

ABB MEASUREMENT & ANALYTICS | 2106300MNAA

ABB Digital Oilfield User Manual FOR IMPLEMENTATIONS USING THE RMC-100

ABI	Last Refresh Time: 01/08/2020 08:46:16 AM 📮 🗼 🚣 Ana Andujar 🕐 🗗								
≡	STATION / ST_X509_Test5 / Plunger					Arrivals			
	Flow Rate AP Line	8 hours 🔻	Line Bar Local UTC	Tooltip	2	Arrival Time	Velocity(ft/sec)	Reason	
					T.	01/08/2020 03:48:35 PM	0.01	1	
2						01/08/2020 03:37:02 PM	0.01	1	
						01/08/2020 03:25:29 PM	0.01	1	
						01/08/2020 03:13:56 PM	0.01	1	
						01/08/2020 03:02:23 PM	0.01	1	
						01/08/2020 02:50:50 PM	0.01	1	
						01/08/2020 02:39:17 PM	0.01	1	
						01/08/2020 02:27:44 PM	0.01	1	
	10:40 10:00 10:00 10:47 10:50 10:00	5 13:14 13:23 13:32 13:41 13:50 13:5	0 44/00 44/47 44/00 44/05 44	44 14:53 15:02 15:11 15:20 15:29 15:5		01/08/2020 02:16:11 PM	0.01	1	
	Current Well State	5 15.14 15.25 15.52 15.41 15.50 15.5	Timers	44 14:05 15:02 15:11 15:20 15:29 15:5	Last Plunger Arrival				
	AP	25 PSIA	Last Open Time	00:00:10:01		Duration	5	View	
	DP	50 InH2O	Last Close Time	00:00:01:32		Current State			
	Temperature	75 Deg F	Hold Close Reason	None		ControllerState	Plunger	Arriving	
	Flow Rate	20898.80 SCF/Hr	Current Open Reason	None		Main Valve State	Open		
	Casing	0	Current Close Reason	TIMER		Plunger Status	Drop		
	Tubing	0 PSIA	Plunger Control			Cycle Status	Running	9	
	Line	10 PSIA	Plunger State	Enable Enable		State Timer	00:00:0	0:25	
			Time Elapsed	00:00:00:25 Disable		Max State Timer	00:00:4	0:00	
			Go to Plunger Status	Manual					

Measurement made easy

Contents

Contents 2					
Су	ber so	ecurity			
Ac	lditior	nal inforr	mation6		
Sa	fety				
	Poten	tial safety	y hazards7		
1.	Prod	uct desci	ription8		
	1.1	Architect	ture8		
	1.2	Core arc	hitecture components9		
	1.3	MQTT-er	nabled Totalflow device description10		
		1.3.1	Standard MQTT functionality10		
		1.3.2	Sparkplug functionality15		
		1.3.3	MQTT device configuration interface16		
	1.4	Digital O	ilfield application description20		
		1.4.1	Supported browsers20		
		1.4.2	Supported Totalflow applications20		
		1.4.3	Home page21		
		1.4.4	Device and application navigation tree view22		
		1.4.5	General device information pages24		
		1.4.6	Application pages25		
2	Prepa	are for d	evice configuration		
	2.1	Prerequis	sites		
	2.2	Determir	ne authentication method		
		2.2.1	Authentication methods		
		2.2.2	Prepare for authentication configuration		
	2.3	Register	the device on the cloud		
	2.4	Device c	onfiguration overview		
3	Initia	l device	configuration		
	3.1	Access th	he Initial Configuration page35		
	3.2	Configur	e the protocol		
	3.3	Configur	e device parameters		
		3.3.1	Device parameters for Standard MQTT protocol41		
		3.3.2	Device parameters for Sparkplug41		
	3.4	Configur	e MQTT parameters42		
		3.4.1	MQTT configuration parameters for Standard MQT protocol44		
		3.4.2	MQTT configuration parameters for Sparkplug44		
	3.5	Configur	e MQTT Server Details45		
		3.5.1	MQTT Server Details for the Standard MQTT Protocol47		
		3.5.2	MQTT Server Details for Sparkplug49		
	3.6	Update c	configuration		
	3.7	Verify co	nnection status		
	3.8	Reset de	vice configuration		

4	Devi	ce applic	ation configuration	55
	4.1	Access tl	he Application Configuration page	55
	4.2	Enable a	pplication data publishing	56
	4.3	Disable a	application data publishing	57
	4.4	Update a	application configuration	57
5	Devi	ce regist	er configuration	59
	5.1	Access tl	he Register Configuration page	59
	5.2	Enable r	egister data publishing	59
	5.3	Disable r	register data publishing	61
	5.4	Update r	egister configuration	61
6	Trou	bleshoot	ing device connection errors	63
	6.1	User-dev	vice connection failure	63
		6.1.1	Checklist to resolve failure to connect to field device	64
	6.2	Device-E	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	Advance	d troubleshooting procedures	66
		6.3.1	Verify processes from SSH	67
		6.3.2	Collect logs using SFTP	71
	6.4	Troubles	hooting when using Sparkplug	79
7	Acces	ss the Di	gital Oilfield	81
	7.1	Log into	the Digital Oilfield	81
	7.2	Navigate	e to devices and applications	82
	7.3	View me	asurement 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 cor	ntrol application data	99
		7.4.1	Plunger Control application	99
		7.4.2	Shutdown application 1	06
		7.4.3	Gas Lift application1	08
	7.5	Access P	lunger Analysis System (PAS) services1	11
		7.5.1	Access PAS options 1	11
		7.5.2	Schedule analyses for pre-defined intervals 1	12
		7.5.3	Schedule analyses for user-defined intervals (custom) 1	13
		7.5.4	View Fault Detection reports1	14

		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 fr	om the cloud interface	118
9	Total	flow dev	vice security	119
	9.1	Device s	ecurity guidelines	119
	9.2	Secure c	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 a	access to the MQTT configuration interface	122
	9.4	Open TC	P 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 d	lata protection for decommissioning	127
10) Admi	inistrato	r tasks for the device	129
	10.1	Enable o	r disable MQTT functionality	129
	10.2	Provide a	and manage certificates	131
	10.3	Generate	e 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	
	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	
		10.4.5	Update User	145
		10.4.6	Delete User	
	10.5		device audit logs	
		10.5.1	Audit Logging web page overview	
		10.5.2	Access the Audit Logging web page	
	10.6		device statistics	
		10.6.1	Access the Statistics web page	
		10.6.2	Device configuration statistics	
		10.6.3	Device-broker connection statistics	
		10.6.4	Sparkplug statistics	
11			r tasks on the Digital Oilfield	
	11.1	Device n	nanagement	
		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 a	application audit logs	165		
12 Admi	nistrato	r 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 Gloss	ary		. 173		
Typogra	ypographical conventions				

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 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 <u>www.abb.com/totalflow</u>.

Figure 0-1: Related documentation				
Documents	Document number			
Configure MQTT How to Guide	<u>2106521</u>			
RMC-100 User Manual	<u>2105552</u>			
RMC-100 Startup Guide	<u>2105551</u>			
Plunger Analysis System Administrator Guide	<u>2105844</u>			
Advanced Ethernet Parameter Description	2105999			

Figure 0-1: Related documentation



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 <u>Glossary</u> for general descriptions of the terms used in this manual. For additional details or component descriptions, see section <u>1.2 Core architecture components</u>.

1.1 Architecture

<u>Figure 1-1</u> 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 <u>9.2 Secure connections</u>.

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.

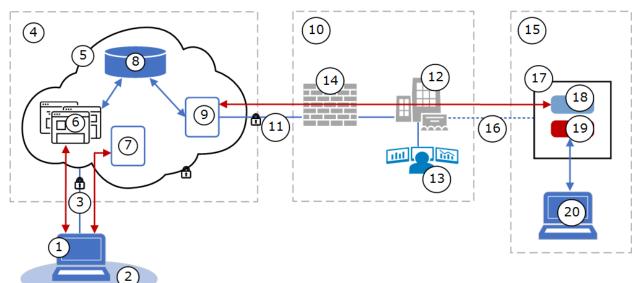


Figure 1-1: Digital Oilfield architecture

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 acces 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	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

<u>Table 1-1</u> provides a high-level description of the major architecture components illustrated in <u>Figure</u> <u>1-1</u> 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.

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 $1.3 \text{ MQTT-enabled Totalflow device}$ for additional details.
Cloud – core infrastructure (Microsoft®	MQTT Broker	The MQTT broker performs the role of the MQTT server. Enables secure MQTT-protocol-based connection of field devices to the cloud.
Azure)		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 <u>1-1</u> : Item 10). Real-time and historical values generated by Totalflow devices, device and application data, alarms and events data.

Table 1-1: Digital Oilfield architecture components

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 <u>1.4 Digital Oilfield application</u> <u>description</u> 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	 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 <u>1.3.1 Standard MQTT functionality</u> or section <u>1.3.2 Sparkplug functionality</u>.
- To review the configuration interface, see section <u>1.3.3 MQTT device configuration interface.</u>



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 <u>9.2 Secure connections</u>.

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. Also see section http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1. Also see section http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf. Also see section http://docs.oasis-open.org/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf. Also see section http://docs.oasis-open.org/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf. The section and proceed to the configuration sections



1

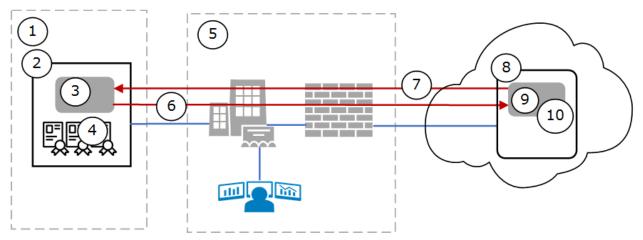
IMPORTANT NOTE: For simplicity, the diagrams in the following sections show the MQTT functionality and data flow for a single device only. The Digital Oilfield is designed to support many devices located across different field sites. The scale of the implementation depends on the customer's specifics,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

1.3.1.1 Connect

<u>Figure 1-2</u> 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

p	Cloud service provid		Customer private network	Field device on site
	MQTT broker	8	Corporate network	Field Local Area Network 5
nctionality	MQTT server functiona	9	Request for connection	Totalflow device (RMC) 6
	MQTT broker verificati certificates/credentials connection	10	Connection granted from broker	MQTT client functionality 7
	certificates/crede		-	Authentication

certificates/credentials

1.3.1.2 Subscribe

<u>Figure 1-3</u> 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 <u>1.3.1.3 Update</u>).

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.

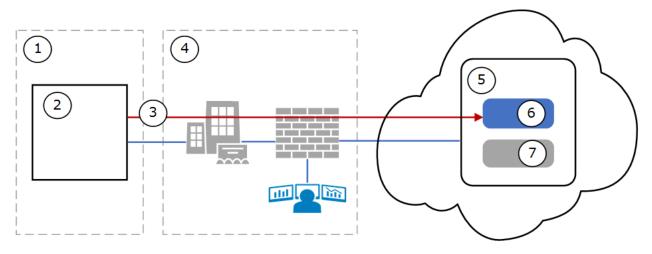
Note that the subscription topic is different from the publish topic (7). The subscription topic is used by the broker to distribute data from the cloud application to the subscribed devices (device-bound data flow). The publish topic is used by the broker to send data updates to the cloud application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

IMPORTANT NOTE: Each device subscribes to the following topic:

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

Figure 1-3: Device subscription

1



Legend for Figure 1-3: Device subscription

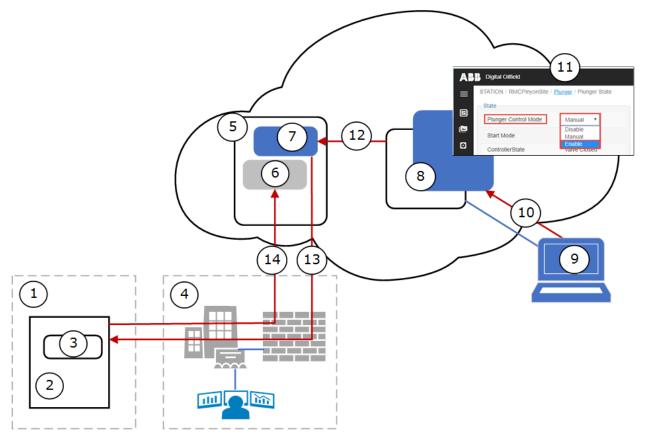
Field device on site	Customer private network		Cloud service provider
1 Field Local Area Network	4 Corporate network	5	MQTT broker
2 Totalflow device (unique ID)		6	Device subscription topic
3 Subscribe to topic on broker		7	Device publish topic

1.3.1.3 Update (register-write)

<u>Figure 1-4</u> 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 <u>1.3.1.2 Subscribe</u>). 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 <u>1.3.1.4</u> 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 4 Network	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 14 application data (register data or records)	updated parameter value back to the cloud to ensure cloud application displays updated value	7	Device publish topic	11	User submits parameter change
		(see <u>Figure 1-5</u>).	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		

1.3.1.4 Publish

<u>Table 1-2</u> 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.

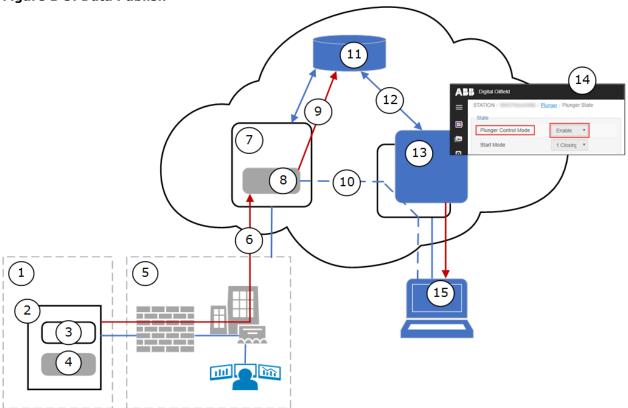
Figure 1-5 shows a simplified view of how the device publishes its data:

- 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



	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	6	Device publishes	8	Device subscription topic		
	(RMC with unique device ID)		data to broker on device topic				
3	Totalflow device application data			9	Broker sends update to database		
	(register data or records)				uatabase		
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).	:	

Legend for Figure 1-5: Data Publish

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.

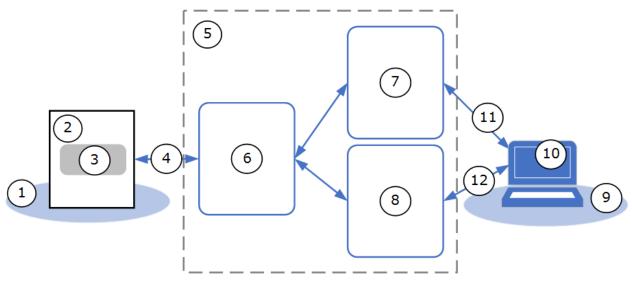


IMPORTANT NOTE: The implementation of the SCADA/IIoT system depends on specific customer requirements and available network topologies. Customers may also implement their solutions end-to-end on their own private networks if not using MQTT brokers on a service provider cloud. In these scenarios, the 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: <u>https://docs.chariot.io/display/CLD/Sparkplug+Specification</u>.

<u>Figure 1-6</u> 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 <u>10.6.4 Sparkplug statistics</u>.

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, <u>Figure 1-6</u> does not show any databases or other services. Databases are typically implemented on-premise for data storage.

i

1

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. <u>Figure 1-7</u> 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.

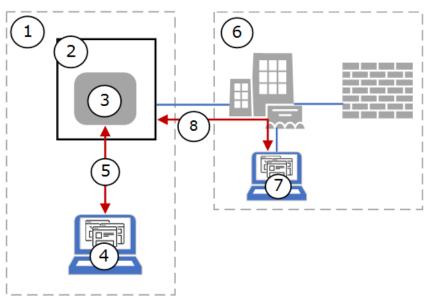


Figure 1-7: Device user interface for MQTT operation

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	8	Connection for remote configuration
	(web configuration pages)		
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 <u>Table 1-3</u>.



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.

<u>Figure 1-8</u> 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.



ABB			🗢 💿 root 🛈 🗗
■ Initial Configuration			
General		MQTT Server Details	
Protocol	Standard MQTT Protocol	Broker IP/Hostname	ABBLighthouseIOT.azure-devices.net
Durin Deventer		Broker Port	8883
Device Parameters Device Timezone ?	(UTC-06)Central Standard Time •	Authentication Option	Certificates 🔻
Device ID	RMC-01	Root Certificate	Choose File root.ca.cer.cer
Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert.pem
Data Polling Interval (in seconds)	1	Client Key	Choose File client-key.pem
		Username	ABBLighthouseIOT.azure-devices.net/RN
MQTT Configuration Parameters — QoS		Password	
Qos	1 •		
Will Details	true 🔹		
Will Topic	devices/RMC-01/messages/events/		
Will Message	OFFLINE		
		Rea	d Config Update Config Connection Status Reset

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.

<u>Figure 1-9</u> 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

ABI	3				۵ 🕈	root (j	G
≡	Application Configuration	1				Select A	
	 ✓ AGA-3 Measurement ✓ Gas Lift 		Plunger Control	d Shutdown System	🗹 API Liqui	d SU	
	Application Instances	✓ AGA7-1	✓ Plunger	SULIQ-1	𝖉 Gas Lift	Select A	JI
					Read Config	Update Cont	fig

i

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 instancespecific register data publishing.

<u>Figure 1-10</u> 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

ABB	3				۵ 🗘	root 🛈 [
≡	Register Configuration					
	Select Application :	AGA-3 Measurement API Liquid SU	 AGA-7 Measurement Gas Lift 	Plunger Control	Shutdown System	
	Select App Instance :	AGA3-1				
	Select All Registers					Select All
	Today's Volume	Today's Ma	ass	Today's Energy	Yesterday's Volume	
	Yesterday's Mass	Yesterday	s Energy	Accumulated Volume	Accumulated Mass	
	Accumulated Energy					
	Application					Select All
	Static Pressure	Differential	Pressure	Flow Rate	Flowing Temperature	- I
	Energy Rate	Mass Rate	e de la companya de l	Device/APP ID	Tube Description	
	Enhanced Mode	Facility Me	asurement Point	Company Name	Contract Hour	
					Read Config	Update Config

1

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).

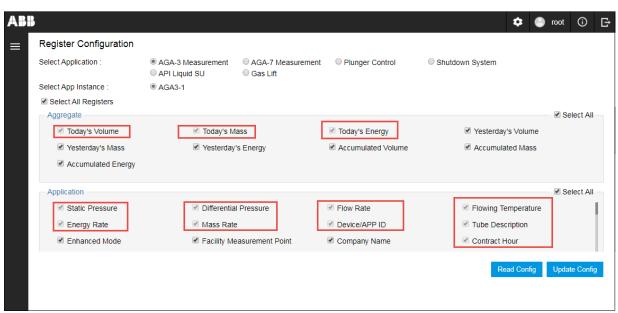


Figure 1-11: Required registers examples (read-only)

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 <u>7</u> Access the Digital Oilfield.

For access, use systems with browser versions listed in section <u>1.4.1 Supported browsers</u>. To determine what applications are supported on the cloud, see section <u>1.4.2 Supported Totalflow</u> <u>applications</u>.

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 <u>Table 1-4</u>.

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

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

1.4.2 Supported Totalflow applications

<u>Table 1-5</u> 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 <u>1.3.3.3</u> <u>Application Configuration page</u>). Alarm data and trends are published for all supported applications if defined and configured from PCCU.

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

Table 1-5: Totalflow application supported on the clo

1.4.3 Home page

1

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

<u>Figure 1-12</u> 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 <u>Figure 1-12</u> 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

List Of Devices 12		10		¹⁵ C
Name	Location	IP Address	Date Time	Status 1
RMC-01 13	Measurement and Control	192.168.1.41	10/25/2019 03:01:55 AM 16	•
SYS_TEST_PRO2	Measurement and Control	192.168.1.56	10/26/2019 05:02:49 PM	•
			< < Page	1 of 1 >

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

<u>Figure 1-13</u> 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.

ABB Digital Oilfield Last Refresh Time: 11/11/2019 05:47:25 PM .±0 À 💄 Ana Andujar **(**) Đ Q search \equiv (2) Current Values STATION Tooltip 🧰 8 hours Line Bar 14.73 PSIA Static Pressure 360_Dev_Device_Test ▶ 365_Dev_Device_Test Differential Pres. 0 inH2O 1 SYS_TEST_PRO2 3 ▼ RMC-01 (60 Deg F Flowing Temper... \$ ► AGA3-1 Flow Rate 0 MCF/Day ► SULIQ-1 ► AGA7-1 1 0 MBTU/Hour Energy Rate ► AGA3-2 (4) Plunger Mass Rate 0 lbm/hour Gas Lift 0 MBTU Today's Energy Today's Volume 0 MCF Today's Mass 0 lbm 12:54 13:31 14:08 14:45 15:22 15:59 16:36 17:49 Units and Periods Constants Vol Calc Period Orifice Diameter 1 in 1 second

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

ABI	Digital Oilfield	Last Refresh Time: 11/11/2019 05:47:2	25 PM 🐺 🌲	🛓 Ana Andujar (🕞
	Q search		- Current Values	
1	▼ RMC-01 ● 3 ▼ AGA3-1	8 hours Line Bar Tooltip 🧾 🦨	Static Pressure	14.73 PSIA
	Application		Differential Pres	0 inH2O
٢	Aggregate Composition		Flowing Temper	60 Deg F
	Digital Outputs Last Calculated		Flow Rate	0 MCF/Day
	Custom Logs		Energy Rate	0 MBTU/Hour
	Daily Logs 4 Alarms		Mass Rate	0 lbm/hour
	Alarm Definitions Trend Definitions		Today's Energy	0 MBTU
	Events SULIQ-1		Today's Volume	0 MCF
	AGA7-1	13:07 13:44 14:21 14:58 15:35 16:12 16:49 18:02	Today's Mass	0 lbm
	 ► AGA3-2 ► Plunger ► Gas Lift 	Units and Periods Vol Calc Period 1 second	Constants Orifice Diameter	1 in

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

Digital Oilfield			 Last Refr 	esh Time: 11/01/2019 09:06:31 AM 🚆	🜲 🔺 Ana Andujar (
STATION / RMC-01		General		Versions	
Station ID	TOTALFLOW	Digital Board Part#	2105023	Flash Software Version	2.3.0-3
IP Address	192.168.1.40	Flash Software Part#	2105457-029	OS Software Version	2.2.0-3
Location	Measurement and Control	OS Software Part#	2105411-032	On-board IO Software Version	2.3.0-3
Date Time	11/01/2019 07:36:28 PM	On-board IO BL Part#	2105458-003	On-board IO BL Software Version	1.0.1-146
Software Build Date Time	10/29/2019 06:54:11 AM	Registry		Lithium Backup Battery	
System Resources		Application Profile	AGA3/AGA7 Standard US Units	Install Date	10/29/2019 mm/dd/yyyy
Current Processor Usage(%)	9	Software Description	G5RMC Source	Rated Capacity	1600 mAH
Average Processor Usage(%)	12.11	Factory Configuration	44	Event Capacity	1568 mAH
System CPU Frequency	720 MHz	Power Supply Battery		Backup Current	0.04 mA
Available Task Memory	225185792 Bytes	Install Date	07/08/2019 mm/dd/yyyy	Depleted Capacity	0 mAH
Available Flash File Space	421942272 Bytes	Rated Life	36.52 Months	Lithium Battery Status	Low Voltage or Not Connected
Available SD Card File Space	0 Bytes	Event Age	18.26 Months	Boot Loader	
Receive Ethernet Usage(%)	0.00	Calender Age	3 months	First Stage Boot Loader Part#	2105412-014
Transmit Ethernet Usage(%)	0.01	Adjusted Age	6.32 Months	Second Stage Boot Loader Part#	

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.

