QuickPanel^{+TM}

OPERATOR INTERFACE
SECURE DEPLOYMENT GUIDE

EMERSON™

Contents

Caution Notes as Used in this Publication

Caution

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

Notes: 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 to be met 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 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 particular purpose.

Chapter 1: Introduction

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

QuickPanel$^+$ Operator Interface Products

Product	Catalog Number	Product Description
QuickPanel$^+$ 7"	IC755CBW07CDA-BB	QuickPanel$^+$ 7" Widescreen Blank Bezel
	IC755CSW07CDA-BF	QuickPanel$^+$ 7" Widescreen Emerson Bezel
	IC755CSW07CDACA-BF	QuickPanel$^+$ 7" Widescreen Emerson Bezel Conformal Coat
QuickPanel$^+$ 10"	IC755CBS10CDA-AB	QuickPanel$^+$ 10" Blank Bezel
	IC755CSS10CDA-AB	QuickPanel$^+$ 10” Emerson Bezel
	IC755CSS10CDACA-AB	QuickPanel$^+$ 10” Emerson Bezel Conformal Coat
QuickPanel$^+$ 12"	IC755CBS12CDB-AB	QuickPanel$^+$ 12” Blank Bezel Ethernetx2
	IC755CSS12CDB-AB	QuickPanel$^+$ 12” Emerson Bezel Ethernetx2
	IC755CSS12CDBCA-AB	QuickPanel$^+$ 12” Emerson Bezel Ethernetx2 Conformal Coat
QuickPanel$^+$ 15"	IC755CBS15CDA-AB	QuickPanel$^+$ 15” Blank Bezel
	IC755CSS15CDA-AB	QuickPanel$^+$ 15” Emerson Bezel
	IC755CSS15CDACA-AB	QuickPanel$^+$ 15” Emerson Bezel Emerson Conformal Coat
QuickPanel$^+$ 6"	IC755CSS06RDA-AA	QuickPanel$^+$ 6” Resistive Emerson Bezel
	IC755CBS06RDA-AA	QuickPanel$^+$ 6” Resistive Blank Bezel

Chapter 2: Security and Secure Deployment

This chapter describes the fundamentals of security and secure deployment.

2.1 What is Security?

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

- Confidentiality: Ensure only the people you want to see 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.

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 Secomea Security Elements

Refer to www.secomea.com for more information.

Effective March 2015, Secomea SiteManager software is installed on QuickPanel+ products as a convenience to Emerson customers, but is not itself a Emerson product. SiteManager™ and its related GateManager™, LinkManager™ and LinkManager Mobile products are licensed, sold, and supported by Secomea and Secomea's licensed distributors. Refer to the chapter Optional Security Features for further details, such as QuickPanel+ product identification.

2.5 General Recommendations

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

- Deploy and configure firewalls to limit the exposure of control system networks to other networks, including internal business networks and the Internet. If a control system requires external connectivity, care must be taken to control, limit and monitor all access, using, for example, virtual private networks (VPN) or Demilitarized Zone (DMZ) architectures.
- Harden system configurations by enabling/using the available security features, and by disabling unnecessary ports, services, functionality, and network file shares.
- Apply all of the latest Emerson Intelligent Platforms product security updates, SIMs, and other recommendations.
- Apply all 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.

2.6 Checklist

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

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. (Refer to the chapter Network Architecture & Secure Deployment.)
5. Configure firewalls and other network security devices
6. Enable and/or configure the appropriate security features on each QuickPanel+ module.
7. For each QuickPanel+ module, change every supported password to something other than its default value.
8. For each QuickPanel+ 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 Historian Communication and Web Services Access.
9. Harden the configuration of each QuickPanel+ module, disabling unneeded features, protocols and ports.
10. Test / qualify the system.
11. 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. For more information about security programs in general, refer to the section Additional Guidance.*

Chapter 3: Communication Protocols

Refer to the section Communication Protocols.

This chapter describes how the supported application protocols for Ethernet and serial ports are used with QuickPanel+. 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 aren't 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 doesn't 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 Supported Protocols

3.1.1 Ethernet Protocols

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

Protocol		QuickPanel$^+$
Link	ARP	✓
	LLDP	✓
Internet	IPv4	✓
	IPv6	✓
	ICMP	✓
	IGMP	✓
Trans	TCP	✓
	UDP	✓
	BOOTP Client	—
	DCE/RPC Client	✓
	DNS Client	✓
	Ethernet Global Data	✓
	FTP server	✓
	HTTP server	✓
	Modbus TCP master	✓
	Modbus TCP slave	✓

Protocol		**QuickPanel$^+$**
Application Layer	PROFINET DCP client	—
	PROFINET DCP server	—
	PROFINET IO	—
	MRP	—
	SNMP v1 & v2c server	✓
	SNTP client	✓
	SRTP client	✓
	SRTP server	✓
	Telnet server	✓
—	LPR /LPD & SMB	✓
—	PCL5	✓

3.1.2 Serial Protocols (RS–232, RS–485)

QuickPanel+ 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.

Protocol	**QuickPanel$^+$**
Application-specific	✓
ASCII Slave	✓
Modbus RTU Slave	✓
SNP Slave	✓

Note: *The 7” QuickPanel$^+$ display unit has a single COM port that supports RS–232 only. Larger models have a second COM port which supports RS–232, RS–422, and RS–485.*

3.1.3 USB Protocols

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

- 2x USB 2.0 (Type-A)
- 1x USB 2.0 (Mini Type-B)

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

Protocol	**QuickPanel$^+$**
Application-specific†	✓
USB†	✓
USB To Serial‡	✓
USB To Ethernet‡	✓
USB to Wi-Fi‡	✓

Protocol	QuickPanel+
† USB printer driver provides support for printing over a USB connection ‡ Recommended Adapters: USB Wi-Fi adapters based on the Ralink chipset - RT2070, 2870, 3070, 3071, or 3072 USB Serial adapters based on FTDI chipset USB Ethernet adapters based on ASIX AX88179 or AX88772B	

3.2 Server

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

Functionality		Required Application Protocols	Example Clients
Ethernet	View OPC Server	OPC	OPC Client
	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
	Web Proprietary Server (TRAPI Server)	HTTP	Web browser on PC
	File Transfer (FTP server)	FTP	ftp.exe on PC
	Web Server	HTTP	—
	Logic OPC Server	OPC	OPC Client
	Print Spooler	LPR	Print
	TRAP and SNMP SET Requests	SNMP	SNMP Manager/NMS
Serial	View OPC Server	OPC (SNP/SNPX)	OPC Client (Runtime)
	QuickPanel+ (View)	Modbus	QuickPanel+/QP
	QuickPanel+ (Control)	Modbus/ASCII	QuickPanel+/QP

3.3 Client

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

Functionality		Required Application Protocols	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

Functionality		Required Application Protocols	Example Servers
	PAC Machine Edition Historian Collector	Collector Shell/ihapi55	Historian Server
	QuickPanel$^+$ target	View Networking	PC
	Printing on QuickPanel$^+$	LPR / TCP IP	Print Server on PC
	SNMP GET/GETNEXT	SNMP	SNMP Manager/NMS

3.4 Ethernet Firewall Configuration

The firewall is disabled on the QuickPanel$^+$ Operator Interface.

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

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

3.4.1 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$^+$ Operator Interface.

