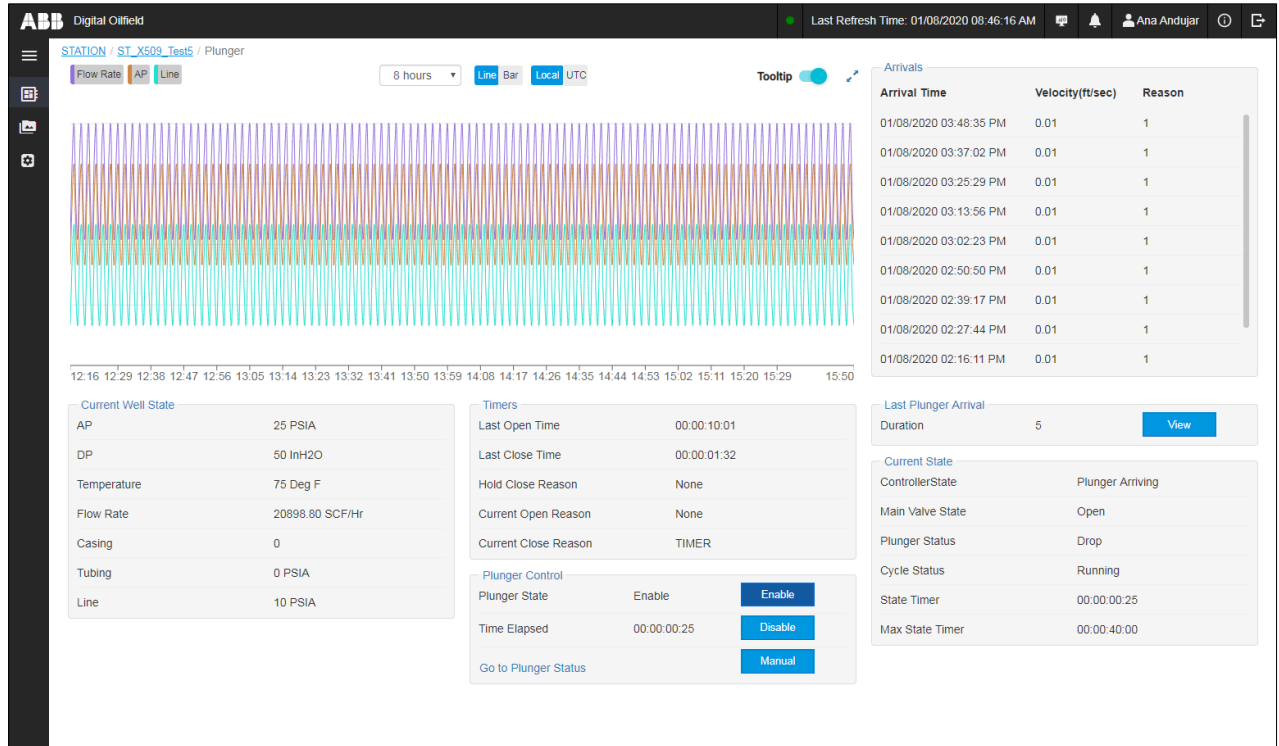


ABB Digital Oilfield User Manual

FOR IMPLEMENTATIONS USING THE RMC-100



Measurement made easy

Contents

Contents	2
Cyber security	6
Additional information	6
Safety	7
Potential safety hazards	7
1. Product description	8
1.1 Architecture.....	8
1.2 Core architecture components	9
1.3 MQTT-enabled Totalflow device description	10
1.3.1 Standard MQTT functionality	10
1.3.2 Sparkplug functionality.....	15
1.3.3 MQTT device configuration interface	16
1.4 Digital Oilfield application description	20
1.4.1 Supported browsers.....	20
1.4.2 Supported Totalflow applications.....	20
1.4.3 Home page.....	21
1.4.4 Device and application navigation tree view.....	22
1.4.5 General device information pages	24
1.4.6 Application pages	25
2 Prepare for device configuration	30
2.1 Prerequisites.....	30
2.2 Determine authentication method	31
2.2.1 Authentication methods.....	31
2.2.2 Prepare for authentication configuration.....	31
2.3 Register the device on the cloud.....	32
2.4 Device configuration overview	33
3 Initial device configuration	35
3.1 Access the Initial Configuration page.....	35
3.2 Configure the protocol.....	38
3.3 Configure device parameters.....	39
3.3.1 Device parameters for Standard MQTT protocol.....	41
3.3.2 Device parameters for Sparkplug	41
3.4 Configure MQTT parameters.....	42
3.4.1 MQTT configuration parameters for Standard MQTT protocol.....	44
3.4.2 MQTT configuration parameters for Sparkplug	44
3.5 Configure MQTT Server Details	45
3.5.1 MQTT Server Details for the Standard MQTT Protocol.....	47
3.5.2 MQTT Server Details for Sparkplug.....	49
3.6 Update configuration.....	51
3.7 Verify connection status	52
3.8 Reset device configuration	54

4	Device application configuration	55
4.1	Access the Application Configuration page.....	55
4.2	Enable application data publishing	56
4.3	Disable application data publishing.....	57
4.4	Update application configuration	57
5	Device register configuration	59
5.1	Access the Register Configuration page	59
5.2	Enable register data publishing.....	59
5.3	Disable register data publishing.....	61
5.4	Update register configuration	61
6	Troubleshooting device connection errors	63
6.1	User-device connection failure.....	63
6.1.1	Checklist to resolve failure to connect to field device.....	64
6.2	Device-Broker connection failure	64
6.2.1	Resolve failure to connect to cloud broker	66
6.2.2	Upload the last successful configuration	66
6.3	Advanced troubleshooting procedures	66
6.3.1	Verify processes from SSH.....	67
6.3.2	Collect logs using SFTP.....	71
6.4	Troubleshooting when using Sparkplug	79
7	Access the Digital Oilfield	81
7.1	Log into the Digital Oilfield.....	81
7.2	Navigate to devices and applications	82
7.3	View measurement application data	83
7.3.1	View application data	86
7.3.2	View aggregate data	88
7.3.3	View composition data	89
7.3.4	View digital outputs	91
7.3.5	View last calculated values.....	92
7.3.6	View custom Logs.....	93
7.3.7	View daily logs.....	95
7.3.8	View alarms.....	96
7.3.9	View alarm definitions.....	97
7.3.10	View trend definitions	97
7.3.11	View events.....	98
7.4	View control application data.....	99
7.4.1	Plunger Control application	99
7.4.2	Shutdown application.....	106
7.4.3	Gas Lift application	108
7.5	Access Plunger Analysis System (PAS) services.....	111
7.5.1	Access PAS options	111
7.5.2	Schedule analyses for pre-defined intervals.....	112
7.5.3	Schedule analyses for user-defined intervals (custom)	113
7.5.4	View Fault Detection reports	114

7.5.5	View Optimization reports	115
7.5.6	View wells with scheduled analyses	116
7.5.7	View well configurations	116
8	PAS access from the cloud interface	118
9	Totalflow device security	119
9.1	Device security guidelines.....	119
9.2	Secure connections.....	119
9.2.1	Field Local Area Network connections	121
9.2.2	Customer corporate network connections.....	121
9.2.3	Web user connections (access)	121
9.2.4	Monitor load on network connection	121
9.3	Secure access to the MQTT configuration interface	122
9.4	Open TCP ports on devices	126
9.5	Services on devices	126
9.5.1	User-enabled services	126
9.5.2	Device-enabled services for MQTT support	127
9.6	Device data protection for decommissioning	127
10	Administrator tasks for the device	129
10.1	Enable or disable MQTT functionality	129
10.2	Provide and manage certificates	131
10.3	Generate certificates for X.509 authentication	132
10.3.1	Using OpenSSL in Windows for self-signed certificates	132
10.3.2	Generate Self-signed certificates.....	133
10.3.3	Generate CA-signed certificates	137
10.3.4	Generate own root CA certificates	138
10.3.5	Generate other root CA certificates	139
10.4	Manage users	140
10.4.1	User Management web page overview	140
10.4.2	Default user accounts and role privileges	141
10.4.3	Access the User Management web page.....	142
10.4.4	Add User.....	143
10.4.5	Update User	145
10.4.6	Delete User	147
10.5	Monitor device audit logs.....	148
10.5.1	Audit Logging web page overview	148
10.5.2	Access the Audit Logging web page.....	150
10.6	Monitor device statistics	152
10.6.1	Access the Statistics web page	153
10.6.2	Device configuration statistics	154
10.6.3	Device-broker connection statistics	156
10.6.4	Sparkplug statistics	159
11	Administrator tasks on the Digital Oilfield	163
11.1	Device management	163
11.1.1	Access the device management web page.....	163

11.1.2	Reset device	164
11.1.3	Delete device	164
11.2	Monitor application audit logs	165
12	Administrator tasks on Azure®	167
12.1	Add and manage cloud users	167
12.1.1	Role privileges on the cloud	167
12.1.2	Password policy	168
12.1.3	Set up new user	168
12.2	Register field devices	168
13	Glossary	173
	Typographical conventions	175

Cyber security

The Digital Oilfield application integrates Totalflow products which are designed to be connected, and communicate information and data, via a network interface. All 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(s) and the customer network as well as a secured and controlled physical access to the hardware equipment, 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, the application of authentication measures, encryption of data, installation of antivirus programs, etc.) to protect the products, the network, its system and its 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 security breaches, unauthorized access, interference, intrusion, leakage and/or theft of data or information.

Although ABB provides functionality testing on the products and updates it releases, the customer should institute its 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, etc.) to ensure that the security measures the customer has implemented have not been compromised and that the system functions in the customer's environment as expected.



IMPORTANT NOTE: This manual includes cyber security topics and recommendations applicable to Digital Oilfield implementations. Refer to each device user manual for additional security details.

Additional information

Additional free publications for the device are available for download at www.abb.com/totalflow.

Figure 0-1: Related documentation

Documents	Document number
Configure MQTT How to Guide	2106521
RMC-100 User Manual	2105552
RMC-100 Startup Guide	2105551
Plunger Analysis System Administrator Guide	2105844
Advanced Ethernet Parameter Description	2105999

Safety

Potential safety hazards

The Digital Oilfield integrates and provides access to field devices running measurement and control applications. Procedures included in this manual describe:

- Instructions to enable new or existing devices for connection to a corporate network with access to IoT service provider's clouds.
- Instructions to access devices and their applications from the cloud

For first time installations, consult the device's manual for details about safety.

For applications that allow fine-tuning or parameter updates from the cloud, follow the precautions required by each application. Changes to control applications such as Plunger Control, Gas lift or Shutdown, must be done by experienced users to prevent personal injury, equipment damage or unintended production shutdown as a result of lost communication connections, configuration changes or submitted commands.

The following conventions are used throughout this document to bring attention to important information:



IMPORTANT NOTE: This symbol indicates operator tips, particularly useful information, or important information about the product or its further uses.



NOTICE – Equipment damage, loss of data or cybersecurity risk. This symbol indicates a potential for equipment damage, loss of data or another unintended outcome. Failure to observe this information may result in damage to or destruction of the product and/or other system components.

1 Product description

The ABB Digital Oilfield provides cloud-based monitoring and management of flow measurement and control applications on Totalflow devices. Customers can implement the digital field on the Microsoft® Azure platform. This solution integrates field devices and processes. It stores field device data on the cloud and supports both web-browser-based configuration and monitoring interfaces. It also supports data access services for the development of value-added applications by ABB or third-party system resellers.



IMPORTANT NOTE: See the [Glossary](#) for general descriptions of the terms used in this manual. For additional details or component descriptions, see section [1.2 Core architecture components](#).

1.1 Architecture

[Figure 1-1](#) shows a high-level view of the Digital Oilfield architecture. The Digital Oilfield (5) is defined and configured on the cloud service provider platform (4). Its foundation is the Message Queue Telemetry Transport (MQTT) network protocol which defines the communication and data flow for field devices and components on the cloud.

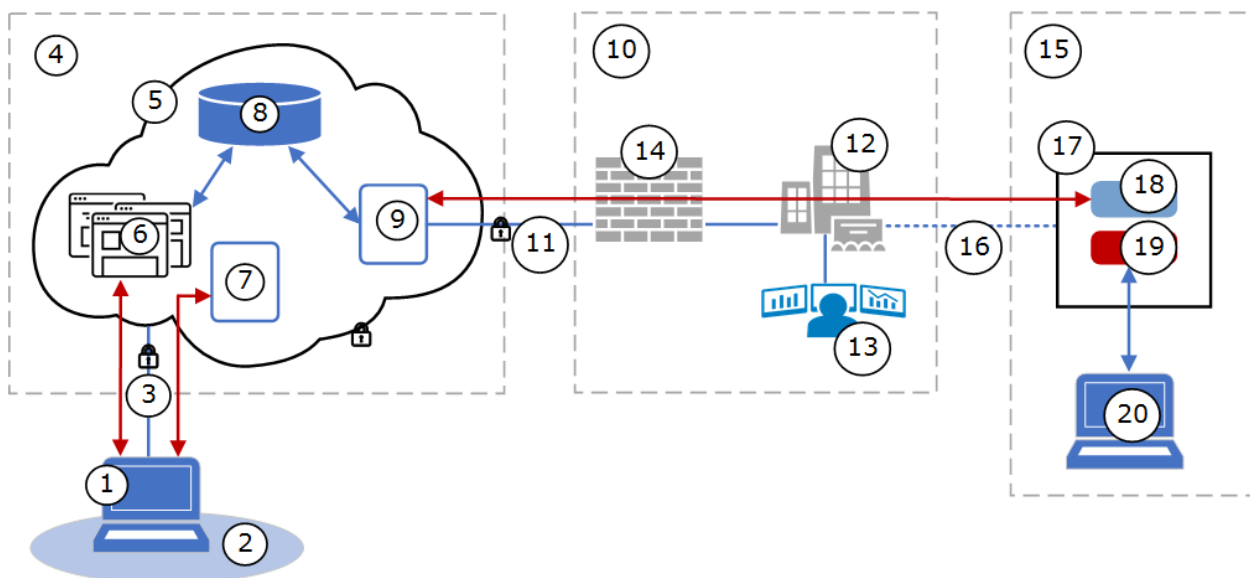
The main components of the Digital Oilfield are the cloud user interface or web application (6), storage for device data (8), and the MQTT broker (9). The main component at the remote customer site is the field device (17) with embedded MQTT functionality (18).



NOTICE – Cybersecurity risk. The field device (17) is not designed to be connected to the Internet directly. ABB strongly recommends that the device connects to the MQTT broker through an Edge gateway and firewall-protected corporate network (10). See additional details in section [9.2 Secure connections](#).

The corporate network must have a secure connection to the cloud (11) for protection of the data and communication traffic flow between the Totalflow device and the MQTT broker.

Figure 1-1: Digital Oilfield architecture



Legend for Figure 1-1: Digital Oilfield architecture

Customer access (1)	Cloud (4)	Customer network (10)	Remote site (15)
1 Web user with client system: PC/laptop or	4 Service provider network	10 Corporate VPN	15 Field Local Area Network

Customer access (1)	Cloud (4)	Customer network (10)	Remote site (15)
mobile devices			
2 Any remote user network (with access to the Internet)	5 Customer Digital Oilfield	11 Secure connection to Digital Oilfield	16 Secure connection to corporate network (may be wireless)
3 Secure connection to the cloud	6 Digital Oilfield interface (web app)	12 Operations center/field office	17 MQTT-enabled Totalflow device (may have additional equipment or peripherals connected, not shown)
	7 Plunger Analysis System (PAS)	13 SCADA/IIoT systems	18 MQTT-ready flash
	8 Database for data storage	14 Firewall	19 REST interface (web pages for device configuration)
	9 MQTT broker		20 Local user

1.2 Core architecture components

[Table 1-1](#) provides a high-level description of the major architecture components illustrated in [Figure 1-1](#) and their roles in the overall implementation.

i **IMPORTANT NOTE:** The Digital Oilfield is implemented over the Microsoft® Azure cloud which provides several layers of hardware and software technologies. Totalflow MQTT-enabled devices support standard functionality fully compatible with the Azure systems.

Table 1-1: Digital Oilfield architecture components

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. An MQTT-enabled device performs the role of the MQTT client. It requests and establishes connection with the MQTT broker. The device flash implements a REST server to support local or remote web-browser-based access to enable and configure its MQTT functionality. Refer to section 1.3 MQTT-enabled Totalflow device for additional details.
Cloud – core infrastructure (Microsoft® Azure)	MQTT Broker	The MQTT broker performs the role of the MQTT server. Enables secure MQTT-protocol-based connection of field devices to the cloud. The successful device-MQTT broker connection allows the device to send (publish) data to the MQTT broker.
	Cloud Data Storage	Cloud service data repository for Totalflow data (Figure 1-1 : Item 10). Real-time and historical values generated by Totalflow devices, device and application data, alarms and events data.

Location	Components	Description
Cloud – Web applications	Digital Oilfield Application	Totalflow web application hosted on the cloud for monitoring, data collection, and analysis for a suite of Totalflow measurement and control applications Refer to section 1.4 Digital Oilfield application description for additional details.
	Plunger Analysis System (PAS)	Totalflow web application hosted on the cloud for optimization of the Plunger lift application. PAS provides optimization, monitoring and training for sites using plunger control.
	Other value-added ABB and third-party applications	Other applications hosted on the cloud and developed by ABB or third-party vendors to meet specific customer requirements or enhance existing data analysis or device management needs.
Customer system/client	Web browser	<ul style="list-style-type: none"> – Access to the device configuration interface to configure the MQTT functionality. – Access to the cloud user interface
	PCCU	Existing host-based user interface to the Totalflow device family. Supports full device configuration and operations. All applications supported on the cloud interface must be configured from PCCU.



IMPORTANT NOTE: Detailed information about the Azure cloud devices, services, and architecture are beyond the scope of this manual. Administrators responsible for setting up cloud access and device management for their technicians must become familiar with Azure services, requirements, and contractual agreements.

1.3 MQTT-enabled Totalflow device description

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 the cloud.

- To review basic operation of communication protocols supported by Totalflow, see section [1.3.1 Standard MQTT functionality](#) or section [1.3.2 Sparkplug functionality](#).
- To review the configuration interface, see section [1.3.3 MQTT device configuration interface](#).



NOTICE – Cybersecurity risk. The following sections assume that the device-MQTT broker connection is established through the customer’s corporate network, not through a direct connection to the cloud. It is assumed that the corporate network provides connections through an edge gateway and has firewall-protected access to the cloud. Totalflow devices must not be connected directly to the Internet. See additional details in section [9.2 Secure connections](#).

1.3.1 Standard MQTT functionality

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 the cloud 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 Totalflow MQTT stack implementation is standards-compliant. The following sections provide a very 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 [13 Glossary](#) for basic terminology descriptions. If you are familiar with the MQTT standard and its principles of operation, skip this section and proceed to the configuration sections of this manual.



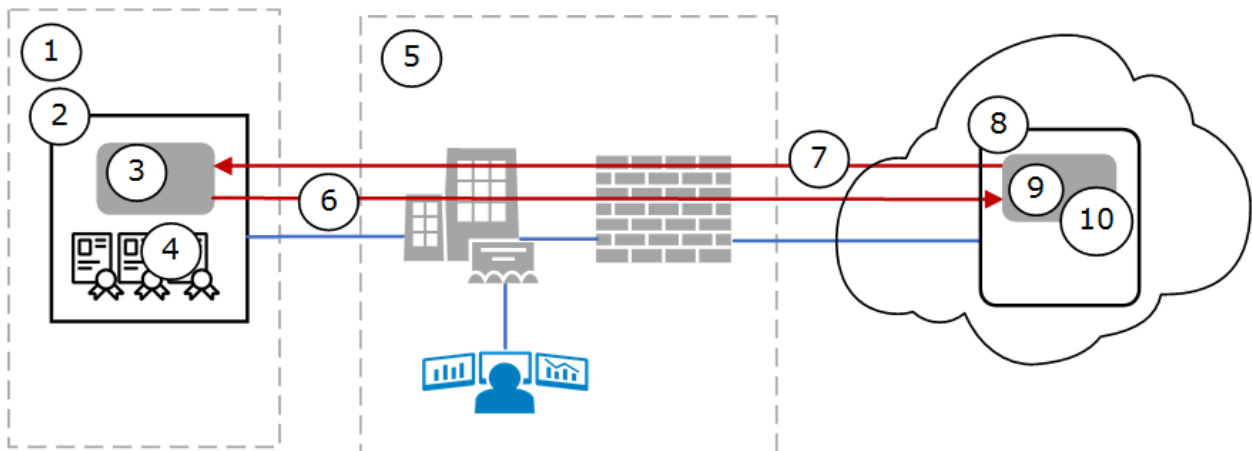
IMPORTANT NOTE: For simplicity, the diagrams in the following sections show the MQTT functionality and data flow for a single device only. The Digital Oilfield is designed to support many devices located across different field sites. The scale of the implementation depends on the customer’s specifics,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

1.3.1.1 Connect

[Figure 1-2](#) 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 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 as required by the cloud service provider, for example Azure).
 - The request must present valid authentication details such as valid credentials or certificates. Certificates 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 from the cloud and available for monitoring or configuring as necessary.

Figure 1-2: MQTT device-broker connection



Legend for Figure 1-2: MQTT Device-Broker connection

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

1.3.1.2 Subscribe

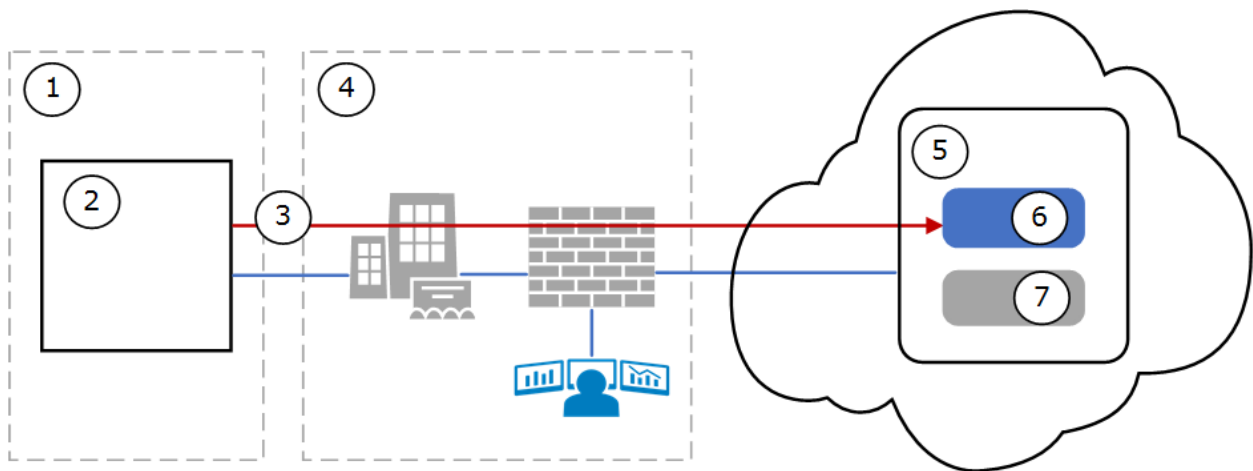
[Figure 1-3](#) shows a simplified view of the device subscription to the broker (5). The device subscribes to the subscription topic (6) on the broker to support device parameter updates from the cloud user interface (See [1.3.1.3 Update](#)).

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.

Note that the subscription topic is different from the publish topic (7). The subscription topic is used by the broker to distribute data from the cloud application to the subscribed devices (device-bound data flow). The publish topic is used by the broker to send data updates to the cloud application (cloud-bound data flow).

IMPORTANT NOTE: Each device subscribes to the following topic:
/devices/<Device-ID>/messages/devicebound/+.

Figure 1-3: Device subscription



Legend for Figure 1-3: Device subscription

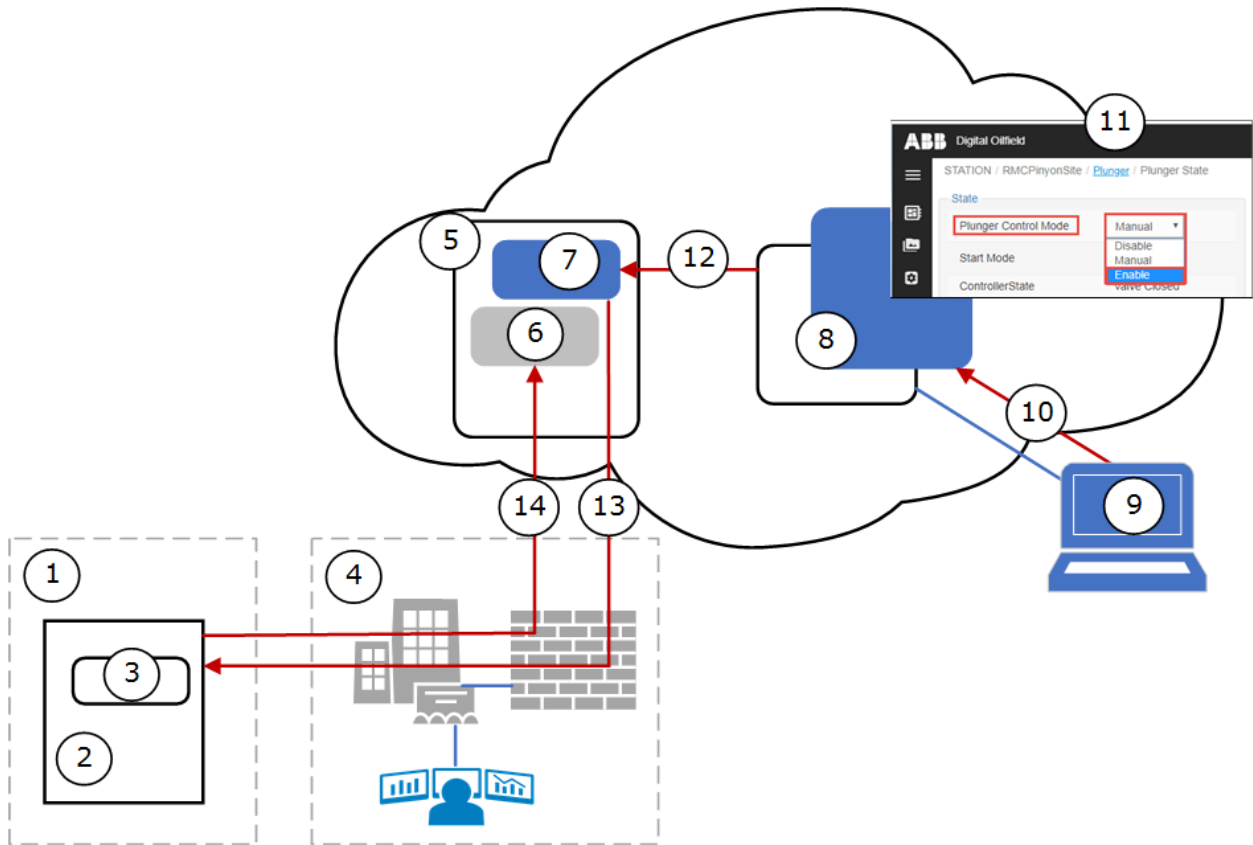
Field device on site	Customer private network	Cloud service provider
1 Field Local Area Network	4 Corporate network	5 MQTT broker
2 Totalflow device (unique ID)		6 Device subscription topic
3 Subscribe to topic on broker		7 Device publish topic

1.3.1.3 Update (register-write)

[Figure 1-4](#) shows a simplified view of how a parameter update submitted from the cloud application is handled across the cloud. The device must be subscribed to receive update requests from the broker (See [1.3.1.2 Subscribe](#)). Users (9) on the cloud 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
- 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 (14) the data to reflect the change. See section [1.3.1.4](#) for details on the publish process.

Figure 1-4: Parameter update



Legend for Figure 1-4: Parameter update

Field device	Customer private network	Cloud service provider	Remote access
1 Field Local Area Network	4 Corporate network	5 MQTT broker	9 Client system (PC/laptop): User logged into the cloud portal and on the device application page
2 Totalflow device	13 Broker sends the parameter change message to the device. Device updates the parameter value.	6 Device subscription topic	10 Application parameter update (Example: Change Plunger Control Mode value from Manual to Enable).
3 Totalflow device application data (register data or records)	14 Device publishes updated parameter value back to the cloud to ensure cloud application displays updated value (see Figure 1-5).	7 Device publish topic	11 User submits parameter change
		8 Digital Oilfield portal and device application page (Example: Station/RMC-1/Plunger-1/Plunger State)	
		12 Cloud application sends change request or command to broker. Request publishes on device	

topic.

1.3.1.4 Publish

Table 1-2 describes the type of data that Totalflow devices publish for each of the applications supported from the cloud.

Table 1-2: Data published

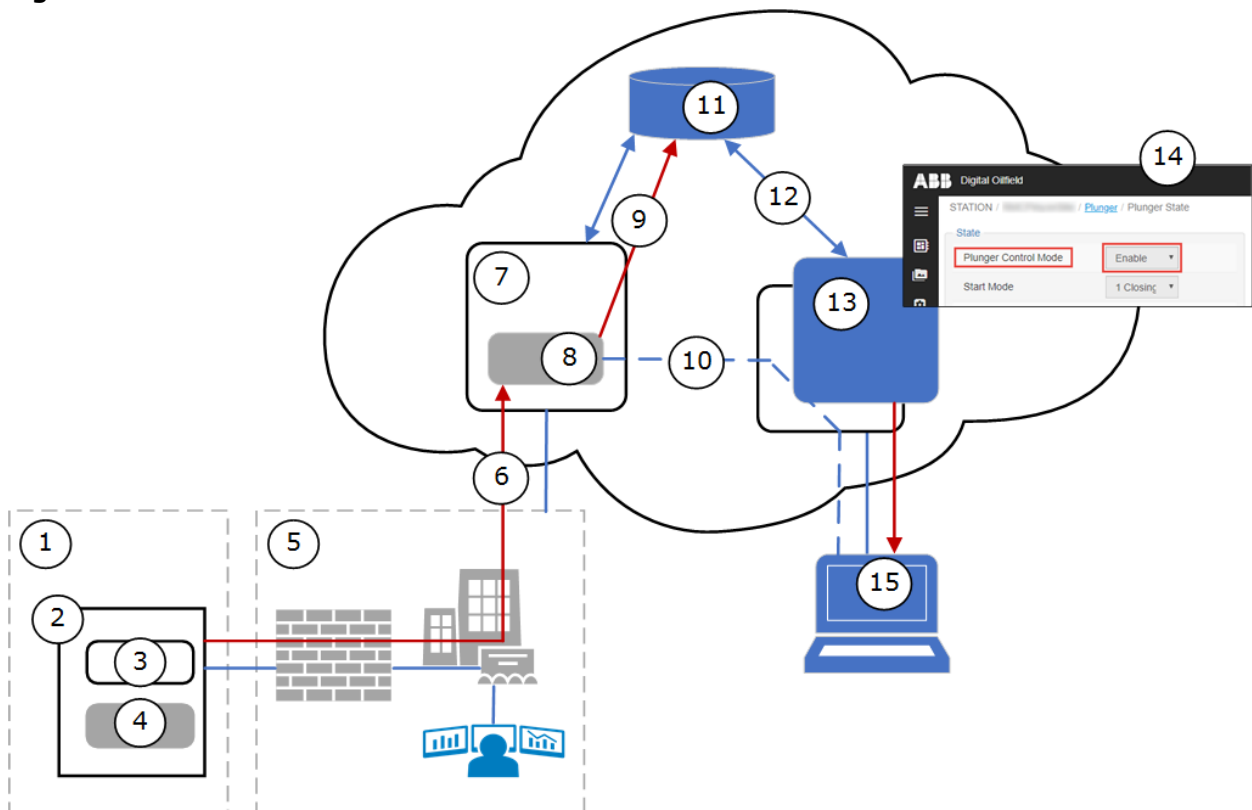
Data type	Description
Application Records	General application information sent by the device at first-time boot or after reboot Information such as enabled registers (registers the device publishes data for) and various records such as Alarm, Trend, Daily Logs, Custom Logs and Events.
Application Register Data	Specific application register values for the Totalflow applications supported on the cloud.

Figure 1-5 shows a simplified view of how the device publishes its data:

- The device (2) sends a publish message (6) with its data to the MQTT broker (7). The device data on the publish topic (8) is identified by unique device ID.
- The broker forwards the device data (9) to the encrypted cloud database (11) for storage.
- The cloud application (13) refreshes the data displayed in the applications pages (14) with the data stored on the database. Data in the database remains up-to-date so web pages reflect current data.

IMPORTANT NOTE: The publish topic (8) is used by the broker to send data updates to the cloud application (cloud-bound data flow). Each device publishes its data on a single topic: /devices/<Device-ID>/messages/events/.

Figure 1-5: Data Publish



Legend for Figure 1-5: Data Publish

Remote site	Customer private network	Cloud service provider	Remote access
1 Field Local Area Network	5 Corporate network	7 MQTT broker	15 Web-user views updated values on application page
2 Totalflow device (RMC with unique device ID)	6 Device publishes data to broker on device topic	8 Device subscription topic	
3 Totalflow device application data (register data or records)		9 Broker sends update to database	
4 Unique device ID		10 Broker notification to client	
		11 Cloud database stores data	
		12 Cloud application updates parameters	
		13 Digital Oilfield portal and device application page (Example: Station/RMC-1/Plunger-1/Plunger State)	
		14 Application page presents updated parameters (Example: Plunger control mode value changed from Manual to Enable).	

1.3.2 Sparkplug functionality

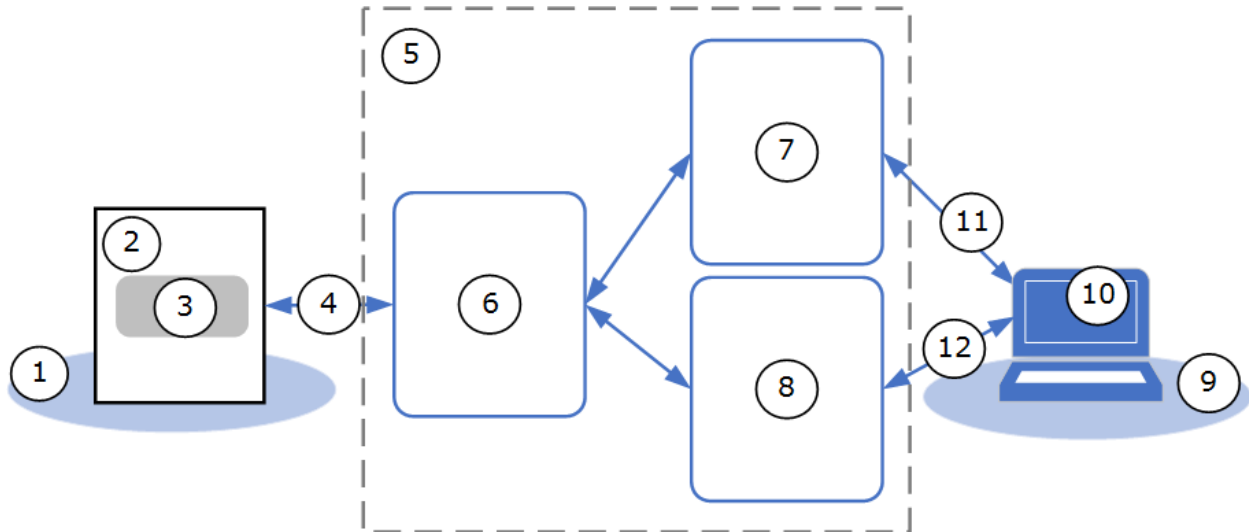
MQTT-enabled devices support Sparkplug B to connect to SCADA or IIoT systems. Sparkplug enhances the standard MQTT protocol to better support the real-time requirements of these systems.

IMPORTANT NOTE: The implementation of the SCADA/IIoT system depends on specific customer requirements and available network topologies. Customers may also implement their solutions end-to-end on their own private networks if not using MQTT brokers on a service provider cloud. In these scenarios, the MQTT broker/server is managed by the customer. 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 1-6 shows a simplified diagram 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 guarantees to support 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 section [10.6.4 Sparkplug statistics](#).

Figure 1-6: Sparkplug high level architecture



Legend for Figure 1-6: Sparkplug high level architecture

Field site	Customer network	Customer access
1 Field Local Area Network	5 Customer corporate network (VPN)	9 Field office network with secure access
2 Totalflow device	6 MQTT 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 1-6](#) does not show any databases or other services. Databases are typically implemented on-premise for data storage.

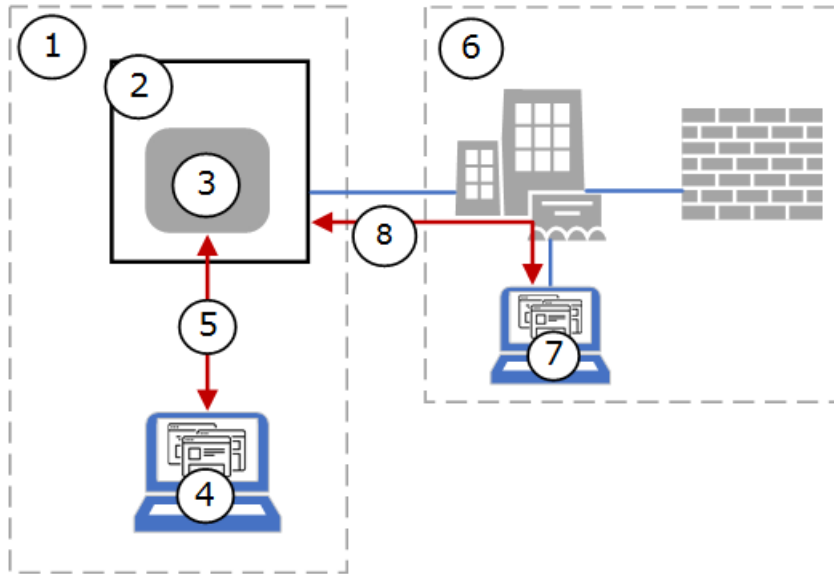


IMPORTANT NOTE: MQTT servers supporting sparkplug must be MQTT v3.1.1 compliant. MQTT servers may be referred to by other names, depending on the vendor implementing them. This manual uses the generic term “server” to indicate the main functionality or role of this component in the overall architecture.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

1.3.3 MQTT device configuration interface

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 1-7](#) 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 1-7: Device user interface for MQTT operation



Legend for Figure 1-7: Device user interface for MQTT operation

Local configuration	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
4 Client system: PC/laptop with browser	
5 Connection for local configuration	

1.3.3.1 Supported browser

The Chrome browser provides access to the device’s MQTT configuration web pages. See the versions supported in [Table 1-3](#).

i **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 1-3: Supported web browser on configuration interface

Browser	Version
Chrome browser	49 or higher

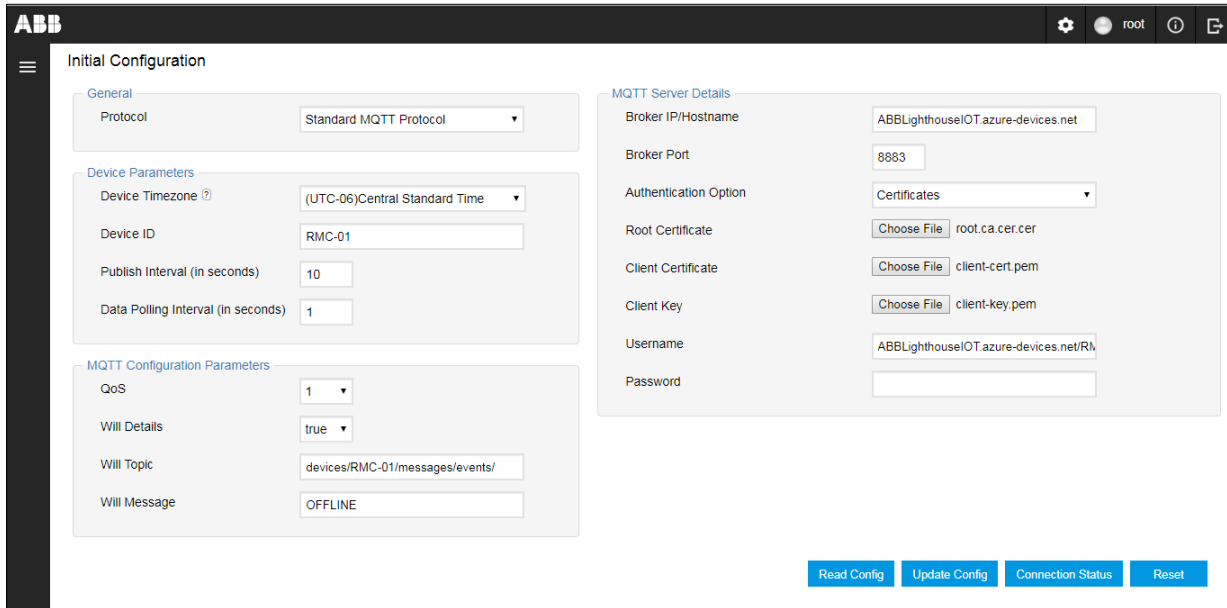
1.3.3.2 Initial Configuration page

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

[Figure 1-8](#) 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 1-8: Initial configuration web page



1.3.3.3 Application Configuration page

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

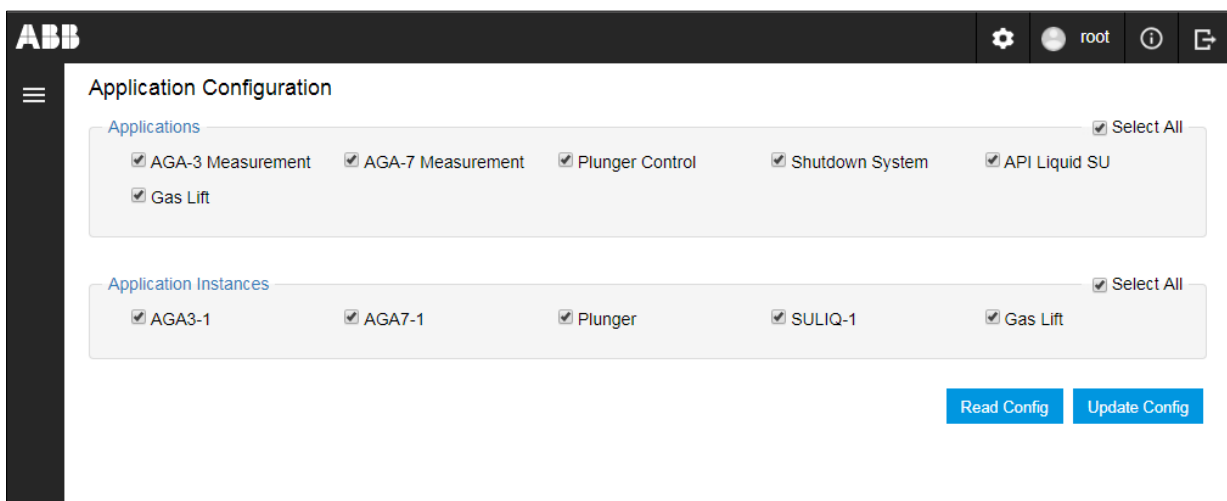
[Figure 1-9](#) shows the Application Configuration web page with the list of applications and application instances configured in the field device. Use checkboxes to configure preferences:

- 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 1-9: 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.

1.3.3.4 Register Configuration page

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

[Figure 1-10](#) 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.

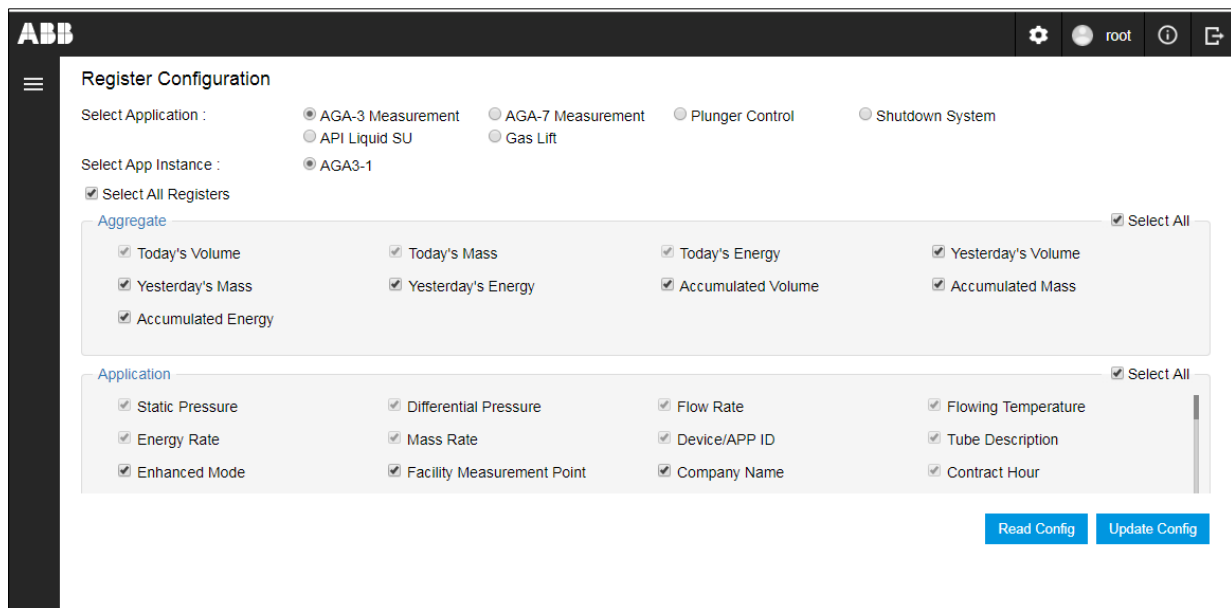
Options to configure register data publishing:

- 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.

Function buttons are available to view and update configuration:

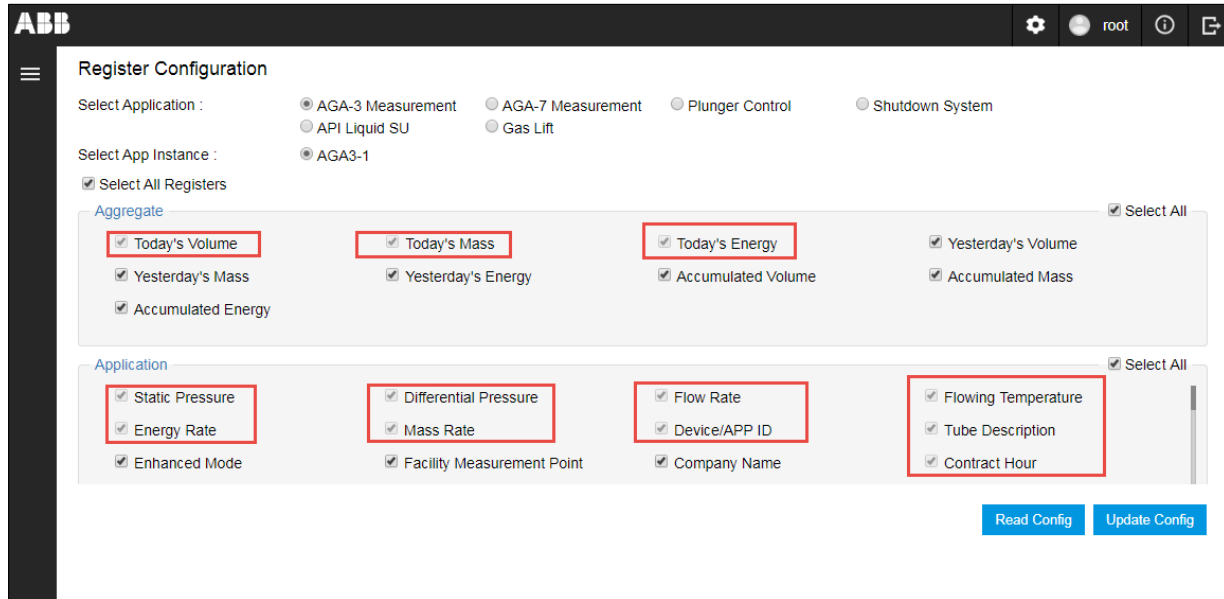
- Read config: retrieves and displays current register selections for publishing.
- Update Config: saves new register selections for publishing after updates.

Figure 1-10: 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 1-11](#)).

Figure 1-11: Required registers examples (read-only)



1.4 Digital Oilfield application description

The Digital Oilfield application is an ABB web application hosted on the Azure platform. It provides remote (web) access to Totalflow devices' application data.

The interface provides web pages with device application data, status information, and services. This section provides an overview of page organization, screen elements and functions to navigate the interface. For access to specific applications, see section [7 Access the Digital Oilfield](#).

For access, use systems with browser versions listed in section [1.4.1 Supported browsers](#). To determine what applications are supported on the cloud, see section [1.4.2 Supported Totalflow applications](#).

1.4.1 Supported browsers

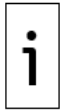
Access to the cloud is web-browser-based. Make sure the device you access the cloud from supports the browser type and versions listed in [Table 1-4](#).

Table 1-4: Supported web browsers on the cloud application

Browser	Version
Chrome	49 or higher
Edge	14 or higher
Firefox	54 or higher
Internet Explorer (IE)	11 or higher
Safari	10 or higher

1.4.2 Supported Totalflow applications

[Table 1-5](#) lists the Totalflow applications supported on the cloud interface. 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 [1.3.3.3 Application Configuration page](#)). Alarm data and trends are published for all supported applications if defined and configured from PCCU.

Table 1-5: Totalflow application supported on the cloud

Application	Description	Cloud function/features
Alarm system	Alarm detection, logging, and reporting application	Displays alarms and alarm definitions.
Trend system	Data trending application	Displays trend definitions. It uses defined trend variables for graphical display.
AGA3	Orifice gas measurement application	Displays data
AGA7	Linear gas measurement application	Displays data
API Liquid SU	Linear liquid measurement	Displays data
Plunger control	Control of a plunger on a production well	Displays data and provides some basic control
Gas lift	Artificial lift for wells with liquid loading problems	Displays data
Shutdown System	Shutdown a well or site	Displays data

1.4.3 Home page

After device configuration, successful connection, and registration on the cloud, customers can view and manage each of their devices and their applications.

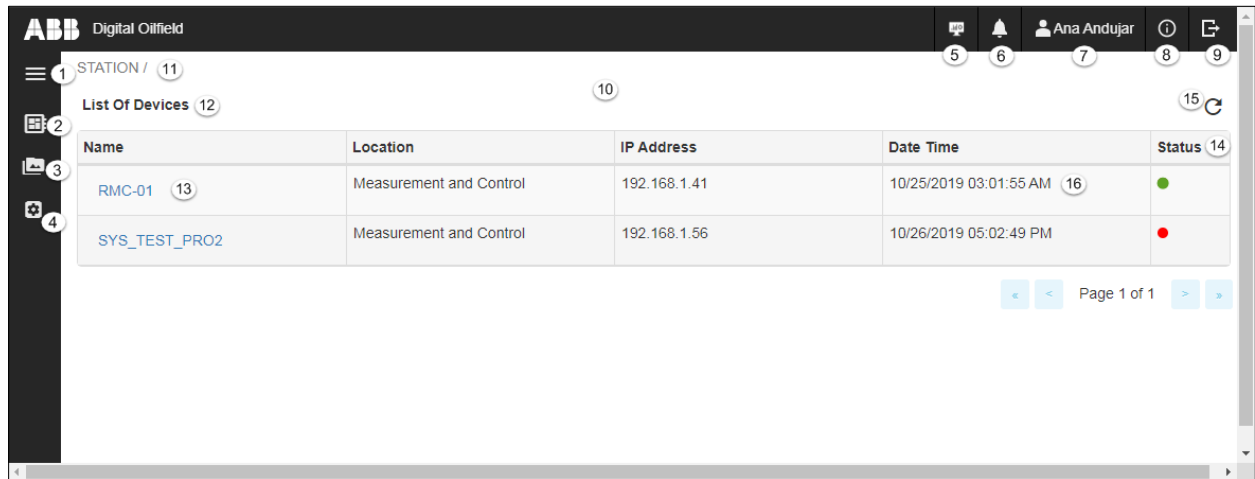
[Figure 1-12](#) shows the Digital Oilfield home page that displays after login. This page presents a device directory with all the registered devices, general information and indicators for device status.

Common functions are available for all pages at the top and left bars (see the legend below the figure for detailed descriptions). Icons 1 through 9 in [Figure 1-12](#) provide links to navigate to different application pages, service options, and management pages for administrator-role users.

Specific functions may be available on the main screen area (10) and depend on the information or application displayed.

On the home page, the device names are links to additional information pages with device-specific data. Use the navigation path (11) to return to the home screen from any of the device-specific pages. The refresh icon (15) updates screen information to display new devices, existing device updates or status change (14). An updated screen should reflect the time stamp of the last data update for each device.

Figure 1-12: Digital Oilfield main page



Legend for Figure 1-12: Digital Oilfield main page

Item	Description	Item	Description
1	Displays additional icons on the left bar.	9	Log out from the cloud
2	Displays devices and applications in navigation-tree format.	10	Main screen area
3	Displays PAS service options in navigation-tree format.	11	Screen navigation path
4	Admin users only. Displays device management page.	12	Data or information. For example, the main screen displays the list of devices available for monitoring from the cloud.
5	Link to third-party PAS portal	13	Device names (link to display additional information)
6	Well notes: Displays area where logged-in users can write or leave messages or notes. Other users can read those notes when they log in. Notes record the username of the note creator and the time stamp.	14	Status: Indicates if a device is connected and available from the cloud. Green: connected/accessible Red: disconnected
7	Logged-in user	15	Refresh
8	Displays cloud interface version	16	Time stamp of last data update

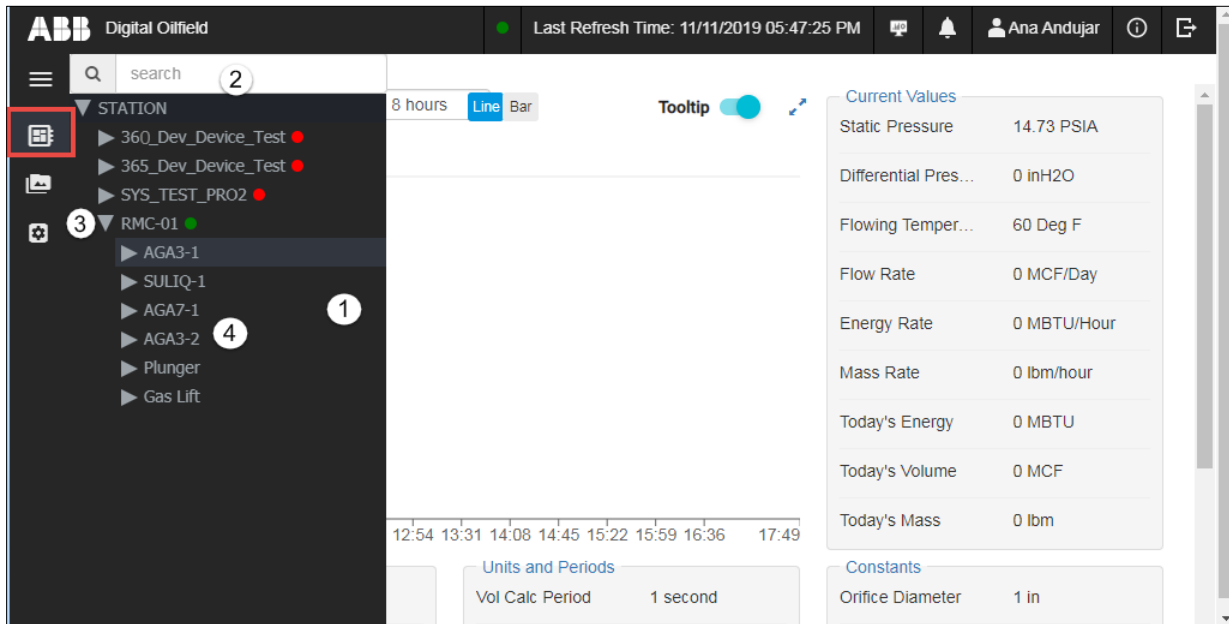
1.4.4 Device and application navigation tree view

[Figure 1-13](#) displays the device and application tree (1). This view shows the location of registered devices and their applications. Expand navigation tree items to display all available pages. Collapse items to have a higher-level view.

Locate the device of interest using the scroll bar to navigate up or down the tree or use the search box (2). The search box provides a quick way to locate a device in large implementations.

Select a device or an application to display data of interest in the main screen area.

Figure 1-13: Device and application navigation tree



Legend for Figure 1-13: Device and application navigation tree

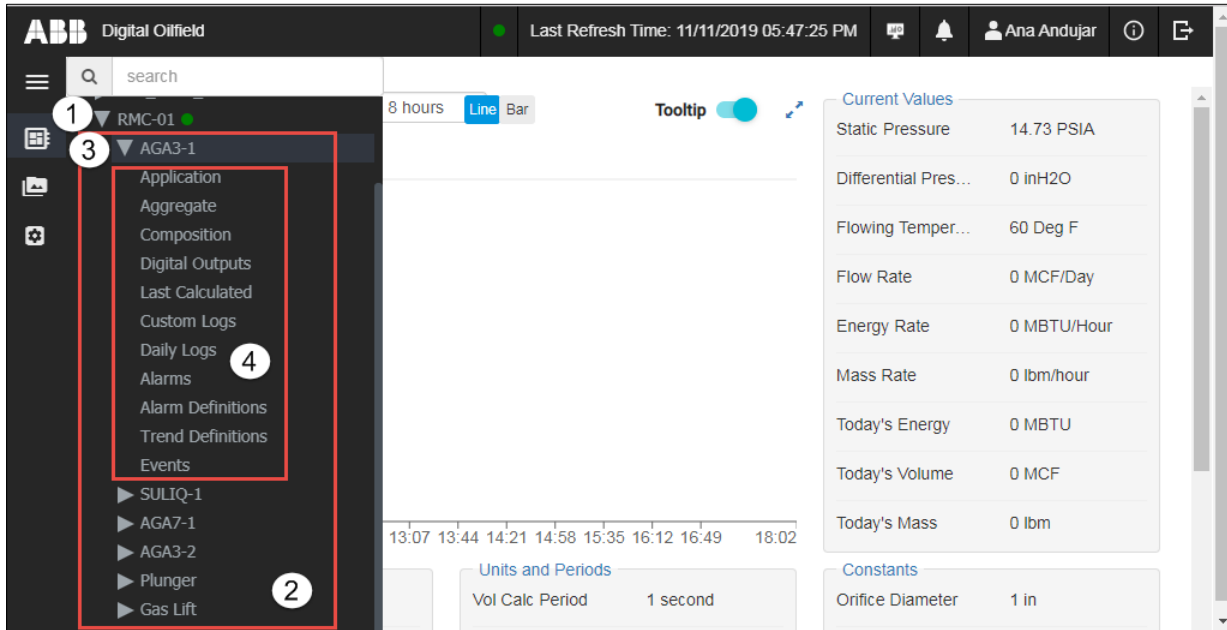
Item	Description	Item	Description
1	Navigation tree	3	Device
2	Search box	4	Device applications

1.4.4.1 Data organization and categories

The cloud user interface displays device data based on the applications enabled on the device and the specific data selections.

The navigation tree organizes application web pages in categories based on the type of information displayed. [Figure 1-14](#) shows all the applications (2) on a field device (1). The device might have several instances of the same application type. For example, two AGA3 measurement application instances show as AGA3-1 and AGA3-2 on the tree. Each application or application instance has several data categories (4). Select any of the application pages to display the data in the main screen area.

Figure 1-14: Device application instances



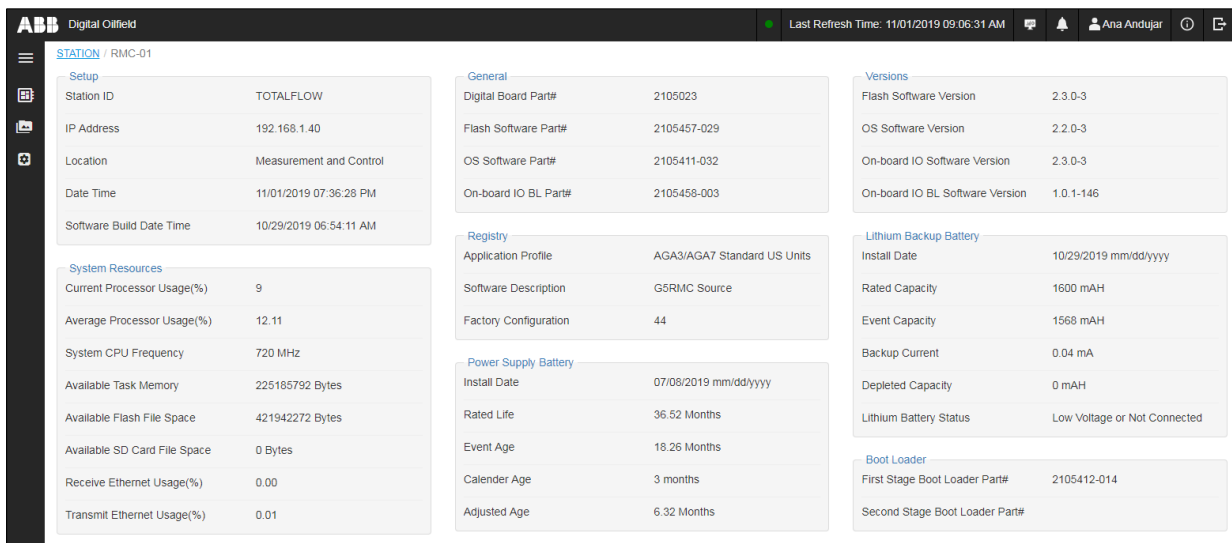
Legend for Figure 1-14: Device application instances

Item	Description	Item	Description
1	Device	3	Application instance
2	Device applications	4	Application instance data categories

1.4.5 General device information pages

Selecting a device from the home page or from the navigation tree displays general information specific to the selected device. [Figure 1-15](#) shows this type of information: basic parameter setup, system resources, hardware and embedded software part number and versions, etc.

Figure 1-15: General device information page



1.4.6 Application pages

The main screen area ([Figure 1-16](#)) displays the data for the selected device or application. The presentation and format of the data in this screen varies depending on the data displayed and the functions available.

Application pages display when an application instance or application instance category is selected from the tree view. Each application instance has a main application or landing page and specific data pages:

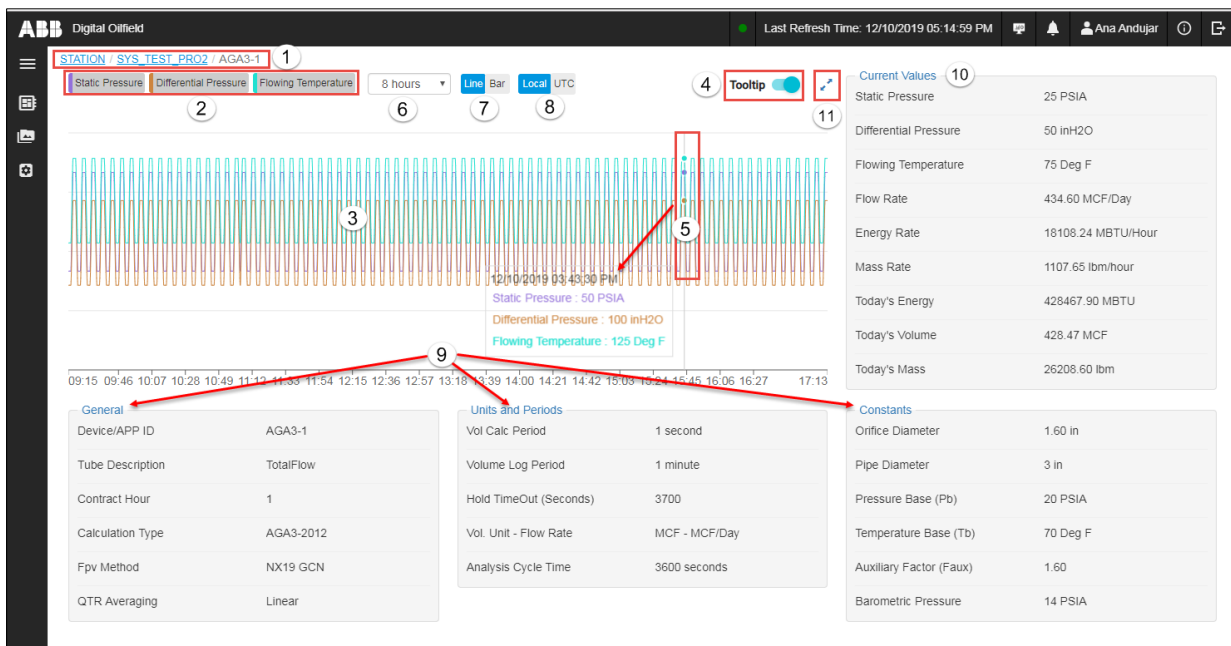
- The main application instance page displays relevant parameter values grouped together: a summary list of read-only measurement or calculated values, configuration parameter values, etc. This main page also provides a graphical view of selected application variables over a selectable period.
- Data pages display more specific data. They display additional read-only measurement and calculated values, or configuration information for an aspect of the application. In the case of control applications, the pages may also contain control state status, or functions available to control applications from the cloud.

The main categories of data displayed are measurement and control data:

- Measurement application pages are mainly for monitoring measurement and calculated values.
- Control applications display read-only data for monitoring, and additional functions for control. Control applications pages may also display values obtained by measurement applications, since measurement values determine the fine-tuning of the controls systems.

This section shows examples of application pages and the data they display. [Figure 1-16](#) shows the main page of an AGA3 application instance. The page provides summary information of the overall setup and main current application values. It displays a graph for a subset of variables, setup data and parameters values, current measurement and calculated values.

Figure 1-16: Main AGA3 page



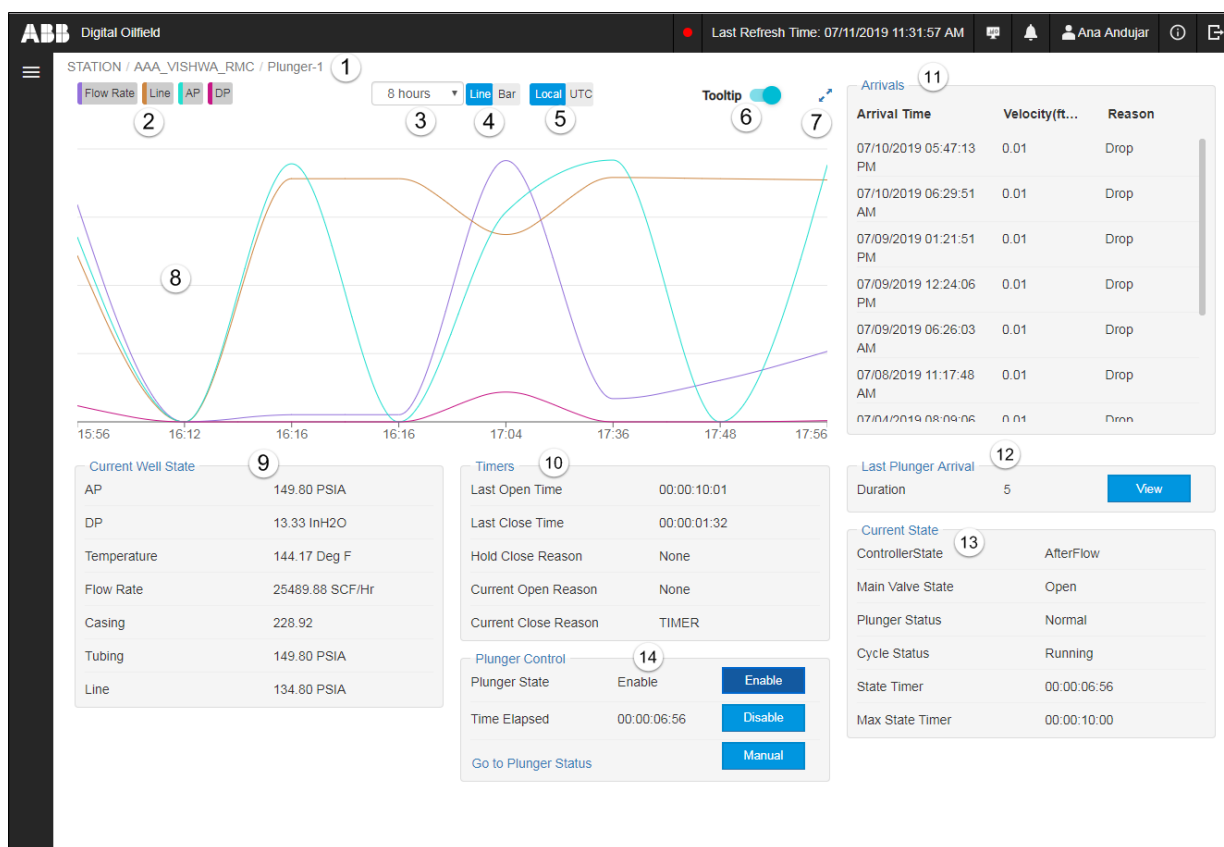
Legend for Figure 1-16: Main AGA3 page

Item	Description	Item	Description
1	Page navigation path	7	Graph type selector (bar or line)
2	Graph legend	8	Time zone

3	Graph of selected application variables (based on trend definitions)	9	Read-only setup parameters
4	Tool tip: On: displays graph point values Off: does not display graph point values.	10	Current measured and calculated values
5	Graph point values (with Tool tip on)	11	Click to expand the graph view to full screen.
6	Time period selector (graph displays values based on data from the last 8, 24, or 72 hours)		

Figure 1-17 shows the main page of the Plunger Lift application. This page displays a graph for a subset of measurement variables and several control parameters, status, and control functions.

Figure 1-17: Main plunger lift application page



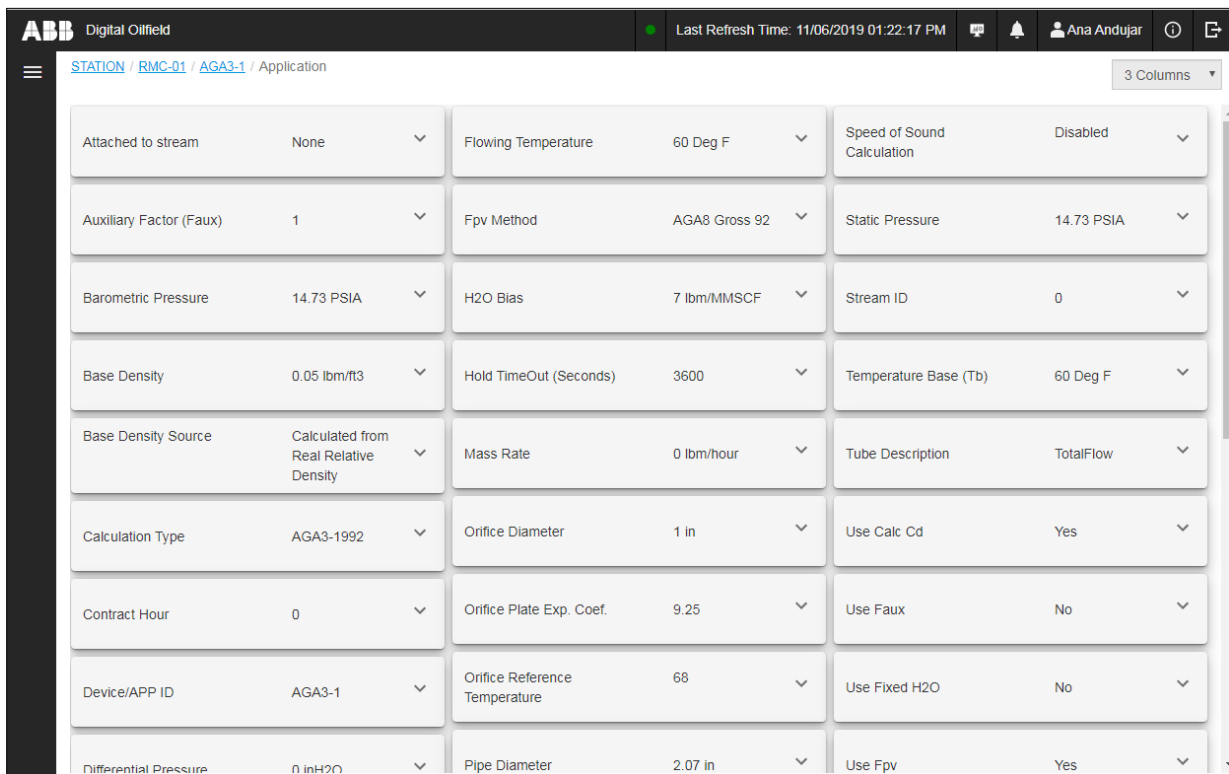
Legend for Figure 1-17: Main plunger lift application page

Item	Description	Item	Description
1	Page navigation path	6	Tool tip- On: displays graph values when hovering over the graph Off: does not display graph point values.
2	Variables represented in the graph	7	Click to expand to full screen graph display

3	Time period selector (graph displays values based on data from the last 8, 24, or 72 hours)	8	Graph for selected application variable (from trend definitions)
4	Graph type selector (bar or line)	9-13	Application data (some data may come from other applications)
5	Time zone	14	Functions available from the cloud

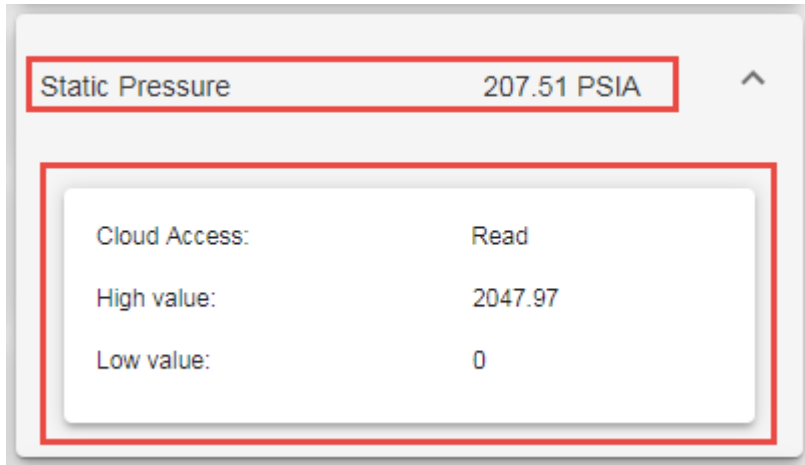
Other application pages display detailed parameter information in alphabetical order. For example, the Application page of the AGA3-1 application ([Figure 1-18](#)), displays all the application parameters available for monitoring from the cloud. Each parameter displays its value and additional attributes when expanded ([Figure 1-19](#)) such as parameter value range (if it applies), and whether the parameter is read-only or user-configurable from the cloud.

