USER MANUAL

EME160A, EME161A-R2, EME164A, EME168A

ALERTWERKS PLUS MQTT MANUAL

24/7 TECHNICAL SUPPORT AT 1.877.877.2269 OR VISIT BLACKBOX.COM





CHAPTER 1: INTRODUCTION
1.1 INTRODUCTION
1.1.1 WHAT IS MQTT
CHAPTER 2: MQTT TOPICS
2.1 TOPIC PRINCIPLE
2.1.1 Single-Level Wildcard - Replaces One Topic Level5
2.1.2 Multi-Level Wildcard - Covers Many Topic Levels
2.2 MQTT Cluster
CHAPTER 3: ALERTWERKS PLUS MQTT FEATURES
3.1 MQTT SUPPORTED FEATURES
3.1.1 MQTT Topics
CHAPTER 4: SENSOR STATUS CODES
4.1 SENSOR STATUS CODES
CHAPTER 5: ALERTWERKS PLUS MQTT CONFIGURATION 10
5.1 CONFIGURATION PAGE
5.2 MQTT SERVER PARAMETERS11
5.3 MQTT SUPPORT (H7 UNITS ONLY)
CHAPTER 6: MQTT MONITORING
6.1 MONITORING MQTT
6.2 HOW TO FIND SENSOR COMPOUND ID
6.3 DETAILED EXPLANATION OF COMPOUND ID STRUCTURE42
APPENDIX A: UPLOADING SSL SECURITY CERTIFICATES
APPENDIX B: REGULATORY INFORMATION
APPENDIX C: DISCLAIMER/TRADEMARKS





1.1 INTRODUCTION

MQTT is a new AlertWerks Plus feature, which allows you to send sensor values and status changes to up to four MQTT servers.

The following "What is MQTT?" introduction information is based on the <u>HiveMQ FAQ</u> documentation.

1.1.1 WHAT IS MQTT?

MQTT is a standardized protocol for messaging and data exchange that was developed by OASIS, ISO/IEC 20922:2016. The technology provides a scalable and cost-effective way to connect devices together with minimal protocol overhead. It is able to deliver data over the Internet in near real-time and guarantee delivery.

MQTT was originally designed to connect sensor nodes over communication networks that are unreliable, highlatency, or both. It is lightweight, which enables low-cost device communication.

MQTT uses TCP. Due to ordering requirements, MQTT over UDP is not possible.

Figure 1-1 illustrates the broker/client relationship.



MQTT follows a Publish/Subscribe paradigm. The sender (Publisher) and receiver (Subscribers) of messages communicate via topics and are decoupled from each other. The connection between them is handled by the MQTT broker. The broker receives and filters all incoming messages, determines who is interested in each message, and distributes messages correctly to the subscribers.

A client is any device that operates an MQTT library and connects to an MQTT broker over a network. A client doesn't have to pull the information it needs, since the broker pushes the information to the client whenever something new is available.



CHAPTER 1: INTRODUCTION



For example, monitoring a temperature sensor via MQTT works according to Figure 1-2:



FIGURE 1-2: DATA FLOW FROM SENSOR TO DEVICE

Reference Information:

HiveMQ Introduction to MQTT

https://www.youtube.com/watch?v=z4r4hlZcp40

MQTT Protocol - How it works

https://www.youtube.com/watch?v=4QWISyd7SOo





2.1 TOPIC PRINCIPLE

Communication in MQTT is based on the topic principle. An MQTT topic is a UTF-8 string that the broker uses to filter messages for each connected client. To receive messages, the client must subscribe to the topic. A topic can have one or more topic levels. Each topic level is separated by a slash.

Each topic must contain at least one character. The topic string permits empty spaces, and topics are case-sensitive. Figure 2-1 illustrates a topic with multiple topic levels.



Topics support wildcard characters. When subscribing to a topic, the user can either subscribe to the exact topic of a published message or can use wildcards to subscribe to multiple topics simultaneously. A wildcard can only be used to subscribe to topics, not to publish a message. There are two different kinds of wildcards: single-level and multi-level.

2.1.1 SINGLE-LEVEL WILDCARD - REPLACES ONE TOPIC LEVEL: +

A single-level wildcard replaces one topic level by using a "+" sign. Figure 2-2 illustrates a topic with a wildcard.

myoffice / firstfloor / + / temperature

Single-level wildcard

FIGURE 2-2: WILDCARD EXAMPLE



2.1.2 MULTI-LEVEL WILDCARD - COVERS MANY TOPIC LEVELS:

A multi-level wildcard covers many topic levels. It only appears at the end of a topic string. Figure 2-3 illustrates a multi-level wildcard.

myoffice / firstfloor /

Multi-level wildcard (only at end; multiple topic levels)

FIGURE 2-3: MULTI-LEVEL WILDCARD

2.2 MQTT CLUSTER

In an MQTT cluster, multiple brokers are handling the same topics.

If a broker receives new data from a sensor or device, it will distribute the new data between all other MQTT brokers for redundancy using inter-node communication channels.

In the event of a broker failure or communications problem, which is called a netsplit event, the data remains available from other cluster members.

If the failed cluster member comes online again, the sensor data missed during the offline period will be replicated from the other nodes.

The subscribed client will get the same data and same topics from any of the brokers participating in the cluster.

The publisher device or sensor can publish its data to any of the brokers participating in the cluster, knowing that the data will be replicated automatically to other brokers.





Figure 2-4 illustrates a MQTT broker cluster.



FIGURE 2-4: MQTT BROKER CLUSTER



CHAPTER 3: ALERTWERKS PLUS MQTT FEATURES



3.1 MQTT SUPPORTED FEATURES

For AlertWerks Plus products, MQTT can be enabled in the Settings menu.

The current implementation supports MQTT v3.1.1 without encryption as described here: <u>https://docs.oasis-open.org/mqtt/mqtt/v3.1.1/os/mqtt-v3.1.1-os.pdf</u>

AlertWerks Plus products use JSON strings to relay sensor information. The MQTT Data type is JSON.

The following features are supported:

- sending sensor status change events on appropriate events from ALL sensors (wired, virtual, etc.)
- periodically sending (updating) all sensor values via MQTT

NOTE: The interval is set on WebUI.

• defining up to 4 MQTT servers in settings

NOTE: The device will randomly select a server to send the MQTT values

The AlertWerks Plus units can queue up to 1,020 MQTT messages if the connection to the MQTT server is lost. These messages contain status and value changes for all online sensors.

The messages in the queue are saved even when the device is powered off. They will be re-sent to the MQTT server once the connection has been reestablished.

3.1.1 MQTT TOPICS

AlertWerks Plus topics:

spp/<DEVICE_MAC_ADDRESS>/sensor/status_change/<SENSOR_COMPOUND_ID>
spp/<DEVICE_MAC_ADDRESS>/sensor/value_change/<SENSOR_COMPOUND_ID>

NOTE: These topics are used for ALL sensor types.



CHAPTER 4: SENSOR STATUS CODES



4.1 SENSOR STATUS CODES

The sensor statuses are sent in the MQTT packets, and they are represented by numbers.

Figure 4-1 shows an example of sensor status information, and Table 4-1 provides sensor status and description information.

5 V		
	V value change	
	0.0.0.2.0 = { "timestamp" : 1627280798, "value" : 65 "status" : 2 }	
	0.0.0.2.1 = { "timestamp" : 162728079 ⁹ "volue" - 22 "status" : 2	
	0.1.0.9.0 = { "timestamp" : 162728079 , "status" : 8	

FIGURE 4-1: SENSOR STATUS EXAMPLE

TABLE 4-1. SENSOR STATUS AND DESCRIPTION

STATUS	DESCRIPTION
NOSTATUS = 1	Sensor is in an unknown or undefined state
SENSORNORMAL = 2	Sensor is in normal state
HIGHWARNING = 3	High warning state for analog sensor types
HIGHCRITICAL = 4	High critical state for analog sensor types
LOWWARNING = 5	Low warning state for analog sensor types
LOWCRITICAL = 6	Low critical state for analog sensor types
SENSORERROR = 7	Sensor error state
SWITCH_LOW_OUT = 8	Low state for switch sensor types
SWITCH_HIGH_OUT = 9	High state for switch sensor types
NO_VOLT_PRESENT = 10	No voltage detected
VOLT_PRESENT = 11	Voltage detected
SWITCH_TIMED_TO_ON = 12	Reserved for future use
STATUS_ACKED = 13	Sensor status is acknowledged
STATUS_OFFLINE = 14	Sensor status is offline
UNREACHABLE = 15	Sensor is unreachable



5.1 CONFIGURATION PAGE

To configure your AlertWerks Plus device:

- 1. Open Settings page -> MQTT.
- 2. Click on the check box to the left of **Enable MQTT** to select it.
- 3. Click on the check box to the left of Broadcast sensor values periodically to select it.
- 4. Set the broadcast interval by entering a value between 1-60 minutes in the corresponding field.

NOTE: Set 1 minute for quick updates and testing.

5. Set the network interface which MQTT will broadcast on by choosing a selection from the drop-down list box. For wired networks, choose **Ethernet**. **GSM (Modem)** is also supported.

Figure 5-1 shows these options.

