ABB MEASUREMENT & ANALYTICS | 2106521MNAB

MQTT Configuration Guide

RMC-100

Additional information

Additional free publications are available for download at www.abb.com/upstream.

Table 0-1: Related documents

Document	Document number
Digital Oilfield User Manual	2106300
MQTT Data Interpretation Code Guide	2107649 (request from product manager)
RMC-100 Startup Guide	2105551

Cyber security

Products with embedded Message Queue Telemetry Transport (MQTT) capability are designed to be connected, and communicate information and data, via a network interface. All ABB Totalflow products should be connected to a secure network. It is the customer's sole responsibility to provide and continuously ensure a secure connection between the product and the customer network or any other network (as the case may be). The customer shall establish and maintain appropriate measures (such as, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, or installation of antivirus programs) to protect this product, the network, its system and interfaces against any kind of security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information. ABB Inc. and its affiliates are not liable for damages and/or losses related to such security breaches, any unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates that it releases, the customer should institute their own testing program for any product updates or other major system updates (to include, but not limited to, code changes, configuration file changes, third party software updates or patches, hardware change out) to ensure that the security measures that the customer has implemented have not been compromised and that system functionality in the customer's environment is as expected.

Malware prevention

Recommendation: As with any downloaded software, scan ABB embedded software packages using a malware prevention solution.

Contents

1 Overview

This guide provides basic steps to enable an ABB Totalflow device for connection to an MQTT broker/server on a private network. ABB Totalflow devices support Standard MQTT and Sparkplug protocols. Consult with your system administrator for specific requirements and configuration based on your implementation.

NOTICE – Cybersecurity risk: MQTT-enabled Totalflow devices are not designed to connect directly to the Internet. ABB strongly recommends that the devices connect to MQTT brokers through an Edge gateway and firewall-protected corporate network.

1.1 Implementation components

Table 1-1 shows the major high-level components of implementations supporting MQTT communication with ABB Totalflow devices:

Table 1-1: Major components required for MQTT support

Location	Components	Description
Field site /well pad	Flow measurement or control devices with embedded MQTT support	Typically, a remote controller such as the RMC-100. Embedded MQTT support consists of: — MQTT functionality (standard protocol stack as part of the software): An MQTT-enabled device performs the role of the MQTT client. It requests and establishes connection with an MQTT broker. — MQTT device configuration interface: The device flash implements a REST server to support local or remote web-browser-based access to configure its MQTT functionality.
Customer system/client	Web browser user interface	Web-based client (for local and remote access). It supports: Access to the device configuration interface (REST server) to configure the MQTT functionality and enable applications for data publishing. This interface supports only MQTT-related configuration. You must use PCCU for application-specific configuration.
	PCCU user interface	Existing host-based interface to the ABB Totalflow device family (for local and remote access). It supports: — Full device configuration and operations. All applications for which data will be published on an MQTT broker must be configured from PCCU. — Enabling or disabling the MQTT client services on a device — Enabling or disabling the REST services on a device
Customer private network (across WAN)	MQTT Broker	The MQTT broker performs the role of the MQTT server. It enables secure MQTT-protocol-based connection of field devices to a private customer wide area network. The successful device-MQTT broker connection allows the device to send (publish) data to the MQTT broker. **Note**: On a private customer network, customers must install and configure their own broker and integrate it with their data collection/management systems.

IMPORTANT NOTE: This document assumes that a broker is already available and ready for device connection requests. Installation, configuration, and integration of private brokers is beyond the scope of the document.

2 MQTT-enabled ABB Totalflow device

2.1 MQTT functionality (MQTT Service)

MQTT-enabled devices support standards-based operation and connection with MQTT brokers. They also provide an interface for the configuration of MQTT parameters and the selection of the application data that the device publishes on an MQTT broker.

- To review the basic operation of communication protocols supported by ABB Totalflow, see section 2.1.1 Standard MQTT functionality or section 2.1.2 Sparkplug functionality.
- To review the configuration interface, see section 2.1.3 MQTT configuration interface (REST service).

NOTICE – Cybersecurity risk. The following sections assume that the device-MQTT broker connection is established through the customer's corporate private network, (not through the internet). It is assumed that the corporate network provides connections through an edge gateway and has firewall-protected access for remote users. ABB Totalflow devices must not be connected directly to the Internet. See additional security topics in the RMC User Manual.

2.1.1 Standard MQTT functionality

ABB Totalflow MQTT-enabled field devices act as MQTT clients. The MQTT protocol stack in the device's embedded software implements this functionality to allow connection to a broker which acts as an MQTT server. It performs the connection setup, connection/session maintenance, and the data exchange between the client and the broker.

The MQTT protocol defines several message or packet types exchanged by the client and server for different purposes. Packet payloads are aligned with the ABB Ability information model. This section provides a basic review of embedded MQTT functionality.

IMPORTANT NOTE: The ABB Totalflow MQTT stack implementation is standards compliant. The following sections provide a basic description of the MQTT functionality to provide background for MQTT parameter configuration or to understand error messages during troubleshooting. For a more detailed explanation of the MQTT protocol, refer to online resources for the MQTT standard documentation at http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf. Also see section 11 Useful terms for basic terminology descriptions. **If you are familiar with the MQTT standard and its principles of operation, skip this section and proceed to section** 4 Prepare for configuration.

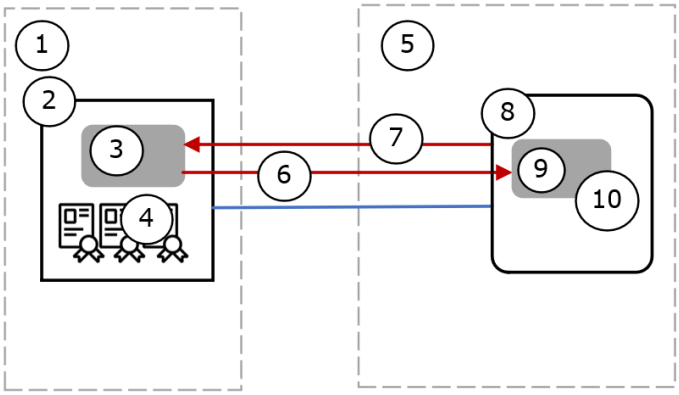
IMPORTANT NOTE: For simplicity, the diagrams in the following sections show the MQTT functionality and data flow for a single device only. Actual implementations support many devices located across different field sites. The scale of the implementation depends on the customer's specifics, but the basic principles of operation apply to all ABB Totalflow devices with MQTT support.

2.1.1.1 Connect

Figure 2-1 shows a simplified view of the connection setup between the device and the MQTT broker. The device initiates communication with the broker. As an MQTT client, the ABB Totalflow device (2):

- Sends a connection request (6) to the MQTT broker (8).
  - The request must contain required protocol details (user-configurable parameters that must be compatible with the broker specification/configuration).
  - The request must present valid authentication details such as valid credentials or certificates. When using certificates, they must reside on the device (4) and must be valid.
- Establishes a secure (encrypted) TCP/IP connection with the broker after the broker authenticates certificates or credentials and grants the request (7).
- Maintains the connection with the broker to ensure the device is always visible to operators for monitoring, data collection or configuring as necessary.

Figure 2-1: MQTT device-broker connection (customer private network)



Legend for Figure 2-1: MQTT Device-Broker connection (customer private network)

ID	Field device on site	ID	Data flow	ID	Customer private network
1	Field Local Area Network	**6**	Request for connection	**5**	Corporate network
2	Totalflow device (RMC)	**7**	Connection granted from broker	**8**	MQTT broker
3	MQTT client functionality			**9**	MQTT server functionality
4	Authentication certificates/credentials			**10**	MQTT broker verification of certificates/credentials for connection

IMPORTANT NOTE: The device's MQTT implementation is designed to automatically re-establish connection to the broker in the event of a restart, network failure, or disconnection.

2.1.1.2 Subscribe

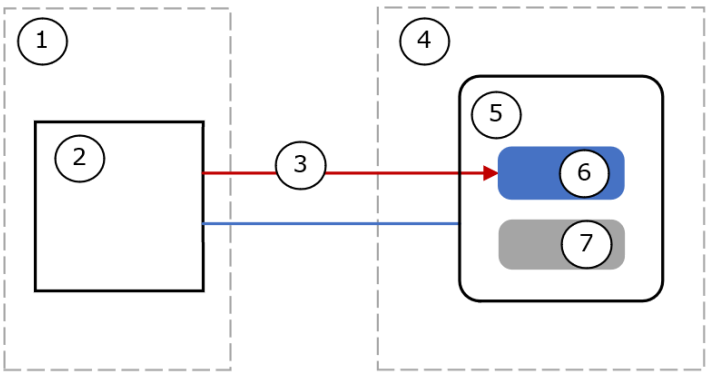
Figure 2-2 shows a simplified view of the device subscription to the broker (5). The device subscribes to the subscription topic (6) on the broker to support device parameter updates (See section 2.1.1.3 Update (register-write).

The subscription topic identifies each device with its unique ID. Unique IDs allow the broker to filter and distribute update requests to the correct device.

IMPORTANT NOTE: Each device subscribes to the following topic:

/devices/<Device-ID>/messages/devicebound/+.

Figure 2-2: Device subscription (customer private network)



Legend for Figure 2-2: Device subscription (customer private network)

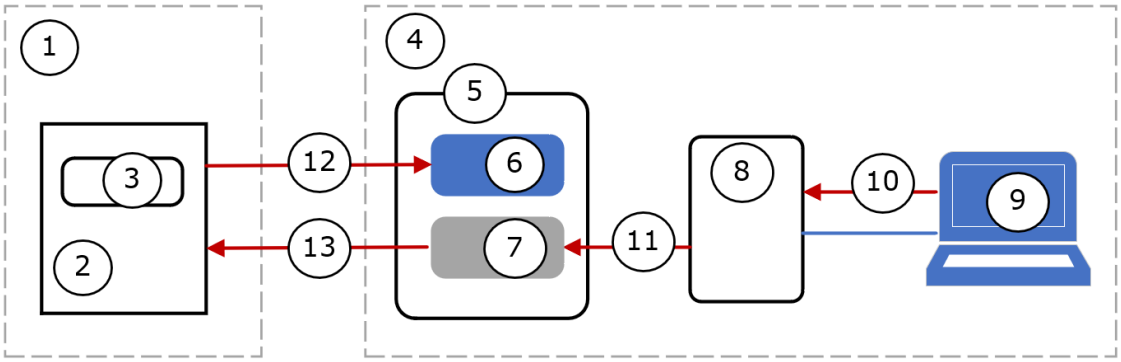
ID	Field device on site	ID	Customer private network
1	Field Local Area Network	**4**	Corporate network
2	Totalflow device (unique ID)	**5**	MQTT broker
3	Subscribe to topic on broker	**6**	Device subscription topic
		7	Device publish topic

2.1.1.3 Update (register-write)

Figure 2-3 shows a simplified view of how a parameter update submitted from client application is handled across a private network. The device must be subscribed to receive update requests from the broker (See 2.1.1.2 Subscribe). Users (9) may submit application parameter update requests (10) to the device through the broker (5). These requests are recorded (published) on the broker as write-to-register commands which must be performed by the device:

- The broker publishes the command on the device topic (7) and forwards (13) a message to the device (2)
- The device receives the message with the write-to-register command from the broker.
- The device updates the value of the indicated register(s) (3).
- The device publishes (12) the data to reflect the change. See section 2.1.1.4 for details on the publish process.

Figure 2-3 Parameter update (customer private network)



Legend for Figure 2-3: Parameter update (Customer private network)

ID	Field device	ID	Customer private network	ID	Data flow
1	Field Local Area Network	**4**	Corporate network	**10**	Parameter initiates update request from customer end system (User Interface)
2	Totalflow device	**5**	MQTT broker	**11**	Client application submits parameter change to broker
3	Totalflow device application data (register data or records)	**6**	Device subscription topic	**13**	Broker sends the parameter change message to the device. Device updates the parameter value
		7	Device publish topic	**12**	Device publishes updated parameter value back to broker
		8	Proprietary Customer application		
		9	User end system (user interface)		

2.1.1.4 Publish

Table 2-1 describes the type of data that ABB Totalflow devices publish for each of the applications supported. See Section 3 Supported applications for data publishing for more details.

Table 2-1: Data published

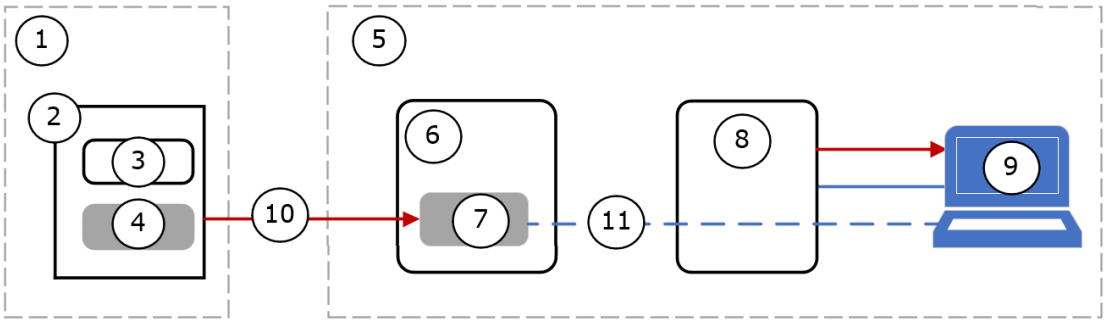
Data type	Description
Application records or Snapshot data	General device or application information sent by the device at first-time boot or after reboot. It includes information about: — Device resources, etc. — Enabled registers (registers the device publishes data for) — Various records (also referred to as snapshot data) such as Alarm, Trend, Daily Logs, Custom Logs and Events
Application register data	Specific application register values for the Totalflow applications supported on the cloud.

Figure 2-4 shows a simplified view of how the device publishes its data:

— The device (2) sends a publish message (10) with its data to the MQTT broker (6). The device data on the publish topic (7) is identified by unique device ID.
— If devices connect to a private network, the storage of the data depends on the specific implementation and how each component is integrated. A proprietary application with MQTT client functionality (8) can be used to fetch the required data to keep data displayed up to date for view by customer end points or stations (9). It is assumed customers will have the required database support for data storage.

IMPORTANT NOTE: The publish topic (7) is used by the broker to send data updates to the client applications. Each device publishes its data on its corresponding device ID topic: /devices/<Device-ID>/messages/events/.

Figure 2-4: Data Publish (Customer private network)



Legend for Figure 2-4: Data publish (customer private network)

ID	Remote site	ID	Customer private network	ID	Data flow
1	Field Local Area Network	**5**	Corporate network	**10**	Device publishes data to broker on device topic
2	Totalflow device (RMC with unique device ID)	**6**	MQTT broker	**11**	Broker notification to MQTT client. Client updates data and end user sees latest data.
3	Totalflow device application data (register data or records)	**7**	Publish topic		
4	Unique device ID	**8**	Proprietary customer application with MQTT client functionality		
		9	End user system (user interface)		

2.1.2 Sparkplug functionality

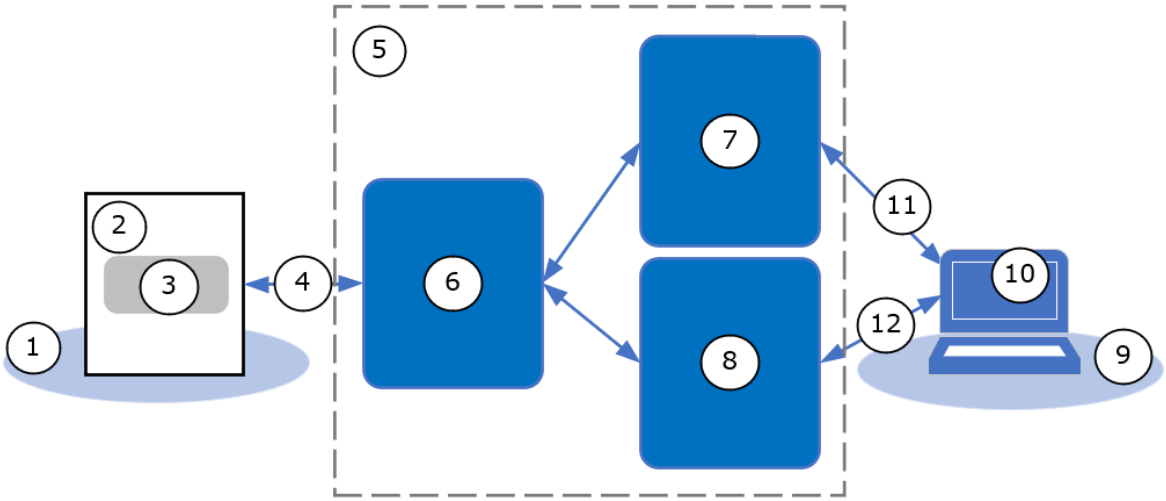
MQTT-enabled devices support Sparkplug B to connect to SCADA or IIoT systems. Sparkplug enhances the standard MQTT protocol to better support the real-time requirements of these systems.

IMPORTANT NOTE: The implementation of the SCADA or IIoT system depends on specific customer requirements and available network topologies. Customers that implement end-to-end solutions on their own private networks manage their own MQTT broker/server. Details on components for different scenarios are beyond the scope of this document. For additional details on the Sparkplug specification, see the following link: https://docs.chariot.io/display/CLD/Sparkplug+Specification.

Figure 2-5 shows a simplified diagram of the functional blocks of a sample Sparkplug architecture implemented on a corporate network (5). The SCADA or IIoT system (7), and the MQTT server are installed at the customer network. The MQTT broker (6) is the intermediary for MQTT communication between the device (2) and the SCADA system applications (7, 8).

When Sparkplug is selected as the device's protocol for connecting with the MQTT broker, the device establishes an MQTT connection (4) and performs both the MQTT device and Edge of Node functionality, as per the Sparkplug specification. As an Edge of Node (EoN), the device supports the Sparkplug session management, topic name space, and payload definitions. This additional support enhances communication and provides better support for real-time data. Sparkplug message payload from the device reflects both roles: the device and Edge of Node roles. For details on monitored Sparkplug packets, see the Sparkplug Statistics section in the Digital Oilfield User Manual (see link in Additional information).

Figure 2-5: Sparkplug high level architecture



Legend for Figure 2-5: Sparkplug high level architecture

ID	Field site	ID	Customer network	ID	Customer access
1	Field Local Area Network	**5**	Customer corporate network (VPN)	**9**	Field office network with secure access
2	Totalflow device	**6**	MQTT broker (server/distributor)	**10**	Client system: PC/Laptop with browser as client to SCADA/IIoT application
3	MQTT client and Sparkplug Device/Edge of Node (EoN) functionality	**7**	SCADA/IIoT Host (Primary Application)	**11**	Connection to primary application
4	MQTT connection	**8**	Other backend application (non-primary SCADA/IIoT client application)	**12**	Connection to other backend application

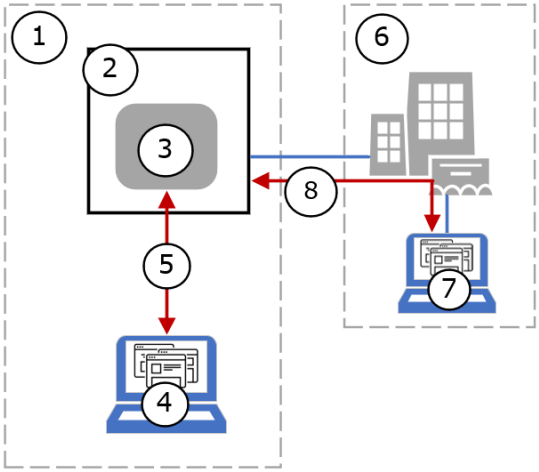
IMPORTANT NOTE: For simplicity, Figure 2-5 does not show any databases or other services. Databases are typically implemented on-premise for data storage. Customer implementations are proprietary and specific to their systems and requirements.

IMPORTANT NOTE: MQTT servers supporting Sparkplug must be MQTT v3.1.1 compliant. MQTT servers may be referred to by other names, depending on the vendor implementing them. This manual uses the generic term "server" to indicate the main functionality or role of this component in the overall architecture. For details, consult your vendor documentation and architectures.

