Honeywell

Experion PKS

Secure Communications User's Guide

EPDOC-X270-en-431A
June 2014

Release 431

Honeywell

Document	Release	Issue	Date
EPDOC-X270-en-431A	431	0	June 2014

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

The Secure Communications User’s Guide describes how to enhance the security of communication between nodes in an Experion system.

Revision history

Revision	Date	Description
A	June 2014	Initial version

Intended audience

This guide is intended primarily for Security Administrators, Product Administrators, and System Engineers who are responsible for administration and maintenance of Secure Communications.

License

The Secure Communications feature is licensed. For more information, contact your local Honeywell sales representative, Honeywell Process Solutions Customer Contact Center (CCC), or Honeywell Technical Assistance Center (TAC).

Prerequisite skills

You must be familiar with the Experion system topology and system security concepts. You must also have experience of working in a Microsoft Windows environment.

Related documents

You may also refer to the following related Experion documents.

Document	Description
Overview	Provides a comprehensive overview of Experion, including basic concepts and terminology.
Experion Network and Security Planning Guide	Provides information about Experion network and security information applicable to Experion.
Software Installation User's Guide	Describes how to perform a clean install of Experion servers and station nodes.
Experion General Release Software Change Notice	Provides information about new features, resolved PARs, issues, special considerations, and last minute documentation updates in Experion.

2 Introduction

Related topics

“About Secure Communications” on page 8
“Secure Communications in Experion” on page 9
“Secure Communications components” on page 10
“Secure Communications terms and definitions” on page 12

2.1 About Secure Communications

Secure Communications overview

With Secure Communications, Experion introduces the encrypted communication technology in Experion to minimize security vulnerabilities in Experion communications. It provides a common infrastructure for all Experion nodes to communicate using cryptographic (encryption, authentication, and message integrity protection) communication technology.

With Secure Communications you can mitigate the following risks.

- Man-in-the-middle (MITM) attacks on Level 2 of the Experion network.
- Disclosure of information in communication between secured nodes.
- Rogue or unauthorized devices added to Level 2 of the Experion network.

In Secure Communications, configuration tasks such as, setting the security policy and administration are restricted to the Security Administrator role to ensure security.

Secure Communications features

Some of the Secure Communications features include:

- Establishment of trust between nodes using certificates issued from a central certificate authority.
- Authentication and message integrity between communicating partners.
- Encryption of data sent on the network.
- Applicable to both physical and virtual Experion nodes.
- Deployment of security policies while the system is on-process.

2.2 Secure Communications in Experion

Experion nodes supporting Secure Communications

The following Experion nodes support Secure Communications.

Node level in Experion topology	Experion node
Level 2	• Experion Server • Experion Console Station • Experion Flex Station • Experion Console Extension Station
Level 1	• C300–50 ms controller

Note

Flex Station on only Level 2 (L2) of Experion topology is supported.

Communication between Experion nodes supporting Secure Communications

The Experion nodes supporting Secure Communications communicate using both Cleartext and Encryption communication technology.

Encryption mode of communication is supported between the following Experion nodes.

- Experion Server and Experion Server
- Experion Server and Experion Console Station
- Experion Server and Experion Flex Station
- Experion Server and Experion Console Extension Station
- Experion Console Station and Experion Console Station
- C300 controller and Experion Server
- C300 controller and Experion Console Station
- Experion Console Station and Experion Console Extension Station

Communication between a secure node and a non-secure node

A secure node uses Encryption for communication with secure nodes of the zone and uses Cleartext for communication with nodes that do not support Secure Communications (within or outside the Security Zone). For example, C300 controller uses Encryption for communication with Server and Console Stations, and uses Cleartext with other C300 controllers and FIMs.

Note

- As Secure Communications is not supported across subnets, Flex Stations connected to Servers across subnets use Cleartext for communication with such Servers.
- If a Flex Station supporting Secure Communications is moved from one cluster to another, it must be added again as a new node.
- If Flex Station and Console Station are both available on a single node, then the node must only be secured once in the security zone.

Supported protocols

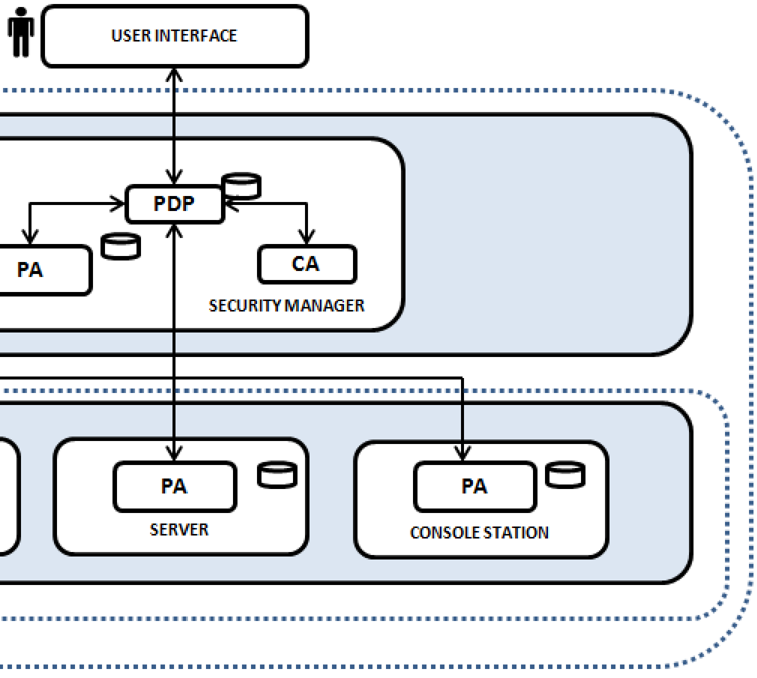
The secure connection between the Experion nodes affects all point to point communication protocols like TCP, and point-point UDP. However, broadcast/multicast protocols are not in the scope of Secure Communications. In Experion, CDA and PDA are examples of protocols that are secured, while FTE diagnostic communications is not secured.

2.3 Secure Communications components

Secure Communications components are installed on the following supported Experion nodes.

Experion node	Secure Communications components
• Server	• Policy Decision Point (PDP) • Certificate Authority (CA) • Policy Agent (PA)
• Experion Console Station • Experion Flex Station • Experion Console Extension Station • C300-50 ms controller	• Policy Agent (PA)

The following is an illustration of the Secure Communications architecture.



The Secure Communications application can be accessed and launched from the Configuration Studio. The Secure Communications components collectively support the configuration, storage, and delivery of certificates and policies to the nodes selected to be secured. The Security Administrator can select a node to act as the Security Manager. The Secure Communications configuration for the entire Security Area is persistent in the Security Manager.

- **Security Manager**

  A node (usually, an Experion Server) is available as a Security Manager when the Secure Communications components, the Policy Decision Point (PDP) and the Certificate Authority (CA) are installed on the node. The PDP is responsible for storing the user configuration data. It is also responsible for distributing node certificates and node policies to the node that sends a request to be secured. The CA is responsible for generating the node certificates for the node to be secured.

- **Security Agent**

  A node is available as a Security Agent when the Secure Communications component, the Policy Agent (PA) is installed on the node. The PA is responsible for establishing certificates and policies for the node on which it resides.

- **Security Area and Security Zones**

  In Secure Communications, a Security Area is a collection of Experion nodes and networks that share similar requirements for protection of information. A Security Area can have multiple Security Zones. A Security Zone is a group of nodes in a Security Area, for which a single policy is configured. Security Zones are automatically established based on the arrangement of nodes in FTE communities and subnets. Secure Communication relationships are not supported between Security Zones.

2.4 Secure Communications terms and definitions

The following terms and definitions associated with Secure Communications are used throughout this guide in the following context.

Secure Communications terminology

Term	Definition
Certificate	A certificate is an electronic document that uses a digital signature to bind a public key with an identity. Experion nodes obtain a certificate signed by the Certificate Authority that is used to represent the nodes identity.
Certificate Authority (CA)	A Certificate Authority is an entity that issues digital certificates. In Experion, there is a single Certificate Authority for each Security Area.
Internet Key Exchange (IKE)	Internet Key Exchange is a protocol to establish secure associations in IPsec protocol suite. IKE uses X.509 certificates for authentication and Diffie-Hellman key exchange to set up shared session secret from which cryptographic keys are derived.
Internet Protocol Security (IPsec)	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
National Security Agency (NSA) Suite B cryptography	Suite B is a set of cryptographic algorithms promoted by the National Security Agency (NSA) to serve as an interoperable cryptographic base for both unclassified and classified information.
Policy	A policy defines how two nodes will communicate with each other.
Policy list	The policy list for a node is a set of policies in accordance with which a node communicates with other nodes.
Policy Decision Point (PDP)	The Policy Decision Point is a component of the Experion Secure Communications architecture responsible for storing the Secure Communications configuration settings and sending certificates and policies to Policy Agents.
Policy Agent (PA)	The Policy Agent is a component of the Experion Secure Communications architecture responsible for establishing certificates and policies for the node on which it resides.
Policy Enforcement Point (PEP)	The Policy Enforcement Point is a component of the Experion Secure Communications architecture responsible for enforcing the configured policies. The TCP/IP communication stack is the Policy Enforcement Point in both C300 controller and Windows nodes.
Security Area	A security area is a collection of Experion nodes and networks that share similar requirements for the protection of information and to which secure communications settings are applied. A Security Area contains a single Security Manager, and is made up of one or more Security Zones.
Security Manager	An Experion node is available as a Security Manager when Policy Decision Point (with a configuration database), Certificate Authority, and Policy Agent components are installed on the node. The node is activated as a Security Manager when you run the Security Manager routing setup utility tool.
Security Manager Proxy	An Experion node is available as a Security Manager Proxy when Policy Decision Point (without a configuration database) and Policy Agent components are installed on the node. The node is activated as a Security Manager Proxy when you run the Security Manager routing setup utility tool.
Security Agent	A Security Agent contains the Policy Agent, a Secure Communications component installed during the Experion installation.
Security credentials	Security credentials contain certificates and policies.

Term	Definition
Security level	The security level is a configuration setting that determines how the nodes of a zone communicate with each other. The options available are Cleartext (standard communication) and Encrypted (nodes authenticated to establish trust and data is encrypted).
Security Zone	A Security Zone is a group of nodes in a Security Area, for which a single policy is configured.
Secure Communications User Interface (UI)	Provides interfaces for managing nodes in the Security Area and configuring policies.
System Server	The server that hosts the EMDB.
X.509	X.509 is an International Telecommunication Union (ITU) standard for public key infrastructure (PKI).

3 Planning and installation

The following topics describe how to plan and install Secure Communications in an Experion network.

Related topics

“Planning for Secure Communications” on page 16
“Installing Secure Communications” on page 27

3.1 Planning for Secure Communications

Prerequisites

- Ensure that you install the supported version of CISCO switches. Refer to the Experion General Release Software Change Notice for the supported version.

  Note

  The supported version of CISCO switch.ensures that the secured traffic is properly prioritized.

- Ensure that you install the supported version of Control Firewall 9 (CF9). Refer to the Experion General Release Software Change Notice for the supported version.

  Note

  The supported version of CF9 ensures the successful deployment of configured policies. It also ensures that the secured traffic is properly prioritized.

- After completing the Experion installation or migration, ensure that the Experion system time synchronization is implemented using Network Time Protocol (NTP) or Precision Time Protocol (PTP). The accuracy of synchronized time between the Experion nodes is important when the policies are deployed and activated. Two nodes need to activate a new policy at nearly the same time in order to avoid interruption in communication. For more information to implement NTP, see the following Experion guides.
  - *Experion Server and Client Planning Guide*
  - *Experion Supplementary Installation Tasks Guide*
- Windows nodes with multiple network adaptors are not supported in Experion networks, and hence are not supported by Secure Communications. This point is reinforced here to ensure that Windows nodes to be secured do not communicate with multiple IP addresses. Dual connections to FTE green and yellow cables are supported in Experion and with Secure Communications too.
- Secure Communications supports only C300-50ms controller. The C300-20ms controller is not supported.

The Secure Communications feature is integrated with Experion and when you install or migrate to Experion, Secure Communications is installed on supported Experion nodes. However, you must set up Secure Communications to use this feature. Before you set up the Secure Communications feature installed on the Experion nodes, it is recommended to perform the following tasks.

Perform the following tasks while planning for Secure Communications.

- “Assign the Security Administrator role” on page 16
- “Identify the Security Area” on page 17
- “Identify locations for Security Manager and Security Manager Proxy(ies)” on page 17
- “Acquire and install the requisite Secure Communications license” on page 18
- “Security Manager routing setup utility” on page 18
- “Guidelines to define Security Area and Security Zone” on page 19
- “Evaluate impact on Windows nodes and C300 controllers” on page 24

3.1.1 Assign the Security Administrator role

A new role, *Security Administrator* is added to the Experion security model.

Role	Description
Security Administrator	Configure and maintain Secure Communications

For more information about Experion security model, see the *Network and Security Planning Guide*.

The Security Administrator is responsible for configuration and maintenance of the Secure Communications. The person assigned the role of Security Administrator should be familiar with the system topology, Windows node names, IP address assignments, and system security objectives.

One of the following Windows group is used for assigning user accounts to Security Administrator role.

Role	Domain account group	Local account group
Security Administrator	SecureComms Administrators	Local SecureComms Administrators

After the Security Administrator is identified, perform the following tasks to provide access to Secure Communications user interface.

- The Windows account of the responsible individual must be assigned to the appropriate SecureComms Administrators or Local SecureComms Administrators groups.
- On all Experion clusters participating in Secure Communications, using Configuration Studio, select **Configure operators and Windows group accounts**. Add a new entry of type ‘Windows Group’ with the Group name ‘Local SecureComms Administrators’ with Domain left blank.

The Security Administrator is responsible for the following tasks.

Task	**Description/Reference**
Managing Security Area • Initialize the Security Area • Rename the Security Area • Rename Security Zones	For information about these tasks, see “Initializing the Security Area” on page 33.
Configuring nodes • Secure nodes • Exempt nodes • Unassign nodes • Discard nodes	For information about these tasks, see “Configuring nodes in the Security Zone” on page 38.
Setting the security policy	For information about this task, see “Setting security policy for the Security Zone” on page 44.
• Performing Security Manager backup and restore **Attention** Ensure to take a backup of the Security Manager node after every session of Secure Communications configuration update. • Resynchronize the Security Area	For information about ‘Performing Security Manager backup and restore’, see “Node maintenance” on page 46. For information about ‘Resynchronize the Security Area’, see “Initializing the Security Area” on page 33.

3.1.2 Identify the Security Area

A Security Area can include multiple Experion clusters as defined by the System Server and the scope of the Enterprise Model Database (EMDB). It is recommended to define the scope of the Security Area as big as possible, so that all planned Secure Communications configurations can be established. The Security Area is implemented in the Experion system when you run the Security Manager routing setup utility tool.

3.1.3 Identify locations for Security Manager and Security Manager Proxy(ies)

Each Security Area has one Security Manager that is responsible for providing the certificates to the nodes and securing the nodes in the Security Zones. Only one Security Manager is allowed in a Security Area.

Following are the recommended guidelines to identify the node to act as the Security Manager.

- The node type must be an Experion Server (ESV).
- The node that hosts the Security Manager must be accessible to all the Level 2 Experion Server nodes within the Security Area.
- Preferably select the System Server that hosts Enterprise Model Database (EMDB) (though this is not mandatory).
- For redundant System Servers or Experion Servers, ensure that you select Server B (secondary server) to be the Security Manager from the redundant pair. Note that the Security Manager function itself is non-redundant.

