

SKF Enlight Collect IMx-1 System



User Manual

Part Number **15V-090-00087-100**

Revision **L** – **January 2025** - **Draft**



Read this manual carefully before using the product. Failure to follow the instructions and safety precautions in this manual can result in serious injury, damage to the product or incorrect readings. Keep this manual in a safe location for future reference.

Copyright © 2019 by SKF Group
All rights reserved.

SKF France
204 Bd Charles de Gaulle, 37540 Saint-Cyr-sur-Loire, France
Telephone: +33 2 47 40 30 00

® SKF is a registered trademark of the SKF Group.

Android is a trademark of Google LLC.

The Bluetooth® word mark and logos are registered trademarks owned by Bluetooth SIG, Inc. and any use of such marks by SKF is under licence.

All other trademarks are the property of their respective owners.

The contents of this publication are the copyright of the publisher and may not be reproduced (even extracts) unless prior written permission is granted. Every care has been taken to ensure the accuracy of the information contained in this publication, but no liability can be accepted for any loss or damage whether direct, indirect or consequential arising out of the use of the information contained herein. SKF reserves the right to alter any part of this publication without prior notice.

Patents: US 4,768,380 • US 5,633,811 • US 5,679,900 • US 5,845,230 • US 5,852,351 • US 5,854,553 • US 5,854,994 • US 5,870,699 • US 5,907,491 • US 5,992,237 • US 6,006,164 • US 6,124,692 • US 6,138,078 • US 6,199,422 • US 6,202,491 • US 6,275,781 • US 6,301,514 • US 6,437,692 • US 6,489,884 • US 6,513,386 • US 6,633,822 • US 6,789,025 • US 6,792,360 • US 7,103,511 • US 7,697,492 • WO/2003/048714

Product Registration

Please take a moment to [register](#) your product to receive exclusive benefits offered only to our registered customers, including technical support, tracking your proof of ownership and staying informed about upgrades and special offers. (Please visit our website for more details on these benefits.)

General Product Information

General information such as datasheets and catalogues are published on the [Condition Monitoring Systems](#) site on SKF.com. Supporting product information can also be downloaded from the [SKF Technical Support](#) self-service web portal.

Product Support Contact Information

[Repair and Calibration Services](#) – Submit a [Return Authorization \(RA\) request](#) to arrange for repair or calibration of your product. You will receive an RA number and shipping instructions usually within 48 business hours.

[Product Support Plans \(PSP\)](#) – SKF offers annual renewal Product Support Plans (PSP) on many condition monitoring products in an effort to extend the life of your product. Software and firmware updates are an exclusive entitlement to PSP customers. Additional benefits include product repair, Annual Preventative Maintenance (APM) and certified calibration - all of which are all carried out on a priority-basis. Enjoy unlimited technical support and access to after-hours support for machine- and process-critical applications.

[Product Sales](#) – For information on purchasing condition monitoring products, services and support on products out of warranty, please contact your [local SKF sales office](#) or [distributor](#).



How to request Technical Support – Please open a support case using the Technical Support group's self-help portal at www.skf.com/cm/tsg. Once your support case is submitted, a technician will contact you to begin working on your issue. For urgent issues we are available at these times:

- Monday through Friday, 5:00 a.m. to 4:00 p.m. Pacific Time
Phone: +1 800 523 7514 within the US or +1 858 496 3627 outside the US.
- Monday through Friday, 8:00 a.m. to 4:00 p.m. Central European Time
Phone: +46 31 337 65 00.
- Monday through Friday, 7:30 a.m. to 4.30 p.m. India Standard Time
Phone: +60 16 699 9506.

120517dm-fp-Feb_2020

Table of contents

1	Product description	9
1.1	Introduction to the SKF Enlight Collect IMx-1 system	9
1.2	System considerations and architectures.....	10
1.3	SKF Enlight Collect IMx-1 wireless sensors.....	11
1.4	SKF Enlight Collect Gateway	12
1.4.1	Connections and interfaces	12
1.4.2	External antennas	14
1.4.3	LED indicators.....	14
1.4.4	Data and event time stamping.....	15
1.4.5	Data acquisition scheduling	15
1.4.6	Local data storage.....	16
1.5	SKF Enlight Collect Manager – Android and iOS app.....	16
1.5.1	Security	19
1.6	Third party licences.....	19
2	Integration with SKF @ptitude Observer	20
2.1	@ptitude Observer overview and prerequisites	20
2.1.1	Communication with the SKF Enlight Collect IMx-1 system.....	20
2.1.2	Users and security role rights	23
2.1.3	Enlight Collect IMx-1 System global settings.....	23
2.2	Hierarchy view – adding sensors and measurements	24
2.2.1	On-demand measurements	28
2.3	Enlight Collect IMx-1 System View.....	28
2.3.1	Gateways	30
2.3.2	Sensors	31
2.3.3	Mesh Statistics	32
2.4	IMx-1 system configuration.....	33
2.4.1	Gateway	33
2.4.2	Sensor.....	40
2.4.3	Synchronisation of configuration changes.....	41
2.4.4	Gateway or sensor Hardware ID	42
2.5	Use of @ptitude Observer machine templates	43
3	Installation and commissioning	44
3.1	Overview and prerequisites	44
3.1.1	System commissioning and security.....	44

3.2	SKF Enlight Collect gateway	46
3.2.1	Introduction	46
3.2.2	Gateway mounting	47
3.2.3	Power requirements	48
3.2.4	Network connections and configuration	50
3.2.5	Commissioning	52
3.2.6	External antennas	53
3.2.7	Other interfaces	56
3.3	SKF Enlight Collect IMx-1 wireless sensors	56
3.3.1	Installation considerations	56
3.3.2	Mounting detail	57
3.3.3	Pre-commissioning tasks	58
3.3.4	Commissioning	58
3.4	Relay node commissioning	59
3.5	Generating a commissioning report	60
3.6	Offsite commissioning	60
4	Maintenance functions	64
4.1	SKF Enlight Collect IMx-1 wireless sensor	64
4.1.1	Updating sensor firmware	64
4.1.2	Sensor replacement or removal	65
4.1.3	Sensor maintenance	66
4.1.4	Sensor performance over time	66
4.2	SKF Enlight Collect Gateway	66
4.2.1	Updating firmware	66
4.2.2	Modify gateway network configuration	67
4.2.3	Decommissioning	67
4.2.4	Replacement	68
4.2.5	Gateway maintenance	69
4.2.6	Gateway performance over time	69
4.3	Troubleshooting	69
4.3.1	Introduction	69
4.3.2	Logs and viewers	70
4.3.3	IMx-1 sensor troubleshooting	74
4.3.4	Gateway troubleshooting	76
4.3.5	Commissioning troubleshooting	77
4.3.6	System connectivity	79
4.3.7	Gateway interfaces for SKF personnel	80

5	CMWA 6100-EX Sensor	83
5.1	Contact.....	83
5.2	ATEX/IECEX hazardous location approval	83
5.2.1	General.....	83
5.2.2	Specific conditions of use ("X")	84
5.3	EX Sensor installation.....	84
5.4	EX Sensor maintenance	84
5.5	EX Sensor repair.....	84
5.6	EX Sensor caution	84
6	CMWA 6600-EX Gateway	85
6.1	Contact.....	85
6.2	Introduction	85
6.3	ATEX/IECEX hazardous location approval.....	87
6.3.1	General.....	87
6.3.2	Specific conditions of use ("X")	88
6.4	EX Gateway cable entry and installation.....	89
6.5	EX Gateway mounting.....	93
7	SKF Enlight Collect IMx-1 System specifications	94
7.1	Enlight Collect Wireless Sensor specifications.....	94
7.1.1	Environmental and physical.....	94
7.1.2	Operational states and battery.....	95
7.1.3	Measurements	95
7.1.4	Signal processing.....	96
7.1.5	Interfaces.....	96
7.1.6	CMWA 6100 certifications.....	97
7.1.7	CMWA 6100-EX certifications.....	100
7.2	Enlight Collect Gateway specifications.....	102
7.2.1	CMWA 6600 – Environmental and physical	102
7.2.2	CMWA 6600-EX – Environmental and physical	104
7.2.3	Power	104
7.2.4	Internal measurement capabilities	105
7.2.5	Interfaces.....	105
7.2.6	CMWA 6600 certifications.....	107
7.2.7	CMWA 6600-EX certifications.....	113
7.3	Product marks and labelling	114
7.3.1	Marks.....	114
7.3.2	Sensor	115



- 7.3.3 Date code115
 - 7.3.4 Gateway116
 - 7.4 Quality control116
- 8 Electrical waste117**
- Appendix A Limited Warranty119**
- SKF – Limited Warranty119**

1 Product description

1.1 Introduction to the SKF Enlight Collect IMx-1 system

The overall architecture of the SKF Enlight Collect IMx-1 System:

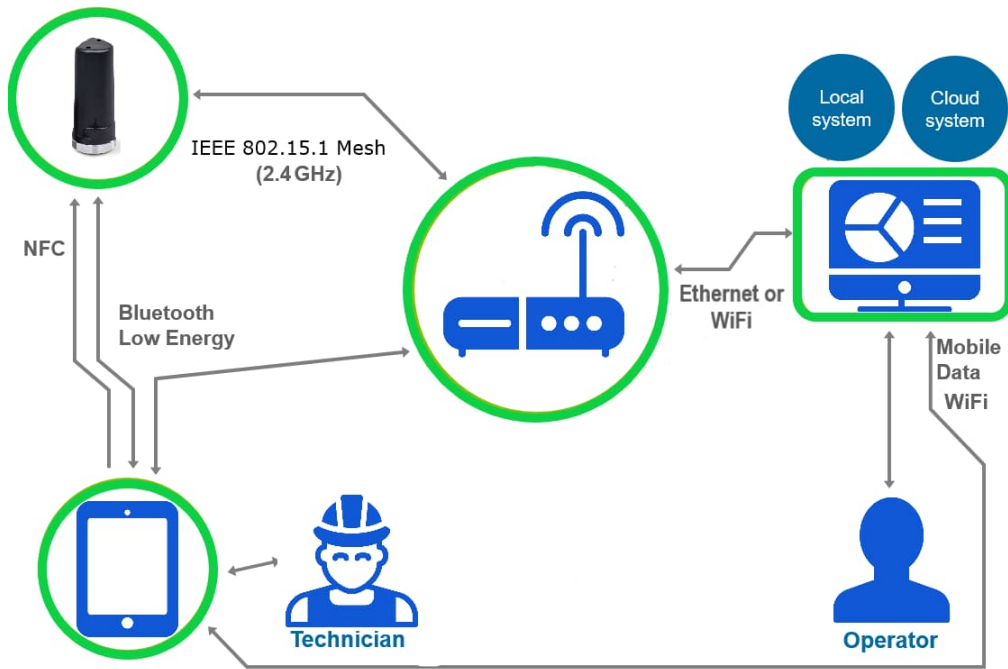


Figure 1 SKF Enlight Collect IMx-1 System architecture – single gateway, one sensor shown

The system consisting of sensors, gateways, analysis and visualisation software and a mobile application for Android and iOS devices, the Enlight Collect Manager app, provides the opportunity for a completely wireless architecture at the monitored machinery.

One gateway and its associated wireless sensors form a communication network. This may also include relay nodes, essentially sensors that have their measurements disabled and that are used to support/extend the wireless mesh. A system consists of the analysis and visualisation software and at least one gateway, although in most systems, multiple gateways are anticipated. Different gateways might typically be applied to different machine groups, production processes or physical plant areas.

According to a user defined schedule, the sensors measure the vibration and temperature of the monitored machinery, pre-process the vibration signals and transmit all the resulting data to the gateway. This is then forwarded to the analysis and visualisation software where the final analysis is performed, and historical data is stored. The analysis and visualisation software, SKF @ptitude Observer, can be installed on a local server at the customer location or as a cloud solution.



If the equipment is used in a manner not specified by the manufacturer, both the safety and functionality of the equipment may be impaired.



Being a Wireless Condition Monitoring System, users must ensure that they abide by the usage requirements and observe the warnings specified in the Product Specifications, Certifications, sections for both the sensor and the gateway.



This equipment is intended for use in a Pollution Degree 2 industrial environment, in overvoltage Category II applications (as defined in IEC publication 60664-1), at altitudes up to 5,000 meters (16,404 ft.) without derating.



For Enlight Collect IMX-1 Ex System product variant usage in hazardous area refer to installation, operation and safety instruction as provided in this manual. Activities including installation, adjustments, putting into service, use, assembly, disassembly, and maintenance are required to be carried out by suitably trained personnel in accordance with the applicable code of practice.

1.2 System considerations and architectures

The sensor – gateway interface is a radio system for wireless mesh networks with a low power consumption and support for over-the-air (OTA) firmware updates. It is specifically designed to enable reliable communication in congested wireless environments and can identify and adapt to changes it has detected. The radio operates on the 2.4 GHz ISM (Industrial, Scientific, Medical) band.

Whilst the wireless range will be dependent on plant topology, being a mesh system, relay nodes can be deployed or outlying sensors can rely on the sensor mesh rather than direct sensor/gateway communication. This assists in industrial environments where a line of sight connection may be restricted or where sensors are situated across wider areas. As a minimum, the system has been designed to support a topography where there are up to 10 node jumps from the gateway to the furthest sensor in the mesh. To provide the sensor mesh with opportunities to adapt, aim for

an installation where each node has at least 3 other nodes within wireless range. This sensor radio interface can operate concurrently with other activity in the same band, including the radios for:

- Wi-Fi or Mobile, a network/@ptitude Observer connection option (refer [Table 12](#) for recommendations on Wi-Fi setup).
- WPAN IEEE 802.15.1 for app interfacing: on a mobile phone, this is known as **Bluetooth®**.

The type of network connection between the gateway and @ptitude Observer software can be chosen to suit specific site requirements. A hard-wired Ethernet connection is the default, but Wi-Fi or Mobile is also provided as a wire free alternative.

Communication between the gateway/sensor and Android/iOS mobile app for on-site sensor and gateway commissioning, is achieved over the phone's Bluetooth Low Energy, radio connection.

For the sensor commissioning, it is first woken from flight mode using the app and the phone to provide an NFC (Near Field Communication) tap. For the gateway, the app **Scan gateway** functionality provides a list of gateways that are broadcasting. By default, the gateway selection from the Bluetooth scan results is manual (select the appropriate gateway from the list) but there is also a QR code option. Using the QR code identification method for the gateway is particularly useful where multiple gateways may be identified in the scan.

Important notes:

Wi-Fi access: for local, on premise, @ptitude Observer installations Wi-Fi access to the server is required so that a connection to the app can be established during commissioning and maintenance. This connection can be just temporary and can precede the commissioning work but is required irrespective of whether Wi-Fi is used for the network connection between the gateway and @ptitude Observer.

Mobile phone: Refer to [SKF Enlight Collect Manager – Android and iOS app](#) for details.

1.3 SKF Enlight Collect IMx-1 wireless sensors

The IMx-1 sensor (CMWA 6100) is aimed at the monitoring of fixed plant and equipment. This battery powered wireless sensor facilitates an Enlight Collect online system replacing traditional periodic monitoring using portable equipment. It supports the following measurements:

- Acceleration
- Velocity
- Enveloping
- Temperature

The sensor has a female mounting thread and can be fixed to the measuring point via a threaded mounting stud or an adapter disc with stud, where the disc is adhesively bonded to the machine.

The CMWA 6100-EX Sensor variant allows for wireless sensor installation in zone 1 hazardous environments.

Note: The general sections of this manual concerning gateway functionality will refer to the standard CMWA 6100 Sensor. Please refer to a separate section on CMWA 6100-EX describing specific installation and operation details for the hazardous area approved assembly variant of the wireless sensor for the IMX-1 system.

1.4 SKF Enlight Collect Gateway

The Enlight Collect Gateway (CMWA 6600) is placed in the production/industrial indoor or outdoor environment, somewhere central to its associated sensors and in a location where power and any required network connections can be made available to it. Each gateway can manage multiple sensors: currently limited to 100 sensors.

The CMWA 6600-EX Gateway enclosure assembly variant allows for gateway installation in zone 2 hazardous environments.

Where possible choose a gateway location that maximises the number of IMx-1 sensors that have a direct line of sight, with it. If the Enlight collect gateway is enclosed inside a metal enclosure, external antennas must be used.

Note: Gateways must be associated with their own set of sensors, a particular sensor can only communicate with one gateway.

Note: The general sections of this manual concerning gateway functionality will refer to the standard CMWA 6600 Gateway. Please refer to a separate section on CMWA 6600-EX describing specific installation and operation details for the hazardous area approved assembly variant of the gateway for the IMx-1 system.

1.4.1 Connections and interfaces

The CMWA 6600 Gateway is housed in an [IP rated](#) enclosure suitable for indoor or outdoor installation (Europe) and has built-in antenna for Wi-Fi/BLE and sensor mesh communications.

The lower panel is the only area normally accessible to the user and conceals connectors for all wired connections. A view of the gateway with its various features and connections highlighted, is shown below:

PRODUCT DESCRIPTION

SKF Enlight Collect Gateway



Figure 2 View on standard (left) and EX gateway (right) electronic modules with key features annotated

To access the connector area, unscrew the two Torx T10 screws on the lower edge of the cover at the locations circled in the figure above.

For EX approved gateway, to access the connector interface, power down the module and remove the top cover of the EX enclosure.

Once this cover is removed, four M12 connectors and one blanking plug are accessible:

1. Connector for dual speed inputs with transducer power (future use)
2. Connector for Ethernet link 2 (future use)
3. **Connector for Ethernet link 1 and PoE**
4. **Connector for DC power input to the gateway**
5. Access to SIM card holder
6. Gateway LED indicators
7. Connector for external Mesh antenna
8. Connector for external Wi-Fi/BLE antenna
9. Connector for external antenna LTE Diversity (Rx) antenna
10. Connector for external LTE Main (Tx/Rx) antenna

Important note: Only the two connectors listed in bold above are usable. Mobile support is only supported through using external antennas. For LTE, both Main and Diversity antennas must be used.

1.4.2 External antennas

When enclosed in an additional (metal) enclosure, external antennas must be connected to communicate via Wi-Fi/BLE, Mesh, Mobile, 3G and 4G.

Note: The external antenna connections are NOT intended for direct antenna installation. At least 20 cm distance will need to be observed between different antennas!

In addition, the usage of an external antenna may be required to optimize wireless reception performance. Different antenna combinations are available depending on the selected type of communication:

- **Ethernet communication:**
 - o Mesh external antenna
 - o BLE external antenna
- **Wi-Fi communication:**
 - o Mesh external antenna
 - o Wi-Fi/BLE external antenna
- **Mobile communication:**
 - o Mesh external antenna
 - o Mobile external antennas
 - o BLE external antenna

1.4.3 LED indicators

The upper front panel of the gateway has positions for two, multi-colour, LED status indicators – item 6 figure 2 above:

- Top, Power LED – furthest from the connector area:
 - o Green fixed: gateway is powered
 - o Off: gateway is unpowered
- Lower, Status LED indicator
 - o Off: gateway is unpowered
 - o White fixed: gateway is starting up
 - o Yellow fixed: gateway is not commissioned

- o Green flashing: gateway is commissioned but not connected to the backend and/or not NTP synchronised
- o Green fixed: gateway connected to the backend and synchronised
- o Red fixed: fatal error (permanent fault, requires manual action)

Connected relates to the establishment of a connection between the gateway and the @ptitude Observer MQTT service.

1.4.4 Data and event time stamping

Each gateway has a backup power capacitor which will maintain the Real Time Clock (RTC) setting for approximately one week if the device is disconnected from power.

1.4.5 Data acquisition scheduling

The gateway is configured with four data acquisition schedules by way of **Interval** and **Interval alarm** settings for both the **Trend measurements** and **Dynamic measurements**. The **Measurement schedule** can be set in **Active time period** by selecting from-to time span. The weekday on which the measurement should be performed can also be selected. These schedules are common to sensors associated with a machine and are set in @ptitude Observer at the Machine Properties level, Enlight Collect IMx-1 System tab, see [Gateways](#).

Notes on scheduling and measurements:

To ensure sensor network stability, the gateway is a master to the multiple sensor “slaves” so a sensor can never initiate a measurement nor the transfer of data to the gateway. Measurement and measurement data transfer is always at the request of the gateway and these requests are sent sequentially to the different sensors.

After a start-up the gateway will wait for the configured interval period before requesting the “first” sensor measurements. If changes are made to the schedule and these changes are synchronised, any ongoing measurement cycle for the machine will complete and then the new schedule will be implemented.

In addition, whenever a sensor receives a new configuration, for example and including its initial configuration during commissioning, the gateway will then request that the sensor make a set of overall measurements, without waiting for the configured time period. This ensures a timelier receipt of data during commissioning rather than having to wait for the scheduled time to elapse.

When the gateway first detects an alarm state change from a sensor on the machine, that will trigger requests for representative TWF data from all sensors on that machine.

If configured schedules cannot be met, all sensors will still be measured, but at the best achievable rate and with some slippage from the configured schedule. Sensors that cannot be reached are assumed to be now, in a normal, non-alarm state.

1.4.6 Local data storage

The gateway will buffer measurement/event data until it is able to be transferred to the host system/software. Initially, this buffering is in volatile RAM but, if the data has not been transferred in 5 minutes, then that data is transferred to non-volatile memory with a capacity of approximately 1 GB. This prevents significant data loss if the gateway loses power.

Locally stored data is transferred to the host system/software on a First In First Out basis. The design aims to safeguard at least a week of data, though the actual time span safeguarded is dependent on the number of sensors, measurement schedule and configuration. If the local storage capacity is reached, the oldest data stored will be overwritten by the newly collected data.

1.5 SKF Enlight Collect Manager – Android and iOS app



Commissioning, decommissioning, or any other operations which require the use of the NFC connection are forbidden inside an explosive atmosphere.

The SKF Enlight Collect Manager app is available for Android and iOS devices and is used to perform on-site system maintenance, commissioning, etc.

The Android device being used must support:

- NFC – Near Field Communications
- Android version 7 or later
- Bluetooth Low Energy version 4.2 or later

Note that as NFC and Bluetooth also rely on device hardware an update of the Android operating system is, in-itself, likely insufficient.

The iOS device being used must support:

- iPhone 7 or later, running iOS 11 or later

Note: there are no visual or behavioural differences between the Android and IOS application.

A user logging into the app must use Username and Password credentials appropriate to the @ptitude Observer database.

To be able to log in through the SKF Enlight Collect Manager app, use the @ptitude Observer internal user or [Active Directory](#) login authentication. Refer to the SKF @ptitude Observer user manual or help file for further details of authentication methods.

As this requires the app to be pre-configured with the MQTT service details of the Observer instance that applies, a separate local access **Enter system settings** is available to set these details:

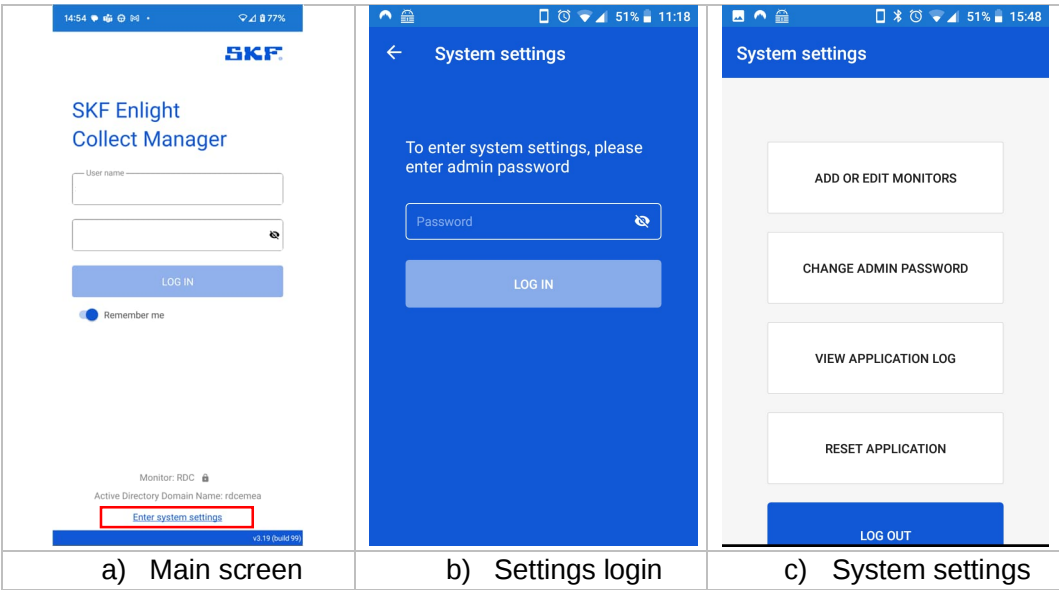


Figure 3 Accessing system settings

When logging in for the first time to the **system settings**, you can choose your password or continue without one. This can be changed at the next screen, if required.