Figure 1-18: AGA3 Application page



[Figure 1-19](#) shows the expanded view of the Static Pressure parameter from the Application page. This is a measured value.

Figure 1-19: Static pressure (read-only parameter)

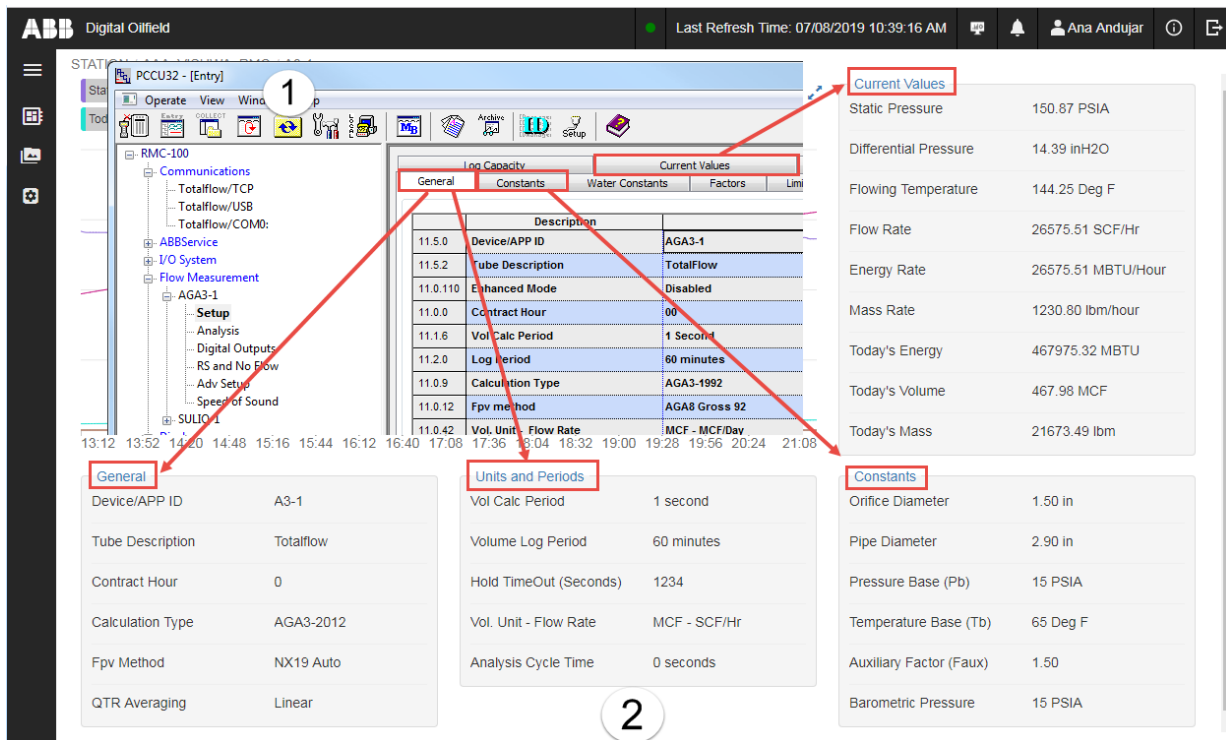


1.4.6.1 Cloud and PCCU data categories

Parameters or device data categories might not be an exact match of the categories in the application tabs in PCCU. Parameters may be grouped or organized differently when viewed from the cloud. There may be additional parameters or parameter name differences.

The main page for the AGA3 measurement application (Figure 1-20), for example, displays parameters from several of the application setup tabs in PCCU (overlay image): General, Constant, and Current Values tabs.

Figure 1-20: Application data in PCCU and the cloud interface



Legend for Figure 1-20: Application data in PCCU and the cloud interface

Item	Description
1	PCCU (overlay)
2	Cloud web page



IMPORTANT NOTE: Parameters on the cloud are organized in alphabetical order. PCCU parameters may not be. Parameters normally displayed in separate tabs in PCCU may be combined in some cloud screens. Make sure to locate the correct parameter. Displayed parameters and functions may change as additional functionality becomes available from the cloud.

[Table 1-6](#) lists, as an example, the AGA3 measurement application categories for the cloud pages and the equivalent tab or screen in PCCU where the parameters in these categories are displayed or configured.

Table 1-6: Measurement application categories

Cloud application category	PCCU Application category	Cloud application category	PCCU Application category
Application	Several setup tabs: General, Constant, and Current Values tabs	Daily Logs	(Measurement App instance)> Daily
Aggregate	Parameters from the Current Values tab	Alarms	Alarms System>Log
Composition	Analysis> Analysis Setup	Alarm Definitions	Alarms System>Current
Digital Outputs	The default number of digital outputs tabs is 2 (Digital Output 1 and Digital Output 2).	Trend Definitions	Trend System
Last calculated	Setup>Last Calc Values	Events	(Measurement App instance)>Events
Custom logs	(Measurement App instance)> Log Period Data		

2 Prepare for device configuration

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

First time cloud 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.

i **IMPORTANT NOTE:** 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, enable, and configure applications from PCCU.

2.1 Prerequisites

This section includes the minimum requirements to support field device configuration. [Table 2-1](#) lists requirements for the RMC-100. [Table 2-2](#) provides requirements for the system (laptop or PC) used to configure the device. Review the requirement lists and their associated tasks.

Table 2-1: Field device prerequisites (RMC-100)

Requirement	Description	Task
MQTT-ready device OS and flash	The device embedded software with the MQTT client functionality.	<ul style="list-style-type: none">– 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 10.1.
Valid IP configuration for cloud connection	IP configuration must include a valid IP address, subnet mask and default gateway.	<ul style="list-style-type: none">– 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 Totalflow device	<ul style="list-style-type: none">– 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 cloud. 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.	<ul style="list-style-type: none">– Determine the authentication method.– Generate or obtain certificate and authentication keys as necessary.

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

i **IMPORTANT NOTE:** [Table 2-2](#) shows the prerequisites of a laptop for local operator access. Access to the device from mobile devices is also supported. User and cloud interfaces adapt their display to the type of mobile device.

Table 2-2: 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 higher).
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.
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.

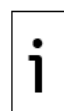
2.2 Determine authentication method

Secure device-cloud connection requires authentication. Authentication might require access credentials, public/private key pairs or security certificates depending on the authentication method or standard used.

2.2.1 Authentication methods

The Totalflow device supports two types of authentication options:

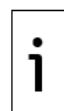
- Authentication using valid username/password. The device embeds a valid username and password in its connection requests. The MQTT Broker verifies that the credentials match those provided and authorized for the customer.
- Authentication using the X.509 standard format. This standard defines the format 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: X.509 CA-signed certificates are preferred over self-signed certificates. Administrators must verify the service provider's policy and support to generate the appropriate certificates.

2.2.2 Prepare for authentication configuration

The authentication method is a required parameter for field configuration. [Table 2-3](#) 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 2-3: Obtain authentication parameters

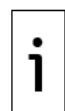
Requirement	Description	Task
Device ID	Name that uniquely identifies the device on the cloud.	– Define a unique name or ID based on your own naming convention.

Requirement	Description	Task
		<ul style="list-style-type: none"> – The Totalflow device supports the definition of the Station ID. The device ID for the cloud connection can match the Station ID if it is unique. – To verify or obtain the station ID on a 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 cloud. The Authentication method in both the device and the cloud IoT hub must match.	<ul style="list-style-type: none"> – Obtain the preferred method from the administrator.
Username/ password	Required for all authentication methods depending on the service provider if used.	<ul style="list-style-type: none"> – Obtain credentials from administrator.
Certificates, Keys	<p>Required for X.509 authentication</p> <p>Digital files with certificate, key and fingerprint that certify the device authenticity for acceptance on the cloud.</p>	<p>Obtain from system administrator the three required files for X.509 authentication.</p> <ul style="list-style-type: none"> – 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. <p>To generate device-specific certificates and keys, see section 10.3, Generate certificates for X.509 authentication.</p>

2.3 Register the device on the cloud

The cloud service provider requires device registration to authenticate and grant connection requests from devices on the field.

Device registration consists of adding and identifying the device on the cloud with its unique ID, defining the type of authentication applied to connection requests, and assigning the device to the correct cloud service. The cloud service that grants connections and authenticates devices is the IoT hub service.



IMPORTANT NOTE: Device registration is a task that an administrator must complete. Coordinate or confirm the registration of devices with the administrator. Device registration procedures depend on the cloud service provider. If not using Azure, follow the procedures specified by your provider.

The high-level administrator tasks for device registration are:

1. Access the portal provided by the cloud service provider.
2. Select the IoT service that will process the field-device connection requests and communication. This service defines the MQTT broker details that the device needs to establish connection.
3. Add the device with its unique device ID.
4. Define the authentication method the MQTT broker uses to verify field devices.
5. Provide any parameters required by the authentication type.



IMPORTANT NOTE: A fingerprint is required for self-signed X.509 certificates. Provide that parameter in the portal.

2.4 Device configuration overview

Review this section to prepare for device configuration. The device factory-default MQTT configuration must be updated to reflect specific device, connection, and authentication parameters. Connection verification is required at first-time configuration. 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.

Use the Device Configuration User Interface to configure field devices. Through this interface, MQTT-enabled devices provide web pages with several configuration options. [Table 2-4](#) identifies the configuration pages and the associated procedures for device configuration. For an overview of the configuration pages see section [1.3.3 MQTT device configuration interface](#).



IMPORTANT NOTE: A successful device-broker connection is required to complete all configuration. Follow the tasks listed in [Table 2-4](#) in the presented order: Configure initial configuration parameters and establish the device’s connection with the broker first. Then configure application and register data for publishing.

Table 2-4: Device configuration overview

Requirement	Description	Task
Initial configuration: Device, connection, broker parameters	Parameters required for device-broker connection: unique device ID, broker identification and connection details, protocol.	Follow procedures in section 3 Initial device configuration . (Initial configuration page)
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 on the device.	
Successful connection	The device is authenticated by the broker and its connection request accepted. 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 3.7 Verify connection status . (Initial configuration page)
Application configuration	Select device applications and instances the device will publish data for.	Follow procedures in section 4 Device application configuration . (Application configuration page)
Register configuration	Select the specific application registers the device will publish data for.	Follow procedures in section 5 Device register configuration . (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.

3 Initial device configuration

The procedures included in this section configure the Totalflow device with the required parameters for communication with the Azure cloud MQTT broker or an MQTT server on a private network (implementations using Sparkplug).



IMPORTANT NOTE: Access to the device configuration interface requires that the MQTT functionality on the device is enabled. If unable to access the configuration pages, make sure to enable MQTT as described in [section 10.1](#).

3.1 Access the Initial Configuration page

This procedure assumes that the laptop that connects to the field device has the supported browser version already installed. See section [2.1 Prerequisites](#). It also assumes that network equipment onsite is already installed and operational and that it has enough ports to connect the devices and the laptop.

Access to the device using the web interface requires a TCP/IP connection. The laptop and device IP configurations must be compatible for successful connection.



IMPORTANT NOTE: The browser-based device configuration interface supports local or remote configuration if the laptop and the device both have valid IP configurations and network connections. For remote configuration, connect the laptop to the corporate network that allows access to the onsite networks. For local configuration, connect the laptop to the onsite network.

To configure multiple devices, access each device separately. Set up multiple connections on different browser tabs. The procedure in this section illustrates the steps for one device. Repeat the steps for each required device.

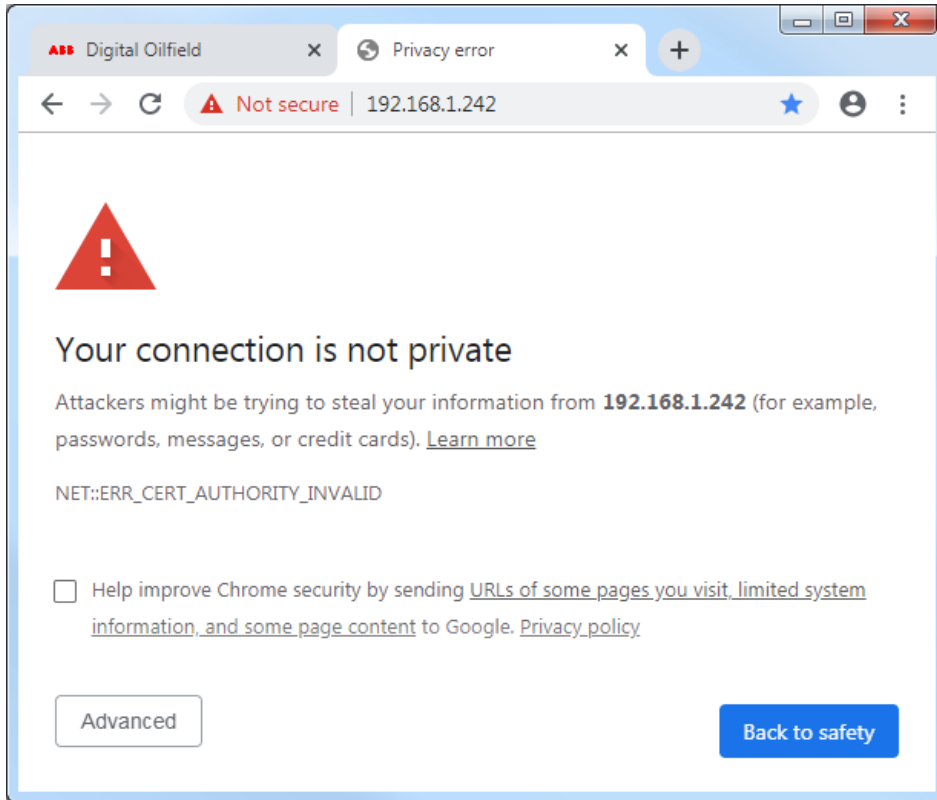
To access the device's Initial Configuration web page:

1. Connect the laptop and the device to the network.
2. 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 on the screen and the URL address field displays "Not Secure".



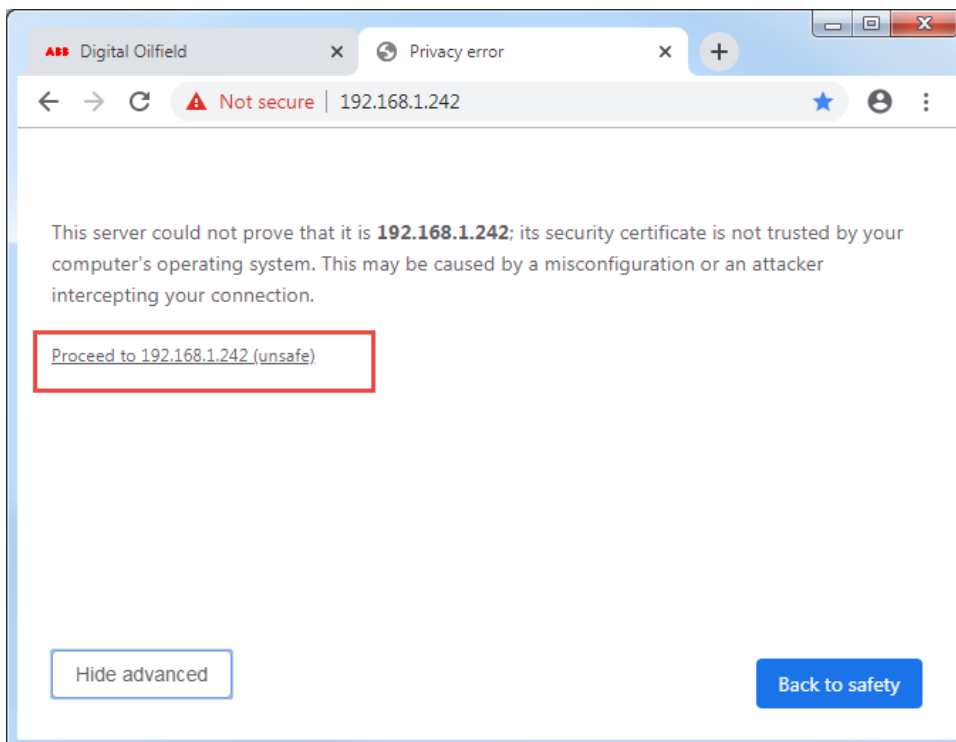
IMPORTANT NOTE: Security warnings displays at first-time login when the device does not have valid certificates ([Figure 3-1](#)). The "Not secure" warning in the URL field displays because the browser does not establish the connection on secure mode. To configure the browser for secure mode, and prevent this warning from reappearing, complete the procedures in this section, and then configure the browser as described in section [9.3 Secure access to the MQTT configuration interface](#).

Figure 3-1: Initial security warning



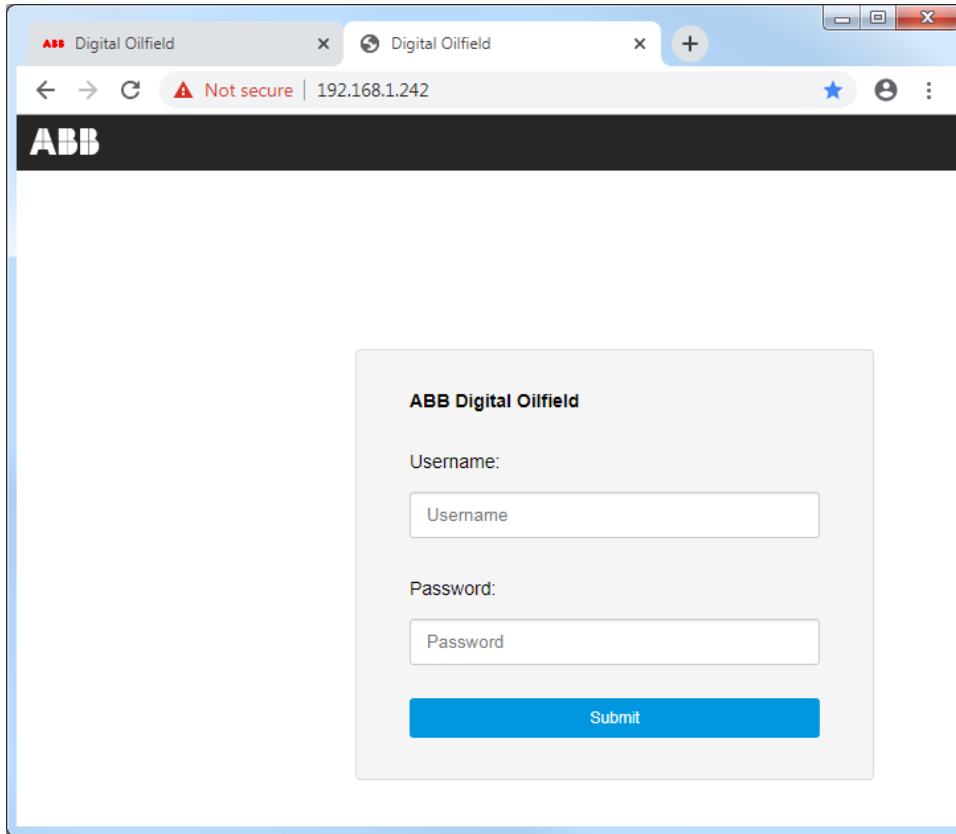
4. Click **Advanced** at the bottom of the screen. Additional security information displays (Figure 3-2) to indicate that the laptop has not found the certificates for secure connection or it has the wrong information. A link to the device is provided to proceed.

Figure 3-2: Second security warning



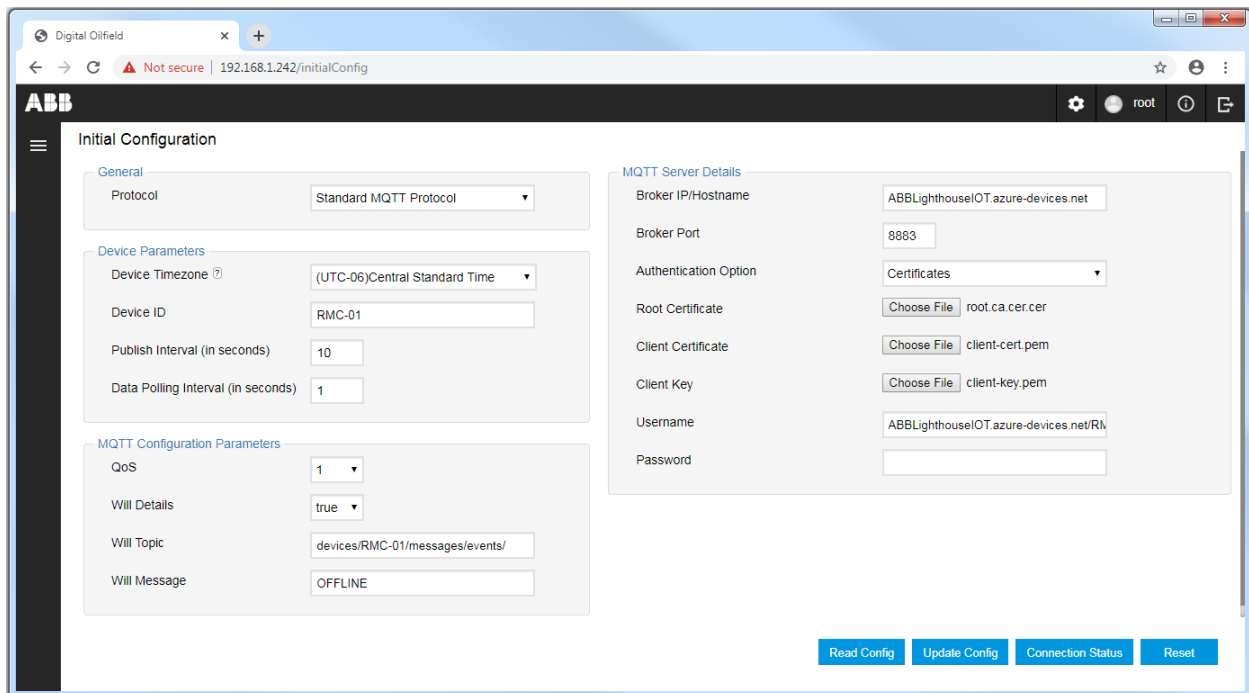
5. Click **Proceed to <device IP address>**. The login screen displays.

Figure 3-3: Device configuration interface login screen



6. Type **root** into the Username field. Type the default root password, **root@123**, into the Password field. Click **Submit**. The Initial Configuration screen displays.

Figure 3-4: Initial Configuration page





IMPORTANT NOTE: Totalflow devices ship with a default MQTT configuration from the factory. The Initial Configuration page displays this configuration at first-time login. This configuration remains on the device until updated. After updates, the device always stores the last successful configuration.

3.2 Configure the protocol

MQTT-enabled devices support connections to MQTT servers on a service provider cloud or on private corporate networks with SCADA/IIoT systems. This section describes how to select the protocol for the required scenario.

The protocol configuration on the device and the MQTT server must match. Consult with your administrator about the preferred protocol option. [Table 3-1](#) describes the protocol options supported by the field device.

Table 3-1: Communication protocol description

Parameter	Description	Values
Protocol	Method of communication for the device-broker connection. The protocol specifies the packet format and types for connection requests and responses between the field device and MQTT server.	<p>MQTT Standard Protocol (default) Select this option when connecting to a broker cloud service provider broker.</p> <hr/> <p>Sparkplug Select this option when connection to a corporate network with its own MQTT server or distributor as part of a SCADA/IIoT architecture.</p>

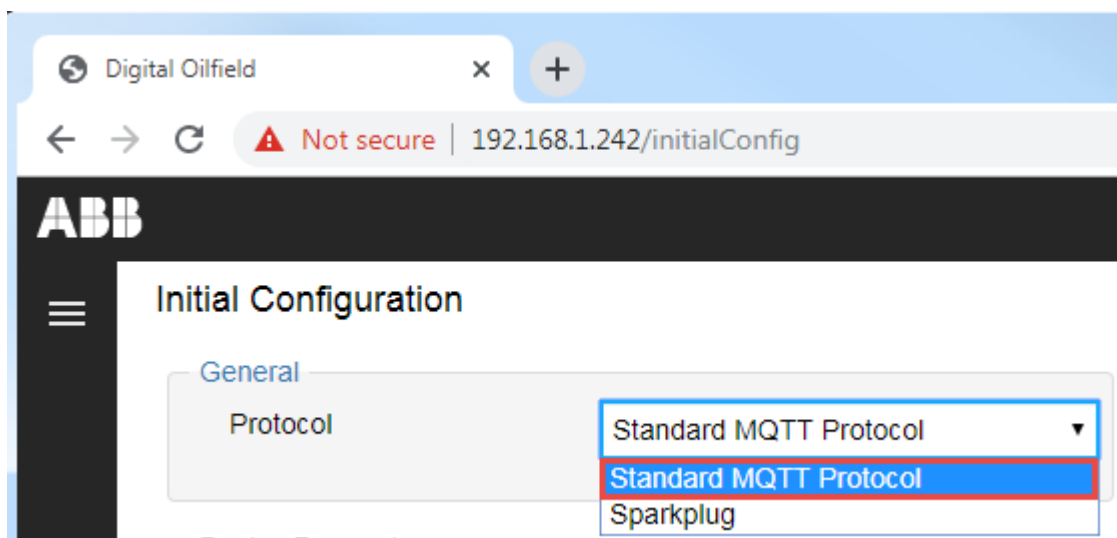


IMPORTANT NOTE: Protocol configuration change causes an existing device-broker connection to reset.

To configure the communication protocol:

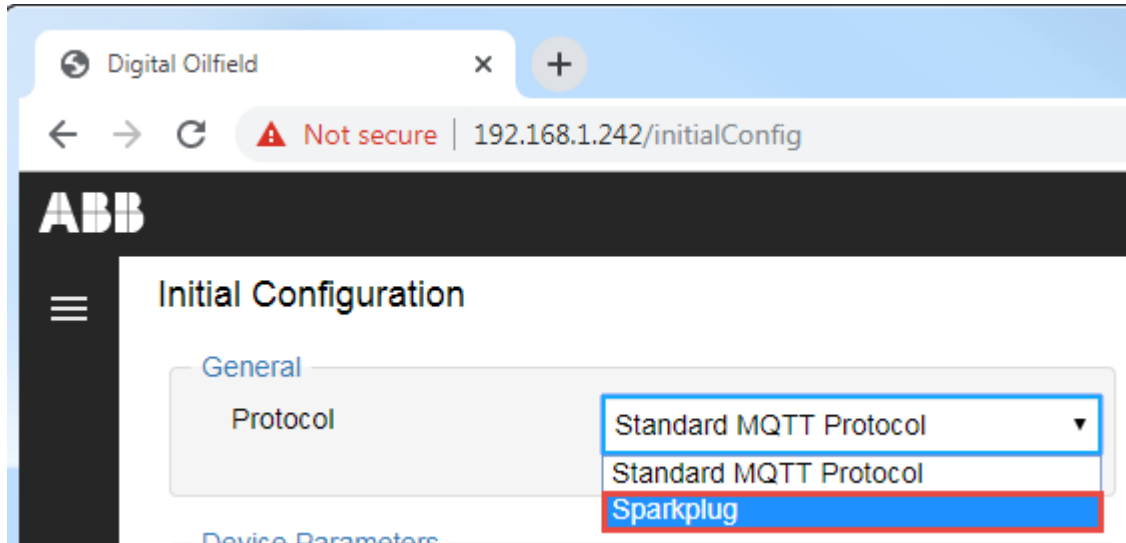
1. Select one of the protocols from the Protocol drop-down list under the General parameter section.
 - a. Select the **Standard MQTT Protocol** (default value) to connect to a service provider MQTT broker.

Figure 3-5: Select Standard MQTT Protocol



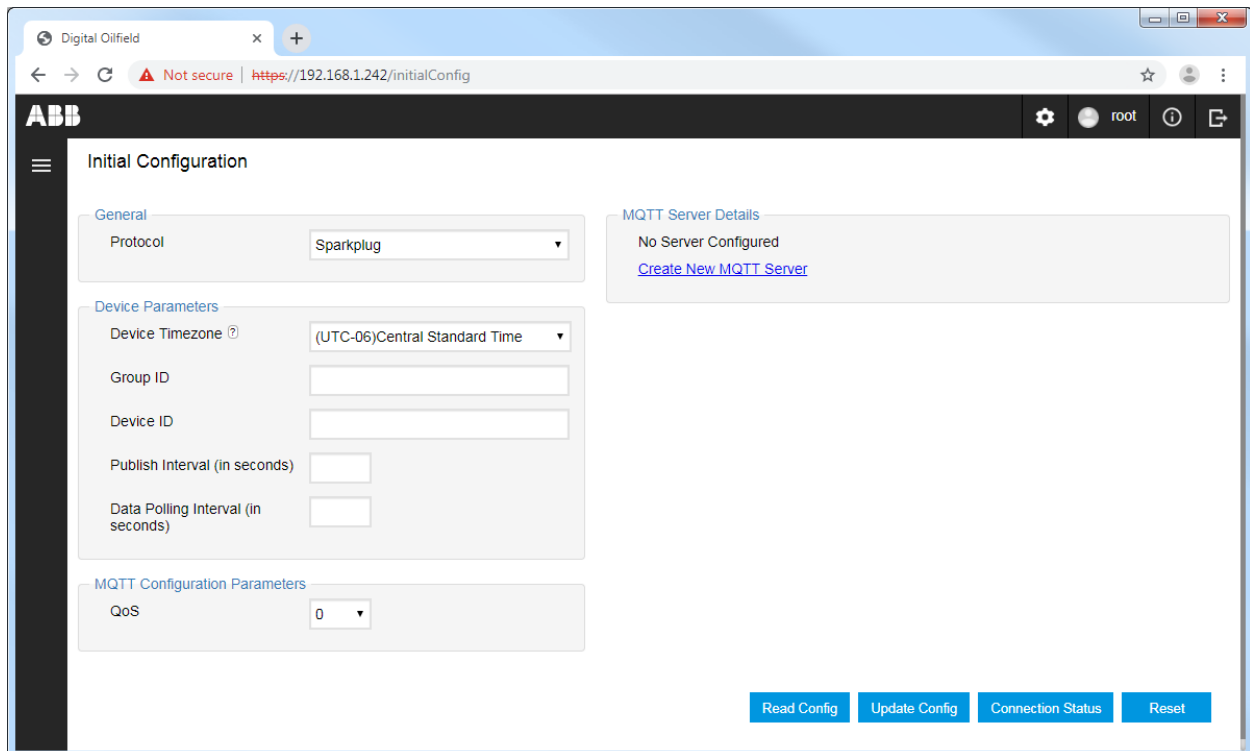
- a.
 - b. Select **Sparkplug** to connect to the customer MQTT server or distributor.

Figure 3-6: Select Sparkplug



IMPORTANT NOTE: Configuration parameters depend on the protocol type. The Initial Configuration web page displays the Standard MQTT Protocol parameters. The configuration page for the Sparkplug protocol is different ([Figure 3-7](#)).

Figure 3-7: Sparkplug protocol configuration page



2. Configure device parameters in section [3.3](#).

3.3 Configure device parameters

[Table 3-2](#) lists the device parameters required for unique device identification on the cloud, assignment of the time zone for the device's location, and the frequency of data polling and publishing by the device.

IMPORTANT NOTE: Device parameters display for both the Standard MQTT Protocol and Sparkplug pages. This procedure applies to both protocol types.



Changing the Group ID, Device ID, or Data Polling interval does not cause an existing device-broker connection to reset.

Changing the Time zone and publish interval is dynamic. It does not affect an existing connection.



IMPORTANT NOTE: Totalflow devices do not support automatic time synchronization. Set the required device time zone at first-time login.

Table 3-2: Device parameter description

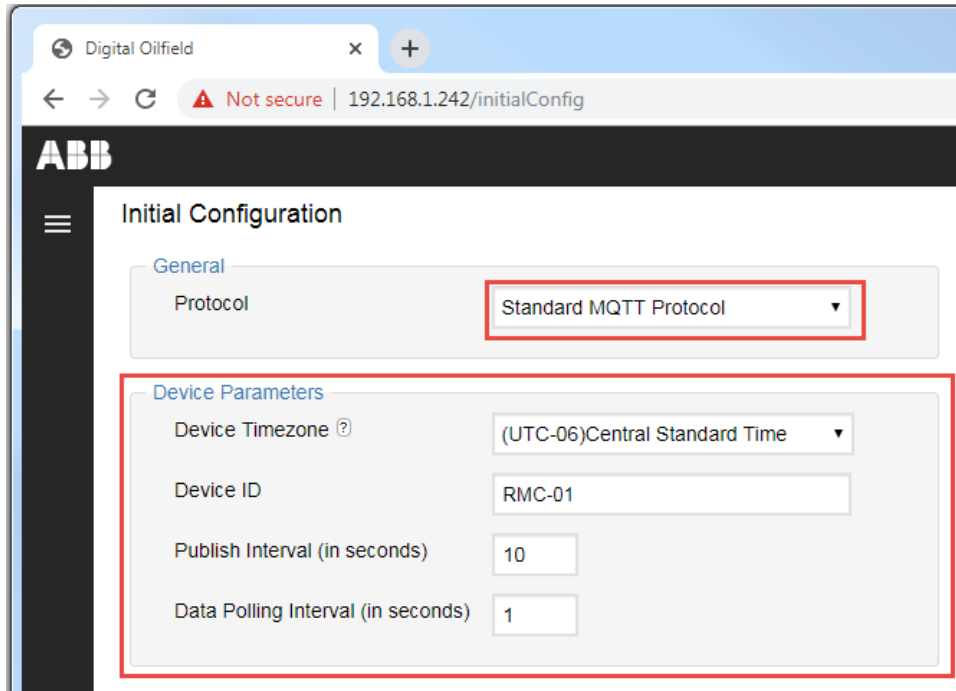
Parameter	Description	Values
Device Time zone	Standard time associated with the device's geographical location	Standard times for several geographical locations, offsets from the Coordinated Universal time (UTC) Central Standard Time (UTC-6) (Default)
Group ID	Name for the group the device belongs to. A group is defined based on any customer criteria. For example, a group can be created to identify the location of several devices. Sparkplug supports the group ID in its topic namespace to provide for logical grouping of EoNs (the device acts as an EoN) This is a parameter for Sparkplug only.	Alphanumeric string
Device ID	Unique identification or name assigned to the field device. The MQTT broker acting as a MQTT server keeps track of MQTT clients with this unique ID.	User-defined Define the naming convention based on your company's policies. When using the Azure cloud services, pre-register the device with this ID prior to device configuration.
Publish Interval (in seconds)	The frequency at which the device publishes its application register data to the MQTT Broker	30 (default) Range: 10 to 120
Data Polling Interval (in seconds)	The frequency at which the device reads its application register data.	1 (default) Range: 1 – (publish interval) or Publish Interval – 1 Set the data polling interval close to the publishing interval to optimize CPU cycles. For example, set the data polling interval to 9 seconds for a publish interval of 10 seconds. The device reads its data every 9 seconds and it publishes the data the following second (at 10 seconds).

3.3.1 Device parameters for Standard MQTT protocol

To configure device parameters:

1. Select an option from the Device Timezone drop-down list.
2. Type the Device ID.
3. Type the Publish Interval.
4. Type the Data Polling Interval.

Figure 3-8: Device parameters for Standard MQTT Protocol (Example)

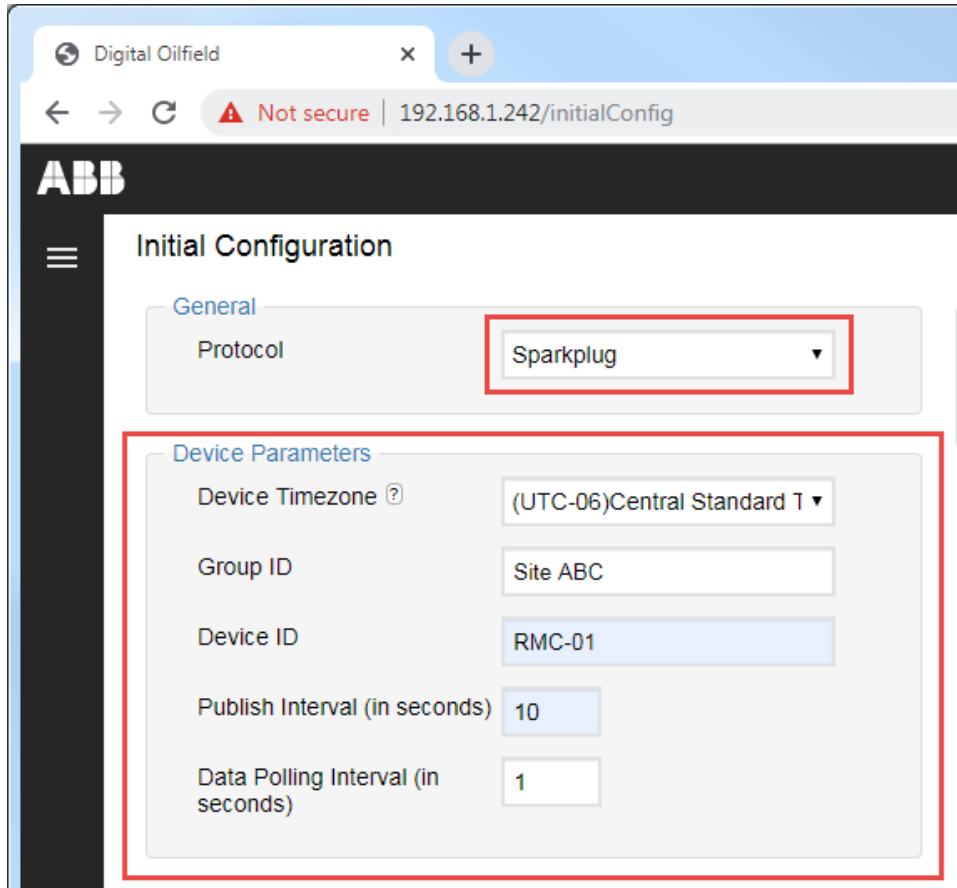


3.3.2 Device parameters for Sparkplug

To configure device parameters:

1. Select an option from the Device Timezone drop-down list.
2. Type the Group ID.
3. Type the Device ID.
4. Type the Publish Interval.
5. Type the Data Polling Interval.

Figure 3-9: Device parameters for Sparkplug (Example)



3.4 Configure MQTT parameters

[Table 3-3](#) describes the MQTT protocol parameters.



IMPORTANT NOTE: MQTT parameter configuration change does not cause an existing device-broker connection to reset.



IMPORTANT NOTE: The Quality of Service (QoS) is the only MQTT parameter required for Sparkplug. The standard MQTT protocol requires the configuration of additional parameters.

Table 3-3: MQTT Configuration parameters

Parameter	Description	Values
QoS	<p>Quality of Service Level on the device-Broker connection. It is the agreement between the device and the broker that defines the guarantee of delivery for data the device publishes. Selection of QoS depends on the reliability of the network the devices connect to.</p> <p>The device exchanges messages with the MQTT broker according to the QoS levels defined by the MQTT specification and supported in the device.</p> <p>Applies to both the Standard MQTT Protocol and Sparkplug.</p>	<p>0 – Best effort delivery. No guarantee of delivery. The broker does not acknowledge receipt of the data and the device does not retransmit the data.</p> <p>1 (Default) – Guarantees at least one-time data delivery. The broker must acknowledge receipt of data message. The device stores the message sent and retransmits it until the broker acknowledges receipt.</p>
Will Details	<p>Feature which allows the device to indicate if it wants the MQTT broker to send a will message (Last Will and Testament, LWT, message) on its behalf.</p> <p>The device sends the LWT message to the broker while connected to the broker specifying details.</p> <p>The broker receives and retains the LWT message. It sends it to other MQTT clients only when it detects the ungraceful disconnection of the device.</p> <p>Standard MQTT protocol only.</p>	<p>True (default) – The device requests the broker to send the LWT message upon ungraceful device disconnection. Recommended.</p> <p>False - the device does not request the broker to send the LWT message upon ungraceful device disconnection.</p>
Will Topic	<p>Topic where the broker publishes the Will message after ungraceful device disconnection.</p> <p>MQTT clients subscribed to this topic receive this notification and are aware of the device disconnection.</p> <p>Standard MQTT protocol only.</p>	<p>The Will topic depends on the definitions set in the cloud. The following is the default string from the factory:</p> <p>devices/<Device ID>/messages/events/</p> <p>The “Device ID” in the Will topic string might be a default name in the factory configuration. Update with the unique Device ID required for the actual field device.</p> <p>Be sure to use the correct format: a topic is a character string with a hierarchical structure that allows subject-based filtering by the MQTT broker. The topic consists of one or more topic levels. Each topic level is separated by a forward slash (topic level separator).</p>
Will Message	<p>Last Will and Testament (LWT) message the broker sends to other MQTT clients on behalf of the device when the device disconnects ungracefully from the MQTT broker (connection loss).</p> <p>Standard MQTT protocol only.</p>	<p>OFFLINE (default)</p>

3.4.1 MQTT configuration parameters for Standard MQTT protocol

To set up MQTT configuration parameters (Figure 3-10):

1. Select the quality of service level from the QoS drop-down list.



IMPORTANT NOTE: Select only a value the MQTT server supports. Consult with your administrator.

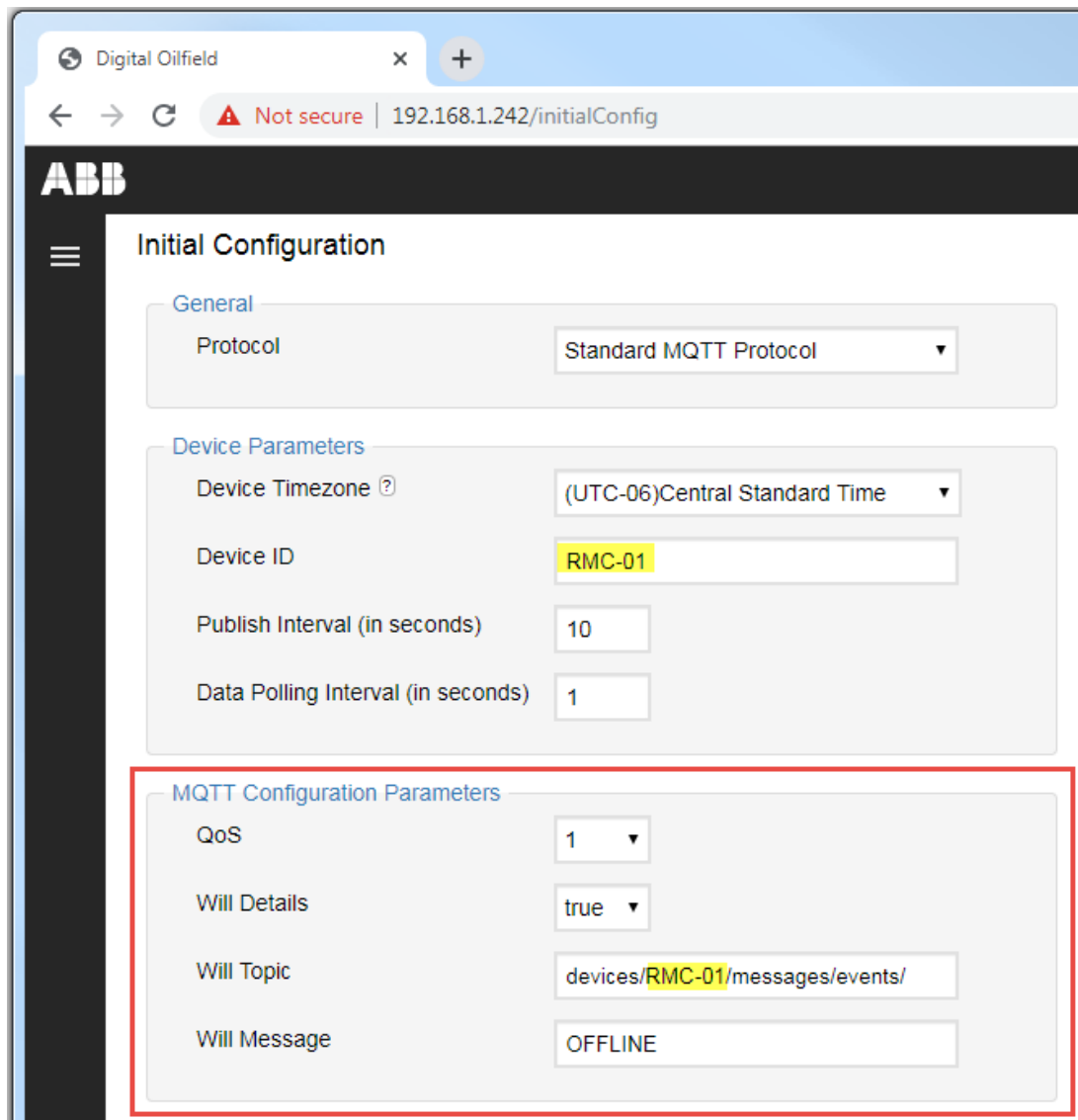
2. Select **true** from the Will Details drop-down list.
3. Type the Will topic string using the following format:
devices/<device ID>/messages/events/



IMPORTANT NOTE: Make sure that the Device ID in the topic matches the Device ID value configured in the Device Parameters section (highlighted in Figure 3-10).

4. Keep the default Will Message value.

Figure 3-10: MQTT configuration parameters for Standard MQTT Protocol



3.4.2 MQTT configuration parameters for Sparkplug

The only required MQTT configuration parameter for Sparkplug is the quality of service (QoS).

To set up the QoS for Sparkplug:

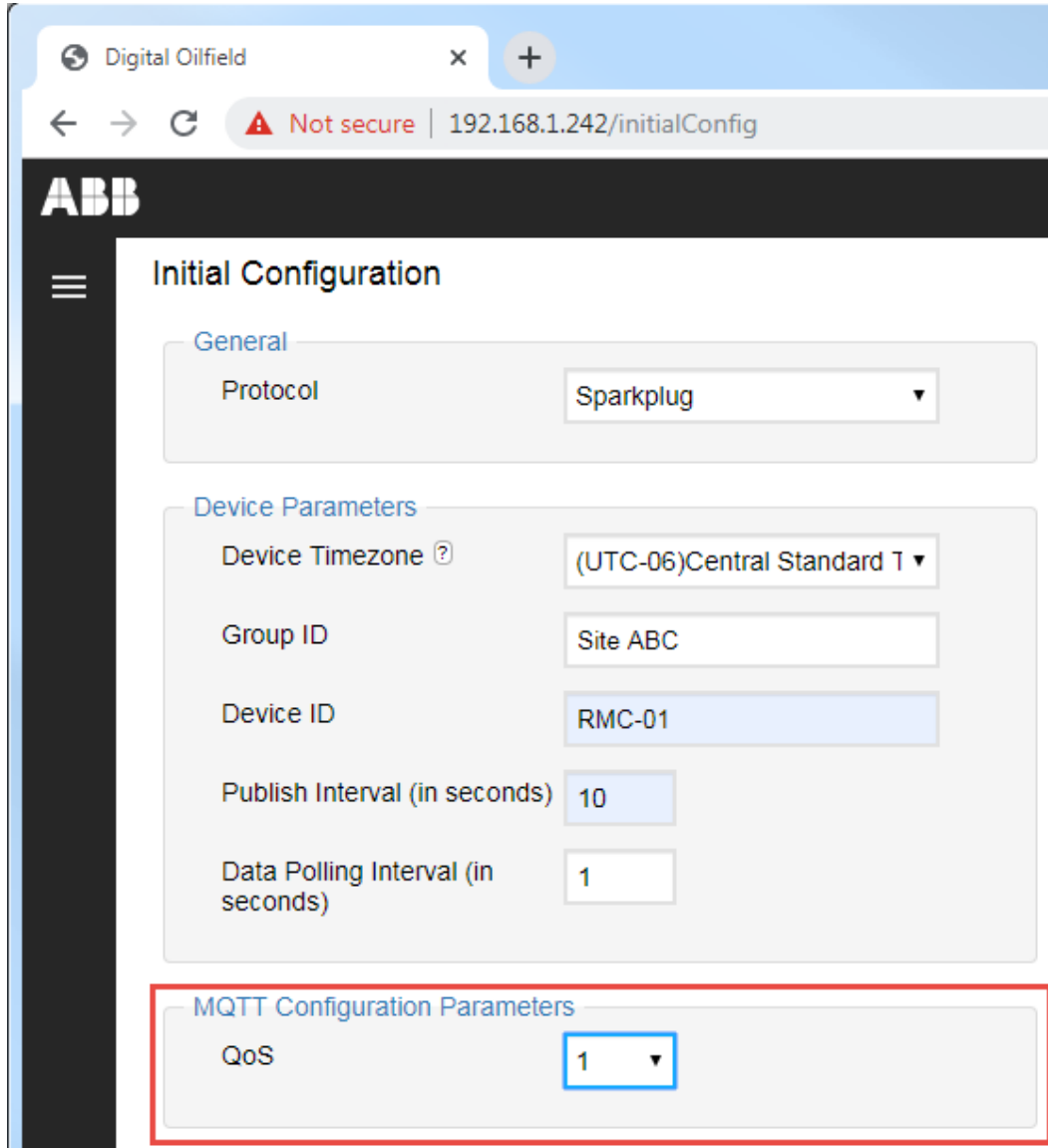
1. Select the quality of service level from the QoS drop-down list.



IMPORTANT NOTE: Select only a value the MQTT server supports. Consult with your administrator and the vendor documentation for your sparkplug systems.

2. Proceed to configure MQTT Server Details in section [3.5](#).

Figure 3-11: MQTT Configuration Parameters for Sparkplug



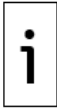
3.5 Configure MQTT Server Details

The procedures in this section configure the TCP/IP and authentication parameters required to establish MQTT communication between the field device and the MQTT server. MQTT communication requires a TCP connection and authentication.

- The TCP/IP parameters identify the broker’s IP address or hostname and the TCP port the server designates for MQTT connection processing. The device establishes the TCP connection with these parameters.
- The authentication parameters identify the method and applicable credentials the server requires to grant the device’s connection request.



IMPORTANT NOTE: Obtain required certificates from your administrator. Each device has its own client-key and client-certificate, but the same root certificate might be used in several devices with a common MQTT broker. You need to have these 3 files ready to complete configuration and verify connection: Root certificate, Client certificate, and Client key.



IMPORTANT NOTE: Changing the MQTT server details configuration causes an existing device-broker connection to reset.

Table 3-4: MQTT Server Details description

Parameter	Description	Values
Broker IP/Hostname	IP address or hostname of the MQTT broker on the cloud	Obtain from administrator.
Broker Port	TCP port assigned to MQTT connections.	<p>For connection to a cloud service provider MQTT server:</p> <ul style="list-style-type: none"> – Use 8883 (default). It is the standard TCP port reserved for secure MQTT connections by Internet authorities. – ABB recommends using the default value for security. This port is used with Transport Layer Security (TLS) protocol. For other ports, verify with your administrator or service provider. <p>For connection to a customer MQTT server or distributor when using Sparkplug:</p> <ul style="list-style-type: none"> – Obtain the port number from the administrator or server documentation. The port must be user-configurable. – Configure a unique IP address/TCP port pair for each server added.
Authentication Option	Format used for validation of field devices before connection to the cloud. The Authentication method configured in both the device and the MQTT Broker must match.	<ul style="list-style-type: none"> - Certificates (Default): X.509-based authentication - Username/Password: obtain from administrator
Root Certificate	Required if authentication option is set to Certificates. Click Choose file to locate and select root certificate.	<ul style="list-style-type: none"> - No file chosen (default) - Name of the root certificate file: displays after browsing and selecting the certificate on the laptop/system used to connect to the device
Client Certificate	Required if authentication option is set to Certificates. Click Choose file to locate and select client certificate.	<ul style="list-style-type: none"> - No file chosen (default) - Name of the client certificate file: displays after browsing and selecting the certificate on the laptop/system used to connect to the device
Client Key	Required if authentication option is set to Certificates. Click Choose file to locate and select client key.	<ul style="list-style-type: none"> - No file chosen (default) - Name of the client key file: displays after browsing and selecting the certificate on the laptop/system used to connect to the device

Parameter	Description	Values
Username	Required for both username/password or certification authentication methods.	User-typed Username provided by administrator
Password	Required for both username/password or certification authentication methods.	User-typed Password provided by administrator



IMPORTANT NOTE: This procedure assumes that the required credentials or certificates are available or accessible from the system the device is configured from. For example, the certificate files must be stored on the laptop used for local (onsite) configuration.



IMPORTANT NOTE: Certificate and key files must reside on the device. This procedure shows how to provide the location of those files, but file upload requires configuration update (See section [3.6 Update configuration](#)). Incorrect credentials or expired certificates prevent device connection to the cloud. Administrators must keep credentials and certificates up-to-date and monitor expiration dates to prevent disconnection.

3.5.1 MQTT Server Details for the Standard MQTT Protocol

For the following procedure, refer to [Figure 3-12](#) for an example of a completed configuration.

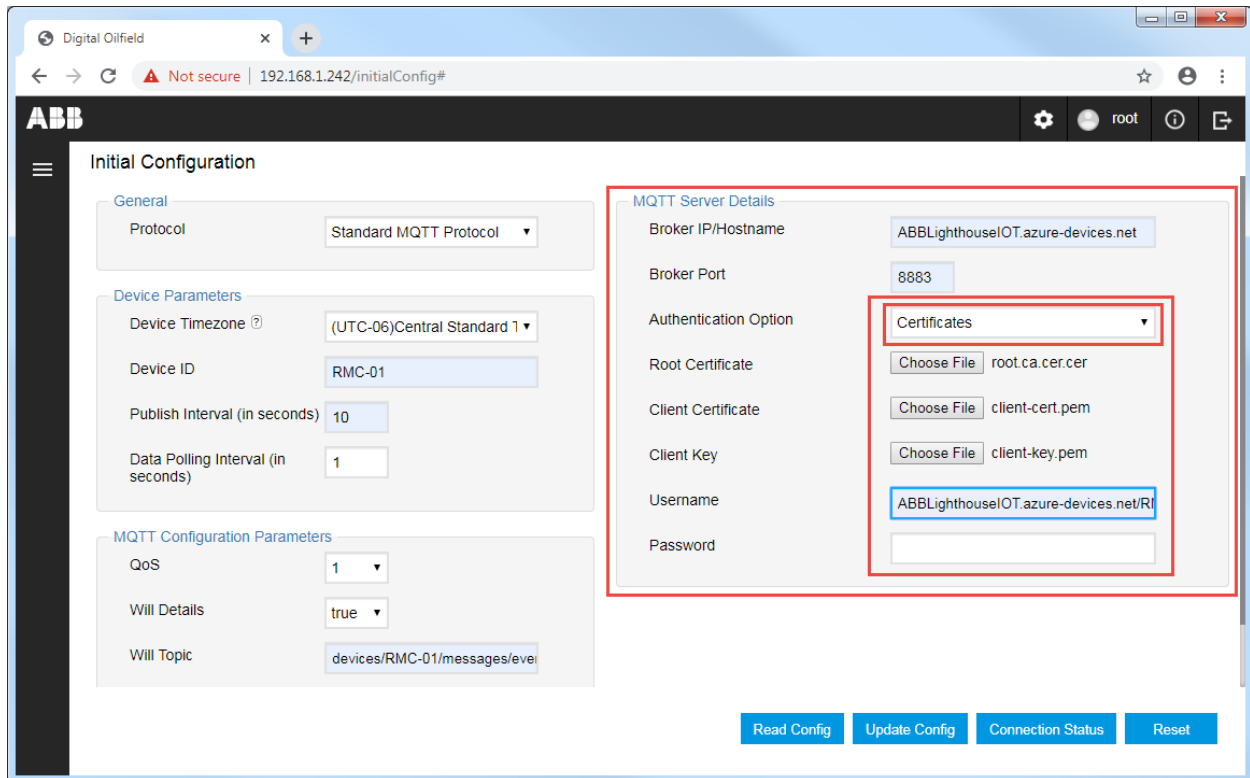
To configure MQTT Server Details:

1. Type the IP address or hostname of the MQTT broker into the Broker IP/Hostname field.
2. Type the MQTT TCP port into the Broker Port field. (Default value recommended.)
3. Select one of the following methods from the Authentication Option drop-down list:
 - a. Certificates for X.509 authentication
 - b. Username/password
4. Configure the following for the Certificates authentication option ([Figure 3-12](#)):
 - a. Click **Choose file** for each certificate type (root certificate, client certificate, and client key). When the file browser opens for each, locate and select the required file. The file name displays after it is selected. Verify the files are correct.
 - b. Type the Username when required.
 - c. Type the Password when required.



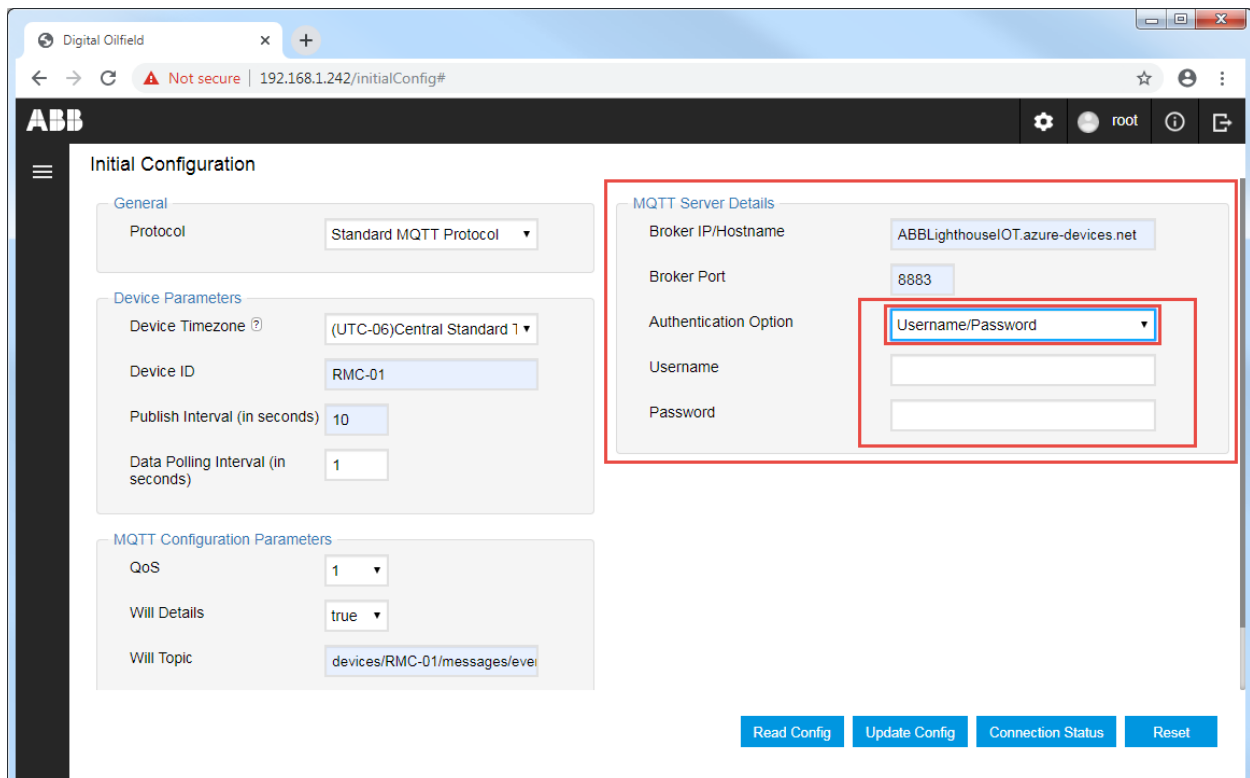
IMPORTANT NOTE: The cloud service provider might require username and password in addition to certificates. Obtain credentials from your administrator and type as necessary. When using Azure, the username is mandatory. This provides an additional security layer.

Figure 3-12: MQTT Server Details - Certificates authentication option (for Azure)



5. Configure the following for the Username/Password authentication option (Figure 3-13):
 - a. Type the Username.
 - b. Type the Password.

Figure 3-13: MQTT Server Details - Username and Password authentication option



6. Update the configuration as described in section [3.6 Update configuration](#) to save parameter values on the device.

3.5.2 MQTT Server Details for Sparkplug

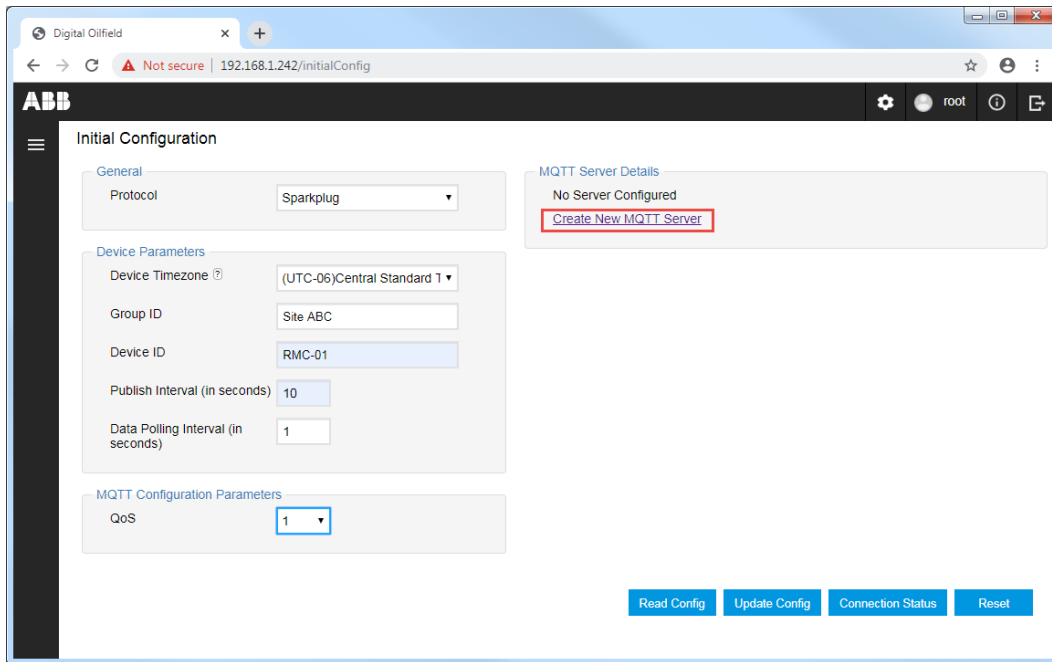
This procedure assumes Sparkplug is the selected communication protocol. Sparkplug supports the configuration of more than one MQTT server. This procedure illustrates the configuration of a single server. Repeat the steps for each server required (the page supports the configuration of up to 5 servers).

Determine the authentication options and MQTT server parameters from your administrator.

To configure MQTT Server Details for Sparkplug:

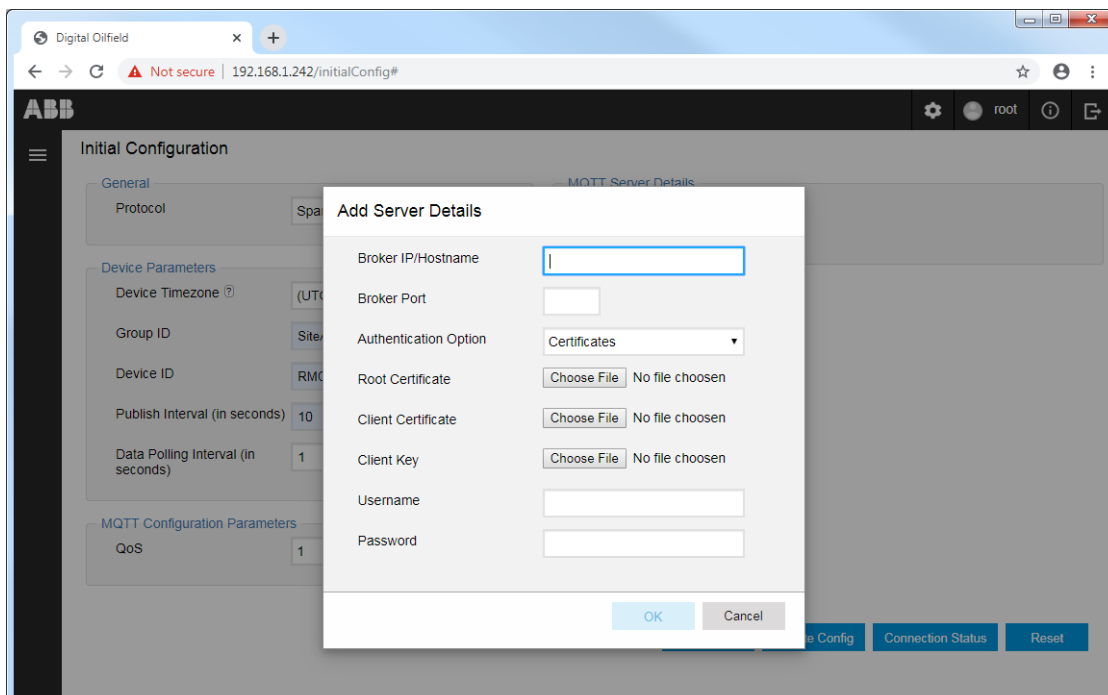
1. Click **Create New MQTT Server** from MQTT Server Details.

Figure 3-14: MQTT Server Details for Sparkplug



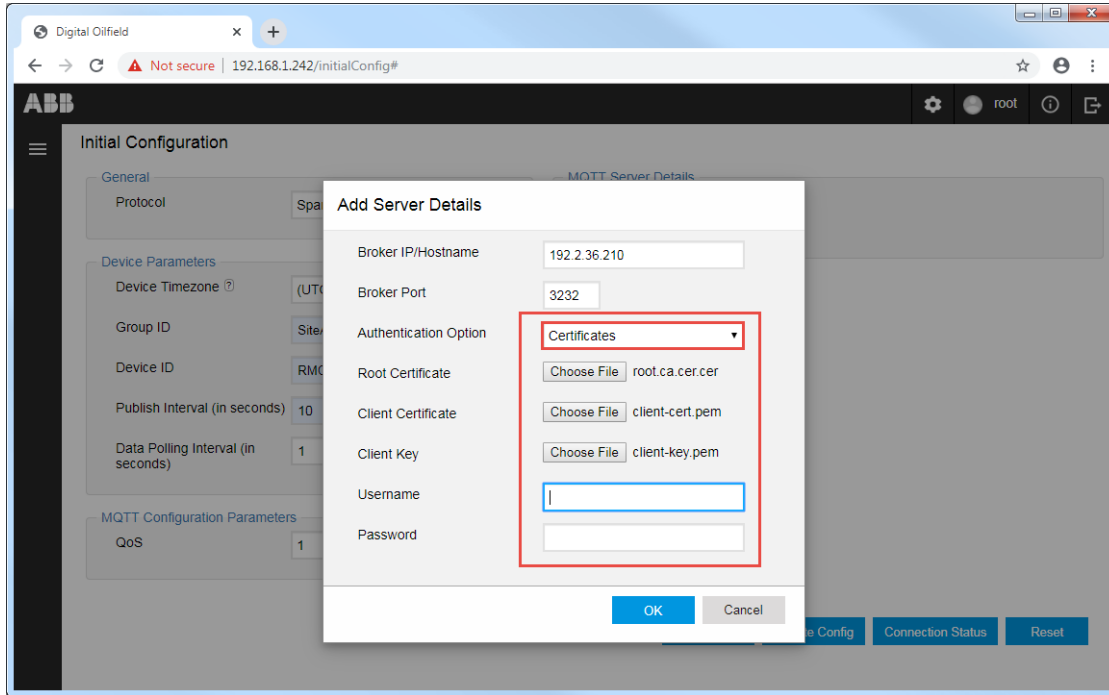
The Add Server Details pop-up displays (Figure 3-15).

Figure 3-15: Add Server Details for Sparkplug



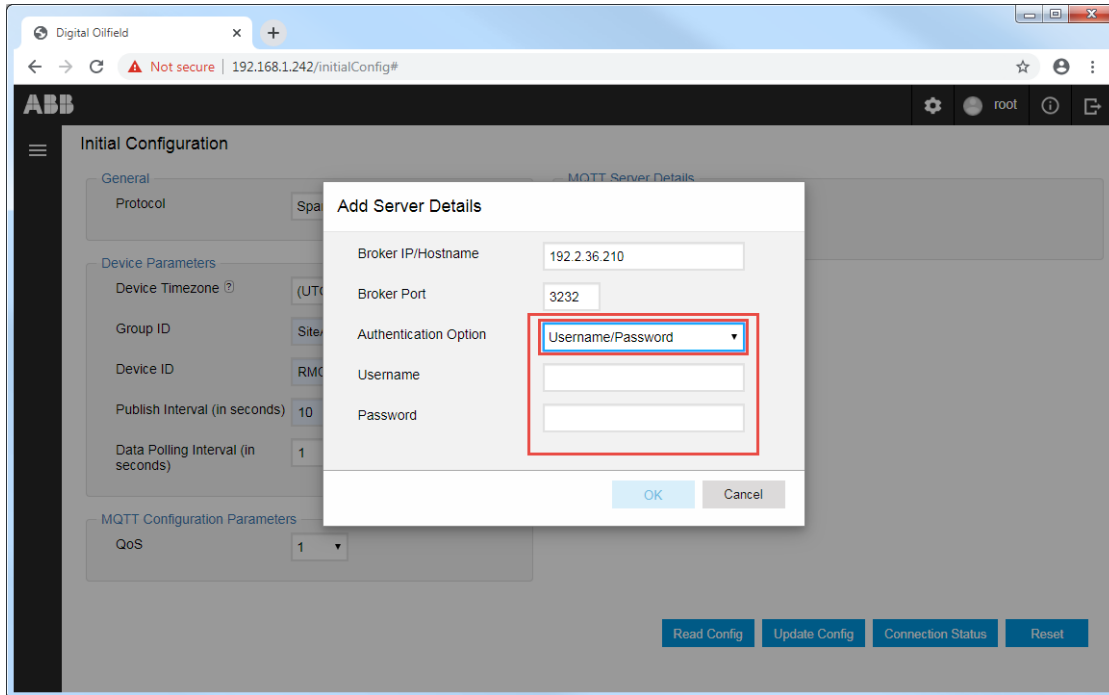
2. Type the IP address or hostname of the MQTT server into the Broker IP/Hostname field.
3. Type the MQTT TCP port into the Broker Port field.
4. Select one of the following methods from the Authentication Option drop-down list:
 - a. Certificates for X.509 authentication
 - b. Username/password
5. Configure parameters for certificate-based authentication (See [Figure 3-16](#)).
 - a. Click **Choose file** for each certificate type and locate and select certificates.
 - b. Type the required credential into Username (if the MQTT server requires a username).

Figure 3-16: Sparkplug Server Details for authentication with certificates



6. Click **OK**.
7. Configure parameters for username and password authentication ([Figure 3-17](#)).
 - a. Type the required username.
 - b. Type the required password.

Figure 3-17: Sparkplug Server Details for authentication with username and password



8. Click **OK**.

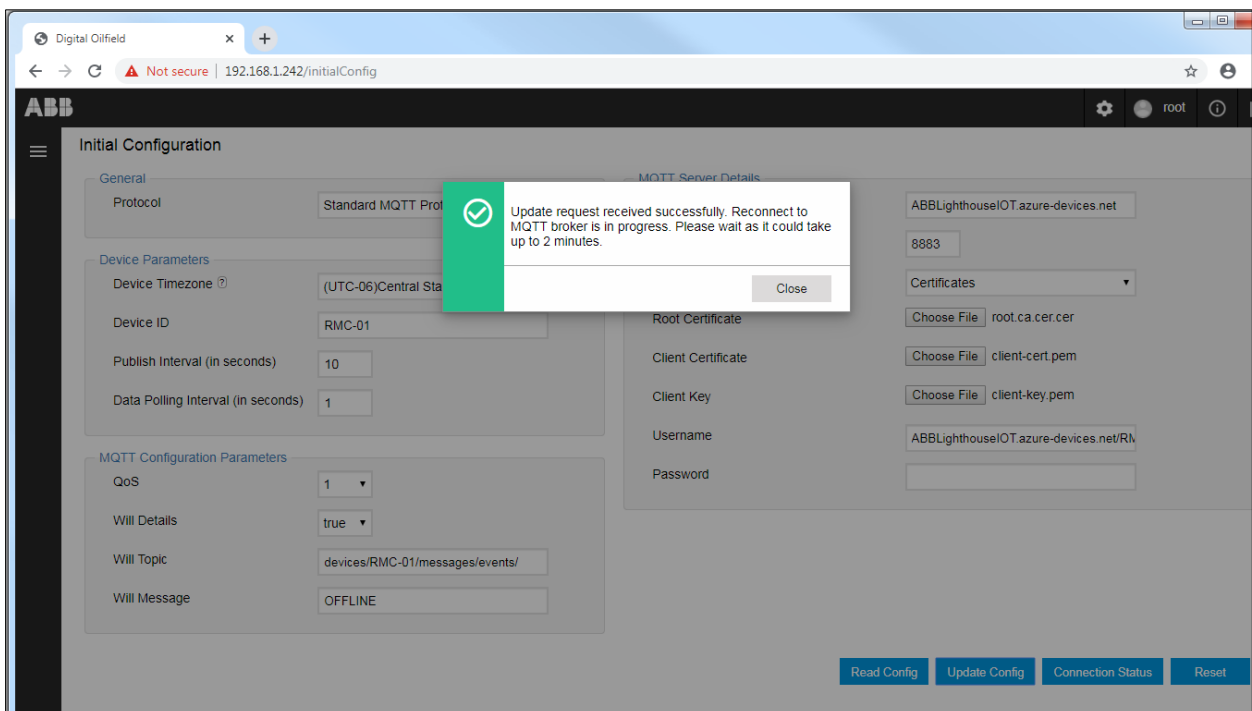
3.6 Update configuration

Update the configuration of device after all parameter configuration or changes are complete. This procedure sends the request for update to the device. The device must accept the request and commit the configuration changes for the new configuration to take effect.