An Experion node is available as a Security Manager Proxy when the Policy Decision Point (without a configuration database) and Policy Agent components are installed on the node. A Security Manager Proxy supports communication between the Security Manager and the nodes in a Security Area when the Security Manager and the node being secured are in two separate FTE communities or network subnets.

The Security Manager Proxy and the Security Manager Proxy (alternate) provide two separate paths of communication to the Security Manager for a node trying to communicate with the Security Manager.

The Security Manager and Security Manager Proxy role selection is implemented in the Experion system when you run the Security Manager routing setup utility tool.

3.1.4 Acquire and install the requisite Secure Communications license

Secure Communications is a separately licensed Experion system option. Model numbers are provided for Windows nodes in counts of 10 and for embedded nodes including C300 controllers in counts of 1. Ensure that you have the requisite licenses for the nodes you plan to secure. Secure Communications licensing for all Windows and embedded nodes in a Security Area are installed on the Experion Server with the Security Manager role. Secure Communication licenses are not required on any other Experion Server in the Security Area.

If Secure Communications is used on one node of a redundant Server or embedded node pair, then licenses must be installed on both partners of the redundant pair. The system counts the number of Windows nodes and C300 controllers that are secured and only permits the number that is licensed.

- If you do not have the requisite license for the Secure Communications feature and, try to access the Secure Communications option on the Configuration Studio, a message informs that the Secure Communications option is not licensed.
- If you have the requisite license for the Secure Communications feature, you can view the license details on the Secure Communications user interface in Configuration Studio. The available licenses for the Windows nodes and controllers are seen in a read-only format.
- When you upgrade your license, you can refresh and view the updated license details.

3.1.5 Security Manager routing setup utility

When you install Experion on the Experion nodes, the Secure Communications components are also installed. After installation of Experion and before the Secure Communications configuration is established, the Security Manager routing setup utility must be run on every Windows node that is intended to be part of the Security Area. The utility provides the IP addresses of the Security Manager and the Security Manager Proxies to the Windows nodes and C300 controllers (from BOOTP server) within a Security Area.

It is mandatory to adhere to the following rules while assigning the Security Manager and Security Manager Proxy roles to the nodes.

- If a Security Zone contains the Security Manager, the nodes in the Security Zone must not use the Security Manager Proxies. All nodes in Security Zone must use the IP Address of the Security Manager for their proxy configuration.
- The Security Manager role is assigned to the Server B (secondary server) of a redundant server pair.

- The Security Manager Proxy (and alternate) nodes are established for each Experion cluster in the Security Zones that do not contain the Security Manager. Ensure that every node in that Security Zone is routed through the Security Manager Proxy.
- The FTE communities with more than one Experion cluster, must enable the BOOTP process on Experion Server (non-redundant server) or Experion Server pair (redundant servers) of only ONE cluster.

  Although using multiple BOOTPs in a multiple cluster FTE community is allowed, it is recommended to use a single BOOTP, so that potential mismatches are avoided. If multiple BOOTPs and multiple Security Manager Proxies are deployed in a multiple cluster FTE community, then it is difficult to determine which Security Manager Proxy is used for each C300 controller. When multiple BOOTPs are enabled, all BOOTPs respond to a C300 controller's request and the C300 controller uses the information from the first response. If you make changes to the nodes that are secured in such an environment, the changes may not be deployed properly if the routing paths are broken.

  With Secure Communications, it is important to follow the suggested best practice of using a single BOOTP in a multiple-cluster FTE community. This ensures that all C300 controllers in the FTE community use the BOOTP-enabled servers in that cluster as the Security Manager Proxy and Security Manager Proxy alternate.

The following information is required when you run the Security Manager routing setup utility.

On an Experion Server node	On a Console Station
• Security Manager IP Address • Security Manager Proxy IP Address • Security Manager Proxy IP Address (alternate)	• Security Manager Proxy IP Address • Security Manager Proxy IP Address (alternate)

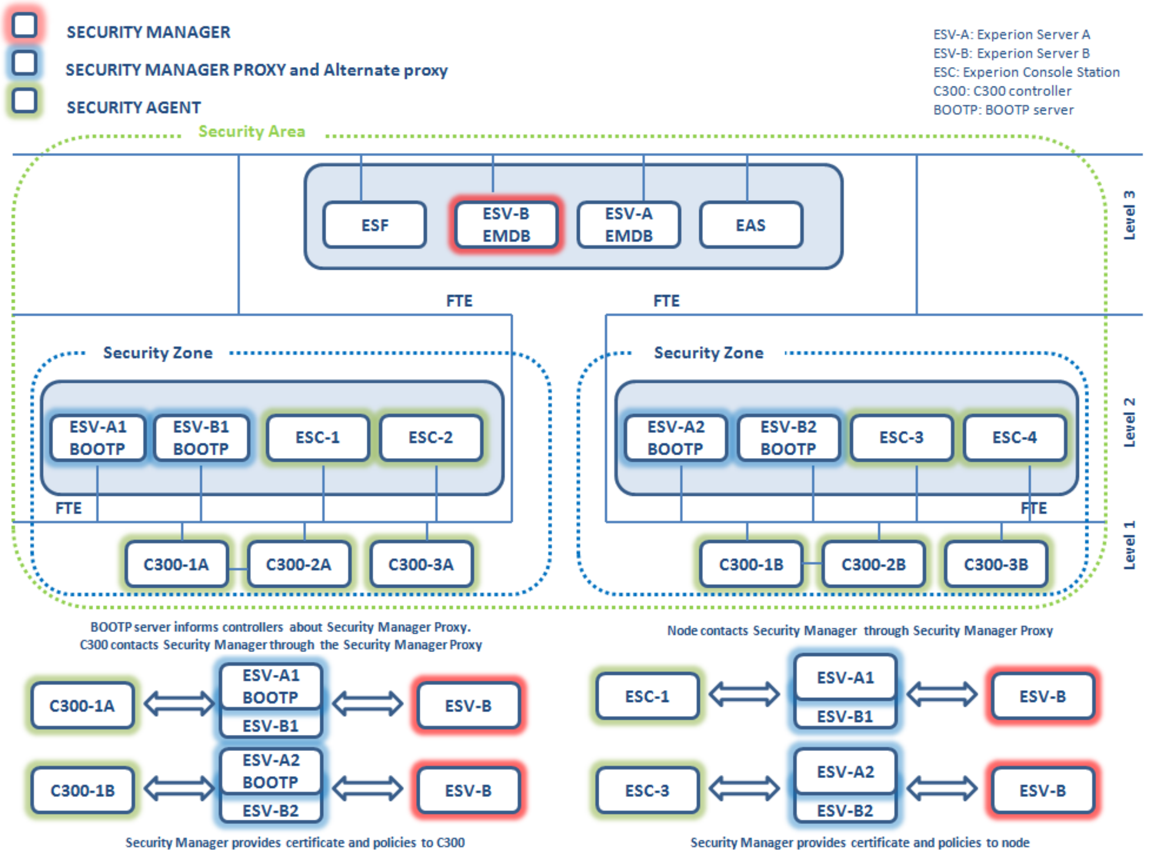
For more information about setting up Secure Communications, see “Installing Secure Communications” on page 27.

For more information about the IP Addresses to be added for the Security Manager routing setup utility, see “Guidelines to define Security Area and Security Zone” on page 19.

3.1.6 Guidelines to define Security Area and Security Zone

Following are a few example Experion topologies that illustrate how the Security Manager and the Security Manager Proxy are assigned to nodes in a Security Area.

Experion topology with Security Manager at Level 3 and two FTE communities



The illustration displays an Experion topology where the Security Manager is located at Level 3 on a System Server that hosts EMDB. Each FTE community contains a Security Manager Proxy and Security Manager Proxy (alternate). The BOOTP is enabled in Server pair of each FTE community.

If the Security Manager is hosted on a Level 3 node, then the Security Administrator must ensure that the Security Manager Proxies are located on Level 2 of the topology. The Security Agent is routed through the Security Manager Proxy to communicate with the Security Manager. The C300 controllers locate the Security Manager after receiving the information from the BOOTP server.

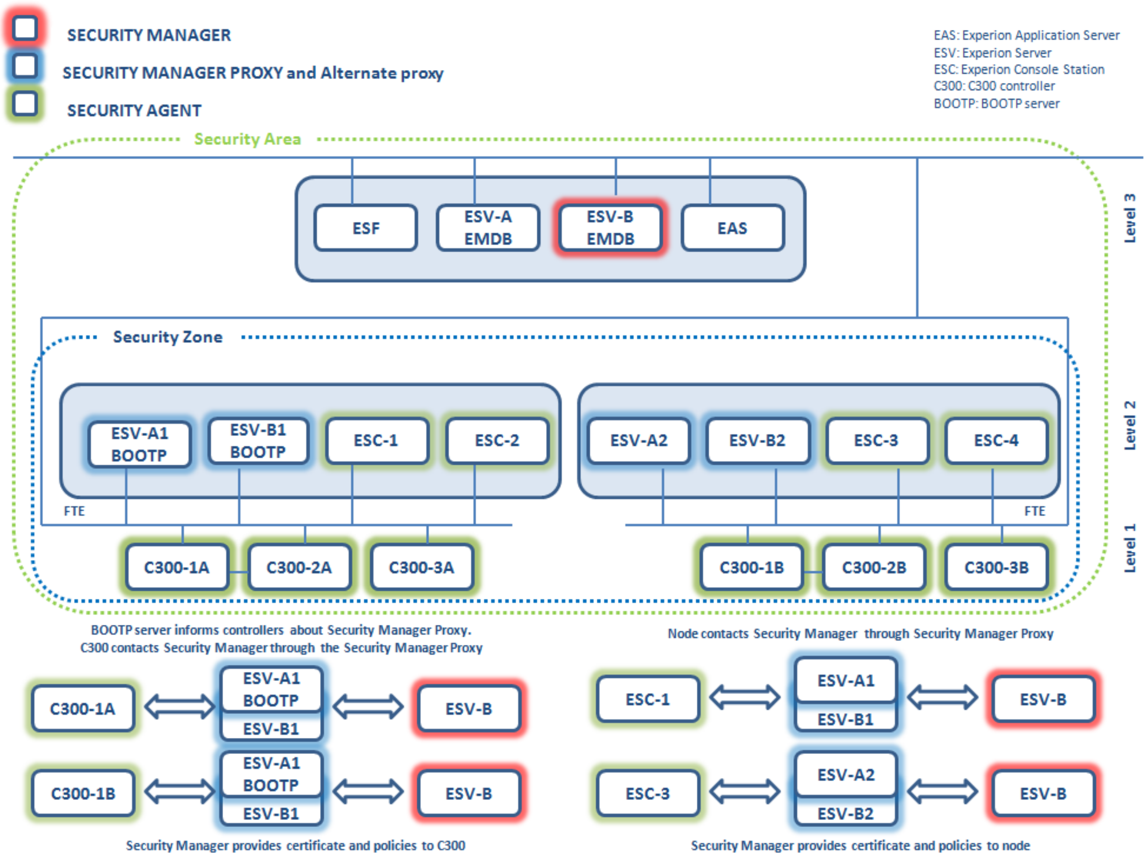
In such a scenario, the IP Addresses for the Security Manager and the Security Manager Proxies are added to the Security Manager routing setup utility as provided in the following tables for Servers and Console Stations.

The Experion server at Level 3 is named as ESV-B. The Experion redundant servers in the left cluster are named as ESV-A1 and ESV-B1. The Experion redundant servers in the right cluster are named as ESV-A2 and ESV-B2.

Security Manager routing setup utility field	**Servers**				
	ESV-A1	**ESV-B1**	**ESV-A2**	**ESV-B2**	**ESV B**
Security Manager IP Address	ESV-B IP address	ESV-B IP address	ESV-B IP address	ESV-B IP address	ESV-B IP address
Security Manager Proxy IP Address	ESV-A1 IP address	ESV-B1 IP address	ESV-A2 IP address	ESV-B2 IP address	ESV-B IP address
Security Manager Proxy IP Address (alternate)	ESV-B1 IP address	ESV-A1 IP address	ESV-B2 IP address	ESV-A2 IP address	0.0.0.0

Security Manager routing setup utility field	**Console Stations**			
	ESC-1	**ESC-2**	**ESC-3**	**ESC-4**
Security Manager Proxy IP Address	ESV-A1 IP address	ESV-A1 IP address	ESV-A2 IP address	ESV-A2 IP address
Security Manager Proxy IP Address (alternate)	ESV-B1 IP address	ESV-B1 IP address	ESV-B2 IP address	ESV-B2 IP address

Experion topology with Security Manager at Level 3 and one FTE community



SECURITY MANAGER
SECURITY MANAGER PROXY and Alternate proxy
SECURITY AGENT
EAS: Experion Application Server
ESV: Experion Server
ESC: Experion Console Station
C300: C300 controller
BOOTP: BOOTP server
Security Area
ESF
ESV-A EMDB
ESV-B EMDB
EAS
Level 3
Security Zone
ESV-A1 BOOTP
ESV-B1 BOOTP
ESC-1
ESC-2
ESV-A2
ESV-B2
ESC-3
ESC-4
Level 2
FTE
FTE
C300-1A
C300-2A
C300-3A
C300-1B
C300-2B
C300-3B
Level 1
BOOTP server informs controllers about Security Manager Proxy.
C300 contacts Security Manager through the Security Manager Proxy
Node contacts Security Manager through Security Manager Proxy
C300-1A
ESV-A1 BOOTP
ESV-B1
ESV-B
C300-1B
ESV-A1 BOOTP
ESV-B1
ESV-B
ESC-1
ESV-A1
ESV-B1
ESV-B
ESC-3
ESV-A2
ESV-B2
ESV-B
Security Manager provides certificate and policies to C300
Security Manager provides certificate and policies to node

The illustration displays a system where the Security Manager is located at Level 3 on a System Server that hosts EMDB. It is a single FTE community and contains a Security Manager Proxy and Security Manager Proxy (alternate) pair for each of the two Experion clusters in the community. The BOOTP is enabled on Server pair of only one cluster in the FTE community.

In such a scenario, the IP Addresses for the Security Manager and the Security Manager Proxies are added to the Security Manager routing setup utility as provided in the following tables for Servers and Console Stations.