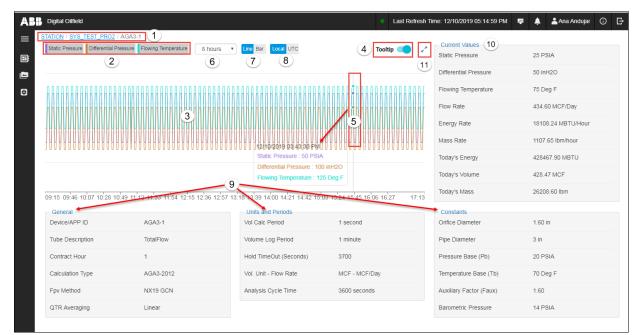


Figure 1-16: Main AGA3 page

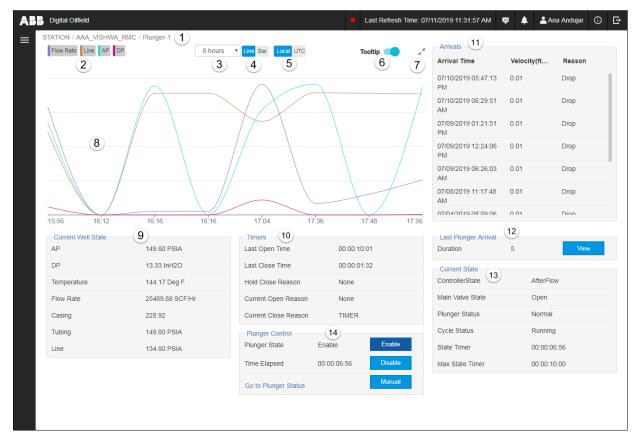
Legend for Figure 1-16: Main AGA3 page

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 (<u>Figure 1-18</u>), displays all the application parameters available for monitoring from the cloud. Each parameter displays its value and additional attributes when expanded (<u>Figure 1-19</u>) 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

ABI	Digital Oilfield			•	Last Refresh Tim	ne: 11/06	/2019 01:22:17 PM 🛛 👜	🚢 Ana Andujar	() E•
≡	STATION / RMC-01 / AGA3-1 / Ap	plication						3 Co	lumns 🔻
	Attached to stream	None	~	Flowing Temperature	60 Deg F	~	Speed of Sound Calculation	Disabled	~
	Auxiliary Factor (Faux)	1	~	Fpv Method	AGA8 Gross 92	~	Static Pressure	14.73 PSIA	~
	Barometric Pressure	14.73 PSIA	~	H2O Bias	7 lbm/MMSCF	~	Stream ID	0	~
	Base Density	0.05 lbm/ft3	~	Hold TimeOut (Seconds)	3600	~	Temperature Base (Tb)	60 Deg F	~
	Base Density Source	Calculated from Real Relative Density	~	Mass Rate	0 lbm/hour	~	Tube Description	TotalFlow	~
	Calculation Type	AGA3-1992	~	Orifice Diameter	1 in	~	Use Calc Cd	Yes	~
	Contract Hour	0	~	Orifice Plate Exp. Coef.	9.25	~	Use Faux	No	~
	Device/APP ID	AGA3-1	~	Orifice Reference Temperature	68	~	Use Fixed H2O	No	~
	Differential Pressure	∩ inH2O	~	Pipe Diameter	2.07 in	~	Use Fpv	Yes	~ .

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

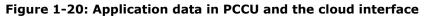
Figure 1-19: Static pressure (read-only parameter)

tatic Pressure	207.51 PSIA	^
		-
Cloud Access:	Read	
High value:	2047.97	
Low value:	0	

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 (<u>Figure 1-20</u>), for example, displays parameters from several of the application setup tabs in PCCU (overlay image): General, Constant, and Current Values tabs.



Digital Oilfield			Last Refresh Time: 03	7/08/2019 10:39:16 AM 🛛 🕎	🛕 💄 Ana Andujar 🕠
STAT	wina 1 , T 💽 💽 🔐 🔠	🎯 🏦 🛄 🔍 🧇		Current Values Static Pressure	150.87 PSIA
B. RMC-100		Log Capacity	Current Values	Differential Pressure	14.39 inH2O
- Totalflow/U	CP Ge	neral Constants Water Co	nstants Factors Limi	Flowing Temperature	144.25 Deg F
		Description 5.0 Device/APP ID	AGA3-1	Flow Rate	26575.51 SCF/Hr
	ient / III -	5.2 Tube Description 0.110 Enhanced Mode	TotalFlow Disabled	Energy Rate	26575.51 MBTU/Hour
Setup		0.0 Contract Hour 1.6 Vol Calc Period	00 1 Second	Mass Rate	1230.80 lbm/hour
Digital C RS and N	lutputs 11	2.0 Log leriod	60 minutes	Today's Energy	467975.32 MBTU
Adv Setu		0.9 Calculation Type 0.12 Fpv method	AGA3-1992 AGA8 Gross 92	Today's Volume	467.98 MCF
13:12 13:52 14:20 14:4	8 15:16 15:44 16:12 16:40	0.42 Vol. Unit Flow Rate 17:08 17:36 8:04 18:32 19:00	MCF - MCF/Day 19:28 19:56 20:24 21:0	Today's Mass	21673.49 lbm
General Device/APP ID	A3-1	Units and Periods Vol Calc Period	1 second	Constants Orifice Diameter	1.50 in
Tube Description	Totalflow	Volume Log Period	60 minutes	Pipe Diameter	2.90 in
Contract Hour	0	Hold TimeOut (Seconds)	1234	Pressure Base (Pb)	15 PSIA
Calculation Type	AGA3-2012	Vol. Unit - Flow Rate	MCF - SCF/Hr	Temperature Base (Tb)	65 Deg F
	NX19 Auto	Analysis Cycle Time	0 seconds	Auxiliary Factor (Faux)	1.50
Fpv Method					

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.

<u>Table 1-6</u> 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.

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.



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.

Prerequisites 2.1

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.

Requirement	Description	Task
MQTT-ready device OS and flash	The device embedded software with the MQTT client functionality.	 Obtain customer package 2105452-032 or later for the RMC-100. Upgrade the device. See PCCU help files or refer to Additional information for links to the RMC-100 documentation. Enable MQTT functionality on the device as described in section <u>10.1</u>.
Valid IP configuration for cloud connection	IP configuration must include a valid IP address, subnet mask and default gateway.	 Obtain valid IP configuration from your IT administrator if configuring a new device or an existing device without IP parameters assigned. Configure the device's IP parameters (address, mask and gateway) from PCCU.
Unique Device ID	Device ID, or name that uniquely identifies the Totalflow device	 Use a naming convention that allows the unique identification of each field device. Assign a unique ID to each device intended for connection to the 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.	 Determine the authentication method. Generate or obtain certificate and authentication keys as necessary.

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

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.



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.

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.

 Table 2-2: Configuration system (laptop) prerequisites

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. <u>Table 2-3</u> 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.

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.

Table 2-3: Obtain authentication parameters

Requirement	Description	Task
		 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.	 Obtain the preferred method from the administrator.
Username/ password	Required for all authentication methods depending on the service provider if used.	 Obtain credentials from administrator.
Certificates, Keys	Required for X.509 authentication Digital files with certificate, key and fingerprint that certify the device authenticity for acceptance on the cloud.	 Obtain from system administrator the three required files for X.509 authentication. Administrators must obtain the common Root Certificate (for all devices) Administrators must obtain (or generate) the device-specific files: Client Certificate and Client Key. Have certificate files available on the system the device is configured from. The certificate files must be copied to the device during configuration. To generate device-specific certificates and keys, see section 10.3, Generate certificates for X.509 authentication.

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.
- 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.

i

1

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, MQTTenabled devices provide web pages with several configuration options. <u>Table 2-4</u> identifies the configuration pages and the associated procedures for device configuration. For an overview of the configuration pages see section <u>1.3.3 MQTT device configuration interface</u>.

IMPORTANT NOTE: A successful device-broker connection is required to complete all configuration. Follow the tasks listed in <u>Table 2-4</u> 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.

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 <u>3</u> <u>Initial device configuration</u> . (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 <u>3.7 Verify connection status</u> . (Initial configuration page)
Application configuration	Select device applications and instances the device will publish data for.	Follow procedures in section <u>4</u> <u>Device application</u> <u>configuration</u> . (Application configuration page)
Register configuration	Select the specific application registers the device will publish data for.	Follow procedures in section <u>5</u> <u>Device register configuration</u> . (Register configuration page)

Table 2-4: Device configuration overview



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 <u>section 10.1.</u>

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 <u>Prerequisites</u>. 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.

i

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.

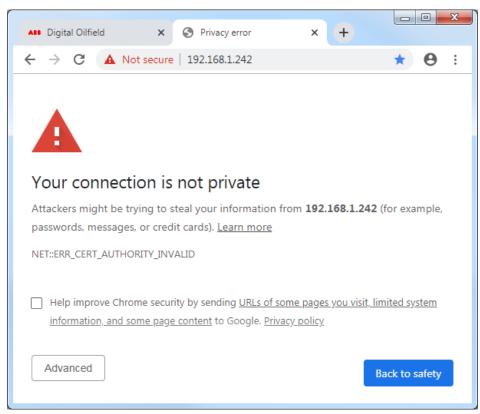
To access the device's Initial Configuration web page:

- 1. Connect the laptop and the device to the network.
- 2. Start the Chrome browser.
- 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



Click Advanced at the bottom of the screen. Additional security information displays (<u>Figure</u> <u>3-2</u>) 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

ABD Digital Oilfield X 🔇 Privacy error	
← → C ▲ Not secure 192.168.1.242	* A =
	* 0 :
This conver could not prove that it is 102 169 1 2	42: its security cortificate is not trusted by your
This server could not prove that it is 192.168.1.2 4 computer's operating system. This may be caused	
intercepting your connection.	
Proceed to 192.168.1.242 (unsafe)	
FIGUEER 10 132.100.1.242 (UII3816)	
Hide advanced	Back to safety

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

ABB Digital Oilfield X	S Digital Oilfield		
\leftarrow \rightarrow C A Not secure 192.	168.1.242	*	Θ :
ABB			
			_
	ABB Digital Oilfield		
	Username:		
	Username		
	Password:		
	Password		
	Submit		

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

O Digital Oilfield × +			
← → C ▲ Not secure 192.168.1.242/	initialConfig		☆ ⊖ :
ABB			🗢 🕒 root 🛈 🕞
		MQTT Server Details	
Protocol	Standard MQTT Protocol	Broker IP/Hostname	ABBLighthouseIOT.azure-devices.net
		Broker Port	8883
Device Parameters		Authentication Option	Certificates
Device Timezone 🕤	(UTC-06)Central Standard Time •	, automodian option	
Device ID	RMC-01	Root Certificate	Choose File root.ca.cer.cer
Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert.pem
Data Polling Interval (in seconds)	1	Client Key	Choose File client-key.pem
		Username	ABBLighthouseIOT.azure-devices.net/RN
MQTT Configuration Parameters —			
QoS	1 •	Password	
Will Details	true 🔻		
Will Topic	devices/RMC-01/messages/events/		
Will Message	OFFLINE		
			Read Config Update Config Connection Status Reset



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. <u>Table 3-1</u> describes the protocol options supported by the field device.

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.	device-broker connection. The protocol specifies the packet	MQTT Standard Protocol (default) Select this option when connecting to a broker cloud service provider broker.
	Sparkplug Select this option when connection to a corporate network with its own MQTT server or distributor as part of a SCADA/IIoT architecture.	

Table 3-1: Communication protocol description



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

🕒 Digita	al Oilfield	×	+
$\leftarrow \ \rightarrow$	C A Not secure	192.1	.68.1.242/initialConfig
ABB			
	Initial Configuration	n	
	General		
	Protocol		Standard MQTT Protocol 🔹
			Standard MQTT Protocol
	D		Sparkplug

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

Figure 3-6: Select Sparkplug

1

O D	igital Oilfield	× +
← -	C A Not secure	192.168.1.242/initialConfig
AB	6	
≡	Initial Configuration	n
	General	
	Protocol	Standard MQTT Protocol
		Standard MQTT Protocol
	Nevice Darameters	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 (<u>Figure 3-7</u>).



S Digital Oilfield × +			
← → C ▲ Not secure https://1	92.168.1.242/initialConfig		☆ 🛎 :
ABB			🌣 🍚 root 🚯 🕞
Initial Configuration			
General		MQTT Server Details	
Protocol	Sparkplug •	No Server Configured Create New MQTT Server	
Device Parameters			
Device Timezone 💿	(UTC-06)Central Standard Time •		
Group ID			
Device ID			
Publish Interval (in seconds)			
Data Polling Interval (in seconds)			
MQTT Configuration Parameters QoS			
200	0 •		
		Read Config Update (Config Connection Status Reset
		r Read Conlig Opdate (connection status Reset

2. Configure device parameters in section <u>3.3</u>.

3.3 Configure device parameters

<u>Table 3-2</u> 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.

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).

Table 3-2: Device parameter description

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)

🚯 Digit	al Oilfield 🗙	< +		
$\leftarrow \ \rightarrow$	C 🔺 Not secure 1	.92.168.1.242/ii	nitialConfig	
ABB				
≡	Initial Configuration			
	General			
	Protocol		Standard MQTT Protocol	•
	Device Parameters			
	Device Timezone ?		(UTC-06)Central Standard Time	•
	Device ID		RMC-01	
	Publish Interval (in se	econds)	10	
	Data Polling Interval	(in seconds)	1	

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.

S Digita	al Oilfield X	÷
$\leftarrow \ \rightarrow$	C A Not secure 192.16	8.1.242/initialConfig
ABB		
	nitial Configuration	
	General	
	Protocol	Sparkplug •
	Device Parameters	
	Device Timezone ?	(UTC-06)Central Standard T ▼
	Group ID	Site ABC
	Device ID	RMC-01
	Publish Interval (in second	is) 10
	Data Polling Interval (in seconds)	1

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 devicebroker 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	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. The device exchanges messages with the MQTT broker according to the QoS levels defined by the MQTT specification and supported in the device. Applies to both the Standard MQTT Protocol and Sparkplug.	 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. 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.
Will Details	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. The device sends the LWT message to the broker while connected to the broker specifying details. 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. Standard MQTT protocol only.	True (default) – The device requests the broker to send the LWT message upon ungraceful device disconnection. Recommended. False - the device does not request the broker to send the LWT message upon ungraceful device disconnection.
Will Topic	Topic where the broker publishes the Will message after ungraceful device disconnection. MQTT clients subscribed to this topic receive this notification and are aware of the device disconnection. Standard MQTT protocol only.	The Will topic depends on the definitions set in the cloud. The following is the default string from the factory: devices/ <device id="">/messages/events/ 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. 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).</device>
Will Message	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). Standard MQTT protocol only.	OFFLINE (default)

3.4.1 MQTT configuration parameters for Standard MQT 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.

- Select **true** from the Will Details drop-down list.
 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

🕙 Digita	al Oilfield × +	
$\leftarrow \ \rightarrow$	C A Not secure 192.168.1.242/i	nitialConfig
ABB		
	nitial Configuration	
	General	
	Protocol	Standard MQTT Protocol •
	Device Parameters	
	Device Timezone 💿	(UTC-06)Central Standard Time •
	Device ID	RMC-01
	Publish Interval (in seconds)	10
	Data Polling Interval (in seconds)	1
	MQTT Configuration Parameters	
	QoS	1 •
	Will Details	true 🔻
	Will Topic	devices/ <mark>RMC-01</mark> /messages/events/
	Will Message	OFFLINE

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 <u>3.5</u>.

Figure 3-11: MQTT Configuration Parameters for Sparkplug

🕥 Digita	al Oilfield X	+
$\leftarrow \ \rightarrow$	C A Not secure 192	2.168.1.242/initialConfig
ABB		
	nitial Configuration	
	General	
	Protocol	Sparkplug •
	Device Parameters	
	Device Timezone ?	(UTC-06)Central Standard T •
	Group ID	Site ABC
	Device ID	RMC-01
	Publish Interval (in sec	conds) 10
	Data Polling Interval (i seconds)	n 1
	MQTT Configuration Par	ameters
	QoS	1 •

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.

i

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

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.	For connection to a cloud service provider MQTT server:		
		 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. 		
		For connection to a customer MQTT server or distributor when using Sparkplug:		
		 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. 		
Option field devices before authentication		 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.	 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.	 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.		 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 		

Table 3-4: MQTT Server Details description

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 <u>3.6</u> <u>Update configuration</u>). 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.

🕥 Digita	al Oilfield × +			
\leftrightarrow \rightarrow	C A Not secure 192.168.1	.242/initialConfig#		☆ 9 :
ABB	C Not secure 192.168.1 nitial Configuration General Protocol Device Parameters Device Timezone ? Device ID Publish Interval (in seconds) Data Polling Interval (in seconds)	Standard MQTT Protocol (UTC-06)Central Standard 1 RMC-01	MQTT Server Details Broker IP/Hostname Broker Port Authentication Option Root Certificate Client Certificate Client Key	ABBLighthouseIOT.azure-devices.net 8883 Certificates Choose File root.ca.cer.cer Choose File client-cert.pem Choose File client-key.pem
	 MQTT Configuration Parameter QoS Will Details Will Topic 	Ts	Username Password Read Config	ABBLighthouseIOT.azure-devices.net/RI

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

O Digital Oilfield × +						
← → C ▲ Not secure 192.168.1.242/initialConfig#	☆ ⊖ :					
SB 💿 root 🕥						
Initial Configuration						
General Protocol Standard MOTT Protocol	MQTT Server Details Broker IP/Hostname ABBL inhthouseIOT azure devices net					
Protocol Standard MQTT Protocol •	Abbelginitodsero i azure devices net					
Device Parameters						
Device Timezone ? (UTC-06)Central Standard 1 •	Authentication Option Username/Password V					
Device ID RMC-01	Username					
Publish Interval (in seconds) 10	Password					
Data Polling Interval (in 1 seconds)						
MQTT Configuration Parameters						
QoS 1 V						
Will Details true 🔻						
Will Topic devices/RMC-01/messages/ever						
	Read Config Update Config Connection Status Reset					

6. Update the configuration as described in section <u>3.6 Update configuration</u> 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

Oigital Oilfield	× +				
\leftrightarrow \rightarrow C	A Not secure 192.168.1	242/initialConfig			☆ \varTheta :
ABB					🗢 🌕 root 🚯 🗗
	Configuration				
Gene	eral		MQTT Server Details		
Pr	rotocol	Sparkplug •	No Server Configured		
			Create New MQTT Server		
	ice Parameters				
De	evice Timezone 💿	(UTC-06)Central Standard 1 •			
Gr	roup ID	Site ABC			
De	evice ID	RMC-01			
Pu	ublish Interval (in seconds)	10			
	ata Polling Interval (in econds)	1			
MQT	TT Configuration Parameter	S			
Q	oS	1 🔻			
			Read Config	Update Config Co	onnection Status Reset

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

Figure 3-15: Add Server Details for Sparkplug

Oigital Oilfield	× +				
	A Not secure 192.168.1	242/iu	aitialConfig#		☆ 🖰 :
_	Not secure 152.108.1	242/11	intalConing#		
ABB					🗢 🍥 root 🛈 🗗
	Configuration				
Gene	eral			MOTT Server Details	
Pro	otocol	Spa	Add Server Details		
Devic	e Parameters		Broker IP/Hostname		
De	vice Timezone 🤊	(UTC	Broker Port		
Gro	oup ID	Site/	Authentication Option	Certificates •	
De	vice ID	RMC	Root Certificate	Choose File No file choosen	
Pu	blish Interval (in seconds)	10	Client Certificate	Choose File No file choosen	
	ta Polling Interval (in conds)	1	Client Key	Choose File No file choosen	
			Username		
	T Configuration Parameter	rs 1	Password		
				OK Cancel	
					nnection Status Reset

- 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

S (Digital Oilfield × +				
÷	→ C A Not secure 192.168.1	1.242/initia	alConfig#		☆ 🖰 :
AB	₿				🗢 🌑 root 🛈 🗗
≡	Initial Configuration				
	General	-		MOTT Server Details	
	Protocol	Spai /	Add Server Details		
	Device Parameters		Broker IP/Hostname	192.2.36.210	
	Device Timezone 🔊	(UT(Broker Port	3232	
	Group ID	Site/	Authentication Option	Certificates	
	Device ID	RMC	Root Certificate	Choose File root.ca.cer.cer	
	Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert.pem	
	Data Polling Interval (in seconds)	1	Client Key	Choose File client-key.pem	
			Username	1	
	MQTT Configuration Parameter QoS	1	Password		
				OK Cancel	
				le Con	nfig Connection Status Reset

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

0	Digital Oilfield × +							
← -	$\leftarrow \rightarrow \mathbb{C}$ A Not secure 192.168.1.242/initialConfig# $\diamond \mathbb{O}$:							
AB	8		🗢 🔘 root 🛈 🗗					
≡	Initial Configuration							
	General		MOTT Server Details	L				
	Protocol	Spa Add Server Details						
	Device Parameters	Broker IP/Hostname	192.2.36.210					
	Device Timezone 💿	(UT(Broker Port	3232					
	Group ID	Site/ Authentication Option	Username/Password •					
	Device ID	RMC Username						
	Publish Interval (in seconds)	10 Password						
	Data Polling Interval (in seconds)	1		l				
			OK Cancel					
	MQTT Configuration Parameter	5						
	QoS	1 •						
			Read Config Update Config Connection Status Reset					

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

🕑 Digital Oilfield 🛛 🗙 🕂									
← → C ▲ Not secure 192.168.1.242/	initialConfig		☆ Θ						
ABB O root 🛈									
General	General MOTT Server Details								
Protocol	Standard MQTT Prot	Update request received successfully. Reconnect to MQTT broker is in progress. Please wait as it could take	ABBLighthouseIOT.azure-devices.net						
Device Parameters		up to 2 minutes.	8883						
Device Timezone 💿	(UTC-06)Central Sta	Close	Certificates •						
Device ID	RMC-01	Root Certificate	Choose File root.ca.cer.cer						
Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert pem						
Data Polling Interval (in seconds)	1	Client Key	Choose File client-key.pem						
		Username	ABBLighthouseIOT.azure-devices.net/RN						
MQTT Configuration Parameters	1 •	Password							
Will Details	true 🔻								
Will Topic	devices/RMC-01/messages/eve	nts/							
Will Message	OFFLINE								
			Read Config Update Config Connection Status Reset						

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. <u>Table 3-5</u> 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 <u>6.4</u> <u>Troubleshooting when using Sparkplug</u>.

