SKF Enlight Collect IMx-1 System

User Manual
P/N Part Number **15V-090-00087-100**
Revision **C - June 2020 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.

SKF Sverige AB
Aurorum 30, 977 75 Luleå, Sweden
Telephone: +46 (0) 31 337 10 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.

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.

Technical Support – SKF's Technical Support Group can be reached during normal business hours via phone, e-mail and live chat. Always check the self-service web portal before contacting your nearest Technical Support Group (TSG) to see if the answer is already published. You may search the vast knowledgebase within the self-service web portal for answers to commonly-asked questions (FAQ), how-to articles, technical specs, installation and user manuals, best practices and more.

Customers in Europe, Middle East and Africa:

- Phone: +46 (0) 31 337 6500
- E-Mail: TSG-EMEA@skf.com
- Chat: www.skf.com/cm/tsg

Customers in the Americas, Asia and all other locations:

- Phone: 1-858-496-3627 or toll-free (USA) 1-800-523-7514
- E-Mail: TSG-Americas@skf.com
- Chat: www.skf.com/cm/tsg

120517dm-fp-Feb_2020

Table of contents

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 can be illustrated by the figure below.

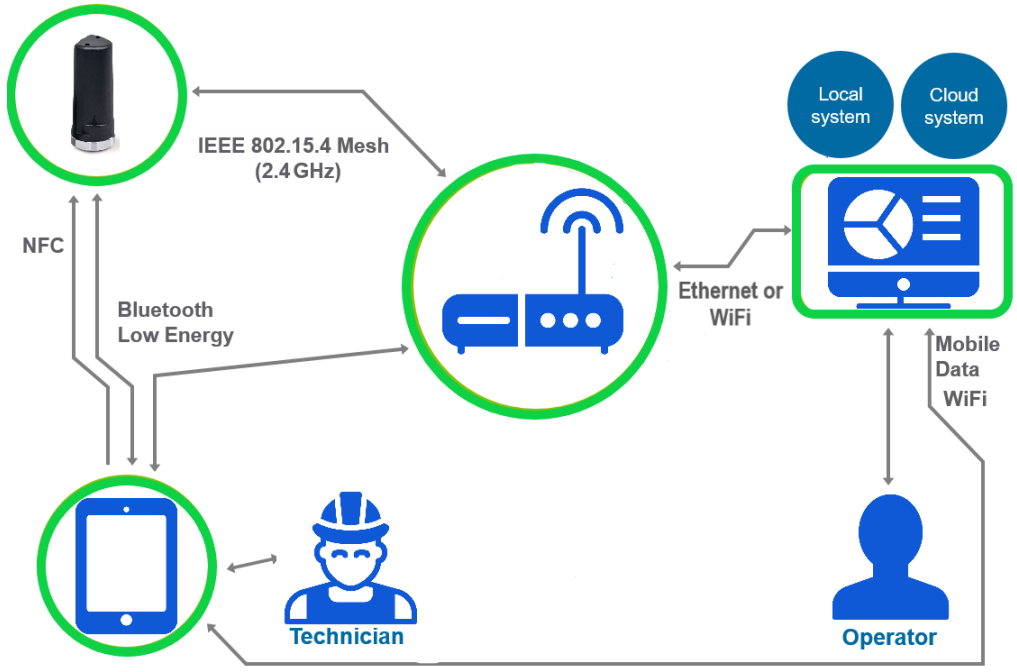


Figure 1 SKF Enlight Collect IMx-1 System architecture – single gateway, one sensor shown

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

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.

On a periodic basis, 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.*

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, a network/@ptitude Observer connection option
- 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 is also provided as a wire free alternative.

Communication between the gateway/sensor and Android 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:

WiFi 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: the Android device being used for the mobile app must support NFC, and as a minimum Android version 7 and Bluetooth Low Energy version 4.2. Refer **section 1.5** for further details.

1.2 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.

1.3 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 50 sensors across a maximum of 10 functional locations.

Where possible choose a gateway location that maximises the number of IMx-1 sensors that have a direct line of sight, with it. As support for external antennas is not

yet implemented do not enclose the gateway inside a further/outer enclosure that would block the radio signals.

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

1.3.1 Connections and interfaces

The gateway is housed in an IP rated enclosure suitable for indoor or outdoor installation and has built-in antenna for Wi-Fi 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:

Figure 2 View on gateway and mounting plate 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 image above. 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 (future use)

6. Gateway LED indicators
7. Connectors for external antenna: LTE x2, Mesh and Wi-Fi (future use)

Important note: Only the two connectors listed in bold above are usable, the remainder relate to potential future functionality and are not currently supported. Normally, no user access is needed to the gateway internals, all user connections are made available externally at these interfaces.

1.3.2 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:
  - Green: gateway is powered
  - Off: gateway is unpowered
- Lower, Status LED indicator
  - Off: gateway is unpowered
  - White: gateway is starting up
  - Yellow: started but not yet connected
  - Green: gateway has started and is also connected

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

1.3.3 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.

1.3.4 Data acquisition scheduling

The gateway is configured with four data acquisition schedules by way of **Interval** and **Interval alarm** settings for both the **Scheduled Trend Storage** and **Scheduled Dynamic Data Storage**. 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 **2.4.1**.

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 time 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. This process will take account of when the last measurement cycle ran so, after a synchronisation, the wait for ‘first’ data will usually be less than the scheduled period.

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.

1.3.5 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. This prevents significant data loss if the gateway loses power. The design aims to safeguard at least a week of data in this way.

1.4 SKF Enlight Collect Manager – Android app

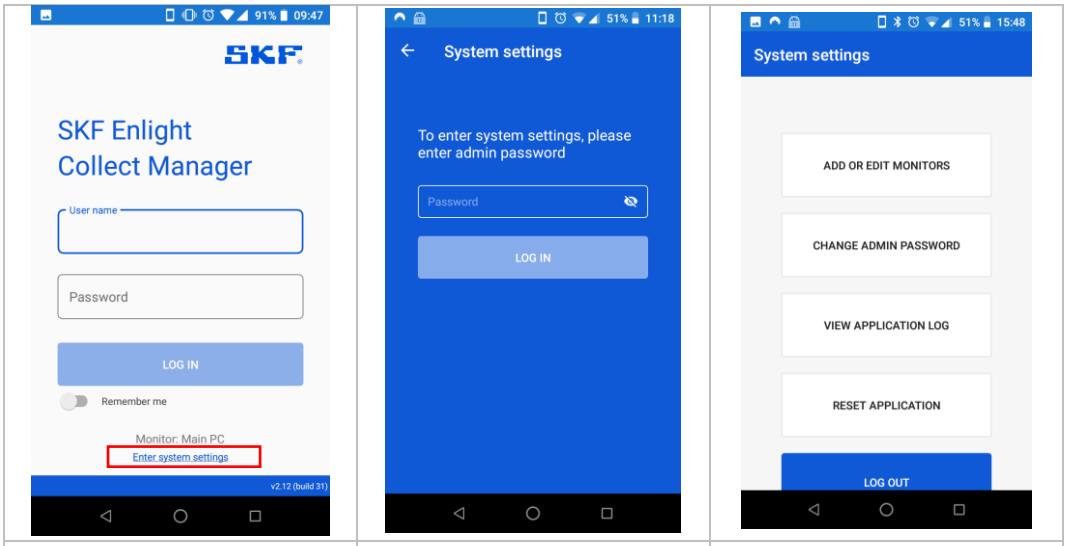
The SKF Enlight Collect Manager app is available for Android devices and is used to perform on-site system maintenance, commissioning, etc. The Android device being used must support:

- 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.

A user logging into the app must use User name and Password credentials appropriate to the @ptitude Observer database for the particular plant or area being commissioned. 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:

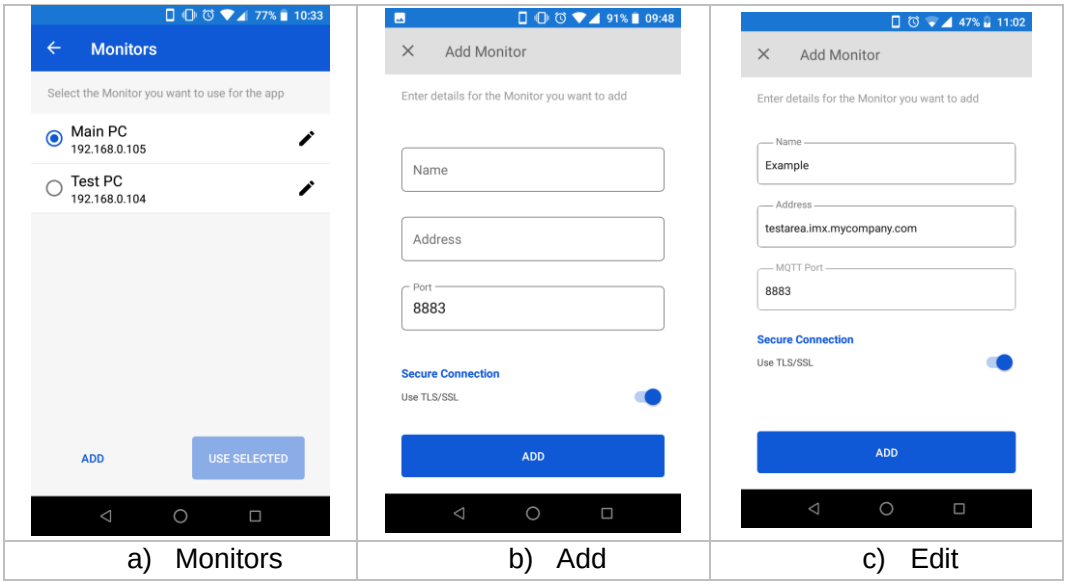


a) Main screen | b) Settings login | c) System settings

Figure 3 Accessing system settings

The default password to access the system settings is ‘admin’ although this can be changed at the next screen, if required.

Once into the system settings the first option “Add or Edit Monitors” is the means by which the active monitor instance can be selected or added/edited if the MQTT connection details don’t already exist in the app:



a) Monitors | b) Add | c) Edit

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.

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'.

1.4.1 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 so as 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. The 'Secure Connection' option is enabled by default.

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 DNS 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.

1.5 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.

- 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**.

