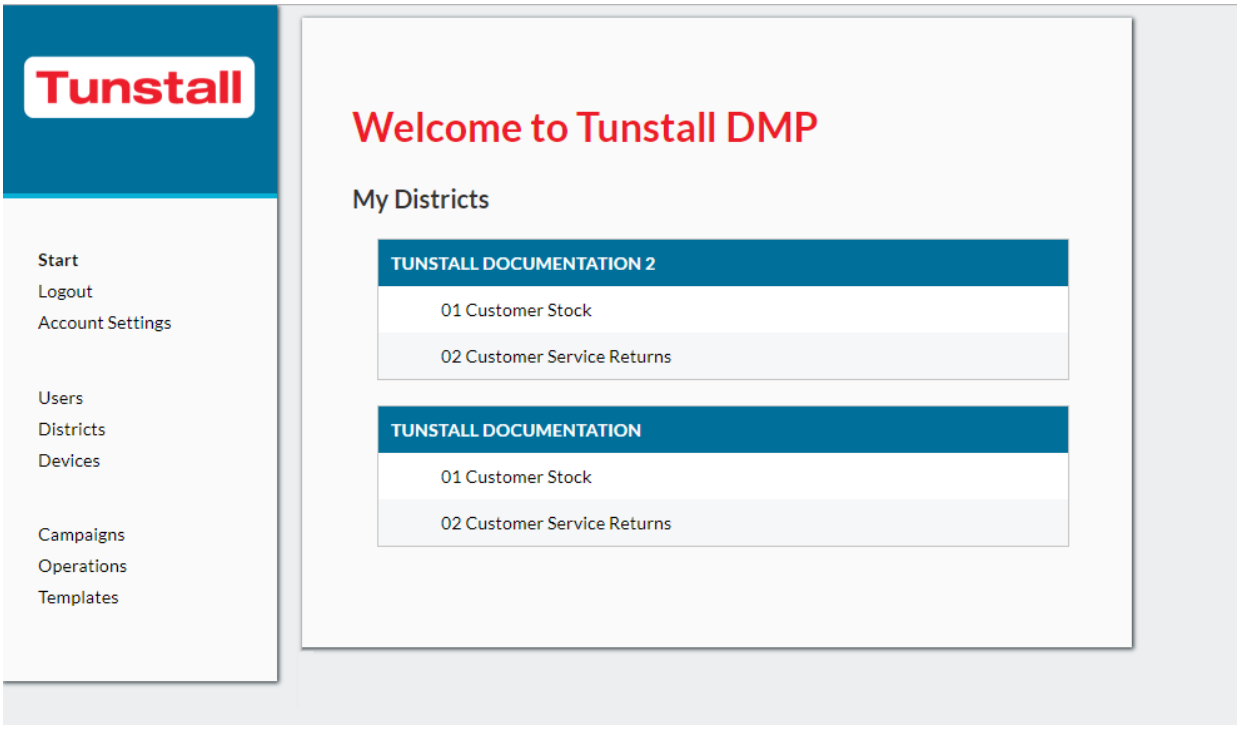
Tunstall

Enabling independent living

Lifeline Smart Hub™ & Device Management Platform



DMP Reference Guide

Contents

Appendices

1 Introduction

1.1 Document purpose

This document describes the Device Management Platform (DMP) and operations you can perform within it. These include both the operations relating to devices defined within the application, including their configuration, and the administration of DMP itself.

1.1.1 Versions

This document reflects DMP version 2.9.9 and Smart Hub firmware version 5.8.8 and related configuration schema version 5.7.3

1.2 Overview

DMP is a cloud-based system which enables secure, remote management of Lifeline Smart Hub™ and Connected Care devices.

The Lifeline Smart Hub is Tunstall's latest home device. It can communicate using digital (IP) protocols over cellular/mobile networks and fixed line broadband. Enabling users to access help 24 hours a day by pressing a button on the device, or from elsewhere in their home by using a radio pendant worn on the wrist or neck.

1.2.1 Smart Hub configuration using DMP

A unique identifier and associated DMP record are automatically created for each Smart Hub when manufactured. This enables DMP to manage the device throughout its lifecycle. The DMP record includes the current configuration of the Smart Hub as well as details of its firmware, district, status and events.

You can use templates to configure devices with default configuration settings. This reduces the number of new settings and changes needed on installation to make the device operational.

Note: DMP does not play any role in the telecare alarm calls handling. It also does not hold records relating to the Smart Hub user.

Smart Hub identification numbers

Each Smart Hub has a unique identification number, fixed at manufacture. This is the number labelled 'Product Code', found on the base of the Smart Hub. Known as the Product Record Code (PRC), DMP uses this number when communicating with the device, for stock item identification, and to ensure full product traceability.

Smart Hubs may also have 'local' identification numbers for communicating with monitoring centres. This enables the service provider to use their existing numbering scheme, and for the device to be compatible with the legacy communication protocols used by the monitoring centres. If a Smart Hub communicates with multiple monitoring centres, it can have different 'local' identification numbers for each destination. Conversely, different Smart Hubs may be given the same 'local' identifier by different monitoring centres and service providers.

Each monitoring system must include the device's Product Code (PRC) number. This enables monitoring centre personnel, familiar with the 'local' identification schemes, to select the device in

DMP when checking its status or making configuration changes. Typically, the PRC is held in a dedicated field or included in a 'Note' field.

Configuration records

DMP holds a record of each Smart Hub's configuration. This can be extremely helpful if a Smart Hub becomes damaged and needs to be replaced as you can quickly apply the original configuration to a new device. It also means that you can view a device's configuration and history, even if the device is disconnected, so helping to resolve technical issues.

DMP initially saves any configuration changes to the DMP record of the device and not to the device itself. When the Smart Hub next contacts DMP, DMP downloads the configuration changes to the device where they are installed. Typically, this is when the device sends DMP a 'heartbeat'. This type of communication occurs at regular intervals and reports on the current status of the device. You can also force the device to communicate with DMP without waiting for the next timed heartbeat, by pressing the green **Cancel** button.

Templates

DMP allows you to create templates which define the value of one or more configuration settings. You can apply a template to multiple devices in one operation, thereby creating a set of devices with the same values for the configuration settings defined by the template. This reduces the number of new settings and changes needed to make the devices operational and ready for the user. Refer to Section 7, Working with device configuration settings, for an overview of the device's configurable features.

1.2.2 Firmware updates

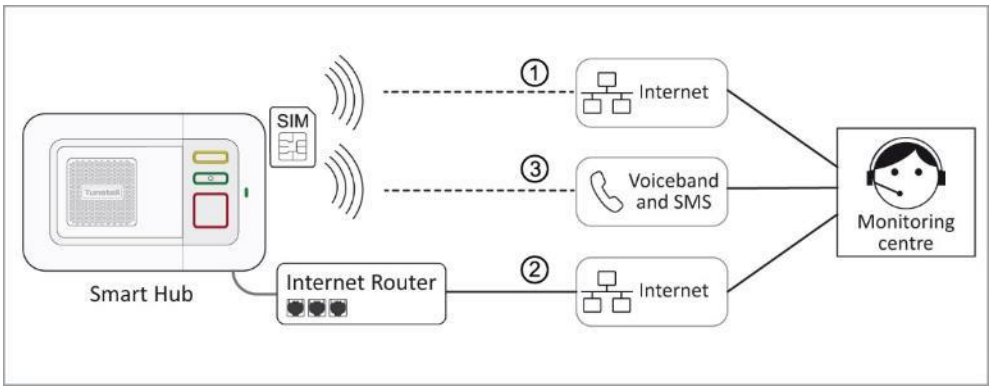
Firmware is the software that is embedded into each Smart Hub. It controls how the device behaves. New firmware typically contains enhancements, new features and protection from new security threats. DMP notifies users of the availability of the new firmware. You can then set up campaigns to roll out the new firmware across your Smart Hub devices.

1.2.3 Smart Hub communication methods

Monitoring centre and Smart Hub

A Smart Hub has three methods of connection to the monitoring centre, so that an alternative method may be used if one or of the others are unavailable. It can communicate:

1. Across a cellular data network to access the internet for communication of data
2. Using an ethernet/fixed broadband line to access the internet for communication of data, including Voice over Internet Protocol (VoIP)
3. Across a cellular network for voiceband, that is, voice, 'tones' and SMS communication.



Communication over cellular connection paths (1 & 3) uses a network accessed by the SIM card. They are used to transmit both data, such as alarm information, and voice calls between the Smart Hub and monitoring centre. In some instances, path 3 can also be used to transmit the alarm call data in the form of an SMS message. Typically, devices can 'roam' between networks, thus maximising coverage and availability. For data transmissions, this method of connection is like accessing the internet on a smart phone network (whilst not on a Wi-Fi), and for making a voiceband call (mobile phone call).

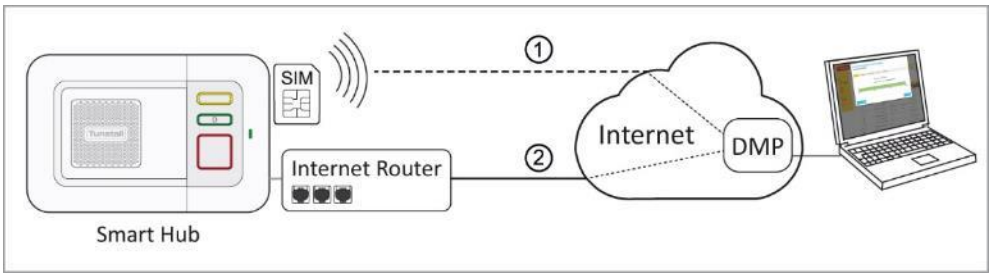
An ethernet/fixed broadband line (2) directly connects the internet to the device, via the user's own domestic or other local broadband router. This can be used to transmit both IP data, such as alarm calls, and VoIP calls between the operator and the Smart Hub user. This method of connection is like using any other device to access the internet via a fixed broadband line.

Domestic broadband connections can be unreliable, especially in the case of a mains power failure to the router/modem. However, cellular services usually remain available, providing the device is within the coverage area of an accessible network. Because of this, Tunstall recommends that you do not rely solely on a domestic ethernet/fixed broadband connection.

DMP and Smart Hub

A Smart Hub has two methods of accessing the internet for connection to DMP. It can communicate:

1. Across a cellular data network
2. Using an ethernet/fixed broadband line.



The connection is used to transmit data such as heartbeats, firmware and configuration updates between DMP and the Smart Hub.

1.2.4 Administering DMP

To support the management of Smart Hub devices, DMP provides facilities to:

- Create and maintain district definitions, which you use to group the devices and control access to them within DMP
- Create and maintain users, including their permission profiles to the districts
- Create and maintain template definitions that are used to re-configure multiple devices in a single operation
- Create and maintain campaign definitions that control the update of devices' firmware.

1.3 Typographical conventions

- Fields, radio buttons etc are shown in **bold**.
- References, including those to external documents, are shown in *italics*.
- Any hyperlinks are shown in teal.
- Notes will be indicated by;

  Note: With extra information to consider.

- Warnings are indicated by the  icon and have rule lines both above and below their text.

1.4 Related documents

Part No	Title
D5727050E	Lifeline Smart Hub Installation Guide
D5727002A	Lifeline Smart Hub™ User Guide - Australia
D5727004A	Lifeline Smart Hub™ Short Guide – Germany
D5727007A	Lifeline Smart Hub™ User Guide – UK
D5727008A	Lifeline Smart Hub™ User Guide – Europe-wide

2 Accessing DMP

2.1 Introduction

Before you can access the Device Management Platform (DMP), you must have a valid email address and pass this on to your DMP administrator. Your DMP administrator uses this email address as your username when they create your DMP user account.

Once you have been added to DMP, you receive an email instructing you on how to generate a password and log on to the system.

You access DMP via an internet browser such as Edge, Internet Explorer, Safari or Firefox, with Chrome being the preferred browser.

DMP is located at:

- Australia: https://dmp-au.tunstall.com
- China: https://dmp-cn.tunstall.com
- Europe: https://dmp-eu.tunstall.com

On entry to DMP, you see the Start page which lists the actions you can take within DMP and the scope of the data you can access. You may be restricted to a single district, several districts within a single customer or even districts across multiple customers. For details refer to Section 4, Working with customers and districts.

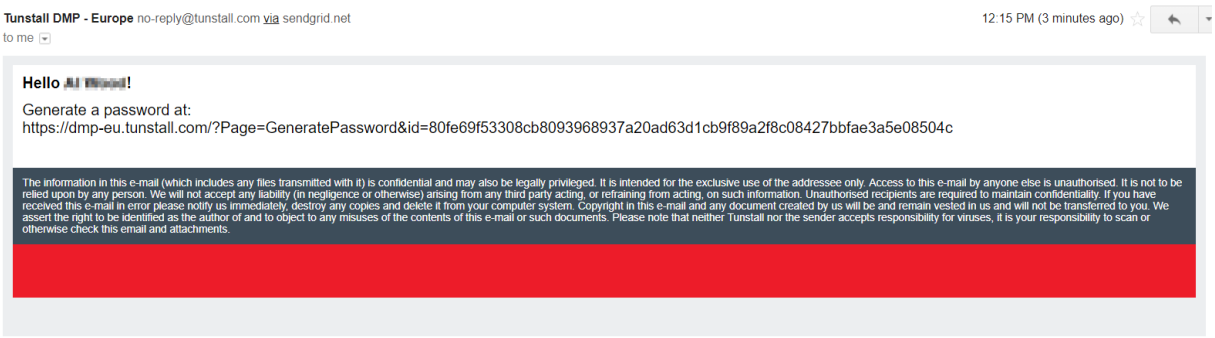
The descriptions and graphics in this manual relate to the most complex scenario, namely they describe the actions you take if you have access to multiple districts across multiple customers. Typically, you will only be working with a single customer. In this case, you will see no reference to a specific customer, or any customer-related field, such as the ones that you use to filter lists. Similarly, if you work within a single district, you will see no filters at district level, etc.

2.2 Generating a DMP password

You receive an email inviting you to generate a password whenever:

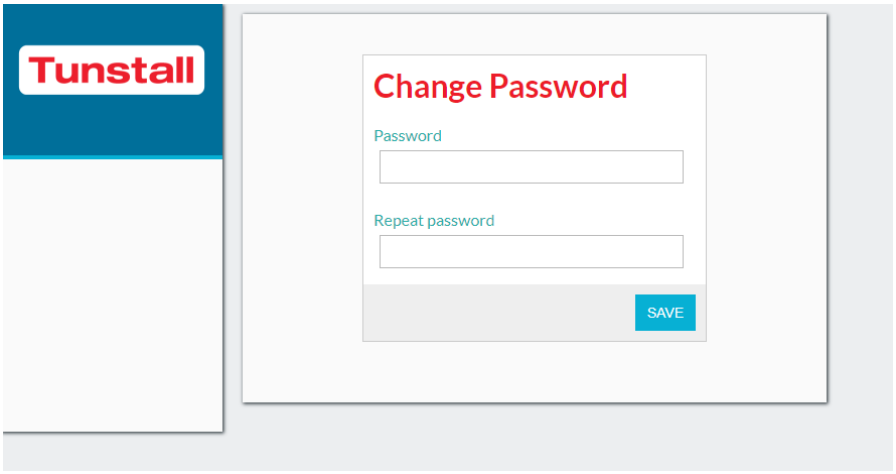
- your administrator creates your account on DMP
- you click **Forgot password?** on the DMP login page
- your password has been in use for almost 90 days and so is close to expiring.

The email will be like the following:



To generate a password:

1. Either click the link in the email or paste it into the address bar of your browser and press **Return**. This displays the Change Password page:



2. Choose a password and enter it in both fields. Your password must be a minimum of eight characters.
3. Click **SAVE**. You now see the Start page of DMP.

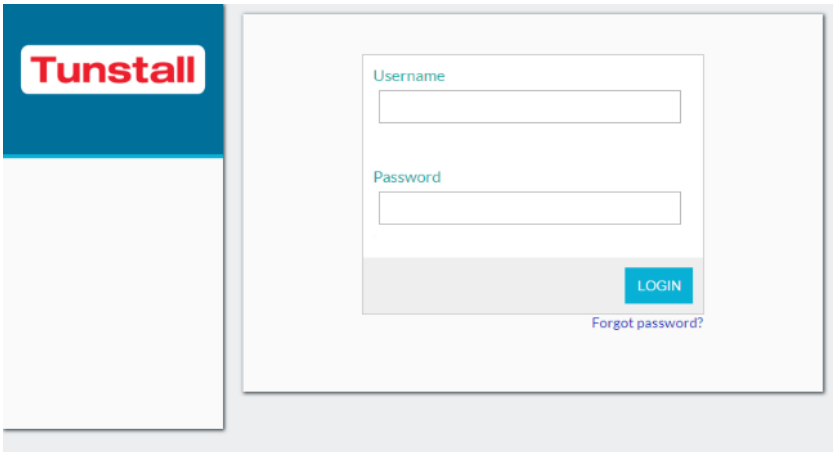
Note: Every 90 days your DMP password expires, DMP will automatically email you as the deadline approaches so that you can generate a new one.

2.3 Logging in to DMP

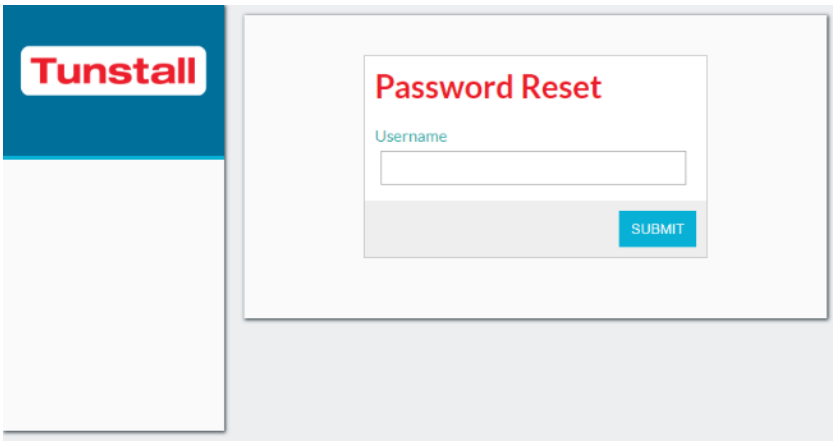
To log in to DMP:

1. Enter the appropriate DMP URL for your region in the address bar of the internet browser, as listed in Section 2.1, Introduction.

   The DMP login page is displayed:



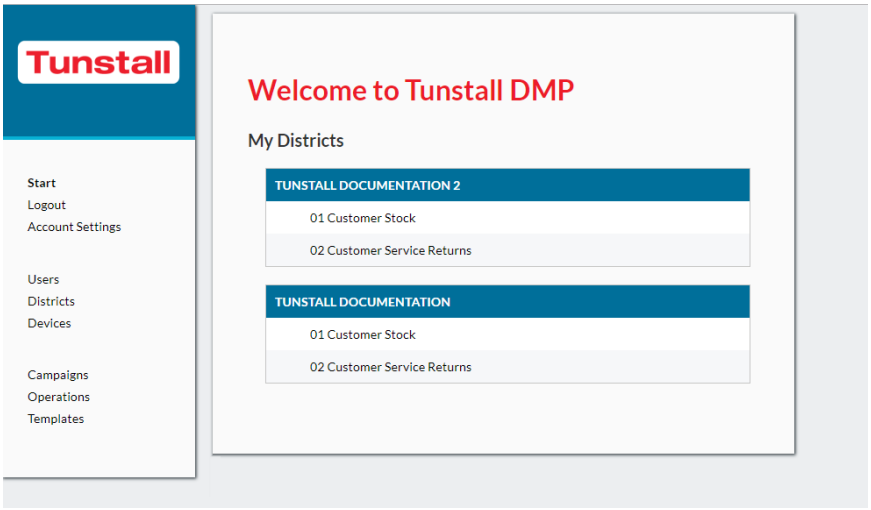
2. Enter your username, which is in the form of an email address.
3. Enter your password and click **LOGIN** to enter DMP and view the Start page.
4. If you cannot remember your password, click **Forgotten password?** You see the following page:



5. Enter your username and click **SUBMIT**. DMP sends an email to the associated email address and you can generate a new password and enter DMP as described in the previous section.

2.4 DMP Start page

You see the DMP Start page, like the one shown below, whenever you log on.



The main part of the page lists the districts to which you have access. If these districts belong to different customers then you see them grouped by customer, as shown above. DMP displays a menu on the left-hand side of the page. This lists the types of information you can access and maintain within these districts. The list depends on the permission profile your administrator gives you for each district.

All users of DMP can:

- view and maintain their own account details
- log out of DMP
- return to the Start page.

If you have access to one or more districts as a 'Customer Basic' user, then for those districts you can also:

- view and maintain devices located within your districts
- view a list of campaigns associated with your districts
- perform additional operations on the devices held within your districts
- view a list of templates associated with the customers of your districts.

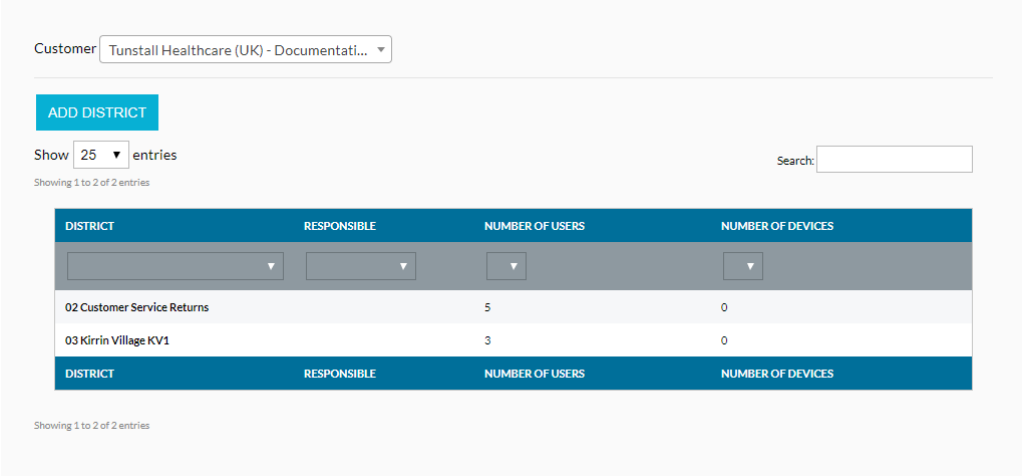
If you have access to at least one district as a 'Customer Advanced' user, then for all your districts you can perform all the 'Customer Basic' operations plus:

- view and maintain the permission profiles of users who belong to the customers related to your districts
- view and maintain the districts and add new ones associated with the customers related to your districts
- maintain templates associated with the customers that own your districts.

For details of the individual operations associated with each permission profile, refer to Appendix A, Permission profiles.

2.5 Using standard list actions

DMP displays much of its information in the form of lists. See below for an example of how it displays districts:



DMP provides a standard set of features to manipulate the display of list data. You can:

- Change the number of entries displayed on a page by choosing a value from the **Show entries** drop-down list
- If you have access to multiple customers/districts, filter the entries by selecting the appropriate customer and/or district
- Filter the list by selecting an option from the drop-down below a column heading
- Sort the list by clicking on a column heading at the top of the list
- Search the list by entering the relevant text in the **Search** field. DMP searches for that character string appearing anywhere within a row. The search is not case-sensitive. For example, when viewing a list of users and searching for someone with the name of 'Shaw' by entering 'sh', this will bring up not only '**Sh**aw' but also 'Dalgli**sh**' and anyone whose language is 'Engli**sh**'.

In addition, some pages may have their own advanced filters. These are described within the relevant page descriptions in this document.

2.6 Logging out of DMP

It is recommended that when you have finished using DMP, you leave the application by clicking the **Logout** option and then closing the browser. This is especially important when using a computer that is accessed by multiple users.

3 Maintaining your DMP user account settings

3.1 Introduction

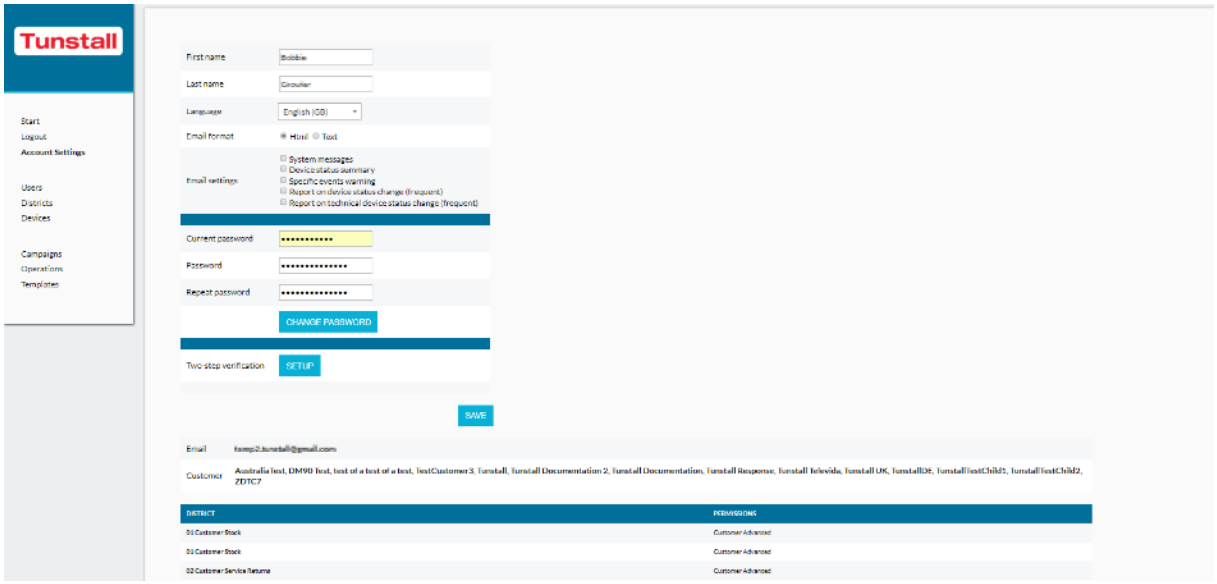
DMP allows you to change most of your personal data held within the system, the only exception being the email address you use to log on to DMP.

In addition, your organisation may use two-step verification for some DMP operations. To use this feature, you must have the Google Authenticator application on your phone or similar device and have registered your DMP user account with Google Authenticator. You can download this application from the Apple App Store, Google Play or Google Account Help.

Once set up, Google Authenticator provides a constantly updating verification code which you enter before you perform the selected operations.

3.2 Account Settings page

You access this page by clicking the **Account Settings** option on the main menu.



This page displays all your general account settings, plus the permission profile of each district you can access and their associated customers.

In addition, **Email settings** controls which email types you receive, including notification of status report production. The three status reports DMP produces are:

- **Device status summary report** – a district-level report which lists each device within the district, together with their current status; typically produced once a day but can be at more frequent intervals
- **Device status change report** – produced whenever a device changes its status and details the device and status change
- **Device technical status change report** – produced whenever a device changes its status and details the device and status change.

If you have a permission profile that is not 'Customer Advanced' or 'Customer Basic', for example 'Base Profile', then it appears as 'Unknown' on the Account Settings page.

Within this page you can:

- Change your general settings by amending their values and then clicking **SAVE**
- Change your password
- Initiate two-step verification setup by clicking **SETUP**. This displays the two-step verification window where you register your user account with Google Authenticator.

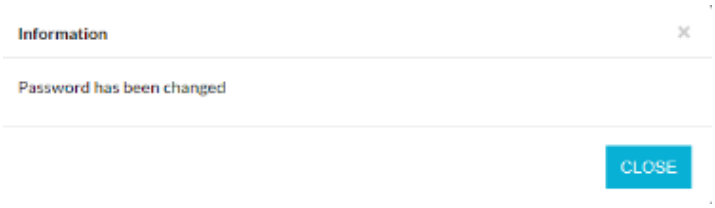
Note: This operation is not available if you have a 'Base Profile' permission profile.

- Initiate display of your QR code by clicking **VIEW QR CODE**. This displays your verification bar code, which you can use to register your DMP account with another device running Google Authenticator.

Note: This operation is not available if you have a 'Base Profile' permission profile.

3.2.1 Changing your password

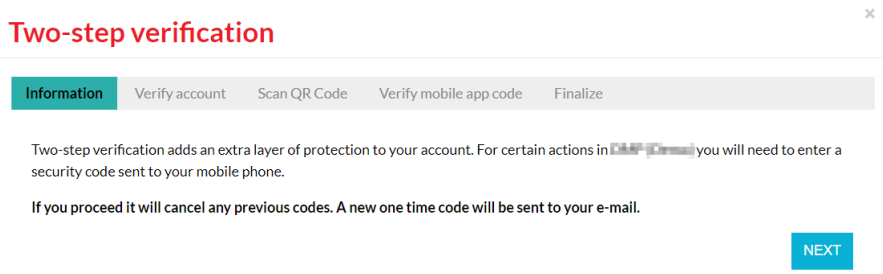
1. Type the new password in the **Password** and **Repeat Password** fields.
2. Click **CHANGE PASSWORD**. DMP displays a confirmation message:



3. Click **Close**. You can now use your new password to access DMP.

3.3 Two-step Verification window

You use the Two-step Verification window to register your DMP account with Google Authenticator so that you can access the DMP operations that use this feature.

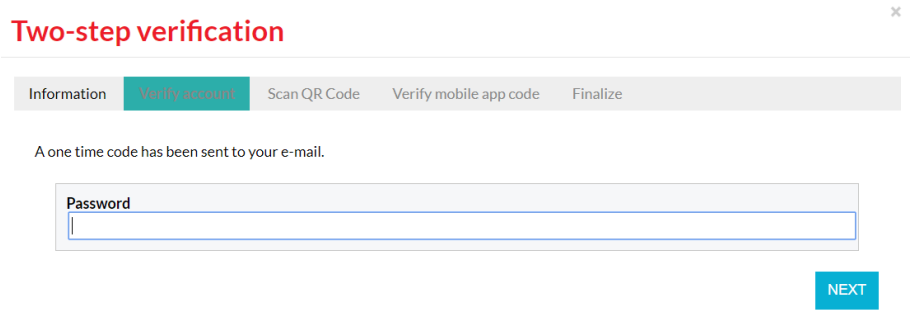


You access this window by:

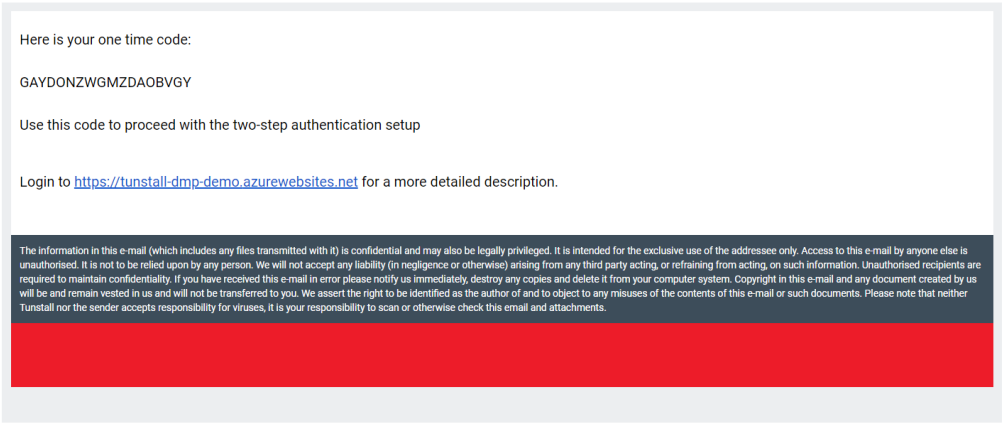
- Clicking **Account Settings** option on the main menu
- Clicking **SETUP** on the Account Settings page.

To register your account with Google Authenticator:

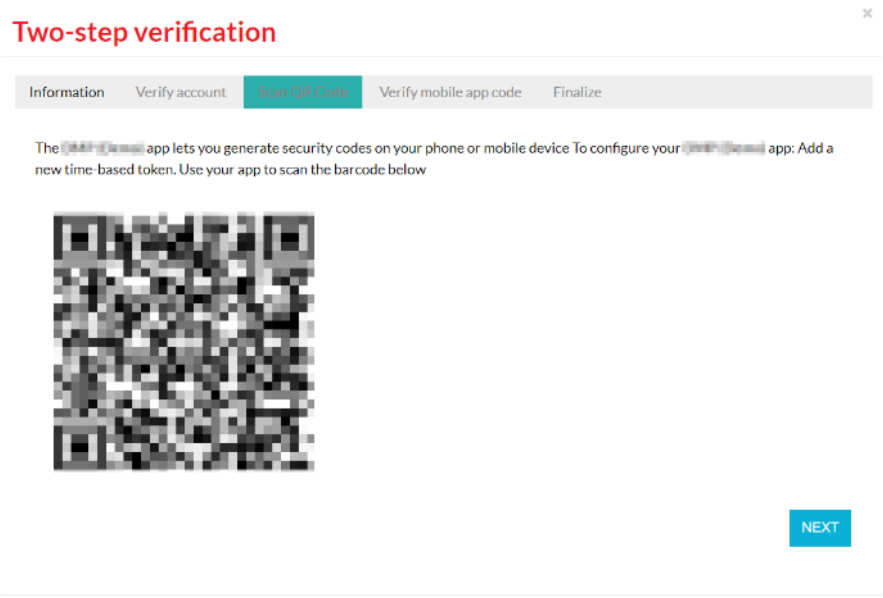
1. Click **NEXT**. DMP displays the following:



2. Go to your email and wait for the one-time code. DMP sends an email, like the following:



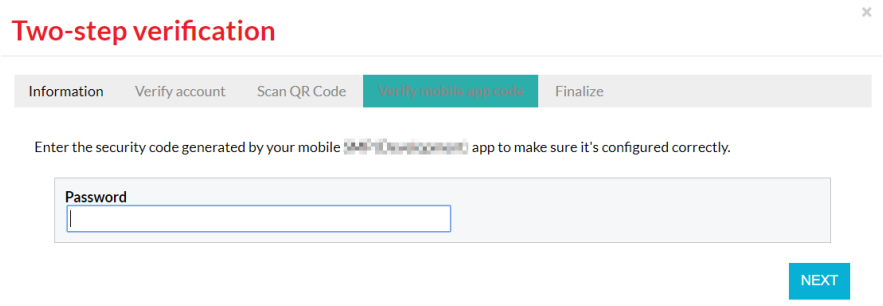
3. Copy the code into the **Password** field of the DMP window and click **NEXT**. DMP then generates the relevant QR (bar) code. This may take some time, but once generated, DMP displays the code as shown below:



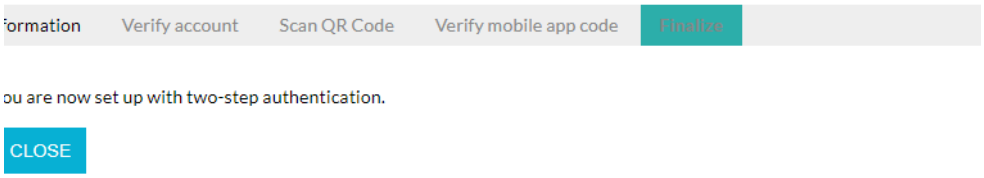
4. Open Google Authenticator and use it to scan the QR code. If this is the first time you have used Google authentication, you are guided by the application through the scanning process. If you have used Google Authenticator before, click the '+' button, select 'Scan barcode' and then hold your mobile phone over the QR code to scan it.

   Google Authenticator displays the name of your DMP system, your token value and the email address you use to access DMP. The token changes at regular intervals.

5. Click **NEXT**. DMP displays a field for you to test your two-step verification.



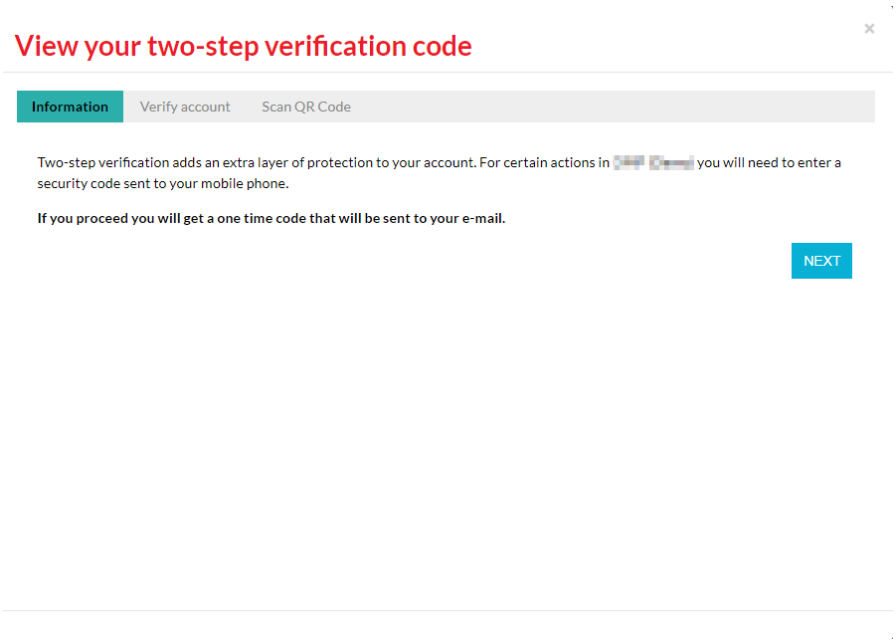
6. Enter the Google Authenticator token currently displayed on your mobile phone. Do not leave a space between any of the six numbers.
7. Click **NEXT**. DMP authenticates the token, and on successful authentication, displays the following page:



8. Click **CLOSE** to complete the operation.

3.4 QR Code window

You use the QR Code window to register your DMP account with Google Authenticator on another device, or re-register with your original device. This operation is only available once you have set up two-step verification.