2.1.3 MQTT configuration interface (REST service)

Totalflow devices provide a user interface specifically implemented for the MQTT configuration. The interface is a REST server which services web-browser-based client connections. Figure 2-6 illustrates two clients (4 and 7) with local and remote access to the field device. Devices require a valid IP address and a network connection to be accessible to clients on local sites (1) or across the corporate network (6). When clients establish connection with the device (5, 8), they can navigate through the configuration web pages and configure or update the MQTT parameters.

Figure 2-6: Device user interface for MQTT operation



Legend for Figure 2-6: Device user interface for MQTT operation

ID	Local configuration	ID	Customer private network
1	Field Local Area Network	**6**	Corporate network
2	Totalflow device	**7**	Client system: remote configuration
3	Device REST interface (web configuration pages)	**8**	Connection for remote configuration (device must have correct IP address in the field)
4	Client system: PC/laptop with browser		
5	Connection for local configuration		

2.1.3.1 Supported browser

The Chrome browser provides access to the device's MQTT configuration web pages. See the versions supported in Table 2-2.

IMPORTANT NOTE: The configuration interface supports only the MQTT configuration (MQTT communication parameter setup, enable publishing for selected application, and register data). For all other device configuration, use PCCU.

Table 2-2: Supported web browser on configuration interface

Browser	Version
Chrome browser	49 or higher

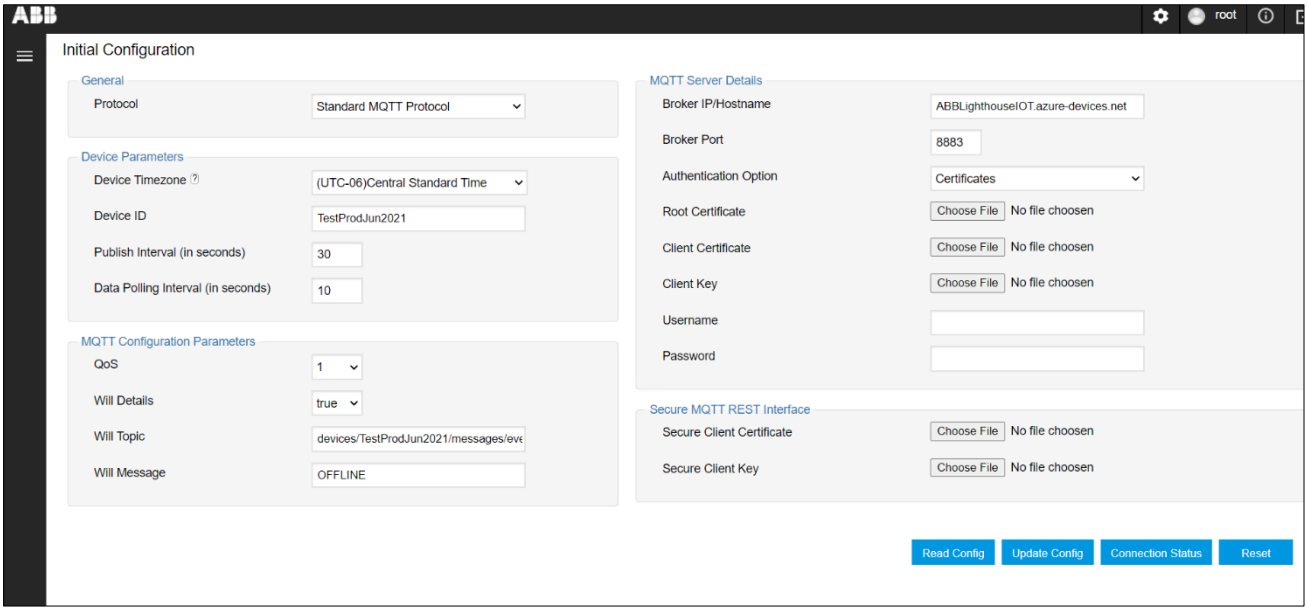
2.1.3.2 Initial Configuration page

The Initial Configuration web page provides the ability to set up the connection and communication with the MQTT broker.

Figure 2-7 shows the initial configuration web page with several parameter categories and function buttons to view, update, verify connection, and reset configuration:

- Read config: retrieves and displays the current configuration stored in the device
- Update Config: saves new configuration in the device after parameter update
- Connection Status: verifies if the connection is successful for the configured parameters
- Reset: overwrites the current configuration with factory defaults

Figure 2-7: Initial configuration web page



2.1.3.3 Application Configuration page

The Application Configuration web page provides the ability to enable or disable the application and instance data publishing.

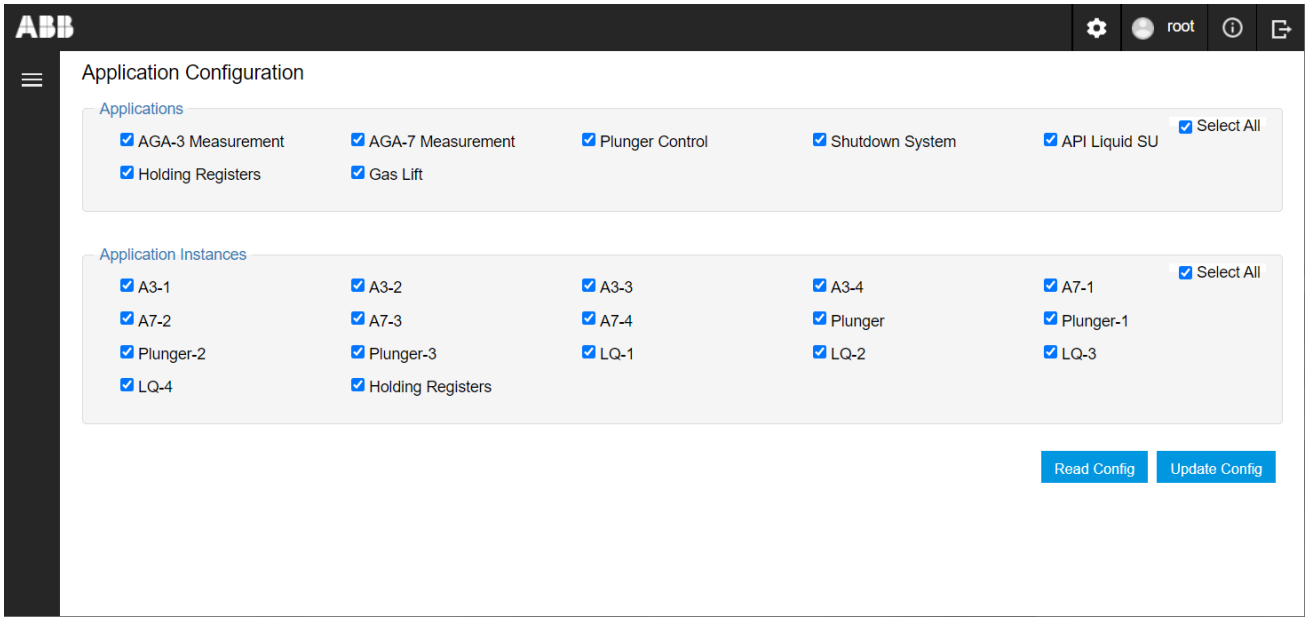
Figure 2-8 shows the Application Configuration web page with the list of applications and application instances configured in the field device. Use checkboxes to configure preferences:

- Check **Select All** to publish data for all application and application instances shown in the list.
- Check an individual application or instance to enable the device to publish that data.
- Clear an individual application or instance to disable the device from publishing that data.

Function buttons are available to view and update configuration:

- Read Config: retrieves and displays the current applications and instances and their setting for data publishing
- Update Config: saves new data publishing settings for the current application and instances after updates

Figure 2-8: Application Configuration web page



IMPORTANT NOTE: The Applications section in the Application Configuration page displays the applications supported by the cloud interface, even if not instantiated. The Application Instances section displays only those instances instantiated from PCCU.

2.1.3.4 Register Configuration page

The Register Configuration web page provides the ability to enable or disable application and instance-specific register data publishing.

Figure 2-9 shows the Register Configuration web page. The page displays the register list for the selected application and specific instance. The first application and its first instance are selected by default. Select the application and instances of interest to view other registers.

The page automatically classifies and displays the registers in categories. These categories might vary based on the application type. For example, for measurement applications, register options are organized in categories such as aggregate, application, and composition registers. These register categories might combine parameters available across different tabs in PCCU or reflect the same parameters as the PCCU tabs.

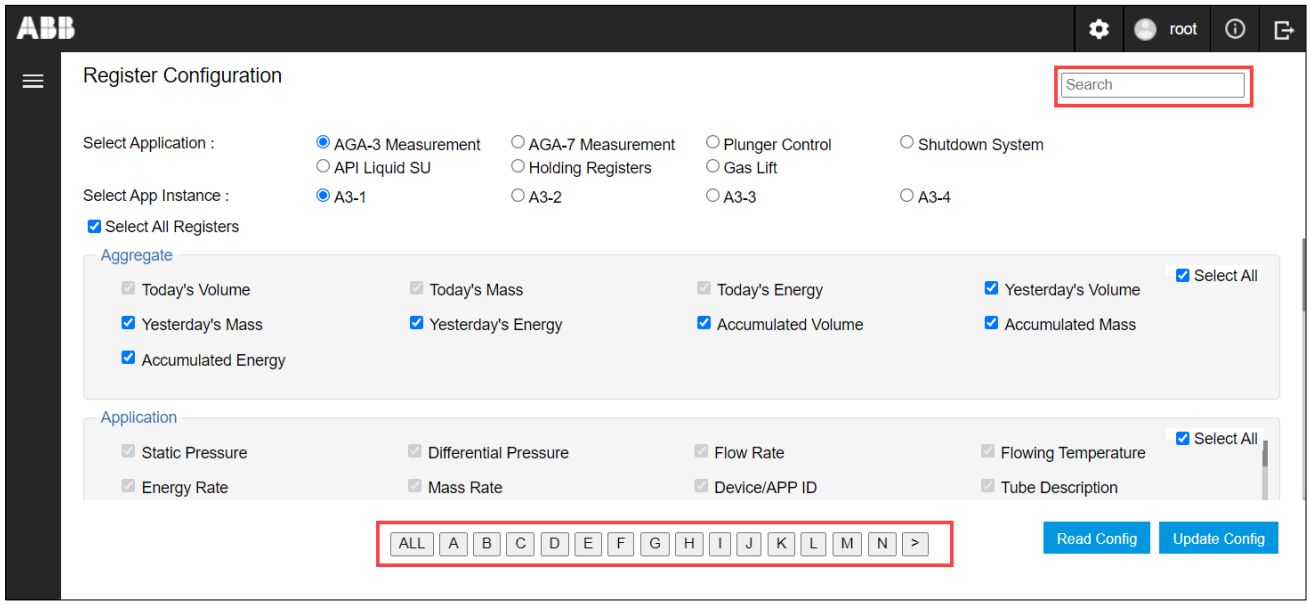
Options to configure register data publishing:

- Select the application and the app instance of interest to display the specific register list.
- Check **Select All Registers** to publish data for all registers for the selected application and instance or select the individual required registers.
- Use Search to configure specific registers or the pagination buttons at the bottom of the screen to see registers per alphabetical order. The screen also has a scroll bar to navigate while searching for specific registers.

Function buttons are available to view and update configuration:

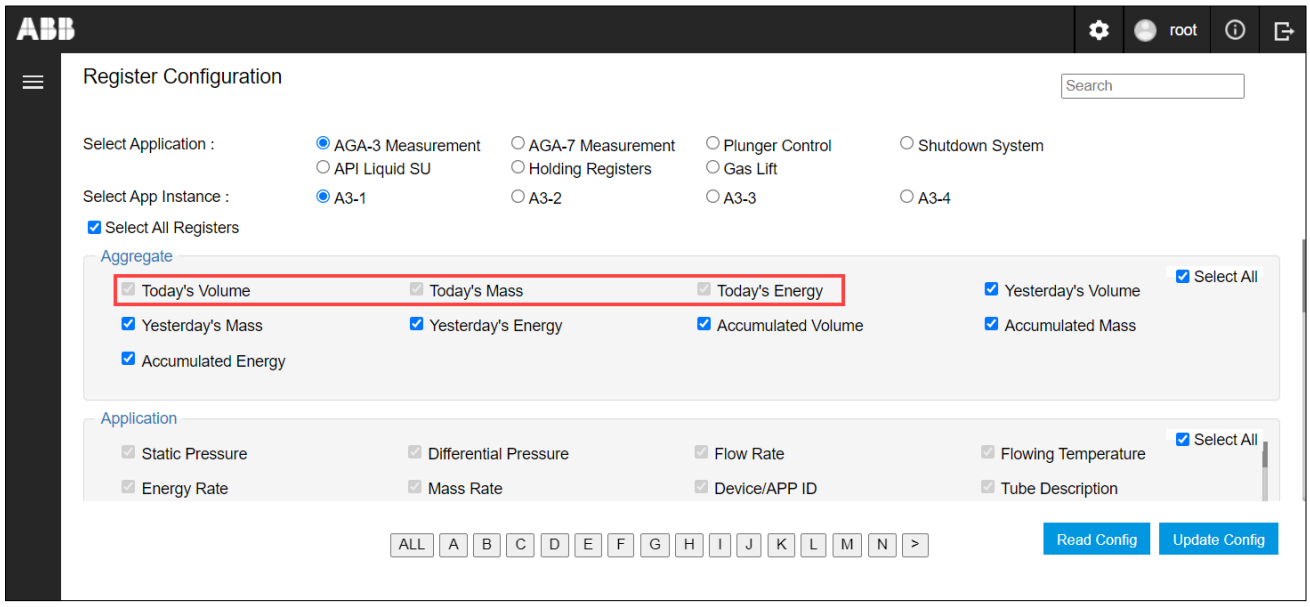
- Read Config: retrieves and displays current register selections for publishing
- Update Config: saves new register selections for publishing after updates

Figure 2-9: Register configuration web page



IMPORTANT NOTE: Some of the registers on the register configuration page are required and will always be enabled. The configuration interface does not allow users to disable the publishing of those registers. Required registers display grayed-out check boxes (See highlighted examples in Figure 2-10).

Figure 2-10: Required registers examples (read-only)



3 Supported applications for data publishing

Table 3-1 lists the ABB Totalflow applications that users can enable to publish data on an MQTT broker. To access data for these applications, they must be fully configured from PCCU and then selected from the device MQTT configuration interface.

IMPORTANT NOTE: The Alarm System and Trend System applications are not listed in the Application configuration web page (see section 8 Configure applications). Alarm data and trends are automatically published for all supported applications if defined and configured from PCCU.

Table 3-1: Totalflow applications supporting publishing

Application	Description	Use
Alarm system	Alarm detection, logging, and reporting application	Obtain or display alarms and alarm definition data.
Trend system	Data trending application	Obtain or display trend definition data. Defined trend variables can be used to generate graphical displays.
Holding Registers	Holding Registers allow the user to custom define how to store values of interest in specific device register ranges. This application is customized per user requirements. The registers are not pre-defined.	Obtain or display data from selected register ranges. Data stored is defined by the user, therefore displayed data depends on user-selections (custom). The holding register applications can be configured for publishing on a broker, but at the time of this writing is not supported on the ABB Digital Oilfield cloud application. Holding register data can be obtained from the broker, but customers must develop their own application to retrieve it. **Note**: If you are connected to any service provider cloud (or the Internet), you must disable this application prior to attempting connection to service.
AGA3	Orifice gas measurement application	Obtain or display data
AGA7	Linear gas measurement application	Obtain or display data
API Liquid SU	Linear liquid measurement	Obtain or display data
Plunger control	Control of a plunger on a production well	Obtain or display data It provides some basic control also. The level of control functionality depends on the customer implementation.
Gas lift	Artificial lift for wells with liquid loading problems	Obtain or display data
Shutdown System	Shut down a well or site	Obtain or display data

4 Prepare for configuration

This section describes device configuration requirements for connection and data publishing on the MQTT broker. Review requirements and associated tasks prior to configuration.

First time MQTT connection of an in-service device requires device restart. Follow your company guidelines to schedule configuration of in-service devices. Obtain required parameters from your administrator prior to configuration.

IMPORTANT NOTE: ABB Totalflow application configuration is beyond the scope of this manual. This document assumes the application configuration is complete and operational in existing devices. For new installations, first instantiate, then enable, and last configure applications from PCCU.

IMPORTANT NOTE: This document assumes that the MQTT broker on the customer private network is already configured and available for connection. Full device configuration requires a successful device-broker connection.

4.1 Prerequisites for device

This section describes the minimum requirements to support device configuration. Table 4-1 lists requirements for the RMC-100 as an example. Review the requirement lists and their associated tasks.

Table 4-1: Prerequisites for RMC-100

Requirement	Description	Tasks
MQTT-ready device OS and flash	The device embedded software with the MQTT client functionality	— Obtain customer package 2105452-032 or later for the RMC-100. — Upgrade the device. See PCCU help files or refer to Additional information for links to the RMC-100 documentation. — Enable MQTT functionality on the device as described in section 6.
Valid IP configuration for cloud connection	IP configuration must include a valid IP address, subnet mask, and default gateway.	— Obtain valid IP configuration from your IT administrator if configuring a new device or an existing device without IP parameters assigned. — Configure the device's IP parameters (address, mask, and gateway) from PCCU.
Unique Device ID	Device ID, or name that uniquely identifies the ABB Totalflow device	— Use a naming convention that allows the unique identification of each field device. — Assign a unique ID to each device intended for connection to the MQTT broker. The device ID can be the same as the station ID assigned using PCCU, if it is unique.
Authentication certificates and keys	Files generated by third-party certificate or security key generators Optional for private network implementations	MQTT servers can support several authentication options. — Determine the authentication method — Generate or obtain certificate and authentication keys as necessary **Note:** The MQTT configuration interface also supports server authentication with usernames and passwords. If a private MQTT server is configured to authenticate connection requests with these credentials, then obtain the required credentials from the server administrator. Customers must configure their authentication methods in their MQTT server. If they choose to use certificates, they are solely responsible for certification generation and management.

4.2 Prerequisites for laptop used in configuration

Table 4-2 provides requirements for the laptop or PC used to configure the device. Review the requirement lists and their associated tasks.

Field device configuration for MQTT requires IP communication. Ensure that both the ABB Totalflow device and the system used to configure the device each have the required IP configuration for successful communication.

IMPORTANT NOTE: Access to the device from mobile devices is also supported. Access interfaces adapt their display to the type of mobile device.

Table 4-2: Configuration system (laptop) prerequisites

Requirement	Description	Task
Chrome browser	The Chrome browser provides access to the device's MQTT configuration web pages.	— Download and install Chrome internet browser (version 49 or later).
PCCU	PCCU is required to add, enable and fine-tune all Totalflow applications.	— Obtain and install PCCU 7.67 or later. — It is assumed all application configuration is complete prior to MQTT configuration. **Note**: PCCU 7.69, 7.69.1, 7.70, and 7.71 have been discontinued and are no longer supported. If you have these versions, obtain the latest PCCU version from the ABB library and upgrade.
Valid IP configuration	The MQTT configuration requires IP communication between the laptop and the device. The laptop's IP configuration must be compatible with the device's IP configuration.	— Obtain a valid IP address from the system administrator. — Configure the laptop with the valid IP address.

4.3 Prerequisites for authentication

Secure device-broker connection requires authentication. Authentication might require access credentials, public/private key pairs or security certificates depending on the authentication method or standard used. When using a private MQTT broker, it is the customer's responsibility to select the preferred authentication method and generate or manage certificates if this form of authentication is configured in their server.

4.3.1 Determine authentication methods

The ABB Totalflow device supports two types of authentication options:

— Authentication using valid username/password. The device embeds a valid username and password in its connection requests. The MQTT Broker verifies that the credentials match those provided and authorized for the customer.
— Authentication using the X.509 standard format. This standard defines the format of public key certificates used in the communication protocols for secure device-broker connections. There are two types of X.509 authentication:
  - Self-signed X.509 authentication uses a self-signed identity certificate.
  - Certification Authority (CA)-signed X.509 authentication uses a certificate signed by a third-party authority trusted by both the customer and the cloud service provider.

IMPORTANT NOTE: CA-signed X.509 certificates are preferred over self-signed certificates. Administrators must verify the service provider's policy and support to generate the appropriate certificates.

4.3.2 Prepare for authentication configuration

The authentication method is a required parameter for field configuration. Table 4-3 provides high level tasks to prepare for authentication configuration.

