QuickPanel+2

SECURE DEPLOYMENT GUIDE

Contents

Warnings and Caution Notes as Used in this Publication

⚠ WARNING

Warning notices are used in this publication to emphasize that hazardous voltages, currents, temperatures, or other conditions that could cause personal injury exist in this equipment or may be associated with its use.

In situations where inattention could cause either personal injury or damage to equipment, a Warning notice is used.

⚠ CAUTION

Caution notices are used where equipment might be damaged if care is not taken.

Note: Notes merely call attention to information that is especially significant to understanding and operating the equipment.

These instructions do not purport to cover all details or variations in equipment, nor to provide for every possible contingency that may arise during installation, operation, and maintenance. The information is supplied for informational purposes only, and Emerson makes no warranty as to the accuracy of the information included herein. Changes, modifications, and/or improvements to equipment and specifications are made periodically and these changes may or may not be reflected herein. It is understood that Emerson may make changes, modifications, or improvements to the equipment referenced herein or to the document itself at any time. This document is intended for trained personnel familiar with the Emerson products referenced herein.

Emerson may have patents or pending patent applications covering the subject matter in this document. The furnishing of this document does not provide any license whatsoever to any of these patents.

Emerson provides the following document and the information included therein as-is and without warranty of any kind, expressed or implied, including but not limited to any implied statutory warranty of merchantability or fitness for a particular purpose.

Section 1: About this Guide

⚠ CAUTION

Emerson provides these general recommendations and guidelines to aid the end-user in managing security risks associated with the operation of QuickPanel+2. It is entirely the owner's responsibility to ensure the security of the Windows 10 IOT Enterprise 2021 LTSC OS and any associated applications deployed on the platform.

This document provides information that can be used to help improve the cyber security of the QuickPanel+2 product.

It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring the QuickPanel+2 product. Secure deployment information is provided in this manual for the QuickPanel+2 product.

1.1 Revisions in this Manual

Table 1: Product Revision

Rev	Date	Description
A	Jul 2026	Initial Publication

The most recent documentation is available on the Emerson technical support website listed at the end of this document.

1.2 Related Documentation

This section provides information on related documents. These documents include product landing pages and related documents that contain additional information.

1.2.1 QuickPanel+2 Documentation

Document ID	Document Title
GFK-3317	QuickPanel+2 User Manual
GFK-3318	QuickPanel+2 Quick Start Guide
GFK-3319	QuickPanel+2 Installation, Management, and Requirements

Section 2: Introduction

This document provides information that can be used to help improve the cyber security of systems that include QuickPanel+2 products. It is intended for use by control engineers, integrators, IT professionals, and developers responsible for deploying and configuring QuickPanel+2 products. Secure deployment information is provided in this manual for the following QuickPanel+2 products.

QuickPanel+2 Products

Product	Catalog Number	Product Description
QuickPanel+2 7"	IC762CSS07CDA	QuickPanel+2 7"screen with View and Control
	IC762CSB07CDA	QuickPanel+2 7"screen with View and Control (with blank bezel)
	IC762COS07CDA	QuickPanel+2 7"screen with View and Control (with SLR screen)
	IC762CSS07CDACA	QuickPanel+2 7"screen with View and Control (with Conformal coating)
	IC762CSB07CDACA	QuickPanel+2 7"screen with View and Control (with blank bezel and conformal coating)
QuickPanel+2 10"	IC762CSS10CDA	QuickPanel+2 10"screen with View and Control
	IC762CSB10CDA	QuickPanel+2 10"screen with View and Control (with blank bezel)
	IC762COS10CDA	QuickPanel+2 10"screen with View and Control (with SLR screen)
	IC762CSS10CDACA	QuickPanel+2 10"screen with View and Control (with Conformal coating)
	IC762CSB10CDACA	QuickPanel+2 10"screen with View and Control (with blank bezel and conformal coating)
QuickPanel+2 12"	IC762CSS12CDA	QuickPanel+2 12"screen with View and Control
	IC762CSB12CDA	QuickPanel+2 12"screen with View and Control (with blank bezel)
	IC762COS12CDA	QuickPanel+2 12"screen with View and Control (with SLR screen)
	IC762CSS12CDACA	QuickPanel+2 12"screen with View and Control (with Conformal coating)
	IC762CSB12CDACA	QuickPanel+2 12"screen with View and Control (with blank bezel and conformal coating)
QuickPanel+2 15"	IC762CSS15CDA	QuickPanel+2 15"screen with View and Control
	IC762CSB15CDA	QuickPanel+2 15"screen with View and Control (with blank bezel)
	IC762COS15CDA	QuickPanel+2 15"screen with View and Control (with SLR screen)

Product	Catalog Number	Product Description
	IC762CSS15CDACA	QuickPanel+2 15"screen with View and Control (with Conformal coating)
	IC762CSB15CDACA	QuickPanel+2 15"screen with View and Control (with blank bezel and conformal coating)

2.1 What is Security?

Security is the process of maintaining the confidentiality, integrity, and availability of a system:

- **Confidentiality**: Ensure that only those people whom you want to see certain information can see it.
- **Integrity**: Ensure the data is what it is supposed to be.
- **Availability**: Ensure the system or data is available for use.

Emerson recognizes the importance of building and deploying products with these concepts in mind and encourages customers to take appropriate care in securing their Emerson products and solutions. As Emerson's product vulnerabilities are discovered and fixed, security advisories are issued to describe each vulnerability in each product version as well as the version in which the vulnerability was fixed. Emerson Product Security Advisories can be found at the following location: https://www.emerson.com/Industrial-Automation-Controls/support.

2.2 I have a Firewall: Isn’t that Enough?

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

Therefore, Emerson recommends taking a Defense in Depth approach to security.