To update:

1. Click **Update Config**.
2. Wait for the device to confirm the update ([Figure 3-18](#)).

Figure 3-18: Device configuration update complete message



3. Click **Close** when the update request completes successfully.

3.7 Verify connection status

Verify the status of the connection between the device and the MQTT broker. Make sure to connect the device to the network. [Table 3-5](#) shows connection status messages displayed on the configuration interface with possible causes if errors occur. Note that there may be several causes with the same error message. For errors related to Sparkplug implementations see section [6.4 Troubleshooting when using Sparkplug](#).

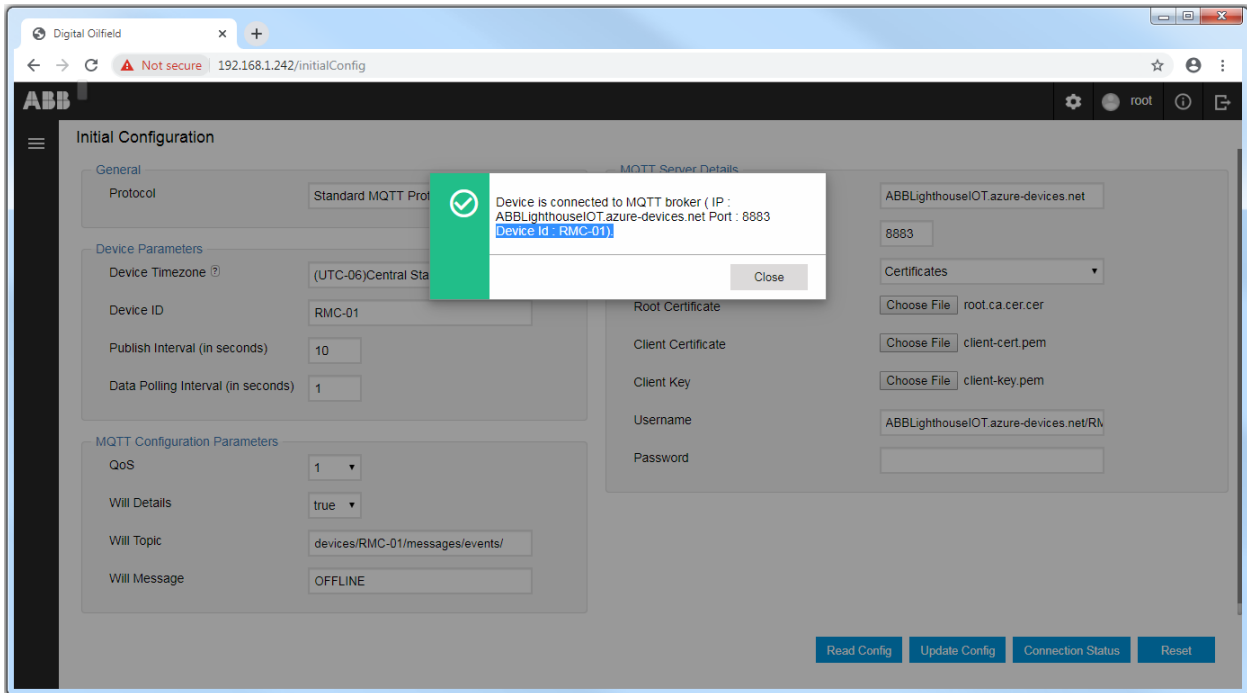
Table 3-5: Connection status messages

Message	Description
Device is connected to MQTT Broker	The connection between the device and the MQTT broker is established successfully.
Device is not connected to MQTT Broker	The connection between the device and the MQTT broker was not established successfully.
Device is waiting for response from MQTT Broker	The device sent a Connection Request to the MQTT Broker and is waiting for the broker's response. This message indicates connection establishment is in progress. Wait for the device and broker to connect.
Trying to reconnect to MQTT broker	The connection between the device and the MQTT broker was lost and the device is trying to re-establish the connection. This message indicates connection re-establishment is in progress. Wait for the device and broker to re-connect.
Device is disconnected from MQTT Broker	Device is disconnected from the MQTT Broker.

To verify the device-broker connection status:

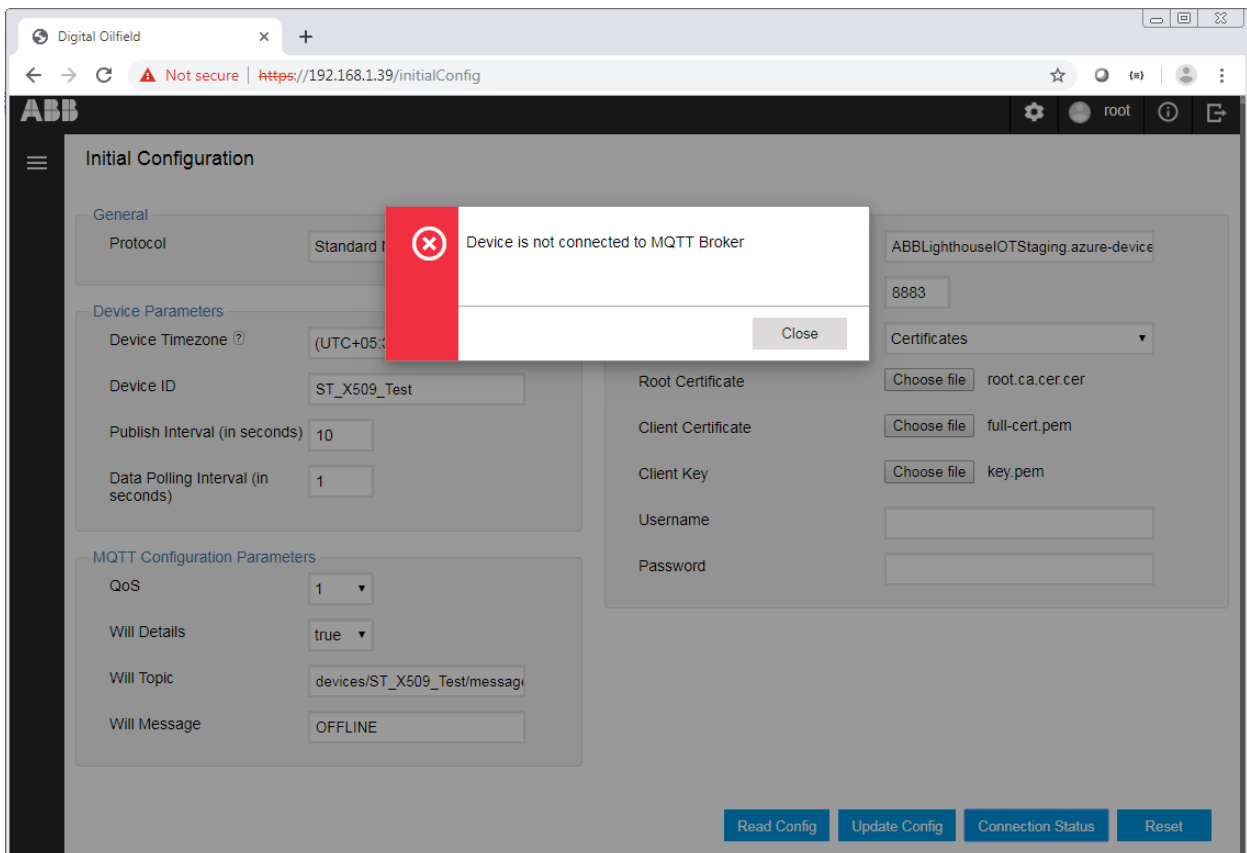
1. Click **Connection Status**.
2. Wait for status verification. A message indicating the status of the connection displays.
 - a. The message for a successful connection identifies that the device is connected to the MQTT broker and identifies the broker's hostname, the TCP port and the device ID.

Figure 3-19: Device-MQTT Broker connection status for successful connection



- b. The message for a failed connection attempt indicates that the device is not connected to the MQTT broker.

Figure 3-20: Device-MQTT Broker connection status for failed connection



- 3. Click **Close** to return to the initial configuration screen.
- 4. Proceed with the device configuration in section 4 [Device application configuration](#) when the device-broker connection is successful.

5. See section [6 Troubleshooting](#) if the device-broker connection fails. If you need to re-configure the device from scratch, reset to factory defaults as described in section [3.8 Reset device configuration](#).

3.8 Reset device configuration

In some situations, it may be necessary to reset the device MQTT configuration to its factory defaults. This can be useful when trying to troubleshoot connection issues. After reset, re-configure the required MQTT parameters and attempt connection again.



IMPORTANT NOTE: Resetting the device configuration will cause an existing device-broker connection to reset.

To reset the configuration:

1. Navigate to the Initial Configuration page.
2. Click **Reset**.

4 Device application configuration

The field device application configuration determines the application data that the device publishes on the cloud. The applications supported on the cloud are listed in [Table 1-5](#). The device publishes data only for those applications that are instantiated and enabled.

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.

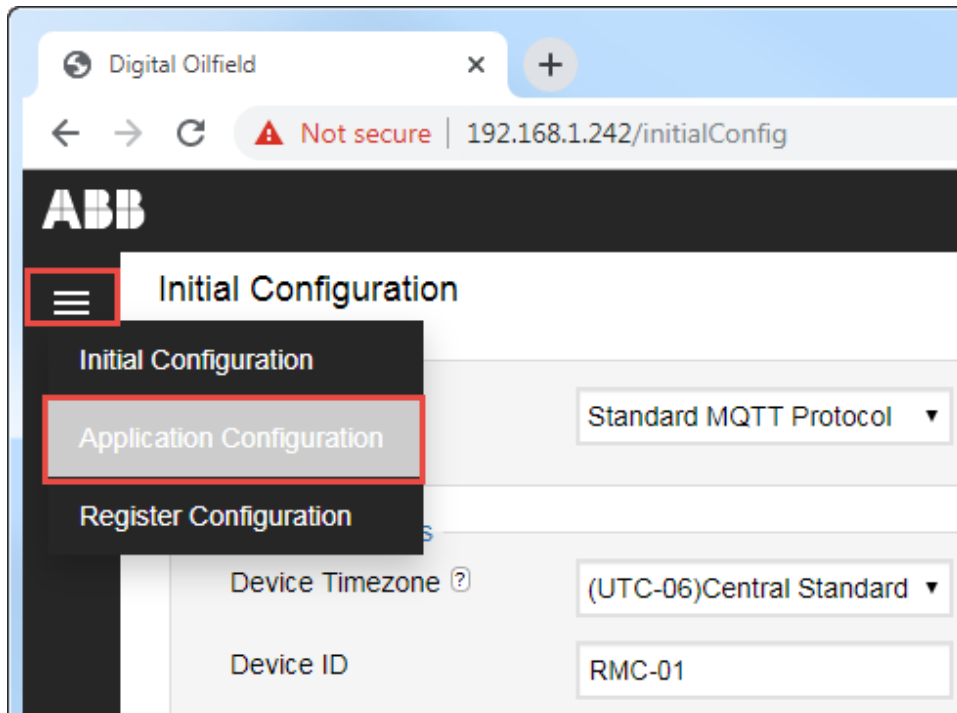
IMPORTANT NOTE: The application web page does not display unless the device has established connection with the MQTT broker.

4.1 Access the Application Configuration page

To access the Application Configuration page:

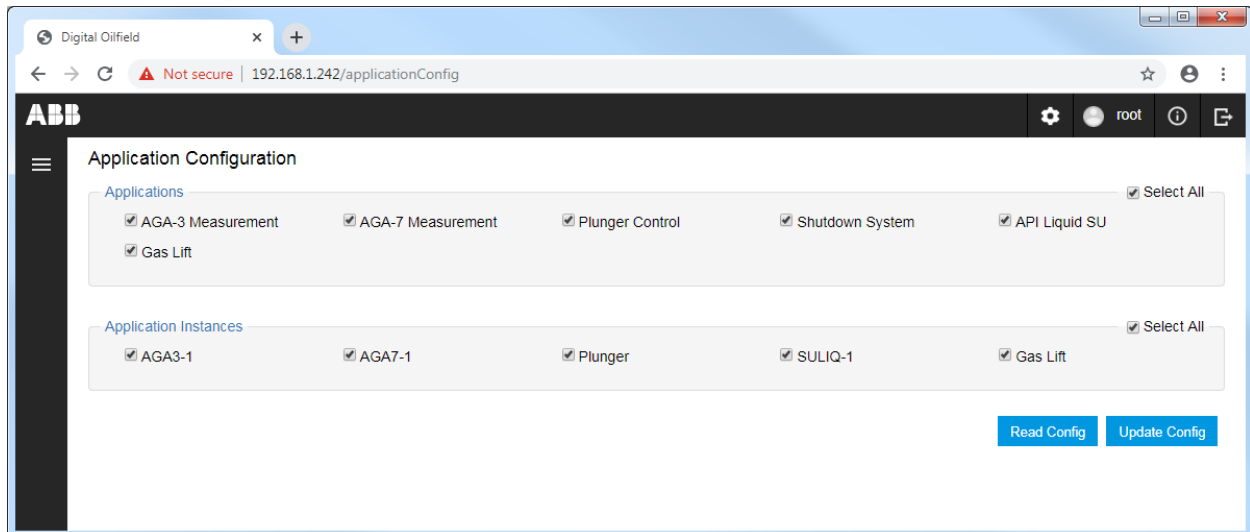
1. Click the menu icon on the left of the Initial Configuration web page.

Figure 4-1: Navigate to the Application Configuration page



2. Select **Application Configuration**. The Application Configuration web page displays.

Figure 4-2: Application Configuration web page



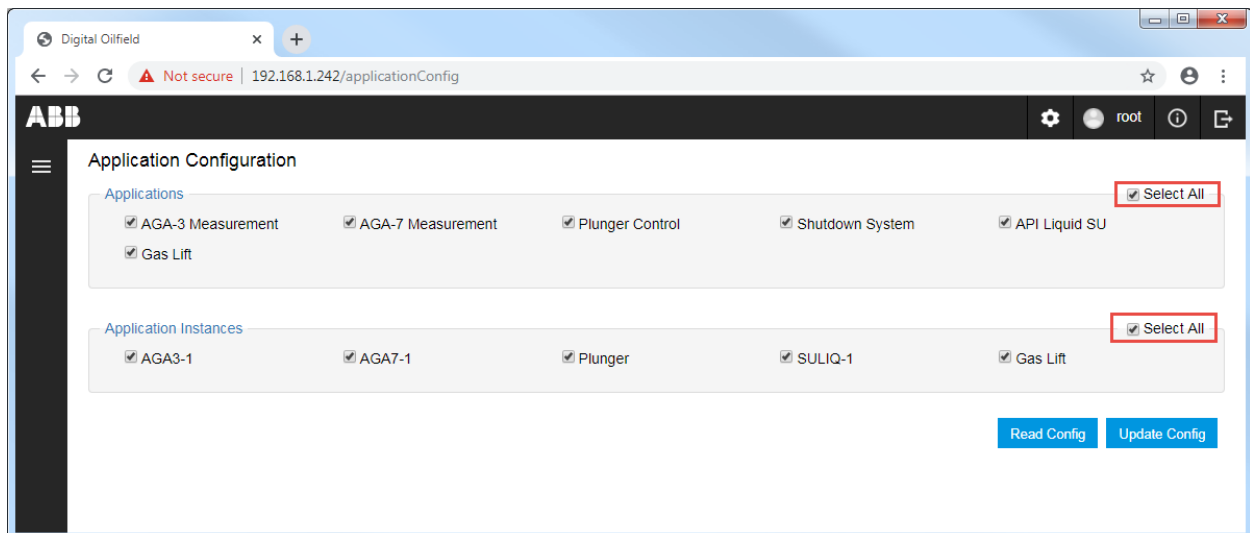
4.2 Enable application data publishing

IMPORTANT NOTE: The Applications list in the application configuration page shows all supported applications selected by default whether there are instances of those applications already configured in the device or not. This procedure assumes that all required instances for the operation of the device have been configured in PCCU. If all required instances are already configured and you plan to manage all applications on the cloud, skip this section. All applications and instances display automatically on the cloud interface.

To enable the applications and instances the device publishes data for:

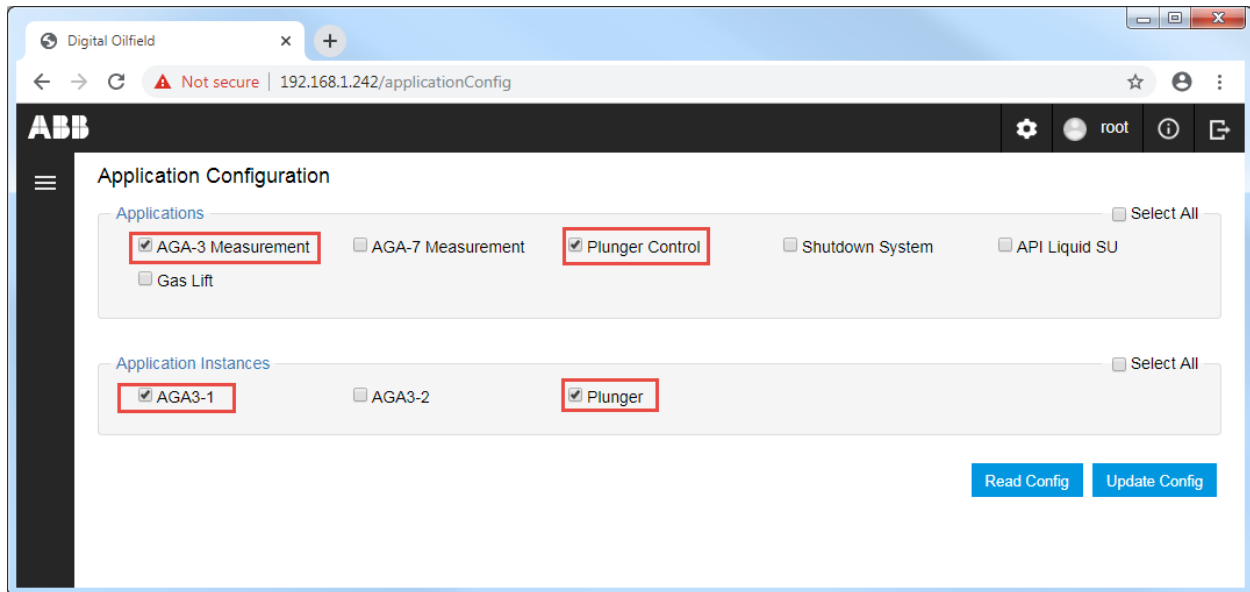
1. Enable all applications and all their instances ([Figure 4-3](#)):
 - a. Click **Select All** in the Applications section.
 - b. Click **Select All** in the Application Instances section.

Figure 4-3: Enable data publishing for all applications and instances



2. To enable specific applications or instances ([Figure 4-4](#)):
 - a. Locate and select the required application in the Applications section.
 - b. Locate and select the required instances for that application in the Application Instances section.
 - c. Repeat steps a and b for each required application.

Figure 4-4: Enable specific application and instances for data publishing

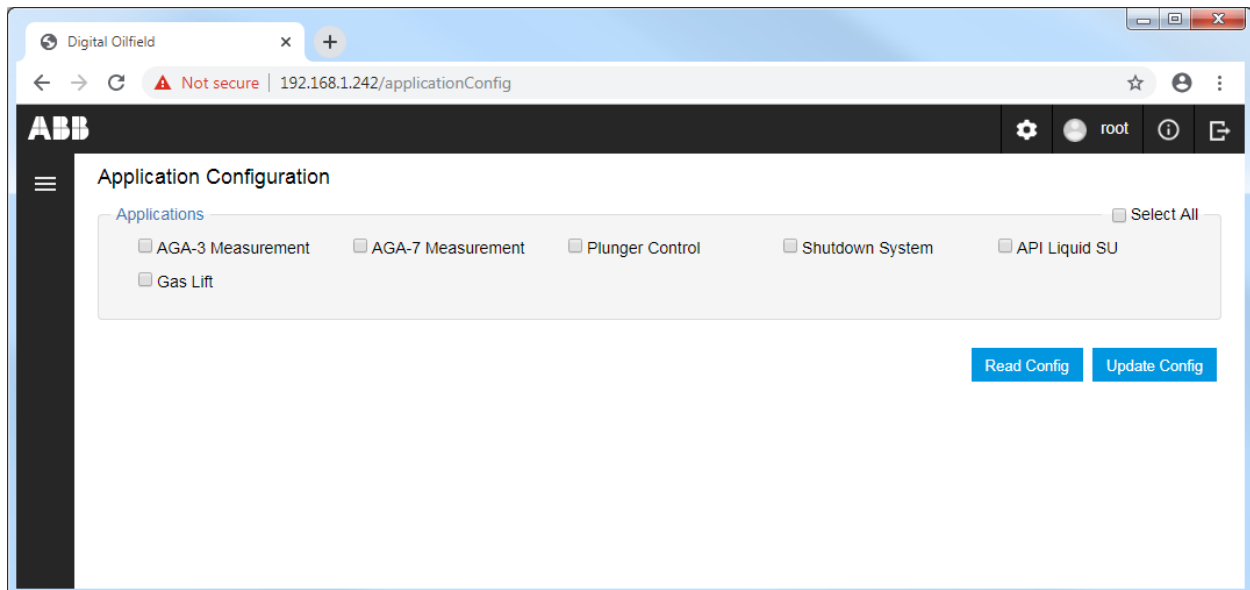


4.3 Disable application data publishing

To disable the applications and instances the device publishes data for:

1. When all applications are selected, clear **Select All**. All Applications checkboxes clear and the Applications instances list is no longer displayed.

Figure 4-5: Disable all applications



2. When not all applications are selected, locate and clear the application(s) checkbox in the Applications section. All instances for that application clear automatically.
3. To disable specific instances, locate and clear the required instance(s) checkbox in the Applications Instance section.

4.4 Update application configuration

Update the configuration when you have enabled or disabled applications or instances.

To update application configuration:

1. Enable or disable applications as described in sections [4.2](#) and [4.3](#).
2. Click **Update Config** ([Figure 4-6](#)). A confirmation for the update displays ([Figure 4-7](#)).

Figure 4-6: Update the Application Configuration

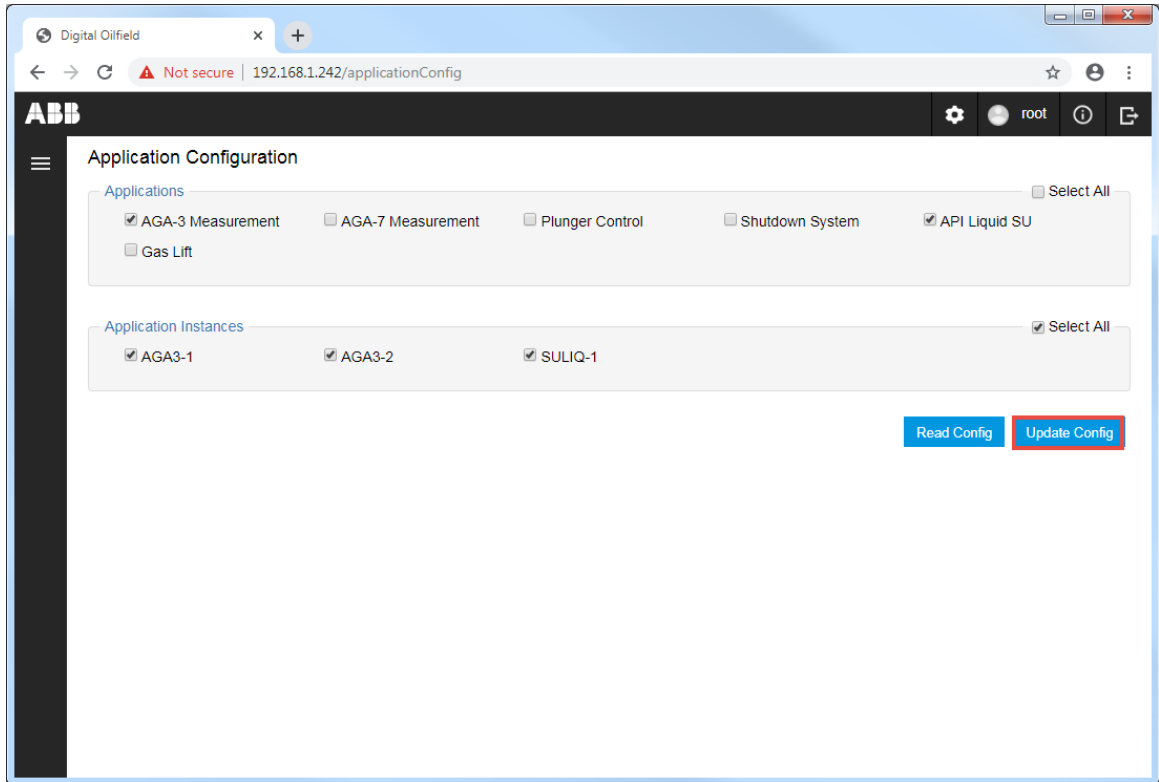
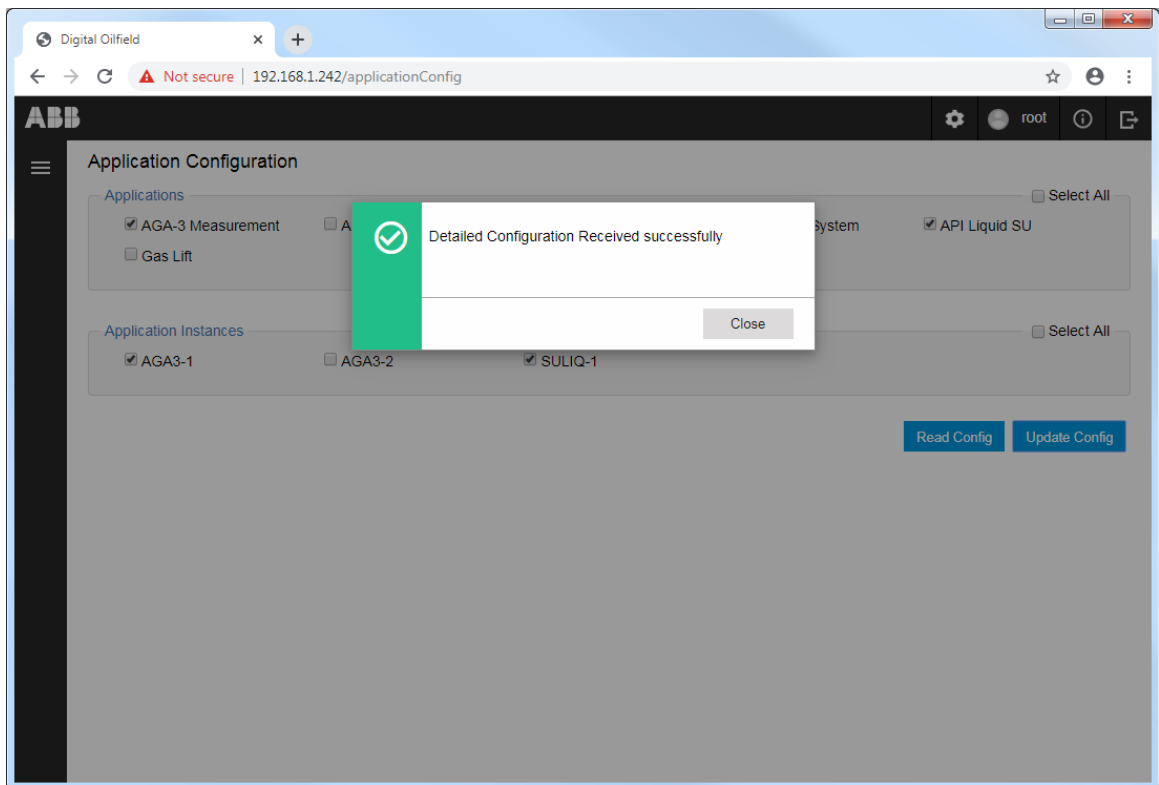


Figure 4-7: Update config successful message



3. Click **Close**.

5 Device register configuration

The field device register configuration determines the specific application register data that the device publishes on the cloud. These are application registers for the applications listed in [Table 1-5](#) and enabled in section [4: Device application configuration](#).

The Totalflow device registers contain the values of the application and instance variables. These values include calculated values, operation results, user-defined constants and parameters, user-defined values representing calculation methods, etc. The number and type of register values depend on the application type, number of instances, and the specific configuration.

The procedures in this section assume that the required applications are already instantiated, enabled and configured. 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.



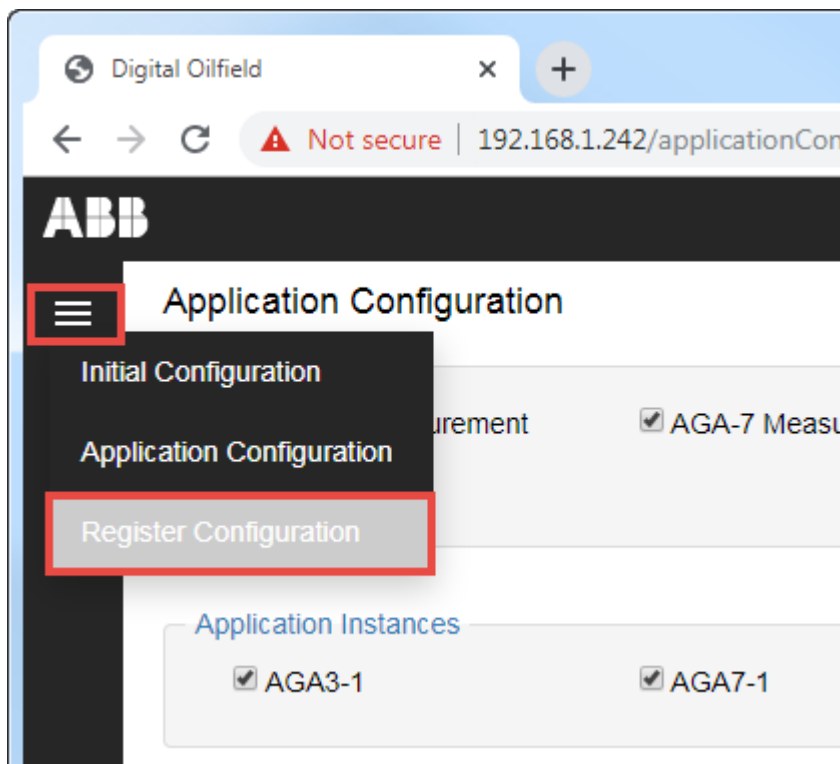
IMPORTANT NOTE: Registers are listed as variable names not numbers. There may be some data category or variable names that do not match register groups or names shown in PCCU tabs.

5.1 Access the Register Configuration page

To access the Register configuration web page:

1. Click the menu icon on the left of the Initial or Application Configuration web pages to display the list of device configuration web pages.

Figure 5-1: Navigate to the Register Configuration page



2. Select **Register Configuration**. The Register configuration web page displays.

5.2 Enable register data publishing

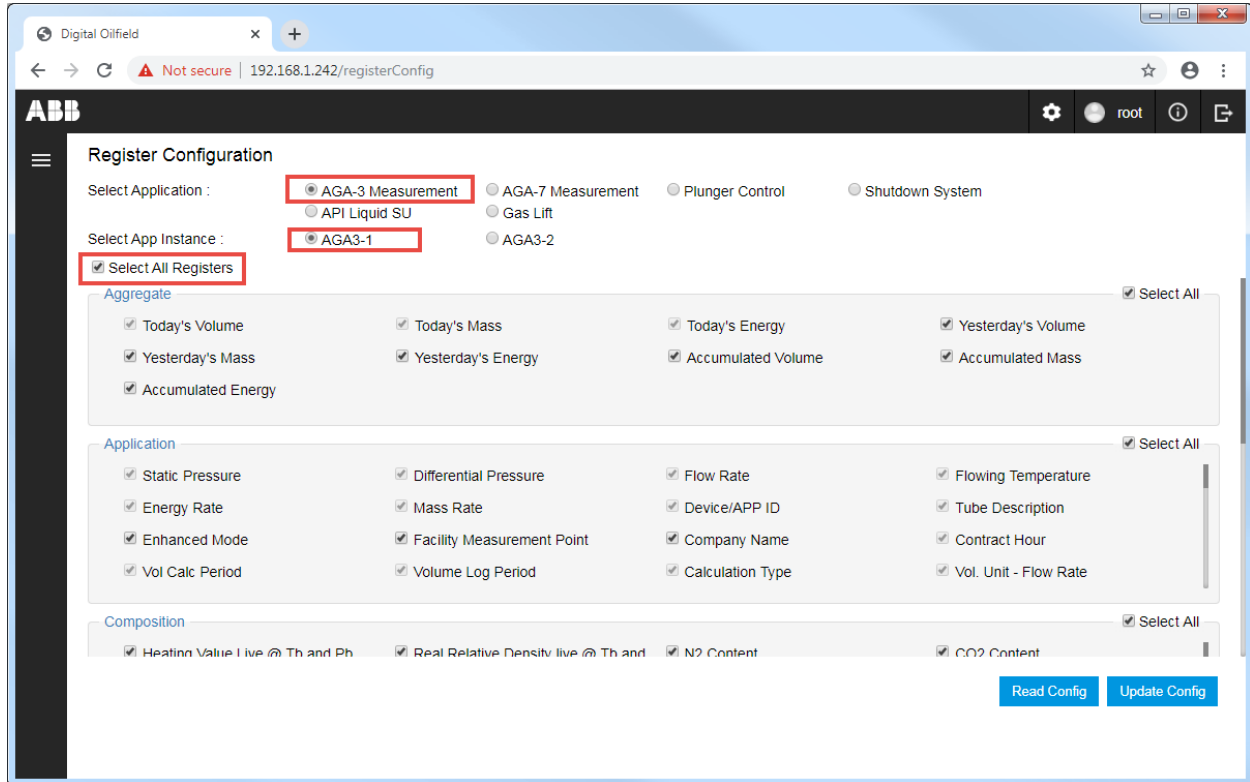


IMPORTANT NOTE: All supported registers are enabled for publishing by default.

Enable the register values to publish.

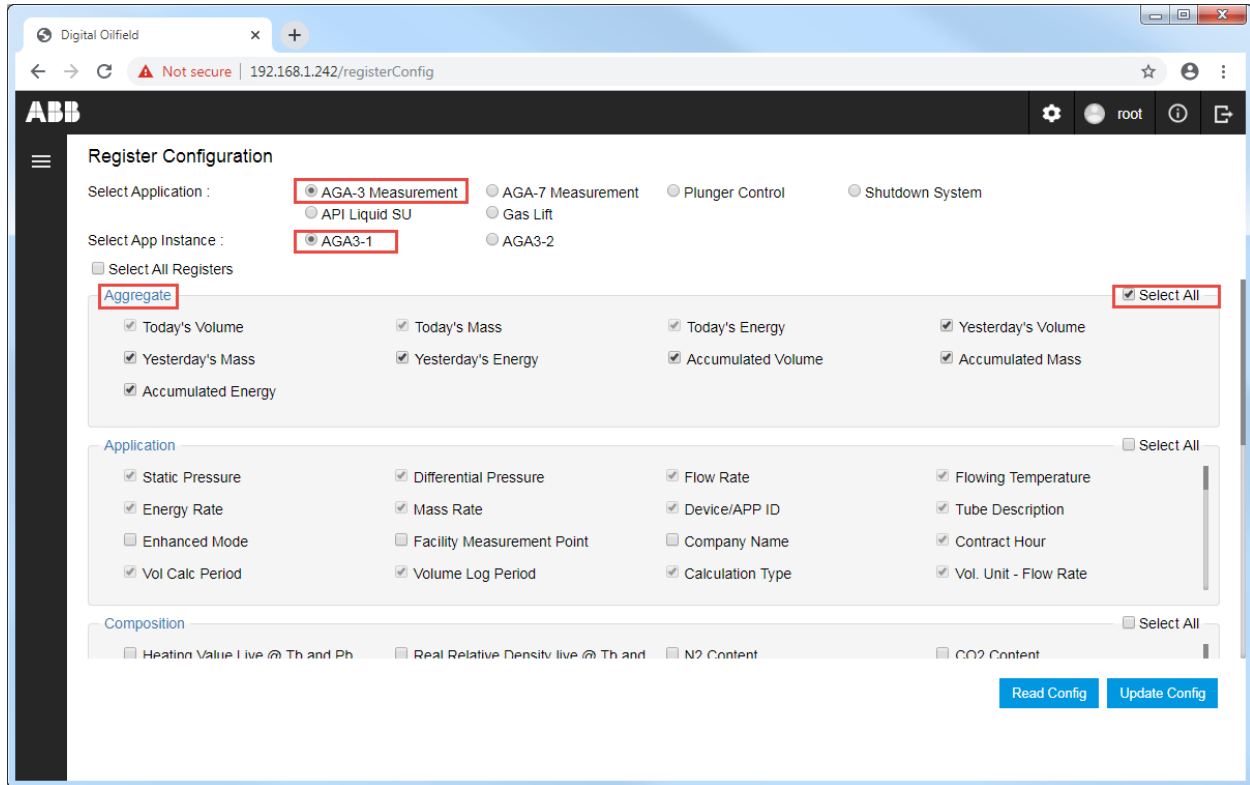
1. To enable all registers for an application:
 - a. Select the application.
 - b. Select the application instance.
 - c. Click **Select All Registers**.
 - d. Repeat steps a-c for each application requiring all registers.

Figure 5-2: Enable all registers for an application and instance



2. To enable an entire group or category of registers:
 - a. Select the application.
 - b. Select the application instance.
 - c. Clear **Select All Registers**.
 - d. Locate register section or group.
 - e. Click **Select All** for that section.

Figure 5-3: Enable all registers in a data category



3. To enable specific registers only:
 - a. Select the application.
 - b. Select the application instance.
 - c. Clear **Select All Registers**.
 - d. Locate the register group or category.
 - e. Clear **Select All**.
 - f. Locate the register(s) and select only the required register.
4. Update configuration as described in section [5.4](#).

5.3 Disable register data publishing

i **IMPORTANT NOTE:** Some registers are required and enabled by default from the factory. The configuration interface does not allow disabling these registers.

To disable the registers the device publishes data for:

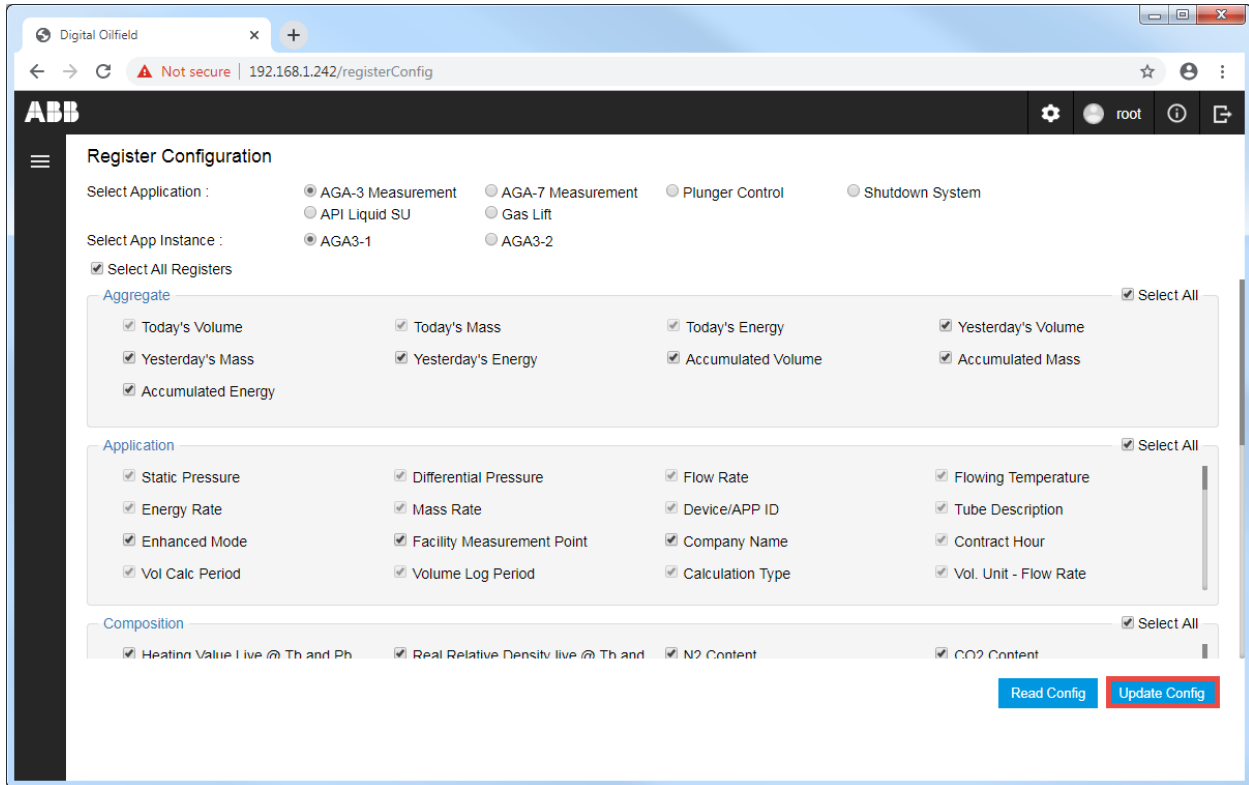
1. Select the application.
2. Select the application instance.
3. If **Select All Registers** or **Select All** boxes are selected, clear to disable publishing of the entire application register set or a register subset.
4. If **Select All Registers** or **Select All** are not selected, locate the specific register and clear to disable publishing.
5. Update configuration as described in section [5.4](#).

5.4 Update register configuration

To update register configuration:

1. Enable or disable registers as described in sections [5.2](#) and [5.3](#).
2. Click **Update Config**.

Figure 5-4: Update Register Configuration



3. Click **Close** when the configuration update is successful.

6 Troubleshooting device connection errors

6.1 User-device connection failure

User-device connection failure is the inability to connect to the device from the browser. There can be many reasons for failure. [Figure 6-1](#) shows a typical browser error message after an attempt to access the device from a laptop. [Figure 6-2](#) shows the error message when attempting to connect to a device that has MQTT functionality disabled.

Figure 6-1: User-device connection failure

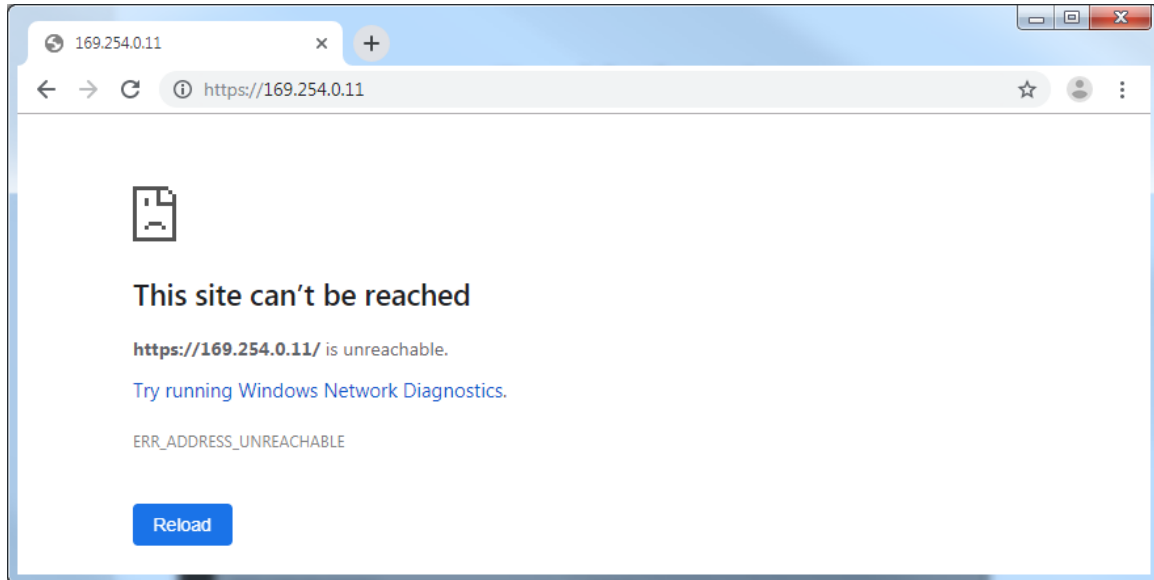
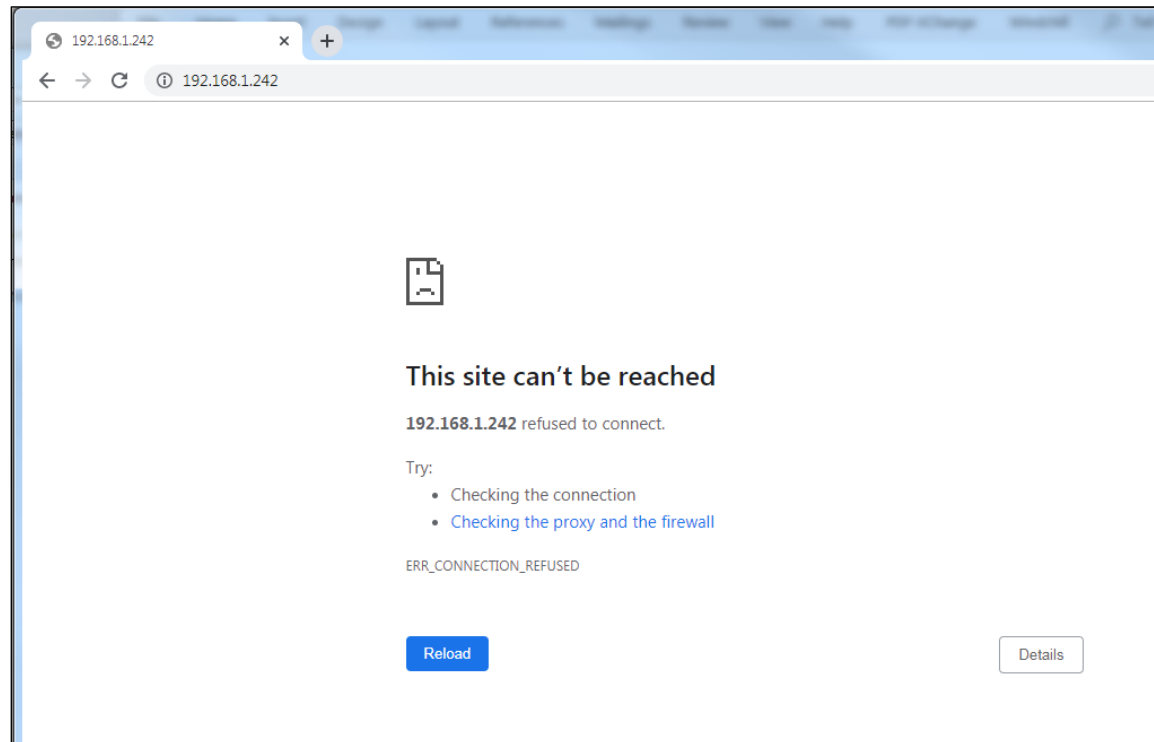


Figure 6-2: User-device connection failure (MQTT disabled on device)



6.1.1 Checklist to resolve failure to connect to field device

[Table 6-1](#) displays a checklist to troubleshoot and resolve connection failure. This is a basic list for common causes of failure. For more advanced troubleshooting, call technical support.



IMPORTANT NOTE: Use the required browser and version to access the device for configuration.

Table 6-1: Basic troubleshooting

Problem	Cause	Resolution
Connection failure	Disabled MQTT	<ul style="list-style-type: none"> – Enable MQTT as described in section 10.1.
	Incorrect URL	<ul style="list-style-type: none"> – Verify the URL required for the device. It should include the device IP address and the TCP port. For example: http://<device’s IP address>:443 – Type the correct URL on the browser and retry connection
	Incorrect IP configuration on the field device	<ul style="list-style-type: none"> – Verify the device’s IP parameter configuration. – Update to a valid configuration. – Restart device as necessary for IP configuration to take effect.
	Incorrect IP configuration on the laptop	<ul style="list-style-type: none"> – Obtain compatible IP parameters or verify the laptop has an IP address (if using DHCP). – Verify the laptop’s IP configuration and correct as necessary.
	Access to the device’s network port may be blocked or network is experiencing heavy traffic	<ul style="list-style-type: none"> – Verify field network connection or equipment configuration for possible port blocking and change configuration as required. – If port access is open, verify network performance on the Ethernet port. See Additional information for link to advanced Ethernet troubleshooting.
	Connection failure on the field device network	<p>Onsite:</p> <ul style="list-style-type: none"> – Verify Ethernet cabling or connectors are intact. Ensure the Ethernet cable connects the device and network equipment. – Ensure network equipment is operational and the network link is up. – Ping the device from the laptop. The device with a good network connection responds to the ping.

6.2 Device-Broker connection failure

Device-broker connection failure is the inability of the device to establish a connection with the MQTT broker. When the connection attempt fails, the device configuration interface displays error messages as the examples shown in [Figure 6-3](#) and [Figure 6-4](#).

Figure 6-3: Device-broker connection failure

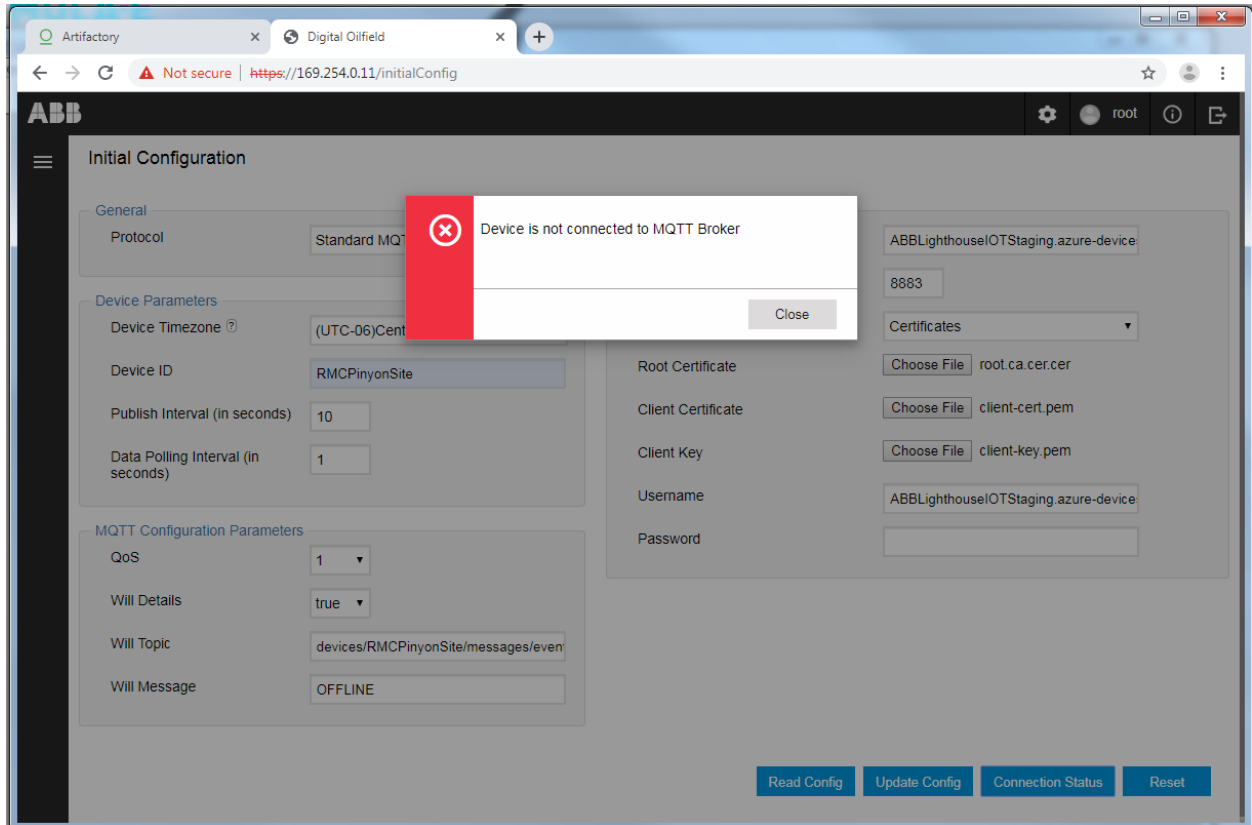
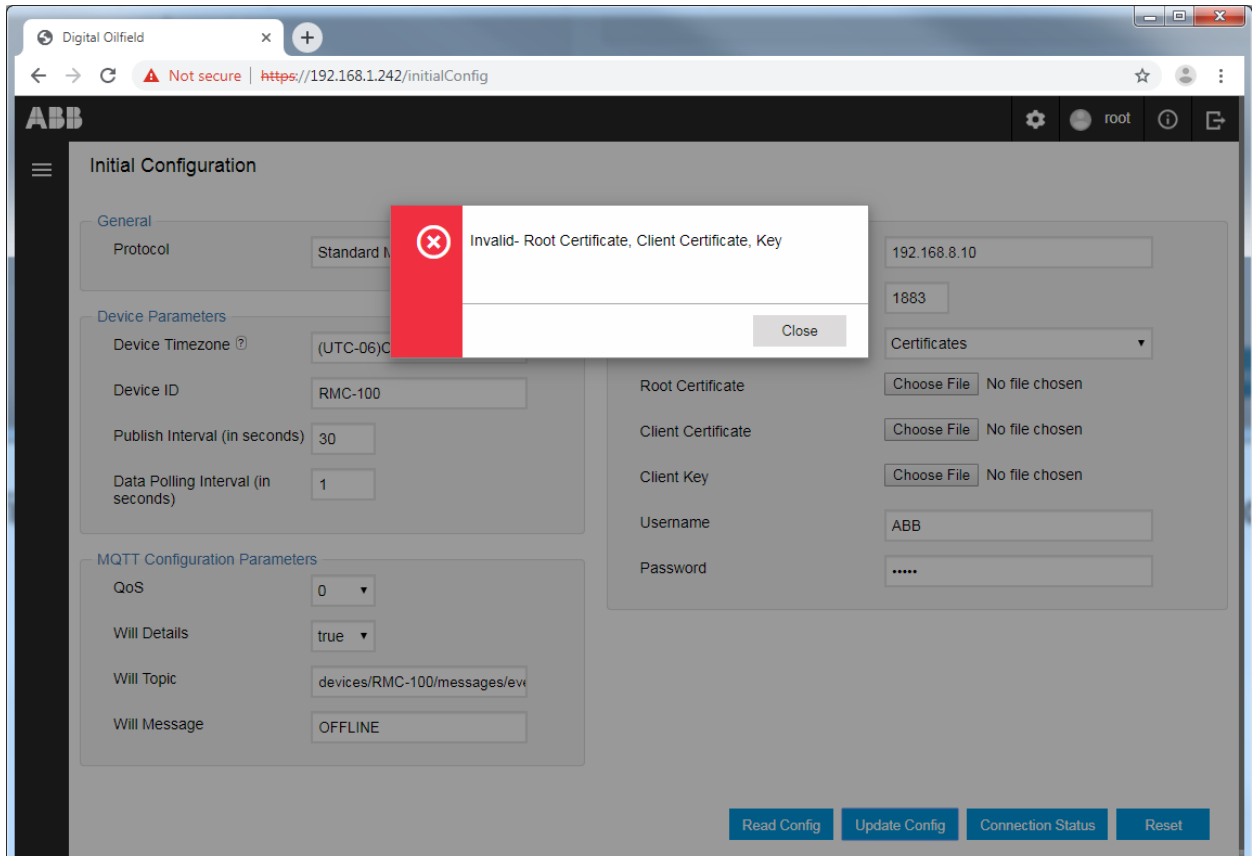


Figure 6-4: Device-broker connection failure (authentication failed)



6.2.1 Resolve failure to connect to cloud broker

Table 6-2 displays the most common causes of device-broker connection failure and how to resolve them. These are basic errors and resolution steps. For more advanced troubleshooting, call technical support.



IMPORTANT NOTE: Troubleshooting device-broker connection failures assumes you can connect to the device configuration interface. Configuration updates or verification require this connection.

Table 6-2: Basic troubleshooting checklist

Problem	Cause	Resolution
Connection failure	Incorrect MQTT broker details, device not able to establish TCP and MQTT connection	<ul style="list-style-type: none"> – Obtain the correct broker IP address or hostname. – Verify that the address and other broker details are configured correctly in the MQTT server details (initial configuration web page)
	Incorrect certificates, device not validated by broker	<ul style="list-style-type: none"> – Obtain the correct certificates for the device. Each device must have its own set of client certificate and client key. Root certificate can be common. – If incorrect certificates were used, update the configuration with the correct certificates in the MQTT server details (initial configuration web page). The new certificates overwrite the incorrect ones.
	Missing username (even when authenticating with certificates)	<ul style="list-style-type: none"> – Determine if a username and password are required in addition to certificates. Azure requires a username for additional security. Amazon Web Services (AWS) does not. For MQTT servers in Sparkplug implementations, consult with your administrator. – Obtain and configure username or password if required.

6.2.2 Upload the last successful configuration

The device stores the last configuration for a successful device-broker connection. Restore or activate that configuration to identify the origin of connection issues.

To restore the last successful configuration:

1. Navigate to the Initial configuration page.
2. Click **Read Config**. The device automatically tries to establish connection with the broker using the configuration just loaded.
3. Click **Connection Status** to see if the device was able to connect with the broker with this configuration.
 - a. If the connection status is OK, then connection failure with the other configuration is not due to network or cloud issues. Check configuration parameters carefully and re-configure if you have used incorrect values.
 - b. If the connection attempt fails, then determine other possible causes.



IMPORTANT NOTE: Authentication certificates do have expiration dates. If the last successful configuration does not result into a connection. Check certificates or generate new ones. Existing certificates in the device may have expired.

6.3 Advanced troubleshooting procedures

The procedures in this section require access to the device using SSH and SFTP. These services must be enabled on the device before connection and you must have the correct credentials. Obtain keys and passwords (passphrases) and store them in the laptop. For additional information, refer to the device's user manual (see [Additional information](#)), or the SSH and SFTP topics in the PCCU help files.



IMPORTANT NOTE: These procedures should be performed only by advanced users or ABB technical support or development personnel. Request default credentials for access from ABB. Call technical support for assistance.



IMPORTANT NOTE: These procedures require third-party SSH/SFTP client software. Download and install the client software as described in the RMC or XSeries^{G5} user manuals.



IMPORTANT NOTE: Make sure the device and laptop or PC used to connect with the device have a compatible IP parameter configuration. A local or remote network connection is required.

6.3.1 Verify processes from SSH

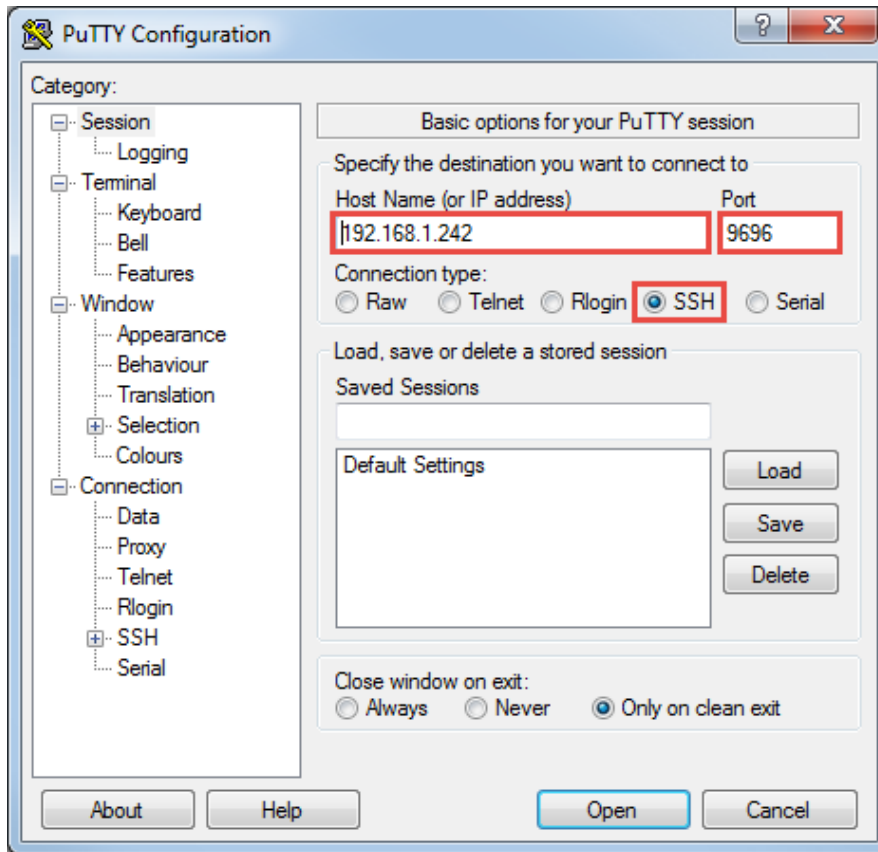
If unable to resolve issues with basic checks, verify that all required processes are running on the device. To verify processes, access the device using SSH and issue commands from the SSH client terminal.

The output of each of the commands should be the process-ID, followed by username (usually root), followed by executable name.

To verify processes running on the device:

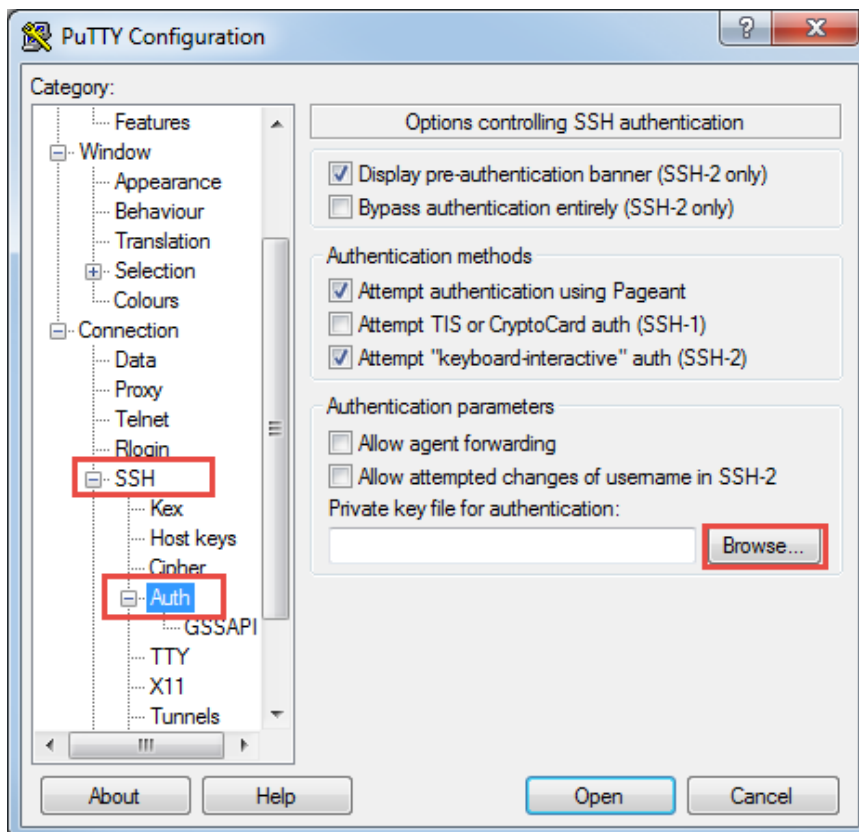
1. Ensure that the Totalflow device and the laptop are connected to the network.
2. Launch the SSH client application (for example PuTTY).
3. On the PuTTY Configuration window ([Figure 6-5](#)), select **Session** on the navigation tree and configure session parameters.
 - a. Type the device IP address into the Host Name field.
 - b. Type the TCP port for SSH on the device. For Totalflow devices this port number is 9696.
 - c. Make sure SSH is selected as the connection type.

Figure 6-5: PuTTY configuration – Session parameters



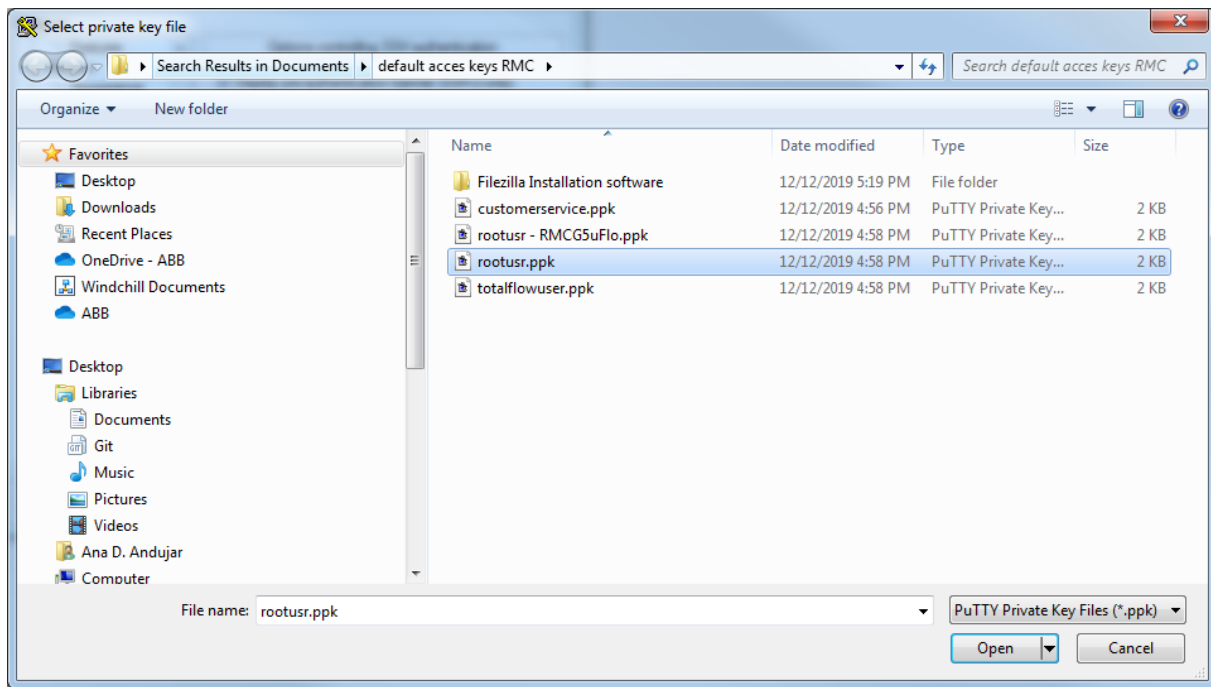
4. On the navigation tree select **Connection > SSH > Auth** (Figure 6-6).

Figure 6-6: Configure authentication key



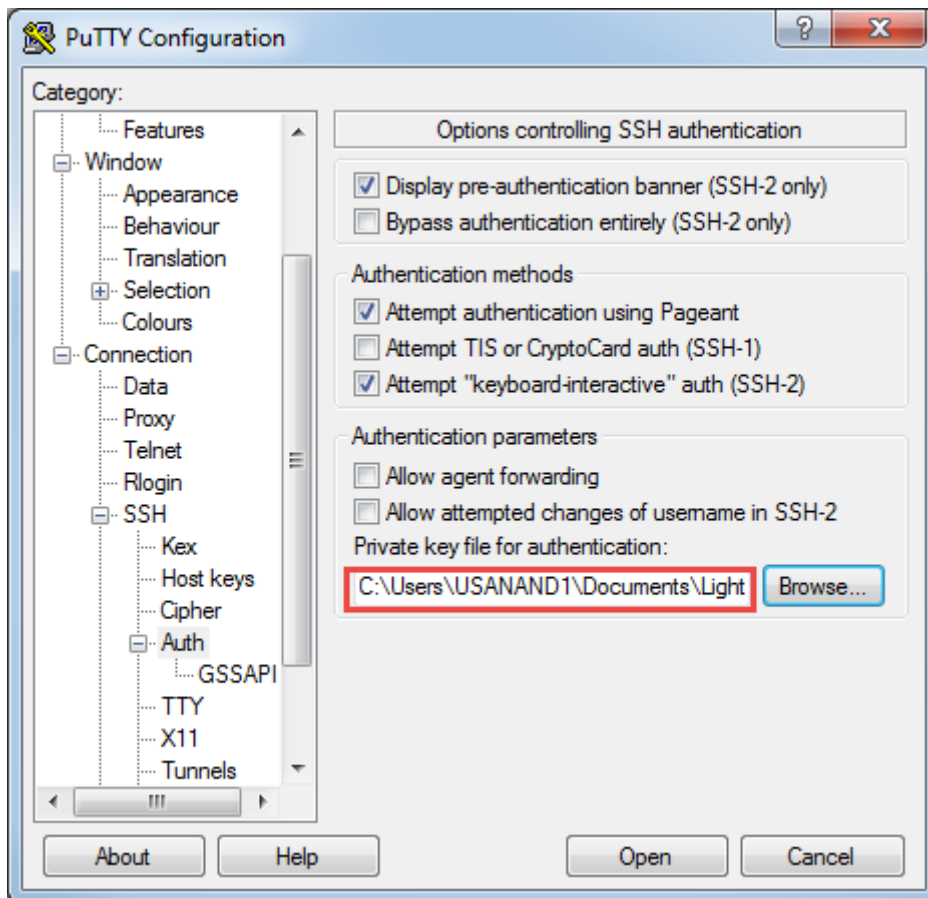
5. Click **Browse** to locate and select the key to authenticate ([Figure 6-7](#)).

Figure 6-7: Locate and select the authentication key



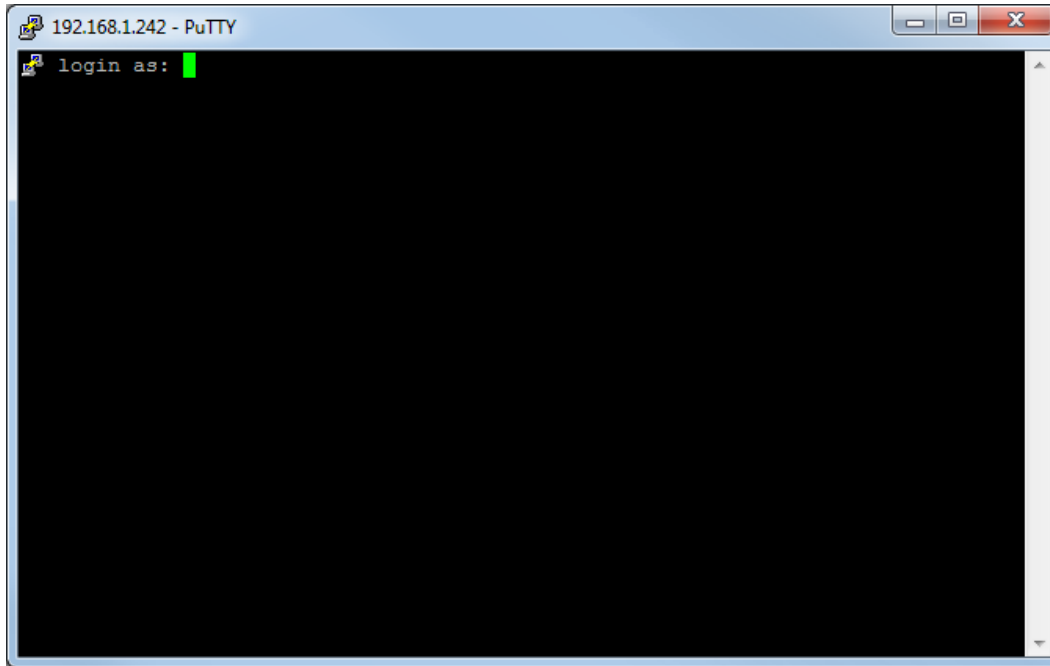
6. Click **Open**. The path to the key is configured for authentication ([Figure 6-8](#)).

Figure 6-8: Configure path to authentication key



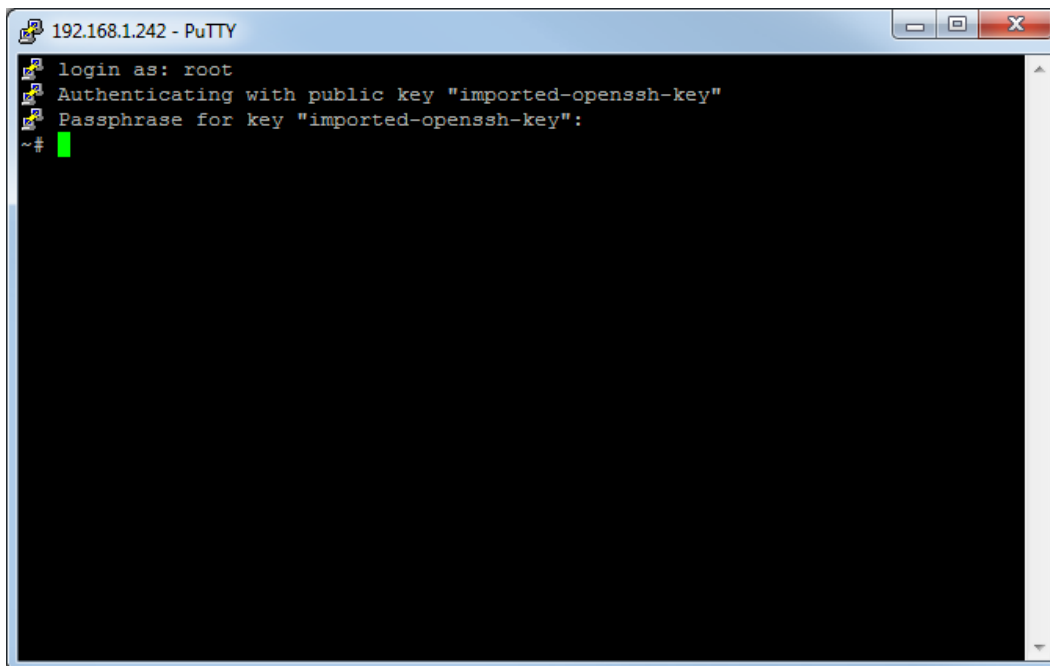
7. Click **Open**. The SSH terminal displays with the login prompt ([Figure 6-9](#)).