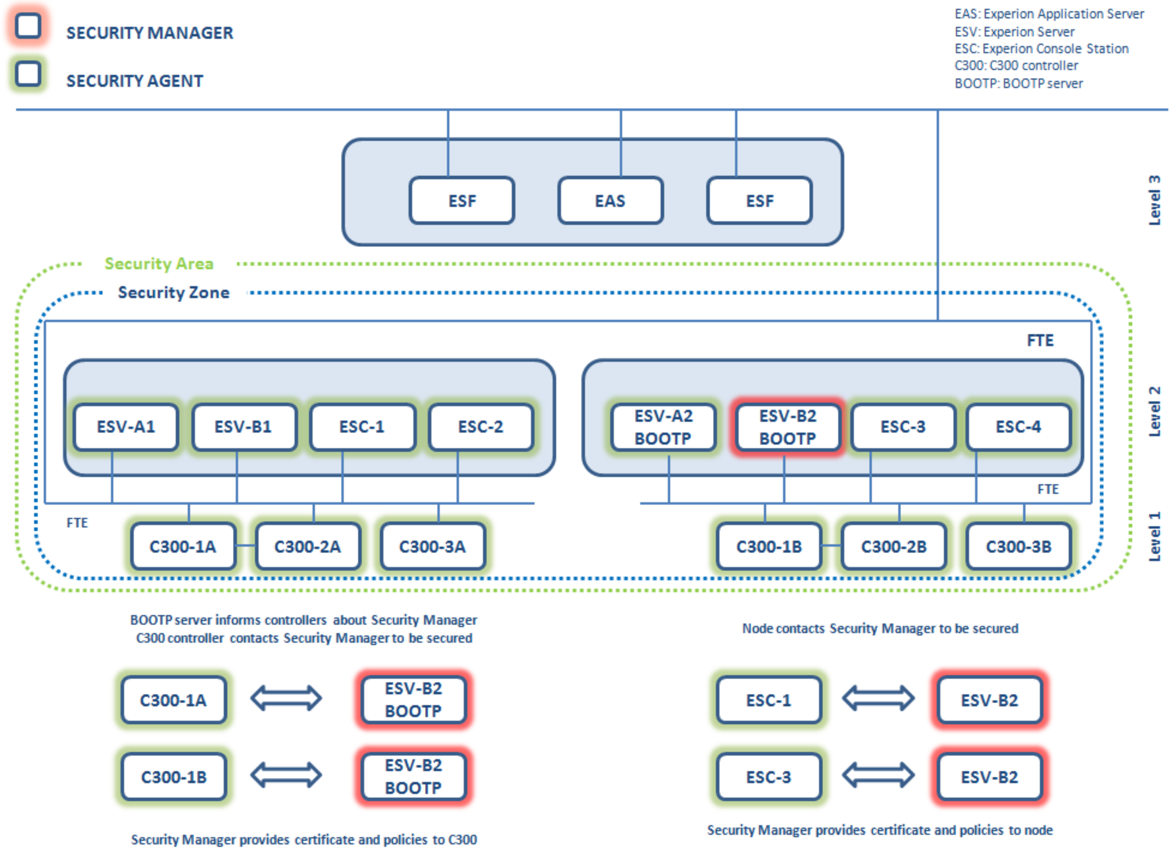
The Experion server at Level 3 is named as ESV-B. The Experion redundant servers in the left cluster are named as ESV-A1 and ESV-B1. The Experion redundant servers in the right cluster are named as ESV-A2 and ESV-B2.

Security Manager routing setup utility field	**Servers**				
	ESV-A1	**ESV-B1**	**ESV-A2**	**ESV-B2**	**ESV-B**
Security Manager IP Address	ESV-B IP address	ESV-B IP address	ESV-B IP address	ESV-B IP address	ESV-B IP address
Security Manager Proxy IP Address	ESV-A1 IP address	ESV-B1 IP address	ESV-A2 IP address	ESV-B2 IP address	ESV-B IP address

Security Manager Proxy IP Address (alternate)	ESV-B1 IP address	ESV-A1 IP address	ESV-B2 IP address	ESV-A2 IP address	0.0.0.0

Security Manager routing setup utility field	**Console Stations**			
	ESC-1	**ESC-2**	**ESC-3**	**ESC-4**
Security Manager Proxy IP Address	ESV-A1 IP address	ESV-A1 IP address	ESV-A2 IP address	ESV-A2 IP address
Security Manager Proxy IP Address (alternate)	ESV-B1 IP address	ESV-B1 IP address	ESV-B2 IP address	ESV-B2 IP address

Experion topology with Security Manager at Level 2 in one FTE community


SECURITY MANAGER
SECURITY AGENT
EAS: Experion Application Server
ESV: Experion Server
ESC: Experion Console Station
C300: C300 controller
BOOTP: BOOTP server
ESF
EAS
ESF
Level 3
Security Area
Security Zone
FTE
ESV-A1
ESV-B1
ESC-1
ESC-2
ESV-A2 BOOTP
ESV-B2 BOOTP
ESC-3
ESC-4
Level 2
FTE
FTE
C300-1A
C300-2A
C300-3A
C300-1B
C300-2B
C300-3B
Level 1
BOOTP server informs controllers about Security Manager
C300 controller contacts Security Manager to be secured
Node contacts Security Manager to be secured
C300-1A
ESV-B2 BOOTP
C300-1B
ESV-B2 BOOTP
ESC-1
ESV-B2
ESC-3
ESV-B2
Security Manager provides certificate and policies to C300
Security Manager provides certificate and policies to node

The illustration displays a system where the Security Manager is located at Level 2 in a single FTE community along with other nodes of the Security Area. In this scenario, no Security Manager Proxies exist. The Security Agent communicates directly with the Security Manager to receive the node certificate and policies. The BOOTP is enabled on Server pair of only one cluster in the FTE community.

In such a scenario, the IP Addresses for the Security Manager and the Security Manager Proxies are added to the Security Manager routing setup utility as provided in the following tables for Servers and Console Stations.

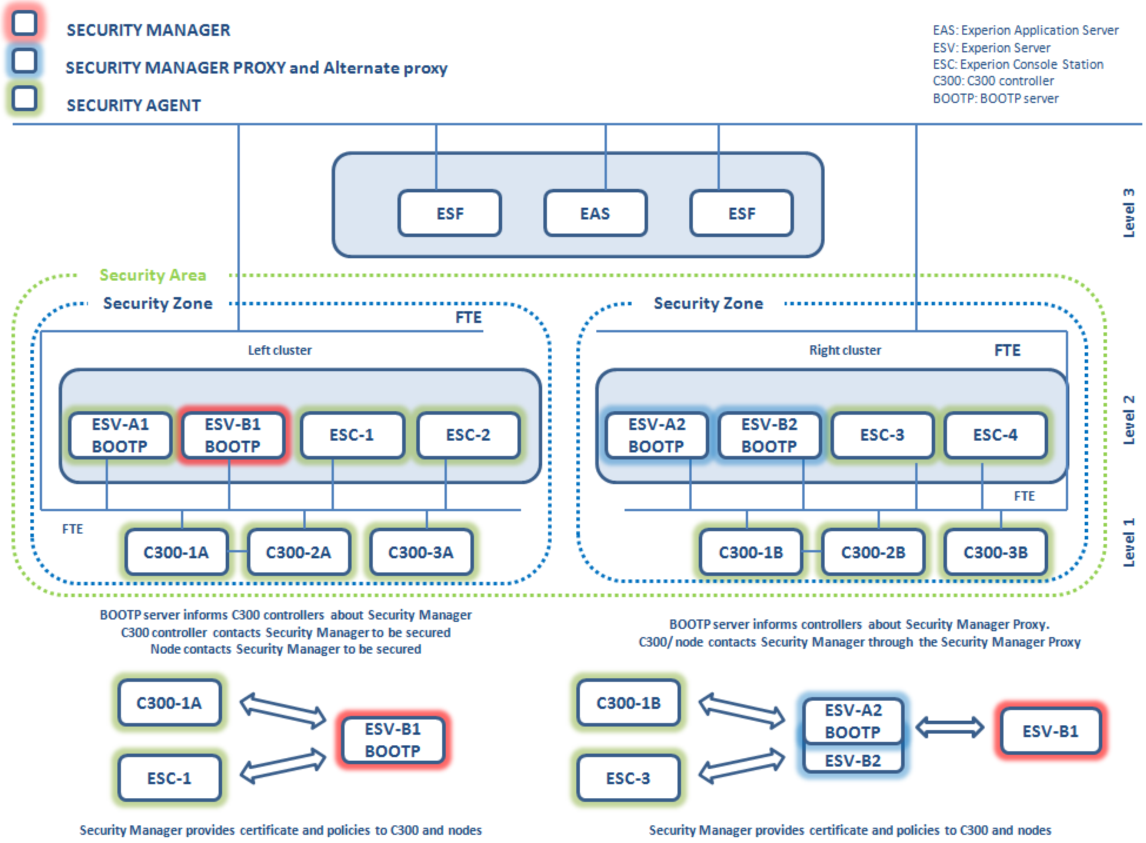
Security Manager routing setup utility field	**Servers**			
	ESV-A1	**ESV-B1**	**ESV-A2**	**ESV-B2**
Security Manager IP Address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address
Security Manager Proxy IP Address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address

Security Manager Proxy IP Address (alternate)	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Security Manager routing setup utility field	Console Stations			
	ESC-1	ESC-2	ESC-3	ESC-4
Security Manager Proxy IP Address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address	ESV-B2 IP address
Security Manager Proxy IP Address (alternate)	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Experion topology with Security Manager at Level 2 and two single cluster FTE communities

The illustration displays a system with a two single cluster FTE communities. The Security Manager is located at Level 2 on Server B. The FTE community with the Security Manager has no proxies, while the FTE community that does not contain the Security Manager has the Security Manager Proxy (alternate) pair. Each FTE community enables BOOTP on the cluster Server pair.


SECURITY MANAGER
SECURITY MANAGER PROXY and Alternate proxy
SECURITY AGENT
EAS: Experion Application Server
ESV: Experion Server
ESC: Experion Console Station
C300: C300 controller
BOOTP: BOOTP server
ESF
EAS
ESF
Level 3
Security Area
Security Zone
FTE
Left cluster
ESV-A1 BOOTP
ESV-B1 BOOTP
ESC-1
ESC-2
FTE
C300-1A
C300-2A
C300-3A
Security Zone
Right cluster
FTE
ESV-A2 BOOTP
ESV-B2 BOOTP
ESC-3
ESC-4
FTE
C300-1B
C300-2B
C300-3B
Level 2
Level 1
BOOTP server informs C300 controllers about Security Manager
C300 controller contacts Security Manager to be secured
Node contacts Security Manager to be secured
BOOTP server informs controllers about Security Manager Proxy.
C300/ node contacts Security Manager through the Security Manager Proxy
C300-1A
ESC-1
ESV-B1 BOOTP
C300-1B
ESC-3
ESV-A2 BOOTP
ESV-B2
ESV-B1
Security Manager provides certificate and policies to C300 and nodes
Security Manager provides certificate and policies to C300 and nodes

In such a scenario, the IP Addresses for the Security Manager and the Security Manager Proxies are added to the Security Manager routing setup utility as provided in the following tables for Servers and Console Stations.

Security Manager routing setup utility field	Servers			
	ESV-A1	ESV-B1	ESV-A2	ESV-B2
Security Manager IP Address	ESV-B1 IP address	ESV-B1 IP address	ESV-B1 IP address	ESV-B1 IP address
Security Manager Proxy IP Address	ESV-B1 IP address	ESV-B1 IP address	ESV-A2 IP address	ESV-B2 IP address

Security Manager Proxy IP Address (alternate)	0.0.0.0	0.0.0.0	ESV-B2 IP address	ESV-A2 IP address

Security Manager routing setup utility field	**Console Stations**			
	ESC-1	**ESC-2**	**ESC-3**	**ESC-4**
Security Manager Proxy IP Address	ESV-B1 IP address	ESV-B1 IP address	ESV-A2 IP address	ESV-A2 IP address
Security Manager Proxy IP Address (alternate)	0.0.0.0	0.0.0.0	ESV-B2 IP address	ESV-B2 IP address

3.1.7 Evaluate impact on Windows nodes and C300 controllers

The two main factors affected when securing a node are as follows:

- Increased CPU usage, because of message authentication and data encryption.
- Slightly reduced network throughput, because of the extra processing.

For Windows nodes, the impact of both these factors is negligible.

For C300 controllers, the impact on network throughput is very small. However, there is an impact on C300 CPU usage that must be considered. For example, to support 14 secure connections to Windows nodes, the C300 will use an additional 8% CPU to maintain the secure connections. You can use the C300 Execution Unit (XU) estimation model to estimate the Secure Communications impact on both the existing C300 and the new C300 controller to be installed.

3.1.8 Recommended number of secured Console Stations in an Experion cluster

In a secured Experion cluster, a C300 switchover is the most process intensive scenario with the establishment or maintenance of the secure associations between nodes.

After a C300 switchover, the new primary module takes over the odd IP Address of the redundant pair and triggers the re-establishment of connections with the Server and the Console Stations of the cluster, in place of the previous connections as the backup using the even IP Address. The negotiation of the new secure associations and re-establishment of connections are completed over a range of time, with some completing as soon as three seconds after the switchover. Based on the free CPU available, only a certain number of connections can be established before *Connection Failed* alarms are reported, which occur when a connection is not reformed within 15 seconds after a C300 switchover. A *Connection Failed* alarm automatically returns to normal when the connection is established.

While connections are being re-established to Servers and Console Stations, the following behaviors are observed:

- Console Stations show values in reverse video
- Attempted operator stores return errors
- Fast history shows a flat line
- Standard and extended history show a gap
- Advanced applications receive errors

The following table provides the recommended maximum number of secured Console Stations for a cluster. This table is based on the lowest percentage of CPU free available of the secured C300 controllers in the cluster. The securing of a non-redundant Experion Server or a redundant Server pair is assumed and therefore not part of the recommendation. It is recommended that you adhere to the information provided in the following table to prevent occurrences of *Connection Failed* alarms after virtually every C300 controller switchover.

Lowest secured C300 CPU free	Maximum number of secured Console Stations
20 – 25 %	2

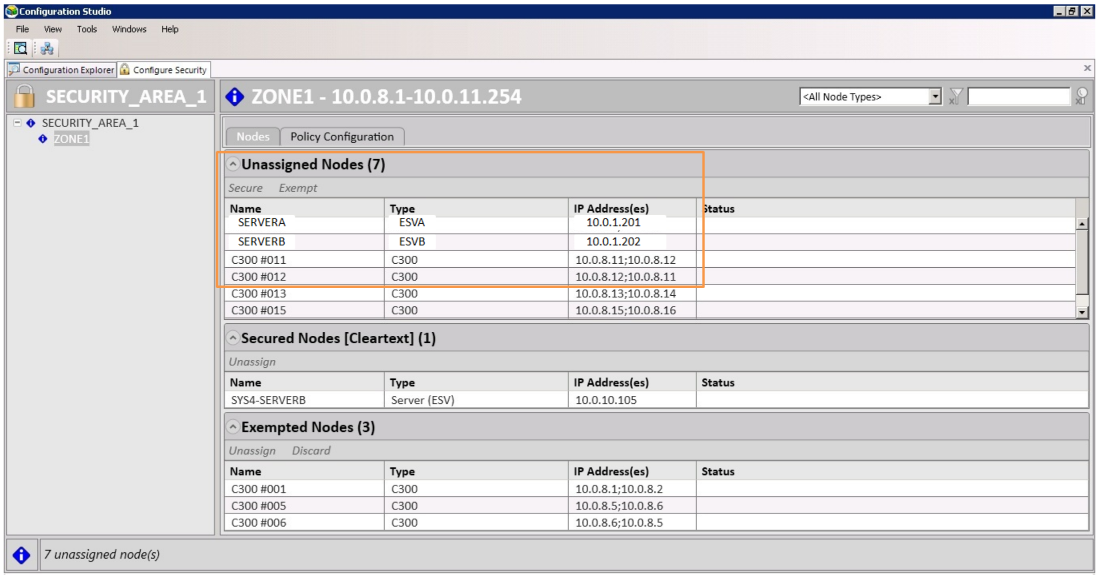
Lowest secured C300 CPU free	Maximum number of secured Console Stations
25 – 30 %	4
30 – 35 %	6
35 – 40 %	8
40 – 45 %	10
45 – 50 %	12
50 – 55 %	14
55 – 60 %	16
60 – 65 %	18
> 65 %	20

Note

- The minimum recommended limit is 20 % CPU free, with or without use of Secure Communications.
- If you opt to secure more than the recommended number of Console Stations, there is an increased likelihood of reconnect times extending past 15 seconds, resulting in *Connection Failed* alarms after C300 module switchovers.
- You need not secure every C300 or Console Station of a cluster. For example, one C300 controller with low CPU free might not be secured if all other C300 controllers of the cluster have appropriate CPU free for the number of secured Console Stations in the cluster.

3.1.9 Recommendation for redundant Experion Servers and C300 controllers

The redundant Experion nodes are displayed in the Secure Communications user interface as two distinct nodes for each redundant pair. For example, the following figure displays redundant Experion Servers and a redundant C300 controller pair.