2.3 What is Defense in Depth?

Defense in Depth is the concept of using multiple, independent layers of security to raise the cost and complexity of a successful attack. To carry out a successful attack on a system, an attacker would need to find not just a single exploitable vulnerability but would need to exploit vulnerabilities in each layer of defense that protects an asset.

For example, if a system is protected because it is on a network protected by a firewall, the attacker only needs to circumvent the firewall to gain unauthorized

access. However, if there is an additional layer of defense, say a username/password authentication requirement, now the attacker needs to find a way to circumvent both the firewall and the username/password authentication.

2.4 General Recommendations

Adopting the following security best practices should be considered when using Emerson products and solutions.

- Edge devices span both control networks and wide area networks (WAN), potentially extending to include access to the Internet as a whole. Network segmentation and firewall rules must be carefully considered to reduce the allowed traffic to the bare minimum needed for operation. Care must be taken to control, limit, and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures. All communication endpoints should be considered individually, and if a specific protocol or the device does not require wide area network access, it is strongly recommended that the relevant protocols be restricted to the most limited network possible.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply the latest Emerson product security updates, SIMs, and other recommendations.
- Apply the latest operating system security patches to control systems PCs.
- Use anti-virus software on control systems PCs and keep the associated anti-virus signatures up to date.
- Use whitelisting software on control systems PCs and keep the whitelist up to date.

2.5 Checklist

This section provides a sample checklist to help guide the process of securely deploying QuickPanel+2 product.

1. Create or locate a network diagram.
2. Identify and record the required communication paths between nodes.
3. Identify and record the protocols required along each path, including the role of each node.
4. Revise the network as needed to ensure appropriate partitioning, adding firewalls or other network security devices as appropriate. Update the network diagram. (For additional details, refer to the section entitled *Network Architecture & Secure Deployment*.)
5. Configure firewalls and other network security devices
6. Enable and/or configure the appropriate security features on each QuickPanel+2 module.
7. For each QuickPanel+2 module, change every supported password to something other than its default value.
8. It is the customer's responsibility to configure and manage Windows services such as security updates, windows patches, and firewall settings.
9. For each QuickPanel+2 module, assign a unique device name to that module. (From the **Control Panel**, select **System**, then select **Device Name**). This is required for customer use cases like Web Services Access.
10. Harden the configuration of each QuickPanel+2 module, disabling unneeded features, protocols, and ports.
11. Test/qualify the system.
12. Create an update/maintenance plan.

Note: Secure deployment is only one part of a robust security program. This document, including the checklist above, is limited to only providing secure deployment guidance

Section 3: Communication Protocols

This chapter describes how the supported application protocols for Ethernet and serial ports are used with QuickPanel+2. Lower-level Ethernet protocols are not discussed here but are instead assumed to be supported when needed by the application protocol.

The security of a control system can be enhanced by limiting the protocols allowed, and the paths across which they are allowed. This can be accomplished by disabling all communication protocols that are not needed on a particular device, and by using appropriately configured and deployed network security devices (firewalls, routers) to block any protocol (whether disabled or not) that does not need to pass from one network/segment to another.

Emerson recommends limiting the protocols allowed by the network infrastructure to only those that are required for the intended application. Successfully doing this requires knowing which protocol is needed for each system-level interaction.

This information is intended to be used to help guide the specification of the network architecture and to help configure firewalls internal to that network. The intent should be to support only the required communications paths for the specific installation.

3.1 Ethernet Protocols

This section indicates which Ethernet protocols are supported by the QuickPanel+2. Note that some of the supported protocols may not be required in each system, since the installation may only be using a subset of the available protocols.

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application Layer are the Transport, Internet, and Link Layers. Information on the supported protocols from these three lower layers is summarized here.

Table 2: Ethernet Protocols

Protocol		QuickPanel+
Link	ARP	✓
	LLDP	✓
Internet	IPv4	✓
	IPv6	✓
	ICMP	✓
	IGMP	✓
Trans	TCP	✓
	UDP	✓
	BOOTP Client	—

Protocol		QuickPanel+
Application Layer	DCE/RPC Client	✓
	DNS Client	✓
	Ethernet Global Data	✓
	TFTP client	—
	HTTPS server	✓
	Modbus TCP master	✓
	Modbus TCP slave	✓
	PROFINET DCP client	—
	PROFINET DCP server	—
	PROFINET IO	—
	MRP	—
	SNTP client	✓
	SRTP	✓
	Telnet Client	✓
	OPC UA Client	✓
	LPR /LPD & SMB	✓
	PCL5	✓
	SRP-6a	✓

3.2 Serial Protocols (RS–232, RS-422, RS–485)

QuickPanel+2 supports communication over serial ports (RS-232, RS-422 and RS-485). The information provided here should be used to help guide the specification of any external security controls required to restrict remote serial access, as well as the specification of any required physical security.

Table 3: Serial Protocols

Protocol	QuickPanel+2
Application-specific	✓
ASCII Slave	✓
Modbus RTU Slave	✓
Modbus RTU Master	✓
Modbus ASCII Master	✓

3.3 USB Protocols

In addition to Ethernet and Serial communications, the QuickPanel+2 device supports USB-based communication with the following ports available:

- 2x USB 3.0 (Type-A)
- Maximum Supply Current: 0.9 A (per port)

In addition to supporting the attachment of external memory media/disk, the QuickPanel+2 USB ports also support the following protocols:

Protocol	QuickPanel+2
Application-specific†	✓
USB†	✓
USB To Serial‡	✓
USB To Ethernet‡	✓
† USB printer driver provides support for printing over a USB connection	

3.4 Server

This section summarizes the available communication-centric functionality, where the communication is initiated by another PC.