Once into the system settings the first option "Add or Edit Monitors" is how the active monitor instance can be selected or added/edited if the MQTT connection details don't already exist in the app:

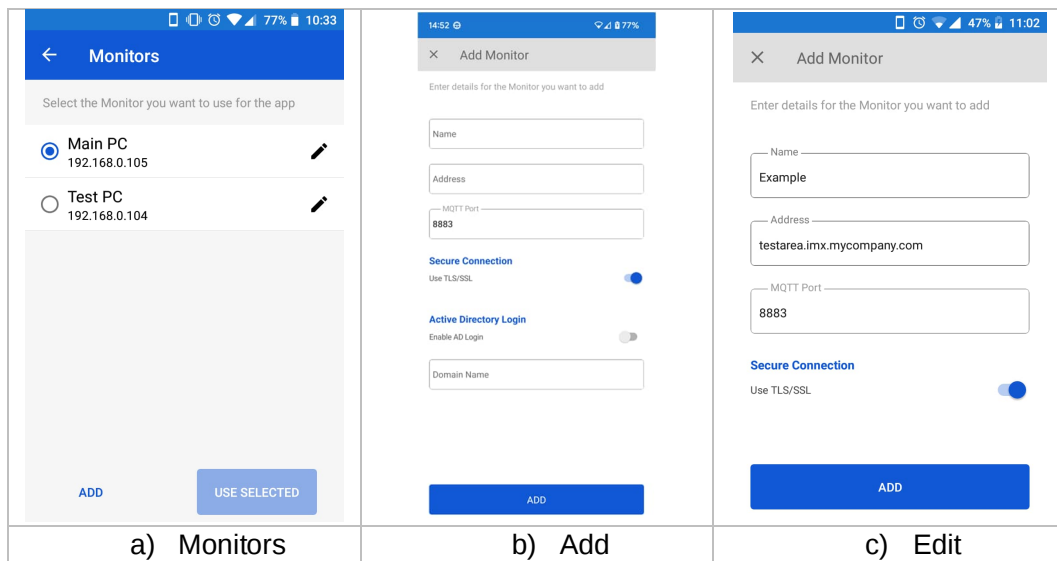


Figure 4 Access the Monitor configuration screens

As can be seen above, for each Observer Monitor instance a friendly informative **Name**, an **Address** and a **Port** number are entered. As these MQTT service address, port and secure connection settings are critical for connecting to Observer Monitor, ensure that they correctly reflect the required instance otherwise a log-in failure can be expected. In general, the address can be entered using domain naming (DNS) or IP addressing noting that where communication to Monitor will be across public networks, the address entered here should be the external facing or public address for the MQTT service. In addition, there is a **TLS/SSL secure connection** option which is on by default. See also [Security](#).

To use an **Active Directory Login** for the app, check the **Enable AD Login** option and enter the Active Directory domain name in the edit box.

Note: to able to use Active directory Login, enable Active Directory authentication in @ptitude Observer, see [Users and security role rights](#).

Multiple connections can be configured, but only one can be active at any time. Ensure the required connection is selected by the radio button and **Use Selected** has been actioned. Note that this button is greyed if the currently selected Monitor is already being used.

Referring back to Figure 3a, it can be seen that when the MQTT connection details for at least one Monitor instance have been configured, the name of the active/selected Monitor server instance is shown on the opening screen of the app, just above **Enter system settings**.

1.5.1 Security

Whilst use of Transport Layer Security (TLS) for app communications with the gateway is automatic, for connection to @ptitude Observer software it is selectable to be able to match the settings there.

If the MQTT service is configured with “Use TLS” enabled, the configuration of the monitor connection in the app must similarly have the “Secure Connection” option enabled, refer to [Figure 5](#) and [Figure 4](#) respectively.

As described in [2.1.1](#), TLS for encrypted communications with @ptitude Observer software requires the app to check the server security certificate when setting up the connection. This includes verifying that the certificate is signed by an official Certificate Authority, known to the phone. If it is not able to verify that, for example because it is a self-signed certificate, at log in the user will be prompted to confirm if the certificate is to be trusted, with options for Trust Just This Once, Trust Always or Do Not Trust (No Log In).

Note that when using TLS and a trusted public Certificate Authority:

- The **Address** specified in the app for the Monitor connection must match the Common Name used in the certificate. The connection must not be specified by either an IP address or a DNS naming related, for example, to a web service provider’s domain.

1.6 Third party licences

Some pieces of licensed software such as open source or third-party libraries have been used when developing this product.

SKF Enlight Collect Gateway firmware version 3.4.

- For a list of these refer to the licence manifest.

SKF Enlight Collect Manager app

- A list is available on the [Support page](#) in the app.

For any enquiries contact SKF’s [Technical Support Group TSG](#).

2 Integration with SKF @ptitude Observer

2.1 @ptitude Observer overview and prerequisites

Before starting pre-commissioning, a suitably licensed version 12.1 or later, @ptitude Monitor/Observer, must be installed and functioning. It should have an appropriate database available with machines created and their operating speeds set. Sub-machines must then be defined ready for IMx-1 sensor placement. As with other types of measurement points and hardware, the @ptitude Observer system log will capture all configuration changes that users make.

General guidance on using @ptitude Observer software can be found in its user manual, part number 32170900. For specific content related to the SKF Enlight Collect IMx-1 System, this must be revision R or later.

2.1.1 Communication with the SKF Enlight Collect IMx-1 system

Like the app, the gateway uses an MQTT login so that only devices with the correct rights can connect, so enable an MQTT service (Message Queuing Telemetry Transport) by the tick box on the **Database > Options > Monitor service tab**:

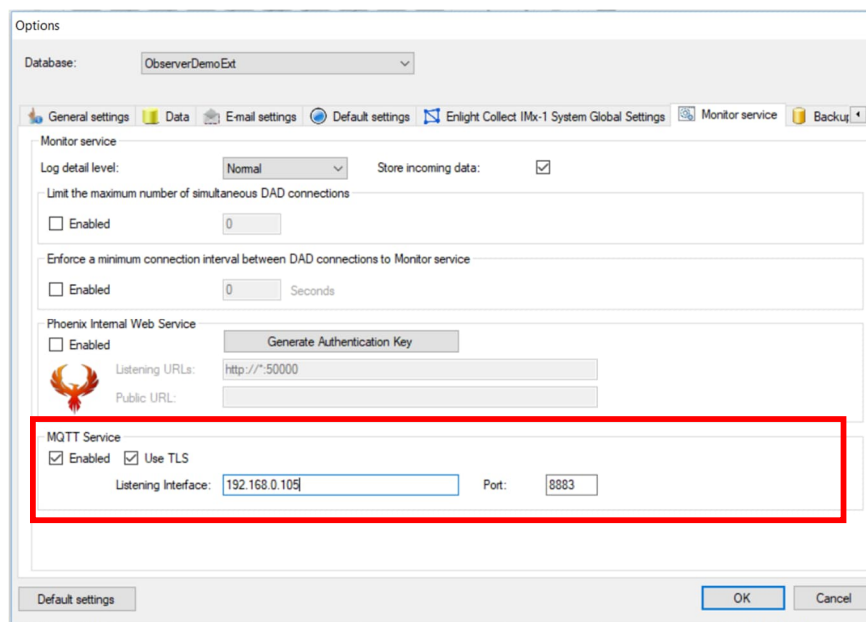


Figure 5 Monitor service tab – MQTT Service

Three configuration parameters then apply:

- **Use TLS** (Transport Layer Security) tick box. In @ptitude Observer 12.1.1 and later the “Use TLS” checkbox enables TLS on the MQTT Service. Enabling TLS ensures the SKF Enlight Collect IMx-1 system, including the

SKF Enlight Collect Manager app, can verify it is connecting to the legitimate @ptitude Observer Monitor server and facilitates encrypted data exchange between them. This is enabled by default on new databases or on those upgraded from @ptitude Observer 12.0 or earlier. When used, a TLS certificate needs to be added to the Monitor service via Monitor Manager (shortcut named: Monitor Service Manager).

The TLS also applies to the Monitor-Gateway interface.

- **Listening interface:** This is the network interface that Monitor will listen on for MQTT messages. The interface is specified by its IP-address, noting that the address entered here should always be the internal or private IP address for the Monitor server and not its public IP address.
- **Port:** The port Monitor will listen to. By default, this is set to the standard TLS, MQTT port 8883. Ensure that incoming MQTT, TCP connections to the designated port are not blocked by a firewall and that where multiple Monitor services are listening on that IP address, unique ports are used for each.

TLS certificate

The app to @ptitude Observer software and the gateway to @ptitude Observer software (back-end) interfaces both support Transport Layer Security using a server certificate and a Certificate Authority (CA) certificate stored in the back-end. The server certificate is used when setting up the TLS connection. The CA certificate contains information about the issuer of the server certificate and is used to ensure that the CA can be trusted.

The server certificate can be a:

- self-signed certificate
- certificate provided by the customer's IT department

A description of how to generate a self-signed certificate is included in the Observer Installation manual, part number 32170700, revision Q or later, or alternatively use the **Generate** function described below.

To protect against "man-in-the-middle" attacks, the CA certificate is sent to the gateway at gateway commissioning, via the app. This CA certificate is used by the gateway when connecting to the back-end, to verify that the server certificate is signed by an official CA and can be trusted.

If TLS is to be used; add the server certificate using @ptitude Observer Monitor Manager. In Monitor Manager, right click the monitor service to which the certificate is to be added and click "properties" or select it then use **Action > Properties** from the menu or just double click it:

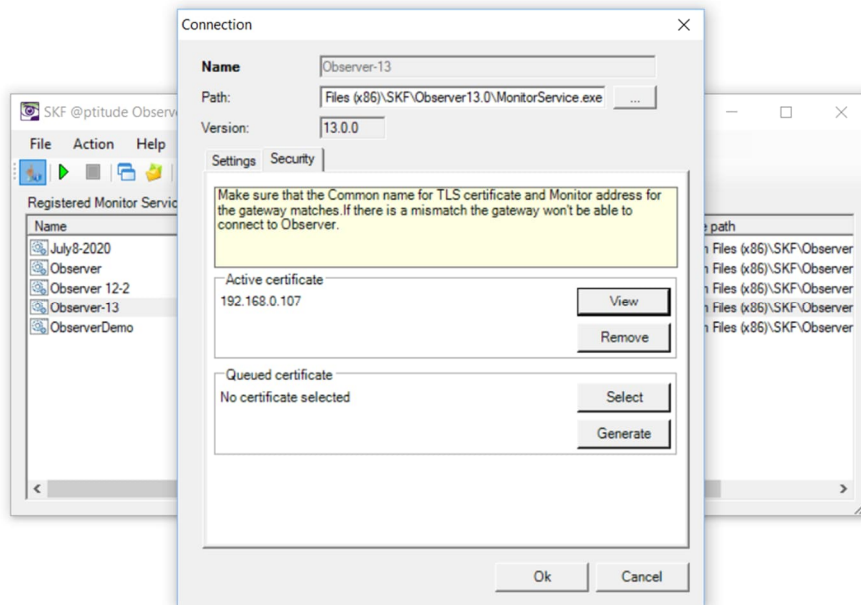


Figure 6 Using Monitor Manager to add up to two TLS certificates

There, on the **Security** tab, the user can **Select** up to two certificates from its windows certificate store (or, for on-premise installations, the user can **Generate** a certificate). The first certificate is added as the **Active certificate**, the second as a **Queued certificate**. This stacking allows for a smooth, automatic transition as the active certificate expires.

When selecting a certificate use **More choices** from the **Windows Security** dialog to see all available certificates. Selected certificates can be managed using the **View** and **Remove** controls shown in Figure 6 above.

The yellow information panel on this tab reminds users to ensure that the Common Name of the certificate matches the Monitor address the gateway/app have, as a mismatch will prevent them connecting to @ptitude Observer Monitor. When using the **Generate** capability, the Common Name of the certificate defaults to the hostname for the Monitor service.

Within @ptitude Observer, if no valid certificate is queued, an expiring certificate (one with 30-days or less validity) will generate a system alarm each day and an expired or missing certificate will cause a daily, critical system alarm. Note that whilst an expired or missing certificate will not immediately cause the connection between the gateway and Observer to stop, if that connection is closed for any reason (Monitor or MQTT restart, TCP disconnection) they will be unable to reconnect until the certificate issue is resolved.

2.1.2 Users and security role rights

All personnel undertaking on-site installation and commissioning tasks using the app must be added as @ptitude Observer users with appropriate rights. There is a specific, single, right that applies to IMx-1 System access and the Enlight Collect Manager app.

Multiple security roles such as Administrator, Maintenance Manager and Machine Operator Level 2 have this right. These roles differ significantly however in their overall scope. For example, the role “Machine Operator Level 2” has otherwise very limited rights so would not allow the user to perform IMx-1 system configuration and maintenance tasks, within @ptitude Observer.

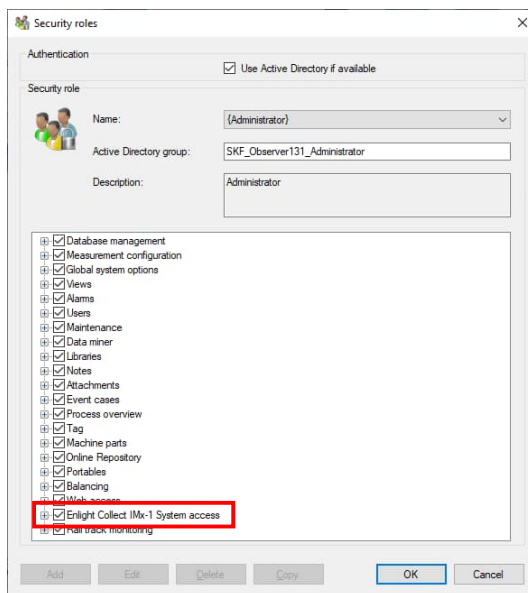


Figure 7 Security roles – IMx-1 System access, user rights

Select **Use Active Directory if available** to enable Active Directory login for the SKF Enlight Collect Manager App.

2.1.3 Enlight Collect IMx-1 System global settings

The selection of engineering units for IMx-1 measurements and the detection methods used, are global settings found under **Database > Options > Enlight Collect IMx-1 System Global Settings** tab:

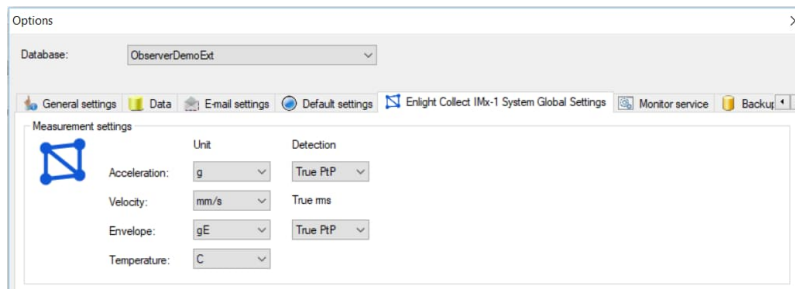


Figure 8 *Enlight Collect IMx-1 System global settings*

Engineering units for each of the four measurement types can be chosen and the following alternatives are available:

- Acceleration: **g** or m/s²
- Velocity: **mm/s** or ips
- Envelope: **gE** or m/s²E
- Temperature: **C** or F

Whilst for Acceleration and Envelope measurements the sensor itself always operates with a true peak-to-peak detection (**True PtP**), in @ptitude Observer the detection can also be configured as half the true peak to peak value (True PtP/2). If this option is chosen, measurement data and any alarm thresholds are automatically adjusted in interactions with the sensor.

Being global settings, these apply to all IMx-1 sensors in the database and also to the units used for the gateway, internal temperature measurement. Pressing the default settings button, on the lower left edge of the dialog, selects the choices in bold above.

2.2 Hierarchy view – adding sensors and measurements

IMx-1 sensors are added to sub-machines in the @ptitude Observer Hierarchy. Right click on the appropriate asset node and select "Enlight Collect IMx-1 Sensor" from the "Add" sub-menu:



Figure 9 *Add – IMx-1 Sensor*

When added to the hierarchy a node for the IMx-1 sensor is created along with a four point cluster of Temperature, Acceleration, Velocity and Envelope measurements, refer the figure below.

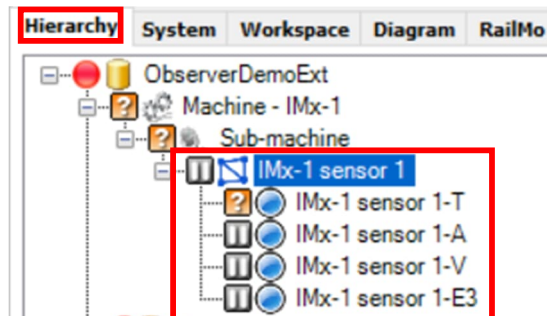


Figure 10 Hierarchy: IMx-1 sensor example

As shown above, the automatic measurement point naming takes the user chosen sensor name, adds a dash/hyphen and then 1 or 2 characters to identify the measurement type. Measurement naming is automatically updated if the sensor name is subsequently changed.

Most @ptitude Observer hierarchical status indications, like Not measured, are supported or applicable to an IMx-1 sensor and measurements except the following: Not active, Outside measurement range, Transient, Outside active range and Outside active range unstable.

In addition the Sensor fault icon is, for the IMx-1, used to indicate that a sensor is unreachable, **Sensor not available**. For further information on the priority of IMx-1 status indications in an @ptitude Observer hierarchy, refer to the SKF @ptitude Observer user manual or help file.

Notes on hierarchy operations:

- IMx-1 sensor nodes can only be added to a sub-machine.
- The user can copy and paste IMx-1 sensors.

To copy one sensor:

1. Right click on the sensor in the hierarchy and select Copy
2. Right click on a submachine and select Paste
3. In the prompt window, enter a value between 1 and 100 and click OK.
The entered number of sensors will be created under the submachine.

To copy multiple sensors:

1. Select multiple sensors under the same sub machine
2. Right click on any of them and select Copy
3. Select Paste.

Users can drag and drop an IMx-1 sensor node but only within the asset and on the same hierarchy level.

Users can only drag and drop an IMx-1 measurement point within its sensor node.

To open the properties of an existing sensor node, right click and select Properties or double click.

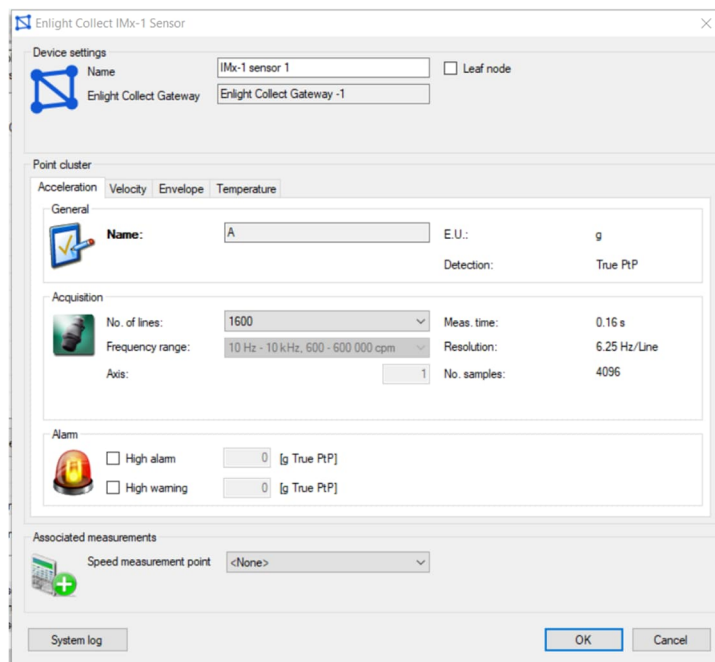


Figure 11 IMx-1 sensor dialog example

Main tab: in the upper area are the sensor **Name** and the **Leaf node** selection, noting that the node type cannot be changed once the sensor is commissioned. Name can usefully be used to indicate the sensor's physical location using standard, vibration measurement point, taxonomy.

Also provided is a read back of the gateway allocation – **Enlight Collect Gateway**. For sensors, this gateway allocation process is indirect, in that measurement sensors are associated with a machine and in the machine's properties, it and all its sensors have a gateway allocated, [Figure 23](#).

Note:

- It is recommended to use the default mesh mode unless it is known that the sensor location is subject to movement or its wireless environment is subject to temporary interruption by vehicle/machinery movements. In these cases, leaf mode can be selected.
- Relay nodes, which make no measurements but are there to support/extend the mesh infrastructure, are created and configured in the Enlight Collect IMx-1 System View.

- Mesh networks auto-adapt but have a rebuild time, therefore:
 - o Do not activate sensors until they are at their mounting position

On the lower part of the main tab is the possibility to add an associated measurement. This can only be a software speed point used to associate a machine speed with the data.

The four measurements each have their own sub-tab in the sensor configuration dialog:

Sub-tabs for each measurement type typically have three zones where aspects of that measurement can be configured or are available for review:

General: an area to report the measurement name, engineering units and detection.

Acquisition: for the vibration measurements to configure the number of lines, select "No. of lines" from the dropdown. Available value is either 400, 800, 1600 or 3200 lines.

To change the "Frequency range" select from the dropdown:

- 10 Hz - 10 kHz, 600 - 600 000 cpm
- 10 Hz - 5 kHz, 600 - 300 000 cpm
- 10 Hz - 2 kHz, 600 - 120 000 cpm
- 10 Hz - 1 kHz, 600 - 60 000 cpm

Alarms: for all measurements an area to configure, set or disable alarms associated with each. Note that low warning and low alarm are available only for temperature measurements. All alarms are disabled by default, with thresholds set to zero.

2.2.1 On-demand measurements

On-demand measurement requests data acquisition to the gateway and is activated in the @ptitude Observer Hierarchy. Request can be triggered at the machine level, sub-machine level or measurement point level.

Right-click on the desired level in the hierarchy and select **Trigger on-demand measurement > Trend data**.

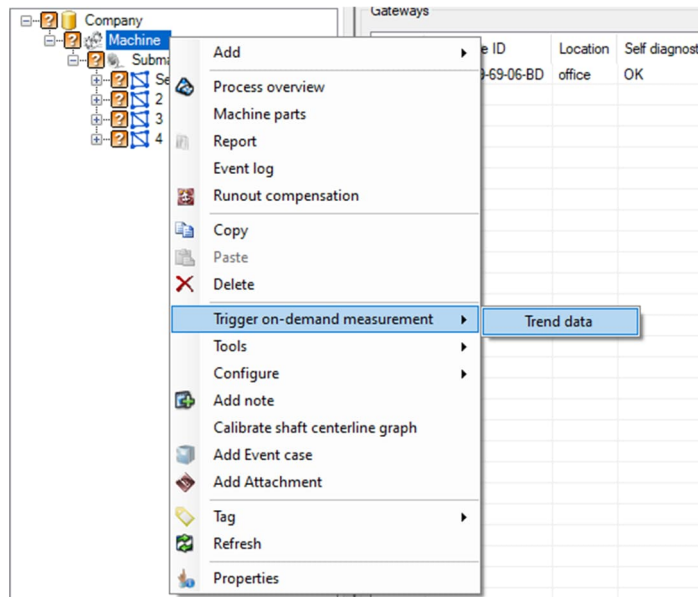


Figure 12 Access the Enlight Collect IMx-1 System view

When the measurement is collected, it can be seen in the Trend List.

For more information about On-demand measurements and other Hierarchy right-click functions, refer to the Observer user manual.

2.3 Enlight Collect IMx-1 System View

This is a dedicated window that provides gateway and sensor information and access to IMx-1 system configuration functions. Get to this system view from **On-line > Enlight Collect IMx-1 System view**:



Figure 13 Access the Enlight Collect IMx-1 System view

The view opens in the main window, where the top section relates to a gateway view or table and the lower section contains a sensor view or table. Within both tables, line entries can be ordered by any column: click on the column header to sort by that column.

Beneath both the gateway and sensor tables are buttons for **Edit** and **Delete** functions as well as a button for adding a **New** gateway or **Add relay node**. In addition, because all synchronisation is carried out at a gateway level, under the gateway table is a **Synchronize** button.

Note that like **Add relay node**, the **Delete** sensor button is only usable for relay mode sensors.

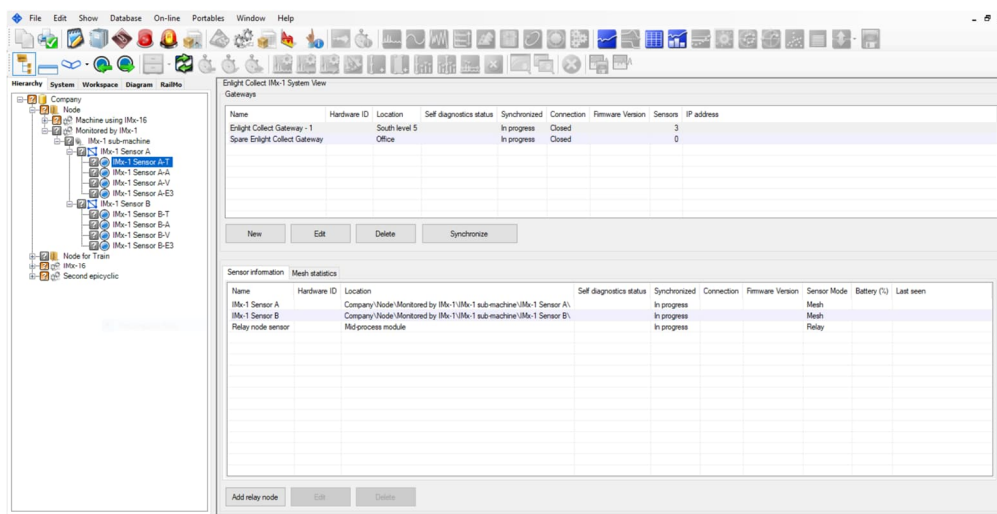


Figure 14 Enlight Collect IMx-1 System view

In this view the upper area is a table of all gateways in the database (see also note about external databases, below). The lower area lists sensors and can be filtered by gateway or by hierarchical position:

- Filter by gateway:
 - o Select an entry in the gateway table/list: the associated measurement and relay sensors for the selected gateway are shown.
- If **Link to hierarchy** is on:
 - o In the Hierarchy view, select a machine or lower level node: if that machine has a linked gateway, the measurement sensors associated with it are shown. The sensor list is cleared if there is no gateway linked to that machine.
 - o **Important note:** if an external database has been added, **Link to hierarchy** must be on for the gateway table to update and reflect the gateways in the database that is currently selected by hierarchical position.