	General	MQTT
⊕	Language	System / MQTT
0	Date / Time	Enable MQTT
‹·· >	Network	Broadcast sensors values periodically
0	MQTT	Broadcast Interval (minutes)
"	Modem	U Please enter a value between 1 and 60.
0-	VPN	
	Cloud Server	Network Interface
\succ	SMTP	
Ţ	SNMP	MQTT Server #1
Ţ	Server Integration	MOTT Server Name
9	Services	
*	Modbus	MQTT Server Port
Ê	Password Checking	Password
	RADIUS & TACACS	
٩	Maintenance	Confirm Password
٠	Heartbeat Messages	
	License Management	MQTT Server #2

FIGURE 5-1: MQTT CONFIGURATION PAGE







NOTE: if the "Broadcast sensor values periodically" option is not turned on, the unit will only send MQTT packages when a sensor status or value reading change occurs.

5.2 MQTT SERVER PARAMETERS

Up to four servers can be configured. If you have an MQTT cluster, you can define all cluster nodes here, and all nodes in the cluster will receive the messages.

Depending on the MQTT server's configuration, you may need to specify the username and password. This is a server setting; AlertWerks Plus can connect without authentication when these fields are blank. If the server requires authentication to accept data from the Gateway, by default the device's MAC address is used as the Username.

For testing MQTT, toggle flag **send values periodically**, and set the broadcasting interval to **1 minute**. New values will appear in MQTT.

If you see status = 1 for a topic, it is disabled.

5.3 MQTTS SUPPORT (H7 UNITS ONLY)

On the newer H7 platform, the secured, encrypted MQTTS is supported in addition to the existing unencrypted MQTT.

MQTT communication methods supported for MQTT on H7:

- unencrypted, unauthenticated (same as on F7 platform)
- unencrypted, authenticated username and password (same as on F7 platform)
- encrypted, unauthenticated
- encrypted, using client certificate
- encrypted, authenticated (username and password + SSL certificate)

For using the SSL (encrypted) method, a client .PEM x509 certificate must be uploaded.

It must be in the same format as the HTTPS certificate; it must contain the client's private key and certificate combined, without a password.

NOTE: The maximum size of the uploaded .PEM file must not exceed 8 Kilobytes.

The client certificate doesn't support multiple client and server certificates combined into one .PEM file for certificate chain validation.

The server's certificate has to be uploaded separately, if required (see below).

If the option "verify peer certificate" is turned on, the trusted CA certificate must be uploaded separately, and it has to be valid (not expired).

If this option is turned off, the server CA certificate is not validated. It could be expired.





In Figure 5-2, the MQTTS is configured with the encrypted SSL certificate method; the certificate validation is turned on; and certificates are being uploaded for MQTTS.

Enable MQTT	
Broadcast sensors values periodically	
Broadcast Interval (minutes)	
✓ Use SSL	
Verify peer certificate	
Upload Client Certificate File mqtts-client-key.pem UPLOAD Upload Trusted CA Certificate File mqtts-trusted_ca.pem UPLOAD	BROWSE
Network Interface Ethernet	Ψ

FIGURE 5-2: EXAMPLE CONFIGURATION SCREEN

You will need to browse and upload each .PEM certificate separately. Once uploaded and the settings are saved, the certificate file names will not be displayed, but they will be in use.

If the .PEM file upload fails and you get an error message, there is a problem with the certificate's format. See "Appendix A: Uploading SSL Security Certificates" for instructions regarding making a correct .PEM file.

NOTE: The maximum size of the uploaded .PEM file must not exceed 8 Kilobytes.

IMPORTANT: To upload the .PEM certificate files, after selecting the file with "Browse" button, you need to click on the "Upload" button for each uploaded client and/or server certificate file.





Figure 5-3 shows the upload screen.

	General	MQTT Vew certificate file uploaded successfully.
	Language	System / MQTT
0	Date / Time	Enable MQTT
<i><</i> ··>	Network	Preadeact concors values periodically
0	MQTT	Broadcast Interval (minutes)
	Modem	1
07	VPN	 ✓ Use SSL □ Verify peer certificate
	Cloud Server	
\succ	SMTP	Upload Client Certificate File mqtts-client.pem BROWSE
Ţ	SNMP	UPLOAD
Ţ	Server Integration	Upload Trusted CA Certificate File
٢	Services	
X	Modbus	
Ô	Password Checking	Network Interface
*	Radius	

FIGURE 5-3: CONFIGURATION SCREEN CONTAINING UPLOAD BUTTON

If you forget to click on the **Upload** button and just click on the **Save** button at the bottom of the page, the system will not upload the certificate files, and the MQTTS feature will fail.

If the .PEM file format is correct and the upload is successful, you will see a green popup message indicating that the file has been uploaded successfully. If you don't see this popup, then your certificate file is not uploaded.



6.1 MONITORING MQTT

To monitor MQTT, we recommend using the free MQTT Explorer application, which is a versatile Windows MQTT client. It can be downloaded here: <u>http://mqtt-explorer.com/</u>

Once downloaded, you will need to configure MQTT Explorer to connect to an MQTT server. Figure 6-1 shows the MQTT Connection screen.

Application Edit View Image: MQTT Explorer Image: Connections MQTT Connection mqtt.eclipse.org mqtt.eclipse.org mqtt:fliget.eclipse.org mqtt1 mqtt1 rest:lingt.eclipse.org mqtt1 Protecol mqtt/11 Validate certificate Encryption (tls) mqtt/12 mqtt/14 mqtt/15 mqtt/15 mqtt/15 mqt	G MQTT Exp	plorer			– 🗆 X
image: connections MQTT Connection mqtt//192.168.1.52:1883/ image: connections mqtt//192.168.1.52:1883/ image: connections mqtt//11 image: connection image: connections image: connection image: connection image: connections		MQTT Explorer	Q Search	0	DISCONNECT 🖎
 Connections MQTT Connection mqtt/192.168.1.52:1883/ mqtt mqtt/1 mqtt/1				Торіс	^
mqtt ecclipse.org mqtt/ingt.selipse.org mqtt1 mqtt1 mqtt1 mqt1 mqt1 mqt1 Protocol mqtt2 192.168.1.52 mqt1 192.168.1.52 mqt1 192.168.1.52 mqt1 Port 183 183		+ Connections	MQTT Connection matt	//192.168.1.52:1883/	
mqtt1 mqtt//192.168.1.52:1883/ Protocol mqtt2// Host mqtt/// Port 192.168.1.52 Port 1883 mqtt2 mqtt//192.168.1.53:1883/ Username Password Image: Connect Co		mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/ test.mosquitto.org mqtt://test.mosquitto.org:1883/	Name mqtt1	Validate certificate	Encryption (tis)
mqtt//192.188.1.53:1883/		mqtt1 mqtt://192.168.1.52:1883/	Protocol Host mqtt:// v 192.168.1.52		Port ^
		mqtt2 mqtt://192.108.1.53:1883/	Username DELETE	Password	کر BLISH CONNECT

FIGURE 6-1: MQTT EXPLORER CONNECTION SCREEN

NOTE: You need an MQTT broker already set up and running before you can connect to it. Depending on the server's configuration, you may need to specify the username and password.





MQTT values will appear from your AlertWerks Plus Gateway. Figure 6-2 shows a MQTT Explorer screen with values from a Gateway.

ଏ 🖁 MQTT Explorer				- 🗆 X
Application Edit View				
MQTT Explorer	Q Search	0	DIS	CONNECT 🗞 💫
<pre>▼ 192.168.1.52</pre>	313985182, "value": 0.02, "status": 6 13985182, "status": 2 } 613985182, "value": "NaN", "status" 13985182, "value": "NaN", "status": 1 13985182, "value": "NaN", "status": 1 13985182, "value": "NaN", "status": 1613985182, "value": "NaN", "status": 1613985182, "value": "NaN", "status" 1613985182, "status": 2 } 1700 1800) : 1) : 1) : 1) : 1) : 1) : 1) : 1) : 1) : 1)	(>) = (*) = "timestamp": 161398481 "status": 1 "status": 2 Comparing with previous mention of the previous menti	QoS: 0 02/22/2021 4:06:52 PM e, tessage: + 1 line, - 1 line tus_change/0.3.0.0.1× PUBLISH

FIGURE 6-2: MQTT EXPLORER SCREEN WITH MQTT VALUES

As noted earlier, the MQTT topic will use the following format: spp/\${DeviceID}/sensor/status_change/\${SensorID} spp/\${DeviceID}/sensor/value_change/\${SensorID}

The **Device ID** is the unit's MAC address.



When a new sensor becomes online on the device, a new topic will appear with a new Sensor ID. Figure 6-3 shows a sensor ID.

또 MQTT Explorer				– 🗆 X
Application Edit View				
MQTT Explorer	Q Search	0	DISC	ONNECT 🗞 💦
▼ 192.168.1.52 \$ \$\$Y\$ (180 topics, 7740 messages) ▼ \$\$yp ▼ 000BDC016906 ▼ sensor ▼ value_change 0.1.0.10.0 = { "timestamp" : 16 3.0.0.241.0 = { "timestamp" : 16 3.0.1.0.0 = { "timestamp" : 16 3.0.1.241.0 = { "timestamp" : 16 3.0.1.242.0 = { "timestamp" : 16 3.0.1.242.0 = { "timestamp" : 16 0.3.0.1.0 = { "timestamp" : 16 0.3.0.1.0 = { "timestamp" : 16 0.3.0.0.0 = { "timestamp" : 16 0.3.0.0.0 = { "timestamp" : 16 0.3.0.1.0 = { "timestamp" : 16	613985482, "value": 0.02, "status": 6 } 13985482, "status": 2 } 1613985482, "value": "NaN", "status": 1 } 13985482, "value": "NaN", "status": 1 } 13985482, "value": "NaN", "status": 1 } 613985482, "value": "NaN", "status": 1 } 1613985482, "value": "NaN", "status": 1 } 1613985482, "value": "NaN", "status": 1 } 13985482, "status": 4 } 13985468, "status": 2 } 13985468, "status": 4 }		<pre></pre>	QoS: 0 02/22/2021 4:17:50 PM 68, "statu 68, "statu s_change/0.3.0.1.(x
	1812.			