IMPORTANT NOTE: Customers are fully responsible for certificate management. Administrators must follow company policies and procedures to maintain and save certificates, keys, fingerprints, verification codes, usernames, and passwords in a safe location.

Table 4-3: Obtain authentication parameters

Requirement	Description	Tasks
Device ID	Name that uniquely identifies the device on the broker	— Define a unique name or ID based on your naming convention.

Requirement	Description	Tasks
		The ABB Totalflow device supports the definition of the Station ID. The device ID for the broker connection can match the Station ID if it is unique. To verify or obtain the station ID on an ABB Totalflow device already in operation, connect to the device with PCCU Entry mode.
Authentication method	Format used for validation of field devices before connection to the broker. The authentication method in both the device and the broker must match.	— Obtain the preferred method from the MQTT server administrator.
Username/ password	Credentials required by the MQTT broker to grant connection requests from field devices. These may be required in addition to certificates or be the sole authentication method.	— Obtain credentials from the MQTT server administrator.
Certificates, Keys	Required for X.509 authentication. Digital files with certificate, key and fingerprint that certify the device authenticity for acceptance by the broker. Optional for private MQTT servers.	— Obtain from MQTT server/system administrator the three required files for X.509 authentication. — Administrators must obtain the common Root Certificate (for all devices) — Administrators must obtain (or generate) the device-specific files: Client Certificate and Client Key. — Have certificate files available on the system the device is configured from. The certificate files must be copied to the device during configuration.

5 Device configuration overview

Review this section before device configuration. Enable MQTT and the configuration interface first. Then update the factory-default MQTT configuration to reflect specific device, connection, and authentication parameters. Connection verification is required at first-time configuration.

Use the Device Configuration User Interface to configure field devices. Through this interface, MQTT-enabled devices provide web pages with several configuration options.

A successful device-broker connection is required to complete all MQTT configuration. Follow the tasks listed in Table 5-1 in the presented order: Enable services, complete initial configuration parameters, and establish the device's connection with the broker. After successful device-broker connection, configure application and register data for publishing.

Table 5-1: Device configuration overview

Requirement	Description	Tasks
Enable MQTT and REST services	The MQTT functionality and configuration interface are disabled by default. They must be enabled to activate the MQTT function and the configuration interface.	— Follow procedures in section 6 Enable MQTT services on the device.
Initial configuration: device, connection, broker parameters	Parameters required for device-broker connection: unique device ID, broker identification and connection details, protocol.	— Follow procedures in 7 Initial configuration (Initial configuration page).

Requirement	Description	Tasks
Common and device-specific authentication credentials or certificates	For certificate-based authentication, the device must have certificates stored in its memory. Certificates generated for the device must be copied onto the device.	
Successful connection	The device is authenticated by the broker and its connection request granted. Required to complete device application and register configurations. These pages do not display until the connection is established.	— Ensure device is connected to the MQTT broker. See section 7.4 Verify device-broker connection status (Initial configuration page).
Application configuration	Select device applications and instances that the device will publish data for.	— Follow procedures in section 8 Configure applications (Application configuration page).
Register configuration	Select the specific application registers the device will publish data for.	— Follow procedures in section 9 Configure registers. (Register configuration page)

IMPORTANT NOTE: The instructions and screen captures included in this manual reflect access using laptops or PCs. Steps, screens, and navigation methods will vary for other mobile device types.

6 Enable MQTT services on the device

The MQTT functionality is disabled by default. There are two ways to enable MQTT, depending on the software build:

- To enable MQTT in RMC-100s with software versions prior to 2105452-034, refer to section 6.1 Enable MQTT from terminal mode.
- To enable MQTT in RMC-100s with software versions 2105452-034 (which contains Flash version 2105457-031) or later, see section 6.2 Enable MQTT from PCCU Communication Services tab.

IMPORTANT NOTE: Enabling MQTT does not require device restart.

6.1 Enable MQTT from terminal mode

Enable MQTT from the PCCU terminal mode. Terminal mode is available from PCCU after connection with the device. Use the USB port for local connection.

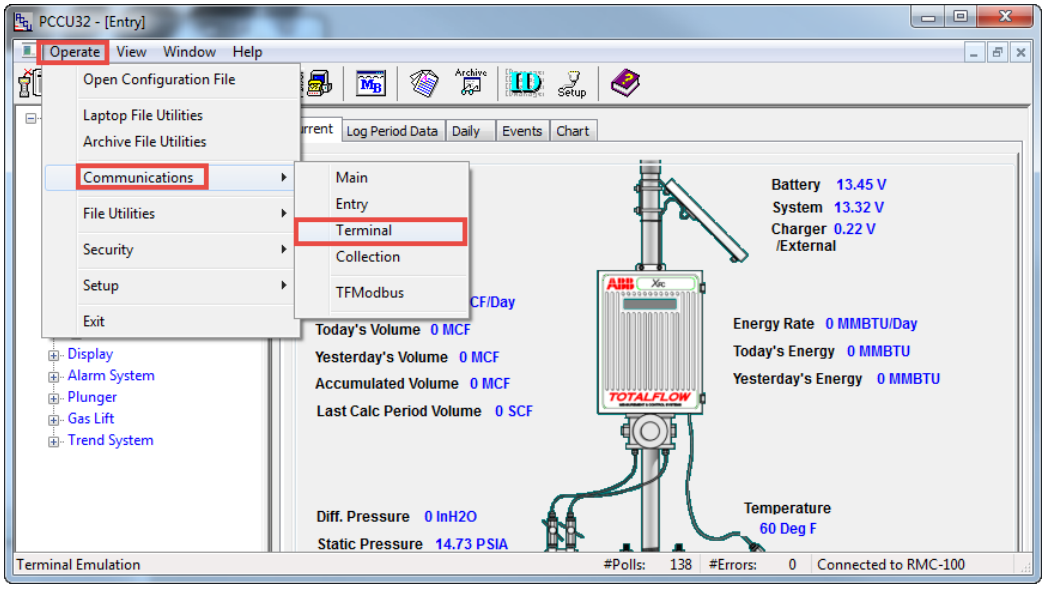
IMPORTANT NOTE: The terminal mode does not issue a confirmation message after MQTT is enabled. It takes 5 to 7 seconds for the change to take effect.

Enabling MQTT on the device also enables the MQTT configuration interface.

To enable MQTT on the device:

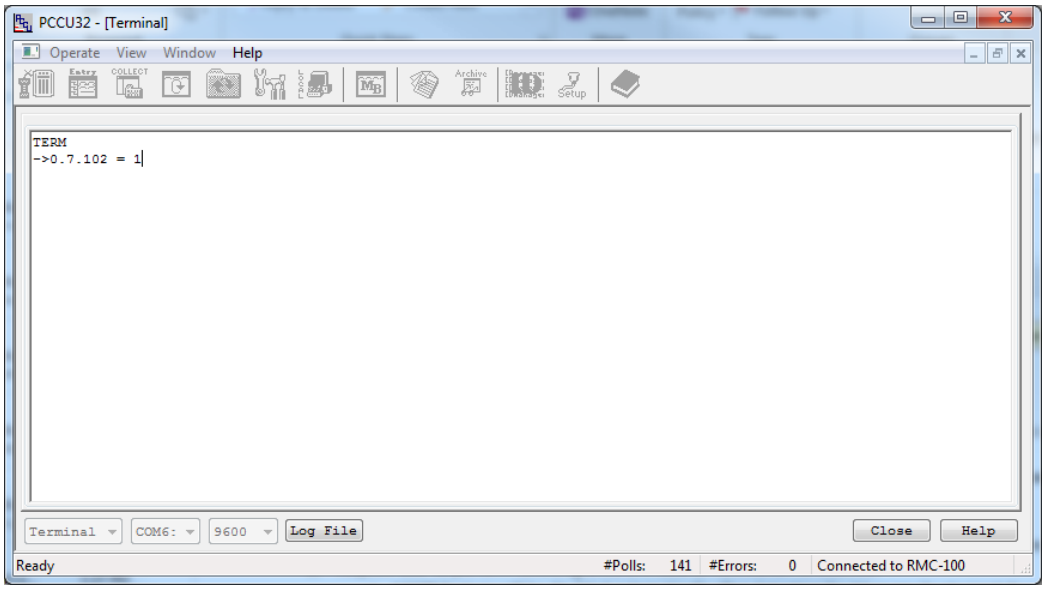
1. Connect the laptop to the USB port on the device.
2. Start PCCU.
3. Click the Entry icon to connect with the device.
4. Select **Operate** > **Communications** > **Terminal** from the top menu to go to terminal mode.

Figure 6-1: Access terminal mode on device



5. To enable MQTT, type **0.7.102 = 1** at the prompt, then press **Enter**.

Figure 6-2: Enable MQTT functionality from terminal mode



6. Click **Close** to exit terminal mode.

6.2 Enable MQTT from PCCU Communication Services tab

This procedure is applicable to RMC-100s with customer software package version 2105452-034 (which contains Flash version 2105457-031) or later.

This procedure enables the MQTT services from the Services tab. The MQTT services are separated into 2 options:

- Enable the MQTT process managing the connection to the MQTT brokers
- Manage the user access to the MQTT configuration interface on the device

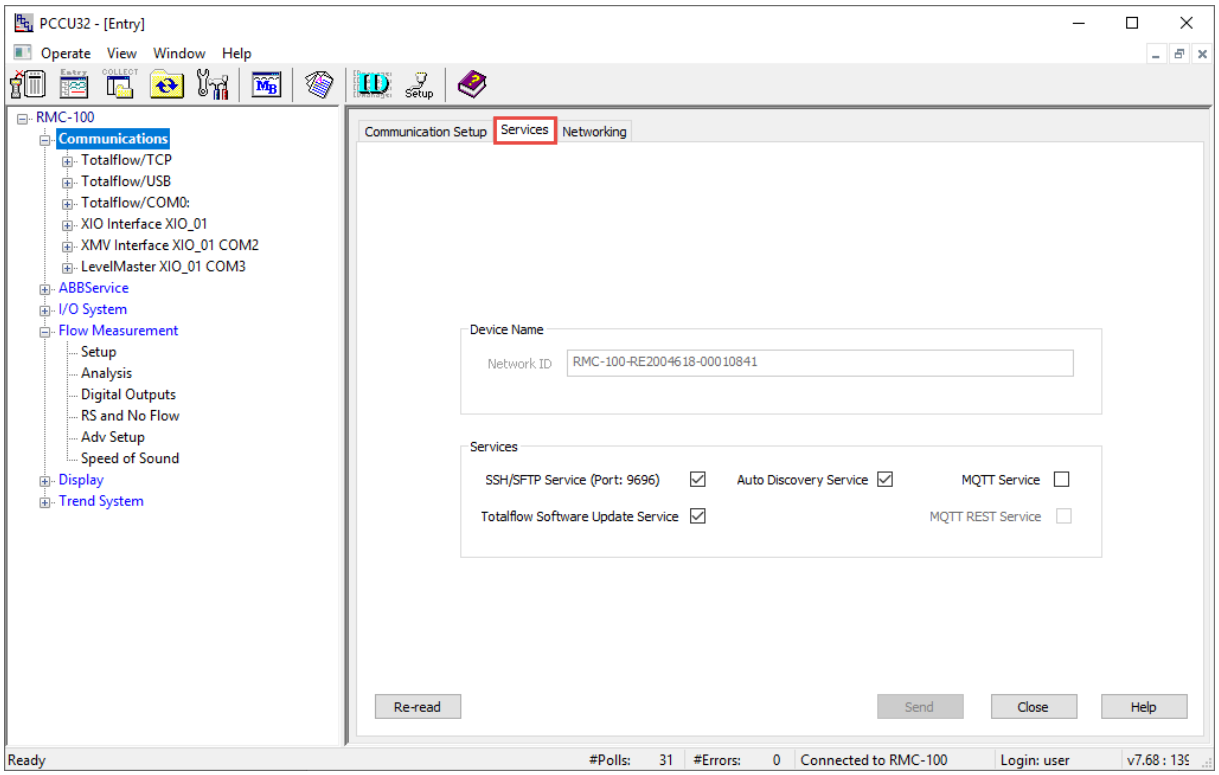
The MQTT configuration interface is separate from PCCU. All MQTT-related configuration must be completed from the MQTT interface.

The MQTT Service should always be enabled if the device is managed from the private or public cloud. The MQTT REST server can be enabled for configuration and verification purposes only but can be disabled after configuration is complete. Disabling the REST MQTT Service depends on your security requirements.

To enable MQTT on the device:

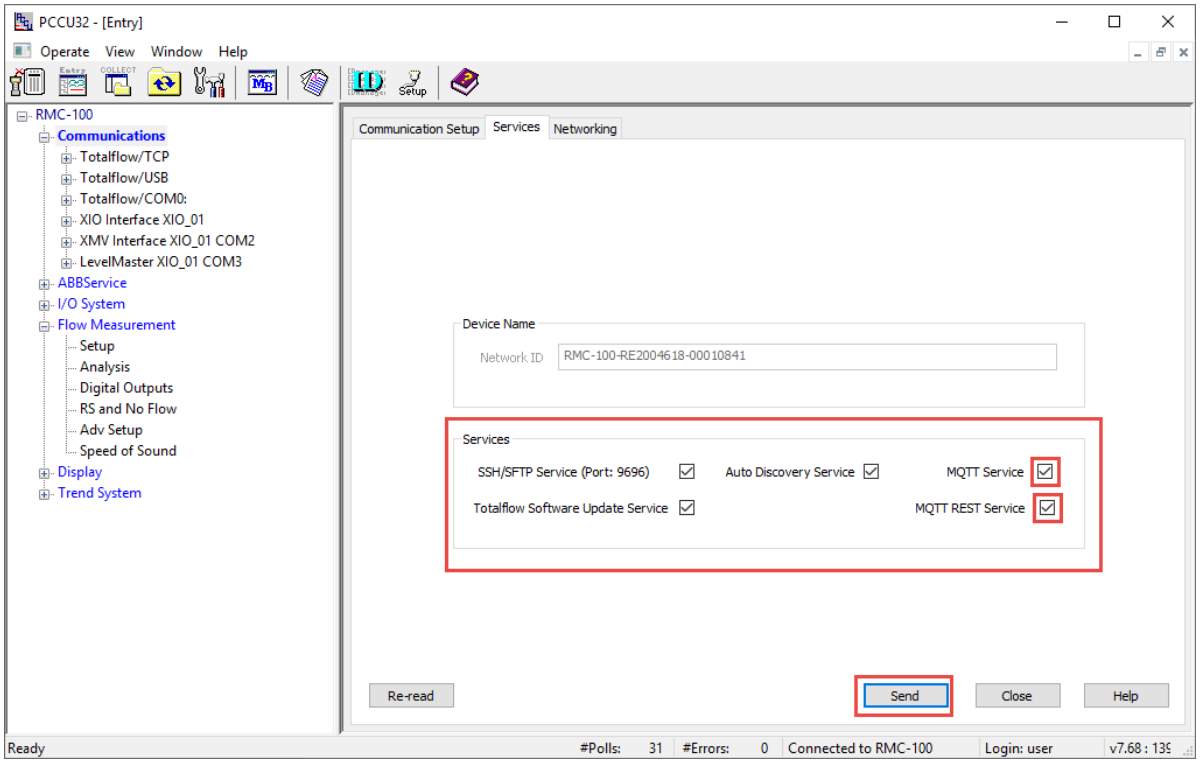
1. Connect the laptop to the USB port on the device.
2. Start PCCU.
3. Click the Entry icon to connect with the device.
4. On the navigation tree, select **Communications**. The Communication Setup screen displays.
5. Select the **Services** tab.

Figure 6-3: Communication Services tab on the RMC-100



6. In the Services section (Figure 6-4):
   a. Select **MQTT Service**. The MQTT REST Service activates.
   b. Select **MQTT REST Service**.
7. Click **Send**.

Figure 6-4: Enable MQTT and REST Services from PCCU Services tab



7 Initial configuration

7.1 Initial access to the MQTT configuration interface

The MQTT configuration interface supports only configuration for MQTT-related parameters. Perform all other device and application configuration from PCCU.

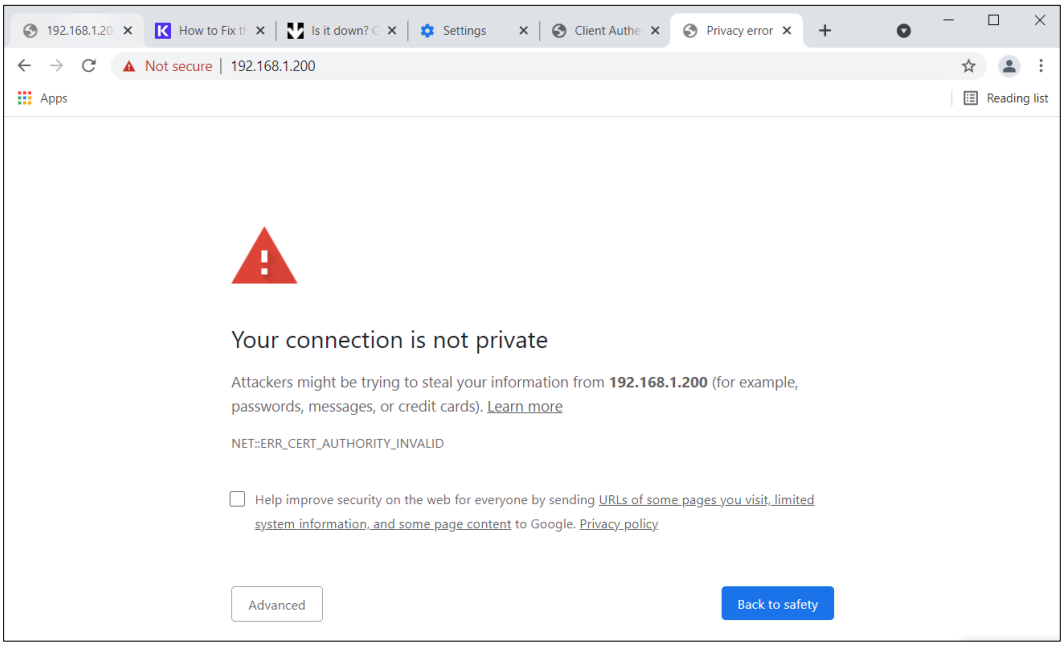
IMPORTANT NOTE: Local access to the MQTT configuration interface requires that both the laptop and the device are connected to the field network (through Ethernet). Both must be configured with valid IP addresses for this communication. MQTT parameters cannot be configured using USB. You must have the IP address of the device to connect with it.

To access the MQTT configuration interface:

1. Connect the laptop and the device to the local field network (Ethernet).
2. On the laptop, start the Chrome browser.
3. Go to the URL address: **https://<Totalflow Device's IP address>:443**. For example, https://10.127.133.220:443. A security warning displays.

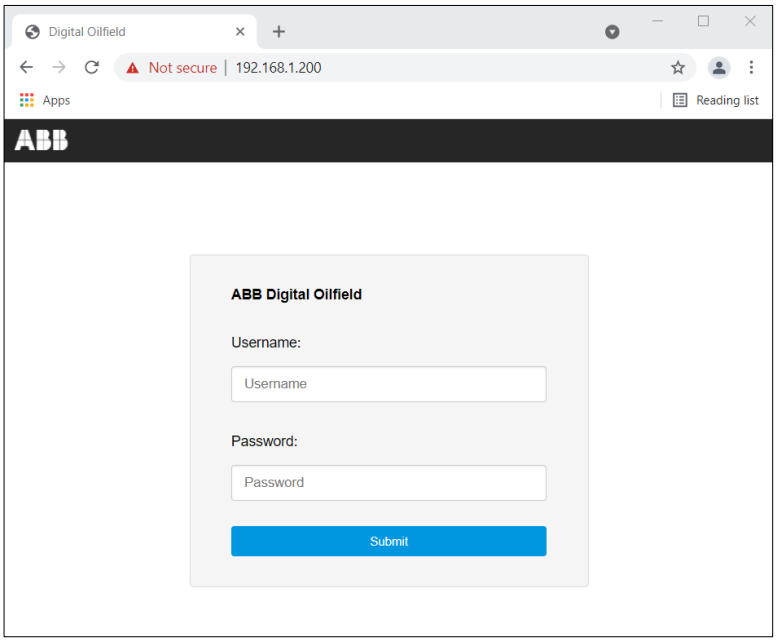
IMPORTANT NOTE: Security warnings displays at first-time login when the end user browser does not have valid certificates to access the device (Figure 7-1). The "Not secure" warning in the URL field displays because the browser does not establish the connection on secure mode. The device supports secure connections from end users, but the end user must have valid certificates. New devices shipped from the factory will have certificates and the warning may not appear. Please note that certificates for secure connection to the device are not the same as the certificates used by a device to connect to a broker. See section 7.2 Configure secure connection to the device for more details.