Unassigned Nodes (7)

Secure Exempt

Name	Type	IP Address(es)	Status
SERVERA	ESVA	10.0.1.201	
SERVERB	ESVB	10.0.1.202	
C300 #011	C300	10.0.8.11;10.0.8.12	
C300 #012	C300	10.0.8.12;10.0.8.11	
C300 #013	C300	10.0.8.13;10.0.8.14	
C300 #015	C300	10.0.8.15;10.0.8.16	

Secured Nodes [Cleartext] (1)

Unassign

Name	Type	IP Address(es)	Status
SYS4-SERVERB	Server (ESV)	10.0.10.105	

Exempted Nodes (3)

Unassign Discard

Name	Type	IP Address(es)	Status
C300 #001	C300	10.0.8.1;10.0.8.2	
C300 #005	C300	10.0.8.5;10.0.8.6	
C300 #006	C300	10.0.8.6;10.0.8.5	

7 unassigned node(s)

- **Redundant Experion Server nodes**

  On the Secure Communications user interface, for redundant Experion nodes, it is recommended that you select redundant nodes in pairs while moving nodes from one table to another

The IP addresses of the Experion nodes do not change, regardless of their current role of being the primary or secondary of the redundant pair. For example, as displayed in the image, SERVERA with an IP Address of 10.0.1.201, always communicates as 10.0.1.201 and SERVERB with an IP Address of 10.0.1.202, always communicates as 10.0.1.202.

For Experion Servers, it is recommended that the server pair be secured together. If only one of the redundant server nodes is secured, for example, if the primary server node is secured, it communicates securely while secondary server communicates using Cleartext. If the servers swap the roles such that the backup server becomes the primary server then it continues communicating using Cleartext. To avoid this scenario, secure the server pair together.

- **Redundant C300 controller pairs**

  For a redundant C300 controller pair, you must always ensure to select the redundant controllers in pairs when you move controllers between the tables in the Secure Communications user interface. The redundant C300 controllers behave differently. For example, C300 modules with device indexes of 11 and 12 use, either 10.0.8.11, or 10.0.8.12 for communication, depending on the redundancy role. The C300 module with the primary role always communicates with an odd IP address, 10.0.8.11, whereas, the C300 module with the secondary role always communicates with an even IP address, 10.0.8.12. The redundant C300 controller pair lose synchronization or modules are not allowed to synchronize when the Secure Communications configuration does not match for the modules. When there is a loss of synchronization alarm because of Secure Communications, a reason of certificate or policy mismatch is provided.

  The following conditions must be ensured while handling redundant C300 controller pairs on the Secure Communications user interface.

  – On the Secure Communications user interface, when both modules of a redundant C300 controller pair are listed in the same table, if any operation is performed, it must be performed on both the modules and they must be moved together to any table.

  – On the Secure Communications user interface, when modules of a redundant C300 controller pair are in different tables, move a module of the C300 controller pair to the same table, such that both the modules are available in the same table.

Securing a redundant or non-redundant C300 controller

Scenario	Procedure
Securing a non-redundant C300 controller	Perform the following steps to secure a non-redundant C300 controller available in the Unassigned Nodes table. For a complete set of steps, see “To secure nodes” on page 40. 1. Select the non-redundant C300 controller and click the Secure option. 2. The non-redundant C300 controller is secured and moves to the Secured Nodes table.
Securing a redundant C300 controller pair	Perform the following steps to secure a redundant C300 controller pair. For a complete set of steps, see “To secure nodes” on page 40. The redundant C300 controller pair is available in the Unassigned Nodes table. 1. Select both the modules. **Note** If you select only one module of the pair and try to secure the module, an error message appears, and the single selected module is not secured. 2. Click the Secure option. 3. The redundant C300 controller pair is secured and moves to Secured Nodes table.

3.2 Installing Secure Communications

Secure Communications components are installed while installing Experion on the Experion nodes. These components are installed on nodes supporting Secure Communications.

Set up Secure Communications

You can set up the Secure Communications by running the Security Manager routing setup utility on each supported node.

Perform the following steps to set up the Secure Communications.

Prerequisites

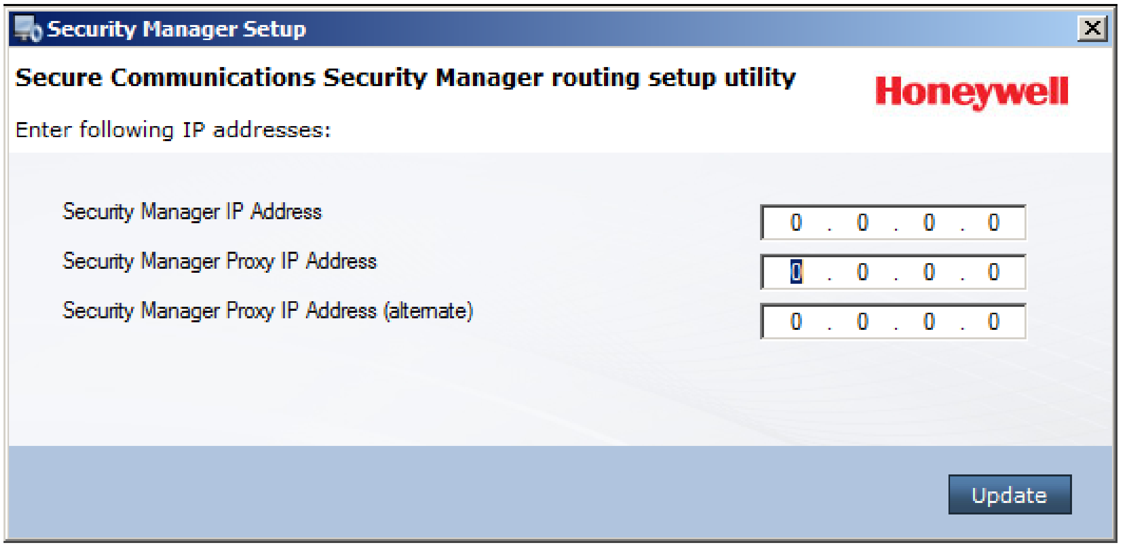
- You must be a member of the Security Administrators or the Product Administrators group.
- Refer to "Planning for Secure Communications" on page 16 to plan for the various components of the Secure Communications.

To run the Secure Communications Security Manager routing setup utility

1 Log on to the Experion node as a user who is a member of the Security Administrators or the Product Administrators group.

2 Browse to `<install folder>:\folder>\Honeywell\Experion PKS\Utilities\SecComConfig` folder.

3 Right-click **seccomconfig.exe** and click **Run as Administrator**.
The **Security Manager Setup** page is displayed. When the tool is run on a Server, the following dialog box appears.



Security Manager Setup

Secure Communications Security Manager routing setup utility

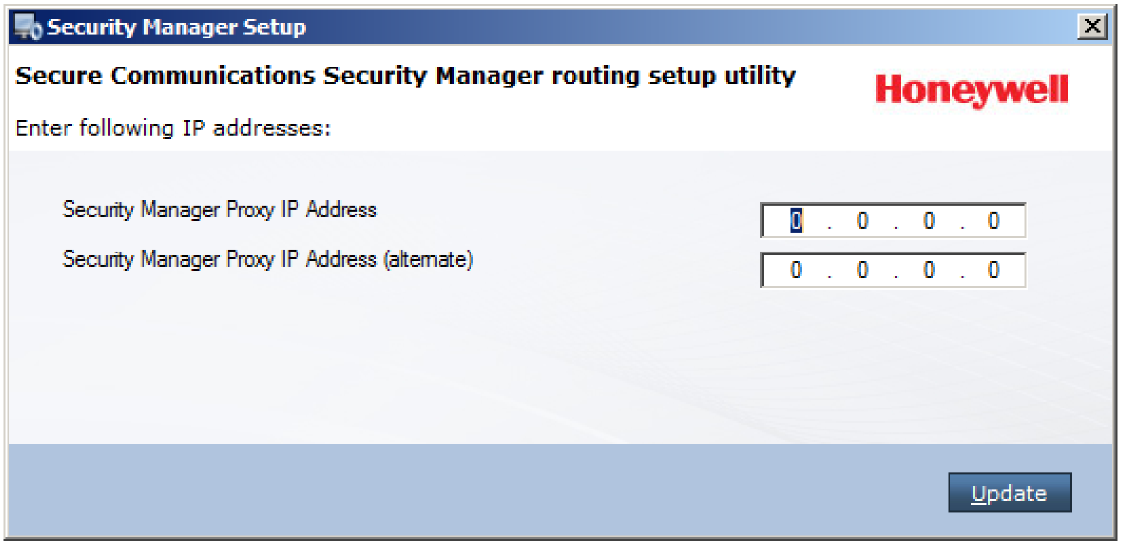
Enter following IP addresses:

Security Manager IP Address: 0 . 0 . 0 . 0

Security Manager Proxy IP Address: 0 . 0 . 0 . 0

Security Manager Proxy IP Address (alternate): 0 . 0 . 0 . 0

When the tool is run on a Console Station, the following dialog box appears.



Security Manager Setup

Secure Communications Security Manager routing setup utility

Enter following IP addresses:

Security Manager Proxy IP Address: 0 . 0 . 0 . 0

Security Manager Proxy IP Address (alternate): 0 . 0 . 0 . 0

If a node is not supported by Secure Communications, the following message appears,

Secure Communications is not supported on this node type.

4 Enter the IP address for each field and click **Update**.

Attention

- Ensure that the IP addresses for Security Manager Proxy IP Address and Security Manager Proxy IP Address (alternate) are not same.
- The IP address for Security Manager Proxy IP Address (alternate) as 0.0.0.0 is allowed.

A message informs that *Experion Secure Communications IP Addresses updated successfully*. This sets the location of the Security Manager and the Security Manager Proxy.

4 Configuration

The following topics describe how to configure Secure Communications in an Experion network from the Configuration Studio.

Related topics

“Guidelines to configure Secure Communications” on page 30
“Configuring Secure Communications” on page 31
“Starting Configuration Studio” on page 32
“Initializing the Security Area” on page 33
“Configuring nodes in the Security Zone” on page 38
“Setting security policy for the Security Zone” on page 44

4.1 Guidelines to configure Secure Communications

It is recommended to adhere to the following guidelines while configuring Secure Communications on the Experion nodes.

Recommended time to configure security policies

The Secure Communications solution renders it easy to configure and deploy policies on-process. It is recommended that you perform the Secure Communications configuration and deployment at a time when brief interruptions of communication can be tolerated. The nodes being secured transition normally from the old policy to the new Secure Communications policy; however, occasionally nodes may stop communicating with each other for a short period of time when the new policy is adopted (it may result in generation of system alarms on the relevant nodes).

Status of nodes

The Secure Communications user interface supports configuration and administration. The time required to complete policy deployments and the associated deployment status is provided, but a live or monitoring view of system status is not supported. You must use existing system displays (for example, System Status Display) to obtain a live view of the status of the nodes.

Recommended order to secure nodes

Though the order of selecting the nodes to secure and set the security level (Cleartext or Encryption) for a Security Zone is not critical, the following logical order of operations is recommended.

1. Set the security level.
2. Ensure that you secure the Security Manager / Security Manager Proxy nodes before you secure the other nodes. This is necessary to ensure that the proxy nodes can deliver certificates and policies to all nodes in the Security Area.

   Note

   If you remove the nodes from a secured network by using the Unassign option, ensure that all the nodes are unassigned before you unassign the Security Manager / Security Manager Proxy nodes. Nodes assigned the role as Security Manager Proxies must be unassigned last.

3. Secure other nodes.

Multiple selection of nodes

While configuring Secure Communications, only one of the following operations is allowed at a time.

- Secure
- Unassign
- Exempt
- Discard

Hence, it is recommended to plan and select multiple nodes before starting any operation.

4.2 Configuring Secure Communications

The Security Administrator performs the following tasks to configure Secure Communications on Experion nodes.

1. “Starting Configuration Studio” on page 32
2. “Initializing the Security Area” on page 33
3. “Configuring nodes in the Security Zone” on page 38
4. “Setting security policy for the Security Zone” on page 44

4.3 Starting Configuration Studio

Using the Configuration Studio, you can open the Secure Communications user interface and configure Secure Communications for a Security Area in an Experion system or an Experion server. The Experion system and Experion nodes connected to the system and server are listed when the Configuration Studio is launched.

Prerequisites

- To log on, you must be a member of the Security Administrator group.

To start the Configuration Studio

1. Choose **Start** > **All Programs** > **Honeywell Experion PKS** > **Configuration Studio**.
   The **Connect** dialog box appears.
2. In the list of systems and servers, click the system or specific server that you want to connect to and click **Connect**.
   The **Login to Server** dialog box appears.
3. Log on to Configuration Studio with the required privileges.

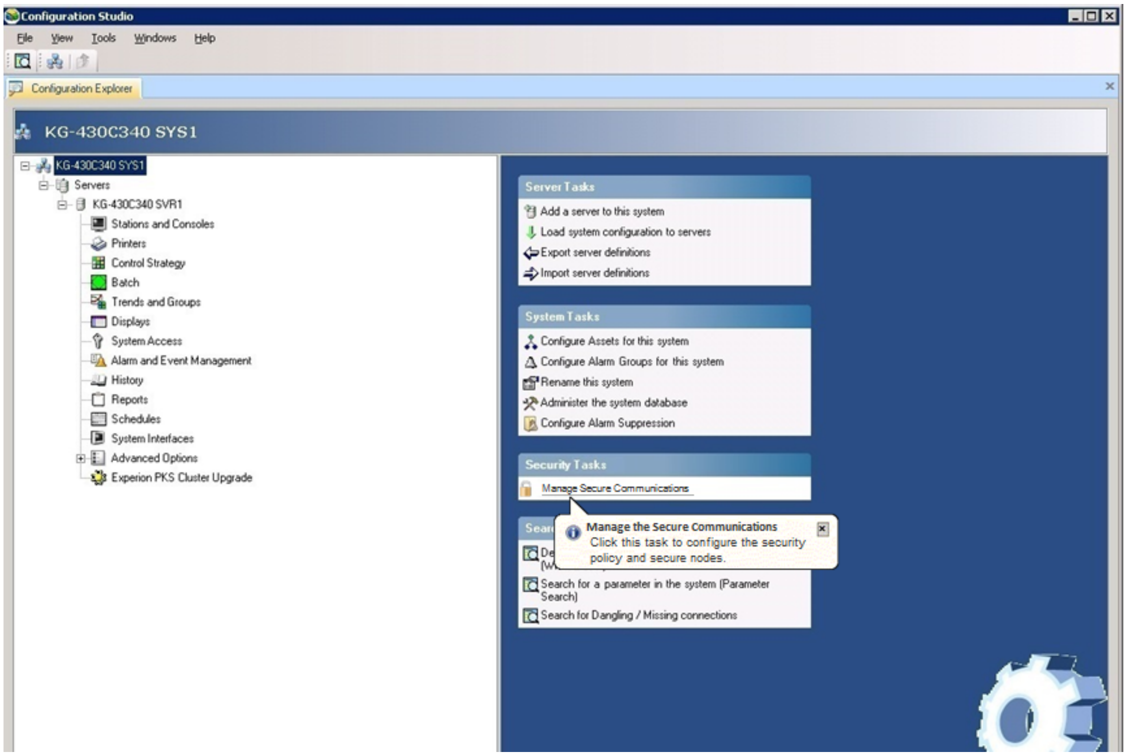
4.4 Initializing the Security Area

The Secure Communications application is hosted in the Configuration Studio and appears as a separate tab. You must initialize the Security Area before securing the nodes. Perform the following steps to initialize the Security Area.