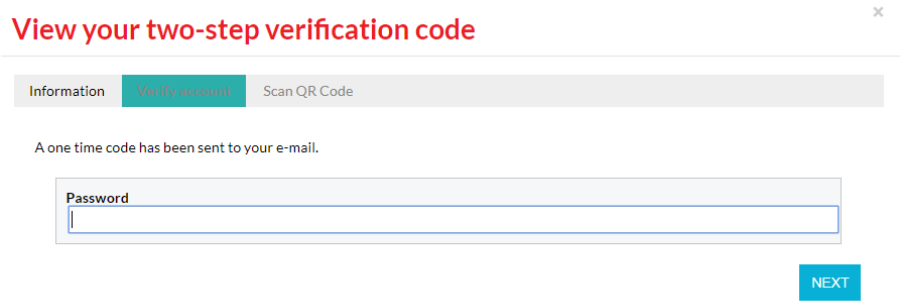


You access this window by:

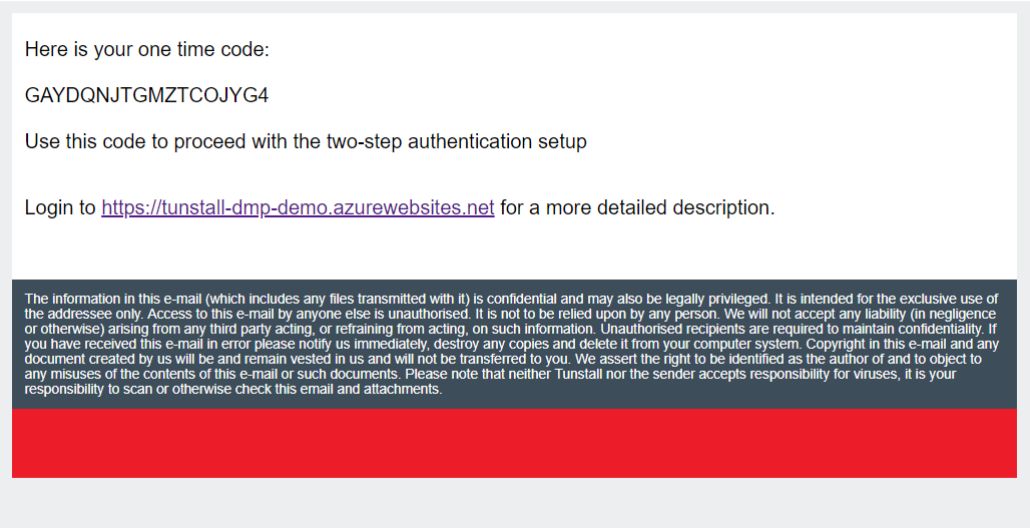
- Clicking **Account Settings** option on the main menu
- Clicking **VIEW QR CODE** on the Account Settings page.

To re-register your account or to register your account with another device using Google Authenticator:

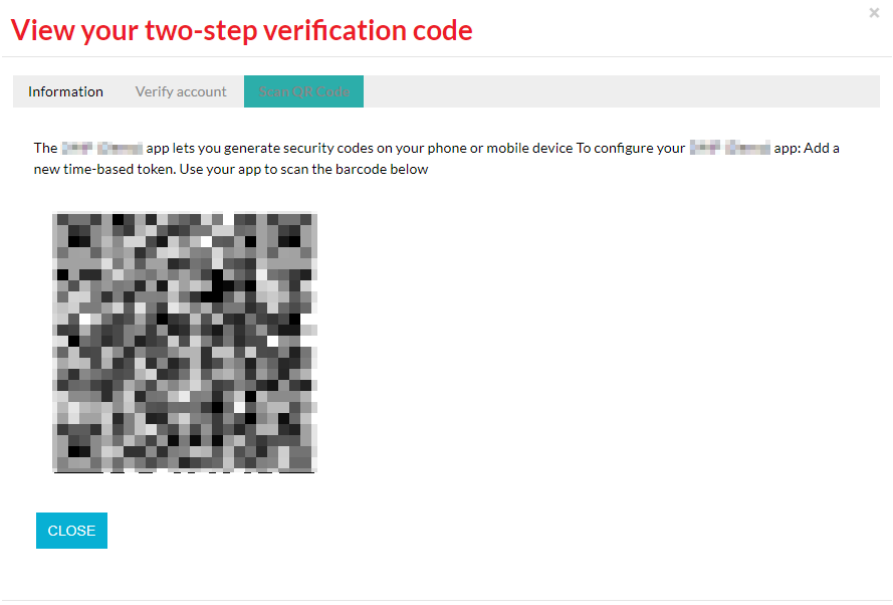
1. Click **NEXT**. DMP displays the following:



2. Go to your email account and wait for the one-time code. DMP sends an email, like the following:



3. Copy the code into the **Password** field of the DMP window and click **NEXT**. DMP then generates the relevant QR (bar) code. Once generated, DMP displays the code as shown below:



4. Open Google Authenticator and use it to scan the QR code. Within Google Authenticator, click the '+' button, select 'Scan barcode' and then hold the phone over the QR code to scan it.
5. Click **CLOSE**.

4 Working with customers and districts

4.1 Introduction

Most users only work with devices belonging to one customer, namely their own organisation. In this case, they see no reference to customers within DMP. For example, although their Start page lists the one or more districts they can access, the View Districts List page does not have a **Customer** field.

Where an organisation administers devices on behalf of multiple customers, some users may perform administration on behalf of several customers. In this case, their Start page contains the list of customers and districts they can access and, when working within DMP, they specify the appropriate customer before each operation they perform.

Customers are arranged in hierarchies, with each customer having a single 'parent' customer. DMP uses this hierarchy to determine which customers and districts can be viewed by users with 'Customer Advanced' permission profiles.

Each customer has a set of sub-groups known as districts. These districts define how Smart Hubs are grouped together in DMP. By default, each customer has the following districts:

- **01 Customer Stock**
  This is the district where all new Smart Hubs are located when purchased from Tunstall.
- **02 Customer Service Returns**
  This district is used to locate Smart Hubs which have been returned to Tunstall within a device's warranty period.

Note: These default districts must not be renamed, edited or deleted as they are required as part of the supplier logistics process when receiving or returning Smart Hubs.

If you have a 'Customer Advanced' permission profile, you can administer the set of districts associated with each of your customers. You can create any number of additional districts. Typically, these additional districts define a geographical area, using either full or partial postal codes depending on the number of devices in the locality, for example 'DN4'.

Using postal codes as a method of grouping devices allows for improved error diagnostics as you can rule out environmental factors. For example, if all the devices within district 'DN4' are reporting "mains failure" it is likely that it is a localised power failure and not a Smart Hub error.

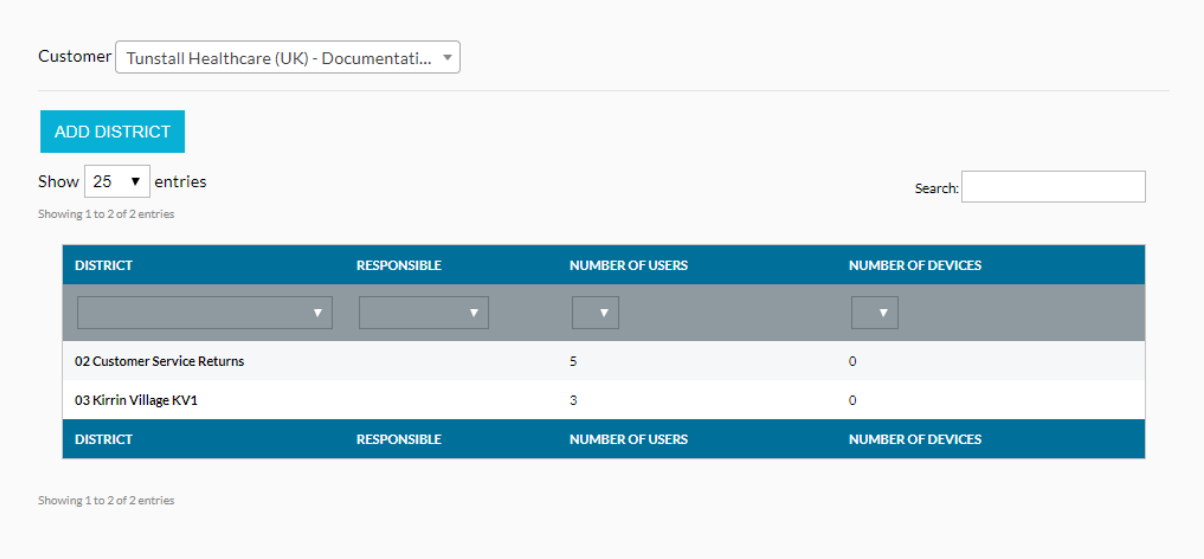
As part of each district definition you specify:

- the personnel responsible for it, together with their contact details
- how DMP is to respond to missed heartbeats and errors reported by the units held within the district
- the permission profiles of the users that can access it.

In addition, you can also view details of any changes of status by each device held within the district.

4.2 View Districts List page

You use this page to view and maintain the details of districts.



You access this page by clicking the **Districts** option on the main menu. This option is only available to users with at least one 'Customer Advanced' permission profile.

The page initially lists the districts alphabetically by name. If you have districts belonging to more than one customer, then you initially see those districts belonging to whichever customer appears first on your DMP Start page.

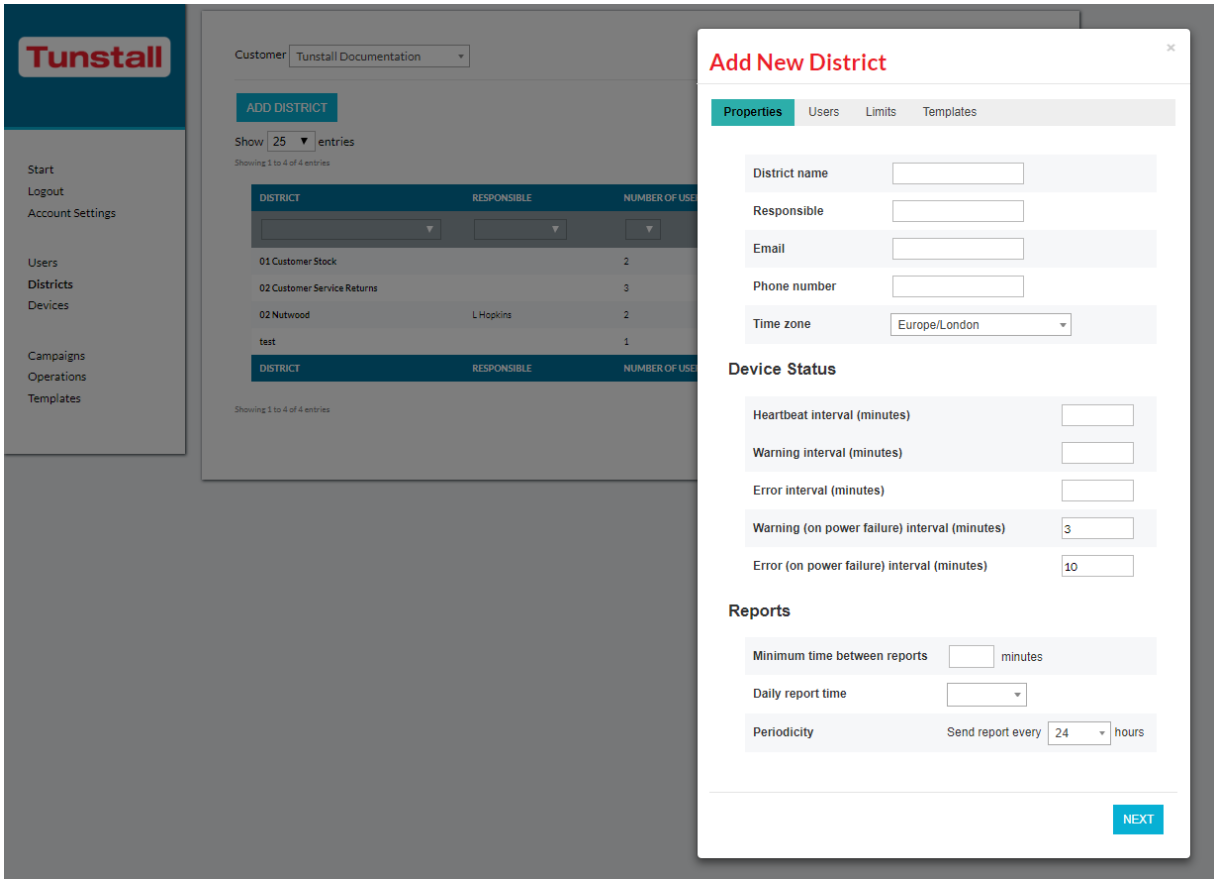
Within this page you can:

- Use the standard table actions to filter, sort and search through the list
- Initiate the creation of a new district by clicking **ADD DISTRICT**. DMP opens an Add New District window for you to specify the district. On creation of the new district, DMP allocates it to the customer to which the districts currently displayed belong.
- Initiate the display/edit of a district by clicking anywhere within its details. DMP opens an Edit District window containing the details of the selected district.

4.3 Add New District window

You use this window to create a new district including:

- general details
- device status parameters
- controls for the generation of device status reports
- users who may access it, together with their permission profiles
- warning state levels and timings to apply to devices in the district
- any templates that may be applied to devices in the district.



You access this window by:

- Clicking the **Districts** option on the main menu – only available to users with at least one 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you maintain districts for more than one customer
- Clicking **ADD DISTRICT**.

The window comprises four tabs which are described below.

To create a new district:

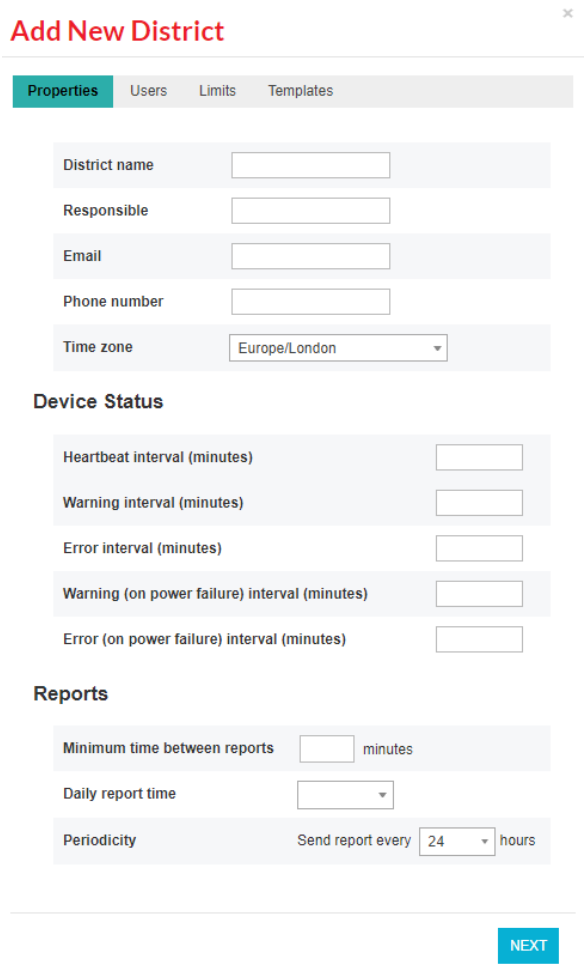
1. Complete the general, device status and report parameters on the **Properties** tab.

2. Click **NEXT**. This automatically displays the **Users** tab.
3. Specify the users that are to access the district and their permission profiles.
4. Go to the **Limits** tab and check that the warning state levels and timings are set to the correct defaults.
5. If required, go to the **Templates** tab and add all the templates that may be applied to devices in the district.
6. Click **SAVE**.

   DMP closes the window, saves the details of the new district and updates the View Districts List page to include the new district.

4.3.1 Properties tab

You use the **Properties** tab to specify the general details of the district, its device status parameters and the controls for report production.



When creating a district, complete all the fields on this tab, and then click **NEXT** to move on to the **Users** tab.

When editing a district, you make the required changes and then either click another tab to make additional changes or click **SAVE** to save any changes you have made over the four tabs.

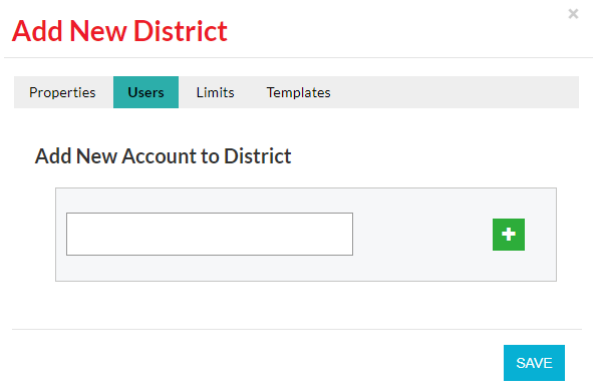
Note: Please consult with your supplier if you wish to use a different interval to those listed below before entering them into DMP.

Field	Description
District name	The name of the district where the Smart Hub devices are to be installed. Typically, this indicates the geographical location of the devices within the district and often incorporates a postal code, for example, 'Leeds LS1'.
Responsible	Defines who, within the customer's organisation, is responsible for the district. Typically, this is a DMP user with a 'Customer Advanced' permission profile for the district.
Email	The email address to which DMP sends system-generated reports relating to the district. Typically, this is a group email address accessed by the personnel responsible for the district.
Phone number	Optional. The phone number of the person responsible for the district.
Time zone	The time zone of the district e.g. 'Leeds LS1' has time zone 'Europe/London'.
Device Status	
Heartbeat interval	Defines in minutes how often DMP expects devices in this district to send a heartbeat to DMP. Should be set to 60.
Warning interval	The amount of time in minutes, starting from the receipt of a heartbeat, that DMP is to wait for the next heartbeat from a device using mains power. If no heartbeat is received from the device before the end of the warning interval, then DMP: • sets the device to a warning status, indicated by a yellow icon • sends a warning email to the address specified in **Email.** Should be set to 75. This must be several minutes longer than **Heartbeat interval** to allow for short-term communication problems.
Error interval	The amount of time in minutes, starting from the receipt of a heartbeat, that DMP is to wait for the next heartbeat from a device using mains power. If no heartbeat is received from the device before the end of the error interval, then DMP: • sets the device to an error status, indicated by a red icon • sends an error email to the address specified in **Email.** Should be set to 150. This should be significantly longer than **Warning interval**.

Field	Description
Warning (on power failure) interval	The amount of time in minutes, starting from the receipt of a heartbeat, that DMP is to wait for the next heartbeat from a device using battery power. If no heartbeat is received from the device before the end of the warning interval, then DMP: • sets the device to a warning status, indicated by a yellow icon • sends a warning email to the address specified in **Email.** Should be set to 75. This must be several minutes longer than **Heartbeat interval** to allow for short-term communication problems.
Error (on power failure) interval	The amount of time in minutes, starting from the receipt of a heartbeat, that DMP is to wait for the next heartbeat from a device using battery power. If no heartbeat is received from the device before the end of the error interval, then DMP: • sets the device to an error status, indicated by a red icon • sends an error email to the address specified in **Email** Should be set to 150. This should be significantly longer than **Warning (on power failure) interval**.
Reports	Controls the production of the **Device status change**, **Technical device status change** and **Device status summary** reports.
Minimum time between reports	Typically, DMP produces **Device status change** or **Technical device status change** reports every time there is a change of state or technical state respectively. However, if the time period between two changes is less than the interval, in minutes, stated here, then no report will be generated for the second change until the minimum time is reached. DMP will then generate a report containing details of all changes that occurred within the interval. Default is 20.
Daily report time	Defines the time the first **Device status summary** report is generated each day. Default is 09:00.
Periodicity	Defines the time period, in hours, between **Device status summary** reports produced during a day. Typically left at the default of 24 so that there is a daily summary of each device's status. Default is 24.

4.3.2 Users tab

You use the **Users** tab to link existing users to the district.



If adding a district, this tab is initially blank. If you are editing an existing district it lists the current users with permission profiles for the district.

When adding or editing a district, you set up the required users and their permission profiles and then either:

- click another tab to set up/amend other values, or,
- click **SAVE** to save the district's details.

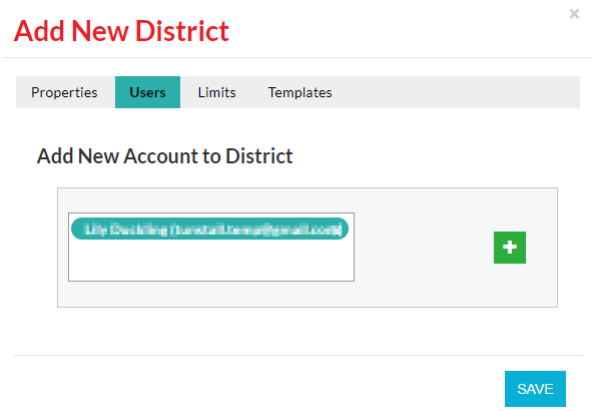
Within this tab you can:

- Add users to the district
- Amend the permission profile of a user account
- Remove a user from the district.

Add users to the district

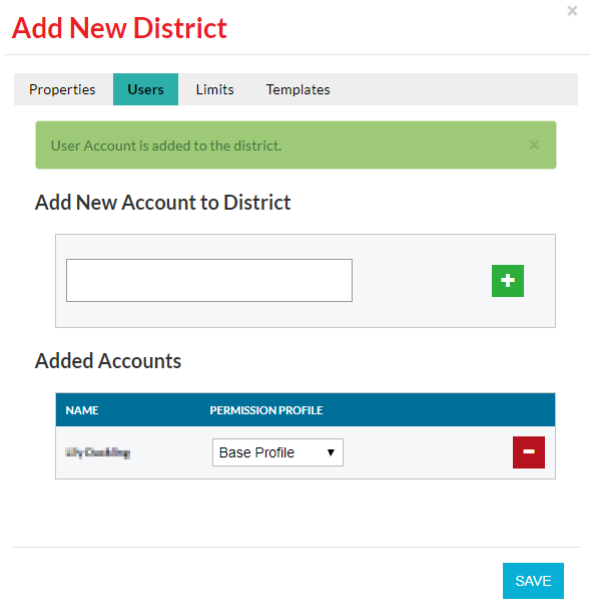
To add users to the district:

1. Partially type the first user's email in the **Add New Account to District** field. DMP lists the users with matching email addresses. If you can access more than one customer, you can see only those users created within the customer currently selected on the View Districts List page.
2. Click the appropriate email address to select it. DMP displays the full username in the **Add New Account to District** field.



3. Repeat steps 1 and 2 until all the users are listed and then click the + button.

   DMP displays each user and their default permission profile in the **Added Accounts** table.



You can now go on to amend their permission profiles and/or remove any user entered in error.

Amend the permission profile of a user

To amend the permission profile of a user, select the appropriate value from the **PERMISSION PROFILE** drop-down list relating to the required user.

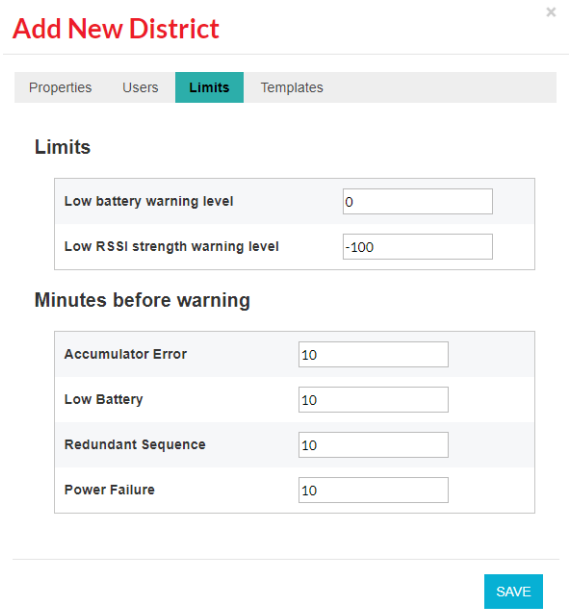
Remove a user account from the district

To remove a user account from the district, click the − button next to their details in the **Added Accounts** table.

4.3.3 Limits tab

You use the **Limits** tab to view the warning state levels and timings applied to devices in the district. These are:

- at what level the device is to generate a warning status for low battery or cellular signal strength
- how long DMP is to wait before setting a device's status to Warning for low battery and other conditions.



When adding or editing a district, you set up the required details and then either:

- click another tab to set up/amend other values, or,
- click **SAVE** to save the district's details.

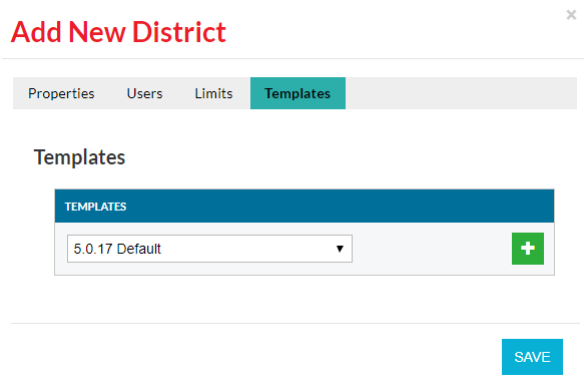
Note: Please consult with your supplier if you wish to use a different value to any of those suggested below before entering it into DMP.

Field	Description
Low battery warning level	Not currently used. Should be set to 0.
Low RSSI strength warning level	The received cellular signal strength at which point DMP will display as 'low signal strength'. Should be set to -100.
Accumulator Error	Defines the number of minutes to elapse between DMP receiving a battery error status from a device, and acting upon that status by changing to a warning state. Should be set to 10.
Low Battery	Defines the number of minutes to elapse between DMP receiving a low battery status from a device, and acting upon that status by changing to a warning state. Should be set to 10.

Field	Description
Redundant Sequence	Defines the number of minutes to elapse between DMP receiving a redundant sequence status from a device and acting upon that status by changing to a warning state. Should be set to 10.
Power Failure	Defines the number of minutes to elapse between DMP receiving a power failure status from a device, and acting upon that status by changing to a warning state. Should be set to 10.

4.3.4 Templates tab

You use the **Templates** tab to specify the templates that may be applied to devices in the district.



If adding a district, this tab is initially blank. If you are editing an existing district, it contains the current templates associated with the district.

When adding or editing a district, you set up the required templates and then either:

- click another tab to set up/amend other values, or,
- click **SAVE** to save the district's details.

Within this tab, you can:

- Enable a template to be applied to devices in the district
- Stop a template from being applied to devices in the district.

Enable a template to be applied to devices in the district

To enable a template to be applied to devices in the district:

1. Select the required template from the drop-down list.
2. Click the + button. The template then appears in the list of templates that can be applied to devices in the district.

Stop a template from being applied to devices in the district

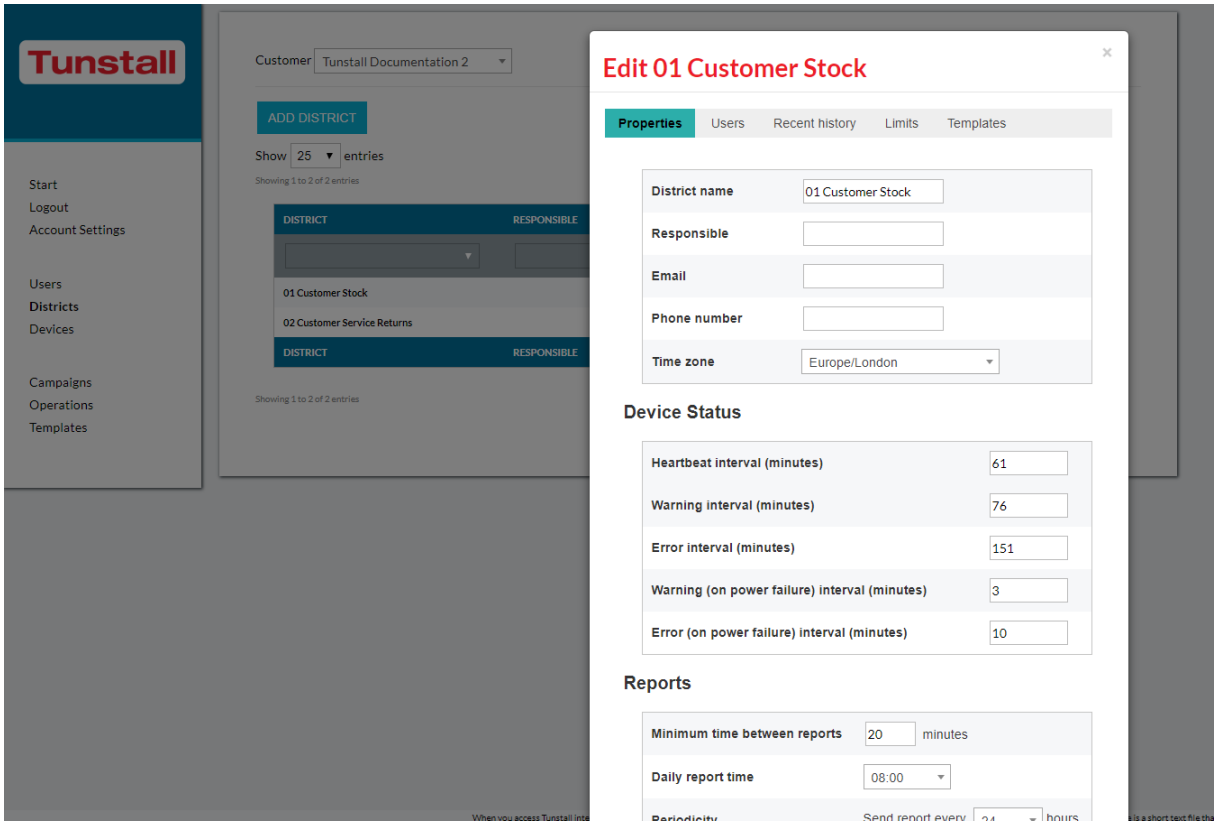
To stop a template from being applied to devices in the district, click the − button beside its name. DMP removes the template from the list and it is no longer available within the district.

4.4 Edit District window

You use this window to view/edit a district's details including:

- general details
- device status parameters
- users who may access it, together with their permission profiles
- warning state levels and timings to apply to devices in the district
- any templates that may be applied to devices in the district.

In addition, you can also use it to view recent changes in status of the devices belonging to the district.



You access this window by:

- Clicking the **Districts** option on the main menu – only available to users with at least one 'Customer Advanced' permission profile
- Clicking within the row containing the details of the district you wish to edit/view.

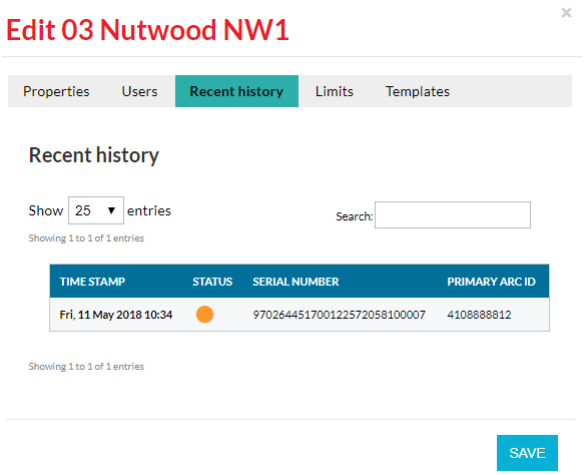
The window comprises five tabs. All the tabs, except for **Recent history**, are described within Section 4.3, Add New District window. The **Recent history** tab is described in the sub-section below.

To view a district's details, select the required tabs in turn and then click **X** in the top-righthand corner of the window.

To edit a district, select the required tabs in turn, make the relevant changes as necessary and then click **SAVE**. DMP closes the window and updates the district's details.

4.4.1 Recent history tab

You use the **Recent history** tab to view any changes in status associated with the district's devices.



Within this tab, you can use the standard table actions to filter, sort and search through the list.

For details on the icon displayed in the **STATUS** column, refer to Appendix B, Heartbeat icons and status.

When you have finished viewing the history, either:

- click another tab to view/amend other values, or,
- if you have made changes on other tabs, click **SAVE** to save the district's details, or,
- if you have not made any changes, click **X** in the top-righthand corner of the window to close it.

5 Working with user accounts

5.1 Introduction

Within DMP, a user account defines:

- general details about the user, including name, password, email address etc.
- which districts, and customers, the user can access, and therefore which devices they can administer and configure
- the set of operations they can perform within DMP, by using permission profiles.

If the administrator creating a user account can only access one customer, then that new account is automatically associated with that customer. If the administrator can access multiple customers, the new account is associated with the customer selected during the creation process.

In the former case, user access can be given to any of the districts owned by the customer. In the latter case, user access can be given to any of the districts owned by either the customer or any of its 'children' within the hierarchy of customers.

The type of access is defined for each district using permission profiles. These are:

- **Customer Basic**
  This allows you to:
  - view and maintain your own account details
  - log out of DMP
  - return to the DMP Start page
  - view and maintain devices located within your districts
  - view a list of campaigns associated with your districts
  - perform additional operations on the devices held within your districts
  - view a list of templates associated with the customers of your districts.
- **Customer Advanced**
  This allows you to:
  - perform any 'Customer Basic' operation
  - view and maintain the permission profiles of users who belong to the customers related to your districts
  - view and maintain the districts and add new ones associated with the customers related to your districts
  - maintain templates associated with the customers that own your districts.

Note: The 'Basic Profile' permission profile gives access to DMP but not to the district. This permission profile is not used in practice.

For details of the individual operations associated with each permission profile, refer to Appendix A, Permission profiles.

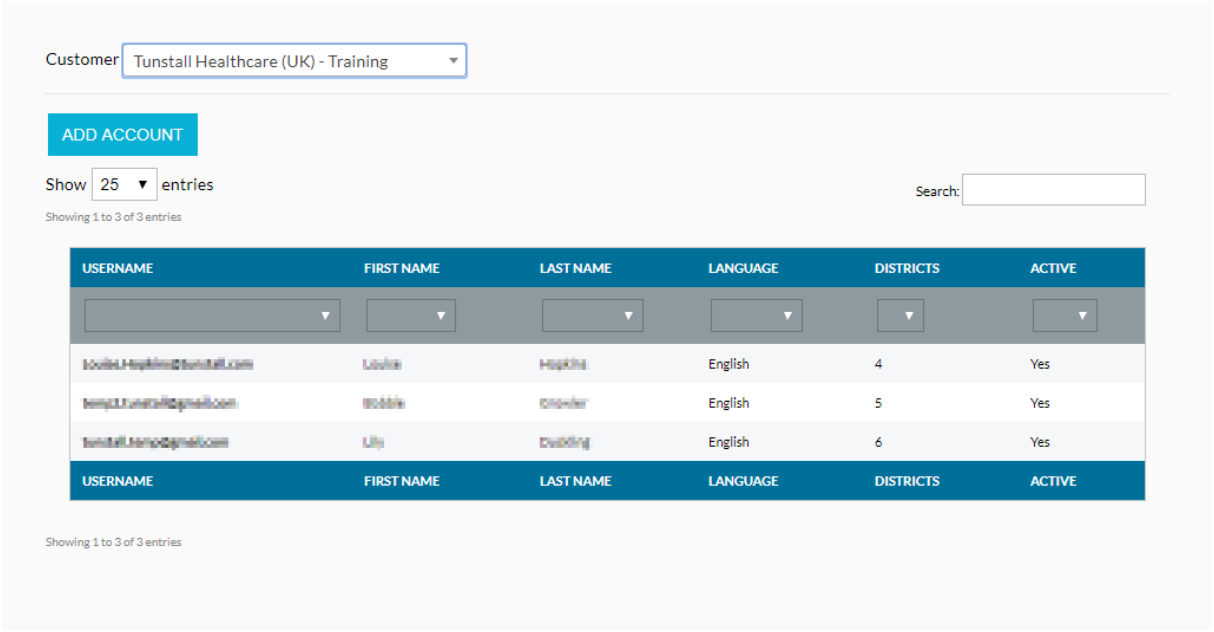
If you set a district's permission profile to 'Customer Basic' for a user, that user can perform operations on devices within that district and other operations relating to the district.

If you set a district's permission profile to 'Customer Advanced' for a user, that user effectively has 'Customer Advanced' permissions for all districts within the current customer. They also have this level of permission for all districts belonging to each of the current customer's 'children', through all levels of the hierarchy. This overrides any permission profiles the user may already have, that apply to other districts belonging to the customer or its 'children'.

5.2 View User Accounts List page

You use this page to view and maintain the details of the user accounts belonging to your customers.

Note: If there are multiple customers, you will not see the user accounts duplicated by district but rather the users associated with the specific customers hierarchy.



You access this page by clicking the **Users** option on the main menu.

Note: This option is only available to users with at least one 'Customer Advanced' permission profile.

The page initially lists the user accounts alphabetically by their username. If you can access more than one customer, you primarily see those users belonging to whichever of those customers appears first on your Start page.