Figure 7-1: Security warning message



4. Click **Advanced** at the bottom of the screen. Additional security information displays. A link to the device is provided to proceed.
5. Click **Proceed to <device IP address>**. The login screen displays.

Figure 7-2: Device MQTT configuration interface login screen



6. Type **root** into the Username field. Type the default root password, **root@123**, into the Password field.
7. Click **Submit**. The Initial Configuration screen displays. Figure 7-3 shows the Initial Configuration page when the device has a valid certificate for secure access to the MQTT REST interface. Figure 7-4 shows an additional section to upload a valid certificate for MQTT REST interface access. This section shows **only if** the certificate embedded in the device has expired or is about to expire. If you need a new certificate, contact ABB. See section 7.2 Configure secure connection to the device for more details.

Figure 7-3: Initial Configuration page – factory defaults

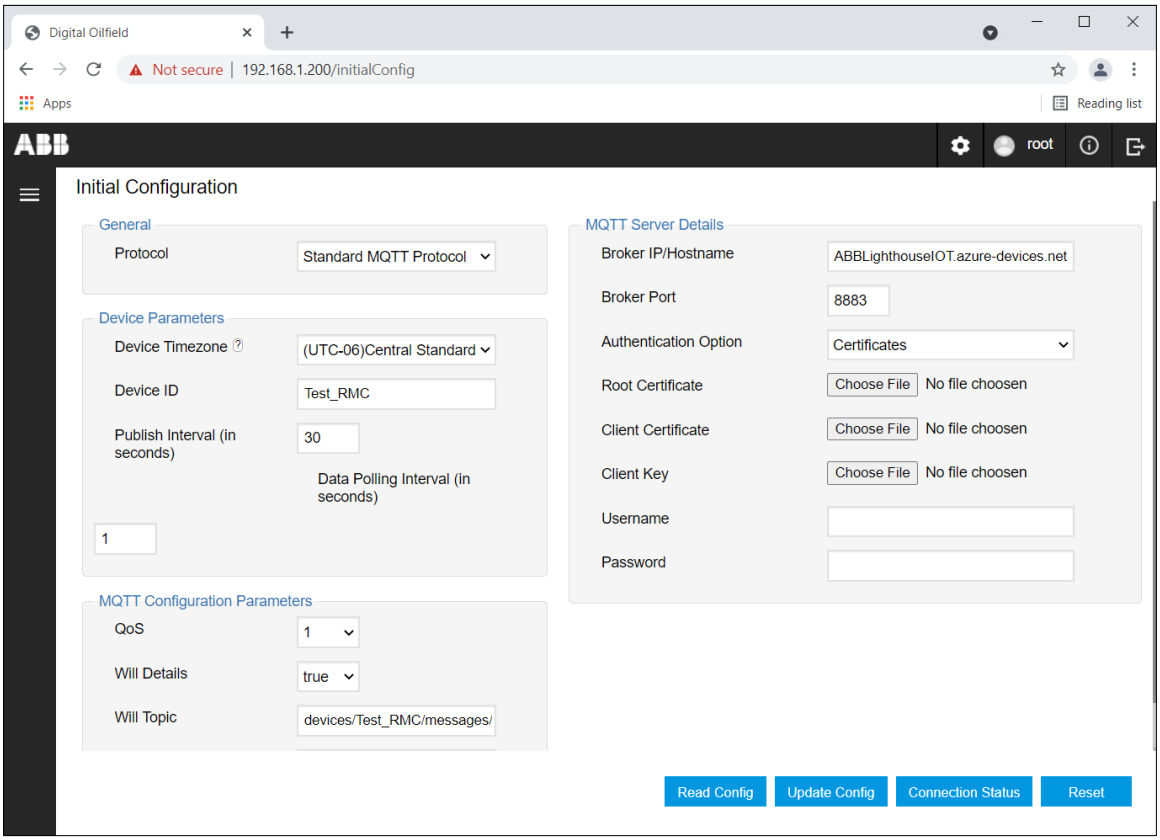
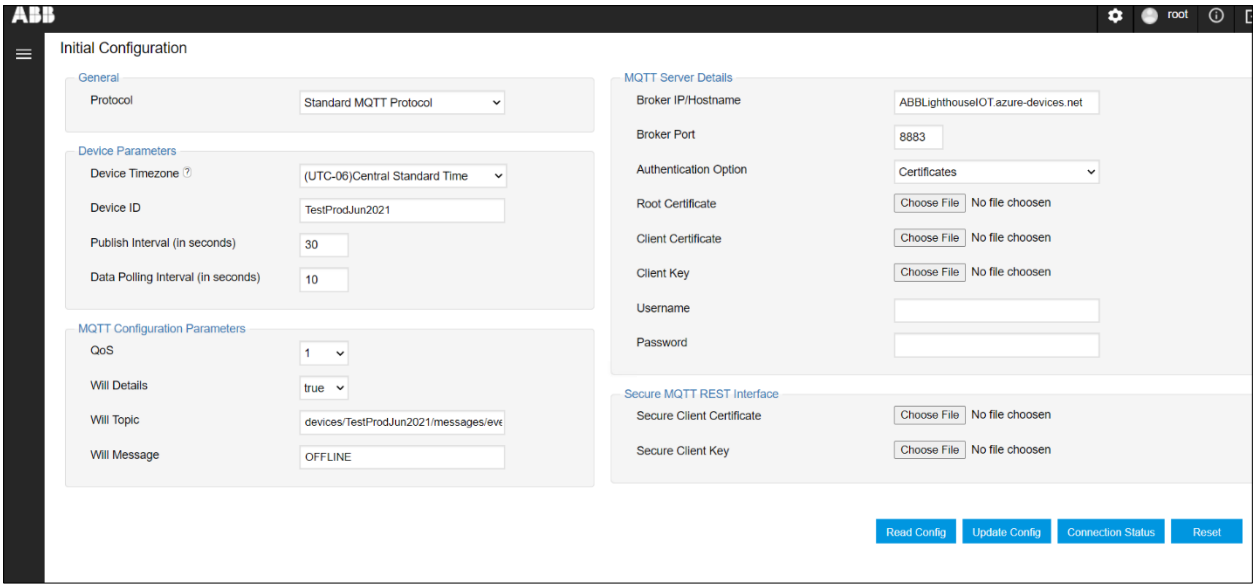


Figure 7-4: Initial Configuration page (New certificate for MQTT REST interface required)



7.2 Configure secure connection to the device

The device MQTT configuration interface supports secure connections from the end user browser with the use of valid certificates. Initial certificates to authenticate connections are included with the embedded software in the device itself. If the Initial Configuration screen displays the Secure MQTT REST Interface section as shown in Figure 7-4, request a new certificate from ABB.

7.2.1 Upload valid certificates (when needed)

Factory default certificates are valid for one year. Prior to the expiration date, the Initial Configuration interface allows certificate update from the Secure MQTT REST Interface section. Request new certificates

from ABB and upload these certificates to the device. ABB generates and provides self-signed certificates upon request.

To update certificates:

1. Request certificates from ABB if the Initial Configuration screen displays the Secure MQTT REST Interface section (Figure 7-5) or when the warning about certificate expiration displays (Figure 7-6). Certificates should be generated for the IP address range assigned to the field devices. There are two files required: client-cert.pem and client-key.pem.

Figure 7-5: Initial Configuration screen displaying the Secure MQTT REST Interface

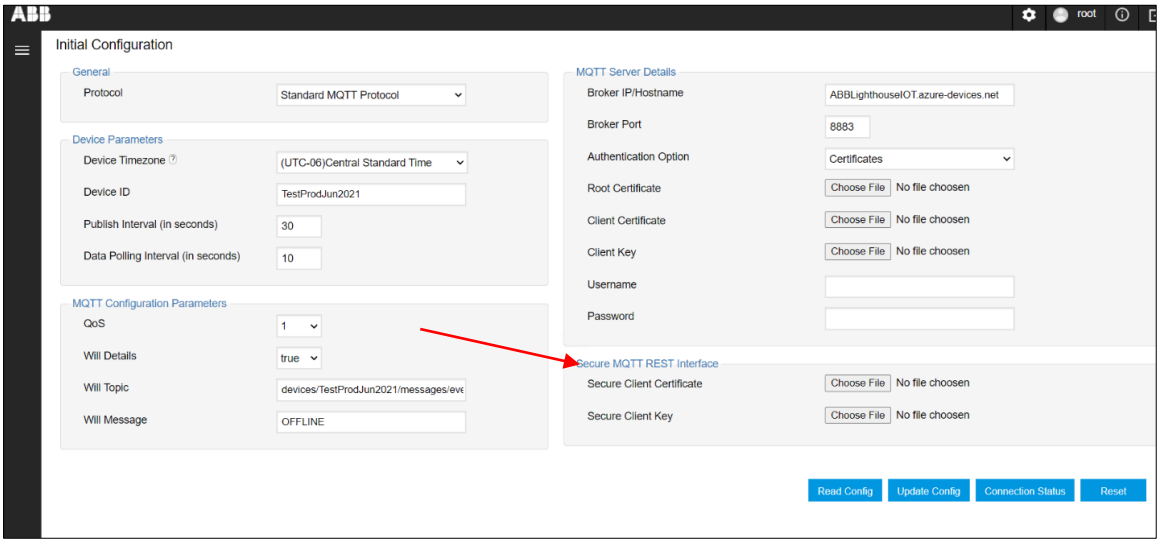
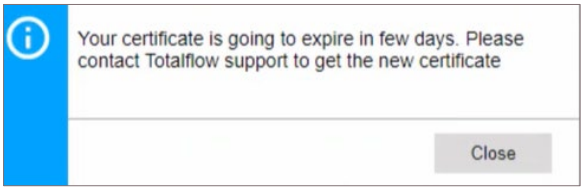
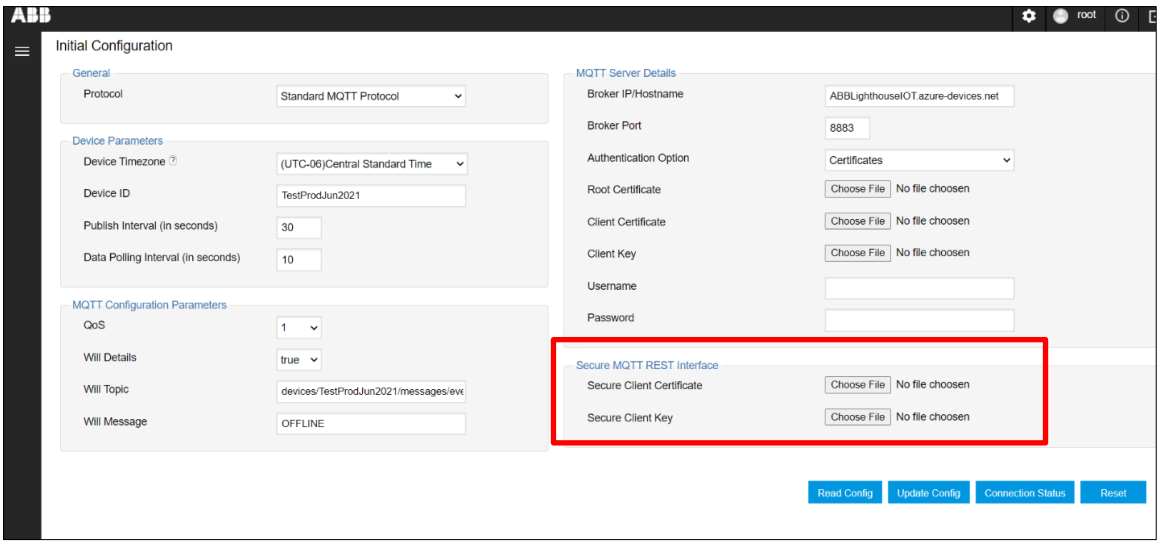


Figure 7-6: Certificate expiration warning



2. Download or copy the certificate files received from ABB to the laptop or PC used to connect with the device(s).
3. Select new certificate files from the **Secure MQTT Rest Interface** section of the Initial Configuration screen (Figure 7-7):

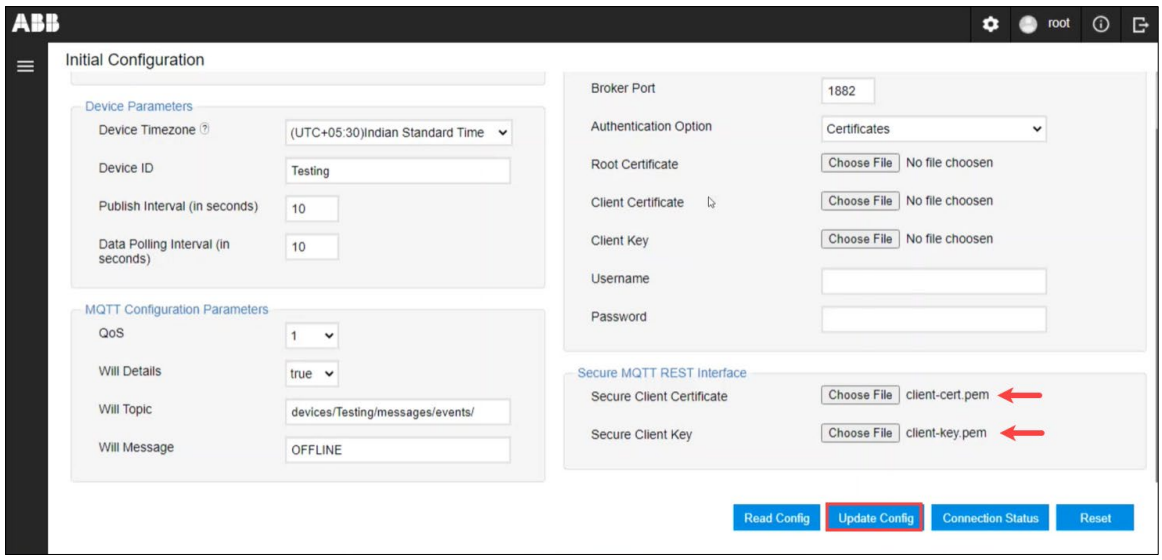
Figure 7-7: Use Secure MQTT REST Interface section to update certificates



a. Click **Choose File** for the Secure Client Certificate (Figure 7-8).
b. Locate and select the file from the file browser window.
c. Click **Open**. The name of the file displays on the screen.
d. Click **Choose File** for the Secure Client Key (Figure 7-8).
e. Locate and select the file from the file browser window.
f. Click **Open**. The name of the file displays on the screen.

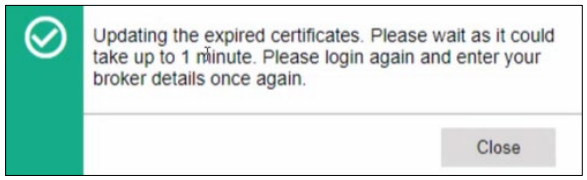
4. Click **Update Config** (Figure 7-8).

Figure 7-8: Upload new certificates using Update Config



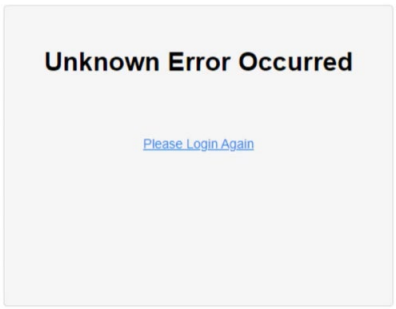
5. Wait for the certificate upload to complete. The following message should display:

Figure 7-9: Certificate update



6. Click **Close**.
7. Refresh the Initial Configuration screen. An error may message display:

Figure 7-10: Error message after certificate update



8. Click **Please Login Again**. The Initial Configuration screen should display without the Secure MQTT Rest Interface section in it. This means that the certificates are valid and not close to expiration. With valid certificates, a secure browser-device connection can be configured in section 7.2.2, next.

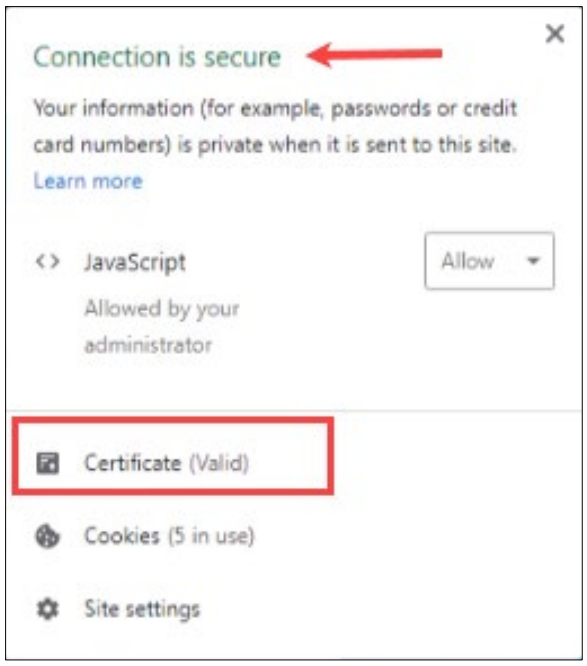
7.2.2 Configure browser for secure connection

When a valid certificate is available in the device, the browser can be configured for secure connection. The browser can detect if the certificate in the device is valid or not upon login:

— If the browser indicates an invalid certificate, obtain valid certificates, upload to the device as shown in section 7.2.1 Upload valid certificates (when needed) and then import certificate into the browser for secure connection as shown in this section.
— If the device indicates a valid certificate, import the certificate into the browser for secure connection as shown in this section.

When the browser does not detect a valid certificate, the "Not Secure" warning displays in the URL if you log into the device. When the certificate is valid and imported into the browser certificate store (as shown in this section), the connection is secure. The goal of the procedure in this section is to configure the browser to trust the valid certificate in the device as shown in Figure 7-11.

Figure 7-11: Secure browser-device connection when device has valid certificate

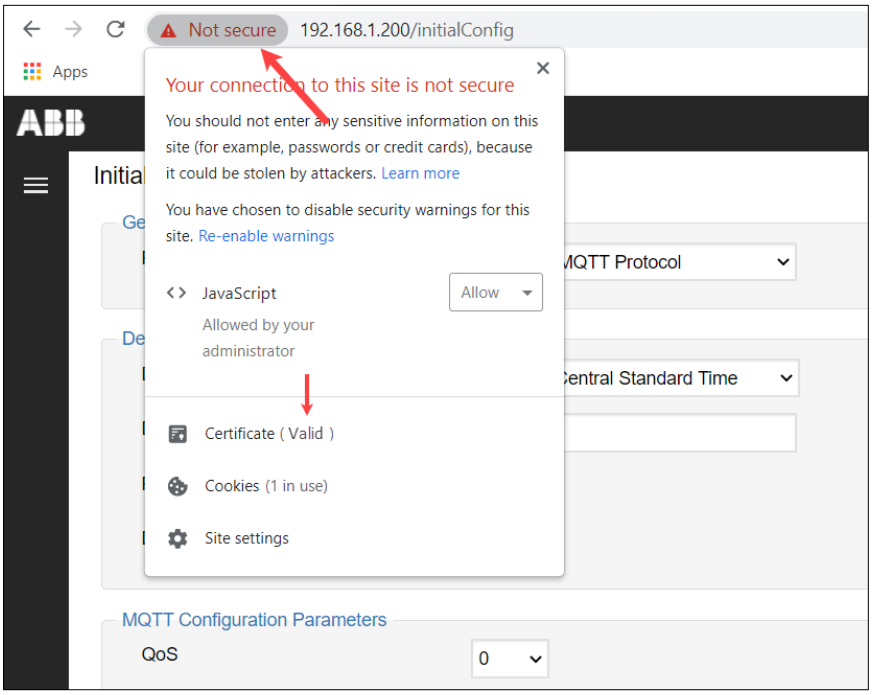


To configure a secure browser–device connection:

IMPORTANT NOTE: This procedure assumes that valid certificates are available in the laptop used to connect with the device.