Figure 6-9: SSH terminal login prompt



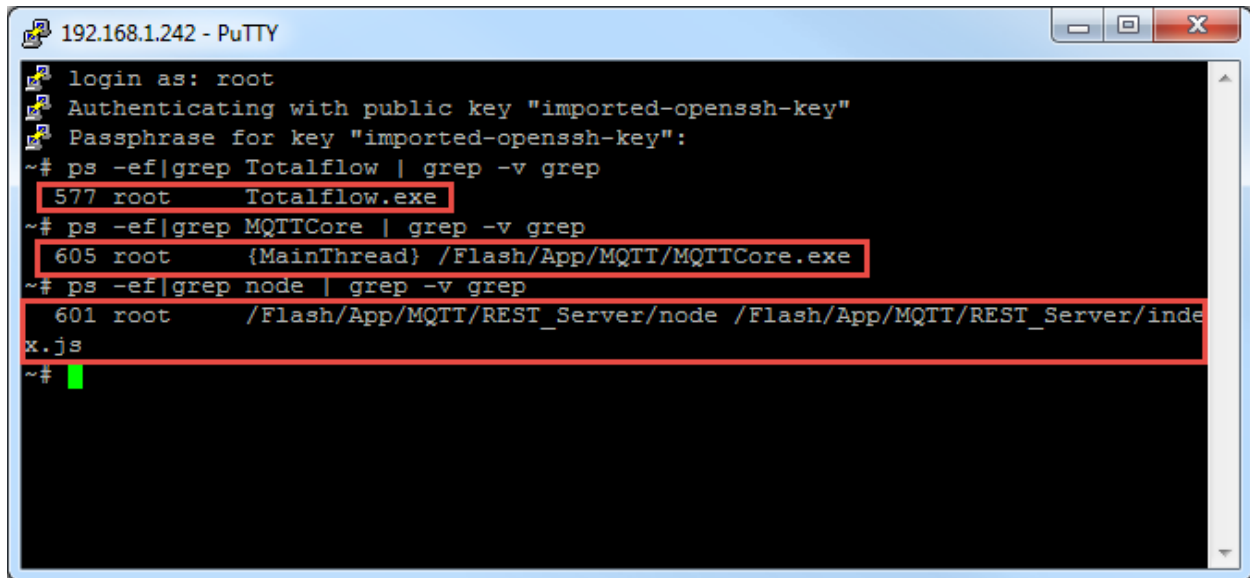
8. Type the user name at the prompt and press **Enter**.
9. Type the passphrase at the prompt and press **Enter**. The terminal prompt displays when authentication completes ([Figure 6-10](#)).

Figure 6-10: SSH authentication and successful connection



10. At the terminal prompt, type the following commands. Press the **Enter** key after each command to display result.
 - **ps -ef | grep Totalflow | grep -v grep**
 - **ps -ef | grep MQTTCore | grep -v grep**
 - **ps -ef | grep node | grep -v grep**
11. Verify that the processes are running, and no errors display. [Figure 6-11](#) shows that all three processes are running in the device.

Figure 6-11: Verify processes are running correctly



```
192.168.1.242 - PuTTY
login as: root
Authenticating with public key "imported-openssh-key"
Passphrase for key "imported-openssh-key":
~# ps -ef|grep Totalflow | grep -v grep
577 root      Totalflow.exe
~# ps -ef|grep MQTTCore | grep -v grep
605 root      {MainThread} /Flash/App/MQTT/MQTTCore.exe
~# ps -ef|grep node | grep -v grep
601 root      /Flash/App/MQTT/REST_Server/node /Flash/App/MQTT/REST_Server/inde
x.js
~#
```

12. If any or all the processes are not running or errors display, contact ABB technical support. MQTT may be disabled or errors have caused the main application to stop running.
13. Type **Exit** at the prompt to close the SSH section.

6.3.2 Collect logs using SFTP

ABB technical support or developers use device log files to help troubleshoot if operators are unable to resolve issues in the field. This procedure describes how to download those logs from the device to a laptop using Filezilla, the SFTP client.

The files that ABB requires reside in the /mmcData directory in the device:

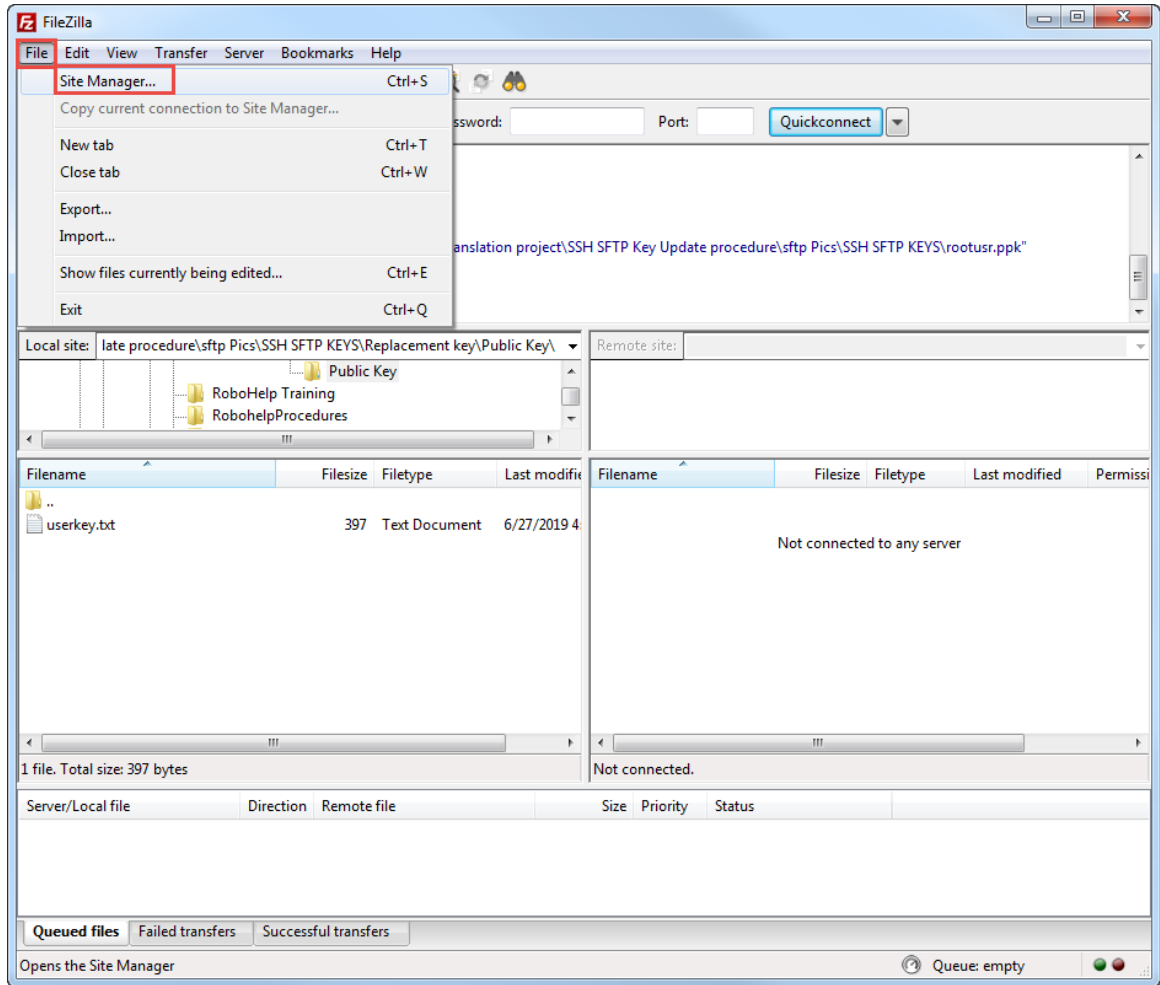
- Logs
- mqtt
- CoreDumps

i **IMPORTANT NOTE:** This procedure assumes that you are familiar with SFTP client access to the device. It should be performed only by advanced users or ABB technical support or development personnel. Call technical support for assistance.

To download files from the device:

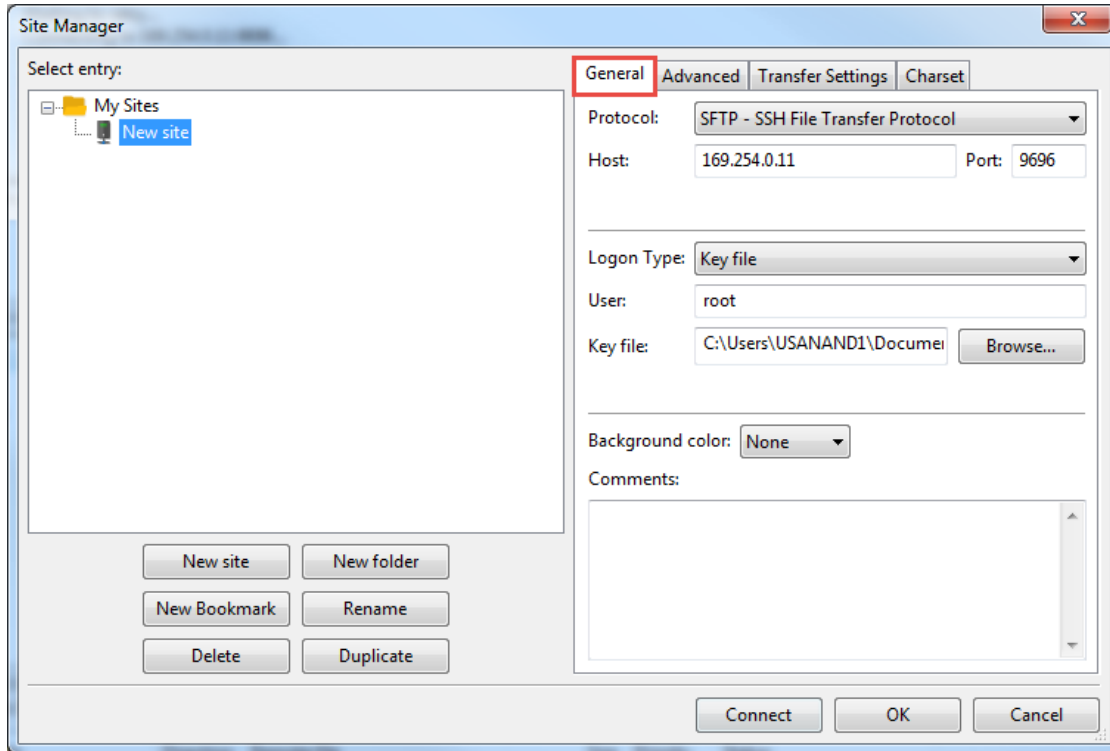
1. Ensure that the Totalflow device and the laptop are connected to the network.
2. Launch the SFTP client application (in this example, FileZilla).
3. Select **File>Site Manager** from the top menu ([Figure 6-12](#)).

Figure 6-12: Launch Site Manager



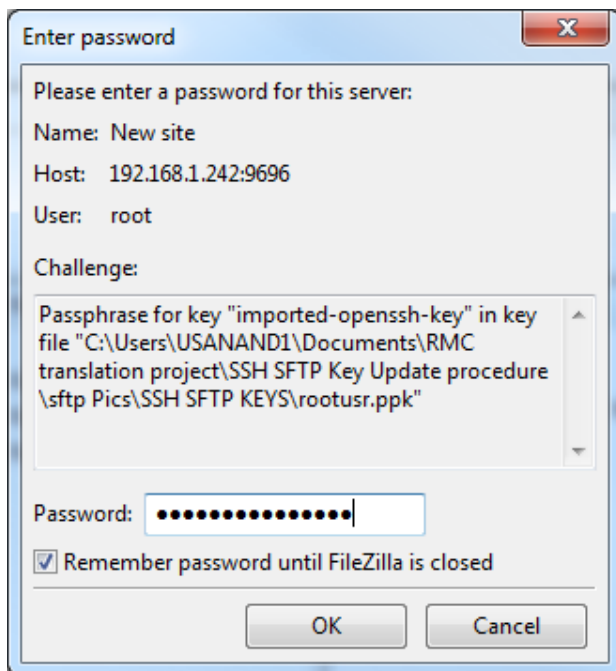
4. Configure the **General** tab parameters on the Site Manager dialog displays ([Figure 6-13](#)).

Figure 6-13: Configure connection parameters on Site Manager



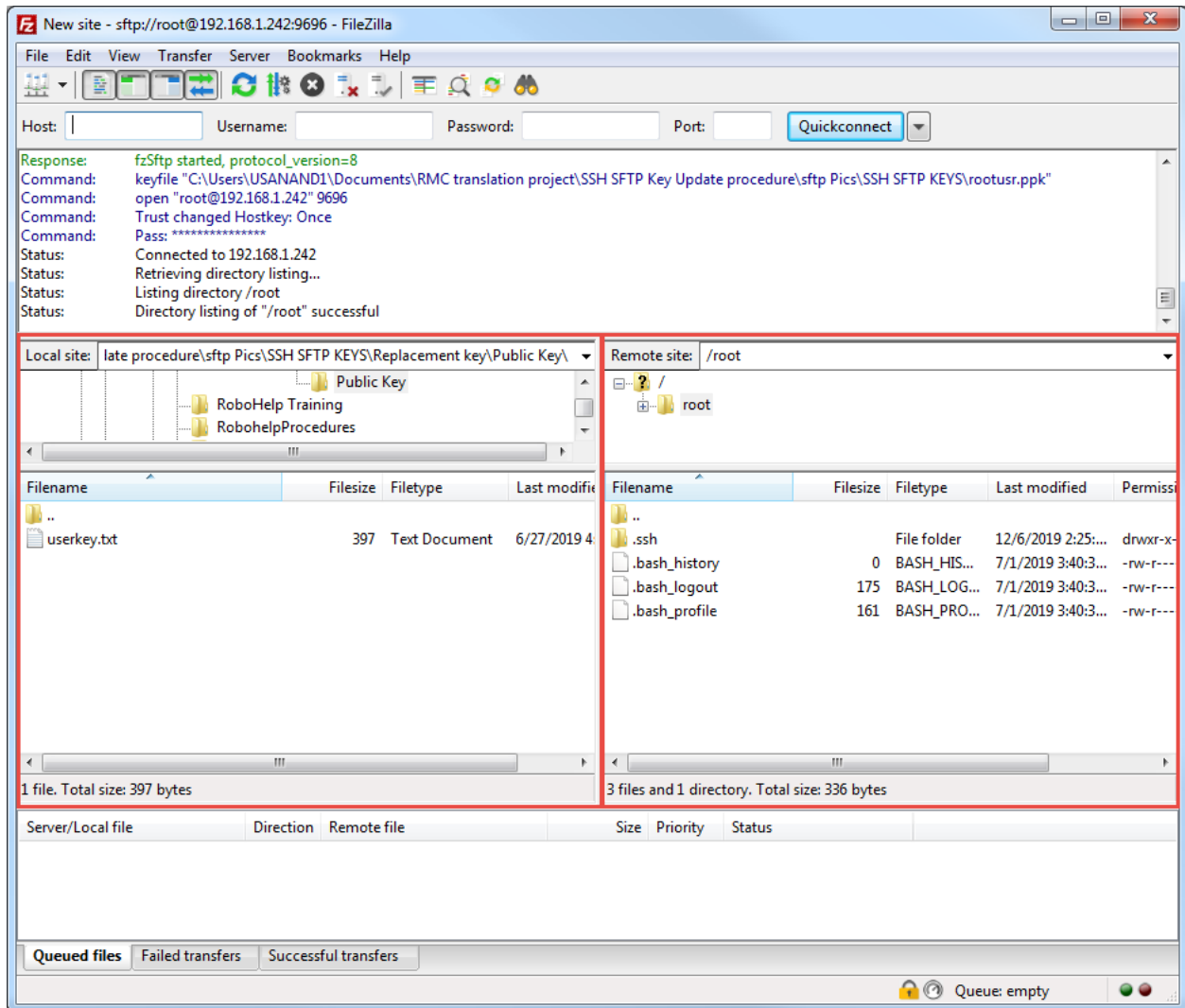
- Protocol: Select **SFTP- SSH File Transfer Protocol** from the drop-down list.
 - Host: Type the device’s IP address.
 - Port: Type **9696**.
 - Logon Type: Select **Key file** from the drop-down list.
 - User: Type **root**.
 - Key file: Click **Browse** to locate and select the current private key stored in your laptop.
5. Click **Connect**. If the private key is passphrase-protected, an additional pop-up displays and requests the passphrase before granting the connection. Type the passphrase into the Password field ([Figure 6-14](#)).

Figure 6-14: Type password or passphrase



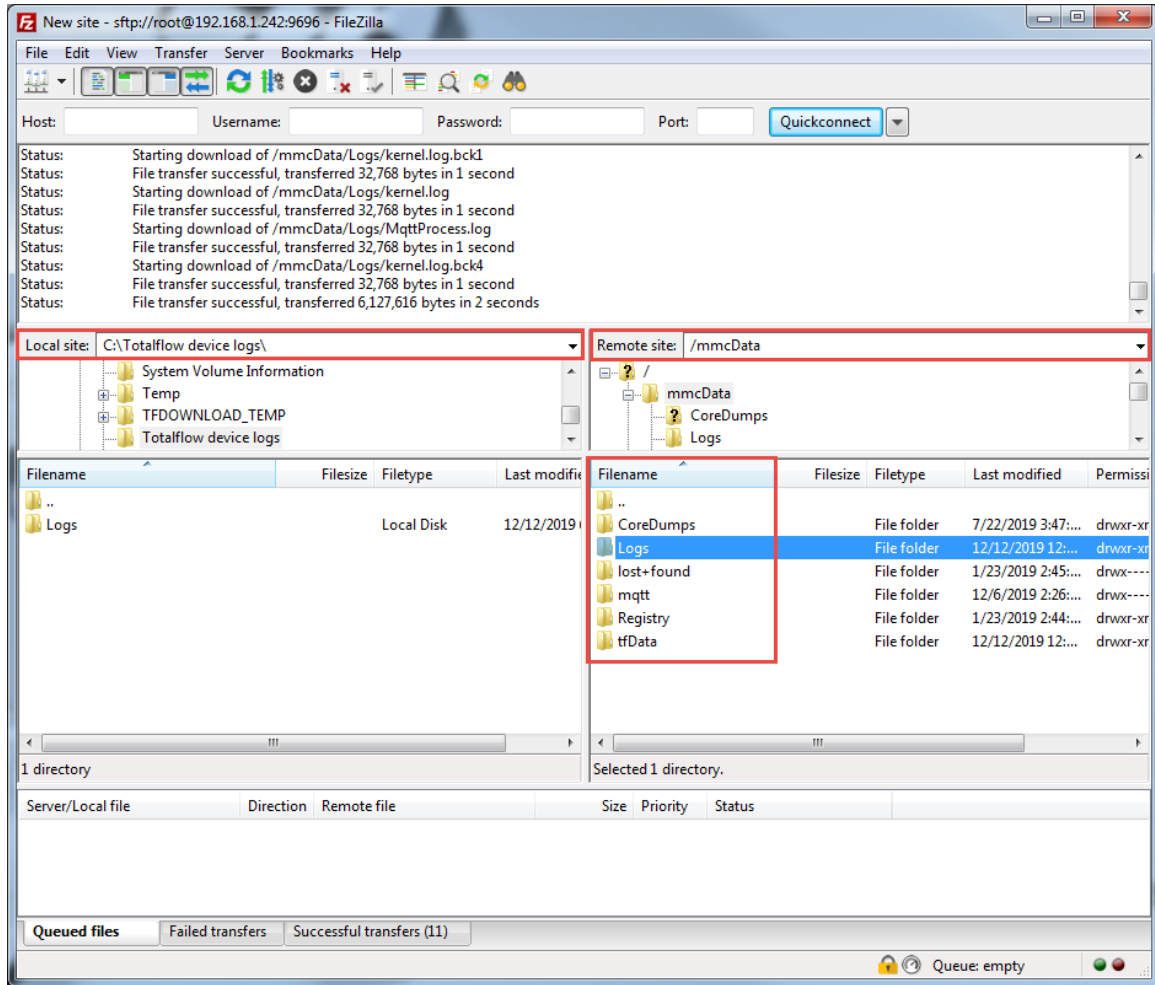
6. Click **OK**. The connection with the device is successful when FileZilla displays the file directories of the laptop or PC (Local Site, on the left) and the device (Remote site, on the right) ([Figure 6-15](#)).

Figure 6-15: FileZilla New Site window



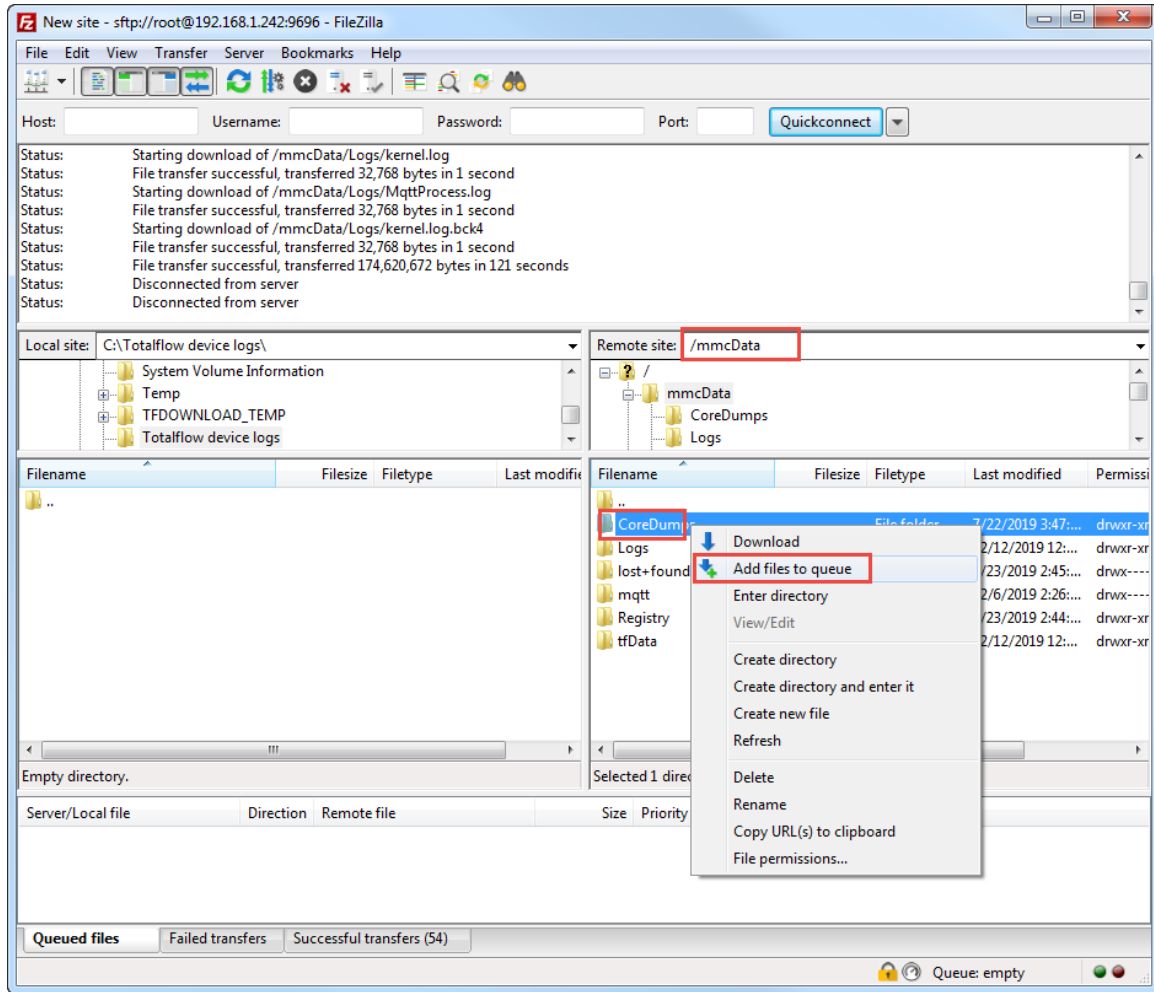
7. Navigate to the required directories on both the laptop and the device ([Figure 6-16](#)):
 - a. On the Local Site (laptop), use the navigation tree or type the path for the directory to store the logs.
 - b. On the Remote Site field, type **/mmcData**. The required logs display.

Figure 6-16: Navigate to required paths on laptop and device



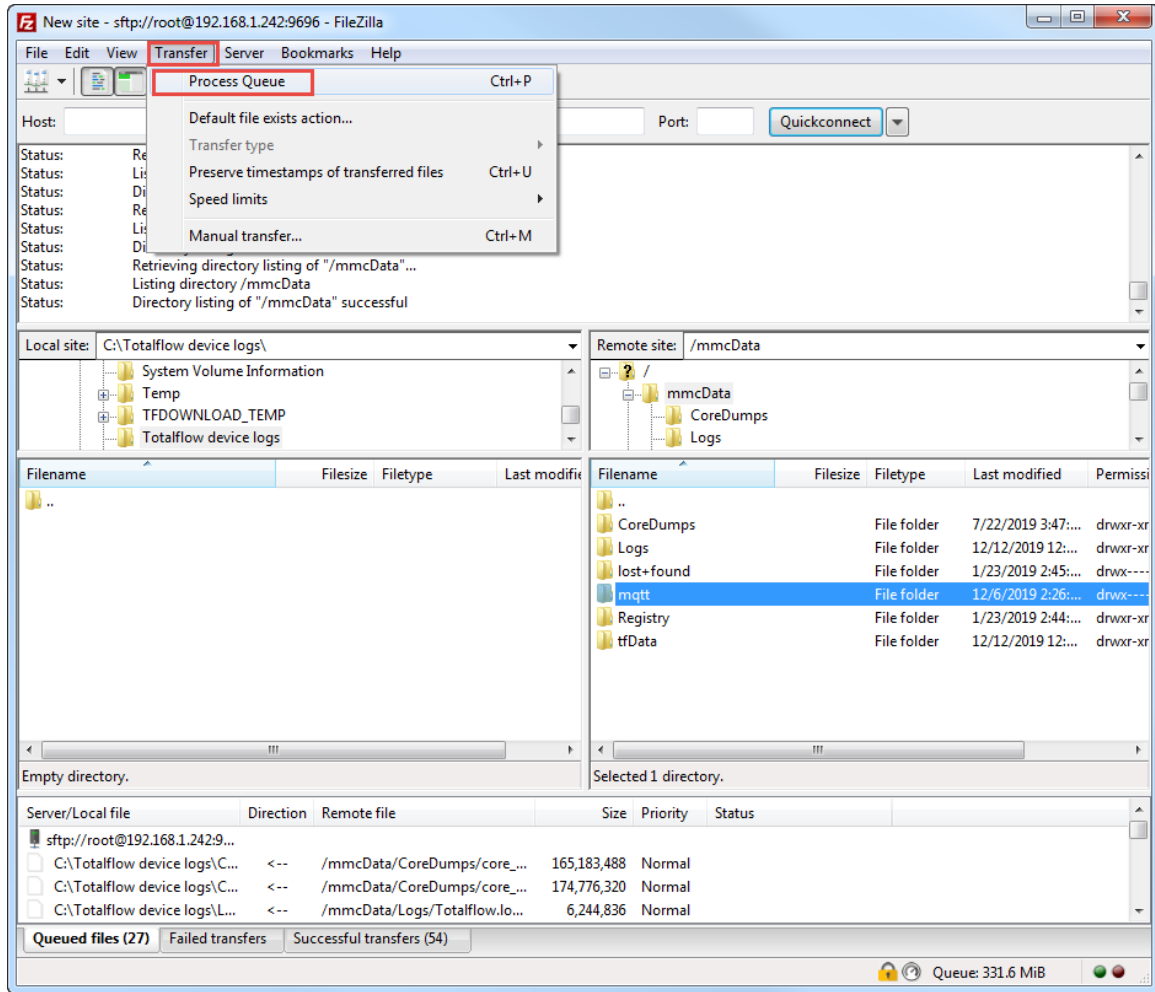
8. To download files, select a file a time, right click, and select **Add files to queue** (Figure 6-17).

Figure 6-17: Add files to download queue



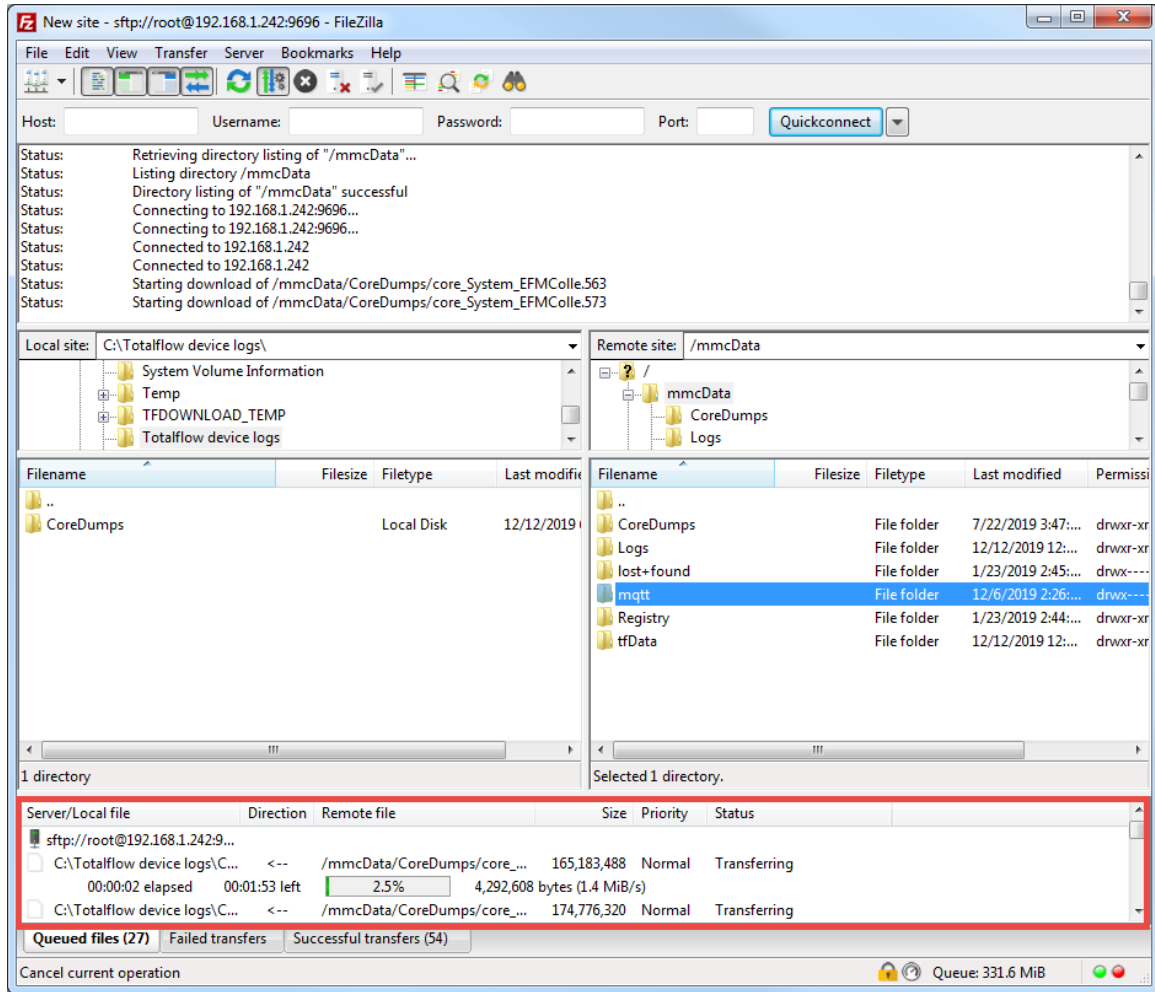
9. After all files are in the queue, select **Transfer>Process Queue** (Figure 6-18). The file download begins. The transfer progress displays below.

Figure 6-18: Start file download (process queue)



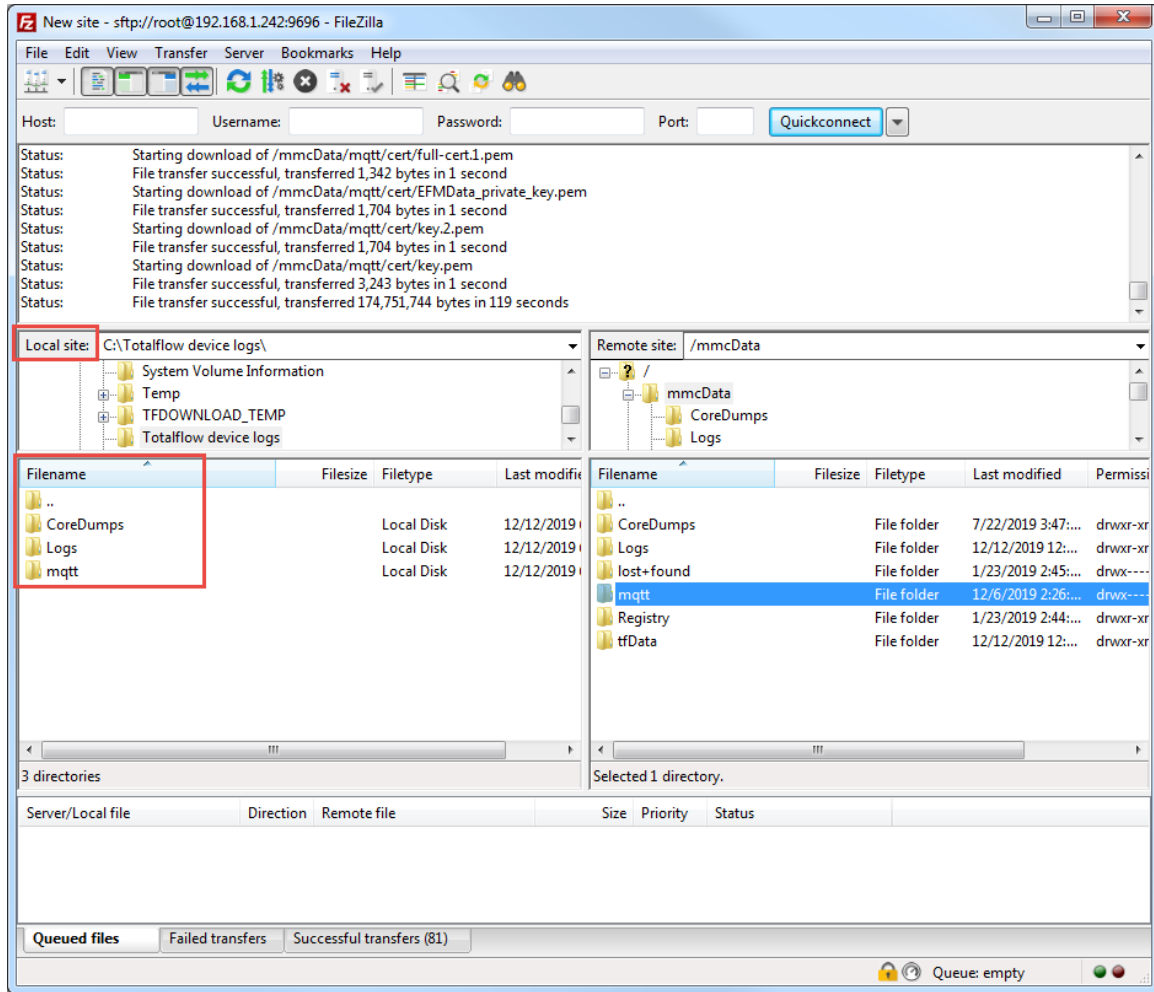
The file download begins. The transfer progress displays below ([Figure 6-19](#)).

Figure 6-19: Log transfer progress bar and status



10. Wait for the transfer of all files to complete.
11. Verify the file download on the Local Site. The local site should display all required files ([Figure 6-20](#)).
12. Provide files to ABB technical support or developers.

Figure 6-20: Verify file download



6.4 Troubleshooting when using Sparkplug

The following error conditions can be present in implementations using Sparkplug. This information assumes that an Ignition® SCADA system is used. In addition to SCADA capabilities, this system can have several MQTT-enabling software modules to provide web support for device data access. This section assumes that the system contains the MQTT Distributor and MQTT Engine modules. The Distributor module performs the MQTT server functions (allows field device connection). The Engine module processes bi-directional communication with the field device once a secure connection is established between the device and the server.



IMPORTANT NOTE: Consult vendor documentation for the Ignition system and modules for additional details. This section provides only basic information and typical errors.



IMPORTANT NOTE: Be sure to disable the following settings in the MQTT Engine: Block Node Commands and Block Device Commands.

[Table 6-3](#) shows basic errors when using Ignition SCADA.

Table 6-3: Error condition in Sparkplug implementation

Problem	Cause	Resolution
Connection status message displayed on the configuration	The MQTT Distributor is enabled, but the MQTT	Make sure to enable the MQTT Engine.

Problem	Cause	Resolution
interface: Device is connected to Sparkplug MQTT broker, but MQTT Engine is Offline.	Engine is disabled. The device is able to establish connection with the broker, but no further communication is processed.	
Sparkplug tags in Ignition Designer indicate stale data values.	Update of data values has failed.	Disable and then re-enable the MQTT functionality. See section 10.1.
Device and MQTT broker are still connected but Sparkplug tags in Ignition Designer indicate stale data values	Update of data values has failed.	Disable and then re-enable the MQTT functionality. See section 10.1.
Device - MQTT broker connection lost	Several reasons can cause connection loss, including loss of network connection or issues with Ignition server functionality (for example an expired Ignition license).	<p>If physical or network connection causes have been eliminated, restart the MQTT functionality on both device and MQTT server:</p> <ul style="list-style-type: none"> - Start and stop Ignition service (Task manager > services > Ignition gateway), right click on Ignition gateway and select Stop Service. This restarts all the modules. - Disable and then re-enable the MQTT functionality. See section 10.1.

7 Access the Digital Oilfield

The Digital Oilfield provides access to device and application data for each of the Totalflow applications supported.



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

7.1 Log into the Digital Oilfield

This procedure assumes you are an authorized user and your account and credentials are already available. Your privileges depend on the role assigned to your account. Obtain the URL to your domain and login credentials from your administrator.

To log into the cloud:

1. Make sure you have a supported web browser version on the system you use to log into the cloud. See supported versions in [Table 1-4](#).
2. Launch a web browser.
3. Go to the URL provided by your administrator. The Login prompt displays.



IMPORTANT NOTE: Login screens may show a different service provider in the sign in option. The example in [Figure 7-1](#) below shows a sign in option with Microsoft. This option is available when using Azure as the cloud service provider. For other providers, the appropriate name displays.

Figure 7-1: Login prompt to access the ABB Digital Oilfield

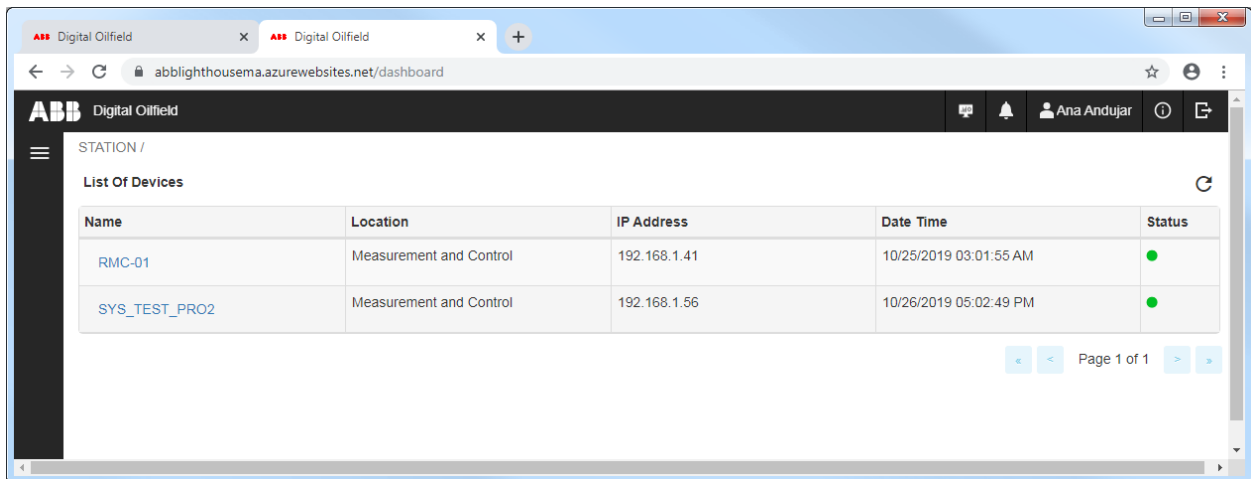
A screenshot of a web browser showing the ABB Digital Oilfield login interface. At the top left, the ABB logo is displayed in white on a black background. The main content area is white and contains a light gray rectangular box with the following elements: the text 'ABB Digital Oilfield' at the top; a 'Username:' label followed by a text input field containing the placeholder text 'Username'; a 'Password:' label followed by a text input field containing the placeholder text 'Password'; and a blue rectangular button with the text 'Submit' centered on it.

4. Sign in or type credentials at the login prompt. The main Digital Oilfield screen displays.



IMPORTANT NOTE: Devices with the green indicator in Status column are connected to the cloud. Devices with the red indicator are not connected to the cloud and their current data is not available for monitoring. Only old data displays for disconnected devices.

Figure 7-2: Digital Oilfield main screen



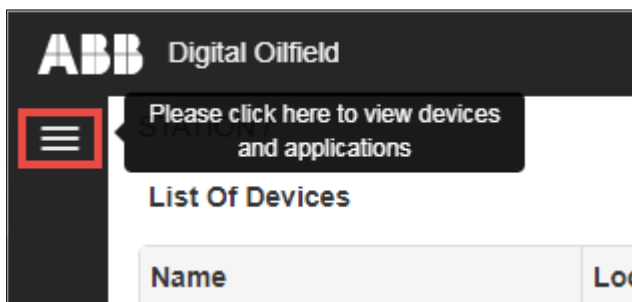
7.2 Navigate to devices and applications

The Digital Oilfield main page displays basic device information but not detailed application data. To locate devices and navigate to application data pages, it is best to use the navigation tree view.

To view devices and their applications from the tree view:

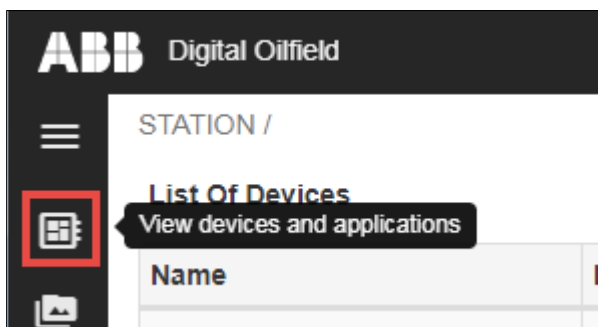
1. Click the menu icon ([Figure 7-3](#)).

Figure 7-3: Menu icon



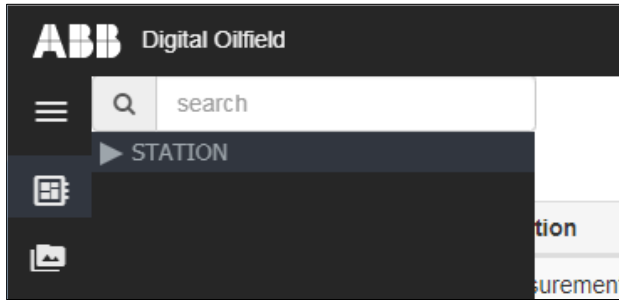
2. Click the device and application view icon ([Figure 7-4](#)).

Figure 7-4: Device and application view icon



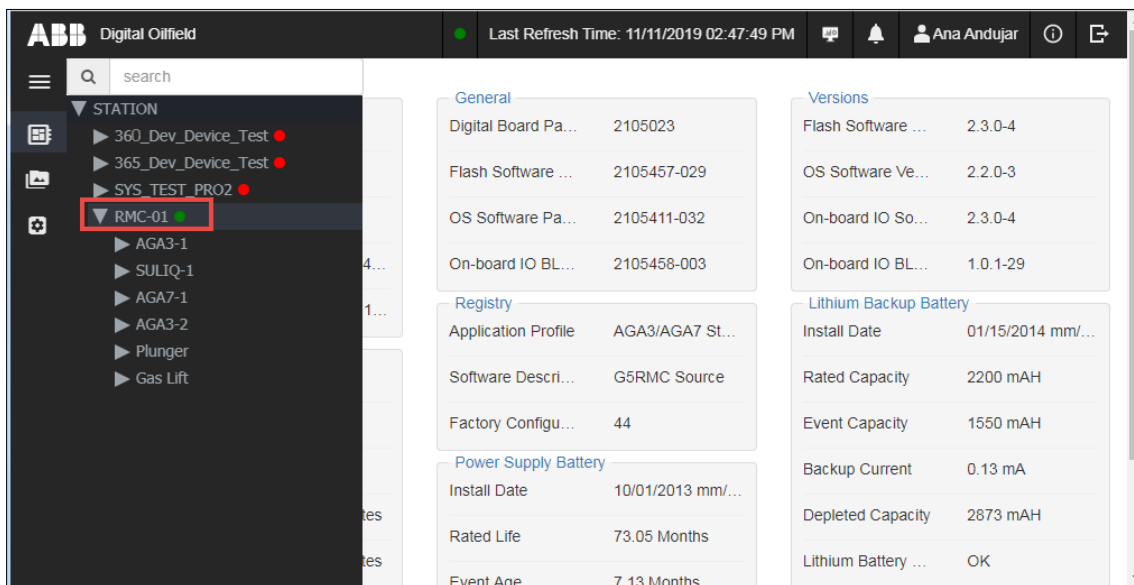
The navigation tree displays ([Figure 7-5](#)). During first-time login, the tree might show only the top node, STATION.

Figure 7-5: Device and application navigation tree view



3. Click **STATION** to display all devices.
4. Locate and click the device to display all its application instances (Figure 7-6). There may be more than one instance of the same application type. In the example shown, there are two instances of the AGA3 measurement application (two tubes).

Figure 7-6: Application instances for a device



5. View device summary on the main screen area or proceed to specific application pages as described in the next two sections.

7.3 View measurement application data

Measurement application data displays on several pages. Each application instance has:

- A main landing page that displays the most relevant measurement, calculated, and configuration data values. It provides an overview of the application instance. It can also display a graphical view of trend variables if trends are configured.
- Pages with additional application detail, configuration, alarm, trend, and event data.



IMPORTANT NOTE: Navigation to each of the application pages is the same for all measurement instances. For illustration purposes, the procedures included in this section show screens for an instance of the Gas Orifice (AGA3) measurement application. For details about specific parameters or application configurations on the device, see the PCCU help files.

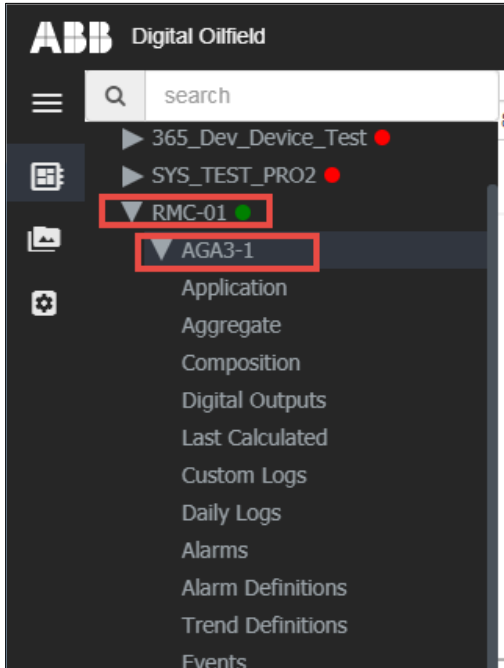


IMPORTANT NOTE: Log validation is available on Log data pages, for example in the custom and daily logs pages. A valid log is one that displays data that has not been altered since it was originally sent by the device to the cloud. A valid log is the same as the one published by the cloud interface. Validating logs provides the assurance that the log records have not been manipulated or changed on the cloud.

To view data for each application instance:

1. Navigate to the device as described in section [7.2 Navigate to devices and applications](#).
2. Locate and click the required application instance. [Figure 7-7](#) shows the first AGA3 instance selected.

Figure 7-7: Navigate to application instance pages



3. Move the mouse to the main screen area to hide the navigation tree.
4. View main application data and configuration. See examples of the main application page for instances of the AGA3 ([Figure 7-8](#)), AGA7 ([Figure 7-9](#)) and Liquid applications ([Figure 7-10](#)). The device for these examples has defined trend variables that are monitored in the graph.

Figure 7-8: Orifice meter gas measurement (AGA3) main page

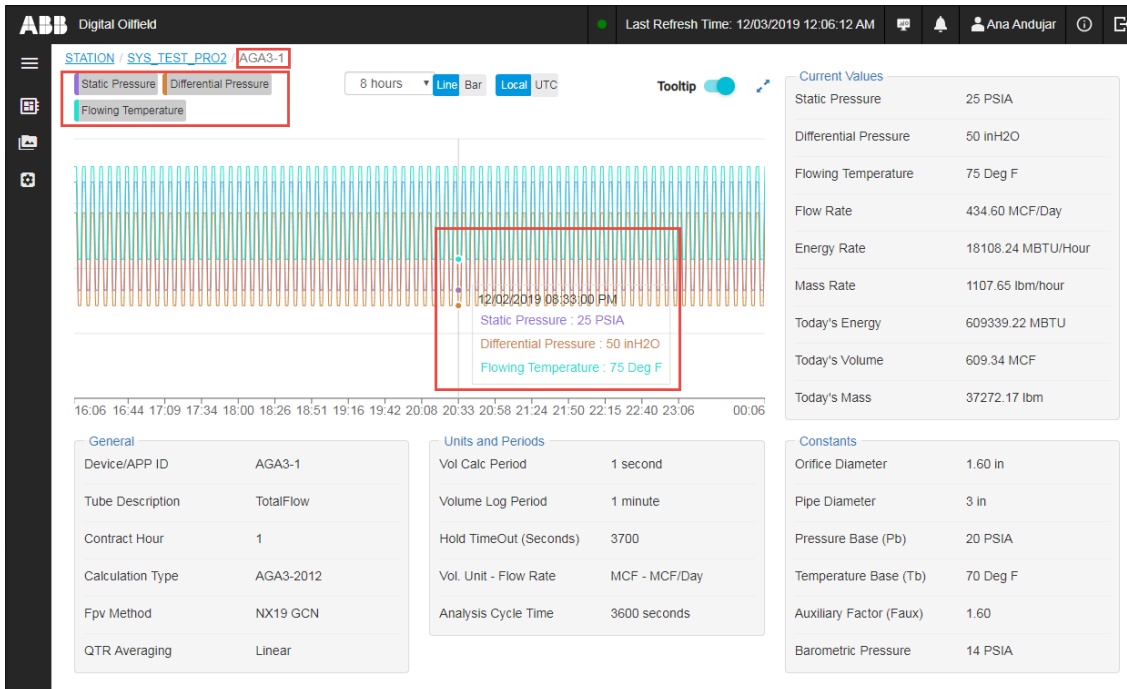


Figure 7-9: Pulse meter gas measurement (AGA7) main page

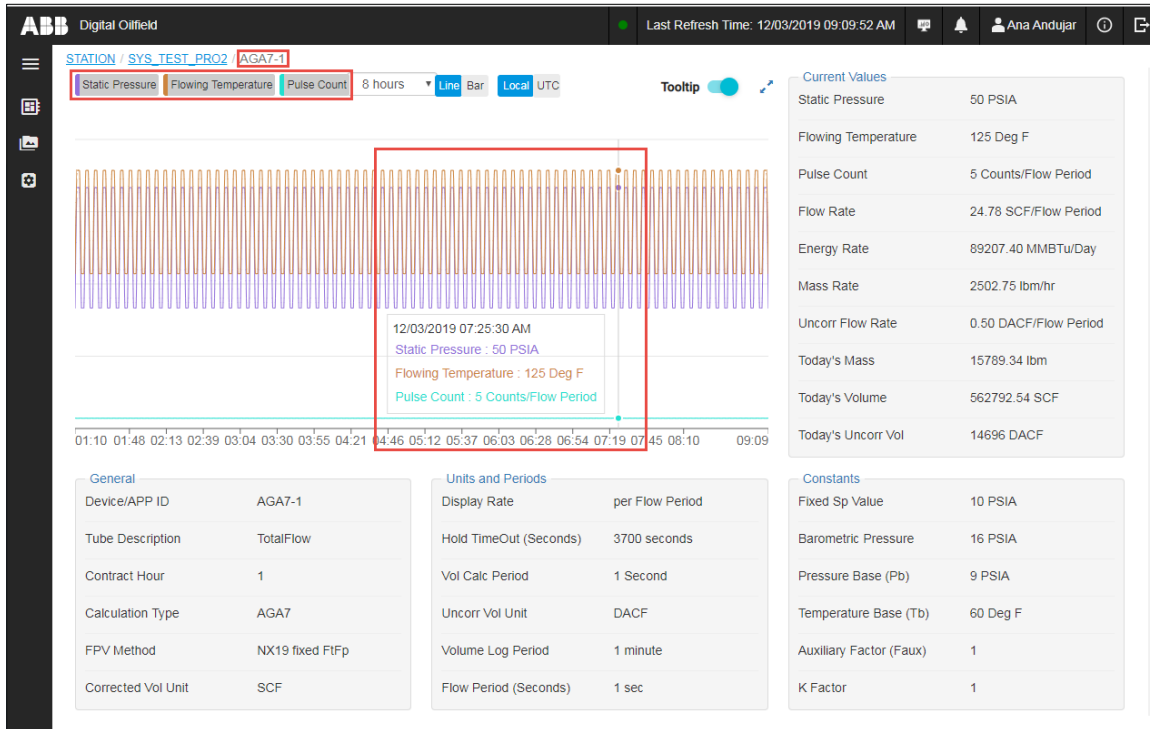
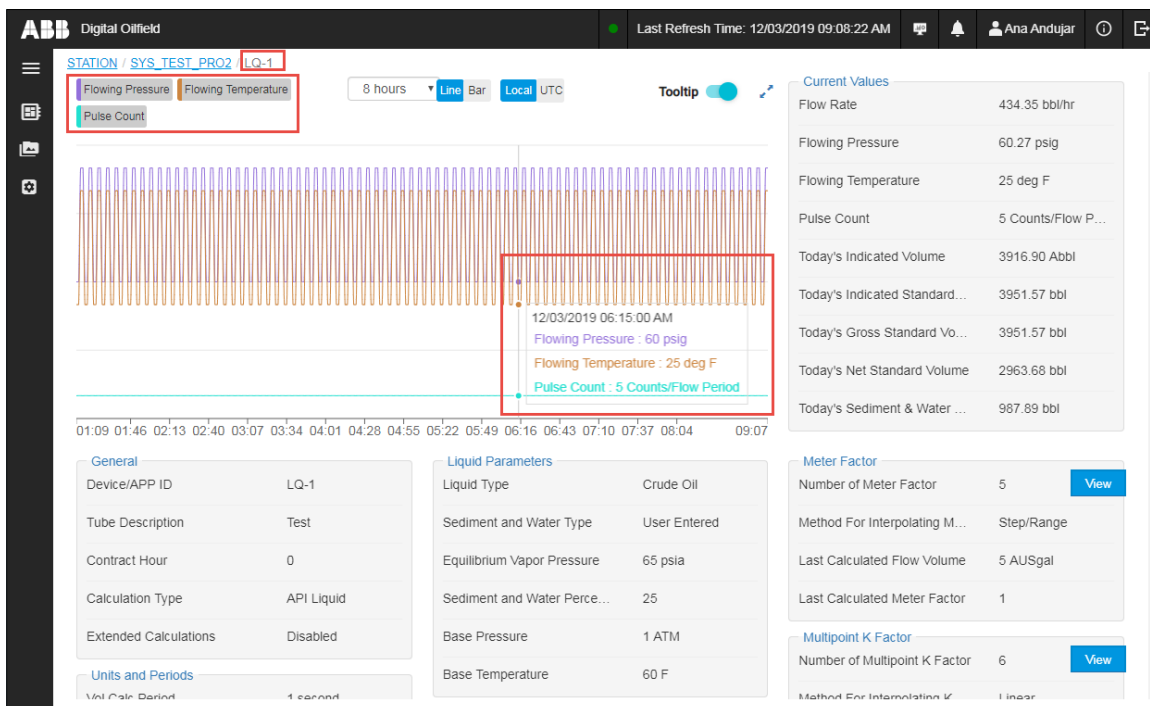
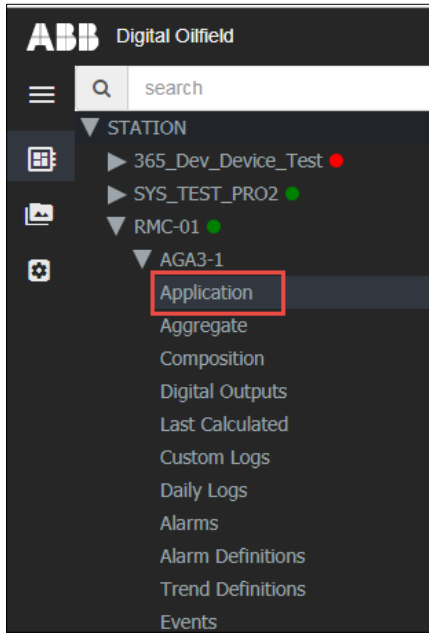


Figure 7-10: API SU Liquid main page



- To view additional data for an application instance, select the data category of interest. [Figure 7-11](#) shows the Application page selected for the AGA3-1 instance. Sections [7.3.1](#) to [7.3.11](#) show each of the pages available for measurement applications.

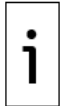
Figure 7-11: Application data categories on navigation tree



7.3.1 View application data

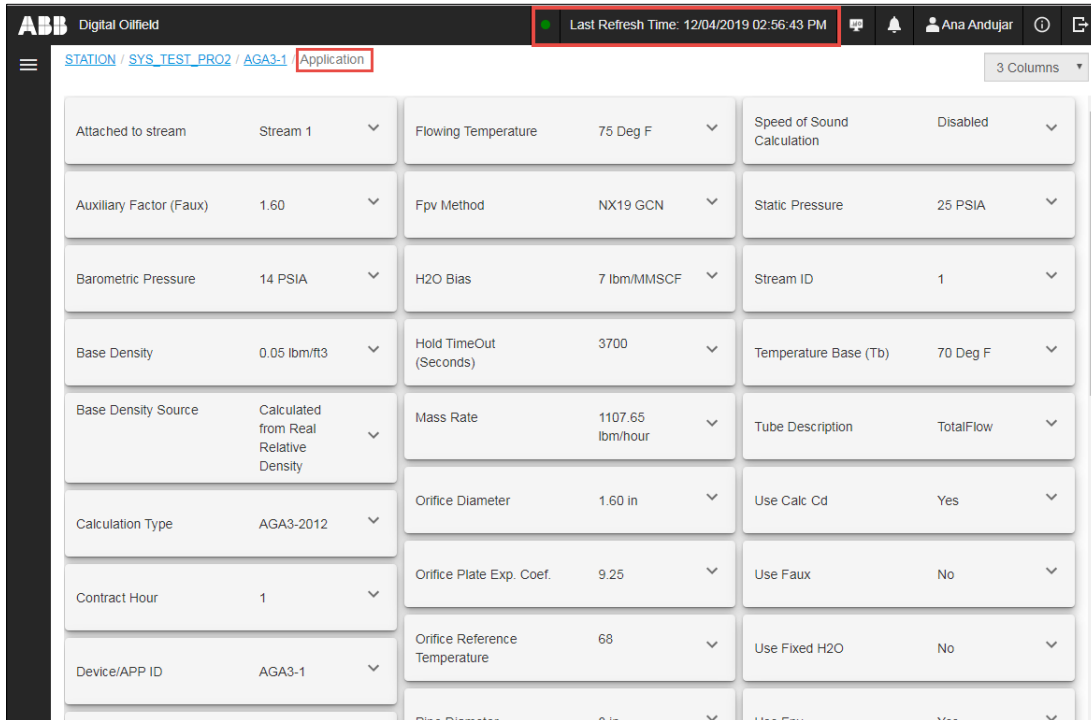
The Application page displays a list of the variables or parameters monitored from the cloud for an application instance. Each parameter in the list displays a configured, measurement or calculated value. Parameters might display additional attributes such as value range (Maximum and Minimum values, if applicable) and access type on the cloud (read-only or user-configurable).

[Figure 7-12](#) shows an example of an application page for an AGA3 instance (one tube). The page displays values as of the last refresh time indicated on top of the screen.



IMPORTANT NOTE: A green indicator next to the refresh time shows that the device is connected to the broker and able to update data at the defined publish interval. A red indicator shows that the device is disconnected and unable to update data.

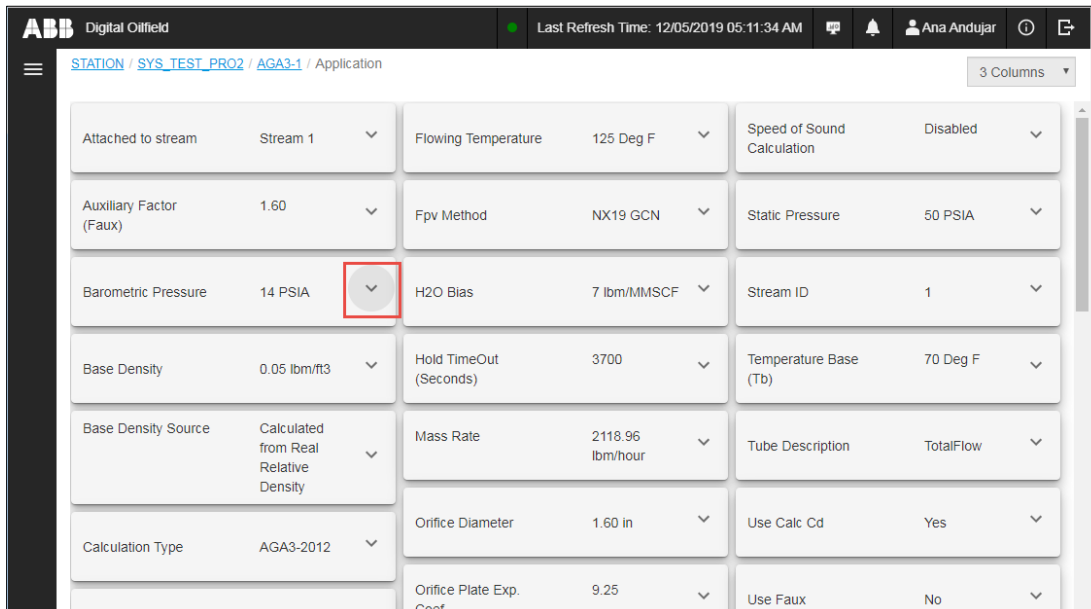
Figure 7-12: Application parameters page



To view application parameter values or details:

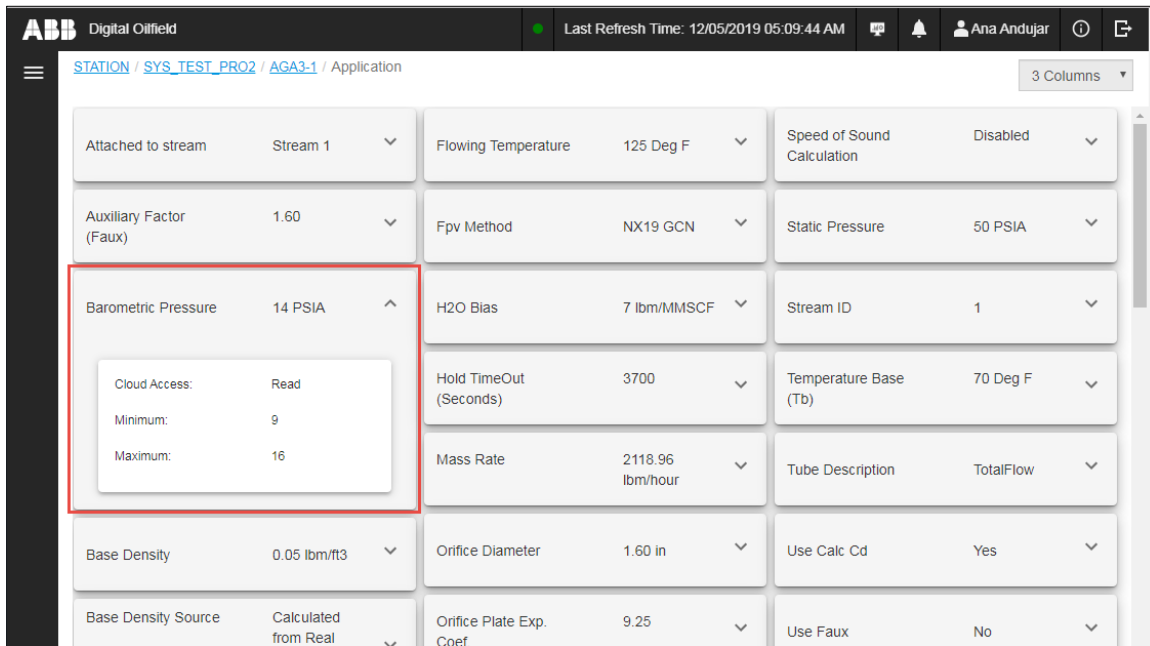
1. Locate and select the application instance on the navigation tree.
2. Select **Application**. The Application page displays.
3. Locate the parameter of interest. For long lists, use the scroll bar to search. Current parameter values display.
4. Click the arrow next to the parameter ([Figure 7-13](#)).

Figure 7-13: Expand parameter information display



5. View additional parameter information and attributes ([Figure 7-14](#)). In this example, the range of possible values for Barometric Pressure display. The current value is within that range.

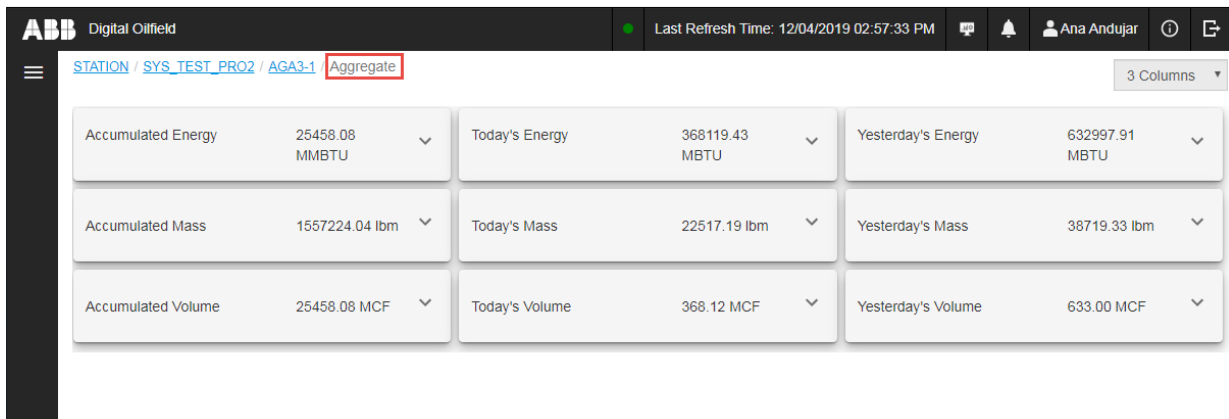
Figure 7-14: Additional parameter information and attributes



7.3.2 View aggregate data

The Aggregate page displays a list of calculated totals for energy, mass and volume values: Accumulated, Today's and Yesterday's totals ([Figure 7-15](#)).

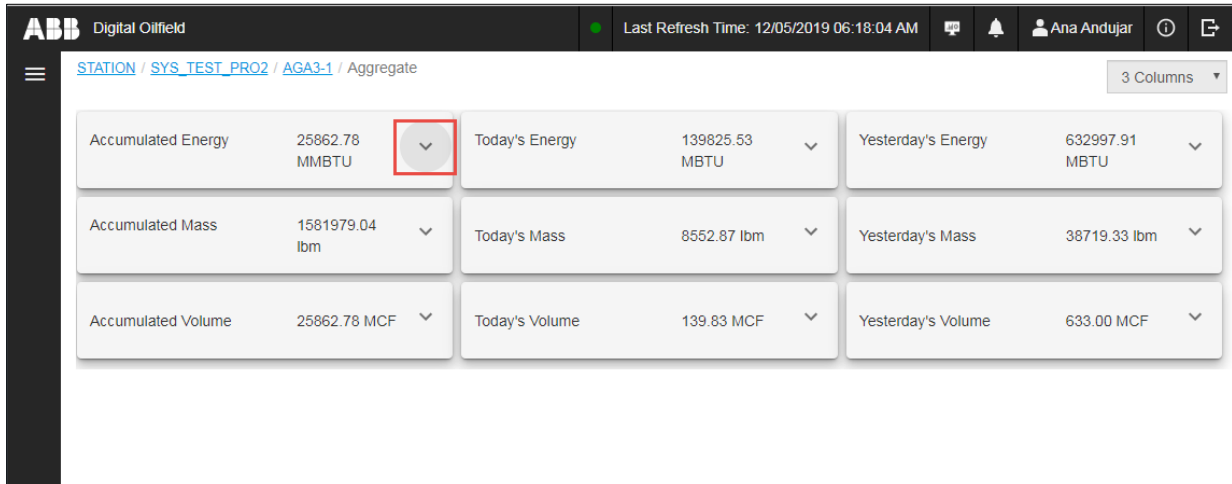
Figure 7-15: Aggregate parameters page



To view aggregate parameter values or details:

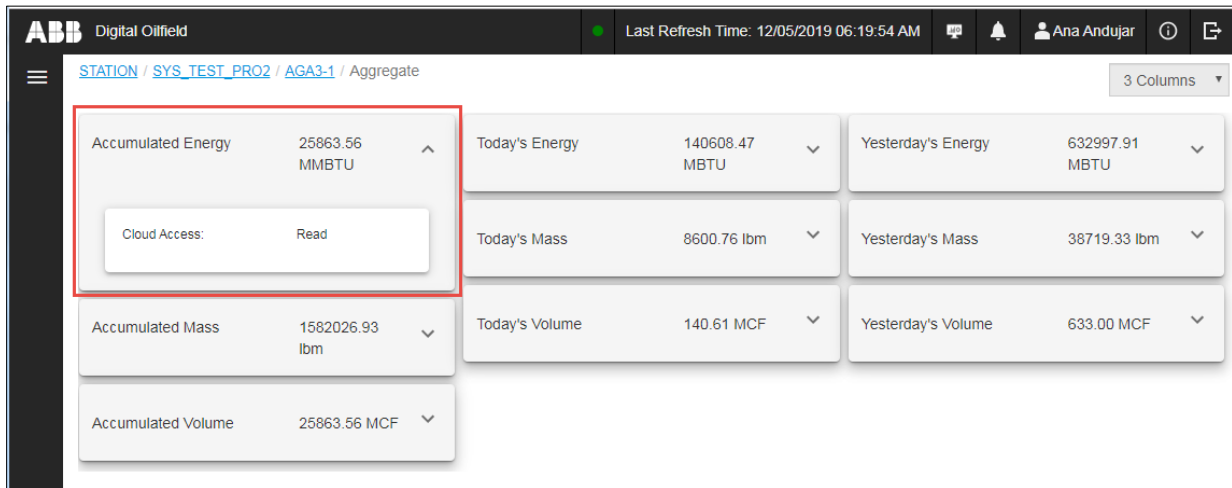
1. Locate and select the application instance on the navigation tree.
2. Select **Aggregate**. The Aggregate page displays.
3. Locate the parameter of interest. Current parameter values display.
4. Click the arrow next to the parameter ([Figure 7-16](#)).

Figure 7-16: Expand parameter information display



5. View additional parameter information and attributes (Figure 7-17). This example selects the Accumulated Energy parameter which shows as a read-only value.

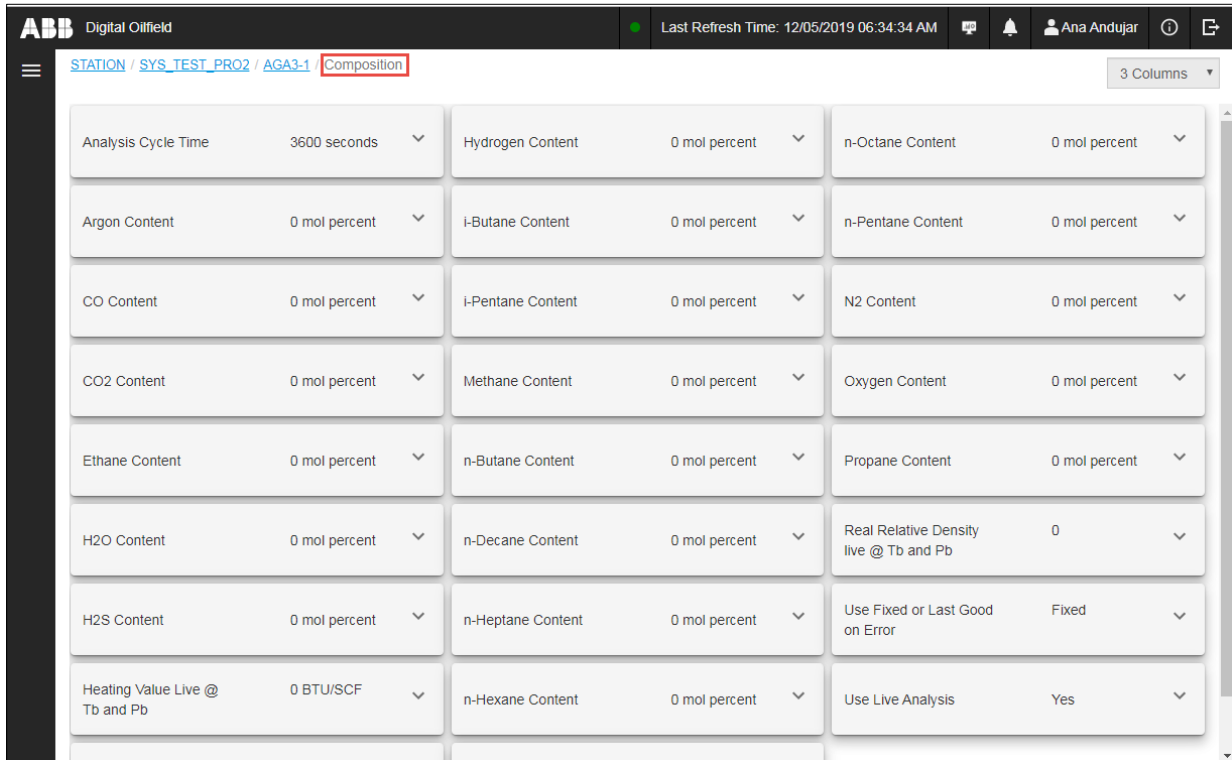
Figure 7-17: Additional parameter information and attributes



7.3.3 View composition data

The Composition page displays an alphabetical list of gas composition analysis configuration parameters and individual component values.

