TecomC4 Operators Manual

P/N MAUSER-TECOMC4 • REV 1.05 • ISS 04APR17

Trademarks and patents

The TecomC4 name and logo are trademarks of UTC Fire & Security.

Other trade names used in this document may be trademarks or registered trademarks of the manufacturers or vendors of the respective products.

Manufacturer

UTC Fire & Security Australia Pty Ltd t/a Interlogix
A UTC Climate, Controls & Security company

Ground Floor, 10 Ferntree Place
Notting Hill, Victoria, 3168, Australia

Contact information

For contact information, see www.interlogix.com.au.

Content

Important information

Limitation of liability

To the maximum extent permitted by applicable law, in no event will Interlogix (a division of UTC Fire & Security Australia Pty Ltd) be liable for any lost profits or business opportunities, loss of use, business interruption, loss of data, or any other indirect, special, incidental, or consequential damages under any theory of liability, whether based in contract, tort, negligence, product liability, or otherwise. Because some jurisdictions do not allow the exclusion or limitation of liability for consequential or incidental damages the preceding limitation may not apply to you. In any event the total liability of Interlogix shall not exceed the purchase price of the product. The foregoing limitation will apply to the maximum extent permitted by applicable law, regardless of whether Interlogix has been advised of the possibility of such damages and regardless of whether any remedy fails of its essential purpose.

Installation in accordance with this manual, applicable codes, and the instructions of the authority having jurisdiction is mandatory.

While every precaution has been taken during the preparation of this manual to ensure the accuracy of its contents, Interlogix assumes no responsibility for errors or omissions.

Preface

Related documentation

Refer to the following documents:

- *TecomC4 Installation Manual*
- *Challenger Series Installation and Quick Programming Manual*
- *Challenger Series Programming Manual*
- *TitanCT Users Manual*

Typographical conventions

This manual uses certain notational and typographical conventions to make it easier for you to identify important information.

Table 1: Notational and typographical conventions

Item	Description
Command sequences	Where appropriate, command sequences are abbreviated with the “>” symbol. For example, the command “Click Start, and then click Run” is written as “Click **Start > Run**”.
Buttons and menu items	Buttons and menu items are written in **bold**.
Tabs	Tabs on TecomC4 panels are written in *italic*.
Notes	Notes alert you to information that can save you time and effort.
Warnings	Warnings are displayed to advise you that failure to take or avoid a specified action could result in loss of data.

1 Introduction

1.1 Product overview

TecomC4 is a centralised, multi-operator, multi-tasking, network-enabled software solution for building security management. The TecomC4 system consists of a single server running the TecomC4 server application and one or more client computers running the TecomC4 client application.

TecomC4 integrates a large variety of security devices, from camera systems to intrusion detection and access control, into one view. Drivers for many security devices can be installed in TecomC4, including a driver for Challenger10.

Operators of the TecomC4 system can be assigned roles according to policy, from monitoring and dispatch to assigning cards and visitor management.

TecomC4 may be used in a range of applications, from a simple monitoring system for a single building to robust, large enterprise solutions to monitor various security devices in multiple buildings, regardless of the distance between them.

TecomC4 provides operators with a wide range of tools for the following:

- Centralised security systems management
- Security system visualization and monitoring
- Security process automation
- Security information analysis and evaluation
- Central identity management
- Crisis management support

1.2 Key concepts and terminology

The TecomC4 **navigation menu** allows an operator to view different sections of the TecomC4 system, such as persons or alarms. These different sections of the TecomC4 system are called **panels**. Only one panel is visible at a time. You can log in multiple times in order to view multiple panels in separate windows. The panels that an operator can view are determined by the operator's permissions.

A **device** is the general term used for a security device such as a Challenger10 or NVR. Each type of device requires a device **driver** for TecomC4 to communicate with the device. You only need to install a driver once for each type of security device. Each device has a **bus controller**, which controls communication with the device. Devices are represented in TecomC4 in a hierarchy called the **Devices tree**.

The **secure installation** is the set of security devices managed by TecomC4. This could include multiple types of security device and those devices can be geographically spread.

People who require access to the TecomC4 system with a login account are called **operators** of TecomC4. Their permissions to view and edit parts of the TecomC4

interface are determined by **roles**. You can override role permissions for individual operators.

Access refers to a person's permission to physically access parts of the secure installation and arm/disarm areas, etc. People who require access to the secure installation are called **users**. In order to access the secure installation, a user requires user credentials such as a card or PIN code. The permissions to enter secure areas and arm/disarm areas etc. are determined by user **access levels**. You can override access level permissions for individual users. Access levels are applied to specific device elements, such as areas and doors, called **access points**.

All individuals associated with the TecomC4 system, whether as operators of the system or people requiring physical access to secure areas, are called **persons**. Persons can be are arranged in a tree-like hierarchy, including organisational units such as companies and departments, called the **organisational structure**. The organisational structure is represented in TecomC4 by the **Persons tree**.

Note: A person can be a user and an operator at the same time. For example, a receptionist has access to a secure site (as a user) and can assign visitor cards (as an operator).

Note: You should only have one entry in the organisational structure for each individual person.

You can make a person a user and/or an operator by assigning **credentials** to them. To make a person a user, assign a card and/or a PIN credential. To make a person an operator, assign a login authentication credential.

Regions are another way for the operator to view the security devices in the system. Regions can contain elements from multiple security devices and can cover multiple geographical areas.

Anything that happens in the entire TecomC4 system, from a user accessing a secure area, to an operator changing permissions for a role, is recorded as an **event** in the system.

Note: TecomC4 is not specific to Challenger10, so some things may be unfamiliar. For example:

- You do not need to program door groups etc. directly. The driver for Challenger10 converts access information behind the scenes into door groups etc. for you.
- Green is used to represent an armed area. Similarly, blue is used to represent a disarmed area.

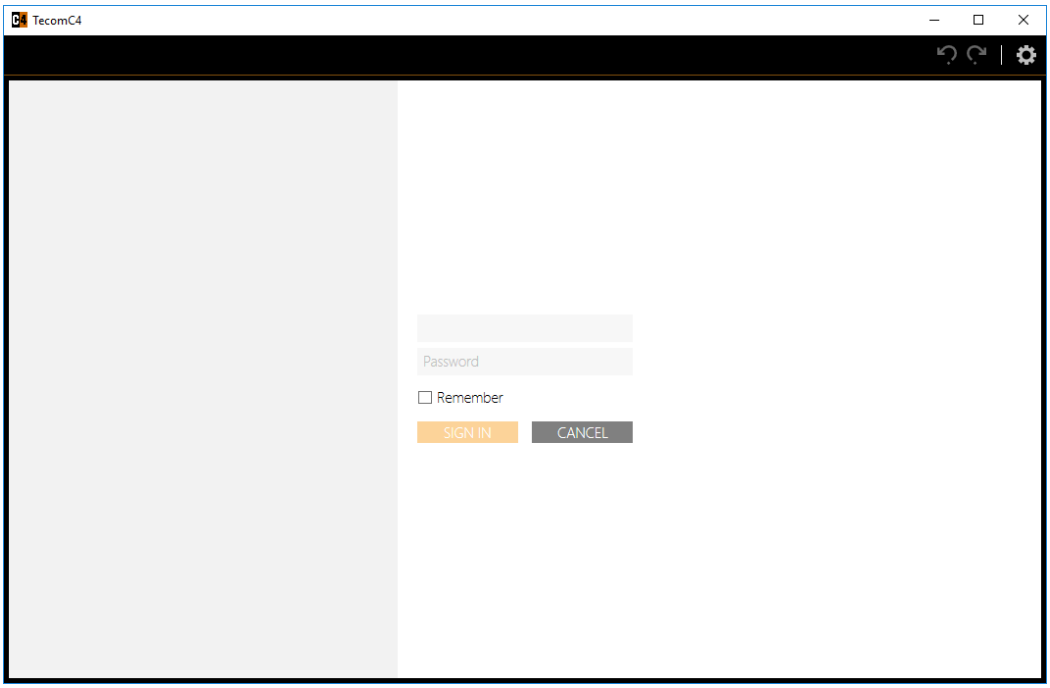
---

2 Logging in to TecomC4

After successful installation of the TecomC4 server and client applications, start the TecomC4 client application by selecting the launch command from the Windows Start menu: **Programs > Gamanet a.s > TecomC4**.

Note: The computer name of the TecomC4 server is included in the shortcut name of the TecomC4 client. In case you have multiple TecomC4 clients for multiple TecomC4 servers installed on the same computer, you would be able to differentiate between the clients.

When you launch the TecomC4 client, a splash screen is displayed. The login screen is then displayed:



Upon initial login, the language of the login screen is determined based on the regional settings of the operating system. Upon subsequent login, the language of the login screen is the same as the language of the operator who was last logged in. In the login window, enter the appropriate information:

- **Sign in** – the operator's login name for the application.
- **Password** – the operator's password for the application.

In this login window you can also choose the following property for logging in to the application:

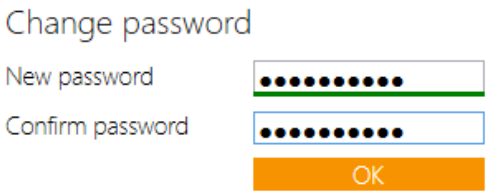
- **Remember** – tick this checkbox for the system to remember your login data, which will be filled in automatically in the login window the next time you run the application.

In the case of a new installation, the TecomC4 system has one standard predefined operator account with the following login name/password:

- **Login name:** support

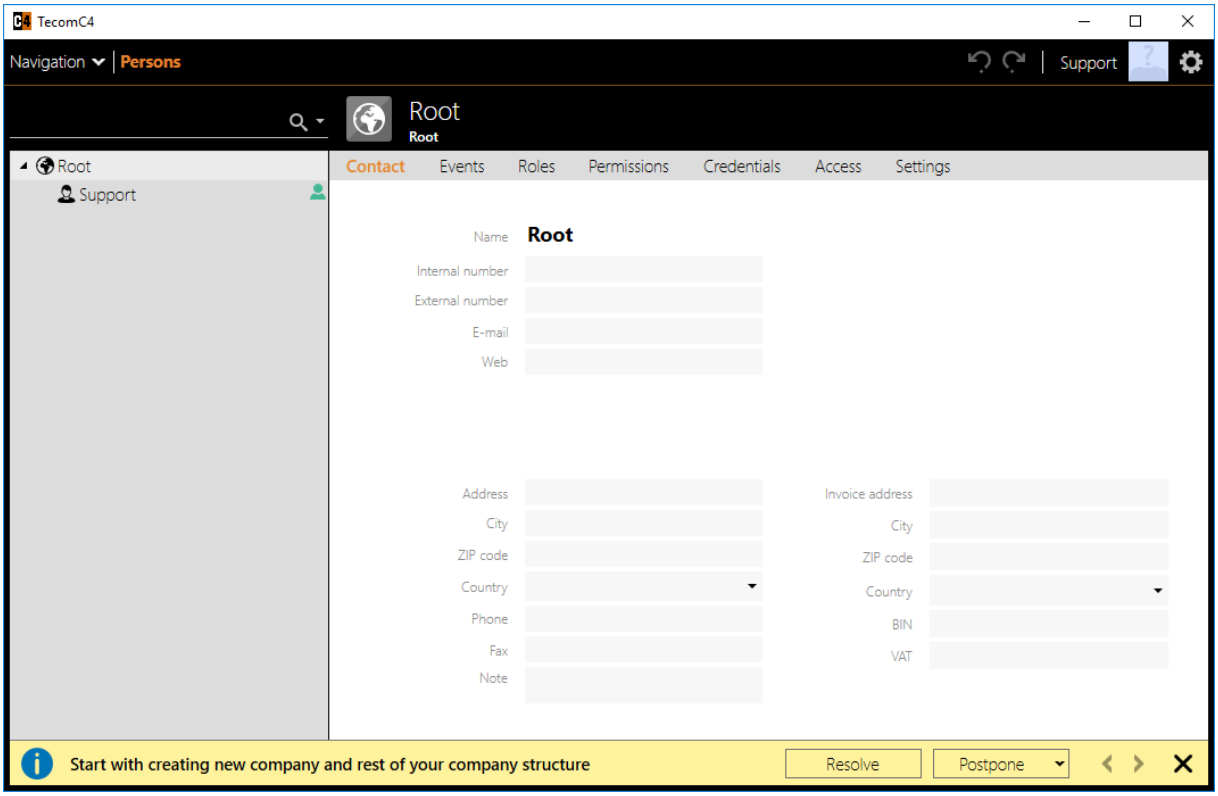
- **Password:** support

For security reasons, the “support” operator will be prompted to change their password after initial login. Upon entering the new password in the **New password** box, the system checks its strength based on built-in security algorithms. The password is considered strong enough when the coloured bar underneath the **New password** box is filled and coloured green:



Confirm the new password by entering it again and then click the **OK** button.

When you first log in, you will be greeted by the following screen:



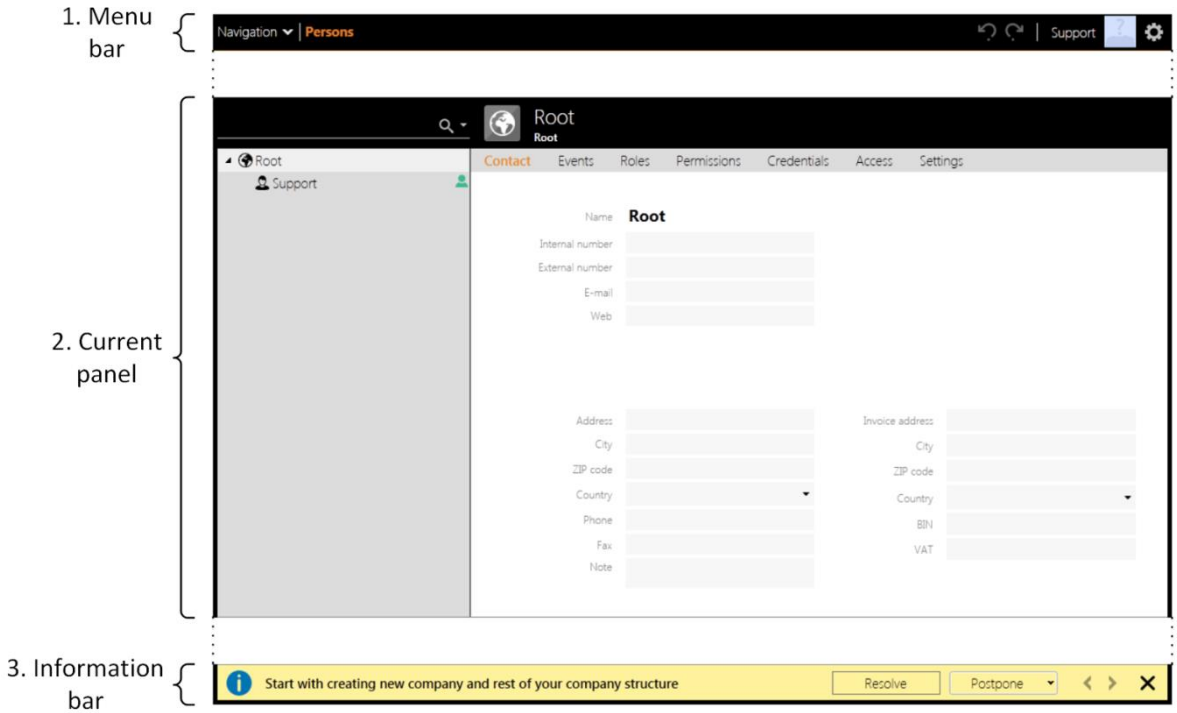
The TecomC4 interface is described in the following chapter.

3 The TecomC4 interface

After a successful operator login to the system, the main screen of the TecomC4 application is displayed.

The TecomC4 application is divided into logical sections, so that even complex data structures can be presented to the operator in a simple manner. The basic information entered into the system is recorded in a tree structure (persons, devices, regions); other objects are represented by lists.

Figure 1: Elements of the TecomC4 interface



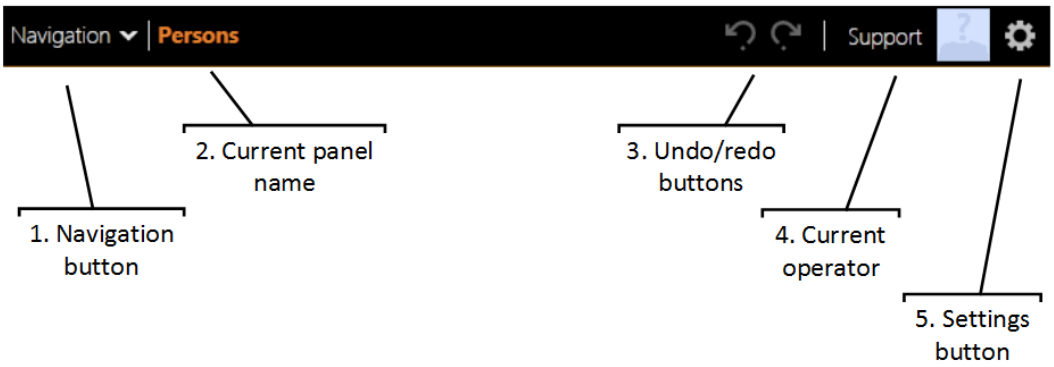
The main elements of the TecomC4 interface, numbered in the figure above, are:

1. The **menu bar**, which contains the main navigation menu button, the undo and redo buttons, and buttons to change settings.
2. The **current panel**, which varies according to the selection of the navigation menu.
3. The **information bar**.

Each element is explained in more detail in the following sections.

3.1 The menu bar

Figure 2: Elements of the menu bar



The menu bar is always visible and contains the following elements, numbered in the figure above:

1. The **navigation button**, which opens the **navigation menu**. You can use the navigation menu to switch between the different sections of the application, which are called **panels**.
2. The **name of the currently displayed panel**, corresponding to the selected menu item from the navigation menu. One panel is displayed at any one time.

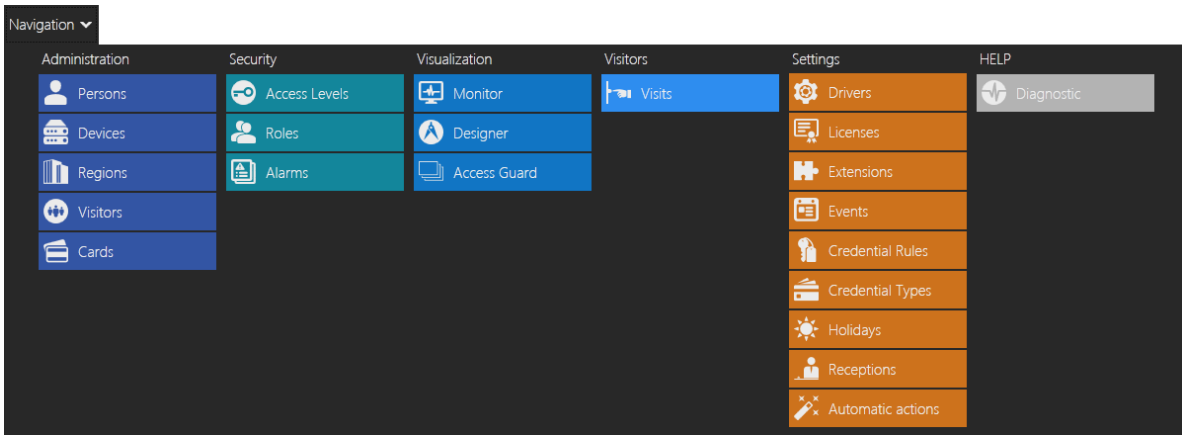
   Note: You can log in multiple times in order to see more than one panel.

3. The **undo** and **redo** **buttons**.
4. The name and picture of the **logged in operator**. Clicking here will open the operator's personal settings (e.g., language).
5. The **settings button**, which has options to restart and exit the application, reset settings or display general information about the application.

The elements of the menu bar are described in more detail in the following sections.

3.1.1 Navigation button

The **navigation menu** can be accessed by clicking the **navigation button** on the left of the menu bar. The navigation menu will appear:



There are six submenus in the navigation menu:

- **Administration** – allows the operator to manage the system, including managing people and organisations, devices, regions and cards.
- **Security** – allows the operator to manage access levels, view alarms, and alter operator roles.
- **Visualization** – allows the operator to design map views and interactions, view maps and alarms, and perform real-time monitoring of doors.
- **Visitors** – allows the operator to manage visits to a site.
- **Settings** – allows the operator to change settings for different aspects of the TecomC4 system.
- **Help** – allows the operator to run diagnostics on the TecomC4 system.

3.1.2 Current panel name

The name of the current panel is shown next to the navigation button.

3.1.3 Undo and redo buttons

If you need to undo a change that has been saved to the TecomC4 database, you can click the undo button at the top of the screen or press CTRL+Z on your keyboard. To redo changes which have been undone, click the redo button at the top of the screen or press CTRL+Y on your keyboard.

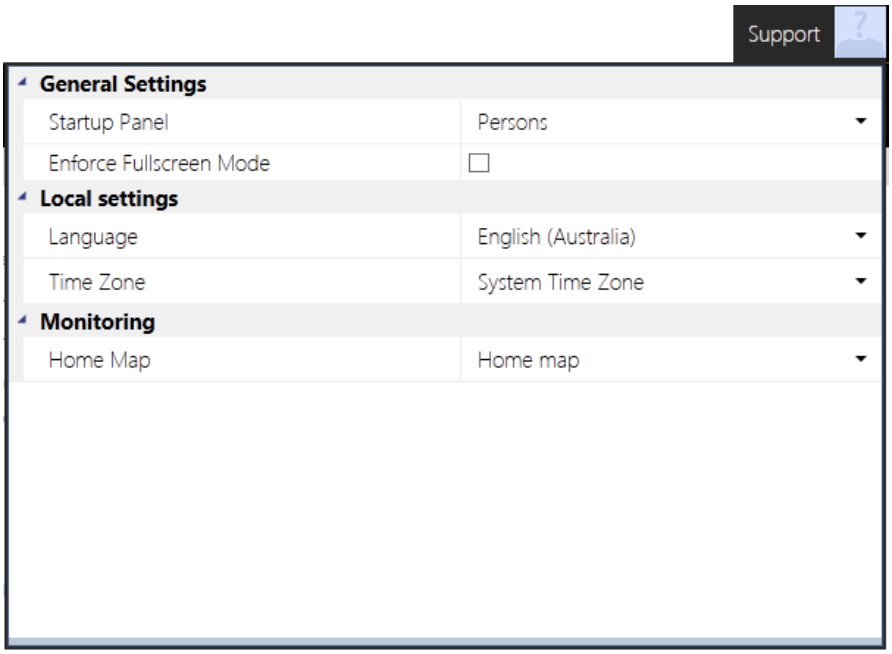
If the undo or redo action is not available, then the respective undo or redo button will be greyed out.

Note: The undo button undoes the last change you made even if the changed field is not visible on the screen at the time.

Note: If you switch away from the panel where you made the changes and switch back to it again, the undo functionality will not be available.

3.1.4 Logged in operator

The name and photo of the currently logged in operator is shown on the menu bar. If you click the name or photo, the following settings will appear:

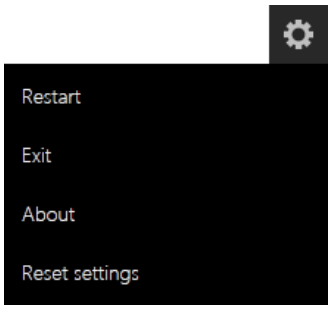


The settings are:

- **Startup Panel** – Select the TecomC4 panel to be shown when the operator logs in.
- **Enforce Fullscreen Mode** – Enforce fullscreen mode for the operator. The TecomC4 client fills the screen and no window border is shown.
- **Language** – Select the language to use in the TecomC4 client. Ensure that English (Australia) is selected since the language setting also includes region-specific terminology such as “Isolate”.
- **Time Zone** – Select the world time zone to use in the TecomC4 client. The default is the computer’s time zone.
- **Home Map** – Select the map displayed when you navigate to the Monitor panel. See the “Monitoring the system” chapter on page 111 for more information about the Monitor panel.

3.1.5 Settings button

If you click the settings button, the following menu is displayed:



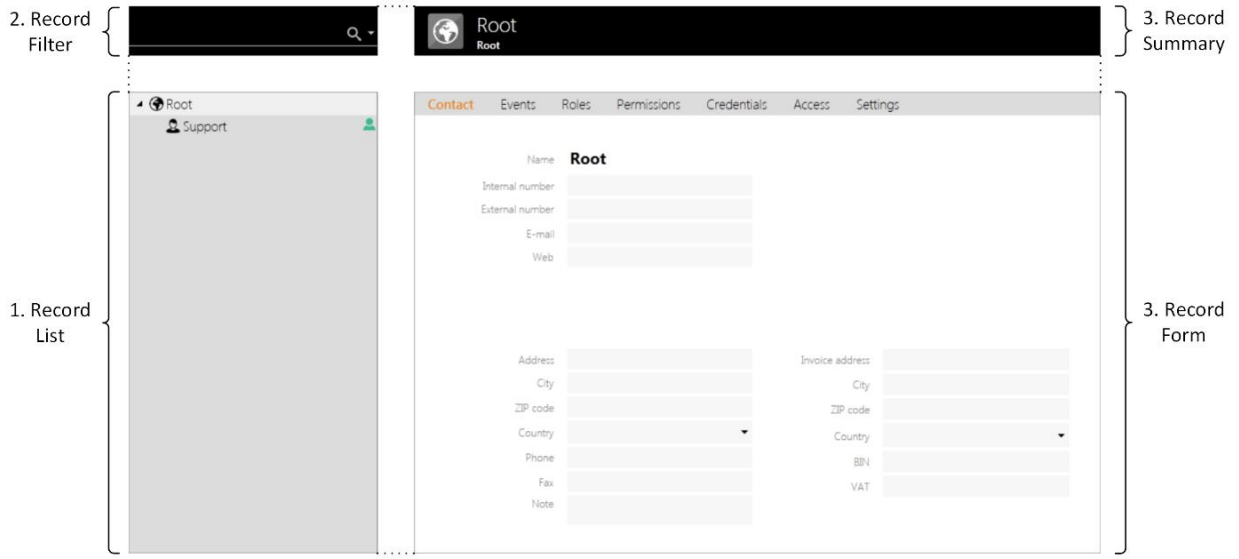
The options on this menu are:

- **Restart** – Log off the TecomC4 client so another operator can log in
- **Exit** – Log off and exit the TecomC4 client
- **About** – Display general information about the TecomC4 software
- **Reset settings** – reset operator settings to their default values, such as the layout of windows.

3.2 The current panel

The current panel varies according to which menu item the operator selected from the navigation menu. Most panels look like the following:

Figure 3: Standard elements of the current panel



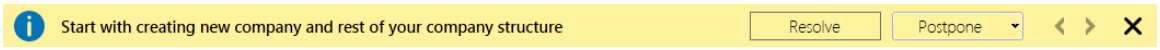
The current panel may contain the following elements, numbered in the figure above:

1. The **record list**, which can display either a hierarchical tree of records or a list of records. Whether a tree or list is present depends on the currently displayed panel. Note that not all panels display a record list (e.g., the Alarms panel does not have a record list). Selecting a record from the record list will change the information displayed in the record summary and record form.
2. The **record filter**, which is used for filtering records in the record list. The record filter is only shown on a panel if the record list is present. See the “Filtering” section on page 15 for more information.
3. The **record summary**, which shows summary information about the currently selected record in the record list (its name and type). The record summary is only shown on a panel if the record list is present.

4. The **record form** showing detailed information about the currently selected record in the record list. The panel consists of **tabs** with information that can be viewed and edited by the operator.

3.3 Information bar

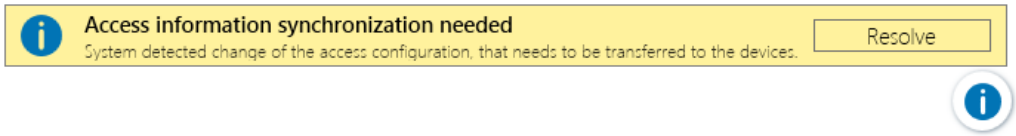
While working with the TecomC4 application, information may appear at the bottom of the window intended to guide the operator to the next operation or to indicate failures in the security system.



You can click the **Resolve** button to continue to resolve the situation. Click the **Postpone** button to postpone the message by a certain time. The message will disappear and reappear after the selected time. Click the cross ✕ in the message to postpone it by 30 minutes (or to permanently close it if the message does not have the option to postpone).

If there are multiple issues, you can scroll through them using the arrow ‹ › buttons.

When you postpone an issue, an icon will appear in the bottom right of the TecomC4 interface, e.g. ⓘ. Clicking the icon will show a tooltip with the issue.



The icon will appear on all TecomC4 clients, so that all operators know that there are postponed issues.

4 Working with the interface

4.1 Saving changes

The TecomC4 system is designed to immediately save changes made in the client application. This requires permanent online connection with the TecomC4 server. If communication with the server is lost, a connection lost warning appears and the operation of the application is disabled until the connection is automatically restored to prevent loss of data.

Changes made by the operator are saved to the backend database the moment the operator leaves the field in which a value was entered. Changes are only saved if the application successfully validates the entered data. Otherwise, a coloured frame appears around the field indicating invalid data. The operator must correct the data or the invalid data will not be saved. This prevents the entry of invalid data to fields (for example, if the system expects a numeric value, it is not possible to enter a text string). If an object is not saved in the database, an exclamation mark  is shown next to the name of the object.

You can navigate away from an invalid field, but the field must be fixed before it will be saved in the TecomC4 database.

The TecomC4 system is a multi-operator network application, so changes made to one client application are continuously sent to other client applications, where other operators can work with the data.