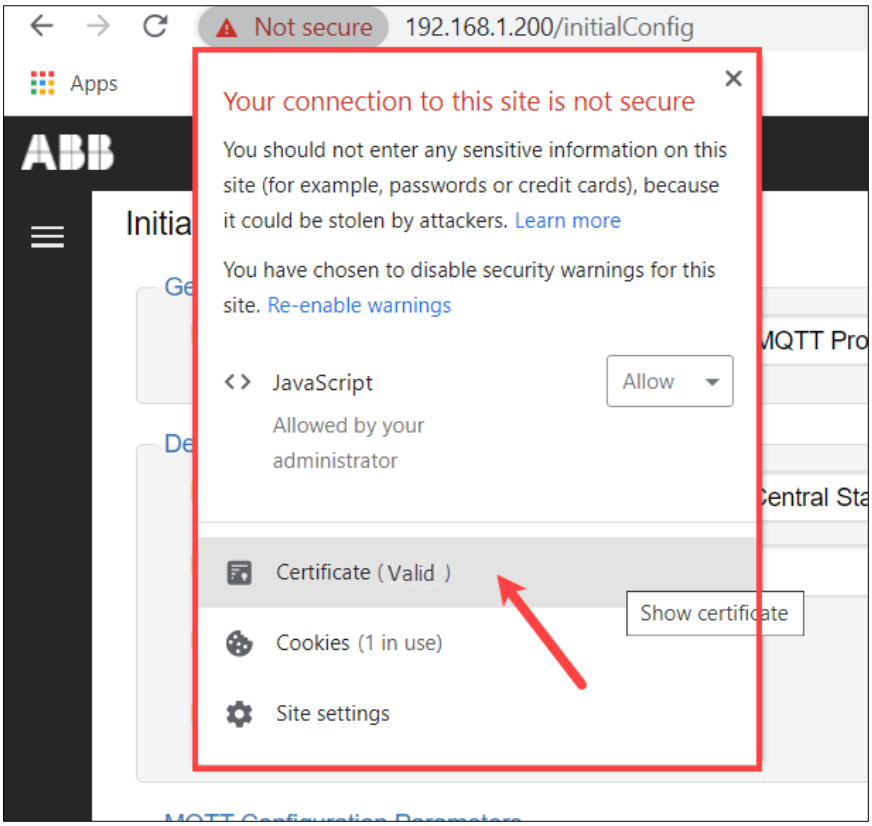
1. Click **Not Secure** in the URL field on top of the screen. Note that if the browser does not detect a valid certificate on the device (the certificate may have expired), it shows: Invalid, next to the Certificate in the drop-down menu.

Figure 7-12: Security warning



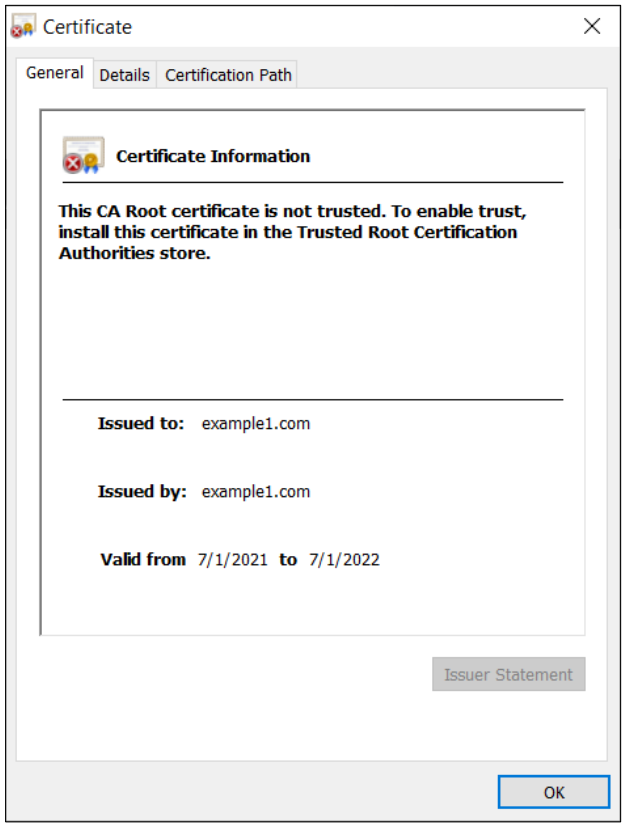
2. Select **Certificate** from the drop-down menu (Figure 7-13).

Figure 7-13: Browser connection drop-down menu



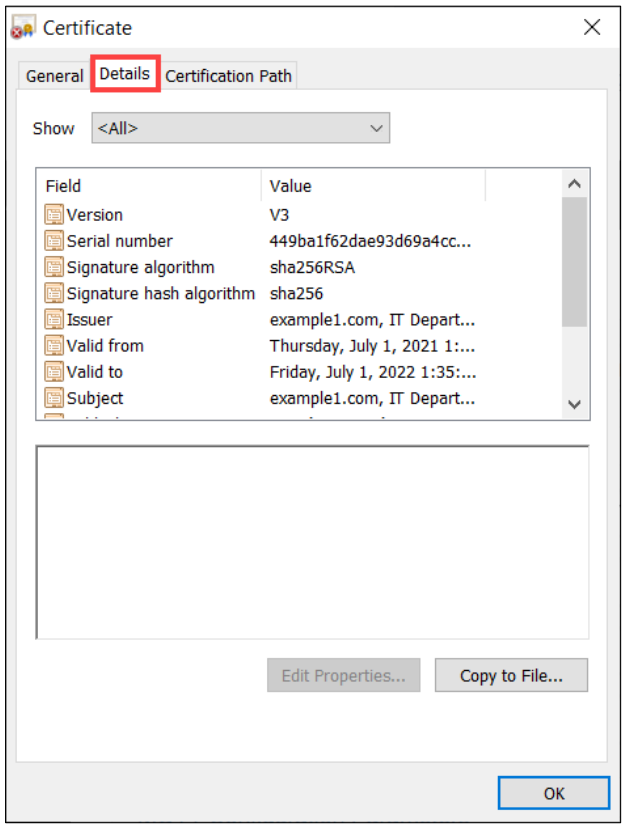
The Certificate dialog window displays (Figure 7-14).

Figure 7-14: Certificate dialog window - General tab



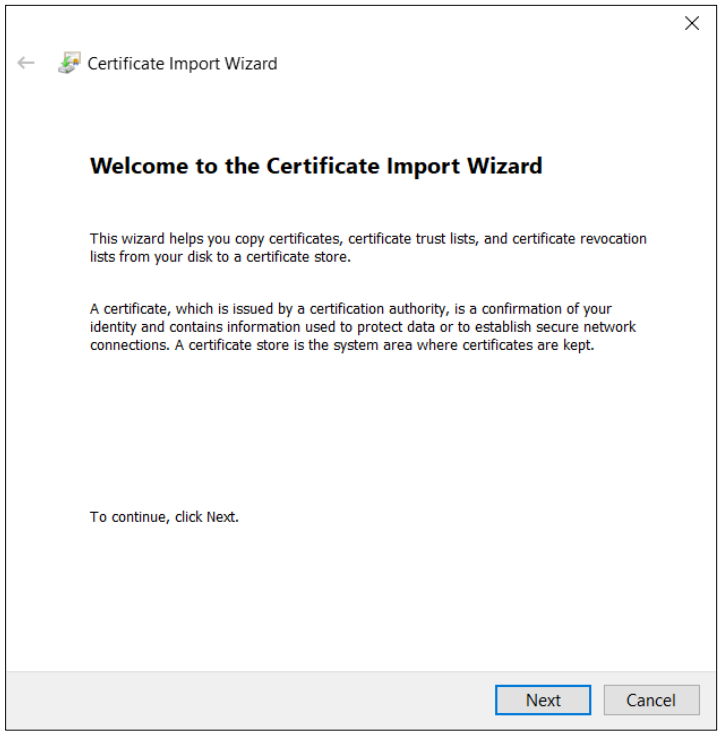
3. Click the **Details** tab.

Figure 7-15: Certificate dialog window Details tab



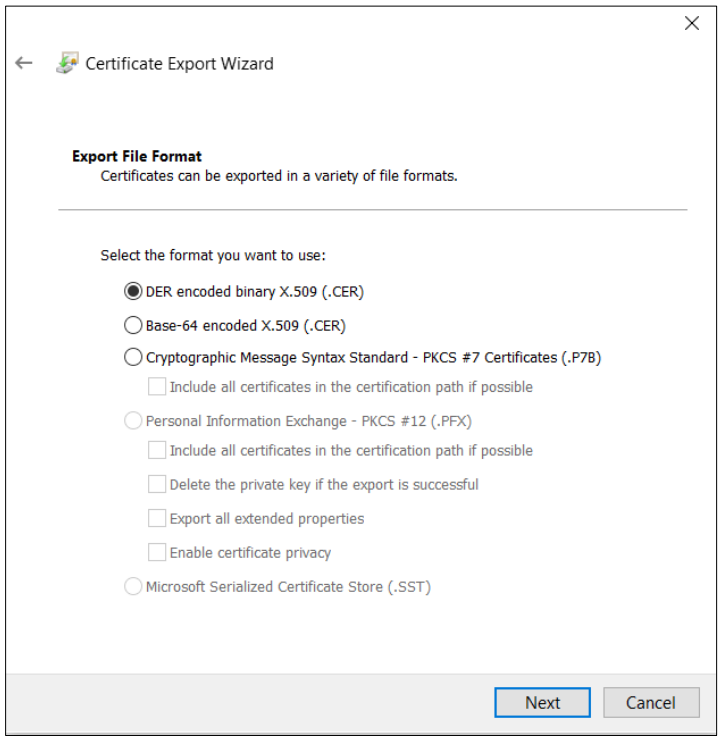
4. Click **Copy to File**. The certificate wizard displays.

Figure 7-16: Certificate Import Wizard



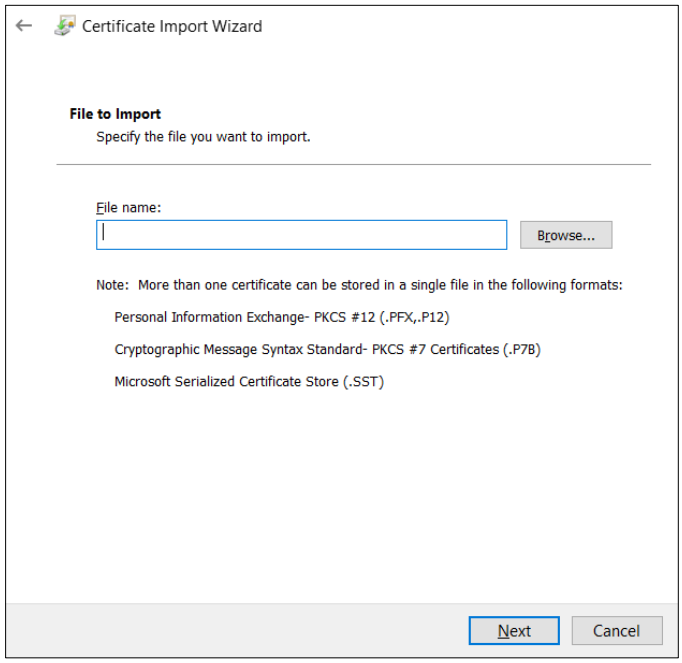
5. Click **Next**.

Figure 7-17: Certificate Import Wizard File Format



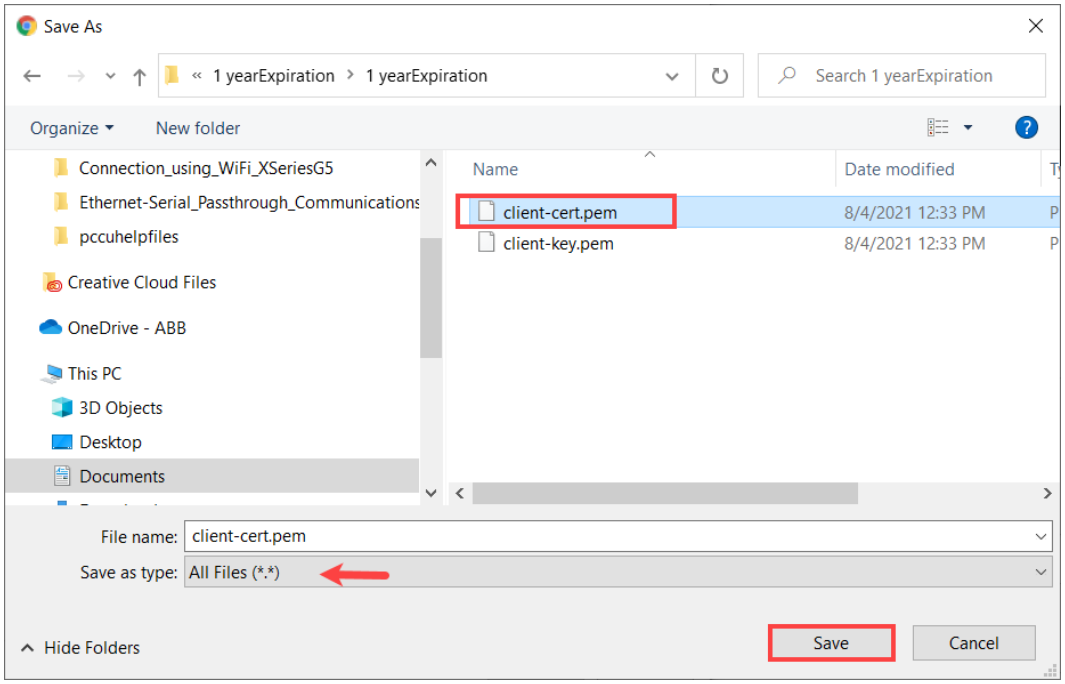
6. Click **Next**.

Figure 7-18: Certificate Import Wizard – File to import



7. Click **Browse**. The file browser displays (Figure 7-19).
   a. Locate and select the client-cert.pem file from the file browser. You may need to select **All Files (*.*)** from the **Save as type** field to display all files before selecting.
   b. Click **Save**.

Figure 7-19: File browser



8. The Certificate window displays the selected path to the certificate file.
9. Click **Next**.
10. Click **Yes** if prompted to confirm.

Figure 7-20: Confirm save of certificate file

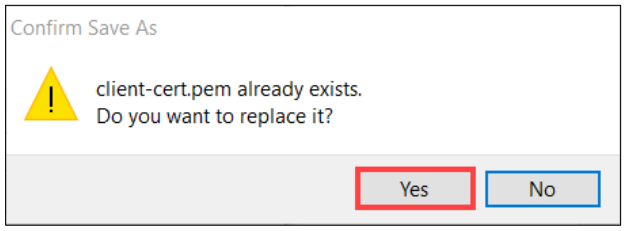
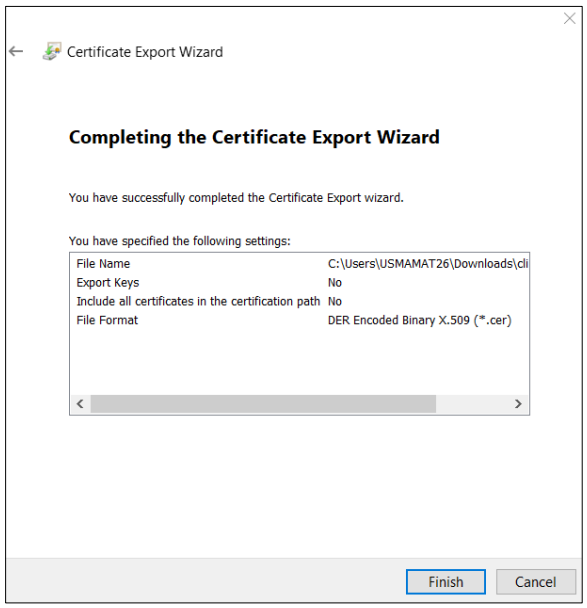


Figure 7-21: Complete the certificate export wizard



11. Click **Finish**.
12. Click **OK** at the successful export message to return to the Details tab.
13. Click **OK** to exit the Certificate window.
14. Select the custom icon on the Chrome browser.
15. Select **Settings** from the drop-down menu (Figure 7-22). The settings page displays (Figure 7-23).

Figure 7-22: Chrome browser settings

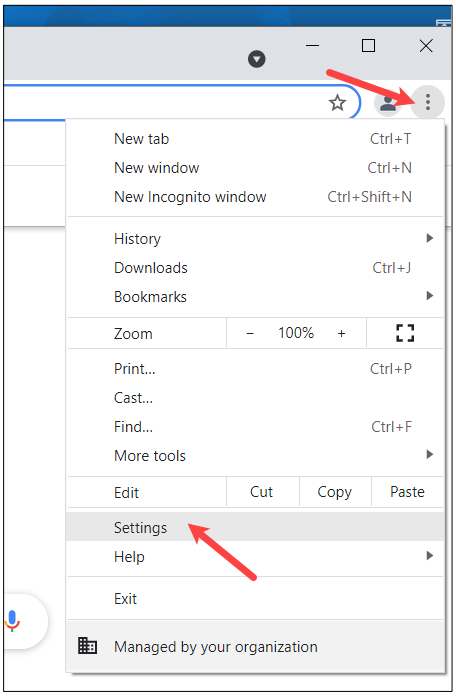
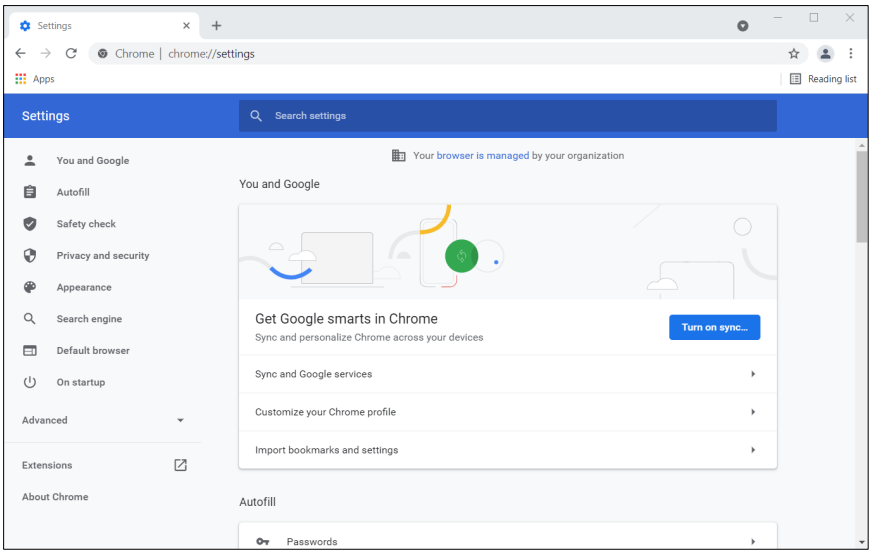
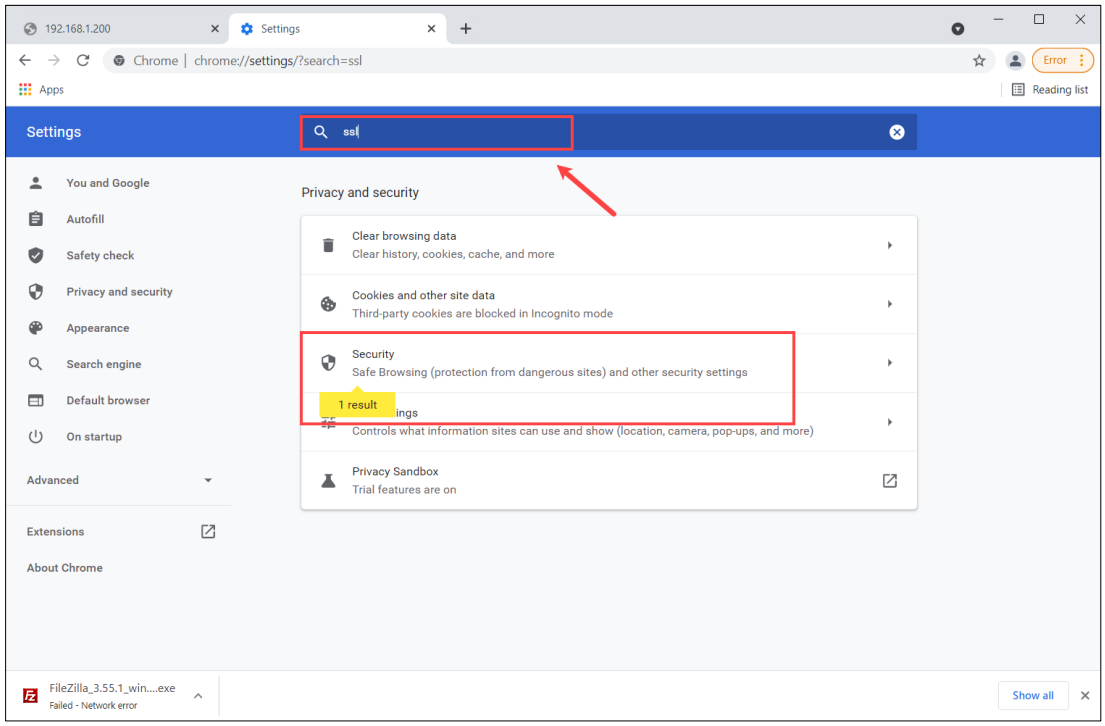