FIGURE 6-3: MQTT EXPLORER SCREEN WITH NEW TOPIC







Example #1:

Figure 6-4 shows a Gateway with a Temperature/Humidity sensor plugged in Port 1.

The Device ID is 000BDC014FDF, which is the unit's MAC address.

The Temperature sensor has the Sensor ID 0.0.0.0.1

MQTT Explorer Application Edit View			- 🗆 X
■ MQTT Explorer Q Search	0		disconnect 🗞 😣
▼ 192.168.1.49 ► \$\$Y\$ (94 topics, 9870 messages) ▼ spp ▼ 000BDC014FDF ▼ sensor	-	0.0.0.1	
▼ value_change 0.0.0.0.0 = { "timestamp" : 1615280529, "value" : 53, "status 0.0.0.0.1 = { "timestamp" : 1615280529, "value" : 33.1, "status 0.1.0.9.0 = { "timestamp" : 1615280529, "status" : 8 }	":2} us":3}	Value 盾	^
		<> ≡	QoS: 0 03/09/2021 4:02:14 PM
		<pre>{ - "timestamp": 16152 - "value": 32.8, * + "timestamp": 16152 </pre>	80469, 80529,
	:	<pre>// volue : 55.1, // "status": 3 } Comparing with previous</pre>	message: + 2 lines , - 2 lines
	-	► History ³⁵	
		Publish	^
		spp/000BDC014FDF/sensc	pr/value_change/0.0.0.0×
		raw xml json	

FIGURE 6-4: MQTT EXPLORER SCREEN WITH TEMPERATURE/HUMIDITY SENSOR



Example #2: MQTT Explorer configuration with online broker

In this example, which uses a public MQTT test server from HIveMQ, a gateway with a Temperature and Humidity sensor is connected.

On the webpage, the MQTT connection settings appear as follows:

MQTT connection settings

Host: broker.hivemq.com

TCP Port: 1883

Configure the MQTT server settings on the AlertWerks Plus Gateway:

- 1. Click on Enable MQTT.
- 2. Click on Broadcast sensor values periodically, and set it to 1 minute interval.
- 3. Since the HiveMQ test broker doesn't use SSL or authentication, don't enable SSL, and do not specify a password (leave it blank). You may use any value for the username, but it will not be used. However, since the AlertWerks Plus Gateway's WebUI form requires a username parameter to save the settings, we will use the value **admin** in our example.
- 4. Enter the connection details for MQTT Server #1: broker.hivemq.com and default port 1883.
- 5. Scroll down and click on the **Save** button.





Next, start MQTT Explorer and create a new connection by clicking on the yellow + sign. Figure 6-5 shows the new connection screen.

🕼 MQTT Explorer			-	
Application Edit View				
	Q Search	0	DISCONNE	ст 🗞
	ļ	Торіс		^
+ Connections	MQTT Connection m	qtt://broker.hivemq.com:1883/		_
mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/ test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Name broker.hivemq.com	Validate certificate	Encryption (tls)	^
mqtt1 mqtt://192.168.1.52:1883/ mqtt2 mqtt://192.168.1.53:1883/	Protocol Host mqtt:// - broker.hivemq.com		Port 1883	^
mqtt3 mqtt://192.188.1.49:1883/ test.mosquitto.org mqtt://test.mosquitto.org:1884/ broker.hivemq.com mqtt://broker.hivemq.com:1883/	Username DELETE	Password	کې Uconnect	BLISH

FIGURE 6-5: MQTT NEW CONNECTION SCREEN

Specify the same connection settings as for the Gateway:

- 1. Connection name: It can be set to any value, In the example shown, we use broker.hivemq.com.
- 2. Do not enable Validate certificate and Encryption (tls) settings; leave them turned off.
- 3. Enter the hostname to connect to: broker.hivemq.com.
- 4. Do not specify any username or password to connect.

Next, click on the **Advanced** button to set the MQTT topic, since we don't want to subscribe to all topics that are available on this public broker.





The default topic configuration is #, which subscribes to all available topics on the server.

We don't want to get values from other devices. Therefore, remove this setting by using the delete icon. Figure 6-6 shows the default topic configuration.

C MQTTE	xplorer			_	o x
	MQTT Explorer	Q Search		DISCONNEC	TΔ
		Торіс			~
	+ Connections	MQTT Connection mqtt://broker.hivemq.com:1883/			
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Торіс	QoS 0 👻	+ ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс		QoS	
	mqtt1 mqtt://192.168.1.52:1883/	#		0	~
	mqtt2 mqtt://192.168.1.53:1883/	\$SYS/#		0	
	mqtt3 mqtt://192.168.1.49:1883/				
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID			BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f	ERTIFICATES	BACK	
	_				

FIGURE 6-6: DEFAULT TOPIC CONFIGURATION





Next, specify the topic that you want to view. This will be the **spp/#** topic and subtree, which will subscribe to any AlertWerks Gateways publishing to this MQTT server.

Type in **spp/#** and click on the **Add** button. Figure 6-7 shows this topic added.

🕼 MQTT Exp	plorer				-	
Application	Edit View					
≡	MQTT Explorer	Q Search	0		DISCONNEC	ст &
		:	Торіс			^
	+ Connections	MQTT Connection	mqtt://broker.hivemq.com:1883/			
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Topic Spp/#		QoS 0 🔻	+ ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс			QoS	
	mqtt1 mqtt://192.168.1.52:1883/	\$\$Y\$/#			0	~
	mqtt2 mqtt://192.168.1.53:1883/					
	mqtt3 mqtt://192.168.1.49:1883/					
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID			_	BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f		ERTIFICATES	N BACK	
		•				

FIGURE 6-7: TOPIC ENTRY

The topic subscription setting will be saved, and you can click "Back" button and connect to the MQTT server.





Figure 6-8 shows the Topic screen after the save is complete.

C MQTT Explorer				_	o x
	0 Search				тΑ
		•		DISCONNEC	
		Торіс			
+ Connections	MQTT Connection	mqtt://broker.hivemq.com:1883/			
mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Topic		QoS 0 👻	+ ADD	^
test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс			QoS	
mqtt1 mqtt://192.168.1.52:1883/	\$\$Y\$/#			0	~
mqtt2 mqtt://192.188.1.53:1883/	spp/#			0	
mqtt3 mqtt://192.168.1.49:1883/					
test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID				BLISH
broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f	CEF	RTIFICATES	BACK	

FIGURE 6-8: MQTT EXPLORER SCREEN SHOWING SAVED TOPIC SUBSCRIPTION SETTING.





If all settings are correct, the connected gateway hostname and all its sensors will be displayed after 1-2 minutes.

In our example that is the 000BDC014FDF host, but there is already another AlertWerks Plus Gateway visible in this topic. Figure 6-9 shows the connected gateways and the 000BDC014FDF host's connected sensors.

🕼 MQTT Explorer				– 🗆 X
Application Edit View				
≡ MQTT Explorer ९	Search	•	DISCONNE	ЕСТ 🛆 🙏
▼ broker.hivemq.com ▼ spp ▶ 000BDC016955 (49 topics, 49 message ▼ 000BDC014FDF	es)		Topic 🚡 👕	^
▼ sensor ▼ value_change 0.0.0.2.0 = { "timestamp" : 16272806 0.0.0.2.1 = { "timestamp" : 16272806 0.1.0.9.0 = { "timestamp" : 16272806	578, "value" : 66, "status" : 2		spp / 000BDC014FDF / sensor / va	lue_change
			Value	^
			► History	
			Publish	^
			Topic spp/000BDC014FDF/sensor/value_cha	ange ×
			raw xml json	

FIGURE 6-9: MQTT EXPLORER SCREEN WITH CONNECTED GATEWAY HOSTNAME AND SENSORS

NOTE: If you only want to subscribe to and display the values for a single host, disconnect the server and go back to the "Advanced" configuration to specify a different topic setting.



In Figure 6-10 we reconfigured the topic to only display sensor values and statuses from our example host (000BDC014FDF).

📽 MQTT Explorer			– 🗆 X
Application Edit View			
	Q Search	0	DISCONNECT 🖎
		Торіс	~
+ Connections	MQTT Connection mqtt.//	broker.hivemq.com:1883/	
mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Topic spp/000BDC014FDF/#	QoS 0 👻	+ ADD
test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс		QoS
mqtt1 mqtt://192.168.1.52:1883/	spp/000BDC014FDF/#		0
mqtt2 mqtt://192.168.1.53:1883/			
mqtt3 mqtt://192.168.1.49:1883/			
test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID	0	BLISH
broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f	CERTIFICATES	BACK

FIGURE 6-10: MQTT EXPLORER SCREEN WITH RECONFIGURED TOPIC

The topic setting is spp/ 000BDC014FDF/#

NOTE: The Topic Principle section in chapter 2 discusses using wildcards.







As shown in Figure 6-11, only our AlertWerks Plus device and its sensors are subscribed with this topic setting.