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:

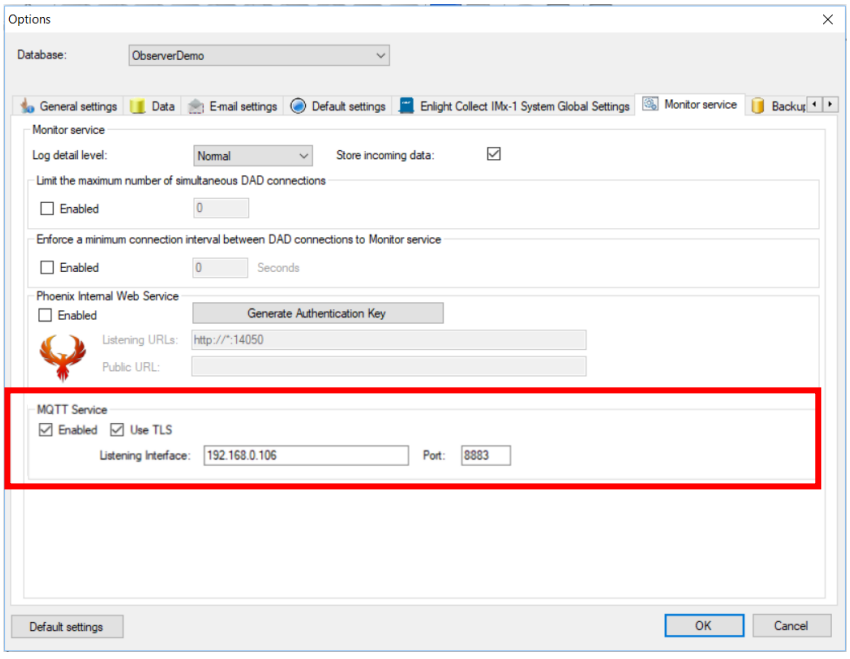


Figure 5 Monitor service tab – MQTT Service

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).

- **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.

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:

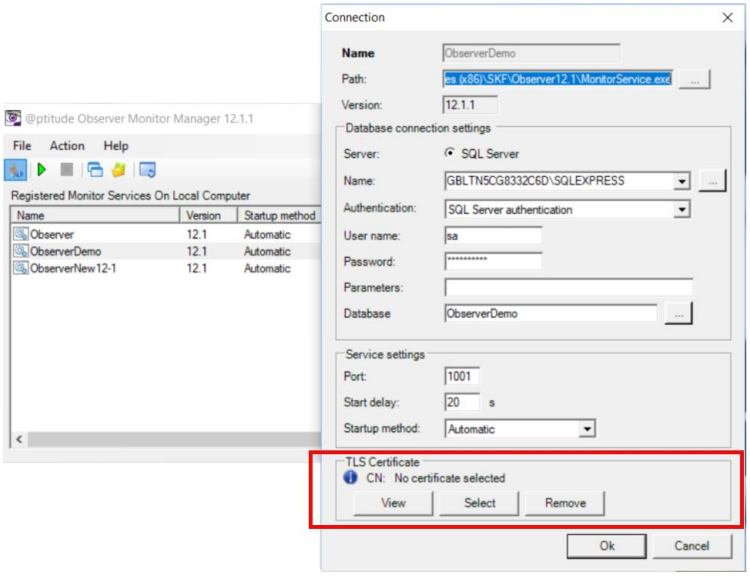


Figure 6 Using Monitor Manager to add a TLS certificate

There, at the bottom of the Properties/Connection dialog, the user can **Select** a certificate from its windows certificate store, **View** a selected certificate or **Remove** a certificate.

CN: The Common Name of the selected certificate is shown here. The blue information icon triggers tool tip text to remind users to ensure that the Common Name matches the Monitor address the gateway/app have, as a mismatch will prevent them connecting to @ptitude Observer Monitor.

Within @ptitude Observer an expiring certificate (one with less than 30-days validity) will generate a system alarm each day and an expired or missing certificate will cause a 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.

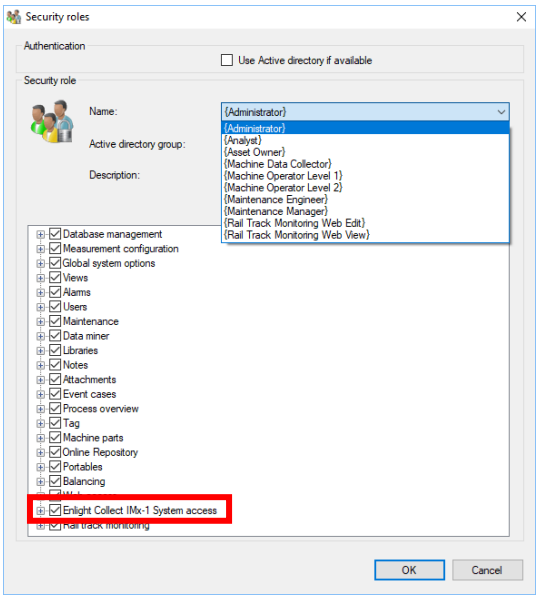


Figure 7 Security roles – IMx-1 System access, user rights

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:

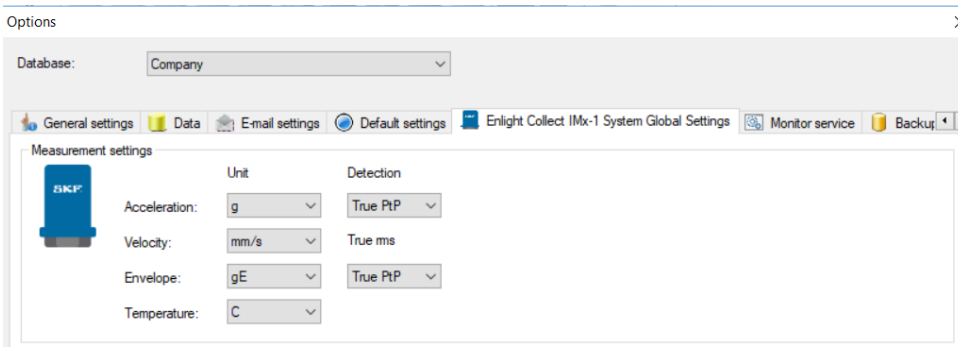


Figure 8 Enlight Collect IMx-1 System global settings

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

- Acceleration: **g** or m/s^2
- Velocity: **mm/s** or ips
- Envelope: **gE** or m/s^2E
- 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:

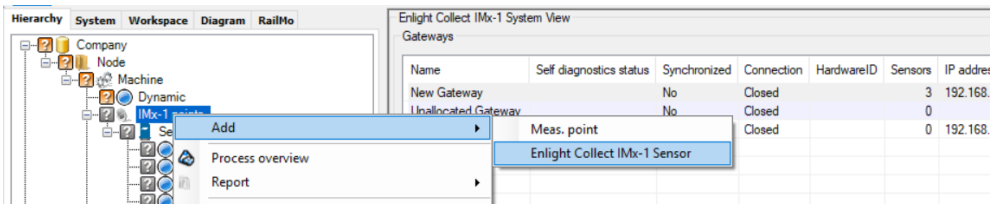


Figure 9 Add – IMx-1 Sensor

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.

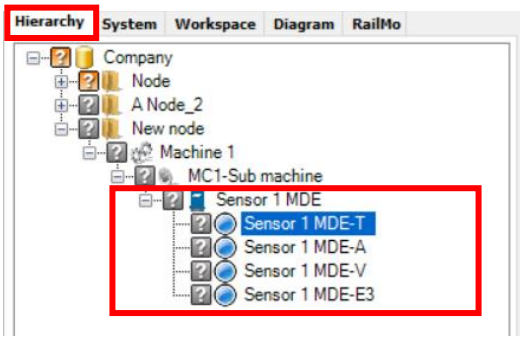


Figure 10 Hierarchy: IMx-1 sensor example

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 Cable 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.
- Neither IMx-1 measurements nor IMx-1 sensor nodes can be copied by using the ‘standard’ copy mechanisms, but they are included when using the Machine Copy Wizard.
    - The assigned gateway will not be copied, during the copy process the user will be asked to select a gateway or ‘None’, for this copied machine.
- 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 up the properties of an existing sensor node, right click and select Properties or double click.

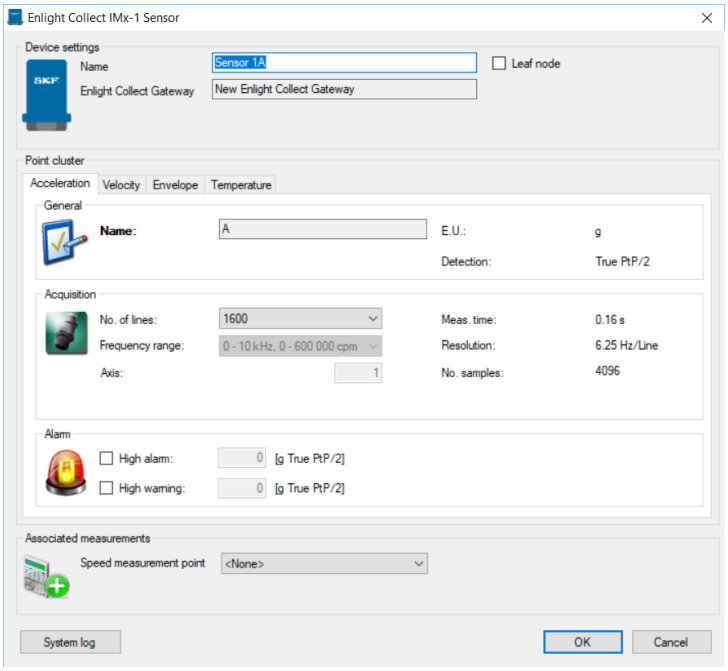


Figure 11 IMx-1 sensor dialog example

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 20**.

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:
    - 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, an area to configure the number of lines and to view the measurement configuration. By default, the "No. of lines" is set to 800.

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.

2.3 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 12 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.

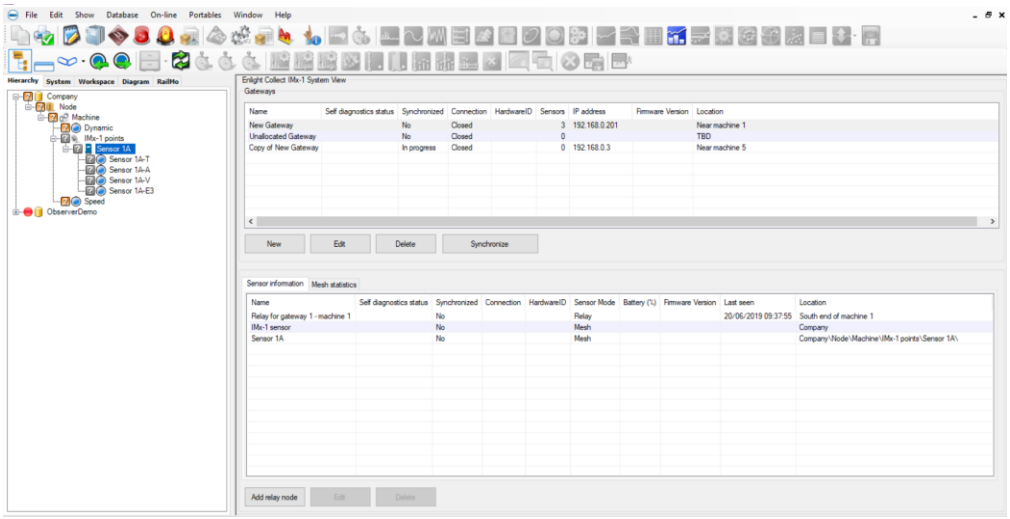


Figure 13 Enlight Collect IMx-1 System view

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:
    - 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:
    - 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.
    - **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.