If you need to undo a change that has been saved to the TecomC4 database, you can click the undo button  at the top of the screen or press CTRL+Z on your keyboard. To redo changes, click the redo button  at the top of the screen or press CTRL+Y on your keyboard.

4.2 Working with the tree

A tree is displayed for the Persons, Devices and Regions panels.

A tree allows complex data structures to be presented to the operator in a relatively simple way. It can be used to quickly browse data in the hierarchical structure. A tree is composed of nodes in a hierarchy. Clicking a tree node displays its details in the form on the right side of the screen.

If the tree pane is not wide enough for all the information to fit, the operator can change the tree pane width by clicking its border and dragging with the mouse.

4.2.1 Node context menu

Right-clicking on a node in the tree displays the node's context menu. Depending on the type of tree and the node's place in the tree hierarchy, a variety of menu options will be available in the context menu.

The context menu can be used to add new nodes, archive and delete nodes, and perform other modification tasks as described in the following sections.

4.2.2 Adding nodes

To add a new node, right-click on an existing node and select the **Add** menu item from the context menu to display the **Add** sub-menu. The items displayed on the Add sub-menu depend on the type of node selected.

Note: The **Add** menu item will only appear in a selected node's context menu if it makes sense to add a new node under the selected node. For example, you can add a new person under a company or department node, but you cannot add a new person under an existing person node.

4.2.3 Expanding and collapsing nodes

A node can be expanded to show its child nodes by clicking the expand icon in the tree. A node can be collapsed to hide its child nodes by clicking the collapse icon in the tree.

The following keyboard shortcuts can be used when working with a tree:

- Expand the selected node without child nodes by pressing the + key on the keyboard's number pad
- Expand the selected node, including child nodes, by pressing the * key on the keyboard's number pad
- Collapse the selected node by pressing the – key on the keyboard's number pad

A selected node's context menu also has **Expand All** and **Collapse All** menu items to expand all child nodes and collapse all child nodes, respectively.

4.2.4 Cutting, copying and pasting nodes

You can cut, copy and paste selected nodes using the CTRL-X, CTRL-C and CTRL-V keyboard shortcuts, respectively. A node can only be pasted under a target node if it would be possible to add a node of that type under the target node.

The system supports the selection of multiple nodes at once, either by holding down the SHIFT key while clicking to select contiguous nodes or by holding down the CTRL key while clicking to select non-contiguous nodes. Only nodes at the same hierarchical level can be selected at the same time.

The system also supports dragging and dropping of nodes within the tree.

4.2.5 Changing node categories

To change a node's category (such as changing a person from a manager to an external employee), access the node's context menu by right-clicking it, select the **Change category** menu item and select the new required node category. If multiple nodes have been selected at once, the category can only be changed if all selected nodes belong to the same category.

4.2.6 Archiving, restoring and deleting nodes

To archive a node and its child nodes, access the node's context menu by right-clicking it and select the **Archive** menu item.

Archived nodes in the tree are only visible if a relevant filter is enabled (e.g., the **Show archived persons** filter or the **Show only archived persons** filter for the Persons tree).

When a node is archived, the following applies:

- The archived node is read-only; its modification is prohibited.
- The structure of the deleted part of the tree is preserved, but changes to the structure are prohibited.
- At the next access data synchronization, archived persons are deleted from devices. At the same time, their accounts to access the TecomC4 application will be blocked.
- You can search the event history of archived nodes.
- Export/import operations ignore archived nodes.

In order to preserve the structure of the tree, it is only possible to restore a node if its parent node is not archived. To restore a node, access the node's context menu by right-clicking it and select the **Restore** menu item. The restored node is inserted at its original place in the tree.

You can also restore the archived node including its child nodes by selecting the **Restore with children** menu item.

To permanently delete the archived node from the system, access the node's context menu by right-clicking it and select the **Delete** menu item. A dialog box will be shown asking you to confirm the deletion.

Note: You can only delete a device from the Devices tree if communication with the device has been stopped.

Warning: If you permanently delete the archived node, its history is also deleted irreversibly.

4.3 Importing and exporting data

It is possible to import data from a CSV (comma-separated values) file into the Devices, Regions and Persons trees. Likewise, it is possible to export data from those trees to a CSV file.

To import or export at a particular node of a tree, open the node's context menu by right-clicking it and select the **External data** menu item to display the External data sub-menu.

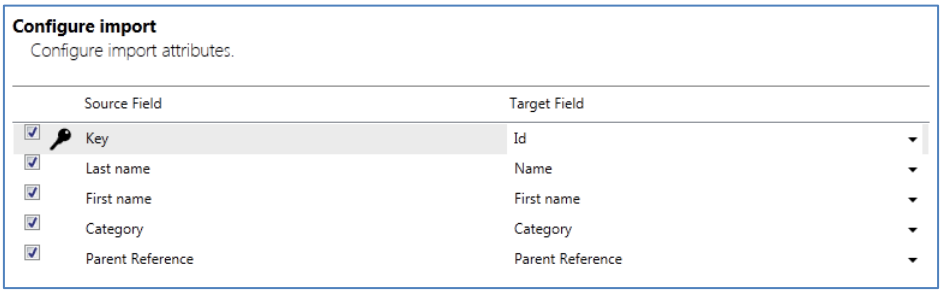
Depending on the type of node selected, the **Import** menu item and/or the **Export** menu item may be displayed. Selecting the **Import** menu item will open an import wizard window where you can select a file to import. Selecting the **Export**

menu item will open an export wizard window where you can select a location on the computer and a filename to save the exported data.

4.3.1 Importing data from a CSV file

To import data from a CSV file, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select the required panel from the navigation menu.
2. Right-click the node of the required tree in the record list to open the node's context menu. Select **External data > Import**, which will open the import wizard window.
3. When the import wizard appears, enter the path to the CSV file to be imported or click the **Browse** ... button to open a file open dialog window. Click the **Next** button.
4. The import wizard will show the source fields available in the CSV file on the left. For each source field, you can select a target field in TecomC4 from a drop-down list on the right. For example:



   Source fields that have a tick in the checkbox next to their name will be imported. The import wizard will attempt to prefill as many of the target fields as it can.

   The import CSV file must contain a column that can be mapped to the "Name" target field, and each record in the import CSV file must have a value entered in that column.

   The import CSV file must contain a column that can be mapped to the "Id" target field, and each record in the import CSV file must have a *unique* value entered in that column. Click in between the checkbox and the name of the source column to add the unique key icon to indicate that this column contains the unique key.

   When you have finished assigning target fields to the source fields, click the **Next** button.
5. The import wizard will display the proposed changes to TecomC4. Confirm the changes by clicking the **Next** button.
6. The import wizard will display an import summary. Click the **Finish** button to close the import wizard.

4.3.2 Exporting data to a CSV file

To export data to a CSV file, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select the required panel from the navigation menu.
2. Right-click the node of the required tree in the record list to open the node's context menu. Select **External data > Export**, which will open the export wizard window.
3. When the export wizard appears, enter the path to the CSV file to be exported or click the **Browse** ... button to open a file open dialog window. There is an option to export protected properties, such as passwords and PIN codes, which can be ticked. Click the **Next** button.
4. The export wizard will display an export summary. Click the **Finish** button to close the export wizard.

Note: If a node is archived, it cannot be exported. If several nodes are selected, only those that are not archived will be exported.

4.4 Filtering

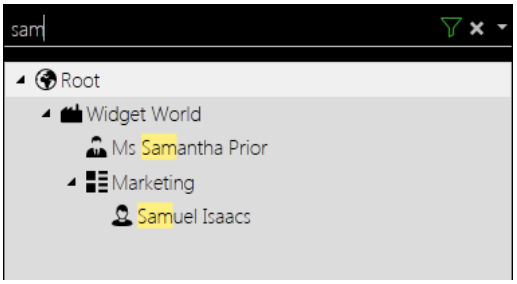
The **filter** is a readily available search tool in many parts of the application. It is available whenever a tree or list is displayed, whether in the record list or within a tab on the record form.

4.4.1 Record filter

When text is entered in the filter bar to the left of the magnifying glass icon in the record filter, the displayed data in the record list will be filtered so that only results containing the text will be displayed. The searched for text will also be highlighted in colour in the record list.

You can search for individual words or use quotation marks to search for phrases. If you enter multiple search terms separated by spaces, then all the search terms must be present in the item for the item to be displayed.

For example, you can filter the Persons tree for specific names:



When you click the triangle next to the filtering magnifying glass, you can display further predetermined filtering criteria depending on where you are in the application.

If filtering is enabled, a green filter icon  is shown. You can click the cancel filter button  to stop filtering.

4.4.1.1 Filter by property

It is possible to filter the record list by a specific property value. Enter the name of the property and the required value separated by a colon.

For example, you could search for devices with the address value of 200 by entering **address:200** in the filter. Or you could search for devices of type detector by entering **category:detector** in the filter.

Note: If the searched for property or value consists of words separated by spaces, then the property or value must be enclosed in quotation marks (for example, **“IP Address”:localhost** or **category:”card reader”**).

4.4.2 Form filter

A filter which works under the same principles as the record filter is also available in many other areas of the TecomC4 system, such as on the *Events* tab in the record form for a selected record.

You can enter a filtering condition in the search bar to the left of the magnifying glass icon  to filter the information displayed. A green filter icon  is shown if filtering is enabled. Filtering can be cancelled by clicking the cancel filter button  .

On some tabs, such as the *Events* tab, there is also a drop-down menu button from which you can select specific filter options.

4.5 Getting help

Press F1 at any time to open context-sensitive help.

You can hover the mouse cursor over icons and buttons to see helpful tooltips.

5 Getting started

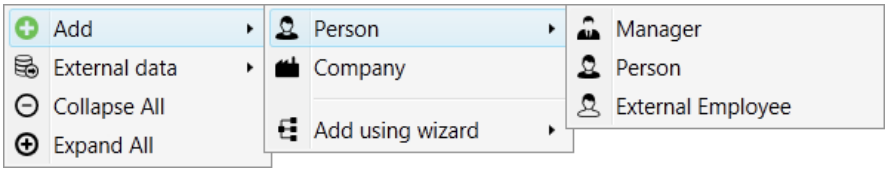
5.1 Creating a system administrator account

Since the TecomC4 system is designed as a multi-operator system with responsibilities divided among individual operators, it is recommended that you create an operator account for the main administrator of the system. This ensures that all other operations will be traceable in the history under the name of a specific operator.

It is recommended that you leave the “support” operator in the system and safely store its changed password. If the account of the main system administrator is disabled, it will be possible to revert to the “support” operator account and to change the administrator’s password or to create a new system administrator.

To create the system administrator’s operator account, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Right-click the **Root** node of the Persons tree to display the Root node’s context menu. Select **Add > Person** and select the required person type.



3. In the form section, enter the person’s contact details on the *Contact* tab. For more information about the fields on this tab, see the “Persons panel: Contact tab” section on page 91.
4. On the *Roles* tab, tick the **Administrator** role.
5. On the *Credentials* tab, click the **Add** button to add a **Forms Authentication** credential and enter the desired account name and password. Upon entering the password, the system checks its strength based on built-in security algorithms. The password is considered strong enough when the green tick symbol appears after the password. Enter the password again in the **Confirm password** text box. Click the **Change** button to confirm the new password.
6. If the **User must change password at next logon** checkbox is ticked, the system will request that the password be changed when the person logs in for the first time.
7. Select the required personal settings on the *Settings* tab. For more information about the fields on this tab, see the “Persons panel: Persons Present tab” section on page 99.

   Note: Ensure that English (Australia) is selected for the Language since the language setting also includes region-specific terminology such as “Isolate”.

8. Restart the application and log in using the new login details.

5.2 License activation

Without the activation of a valid licence, the system can only work in trial mode for 60 days. A license reminder notification will appear in the information bar before the trial period expires.

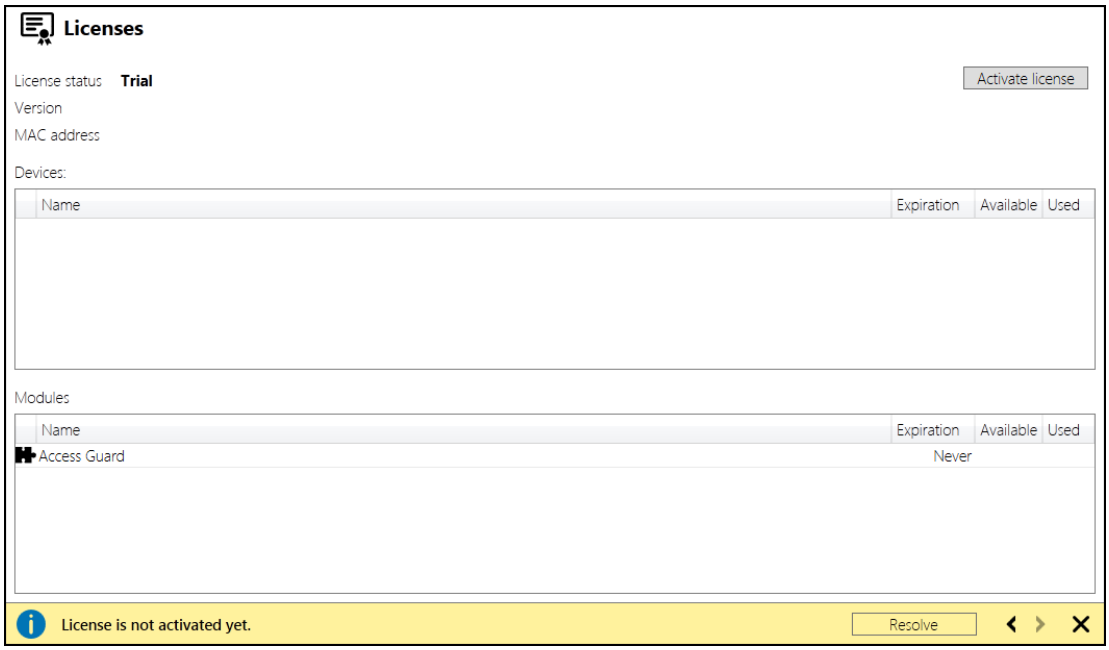
A valid license must be activated to ensure the correct and permanent operation of the system. A valid license allows the operator to use the TecomC4 system legally.

Activated licenses for TecomC4 are shown on the Licenses panel.

5.2.1 Licenses panel

The Licenses panel can be opened by clicking the **Navigation** button and selecting **Licenses** from the Settings menu.

The Licenses panel looks like this:



If you own a trial version of the TecomC4 system and you do not have a license, the attributes in this panel are empty.

If you already own a license, the attributes contain the current license information. If you want to connect further devices to the system or gain access to new functions, you may have to update the licence.

The Licenses panel contains the following information:

- **License status** – The status of the currently active license.
- **Version** – The software product version for which the license is issued.
- **MAC address** – The hardware identifier of the device with the activation key assigned to it.
- **Devices** – The list of devices allowed to be connected based on the license.

- **Modules** – Contains the list of application modules that the operator can access in the application. There may be a separate limitation for each application module in terms of the license expiry date.

5.2.2 Activating a license

A license is received in the form of an activation key from the supplier of your TecomC4 system upon fulfilling the licensing conditions.

To activate a license, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Licenses** to open the panel with the current license information. If you own a trial version of the TecomC4 system and you do not have a license, the attributes in this panel are empty.
2. Click the **Activate license** button. The button opens a dialog window.
3. Click the **open from file** button to open a file open dialog window. Navigate to your license file and open the file to install the license.

5.3 Configuring a TecomC4 system

There are many aspects to configuring a TecomC4 system. The following chapters outline the most important parts of configuring a system:

1. Defining holidays (page 21) – defining holidays
2. Installing drivers (page 24) – installing drivers for security devices
3. Configuring devices (page 26) – configuring and connecting devices
4. Configuring regions (page 46) – configuring regions
5. Configuring visualization (page 53) – configuring maps for visualization
6. Configuring user credentials (page 62) – configuring user credentials (cards and PINs)
7. Configuring user access levels (page 71) – configuring user access
8. Configuring operator roles (page 81) – configuring operator roles
9. Persons management (page 90) – configuring persons, including assigning credentials as users and operators, assigning user access levels and assigning operator roles

Ongoing monitoring of a TecomC4 system is discussed in the following chapter:

- Monitoring the system (page 111)

More advanced configuration is discussed in the following chapters:

- Events (page 124)
- Automatic actions (page 128)
- Advanced system properties (page 134)

- Visitor management (page 139)
- System maintenance (page 146)

6 Defining holidays

Holidays and non-working days are important for user access management so they must be defined correctly. Holidays are divided into holiday groups, which are sets of holidays that are valid for a specific area such as a state. For devices that support access management, such as Challenger10, a holiday group can be set on the device.

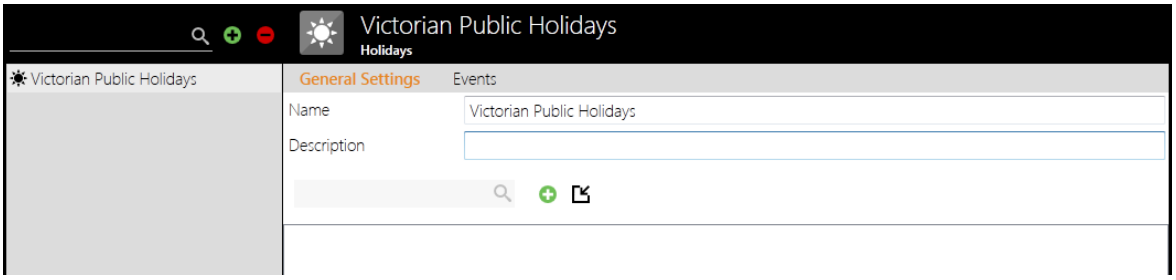
Note: Holidays are sent to Challenger10 devices every night. Only holidays that are in the future are sent to Challenger10 devices. If required, you can force the sending of holidays by running the **Send All Credentials** command. See the "Sending credentials and access information to devices" section on page 43 for more information on the command.

Note: There is a limit of 24 holidays that can be sent to Challenger10 devices.

6.1 Holidays panel

Holidays are defined on the Holidays panel, which can be opened by clicking the **Navigation** button and selecting **Holidays** from the Settings menu.

The Holidays panel looks like this:



The record list shows a list of holiday groups.

The record filter can be used to filter holiday groups in the record list.

The record form has the following tabs:

- General Settings
- Events

The tabs are described in the following sections.

6.1.1 Holidays panel: General Settings tab

The *General Settings* tab shows the following fields for the selected holiday group:

- **Name** – Name of the holiday group
- **Description** – Optional description of the holiday group

There is a filter to filter the list of holidays, as well as buttons to add single holidays to the holiday group and import holidays from a file into the holiday group.

6.1.2 Holidays panel: Events tab

The *Events* tab shows all events associated with the selected holiday group. See the "Events" chapter on page 124 for more information about the *Events* tab.

6.2 Defining holidays

To define a new holiday group and add holidays to it, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Holidays** to open the Holidays panel.
2. Click the **Add** button next to the record filter to add a new holiday group.
3. Enter a name and optional description on the *General Settings* tab.
4. When defining holidays, there are two ways to enter information:
   - **Adding manually:** on the *General Settings* tab, click the **Add** button. Enter the name and date of the holiday. To remove the holiday, click the **Delete** button next to the date of the holiday.
   - **Importing from file:** on the *General Settings* tab, click the **Import from file** button. When the import wizard appears, enter the path to the holiday file to be imported or click the **Browse** button to open a file open dialog window. Click the **Next** button.

     Select the holiday group you wish to import and click the **Next** button. Confirm the changes and click the **Next** button. The imported holidays will be added to the holiday group. Click the **Finish** button to close the import wizard.

You can click the **Delete** button next to the record filter to delete the selected holiday group. A dialog box will be shown asking you to confirm the deletion.

Warning: Changes made to holidays will only take effect on a connected security device when the holidays are sent to the device. Holidays are sent to devices every night. If required, you can force the sending of holidays by running the **Send All Credentials** command. See the "Sending credentials and access information to devices" section on page 43 for more information on the command.

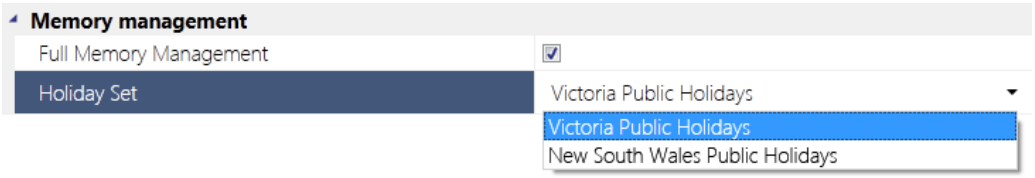
6.3 Setting holidays on Challenger10

If only one holiday group is defined in TecomC4, then that holiday group will be set on all connected Challenger10 devices. If there is more than one holiday group defined, then you can select the holiday group to be set on each connected Challenger10 individually.

To set the holiday group on a Challenger10, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Select the Panel element of the Challenger10 device.

3. On the *General Settings* tab select **Holiday Set** under the **Memory Management** section. Select the holiday group to set on the Challenger10 device from the drop-down list. For example:



7 Installing drivers

In order for the TecomC4 system to be able to communicate with a security device, a **driver** for the device must be installed within TecomC4. TecomC4 supports many different security devices for which drivers are available, including Challenger10.

Note: If you have multiple devices of the same type (e.g. several Challenger10 devices), you only need to install the relevant driver once.

7.1 Drivers panel

Drivers are installed on the Drivers panel, which can be opened by clicking the **Navigation** button and selecting **Drivers** from the Settings menu.

The Drivers panel looks like this:

The Drivers panel has a toolbar with a filter to filter the list of drivers and a button to add a new driver from file, if required. The panel has the following tabs:

- **Installed drivers** – Shows a list of drivers installed in the system.
- **Online** – Shows all drivers available for installation online.
- **Updates** – Shows installed drivers for which there is an update available online.

7.2 Installing a driver

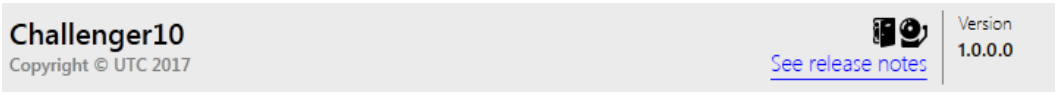
A new driver can be installed from online. Follow these steps to install a driver:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Drivers** to open the Drivers panel. The Drivers panel initially shows the list of installed drivers on the *Installed drivers* tab.
2. Click the *Online* tab and install the required driver (e.g. Challenger10) from the list.

Note: In some cases, you may also be requested to accept a license agreement for a specific driver, which can be done by clicking the **I Accept** button.

Note: After installation of a new driver, update of TecomC4 client applications may be required. Client application updates will be performed automatically in the background. You may be required to restart the client application after it has finished updating, as indicated on the information bar. This notification must be dealt with by clicking the **Resolve** button on the information bar.

The new driver will appear in the list of drivers on the Drivers panel. Information about the driver, such as its version number will appear. Icons showing the driver's capabilities are also shown. The Challenger10 driver provides Access Control and Intrusion Alarm capabilities, as shown in the figure below:



Hover the mouse cursor over the icons to see the relevant driver capabilities.

Note: If you have been supplied with a driver installation package (a file with the *.c4driver* file extension), then you can install the driver by clicking the **Install driver from file** button. A file open dialog window will open. Locate the driver installation package and click the **Open** button.

7.3 Upgrading a driver

A driver upgrade can be installed from online. Follow these steps to upgrade a driver:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Drivers** to open the Drivers panel. The Drivers panel shows the list of installed drivers.
2. Click the *Updates* tab and install the required driver upgrade.

Note: If you have been supplied with a driver installation package (a file with the *.c4driver* file extension), then you can upgrade the driver by clicking the **Install driver from file** button. A file open dialog window will open. Locate the driver installation package and click the **Open** button.

8 Configuring devices

An essential part of setting up a TecomC4 system is the connection of security devices, such as Challenger10 devices and NVRs.

Devices have elements such as doors and CCTV cameras, depending on the type of device. A device's elements are displayed in a tree structure. All of the devices and their tree structures are displayed in the **Devices tree** on TecomC4's Devices panel.

Each device has a **bus controller**, which controls communication with the device. The bus controller acts as the root of the Devices tree.

After devices are connected to the system, you can perform various operations with them: using remote device control, visualizing devices on maps, monitoring the status of devices and dealing with alarms.

Connecting a security device to the TecomC4 system consists of the following steps:

1. Installing a driver for the device
2. Setting up the device for communication with TecomC4
3. Creating a Devices tree (either by adding device elements manually or by using a wizard)
4. Starting communication with the device

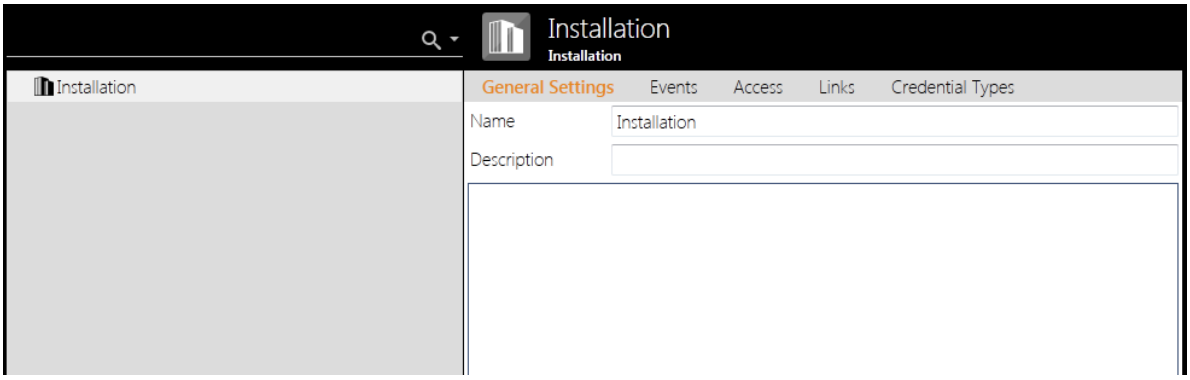
The first step above is covered in the "Installing drivers" chapter on page 24. The remaining steps are covered in this chapter.

Once communication has started, you can view the status of device elements via icons displayed to the right of the elements in the Devices tree and via the colour of elements in the Devices tree. You can also send commands to device elements, such as arming areas and isolating inputs.

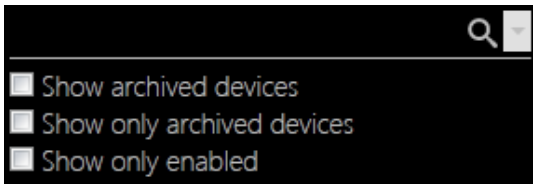
8.1 Devices panel

The Devices panel can be opened by clicking the **Navigation** button and selecting **Devices** from the Administration menu.

The Devices panel looks like this:



The record list shows the Devices tree. The Devices tree can be filtered by typing text in the record filter or by selecting a pre-determined filter option from the filter drop-down menu :



The available filter options are:

- **Show archived devices** – By default, archived devices are not shown in the Devices tree. Clicking this option will show archived devices. See the “Archiving, restoring and deleting nodes” section on page 13 for more information.
- **Show only archived devices** – Only show devices that have been archived. This will allow you to easily find devices to **Delete** or **Restore** from the device’s context menu.
- **Show only enabled** – Only show enabled devices.

The record form has the following tabs:

- General Settings
- Events
- Access
- Links
- Access Levels
- Cameras
- Credential Types

The tabs are described in the following sections.

8.1.1 Devices panel: General settings tab

The *General Settings* tab shows general settings for the selected device. The selected device’s name and description are always shown. Other settings displayed depend on the type of the selected device element. Settings are shown in groups.

Specific settings for Challenger10 bus controller and Challenger10 panel devices are described in the following sections.

8.1.1.1 Challenger10 bus controller settings

A Challenger10 bus controller device has the following settings:

- **Category**
  - **Computer address** – Computer address (account code) of the Challenger10.

- **Communication**
    - **Communication type** – Communication type for communication with the Challenger10 (can only be UDP).
    - **Encryption type** – Encryption type for communication with the Challenger10 (can be None or AES256). If AES256 is selected, the Encryption Key field will appear.
    - **Encryption key** – The encryption key used when AES256 encryption is used.
    - **Network monitoring enabled** – Whether network monitoring is enabled.
    - **Password** – Password for communicating with the Challenger10.
    - **Timeout for response from the device** – Timeout for response from the Challenger10, in HH:MM:SS format.
    - **IP address** – IP address of the Challenger10.
    - **Port** – Port for communicating with the Challenger10.
- **Driver settings**
    - **Enabled** – Whether the device is enabled.
    - **Time zone** – World time zone for the device.

8.1.1.2 Challenger10 panel settings

A Challenger10 panel  device has the following settings:

- **Category**
    - **Persons management** – Whether any user information, including users, credentials, alarm groups, etc. are sent to the Challenger10.
    - **Status querying** – Whether TecomC4 should query the Challenger10's status.
    - **Time synchronization interval** – Time interval for synchronizing time between TecomC4 and the Challenger10, in HH:MM:SS format.
- **Communication**
    - **Query interval** – Time interval for querying the status of the Challenger10 if the Status Querying setting above is enabled, in HH:MM:SS format.
- **Memory management**
    - **Full memory management** – Whether full memory management of the Challenger10 is handled by the driver. If you clear this checkbox, then more fields will appear where you can explicitly set properties such as the minimum and maximum alarm group numbers for the Challenger10.

      This allows you to restrict the ranges of alarm groups, floor groups, area groups and time zones that TecomC4 will configure on the Challenger10. Thus, TecomC4 can be set up to not overwrite non-user programming on the Challenger10.