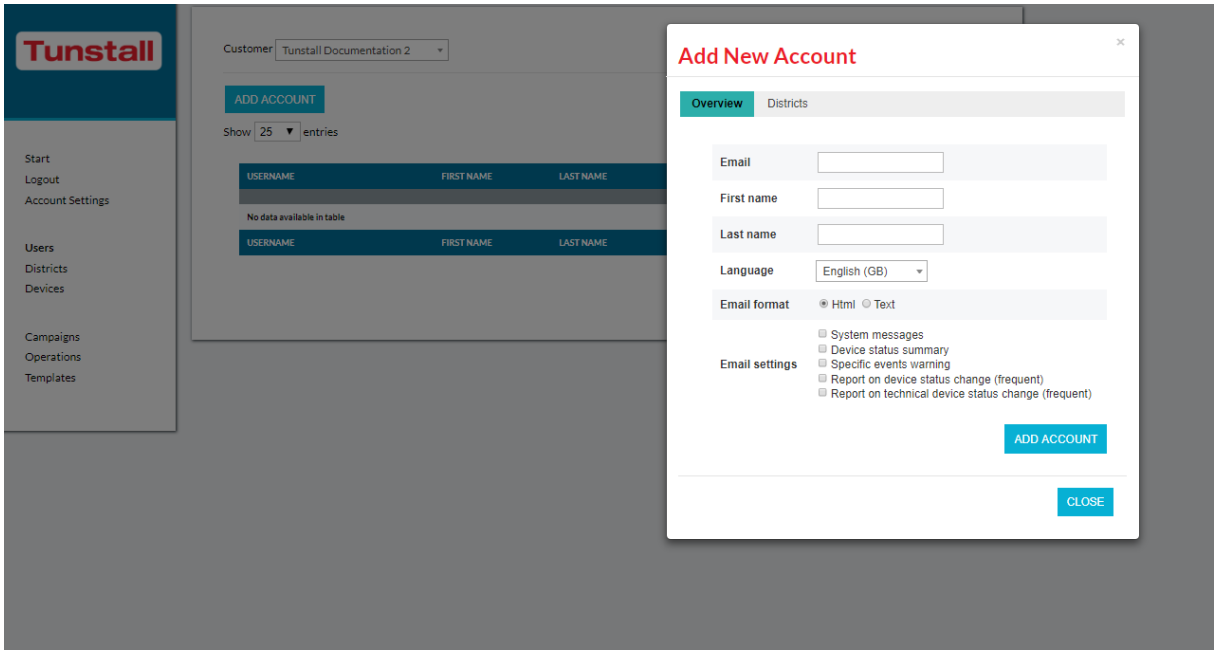
Within this page you can:

- Use the standard table actions to filter, sort and search through the list
- Initiate the creation of a new user account by clicking **ADD ACCOUNT**. DMP opens an Add New Account window for you to specify the user account.
- Initiate the display/edit/unlocking of a user account by clicking anywhere within its details. DMP opens an Edit Account window containing the details of the selected user account.

5.3 Add New Account window

You use this window to create a new user account including:

- general details
- the districts that the account may access, together with the permission profile for each district.



You access this window by:

- Clicking the **Users** option on the main menu – only available to users with at least one 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you maintain user accounts for more than one customer
- Clicking **ADD ACCOUNT**.

The window comprises two tabs which are described in the following sub-sections.

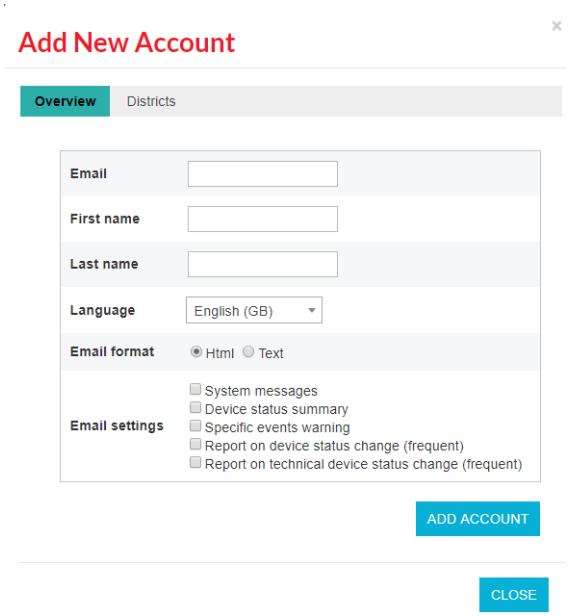
To create a new user account:

1. Complete the general details on the **Overview** tab.
2. Click **ADD ACCOUNT**. This automatically displays the **Districts** tab.
3. Specify the districts that the user can access, together with their permission profile for each district.
4. Click **SAVE**.

   DMP closes the window, saves the details of the new user account and updates the View User Accounts List page to include the new user.

5.3.1 Overview tab

You use the **Overview** tab to specify the general details of the user account.



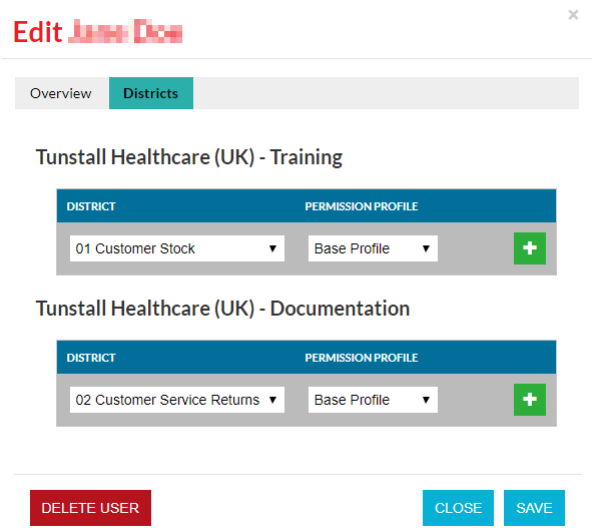
When creating a user account, complete all the fields on this tab and then click **ADD ACCOUNT** to move on to the **Districts** tab.

When editing a user account, you make the required changes and then either click the **Districts** tab to make additional changes or click **SAVE** to save any changes you have made over the two tabs.

Field	Description
Email	The email address of the new user. This becomes their username.
First Name	The first name of the new user.
Last Name	The surname of the new user.
Language	The account language of the new user.
Email format	The format of the emails received from DMP. Tunstall recommends that you set it to “Html”.
Email settings	A set of checkboxes defining the types of emails the new user is to receive.

5.3.2 Districts tab

You use the **Districts** tab to link existing districts to the user account.



If adding a user account, this tab initially lists the customers from which you can choose districts to be accessed by the user. This list comprises all the customers displayed on your Start page. If you are editing an existing user account, the tab also lists the districts that the user account can access currently, together with the associated permission profiles.

When adding or editing a user account, you set up the required districts and associated permission profiles and then either:

- Click the **Overview** tab to set up/amend other values, or,
- Click **SAVE** to save the account's details.

Within this tab you can:

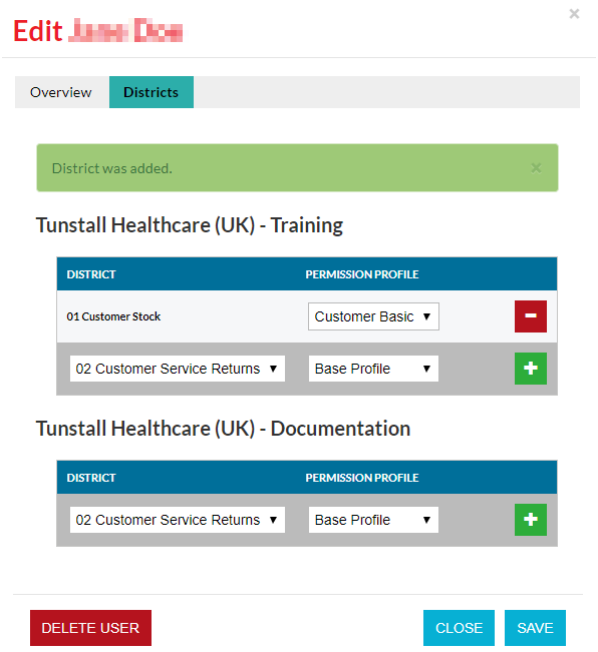
- Make a district accessible to the user account
- Amend the user account's permission profile for a district
- Remove access to a district from the user account.

Make a district accessible to the user account

To make a district accessible to the user account:

1. Select the required district from the appropriate **DISTRICT** drop-down list.
2. Select the associated **PERMISSION PROFILE**, normally "Customer Basic".
3. Click the + button.

   DMP displays the district and its permission profile in the table above the drop-down lists.



You can now go on to amend their permission profiles and/or remove any user entered in error.

Amend the user account's permission profile for a district

To amend the user account's permission profile for a district, select the appropriate value from the **PERMISSION PROFILE** drop-down list relating to that district.

Remove access to a district from the user account

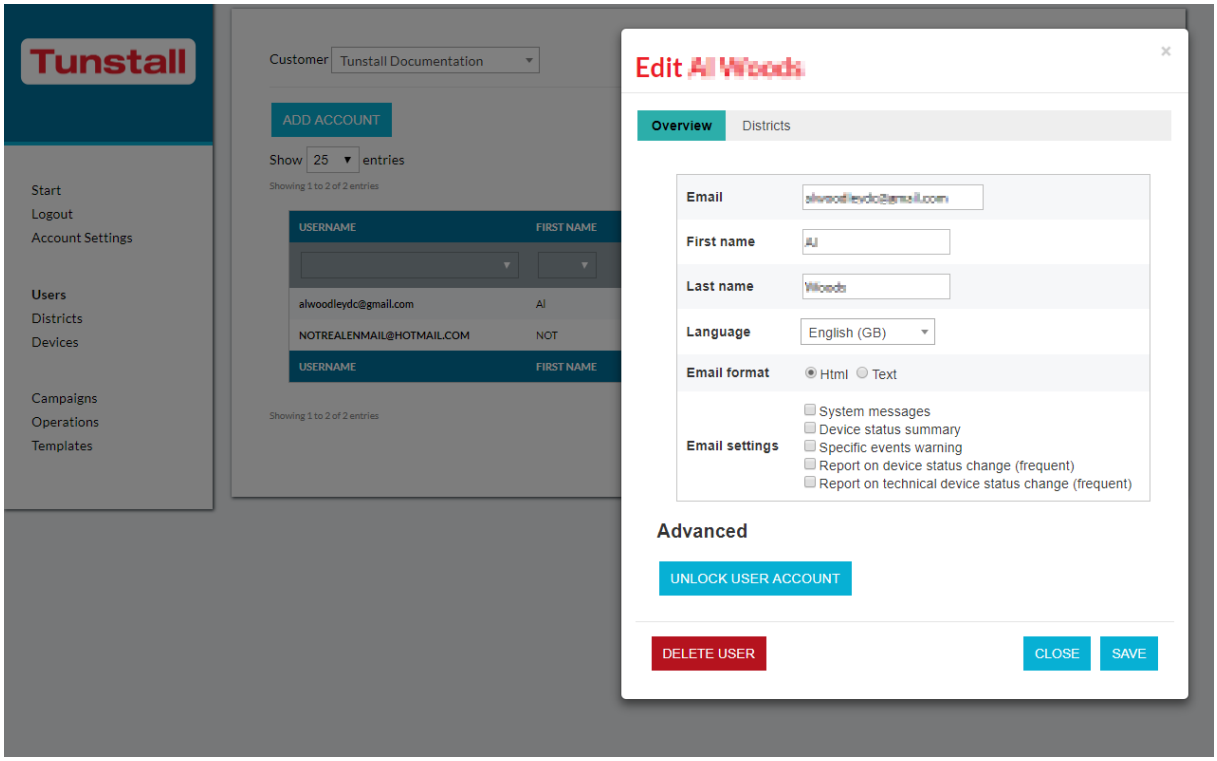
To remove access to a district from the user account, click the − button next to the district details.

5.4 Edit User Account window

You use this window to view/edit a user account's details including:

- general details
- the districts that the account may access, together with the permission profile for each district.

In addition, you can also use it to unlock or delete the account.



You access this window by:

- Clicking the **Users** option on the main menu – only available to users with at least one 'Customer Advanced' permission profile
- Clicking within the row containing the details of the user account you wish to view or work on.

The window comprises two tabs which are described within Section 5.3, Add New Account window.

Within this window you can:

- View a user account's details
- Edit a user account
- Unlock a user account
- Delete a user account.

View a user account's details

To view a user account's details, select the required users tab.

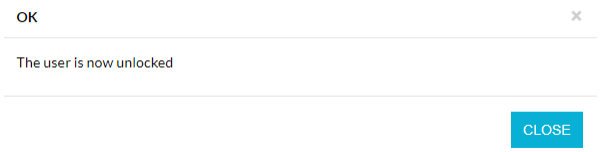
Edit a user account

To edit a user account, make the relevant changes required and then click **SAVE**. DMP closes the window and updates user account's details.

Unlock a user account

To unlock a user account:

1. Click the **UNLOCK USER ACCOUNT** button. DMP unlocks the account and displays an information message:

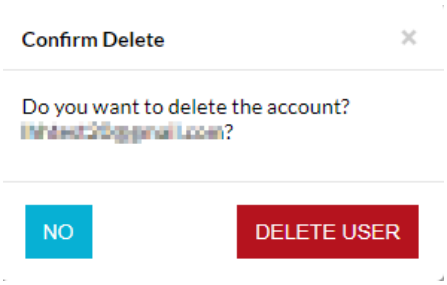


2. Click **CLOSE** to return to the Edit User Account window.

Delete a user account

To delete a user account:

1. Click the **DELETE USER** button. DMP displays a confirmation message:



2. Click **DELETE USER**. DMP then removes the account details from the View User Account List page, deletes the user account, its settings and all permission profiles, and closes the Edit User Account window.

6 Working with devices

6.1 Introduction

Within DMP, a ‘device’ defines a single Smart Hub unit. The main functions of DMP are to administer the Smart Hub units and to monitor that they are functioning correctly.

DMP constantly monitors the heartbeats sent to it from each unit. The health of the unit is represented within DMP by traffic light icons, as described in Appendix B, Heartbeat icons and status. This heartbeat status is also used to indicate the status of the unit during installation of new configuration settings and firmware.

Within DMP, you can view graphical representations of the heartbeats received from a unit over the past 24 hours. In addition, you can view details of the heartbeats received over the last seven days, in tabular form.

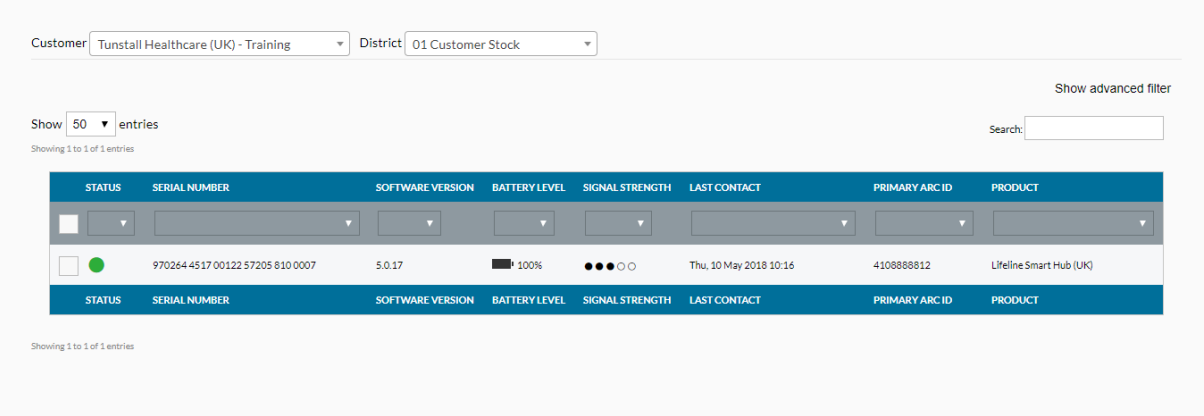
In addition to heartbeats, DMP records each DMP event that relates to the administration of a unit. The administration operations you can perform within DMP are:

- Editing the details held about the unit, including activating and deactivating it
- Moving the unit to a different district
- Updating its configuration settings by manually changing the unit’s configuration settings within DMP, as described in Section 7, Working with device configuration settings
- Updating its configuration settings by using a template. For details on templates, refer to Section 9, Working with templates
- Updating the unit’s firmware by using a campaign. For details on campaigns, refer to Section 8, Working with firmware and campaigns.

When updating the configuration or firmware of a unit, DMP waits to receive a heartbeat from it and then downloads the new settings or firmware for the unit to install. Whilst the download and installation/upgrade is taking place, the device has a technical heartbeat status, indicated by the colour blue. On successful installation of the firmware or completion of the upgrade, the heartbeat status changes to ‘OK’, indicated by green. Whilst changes to a device’s settings are outstanding, DMP locks the device so that you cannot specify any further changes.

6.2 View Devices List page

You use this page to view, maintain and configure devices that reside within the districts to which you have access.



You access this page by clicking the **Devices** option on the main menu.

Note: This option is only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile.

The page initially lists the devices numerically ascending by their serial number. If you have 'Customer Basic' or 'Customer Advanced' permission profiles for more than one customer or district, then you primarily see those devices located within the customer/district combination that appears first on your Start page.

The list contains, among other values, the status of the latest heartbeat, the current cellular signal strength and a calculated estimate of remaining battery capacity.

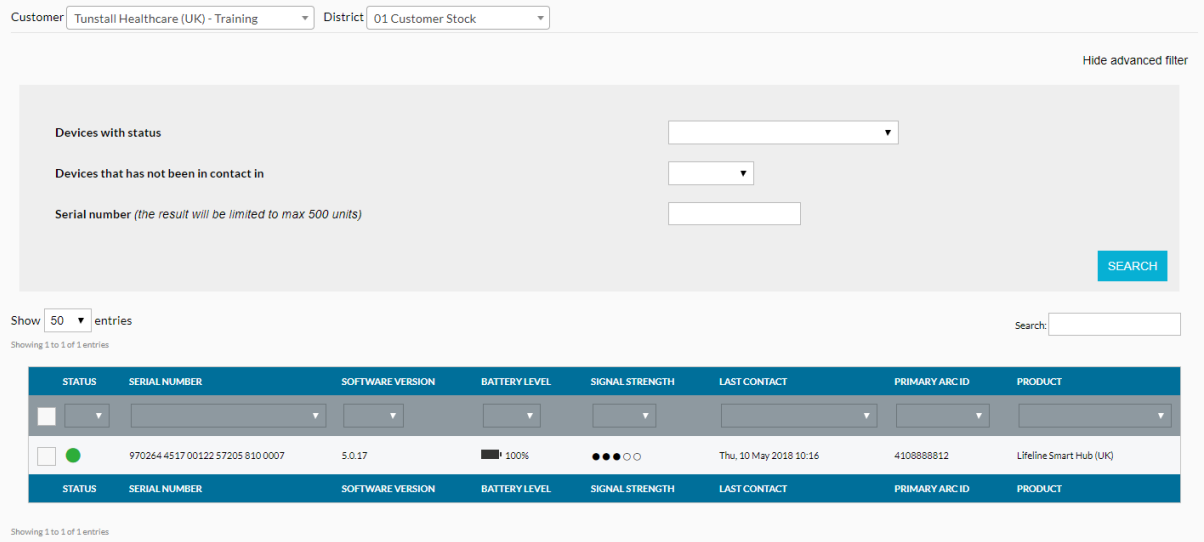
Within this page you can:

- Use the standard table actions to filter, sort and search through the list
- Use the advanced filter to view a sub-set of devices
- Initiate the display/edit of a device's details, including its district and Smart Hub configuration settings, by clicking anywhere within its details. DMP opens a Device Information window containing the details of the selected device.
- Initiate the migration of one or more devices to another district
- Initiate the update of the firmware on one or more devices – only available to users with at least one 'Customer Advanced' permission profile
- Initiate the application of a template to one or more devices.

Use the advanced filter to view a sub-set of devices

To use the advanced filter to view a sub-set of devices:

1. Click **Show advanced filter**. DMP expands the page to show three extra fields:



2. Select the filter parameters by performing one or more of the following actions:
   - Restrict the list to devices of a specified status by choosing a value from the **Device with status** drop-down list
   - Restrict the list to devices that have not been in contact for a specified amount of time by choosing a value from the **Devices that has not been in contact in** drop-down list
   - Enter all or part of a serial number to restrict the list to those devices that have matching serial numbers.
3. Click **SEARCH**. DMP filters the list according to the conditions you entered in the previous step.

Initiate the migration of one or more devices to another district

To initiate the migration of one or more devices to another district:

1. Select the checkbox at the start of the details of each device to be migrated. If required, use the filter, sort and search facilities to view the relevant devices. On selection of the first device, DMP displays three additional buttons above the list of devices. As you select the devices, DMP increments the number within the **MIGRATE DEVICES** button.
2. Once you have selected all the required devices, click the **MIGRATE DEVICES** button. DMP opens the Migrate Devices window where you specify where they are to be relocated, as described in Section 6.4, Migrate Devices window.

Initiate the update of firmware on one or more devices

To initiate the update of firmware on one or more devices:

1. Select the checkbox at the start of the details of each device to be upgraded. If required, use the filter, sort and search facilities to view the relevant devices. On selection of the first device, DMP displays three additional buttons above the list of devices. As you select the devices, DMP increments the number within the **UPGRADE FIRMWARE** button.
2. Once you have selected all the required devices, click the **UPGRADE FIRMWARE** button. DMP opens the Start Campaign window where you specify the firmware to be applied and how the upgrade is to take place, as described in Section 6.5, Start Campaign window.

Note: Attempting to upgrade a device more frequently than once every two hours may result in the later attempts failing until the Smart Hub completes the background tasks associated with firmware memory management.

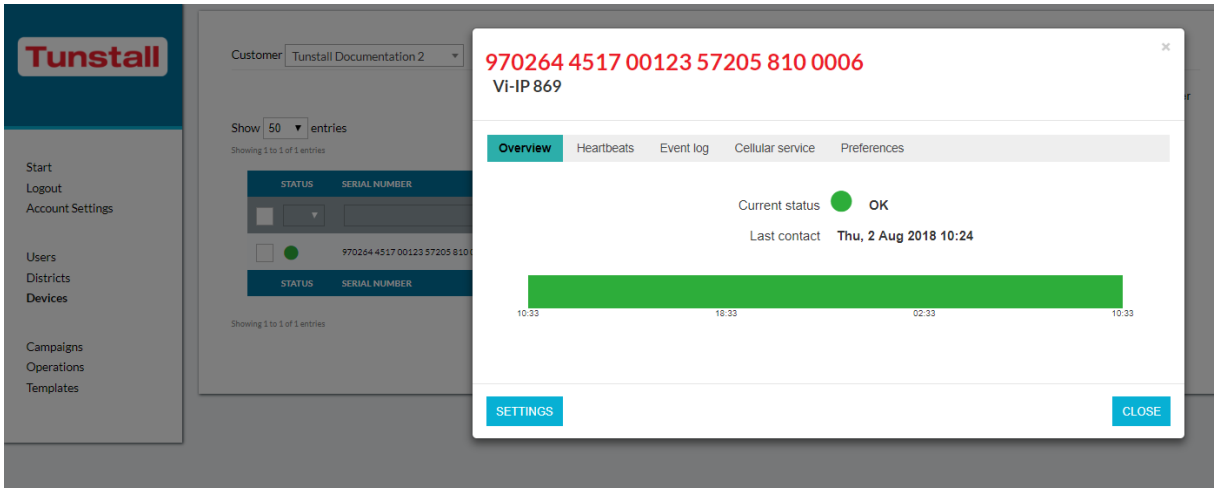
Initiate the application of a template to one or more devices

To initiate the application of a template to one or more devices:

1. Select the checkbox at the start of the details of each device to which the template is to be applied. If required, use the filter, sort and search facilities to view the relevant devices. On selection of the first device, DMP displays three additional buttons above the list of devices. As you select the devices, DMP increments the number within the **SET SETTINGS TEMPLATE** button.
2. Once you have selected all the required devices, click the **SET SETTINGS TEMPLATE** button. DMP opens the Assign Template window where you specify the template to be applied, as described in Section 6.6, Assign Template window.

6.3 Device Information window

You use this window to view the information relating to a single device. In addition, you can migrate the device to another district and initiate the display/edit of its settings.



You access this window by:

- Clicking the **Devices** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you maintain devices for more than one customer
- Selecting the appropriate district, if you maintain devices for more than one district
- Clicking within the row containing the relevant device.

The window comprises four tabs which are described below.

If the window's contents become out-of-date, DMP displays a warning sign as shown below:

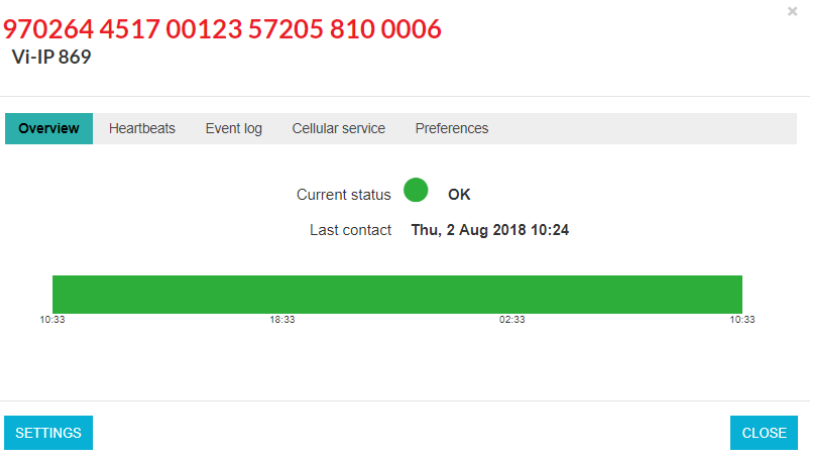
In this case, you should close and then re-open the window to update the device details.

Within this window you can:

- Initiate the display/edit of a device's settings by clicking the **SETTINGS** button. For details of these, refer to Section 7, Working with device configuration settings.
- Update the device's details, including migrating it to another customer/district, as described in Section 6.3.5, Preferences tab.

6.3.1 Overview tab

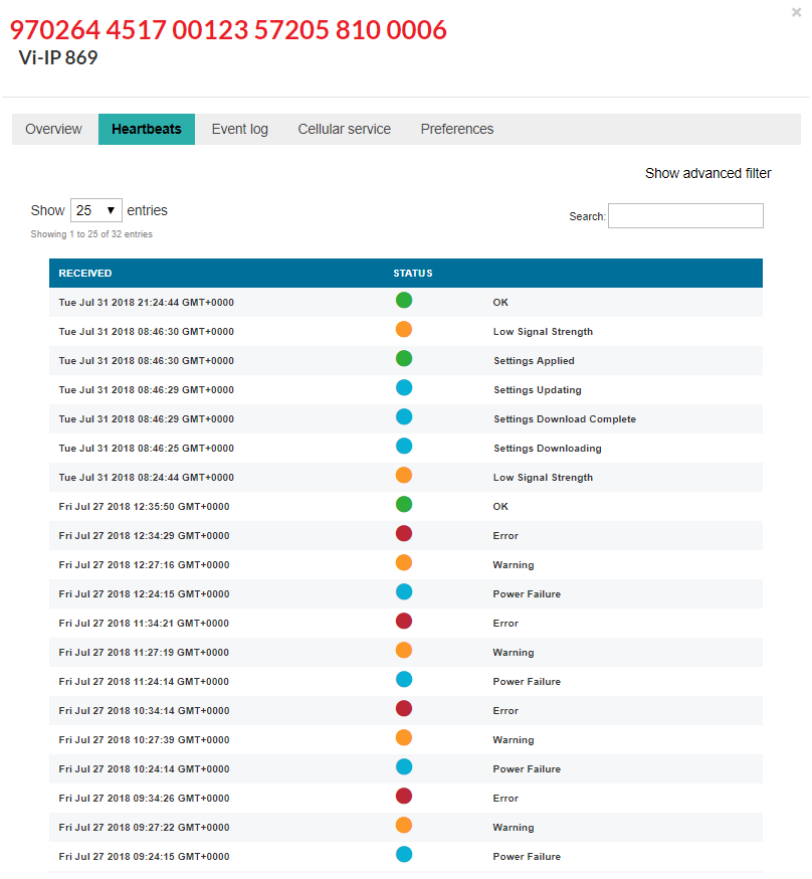
You use the **Overview** tab to view the status of the device over the last 24 hours.



The last recorded status of the device is displayed, together with the time of contact. Below this is a time bar showing the changes in status over the last 24 hours. Each different status is colour-coded as defined in Appendix B, Heartbeat icons and status. You can view the status type and its duration by placing the cursor over the relevant section of the time bar.

6.3.2 Heartbeats tab

You use the **Heartbeats** tab to view the status of the device over the last seven days.



For additional details on the colour coding and meaning of each status, refer to Appendix B, Heartbeat icons and status.

The tab initially displays only those heartbeats that changed the status of the device. You can display all heartbeats and/or exclude any heartbeat with a technical status by using the advanced filter.

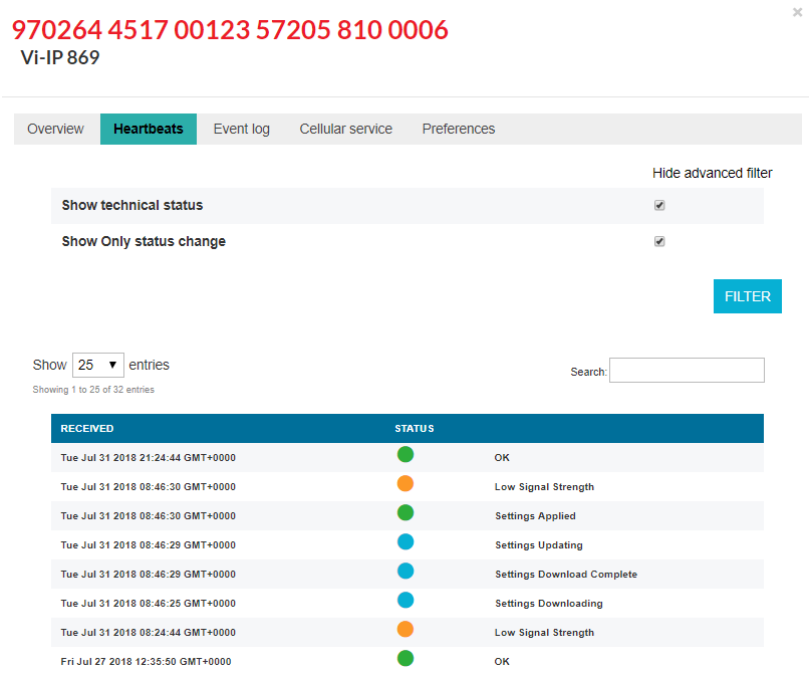
Within this tab you can:

- Use the standard table actions to filter, sort and search through the list
- Use the advanced filter to change the set of heartbeats displayed.

Use the advanced filter to change the set of heartbeats displayed

To use the advanced filter to change the set of heartbeats displayed:

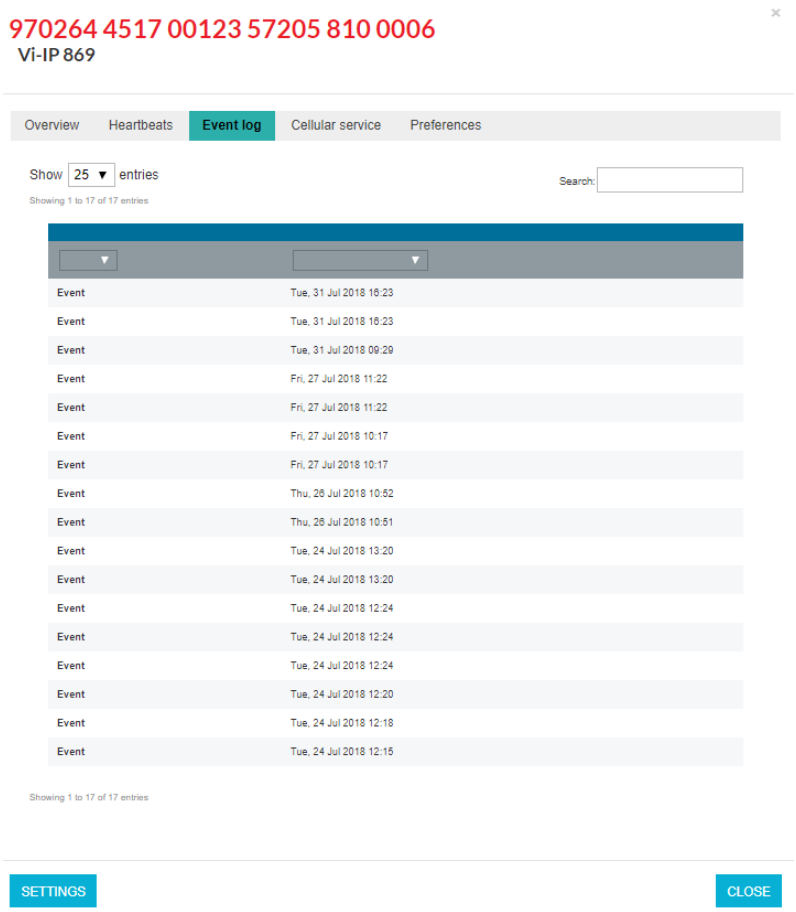
1. Click **Show advanced filter**. DMP expands the window to show two extra fields:



2. Select/deselect the filter parameters. If you check:
   - **Show technical status**, the list includes each heartbeat that reported a technical status
   - **Show Only status change,** the list includes each heartbeat whose status was not the same as the previous heartbeat status.
3. Click **FILTER**. DMP filters the list according to the conditions you entered in the previous step.

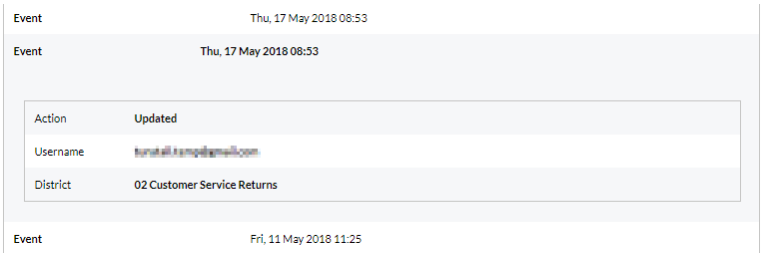
6.3.3 Event log tab

You use the **Event log** tab to view the events associated with the device. The event log will cover the last 14 days.



Within this tab you can:

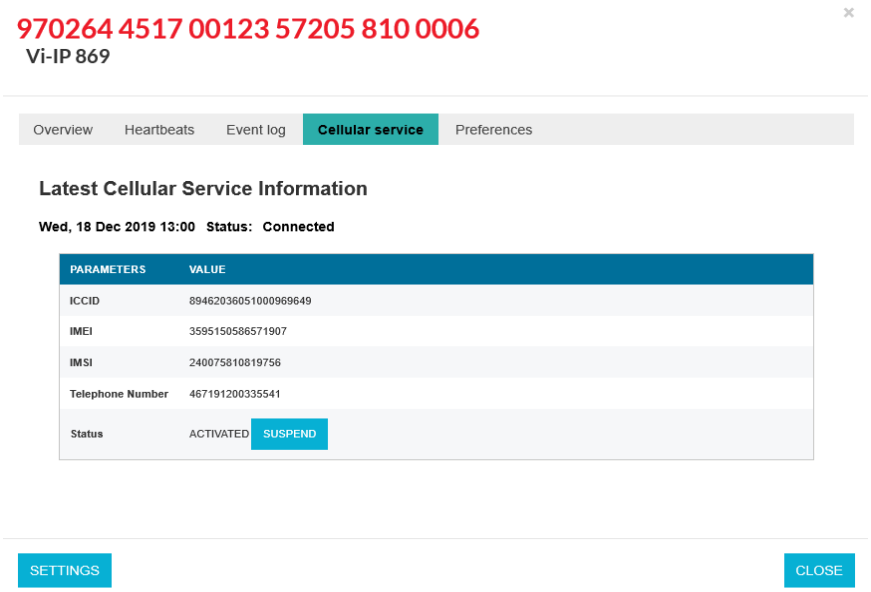
- Use the standard table actions to filter, sort and search through the list
- View the details of a specific event by clicking on its row. DMP displays the following information:



When you have finished viewing the event's details, click within the information to hide it.

6.3.4 Cellular service tab

You use the **Cellular service** tab to view details of the device's SIM card and the associated cellular service. Typically, you use these parameters for financial billing and other reports.



The details displayed are:

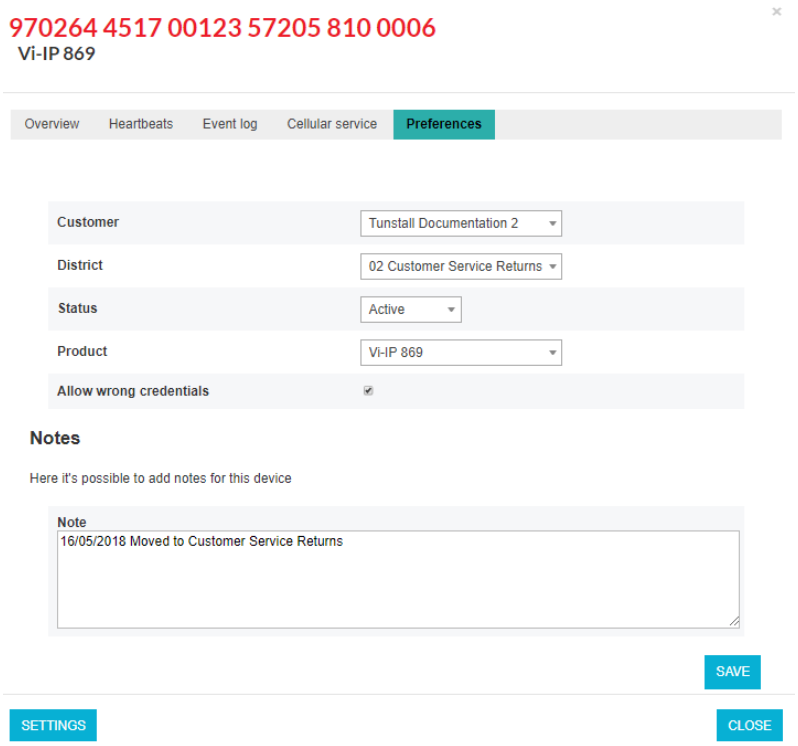
- Most recent cellular connection status
- Integrated circuit card identifier (ICCD) of the SIM
- International mobile equipment identity (IMEI) of the Smart Hub
- International mobile subscriber identity (IMSI) of the SIM card
- Telephone number
- Current activation status of the SIM; either 'activated' or 'inactive'.