1 On the Configuration Studio, click **Manage Secure Communications**.

Attention

If your current Windows logon does not belong to Local SecureComms Administrators group or you have logged into Configuration Studio (non single-signon) using an operator logon that does not belong to Local SecureComms Administrators group, the Secure Communications user interface is not displayed. For more information, see “Assign the Security Administrator role” on page 16.


Configuration Studio
File View Tools Windows Help
Configuration Explorer
KG-430C340 SYS1
KG-430C340 SYS1
Servers
KG-430C340 SVR1
Stations and Consoles
Printers
Control Strategy
Batch
Trends and Groups
Displays
System Access
Alarm and Event Management
History
Reports
Schedules
System Interfaces
Advanced Options
Experion PKS Cluster Upgrade
Server Tasks
Add a server to this system
Load system configuration to servers
Export server definitions
Import server definitions
System Tasks
Configure Assets for this system
Configure Alarm Groups for this system
Rename this system
Administer the system database
Configure Alarm Suppression
Security Tasks
Manage Secure Communications
Sear
De
(W
Search for a parameter in the system (Parameter Search)
Search for Dangling / Missing connections

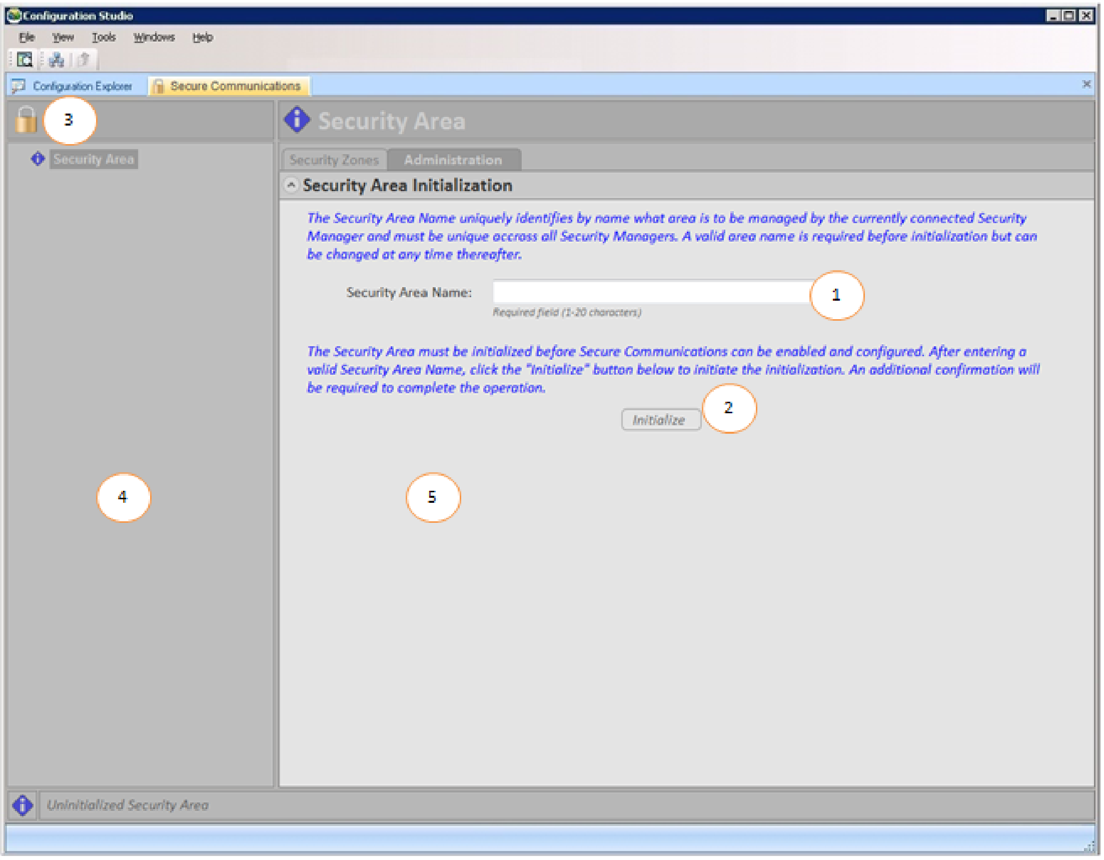
Manage the Secure Communications
Click this task to configure the security policy and secure nodes.

The Secure Communications application is hosted on the Configuration Studio and appears as a separate tab. The Secure Communications user interface consists of the Security Area tree pane and the Security Area details pane. The Security Area tree pane provides information about the Security Area and its Security Zones. In the Security Area details pane, the Security Area and Security Zones have information organized in separate tabs.

The following tabs are available on the Security Area details pane.

- Security Zones
- Administration

2 When you click the Administration tab, the following user interface appears.



The Security Area Name uniquely identifies by name what area is to be managed by the currently connected Security Manager and must be unique accross all Security Managers. A valid area name is required before initialization but can be changed at any time thereafter.

Security Area Name:

Required field (1-20 characters)

The Security Area must be initialized before Secure Communications can be enabled and configured. After entering a valid Security Area Name, click the "Initialize" button below to initiate the initialization. An additional confirmation will be required to complete the operation.

The following information is displayed on the Administration tab.

Number	Field	Description
1	Security Area Name box	Provides a valid name for the Security Area.
2	Initialize	Initializes the Security Area Name.
3	Security Area Name on the tree pane	Displays the name provided to the Security Area.
4	Security Area tree pane	Provides information about Security Area and its Security Zones.
5	Security Area details pane	Provides tabs to update information about Security Area and Security Zones.

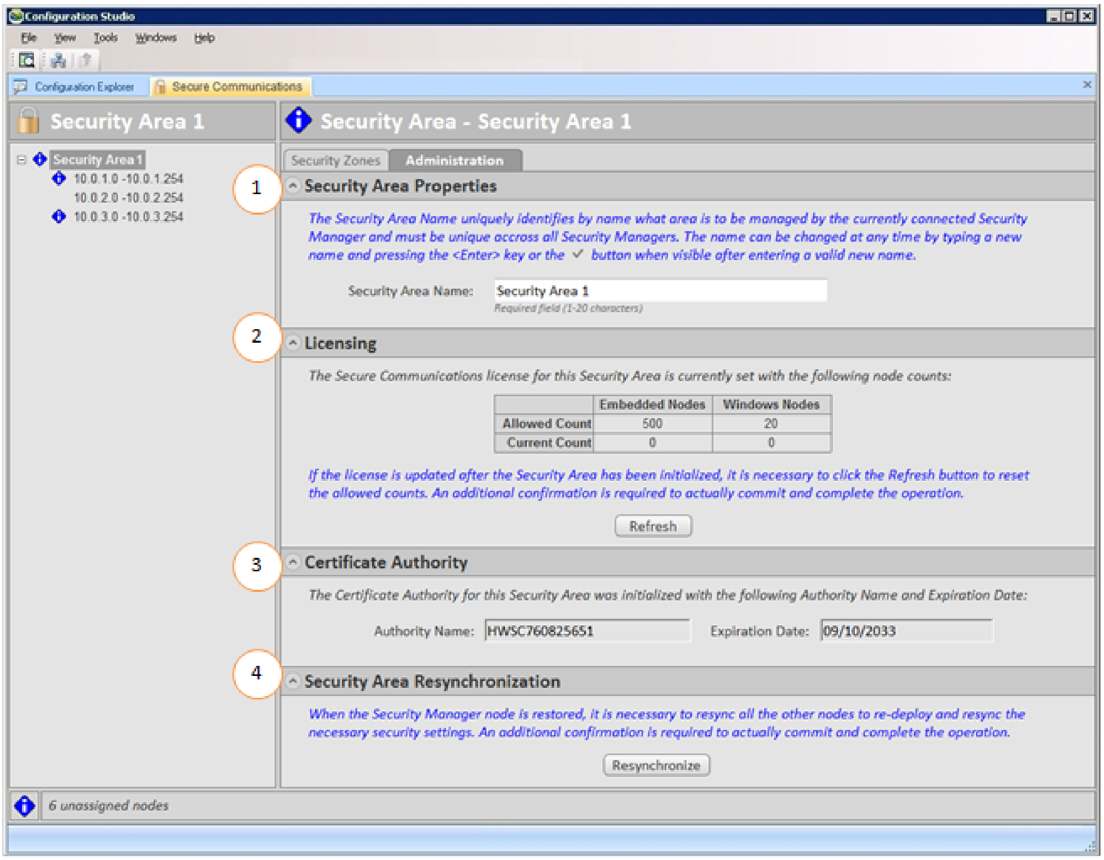
Note

You must initialize the Security Area before enabling and configuring the Secure Communications. This option is available the first time you open the Secure Communications user interface. The Security Area name must be unique.

Perform the following steps to initialize the Security Area.

1. In the Secure Communications user interface, click **Administration** tab and expand **Security Area Properties**.
2. Type a valid name for the **Security Area Name**.
3. Click **Initialize**.
4. Click **Confirm** and click **OK** to complete the initialization.

After initialization, the following information is displayed on the Administration tab.



Security Area Properties

The Security Area Name uniquely identifies by name what area is to be managed by the currently connected Security Manager and must be unique accross all Security Managers. The name can be changed at any time by typing a new name and pressing the <Enter> key or the ✓ button when visible after entering a valid new name.

Security Area Name: Security Area 1

Required field (1-20 characters)

Licensing

The Secure Communications license for this Security Area is currently set with the following node counts:

	Embedded Nodes	Windows Nodes
Allowed Count	500	20
Current Count	0	0

If the license is updated after the Security Area has been initialized, it is necessary to click the Refresh button to reset the allowed counts. An additional confirmation is required to actually commit and complete the operation.

Certificate Authority

The Certificate Authority for this Security Area was initialized with the following Authority Name and Expiration Date:

Authority Name: HWSC760825651 Expiration Date: 09/10/2033

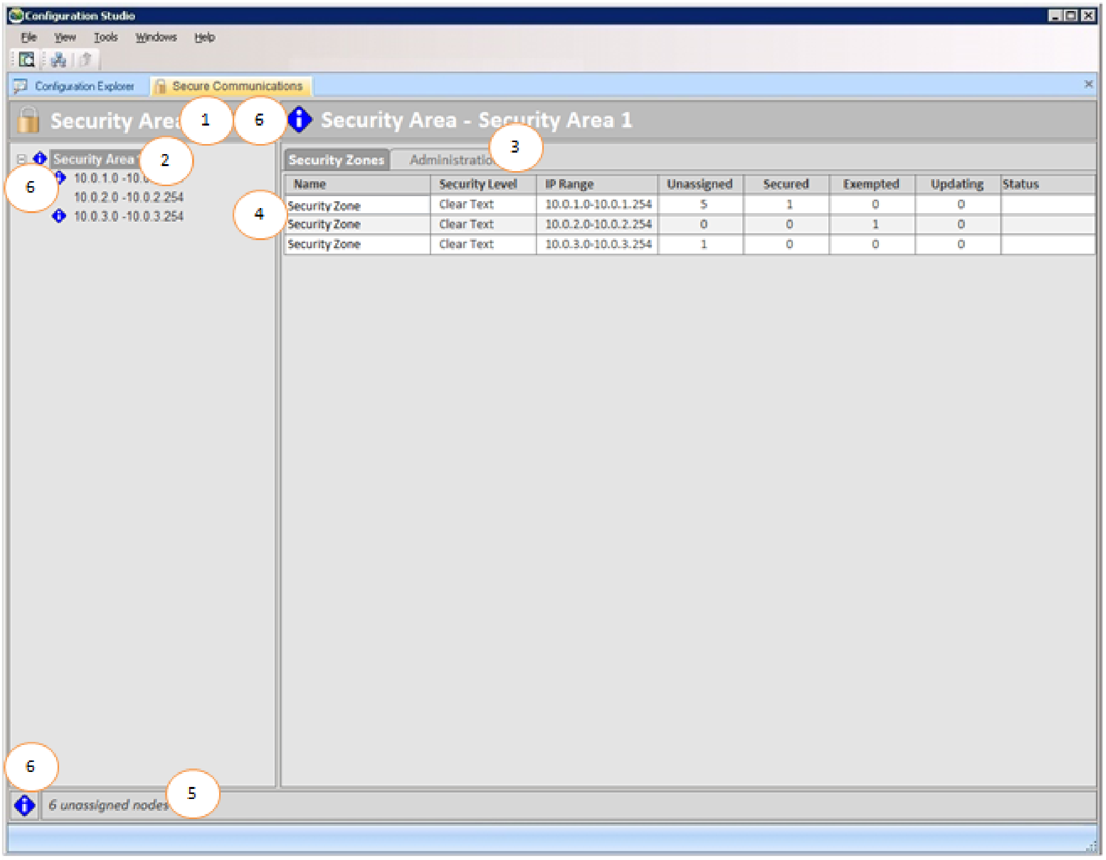
Security Area Resynchronization

When the Security Manager node is restored, it is necessary to resync all the other nodes to re-deploy and resync the necessary security settings. An additional confirmation is required to actually commit and complete the operation.

Number	Field	Description
1	Security Area Properties	Enables modification of the name provided for the Security Area at any time.
2	Licensing	Displays the various license-related counts in a read-only table. You can refresh the licence count when the license is upgraded or downgraded.
3	Certificate Authority	Displays the Authority Name and Expiration Date in read-only fields.
4	Security Area Resynchronization	Provides ability to resynchronize the nodes after a restore operation.

3 Click the **Security Zones** tab to verify the security level of the nodes in the Security Zone.

The **Security Zones** tab displays the following information.



Name	Security Level	IP Range	Unassigned	Secured	Exempted	Updating	Status
Security Zone	Clear Text	10.0.1.0-10.0.1.254	5	1	0	0	
Security Zone	Clear Text	10.0.2.0-10.0.2.254	0	0	1	0	
Security Zone	Clear Text	10.0.3.0-10.0.3.254	1	0	0	0	

Number	Field	Description
1	Security Area Name	Displays name of the Security Area that includes various Security Zones.
2	Security Area tree node	Displays the Security Area tree view when selected.
3	Administration tab	Use the Administration tab to modify the Security Area Name.
4	Security Zones grid	Provides summary of all security zones and their details, names, security level, IP ranges, and various node statistics. Security Zone names can be customized directly in the grid.
5	Status message text	Displays the count of all unassigned nodes in the Security Area.
6	Information icon	Indicates that some unclassified nodes currently exist in either the Security Area or one or more of its Security Zones.

4.4.1 Rename the Security Area

1. In the Secure Communications user interface, click the **Administration** tab and expand **Security Area Properties**.
2. Type the name for the Security Area in the **Security Area Name** box.
   A check mark appears on the right side of the typed name.
3. Click the check mark or press ENTER.
   The new Security Area name appears in the **Security Area Name** box and the Security Area pane.

4.4.2 Rename the Security Zones

1. In the Secure Communications user interface, click the **Security Zones** tab.

2 Type the new name for Security Zone in the **Name** column.

A check mark appears on the right side of the name you type.

3 Click the check mark or press ENTER.

The new name for the Security Zone appears on the screen.

4.4.3 Resynchronize the Security Area

1 In the Secure Communications user interface, click **Administration** tab and expand **Security Area Resynchronization**. This task is usually performed after a Security Manager node restore operation.

2 Click **Resynchronize**.

> ! **Attention**
>
> The Resynchronize command is not required, if there is confidence that the current set of policies deployed to the system match the content of a restored Security Manager. The Security Manager is properly restored and subsequent updates can be successfully performed.
>
> The Resynchronize command deploys all policies in the Secure Communications database to the system, even if the policies are different from what is currently operating in the system. If there is a mismatch between the *current* and *being deployed* set of policies, depending on the differences, the nodes may stop communicating with each other. The configuration database and the system can be synchronized during the subsequent system shutdown or maintenance period.