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

3.4.2 Application Layer Protocols

The QuickPanel+ is capable of acting 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
DCE/RPC	—	34964 on server >1023 on client
DNS	53	53 on server >1023 on client
View Runtime Server	12397	—
Control Runtime Server	12396	—
TRAPI Server	57176	—
View Networking	22739, 22740	—
Control – Warm Standby	12399	—
Ethernet Global Data	—	18246
FTP	21	—
HTTP	80, 8080	—
Modbus TCP	502	—
SNTP	—	123
SRTP	18245	—
SNMP	161	161, 162

3.5 Simple Network Management Protocol (SNMP) Agent

The SNMP is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 that is used for exchanging management information between network devices. It is a part of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite.

The QuickPanel+ Operator Interface is enabled as an SNMP Agent with the capability to communicate with SNMP Managers (software tools run independently and are not part of QuickPanel+ Operator Interface) for the following purposes:

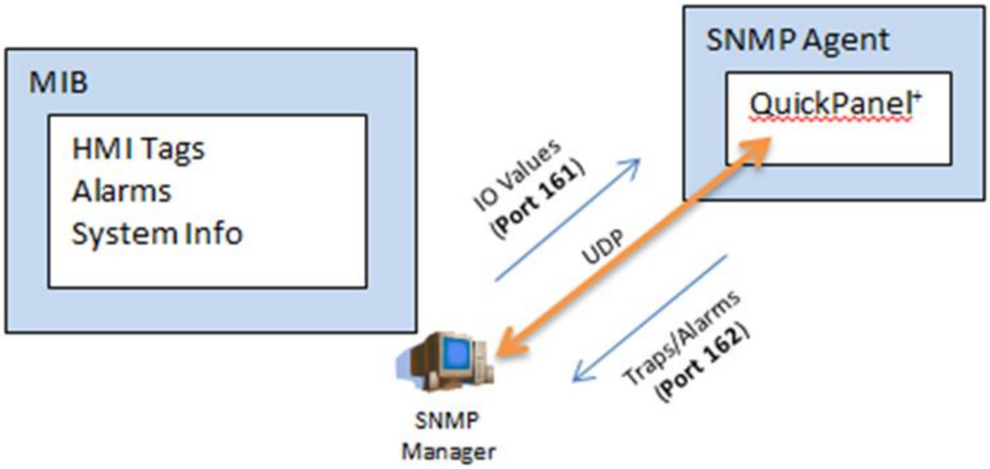
- Send notification of HMI Alarms as Traps
- Provide live values for SNMP Manager’s GET/GETNEXT Query calls for HMI Tags

Note: *Refer to the section Enable or Disable SNMP Agent for the procedure to enable and disable the SNMP on the QuickPanel+ device.*

In typical uses of SNMP, one or more administrative computers called SNMP Managers monitor or manage a group of networks connected QuickPanel+ devices on a network. Each managed QuickPanel+ device constantly runs a software component called a SNMP Agent that reports information through the SNMP to the SNMP Manager.

The following diagram illustrates the QuickPanel⁺ operating as the SNMP Agent to communicate with a SNMP Manager for Traps notification and responding to Query HMI Tag values.

Figure 1: QuickPanel⁺ as SNMP Agent



SNMP Agents display management data on the managed devices as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible through the SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable) are described by Management Information Bases (MIBs) (for example, QuickPanelMIB.mib for the QuickPanel⁺ device).

The MIB is a collection of information for managing network elements. It is a plain text file, self-explanatory, and prepared based on the Structure of Management Information (SMI), an adapted subset of Abstract Syntax Notation One (ASN.1) standard and notation.

NOTICE

The QuickPanel⁺ MIB is follows the SNMP V2c and is also compatible with SNMP V1 based on the strictness of the MIB compilers supported by SNMP Managers.

A SNMP-managed network consists of three key components (as illustrated in the figure QuickPanel+ as SNMP Agent):

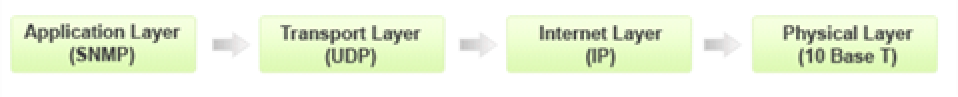
- QuickPanel+ device
- SNMP Agent (software running on QuickPanel+ device)
- Network Management Station (NMS) (software running on SNMP manager)

The QuickPanel+ managed device is a network node that implements an SNMP interface that currently allows unidirectional (Read-only) access to node-specific information.

3.5.1 Typical SNMP Communication

As part of the TCP/ IP protocol suite, SNMP messages are wrapped as User Datagram Protocol (UDP) and internally wrapped and transmitted in the Internet Protocol. The following diagram illustrates the four–layer model developed by the Department of Defense (DoD)

Figure 2: SNMP Communication Dataflow



3.5.2 SNMP Versions

Although SNMP has gone through significant upgrades since its inception and SNMP v1 and v2c are the most frequently implemented versions. Both Community-based security versions are supported by the Windows Embedded Compact 7 Operating System that runs on the QuickPanel+ device. The QuickPanel+ device uses Public as the community for both of these versions.

Note:

- *SNMPv1 is the first version of the protocol, which is defined in RFCs 1155 and 1157.*
- *SNMPv2c is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure (community-based and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, RFC 1906, RFC 2578.*
- *SNMPv2c supports a plain text community string, which makes the communication vulnerable to data sniffing. It is recommended that this feature be disabled when it is not being used. For additional security, SNMP communication can be embedded within the secured communication channel provided by Secomea. For additional information on Secomea, refer to the section SNMP within Secomea (Optional) and the QuickPanel+ Operator Interface User Manual, the chapter Secomea Security (Optional).*

3.5.3 SNMP within Secomea (Optional)

For additional security, SNMP communication can be enabled within the Secomea infrastructure by adding UDP ports 161, 162 to the QuickPanel+ agent properties using the Secomea SiteManager GUI (embedded on the QuickPanel+) device.

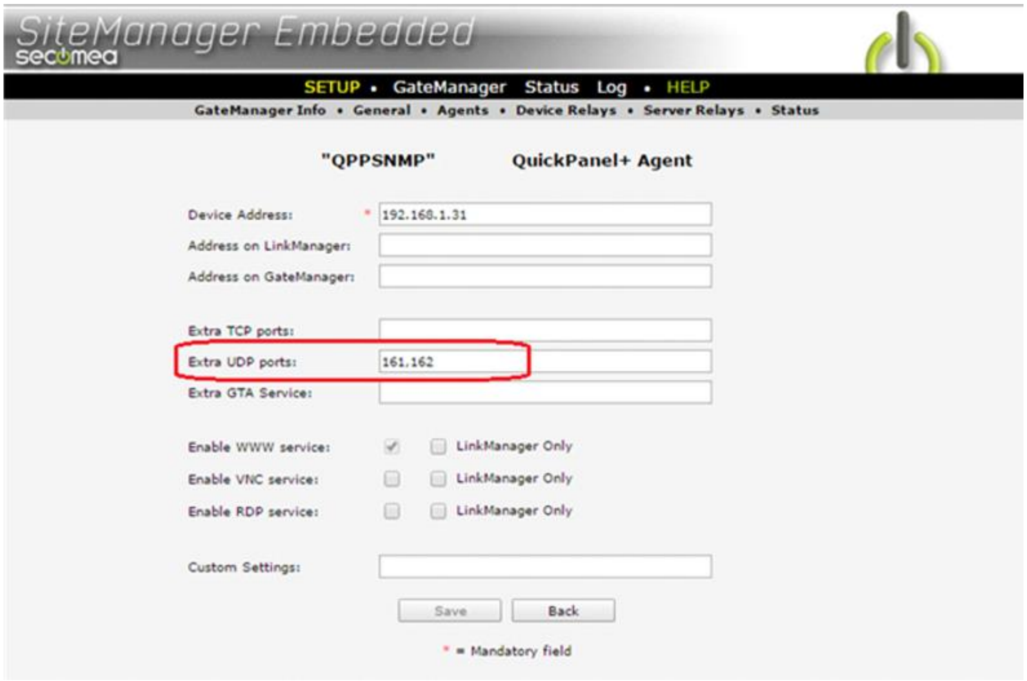
Note: *For additional details, refer to the section Secomea Products. Further clarification for establishing SNMP communication within Secomea is available at www.secomea.com.*

To add UDP ports to the QuickPanel$^+$ SNMP agent: from the **SiteManager**, select **Properties** on the QuickPanel$^+$ agent and enter **161,162** in the **Extra UDP ports** field.