Functionality		Required Application	Example Clients
Ethernet	EGD Consumption	Ethernet Global Data	Other controllers
	Process EGD Commands	Reliable Datagram Svc	Other controllers
	Modbus TCP Slave	Modbus TCP	HMI Other controllers third-party Masters
	TRAPI Server	SRP-6a	HMI and PME communication
	Web Server	HTTPS	HTML Dashboard
	Print Spooler	LPR	Print
	Connext IO Data Server	OPC UA	QuickPanel+2
Serial	QuickPanel+2	Modbus Serial RTU Modbus RTU Master Modbus ASCII Master Modbus ASCII Slave	QuickPanel+2

3.5 Client

This section summarizes the available communication-centric functionality, where the communication is initiated by the QuickPanel+2 device. The servers involved in these communications are selected by the user application and/or configuration.

Functionality		**Required Application**	**Example Servers**
Ethernet	SRTP	SRTP	Other controllers
	Modbus TCP	Modbus TCP	3rd-party device other controllers
	EGD Production	Ethernet Global Data	Other controllers
	Send EGD Commands	Reliable Datagram Svc	Other controllers
	Time Synchronization	SNTP	SNTP server
	Lookup IP addresses by	DNS	DNS server
	Connext Historian Manager	OPC UA HDA	Historian Database (SQL Server 2019, MySQL, PostgreSQL)
	QuickPanel+2 target	View Networking	PC
	Printing on QuickPanel+2	LPR / TCP IP	Print Server on PC

3.6 Ethernet Firewall Configuration

Network-based and host-based firewalls should be configured only to allow expected and required network traffic. This section identifies the Ether Types and the TCP/UDP ports used by the protocols supported on the device.

This information should be used to help configure network firewalls, to support only the required communications paths for any installation.

QuickPanel+2 firewall/network profile is set to public. This profile is most restrictive and secure. It is configured to support application layer protocol-specific ports.

The *Clients for Microsoft Network* is a core Windows networking component that allows a computer to access shared files, printers, and other shared network resources hosted on Windows servers.

In QuickPanel+2 devices, this feature is **disabled by default** to enhance system security. If required, it can be enabled manually by clearing the **Allow Remote Assistance Connections to this Computer** option under **Ethernet Properties → Networking**.

Configurations	Description
Client for Microsoft Networks	Enables a Windows system to access shared files, printers, and other network resources on a Windows server
File and Printer Sharing for Microsoft Networks	Allows other network devices to access shared filed and printers on the local system.
QoS Packet Scheduler	Manages network bandwidth allocation for Quality of Service (QoS).
Microsoft Network Adapter Multiplexor Protocol	Supports network adapter teaming for load balancing and fault tolerance.
Microsoft LLDP Protocol Driver	Implements the Link Layer Discovery Protocol (LLDP) for device discovery and topology mapping.
Link-Layer Topology Discovery Mapper I/O Driver	Identifies and maps devices on the network.
Link-Layer Topology Discovery Responder	Allows the device to be discovered and displayed in network topology maps.
Internet Protocol Version 6 (IPv6)	Provides next-generation IP addressing and connectivity.
Registration of IPv4 address in DNS / NetBIOS over TCP/IP	Registers the device's IPv4 address in DNS and supports NetBIOS communication over TCP/IP.

3.7 Lower-level Protocols

Ethernet communication is typically described using four layers, each with its own set of protocols. At the top of that hierarchy is the Application layer. Below the Application layer are the Transport, Internet, and Link layers.

Information on the supported protocols from these three lower layers is summarized in the following tables. Each of these lower-level protocols is required by one or more of the application protocols supported on the QuickPanel+2 device.

Link Layer Protocols

Protocol	EtherType
ARP	0x0806
LLDP	0x88cc

Internet Layer Protocols

Protocol	EtherType	IP Protocol #
IPv4	0x0800	N/A
ICMP		1
IGMP		2

Transport Layer Protocols

Protocol	EtherType	IP Protocol #
TCP	0x0800	6
UDP		17

3.7.1 Application Layer Protocols

The QuickPanel+2 can act as a server (OPC Server), responding to requests sent over OPC. It is also capable of acting as a client, sending requests to other servers using OPC. The exact set of protocols that are enabled/used will depend on which components are installed/ downloaded from the PAC Machine Edition configurator, how they are configured, and the details of the application program that is running on the device.

Protocol	Server TCP Port	Dest UDP Port
DCERPC	135 Dynamic Ports 49152–65535: used for actual RPC service communication after endpoint mapping	
DNS	53	53 on server >1023 on client
View Runtime Server	12396, 12397	—
TRAPI Server	57176	—
View Networking	22739, 22740	—
Control – Warm Standby	12399	—
Ethernet Global Data	—	18246
HTTPS	9090	—
Modbus TCP	502	—
SNTP	—	123
SRTP	18245	—

3.8 Firewall with Advanced Security

By default, all the listening ports of Windows are disabled in the firewall. Only required ports are enabled by default.

- The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4 networks to establish multicast group memberships. Mostly used for online streaming video and gaming. IGMP is disabled by default in QuickPanel+2.
- UPnP protocol is used for ease of configuration; for example, computer games running on the system can auto-configure the system firewall to let external players on the internet join in. If an attacker gains access to the system, he can use this feature to compromise the firewall settings. UPnP port 1900 is disabled in QuickPanel+2.
- SMB protocol is used for file and printer sharing and also as inter-process communication. Attackers exploit this feature using worms that could gain complete control of the system. SMB v1 protocol is disabled in QuickPanel+2.