3 Click **Confirm** to initiate resynchronization. Click **OK**.

4.4.4 Refresh the license

1 In the Secure Communications user interface, click **Administration** tab and expand **Licensing**.

2 After you upgrade or downgrade the license for a Security Area, click **Refresh**.

The latest license details are displayed.

4.5 Configuring nodes in the Security Zone

To open the Security Zone view, click the IP address or the Security Zone name in the Security Area tree pane. You can perform various operations for a node in the Security Zone.

The Security Zone view has the following tabs.

- Nodes
- Policy Configuration

The Nodes tab contains the following tables.

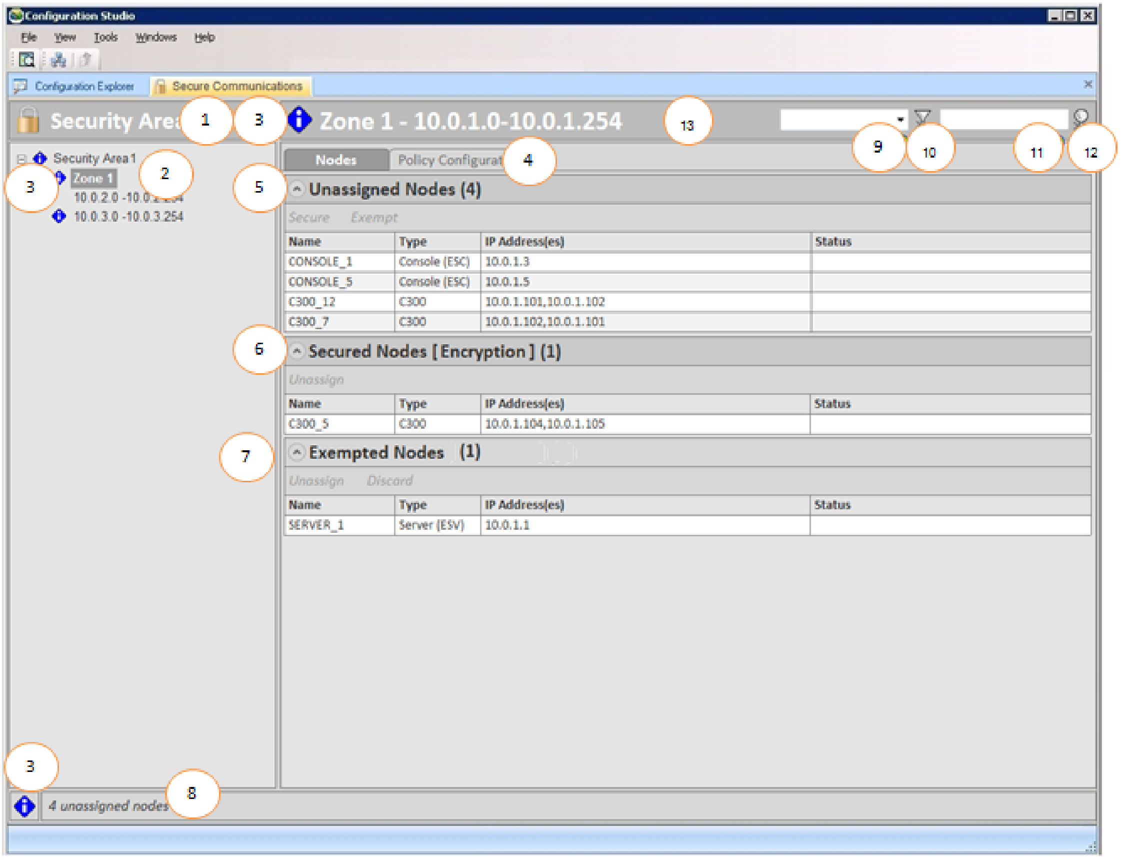
- Unassigned Nodes

  The Unassigned Nodes table lists the nodes to be secured in a Security Zone. You have the option to secure or exempt a node.
- Secured Nodes

  The Secured Nodes table lists the nodes that are secured. The current security level for the Security Zone is displayed with the table name. With this table, you have the option to unassign one or more nodes.
- Exempted Nodes

  The Exempted Nodes table lists the nodes that are exempted. The current security level for the exempted nodes is displayed with the table name. You have the option to unassign or discard one or more nodes.

The Nodes tab displays the following information.



Unassigned Nodes (4)

Secure Exempt

Name	Type	IP Address(es)	Status
CONSOLE_1	Console (ESC)	10.0.1.3	
CONSOLE_5	Console (ESC)	10.0.1.5	
C300_12	C300	10.0.1.101,10.0.1.102	
C300_7	C300	10.0.1.102,10.0.1.101	

Secured Nodes [Encryption] (1)

Unassign

Name	Type	IP Address(es)	Status
C300_5	C300	10.0.1.104,10.0.1.105	

Exempted Nodes (1)

Unassign Discard

Name	Type	IP Address(es)	Status
SERVER_1	Server (ESV)	10.0.1.1	

Number	Field	Description
1	Security Area Name	Displays name of the Security Area that includes various Security Zones.

Number	Field	Description
2	Security Zone tree node	Displays the Security Zone tree view. The zone tree node name is displayed as either the IP address range for the zone or a custom name when the default name Security Zone is provided a name.
3	Information icons	These icons indicate that some unassigned nodes currently exist in the Security Zone.
4	Policy Configuration tab	Access this tab to set the security policy for the Security Zone.
5	Unassigned Nodes table	This table contains nodes that are yet to be secured or exempted. The table header displays the current node count. A command bar provides the Secure and Exempt options after a selection is made in the table. Securing an unassigned node moves it to the Secured Nodes table. Exempting an unassigned node moves it to the Exempted Nodes table. The table provides details about the nodes, name, type, IP address(es), and status. The status column provides information when the node is updating. It indicates that the security deployment or activation is in progress and is yet to be completed.
6	Secured Nodes table	This table contains nodes that have been secured. The table header displays the current node count. A command bar provides the option to Unassign after selecting a node. Unassigning a secured node removes it from the Secured Nodes table and lists the node in the Unassigned Nodes table. In addition, this table header also displays the current security level for this security zone. The security level can be modified in the Policy Configuration tab.
7	Exempted Nodes table	This table contains nodes that are exempted. The table header displays the current node count. A command bar provides the options to Unassign and Discard after a selection is made in the list. Unassign removes an exempted node from the Exempted Nodes table and adds it back to the Unassigned Nodes table. Discard removes an exempted node from the Exempted Nodes table.
8	Status Message text	Displays the count of all unassigned nodes in the Security Zone.
9	Filter drop down list	Provides a list of node types to filter. The nodes available in the Security Zones are filtered based on the node selected. When filtering or search is in effect, the node count in the list headers is updated to display both the filtered and the total node count in parentheses with a '/' to separate them. For example, 1/4 means that one node matches the filter/search combination out of a total of four nodes.
10	Filter/Clear filter button	Clears the current filter selection. The Clear Filter button is enabled after a selection is made in the dropdown list.
11	Search text field	Provides an option to search nodes based on a specified search string. Click Search or press ENTER to search. The search-based filtering is combined with the dropdown list-based filtering.
12	Search/Clear search button	Clears the current search filter selection. The Clear Search button is enabled after a search string is entered.
13	Security Zone	Provides current Security Zone name as well as the IP address range.

The Security Administrator is responsible for the tasks related to node configuration.

Node configuration is performed on the Secure Communications user interface and includes the following operations.

- Secure nodes
- Exempt nodes
- Unassign nodes
- Discard nodes

Attention

The deployment of policies to the system is staggered over time, to ensure a smooth system transition from the previous configuration to the new configuration.

The C300 controllers negotiate one new policy at a time, and the Windows nodes, at most, negotiate two policies at the same time. A Windows node negotiates with both the partners of a redundant C300 controller at the same time, to ensure that the C300 redundant partners do not lose synchronization.

The interval for policy deployment is one second, which means that when the policies are activated and negotiated, every interval one to two policies are activated. For example, the first second, two nodes Experion Server A and Experion Server B activate a new policy. The next second, two more nodes, Experion Server A and a Console Station activate a new policy, and so on.

4.5.1 To secure nodes

In the Secure Communications user interface, after initializing the Security Area, use the Secure option to secure a node in the Security Area. This option is enabled only when you select a node. It is recommended to select multiple nodes while securing the nodes as only one operation is supported at a time. This operation moves the node from the Unassigned Nodes table to the Secured Nodes table on the Secure Communications user interface.

Attention

Once secured, the server nodes available as the Security Manager Proxy and Security Manager Proxy alternate roles for all nodes of a multiple cluster FTE community should remain secured, because the Proxies provide the routing linkage between the Security Manager and the nodes.

If these nodes providing the Security Manager Proxy function are unassigned for some reason (for example, during troubleshooting), then the routing path is broken between the Security Manager and the nodes. The nodes providing the Security Manager Proxy function must be secured again as soon as possible to restore the routing linkage.

Perform the following steps to secure a node.

1 Open **Configuration Studio > Manage Secure Communications**. Ensure that the Security Area is initialized. If not, initialize the Security Area.

2 Click the **Security Zone name** or the **IP address** on the left pane.

3 On the **Nodes** tab, expand the **Unassigned Nodes** table.

4 To initiate the Secure operation:

a Select nodes in the **Unassigned Nodes** table.

b Click **Secure**.

Note

The **Secure** option is enabled only after a node is selected in the table.

5 Click **Confirm**. The operation to secure the node starts after you confirm. However, if you want to abort the operation, click **Cancel**.

The status bar indicates that the operation is in progress and also displays the remaining time for the operation to complete. If the request to initiate securing nodes is successful, the following message is displayed.

Secure Node operation completed.

6 Click **OK**. You can also wait until all the nodes are updated and then click **OK**. The status of each node can be viewed in the **Status** column.

After successful completion of securing the nodes, the secured nodes appear in the **Secured Nodes** table.

Note

If the following error is displayed, click **OK** to acknowledge the failed operation. Repeat the steps for the node.

Secure Node operation completed with error(s).

The **Status** cell also displays the error icon and details of the error, if applicable.

4.5.2 To exempt nodes

If you decide not to secure a node in the Security Area, use the Exempt option and remove the node from the Unassigned Nodes table on the Secure Communications user interface. This operation moves the node from the Unassigned Nodes table to the Exempted Nodes table.

Perform the following steps to exempt a node.

1. Open **Configuration Studio > Manage Secure Communications**. Ensure that the Security Area is initialized. If not, initialize the Security Area.
2. Click **Security Zone name** or the **IP address** on the left pane.
3. Click the **Nodes** tab and expand the **Unassigned Nodes** table.
4. To initiate the Exempt operation:
   a. Select nodes in the **Unassigned Nodes** table.
   b. Click **Exempt**.

   Note

   The **Exempt** option is enabled only after a node is selected in the table.
5. Click **Confirm**. The operation to exempt the node starts after you confirm. However, if you want to abort the operation, click **Cancel**.

   If the request to initiate exempting nodes is successful, the following message is displayed.

   Exempt Node operation completed
6. Click **OK**. You can also wait until all the nodes are updated and then click **OK**. The status of each node can be viewed in the **Status** column.

   After successful completion of the operation, the node appears in the **Exempted Nodes** table.

Note

If the following error is displayed, click **OK** to acknowledge the failed operation. Repeat the steps for the node.

Exempt Node operation completed with error(s).

The **Status** cell also displays the error icon and details of the error, if applicable.

4.5.3 To unassign nodes

After a node is classified as a secure or exempted node, and moved to the Secured Nodes or the Exempted Nodes table respectively, if you decide to reverse that classification, use the Unassign option. This option is available on the Secured Nodes and the Exempted Nodes table.

When you click the Unassign option on the Secured Nodes / Exempted Nodes table, the node moves to the Unassigned Nodes table. The node can be secured, if required.

Perform the following steps to unassign a node.

1. Open **Configuration Studio > Manage Secure Communications**. Ensure that the Security Area is initialized. If not, initialize the Security Area.
2. Click **Security Zone name** or the **IP address** on the left pane.
3. On the **Nodes** tab, expand the **Secured Nodes** table or the **Exempted Nodes** table.
4. To initiate the Unassign operation:

a Select nodes in the **Secured Nodes** table or the **Exempted Nodes** table.

b Click **Unassign**.

Note

The **Unassign** option is enabled only after a node is selected in the table.

5 Click **Confirm**. The operation to unassign the node starts after you confirm. However, if you want to abort the operation, click **Cancel**.

The status bar indicates that the operation is in progress and also displays the remaining time for the operation to complete. If the request to initiate unassign nodes is successful, the following message is displayed.

Unassign Node operation completed

6 Click **OK**. You can also wait until all the nodes are updated and then click **OK**. The status of each node can be viewed in the **Status** column.

After successful completion of the operation, the node appears in the **Unassigned Nodes** table.

Note

If the following error is displayed, click **OK** to acknowledge the failed operation. Repeat the steps for the node.

Unassign Node operation completed with error(s).

The **Status** cell also displays the error icon and details of the error, if applicable.

4.5.4 To discard nodes

To remove a node from the Security Area configuration database, use the Discard option on the Secure Communications user interface. This operation removes the node from the Exempted Nodes table and the node does not appear in any of the tables on the Secure Communications user interface.

Attention

A discarded node may appear in the Unassigned Nodes table if the following operations are performed followed by the discard operation.

- An exempted node is restarted
- Switchover of an exempted C300 controller is performed
- C300 controller firmware is upgraded or patch is installed
- C300 controller power recycle is performed
- Windows node is restarted
- Experion services are stopped and restarted either during Experion patch installation or by manual service restart from service panel

Perform the following steps to discard a node.

1 Open **Configuration Studio > Manage Secure Communications**. Ensure that the Security Area is initialized. If not, initialize the Security Area.

2 Click the **Security Zone name** or the **IP address** on the left pane.

3 On the **Nodes** tab, expand the **Exempted Nodes** table.

4 To initiate the Discard operation:

a Select nodes in the **Exempted Nodes** table.

b Click **Discard**.

Note

The **Discard** option is enabled only after a node is selected in the table.

5 Click **Confirm**. The operation to discard the node starts after you confirm. However, if you want to abort the operation, you can click **Cancel**.

If the request to initiate discarding nodes is successful, the following message is displayed.

Discard Node operation completed

6 Click **OK**. You can also wait until all the nodes are updated and then click **OK**. The status of each node can be viewed in the **Status** column.

After successful completion of the operation, the node does not appear in any of the tables.

Note

If the following error is displayed, click **OK** to acknowledge the failed operation. Repeat the steps for the node.