📽 MQTT Explorer			-	o x
Application Edit View				
	Q Search	•	DISCONNECT 🖄	
▼ broker.hivemq.com ▼ spp ▼ 000BDC014FDF ▼ sensor			Topic 🖺 👕	^
0.0.0.2.0 = { "timestamp" : 162 0.0.0.2.1 = { "timestamp" : 162 0.1.0.9.0 = { "timestamp" : 162	27280798, "value" : 65, "status" : 2		spp / 000BDC014FDF / sensor / value_cha	nge
			Value	^
			► History	
		1	Publish	^
			spp/000BDC014FDF/sensor/value_change	X
			raw xml json	IBLISH
				_

FIGURE 6-11: MQTT EXPLORER SCREEN SHOWING TOPIC RESULTS FOR SPECIFIED SETTING

As noted earlier, supported MQTT topic settings on WTG and SP+ units have the following format: spp/\${DeviceID}/sensor/status_change/\${SensorID} spp/\${DeviceID}/sensor/value_change/\${SensorID}

You can narrow down the topic subscription, based upon your needs.



Example MQTTS configuration with online broker

In the following example we will use the public MQTT test server from Mosquitto (test.mosquitto.org). An AlertWerks Gateway with a Temperature and Humidity sensor is connected to the test server.

On the webpage, the MQTTS connection settings are shown as follows: MQTTS connection settings (encrypted, authenticated) Host: **test.mosquitto.org** TCP Port: **8885**

MQTTS connection requires certificates.

The Mosquitto test server's certificate **mosquitto.org.crt** can be downloaded from the webpage, or you can use this link: <u>http://test.mosquitto.org/ssl/mosquitto.org.crt</u>

To generate the Gateway's client certificate that is accepted by this test server:

- Generate a CSR using the openssl utility
- Generate a private key: openssl genrsa -out spxclient.key
- Generate the CSR: openssl req -out spxclient.csr -key spxclient.key -new

NOTE: You can directly run the Openssl commands below in a Linux terminal or on Windows if the Openssl package is installed. You cannot run Openssl on the gateways; the request must be generated on their behalf.

NOTE: You must specify custom values for the following parameters when generating the request, or it will not be accepted by the test.mosquitto.org server.

Required custom values: Country Name (2 letter code) State or Province Name (full name) Organization Name (for example, company) Common Name (for example, server FQDN or YOUR name)

Copy and paste the contents of the spxclient.csr file to the webpage at http://test.mosquitto.org/ssl/

If there are any problems with your request, such as missing common name field, the webpage will indicate that a problem occured.

If the request is accepted, the certificate file **client.crt** will be downloaded automatically.







At this stage you should have three files:

spxclient.key

client.crt and

mosquitto.org.crt.

Additional steps are necessary to create the .PEM certificate files that can be uploaded on the Gateway.

To prepare the test .PEM certificate files:

- 1. Open the file spxclient.key with Notepad++.
- 2. Go to the end of the file, and copy and paste the contents of **client.crt** just below it. Now you should have a file with the private key and certificate combined.
- 3. Save the file, using **spxtest.pem** as the filename.
- 4. Rename the file mosquitto.org.crt and use mosquitto.org.pem as the new filename.

Now you should have two files which can be uploaded to the Gateway:

spxtest.pem (client certificate) and

mosquitto.org.pem (server certificate).

To set up MQTTS on the AlertWerks Plus Gateway, you need to configure the MQTTS settings.

To configure these settings:

- 1. Click on Enable MQTT.
- 2. Click on Broadcast sensor values periodically and set it to a 1 minute interval.
- 3. Click on Use SSL to enable MQTTS.
- 4. (optional) Click on Verify peer certificate to enable the certificate verification.
- 5. After you browse to the file **spxtest.pem**, click on the **Upload** button to upload the client certificate.
- 6. After you browse to the file mosquitto.org.pem, click on the Upload button to upload the server certificate.

NOTE: You should see two green popup messages indicating that the certificate files have been uploaded successfully. If you don't see these messages, there is a problem with the .PEM certificate files, and you should try to create them again.





Figure 6-12 shows a screenshot with messages stating that certificate files uploaded successfully.

MQTT System / MQTT	 New certificate file uploaded successfully. New certificate file uploaded successfully. 	
Enable MQTT		
Broadcast sensors	s values periodically	
1 Use SSL Verify peer certific	ate	
Upload Client Certificate File		BROWSE
spxtest.pem		
Upload Trusted CA Certificate Fi mosquitto.org.pem	ile	BROWSE
UPLOAD		
Network Interface Ethernet		~

FIGURE 6-12: SCREEN SHOWING SUCCESSFUL CERTIFICATE UPLOAD MESSAGES

- 7. Enter the connection details for MQTT Server #1: test.mosquitto.org and port 8885.
- 8. Enter **rw** for the MQTT username.
- 9. Enter readwrite for the password.
- 10. Scroll down and click on the **Save** button.

BLACKBOX.COM



Figure 6-13 shows this information entered.

AQTT Server #1			
MQTT Server Name			
test.mosquitto.org			
MQTT Server Port			
8885			
MQTT Username			
ſW			
Password			
Confirm Password			
······			

FIGURE 6-13: MQTT SERVER INFORMATION SCREEN



Next, start MQTT Explorer and create a new connection by clicking on the yellow + sign. Figure 6-14 shows the New Connection screen.

🕼 MQTTE	xplorer					
Application	Edit View					
≡	MQTT Explorer	Q Search		0	DISCONNE	ст 🗞
	_	:		Торіс		^
	+ Connections	MQTT C	connection matt	://test.mosquitto.org:8885/		
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Name		-	-	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	test.mosquitto.o	org S	Validate certificate	Encryption (tls)	
	mqtt1 mqtt://192.168.1.52:1883/ mqtt2 mqtt://192.168.1.53:1883/	Protocol mqtt:// 👻	Host test.mosquitto.org		Port 8885	^
	mqtt3 mqtt://192.168.1.49:1883/	Username rw		Password	Ø	
	test.mosquitto.org mqtt://test.mosquitto.org:1884/ broker.hivemq.com mqtt://broker.hivemq.com:1883/	DELETE	ADVANCE	D	() CONNECT	BLISH



Specify the same connection settings as for the AlertWerks Plus Gateway:

- 1. Connection name: It can be set to any value, In the example shown, we use test.mosquitto.org S.
- 2. Enable Validate certificate and Encryption (tls) settings.
- 3. Enter test.mosquitto.org as the hostname to connect to.
- 4. Enter **rw** as the username.
- 5. Enter readwrite as the password.
- 6. Click on the **Advanced** button to set the certificate files for the connection.
- 7. Click on the **Certificates** button. Figure 6-15 shows the screen with this button.



🕼 MQTT B	xplorer			-	
Application	Edit View				
=	MQTT Explorer	Q Search	0	DISCONNE	ст 🖎
	_		Торіс		^
	+ Connections	MQTT Connection	mqtt://test.mosquitto.org:8885/		
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Торіс		QoS 0 ➡ + ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс		QoS	
	mqtt1 mqtt://192.168.1.52:1883/	\$SYS/#		0	^
	mqtt2 mqtt://192.168.1.53:1883/	spp/#		0	
	mqtt3 mqtt://192.168.1.49:1883/				
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID	Manage tis con	nection certificates	BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-1466d587	CER	TIFICATES	

FIGURE 6-15: MQTT CONNECTION SCREEN SHOWING CERTIFICATES BUTTON.





- 7. Choose the certificate files from your PC:
 - Server certificate (CA): **mosquitto.org.pem** Client certificate: **client.crt** and Client key: **spxclient.key**

Figure 6-16 shows the certificate files and client key.



FIGURE 6-16: MQTT CONNECTION SCREEN SHOWING CERTIFICATE FILES

BLACKBOX.COM

8. Click on the **Back** button.



We will configure the MQTT topic subscription, since we don't want to subscribe to all topics that are available on this public broker.

Figure 6-17 shows the default topic configuration, #, which subscribes to all available topics on the server.

9. Since don't want to include values from other devices, remove this setting by using the delete icon which looks like a trash can.

C MQTT Exp	plorer				-	o x
	MQTT Explorer	Q Search	0		DISCONNEC	т۵
			Торіс			~
	+ Connections	MQTT Connection	mqtt://broker.hivemq.com:1883/			
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Topic		QoS 0 🔻	+ ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс			QoS	
	mqtt1 mqtt://192.168.1.52:1883/	#			0	~
	mqtt2 mqtt://192.168.1.53:1883/	\$\$Y\$/#			0	
	mqtt3 mqtt://192.168.1.49:1883/					
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID				BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f	CEI	RTIFICATES	N BACK	

FIGURE 6-17: MQTT TOPIC SCREEN



10. Specify the topic that you want to view. This will be the spp/# topic and subtree, which will subscribe to any AKCP devices publishing to this MQTT server.

Enter **spp/#** and click on the **Add** button.

Figure 6-18 shows the screen where you can add this topic.

MQTT Expl	lorer				-	o x
	MQTT Explorer	Q Search	0		DISCONNEC	τø
			Торіс			^
	+ Connections	MQTT Connection	mqtt://broker.hivemq.com:1883/			
	mqtt.eclipse.org mqtt.//mqtt.eclipse.org:1883/	Topic Spp/#		QoS	+ ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс			QoS	_
	mqtt1 mqtt://192.168.1.52:1883/	\$SYS/#			0	~
	mqtt2 mqtt://192.168.1.53:1883/					
	mqtt3 mqtt://192.168.1.49:1883/					
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID	0			BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f		RTIFICATES	N BACK	
		•				

FIGURE 6-18: MQTT CONNECTION SCREEN WITH UPDATED TOPIC LIST







The topic subscription setting will be saved. Figure 6-19 shows this topic added.