Figure 7-23: Chrome settings page



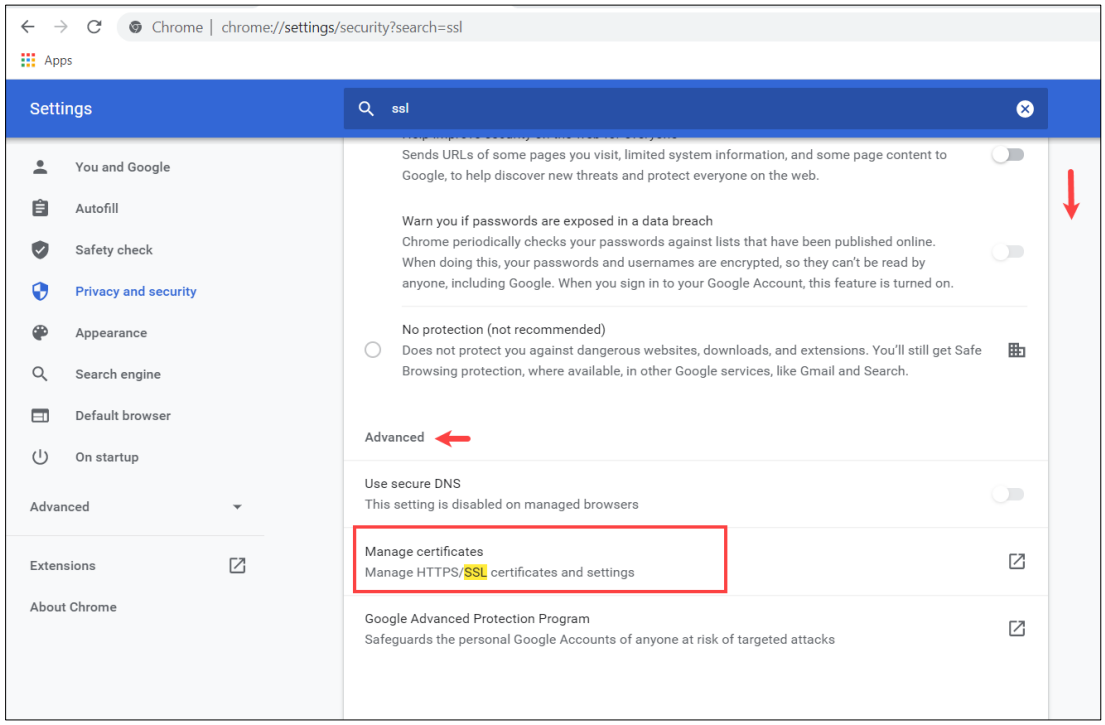
16. Type **SSL** in the search box or scroll down to select **Security** (Figure 7-24).

Figure 7-24: Security options



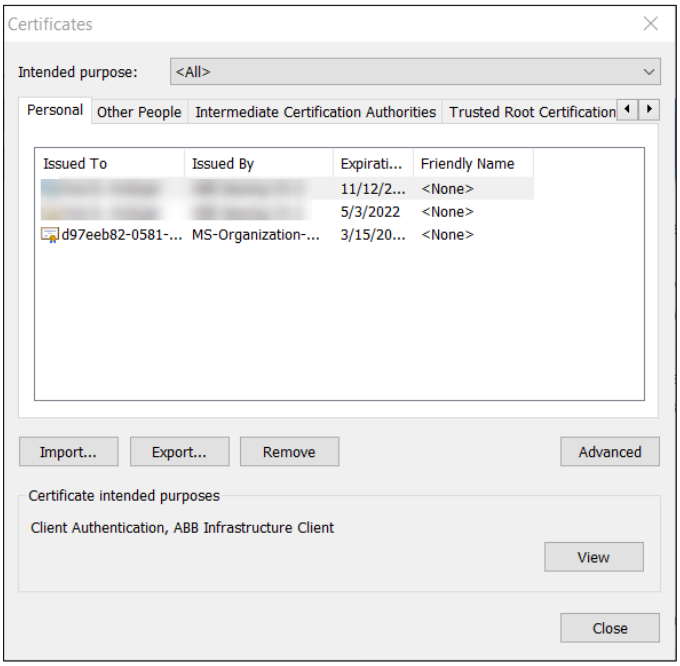
17. Scroll down to the Advanced section. Locate the **Manage certificate** option (Figure 7-25).

Figure 7-25: Advanced Security – Manage Certificate option



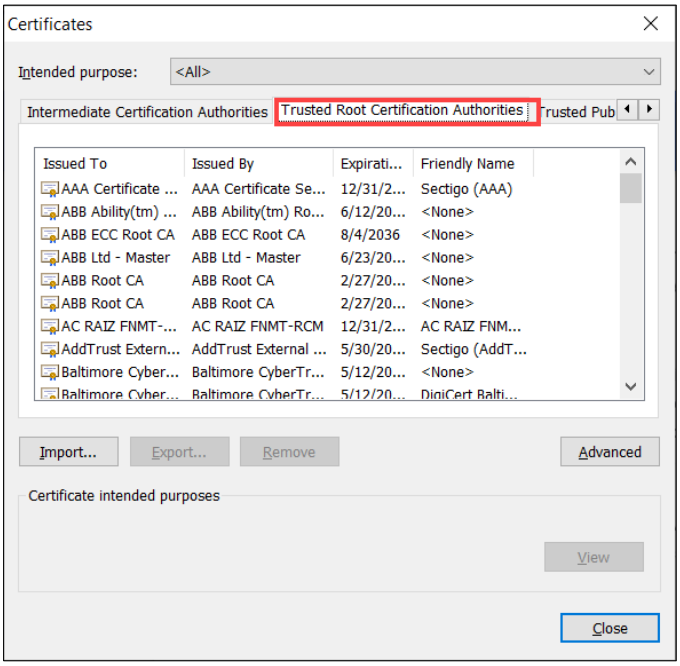
18. Select **Manage Certificates**. The Certificates window displays (Figure 7-26).

Figure 7-26: Certificates window



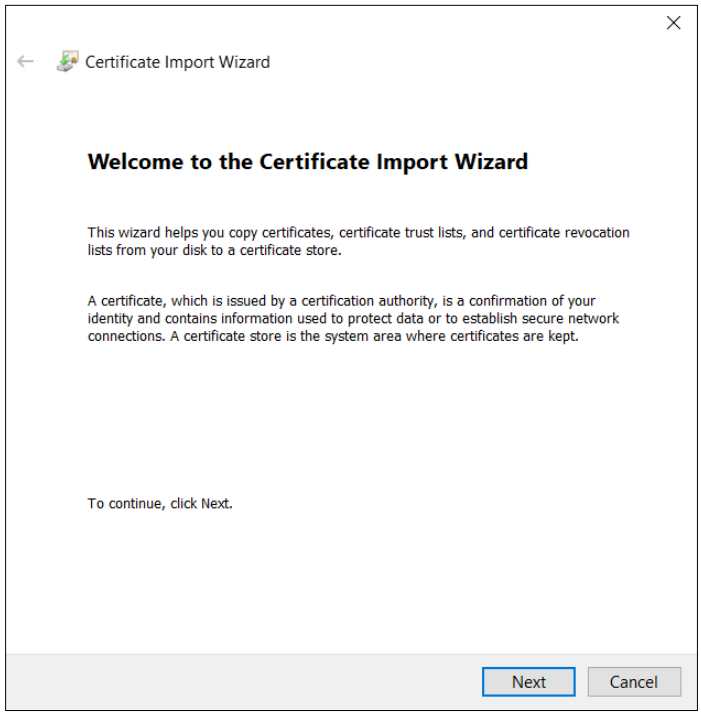
19. Select the **Trusted Root Certification Authorities** tab.

Figure 7-27: Trusted Root Certification Authorities tab



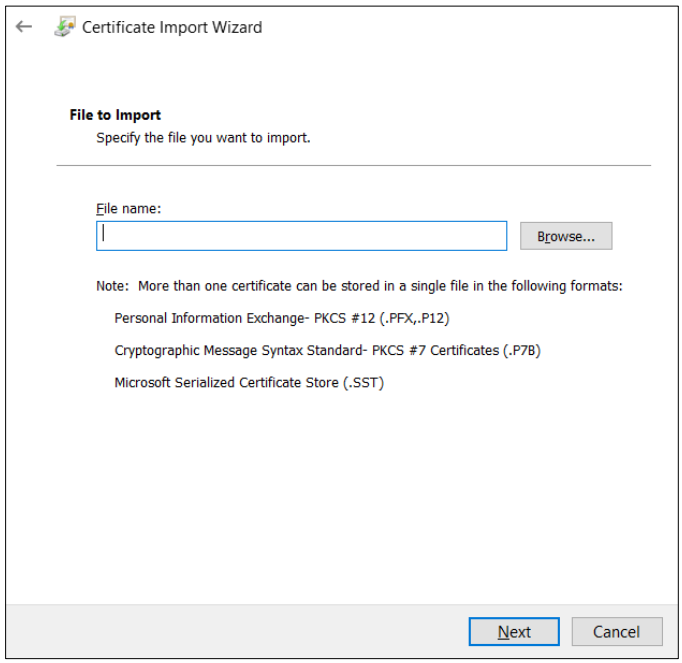
20. Click **Import**. The Import Wizard begins.

Figure 7-28: Certificate Import Wizard



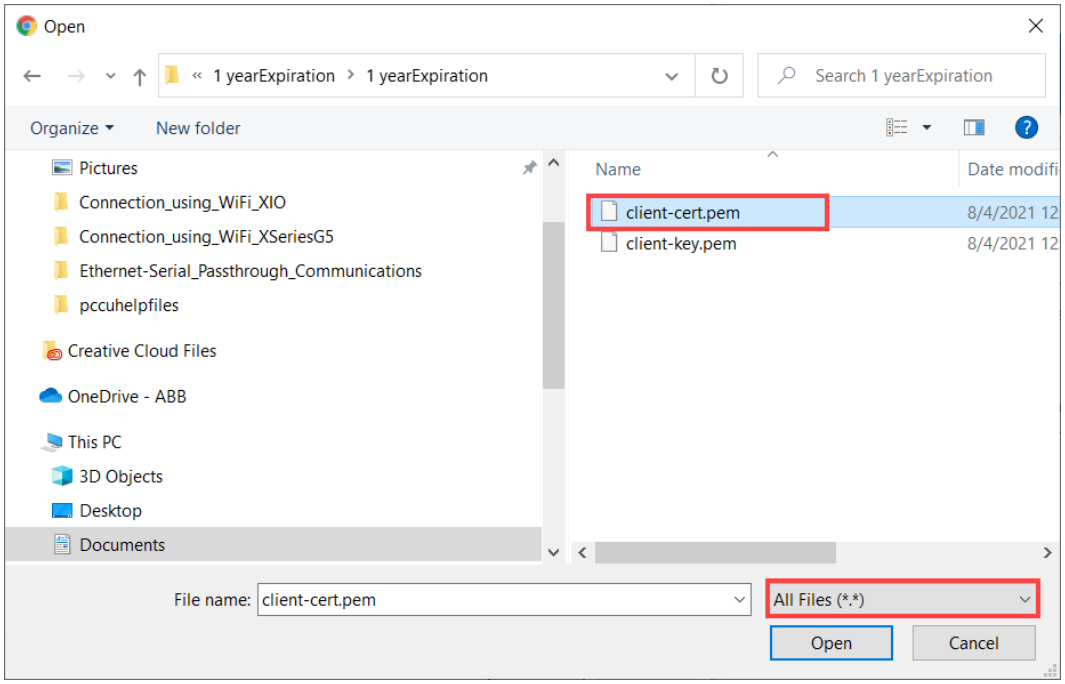
21. Click **Next**.

Figure 7-29: File to import



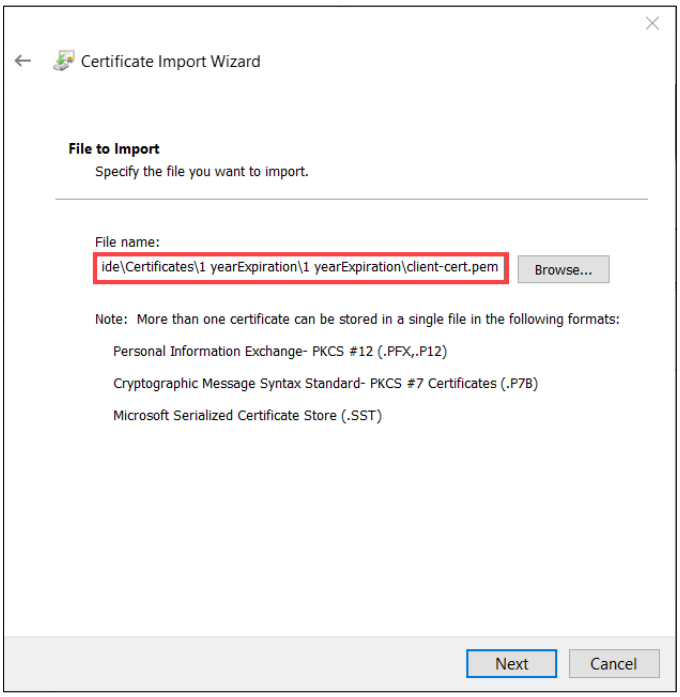
22. Click **Browse**.
23. Locate and select the certificate from the file browser, then click **Open**. You may need to select **All Files (*.*)** next to File name to display files before selecting (Figure 7-30).

Figure 7-30: File browser



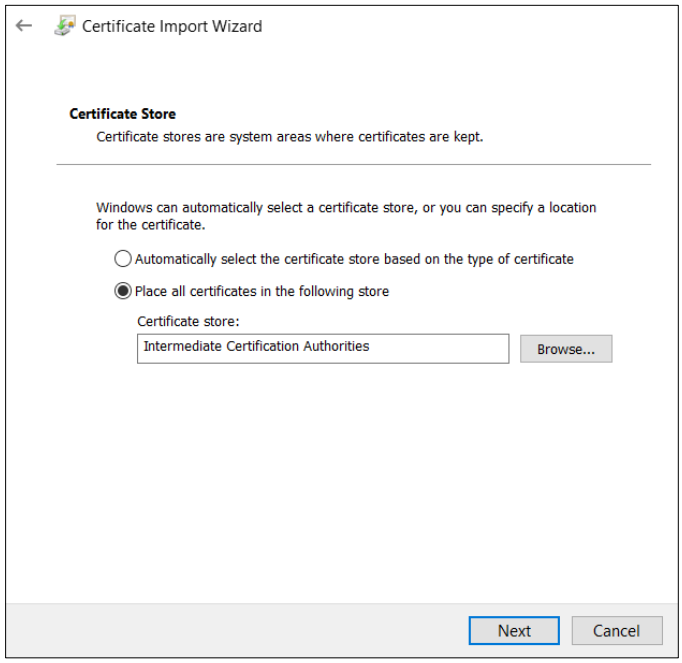
24. Click **Open**.

Figure 7-31: Certificate Wizard - Specify file to import



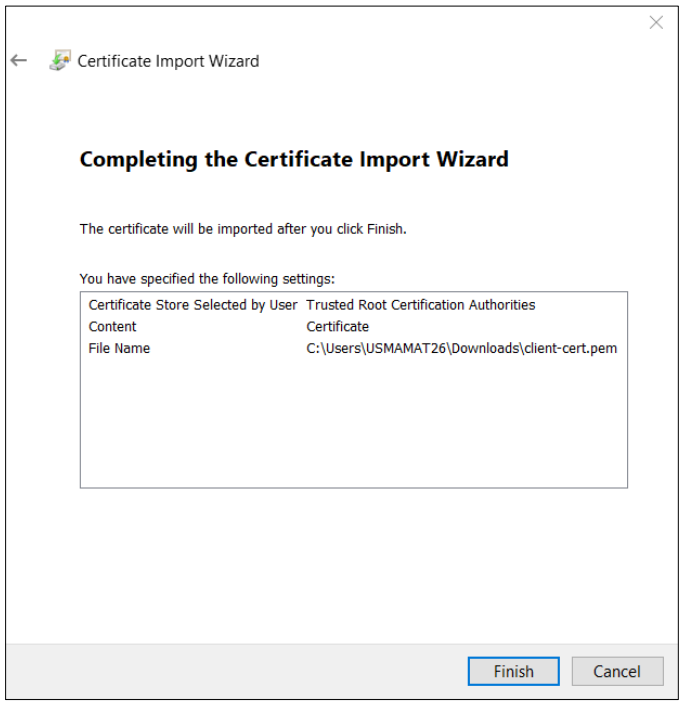
25. Click **Next**. The Certificate store location selection displays. Keep default selections.

Figure 7-32: Certificate store location on local drive



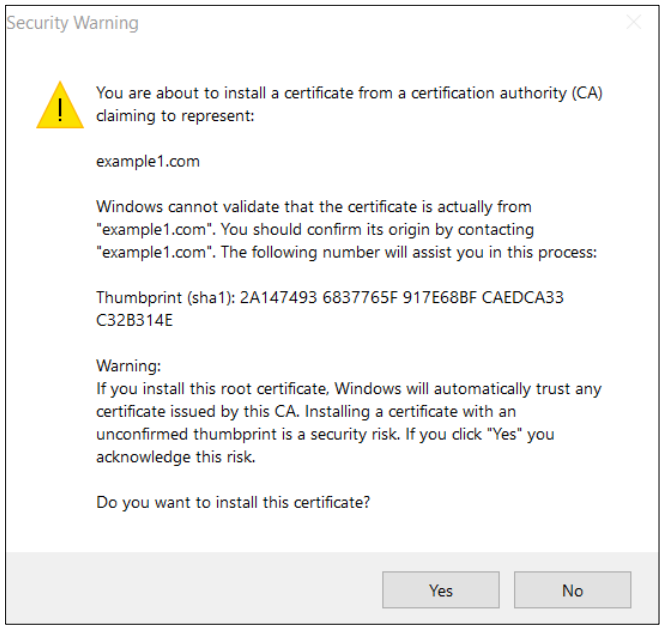
26. Click **Next**.

Figure 7-33: Completing the Certificate Import Wizard



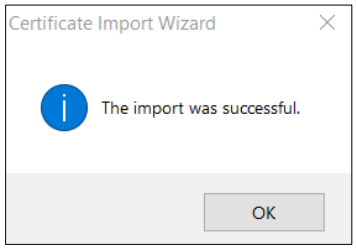
27. Click **Finish**.

Figure 7-34: Install Certificate warning



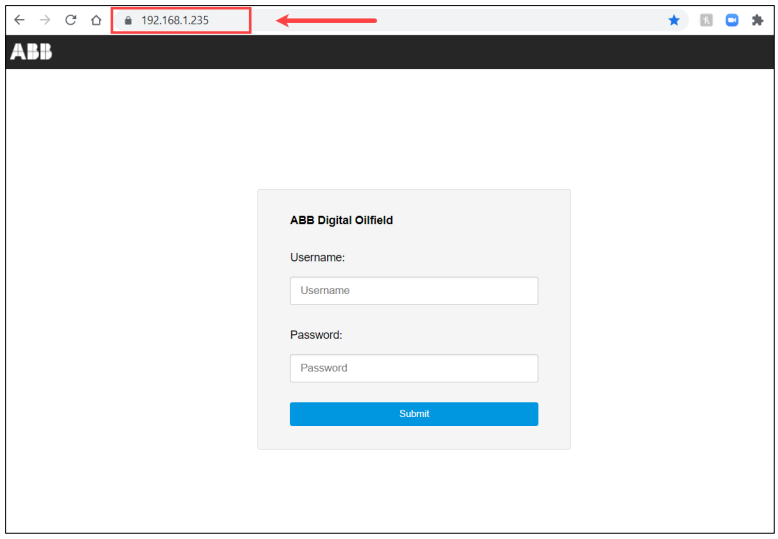
28. Click **Yes**.

