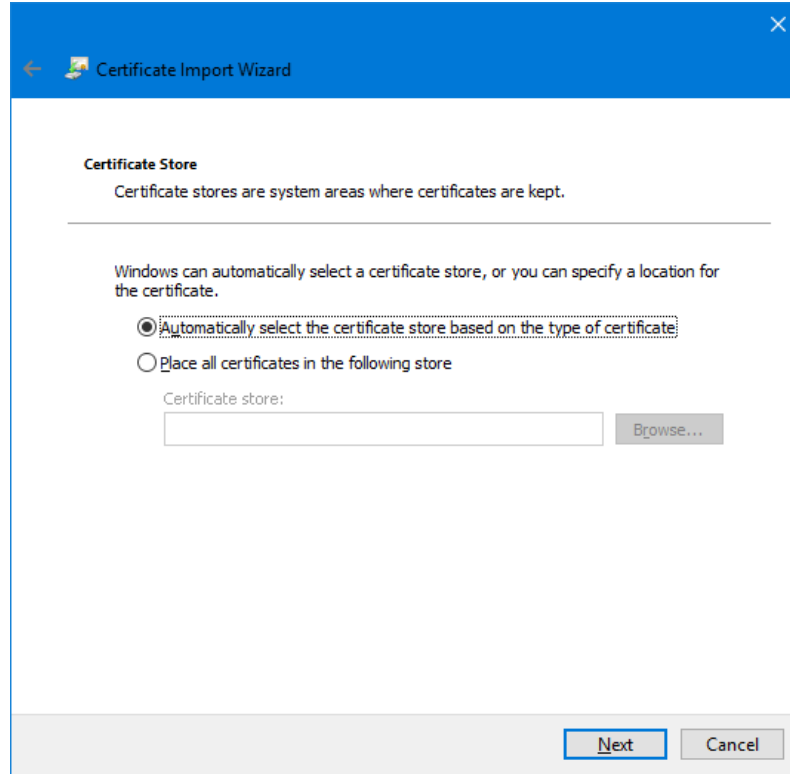
- For the TLS certificate type only:
  At **Certificate Store** dialog, select **Place all certificates in the following store**. Click **Browse...** to specify **Web Hosting** in **Select Certificat Store** window and click **OK**. Then click **Next** back at **Certificate Store** dialog.
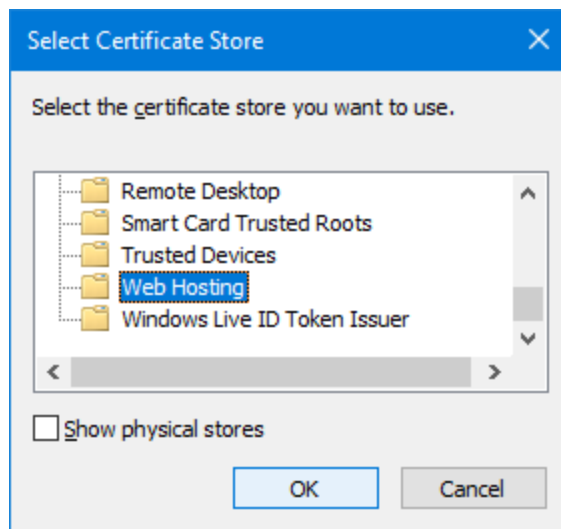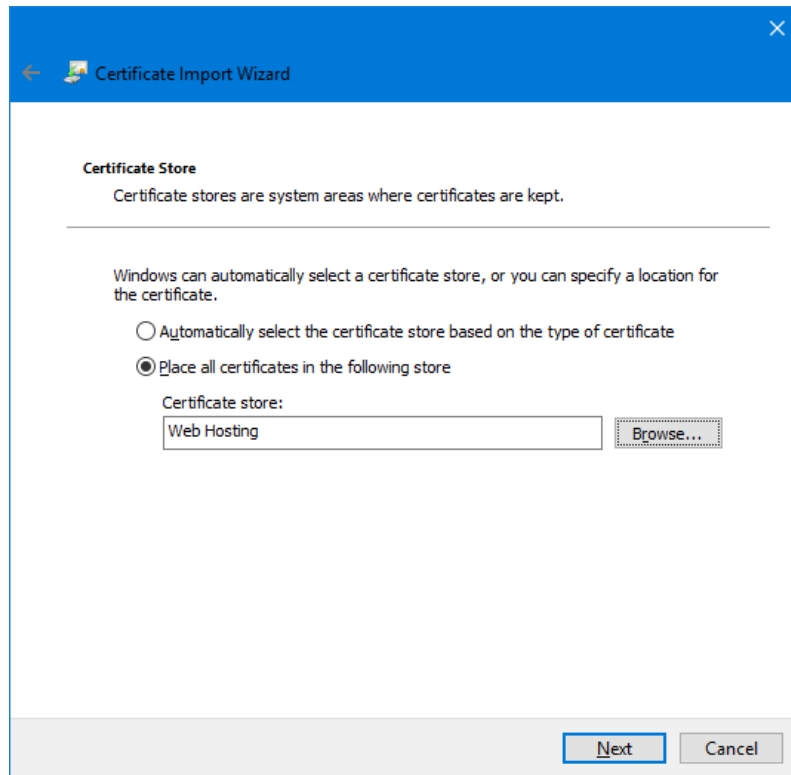
7. At the **Completing the Certificate Import Wizard** dialog, click **Finish** .
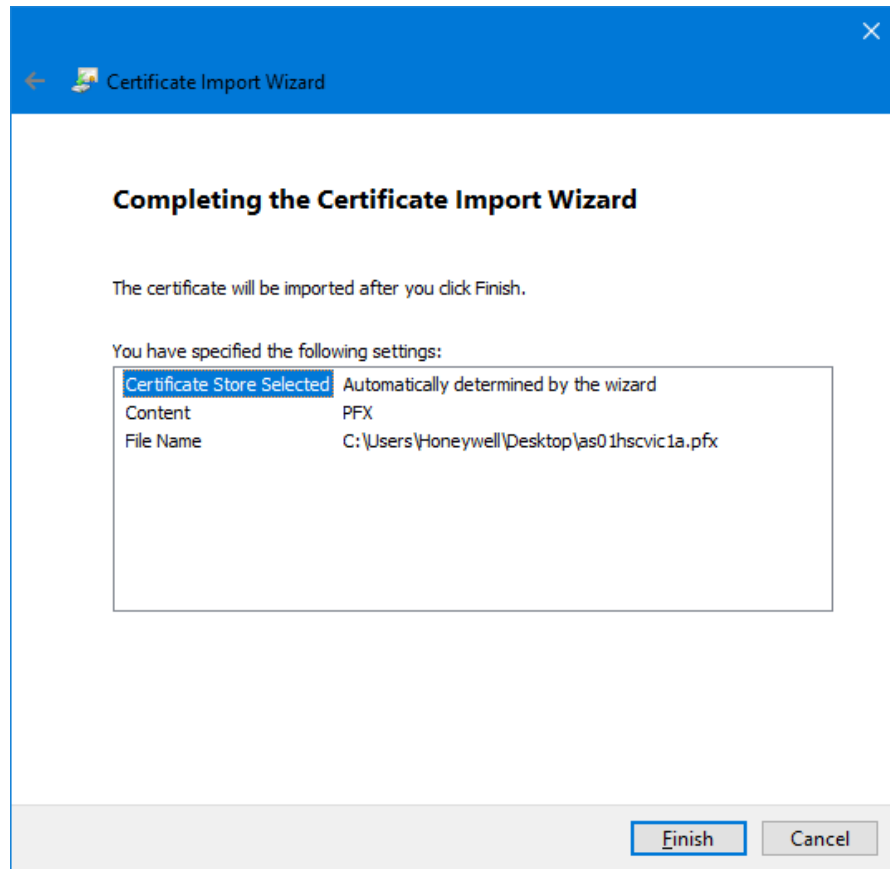
8. After the certificate import completes, a dialog displays to confirm that the import was successful and click **OK**.
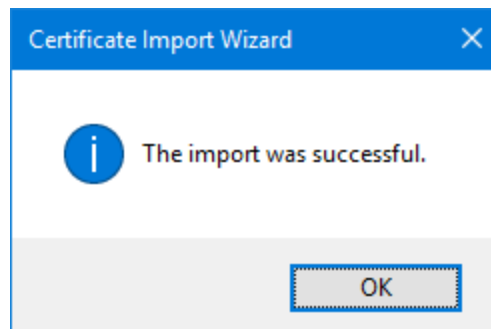
With the certificate installed, the CA is installed as a Trusted Root CA. This certificate and others issued by the CA are accepted by this machine without that the CA to be online.

Configure ControlEdge PLC/RTU for use with IPsec

This section explains how to configure IPsec onto the PLC/RTU, but not enable it. Instructions to enable it should be undertaken when all PCs, devices and PLCs/RTUs have been configured for IPsec, and are all ready to be enabled. See Enable IPsec policy rules in the PLC/RTU for more information.

Installing Certificate Manager Configuration Console

Take ControlEdge PLC as an example:

1. From the Experion HS R500 media, install the MSI file Secured Communications for ControlEdge PLC/RTU and Experion HS.msi and do not change the default setting.

2. Go to the machine to use for configuring certificates to the PLC/RTU, and note this machine should not be the CA Server. Then open Windows Explorer on this machine and in the root directory of `C:\` make a new folder named CertMgmt and then navigate into this folder.
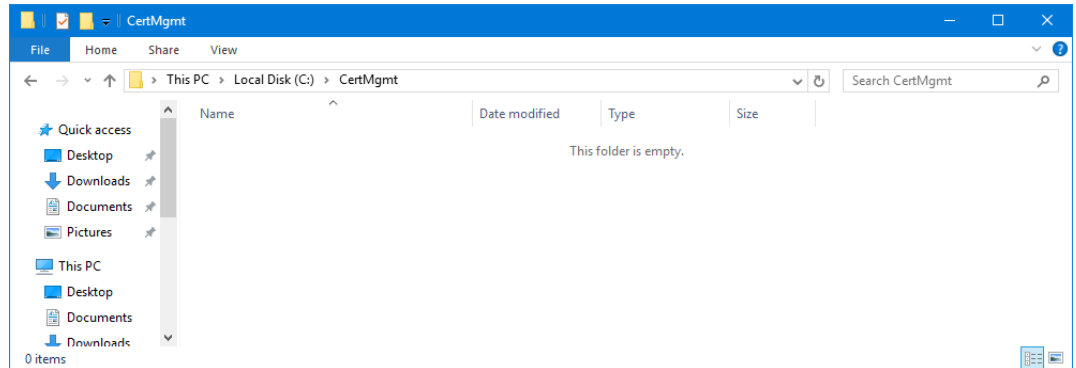
3. Copy the contents of CertManagerConfigConsole.zip stored in `C:\Program Files (x86)\Honeywell\Experion PKS\CertAuth` into this folder so that there is a CertManagerConfigConsole folder (or similar) in `C:\CertMgmt` folder.
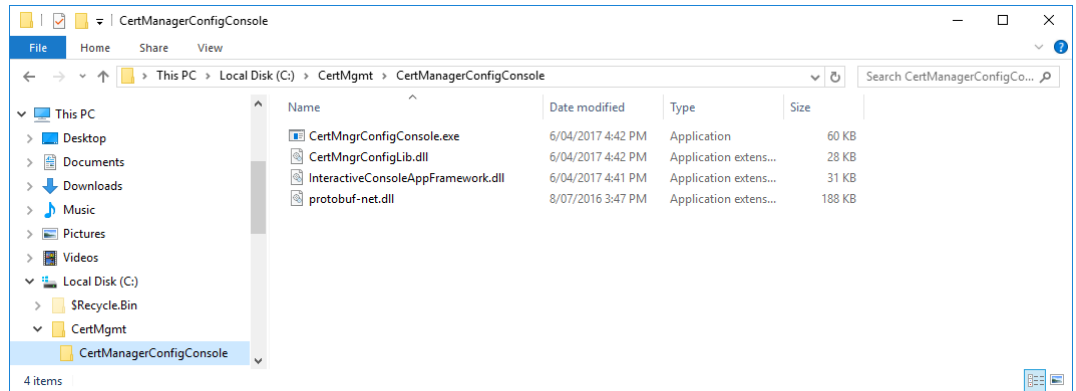
4. See Creating a certificate for a Windows node for more information. To create a certificate of type CMCC for the Windows computer, just install the CMCC software, and make sure that you install it to the Current User store. See Importing certificate and private key on target machine for more information.