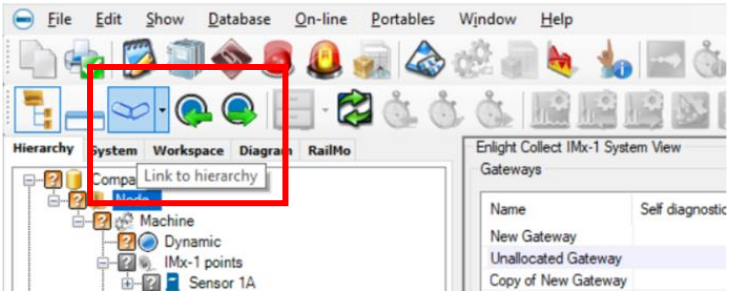


Figure 14 Activate/deactivate link to hierarchy view

2.3.1 Gateways

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

Name: Name given to the gateway.

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:

- Mesh module licence error.
- Missing/invalid network and identity configuration. This is a configuration known as ‘configuration 2’, in the event log.
- Missing/invalid ‘other’ configuration. This configuration includes measurement configuration. See also **Missing/invalid**.
- NTP Error.
- 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

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.

Sensors: The number of sensors linked to the gateway.

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

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

Location: Descriptive text for the physical location.

2.3.2 Sensors

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

Name: Name given to the sensor.

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:
    - Battery level low (1)
    - External Flash memory failure (16)
    - Configuration CRC failure (64)
    - Firmware update error (128)

- Watchdog reset (256)
- 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 **4.3.3**.

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.

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.

Sensor Mode: Mesh, Leaf or Relay. Refer description and notes on **Sensor Mode** and **2.4.2**.

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.

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.

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

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 21**.

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.

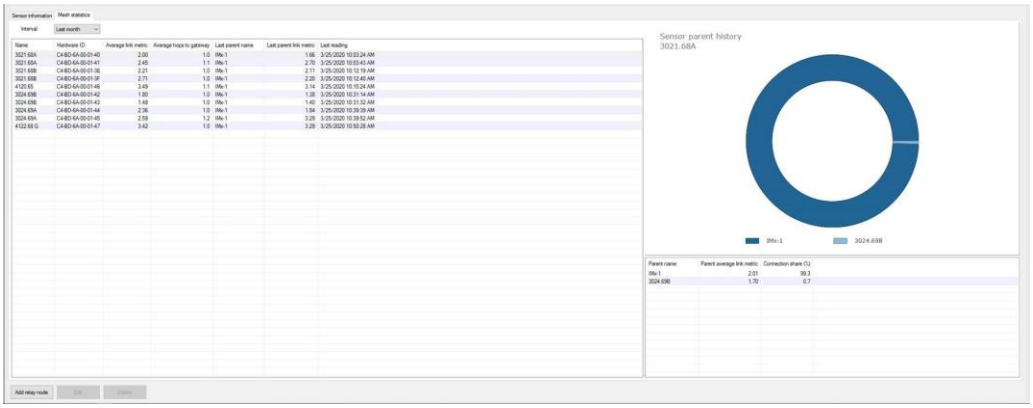


Figure 15 Mesh statistics tab

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** and a **Hardware ID**. 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.

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.

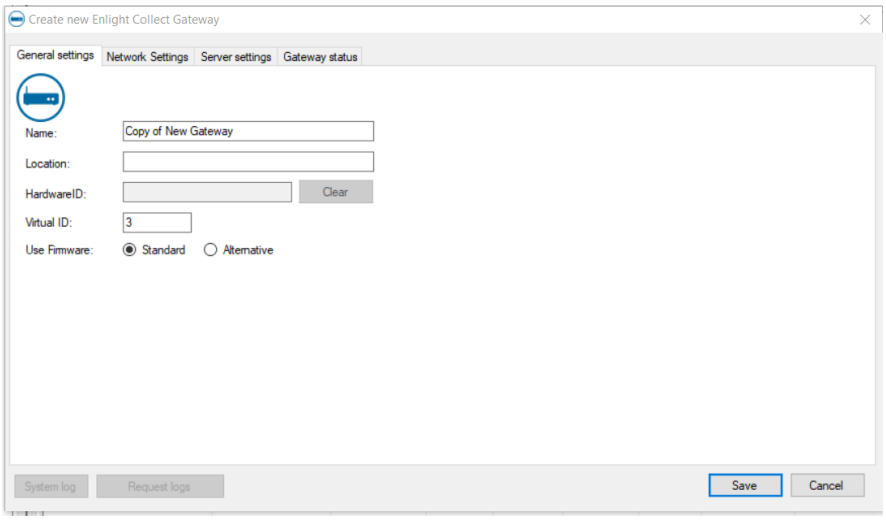


Figure 16 Configuring a new gateway – General settings tab

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)** or **WiFi** and to be set for dynamic (**DHCP**) or static addressing and as appropriate to allocate static settings for its own **IP Address**, **Sub-net Mask**, the network **Gateway** address, DNS addresses, etc.

Wi-Fi specific selections include as a minimum **Security** type, **Password**, **Country** and **SSID** for the wireless network. Note that the country setting is used by the gateway to determine the correct frequencies to be used for Wi-Fi.

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.

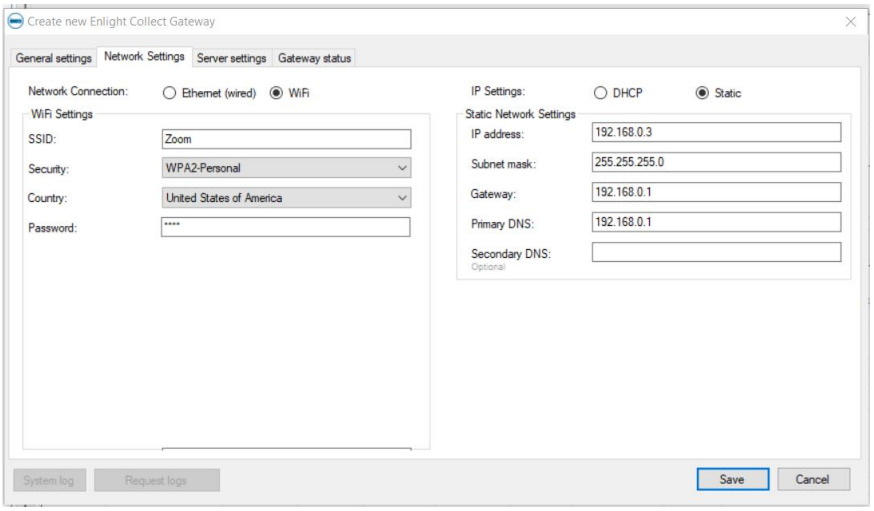


Figure 17 Gateway properties – Network settings tab

The third tab is Server settings:

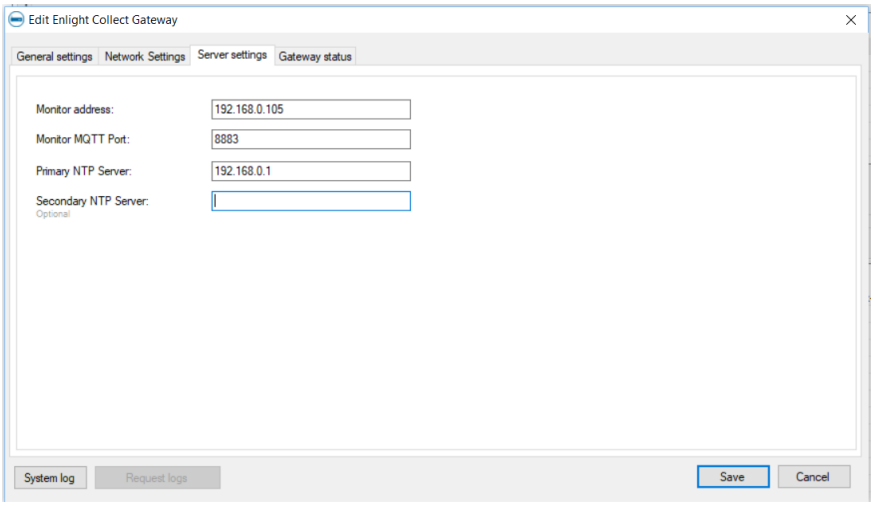


Figure 18 Gateway properties – Server settings tab

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 DNS 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', 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:

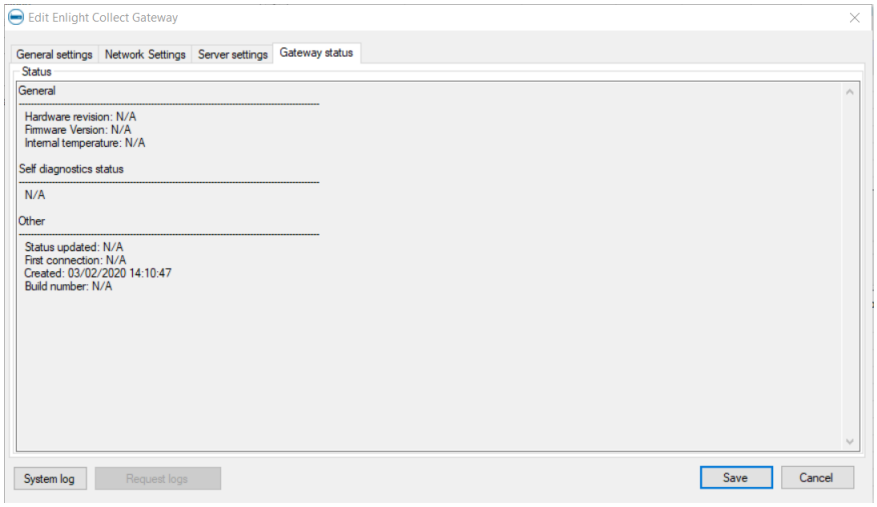


Figure 19 Gateway properties – Gateway status tab

The status tab feeds back information on **Hardware revision** and **Firmware version**, gateway **Internal temperature**, its **Self-diagnostics** status, **WiFi 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:

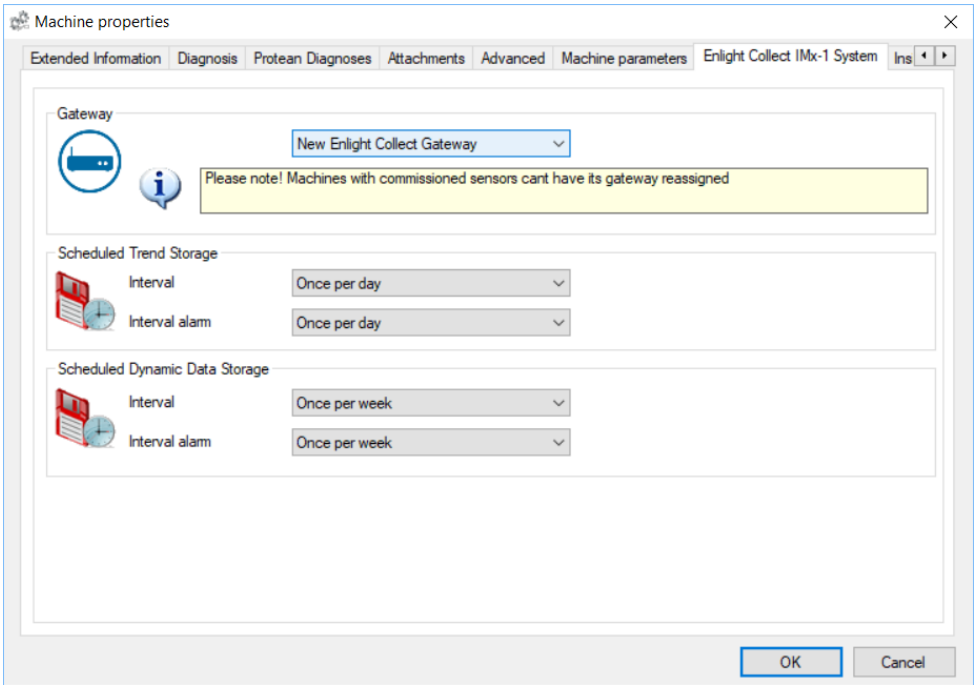


Figure 20 Machine properties, Enlight Collect IMx-1 System tab example

Gateway: There, a drop-down list 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>*'.

Scheduled Trend and **Scheduled Dynamic Data Storage**:

Both **Interval** and **Interval Alarm** settings for Trend storage default to '*Once per day*' and for Dynamic Data storage, '*Once per week*'. These are the least demanding, less frequent settings and if required can be set to shorter intervals:

Further options for the Trend storage: twice, four or eight times a day or every hour.

Further options for the Dynamic Data storage: every two days, day or every hour.

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.

In addition, the **Interval Alarm** setting for Trend or Dynamic Data can only be set at the same or at a faster capture rate than the equivalent **Interval** setting.

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

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.

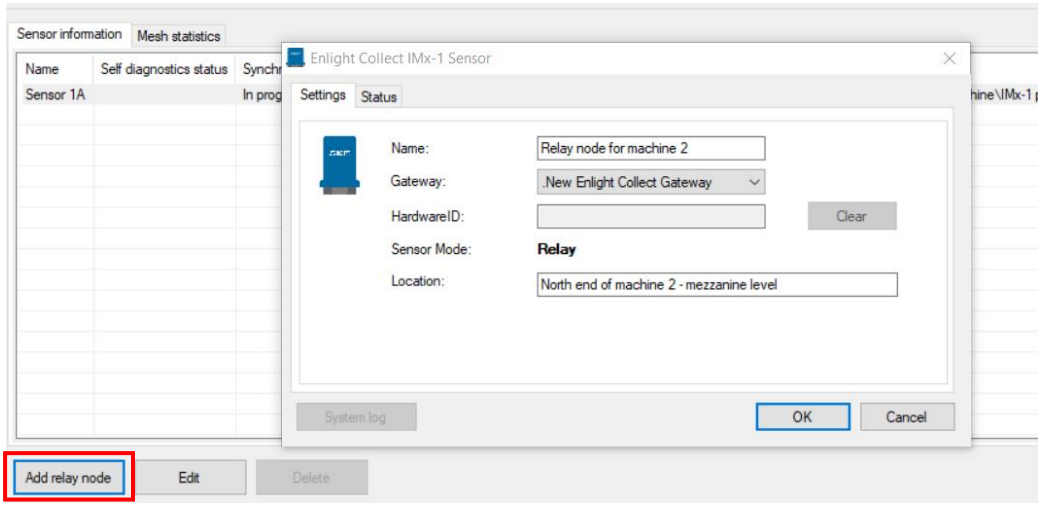


Figure 21 Relay node dialog example

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.

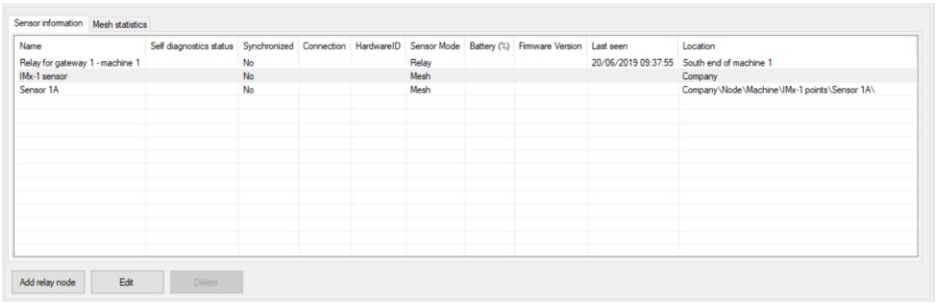
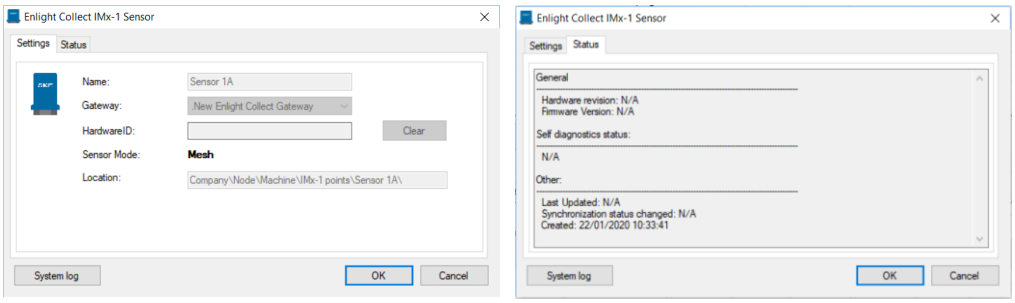


Figure 22 Sensor table example

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.



a) Settings tab b) Status tab

Figure 23 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**.

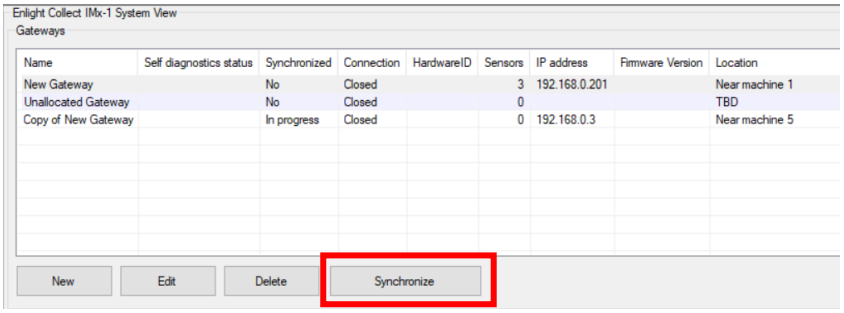


Figure 24 Synchronize button for configuration and firmware update

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 Clear a 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.

To connect a different physical device or just remove the current device, after decommissioning the device the existing Hardware ID can be cleared: the sensor properties dialog and the gateway properties dialog are both accessible from the Enlight Collect IMx-1 System View and include a **Clear** button to clear their respective hardware IDs.

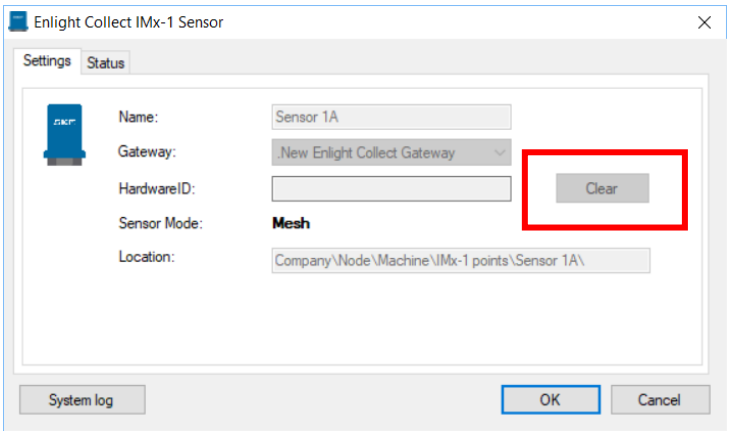


Figure 25 Hardware ID clear button – Relay mode sensor example

Clearing a Hardware ID does not remove measurement data but allows another physical device to be commissioned as a replacement for the previous one.

Note that similarly, if just moving a sensor from one monitoring location to another (decommission it and then recommission it in a new position), until the sensor's Hardware ID is cleared from the first location, it will be unable to connect in its new position due to the system having two sensors with the same Hardware ID. In this condition the gateway will report its Self diagnostic status as 'Missing/Invalid Configuration' until the duplication is corrected by clearing the sensor Hardware ID from the 'old' location.

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 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.

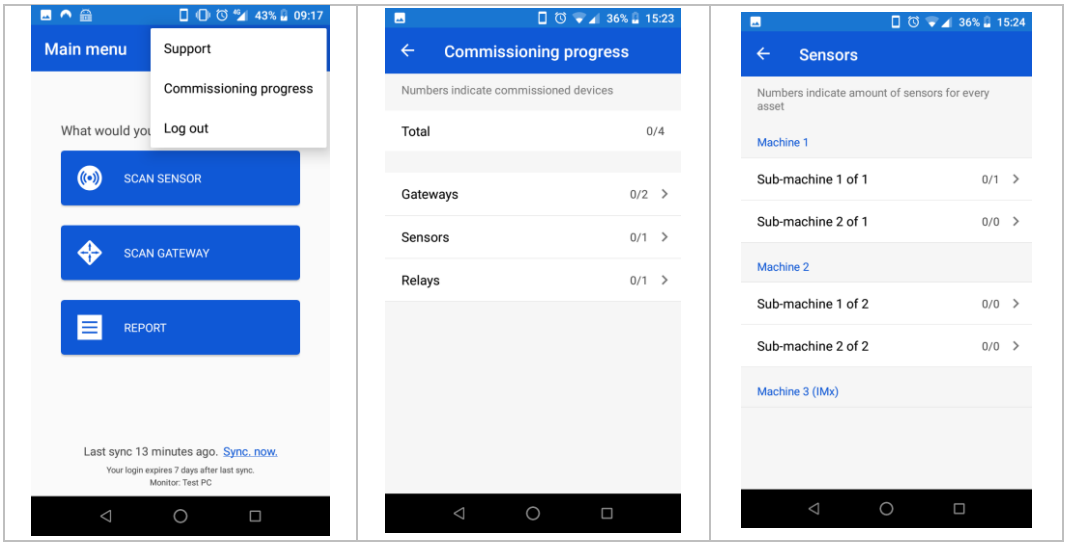
Note: like an @ptitude Observer login, the user name entry is not case sensitive.

