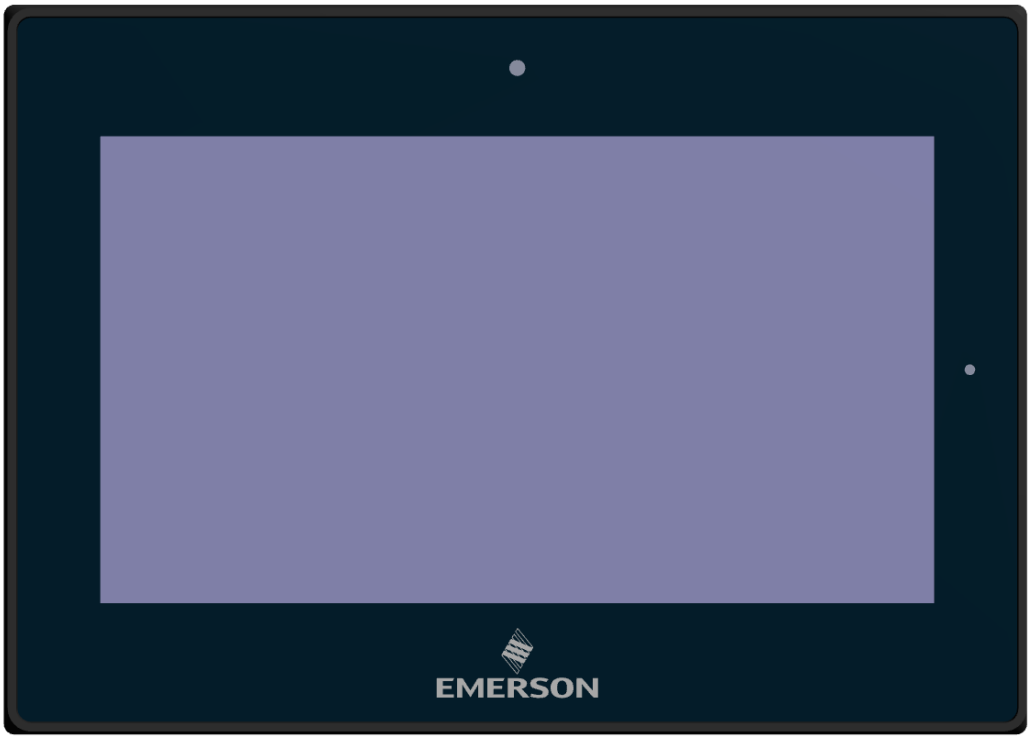
PACSystems™ RXi Web Panel

SECURE DEPLOYMENT GUIDE



EMERSON

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 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.

Contents

Section 1:About this Guide

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

Secure deployment information is provided in this manual for the following Web Panel Products.

Table 1: Web Panel Options

Product	Catalog Number	Product Description
7” RXi – Web Panel	IC757CSW07WHMI	Web Panel 7” Wide Screen
10” RXi – Web Panel	IC757CSW10WHMI	Web Panel 10” Standard
12” RXi – Web Panel	IC757CSW12WHMI	Web Panel 12” Standard
15” RXi - Web Panel	IC757CSW15WHMI	Web Panel 15” Standard
19” RXi – Web Panel	IC757CSW19WHMI	Web Panel 19” Wide Screen
24” RXi – Web Panel	IC757CSW24WHMI	Web Panel 24” Wide Screen
7” RXi – Web Panel	IC757COW07WHMI	Web Panel 7” Outdoor SLR Wide Screen
10” RXi – Web Panel	IC757COW10WHMI	Web Panel 10” Outdoor SLR Wide Screen
12” RXi – Web Panel	IC757COW12WHMI	Web Panel 12” Outdoor SLR Wide Screen
15” RXi – Web Panel	IC757COW15WHMI	Web Panel 15” Outdoor SLR Wide Screen
12” RXi – Web Panel	IC757NSW12WHMI	WEB WS BLK FRM OVRLY