Section 4: Security Capabilities

4.1 External Storage – SD Card

The QuickPanel+2 device provides an SDXC card slot for external storage. The View Runtime application running on this device can use this external storage for logging real-time data. The SDXC card can be used as a buffer medium to transfer the real-time data to a Proficy Historian Server. When **alarm logging** is enabled in the View Runtime application, the logs are by default sent to the SD card if the card was inserted before the Runtime started.

It is up to the user to decide how he wants to archive/protect the data on the SD card. However, with Enhanced Security enabled for the configured QuickPanel+2 target, the user can have the data archived to the SD card only after providing the password to download/start Runtime.

4.2 Local Media Download

Local Media Download is the functionality for upgrading the Runtime application using an SD card. This process is inherently more secure than other upgrade processes because it requires that the user be physically present.

The user must first back up the Runtime Project to the SD card by using one of the following methods:

- Download the QuickPanel+2 target to a local folder on the PC and then transfer the folder contents to the SD card, or directly download to the SD card media connected to the PC.

  Or

- Install the SD card media into the QuickPanel+2 and run the **Copy Project to SD Card** tool available on the device desktop.

Once the Runtime project is backed up to the SD card, the user can upgrade the runtime application/project on the targeted device.

4.3 Firmware Updates

The steps required to update the firmware are provided in Image Recovery in Section 7 Image Recovery of the GFK-3317 QuickPanel+2 User Manual.

4.4 TRAPI Server

The TRAPI Server is a proprietary service built on the TCP/IP layer. TRAPI Server running on the device helps the PAC Machine Edition Configurator (editor) connect to the target device available on the network (IP Address). It supports many different operations that require connecting to the device, including:

- Upload / Download the user application and configuration to the QuickPanel+2
- Start/Stop the View Runtime
- Going online with the QuickPanel+2
- Verify Equality/upgrade of correct version of TrapiServer.exe on the device.

Note: *TRAPI Server is built on the TCP/IP transfer layer, and it supports both secured (using SRP-6a protocol) and unsecured connections.*

4.5 Connext I/O Data Server

I/O Data Server module manages:

- Field communications by defining and centralizing variables.
- Process data recordings using the Historian

4.6 List Privileges

List privilege means configuring the system so that it is only capable of doing things that it is expected to do, and nothing else. In simple terminology, disable all features that are not normally needed by the product.

By default, services that are not required, like TFTP, SSH login, are disabled in QuickPanel+2. The user enables those services if it is required for the user application.

4.7 User Access Control (UAC)

UAC is turned to the maximum security level by default in QuickPanel+2.

Section 5: Configuration Hardening

This section is intended to assist in reducing the potential attack surface by providing information that can be used to harden the configurations that are present in a PACSystems OI configuration. Configuration hardening should be considered in addition to enabling and using security features such as Authentication, Access Control, and Authorization.

In general, Emerson recommends disabling all services and protocols that are not required for the intended application.

It is the customer's responsibility to configure and manage Windows services such as security updates, Windows patches, and firewall settings.

5.1 Harden Access to each Industrial Data Source

When implementing applications consuming industrial data from a data source like an OPC UA Server, it is important to configure the visibility of variables or registers such that only those tags that are expected to be consumed are readable by the application and other network nodes.

For example, OPC UA variables in the PACSystems CPUs can be left unpublished, published internally to other components of the User Application, published as External Read-Only, or published as External Read/Write. Variables should not be published as External Read-Only unless they need to be read by an embedded Linux application or another network node. Variables should not be published as External Read/Write unless they need to be read and written to by a Field Agent or another network node.

As an additional layer of security, Emerson strongly recommends enabling authentication for read and write operations on industrial data sources wherever supported. For example, PACSystems CPUs should have Enhanced Security enabled with passwords protecting PRIV Levels 2, 3, and 4. With this set, an attacker on the network would be unable to, for example, write to any OPC UA variables that are accidentally published as read/write on a PACSystems OPC UA Server without knowing the PRIV Level 2 password.

If more granular control of specific read and write operations to industrial data sources is required, an application-level firewall with knowledge of industrial protocols can be placed in line between the industrial data source and Field Agent. The firewall can be configured to enforce policies that whitelist specific devices from reading or writing to specific OPC UA variables.

5.2 Disabled Network Clients

Due to security concerns, the following servers are disabled by default on the QuickPanel+2 device:

- SNTP Client
- TFTP Client
- Telnet Client

5.3 Enhanced Security

PAC Machine Edition is the configuration tool for the QuickPanel+2 device. If the Enhanced Security feature is enabled on the PAC Machine Edition Configurator (editor) connected to the QuickPanel+2, user password entry and authentication are required when an attempt is made to change the configuration of the QuickPanel+2 device. Specifically, when you use the editor to attempt one of the following operations, you must provide a password:

- Downloading
- Uploading
- Going online
- Starting Runtime
- Stopping Runtime
- Updating the security settings

Enhanced Security is disabled by default on the PAC Machine Edition Configurator, and it reports warnings that occur during validation of the QuickPanel+2 configuration. Configuring a QuickPanel+2 using a PAC Machine Edition Configurator with Enhanced Security enabled causes Enhanced Security to be enabled on the QuickPanel+2 device.

Note:

- *If the user forgets the password, run the Reset Enhanced Security tool that is available through the Programs and System menu, or contact the technical support for any further issues. Refer to the section QuickPanel+2 Utilities*
- *for further details on the Reset Enhanced Security tool.*

5.4 Network Devices and Features

Table 4: Network Devices and Features

Device/ Feature	Enable/ Disable
Remote Desktop Device Redirector Bus	Disabled
Microsoft Kernel Debug Network Adapter	Disabled. bcdedit /debug off (Default not shown in “Device Manager”)
Autoplay for USB	Disabled. Use Edit Group Policy Option
DEP (Data Execution Prevention)	Enabled
Remote Assistance	Disabled

5.5 QuickPanel+2 Utilities

The QuickPanel+2 Utilities can be launched from the desktop using the shortcut icon from the Start menu. This tool is used to launch frequently used applications like Task Manager, Device Manager, PACS Analyzer, etc., to configure brightness, backlight, store the settings of certain parameters of the device to a file, and then apply/ restore the saved settings to the same or any other device from the saved encrypted file whenever required.