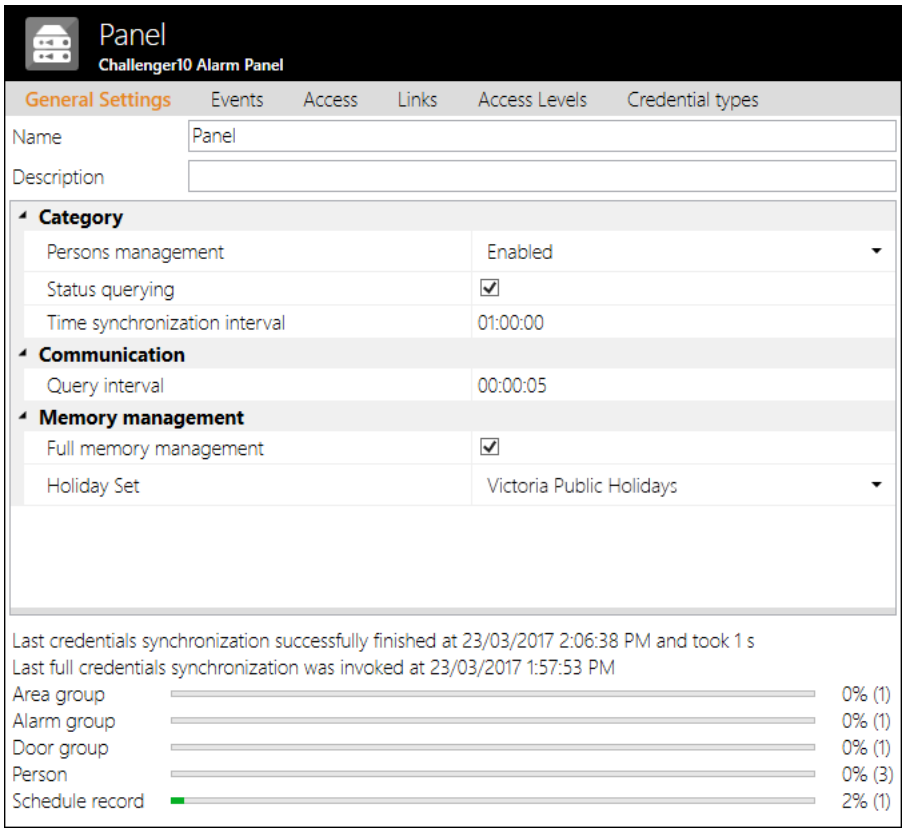
- **Holiday Set** – The holiday group set on the Challenger10. This field only appears if there is more than one holiday group defined. See the “Setting holidays on Challenger10” section on page 22.

Note: Even with full memory management disabled, you cannot create or overwrite the following:

- Area group 1
- User 50
- Alarm groups 1 to 10
- Time zones 26 to 41 (soft time zones)

When a Challenger10 panel device is selected, the *General Settings* tab shows information about the last time that access synchronization occurred at the bottom of the tab.

The bottom of the tab also shows the internal capacity of the Challenger10, in terms of the number of users, area groups etc. For example:



If the Challenger10 is reaching capacity, e.g., the number of alarm groups programmed on the Challenger10 is approaching the maximum allowed, then this may affect your ability to create new access levels.

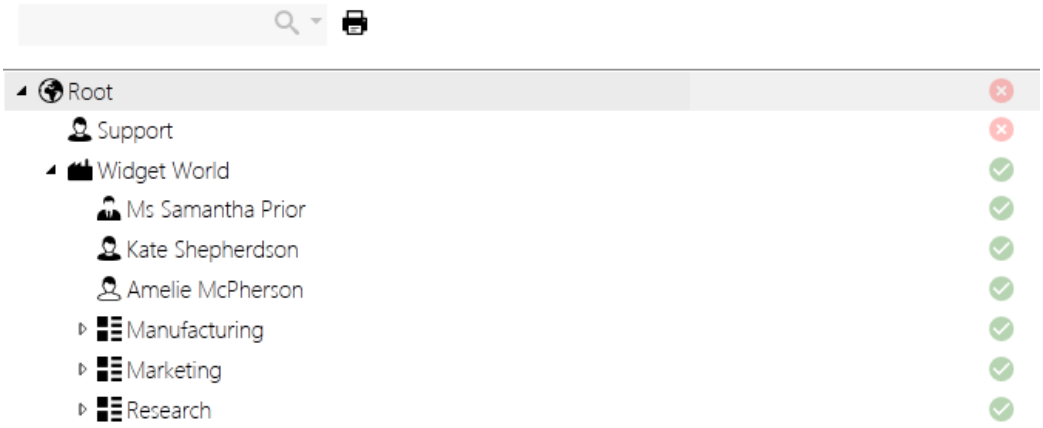
8.1.2 Devices panel: Events tab

The *Events* tab shows all events associated with the selected nodes of the Devices tree. See the “Events” chapter on page 124 for more information about the *Events* tab.

8.1.3 Devices panel: Access tab

The *Access* tab shows the persons in the Persons tree and indicates whether they have access to the selected security device.

For example:



You can click on the coloured circles to change the access for a person or other organisational unit. Right-clicking a coloured circle opens a context menu with the following options:

- **Allow with inheritance** – The organisational unit and its child nodes are allowed access to the selected device.
- **Deny** – The organisational unit and its child nodes are denied access to the selected device.
- **Revoke** – Revoke specific access from the organisational unit and its child nodes. Access reverts to that defined higher in the Persons tree hierarchy or as defined by the organisational unit's access level.

You can also click a coloured circle to cycle through the above options.

The possible colours for the coloured circles are:

- – Access is explicitly allowed for the organisational unit
- – Access is allowed for the organisational unit due to access being determined higher in the Persons tree hierarchy or by the unit's access level
- – Access is explicitly denied for the organisational unit
- – Access is denied for the organisational unit due to access being determined higher in the Persons tree hierarchy or by the unit's access level

If you hover the mouse cursor over a coloured circle, a tooltip will be displayed with a list showing how access is decided for the person. The top entry in the list shows the deciding access permission.

By default, only enabled persons are shown in the Persons tree. You can filter the Persons tree by entering text in the filter above the Persons tree. You can also click the drop-down menu icon in order to also show persons who are not enabled or to only show persons who have access to the selected device:

See the “Form filter” section on page 16 for more information on the form filter.

You can print a report showing a matrix of information about access permissions for the selected parts of the Persons and Devices trees by clicking the **Print** button. See the “Generating access reports” section on page 80 for more information.

Note: It is recommended that you use access levels to define a user’s access instead of defining their access permissions directly on the *Access* tab.

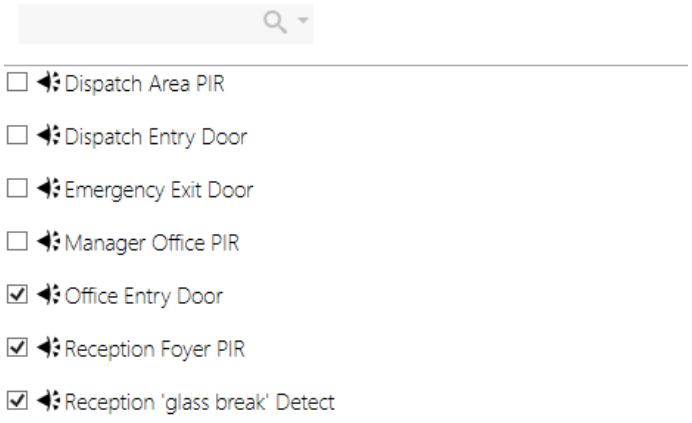
Note: The persons who have access to devices can also be set on the *Access* tab of the Persons panel. See the “Persons panel: Access tab” section on page 97.

8.1.4 Devices panel: Links tab

The *Links* tab shows links between the selected device and other devices in the secure installation. See the “Linking devices” section on page 44 for more information on linking devices.

You can tick the checkbox next to a device to create a link between the devices. For example, you may want to link a secure area with a PIR detector. If an alarm event occurs with the detector, then the linked area will be in alarm condition.

For example:



You can filter the list of devices by entering text in the filter above the devices list. You can also click the drop-down menu icon in order to only show devices that are already linked:

See the “Form filter” section on page 16 for more information on the form filter.

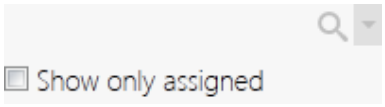
Note: Links created in TecomC4 are not created as links in Challenger10.

8.1.5 Devices panel: Access Levels tab

If the selected device can have an access level associated with it (e.g. an area) and at least one access level has been defined in the TecomC4 system, then the *Access Levels* tab shows the selected device’s associated access levels.

Tick the checkbox next to the access levels that apply to the selected device.

You can filter the list of devices by entering text in the filter above the devices list. You can also click the drop-down menu icon in order to only show devices that are already assigned:



See the “Form filter” section on page 16 for more information on the form filter.

8.1.6 Devices panel: Cameras tab

The *Cameras* tab shows links between the selected device and camera devices in the secure installation. See the “Linking cameras to devices” section on page 45 for more information on linking cameras to devices.

You can tick the checkbox next to a camera to create a link between the camera and the selected device.

You can filter the list of cameras by entering text in the filter above the cameras list. You can also click the drop-down menu icon in order to only show cameras that are already linked:

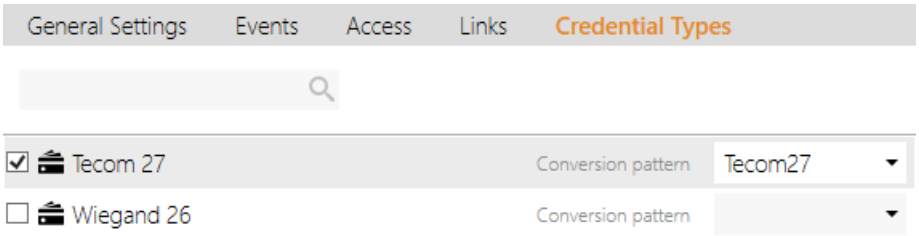
See the “Form filter” section on page 16 for more information on the form filter.

8.1.7 Devices panel: Credential Types tab

The *Credential Types* tab shows which credential types defined in the TecomC4 system can be used with the selected device. You must tick the checkbox next to a credential type to enable it for the selected device.

Credential types must be enabled in the TecomC4 system to be visible on the *Credential Types* tab. See the “Enabling credential types” section on page 64 for instructions on how to enable credential types. You can also select a conversion pattern if necessary.

For example:



See the “Configuring card types on security devices” section on page 65 for more information.

Note: For Challenger10, the required credential types must be enabled for use by selecting the Panel device (as opposed to the bus controller or any other part of the Devices tree).

Note: For the predefined Tecom 27 and Wiegand 26 card types, you must specify the appropriate predefined conversion pattern when you enable the card type for use with the selected device.

8.2 Setting up a device

Device configuration depends on the type of device you are connecting. Challenger10 devices are covered in the next section. For other device types, please refer to the relevant manufacturer documentation.

8.2.1 Setting up a Challenger10

Note: The Challenger10 firmware must be V10-06.12250 or later.

To allow communication between the TecomC4 system and a Challenger10, some information must be configured on the Challenger10, such as the TecomC4 server’s IP address.

You must also gather some information from the Challenger10 for configuring TecomC4.

Challenger10 configuration can be done using TitanCT or LCD RAS. If using TitanCT to program the Challenger10, please refer to the *TitanCT User Manual* for instructions. If using an LCD RAS to program the Challenger10, please refer to the *Challenger Series Installation and Quick Programming Manual* for instructions.

You will need the **IP address** of the TecomC4 server. Contact the site’s network administrator if necessary.

Configure the Challenger10 communications hardware and path settings according to the following table. It is recommended that you use Communications Path 3 for Management Software.

Table 2: Challenger10 communications settings

Challenger10 field	Setting
Communications Hardware (Communications > Hardware)	
Ethernet	Set to Enabled
IP Address Subnet Mask Gateway Address	Set as specified by the site's network administrator
Communications Path (Communications > Path)	
Path main > Format	Set to Computer Event
Path main > Enabled	Set to Enabled
Path main > Location	Set to Onboard
Path main > Slot	Set to Ethernet
Path main > Account code	Set as required (the default is 0001)
Path main > Computer password	Set as required (the default is 0000000000)
Path IP Address > Send to IP Address	Set to the IP address of the TecomC4 server
Path IP Address > Send IP Port Path IP Address > Listen IP Port	Ports must match (the default is 3001)
Path IP Address > IP Mode	Set to UDP/IP
Path Encryption Settings > Type	Set to None or AES256 as required
Path Encryption Settings > Key	Set encryption key if encryption type is AES256

Note: If connecting multiple Challenger10 devices to TecomC4, each device must have a unique port.

Note: The port must not be used by other software such as TitanCT.

8.3 Adding a device tree

A device tree may be added to TecomC4 using the wizard interface (if supported by the device's driver), by adding the device's elements manually, or by importing the device tree configuration from file.

Note: It is recommended that you add a Challenger10 device tree using the wizard method. If you add a Challenger10 device tree manually or by importing from a file, then you will not be able to update TecomC4 with any changes to the Challenger10 configuration by running the **Load configuration from device** option (see the “Updating device configuration” section on page 40). Any changes would have to be made manually.

8.3.1 Adding a device tree via wizard

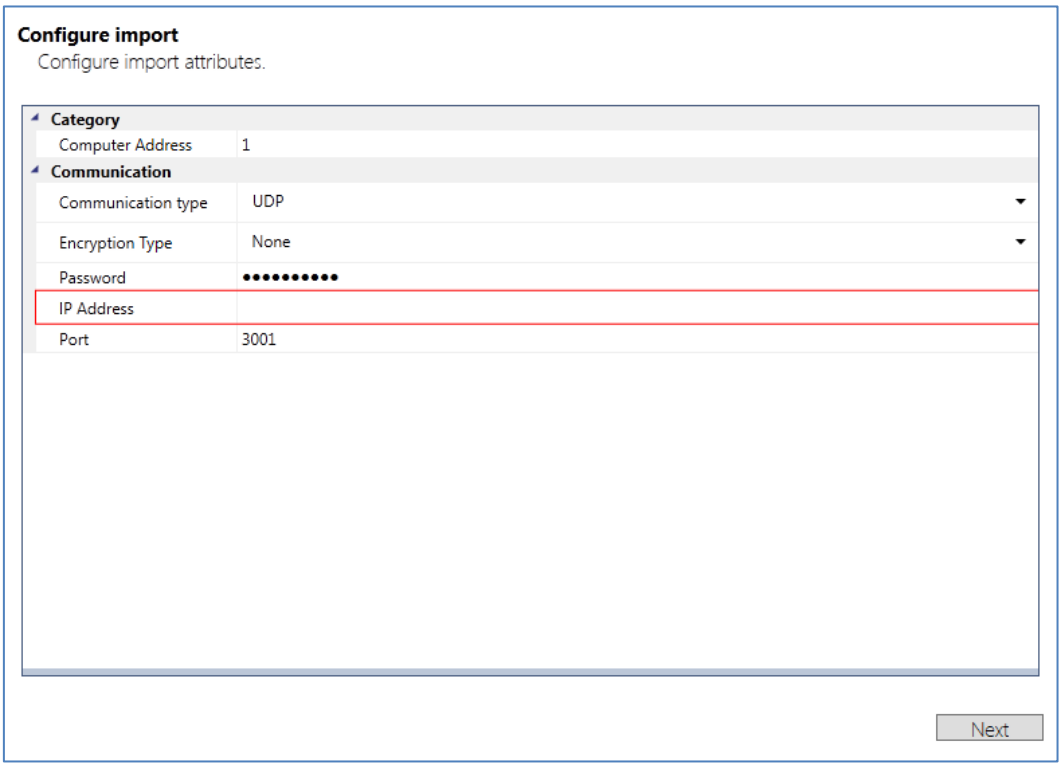
Many devices, such as Challenger10, allow the TecomC4 system to detect elements configured on the device and to load these elements into nodes in the Devices tree.

To add the device and its elements by auto-detection, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Right-click the root Installation node to open its context menu. Select **Add > Add using wizard** and select the name of the required wizard.
3. In the resulting wizard window, enter the properties required to establish communication with the device and click the **Next** button. For specific information on setting up a Challenger10 for communication with TecomC4, see the “Adding a Challenger10” section below.
4. After successful connection to the device, the wizard will display a summary of the elements to be imported. Confirm the changes by clicking the **Next** button.
5. The wizard will show a summary of the import. Click the **Finish** button to complete the import. The device and its elements are now present as nodes in the Devices tree.

8.3.1.1 Adding a Challenger10

For the specific case of adding a Challenger10 device via the wizard, the wizard at step 3 above will look like this:



You must specify the following information in the add device wizard window:

Table 3: Connection settings for Challenger10

TecomC4 setting	Challenger10 setting
Category	
Computer Address	Communication path's account code. The default is 1. (Communications > Path > Path main > Account code)
Communication	
Communication type	Communication type. This must be set to UDP. (Communications > Path > Path IP Address > IP Mode)
Encryption type	Encryption type for communication with the Challenger10. Must be None or AES256. (Communications > Path > Path Encryption Settings > Type)
Encryption key	Encryption key for secure communication with the Challenger10. This field only appears if the Encryption Type above is not set to None. (Communications > Path > Path Encryption Settings > Key)
Password	Computer password. The default is 0000000000. (Communications > Path > Path main > Computer password)
IP address	IP address of the Challenger10. (Communications > Hardware > IP Address)

TecomC4 setting	Challenger10 setting
Port	Port for communication with TecomC4. The default value for Challenger10 is 3001. (Communications > Path > Path IP Address > Send IP Port) (Communications > Path > Path IP Address > Listen IP Port)

8.3.2 Adding a device tree manually

The manual creation of a device tree is only recommended if an existing tree is being extended or if the device's driver does not support device tree auto-detection.

Warning: Do not attempt to add a second Challenger10 panel device under a Challenger10 bus controller. Each Challenger10 panel device must have its own bus controller device.

Note: It is recommended that you add a Challenger10 device tree using the wizard method. If you add a Challenger10 device tree manually, then you will not be able to update TecomC4 with any changes to the Challenger10 configuration by running the **Load configuration from device** option (see the "Updating device configuration" section on page 40). Any changes would have to be made manually.

To add a device and its elements manually, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Right-click the root Installation node to open its context menu. Select **Add** and select the required device.
3. Enter element properties based on the integration manual for the device and continue adding more elements until the device tree is complete. The method of adding an element to the tree depends on the menu displayed upon right-clicking the node under which you wish to add the new element. The system contains controlled hierarchy support; that is, it verifies what type of elements can be created at any given node.

The tree structure should reflect the actual connection of devices including all connected elements.

Note: A responsible person may forget to add some elements configured on the device to the device tree. If there is any activity on this missing element and the device sends the information to the TecomC4 system, a missing device event appears in the event history.

8.3.3 Importing a device tree from file

A device tree can be imported from a CSV file. The CSV file may have been previously exported from TecomC4 (say, on a different TecomC4 server) or created through a third-party application.

A device tree can only be imported to the root Installation node of the Devices tree.

See the “Importing data from a CSV file” section on page 14 for information on importing data from a CSV file.

Note: It is recommended that you add a Challenger10 device tree using the wizard method. If you add a Challenger10 device tree by importing from a file, then you will not be able to update TecomC4 with any changes to the Challenger10 configuration by running the **Load configuration from device** option (see the “Updating device configuration” section on page 40). Any changes would have to be made manually.

8.4 Starting communication with a device

After creating the device tree, the system can show device statuses in real time. To establish communication between the device and the TecomC4 system, it is necessary to start communication with the device. Right-click the device’s bus controller to display its context menu and select the **Commands > Start** menu item.

After communication has been initialised, you will notice the changing colour statuses of the individual nodes in the device tree, which indicate the real statuses of the connected devices.

You can stop communication with the device by right-clicking on the device’s bus controller to display its context menu and selecting the **Commands > Stop** command.

Note: If communication is already started and you click the **Start** command again, then communication will be restarted with the device.

Warning: If there is an error in a device’s configuration, i.e. the device has a configuration error icon, then communication with the device will be stopped. You must correct the configuration error and start communications again.

Warning: Changes made directly to a Four-Door Controller device will require a communications restart to ensure that events from the Four-Door Controller are received by TecomC4.

Note: It is possible to get an event indicating that the bus controller has started even if the Challenger10 is offline, since the event indicates that the Challenger10 driver has started. The online status of a Challenger10 is indicated by the colour of the relevant icons in the Devices tree. See the “Device status colours” section on page 40 for more information on device status colours.

8.5 Device status icons

While working with the Devices tree, you may encounter the following device status icons next to nodes in the tree:

- – Disabled device. The device has been disabled in the TecomC4 system, which means that the device does not communicate.
- – Device configuration error. Some of the device’s properties in TecomC4 are specified incorrectly.

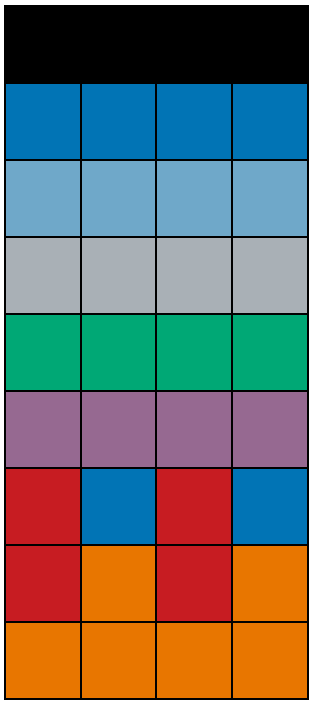
-  – Connection restart is required. This occurs after you make a change in the Devices tree in TecomC4 (i.e., elements added/removed or properties modified).
-  (spinning) – Processing a command. This is displayed after a command is issued for a device until the command has finished processing. It is only visible for commands that take longer to complete, such as communication restart or synchronization of credentials.
-  – Connecting or reconnecting. This occurs while initiating connection to the device.
-  – Network trouble. This occurs when there is a problem with network connection between device and TecomC4.
-  – Synchronizing credentials/access information. This occurs when the sending of access information and credentials to the device is underway.
-  – Synchronization of credentials/access information failed.
-  – Device is archived. See the “Archiving, restoring and deleting nodes” section on page 13.

8.6 Device status colours

In TecomC4, Devices tree nodes may have statuses as indicated by the colour of the icon next to the node name. In the following colour chart, each status is indicated by four colours in succession.

For example, an unknown status is indicated by solid black and an alarm status is indicated by alternating red and blue colour.

The colour statuses for Challenger10 are:



Black – unknown/communications stopped/offline

Blue – normal status/disarmed

Pale blue – processing

Grey – isolated

Green – armed/automation zone on

Violet – activated

Red/Blue – alarm

Red/Orange – tamper

Orange – disconnected

For a full table of possible device colour statuses for all devices, see “Appendix B: Device status colours” section on page 152.

When a device’s status is shown via its colour in the Devices tree, the following priority is used when the device has multiple applicable statuses: isolated, disconnected, tamper.

8.7 Updating device configuration

If you make changes to a device directly, such as configuring a new input on a Challenger10, you can load the updated configuration into TecomC4.

Right-click on the bus controller device to open its context menu. Select **Load configuration from device** to open a window that matches the add device wizard. See the “Adding a device tree via wizard” section on page 35 for information on the wizard. If necessary, you can change the fields for connecting to the device.

Click the **Next** button to show information about any changes that will be loaded into TecomC4. Click the **Next** button to confirm loading the changes. Click the **Finish** button to close the window.

Note: Updating device configuration will only work on Challenger10 if you added the Challenger10 device tree using the wizard method.

Note: If you change the name of a device element directly on a Challenger10, then loading the configuration from the device will change the name of the device element in TecomC4.

Note: If you remove a device element from a Challenger10 directly, then loading the configuration from the device will cause the device element to be archived in TecomC4.

Note: If a device element has been archived in TecomC4, but it still exists on a Challenger10, then loading the configuration from the device will cause the device element to be restored from archive in TecomC4.

Note: If a DGP is added to the Challenger10, then loading the configuration from the Challenger10 will not cause TecomC4 to move inputs and relays from the Challenger10 panel node of the Devices tree to the DGP node. Instead, TecomC4 will archive the original Challenger10 inputs and relays and will either create new inputs and relays under the DGP, or restore them to the DGP from archive if they had been previously archived.

Similarly, if a DGP is removed (depolled) from the Challenger10, then loading the configuration from the Challenger10 will not cause TecomC4 to move the inputs and relays from the DGP node of the Devices tree to the Challenger10 panel node, but will archive the DGP inputs and relays. TecomC4 will either create or restore inputs and relays under the Challenger10 node.

8.8 Controlling devices remotely

After communication with a device has been successfully established, device statuses can be monitored and devices can be controlled remotely. For example, you can remotely arm an area or open a door. The TecomC4 system verifies which commands can be executed on a particular device.

Open the device's context menu by right-clicking it. Select **Commands** and select the required command from the menu. After the command is executed, the device's status is visible through the changing colour of the corresponding node in the Devices tree.

If supported by the device driver, some commands may be greyed out depending on the current context and status of the device, in order to prevent an invalid command from being executed. (For example, it is not possible to arm an area that has already been armed.) This behaviour can be overridden by pressing the SHIFT key, which enables all commands.

Note: It is possible to disable individual device commands for TecomC4 operators. See the "Role permissions" section on page 83.

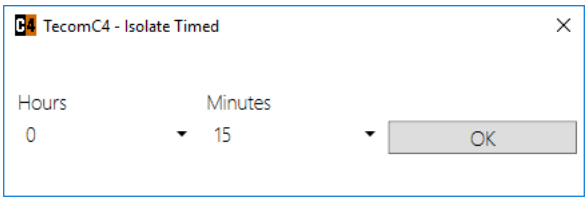
The following section has information on the specific commands that can be sent to Challenger10 devices.

8.8.1 Challenger10 commands

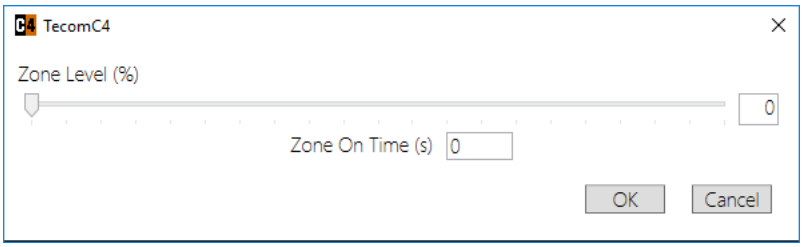
See the “Appendix A: Challenger10 devices and commands” section on page 149 for information on which commands can be sent to which Challenger10 devices.

The commands that can be run on Challenger10 devices are:

- **Arm** – arm the selected area.
- **DeIsolate** – deisolate the selected device (e.g. input).
- **Disable** – disable the selected device (e.g. door).
- **Disarm** – disarm the selected area.
- **Enable** – enable the selected device (e.g. door).
- **Isolate** – isolate the selected device (e.g. input).
- **Isolate Timed** – isolate the selected device (e.g. input) for a specified time. A new window will open in which you can specify the isolate time in hours and minutes. Click the **OK** button to send the Isolate Timed command to the device.

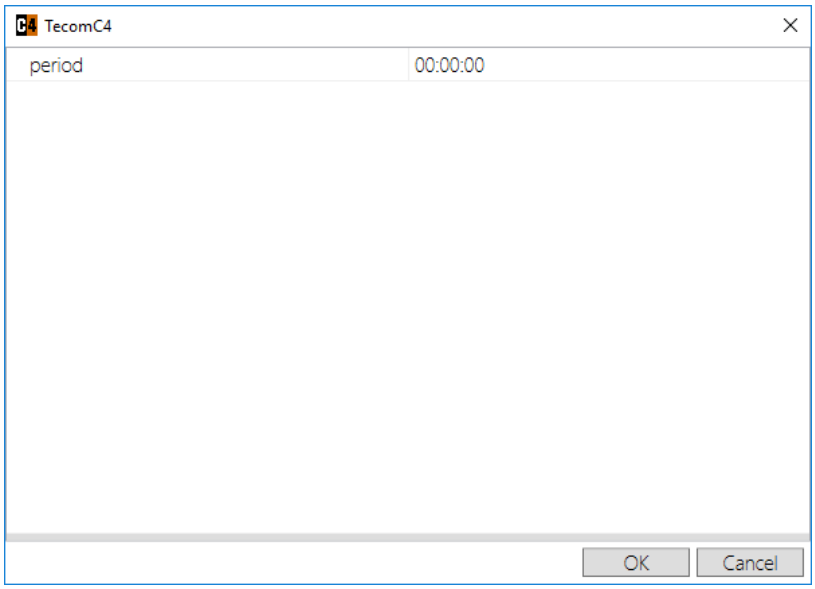


- **Level** – set the level for the selected automation zone. A new window will open in which you can set the **Zone Level** percentage and the **Zone On Time** in seconds. Click the **OK** button to send the Level command to the automation zone.



- **Lock** – lock the selected door.
- **Off** – switch off the selected device (e.g. output).
- **On** – switch on the selected device (e.g. output).
- **Open** – open the selected device (e.g. door).

- **Open Timed** – open the selected door for a specified time. A new window will open in which you can specify the period of time the door will be opened, in HH:MM:SS format. Click the **OK** button to send the Open Timed command to the door.