Note: The "SUSPEND" button in the 'STATUS' category deactivates the SIM Card and sets the Smart Hub status to inactive. Whilst suspended the Smart Hub will not be able to make alarm calls using the suspended SIM or be programmed via the DMP.

Note: The SIM card must have been provided by Tunstall for the 'inactive' status to be displayed.

6.3.5 Preferences tab

You use the **Preferences** tab to view and edit general properties of the device, including its status and location.



The tab contains the following fields:

Field	Description
Customer	The customer to which the device belongs. Displayed only if you can access districts belonging to more than one customer. If you change customer, you must also specify the district where the device is located.
District	The district in which the device is located. The drop-down list comprises all the districts to which you have access, and which belong to the specified customer, if any. On purchase, a device is placed in “01 Customer Stock”. If it needs to be returned to Tunstall, it should be placed in “02 Customer Service Returns”.
Status	Indicates whether the device is active/inactive - operational in DMP, or not.

Field	Description
Template	The template to be automatically applied to the device on its migration to the new district. Displayed only if the district has one or more associated templates. The drop-down list contains the templates that are currently assigned to the selected district. For details on how to create and assign a template, refer to Section 9.3, Add New Template window. Alternatively, you can assign templates to a district whilst administering that district as described in Section 4.3.4, Templates tab.
Product	The product type of the Smart Hub. Typically, there are differences in the default configuration depending on the geographical area, and this is reflected in the product type name.
Allow wrong credentials	Not currently used.
Note	Use for additional information on the device. You should **NOT** use this field to enter details about the end user of the device. For data privacy reasons, such information should only be held in the alarm call receiving system.

To change the general properties of the device, specify the required values for the fields and then click **SAVE.**

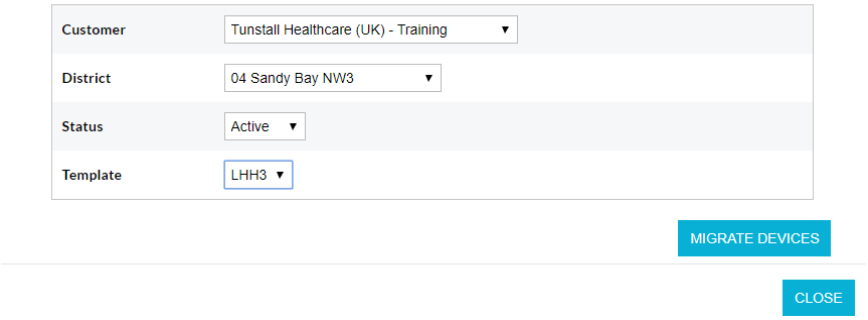
Amending the **District** drop-down list, or **Customer** and **District** drop-down lists, migrates the device to a new location. In this case, if there is a template to apply, DMP waits until the device sends a heartbeat. It then downloads the template settings for the device to apply. Whilst the download and upgrade is taking place, the device has a technical status indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, prompting a DMP connection and initiating the download.

6.4 Migrate Devices window

You use this window to move one or more devices to a different district. As part of the move, you also:

- specify whether the devices are to be active or inactive (operational in DMP).
- specify which template is to be applied to each of the devices, if there are any templates associated with the new district.



You access this window by:

- Clicking the **Devices** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you maintain devices for more than one customer
- Selecting the appropriate district, if you maintain devices for more than one district
- Selecting one or more devices and then clicking the **MIGRATE DEVICES** button.

The window contains the following fields:

Field	Description
Customer	The customer to which the devices belong. Displayed only if you can access districts belonging to more than one customer. If you change customer, you must also specify the district where the devices are to be located.
District	The district to which the devices are to be migrated. The drop-down list comprises all the districts to which you have access, and which belong to the specified customer, if any. On purchase, a device is placed in "01 Customer Stock". If it needs to be returned to Tunstall, you should place it in "02 Customer Service Returns".
Status	This indicates whether the devices are active, that is, operational in DMP, or not.

Field	Description
Template	The template to be automatically applied to the devices on their migration to their new district. Displayed only if the district has one or more associated templates. The drop-down list contains the templates that are currently assigned to the selected district. For details on how to create and assign a template, refer to Section 9, Working with templates.

To move the devices to their new district, specify the required values for the fields and then click **MIGRATE DEVICES.**

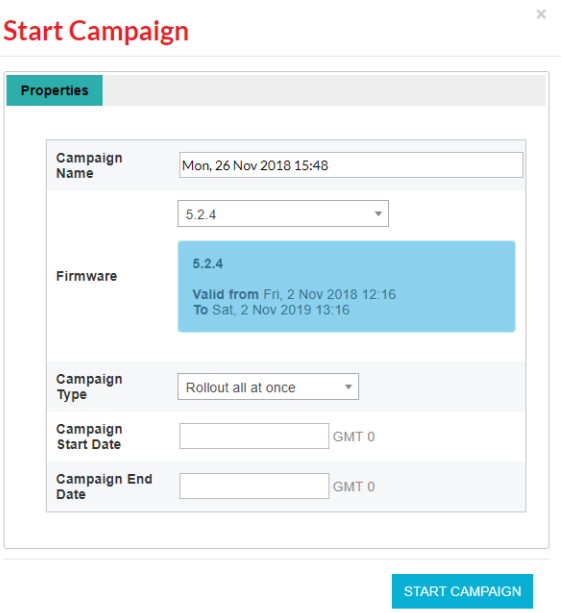
DMP moves the devices to the appropriate district. If there is a template to apply, then for each selected device, DMP waits until the device sends a heartbeat. It then downloads the template settings for the device to apply. Whilst the download and upgrade are taking place, the device has a technical status, indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, prompting a DMP connection and initiating the download.

6.5 Start Campaign window

You use this window to define how DMP is to apply a firmware upgrade to one or more devices, and to initiate this upgrade. This definition is known within DMP as a 'campaign'.

Note: Attempting to upgrade a device more frequently than once every two hours may result in the later attempts failing until the Smart Hub completes the background tasks associated with firmware memory management.



To access this window, you must have at least one 'Customer Advanced' permission profile.

You access this window by:

- Clicking the **Devices** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer if you maintain devices for more than one customer
- Selecting the appropriate district if you maintain devices for more than one district
- Selecting one or more devices and then clicking the **UPGRADE FIRMWARE** button – only available to users with at least one 'Customer Advanced' permission profile.

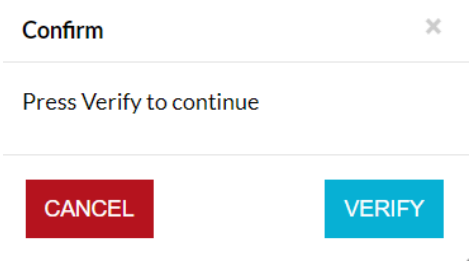
The window contains the following fields:

Field	Description
Campaign Name	The unique name for the campaign. Default is the current day, date and time.
Firmware	The version of firmware that DMP is to download to the devices.

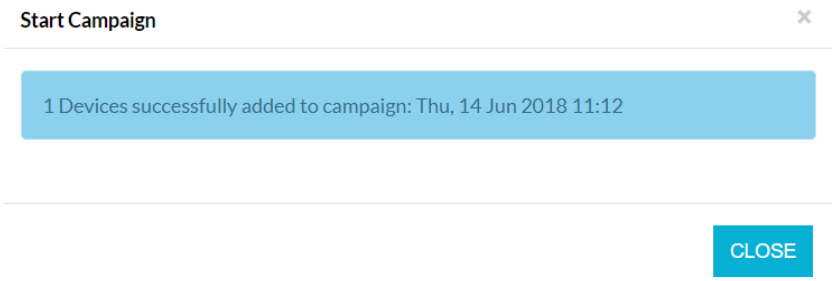
Field	Description
Campaign Type	Indicates how the downloads are to be managed. Can be one of: • 'Rollout at once' DMP downloads the firmware simultaneously to all selected devices when the **Campaign Start Date** is reached • 'Start with 10' DMP downloads the firmware to batches of 10 devices at a time; the download of a new batch starts when the download for all 10 devices of the previous batch completes. In both cases, downloading continues until either all selected devices have received the firmware, or the **Campaign End Date** is reached, whichever is earlier.
Campaign Start Date	The date and time the process of updating the device firmware is to start. The offset of this time from Greenwich Mean Time (GMT) is shown next to the field in grey. **Note: After a firmware upgrade has been installed, it is possible that the Smart Hub may make alarm calls. These calls arise from the clearing of memorised calls which previously failed to connect and were not acknowledged by pressing the green Cancel button at the time. This should be considered when scheduling updates.**
Campaign End Date	The date and time the process of updating the device firmware is to end. The offset of this time from GMT is shown next to the field in grey. If the firmware download to a device starts and the campaign ends before the installation of that firmware completes, the device continues with the upgrade. If the download of firmware to a device has not started when the campaign ends, no downloading takes place, with the firmware remaining unchanged until another campaign upgrades it.

To define and initiate a campaign:

1. Specify the required values for the fields.
2. Click **START CAMPAIGN**. DMP displays the following confirmation message:



3. Click **VERIFY**. DMP saves the details of the campaign and displays the following summary message:



4. Click **CLOSE**.

Then, at the specified start date/time, DMP downloads the firmware to the selected devices.

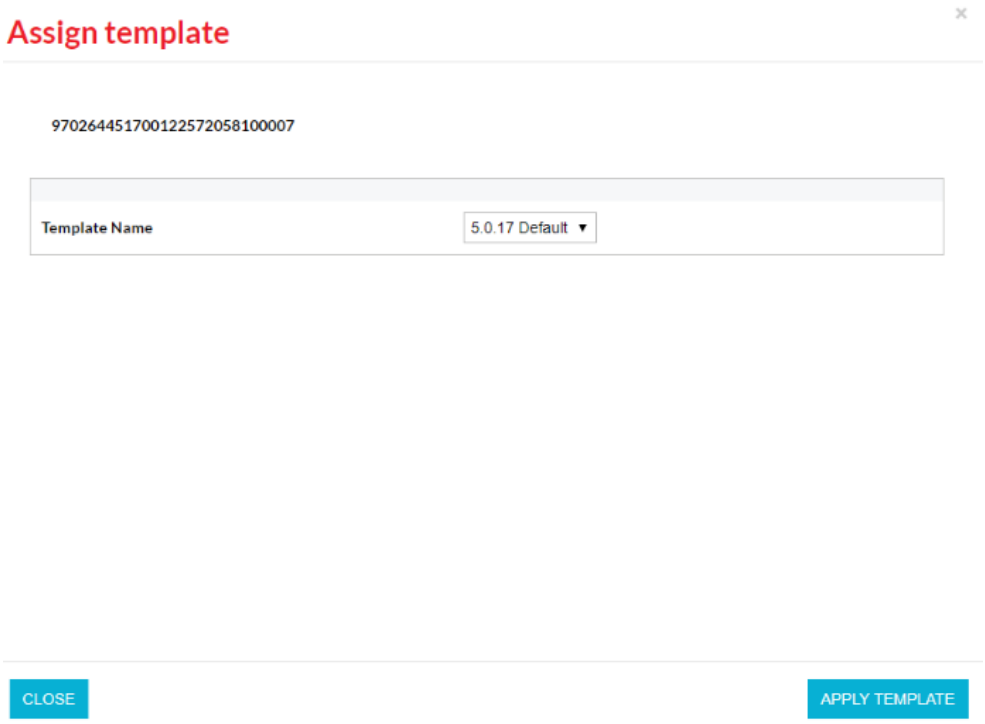
Note: Attempting to upgrade a device more frequently than once every two hours may result in the later attempts failing until the Smart Hub completes the background tasks associated with firmware memory management.

During the download and installation of the firmware, a device has a technical status, indicated by the colour blue. On successful installation of the firmware, its status changes to 'OK', indicated by green. If the download is unsuccessful, its status changes to red, indicating an error has occurred. A period of downtime where DMP is inaccessible may be experienced when the device has a technical or error status.

Note: Please be aware when scheduling upgrades that a Smart Hub may make alarm calls after its upgrade. These are memorised calls which previously failed to connect and were not cancelled by pressing the green Cancel button.

6.6 Assign Template window

You use this window to apply a template to one or more devices.



You access this window by:

- Clicking the **Devices** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer if you maintain devices for more than one customer
- Selecting the appropriate district if you maintain devices for more than one district
- Selecting one or more devices and then clicking the **SET SETTINGS TEMPLATE** button.

The window contains the following fields:

Field	Description
Name	The name of the template to be applied to the selected devices. The drop-down list displays the templates that are currently assigned to the district where the selected devices are located. For details on how to create and assign a template, refer to Section 9, Working with templates.

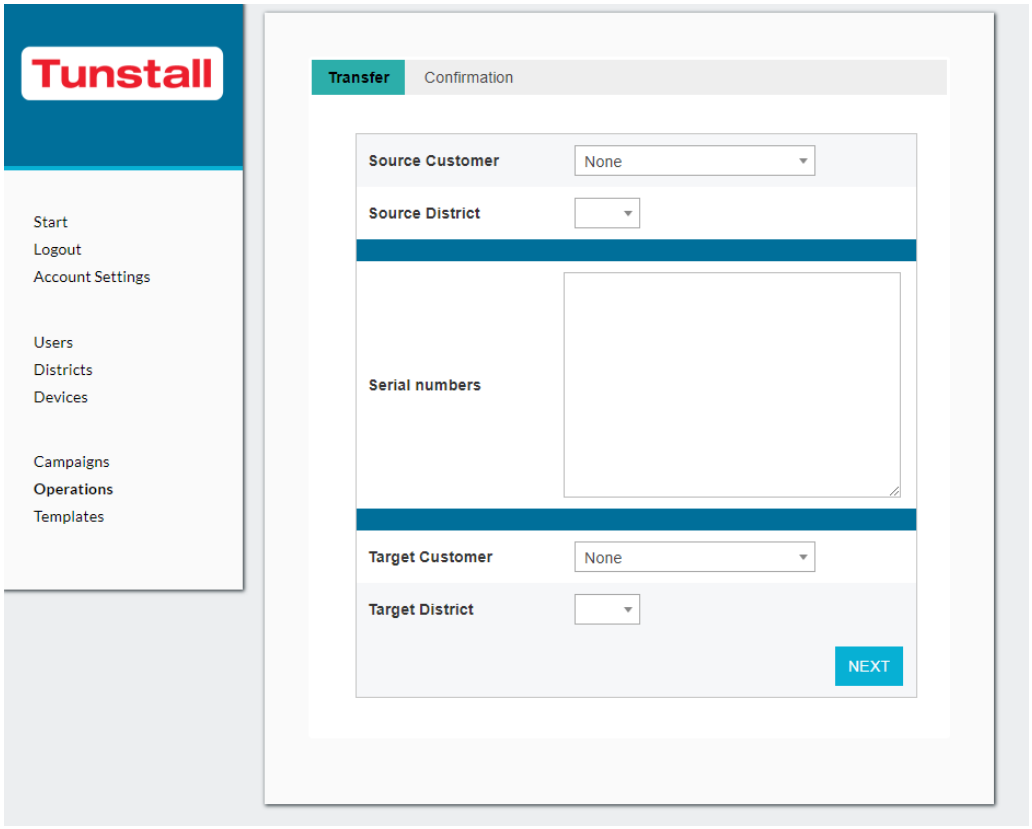
To apply a template, select the required template and then click **APPLY TEMPLATE.**

For each selected device, DMP waits until the device sends a heartbeat. It then downloads the template settings for the device to apply. Whilst the download and upgrade are taking place, the device has a technical status, indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, so prompting a DMP connection and initiating the download.

6.7 Operations page

You use this page to move one or more devices to a different district. As part of the move, you can also specify which template is to be applied to each of the devices, if there are any templates associated with the new district.



You access this page by:

- Clicking the **Operations** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile.

You initially see the Transfer tab where you specify the details of the transfer. Once you have completed the tab and clicked **NEXT**, DMP displays the Confirmation tab. This tab indicates whether each transfer will be successful or not. From here, you can either click **BACK** to return to the Transfer tab or click **TRANSFER** to initiate the transfer.

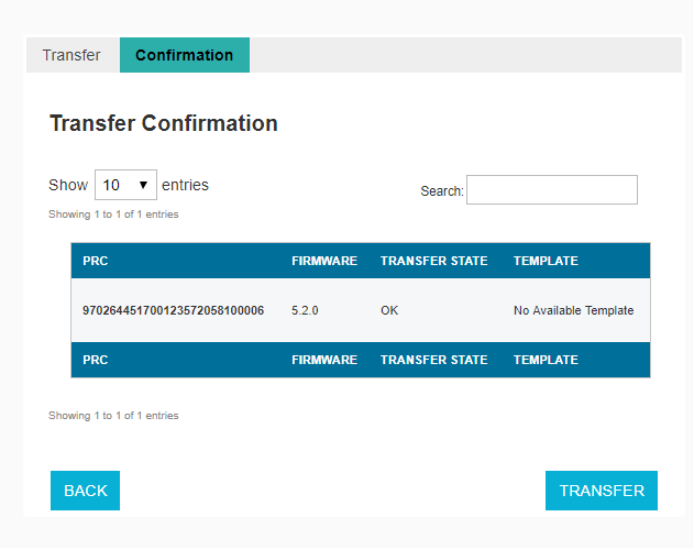
The page contains the following fields:

Field	Description
Source Customer	The customer to which the devices belong. Displayed only if you can access districts belonging to more than one customer. If you change customer, you must also specify the district where the devices are currently located.
Source District	The district to which the devices belong. The drop-down list comprises all the districts to which you have access and belong to the specified source customer, if any.
Serial numbers	The product codes (PRCs) of the devices to be moved. Can be scanned or manually entered. In the latter case you need to ensure that each code is on a new line.
Target Customer	The customer to which the devices are to be transferred. Displayed only if you can access districts belonging to more than one customer. If you change customer, you must also specify the district where the devices are to be located.
Target District	The district to which the devices are to be transferred. The drop-down list comprises all the districts to which you have access and belong to the specified target customer, if any. On purchase, a device is placed in “01 Customer Stock”. If it needs to be returned to Tunstall, you should place it in “02 Customer Service Returns”.
Template	The template to be automatically applied to the devices on their transfer to the new district. The drop-down list contains the templates that are currently assigned to the selected district. For details on how to create and assign a template, refer to Section 9, Working with templates.

To move devices to a new district:

1. Specify the current location of the devices by completing **Source District** and, if you can access multiple customers, the **Source Customer** field.
2. Specify the product codes of the devices to be moved in **Serial numbers**. You do this typically by scanning each unit, but you can enter their codes manually. In the latter case you need to ensure that each code is on a new line.
3. Specify the new location of the devices by completing **Target District** and, if you can access multiple customers, the **Target Customer** field.
4. If required, select the name of the template to be applied from the **Template** drop-down list.
5. Click **NEXT**.

DMP displays the Confirmation tab:



6. Check that the units will be successfully transferred. If not, return to the **Transfer** tab and amend as required, before returning to the **Confirmation** tab.
7. Click **TRANSFER**.

   DMP moves the devices to the appropriate district, retaining their current status of active or inactive. If there is a template to apply, then for each selected device, DMP waits until the device sends a heartbeat. It then downloads the template settings for the device to apply. Whilst the download and upgrade is taking place, the device has a technical status, indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

   Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, so prompting a DMP connection and initiating the download.

7 Working with device configuration settings

7.1 Introduction

You use DMP to maintain each device's configuration settings. Each Smart Hub has the same set of configurable attributes which can be tailored to comply with local regulations, supplier policies, end-user requirements, etc.

You amend the relevant settings using the menu options on the Device Setting window. Each setting relates to a Smart Hub functional feature. These functional features, with a few exceptions, map to the corresponding menu option on the Device Settings window. When you make a change to an attribute field, DMP highlights it with a red border.

When you save the changes, they are stored within DMP but not immediately downloaded to the Smart Hub. DMP waits until the device sends a heartbeat. It then downloads the updated settings for the device to apply. Whilst the download and upgrade is taking place, the device has a technical status, indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

The following table lists each functional feature that can be configured, references the sections of this chapter which configure the feature and provides descriptions of the related configuration settings.

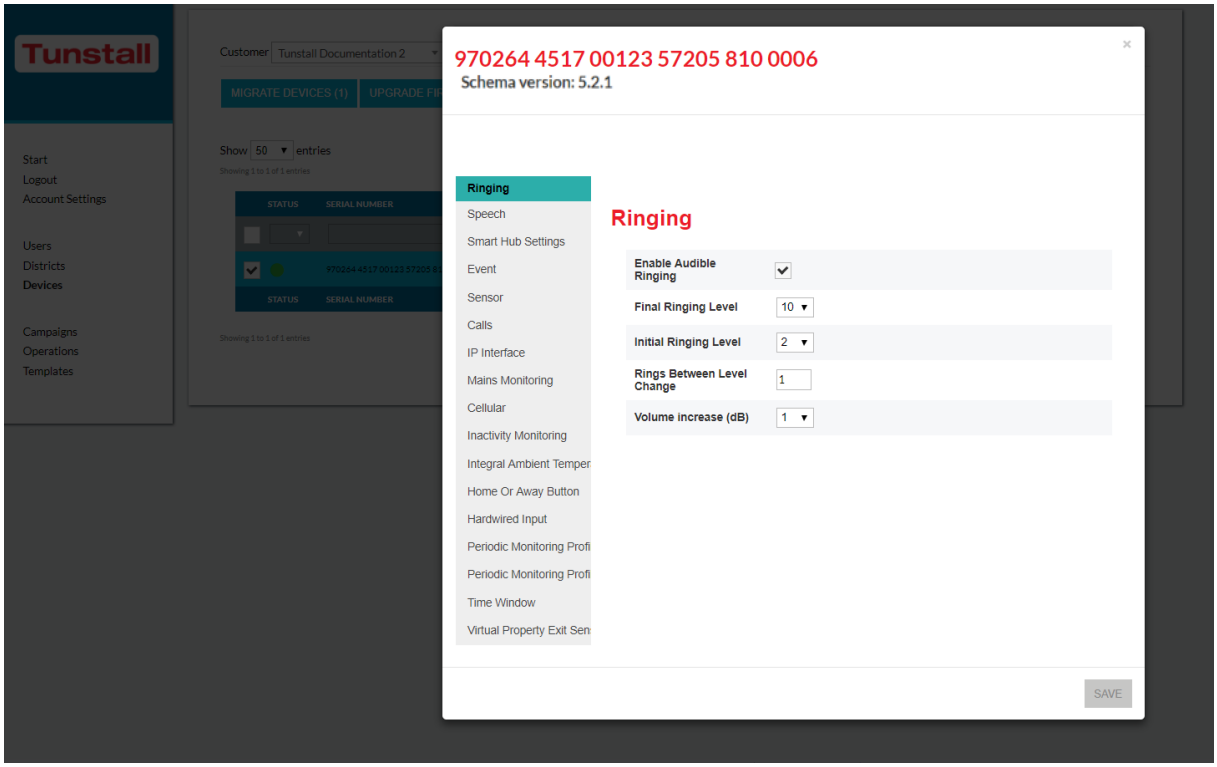
Feature	Related Section	Overview
Call Destinations	7.2.6 Device Settings window – Calls menu option	Defines the communication paths used for alarm calls. Each path comprises a call sequence with up to ten destinations that the unit attempts to contact sequentially.
Cellular Operation	7.2.9 Device Settings window – Cellular menu option	Defines how cellular connectivity and operation is configured.
Event Configuration	7.2.4 Device Settings window – Event menu option 7.2.17 Device Settings window – Time Window menu option	Every event has their own set of attributes, so allowing the action resulting from an occurrence of the event to be customised. For example, a smoke detector alarm can be sent to a different monitoring centre than alarms raised manually. Events can also be blocked within specific time windows.
Fault Monitoring via time	7.2.2 Device Settings window – Speech menu option	Configures how alarms are to be suppressed based on the time. For example, low temperature alarms are suppressed during sleeping hours.
Hardwired Input	7.2.13 Device Settings window – Hardwired Input menu option	Defines an external device that signals with normally open or normally closed contacts when connected to the hardwired input.
Hardwired Output	7.2.4 Device Settings window – Event menu option	Defines the events that can be configured to operate a set of relay contacts available to interface with external equipment.
Home/Away	7.2.12 Device Settings window – Home Or Away Button menu option	Defines the suspension of monitoring for certain types of alarm conditions, such as inactivity monitoring etc., typically whilst the user is out of the home. The time period of this suspension is controlled by user operation of the **Home/Away** button.

Feature	Related Section	Overview
Inactivity Monitoring	7.2.10 Device Settings window – Inactivity Monitoring menu option	Defines the attributes relating to inactivity monitoring, including: • the time period of inactivity that causes the associated event to occur • the inactivity pre-alarm period during which the client can cancel the alarm that is due to be raised.
Incoming Calls	7.2.9 Device Settings window – Cellular menu option 7.2.1 Device Settings window – Ringing menu option	Defines how incoming calls originating from the monitoring centre or other authorised/related source are supported when using cellular voice, for example, how ringing volume increases depending on the length of time the unit is ringing.
IP Interface	7.2.7 Device Settings window – IP Interface menu option	Defines how the unit can communicate using Internet Protocol (IP) using cellular data or ethernet (e.g. to fixed line broadband).
Mains Monitoring	7.2.8 Device Settings window – Mains Monitoring menu option	Configures how the unit monitors its mains supply and raises alarms when the mains fail.
Periodic Monitoring of Connectivity	7.2.15 Device Settings window – Periodic Monitoring Profile On Mains menu option 7.2.16 Device Settings window – Periodic Monitoring Profile On Battery menu option	Defines how the unit periodically checks availability and operation of the connectivity channel to DMP and the monitoring centre.
Radio Interference Monitor	7.2.3 Device Settings window – Smart Hub Settings menu option	Configures the monitoring for radio interference and reporting of this as an alarm call.
Radio Sensor Configuration	7.2.5 Device Settings window – Sensor menu option 7.2.18 Device Settings window – Virtual Property Exit Sensor menu option	Defines each personal trigger and telecare sensor registered with the unit. Provides a virtual property exit sensor that comes into effect for different time periods, depending on the day of the week.

Feature	Related Section	Overview
Speech Configuration	7.2.2 Device Settings window – Speech menu option	Controls the announcements made by the unit, including • their volume and language • format of reassurance announcements • format of local trigger/sensor registration announcements.
Temperature Monitoring	7.2.11 Device Settings window – Integral Ambient Temperature menu option	Defines whether the unit is to monitor the ambient temperature and, if so, what thresholds to be monitored and whether monitoring is to continue during night time. An event occurs if a threshold is reached during monitoring.
Time and Date	7.2.3 Device Settings window – Smart Hub Settings menu option	Configures the time zone, so enabling the automatic update of time and date settings from the internet.
Update Announcements	7.2.14 Device Settings window – DMP option	Controls whether the unit is to make or suppress announcements whilst receiving and installing firmware and configuration settings from DMP.

7.2 Device Settings window

You use this window to view and amend a device's settings.



You access this window by:

- Clicking the **Devices** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you maintain devices for more than one customer
- Selecting the appropriate district, if you maintain devices for more than one district
- Clicking within the row containing the relevant device, to display the Device Information window
- Clicking **SETTINGS**.

The window comprises two sections: a menu on the left-hand side and the main panel which displays the fields relating to the chosen menu option. The following sub-sections describe the main panel's contents on selection of each of the menu options. The descriptions include all fields that are visible to a user with a 'Customer Advanced' permission profile for the district in which the device is located. If you have a 'Customer Basic' permission profile, you may not see all the described fields.

Within this window you can:

- View a device's settings
- Edit a device's settings.

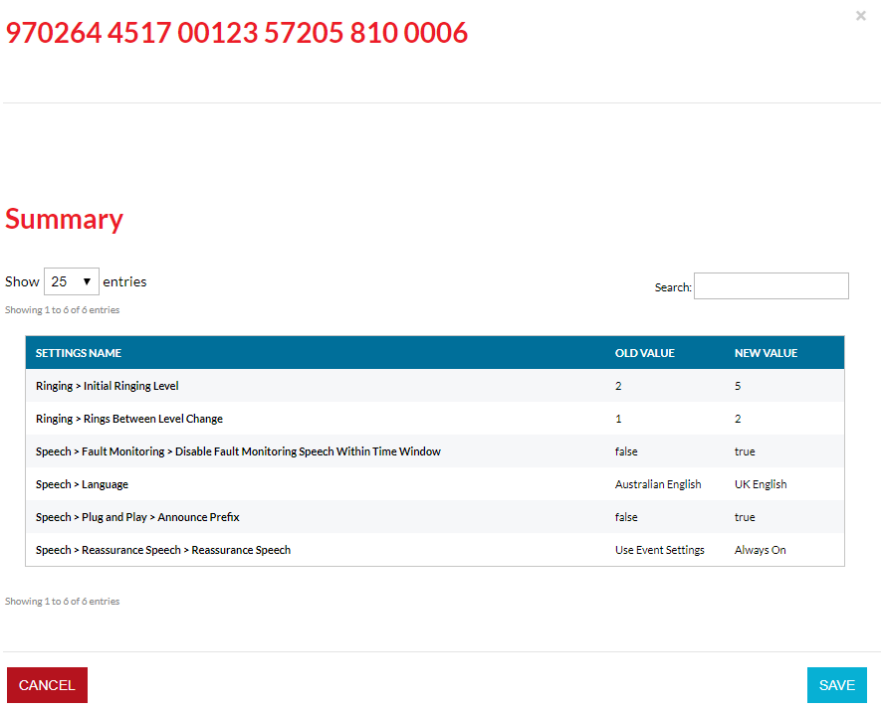
View a device's settings

To view a device's settings, select the required menu options in turn and then click **X** in the top-righthand corner of the window. The window closes and you return to the Device Information window.

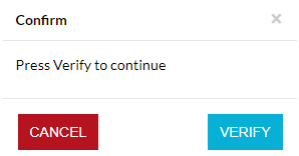
Edit a device's settings

To edit a device's settings:

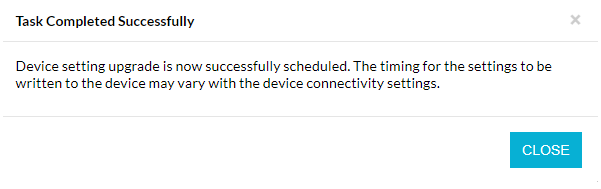
1. Select the required menu options in turn and make the relevant changes. As you change each setting, DMP outlines its field in red.
2. Click **SAVE**. DMP displays a list containing a summary of the changes you have made.



3. If required, use the standard table actions to filter, sort and search through the list.
4. If the changes are complete and correct, click **SAVE**. DMP displays a confirmation message:



5. Click **VERIFY**. DMP displays an information message:



6. Click **CLOSE**.

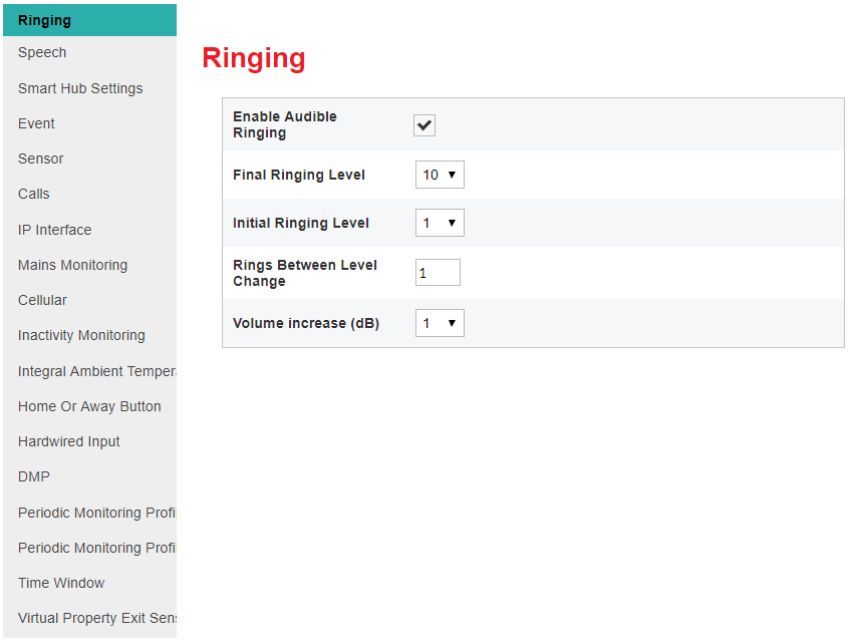
   DMP waits until the device sends a heartbeat. It then downloads the amended settings for the device to apply. Whilst the download and upgrade are taking place, the device has a technical status, indicated by the colour blue. On successful completion of the upgrade, the status changes to 'OK', indicated by green.

   Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, so prompting a DMP connection and initiating the download.

7.2.1 Device Settings window – Ringing menu option

You use the **Ringing** menu option to control the device's ringing behaviour and volume when it receives an incoming call to its mobile number.

Unlike previous Tunstall products, the Smart Hub does not utilise the user's home telephone service, so cannot be used as a hands-free phone. However, it can accept incoming calls relating to the user's telecare service, typically from the monitoring centre in response to an alarm call.



With this menu option, the main panel contains the following fields:

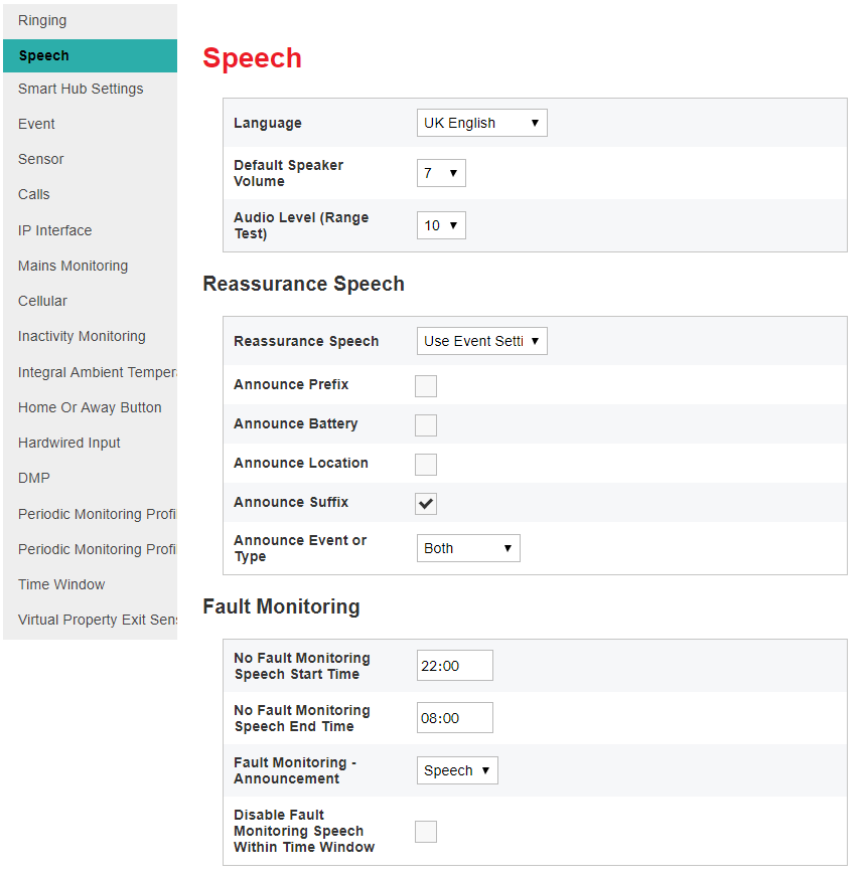
Field	Description
Enable Audible Ringing	If ticked, enables the device to ring if the Ringer On/Off switch on the base of the device is set to 'On'. If unticked, the device cannot ring, regardless of the setting of the Ringer On/Off switch. Default is ticked.
Final Ringing Level	The maximum volume level to which the device's ringing will rise. Can be set from 1 to 10 where 1 is the lowest noise level. Default is 10.

Field	Description
Initial Ringing Level	The initial volume level for a device. A device starts ringing at this level and increases to the maximum level defined in the previous field, at a rate specified by the next two fields. Can be set from 1 to 10 where 1 is the lowest noise level. Default is 1.
Rings Between Level Change	The number of rings to be made before DMP increases the noise level. Default is 1.
Volume Increase	The level by which DMP increases the volume after each set of rings. Default is 1. For example, if you have an initial volume level of 1, a final volume level of 10 and choose a volume increase of 4 then the ringing will begin at volume level 1, then after each set of ring bursts, jump to level 5, level 9 and then the maximum possible level 10.