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.

Oigital Oilfield × +							
← → C ▲ Not secure 192.168.1.242/	initialConfig		x 🛛 😆 🗄				
ABB			🗢 🌑 root 🛈 🕞				
General		MOTT Server Details					
Protocol	Standard MQTT Prot OPPrice is conne	ected to MQTT broker (IP :	ABBLighthouseIOT.azure-devices.net				
Device Parameters	Device Id : RM	elOT.azure-devices.net Port : 8883 (C-01)	8883				
Device Timezone ?	(UTC-06)Central Sta	Close	Certificates •				
Device ID	RMC-01	Root Certificate	Choose File root.ca.cer.cer				
Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert.pem				
Data Polling Interval (in seconds)	1	Client Key	Choose File client-key.pem				
MQTT Configuration Parameters		Username	ABBLighthouseIOT.azure-devices.net/RN				
QoS	1 •	Password					
Will Details	true 🔻						
Will Topic	devices/RMC-01/messages/events/						
Will Message	OFFLINE						
			Read Config Update Config Connection Status Reset				

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

Oigital Oilfield	< +		
← → C ▲ Not secure ≠	https://192.168.1.39/initialConfig		☆ 📿 🖘 😩 :
АВВ			🗢 💿 root 🛈 🕞
Initial Configuration			
General Protocol	Standard I Oevice is not cor	nnected to MQTT Broker	ABBLighthouseIOTStaging.azure-device
Device Parameters	(UTC+05:	Close	Certificates •
Device ID	ST_X509_Test	Root Certificate	Choose file root.ca.cer.cer
Publish Interval (in sec	onds) 10	Client Certificate	Choose file full-cert.pem
Data Polling Interval (ir seconds)	1	Client Key	Choose file key.pem
		Username	
MQTT Configuration Para QoS	ameters 1 T	Password	
Will Details	true 🔻		
Will Topic	devices/ST_X509_Test/message		
Will Message	OFFLINE		
		Read Config	Update Config Connection Status Reset

- 3. Click **Close** to return to the initial configuration screen.
- 4. Proceed with the device configuration in section <u>4 Device application configuration</u> when the device-broker connection is successful.

5. See section <u>6</u> <u>Troubleshooting</u> if the device-broker connection fails. If you need to re-configure the device from scratch, reset to factory defaults as described in section <u>3.8</u> <u>Reset device</u> <u>configuration</u>.

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 <u>Table 1-5</u>. 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.



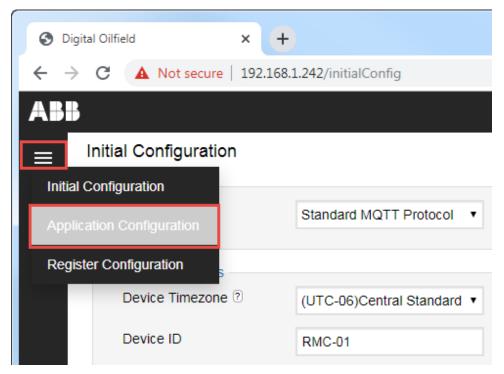
IMPORTANT NOTE: The application web page does not display unless the device has established connection with the MQTT broker.

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

Oigital Oilfield ×	+				
← → C ▲ Not secure 19	92.168.1.242/applicationConfig				☆ \varTheta :
ABB				🗢 🕒 🕫	oot (i) 🗗
Application Configura	ation				
Applications AGA-3 Measureme Gas Lift	ent	Plunger Control	Shutdown System	API Liquid SU	✓ Select All —
Application Instances	☑ AGA7-1		SULIQ-1	🕑 Gas Lift	Select All —
				Read Config U	Ipdate Config

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

0	Digital Oilfield × +				
÷	→ C A Not secure 192.168	3.1.242/applicationConfig			☆ \varTheta :
A	3B				🔹 🌕 root 🛈 🕞
≡	Application Configuration Applications	Z AGA-7 Measurement		Shutdown System	Select All
	Application Instances AGA3-1		✓ Plunger	SULIQ-1	Gas Lift
					Read Config Update Config

- 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

S Digit	tal Oilfield × +					
$\leftarrow \ \rightarrow$	C 🔺 Not secure 192.168	.1.242/applicationConfig				☆ \varTheta :
ABB					¢ 😔	root 访 🗗
≡	Application Configuration Applications C AGA-3 Measurement G as Lift	AGA-7 Measurement	Plunger Control	Shutdown System	🗆 API Liquid	Select All
	Application Instances	AGA3-2	Plunger			Select All
					Read Config	Update Config

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

🕑 Digit	tal Oilfield × -	Ð			
$\leftarrow \ \rightarrow$	C A Not secure 192.168	3.1.242/applicationConfig			☆ 🖰 :
ABB					🔹 🍚 root 🛈 🕞
≡	Application Configuration				
	Applications	AGA-7 Measurement	Plunger Control	Shutdown System	Select All API Liquid SU
	Gas Lift	GAGA-7 Measurement		Shutdown System	
					Read Config Update Config

- 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 <u>4.2</u> and <u>4.3</u>.
- 2. Click **Update Config** (Figure 4-6). A confirmation for the update displays (Figure 4-7).

Figure 4-6: Update the Application Configuration

🗿 Dig	pital Oilfield × +				
\leftrightarrow \rightarrow	C A Not secure 192.168	.1.242/applicationConfig			☆ \varTheta :
ABI	6				🗢 🌕 root 🛈 🕞
≡	Application Configuration				
	Applications				Select All
	AGA-3 Measurement	AGA-7 Measurement	Plunger Control	Shutdown System	API Liquid SU
	Gas Lift				
	A collection to store as				
	Application Instances	AGA3-2	SULIQ-1		Select All
					Read Config Update Config

Figure 4-7: Update config successful message

🚯 Digi	tal Oilfield × +	•			
$\leftarrow \ \rightarrow$	C A Not secure 192.168	3.1.242/application	Config		☆ 🖰 :
ABB					🗢 💿 root 🚯 🕞
≡	Application Configuration Applications Application Gas Lift Application Instances	□ ▲ 🔗	Detailed Configuration Received success	fully System	☐ Select All
	AGA3-1	AGA3-2	SULIQ-1	_	Select All
					Read Config Update Config

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 <u>Table 1-5</u> and enabled in section <u>4: Device application configuration</u>.

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.



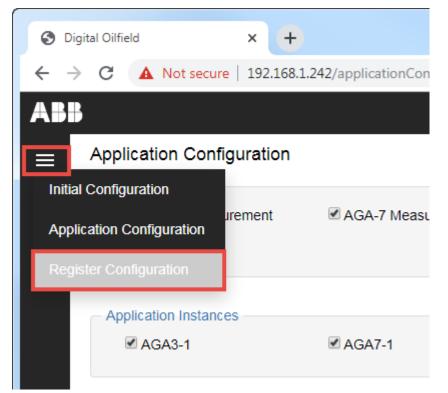
IMPORTANT NOTE: Registers are listed as variable names not numbers. There may be some data category or variable names that do not match register groups or names shown in PCCU tabs.

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

۲	Digi	tal Oilfield	×	+						_
←	\rightarrow	C A Not secure	192.1	L68.1.242/register	Config				☆ \varTheta :	
A	B							¢ 🔵	root (i) E	
≡		Register Configurat Select Application : Select App Instance : Select All Registers	tion	AGA-3 Me API Liquid AGA3-1		 AGA-7 Measurement Gas Lift AGA3-2 	Plunger Control	Shutdown System		
		Aggregate Today's Volume Yesterday's Mas Accumulated Er	ss		 Today's M Yesterday 		 Today's Energy Accumulated Volume 	 ✓ Yesterday's Volume ✓ Accumulated Mass 	Select All	
		Application							Select All	ł
		Static Pressure			Ø Differentia	I Pressure	Flow Rate	Flowing Temperature	1	
		Energy Rate			Mass Rate	e	Device/APP ID	Tube Description		
		Enhanced Mode	е		Facility Me	easurement Point	Company Name	Contract Hour		
		Vol Calc Period			Volume Lo	og Period	Calculation Type	Vol. Unit - Flow Rate		
		Composition							Select All	
		Heating Value I	ive 🭙	Th and Ph	🖉 Real Rela	tive Density live @ Th and	N2 Content	CO2 Content	1	J
								Read Config	Update Config	

- 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.

Oigital Oilfield × + ← → C ▲ Not secure | 192.168.1.242/registerConfig ☆ **A** : ABB ۵ ĵ ⊡ root **Register Configuration** ≡ Select Application : AGA-3 Measurement AGA-7 Measurement Plunger Control Shutdown System API Liquid SU Gas Lift Select App Instance : AGA3-1 O AGA3-2 Select All Registers Select All Aggregate Today's Mass Today's Volume Today's Energy Yesterday's Volume Yesterday's Energy Accumulated Volume Accumulated Mass Yesterday's Mass Accumulated Energy Select All Application Static Pressure Differential Pressure Flow Rate Flowing Temperature Energy Rate Mass Rate Device/APP ID Tube Description Enhanced Mode Facility Measurement Point Company Name Contract Hour Vol. Unit - Flow Rate Vol Calc Period Volume Log Period Calculation Type Composition -Select All Heating Value Live @ Th and Ph Real Relative Density live @ Th and N2 Content CO2 Content 1 Read Co Jodate Config

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.
 - Update configuration as described in section <u>5.4</u>.

5.3 Disable register data publishing

i

4.

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 <u>5.4</u>.

5.4 Update register configuration

To update register configuration:

- 1. Enable or disable registers as described in sections <u>5.2</u> and <u>5.3</u>.
- 2. Click Update Config.

Figure 5-4: Update Register Configuration

\rightarrow	C A Not secure 192.1	68.1.242/registerConfig				☆ \varTheta
BB					¢ 🌒	root 🛈
Г	Register Configuration					
	Select Application :	AGA-3 Measurement API Liquid SU	AGA-7 Measurement Gas Lift	Plunger Control	Shutdown System	
	Select App Instance :	AGA3-1	AGA3-2			
	Select All Registers					Select All
	Today's Volume	Today's	Mass	Today's Energy	Yesterday's Volume	
	Yesterday's Mass	Yesterda	ay's Energy	Accumulated Volume	Accumulated Mass	
	Accumulated Energy					
	Application					Select All
	Static Pressure	Different	ial Pressure	Flow Rate	Flowing Temperature	
	Energy Rate	Mass Ra	ite	Device/APP ID	Tube Description	
	Enhanced Mode	Facility N	Measurement Point	Company Name	Contract Hour	
	Vol Calc Period	Volume I	Log Period	Calculation Type	Vol. Unit - Flow Rate	
	Composition					Select All
	Heating Value Live @	Th and Ph 🛛 🕅 Real Rel	ative Density live @ Th and	N2 Content	CO2 Content	1
					Read Config	Update Config

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

6 Troubleshooting device connection errors

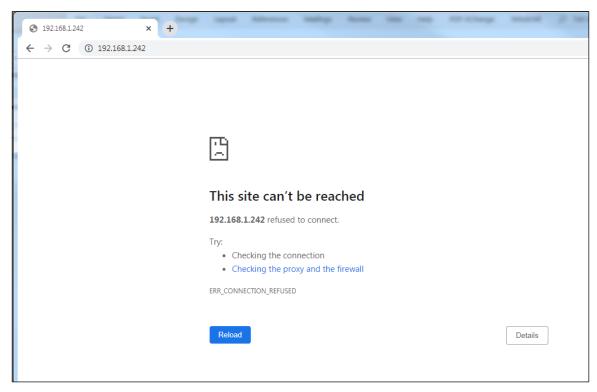
6.1 User-device connection failure

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

S 169.254.0.11 × +	
\leftrightarrow \rightarrow C (1) https://169.254.0.11	☆ 🕚 :
This site can't be reached	
https://169.254.0.11/ is unreachable.	
Try running Windows Network Diagnostics.	
ERR_ADDRESS_UNREACHABLE	
Reload	

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



6.1.1 Checklist to resolve failure to connect to field device

<u>Table 6-1</u> 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.

Problem	Cause	Resolution
Connection failure	Disabled MQTT	– Enable MQTT as described in section 10.1 .
	Incorrect URL	 Verify the URL required for the device. It should include the device IP address and the TCP port. For example: http://<device's address="" ip="">:443</device's> Type the correct URL on the browser and retry connection
	Incorrect IP configuration on the field device	 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	 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	 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 <u>Additional information</u> for link to advanced Ethernet troubleshooting.
	Connection failure on the field device network	 Onsite: 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.

Table 6-1: Basic troubleshooting

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.

Q 4	Artifactory × 📀	Digital Oilfield × +		
÷ -	C A Not secure https://1	169.254.0.11/initialConfig		☆ 👶 :
AB	₿			🗢 🔵 root 🛈 🕞
≡	Initial Configuration			
	General Protocol	Standard MQ ⁻ Oevice is not o	connected to MQTT Broker	ABBLighthouseIOTStaging.azure-device
	Device Parameters Device Timezone 💿	(UTC-06)Cent	Clu	See Certificates •
	Device ID	RMCPinyonSite	Root Certificate	Choose File root.ca.cer.cer
	Publish Interval (in seconds)	10	Client Certificate	Choose File client-cert.pem
	Data Polling Interval (in seconds)	1	Client Key	Choose File client-key pem
	·		Username	ABBLighthouseIOTStaging,azure-device
	MQTT Configuration Parameters QoS	s 1 ▼	Password	
	Will Details	true 🔻		
	Will Topic	devices/RMCPinyonSite/messages/even		
	Will Message	OFFLINE		
			Rez	ad Config Update Config Connection Status Reset

Figure 6-3: Device-broker connection failure



S Digital Oilfield ×	+		
← → C ▲ Not secure https://	/192.168.1.242/initialConfig		☆ 😩 :
ABB			🗢 🔵 root 🛈 🕞
Initial Configuration			
General	_		
Protocol	Standard N Standard N	tificate, Client Certificate, Key	192.168.8.10
			1883
Device Parameters		Close	
Device Timezone ?	(UTC-06)C		Certificates
Device ID	RMC-100	Root Certificate	Choose File No file chosen
Publish Interval (in seconds)	30	Client Certificate	Choose File No file chosen
Data Polling Interval (in seconds)	1	Client Key	Choose File No file chosen
		Username	ABB
MQTT Configuration Parameter	rs	Password	
QoS	0 •		
Will Details	true 🔻		
Will Topic	devices/RMC-100/messages/eve		
Will Message	OFFLINE		
		Read Config Up	odate Config Connection Status Reset

6.2.1 Resolve failure to connect to cloud broker

<u>Table 6-2</u> 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.

Problem	Cause	Resolution			
Connection failure	Incorrect MQTT broker details, device not able to establish TCP and MQTT connection	 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	 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)	 Determine if a username and password are required in addtion to certtificates. Azure requires a username for additional security. Amazon Web Services (AWS) does not. For MQTT servers in Sparkplug implementations, consult with your adminstrator. Obtain and configure username or password if required. 			

Table 6-2: Basic troubleshooting checklist

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 <u>Additional information</u>), 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.

•
1

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 the that 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 (<u>Figure 6-5</u>), 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.

🕵 PuTTY Configuration	? ×
Category:	
Category: Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour Translation Selection Colours Connection Proxy Telnet Rlogin Serial	Basic options for your PuTTY session Specify the destination you want to connect to Host Name (or IP address) Port [192.168.1.242 9696 Connection type: Raw Raw Telnet Rlogin Coad, save or delete a stored session Serial Load, save or delete a stored session Saved Default Settings Load Save Delete Close window on exit: Always Never Only on clean exit
About Help	Open Cancel

Figure 6-5: PuTTY configuration – Session parameters

4. On the navigation tree select **Connection**> **SSH**> **Auth** (<u>Figure 6-6</u>). **Figure 6-6: Configure authentication key**

🕵 PuTTY Configuration		? ×
Category:		
Features	*	Options controlling SSH authentication
Window Appearance		Display pre-authentication banner (SSH-2 only)
Behaviour		Bypass authentication entirely (SSH-2 only)
···· Translation ⊕ Selection		Authentication methods
Colours		Attempt authentication using Pageant
Connection Data		Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH-2)
Proxy		
	=	Authentication parameters
i⊷ Rlogin i⊐· SSH		Allow agent rorwarding Allow attempted changes of usemame in SSH-2
Kex		Private key file for authentication:
Host keys		Browse
GSSAPI		
TTY X11		
Tunnels	-	
About	lelp	Open Cancel

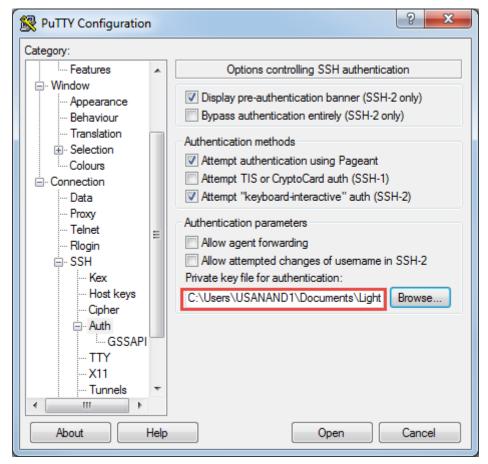
5. Click **Browse** to locate and select the key to authenticate (Figure 6-7).

Figure 6-7: Locate and select the authentication key

🕵 Select private key file					×
Search Results in Documents + det	efault acces keys RMC 🕨		•	Search default ac	cces keys RMC 🔎
Organize 🔻 New folder				:==	• 🔳 🔞
☆ Favorites	^ Name	*	Date modified	Туре	Size
🧮 Desktop	📕 Filezilla Installa	ition software	12/12/2019 5:19 PM	File folder	
📕 Downloads	🔹 customerservi	ce.ppk	12/12/2019 4:56 PM	PuTTY Private Key	2 KB
🖳 Recent Places	🔹 rootusr - RMC	G5uFlo.ppk	12/12/2019 4:58 PM	PuTTY Private Key	2 KB
 OneDrive - ABB 	E rootusr.ppk		12/12/2019 4:58 PM	PuTTY Private Key	2 KB
🔀 Windchill Documents	🔹 totalflowuser.p	opk	12/12/2019 4:58 PM	PuTTY Private Key	2 KB
 ABB Desktop Libraries Documents Git Music Pictures Videos Ana D. Andujar Comouter 	•				
File name: rootusr.ppk				PuTTY Private Key	
				Open 🔻	Cancel

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

Figure 6-8: Configure path to authentication key



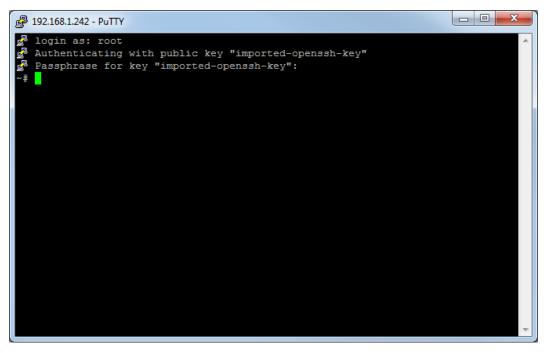
7. Click **Open**. The SSH terminal displays with the login prompt (Figure 6-9).

Figure 6-9: SSH terminal login prompt

國 192.168.1.242 - PuTTY	x
g ⁸ login as:	^
	Ŧ

- 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. <u>Figure 6-11</u> shows that all three processes are running in the device.

Figure 6-11: Verify processes are running correctly

P 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
- matt
- CoreDumps



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

E FileZilla						
File Edit View Transfer Server	Bookmarks Help					
Site Manager	Ctrl+S	1 🖉 🧥				
Copy current connection to Site	Manager	ssword:	Port:	Quickconnect	1	
New tab	Ctrl+T		Pole	Quickconnect		A
Close tab	Ctrl+W					<u> </u>
Export Import		anslation project\SSI	H SFTP Key Update	e procedure\sftp Pics\SSH SFT	P KEYS\rootusr.ppk"	
Show files currently being edited	Ctrl+E					=
Exit	Ctrl+Q					-
Local site: late procedure\sftp Pics\S	SH SFTP KEYS\Replacement	t key\Public Key\ 🔻	Remote site:			-
Public Key A RoboHelp Training RobohelpProcedures						
Filename	Filesize Filetype	Last modifie	Filename	Filesize File	type Last modified	Permissi
₩ Userkey.bt	397 Text Docu	ment 6/27/20194:		Not connected to	any server	
•		Þ	•			÷.
1 file. Total size: 397 bytes			Not connected.			
Server/Local file Dire	ection Remote file		Size Priority	Status		
Queued files Failed transfers S Opens the Site Manager	uccessful transfers				Queue: empty	

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

Site Manager	X
Select entry:	General Advanced Transfer Settings Charset
Bare Bare Bare Bare Bare Bare Bare Bare	Protocol: SFTP - SSH File Transfer Protocol 🔹
-	Host: 169.254.0.11 Port: 9696
	Logon Type: Key file 🔻
	User: root
	Key file: C:\Users\USANAND1\Documei Browse
	Background color: None
New site New folder	*
New Bookmark Rename	
Delete Duplicate	v
	Connect OK Cancel

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

Enter password						
Please enter a password for this server:						
Name: New site						
Host: 192.168.1.242:9696						
User: root						
Challenge:						
Passphrase for key "imported-openssh-key" in key file "C:\Users\USANAND1\Documents\RMC translation project\SSH SFTP Key Update procedure \sftp Pics\SSH SFTP KEYS\rootusr.ppk"						
	-					
Password:						
Remember password until FileZilla is closed						
OK Cancel						

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) (<u>Figure 6-15</u>).