- **Reset** – reset the selected input.
- **Send All Credentials** – send all credentials and access information to the selected Challenger10 panel device. This command deletes all existing user-related information on the Challenger10. See the “Sending credentials and access information to devices” section on page below.
- **Send Panel Access Changes** – send all changes to access information to the selected Challenger10 panel device. See the “Sending credentials and access information to devices” section on page below.
- **Start** – start communication with the selected Challenger10 bus controller. See the “Starting communication with a device” section on page 38.
- **Stop** – stop communication with the selected Challenger10 bus controller. See the “Starting communication with a device” section on page 38.
- **Trigger** – trigger the selected activation zone.
- **Unlock** – unlock the selected device (e.g. door).

8.9 Sending credentials and access information to devices

Upon first setting up a TecomC4 system, including users, access and credentials, you should run the **Send All Credentials** command to send the information to the Challenger10. Right-click the Challenger10 panel device in the Devices tree to open its context menu and select **Commands > Send All Credentials**.

Warning: Running the **Send All Credentials** command will delete all existing user-related information on the Challenger10 that TecomC4 has access to, including users, alarm groups, door groups, etc.

If the **Full Memory Management** checkbox is ticked on the *General Settings* tab for the Challenger10 panel device in the Devices tree, then all user-related information will be deleted. If the **Full Memory Management** checkbox is cleared, then some user-related information may be reserved from deletion. See the “Challenger10 panel settings” section on page 28 for more information.

TecomC4 then sends all of its user information to the panel. This ensures that the user information on the Challenger10 is synchronized with TecomC4.

Warning: If the **Full Memory Management** checkbox is not ticked on the *General Settings* tab for the Challenger10 panel device in the Devices tree, then the **Send All Credentials** command could take a very long time to run, since all alarm groups, door groups, etc. are individually deleted from the Challenger10.

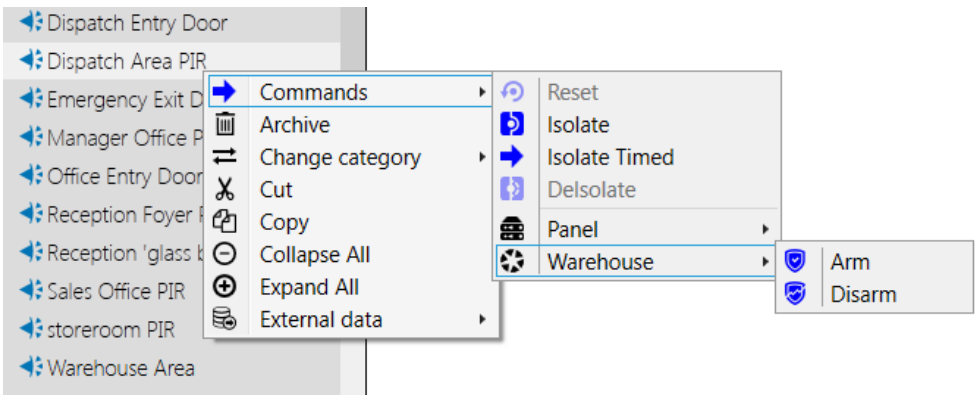
Note: Holidays that are set for the Challenger10 are sent when you run the **Send All Credentials** command. See the “Defining holidays” chapter on page 21 for more information on holidays.

Subsequent changes to users, credentials and access can be sent to all connected Challenger10 panels by responding to the access synchronization request in the information bar when required. See the “Sending access information to devices” section on page 109.

You can send access changes to an individual Challenger10 by running the **Send Panel Access Changes** command. Right-click the Challenger10 panel device in the Devices tree to open its context menu and select **Commands > Send Panel Access Changes**.

8.10 Linking devices

You can link devices so that commands can be run on linked devices. For example, you may want to link a secure area with a PIR detector. You can then access commands for the linked area from the context menu of the detector:



In addition, if an alarm event occurs with the detector, then the linked area will be in alarm condition.

The *Links* tab shows links between the selected device and other devices in the secure installation. You can tick the checkbox next to a device to create a link between the devices.

Note: Links created in TecomC4 are not created as links in Challenger10.

Note: If areas and inputs are already linked in a Challenger10, then the linkage information is loaded from the Challenger10 into TecomC4 when the configuration is loaded.

8.11 Linking cameras to devices

Since alarm conditions must be investigated and resolved, it can be helpful to link devices, such as inputs, with cameras that have an appropriate view of the device. This will allow you to open a live camera feed directly from the linked device, without having to search for the camera that could have seen the incident.

The *Cameras* tab shows links between the selected device and cameras in the secure installation. You can tick the checkbox next to a camera to create a link between the device and the camera. Multiple cameras can be linked to a device.

If any event, such as an alarm, occurs with the device, you can right-click the event to open its context menu and click the **Show recorded video on** menu item to play back video recording from linked cameras.

You can set the time before an event that playback of the video recording should start. Select the camera device in the Devices tree of the Devices panel. On the General Settings tab, set the **Record Playback Delay** value. Playback of recordings from that camera will start from the set time before an event.

9 Configuring regions

Regions can be used to restrict which security devices an operator can see and interact with. You can create a hierarchy of regions and add devices to regions.

A region can contain elements from multiple security devices. A region can cover an arbitrary geographical area, such as a state, city, building or floor.

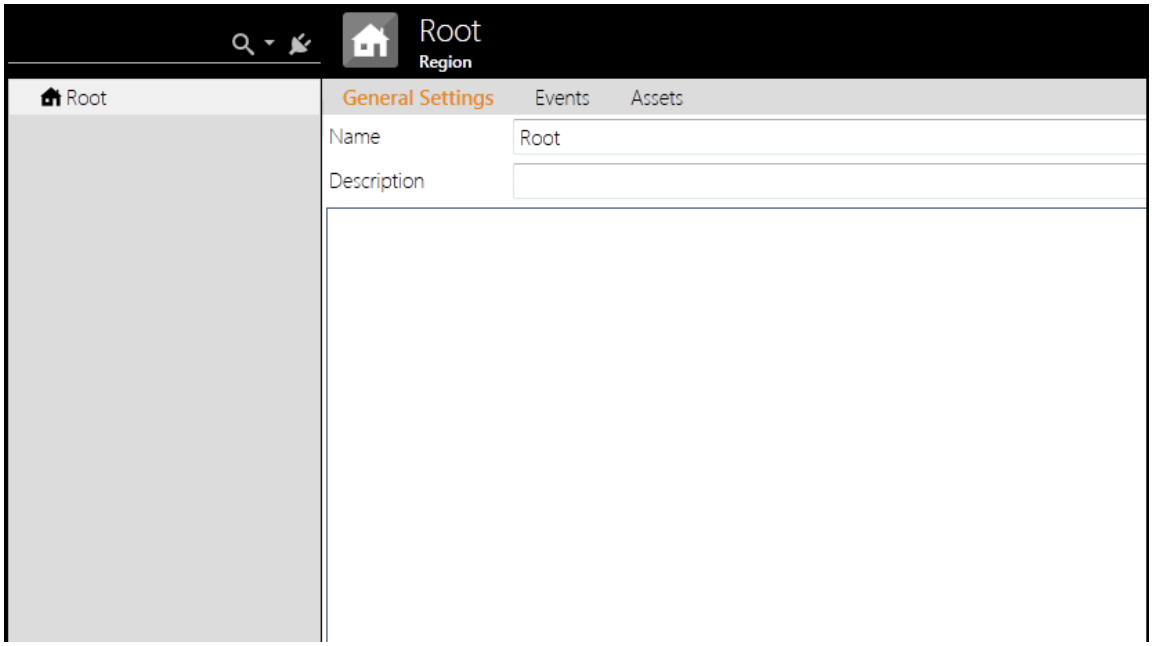
It is also possible for TecomC4 to count the number of persons in a region.

Note: Regions in TecomC4 are unrelated to Challenger10 regions.

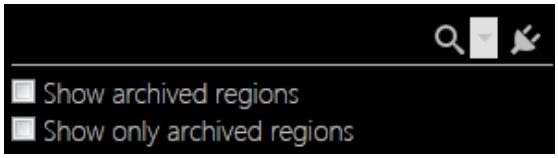
9.1 Regions panel

The Regions panel can be opened by clicking the **Navigation** button and selecting **Regions** from the Administration menu.

The Regions panel looks like this:



The record list shows the Regions tree. The Regions tree can be filtered by typing text in the record filter or by selecting a pre-determined filter option from the filter drop-down menu  :



The filter options available are:

- **Show archived regions** – by default, archived regions are not shown in the Regions tree. Clicking this option will show archived regions. See the “Archiving, restoring and deleting nodes” section on page 13.

- **Show only archived regions** – show only regions that have been archived. This will allow you to easily find regions to delete or restore from the region's right-click context menu.

The record form has the following tabs:

- General Settings
- Events
- Assets
- Persons Present

The tabs are described in the following sections.

9.1.1 Regions panel: General Settings tab

The *General Settings* tab shows the following attributes of the currently selected node:

- **Name** – region's name
- **Description** – region's description

9.1.2 Regions panel: Events tab

The *Events* tab shows all events associated with the selected nodes of the Regions tree. See the "Events" chapter on page 124 for more information about the *Events* tab.

9.1.3 Regions panel: Assets tab

The *Assets* tab shows the region's assets. See the "Adding region assets" section on page 49 for more information on assets.

9.1.4 Regions: Persons Present tab

The *Persons Present* tab only appears if the **Counting Persons in Regions** extension is enabled. See the "Counting persons in regions" section on page 50 for more information.

The *Persons Present* tab shows a list of persons present in the selected regions, with the following columns:

- **Time** – the time the person entered the selected region
- **Person** – the person who is in the selected region
- **Region** – the selected region
- **Door** – the door that the person used to enter the selected region

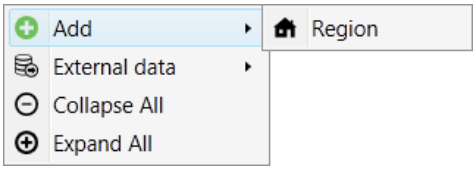
9.2 Creating a region hierarchy

You can add a region hierarchy manually or by importing from file.

9.2.1 Creating a region hierarchy manually

To create a region hierarchy, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Regions** to open the Regions panel.
2. Right-click the Root node in the Regions tree on the left to show its context menu. Select **Add > Region**.



   Give the new region a name and an optional description on the *General Settings* tab.

3. Continue adding regions to the Regions tree, creating a hierarchy of regions representing the areas of the secure installation (such as states, cities, buildings, floors and rooms).

9.2.2 Importing regions from a file

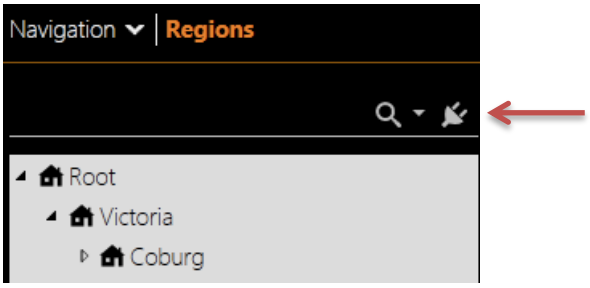
A regions tree can be imported from a CSV file. The CSV file may have been previously exported from TecomC4 (say, on a different TecomC4 server) or created through a third-party application.

See the “Importing data from a CSV file” section on page 14 for information on importing data from a CSV file.

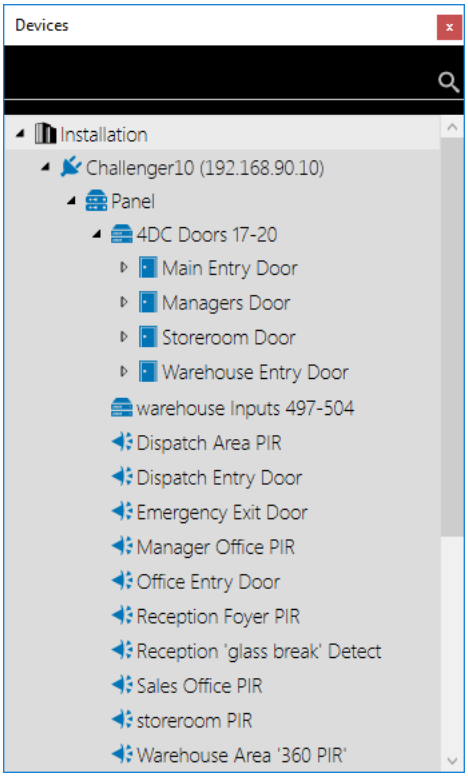
9.3 Adding devices to a region

To add devices to a region, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Regions** to open the Regions panel.
2. Click the **Devices** icon next to the record filter to display the Devices tree:



The Devices tree will open in a new window. For example:



You can filter the Devices tree by entering text in the filter at the top of the window.

3. Locate the required device in the Devices tree and drag the device to the desired region in the Regions tree and drop it. Each device can be placed in each region only once.

9.4 Adding region assets

Each region can have assets assigned to it on the *Assets* tab. Click the **Add** button to add one of the following assets:

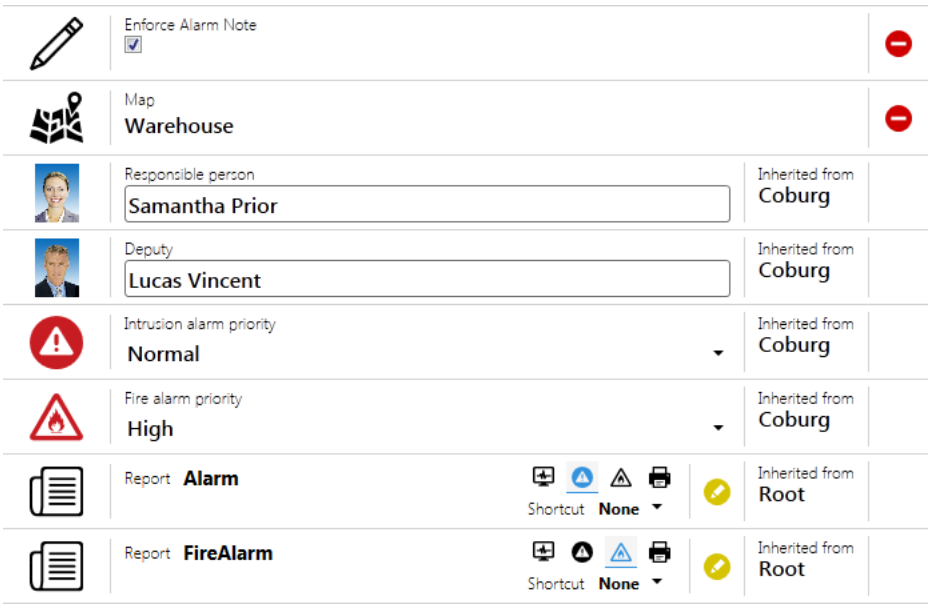
- **Responsible person** – select a responsible person for the region from the Persons tree displayed in a new window
- **Deputy** – select a deputy person responsible for the region from the Persons tree displayed in a new window
- **Intrusion alarm priority** – change the priority for alarm events in the region
- **Fire alarm priority** – change the priority for fire alarm events in the region
- **Enforce Alarm Note** – tick this option to require that a note be added after an alarm is resolved in the region
- **Map** – select a map for the region from the Maps tree displayed in a new window

Adding intrusion alarm and fire alarm priorities mean that alarms from one region can have a higher priority than alarms from another region. Alarms are sorted on the

Monitor panel according to their priority. Alarms and Fire Alarms can have the following priorities:

- High
- Normal
- Low
- None

Assets are inherited down the Regions tree, but you can override an asset at any level of the tree. For example:



An asset can be removed by clicking the **Remove** button.

In addition to the assets that can be added at any node of the Regions tree, there are two assets that are defined at the Root of the Regions tree and are inherited down the tree. These assets determine the layout of the reports available when an operator responds to an alarm or fire alarm from the Monitor panel. You can click the **View** button to open a window with a preview of the report format.

Warning: Do not remove the report assets from the Root of the Regions tree unless you are certain you will not need them. They cannot be added again.

9.5 Counting persons in regions

The TecomC4 system can count the number of persons in regions. An operator can quickly see where a specific user is currently located or how many users are in a specific region.

The counting is performed on the basis of credential usage when entering and leaving a region. Therefore, you must assign entry and exit readers for the region.

The person counting functionality must first be enabled in the TecomC4 system settings:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Counting Persons In Regions** extension.
    - If you expand the extension details by pressing the expand button, you can also enable the **Soft Antipassback Enabled** option, which triggers a warning event in the case of repeated entry of a person into the same region.

To enable the counting of persons in a specific region, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Regions** to open the Regions panel.
2. If you have not done so already, create the region hierarchy and add devices to the Regions tree, as described in the “Creating a region hierarchy” section on page 48. Add reader devices as required and set the Direction to one of the following values:
    - **Ingress** – for incrementing the number of persons in the region
    - **Egress** – for decrementing the number of persons in the region
    - **None** – for no change in the number of persons in the region

    Each device can be placed in each region only once.
3. The reader direction must be set for each reader depending on whether it is used for entry to the region or departure from it. Select the reader in the Regions tree and on the *General Settings* tab set the **Direction** property to the required value.

Note: Counting persons in regions is TecomC4 functionality that may or may not reflect the device settings for antipassback or other properties.

Note: If using a Four-Door Controller, do not use regions programmed in the Four-Door Controller. Also, do not use both the ingress and egress readers on the same door; instead, use separate doors for the ingress and egress readers.

Note: Each person can normally be present only once in each region. The exception is when a reader provides entry to several regions at the same time. The moment the person exits one of these regions, their presence will be automatically terminated in the other regions too.

Enabling the **Counting Persons in Regions** option adds the *Persons Present* tab to the Persons and Regions panels.

9.5.1 Persons panel

On the Persons panel, the *Persons Present* tab shows the selected persons names, the regions they are in, their times of entry and their doors of entry.

To remove a person from a region, click the **Remove** button. This operation will also reset the person's antipassback flag on the device (if that operation is supported by the device's driver) and the person can enter the region again.

Persons who are present in a region are indicated by the **person present** status icon next to their name in the Persons tree. Enabling the **Show only persons on premises** filter option above the Persons tree will only display the persons currently present in one of the regions of the TecomC4 system:

9.5.2 Regions panel

On the Regions panel, the *Persons Present* tab shows the selected regions, persons who are present in those regions, their times of entry and their doors of entry.

To remove a person from a region, click the **Remove** button. This operation will also reset the person's antipassback flag on the device (if that operation is supported by the device's driver) and the person can enter the region again.

Regions that have persons present in them are indicated by a **person count** status icon next to their name in the Regions tree. The icon shows the number of persons present in the region.

10 Configuring visualization

Visualization graphically represents devices in the TecomC4 system in terms of their physical location and layout.

The main visualization element is a map representing individual parts of the installation (such as a country, city, area, building, floor, or floorplan). A map can be created from any image, so you could also have a visual menu or a photo of a building.

Devices visualized on maps can subsequently be controlled by operators from the Monitor panel. See the “Monitoring the system” chapter on page 111 for more information.

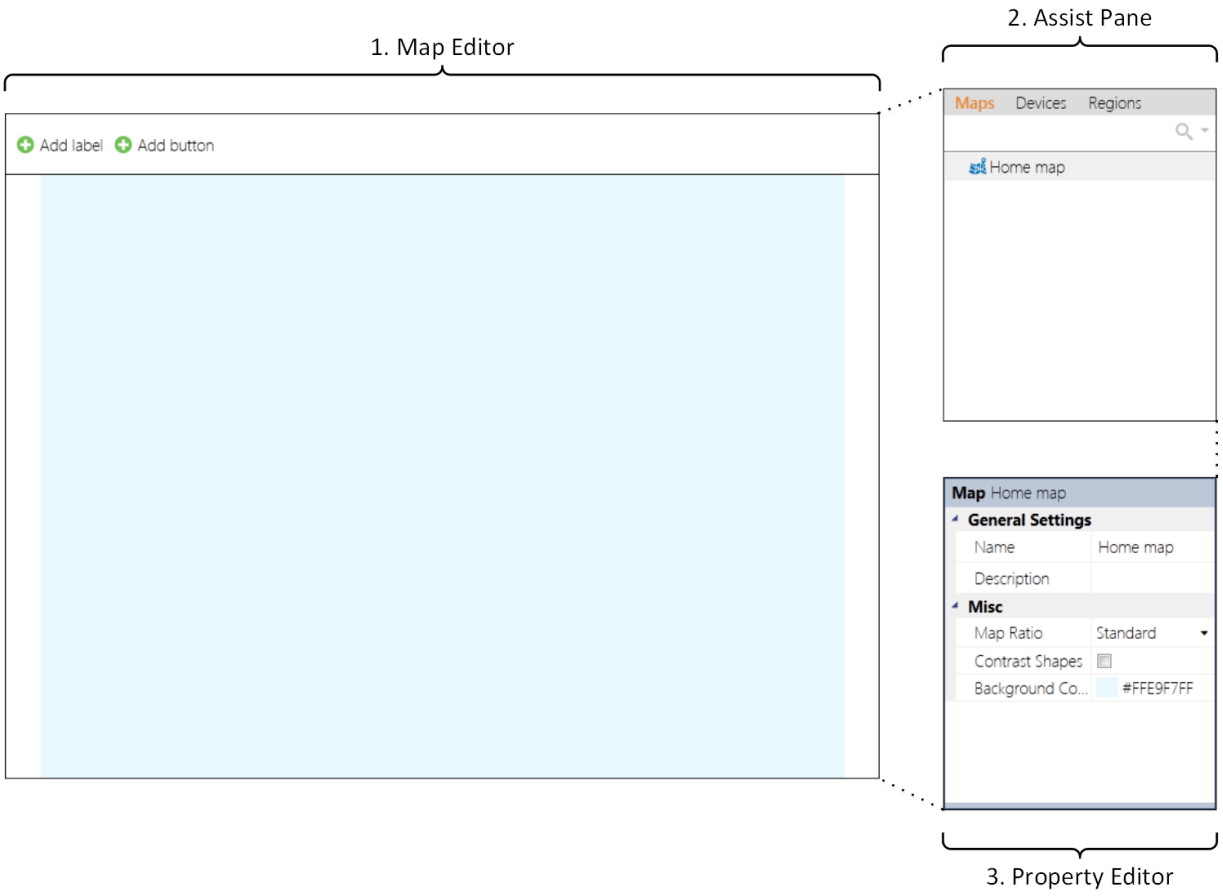
There is one predefined blank map in the system called the **Home map**.

You can create and edit maps, and add device elements to maps using the Designer panel.

10.1 Designer panel

Open the Designer panel by clicking the **Navigation** button and selecting **Designer** from the Visualization menu.

Figure 4: Elements of the Designer panel



The Designer panel consists of three main elements, numbered in the figure above:

- **Map editor** – the main part of the Designer panel, where map images can be added and map objects can be added and edited.
- **Assist pane** – appears in the top right corner of the Designer panel, containing trees for easily adding objects to maps.
- **Property editor** – appears in the bottom right corner of the Designer panel, containing editable properties of the currently selected map or map object.

The three elements are described in the following sections.

10.1.1 Map editor

The map editor is the main section of the Designer panel. From here, you can add map images in vector (AutoCAD) or raster image format (.jpg, .gif, etc.). See the “Adding a map image” section on page 56 for information on how to add a map image.

You can also add map objects to the map, including devices. See the “Adding map objects” section on page 56.

10.1.1.1 Map editor context menu

When you right-click the coloured background of the map editor, the following context menu appears:

- **Add shape**:
  - **Label** – add a label to the map. A label is designed for adding a text description to other objects on the map. Press CTRL+Enter to finish editing the label text.
  - **Button** – add a button to the map. You can use the button to trigger defined commands directly from the map.
- **Add AutoCAD Map** – add a map image with vector graphics in the AutoCAD format (with .dwfx file extension). Refer to your AutoCAD manual for information on how to export a .dwfx file.
- **Add Image Map** – add a map image with raster graphics in several standard formats (.jpg, .jpeg, .png, .gif or .bmp extensions).
- **Select All** – select all objects on the map.
- **Delete map** – remove the map image.

10.1.2 Assist pane

The Designer panel contains an assist pane in the top right corner with the following tabs:

- **Maps** – shows the tree of maps in the system. See the “Creating a map tree” section on page 55 for instructions on adding maps to the tree.

- **Devices** – shows the tree of devices in the system that can be visualized. See the “Adding devices” section on page 56 for instructions on adding devices from the tree to the map.
- **Regions** – shows the tree of regions in the system, with devices that can be visualized. See the “Adding devices” section on page 56 for instructions on adding devices from the tree to the map.

10.1.3 Property editor

Underneath the assist pane, there is the property editor of the currently selected object on the map. If no object is selected, the properties of the current map are shown.

10.2 Creating a map tree

An operator’s visualization may be divided across more than one map, with individual maps representing different geographical areas (such as cities, buildings, floors and rooms).

You can have an arbitrary hierarchy of maps and each map can be any image. For example, you could have a menu of buttons on the Home map, linking to photos of all the managed buildings. Under each building photo “map”, you could have floor plans of each floor of each building.

To create a map tree, follow these steps:

1. In the Assist pane, select the *Maps* tab. Right-click the Home map to display its context menu. Select **Add > Map** to add a new map. In the property editor for the new map, enter a name and optional description for the map.
2. Add more maps to the tree as desired.

If required, you can move maps around the Maps tree on the *Maps* tab by dragging and dropping.

You can remove a map from the map tree by right-clicking the map in the *Maps* tab of the assist pane and selecting the **Archive** menu item.

By clicking the drop-down menu button next to the filter text box above the Maps tree on the *Maps* tab, you can activate the following filter options in order to see archived maps:

- **Show archived maps** – show all maps
- **Show only archived maps** – show only archived maps

In order to preserve the structure of the maps tree, it is only possible to restore a map if its parent map is not archived.

To restore a map, access the map’s context menu by right-clicking on it and select the **Restore** menu item. The restored map is inserted at its original place in the tree. You can also restore an archived map including its child maps by selecting the **Restore with children** menu item.

To permanently delete an archived map, access the map's context menu by right-clicking it and select the **Delete** menu item. A dialog box will be shown asking you to confirm the deletion.

10.3 Adding a map image

To add a map image, right-click in the map editor to display the context menu and select either of the **Add AutoCAD Map** or **Add Image Map** commands. A file open dialog window will appear from which you can select the desired image file.

10.4 Editing map properties

The following properties can be set for map images in the property editor:

- **General Settings:**
  - **Name** – name of the map.
  - **Description** – a meaningful description of the map (optional).
- **Misc**:
  - **Map Ratio** – specifies the map aspect ratio. If the field is set to "None", then the map is shown full size and an "Eagle eye window" appears, from which you can scroll the current view of the map.
  - **Contrast Shapes** – specifies if visualization shapes on the map should have emphasised edges. If selected, the **Colour of Contrast Shapes** property will appear, from which you can specify the highlight colour.
  - **Background Colour** – background colour of the map.

10.5 Adding map objects

You can add a variety of map objects to maps to aid visualization: devices, buttons, labels and map links.

10.5.1 Adding devices

To add a device to a map, follow these steps:

1. In the assist pane, open the *Maps* tab and select the desired map from the Maps tree. The map will appear in the map editor.
2. In the assist pane, open the *Devices* tab or the *Regions* tab and select a device from the Devices tree or Regions tree to be visualized on the map.
3. Drag and drop the device to the required position on the map in the map editor. This creates the device object on the map.
4. You can drag the corners of the object to change its size and use the rotation control to rotate the object.

Next to the filter above the Devices tree on the *Devices* tab or the Regions tree on the *Regions* tab, you can activate the following filters for more efficient configuration:

- **Show only not visualized** – only show those devices that are not visualized on any map in the system.
- **Show only not visualized on current map** – only show those devices that are not visualized on the current map.

See the “Editing map objects” section on page 57 for information on editing device objects.

10.5.2 Adding buttons and labels

You can add a label to the map by clicking the **Add label** button in the map editor. A label is designed for adding a text description to other objects on the map. Press CTRL+Enter to finish editing the label text. You can drag the corners of the label to change its size and use the rotation control to rotate the object.

You can add a button to the map by clicking the **Add button** button in the map editor. You can drag the corners of the label to change its size and use the rotation control to rotate the button. You can edit the button object’s properties in the property editor so that defined commands are triggered when the button is pressed on the Monitor panel.

See the “Editing map objects” section on page 57 for information on editing button and label objects.

10.5.3 Adding map links

You can add map links to a map so that you can quickly switch maps in the Monitor panel.

In the assist pane, open the *Maps* tab to view the Maps tree. Drag the target map to the map editor, creating a map link object on the map. You can drag the corners of the label to change its size and use the rotation control to rotate the map link.

See the “Editing map objects” section on page 57 for information on editing map link objects.

Note: A single map can contain any number of links to other maps, so you can create a hierarchy of maps reflecting the layout of the secure installation and its devices. You can also add a map link several times. The system does not allow the insertion of a map link pointing to itself.

10.6 Editing map objects

Map objects (devices, buttons, labels and map links) can be edited in any one of three ways:

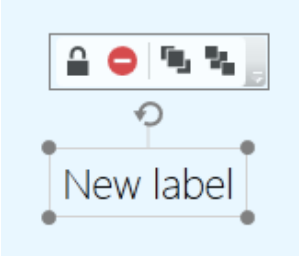
- **Map object control** – appears above the object when you select it
- **Map object context menu** – appears when you right-click on the object

- **Map object properties** – appear in the property editor when you select an object

The three methods are described in the following subsections.