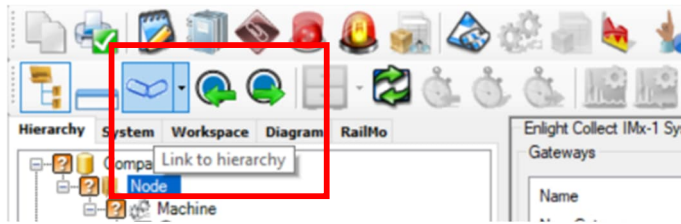


Figure 15 Activate/deactivate link to hierarchy view

2.3.1 Gateways

For each gateway, the following properties are shown in the gateway table:

Name: Name given to the gateway.

Hardware ID: The unique identifier of the gateway. If the gateway is commissioned and has successfully connected to @ptitude Observer, it will show a MAC address in this field.

Location: Descriptive text for the physical location.

Self diagnostics status: Displays the latest reported self-diagnostic status or in case of multiple errors the item considered most critical. "Ok" or an error in the following priority order:

- o Mesh module licence error.
- o Missing/invalid network and identity configuration. This is a configuration known as "configuration 2", in the event log.
- o Missing/invalid "other" configuration. This configuration includes measurement configuration. See also [Missing/invalid](#).
- o NTP Error.
- o Manufacturing data fault or corruption (QSPI)

The status field will initially be empty until the actual gateway status has been received. Note that double clicking a gateway entry or selecting it and then choosing **Edit**, will launch the gateway properties dialog where extended status information can be viewed on the Gateway status tab.

If the gateway status deviates from OK, this will also be reflected by appropriate system or critical system alarms being raised.

Synchronized:

- No: the configuration held by @ptitude Monitor/Observer is different to that in the gateway.
- In progress: a synchronise action is under way.
- Yes: the configuration in @ptitude Monitor/Observer and in the gateway are verified as being the same.

Connection:

- Connected
- Closed

Firmware Version: The version of firmware, installed in the gateway.

Sensors: The number of sensors linked to the gateway.

IP Address: The IP address that is used by the gateway.

2.3.2 Sensors

Similarly, for sensors the following properties are shown in the sensor table:

Name: Name given to the sensor.

Hardware ID: The unique identifier for the sensor, if the sensor is commissioned and has successfully connected via the gateway to @ptitude Observer, it will show a MAC address in this field.

Location: For a measurement sensor, Leaf or Mesh, the hierarchical location where that sensor and measurement points have been created. For a relay node, this field contains the descriptive location information entered by the user, [Figure 25](#).

Self diagnostics status: Displays the latest reported self-diagnostic status or in case of multiple errors the item considered most critical. The status field will initially be empty until the actual sensor status has been received.

- "Ok" or an error of any of the following types. Values in brackets are decimal values corresponding to the bit set in the mesh network information log, Self-Diagnostic entry, when the error is true:
 - o Battery level low (1)
 - o External Flash memory failure (16)
 - o Configuration CRC failure (64)
 - o Firmware update error (128)
 - o (Watchdog reset (256) – only available in the log file)
 - o Network instability (512)

Self-diagnostic errors may also raise a system or critical system alarm in @ptitude Observer. Note that the network instability error can have significant ramifications for sensor battery life and urgent action should be taken, refer to [IMx-1 sensor troubleshooting](#).

Double clicking a sensor entry or selecting it and then choosing **Edit**, will launch the sensor properties dialog where extended status information can be viewed on the second tab, named Status.

Synchronized:

- No: the configuration held by @ptitude Monitor/Observer is different to that in the sensor.
- In progress: a synchronise action is underway.
- Yes: the configuration in @ptitude Monitor/Observer and in the sensor are verified as being the same.

Connection: Current connection status for the sensor, may indicate OK, Temporarily unreachable or Unreachable.

Firmware Version: The firmware version that is installed in the sensor. Note that before a connection to the sensor has been established this field will be empty.

Sensor Mode: Mesh, Leaf or Relay. Refer description and notes on [Sensor Mode](#) and Sensor.

Battery (%): A battery health indication of the estimated percentage battery life remaining. Note that before a connection to the sensor has been established this field will be empty.

Last seen: A date and time corresponding to when the sensor was last communicated with.

2.3.3 Mesh Statistics

Within the sensor table area, a second tab: Mesh statistics, provides data to support an understanding of how the wireless mesh is performing and adapting to the physical sensor layout.

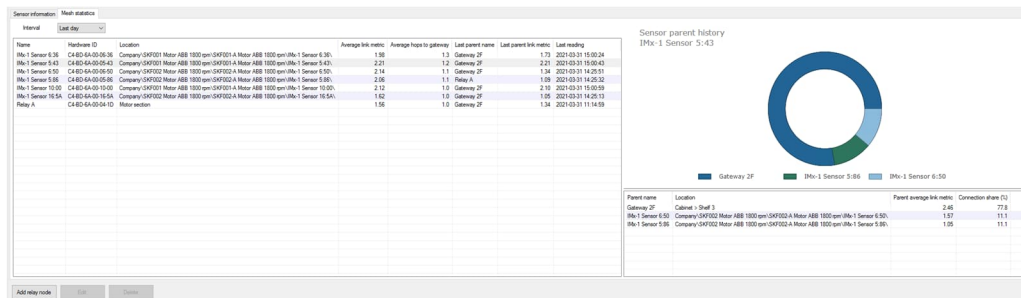


Figure 16 Mesh statistics tab

Using the drop-down, the mesh statistics can be based on an **Interval** setting of *All*, *Last day*, *Last week*, *Last month* or *Last year*.

In the main table each sensor occupies one row and is identified by a **Name**, **Hardware ID** and its **Location**. The statistics give an indication of the routing being taken by providing **Last parent name** and **Average hops to gateway**. A guide to the quality of the routing is offered by way of **Average link metric** and **Last parent link metric**. Here the metric is effectively the average number of attempts needed to make the communication so a metric of 1 is perfect and a metric of 7 would indicate a poor quality routing that invoked the maximum number of retries allowed. The mesh

statistics are only updated when a particular sensor is communicating, the time/date provided in the **Last reading** column will convey when that was.

Selecting a particular entry in the main table populates the **Sensor parent history**. For the selected sensor this will show not just the last parent but all parents within the selected interval. For each a **Parent name**, **Parent average link metric** and **Connection share (%)** will be shown. The connection share shows the proportion of the total connections that were made through that particular parent. Similar to the main table, a **Location** column is displayed for identification purposes, this time of the parent device.

2.4 IMx-1 system configuration

2.4.1 Gateway

Being part of the mesh infrastructure, gateways are mostly configured in the @ptitude Observer, IMx-1 system view.

Select a gateway from the upper gateway table/list then double click or right click and select properties or for a new gateway, press **New**. When a new gateway is created, where appropriate, the properties of the last gateway created/modified will be re-used.

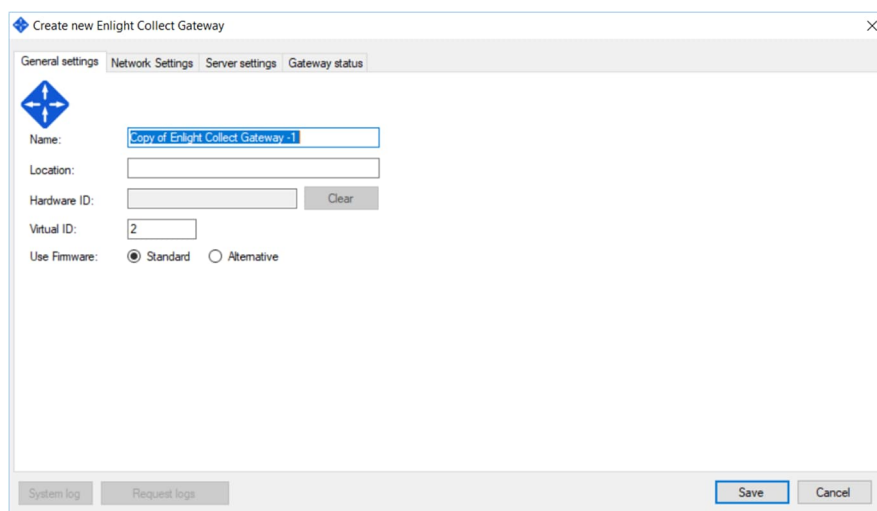
The screenshot shows a software window titled "Create new Enlight Collect Gateway" with a close button (X) in the top right corner. The window has four tabs: "General settings" (selected), "Network settings", "Server settings", and "Gateway status". On the left side of the "General settings" tab is a blue diamond icon with a white crosshair. The main area contains several input fields: "Name:" with a text box containing "Copy of Enlight Collect Gateway-1", "Location:" with an empty text box, "Hardware ID:" with an empty text box and a "Clear" button to its right, and "Virtual ID:" with a text box containing the number "2". Below these is a "Use Firmware:" section with two radio buttons: "Standard" (which is selected) and "Alternative". At the bottom of the window are three buttons: "System log", "Request logs", and a pair of "Save" and "Cancel" buttons.

Figure 17 Configuring a new gateway – General settings tab

The General settings tab has user editable areas for a gateway descriptive **Name**, a descriptive **Location**, a **Virtual ID** and a choice of using **Standard** or **Alternative** firmware. Refer to the SKF @ptitude Observer user manual or help file for an understanding of why Alternative firmware might be used in some circumstances.

Virtual ID is a unique identifying number for each gateway in the database. Valid assignments are in the range 1 to 65 535, the system will suggest the lowest available Virtual ID.

The Virtual ID can be thought of as a reference to a specific slot or position in the database. During commissioning an individual gateway's Hardware ID is assigned to that position to ensure that data reaches the intended destination. If a gateway has to be replaced, that assignment of Hardware ID to Virtual ID has to be cleared before the new gateway can connect to that Virtual ID.

If a user has appropriate rights, the **Request logs** button can be used to upload log files from the gateway to the file system on the @ptitude Observer computer. The log files can be useful for IMx-1 system troubleshooting and are uploaded as a single, password protected, zip file. The file transfer dialog will confirm the location where the file has been stored.

The Network settings tab allows the gateway network connection to be selected as:

Ethernet (wired) and to be set for dynamic (**DHCP**) or **static** addressing and as appropriate to allocate static settings for its **IP Address**, **Subnet mask**, the network **Gateway** address, DNS addresses, etc. Use of external antenna **Mesh** or/and **BLE** (Bluetooth low energy) is also selected in this menu.

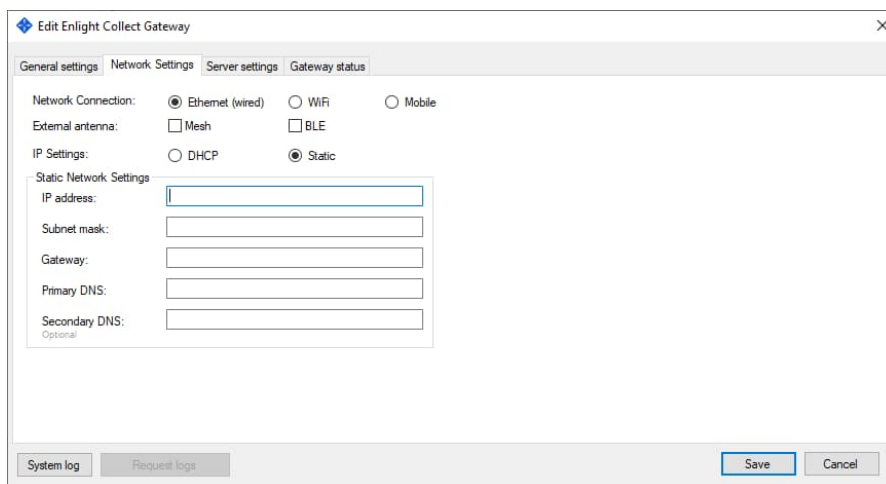


Figure 18 Network settings – Ethernet

Wi-Fi specific selections include a **SSID** and **Security** type protocol for the wireless network. For security, there is a choice between *WPA2-Personal* and *WPA2-Enterprise*. Being a certificate based authentication, be aware that selecting *WPA2-Enterprise* will require additional configuration fields to be completed over and above those shown in the *WPA2-Personal* example below. These include **CA** (Certificate Authority) **certificate**, **EAP** (Extensible Authentication Protocol), user **Identity** etc. If **external antenna** is used, it can be selected in this window.

The screenshot shows the 'Edit Enlight Collect Gateway' window with the 'Network Settings' tab selected. The 'Network Connection' section has 'WiFi' selected with a radio button. The 'External antenna' section has 'Mesh' and 'WiFi/BLE' checkboxes, both of which are unchecked. The 'IP Settings' section has 'Static' selected with a radio button. The 'Static Network Settings' section contains fields for 'IP address' (255.255.255.0), 'Subnet mask' (255.255.255.0), 'Gateway' (13.34.34.32), 'Primary DNS' (13.34.34.32), and 'Secondary DNS' (Optional). The 'WiFi Settings' section contains fields for 'SSID', 'Security' (WPA2-Personal), 'Country' (United States of America), and 'Password'. At the bottom, there are buttons for 'System log', 'Request logs', 'Save', and 'Cancel'.

Figure 19 Network settings – Wi-Fi

Mobile support is only available using external antennas. Type of antenna can be selected under **External antenna**.

Mobile network connections include 3G or 4G connectivity service. It also includes **SIM PIN**, **Access Point name**, **Authentication name**, **Username** and **Password**.

The screenshot shows the 'Edit Enlight Collect Gateway' window with the 'Network Settings' tab selected. The 'Network Connection' section has 'Mobile' selected with a radio button. The 'External antenna' section has 'Mesh', 'BLE', and 'Mobile' checkboxes, all of which are unchecked. The 'Mobile' section contains fields for 'Mobile connectivity services' (4G/3G), 'Sim Pin Code', 'Access Point Name', 'Authentication Type' (CHAP), 'Authentication username', and 'Authentication password'. At the bottom, there are buttons for 'System log', 'Request logs', 'Save', and 'Cancel'.

Figure 20 Network settings – Mobile

The third tab is **Server settings**:

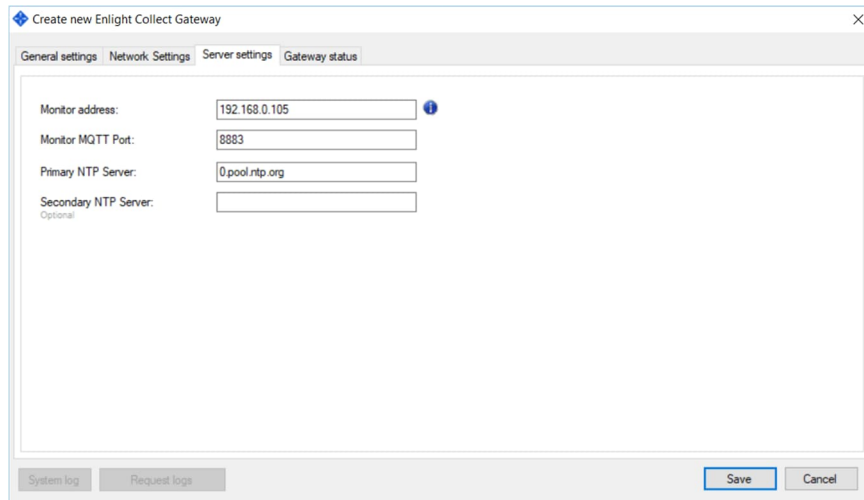


Figure 21 Gateway properties – Server settings tab

There address and port settings relate to the location of Monitor. In general, the address can be entered using domain naming or IP addressing noting that if an IP address is entered here for a system communicating across public networks, it should be the external facing or public IP address for the Monitor server.

Note also that when using TLS and a trusted public Certificate Authority, the **Monitor address** must match the Common Name used in the certificate.

The connection must not be specified by either an IP address or a DNS naming related, for example, to a web service provider's domain.

See also [TCP and UDP Port Usage](#).

NTP settings indicate to the gateway where an NTP server can be contacted. An entry for at least the **Primary NTP Server**, is required before the configuration can be saved. Like other IMx devices, in **Database > Options > Device settings** tab, time synchronisation thresholds can be configured to generate system alarms if time synchronisation is lost.

Status information when/as it is available, is presented on the Gateway status tab:

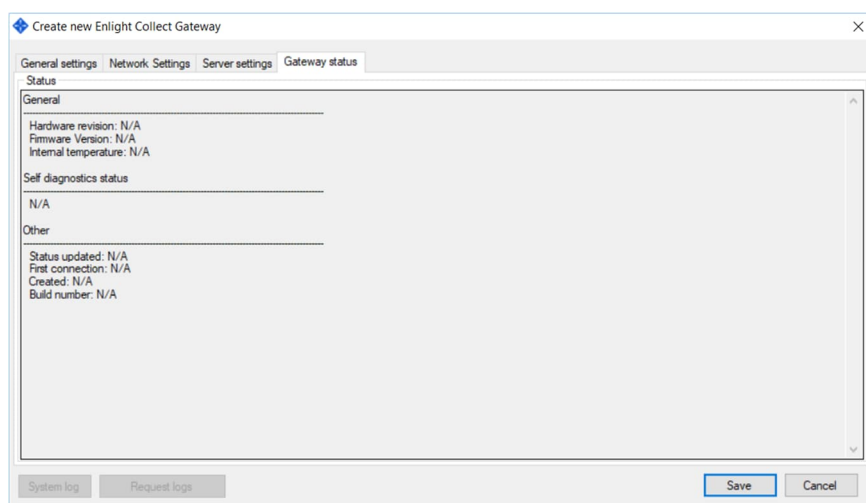


Figure 22 Gateway properties – Gateway status tab

The status tab feeds back information on **Hardware revision** and **Firmware version**, gateway **Internal temperature**, its **Self-diagnostics** status, **Wi-Fi SSID** and **Signal strength** and when **Created/First connection/Status updated**, firmware **Build number**. Note the information provided is updated on opening the dialog box, not in real time.

Important Note: the gateway allocation to a particular machine or machines is set on the **Machine Properties > Enlight Collect IMx-1 System tab**, and must be allocated before commissioning.

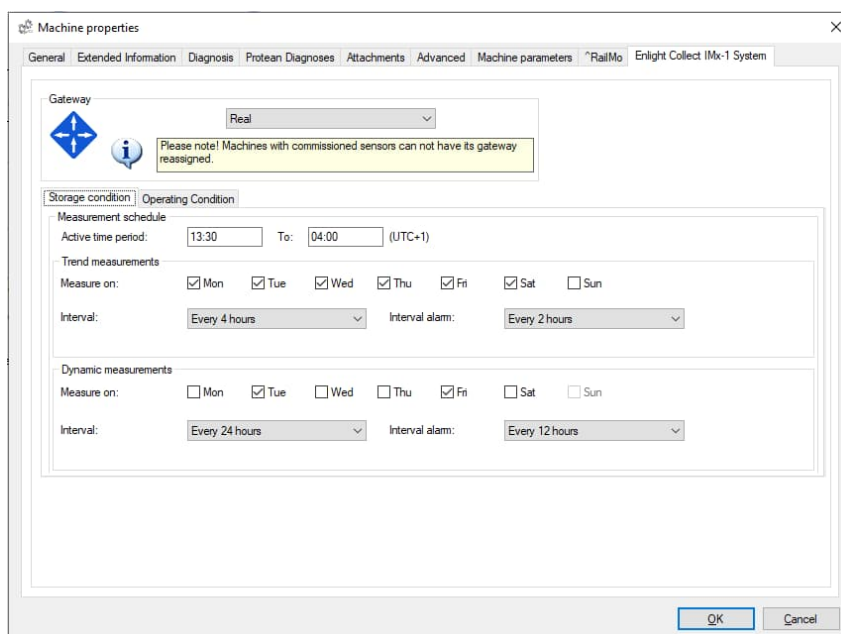


Figure 23 Machine properties, Enlight Collect IMx-1 System tab example

Gateway has a drop-down list that allows the selection of any gateway that exists in the system, or *<None>*. Note also that whilst gateways can be associated with multiple machines, multiple sensors on a machine can only connect to the same, single gateway. In addition, whilst a machine has a commissioned sensor, it is not possible to change to another gateway or select *<None>*.

Storage condition allows the user to configure the time when measurement acquisition should be performed.

Measurements schedule is used for selection of the active time period.

Trend measurements can be selected on one or several days of the week. It contains two settings: measurement **interval** and **Interval alarm**. With options for *Every 1 hour*, *Every 2 hours*, *Every 3 hours*, *Every 4 hours*, *Every 8 hours*, *Every 12 hours* and *Every 24 hours* (default).

Dynamic measurements can also be selected on one or several days of the week. Measurement **intervals** and **Interval alarm** have same options as well *Every 1 hour*, *Every 2 hours*, *Every 3 hours*, *Every 4 hours*, *Every 8 hours*, *Every 12 hours* and *Every 24 hours* (default).

When selecting the above intervals consider the following rules:

- Trend measurement in alarm interval ($\geq$) greater than or equal to Trend measurement interval
- Dynamic measurement interval ($\geq$) greater than or equal to Trend measurement interval
- Dynamic measurement ($\geq$) interval greater than or equal to Dynamic alarm interval and ($\geq$) greater than or equal to Trend measurement alarm interval

In the example above, Figure 23:

Trend measurement interval will measure on:
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
With **Active time period** over-night from 13:30 to 04:00, Every 4 hours.
[13:30, 17:30, 21:30, 01:30]

If the measurement starts on Saturday, all measurements planed after midnight (00.00) will execute on Monday, although it is not marked in the user interface.
If the measurement starts on Monday, the last measurement at 01:30 will not execute because Sunday is not marked in the user interface.

Trend measurement interval alarm will measure on:
Monday, Tuesday, Wednesday, Thursday, Friday, Saturday.
With **Active time period** over-night from 13:30 to 04:00, Every 2 hours.
[13:30, 15:30, 17:30, 19:30, 21:30, 23:30, 01:30, 03:30]

Dynamic measurement interval will measure on:
Tuesday and Friday. At 13:30, Every 24 hours.

Dynamic measurement interval alarm will measure on:

Tuesday and Friday. Over-night from 13:30 to 04:00, Every 12 hours.

[13:30, 01:30]

If the measurement starts on Tuesday or Friday, all measurements planned after midnight (00:00) will execute on Wednesday or Saturday, although these days are not marked in the user interface.

If the measurement starts on any other day, the 01:30 measurement on Tuesday and Friday will not be executed because Monday and Thursday are not marked.

It's not possible to configure a schedule with no dynamic measurements.

As soon as an alarm is triggered, the gateway will switch to the alarm schedules.

Note that the *Every hour* selection for dynamic data is only available where the user has selected the same setting for the respective, Interval or Interval Alarm Trend storage setting.

If *Every 24 hours* selection is made on all available options in Trend and Dynamic measurements, the user must set the time in the **Active time period**. The measurement is performed in the time specified.

Be aware that the frequency of data collection affects sensor power usage and that shorter acquisition intervals will always tend to reduce battery life.

Operating condition:

Amplitude gating: To reduce the total amount of data sent from sensors, amplitude gating in the gateway checks the overall acceleration value received from a sensor after a scheduled measurement request. If the amplitude is below a configurable threshold, the gateway does not retrieve any associated time waveforms from the sensor. Values accepted in the **Gating threshold** field range between 0 and 50 g.

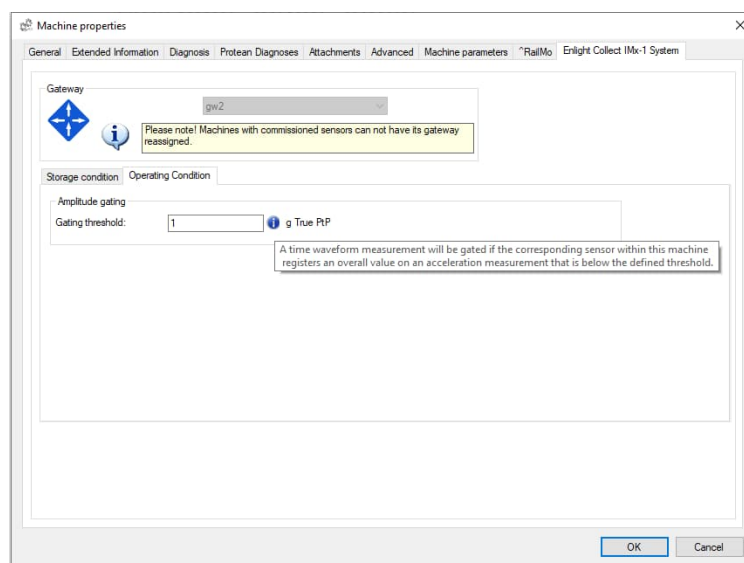


Figure 24 Machine properties, Enlight Collect IMx-1 System tab example Operating condition

2.4.2 Sensor

Sensors can operate in different modes:

- Mesh – default mode, makes measurements and contributes to the sensor mesh network.
- Leaf – makes measurements only and uses but doesn't contribute to, the sensor mesh network.
- Relay – contributes only to the sensor mesh network and makes no measurements.

Mesh/leaf modes are associated with a hierarchical location as they relate to machine monitoring. Relay nodes however are related only to the mesh infrastructure and can only be added directly to a gateway in the Enlight Collect IMx-1 system view. To add a relay node:

- Select a gateway in the Enlight Collect IMx-1 system view.
- Beneath the lower sensor table, click on **Add relay node**.
- In the dialog a descriptive **Name**, **Gateway** and **Location** descriptor can be assigned.