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:



a) Main menu | b) Commissioning progress | c) View sensors

Figure 26 Viewing the commissioning progress

Before commencing commissioning work, or at any time later, the user can view a commissioning progress summary. Access this from the Main menu, touch more options, vertical ellipsis ⋮, then select 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. The SIM card holder is for future use as a mobile data connection is not currently supported.

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 27 Example of connector/cable assemblies

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

3.2.2 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 28 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 other gateway circuitry.

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.

3.2.3 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.

3.2.3.1 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.

3.2.3.2 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.

3.2.3.3 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.

3.2.3.4 LTE/UMTS mobile data

Whilst the gateway does not currently support an integrated mobile data connection an external 3G/4G modem could still be used.

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

3.2.5 Other interfaces

3.2.5.1 USB service interface

A USB service interface is available internally, for SKF use only or under the direction of 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:
    - Depth: greater of 8 mm (0.31 in.) or stud length plus 2-threads.
    - Drilled perpendicular to the mounting surface, within ±1°.
    - Flat mounting surface for the IMx-1 – within 25 µm (0.001 in.).

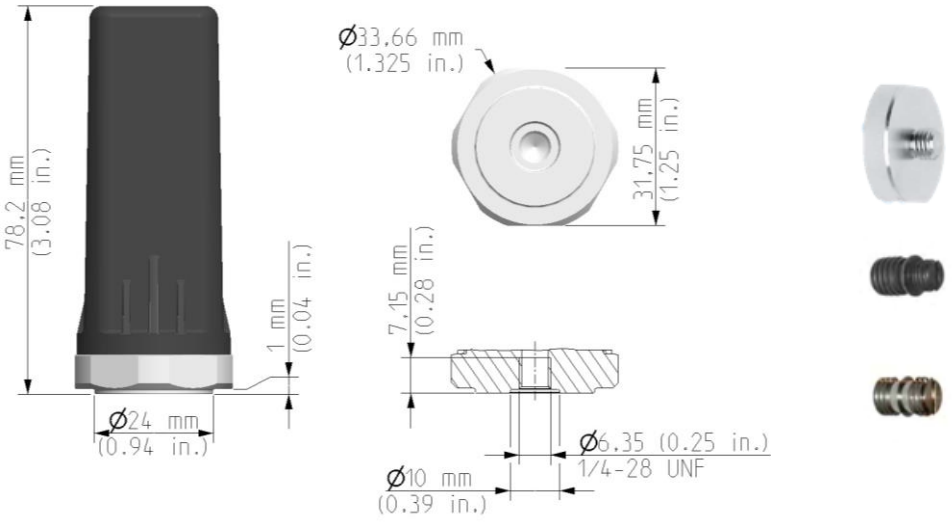
- Surface roughness no greater than 0.8 µm (32 µin.).
- When fitting, ensure there is no gap between the mounted sensor and the mounting surface.

- 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 29 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 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 ‘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.
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’.
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**.

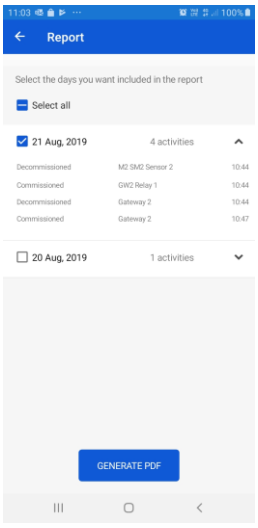
3.4 Relay node commissioning

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

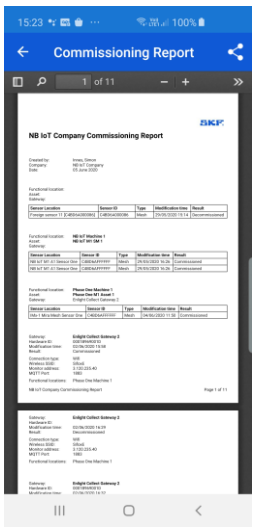
A. Launch the app. An earlier log in with network access is recommended.
B. Select ‘Scan Sensor’ function
    a. Bring the device close to the sensor to use NFC to wake it up, out of flight mode.
C. After a period for Bluetooth search the ID of the sensor will be displayed. Select it to connect and display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



a) Select data for report



b) Commissioning report

Figure 30 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.

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.

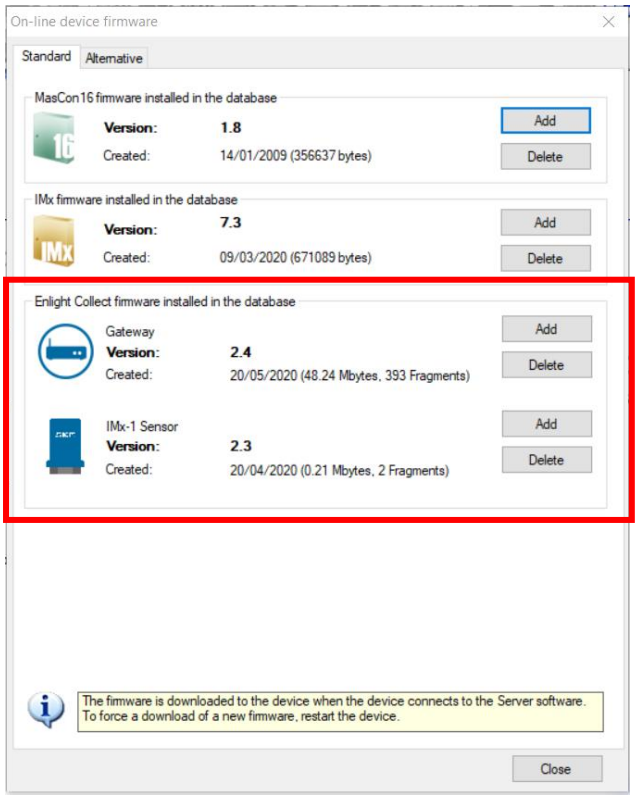


Figure 31 Gateway and sensor firmware is stored in @ptitude Observer

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:

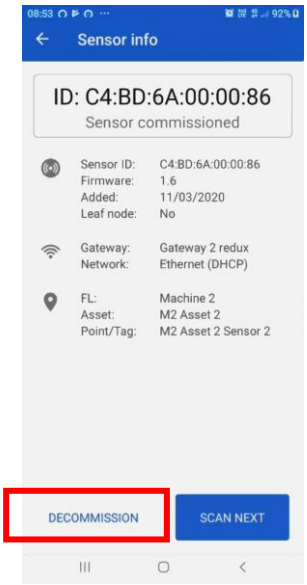


Figure 32 App Decommission button

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 has to re-establish its sensor relationships.

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.

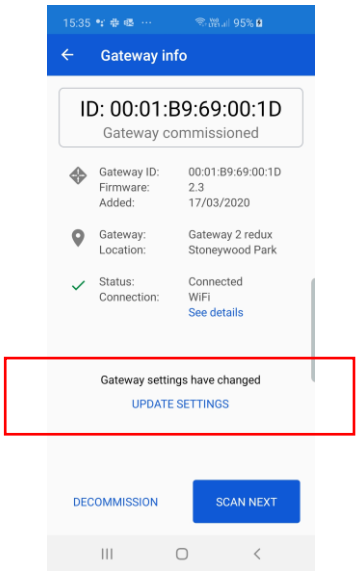


Figure 33 Update gateway network configuration

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
- Clear the device Hardware ID: that physical gateway can no longer connect to @ptitude Observer.

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

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.

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 a 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 **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:

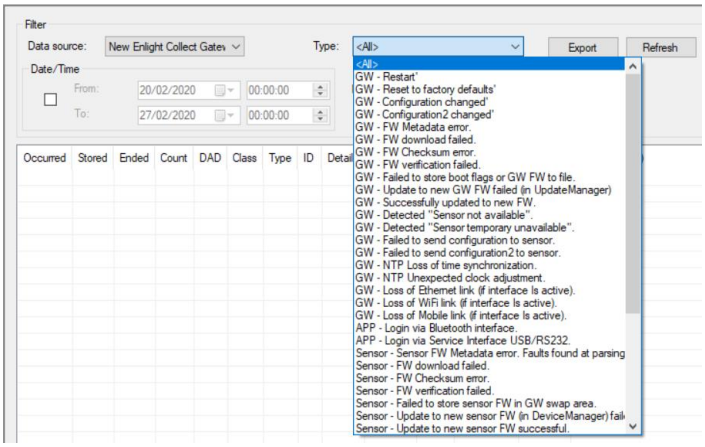


Figure 34 Event log filtering

- Count is related to the duration of an event:
  - 0 for an event without duration, for example gateway restarted.
  - 1 event ‘start’ for example log-in or loss of connectivity.
  - -1 for event ‘end’ for example log-out or connectivity regained.
- Some event types are ‘adapted’ for a wireless sensor:
  - A gateway detecting that a sensor has not responded to a communication, 3 tries at 5-minute intervals, results in a ‘Sensor temporarily unavailable’ event. This causes @ptitude Observer to set a, sensor ‘Not measured’, status.
  - 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 ‘Cable fault’ status.
  - 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