10.6.1 Map object control

If you click on a map object in the map editor, such as a button, label or device, then a map object edit control is shown above the selected object:



You can perform various actions from the map object edit control:

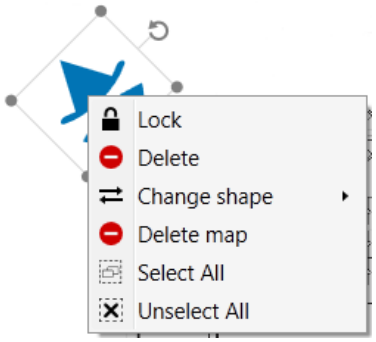
- Change the object's size by moving the sizing handles at the corners of the object's frame.
- Change the rotation of the object by clicking the rotate control.
- Lock the object to prevent further changes with the lock button. A small lock icon will appear in the upper right corner of the map object.
- Delete the object with the delete button.
- Bring the object to the front with respect to other objects on the map with the "bring to front" button.
- Send the object to the back with respect to other objects on the map with the map with the "send to back" button.

If you select multiple objects on the map, you will also see the following additional options in the map object edit control:

- – Align all selected objects to the left with respect to the first selected object.
- – Align all selected objects to the horizontal centre with respect to the first selected object.
- – Align all selected objects to the right with respect to the first selected object.
- – Align all selected objects to the top with respect to the first selected object.
- – Align all selected objects to the vertical centre with respect to the first selected object.
- – Align all selected objects to the right with respect to the first selected object.

10.6.2 Map object context menu

You can display a context menu for a map object by right-clicking it:



You can perform the following actions from the map object context menu, depending on the object selected:

- **Lock** – lock the object to prevent further changes. A small lock icon will appear in the upper right corner of the map object.
- **Lock** – indicates that the object is locked. Select this menu item to unlock the object and allow changes.
- **Delete** – remove the object from the map (this command does not remove the object itself from the TecomC4 system).
- **Change shape** – change the shape of the object. Depending on the object's current shape, you may see some of the following options:
  - **Button** – change object to a button.
  - **Ellipse** – change object to an ellipse.
  - **Icon** – change object to its default icon (e.g. change an area rectangle to an area icon).
  - **Label** – change object to a label.
  - **Polygon** – change object to a polygon. Click points on the map to be the points of the polygon. When you double-click the last point TecomC4 will complete the polygon. The extents of a polygon object are the entire map.
  - **Rectangle** – change object to a rectangle (this is the default shape for areas and map links).
- **Select All** – select all objects on the map.
- **Select <object>** – select specified object. If objects overlap on the map, you can use this menu item to select the desired object.
- **Unselect All** – unselect all objects on the map.

Note: TecomC4 remembers the shape of map objects. For example, if you have added an input to a map and changed its shape to a rectangle, all other inputs added to a map will be created using the rectangle shape until you change it again. These settings are preserved for each object type.

10.6.3 Map object properties

The following properties can be set for map objects, depending on the type of object selected:

- **General Settings:**
  - **X** – horizontal position of the object from the left.
  - **Y** – vertical position of the object from the top.
  - **Width** – width of the object.
  - **Height** – height of the object.
  - **Angle** – rotation angle of the object.
  - **Opacity** – opacity of the object from 0 (transparent) to 1 (opaque).
- **Misc**:
  - **Background Colour** – background colour of the object.
  - **Commands** – commands can be assigned to be executed when you click the map object in the Monitor panel.

    Click the **command editor**  button to display the command editor window where you can enter the commands to be executed. See the “Command editor” section on page 61 for a description of the command editor.

    The list of available commands will vary according to what actions can be performed on the device element. When you click the map object in the Monitor panel, only those commands which are valid according to the status of the device element are performed.
  - **Fill Colour** – fill colour for objects that have an ellipse, polygon or rectangle shape.
  - **Font** – font for text.
  - **Stroke Colour** – colour of the object’s border.
  - **Stroke Visibility** – whether the object’s border is visible.
  - **Text** – text contents.
  - **Text Colour** – colour of text.
- **Status Propagation:**
  - **Alarm Propagation** – an alarm from the device will be displayed on the map.
  - **Failure Propagation** – a fault from the device will be displayed on the map.

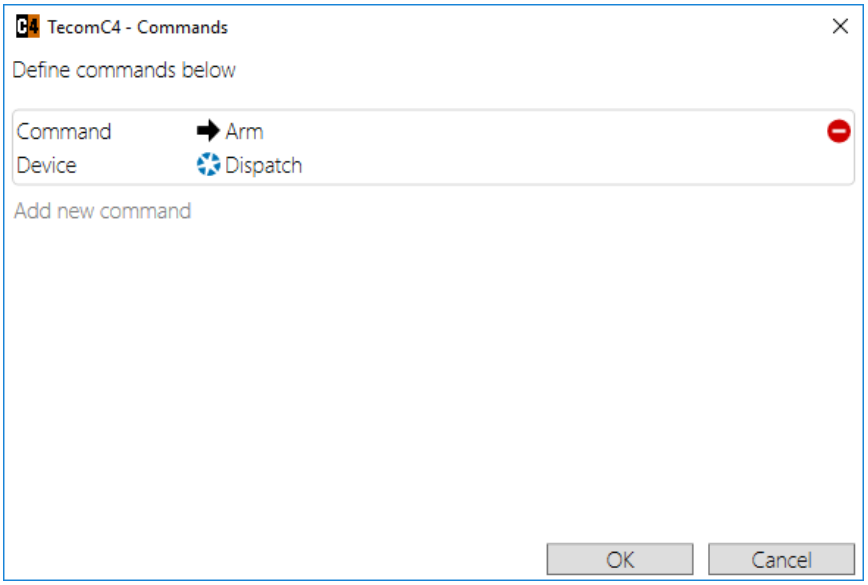
10.7 Command editor

If a map object is selected and you click on the **display command editor** ... button in the **Commands** property of the object's property editor, then the command editor will be displayed in a new window.

Click the **Add new command** button to add a new command. A new window will appear showing the valid commands for the selected object. The valid commands for device objects are the commands that can be sent to the device. For example, the valid commands for an input device object are Isolate, DeIsolate and Reset. For button and label objects there is a larger set of commands that can be run, such as sending a command to any device or changing the view to a different map.

Select the command to be run and click the **OK** button.

The command editor will show the command and the object that the command relates to. For example:



You can add additional commands by selecting the **Add new command** button again. Delete a command by clicking the **Delete** button next to the command.

The following are some examples of objects running commands:

- Click on an area object to arm the area
- Click on a door object to open the door
- Click on a map link to change to a specified map
- Click on a button to open all doors
- Click on a button to show camera footage from a camera on an operator's TecomC4 client.

11 Configuring user credentials

User credentials such as cards and PIN codes allow a person to access parts of the secure installation.

Configuring user credentials involves the following steps:

1. Configuring credential types (i.e. card types)
2. Configuring validation rules for credentials
3. Creating card decks (if required) and adding cards to decks

The steps are described in the following sections.

11.1 Configuring credential types

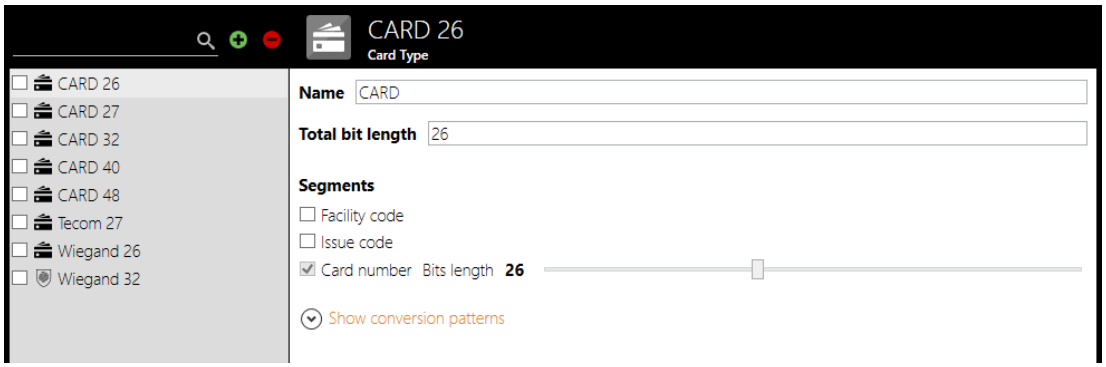
The TecomC4 system allows the use of various types of credentials (cards and PIN codes). It is recommended that you only enable the types of cards that will actually be used in the secure installation. This provides better transparency of the security system and prevents issuing an unsupported card type to a person by mistake.

Credential types can be configured on the Credential Types panel.

11.1.1 Credential Types panel

The Credential Types panel can be opened by clicking the **Navigation** button and selecting **Credential Types** from the Settings menu.

The Credential Types panel looks like this:



The record list shows a list of credential types.

The list of credential types can be filtered by typing text in the record filter.

The record form shows details for the selected credential type. The following fields are shown on the form:

- **Name** – a name for the credential type
- **Total bit length** – the total bit length of the credential type. This field automatically updates as you increase the bit lengths of the credential type's segments.

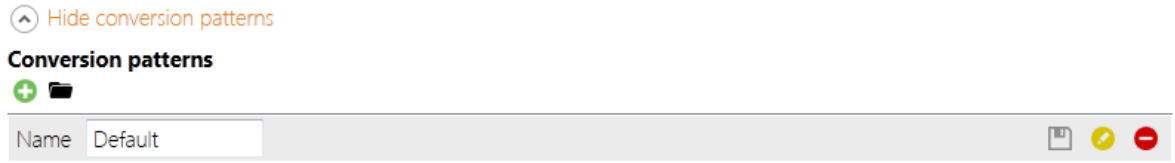
- **Segments:**
  - **Facility code** – bit length for the credential type's facility code
  - **Issue code** – bit length for the credential type's issue code
  - **Card number** – bit length for the credential type's card number
  - You can click the down arrow next to the **Show conversion patterns** text to create or edit conversion patterns for the credential type. See the "Conversion patterns" section below.

The name displayed for the credential type in the list on the left is a combination of the credential type's name field and its total bit length field.

Note: Once a credential type has been assigned to a person in the TecomC4 system, its bit lengths cannot be changed.

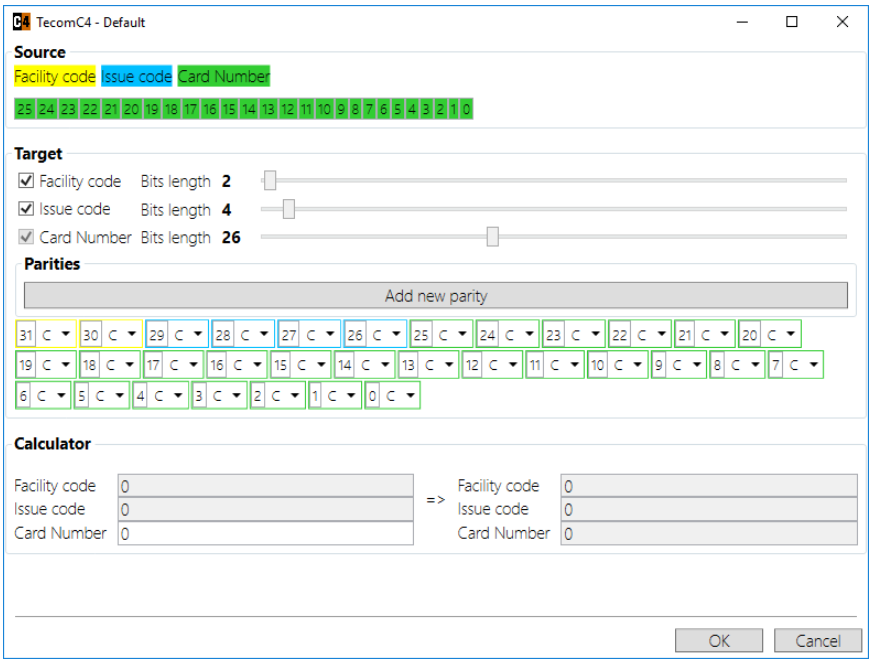
11.1.1.1 Conversion patterns

When you click the down arrow next to the **Show conversion patterns** text in the Credential Types form, you will see a list of conversion patterns for the credential type.



Click the **Add** button to add a new conversion pattern or load a conversion pattern from file by clicking the **Open from file** button, which opens a file open dialog window. Conversion pattern files have the filename extension *.cfc*.

Once you have created a new conversion pattern or opened one from file, you can click on the **Edit** button to open a new window where you can edit the conversion pattern:



Click the **Okay** button when you have finished editing the conversion pattern.

Click the **Save** button to open a File Save dialog window to save the conversion pattern to file.

Click the **Delete** button to delete the conversion pattern.

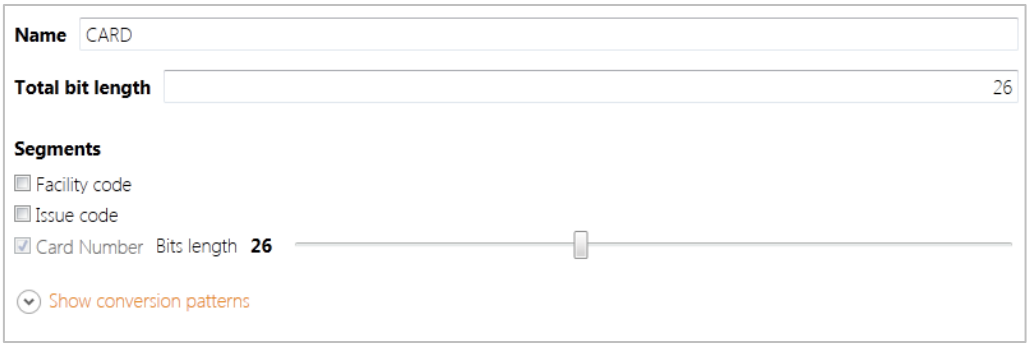
Warning: Do not delete the predefined conversion patterns for the Tecom 27 and Wiegand 26 card types.

11.1.2 Enabling credential types

Note: Only enable credential types that will be used in order to avoid confusion.

To enable a credential type, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Credential Types** to open the Credential Types panel.
2. Tick the checkboxes next to the card formats you plan to use in the secure installation. If necessary, you can create a new card type by clicking the **Add** button next to the record filter.
3. You can change the name of the card in the **Name** field. The card type's name displayed on the left of the panel is composed of the **Name** field and **Total bit length** field.



The card number can be made up of several segments. The following segments of the card number can be enabled and their bit lengths set:

- Facility code
- Issue code
- Card number

Set the individual bit lengths as necessary. Each bit length can range from 1 to 64.

The **Total bit length** field will automatically increase as you increase the bit lengths of the segments. It will not decrease as you decrease the bit lengths of the segments, but you can set it manually (as long as you set it to a value greater than or equal to the actual total bit length).

Warning: Changes to the card type can only be made as long as there is no card of that type assigned to a user in the TecomC4 system.

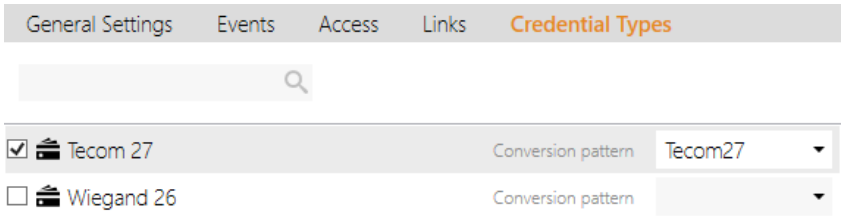
Note: As different security devices can interpret the same card in various ways, it may be necessary to create conversion formulas for specific security devices. These formulas will convert the card number to a format that the device can accept. Formulas can be created manually or loaded from a file by clicking the down arrow next to **Show conversion patterns**.

11.1.3 Configuring card types on security devices

You must specify the card type(s) to be used on all connected devices that support user management. This can be done by selecting the card type(s) on the *Credential Types* tab for each relevant device in the Devices tree. If the card type has a conversion pattern defined, then you can also specify the conversion pattern to be used with each connected security device.

To set the card types used with security device:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Select the desired security device from the Devices tree and open the *Credential Types* tab. For Challenger10 devices, select the Panel element of the Challenger10 device.
3. Tick the checkboxes next to the card formats you wish to use with the security device. You can also specify the conversion pattern to use if any are defined.



Note: When enabling the Tecom 27 or Wiegand 26 card types for use with a Challenger10, you must select the appropriate predefined conversion pattern for the card.

Note: Do not enable two card types with the same bit lengths on the same device.

11.2 Configuring validation rules for credentials

PIN codes must be at least four digits long.

Note: PIN codes longer than ten digits will not be sent to a Challenger10.

Warning: Extension PIN codes are not supported by Challenger10. Do not use.

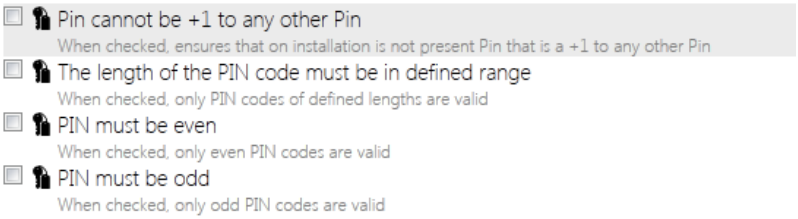
Warning: An extension PIN can be a duplicate of an existing PIN or extension PIN.

TecomC4 allows you to define extra validation rules for PIN codes. You can use this functionality to ensure that, for example, only PIN codes of a certain length meeting the security criteria are entered into the system.

11.2.1 Credential Rules panel

Extra validation rules can be enabled on the Credential Rules panel, which can be opened by clicking the **Navigation** button and selecting **Credential Rules** from the Settings menu.

The Credential Rules panel looks like this:



11.2.2 Enabling credential rules

To enable additional validation rules, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Credential Rules** to open the Credential Rules panel.
2. Tick the checkboxes next to the validation rules to be applied when new credentials are entered. The available validation rules are:
    - **Pin cannot be +1 to any other Pin** – A PIN cannot be +1 another PIN. This is so that an existing PIN's duress code is not used. Only the last digit is affected. For example, if there is an existing PIN of 8919, then a new PIN cannot be 8910.
    - **The length of the PIN code must be in defined range** – Maximum length of PIN is 8.
    - **PIN must be even** – PIN must be even
    - **PIN must be odd** – PIN must be odd

Warning: If the system already contains credentials violating the validation rule you want to enable, these conflicts must first be resolved manually. The validation rule can only be enabled after all the conflicts with the rule are resolved.

Note: The validation rules do not apply to extension PIN codes for cards.

11.3 Configuring card decks

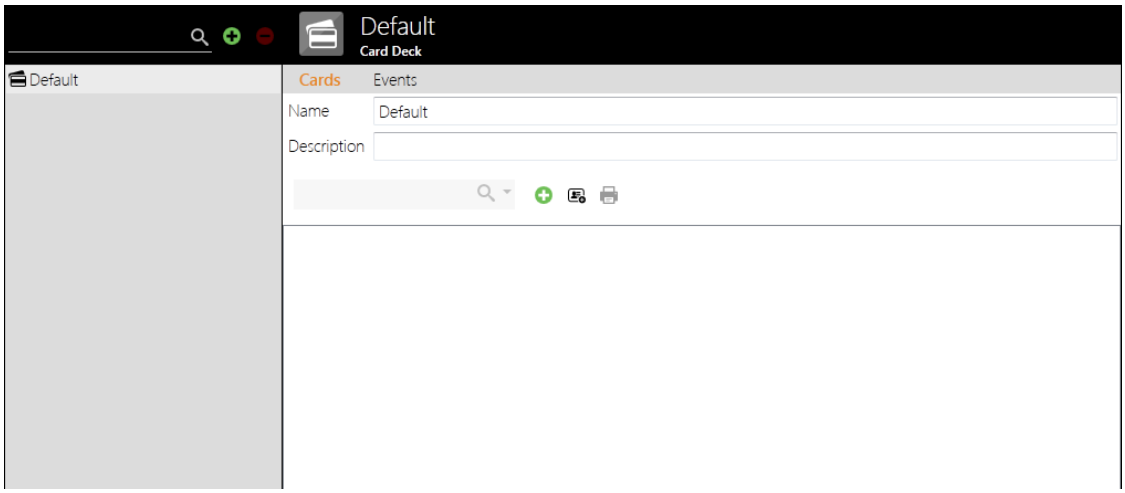
You can define multiple **card decks** in the TecomC4 system. Card decks are used to help operators keep track of the cards in the system. Operator roles allow you to restrict which operators can issue cards from which card deck.

Card decks are configured on the Cards panel.

11.3.1 Cards panel

The Cards panel can be opened by clicking the **Navigation** button and selecting **Cards** from the Administration menu.

The Cards panel looks like this:



The record list shows a list of card decks.

The record filter can be used to filter the card decks in the record list.

The record form has the following tabs:

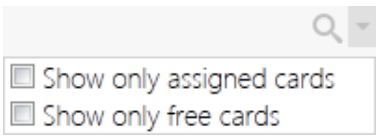
- Cards
- Events

The tabs are described in the following sections.

11.3.1.1 Cards panel: Cards tab

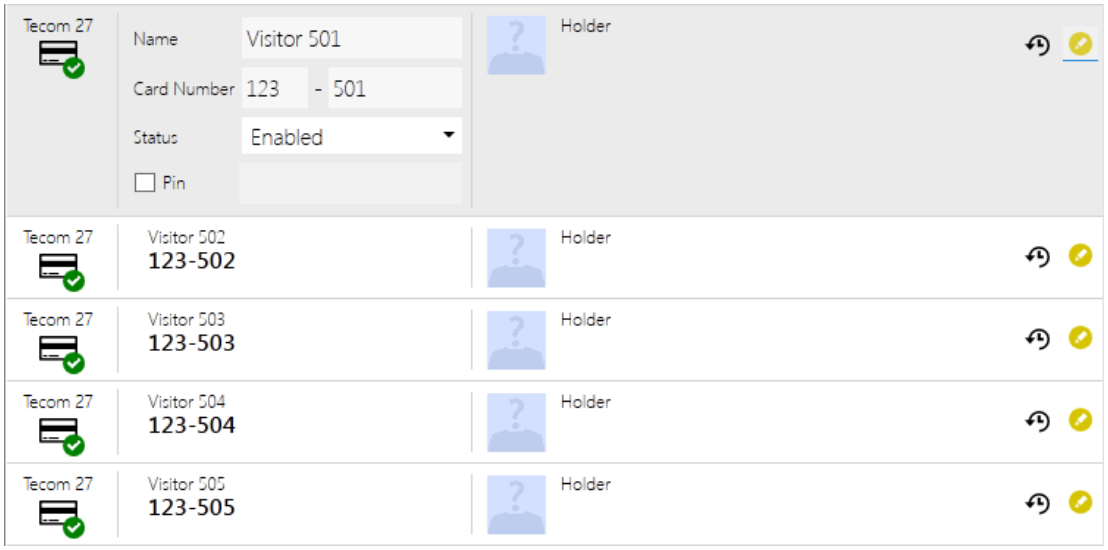
The *Cards* tab shows a name and description of the selected card deck, a toolbar with a filter for filtering the cards and buttons for creating cards and printing a card's layout, and a list of all the cards in the card deck.

The card list shows all cards in the card deck by default. You can filter the list by entering text in the filter. You can also click the drop-down menu icon in order to only show assigned cards or free cards.



See the "Form filter" section on page 16 for more information on the form filter.

For each card in the card deck, the card list entry has several columns of information about the card:



The first column shows the type of card with an icon showing whether the card is either Enabled (), or Disabled or Lost (). The second column shows the name of the card and its number (which may be composed of a facility code, issue code and card number). The third column shows the name and photo of the card's holder. Finally, there is a **History** button to show the history of the card (see the "Viewing a card's history" section on page 70) and an **Edit** button to edit the card's attributes (see the "Changing a card's attributes" section on page 70).

11.3.1.2 Cards panel: Events tab

The Events tab shows all events associated with the selected card deck. See the "Events" chapter on page 124 for more information about the *Events* tab.

11.3.2 Creating a card deck

One predefined card deck called "Default" is present by default in the system. If necessary, you can create a new deck by following these steps:

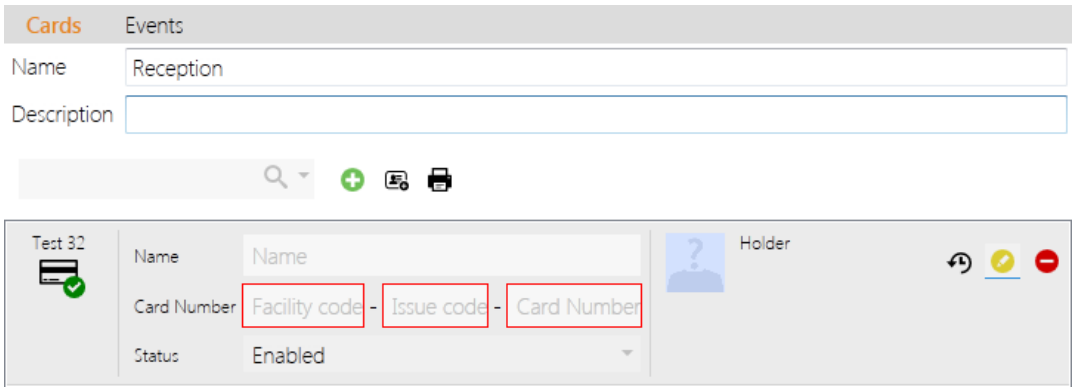
1. Click the **Navigation** button to open the navigation menu. Select **Administration > Cards** to open the Cards panel.
2. Click the **Add** button next to the record filter to create a new card deck.
3. Enter a name and optional description for the card deck.

11.3.3 Adding cards to a card deck

You can now add cards to the card deck if you wish. To add a single card, follow these steps:

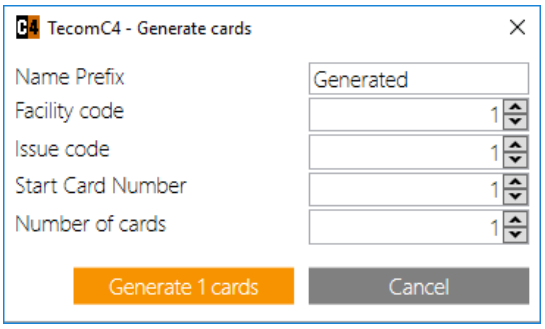
1. Click the **Add** button on the *Cards* tab to add a single new card to the deck. Select the card format of the card you want to add from the drop-down list.

2. Enter a name for the card and the required card parameters, based on the card format settings previously defined for the card type, i.e. facility code, issue code and card number.



If a large number of cards must be entered in the system, it is recommended that you use the bulk card generating function:

1. Click the **Generate cards** button and select the card format of the cards you want to add from the drop-down list.
2. In the next window, enter a prefix for the names of the generated cards. Enter the required card parameters based on the card format settings previously defined for the card type, i.e. facility code and issue code. Enter a starting card number and the number of cards to generate.



3. Enter the initial card code and the number of cards to be generated and click the **Generate <n> cards** button, where <n> is the number of cards to be generated.
4. The requested number of new cards will be generated automatically by the system. The names of the generated cards will be composed of the entered prefix and the card number.

A card deck can be deleted by clicking the **Delete** button, but only if no cards in the card deck are assigned to persons. The predefined “Default” card deck cannot be deleted.

Once cards have been added to a card deck, they can be assigned to persons in the TecomC4 system. See the “Assigning user credentials” section on page 106. Note that cards can also be created when assigning cards to users on the Persons panel.

Once cards have been added to the system you can perform various other actions such as printing card layouts and checking the history of a card’s usage. These actions are described in the following sections.

11.3.4 Changing a card's attributes

To change a card's attributes, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Cards** to open the Cards panel.
2. On the *Cards* tab, select the card whose attributes you wish to change.
3. Click the **Edit** button to expand the view of the card to include its attributes. You can change the name and card number, and set the card's status to Enabled, Disabled or Lost. You can also assign an extension PIN to the card, to be used in the case of combined authentication using a card reader. This option only becomes available when the card has been assigned to a person.

   Warning: Extension PIN codes are not supported by Challenger10. Do not use.

11.3.5 Printing a card's layout

To print a card's layout, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Cards** to open the Cards panel.
2. On the *Cards* tab, select the card whose layout you wish to print.
3. Click the **Print** button above the card list to generate the card layout for the selected card. The card layout will open in a new window. From this window, the card layout can be sent to a printer or exported to a variety of file types such as PDF. The layout can be changed by clicking the **Edit** button.

11.3.6 Viewing a card's history

To view a card's history, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Cards** to open the Cards panel.
2. On the *Cards* tab, select the card whose history you wish to view.
3. Click the **History** button to expand the view of the card to include its history, including times of use and access points where it was used. The history shows all events related to the selected card. The format of the expanded view is similar to the *Events* tab seen in many panels of TecomC4. For more information on viewing event history, see the "Event history" section on page 124.

12 Configuring user access levels

User access refers to permission to enter a secure area of the installation using personal credentials such as a card or PIN code. See the “Configuring user credentials” chapter on page 62 for information on configuring user credentials.

The permissions to enter secure areas and arm/disarm areas etc. are determined by user **access levels**. You can override access level permissions for individual users. Access levels are applied to specific device elements, such as areas and doors, called **access points**.

You do not need to know the physical layout of devices to configure access levels. An access level can have access points from multiple security devices, which can also be geographically spread.