⚠CAUTION

Make sure that both the QuickPanel+ device and the computer running with LinkManager, GateManager, and SNMP Managers are on same domain.

Figure 3: Secomea SiteManager Window with 161, 162 UDP Ports Added


SiteManager Embedded
secomea
SETUP • GateManager Status Log • HELP
GateManager Info • General • Agents • Device Relays • Server Relays • Status
Save
Back

"QPPSNMP" QuickPanel+ Agent

Device Address: * 192.168.1.31
Address on LinkManager:
Address on GateManager:

Extra TCP ports:
Extra UDP ports: 161,162
Extra GTA Service:

Enable WWW service: ☑ □ LinkManager Only
Enable VNC service: □ □ LinkManager Only
Enable RDP service: □ □ LinkManager Only

Custom Settings:

* = Mandatory field

Chapter 4: Security Capabilities

4.1 External Storage – SD Card

The QuickPanel+ Operator Interface provides an SD/SDHC card slot for external storage. The View Runtime application running on this device can use this external storage for logging real time data. The SD/SDHC card can be used as a buffer media to transfer the real-time data to a Proficy Historian Server. When 'alarms 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+ 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 a 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 backup the Runtime Project into the SD card by using one of the following methods:

- Download the QuickPanel+ 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 PC.

  Or

- Install SD card media into the QuickPanel+ 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

Firmware updates are not supported over Ethernet or Serial interfaces. The current mechanism is to copy the required files into the media (SD Card/USB), physically insert the media into the QuickPanel+ Operator Interface and upgrade the firmware by running the QPPlusUpdate.exe tool. To further enhance security, this process involves the use of a DIP Switch† and requires that the user be physically present. Currently, Hardware Configuration, Boot Loader, and the OS are updated at the same time during the firmware upgrade process.

Note: *† The QuickPanel+ Update tool prompts the user to set DIP Switch 2 (SW2 Switch) Position 1 to ON. This requires removal of the QuickPanel+ back plate. After the firmware upgrade has been accepted, the user is also prompted to cycle power. For security reasons, be sure to change DIP Switch 2 (SW2 Switch) Position 1 to OFF before replacing the back plate.*

Note: *The firmware update will remove the application and change the IP Address of the QuickPanel+ Operator Interface.*

Note: *The firmware package contains encrypted .nbo files. Use the PreUpdate.exe tool to decrypt the .nbo files before using them for upgrade.*

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+
- Start/Stop the View Runtime (or PC Control)
- Going online with the QuickPanel+
- 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 Historian Collector Communication

The QuickPanel+ device acting as a collector can establish both secured and unsecured communication with the Proficy Historian Server. A secured connection with the Historian server is based on the Windows Domain Controller, Kerberos. To establish the secured connection, the user must log into the domain as an owner on QuickPanel+

Security is enabled/disabled at the Historian Server. Without Security enabled at the Historian Server, the QuickPanel+ acting as a collector can still connect to the server in an unsecured fashion.

Setting a unique device name for each QuickPanel+ is particularly important when the QuickPanel+ is acting as a Historian Collector and archiving data to a Historian Server. The Historian Server recognizes/identifies its collector by device name. If multiple QuickPanel+ have the same default device name, usually Compact or Compact7, the Archiver process will only be able to establish communication with one QuickPanel+ and thus will not work properly. The device name setting for the QuickPanel+ can also affect other customer use cases.

Chapter 5: Configuration Hardening

Note: *For additional information, refer to the following locations:*

Windows Embedded Compact 7 contains various device drivers

Local Authentication Sub System (LASS) – Local Authentication Plug-in (LAP) support available on QuickPanel⁺.

5.1 Server Default States

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

- FTP server
- HTTP server
- SNTP client

5.2 Enhanced Security

PAC Machine Edition is the configuration tool for the QuickPanel⁺ Operator Interface. If the Enhanced Security feature is enabled on the PAC Machine Edition Configurator (editor) connected to the QuickPanel⁺, user password entry and authentication is required when an attempt is made to change the configuration of the QuickPanel⁺ 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
- Resetting Runtime (for Windows PC Control targets only)
- Updating the security settings

Enhanced Security is enabled by default on the PAC Machine Edition Configurator and it reports errors that occur during validation of the QuickPanel+ configuration. Configuring a QuickPanel+ using a PAC Machine Edition Configurator with Enhanced Security enabled causes Enhanced Security to be enabled on the QuickPanel+ Operator Interface. The Enhanced Security setting also determines the QuickPanel+ VNC Server’s authentication setting for VNC Viewers.

Note:

- *If the user forgets the password, run the Reset Enhanced Security tool that is available through Programs and System menu, or contact the technical support for any further issues. Refer to the section QuickPanel+ OS Utilities Settings Tool for further details on the Reset Enhanced Security tool.*
- *The PAC Machine Edition Remote Target Viewer tool (available on PC) will not be able to connect to a secured QuickPanel+ device.*

5.3 QuickPanel+ OS Utilities Settings Tool

DIP switches are set in the OFF position (default) in the factory.

DIP switches are set in the OFF position (default) in the factory.

DIP Switch 1 (SW2 Switch) enables firmware upgrade. Firmware upgrade is allowed only after turning this switch in the ON position. It is highly recommended to turn the switch position to OFF after firmware upgrade is completed as a security measurement.

DIP Switch 2 (SW2 Switch) controls Force Startup. Turning this switch to the ON position forces the startup applications to run when the operating system is started.

The DIP Switch feature is designed as a security measurement. However, security requirements can also be met using the gesture-based feature.

Prior to the listed firmware builds, these operations were only supported using the DIP

Switch settings.

Some operators find it difficult to use the DIP Switch settings to perform these functions (such as removing the back plate of the device and adjusting the positions of DIP Switch for each operation). As an alternative to using the DIP Switch settings, the QuickPanel+ OS Utilities Settings tool contains finger gesture-based utilities to perform the same operations. This functionality is available with the firmware builds listed in the following table

QuickPanel+ OS Utilities Settings Tool Support

QuickPanel+ Product	Firmware Build
IC755CxS06RDx (6" Display)	01 (initial release)
IC755CxW07CDx (7” Display)	21
IC755CxS10CDx (10” Display)	12
IC755CxS12CDx (12” Display)	
IC755CxS15CDx (15” Display)	

The tool operation buttons for each utility only respond to a double-tap finger gesture. It will not accept any keyboard or mouse clicks, finger simulator-based inputs, or click inputs from any remote touch-based device. The user can access the tool from the **Start** menu by selecting **Programs, System**, and **QuickPanel+ OS Utilities Settings** on the device. The tool can be used to perform the following operations using the double-tap feature, without adjusting the DIP Switch positions:

- Firmware Upgrade
- Bypass Startup Programs
- Reset Enhanced Security
- Enable or Disable SNMP Agent

⚠CAUTION

For security, only permit these operations when the operator is physically located near the QuickPanel+ and require that users perform a physical action on the device.

