

# Rosemount™ 2405 Monitoring Hub



## Safety messages

### **WARNING**

#### **Physical access**

Unauthorized personnel may potentially cause significant damage to and/or misconfiguration of end users' equipment. This could be intentional or unintentional and needs to be protected against.

Physical security is an important part of any security program and fundamental in protecting your system. Restrict physical access by unauthorized personnel to protect end users' assets. This is true for all systems used within the facility.

---

# Contents

|                  |                                             |           |
|------------------|---------------------------------------------|-----------|
| <b>Chapter 1</b> | <b>Introduction.....</b>                    | <b>5</b>  |
| <b>Chapter 2</b> | <b>System overview.....</b>                 | <b>7</b>  |
|                  | 2.1 General information.....                | 7         |
|                  | 2.2 System design.....                      | 7         |
|                  | 2.3 Security model.....                     | 7         |
|                  | 2.4 Expected operating environment.....     | 8         |
| <b>Chapter 3</b> | <b>Commissioning.....</b>                   | <b>11</b> |
|                  | 3.1 General information.....                | 11        |
|                  | 3.2 Installation.....                       | 11        |
|                  | 3.3 Configuration.....                      | 11        |
| <b>Chapter 4</b> | <b>Operation.....</b>                       | <b>13</b> |
|                  | 4.1 General information.....                | 13        |
|                  | 4.2 Backup and restore.....                 | 13        |
|                  | 4.3 Audit log.....                          | 13        |
|                  | 4.4 Security incident reporting .....       | 14        |
|                  | 4.5 Security update management.....         | 14        |
|                  | 4.6 Application user privilege levels.....  | 14        |
| <b>Chapter 5</b> | <b>Decommissioning.....</b>                 | <b>17</b> |
|                  | 5.1 General information.....                | 17        |
|                  | 5.2 Decommissioning the Rosemount 2405..... | 17        |



# 1 Introduction

The Rosemount 2405 Security Manual is intended to complement the Rosemount 2405 Reference Manual. The information contained in this document provides information on how to install, operate and discard the product in a secure way. This documentation must be followed during the entire life cycle of the product.

## **Related information**

[Rosemount 2405 Reference Manual](#)

[Rosemount 2405 Quick Start Guide](#)

[Rosemount 2405 Product Data Sheet](#)



## 2 System overview

### 2.1 General information

This Security Manual covers the Rosemount 2405 Monitoring Hub security features and how they shall be applied. The Security Manual complements the Product Data Sheet, Quick Start Guide and Reference Manual with security related information in adherence to IEC 62443-4-1: "Secure product development lifecycle requirements".

### 2.2 System design

The Rosemount 2405 Monitoring Hub delivers inventory control and monitoring of multiple storage tanks. Tank and inventory data can be viewed either locally in the field, or via a web browser. The monitoring hub is an all-in-one device that integrates a data concentrator, display, and communication unit.

The Rosemount 2405 provides the following interfaces:

- A graphical field display together with physical buttons for configuration, and to visualize the system and measured values
- Web interface for configuration, and to visualize the system and measured values
- Sensor inputs for sensor connection using HART® multidrop
- Digital inputs for hardwired digital signals
- Relay outputs for hardwired system failure and alarm outputs
- Analog outputs for hardwired analog signals
- Modbus® TCP/IP connection to host systems for access to measured and calculated tank data
- HART-IP interface to enable remote configuration and diagnostics of the HART devices from an asset management system that supports HART-IP gateways, such as AMS Device Manager

The Rosemount 2405 offers seamless integration with the Rosemount TankMaster and TankMaster Mobile inventory management platforms, and reliable connectivity with third-party host systems.

### 2.3 Security model

The Rosemount 2405 Monitoring Hub connections should be installed on a secure network in accordance with local IT policies (e.g., a process network). To fully utilize all security features of the Rosemount 2405, it must be protected from exposure to the Internet or any other potentially unsafe connections. Firewalls or other network protection mechanisms, such as rate limiting, are required to defend against denial-of-service attacks. Additionally, the Rosemount 2405 still needs to adhere to the preconditions outlined in the manuals.