5.5.1 Reset Enhanced Security

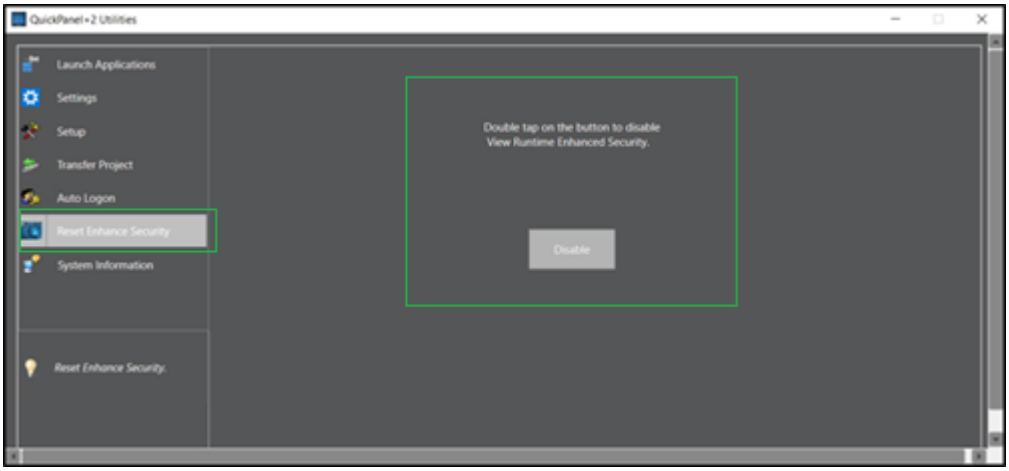
The QuickPanel+2 is configured using the PAC Machine Edition application. Using the PAC Machine Edition Enhanced Security feature, users can specify password protection for any network-connected QuickPanel+2 device to perform certain operations, such as the download operation. Every operation to connect to the device requires a password.

If you forget or do not know your password, the Reset Enhanced Security feature enables a QuickPanel+2 configuration download on the device by permitting the user to disable the Enhanced Security feature using the double-tap feature.

To disable Enhanced Security

1. Open the **QuickPanel+2 Utilities** and navigate to the **Reset Enhanced Security** page.
2. Disable the Enhanced Security setting by double tab on **Disable** button.

Figure 1 QuickPanel+2 Utilities



5.5.2 Ethernet Interface

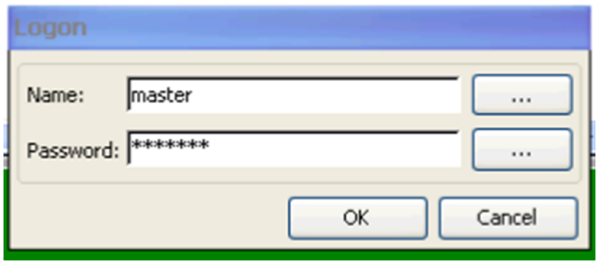
Interface	Availability
Bootp Client	Not available on the QuickPanel+2
TFTP Client	Can be enabled/disabled using the Windows feature settings
IP Routing	Can be disabled by configuring the network port in Control Panel
DNS Client	Can be disabled by configuring the network port in Control Panel
SNTP Client	Can be enabled/disabled using the QuickPanel+2 Utilities Tool
Web Server	Can be enabled/disabled using the QuickPanel+2 Utilities Tool

5.6 User Management Facility

The User Management facility, provided by the View applications on the QuickPanel+2 device, can be utilized to manage users with restricted privileges.

View Runtime running on QuickPanel+2 provides the functionality to add new users and provides the required permissions/privileges to access the functionality.

Figure 2: User Management Utility



The Master displayed in the following figure has full privileges (Exit Runtime, View Inspectors, Change Data, and Context Menus).

Figure 3: Edit User List

Like the Master, an Administrator can add/delete users and assign required permissions as illustrated in the following figure.