5.3.1 Firmware Upgrade

This utility operates similar to the QuickPanel+ Update Tool, which comes with the OS image upgrade binaries. The operator can continue to use the QuickPanel+ Update Tool to use the DIP Switch feature.

The Firmware Upgrade utility setting enables operators to upgrade the firmware. Firmware updates are not supported over Ethernet or Serial interfaces. Insert the media (SD Card) containing the required files for firmware upgrade and perform the following procedure.

Note: *Make sure the copy of required binaries to the SD card is not within a folder.*

Note: *The firmware package contains encrypted .nbo files. Use the PreUpdate.exe tool to decrypt the .nbo files before using them for upgrade.*

After a firmware upgrade, which refreshes the device fresh, the user must download the project again and install their own tools (including third party tools) on the device.

Note: *It is recommended that the user back up any important data prior to firmware upgrade so that they can replace the data after firmware upgrade if necessary.*

⚠CAUTION

If the current firmware build version on the QuickPanel+ is any of the following, refer to the section Firmware Upgrade for Specific Build Version:

- Build 3 or below for IC755CxS06RDx

  (6” Display)
- Build 23 or below for IC755CxW07CDx

  (7” Display)
- Build 14 or below for IC755CxS10CDx

  (10" Display), IC755CxS12CDx

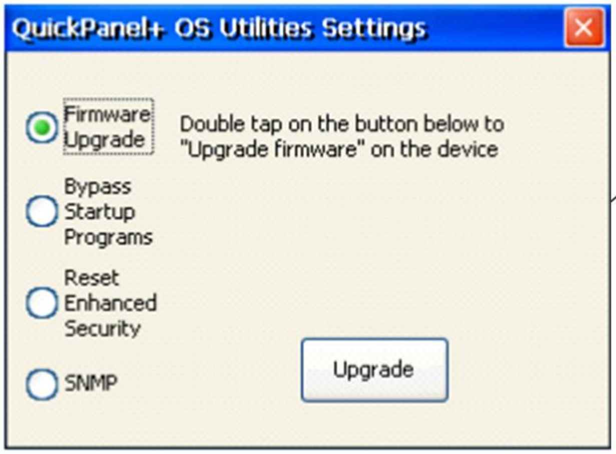
  (12” Display), and IC755CxS15CDx

  (15” Display)

To perform a firmware upgrade

1. From the **Start** menu, select **Programs**, **System**, and **QuickPanel+ OS Utilities Settings Tool** to display the QuickPanel+ OS Utilities Settings window.
2. Upgrade the firmware.

Figure 4:



QuickPanel+ OS Utilities Settings

● Firmware Upgrade
○ Bypass Startup Programs
○ Reset Enhanced Security
○ SNMP

Double tap on the button below to "Upgrade firmware" on the device

From the QuickPanel$^+$ OS Utilities Settings window, select **Firmware Upgrade**, then double-tap **Upgrade**.

3. The operator interface guides the operator through the firmware upgrade process. After successful upgrade, restart the device.
4. Download the project and install any site-specific tools, including third party tools, on the device.

5.3.2 Firmware Upgrade for Specific Build Version

The following procedure is applicable to the following QuickPanel+ display units:

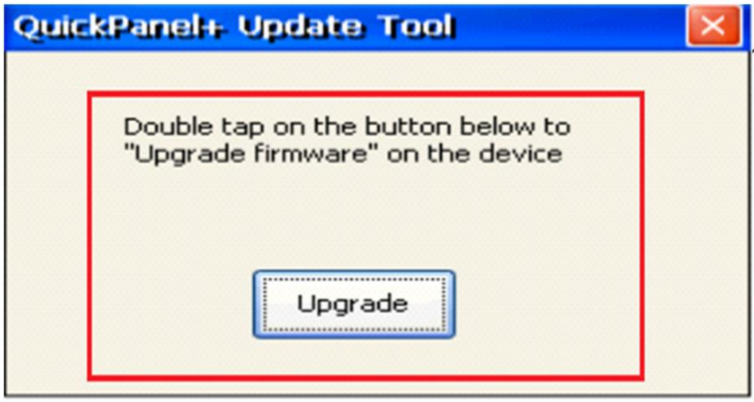
- QuickPanel+ IC755CxS06RDx (6” Display) with build 3 or below
- QuickPanel+ IC755CxW07CDx (7” Display) with build 23 or below
- QuickPanel+ IC755CxS10CDx (10" Display), IC755CxS12CDx (12” Display), and IC755CxS15CDx (15” Display) with build 14 or below

To perform a firmware upgrade for a specific firmware, build version

1. Put the files in the firmware package on the SD Card.
2. Double-click QPPlusUpdate.exe and run the program.
3. Perform the firmware upgrade.

Figure 5:

From the QuickPanel$^+$ Update Tool dialog box, click **Upgrade**.



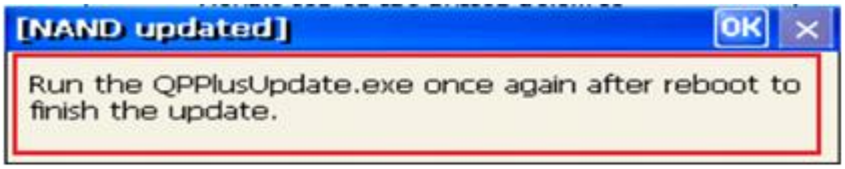
QuickPanel+ Update Tool

Double tap on the button below to "Upgrade firmware" on the device

⚠CAUTION

For a QuickPanel+ 7" inch Display unit, the following message displays during the process of firmware upgrade. You must re-run the QPPlusUpdate.exe program after reboot, which means you will run the QPPlusUpdate.exe program a total of two times to complete the upgrade process.

Figure 6: QuickPanel+ 7" inch Display Reboot and Run Program Message



Run the QPPlusUpdate.exe once again after reboot to finish the update.

5.3.3 Bypass Startup Programs

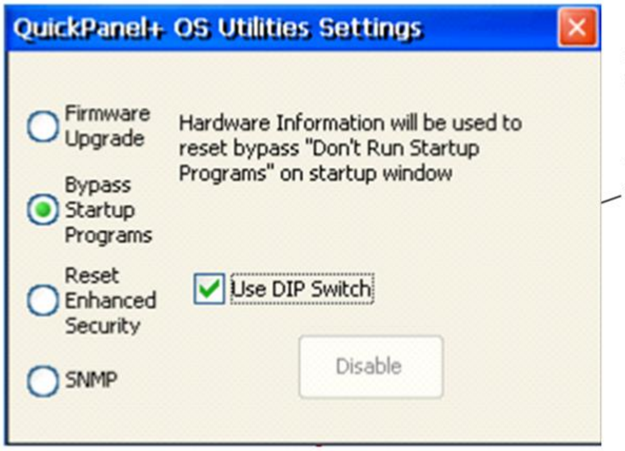
This utility functions the same as disabling or enabling the Don't startup Program functionality using DIP Switch Position 2.

The Bypass Startup Programs utility enables the operator to choose the gesture-based feature or DIP Switch (Use DIP Switch) feature to perform the Force Startup operation.

To bypass startup programs and force startup

1. From the **Start** menu, select **Programs**, **System**, and **QuickPanel+ OS Utilities Settings Tool** to display the QuickPanel+ OS Utilities Settings window.
2. Enable or disable the bypass startup programs feature.