The Rosemount 2405 is intended for use in industries requiring inventory monitoring functionality, where it would be installed inside an industrial facility or at least in an area with restricted access (fencing, gates, etc.). It would be connected to the process control network (level 1 or 2 in the Purdue model) only and be accessed from SCADA/DCS/HMIs at network levels 2 and 3. Industry-standard separation between network levels using firewalls etc. is expected.

Security context is defined by threat and risk model and assumptions made there. There are several interfaces that need to be considered. Three network interfaces HART<sup>®</sup>-IP, Modbus<sup>®</sup> TCP, REST HTTPS interfaces and two user interfaces (local display and web interface). The communication on the REST HTTPS is protected via TLS v1.2.

The communication channel on Modbus is not protected via encryption but writing a PIN code is required for modifying the registers. Modbus TCP/IP connectivity is enabled by default in read-only mode. Configuration changes via Modbus can be permitted by adjusting the remote access settings.

There is no inherent protection on the HART-IP interface. Remote access via HART-IP is disabled as default.

The storage memory in the Rosemount 2405 device is divided into two sections: one that is inaccessible externally, and another that is encrypted to prevent unauthorized access to the information.

User access is based on roles, with two separate accounts assigned for operator and administrator functions. Each role has clearly defined permission rights and responsibilities. Grant user privileges based on the least privilege principle, only what is necessary for the task.

The web interface is protected via sign-in using passwords for operators and administrators. The default web interface password is unique for each device. Passwords must be updated using strong and unique combinations to ensure secure access.

The local display is protected via login using a PIN code for configuration sensitive menus accessible only for administrators. It is assumed that due to security context and installation environment everyone having physical access to the device will be assigned the default role of operator while administrators will be the only ones having access to the PIN code. The default PIN code from factory is identical across all devices. It is recommended to change the PIN code to enhance security. Disabling the PIN code is possible, but doing so may increase security risks.

#### Related information

[Application user privilege levels](#)

## 2.4 Expected operating environment

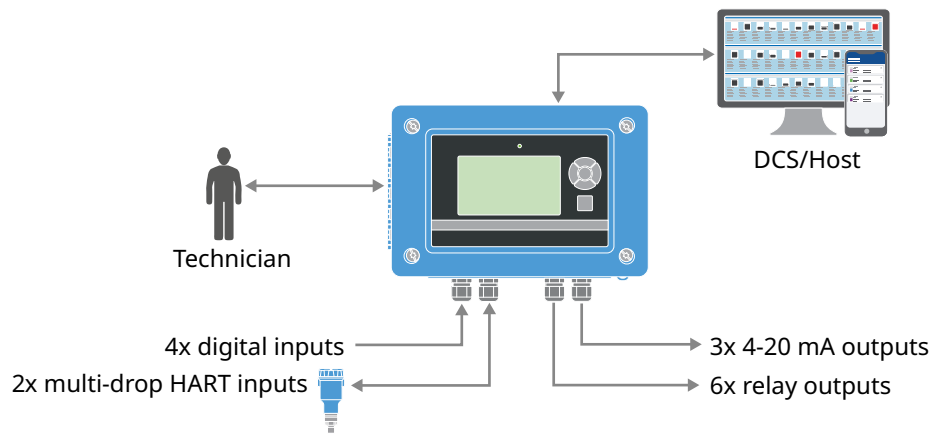
When designing a system it is important to take into consideration where the Rosemount 2405 is to be installed. This in order to ensure proper security measures are implemented in a correct manner and continuously followed. If identified security measures are not implemented and followed correctly the device could be exposed to risk. To achieve sufficient security and further protect the device once in use, the customer is encouraged to use a defense-in-depth approach.