5. Start up a management console (mmc.exe) accepting a User account control prompt or providing appropriate credentials if shown:
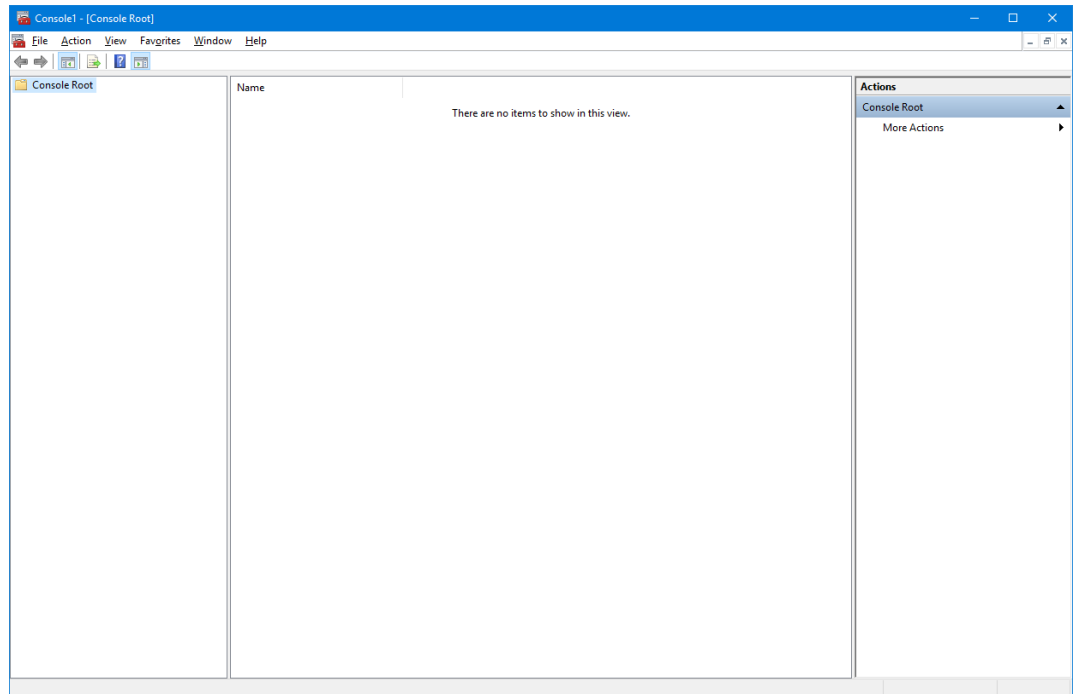
6. From the **File** menu, click **Add/Remove Snap-in**.
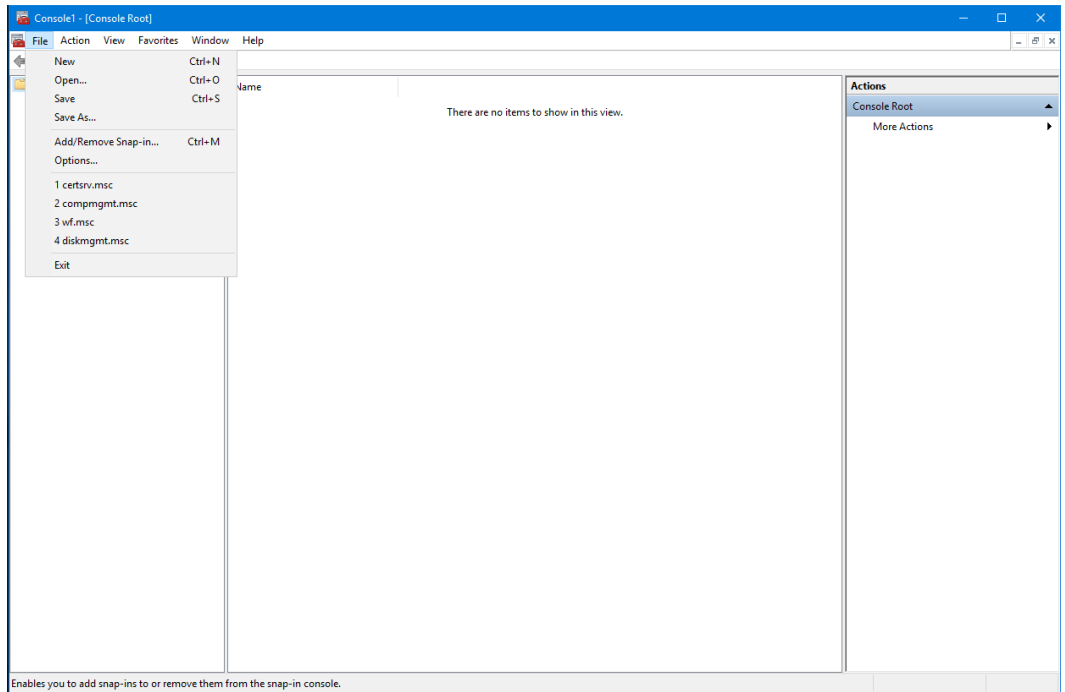
7. In **Add or Remove Snap-Ins** dialog, select **Certificates** and click **Add** .
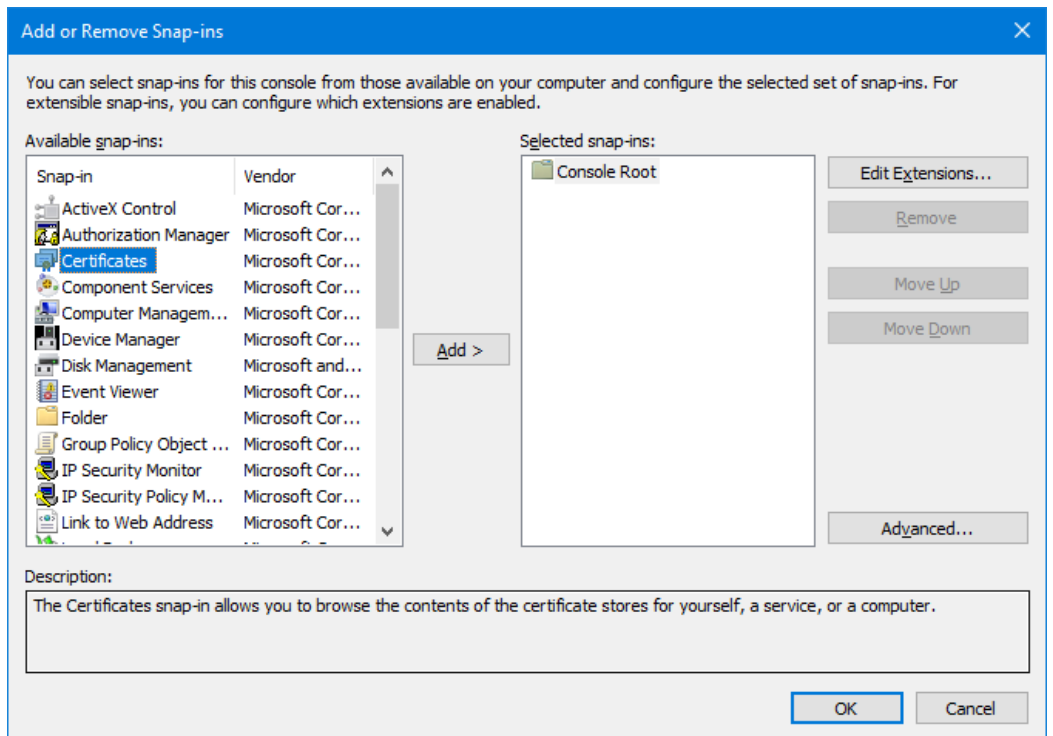
8. In **Certificates snap-in** , select **My user account** and click **Finish**.
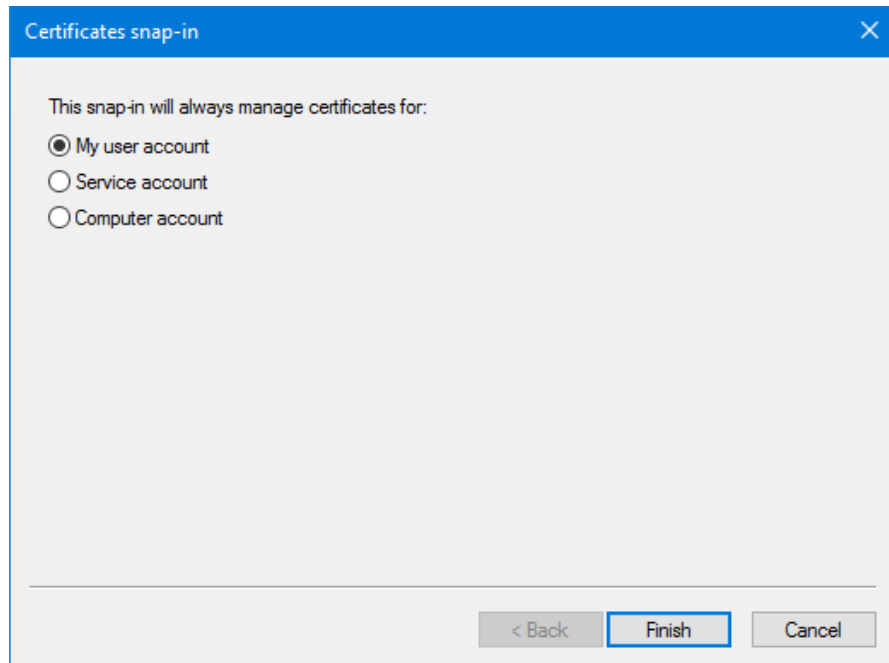
9. Back to **Add or Remove Snap-ins** dialog, make sure that **Certificates – Current User** is under **Selected snap-ins** and then click **OK**.
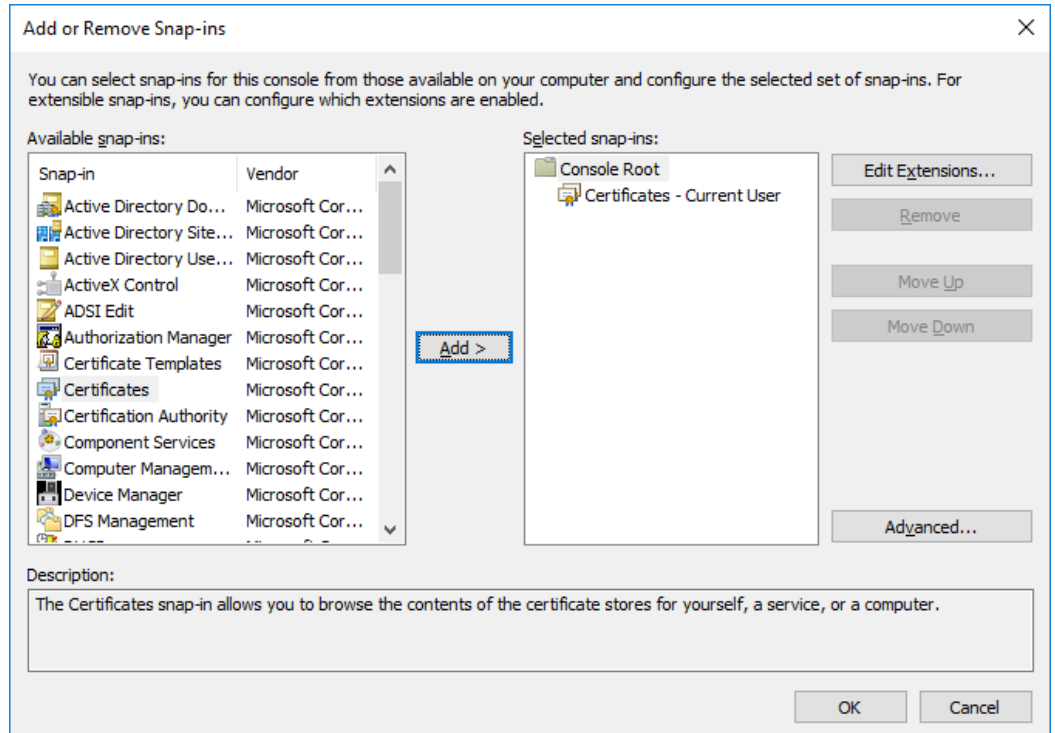
10. Go to **File** menu and click **Save**.
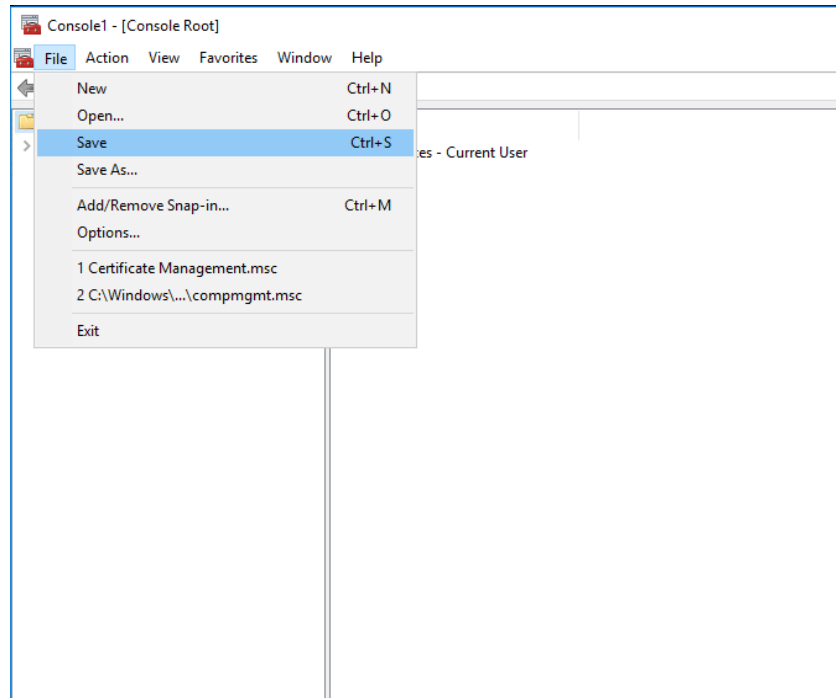
11. Save this console named "Certificate Management" and to the target location, and in this example it is saved to the desktop.
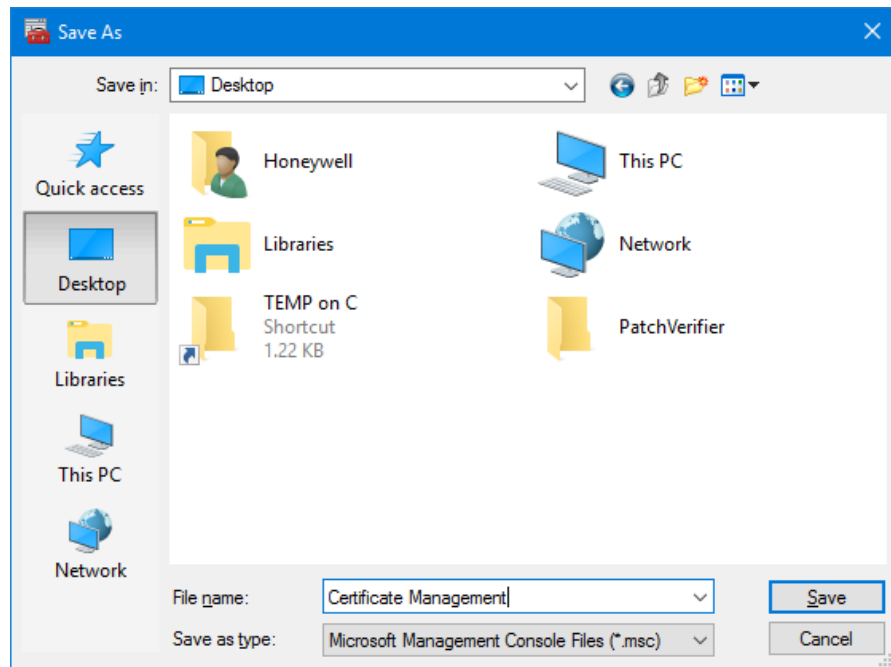
12. In the left hand navigation pane, navigate to **Certificates – Current User**, click **Trusted Root Certification Authorities-> Certificates**, on the right hand pane, it displays the CA's certificate imported.
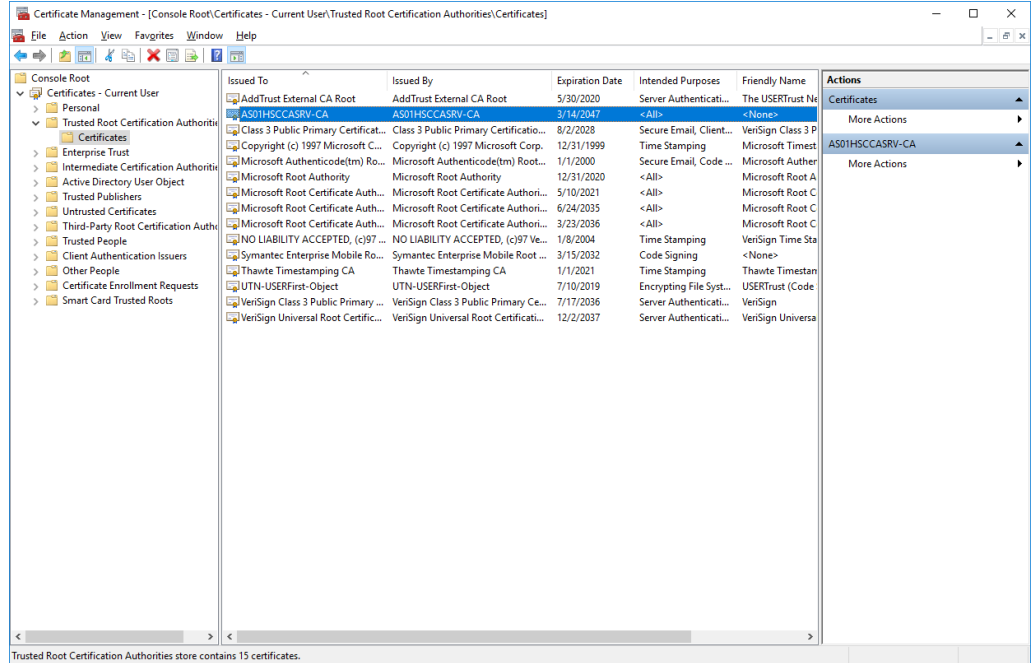
13. Double-click the certificate and navigate to the **Details** tab.
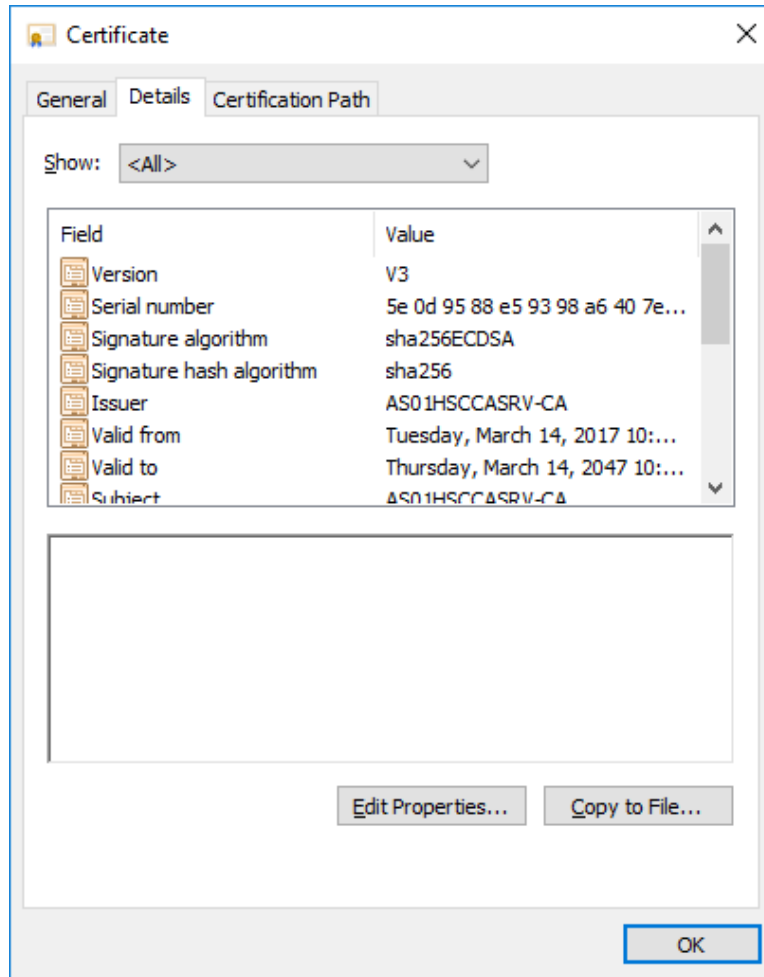
14. On **Certificate** dialog **Details** tab, click **Copy to File...** to save the certificate.