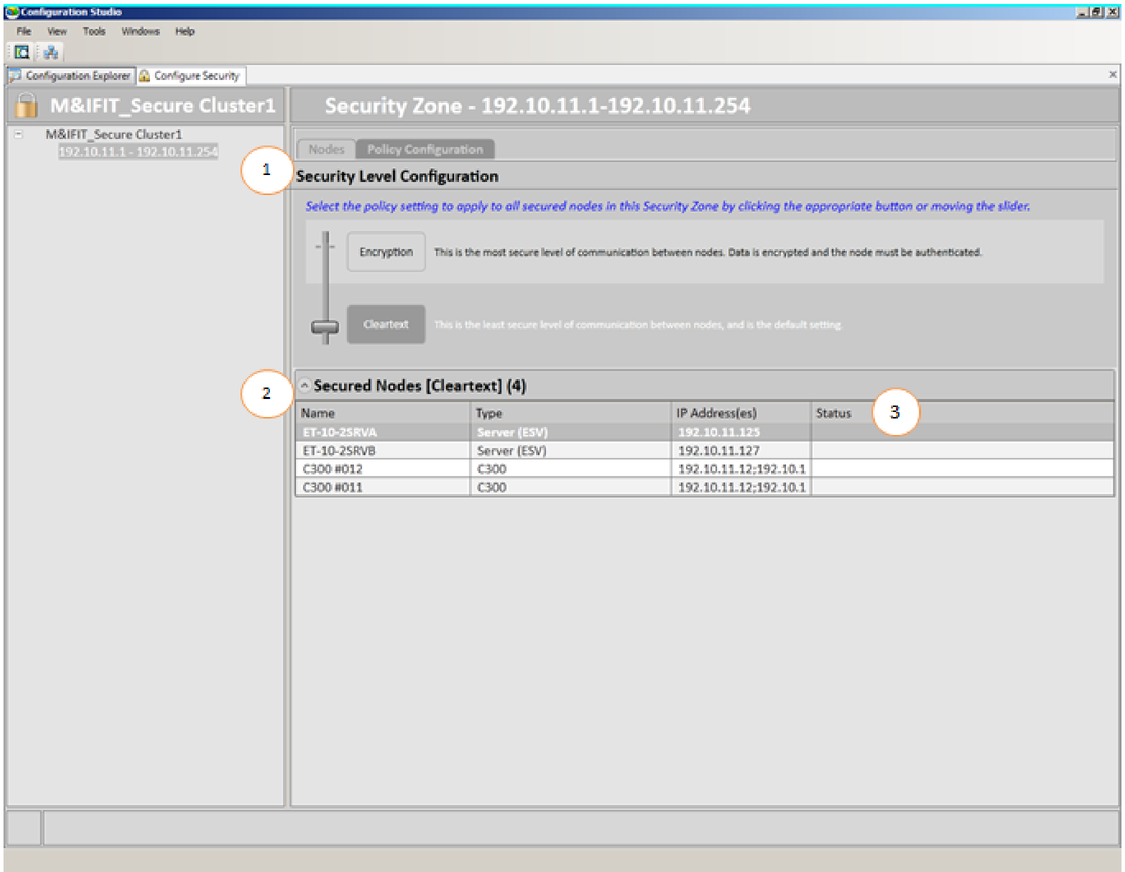
Discard Node operation completed with error(s).

The **Status** cell also displays the error icon and details of the error, if applicable.

4.6 Setting security policy for the Security Zone

The Security Administrator determines security policies for the defined Security Zone in the Security Area.

The policy configuration for the nodes to be secured is configured using the Policy Configuration tab. By using the slider or the security level button in the Security Level Configuration area, you can configure the security level for selected nodes in a specific Security Zone. In addition, the list of currently secured nodes in the Security Zone is displayed under the Secured Nodes header. The node security policies decide the communication format between the nodes.



Select the policy setting to apply to all secured nodes in this Security Zone by clicking the appropriate button or moving the slider.

Encryption: This is the most secure level of communication between nodes. Data is encrypted and the node must be authenticated.

Cleartext: This is the least secure level of communication between nodes, and is the default setting.

Name	Type	IP Address(es)	Status
ET-10-2SRVA	Server (ESV)	192.10.11.125	
ET-10-2SRVB	Server (ESV)	192.10.11.127	
C300 #012	C300	192.10.11.12;192.10.1	
C300 #011	C300	192.10.11.12;192.10.1	

Number	Field	Description
1	Security Level Configuration	Modify security level by clicking the required security level button or by using the slider. You can select the policy setting as Encryption or Cleartext.
2	Secured Nodes list	Contains the current list of secured nodes to be secured by the new security level deployment and activation. The list provides details about the nodes, such as name, type, IP address(es), and status.
3	Status column	Contains status information while the security level is modified on a node per node basis.

The Security Administrator determines security policies for a Security Zone in a Security Area.

Perform the following steps to set the security policy.

1. In the Secure Communications user interface, select a **Security Zone** and click **Policy Configuration** tab.
2. Move the slider or click the required button to set the security policy.
3. Click **Confirm**. Click **OK**.

5 Operations and maintenance

The following topics describe the Secure Communications operations and maintenance.

Related topics

"Node maintenance" on page 46

5.1 Node maintenance

After a node is secured, the Security Administrator might have to perform further operations, for example, a secured non-redundant controller may have to be converted as a secured redundant controller. This section provides information about node maintenance in such scenarios.

Scenario	Procedure
Converting a secured non-redundant C300 controller to a redundant C300 controller.	Perform the following steps to convert a secured non-redundant C300 controller to a redundant C300 controller. The non-redundant C300 controller is secured and is available in the Secured Nodes table. 1. Insert a new C300 module in the C300 IOTA to serve as the redundant partner. The new module appears in the Unassigned Nodes table. 2. Select the new C300 module. 3. Click Secure. The new C300 module is secured and moved to the Secured Nodes table. 4. Synchronize the secured C300 controller modules. **Note** The C300 redundant pair cannot be synchronized until both the modules are in the same table.
Secured secondary Experion Server of the redundant Experion Server pair fails and has to be replaced.	For information about replacing a redundant secured server, see the *Restoring server B from a hardware failure or corrupted database* topic in *System Administration Guide*. If a clean Experion installation is being performed on the node to be replaced, then perform the following steps after the node is connected to the network. **Note** If the replacement node is fully configured, then these two steps need not be performed. 1. Run Security Manager routing setup utility on the node to identify the location of the Security Manager and identify the server node as a Security Manager Proxy. 2. In the Secure Communications user interface, select the node after it appears in the Unassigned Nodes table, and use the Secure option to secure the node.
Secured Console Station fails and needs to be replaced.	Perform the following steps. 1. Replace the failed Console Station. 2. If a clean Experion installation is being performed on the station to be replaced, then perform the following steps after the node is connected to the network. a. Run Security Manager routing setup utility on the Console Station to identify the location of the Security Manager and the Security Manager Proxies. b. In the Secure Communications user interface, select the Console Station after it appears in the Unassigned Nodes table, and use the Secure option to secure the station. **Note** Note that if the replacement node is fully configured, then these two steps need not be performed.

<table>
<tr><th>Scenario</th><th>Procedure</th></tr>
<tr><td>Replacing a module of a secured redundant C300 controller pair.</td><td>
<p>Perform the following steps to replace a module of a secured redundant C300 controller pair.</p>
<p>You may have to replace a C300 module of a secured redundant C300 controller pair if the module hardware fails for some reason. In such a case, notifications are generated for the hardware failure and loss of synchronization.</p>
<ol>
<li><p>Replace the failed module with a new C300 module in the C300 IOTA to serve as the redundant partner.</p>
<p>The new module now appears in the Unassigned Nodes table. The Secure Communications user interface appears as follows:</p>
<p>Unassigned Nodes table</p>
<table>
<tr><th>Name</th><th>Type</th><th>IP Address</th></tr>
<tr><td>C300 # 12</td><td>C300</td><td>10.0.1.12, 10.0.1.11</td></tr>
</table>
<p>Secured Nodes table</p>
<table>
<tr><th>Name</th><th>Type</th><th>IP Address</th></tr>
<tr><td>C300 # 11</td><td>C300</td><td>10.0.1.11, 10.0.1.12</td></tr>
<tr><td>C300 # 12</td><td>C300</td><td>10.0.1.12, 10.0.1.11</td></tr>
</table>
<p><b>Note</b></p>
<ul>
<li>At this point, the new C300 #12 module in the Unassigned Nodes table is not be able to communicate with the Windows nodes in the secured list. The module does not communicate until it is secured.</li>
<li>Also, the C300 modules cannot establish synchronization because of the mismatch in Secure Communications configuration.</li>
</ul>
</li>
<li>Select the new C300 module.</li>
<li><p>Click <b>Secure</b>.</p>
<p>The new C300 module is secured and moved to the Secured Nodes table.</p>
<p>The Secure Communications user interface appears as follows:</p>
<p>Unassigned Nodes table</p>
<table>
<tr><th>Name</th><th>Type</th><th>IP Address</th></tr>
<tr><td></td><td></td><td></td></tr>
</table>
<p>The C300 # 12 module moves to Secured Nodes table after being secured.</p>
<p>Secured Nodes table</p>
<table>
<tr><th>Name</th><th>Type</th><th>IP Address</th></tr>
<tr><td>C300 # 11</td><td>C300</td><td>10.0.1.11, 10.0.1.12</td></tr>
<tr><td>C300 # 12</td><td>C300</td><td>10.0.1.12, 10.0.1.11</td></tr>
</table>
</li>
<li><p>Synchronize the secured C300 controller modules.</p>
<p><b>Note</b></p>
<p>Ensure that the Secure Communications configuration is same for the controller modules before synchronizing. The Secure Communications configuration must match for a successful synchronization of the redundant C300 controller pair.</p>
</li>
</ol>
</td></tr>
</table>

Scenario	Procedure
Add a Console Station to a secured cluster.	Perform the following steps. 1. Run Security Manager routing setup utility on the Console Station to identify the location of the Security Manager and the Security Manager Proxies. 2. In the Secure Communications user interface, select the Console Station after it appears in the Unassigned Nodes table, and use the Secure option to secure the station.
Upgrade C300 firmware as part of replacement scenario	If you have secured C300 controllers, it is important to keep spare modules up-to-date with the latest C300 firmware revision. A spare module is not part of the secured list of nodes for a Security Zone. When the spare module is connected to the network to replace a failed module, the secured nodes cannot communicate with the newly-added module. Hence, these nodes cannot be used to update the C300 module firmware. Perform any of the following procedures to upgrade the C300 firmware. • Temporary change of C300 device index 1. Find an unused device index and change the index of the replaced module to this index. 2. Use any secured Server or Console Station to load the latest C300 firmware as the module does not have a secure policy with the temporary device index. 3. After the firmware is successfully updated, change the device index back to the proper value and restart the module. 4. Secure the replaced module from the Secure Communications user interface. Or, • Temporarily unassign Console Station 1. You must have Security Administrator privilege to perform this procedure. 2. Select a Console Station to update the C300 firmware. . 3. Unassign the Console Station from the Secure Communications user interface. The Console Station can now communicate with the replacement module and update the firmware. 4. Secure the Console Station by using the Secure option. Or, • Temporarily unassign C300 module 1. You must have Security Administrator privilege to perform this procedure. 2. Using the Secure Communications user interface, unassign the C300 redundant pair in which has a module being replaced. 3. Use a Console Station to update the firmware. 4. Secure the C300 redundant controller pair by using the Secure option.

Scenario	Procedure
Changing/ugrading firmware for C300–50 ms controller	If you plan to change firmware for C300–50 ms controller or plan to use the C300-50 ms controllers, the following guidelines must be observed. • Before securing nodes, make sure there is no firmware upgrade in progress. Firmware upgrades must be completed before trying to secure nodes. • Before securing nodes, remove any C300-20 ms controller from the Unassigned list. • If firmware of a C300-50 ms controller is being changed to a C300-20 ms controller and the C300-50msec is already secured, unassign the controller. It must be unassigned before the firmware modification is started. **Note** The Secure Communications user interface does not display information about the C300 personality (50ms or 20ms). However, you can determine the personality based on the device index of the C300 contained within the display name of the C300 controllers. This information can be used to determine which C300 controller is 20ms or 50ms.
Moving a secured node to a different IP address.	Perform the following steps to move the IP address of a secured node to a different IP address. 1. Use the Unassign option to unassign the node and move it to the Unassigned Nodes table. 2. Connect the node to a network with a different IP address and restart. The security credentials of the node are deleted. 3. The node with the new IP address is now available in the Unassigned Nodes table. It can be secured, if required.
Reset security credentials of a node.	Perform the following steps to reset or clear the security credentials of a node. 1. If the node is yet to be secured, use the Exempt and subsequently Discard options to remove the node from the Security Area. If the node is already secured, use the Unassign option to unassign the node. Subsequently use the Exempt and Discard options to remove the node from the Security Area. 2. Restart the node. 3. Connect the node to a network with a different IP address and restart. The security credentials of the node are deleted. 4. The node with the new IP address is now available in the Unassigned Nodes table. It can be secured, if required.
SQL server replication and Secure Communications	Ensure that you do not configure the SQL client/server replication through the SQL Server Configuration Manager. This enables a Microsoft supported secure connection specific SQL protocol. The Experion Secure Communications solution must be used to form a secure connection that is used by all protocols between nodes.
DSA Multicast and Secure Communications	The secure connection between the nodes does not affect broadcast/multicast traffic. Experion Server DSA has an option to select multicast, and when selected, this option causes the transfer of low level status information to be sent through multicast. It has no effect on the primary data transfer mechanisms between servers. When the two Experion Servers connected through DSA are secured, the bulk of the data shared between them is done securely, regardless of the DSA multicast option setting.
Level 3 router configuration and Secure Communications	If you implement point-to-point restrictions by IP address in the Level 3 router, ensure that the Security Manager and the Security Manager Proxy paths are added, if needed. If the Security Manager is hosted on the system server that hosts the EMDB, then the communication is probably already enabled because of the EMDB requirement for Experion Server communication.

Scenario	Procedure
Virtualization/Node Rename and Secure Communications	Do not create the nodes that you are planning to secure, by physical node cloning or by deployment of virtual machines from a template. These mechanisms currently do not create unique machine IDs. This issue is to be resolved in a future Experion release. Do not use the *noderenameutil* utility if you are planning to secure the node. This is applicable for both virtual and physical machines where the *node rename* feature is supported without cloning.
Domain Controller Security Package and Secure Communications	To use Secure Communications, all pre-R430.1 domain controllers in the system must be upgraded to the R430.1 High Security Domain Controller Package, so that the SecureComms Administrators and the Local SecureComms Administrators groups are established. For more information about installing the High Security Domain Controller Package, see the *Network and Security Planning Guide*.
Ensure to use the Secure Communications user interface and the Unassign option to clear the certificates and policies in a node.	Ensure to use the Secure Communications user interface and the Unassign option to clear nodes of their certificates and policies, as this ensures that all other secured nodes in the Security Zone are properly updated. If this is not done, then it is possible that nodes may not be able to communicate. Following scenarios may occur if you have not used the Secure Communications user interface and the Unassign option. • Console Station is moved to a different IP address and the old address subsequently reused. – Secured Console Station (CS1) is assigned a different IP address and restarted to clear its certificate and policies. Console Station CS1 now communicates with other nodes of the system using Cleartext until it is secured. A new Console Station (CS2) is added to the system with the IP address that belonged to CS1. It is observed that the Console Station CS2 cannot communicate with other nodes of the system, because the other nodes are still expecting to communicate with that IP address securely. • C300 device index is changed and the old device index is subsequently reused. – Device index of a secured C300 (C300_1) is changed and the controller restarted, which clears its certificate and policies. Now, C300_1 communicates with other nodes of the system using Cleartext until it is secured. A new C300 (C300_2) is added to the system with the device index that belonged to C300_1. It is observed that the C300_2 cannot communicate with other nodes of the system, because the other nodes are still expecting to communicate securely with that device index.

Scenario	Procedure
Restoring Security Manager with a valid backup	The Security Administrator is responsible for taking a backup of the node on which the Security Manager is installed. The backup process can be performed by using the existing Experion backup mechanism, for example Experion Backup and Restore (EBR). The Security Administrator coordinates with the person responsible for taking the Experion backup to ensure that a backup of the node is taken regularly. It is recommended to take backup of the Security Manager node and its Secure Communications configuration whenever a new node has been secured or an already secured node has been unassigned. If a Security Manager node fails: • and the Security Manager node is restored with a valid backup, the Security Administrator may resynchronize the Secure Communications configuration by using the Resynchronize command. For more information about resynchronizing, see "Initializing the Security Area" on page 33. • and no action is taken, the previously deployed policies continue to operate without any issues. **Attention** The Resynchronize command is not required, if there is confidence that the current set of policies deployed to the system match the content of a restored Security Manager. The Security Manager is properly restored and subsequent updates can be successfully performed. The Resynchronize command deploys all policies in the Secure Communications database to the system, even if the policies are different from what is currently operating in the system. If there is a mismatch between the *current* and *being deployed* set of policies, depending on the differences, the nodes may stop communicating with each other. The configuration database and the system can be synchronized during the subsequent system shutdown or maintenance period.