Configuring a person as a user of the secure installation involves the following steps:

1. Defining access permissions with access levels
2. Assigning user credentials to the person
3. Assigning user access levels to the person
4. Sending access information to security devices

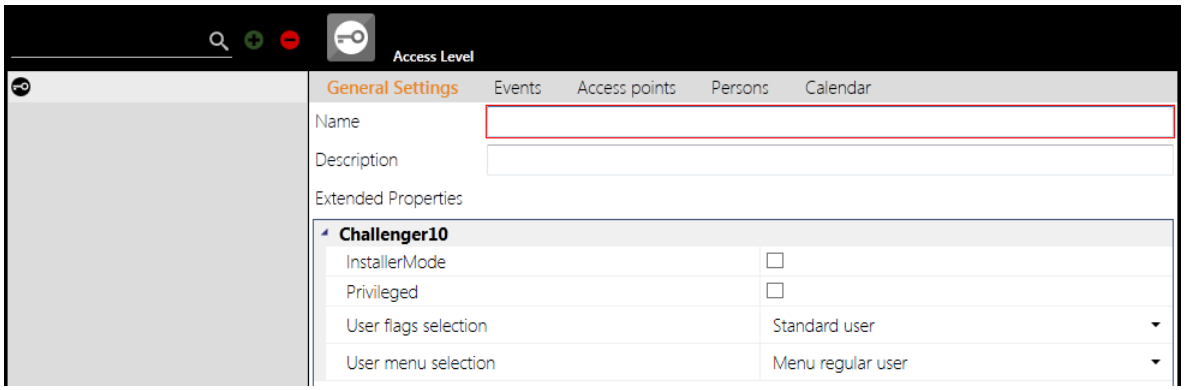
This chapter covers defining access permissions with access levels. The subsequent steps are covered in the “Assigning a user” section on page 106.

This chapter also describes how to generate access reports about users and security devices.

12.1 Access Levels panel

Access Levels are defined on the Access Levels panel, which can be opened by clicking the **Navigation** button and selecting **Access Levels** from the Security menu.

The Access Levels panel looks like this:



The record list shows a list of access levels.

The record filter can be used to filter access levels in the record list.

The record form has the following tabs:

- General Settings

- Events
- Access points
- Persons
- Calendar

The tabs are described in the following sections.

12.1.1 Access Levels panel: General Settings tab

The *General Settings* tab shows the following fields for the selected access level:

- **Name** – Name of the access level
- **Description** – Description of the access level
- **Extended Properties** – Extended properties of the access level. The properties shown here depend on which device drivers are installed in the system.

For the Challenger10 driver, the extended properties are:

- **Installer Mode (Alarm Group 3)** – A user with the selected access level will be assigned to Alarm Group 3 (“Master Code”). Areas assigned to the access level are ignored since Alarm Group 3 contains Area Group 1, which contains all areas.

  Note: In order for a user with the selected access level to have Alarm Group 3 on a Challenger10, you must assign at least one access point from the Challenger10 to the access level. If a user requires Alarm Group 3 on multiple Challenger10 panels, then an access point from each relevant Challenger10 must be assigned to the access level. See the “Access Levels panel: Access points tab” section on page 75 for information on assigning access points to an access level.

- **Privileged** – Whether a user with the selected access level has the “Privileged” user flag set for them on the Challenger10.
- **User flags selection** – User flags drop-down list. See the “User flags selection” section below for more information.
- **User menu selection** – User menu drop-down list. See the “User menu selection” section on page 74 for more information.

12.1.1.1 User flags selection

The User Flags Selection field determines the abilities that a user with the selected access level has, such as the ability to arm areas associated with the access level or the ability to reset system alarms.

Access levels in TecomC4 correspond to alarm groups in Challenger10, so these abilities correspond to the options for programming alarm groups in Challenger10. Refer to the “Option 5. Alarm Groups” section of the *Challenger Series Programming Manual* for more information on the options that can be programmed for alarm groups.

The available options for the User flags selection field are:

- Advanced user
- Audit log only user
- Detailed configuration
- Limited user
- Standard user

The following table shows which alarm group programming options will be enabled when you select each option for the User flags selection field (except for the Detailed configuration option). Alarm group programming options not listed in the table are not enabled for any of the User flags selection options in the table. If you need to enable any of the alarm group programming options not listed, then you must select the Detailed configuration option.

Table 4: User flags selection options

Alarm group programming option	Advanced User	Audit Log Only User	Limited User	Standard User
User alarm group	✓	✓	✓	✓
Alarm system control	✓	✓	✓	✓
Reset system alarms	✓			
Can area be armed	✓		✓	✓
Can area be disarmed	✓		✓	✓
Can area be reset	✓		✓	✓
Can area be timed	✓		✓	✓
Disable auto-deisolate	✓			✓

If you select Detailed configuration, then more fields will appear with detailed configuration options, corresponding to the indicated alarm group programming options:

Table 5: Detailed configuration options

Access level configuration option	Alarm group programming option
Allow alarm group to be assigned to user	User alarm group
Allow user to activate user category timers	Can area be timed
Allow user to arm the assigned area	Can area be armed
Allow user to control the alarm system	Alarm system control
Allow user to disarm the assigned area	Can area be disarmed
Allow user to force arm an area that has unsealed inputs	Forced arming when inputs unsealed
Allow user to generate a duress alarm on a keypad	Keypad duress
Allow user to reset system alarms	Reset system alarms
Allow user to reset the assigned area	Can area be reset
Alternate alarm group	Alternate alarm group

Access level configuration option	Alarm group programming option
Assign user category timer 1	User category 1
Assign user category timer 2	User category 2
Assign user category timer 3	User category 3
Assign user category timer 4	User category 4
Assign user category timer 5	User category 5
Assign user category timer 6	User category 6
Assign user category timer 7	User category 7
Assign user category timer 8	User category 8
Automatically isolate unsealed inputs when arming	Auto isolate unsealed inputs
Enable area search procedure	Enable area search
Prevent arming if user category timer not running	No arming if user category not timing
Prevent automatic de-isolation of inputs when area disarmed	Disable auto-deisolate
Prevent disarming when inputs are unsealed	Prevent forced disarming
User can access via remote	Can user access via remote
User will be presented with a list of areas on a keypad	Prompt with list of areas

The remaining options for programming alarm groups that are not listed in the table above are:

- “Alarm group number” and “Alarm group name” – determined by the Challenger10 driver
- “Areas assigned” – determined by which areas are ticked on the *Access points* tab for the selected access level
- “Alarm group time zone” – determined by the timeframes defined on the *Calendar* tab for the selected access level
- “User menu options” – discussed in the “User menu selection” section below

12.1.1.2 User menu selection

The User menu selection field determines which of the 24 top-level user menus in the Challenger10 system will be visible to users with the selected access level. Refer to the “User Menu Structure” section of the *Challenger Series Programming Manual* for more information on the user menus.

The available options for the User menu selection field are:

- Menu extended user
- Menu regular user
- Menu supervisor

The following table shows which user menus will be visible for each option of the User Menu Selection field:

Table 6: User menu selection

Challenger10 Menu	Menu extended user	Menu regular user	Menu supervisor
1. Panel Status	✓	✓	✓
2. Input Unsealed	✓	✓	✓
3. Input In Alarm	✓	✓	✓
4. Input Isolated	✓	✓	✓
5. History	✓		✓
6. Test Report			✓
7. Service Menu			✓
8. Film Counters			✓
9. Input Text			✓
10. Isolate	✓		✓
11. Deisolate	✓		✓
12. Test Input			✓
13. Start Auto Access Test			✓
14. Program Users			✓
15. Time and Date			✓
16. Isolate/Deisolate RAS/DGP	✓		✓
17. Enable/Disable Service Tech			✓
18. Reset Cameras			✓
19. Install Menu			✓
20. Door and Floor Groups			✓
21. Holidays			✓
22. Open Door			✓
23. Unlock, Lock, Disable and Enable			✓
24. Automation Control	✓		✓

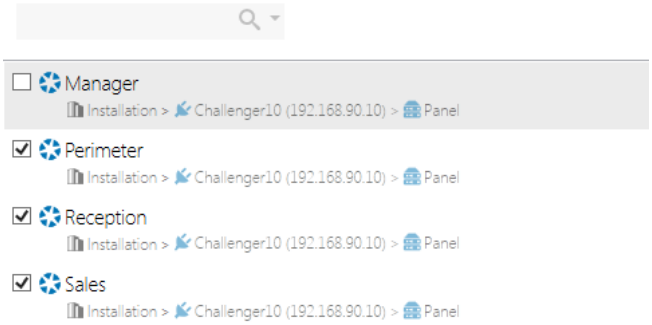
12.1.2 Access Levels panel: Events tab

The *Events* tab shows all events associated with the selected access level. See the “Events” chapter on page 124 for more information about the *Events* tab.

12.1.3 Access Levels panel: Access points tab

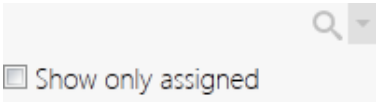
The *Access Points* tab shows a list of all of the access points in the system that the current operator has permission to view. Below each access point in the list is shown a chart indicating the access point’s position in the Devices tree hierarchy.

For example:



Tick the access points of the secure installation that persons with the selected access level will be allowed to access.

The tab's form filter can be used to filter the access points shown. You can also click the drop-down menu icon in order to only show access points to which the selected access level is assigned:

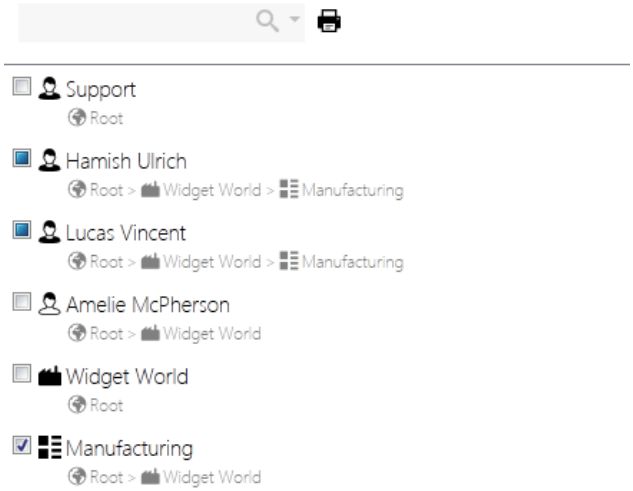


See the "Form filter" section on page 16 for more information on the form filter.

12.1.4 Access Levels panel: Persons tab

The *Persons* tab shows a list of persons and other organisational units from the Persons tree that the current operator has permission to view. Below each item in the list is shown a chart indicating the item's position in the Persons tree hierarchy.

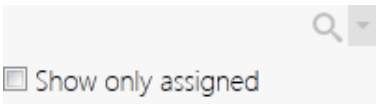
For example:



To assign the selected access level to a person or other organisational unit in the list, tick the checkbox next to the item's name.

If you assign the selected access level to organisational unit, such as a company, then all child nodes will also be assigned the access level, e.g. a person in the company.

The tab's form filter can be used to filter the names shown. You can also click the drop-down menu icon in order to only show persons to whom the selected access level is assigned:



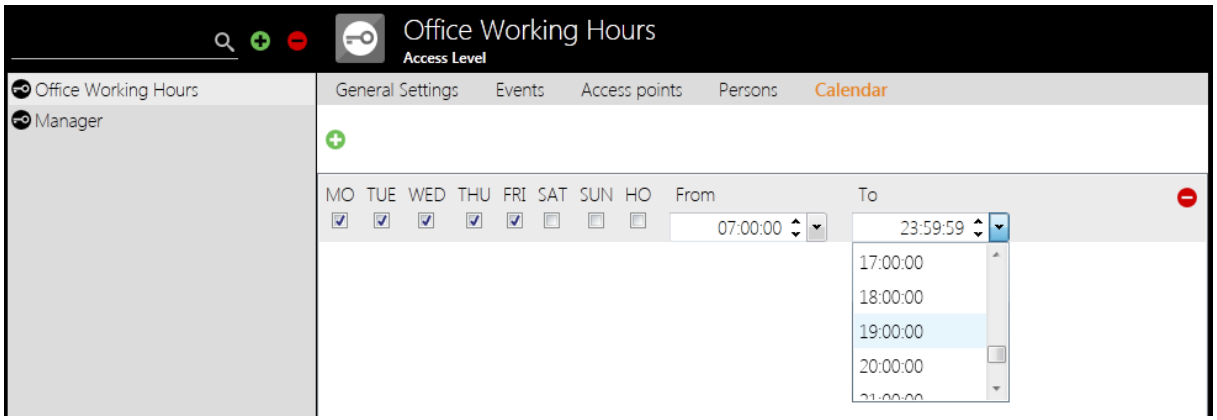
See the "Form filter" section on page 16 for more information on the form filter.

You can print a report listing the persons assigned to the selected access level by clicking the **Print** button.

Note: Assigning persons to access levels can also be done on the *Access Levels* tab of the Persons panel. See the "Persons panel: Access Levels tab" section on page 96.

12.1.5 Access Levels panel: Calendar tab

The *Calendar* tab shows the timeframes to which the selected access level applies.



Click the **Add** button to add a new timeframe to the selected access level's calendar.

Select the days of the week (and holidays, represented by HO) that the selected access level applies to. Enter **From** and **To** times, in HH:MM:SS format, for the selected access level.

Click the **Delete** button to delete the selected timeframe.

Note: Challenger10 devices can have up to eight timeframes for each access level.

12.2 Creating an access level

An **access level** is a set of permissions for devices (access points) in the secure installation. Access levels can be assigned to users in the system. Users who require the same access permissions can be assigned the same access level. This allows for changing access permissions for a group of users in one place.

To create an access level, follow these steps:

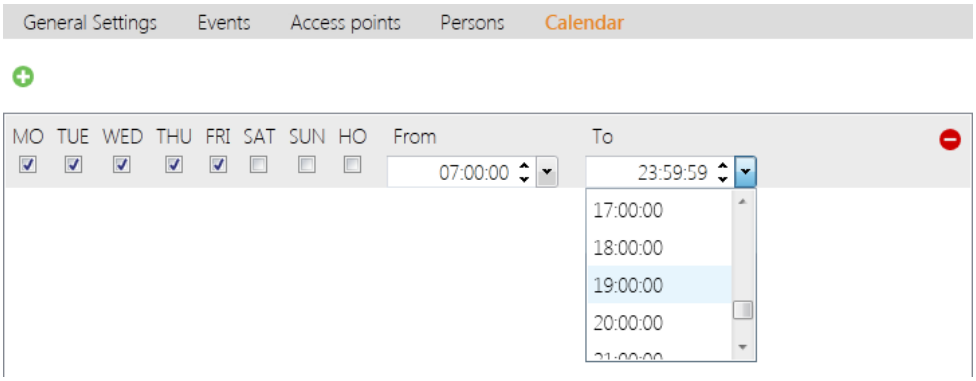
1. Click the **Navigation** button to open the navigation menu. Select **Security > Access Levels** to open the Access Levels panel.
2. Click the **Add** button next to the record filter to create a new access level.
3. On the *General Settings* tab, enter a name and (optional) description for the new access level.
4. On the *General Settings* tab, set any extended properties as necessary. The properties shown here depend on which security devices are connected to the TecomC4 system. Extended properties specify additional settings and rights that users with the access level have for specific types of security devices.

   See the “Access Levels panel: General Settings tab” section on page 72 for information on the extended properties for Challenger10.
5. On the *Access Points* tab, tick the access points such as areas and doors that users with this access level will be allowed to access.
6. On the *Persons* tab, you can tick the organisational units to which the access level will apply.

   Note: You can assign persons and other organisational units to an access level in the Persons tree by clicking the *Access Levels* tab and ticking the required access level.

If necessary, timeframes can be added to specify which days and times the access level is in effect:

1. Click the *Calendar* tab.
2. Click the **Add** button to add a new timeframe. A timeframe entry will appear:



   Tick the days for the timeframe to be active, and enter the start and end time of its validity.

   The HO column represents holidays. Holidays are defined within TecomC4 and set on connected security devices. If the HO column is ticked, then the timeframe will be active for any holidays set on the security devices that the relevant access points are part of. See the “Defining holidays” chapter on page 21 for information on defining holidays.

Several timeframes can be added to the access level. To remove a timeframe, click the **Delete** button to the right of the respective timeframe.

Note: Challenger10 devices can have up to eight timeframes for each access level.

You can click the **Delete** button next to the record filter to delete the selected access level. A dialog box will be shown asking you to confirm the deletion.

To duplicate an access level, right-click the name of the access level in the record list to display the access level's context menu and select the **Duplicate** menu item.

Warning: To ensure that access information changes are also transferred to devices, it is necessary to synchronize access information (see the "Sending access information to devices" section on page 109).

Warning: You can delete an access level even if users are assigned to it.

Warning: Areas and calendars of access levels are cumulative. That is, if a user is assigned to several access levels with different areas and/or timeframes defined for each level, the user's access will reflect the sum of all areas and calendars from all access levels assigned to the user.

For example, if Access Level 1 grants the user access on weekdays from 8:00 am to 5:00 pm in area X and Access Level 2 grants the user access every day of the week from 9:00 am to 6:00 pm in area Y, then the user will be granted access from 8:00 am to 6:00 pm on weekdays and from 9:00 am to 6:00 pm on weekends, to both areas X and Y.

For Challenger10, the user is assigned an alarm group that has an area group with all the areas from all assigned access levels. The alarm group has a time zone with all timeframes from the calendars of all assigned access levels.

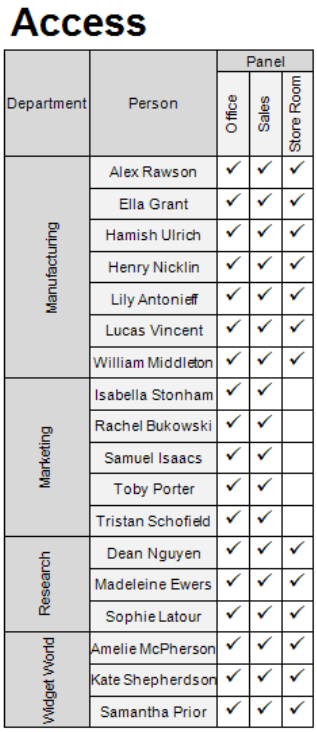
Warning: A user who has an access level assigned which has no calendar restriction, or who is granted access directly from the *Access* tab of the Persons or Devices panels, can have their access to an access point restricted if:

- they are assigned another access level that has a calendar restriction for the access point, or
- they inherit an access level that has a calendar restriction for the access point.

To ensure unrestricted access, set up an access level with a calendar with all days ticked and the time set from 00:00:00 to 23:59:59.

12.3 Generating access reports

The TecomC4 system allows you to create printable reports about access permissions. Generated reports contain a matrix of information about access permissions for selected parts of the Persons and Devices trees. For example:



Access

Department	Person	Panel		
		Office	Sales	Store Room
Manufacturing	Alex Rawson	✓	✓	✓
	Ella Grant	✓	✓	✓
	Hamish Ulrich	✓	✓	✓
	Henry Nicklin	✓	✓	✓
	Lily Antonieff	✓	✓	✓
	Lucas Vincent	✓	✓	✓
	William Middleton	✓	✓	✓
Marketing	Isabella Stonham	✓	✓	
	Rachel Bukowski	✓	✓	
	Samuel Isaacs	✓	✓	
	Toby Porter	✓	✓	
	Tristan Schofield	✓	✓	
Research	Dean Nguyen	✓	✓	✓
	Madeleine Ewers	✓	✓	✓
	Sophie Latour	✓	✓	✓
Widget World	Amelie McPherson	✓	✓	✓
	Kate Shepherdson	✓	✓	✓
	Samantha Prior	✓	✓	✓

To generate an access report, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Select the parts of the Persons tree in the record list about which you want to generate an access report.
3. On the *Access* tab, select the parts of the Devices tree about which you want to generate an access report.
4. Click the **Print** button and select the required report type:
    a. **Print** – print all access permissions for access points.
    b. **Print only allowed** – print only allowed access permissions for access points.
5. A new window will open with the generated access report. The report can be printed or exported to a range of file types, such as PDF.

Note: Access reports can also be generated from the Devices panel. Select the parts of the Devices tree in the record list that you want to generate an access report on, then go to the *Access* tab and select the parts of the Persons tree you want to generate an access report on. Click the **Print** button and select the required report type.

---

13 Configuring operator roles

Roles can be used to define the access rights of operators to all parts of the TecomC4 system. A role is a set of permissions assigned to persons who will be operators of the TecomC4 system.

A role can be assigned to multiple operators with the same responsibilities. This will ensure a transparent structure of defined permissions and the possibility of easily changing them in one place if it is necessary in the future.

Roles define operator permissions for every aspect of the TecomC4 system, from which panels are visible to an operator to what commands the operator can send to security devices.

Configuring a person as an operator involves the following steps:

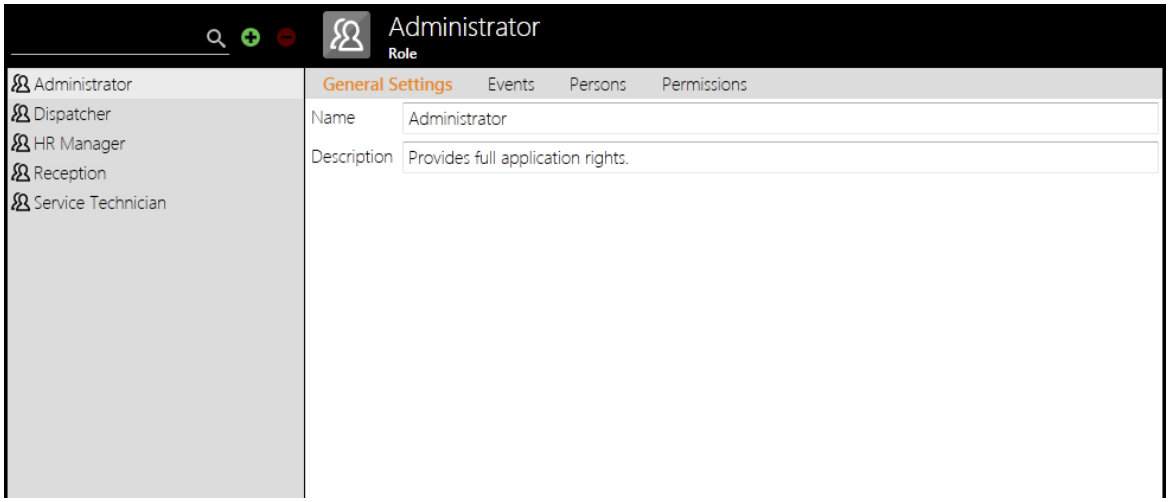
1. Defining operator permissions with roles
2. Assigning operator credentials to the person
3. Assigning operator roles to the person
4. Installing a TecomC4 client for the operator

This chapter covers defining permissions with roles, including a detailed explanation of operator permissions. The subsequent steps are covered in the “Assigning an operator” section on page 104.

13.1 Roles panel

Roles are configured on the Roles panel, which can be opened by clicking the **Navigation** button and selecting **Roles** from the Security menu.

The Roles panel looks like this:



The record list shows a list of roles.

The record filter can be used to filter the roles in the record list.

The record form has the following tabs:

- General Settings

- Events
- Persons
- Permissions

The tabs are described in the following sections.

13.1.1 Roles panel: General Settings tab

The *General Settings* tab shows the name and description of the selected role.

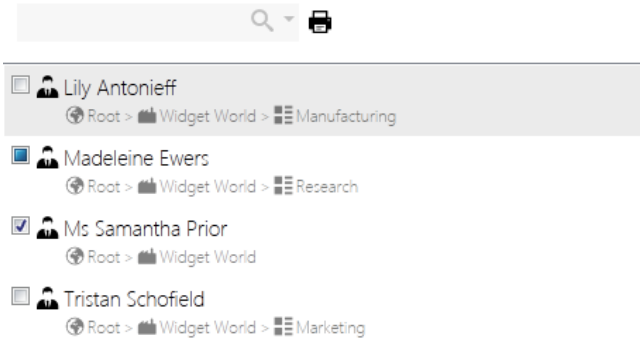
13.1.2 Roles panel: Events tab

The *Events* tab shows all events associated with the selected role. See the “Events” chapter on page 124 for more information about the *Events* tab.

13.1.3 Roles panel: Persons tab

The *Persons* tab shows a list of persons and other organisational units from the Persons tree that the current operator has permission to view. Below each item in the list is shown a chart indicating the item’s position in the Persons tree hierarchy.

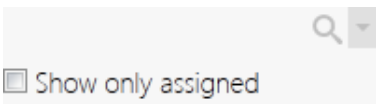
For example:



To assign the selected role to a person or other organisational unit in the list, tick the checkbox next to the unit’s name.

If you assign the selected role to organisational unit, such as a company, then all child nodes will also be assigned the access level, e.g. a person in the company.

The tab’s form filter can be used to filter the names shown. You can also click the drop-down menu icon in order to only show persons to whom the selected role is assigned.



See the “Form filter” section on page 16 for more information on the form filter.

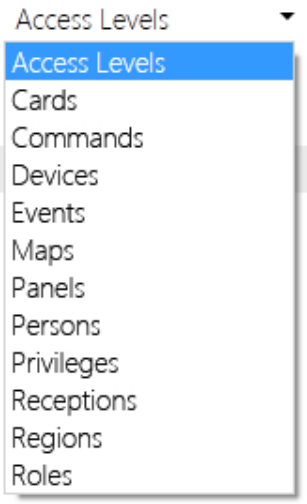
You can print a report listing the persons assigned to the selected role by clicking the **Print** button.

Note: Assigning persons to roles can also be done on the *Roles* tab of the Persons panel. See the “Persons panel: Roles tab” section on page 94.

13.1.4 Roles panel: Permissions tab

The *Permissions* tab shows detailed permissions for all aspects of the TecomC4 system for the selected role.

At the top of the Permissions tab, there is a drop-down list showing the categories for which role permissions can be changed, as shown below:



The following section gives detailed information about setting role permissions for these categories.

13.2 Role permissions

The following sections describe the categories for which permissions can be set and how to set permissions.

13.2.1 Role permission categories

Role permissions can be changed for the following categories:

- **Access Levels** – Determines whether the operator can view and modify existing access levels. See the “Configuring user access levels” section on page 71 for more information on access levels. The tab shows the existing access levels, with columns of the following permissions:
  - **View** – view the specified access level
  - **Modify** – modify the specified access level
  - **Delete** – delete the specified access level
  - **Assign to** – assign the specified access level to persons
  - **Modify Permissions** – modify permissions of the specified access level

- **Cards** – Determines whether the operator can view and modify existing card decks. See the “Configuring card decks” section on page 66 for more information on card decks. The tab shows the existing card decks, with columns of the following permissions:
  - **View** – view the specified card deck
  - **Modify** – modify the specified card deck
  - **Delete** – delete the specified card deck
  - **Modify State** – modify state of the specified card deck
  - **Modify Permissions** – modify permissions of the specified card deck
- **Commands** – Determines whether the operator can execute remote commands on devices in the system. The tab shows the Devices tree, with permission indicators on the right for commands. The arrow icon ➡ indicates all commands available in the system. You can click the **expand details** ••• button on the left of the panel to show all of the commands for which permissions can be set.

  See the “Challenger10 commands” section on page 42 for information on the commands that can be sent to Challenger10.
- **Events** – Determines whether the operator can view and modify events. The tab shows the complete list of events in the TecomC4 system, with columns of the following permissions:
  - **View** – view the specified event
  - **Modify** – modify the specified event
- **Maps** – Determines whether the operator can view and modify maps. The tab shows the hierarchy of maps, with columns of the following permissions:
  - **View** – view the specified map
  - **Modify** – modify the specified map
  - **Delete** – delete the specified map
  - **Create in Container** – create a map under the specified map
  - **Change Parent** – move the specified map to a different parent in the hierarchy
  - **Modify Permissions** – modify permissions of the specified map
- **Panels** – Determines which panels of the TecomC4 application the operator can view. The navigation menu for the operator will change accordingly. Each panel has a checkbox next to it that can be ticked to allow access to the operator. The panels available in TecomC4 are:
  - Access Guard
  - Access Levels
  - Alarms
  - Automatic actions

- Cards
- Credential Rules
- Credential Types
- Designer
- Devices
- Diagnostic
- Drivers
- Events
- Extensions
- Holidays
- Licenses
- Monitor
- Persons
- Receptions
- Regions
- Roles
- Visitors
- Visits

Note: The Receptions, Visitors and Visits panels are only visible to operators if Visitors Management has been enabled. See the “Visitor management” chapter on page 139 for more information.

- **Persons** – Determines whether the operator can view and edit persons and other organisational units in the Persons tree. The tab shows the Persons tree, with columns of the following permissions:
  - **View** – view the specified node
  - **Modify** – modify the specified node
  - **Delete** – delete the specified node
  - **Create in Container** – create a new Persons tree node under the specified node
  - **Change Parent** – move the specified node to a different parent Persons tree
  - **Modify Permissions** – modify permissions for the specified node
- **Privileges** – Determines whether the operator has certain specific privileges within the TecomC4 system. The privileges that can be enabled are:
  - **Administrator** – operator has full administrator rights to TecomC4

- **Create new access level** – operator can create a new access level
- **Create new card deck** – operator can create a new card deck
- **Create new reception** – operator can create a new reception (Visitors Management must be enabled)
- **Create new role** – operator can create a new role
- **Create new visitors** – operator can create new visitors (Visitors Management must be enabled)
- **Create unacceptable visit** – operator can create a visit from an unacceptable visitor (Visitors Management must be enabled)
- **Export protected properties** – operator can export protected properties such as passwords and PIN codes.
- **Manage alarms** – operator can manage alarms (Alarms Processing must be enabled)
- **Manage holidays** – operator can manage holidays
- **Manage passwords** – operator can change passwords for operators
- **Modify reports** – operator can modify the formatting of reports

- **Receptions** – Determines whether the operator can view and edit receptions (Visitors Management must be enabled to view receptions). The tab shows a list of receptions, with columns of the following permissions:
  - **View** – view the specified reception
  - **Modify** – modify the specified reception
  - **Delete** – delete the specified reception
  - **Modify Permissions** – modify permissions of the specified reception
- **Regions** – Determines whether the operator can view and edit regions in the Regions tree. The tab shows the Regions tree, with columns of the following permissions:
  - **View** – view the specified region
  - **Modify** – modify the specified region
  - **Delete** – delete the specified region
  - **Create in Container** – create a new region under the region
  - **Change Parent** – move the specified region to a different parent region
  - **Modify Permissions** – modify permissions of the specified region
- **Roles** – Determines whether the operator can view and edit operator roles. The tab shows a list of operator roles, with columns of the following permissions:
  - **View** – view the specified role
  - **Modify** – modify the specified role

- **Delete** – delete the specified role
- **Assign to** – assign the specified role to persons
- **Modify Permissions** – modify permissions of the specified role

13.2.2 Setting role permissions

Except for the Privileges and Panels categories, each category has columns of permissions with coloured circles indicating the current permission status for the selected role.