15. Under **Certificate Export Wizard**, click **Next**.
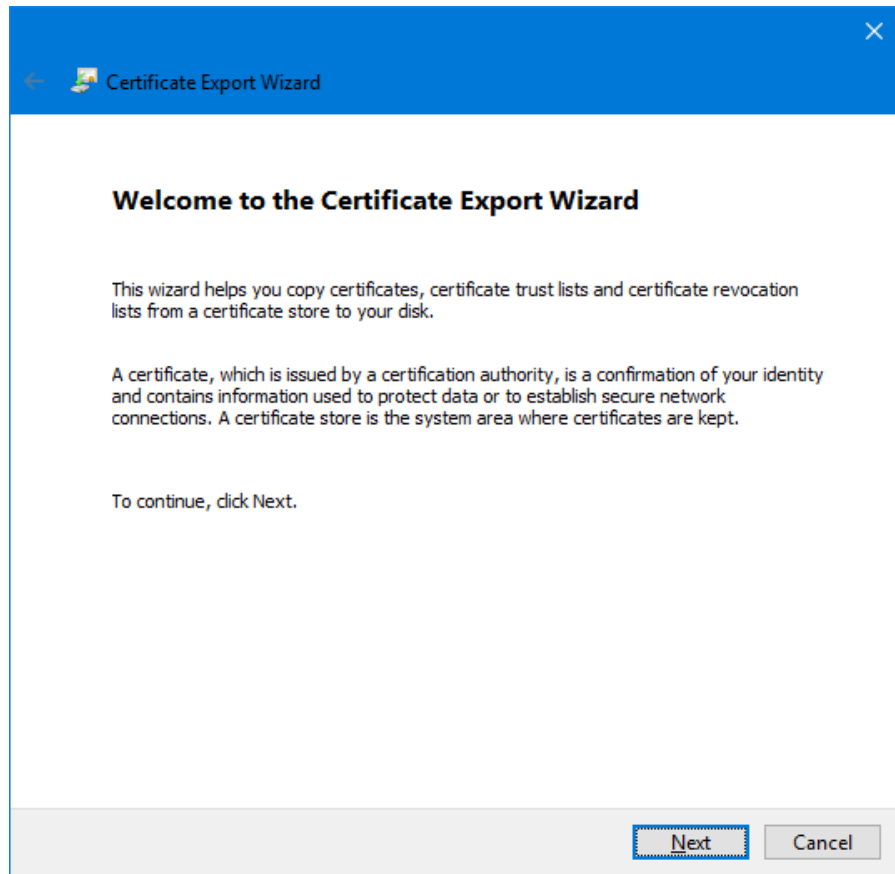
16. Under **Export File Format** , select **DER encoded binary X.509 (.CER)** and then click **Next**.
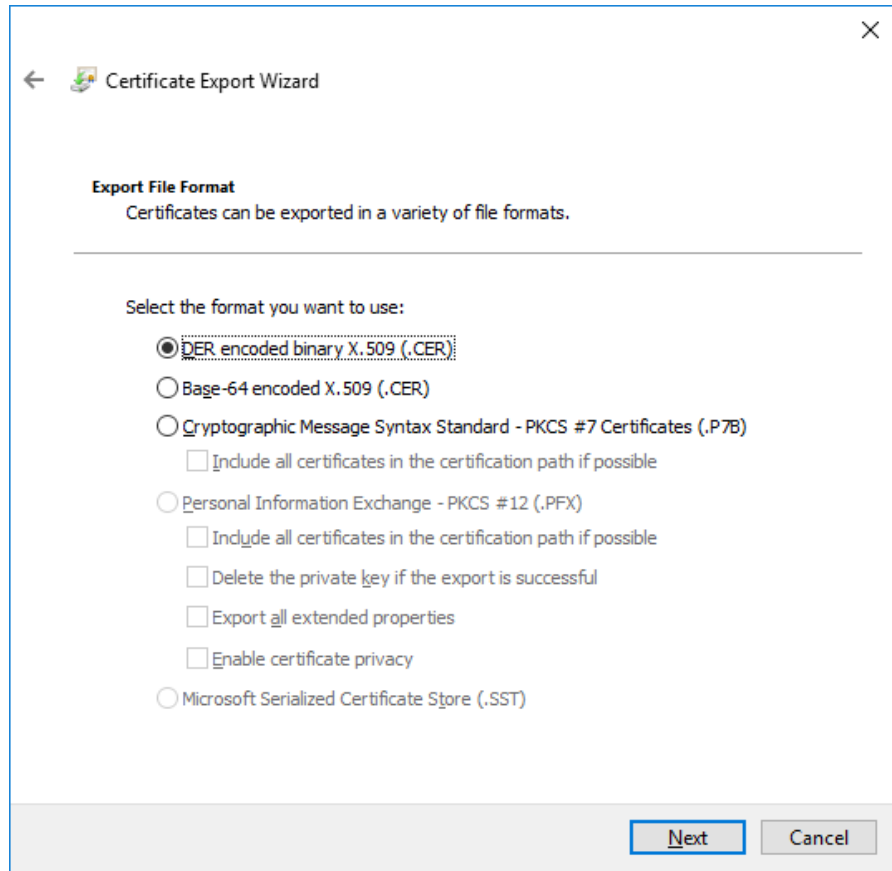
17. Under **File to Export** , specify a file to store the certificate with .CER extension and then click **Next**.
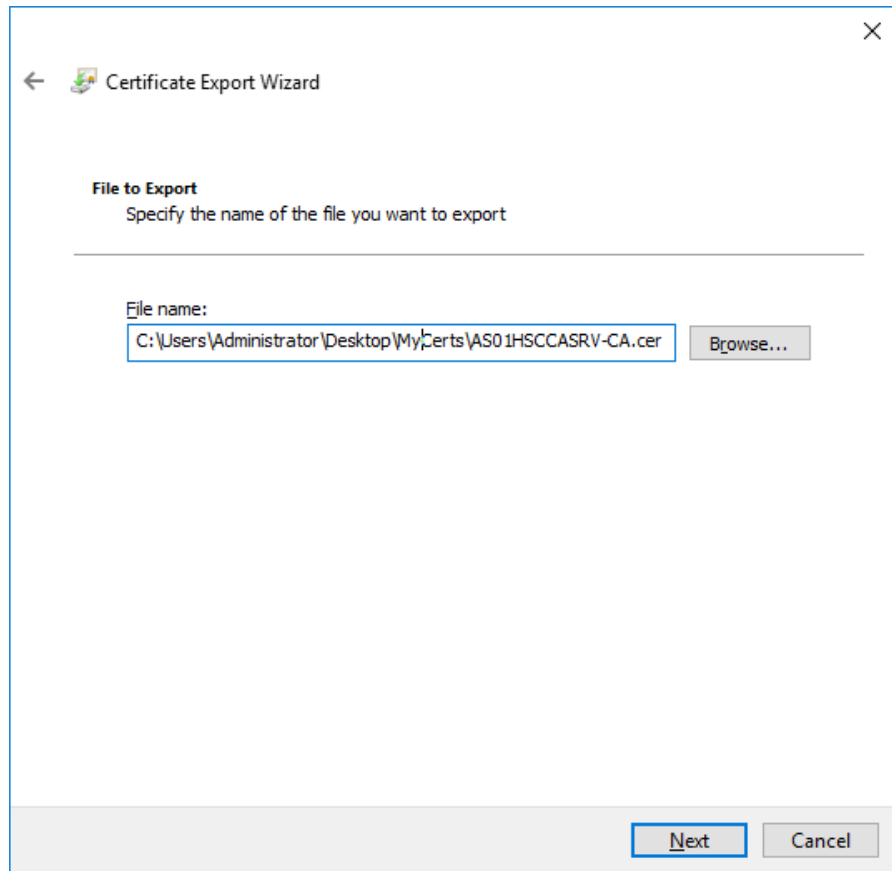
18. Under **Completing the Certificate Export Wizard**, click **Finish** to complete the export.
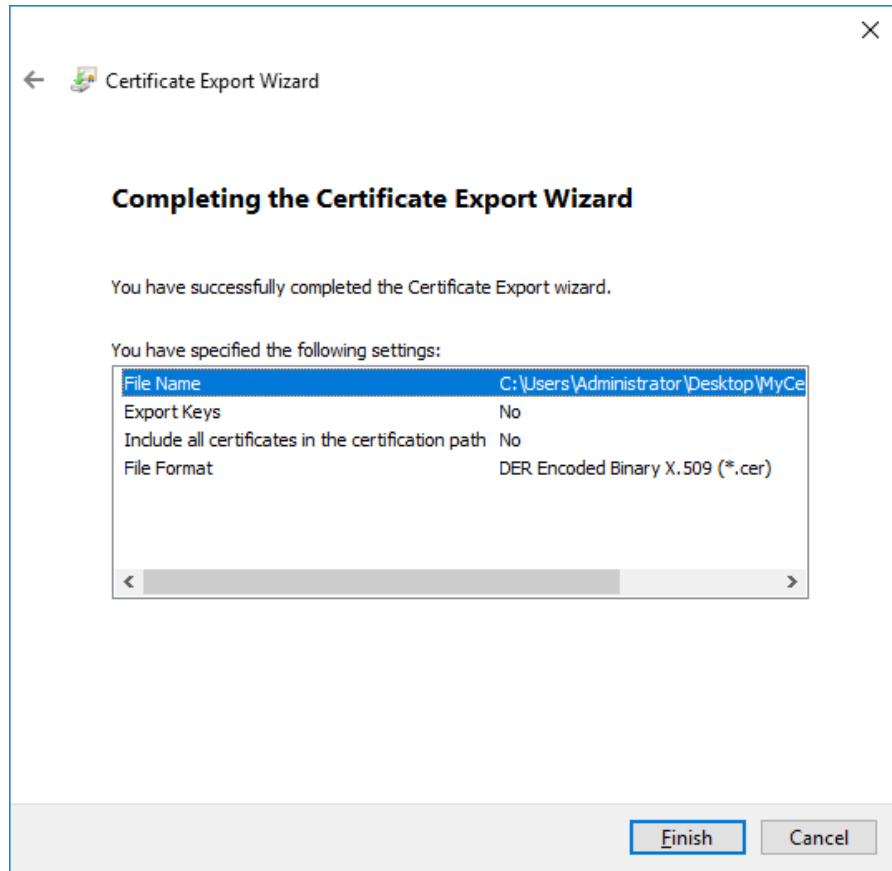
19. A dialog is displayed to indicate that **The export was successful**, then click **OK**.
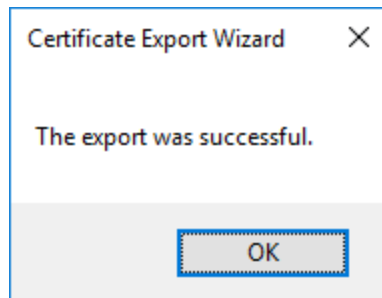
> **TIP:** This .CER file will be used at step 4 in the next section.

Setup certificates and IPsec policy in PLC/RTU

Take PLC as example:

1. Start a Command Prompt and change to the Certificate Manager Configuration Console (CMCC) folder with the following command (or similar):

   `cd \CertMgmt\CertManagerConfigConsole`

   ```
   Command Prompt                                          —   □   ×
   Microsoft Windows [Version 10.0.14393]
   (c) 2016 Microsoft Corporation. All rights reserved.

   C:\Users\Honeywell>cd \CertMgmt\CertManagerConfigConsole

   C:\CertMgmt\CertManagerConfigConsole>_
   ```

2. Run the following command:

   `CertMngrConfigConsole.exe ip:<PLC IP Address>`
   Where <PLC IP Address> is the IP of the PLC, or the Primary PLC if using redundant PLCs.

   ```
   Command Prompt - CertMngrConfigConsole.exe  ip:159.99.79.146                —   □   ×
   C:\CertMgmt\CertManagerConfigConsole>CertMngrConfigConsole.exe ip:159.99.79.146
   Application version: 1.1.0.0
   Available commands and their shortcuts:
   (Enter either one letter shortcut or few initial letters.)
   (To see more details enter 'help command' e.g. 'help c' or 'h c')
   A    reconnect         Disconnects from the device and connects again
   B    HasEnrollInfo     Has the device all data necessary to obtain certificates?
   C    GetEnrollInfo     Downloads and shows current enrollment info
   D    SetEnrollInfo     Enter the data necessary for profile enrollment
   F    ResetToDefault    Factory reset of Certificate Manager in the device
   G    CMProfile         Opens CMProfile submenu or invokes command above CMProfile
   I    Profiles          Opens profile submenu or invokes command above a profile
   J    AddTrustedCA      Add trusted certificate authority to a list of trusted CAs
   K    ListTrustedCA     Shows list of all Trusted CA
   L    RemoveTrustedCA   Removes Certificate Authority from the list of trusted CAs
   M    GetTrustedCA      Downloads certificate of trusted CA from device
   N    IPSec             Opens IPSec submenu or invokes IPSec command
   E    exit
   H    help
   Connected via non-secure channel to 159.99.79.146
   Only commands A to G are available!
   Device is not yet ready for secure connection.
   EnrollmentInfo must be set first by 'SetEnrollInfo'
   Device Time: 2017-04-11T23:44:40Z

   (Press <UpArrow> or <DownArrow> to select)
   >  _
   ```

3. To set the enrolment information, type in the CMCC prompt :

   `SetEnrollInfo`

   ```
   Command Prompt - CertMngrConfigConsole.exe  ip:159.99.79.146                —   □   ×
   (Press <UpArrow> or <DownArrow> to select)
   > SetEnrollInfo
   The Device has no Enrollment Information. It is necessary to enter all items.
   Enter certificate of zone CA signing our CSRs
   (to keep it unchanged leave the cell empty and press <Enter>)
   (Press <Tab> to select)
   CACertificate: _
   ```

4. At the prompts, enter the following information:
   CACertificate – Enter the full path to a copy of the CA certificate (this is the .CER file saved. See Installing Certificate Manager Configuration Console)
   for more information. CAHostname – Enter the IP address of the CA
   CAPort - Leave this at default of 80
   SntpHostname – Leave this as default if there is no SNTP server; enter the host name of the SNTP Server if there is.
   DeviceIPAddressN – Enter the IP addresses of the PLC (first two should be for the primary PLC and the last two for the secondary

PLC if using redundant PLCs). Press Enter after each and if less than 4 then press Enter at a blank prompt. This will indicateto stop further DeviceIPAddress prompts. The first IP address should be pre-populated with the IP address you used to start the CMCC.

5. To verify that the enrolment information has been set in the PLC at the CMCC prompt type:

GetEnrollInfo

<Enter>

6. To enrol the Certificate Manager, type in CMCC prompt :

CMProfile

This makes the CMProfile menu to enroll the Certificate Manager

in the PLC with the CA.

7. Open a web browser to the CA Server:

    `https://<CA Server IP Address>/GetChallenge`

NOTE: If you are using Internet Explorer on a Windows Server OS, first add the CA site to your "Trusted Sites". When prompted login with the local Administrator account credentials for the CA Server, ensure "Remember my credentials" remains un-checked.

NOTE: If your web browser is running on a machine in a domain ensure you use ".\Administrator" as the user name.
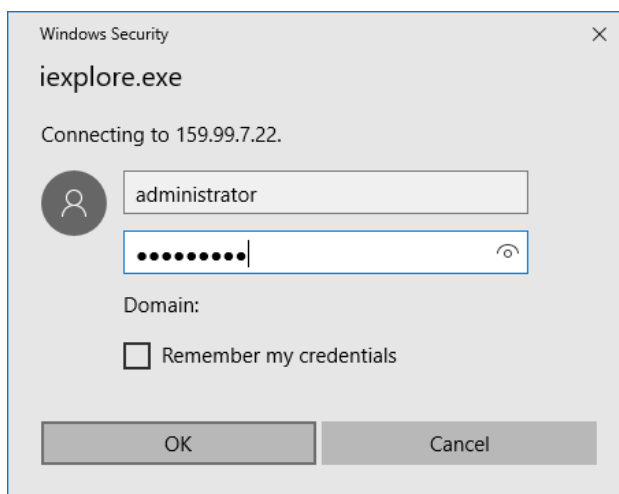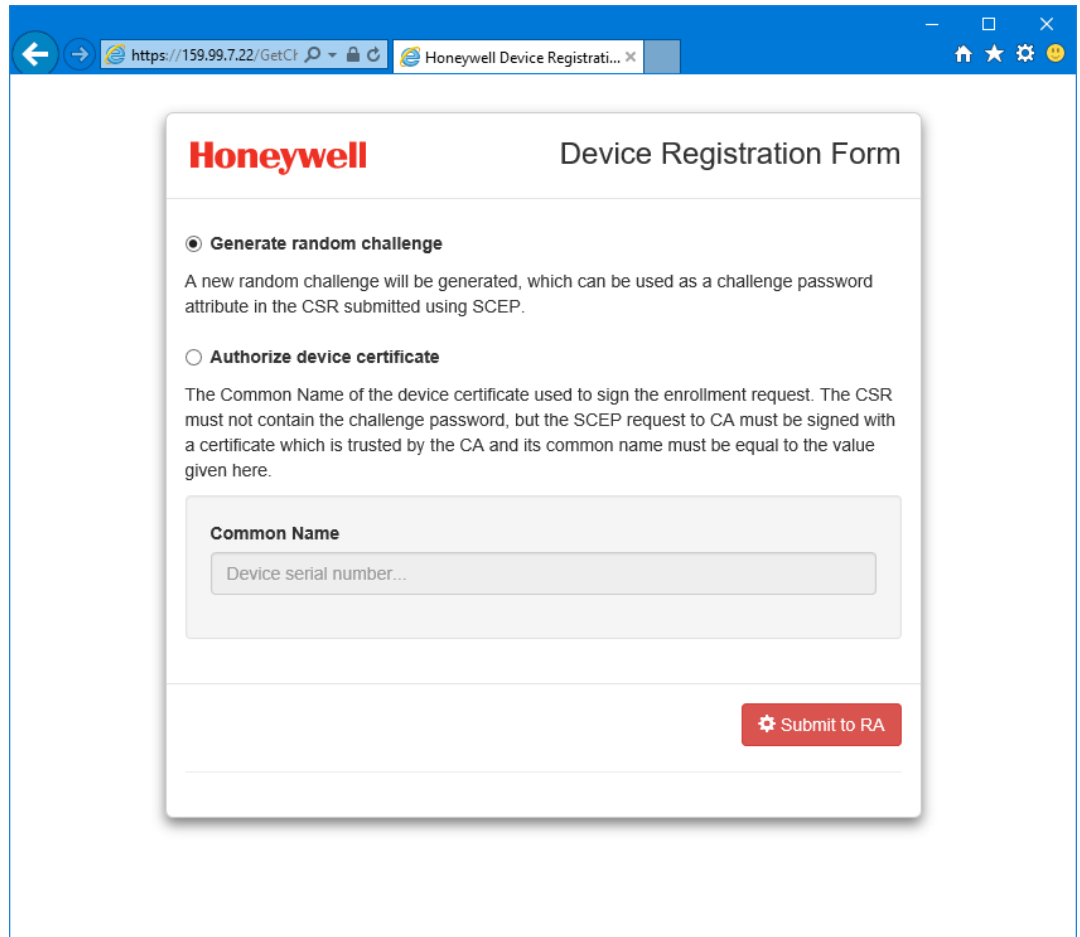
8. Select **Generate random challenge** and click **Submit to RA**, the page then displays **Generated Challenge** (also known as a one time password, OTP).

> **ATTENTION:** The OTP should be handled with extreme care and ensure the value is communicated to the PLC in a controlled manner. Loss of the OTP may allow the introduction of a separate node as a trusted node within the system, if it is used elsewhere between generation and step 9 below you will receive an error from the CMCC tool indicating the OTP is invalid.

9. Back in the CMCC tool, to enrol the PLC's Certificate Manager module, type the following command at the CMCC prompt:
   EnrollWithPassword
   Then type the OTP from the previous step, the enrolment then succeed.

10. To exit the CMProfile menu, run the following commands:
    exit

11. To re-connect CMCC to the PLC securely, type the following commands at the CMCC prompt:
    Reconnect

12. A pop-up window is displayed, select the CMCC client certificate created and installed at step 3 of last section. See Installing Certificate Manager Configuration Console for more information.

13. The CMCC will reconnect to the PLC but will use TLS security on the connection. To start the Enroll IPsec process on the PLC, type the following command at the CMCC prompt:
    Profiles

14. Press **Enter** to choose IPSec.

15. Start a new web browser instance and connect to the CA Server:
    `https://<CA Server IP Address>/GetChallenge`

> **NOTE:** If you are using Internet Explorer on a Windows Server OS, at first ensure the CA site has been added to your "Trusted Sites".
> When prompted login with the local Administrator account credentials for the CA Server, make sure "Remember my credentials" is not selected.