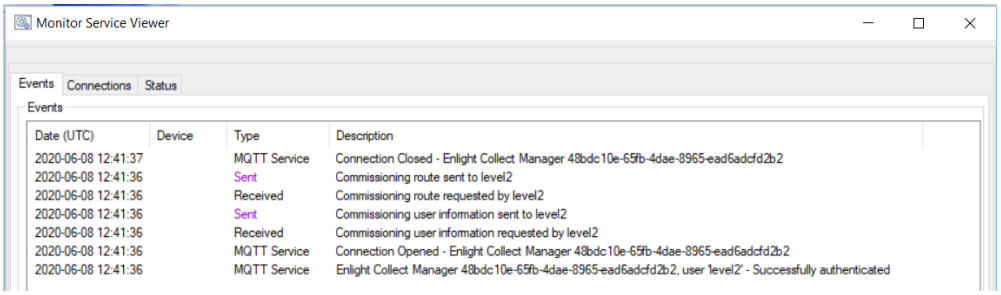
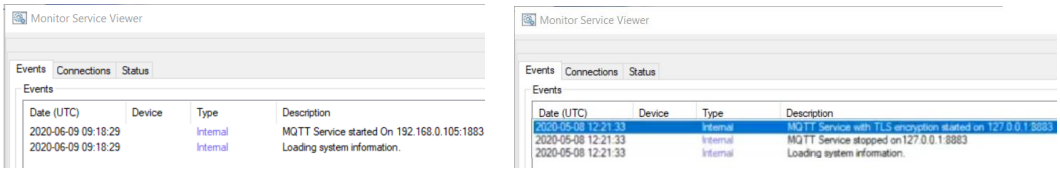


Figure 35 Monitor Service Viewer – Events – EC Manager app sync request – non-TLS



a) Without TLS b) With TLS

Figure 36 Monitor Service Viewer – Events – MQTT service started

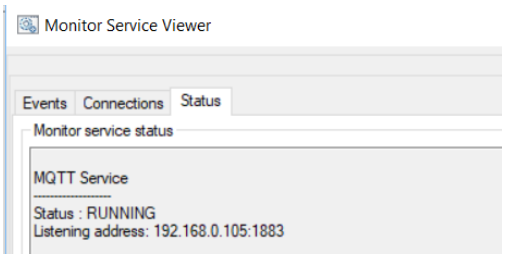


Figure 37 Monitor Service Viewer – Status – MQTT Running (TLS not enabled, example)

When troubleshooting use 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:

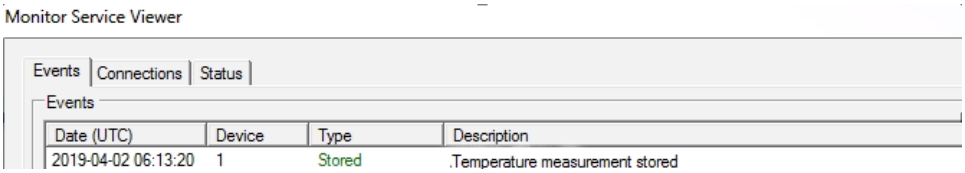


Figure 38 Monitor Service Viewer example

- 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:

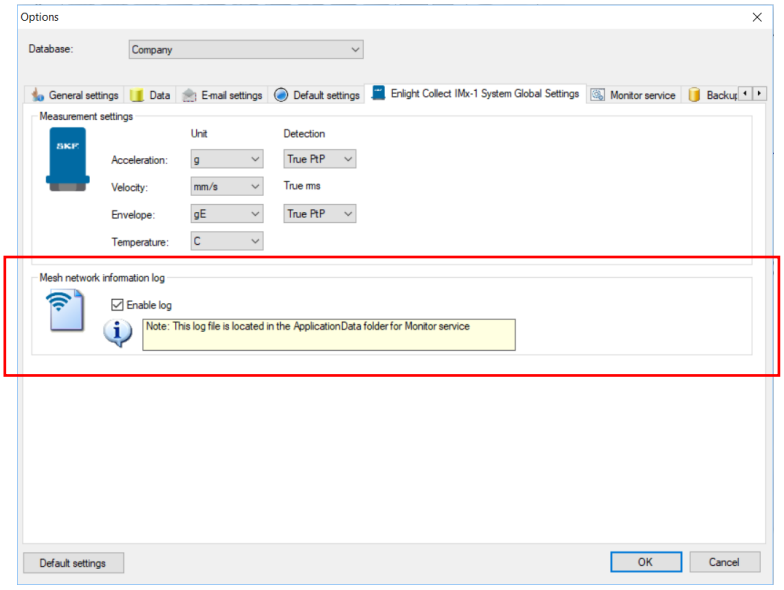


Figure 39 Enabling the 'Mesh network information log'

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.

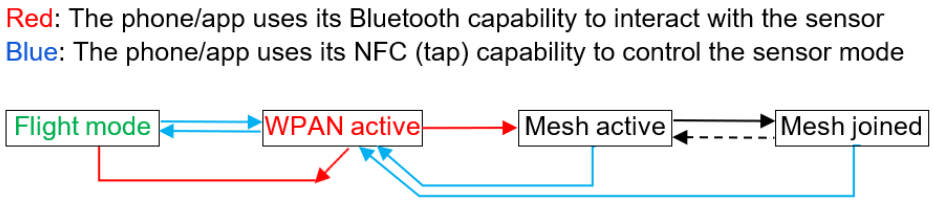


Figure 40 Sensor radio interactions and flow – all conditions

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.

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.
- 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:

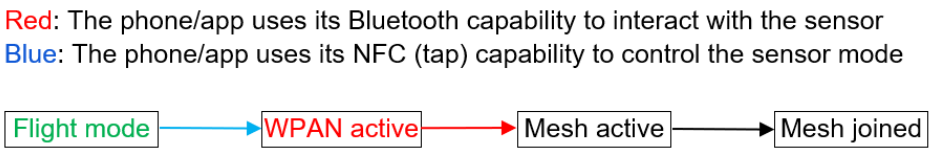


Figure 41 The commissioning flow – app controlled

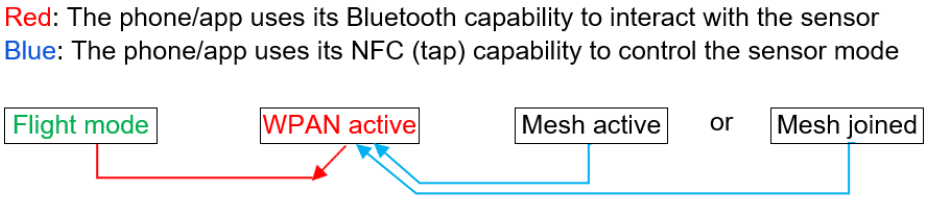


Figure 42 The decommissioning flow – app controlled

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 green. 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.

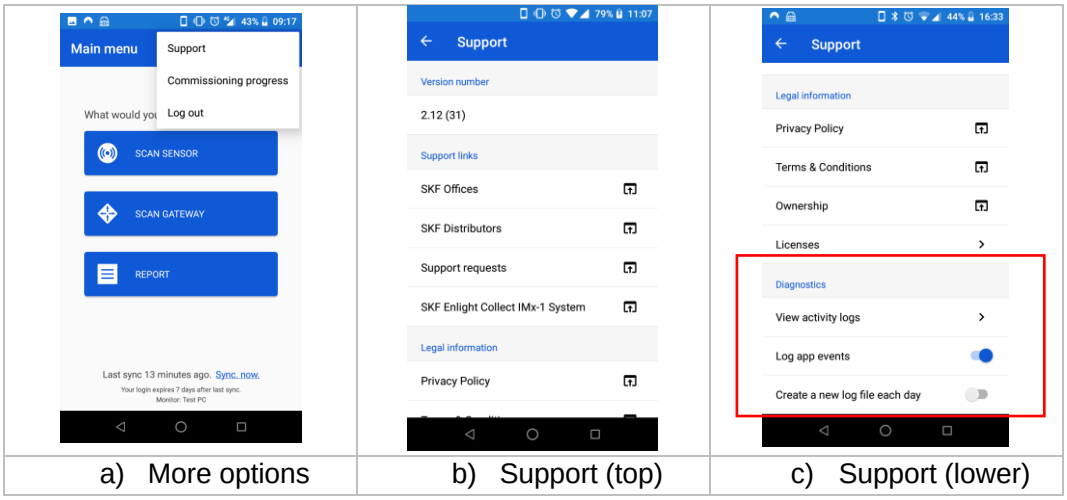
The sensor antenna is located internally, towards the middle of the ‘flat side’ of the sensor case. Its approximate location is marked in the figure below:

Figure 43 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 touch the more options, vertical ellipsis ⋮, then select Support:



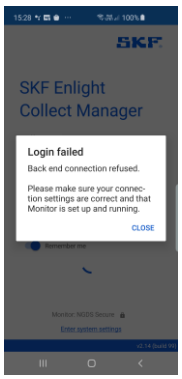
a) More options | b) Support (top) | c) Support (lower)

Figure 44 Enabling the app, log file feature via App Support options

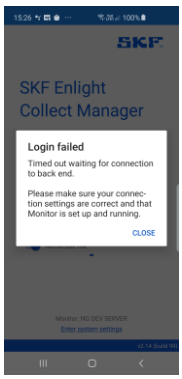
In the Diagnostics section, which is in the lower half of the Support list, there is an option to enable log file storage, a further option to choose between a single continuous file or separate files each day and an option to view the created logs in app. When viewing a log file, it can be directly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



c) App TLS to Monitor non TLS



d) App non TLS to Monitor TLS

Figure 45 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 can be expected if the gateway status LED indication shows anything other than green. 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 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.

4.3.7.1 USB service interface

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

Figure 46 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:
    - "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.
    - 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:

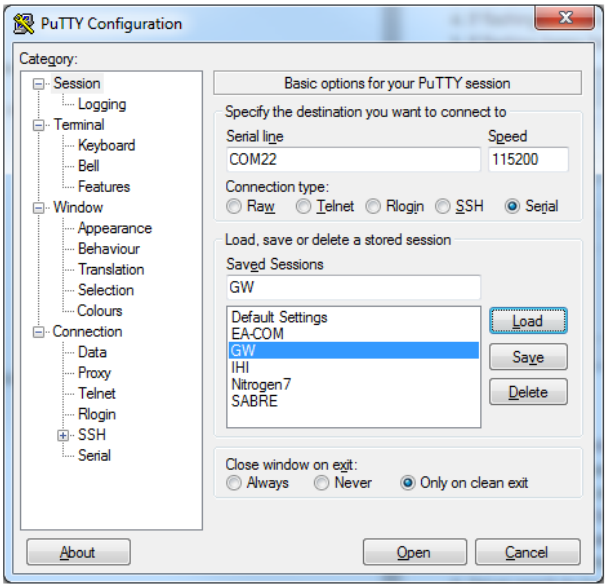


Figure 47 A typical terminal configuration for using the service interface

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 **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:

- 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.

- 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.