The following examples of measures should be considered for increased protection of the Rosemount 2405:

- Operating environments should have access control and appropriate surveillance.
- Access to the system should only be permitted by authorized personnel.
- Operating personnel should receive training and instructions on how to securely use the product with special consideration taken to identified risks.
- The defense-in-depth principle is applied in the environment where the Rosemount 2405 is installed.



Figure 2-1: Rosemount 2405 Interfaces





## 3 Commissioning

### 3.1 General information

This section includes information regarding installation and configuration of the Rosemount 2405 Monitoring Hub.

### 3.2 Installation

During installation of the Rosemount 2405, follow the steps provided in the Quick Start Guide. To limit the risk of tampering ensure the device is properly mounted and be aware of any potential risks regarding physical access. It is expected that the customer will properly physically secure the device and that any access to device is limited and secure.

The personnel performing the installation must have relevant qualifications required for this task, including the following:

- Authorized by the relevant authority
- Understand specific federal and/or national regulations
- Prior to installation, having read and understood all the relevant instructions
- Must follow the instructions and comply with all general policies and recommendations

### 3.3 Configuration

Refer to Rosemount 2405 Reference Manual for information on configuration. After configuration it is recommended to:

- Change passwords for web interface
- Change pin code
- Configure the Rosemount 2405 with the correct date, time and time zone, to ensure valid timestamps in all audit logs.
- Customize HART®-IP remote access
- Customize Modbus® TCP remote access
- Customize the local display authorization information message to ensure compliance with applicable local regulations and system requirements
- Save a backup of the configuration

#### 3.3.1 Certificate

Use encrypted communication protocols for remote access and configuration. The device uses TLS with certificates that need to be installed on the client machine in order to avoid security warnings in the web browser.

#### Add the certificate to your Certificate Authority (CA) store

##### Procedure

1. Enter the monitoring hub's IP address into your web browser.

2. Select the **Not Secure** icon in the address bar.
3. Select **Certificate details** (or similar).
4. In the **Certificate Viewer**, select the **Details** tab.
5. Select the Server certificate (not the IP address/device certificate) that is named **Rosemount 2405 Monitoring Hub**.
6. Select **Export** or **Copy to File** (depends on OS).
7. Select Base64 (.cer) or DER (.crt) format.
8. Save the file.
9. Install the downloaded root certificate into your operating system's store of trusted root certification authorities.
10. Restart the browser to enable loading of the certificate into the browser and go to the login page for Rosemount 2405 Monitoring Hub.

## Add custom certificate

This feature allows administrators to configure the device to use the customer's own certificate chain, integrating with their existing network infrastructure, trust chain, and company policies. Administrators can upload a custom private key and corresponding certificate via the web interface.

### Prerequisites

You have a generated private key and a certificate signed according to your organization's chain of trust. The certificate must use a 1024-bit RSA key. The certificate file and the corresponding key file must be in either .pem or .crt format.

### Procedure

1. Log on to the web interface as administrator.
2. Select **Settings** → **Security** → **Certificates**.
3. Select the **Select certificate file** button.
  - a) Browse to the certificate file and select **Open**.
4. Select the **Select key file** button.
  - a) Browse to the key file and select **Open**.
5. Select the **Upload certificate** button.

### Postrequisites

Custom certificate can be removed and replaced with default self-signed certificate from a PIN code-protected menu on the local display.

## 4 Operation

### 4.1 General information

This section includes information regarding secure operation of the Rosemount 2405. It contains requirements for the operating personnel and how to perform secure maintenance on the system (e.g., how to update and install security related software updates).

The personnel responsible for operations should have relevant qualifications needed for this task, including the following:

- Authorized by the relevant authority
- Understand specific federal and/or national regulations
- Prior to installation, having read and understood all the relevant instructions
- Must follow the instructions and comply with all general policies and recommendations

### 4.2 Backup and restore

The web interface provides the functionality to take a backup of the current Rosemount 2405 configuration. In the event of a disruption or failure, configuration recovery is supported. The Rosemount 2405 can be restored to a known previous state by reloading all configuration settings from a backup file. Store the back-up securely according to local organizational and regulatory guidelines.