Figure 7:



○ Firmware Upgrade
● Bypass Startup Programs
○ Reset Enhanced Security
○ SNMP

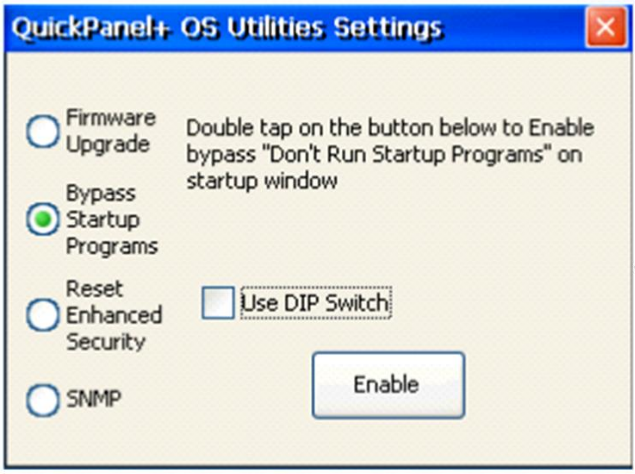
Hardware Information will be used to reset bypass "Don't Run Startup Programs" on startup window

☑ Use DIP Switch

From the QuickPanel + OS Utilities Settings window, select **Bypass Startup Programs**.

To use the DIP Switch feature to perform this operation, select **Use DIP Switch**.

Figure 8:



QuickPanel+ OS Utilities Settings

○ Firmware Upgrade

● Bypass Startup Programs

○ Reset Enhanced Security

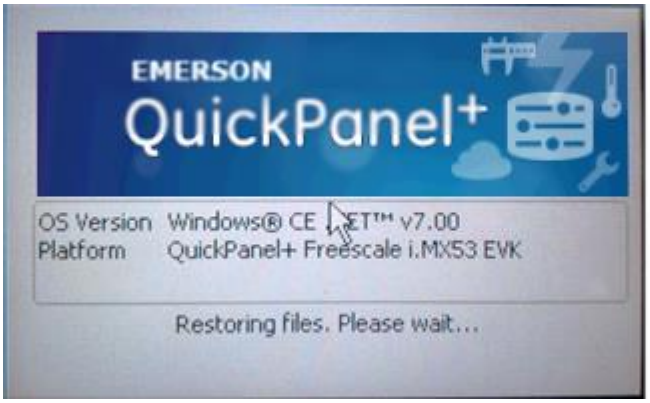
○ SNMP

Double tap on the button below to Enable bypass "Don't Run Startup Programs" on startup window

□ Use DIP Switch

To use the double-tap feature to perform this operation , double -tap **Enable**.

Figure 9:

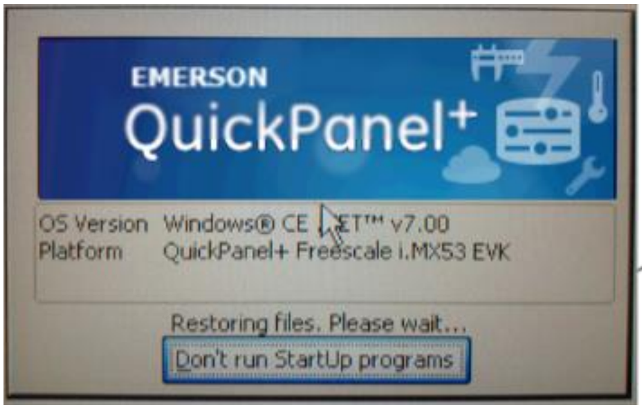


OS Version Windows® CE .NET™ v7.00
Platform QuickPanel+ Freescale i.MX53 EVK

Restoring files. Please wait...

If **Enable** is double-tapped, the startup window displays and all startup programs are enabled to run .

Figure 10:



OS Version Windows® CE .NET™ v7.00
Platform QuickPanel+ Freescale i.MX53 EVK

Restoring files. Please wait...

If **Disable** is double-tapped, the startup window displays . Click **Don't run Startup programs** to stop all startup programs from running .

If Use DIP Switch is selected, **Don't run StartUp Programs** displays on the startup window based on the position of DIP Switch 2.

5.3.4 Reset Enhanced Security

The QuickPanel+ Operator Interface 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+ device to perform certain operations, such as the download operation. Every operation to connect to the device requires a password.

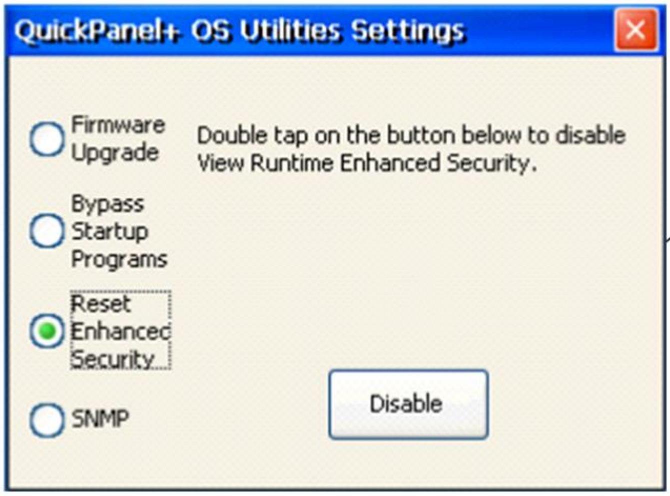
If you forget or do not know your password, the Reset Enhanced Security feature enables a QuickPanel+ configuration download on the device by permitting the user to disable the Enhanced Security feature using the double-tap feature.

Note: *Prior to support of the QuickPanel+ OS Utilities Settings Tool, if the user forgot or did not know their password, the only resolution was to contact Technical Support to reset the password or upgrade the firmware on the device.*

To disable Enhanced Security

1. From the **Start** menu, select **Programs**, **System**, and **QuickPanel+ OS Utilities Settings Tool** to display the QuickPanel+ OS Utilities Settings window.
2. Disable the Enhanced Security setting.

Figure 11:



○ Firmware Upgrade
○ Bypass Startup Programs
● Reset Enhanced Security
○ SNMP

Double tap on the button below to disable View Runtime Enhanced Security.

From the QuickPanel+ OS Utilities Settings window, select **Reset Enhanced Security**, then double-tap **Disable**.

5.3.5 Enable or Disable SNMP Agent

The QuickPanel+ Operator Interface can be enabled as a Simple Network Management Protocol (SNMP) Agent with the capability to communicate with SNMP Managers for notification of Traps and responding to Query HMI Tag values.

Since it is designed to run over a public network, SNMP communication is disabled by default on the QuickPanel+ device for security reasons. As a security measure, the SNMP feature requires a tactile input gesture to enable and disable SNMP communication.

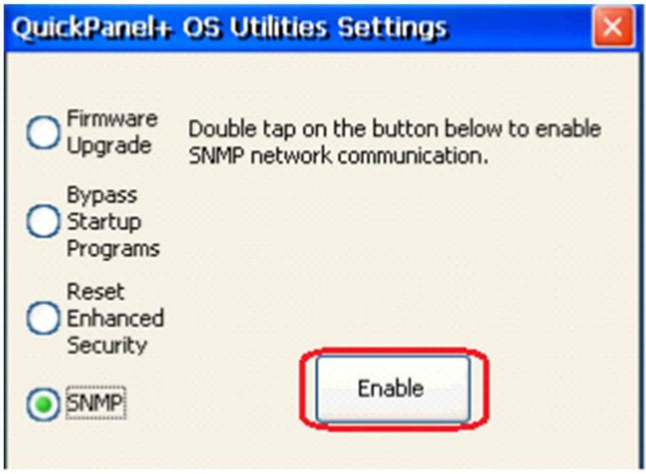
Note: *Refer to the section Simple Network Management Protocol (SNMP) Agent for further details.*

Note: *Enabling or disabling SNMP communication is a one-time user configuration.*

To enable the SNMP Agent

1. From the **Start** menu, select **Programs**, **System**, and **QuickPanel+ OS Utilities Settings Tool** to display the QuickPanel+ OS Utilities Settings window.
2. Enable SNMP communication.