🕼 MQTTE	xplorer				-	
Application	Edit View					
=	MQTT Explorer	Q Search	0		DISCONNEG	ст 🗞
	_		Торіс			^
	+ Connections	MQTT Connection	mqtt://broker.hivemq.com:1883/			
	mqtt.eclipse.org mqtt://mqtt.eclipse.org:1883/	Topic		QoS	+ ADD	^
	test.mosquitto.org S mqtt://test.mosquitto.org:8885/	Торіс			QoS	
	mqtt1 mqtt://192.168.1.52:1883/	\$\$Y\$/#			0	~
	mqtt2 mqtt://192.168.1.53:1883/	spp/#			0	
	mqtt3 mqtt://192.168.1.49:1883/					
	test.mosquitto.org mqtt://test.mosquitto.org:1884/	MQTT Client ID				BLISH
	broker.hivemq.com mqtt://broker.hivemq.com:1883/	mqtt-explorer-11870c2f	CE	ERTIFICATES	M BACK	

FIGURE 6-19: MQTT CONNECTION SCREEN WITH UPDATED TOPIC LIST

You can click on the **Back** button and connect to the MQTT server.





If all settings are correct, the connected Gateway hostname and all its sensors will be displayed after 1-2 minutes. Figure 6-20 shows hostname and sensor information for a connected Gateway.

🕼 MQTT Explorer				- 🗆 X
Application Edit View				
	Q Search	•		DISCONNECT 🗞 🙏
<pre>▼ test.mosquitto.org ▼ spp ▶ 000BDC016910 (16 topics, 267 m ▼ 000BDCDD7704 ▼ sensor ▼ value_change 0.0.0.1.0 = { "timestamp" : 16: 0.0.0.1.1 = { "timestamp" : 16:</pre>	1essages) 30924115, "value" : 51, "status" : 2 } 30924115, "value" : 26.8, "status" : 2 }		Value History Publish Topic spp/000BDCDD7704/sens raw xml json O O O O O O O O O O O O O	or/value_change ×

FIGURE 6-20: MQTT EXPLORER SCREEN SHOWING GATEWAY HOSTNAME AND CONNECTED SENSORS

In our example, that is the 000BDCDD7704 host, but there is already another AlertWerks Plus Gateway visible in this topic.

NOTE: If you only want to subscribe to and display the values for a single host, disconnect the server and go back to the "Advanced" configuration to specify a different topic setting.





In Figure 6-21, we reconfigured the topic to only display sensor values and statuses from 000BDCDD7704, our example host.

The topic setting is spp/000BDCDD7704/#.

🕼 MQTT Explorer			-	o x	
Application Edit View					
	Q Search		DISCONNE	ст 🕹	
+ Connections mqtt.eclipse.org mqtt://mqtt.eclipse.org:188 test.mosquitto.org mqtt://test.mosquitto.org:88 mqtt1 mqtt://192.168.1.52:1883/ mqtt2 mqtt://192.168.1.53:1883/	MQTT Connection mqtt://test.m Topic spp/000BDCDD7704/# S S S S S S S S S S S S S	nosquitto.org:8885/ QoS 0 🕶	+ ADD QoS 0 0	A X BLISH	
mqtt3 mqtt://192.188.1.49:1883/ test.mosquitto.org mqtt://test.mosquitto.org:18 broker.hivemq.com mqtt://broker.hivemq.com:1	84/ MQTT Client ID mqtt-explorer-1466d587	CERTIFICATES	► BACK) retain	

FIGURE 6-21: MQTT CONNECTION SCREEN WITH RECONFIGURED TOPIC

NOTE: The Topic Principle section in chapter 2 discusses using wildcards.



As shown Figure 6-22, only our Gateway and its sensors are subscribed to this topic.

MQTT Explorer Application Edit View						- 🗆 X
MQTT Explorer	Q Search	0			DISCONNEC	т 🛆 😣
▼ test.mosquitto.org ▼ spp ▼ 000BDCDD7704 ▼ sensor		-				
▼ value_change 0.0.0.1.1 = { "timestamp" : 163 0.0.0.1.0 = { "timestamp" : 163	0924595, "value" : 29.3, "status" : 2		Value			^
		-	 History 			
			Publish			^
		:	spp/000BDC	DD7704/se	nsor/value_char	ige ×
			0 (0		PUBLISH

FIGURE 6-22: MQTT EXPLORER SCREEN WITH TOPIC SETTING RESULTS

As noted earlier, the supported MQTT topic settings on AlertWerks Plus Gateways have the following format: spp/\${DeviceID}/sensor/status_change/\${SensorID} spp/\${DeviceID}/sensor/value_change/\${SensorID}

You can narrow down the topic subscription, based on your needs.





6.2 HOW TO FIND SENSOR COMPOUND ID

The compound ID could be found from any SNMP OID of the given sensor.

In Figure 6-23, a temp/humidity sensor is connected to port 3. The active sensor is the Humidity sensor.





After you connect the sensor, open the **Get SNMP OID** window and choose any OID for the humidity sensor. Figure 6-24 shows SNMP OID information.

🕤 SN	MP OID of Dual Humidity Port 3 - Google Chrome			-	×
	lot secure http://192.168.1.57/app.html#/sensorOid/51	2/2/Dual%20Humidity%20Port%	6203		
SN	IMP OID of Dual Humidity Port 3				
	↑ Description	∱ Syntax	Access	SNMP OID	
	humidityAcknowledge	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.70.0.0.2.0	
	humidityDelayError	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.14.0.0.0.2.0	
	humidityDelayHighCritical	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.19.0.0.0.2.0	
	humidityDelayHighWarning	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.18.0.0.0.2.0	
	humidityDelayLowCritical	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.16.0.0.0.2.0	
	humidityDelayLowWarning	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.17.0.0.0.2.0	
	humidityDelayNormal	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.15.0.0.0.2.0	
	humidityDescription	DISPLAY STRING	read-write	.1.3.6.1.4.1.3854.3.5.3.1.2.0.0.0.2.0	
	humidityDisplayStyle	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.45.0.0.0.2.0	
	humidityGoOffline	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.8.0.0.0.2.0	
	humidityHighCritical	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.12.0.0.0.2.0	
	humidityHighCriticalColor	INTEGER	read-write	.1.3.6.1.4.1.3854.3.5.3.1.54.0.0.0.2.0	

FIGURE 6-24: SCREEN SHOWING SNMP OID INFORMATION

The last 5 digits of the OID is the compound ID, such as .1.3.6.1.4.1.3854.3.5.3.1.70.0.0.2.0

Then associate the same compound ID when viewing MQTT data.







In Figure 6-25, you can see 0.0.0.2.0 compound ID belonging to the humidity sensor.

C MQTT Explorer				- 🗆 X
MQTT Explorer	Q Search	•	DISCO	NNECT 🗞 🙏
▼ broker.hivemq.com ▼ spp ▼ 000BDC014FDF ▼ sensor ▼ value_change 0.0.0.2.0 = { "timestamp" : 162	7280798, "value" : 65, "status" : 2 }		Topic 🚡 📑 3	∧ value_change
0.0.0.2.1 = { "timestamp" : 162 0.1.0.9.0 = { "timestamp" : 162	7280798, "value" : 32.0, "status" : 2 } 7280798, "status" : 8 }		Value	^
			► History	_
		:	Publish	^
			raw xml json	_change ×

FIGURE 6-25: SCREEN SHOWING SENSOR WITH ASSOCIATED COMPOUND ID



6.3 DETAILED EXPLANATION OF COMPOUND ID STRUCTURE

Compound ID consists of:

Expansion port	Board position	PCard position		Sensor port	Sensor sub-port
0: Main board	0: Main board	PCard		Starting	Starting
1: Exp chain	1: Internal board	I2C address		from 0	from 0
2: Exp I2C BEB	3: Virtual board				
	4: *Software board				
	6: Modbus board				
	* = not used				
Examples of Compoun	d IDs:				
Dry Contact on Main	RJ-45 Sensor port 1:	C	0.0.0.0.0		
Temperature sensor o	n Main RJ45 Sensor por	t 3 subport 2: 0	0.0.0.2.1		
Virtual sensor port 6:		C	0.3.0.5.0		
Temperature sensor o	n port 3 of Sensor4:	C	0.0.1.2.0		
Relay port 2 of Relay	PCard, module 1.2 on BE	:B: 2	2.1.2.1.0		







A.1 UPLOADING SSL SECURITY CERTIFICATES

A.1.1 BROWSER CONNECTIONS AND LOG IN ISSUES

NOTE:

The only supported browsers are Google Chrome and Mozilla Firefox. With other browsers, the Web UI might not load correctly. Newer versions of third-party browsers (from 2020 on), including Chrome, will eventually include new security restrictions for HTTPS that will affect your connections to our gateways and to our management web interface.

You have two options to avoid the browser connection issues when connecting to our units' web interfaces. The first option is to simply use HTTP and not HTTPS. The second option is to replace or upload your own valid, trusted HTTPS certificate, and, if necessary, add this certificate to your trusted certificate lists within the browser.

A.1.2 HTTPS

The HTTPS port on the units and APS is always enabled. You can change its listening port, if necessary. On the Plus Gateways, the HTTPS supports TLS v1.1 and v1.2.

The HTTPS cypher suites are not customizable.

To eliminate browser warnings about the self-signed SSL certificate, you will need to replace it.