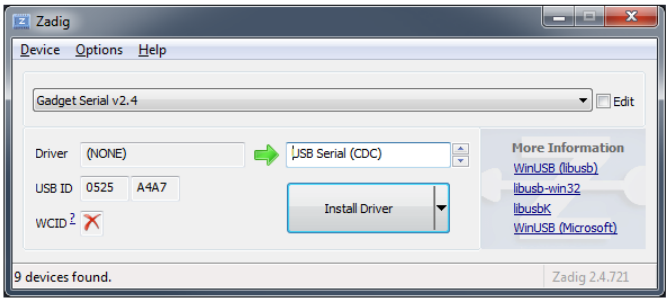


Figure 48 Using Zadig utility to install the USB device driver

4.3.7.2 Ethernet LEDs

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

5 Product specifications

5.1 IMx-1 wireless sensor specifications

5.1.1 Environmental and physical

Table 4 Wireless sensor environmental specifications

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 ^{0}C (–40 to +185 ^{0}F)
Storage	Recommended maximum temperature: 30 °C (86 °F) To avoid excessive self-discharge of the battery, do not store at high temperatures (30 ^{0}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	Currently safe area use only (ATEX/IECEx Zone 1 pending)

5.1.2 Operational states and battery

Table 5 Wireless sensor operational states and battery specifications

Model designation	IMx-1
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.

5.1.3 Measurements

Table 6 Wireless sensor measurement specifications

Model designation		IMx-1
Enveloping		Band 3
	Resolution	0.001 gE
Acceleration		Yes
	Dynamic range	50 g peak
	Resolution	0.002 g
Velocity		Yes
	Dynamic range	100 mm/s (3.94 in/s) RMS
	Resolution	0.0125 mm/s (0.0005 in/s) RMS
Temperature		Yes
	Measurement range	–40 to +85 ^{0}C (–40 to +185 ^{0}F)
	Resolution	1 ^{0}C (1.8 ^{0}F)
	Accuracy	±3 ^{0}C (±5.4 ^{0}F)
	Maximum and minimum temperatures	Stored by the sensor

Notes:

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

5.1.4 Signal processing

Table 7 Wireless sensor signal processing specifications

Model designation	IMx-1
Enveloper 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 ^{0}C (–56.2 to +401 ^{0}F)
Self-diagnostics	Yes

5.1.5 Interfaces

Table 8 Wireless sensor interface specifications

Model designation	IMx-1
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.
Proximity IEC 14443: NFC (Near Field Communication) certification is pending.

OTA: Over The Air device firmware updates

5.1.6 Certifications

Europe

- Radio Equipment Directive (RED) and CE certified (radio, EMC and product safety)
  - Radio testing according to:
    - EN 300328 for IEEE 802.15.4 Sensor radio
    - EN 300328 for Bluetooth Low Energy
    - EN 300330 for NFC
    - EN 62479
    - EN 62369-1 and 50364
  - EMC testing according to:
    - EN 301489-1
    - EN 301489-3
    - EN 301489-17
    - 61000-6-4
    - 61000-4.3
    - 61000-4.2
  - Safety requirements according to EN 61010-1

North America

- Radio testing according to:
  - FCC 15.247 for IEEE 802.15.4 Sensor radio
  - FCC 15.247 for Bluetooth Low Energy
  - FCC 15.207 for NFC
- 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.

Central/South America

- Anatel certification Brazil: Anatel, this certification is pending.

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.

5.2 Enlight Collect gateway specifications

5.2.1 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 ^{0}C (–4 to +140 ^{0}F)
Storage	–40 to +85 ^{0}C (–40 to +185 ^{0}F)
Humidity	Maximum 95% relative non-condensing
Altitude	Maximum 5 000 m (16,404 ft.)
Hazardous area rating	Safe area use only (ATEX/IECEx Zone 2 future)

5.2.2 Power

Table 10 Gateway power specifications

Parameter	Specification
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.

5.2.3 Internal measurement capabilities

Table 11 Gateway Internal measurement capabilities

Parameter	Specification
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.

5.2.4 Interfaces

Table 12 Gateway interface specifications

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
	WPA2-Personal (with AES encryption) or
	WPA2-Enterprise
Time synchronisation	NTP for synchronisation of the internal real time clock
	Two configurable NTP server IP addresses
	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:
WPAN IEEE 802.15.1: Bluetooth SIG certification has been achieved.
Wi-Fi, WPAN and sensor wireless mesh radio can co-exist on 2.4 GHz ISM, band
OTA: Over-the-air device firmware updates

5.2.5 Certifications

EU Declaration of Conformity

Manufacturer: SKF Sverige AB

Address: Aurorum 30, 977 75 Luleå

Country: Sweden

Type of Equipment: Wireless Condition Monitoring System

Part Number:	**Part Name:**
CMWA 6600	SKF Enlight Collect Gateway

The manufacturer declares under sole responsibility that the products listed above conform to the requirements of the following directives:

Radio Equipment Directive	(RED) 2014/53/EU
Restriction of Hazardous Substances	(ROHS 3) 2015/863/EU

The conformity assessment procedure referenced to article 10 and detailed in Annex III of the Radio Equipment Directive 2014/53/EU has been followed and performed with the involvement of a notified body.

The following harmonized standards and normative documents are those to which the product's conformance is declared, and by specific reference to the essential requirements of the referenced Directives:

Health & Safety (Article 3.1(a) of RED)	EN 62311:2008
	IEC 62368-1:2014 (Second Edition)
	EN 62368-1:2014 + AC:2015 + A11:2017
	IEC 62368-1 – Ed. 3, Annex Y only
EMC (Article 3.1(b) of RED)	ETSI EN 301 489-1 - V2.1.1 - 2017
	ETSI EN 301 489-17 – V3.1.1 - 2017
Spectrum (Article 3.2 of RED)	ETSI EN 300 328 - V2.1.1 - 2016
	ETSI EN 301 893 - V2.1.1 - 2017
RoHS Prevention (Article 4.1)	EN 50581:2012

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
  - EMC testing according to:
    - FCC Part 15B/ICES003 Unintentional Radiator portion
  - Radio testing according to:
    - FCC 15.247 / RSS247
      - Simultaneous-transmission measurement
      - FCC/ISED correlation

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.

Central/South America

- Anatel certification: this certification is pending.

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 Qualification process completed.

5.2.6 Gateway mounting

The SKF Enlight Collect Gateway, excluding mounting plate, has overall dimensions of 220 mm high, 220 mm wide and 50.5 mm deep. It is supplied fitted to the mounting plate shown below. This mounting plate has overall dimensions of 195 mm wide, 250 mm high and is 6 mm thick. It provides for a 4-point mounting and has four 6.5 mm, clearance for M6, holes on a 150 mm by 220 mm pitch.

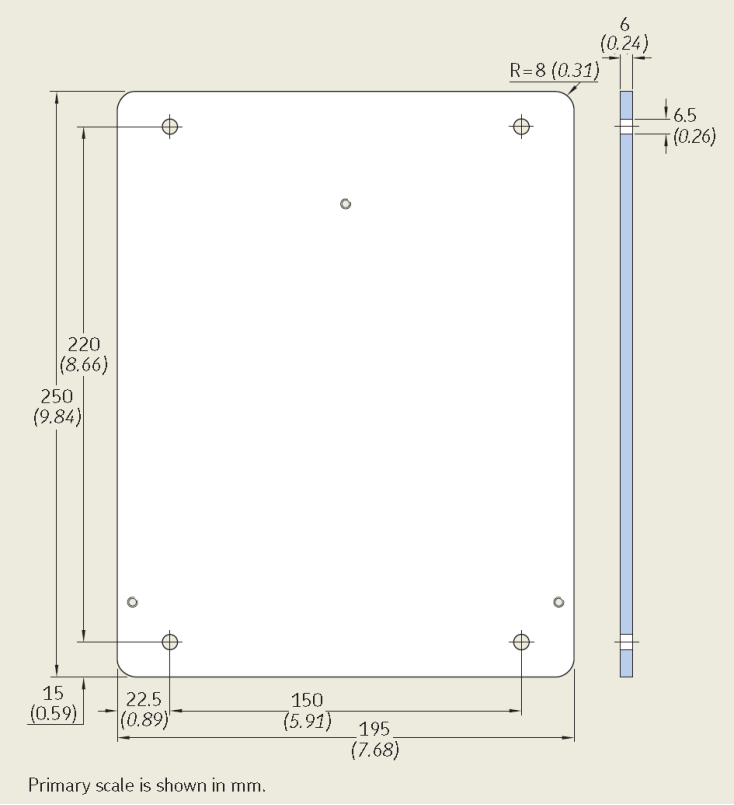


Figure 49 Gateway mounting plate dimensional drawing

To mount the gateway by its mounting plate it is only necessary to 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.*

5.3 Product marks and labelling

5.3.1 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 13 Explanation of marks

Mark	Meaning
	CE marking according to CE 2014-53-UE
	Certification: FCC
	Certification: Bluetooth SIG
	Certification: ATEX
	Certification: Anatel
	WEEE: Waste Electrical and Electronic Equipment Directive (2012/19/EU)

5.3.2 Sensor

Figure 50 Sensor labelling

There is a flat area on one face of the sensor case where the SKF product marking is placed. Below that is a small area that may be used by the customer to place their own identification marking on the sensor, if this is required.

5.3.3 Gateway

On the front face of the case a manufacturing data label, Figure 51, 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.

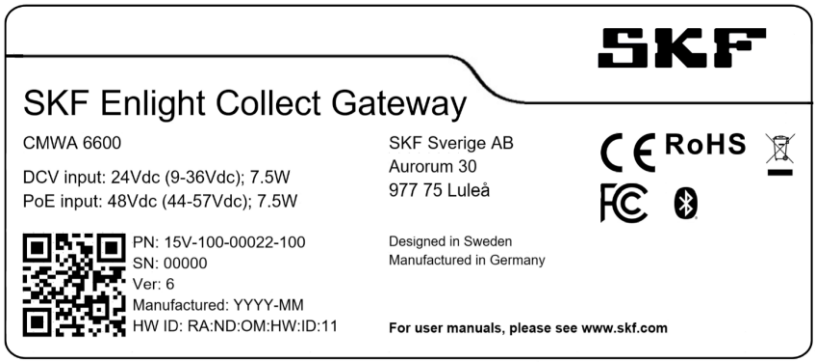


Figure 51 Gateway labelling

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

5.4 Quality control

- SKF Sverige AB, Luleå and SKF (UK) Ltd, Livingston are ISO 9001:2015 certified.

6 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.

The SKF Enlight Collect gateway is manufactured by SKF Sverige AB:

SKF Sverige AB
Aurorum 30
977 75 Luleå
Sweden

The SKF Enlight Collect IMx-1 wireless sensor is manufactured by SKF (UK) Ltd:

SKF (UK) Ltd
2 Michaelson Square
Livingston
EH54 7DP
United Kingdom

Appendix A Limited Warranty

SKF – Limited Warranty

WARRANTY

Subject to the terms and conditions contained herein and provided that there is no applicable written agreement between the selling entity in the SKF Group ("SKF") and the Buyer specifically covering the sale of the Products (as defined below) that includes a product warranty, SKF warrants to the Buyer that for the warranty period indicated below the products sold by SKF that are listed below (the "Products"), when properly installed, maintained and operated, will be free from defects in material and workmanship and shall be fit for the ordinary purposes for which the Products are designed.