> **NOTE:** If your web browser is running on a machine in a domain, make sure you use ".\Administrator" as the user name.

16. Select **Generate random challenge** and click on **Submit to RA**, then it displays the Generated Challenge (also known as a one time password, OTP).

17. Back in the CMCC tool, to enrol the PLC's IPSec, type the following command at the CMCC prompt:
    EnrollWithPassword
    Then type the OTP from the previous step, the enrolment succeeds.

18. In the CMCC tool, to revert back to the top level menu, type the following command at the CMCC prompt:
Exit

Skip to step 34 for non-redundant PLCs.

> **TIP:** Screenshots have been omitted for most steps for Backup PLC as they are identical to those previously seen for Primary PLC.

19. Redundant PLCs only:
to exit out of the CMCC , run the following command:
Exit

20. Redundant PLCs only:
Run the following command:
`CertMngrConfigConsole.exe ip:<PLC IP Address>`
Where <PLC IP Address> is the IP of the secondary PLC.

21. Redundant PLCs only:
Open a web browser to the CA Server:
`https://<CA Server IP Address>/GetChallenge`
Note: If you are using Internet Explorer on a Windows Server OS, first ensure the CA site has been added to your "Trusted Sites". When prompted login with the local Administrator account credentials for the CA Server, ensure "Remember my credentials" remains un-checked.
Note: If your web browser is running on a machine in a domain ensure you use ".\Administrator" as the user name.

22. Redundant PLCs only:
To enrol the Certificate Manager, type at the CMCC prompt :
CMProfile
This makes the CMProfile menu to enroll the Certificate Manager in the PLC with the CA.

23. Redundant PLCs only:
Select **Generate random challenge** and click **Submit to RA**, and it displays the Generated Challenge (also known as a one time password, OTP).

24. Redundant PLCs only:
    Back in the CMCC tool, to enrol the PLC's Certificate Manager
    module, type the following command at the CMCC prompt type:
    EnrollWithPassword
    Then type the OTP from the previous step, the enrolment
    succeeds.

25. Redundant PLCs only:
    A pop-up window is displayed, and select the CMCC client
    certificate created and installed at step 3 of last section. See
    Installing Certificate Manager Configuration Console for more
    information.

26. Redundant PLCs only:
    To continue to re-connect CMCC to the PLC securely, type the
    following commands at the CMCC prompt to exit from the current
    menu and then re-connect:
    Exit
    Reconnect

27. Redundant PLCs only:
    The CMCC will reconnect to the PLC but using TLS security on
    the connection , and to start the Enroll IPsec process on the PLC,
    type the following command at the CMCC prompt type:
    Profiles

28. Redundant PLCs only:
    Press **Enter** to choose IPSec.

29. Redundant PLCs only:
    Start a new web browser instance and connect to the CA Server:
    `https://<CA Server IP Address>/GetChallenge`

    > **NOTE:** If you are using Internet Explorer on a Windows
    > Server OS, at first make sure the CA site has been added to
    > your "Trusted Sites".
    > When prompted login with the local Administrator account
    > credentials for the CA Server, keep "Remember my
    > credentials" not selected.

    > **NOTE:** If your web browser is running on a machine in a
    > domain ensure you use ".\Administrator" as the user name.

30. Redundant PLCs only:
    Select **Generate random challenge** and click **Submit to RA**, then it

displays the Generated Challenge (also known as a one time password, OTP).

31. Redundant PLCs only:
Back in the CMCC tool, enrol the PLC's IPSec enrol, type the following command at the CMCC prompt type:
EnrollWithPassword
Then type the OTP from the previous step, the enrolment succeeds.

32. Redundant PLCs only:
To exit the CMCC tool, run the following commands:
Exit
Exit

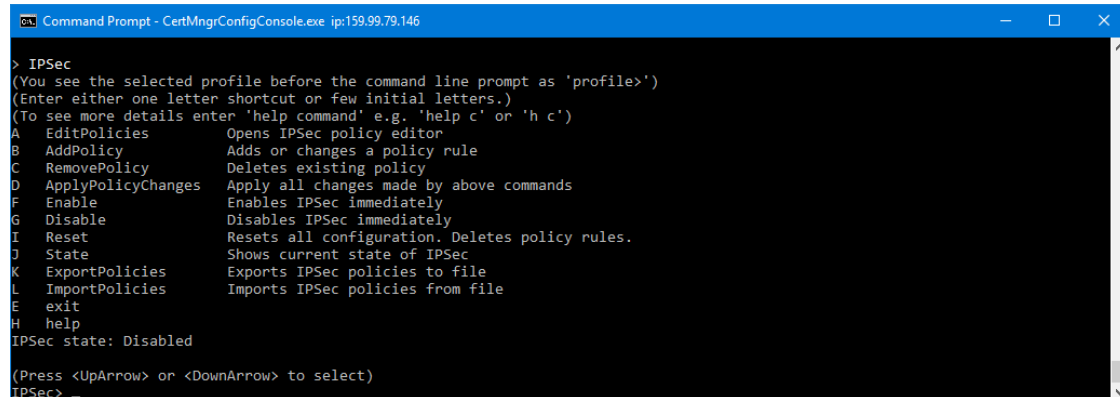33. Redundant PLCs only:
Run the following command:
`CertMngrConfigConsole.exe ip:<PLC IP Address>`
Where <PLC IP Address> is the IP of the Primary PLC.

Re-join steps here for single PLC, and continue on for Redundant PLCs:

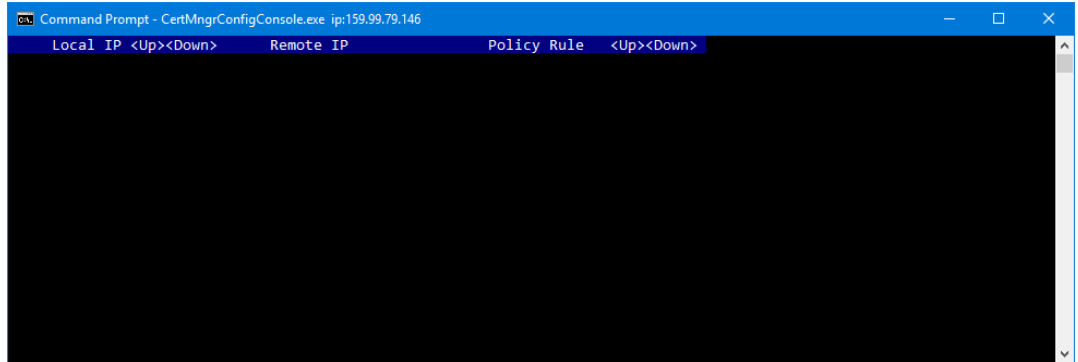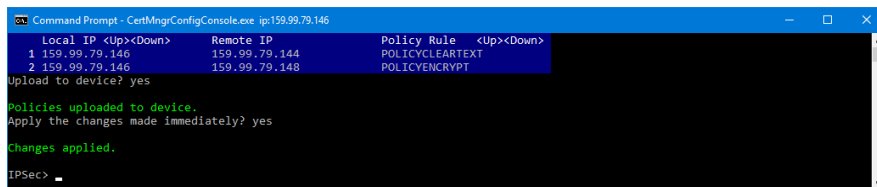34. Enter the following command to enter the IPsec menu at the CMCC prompt:
IPsec

35. Enter the following command to Edit Policies at the CMCC prompt:

EditPolicies

36. Press Ctrl+Insert to insert a new line into the policies list and press Enter to edit the first column (Local IP).

1. Type the PLC's IP address (159.99.79.146 in this example) in the Local IP column and press Enter.

2. Move to the right (press right arrow key) and press Enter, and type the PC accessing the PLC's IP address (159.99.79.148 in this example), then press Enter.

3. Move to the right (press right arrow key) and press Enter, and select the required policy rule using up and down arrows (encrypt/plain-text/authenticate) in this example POLICYENCRYPT, then press Enter.

4. Use Ctrl+Insert plus steps a to c to add more rules for all IP addresses for primary and secondary controllers (in Local IP column), and for each Windows PC (Remote IP column) requiring access (eg Primary and Secondary Server as well as ControlEdge Builder).

5. Use Crtrl+Insert plus steps a to c to add more rules for all IP addresses for primary and secondary controllers (in Local IP column) to any EPM (Remote IP column) connected to the PLC, however create these with a cleartext policy.

6. Then press Esc, Enter and Enter again to apply the policies.

> **NOTE:** The POLICYCLEARTEXT rule above is for an EPM. To delete the selected rule, use Ctrl+Delete.

37. To exit the tool, type the following commands at the CMCC prompt:

Exit

Exit

> **TIP:** If using redundant controllers, the policies will be saved and applied automatically at the secondary controller.

Configuring IPsec to secure traffic to the PLC/RTU

Prerequisites

Time synchronisation is critical to IPsec, otherwise authentication would be failed and the communication would be blocked. To use IPsec secure communication, users must synchronise the time on Controller, external devices and SCADA. For how to enable time synchronisation, see "Setting time source" in *ControlEdge Builder Use's Guide* for more information.

Enable IPsec policy on PCs

This section explains rules based on the setup outlined in section Obtaining and installing the software, using the device IP addresses below for a non-FTE dual network:

- RDP Client – 192.168.1.1
- CA Server – 192.168.2.2
- Experion HS Server (Windows Node 3) – 192.168.10.3, 192.168.11.3
- Experion HS eServer or Station (Windows Node 4) – 192.168.10.4, 192.168.11.4
- Experion HS Configuration Studio and ControlEdge Builder (Windows Node 5) – 192.168.10.5, 192.168.11.5
- ControlEdge PLC/RTU – 192.168.10.6, 192.168.11.6

- 3rd party PLC – 192.168.10.7, 129.168.11.7

- SNTP Server (Windows Node 6)–192.168.10.8

Before applying IPsec, make sure: All machines that need to communicate with the PLC/RTU and the PLC/RTU have installed their certificates and have the CA in their Trusted Root CA list.

Application of IPsec policy involves setting a number of exceptions to this rule to control how the various nodes and devices communicate with and without IPsec.

Use the examples below to create your own policies.

> **CAUTION:** The configuration performed in this section should not be performed in an on-process/live system, as you will lose communications to one or all of the nodes in the system when you are deploying this policy, until all nodes have been configured.

To enable IPsec, a series of commands must be executed to setup the various policies. These policies take effect immediately, so once the "Default Closed" policy is applied, non–IPsec (clear text) communications to the nodes will be lost. So it is important that an exception for RDP is made if the configuration of the nodes is being performed via RDP, otherwise this connection will be lost.

The following set of steps should be run on all nodes connecting to the PLC/RTU, and in the example, these steps need to be performed on Node 3 and Node 5. Note in all examples, below "endpoint2" represents the node the rule is being added on, and "endpoint1", where specified, is the node that is being remotely connected to/from.

1. Create and install an IPsec certificate for this Windows node. See Creating a certificate for a Windows node for more information.

2. Start an Administrative Command prompt.

3. Run the following commands to set the main mode parameters on Node 3 and Node 5 only (as those nodes alone communicate to the PLC/RTU).

   - netsh advfirewall set global mainmode mmsecmethods ecdhp256:aes128-sha256

   - netsh advfirewall set global mainmode mmforcedh yes

   - netsh advfirewall consec delete rule name=all

4. To setup the clear text communication exception rules for the control system subnet, using the example earlier, this system need to allow Node 4 and Node 5 to connect to Node 3, and Node 3 and Node 4 to connect to Node 5.

    1. When configuring on Node 3, run the following commands , note each point is a single command:

        *   netsh advfirewall consec add rule name="*Node 4* Exception" description="*Node 4* to this node clear text comms" action=noauthentication endpoint1="*192.168.10.4,192.168.11.4*" endpoint2="*192.168.10.3,192.168.11.3*"

        *   netsh advfirewall consec add rule name="*Node 5* Exception" description="*Node 5* to this node clear text comms" action=noauthentication endpoint1="*192.168.10.5,192.168.11.5*" endpoint2="*192.168.10.3,192.168.11.3*"

        *   More commands similar to these would be run for any other non–IPsec nodes that connect to Node 3, modify the values in italic to make it for the system.

    2. When configuring on Node 5, run the following commands, note each point is a single command:

        *   netsh advfirewall consec add rule name="*Node 3* Exception" description="*Node 3* to this node clear text comms" action=noauthentication endpoint1="*192.168.10.3,192.168.11.3*" endpoint2="*192.168.10.5,192.168.11.5*"

        *   netsh advfirewall consec add rule name="*Node 4* Exception" description="*Node 4* to this node clear text comms" action=noauthentication" endpoint1="*192.168.10.4,192.168.11.4*" endpoint2="*192.168.10.5,192.168.11.5*"

        *   More commands similar to these would be run for other non–IPsec nodes that connect to Node 5, modify the values in italic to make it for the system.

5. If you are using RDP to connect to the nodes that will communicate with the PLC/RTU, then you will need to create an RDP exception rule (RDP uses TCP port 3389 on the machine being connected to, for example Nodes 3 and 5 below).

   1. When configuring on node 3, run the following commands :

      * netsh advfirewall consec add rule name="*Node 1* RDP Exception" description="*Node 1* RDP clear text comms" action=noauthentication endpoint1="*192.168.1.1*" endpoint2="*192.168.10.3,192.168.11.3*" port2="3389" protocol="tcp"

      * If there are additional nodes that use RDP to this node, then just create additional exception rules by modifying the text in bold underline.

   2. When configuring on node 5 the following command needs to be run:

      * netsh advfirewall consec add rule name="Node 1 RDP Exception" description="Node 1 RDP clear text comms" action=noauthentication endpoint1="192.168.1.1" endpoint2="192.168.10.5,192.168.11.5" port2="3389" protocol="tcp"

      * If there are additional nodes that use RDP to this node, create additional exception rules by modifying the text in italic.

6. For Windows PC nodes that use the CMCC tool to connect to the PLC/RTU , you need the following exceptions to allow CMCC to communicate in clear text to the PLC/RTU when IPsec is enabled. CMCC uses TLS to encrypt this traffic and the PLC/RTU has internal rules to not require IPsec on this connection, so this rule ensures Windows PC nodes do the same. For such nodes, you need to create an RDP exception rule, take PLC as example:

   1. If node 3 uses CMCC, run the following command:

      * netsh advfirewall consec add rule name="PLC CM port Exception" description="PLC CertMngr to this node clear text comms" action=noauthentication endpoint1="*192.168.10.6,192.168.11.6*" endpoint2="192.168.10.3,192.168.11.3"

port1="55601,55602" protocol=tcp

- If there are additional PLCs that this node uses CMCC to connect to, create additional exception rules by modifying the text in italic.

2. If node 5 uses CMCC, run the following commands:

- netsh advfirewall consec add rule name="PLC CM port Exception" description="PLC CertMngr to this node clear text comms" action=noauthentication endpoint1="*192.168.10.6,192.168.11.6*" endpoint2="192.168.10.5,192.168.11.5" port1="55601,55602" protocol=tcp

- If there are additional PLCs that this node uses CMCC to connect to, create additional exception rules by modifying the text in italic.

7. For nodes that use the ControlEdge Builder, a clear text exception rule should be created for the ControlEdge Builder to receive multi-cast packets to detect the presence of a ControlEdge PLC/RTU, taking PLC as example:

1. When configuring node 5, run the following command :

- netsh advfirewall consec add rule name="ControlEdge PLC Discovery Exception" description="ControlEdge PLC discovery port exception" action=noauthentication endpoint1="192.168.10.5,192.168.11.5" endpoint2="192.168.10.6,192.168.11.6" port2="24558" protocol=udp

> NOTE: The value of port2 specifies the multicast address port that the packets are received from, and this is fixed port for all ControlEdge PLCs.

8. To apply IPsec encryption to the nodes communicating with the PLC/RTU, apply the following IPsec rules, takeing PLC as example:

1. When configuring node 3, run the following commands:

- netsh advfirewall consec add rule name="*PLC* Encryption" description="PC to PLC encrypted comms" action=requireinrequireout auth1=computercertecdsap256 endpoint1="*192.168.10.6,192.168.11.6*"

        endpoint2="192.168.10.3,192.168.11.3"
        auth1ecdsap256ca="<*CA Cert SubjectName*>"
        qmsecmethods=ESP:aesgcm128-aesgcm128

- For additional PLCs this PC needs to connect, update the items in italic and run for each PLC.

- The <CA Cert SubjectName> is the string in the Subject field of the CA certificate, with items in reverse order, eg "C=US, O=Honeywell, CN=AS01HSCCASRV" or based on CA created in section Creating the Certificate Authority simply "CN=AS01HSCCASRV-CA". See Creating the Certificate Authority for more information.

- If you have redundant PLCs you need to either make a second version of this rule, or add the secondary PLC's IP addresses into the endpoint1 parameter, separating them by commas.

2. When configuring node 5, run the following command:

- netsh advfirewall consec add rule name="*PLC* Encryption" description="PC to PLC encrypted comms" action=requireinrequireout auth1=computercertecdsap256 endpoint1="*192.168.10.6,192.168.11.6*" endpoint2="192.168.10.5,192.168.11.5" auth1ecdsap256ca="<CA Cert SubjectName>" qmsecmethods=ESP:aesgcm128-aesgcm128

- For additional PLCs this PC needs to connect, update the items in italic and run for each PLC.

- The <CA Cert SubjectName> is the string in the Subject field of the CA certificate, with items in reverse order, eg "C=US, O=Honeywell, CN=AS01HSCCASRV" or based on CA created in sectionCreating the Certificate Authority simply "CN=AS01HSCCASRV-CA". See Creating the Certificate Authority for more information.

- If you have redundant PLCs you need to either make a second version of this rule, or add the secondary PLC's IP addresses into the endpoint1 parameter, separating them by commas.

9. Finally apply the "default close" rule, and this will block all communications except where a rule has been previously created.