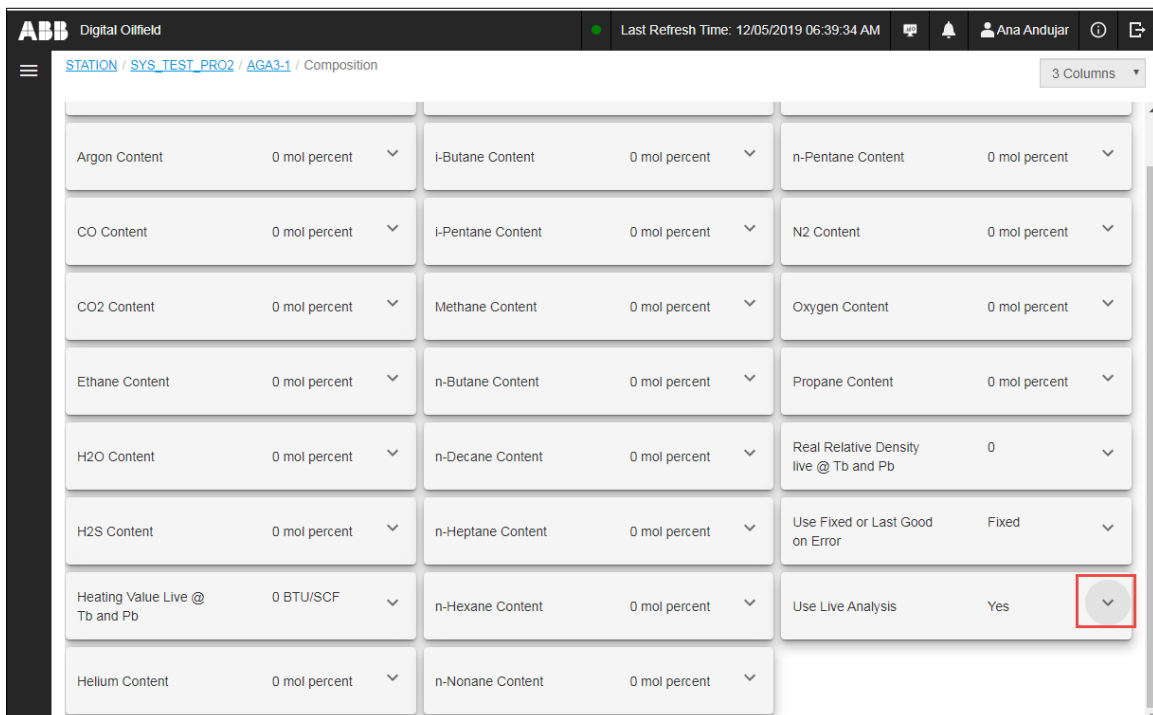
Figure 7-18: Composition parameter page



To view composition parameter values or details:

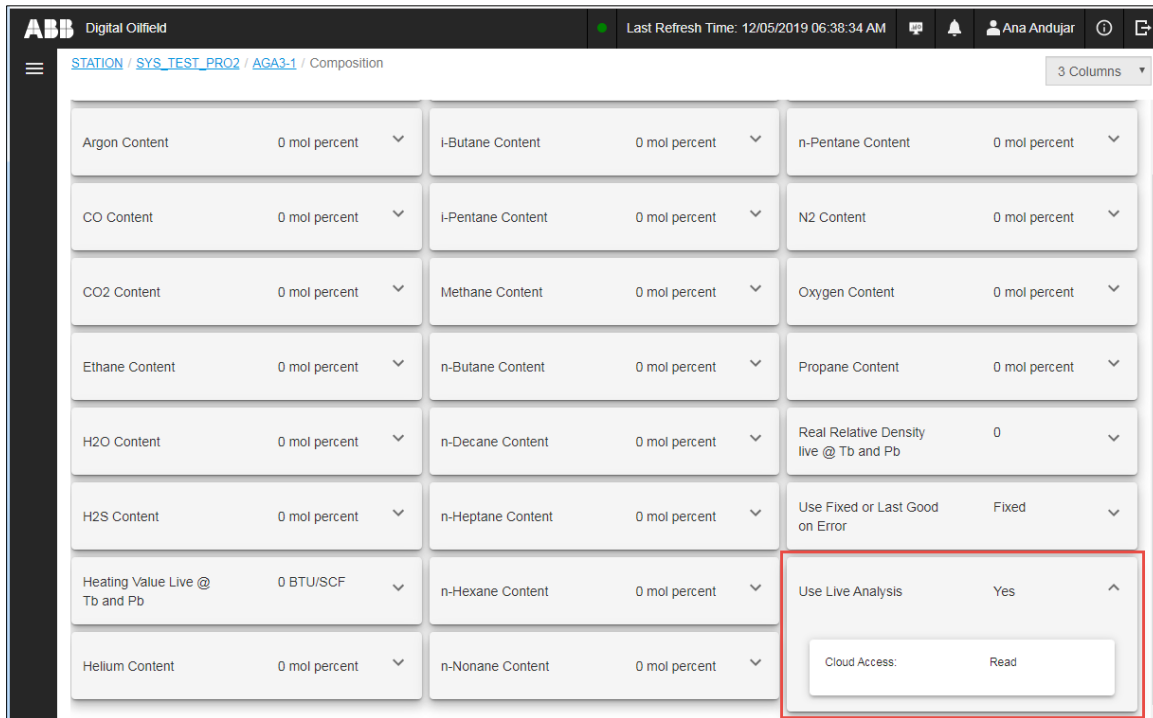
1. Locate and select the application instance on the navigation tree.
2. Select **Composition**. The Composition page displays.
3. Locate the parameter of interest. For long lists, use the scroll bar to search. Current parameter values display.
4. Click the arrow next to the parameter ([Figure 7-19](#)).

Figure 7-19: Expand parameter information display



- View additional parameter information and attributes ([Figure 7-20](#)). This example selects the "Use Live Analysis" configuration parameter. This parameter has read-only access from the cloud.

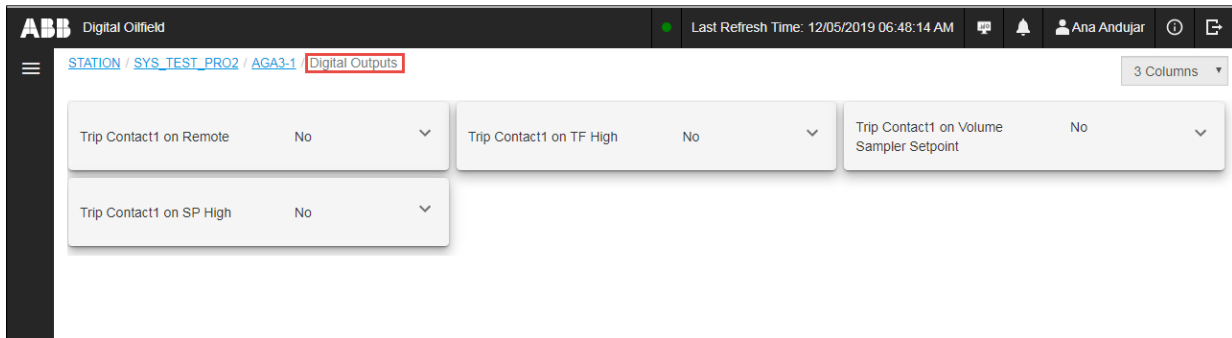
Figure 7-20: Additional parameter information and attributes



7.3.4 View digital outputs

The Digital Outputs (DO) page displays a list of digital outputs configuration parameters.

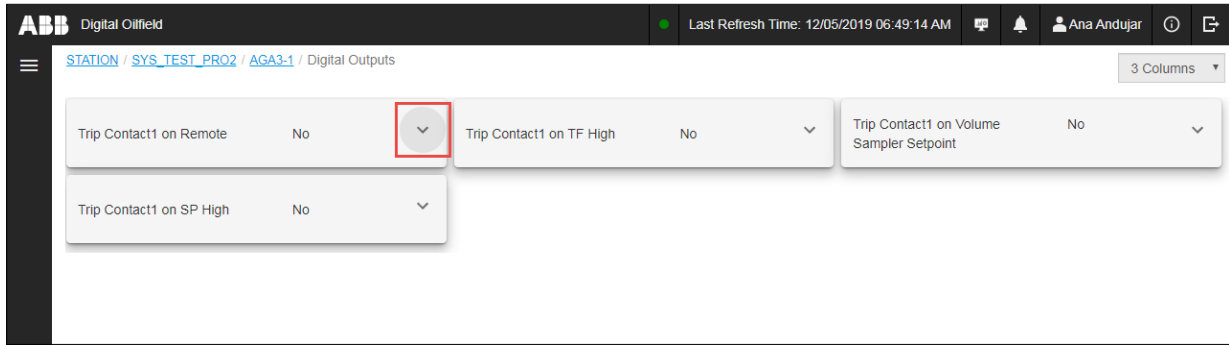
Figure 7-21: Digital outputs parameter page



To view digital outputs parameter values or details:

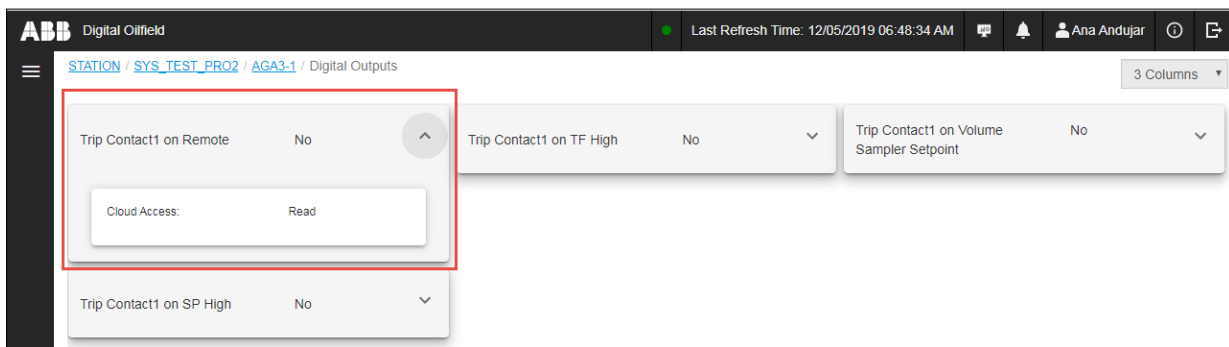
- Locate and select the application instance on the navigation tree.
- Select **Digital Outputs**. The Digital Outputs page displays.
- Locate the parameter of interest. Current parameter values display.
- Click the arrow next to the parameter ([Figure 7-22](#)).

Figure 7-22: Expand parameter information display



5. View additional parameter information and attributes ([Figure 7-23](#)). This example selects the Trip Contact1 on Remote parameter.

Figure 7-23: Additional parameter information and attributes



7.3.5 View last calculated values

The Last Calculated page displays the last calculated values of variables that are specific to volume calculations ([Figure 7-24](#)). The update frequency of these values is based on the value of the Volume Calculation Period parameter (shown in the application page).

Figure 7-24: Last calculated (values) page

Argon Content	2 mol percent	H2S Content	5 mol percent	Oxygen Content	5 mol percent
Base Compressibility	1.00	Heating Value	1000	Pipe Expansion Coefficient	6.20 in/in-F
Base Density	0.06 lbm/ft3	Helium Content	5 mol percent	Propane Content	5 mol percent
C Prime	11843.07	Hydrogen Content	3 mol percent	Qm	1107.65 lbm/Hour
C-Prime Static Factors (cp_s)	1.60	i-Butane Content	5 mol percent	Qv	18108.24 SCF/Hour
CO Content	5 mol percent	i-Pentane Content	5 mol percent	Real Relative Density	0.60
CO2 Content	5 mol percent	Live Flowing Density	0 lbm/ft3	Relative Density	0.60
Contract Barometric Pressure	14 PSIA	Mass	0.31 lbm	Specific Heat Ratio	1.30
Differential Pressure	50 inH2O	Methane Content	5 mol percent	Static Pressure	25 PSIA

To view last calculated values or details:

1. Locate and select the application instance on the navigation tree.
2. Select **Last Calculated**. The Last Calculated page displays.

3. Locate the parameter of interest. Current parameter values display.
4. Click the arrow next to the parameter ([Figure 7-25](#)).

Figure 7-25: Expand parameter information display

Parameter	Value	Unit	Parameter	Value	Unit	Parameter	Value	Unit
Argon Content	2 mol percent		H2S Content	5 mol percent		Oxygen Content	5 mol percent	
Base Compressibility	1.00		Heating Value	1000		Pipe Expansion Coefficient	6.20 in/in-F	
Base Density	0.05 lbm/ft3		Helium Content	5 mol percent		Propane Content	5 mol percent	
C Prime	11843.07		Hydrogen Content	3 mol percent		Qm	1107.65 lbm/Hour	
C-Prime Static Factors (cp_s)	1.60		i-Butane Content	5 mol percent		Qv	18108.24 SCF/Hour	
CO Content	5 mol percent		i-Pentane Content	5 mol percent		Real Relative Density	0.60	
CO2 Content	5 mol percent		Live Flowing Density	0 lbm/ft3		Relative Density	0.60	
Contract Barometric Pressure	14 PSIA		Mass	0.31 lbm		Specific Heat Ratio	1.30	
Differential Pressure	50 inH2O		Methane Content	5 mol percent		Static Pressure	25 PSIA	

5. View additional parameter information and attributes ([Figure 7-26](#)). This example selects the CO Content parameter. This read-only value also has a defined range.

Figure 7-26: Additional parameter information and attributes

Parameter	Value	Unit	Parameter	Value	Unit	Parameter	Value	Unit
C-Prime Static Factors (cp_s)	1.60		i-Butane Content	5 mol percent		Qv	34641.58 SCF/Hour	
CO Content	5 mol percent		i-Pentane Content	5 mol percent		Real Relative Density	0.60	
CO2 Content	5 mol percent		Live Flowing Density	0 lbm/ft3		Relative Density	0.60	
Contract Barometric Pressure	14 PSIA		Mass	0.59 lbm		Specific Heat Ratio	1.30	
Differential Pressure	100 inH2O		Methane Content	5 mol percent		Static Pressure	50 PSIA	
			n-Butane Content	5 mol percent		Super Compressibility	1.00	
			n-Decane Content	5 mol percent		Temperature Corrected Orifice ID	1.60 in	

Cloud Access: Read

Minimum: 0

Maximum: 100

7.3.6 View custom Logs

The Custom Logs page displays the values of application variables for the configured log period ([Figure 7-27](#)). The default log period is one hour (3600 seconds). The page displays the date and time stamp for each log. Several logs display per day. The cloud interface supports up to 5000 custom log records.

Figure 7-27: Custom Logs page

Date/Time	Date/Time (UTC)	Period Time	Sequence Number	Alarms	SP	DP	TF	Integral	Volume	Energy
12/05/2019 08:27:00 AM	12/05/2019 02:27:00 PM	60	58983	LC AN	48.33	96.67	121.67	0.05	0.56	0.56
12/05/2019 08:26:00 AM	12/05/2019 02:26:00 PM	60	58982	LC AN	26.67	53.33	78.33	0.03	0.32	0.32
12/05/2019 08:25:00 AM	12/05/2019 02:25:00 PM	60	58981	LC AN	48.33	96.67	121.67	0.05	0.56	0.56
12/05/2019 08:24:00 AM	12/05/2019 02:24:00 PM	60	58980	LC AN	26.67	53.33	78.33	0.03	0.32	0.32
12/05/2019 08:23:00 AM	12/05/2019 02:23:00 PM	60	58979	LC AN	48.33	96.67	121.67	0.05	0.56	0.56
12/05/2019 08:22:00 AM	12/05/2019 02:22:00 PM	60	58978	LC AN	26.67	53.33	78.33	0.03	0.32	0.32
12/05/2019 08:21:00 AM	12/05/2019 02:21:00 PM	60	58977	LC AN	48.33	96.67	121.67	0.05	0.56	0.56
12/05/2019 08:20:00 AM	12/05/2019 02:20:00 PM	60	58976	LC AN	26.67	53.33	78.33	0.03	0.32	0.32
12/05/2019 08:19:00 AM	12/05/2019 02:19:00 PM	60	58975	LC AN	48.33	96.67	121.67	0.05	0.56	0.56
12/05/2019 08:18:00 AM	12/05/2019 02:18:00 PM	60	58974	LC AN	26.67	53.33	78.33	0.03	0.32	0.32

To view custom logs:


1. Locate and select the application instance on the navigation tree.
2. Select **Custom Logs**. The Custom Logs page displays. The network connection and number of records affect how fast the page displays the records. The logs may take a few seconds to load. The logs are listed in chronological order. If the list is long, use the page buttons to display additional logs.
3. Scroll to the right to show all columns for the logs and to display the validate column ([Figure 7-28](#)).

Figure 7-28: Validate feature for custom logs

Date/Time (UTC)	Period Time (seconds)	Sequence Number	Alarms	SP	DP	TF	Integral	Volume	Energy	Flow Time	Validate
05/2019 03:30:00 PM	60	59046	LC AN	26.67	53.33	78.33	0.03	0.32	0.32	60	Validate
05/2019 03:29:00 PM	60	59045	LC AN	48.33	96.67	121.67	0.05	0.56	0.56	60	Validate
05/2019 03:28:00 PM	60	59044	LC AN	26.67	53.33	78.33	0.03	0.32	0.32	60	Validate
05/2019 03:27:00 PM	60	59043	LC AN	48.33	96.67	121.67	0.05	0.56	0.56	60	Validate
05/2019 03:26:00 PM	60	59042	LC AN	26.67	53.33	78.33	0.03	0.32	0.32	60	Validate
05/2019 03:25:00 PM	60	59041	LC AN	48.33	96.67	121.67	0.05	0.56	0.56	60	Validate
05/2019 03:24:00 PM	60	59040	LC AN	26.67	53.33	78.33	0.03	0.32	0.32	60	Validate
05/2019 03:23:00 PM	60	59039	LC AN	48.33	96.67	121.67	0.05	0.56	0.56	60	Validate
05/2019 03:22:00 PM	60	59038	LC AN	26.67	53.33	78.33	0.03	0.32	0.32	60	Validate
05/2019 03:21:00 PM	60	59037	LC AN	48.33	96.67	121.67	0.05	0.56	0.56	60	Validate

4. Click **Validate** to determine if the log is valid. A valid log shows a green check mark ([Figure 7-29](#)). An invalid log shows a red X.

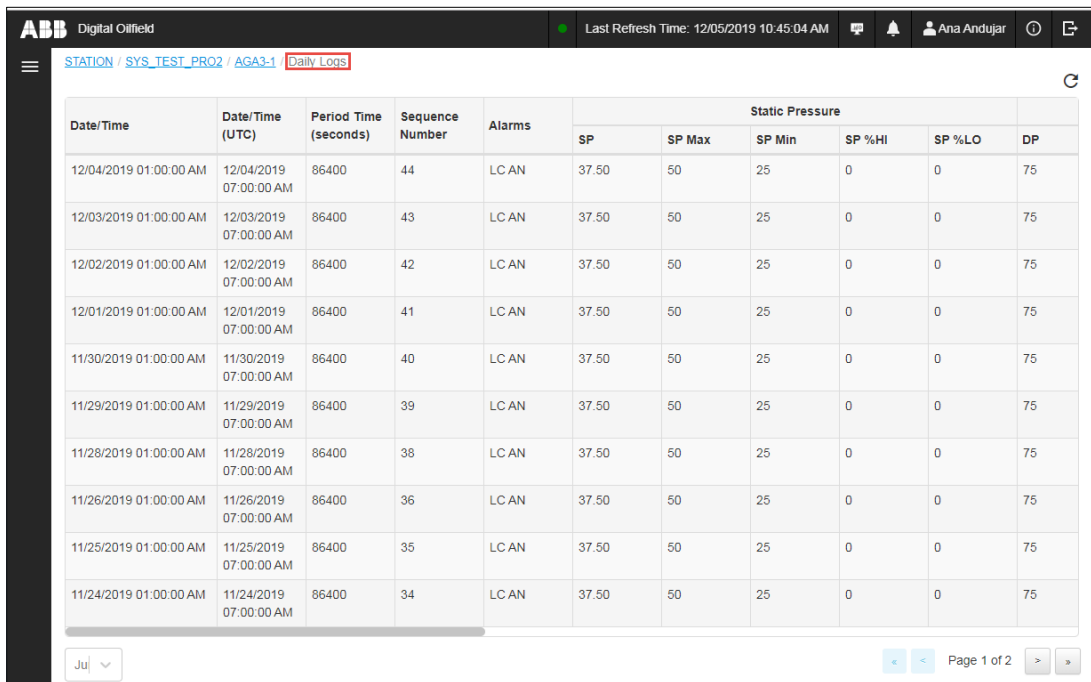
Figure 7-29: Validated log

Volume	Energy	Flow Time	Validate
0	0	0	
0	0	0	Validate

7.3.7 View daily logs

The Daily Logs page displays the daily average value of the application variables. The page displays a log for each day ([Figure 7-30](#)).

Figure 7-30: Daily logs page



Date/Time	Date/Time (UTC)	Period Time (seconds)	Sequence Number	Alarms	Static Pressure					
					SP	SP Max	SP Min	SP %HI	SP %LO	DP
12/04/2019 01:00:00 AM	12/04/2019 07:00:00 AM	86400	44	LC AN	37.50	50	25	0	0	75
12/03/2019 01:00:00 AM	12/03/2019 07:00:00 AM	86400	43	LC AN	37.50	50	25	0	0	75
12/02/2019 01:00:00 AM	12/02/2019 07:00:00 AM	86400	42	LC AN	37.50	50	25	0	0	75
12/01/2019 01:00:00 AM	12/01/2019 07:00:00 AM	86400	41	LC AN	37.50	50	25	0	0	75
11/30/2019 01:00:00 AM	11/30/2019 07:00:00 AM	86400	40	LC AN	37.50	50	25	0	0	75
11/29/2019 01:00:00 AM	11/29/2019 07:00:00 AM	86400	39	LC AN	37.50	50	25	0	0	75
11/28/2019 01:00:00 AM	11/28/2019 07:00:00 AM	86400	38	LC AN	37.50	50	25	0	0	75
11/26/2019 01:00:00 AM	11/26/2019 07:00:00 AM	86400	36	LC AN	37.50	50	25	0	0	75
11/25/2019 01:00:00 AM	11/25/2019 07:00:00 AM	86400	35	LC AN	37.50	50	25	0	0	75
11/24/2019 01:00:00 AM	11/24/2019 07:00:00 AM	86400	34	LC AN	37.50	50	25	0	0	75

To view daily logs:


1. Locate and select the application instance on the navigation tree.
2. Select **Daily Logs**. The Daily Logs page displays. The logs are listed in chronological order. If the list is long, use the page buttons to display additional logs.
3. Scroll to the right to show all columns for the logs and to display the validate column ([Figure 7-31](#)).

Figure 7-31: Validate feature for daily logs

The screenshot shows the ABB Digital Oilfield interface. At the top, it displays 'Last Refresh Time: 12/05/2019 10:45:04 AM' and the user 'Ana Andujar'. The main content area is titled 'STATION / SYS_TEST_PRO2 / AGA3-1 / Daily Logs'. Below this is a table with columns: Temperature (sub-columns: TF Max, TF Min, TF %HI, TF %LO), Integral, Volume, Energy, Flow Time, Back Flow, Contract Hr, and Validate. The 'Validate' column contains a 'Validate' button for each row. The first 'Validate' button is highlighted with a red box. The table contains 10 rows of data with identical values: TF Max: 125, TF Min: 75, TF %HI: 0, TF %LO: 0, Integral: 53.44, Volume: 633.00, Energy: 633.00, Flow Time: 86400, Back Flow: 0, Contract Hr: 1.

4. Click **Validate** to determine if the log is valid. A valid log shows a green check mark (Figure 7-32). An invalid log shows a red X.

Figure 7-32: Validated log

Flow Time	Back Flow	Contract Hr	Validate
86400	0	1	
86400	0	1	Validate

7.3.8 View alarms

The Alarms page displays logged alarms and their date/time stamps (Figure 7-33). The alarms displayed can be user-defined or system alarms. For details on user-defined alarms see [7.3.9 View alarm definitions](#).



IMPORTANT NOTE: Alarm definitions are created in PCCU. The cloud user interface reflects these definitions automatically. The cloud user interface does not support alarm definition.

To view alarms:

1. Locate and select the application instance on the navigation tree.
2. Select **Alarms**. The Alarms page displays. The alarms display in chronological order. If the list is long, use the navigation buttons to display additional alarms.

Figure 7-33: Alarms page

Date/Time	Date/Time (UTC)	Name	Value	Sequence Number	State	Severity
12/05/2019 11:05:05 AM	12/05/2019 05:05:05 PM	AGA3-1 DP	100 inH2O	177403	Active	Normal
12/05/2019 11:03:05 AM	12/05/2019 05:03:05 PM	AGA3-1 DP	100 inH2O	177397	Active	Normal
12/05/2019 11:01:05 AM	12/05/2019 05:01:05 PM	AGA3-1 DP	100 inH2O	177391	Active	Normal
12/05/2019 10:59:05 AM	12/05/2019 04:59:05 PM	AGA3-1 DP	100 inH2O	177385	Active	Normal
12/05/2019 10:57:05 AM	12/05/2019 04:57:05 PM	AGA3-1 DP	100 inH2O	177379	Active	Normal
12/05/2019 10:55:05 AM	12/05/2019 04:55:05 PM	AGA3-1 DP	100 inH2O	177373	Active	Normal
12/05/2019 10:53:05 AM	12/05/2019 04:53:05 PM	AGA3-1 DP	100 inH2O	177367	Active	Normal
12/05/2019 10:51:05 AM	12/05/2019 04:51:05 PM	AGA3-1 DP	100 inH2O	177361	Active	Normal
12/05/2019 10:49:05 AM	12/05/2019 04:49:05 PM	AGA3-1 DP	100 inH2O	177355	Active	Normal
12/05/2019 10:47:05 AM	12/05/2019 04:47:05 PM	AGA3-1 DP	100 inH2O	177349	Active	Normal

7.3.9 View alarm definitions

The Alarm Definitions page displays user-defined alarms from the Alarm System Application. These definitions are created in PCCU and the cloud user interface displays them automatically.

To view the Alarm Definitions page:

1. Locate and select the application instance on the navigation tree.
2. Select **Alarm Definitions**. The Alarm Definitions page displays (Figure 7-34).

Figure 7-34: Alarm Definitions page

Description	Input Variable	Condition	Threshold Value	Severity	Suppress	Filter Threshold	Alarm Type
AGA3-1 DP	differentialPressure	GT	80	Normal	Disabled	0 (sec)	Active

3. Review alarm definitions. If the list is long, use page navigation buttons to locate and display additional definitions.

7.3.10 View trend definitions

The Trend Definitions page displays the user-selected application variables that the device scans and logs at specified time intervals. The graph on the main application instance page reflects some of these variables. Trends are defined on the Trend System application in PCCU.



IMPORTANT NOTE: Totalflow devices support the definition of multiple trend files with different variable sets. These files are named and saved separately in the device. The cloud application merges all variable sets from these different trend files and consolidates the display. The Trend definition page displays as many variables as defined in the device trend files. The graph on the main application instance page limits concurrent variable display to 5 variables.

To view Trend Definitions:

1. Locate and select the application instance on the navigation tree.
2. Select **Trend Definitions**. The Trend Definitions page displays. The example in Figure 7-35 shows a simple trend definition with three variables. Figure 7-36 shows the events page of a device without defined trends.

Figure 7-35: Trend Definitions page

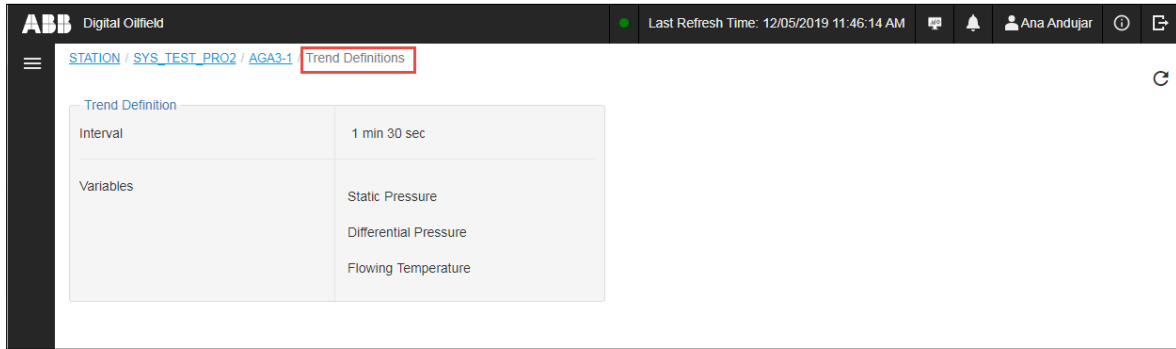
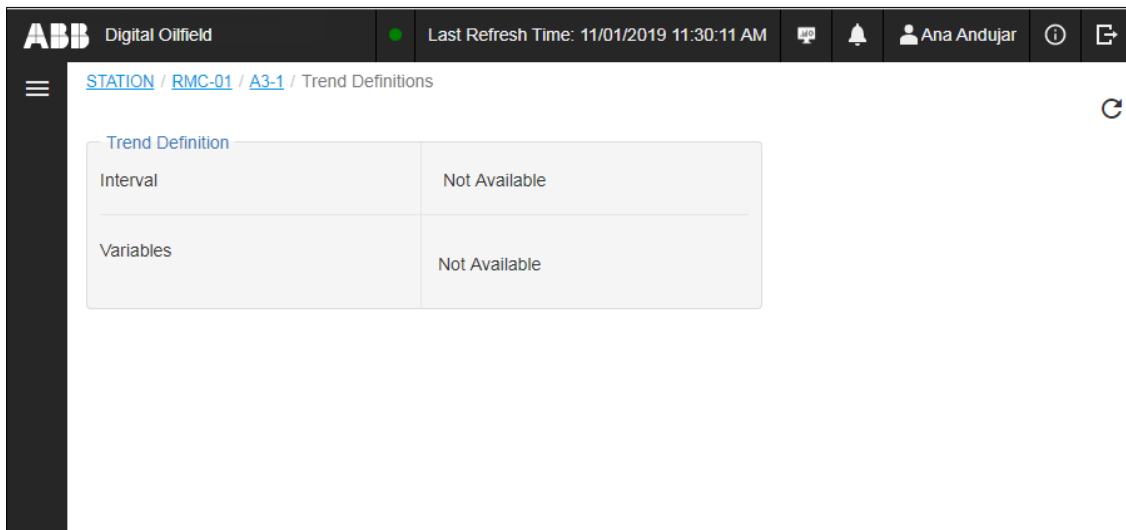


Figure 7-36: No trend definitions



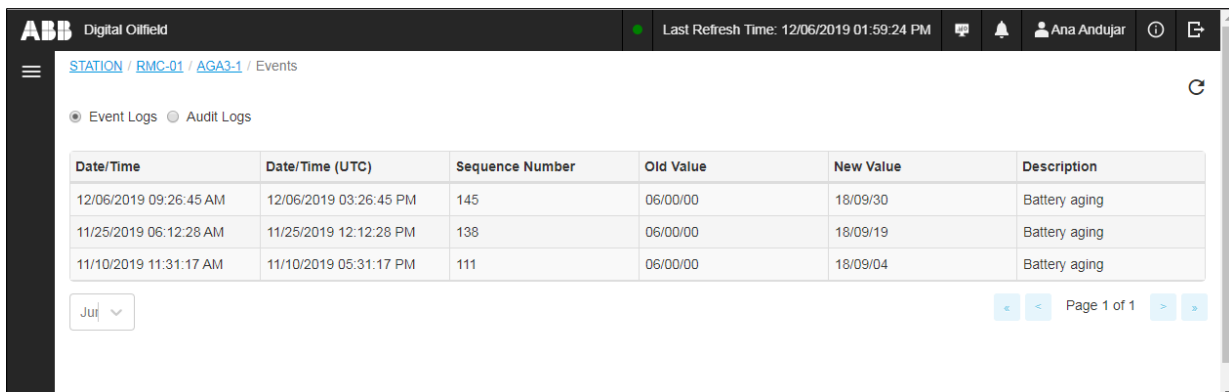
7.3.11 View events

The Events page displays system or user-triggered events. Each event log displays the date/time stamp. Events triggered by parameter value changes will display the values both prior to and after the change. It is important to monitor parameter value changes as they might affect calculation values.

To view events:

1. Locate and select the application instance on the navigation tree.
2. Select **Events**. The Events page displays.

Figure 7-37: Events page



3. View events. If the list is long, use the page navigation buttons to view additional events.

7.4 View control application data

Control application pages provide control function and views of relevant data. Control functions allow some basic operation of the control systems from the cloud. Each control application instance has:

- A main landing page that displays the most relevant control information
- Pages with additional control states, configuration, alarm, trend, and event data

7.4.1 Plunger Control application

[Table 7-1](#) shows the Plunger Control application pages. These pages display the different states of the plunger in addition to alarms and trend data. Navigate to the state-specific page for detailed information. The relevant page will depend on the current main-valve-state and plunger-status value.

The Plunger Control application supports control functions which allow operators to change certain parameters and control the plunger's behavior. The ability to use those functions or modify parameters depends on the user's access permissions.

Table 7-1: Plunger Control application page list

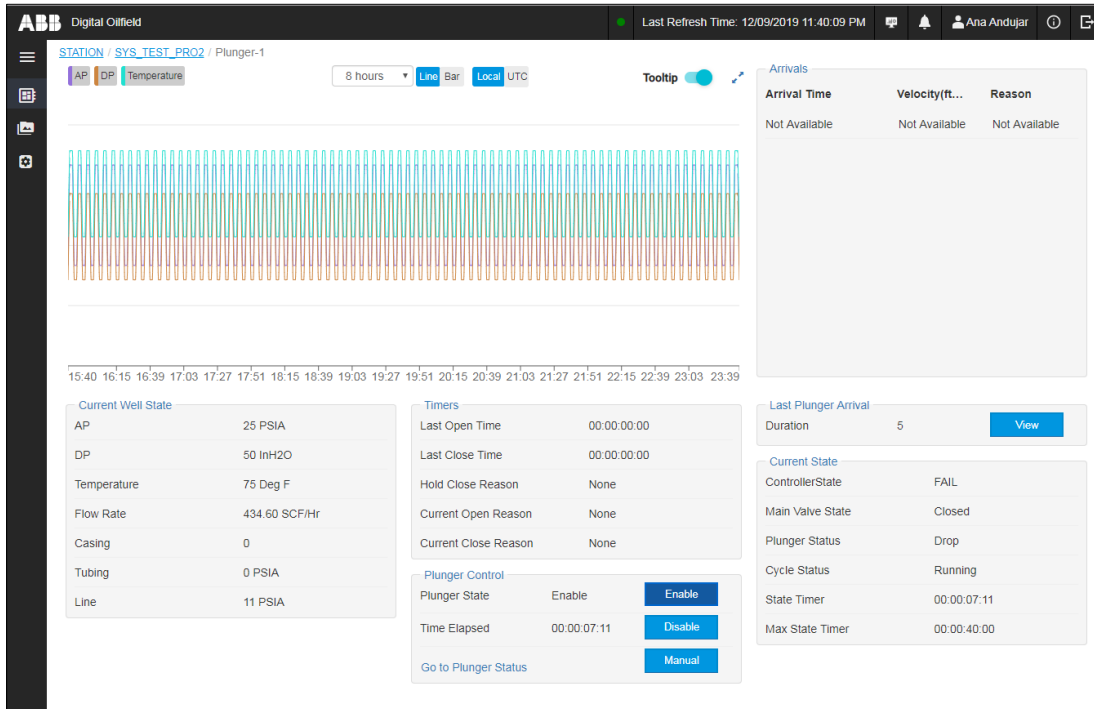
Application Pages	Description
Plunger State	Contains most of the relevant variables for the Plunger
Plunger Valve Closed	Contains the parameters specific to plunger state Plunger Valve Closed
Plunger Arrived	Contains the parameters specific to plunger state Plunger Arrived
Plunger Afterflow	Contains the parameters specific to plunger state Plunger Afterflow
Plunger Arriving	Contains the parameters specific to plunger state Plunger Arriving
Plunger Closing Valve	Contains the parameters specific to plunger state Plunger Closing Valve
Plunger Control	Contains parameters to control the well and plunger attributes, including Well Geometry, control, tuning and swabbing options
Plunger Afterflow Sub	Shows all optional parameters, which can be used to close the valve once the plunger is in Afterflow state
Plunger Valve Closed Sub	Shows all optional parameters, which can be used to open the valve
Alarms	Displays logged alarms and their date/time stamps. The alarms displayed can be user-defined or system alarms.
Alarm Definitions	Displays user-defined alarms in the Alarm System Application
Trend Definitions	Displays the user-selected application variables that the device scans and logs at specified time intervals. Trends are defined on the Trend System application.
Plunger Cycles	Contains historical data for past 30 plunger cycles, including start and end timestamp for a particular cycle

7.4.1.1 View main page

To view a plunger application instance landing page:

1. Locate and select the plunger instance on the navigation tree.
2. Move the mouse to hide the navigation tree and view the application summary ([Figure 7-38](#)).

Figure 7-38: Plunger control application landing page

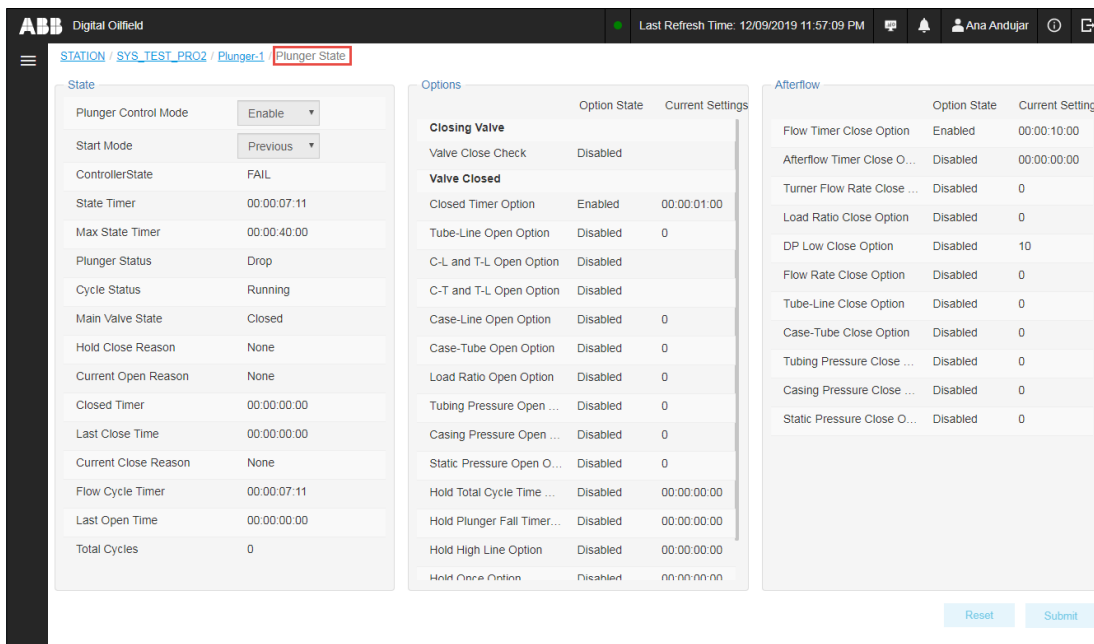


7.4.1.2 View the Plunger state page

To view the plunger state page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger State**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-39: Plunger State page



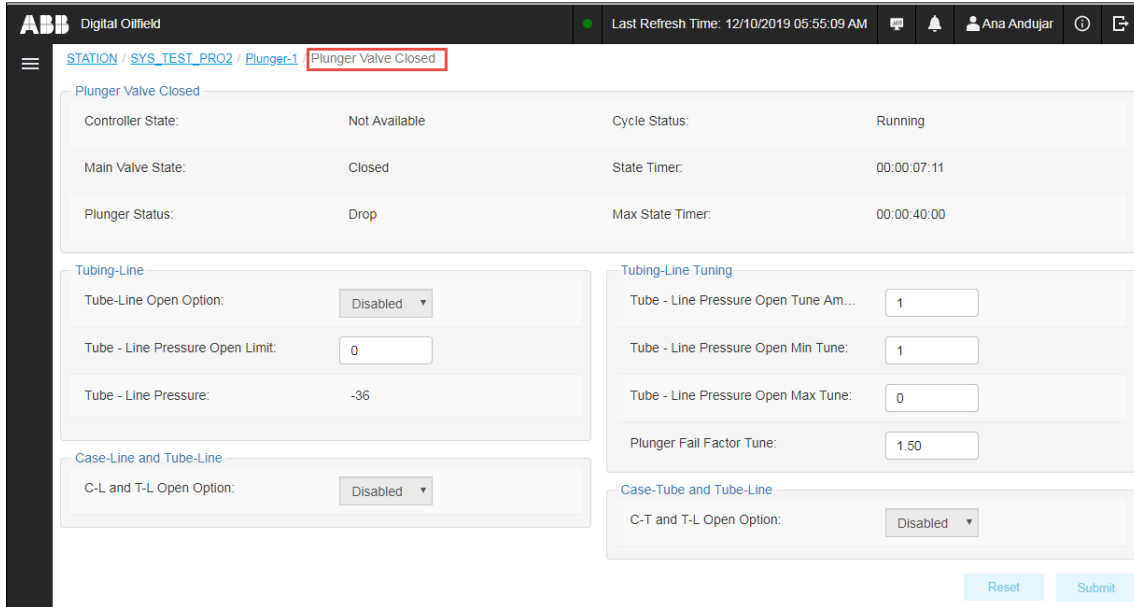
7.4.1.3 View the Plunger Valve Closed page

To view the Plunger Valve Closed page:

1. Locate and select the plunger instance on the navigation tree.

2. Select **Plunger Valve Closed**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-40: Plunger Valve Closed page

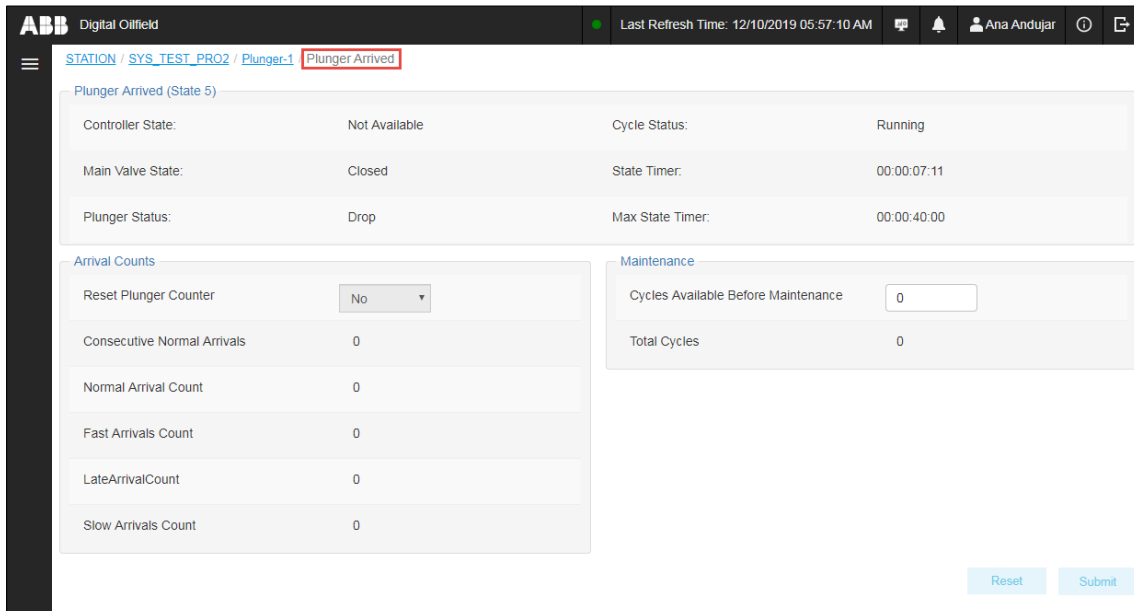


7.4.1.4 View the Plunger Arrived page

To view the Plunger Arrived page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Arrived**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-41: Plunger Arrived page



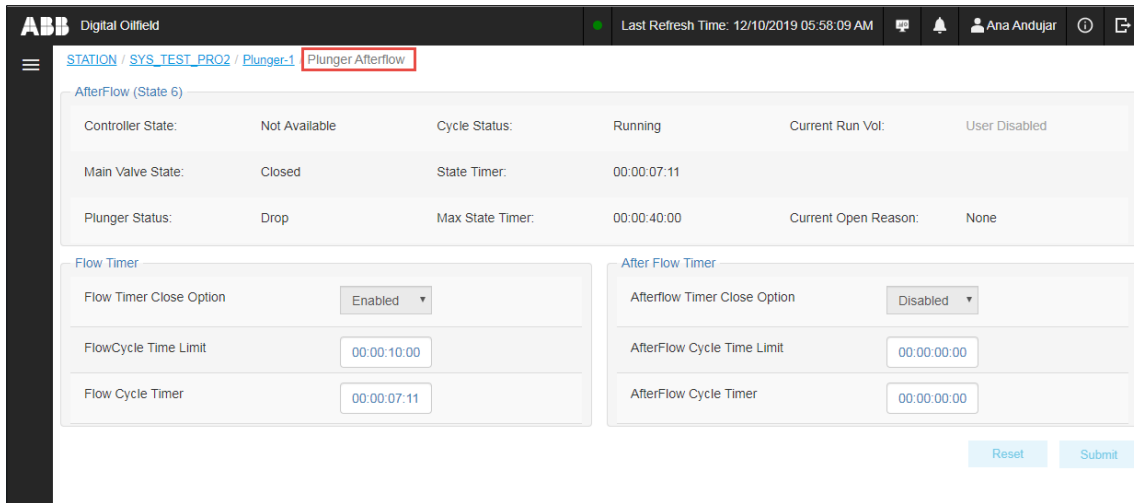
7.4.1.5 View the Plunger Afterflow page

To view the Plunger Afterflow page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Afterflow**.

3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-42: Plunger Afterflow page

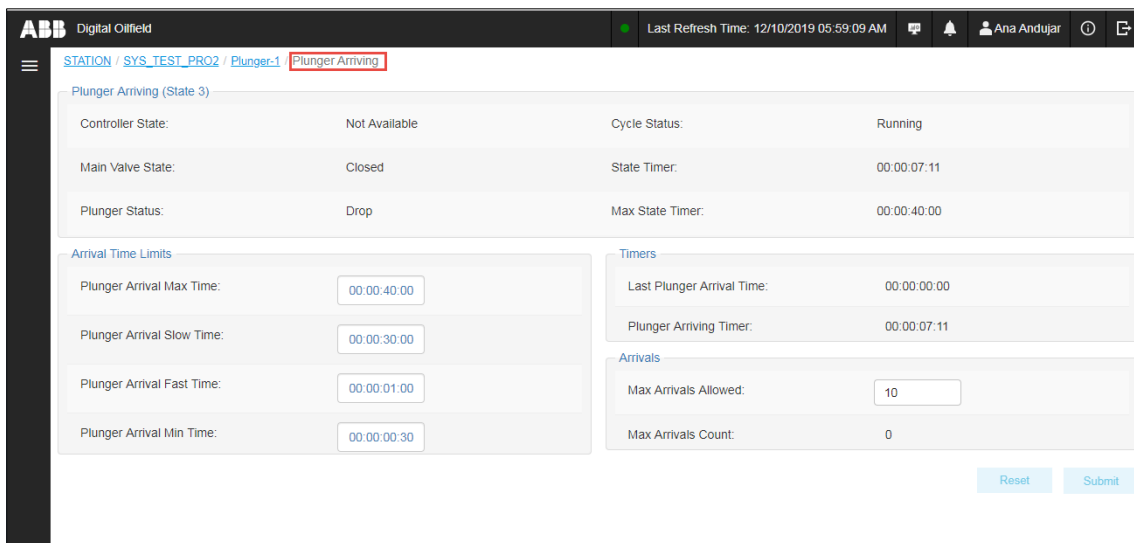


7.4.1.6 View the Plunger Arriving page

To view the Plunger Arriving page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Arriving**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-43: Plunger Arriving page

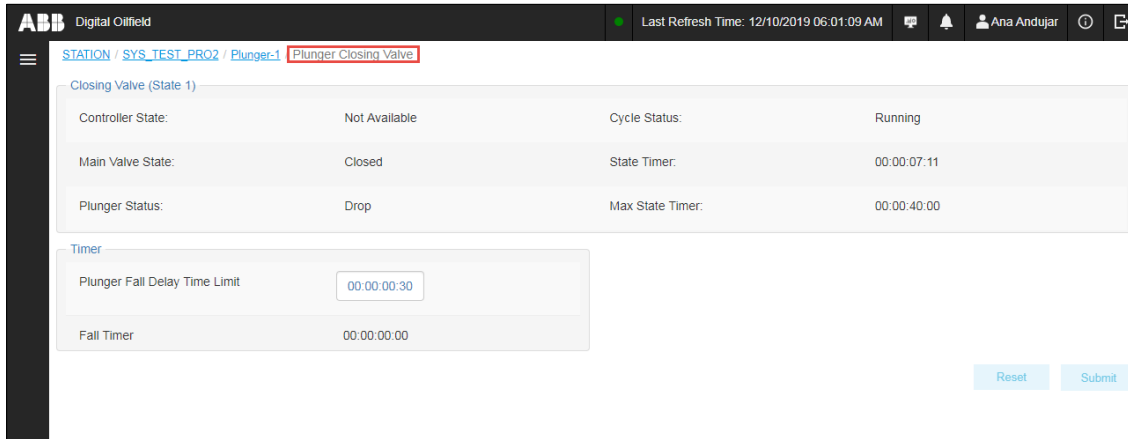


7.4.1.7 View the Plunger Closing Valve page

To view the Plunger Closing Valve page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Closing Valve**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-44: Plunger Closing Valve page

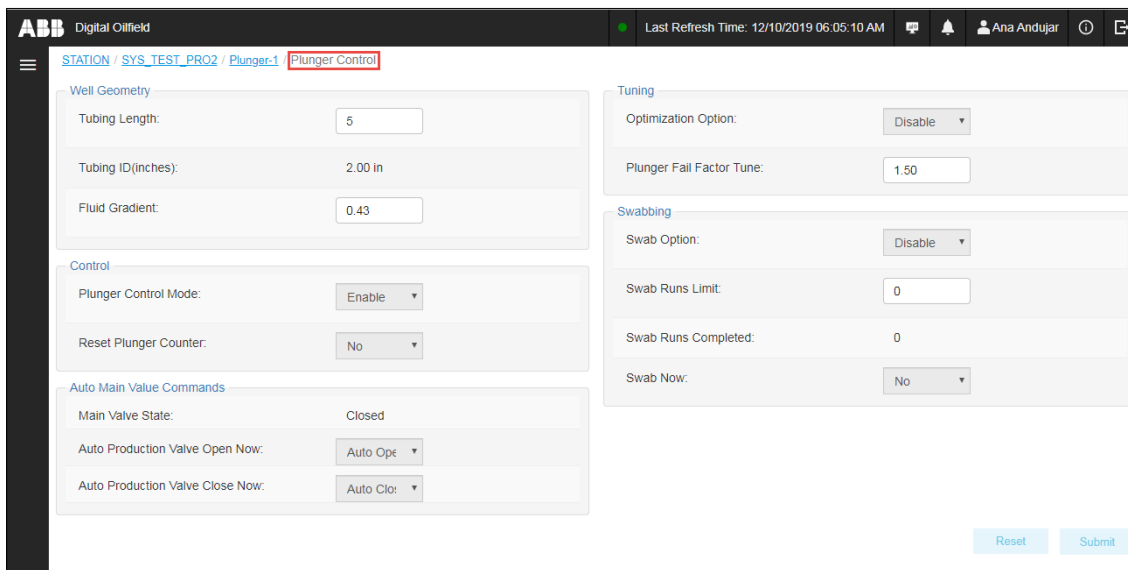


7.4.1.8 View the Plunger Control page

To view the Plunger Control page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Control**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-45: Plunger Control page

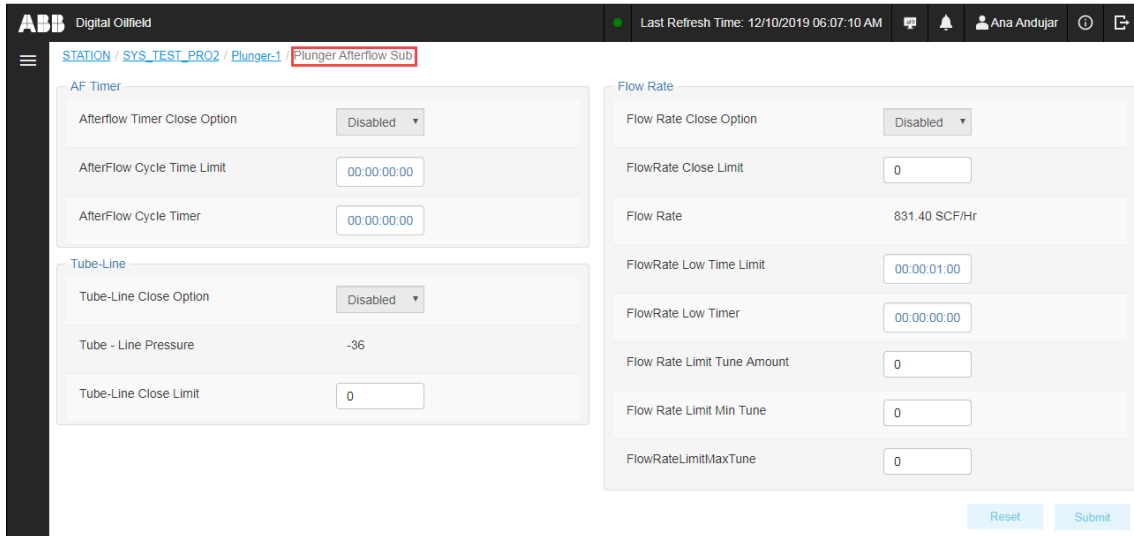


7.4.1.9 View the Plunger Afterflow Sub page

To view the Plunger Afterflow Sub page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Afterflow Sub**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-46: Plunger Afterflow Sub page

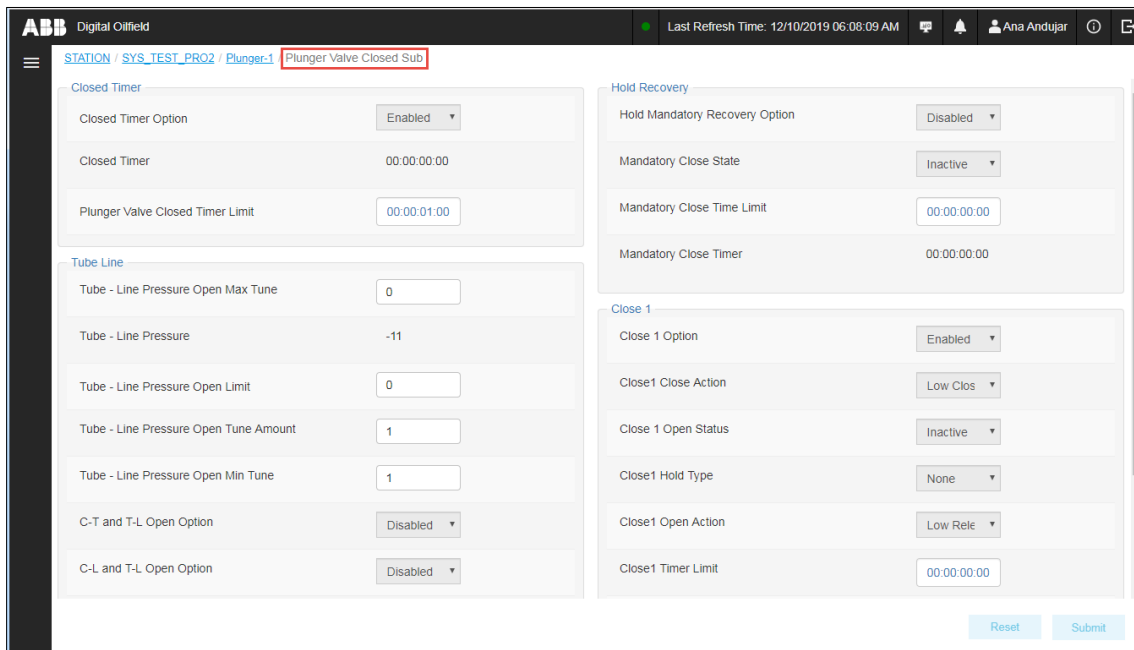


7.4.1.10 View the Plunger Valve Closed Sub page

To view the Plunger Valve Closed Sub page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Valve Closed Sub**.
3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-47: Plunger Valve Closed Sub page

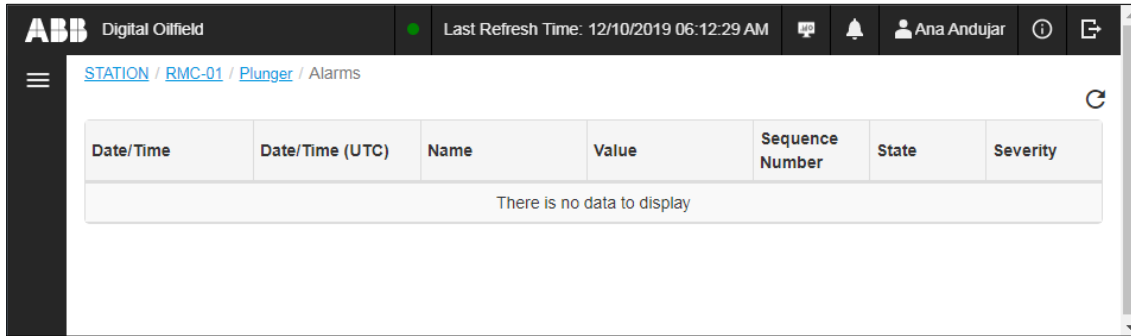


7.4.1.11 View Alarms

To view alarms:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Alarms**.
3. Move the mouse to the main screen area to hide the navigation tree and view the logged alarms.

Figure 7-48: Alarms

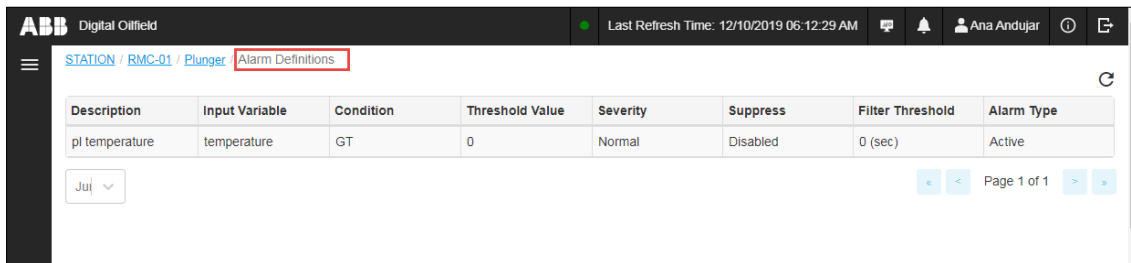


7.4.1.12 View Alarm Definitions

To view alarm definitions:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Alarm Definitions**.
3. Move the mouse to the main screen area to hide the navigation tree and view alarm definitions.

Figure 7-49: Alarm Definitions

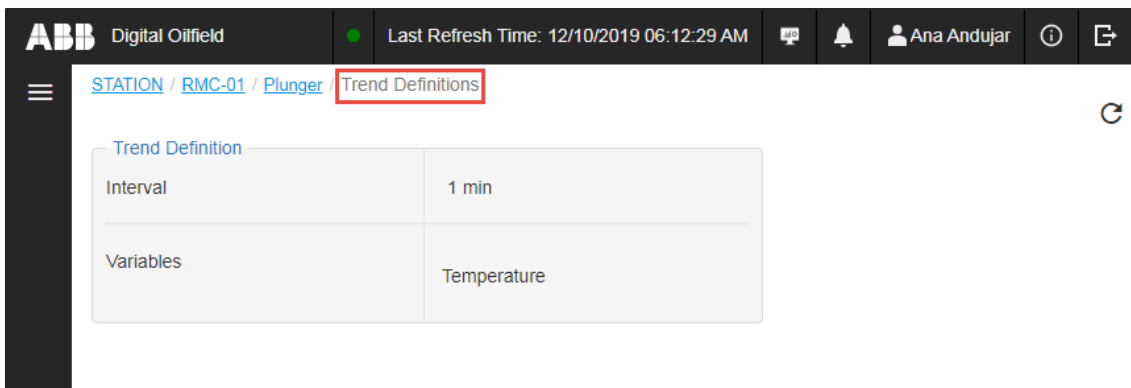


7.4.1.13 View Trend Definitions

To view Trend Definitions:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Trend Definitions**.
3. Move the mouse to the main screen area to hide the navigation tree and view the trend definitions. For simplicity, [Figure 7-50](#) shows a single variable, Temperature. Plunger application have more variables to trend. If planning to run plunger analyses on a well, ensure the required trends are defined. See section [7.5.7 View well configuration](#).

Figure 7-50: Trend Definitions page



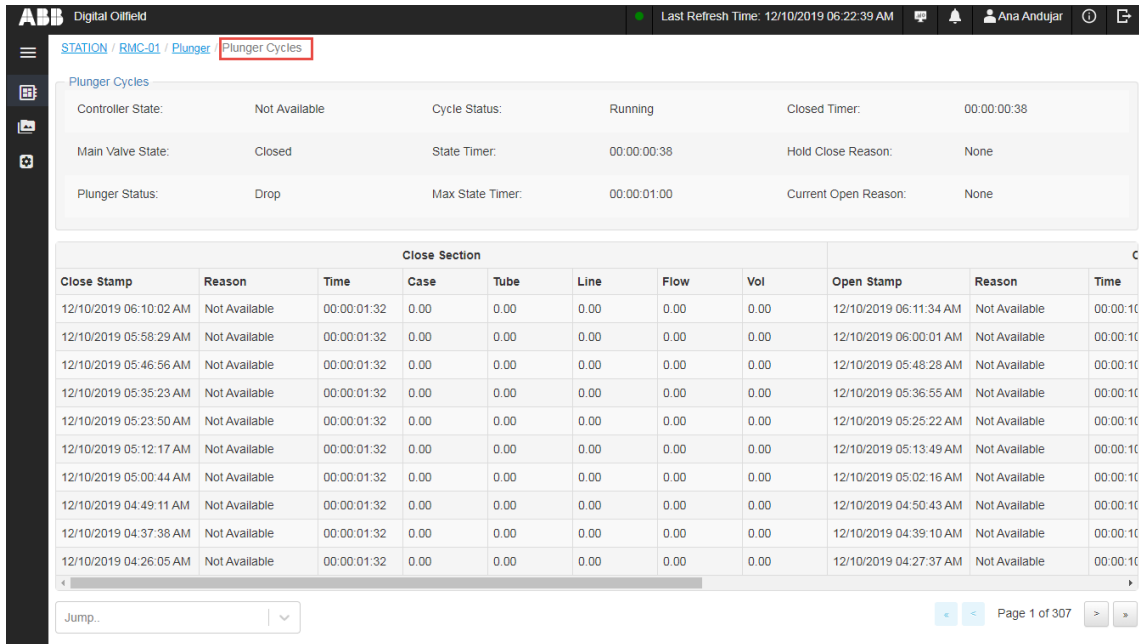
7.4.1.14 View Plunger Cycles

To view the Plunger Cycles page:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Plunger Cycles**.

3. Move the mouse to the main screen area to hide the navigation tree and view the application data and control parameters.

Figure 7-51: Plunger Cycles page

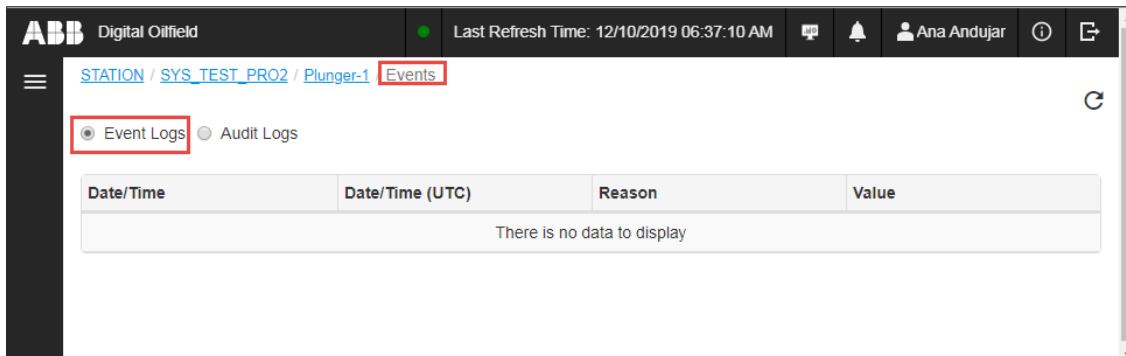


7.4.1.15 View Events

To view the plunger application events:

1. Locate and select the plunger instance on the navigation tree.
2. Select **Events**.
3. Move the mouse to the main screen area to hide the navigation tree and view logged events.

Figure 7-52: Events page



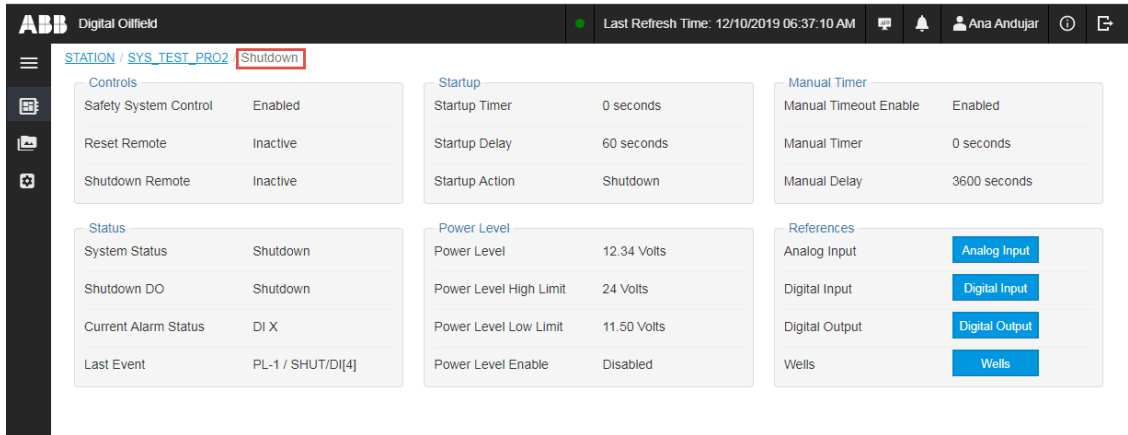
7.4.2 Shutdown application

7.4.2.1 View main page

To view the shutdown landing page:

1. Locate and select the shutdown instance on the navigation tree.
2. Move the mouse to the main screen area to hide the navigation tree and view shutdown information.

Figure 7-53: Main Shutdown page

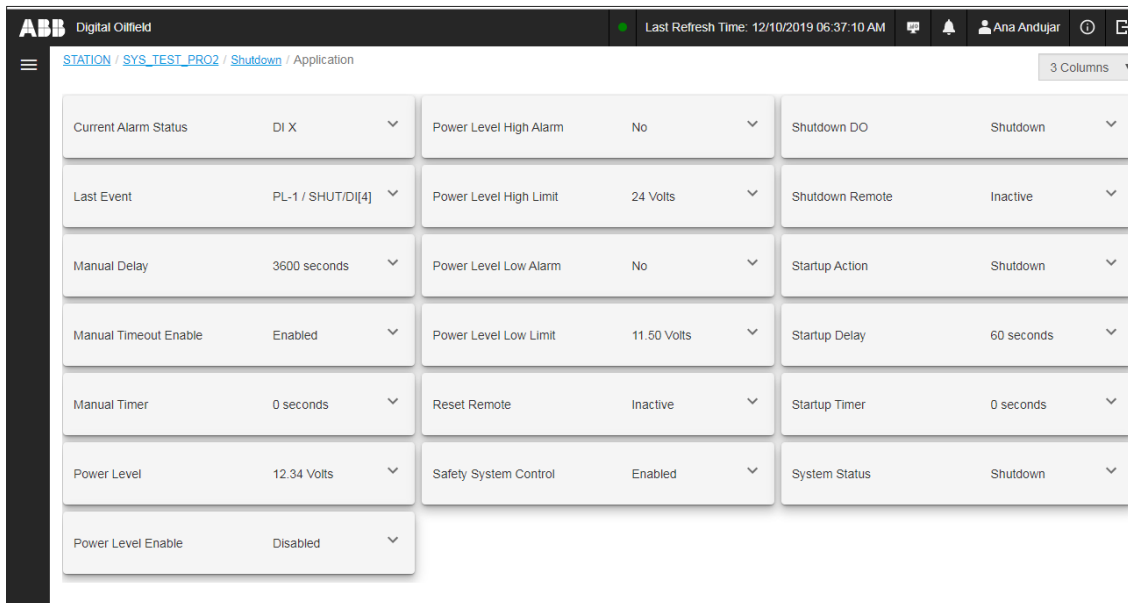


7.4.2.2 View Application page

To view the shutdown Application page:

1. Locate and select the shutdown instance on the navigation tree.
2. Select **Application**.
3. Move the mouse to the main screen area to hide the navigation tree and view shutdown Application information.

Figure 7-54: Shutdown Application page

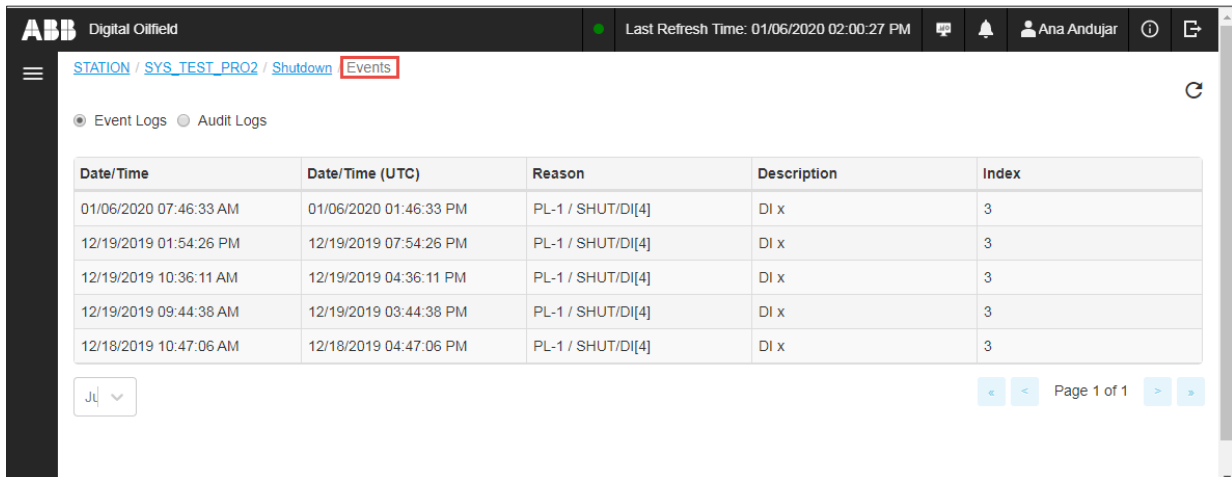


7.4.2.3 View Events

To view shutdown events:

1. Locate and select the shutdown instance on the navigation tree.
2. Select **Events**.
3. Move the mouse to the main screen area to hide the navigation tree and view events.