Scenario	Procedure
Restoring Security Manager without a valid backup	If the Security Manager node is replaced and a backup of the Secure Communications configuration (through EBR or other means) was not taken or cannot be restored, the configuration data is effectively lost and secured nodes can no longer be managed through the Secure Communications tool. If it is decided to recover from this situation, then the system must be “reset” to have no Secure Communications behaviors, that matches the empty configuration of a default Security Manager. The Secure Communications configuration can be initiated from the beginning. Perform the following steps to recover. 1. Reinstall the server node that was hosting the Security Manager. Be sure to use the same IP Address that was used previously. This creates an empty Secure Communications configuration database, and preserves the routing paths to the rest of the system. 2. Run the Security Manager routing setup utility on the restored node and identify the node as the Security Manager. 3. Clear the security credentials of all nodes that were previously secured. • For Windows nodes, restart the node. • For redundant C300 controllers perform two consecutive switchovers. • For non-redundant C300 controllers, restart the node. – This step cannot be performed while on-process. If other nodes of the system are restarted and the controller is not started, then communication breaks between the controller and the restarted nodes. – If non-redundant C300 controllers have been secured and a restart cannot be tolerated, then the recovery of the Security Manager should be postponed until the non-redundant controllers can be restarted. When all the nodes appear in the Unassigned Nodes table of the Secure Communications user interface, a new configuration can be established.

6 Migration and interoperability

Related topics

"Migrating to a secure Experion network" on page 54

6.1 Migrating to a secure Experion network

Secure Communications supports migration from a non-secure Experion system to a secure Experion system. The Secure Communications components are installed on the supported Experion nodes during an Experion migration.

For more information about migrating to a secure Experion system, see the respective Experion migration guides.

6.1.1 Setting up Secure Communications

Perform the following steps to set up Secure Communications.

1. Refer to “Planning for Secure Communications” on page 16 to plan for the various components of the Secure Communications.
   - **Recommendation for migrating C300 controllers**

     When you set up Secure Communications, you have to run the Security Manager routing setup utility and restart the nodes. You can avoid an additional restart of C300 controllers if you plan to set up Secure Communications at the time of migration to Experion R431.1 . While migrating to Experion R431.1 , you can plan for Secure Communications and run the Security Manager routing setup utility as part of the migration process before performing the on-process migration of the controllers. When the controllers are restarted as part of the controller migration, the required Secure Communications information is provided to the controllers by BOOTP server.

     If Secure Communications is set up at some point after migration to Experion R431.1 , you have to restart the controllers once again after running the Security Manager routing setup utility.

     – For redundant C300 controllers, you can perform two consecutive switchovers.

     – For non-redundant C300 controllers, the controller must be restarted at the next appropriate opportunity.
2. Run the Security Manager routing setup utility on all the nodes supporting Secure Communications.

Upgrading to Experion

For upgrading to Experion R430.x patches or point releases, no specific actions are required. The Secure Communications policies remain in operation during and after installation of the patches or point releases.

7 Troubleshooting

This section provides guidance and background information about the causes and remedies for failures which may occur in the Windows nodes or C300 controllers on which Secure Communications is set up. The following topics are provided here.

Related topics

"Secure Communications troubleshooting mechanisms" on page 56
"Logs and service names" on page 58
"Troubleshooting issues" on page 59

7.1 Secure Communications troubleshooting mechanisms

Turning ‘off’ or disabling the Secure Communications

While troubleshooting, if you suspect Secure Communications to be a cause for communication issues, you can turn ‘off’ or disable Secure Communications. Turning Secure Communications ‘off’ causes all secured nodes to communicate with each other using Cleartext, instead of Encryption.

You can turn ‘off’ Secure Communications in the following ways.

- Change the security level from Encryption to Cleartext. The mode of communication changes from Encryption to Cleartext. However, the nodes retain the certificates.

  Perform the following steps.

  1. In the Secure Communications user interface, select a **Security Zone** and click **Policy Configuration** tab.
  2. Move the slider or click the required button to set the security policy as **Cleartext**.
  3. Click **Confirm**. Click **OK**.

  OR,

- Select nodes in the Secured Nodes table and use the Unassign option to convert the secured nodes to unassigned nodes. See the section, “To unassign nodes” on page 41. The certificates of the nodes are deleted. Ensure to unassign all nodes before you unassign the Security Manager Proxy nodes.

Avoid direct certificate and policy management with Windows components

Though you can view the certificates and policies of a node, updates to the certificates or policies should never be made directly from Windows unless recommended by Honeywell. The Experion Secure Communications components will update the Windows nodes as needed when changes to the Secure Communications configuration are made.

Windows Firewall settings

Modifying your Windows Firewall settings during troubleshooting may cause a severe impact on the Secure Communications configuration of a system. For example, if the Windows Firewall is turned off, a secured node is not be able to communicate with other secured nodes. Hence, be careful when considering modification of Windows Firewall settings.

Reset a Windows node or a C300 controller to factory settings

A factory setting of a node can be performed for various reasons. For example, a factory setting can be performed after completion of factory acceptance testing. The security credentials of the node are cleared before the nodes are shipped to the site.

You can reset to factory settings in the following ways.

To perform factory settings	Procedure
When access to Secure Communications user interface is available	**Prerequisites** You must be a member of the Secure Comms Administrators group. **Procedure** To unassign a Windows node or a C300 controller, see “To unassign nodes” on page 41.

When reset must be done locally on the node without access to Secure Communications user interface	**Prerequisites** • You must be a member of the Secure Comms Administrators group. • Unassign the node from the Secure Communications user interface. To unassign a node, refer to section “To unassign nodes” on page 41. **Procedure to reset a Windows node to factory settings** Perform the following steps to reset a Windows node to factory settings. 1. Stop the Experion PKS PolicyAgent service. 2. Browse to Secure Communications folder (for example, *C:\Program Data \Honeywell\Experion PKS\Secure Communication*) 3. Open the folder and delete the file PaCache.xml. 4. Start the Experion PKS Policy Agent service. The certificates and policies are deleted and the node is restored to the factory reset state.
	Procedure to reset a C300 controller to factory settings To reset a C300 controller to factory settings, see *Reset Device Index and IP address of a controller* in the *C300 Controller User’s Guide*.

Use of Wireshark with Secure Communications

The common network monitoring tool Wireshark can continue to be used with Experion systems, however, the data of encrypted messages is not viewable. Encrypted messages are displayed as ESP protocol and it can be observed that a message was sent, but the details cannot be exposed.

PING command usage

Use the PING command to test ICMP traffic flow between two nodes to get additional information beyond the success or failure of Honeywell applications.

Honeywell applications use TCP, UDP, and ICMP protocols for various application communications.

PING uses the ICMP (Internet Control Message Protocol) communication protocol. ICMP traffic is secured by Secure Communications in Experion.

Note

This command can be used only in Windows nodes.

7.2 Logs and service names

Experion service names for PDP and PA components

Following are the Windows Service names for the Secure Communications components.

Secure Communications component	Windows Service Name
Policy Agent (PA)	Experion PKS Policy Agent
Policy Decision Point (PDP)	Experion PKS Policy Decision Point

The following logs provide status for the secured connections. You can refer to the following logs to troubleshoot Secure Communications issues.

Logs	Description
Windows security event logs	Provides security events for the secured Experion Servers and Console Stations. Windows security events are available through the Windows Event Viewer.
Policy Decision Point, Certificate Authority, Policy Agent, and User Interface process application logs	Provides information on success or failure of Secure Communications activities. The logged details are controlled by a collection of paranoid settings. Use the Honeywell Log Viewer tool to adjust the paranoid settings for the following components. • SECPDP – Policy Decision Point • SECCERT – Certificate Authority • SECPA – Policy Agent • SECTOOLS – User Interface These logs are available at: • `<Custom Installation Path Runtime>\Honeywell\Experion PKS\securecommslog.txt` OR `C:\ProgramData\Honeywell\Experion PKS\securecommslog.txt` You can use the Diagnostic Capture tool (DCT) to create a diagnostic package, which the Honeywell Technical Assistance Center (TAC) uses for detailed analysis of the problem. For more information about DCT, see the *Troubleshooting Guide*.
C300 history log	Provides information about the C300 controllers participating in Secure Communications. You can use the CTool utility to capture crash block or user log diagnostic data associated with a given Series C device as well as view history log data. For more information about troubleshooting the controller issues, you can also see the *Troubleshooting* section in the *C300 Controller User's Guide*.

7.3 Troubleshooting issues

Issue description	Recovery	Workaround
Secure communication is not licensed error is displayed.	None	Restart the Secure Communications user interface to get a fresh read of the license from the Security Manager. This scenario may occur if the Policy Decision Point service is started before the Security Manager license server component.
The C300 load operation fails with an error *connection could not be established with controller*. After setting up the Secure Communications if you have unloaded/deleted a controller from the Monitoring side, a first time load failure is observed when you attempt to reload the unloaded/deleted controller after a long period of time. This issue is observed when the following conditions are met. • Controller is participating in Secure Communications and Secure Communications is enabled. • Controller has been unloaded/deleted from the Monitoring side (and only resides on the Project side). • Controller reload has been attempted at least five minutes after being unloaded/deleted.	Attempt to load the controller within five minutes of the failure.	• Reload the controller within the five minutes of unloading/deleting the controller. OR • Attempt another reload when five minutes have elapsed and first time load has failed.

8 Notices

Trademarks

Experion®, PlantScape®, SafeBrowse®, TotalPlant®, and TDC 3000® are registered trademarks 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/ps/thirdpartylicenses.

8.1 Documentation feedback

You can find the most up-to-date documents on the Honeywell Process Solutions support website at:

http://www.honeywellprocess.com/support

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 your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

8.2 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://honeywell.com/pages/vulnerabilityreporting.aspx

Submit the requested information to Honeywell using one of the following methods:

- Send an email to security@honeywell.com.

  or

- Contact your local Honeywell Process Solutions Customer Contact Center (CCC) or Honeywell Technical Assistance Center (TAC) listed in the “Support and other contacts” section of this document.

8.3 Support and other contacts

For support, contact your local Honeywell Process Solutions Customer Contact Center (CCC).

North America

Country	Phone	Facsimile	Email
Canada and United States	800-822-7673	973-455-5000	askssc@honeywell.com

Northern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Denmark	07:00 – 18:00	80–252165	+45 6980 2349	hpscustomersupport@honeywell.com
Finland	08:00 – 19:00	0800–9–15938	+358 (0)9 2319 4396	hpscustomersupport@honeywell.com
Ireland	06:00 – 17:00	1800939488	+353 (0)1 686 4905	hpscustomersupport@honeywell.com
Netherlands	07:00 – 18:00	0800 020 3498	+31 (0)20 524 1609	hpscustomersupport@honeywell.com
Norway	07:00 – 18:00	800–11478	47–852–287–16	hpscustomersupport@honeywell.com
Sweden	07:00 – 18:00	0200883167	+46 (0)8 509 097 84	hpscustomersupport@honeywell.com
United Kingdom	06:00 – 17:00	08002797226	+44 (0)20 3031 1064	hpscustomersupport@honeywell.com

Southern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Belgium	07:00 – 18:00	080048580	+32 (0)2 791 96 02	hpscustomersupport@honeywell.com
France	07:00 – 18:00	0805100041	+33 (0)1 72 74 33 44	hpscustomersupport@honeywell.com
Luxembourg	07:00 – 18:00	8002–8524	+352 24611292	hpscustomersupport@honeywell.com
Spain	07:00 – 18:00	800099804	+34 91 791 56 25	hpscustomersupport@honeywell.com
Portugal	06:00 – 17:00	800–8–55994	+34 91 791 56 25	hpscustomersupport@honeywell.com

Eastern Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Bulgaria	08:00 – 19:00	700 20771	+359 (0)2 489 7384	hpscustomersupport@honeywell.com
Croatia	07:00 – 18:00	0800 80 6392	+420 227 204 957	hpscustomersupport@honeywell.com
Czech Republic	07:00 – 18:00	800 142 784	+420 227 204 957	hpscustomersupport@honeywell.com
Hungary	07:00 – 18:00	06 800 20 699	+36 (06) 1 577 7371	hpscustomersupport@honeywell.com
Poland	07:00 – 18:00	00 800 121 50 46	+48 22 485 35 10	hpscustomersupport@honeywell.com
Romania	08:00 – 19:00	0 800 800 178	+40 (0)31 710 7590	hpscustomersupport@honeywell.com
Russia Federation	09:00 – 20:00	8.10.80 02-412 50 11	+7 495 796 98 94	hpscustomersupport@honeywell.com

Country	Local Time Business Hours	Phone	Facsimile	Email
Slovakia	07:00 – 18:00	0800 002 340	+421 (0)2 3301 0376	hpscustomersupport@honeywell.com

Central Europe

Country	Local Time Business Hours	Phone	Facsimile	Email
Austria	07:00 – 18:00	0800 006438	+43 (0)1 253 6722 4904	hpscustomersupport@honeywell.com
Germany	07:00 – 18:00	0800 7239098	+49 (0)30 6908 8463	hpscustomersupport@honeywell.com
Greece	08:00 – 19:00	00800 12 9493	+30 21 1 268 6973	hpscustomersupport@honeywell.com
Israel	08:00 – 19:00	1 809 407 309	+972 (0)2 591 6148	hpscustomersupport@honeywell.com
Italy	07:00 – 18:00	8000 35205	+39 06 96681356	hpscustomersupport@honeywell.com
Switzerland	07:00 – 18:00	00 080 035	+41 (0)31 560 41 60	hpscustomersupport@honeywell.com

Middle East and South Africa

Country	Local Time Business Hours	Phone	Email
Bahrain	08:00 – 19:00	8008 1343	hpscustomersupport@honeywell.com
Oman	08:00 – 19:00	8007 7595	hpscustomersupport@honeywell.com
Qatar	08:00 – 19:00	800 5460	hpscustomersupport@honeywell.com
Saudi Arabia	08:00 – 19:00	800 844 5309	hpscustomersupport@honeywell.com
South Africa	07:00 – 18:00	0800 983 634	hpscustomersupport@honeywell.com
Turkey	08:00 – 19:00	00800 448823587	hpscustomersupport@honeywell.com
United Arab Emirates	09:00 – 20:00	8000 444 0300	hpscustomersupport@honeywell.com

Other regions

In other regions, contact your local Honeywell Technical Assistance Center (TAC) for support.

Region	Phone	Facsimile	Email
Pacific	1300-364-822 (toll free within Australia) +61-8-9362-9559 (outside Australia)	+61-8-9362-9564	GTAC@honeywell.com
India	+91-20-6603-2718 / 19 1800-233-5051	+91-20-6603-9800	Global-TAC-India@honeywell.com
Korea	+82-80-782-2255 (toll free within Korea)	+82-2-792-9015	Global-TAC-Korea@honeywell.com
People’s Republic of China	+86-21-2219-6888 800-820-0237 400-820-0386		Global-TAC-China@honeywell.com
Singapore	+65-6823-2215	+65-6445-3033	GTAC-SEA@honeywell.com
Japan		+81-3-6730-7228	Global-TAC-JapanJA25@honeywell.com

World Wide Web

Honeywell Process Solutions support website:

http://www.honeywellprocess.com/support

Elsewhere

Contact your nearest Honeywell office.

8.4 Training classes

Honeywell holds technical training classes on Experion PKS. These classes are taught by experts in the field of process control systems. For more information about these classes, contact your Honeywell representative, or see http://www.automationcollege.com.