1.1 Revisions to this Manual

Table 2: Revisions

Revision	Date	Description
E	Oct 2023	“Save” Button added to Setup Pages.
D	Nov 2022	Adds support for Remote Firmware Update
C	Jul 2022	Updates to support revised user privilege names. Adds support for SSH. Updates to Chromium browser support New Linux update (5.15.5) Removed Firefox browser support Updates to firewall rules: traffic allowed at ports 5001 and 1880
B	Feb 2022	RXi Web Panel Enhancement and added a new catalog item, number IC757NSW12WHMI
A	Jun 2019	Initial Release

1.2 Related Documents

Document No.	Description
GFK-3073	PACSystems RXi - Web Panel Quick Start Guide
GFK-3138	PACSystems RXi - Web Panel User Manual

Section 2: Introduction

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

- **Confidentiality**: Ensure only the people you want to see the 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 the appropriate care in securing their Emerson products and solutions.

2.1 Firewall

Firewalls and other network security products, including Data Diodes and Intrusion Prevention Devices, can be an important component of any security strategy. There should be firewalls and other security devices at the boundary of each network segment. By segmenting your network by general functionality, you can have greater control over what types of traffic are needed and prohibits activities that are not needed in that network segment, preventing them from being misused by malicious actors. However, a strategy based solely on any single security mechanism will not be as resilient as one that includes multiple, independent layers of security.

2.2 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. Network segmentation is part of this, but it is recommended to evaluate multiple security measures for each network segment.

2.3 General Recommendations

Adopting the following security best practices should be considered when using Emerson 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 product security updates, SIMs, and other recommendations.

Apply all of 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.

2.4 Check List

This section provides a sample checklist to help guide the process of securely deploying Web Panel 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 Web Panel module.
7. For each Web Panel module, change every supported password to something other than its default value.
8. For each Web Panel module, assign a unique device name to that module.
9. Harden the configuration of each Web Panel module, disabling unneeded features,
10. 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. For more information about security programs in general, see the section, Additional Guidance.

Section 3: Communication Protocols

This section describes how the supported application protocols for Ethernet and serial ports are used with Web Panel. 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 Automation Solutions 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 Web Panel.

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.

Table 3: Supported Protocols

Media	Protocol	Web Panel
Link	ARP	✓
	LLDP	—
Internet	IPv4	✓
	IPv6	—
	ICMP	✓
	IGMP	—
Trans	TCP	✓
	UDP	✓
Application Layer	DHCP/BOOTP Client	✓
	DCE/RPC Client	—
	DNS Client	✓
	FTP server	—
	HTTP server	—
	MRP	—
	SNMP v1 & v2c server	—
	SNTP client	✓
	SRTP client	—
	SRTP server	—
	Telnet server	—
	SSH/SFTP client	✓
	SSH/SFTP server	✓

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

Protocol	Web Panel
Application-specific	—
ASCII Terminal	—
Modbus RTU Slave	—
SNP Slave	—

3.1.3 USB Protocols

Web Panel supports USB-based communications with the available following ports.

- 1 X USB 2.0 Type A
- 1 X USB OTG (Micro-B)

The media like SD and USB are only available to the privileged wpadmin user. USB Protocols supported are as indicated below.

Protocol	Web Panel
Application-specific	—
USB	—
USB To Serial	—
USB To Ethernet	—
USB to Wi-Fi	—
USB OTG	Used for Firmware Upgrade
USB Storage	✓

3.1.4 SD/SDIO

Web Panel supports one micro SD Card.

Protocol	Web Panel
SD/SDIO	✓

3.2 Network Servers

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

Functionality	Required Application Protocols	Example Clients
Remote Shell Access	SSH/SFTP	putty, ssh, scp, sftp

3.3 Network Clients

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

Functionality	Required Application Protocols	Example Server
Web browser (Chromium)	HTTP, HTTPS	Apache, nginx, IIS
DNS Resolver	DNS	ISC BIND, Microsoft DNS
Dynamic Network Configuration	DHCP	ISC DHCP server, udhcpd

3.4 Ethernet Firewall Configuration

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, to support only the required communications paths for any particular installation.

RXi Web Panel supports a built-in iptables firewall. All unused networking ports other than HTTP, HTTPS, SSH, ICMP, TCP, and SNTP will be disabled.