7 New site - sftp://root@192.168.1.24	42:9696 - FileZilla						x
File Edit View Transfer Server	Bookmarks Help						
	8 😣 📜 💷	्र 🧧 🧥					
Host: Usernam	e:	Password:	Port:	Quickconnec	t 💌		
Response: fzSftp started, protocol_version=8 Command: keyfile "C:\Users\USANAND1\Documents\RMC translation project\SSH SFTP Key Update procedure\sftp Pics\SSH SFTP KEYS\rootusr.ppk" Command: open "root@192.168.1.242" 9696 Command: Trust changed Hostkey: Once Command: Pass: ***********************************							
Local site: late procedure\sftp Pics\S	SH SFTP KEYS\Replacem	ent key\Public Key\ 👻	Remote site: /r	oot			-
• · · · · · · · · · · · · · · · · · · ·	Public Key p Training pProcedures	•					
Filename	Filesize Filetyp	e Last modifie	Filename	Filesize	Filetype	Last modified	Permissi
₩ userkey.txt	397 Text Do	ocument 6/27/2019 4	 .ssh .bash_history .bash_logout .bash_profile	175	-	12/6/2019 2:25: 7/1/2019 3:40:3 7/1/2019 3:40:3 7/1/2019 3:40:3	drwxr-x- -rw-r -rw-r -rw-r
٠ [11	- F	•	III			۰.
1 file. Total size: 397 bytes 3 files and 1 directory. To							
Server/Local file Dire	ection Remote file		Size Priority	Status			
Queued files Failed transfers S	uccessful transfers						
					🔒 🕜 Quei	ue: empty	••

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.

R New	site - sftp://root@192.168.1.24	12:9696 - FileZill	3						X
File Ed	lit View Transfer Server	Bookmarks H	lein						
		* • = =		- A6.					
- ₩ -		s 🔮 . 🗙	/ I I Q 🤇	00					
Host:	Usernam	2:	Passwo	ord:	Port:	Quickconnec	t 💌		
Status:	Starting download of								*
Status:	File transfer successfu			cond					
Status: Status:	Starting download of File transfer successfu			cond					
Status:	Starting download of								
Status:	File transfer successfu								
Status:	Starting download of								
Status:	File transfer successfu								
Status:	File transfer successfu	l, transferred 6,1	27,616 bytes in 2	seconds					-
Local sit				-	Remote site: /mmcData				•
		rmation		*					<u> </u>
	🗄 🕌 Temp				🖃 🌗 mmcData				
	IFDOWNLOAD_TEN				CoreDump	s			
	Totalflow device log	s		*	Logs				-
Filenam	e	Filesize	Filetype	Last modifie	Filename	Filesize	Filetype	Last modified	Permissi
I					퉲				
🛯 📔 Logs			Local Disk	12/12/2019	CoreDumps		File folder	7/22/2019 3:47:	drwxr-xr
					📗 Logs		File folder	12/12/2019 12:	drwxr-xr
					퉬 lost+found		File folder	1/23/2019 2:45:	drwx
					퉬 mqtt		File folder	12/6/2019 2:26:	drwx
					📗 Registry		File folder	1/23/2019 2:44:	drwxr-xr
					📗 tfData		File folder	12/12/2019 12:	drwxr-xr
					~				
•	1	11		E F	•				F.
1 directo	ry				Selected 1 directory.				
Server/L	.ocal file Dire	ction Remote	file		Size Priority Status				
		1							
Queue	d files Failed transfers	Successful tra	ansfers (11)						
							🔒 🕐 Que	eue: empty	••

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

Rew site - sftp://root@192.168.1.242:9696 - FileZilla					
File Edit View Transfer Server Bookmarks Help					
Host: Username: Password:	Port: Quickconnect				
Status: Starting download of /mmcData/Logs/kernel.log Status: File transfer successful, transferred 32,768 bytes in 1 second Status: Starting download of /mmcData/Logs/MqtProcess.log Status: File transfer successful, transferred 32,768 bytes in 1 second Status: Starting download of /mmcData/Logs/KqtProcess.log Status: Starting download of /mmcData/Logs/kernel.log.bck4 Status: File transfer successful, transferred 32,768 bytes in 1 second Status: File transfer successful, transferred 174,620,672 bytes in 121 seconds Status: Disconnected from server Status: Disconnected from server	^ 				
Local site: C:\Totalflow device logs\	Remote site: /mmcData 👻				
System Volume Information Temp TFDOWNLOAD_TEMP Totalflow device logs	CoreDumps Logs				
Filename Filesize Filetype Last modifi	Filename Filesize Filetype Last modified Permissi				
₩	Image: State of the state				
4	< Refresh +				
Empty directory.	Selected 1 direc Delete				
Server/Local file Direction Remote file	Size Priority Rename Copy URL(s) to clipboard File permissions				
Queued files Failed transfers Successful transfers (54)					
	🔒 🞯 Queue: empty 🛛 👄 🚊				

 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)

New site - sftp://root	@192.168.1.242:9696	6 - FileZilla							×
File Edit View Tran	sfer Server Book	marks Help							
	Process Queue		Ctrl+P						
Host:	Default file exists ac	tion			Port:	Quickconnec	t		
Status: Re	Transfer type		· · F						*
Status: Li	Preserve timestamp	s of transferred files	Ctrl+U						
Status: Di Status: Re	Speed limits		•						
Status: Re Status: Lis			~						
Status: Di	Manual transfer		Ctrl+M						
	ng directory listing o	f "/mmcData"							
	directory /mmcData								
Status: Director	y listing of "/mmcDa	ata successful							-
	device logs\		•	Remote si	ite: /mmcData				-
	n Volume Informatio	'n	^	· · · · · · · ·					
E Temp				••• 					
	WNLOAD_TEMP				CoreDumps	;			
l otain	low device logs				- 📙 Logs				-
Filename		Filesize Filetype	Last modifi	Filename	·	Filesize	Filetype	Last modified	Permissi
📲									
				CoreD	umps		File folder	7/22/2019 3:47:	drwxr-xr
				🔒 Logs			File folder	12/12/2019 12:	drwxr-xr
				🛯 📗 lost+fo	ound		File folder	1/23/2019 2:45:	drwx
				🃗 mqtt			File folder	12/6/2019 2:26:	drwx
				🔒 Registi	ry		File folder	1/23/2019 2:44:	drwxr-xr
				🔒 tfData			File folder	12/12/2019 12:	drwxr-xr
•			•	•					F.
Empty directory.				Selected 1	directory.				
Server/Local file	Direction	Remote file		Size Pri	ority Status				<u>_</u>
sftp://root@192.168.1	.242:9								
C:\Totalflow device	logs\C <	/mmcData/CoreDump	s/core 165,	L83,488 No	rmal				
C:\Totalflow device	logs\C <	/mmcData/CoreDump	core 174,	776,320 No	rmal				
C:\Totalflow device	-	/mmcData/Logs/Totalf		244,836 No	rmal				-
Queued files (27) Fa	iled transfers Suc	cessful transfers (54)							
							🔒 🕐 Que	eue: 331.6 MiB	••

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

Figure 6-19: Log transfer progress bar and status

E New site - sftp://root@192.168.1.242:9696 - FileZilla						X
File Edit View Transfer Server Bookmarks Help	File Edit View Transfer Server Bookmarks Help					
	T 🔍 🍳 🧥					
	= ⋈ ⋈ 00					
Host: Username:	Password:	Port:	Quickconnec	t		
Status: Retrieving directory listing of "/mmcData"	"					*
Status: Listing directory /mmcData Status: Directory listing of "/mmcData" successfu	d.					
Status: Connecting to 192.168.1.242:9696	11					
Status: Connecting to 192.168.1.242:9696						
Status: Connected to 192.168.1.242 Status: Connected to 192.168.1.242						
Status: Connected to 192.108.1.242 Status: Starting download of /mmcData/CoreDur	mps/core System EFMColle.5	63				
Status: Starting download of /mmcData/CoreDu						-
Local site: C:\Totalflow device logs\	•	Remote site: /mmcData				
	*					<u> </u>
i ⊕∰ Temp 		in mmcData				
Totalflow device logs	-	Logs				-
Filename Filesize File	etype Last modifie	Filename	Filesize	Filetype	Last modified	Permissi
		J				
CoreDumps Loo	cal Disk 12/12/2019	CoreDumps		File folder	7/22/2019 3:47:	drwxr-xr
		퉬 Logs		File folder	12/12/2019 12:	drwxr-xr
		lost+found		File folder	1/23/2019 2:45:	drwx
		🌆 mqtt		File folder	12/6/2019 2:26:	drwx
		legistry		File folder	1/23/2019 2:44:	
		퉬 tfData		File folder	12/12/2019 12:	drwxr-xr
·		•				
1 directory		Selected 1 directory.				
Server/Local file Direction Remote file		Size Priority Status				<u>^</u>
sftp://root@192.168.1.242:9	💂 sftp://root@192.168.1.242:9					
C:\Totalflow device logs\C < /mmcData/CoreDumps/core 165,183,488 Normal Transferring						
00:00:02 elapsed 00:01:53 left 2.5% 4,292,608 bytes (1.4 MiB/s)						
C:\Totalflow device logs\C < /mmcData/CoreDumps/core 174,776,320 Normal Transferring						
Queued files (27) Failed transfers Successful transfers (54)						
Cancel current operation				🔒 🕐 Que	ue: 331.6 MiB	

- 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 (<u>Figure 6-20</u>).
- 12. Provide files to ABB technical support or developers.

Figure 6-20: Verify file download

Rew site - sftp://root@1	192.168.1.242:9696 - File	lilla						X
File Edit View Transfe	File Edit View Transfer Server Bookmarks Help							
	1 • R • • • • • • • • • • • • • • • • •							
Host:	Username:	Passwor	d:	Port:	Quickconnec	t		
	ownload of /mmcData/m							*
	er successful, transferred ownload of /mmcData/m							
	er successful, transferred							
	ownload of /mmcData/m							
	er successful, transferred		nd					
	ownload of /mmcData/m er successful, transferred		nd					_
	er successful, transferred							-
		-						
Local site: C:\Totalflow de	2		•	Remote site: /mmcData				
	olume Information		^					
	NLOAD TEMP			CoreDumps				
I T T	v device logs		-	Logs	2			-
	_	E 11 - 1						
Filename	Filesiz	e Filetype	Last modifie	Filename	Filesize	Filetype	Last modified	Permissi
<u>.</u>				Jan 1997 - 1997				
CoreDumps		Local Disk	12/12/2019	CoreDumps		File folder	7/22/2019 3:47:	drwxr-xr
Logs		Local Disk	12/12/2019	Logs		File folder	12/12/2019 12:	drwxr-xr
퉬 mqtt		Local Disk	12/12/2019	lost+found		File folder	1/23/2019 2:45:	
				mqtt		File folder	12/6/2019 2:26:	drwx
				Registry		File folder	1/23/2019 2:44:	
				鷆 tfData		File folder	12/12/2019 12:	drwxr-xr
•			•	٠	m			F.
3 directories				Selected 1 directory.				
Server/Local file	Direction Remo	te file		Size Priority Status				
Queued files Faile	d transfers Successfu	transfers (81)						
						🔒 🕜 Que	ue: empty	کې کې

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.	



1

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	If physical or network connection causes have been eliminated, restart the MQTT functionality on both device and MQTT server:
	Ignition server functionality (for example an expired Ignition license).	 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 <u>10.1.</u>

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 <u>Table 1-4</u>.
- 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 <u>Figure 7-1</u> 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

ABB Digital Oilfield Username: Username
Username:
Username:
Username:
Username:
Usemame
osemalite
Password:
Password
Submit

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

Digital Oitfield			🛒 🌲 Ana A	ndujar (i) [
List Of Devices				(
Name	Location	IP Address	Date Time	Status
RMC-01	Measurement and Control	192.168.1.41	10/25/2019 03:01:55 AM	•
SYS_TEST_PRO2	Measurement and Control	192.168.1.56	10/26/2019 05:02:49 PM	•
			« < Pa	age 1 of 1 >

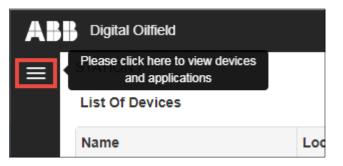
7.2 Navigate to devices and applications

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:

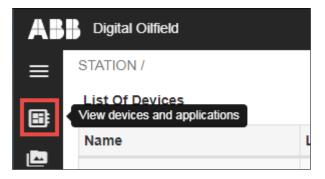
1. Click the menu icon (Figure 7-3).

Figure 7-3: Menu icon



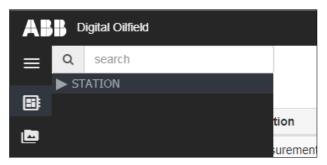
2. Click the device and application view icon (Figure 7-4).

Figure 7-4: Device and application view icon



The navigation tree displays (<u>Figure 7-5</u>). 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

AB	Bigital Oilfield		Last Refresh Tir	me: 11/11/2019 02:47:49	РМ ም 🜲 🚢 А	na Andujar (🕞
≡	Q search		General		Versions	
	 STATION 360_Dev_Device_Test 		Digital Board Pa	2105023	Flash Software	2.3.0-4
	365_Dev_Device_Test 365_Dev_Device_Test SYS_TEST_PRO2		Flash Software	2105457-029	OS Software Ve	2.2.0-3
۵	▼ RMC-01 ●		OS Software Pa	2105411-032	On-board IO So	2.3.0-4
	► AGA3-1 ► SULIQ-1	4	On-board IO BL	2105458-003	On-board IO BL	1.0.1-29
	 ▶ AGA7-1 ▶ AGA3-2 	1	Registry Application Profile	AGA3/AGA7 St	Lithium Backup Bat	tery 01/15/2014 mm/
	▶ Plunger ▶ Gas Lift		Software Descri	G5RMC Source	Rated Capacity	2200 mAH
			Factory Configu	44	Event Capacity	1550 mAH
			Power Supply Batter	y 10/01/2013 mm/	Backup Current	0.13 mA
		tes	Rated Life	73.05 Months	Depleted Capacity	2873 mAH
		tes	Event Aae	7.13 Months	Lithium Battery	ОК

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 age 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. <u>Figure 7-7</u> shows the first AGA3 instance selected.

Figure 7-7: Navigate to application instance pages

ABB Digital Oilfield									
≡	Q search								
	365_Dev_Device_Test								
=	SYS_TEST_PRO2								
_	▼ RMC-01 ●								
	AGA3-1								
۵	Application								
•	Aggregate								
	Composition								
	Digital Outputs								
	Last Calculated								
	Custom Logs								
	Daily Logs								
	Alarms								
	Alarm Definitions								
	Trend Definitions								
	Fvents								

- 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

Bigital Oilfield			Last Refresh Time: 12/03/2	019 12:06:12 AM 🛛 👳 🛕	🛓 📥 Ana Andujar (i
STATION / SYS_TEST_PRO Static Pressure Different: Flowing Temperature		urs v Line Bar Local UTC	Tooltip 👥 🧳	Current Values Static Pressure	25 PSIA
				Differential Pressure	50 inH2O
100000000000000000000000000000000000000				Flowing Temperature	75 Deg F
			1144446666	Flow Rate	434.60 MCF/Day
				Energy Rate	18108.24 MBTU/Hour
		12/02/2019 08:33:00	PM	Mass Rate	1107.65 lbm/hour
		Static Pressure : 25	PSIA	Today's Energy	609339.22 MBTU
		Differential Pressure Flowing Temperature		Today's Volume	609.34 MCF
16:06 16:44 17:09 17:34	18:00 18:26 18:51 19:16 19:	42 20:08 20:33 20:58 21:24 21:50 2	22:15 22:40 23:06 00:06	Today's Mass	37272.17 lbm
General		Units and Periods		Constants	
Device/APP ID	AGA3-1	Vol Calc Period	1 second	Orifice Diameter	1.60 in
Tube Description	TotalFlow	Volume Log Period	1 minute	Pipe Diameter	3 in
Contract Hour	1	Hold TimeOut (Seconds)	3700	Pressure Base (Pb)	20 PSIA
Calculation Type	AGA3-2012	Vol. Unit - Flow Rate	MCF - MCF/Day	Temperature Base (Tb)	70 Deg F
Fpv Method	NX19 GCN	Analysis Cycle Time	3600 seconds	Auxiliary Factor (Faux)	1.60
				Barometric Pressure	

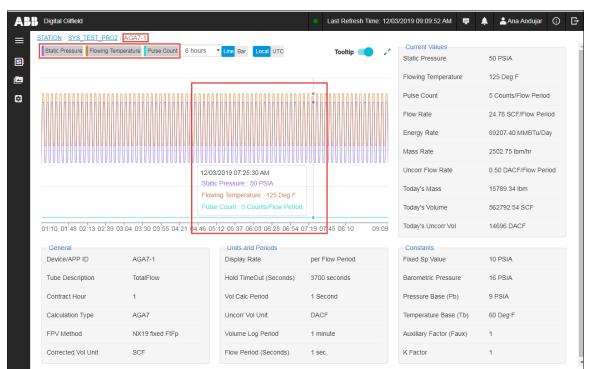
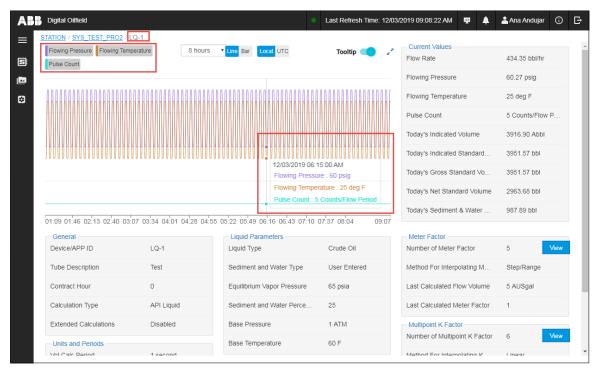


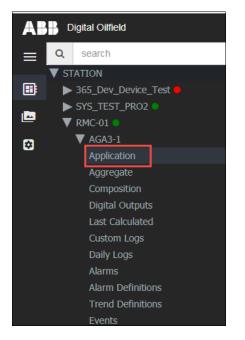
Figure 7-9: Pulse meter gas measurement (AGA7) main page

Figure 7-10: API SU Liquid main page



5. To view additional data for an application instance, select the data category of interest. Figure $\frac{7-11}{1}$ shows the Application page selected for the AGA3-1 instance. Sections $\frac{7.3.1}{7.3.1}$ to $\frac{7.3.11}{7.3.11}$ 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).

<u>Figure 7-12</u> 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.

Digital Oilfield			•	Last Refresh Time: 1	2/04/20 [,]	19 02:56:43 PM 🛛 👰 🔔	💄 Ana Andujar	()
STATION / SYS_TEST_PRO2	/ <u>AGA3-1</u> / Applicati	ion					3 0	Columns
Attached to stream	Stream 1	~	Flowing Temperature	75 Deg F	~	Speed of Sound Calculation	Disabled	~
Auxiliary Factor (Faux)	1.60	~	Fpv Method	NX19 GCN	~	Static Pressure	25 PSIA	~
Barometric Pressure	14 PSIA	~	H2O Bias	7 lbm/MMSCF	~	Stream ID	1	~
Base Density	0.05 lbm/ft3	~	Hold TimeOut (Seconds)	3700	~	Temperature Base (Tb)	70 Deg F	~
Base Density Source	Calculated from Real Relative	~	Mass Rate	1107.65 Ibm/hour	~	Tube Description	TotalFlow	~
Calculation Type	AGA3-2012	~	Orifice Diameter	1.60 in	~	Use Calc Cd	Yes	~
Contract Hour	1	~	Orifice Plate Exp. Coef.	9.25	~	Use Faux	No	~
Device/APP ID	AGA3-1	~	Orifice Reference Temperature	68	~	Use Fixed H2O	No	~
			Dina Diamatar		~			

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

ABI	Digital Oilfield			• Las	st Refresh Time: 12/05	5/2019 (05:11:34 AM 🛛 🕎 🔔	📥 Ana Andujar	0 E
≡	STATION / SYS_TEST_PRO2	2 / <u>AGA3-1</u> / Appl	ication					3 Cc	olumns 🔻
	Attached to stream	Stream 1	~	Flowing Temperature	125 Deg F	~	Speed of Sound Calculation	Disabled	~
	Auxiliary Factor (Faux)	1.60	~	Fpv Method	NX19 GCN	~	Static Pressure	50 PSIA	~
	Barometric Pressure	14 PSIA	~	H2O Bias	7 lbm/MMSCF	~	Stream ID	1	~
	Base Density	0.05 lbm/ft3	~	Hold TimeOut (Seconds)	3700	~	Temperature Base (Tb)	70 Deg F	~
	Base Density Source	Calculated from Real Relative	~	Mass Rate	2118.96 Ibm/hour	~	Tube Description	TotalFlow	~
	Calculation Type	Density AGA3-2012	~	Orifice Diameter	1.60 in	~	Use Calc Cd	Yes	~
			_	Orifice Plate Exp. Coef.	9.25	~	Use Faux	No	~

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.

Digital Oilfield STATION / <u>SYS_TEST_PRO</u>	2 / <u>AGA3-1</u> / Appli	cation	Last	Refresh Time: 12/05	6/2019 (05:09:44 AM 🖷 🌲	Ana Andujar	i E
Attached to stream	Stream 1	~	Flowing Temperature	125 Deg F	~	Speed of Sound Calculation	Disabled	~
Auxiliary Factor (Faux)	1.60	~	Fpv Method	NX19 GCN	~	Static Pressure	50 PSIA	~
Barometric Pressure	14 PSIA	^	H2O Bias	7 lbm/MMSCF	~	Stream ID	1	~
Cloud Access: Minimum:	Read 9		Hold TimeOut (Seconds)	3700	~	Temperature Base (Tb)	70 Deg F	~
Maximum:	16		Mass Rate	2118.96 Ibm/hour	~	Tube Description	TotalFlow	~
Base Density	0.05 lbm/ft3	~	Orifice Diameter	1.60 in	~	Use Calc Cd	Yes	~
Base Density Source	Calculated from Real	~	Orifice Plate Exp. Coef.	9.25	~	Use Faux	No	~

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 (<u>Figure 7-15</u>).

