The Cybersecurity Guide

Configuration Guideline

Version 1.0

Disclaimer

Subject to change without notice

The information contained in this document is provided for informational purposes only. While efforts were made to verify the accuracy of the information contained in this documentation, it is provided 'as is' without warranty of any kind.

- The copyright of this manual is owned by Exor International S.p.A.
- Unauthorized reproduction of this manual is strictly prohibited.
- Windows is a registered trademark of Microsoft Corporation in the U.S. and other countries.
- Ethernet is a registered trademark of FUJIFILM Business Innovation Co., Ltd. and Xerox Corporation.
- Other company and product names are trademarks or registered trademarks of their respective companies.

Third-party brands and names are the property of their respective owners.

The example companies, organizations, products, domain names, e-mail addresses, logo, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

For more details or for a copy of sources where required by license , as well as the respective copyright notice, please ref to device settings menu or https://www.exorint.com or contact us at support.it@exorint.com

Contents

Cybersecurity Guide

This document provides the guidelines for correctly configuring the HMI device's functionality, making it as secure as possible from external Cyber Attacks.

> It is assumed that the most recent **v4.1** or **v5.1** versions have been installed on the HMI devices and that they are updated whenever a new version is made available on the manufacturer's website.

The HMI device is designed for use in typical industrial and naval automation operating environments, which usually involves communication with programmable logic controllers (PLCs). The overall system is assumed to operate at **Security Level 2**. Consequently, the products are designed to meet the security requirements for this level.

The **Software Bill of Materials (SBOM)** for the HMI device is accessible from the device System Settings page.

Operational States

The HMI device has three operating states:

- **Boot Mode**

  Upon power-on, essential services are started, and system components are loaded and initialized to enable the device's normal operations (Operating mode). During this phase, unless expressly disabled, the TAP TAP feature is available on the touchscreen to activate the device in Recovery Mode.

- **Operating Mode (mainOS)**

  In operating mode, the device is controlled by the loaded application (the user-level application that implements the functionality required by the end customer). If an application isn't present, or if its startup is disabled, the HMI device's "Launcher Screen" will be displayed. From this interface, you can install an application to run or configure system parameters.

- **Recovery Mode (configOS)**

  This operational state is dedicated to system recovery and machine configuration tasks. In this state, a system configuration with parameters adapted to the specific recovery functionality is loaded. Any changes to the system parameters will be temporary and will be lost on the next device reboot.

Unboxing

At the first attempt to access the device's System Settings, you will be asked to define a password that will be associated with the "admin" user. If you try to access it remotely via a web browser, you'll need to authenticate as the "admin" user with the password "admin" to access the password definition. Next, once you've defined the password for the "admin" user, all BSP parameters will be accessible.

> It is assumed that the initial development and configuration stages will take place in a secure environment. Ensure the device is properly configured before moving it to its operational environment.

Device security-related parameters

By default, the main security functions are enabled, but the default configuration is primarily designed to facilitate the development and commissioning of the HMI device. The following lists the security features available on the device, so you can review and configure them based on your requirements.

> It is the responsibility of the system integrator and the application developer to verify the correct device configuration in order to achieve the desired level of security. This guide is intended to provide support for a quick configuration of the available security feature

Some features are mandatory and cannot be disabled, while others are optional and can be disabled or configured differently.

A security feature can be disabled because it is not needed (e.g., the firewall is not needed if the device is not connected to the network) or to allow the management of devices that do not support the highest security standards (e.g., enable the possibility to use the HTTP or FTP protocols instead to force using HTTPs and FTPs). The disabling of security-related functions, when possible, is the responsibility of the developer of the application, who must take care to make up for it with alternative measures.

Often some features related to security are disabled during the development phase of the application to be able to access the device resources more easily. It is a good practice to remember to perform a check before releasing the developed application in order not to risk leaving unnecessary services active which could compromise the safety of the device.

It's recommended to read the detailed description of each security-related parameter in the manual before modifying it.

Logs

- To reduce the risk of data saved in log files being lost, you can also configure and send all data to a remote server (SysLog).

Date & Time

- The device's date must be set correctly. If the device is connected to the internet, you can enable automatic date updates through an NTP server.

Network

- The 802.1X authentication protocol can be configured to get access protected networks that require this type of authentication.

Security

- It's possible to configure the device so that it does not use unknown external memory cards.

Disable external USB devices	
Default state	FALSE
Suggested state to maximize security	TRUE

Disable SD card automount	
Default state	TRUE
Suggested state to maximize security	TRUE

- It's possible to configure the device so that all software module updates are only accepted if they are digitally signed.

Allow installation of unsigned modules (insecure mode)	
Default state	TRUE
Suggested state to maximize security	FALSE

Applications

- It's possible to configure the device so that all applications run in restricted user mode.

Execute all applications as root	
Default state	FALSE
Suggested state to maximize security	FALSE

Services

There are several services supported by HMI devices that can be enabled or disabled to meet the needs of different work environments.

> It is recommended to disable any services that are not strictly necessary in order to reduce the attack surface and minimize opportunities for a potential attacker.

Autorun scripts from external storage

- It is possible to disable the automatic execution of scripts from external storage devices (USB and SD card).

Enabled Autorun scripts from external storage	
Default state	FALSE
Suggested state to maximize security	FALSE

- Through the "Allow only user-certified scripts" parameter, you can configure the device to execute only the scripts that have been validated by the HMI device administrator..