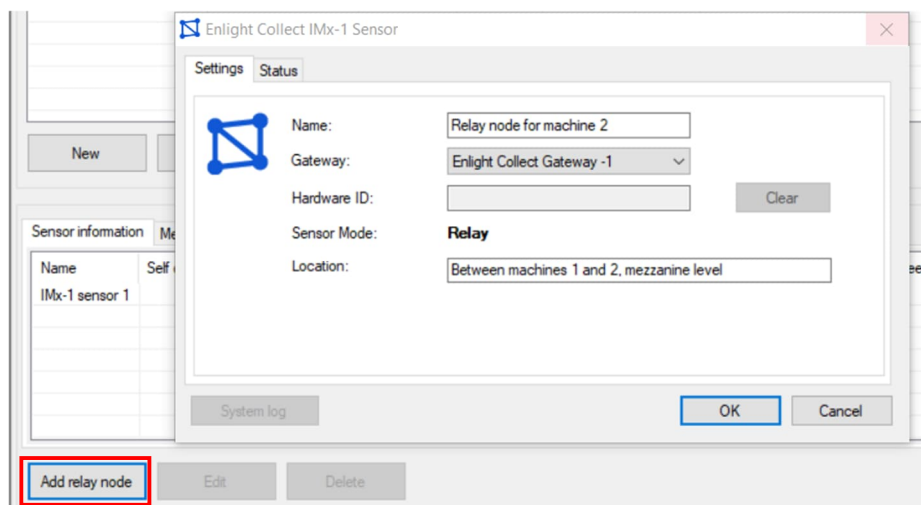


Figure 25 Relay node dialog example

Note:

- Although the location field entry will be displayed in the app during commissioning, when configuring a relay node, a name that hints at its physical location or position in the mesh may still be useful.
- As well as being created, a relay node can also be deleted, by selecting it in the Enlight Collect IMx-1 System View and pressing the **Delete** button below the sensor list.

[illegible]

Figure 26 Sensor table example

All types of configured sensors allocated to a gateway will be shown in the sensor table, as illustrated in the example shown above. When a sensor has been commissioned the device MAC address will be reported in the Hardware ID column.

To edit or view the properties dialog of a sensor, select its associated gateway to update the sensor list and then select the sensor from that list. Click the **Edit** button below the sensor list or directly double click the table entry to open the sensor properties dialog.

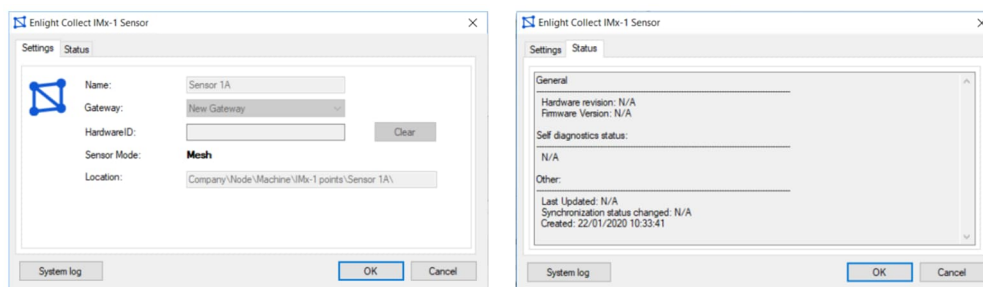


Figure 27 Mesh mode sensor example – Enlight Collect IMx-1 Sensor properties

A mesh or leaf mode sensor is configured in the hierarchy so most settings/actions, aside from **Clear** Hardware ID, are read only.

A second tab, Status, feeds back information on **Hardware revision** and **Firmware Version, Self-diagnostics status** and when **Created, Last updated** and **Synchronization status changed**. Note the information provided is updated on opening the dialog box, not in real time.

Updating the sensor list by selecting the relevant gateway acts as a useful check that the gateway is actually associated with the machines it should be. If it is, the expected sensors will be displayed.

2.4.3 Synchronisation of configuration changes

By completing all the configuration and pre-commissioning work described, the machine hierarchy, sensor and gateway information will be available as a **Commissioning Route**, when the sensor installer starts the app and connects to

@ptitude Observer. The installation and commissioning process will then associate specific sensor and gateway devices with the locations and identities pre-configured in @ptitude Observer. Once commissioned, the configuration in @ptitude Observer can be pushed down to the on-line system by gateway synchronisation.

For an IMx-1 system the synchronisation process is automatic on configuration change or when a firmware update is available in @ptitude Observer but it can also be manually initiated.

Synchronisation is implemented at a gateway level so to synchronise, select an appropriate gateway from the table list, confirm that its **Connection** state is **Connected** and then press **Synchronize**.

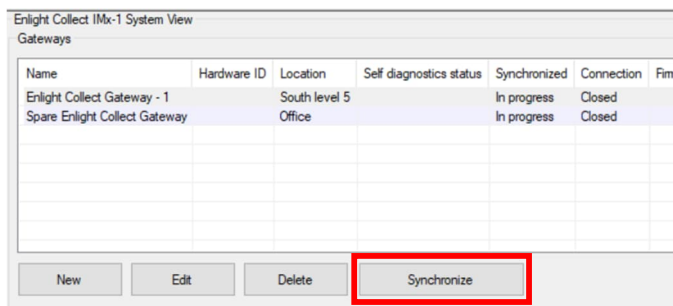


Figure 28 Synchronize button for configuration and firmware update

Initially this sets the gateway and sensor status to **In progress** meaning the synchronisation process is underway. The gateway and all sensors reporting a Hardware ID will be synchronised, any sensors not yet reporting their ID will remain as **In progress**.

To ease commissioning, once any of these sensors join the system and report their Hardware ID then synchronisation is automatic and doesn't require the user to manually synchronise the gateway.

2.4.4 Gateway or sensor Hardware ID

The **Hardware ID** is the parameter that links a specific physical device, gateway or sensor, to a configured location in the system.

After recommissioning, the Hardware ID is cleared automatically.

If necessary, it can be cleared from the Enlight Collect IMx-1 System View.

Click on the Clear button to clear the Hardware ID.

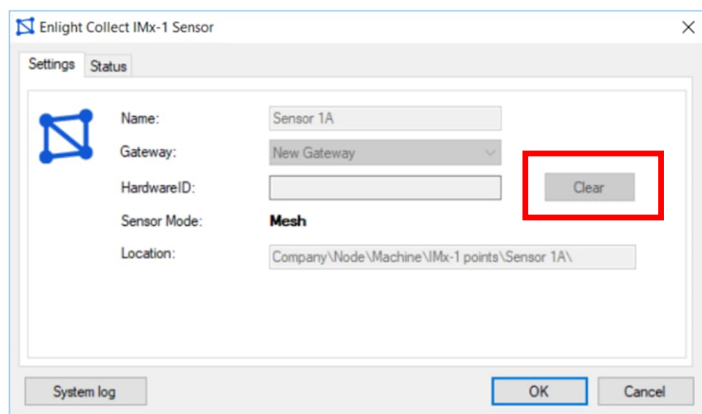


Figure 29 Hardware ID clear button – Mesh mode sensor example

2.5 Use of @ptitude Observer machine templates

When creating a new machine, @ptitude Observer supports the use of machine templates, where the template to be used is selectable from a drop-down list. These templates are complete with all machine and measurement point properties.

As IMx-1 measurements are somewhat different to those performed by other IMx devices it is important to be able to easily distinguish IMx-1 templates. To achieve this, it is recommended that users adopt the following naming taxonomy for all machine templates:

DAD_Asset Class_Asset Type_Manufacturer Name_Manufacturer Model

Example IMx1_Turbine_Wind_Company_V99

- DAD (Data Acquisition Device): IMx1
- Asset Class: Turbine
- Asset Type: Wind
- Manufacturer Name: Company
- Manufacturer Model: V99

3 Installation and commissioning

3.1 Overview and prerequisites

Installation of an IMx-1 wireless system interfacing to SKF @ptitude Observer software must be top-down, that is:

- Decide whether a cloud or local-server based system is required. Note: to download the commissioning route the mobile app must be able to use a mobile data or Wi-Fi connection to access the server.
- Have a database populated with the gateway and sensor/measurement point information.
- With the interconnecting network structures in place and an NTP server available.
- Locally at the asset, the gateways must be present and powered.

Then at this point gateways can be commissioned, wireless sensors can be installed and correctly associated with the appropriate machine measurement locations. Finally, with all the hardware in place and commissioned the system must be synchronised, a manual action from @ptitude Observer.

3.1.1 System commissioning and security

On-site system commissioning and troubleshooting uses the SKF Enlight Collect Manager mobile app. This is an SKF app for Android and iOS devices that provides features to manage and configure the system:

- Configure the connection to an @ptitude Observer instance.
- Log in and retrieve mesh/network configuration data from @ptitude Observer.
- Scan for gateways or later, scan for sensors.
- Commission a gateway.
- Wake-up and commission a sensor or add as a relay node.
- Retrieve and display device information, for example ID, firmware version.
- Generate a commissioning report.

To access an Enlight Collect IMx-1 system, users must be pre-registered within @ptitude Observer with appropriate rights/roles. The app system settings should reflect the @ptitude Observer instance for the system being worked on. This is important not only to be able to receive commissioning data for that system but for the app to have the correct credentials for access to a commissioned gateway. For

cloud scenarios this endpoint will be the public address where the Monitor service can be reached from outside of the cloud.

Note: like an @ptitude Observer login, the user name entry is not case sensitive.

When logging in to the app it will attempt to communicate with @ptitude Observer Monitor to retrieve a commissioning route for the system and store it in a local device database. After that, local network or internet access from the device to @ptitude Observer is not required as the local device copy provides all the information needed to complete the commissioning process even though the device may be then offline.

The user log in is valid for 7 days so within that period a user may log-in to the app offline, without a connection to @ptitude Observer. Resuming app use after minimising or hiding the app without logging out, will not require any log in unless the 7-day session timer has expired.

After 7 days from the last sync, to log in, a connection to @ptitude Observer is required. The elapsed time since last online log in or sync action is displayed in-app towards the bottom of the main menu.

To refresh the app's local device database a network connection to @ptitude Observer is needed. When entering either of the scan options from the main menu, if the phone is online, the app will do a background refresh of the route and this will extend the 7-day session timer. To otherwise force a refresh, use the **Sync. now** function on the Main menu page:

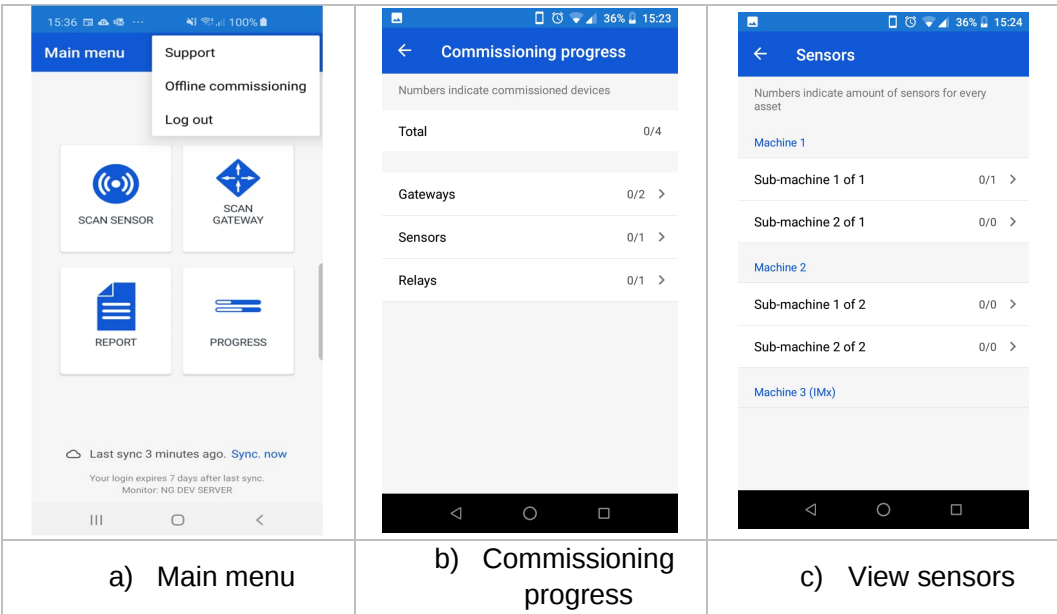


Figure 30 Viewing the commissioning progress

Before commencing commissioning work, or at any time later, the user can view a commissioning progress summary. Tap the **PROGRESS** button in the main menu to access the commissioning progress.

In the example above the equipment to be commissioned is:

- Installed across two machines
- Each with two sub-machines
- There are two sensors to be commissioned
- A gateway and a relay node

From the commissioning progress screen, by selecting **Sensors**, it is possible to drill down through functional locations, then sub-machines to the sensor names and similarly for the relay node to confirm its name and associated gateway.

3.2 SKF Enlight Collect gateway

3.2.1 Introduction

When selecting a location for the gateway choose somewhere central to its associated sensors where power and any required network connections can be made available to it.

Cable connections to the gateway, such as for incoming DC power and Ethernet cabling, are made in the lower part of the enclosure. To access this area, remove only the two retaining screws holding the lower cover.

With the lower cover removed, incoming cabling can be terminated at the available connectors. A blanking plug provides access to a micro-SIM card holder.

Important safety warning:



Only remove the blanking plug when it is necessary to access the SIM card holder. Otherwise ensure the blanking plug remains in place.

With each gateway SKF provide one 1.5 m power supply connector/cable assembly and one 1 m connector/cable assembly for the hard-wired Ethernet connection.



Figure 31 Example of connector/cable assemblies

Longer cable assemblies or intermediate junction boxes may be required depending on site layout and requirements.

3.2.2 Gateway mounting

The SKF Enlight Collect Gateway, excluding a mounting plate, has dimensions of

- 220 mm high
- 220 mm wide
- 50.5 mm deep

It is supplied fitted to the mounting plate shown below. This mounting plate has dimensions of

- 195 mm wide
- 250 mm high
- 6 mm thick

It provides a 4-point mounting and has four 6.5 mm, clearance for M6 and holes on a 150 mm by 220 mm pitch.

To mount the gateway by its mounting plate, remove the lower connection area cover. The mounting plate protrudes above the gateway housing and the upper two mounting positions are accessible there.

Important safety warning:



Always utilise all provided fixing points to secure it to the mounting surface, using fasteners appropriate for that material.

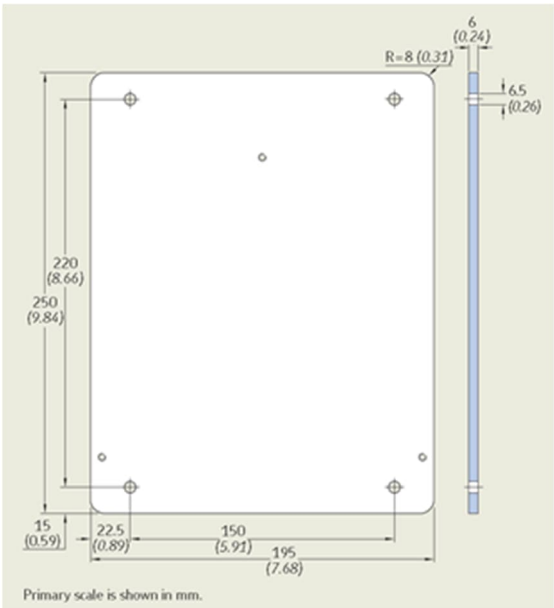


Figure 32 Gateway mounting plate dimensional drawing

3.2.3 Power requirements

The SKF Enlight Collect Gateway is designed to be powered from either PoE or an industrial range 24 V DC supply, including 12 V battery operation. The connection details for the DC supply are as shown in the figure and table below.



Figure 33 Incoming power supply connection

Table 1 DC in connections

DC Power In	Connector pin	Cable core colour
0 V (Power supply return)	1 and 4	Blue/White
+ 24 V (9–36V DC)	2 and 3	Brown/Black

Refer to the [Important safety warnings](#).

It is recommended to use all 4 connections to minimise voltage drop across the cable.

Incoming power is isolated from another gateway circuitry.

Note that whilst both the power source alternatives (PoE and DC supply) can be connected at the same time this is not intended as and will not provide, true power redundancy.

To avoid that even in an error condition the gateway is not exposed to more than 15 W, by design, the two supplies are never enabled simultaneously. The DC supply is the master and if this is present the PoE internal power circuitry will be disabled. If the DC supply is lost, the PoE supply will then be enabled but due to the time taken for this to establish itself the gateway will likely power down and restart.

Important safety warnings:



In some countries, the installer must be certified to connect equipment, such as a gateway, to plant systems.



Make sure that the power is disconnected before the installation begins.



The system power supply must be provided with an appropriately positioned, clearly labelled full pole isolator or switch that can be used to isolate and lock-out power from the gateway during installation, maintenance or modification work. The switch must be labelled "SKF Enlight Collect gateway" or similar, with clear identification of which gateway, if multiple units are deployed. The On/Off position must be clearly marked.

The supply scheme should also incorporate suitable fusing or circuit breakers for the protection of the supply cable being used.

3.2.4 Network connections and configuration

Network configuration designates the type of network connection that the gateway will use and is a part of the gateway configuration process. A wired, Ethernet connection is the default, but the alternative Wi-Fi connection can be used, where preferred.

3.2.4.1 Ethernet (wired)

The gateway has one, 10/100/1 000 Mbit, Ethernet port for connection to a local network. This port supports PoE as a means of powering the gateway rather than using the DC power input connector.

If the system is correctly connected to the software the front panel status LED will reflect that.

The port has auto MDI-X for crossover or straight through cable detection and is available at a connector, [Figure 2](#) and below, Table 2. Connection details depend on the network standard being used, but all 4-pairs are available to support 1000Base-T operations:

Table 2 Ethernet interface connector pin allocation

Pin	Function
1	Pair A +
2	Pair A –
3	Pair B +
4	Pair B –
5	Pair C +
6	Pair C –
7	Pair D +
8	Pair D –
9/shell	Cable shield when applicable

Note that the above pinout is for this connector only, it may not be one-to-one numbering with connecting equipment.

Use an Ethernet cable of sufficient CAT rating for the network being connected to and preferably an SFTP (shielded and foiled, twisted pair) type. For grounding of shielded Ethernet cables, a single-point ground of the shield at the hub/switch end of the cable is recommended. For long and outdoor Ethernet connections using PoE it is recommended to allow for dual-point grounding of shielded cables to minimize the impact of surge influences on the power sourcing equipment (PSE) being used. This precaution is to prevent potential loss of power to the IMx-1 gateway.

Note that typically, twisted pair Ethernet cables have a maximum working distance of 100 m. If longer cable lengths are needed, fibre optic cables may be used along with appropriate media converters: fibre optic to SFTP and vice versa.

When using fibre optics or PoE, suitable network hardware must be in place.

3.2.4.2 Wi-Fi

The built-in Wi-Fi module provides an alternative network connection method where a wireless network is available. The gateway provides an integral radio antenna, no connection to an external antenna is required, although supported.

3.2.4.3 TCP and UDP port usage

The following table lists the default port usage for the various types of external connection the gateway needs to establish, ensure that legitimate traffic through the actual ports being used is not being blocked by a firewall.

Table 3 TCP and UDP Port Usage

Port	Type	Comment
8883	TCP	Default MQTT broker port where Transport Layer Security (TLS) is used
1883	TCP	Default MQTT broker port where TLS is not used
123	UDP	NTP (Network Time Protocol) server.
53	UDP/TCP	DNS (Domain Name Server) – usually UDP.

3.2.4.4 LTE/UMTS mobile data

The mobile connectivity option is supported only through the use of external antennas. The Main antenna can be used for 3G/UMTS. Use of Main and Diversity antenna is mandatory for 4G/LTE.

The gateway supports multiple bands to allow worldwide coverage and requires the end-user to select an appropriate provider and install the associated micro-SIM card.

Note: Mobile connectivity has limited country-specific radio approvals, besides general support for RED/FCC/ISED. Please refer to [Certifications](#) for details. If Mobile Data Connection is not supported, an external 3G/4G modem can still be used.

To install the SIM card:

1. Remove the lower top cover and the blanking plug
2. Insert the SIM card as shown in the figure below
3. Ensure the SIM card is in a locked position
4. Install the blanking plug ensuring that the IP65 seal is positioned properly



Figure 34 SIM card installation

Note: To remove the SIM card, press the SIM card to release the internal locking mechanism.

3.2.5 Commissioning

The Enlight Collect Manager app guides the user through the related processes of gateway commissioning and decommissioning. Gateway commissioning requires a gateway in a non-commissioned state and the app running on a mobile device with an active Bluetooth interface. The pre-requisite configuration work in @ptitude Observer software must also have been completed, refer to sections 2.1 through 2.4.

- A. Launch the app. Note that an earlier log in with network access is recommended.
- B. Select **Scan Gateway** function, from the Main menu.

With the gateway powered and in place the user can choose, in-app, to scan for and then identify the gateway via either:

- **QR** (Quick Response) code
- **Bluetooth**, the user chooses from a list of gateways that are in range

Note: If due to its physical location it is not possible to reach the gateway to uniquely identify it and the Bluetooth method is used, be aware that multiple gateways may be detected by a scan and take care to identify the correct device.

- C. Select the gateway to connect to it and view its status.
- D. The gateway should be decommissioned, press Commission to proceed.
- E. Now choose the virtual gateway, configured in @ptitude Observer, that this physical gateway should be associated with. Virtual gateways will be listed with both their name and location text visible. Virtual gateway locations that are already commissioned will have MAC addresses associated with them and be unavailable for selection.
- F. Having now selected the associated physical and virtual gateways press Commission to complete the process.

The configuration the gateway now has is not the measurement configuration but the settings that facilitate data exchange with its sensors and the @ptitude Observer software. The latter includes:

- The gateway networking interface:
 - o **Ethernet (wired)**
 - o Wi-Fi
 - o Mobile
- IP configuration for the selected network interface
 - o **DHCP** or
 - o Static: IP address, subnet mask, gateway and DNS settings
- Wi-Fi connection setup, where Wi-Fi selected
 - o Security: **WPA2-Personal** or WPA2-Enterprise
 - o SSID and password: password received and stored by the gateway as an encrypted string
 - o Country
 - o CA (Certificate Authority) certificate, EAP (Extensible Authentication Protocol), Identity and similar configuration data where WPA2-Enterprise security is in use.
- Sensor, mesh radio setup
 - o Security: 128-bit AES encryption key
 - o A unique, mesh network, identifier
- Configuration for the software connection
 - o @ptitude Observer Monitor connection address
 - o Client certificate (if TLS is being used)

Note that default values are those shown above, in bold. Any errors encountered in transferring the configuration are reported in-app. All credentials stored are encrypted.

On successful completion of the commissioning activity, the gateway status is changed to commissioned and the networking and sensor mesh radio, are activated. Sensors can now be commissioned.

3.2.6 External antennas

The use of external antennas creates options for placing the gateway inside metal enclosures. They do not provide significant improvement on the range over the internal antennas, but in specific cases, the wireless connectivity quality can be improved. Wireless radio standards dictate some requirements for antenna selection and installations.

Note: Use of external antennas is mandatory for use of internal gateway Mobile connectivity support.

Based on the below selection requirements, the DeLock 12545 broad-band antenna has been selected and certified with the CMWA6600 Gateway. The same antenna model may be used for all connections: Miramesh, WiFi/BLE and Mobile (3G/4G).

To comply with North American and European standards, the DeLock 12545 can be used, but other alternatives are possible, provided they meet the following criteria and specific limitations as listed in section [Certifications](#) which, defines specific certification details.

Note: For specific frequency band purpose, specific antenna selection can result in better performance. The DeLock 12545 will serve all frequency bands, but performance may not be optimal for all supported frequencies.

Antenna Requirements:

- Maximum cable length: 3 m
 - o Cable quality and length determine power loss that will affect maximum radiated power levels and associated wireless range
- Antenna separation at least 20 cm
 - o Multiple antennas cannot be directly placed on the gateway antenna connectors
 - o Installation provisions need to be planned for the external placement of the antennas. Default cable length of 1m should be sufficient to comply with antenna separation requirement
 - o Ensure perpendicular installation of Main and Diversity antenna to optimize overall signal reception
- Maximum antenna gain (dBi peak) excluding cable loss
 - o Miramesh – 2.4 GHz: 3.4 dBi
 - o Wi-Fi/BLE – 2.4 GHz: 1.8 dBi
 - o Wi-Fi – 5 GHz: 4.1 dBi
 - o Mobile 3G/UMTS:
 - **Band 2** 8.01 dBi
 - **Band 4** 5.00 dBi
 - **Band 5** 6.11 dBi
 - o Mobile 4G/LTE:
 - Band 1 5.00 dBi
 - **Band 2** 8.01 dBi
 - Band 3 5.00 dBi
 - **Band 4** 5.00 dBi
 - **Band 5** 6.11 dBi
 - **Band 7** 8.01 dBi

▪ Band 8	4.20 dBi
▪ Band 12	5.61 dBi
▪ Band 18	6.07 dBi
▪ Band 19	6.11 dBi
▪ Band 20	5.15 dBi
▪ Band 28	4.20 dBi

Note: maximum antenna gain requirement for Mobile applies specifically for bands used in North America (**bold** font) and governed by FCC/ISED. Other supported 4G/LTE bands are listed as references in this overview to aid in antenna selection (no data is available on European 3G/UMTS bands, but bands 1, 2, 4, 5, 8, 9 and 19 are supported by cellular radio).

Antenna recommendation

The Delock 12545 antenna has been regulatory tested with the CMWA6600 GW to serve as an all-band antenna solution for Miramesh, Wi-Fi/BLE and Cellular applications.

This antenna, suitable for indoor and outdoor use, has a 1m integral cable and male SMA connector for direct interfacing to the CMWA6600 GW antenna connections. Furthermore, this antenna has easy nut based mounting capabilities.