7.2.2 Device Settings window – Speech menu option

You use the **Speech** menu option to specify:

- the general attributes of the announcements played through the loudspeaker to the user
- the format of alarm call reassurance announcements and sensor registration announcements
- how faults such as power failure are to be communicated to the user.



With this menu option, the fields are split into four sections:

- **Unlabelled first section**
  This specifies the general attributes of all announcements
- **Reassurance Speech**
  This specifies the elements of the announcement to be played whenever an alarm call is raised, either automatically by a sensor or manually by the user. The device plays the elements in the following order:

  <Prefix><Type><Event><Battery Status><Location><Suffix>

  For example, if the <Prefix> <Type> and <Suffix> elements are to be played, the user may hear:

  Alarm – Flood detector – Do not worry, contacting assistance
- **Fault Monitoring Speech**
  This specifies how faults are to be communicated to the user. It includes an option to turn off this communication for a set time period each day, typically overnight, though all faults are reported

to the monitoring centre. This functionality applies to fault events, but not alarms. The set of fault events comprise:

- communication path failures
- main power failure
- battery fault
- SIM card problems
- button stuck down
- no user activity detected by sensors
- hardwired relay connection failure.

- **Plug and Play Configuration**
  This specifies the elements of the announcement to be played when registration of a sensor/trigger is complete. The elements are played in the following order:

  <Prefix><Type><Suffix>

  For example, if the <Prefix> <Type> and <Suffix> elements are to be played, the user may hear:

  Radio Trigger – Flood detector – Registered

With this menu option, the main panel contains the following fields:

Field	Description
Language	The language of each announcement. Default is “UK English”.
Default Speaker Volume	The default speaker volume of the device. Can be between 1 and 10. Default is 7.
Audio Level (Range Test)	The speaker volume of the device during range tests. Can be between 1 and 10. Default is 10.

Reassurance Speech

Reassurance Speech	Indicates whether an announcement is to be played whenever an alarm call is raised, that is, when an event configured using the **Events** menu option occurs. Can be one of: • Off – the device does not play an announcement • Use Event Settings – the device plays an announcement if the event that triggers the alarm call has its **Audible Reassurance** attribute enabled • Always On – the device plays an announcement. Default is “Use Event Settings”.
Announce Prefix	If ticked, the device includes the <Prefix> element of the announcement; if clear, it is omitted. The <Prefix> element is the word “Alarm”. Default is unticked.

Field	Description
Announce Battery	If ticked, the device includes the <Battery Status> element of the announcement whenever the battery status is low; if clear, it is omitted. The <Battery Status> element is the phrase “Low battery”. Default is unticked.
Announce Location	If ticked, the device includes the <Location> element of the announcement; if clear, it is omitted. The <Location> element is the location of the sensor that raises the alarm call, for example, “Kitchen”. Default is unticked.
Announce Suffix	If ticked, the device includes the <Suffix> element of the announcement; if clear, it is omitted. The <Suffix> element is the phrase “Do not worry, contacting assistance”. Default is ticked.
Announce Event or Type	Indicates the inclusion/omission of the <Event> and <Type> elements of the announcement. Can be one of: • Neither – the device omits both <Event> and <Type> elements from the announcement • Type Only – the device includes the <Type> element of the announcement but omits the <Event> element • Event Only – the device includes the <Event> element of the announcement but omits the <Type> element • Both – the device includes both <Event> and <Type> elements of the announcement. Default is “Both”. The <Event> element is the name of event that initiates the alarm call, for example, “CO Detector Activation”, which maps to one of the events listed when you select the **Events** menu option. The <Type> element is the type of sensor/trigger that raises the alarm call, for example, “Flood detector”. The device derives this from the sensor/trigger’s **Sensor Type** field entry you see when you select the **Sensor** menu option. For details, refer to Appendix C, List of supported radio peripherals.

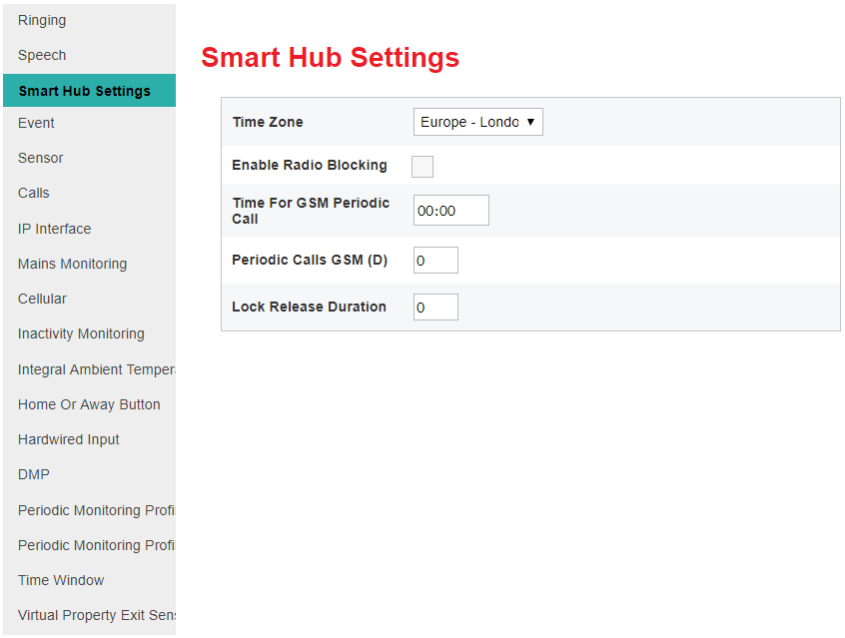
Fault Monitoring

No Fault Monitoring Speech Start Time	Specifies the start time of the time period for which the device will not warn the user of any fault. This suspension of fault reporting to the user is dependent on other fields in this section. Default is 22:00.
No Fault Monitoring Speech End Time	Specifies the end time of the time period for which the device will not warn the user of any fault. This suspension of fault reporting to the user is dependent on other fields in this section. Default is 08:00.

Field	Description
Fault Monitoring – Announcement	Defines how the device warns the user of a fault. Can be one of: • Off – does not warn the user • Beeps – uses tones to warn the user • Speech – uses a spoken announcement to warn the user. Default is “Speech”.
Disable Fault Monitoring Speech Within Time Window	If ticked, the device does not warn the user if it detects a fault during the specified time period; if clear or outside the specified time period, the device warns the user, as defined by the **Fault Monitoring Speech – Announcement** field. Default is unticked. **Note: This does not disable fault monitoring by the device nor the reporting of faults to the monitoring centre.**
Plug and Play	
Announce Prefix	If ticked, the unit includes the <Prefix> element of the announcement made when a ‘plug and play’ sensor/trigger is registered locally, that is, directly with the Smart Hub, bypassing DMP. The <Prefix> element is the phrase “Radio Trigger”. Default is unticked.
Announce Type	If ticked, the unit includes the <Type> element of the announcement made when a ‘plug and play’ sensor/trigger is registered locally, that is, directly with the Smart Hub, bypassing DMP. The <Type> element is the type of sensor being registered, for example, “Flood detector”. Default is ticked.
Announce Suffix	If ticked, the unit includes the <Suffix> element of the announcement made when a ‘plug and play’ sensor/trigger is registered locally, that is, directly with the Smart Hub, bypassing DMP. The <Suffix> element is the word “Registered”. Default is ticked.

7.2.3 Device Settings window – Smart Hub Settings menu option

You use the **Smart Hub Settings** menu option to configure the device's time zone, radio blocking interference reporting, GSM periodic call interval and the door lock release duration.



With this menu option, the main panel contains the following fields:

Field	Description
Time Zone	Time zone of the device. Should reflect the installation location of the device. Default is "Europe – London".
Enable Radio Blocking	Controls the reporting of detection of radio blocking interference. If enabled, on detection of interference, the unit: • reports the interference to DMP, but without changing the device's status • makes an appropriate announcement to the user • changes the LED status light on the unit to indicate poor radio coverage. Default is unticked.
Time for GSM Periodic Call	Not currently used.
Periodic Calls GSM	The number of days between voice band (GSM) test calls. If set to zero, the device does not make any GSM test calls. Can be between zero and 31. Default is zero.

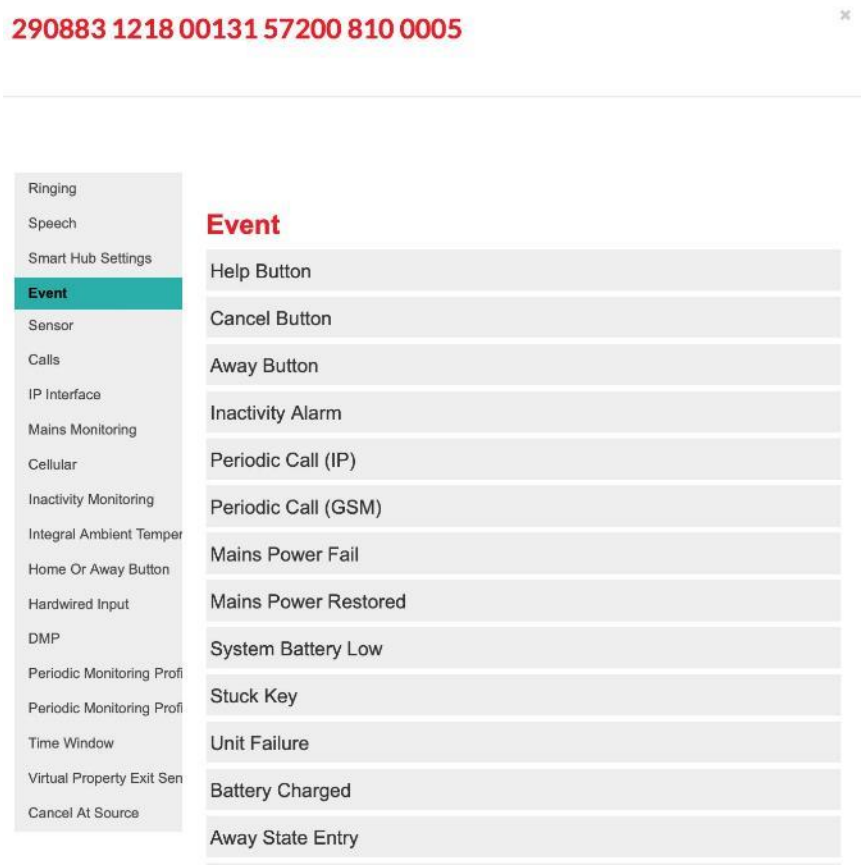
Field	Description
Lock Release Duration	Only relevant if the Smart Hub has a hardwired output that controls a door lock release mechanism. In this case, it defines the time in seconds for which the lock will be released whenever a release request is made by a monitoring centre operator.

7.2.4 Device Settings window – Event menu option

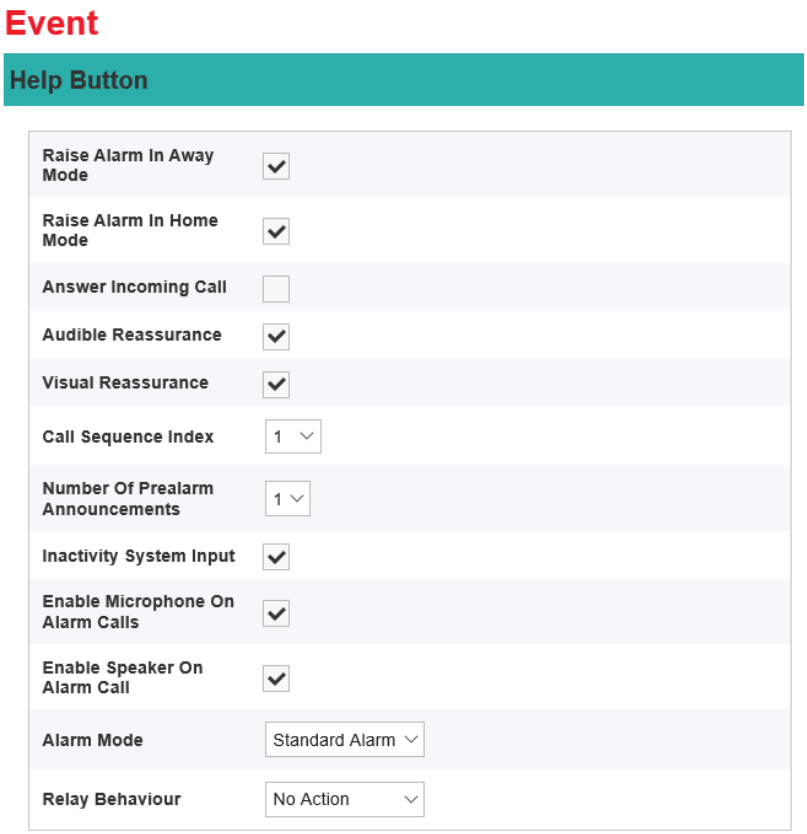
You use the **Event** menu option to define how the device handles any event that occurs, for example, when the user presses the red **Help** button, or a sensor is activated. Each event has the same set of attributes, which DMP uses to define:

- the appropriate alarm, if any, including its route to the monitoring centre
- reassurance of the client
- any output behaviour for the event, such as activating the hardwired output relay or resetting the inactivity timer.

For a list of the events and the default settings of their attributes, refer to Appendix D, Default settings of event attributes. Note that Tunstall may deliver devices with different defaults according to local requirements, or that your organisation may automatically apply a template on receipt of each device which updates this configuration.



With this menu option, the main panel initially lists each of the possible events. Click on an event to display its configuration:



The following fields define the behaviour of the device whenever the specified event occurs:

Field	Description
Raise Alarm In Away Mode	Relevant only if the yellow **Home/Away** button is configured to change monitoring levels, as described in Section 7.2.12, Device Settings window – Home Or Away Button menu option. In this case, ticking this field causes the device to raise an alarm call to the monitoring centre even if the device is in Away mode. If unticked, the device takes no action when the device is in Away mode.
Raise Alarm In Home Mode	If ticked, this field causes the device to raise an alarm call to the monitoring centre and either: • the Home and Away modes are in use and the device is in Home mode, or, • the Home and Away modes are not in use. If unticked, the device takes no action.

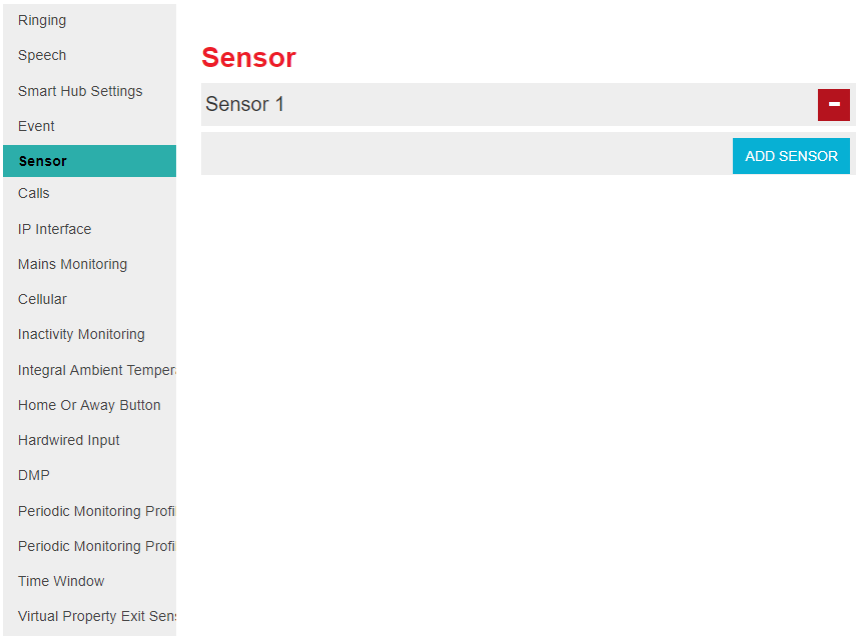
Field	Description
Answer Incoming Call	If ticked, the event can be used to trigger the connection of an incoming call. **Note: This should be disabled for the Away Button event and, most importantly, for the Help Button event which occurs when the user raises an alarm by pressing the red Help button.**
Audible Reassurance	If ticked, the device provides audible reassurance to the user. Refer to Section 7.2.2, Device Settings window – Speech menu option, for details on the structure of this reassurance.
Visual Reassurance	If ticked, the device provides the visual assurance to the user by causing the red **Help** button to flash once every second, indicating an alarm call has been raised.
Call Sequence Index	The call sequence index to be used for the event. This determines the destination, that is, the monitoring centre, to which the device is to send any alarm call associated with the event, and how the call is to be sent. For details on the mapping of destinations and call sequence indexes, refer to Section 7.2.6, Device Settings window – Calls menu option. By convention, organisations use call sequence indexes 9 and 10 for the IP Periodic Call (IP) event and IP Periodic Call (GSM) event respectively.
Number Of Pre-Alarm Announcements	The device informs the user about the event by making an announcement, at regular intervals, before raising the alarm call at the monitoring centre. This field defines the number of announcements to be made before the alarm call is raised. During this time, the user can cancel the alarm, if required.
Inactivity System Input	If ticked, the event is used as a monitor of user inactivity as described in Section 7.2.10, Device Settings window – Inactivity Monitoring menu option.
Enable Microphone On Alarm Calls	If ticked, the device enables its internal microphone when it raises the alarm call for the event, so allowing the user to speak to the monitoring centre operator. If unticked, the microphone remains disabled.
Enable Speaker On Alarm Call	If ticked, the device enables its internal speaker when it raises the alarm call for the event, so allowing the monitoring centre operator to speak to the user. If unticked, the speaker remains disabled.
Alarm Mode	Set to “Standard Alarm” by default. Should be changed to “Cancel At Source” if this type of response is appropriate. The “Callback” option is not currently used.

Field	Description
Relay Behaviour	Used for events which are required to operate the Smart Hub's relay. The relay allows external equipment to be controlled by wired connection. This field defines the relay switching pattern and is one of: • No Action • Relay On • Relay Off • Single Pulse 1 Second • Single Pulse 2 Second • Single Pulse 4 Second • Pulse 1 SEC • Pulse 2 SEC • Pulse 4 SEC. Default is "No Action".

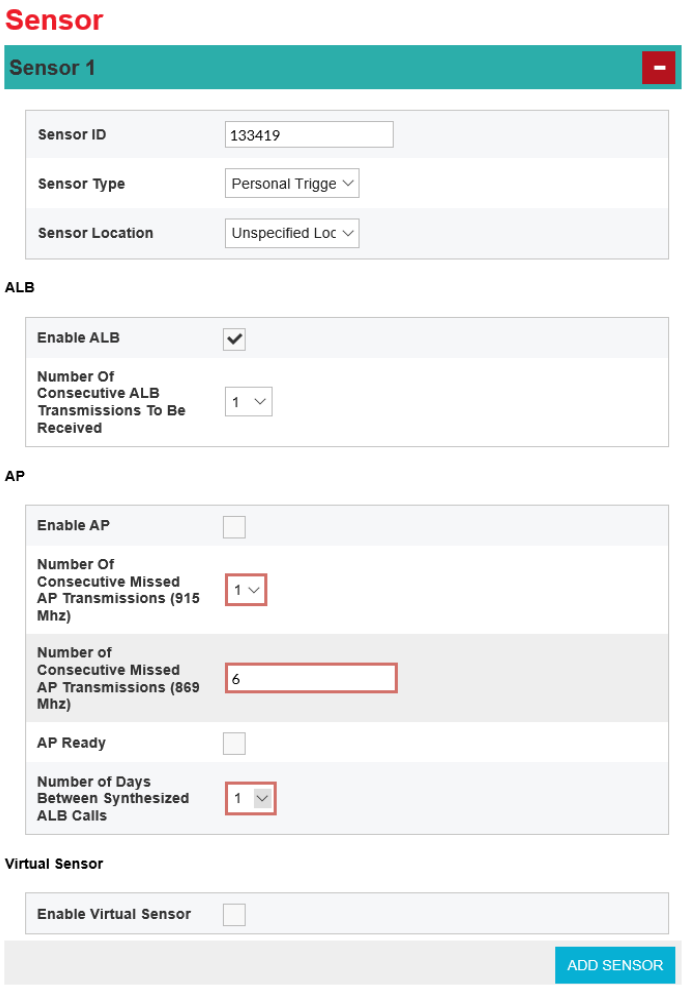
7.2.5 Device Settings window – Sensor menu option

You use the **Sensor** menu option to register and maintain the telecare sensors and personal triggers associated with the device. These comprise the pendant radio trigger provided with the Smart Hub, plus additional radio triggers and telecare sensors. For a full list of available sensors/triggers, refer to Appendix C, List of supported radio peripherals. Note that the pendant radio trigger provided with the Smart Hub comes pre-registered.

Alternatively, 'plug and play' sensors/triggers may be registered directly with the Smart Hub, bypassing DMP. In this case, DMP will not display details of these sensors/triggers until the Smart Hub connects to DMP and updates DMP with the new sensor/trigger details. For further details, refer to the *Smart Hub Installation Guide*.



With this menu option, the main panel initially lists an index citing each sensor/trigger currently registered. Click on a sensor/trigger index bar to display the configuration of the associated sensor/trigger:



Each sensor/trigger panel contains the following fields:

Field	Description
Sensor ID	The identifier of the registered sensor/trigger.
Sensor Type	The type of the registered sensor/trigger, for example, “Personal Trigger”, “Fall Detector” or “Pressure Mat”.
Sensor Location	Used to distinguish multiple sensors of the same type, such as: • by resident to identify the owner of the sensor • by location of the registered sensor, for example, “Kitchen”. Used only for fixed location sensors such as fire detectors. • by appliance names, for example, for temperature detectors “Stove” • the type of door, for example, “Medicine Cabinet Door” or “Fridge Door” for “Door Contact” sensors.
ALB – Auto Low Battery	
Enable ALB	If ticked enables Auto Low Battery – The Sensor will automatically test its battery every 7 days. Generates a notification to the Smart Hub, if the Sensor’s battery is low.
Number Of Consecutive ALB Transmissions To Be Received	Defines the number of unsuccessful transmissions between the Smart Hub and the Sensor before an alarm is raised. Parameters can be set between 1-10 transmission
AP – Auto Presence	
Enable AP	Enables Auto Presence – The generation of a signal between the Smart Hub and the Sensor to notify that they are in communication. If successful communication is not maintained an alarm will be raised.
Number of Consecutive Missed AP Transmissions (915 MHz)	Defines the number of unsuccessful transmission signals that can be made in sequence between the Sensor and Smart Hub before an alarm is raised. For devices operating at 915 MHz a signal is sent every 24 hours. Parameters can be set between 1-7 transmission fails (1-7 days). The default is 1 (day).
Number of Consecutive Missed AP Transmissions (869 MHz)	Defines the number of unsuccessful transmission signals that can be made in sequence, between the Sensor and Smart Hub before an alarm is raised. For devices operating at 869 MHz a signal is sent every 4 hours. Parameters can be set between 1–42 transmission fails (4-96 hours). The default is 6 (24 hours).

Field	Description
AP Ready	Disables AP monitoring until an AP transmission is received from this sensor. It is used if the sensor is being pre-assigned and then dispatched by post to arrive at the Smart Hub later.
Number of Days Between Synthesised ALB Calls	The sensor will issue an ALB notification to the Smart Hub alongside its AP signal when the battery is low. This option sets the number of days from 1-15, for the ALB AP transmission to pass before an alarm is raised. This should be adjusted depending on the sensor type e.g., a smoke detector should be set to 1.
Virtual Sensor	
Enable Virtual Sensor	Only relevant for "Door Contact" and "Passive Infrared (PIR) sensors". Must be unticked for all other types of sensors. If ticked, indicates that the sensor is one of the two that make up the virtual property exit sensor. To implement the virtual property exit sensor, you need to enable at least one "Door Contact" and one "Passive Infrared (PIR)" sensor.

With this menu option, you can also:

- add a new sensor/trigger
- delete an existing sensor/trigger.

Add a new sensor/trigger

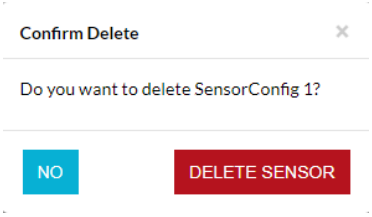
To add a new sensor/trigger:

1. Click the **ADD SENSOR** button. DMP displays the configuration fields for the sensor/trigger.
2. Update the settings of the fields as required. DMP will save the details of the sensor/trigger when you complete the update of the device settings by clicking the **SAVE** button.

Delete an existing sensor/trigger

To delete an existing sensor/trigger:

1. Click the appropriate sensor/trigger index bar to display its configuration.
2. Ensure you have selected the correct sensor/trigger by checking the **Sensor ID** field.
3. Click the − button in the sensor/trigger index bar. DMP displays the following confirmation message:



4. Click the **DELETE SENSOR** button. DMP will remove the details of the sensor/trigger from the device's record when you complete the update of the device settings by clicking the **SAVE** button.

7.2.6 Device Settings window – Calls menu option

You use the **Calls** menu option to define the destinations of alarm calls, how they are to be routed and general management of the calls.

DMP provides a highly flexible mechanism to define the routing of alarms, this feature allows for alarms to be routed to different destinations according to alarm type. In the case of connection failure, it allows different connection protocol/technologies to be used, or even the automatic switching of the destination to an alternative monitoring centre. This ensures that an alarm call always has a fall-back route. For a simple example of how this may be configured within DMP, refer to Appendix E, Call sequence usage example.

Typically, an organisation only requires relatively simple routing, with one or two different routings of calls. DMP however, can handle much more complex routing with varying multiple destinations for different events.

Due to the possible complexity of routing calls, Tunstall recommends organisations set up the attributes relating to this menu option by means of a template, as described in Section 6.6, Assign Template window, to ensure each device has correct configuration.

Call sequences

To enable this flexible calling mechanism, the Smart Hub maintains a set of 'call sequences', as used by other Tunstall Lifeline products. Each call sequence comprises:

- up to 10 'destinations' that are to be called in their defined order, until a connection is made
- for each defined destination, the number of connection attempts that are to be made to that destination before moving on to the next one in the sequence
- a flag indicating if the sequence of calls is to be repeated if all connection attempts to all destinations fail

The pairs of destination and connection attempt numbers are known as 'call sequence records'.

Each device can have up to 10 call sequences. They are identified by a number from 1 to 10, known as the 'call sequence index'. To route different types of alarm calls to different destinations, you set up the call sequences with the appropriate destinations, and then allocate the appropriate call sequence index to the relevant event. The allocation of the call sequence indexes is described in Section 7.2.4, Device Settings window – Event menu option.

If an organisation uses IP periodic calling, then by convention, call sequence indexes "9" and "10" are allocated for use by the IP Periodic Call (IP) event and IP Periodic Call (GSM) event respectively. As such, all the destinations defined for call sequence "9" must define IP destinations and all the destinations defined for call sequence "10" must define telephone destinations.

Destinations

A Smart Hub can have up to 10 defined 'destinations' that define both the end location of the call and the method to be used to make the call. Each destination comprises:

- the local identifier of the Smart Hub used by the monitoring centre
- indication of whether the call is to use a telephone or an IP connection mode
- if the call is a telephone call:
  - the number to use for the call
- if the call is an IP call:

- the URL/IP address of the destination
- protocol to be used
- ARC port and number
- SIP details
- type of connection path to be used
- type of voice channel to be used
- if the call is a GSM call using the IPACS protocol, the origin of the call.

Each destination can be used in multiple call sequences. The destinations are identified by a number from 1 to 10, known as the 'destination index'. You identify a destination by its index when creating call sequences.

Whenever possible, the final destination of each call sequence should define a telephone call, as this requires the minimum level of cellular network service. When this is not possible, an SMS connection could be defined as this is often available when IP data communications are not, though no delivery time, or even actual delivery, is guaranteed by the network.

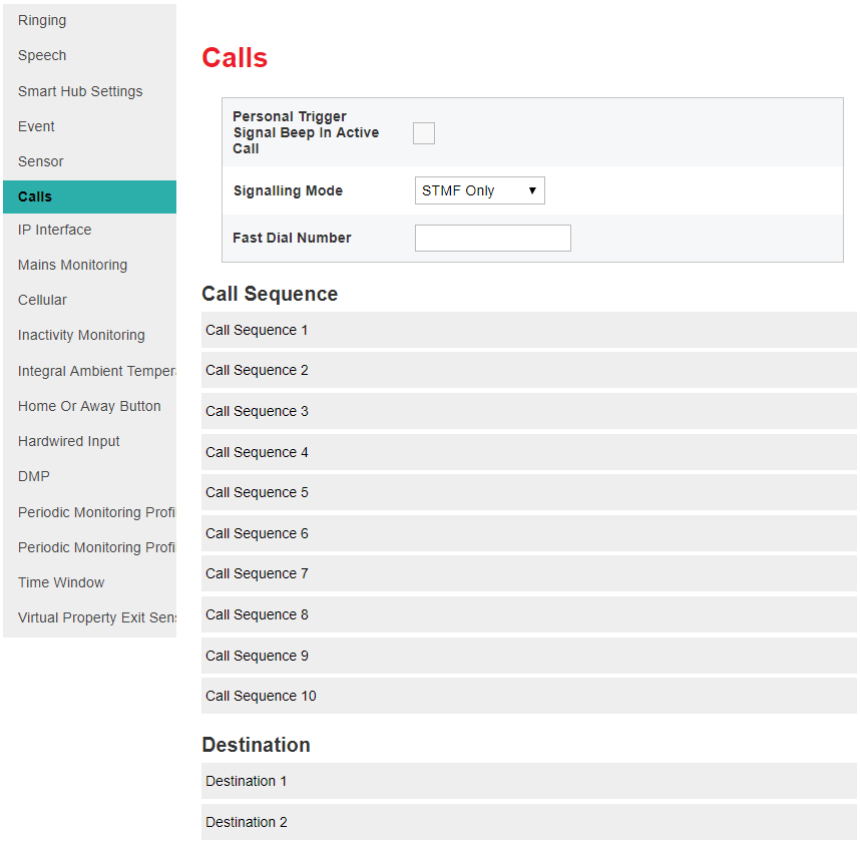
Other attributes relating to the Call menu option

You also use the **Calls** menu option to define other call-related attributes, namely:

- whether the client can use the supplied pendant trigger to send audio beeps to the operator after making an alarm call with it
- the signalling mode to be used for tone protocols, i.e. all destinations that are defined as telephone calls.

Screen description

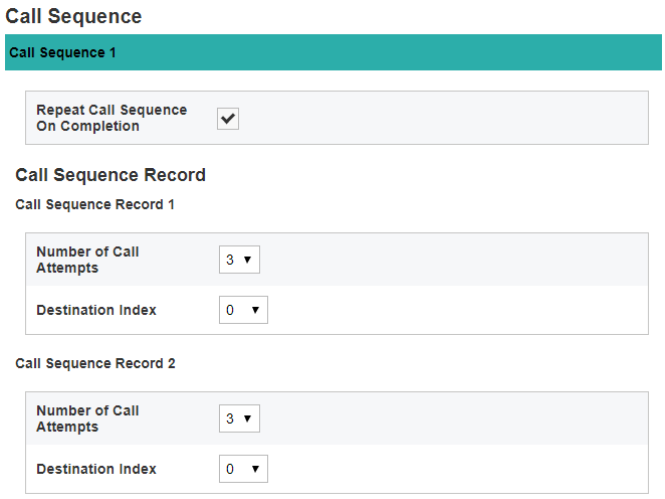
With this menu option, the main panel initially lists three general call-related attributes and then the 10 call sequences followed by the 10 destinations.



The three general attributes are:

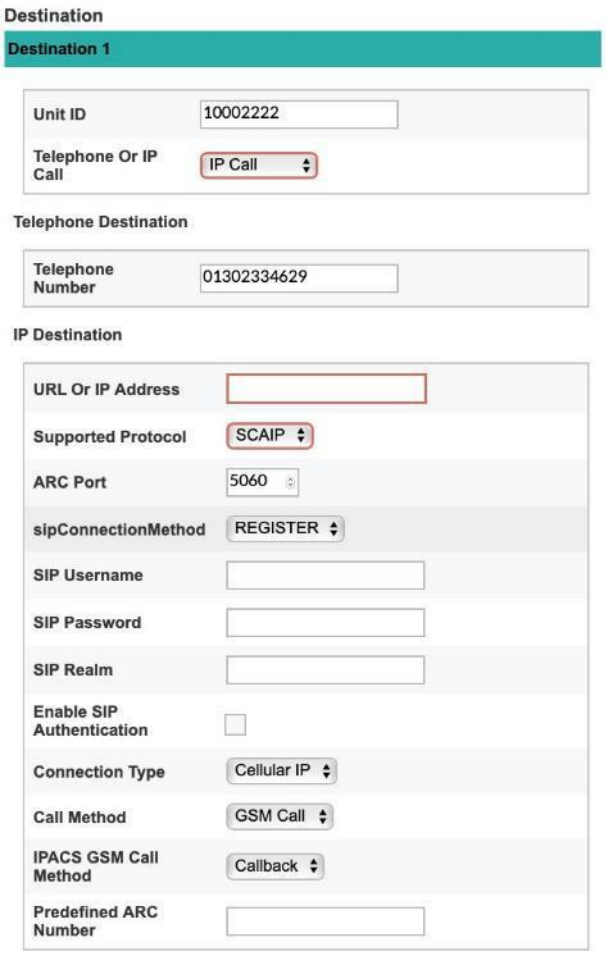
Field	Description
Personal Trigger Signal Beep In Active Call	Allows the pendant trigger that raised the alarm call to be used to communicate with the operator using its audio beeps once a call connects. This is for use when the client cannot speak or be heard by the operator. Default is unticked.
Signalling Mode	Specifies the signalling mode to be used for all 'Telephone Call' destinations. Can be one of: • STMF Only – preferred option as it is more resilient over cellular voice band connections • DTMF Only – use only if the destinations use the BS8521 protocol • Last Successful – switches signalling modes when necessary. However, switching modes may cause noticeable connection delays and so this option should only be used if the telephone destinations are only used once IP connections have been attempted. Default is "STMF Only".
Fast Dial Number	Not currently used.

When you click on a sequence you see the following fields, with 10 sequence records visible:



Field	Description
Repeat Call Sequence On Completion	Indicates whether to repeat the call sequence after all the connection attempts on the call sequence have been made. If ticked, the call sequence repeats endlessly until the alarm call succeeds. For those alarms that have a pre-alarm period, the user may cancel the alarm during that period by pressing the green **Cancel** button. If clear and all the connection attempts defined by the call sequence have been made, the Smart Hub announces, "The Call Sequence has ended". It repeats this announcement indefinitely until the client presses the green **Cancel** button. Each alarm call that fails to connect requires its own individual cancellation. **Note: Check your national legislation allows the use of this feature if the sequence defines a telephone call. Consider cellular data usage if the sequence defines an IP call. Your supplier can advise further.** Default is ticked.
For each call sequence record:	
Number of Call Attempts	Defines the number of attempts to be made to connect to the specified destination. When set to 0, no attempt is made to connect to the destination. Can be between 0 and 10. Default is 3.
Destination Index	Indicates the destination to which a connection is to be made. Default is 0.

When you click on a destination you see the following fields:



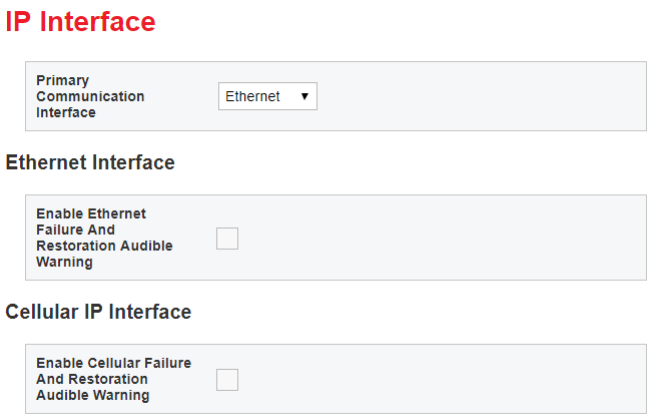
Field	Description
Unit ID	Identifies the Smart Hub at the monitoring centre. Different destinations may use different identifier numbers for a device, or they may be coordinated and use the same one. Note that this is not the unique PRC identifier used by Tunstall and within DMP. Default is 4108888812.
Telephone Or IP Call	D whether Smart Hub initiates an IP connection or initiates a telephone call or uses SMS messaging when attempting to connect to this destination. Can be one of: • IP Call • Telephone Call • SMS. You complete either the **Telephone Destination** or **IP Destination** set of attributes, depending on the selected value. Default is “IP Call”.