    1. When configuring node 3, run the following command:

- netsh advfirewall consec add rule name="Default Close" description=" Connection Rule to close all defaults"

action=requireinrequireout auth1=computercertecdsap256 endpoint1="Any" endpoint2="192.168.10.3,192.168.11.3" endpoint1="Any" auth1ecdsap256ca="<CA Cert SubjectName>" qmsecmethods=ESP:aesgcm128-aesgcm128

- The <CA Cert SubjectName> is the string in the Subject field of the CA certificate, with items in reverse order, eg "C=US, O=Honeywell, CN=AS01HSCCASRV" or based on CA created in section Creating the Certificate Authority, simply "CN=AS01HSCCASRV-CA". See Creating the Certificate Authority for more information.

2. When configuring on node 5, the following command needs to be run:

- netsh advfirewall consec add rule name="Default Close" description=" Connection Rule to close all defaults" action=requireinrequireout auth1=computercertecdsap256 endpoint1="Any" endpoint2="192.168.10.5,192.168.11.5" auth1ecdsap256ca="<*CA Cert SubjectName*>" qmsecmethods=ESP:aesgcm128-aesgcm128

- The <CA Cert SubjectName> is the string in the Subject field of the CA certificate, with items in reverse order eg, "C=US, O=Honeywell, CN=AS01HSCCASRV" or based on CA created in section Creating the Certificate Authority, simply "CN=AS01HSCCASRV-CA". See Creating the Certificate Authority for more information.

3. Repeat these commands on other Windows nodes that have IPsec rules applied to by modifying the text in italic.

10. For nodes that use the SNTP server, a clear text exception rule needs to be created for the ControlEdge Builder to be able to receive multi-cast packets to synchronize with the SNTP server:

When configuring node 6, run the following command:

- netsh advfirewall consec add rule name="SNTP Server Exception" description="SNTP Server port exception" action=noauthentication endpoint1="192.168.10.8" endpoint2="192.168.10.6,192.168.11.6" port1="123" protocol=udp

> **ATTENTION:** The value of port1 specifies the multicast address port that the packets are received from, this is fixed port for all devicess.

To make enabling of IPsec policy easy on Windows nodes, it is suggested to create a batch file per Windows node, enableIPsec.bat, and storr all the required netsh commands in this file. It makes it easier to add new rules when new nodes are introduced to the system. It also allows to backup your Windows node IPsec rules configuration by taking a copy of this file. And you need a separate instance of this batch file for each machine.

> **CAUTION:** The rules above will appear in the Windows Advanced Firewall console under Connection Security, do not use that console to modify these rules because some of the settings in these rules are not supported by the console and may result in the rules being inadvertently modified to an unusable state.

Disable IPsec policy on PCs

1. Start an Administrative Command prompt.
2. Run the following command to clear the IPsec rules:

   `netsh advfirewall consec delete rule name=all`

To disable IPsec on a Windows node, it is suggested to create a batch file per Windows node, disableIPsec.bat, and store the command above in it, because remembering to type "disableIPsec" to disable IPsec is easier than the command above. Keeping no machine specific data in this batch file, a single disableIPsec.bat can be copied and used on multiple nodes.

Enable IPsec policy rules in the PLC/RTU

Before enabling IPsec policy rules in the PLC/RTU ensure:

- The system is not on process.
- All PCs connected to the PLC/RTU and other devices using IPsec to the PLC/RTU are completely configured to use an IPsec Encrypted policy.

Perform the following steps to enable IPsec policy rules in the PLC/RTU:

1. Connect the CMCC tool to the PLC/RTU with the following command:
   CertMngrConfigConsole.exe ip:<PLC/RTU IP address>
   <PLC/RTU IP address> is the IP address of the PLC/RTU (Primary PLC/RTU if using redundant PLCs/RTUs)

```
C:\CertMgmt\CertManagerConfigConsole>CertMngrConfigConsole.exe ip:159.99.79.146
```

2. Click **OK** to confirm the certificate to use for CMCC.

3. At the top menu, type the following command to enter the IPSec menu:

IPsec

4. Make sure the current IPSec state is Disabled, and type the following command to enable IPsec at the CMCC prompt type:

   Enable

5. To exit the tool, type the following commands at the CMCC prompt:

   Exit

   Exit

> **TIP:** If using redundant PLCs/RTUs when IPsec is enabled on the primary PLC/RTU, this change will be replicated to and enabled on the secondary PLC/RTU.

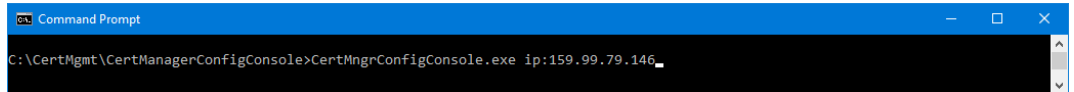## Disable IPsec policy rules in the PLC/RTU

Before disabling IPsec policy rules in the PLC/RTU, make sure:

- The system is not on process.
- TAll PCs connected to the PLC/RTU and other devices using IPsec to the PLC/RTU are configured to use IPsec policies to this device set to Cleartext.
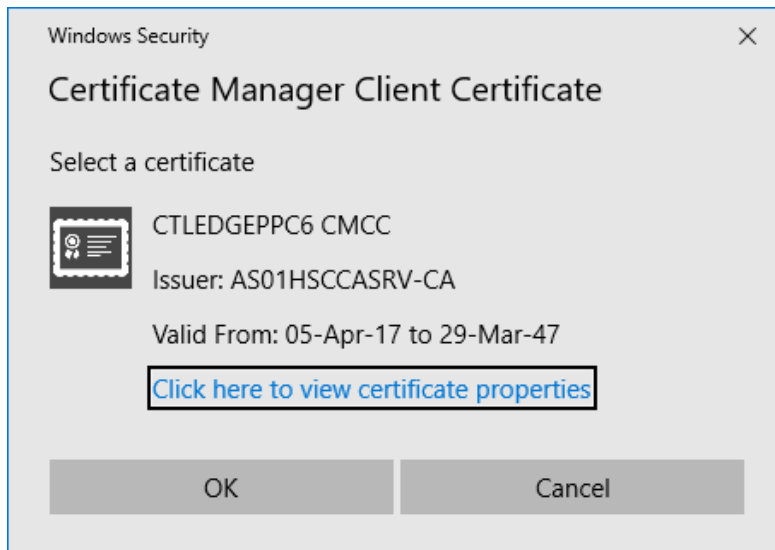
Perform the following steps to disable IPsec policy rule in the PLC/RTU:

1. Connect the CMCC tool to the PLC/RTU with the following command:
   CertMngrConfigConsole.exe ip:<PLC/RTU IP address>
   <PLC/RTU IP address> is the IP address of the PLC (Primary PLC/RTU if using redundant PLCs/RTUs).

2. To confirm the certificate to use for CMMC, click **OK** .

3. At the top menu, type the following commands to enter the IPSec menu:

IPsec

4. Make sure the current IPSec state is Enabled, and type the following command to enable IPsec at the CMCC prompt:

   Disable

5. To exit the tool, type the following commands at the CMCC prompt:

   Exit

   Exit

> **TIP:** If using redundant PLCs/RTUs when IPsec is enabled on the primary PLC/RTU, this change will be replicated to and enabled on the secondary PLC/RTU.

Backup and Restore of CA

Backup

1. On the CA Server, start up a management console (mmc.exe) accepting a User account control prompt or providing appropriate credentials if it displays.
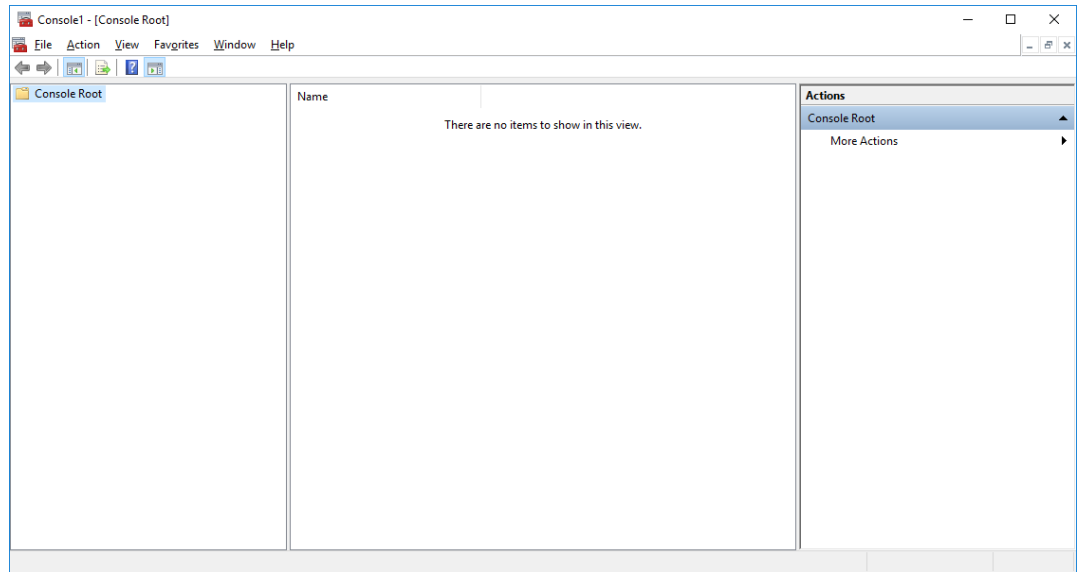
2. From the File menu, click **Add/Remove Snap-in**.
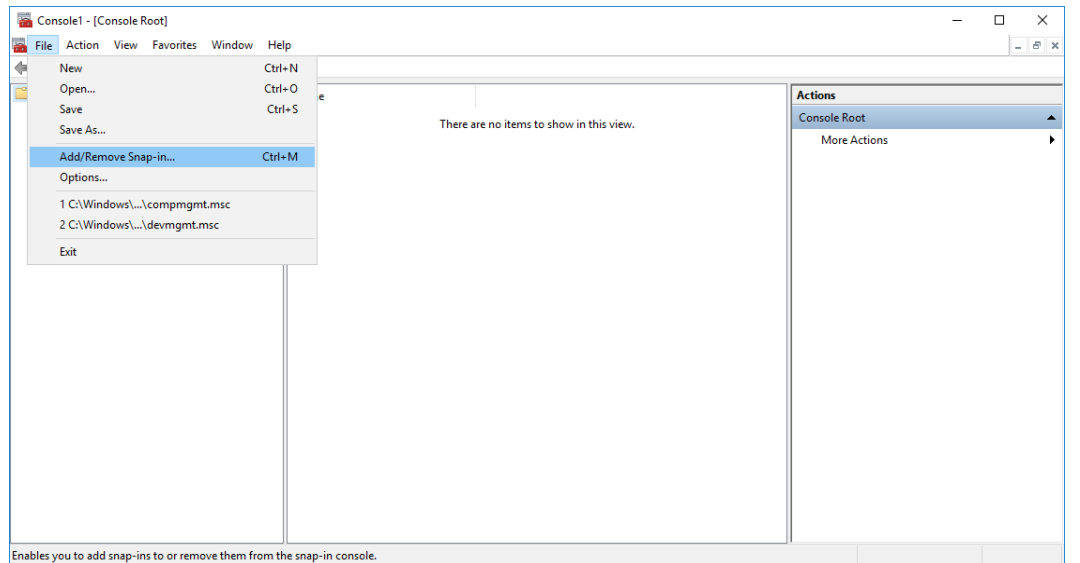
3. In the left column, select **Certification Authority** and click **Add**, and select **Local Computer** and click **Finish** and then **OK**.
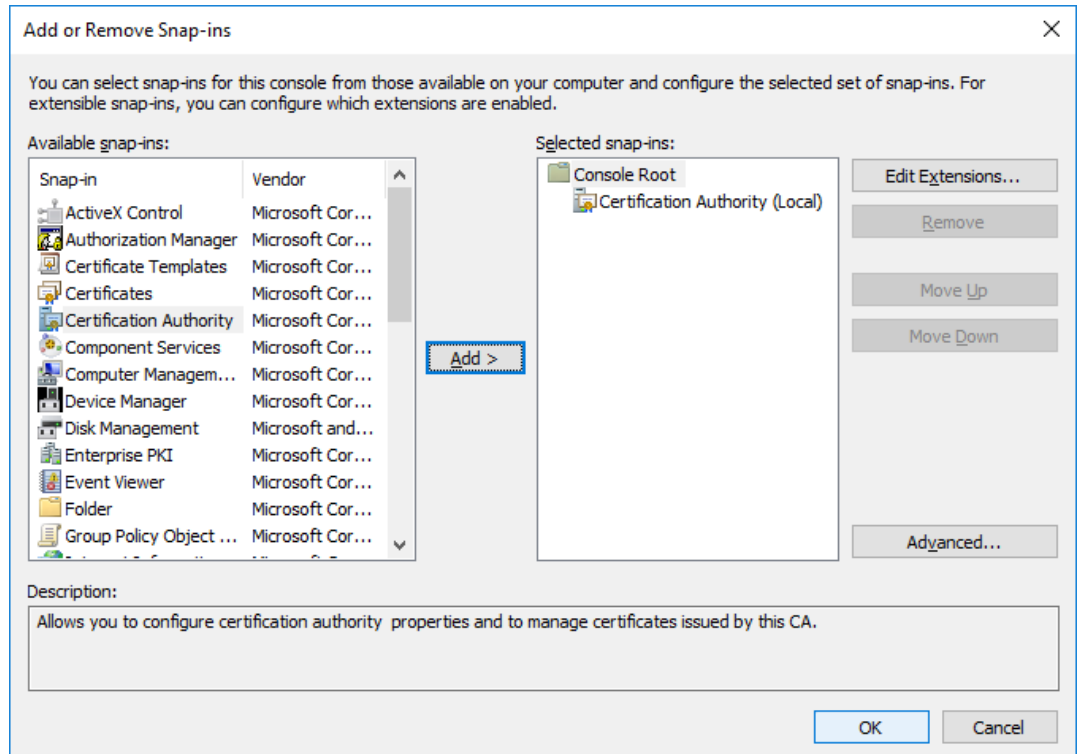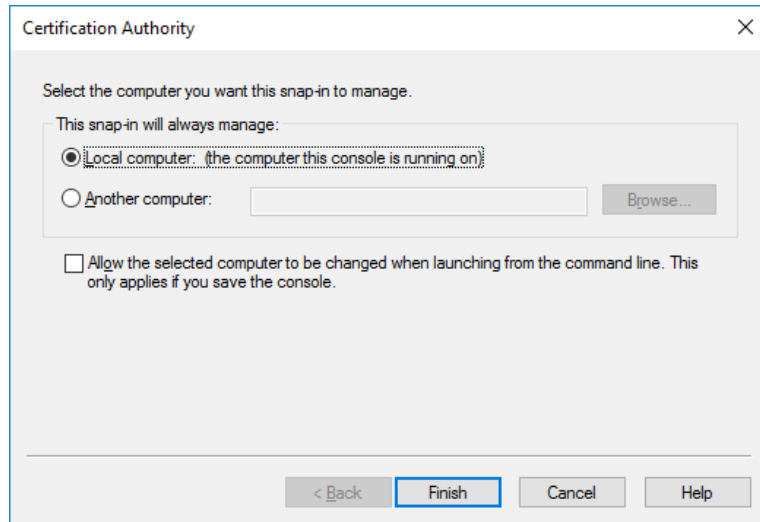
4. In the left hand pane, expand Certification Authority (Local) and then right-click your CA and select **All Tasks** ->**Back up CA...** .
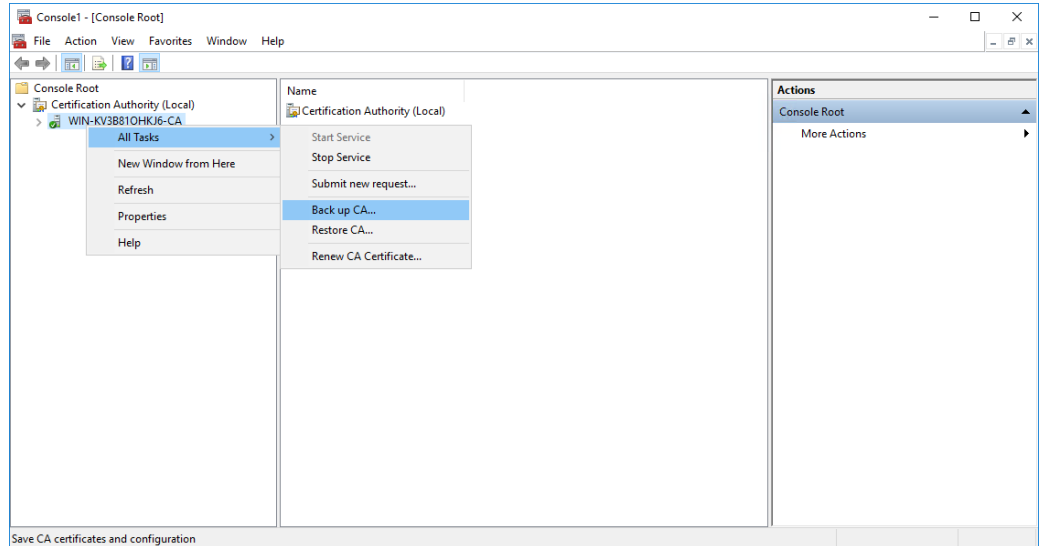
5. At the Welcome to the Certification Authority Backup Wizard dialog, click **Next** .
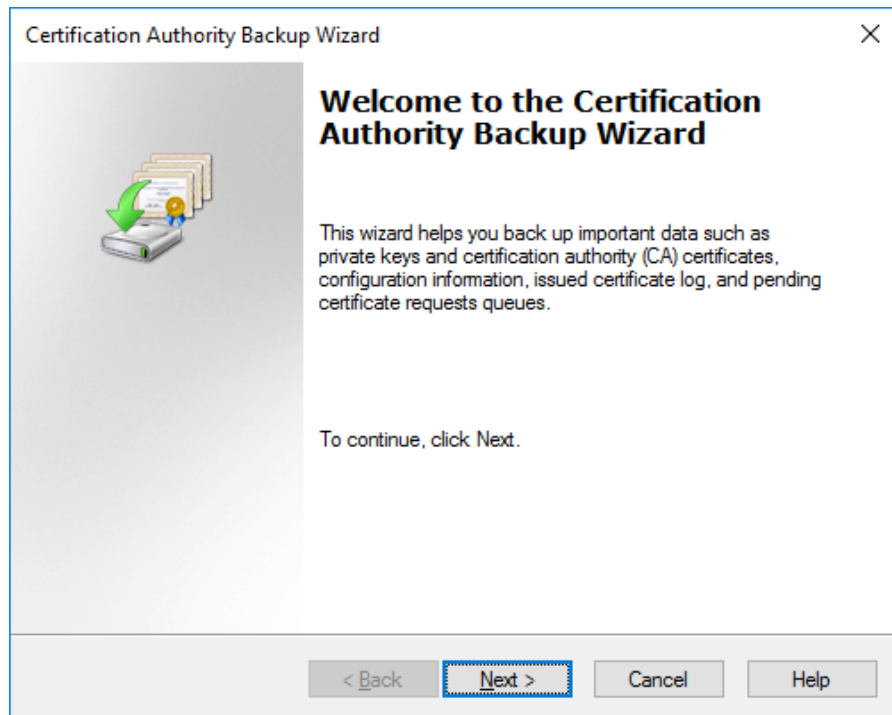
6. Select both **Private key and CA certificate** and **Certificate database and certificate database log** , and specify a directory to back up to (if it does not exist, you will be prompted to confirm the creation of it) and click **Next** .