3.4.1 Built-In Firewall

To load the default firewall rules , run this script:

/usr/bin/iptables_rule.sh

Note: Only the privileged wpadmin user may modify the above script.

1. To view the active firewall rules, use the following steps:
   a. Open a terminal window or log in remotely using SSH.
   b. Switch to the privileged user wpadmin by running the **su wpadmin** command and entering the password for the wpadmin user
   c. Run **sudo iptables --list-rules** to view the current rules.

Figure 1: Sample Output for Firmware Revision 'r311 (20220623)

```
webpanel:~$ su wpadmin
Password:
webpanel:/home/wpuser$ sudo iptables --list-rules
Password:
-P INPUT DROP
-P FORWARD DROP
-P OUTPUT DROP
-A INPUT -p udp -m udp --sport 53 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 80 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 443 -j ACCEPT
-A INPUT -p tcp -m tcp --dport 22 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A INPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A INPUT -i lo -j ACCEPT
-A INPUT -p udp -m udp --sport 123 -j ACCEPT
-A INPUT -p tcp -m tcp --tcp-flags RST RST -m limit --limit 2/min --limit-burst 2 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 1880 -j ACCEPT
-A INPUT -p tcp -m tcp --sport 5001 -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK SYN -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p udp -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 8 -m limit --limit 1/sec -j ACCEPT
-A FORWARD -p tcp -m tcp --tcp-flags FIN,SYN,RST,ACK RST -m limit --limit 1/sec -j ACCEPT
-A OUTPUT -p udp -m udp --dport 53 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 80 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 443 -j ACCEPT
-A OUTPUT -p tcp -m tcp --sport 22 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 0 -j ACCEPT
-A OUTPUT -p icmp -m icmp --icmp-type 8 -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -p udp -m udp --dport 123 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 1880 -j ACCEPT
-A OUTPUT -p tcp -m tcp --dport 5001 -j ACCEPT
```

3.4.2 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 Web Panel.

Table 4: Link Layer Protocols

Protocol	Ethernet Type
ARP	0x0806
LLDP	0x88cc

Table 5: Internet Layer Protocols

Protocol	Ethernet Type	IP Protocol
IPv4	0x0800	N/A
ICMP		1
IGMP		2

Table 6: Transport Layer Protocols

Protocol	Ethernet Type	IP Protocol
TCP	0x0800	6
UDP		17

Table 7: Application Layer Protocols

Protocol	Server TCP Port	Dest UDP Port
DCE/RPC	—	34964 on server >1023 on client
DNS	53	53 on server >1023 on client
FTP	—	—
HTTP	80	—
HTTPS	443	—
SNMP	—	—
SSH	22	—
DHCP/BOOTP	69	—
Web Socket	9001[1]	

[1] The Rxi Web Panel build R328 by default enables WebSocket Service to listen messages over TCP/IP port 9001.

Section 4:Security Capabilities

4.1 External Storage

The Web Panel supports SD 3.0, MMC, SDIO cards, and USB for external storage. The cards can be used as a buffer media to transfer data. It is up to the user to decide how he wants to archive/protect the data on the SD card. Media like SD and USB are only available to the privileged wpadmin user.

4.2 Firmware Updates

To upgrade the Web Panel's firmware, the user must download the required files from the Emerson Support Center and copy them to a laptop or PC (with Windows 10 or later). *The user can update the firmware over a micro-USB connection until **R313** build versions and from R328 build versions also:*

The steps are documented in GFK-3138, Industrial Display User Manual, "Section 10.1: Firmware Update Instructions for the RXi - Web Panel".

4.3 Remote Firmware Updates

To remotely upgrade the Web Panel's firmware, the user must download the required files from salesforce and copy them to a laptop/PC (with Windows 10 or later). *The user can update the firmware over SSH from the **R32X** build versions or later version:*

The steps are documented in GFK-3138, Industrial Display User Manual, "Section 10.2: Updating Firmware Remotely".

4.4 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, the FTP service is disabled in Web Panel whereas the SSH service is disabled for the user to log in and look at the log files.