Figure 7-35: Import successful message



29. Click **OK** at the successful import message.
30. Click **Close** to exit the Certificates window.
31. Close the web browser. Exit all tabs.
32. Restart the web browser and type the device address in the URL field to try connection. The login screen displays again. Notice that the ”Not Secure” message does not display in the URL field (Figure 7-36). Also, the lock icon indicates a secure connection.

Figure 7-36: “Not Secure” warning no longer displays



33. Type valid credentials and log into the device. The Initial configuration screen displays.
34. Be sure to change factory default credentials to allow device access for authorized personnel only (see section 10 Change default login configuration credentials).

7.3 Configure main parameters (Initial configuration)

The parameters in the Initial Configuration screen set the device for authentication and connection with the MQTT broker. This procedure assumes you have all the required values for those parameters and authentication certificates or credentials.

When using authentication certificates, certificate and key files are copied from the laptop to the device during this procedure. After configuration, these files reside in the device and ensure automatic re-authentication in case of disconnection from the broker. Certificate files do have expiration dates and must be maintained. Certificate generation and management are the sole responsibility of the customer. Ensure you have the certificate files ready before starting configuration.

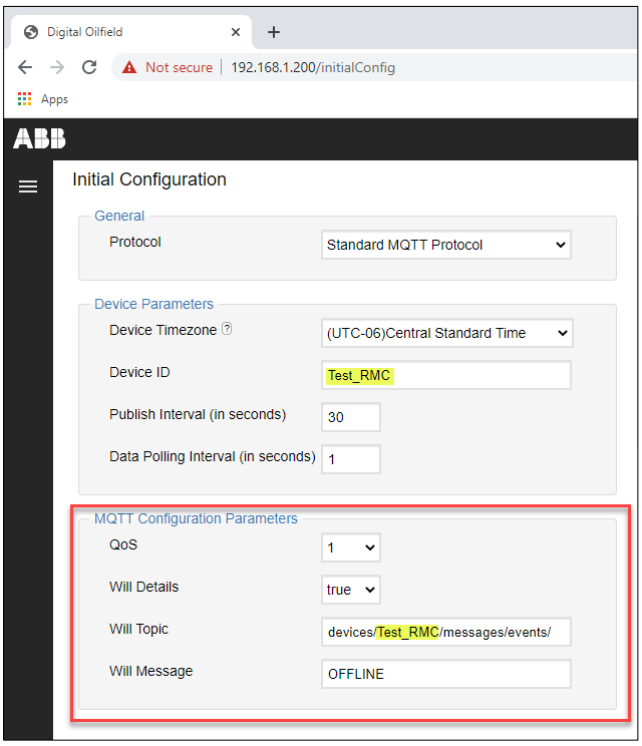
IMPORTANT NOTE (ABB Digital Oilfield customers only): When configuring for connection to a service provider cloud, the device must be registered on the cloud before attempting configuration or connection. Ensure your administrator has registered the device and determined the authentication preferences.

If the main MQTT broker is not available at the time of configuration, or connection from the field is not yet possible, customers can install and use a local "thin" broker on the laptop or system used to configure the device. The device configuration described in this document uses a local broker. This is for configuration purposes only. It provides a convenient way to complete the configuration. Devices can remain connected to the local broker for initial configuration, but customers must remember to configure the actual parameters of the permanent broker before leaving the site.

On the Initial Configuration screen:

1. Select the protocol from the protocol drop-down list.
2. Configure device parameters.

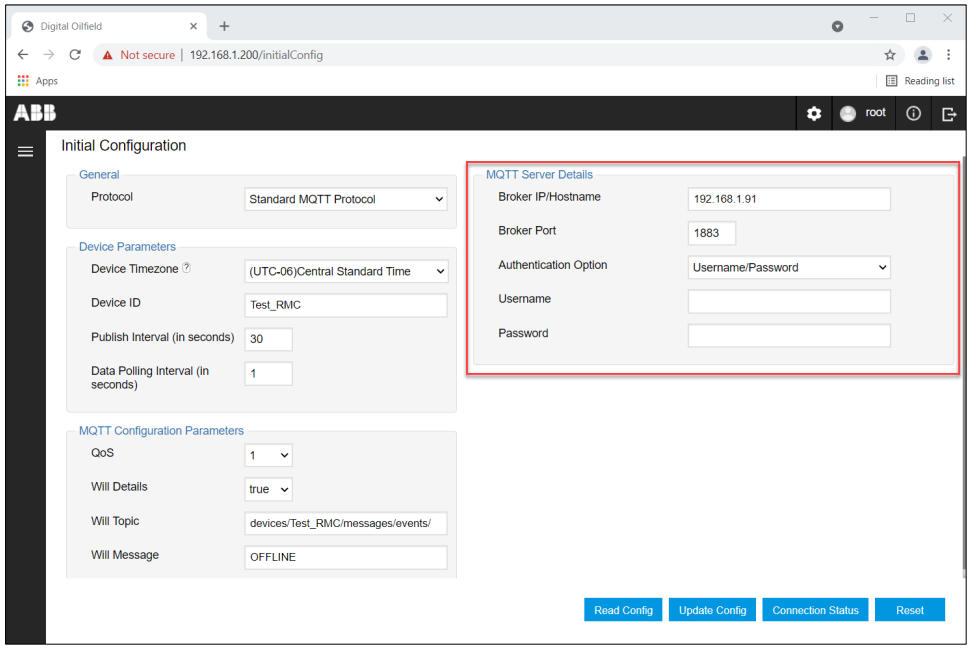
Figure 7-37: MQTT configuration parameters for Standard MQTT protocol



3. Configure MQTT parameters. Make sure that the Device ID in the Will topic matches the Device ID configured in the Device Parameters section (highlighted in Figure 7-37 above).
4. Configure MQTT server details (Figure 7-38).
   a. Configure the MQTT broker details based on your implementation. In this example, since a local broker is used to complete configuration, the IP address of the laptop and the default TCP port are configured.

b. Select the authentication method from the **Authentication Option** drop-down list. In this example, the authentication is only based on credentials. The Username/Password authentication option is selected. Type credentials as necessary.

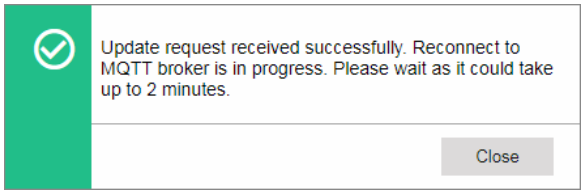
Figure 7-38: MQTT Server Details



IMPORTANT NOTE: For Certificates, click **Choose File** to locate and upload each required file: Root Certificate, Client Certificate, and Client Key. These files are required when the MQTT broker uses certificates as the authentication method.

5. Click **Update Config**. Wait for update confirmation.

Figure 7-39: Update factory default configuration



6. Click **Close** when the update request completes successfully.
7. Verify the device-broker connection next.

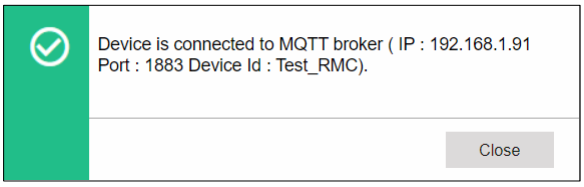
7.4 Verify device-broker connection status

Verify that the device can connect with the broker after Initial configuration update.

On the Initial Configuration screen:

1. Click **Connection Status**.
2. Wait for status verification.
3. Verify the status message. The message for a successful connection identifies that the device is connected to the MQTT broker and identifies the broker's hostname (or IP address), the TCP port and the device ID. The message for a failed connection attempt indicates that the device is not connected to the MQTT broker.

Figure 7-40: Verify device-broker connection status (local test broker)



4. When the connection is successful, proceed to section 8 Configure applications, then proceed to section 9 Configure registers.

IMPORTANT NOTE: A successful device-broker connection is required to continue with the application and register configuration in the next sections. Device-broker connection failure prevents display of the application and register configuration screens.

IMPORTANT NOTE: The device's MQTT implementation is designed to automatically re-establish connection to the broker in the event of a restart, network failure or disconnection.

8 Configure applications

Configure the applications that the device publishes data for. The device transfers or sends application data through the broker. Data is kept on the service provider or private network database(s) depending on the implementation.

IMPORTANT NOTE: The procedures in this section assume that the required applications are already instantiated, configured, and enable on the device. Use PCCU to add and configure additional applications or instances if necessary. The device application configuration in this section does not provide the ability for full application configuration.

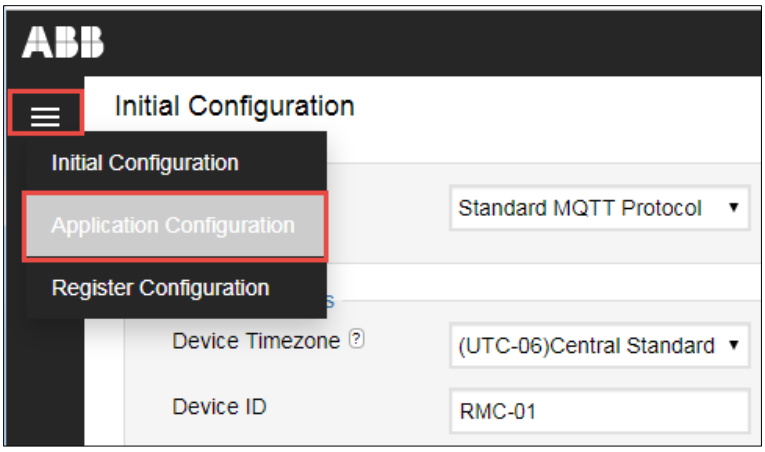
IMPORTANT NOTE: The Application Configuration web page does not display unless the device has established connection with the MQTT broker. Ensure you are connected to the broker.

8.1 Measurement and control applications

To select applications data is published for:

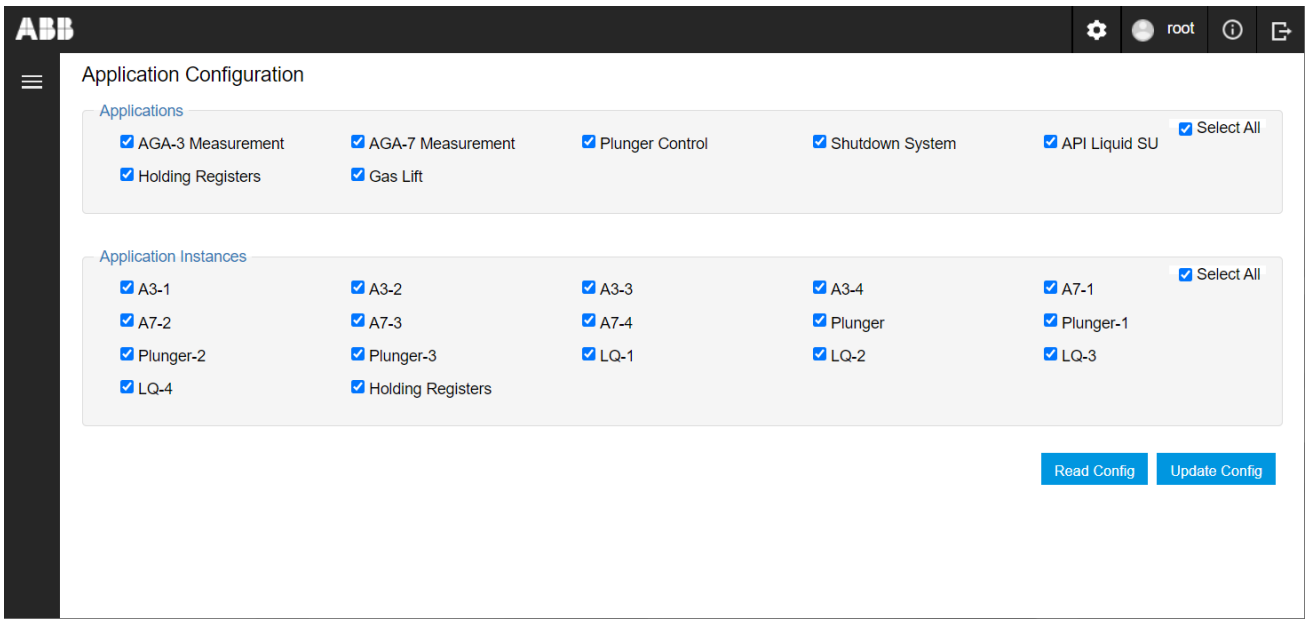
1. Click the menu icon on the left of the Initial Configuration screen and select **Application Configuration**.

Figure 8-1: Navigate to Application Configuration



2. On the Application Configuration screen, select specific applications and instances or keep the **Select All** option checked.

Figure 8-2: Application Configuration page

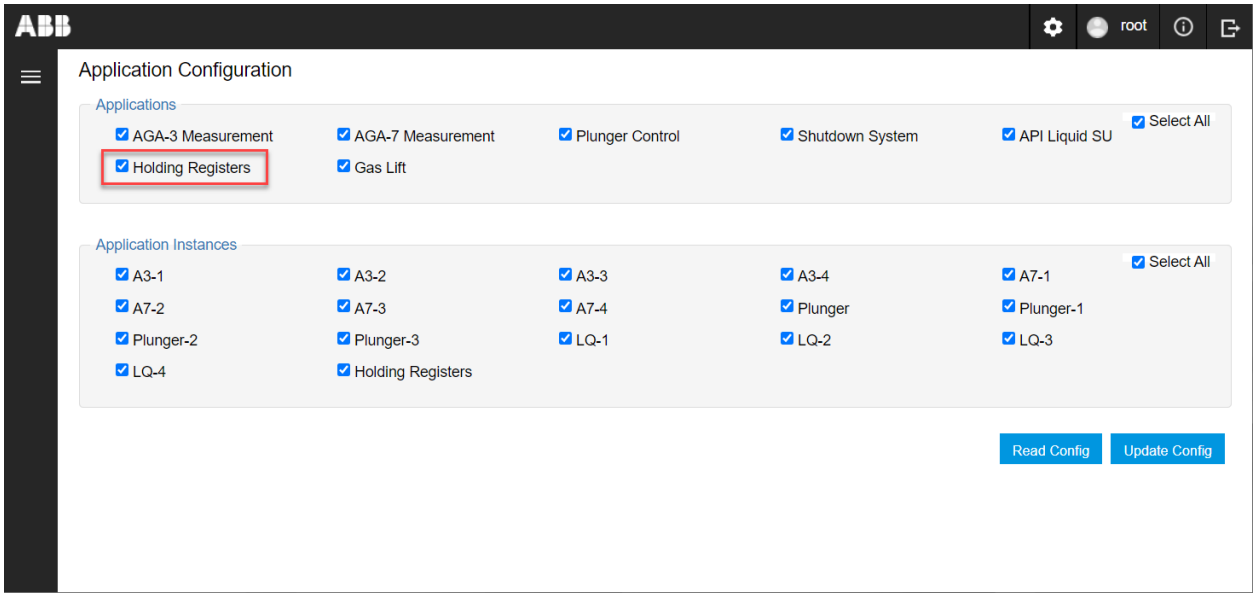


3. Click **Update Config** if you changed default selections. A confirmation for the update displays.
4. Click **Close** when the configuration update is successful.

8.2 Holding Registers application (private networks only)

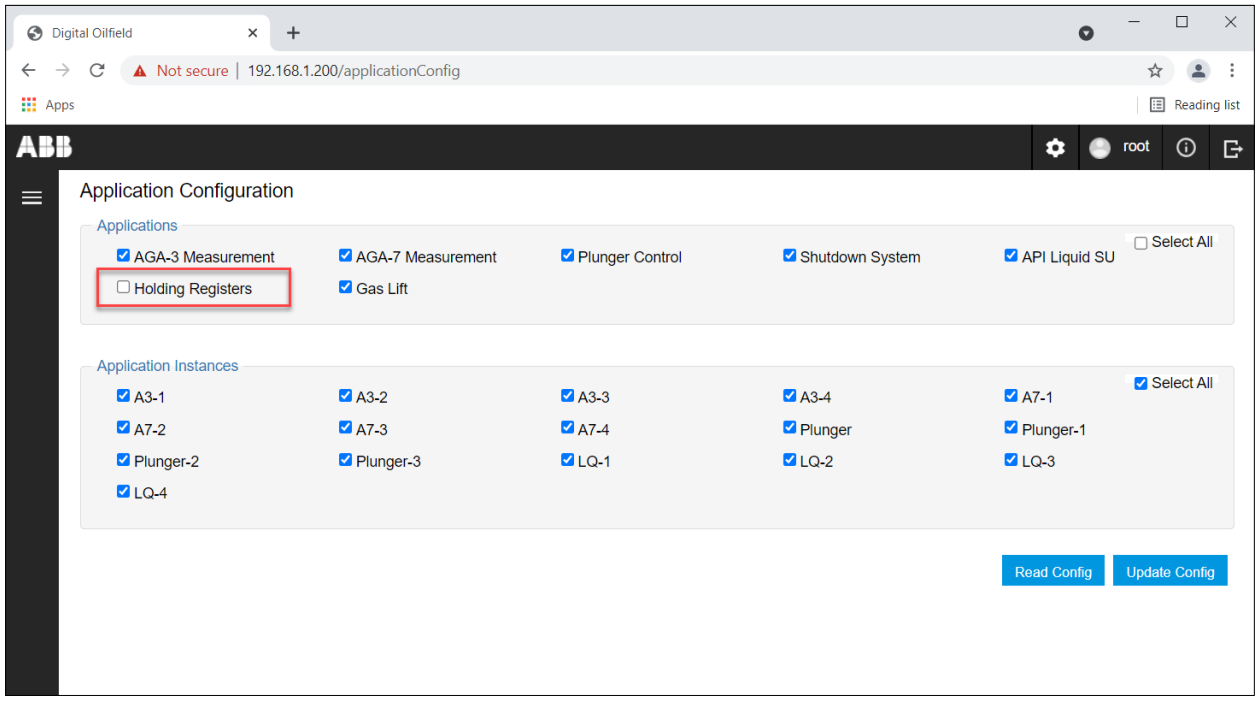
The Holding Registers application allows the user to custom define how to store values of interest in specific device register ranges. This application is customized per user requirements. The registers are not pre-defined as with the other supported applications.

Figure 8-3: Support for Holding Registers (private network only)



IMPORTANT NOTE: At time of this writing, this application is supported only in private customer implementations, not on service provider clouds or on systems connected to the internet. If you are connecting to a MQTT broker on the cloud, clear the Holding Register check box from the application configuration page to disable publishing by this application (Figure 8-4). The ABB Digital Oilfield does not support the Holding Register application and will not be able to display any data even if the application is enabled for publishing.

Figure 8-4: Disable Holding Register publishing (ABB Digital Oilfield customers)



9 Configure registers

Configure the registers that the device publishes data for. The device sends specific application register data through the broker.

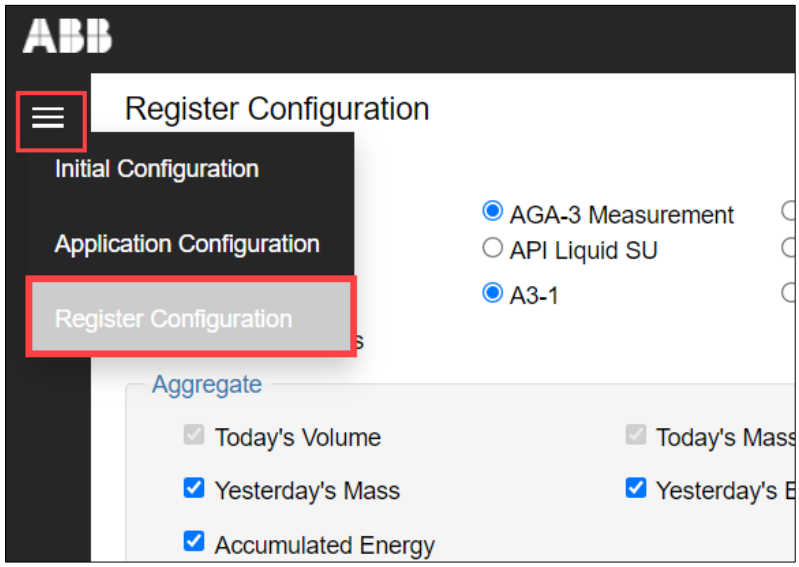
IMPORTANT NOTE: The Register Configuration web page does not display unless the device has established connection with the MQTT broker. Ensure you are connected to the broker.