To simplify setting permissions, the system can allow permissions to be inherited down a tree. If you set the permission for a parent, then that permission can be inherited by its children. Inheritance of permissions is applicable to categories that have a tree structure, i.e. the Commands, Devices, Maps, Persons and Regions categories. If an inherited permission is not suitable, it can be changed individually. It is also possible to set permissions that are not inherited by children in the tree.

Permissions can be set at any level of the tree.

The possible colours for the coloured circles are:

- – Permission is explicitly allowed for the specified item. Permission is not inherited down the tree (if applicable).
- – Permission is explicitly allowed for the specified item. Permission is inherited down the tree.
- – Permission is allowed for the specified item due to permission being inherited from higher up the tree.
- – Permission is explicitly denied for the specified item. Permission is inherited down the tree (if applicable).
- – Permission is denied for the specified item due to permission being inherited from higher up the tree.
- – Permission is not set or inherited for the specified item. The permission defaults to permission denied.

Right-clicking a coloured circle opens a context menu with the following options:

- **Allow** – Allow permission for the specified item. Permission is not inherited down the tree if there is one.
- **Allow with inheritance** – Allow permission for the specified item. Permission is inherited down the tree. This option is only available when dealing with a tree structure, i.e. for the following categories: Commands, Devices, Maps, Persons and Regions.
- **Deny** – Deny permission for the specified item. Permission is inherited down the tree if there is one.
- **Revoke** – Revoke specific permission for the specified item. Permission is reverted

You can also click a coloured circle to cycle through the above options.

If you hover the mouse cursor over a coloured circle, a tooltip will be displayed with a list showing how permission is decided for the specified item. The top entry in the list shows the deciding permission.

13.2.2.1 Combination of permissions

In order for the role to function as expected, you must consider the combination of all the permissions required for the operator to perform certain actions.

For example, to allow an operator to add persons to an access level from the Persons tree, the role must have the following permissions:

- Permission to view the Persons panel (from the Panels category)
- View permission for the Persons tree (from the Persons category)
- View and Assign to permission for the access level (from the Access Levels category)

13.3 Creating a role

Follow these steps to create a role:

1. Click the **Navigation** button to open the navigation menu. Select **Security > Roles** to open the Roles panel.
2. Click the **Add** button to add a new role. Enter the role's name and an optional description.
3. On the *Permissions* tab, you will find a drop-down list with all the categories of TecomC4 for which permissions can be defined. Use the drop-down list to go through the categories for which you wish to define permissions. Refer to the detailed explanations in the "Role permissions" section on page 83.
4. When all required permissions are assigned, click the *Persons* tab and tick the organisational units to which the role should be applied.

From this point on, the operator will be able to access the TecomC4 based on the permissions resulting from their assigned role. More than one role can be assigned to the operator. In such a case, the assigned permissions are added together.

Note: In addition to persons, a role can also be set on other organisational units, where the assigned role is subsequently inherited by persons under the organisational unit. In this way, one role can be assigned to an entire department (for example, reception) and all persons placed under this department will inherit the role and its permissions.

In the TecomC4 system, permissions can be defined directly for organisational units, without the need to use roles. In the long run, however, this approach is less efficient as the organisational units become the owners of permission definitions. If a node with explicitly defined permissions is removed from the organisational structure, the permissions defined for the node are lost. Therefore, the preferred method for defining TecomC4 permissions is to use roles and to assign them to organisational units.

Note: To duplicate a role, right-click the name of the role in the Roles list to display its context menu and select the **Duplicate** menu item.

Note: It is not possible to duplicate the Administrator role.

Note: A role can also be assigned to persons or other organisational units in the Persons tree by ticking the required role on the *Roles* tab. See the “Persons panel: Roles tab” section on page 94.

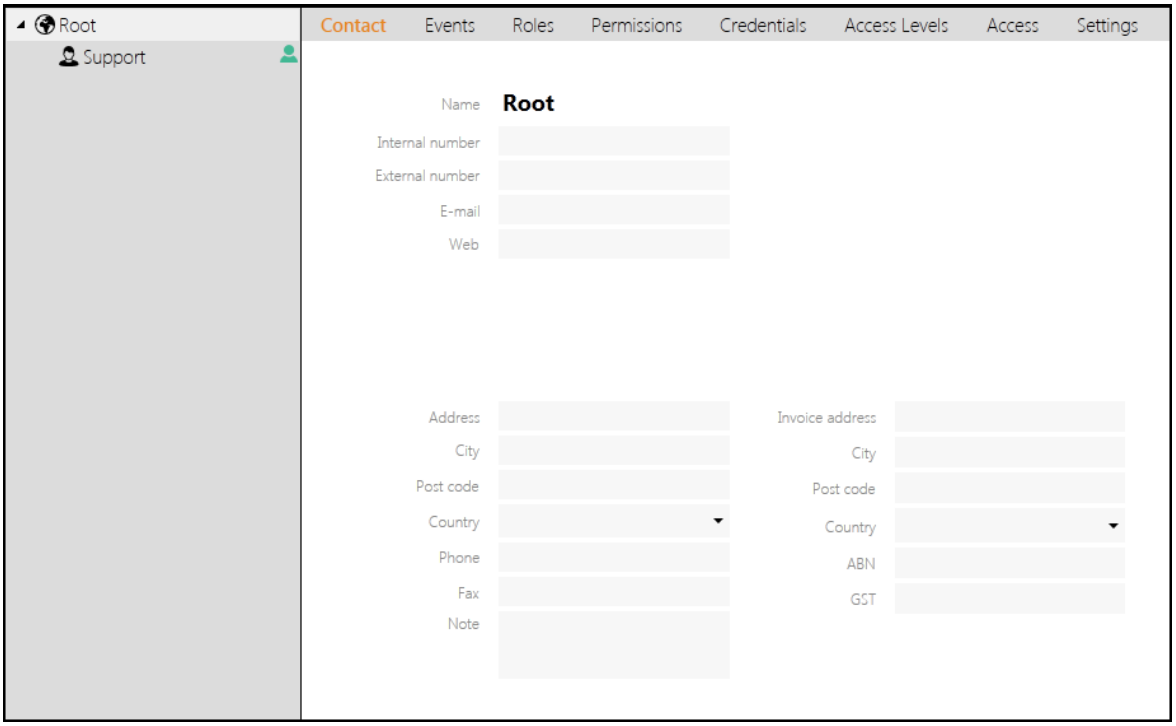
14 Persons management

The TecomC4 system allows the management of persons in the organisational structure, the assignment of credentials (cards, PINs, etc.) to persons and the definition of permissions for persons to access secure sites and the TecomC4 system. The Persons tree serves for complex management of a company's organisational structure.

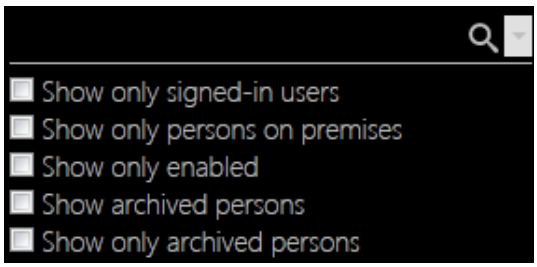
14.1 Persons panel

Person management is done on the Persons panel, which can be opened by clicking the **Navigation** button and selecting **Persons** from the Administration menu.

The Persons panel looks like this:



The record list shows the Persons tree. The Persons tree can be filtered by typing text in the record filter or by selecting a pre-determined filter option from the filter drop-down menu  :



The filter options available are:

- **Show only signed-in users** – show only those operators who are signed into a client of the TecomC4 system.

- **Show only persons on premises** – show only those persons who are present on the premises. The Counting Persons in Regions functionality must be enabled (see the “Counting persons in regions” section on page 50).
- **Show only enabled** – show only those persons who are enabled according to their start and end dates.
- **Show archived persons** – by default, archived persons are not shown in the Persons tree. Clicking this option will show archived persons and other archived nodes of the Persons tree. See the “Archiving, restoring and deleting nodes” section on page 13 for more information.
- **Show only archived persons** – show only persons that have been archived. This will allow you to easily find persons to delete or restore from the person’s right-click context menu.

The record form has the following tabs:

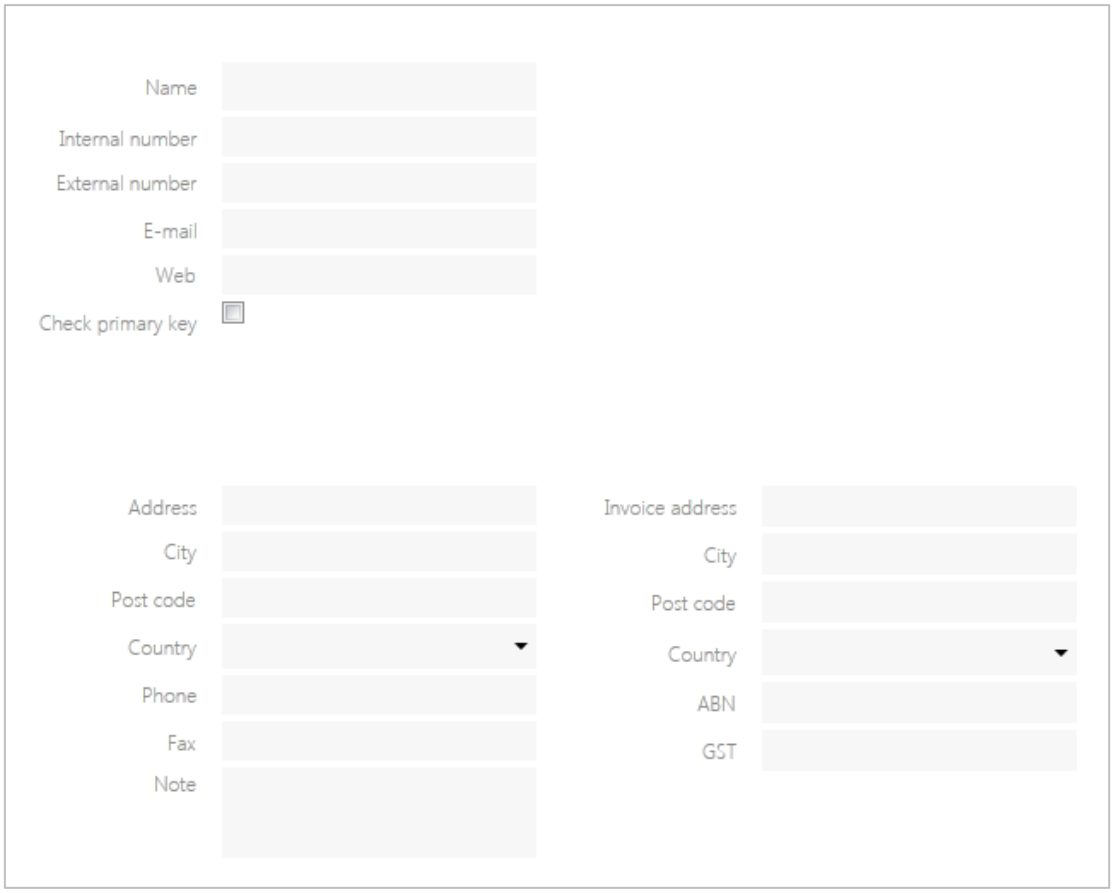
- Contact
- Events
- Roles
- Permissions
- Credentials
- Access Levels
- Access
- Persons Present
- Settings

The tabs are described in the following sections.

14.1.1 Persons panel: Contact tab

The *Contact* tab shows contact information for the selected node of the Persons tree. The information shown on the *Contact* tab varies depending on whether the selected node is a person or an organisational unit such as a company or department.

The following image shows the *Contact* tab for a company:

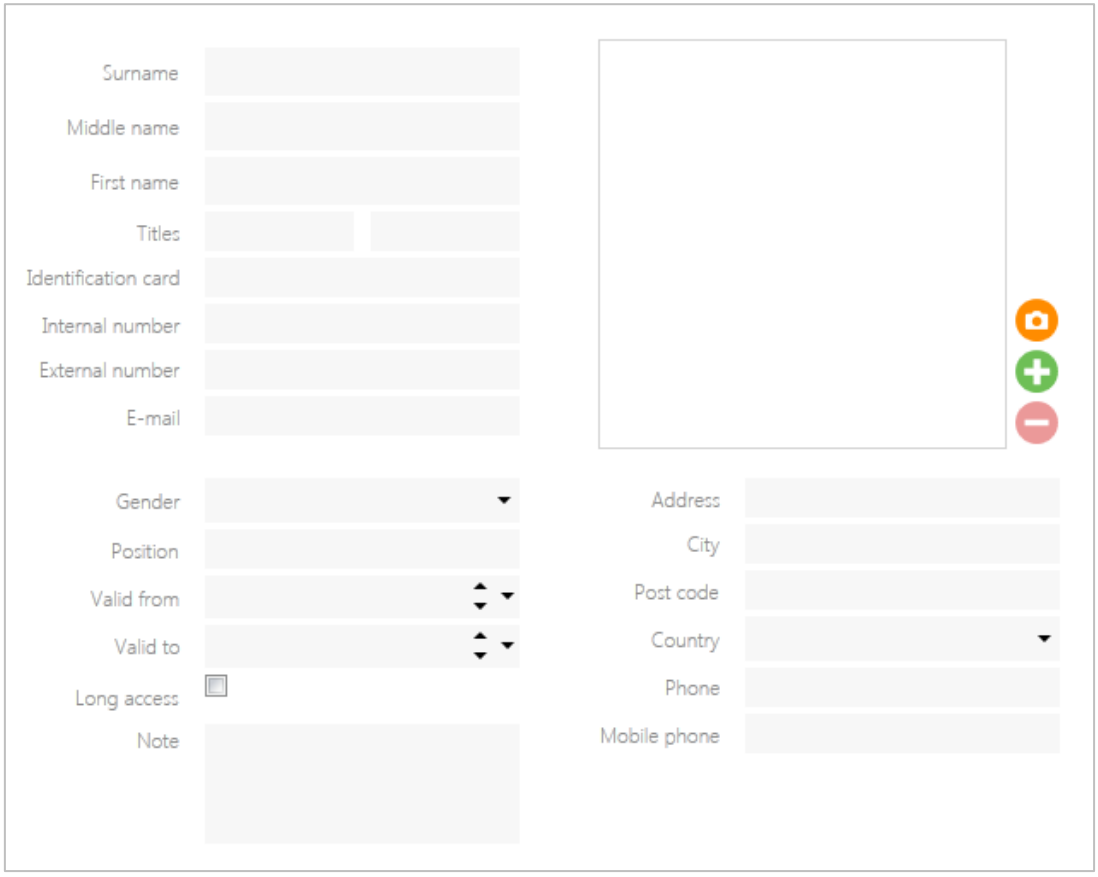


The following fields are shown if the selected node is the Root, a company, a division, a centre or a department:

- **Name** – entity name.
- **Internal number** – entity's internal number.
- **External number** – entity's external number.
- **E-mail** – entity's contact e-mail address.
- **Web** – entity's web address.
- **Check primary key** (this field applies to company nodes only) – if ticked, persons in the company must have unique internal numbers. See the "Check primary key" section on page 103.
- **Address** – entity's address.
- **City** – city of the entity's address.
- **Post code** – post code of the entity's address.
- **Country** – country of the entity's address.
- **Phone** – entity's phone number.
- **Fax** – entity's fax number.
- **Note** – text field to add any relevant notes about the entity.

- **Invoice address** – entity's invoice address.
- **City** – city of the entity's invoice address.
- **Post code** – post code of the entity's invoice address.
- **Country** – country of the entity's invoice address.
- **ABN** – the entity's ABN.
- **GST** – the entity's GST.

The following image shows the *Contact* tab for a person:



The following fields are shown if the selected node is a person:

- **Surname** – person's surname.
- **Middle name** – person's middle name.
- **First name** – person's first name.
- **Titles** – person's titles, e.g. Mr, Ms. There are two fields available for titles.
- **Identification card** – person's identification card.
- **Internal number** – person's internal number. If the person has a parent company with the **Check primary key** field ticked, then each person in the company must have a unique internal number. See the "Check primary key" section on page 103.
- **External number** – person's external number

- **E-mail** – person's email address.
- **Gender** – person's gender.
- **Position** – person's position.
- **Valid from** – date that the person is valid from.
- **Valid to** – date that the person is valid to.

  Note: The Valid from and Valid to dates are not sent directly to Challenger10. If a person is valid as determined by the dates, then they will be set as a user on Challenger10. If a person is not valid as determined by the dates, then they will be removed as a user from Challenger10.

- **Long access** – whether the person requires extended access time for doors.

  Note: A user with the Long access option enabled will have the "Long Access" user flag set for them in Challenger10.

- **Note** – text field to add any relevant notes about the person.
- **Address** – person's street address.
- **City** – city of the person's address.
- **Post code** – post code of the person's address.
- **Country** – country of the person's address.
- **Phone** – person's phone number.
- **Mobile phone** – person's mobile phone number.
- **Photo** – person's photo. You can use the buttons on the side of the photo area to add a photo from file, delete an existing photo, or take a photo using the computer's web camera. The photo is used when printing cards.

Note: Contact information is not propagated to child nodes.

14.1.2 Persons panel: Events tab

The *Events* tab shows all events associated with the selected nodes of the Persons tree. See the "Events" chapter on page 124 for more information about the *Events* tab.

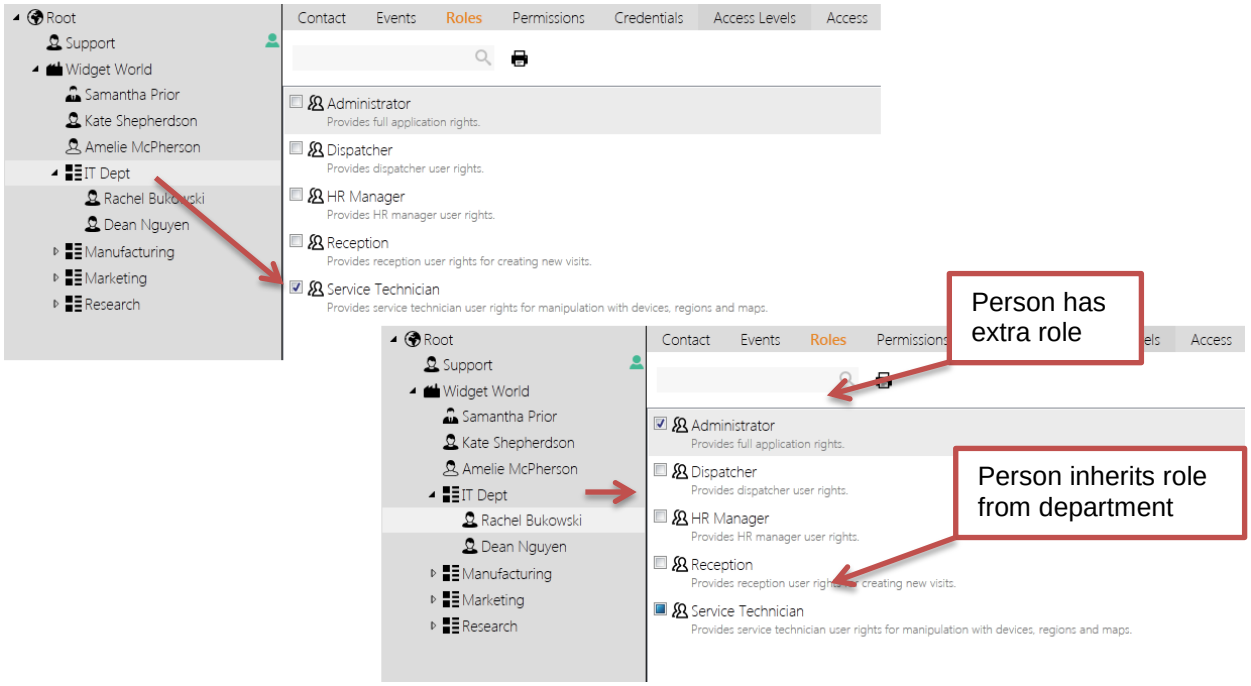
14.1.3 Persons panel: Roles tab

The *Roles* tab shows the roles assigned to the selected nodes of the Persons tree and all of their child nodes. A person's role determines their access to the TecomC4 system as an operator.

There are five preconfigured roles in TecomC4 (Administrator, Dispatcher, HR Manager, Reception and Service Technician). New roles can be created or the rights of existing roles can be changed. See the "Configuring operator roles" chapter on page 81 for more information on creating and editing roles.

Tick the checkbox ☑ next to each role to add the rights associated with the role to the selected node of the Persons tree (and all of its child nodes, if applicable). If a person inherits a role from a parent node, then the checkbox will be filled in: ■.

In the following example, the department has the Service Technician role, as indicated by the ☑ icon. The person inherits that role, as indicated by the ■ icon, and also has the Administrator role.



If multiple nodes of the Persons tree are selected and they have different roles, then the checkboxes will be filled in.

You can print a report listing the roles assigned to the selected organisational unit by clicking the **Print** button.

Note: Assigning persons to roles can also be done on the *Persons* tab of the Roles panel. See the “Roles panel: Persons tab” section on page 82.

14.1.4 Persons panel: Permissions tab

The *Permissions* tab shows operator permissions for the selected nodes of the Persons tree and all of their child nodes. If a person or other organisational unit has operator permissions determined by its role, then you can override specific operator permissions in this tab.

Note: In general, you should use roles to define operator permissions. If operator permissions are defined per person then a person’s set of permissions will be lost if they are deleted from the TecomC4 system.

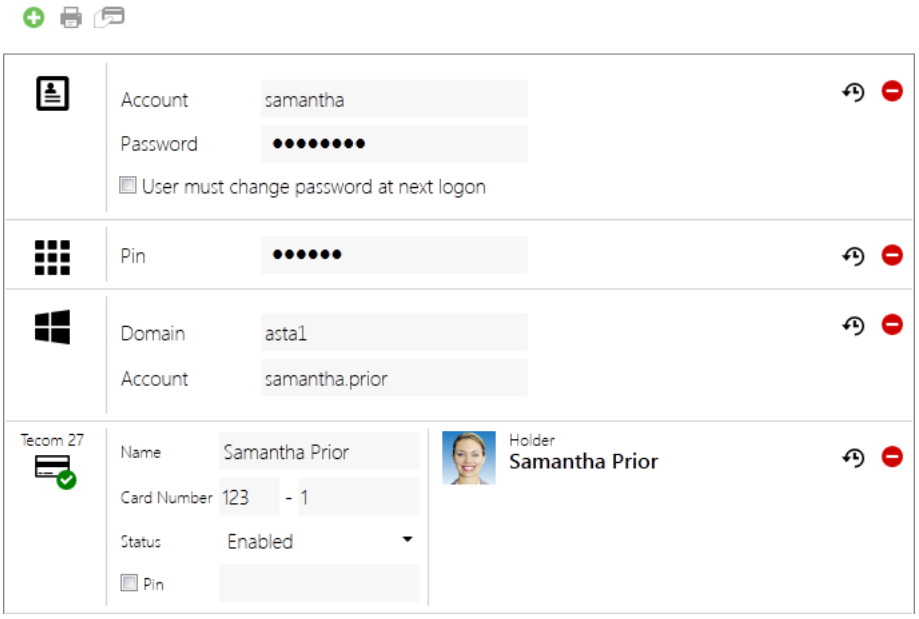
The format of the *Permissions* tab is the same as the *Permissions* tab on the Roles panel. See the “Roles panel: Permissions tab” section on page 83.

14.1.5 Persons panel: Credentials tab

Credentials define whether the person is an operator of the TecomC4 system or a user with access to the secure installation, or both.

If the selected node is an organisational unit other than a person, e.g. a department, then the *Credentials* tab shows a list of all cards assigned to persons under the selected organisational unit.

If the selected node is a person then the *Credentials* tab shows a list of all credentials assigned to the person. For example:



There is a toolbar with buttons to:

- **Add** a new credential
- **Print** a card layout if a card is selected in the credential list
- **Learn** a card from a card reader device.

Click the **History** button to expand the view of a credential to include its history, including times of use and, for user credentials, access points where it was used.

You can add operator credential types for a person to access the TecomC4 system as an operator. See the “Assigning operator credentials” section on page 105.

You can add the user credential types for a person to have access to the secure installation. See the “Assigning user credentials” section on page 106.

14.1.6 Persons panel: Access Levels tab

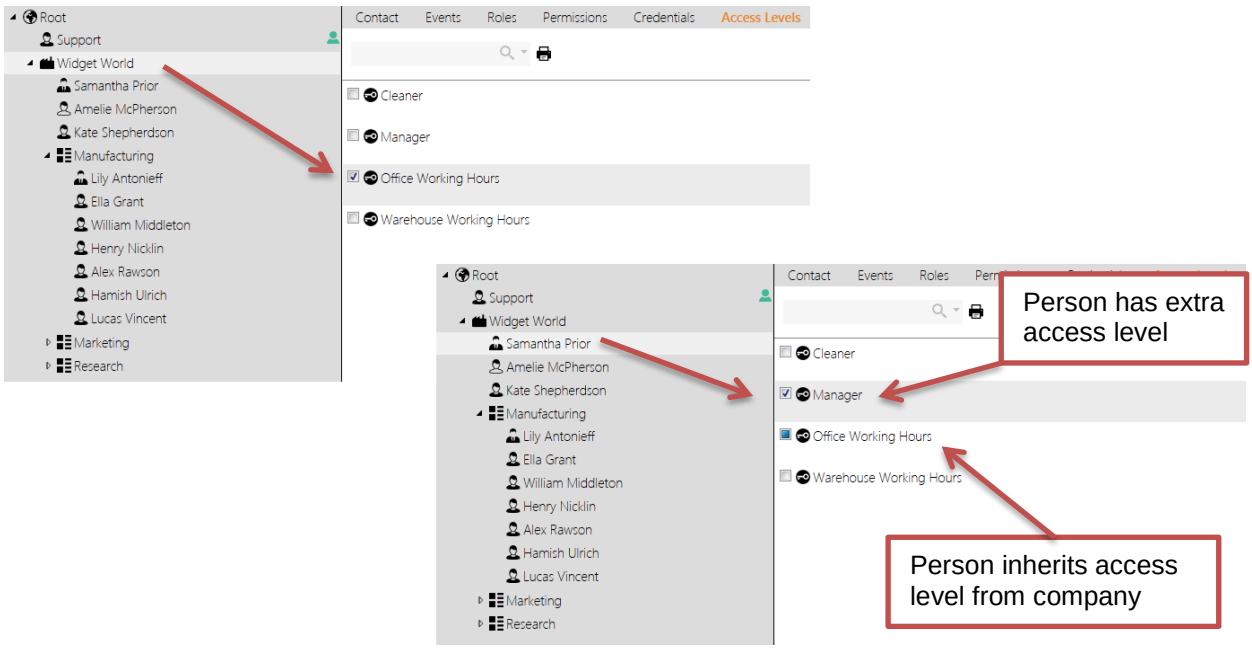
The *Access Levels* tab shows the access levels assigned to the selected node of the Persons tree and all of its child nodes. A person’s access level determines their access to the secure installation as a user.

Note: The *Access Levels* tab only appears if there is at least one access level defined.

See the “Configuring user access levels” chapter on page 71 for detailed information about access levels.

Tick the checkbox next to each role to add the rights associated with the access level to the selected node of the Persons tree (and all of its child nodes, if applicable). If a person inherits an access level from a parent node, then the checkbox will be filled in: .

In the following example, the company has the Office Working Hours access level, as indicated by the icon. The person inherits that access level, as indicated by the icon, and also has the Manager access level.



If multiple nodes of the Persons tree are selected and they have different access levels, then the checkboxes will be filled in.

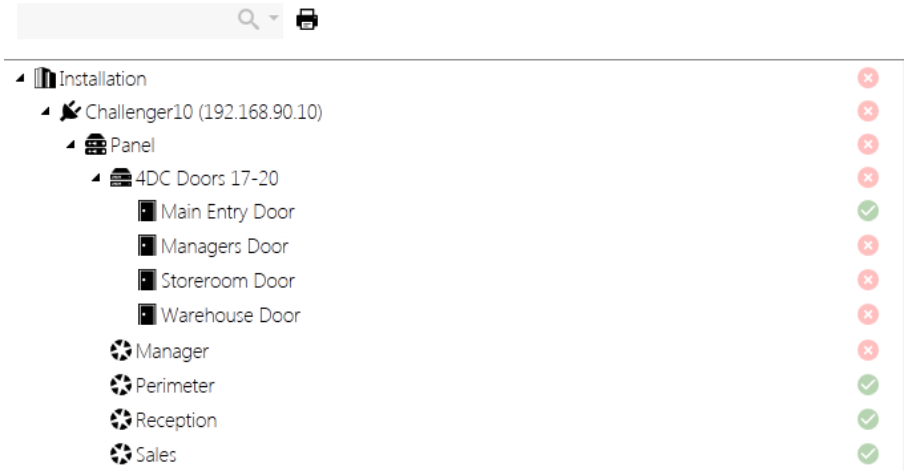
You can print a report listing the access levels assigned to the selected organisational unit by clicking the **Print** button.