Figure 35 Delock 12545 antenna

Antenna Gain (max pk):

• 698 – 960 MHz:	1.7 dBi
• 1710 – 2170 MHz:	1.7 dBi
• 2300 – 2700 MHz:	2.0 dBi
• 5180 – 5825 MHz:	2.9 dBi

VSWR (max):

• 698 – 960 MHz:	6.0
• 1710 – 2170 MHz:	2.5
• 2300 – 2700 MHz:	2.5
• 5180 – 5825 MHz:	2.3

Other specifications:

- Operating temperature: -40 °C ~ 85 °C
- Housing material: polycarbonate
- Protection class: IP67
- Colour: white
- Cable: coaxial
- Cable type: ULA100
- Cable colour: black
- Cable diameter: ca. 2.8 mm
- Cable attenuation: 0.98 dB @ 1500 MHz per meter
- Smallest bending radius: 14 mm
- Cable length incl. connectors: ca. 1 m
- Dimensions (LxD): ca. 77 × 45 mm

3.2.7 Other interfaces

- **USB service interface**

A USB service interface is available internally, for SKF use only or under the direction of SKF's [Technical Support Group TSG](#) or SKF application engineers

3.3 SKF Enlight Collect IMx-1 wireless sensors

3.3.1 Installation considerations

When selecting a location for the sensor bear in mind that the sensor is single axis, the vibration sensitive axis is through and perpendicular to, the mounting face. Choose an appropriate installation position:

- Suitable for the machine vibration/temperature measurement envisaged
- Avoiding unnecessary exposure to sources of radiant heat
- That doesn't impede routine maintenance of the machine
- Where the transducer is not easily damaged
- Of a suitable size and with clearance for mounting and accessing the sensor
- With the mounting area suitably prepared to ensure a good contact interface
- Mount it securely using stud or adhesive-stud mounting

Ensure that maintenance procedures are updated to include, where necessary, the decommissioning and/or safe removal of the wireless sensors during machine maintenance and overhaul.

3.3.2 Mounting detail

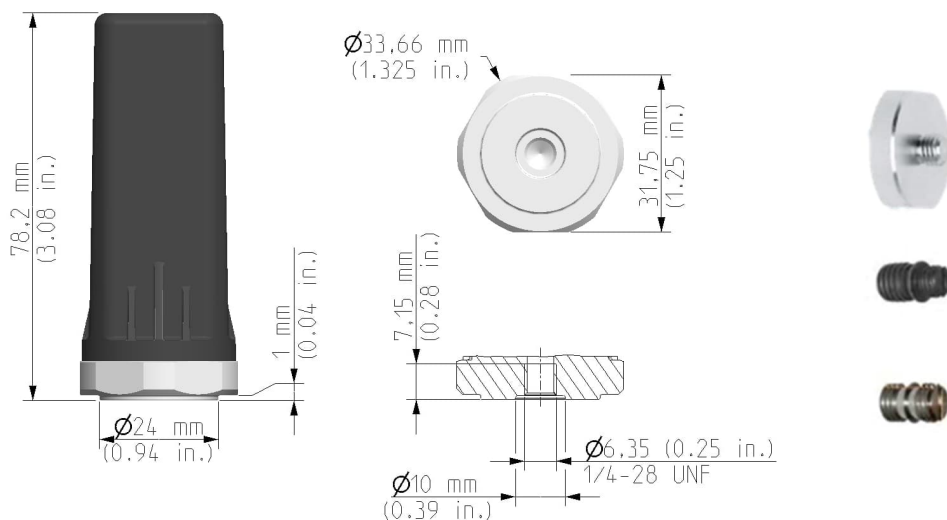
Once the mounting/measurement point location is decided, prepare the surface appropriately:

- For direct stud mounting, drill and tap to suit the stud being used and spot face an area if necessary. Recommendations:
 - o Depth: greater of 8 mm (0.31 in.) or stud length plus 2-threads.
 - o Drilled perpendicular to the mounting surface, within $\pm 1^\circ$.
 - o Flat mounting surface for the IMx-1 – within 25 μm (0.001 in.).
 - o Surface roughness no greater than 0.8 μm (32 $\mu\text{in.}$).
 - o When fitting, ensure there is no gap between the mounted sensor and the mounting surface.
- For adhesive stud mounting, remove paint, clean and apply the adhesive. Apply activator to the stud base, position and apply pressure until the adhesive cures.

To minimise any sensitivity to pick-up from nearby mains powered equipment or switching from frequency inverters, the use of direct mounting or an electrically conductive adhesive is recommended to ensure a good earth connection to the sensor base.

Note that the mounting detail of the IMx-1 sensor is identical to the SKF Wireless Machine Condition Sensor, CMWA 8800, and being as the IMx-1 is a little shorter, the same tools and similar procedures can be applied.

The sensor base, sensor mounting detail and typical mounting studs are shown in the figure:



- a) Sensor base/mounting detail
- b) Various studs

Figure 36 Key sensor dimensions and example stud fixing options

The sensor mounting nut is 6-sided, “6-point”. When fitting the sensor to the stud, always apply torque to that mounting nut rather than using the main sensor housing. See also sensor [environmental and physical](#) specifications for other dimensional data and spanner sizes.

3.3.3 Pre-commissioning tasks

Before any commissioning of sensors commences, each sensor location being populated should have an associated machine/system location, in the database. This pre-commissioning work should be done ahead of time so that the database is



Commissioning, decommissioning, or any other operations which require the use of the NFC connection are forbidden inside an explosive atmosphere.

populated with information on the sensor configuration and location. Prepare the app by configuring connection details for that @ptitude Observer instance.

3.3.4 Commissioning

Assuming the sensor pre-commissioning steps have been completed and a commissioned gateway is within range, once at the machine proceed as follows:

- A. Launch the app. An earlier log in with network access is recommended.
- B. Select the **Scan Sensor** function.
 - a. Bring the device close to the sensor to use NFC to wake it up, out of flight mode. Refer to [Commissioning troubleshooting](#) for guidance on positioning the device relative to the sensor when using NFC.
- C. After a period for Bluetooth search the ID of the sensor will be displayed. Select it to connect and display sensor status and other information.

Note: sensors that are running firmware 3.0 or later will skip the selection step and provide their ID through the NFC.
- D. To commission it:
 - a. Press **Commission**.
 - b. Drill down through the **Functional location > Asset >** to the desired Location tag.
 - c. Leaf mode “yes”/”no” set in @ptitude Observer, can be overridden at this point if needed.
 - d. Confirm selections by pressing **Commission**.
- E. App shows confirmation of successful commissioning or error. After exiting this screen, the app will instruct the commissioned sensor to activate its mesh radio and attempt to connect. If the commissioning attempt was unsuccessful then the process can be repeated by pressing **Try Again**.

Relay node commissioning

- F. If not installed prior to commissioning, install the sensor now.
- G. Repeat steps B to F for all sensors being processed.
- H. Note that it can take some time before a sensor joins the mesh and is able to send a notification to @ptitude Observer. When @ptitude Observer displays the sensor Hardware ID, this is the indication that this process is complete and sensor configurations can be synchronised.

Note: as mesh networks adapt, the sensors should not be activated until they are at their mounting location.

For a more complete understanding of the interaction between the sensor's proximity, WPAN and mesh radio systems and the normal process flow, refer to the description in [IMx-1 sensor troubleshooting](#).



Commissioning, decommissioning, or any other operations which require the use of the NFC connection are forbidden inside an explosive atmosphere.

3.4 Relay node commissioning

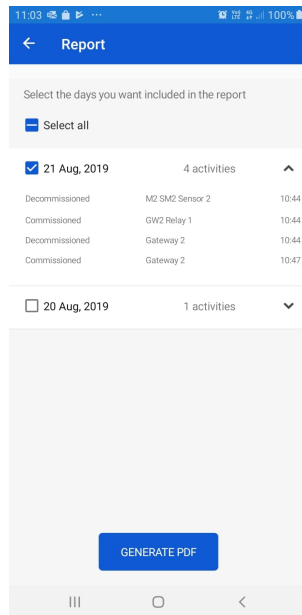
First, complete the pre-commissioning task in @ptitude Observer. Then the on-site commissioning of the node mirrors closely the sensor commissioning process:

- A. Launch the app. An earlier log in with network access is recommended.
- B. Select **Scan Sensor** function
 - a. Bring the device close to the sensor to use NFC to wake it up, out of flight mode.
- C. After a period for Bluetooth search the ID of the sensor will be displayed. Select it to connect and display status and other sensor information.

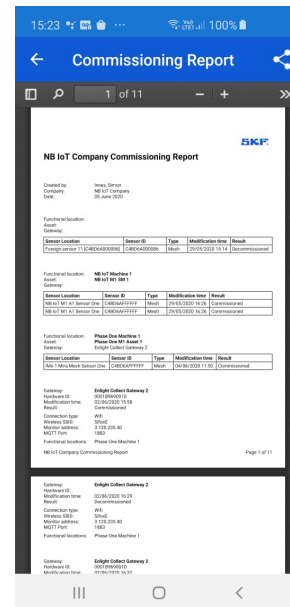
Note: sensors that are running firmware 3.0 or later will skip the selection step and provide their ID through the NFC.
- D. To add it as a relay node:
 - a. Press **Add As Relay**.
 - b. Select from the list of available gateways and choose the appropriate relay node. To aid the selection process, in the lists of gateways and then relay nodes associated with a selected gateway, both device name and location text will be visible.
 - c. Confirm selections by pressing **Commission**.
- E. App shows confirmation of successful commissioning or error. After exiting this screen, the app will instruct the commissioned relay node to activate its mesh radio and attempt to connect. If the commissioning attempt was unsuccessful then the process can be repeated by pressing **Try Again**.
- F. Repeat steps B to E for all relay nodes being processed.

3.5 Generating a commissioning report

To generate a commissioning report, select **Report** from the main menu. The data to be included can be from one or more workdays:



a) Select data for report



b) Commissioning report

Figure 37 Preparing and viewing a commissioning report

The report is stored, in pdf format, to the app's private cache directory but can be exported using the standard device Share functionality to e-mail, cloud storage, etc.

3.6 Offsite commissioning

Choose this option if you need to commission sensors in advance at a different physical location before installing them at their final position on-site. This option will put the commissioned sensors into flight mode and thus prevent significant battery degradation while waiting or in transit.

Once in its final position, when the NFC tap process is followed, the sensor will automatically go into mesh mode. This allows you to quickly activate the sensors onto the network.

Note: you should ensure that sensors are clearly labelled beforehand so they can be mounted at the correct positions and that the associated gateway is in place and powered on.

To activate the offsite commissioning, in the main menu click on the vertical ellipsis , select **Offsite commissioning** and toggle the **Commissioning sensors offsite** button. Or go to the Scan sensor view and select the **Offsite commissioning** banner located at the top of the screen.

INSTALLATION AND COMMISSIONING

Offsite commissioning

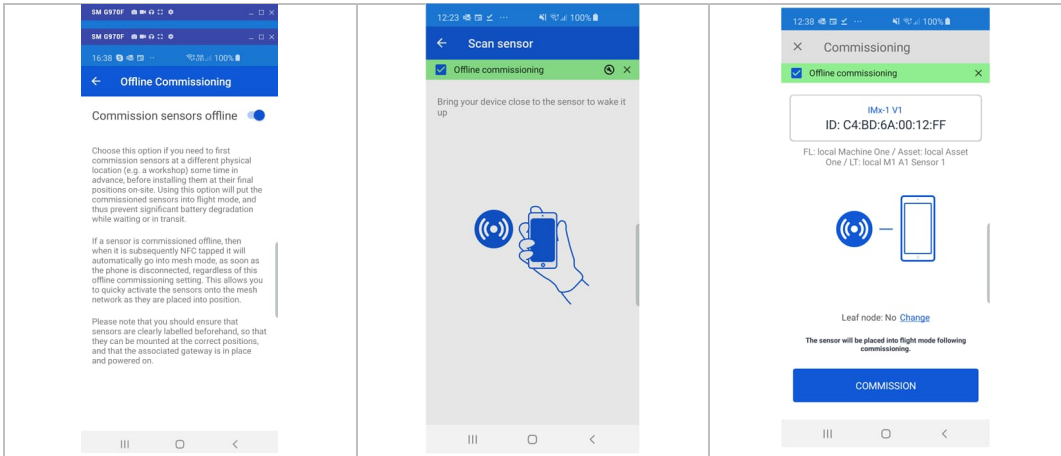


Figure 38 Offsite Commissioning

To perform an offsite commissioning of sensors, go to the Sensor scan view and tap the sensor to connect to it.

When the user connects to a non-commissioned sensor, there is an offsite commissioning icon at the top right of the screen. Tap the icon to open a banner with controls to activate or deactivate offsite commissioning mode.

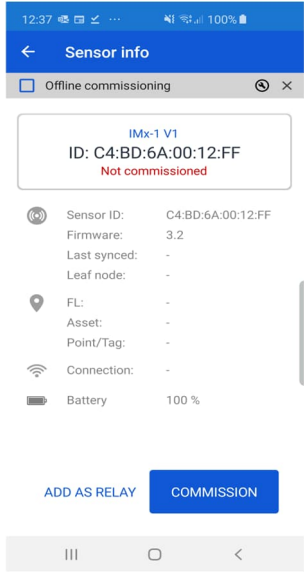


Figure 39 Sensor scan – offsite commissioning icon

If the selected option is commissioning in offsite commissioning mode, a note saying the sensor is placed in flight mode following will be shown.

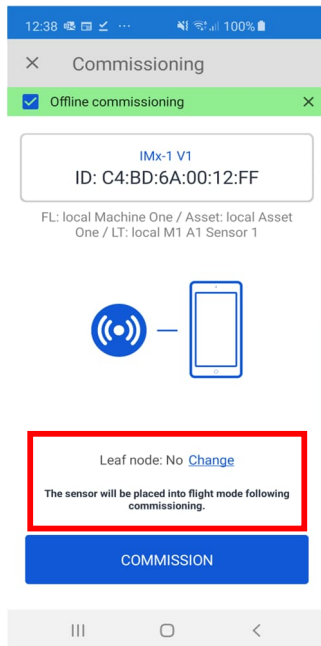


Figure 40 Commissioning – sensor placed in flight mode information

On completion of offsite commissioning of a sensor, there will be a note on the results screen reminding the user that the sensor has been placed into flight mode and needs to be tapped once more to put it into mesh mode.

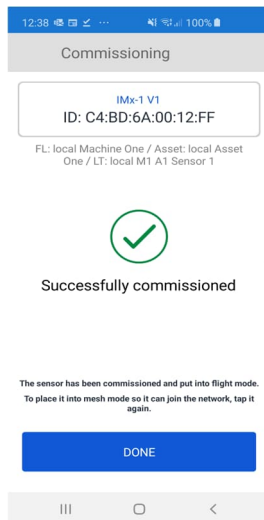


Figure 41 Successfully commissioned – with reminder to place the sensor into mesh mode

To install the sensor and place it into mesh mode, select the **Scan Sensor** option and the sensor will be tapped as normal. If offsite commissioning is selected, the banner will change its colour from grey to green.

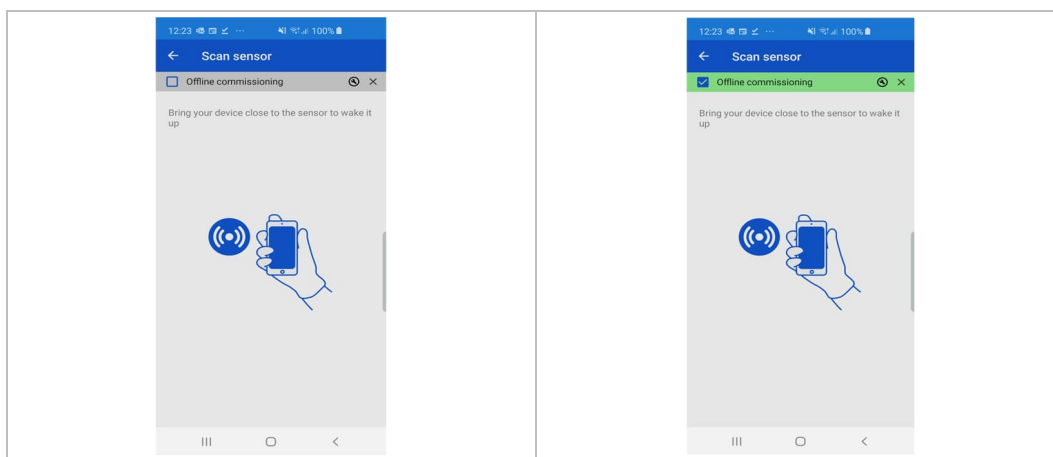


Figure 42 Scan sensor

You can also minimise the banner by tapping the ✕ button. The banner will appear as shown below:

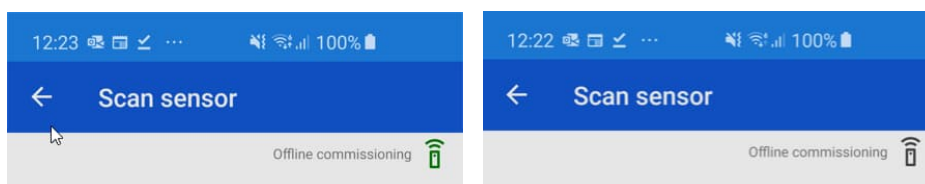


Figure 43 Offsite commissioning banner minimised

If the app finds the sensor is commissioned already, then it will connect, place the sensor into mesh mode, disconnect and then present this pop-up message:

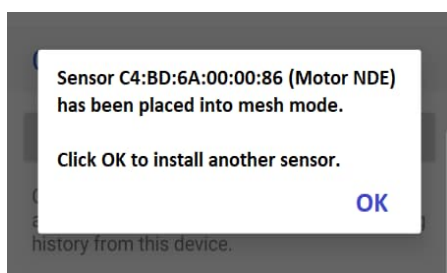


Figure 44 Pop-up info – Sensor placed in mesh mode

After the user dismisses this message, the app will return to the Scan Sensor view and a user can go to scan and install the next sensor.

4 Maintenance functions

4.1 SKF Enlight Collect IMx-1 wireless sensor

4.1.1 Updating sensor firmware

Like gateway firmware, sensor firmware is stored in @ptitude Observer and is first transferred to the gateway. Standard or Alternative firmware are supported, this choice is a gateway level selection, so applies to both sensors and gateway.

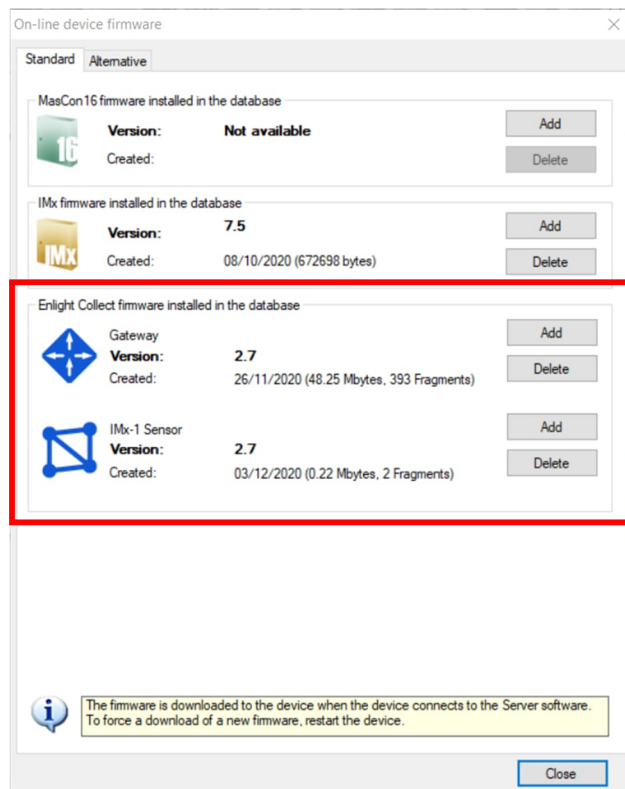


Figure 45 Gateway and sensor firmware is stored in @ptitude Observer

Once loaded to @ptitude Observer new sensor firmware is downloaded automatically to connected gateways and from there propagates across the wireless mesh. During this transfer, which for a system of 20 sensors may take 12 or more hours to complete depending on network transfer time, measurement data continues to be collected per the schedule but when a sensor is downloading firmware some missed measurements should be expected, typically corresponding to a period of around 7-hours.

When the process is complete the new sensor firmware revision is reported to the gateway and onward to @ptitude Observer. Note that depending on when the next

gateway status message is due to be sent, the reporting of the sensor firmware update may lag actual completion of that update by up to 48 hours.

For sensor firmware updates from @ptitude Observer, both the sensors and the controlling gateway must be commissioned. The gateway supports only a single sensor firmware image, all sensors associated with the gateway will be updated to that same firmware version.

Note that whilst sensor firmware can be deleted from @ptitude Observer, that deletion doesn't affect the copy stored at the gateway and if a distribution of that firmware is underway (staged), it will continue.

4.1.2 Sensor replacement or removal

A wireless sensor may need to be replaced if a fault occurs or when the battery is reaching the end of its life.

At the physical machine, remove the old sensor and if still operating, decommission it using the app. Scan for and select the sensor, the sensor status should show as commissioned with the Decommission option available:

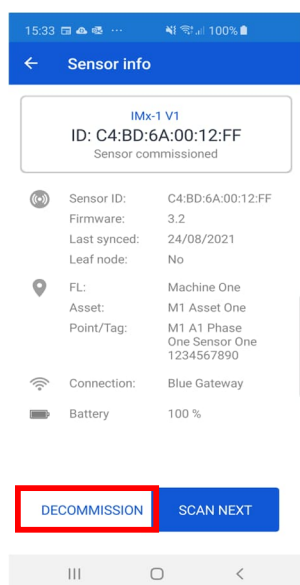


Figure 46 App Decommission button

The app Decommission process clears the association the sensor has with the database location, mesh parameters and puts the sensor into flight mode. If it is being replaced, now install and commission the replacement sensor as described in sensor commissioning.

Finally, in @ptitude Observer clear the Hardware ID of the previous sensor from the database. Where a replacement sensor has been installed, this leaves the sensor position free and available for accepting data from the new sensor.

4.1.3 Sensor maintenance

The IMx-1 hardware is maintenance free, non-repairable and users must not attempt to open the device. Firmware updates are available OTA, from @ptitude Observer software.

4.1.4 Sensor performance over time

No significant performance degradation over time is expected, until the integral battery has reached the end of its life. Good practice is to be aware of the estimated remaining battery life, investigate any apparently anomalous readings or status errors and when needed initiate a sensor exchange.

4.2 SKF Enlight Collect Gateway

4.2.1 Updating firmware

Gateway firmware is stored in @ptitude Observer and the process for updating firmware is as follows:

- First, be aware of whether the target gateway is using Standard or Alternative firmware. Check this at IMx-1 System View > Gateway properties.
- Go to **On-line > Firmware > Enlight Collect firmware installed in the database** and select the **Standard** or **Alternative** tab.
- To add new gateway firmware, click the appropriate **Add** button and select and open the gateway firmware package/zip. The firmware file will be imported/added to @ptitude Observer.
- Once added, the firmware will be automatically downloaded to connected gateways. If required, this download process can also be initiated manually: return to the IMx-1 System View and select the target gateway. Verify the **Connection State** is **Connected**, and press **Synchronize**.

The gateway will check the compatibility and integrity of the firmware package before implementation to avoid loading a non-functional firmware. Note that firmware update will take the gateway offline for a few minutes, maximum.

When the process is complete the gateway firmware version reported in @ptitude Observer will update. Note that on cloud-based systems, the transfer of the gateway firmware may take some time to complete.

For gateway firmware updates from @ptitude Observer, the gateway must be commissioned.

4.2.2 Modify gateway network configuration

Whilst the network configuration of a commissioned gateway can be updated by decommissioning and recommissioning, this has the disadvantage that the gateway loses and then must re-establish its sensor relationships.

Changes in the network configuration are automatically sent to the applicable gateway only if the gateway is commissioned and connected to Observer.

To avoid this additional work and delay, the Enlight Collect Manager app provides an UPDATE SETTINGS button that allows a commissioned gateway's network configuration to be refreshed without disturbing the sensor mesh.

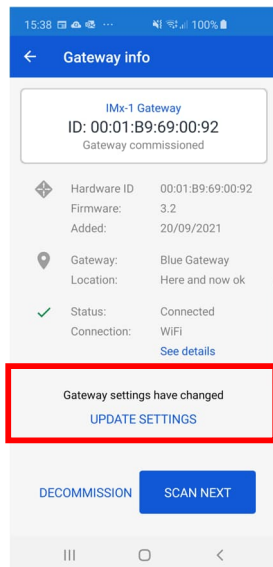


Figure 47 Update gateway network configuration

4.2.3 Decommissioning

Decommissioning is required if a gateway is to be relocated or replaced as it avoids any possibility of two similarly configured and commissioned gateways attempting to connect with the same set of sensors. When a gateway is being replaced, never leave it commissioned and powered in the same area, even if disconnected from the wider network.

Like commissioning, this is a 2-step process requiring software changes and the mobile app. Refer also the notes below.

In @ptitude Observer:

- In the IMx-1 System View, select the gateway to be decommissioned

Assuming the gateway is responsive, on-site the mobile app is used to complete the decommissioning of the gateway. With the gateway powered and in place, the app can scan for and then identify the gateway via either:

- QR (Quick Response) code

- Bluetooth, the user chooses from a list of gateways that are in range

The user can at this point, select **decommission**.

- App shows confirmation of successful decommissioning or error

Decommissioning sets the gateway back to a factory default state:

- disables the network and mesh radio interfaces
- erases configuration, measurement and event data stored on the gateway and the sensor firmware package
- Clear the device Hardware ID: that physical gateway can no longer connect to @ptitude Observer.

Notes:

The current gateway firmware is maintained, not reverted.