Figure 7-15: Aggregate parameters page

AB	Digital Oilfield			Last Refresh Time:	12/04/201	19 02:57:33 PM 🛛 👳 🙏	📥 Ana Andujar 🛛	ĵ ₽
≡	STATION / SYS_TEST_PRO2	/ AGA3-1 / Aggregate					3 Coli	umns 🔻
	Accumulated Energy	25458.08 MMBTU	Today's Energy	368119.43 MBTU	~	Yesterday's Energy	632997.91 MBTU	~
	Accumulated Mass	1557224.04 lbm	✓ Today's Mass	22517.19 lbm	~	Yesterday's Mass	38719.33 lbm	~
	Accumulated Volume	25458.08 MCF	✓ Today's Volume	368.12 MCF	~	Yesterday's Volume	633.00 MCF	~

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

AB	Digital Oilfield			Last Refresh Tir	ne: 12/05/2019	06:18:04 AM	₩ 🖡	占 Ana Andujar	© ₽
≡	STATION / SYS_TEST_PRO2	2 / AGA3-1 / Aggregate						3 Co	umns 🔻
	Accumulated Energy	25862.78 MMBTU	Today's Energy	139825 MBTU	i.53 🗸	Yesterday	's Energy	632997.91 MBTU	~
	Accumulated Mass	1581979.04 🗸	Today's Mass	8552.8	7 lbm 🗸 🗸	Yesterday	's Mass	38719.33 lbm	~
	Accumulated Volume	25862.78 MCF 💙	Today's Volume	e 139.83	MCF 💙	Yesterday	's Volume	633.00 MCF	~

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

AB	Bigital Oilfield			•	Last Refresh Time: 12/0	5/2019 0	16:19:54 AM 🛛 🐺	<u>ب</u>	🛓 Ana Andujar (D E
≡	STATION / SYS_TEST_PRO2	/ AGA3-1 / Aggregate	è						3 Colu	mns 🔻
	Accumulated Energy	25863.56 MMBTU	^	Today's Energy	140608.47 MBTU	~	Yesterday's Ene	rgy	632997.91 MBTU	~
	Cloud Access:	Read		Today's Mass	8600.76 lbm	~	Yesterday's Mas	s	38719.33 lbm	~
	Accumulated Mass	1582026.93 Ibm	~	Today's Volume	140.61 MCF	~	Yesterday's Volu	ime	633.00 MCF	~
	Accumulated Volume	25863.56 MCF	~							

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

Digital Oilfield	/ <u>AGA3-1</u> / Compositio	n				2019 06:34:34 AM 🛛 🖷 🔔	Ana Andujar	() lumns
Analysis Cycle Time	3600 seconds	~	Hydrogen Content	0 mol percent	~	n-Octane Content	0 mol percent	~
Argon Content	0 mol percent	~	i-Butane Content	0 mol percent	~	n-Pentane Content	0 mol percent	~
CO Content	0 mol percent	~	i-Pentane Content	0 mol percent	~	N2 Content	0 mol percent	~
CO2 Content	0 mol percent	~	Methane Content	0 mol percent	~	Oxygen Content	0 mol percent	~
Ethane Content	0 mol percent	~	n-Butane Content	0 mol percent	~	Propane Content	0 mol percent	~
H2O Content	0 mol percent	~	n-Decane Content	0 mol percent	~	Real Relative Density live @ Tb and Pb	0	~
H2S Content	0 mol percent	~	n-Heptane Content	0 mol percent	~	Use Fixed or Last Good on Error	Fixed	~
Heating Value Live @ Tb and Pb	0 BTU/SCF	~	n-Hexane Content	0 mol percent	~	Use Live Analysis	Yes	~

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

Bigital Oilfield				Last Refresh Time	: 12/05/2	2019 06:39:34 AM 🛛 🛒 🌲	💄 Ana Andujar 🤅
STATION / SYS_TEST_PRO:	2 / AGA3-1 / Compositio	n					3 Colum
Argon Content	0 mol percent	~	i-Butane Content	0 mol percent	~	n-Pentane Content	0 mol percent
CO Content	0 mol percent	~	i-Pentane Content	0 mol percent	~	N2 Content	0 mol percent
CO2 Content	0 mol percent	~	Methane Content	0 mol percent	~	Oxygen Content	0 mol percent
Ethane Content	0 mol percent	~	n-Butane Content	0 mol percent	~	Propane Content	0 mol percent
H2O Content	0 mol percent	~	n-Decane Content	0 mol percent	~	Real Relative Density live @ Tb and Pb	0
H2S Content	0 mol percent	~	n-Heptane Content	0 mol percent	~	Use Fixed or Last Good on Error	Fixed
Heating Value Live @ Tb and Pb	0 BTU/SCF	~	n-Hexane Content	0 mol percent	~	Use Live Analysis	Yes
Helium Content	0 mol percent	~	n-Nonane Content	0 mol percent	~		

5. 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.

	Oilfield	CA2.1 / Composition		•	Last Refresh Time	e: 12/05/2	2019 06:38:34 AM 🛛 🛒 🛕	💄 Ana Andujar	() ()
STATION	/ <u>515_1251_FR02</u> / A	<u>5A3-1</u> / Composition						3 Col	umns
Argon	Content	0 mol percent	~	i-Butane Content	0 mol percent	~	n-Pentane Content	0 mol percent	~
CO Co	ntent	0 mol percent	~	I-Pentane Content	0 mol percent	~	N2 Content	0 mol percent	~
CO2 C	ontent	0 mol percent	~	Methane Content	0 mol percent	~	Oxygen Content	0 mol percent	~
Ethane	Content	0 mol percent	~	n-Butane Content	0 mol percent	~	Propane Content	0 mol percent	~
H20 C	ontent	0 mol percent	~	n-Decane Content	0 mol percent	~	Real Relative Density live @ Tb and Pb	0	~
H2S Co	ontent	0 mol percent	~	n-Heptane Content	0 mol percent	~	Use Fixed or Last Good on Error	Fixed	~
Heating Tb and) Value Live @ Pb	0 BTU/SCF	~	n-Hexane Content	0 mol percent	~	Use Live Analysis	Yes	^
Helium	Content	0 mol percent	~	n-Nonane Content	0 mol percent	~	Cloud Access:	Read	

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

AB	Digital Oilfield				۰	Last R	efresh Time: 12/05	5/2019 06:48:14 AM	щ	٨	占 Ana Andujar	6	G
≡	STATION / SYS_TEST_PRO2 /	AGA3-1 / Digital Ou	tputs								3 (olumn	IS 🔻
	Trip Contact1 on Remote	No	~	Trip Contact1 on TF High		No	~	Trip Contact1 on N Sampler Setpoint	/olume		No		~
	Trip Contact1 on SP High	No	~										

To view digital outputs parameter values or details:

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

Figure 7-22: Expand parameter information display

ABB	Digital Oilfield				Last Ref	fresh Time: 12/05	6/2019 06:49:14 AM	Ţ	<u>ب</u>	💄 Ana Andujar	ĵ €
≡	STATION / SYS_TEST_PRO2	/ <u>AGA3-1</u> / Digital C	Outputs							3 (Columns 🔻
	Trip Contact1 on Remote	No	~	Trip Contact1 on TF High	No	~	Trip Contact1 on N Sampler Setpoint	/olume		No	~
	Trip Contact1 on SP High	No	~								

5. View additional parameter information and attributes (<u>Figure 7-23</u>). This example selects the Trip Contact1 on Remote parameter.

Figure 7-23: Additional parameter information and attributes

AB	Digital Oilfield				Last Refresh Ti	me: 12/05	5/2019 06:48:34 AM	<u>94.</u>	📥 Ana Andujar	í	G
≡	STATION / SYS_TEST_PRO2 /	AGA3-1 / Digital C	Dutputs						3 (Column	s ▼
	Trip Contact1 on Remote	No	^	Trip Contact1 on TF High	No	~	Trip Contact1 on V Sampler Setpoint	/olume	No		~
	Cloud Access:	Read									
	Trip Contact1 on SP High	No	~								

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

STATION / SYS_TEST_PRO2 /	AGA3-1 / Last Calculated						3 Colu	Imr
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

Digital Oilfield				Last Refres	h Time: 12	2/05/2019 08:16:24 AM 🛛 🖷 🌲	🛓 Ana Andujar	0 G
STATION / SYS_TEST_PRO	02 / AGA3-1 / Last Calculated						3 Colt	imns 🔻
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	~

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

Figure 7-26: Additional parameter information and attributes

ABI					Last Refresh	Time: 12	2/05/2019 08:33:14 AM 🛛 🖤 🌲	🛓 Ana Anduja	r i) E
≡	STATION / SYS_TEST_PRO2 / AG	A3-1 / Last Calculated						3 (Columns 🔻
	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	~
	Cloud Access: Minimum:	Read 0		Live Flowing Density	0 lbm/ft3	~	Relative Density	0.60	~
	Maximum:	100		Mass	0.59 lbm	~	Specific Heat Ratio	1.30	~
	CO2 Content	5 mol percent	~	Methane Content	5 mol percent	~	Static Pressure	50 PSIA	~
	Contract Barometric Pressure	14 PSIA	~	n-Butane Content	5 mol percent	~	Super Compressibility	1.00	~
	Differential Pressure	100 inH2O	~	n-Decane Content	5 mol percent	~	Temperature Corrected Orifice ID	1.60 in	~

7.3.6 View custom Logs

The Custom Logs page displays the values of application variables for the configured log period (<u>Figure 7-27</u>). 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	Energ
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.
- 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 ($\frac{\text{Figure}}{7-28}$).

Figure 7-28: Validate feature for custom logs

e/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 <u>7-29</u>). An invalid log shows a red X.

Figure 7-29: Validated log

Volume	Energy	Flow Time	Validate Valid Signature
0	0	0	Ò
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	Period Time	Sequence				Static Pressu	re		
Date/Time	(UTC)	(seconds)	Number	Alarms	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).

	Temperate	ure			Volume		Flow Time	Back Flow	O anter at the	Validate
TF Max	TF Min	TF %HI	TF %LO	Integral	volume	Energy	Flow Time	Back Flow	Contract Hr	valida
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid
125	75	0	0	53.44	633.00	633.00	86400	0	1	Valid

Figure 7-31: Validate feature for daily logs

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

Figure 7-32: Validated log

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

7.3.8 View alarms

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

i

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

Digital Oilfield			•	Last Refresh Time:	12/05/2019 11:27:44 A	м 🕶 🛓 🚣	Ana Andujar (🛛
<u>STATION</u> / <u>SYS_TE</u>	<u>ST_PRO2</u> / <u>AGA3-1</u> / <mark>Alarm</mark>	Definitions					(
Description	Input Variable	Condition	Threshold Value	Severity	Suppress	Filter Threshold	Alarm Type
AGA3-1 DP	differentialPressure	GT	80	Normal	Disabled	0 (sec)	Active
Jul						« <	Page 1 of 1 >

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.
- 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

AB	Digital Oilfield		۲	Last Refresh Time: 12/05/2019 11:46:14 AM	Ŷ	۴	占 Ana Andujar	()	Ð
≡		d Definitions							G
	Trend Definition	1 min 30 sec							
	Variables	Static Pressure Differential Pressure Flowing Temperature							

Figure 7-36: No trend definitions

ABB	Digital Oilfield	•	Last Refresh Time: 11/01/2019 11:30:11 AM	.ide	۰	🛓 Ana Andujar	6	Ð
	STATION / RMC-01 / A3-1 / Trend Def	initio	ns					с
	Trend Definition							Ŭ
	Interval		Not Available					
	Variables		Not Available					

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

STATION / RMC-01 / AGA3-1 Event Logs Audit Log					
Date/Time	Date/Time (UTC)	Sequence Number	Old Value	New Value	Description
12/06/2019 09:26:45 AM	12/06/2019 03:26:45 PM	145	06/00/00	18/09/30	Battery aging
11/25/2019 06:12:28 AM	11/25/2019 12:12:28 PM	138	06/00/00	18/09/19	Battery aging
11/10/2019 11:31:17 AM	11/10/2019 05:31:17 PM	111	06/00/00	18/09/04	Battery aging
Jul					< Page 1 of 1 >

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

<u>Table 7-1</u> 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.

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

Table 7-1: Plunger Control application page list

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).

Digital Oilfield	02 / Plunger-1		Last Re	efresh Time: 12	2/09/2019 11:40:09 PM	ም 🌲 🏝 Ai	na Andujar (
AP DP Temperature	-	nours V Line Bar Local UTC	Tooltip		Arrivals Arrival Time	Velocity(ft	Reason
					Not Available	Not Available	Not Available
15:40 16:15 16:39 17:0	13 17'27 17'51 18'15 18'39 19'03	13 19'27 19'51 20'15 20'39 21'03 2	1'27 21'51 22'15 22'39 3	23:03 23:39			
Current Well State		13 19'27 19'51 20'15 20'39 21'03 2 Timers		23:03 23:39	Last Plunger Arrival – Duration	5	View
	33 17:27 17:51 18:15 18:39 19:0: 25 PSIA 50 InH2O		1:27 21:51 22:15 22:39 3 00:00:00 00:00:00	23:03 23:39	Duration	5	View
Current Well State	25 PSIA	Timers Last Open Time	00:00:00:00	23:03 23:39		5 FAIL	View
Current Well State	25 PSIA 50 InH2O	Timers Last Open Time Last Close Time	00:00:00:00	23:03 23:39	Duration Current State		View
Current Well State AP DP Temperature	25 PSIA 50 InH2O 75 Deg F	Timers Last Open Time Last Close Time Hold Close Reason	00:00:00:00 00:00:00:00 None	23'03 23:39	Duration Current State ControllerState	FAIL	View
Current Well State AP DP Temperature Flow Rate	25 PSIA 50 InH2O 75 Deg F 434.60 SCF/Hr	Timers Last Open Time Last Close Time Hold Close Reason Current Open Reason	00:00:00:00 00:00:00 None None	23:03 23:39	Duration Current State ControllerState Main Valve State	FAIL Closed	
AP DP Temperature Flow Rate Casing	25 PSIA 50 InH2O 75 Deg F 434.60 SCF/Hr 0	Timers Last Open Time Last Close Time Hold Close Reason Current Open Reason Current Close Reason	00:00:00:00 00:00:00:00 None None	23'03 23.39 nable	Duration Current State ControllerState Main Valve State Plunger Status	FAIL Closed Drop	,
Current Well State AP DP Temperature Flow Rate Casing Tubing	25 PSIA 50 InH2O 75 Deg F 434.60 SCF/Hr 0 0 PSIA	Timers Last Open Time Last Close Time Hold Close Reason Current Open Reason Current Close Reason Plunger Control	00:00:00:00 00:00:00:00 None None Enable		Duration Current State ControllerState Main Valve State Plunger Status Cycle Status	FAIL Closed Drop Running	1 7:11

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

STATION / SYS_TEST_PRO2 / I	Plunger-1 / Plunger State						
State Plunger Control Mode	Enable •	Options	Option State	Current Settings	Afterflow	Option State	Current Setting
	Ellable *	Closing Valve			Flow Timer Close Option	Enabled	00:00:10:00
Start Mode	Previous *	Valve Close Check	Disabled		Afterflow Timer Close O	Disabled	00:00:00:00
ControllerState	FAIL	Valve Closed			Turner Flow Rate Close	Disabled	0
State Timer	00:00:07:11	Closed Timer Option	Enabled	00:00:01:00	Load Ratio Close Option	Disabled	0
Max State Timer	00:00:40:00	Tube-Line Open Option	Disabled	0	DP Low Close Option	Disabled	10
Plunger Status	Drop	C-L and T-L Open Option	Disabled		Flow Rate Close Option	Disabled	0
Cycle Status	Running	C-T and T-L Open Option	Disabled		Tube-Line Close Option		0
Main Valve State	Closed	Case-Line Open Option	Disabled	0	· · · · ·	Disabled	
Hold Close Reason	None	Case-Tube Open Option	Disabled	0	Case-Tube Close Option	Disabled	0
Current Open Reason	None	Load Ratio Open Option	Disabled	0	Tubing Pressure Close	Disabled	0
Closed Timer	00:00:00:00	Tubing Pressure Open	Disabled	0	Casing Pressure Close	Disabled	0
Last Close Time	00:00:00:00	Casing Pressure Open	Disabled	0	Static Pressure Close O	Disabled	0
Current Close Reason	None	Static Pressure Open O	Disabled	0			
Flow Cycle Timer	00:00:07:11	Hold Total Cycle Time	Disabled	00:00:00:00			
Last Open Time	00:00:00:00	Hold Plunger Fall Timer	Disabled	00:00:00:00			
Total Cycles	0	Hold High Line Option	Disabled	00:00:00:00			
		Hold Once Ontion	Disabled	00.00.00.00			
						Reset	Submit

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

AB	Digital Oilfield		Last Refresh Time: 12/10/2019 05:55:09 AM	₩	۰	🚢 Ana Andujar	(i)	G
	STATION / SYS_TEST_PRO2 / Plunger-1 / Plun	nger Valve Closed						
	Plunger Valve Closed							
	Controller State:	Not Available	Cycle Status:	Runnii	ng			
	Main Valve State:	Closed	State Timer:	00:00:	D7:11			
	Plunger Status:	Drop	Max State Timer:	00:00:	40:00			
	Tubing-Line		Tubing-Line Tuning					
	Tube-Line Open Option:	Disabled •	Tube - Line Pressure Open Tune Am	1				
	Tube - Line Pressure Open Limit:	0	Tube - Line Pressure Open Min Tune:	1				
	Tube - Line Pressure:	-36	Tube - Line Pressure Open Max Tune:	0				
	Case-Line and Tube-Line		Plunger Fail Factor Tune:	1.5	0			
	C-L and T-L Open Option:	Disabled •	Case-Tube and Tube-Line					
			C-T and T-L Open Option:	Dis	abled	*		
						Reset	Subr	mit

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

AB	Digital Oilfield		•	Last Refresh Time: 12/10/2019 05:57:10 A	∕1 ₩	۹	📥 Ana Andujar	G	G
≡	STATION / SYS_TEST_PRO2 / Plunger-1 / Plun	ger Arrived							
	Plunger Arrived (State 5)								
	Controller State:	Not Available		Cycle Status:	Runnir	g			
	Main Valve State:	Closed		State Timer:	00:00:	07:11			
	Plunger Status:	Drop		Max State Timer:	00:00:	40:00			
	Arrival Counts			Maintenance					
	Reset Plunger Counter	No		Cycles Available Before Maintenance	0				
	Consecutive Normal Arrivals	0		Total Cycles	0				
	Normal Arrival Count	0							
	Fast Arrivals Count	0							
	LateArrivalCount	0							
	Slow Arrivals Count	0							
							Reset	Subi	mit

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

AB	Digital Oilfield			• Li	ast Refresh Time: 12/10/2	2019 05:58:09 AM	¥	<u>۽</u>	占 Ana Andujar	í	G
≡	STATION / SYS_TEST_PRO2 /]	Plunger-1 Plunger Afterflo	W								
	AfterFlow (State 6)										
	Controller State:	Not Available	Cycle Status:	Ru	nning	Current Run Vol			User Disabled		
	Main Valve State:	Closed	State Timer:	00:	00:07:11						
	Plunger Status:	Drop	Max State Timer:	00:	00:40:00	Current Open Re	eason:		None		
	Flow Timer			A	fter Flow Timer						
	Flow Timer Close Option	Enable	j v		Afterflow Timer Close Op	tion	Disal	bled	Ŧ		
	FlowCycle Time Limit	00:00:1	0:00		AfterFlow Cycle Time Lin	nit	00:00	0:00:00	D		
	Flow Cycle Timer	00:00:0	7:11		AfterFlow Cycle Timer		00:00	0:00:00	C		
									Reset	Subr	nit

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

ABB Digital Oilfield		Last Refresh Time: 12/10/2019 05:59:09 AM	🛒 🌲 🏝 Ana Andujar 🛈 🕞
STATION / SYS_TEST_PRO2 / Plunger-1	Plunger Arriving		
Plunger Arriving (State 3)			
Controller State:	Not Available	Cycle Status: Runn	ning
Main Valve State:	Closed	State Timer: 00:00	00:07:11
Plunger Status:	Drop	Max State Timer: 00:00	0:40:00
Arrival Time Limits		Timers	
Plunger Arrival Max Time:	00:00:40:00	Last Plunger Arrival Time: 00:	:00:00:00
Plunger Arrival Slow Time:	00:00:30:00	Plunger Arriving Timer: 00: Arrivals	:00:07:11
Plunger Arrival Fast Time:	00:00:01:00	Max Arrivals Allowed: 10	
Plunger Arrival Min Time:	00:00:00:30	Max Arrivals Count: 0	
			Reset Submit

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

ABB Digital Oilfield		Last Refresh Time: 12/10/20	19 06:01:09 AM 👎 🌲 🏝 Ana Andujar (Ð
STATION / SYS_TEST_PRO2 / Plunger-1	Plunger Closing Valve			
Closing Valve (State 1)				
Controller State:	Not Available	Cycle Status:	Running	
Main Valve State:	Closed	State Timer:	00:00:07:11	
Plunger Status:	Drop	Max State Timer:	00:00:40:00	
- Timer				
Plunger Fall Delay Time Limit	00:00:00:30			
Fall Timer	00:00:00:00			
			Reset	Submit

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

	•	Last Refresh Time: 12/10/2019 06:05:10 AM	👳 🌲	🚢 Ana Andujar	()	G
STATION / SYS_TEST_PRO2 / Plunger-1 / Plunger Contro	-					
Well Geometry Tubing Length: 5		uning Optimization Option:	Disable •			
Tubing ID(inches): 2.00	in F	Plunger Fail Factor Tune:	1.50			
Fluid Gradient: 0.43		wabbing Swab Option:	Disable •			
Control Plunger Control Mode: Enab	ble 🔻	Swab Runs Limit:	0			
Reset Plunger Counter: No	Ŧ	Swab Runs Completed:	0			
Auto Main Value Commands	5	Swab Now:	No *			
Main Valve State: Close	ed					
Auto Production Valve Open Now: Auto	Ο Ορε 🔻					
Auto Production Valve Close Now: Auto	O Clo: T					
				Reset	Subm	iit

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

	Last Refresh Time: 12/10/2019 06:07:10 A	M 🐺 🌲 🏝 Ana Andujar 🛈 🗗
STATION / SYS_TEST_PRO2 / Plunger-1 / Plunger Afterflow Sub		
AF Timer	- Flow Rate	
Afterflow Timer Close Option Disabled •	Flow Rate Close Option	Disabled •
AfterFlow Cycle Time Limit 00:00:00	FlowRate Close Limit	0
AfterFlow Cycle Timer 00:00:00	Flow Rate	831.40 SCF/Hr
Tube-Line	FlowRate Low Time Limit	00:00:01:00
Tube-Line Close Option Disabled •	FlowRate Low Timer	00:00:00:00
Tube - Line Pressure -36	Flow Rate Limit Tune Amount	0
Tube-Line Close Limit 0	Flow Rate Limit Min Tune	0
	FlowRateLimitMaxTune	0
		Reset Submit

7.4.1.10 View the Plunger Valve Closed Sub page

To view the Plunger Valve Closed Sub page:

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

Figure 7-47: Plunger Valve Closed Sub page

Digital Oilfield		Last Refresh Time: 12/10/2019 06:08:09	9 AM 🖤 🌲 🏝 Ana Andujar 🤅
STATION / SYS_TEST_PRO2 / Plunger-1 / Plunger Val	ve Closed Sub		
Closed Timer		Hold Recovery	
Closed Timer Option	Enabled •	Hold Mandatory Recovery Option	Disabled •
Closed Timer	00:00:00:00	Mandatory Close State	Inactive •
Plunger Valve Closed Timer Limit	00:00:01:00	Mandatory Close Time Limit	00:00:00:00
Tube Line		Mandatory Close Timer	00:00:00
Tube - Line Pressure Open Max Tune	0	Close 1	
Tube - Line Pressure	-11	Close 1 Option	Enabled •
Tube - Line Pressure Open Limit	0	Close1 Close Action	Low Clos
Tube - Line Pressure Open Tune Amount	1	Close 1 Open Status	Inactive •
Tube - Line Pressure Open Min Tune	1	Close1 Hold Type	None *
C-T and T-L Open Option	Disabled *	Close1 Open Action	Low Rele *
C-L and T-L Open Option	Disabled •	Close1 Timer Limit	00:00:00

7.4.1.11 **View Alarms**

To view alarms:

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

Figure 7-48: Alarms

Digital Oilfield		Last Refresh Time:	12/10/2019 06:12:29 A	м ም 🌲	📥 Ana Anduj	jar (j	Ð
STATION / RMC-01 /	Plunger / Alarms						G
Date/Time	Date/Time (UTC)	Name	Value	Sequence Number	State	Severity	
		There is no	data to display				

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

AB	Digital Oilfield				•	Last Refresh Time: 1	12/10/2019 06:12:29 A	M 🕎		🛓 Ana	a Andujar	6	₿.
≡	STATION / RMC-01 / P	lunger / Alarm Definition	IS										G
	Description	Input Variable	Condition	Threshold Value	s	Severity	Suppress	Filter T	hresho	ld	Alarm Type	•	
	pl temperature	temperature	GT	0	٢	Normal	Disabled	0 (sec)			Active		
	v jul								¢	< F	Page 1 of 1	~	2

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.
- Move the mouse to the main screen area to hide the navigation tree and view the trend definitions. For simplicity, <u>Figure 7-50</u> 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 <u>7.5.7 View well configuration</u>.