Note: The Web Panel only acts as a user interface display rendering device, the user activities are done and controlled by web servers, so the critical system logo should be put on the web servers, not on Web Panel.

4.5 User Access Control (UAC)

Web Panel will provide list privileges to all the files and directories in the system to make sure not all the files and directories are readable/writable/executable by everyone.

Web Panel will make sure that files that are readable, writable, and executable by the wpadmin should only be owned and group-owned by the wpadmin. The file system can only be modified by the wpadmin user, and the browser only has one-wpadmin user access right.

Web Panel will use appropriate security options like nosuid, nodev, noexec, or while mounting the filesystem.

The chromium web browser in Web Panel will run under normal wpuser privilege.

Following are the restrictions on user privileges for the System Setup page usage.

- The privileged wpadmin can enable/ disable the SSH option for secure connectivity.
- Non-privileged wpuser cannot change the privileged wpadmin password.
- Non-privileged wpuser only can use a terminal emulator like putty.
- Shell terminal cannot be opened using ALT+F1, ALT + F4 to F6.
- The unmounted filesystems/block devices and promiscuous/packet-capture mode on the NIC cannot be accessed.
- Non-privileged wpuser cannot access physical memory via /dev/mem and /dev/kmem.
- The privileged (wpadmin) can enable/ disable the USB storage option.
- Non-privileged wpuser cannot mount the removable media.

4.6 Available User Types

Table 8: User Accounts and Default Passwords

Account Type	Account Name	Default Password
Non-privileged	wpuser	EMwpuser
Privileged	wpadmin	EMwpadmin

4.7 Security Boot

The secure boot will be enabled and cannot be disabled once the OTP (one-time program) fuse has been burned to prevent malicious attackers from running a compromised bootloader/ operation. The system only can be booted with the image signed by the keys of the secure boot, the keys are programmed in hardware OTP fuses, which cannot be modified.

TPM (Trusted Platform Module) interface is only available for x86 systems, not on ARM systems, the TPM module works with LPC (Low pin count) hardware interface, which is only available on x86 CPU.

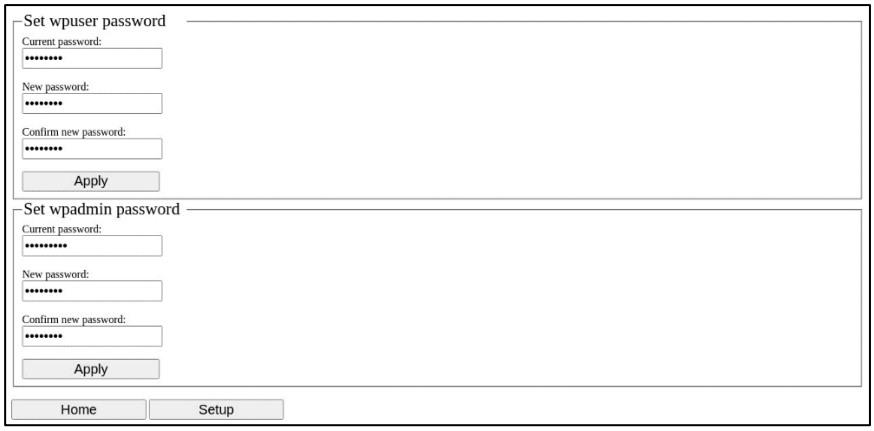
4.8 Web Panel Start-Up Behavior

When the web panel boots for the first time, the following screens will be shown to the user, and the user will be required to change the wpuser/wpadmin default passwords. The **Home** and **Setup** buttons are not visible until both the wpuser and wpadmin passwords are set.

Notes:

- Access to the privileged wpadmin is a product feature, and the non-privileged wpuser account does not have full access to the privileged wpadmin account.
- Web Panel shall not allow setting the same passwords for privileged wpadmin and non-privileged wpuser accounts.