The steps taken above in @ptitude Observer and on site using the app are independent and any one action can be taken without the other with no significant consequences. Any one action will stop the measurement data flow from that machine, or machines, to @ptitude Observer. Until the Hardware ID is cleared another gateway cannot replace the earlier unit and until it is replaced or the ID cleared, some errors may be logged due to the loss of connection with the decommissioned gateway.

Also note that measurement data already transferred to @ptitude Observer remains available.

To decommission a gateway, follow the guidance above. Using the **Delete** button to remove a gateway is different and should not be actioned without recognising that it has the following implications:

- Associated relay sensors will be deleted.
- Gateways cannot be deleted without first unlinking them from associated machines.
- Unlinking a gateway from a machine requires any commissioned sensors to be deleted first, thereby losing any associated measurement data.
- DO NOT delete a virtual gateway if the physical gateway is still commissioned and working, as it will be impossible for the app to connect to that gateway afterwards to decommission it (due to security requirements for accessing commissioned gateways). If this happens, the only way to recover the gateway is to factory reset it.

4.2.4 Replacement

Gateway replacement may be required if a faulty or damaged gateway is identified. A specific feature/function for gateway replacement is not included in this release, replacement is achieved by decommissioning the old gateway and then commissioning the new gateway.

4.2.5 Gateway maintenance

The SKF Enlight Collect Gateway hardware is designed to be maintenance free and incorporates no batteries and no fans.

It does not contain any user accessible fuses. Active power limitation is used with an internal fuse acting only as a last resort protection in case of failure of this circuitry. Any repairs can only be carried by an SKF repair centre.

Firmware updates will be available from @ptitude Observer software.

4.2.6 Gateway performance over time

No significant performance degradation over time is expected. Good practice is to investigate any apparently anomalous behaviour or status errors and if needed initiate a gateway exchange.

4.3 Troubleshooting

4.3.1 Introduction

This section is intended as an aid to fault finding, on an SKF Enlight Collect IMx-1 System. It is designed for instrumentation and system engineers with sufficient knowledge of troubleshooting including safe working procedures, in industrial electronic systems powered by 9 to 36 V DC.

SKF strives to provide information that is as accurate as possible. However, SKF cannot be held responsible for any injury or damage to persons or material that occur in the interpretation of, or due to actions taken based on, information in this document.



The product warranty will be invalidated if the sensor or gateway has been mishandled or if incorrect connections have been made to the gateway that expose any sub-system/circuit to voltages in excess of their operational rating.

Installation errors that require the involvement of SKF personnel to rectify, may incur additional charges.

The following sections list some further considerations when troubleshooting a system. If a resolution to the problem is not forthcoming, contact SKF's [Technical Support Group TSG](#) for further advice: @ptitude Observer, Monitor and the [gateway](#) maintain a number of logs that TSG may request to aid fault finding.

4.3.2 Logs and viewers

Event log

@ptitude Observer maintains a time stamped event log and this supports the SKF Enlight Collect Gateway and its associated sensors. Always check this event log for evidence of errors, activity or status changes that might explain any functional issues.

For the Event Log the following notes apply:

- Access the Event log from On-line > Event Log.
- For an Enlight Collect IMx-1 System, class will be shown as **S**.
- Event types cover a range of different conditions related to firmware update, configuration change, loss of connectivity, gateway restart or reset, user log-in to the gateway and integrity checks, etc.
- The display can be filtered by the DAD that is the source of the event, for example a specific gateway, by date range and by event Type:

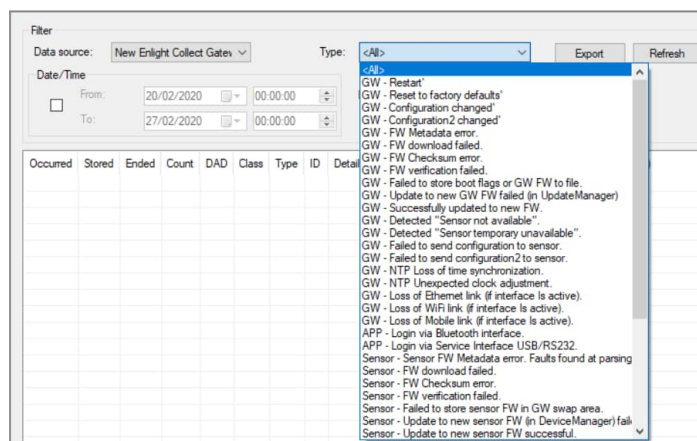


Figure 48 Event log filtering

- Count is related to the duration of an event:
 - o 0 for an event without duration, for example gateway restarted.
 - o 1 event start for example log-in or loss of connectivity.
 - o -1 for event end for example log-out or connectivity regained.
- Some event types are adapted for a wireless sensor:
 - o A gateway detecting that a sensor has not responded to a communication results in a **Sensor temporarily unavailable** event. This causes @ptitude Observer to set a sensor **Not measured**, status.

- o A gateway detecting that a sensor has been unavailable for 24-hours results in a **Sensor not available** event that causes @ptitude Observer to set a sensor 'Sensor fault' status.
- o Note also that in terms of the status displayed in the @ptitude Observer hierarchy, receiving no measurement data for twice the expected interval will also cause the sensor and its measurement points to be set to **Not measured** status.
- An Export function allows the export of events to an Excel file for further analysis or sharing.

Monitor service log and viewer

As it is the Monitor service that receives the data from the IMx-1 system, that interface can contain relevant information regarding the system performance and MQTT connection status.

To view current **Status** and recent **Events**, open the @ptitude Observer Monitor service viewer:

- From @ptitude Observer, access it from **On-line > Monitor service viewer**
- Or, double click the Monitor area in the lower status bar

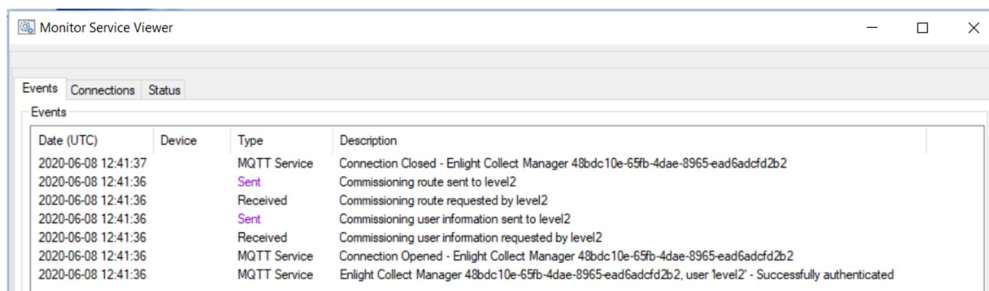
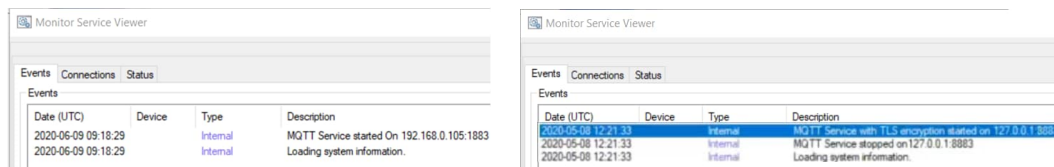


Figure 49 Monitor Service Viewer – Events – EC Manager app sync request – non-TLS



a) Without TLS

b) With TLS

Figure 50 Monitor Service Viewer – Events – MQTT service started

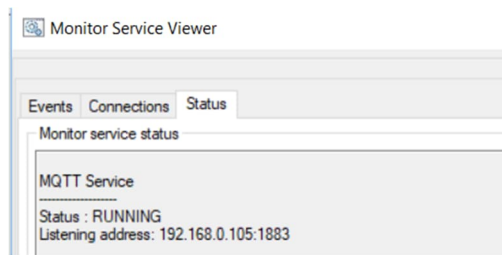


Figure 51 Monitor Service Viewer – Status – MQTT Running (TLS not enabled, example)

When troubleshooting uses these tools to ensure that the expected MQTT service is running (IP address, port, with/without TLS) and that successful connections are being made.

For events related to IMx-1 sensor data:

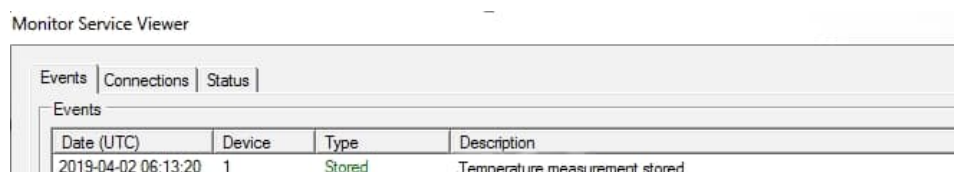


Figure 52 Monitor Service Viewer example

- Events: types for IMx-1 sensor data can be Stored or Error.
- Note that data time stamped earlier than 3 years before the current date will be rejected. The description field will include the invalid date that caused the data to be 'trashed' and the event Type will be set as Error.
- Internal: generally, relates to 'internal' actions being initiated or completed as data is processed.

The associated Monitor log file can be accessed directly from the Application data folder (log file naming follows the connection naming) or alternatively open from the @ptitude Observer Monitor Manager software by selecting the appropriate service then **Action > View log file**. The contents of that file, the level of detail stored, are influenced by the Log detail level settings made in @ptitude Observer, **Database > Options > Monitor service tab**.

Mesh network information log

For troubleshooting and understanding the mesh characteristics of an Enlight Collect IMx-1 system, this logfile can be enabled via **Database > Options > Enlight Collect IMx-1 System Global Settings**, tab:

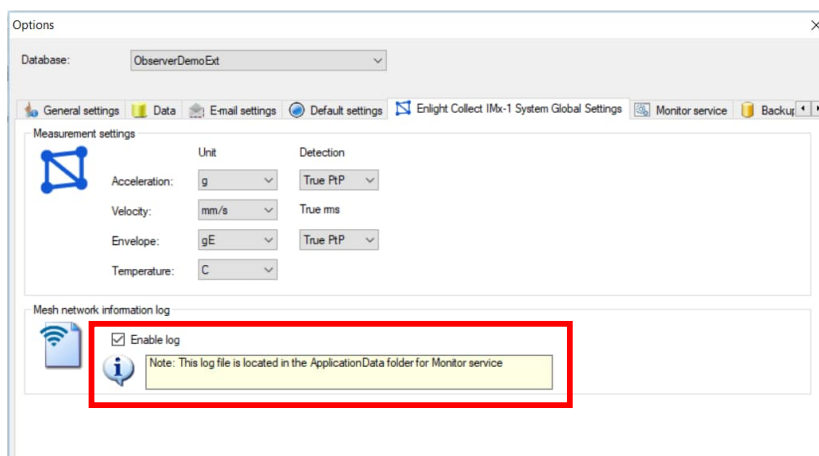


Figure 53 Enabling the 'Mesh network information log'

The log will be created in the application folder for the monitor service and will be named <MonitorName>IMx1SensorMeshInformation.log, i.e. prefixed by the actual name of the monitor service. It is a human readable CSV format file that provides information on sensor mesh, parent-child relationships and performance statistics such as packet loss and transfer time:

- Log time
- Timestamp from sensor
- Sensor hardware ID
- The last 8-bytes of the sensor address
- The last 8-bytes of the sensor parent address
- Parent link metric
- Packets sent
- Packets lost
- Packets round trip minimum
- Packet round trip maximum
- Packets round trip average
- Network instability flag
- Watchdog reset flag
- Sensor self-diagnostic (see also Status, [2.3.2](#), for decoding information)
- Gateway Hardware ID
- The last 8-bytes of the gateway address

Such information can be invaluable when troubleshooting issues with the performance or behaviour of the sensor mesh.

4.3.3 IMx-1 sensor troubleshooting

Possible causes for a non-responsive sensor include:

- Sensor is in flight mode.
- Incorrect or incomplete configuration.
- Mechanical damage.
- Sensor fault including discharged battery.
- Loss of mesh communications – likely multiple sensors affected.

In working on IMx-1 systems the interaction between the various radio systems that the sensor incorporates should be considered. Be aware that, as described below, various timeouts apply to the sensor radios to avoid unnecessary battery drain.

Red: The phone/app uses its Bluetooth capability to interact with the sensor
Blue: The phone/app uses its NFC (tap) capability to control the sensor mode

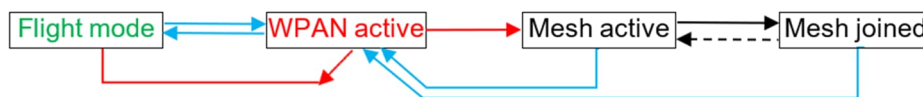


Figure 54 Sensor radio interactions and flow – all conditions

Start point for the flow described in the figure above, is a sensor in flight mode. An NFC tap from the phone/app will take the sensor out of flight mode and activate its WPAN radio, so the sensor is discoverable by the app using the phone's Bluetooth radio.

- At this stage a further NFC tap would have no consequence.
- If the app doesn't connect to the sensor via Bluetooth then after a few minutes the sensor will revert to flight mode.
Note that with sensor firmware 3.3 the sensor will timeout back to mesh mode if it is in a commissioned state.

For a new sensor being commissioned, the app will normally then connect via Bluetooth, configure it and instruct it to switch to its mesh radio. If this process doesn't complete properly, the following apply:

- Having connected, if the app communications aren't properly closed or are not maintained, after 10-minutes of inactivity the sensor will revert to flight mode.
- Similarly, once connected, a second tap will also return the sensor to flight mode.

With the mesh identity configured and mesh radio activated, the sensor will attempt to join the mesh. The mesh active state may also be resumed if for some reason mesh connectivity is subsequently lost. This is shown by the dotted, return line.

- Note that in the mesh active state, the mesh radio will be deactivated if after 5-minutes it hasn't successfully joined the mesh. This initial deactivation or

sleep period lasts for 5-minutes but after subsequent failures it increases in coarse steps from 10 minutes up to 24 hours between mesh connection attempts.

An NFC tap on a sensor with its mesh radio enabled, joined, active or 'sleep' state, switches it back to WPAN radio, active mode.

- An NFC tap on a sensor will wake it from a sleep state and show in app a commissioned sensor's location in the hierarchy. Note that an NFC tap on a commissioned sensor temporarily takes it out of the mesh. The app knows from the sensor what mode it was in before the app connected and unless commissioning or decommissioning, will always set it back into that mode when disconnecting.

With WPAN active again, a command can return the sensor to flight mode.

- This is part of the process of sensor decommissioning, where the app clears the sensor of its configuration, before then instructing it to adopt flight mode.

Be aware that in addition to the normally expected flow, the following apply:

- If the app doesn't connect to the sensor via Bluetooth then after a few minutes the sensor will revert to mesh mode.
- If however, the app has connected but the app communications aren't properly closed or are not maintained, after 10-minutes of inactivity the sensor will move to flight mode.
Note that with sensor firmware 3.3 the sensor will timeout back to mesh mode if it is in a commissioned state.
- Similarly, once connected, a second NFC tap will also place the sensor in flight mode.

Sensor commissioning and decommissioning are subsets of the general interactions and can be similarly illustrated as follows:

Red: The phone/app uses its Bluetooth capability to interact with the sensor
Blue: The phone/app uses its NFC (tap) capability to control the sensor mode



Figure 55 The commissioning flow – app controlled

Red: The phone/app uses its Bluetooth capability to interact with the sensor
Blue: The phone/app uses its NFC (tap) capability to control the sensor mode



Figure 56 The decommissioning flow – app controlled

Important note: Sensor power consumption in mesh active mode is of the order of 100x greater than the consumption when the mesh has been successfully joined. Despite that the mesh radio will be deactivated if after 5-minutes the sensor hasn't successfully joined the mesh, there remains the possibility that in conditions of mesh instability, the sensor may experience frequent but short duration disconnections that will result in very high drain of the battery because the time-out mechanism is not being triggered. If this were to be sustained and left uncorrected, battery lifetime could be reduced to just a few weeks.

To detect this type of condition, the sensor self-monitoring will flag if three disconnections have occurred within a 24-hour period. System users should therefore be alert to:

- A system alarm in @ptitude Observer that flags that a sensor is reporting disconnections and/or frequent resets: Network Instability. The state of the network instability flag is also logged in the mesh network information log.
- Unexpectedly rapid loss of indicated, remaining battery life.

When either is apparent the user must take urgent action to stop the battery drain and correct the sensor mesh issues. If the sensor mesh will take time to evaluate and correct, to preserve remaining battery life, place the affected sensor in flight mode until the underlying mesh, network issues can be properly investigated and addressed.

4.3.4 Gateway troubleshooting

In the first instance, check the gateway status LED indication: for a gateway that is powered and connected to @ptitude Observer both LEDs should be fixed green light.

If the gateway status LED indicator manifests anything other than fixed green light, check for loss of system connectivity.

When the status LED indicator is flashing green, it may indicate that the system connectivity is OK, but the GW has not managed to synchronize its time.

In addition, the app functionality can be utilised for basic gateway and system troubleshooting, by observing whether the device is responsive in a scan of the area. Possible causes for a non-responsive or non-functioning gateway include:

- Incorrect or incomplete configuration.
- A defective or damaged gateway.
- Local hard wired or Wi-Fi network fault.
- Loss of power or internal fuse/circuit failure.

If the gateway is powered and believed functional but is not connecting to @ptitude Observer, consult also the [System connectivity](#) section.

4.3.5 Commissioning troubleshooting

NFC is a higher frequency, very short-range radio system so positioning and closeness are important. When using an NFC tap to toggle the mode of a sensor, be aware that the 'sweet spot' for NFC will be device dependent. To ascertain this for a particular device, move it around so that different areas of the rear of the phone are in close proximity to/touching the sensor. It may also be necessary to remove any external case or cover around the phone.

On iOS mobile phones, the NFC scanner is located at the top of the phone. Point the NFC scanner to the sensor to activate the NFC tab.

The sensor antenna is located internally, towards the middle of the 'flat side' of the sensor case. Its approximate location is marked in the figure below:



Figure 57 Approximate NFC antenna location

In a quiet environment it may be possible to hear an audible ding as a notification that the NFC tap was registered by the phone.

Be aware that the consistency of NFC and Bluetooth interactions with IMx-1 sensors may vary between phone models, even within those from the same manufacturer, due to differences in the detailed design. Where practicable, for IMx-1 system commissioning, standardise on known good performers and check the behaviour of new models before deploying them widely.

The app includes the capability to store application, activity log files. To enable the feature, from the Main menu tap the more options, vertical ellipsis ⋮, then select **Support**:

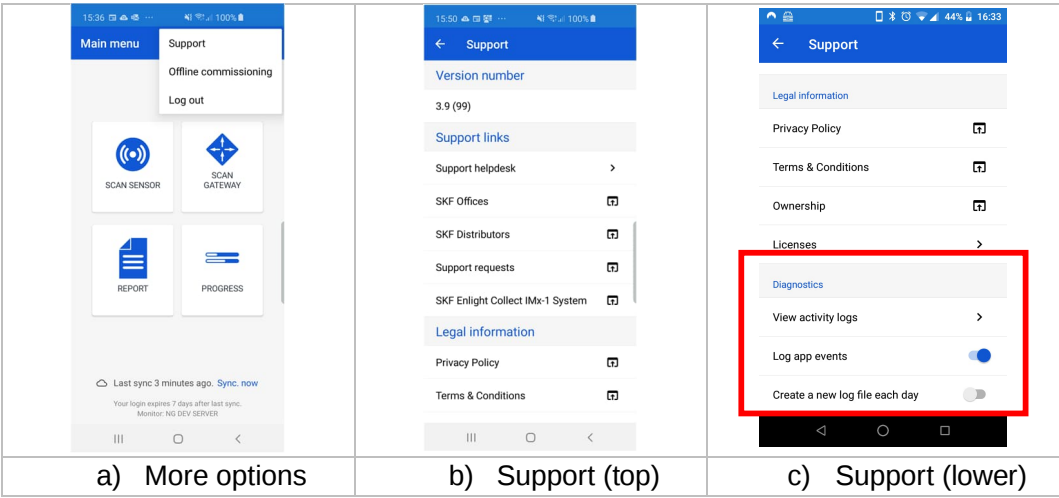


Figure 58 Enabling the app, log file feature via App Support options

In the Diagnostics section, which is in the lower half of the Support list, there is an option to enable log file storage, a further option to choose between a single continuous file or separate files each day and an option to view the created logs in app. When viewing a log file, it can be directly shared using phone's share capabilities.

As access to the above menu structure requires the ability to log in or still be logged in to a Monitor instance, an application log is also available via the system settings menu, [Figure 3](#). The application log includes information about the login process, so can assist troubleshooting in situations where this access hasn't been achieved.

If difficulty is experienced connecting to Monitor double check that the app Monitor configuration settings, [Figure 4](#), are correct for the Monitor server being connected to. In particular note that a mismatch of secure connection settings will not give an error that specifically mentions security and will return different errors depending on the exact nature of the mismatch:

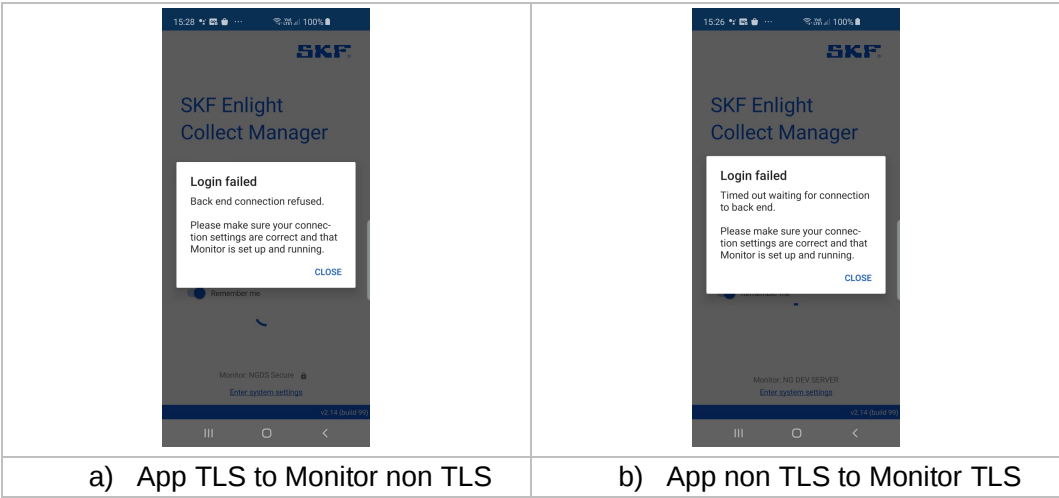


Figure 59 A mismatch of TLS settings causes connection errors

If difficulty is experienced detecting sensors in a scan and/or connecting to sensors that have been detected, this may be related to the phone's Bluetooth stack. To remedy this, consider the following possible actions to clear the issue:

- switch Bluetooth on the phone off then on.

If that doesn't result in an improvement, then:

- restart the phone or clear the Bluetooth cache and then restart the phone.

If sensors can be detected and connected to but unexpected difficulty is then experienced in commissioning them, check that in @ptitude Observer, the gateway has been assigned to the machine.

4.3.6 System connectivity

A loss of system connectivity is likely if the gateway status LED indication shows anything other than fixed green. When the status LED is flashing green, it may indicate that the system connectivity is OK, but the GW has not managed to synchronize its time. Possible causes for a loss of system connectivity include:

- Loss of power.
- Incorrect or incomplete configuration of the gateway.
- Local network fault.
- Wide area network fault, where @ptitude Observer is cloud based.
- Server-side failures:
 - @ptitude Observer Monitor error or not running.
- Gateway internal failure.

Secure connections add a further layer of complexity and opportunity for error aside from the basic IP connection information. Check that:

- The correct certificate is selected, it is in date and that the gateway has been commissioned with this information.
- There are not certificate related system and critical system alarms already flagged in the System alarm list.
- The [Monitor service viewer](#) is showing that the expected MQTT service has been opened.

Certificate expiration date is checked daily by Monitor and this check drives any related system or system critical alarms. If changing an existing certificate restart the @ptitude Observer system to trigger a refreshed loading evaluation of the certificate.

If any aspects of the network configuration change (including TLS aspects), complete the reconfiguration work in the @ptitude Observer system, update the app settings

as necessary, sync with Monitor and then use the app to [update the network settings](#) of affected gateways.

4.3.7 Gateway interfaces for SKF personnel

The gateway main enclosure should only be opened by or under the direction of appropriate SKF Application Engineers or SKF's [Technical Support Group TSG](#) personnel. To access the main gateway compartment first remove the lower cover and then unscrew the two Torx T10 screws that are now visible and lift the main enclosure lid away. Be aware that with the lid removed the LEDs will be very bright, it may be useful to have something to cover them temporarily whilst working on the gateway.

Note, on reassembly ensure that the main lid seal is correctly in place to preserve the enclosure IP rating.

- **USB service interface**

A micro-USB header provides access to the service interface. This interface is identified, circled, in the figure below.



Figure 60 Location of USB service interface connector

Important: Whilst the procedure for a factory reset of the gateway is described below it is always recommended to first attempt to achieve that, by decommissioning a gateway using the app.