Figure 7-50: Trend Definitions page

ABI	Digital Oilfield • Las	t Refresh Time: 12/10/2019 06:12:29 AM	.ide	۴	📥 Ana Andujar	6	G
≡	STATION / RMC-01 / Plunger / Trend De	finitions					c
	Trend Definition						
	Interval	1 min					
	Variables	Temperature					

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

Plunger Cycles										
Controller State:	Not Availab	le	Cycle St	atus:	Runnir	g	Closed	I Timer:	00:00:00:38	
Main Valve State:	Closed		State Tir	mer:	00:00:0	0:38	Hold C	lose Reason:	None	
Plunger Status:	Drop		Max Sta	te Timer:	00:00:0)1:00	Curren	t Open Reason:	None	
			Close Section	n						
Close Stamp	Reason	Time	Case	Tube	Line	Flow	Vol	Open Stamp	Reason	Tin
12/10/2019 06:10:02 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 06:11:34 AM	Not Available	00
12/10/2019 05:58:29 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 06:00:01 AM	Not Available	00
12/10/2019 05:46:56 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 05:48:28 AM	Not Available	00
12/10/2019 05:35:23 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 05:36:55 AM	Not Available	00
12/10/2019 05:23:50 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 05:25:22 AM	Not Available	00
12/10/2019 05:12:17 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 05:13:49 AM	Not Available	00
12/10/2019 05:00:44 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 05:02:16 AM	Not Available	00
12/10/2019 04:49:11 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 04:50:43 AM	Not Available	00
12/10/2019 04:37:38 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 04:39:10 AM	Not Available	00
12/10/2019 04:26:05 AM	Not Available	00:00:01:32	0.00	0.00	0.00	0.00	0.00	12/10/2019 04:27:37 AM	Not Available	00

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

AB	Digital Oilfield	٠	Last Refresh Tirr	e: 12/10/2019 06:37:10 AM	щ°	۴	🛓 Ana Andujar	i	G	
≡	STATION / SYS_TEST_PRO2 / Plun	nger-1 Events]						c	
	Event Logs								Ŭ	
	Date/Time	Date/Time (U	JTC) Reason				Value			
			There is no	data to display						

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

	YS_TEST_PRO2 / S	Shutdown				
Safety S	ystem Control	Enabled	Startup Startup Timer	0 seconds	Manual Timer Manual Timeout Enable	Enabled
Reset Re	emote	Inactive	Startup Delay	60 seconds	Manual Timer	0 seconds
Shutdow	n Remote	Inactive	Startup Action	Shutdown	Manual Delay	3600 seconds
System S	Status	Shutdown	Power Level Power Level	12.34 Volts	References Analog Input	Analog Input
Shutdow	n DO	Shutdown	Power Level High Limit	24 Volts	Digital Input	Digital Input
Current	Alarm Status	DI X	Power Level Low Limit	11.50 Volts	Digital Output	Digital Output
Last Eve	nt	PL-1 / SHUT/DI[4]	Power Level Enable	Disabled	Wells	Wells

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**.
- Move the mouse to the main screen area to hide the navigation tree and view shutdown 3. Application information.

Figure 7-54: Shutdown Application page

AB	Digital Oilfield				Last Refresh	n Time: 12/10	0/2019 06:37:10 AM 🕎 🌲	🚢 Ana Andujar 🛛 () F
≡	STATION / SYS_TEST_PRO2 / Shute	down / Application						3 Colu	imns 🔻
	Current Alarm Status	DI X	~	Power Level High Alarm	No	~	Shutdown DO	Shutdown	~
	Last Event	PL-1 / SHUT/DI[4]	~	Power Level High Limit	24 Volts	~	Shutdown Remote	Inactive	~
	Manual Delay	3600 seconds	~	Power Level Low Alarm	No	~	Startup Action	Shutdown	~
	Manual Timeout Enable	Enabled	~	Power Level Low Limit	11.50 Volts	~	Startup Delay	60 seconds	~
	Manual Timer	0 seconds	~	Reset Remote	Inactive	~	Startup Timer	0 seconds	~
	Power Level	12.34 Volts	~	Safety System Control	Enabled	~	System Status	Shutdown	~
	Power Level Enable	Disabled	~						

7.4.2.3 **View Events**

To view shutdown events:

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

Figure 7-55: Shutdown Events page

Digital Oilfield <u>STATION / SYS_TEST_PRO2 /</u> Event Logs Audit Logs				
Date/Time	Date/Time (UTC)	Reason	Description	Index
01/06/2020 07:46:33 AM	01/06/2020 01:46:33 PM	PL-1 / SHUT/DI[4]	DI x	3
12/19/2019 01:54:26 PM	12/19/2019 07:54:26 PM	PL-1 / SHUT/DI[4]	DI x	3
12/19/2019 10:36:11 AM	12/19/2019 04:36:11 PM	PL-1 / SHUT/DI[4]	DI x	3
12/19/2019 09:44:38 AM	12/19/2019 03:44:38 PM	PL-1 / SHUT/DI[4]	DI x	3
12/18/2019 10:47:06 AM	12/18/2019 04:47:06 PM	PL-1 / SHUT/DI[4]	DI x	3
Ju v				< Page 1 of 1 >

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

			Last Refresh Time: 12/1	10/2019 06:44:10 AM 🛛 🖳 🜲	🛓 Ana Andujar (
STATION / SYS_TEST_PRO2 / Gas Production AP Production DP Pro		Line Bar Local UTC	Tooltip 👥 🥜	Current Values Casing Pressure	115 PSIG
				Tubing Pressure	40 PSIG
				Inject Pressure	11 PSIG
	100000000000000000000000000000000000000			Prod Line Pressure	11 PSIG
				Inject AP	25
		12/10/2019 05:09:00 AM		Today's Production Volume	151.28 MCF
111000000000000000000000000000000000000		Production AP : 25		Today's Injection Volume	77.33 MCF
		Production DP : 50 Production TF : 75		Yesterday's Production Volume	633.00 MCF
		02:45 03:10 03:36 04:01 04:27 04		Yesterday's Injection Volume	323.56 MCF
22:45 23:21 23:46 00:12 00:37 0	01:03 01:28 01:54 02:19 0	02:45 03:10 03:36 04:01 04:27 04	54 05:19 05:46 06:43	Elow Rate	
Gas Lift Mode	Plunger	Hold Status	Run	Production Flow Rate	434.60 PSIG
Gas Lift State	Closed	Shutdown Status	Running	Net Flow Rate	212.47 PSIG
Gas Lift Enable	ON	Inject Valve Position	0	Registers	
Injection Tube Description	Injection Tube Test	Inject Flow Rate/ Setpoint	222.13	Production Tube	View
Production Tube Description	TotalFlow	Injection Setpoint	0	Injection Tube	View

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

	Digital Oilfield				Last Refresh Time:	12/10/201	19 08:45:59 AM 🖤 🌲	💄 Ana Andujar	0 F
≡	STATION / SYS_TEST_PRO	2 / <u>Gas Lift-1</u> Ap	plication					3 Co	lumns 🔻
	After Flow Assist	ON	~	Gas Lift Mode	Plunger	~	Plunger Valve State	Closed	×
	After Flow Multiplier	100	~	Gas Lift State	Closed	~	Pre-charge	OFF	~
	Afterflow Evaluation Time Limit	0	~	Hold Status	Run	~	Pre-charge High Casing Limit	0	~
	Afterflow Evaluation Timer Remaining	0	~	Inject AP	50	~	Pre-charge Injection Rate	0	~
	Afterflow Max Flow Rate	0	~	Inject Flow Rate/ Setpoint	424.99	~	Pre-charge Low Casing Limit	0	~
	Afterflow Remain	60	~	Inject Pressure	36 PSIG	~	Prod Line Pressure	36 PSIG	~
	Afterflow Time Limit	60	~	Inject Valve Position	0	~	Production Flow Rate	831.40 PSIG	~

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

AB	Digital Oilfield				Last Refresh Tim	e: 12/10/2	019 08:46:59 AM 👳 🎍	💄 📥 Ana Andujar	© ₽
≡	STATION / SYS_TEST_PRO2 / 0	Gas Lift-1 / <mark>Aggregate</mark>						3 Co	olumns 🔻
	Today's Injection Volume	104.87 MCF	~	Today's Production Volume	205.16 MCF	~	Yesterday's Net Volume	309.44 MCF	~
	Today's Net Volume	100.29 MCF	~	Yesterday's Injection Volume	323.56 MCF	~	Yesterday's Production Volume	633.00 MCF	~

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

cription Input Variable Condition		Threshold Value	Severity	Suppress	Filter Threshold	i Alarm Type		
GasLift-1 DP productionDP	GT	80	Normal	Disabled	0 (sec)	Active		

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

ABB		뿟	۰	📥 Ana Andujar	(j)	G	
STATION / SYS_TEST_PRO2 / Gas Lift-1 / Trend Definition	5						G
Trend Definition							
Interval	1 min 3	30 sec					
Variables	Product	tion AP					
	Product	tion DP					
	Product	tion TF					

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

AB	Digital Oilfield			Last Refresh Time: 12/	10/2019 09:24:39 AM	щe	۵	🚢 Ana Anduja	r (i)	G	Â
≡	<u>STATION</u> / <u>SYS_TEST</u>	_PRO2 / <u>Gas Lift-1</u> / Ev	rents							с	
	🖲 Event Logs 🔘 Au	idit Logs								Ū	
	Date/Time	Date/Time (UTC)	Mode	Event	Production Ra	ate	Injec	tion Rate	Critical	Rate	
				There	is no data to display						
											•

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:

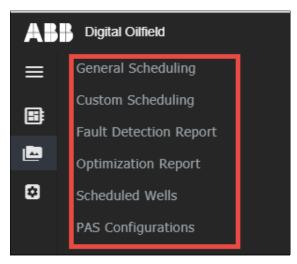
1. Click the PAS service icon (<u>Figure 7-62</u>).

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

AB	Digital Oilfield
≡	STATION /
s	List Of Devices
	Schedule PAS analysis, View PAS
	reports and more
\$	
	SYS_TEST_PRO2
	RMC-01

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.

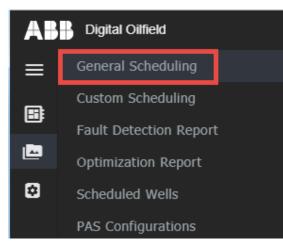
General scheduling supports two scheduling modes: daily or weekly. If these options do not meet your requirements, refer to section <u>7.5.3</u> <u>Schedule analyses for user-defined intervals</u>.

Analysis results are stored in reports and viewable based on type. See section <u>7.5.4 View Fault</u> <u>Detection reports</u> and <u>7.5.5 View Optimization reports</u>.

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

AB	Digital Olifield	<u>#</u>	Ļ	🛓 Ana Andujar	()	G
≡	General Scheduling					
	Scheduling Time Feature Details					
	Daily	ptimizat	tion			
\$	Device Details			S	elect A	
	365_Dev_Device_Test SYS_TEST_PRO2 RMC-01					
			[Reset Sc	hedule:	

- 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 <u>Figure 7-66</u> 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

AB	Digital Oiffield		₩ 🔶	🚢 Ana Andujar	0 E	• Î
≡	General Scheduling					
:: •	Scheduling Time Daily 11:30	Feature Details	Optimization			
۵	Device Details 365_Dev_Device_Test SYS_TEST_PRO2 RMC-01				Select All —	
	Well Details					
				Reset	chedule	-

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

AB	Digital Oilfield	Ψ		🚢 Ana Anduja	(j)	G
≡	Custom Scheduling					
	Date and Time					
	From: 12/09/2019 12:01 To: 12/10/2019 12:	01				
۵	Feature Details					
	Fault detection Optimization					
	Device Details 365_Dev_Device_Test SYS_TEST_PRO2 RMC-01				Select A	All
			[Reset	Schedule	

- 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

A	Digital Oilfield	.	Ana Andujar	()	G
≡	Custom Scheduling				
::: •	Date and Time To: 12/10/2019 12:01				
\$	Feature Details Fault detection Optimization				
	Device Details		S	elect All	
	Well Details Plunger(RMC-01)				
		R	eset So	hedule:	

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

AB	Di	gital Oilfield					P	۴	📥 Ana Andujar	()	G Î
≡	Fa	ult Detection Rep	ort								
:: :	F	ilter Details									
L		Start Date:	MM/DD/YYYY	End	Date: MM/DD/YYYY		Device:		Select		
8											
									Reset	Filter	
	Re	port Type	Start Date		End Date	Device			Wells		
						Ther	re is no data to disp	lay			

- Select the Start and End dates for the report.
 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

ABB	Digital C	Dilfield								Ţ	۵	🚢 Ana Andujar	6	G
=	Fault D	etection Report												
=	Filter D	Details												
	s	Start Date:	10/28/2019	Er	ind Date:	12/09/2019		Devid	e:	RMC	-01	~]		
⇔				•										
												Reset	Filter	n I
														11
	Report 1	Туре	Start Date	End Date		Device	Wells		Download Input Da	ta	0	ownload Report		
						There is no data to display								

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.
- Select **Optimization Report** from the navigation tree. The Fault Detection Report page displays (<u>Figure 7-71</u>).

Figure 7-71: Optimization Report page

ABB	Digital Oilfield				₩ 单	🛓 Ana Andujar (🕞
≡	Optimization Report					
:: :	Filter Details					
	Start Date:	MM/DD/YYYY	End Date: MM	I/DD/YYYY	Device : Select	
ø						
						Reset Filter
	Report Type	Start Date	End Date	Device	Wells	Download Input Data
				There is no data to display		

- 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

Digital Oilfield					₽ 🐥	🚢 Ana Andujar	6	G
Optimization Report								
Filter Details								
Start Date:	09/29/2019	End Date: 12/1	6/2019	Device :	RMC	C-01 🗸 🗸	·	
						Reset	Filter	
Report Type	Start Date	End Date	Device	Wells		Download Inp	out Data	a
			There is no data to display					
	Optimization Report	Optimization Report Filter Details Start Date: 09/29/2019	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/1	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/16/2019	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/16/2019 Device :	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/16/2019 Device : RMC Report Type Start Date Device Start Date End Date Device Wells	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/16/2019 Device : RMC-01 Reset Reset Report Type Start Date Device Bend Date Device Wells Download Ing	Optimization Report Filter Details Start Date: 09/29/2019 End Date: 12/16/2019 Device : RMC-01 Reset Filter Report Type Start Date 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 <u>7.5.1</u>.
- 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

Digital Oilfield				🖤 🌲 👗 Ana Andujar	0 E
Scheduled Wells					
Filter Details					
Device :	Select	Schedule Ty	Select	~	
				Reset	filter
Feature	Device	Wells	Schedule Type	Schedule Time (in 24 Hrs)	Delete
Fault Detection	RMC-01	Plunger (RMC-01)	Daily	11:30:00	Û

- 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

AB	- Diç	gital Oilfield					1	🜲 🔺 Ana Anduja	r (j	G
≡	Wel	I Configuration								
	+	Device Name	Plunger Name	Tubing ID	Well Depth	Plunger Stop	Casing ID	Plunger typ	e	
D	~	365_Dev_Device_Test								
*	~	SYS_TEST_PRO2								
	~	RMC-01								
	Jum	up. ~				e e	Page 1 of 1 > >	Reset	Submit	

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

-	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	1.9950000047	7000	6970	4 *	Dual Pad •
		Plunger-3	1.9950000041	7000	6970	4	Dual Pad 🔹
		Plunger-4	1.995000004	7000	6970	4 •	Dual Pad •
~	RMC-01	Plunger-4	1.995000004;	7000	6970	4 •	Dual Pad

- Configure parameters as necessary.
 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 <u>Additional information</u> for a link to the document.

To access the Plunger application page:

1. Click the PAS icon.

Figure 8-1: Select the PAS icon

ABB	Digital Oilfield		Last F	Refresh Time: 12/06/2019 0	02:41:43 PM 📮 🌲	• 0 I	G
	STATION / RMC-01						
	Setup		General		- Versions		
:	Station ID	RMC-100	Digital Board Part#	2105023	Flash Software Ver	2.3.0-4	
	IP Address	192.168.1.242	Flash Software Part#	2105457-029	OS Software Version	2.2.0-3	
\$	Location	ABB Totalflow	OS Software Part#	2105411-032	On-board IO Softw	2.3.0-4	
	Date Time	12/06/2019 02:41:4	On-board IO BL Pa	2105458-003	On-board IO BL So	1.0.1-29	

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

Figure 8-2: PAS portal

💵 Digital Oilfield 🛛 🗙 🏨 ABB	3 Plunger Analysis System × +	
\leftrightarrow \rightarrow C \cong https://abbpas.southcentra	alus.cloudapp.azure.com/#/login	☆ 👶 :
ABB		Support
	ABB Plunger Analysis System Optimizes plunger, Detects faults, Improves well production.	
	User ID. Enter email ID	
	Password: Enter password	
FaultDetection	Optimization	/
Detects the faults present in the plunger in order to o well production.	optimize the Optimizes the well production by analyzing the plunger and displaying averages of critical fields. Provides a training simulation for the users to ecosystem of plunger analysis.	understand the
More Informati	ion More Information More Info	ormation

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. <u>Table 9-1</u> 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 <u>Additional information</u> for links to manuals.

Note of the connect directly to the Internet. See section 9.2 Secure connections.Secure access to the device user interfaceChange 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 credentialsStore 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 brokerSelect 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 certificatesGenerate and upload valid certificates to the device. Store all authentication certificates in safe locations. Change or update authentication certificates as needed.Purge sensitive device dataDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user	Recommendation	Description
Secure access to the device user interfaceChange 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 credentialsStore 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 brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	Secure network connection	
user interfacecreated 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 credentialsStore 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 brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.		See section 9.2 Secure connections.
Credentials. See section 10.4 Manage users.Manage configuration interface credentialsStore 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 brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	Secure access to the device user interface	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
Manage configuration interface credentialsStore all private device interface credentials in safe locations. Share private device interface credentials only with properly trained and authorized personnel. 		
interface credentialsShare private device interface credentials only with properly trained and authorized personnel. Change or update private credentials as needed.Secure connection with the MQTT brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.		See section <u>10.4</u> <u>Manage users</u> .
Shale private device interface credentials only with property trained and authorized personnel. Change or update private credentials as needed.Secure connection with the MQTT brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	Manage configuration	Store all private device interface credentials in safe locations.
Secure connection with the MQTT brokerSelect 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 certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	interface credentials	
MQTT broker(TLS connections on port 8883). See section 3.5 Configure MQTT Server Details.Manage MQTT credentials and authentication certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.		Change or update private credentials as needed.
Manage MQTT credentials and authentication certificatesGenerate 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 decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	Secure connection with the MQTT broker	
And authentication certificatesStore all authentication certificates in safe locations. Change or update authentication certificates as needed.Purge sensitive device data when decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.		See section 3.5 Configure MQTT Server Details.
and authentication certificatesStore all authentication certificates in safe locations. Change or update authentication certificates as needed.Purge sensitive device data when decommissioningDevice decommissioning procedures must include: Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	Manage MOTT credentials	Generate and upload valid certificates to the device.
Purge sensitive device data Device decommissioning procedures must include: Purge sensitive device data Purging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	and authentication	Store all authentication certificates in safe locations.
Purge sensitive device dataPurging sensitive data stored in the device such as certificates, keys, credentials, and other proprietary company or user information.	certificates	Change or update authentication certificates as needed.
when decommissioning keys, credentials, and other proprietary company or user information.		Device decommissioning procedures must include:
See 9.6 Device data protection for decommissioning.	Purge sensitive device data when decommissioning	keys, credentials, and other proprietary company or user
		See 9.6 Device data protection for decommissioning.