Figure 2: Web Panel Start-Up Behavior



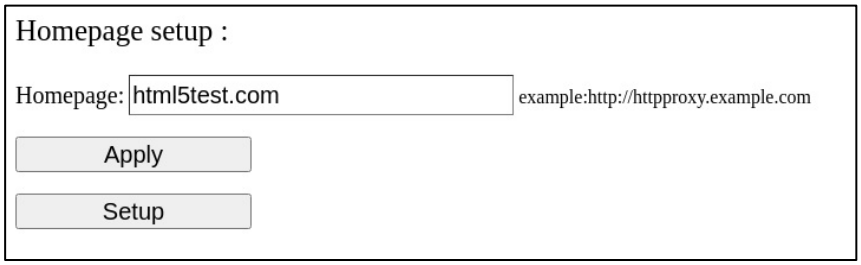
Note: The **Home** and **Setup** buttons will not appear until the passwords for wpuser and wpadmin have been set.

New passwords must follow these rules:

- Must contain at least 8 characters
- Must be fewer than 32 characters
- Must be a combination of both upper-case and lower-case letters (case sensitivity)
- Must contain at least one numerical digit

Once the wpuser or the wpadmin passwords have been changed successfully, the user should configure the homepage address using the following screen. The user will need to input the URL/ IP address to run the Chromium browser in kiosk mode. Chromium is set as a default browser.

Figure 3: Homepage Setup



Section 5: Configuration Hardening

5.1 Server Default States

Due to security concerns, the following servers are disabled/ enabled by default on the Web Panel device:

- FTP server Disabled
- HTTP server Disabled
- SNTP client - Enabled
- SSH - Disabled

5.2 Ethernet Interface

Interface	Availability
Bootp Client	Not Available
FTP Server	Not Available
IP Routing	Available
DNS Client	Available
SNTP Client	Available. On console key-in “systemctl stop ntpdate.service”
Web Server	Not Available.

5.3 Device/ Web Configuration

Device/ Web browser	Enabled/ disabled
Access to physical memory via /dev/mem and /dev/kmem	Disabled. Web Panel Application doesn’t have root access rights.
Web browser plug-ins	No plug-in was available in the Chromium web browser.
Web browser extensions	Except for the following, the browser won’t allow adding more extensions, • LAN port IP setting • LCD backlight adjustment setting
Web browser security configuration	Only HTTPS protocol configuration is enabled.
SD-Card/USB configuration	Only HID keyboard and mouse devices can be detected and used on the USB port, the USB host port for embedded Linux system is without autoplay/autorun capability.

5.4 Web Panel System Setup

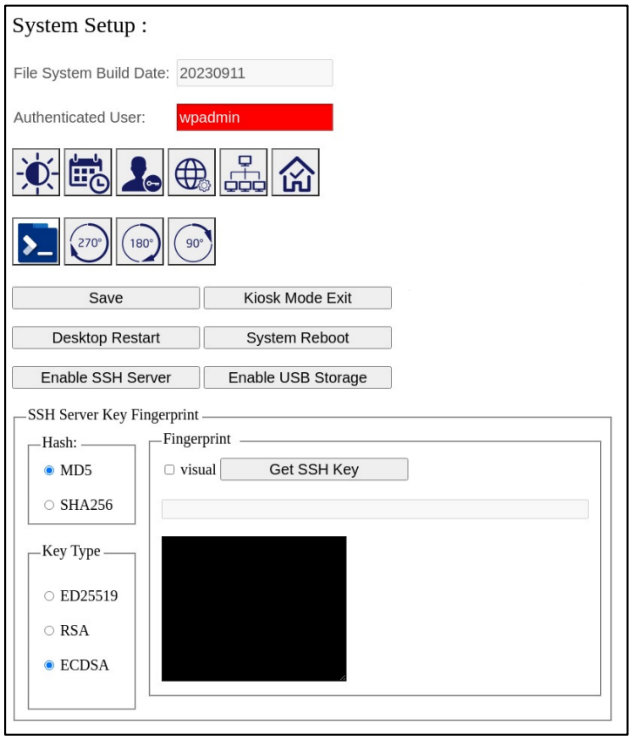
The setup page is used to configure the Web Panel settings. The user needs to click on the **Setup** button on the Homepage setup page or on the startup screen to access the System Setup page.