BUYER'S LIMITED REMEDIES

This limited warranty defines SKF's sole and exclusive liability and Buyer's sole and exclusive remedy for any claim arising out of, or related to, any alleged deficiency in any Product sold by SKF, even if such claim is based on tort (including negligence or strict liability), breach of contract, or any other legal theory. If the Product does not conform to this limited warranty, Buyer must notify SKF or SKF's authorized service representative within thirty (30) days of discovery of the nonconformity; provided, however, that SKF shall not be liable for any claim for which notice is received by SKF more than thirty (30) days following the expiration of the applicable warranty period for the Product. Upon receipt of timely notification from Buyer, SKF may, at its sole option, modify, repair, replace the Product, or reimburse Buyer for any payment made by Buyer to SKF for the purchase price of the Product, with such reimbursement being pro-rated over the warranty period.

WARRANTY PERIOD

Except as expressly provided below, the warranty period for each Product shall commence on the date the Product is shipped by SKF to Buyer.

90-DAY WARRANTY

Products warranted for ninety (90) days by SKF are as follows: cable assemblies, MARLIN QuickConnect (MQC), magnetic temperature probes, and all refurbished equipment.

ONE-YEAR WARRANTY

Products warranted for one (1) year by SKF are as follows: all Microlog products and accessories, all Microlog Inspector applications including hand-held computers, all MARLIN data managers (MDM), all MARLIN Condition Detectors (MCD), all Wireless Machine Condition Detectors (WMCD), all Multilog Condition Monitoring Units (CMU, TMU), Multilog Local Monitoring Units (LMU), all Multilog Wireless Monitoring Units (WMx), Multilog On-line System Wireless Vibration Transmitter ISA100, all Wireless Monitoring Systems V/T, all Vibration PenPlus, all Machine Condition Advisors (MCA), all Machine Condition Indicators (MCI), all transmitters, all Monitor Interface Modules (MIM), all Machine Condition Transmitters (MCT), all MicroVibes and Custom Products with the prefix of CMCP (with the exception of any consumable or expendable items), Shaft Alignment Systems TKSA 60 and TKSA 80 including hand-held computer, measuring units and accessories.

TWO-YEAR WARRANTY

Products warranted for two (2) years by SKF are as follows: all standard Eddy Probes, Eddy Probe Drivers, and Eddy Probe Extension Cables, all Multilog On-line Systems (IMx) and all Wireless Machine Condition Sensors.

For all On-line Systems (as defined below) that have satisfied Criteria 1 and 2 below, the warranty period shall be either thirty (30) months from the date the On-line System is shipped by SKF to Buyer, two (2) years from the date the On-line System is installed and commissioned by SKF, or two (2) years from the date on which the installation of the On-line System has been audited and commissioned by SKF or its authorized service representative, whichever period ends first.

Criteria 1.

Devices used with a Multilog On-line System (IMx), Multilog Condition Monitoring Unit (CMU), Multilog Local Monitoring Unit (LMU), including, but not limited to, the sensing device, the interconnect cabling, junction boxes, if any, and the communications interface, must consist only of SKF-supplied or SKF-approved devices and/or components. The computer provided by Buyer must meet the requirements stipulated by SKF.

Criteria 2.

SKF or its authorized service representative has installed the On-line System or has audited the installation and commissioned the On-line System.

"On-line Systems" are defined as systems consisting of Multilog On-line System (IMx), Multilog Condition Monitoring Unit(s) (CMU), Multilog Local Monitoring Unit(s) (LMU), and any sensing or input devices, the interconnect cabling between the sensing or input devices and the Multilog On-line System (IMx), Multilog Condition Monitoring Unit(s) (CMU), Multilog Local Monitoring Unit(s) (LMU), and the cabling between the Multilog On-line System (IMx), Multilog Condition Monitoring Unit (CMU), Multilog Local Monitoring Unit (LMU) and the proprietary SKF communications interface with the host computer.

FIVE-YEAR WARRANTY

Products warranted for five (5) years by SKF are as follows: special seismic sensors.

LIMITED LIFETIME WARRANTY

Products covered under this Limited Lifetime Warranty (as set forth below) are as follows: standard seismic sensors of the CMSS 2XXX and CMSS 7XX series (accelerometers and velocity transducers) as marked and published in the SKF Vibration Sensor Catalogue.

(A) Subject to the terms herein, SKF will provide a "Limited Lifetime Warranty" for the products specified above sold by SKF after April 15, 2014. Under the Limited Lifetime Warranty, those products shall, at the time of shipment, be free from defects in material and workmanship. If any of these products fail to meet the terms of this Limited Lifetime Warranty during the life of such products, SKF, in its sole discretion, will repair, replace or exchange the products for the same model if the necessary components for the products are still available to SKF on a commercially reasonable basis. SKF will not provide a Limited Lifetime Warranty on products damaged by accident, abuse, misuse, neglect, improper installation, problems with electrical power, natural disaster, or by any unauthorized disassembly, repair or modification.

(B) Upon receipt of any product covered by the Limited Lifetime Warranty, SKF will pay all shipping charges to send the repaired, replaced or exchanged product to the original point of shipment. SKF reserves the right to decline repair or replacement if no fault is found in the product.

(C) For any warranty claim, the original Buyer must provide SKF with the applicable model and serial numbers, the date of purchase, the nature of

the problem, and proof of purchase. SKF, in its sole discretion, will determine if the Buyer must return the product covered under this warranty to SKF.

(D) The express warranty set forth in the Limited Lifetime Warranty is in lieu of and excludes any and all other warranties express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

(E) SKF's sole obligations under this Limited Lifetime Warranty are set forth in paragraphs (A) and (B), and SKF's liability under this Limited Lifetime Warranty shall not exceed the purchase price of the product, plus any shipping and handling charges that SKF may be obligated to pay pursuant to paragraph (B).

(F) **IN NO EVENT SHALL SKF BE LIABLE OR OBLIGATED TO THE BUYER OR ANY OTHER PERSON FOR SPECIAL, EXEMPLARY, PUNITIVE, INCIDENTAL, DIRECT, INDIRECT, GENERAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BY WAY OF EXAMPLE ONLY, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR LOSS OF USE) OR ANY OTHER LOSS, COST OR EXPENSE IN CONNECTION WITH THE PRODUCTS REGARDLESS OF WHETHER OR NOT ANY OF THE FOREGOING WERE FORESEEABLE OR THAT SKF WAS ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES, LOSS, COST, OR EXPENSE.**

(G) The Limited Lifetime Warranty applies solely to the original Buyer and is non-transferrable.

OTHER SKF PRODUCTS

Any SKF product supplied hereunder but not covered by this limited warranty shall be either covered by the applicable SKF limited warranty then in place for such product or, if no such warranty exists, shall be covered by the 90-day warranty stated above.

THIRD PARTY PRODUCT WARRANTIES

For any third party products sold to Buyer by SKF, SKF will transfer to Buyer any warranties made by the applicable third party product vendor to the extent such warranties are transferable.

CONDITIONS

As a condition to SKF's warranty obligations hereunder and if requested or authorized in writing by SKF, Buyer shall forward to SKF any Product claimed by Buyer as being defective. Buyer shall prepay all transportation charges to SKF's factory or authorized service center. SKF will bear the cost of shipping any replacement Products to Buyer. Buyer agrees to pay SKF's invoice for the then-current price of any replacement Product furnished to Buyer by SKF, if the Product that was replaced is later determined by SKF to conform to this limited warranty.

SKF shall not be obligated under this limited warranty or otherwise for normal wear and tear or for any Product which, following shipment and any installation by SKF (if required by the contract with the Buyer), has, in SKF's sole judgment, been subjected to accident, abuse, misapplication, improper mounting or remounting, improper lubrication, improper repair or alteration, or maintenance, neglect, excessive operating conditions or for defects caused by or attributable to the Buyer, including without limitation Buyer's failure to comply with any written instructions provided to Buyer by SKF.
SKF shall be free to conduct such tests, investigations and analysis of the Products returned to SKF, as it deems reasonable and proper in the exercise of its sole judgment.
As a further condition to SKF's obligations hereunder, Buyer shall offer its reasonable cooperation to SKF in the course of SKF's review of any warranty claim, including, by way of example only, Buyer's providing to SKF any and all information as to service,

operating history, mounting, wiring, or re-lubrication of the Product which is the subject of the Buyer's warranty claim.

EXCEPT WARRANTY OF TITLE AND FOR THE WARRANTIES EXPRESSLY SET FORTH IN HEREIN, IT IS UNDERSTOOD AND AGREED THAT:

(A) SKF MAKES NO OTHER WARRANTY, REPRESENTATION OR INDEMNIFICATION, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT;

(B) IN NO EVENT SHALL SKF BE LIABLE OR OBLIGATED FOR SPECIAL, EXEMPLARY, PUNITIVE, INCIDENTAL, DIRECT, INDIRECT, GENERAL OR CONSEQUENTIAL DAMAGES (INCLUDING, BY WAY OF EXAMPLE ONLY, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR LOSS OF USE) OR ANY OTHER LOSS, COST OR EXPENSE IN CONNECTION WITH THE PRODUCTS AND RELATED SERVICES, IF ANY, PROVIDED BY SKF, AND THIS DISCLAIMER SHALL EXTEND AS WELL TO ANY LIABILITY FOR NONPERFORMANCE CAUSED BY SKF'S GROSS OR ORDINARY NEGLIGENCE, AND IN ALL CASES REGARDLESS OF WHETHER OR NOT ANY OF THE FOREGOING WERE FORESEEABLE OR THAT SKF WAS ADVISED AS TO THE POSSIBILITY OF SUCH DAMAGES, LOSS, COST, OR EXPENSE; AND

(C) NO PERSON HAS BEEN AUTHORIZED BY SKF TO MAKE ANY FURTHER OR CONTRARY INDEMNITIES, REPRESENTATIONS OR WARRANTIES ON BEHALF OF SKF. THE FOREGOING LIMITATIONS AND DISCLAIMERS OF LIABILITY SHALL BE MADE APPLICABLE TO THE SALE OF ANY PRODUCT BY SKF TO THE FURTHEST EXTENT PERMITTED BY APPLICABLE LAW.

The exclusive remedies provided in this limited warranty shall not be deemed to have failed of their essential purpose so long as SKF is willing and able to perform to the extent and in the manner prescribed in this limited warranty.

CM-F0001 EN
Revision ZA, April 2018