Figure 7-55: Shutdown Events page



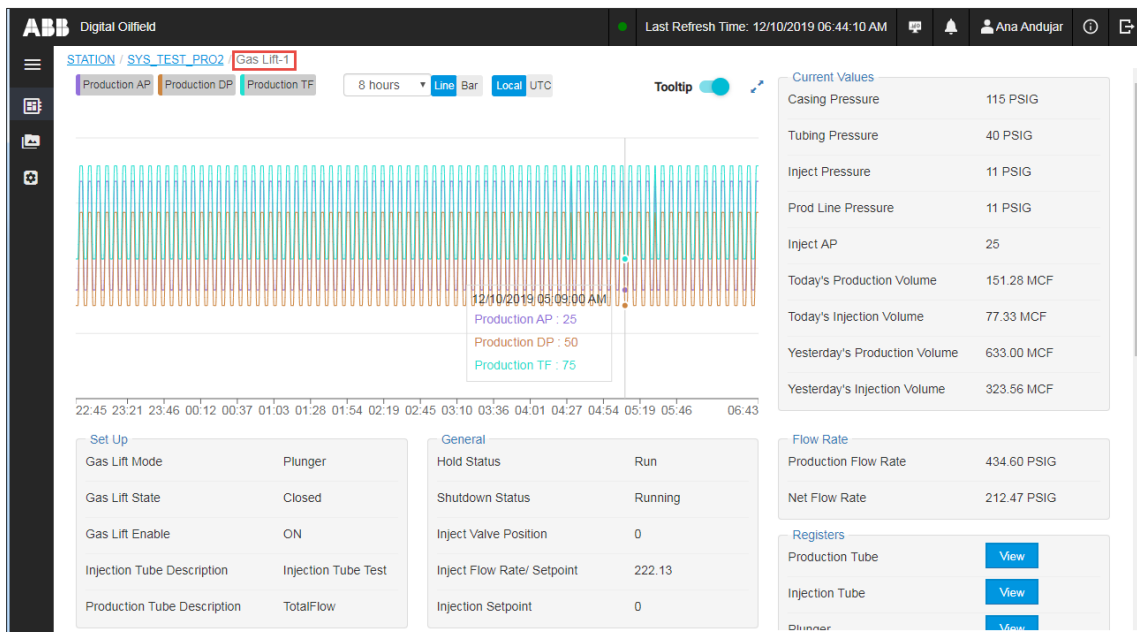
7.4.3 Gas Lift application

7.4.3.1 View the Gas Lift main page

To view the main gas lift page:

1. Locate and select the gas lift instance on the navigation tree.
2. Move the mouse to the main screen area to hide the navigation tree and view gas lift information.

Figure 7-56: Main Gas Lift application page

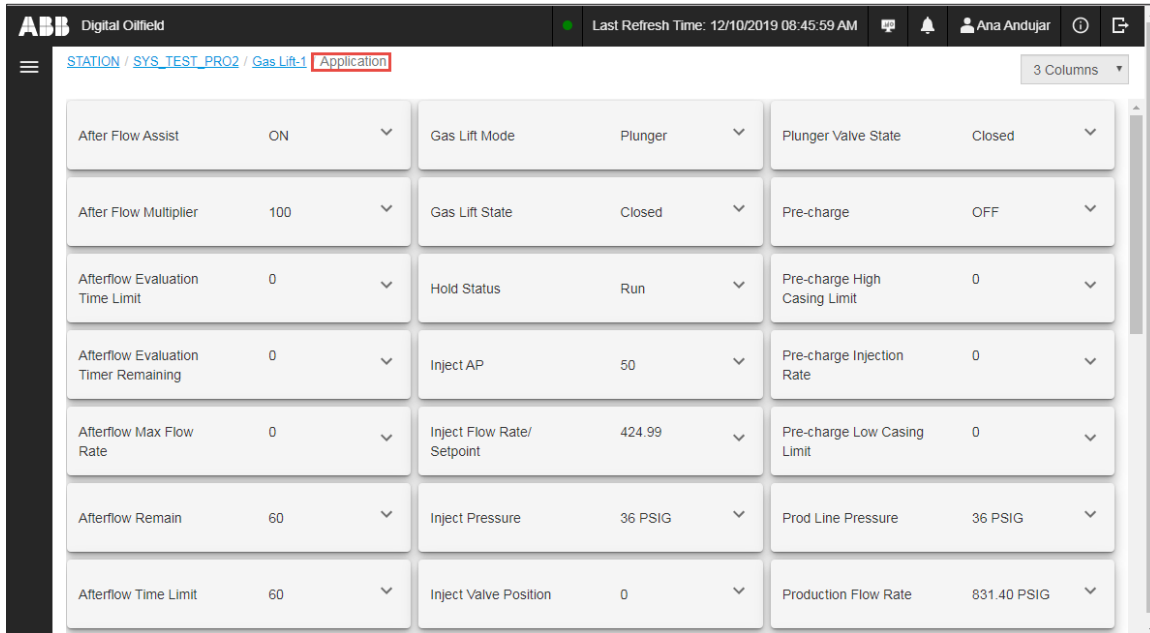


7.4.3.2 View the Application page

To view the application page:

1. Locate and select the gas lift instance on the navigation tree.
2. Select **Application**.
3. Move the mouse to the main screen area to hide the navigation tree and view gas lift application information.

Figure 7-57: Gas lift Application page

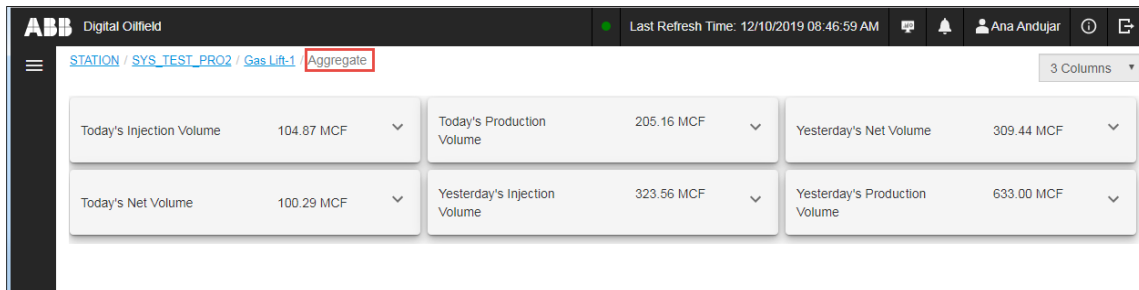


7.4.3.3 View the Aggregate page

To view the view aggregate page:

1. Locate and select the gas lift instance on the navigation tree.
2. Select **Aggregate**.
3. Move the mouse to the main screen area to hide the navigation tree and view gas lift aggregate information.

Figure 7-58: Gas lift Aggregate page



7.4.3.4 View alarms

To view alarms:

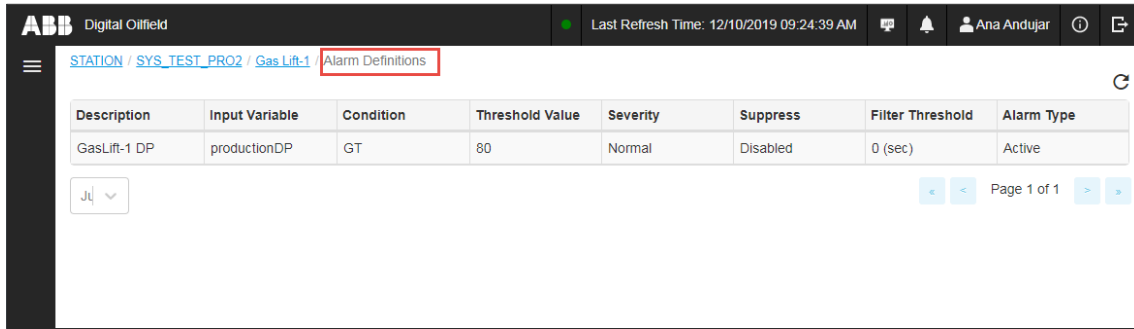
1. Locate and select the gas lift instance on the navigation tree.
2. Select **Alarms**.
3. Move the mouse to the main screen area to hide the navigation tree and view alarms.

7.4.3.5 View Alarm definitions

To view alarms definitions:

1. Locate and select the gas lift instance on the navigation tree.
2. Select **Alarm Definitions**.
3. Move the mouse to the main screen area to hide the navigation tree and view alarm definitions.

Figure 7-59: Gas lift Alarm Definition page

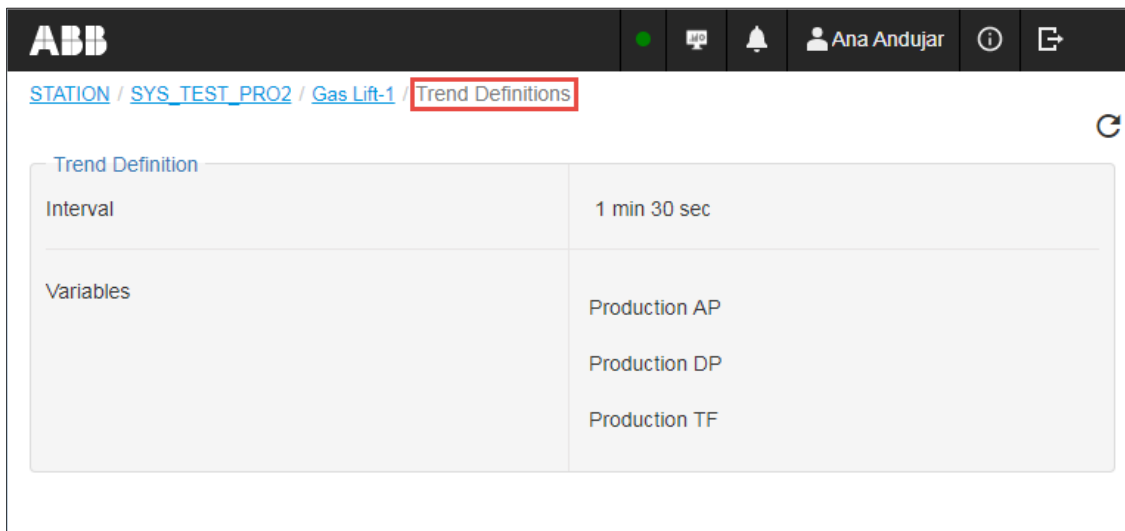


7.4.3.6 View Trend definitions

To view trend definitions:

1. Locate and select the gas lift instance on the navigation tree.
2. Select **Trend Definitions**.
3. Move the mouse to the main screen area to hide the navigation tree and view trend definitions.

Figure 7-60: Gas lift Trend Definitions page

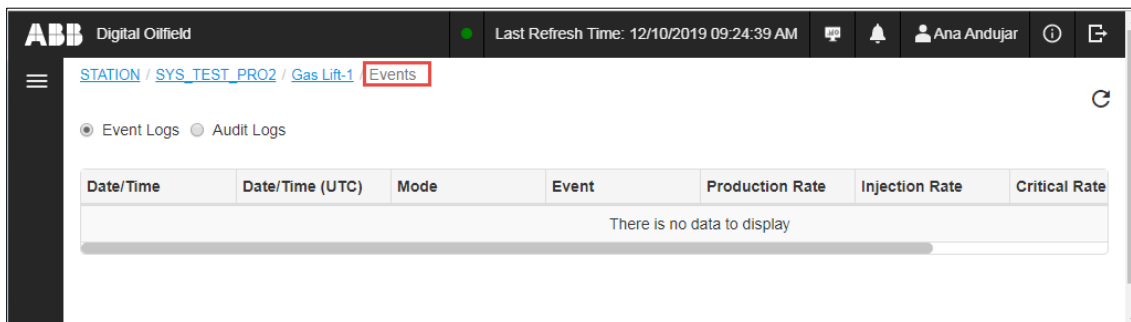


7.4.3.7 View events

To view events:

1. Locate and select the gas lift instance on the navigation tree.
2. Select **Events**.
3. Move the mouse to the main screen area to hide the navigation tree and view events.

Figure 7-61: Gas lift Events page



7.5 Access Plunger Analysis System (PAS) services

The Plunger Analysis services use plunger-related data to perform optimization or fault detection analysis for wells using plungers. This information assists operators in fine-tuning the plunger configuration for optimal gas extraction and production. The analysis services fetch required data from the database on the cloud or private network. It assumes this data is already available on the database.



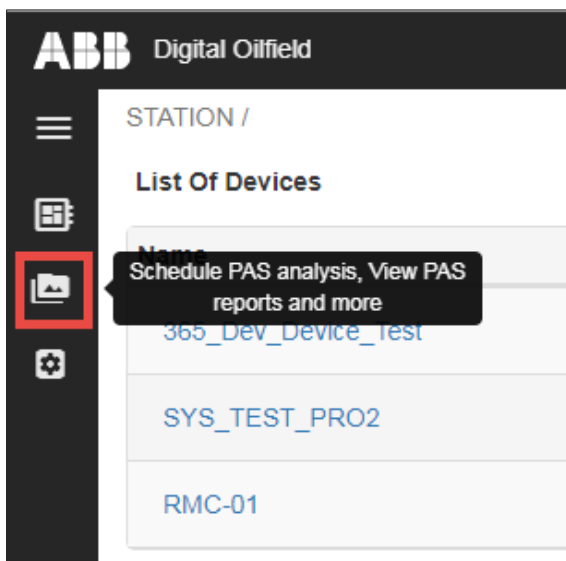
IMPORTANT NOTE: Plunger analysis services require the definition of trend files with specific plunger variables needed for the analysis. When planning to perform an analysis, make sure to create those files so data is available when needed.

7.5.1 Access PAS options

To access the PAS options:

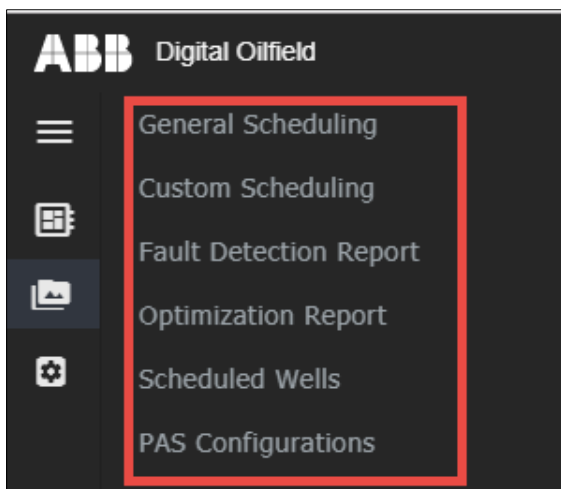
1. Click the PAS service icon ([Figure 7-62](#)).

Figure 7-62: Access to PAS scheduling and report view



2. Select the required option from the list displayed. See the next sections for details about each option.

Figure 7-63: Plunger analysis system options



7.5.2 Schedule analyses for pre-defined intervals

The General Scheduling page provides pre-defined options to schedule optimization and fault detection analysis for specific devices and associated wells. You can select one analysis feature or both.

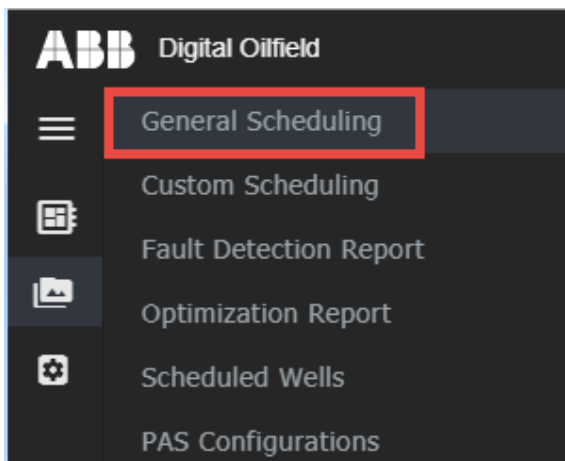
General scheduling supports two scheduling modes: daily or weekly. If these options do not meet your requirements, refer to section [7.5.3 Schedule analyses for user-defined intervals](#).

Analysis results are stored in reports and viewable based on type. See section [7.5.4 View Fault Detection reports](#) and [7.5.5 View Optimization reports](#).

To set General Scheduling:

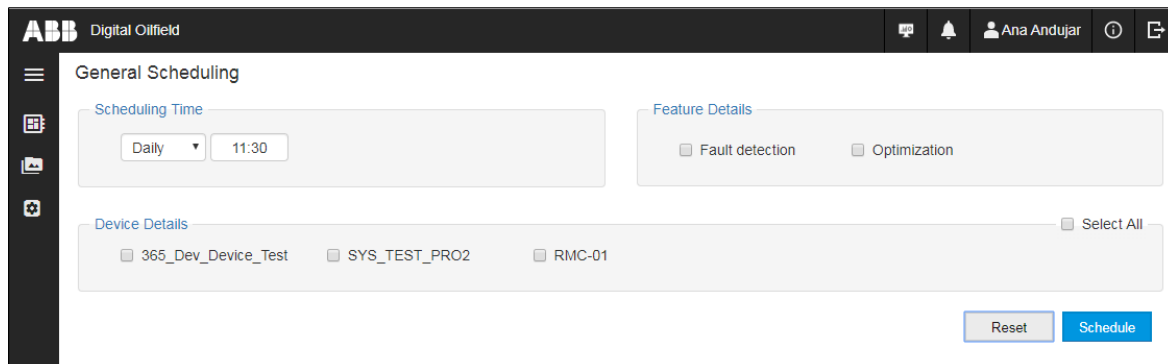
1. Access PAS options as described in section [7.5.1](#).
2. Select **General Scheduling** from the navigation tree ([Figure 7-64](#)).

Figure 7-64: Access PAS General Scheduling



The General scheduling page displays ([Figure 7-65](#)).

Figure 7-65: PAS General Scheduling page

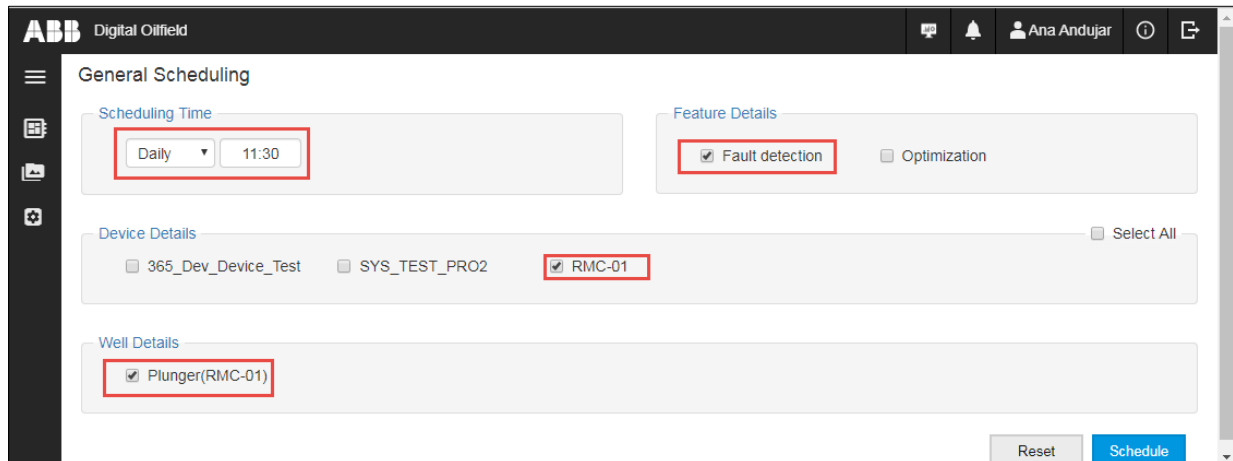


3. Set the scheduling mode and time.
4. In the Feature Details section, select the PAS feature. Select one or both as necessary.
5. Select which device to schedule or click **Select All** to schedule all devices managed from the cloud.
6. In the Well Details section, select which well to schedule or click **Select All** to schedule all wells associated with each of the selected devices. The well name identifies, in parentheses, the device it is associated with. The example in [Figure 7-66](#) shows the schedule for a single device and its associated well for PAS fault detection.



IMPORTANT NOTE: To make different selections, click **Reset** to clear. The screen returns to default values.

Figure 7-66: Example of daily fault detection analysis scheduled for a single well



7. Click **Schedule**.

7.5.3 Schedule analyses for user-defined intervals (custom)

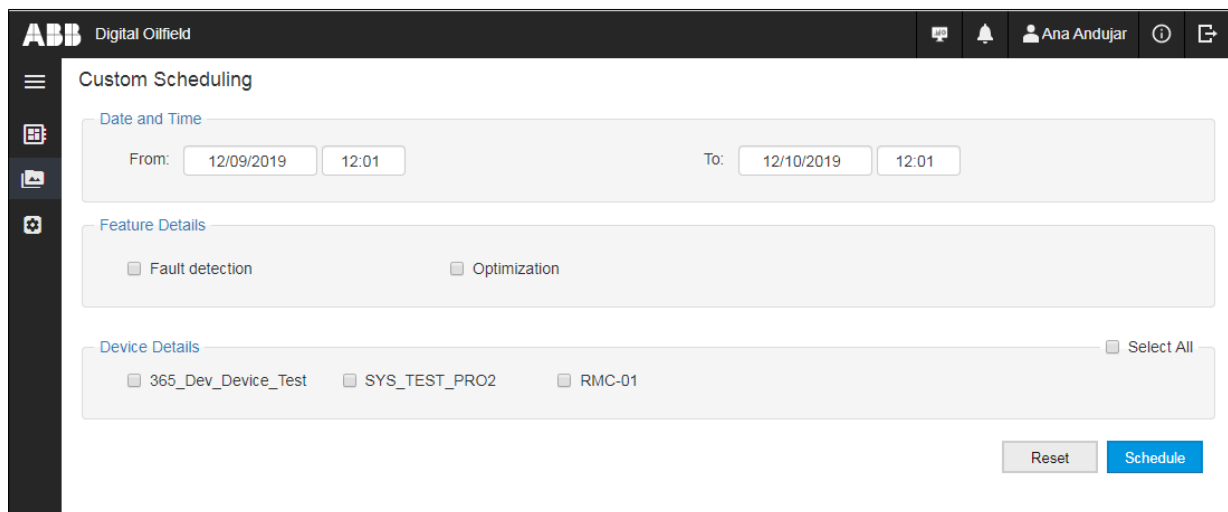
The Custom Scheduling page allows the configuration of a user-defined time interval to run plunger analysis for selected wells. You can select one analysis feature or both.

Analysis results are stored in reports and viewable based on type. See sections [7.5.4 View Fault Detection report](#) and [7.5.5 View Optimization report](#).

To set Custom Scheduling:

1. Access PAS options as described in section [7.5.1](#).
2. Select **Custom Scheduling** from the navigation tree.

Figure 7-67: Custom Scheduling page

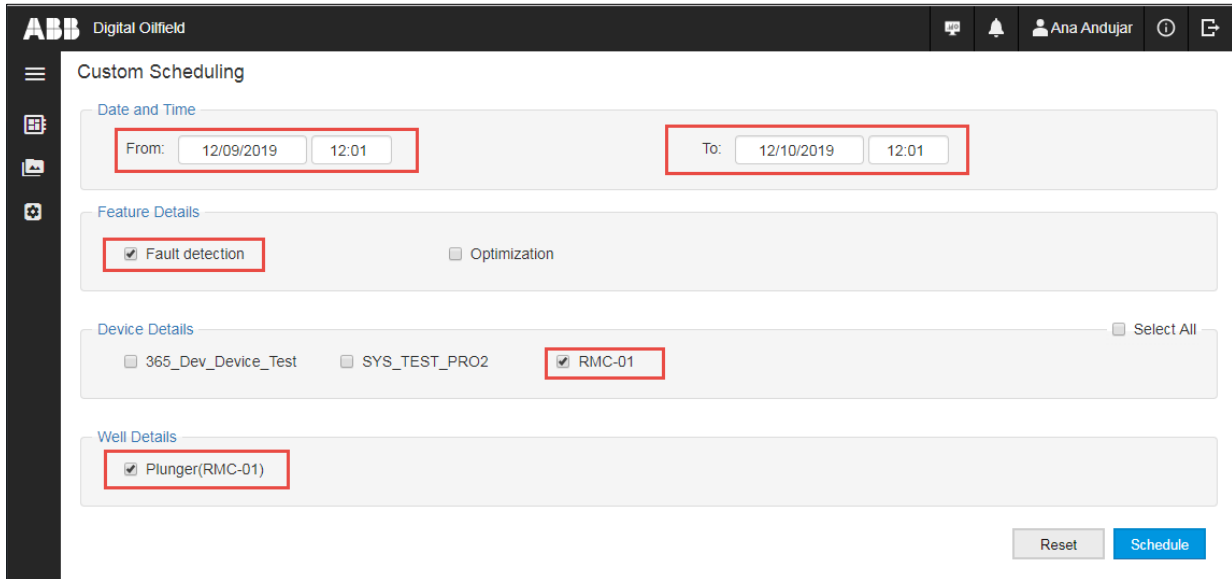


3. Set the beginning and end date and time of the scheduled analysis run.
4. In the Feature Details section, select the PAS feature in Feature Details. Select one or both as necessary.
5. Select which device to schedule or click **Select All** to schedule all devices managed from the cloud.
6. In the Well Details section, select which well to schedule or click **Select All** to schedule all wells associated with each of the selected devices. The well name identifies, in parentheses, the device it is associated with.



IMPORTANT NOTE: To make different selections, click **Reset** to clear. The screen returns to default values.

Figure 7-68: Example of custom fault detection analysis scheduled for a single well



7. Click **Schedule**.

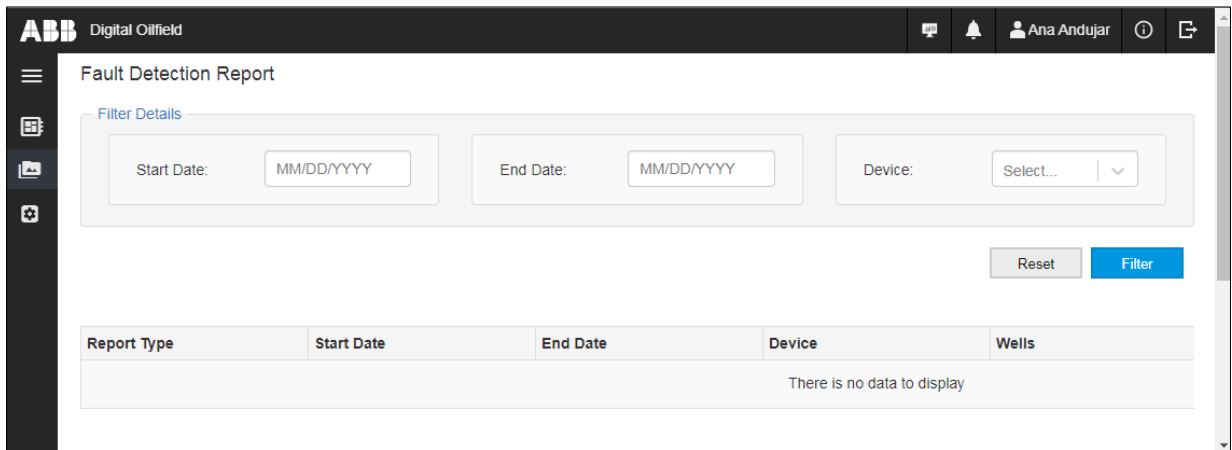
7.5.4 View Fault Detection reports

The Fault Detection report screens provide access to view analysis reports generated when analyses are scheduled for fault detection. The page provides filters to narrow down the report search.

To view Fault Detection report(s):

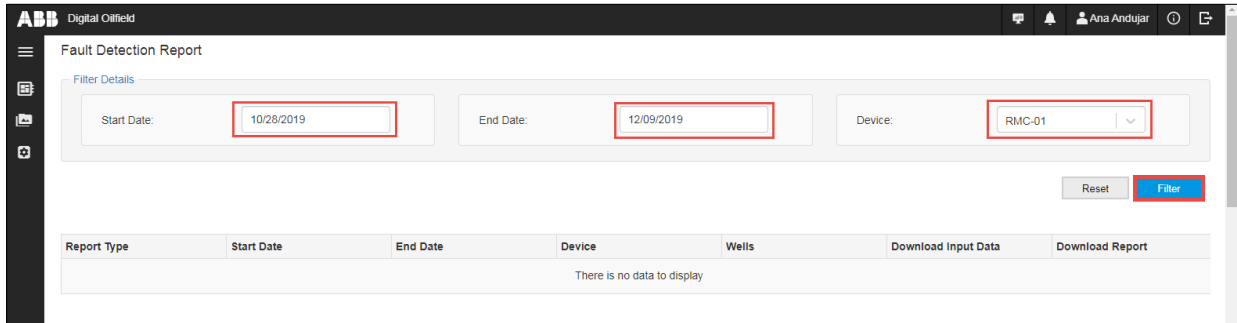
1. Access PAS options as described in section [7.5.1](#).
2. Select **Fault Detection Report** from the navigation tree. The Fault Detection Report page displays ([Figure 7-69](#)).

Figure 7-69: Fault Detection Report page



3. Select the Start and End dates for the report.
4. Select the device to list reports for.
5. Click **Filter**. View reports (if any) displayed below.

Figure 7-70: Filter report view by scheduled interval and device



6. Click **Reset** to apply different filters.

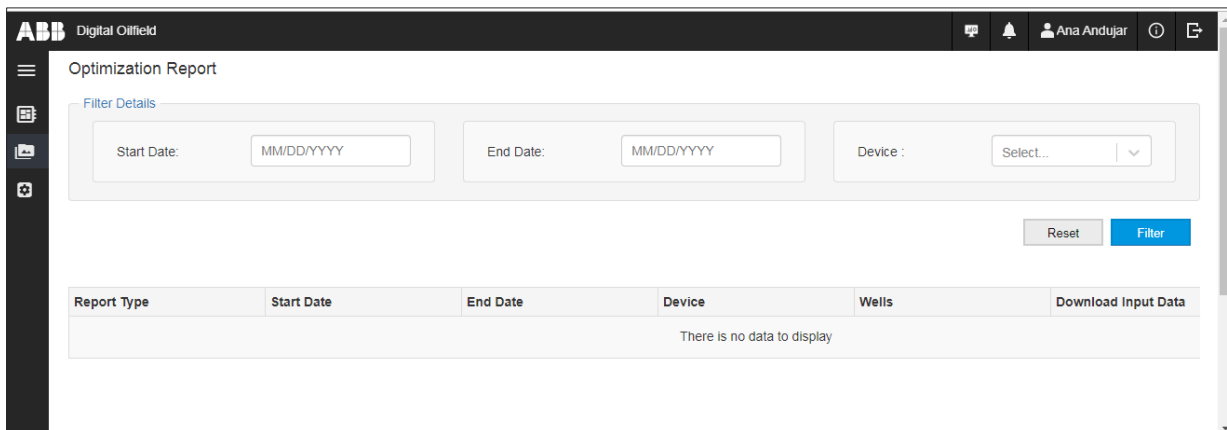
7.5.5 View Optimization reports

The Optimization report screens provide access to view analysis reports generated when analyses are scheduled for well optimization. The page provides filters to narrow down the report search.

To view optimization reports:

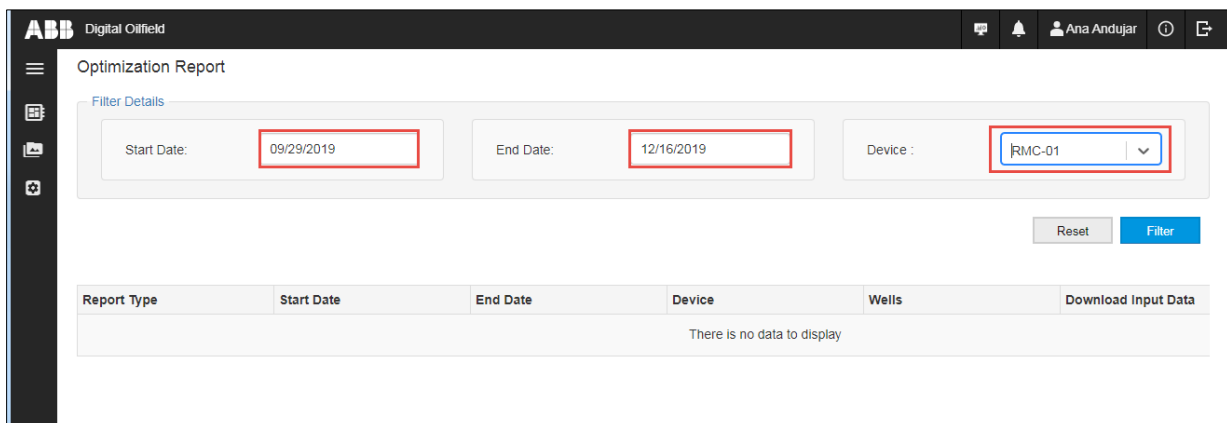
1. Access PAS options as described in section [7.5.1](#).
2. Select **Optimization Report** from the navigation tree. The Fault Detection Report page displays ([Figure 7-71](#)).

Figure 7-71: Optimization Report page



3. Select the Start and End dates for the report.
4. Select the device to list reports for.
5. Click **Filter**. View reports (if any) displayed below.

Figure 7-72: Filter report view by scheduled interval and device



6. Click **Reset** to apply different filters as necessary.

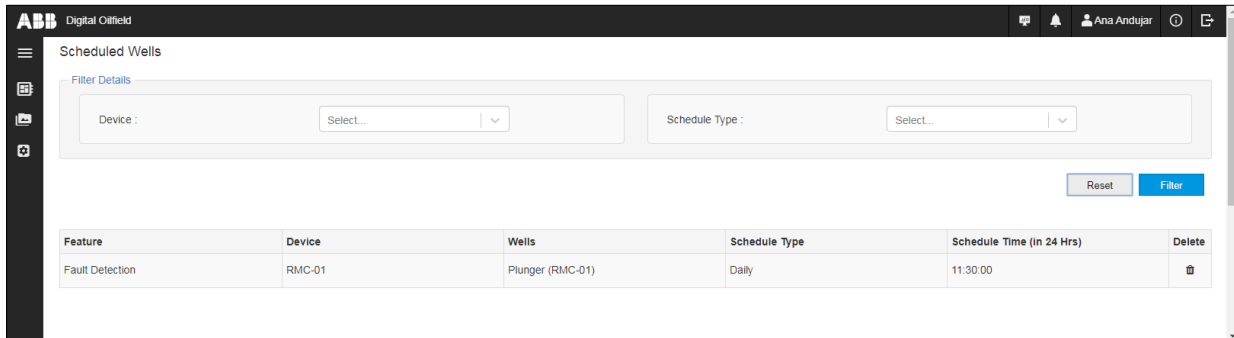
7.5.6 View wells with scheduled analyses

The View Scheduled Wells page displays the wells that have scheduled analyses. You can review or clear schedules from this page.

To view scheduled wells:

1. Access PAS options as described in section [7.5.1](#).
2. Select **Scheduled Wells** from the navigation tree. The Scheduled Wells page displays. If there are scheduled analysis jobs, they display in the page.

Figure 7-73: Scheduled Wells



3. If the well list is long, select the device of interest and schedule type and click **Filter**. The filter narrows down the view to simplify search.
4. To remove a scheduled well, click on the delete icon.
5. Click **Yes** to confirm.

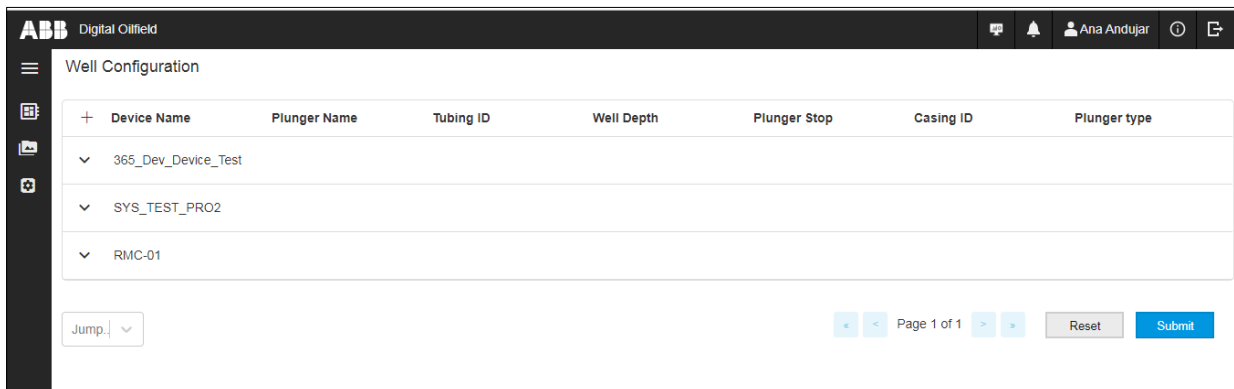
7.5.7 View well configurations

The Well Configurations page displays details for each scheduled well. The plunger application variables that are required for analysis display.

To view PAS configurations:

1. Access PAS options as described in section [7.5.1](#).
2. Select **PAS Configurations** from the navigation tree. The Well Configuration page displays with a list of devices with plunger applications instances.

Figure 7-74: Well Configuration page



3. Click the device of interest for additional detail. The plunger application instances configured in the device display with the configuration parameters used for plunger analysis. Each plunger application handles a single well.

Figure 7-75: Required variables for plunger analysis

The screenshot shows the 'Well Configuration' interface in the ABB Digital Oilfield system. The interface is titled 'Well Configuration' and features a sidebar with navigation icons. The main content area displays a table of well configurations. The table has the following columns: Device Name, Plunger Name, Tubing ID, Well Depth, Plunger Stop, Casing ID, and Plunger type. The table is currently expanded to show the configuration for the device 'SYS_TEST_PRO2'. The configuration details are as follows:

Device Name	Plunger Name	Tubing ID	Well Depth	Plunger Stop	Casing ID	Plunger type
365_Dev_Device_Test						
SYS_TEST_PRO2	Plunger-1	1.995000004	5	5	4	Dual Pad
	Plunger-2	1.995000004	7000	6970	4	Dual Pad
	Plunger-3	1.995000004	7000	6970	4	Dual Pad
	Plunger-4	1.995000004	7000	6970	4	Dual Pad

At the bottom of the interface, there is a 'Jump' dropdown menu, a 'Page 1 of 1' indicator, and 'Reset' and 'Submit' buttons.

4. Configure parameters as necessary.
5. Click **Submit**.

8 PAS access from the cloud interface

The cloud interface provides a link to the Plunger Analysis System (PAS), a standalone ABB web application featuring plunger application fault detection and optimization analysis as well as training. This application is also hosted on Azure, but it is independent from the Digital Oilfield. The trend files required for PAS must be uploaded to run the analyses. PAS does not use data stored on the Digital oilfield database.

To have full access to all the PAS features, you must purchase any of the different service options and obtain login credentials from your administrator. The credentials for PAS are not the same as those used to access the Digital Oilfield.

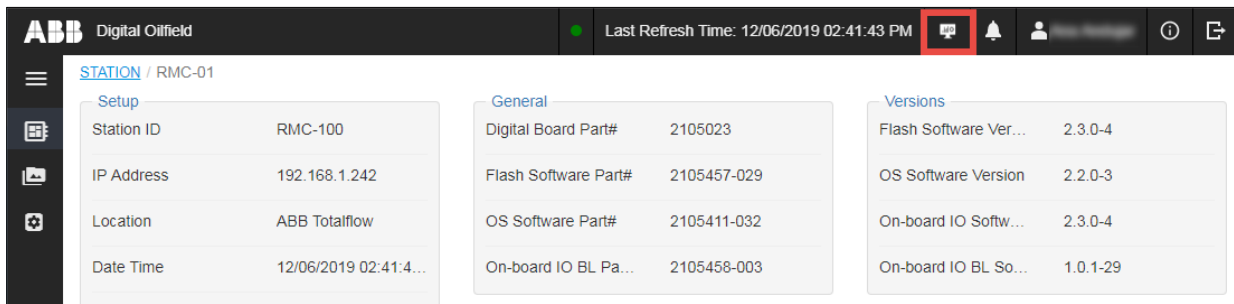


IMPORTANT NOTE: Refer to the Plunger Analysis System Administration Guide for details on this web application. See [Additional information](#) for a link to the document.

To access the Plunger application page:

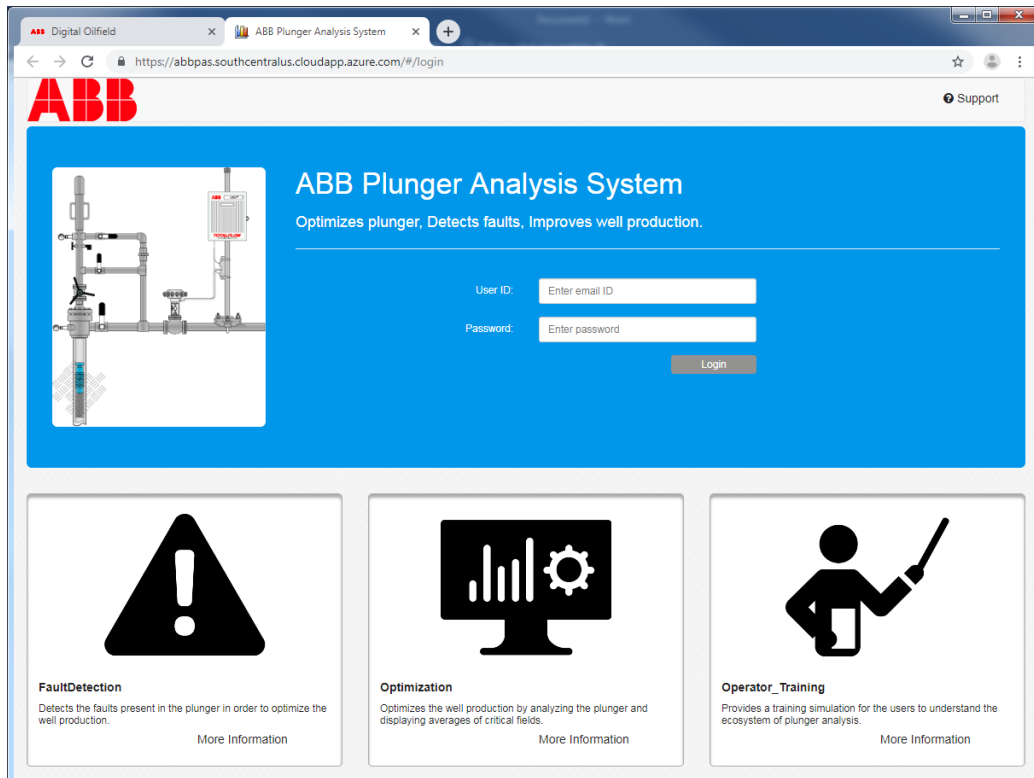
1. Click the PAS icon.

Figure 8-1: Select the PAS icon



2. Ensure that the PAS login page displays ([Figure 8-2](#)).

Figure 8-2: PAS portal



9 Totalflow device security

The following sections include information regarding security for Totalflow devices connected to the Digital Oilfield. Review guidelines, recommendations, and additional device details prior to connecting and configuring MQTT-enabled devices.

9.1 Device security guidelines

This section contains recommended guidelines to secure access to the Totalflow device. [Table 9-1](#) lists guidelines applicable to MQTT configuration interface and operation.



IMPORTANT NOTE: Refer to the device user manual for detailed guidelines and procedures to secure physical access to the device or access from PCCU. This manual only includes procedures relevant to the MQTT functionality. See [Additional information](#) for links to manuals.

Table 9-1: Guidelines for MQTT device configuration user interface and operation

Recommendation	Description
Secure network connection	Connect the device only to a firewall-protected private network. Do not connect directly to the Internet. See section 9.2 Secure connections .
Secure access to the device user interface	Change default passwords to private passwords on user accounts created at the factory. The device enforces a strong password policy which allows defining passwords with a minimum and maximum length, the use of special characters and upper- and lower-case letters, etc. Add new user accounts and assign appropriate roles and private credentials. See section 10.4 Manage users .
Manage configuration interface credentials	Store all private device interface credentials in safe locations. Share private device interface credentials only with properly trained and authorized personnel. Change or update private credentials as needed.
Secure connection with the MQTT broker	Select cloud service options that support secure MQTT connections (TLS connections on port 8883). See section 3.5 Configure MQTT Server Details .
Manage MQTT credentials and authentication certificates	Generate and upload valid certificates to the device. Store all authentication certificates in safe locations. Change or update authentication certificates as needed.
Purge sensitive device data when decommissioning	Device decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information. See 9.6 Device data protection for decommissioning .

9.2 Secure connections

[Figure 9-1](#) shows a simplified high-level view of the Digital Oilfield implementation. Remote connections to and from the device must be established over the corporate network for security. Field local area network equipment access for local operator connections should be protected.

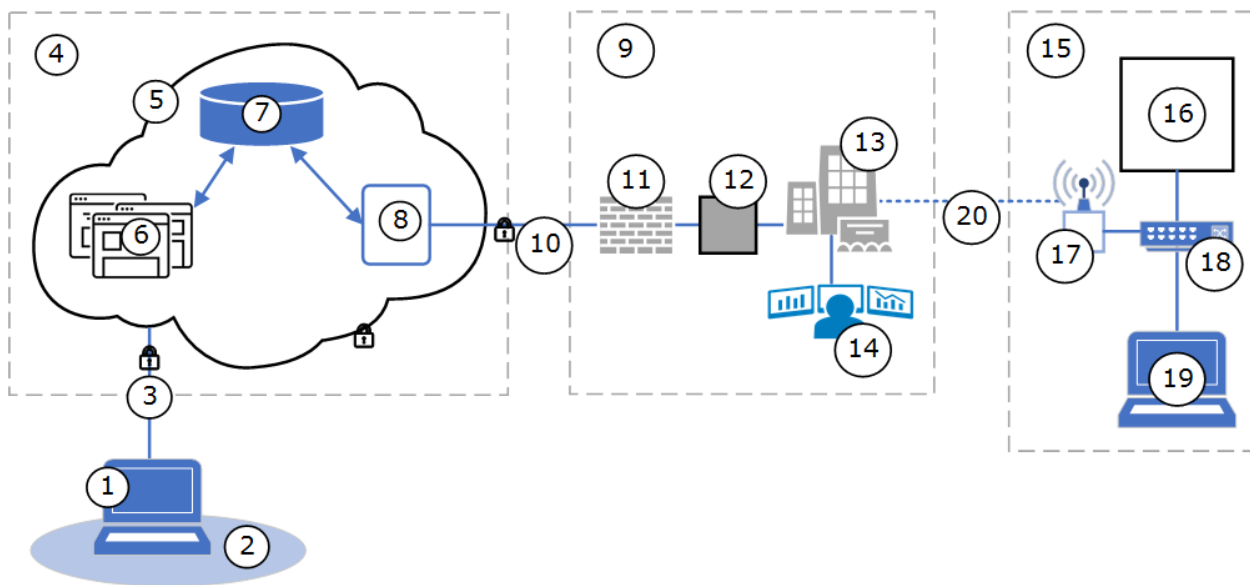


IMPORTANT NOTE: The RMC-100 is not an internet-facing device. Do not connect directly to the Internet. An MQTT gateway is required between the Digital Oilfield and the RMC. In the event that the customer’s corporate network firewall is compromised, the RMC-100 would be at risk without the MQTT gateway.



IMPORTANT NOTE: [Figure 9-1](#) is a basic illustration. Specific equipment, connections, and network topologies depend on the customer specifics at their sites. Communication equipment options and configuration at customer field sites vary depending on site complexity and available communication technology and services. Sites can be equipped with managed switches supporting firewall, rate limiting, SNMP and other capabilities. In addition, wireless gateways connect the site to the corporate network over a radio-based private network (VPN).

Figure 9-1: Digital Oilfield implementation connections



Legend for Figure 9-1: Digital Oilfield implementation connections

Remote access to cloud service provider	Customer private network	Field site
1 Web user with client system: PC/laptop or mobile devices	9 Corporate network	15 Field Local Area Network
2 Access network/internet	10 Secure connection to Digital Oilfield	16 MQTT-enabled Totalflow device (connected peripherals not shown)
3 Secure connection to the cloud (using corporate VPN)	11 Firewall	17 Wireless router (Ethernet-to-radio)
4 Service provider network/platform	12 MQTT gateway	18 Managed Ethernet switch (Supports connections for all devices on site)
5 Customer Digital Oilfield	13 Operations center/field office	19 Local user
6 Digital Oilfield interface (web app)	14 SCADA/IIoT systems	20 Secure (wireless) connection to corporate network
7 Database for data storage		
8 MQTT broker		



IMPORTANT NOTE: It is the customer's responsibility to ensure that local and network connections with the device are secure. Communication equipment at the site must be protected and configured to prevent unauthorized access. Devices should never be connected directly to the Internet. Call ABB for information about ABB communication equipment and solutions.

9.2.1 Field Local Area Network connections

The customer field Local Area Network (LAN) may have a combination of Ethernet and wireless network equipment available. This equipment is for local connections of field devices and the connection (or uplink) of the entire site to the corporate network. The following connections should be supported on the site LAN:

- MQTT-enabled device-to-network equipment connection. Use the device's Ethernet port and configure valid IP parameters on the device.
- Local operator laptop-to-network equipment connection. Local connection supports access to the device configuration interface for MQTT operation.



IMPORTANT NOTE: The RMC-100 is not an internet-facing device. Do not connect directly to the Internet. An MQTT gateway is required between the Digital Oilfield and the RMC. In the event that the customer's corporate network firewall is compromised, the RMC-100 would be at risk without the MQTT gateway.

9.2.2 Customer corporate network connections

Traffic flow between the MQTT-enabled devices and the MQTT broker must be protected. The data traffic must remain within the customer private network. The customer private network must:

- Support the site network equipment connection (or wireless access)
- Support secure connection to the cloud, firewall-protected
- Support an MQTT Edge gateway adding an additional layer of security for MQTT-enabled devices

9.2.3 Web user connections (access)

Authorized remote web users should have access to a secure connection from the customer premises or use the corporate VPN.

Once on the VPN, web users can access:

- The Digital Oilfield cloud user interface (web app) to view data
- The device configuration interface for MQTT operation or configuration

9.2.4 Monitor load on network connection

Network load (packets received on the device network interface) affects CPU utilization and the efficiency of data packet processing in the device.

Heavy network load or a malicious Denial of Service (DOS) attack can impact the ability of the device to communicate with the cloud to publish its data and receive data update requests or commands in a timely manner.

The percentage (%) of CPU utilization and the data processing efficiency (Bytes processed/Bytes received) in Totalflow devices have been tested for several network traffic conditions:

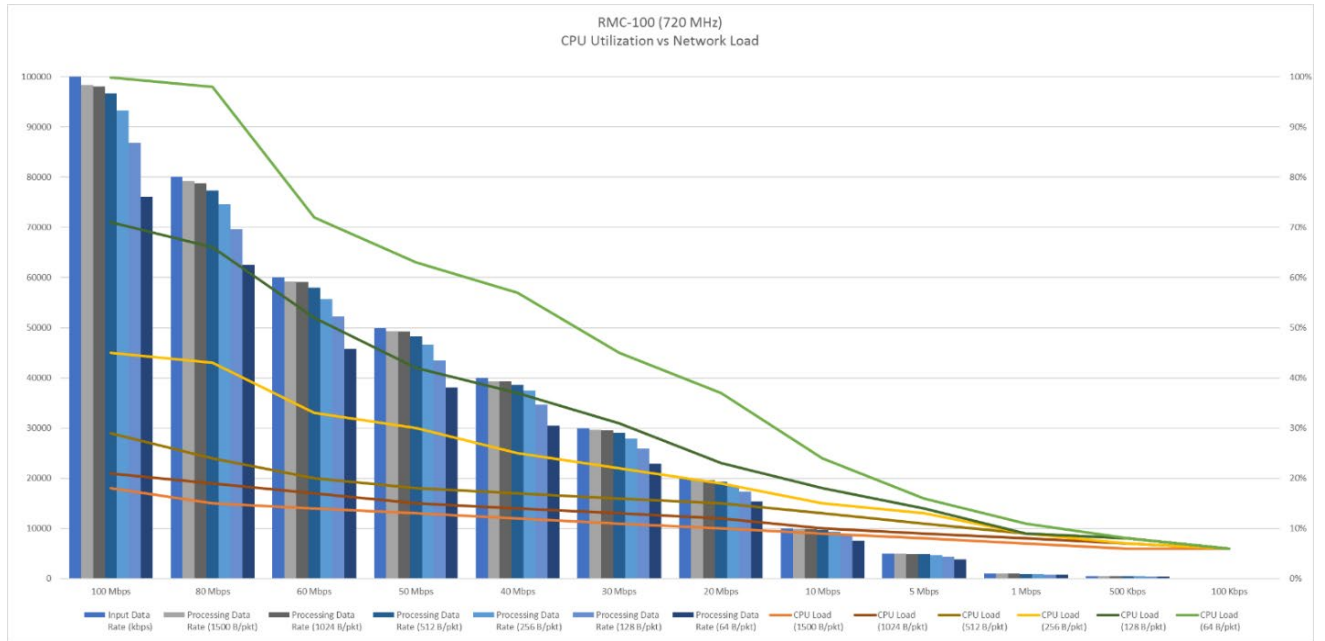
- Data rate range: 100 Kbps – 100 Mbps
- Packet sizes (bytes): 64, 128, 256, 512, 1024, 1500
- Input packet rates:
 - Highest Packet Rate at 100 Mbps - 195313 packet/sec (64 Bytes/packet)
 - Lowest Packet Rate at 100 Mbps - 8333 packet/sec (1500 Bytes/packet)

[Figure 9-2](#) shows the results of the tests for the RMC-100 (on its Ethernet interface).



IMPORTANT NOTE: When devices connect to the cloud, it is important to monitor their network connection to ensure they handle the network load optimally. Refer to the PCCU help files for information about parameters monitored on the Ethernet ports. Refer to [Additional information](#) for links to documents related to Ethernet parameters.

Figure 9-2: CPU utilization vs network load



9.3 Secure access to the MQTT configuration interface

When logging into the MQTT device configuration interface for the first time, the connection to the device shows as “Not secure”. To prevent certificate or connection errors from displaying, configure the browser for protected mode.

This procedure imports the device’s certificate to the browser’s Trusted Root Certification Authorities certificate store. It requires the following:

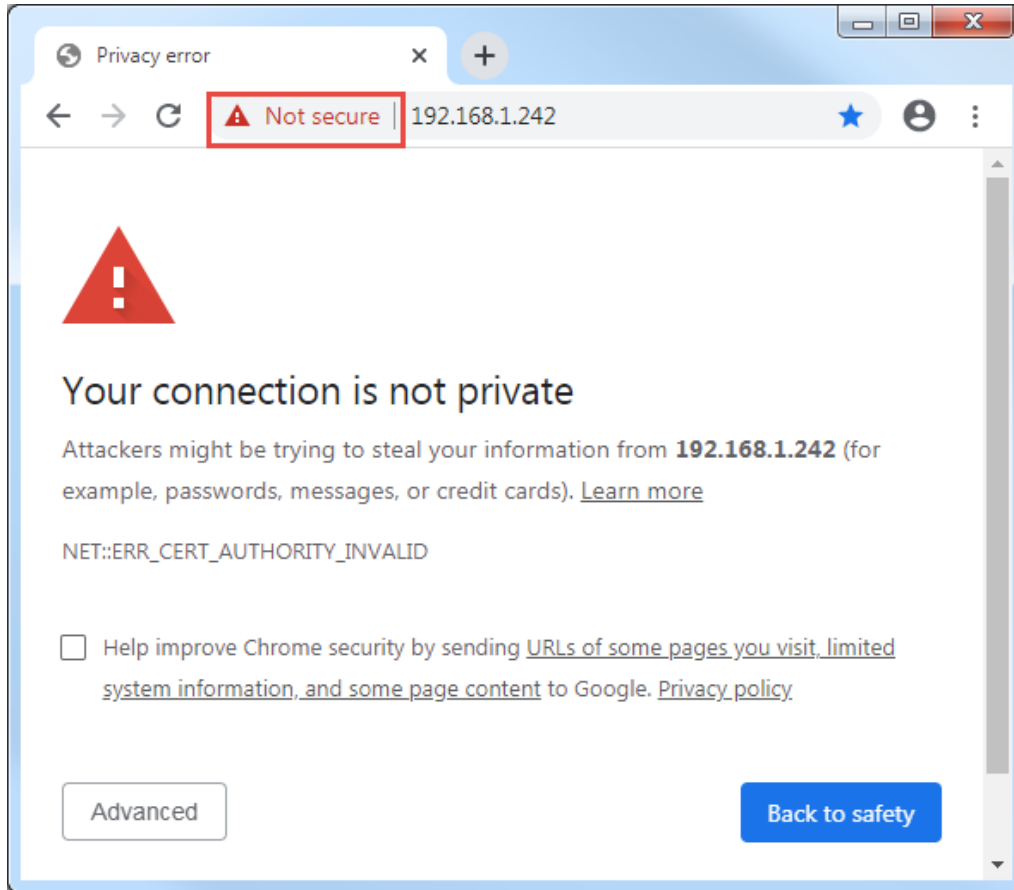
- The device’s certificates are ready, generated with the specific device information, and named correctly. Complete certificate generation is described in section [10.3 Generate certificates for X.509 authentication](#) .
- Certificates are saved on the device. Complete certificate upload from the Initial Configuration screen is described in section [3.5 Configure MQTT Server Details](#).

i **IMPORTANT NOTE:** When generating device certificates, you must generate for the device’s fully qualified domain name (FQDN) or IP address. Certificates files must be renamed as “client-cert.pem” and “client-key.pem”. See section [10.3 Generate certificates for X.509 authentication](#) .

To add certificates to the browser configuration:

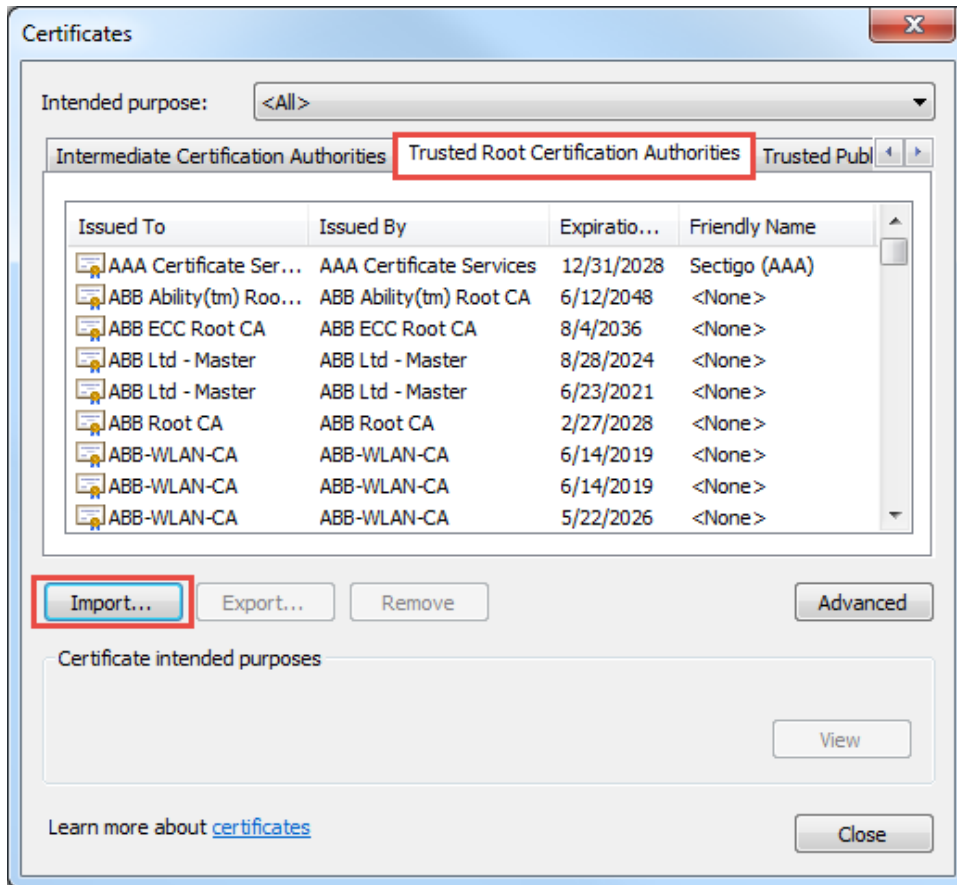
1. Start Chrome browser.
2. Go to the URL address: **https://<Totalflow device’s IP address >:443**. For example, https://192.168.1.42:443. A security warning displays on the screen and the URL address field shows the “Not Secure” warning ([Figure 9-3](#)).

Figure 9-3: Security warnings: browser-device connection



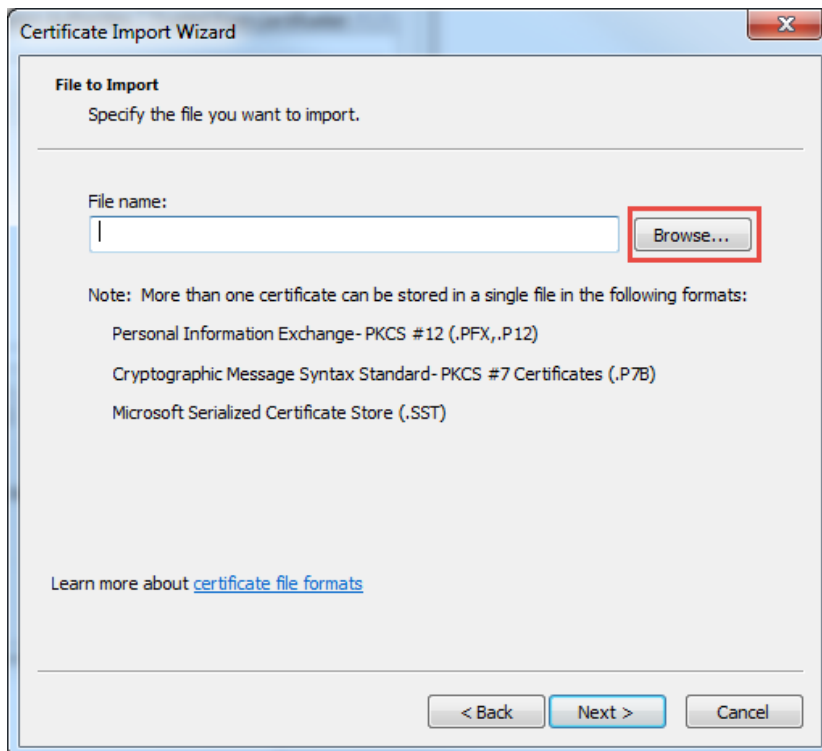
3. Select **Not secure**.
4. Click **Site Settings**.
5. Select **Manage Certificates**. The Certificates window displays (Figure 9-4).
6. Select **Trusted Root Certification Authorities > Import** (Figure 9-4). The certificate import wizard may display. Click **Next** as necessary for the prompts to complete the import.

Figure 9-4: Chrome certificate management window



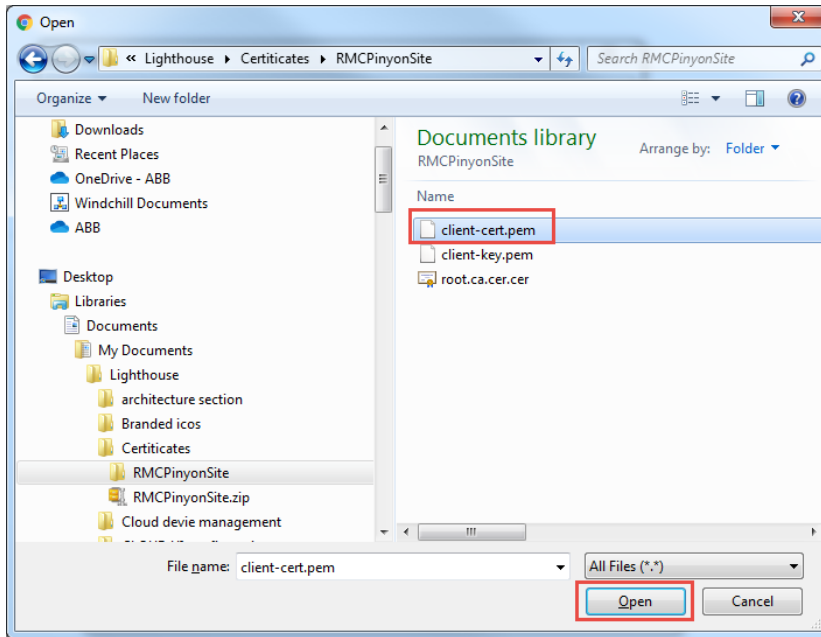
7. On the Certificate Import Window (Figure 9-5), click **Browse** to search for the certificate file. Click **Next** to proceed.

Figure 9-5: Certificate import



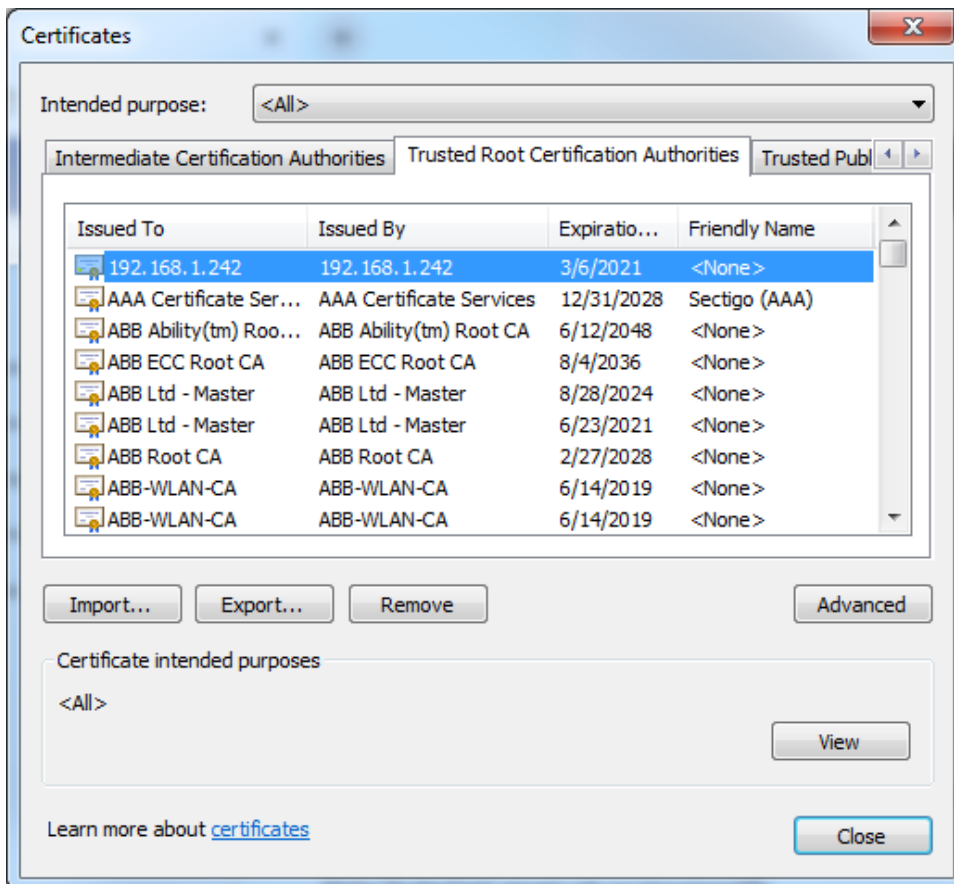
- On the file browser window (Figure 9-6), locate and select the certificate file named "client-cert.pem" and click **Open** to import.

Figure 9-6: Import device certificate for browser



- Once the import is complete, click **Finish** to exit the wizard and return to the Certificates window.
- Ensure that the certificate is imported into the Trusted Root Certification Authorities certificate store. The certificate is listed identifying the IP address of the device (Figure 9-7).

Figure 9-7: Device certificate in the Trusted Root Certification Authorities certificate store



11. Click **Close**. The protected mode should be enabled in the security section of the browser.
12. Relaunch the browser and reconnect to the device. The certificate error should not display.

9.4 Open TCP ports on devices

The table below lists the open Transmission Control Protocol (TCP) ports on MQTT-enabled Totalflow devices such as the RMC-100. These ports are used for all TCP/IP based connections which are supported by the Ethernet ports.

Protocols over TCP can be standard like SSH, or proprietary like Totalflow (remote or local).

Table 9-2: Open TCP ports on device

Default TCP port	User-configurable	Service or protocol using the port	Description
443	No	HTTPS	Assigned to connections used for device configuration and management of MQTT communication and operation. Web browser clients request these connections within onsite networks or corporate intranets. Clients access web pages hosted by the device.
9999	Yes	Totalflow/TCP	Assigned to connections used for device monitoring, configuration and data collection or polling. PCCU, WinCCU, TDS and third-party SCADA systems request these connections.
65535	No	Totalflow Device Loader/TCP	Assigned to the device loader connections for device software update. PCCU requests this type of connection.
9696	No	SSH/TCP	Assigned to secure shell (SSH/SFTP) connections. Third-party SSH/SFTP clients request these connections.
502	Yes	Modbus /TCP	Assigned to connections between the RMC and external Modbus devices for communication and data transfer

9.5 Services on devices

Services are software processes that run on Totalflow devices. External users, external applications or internal processes within the device can access these services for several purposes. Some services are user-enabled, others are automatically enabled by the device at startup. Sections [9.5.1](#) and [9.5.2](#) provide lists of exposed services.

9.5.1 User-enabled services

[Table 9-3](#) lists user-enabled services that open access to the embedded software file system. Unauthorized or malicious use of these services can cause file corruption and render a device inoperable.

IMPORTANT NOTE: Users can enable or disable the services in [Table 9-3](#) from PCCU. Implement security features as soon as the device is installed to prevent unauthorized users from changing the desired state of these services.

Table 9-3: User-enabled services in the RMC-100 and XSeries^{G5} products

Service Name (port)	Default state	Description	Security feature available
SSH/SFTP Service (9696)	Disabled	Serves connection requests for secure login shell and file transfer. Supports connection requests from third-party SSH/SFTP clients	Authentication based on private-public key pairs, passphrase-protected keys
Totalflow Software	Enabled	Enables or blocks the ability	None specific to the service. Must

Service Name (port)	Default state	Description	Security feature available
Update Service (65535)		of the device loader to update the embedded software	use Bi-level security passcode or Role-Based Authentication (Role-Based Authentication, RBAC)

9.5.2 Device-enabled services for MQTT support

[Table 9-4](#) lists device-enabled services or processes affected by or associated with MQTT functionality and configuration. These services are automatically started at device startup.

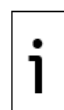
MQTT-related services provide access to authorized third-party devices, such as MQTT brokers on a cloud, or to users for device configuration.

Table 9-4: Services required for MQTT operation

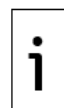
Service/ Process	Default state	Description	Security feature available
Totalflow application	Enabled	Core Totalflow application process that monitors and collects the specific register data it sends to the MQTT core process/service. The Totalflow application is independent of the MQTT functionality. Normal device operation is not affected by disconnection from the MQTT broker or other MQTT issues.	None specific to the application. Users do have the ability to shut down or restart the Totalflow application from PCCU, or the onboard restart button, which disrupts device operation. Follow general guidelines to protect access to the device: Restrict physical access, use Bi-level security passcode or Role-Based Authentication (Role-Based Authentication, RBAC).
MQTT core	Enabled	Process that performs the MQTT client function for communication with the MQTT broker. The client initiates communication with the MQTT broker by sending a connection request.	Security features inherent to the secure (TLS) connection standard used on the device-MQTT broker connection. Authentication certificates
REST server	Enabled	Serves connection requests for client access to the device configuration web pages (configuration interface for MQTT related parameters). The service listens to TCP port 443 for connection requests.	Access to the device is protected by role-based access control: Access requires credentials-based authentication. The device configuration interface supports a user management to add users and assign roles. Users can replace factory default credentials with private credentials for authentication of authorized personnel only.

9.6 Device data protection for decommissioning

Device decommissioning must include purging sensitive data stored on the device. Totalflow devices support the reset to factory default configuration which removes the existing configuration and device data.



IMPORTANT NOTE: To reuse application credits on other devices, be sure to transfer credits from the device to the credit key before decommissioning. See the Application Licensing help topic in the PCCU help files for detailed procedures.



IMPORTANT NOTE: Restoring factory defaults deletes all data and configuration. Be sure to collect measurement data and back up configuration as necessary.

To reset to factory defaults before decommissioning:

1. Start PCCU.
2. Click the **32-bit loader** icon on the top menu.
3. Connect with the device. The device loader screen displays.
4. Click **Services > Restart using factory configuration** from the device loader toolbar. The device restores the factory configuration and restarts.
5. Exit the device loader.
6. Proceed to decommission the device.



IMPORTANT NOTE: Refer to the device's user manual (see [Additional information](#)) or the Device Loader help topics in the PCCU help files for detailed procedures.

10 Administrator tasks for the device

The procedures in this section are tasks for advanced users or administrators using the MQTT device configuration interface.



IMPORTANT NOTE: Administrator tasks on the MQTT configuration interface require access with the administrator role. Be sure to log in as an administrator. When logged in with the administrator role, the settings (gear) icon should display on the left tool bar on the screen.



IMPORTANT NOTE: Certification generation and management require IT-background and familiarity with authentication methods and certificate generation tools. Administrators must provide configuration parameters and service provider (MQTT broker) details to personnel configuring MQTT-enabled devices.

10.1 Enable or disable MQTT functionality

This procedure enables or disables the MQTT and REST (configuration interface) processes on a device from the PCCU terminal mode. Terminal mode is available in PCCU after connection with the device.

MQTT and REST are processes independent from the Totalflow application. Enabling or disabling them does not require a device restart and does not affect the normal operation of the applications on a device already in service.



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

Disabling MQTT disconnects the device from the MQTT broker and the device is no longer able to update its data on the cloud. The device remains disconnected until MQTT is enabled again.

The device configuration interface is not available with MQTT disabled.

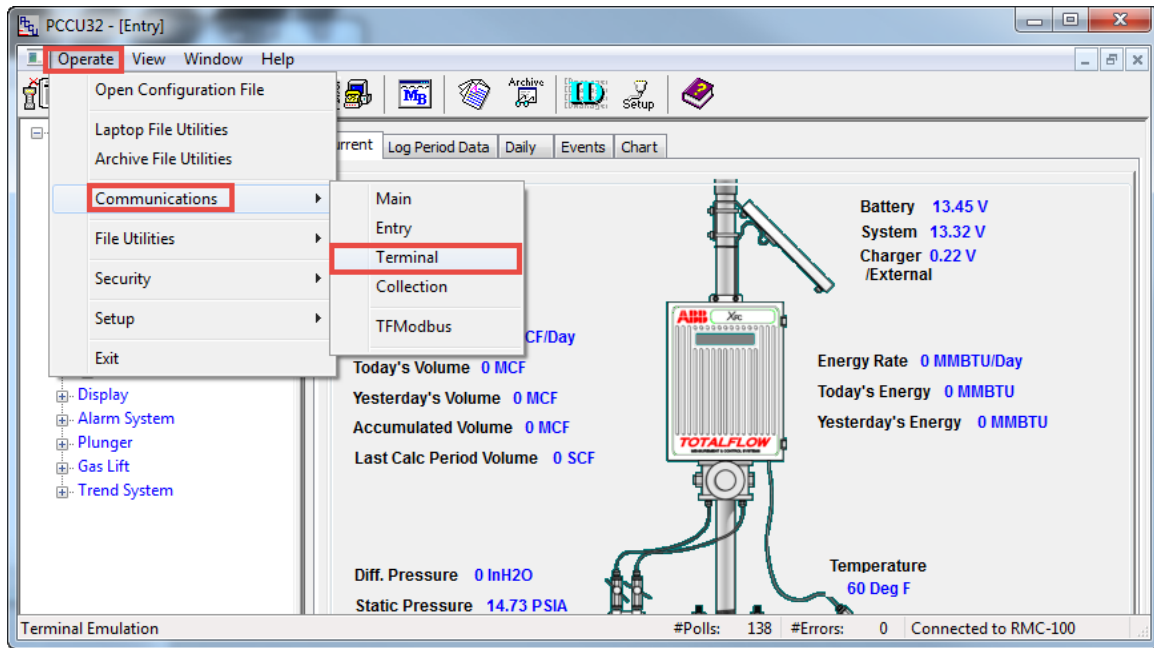


IMPORTANT NOTE: Enabling MQTT and REST server processes does use memory. For security and optimal use of the device resources, enable MQTT only when ready to use it.