Access USB service interface

Prerequisites for this work:

- Have available a PC with a terminal emulator, like Tera Term or PuTTY
- Connect the micro-USB cable between PC and gateway

- If not already powered, power the gateway
- Use Device Manager to confirm Ports (COM & LPT) has a device called:
 - o “Gadget Serial”
- For Windows 10 a driver should already be installed, for Windows 7 it will need to be manually installed. If the device isn't present or has errors, use the Zadig.exe described later.
 - o Note that Microsoft support for Windows 7 has ended and that SKF always recommends using supported operating systems and installing the latest updates.
- With the driver installed and the terminal emulator launched, connect at 115 200 baud and 8-N-1: 8 data bits, no parity and 1 stop bit. A typical configuration is shown below:

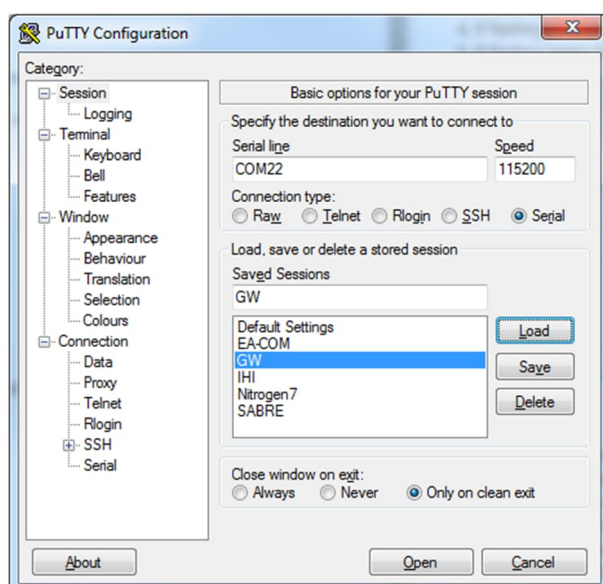


Figure 61 A typical terminal configuration for using the service interface

Reset to factory defaults

- At the login prompt, initiate the reset by using appropriate credentials for both Username and Password. When needed, these credentials can be provided by SKF's [Technical Support Group TSG](#).

Note: The gateway will respond with the message "Job for factory-reset.service canceled." when it has completed the factory reset.

Other diagnostic commands and functionality

The Username and Password credentials used above are only valid for the **Reset to Factory default** functionality. Other diagnostic commands and procedures that from time to time SKF may recommend or request, are subject to a secure logon with credentials specific to the particular gateway.

Windows 7 driver installation

- Have the USB driver installer utility: Zadig.exe, no installation needed, but note that admin rights are still required.
- Whilst connected to the gateway, run it and install the Gadget Serial driver:
 - o The Zadig main drop-down will list any devices not already having a driver, so from it select the **Gadget Serial** device, refer Zadig screenshot below.
 - o The Driver will be (None) – meaning no current driver, in the adjacent field use the up/down buttons to select USB Serial (CDC) as shown and then press Install Driver.

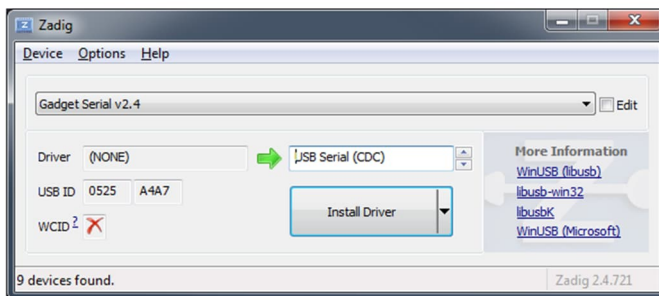


Figure 62 Using Zadig utility to install the USB device driver

- **Ethernet LEDs**

Although not visible externally, to aid fault finding, link and activity LEDs are available on-board for the Ethernet interface.

5 CMWA 6100-EX Sensor

5.1 Contact

SKF Development Centre Sensors
204 bd Charles de Gaulle
37540 Saint Cyr sur Loire
France

The SKF Development Centre Sensors can be contacted through the SKF's [Technical Support Group TSG](#).

5.2 ATEX/IECEx hazardous location approval

5.2.1 General

Concerning explosive atmospheres, according to version in user hands, the marking of CMWA 6100-EX is:

 II 2G Ex ib IIB T4 Gb,

this version is useable in gas explosive atmosphere of group IIB and temperature class T4 in an ambient temperature from -40°C to +85°C,

Or

 II 2G Ex ib IIC T4 Gb,

this version is useable in gas explosive atmosphere of group IIC and temperature class T4 in an ambient temperature from -40°C to +85°C.

Those two versions of CMWA 6100-EX are category two and can be used in areas 1 and 2.

The respect of essential safety requirements defined in the 2014/34/UE directive from the 26th of February 2014, is obtained, for both versions, by the apparatus conformity to standards:

- EN IEC 60079-0:2018, IEC 60079-0:2017
- EN 60079-11:2012, IEC 60079-11:2011

5.2.2 Specific conditions of use (“X”)

CMWA 6100-EX operational temperature range is from -40°C to +85°C.

5.3 EX Sensor installation

If CMWA 6100-EX or associated mounting accessory is installed by using glue, check if the glue is suitable for use in an explosive atmosphere. The glue should not electrically insulate the CMWA 6100-EX from the monitored machine.

5.4 EX Sensor maintenance

As electronic boards and the battery of CMWA 6100-EX are protected by resin, it is not possible to access the electronic components to perform maintenance operations or replace the battery.

5.5 EX Sensor repair

CMWA 6100-EX is a non-reparable wireless sensor. Therefore, at product end of life, it shall be recycled by appropriate means.

5.6 EX Sensor caution

If cracks are detected on the plastic cover of the CMWA 6100-EX, the sensor needs to be replaced.

Commissioning, decommissioning, or any other operations which require the use of the NFC connection are forbidden inside an explosive atmosphere. Commissioning and decommissioning operations must be done outside an explosive atmosphere, before/after physical assembly/disassembly of the sensor on/from the monitored machine.

As soon as any failure or incorrect working is detected on a CMWA 6100-EX, it has to be removed from the hazardous area.

6 CMWA 6600-EX Gateway

6.1 Contact

SKF Development Centre Sensors
204 bd Charles de Gaulle
37540 Saint Cyr sur Loire
France

The SKF Development Centre Sensors can be contacted through the SKF's [Technical Support Group TSG](#).

6.2 Introduction

The IMx-1 system allows for use in hazardous area environments where the CMWA 6100 sensor is allowed for use in zone 1 environments without special operation conditions based upon using intrinsic safety as protection method.

For the gateway, the CMWA 6600-EX assembly variant is approved for use in zone 2 hazardous area environment, using increased safety as protection method. The CMWA 6600-EX uses a hazardous area approved enclosure as a rugged



The CMWA 6600 Gateway is not allowed for use in hazardous area environments. The standard gateway product is allowed for safe area use only!

IP66/Type 4X enclosure for the gateway electronics. This industrial glass fibre reinforced polyester enclosure replaces the standard gateway IP65 enclosure. The electronics are installed using a metal mounting bracket with a plastic protective cover, including the status LEDs.

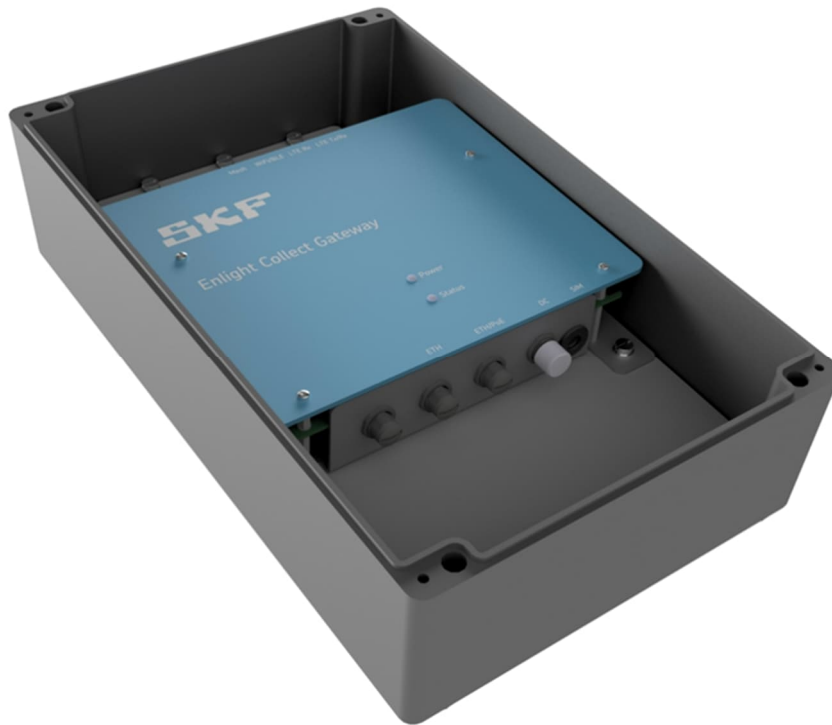


Figure 63 CMWA 6600-EX Enclosure Assembly variant

Note: In normal operation the enclosure cover does not allow visual access to the gateway status LEDs. For status monitoring, use the IMx-1 App and/or the @ptitude Observer software.

The polyester base enclosure does not use typical carbon loading and allows equal internal antenna performance as the standard CMWA 6600 Gateway. From an installation perspective, the use of internal antennas is recommended. However, the use of external or potentially integral (inside the enclosure) antennas is supported and will be required for use of the Mobile connectivity option.

Important warnings:



Static hazard! Use **only** a damp cloth to clean the gateway.



The CMWA 6600-EX Gateway enclosure does not allow for installation of AC/DC power supply module.

Standard delivery of the CMWA 6600-EX Gateway is enclosure assembly **with no provisions for enclosure cable entry**.

Given various regulations for hazardous area installation in distinct regions/countries and possible different gateway use cases (Ethernet/PoE, Power, Power and Ethernet and various possible external antenna configurations depending on active radio connections), it is more flexible that the EX gateway enclosure can be fully adapted to the end-user application.

Note: The polyester enclosure allows for easy mechanical processing and cable entry is allowed on all sides of the enclosure.

In addition, the hazardous area certification for the CMWA 6600-EX variant is also based upon this principle of not providing the cable entry accessories (cable glands). Please refer to the following section for installation requirements.

CMWA 6600-EX Gateway variant uses the M12 connectors for power and ethernet connections. However, based on the above restriction on cable entry provisions, standard 5m cable assemblies for ethernet and/or power connectivity are provided. These cable assemblies have M12 connector on one side and flying leads on other side. This allows installation wiring to be terminated with proper interface connectors inside the CMWA 6600-EX enclosure. Furthermore, standard delivery will provide Ethernet RJ45 connector for termination of the Ethernet communication cable.

SIM card access is covered by a rubber grommet on the front side of the input connector panel left from the input power connector.

The CMWA 6600-EX Gateway does not require/provide support for safety ground connection.

The layout of the mounting plate and positioning of the gateway electronics allow for custom installation of additional cable clamping if required for the application.

6.3 ATEX/IECEEx hazardous location approval

6.3.1 General

The following information applies for European Zone 2 certification (indicated by equipment bearing the Ex or IECEx marking).

This equipment is intended for use in potentially explosive atmospheres as defined by European Union **Directive 2014/34/EU** and has been found to comply with the Essential Health and Safety Requirements relating to the design and construction of Category 3 equipment intended for use in potentially explosive atmospheres, given in Annex II to this Directive.

Compliance with the Essential Health and Safety requirements has been assured by compliance with **IEC 60079-0** and **IEC 60079-7**.

Warning: Explosion hazard!



Do not disconnect or replace the equipment unless power has been removed or the area is known to be non-hazardous.



The CMWA 6600-EX Gateway shall be used within its specified ratings as defined by SKF and shall only be used for fixed installations in a pollution degree 2 environment.



Provisions shall be made to prevent the rated voltage from being exceeded by transient disturbances of more than 40% when applied in Zone 2 environments.



Secure any external connections that mate to this equipment by using screws, sliding latches, threaded connectors, or other means provided with this product.



This equipment must be used only with ATEX/IECEx certified components. Ensure that cable entries have proper Ex-e approval, minimum IP54 rating and operating temperature specifications.

6.3.2 Specific conditions of use (“X”)

The following specific conditions of use apply for the CMWA 6600-EX Gateway:

- CMWA 6600-EX gateway ambient temperature range is from -20°C to +60°C
- CMWA 6600-EX gateway shall only be used in fixed installation
- CMWA 6600-EX gateway shall only be used in an area of at least pollution degree 2, as defined in IEC 60664-1
- Transient protection shall be provided that is set at a level not exceeding 140% of the peak rated voltage value at the supply terminals to the equipment
- There are potential electrostatic charge and discharge hazards on the equipment, the user shall touch equipment with an insulating object and clean with damp cloth only
- Suitably certified cable gland shall be used for cable entries. Unused cable entries shall be fitted with appropriately Ex-e certified and approved stopping plug which ensure appropriate IP rating (minimum IP54)

6.4 EX Gateway cable entry and installation

The CMWA 6600-EX Gateway enclosure assembly variant is delivered and certified without preparations for cable entries.

It is therefore the responsibility of the end-user to ensure that the cable entry system and field wiring are in accordance with the applicable code of practice and carried out by suitably trained personnel.

Example:

For ATEX/IECEx certification certified EX-e cable glands will be required for installation with a minimum IP54 rating.

Note: CMWA 6600-EX Enclosure supports IP66

A possible cable gland selection can be Stahl series 8161/7.

This black, long thread cable gland with a reduction ring allows a cable diameter of 1 to 6 mm with a reduction ring with M12×1.5 mm thread size.

This single selection could allow for support of all expected cable types, but with chosen approval principle, the end-user/installer has a flexible choice.

For North American installations, conduit systems may be used with sealing type cable/conduit enclosure connectors.

For Ethernet/Power cable entry, bottom access is preferred. The selected enclosure has a bottom side cable entry envelope of 170×84 mm. Enclosure wall thickness is 6mm. Hence, cable glands with wall threading can be used or as used in the example, long thread cable glands can be used with nut mounting.

Note: As where CMWA 6600-EX internal antenna performance is equal to the performance of the safe area CMWA 6600 Gateway for the Miramesh sensor radio, WiFi and Bluetooth BLE, the internal antennas for Mobile connectivity are not available. However, due to larger size of the EX-enclosure it is feasible to use integral antennas for Main and Diversity antennas inside the enclosure, and as such, avoid need for cable entry.

Once the cable entry strategy is determined, the glass fibre reinforced polyester enclosure allows straightforward mechanical rework.

The following requirements apply for on-site addition of cable entries:

1. Entries may be clearance or threaded.
2. Clearance entries may only be provided when the thread length of the entry device is at least 10 mm.
3. Clearance entries shall be 0.5 mm larger in diameter than the nominal diameter of the thread on the cable entry device.
4. The drill used to create the hole (either clearance size or tapping size) must be sharp to prevent hole delamination or 'punch through'.
5. Drill speed and feed rate vary with drill sharpness and hole size. This is best learned by experience. As a guide, the most common values are:
DRILL SPEED 500 rpm with FEED RATE 4.5 revs per mm.

6. There is no need to drill a pilot hole in GRP material.
7. When the entry is to be threaded the tap must be sharp to avoid damage to the thread and the box wall.

Note: Before mechanical preparation of the CMWA 6600-EX enclosure, loosen the 6ea M6 screws to remove the mounting plate, including the electronics, to avoid potential damage to electronics and connectors.

Mating connectors for ethernet and power cable termination allow running the required cables directly into the CMWA 6600-EX Gateway without the need for further (EX) terminal boxes.

Cable entry specification:

Bottom enclosure entry (Power and Ethernet connections)

- Cable gland: Suitable type Ex-e cable gland providing minimum IP54 protection
- Maximum cable entries: 5ea
- Maximum cable gland size: M20
- Minimum cable gland clearance (centre to centre): 40mm

Top/Side enclosure entry (Power and Ethernet connections)

- Cable gland: Suitable type Ex-e cable gland providing minimum IP54 protection
- Maximum cable entries: 4ea
- Maximum cable gland size: M16
- Minimum cable gland clearance (centre to centre): 32mm

Cable Assembly

Standard delivery provides pre-assembled 5m cables for power and Ethernet with M12 connector and flying leads termination. This allows for use of approved cable glands and flexibility in connecting the Gateway to power distribution and ethernet switch/router with respect to cable length adjustment. A separate RJ45 connector is provided to allow termination of the Ethernet cable.



Figure 64 CMWA 6600-EX Cable / Connector Accessories

- **Power Cable** – Phoenix Contact – SAC-4P-5,0-PUR/M12FS – 1668124
- **Ethernet Cable** – Phoenix Contact – NBC-M12MSX/5,0-94F – 1407469
- **RJ45 Connector** – Phoenix Contact – VS-08-RJ45-5-Q/IP20 – 1656725

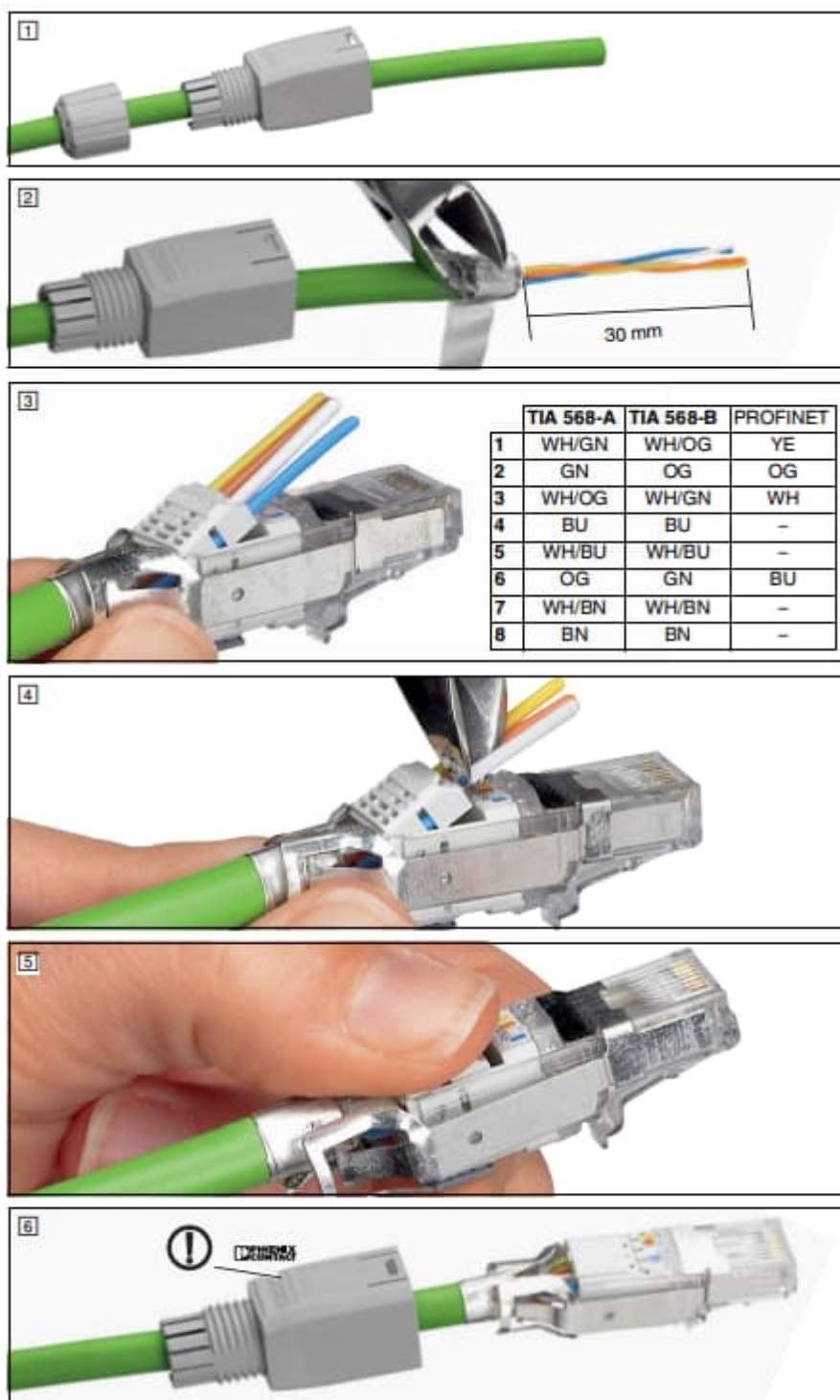


Figure 65 Ethernet RJ45 Assembly

Note: Colour coding TIA 568-B will apply for the M12 connector termination.

Alternate option for gateway installation is the use of separate wiring and making use of M12 connector termination inside the EX gateway enclosure.

Below overview of connectors, which need to be separately sources as these options are not provided by SKF, can be used for custom gateway installations:

Power Connector

Phoenix Contact – SACC-M12FS-4CON-PG7-VA – 1553242 Connector, universal, 4 position, socket straight M12, screw connection, external cable diameter 4 – 6 mm.

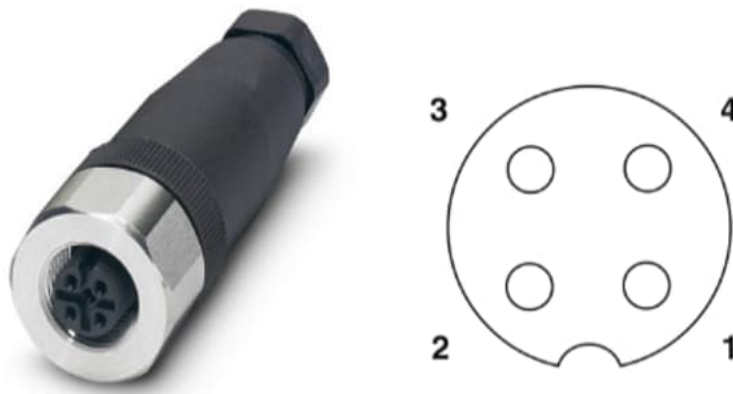


Figure 66 Power connector – Phoenix contact

This connector allows the cable to be terminated using screw connections. Alternate types are available, allowing support for different cable diameters.

Ethernet connector – Phoenix Contact – VS-08-M12MS-10G-SCO – 1417430

Data connector, Ethernet CAT6A, 8 positions, shielded, plug straight M12 speedcon, external cable diameter 4 – 8 mm.

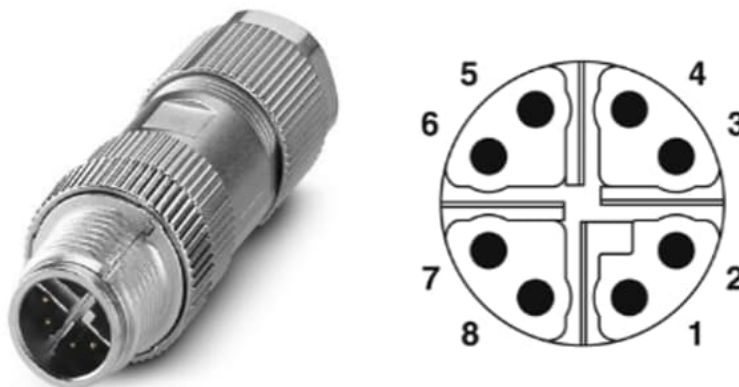


Figure 67 Ethernet connector – Phoenix contact

This connector makes use of insulation displacement connectivity, allowing network connection installation quickly and flexible on-site (demo video).

6.5 EX Gateway mounting

The SKF Enlight Collect EX Gateway has overall dimensions of:

- 400 mm high
- 250 mm wide
- 120 mm deep

The enclosure provides for a 4-point mounting and has four 7 mm, clearance for M6 and holes on a 200 mm by 380 mm pitch.

To mount the EX Gateway, you must unscrew the 4ea captive Phillips screws to remove the enclosure cover.

Important safety warning:



*Always utilise all provided fixing points to secure it to the mounting surface, using fasteners appropriate for that material.
Ensure to properly re-install the enclosure cover to ensure the IP66 enclosure rating.*

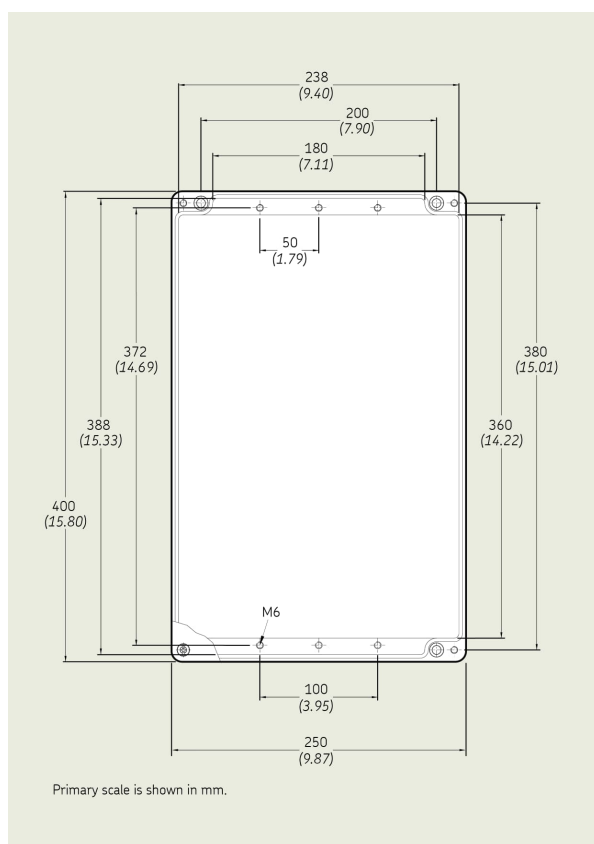


Figure 68 EX Gateway enclosure dimensions

7 SKF Enlight Collect IMx-1 System specifications

7.1 Enlight Collect Wireless Sensor specifications

7.1.1 Environmental and physical

Table 4 Wireless sensor environmental specifications



Model designation	CMWA 6100 and CMWA 6100-EX	
Mounting	¼–28 UNF female, recommended torque 2.9 Nm (2.14 lb-ft)	
Spanner/wrench	1–1/4 inch AF: Across Flats, 31.75 mm	
Material	Thermoplastic housing	
	304L or 303 stainless steel base	
Diameter (maximum at base)	33.66 mm (1.33 inch)	
Height	78.2 mm (3.08 inch)	
Weight	142 g (5 oz)	
Operating	-40 to +85 °C (-40 to +185 °F)	
Storage	Recommended maximum temperature: 30 °C (86 °F) To avoid excessive self-discharge of the battery, do not store at high temperatures (30 °C or above) for extended periods.	
Altitude	Maximum 5 000 m (16,404 ft.)	
Humidity	Maximum 95% relative non-condensing	
Conditions of use	Indoor or outdoor	
Pollution degree	4	
IP rating	IP69K according to ISO 20653:2013	
Mechanical impact rating	According to IEC 60068-2-31, free fall procedure 1	
Flammability	UL 94 V-0	
Hazardous area rating	To be used in safe area only	See chapter 5

7.1.2 Operational states and battery

Table 5 Wireless sensor operational states and battery specifications

Model designation	CMWA 6100 and CMWA 6100-EX
Type	Non-replaceable lithium thionyl battery
Typical lifetime	4 years, configuration dependent
Modes	WPAN IEEE 802.15.1, Mesh and Flight modes
Mode switch	By Bluetooth/NFC from app or a timeout
	Decommissioning by app: Bluetooth is used to place the sensor in flight mode

Notes:

Typical battery lifetime is based on all four overall measurements being collected four times per day, with time waveforms transmitted once per week. Lifetime range reflects that actual lifetime is dependent on application/environmental temperature.