9.1 Configure measurement and control applications

To select registers data is published for:

1. Click the menu icon and select **Register Configuration** (Figure 9-1).

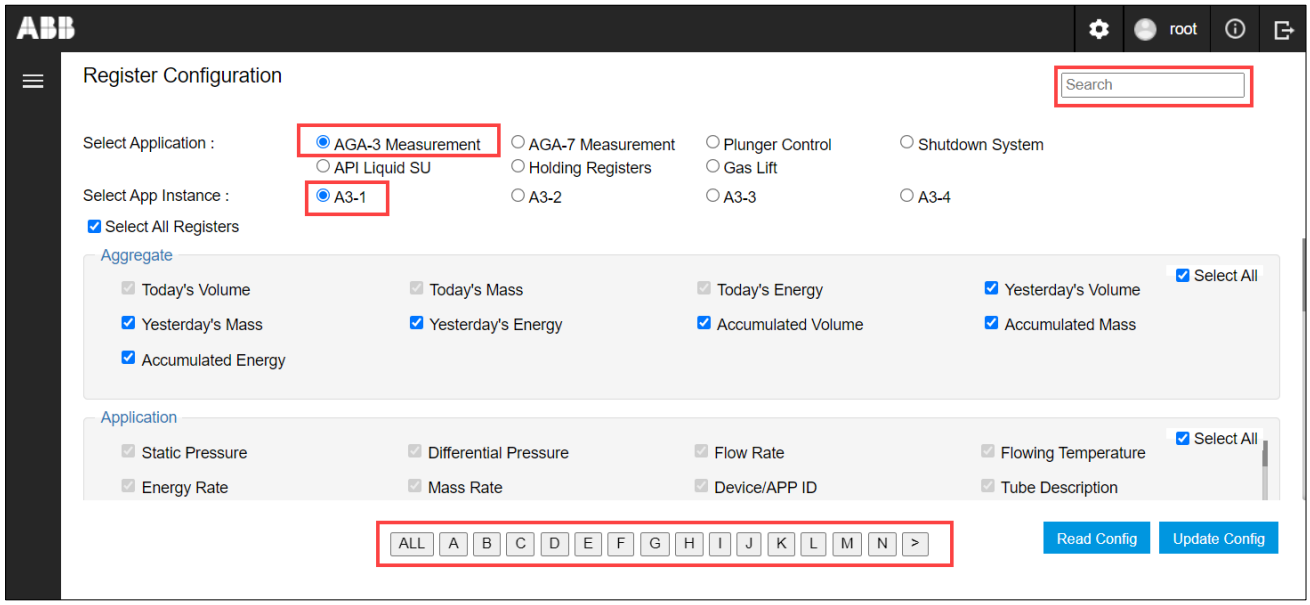
Figure 9-1: Navigate to Register Configuration



2. On the Register Configuration page (Figure 9-2), select the application and instance.

3. Select specific registers or click **Select All**. Use the search or pagination filters to locate specific registers if not selecting all registers.
4. Repeat steps 2-3 for each application instance.
5. Click **Update Config** if defaults are changed.
6. Click **Close** after update confirmation.

Figure 9-2: Register Configuration page



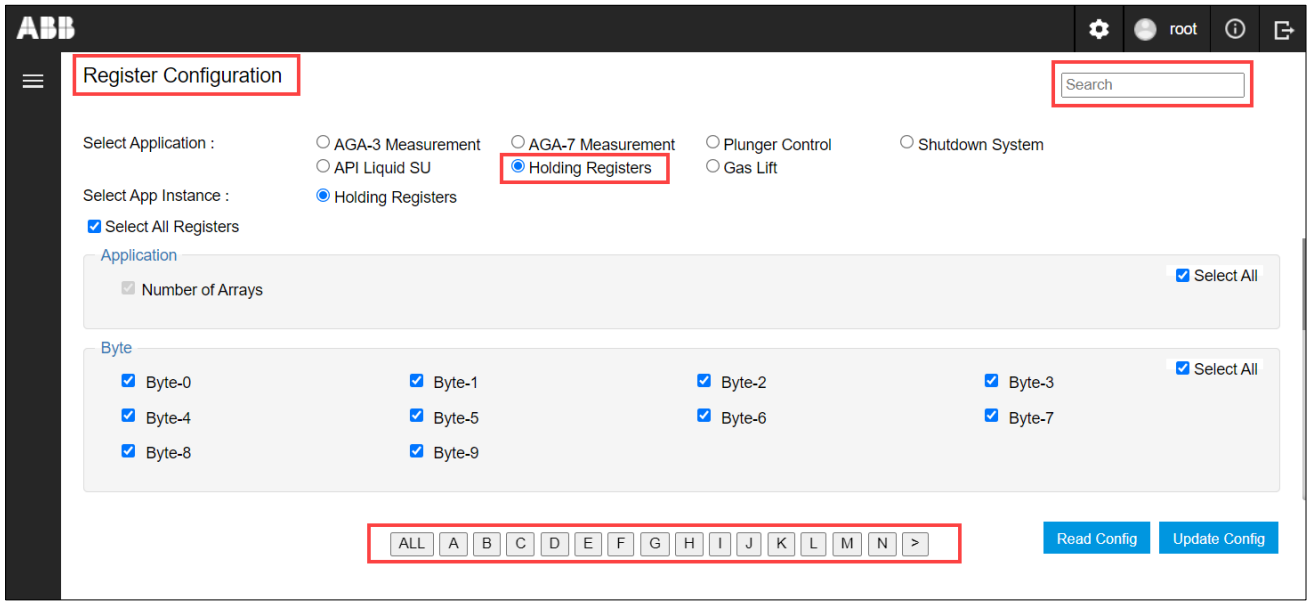
9.2 Configure Holding Registers

Holding Registers publish data based on the custom definitions.

To enable Holding Registers for publishing:

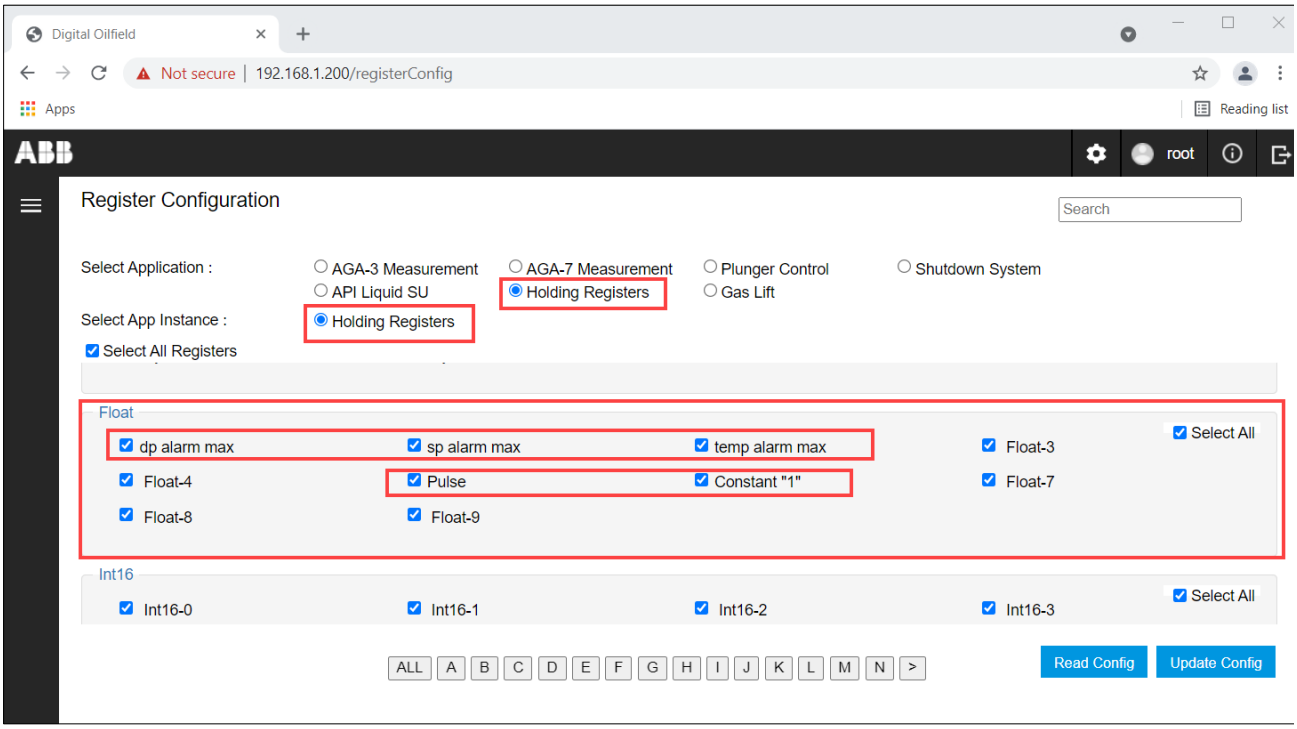
1. Select **Holding Registers** from the Register Configuration page.
2. Select the Holding Register application instance.
3. Leave the **Select All Registers** option checked to publish all data, or clear to select specific registers.

Figure 9-3: Configure Holding Registers



4. Select custom register definitions to publish specific data. Use the search or pagination buttons to locate specific registers or use the scroll bar to navigate the screen. In the example below, several custom definitions display. They can be selected to publish their values.

Figure 9-4: Select to publish



5. Click **Update Config**.
6. Click **Close** after the update confirmation.

IMPORTANT NOTE: Once all application and register configuration is completed, and the permanent broker is available for connection, make sure to configure the correct broker parameters before leaving the field. Verify the connection to the broker is successful.

10 Change default login configuration credentials

Once you have verified that the device-broker connection is successful, secure your device's configuration login credentials with private passwords before leaving the field.

To configure private passwords on default user accounts:

1. Navigate to the Initial Configuration page.
2. Click the settings icon and then **User Management** from the drop-down list.

Figure 10-1: Access User Management

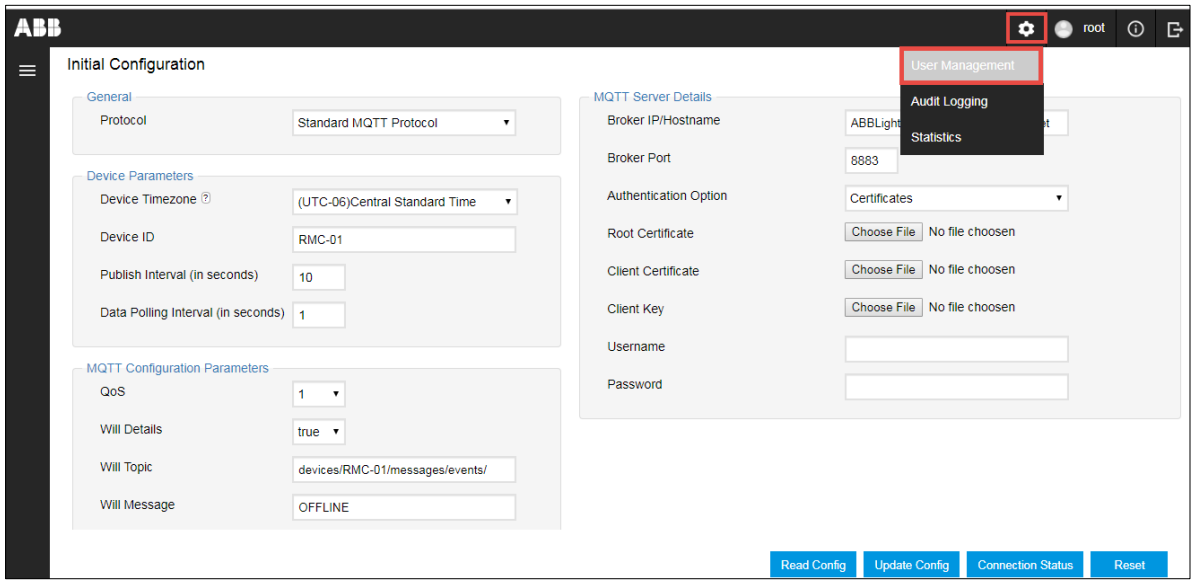
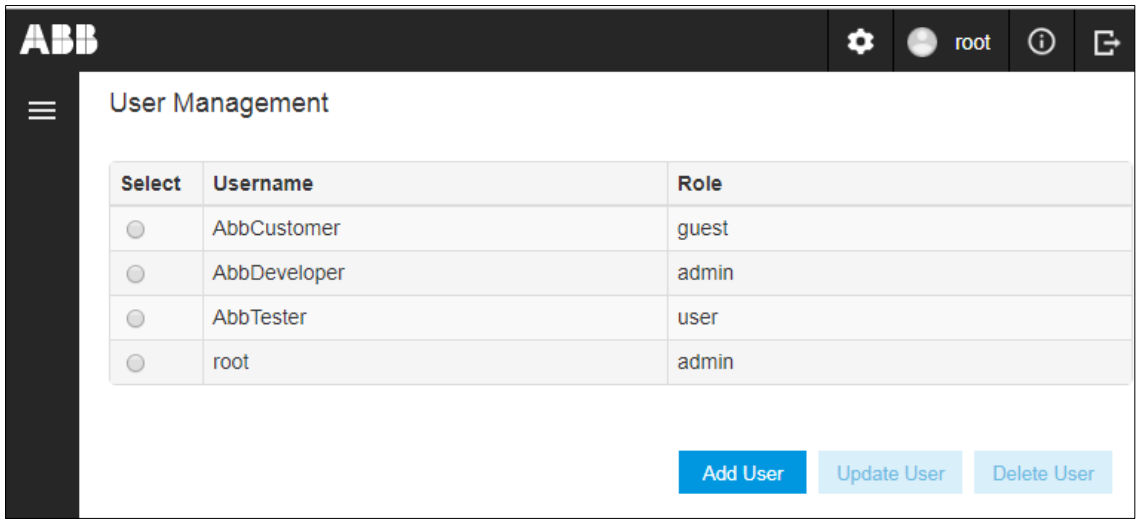


Figure 10-2: MQTT configuration interface - User Management



3. Select the user from the list on the User Management web page. The **Update User** and **Delete User** buttons activate.
4. Click **Update User**.
5. Update the password at the Update User dialog box. Use a private password known only to authorized users. Take note of the password used.
6. Click **Update**.
7. Repeat steps 3-6 for each default user.

11 Useful terms

Table 11-1 provides a general description of the terms used in this manual for quick reference. For technical details on protocol implementation, infrastructure components or cloud architecture definitions, consult standard committees' websites or other online resources.

IMPORTANT NOTE: Refer to online resources for the MQTT standard documentation at this link: http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf.

IMPORTANT NOTE: Refer to online resources for the Sparkplug protocol at this link: https://docs.chariot.io/display/CLD/Sparkplug+Specification.

Table 11-1: Useful terms

Term/Acronym	Description
ABB Ability™	A set of tools, software processes and data models available for each ABB cloud-based domain-specific solution. The Totalflow web applications are solutions specific for oil and gas upstream production and constitute one of the many ABB solutions offered on the cloud.
Cloud/Cloud Services	Hardware and software infrastructure enabling connectivity of devices, systems and processes across a large geographical area. Cloud solutions can be offered over proprietary vendor-owned infrastructures or over third-party service providers. ABB offers solutions over the Microsoft® Azure Platform or cloud services.
IoT	Internet of Things Hardware and software platforms supporting remote device integration for web-based access to device data and control capabilities
IIoT	Industrial Internet of Things The use of the Internet of Things platforms to support and enhance industrial and manufacturing processes such as factory or plan-floor control, automation, and other complex systems.
IoT Hub (device)	System on the cloud service platform processing communication with field MQTT clients (MQTT-enabled field devices)
MQTT	Message Queue Telemetry Transport (Standard MQTT) A client-server publish-subscribe messaging protocol for use on top of the TCP/IP protocol. This protocol enables connectivity and integration of field devices into the cloud. Packet payload for the standard MQTT protocol supports the ABB Ability format.
MQTT client	Functionality that performs the client role in MQTT communication. Typically implemented on field devices.
MQTT server	Functionality that performs the server role in MQTT communication. Typically implemented on systems serving as IoT hubs or MQTT brokers.
MQTT-enabled field device	ABB Totalflow devices with embedded capability to connect and communicate with an MQTT broker. These devices support the MQTT client functionality which requests connections to the broker and establishes the communication links for data transfer to and from the broker.
MQTT Broker	The system with the MQTT server functionality that authenticates and accepts connection requests, establishes communication links, and allows data transfer for MQTT clients.
MQTT Control packets	MQTT communication packets sent by client to server or server to client to establish the connection for the data transfer between the device and the cloud. MQTT has several types of control packet types: CONNECT, SUBSCRIBE, PUBLISH. Each of these packets has a specific function and format.
CONNECT packet	The first packet sent by the MQTT client to the MQTT server after the connection between the two is successfully established.

Term/Acronym	Description
PINGREQ (Ping request) packet	Packet is sent from a client to the server to: — Indicate to the Server that the Client is alive in the absence of any other MQTT Control Packets being sent from the Client to the Server — Request that the Server responds to confirm that it is alive — Exercise the network to indicate that the Network Connection is active This packet is used in Keep Alive processing.
PINGRESP (PING response) packet	Packet is sent by the server to the client in response to a PINGREQ packet. It indicates that the server is alive. This packet is used in Keep Alive processing.
DISCONNECT (Disconnect notification packet)	Final MQTT Control Packet sent from the client or the server before device-broker connection is closed
SUBSCRIBE (request) packet	Packet sent from the client to the server to create one or more subscriptions. Each subscription registers a Client's interest in one or more Topics. The Server sends PUBLISH packets to the Client to forward Application Messages that were published to Topics that match these Subscriptions. The SUBSCRIBE packet also specifies (for each Subscription) the maximum QoS with which the Server can send Application Messages to the Client.
UNSUBSCRIBE packet	Packet sent by the Client to the Server to unsubscribe from topics
PUBLISH packet	A PUBLISH packet is sent from a Client to a Server or from a Server to a Client to transport an Application Message.
Payload	The actual data in a packet or file minus all headers attached for transport and minus all descriptive meta-data. The payload format depends on the communication protocol used: MQTT or Sparkplug.
Topic	Topic Name that identifies the information channel to which payload data is published.
MQTT TCP port	TCP port number assigned for the MQTT protocol. TCP ports 8883 and 1883 are registered with IANA for MQTT Transport Layer Security (TLS) and non-TLS communication respectively. Port 8883 is recommended for secure connection.
Sparkplug	Communication protocol that enhances the standard MQTT protocol to support field device connection with real-time SCADA or IIoT systems. The Sparkplug packet payload format is different from the format used by standard MQTT. Sparkplug requires specific payload format definitions.

ABB Inc.

Measurement & Analytics
Quotes: US-IAMA.inquiry@us.abb.com
Orders: US-IAMA.order@us.abb.com
Training: US-IAMA.training@us.abb.com
Support: upstream.support@us.abb.com
+1 800 442 3097 (opt. 2)

Additional free publications are available for download at:
www.abb.com/upstream

Main Office - Bartlesville
7051 Industrial Blvd
Bartlesville, OK 74006
Ph: +1 918 338 4888

Kansas Office - Liberal
2705 Centennial Blvd
Liberal, KS 67901
Ph: +1 620 626 4350

Texas Office - Houston
3700 W. Sam Houston
Parkway S., Suite 600
Houston, TX 77042
Ph: +1 713 587 8000

Texas Office – Odessa
8007 East Business 20
Odessa, TX 79765
Ph: +1 432 272 1173

Texas Office – Pleasanton
150 Eagle Ford Road
Pleasanton, TX 78064
Ph: +1 830 569 8062

2106521MNAB