1. The user needs to provide the non-privileged wpuser and privileged wpadmin credentials and click on the **Confirm** button to access Web Panel settings (Figure 4).

Figure 4: System Setup

2. The user can configure the Web Panel settings (Figure 5).

Figure 5: System Setup



3. File System Build Date is the date at which files were built and released to the customer. The firmware image version RXi_Yocto_Linux_WebPanel_No_EMRLogo_r3XX_rcv.zip and RXi_Yocto_Linux_WebPanel_r3XX_rcv.zip will have the File System Build Date as YYYYMMDD the date when it was built.

   Example: Build R328 will have File System Build Date as 20230911

⚠ WARNING:

- Be cautious when accessing a shell terminal using privileged wpadmin access, since the entire system access can be gained using the terminal.
- It is the user's responsibility to be sure they know what they are doing if they choose to log in as a non-privileged wpuser or privileged wpadmin.
- The non-privileged wpuser or privileged wpadmin cannot update critical OS files like the kernel, device tree, and ramdisk.
- It is the user's responsibility to be sure they know what they are doing if they choose to update other land programs as a non-privileged wpuser or privileged wpadmin.

5.5 Secure Shell (SSH)

SSH uses encryption to secure network connections over an insecure network. To establish a secure connection, encryption keys are automatically exchanged between server and client. If establishing an SSH client connection for the first time, the user will be asked to accept the remote host public key. Accepted public keys are stored in a client database to be used in future communications. If an authorized server tries to masquerade as a known server whose public key is already stored in the client database, SSH tools will warn about a key change, thus enabling the user to identify the fraud.

5.5.1 WebPanel System SSH

The keypairs are used to uniquely identify devices on the network when using the SSH protocol. The SSH-Host-Key-Pairs (public and private) are stored in the directory /etc/ssh. These keys are not populated at the time of delivery. Therefore, each RXi Web Panel generates a set of asymmetric cryptography keypairs upon its first boot.

The system setup page displays fingerprints for the RXi Web Panel's OpenSSH server public keys. The hashing algorithm and the key type can be selected interactively to display the fingerprints in formats that SSH clients will commonly use. The public key will be displayed to the user for an unrecognized SSH server for interactive confirmation of trust. The users may use these generated key pairs or may choose to create new ones with the ssh-keygen command post logging into SSH Terminal.

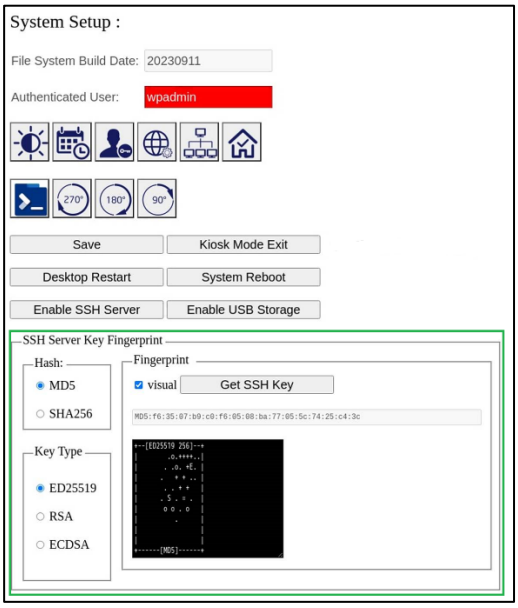
5.5.3 Steps to View SSH Server Key

1. Click the **Setup** button on the Homepage setup page or on the startup screen to access the System Setup page.
2. Provide the non-privileged wpuser and privileged (wpadmin) credentials and click on the **Confirm** button to access Web Panel settings.

Figure 6: System Setup

3. Select the hashing algorithm, and the key type and enable the **visual** checkbox. Click on the **Get SSH Key** button to view fingerprints in formats that SSH clients will commonly use.

Figure 7: SSH Server Key Fingerprint



5.6 Linux Command Usage

The user can switch to a wpadmin user by using the **sudo** command before running any command.