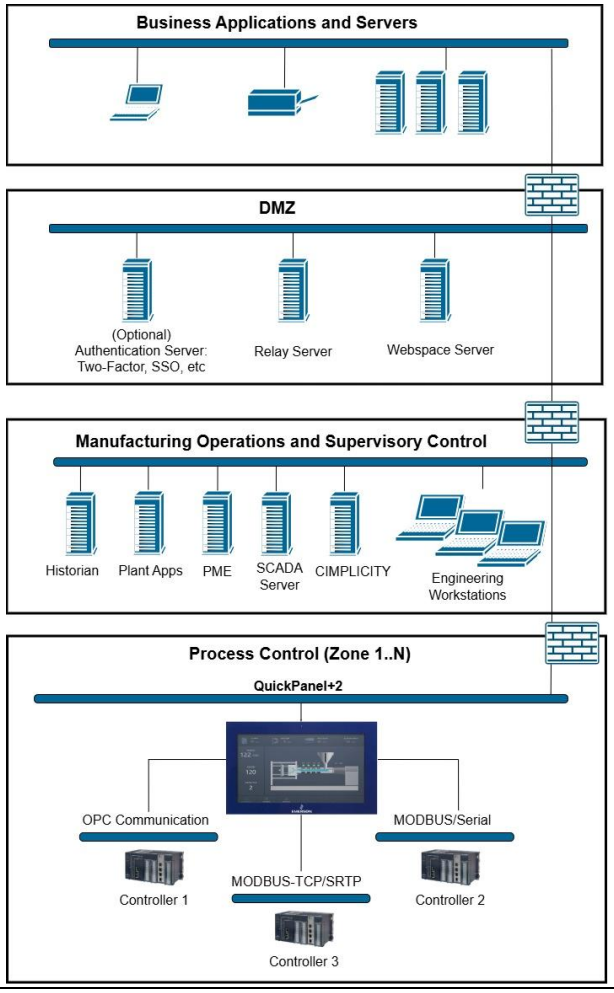
Figure 4: Assembly Operator

Section 6: Network Architecture and Secure Deployment

This chapter provides security recommendations for deploying QuickPanel+2 controllers in the context of a larger network.

The Manufacturing Zone networks (which include the Manufacturing Operations, Supervisory Control, and Process Control networks) are segregated from other untrusted networks, such as the enterprise network (also referred to as the business network, corporate network, or intranet) and the internet, using a Demilitarized Zone (DMZ) architecture. The Process Control networks have limited exposure to traffic from higher-level networks, including other networks in the Manufacturing Zone, as well as from other Process Control networks.

Figure 5: Network Architecture



6.1 Remote Access and Demilitarized Zones (DMZ)

A DMZ architecture uses two firewalls to isolate servers that are accessible from untrusted networks. The DMZ should be deployed such that only specific (restricted) communication is allowed between the business network and the DMZ, and between the control network and the DMZ. The business network and the control networks should ideally not communicate directly with each other.

If direct communication to a control network is required from the business network or from the internet, carefully control, limit, and monitor all access. For example, require two-factor authentication for a user to obtain access to the control network using Virtual Private Networking (VPN), and even then, restrict the allowed protocols/ports to just the minimum set required. Further, every access attempt (successful or not) and all blocked traffic should be recorded in a security log that is regularly audited.

6.2 Access to Process Control Networks

Ethernet traffic from the Supervisory Control network to the Process Control networks should be restricted to support only the functionality that is required. If a protocol (such as Modbus TCP) doesn't need to be used between those regions, then the firewall should be configured to block that protocol. Additionally, if a controller has no other reason to use that protocol, then – in addition to blocking it at the firewall – the controller itself should be configured to disable support for the protocol.

Note: *Network Address Translation (NAT) firewalls typically do not expose all the devices on the trusted side of the firewall to devices on the untrusted side of the firewall. Further, NAT firewalls rely on mapping the IP address/port on the trusted side of the firewall to a different IP address/port on the untrusted side of the firewall. Since communication to QuickPanel+2 controllers will typically be initiated from a PC on the untrusted side of the Process Control network firewall, protecting a Process Control network using a NAT firewall may cause additional communication challenges. Before deploying NAT, carefully consider its impact on the required communications paths.*

Section 7: Auto Logon

Auto Logon is the procedure to enable/ disable the Windows login when the QuickPanel+2 device boots. If the Auto Logon is enabled, Windows does not prompt the user to enter login credentials during device bootup. The following sections will detail the procedure to enable/ disable Auto Logon during the out-of-the-box experience flow and from second-time bootup.

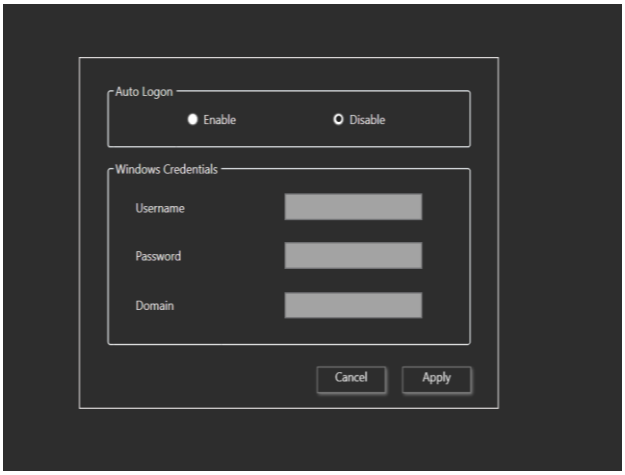
⚠ CAUTION

Automatic logon reduces system security by bypassing user authentication during startup. Do not enable this feature on devices installed in untrusted or publicly accessible locations where unauthorized users could gain physical access to the device.

7.1 First-Time Behavior

Once QuickPanel+2 is configured and ready to use, the **QuickPanel+2 Logon** tool will run automatically in full-screen mode as shown below:

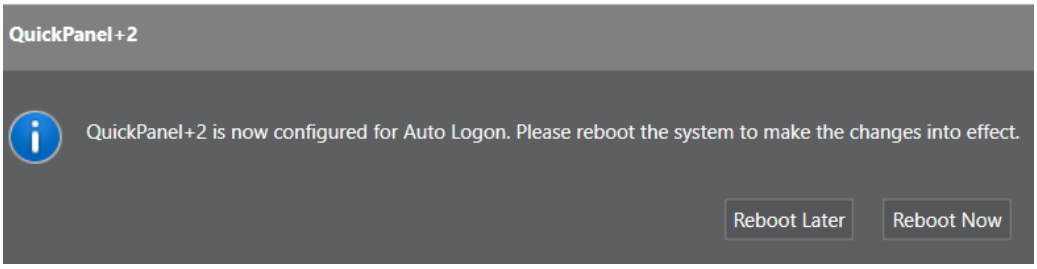
Figure 6: QuickPanel+2 Auto Logon Tool



The following steps need to be performed to enable the Auto Logon process for the current user:

1. Select the **Enable** option to log in to QuickPanel+2 device without credentials on every reboot.
2. Enter the Username, Password, and Domain (if applicable) and click the **Apply** button. If the entered credentials are valid, then Auto Logon will be enabled for the specific user. The user will be prompted to either Reboot Now or defer to later, as shown below.