Field	Description
Telephone Destination - completed when “Telephone Call” or “SMS” is selected from the **Telephone Or IP Call** drop-down list.	
Telephone Number	Telephone number of the call/SMS destination. As the SIM card provided with the device can operate on multiple networks (‘roaming SIM’), you must use the full international number style, for example, “0044” or “+44” for a UK number. Similarly, you should not use any number which has a non-geographical code, such as “0800”.
IP Destination – completed when “IP Call” is selected from the **Telephone Or IP Call** drop-down list.	
URL Or IP Address	Either the written or numeric IP address of the destination, e.g. “example.domain.com” or “123.456.789.012”.
Supported Protocol	The IP alarm protocol to be used to communicate with the monitoring centre. Must match the capability of the monitoring centre. Can be one of: • IPACS – used with Tunstall’s Piper Network Controller (PNC) software • SCAIP – used with some third party alarm monitoring software. Default is “SCAIP”.
ARC Port	The port to be used for the IP Alarm protocol, either SCAIP or IPACS. Determined by the monitoring centre’s network configuration. Default is 5060.
SIP Connection Method	Determined by the monitoring centre's protocol implementation and configuration. Default is Register.
SIP Username	The username used to register with the SIP registrar. Determined by the monitoring centre’s network configuration.
SIP Password	The password used to authenticate with the SIP registrar. Determined by the monitoring centre’s network configuration.
SIP Realm	May be required for SIP registration. Determined by the monitoring centre's configuration.
Enable SIP Authentication	Indicates whether SIP authentication, that is, SIP registration, is enabled. Determined by the monitoring centre’s network configuration.
Connection Type	The type of connection path to be used for the alarm call. Can be one of: • Ethernet • Cellular IP. Default is “Ethernet”.

Field	Description
Call Method	The type of voice channel to be used during the call. This defines how voice is to be transmitted during the alarm call. Can be one of: • VoIP Call • GSM Call. Default is “VoIP Call”.
IPACS GSM Call Back Method	Used only for GSM calls using the IPACS protocol, its value is ignored for all other types of calls. Defines whether the voice call is to originate from the monitoring centre or Smart Hub respectively. Can be one of: • Callback – voice call is to originate from the monitoring centre • Dial out – voice call is to originate from the Smart Hub. Default is “Callback”.
Predefined ARC Number	Not currently used.

7.2.7 Device Settings window – IP Interface menu option

You use the **IP Interface** menu option to register the preferred channel for communications between the Smart Hub and DMP using digital internet protocols (IP). Communications may take place using fixed line broadband (Ethernet Interface) or cellular/mobile networks (Cellular IP Interface). You also use this menu option to define whether the device announces the failure and restoration of the preferred channel to the user.

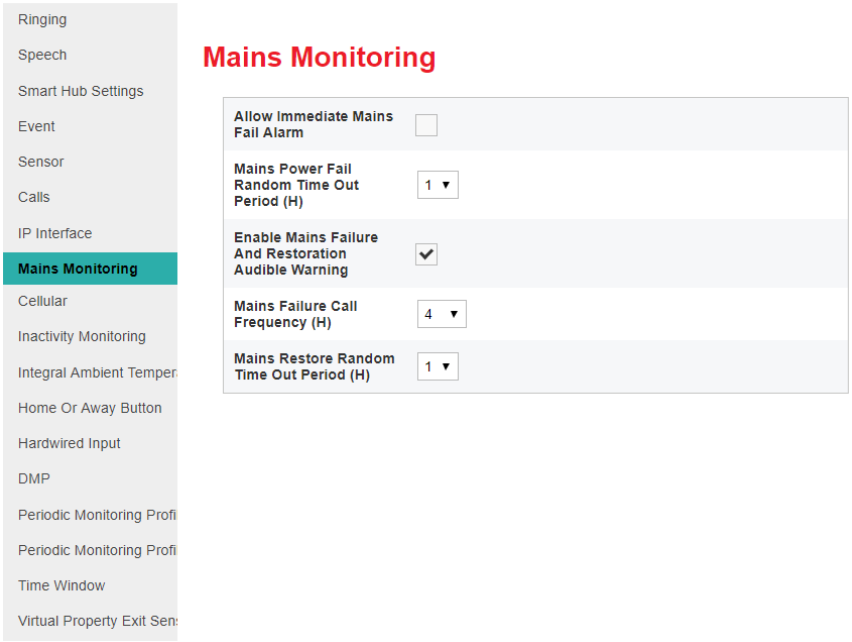


With this menu option, the main panel contains the following fields:

Field	Description
Primary Communication Interface	The preferred channel for communicating with DMP. If unavailable, the device attempts to communicate using the other channel. Can be one of: • Ethernet • Cellular IP. Default is “Ethernet”.
Ethernet Interface	
Enable Ethernet Failure And Restoration Audible Warning	If ticked, the device announces each ethernet failure and each ethernet restoration. If unticked and “Ethernet” is the preferred channel, no announcements are made. Typically, the checkbox is unticked so that the client is not disturbed during network interruptions or maintenance and only ticked for diagnostic purposes. This setting does not affect the status indicators on the Smart Hub nor the announcement made whenever both connections are unavailable. Default is unticked.
IP Cellular Interface	
Enable Cellular Failure And Restoration Audible Warning	If ticked, the device announces each cellular IP failure and each cellular IP restoration. If unticked and “Cellular IP” is the preferred channel, no announcements are made. Typically, the checkbox is unticked so that the client is not disturbed during network interruptions or maintenance and only ticked for diagnostic purposes. This setting does not affect the status indicators on the Smart Hub nor the announcement made whenever both connections are unavailable. Default is unticked.

7.2.8 Device Settings window – Mains Monitoring menu option

You use the **Mains Monitoring** menu option to control how the device monitors a failure or restoration of the external power source, in conjunction with the attributes of the Mains Power Fail and Mains Power events and the device's fault monitoring settings.



.

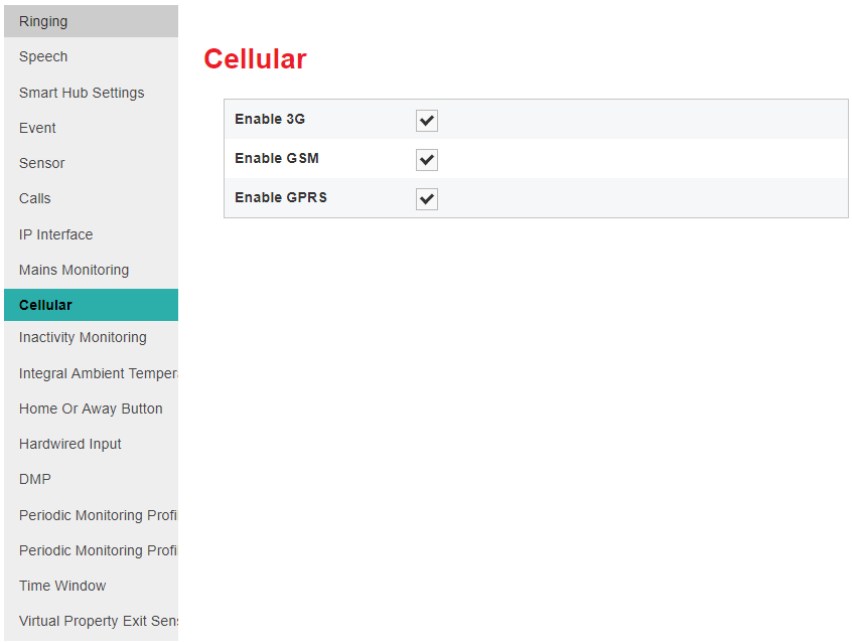
With this menu option, the main panel contains the following fields:

Field	Description
Allow Immediate Mains Fail Alarm	If ticked, the device immediately raises an alarm call to the monitoring centre whenever: • the device detects a mains power failure, and, • the Mains Fail event is configured to raise an alarm call, as described in Section 7.2.4, Device Settings window – Event menu option. Ticking this field overrides the timeout period specified by **Mains Power Fail Random Timeout Period**. If unticked, the **Mains Power Fail Random Timeout Period** setting determines when the device raises the alarm call. **Note: Tunstall suggest you enable this option only for selected, high-risk clients; otherwise, an area outage may result in the monitoring centre 'flooding' with simultaneous calls from devices in the area.**

Field	Description
Mains Power Fail Random Timeout Period	The minimum time in hours to delay raising an alarm call about the failure to the monitoring centre. The device then raises the alarm call at a random point in the following hour, to avoid 'flooding' the monitoring centre in the case of an area outage. For example, if this field is set to 1, the device raises an alarm at some time between one and two hours after detecting the failure. Applies only if the Mains Power Fail event is configured to raise an alarm call, as described in Section 7.2.4, Device Settings window – Event menu option; otherwise the device does not raise an alarm call. Default is 1.
Enable Mains Failure And Restoration Audible Warning	If ticked, the device makes an announcement whenever it detects a mains failure or restoration; otherwise the user is not informed. Both failure and restoration are defined as faults rather than alarms. This means that you can use the fault monitoring feature to suppress the announcement for a time, typically overnight, as described in Section 7.2.3, Device Settings window – Smart Hub Settings menu option. Default is ticked.
Mains Failure Call Frequency	Defines the frequency, in hours, that the device sends alarm calls to the monitoring centre in the case of mains failure. Default is 4.
Mains Restored Random Timeout Period	The minimum time in hours to delay raising an alarm call about the restoration of power to the monitoring centre. The device then raises the alarm call at a random point in the following hour, to avoid 'flooding' the monitoring centre in the case of an area outage. For example, if this field is set to 1, the device raises an alarm at some time between one and two hours after detecting the restoration. Applies only if the Mains Power event is configured to raise an alarm call, as described in Section 7.2.4, Device Settings window – Event menu option; otherwise the device does not raise an alarm call. Default is 1.

7.2.9 Device Settings window – Cellular menu option

The **Cellular** menu option displays settings relating to the cellular communication channels used by the device. You should leave them unchanged, unless advised by your supplier.



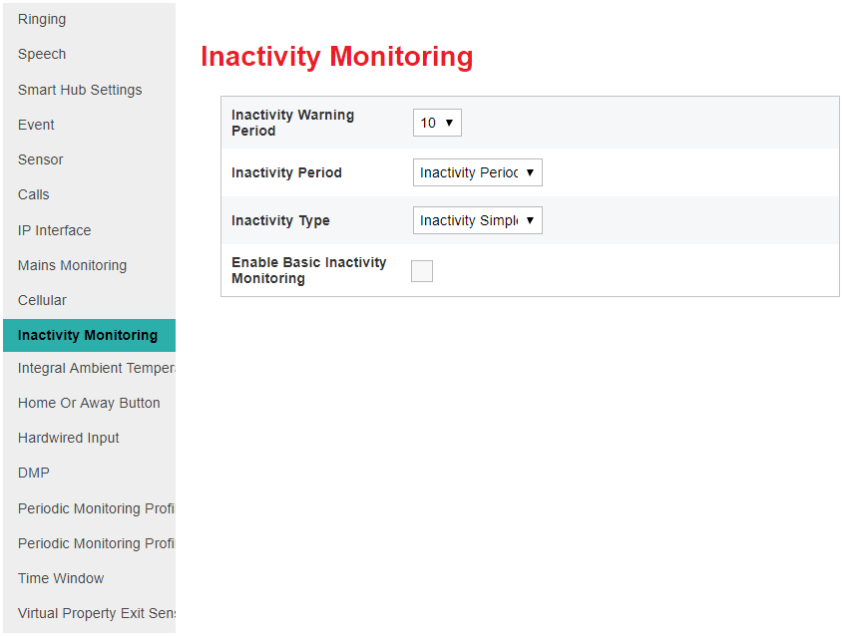
With this menu option, the main panel contains the following fields:

Field	Description
Enable 3G	If ticked, enables cellular communication using the 3G networks. Do not change this setting unless advised by your supplier. Default is ticked.
Enable GSM	If ticked, enables cellular communication using the 2G networks. Do not change this setting unless advised by your supplier. Default is ticked.
Enable GPRS	If ticked, enables cellular data communication using the GPRS data service. Do not change this setting unless advised by your supplier. Default is ticked.

7.2.10 Device Settings window – Inactivity Monitoring menu option

You use the **Inactivity Monitoring** menu option to control how, if at all, the Smart Hub monitors for user inactivity, in other words, an absence of user activity. User activity is inferred by the device whenever it detects an event that is defined as reporting activity. For details of which events report activity, refer to Appendix D, Default settings of event attributes.

If the unit detects no such activity for the inactivity monitoring time period, it continually announces, “An inactivity alert is about to be made; please press cancel”, for a defined time period, known as the inactivity warning period. If the user does not cancel the alarm during the inactivity warning period, the unit then raises an alarm call to the monitoring centre.



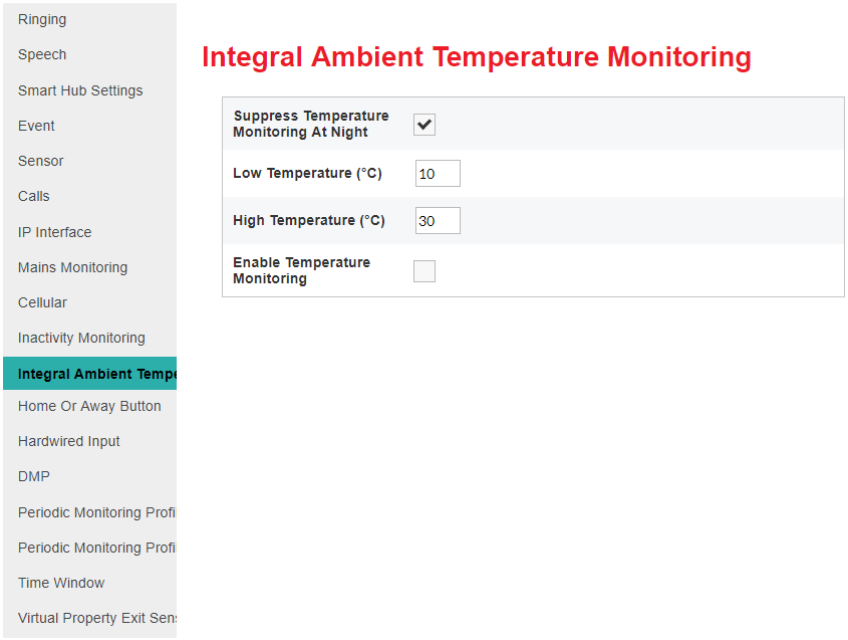
With this menu option, the main panel contains the following fields:

Field	Description
Inactivity Warning Period	Before an inactivity alarm is raised, an inactivity warning period occurs. This warning period is intended to inform the user that an inactivity alarm is about to be raised, therefore giving them the opportunity to cancel the alarm. Can be between 0 and 10 minutes. Default is 10.

Field	Description
Inactivity Period	If an event which reports activity does not occur for this time period, the device enters an inactivity warning period and begins the pre-alarm announcements. Can be one of: • Inactivity Period 12 Hours • Inactivity Period 24 Hours. If the device goes into an Away state, as described in Section 7.2.12, Device Settings window – Home Or Away Button menu option, it suspends monitoring until it returns to a Home state. As the Home State Entry event is one of the events that reports activity, the time period is reset on return to this state. Default is “Inactivity Period 12 Hours”.
Inactivity Type	Indicates, together with **Enable Basic Inactivity Monitoring**, whether the inactivity feature is enabled or disabled. Can be one of: • Inactivity Simple • Inactivity Disabled. Default is “Inactivity Simple”.
Enable Basic Inactivity Monitoring	If ticked and **Inactivity Type** is set to “Inactivity Simple” then the inactivity feature is enabled; otherwise the feature is disabled. Default is unticked.

7.2.11 Device Settings window – Integral Ambient Temperature menu option

You use the **Integral Ambient Temperature** menu option to control temperature detection, and any subsequent announcements and alarm calls. If a Smart Hub or associated sensor detects a temperature outside the ambient temperature range, a Temperature Extremes Sensor (TES) High Temp or TES Low Temp event occurs, as appropriate, which the device handles as defined by the event's attributes. Refer to Section 7.2.4, Device Settings window – Event menu option, for details on setting up these attributes.



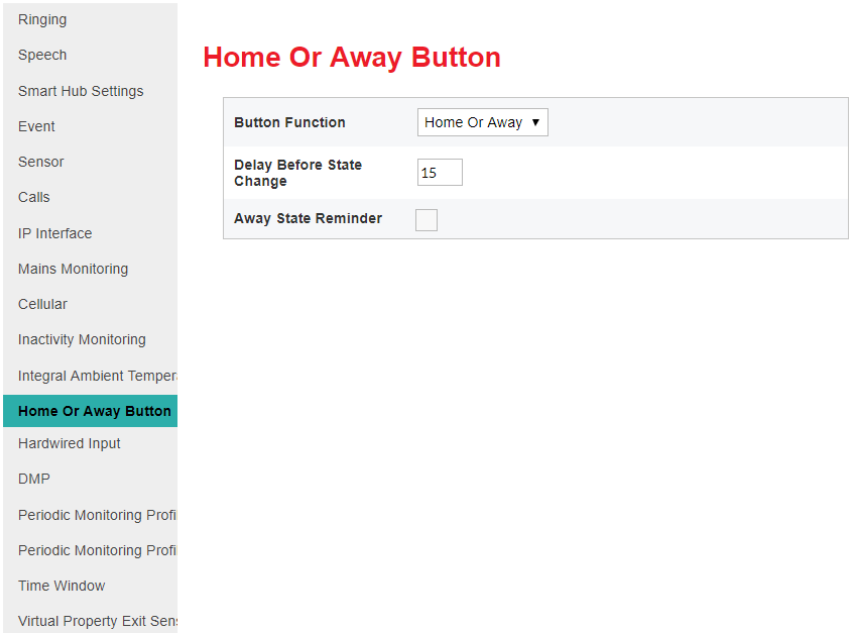
With this menu option, the main panel contains the following fields:

Field	Description
Suppress Temperature Monitoring At Night	If ticked, the device suppresses the generation of temperature monitoring events for the time period specified by the fault monitoring feature, described in Section 7.2.2, Device Settings window – Speech menu option; otherwise it always actions them. Typically, this time period will be overnight, but it can be any portion of a day. Default is ticked.
Low Temperature (°C)	The threshold for generating a TES Low Temp event in degrees Celsius. Can be between 0 and 50. Default is 10.
High Temperature (°C)	The threshold for generating a TES High Temp event in degrees Celsius. Can be between 0 and 50. Default is 30.

Field	Description
Enable Temperature Monitoring	If ticked, the device monitors for low and high temperature detection and initiates events as specified by the feature; if unticked, no temperature monitoring takes place. Note that whenever a device is powered on, monitoring is automatically disabled for a time period, typically 90 minutes, to allow for the regularisation of any extremes of temperature during transportation. Default is unticked.

7.2.12 Device Settings window – Home Or Away Button menu option

You use the **Home Or Away** menu option to specify the function of the yellow **Home/Away** button. Typically, this button is used to switch the unit between Home and Away mode. If you define the button for this use, the remainder of the fields configure the device's actions while in Away mode.



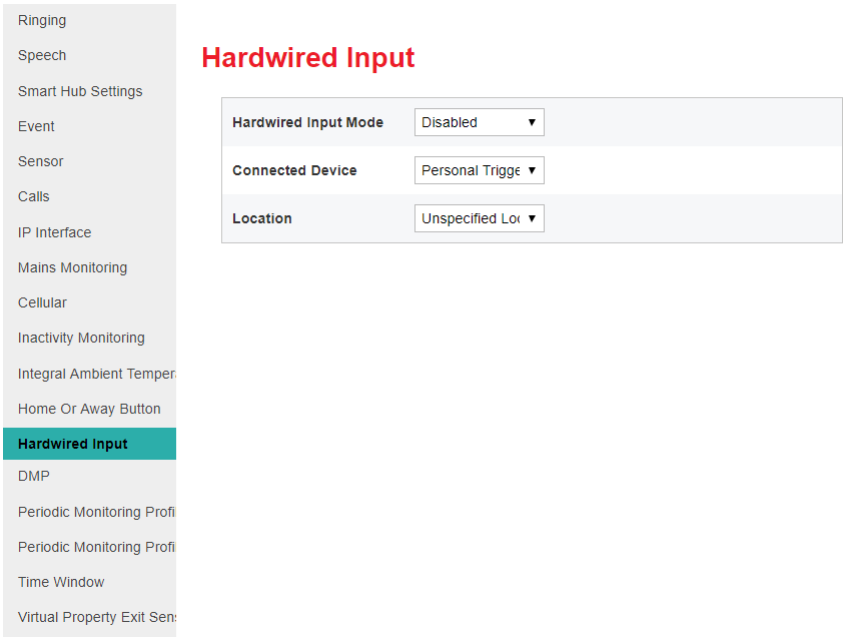
With this menu option, the main panel contains the following fields:

Field	Description
Button Function	Defines the function of the yellow **Home/Away** button on the Smart Hub. Can be one of: • Home Or Away – Pressing the button switches the device between Home and Away modes. The device suspends any inactivity monitoring when in the Away mode and re-starts on return to Home state, as described in Section 7.2.10, Device Settings window – Inactivity Monitoring menu option. If the device is in Away mode, pressing the green **Cancel** or red **Alarm** button will return the device into Home mode in addition to cancelling/raising an alarm. • Fast Dial – Not currently used • Disable – Pressing the button has no effect. Default is “Home Or Away”.
Delay Before State Change	Time delay in seconds from pressing the button to the device switching its mode. Can be between 0 and 99. Default is 15.
Away State Reminder	If ticked and an activity-related event occurs whilst the unit is in Away mode, the device issues regular reminders to inform the user that the device is in Away mode. These reminders take the form of an ascending tone sequence followed by the announcement "Activity detected, please press the yellow button to return to home mode". The interval for the reminder starts after 30 minutes on mains power, and 1 hour when using batteries. If ticked and no activity-related event occurs whilst the unit is in Away mode, then no reminders are made relating to the state of the device. If unticked, then no reminders are made relating to the state of the device regardless of whether activity is detected. Default is unticked.

7.2.13 Device Settings window – Hardwired Input menu option

Some sensors/triggers may need to be hardwired for them to be able to interface with the Smart Hub, for example, a sip-blow tube. You use the **Hardwired Input** menu to set up such sensors/triggers, indicating the type of sensor and location and the input mode.

If the device detects input from the sensor/trigger, a Hardwired Input event occurs which the device handles as defined by the event's attributes. Refer to Section 7.2.4, Device Settings window – Event menu option, for details on setting up these attributes.

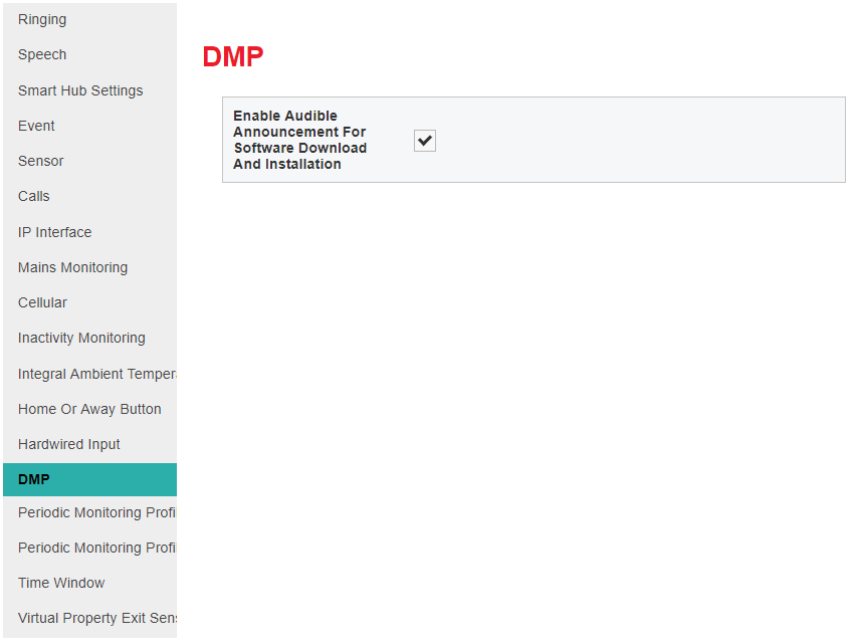


With this menu option, the main panel contains the following fields:

Field	Description
Hardwired Input Mode	Indicates the contact when the connected device is activated and needs to report to the device. Can be one of: • Disabled – the device ignores any signal from the device and does not raise an event • Normally Open – activated when a contact closes • Normally Closed – activated when a contact opens. Default is "Disabled".
Connected Device	The type of sensor/trigger. Default is "Personal Trigger".
Location	The location of the sensor/trigger. Default is "Unspecified Location 01".

7.2.14 Device Settings window – DMP option

You use the **DMP** menu option to indicate whether the unit is to make or suppress announcements whilst receiving and installing firmware and configuration settings from DMP. Suppressing announcements avoids disturbing the client.



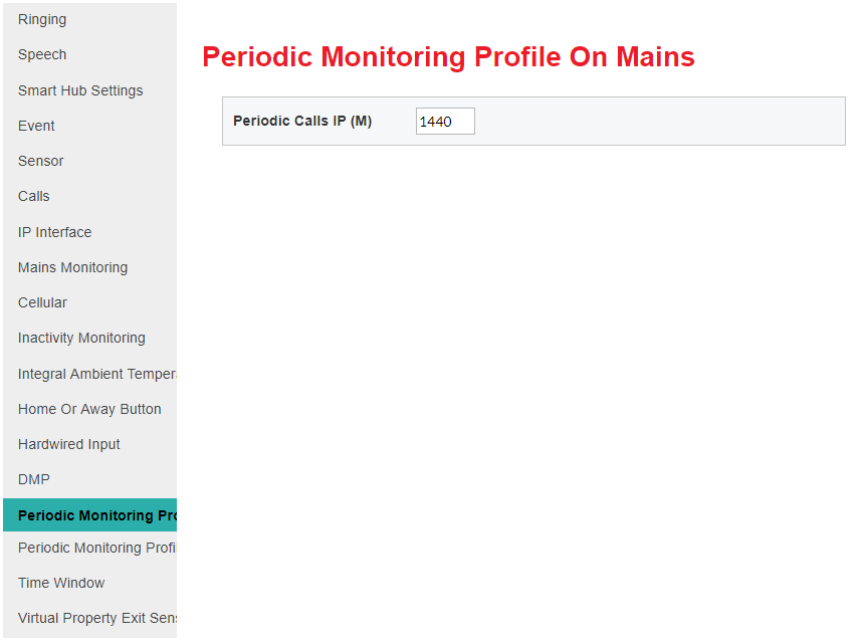
With this menu option, the main panel contains the following fields:

Field	Description
Enable Audible Announcement For Software Download And Installation	Indicates whether the unit is to make or suppress announcements whilst receiving and installing firmware and configuration settings from DMP. It should be ticked during installation so that the success of any updates that occur during the installation process can be confirmed. Default is ticked.

7.2.15 Device Settings window – Periodic Monitoring Profile On Mains menu option

You use the **Periodic Monitoring Profile On Mains** menu to set the frequency of the automated periodic test calls to the monitoring centre when the device is on mains power. These calls require the Periodic Call (IP) event to be correctly configured for it to have an appropriate call sequence index. This index should define IP channels only, so confirming that the monitoring centre can receive IP alarm calls raised by the device. For details of event configuration refer to Section 7.2.4, Device Settings window – Event menu option. For details of call sequence index configuration, refer to Section 7.2.6, Device Settings window – Calls menu option.

Note: The monitoring centre must be correctly configured to handle the periodic IP test calls. If a call fails to arrive, this indicates a possible Smart Hub or communications network failure which should be reported by the monitoring centre.



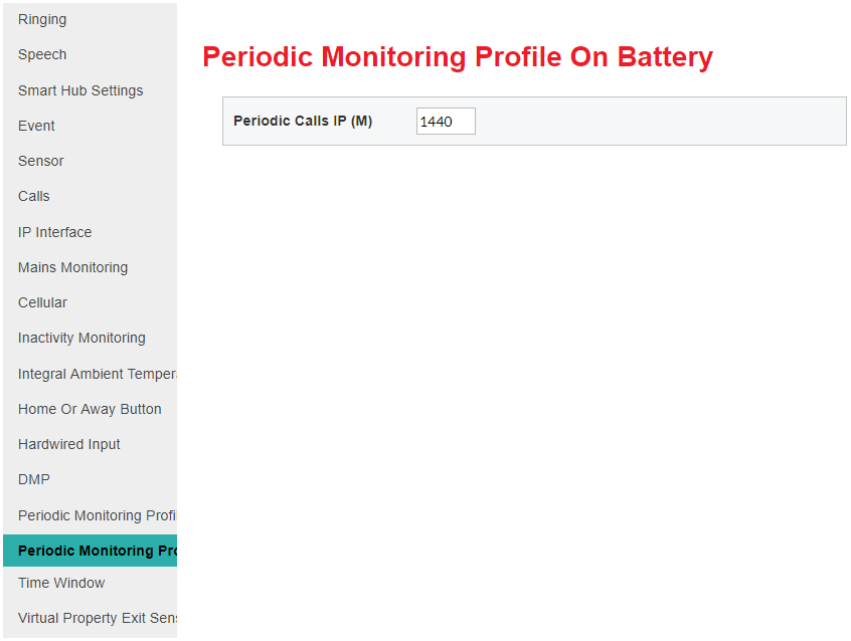
With this menu option, the main panel contains the following fields:

Field	Description
Periodic Calls IP (M)	The number of minutes between each automated periodic test call whilst the Smart Hub is mains powered. Can be between 1 and 1440. These calls should check connectivity with the monitoring centre using IP protocols only. Changing the value of this field affects the amount of data the device uses, and may incur additional charges. It is recommended that a change takes place only after discussion with your supplier. Default is 1440 minutes which equates to 24 hours.

7.2.16 Device Settings window – Periodic Monitoring Profile On Battery menu option

You use the **Periodic Monitoring Profile On Battery** menu to set the frequency of the automated periodic test calls to the monitoring centre when the device is on battery power. These calls require the Periodic Call (IP) event to be correctly configured, for it to have an appropriate call sequence index. This index should define IP channels only, so confirming that the monitoring centre can receive IP alarm calls raised by the device. For details of event configuration refer to Section 7.2.4, Device Settings window – Event menu option. For details of call sequence index configuration, refer to Section 7.2.6, Device Settings window – Calls menu option.

Note: The monitoring centre must be correctly configured to handle the IP periodic test calls. If a call fails to arrive, this indicates a possible Smart Hub or communications network failure which should be reported by the monitoring centre.



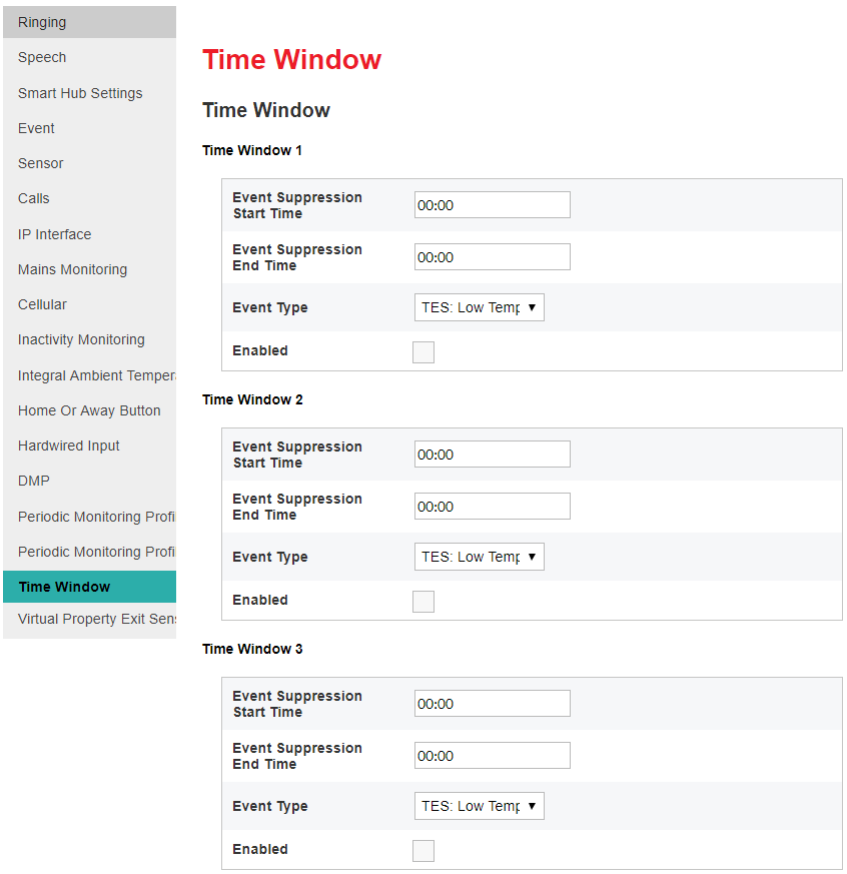
With this menu option, the main panel contains the following fields:

Field	Description
Periodic Calls IP (M)	The number of minutes between each automated periodic test call whilst the Smart Hub is powered by its batteries. Can be between 1 and 1440. These calls should check connectivity with the monitoring centre using IP protocols only. Changing the value of this field affects the amount of data the device uses, and may incur additional charges. It is recommended that a change takes place only after discussion with your supplier. Default is 1440 minutes which equates to 24 hours.

7.2.17 Device Settings window – Time Window menu option

You use the **Time Window** menu to block a type of event that occurs within a specific time window so that alarms relating to the event are not raised during that period. The types of event that can be blocked are:

- TES Low Temp
- Door Usage Opening
- Door Usage Closing
- Pressure Mat Activation
- Enuresis Activation.



You can specify up to 10 time windows for varying events. The following fields are used to define each time window:

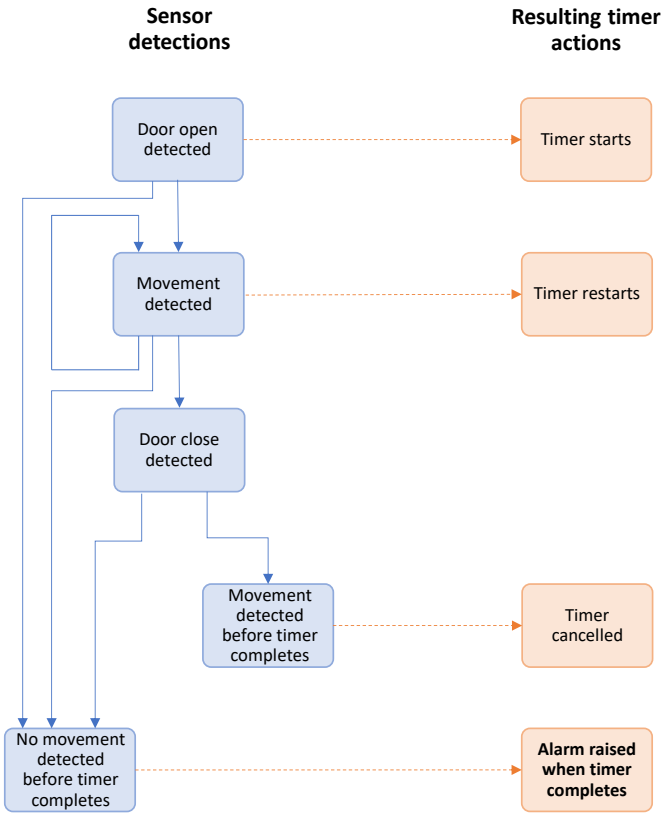
Field	Description
Event Suppression Start Time	The time that event blocking is to start for the day of the week specified in the set of fields heading. Default is 00:00.
Event Suppression End Time	The time that event blocking is to end. If the data in this field is less than that which is in the **Event Suppression Start Time** field, then the time refers to the following day. For example, if you have 23:00 to 7:00 in the start and end fields then blocking starts late evening, ending at 7:00am the following morning. Default is 00:00.
Event Type	The type of event to be blocked. Default is “TES: Low Temperature”.
Enabled	If ticked, the device blocks the specified event if it occurs during the specified time period, so that no alarm is raised; if unticked or outside the specified time period, then an alarm is raised when the event occurs. Default is unticked.

7.2.18 Device Settings window – Virtual Property Exit Sensor menu option

You use the **Virtual Property Exit Sensor** menu to configure the virtual property exit sensor so that it correctly triggers the Smart Hub to take appropriate action, including raising an alarm to the monitoring centre. The virtual property exit sensor can be configured to come into effect for different time periods, depending on the day of the week.

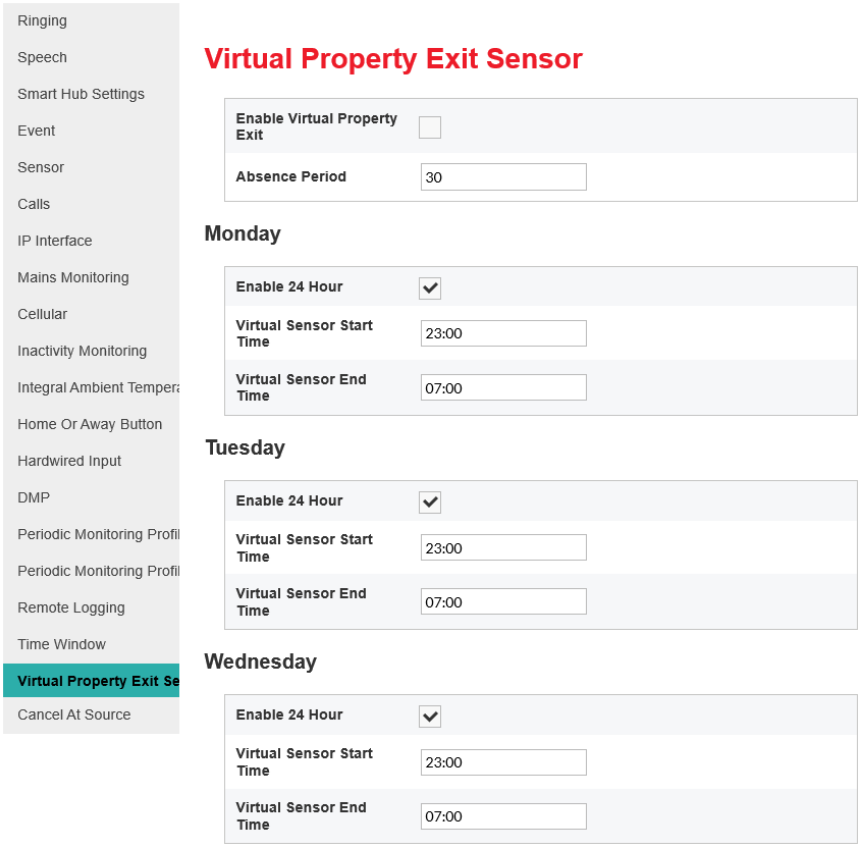
The virtual property exit sensor determines absence from the residence by detecting the opening of a door followed by no movement activity. To do this, it monitors input from one or more door contacts and associated PIR (Passive Infra-Red) movement sensors; this use being defined as part of the each sensor's configuration, described in Section 7.2.5, Device Settings window – Sensor menu option.