Certification Authority Backup Wizard ✕

Items to Back Up
You can back up individual components of the certification authority data.

Select the items you wish to back up:

☑ Private key and CA certificate

☑ Certificate database and certificate database log

☐ Perform incremental backup

Back up to this location:

C:\Backup\CA   Browse...

Note: The backup directory must be empty.

< Back   Next >   Cancel   Help

Certification Authority Backup Wizard ✕

The directory C:\Backup\CA does not exist. Do you want to create it?

OK   Cancel

7. Type and confirm a password to protect the CA's private key and then click **Next** .
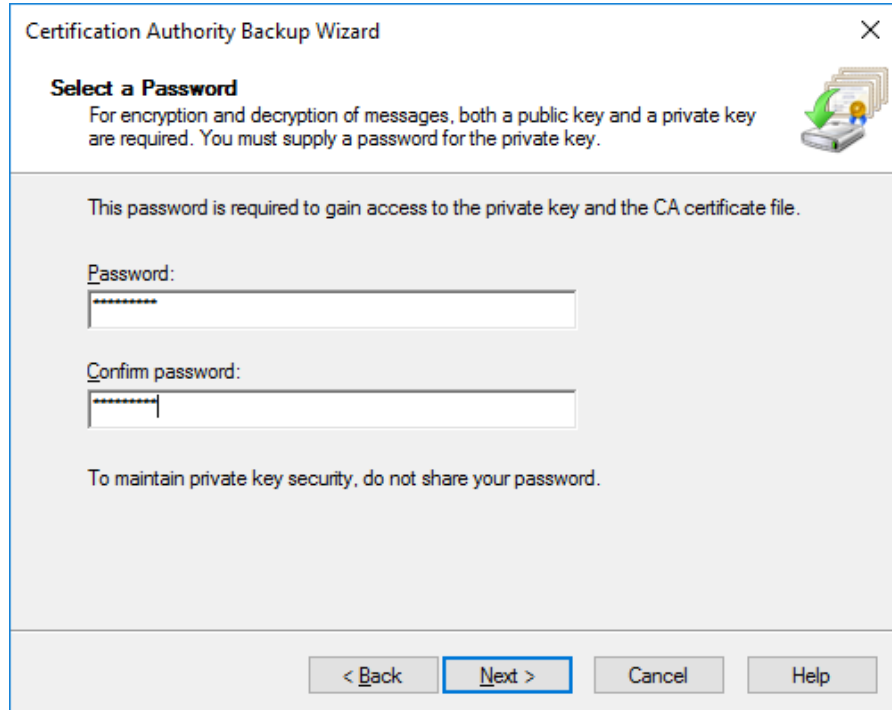
8. Confirm the settings and click **Finish**.
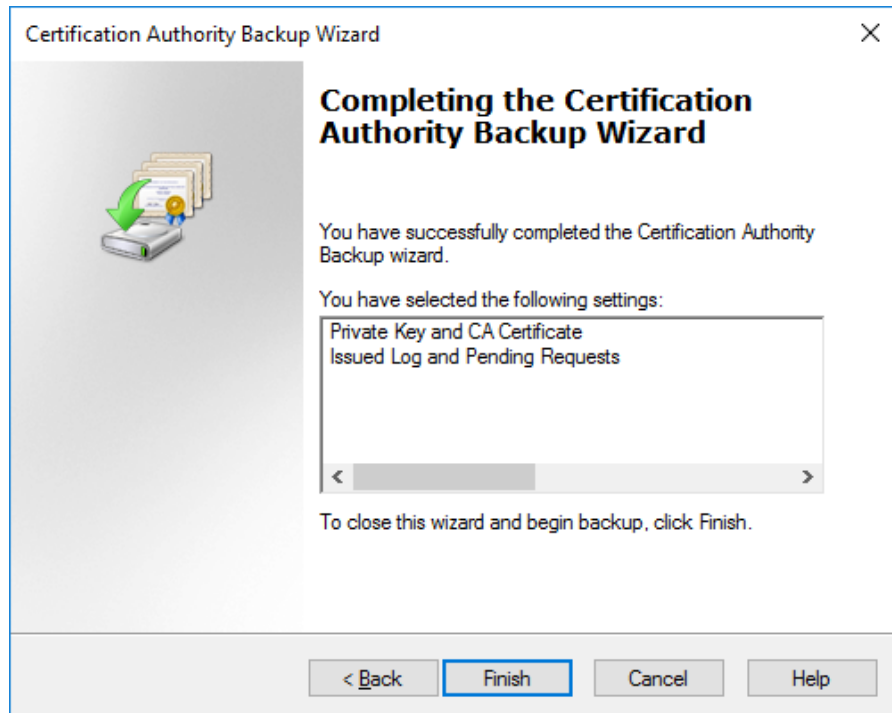
9. To confirm that the backup, use Windows Explorer to navigate to the folder you specified in step 6 and check that files have been output to that folder.
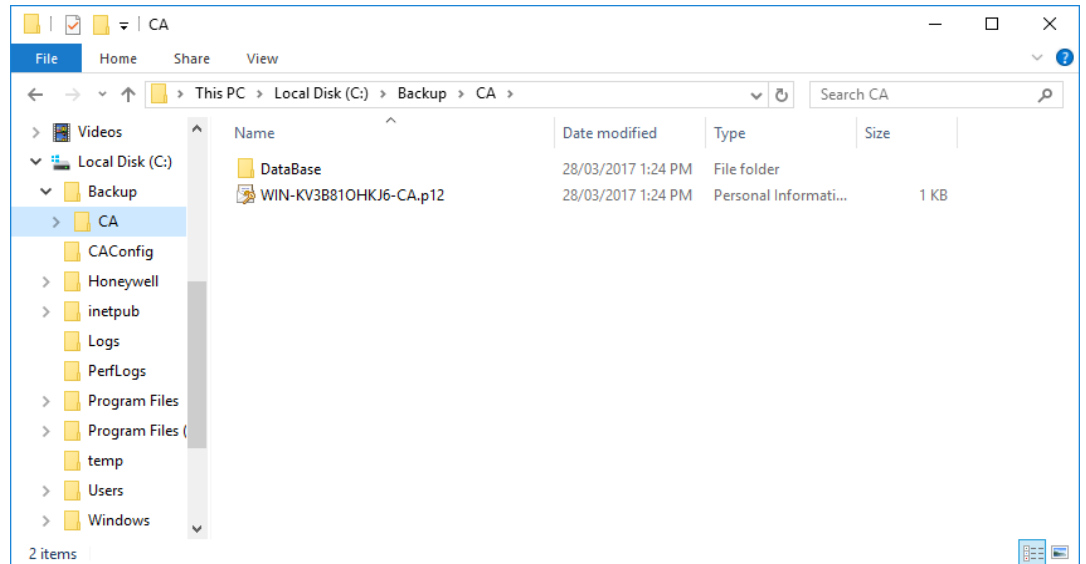
The CA has been backed up to the location specified, and make sure this location is included in any backup jobs, or copy the directory and all its contents to a backup location. You should also backup the folder you store certificates created for CMCC, TLS and IPsec. See Creating a certificate for more information.

Restore

1. On the CA Server, start up a management console (mmc.exe) accepting a User account control prompt or providing appropriate credentials if it displays.
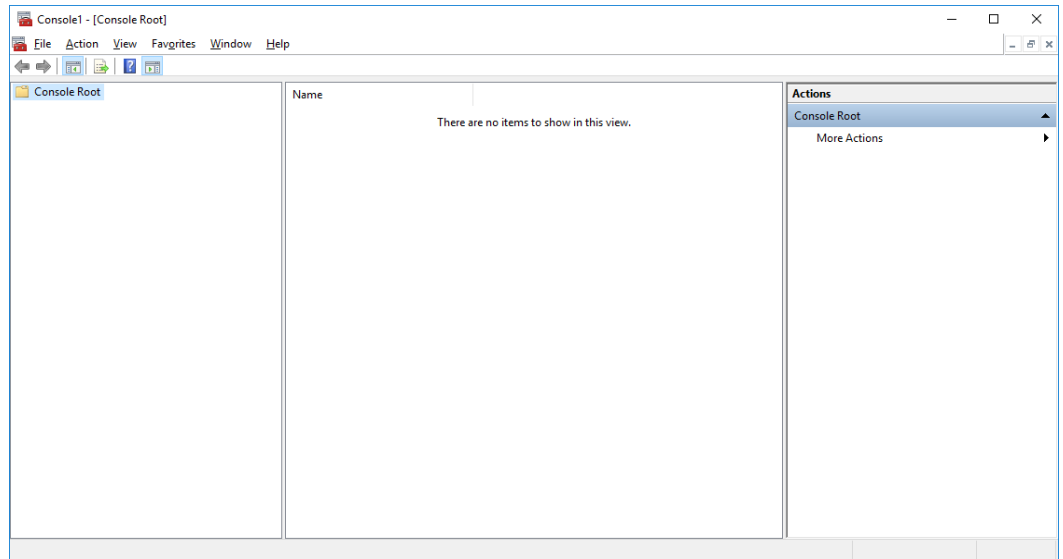
2. From the File menu, select **Add/Remove Snap-in** .

3. In the left column, select **Certification Authority** and click **Add**, and select **Local Computer** and click **Finish** and then **OK.**
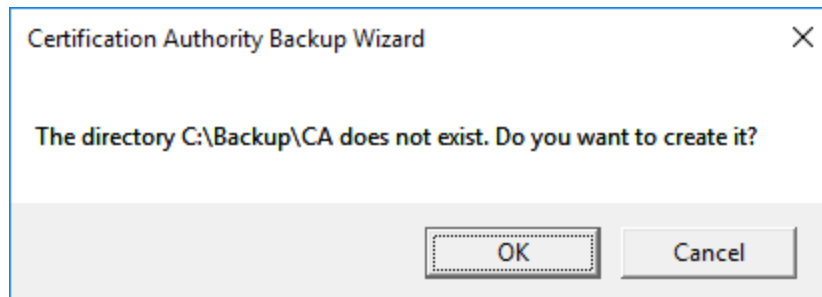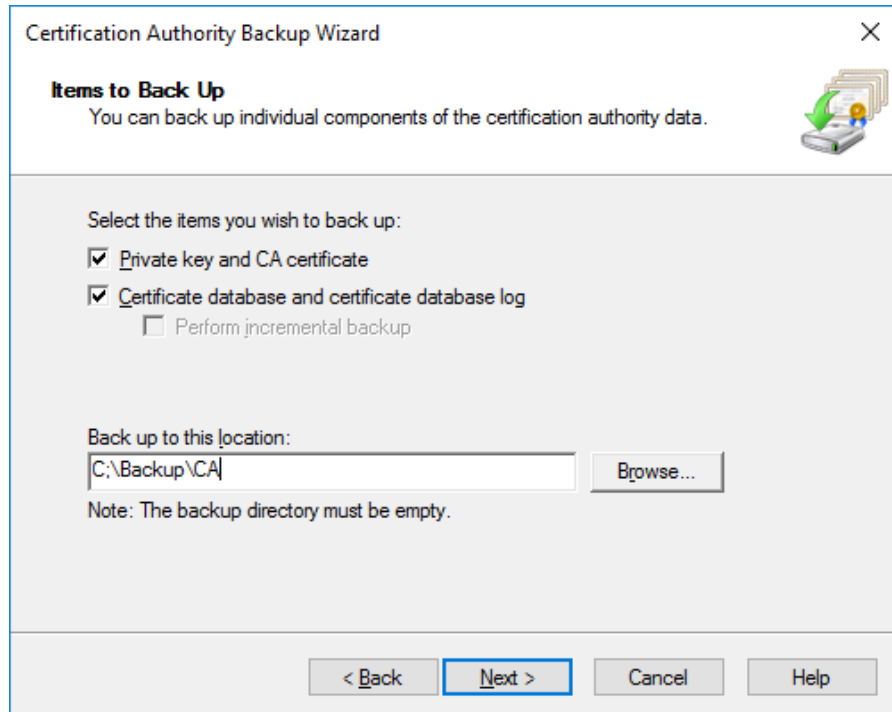
Certification Authority ✕

Select the computer you want this snap-in to manage.

This snap-in will always manage:

◉ Local computer: (the computer this console is running on)

○ Another computer: [   ] Browse...

☐ Allow the selected computer to be changed when launching from the command line. This
only applies if you save the console.

< Back   **Finish**   Cancel   Help

Add or Remove Snap-ins ✕

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificate Templates	Microsoft Cor...
Certificates	Microsoft Cor...
Certification Authority	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Enterprise PKI	Microsoft Cor...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...

Selected snap-ins:

📁 Console Root
    📄 Certification Authority (Local)

Edit Extensions...
Remove
Move Up
Move Down

Add >

Advanced...

Description:
Allows you to configure certification authority properties and to manage certificates issued by this CA.

OK   Cancel

4. In the left hand pane, expand Certification Authority (Local) and then right- click your CA and select **All Tasks** -> **Restore CA**.
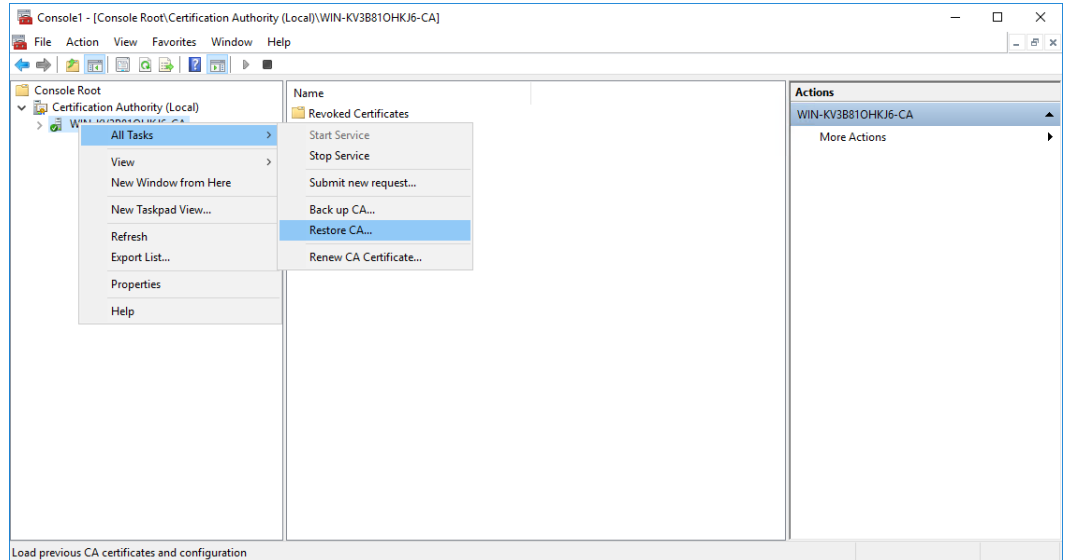
5. If the CA is running, a prompt will be displayed to confirm that it will be stopped, click **OK** .
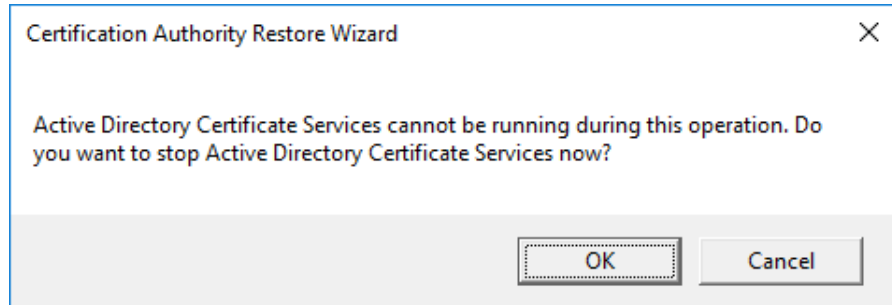
6. At the Welcome to the Certification Authority Restore Wizard, click
   Next.
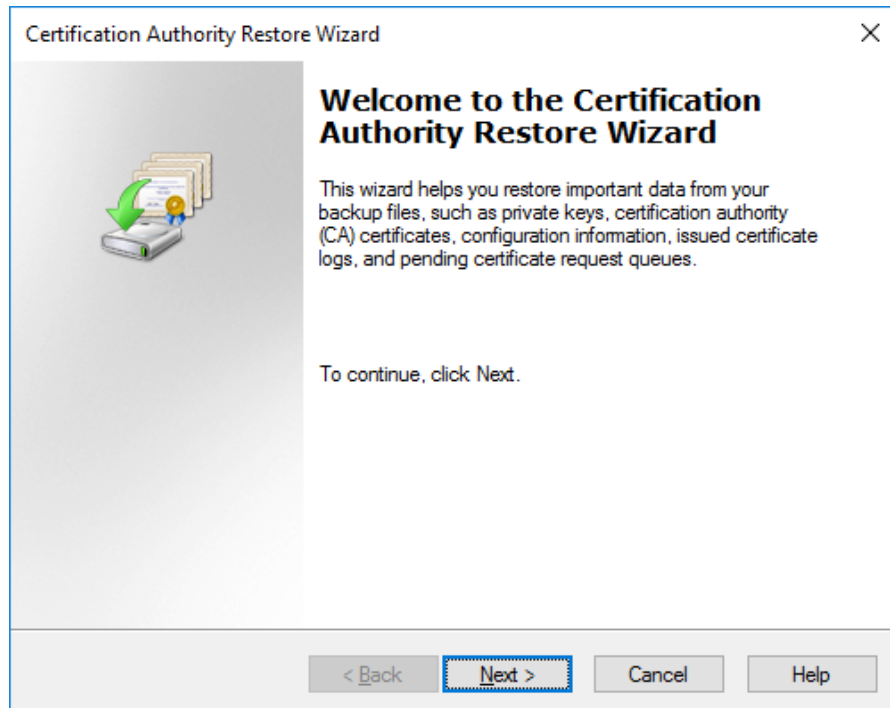
7. Select both **Private key and CA certificate** and **Certificate database and
   certificate database log** and specify a directory to restore the CA,