Enable or disable the device MQTT functionality from terminal mode:

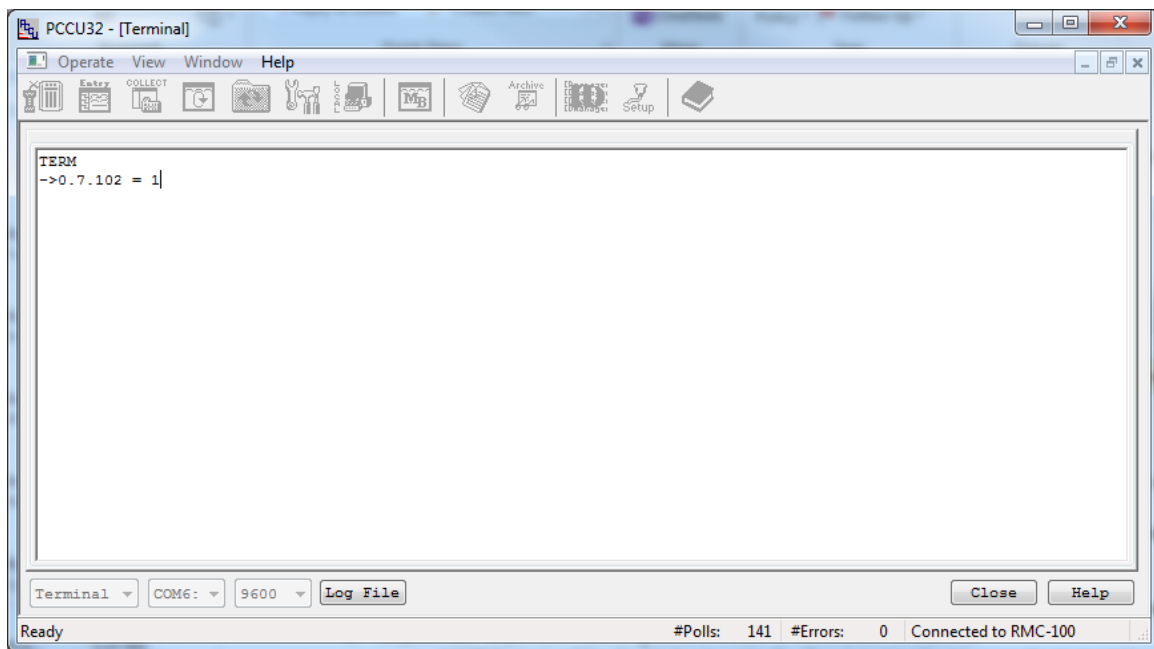
1. Start PCCU.
1. Click the Entry icon to connect with the device.
2. Select **Operate** > **Communications** > **Terminal** from the top menu to go to terminal mode.

Figure 10-1: Access terminal mode on device



3. To enable, type **0.7.102 = 1** at the prompt (Figure 10-2), then press **Enter**.

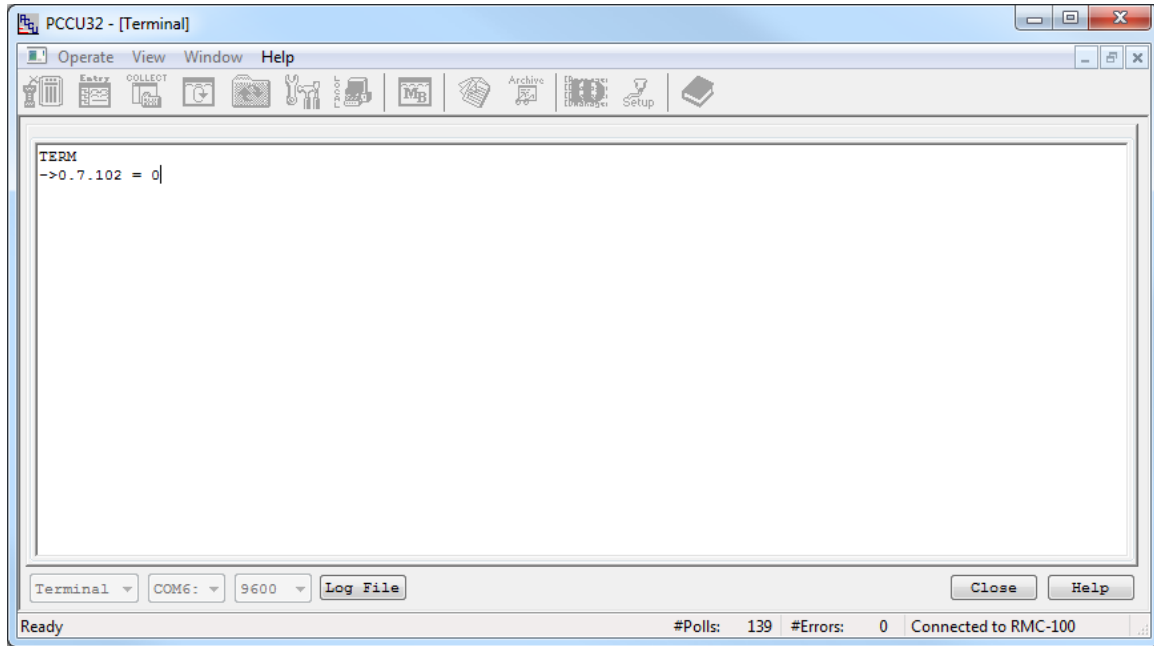
Figure 10-2: Enable MQTT functionality from terminal mode



i **IMPORTANT NOTE:** Devices with a successful connection with the MQTT broker prior to disabling MQTT will reconnect to the broker automatically after MQTT is enabled again. ABB recommends checking the connection status after re-enabling MQTT. See section [3.7 Verify connection status](#).

4. To disable, type **0.7.102 = 0** at the prompt, then press **Enter**.

Figure 10-3: Disable MQTT functionality from terminal mode



5. Click **Close** to end terminal mode session.

i **IMPORTANT NOTE:** When cloud-registered devices disconnect due to disabled MQTT functionality, the connection status indicator shows red ([Figure 10-4](#)).

Figure 10-4: Disconnected device – status indicator



10.2 Provide and manage certificates

Customers are solely responsible for generating or obtaining required certificates for device authentication by MQTT brokers.

Administrators must determine what certificates are required based on their implementation. For information on X.509 certificate generation for service provider brokers such as those by Azure, see section [10.3 Generate certificates for X.509 authentication](#).

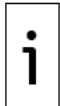
i **IMPORTANT NOTE:** Customers need to provide and manage appropriate certificates for the MOSCA brokers (Auto Refresh certificate).

10.3 Generate certificates for X.509 authentication

Devices connecting to a cloud MQTT broker require unique authentication certificates when configured for the X.509 authentication methods. Each device requires the following certificates:

- Root Certificate: can be common to all devices
- Client Certificate: must be unique to the device
- Client Key: must be unique to the device

Obtain or generate authentication certificates prior to field configuration. Valid certificates must reside on the device before attempting connection to the cloud. Once certificates are generated and available in the system used to configure the device, use the Initial Configuration page to select and copy the certificates to the device. Section [3.5 Configure MQTT Server Details](#).



IMPORTANT NOTE: For details on X.509 certificate generation see the following links: <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-security-x509-get-started>, or <https://github.com/Azure/azure-iot-sdk-c/blob/master/tools/CACertificates/CACertificateOverview.md>

Sections [10.3.2 Generate Self-signed certificates](#) and [10.3.3 Generate CA-signed certificates](#), provide steps to generate client certificates and client keys based on the authentication method supported by the broker. You can also purchase these certificates and the Root Certificate from a root certification authority (CA) (recommended).



IMPORTANT NOTE: Certificate generation is the sole responsibility of the customer. There are several ways, software tools, and systems used to generate certificates. The procedures described in the following sections are used as examples. They may not reflect the exact steps when using other systems or tools.

It is also assumed that the cloud service provider is Azure. For other service providers, refer to their documentation and service specifications. Screens and configuration options on service providers portals may change. Adapt steps to the most current options.

10.3.1 Using OpenSSL in Windows for self-signed certificates

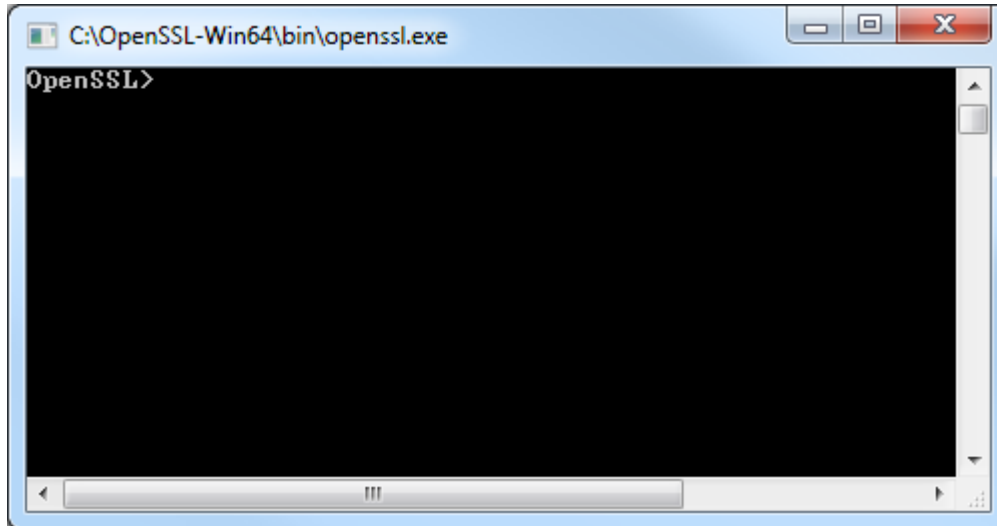
To generate self-signed certificates, you can download OpenSSL into a Windows system. Complete documentation on installing and using OpenSSL is beyond the scope of this document. Search for OpenSSL online resources, tutorials, and download/installation instructions.

OpenSSL can generate certificates and keys on Windows or Linux systems. It is assumed that the software is already successfully installed.

To launch OpenSSL from a system with Windows OS:

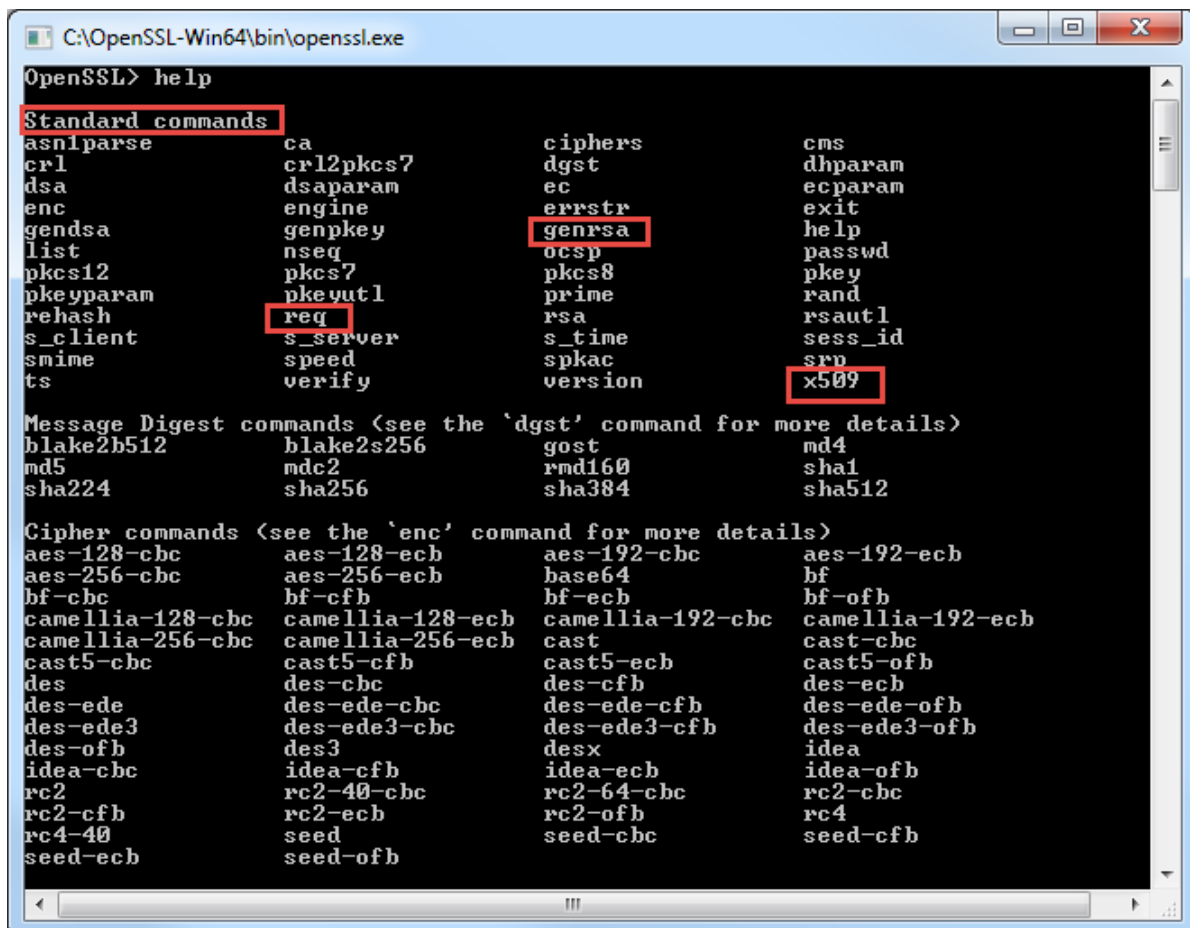
1. Click the Start button in Windows.
2. In the Search programs and files field, type **Openssl**. The OpenSSL command screen displays.

Figure 10-5: OpenSSL windows command line screen



3. To display applicable commands, type **help** at the OpenSSL prompt. A list of commands displays. Some of the commands used in the following procedures display under Standard commands (Figure 10-6).
4. Proceed to generate commands as described in section 10.3.2 [Generate Self-signed certificates](#).

Figure 10-6: Command screen - OpenSSL Standard commands



10.3.2 Generate Self-signed certificates

A self-signed certificate is an identity certificate that is signed by the same entity whose identity it certifies. In technical terms a self-signed certificate is one signed with its own private key.

This procedure uses OpenSSL on Windows to show an example of the process. Adapt instructions to your own systems. Certificate generation commands are issued from the OpenSSL command line screen.

In this procedure, file names for outputs are examples. Customer must follow their name conventions.



IMPORTANT NOTE: For Azure, this is the type of certificate required for the “X.509 Self-Signed” authentication type. If you use this authentication method, be sure to create the certificates before device registration (section [12.2 Register field devices](#)).

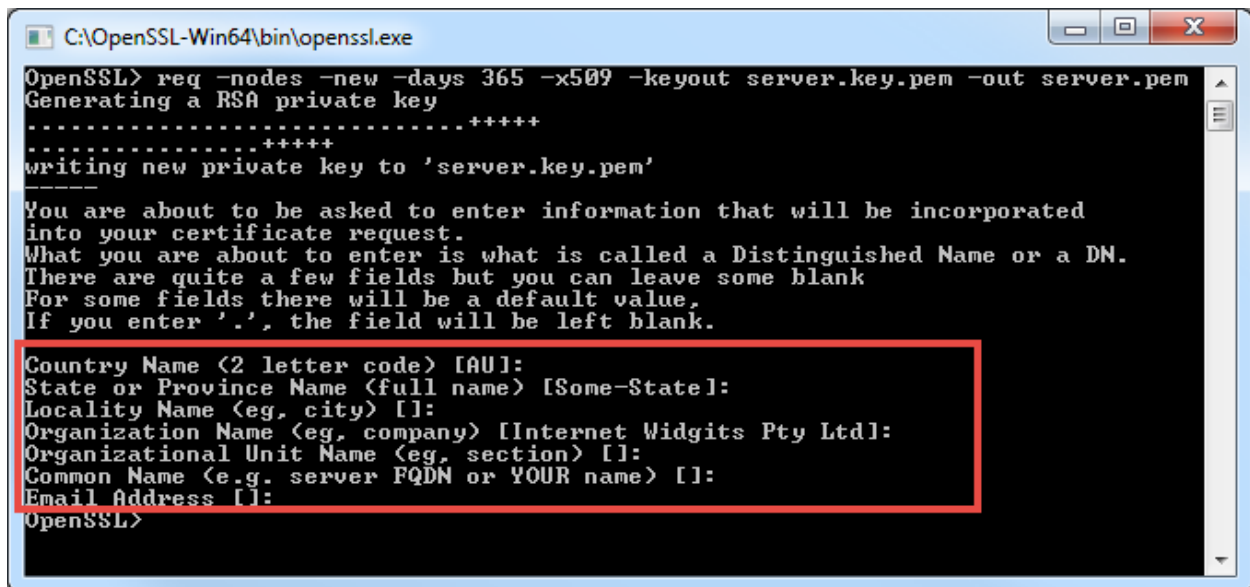
To generate self-signed certificates:

1. Generate certificate and key:
 - a. Type the following command at the prompt:

OpenSSL> req -nodes -new -days 365 -x509 -keyout server.key.pem -out server.pem

- b. Wait while the private key is generated and written into the output file.
- c. When the instructions display, type details as required at each prompt. To leave attributes blank, type a period (.) and press the Enter key.
 - Country Name (2 letter code) [AU]:
 - State or Province Name (full name) [Some-State]:
 - Locality Name (eg, city) []:
 - Organization Name (eg, company) [Internet Widgits Pty Ltd]:
 - Organizational Unit Name (eg, section) []:
 - Common Name (e.g. server QDN or YOUR name) []:
 - Email Address []

Figure 10-7: Additional device information request

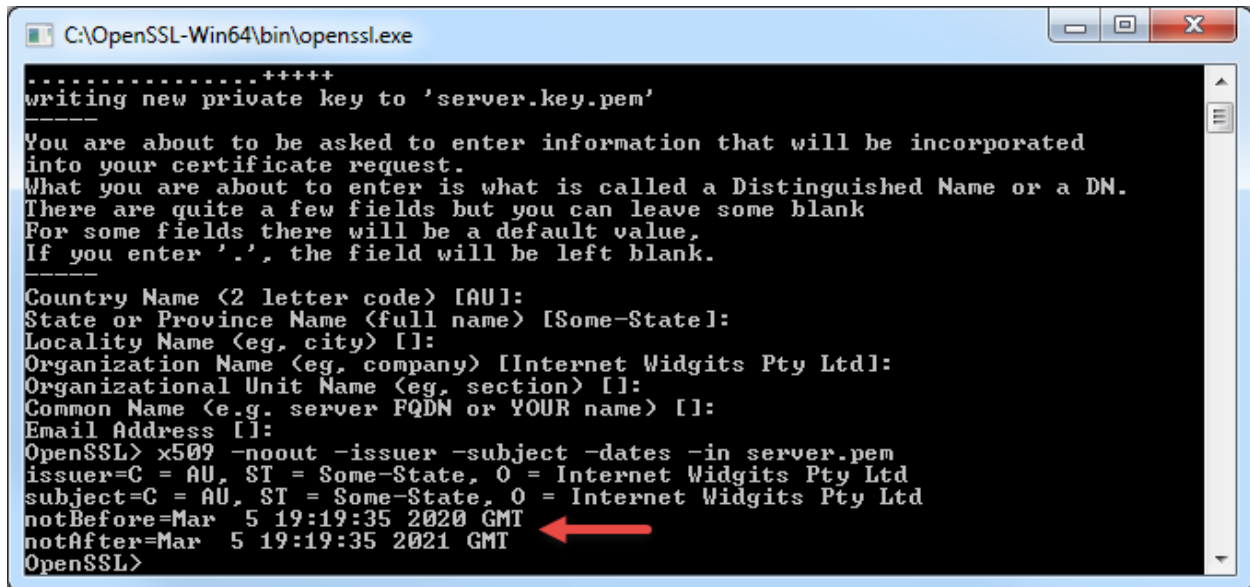


2. Check certificate validity by typing the following command at the prompt:

OpenSSL> x509 -noout -issuer -subject -dates -in server.pem

3. Verify that the previously typed certificate information displays ([Figure 10-8](#)). The time period during which the certificate is valid displays also. In the example shown in [Figure 10-8](#) the certificate displays a validity of a full year as the number of days (-days) option specified 365.

Figure 10-8: Certificate information



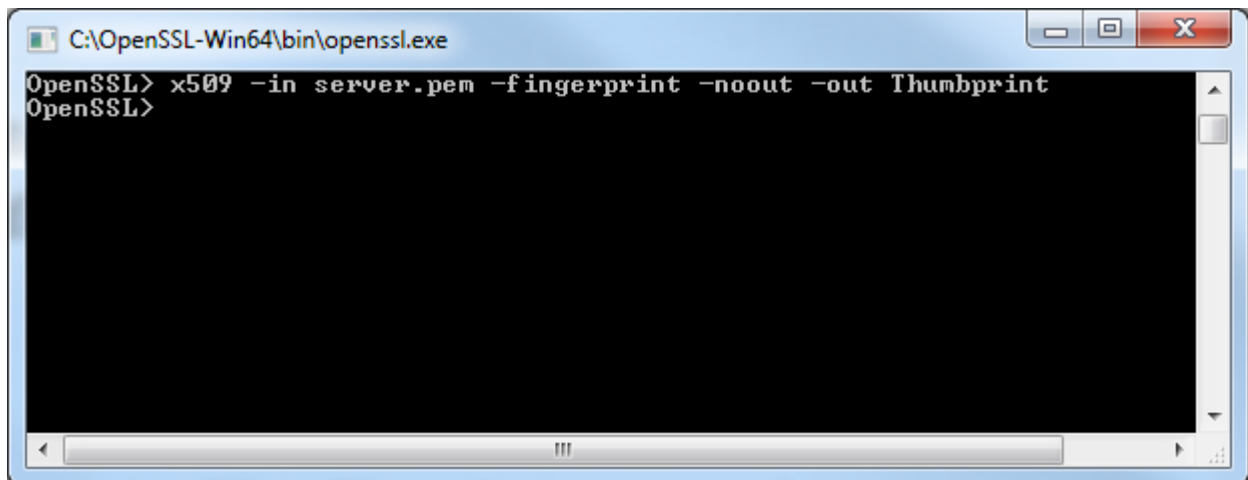
4. Generate the fingerprint of the certificate and copy the fingerprint into a file.

OpenSSL> x509 -in server.pem -fingerprint -noout -out <filename>



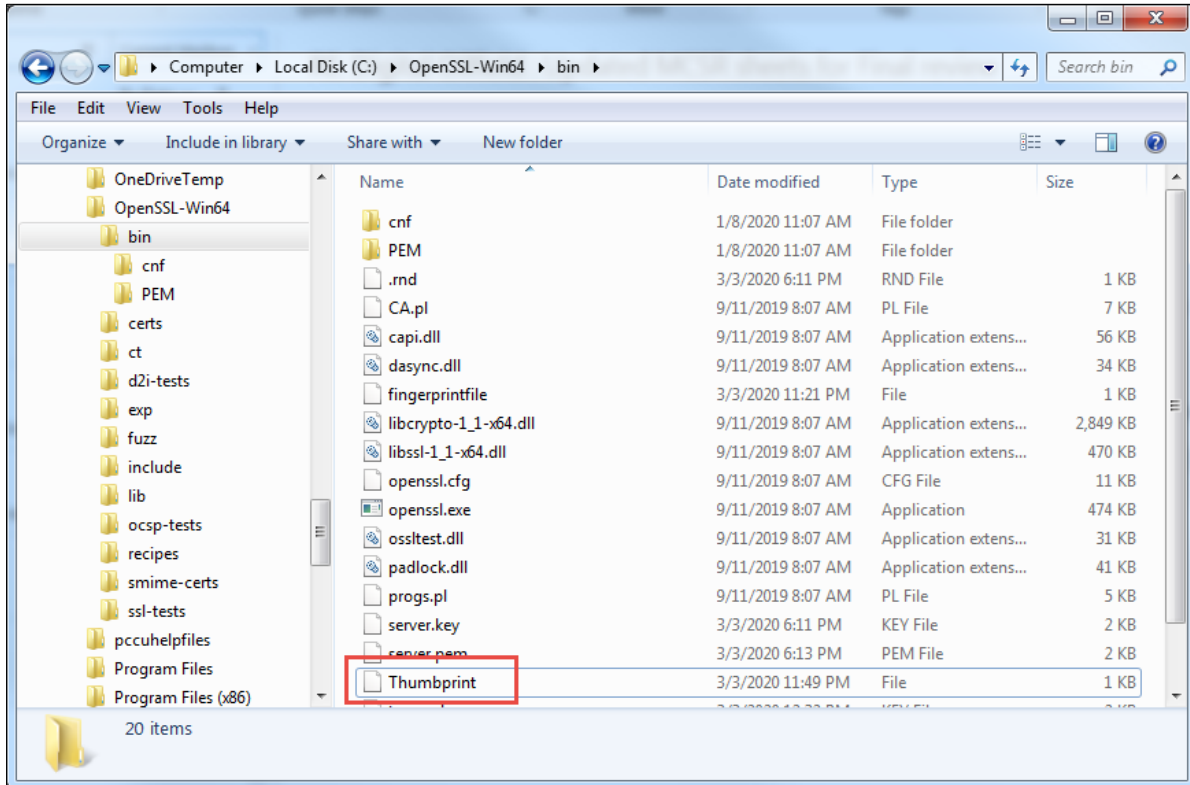
IMPORTANT NOTE: The fingerprint is also referred to as “thumbprint.” The thumbprint is required when using the Azure services and will be requested when registering the device. The command uses the certificate generated earlier as input to extract the fingerprint and generates the output in the specified filename. In the example shown ([Figure 10-9](#)) the filename for the output is “Thumbprint.” If the “-out” option is not used, the fingerprint is displayed on the screen.

Figure 10-9: Generate certificate fingerprint and copy into file



5. Locate the fingerprint file using file manager. OpenSSL saves the generated fingerprint file in its installation directory. If default directories were used for the installation, the file should be in C:\OpenSSL-Win64\bin ([Figure 10-10](#)).

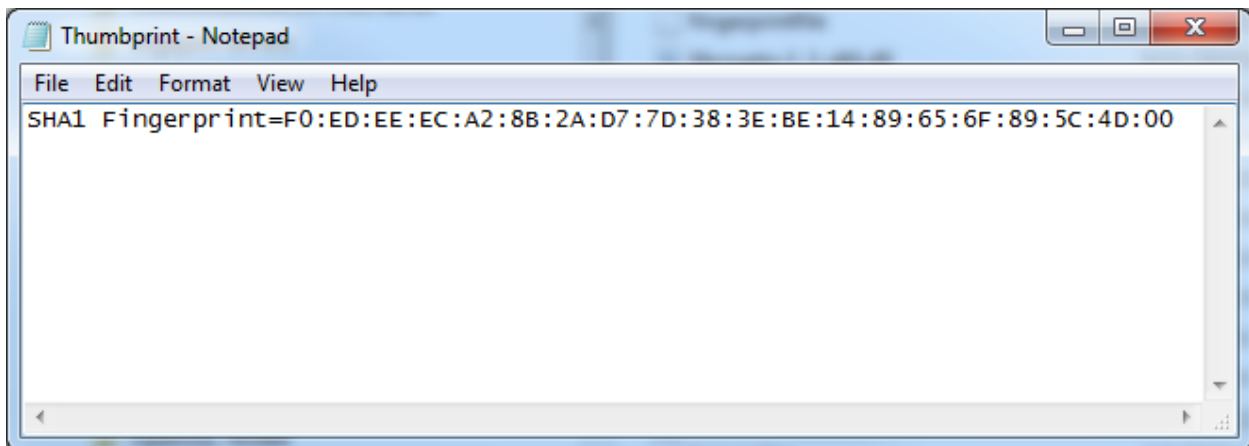
Figure 10-10: Generated fingerprint output file (user-defined filename)



6. Double-click the file. The Open with window displays.
7. Open the file with Notepad or other text editor. The example shown in [Figure 10-11](#) uses Notepad. The fingerprint displays:

SHA1 Fingerprint=F0:ED:EE:EC:A2:8B:2A:D7:7D:38:3E:BE:14:89:65:6F:89:5C:4D:00

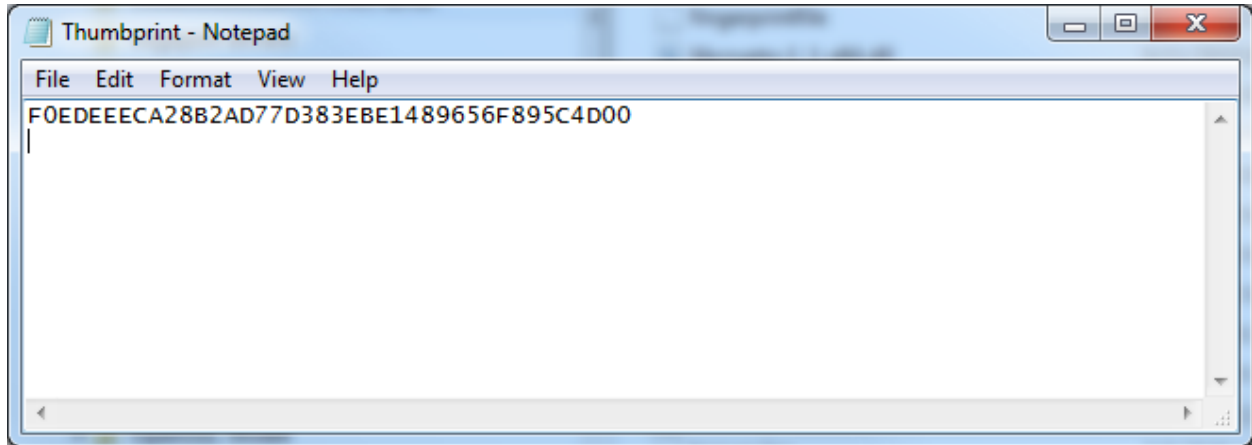
Figure 10-11: Fingerprint contents in output file



8. Remove "SHA1 Fingerprint=" and the colons from the fingerprint. For example, for the fingerprint generated above, the edited fingerprint text should be:

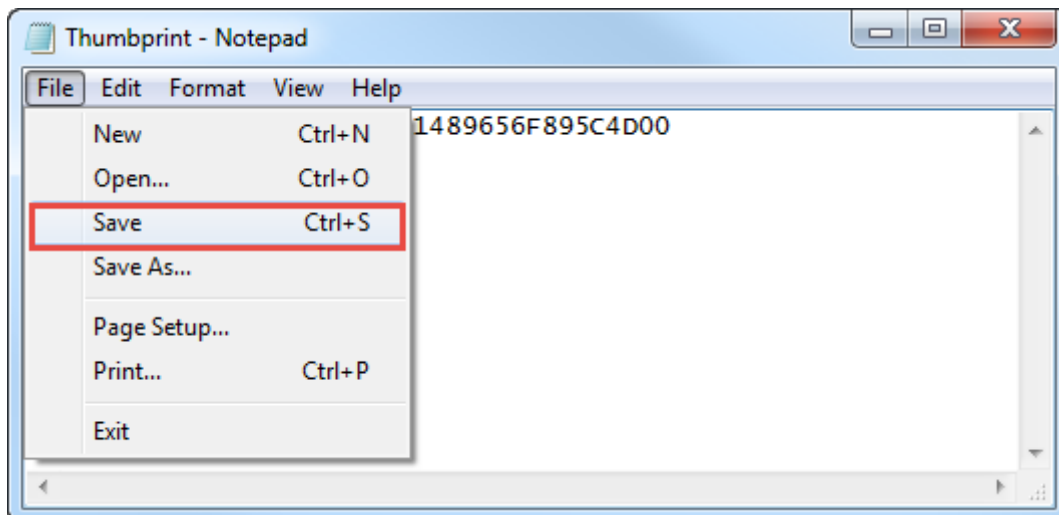
F0EDEEECA28B2AD77D383EBE1489656F895C4D00

Figure 10-12: Edit the generated fingerprint output



9. On the Notepad top menu select **File > Save**. If you wish to save with a different name or in a different directory, select **Save As...** instead. Keep track of where you save the file as you will need to copy the fingerprint into the Azure thumbprint fields when registering the device and configuring its authentication parameters (see section [12.2 Register field devices](#)).

Figure 10-13: Save fingerprint file



10. If you used another system to generate the certificates, copy generated certificate files onto the laptop used to configure the device. The device configuration and connection verification require these files and they should be ready.
11. Copy the generated certificates to the device from the Initial Configuration page as described in section [3.5 Configure MQTT Server Details](#). Use server.pem as client certificate and server.key.pem as client key.
12. Add device and configure X.509 Self-Signed authentication on Azure as described in section [12.2 Register field devices](#).

10.3.3 Generate CA-signed certificates

A certificate authority or certification authority (CA) is an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or on assertions made about the private key that corresponds to the certified public key. A CA acts as a trusted third party—trusted both by the subject (owner) of the certificate and by the party relying upon the certificate. The format of these certificates is specified by the X.509 standard.

There are two 2 types of CA-signed certificates:

- Own Root CA certificate (See section [10.3.4 Generate own root CA certificates](#).)
- Other CA certificates (See section [10.3.5 Generate other root CA certificates](#).)



IMPORTANT NOTE: For Azure, the two types above, are the types of certificates required for the X.509 CA Signed authentication type. If you use this authentication method, be sure to create the certificates before device registration (see section [12.2 Register field devices](#)).



IMPORTANT NOTE: For details on X.509 certificate generation, see the following links: <https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-security-x509-get-started>, or <https://github.com/Azure/azure-iot-sdk-c/blob/master/tools/CACertificates/CACertificateOverview.md>

10.3.4 Generate own root CA certificates

The steps in this section generate two sets of certificate files: one to upload to the Azure IoT hub, the other for the device:

- Certificate generation steps in these sections are performed on a system with Azure-iot-sdk development environment. This environment has built-in scripts to generate certificates such as certGen.sh, a PowerShell script.
- IoT hub certificate upload and verification steps are performed on the Azure cloud.

10.3.4.1 Generate root CA and verification certificate files for the IoT hub

1. At the command prompt, to generate the root CA certificate, type the following:

```
>Run ./certGen.sh create_root_and_intermediate
```

A root CA file is created.

2. On the Azure IoT Hub, upload the root CA file and generate a verification code:
 - a. Select **Certificates**.
 - b. Select **Add** and provide root CA file at the prompt (.\\RootCA.pem in PowerShell and ./certs/azure-iot-test-only.root.ca.cert.pem in Bash.)
 - c. Select the newly added certificate. The Certificate Details display.
 - d. On the Certificate Details pane, select **Generate verification Code**. Azure generates a character string or code that will be used to create a verification certificate. Copy the code and use as the argument to the command in step 3 (verification certificate generation).
 - e. Keep the Certificate Details pane open.
3. At the command prompt, to generate a verification certificate, type the following including the verification code just obtained from Azure:

```
>Run ./certGen.sh create_verification_certificate  
106A5SD242AF512B3498BD6098C4941E66R34H268DDB3288
```

The script will output the name of the file containing:
"CN=106A5SD242AF512B3498BD6098C4941E66R34H268DDB3288" to the screen.

4. In the Certificate Details pane, upload the verification certificate file to the IoT hub.
 - a. Click the browse icon next to the "Verification Certificate .pem or cer file" field.
 - b. Locate and select the verification certificate.
 - c. Click **Open** to upload.
 - d. Select **Verify**.
5. Add device and configure X.509 CA Signed authentication on Azure as described in section [12.2 Register field devices](#).

10.3.4.2 Generate certificate files for the device

This procedure generates the certificates files for the devices.



IMPORTANT NOTE: If you're using this certificate as a DPS registration ID, the ID must use lowercase letters, or the server will reject it.

To generate:

1. At the prompt, create the new device key certificate files by typing the following command (identify the device in the file name; for example, the device to generate the certificate for is "new-device"):

```
>Run ./certGen.sh create_device_certificate new-device
```

This command creates the following files (path to files shown):

- ./certs/new-device.* which contains the public key and PFX
 - ./private/new-device.key.pem which contains the device's private key
2. Type the following command to generate the client certificate file (this command concatenates intermediate and root certificates):

```
>cd ./certs && cat new-device.cert.pem azure-iot-test-only.intermediate.cert.pem azure-iot-test-only.root.ca.cert.pem > new-device-full-chain.cert.pem
```

3. If you used another system to generate the certificates, copy generated certificate files onto the laptop used to configure the device. The device configuration and connection verification require these files and they should be ready.
4. Copy the generated certificates to the device from the Initial Configuration page as described in section [3.5 Configure MQTT Server Details](#). Use new-device-full-chain.cert.pem as client certificate and new-device.key.pem as client key.

10.3.5 Generate other root CA certificates

Certificate generation steps in these sections are performed on a system with Azure-iot-sdk development environment.

To generate:

1. Create Root key, type the following command at the prompt:

```
>openssl genrsa -out rootCA.key 4096
```

2. Create and self-sign the Root Certificate:

```
>openssl req -x509 -new -nodes -key rootCA.key -sha256 -days 1024 -out rootCA.pem
```

- a. Create new root certificate in the Azure portal.
 - b. Upload rootCA.pem as root certificate.
 - c. Verify the certificate. Generate verification Code.
3. Create a verification certificate:

- a. Type the following commands:

```
>openssl genrsa -out mydomain.com.key 2048
```

```
>openssl req -new -key mydomain.com.key -out mydomain.com.csr
```

(pass common name as verification code from azure portal)

```
>openssl x509 -req -in mydomain.com.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial -out mydomain.com.pem -days 500 -sha256
```

- b. Upload mydomain.com.pem as verification certificate
4. Generate device certificate
- a. Create device key, type the following command:

```
>openssl genrsa -out Dev_ORCA.key.pem 2048
```

5. Create certificate sign request, type the following:

```
>openssl req -new -key Dev_ORCA.Key.pem -out Dev_ORCA.key.csr
```

- a. Create device certificate, type the following:

```
>openssl x509 -req -in Dev_ORCA.key.csr -CA rootCA.pem -CAkey rootCA.key -CAcreateserial
```

-out Dev_ORCA.pem -days 500 -sha256

6. If you used another system to generate the certificates, copy generated certificate files onto the laptop used to configure the device. The device configuration and connection verification require these files and they should be ready.
7. Copy the generated certificates to the device from the Initial Configuration page as described in section [3.5 Configure MQTT Server Details](#). Use Dev_ORCA.pem as client certificate and Dev_ORCA.key.pem as client key.
8. Configure X.509 CA Signed authentication on Azure as described in section [12.2 Register field devices](#).

10.4 Manage users

Totalflow devices support role-based access control (RBAC) on the device configuration user interface. Configure users and roles from the User Management web page.

Totalflow devices store the defined users and their credentials in an encoded file (SHA-1 storage).



IMPORTANT NOTE: The user management web page is available only for users with the admin role. To complete the procedures in this section, you must log into the device as an administrator.

Define users and their roles on each device.



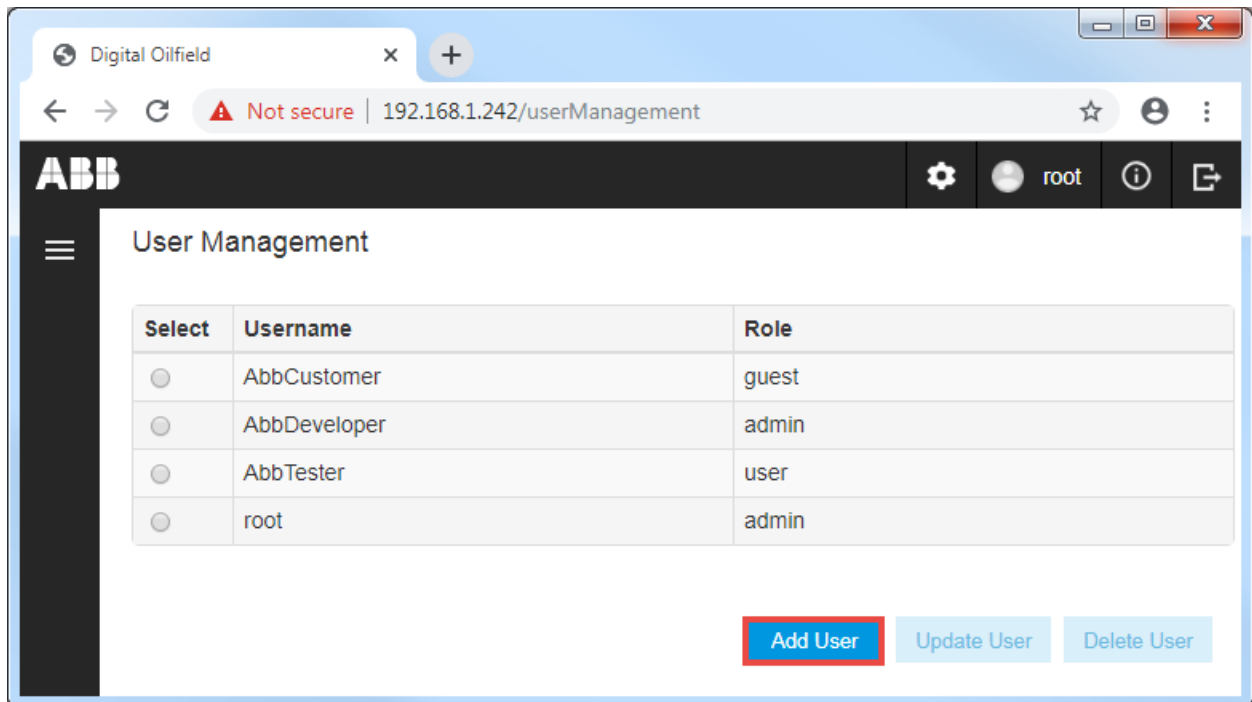
IMPORTANT NOTE: Users defined in this section access the device configuration interface for MQTT operation. These users are different from those defined for device access using PCCU.

10.4.1 User Management web page overview

The User Management web page ([Figure 10-14](#)) is available to define and control access to the Totalflow device for MQTT configuration. The page displays the users that have access to the device and their assigned role. The role determines the access level granted upon login.

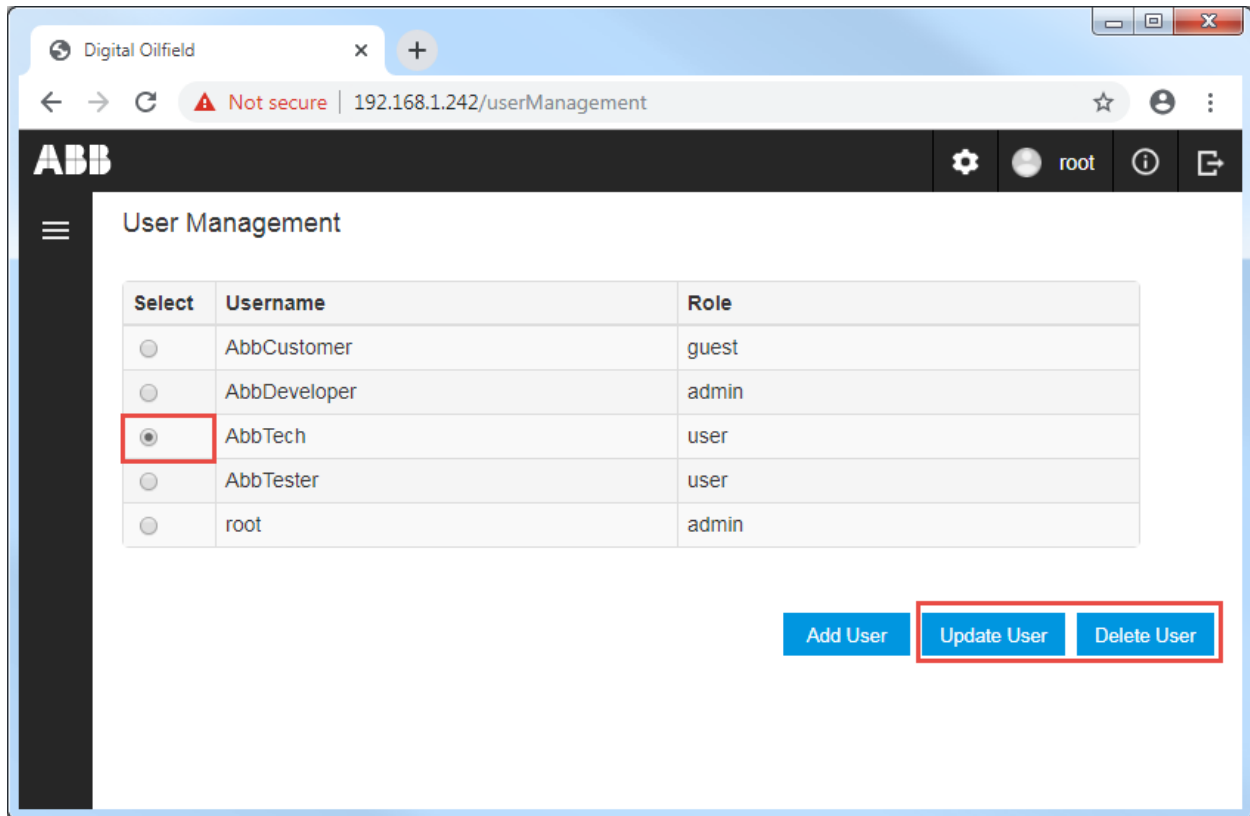
Function buttons to add, update and delete users are available. The Add User button is active as soon as the page displays.

Figure 10-14: User Management web page (for admin role only)



The Update User and Delete User buttons activate after you select a user ([Figure 10-15](#)).

Figure 10-15: Select existing user



10.4.2 Default user accounts and role privileges

[Table 10-1](#) lists the default users, roles, and credentials in the MQTT-enabled Totalflow device.

i **IMPORTANT NOTE:** Change factory default passwords to private passwords at first-time login. Do not leave devices with default passwords after installation and commissioning or after flash upgrade to MQTT-enabled flash. Be sure to set strong passwords. The device enforces strong password attributes: it ensures the password is within the minimum and maximum password length and allows the use of special characters, numbers, upper- and lower-case letters, etc.

Table 10-1: Default user accounts on device

User Name	Role	Password
AbbCustomer	guest	root@123
AbbDeveloper	admin	root@123
AbbTester	user	root@123
root	admin	root@123

[Table 10-2](#) lists roles and access levels available on the Totalflow device.

Table 10-2: Role privileges on device

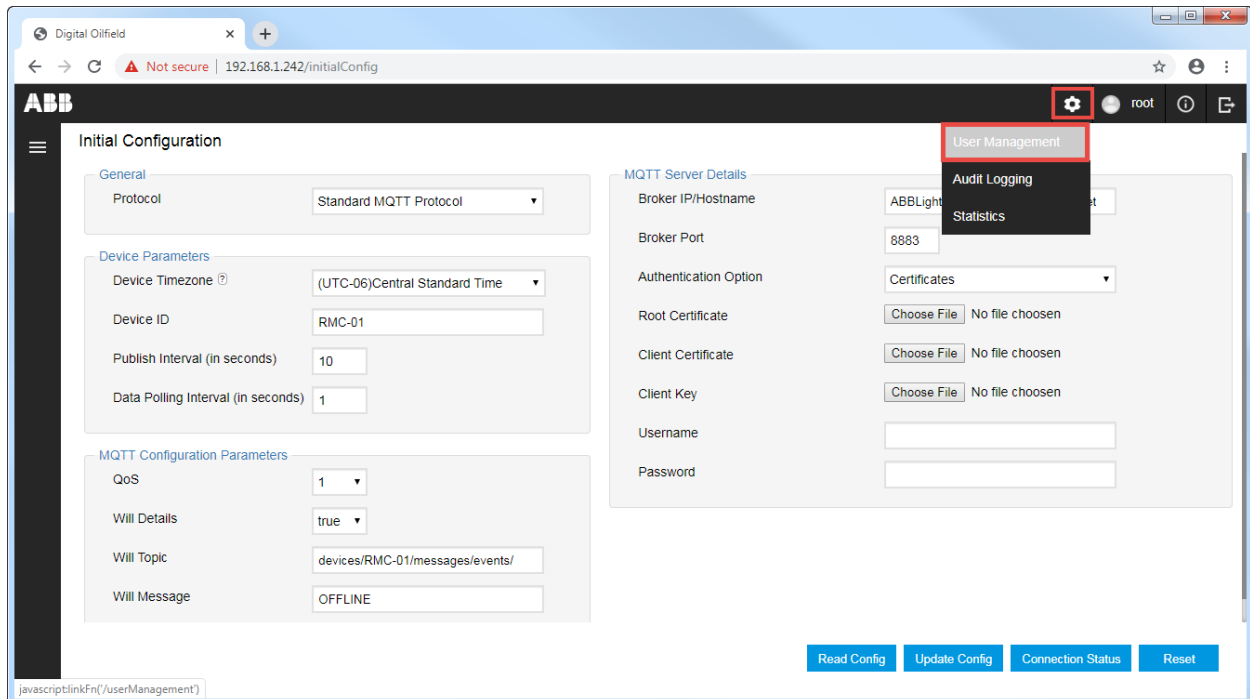
Role	Access level	Description
admin	Read and write (update) Manage users: add, delete or update users	The admin role has the following privileges: <ul style="list-style-type: none"> – View (read) and update device parameters (if applicable) in all device configuration pages (Initial, Application and Register configurations pages) – Add new users, delete existing users and update user attributes in the device’s User Management page – Access the device Audit Logging and Statistics pages
user	Read and write (update/edit)	The user role has the following privileges: <ul style="list-style-type: none"> – View (read) and update device parameters (if applicable) in all device configuration pages (Initial, Application and Register configurations pages) – Access the device Audit Logging and Statistics pages
guest	Read-only access	The guest has minimum privileges: <ul style="list-style-type: none"> – View (read) device parameters in all device configuration pages (Initial, Application and Register configurations pages)

10.4.3 Access the User Management web page

To access the User Management page:

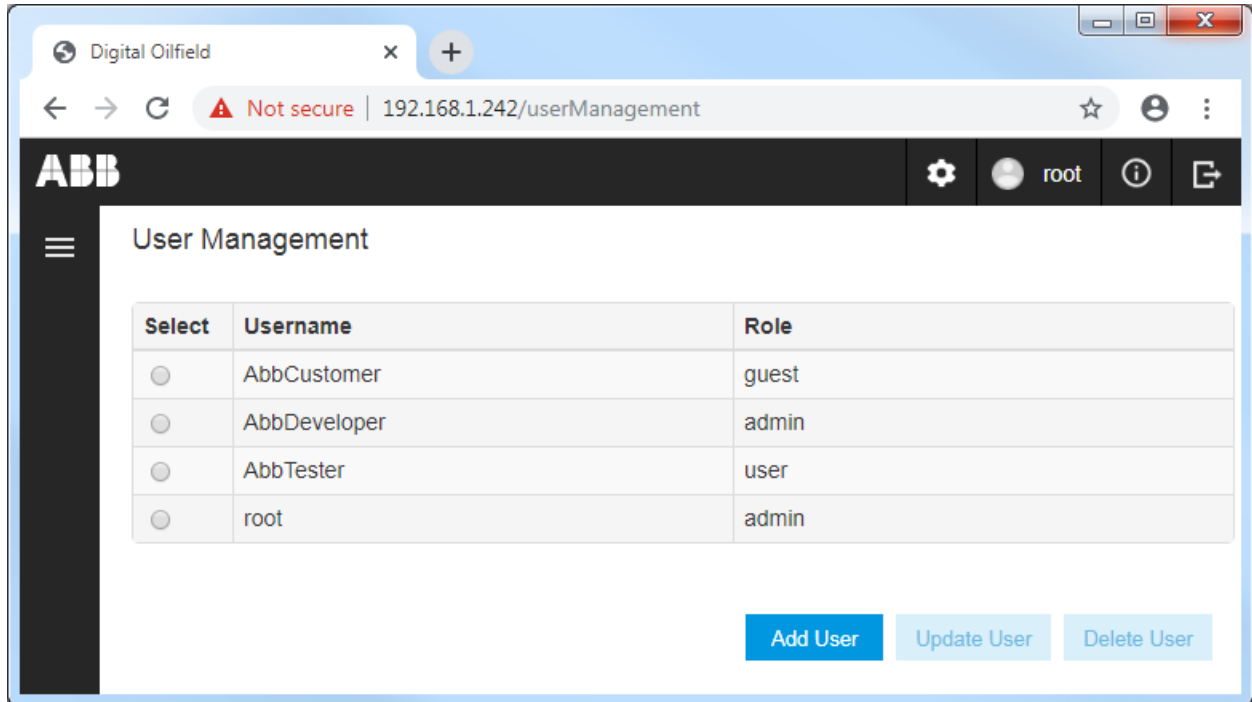
1. Navigate to the Initial Configuration page.
2. Click the settings icon and then **User Management** from the drop-down list (Figure 10-16).

Figure 10-16: Access the User Management web page



The User Management web page displays (Figure 10-17).

Figure 10-17: User Management web page

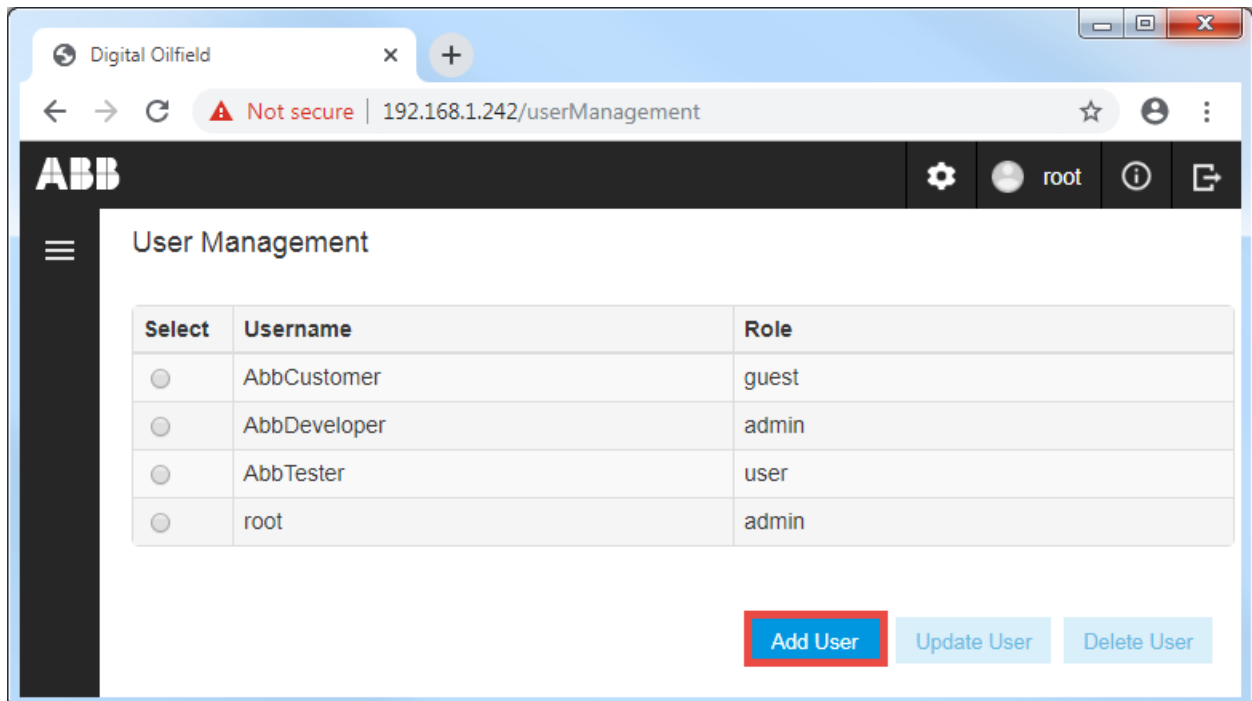


10.4.4 Add User

Add additional users to the defined defaults:

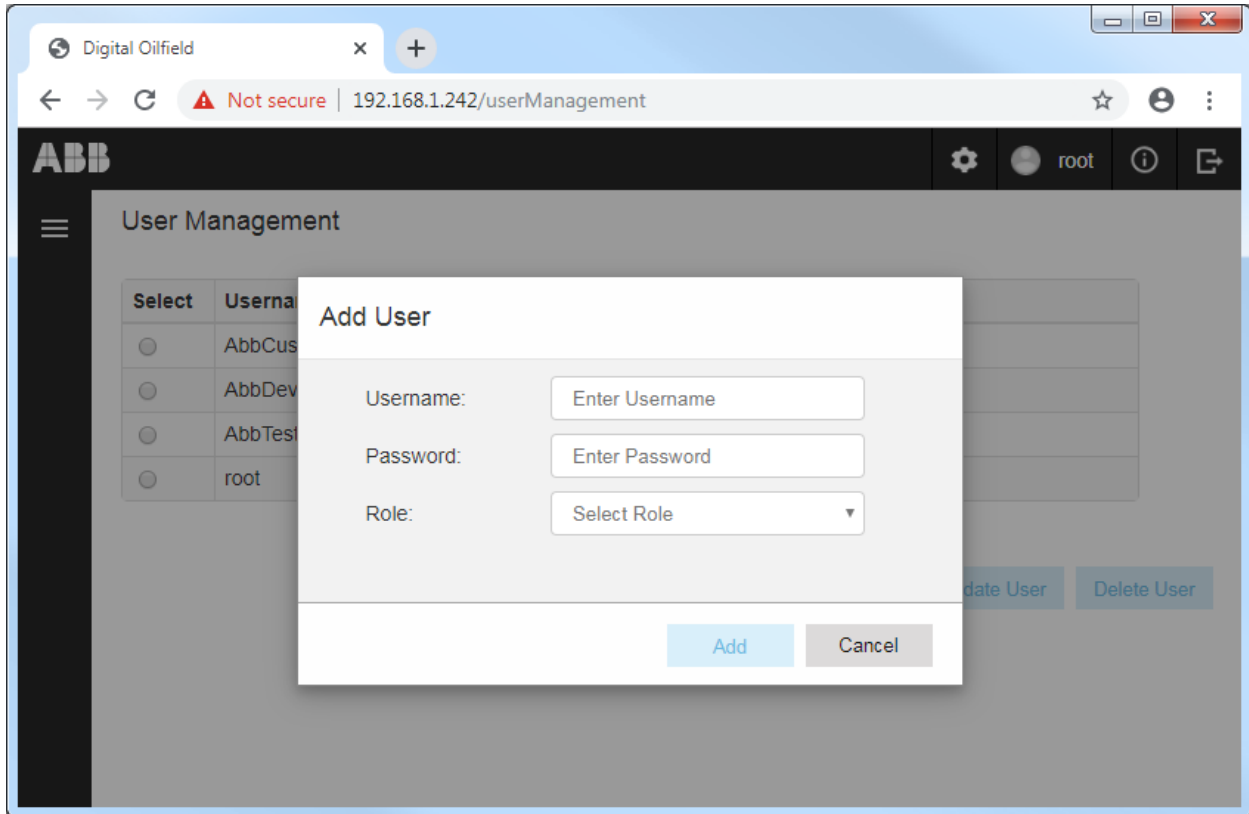
1. Click **Add User** on the User Management web page.

Figure 10-18: Add new user



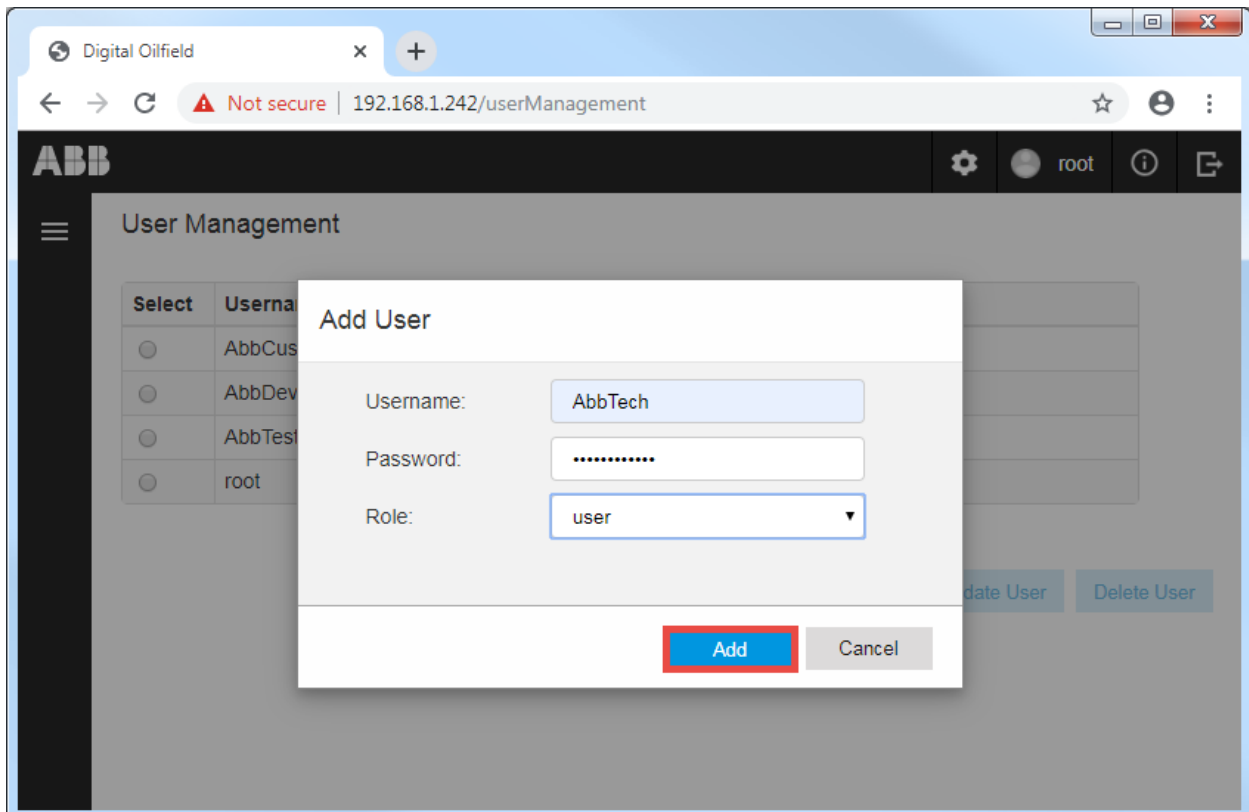
The Add User dialog displays.

Figure 10-19: Add User dialog box



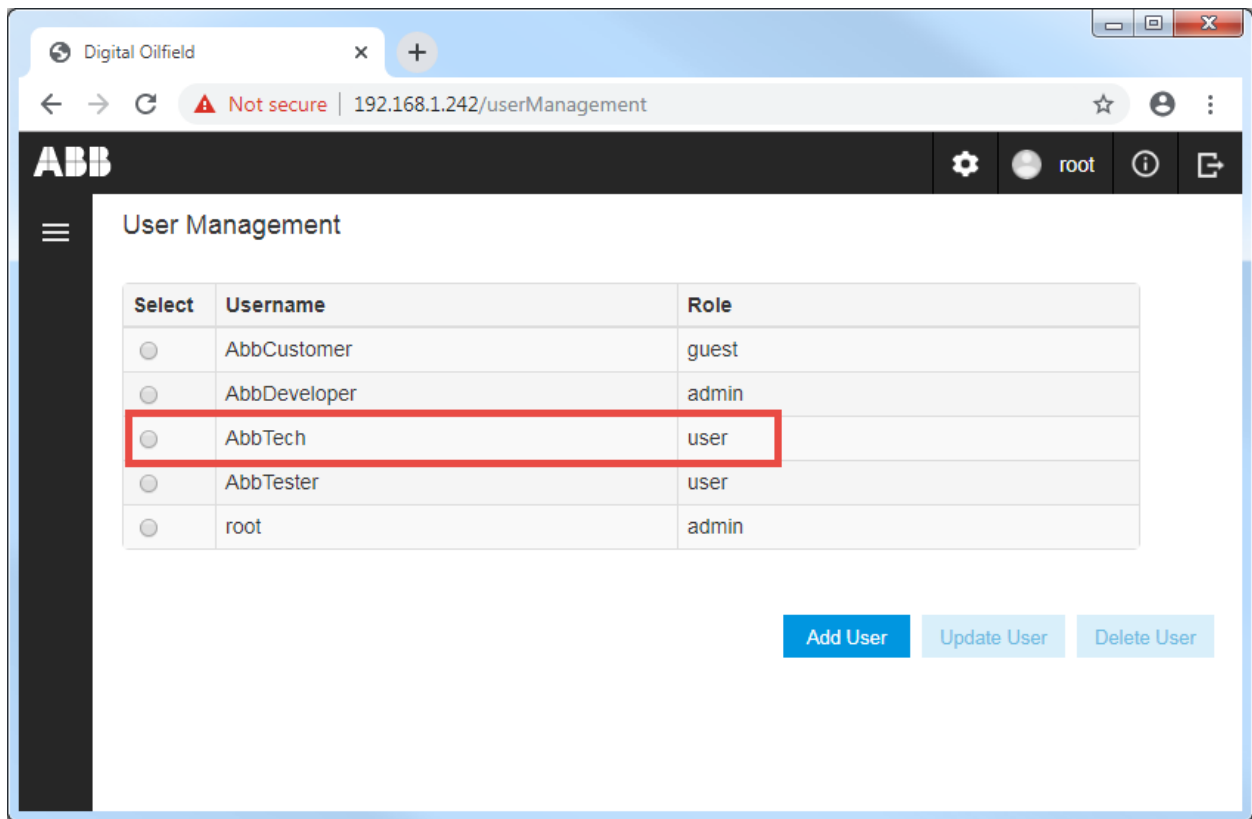
2. Type credentials.
3. Select the Role from the drop-down menu and click **Add** (Figure 10-20). In this example, the new user "AbbTech" is assigned the "user" role.

Figure 10-20: Add new user credentials and role



4. Verify that the new user displays in the list

Figure 10-21: Verify new user



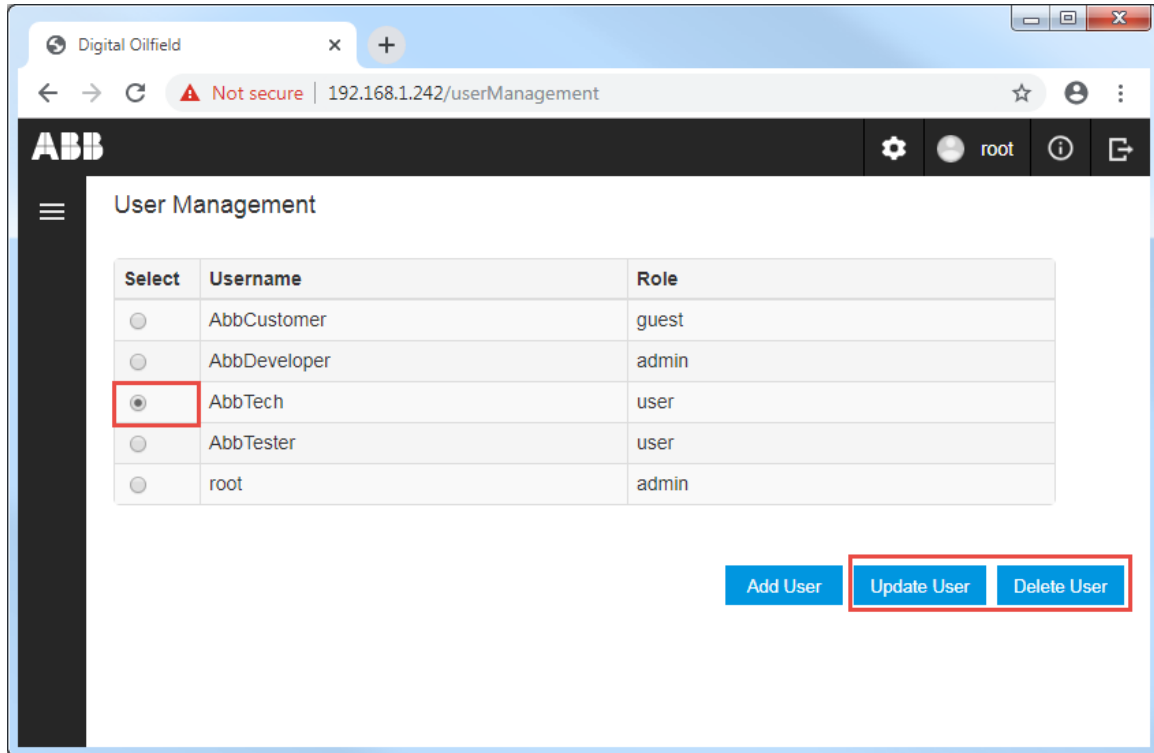
10.4.5 Update User

The Update User function allows the change of the password or role assigned to an existing user. Username change is not supported. To create the same account with a different name, delete the user and create the account with the correct name.

To update an existing user account:

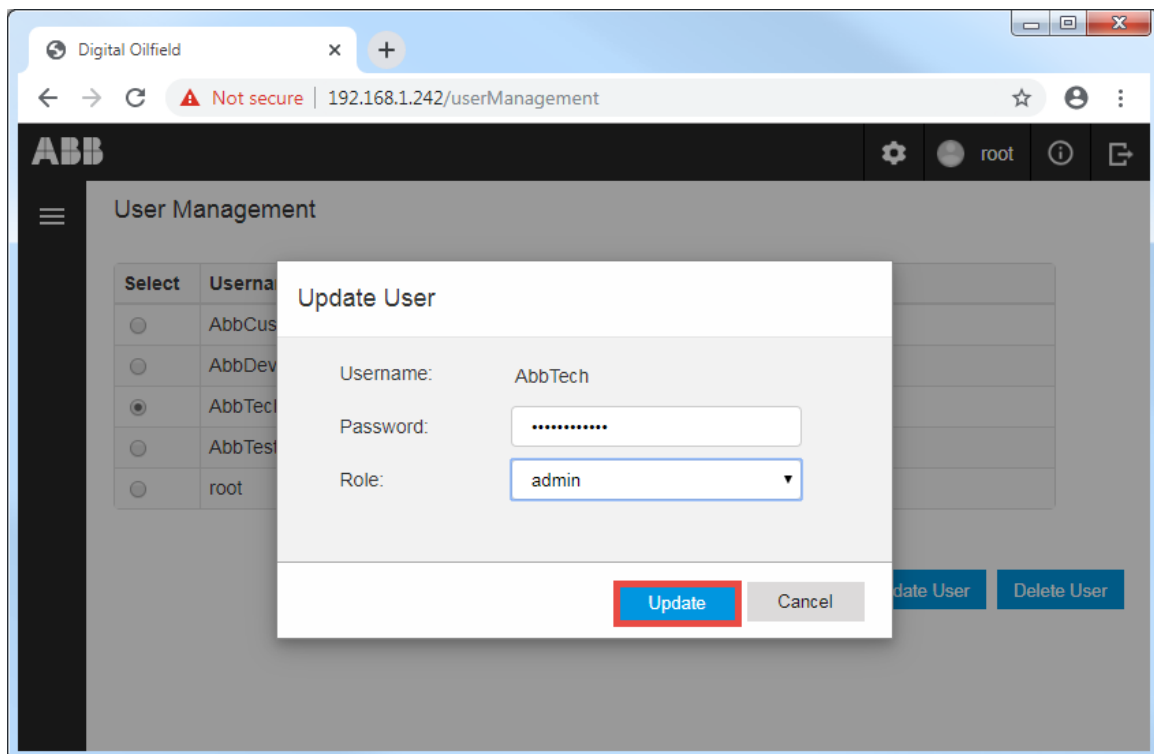
1. Select the user from the list on the User Management web page. The Update User and Delete User buttons activate.