Wireless environment and battery life are linked: having more data to upload affects mesh performance and physical obstacles to the wireless network can increase transmission times and create heavily loaded nodes. Sensors used as measurement only leaf nodes have a longer expected lifetime than mesh nodes that both perform measurements and contribute to the sensor mesh.

7.1.3 Measurements

Table 6 Wireless sensor measurement specifications

Model designation	CMWA 6100 and CMWA 6100-EX
Enveloping	Band 3
Acceleration	Yes
Dynamic range	50 g peak
Velocity	Yes
Dynamic range	100 mm/s (3.94 in/s) RMS
Temperature	Yes
Measurement range	-40 to +85 °C (-40 to +185 °F)
Resolution	1 °C (1.8 °F)
Accuracy	±3 °C (±5.4 °F)
Maximum and minimum temperatures	Stored by the sensor

Note:

The velocity dynamic range is only achievable if within overall sensor acceleration dynamic range.

7.1.4 Signal processing

Table 7 Wireless sensor signal processing specifications

Model designation	CMWA 6100 and CMWA 6100-EX
Envelope 3	0 to 1 kHz
Source	0.5 to 10 kHz
'E3' measurement	True pk-pk
Acceleration	10 Hz to 10 kHz
'A' measurement	True pk-pk
Velocity	10 to 1000 Hz
'V' measurement	RMS
All vibration	TWF:1 each A, V, Env.
TWF samples	Up to 16 384 (currently 400, 800 or 1600-line FFT in @ptitude Observer)
Temperature	Latest and 256 last saved values
Alarm thresholds	Configurable Alert & Danger
Sources	All overall measurements
Measurement alarm thresholds Vibration	0 to greater than IMx-1 dynamic range
Temperature (maximum configurable range)	-49 to 205 °C (-56.2 to +401 °F)
Self-diagnostics	Yes

7.1.5 Interfaces

Table 8 Wireless sensor interface specifications

Model designation	CMWA 6100 and CMWA 6100-EX
WPAN IEEE 802.15.1	Yes
Range	3 m (10 ft) typical
Proximity IEC 14443	Yes
Range	< 20 cm
Mesh network	Yes
Maximum range	10 to 20 m (33 to 66 ft) typical node–node in an industrial environment
Interface to gateway	Mesh network as above
Interface to app	Proximity and WPAN (In app this uses NFC and Bluetooth)
OTA FW update	Yes

Notes: WPAN IEEE 802.15.1: Bluetooth SIG certification is pending.
 OTA: Over The Air device firmware updates.

7.1.6 CMWA 6100 certifications

Europe

- Radio Equipment Directive (RED) and CE certified (radio, EMC and product safety)
 - o Radio testing according to:
 - EN 300328 for IEEE 802.15.1 Sensor radio
 - EN 300328 for Bluetooth Low Energy
 - EN 300330 for NFC
 - EN 62479
 - EN 62369-1 and 50364
 - o EMC testing according to:
 - EN 301489-1
 - EN 301489-3
 - EN 301489-17
 - 61000-6-4
 - 61000-4.3
 - 61000-4.2
 - o Safety requirements according to EN 61010-1

North America

- FCC/ISED certification
 - o Radio testing according to:
 - FCC 15.247 for IEEE 802.15.1 Sensor radio
 - FCC 15.247 for Bluetooth Low Energy
 - FCC 15.207 for NFC
 - FCC/ISED correlation
 - o EMC testing according to:
 - FCC Part 15 Subpart B

FCC compliance statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide a reasonable protection against harmful interference in an industrial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with FCC RF radiation exposure limits set forth for general population (uncontrolled exposure). This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.

ISED - Canada regulatory statement (English)

This equipment contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license exempt RSS(s). Operation is subject to the following two conditions:

1. This equipment may not cause interference
2. This equipment must accept any interference, including interference that may cause undesired operation of the device.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

ISED - Canada regulatory statement (French)

L'émetteur/récepteur exempt de licence contenu dans le présent équipement est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

1. L'équipement ne doit pas produire de brouillage.
2. L'équipement doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'un compromettre le fonctionnement.

Cet équipement est conforme aux limites d'exposition de rayonnement d'IC RSS-102 déterminées pour un environnement non contrôlé. Cet équipement devrait être installé et actionné avec la distance minimum 20 cm entre le radiateur et votre corps.

Central/South America

- Anatel certification, Brazil.

*Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados.
Para maiores informações, consulte o site da ANATEL – www.anatel.gov.br*

Bluetooth: The Bluetooth SIG certification is pending.

Japan



Giteki certification R 003-210247

Korea

- KCC Certification, South Korea
- R-R-S2F-CMWA_6100



상호 : 에스케이에프코리아부산지점

기자재 명칭 : Sensor

모델명: CMWA 6100

제조년월: 2020 년 1 월

제조자 및 제조국가 : SKF Sverige AB
/스웨덴

R-R-S2F-CMWA_6100

7.1.7 CMWA 6100-EX certifications

Europe

- Radio Equipment Directive (RED) and CE certified (radio, EMC and product safety)
 - o Radio testing according to:
 - EN 300328 for IEEE 802.15.1 Sensor radio
 - EN 300328 for Bluetooth Low Energy
 - EN 300330 for NFC
 - EN 62479
 - EN 62369-1 and 50364
 - o EMC testing according to:
 - EN 301489-1
 - EN 301489-3
 - EN 301489-17
 - 61000-6-4
 - 61000-4.3
 - 61000-4.2
 - o Safety requirements according to EN 61010-1

European Certification ATEX

EN IEC 60079-0:2018

EN 60079-11:2012

ATEX certificate number: INERIS 22ATEX0007X

International Certification, IECEx

IEC 60079-0:2017

IEC 60079-11:2011

Certificate of Compliance number: INE 22.0011X

North America

- FCC/ISED certification
 - o Radio testing according to:
 - FCC 15.247 for IEEE 802.15.1 Sensor radio
 - FCC 15.247 for Bluetooth Low Energy
 - FCC 15.207 for NFC
 - FCC/ISED correlation
 - o EMC testing according to:
 - FCC Part 15 Subpart B

FCC compliance statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide a reasonable protection against harmful interference in an industrial installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna
- Increase the separation between the equipment and receiver
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected
- Consult the dealer or an experienced radio/TV technician for help

This device complies with FCC RF radiation exposure limits set forth for general population (uncontrolled exposure). This device must be installed to provide a separation distance of at least 20 cm from all persons and must not be collocated or operating in conjunction with any other antenna or transmitter.

ISED - Canada regulatory statement (English)

This equipment contains licence-exempt transmitter(s)/receiver(s) that comply with Innovation, Science and Economic Development Canada's license exempt RSS(s). Operation is subject to the following two conditions:

1. This equipment may not cause interference
2. This equipment must accept any interference, including interference that may cause undesired operation of the device.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

ISED - Canada regulatory statement (French)

L'émetteur/récepteur exempt de licence contenu dans le présent équipement est conforme aux CNR d'Innovation, Sciences et Développement économique Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes :

3. L'équipement ne doit pas produire de brouillage.
4. L'équipement doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'un compromettre le fonctionnement.

Cet équipement est conforme aux limites d'exposition de rayonnement d'IC RSS-102 déterminées pour un environnement non contrôlé. Cet équipement devrait être installé et actionné avec la distance minimum 20 cm entre le radiateur et votre corps.

Central/South America

- Anatel certification, Brazil.

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. Para maiores informações, consulte o site da ANATEL – www.anatel.gov.br

7.2 Enlight Collect Gateway specifications

7.2.1 CMWA 6600 – Environmental and physical

Table 9 Gateway environmental specifications



Housing material	ASA+PC-FR Flame Retardant Acrylonitrile Styrene Acrylate + Polycarbonate
Flammability	UL 94 V-0
Dimensions	220 x 220 x 50.5 mm (8.66 x 8.66 x 1.99 in.)
Mounting	4-point
Weight	1.2 kg
IP rating	IP65
User connections	Four connectors: refer Figure 2
Operating	-20 to +60 °C (-4 to +140 °F)
Storage	-40 to +60 °C (-40 to +140 °F)
Humidity	Maximum 95% relative non-condensing
Altitude	Maximum 5 000 m (16,404 ft.)
Hazardous area rating	Safe area use only

7.2.2 CMWA 6600-EX – Environmental and physical

Table 10 Gateway power specifications



Housing material	Glass Fibre Reinforced Poylester
Flammability	UL 94 V-0
Dimensions	400 × 250 × 120 mm (15.75 × 9.84 × 4.72 in.)
Mounting	4-point
Weight	4 kg
IP rating	IP66
User connections	Four connectors: refer Figure 2
Operating	-20 to +60 °C (-4 to +140 °F)
Storage	-40 to +60 °C (-40 to +140 °F)
Humidity	Maximum 95% relative non-condensing
Altitude	Maximum 5 000 m (16,404 ft.)
Hazardous area rating	ATEX zone 2 - II 3 G Ex ec IIC T4 Gc IECEX Zone 2 – Ex ec IIC T4 Gc

7.2.3 Power

Table 11 Gateway power specifications

Parameter	CMWA 6600 and CMWA 6600-EX
Powering options	Industrial range 24 V DC or PoE
24V input voltage range	9 to 36 V DC
Power over Ethernet	IEEE 802.3af: nominal voltage 48 V, 13 W maximum PoE is available at the Ethernet 1 connection
Power consumption	7.5 W maximum
Other protection	Reversed supply, transient voltage protection
Redundancy	No, unless external provision is made

Notes:

The gateway circuitry is isolated from the supply connections.

7.2.4 Internal measurement capabilities

Table 12 Gateway Internal measurement capabilities

Parameter	CMWA 6600 and CMWA 6600-EX
Status	Self-monitoring, network and sensor/mesh status monitoring Supports @ptitude Observer event log
Temperature	Gateway internal
Range	Greater than gateway operating range
Other	Including: watchdog, supply voltage monitoring

Notes:

In addition to dynamic status information, static or rarely changing information such as sensor hardware and firmware revisions and ID are also available. Errors and change in status are generally available in the @ptitude Observer event log.

7.2.5 Interfaces

Table 13 Gateway interface specifications

Parameter	CMWA 6600 and CMWA 6600-EX
Sensor	Sensor wireless mesh, 2.4 GHz ISM
OTA FW update	Yes, to all sensors associated with the gateway
App interface	WPAN IEEE 802.15.1 (Bluetooth Low Energy 4.2)
Network interface options	Ethernet or Wi-Fi DHCP or fixed IP address
Ethernet (wired)	10/100/1000 Mbps auto negotiation and auto MDI-X For the Ethernet 1 connector location refer Figure 2 .
Wi-Fi	802.11a/b/g/n/ac 2.4 and 5 GHz (5 GHz recommended, see also note) WPA2-Personal (with AES encryption) or WPA2-Enterprise
Mobile	External antenna support only (integral antenna possible for CMWA 6600-EX) 3G/UMTS – bands 1, 2, 4, 5, 8, 9 and 19 4G/LTE – bands 1, 2, 3, 4, 5, 7, 8, 12 (17), 18, 19, 20 and 28 Automatic 4G/3G fallback
Time synchronisation	NTP for synchronisation of the internal real time clock Two configurable NTP server IP addresses

Parameter	CMWA 6600 and CMWA 6600-EX
	Absolute accuracy of time stamped data: ± 1 s
	App sets gateway clock at commissioning
	Manual synchronisation is possible in @ptitude Observer
Data buffering	More than 1-week of data. Storage: non-volatile, FIFO

Notes: If 2.4 GHz Wi-Fi must be used, use only with a 20 MHz (not 40 MHz) bandwidth
OTA: Over-the-air device firmware updates

7.2.6 CMWA 6600 certifications

Note: most of below radio certifications apply for both CMWA 6600 and CMWA 6600-EX gateway variant. In case of deviations these are explicitly referenced.

Europe

- Radio Equipment Directive (RED) and CE certified (radio, EMC and product safety)
 - o Radio testing according to:
 - ETSI EN 300 328 - V2.2.2 - 2019
 - ETSI EN 301 893 - V2.1.1 - 2017
 - ETSI EN 301 908-1 - V13.1.1 - 2019
 - o EMC testing according to:
 - ETSI EN 301 489-1 - V2.2.3 – 2019
 - ETSI EN 301 489-17 - V3.2.4 - 2020
 - ETSI EN 301 489-52 - V1.1.2 - 2020
 - o Electrical Safety testing according to:
 - EN 62311:2008
 - IEC 62368-1:2018 (Edition 3.0)
 - EN IEC 62368-1:2020 + A11:2020

The CMWA6600 Enlight Collect Gateway is defined as class-2 radio equipment.

This multi-radio device enables operation in the following frequency bands:

- Mesh Sensor radio, ISM band 2400 – 2483.5 MHz
- Bluetooth BLE, ISM band 2400 – 2483.5 MHz
- WLAN, ISM band 2400 – 2483.5 MHz
- WLAN, U-NII bands 5150 – 5350 MHz, 5470 – 5725 MHz (excluding 5600 – 5650 MHz) and 5725 – 5825 MHz

Following restrictions apply when operating Wi-Fi in fixed client mode at different bands within the European countries:

Band	Channel	Frequency [MHz]	Indoor use allowed	Outdoor use allowed	Max EIRP
ISM	1 - 11	2412 - 2462	Yes	Yes	100 mW / 20 dBm
U-NII 1	36 - 48	5180 - 5240	Yes	No	200 mW / 23 dBm
U-NII 2	52 - 64	5260 - 5320	Yes	No	200 mW / 23 dBm
U-NII-2e	100 - 140	5500 - 5700	Yes	Yes	1 W / 30 dBm
U-NII 3	149 - 165	5750 - 5825	Yes	Yes	25 mW / 14 dBm

Country warnings:										
	AT	BE	BG	CH	CY	CZ	DE	DK	EE	EL
	ES	FI	FR	HR	HU	IE	IS	IT	LI	LT
	LU	LV	MT	NL	NO	PL	PT	RO	RS	SE
	SI	SK	TR	UK						

CAUTION:

IEEE 802.11.x wireless LAN with 5.15 to 5.35 GHz frequency band is restricted to indoor use in all countries included in the above matrix. Using this WLAN application outdoors may lead to interference issues with existing radio services.

North America

- FCC/ISED certification
 - o Support for Miramesh, WiFi/BLE (internal and external antenna support) and Mobile radio (external antenna support only)
 - o EMC testing according to:
 - FCC Part 15B/ICES003 Unintentional Radiator portion
 - o Radio testing according to:
 - FCC 15.247 / RSS247
 - Simultaneous-transmission measurement
 - FCC/ISED correlation
 - o FCC ID: 2AVQ-CMWA6600
 - o ISED IC: 258940CMWA6600

FCC - USA compliance statement

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. This device may not cause harmful interference, and
2. This device must accept any interference received, including interference that may cause undesired operation.

Non-authorized modification could void authority to use this equipment.

The internal / external antenna(s) used for this module must provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

This equipment has been tested and found to comply with the limits for a Class A 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 the instruction manual, 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 own expense.

ISED - Canada regulatory statement (English)

This Class A digital apparatus complies with Canadian ICES-003 and RSS-247. Operation is subject to the following two conditions:

1. this device may not cause interference, and
2. this device must accept any interference, including interference that may cause undesired operation of the device.

Operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

Operation in the 5600-5650 MHz band is not allowed in Canada. High-power radars are allocated as primary users (i.e. priority users) of the bands 5250-5350 MHz and 5650-5850 MHz and that these radars could cause interference and/or damage to LE-LAN devices.

This equipment complies with IC RSS-102 radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20 cm between the radiator and your body.

ISED - Canada regulatory statement (French)

Cet appareil numérique de classe A est conforme aux normes canadiennes ICES-003 et RSS-247. Son fonctionnement est soumis aux deux conditions suivantes:

1. l'appareil ne doit pas produire de brouillage, et
2. l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

Le dispositif de fonctionnement dans la bande 5150-5250 MHz est réservé à une utilisation en intérieur pour réduire le risque d'interférences nuisibles à la co-canal systèmes mobiles par satellite

Opération dans la bande 5600-5650 MHz n'est pas autorisée au Canada. Haute puissance radars sont désignés comme utilisateurs principaux (c.-à-d. utilisateurs prioritaires) des bandes 5250-5350 MHz et 5650-5850 MHz et que ces radars pourraient causer des interférences et/ou des dommages à dispositifs LAN-EL.

Cet équipement est conforme aux limites d'exposition de rayonnement d'IC RSS-102 déterminées pour un environnement non contrôlé. Cet équipement devrait être installé et actionné avec la distance minimum 20 cm entre le radiateur et votre corps.

FCC/ISED External Antenna Restrictions

Following restrictions apply, with respect to general requirements but with exception of the CMWA6600 certified specified reference antenna, for North American FCC/ISED external antenna selections:

- **WiFi/BLE** - Following approved external antennas are approved for use with WiFi/BLE (2.4/5GHz dual band):
 - o Linx - ANT-DB1-RAF-RPS
 - o Taoglas - GW.40.2153
 - o Taoglas - GW.59.3153
 - o Walsin - RFDPA870900 SBLB8G1
 - o Delock – 88395

Note: These antennas may also be used for Miramesh but will not be suitable for Mobile purposes.

- **Mobile** - Following maximum antenna gain limitations apply for both FCC/ISED:
 - o Mobile 3G/UMTS:

▪ Band 2	8.01 dBi
▪ Band 4	5.00 dBi
▪ Band 5	6.11 dBi
 - o Mobile 4G/LTE:

▪ Band 2	8.01 dBi
▪ Band 4	5.00 dBi
▪ Band 5	6.11 dBi
▪ Band 7	8.01 dBi
▪ Band 12	5.61 dBi
▪ Band 18	6.07 dBi
▪ Band 19	6.11 dBi

Central/South America

- Support for Miramesh, WiFi/BLE (internal and external antenna support)
- Mobile support – certification pending
- Anatel certification, Brazil.
- UL-BR 20.0864

Este equipamento não tem direito à proteção contra interferência prejudicial e não pode causar interferência em sistemas devidamente autorizados. Para maiores informações, consulte o site da ANATEL – www.anatel.gov.br

Bluetooth

Bluetooth SIG Qualified:

Declaration ID: D055000 - CMWA 6600 / CMWA 6600-EX

QDID(s):

87047 - Controller Subsystem

165284 - Host Subsystem.

Japan

- Support for Miramesh, WiFi/BLE (internal and external antenna support)
- Mobile **not** supported – when mobile connectivity is required, the use of an external ethernet-mobile bridge/router is recommended



Giteki certification:

R 003-210248

R 207-16-EMMY

Note: The CMWA 6600-EX gateway is not Giteki certified. Despite valid radio certification the CMWA 6600-EX gateway is not hazard area certified for use in Japan.

Korea

- KCC Certification, South Korea
- Support for Miramesh, WiFi/BLE (internal and external antenna support)
- Mobile support – certification pending
- R-R-S2F-CMWA_6600



상호: 에스케이에프코리아부산지점

기자재 명칭: Gateway

모델명: CMWA 6600

제조년월: YYYY 년 MM 월

제조사 및 제조국가: SKF Sverige AB

AG/독일

R-R-S2F-CMWA_6600

Note: The CMWA 6600-EX gateway is not EAC certified.

7.2.7 CMWA 6600-EX certifications

Following additional certifications apply for CMWA 6600-EX in addition to standard certifications of standard gateway product variant.

Note: refer to standard CMWA 6600 Gateway certification section for deviations of specific country certifications!

Europe

- Radio Equipment Directive (RED) and CE certified (radio, EMC and product safety)
 - o Radio testing according to:
 - ETSI EN 300 328 - V2.2.2 - 2019
 - ETSI EN 301 893 - V2.1.1 - 2017
 - ETSI EN 301 908-1 - V13.1.1 - 2019
 - o EMC testing according to:
 - ETSI EN 301 489-1 - V2.2.3 – 2019
 - ETSI EN 301 489-17 - V3.2.4 - 2020
 - ETSI EN 301 489-52 - V1.1.2 - 2020
 - o Electrical Safety testing according to:
 - EN 62311:2008
 - IEC 62368-1:2018 (Edition 3.0)
 - EN IEC 62368-1:2020 + A11:2020
 - o ATEX Hazardous Area testing according to:
 - EN IEC 60079-0:2018
 - EN IEC 60079-7:2015+A1:2018

European Certification ATEX

EN IEC 60079-0:2018

EN IEC 60079-7:2015+A1:2018

ATEX certificate number: CSANe 22ATEX1073X

International Certification, IECEx

IEC 60079-0:2017 Ed. 7

IEC 60079-7:2017 Ed 5.1

Certificate of Compliance number: IECEx CSAE 22.0051X

UKCA Certification, UKEX

EN IEC 60079-0:2018

EN IEC 60079-7:2015+A1:2018

UKEX certificate number: CSAE 22UKEX1204X

7.3 Product marks and labelling

7.3.1 Marks

Marks are symbols or logos that may be found on the product, its labelling and/or packaging. Note that the inclusion of a mark in the table below does not indicate that the product has attained this certification.

Table 14 Explanation of marks

Mark	Meaning
	CE marking according to CE 2014-53-UE
	Certification: FCC
	Certification: KCC (Korea)
	Certification: Bluetooth SIG
	Certification: ATEX
	Certification: Anatel
	WEEE : Waste Electrical and Electronic Equipment Directive (2012/19/EU)
	Certification: GITEKI (Japan)
	Certification: UK Conformity Assessed (UKCA)

7.3.2 Sensor



Figure 69 Sensor labelling

Note: The SKF product marking may differ. The information above should only be used as a reference in terms of where the marking can be found on the product.

7.3.3 Date code

The Number is unique and is defined as followed: DDDY NNNN

- **DDD** The number of the day of production
- **Y** A letter representing the year of production according to SKF letter year
- **NNNN** The number of the part produced this day
SKF production letter / Date

SKF production letter / Date

R	S	T	U	W	X	Y	Z	A	B	D	E	F
2019	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029	2030	2031



Figure 70 Date Code - example

7.3.4 Gateway

On the front face of the case a manufacturing data label, confirms product and company information, CE marking, WEEE marking and RoHS compliance. The QR code contains the product information shown alongside it. Note the QR code can be used to identify the gateway during commissioning.

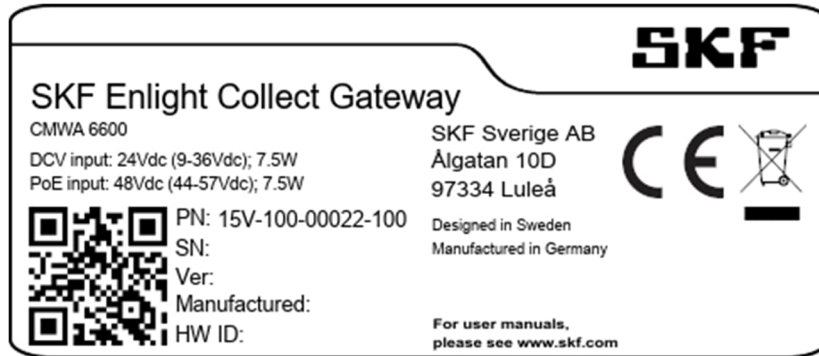


Figure 71 Gateway labelling example

A second label provides the additional radio equipment approval information and warnings that are required to comply with those approvals.

A combined product and certification label is used for CMWA 6600-EX gateway

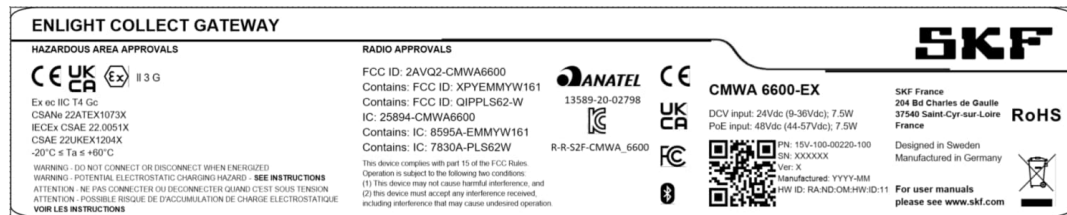


Figure 72 CMWA 6600-EX Gateway labelling example

7.4 Quality control

SKF Sverige AB, Luleå is ISO 9001:2015 certified.

8 Electrical waste



Electrical waste and electrical equipment should be recycled as specified by the WEEE-directive and not be placed in the general refuse. Product should be sent to an approved recycling centre for safe recycling, recovery, reuse or returned to SKF for proper recycling.

SKF France
204 Bd Charles de Gaulle
37540 Saint-Cyr-sur-Loire
France

Appendix A Limited Warranty

SKF – Limited Warranty

Download the latest version from
[skf.com](https://www.skf.com).