Use the **Upload Certificate File** option to upload an SSL certificate that will be used by the unit or APS Web UI for HTTPS connection (see below).

A.1.3 SSL CERTIFICATE

SSL certificates are generated for DNS host names and not IP addresses. Therefore, you should set a host name for the Plus gateway in your local DNS server or DHCP server, and then generate the SSL certificate for that host name. APS on Windows will use the computer's hostname, and L-DCIM can customize the host name in the **Settings** menu.

Example full hostname: spplus.mycompany.org

Wildcard SSL certificates, such as *.mycompany.org, should also work, but this hasn't been tested.

If the name doesn't match the one in the certificate, the browser will display a security warning.

You can purchase a certificate from a trusted, verified Certificate Authority, such as GoDaddy, or use your company's own CA if you have one.

NOTE: Only non-password protected certificate files are supported.



When you select the file for uploading, a warning will appear if the file is not in the correct .PEM format, as shown in Figure A-1:



The web server used in the Plus gateways and APS WebUI uses a special Linux format (PEM) for the certificate.

The .PEM file is the private key + certificate combined in one file (key on the top and certificate right below it). You can copy them to one file using Notepad++ if you have two separate files, as shown in Figure A-2.

NOTE: The file must be in Unix Line Format, not Windows format.

📔 us	erkey.pem - N	Votepad++											_	x
<u>F</u> ile	<u>E</u> dit <u>S</u> earch	<u>V</u> iew E <u>n</u>	coding	<u>L</u> anguage	Settings	Macro	<u>R</u> un <u>F</u>	lugins	Window	2				 X
1	BEGI	N RSA PRI	VATE K	EY										~
2	MIIEowIBA	AKCAQEA2w	ikww35S	96aYwv9KK	3RzABhpVE	39S70pP(<u>)</u> VmXrXR	c2YhKri	BfF					
3	IfIV1/mn1	IPqFVUJyK	wpSIg9	D38d0TCfS	U5bMT4000	(61/V4g	Qz2AU7	9qfVUQ	191					
4	DhJq7CMp4	HpLq9Mcrd	J+Rs0X	yy+Z3TITc	eiAktA6G[)xY2mEf\	/UTPgGu	bEYWOp	QqA					
5	LEBNOWcqR	gU7nRipbp	5f/EnA	uYoLGN3Dq	WbB7zXmy	g9ZRdCQ9	SFQKB69	Susi1b	NgW					
6	8Mc5dmFcF	XgfUcubQu	UpynaR	7frlxfNIw	3b9on7Ekf	MSTCCI	f4wDSgz	wW0dxp	1CH					
7	Eo3QVA/1+	tS0Aqooa+	ypuZ4c	R4yIexYAd	ukseQIDA(ABAOIBA	QCF6t+	SlviZC	5WY					
× ×	m0c4vFDXT	RVg5mnptb	вртука	XVUCCGXTR	AU2FPIAAI	LDZWEIS	BRCSC5	P12Q1X	110					
10	MOTO MARK	SLEINWIDH	GNoGOO	VZOEGEZYK	+/REPemur	MVpMOSI	15501N	~DPDDAT	eo/ 4cA					
11	v5bmcNJsE	ov@Udp1c3	GwV9pv	FLVOHdd35	<pre>cA8d01/5l</pre>	1/V3mv59	Mixor7p	UwUnid	4CA 2v5					
12	RSVHOTHTO	VEckmVBko	ZBd1MC	wi /40076w	idBX0aKW9	ai2Btyl	IPKyTfR	v/Wsllc	אדר אדר					
13	c+vLibrRA	oGBAP6C2M	25230n	ZB5CKJTmA	a4xKm/Raz	DSiwkJł	F98fH2	uKm6Z5	fsR					
14	/ek0iD0t+	2xI7tX7jf	0ZS5rz	18e3ymB29	70DnwcMi2	288yb00k	cEwfk1	HcLiRr	faG					
15	+PZz1vsyt	qoTmhj3ĎM	l+ML6eG	837T5usvC	VoPhL2By(:ycfeQ+:	J14TmXR	1AoGBAI	N×R					
16	N16Jsjfpp	cBDhWQ7HS	L9W9Yb	VØs6VVXEP	9JYxiaNYv	vvQAWjJe	elct0eB	Cm8LbC	gq/					
17	qwVZ18SId	/v85mBP/w	+tV5pn	h3aejZGsr	FJh0oezVf	F/+5311d	eGN77e	+LIfc7	AVe					
18	NikCNFMww	ER5hvVa6y	4eU5U5	4y4bzJ21U	ZhPQMd1Ac	GAIrHno	DPbiaD	jDxTpv:	1KT					
19	jBF7vX6I5	EapFXRMrU	+1EOT7	N9SW+2D6g	hjPDGx9R8	3exd04x	jv0xx0/	Jsxok5	n2R					
20	StF4j1dxc	pqQzdAqxn	E750EE	psSF0IQx0	Db+aYQCTr	EZYqnof	WSA3A+	ThgiRB	CKH					
21	XdWbvNHCX	gJ/TuwCAv	UdCDKC	gYAdjYtml	AO1+mVwd9	4xxrgul	LFt4Sey	Yu/dsri	MI+					
22	Iseirjur/	X3NK32TAS	NW+J5a	MTW14YT41	MT JpgaqW	19 Ingeul	18/Pa2m	IYK10Z	CHF Ewd					
25	MR0wb0KRg	A1-19001-2	TCOrda						2WL					
24	PiaGvyOav	AIJOPFE23 AAIJOPFE23	ACST-0	RhhuuV404		11 UNI K2	ann Smith	iOnhiel	PJJ F78					
26	e6nvThd2a	S1mPhUdDh	YTa7Uk	1c7En/P20	RhNNØPRde	aoU721	IVEB	TOUDEC	220					
27	END	RSA PRIVA	TE KEY		itoritor ita:									
28	BEGI	N CERTIFI	CATE											
29	MIIDTjCCA	jYCCQDLi/	D8hB/C	1DANBgkqh	kiG9w0BAQ	UFADBp	IQswCQY	DVQQGE	wJa					
30	WjEWMBQGA	1UECAwNVX	Nlc19M	b2NhdG1vb	jEVMBMGA1	LUECgwM	/XNlcl9	Db21wY	W55					
31	MQØwCwYDV	QQDDARVc2	VyMRww	GgYJKoZIh	vcNAQkBFg	g11c2Vy(QHVzZXI	ubmV0M	B4X					
32	DTE3MDcwN	DA4MzkyM1	oXDTI3	MDcwMjA4M	zkyM1owa1	relmakg/	A1UEBhM	CWloxF	jAU					
33	BgNVBAgMD	VVzZXJfTG	i9jYXRp	b24xFTATB	gNVBAoMDF	VzZXJf	29tcGF	ueTENM	AsG					
34	A1UEAwwEV	XN1cjEcMB	oGCSqG	SIb3DQEJA	RYNdXN1c	Blc2Vyl	.m5ldDC	CASIWD	QYJ					
35	KoZIhvcNA	QEBBQADgg	EPADCC	AQOCggEBA	NSJMMN+U\	/emmML/S	Sit0cwA	YaVQ†U	u9K					
30	10F21610X	NMISQWXXS	нугатъ	Pasperente	CISKUIIP(29/HOEWr	1010WZE	+NDqut	TIE Nob					
38	H1VE74Bcm	VGETOLIKOC	'×∆TTln	KED050VIII KEVE050Va	KOSTKUNFO WGeV/v1wl	mKCvidu	iShogut Glmwe8	QUIIBOW 15soPul	ирп ПХО					
39	kEhUCgevU	rrTtW7YEv	DHOX7h	XBV4H1HI m	ØI 1Kcn2ke	-365cX79	5MN2/al	+x38T0	llwø					
40	iE+MA0oM8	FtHcadOhx	KNØFOP	SfrUtAKaK	GvsabmeHE	EeMiHsW4	AHbpLHk	CAWEAA	TAN					
41	BgkahkiG9	WOBAQUFAA	OCAOEA	movxRB7V0	aMYTtUI+	omTg1IFL	.sg8DUL	Xfau7k	vmr					
42	MPIuYFFLB	nYzgeXHsH	IsHujvg	veKhBmAnZ	IWEWKK2RF	RkveBqZe	b3XCUt	ohuHTx	U17					
43	721mHWlku	yWMnQnRsu	pOwZcx	R5c05uhXz	vs1xP2MHz	zzGa7hBn	n/Zzxaz	00j5s8	Ced					
44	7ElbAKt7E	5nr0D8yzE	Sqb4uS	BonhUuy7/	XKdNHcBIE	BzNYtnT	jw0dVLo	9srQy4	Ka9					
45	Axm3yrIny	tiF+0mWt+	VOiAfW	1UX2J1Xmp	8VJnM5H1l	JGh7NZG	59qGvGK	Ex1qcK	XxH					
46	rr3DPTV54	XCws4eCE9	YSVDBC	bngd7Ye8c	qTd/WT+Ql	<1P4A==								
47	END	CERTIFICA	TE											~
Normal	text file		ler	nath : 2 884	lines : 48		In:1	Col: 1	Sel: 010)	Unix (LE)	UTE-	8	NS .
. tornia	i ceste rine		101	.gan . 2,004		_		Contra	Serroro		STIX (EF)	UII-	-	

FIGURE A-2: .PEM FILE EXAMPLE

1.877.877.2269



If you don't upload a certificate, the built-in certificate will be used. A browser warning about an incorrect certificate will appear upon opening the Web UI. This is normal, and you should add it as an exception or proceed, depending on your browser.