Figure 12:



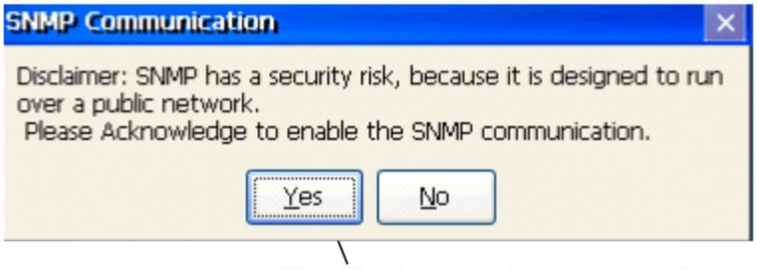
QuickPanel+ OS Utilities Settings

Double tap on the button below to enable SNMP network communication.

From the QuickPanel$^+$ OS Utilities Settings window, select **SNMP**.

Double-tap **Enable** to enable SNMP communication.

Figure 13:



SNMP Communication

Disclaimer: SNMP has a security risk, because it is designed to run over a public network.
Please Acknowledge to enable the SNMP communication.

Click **Yes** to acknowledge the security risk and enable SNMP communication.

⚠CAUTION

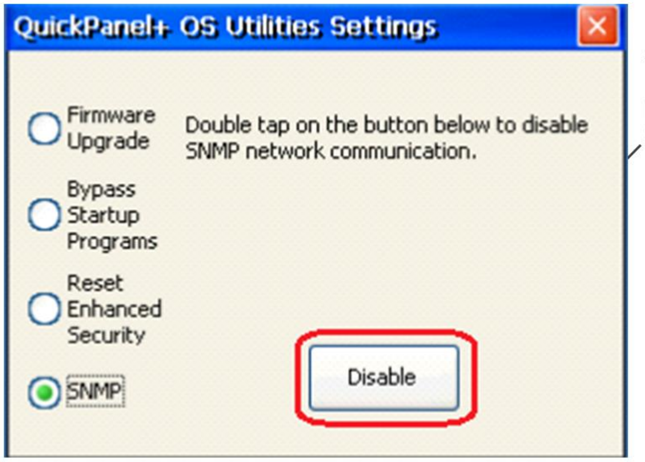
SNMP communication is enabled on the device only when the user acknowledges this security dialog box and clicks Yes.

Note: *Any failure or errors while enabling or disabling the SNMP service would be communicated to the user through a dialog box.*

To disable the SNMP Agent

1. From the **Start** menu, select **Programs**, **System**, and **QuickPanel+ OS Utilities Settings Tool** to display the QuickPanel+ OS Utilities Settings window.
2. Disable SNMP communication.

Figure 14:



Double tap on the button below to disable SNMP network communication.

From the QuickPanel+ OS Utilities Settings window, select **SNMP**.

Double-tap **Disable** to disable SNMP communication.

5.4 Ethernet Interface

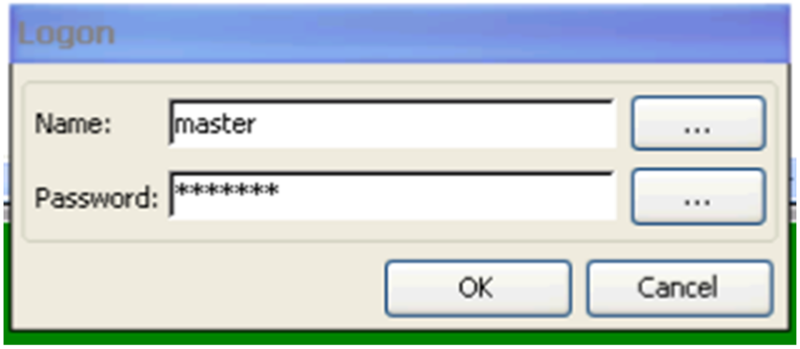
Interface	Availability
Bootp Client	Not available on the QuickPanel+
FTP Server	Can be enabled/disabled using the QuickPanel+ Setup Tool Services tab
IP Routing	Can be disabled by configuring the network port in Control Panel
DNS Client	Can be disabled by configuring the network port in Control Panel
SNTP Client	Can be enabled/disabled using the QuickPanel+ Setup Tool SNTP tab
Web Server	Can be enabled/disabled using the QuickPanel+ Setup Tool Services tab

5.5 User Management Facility

The User Management facility, provided by the View/Control applications on the QuickPanel+ Operator Interface, can be utilized to manage users with restricted privileges.

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

Figure 15:

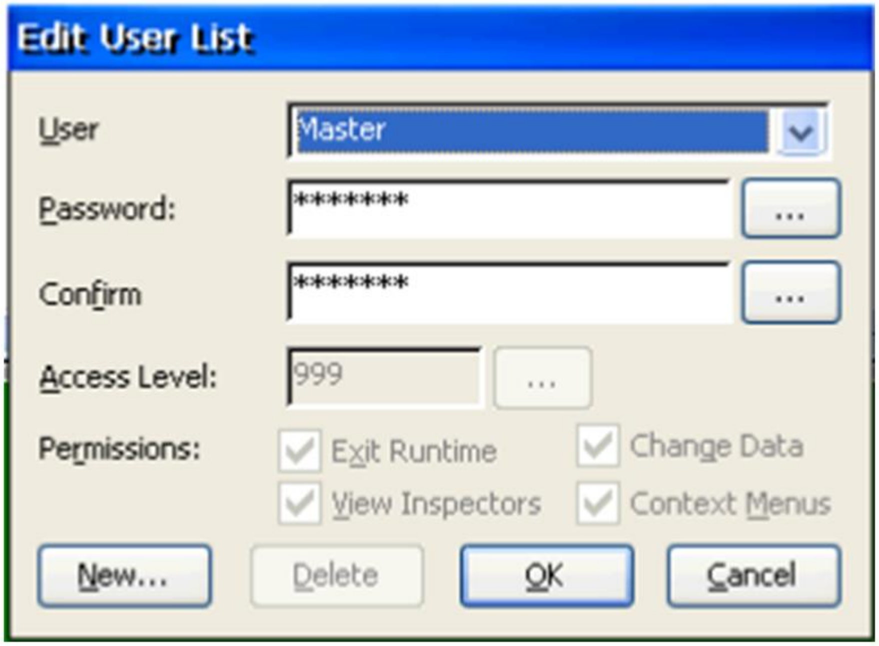


Name: master

Password: ********

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

Figure 16:



Edit User List

User Master

Password: *******

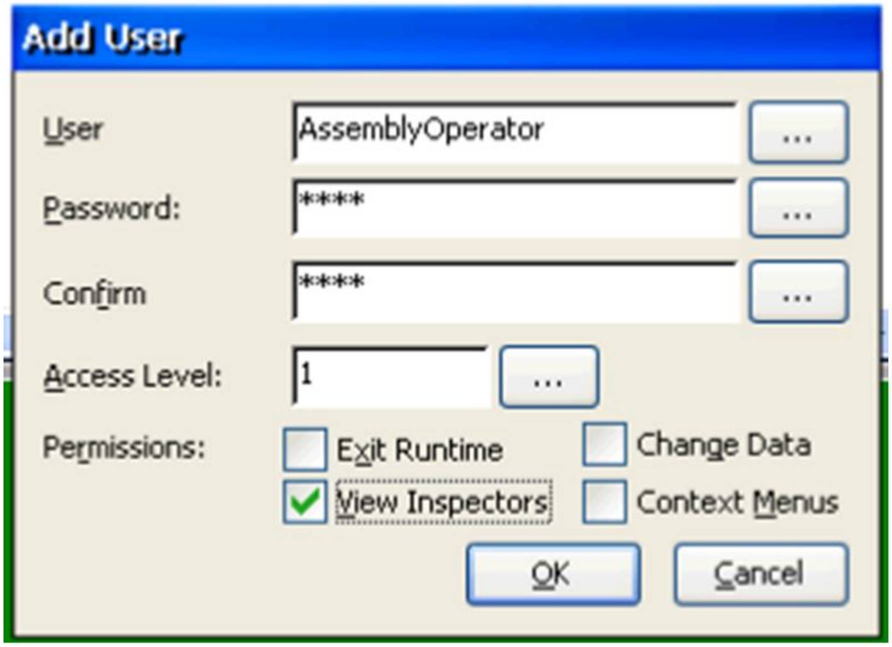
Confirm *******

Access Level: 999

Permissions: ☑ Exit Runtime ☑ Change Data ☑ View Inspectors ☑ Context Menus

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

Figure 17:



Add User

User AssemblyOperator

Password: ****

Confirm ****

Access Level: 1

Permissions: ☐ Exit Runtime ☐ Change Data ☑ View Inspectors ☐ Context Menus

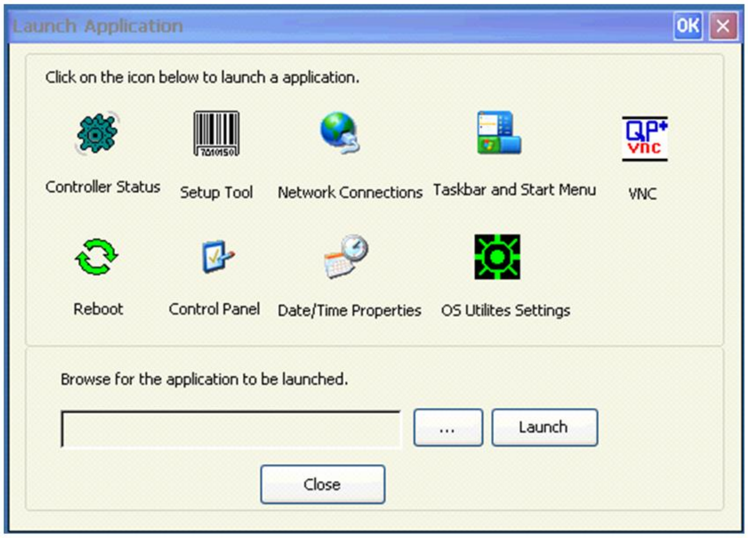
5.6 VNC Server

The VNC Server enables remote, visual connectivity to the QuickPanel+ Operator Interface from a laptop computer or a mobile device through the remote VNC Viewers. User authentication of the VNC Server in the QuickPanel+ is determined by the configuration of the Enhanced Security feature on the device. If the Enhanced Security feature is enabled for the device, a VNC Viewer can connect to the QuickPanel + on the VNC Server. Connection is dependent upon user authentication with the correct password. User password entry is validated with the Enhanced Security password. If the Enhanced Security feature is disabled for the device, the VNC Server does not enforce authentication of VNC Viewers.

The VNC Server is automatically launched during QuickPanel+ startup. It can also be launched manually from the Launch Application.

To manually launch the VNC Server: from the **Start** menu, select **Programs, System, Launch Application** and start the **VNC Server** application.

Figure 18:



From the Launch Application window, tap the **QP$^+$ VNC Server application icon**.

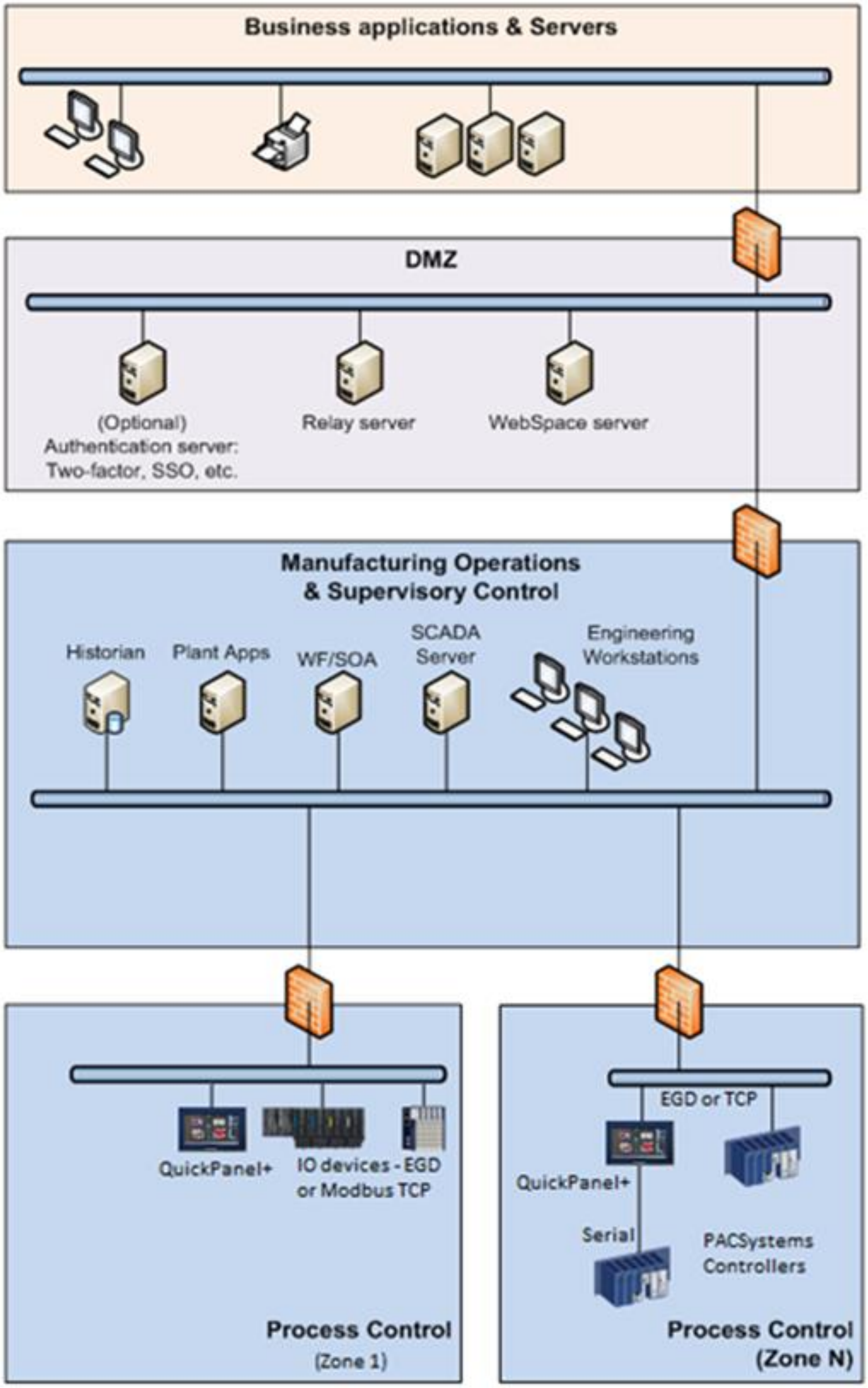
Note: *The VNC server starts approximately 40 sec after the QuickPanel+ startup process has completed.*

Chapter 6: Network Architecture & Secure Deployment

This chapter provides security recommendations for deploying QuickPane^{l+} 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 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 19: 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 of 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+ 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.*

Chapter 7: Optional Security Features

This functionality is optional for Emerson customers.