and click **Next**.
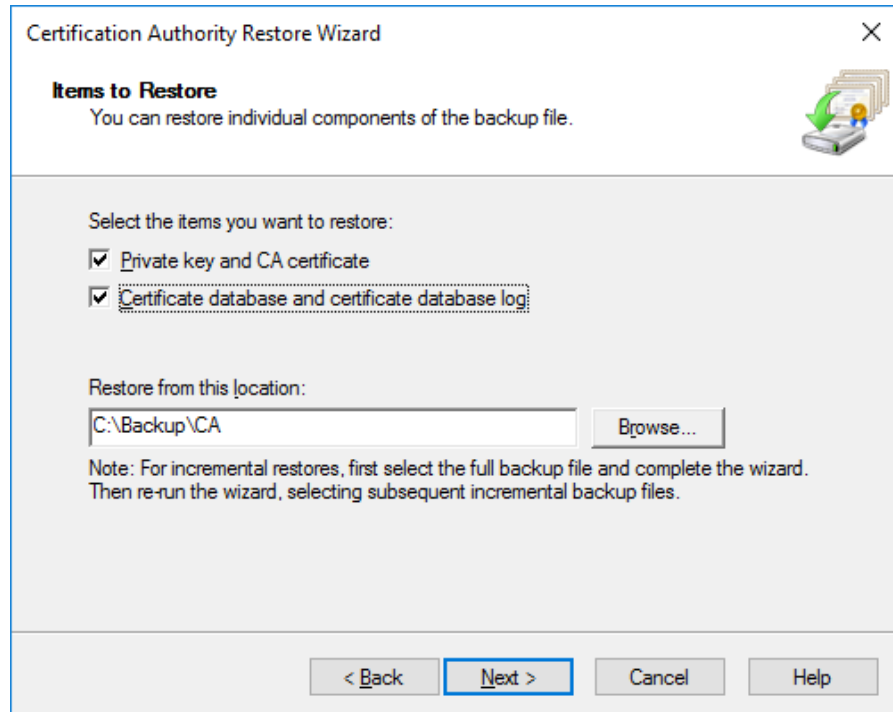
8. At the Provide Password dialog, type the password that was used at step 7 of Backup and click **Next**.
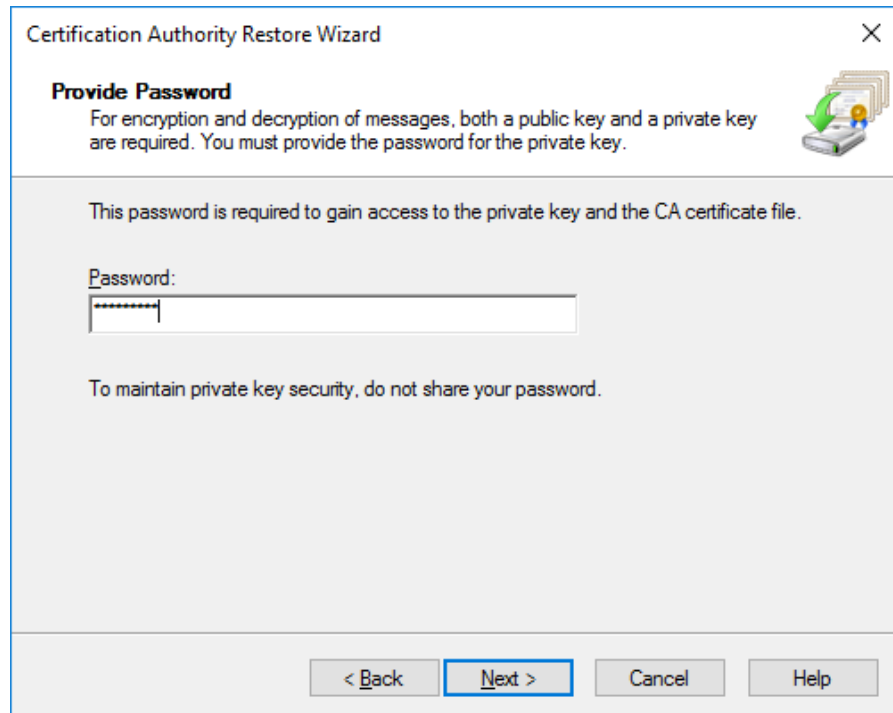
9. Confirm the settings and click **Finish.**
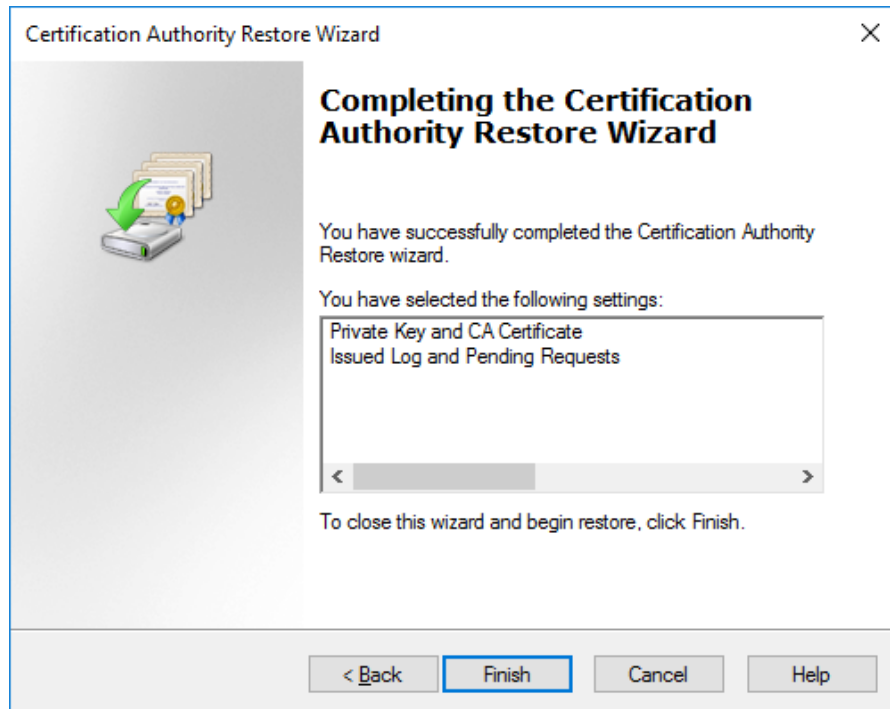
10. Once the restore is complete, click **Yes** to restart the CA.
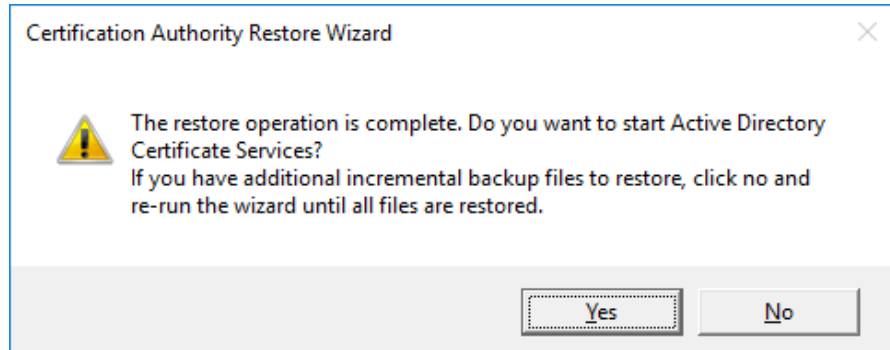
The CA Server has been restored to have the state, starting from the time of the backup is used.

Renewal and revocation of certificates

If the CA Server is installed via the scripts explained in this chapter, the certificates generated for TLS, CMCC and IPsec will be valid for 20 years or the remaining life of the CA root certificate.

CA Root certificate

Based on the install scripts in this chapter, the CA root certificate will be valid for 50 years.

Renewing the CA Root certificate

1. Start the Certificate Management console on the CA Server and in the left pane navigate to your Certification Authority.
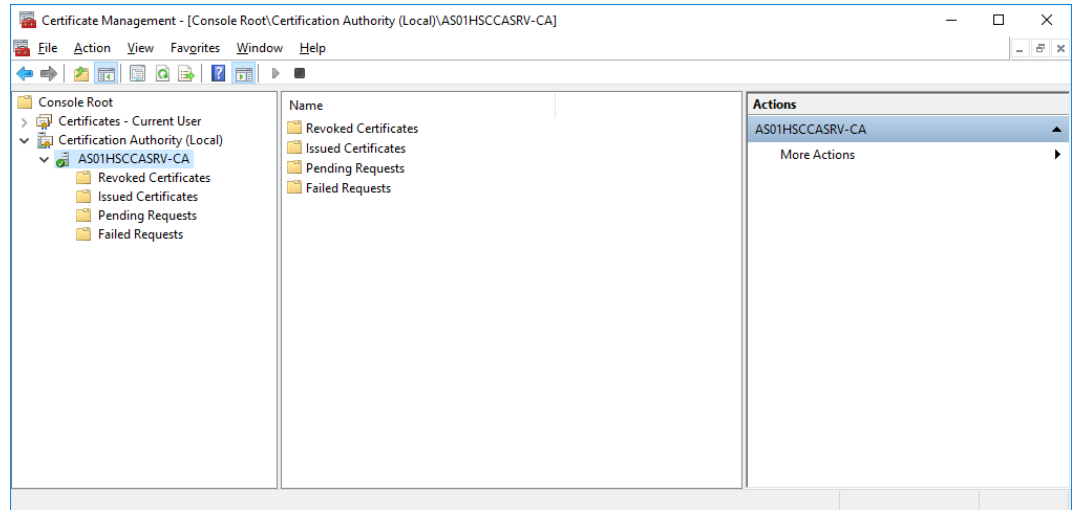
2. Right-click the CA and select **All Tasks-> Renew CA Certificate**.
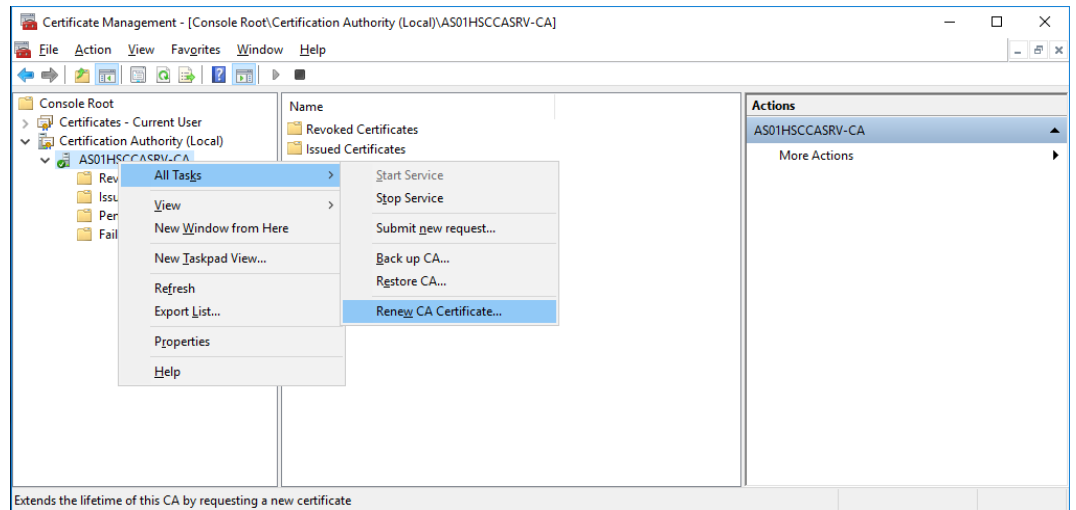
3. At the Install CA Certificate dialog, click **Yes** to stop the Active Directory Certificate Services

Install CA Certificate ✕

Active Directory Certificate Services cannot be running during this operation. Do you want to stop Active Directory Certificate Services now?

Yes   No
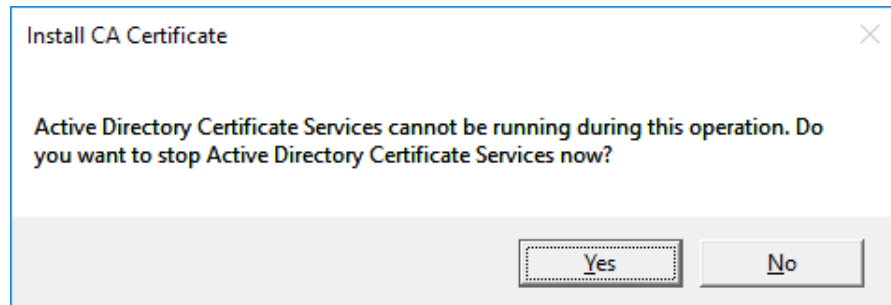
4. At the Renew CA Certificate dialog box, select **No** to re-use the existing CA keys and click **OK**.

Renew CA Certificate ✕

In addition to obtaining a new certificate for your certification authority (CA), you also have the option of generating a new signing key.

You need a new certificate for your CA when:

The lifetime of the certificates you are currently issuing is reduced.

You need a new signing key when:

The signing key is compromised.

You have a program that requires a new signing key to be used with a new CA certificate.

The current certificate revocation list (CRL) is too big, and you want to move some of the information to a new CRL.

Do you want to generate a new public and private key pair? The cryptographic service provider and hash algorithm settings will be preserved. If the existing key length is less than 1024 bits, it may be increased.

○ Yes
◉ No

OK   Cancel

5. The Root certificate will then be renewed and the Active Directory Certificate Services restarted.

PC certificates

Renewal

To renew the CMCC and IPsec certificates, see Creating a certificate for a Windows node to issue and install new certificates for each type for the PC. Once the new certificate has been installed, you can optionally delete the old certificate by right-clicking on it and then click Delete. If the old certificate was in use, deleting it will force the connection to re-negotiate its encryption with the new certificate. Optionally, you could also revoke the certificate at the CA Server once you've deleted it from the PC using it.

To renew the CMCC and IPsec certificates, see Creating a certificate for a Windows node to issue and install new certificates for each type for the PC. Once the new certificate has been installed, you can optionally delete the old certificate by right-clicking on it and then click Delete. If the old certificate was in use, deleting it will force the connection to re-negotiate its encryption with the new certificate. Optionally, you could also revoke the certificate at the CA Server once you've deleted it from the PC using it.

Revocation

If you need to revoke a PC's CMCC or IPsec certificate then, perform the following steps:

1. Start the Certificate Management console on the CA Server and in the left pane navigate to your Certification Authority.
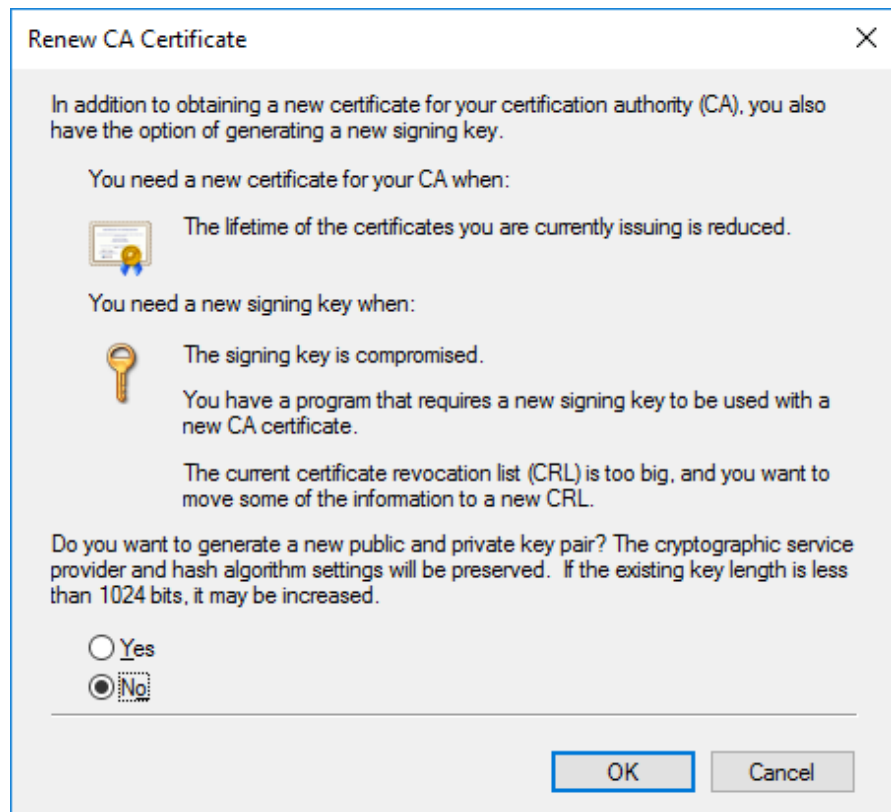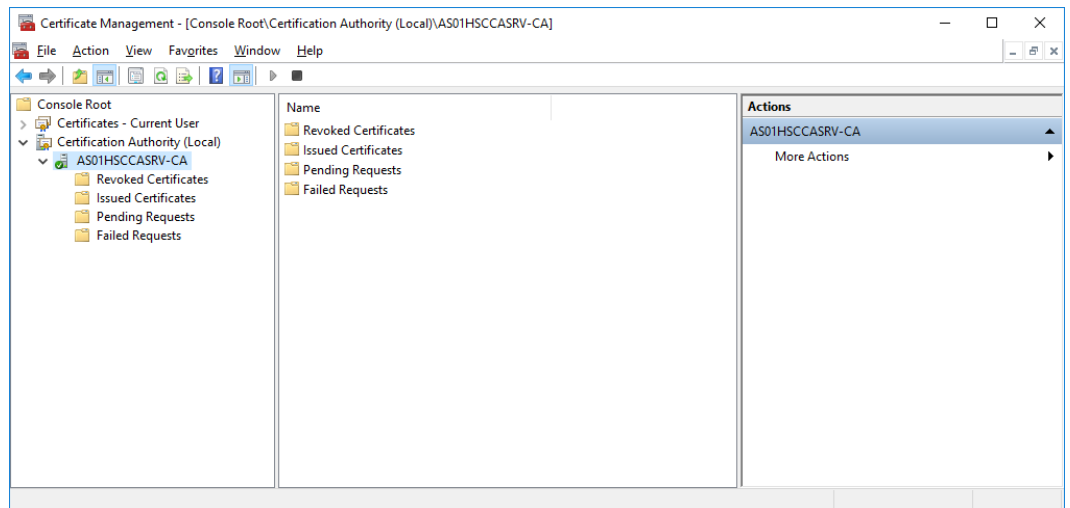
2. Then navigate to Issued Certificates and in the middle pane, search for the certificate you wish to revoke.
   The following are tips to help to find the correct certificate:

    1. The Issued Common Name column contains the name of the computer which the certificate was created for.
    2. If you open a certificate and go to **Details** tab:

        i. A CMCC certificate should:

            - Have the computer name as the CN value in the Subject field
            - Have an Enhanced Key Usage field with value Client Authentication,
            - Have a Key Usage field with value Digital Signature

        ii. A TLS certificate should:

            - Have the computer name as the CN value in the Subject field
            - Have an Enhanced Key Usage field with value Server Authentication,
            - Have a Key Usage field with value Digital Signature

        iii. An IPsec certificate should:

            - Have the computer name as the CN value in the Subject field
            - NOT have an Enhanced Key Usage field at all
            - Have a Key Usage field with values Digital Signature and Key Agreement.