If, after the door has opened, there is no movement activity for a specified absence period, then the unit raises an alarm to the monitoring centre. The following diagram shows the interaction between the sensors and the timer that is used to measure the absence period:



If the sensor is to come into effect for specific time periods only, then only absence during the monitoring period contributes to the absence period. For example, suppose the absence period is 30 minutes and the monitoring period is between 23:00 and 7:00 overnight, then:

- If a unit detects the door opening after 6:30, no alarm will be raised regardless of whether the door is left open or closed, as the absence period ends after the monitoring period.
- If a unit detects the door opening in the 30 minutes before 23:00, no alarm will be raised because the client has left the property before the start of the monitoring period. However, an alarm will be raised at 23:30 if the door is open, as the property is insecure during the monitoring period.



Field	Description
Enable Virtual Property Exit	If ticked, the virtual property exit sensor monitors absence from the property. Monitoring occurs during the time periods specified in the other panels of this window. If unticked, no monitoring takes place and the device ignores the settings in the other panels. Default is unticked.
Absence Period	The time period in minutes that the Smart Hub is to monitor, on detection of a door opening, for activity detected by the appropriate PIR sensor(s). If, at the end of the time period, no activity has been reported by the PIR sensor(s), then the unit raises an alarm. Default is 30.
For each day of the week:	
Enable 24 Hour Monitoring	If ticked, monitoring takes place throughout the day and the Smart Hub ignores the **Start Time** and **End Time** field values.
Start Time	The time that monitoring is to start for the day of the week specified in the set of fields heading. Default is 00:00.

Field	Description
End Time	The time that monitoring is to end. If the data in this field is less than that which is in the **Start Time** field, then the time refers to the following day. For example, if you have 23:00 to 7:00 in the start and end fields for Monday then monitoring starts late Monday evening, ending at 7:00am on Tuesday. Default is 00:00.

7.2.19 Device Settings window – Cancel At Source menu option

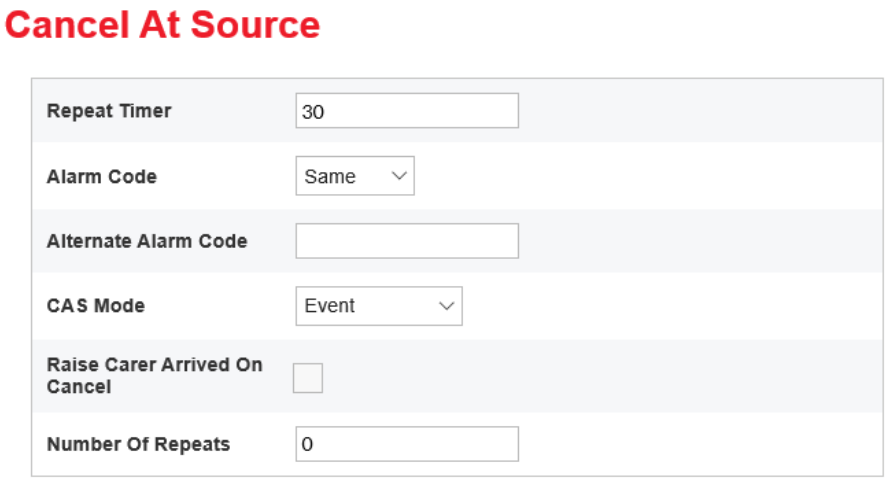
Cancel At Source is a feature where an alarm is repeated until cancellation is made physically at the Smart Hub. This can be used to ensure high dependency clients are visited by a carer, prior to an alarm being fully closed.

Alarms are raised to the monitoring centre and the calls cleared by the operator in the usual manner. If the configured alarm is not cancelled locally at the Smart Hub, then repeat calls to the monitoring centre will automatically be made.

Whilst an alarm is pending local cancellation, the yellow **Home/Away** button surround will flash slowly. Upon arrival, a carer then presses the green **Cancel** button to fully cancel the alarm. This stops any more repeat calls.

Note: Limitations: To avoid undesirable results, it is recommended that Cancel At Source mode is only used with radio trigger, red Help button, inactivity, virtual property exit sensor and hardwired input events. It should not be used for 'technical' alarms, such as those reporting sensor low batteries, auto presence or mains power failures.

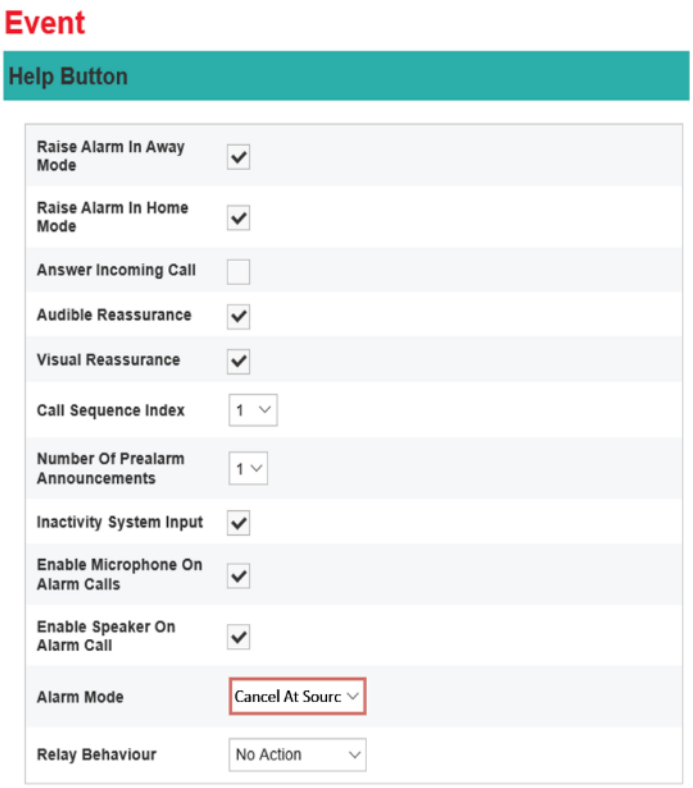
The Cancel At Source menu is displayed within DMP as follows:



Field	Description
Repeat Timer	The interval, in minutes, between alarm repeats. This should be set in accordance with local policy. Default is 30.
Alarm Code	Defines if the repeat alarm will be the same or an alternative to the cause of the initial cancel at source trigger. If 'Alternative' is selected a code must be entered in the 'Alternate Alarm Code' box. Default is: Same.
Alternate Alarm Code	Enter the alternative TT21 alarm code that will be generated instead of the source alarm.

Field	Description
CAS Mode	Defines which type of alarms require a cancel at source: • None, CAS is not required. • Non-technical, only non-technical alarms will require a CAS event. • Event, only event related alarms will require a CAS. • All, all alarm types will require a CAS. The different CAS modes should be selected in relation to the dependency of the end user and their requirements.
Raise Carer Arrived On Cancel	If ticked, a 'Carer Arrived' event will be generated upon the alarm being cancelled at the Smart Hub unit, confirming the cancellation. If enabled both the "Carer Arrived" and "Carer non arrival" events will need to be configured from the **Event** Device Settings menu. Default is unticked.
Number of Repeats	The maximum number of repeat calls which can be made for each alarm. Default is 0, indicating that there is no limit to the number of repeat calls.

For the types of alarm that should be handled with a Cancel At Source response, each type should be selected in the **Event** menu and the **Alarm Mode** entry set to 'Cancel At Source':



Where a sensor that has been configured for a Cancel At Source response is triggered, and repeat alarms fall during a blocking period, the time window settings (detailed in section 7.2.17) will take precedence over the Cancel At Source settings and alarm repeats will be paused until the blocking period has elapsed.

8 Working with firmware and campaigns

8.1 Introduction

Firmware is the software embedded in the Smart Hub units. Firmware controls how the unit behaves. Tunstall recommends that you update the firmware on your Smart Hub unit whenever new firmware becomes available. New firmware typically contains enhancements, new features and protection from new security threats.

Whenever new firmware is available for your Smart Hub unit, DMP sends out a system message in the form of an email, notifying relevant users of the availability of the new firmware. DMP also displays a message on the start page when a user first logs into DMP.

On notification of a firmware update, you can apply the update to a group of Smart Hub units; the definition of when and how the firmware is to be deployed is called a 'campaign'. For details on how to create a campaign for a group of units, refer to Section 6.5, Start Campaign window.

Campaigns start at a specific time and date. When that time/date is reached, DMP uploads the firmware either in batches or across all units.

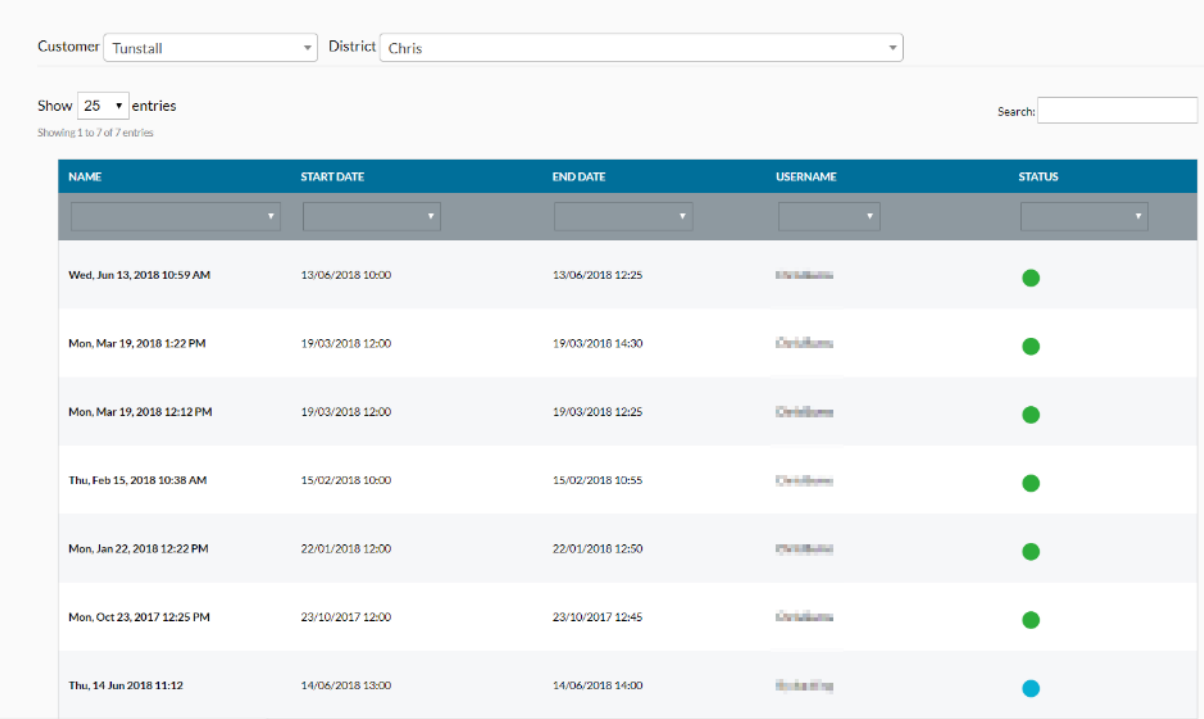
For each unit, DMP waits until the unit sends a heartbeat. It then downloads the firmware for the unit to install. Whilst the download and installation is taking place, the unit has a technical status, indicated by the colour blue. On successful installation of the firmware, the status changes to 'OK', indicated by green.

With batch uploads, DMP waits until all the units in the batch have successfully downloaded/installed the firmware before moving on to the units in the next batch.

Note: Attempting to upgrade a device more frequently than once every two hours may result in the later attempts failing until the Smart Hub completes the background tasks associated with firmware memory management.

8.2 Campaigns List page

You use this page to view the details of all the campaigns associated with the districts to which you have access, that is, those campaigns that upgrade the devices within your districts.



You access this page by clicking the **Campaigns** option on the main menu. This option is only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile.

The page initially lists the campaigns alphabetically ascending by their name. If you have 'Customer Basic' permission profiles for more than one customer or district, then you initially see those campaigns relating to the customer/district combination that appears first on your Start page.

The current status of the campaign is indicated by its status icon as follows:

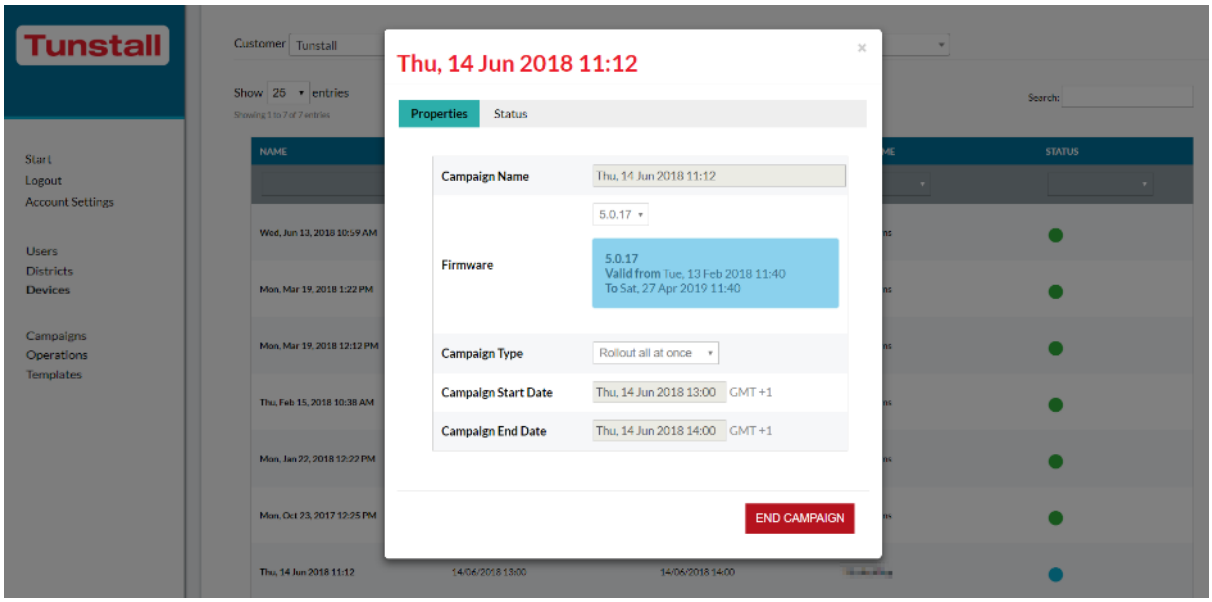
Campaign status icon	Description
	The campaign is complete and has successfully updated the firmware of the required units.
	The campaign is either waiting for its start date/time or is currently rolling out the firmware update.
	The campaign is complete but did not successfully update the firmware of all the required units, therefore warnings have been raised. This may be due, for example, to network communication problems. In this case, create a new campaign relating to the firmware and add any unit that failed to upgrade.

Within this page you can:

- use the standard table actions to filter, sort and search through the list
- initiate the display of a campaign's details, including its properties and the progress of the campaign, by clicking anywhere within its details. DMP opens a Campaign Information window containing the details of the selected campaign. This is only available if you have a 'Customer Advanced' permission profile.

8.3 Campaign Information window

You use this window to view the information relating to a campaign, including both its properties and its progress. In addition, you can end a campaign which has not started yet or is currently running.



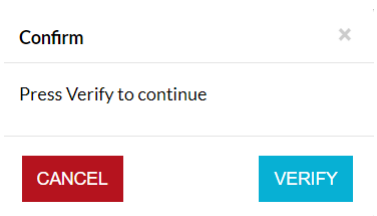
You access this window by:

- Clicking the **Campaigns** option on the main menu – only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile
- Selecting the appropriate customer, if you can access districts for more than one customer
- Selecting the appropriate district, if you can access more than one district
- Clicking within the row containing the relevant campaign menu – only available to users with at least one 'Customer Advanced' permission profile.

The window comprises two tabs which are described in the sub-sections below.

To end a campaign:

1. Click **END CAMPAIGN**. DMP displays the following confirmation message:



2. Click **VERIFY**.

   DMP ends the campaign, updating its **End Date** field with a timestamp of the time you ended the campaign.

8.3.1 Properties tab

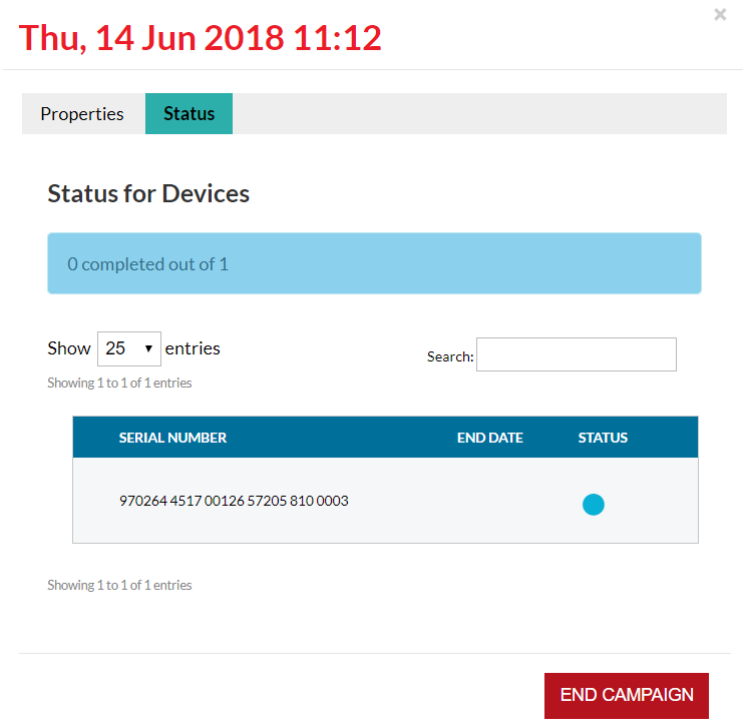
You use the **Properties** tab to specify the general details of the campaign.

The tab contains the following fields:

Field	Description
Campaign Name	The name of the campaign. Typically, this includes a timestamp of when the campaign was created.
Firmware	The version of firmware that DMP is to download to the devices.
Campaign type	Describes how the downloads are to be managed. Can be one of: • Rollout at once DMP makes the firmware available simultaneously to all selected devices when the **Campaign Start Date** is reached. They then download the firmware following their next successful heartbeat. • Start with 10 DMP makes the firmware available to batches of 10 devices at a time; the download of a new batch starting when the download for all 10 devices of the previous batch completes. In each case, downloading continues until either all selected devices have received the firmware, or the **Campaign End Date** is reached, whichever is earlier.
Campaign Start Date	The date and time the process of updating the device firmware is to start. The offset of this time from Greenwich Mean Time (GMT) is shown next to the field in grey.
Campaign End Date	The date and time the process of updating the device firmware is to end. The offset of this time from GMT is shown next to the field in grey. If the firmware download to a device starts and the campaign ends before the installation of that firmware completes, the device continues with the upgrade. If the download of firmware to a device has not started when the campaign ends, no downloading takes place with the firmware remaining unchanged until another campaign upgrades it.

8.3.2 Status tab

You use the **Status** tab to view the progress of the campaign.



The **Status** tab lists each of the devices that are to be upgraded by the campaign. Their status is shown by a status icon, as follows:

Device status icon	Description
	Upgrade of the unit has been successful.
	Unit is waiting to be upgraded or the firmware download is in progress.
	DMP was unable to update the device. You should correct any errors and add the device to a new firmware campaign at the earliest opportunity.

9 Working with templates

9.1 Introduction

Templates allow users to apply consistent configuration settings across multiple devices. They define a set of configuration attributes and the corresponding values to be applied to the devices. The only settings that you cannot include in a template are those relating to sensors/triggers.

Typically, you use templates to pre-configure devices prior to their installation. Use of templates has two benefits:

- Configuration of devices takes less time than manually configuring them, and,
- They are subject to less 'human error' during the configuration process.

Templates are created and held at customer level. You cannot migrate them across customers. You can only create a template if you have a 'Customer Advanced' permission level for at least one of the customer's districts; these are 'personal' templates.

In addition, your supplier may provide you with one or more templates for use with your customer. These are known as 'public' templates.

If you have 'Customer Basic' permission levels only then you see the list of 'public' templates when you select the **Templates** menu option on the Start page. If you have a 'Customer Advanced' permission level, then you see a list containing 'public' templates plus any 'personal' templates you created. You can edit, delete or view the details of 'personal' templates.

As part of the creation process, you assign the template to one or more districts. Alternatively, you can assign them when creating or editing a district, as described in Section 4.3.4, Templates tab.

Then, whenever a user migrates a device to one of those districts, they can specify the template to be applied to the device on migration, as described in Section 6.4, Migrate Devices window.

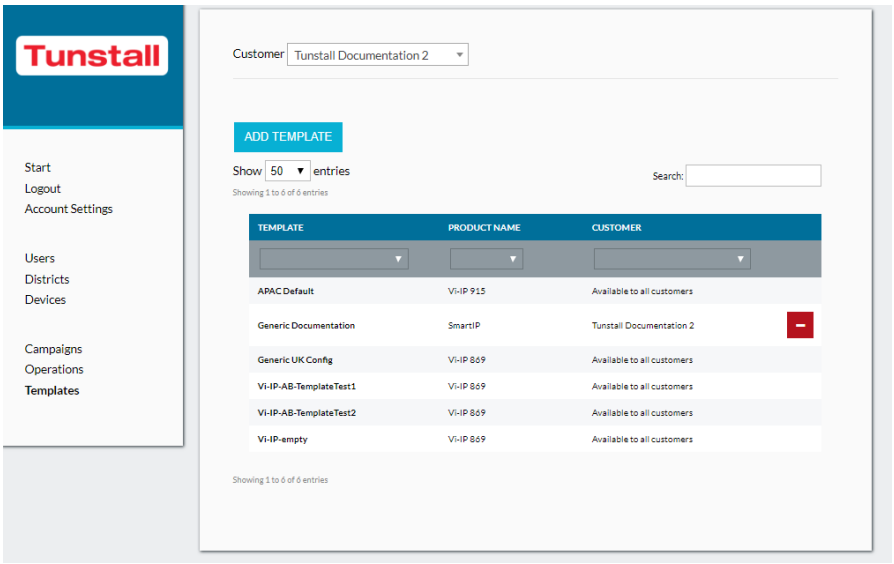
Applying template settings to the unit is the same process as applying manual setting changes to the unit. DMP waits until the device sends a heartbeat. It then downloads the template settings for the device to install. Whilst the download and installation are taking place, the device has a technical status, indicated by the colour blue. On successful installation of the template's settings, the status changes to 'OK', indicated by green.

Whilst changes to a device's settings are outstanding, DMP locks the device so that you cannot specify any further changes. If the Smart Hub is to hand, you can reduce the time the device is locked by pressing the device's green **Cancel** button, so prompting a DMP connection and initiating the download.

9.2 View Templates List page

If you have a 'Customer Basic' permission profile for one or more districts but no 'Customer Advanced' permission profiles, you use this page to view templates belonging to the customers associated with those districts.

If you have at least one 'Customer Advanced' permission profile, use this page to view all the templates belonging to any of your customers and to maintain 'personal' templates.



You access this page by clicking the **Templates** option on the main menu. This option is only available to users with at least one 'Customer Basic' or 'Customer Advanced' permission profile.

The page initially lists the templates in ascending order by their name. If you have 'Customer Basic' or 'Customer Advanced' permission profiles associated with more than one customer, then you initially see templates belonging to the customer that appears first on your Start page.

For 'Customer Advanced' users, the list includes both 'public' templates, that is, those created by your supplier and 'personal' templates, that is, those created by yourself. For 'Customer Basic' users, the list includes only 'public' templates. You cannot view, edit or delete public templates.

Tip: You can identify 'personal' templates by the − button at the end of their details.

Within this page you can:

- use the standard table actions to filter, sort and search through the list.

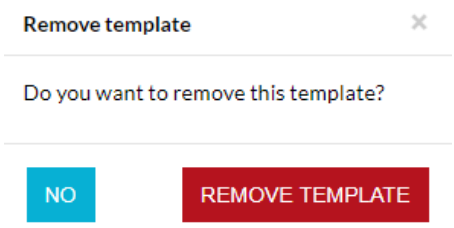
In addition, if you have a 'Customer Advanced' permission profile, you can:

- initiate the creation of a new personal template by clicking **ADD TEMPLATE**. DMP opens an Add New Template window for you to specify the template. On creation of the new template, DMP allocates it to the customer to which the templates currently displayed belong.
- initiate the display/edit of a personal template by clicking anywhere within its details. DMP opens an Edit Template window containing the details of the selected template.
- delete a personal template.

9.2.1 Delete a personal template

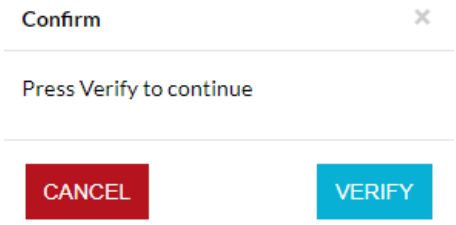
To delete a personal template:

1. Use the standard table actions to display the required template.
2. Click the − button next to the template details. DMP displays the following confirmation message:



3. Click **REMOVE TEMPLATE**.

   DMP displays the following message:



4. Click **VERIFY**.

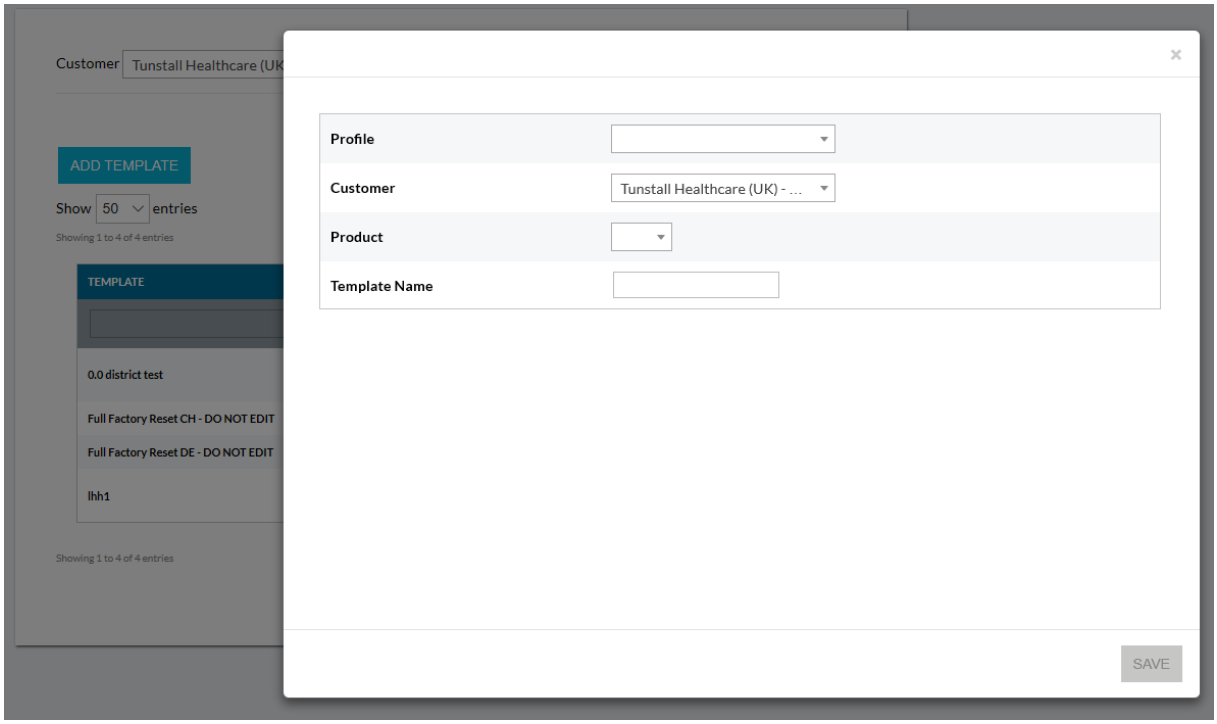
   DMP deletes the selected template.

9.3 Add New Template window

You use this window to create a new template including:

- general details, such as the customer to which it belongs, its name and the type of associated units and sensor.
- the districts that can apply the template
- the unit settings to be updated and their new values.

To access this window, you must have at least one 'Customer Advanced' permission profile.

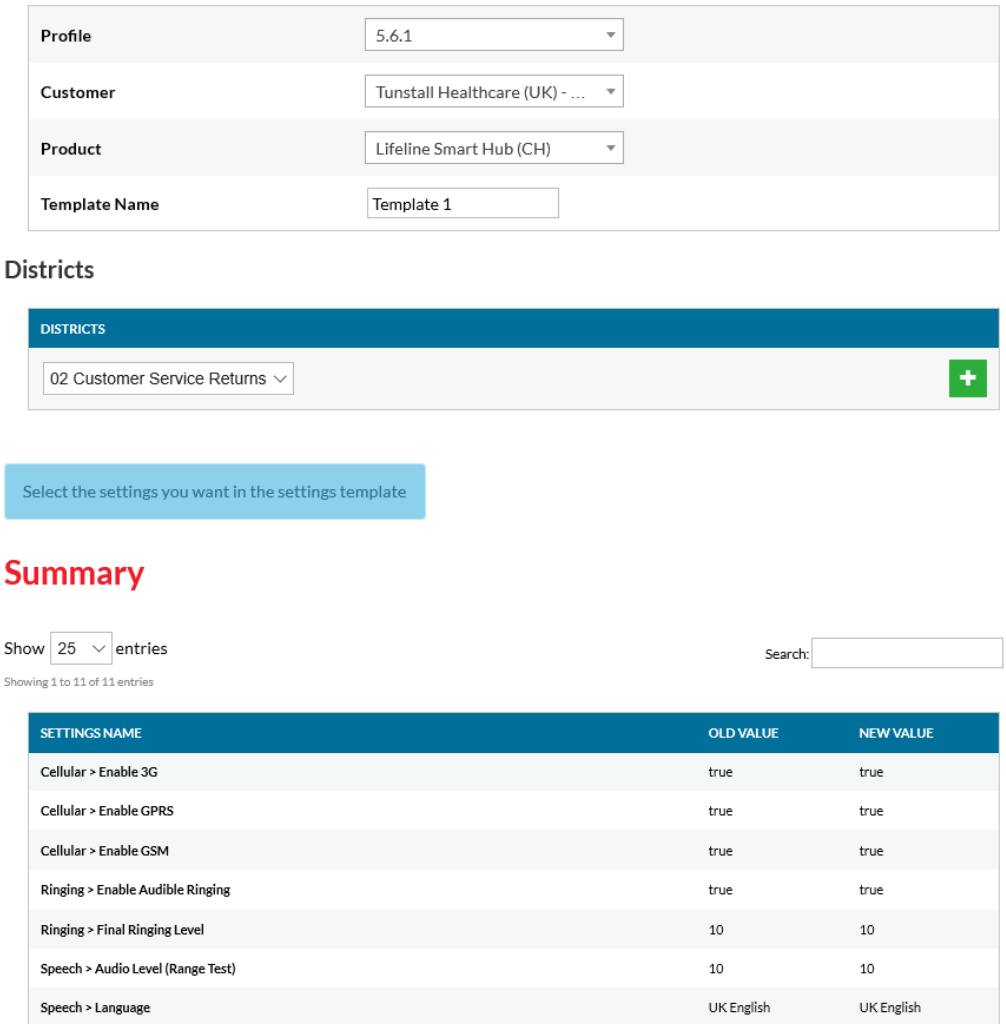


You access this window by:

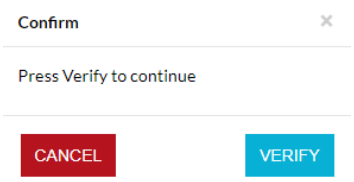
- Clicking the **Templates** option on the main menu
- Selecting the appropriate customer, if you maintain templates for more than one customer
- Clicking **ADD TEMPLATE** – only available to users with at least one 'Customer Advanced' permission profile.

To create a new template:

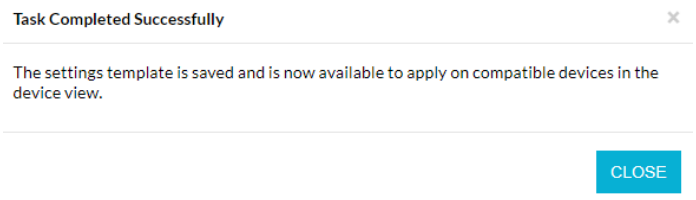
1. Specify the template's general properties, as detailed in Section 9.3.1, Specifying the template's general properties.
2. Define the districts that can apply the template, as detailed in Section 9.3.2, Defining the districts that can apply the template.
3. Define the values of the template settings, as detailed in Section 9.3.3, Defining the values of the template settings.
4. Click **SAVE AS TEMPLATE**. DMP displays a list containing a summary of the configuration changes the template makes.



5. If required, use the standard table actions to filter, sort and search through the list.
6. If the changes are complete and correct, click **SAVE**. DMP displays a confirmation message:



7. Click **VERIFY**. DMP displays an information message:



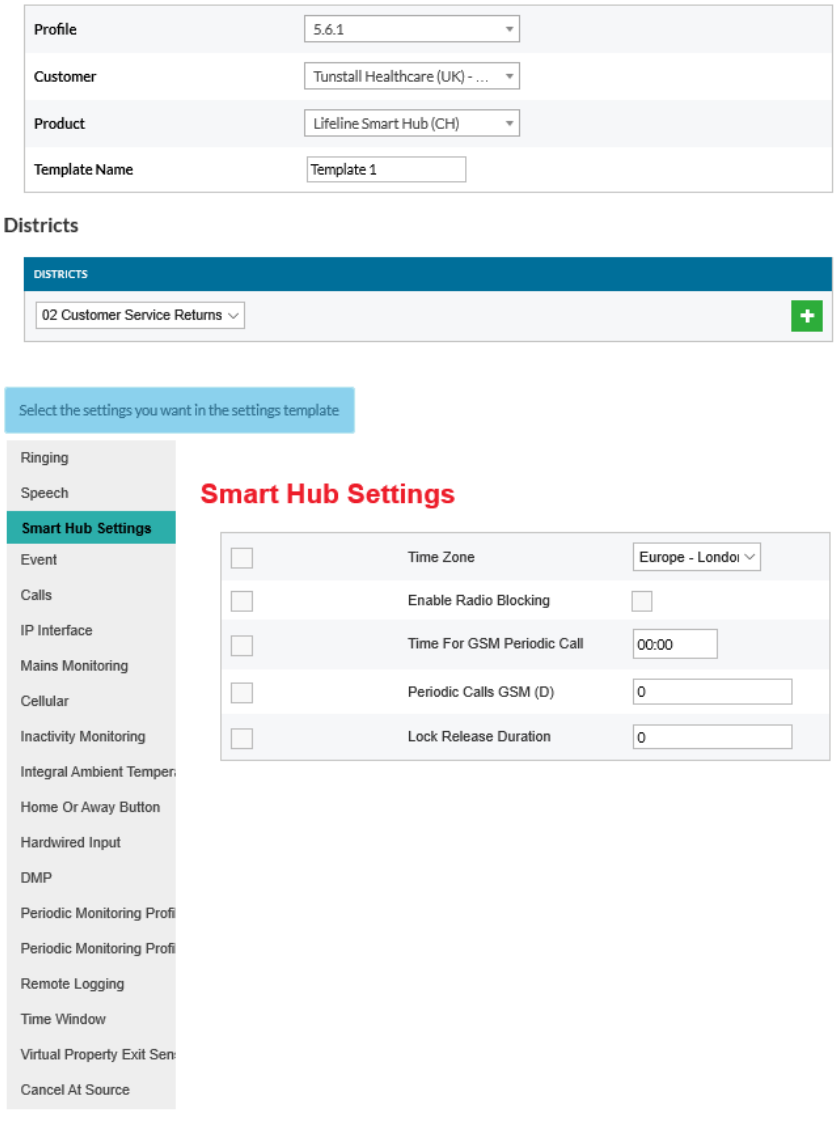
8. Click **CLOSE** to return to the View Templates List page.

9.3.1 Specifying the template's general properties

A template's general properties comprise:

Field	Description
Profile	Defines the schema version to which the template relates. This determines the set of attributes that the template may configure. The current schema version of a device is displayed on the **Device Settings** window.
Customer	Defines the customer to which the template belongs.
Product	The type of unit associated with the template. Typically, there are different products for different regions of the world. The unit type determines the set of devices to which the template can be applied.
Template Name	The name of the template. This must be unique within the set of templates belonging to a customer.

The DMP display includes the template's districts and configuration settings, as shown below:



9.3.2 Defining the districts that can apply the template

You define the set of districts that can apply the template as follows:

Add a district to the list

To add a district to the list:

1. Select the required district from the drop-down list.
2. Click the + button.

   DMP displays the district in a table above the drop-down list:

Remove a district from the list

To remove a district from the list, click the − button next to the district details.