Allow only user-certified scripts	
Default state	FALSE
Suggested state to maximize security	TRUE

Avahi Daemon

- It's possible to prevent the device from being identified on the network by its name by disabling the Avahi Daemon.

Enabled Avahi Daemon	
Default state	FALSE
Suggested state to maximize security	FALSE

Cloud / VPN Service

- Through Cloud/VPN services, it is possible to access the panel from the outside.

Enabled Cloud / VPN Service	
Default state	FALSE
Suggested state to maximize security	FALSE

Device Discovery

- It's possible to prevent the device from being identified on the network via the Device Discovery message.

Enabled Device Discovery	
Default state	TRUE
Suggested state to maximize security	FALSE

Enable device restore via TAP TAP option

- It's possible to disable the ability to perform a factory restore of the device through the “TAP TAP”.

Enable device restore via TAP TAP option	
Default state	TRUE
Suggested state to maximize security	FALSE

> If the ability to restore the device is disabled both via the TAP TAP option and through a USB drive then, in the event the administrator password is lost, the device can only be recovered by returning it to the manufacturer.

Enable device restore via USB

- It is possible to disable the ability to perform a factory restore of the device by reading the special file from the USB device.

Enable device restore via USB	
Default state	TRUE
Suggested state to maximize security	FALSE

> If the ability to restore the device is disabled both via the TAP TAP option and through a USB drive then, in the event the administrator password is lost, the device can only be recovered by returning it to the manufacturer.

Enable TAP TAP menu via touchscreen or mouse

- It's possible to disable access to the device configuration via the TAP TAP on touchscreen or mouse (keyboard access, via the CANC key on a USB keyboard, will remain unaffected by this setting)..

Enable TAP TAP menu via touchscreen or mouse	
Default state	TRUE
Suggested state to maximize security	FALSE

Firewall Service

- The device is equipped with a firewall that allows you to define which connections will be accepted while excluding all remaining undefined connections.

Enable Firewall Service	
Default state	FALSE
Suggested state to maximize security	TRUE

Network Rate Limiter

- Rate limiting controls the amount of network traffic by setting limits on the number of requests allowed within a specific time frame. This prevents system overload and protects against Denial-of-Service (DoS) attacks. It lets you create rules to limit the maximum number of packets transmitted on network interfaces.

Enable Network Rate Limiter	
Default state	FALSE
Suggested state to maximize security	TRUE

Router / NAT / Port forwarding

- This service allows network devices to be accessed from the outside through the HMI device.

Enable Router / NAT / Port forwarding	
Default state	FALSE
Suggested state to maximize security	FALSE

SNMP Server

- When the SNMP service is enabled, an SNMP client can retrieve various information from the device using the SNMP protocol.

Enable SNMP Server	
Default state	FALSE
Suggested state to maximize security	FALSE

SSH Server

- Through this service, you can access any resource on the HMI device. The service was designed to be used only by expert users during application development.

Enable SNMP Server	
Default state	FALSE
Suggested state to maximize security	FALSE

VNC Service

- VNC is a service that allows remote access to the HMI device's display.

Enable VNC Service	
Default state	FALSE
Suggested state to maximize security	FALSE

> If enabled, the service provides several security-related parameters (authentication, encryption, certificates, session timeout, etc.) that must be configured to suit your specific needs.

Web Server

- For backward compatibility, by disabling the "Allow only Secure HTTPS connections" parameter, access to the HMI device parameters is also accepted from insecure web connections.

Allow only Secure HTTPs connections	
Default state	TRUE
Suggested state to maximize security	TRUE

- Using the CORS (Cross-Origin Resource Sharing) parameter, you can enable access to the HMI device's system parameters from websites on a different domain. If enabled, make sure the CORS domains filter" parameter contains the list of external domains that will be accepted because, if left empty, any domain will be accepted.

CORS domains enabled	
Default state	FALSE
Suggested state to maximize security	FALSE

Management

- It does not contain parameters related to security. However, from this page, you can back up and restore the entire HMI device. A policy for regular backups is useful for maximizing the security of the HMI device.

Authentication

- The "Session" panel contains parameters that are useful for strengthening the defense against potential cyber threats, such as brute-force attacks aimed at guessing account passwords. These parameters should be adjusted on a case-by-case basis, depending on the work environment that will host the HMI device. The default values are designed to suit the most common work environments.
- By default, a “Password security policy” is already in place, which should be sufficient for most cases. If needed, you can redefine it to better suit your specific requirements.

Safe disposal

When the HMI device is decommissioned and needs to be disposed of, it's important to remember that it may contain confidential information. This data must be erased to ensure it is not left on the device after disposal.

All information can be deleted by performing a factory reset. You should also check that any removable storage (USB or SD card) is not left inside the device.

Security Disclosure Policy

For general information or inquiries related to cyber security, please contact our Technical Support team through the standard communication channels.

If you have identified a potential security vulnerability affecting our products or devices, we kindly ask you to report it by sending a detailed disclosure to: security@exorint.com.

We are committed to investigating all reports and taking appropriate action to ensure the security and integrity of our solutions.

Exor International S.p.A.
Via Monte Fiorino 13
37057 San Giovanni Lupatoto (Verona)
Italy

The Cybersecurity Guide
Configuration Guideline

1.0
2025-09-08

www.exorint.com
info@exorint.it
phone: +39 045 8750404
fax: +39 045 8779023