Refer to the Reference Manual for instructions on how to create a backup file, and to restore system configuration.

### 4.3 Audit log

The web interface provides an audit log that logs actions performed in the system. As a system administrator these logs can be reviewed to identify malicious use and to provide the property of non-repudiation on operation critical tasks. It is recommended to regularly review audit logs. Refer to the Reference Manual on how to view and download audit log file.

The following types of events are recorded in the audit log:

- **Access control event** indicates an event related to access permissions or authentication attempts within the system.
- **Configuration change event** denotes any modifications made to the system's configuration, including updates to settings or parameters, backup and restore operations, tank alarm configurations, and any changes that affect values in the holding register.
- **Audit log event** refers to any event that does not fit into the previous categories. This includes reset events, password and PIN changes, demo mode activations and deactivations, as well as event log circular buffer reset to the first index.

## 4.4 Security incident reporting

You are encouraged to report any suspicious activity or security incidents regarding the product to Emerson. See [Report product vulnerability](#) for instructions.

Security notifications for your Emerson product can be found on [Emerson.com/support/security-notifications](https://emerson.com/support/security-notifications).

### 4.4.1 Report product vulnerability

In case you encounter a security incident with your Emerson product you may report it by submitting a form to Emerson Product Security Incident Response Team.

#### Procedure

1. Open a web browser and navigate to [Emerson.com](https://emerson.com).
2. Scroll down to the bottom of the web page.
3. Locate and select [Report a vulnerability](#).
4. Fill in the form and submit when done.

## 4.5 Security update management

Software updates are critical when it comes to ensuring the system functionality and security. If the device software is not kept up to date, there is a risk that the device is exposed to vulnerabilities that arise over time. It is therefore important to maintain the management of new software updates.

Apply security patches and updates as they are released. Please contact your local Emerson representative for more information on security patches and updates.

Firmware upgrade shall be done by administrators via web interface. Administrators shall use the official firmware file and update the system unit via the web interface. When update is completed the administrator shall verify the update version by checking the about page firmware version. Firmware files used for upgrades are encrypted to protect their integrity.

Failure to update the system may leave the product vulnerable to known security threats. Regularly check for new updates and apply them as recommended in the product documentation. Subscribe to notifications from Emerson about new updates. Refer to the Reference Manual on how to update firmware using the web interface.

## 4.6 Application user privilege levels

The web interface is protected via password-based sign-in for both operator and administrator roles. One account available for each role. The Rosemount 2405 local display is protected via login using a PIN code for configuration sensitive menus accessible only for administrators.

**Table 4-1: Configuration**

| Function                    | Local display     | Web interface |               |
|-----------------------------|-------------------|---------------|---------------|
|                             | PIN code required | Operator      | Administrator |
| Search and add HART sensors | Yes               | No            | No            |
| Configure HART sensors      | Yes               | No            | Yes           |

**Table 4-1: Configuration (continued)**

| Function                                                          | Local display     | Web interface |               |
|-------------------------------------------------------------------|-------------------|---------------|---------------|
|                                                                   | PIN code required | Operator      | Administrator |
| Configure tanks                                                   | Yes               | No            | Yes           |
| Configure analog outputs, digital inputs, relays, and tank alarms | Yes               | No            | Yes           |
| Configure Tank Card setup                                         | No                | No            | No            |

**Table 4-2: Monitoring/status**

| Function                                                      | Local display     | Web interface |               |
|---------------------------------------------------------------|-------------------|---------------|---------------|
|                                                               | PIN code required | Operator      | Administrator |
| Monitor tanks                                                 | No                | Yes           | Yes           |
| View tank log graphs                                          | No                | Yes           | Yes           |
| Status of monitoring hub                                      | No                | Yes           | Yes           |
| Status of sensors, analog outputs, digital inputs, and relays | No                | Yes           | Yes           |
| Failure alarms table                                          | N/A               | Yes           | Yes           |
| Tank alarms table                                             | N/A               | Yes           | Yes           |