Effective March 2015, QuickPanel+ products were upgraded to include Secomea SiteManager and provide compatibility with the external Secomea Products. Refer to the table QuickPanel+ Operator Interface Products

for the product versions that support this functionality.

Customers wanting to update the product prior to these upgrades may update the software within their own QuickPanel + device by downloading the software update appropriate for the product from the Emerson support site. Review the Important Product Information (IPI) for the corresponding product.

7.1 Secomea Products

Activation and deployment of the Secomea product features is optional. SiteManager, GateManager, and LinkManager products are licensed, sold, and supported by Secomea and Secomea's licensed distributors.

QuickPanel+ customers wanting to activate licenses for Secomea products can do so at www.secomea.com.

The available Secomea SiteManager (embedded on QuickPanel+), GateManager, and LinkManager products are described as follows:

SiteManager is a device-monitoring front-end feature for multiple industrial devices on a location. Working with GateManager and LinkManager, it ensures uninterrupted and secure access to remote devices over the Internet or a private Wide-area Network (WAN) for all users.

LinkManager is an off-the-shelf software component in Remote Device Management Solutions from Secomea that provides security for external programming and monitoring applications. **LinkManager** Mobile provides similar functionality for mobile devices.

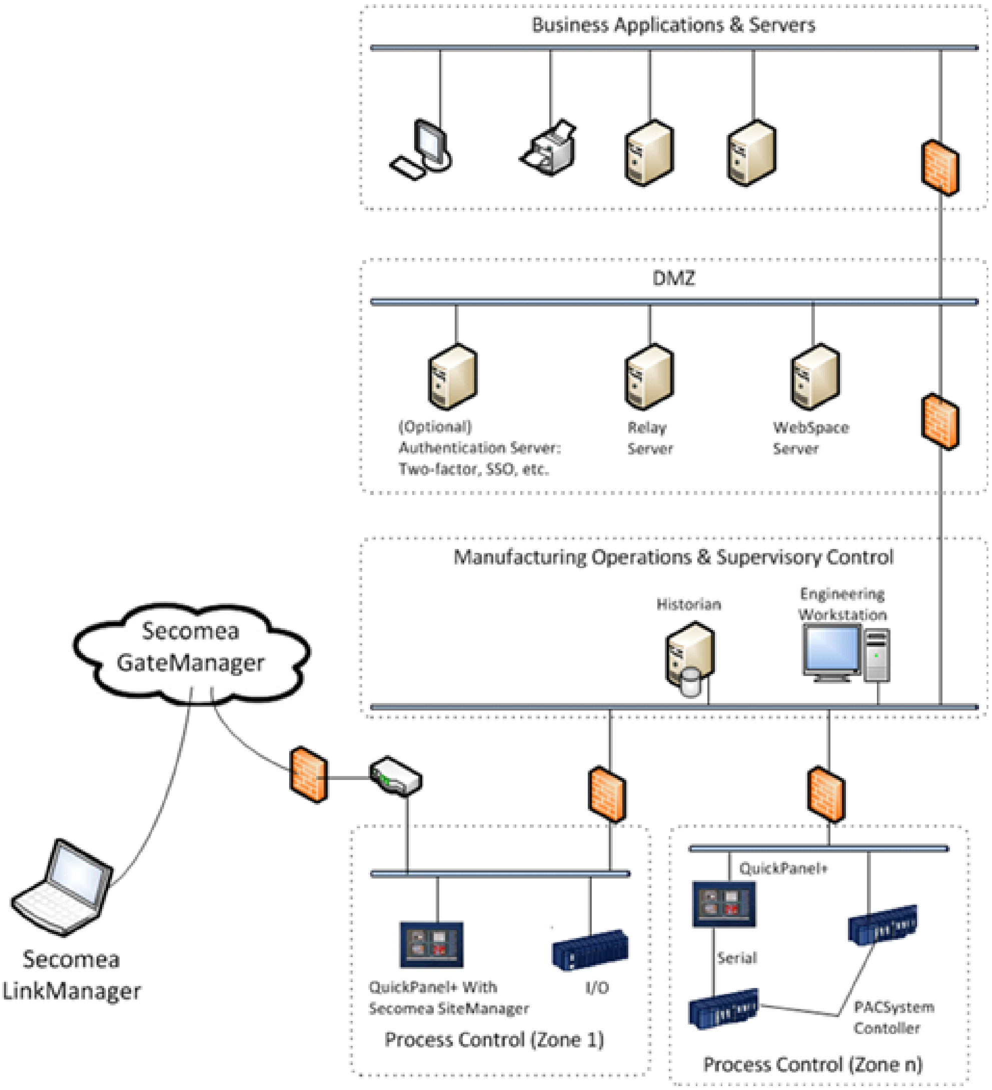
GateManager is the central component of Secomea's Industry solution. The GateManager M2M Server operates as a termination point for all LinkManagers and SiteManagers. All connections and the encrypted traffic between LinkManagers and devices controlled by SiteManagers are handled by the GateManager, where all events arealso logged.

Note: *The GateManager is typically offered as a service hosted by Secomea. Users will receive an isolated domain on the GateManager and benefit from central hosting and back-up by Secomea. Or, the user can host their own GateManager.*

Additionally, other devices such as PLCs and PCs (in addition to the QuickPanel+) 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 extended license feature from Secomea.

Note: *Secomea products installed throughout the application as suggested by the following figure do not intrinsically provide the level of security associated with firewalls. The network architect needs to satisfy himself or herself that the security level required by the application is present in the overall implementation.*

Figure 20: Secomea Products used with QuickPanel+ in Application



Chapter 8: Other Considerations

8.1 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+ controller be temporarily taken out of service.

Finally, some installations require extensive qualification 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.

8.2 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 PROFINET IO, Ethernet Global Data, and Reliable Datagram Service protocols are 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

8.3 TCP SYN Storm Denial of Service

To establish a TCP connection between a source host and destination host, a handshake sequence must occur. First, the source host sends a SYN packet to the destination host. If the destination host is listening for the SYN packet, it will respond with a SYN/ACK packet. The source host then acknowledges with an ACK packet and the connection between source host and destination host is established.

During the response of the SYN/ACK from the destination host (a QuickPanel+ Operator Interface in this case), a block of memory is set up to contain the data of the established connection. If for some reason an ACK is never received from the source host, a timeout occurs, and the block of memory winds up being allocated but unused. This behavior can be used in a well-known attack against TCP implementations, known as a TCP SYN Storm. In a TCP SYN Storm, the attacker will continually send a SYN packet to a destination host, without sending an ACK. If not properly mitigated, this can eventually consume all the memory on the destination host that is used to manage legitimate connections, resulting in a denial of service on the destination host.

TCP SYN Storm attacks can be detected and mitigated by monitoring source host SYN packets that do not have accompanying source host ACK response packets. Most mid-range to high-end firewalls today have this capability and should be used to mitigate the effects of TCP SYN Storm Denial of service attacks that originate from devices in a less-trusted security zone/network.

8.4 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+ 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.

8.5 Additional Guidance

8.5.1 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.

8.5.2 Government Agencies and Standards Organizations

Government agencies and international standards organizations may provide guidance 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 on Recommended Practices for cyber security 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 specifications to provide guidance on establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

Technical Support & Contact Information:

Home link: http://www.Emerson.com/Industrial-Automation-Controls

Knowledge Base: https://www.emerson.com/Industrial-Automation-Controls/support

Note: If the product is purchased through an Authorized Channel Partner, please contact the seller directly for any support.

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.