Figure 10-22: Select existing user to update



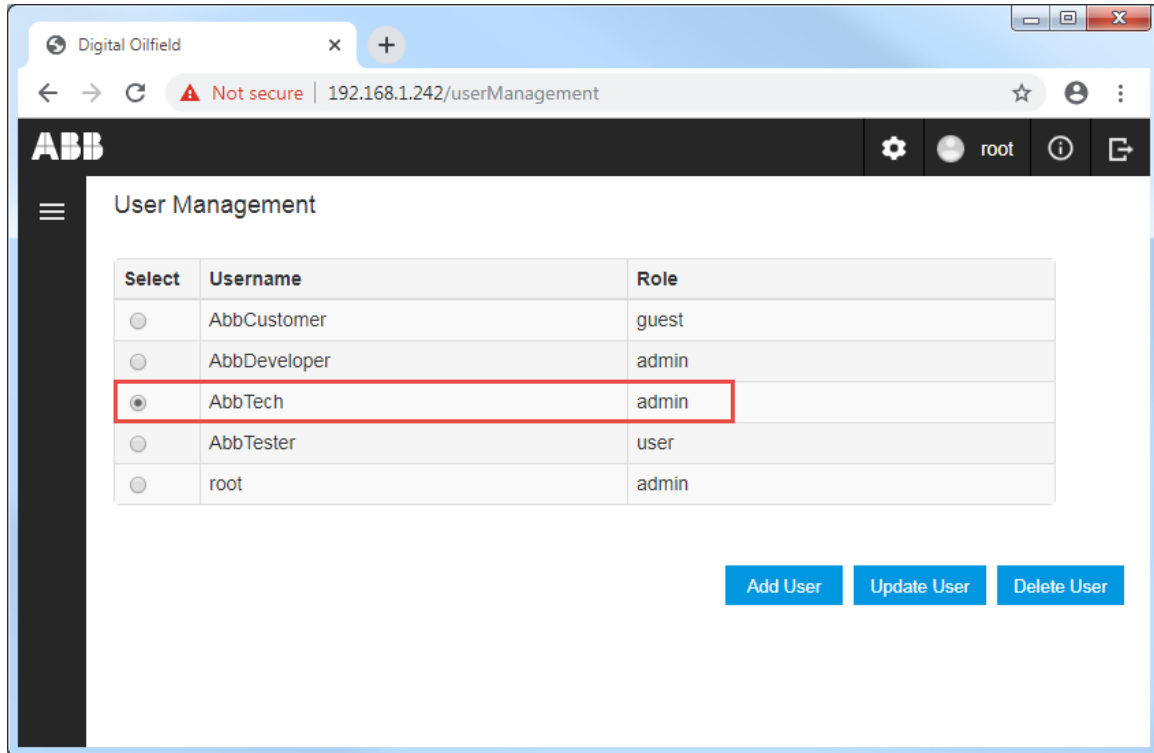
2. Click **Update User**.
3. Update the password or role at the Update User dialog box ([Figure 10-23](#)). In this example the password is the same, but the role is updated from "user" to "admin".
4. Click **Update**.

Figure 10-23: Update password or role for an existing user



5. Verify the update in the User Management page ([Figure 10-24](#)).

Figure 10-24: Verify existing user update



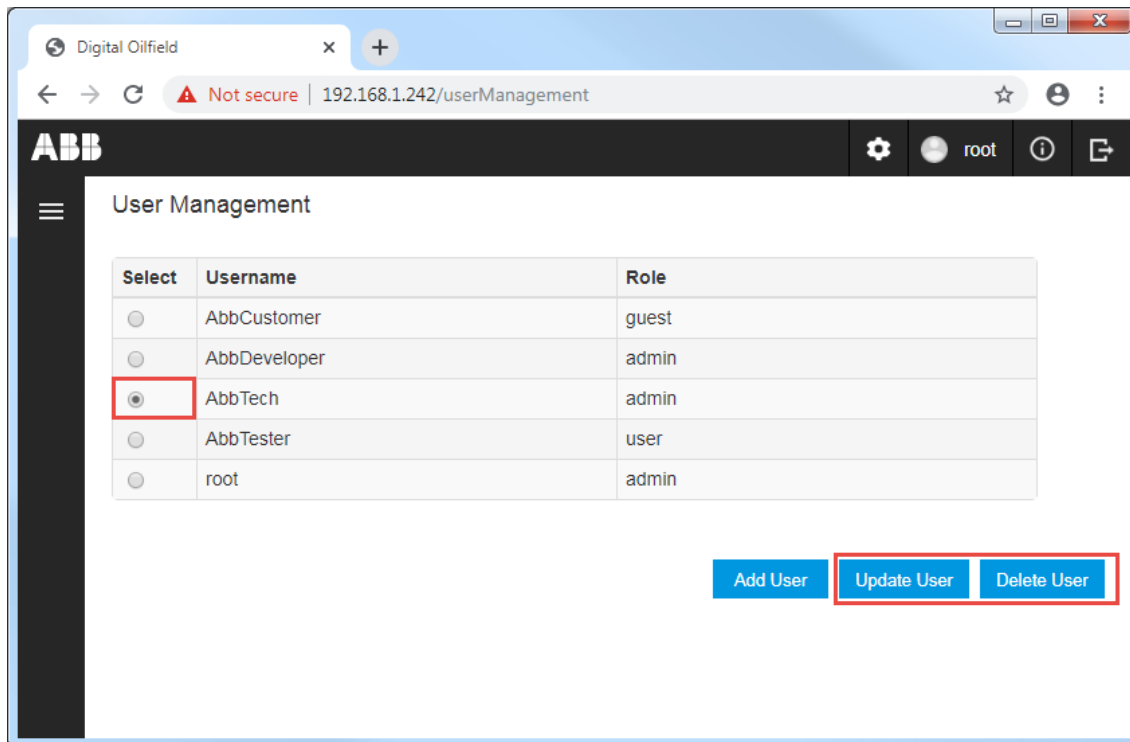
10.4.6 Delete User

The Delete User function removes an existing user.

To delete a user:

1. Select the user from the list on the User Management web page ([Figure 10-25](#)). The Update User and Delete User buttons activate.

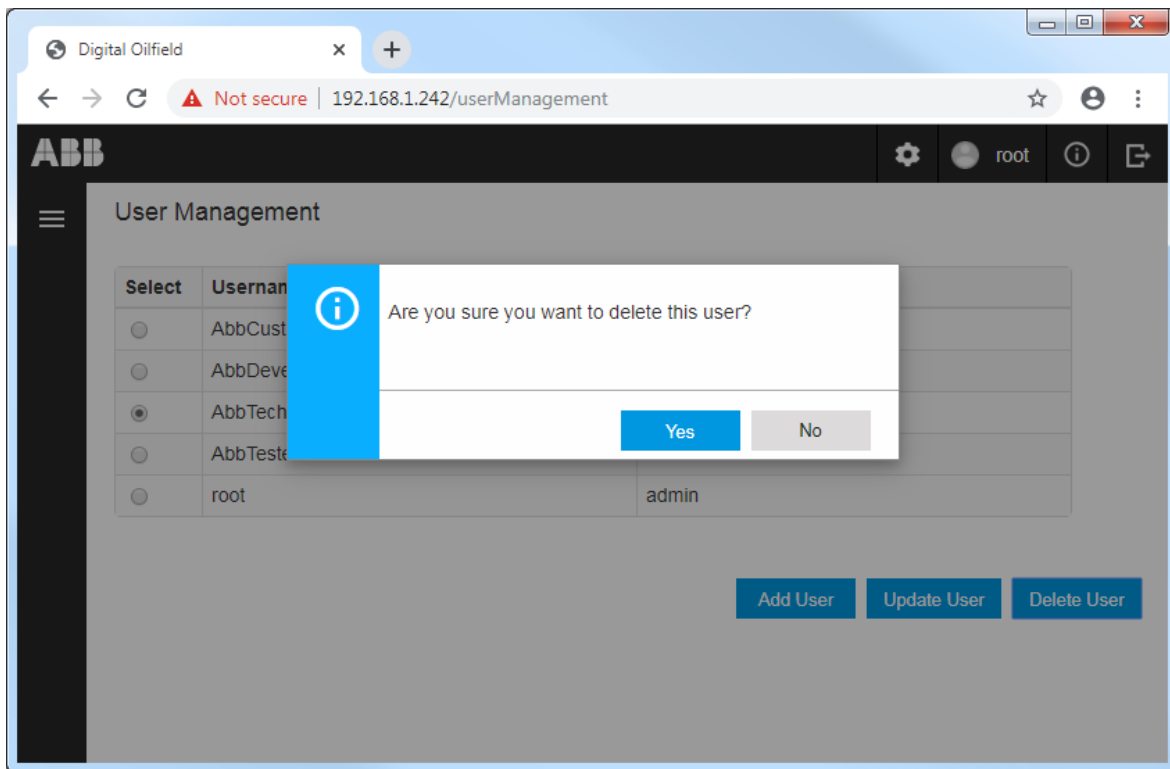
Figure 10-25: Select user to delete



2. Click **Delete User**.

3. Click **Yes** when prompted to confirm ([Figure 10-26](#)).

Figure 10-26: Confirm message to delete existing user



4. Verify that the user no longer displays in the User Management page.

10.5 Monitor device audit logs



IMPORTANT NOTE: Access to the Audit Logging web page is available for user and admin roles.

10.5.1 Audit Logging web page overview

The Audit Logging web page displays device configuration update activity ([Figure 10-27](#)). The logs record the parameter change and its value before (old) and after (new) the update. Each log has a time stamp and records the user and role at the time of the update.

The device stores up to 100 logs. When the number of logs reaches this limit, the device overwrites the older logs to continue to store and display the most current information.

Figure 10-27: Audit Logging web page

TimeStamp	S.No	Username	Role	Request Type	Old Value	New Value	Req. Status
11/10/2019 11:19:46 AM	7	root	admin	Update Register Configuration	InstanceName:AGA3-1 model:Aggregate	InstanceName:AGA3-1 model:Aggregate	Success
11/08/2019 12:41:43 PM	6	root	admin	Update Application Configuration	AGA-7 Measurement:Disable Plunger Control:Disable	AGA-7 Measurement:Enable Plunger Control:Enable	Success
11/08/2019 12:40:52 PM	5	root	admin	Update Register Configuration	InstanceName:AGA3-1 model:Aggregate	InstanceName:AGA3-1 model:Aggregate	Success
11/08/2019 12:37:35 PM	4	root	admin	Update Application Configuration	AGA3-2 :Disable	AGA3-2 :Enable	Success
11/08/2019 12:35:05 PM	3	root	admin	Update Application Configuration	API Liquid SU:Disable	API Liquid SU:Enable	Success
11/08/2019 12:31:54 PM	2	root	admin	Update Application Configuration	AGA-7 Measurement:Enable Plunger Control:Enable	AGA-7 Measurement:Disable Plunger Control:Disable	Success
11/05/2019 09:27:50 AM	1	root	admin	Update Initial Configuration	TimeZone:330 Device_Id:RMCPinyonSite	TimeZone:-360 Device_Id:RMC-01	Success

[Table 10-3](#) describes the attributes on the audit logging page.

Table 10-3: Device audit logging parameter description

Field	Description	Values
Time Stamp	Date and time of the update by the logged-in user	Date and time match the date and time kept by the device
S. No	Serial number of the audit log	Logs are numbered sequentially with decimal numbers beginning at 1 for the first log. Serial numbers do not restart when the number of logs reaches its limit of 100.
Username	Identifies the logged-in user at the time of the update	Any user already defined in the User Management web page
Role	Identifies the role of the logged-in user	Role assigned to logged-in user (admin, user, guest)
Request type	Identifies the device configuration page that the update originated from	Update Initial Configuration Update Application Configuration Update Register Configuration Reset Statistics
Old Value	Name and value of parameter or configuration option prior to the update request from the logged-in user	Values applicable to the parameter type Values might be user-defined or selected from drop-down menus.
New Value	Name and value of parameter or configuration option after the device completes update request by the logged-in user	Values applicable to the parameter type Values might be user-defined or selected from drop-down menus.

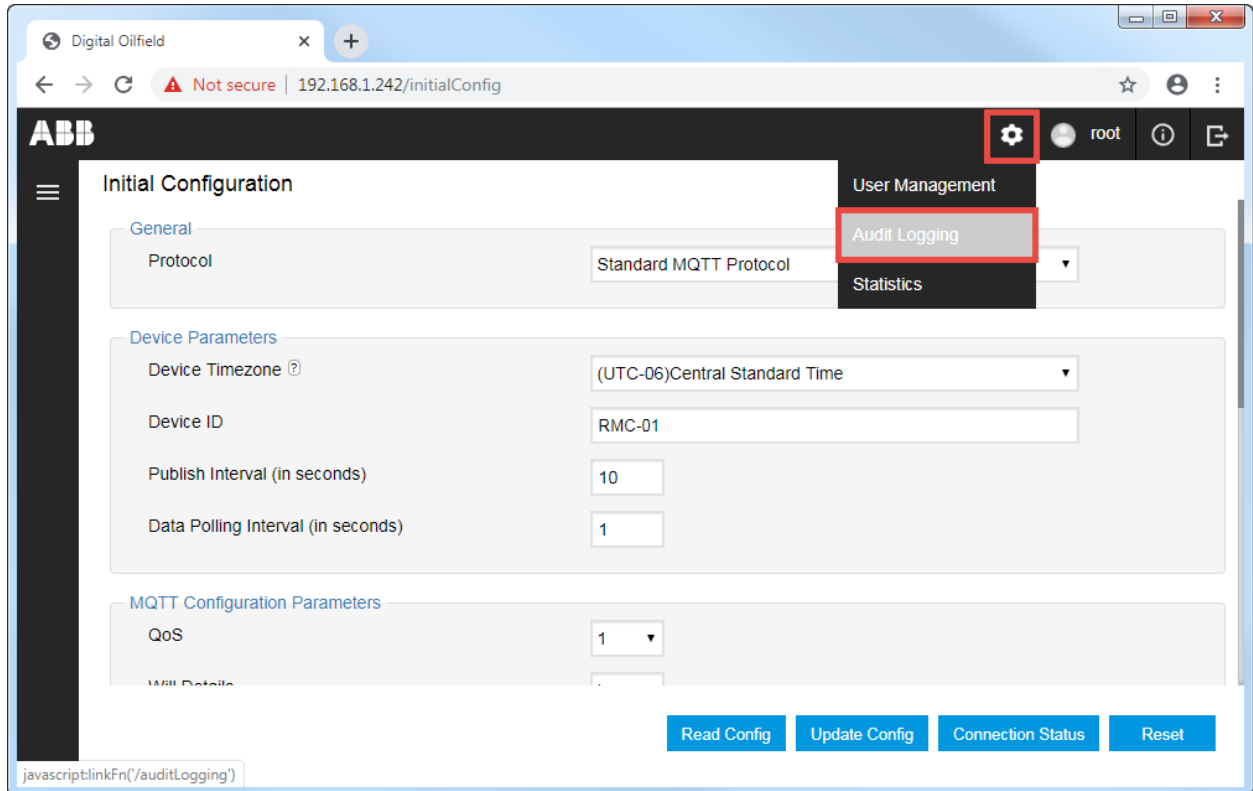
Field	Description	Values
Re. Status	Request Status Indicates the status of the update request by the logged-in user	Success – The update request message is validated and is being applied by software. Failure - The update request message validation has failed.

10.5.2 Access the Audit Logging web page

To access the audit logging page:

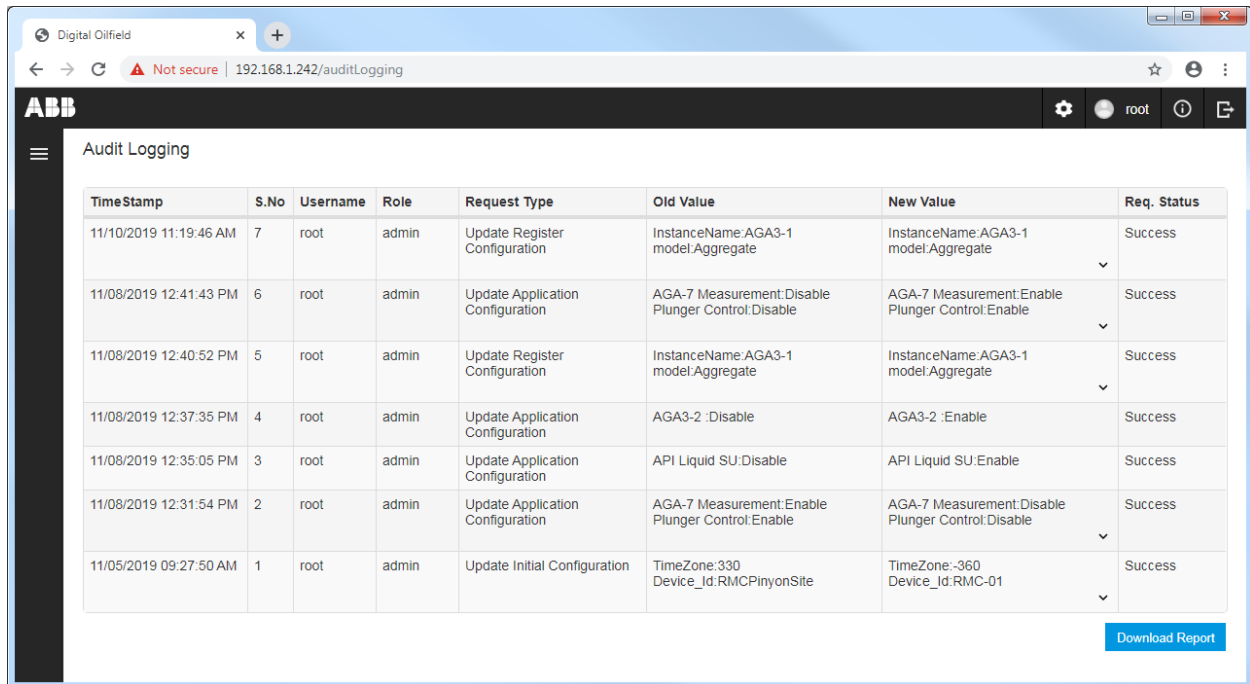
1. Click on the settings icon and select **Audit logging** from the drop-down list ([Figure 10-28](#)).

Figure 10-28: Access the Audit logging page



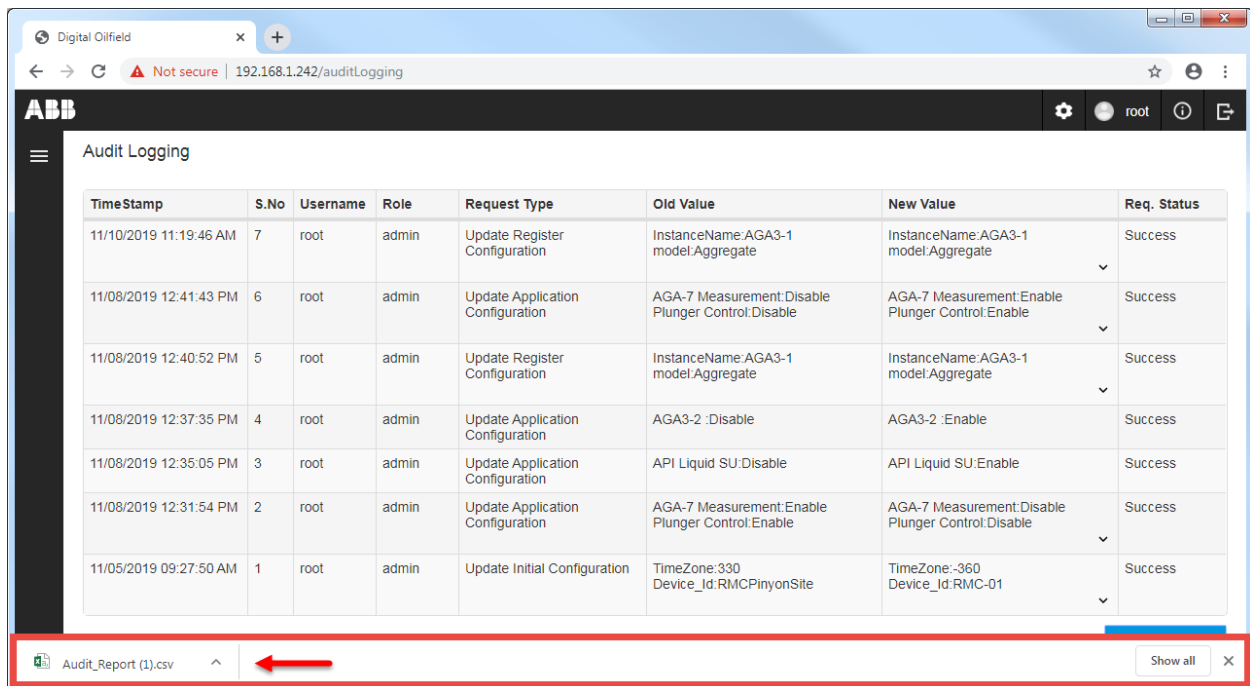
The Audit Logging web page displays.

Figure 10-29: Audit logging page



2. Locate the log of interest or list review logs as necessary.
3. To generate and save a copy of the logs, click **Download Report**. A file with .csv extension saves automatically in the download folder of your laptop or PC (Figure 10-30).

Figure 10-30: Audit Report file generated and downloaded to local laptop



4. Click **Show All**.
5. Select the Audit_Report file from the download list. The file opens (Figure 10-31).

Figure 10-31: Audit report downloaded from the cloud.

	A	B	C	D	E	F	G	H	I	J	K	L
1												
2	TimeStamp	SeqNo	Username	Role	RequestType	OldValue	NewValue	RequestStatus				
3	11/10/2019 11:19	7	root	admin	Update Register Configuration	Instance	InstanceN	Success				
4	11/8/2019 12:41	6	root	admin	Update Application Configuration	AGA-7	AGA-7	Success				
5	11/8/2019 12:40	5	root	admin	Update Register Configuration	Instance	InstanceN	Success				
6	11/8/2019 12:37	4	root	admin	Update Application Configuration	AGA3-2	AGA3-2	Success				
7	11/8/2019 12:35	3	root	admin	Update Application Configuration	API	API Liquid	Success				
8	11/8/2019 12:31	2	root	admin	Update Application Configuration	AGA-7	AGA-7	Success				
9	11/5/2019 9:27	1	root	admin	Update Initial Configuration	TimeZon	TimeZone:	Success				
10												

6. Save the file in the desired folder to keep a backup copy.

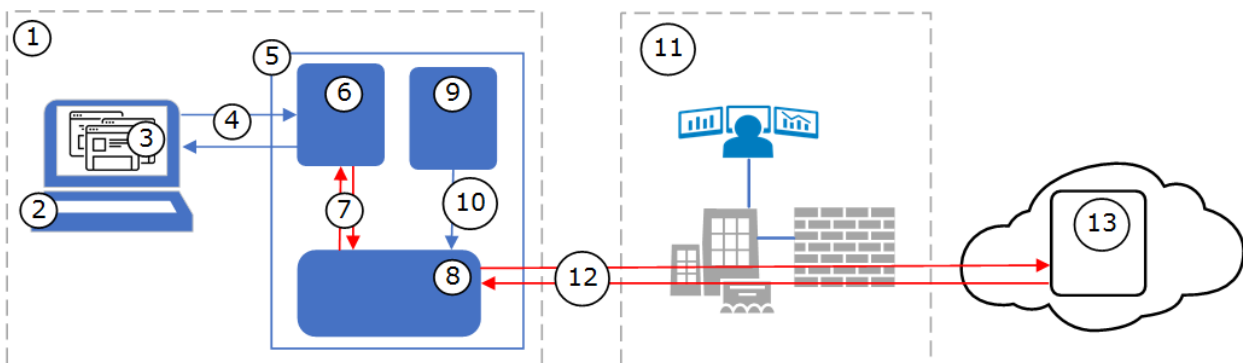
10.6 Monitor device statistics

The Statistics web page provides valuable information to monitor the device configuration process and the device-MQTT broker communication. The device tracks certain parameters such as the number and type of MQTT packets sent or received, disconnection events, etc.

The high-level diagram in [Figure 10-32](#) illustrates a simplified view of the intra-process communication and the device-broker communication for which the device keeps statistics:

- Configuration-related statistics keep track of the internal communication between the processes that handle MQTT-related configuration in the device. This communication consists of configuration requests/responses (7) exchanged between the user interface/REST server (6) and the MQTT stack (8). This example shows a local user connected to the Totalflow device at the site. Statistics are also logged for configuration through a remote connection. Details for these statistics are described in section [10.6.2 Device configuration statistics](#).
- Device-broker connection statistics keep track of the communication between the device (5) and the broker (13) over the network connection (12). Details for these statistics are described in section [10.6.3 Device-broker connection statistics](#).

Figure 10-32: Intra-process and device-broker communication



Legend for Figure 10-32: Intra-process and device-broker communication

	Field device on site	Customer private network	Cloud service provider
1	Field Local Area Network	11 Corporate network	13 MQTT broker
2	Configuration client	12 Device-broker communication, data flow	

3 Configuration web pages

4 Configuration update requests

5 Totalflow device (RMC-100)

6 REST server

7 MQTT configuration intra-process communication

8 MQTT stack processes

9 Application data collector

10 Publish application data

10.6.1 Access the Statistics web page

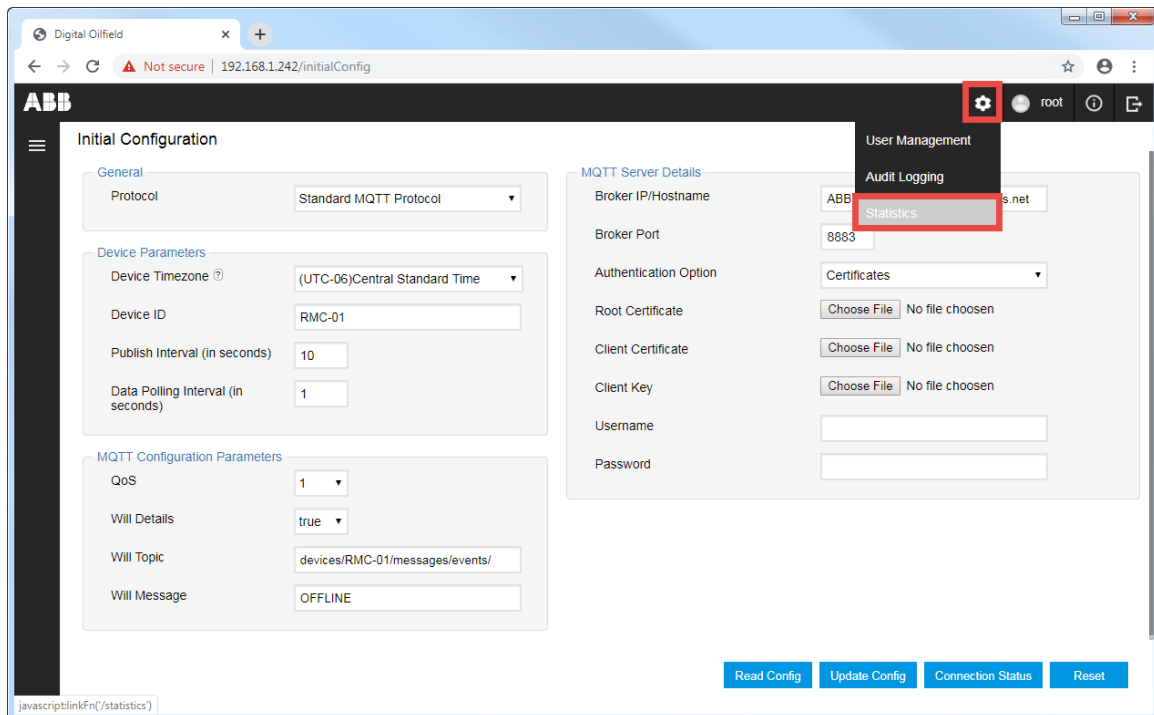


IMPORTANT NOTE: Access to the Statistics web page is available for user and administrator roles.

To view the Statistics page:

1. Click the settings icon and select **Statistics** from the drop-down menu (Figure 10-33).

Figure 10-33: Access the device Statistics page



The statistics web page displays.

Figure 10-34: Statistics for standard MQTT protocol

Statistics Type	Statistics Name	Count
MQTT Configuration Request	Initial Config Update Invalid	0
	Initial Config Update Valid	0
	App Config Update Rejected	0
	App Config Update Accepted	0
	Register Config Update Rejected	0
	Register Config Update Accepted	0
MQTT Configuration Response	Initial Config Update Failed	0
	Initial Config Update Successful	0
	App Config Update Failed	0
	App Config Update Successful	0
	Register Config Update Failed	0
	Register Config Update Successful	0
MQTT Connection Request	MQTT Connection Sending Failed	0
	MQTT Connection Sending Successful	0
MQTT Connection Response	MQTT Connection Successful	0
	MQTT Connection Failed, refused	0
	MQTT Connection Failed, not authorized	0
	MQTT Connection retry count	0

2. Review the information as necessary.
3. If monitoring activity, click **Reset** any anytime to set the counts to zero. Packets counts that do not increase when expected may indicate connection issues.

i **IMPORTANT NOTE:** If sparkplug is the selected protocol, sparkplug-related statistics display in addition to the MQTT statistics. See section [10.6.4 Sparkplug statistics](#) for additional information.

10.6.2 Device configuration statistics

The device supports the configuration of MQTT-related parameters from client’s web browsers. [Table 10-4](#) lists the device configuration statistics sets that track the internal communication between the processes that handle configuration requests and the user interface. [Table 10-5](#) and [Table 10-6](#) provide details for each set.

Table 10-4: Device configuration interface statistics

Type	Description	Monitored packets
MQTT Configuration Request	Packets that the MQTT stack receives from the device user interface for configuration updates	Initial Config Update Invalid Initial Config Update Valid App Config Update Rejected App Config Update Accepted Register Config Update Rejected Register Config Update Accepted
MQTT Configuration Response	Packets that the MQTT stack sends to the device user interface in response to configuration requests	Initial Config Update Failed Initial Config Update Successful App Config Update Failed App Config Update Successful Register Config Update Failed Register Config Update Successful

[Table 10-5](#) describes each of the monitored packets in the configuration requests statistic set. These statistics keep track of packets the MQTT stack receives when a user submits updates from the initial, application, or register configuration pages.

Table 10-5 Configuration requests statistics

Packet name	Description
Initial Config Update Invalid	Packets received with invalid Initial Configuration update values. For example, the user may have submitted an update request with incorrect MQTT device or broker parameters or invalid certificates.
Initial Config Update Valid	Packets received with valid Initial Configuration update values. Values submitted on the Initial Configuration page such as MQTT device and broker parameters and certificates are correct or valid.
App Config Update Rejected	Packets received with invalid updates on the application configuration page. These may include attempts to enable applications that may have been deleted from the device.
App Config Update Accepted	Packets received with valid updates on the Application Configuration page. These may include enabling or disabling some or all the applications configured in the device.
Register Config Update Rejected	Packets received with invalid updates on the register configuration page. These may include attempts to enable registers for applications that may have been deleted from the device.
Register Config Update Accepted	Packets received with valid updates on the Register Configuration page. These may include enabling or disabling some or all the user-configurable registers for the supported applications. Some registers are mandatory and do not allow selection by the user. Mandatory registers remain enabled through any update request.

[Table 10-6](#) describes each of the monitored packets in the configuration response statistic set. These statistics keep track of packets the device sends in response to configuration update requests submitted from the initial, application, or register configuration pages.

Table 10-6: Configuration response statistics

Name	Description
Initial Config Update Failed	Packets that MQTT stack sends to the user interface to notify that it could not apply an update request submitted from the initial configuration page. For example, the device cannot update the configuration because the MQTT broker did not accept certificates submitted or the request had other invalid broker parameter values.
Initial Config Update Successful	Packets that MQTT stack sends to the user interface to notify that it successfully applied the update request submitted from the initial configuration page. This packet is also generated when connection to a new broker has been established successfully in the case where the configuration update involved certificate or MQTT broker hostname change.
App Config Update Failed	Packets that the MQTT stack sends to the user interface to notify that it could not apply an update request submitted from the application configuration page. For example, the device fails to apply the selection (enabling) of an application that is no longer instantiated on the device. This packet type is also generated when the device is not connected to the MQTT broker.

Name	Description
App Config Update Successful	Packets that the MQTT stack sends to the user interface to notify that it successfully applied the update request submitted from the application configuration page. For example, the device accepts the selection of an application that is instantiated and enabled in the device.
Register Config Update Failed	Packets that the MQTT stack sends to the user interface to notify that it could not apply an update request submitted from the register configuration page. For example, the device could not apply the enabling or disabling of a register for an application that is no longer instantiated or enabled in the device. This packet type is also generated when the device is not connected to the MQTT broker.
Register Config Update Successful	Packets that the MQTT stack sends to the user interface to notify that it successfully applied the update request submitted from the register configuration page.

10.6.3 Device-broker connection statistics

[Table 10-7](#) lists the device-broker connection statistics sets that keep track of the communication between the device and the MQTT broker. Some of these statistics apply to both the standard MQTT protocol and Sparkplug. Others apply only to the standard MQTT protocol. For statistics that are specific to Sparkplug, see also section [10.6.4 Sparkplug statistics](#).

Table 10-7: Device-broker connection statistics

MQTT packet type	Description	Packets
MQTT Connection Request	Packets generated by the MQTT stack to indicate if it was able to send a connection request to the MQTT broker Standard MQTT and Sparkplug	MQTT Connection Sending Failed MQTT Connection Sending Successful
MQTT Connection Response	Packets the device receives from the MQTT broker in response to a connection request Standard MQTT and Sparkplug	MQTT Connection Successful MQTT Connection Failed, refused MQTT Connection Failed, not authorized MQTT Connection retry count MQTT Connection reconnect count
MQTT Packet Received	Packets the device receives from the broker over the device-broker connection Standard MQTT protocol only	Register Write Request

MQTT packet type	Description	Packets
MQTT Packet Sent	Packets the device sends to the broker over the device-broker connection Standard MQTT protocol only	Device Packet Count Application Structure Packet Count Trend Definition Packet Count Alarm Definition Packet Count Register Packet Count Trend Packet Count Daily_Log Packet Count Custom_Log Packet Count Event Packet Count Alarm Packet Count Plunger Cycles Packet Count Gaslift Events Packet Count References Packet Count Plunger Events Packet Count Shutdown Events Packet Count Device Packet Count
MQTT disconnect	Packets the device sends or receives prior to device-broker connection graceful termination. Standard MQTT and Sparkplug	MQTT Connection disconnected by device MQTT Connection disconnected by broker

[Table 10-8](#) describes the monitored packets in the MQTT connection request statistic set. These statistics keep track of packets that indicate if connection requests have reached the MQTT broker.

Table 10-8: MQTT connection request (Standard MQTT and Sparkplug)

Name	Description
MQTT Connection Sending Failed	Packet generated by the MQTT stack connection manager process when it is unable to send a connection request to the broker on behalf of the device. The connection request never reached the broker. This can be caused by invalid broker parameters, network error, or an unreachable broker.
MQTT Connection Sending Successful	Packet generated by the MQTT stack connection manager process when it is able to send a connection request to the broker on behalf of the device. The request has reached the device.

[Table 10-9](#) describes the monitored packets in the MQTT connection response statistic set. These statistics keep track of packets that the device receives from the broker after it has issued connection requests.

Table 10-9: MQTT Connection response (Standard MQTT and Sparkplug)

Name	Description
MQTT Connection Successful	Packet that the broker sends to the device when the device successfully establishes a connection with the broker. The broker validates and accepts the connection request from the device.

Name	Description
MQTT Connection Failed, refused	Packet that the broker sends to the device to reject a connection request. The device-broker connection is not established.
MQTT Connection Failed, not authorized	Packet that the broker sends to the device to reject a connection request due to invalid or unauthorized certificates. The device-broker connection is not established.
MQTT Connection retry count	Number of times the device tries to reconnect with the broker since the last successful connection. The device triggers automatic retries as soon as it loses connection with the broker.
MQTT Connection reconnect count	Number of times the device reconnects with a broker

[Table 10-10](#) below describes the packets the device receives from the broker on the device-broker connection.

Table 10-10: MQTT packets received (Standard MQTT protocol only)

Name	Description
Register Write Request	PUBLISH packets received from the MQTT broker that request an application register update on the device. Register update requests are submitted from the cloud user interface on specific application pages. The MQTT broker forwards those requests to the appropriate device.

[Table 10-11](#) below describes the monitored packets in the MQTT packet sent statistic set. These statistics keep track of packets that the device sends to the MQTT broker. Packets sent counts depend on the applications the device is publishing data for and the configured publish interval or frequency.

Table 10-11: MQTT packet sent (Standard MQTT protocol only)

MQTT packet type	Description
Device Packet Count	Any of the PUBLISH packets the device sends to the broker
Application Structure Packet Count	Packets sent with the device structure in the payload
Trend Definition Packet Count	Packets sent with trend definitions in the payload
Alarm Definition Packet Count	Packets sent with alarm definitions in the payload
Register Packet Count	Packets sent with payloads containing information required for register data updates. These packets identify the variable names associated with the register number, old and new values, etc.
Trend Packet Count	Packets sent with trend logs in the payload
Daily_Log Packet Count	Packets sent with a daily log in the payload
Custom_Log Packet Count	Packets sent with a custom log in the payload
Event Packet Count	Packets sent with an event in the payload
Alarm Packet Count	Packets sent with alarm logs in the payload

MQTT packet type	Description
Plunger Cycles Packet Count	Packets sent with plunger cycles in the payload
Gaslift Events Packet Count	Packets sent with gaslift events in the payload
References Packet Count	Packets sent with reference data in the payload (applicable to Gas Lift, Liquid and shutdown applications only). Example of reference data include meter factors or multipoint K factors configured for these applications.
Plunger Events Packet Count	Packets sent with plunger events in the payload
Shutdown Events Packet Count	Packets sent with shutdown events in the payload

[Table 10-12](#) below describes the monitored packets for device-broker disconnection. Disconnection notifications can be triggered from the device or from the broker. These packets contain the DISCONNECT notification in the payload.

Table 10-12: MQTT disconnect (Standard MQTT and Sparkplug)

Name	Description
MQTT Connection disconnected by device	Packets the device sends to the broker to notify it will disconnect from the broker. The device can send this packet before a graceful device shutdown.
MQTT Connection disconnected by broker	Packets the broker sends to the device to notify it will disconnect from the device. The broker can send this packet if the device is disabled from the Azure portal.

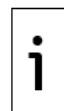
10.6.4 Sparkplug statistics

Sparkplug statistics display when sparkplug is the communication protocol selected for the device-broker connection. These statistics keep track of the packets or messages that flow between the device and the MQTT server.

[Figure 10-35](#) shows a simplified diagram for Sparkplug-specific messages. The message set for which statistics are tracked are sparkplug packets sent (5) or received (6) by the device through the MQTT connection with the server. The SCADA/IIoT primary application (9) acts as an MQTT client and establishes a connection with the MQTT server. Requests for data update are issued in command messages (11) sent by the application to the MQTT server (8).



IMPORTANT NOTE: 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. Component functionality may be implemented as standalone or as software modules in some solutions.

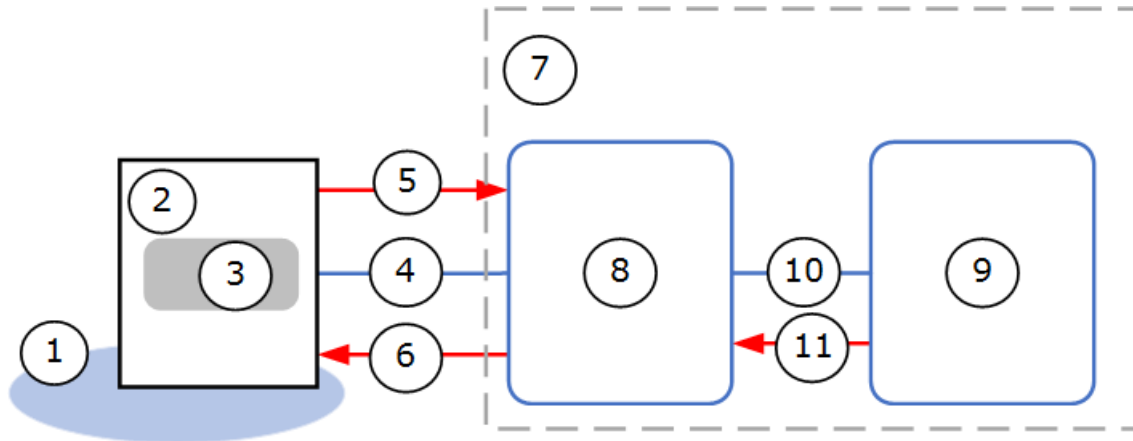


IMPORTANT NOTE: The MQTT-enabled device performs both the device and Edge of Node (EoN) function. Totalflow MQTT-enabled devices support register writes requests only for the Plunger Application.



IMPORTANT NOTE: Totalflow MQTT-enabled devices support register writes requests only for the Plunger Application.

Figure 10-35: Sparkplug-specific message flow



Legend: Sparkplug-specific message flow

Field site		Customer network	
1	Field Local Area Network	7	Customer corporate network (VPN)
2	Totalflow device	8	MQTT server/distributor
3	MQTT client and Sparkplug Device/Edge of Node (EoN) functionality	9	SCADA/IIoT Host (Primary Application)
4	Device - MQTT connection	10	Application-MQTT server connection
5	Sparkplug packets sent: NBIRTH, NDATA or DDATA messages	11	Sparkplug messages sent: NCMD, DCMD, STATE messages
6	Sparkplug packets received: NCMD, DCMD, STATE messages		

IMPORTANT NOTE: The statistics screen for a device using sparkplug also shows the MQTT Connection Request, MQTT Connection Response and MQTT disconnect statistics sets. These are the same statistic types as for the standard MQTT protocol. See section [10.6.3 Device-broker connection statistics](#) for details.

IMPORTANT NOTE: For additional details on sparkplug message types and device-MQTT server message flow, refer to the following link: <https://docs.chariot.io/display/CLD/Sparkplug+Specification>.

[Table 10-13](#) shows the sparkplug-specific statistic sets and message types with payloads defined by the sparkplug specification.

Table 10-13: Sparkplug-specific statistics

Type	Description	Monitored packets
Sparkplug Packet Received	Packets with sparkplug-specific payloads that the device receives from the MQTT server	Sparkplug NCMD Message Count Sparkplug DCMD Message Count Sparkplug STATE Message Count
Sparkplug Packet sent	Packets with sparkplug-specific payloads that the device sends to the MQTT server	Sparkplug NBIRTH Message Count Sparkplug NDATA Message Count Sparkplug DDATA Message Count

[Table 10-14](#) describes each of the packet types the device receives from the MQTT server.

Table 10-14: Sparkplug Packet Received statistics

Name	Description
Sparkplug NCMD Message Count	<p>Number of Node Command (NCMD) messages</p> <p>This message type is used to send commands to the Edge of Node (EoN) to update data values related to node control messages like REBIRTH requests. These requests are initiated by the Ignition servers when they receive corrupted data. The SCADA/IIoT primary application publishes the NCMD message to the MQTT server. The MQTT server ensures that the device receives the command and updates the data values as required.</p> <p>Note that the MQTT-enabled Totalflow device acts as an Edge of Node (EoN) when sparkplug is used. No separate Edge of Node device (gateway) is required for sparkplug support as this functionality is implemented as part of the MQTT stack in the Totalflow device.</p>
Sparkplug DCMD Message Count	<p>Number of Device Command (DCMD) messages</p> <p>This message type is used to send commands to the device to update data values related to device information primarily sent in DDATA.</p> <p>The SCADA/IIoT primary application publishes the DCMD message to the MQTT server. The MQTT server ensures that the device receives the command and updates the data values as required. Totalflow MQTT-enabled devices support register writes requests only for the Plunger Application.</p>
Sparkplug STATE Message Count	<p>Number of critical application state messages</p> <p>This message type is used to indicate the state of the primary SCADA/IIoT host application(s). The SCADA/IIoT system acts as an MQTT client and must publish its state for its own connection and session with the MQTT server. The STATE of the application can be:</p> <ul style="list-style-type: none"> – OFFLINE: The application is not connected, and the device/EoN tries to connect to the next registered MQTT server provided in the initial configuration page. – ONLINE: The application is connected. After reception of this message only, the device/EoN starts sending messages to the MQTT server (Birth and delta messages are not required). <p>The MQTT server ensures that the device is aware of the application state.</p>

[Table 10-15](#) describes each of the packet types the device sends to the MQTT server.

Table 10-15: Sparkplug Packet sent statistics

Name	Description
Sparkplug NBIRTH Message Count	<p>Number of Node birth certificate (NBIRTH) messages</p> <p>The device sends this message type to communicate that it has established a session with the MQTT broker and is ready to start publishing its data. The NBIRTH message is the first message that the device publishes upon establishing a session.</p>
Sparkplug NDATA Message Count	<p>Number of Edge of Node (EoN) Data (NDATA) messages</p> <p>The device sends this message type to enable the continuous session awareness that monitors the state of the Edge of Node connection to the cloud.</p> <p>The device sends this message type to send the latest values of node parameters like CPU, memory usage, etc. to the SCADA System via MQTT Broker based on publish interval.</p> <p>Note that the MQTT-enabled Totalflow device acts as an Edge of Node (EoN) when sparkplug is used. No separate Edge of Node device (gateway) is required for sparkplug support since this functionality is implemented as part of the MQTT stack in the Totalflow device.</p>

Name	Description
Sparkplug DBIRTH Message Count	<p>Number of device birth certificate (DBIRTH) messages</p> <p>The device sends this message type to communicate that it has established a session with the MQTT broker and is ready to start publishing its application/device data. The DBIRTH message is the message sent just after NBIRTH message.</p>
Sparkplug DDATA Message Count	<p>Number of Device Data (DDATA) messages</p> <p>The device sends this message type to send the changed values of device/application parameters, like application registers to the SCADA System via MQTT Broker.</p>

11 Administrator tasks on the Digital Oilfield

The procedures in this section are tasks for advanced users or administrators on the Digital Oilfield interface.

i **IMPORTANT NOTE:** Administrator tasks require access with administrator role. Make sure to log into the Digital Oilfield as an administrator. When logged in with the administrator role, the settings icon displays on the left tool bar on the screen.

11.1 Device management

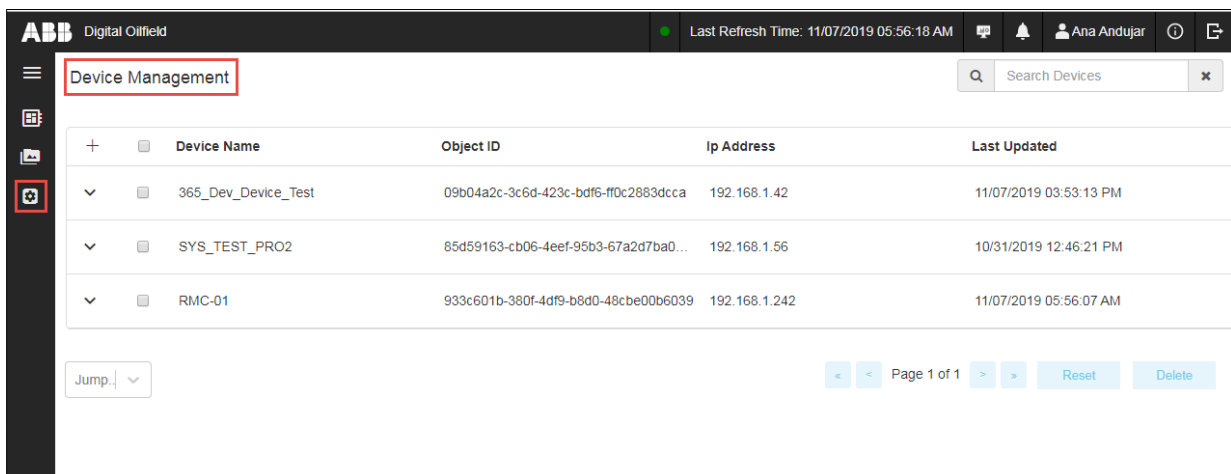
The device management page provides the full list of all the devices managed from the cloud. The default view provides general information for each device. Select a device of interest to display additional information, such as the list of applications the device is publishing data for. Reset or delete devices from this page.

11.1.1 Access the device management web page

To access the device management web page:

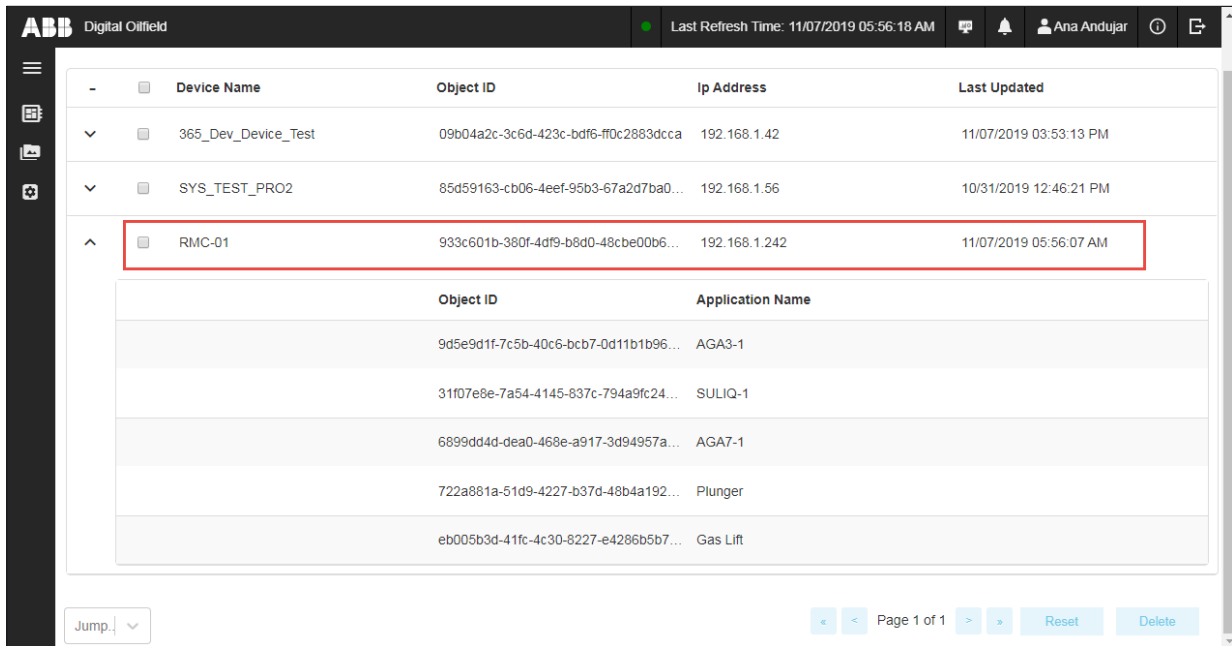
1. Click on the settings icon on the left tool bar ([Figure 11-1](#)). The Device Management web page displays.

Figure 11-1: Device Management web page



2. Locate the device of interest.
3. Click on the device to display additional device details ([Figure 11-2](#)).

Figure 11-2: Additional Device information

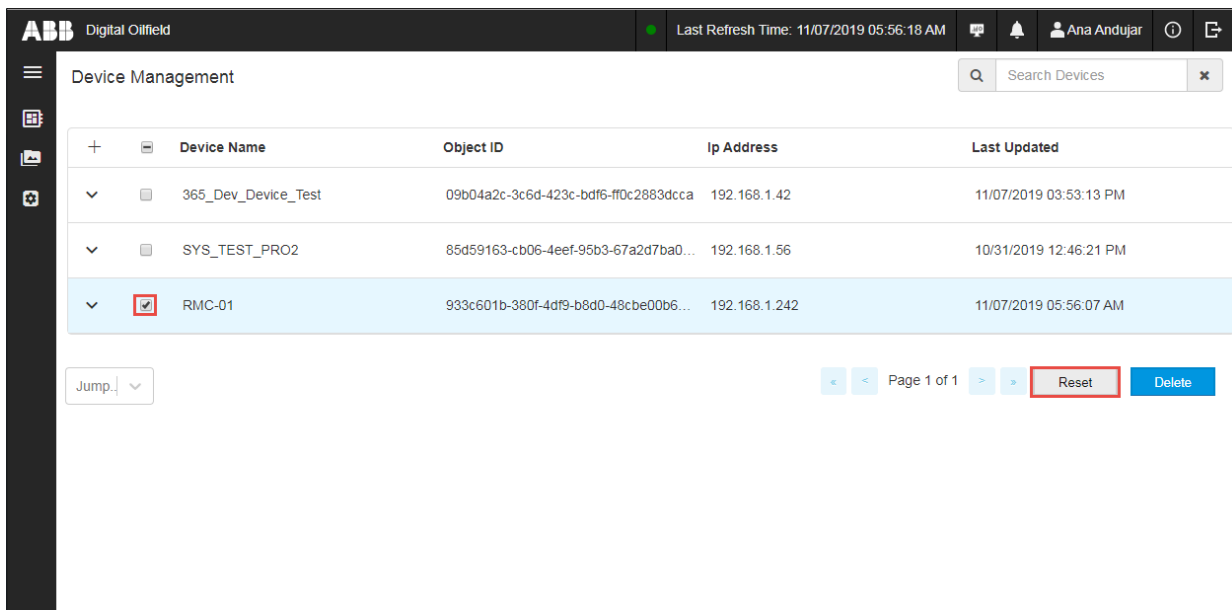


11.1.2 Reset device

To reset a device:

1. Select the device ([Figure 11-3](#)).
2. Select **Reset**.

Figure 11-3: Reset a device from the Device management page

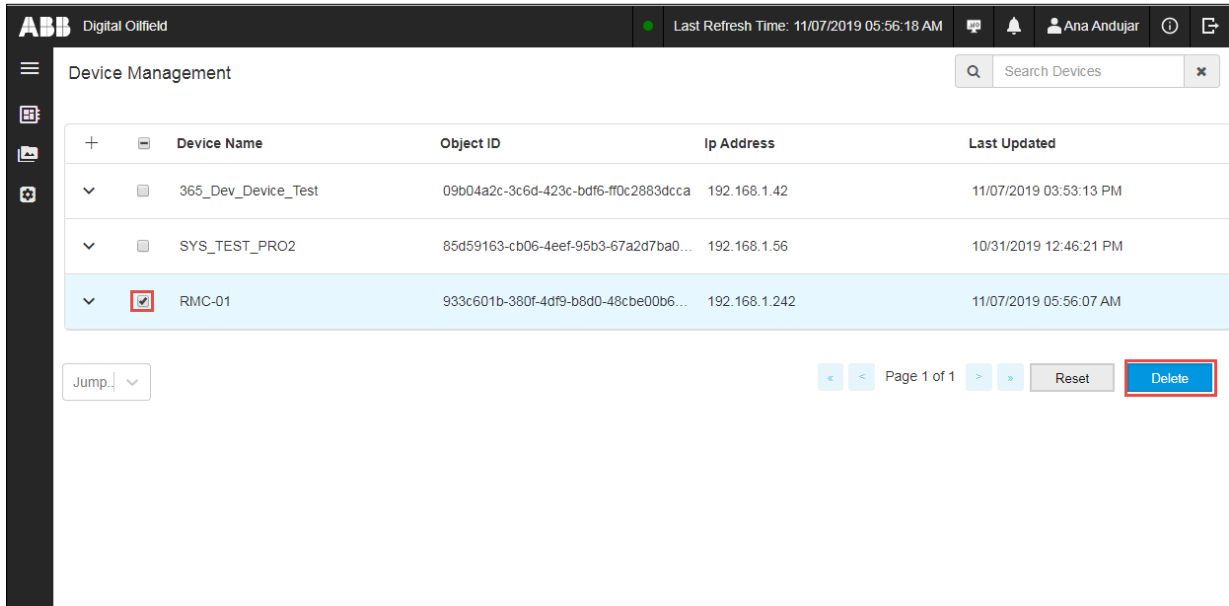


11.1.3 Delete device

To delete a device:

1. Select the device ([Figure 11-4](#)).
2. Select **Delete**.

Figure 11-4: Delete a device from the Device Management page



11.2 Monitor application audit logs

The Digital Oilfield application supports audit logs which keep track of application parameter value updates performed by users from the cloud.

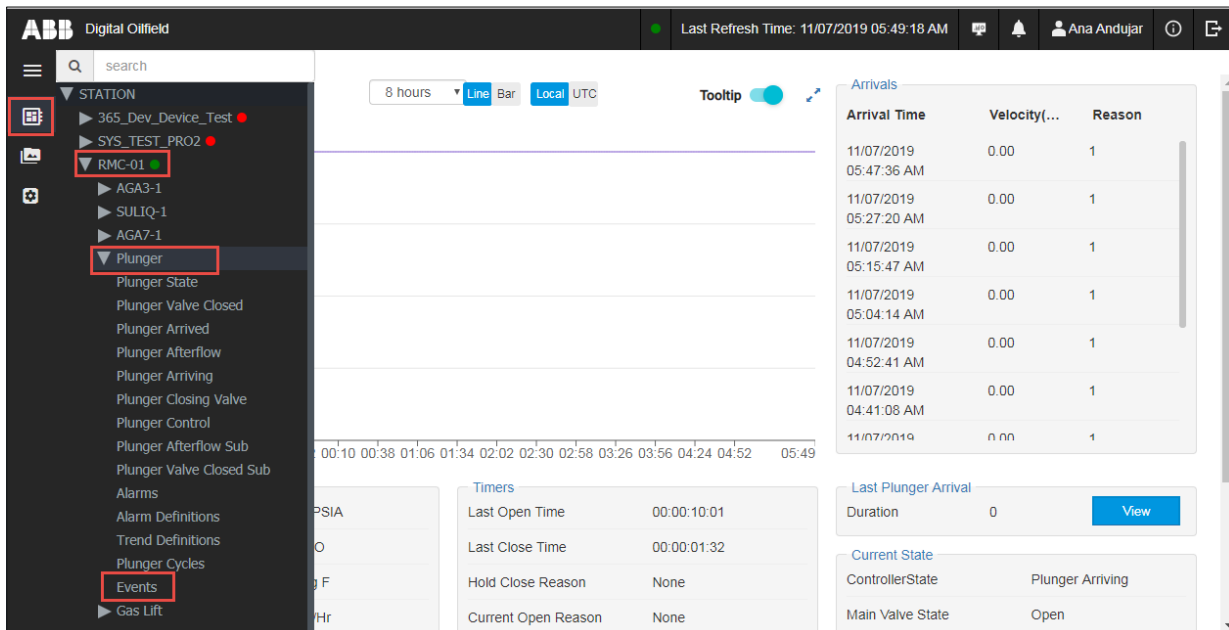


IMPORTANT NOTE: The initial Digital Oilfield release provides this capability only for the Plunger Application on its Event page.

To monitor audit logs:

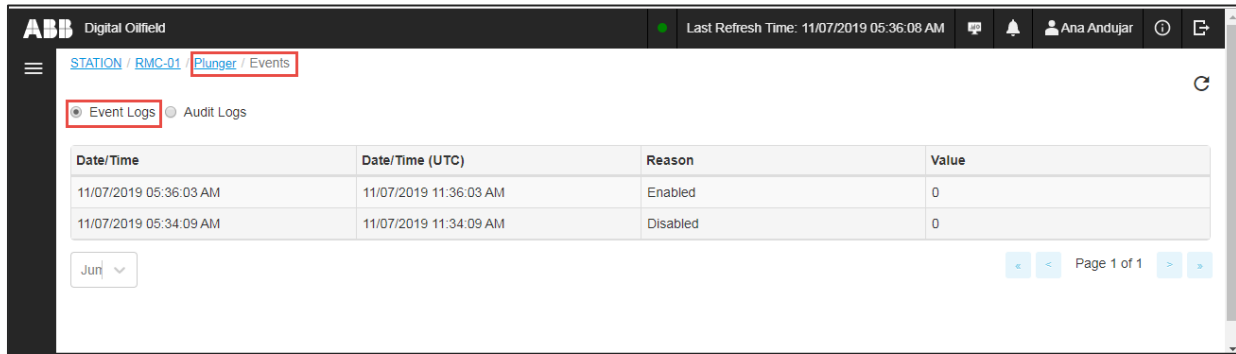
1. Click the device and application view icon to display the navigation tree ([Figure 11-5](#)).
1. Select the device of interest.
2. Select **Plunger**.
3. Select **Events**.

Figure 11-5: Navigate to Plunger Events page



The Events page displays ([Figure 11-6](#)).

Figure 11-6: Plunger application Events page



4. Select **Audit Logs** (Figure 11-7). The list of logs displays. See Table 11-1 for audit logs parameter description.

Figure 11-7: Plunger application audit logs

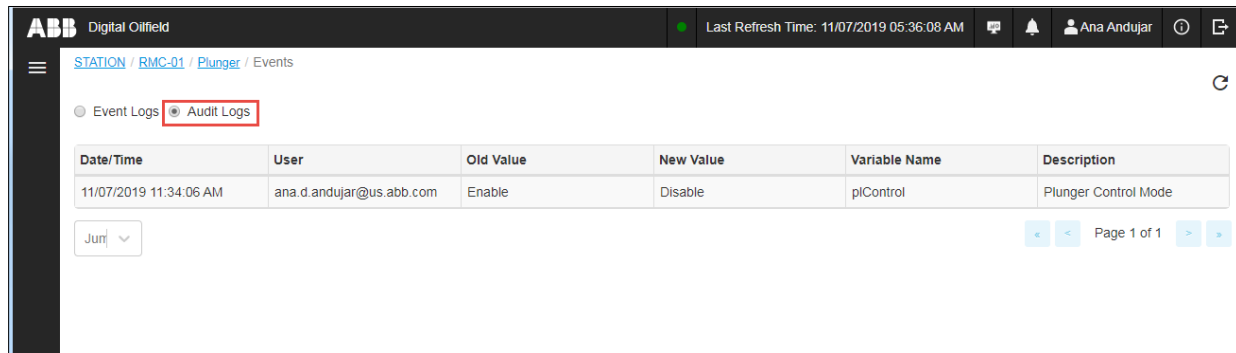


Table 11-1: Application audit logging parameter description

Field	Description	Values
Date/Time	Date and time of the update by the logged-in user (Log time/date stamp)	Date and time match the date and time kept by the device
User	Identifies the logged-in user that updated the application parameter or variable	Any user already setup and authorized for access to the cloud application.
Old Value	Value of the application variable or configuration option prior to update by logged-in user	Applicable values to the parameter type Values might be user-defined or selected from drop-down menus.
New Value	Value of the application variable or configuration option after update by logged-in user	Applicable values to the parameter type Values might be user-defined or selected from drop-down menus.
Variable Name	Name of the variable which holds the value for the parameter or configuration option updated by the logged-in user	Any application variable that applies
Description	Name of application parameter or configuration option as displayed on the application web page.	Any parameter name monitored and supported by the cloud interface

12 Administrator tasks on Azure®

This section describes the tasks administrators must perform to ensure field technicians and operators can access the Digital Oilfield and incorporate field devices onto the service provider cloud. Administrators perform these tasks from the service provider portal:

- Define and manage cloud users and permissions. Provide the personnel responsible for field device configuration with the parameters and authentication certificates/credentials for each device. Parameters must be compatible with the customer's network implementation and the services implemented by the service provider.
- Register devices on the cloud to ensure automatic connection and authentication when the MQTT functionality is enabled and configured in the field.



IMPORTANT NOTE: This section includes procedures at the Azure portal. Azure portal screens might change. Administrators must be familiar with Azure tools. Consult Azure documentation for more information.

12.1 Add and manage cloud users

The cloud service provider determines user access options to ABB's Digital Oilfield. Customers are responsible for defining and managing user accounts and privileges with the cloud service provider. The customer's administrators must set up user accounts and provide access credentials to each required user before they attempt to log into the ABB cloud application.



IMPORTANT NOTE: Users do not have the ability to set up accounts or add users from the Digital Oilfield cloud user interface. Customers using Azure must set up users and assign appropriate roles as specified by Azure and on their portal. The content in this section provides limited information on how to set up new users and assign them to pre-defined permission groups on Azure. Additional details on how to use Azure's portal are beyond the scope of this manual. Administrators must become familiar with Azure's access portals and procedures for user, role, and permission groups setup.

The procedure included in this section creates a new user and assigns permissions. The administrator provides the user's email address for the service provider to notify the user of the new account. The service provider validates the user's response before granting access.

12.1.1 Role privileges on the cloud

[Table 12-1](#) lists roles and their privileges on the cloud. These roles are examples of the roles defined on the Azure cloud.



IMPORTANT NOTE: User roles might reflect permissions to the different data services involved in the processing of the device data. For example, [Table 12-1](#) reflects the read role for both the live data service and data model service access. The Azure cloud distributes the processes required by the cloud interface in separate services.

Table 12-1: Role privileges on the cloud

Role	Access level	Description
Idsadmin	Read and Update	Live Data Service (Ids) admin user Privileges: Read and update data on any of the cloud application pages Access to Audit Logs and Device Management pages
Idsedit	Read and Write	Live Data service (Ids) editor Privileges: Read and write both operations Ability to edit parameter values where applicable or allowed

Role	Access level	Description
ldsread	Read	Live Data Service (lds) read user Privilege: Read access for Live data service which returns the Information Model data.
dmread	Read-only access	Data model (dm) read user Privilege: Read access for data model service which returns the data schema

12.1.2 Password policy

The Digital Oilfield application supports a strong password policy. The application enforces strong password attributes: it ensures the password is within the minimum and maximum password length, and allows the use of special characters, numbers, upper and lowercase letters, etc.

12.1.3 Set up new user

Authorized cloud users are set up on Azure's Active Directory (AD). Azure may have groups with privileges or permission levels already defined. Administrators can assign a new user to the required group and be automatically granted the permissions associated with the group. Administrators must provide user email addresses. Azure automatically sends the email inviting the user to accept membership.

To set up a new user on Azure:

1. Open a web-browser.
2. Log into the Azure Portal.
3. Click **Azure Active Directory** from the sidebar.
4. Click **All users**.
5. Click **New guest user**.
6. Type the user's email address.
7. Type a message with the invitation.
8. Click **Invite**. The portal's screen refreshes and displays the new user.



IMPORTANT NOTE: The new user must accept the invitation from Azure from the email it receives. Azure validates the user's response.

To assign permissions to a new user:

1. Select the new user from the list.
2. Click on **Add membership**. The Select Group sidebar displays on the right with several permission groups.
3. Click the group(s) for the new user.
4. Click **Select**.
5. Click **Refresh**. The group(s) the new user is assigned to display.

12.2 Register field devices

This procedure shows general steps to register (add) a device on the Azure cloud portal. Each device connecting to the cloud must be registered with its unique ID and authentication parameters. Generate the required authentication files based on the preferred authentication method. See section [10.3 Generate certificates for X.509 authentication](#).



IMPORTANT NOTE: Other service providers may have different requirements. Adapt and document procedures for other providers as necessary.

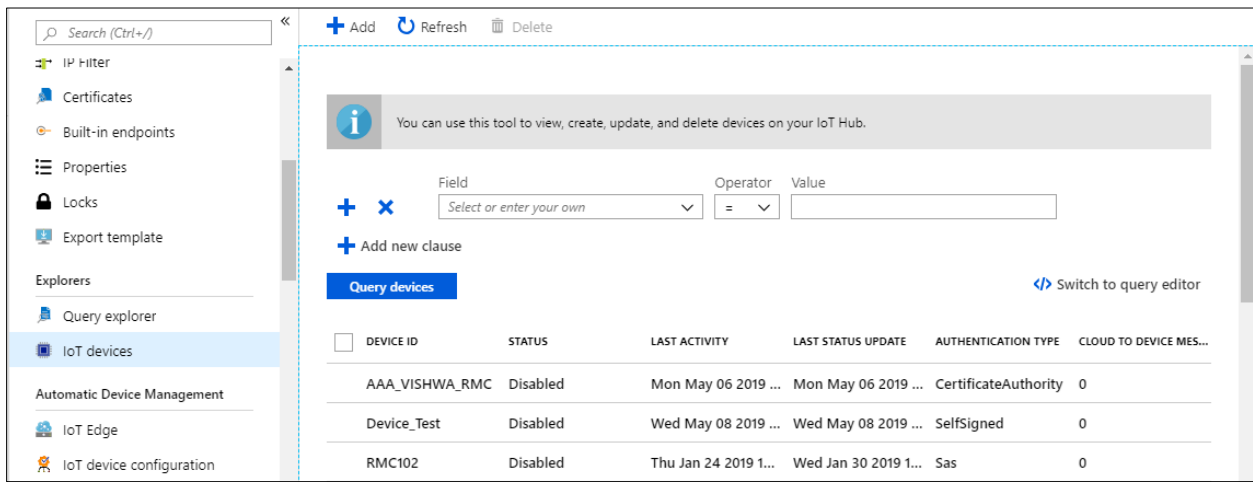


IMPORTANT NOTE: The field device configuration cannot be completed without a successful MQTT device-cloud connection. This connection requires a registered device. Coordinate and plan device registration prior to device installation and configuration to reduce onsite errors and troubleshooting time.

To register a device:

1. Open a web-browser.
2. Go to the Azure portal address (URL): portal.azure.com.
3. Log in. The portal displays the available ABB services or resources (Resources are of the IoT Hub type).
4. Locate and select the required service or resource. The specific IoT service web page displays with information such as the host name for the IoT hub. The host name uniquely identifies the MQTT server.
5. Take note of the Hostname. As an administrator you need to provide the IoT hostname to technicians configuring devices for connection to the service. The hostname is a required parameter to establish and verify connection on initial configuration.
6. On the navigation pane for the selected service, locate and select **IoT devices**. The device list web page displays.

Figure 12-1: Device list



7. Click **Add**. The Create a Device pane displays.

Figure 12-2: Add or create new device on the Azure cloud

Create a device

Find Certified for Azure IoT devices in the Device Catalog

* Device ID ⓘ
The ID of the new device

Authentication type ⓘ
Symmetric key X.509 Self-Signed X.509 CA Signed

* Primary key ⓘ
Enter your primary key

* Secondary key ⓘ
Enter your secondary key

Auto-generate keys ⓘ

Save

8. Type the Device ID.
9. Select the Authentication type and configure parameters accordingly.
 - a. For X.509 Self-signed authentication:
 - i. If you have not done so, generate certificates and fingerprint or thumbprint as described in section [10.3.2 Generate Self-signed certificates](#).
 - ii. Locate the file with the thumbprint.
 - iii. Select **X.509 Self-signed**.

Figure 12-3: Select X.509 Self-signed authentication method

The screenshot shows a 'Create a device' form with the following elements:

- Header: 'Create a device' with a close button.
- Information banner: 'Find Certified for Azure IoT devices in the Device Catalog' with an external link icon.
- Device ID field: Labeled '* Device ID' with a help icon, containing the placeholder text 'The ID of the new device'.
- Authentication type: Labeled 'Authentication type' with a help icon. It features three buttons: 'Symmetric key', 'X.509 Self-Signed' (which is selected and highlighted with a purple border), and 'X.509 CA Signed'.
- Primary Thumbprint field: Labeled '* Primary Thumbprint' with a help icon, containing the placeholder text 'Enter your primary thumbprint here'.
- Secondary Thumbprint field: Labeled '* Secondary Thumbprint' with a help icon, containing the placeholder text 'Enter your secondary thumbprint here'.
- IoT Hub connection: Labeled 'Connect this device to an IoT hub' with a help icon. It has two buttons: 'Enable' (selected) and 'Disable'.
- Save button: A blue button labeled 'Save' at the bottom of the form.

- iv. Open fingerprint or thumbprint file saved during certificate generation.
 - v. Select and copy (CTRL+C) the thumbprint.
 - vi. Paste (CTRL +V) the thumbprint into the Primary and Secondary thumbprint fields.
- b. For X.509 CA Signed authentication:
- i. If you have not done so, generate root and verification certificates, and upload certificates to the IoT hub as described in sections [10.3.4 Generate own root CA certificates](#) or [10.3.5 Generate other root CA certificates](#).
 - ii. Select **X.509 CA Signed**.

Figure 12-4: Select X.509 CA Signed authentication method

The screenshot shows a web form titled "Create a device". At the top left is an information icon and the text "Find Certified for Azure IoT devices in the Device Catalog". Below this is a "Device ID" field with a red asterisk and a help icon, containing the placeholder text "The ID of the new device". The "Authentication type" section has three options: "Symmetric key", "X.509 Self-Signed", and "X.509 CA Signed", with the latter selected. The "Connect this device to an IoT hub" section has two buttons: "Enable" (highlighted in blue) and "Disable". The "Parent device" section shows "No parent device" and a link "Set a parent device". A blue "Save" button is located at the bottom left of the form.

10. Be sure to enable the device for connection to the cloud. Set Connect this device to the IoT hub to **Enable**.
11. Click **Save**.
12. Verify that the new device displays in the device list and that it shows enabled.
13. When device registration is complete, verify device-broker connection during the initial configuration as described in section [3.7 Verify connection status](#).

13 Glossary

Table 13-1 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 13-1: Glossary

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	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.

Term/Acronym	Description
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.
PINGREQ (Ping request) packet	Packet is sent from a client to the server to: <ul style="list-style-type: none"> – 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

Typographical conventions

Element	Convention	Example
Cross-reference to a figure or table in the document	Hyperlink to the figure or table	See Figure 2 .
Cross-reference to a specific section in the document	Hyperlinks to sections referenced throughout the document appear in blue, with underline.	See section 9.1
Cross-reference to another document or website	Hyperlink to the website in blue, with underline	Go to the RMC User Manual at abb.com .
Greater-than character (>)	Indicates that the following item is an additional menu selection	From the menu, locate and select Calibrate > Diff. Press. Sensor > Calibration Units > Edit.
Name of selection buttons, menus, or navigation tree items in instructions that the user will locate and click	Bold text, and the capitalization agrees with the name as displayed on the user interface	Click the Monitor tab and select the Add Advanced Setup tab.
Programs, including utility and accessory programs	Title capitalization	Microsoft Word
URL	All lowercase for a fully specified URL. Blue hyperlink with underline.	www.abb.com/totalflow
User input	Bold and lowercase, unless case sensitive. If the user-input string contains placeholder text, that text is set off with <>.	Type config. < place holder text >



ABB Inc.

Measurement & Analytics

Quotes: totalflow.inquiry@us.abb.com

Orders: totalflow.order@us.abb.com

Training: totalflow.training@us.abb.com

Support: upstream.support@us.abb.com

+1 800 442 3097 (opt. 2)

www.abb.com/upstream

Additional free publications are available for download at:

www.abb.com/totalflow

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 – Pleasanton

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

Texas Office – Odessa

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

We reserve the right to make technical changes or modify the contents of this document without prior notice. With regard to purchase orders, the agreed particulars shall prevail. ABB does not accept any responsibility whatsoever for potential errors or possible lack of information in this document.

We reserve all rights in this document and in the subject matter and illustrations contained therein. Any reproduction, disclosure to third parties or utilization of its contents - in whole or in parts - is forbidden without prior written consent of ABB.

Sparkplug is an open source software specification developed by Cirrus Link Solutions.

Ignition® is registered trademark of Inductive Automation

Azure® is a registered trademark of Microsoft.

Windows® is a registered trademark of Microsoft.

AWS is a registered trademark name of Amazon Web Services Inc.

2106300MNAA

Copyright© 2020 ABB all rights reserved