**Table 4-3: Settings**

| Function                 | Local display     | Web interface |               |
|--------------------------|-------------------|---------------|---------------|
|                          | PIN code required | Operator      | Administrator |
| Date and time settings   | Yes               | No            | Yes           |
| Display settings         | Yes               | No            | No            |
| IP settings              | Yes               | No            | No            |
| Security settings        | Yes               | No            | No            |
| Remote services settings | Yes               | No            | No            |
| System units settings    | No                | Yes           | Yes           |

**Table 4-4: Service**

| Function                                                         | Local display     | Web interface |               |
|------------------------------------------------------------------|-------------------|---------------|---------------|
|                                                                  | PIN code required | Operator      | Administrator |
| Info and status of monitoring hub                                | No                | Yes           | Yes           |
| Status of sensors, analog outputs, digital inputs, and relays    | No                | No            | Yes           |
| Factory reset                                                    | Yes               | No            | No            |
| Tank log reset, Field calibration reset, and Failure alarm reset | Yes               | No            | No            |
| Activate demo mode and configure sensor value simulations        | Yes               | No            | No            |
| Analog output field calibration                                  | Yes               | No            | No            |

**Table 4-4: Service (continued)**

| Function           | Local display     | Web interface |               |
|--------------------|-------------------|---------------|---------------|
|                    | PIN code required | Operator      | Administrator |
| Download data logs | N/A               | No            | Yes           |
| Upgrade firmware   | N/A               | No            | Yes           |

### 4.6.1 Inactivity timeout

Users logged into PIN code-protected menus on the local display and web interface will be automatically logged out after 5 minutes of inactivity.

Users are locked out for 1 minute after attempting to sign in using invalid passwords for a configurable number of times.

### 4.6.2 Reset web interface passwords

Web interface passwords can be reset to factory defaults from a PIN code-protected menu on the local display.



## 5 Decommissioning

This section includes information regarding securely decommissioning the Rosemount 2405 at the end of its life. This is performed to ensure that data e.g., intellectual property is not left in the system in a way that it can be unlawfully retrieved. The following instructions outline how to securely wipe data, revoke credentials, and properly dispose of the product to mitigate security risks. Example to include removing the static IP configuration from the network and system integration/device in the installation environment.

### 5.1 General information

Decommissioning, or removing the product from use, is a critical step in its lifecycle from a security perspective. There are several key reasons why secure decommissioning is necessary in the product security context:

- Data stored inside the product must be securely erased to prevent unauthorized access and information disclosure.
- The product could be repurposed in an insecure or unintended manner, posing a risk to user safety and system integrity.
- Proper decommissioning ensures compliance with industry standards and legal requirements.

### 5.2 Decommissioning the Rosemount 2405

#### Pre-decommissioning

Identify and document network dependencies and connected sensors. Disconnect sensors and remove the device from lists in integration system and network. Where needed blacklist the IP or re-assign it to new device. System integrators may want to run back-up of state of the device via the web interface by using the back-up option as well downloading the tank, event, and audit logs before running factory reset. Store the back-up securely according to local organizational and regulatory guidelines.

#### Decommissioning

- Disconnect device from network.
- Run a factory reset in order to erase any files/logs and configuration.
- Where necessary and if certificates are used, revoke the certificates used by the device and remove any certificates already installed in system integration devices.
- Power off the device.

#### Post decommissioning

If reusing the device ensure the device is updated to the latest firmware version.

Permanent decommissioning should include shredding and physically destroying the flash memory and following the NIST 800-88 e-waste disposal standards.

For more information: [Emerson.com/global](https://emerson.com/global)

©2025 Emerson. All rights reserved.

Emerson Terms and Conditions of Sale are available upon request. The Emerson logo is a trademark and service mark of Emerson Electric Co. Rosemount is a mark of one of the Emerson family of companies. All other marks are the property of their respective owners.

**ROSEMOUNT™**