A.1.4 UPLOADING THE .PEM FOR APS WEB UI

You can upload the .PEM file in the Server Settings / Services menu as shown in the Figure A-3 below:

-		
Serv	ver Settings	Services
*	Connections	Settings / Server Settings / Services
07	VPN	Active Services
	Event Logs	Web Istorface (HTTD)
۲	Notification	
0	NTP	HTTP Port 80
Ô	LDAP	
0	Language	Secure Web Interface (HTTPS)
0	Services	443
_		Upload Certificate File
		Select Certificate File UPLOAD
		SAVE CANCEL

FIGURE A-3: UPLOAD BUTTON ON SERVICES MENU

- 1. Use the **Browse** button to locate your .PEM file.
- 2. Once you locate your file, use the **Upload** button to upload it.
- 3. After you click on the **Save** button, you will be asked to restart the APS service in order to proceed with the new certificate, as shown in Figure A-4:

Server Restarting

For the changes to take effect, the Server must be restarted. Do you want to continue? The system will automatically redirect to login page.

NO

YES

FIGURE A-4: RESTART CONFIRMATION SCREEN



A.1.5 MANUALLY REPLACING THE HTTPS CERTIFICATE FOR APS

If you cannot upload the .PEM, manually replace the HTTPS certificate of APS HTML UI on Windows.

To manually replace the certificate:

1. Create the correct PEM file.

(If necessary, ask your local system administrator for help with this process or follow the previous instructions.)

- 2. Stop all APS services using the **Server Manager**: **Service** menu / **Stop service**.
- 3. Navigate to C:\Program Files (x86)\Black Box\AKCess Pro Server\bin\SSL.
- 4. Make a backup of the existing **http_cert.pem** file.
- 5. Copy your custom .pem file there.
- 6. Delete the old http_cert.pem file.

CAUTION: Don't delete "server.pem".

- 7. Rename your custom .pem to http_cert.pem.
- 8. Start all APS services again using the Server Manager.
- 9. Open the APS HTML UI and verify your SSL certificate has been replaced.

Favorites	Name *	Date modified	Туре	Size
Desktop	http_cert - Copy.pem	4/2/2018 2:59 AM	PEM File	3 KB
E Recent Places	http_cert.pem	7/4/2017 3:45 PM	PEM File	3 KB
Libraries	server.pem	4/2/2018 2:59 AM	PEM File	2 KB

FIGURE A-5 DELETING HTTP_CERT.PEM FILE

NOTE: The HTTPS issues discussed above are not problems with our server software or AlertWerks gateways. They are caused by a generic security feature in third-party web browsers that we cannot control.

Moreover, f you decide to use the manual replace method, it is your responsibility to manage your own HTTPS certificates in order to access our product's web user interface.







A.1.6 UPLOADING THE .PEM FOR PLUS GATEWAY WEB UI

To upload the .PEM for the Plus Gateway Web UI, open the Settings / Services menu as shown in Figure A-6:

System System Services System / Services Web Interface Modem Cloud Server Cloud Server SMTP SMTP SMMP Services Services			
Services Date / Time Date / Time Network Web Interface Modem Cloud Server Cloud Server NTTP Port SMTP SMTP SMMP Services	System		
Bate / Time System / Services Network Web Interface Modem Web Interface (HTTP) Cloud Server HTTP Port SoftP 80 SMTP Enable © Disable © Use as Default SMMP HTTPS Port Server Integration Upload Certificate File Services Save Services Save Services Save Services Save	🗱 General	Services	
Metwork Web Interface Moden Web Interface (HTTP) Cloud Server HTTP Port SMTP 80 SMTP Enable SMP Enable Services Upload Certificate File Services Save Modbus Cancel	🋗 Date / Time	System / Services	
Kodem Web Interface (HTTP) Enable Cloud Server HTTP Port 80 VPN SMTP SMTP SNMP Server Integration Upload Certificate File Services Services Modbus Password Checking	📥 Network	Web Interface	
 ▲ Cloud Server ▲ VPN ▲ SMTP ▲ SNMP ▲ Server Integration ▲ Services ▲ Services ▲ Services ▲ Password Checking 	< Modem	Web Interface (HTTP)	enable Oisable
◇ VPN > SMTP → SNMP ◇ Server Integration > Services ◇ Modbus → Password Checking	Cloud Server	HTTP Port	80
SMTP SMTP SNMP Server Integration Services Services Save Cancel	VPN		
► SNMP 443 ✓ Server Integration Upload Certificate File ▲ Services Choose file ▲ Modbus Save Cancel ● Password Checking	SMTP	Secure Web Interface (HTTPS)	Enable O Disable O Use as Default
✓ Server Integration Upload Certificate File Choose file Services Save Cancel		HTTPS Port	443
 Services Modbus Password Checking 	Server Integration	Upload Certificate File	Choose file
Modbus	Services		Cancel
Password Checking	A Modbus		Calicer
	Password Checking		



1. Click on the Choose file button next to the Upload Certificate File field.

If the file format is correct (see instructions below), then your certificate can be used immediately. You can open Web UI with HTTPS and verify that your SSL certificate is used.

If there is a problem with the certificate and Web UI doesn't open with HTTPS, open it again using HTTP and replace the .PEM file again.

NOTE: On older F4 platform gateways, the .PEM's total file size must be less than 4KB, regardless of the used private key size. If you exceed this file size, the unit won't be able to use the certificate, and the Web UI won't load over HTTPS.

Also note that using a very large private key can cause Web UI slowdown. The newer F7 platform units, however, don't have this limitation.



A.1.7 UPLOADING THE .PEM FOR V4E WEB UI

Open the **Settings** / **Services and Security** menu and click on the **Add Key** button to upload the .PEM file. as shown in Figure A-7:

Sensors	Notification	Settings	Applications
	Services and Sec	urity	
	Active Services		
Active S	Nagios Secure Shel Telnet Web Interfac port to use Secure Web port to use Add Key Simple Netw Serial to Netw AKCess Pro Ethernet Wa	II ce (HTTP) 8 80 Available 9 Interface (HTTPS) 9 443 Available vork Management Protoc vork Management Protoc twork Proxy (ser2net) 9 Server Integration atchdog	Port Port ol Version 1 (SNMPv1) ol Version 3 (SNMPv3)
	Save Reset		

FIGURE A-7: "ADD KEY" OPTION

After you click on the Add Key button, a pop-up window, as shown in Figure A-8, will appear.

Select ssl key
File - Chasse File No file shoren
File : Choose File No file chosen
Add File
file name must be userkey.pem
Close

FIGURE A-8: CHOOSE FILE POP-UP WINDOW

When you select the file for uploading in the popup window, a warning message will appear if the file is not in the correct .PEM format (see below).

NOTE: The file name MUST be "userkey.pem". Rename the file, if necessary. Also note that using a very large private key can cause Web UI slowdown.





See below for troubleshooting instructions in case the unit's WebUI no longer loads.

A.1.8 HOW TO TROUBLESHOOT A FAILED WEB UI ON THE SEC5

NOTE: These steps are only for troubleshooting a bad SSL certificate file, which prevents the unit's Web UI from appearing because the Apache service cannot start.

The SSL certificate which you can upload from the Web UI will be stored as this file:

/flash1/user/init.d/userkey.pem

If this file doesn't exist, then the unit's built-in certificate will be used. If the uploaded certificate is a broken file, remove it and restart Apache to get a working Web UI.

1. Log in to the unit's SSH console as the root user. (The password is whatever the SNMP write community is named.)

You then have two options:

a) Remove the corrupt .pem file, which will cause the default certificate to be used by using the following command:

rm /flash1/user/init.d/userkey.pem

b) Overwrite the corrupt .pem file with a file that you know is good by using the following command:

cat >/flash1/user/init.d/userkey.pem

and then copy the certificate contents, press <Enter> and then press <Ctrl> <D>.

2. After removing or overwriting the certificate, restart Apache by using the following command: /etc/rc.d/init.d/apache restart

3. Try to log in to the Web UI again.





A.1.9 HOW TO GENERATE A PROPER .PEM FILE FROM A WINDOWS CA

NOTE: Only non-password-protected certificate files are supported.

First, make the .PFX file export using the steps below: (taken from <u>https://www.sslsupportdesk.com/export-ssl-certificate-private-key-pfx-using-mmc-windows/</u>)

To create a backup, export an SSL certificate with its private key and intermediates by following the steps below:

Step 1: Create an MMC Snap-in for Managing Certificates on the first Windows system where the SSL certificate is installed by following the steps below:

1. Start > run > MMC.

🖅 Run		X
	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
Open:	mmc	
	🕐 This task will be created with administrative privileges.	
	OK Cancel Browse	
	FIGURE A-9: START/RUN SCREEN	

- 2. Click on the **OK** button.
- 3. Go into the Console Tab > File > Add/Remove Snap-in.