5.6.1 Access a terminal prompt on the Web Panel:

Option A – Local Access

1. Click the **Setup** button on the Homepage setup page or on the startup screen to access the System Setup page.
2. Log in as either the wpuser or the wpadmin user.
3. Select the **Terminal**  icon.
4. To exit the shell when done, type **exit** or Control-D.

Option B – Remote Access

1. Enable the SSH server as documented in Section 5.5.2.
2. Confirm the IP address using the **Network** setup page. Note: This step is necessary if using a DHCP address, Link-Local, or otherwise.
3. Connect to the Web Panel from your client.
4. Verify the fingerprint and trust it, if is correct.

Figure 8: Verify and Trust the SSH Fingerprint

```
: user@laptop; ssh wpuser@169.254.16.106
The authenticity of host '169.254.16.106 (169.254.16.106)'
can't be established.
ED25519 key fingerprint is
SHA256:jGwFv9B3DzqrELK7MfZORNSSYsbKQK950GhQxrc+6hQ. COMPARE-TO-
SETUP-PAGE-FINGERPRINT
This key is not known by any other names
Are you sure you want to continue connecting
(yes/no/[fingerprint])? yes
Warning: Permanently added '169.254.16.106' (ED25519) to the
list of known hosts.
```

5. Enter the wpuser password.

Figure 9: Enter the wpuser password

```
wpuser@169.254.16.106's password: <WPUSER-PASSWORD>
The server has updated its host keys.
These changes were verified by the server's existing trusted
key.
```

6. To exit the shell when done, type **exit** or Control-D.

5.6.2 Run Commands as the Root User

1. Log in locally using the Terminal app or remotely using SSH as a wpuser.
2. Switch to the wpadmin user by running **su wpadmin** and entering the wpadmin password.

Figure 10: Log in as wpadmin

```
webpanel:~$ su wpadmin
Password: <WPADMIN-PASSWORD>
```

Running Wpadmin Commands as Root Using Two Methods

1. Single commands can be run using the **sudo** command.

Figure 11: sudo command example

```
webpanel:/home/wpuser$ sudo id
Password: <WPADMIN-PASSWORD>
uid=0(root) gid=0(root) groups=0(root)
```

Examples:

- sudo poweroff
- sudo reboot
- sudo journalctl -f
- sudo iptables --list-rules

2. Multiple commands can be run by starting a shell running as root using the command **sudo -s**.

Figure 12: Commands

```
webpanel:/home/wpuser$ sudo -s
webpanel:/home/wpuser# id
uid=0(root) gid=0(root) groups=0(root)
webpanel:/home/wpuser#
```