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

9.2 Secure connections

<u>Figure 9-1</u> 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.

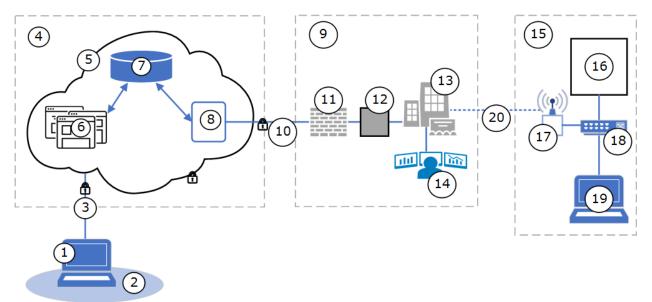


IMPORTANT NOTE: The RMC-100 is not an internet-facing device. Do not connect directly to the Internet. An MQTT gateway is required between the Digital Oilfield and the RMC. In the event that the customer's corporate network firewall is compromised, the RMC-100 would be at risk without the MQTT gateway.



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).





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	11	Firewall	17	Wireless router
	(using corporate VPN)				(Ethernet-to-radio)
4	Service provider	12	MQTT gateway	18	Managed Ethernet switch
	network/platform				(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:

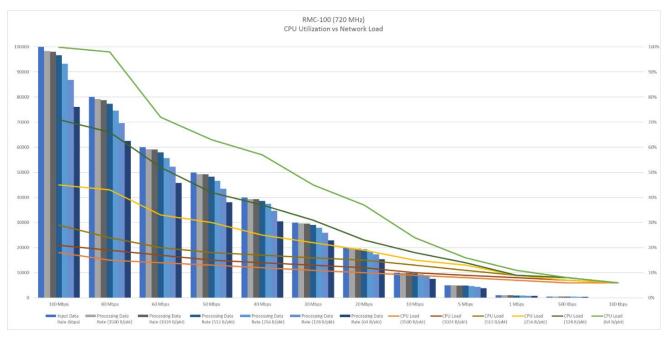
- Data rate range: 100 Kbps 100 Mbps
- Packet sizes (bytes): 64, 128, 256, 512, 1024, 1500
- Input packet rates:
 - Highest Packet Rate at 100 Mbps 195313 packet/sec (64 Bytes/packet)
 - Lowest Packet Rate at 100 Mbps 8333 packet/sec (1500 Bytes/packet)

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 <u>Additional information</u> 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 <u>10.3</u> <u>Generate certificates for</u> <u>X.509</u> authentication .
- Certificates are saved on the device. Complete certificate upload from the Initial Configuration screen is described in section <u>3.5</u> <u>Configure MQTT Server Details</u>.



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 <u>10.3 Generate certificates for X.509</u> authentication .

To add certificates to the browser configuration:

- 1. Start Chrome browser.
- 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).

S Privacy error	× +	
← → C ▲ Not se	ecure 192.168.1.242	★ ⊖ :
		-
Vous coursetion		
Your connectior	h is not private	
Attackers might be trying) to steal your information fro	m 192.168.1.242 (for
example, passwords, mes	sages, or credit cards). <u>Learn i</u>	more
NET::ERR_CERT_AUTHORITY	_INVALID	
Help improve Chrome	security by sending <u>URLs of som</u>	e pages you visit, limited
system information, and	<u>d some page content</u> to Google.	. <u>Privacy policy</u>
Advanced		Participant for the
Advanced		Back to safety
		•

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

- Select Not secure.
 Click Site Settings.
 Select Manage Certificates. The Certificates window displays (Figure 9-4).
 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.

ntermediate Certification Au	thorities Trusted Root Ce	ertification Aut	horities Trusted Pu	ibl 1
Issued To	Issued By	Expiratio	Friendly Name	1
AAA Certificate Ser ABB Ability(tm) Roo ABB ECC Root CA ABB Ltd - Master ABB Ltd - Master ABB Root CA ABB-WLAN-CA ABB-WLAN-CA ABB-WLAN-CA	ABB Ability(tm) Root CA ABB ECC Root CA ABB Ltd - Master ABB Ltd - Master ABB Root CA ABB-WLAN-CA		<none> <none> <none> <none> <none> <none></none></none></none></none></none></none>	
Import Export	Remove		Adva	ance

Figure 9-4: Chrome certificate management window

 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

Certificate Import Wizard
File to Import Specify the file you want to import.
File name:
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard-PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
·
< Back Next > Cancel

8. 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

C Open	×
Coover lighthouse > Certiticates > RMCPinyo	onSite
Organize 🔻 New folder	8= - 1 💿
Image: Second Places ▲ Image: Second Places Image: Second Places Image: OneDrive - ABB Image: Second Places Image: Second Places Image: Second Places	Documents library Arrange by: Folder ▼ RMCPinyonSite Name
ABB	client-cert.pem client-key.pem
Cibraries	
 My Documents Lighthouse architecture section 	
Branded icos Certiticates	
RMCPinyonSite G. RMCPinyonSite.zip Cloud devie management	< >
File name: client-cert.pem	

- 9. Once the import is complete, click **Finish** to exit the wizard and return to the Certificates window.
- 10. 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

ntermediate Certification Au	thorities Trusted Root Co	ertification Aut	horities Trusted Publ
Issued To	Issued By	Expiratio	Friendly Name
5 192.168.1.242	192.168.1.242	3/6/2021	<none></none>
AAA Certificate Ser	AAA Certificate Services	12/31/2028	Sectigo (AAA)
ABB Ability(tm) Roo	ABB Ability(tm) Root CA	6/12/2048	<none></none>
ABB ECC Root CA	ABB ECC Root CA	8/4/2036	<none></none>
🔄 ABB Ltd - Master	ABB Ltd - Master	8/28/2024	<none></none>
🔄 ABB Ltd - Master	ABB Ltd - Master	6/23/2021	<none></none>
🔄 ABB Root CA	ABB Root CA	2/27/2028	<none></none>
🔄 ABB-WLAN-CA	ABB-WLAN-CA	6/14/2019	<none></none>
ABB-WLAN-CA	ABB-WLAN-CA	6/14/2019	<none></none>
Import Export Certificate intended purpose	Remove		Advance
<all></all>			View

- 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).

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.
	NL -		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

Table 9-2: Open TCP ports on device

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 <u>9.5.1</u> and <u>9.5.2</u> provide lists of exposed services.

9.5.1 User-enabled services

1

<u>Table 9-3</u> 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 <u>Table 9-3</u> from PCCU. Implement security features as soon as the device is installed to prevent unauthorized users from changing the desired state of these services.

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

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

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

<u>Table 9-4</u> 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.

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.

Table 9-4: Services required for MQTT operation

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.

- Click the **32-bit loader** icon on the top menu.
 Connect with the device. The device loader screen displays.
 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.

i

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.

मिन् PCCU32 - [Entry]	5	
Operate View Window Help	-	_ B ×
Open Configuration File	🛃 🚟 🔇 Archive	<i>🛛</i>
- Laptop File Utilities Archive File Utilities	rrent Log Period Data Daily Events Chart	
Communications	Main	Battery 13.45 V
File Utilities	Entry Terminal	System 13.32 V Charger 0.22 V
Security +	Collection	/External
Setup 🕨	TFModbus CF/Day	
Exit	Today's Volume 0 MCF	Energy Rate 0 MMBTU/Day
i Display	Yesterday's Volume 0 MCF	Today's Energy 0 MMBTU
i Alarm System	Accumulated Volume 0 MCF	Yesterday's Energy 0 MMBTU
in Plunger	Last Calc Period Volume 0 SCF	TOTALFLOW
⊕ Gas Lift ⊕ Trend System	Diff. Pressure 0 InH20	Temperature
		60 Deg F
Terminal Emulation	Static Pressure 14.73 PSIA	#Polls: 138 #Errors: 0 Connected to RMC-100
l erminal Emulation		#Polls: 138 #Errors: 0 Connected to RMC-100

Figure 10-1: Access terminal mode on device

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

Figure 10-2: Enable MQTT functionality from terminal mode

Bu PCCU32 - [Terminal]		And a second second	
I Operate View Window Help			_ & ×
10 🛎 🖫 C 🔊 17 1.8 🛛	I 🚳 🛱 🎆 Setup 🥏		
TERM			1
->0.7.102 = 1			
Terminal v COM6: v 9600 v Log File		Clos	e Help
Ready	#Polls:	141 #Errors: 0 Connected to	RMC-100

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 <u>3.7 Verify connection status</u>.

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

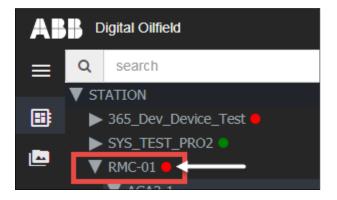
Figure 10-3: Disable MQTT functionality from terminal mode

terminal]	
Operate View Window Help	_ 8 ×
10 📅 🖫 🖸 🔊 Vii 🛃 🚾 🗇 節 🗰 🎝	
TERM ->0.7.102 = 0	
Terminal v COM6: v 9600 v Log File	Close Help
Ready #Polls: 139 #Errors: 0 Connecte	ed to RMC-100

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

IMPORTANT NOTE: When cloud-registered devices disconnect due to disabled MQTT functionality, the connection status indicator shows red (<u>Figure 10-4</u>).

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 <u>10.3</u> <u>Generate certificates for X.509 authentication</u>.



1

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 <u>3.5 Configure MQTT Server Details</u>.



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

c/blob/master/tools/CACertificates/CACertificateOverview.md

Sections <u>10.3.2</u> <u>Generate Self-signed certificates</u> and <u>10.3.3</u> <u>Generate CA-signed certificates</u>, 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

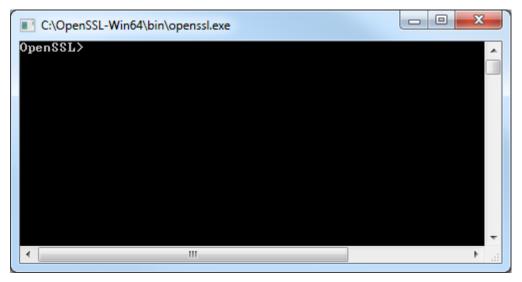
To generate self-signed certificates, you can download OpenSSL into a Windows system. Complete documentation on installing and using OpenSSL is beyond the scope of this document. Search for OpenSSL online resources, tutorials, and download/installation instructions.

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:

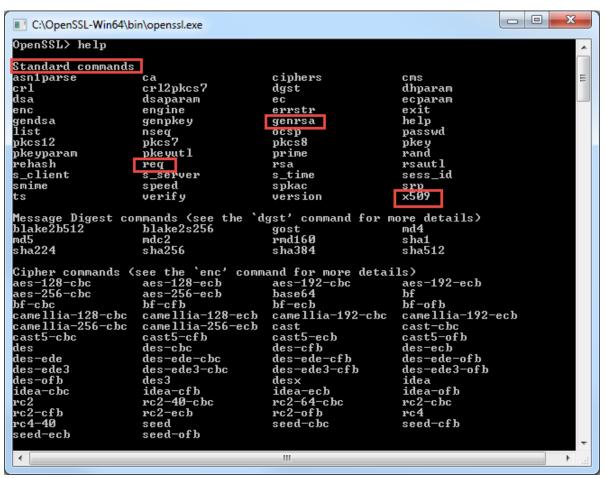
- 1. Click the Start button in Windows.
- 2. In the Search programs and files field, type **Openssl**. The OpenSSL command screen displays.

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 <u>10.3.2</u> <u>Generate Self-signed certificates</u>.

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 <u>12.2 Register field devices</u>).

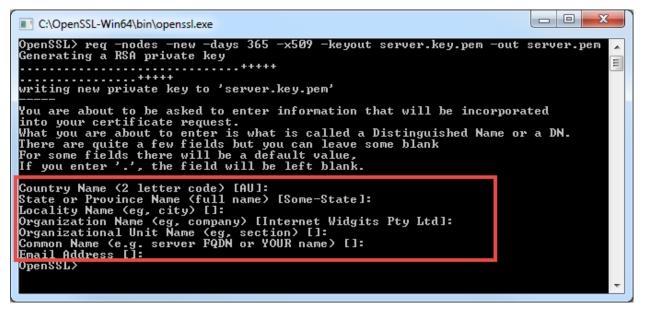
To generate self-signed certificates:

- 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

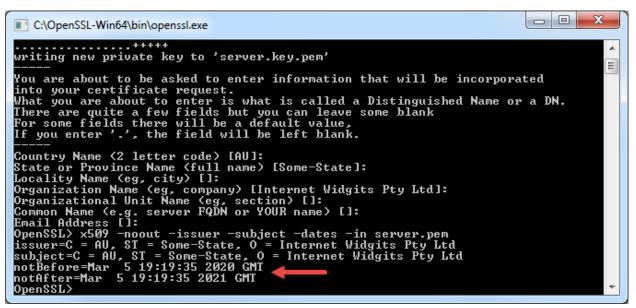


2. Check certificate validity by typing the following command at the prompt:

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



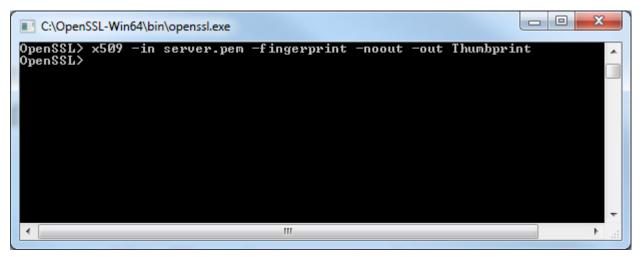
4. Generate the fingerprint of the certificate and copy the fingerprint into a file.

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



 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).

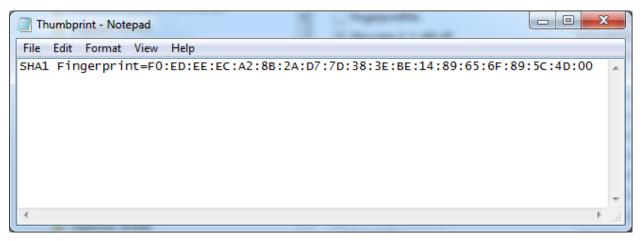
Edit View Tools Help				
anize 🔻 Include in library				•
퉬 OneDriveTemp	^ Name	Date modified	Туре	Size
OpenSSL-Win64	Cnf	1/8/2020 11:07 AM	File folder	
🍌 bin	PEM	1/8/2020 11:07 AM	File folder	
🎍 cnf	.rnd	3/3/2020 6:11 PM	RND File	1 K
PEM	CA.pl	9/11/2019 8:07 AM	PL File	7 K
oerts	🚳 capi.dll	9/11/2019 8:07 AM	Application extens	56 K
📕 ct	🚳 dasync.dll	9/11/2019 8:07 AM	Application extens	34 K
🎍 d2i-tests	fingerprintfile	3/3/2020 11:21 PM	File	1 K
🎳 exp	libcrypto-1_1-x64.dll	9/11/2019 8:07 AM	Application extens	2,849 K
🎳 fuzz	🚳 libssl-1_1-x64.dll	9/11/2019 8:07 AM	Application extens	470 K
include	openssl.cfg	9/11/2019 8:07 AM	CFG File	11 K
🍌 lib	openssl.exe	9/11/2019 8:07 AM	Application	474 k
ocsp-tests	ossitest.dll	9/11/2019 8:07 AM	Application extens	31 k
recipes	🔜 💿 padlock.dll	9/11/2019 8:07 AM	Application extens	41 K
ssi-tests	progs.pl	9/11/2019 8:07 AM	PL File	5 K
	server.key	3/3/2020 6:11 PM	KEY File	2 K
pccuhelpfiles	Sen/er pem	3/3/2020 6:13 PM	PEM File	2 K
Program Files Program Files (x86)	Thumbprint	3/3/2020 11:49 PM	File	1 K

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 <u>Figure 10-11</u> 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

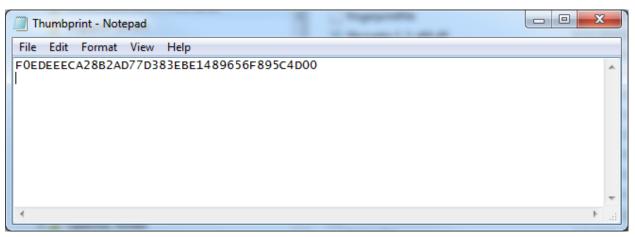
Figure 10-11: Fingerprint contents in output file



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 <u>12.2 Register field devices</u>).

Figure 10-13: Save fingerprint file

(<u>)</u> TI	humbprint - Note	epad			x
File	Edit Format	View Help			
	New	Ctrl+N	1489656F895C4D00		*
	Open	Ctrl+O			
	Save	Ctrl+S			
	Save As				
	Page Setup				
	Print	Ctrl+P			
	Exit				
			1		-
•					► 34

- 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.
- Copy the generated certificates to the device from the Initial Configuration page as described in section <u>3.5 Configure MQTT Server Details</u>. 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 <u>12.2 Register field devices</u>.

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 <u>10.3.4</u> <u>Generate own root CA certificates</u>.)
- Other CA certificates (See section <u>10.3.5</u> <u>Generate other root CA certificates</u>.)



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 <u>12.2 Register field devices</u>).



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-sdkc/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.

- On the Azure IoT Hub, upload the root CA file and generate a verification code: 2.
 - 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).
 - Keep the Certificate Details pane open. e.
- At the command prompt, to generate a verification certificate, type the following including the 3. 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.
 - Click **Open** to upload.
 - с. d. Select Verify.
- Add device and configure X.509 CA Signed authentication on Azure as described in section 12.2 5. 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:

 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 <u>3.5 Configure MQTT Server Details</u>. 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 genrasa -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.
- Copy the generated certificates to the device from the Initial Configuration page as described in section <u>3.5 Configure MQTT Server Details</u>. 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 <u>12.2 Register field</u> <u>devices</u>.

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)

🕑 Digit	al Oilfield	× +	
$\leftarrow \ \rightarrow$	C 🔺	Not secure 192.168.1.242/userManagement	☆ ⊖ :
ABB			🌣 🌖 root 🛈 🕞
≡	User M	anagement	
	Select	Username	Role
	\odot	AbbCustomer	guest
	\bigcirc	AbbDeveloper	admin
	\bigcirc	AbbTester	user
	\bigcirc	root	admin
			Add User Update User Delete User

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

Figure 10-15: Select existing user

S D	igital Oilfield	× +	
← -	> C 🚺	Not secure 192.168.1.242/userManagemen	nt 🖈 🖰 :
AB	•		🗢 🍥 root 🛈 🗗
≡	User M	lanagement	
	Select	Username	Role
	0	AbbCustomer	guest
	\odot	AbbDeveloper	admin
	۲	AbbTech	user
	\odot	AbbTester	user
	\odot	root	admin
			Add User Update User Delete 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.



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: Delault us	able 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 10-1: Default	user	accounts	on	device
---------------------	------	----------	----	--------

Table 10-2 lists roles and access levels available on the Totalflow device.

Role	Access level	Description
admin	Read and write (update) Manage users: add, delete or update users	 The admin role has the following privileges: 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: 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: 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

S Digital Oilfield × +			
← → C ▲ Not secure 192.168.1.242/	initialConfig		☆ ⊖ :
ABB			🗢 💿 root 🛈 🗗
⊨ Initial Configuration			User Management
General		MQTT Server Details	Audit Logging
Protocol	Standard MQTT Protocol	Broker IP/Hostname	ABBLight st Statistics
Device Parameters		Broker Port	8883
Device Timezone ?	(UTC-06)Central Standard Time	Authentication Option	Certificates •
Device ID	RMC-01	Root Certificate	Choose File No file choosen
Publish Interval (in seconds)	10	Client Certificate	Choose File No file choosen
Data Polling Interval (in seconds)		Client Key	Choose File No file choosen
Data Poining Interval (in Seconds)	1	Username	
MQTT Configuration Parameters —			
QoS	1 •	Password	
Will Details	true 🔻		
Will Topic	devices/RMC-01/messages/events/		
Will Message	OFFLINE		
		R	tead Config Update Config Connection Status Reset
javascript:linkFn('/userManagement')			

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

Figure 10-17: User Management web page

	C 🔺	Not secure 192.168.1.242/userManagement	☆ Θ
BB			🗢 🕘 root 🛈 [
ا ا	User M	anagement	
	Select	Username	Role
	0	AbbCustomer	guest
	\bigcirc	AbbDeveloper	admin
	\bigcirc	AbbTester	user
	\bigcirc	root	admin

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

0	Digital Oilfield	× (+	
÷	→ C 🚺	Not secure 192.168.1.242/userManagement	☆ 🖰 :
AB	B		🗢 🍥 root 🛈 🗗
≡	User M	anagement	
	Select	Username	Role
	0	AbbCustomer	guest
	0	AbbDeveloper	admin
	0	AbbTester	user
	0	root	admin
			Add User Update User Delete User

The Add User dialog displays.