3. Right-click the certificate and select **All Tasks** -> **Revoke Certificate** .
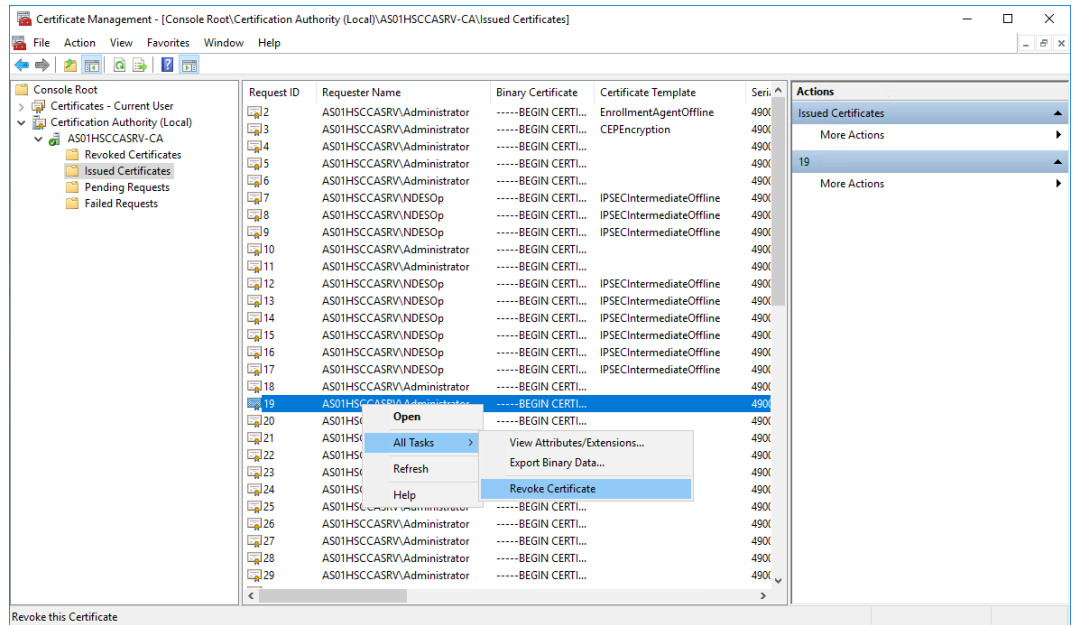
4. From the Certificate Revocation dialog, select an appropriate Reason code and specify the date and time to revoke the certificate from. Note the default setting is the current time.
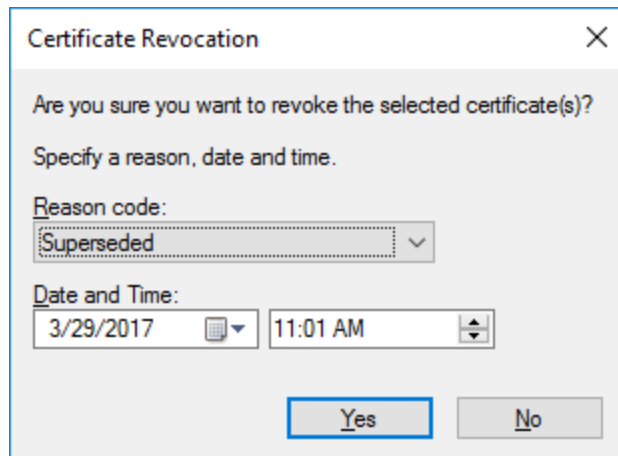
5. Click **Yes** to revoke the certificate, and it revokes the certificate. The certificate is in the Revoked Certificates list for the CA.
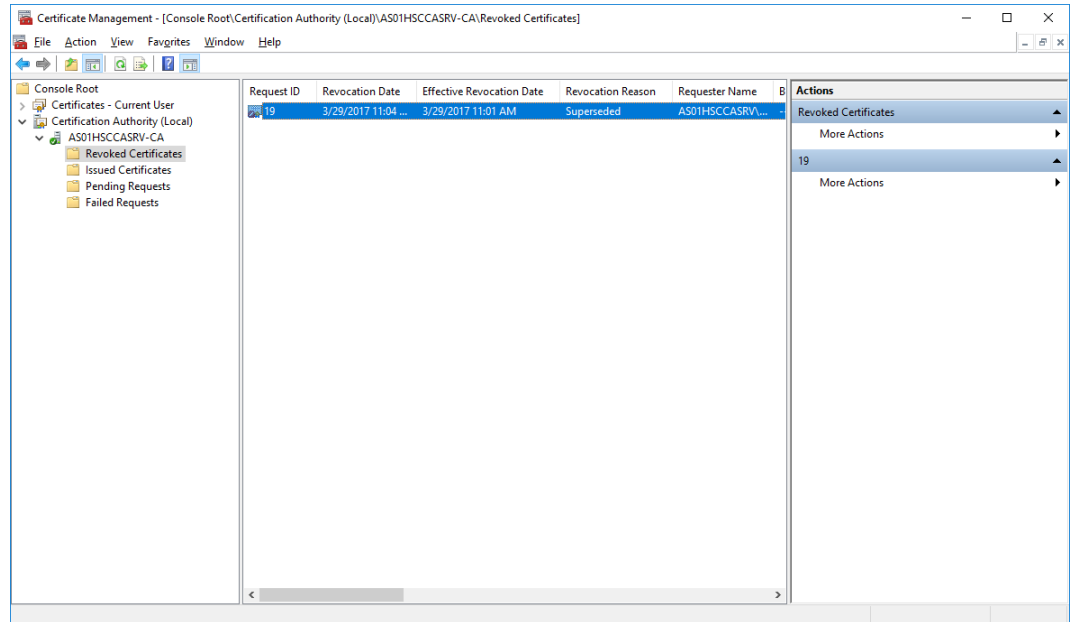
PLC/RTU certificates

Renewal

The built-in Certificate Manager to the PLC/RTU checks the lifetime of its certificate at least once every seven days, and if the CA is available to communicate with, it will automatically renew the certificate with its CA within 90 days of its expiry.

The CMCC tool also provides a manual method to renew the certificate if the CA is not always available. Use the "Renew" button on the "CMProfiles" and "Profiles" menus.

Revocation

If the PLC/RTU certificate is revoked in the CA, it continues to work until the nodes it is connecting to receive an updated CRL from the CA Server. Typically it takes 48 hours for the certificate to be revoke at the CA.

The Certificate Manager on the PLC/RTU retrieves the Certificate Revocation List (CRL) from the CA once every 24 hours if the CA is available. The CA will publish a full CRL once every 30 days and a delta CRL every day. The CRL is valid for up to 30 days past the CRL publish period by the CA Server (30 days publish + 30 days overlap = 60 days CRL validity).

For example, if the CA Server publishes a CRL on September 1st, and then its next CRL on October 1, if the PLC/RTU retrieves the CRL during September, this CRL remains valid until October 31st (30 days after October CRL is published, or 60 days after September CRL was published).

Troubleshooting

If PLC or RTU is not communicating to Experion Server

Disable IPsec on PLC or RTU and Windows, and restart configuration.

See Installing Certificate Manager Configuration Console for more information.

How to reset PLC or RTU for IPsec configuration?

Perform the following steps to reset PLC or RTU for IPsec configuration:

1. Connect the CMCC tool to your PLC or RTU.

2. From the top level menu, type "ResetToDefault" to reset the Certificate Manager in the PLC or RTU. And it resets only the IPsec functionality in the PLC or RTU.

3. Setup and enable IPsec in the PLC or RTU again.See Setup certificates and IPsec policy in PLC/RTU for more information.

   - See Setup certificates and IPsec policy in PLC/RTU for more information.

   - See Enable IPsec policy rules in the PLC/RTU for more information.

How to reset IPsec configuration on Windows?

Perform the following steps to reset IPsec Configuration on Windows:

1. See Disable IPsec policy on PCs for more information.

   See Disable IPsec policy on PCs for more information.

2. Second, Configure IPsec on Windows.

   See Enable IPsec policy on PCs for more information.

Diagnosing IPsec with Network Analysis Software

Network traffic analysis software including WireShark, can be used to help check whether IPsec is being used for communication between the Windows nodes and PLC/RTU. If this software is running on the Experion Server, set a filter for the PLCs/RTUs , on aspect of IP address and viewing traffic to/from that node.

- If clear text is in use, you will see packets marked as "OPCUA" and "TCP" in several packet types between the PC and PLC/RTU.

- If an IPsec session is being established, you can see some packets marked with "ISAKMP" , because the IPsec connection is established.

- And once IPsec communication is established, all packets are marked as "ESP".

If CMCC uploads a large number of policies, the read data from the transport connection can not be received

The default time out value in CMCC is not sufficient for ControlEdge RTU/PLC to handle all of the policies.

Workround:

1. Start a Command Prompt and change to the Certificate Manager Configuration Console (CMCC) folder with the following command (or similar):
   cd \CertMgmt\CertManagerConfigConsole

2. Run the following command:
   CertMngrConfigConsole.exe ip:<CMCCtimeout catimeout:CMCCtimeout> <PLC IP Address>
   <PLC IP Address> is the IP of the PLC/RTU, or the Primary PLC/RTU if using redundant PLCs/RTUs and <CMCCtimeout> is the timeout for the policies.

Window Firewall can not automatically startup after Windows PC reboot

To make the Windows Firewall automatically startup after Windows PC reboot, perform the following steps:
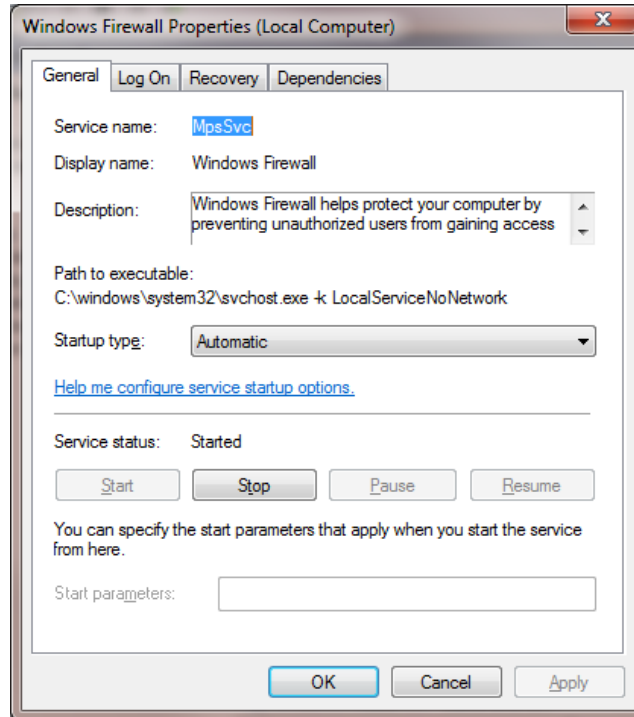
1. To display the Run window, press the Windows logo key + R. And type "SERVICES.MSC" in the Open box and click **OK**.
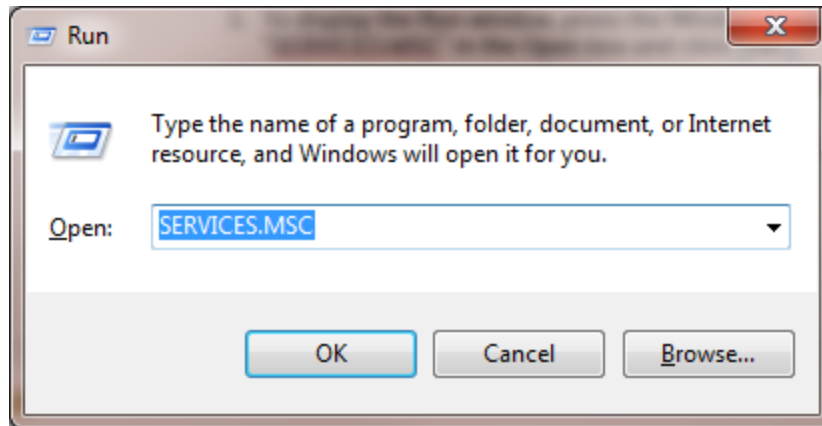
2. In the pop-up Service window, select **Extended** tab, and double-click **Windows Firewall**.
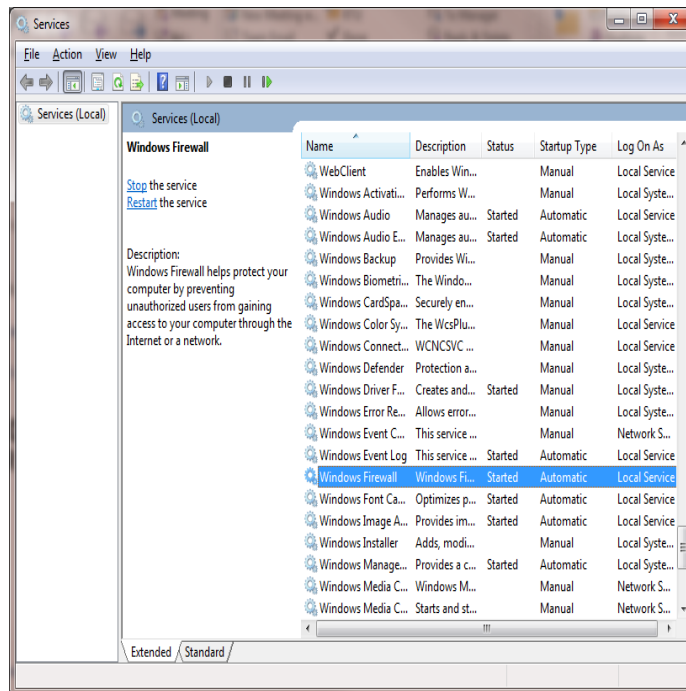
3. In the pop-up Windows Firewall Properties window, select the General tab, select **Automatic** in **Statup type** drop-down list and select **OK**.

NOTICES

Trademarks

Experion® is a registered trademark of Honeywell International, Inc.

ControlEdge™ is a trademark of Honeywell International, Inc.

OneWireless™ is a trademark of Honeywell International, Inc.

Other trademarks

Microsoft and SQL Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Trademarks that appear in this document are used only to the benefit of the trademark owner, with no intention of trademark infringement.

Third-party licenses

This product may contain or be derived from materials, including software, of third parties. The third party materials may be subject to licenses, notices, restrictions, and obligations imposed by the licensor. The licenses, notices, restrictions and obligations, if any, may be found in the materials accompanying the product, in the documents or files accompanying such third party materials, in a file named third_party_licenses on the media containing the product, or at http://www.honeywell.com/en-us/privacy-statement.

Documentation feedback

You can find the most up-to-date documents in the Support section of the Honeywell Process Solutions website at: https://process.honeywell.com/us/en/support/product-documents-downloads

If you have comments about Honeywell Process Solutions documentation, send your feedback to: hpsdocs@honeywell.com

Use this email address to provide feedback, or to report errors and omissions in the documentation. For immediate help with a technical problem, contact HPS Technical Support through your local Customer Contact Center, or by raising a support request on the Honeywell Process Solutions Support website.

How to report a security vulnerability

For the purpose of submission, a security vulnerability is defined as a software defect or weakness that can be exploited to reduce the operational or security capabilities of the software.

Honeywell investigates all reports of security vulnerabilities affecting Honeywell products and services.

To report a potential security vulnerability against any Honeywell product, please follow the instructions at:

https://www.honeywell.com/en-us/product-security.

Support

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC). To find your local CCC visit the website, https://process.honeywell.com/us/en/contact-us.

Training classes

Honeywell holds technical training classes that are taught by process control systems experts. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.