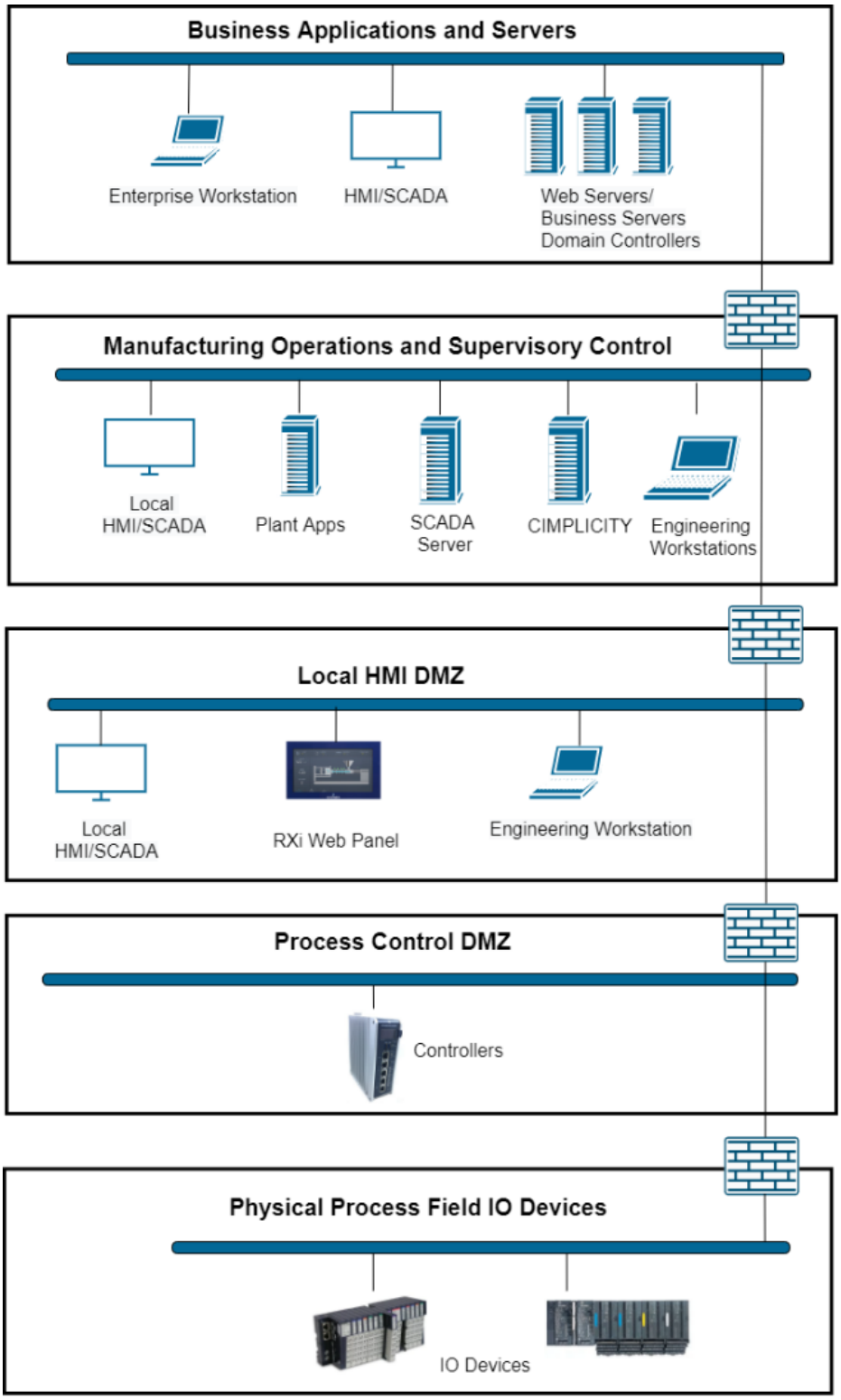
Note: When the shell is running as wpadmin, the character at the end of the default prompt will change from a **$** to **#**.

Section 6: Network Architecture and Secure Deployment

This section provides security recommendations for deploying Web Panel 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 13: System 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 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 particular 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 particular 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.

Section 7: Other Considerations

7.1 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 Web Panel services be taken to out of service.

Finally, some installations require extensive qualifications 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.

7.2 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 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.

7.3 TCP SYN Storm Denial of Service

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

During the response of the SYN/ACK from the destination host (Web Panel 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 an 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.

7.5 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 Web Panel 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.

Section 8: Additional Guidance

8.1 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.

8.2 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 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 guide establishing and operating a cyber-security program, including recommended technologies for industrial automation and control systems.

General Contact Information

Home link: http://www.emerson.com/industrial-automation-controls

Knowledge Base: https://www.emerson.com/iac-support

Technical Support

Americas
Phone: 1-888-565-4155
1-434-214-8532 (If toll-free option is unavailable)

Customer Care (Quotes/Orders/Returns): customercare.mas@emerson.com
Technical Support: support.mas@emerson.com

Europe
Phone: +800-4444-8001
+420-225-379-328 (If toll-free option is unavailable)
+39-0362-228-5555 (from Italy - if toll-free 800 option is unavailable or dialing from a mobile telephone)

Customer Care (Quotes/Orders/Returns): customercare.emea.mas@emerson.com
Technical Support: support.mas.emea@emerson.com

Asia
Phone: +86-400-842-8599
+65-3157-9591 (All Other Countries)

Customer Care (Quotes/Orders/Returns): customercare.cn.mas@emerson.com
Technical Support: support.mas.apac@emerson.com

Any escalation request should be sent to: mas.sfdcescalation@emerson.com

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.

EMERSON