FIGURE A-10: ADD/REMOVE SNAP-IN OPTION





4. Click on Add > Click on Certificates and click on OK.

ap-in	Vendor		Console Root	Edit Extensions
ActiveX Control	Microsoft Cor			
Authorization Manager	Microsoft Cor			Remove
Certificates	Microsoft Cor			
Component Services	Microsoft Cor			Move Up
Computer Managem	Microsoft Cor	_		
Device Manager	Microsoft Cor			Move Down
Disk Management	Microsoft and			
Event Viewer	Microsoft Cor			
Folder	Microsoft Cor			
Group Policy Object	Microsoft Cor			
Internet Information				
IP Security Monitor	Microsoft Cor			
IP Security Policy Ma	Microsoft Cor			Advanted
Link to Web Address	Microsoft Cor	-	1	Advanced
riotion:				
Link to Web Address	Microsoft Cor	1	1	Autorocom

FIGURE A-11: CERTIFICATES ADD OPTION

5. Choose Computer Account.

tificates snap-in			2
This snap-in will always manage certificates for:			
C My user account			
C Service account			
 Computer account 			
	< Back	Next >	Cancel

FIGURE A-12: NEXT BUTTON

- 6. Click on the **Next** button.
- 7. Choose the Local Computer option.



lect the computer you wa	ant this snap-in to manage.
This snap-in will always m	anage:
Local computer: (the	computer this console is running on)
C Another computer:	Browse
Allow the selected co only applies if you sa	omputer to be changed when launching from the command line. This we the console.

FIGURE A-13: FINISH BUTTON

- 8. Click on the **Finish** button.
- 9. Close the Add Standalone Snap-in window.
- 10. Click on OK at the Add/Remove Snap-in window.





Step 2: Export/Backup certificate to .pfx file:

- 1. In MMC, double-click on Certificates (Local Computer) in the center window.
- 2. Double-click on the **Personal folder**, and then click on **Certificates**.
- 3. Right-click on the certificate that you would like to back up and choose > ALL TASKS > Export.
- 4. Follow the Certificate Export Wizard's instructions to back up your certificate to a .pfx file.



FIGURE A-14: CERTIFICATE EXPERT WIZARD





5. Choose Yes, export the private key.

Certificate Export Wizard			×
Export Private Key			
You can choose to export the private key	with the certificate.		
Private keys are password protected. If y certificate, you must type a password on a	ou want to export the a later page.	private key w	ith the
Do you want to export the private key wit	h the certificate?		
 Yes, export the private key 			
🔿 No, do not export the private key			
Learn more about exporting private keys			
	< Back	Next >	Cancel

FIGURE A-15: EXPORT PRIVATE KEY SCREEN





- 6. Click on the **Next** button.
- 7. Choose Include all certificates in certificate path if possible, but leave Delete the private key if the export is successful unchecked.

Certificate Export Wizard X
Export File Format Certificates can be exported in a variety of file formats.
Select the format you want to use:
C DER encoded binary X.509 (,CER)
C Base-64 encoded X.509 (.CER)
 Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B) Include all certificates in the certification path if possible
 Personal Information Exchange - PKCS #12 (.PFX) Include all certificates in the certification path if possible Delete the private key if the export is successful
Export all extended properties
${f C}$ Microsoft Serialized Certificate Store (.SST)
Learn more about <u>certificate file formats</u>
< Back Next > Cancel

FIGURE A-16: SCREENSHOT WITH "INCLUDE ALL CERTIFICATES IN CERTIFICATION PATH IF POSSIBLE" SCREEN

- 8. Click on the **Next** button.
- 9. Enter a password that you will remember.
- 10. Choose to save file on a set location.
- 11. Click on the **Finish** button.



Certificate Export Wizard		×
	Completing the Certificate Exp Wizard	ort
	You have successfully completed the Certificate Expo wizard. You have specified the following settings:	ort
	File Name C:\L	Jsei
	Export Keys Yes	
	Include all certificates in the certification path Yes	
		•
	< Back Finish (Cancel

FIGURE A-17: COMPLETING THE CERTIFICATE EXPORT WIZARD SCREEN

12. After you receive a message stating "The export was successful," click on the **OK** button. The .pfx file backup is now saved in the location that you selected.

After this process is complete, you can peform the .PEM conversion in two ways: using OpenSSL (recommended) or using the DigiCert utility.

Option 1: Use OpenSSL with proper parameters.

Refer to:

http://www.thawte.nl/en/support/manuals/microsoft/all+windows+servers/export+private+key+or+certificate/

- Export the private key file from the pfx file: openssl pkcs12 -in filename.pfx -nocerts -out key.pem
- 2. Export the certificate file from the pfx file:

openssl pkcs12 -in filename.pfx -clcerts -nokeys -out cert.pem





- 3. Remove the passphrase from the private key: openssl rsa -in key.pem -out server.key
- 4. When the exports complete, combine the **server.key** (without password) and **cert.pem** files with Notepad++ and save as **USERKEY.PEM**.

Option 2: Use the DigiCert utility and export it as Apache compatible key.

Refer to:

https://www.digicert.com/util/copy-ssl-from-windows-iis-to-apache-using-digicert-certificate-utility.htm

			DigiCert Certific	ate Utility for W	Vindows©	
digice	rť	CERTIFICA	TE UTILITY /	or windows"	\$ 1.80	0.896.7973
551	Certificates				C Overte CSR	± Import Citationh
Issued	To		Expire Date	Serial Number	Friendly Name	Insuer
Code Signing						
×						
Tools						
Account						
					Export Certificate Test Ke	View Certificate

FIGURE A-18: DIGICERT UTILITY

This webpage shows the SSL already in the DigiCert tool. However, you must perform the following steps:

- 1. Import the .PFX that you just exported from the Windows Cert Manager.
- 2. After the file is imported, proceed with the export steps as written on the page.
- 3. When the export is done, combine the Server Cert and Private Key with Notepad++ and save the new file as **USERKEY.PEM.**

The .PEM file is the private key + certificate combined. You can copy them to one file using Notepad++ if you have two separate files.

NOTE: The file must be in Unix Line Format, not Windows format.

Contact Support if you have any further technical questions or problems.



B.1 FCC STATEMENT

This equipment has been tested and found to comply with the regulations for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this Quick Installation Guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case, the user will be required to correct the interference at his/her own expense.

B.2 CE STATEMENT

This is a Class B product in a domestic environment, this product may cause radio interference, in which case the user may be required to take adequate measures.

B.3 ROHS

This product is RoHS compliant.



B.4 NOM STATEMENT

- 1. Todas las instrucciones de seguridad y operación deberán ser leídas antes de que el aparato eléctrico sea operado.
- 2. Las instrucciones de seguridad y operación deberán ser guardadas para referencia futura.
- 3. Todas las advertencias en el aparato eléctrico y en sus instrucciones de operación deben ser respetadas.
- 4. Todas las instrucciones de operación y uso deben ser seguidas.
- 5. El aparato eléctrico no deberá ser usado cerca del agua-por ejemplo, cerca de la tina de baño, lavabo, sótano mojado o cerca de una alberca, etc.
- 6. El aparato eléctrico debe ser usado únicamente con carritos o pedestales que sean recomendados por el fabricante.
- 7. El aparato eléctrico debe ser montado a la pared o al techo sólo como sea recomendado por el fabricante.
- 8. Servicio-El usuario no debe intentar dar servicio al equipo eléctrico más allá a lo descrito en las instrucciones de operación. Todo otro servicio deberá ser referido a personal de servicio calificado.
- 9. El aparato eléctrico debe ser situado de tal manera que su posición no interfiera su uso. La colocación del aparato eléctrico sobre una cama, sofá, alfombra o superficie similar puede bloquea la ventilación, no se debe colocar en libreros o gabinetes que impidan el flujo de aire por los orificios de ventilación.
- 10. El equipo eléctrico deber ser situado fuera del alcance de fuentes de calor como radiadores, registros de calor, estufas u otros aparatos (incluyendo amplificadores) que producen calor.
- 11. El aparato eléctrico deberá ser connectado a una fuente de poder sólo del tipo descrito en el instructivo de operación, o como se indique en el aparato.
- 12. Precaución debe ser tomada de tal manera que la tierra fisica y la polarización del equipo no sea eliminada.
- 13. Los cables de la fuente de poder deben ser guiados de tal manera que no sean pisados ni pellizcados por objetos colocados sobre o contra ellos, poniendo particular atención a los contactos y receptáculos donde salen del aparato.
- 14. El equipo eléctrico debe ser limpiado únicamente de acuerdo a las recomendaciones del fabricante.
- 15. En caso de existir, una antena externa deberá ser localizada lejos de las lineas de energia.
- 16. El cable de corriente deberá ser desconectado del cuando el equipo no sea usado por un largo periodo de tiempo.
- 17. Cuidado debe ser tomado de tal manera que objectos liquidos no sean derramados sobre la cubierta u orificios de ventilación.
- 18. Servicio por personal calificado deberá ser provisto cuando:
 - A: El cable de poder o el contacto ha sido dañado; u
 - B: Objectos han caído o líquido ha sido derramado dentro del aparato; o
 - C: El aparato ha sido expuesto a la lluvia; o
 - D: El aparato parece no operar normalmente o muestra un cambio en su desempeño; o
 - E: El aparato ha sido tirado o su cubierta ha sido dañada.





C.1 DISCLAIMER

Black Box Corporation shall not be liable for damages of any kind, including, but not limited to, punitive, consequential or cost of cover damages, resulting from any errors in the product information or specifications set forth in this document and Black Box Corporation may revise this document at any time without notice.

C.2 TRADEMARKS USED IN THIS MANUAL

Black Box and the Black Box logo type and mark are registered trademarks of BB Technologies, Inc..

Any other trademarks mentioned in this manual are acknowledged to be the property of the trademark owners.





NOTES



NEED HELP? LEAVE THE TECH TO US



1.877.877.2269



© COPYRIGHT 2022. BLACK BOX CORPORATION. ALL RIGHTS RESERVED EME160A_EME161A-R2_EME164A_EME168A_MQTT_USER_REV1.PDI