Figure 7: QuickPanel+2 Reboot Prompt Message

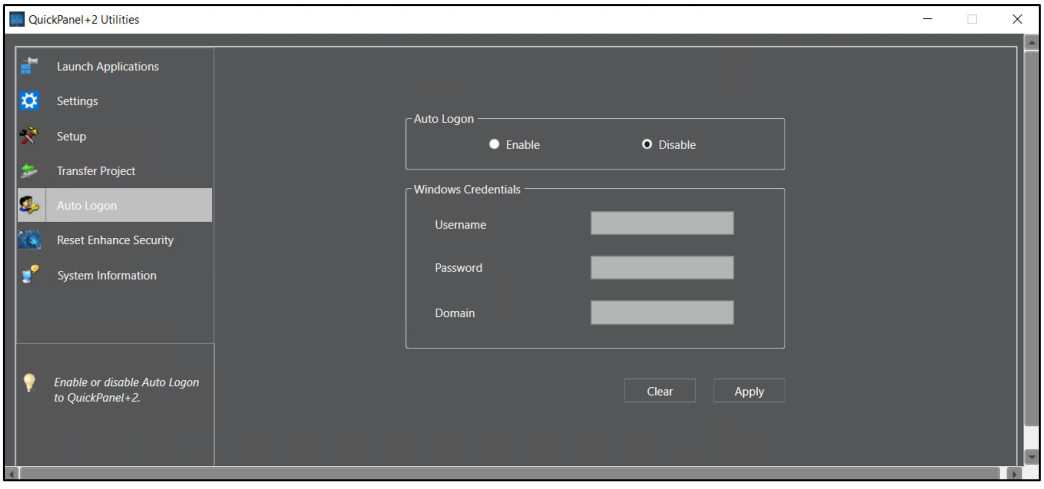


7.2 Second-Time Behavior

The user needs to explicitly run the **QuickPanel+2 Auto Logon Tool** from then on if Auto Logon needs to be enabled or disabled.

1. Select the **Disable** option as shown below to disable the Auto Logon if Auto Logon is already enabled.
2. Enter Username, Password, and Domain (if available), and click on the **Apply** button as shown below. If the entered credentials are valid, then Auto Logon will be disabled for the specific user. The user will be prompted to either Reboot Now or defer to later.
3. If the entered credentials are not valid, an appropriate failure message will be shown to the user.

Figure 8: QuickPanel+2 Auto Logon



Note: Follow the **Second Time Behavior** steps with the option to enable the Auto Logon.

Section 8: Optional Security Features

This functionality is optional for Emerson customers.

QuickPanel+2 includes Secomea SiteManager and provides compatibility with the external Secomea Products.

8.1 Secomea Products

Secomea provides secure remote access solutions for industrial equipment and automation systems. Its technology enables authorized personnel to remotely monitor, diagnose, maintain, and support industrial devices over the Internet while maintaining strict access control and cybersecurity. Secomea solutions are widely used in manufacturing, process automation, utilities, and machine-building applications.

The Emerson QuickPanel+2 includes Secomea SiteManager Embedded, a software-based secure remote access gateway that is pre-installed on the device. SiteManager Embedded enables the QuickPanel+2 to become part of a secure remote access infrastructure, allowing authorized engineers and service personnel to securely access the HMI and connected industrial equipment from a remote location for maintenance, troubleshooting, and support.

The Secomea secure remote access solution consists of several software components that work together to provide secure access to industrial equipment and automation systems:

SiteManager Embedded: SiteManager Embedded is installed on the QuickPanel+2 and acts as the secure remote access gateway. When enabled, it establishes an encrypted outbound connection to the Secomea GateManager server and provides controlled remote access to the QuickPanel+2 and, when permitted, other devices on the same industrial network.

GateManager: GateManager is the central management and tunnel proxy server of the Secomea solution. It authenticates users, manages access permissions, and brokers secure connections between authorized users and remote equipment. Rather than allowing direct inbound connections to industrial devices, GateManager acts as a secure intermediary, routing encrypted communication between LinkManager clients and SiteManager Embedded devices. GateManager maintains secure connections with registered SiteManager devices and provides centralized user management, access control, auditing, and connection logging. GateManager can be deployed as a cloud-hosted service or installed on-premises.

LinkManager: LinkManager is the client application used by authorized users, such as service engineers and system administrators. After authentication, LinkManager provides secure access to devices connected through SiteManager Embedded, allowing remote monitoring, troubleshooting, maintenance, and support activities.