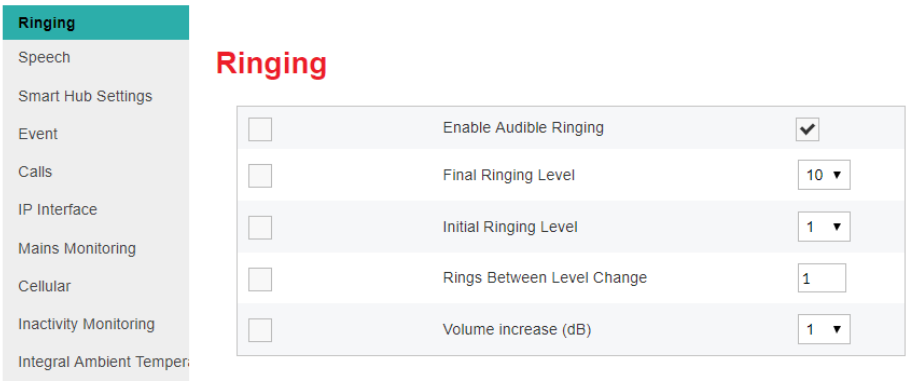
9.3.3 Defining the values of the template settings

The final section of the template window displays the settings. You use this section to define the settings to be updated by the template. To do this:

1. Select the required menu option from the menu on the left-hand side of the window. The list of options depends on the configuration schema and matches the set of options you see when configuring a device in this schema. The only exception is the Sensor option which is always omitted from the list. The Sensor option is not required as templates cannot update sensor/trigger details, including the unit's own radio pendant.

   On selection of a menu option, DMP displays the same attributes available when the same option is chosen to update a unit's settings.

   In addition, each attribute has a checkbox beside its label, as illustrated below:

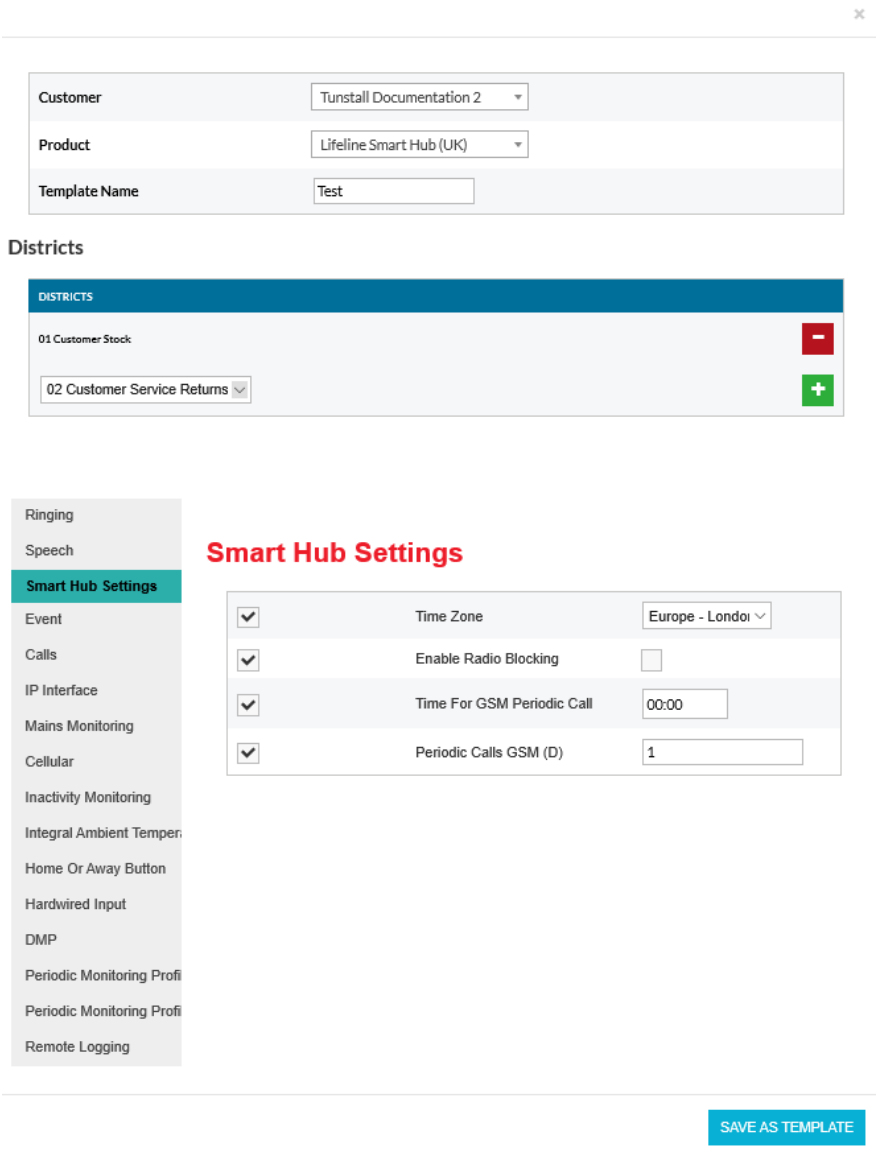


2. For each attribute you wish to update:
   a. Select the checkbox next to the attribute's label.
   b. Set the attribute to the required value. If you are unsure of its value, refer to the appropriate sub-section of Section 7.2, Device Settings window. The required field may not be described in the sub-section, depending on the contents of the configuration schema associated with the template.
3. Repeat steps 1 and 2 until all the required attribute values are defined.

9.4 Edit Template window

You use this window to view/edit a template's details including:

- general details, such as the customer to which it belongs, its name and the type of associated units
- the districts that can apply the template
- the unit settings to be updated and their new values.



You access this window by:

- Clicking the **Templates** option on the main menu
- Selecting the appropriate customer, if you maintain templates for more than one customer
- Clicking within the row containing the details of the template you wish to view or work on.

To access this window, you must have at least one 'Customer Advanced' permission profile.

The window comprises three sections which are described under Section 9.3, Add New Template window.

Within this window you can:

- view a template's details
- edit a template's details.

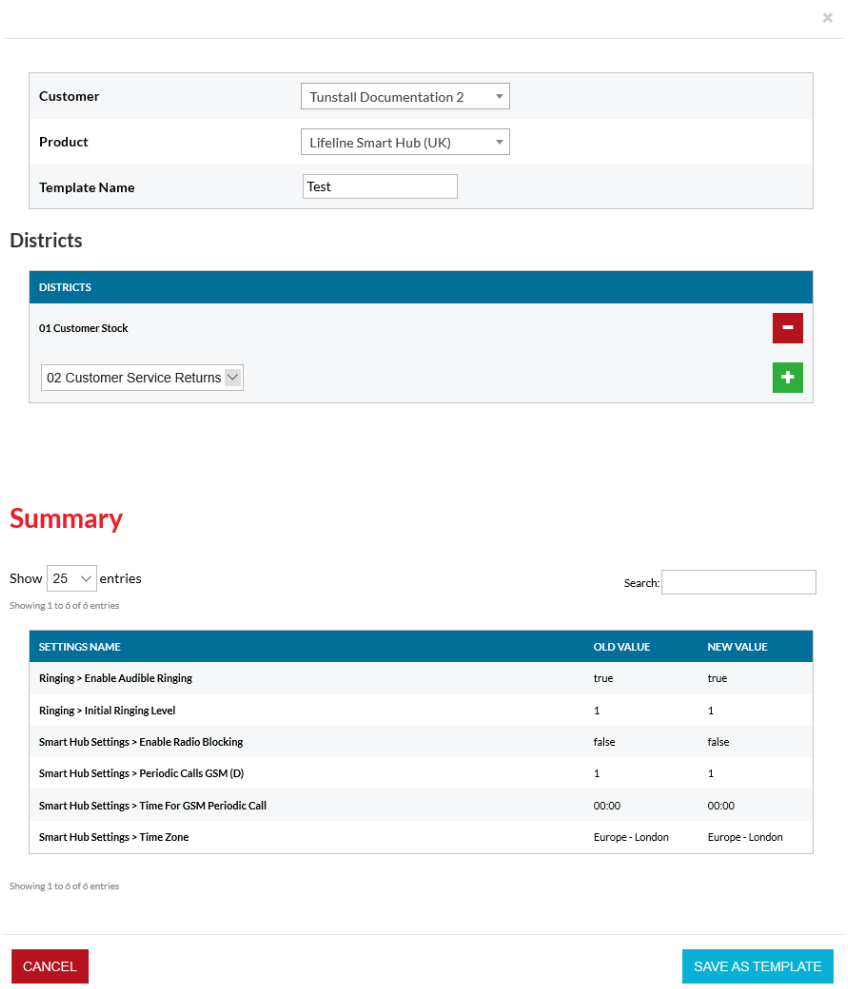
View a template's details

To view a template's details, select the menu options as required and then click **X** in the top-righthand corner of the window.

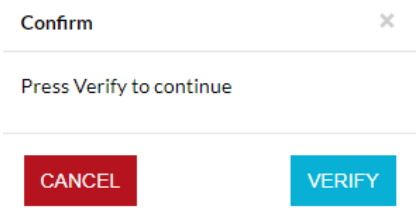
Edit a template

To edit a template:

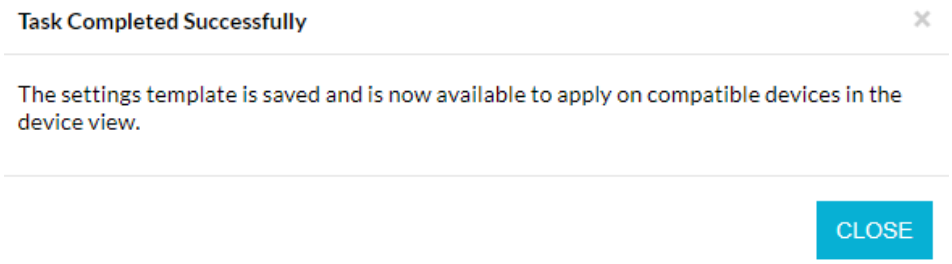
1. Make the relevant changes required, as described in Section 9.3, Add New Template window.
2. Click **SAVE AS TEMPLATE**. DMP displays a list containing a summary of the configuration changes the template makes.



3. If required, use the standard table actions to filter, sort and search through the list.
4. If the changes are complete and correct, click **SAVE AS TEMPLATE**. DMP displays a confirmation message:



5. Click **VERIFY**. DMP displays an information message:

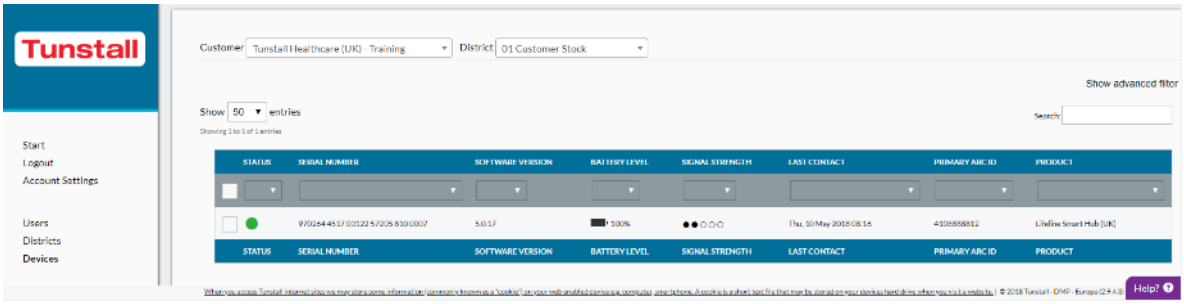


6. Click **CLOSE** to return to the View Templates List page.

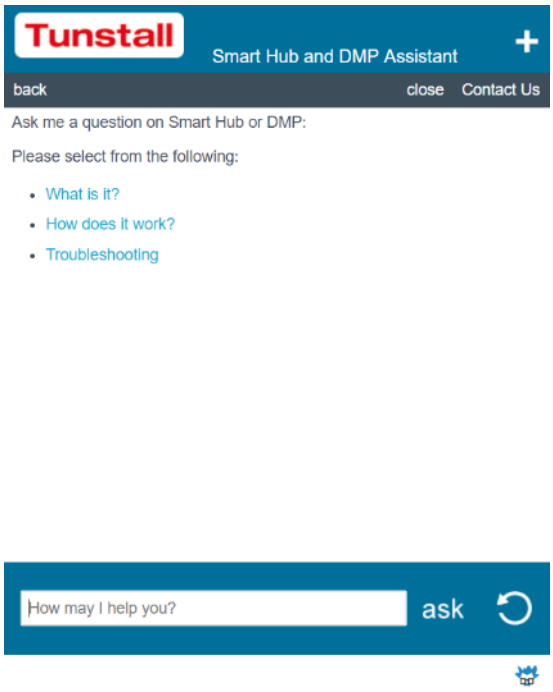
10 DMP online help

The online help within DMP is provided by the Smart Hub and DMP Assistant.

You access it by clicking the **Help?** Button that appears in the bottom right-hand corner of the DMP page:



DMP opens a new popup window:



You enter the question you wish to ask in the field at the bottom of the popup and click the **ask** button. Information relating to your question then appears in the main part of the popup. For example, if you ask, “How do I add a pendant?”, the online help displays step-by-step instructions on how to add a pendant.

Alternatively, you can select from the options shown in the main part of the popup.

If you need to review information you have already seen, click the **back** button on the menu bar at the top of the popup. If you wish to clear your help and restart your search, click the button. When you have finished using the online help, click the **close** button on the menu bar to shut down the popup.

A Permission profiles

DMP has three permission profiles, but users are given Customer Basic and Customer Advanced profiles, as a base profile does not give access to any device management information.

Menu Option/ Operation	Base Profile	Customer Basic	Customer Advanced
Start menu option	✓	✓	✓
Logout menu option	✓	✓	✓
Account Settings menu option	✓	✓	✓
View account settings and district permission profiles	✓	✓	✓
Edit name, language, email format and, if configured, email settings	✓	✓	✓
Change password	✓	✓	✓
Setup two-step verification		✓	✓
View two-step verification QR code		✓	✓
Users menu option			✓
Filter, sort and search through the list of user accounts			✓
Add a user with ‘Base Profile’ or ‘Customer Basic’ permission profiles			✓
View a user’s details			✓
Edit a user’s name, language and email format			✓
Add a district to a user account			✓
Change the permission profile of the user within a district – ‘Customer Basic’ or ‘Base Profile’			✓
Remove a district from a user account			✓
Unlock a user account			✓
Delete a user account			✓

Menu Option/ Operation	Base Profile	Customer Basic	Customer Advanced
Districts menu option			✓
Filter, sort and search through the list of districts			✓
Add a new district to a customer			✓
View a district's details			✓
Edit a district's name, details of the person responsible for the district language, time zone and device status details for each device held by the district			✓
Add a user account to a district			✓
Change the permission profile of a user within a district			✓
Remove a user account from a district			✓
View the recent history of communication between a district's devices and ARC			✓
Edit the warning status and limits of a district			✓
Add a template to the set of templates that may be applied to a device in the district			✓
Remove a template from the set of templates that may be applied to a device in the district			✓
Devices menu option		✓	✓
Filter, sort and search through the list of devices		✓	✓
View the status of a device over the last 24 hours		✓	✓
View all changes of status and heartbeats received from a device		✓	✓
View all events sent by the device to DMP		✓	✓
Migrate the device to a different district, including other customers' districts		✓	✓
Change the status of a device to 'Active' or 'Inactive'		✓	✓

Menu Option/ Operation	Base Profile	Customer Basic	Customer Advanced
Allow wrong credentials – not currently used		✓	✓
Enter/edit notes on the device		✓	✓
Change the configuration settings of a device		✓	✓
Upgrade the firmware of a device			✓
Apply a template to the device		✓	✓
Campaigns menu option		✓	✓
Filter, sort and search through the list of campaigns		✓	✓
View the details of a campaign			✓
End a campaign			✓
Operations menu option		✓	✓
Migrate a set of devices to a different district, including other customers' districts		✓	✓
Templates menu option		✓	✓
Filter, sort and search through the list of templates		✓	✓
Add a template			✓
View the details of a template			✓
Edit a template's general properties			✓
Edit the set of districts that can use a template			✓
Edit the configuration defined by a template			✓
Online help button		✓	✓
Online help queries		✓	✓

B Heartbeat icons and status

The heartbeat icon identifies the current status of a device as shown below:

Heartbeat	Description
	The device is functioning correctly and is sending heartbeats at the interval expected by the device's district, as described in Section 4.3.1, Properties tab. The property that defines the expected heartbeat interval is: • **Heartbeat interval (minutes).**
	The device sends heartbeats but has a technical status, for example: • there is a mains power failure, the battery charge is low or there is a battery error • the device is in the process of updating its firmware or settings. You get information about the cause of the technical status by hovering the cursor above the icon.
	The status of the device is unclear. Circumstances that set the heartbeat icon to this status include: • a temporary communication problem • low cellular signal level • the device is registered but not turned on, that is, before the device sends its first heartbeat • the device is connected incorrectly. DMP displays a yellow icon when no heartbeat is received for a time period defined by the device's district, as described in Section 4.3.1, Properties tab. The properties that control this change of status are: • **Warning interval (minutes)**, if the device is using mains power • **Warning (on power failure) interval (minutes)**, if the device is using battery power.
	This indicates there is an error requiring action, for example, the device is switched off or is out of touch with the outside world. DMP displays a red icon when no heartbeat is received for a time period defined by the device's district, as described in Section 4.3.1, Properties tab. The properties that control this change of status are: • **Error interval (minutes),** if the device is using mains power • **Error (on power failure) interval (minutes)**, if the device is using battery power.

Heartbeat	Description
	This indicates the device has been set to ‘Inactive’ within DMP, that is, has been temporarily taken out of service. For details, refer to Section 6.3.5, Preferences tab.

C List of supported radio peripherals

In addition to the supplied personal trigger, the Smart Hub supports a wide range of radio-controlled peripherals as listed below. Note that availability of peripherals may vary by country and permitted radio frequency.

The types of peripheral supported are:

- Bath Sensor
- Bed/Chair Occupancy Sensor
- Bed In/Out
- Bogus Caller Trigger
- Carbon Monoxide Detector
- Door Contact Open/Closed
- Door Guard
- Enuresis Sensor
- Epilepsy Sensor
- Fall Detector
- Flood Detector
- Medication Dispenser
- Natural Gas Detector
- Passive Infrared Movement (PIR)
- Personal Trigger
- Pressure Mat
- Property Exit Sensor
- Pull Cord
- Radio Output Module (ROM)
- Smoke Detector
- Temperature Extreme Sensor
- TX4 Pendant
- Universal Sensor.

D Default settings of event attributes

Note: This appendix lists the default factory settings for each event's attributes. Some of these settings may be changed due to local regulations and/or customer templates applied prior to installation.

Key:
✓ means true/enabled
Clear means false/disabled

Event Type	Raise Alarm In Away	Raise Alarm In Home	Answer Incoming Call	Audible Reassurance	Visual Reassurance	Call Sequence Index	No. of Pre-alarm Announcements	Inactivity System Input	Enable Microphone On Alarm	Enable Speaker On Alarm Call	Alarm Mode	Relay Behaviour
Help Button (Alarm)	✓	✓		✓	✓	1	1	✓	✓	✓	Standard	None
Cancel Button			✓			1	0	✓			Standard	None
Away Button				✓	✓	1	1	✓	✓	✓	Standard	None
Inactivity Alarm		✓		✓	✓	1	1		✓	✓	Standard	None
Periodic Call (IP)					✓	9	1				Standard	None
Periodic Call (GSM)	✓	✓			✓	10	1				Standard	None
Mains Power Fail	✓	✓			✓	1	1				Standard	None
Mains Power					✓	1	1				Standard	None
System Battery Low	✓	✓			✓	1	1				Standard	None
Stuck Key	✓	✓			✓	1	1				Standard	None
Unit Failure	✓	✓			✓	1	1				Standard	None
Battery Charged					✓	1	1				Standard	None
Away State Entry					✓	1	1				Standard	None
Home State Entry					✓	1	1				Standard	None
IP Module Fail					✓	1	1				Standard	None
IP Connectivity Fail					✓	1	1				Standard	None
IP Connectivity Restore					✓	1	1				Standard	None
Failed To Contact the ARC						1	1				Standard	None
Personal Trigger Activation	✓	✓	✓	✓	✓	1	1	✓	✓	✓	Standard	None
TES High Temperature	✓	✓		✓	✓	1	1		✓	✓	Standard	None
TES Low Temperature	✓	✓		✓	✓	1	1		✓	✓	Standard	None
TES Fault	✓	✓		✓	✓	1	1		✓	✓	Standard	None
TES Temperature Rise	✓	✓		✓	✓	1	0		✓	✓	Standard	None
Flood Detector Activation	✓	✓		✓	✓	1	1		✓	✓	Standard	None
CO Detector Activation	✓	✓		✓	✓	1	0		✓	✓	Standard	None

Event Type	Raise Alarm In Away	Raise Alarm In Home	Answer Incoming Call	Audible Reassurance	Visual Reassurance	Call Sequence Index	No. of Pre-alarm Announcements	Inactivity System Input	Enable Microphone On Alarm	Enable Speaker On Alarm Call	Alarm Mode	Relay Behaviour
CO Detector End Of Life	✓	✓		✓	✓	1	1		✓	✓	Standard	None
CO Detector Fault	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Smoke Detector Activation	✓	✓		✓	✓	1	0		✓	✓	Standard	None
Door Usage Opening				✓	✓	1	1	✓	✓	✓	Standard	None
Door Usage Closing				✓	✓	1	1	✓	✓	✓	Standard	None
Pressure Mat Activation				✓	✓	1	1	✓	✓	✓	Standard	None
Pullcord Activation	✓	✓		✓	✓	1	1	✓	✓	✓	Standard	None
Enuresis: Activation	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Bed or Chair Not In		✓		✓	✓	1	1		✓	✓	Standard	None
Bed or Chair Not Up		✓		✓	✓	1	1		✓	✓	Standard	None
Bed or Chair Absence	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Bed or Chair Other	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Fall Detector Button	✓	✓	✓	✓	✓	1	1	✓	✓	✓	Standard	None
Fall Detector Fall	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Fall Detector Not Worn		✓		✓	✓	1	1		✓	✓	Standard	None
Fall Detector Activation Cancelled	✓	✓				1	1				Standard	None
PIR EE Activation				✓	✓	1	1	✓	✓	✓	Standard	None
PIR Non EE Activation				✓	✓	1	1	✓	✓	✓	Standard	None
PIR Tamper				✓	✓	1	1		✓	✓	Standard	None
ROM1-4 Event 1-4	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Natural Gas Detector Activation	✓	✓		✓	✓	1	0		✓	✓	Standard	None
PES Door Left Open	✓	✓		✓	✓	1	1		✓	✓	Standard	None
PES Client Wandered	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Bogus Caller Activation	✓	✓			✓	1	1	✓	✓		Standard	None
Medication Dispenser Dose Missed		✓		✓	✓	1	1		✓	✓	Standard	None
Medication Dispenser Device Fault	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Medication Dispenser Dose Taken	✓	✓		✓	✓	1	1	✓	✓	✓	Standard	None
Bath High Level	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Bath High Temperature	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Bath Low Temperature	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Epilepsy Sensor Activation	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Epilepsy Sensor Other	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Auto Presence Failure	✓	✓			✓	1	1				Standard	None
Auto Presence Restore					✓	1	1				Standard	None

Event Type	Raise Alarm In Away	Raise Alarm In Home	Answer Incoming Call	Audible Reassurance	Visual Reassurance	Call Sequence Index	No. of Pre-alarm Announcements	Inactivity System Input	Enable Microphone On Alarm	Enable Speaker On Alarm Call	Alarm Mode	Relay Behaviour
Auto Low Battery	✓	✓			✓	1	1				Standard	None
Radio Blocking					✓	1	1				Standard	None
Radio System Fault						1	1				Standard	None
Hardwired Input	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Carer Arrived	✓	✓		✓	✓	1	1		✓	✓	Standard	None
Carer Non-Arrival	✓	✓		✓	✓	1	1		✓	✓	Standard	None

E Call sequence usage example

E.1 Scenario

- The organisation has a single monitoring centre.
- IP communications with the centre always use Tunstall's own IPACS protocol with GSM. There is no support for VoIP.
- Telephony communications with the centre always use the same telephone number.
- Some of the organisation's clients have their own fixed broadband service (ethernet) but some do not.
- The organisation's units are configured to make an IP periodic call once a day but no other periodic calls.
- The organisation wants all calls raised by events to be routed in a similar way. All calls, except IP periodic calls, include a telephony fall-back route.

E.2 Installation instructions

E.2.1 Instructions for clients with a fixed broadband service

Three destinations:

Name	Type	Phone No.	URL	Supported Protocol	Connection Type	Call Method
Destination 1	IP Call		■■■■■■■■	IPACS	Ethernet	GSM
Destination 2	IP Call		■■■■■■■■	IPACS	Cellular	GSM
Destination 3	Telephone Call	■■■■■■■■				

Two call sequences:

Name	Repeat	Record 1		Record 2		Record 3	
		Destination	No. of attempts	Destination	No. of attempts	Destination	No. of attempts
Call Sequence 1	Yes	1	3	2	3	3	3
Call Sequence 2	No	1	4	2	4		

Each of the alarm events is to be allocated call sequence index 1, while the IP periodic call event is to be allocated call sequence 2.

E.2.2 Instructions for clients without a fixed broadband service

Two destinations:

Name	Type	Phone No.	URL	Supported Protocol	Connection Type	Call Method
Destination 1	IP Call		■■■■■■■■	IPACS	Cellular	GSM
Destination 2	Telephone Call	■■■■■■■■				

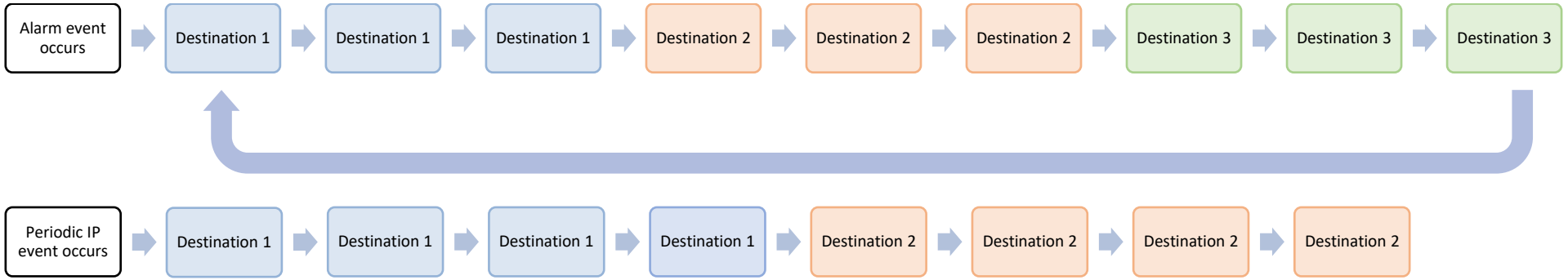
Two call sequences:

Name	Repeat	Record 1		Record 2	
		Destination	No. of attempts	Destination	No. of attempts
Call Sequence 1	Yes	1	3	2	3
Call Sequence 2	No	1	4		

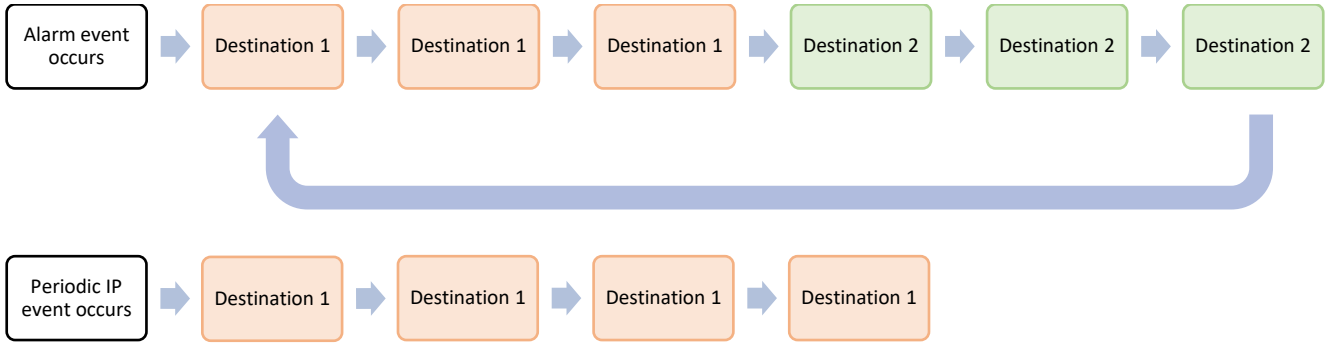
Each of the alarm events is to be allocated call sequence index 1, while the IP periodic call event is to be allocated call sequence 2.

E.3 Calls made by Smart Hub units

E.3.1 Located at clients with a fixed broadband service



E.3.2 Located at clients without a fixed broadband service



F Glossary

Term/Acronym	Description
APN	Access Point Name. The name of a gateway between a GSM, General Packet Radio Service, 3G or 4G mobile network and another computer network, frequently the public internet.
ARC	Alarm Receiving Centre. Also referred to as the monitoring centre or response centre.
BS8521	A British Standards Document that specified the Dual-Tone Multi-Frequency (DTMF) signalling protocol for social alarm systems.
CAT5	Category 5 cable. A twisted-pair cable for computer networks.
DC	Direct Current. A single direction flow of electrical charge.
DMP	Device Management Platform
DTMF	Dual-tone multi-frequency signalling. An in-band telecommunication signalling system using the voice-frequency band over telephone lines between telephone equipment and other communications devices and switching centres. Also known as tone dialling.
GPRS	General Packet Radio Service. A packet-oriented mobile data service on the 2G and 3G cellular communication systems' global system for mobile communications (GSM).
GSM	Global System for Mobile communications. A standard developed by the European Telecommunications Standards Institute (ETSI) to describe the protocols for digital cellular networks used by mobile devices.
Hrs	Hours
HTML	Hypertext Markup Language. The standard mark-up language for creating web pages and web applications. An option within DMP which provides a wider range of formatting options than text when creating emails, at a cost of increasing the email file size.
Hz	Hertz. A unit of frequency.
ICCID	Integrated Circuit Card Identifier. A unique serial number used to identify the SIM card.
ID	Identifier

Term/Acronym	Description
IMEI	International Mobile Equipment Identity. This is a number, usually unique, which is used to identify the device. Used by the GSM network to identify valid devices.
IMSI	International Mobile Subscriber Identity. Used to identify the subscriber of a cellular network and is a unique identification associated with all cellular networks. It comprises country and network code together with a subscriber identification number. An IMSI is usually presented as a 15 digit number.
IP	Internet Protocol. The communications protocol used for relaying packets across network boundaries. Its routing function enables internetworking, and essentially establishes the internet.
IPACS	Independent Protocol for Alarm Communication Systems. Tunstall's IP protocol.
LED	Light-emitting diode
MHz	Megahertz
PC Connect	Programming tool used by other Tunstall Lifeline products.
PIN	Personal Identification Number. A numeric or alpha-numeric password or code used in the process of authenticating or identifying a user to a system and a system to a user.
PIR	Passive Infrared sensor. An electronic sensor that measures infrared light radiating from objects in its field of view, used in PIR-based motion detectors.
PNC	Piper Network Controller. Tunstall's ARC product.
PRC	Product Code. The long number printed on the label on the base of the unit. This unique identity is used when communicating with DMP, for stock item identification, and it also allows full product traceability.
QR Code	Quick Response Code. A type of matrix barcode (or two-dimensional barcode) that consists of black squares arranged in a square grid on a white background, which can be read by an imaging device such as a camera. The required data is extracted from patterns that are present in both horizontal and vertical components of the image. Used in two-step verification access to DMP.
RF	Radio Frequency
RSSI	Received Signal Strength Indicator. A measurement of the power present in a received radio signal.

Term/Acronym	Description
SCAIP	Social Care Alarm Internet Protocol. An open IP protocol published by the Swedish Standards Institute. Used for handling multimedia communication streams and sending event messages between the Alarm Sender and the Alarm Receiver over an IP communication network such as the internet. The alarm protocol is defined as an XML schema including the alarm types, codes and additional information required to fulfil the requested functionality.
SIP	Session Initiation Protocol. A communications protocol for signalling and controlling multimedia communication sessions in applications of internet telephony for voice and video calls, in private IP telephone systems, as well as in instant messaging over IP networks.
SMS	Short Message Service. A text messaging service component of most telephone, World Wide Web, and mobile device systems.
STMF	Sequential-tone multi-frequency signalling. Tunstall's alternative to DTMF, designed to provide improved reliability when communicating over cellular and VoIP connections.
TES	Temperature Extremes Sensor
TT21	A Tunstall tone protocol using DTMF or STMF signalling.
TT92	A Tunstall tone protocol using DTMF or STMF signalling.
URL	Uniform Resource Locator. Also known as a web address, this is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
VoIP	Voice over Internet Protocol. A methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the internet.
Wi-Fi	A technology for wireless local area networking with devices based on the IEEE 802.11 standards.

G Contact details

Australia
Tunstall Australasia
Unit 1, 56 Lavarack Ave
Eagle Farm
Queensland 4009
Australia

Mail address:
Locked Bag 1
985 Kingsford Smith Drive
Eagle Farm QLD 4009
Australia

Tel: +61 7 3637 2200

Email: info@tunstallhealthcare.com.au
Website: www.tunstallhealthcare.com.au
Twitter: @TunstallAPAC

Belgium
Tunstall N.V.
Rusatiralaan 1
1083 Brussels
Belgium

Tel +32 2 51 000 70

Email: info@tunstall.be
Website: www.tunstall.be
Twitter: @tunstallbenelux

Canada
Tunstall Canada Inc.
111 Zenway Blvd
Unit 6A
Woodbridge
Ontario L4H 3H9
Canada

Tel: +1 905 677 1144

Email: sales@tunstallamerica.com
Website: www.canada.tunstall.com
Twitter: @TunstallAmerica

Denmark
Tunstall A/S
Niels Bohrs Vej 42
Stilling
8660 Skanderborg
Denmark

Tel: +45 87 93 50 00

Email: info@tunstallnordic.com
Website: www.tunstallnordic.com
Twitter: @TunstallNordic

Finland
Tunstall Oy
Äyritie 22
01510 Vantaa
Finland

Tel: +358 10 320 1690

Email: info@tunstallnordic.com
Website: www.tunstallnordic.com
Twitter: @TunstallNordic

France
Pantin manufacture Bat C3
140 Avenue Jean Lolive
93500 Pantin
FRANCE

Tel: +33 810 00 55 63

Email: contact@tunstall.fr
Website: www.tunstall.fr

Germany
Tunstall GmbH
Orkotten 66
48291 Telgte

Tel: +49 2504 701-0

Email: info@tunstall.de
Website: www.tunstall.de
Twitter: @TunstallGmbH

Malta
emCare Group Malta Limited
6PM Business Centre
Triq it-Torri
Swatar
BKR 4012

Tel: +356 2142 4949

New Zealand
Tunstall New Zealand
306 Cameron Road
Tauranga

Mail Address:
PO Box 13153
Tauranga
New Zealand

Tel: +64 (0)7 517 2685

Email: info@tunstall.co.nz
Website: www.tunstall.co.nz
Twitter: @TunstallAPAC

Norway
Vakt og Alarm AS
Guard and Alarm AS
Etne Village Center
5590 Etne
Norway

Tel: +47 53771001

Email: lillian@vaktogalarm.no
Website: www.vaktogalarm.no

Spain
Tunstall Televida
Avda. de Castilla
2 Parque Empresarial San Fernando
Edificio Munich
2ª Planta
28830 San Fernando de Henares
Madrid
Spain

Tel: +34 91 655 58 30

Email: teleasistencia@televida.es
Website: www.tunstalltelevida.es
Twitter: @TunstallTlevida

Sweden
Tunstall AB
Agnesfridsvägen 113 A
Box 9028
SE-200 39 Malmö
Sweden

Tel: +46 40 625 25 00

Email: info@tunstallnordic.com
Website: www.tunstallnordic.com
Twitter: @TunstallSverige

Switzerland
Tunstall AG
Atte Lyssstrasse 1
3270 Aarberg
Switzerland

Tel: +41 264 93 43 46

Email: s.beyeler@tunstall.ch
Website: www.tunstall.ch

The Netherlands
Tunstall B.V.
Oslo 28
2990 AH Barendrecht
The Netherlands

Tel: +31 180 696 696

Email: info@tunstall.nl
Website: www.tunstall.nl
Twitter: @TunstallNederland

United Kingdom
Tunstall Healthcare (UK) Ltd
Whitley Lodge
Whitley Bridge
Yorkshire
DN14 0HR
United Kingdom

Tel: +44 1977 661234

Email: enquiries@tunstall.com
Website: www.uk.tunstall.com
Twitter: @TunstallHealth

United Kingdom
Tunstall Response
Ascot House
Unit 1
Malton Way
Adwick le Street
Doncaster DN6 7FE
United Kingdom

Tel: 08450 565456

Email: enquiries@tunstallresponse.co.uk
Website:
www.uk.tunstall.com/monitoring

Tunstall Group Limited, Whitley Lodge, Whitley Bridge, Yorkshire DN14 0HR

t: **01977 661234**
e: **enquiries@tunstall.co.uk**
w: **tunstall.co.uk**