🚱 Di	igital Oilfield		× +	
← -) C 🔺	Not secu	ure 192.168.1.242/use	rManagement 🖈 😁 :
АВ	\$			🌣 🥥 root 🛈 🕞
≡	User M	anagem	ent	
	Select	Userna	Add User	
	\odot	AbbCus		
		AbbDev	Username:	Enter Username
		AbbTest	Password:	Enter Password
	\odot	root		
			Role:	Select Role
				date User Delete User
				Add Cancel
				Aud

- Type credentials.
 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

S 1	Digital Oilfield		× +					x
←	→ C 🔺	Not secu	ure 192.168.1.242/use	rManagement			☆ 0	:
AB	₿				;	🗘 🌑 ro	ot (i)	Ð
≡	User M	anagem	ent					
	Select	Userna	Add User					
	0	AbbCus						
	0	AbbDev	Username:	AbbTech				
	0	AbbTest	Password:	•••••				
	0	root						
			Role:	user	•			
						date User		er
				Add	Cancel			
					_			

4. Verify that the new user displays in the list

Figure 10-21: Verify new user

🚯 Dig	ital Oilfield	×	+						
\leftrightarrow \rightarrow	C 🔺	Not secure 192	168.1.242/userMa	anagement				☆	Θ:
ABB	6						¢ 🕯	root	0 F
≡	User M	anagement							
	Select	Username			Role				
	0	AbbCustomer			guest				
	0	AbbDeveloper			admin				
	0	AbbTech			user				
	0	AbbTester			user				
	\odot	root			admin				
						Add User	Update Use	er Dele	te 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

S Digit	tal Oilfield	× +			• X
$\leftarrow \rightarrow$	C 🔺	Not secure 192.168.1.242/userManagement		☆	Θ :
ABB			:	🕫 🌔 root 🤇	ĵ ₽
≡	User M	anagement			
	Select	Username	Role		
	0	AbbCustomer	guest		
	0	AbbDeveloper	admin		
	۲	AbbTech	user		
	0	AbbTester	user		
	\bigcirc	root	admin		
			Add User U	pdate User Dele	te User

- Click **Update User**.
 Update the password or role at the Update User dialog box (<u>Figure 10-23</u>). 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

🕑 Di	gital Oilfield		×	+								x
\leftarrow	C 🔺	Not secu	ire 192.	.168.1.242/us	er Management					☆	Θ	:
ABI	}							;	¢ 🕒	root	í	G
≡	User M	anagem	ent									
	Select	Userna	Updat	e User								
		AbbCus										
		AbbDev	Us	ername:	AbbTech							
	۲	AbbTecl	Pa	ssword:								
		AbbTest										
		root	Ro	le:	admin		•					
						Update	Car	ncel	date User	De	lete Use	er

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

Figure 10-24: Verify existing user update

S Digit	al Oilfield	× +				
$\leftarrow \rightarrow$	C 🔺	Not secure 192.168.1.242/userManagement				☆ \varTheta :
ABB					¢ 🕒	root (i) 🗗
≡	User Ma	anagement				
	Select	Username	Role			
	0	AbbCustomer	guest			
	\bigcirc	AbbDeveloper	admin			
	۲	AbbTech	admin			
	\bigcirc	AbbTester	user			
	\bigcirc	root	admin			
				Add User	Update User	Delete User

10.4.6 Delete User

The Delete User function removes an existing user.

To delete a user:

z

1. Select the user from the list on the User Management web page (<u>Figure 10-25</u>). The Update User and Delete User buttons activate.

Figure 10-25: Select user to delete

Select Username Role AbbCustomer guest AbbDeveloper admin
AbbDeveloper admin
AbbTech admin
O AbbTester user
o root admin
AbbTester user

2. Click **Delete User**.

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

Figure 10-26: Confirm message to delete existing user

6	Digital Oilf	ield		×	+					x
÷	\rightarrow G		Not secure	192.	168.1.242/userManagement			☆	Θ	:
A	3 B					۵		oot	(j)	G
=	Use	r Ma	anagemer	nt						
	Sele	ect	Usernan							
	0		AbbCust	(i)	Are you sure you want to delete this user?					
	0		AbbDeve							
	۲		AbbTech		Yes No					
	0		AbbTeste			-11				
	0		root		admin					
								_		
					Add User	Update	e User	Del	ete Use	er

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

10.5 Monitor device audit logs

1

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 (<u>Figure 10-27</u>). 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	Figure	10-27:	Audit	Logging	web	page
--------------------------------------	--------	--------	-------	---------	-----	------

C A Not secure 1	92.100.1	242/auditLog	gging				☆
3						\$	🕘 root (
Audit Logging							
TimeStamp	S.No	Username	Role	Request Type	Old Value	New Value	Req. Statu
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

<u>Table 10-3</u> describes the attributes on the audit logging page.

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.

Table 10-3: Device audit logging parameter description

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**

O Digital Oilfield × +	
← → C ▲ Not secure 192.168.1.242/initialConfig	☆ ⊖ :
ABB	🗢 💿 root 🛈 🕞
Initial Configuration	User Management
General	Audit Logging
Protocol	Standard MQTT Protocol Statistics
Device Parameters	
Device Timezone 💿	(UTC-06)Central Standard Time
Device ID	RMC-01
Publish Interval (in seconds)	10
Data Polling Interval (in seconds)	1
MQTT Configuration Parameters	
QoS	1 •
Mill Datella	
	Read Config Update Config Connection Status Reset
javascript:linkFn('/auditLogging')	

The Audit Logging web page displays.

Figure 10-29: Audit logging page

		242/auditLog	Jging				\$
i						\$	🅘 root 🤅
Audit Logging							
TimeStamp	S.No	Username	Role	Request Type	Old Value	New Value	Req. State
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

- 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

}						\$	🕒 root (
Audit Logging							
TimeStamp	S.No	Username	Role	Request Type	Old Value	New Value	Req. Statu
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

- 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.

F	ile Home	insert I	Page Layout	Formu	ilas Data	Review V	iew	Help I	PDF-XChange	e Windchill	, Про Теl	l me	🖻 Share	🖵 Comr	nents
	Calibr aste ↓ ♂ lipboard 5		• <u>11</u> • A ⊡ • <u>⊘</u> • ıt		E = = ≫ • E = E E E E Alignment	ab Ce Prot ∎ Far Prote	tect	General \$ - % 9 €0 -00 Number		ditional Formatting * nat as Table * Styles * Styles	200 D	nsert + Pelete + ormat + Cells		u Find & er ▼ Select ▼	
1	A	В	с	D		E		F	G	Н	I	J	K	L	
1															
2	TimeStamp	SeqNo	Username	Role	RequestType			OldValue	NewValue	RequestStatus					
3	11/10/2019 11:19	7	root	admin	Update Registe	er Configuratio	on	Instance	InstanceN	Success					
ŧ	11/8/2019 12:41	6	root	admin	Update Applica	ation Configur	ration	AGA-7	AGA-7	Success					
5	11/8/2019 12:40	5	root	admin	Update Registe	er Configuratio	on	Instance	InstanceN	Success					
5	11/8/2019 12:37	4	root	admin	Update Applica	ation Configur	ration	AGA3-2	AGA3-2	Success					
7	11/8/2019 12:35	3	root	admin	Update Applica	ation Configur	ration	API	API Liquid	Success					
B	11/8/2019 12:31	2	root	admin	Update Applica	ation Configur	ration	AGA-7	AGA-7	Success					
•	11/5/2019 9:27	1	root	admin	Update Initial	Configuration		TimeZon	TimeZone:-	Success					
0															
			(1)												_

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

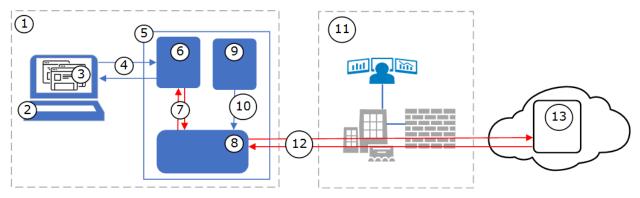
10.6 Monitor device statistics

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 <u>Figure 10-32</u> 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 <u>10.6.2 Device configuration statistics</u>.
- 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 <u>10.6.3 Device-broker connection statistics</u>.

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).



C A Not secure 192.168.1.242/initialConfig Initial Configuration General Protocol Device Parameters	MQTT Server Details Broker IP/Hostname ABB	rà € root ① nagement
Initial Configuration General Protocol Standard MQTT Protocol •	MQTT Server Details Audit Log	nagement
General Protocol Standard MQTT Protocol •	MQTT Server Details Audit Log	nagement
Protocol Standard MQTT Protocol •	Audit Log	laina
Device Perspectore	Statistics	s.net
	Broker Port 8883	
Device Parameters Device Timezone ? (UTC-06)Central Standard Time	Authentication Option Certificates	
Device ID RMC-01	Root Certificate Choose File N	o file choosen
Publish Interval (in seconds) 10	Client Certificate Choose File N	o file choosen
Data Polling Interval (in 1	Client Key Choose File N	o file choosen
seconds)	Username	
MQTT Configuration Parameters	Password	
QoS 1 🔹	Fasswold	
Will Details true •		
Will Topic devices/RMC-01/messages/events/		
Will Message OFFLINE		
criptlinkFn(/statistics)	Read Config Update Config	Connection Status Reset

The statistics web page displays.

			🗢 🍥 root 🕞
Statistics			
Statistics Type	Statistics Name	Count	
	Initial Config Update Invalid	0	
	Initial Config Update Valid	0	
MQTT Configuration Request	App Config Update Rejected	0	
MQTT Conliguration Request	App Config Update Accepted	0	
	Register Config Update Rejected	0	
	Register Config Update Accepted	0	
	Initial Config Update Failed	0	
	Initial Config Update Successful	0	
MQTT Configuration Response	App Config Update Failed	0	
Mort coniguration response	App Config Update Successful	0	
	Register Config Update Failed	0	
	Register Config Update Successful	0	
MQTT Connection Request	MQTT Connection Sending Failed	0	
MQ11 Connection Request	MQTT Connection Sending Successful	0	
	MQTT Connection Successful	0	
	MQTT Connection Failed, refused	0	
MQTT Connection Response	MQTT Connection Failed, not authorized	0	
	MQTT Connection retry count	0	_

Figure 10-34: Statistics for standard MQTT protocol

- 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 <u>10.6.4</u> 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 <u>10-4</u> lists the device configuration statistics sets that track the internal communication between the processes that handle configuration requests and the user interface. Table <u>10-5</u> and <u>Table 10-6</u> provide details for each set.

Туре	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 10-4: Device configuration int	terface statistics
--------------------------------------	--------------------

<u>Table 10-5</u> 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.

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.

<u>Table 10-6</u> 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 statist	ics
--	-----

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

<u>Table 10-7</u> 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 <u>10.6.4</u> <u>Sparkplug statistics</u>.

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

Table 10-7: Device-broker connection statistics

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.

<u>Table 10-9</u> 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

<u>Table 10-10</u> below describes the packets the device receives from the broker on the device-broker connection.

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.

<u>Table 10-11</u> 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 conifgured 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

<u>Table 10-12</u> 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.

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.

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

10.6.4 Sparkplug statistics

Sparkplug statistics display when sparkplug is the communication protocol selected for the devicebroker 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.

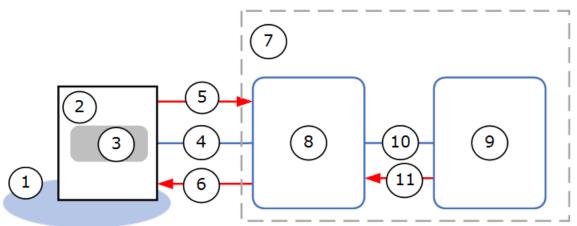
•	
•	

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 <u>10.6.3 Device-broker</u> <u>connection statistics</u> for details.

1

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.

<u>Table 10-13</u> shows the sparkplug-specific statistic sets and message types with payloads defined by the sparkplug specification.

Туре	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 10-13: Sparkplug-specific statistics

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	Number of Node Command (NCMD) messages 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. 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.			
Sparkplug DCMD Message Count	Number of Device Command (DCMD) messages This message type is used to send commands to the device to update data values related to device information primarily sent in DDATA. 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.			
Sparkplug STATE Message Count	 Number of critical application state messages 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: 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). The MQTT server ensures that the device is aware of the application state. 			

<u>Table 10-15</u> describes each of the packet types the device sends to the MQTT server.

Name	Description
Sparkplug NBIRTH Message Count	Number of Node birth certificate (NBIRTH) messages 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.
Sparkplug NDATA Message Count	Number of Edge of Node (EoN) Data (NDATA) messages 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. 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. 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.

Table 10-15: Sparkplug Packet sent statistics

Name	Description
Sparkplug DBIRTH Message Count	Number of device birth certificate (DBIRTH) messages 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.
Sparkplug DDATA Message Count	Number of Device Data (DDATA) messages 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.

11 Administrator tasks on the Digital Oilfield

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



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 (<u>Figure 11-1</u>). The Device Management web page displays.

Figure 11-1: Device Management web page

AB	B Digital	Oilfield			۰	Last Refresh Time: 11/07/2019 05:56:18 AM	뿟	۵	🚢 Ana Andujar	6	G
≡	Device	Mana	agement				٩	Searc	h Devices		×
	+		Device Name	Object ID		lp Address	Last	t Updat	ed		
8	~		365_Dev_Device_Test	09b04a2c-3c6d-423c-bdf6-ff0c288	3dcca	a 192.168.1.42	11/0)7/2019	03:53:13 PM		
	~		SYS_TEST_PRO2	85d59163-cb06-4eef-95b3-67a2d7	7ba0	. 192.168.1.56	10/3	31/2019	12:46:21 PM		
	~		RMC-01	933c601b-380f-4df9-b8d0-48cbe0	0b603	39 192.168.1.242	11/0)7/2019	05:56:07 AM		
	Jump	~				c < Page 1 of	1 >	>	Reset	Delete	

- 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

AB	Digita	I Oilfield	I Contraction of the second	• La	ist Refresh Time: 11/07/2019 05:56:18 AM	躍 🌲 📤 Ana Andujar 🛈 🗗
	-		Device Name	Object ID	Ip Address	Last Updated
	~		365_Dev_Device_Test	09b04a2c-3c6d-423c-bdf6-ff0c2883dcca	192.168.1.42	11/07/2019 03:53:13 PM
\$	~		SYS_TEST_PRO2	85d59163-cb06-4eef-95b3-67a2d7ba0	192.168.1.56	10/31/2019 12:46:21 PM
	^		RMC-01	933c601b-380f-4df9-b8d0-48cbe00b6	192.168.1.242	11/07/2019 05:56:07 AM
				Object ID	Application Name	
				9d5e9d1f-7c5b-40c6-bcb7-0d11b1b96	AGA3-1	
				31f07e8e-7a54-4145-837c-794a9fc24	SULIQ-1	
				6899dd4d-dea0-468e-a917-3d94957a	AGA7-1	
				722a881a-51d9-4227-b37d-48b4a192	Plunger	
				eb005b3d-41fc-4c30-8227-e4286b5b7	Gas Lift	
	Jump.	~			< Page 1 of 1	> » Reset Delete

11.1.2 **Reset device**

To reset a device:

- Select the device (<u>Figure 11-3</u>).
 Select **Reset**.

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

AB	Bigita	al Oilfield	I	•	Last Refresh Time: 1	1/07/2019 05:56:18 AM	MO.		📥 Ana Andujar	()	G
≡	Device	e Man	agement				٩	Sear	ch Devices		×
	+	-	Device Name	Object ID	lp Address		1.00	t Upda	4a.d		
	- T		Device Name	Object ID	Ip Address		LdS	t opda	ited		
٢	~		365_Dev_Device_Test	09b04a2c-3c6d-423c-bdf6-ff0c2883dd	ca 192.168.1.42		11/	07/2019	9 03:53:13 PM		
	~		SYS_TEST_PRO2	85d59163-cb06-4eef-95b3-67a2d7ba	0 192.168.1.56		10/	31/201	9 12:46:21 PM		
	~		RMC-01	933c601b-380f-4df9-b8d0-48cbe00b6	192.168.1.242		11/	07/2019	9 05:56:07 AM		
	Jump	~				C Page 1 of 1	>	2	Reset	Delete	

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

AB	Digita	l Oilfield	1	• L	ast Refresh Time: 11	/07/2019 05:56:18 AM	ЩQ.	🛕 🔒 Ana Andujar 🛛	0 F
≡	Device	e Mana	agement				٩	Search Devices	×
::: •	+		Device Name	Object ID	Ip Address		Las	t Updated	
8	~		365_Dev_Device_Test	09b04a2c-3c6d-423c-bdf6-ff0c2883dcc	a 192.168.1.42		11/(07/2019 03:53:13 PM	
	~		SYS_TEST_PRO2	85d59163-cb06-4eef-95b3-67a2d7ba0.	192.168.1.56		10/	31/2019 12:46:21 PM	
	~		RMC-01	933c601b-380f-4df9-b8d0-48cbe00b6	. 192.168.1.242		11/(07/2019 05:56:07 AM	
	Jump.	~				< Page 1 of 1	>	» Reset De	elete

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.

i

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

ABB Digital Oilfield			Last Refresh Time: 11/	07/2019 05:49:18 AM	₩ 4 4	Ana Andujar (
Q search ▼ STATION ▶ 365_Dev_Device_Test	8 hours	Line Bar Local UTC	Tooltip 🛑 🤟	Arrivals Arrival Time	Velocity(Reason
► SYS_TEST_PRO2 ■ ▼ RMC-01 ■	<u> </u>			11/07/2019 05:47:36 AM	0.00	1
AGA3-1 SULIQ-1				11/07/2019 05:27:20 AM	0.00	1
► AGA7-1 ▼ Plunger				11/07/2019 05:15:47 AM	0.00	1
Plunger State Plunger Valve Closed				11/07/2019 05:04:14 AM	0.00	1
Plunger Arrived Plunger Afterflow				11/07/2019 04:52:41 AM	0.00	1
Plunger Arriving Plunger Closing Valve Plunger Control				11/07/2019 04:41:08 AM	0.00	1
Plunger Afterflow Sub Plunger Valve Closed Sub	00:10 00:38 01:06 01	1:34 02:02 02:30 02:58 03:26	03:56 04:24 04:52 05:49	11/07/2019	0 00	1
Alarms Alarm Definitions	PSIA	Timers Last Open Time	00:00:10:01	Last Plunger Arrival	0	View
Trend Definitions Plunger Cycles	0	Last Close Time	00:00:01:32	Current State		
Events	J F	Hold Close Reason	None	ControllerState		ger Arriving
► Gas Lift	/Hr	Current Open Reason	None	Main Valve State	Oper	n

The Events page displays (Figure 11-6).

Figure 11-6: Plunger application Events page

	Last Refresh Time: 11/07	7/2019 05:36:08 AM 🐺 🛕 💄 Ana	Andujar 🛈 🖸
			C
Date/Time (UTC)	Reason	Value	
11/07/2019 11:36:03 AM	Enabled	0	
11/07/2019 11:34:09 AM	Disabled	0	
		ε < P	age 1 of 1 > 3
	11/07/2019 11:36:03 AM	Date/Time (UTC) Reason 11/07/2019 11:36:03 AM Enabled	Date/Time (UTC) Reason Value 11/07/2019 11:36:03 AM Enabled 0 11/07/2019 11:34:09 AM Disabled 0

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

AB	Digital Oilfield			۰	Last Refresh Time: 11/0)7/2019 05:36:08 AM	<u>10</u>		🛓 Ana Andujar	()	Ð
≡	STATION / RMC-01 / Plunger / Ev	vents									c
	Event Logs Audit Logs										Ŭ
	Date/Time	User	Old Value	New \	/alue	Variable Name		D	escription		
	11/07/2019 11:34:06 AM	ana.d.andujar@us.abb.com	Enable	Disab	e	plControl		P	lunger Control Mod	le	
	v jnut							«	< Page 1 of 1	>	2

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

Table 11-1: Application audit logging parameter description

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, <u>Table 12-1</u> 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.

Role	Access level	Description
ldsadmin	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
ldsedit	Read and Write	Live Data service (lds) 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): <u>portal.azure.com</u>.
- 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

	+ Add 🕐 Refresh 🛍 Delete
⊒ <mark>≓</mark> IP Filter ▲	
 Certificates Built-in endpoints 	You can use this tool to view, create, update, and delete devices on your IoT Hub.
Properties	Field Operator Value
Locks	+ X Select or enter your own V = V
😫 Export template	Add new clause
Explorers	Query devices I Switch to query editor
🔎 Query explorer	
IoT devices	DEVICE ID STATUS LAST ACTIVITY LAST STATUS UPDATE AUTHENTICATION TYPE CLOUD TO DEVICE MES
Automatic Device Management	AAA_VISHWA_RMC Disabled Mon May 06 2019 Mon May 06 2019 CertificateAuthority 0
🔮 IoT Edge	Device_Test Disabled Wed May 08 2019 Wed May 08 2019 SelfSigned 0
😤 IoT device configuration	RMC102 Disabled Thu Jan 24 2019 1 Wed Jan 30 2019 1 Sas 0

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	Ľ	•
* 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 🚯		1
Enter your secondary key		
Auto-generate keys 🕜		•
Save		

- Type the Device ID.
 Select the Authentication type and configure parameters accordingly.
 - a. For X.509 Self-signed authentication:
 - If you have not done so, generate certificates and fingerprint or thumbprint as described in section <u>10.3.2</u> <u>Generate Self-signed certificates</u>. i.
 - ii. Locate the file with the thumbprint.
 - iii. Select X.509 Self-signed.

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

Create a device		×
Find Certified for Azure IoT devices in the Device Catalog	Ľ	I
* Device ID 🚯		
The ID of the new device		
Authentication type 👩		
Symmetric key (X.509 Self-Signed) X.509 CA Signed		
* Primary Thumbprint 🕦		
Enter your primary thumbprint here		
* Secondary Thumbprint 👩		
Enter your secondary thumbprint here		
Connect this device to an IoT hub 🕦		
Enable Disable		-
Save		

- iv. Open fingerprint or thumbprint file saved during certificate generation.
- v. Select and copy (CRTL+C) the thumbprint.
- vi. Paste (CRTL +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 <u>10.3.4 Generate own root</u> <u>CA certificates</u> or <u>10.3.5 Generate other root CA certificates</u>.
 - ii. Select X.509 CA Signed.

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

💦 Create	e a device		×
			*
Find	Certified for Azure IoT devices in the Device Catalog	Z	I.
* Device ID 🚯			1
The ID of the n	ew device		
Authentication	type 🕦		1
Symmetric key	X.509 Self-Signed X.509 CA Signed		
Connect this de	evice to an IoT hub 🕦		
Enable D	isable		1
Parent device (9		1
No parent d	levice		
Set a parent o	levice		
			*
Save			
Jave			

- 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 <u>3.7 Verify connection status</u>.

13 Glossary

<u>Table 13-1</u> 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: <u>http://docs.oasis-open.org/mqtt/wqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf</u>.



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

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.		
ΙοΤ	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: 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.		
Торіс	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 <u>Figure 2</u> .
Cross-reference to a specific section in the document	Hyperlinks to sections referenced throughout the document appear in blue, with underline.	See section <u>9.1</u>
Cross-reference to another document or website	Hyperlink to the website in blue, with underline	Go to the RMC User Manual at <u>abb.com.</u>
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=""></place>



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

Texas Office - Houston

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

Kansas Office - Liberal

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

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 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

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.