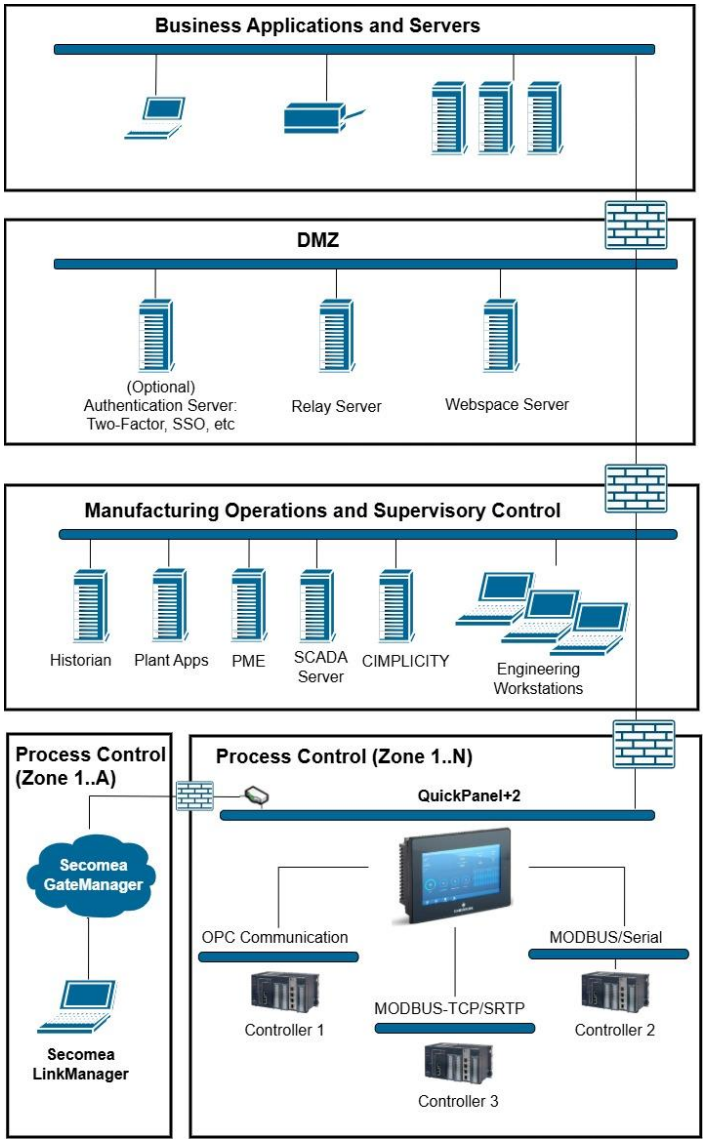
Note: SiteManager Embedded and its associated software remain inactive until they are configured and licensed. Licenses and subscriptions are available through Secomea and its

authorized distributors. To request a license or obtain additional information, visit secomea.com/license

Additionally, other devices such as PLCs and PCs (in addition to the QuickPanel+2) can be added as new agents on the Secomea network to be part of Secured Communication using the Add Agents feature in the SiteManager GUI. This can be achieved using the extended license feature from Secomea.

Note: Secomea products installed within the application, as outlined in the accompanying diagram, do not intrinsically provide the same level of security as firewalls. It is essential for network architects to ensure that the required security levels for the application are met in the overall implementation.

Figure 9: Secomea Products used with QuickPanel+2 in Application



Section 9: Other Considerations

9.1 Patch Management

A strategy for applying security fixes, including patches, firmware updates, and configuration changes, should be included in a facility's security plan. Applying these updates will often require that an affected QuickPanel+2 controller be temporarily taken out of service.

Finally, some installations require extensive qualification to be performed before changes are deployed to the production environment. While this requirement is independent of security, ensuring the ability to promptly apply security fixes while minimizing downtime may drive the need for additional infrastructure to help with this qualification.

QuickPanel+2 is integrated with Windows 10 IoT Enterprise 2021 LTSC. To receive the latest security protections, customers must apply the newer cumulative updates directly on to their devices through Windows Update.

9.2 Real-time Communication

When designing the network architecture, it is important to understand what impact the network protection devices (such as firewalls) will have on the real-time characteristics of the communications traffic that must pass through them. In particular, the Ethernet Global Data protocol is generally expected to operate with small, known, worst-case bounds on their communications latency and jitter. As a result, network architectures that require real-time communications to pass through such devices may limit the applications that can be successfully deployed.

9.3 Gratuitous ARP

The purpose of an ARP (Address Resolution Protocol) request is to associate an IP address with a physical address (MAC). A host can obtain a physical address by broadcasting an ARP request on the TCP/IP network. This is a required capability when using IPv4 communication on a QuickPanel+2 device.

The ARP protocol also allows hosts to broadcast unsolicited ARP replies, which is known as Gratuitous ARP (GARP). There is generally no need for Gratuitous ARP, and there are well-known attacks (such as man-in-the-middle) that rely on it. An Ethernet switch that blocks gratuitous ARP packets can help mitigate ARP-based attacks.

9.4 Additional Guidance

9.4.1 Protocol-specific Guidance

Protocol standards bodies may publish guidance on how to securely deploy and use their protocols. Such documentation, when available, should be considered in addition to this document.

9.4.2 Government Agencies and Standards Organizations

Government agencies and international standards organizations may guide on creating and maintaining a robust security program, including how to securely deploy and use Control Systems. For example, the U.S. Department of Homeland Security has published guidance on Secure Architecture Design and Recommended Practices for cybersecurity with Control Systems. Such documentation, when appropriate, should be considered in addition to this document. Similarly, the International Society of Automation publishes the ISA-99 and IEC-62443 specifications to guide the establishment and operation of a cybersecurity program, including recommended technologies for industrial automation and control systems.

Contact Information and Support Guide

Questions? We are here to help.

Before starting a case or making a call, try searching our Knowledge Base on the Customer Center website—it might have the answer you need right away.

If you have a question, try the following steps:

Search our Knowledge Base	Open a Support Ticket	Register for a Customer Account
pacsystems.co/knowledge	pacsystems.co/support	pacsystems.co/signup

Other Helpful Links

Customer Center Home Page	Commercial Website	Contact Information
pacsystems.co/customercenter	pacsystems.co/commercial	pacsystems.co/contactus

Emerson reserves the right to modify or improve the designs or specifications of the products mentioned in this manual at any time without notice. Emerson does not assume responsibility for the selection, use, or maintenance of any product. Responsibility for proper selection, use, and maintenance of any Emerson product remains solely with the purchaser.