Note: Assigning persons to access levels can also be done on the *Persons* tab of the Access Levels panel. See the “Access Levels panel: Persons tab” section on page 76.

14.1.7 Persons panel: Access tab

The *Access* tab shows the devices in the Devices tree and indicates whether the selected person has access to those parts of the secure installation.

For example:



You can click on the coloured circles to change the access for a device. Right-clicking a coloured circle opens a context menu with the following options:

- **Allow with inheritance** – The selected person is allowed access to the device and its child nodes.
- **Deny** – The selected person is denied access to the device and its child nodes.
- **Revoke** – Revoke specific access from the selected person for the device and its child nodes. Access reverts to that defined higher in the Devices tree hierarchy or as defined by the selected person's access level.

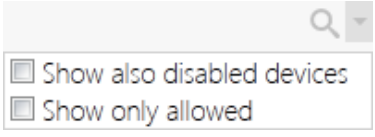
You can also click a coloured circle to cycle through the above options.

The possible colours for the coloured circles are:

- – access is explicitly allowed for the device
- – access is allowed for the device due to access being determined higher in the Devices tree hierarchy or by the selected person's access level
- – access is explicitly denied for the device
- – access is denied for the device due to access being determined higher in the Devices tree hierarchy or by the selected person's level

If you hover the mouse cursor over a coloured circle, a tooltip will be displayed with a list showing how access is decided for the device. The top entry in the list shows the deciding access permission.

By default, only enabled devices are shown in the Devices tree. You can filter the Devices tree by entering text in the filter above the Devices tree. You can also click the drop-down menu icon in order to also show devices that are not enabled or to only show devices for which the selected person has access:



See the “Form filter” section on page 16 for more information on the form filter.

You can print a report showing a matrix of information about access permissions for the selected parts of the Persons and Devices trees by clicking the **Print** button. See the “Generating access reports” section on page 80 for more information.

Note: It is recommended that you use access levels to define a user’s access instead of defining their access permissions directly on the *Access* tab.

Note: The persons who have access to devices can also be set on the *Access* tab of the Devices panel. See the “Devices panel: Access tab” section on page 30.

14.1.8 Persons panel: Persons Present tab

The *Persons Present* tab only appears if the **Counting Persons in Regions** extension is enabled. See the “Counting persons in regions” section on page 50 for more information.

The *Persons Present* tab shows a list of persons (under the selected node of the Persons tree) present in selected regions, with the following columns:

- **Time** – the time the person entered the region
- **Person** – the person who is in the region
- **Region** – the region
- **Door** – the door that the person used to enter the region

14.1.9 Persons panel: Settings tab

The *Settings* tab shows settings applicable to the selected node and all of its child nodes:

- **Startup Panel** – Select the TecomC4 panel to be shown when the operator logs in.
- **Enforce Fullscreen Mode** – Enforce fullscreen mode for the operator. The TecomC4 client fills the screen and no window border is shown.
- **Language** – Select the language to use in the TecomC4 client. Ensure that English (Australia) is selected since the language setting also includes region-specific terminology such as “Isolate”.
- **Time Zone** – Select the world time zone to use in the TecomC4 client. The default is the computer’s time zone.
- **Home Map** – Select the map displayed when you navigate to the Monitor panel. See the “Monitoring the system” chapter on page 111 for more information about the Monitor panel.

Note: The settings for the currently logged in operator can be changed by clicking the operator’s photo at the top right of the TecomC4 screen.

14.2 Person status icons

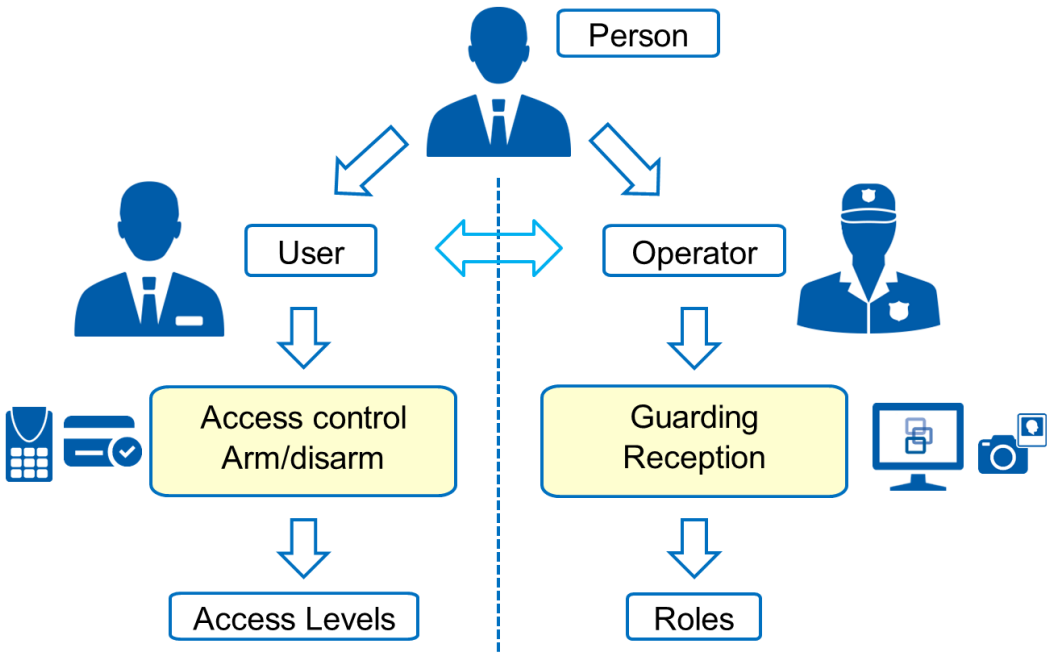
While working with the person tree, you may encounter the following person status icons next to nodes in the tree:

- – Person is online, i.e. logged into a TecomC4 client as an operator.
- – Person is not enabled (according to their start and end dates). The person cannot access the secure installation as a user or log into the TecomC4 system as an operator.
- – Person is on premises. This can only appear if counting persons in regions is enabled. See the “Counting persons in regions” section on page 50 for more information.
- – Person is archived. See the “Archiving, restoring and deleting nodes” section on page 13.
- – Person data has an error.

14.3 Users vs Operators

Users are persons in the TecomC4 system that can have physical access to the secure installation via a card or other credential. **Operators** are persons in the TecomC4 system that can login and operate the TecomC4 system.

Figure 5: Persons, Users and Operators



In order to grant access to a user you must assign them a user credential, such as a card or PIN, as well as access to at least one access point, such as a door or area, in the secure installation. The parts of the secure installation that a user can access are determined by the user’s **access level**.

In order to grant access to an operator you must assign them an operator credential, such as a login account to TecomC4. The parts of TecomC4 that an operator can see, and the actions they can perform are determined by the operator's **role**.

Note: A person can be both an operator and a user.

14.4 Creating an organisational structure

The organisational structure is created by adding individual organisational units to the Persons tree. The root of the Persons tree is called the Root node. Organisational units can be created from this node.

14.4.1 Creating an organisational structure manually

To manually create a basic organisational structure, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Right-click the Root node in the Persons tree to open its context menu. Select the **Add > Company** menu item to create a new Company node.
3. Enter the company's contact details in the node's record form.
4. Right-click the company in the Persons tree to create the required divisions, departments, and centres. These elements symbolise smaller organisational units for more transparent placement of employees according to their work responsibilities or locations.
5. In the Persons tree, right-click the organisational unit under which you want to create a new person. Select the **Add > Person** menu item and select the person type to be created.

   Note: The person type (Manager/Person/External Employee) can be used to aid the operator; it has no effect on the functionality of TecomC4.

6. Enter the created person's contact details in the record form. Click the **Add** button to assign a photo or click the **Delete** button to delete the person's existing photo. The supported photo formats are .png, .jpg, .jpeg, and .gif. It is also possible to capture the photo by means of a web camera (if available) when you click the **Take photo** button.

The system contains controlled hierarchy support, which means it verifies what type of nodes can be created at the given tree node. This is reflected in what is available in the context menu when adding a new organisational unit.

The system allows the creation of multiple companies in the tree. When adding persons into individual companies, one person cannot be assigned to two or more companies. However, the added person can be transferred between companies or other organisational units.

14.4.2 Importing persons and credentials from file

An organisational hierarchy can be imported from a CSV file. The CSV file may have been previously exported from TecomC4 (say, on a different TecomC4 server) or created through a third-party application. The import CSV file can also contain credential information for persons.

See the “Importing data from a CSV file” section on page 14 for information on importing data from a CSV file, keeping in mind the following points:

- If importing a hierarchy into the Persons tree, the import CSV file must contain a column that can be mapped to the “Parent” target field. Each record in the import CSV file should have the “Id” of the record’s parent in the hierarchy in that column.

  The import CSV file must also contain a column that can be mapped to the “Category” target field. The following are the valid values for entries in this column:

  - **Company** – company
  - **Division** – division
  - **Center** – centre
  - **Department** – department
  - **ManagerEmployee** – manager
  - **Person** – person
  - **ExternalEmployee** – external employee

  The combination of “Parent” and “Category” must also be valid in terms of the hierarchy. For example, a Department could not have a Person as a parent.

  If no category is specified in a record of the import CSV file, then the record is imported as a Person.

  The category of the root of the hierarchy to be imported must be valid for the intended target node of the Persons tree. For example, you cannot import a hierarchy whose root is a Company into a Department node in the Persons tree.
- To import PIN codes, the import CSV file must contain a column that can be mapped to the “PIN” target field. Multiple PIN codes can be separated with a vertical bar “|” character in the import CSV file. Imported PIN codes must not already exist in the TecomC4 system and must meet any validation rules set for PIN codes (see the “Configuring validation rules for credentials” section on page 65 for information on validation rules).
- When cards are imported, the import CSV file must contain columns that can be mapped to the “Card name” and “Card code” target fields. If the card type has a facility code and/or an issue code then the import CSV file must contain columns that can be mapped to the “Facility code” and “Issue code” target fields, respectively.

- You can import multiple cards per person, as long as the requirements in the point above are met for each card. The cards must be of the same type.
- If cards have an associated extension PIN, then the import CSV file must contain a column that can be mapped to the “Extension PIN” target field.
- If there is more than one card deck defined in TecomC4, then you will have the opportunity to select which card deck the imported cards should be added to.
- If there is more than one card type defined in TecomC4, then you will have the opportunity to select the card type of the imported cards. All cards imported must be of the same type.
- If you want to assign access levels to imported persons, then the import CSV file must contain a column that can be mapped to the “Access Levels” target field. Entries in this column must be the names of access levels which already exist in the TecomC4 system. Multiple access levels can be separated with a vertical bar “|” character.

  Note: If there are no access levels assigned to a person in the import CSV file and the person already exists in the TecomC4 system, then any existing access levels assigned to the person will not be cleared.

- If you want to assign roles to imported persons, then the import CSV file must contain a column that can be mapped to the “Roles” target field. Entries in this column must be the names of roles which already exist in the TecomC4 system. Multiple roles can be separated with a vertical bar “|” character.

14.4.3 Check primary key

The system allows the enforcement of a unique primary key for persons within a Company. This means that no two persons in the company can have the same internal number. To enable this functionality, select the company in the Persons tree and tick the **Check primary key** checkbox on the company’s *Contact* tab.

If some persons have the same internal numbers and this function is turned enabled, the persons will be flagged with an exclamation mark icon. The information bar also appears to indicate an invalid configuration. The conflicting internal number is also indicated by a red frame in the internal number field on the person’s *Contact* tab.

14.4.4 Deleting an organisational unit

The system supports the two-step deletion of an organisational unit with the aim of preventing accidental deletion of important data. Right-clicking on a node in the Persons tree and selecting **Archive** from the context menu will archive the selected node (including its child nodes if applicable).

The following applies to the archived nodes:

- The structure of the deleted part of the tree is preserved.
- Upon next access synchronization, persons will be removed from connected devices.

- The persons' accounts to access the TecomC4 application as operators will be blocked.
- You can search the event history of archived nodes.
- The modification of archived nodes and their structure is not allowed.
- The export/import operations ignore the archived content.

To show archived nodes in the Persons tree, select the **Show archived persons** filter option from the drop-down menu in the record filter. After the archived nodes are shown in the Persons tree, they can be restored by right-clicking on a node and selecting the **Restore** menu item from its context menu.

When a part of the tree is to be restored, either a full branch of the tree (using multiple selection) or the hierarchically highest archived level can be restored. For example, the system does not allow a person to be restored if the person's parent department remains archived.

The restored nodes are placed back in their original position in the hierarchy. It is also possible to restore a node with all of its child nodes by selecting the **Restore with children** menu item from its context menu.

To permanently remove a node from the system, right-click the archived node and select the **Delete** menu item from its context menu. The node will be permanently removed from the system including all child nodes and complete history.

Warning: Permanent deletion is irreversible and the data about the deleted node is lost, so this action should only be carried out with the approval of an authorized person.

14.5 Assigning an operator

A person that exists in the system can be assigned a login account to become an operator of the TecomC4 application. Using complex permission management, the person can be given permissions for those parts of the application that they need to use based on their work responsibilities. The person's access to the other parts of the application can be denied to prevent possible misuse of TecomC4 data.

Granting access to the TecomC4 system consists of the following general steps:

1. Assigning operator credentials to a person
2. Assigning roles and permissions to the operator
3. Installing the TecomC4 client on the operator's computer and logging in to the operator account

The following sections contain a detailed description of how to grant system access for a TecomC4 operator.

14.5.1 Assigning operator credentials

To assign operator credentials to a person, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Click on the person in the Persons tree to whom you want to assign the operator account.
3. On the *Credentials* tab in the person's form, click the **Add** button to add one of the following credential types:
    - **Forms Authentication** – Enable access to the TecomC4 client using the specified operator account name and password. This authentication type is a regular login when the operator account name and password are stored in the TecomC4 database. Enter the required account name and password. Upon entering the password, the system checks its strength based on built-in security algorithms. The password is considered strong enough when the green tick symbol appears after the password. Enter the password again in the **Confirm password** text box. Click the **Change** button to confirm the new password. You can also tick the **User must change password at next logon** checkbox to force the operator to change their password at their next login.
    - **Windows Authentication** – This login method uses the password defined for logging in to Windows as the account password. For a local Windows account, enter the account the operator will use to log in. For a domain account, also enter the name of the domain to which the operator belongs.
4. Select the person's required personal setting on the *Settings* tab, such as the startup panel and language.

This procedure has created a TecomC4 operator account for the person. However, once logged in, the person will not be able to perform any operations due to missing permissions. Therefore, proceed with defining permissions based on the operator's responsibilities.

14.5.2 Assigning operator roles

After the operator is granted access to the TecomC4 application, it is recommended that you assign a role with specified permissions to access the required sections of the TecomC4 system based on the operator's responsibilities.

See the "Creating a role" section on page 88 for instructions on creating a role.

Note: It is possible to assign simple access permissions to an individual user without using roles. This can be done from the *Permissions* tab of the Persons panel. However, it is recommended that access levels be used to define operator permissions since it allows you to transparently manage permissions for groups of operators.

To assign an existing role to the operator, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Click on the person in the Persons tree to whom you want to assign the operator role.
3. On the *Roles* tab, tick the checkboxes next to the roles that you want to assign to the operator.
4. If you wish to override specific role permissions for the operator, go to the *Permissions* tab and change the required permissions. For detailed information on permissions, see the “Role permissions” section on page 83.

Note: The final permissions for an operator are a result of inheriting and setting permissions. The setting at the lowest level of the hierarchy has the highest priority: organisational structure > role > person. Thus, the permission setting for a person has the highest priority, overriding permissions for higher in the organisational structure or from the person’s role.

14.5.3 Installing the TecomC4 client

See the *TecomC4 Installation Manual* for instructions on installing the TecomC4 client on the operator’s computer.

14.6 Assigning a user

Granting access to the secure installation consists of the following general steps:

1. Assigning user credentials to a person
2. Assigning user access to the person
3. Synchronizing access information with devices

The following sections contain a detailed description of how to grant access to the secure installation for a user.

14.6.1 Assigning user credentials

To assign user credentials to a person, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Select the person in the Persons tree to whom you wish to assign the credential.
3. On the *Credentials* tab in the selected person’s form, click the **Add** button to add one of the following credential types:
   - **Pin** – Enter a unique PIN code in compliance with the validation criteria (see the “Configuring validation rules for credentials” section on page 65 for more information on the validation criteria.

     Note: The PIN must be at least 4 digits long.

Note: PIN codes longer than 10 digits will not be sent to a Challenger10.

- **Fingerprint** – A fingerprint can be associated with the person. Fingerprints can only be added if there is a fingerprint reader device present in the TecomC4 system and a fingerprint type is enabled in the Credential Types panel. After creation, the **Card Number** field is filled in automatically. Displayed squares represent individual fingerprints. Click one of them, select a fingerprint reader and read the fingerprint.

  Note: Fingerprints are not supported by Challenger10.

- **Card** – A new window will open showing the list of unassigned cards available in the system. Select the required card and click the **Assign** button to assign the card to the selected person.

  To view already assigned cards, you can click the drop-down menu icon next to the filter in the window and enable the **Include assigned cards** option. This will allow you to reassign a card from an existing user.

  To assign a card from the window, select a card and click the **Assign** button.

  If the required card is not yet present in the system, you can create it by clicking the **Create new card** button. A new window appears where you must select the card deck to which the new card will be stored. When selected, click the **OK** button. Next, specify the format of the new card and click the **OK** button.

  Note: These settings are not shown if there is only one card deck in the system or only one card format is in use.

  Enter the required card parameters (based on the card format) such as the facility code, issue code and card number.

  By ticking the **Pin** checkbox you can add an extension PIN, which will have to be used when combined authentication is set on a card reader.

  Warning: Extension PIN codes are not supported by Challenger10. Do not use.

  Warning: The extension PIN can be a duplicate of an existing PIN or extension PIN. The extension PIN is not checked against the credential validation criteria.

Warning: PIN codes will remain assigned to a person within TecomC4 even after the person is archived (but the person is removed as a user from any connected Challenger10). Therefore, the TecomC4 system does not allow the same PIN code to be assigned to another person as long as the original PIN holder is present in the database. The PIN code will be released when the original holder is permanently removed from the system. An alternative method is to cancel the PIN code for the original holder before the person is archived.

Note: If you assign a card and a PIN to the same person, then TecomC4 will assign them to a single user in Challenger10.

Warning: If more than one card or PIN is assigned to a single person in TecomC4, then more than one user will be created in Challenger10. In this case, it is not possible to determine which PIN or card is associated with which Challenger10 user from within TecomC4.

14.6.1.1 Card learning

To speed up assignment of new cards in a TecomC4 system, it is possible to load cards directly from a card reader device, by simply swiping cards through the reader.

Note: If you want to learn cards at a card reader attached to a Four-Door Controller, the card reader must be set as an IN reader.

Follow these steps to learn cards:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Select the person in the Persons tree to whom you wish to assign the credential.
3. On the Credentials tab, click the **Learn card** button. The button will turn blue with a blue line underneath to indicate that card learning mode is active.
4. A new window showing the Devices tree will open. Select the card reader to be used to swipe the card and click the **OK** button.
5. A new entry appears in the list of credentials, indicating that the system is waiting for the card to be swiped at the reader.

   If you have more than once card deck defined in the system, you can change the card deck that the new card will be added to by clicking the name of the card deck in the credential entry. A new window will open with a list of the card decks in the system. Select the required card deck and click the **OK** button.
6. Swipe the card through the card reader. The card will be loaded into the system and the card number will be filled in automatically.
7. When finished, click the **Learn card** button again to exit card learning mode.

Warning: If you load a card that is already present in TecomC4 and not assigned to anybody, it will be assigned to the selected person. If the card has been assigned to somebody, it will be removed from that person and assigned to the selected person.

Note: You must have exactly one card type enabled for the connected card reader device. See the “Configuring card types on security devices” section on page 65.

Note: The card learning functionality is supported only if the card reader device sends the card code to the TecomC4 system.

14.6.2 Assigning user access

See the “Creating an access level” section on page 77 for instructions on creating an access level.

Note: It is possible to assign simple access permissions to an individual user without using access levels. This can be done from the *Access* tab of the Persons or Devices panels. However, it is recommended that access levels be used to define user access since it allows you to transparently manage access for groups of users.

If you assign simple access permission to a user, their access may be restricted if they have an access level with a calendar restriction for the access point. To ensure unrestricted access, set up an access level with a calendar with all days ticked and the time set from 00:00:00 to 23:59:59.

To assign an existing access level to the user, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Persons** to open the Persons panel.
2. Click on the person in the Persons tree to whom you want to assign the access level.
3. On the *Access Levels* tab, tick the checkboxes next to the access levels that you want to assign to the user.
4. If you wish to override specific access permissions for the user, go to the *Access* tab and change the required permissions.

Note: If the TecomC4 system receives an access denied event for a person known in the TecomC4 system, you can easily grant access for this person to the access point by right-clicking on the event.

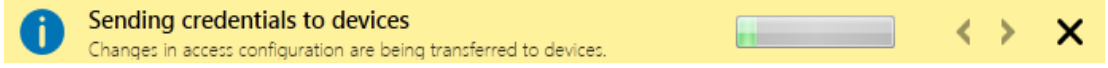
14.6.3 Sending access information to devices

TecomC4 detects all changes made to user access permissions.

If an access-related change occurs (such as adding a user credential to a person or changing a user’s access permissions), TecomC4 will display a notification in the information bar that synchronization of access information to security devices is required.

The operator can click the **Resolve** button on the information bar to confirm immediate synchronization of access information to all connected security devices. Alternatively, the operator can click the **Postpone** button on the information bar if more access-related changes are anticipated.

The information bar will display a progress bar while synchronizing access information:



If access information is currently being sent to a device, then the synchronization status icon will be shown next to the device in the Devices tree on the Devices panel.

You can check the result of the last synchronization to a Challenger10 by selecting the Panel element of the Challenger10 device in the Devices tree on the Devices panel. At the bottom of the *General Settings* tab the result of the last synchronization is shown. See the “Challenger10 panel settings” section on page 28.

Note: You can send access information changes to individual Challenger10 panels by running the **Send Panel Access Changes** command. See the “Sending credentials and access information to devices” section on page 43 for more information.

Note: If you remove a person as a user from TecomC4 by archiving the person, removing all their user credentials or removing all of their access to the secure installation, then synchronizing access information with a Challenger10 will delete the user from the Challenger10. Similarly, any unused alarm groups, door groups etc. will be deleted.

Note: Upon first setting up a TecomC4 system and connecting to Challenger10 devices, you should run the **Send All Credentials** command on each Challenger10 device instead of synchronizing access from the information bar. This ensures that the user information on the Challenger10 is synchronized with TecomC4. See the “Sending credentials and access information to devices” section on page 43 for more information.

---

15 Monitoring the system

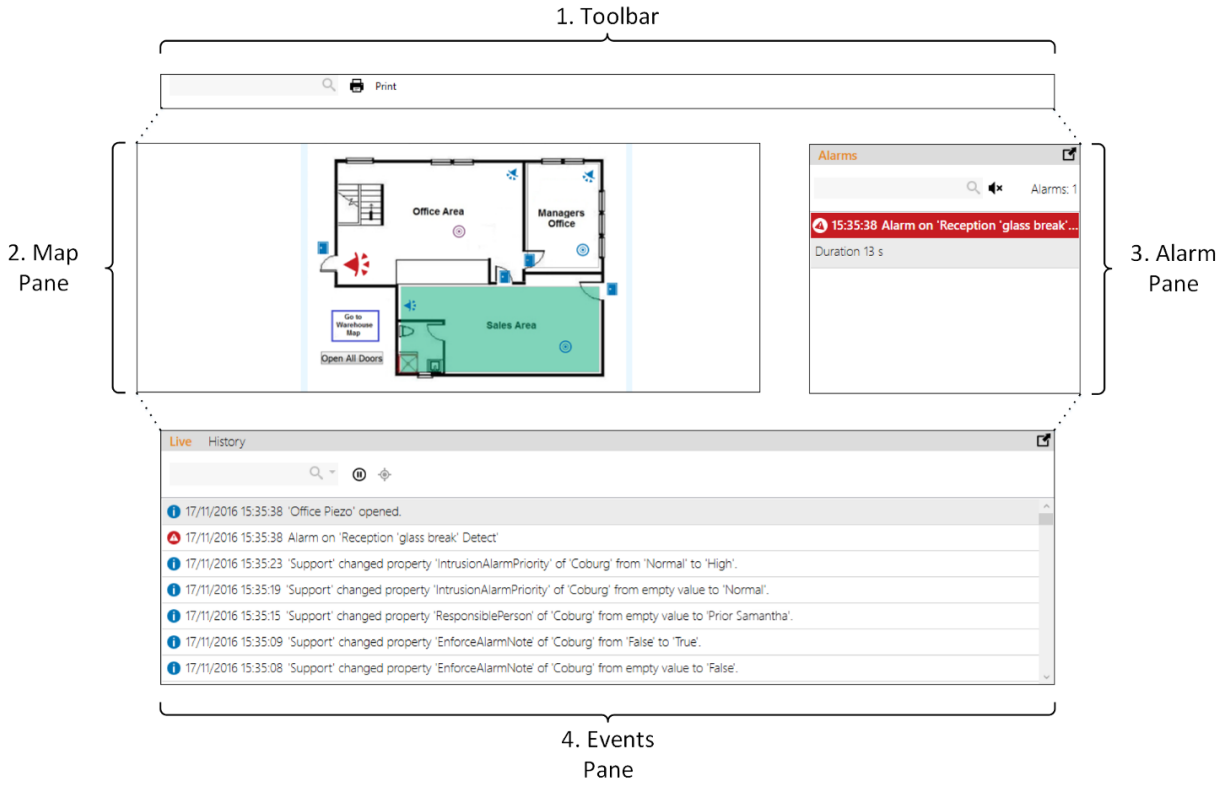
The Monitor panel is the main panel used for ongoing monitoring of a TecomC4 system. The Monitor panel provides an operator with constant surveillance of the security of the system, a real-time overview of the statuses of all connected devices, the remote control of devices, and the ability to deal with alarms.

The Alarms panel can be used to view a history of alarms.

15.1 Monitor panel

The Monitor panel can be opened by clicking the **Navigation** button and selecting **Monitor** from the Visualization menu.

Figure 6: Elements of the Monitor panel



The monitor panel contains the following elements, numbered in the figure above:

1. **Toolbar** – search and print functionality
2. **Map pane** – displays maps with visualized devices and other objects, allowing them to be controlled remotely.
3. **Alarms pane** – displays current alarms
4. **Events pane** – has tabs to display a live event log or an event history log

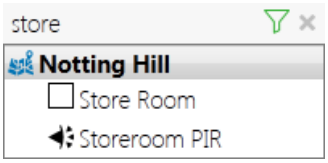
15.1.1 Navigating between maps

There are several ways to navigate between maps:

- The home map (the first map opened when an operator navigates to the Monitor panel) can be set for the operator. See the “Persons panel: Settings tab” section on page 99.
- On the navigation bar where the current panel name usually is, there is a drop-down menu of available maps from the operator’s home map. Select the required map to open it.
- To the left of the currently opened map, recently opened maps are listed, which you can access by clicking the respective map name.
- You can use links to other maps created during the visualization (see the “Adding map links” section on page 57). If a link to another map has been defined for a map object, upon hovering the mouse cursor over the object a hand-shaped icon is shown to indicate the option to switch to the other map.

15.1.2 Toolbar

The toolbar has an entry box for searching for maps and elements visualized on them. For example:



The Print button can be clicked to print a report on isolated devices in the TecomC4 system.

15.1.3 Events pane

The events pane has two tabs: *Live* and *History*.

The *Live* tab displays events that have recently been received by the TecomC4 system. You can click on parts of an event (such as a person’s name) to see more information (such as a person’s photo).

The *Live* tab displays events as they occur. New events appear at the top of the list. You can temporarily suspend receiving events in order to analyse a particular event by clicking the **Suspend** button. The button will now have a blue line underneath it. Restart the receiving of events by clicking the **Suspend** button again. All events that have occurred during the suspended period will be shown.

If a selected event is related to an object on a map, you can navigate to the map by clicking the **Go to map** button.

The *History* tab allows you to search past events related to devices on the currently viewed map.

Note: Only events relating to devices that are present on the currently viewed map are shown on the *History* tab.

The events pane can be popped out of the main TecomC4 window into a separate movable window by clicking the **Popout** button. The window can be moved around the screen or moved to a second screen. To lock the window back in the main TecomC4 window, close the window.

15.1.4 Alarms pane

The alarms pane will be displayed if the system receives an alarm event. The Alarms Processing extension must also be enabled (see the “Enabling alarms processing” section on page 113). The alarms pane is shown if there are any unresolved alarms in effect. After all alarms are resolved, the window closes automatically.

Alarms are sorted in the alarms pane by their priority. See the “Adding region assets” section on page 49 for instructions on setting alarm priorities for a region.

For a detailed description of alarms management, see the “Dealing with alarms” section on page 114.

The alarms pane can be popped out of the main TecomC4 window into a separate movable window by clicking the **Popout** button. The window can be moved around the screen or moved to a second screen. To lock the window back in the main TecomC4 window, close the window.

15.1.5 Map pane

The map pane shows the current map and its objects, such as devices, buttons and map links.

The map pane can be used to control devices remotely, i.e. run commands on devices. Control is similar to using the Devices tree. Right-click a device on the map to open its context menu. Then select the required command from the **Commands** menu.

Left-clicking a map object such as a device will execute the defined command for the object. See the “Command editor” section on page 61 for defining commands for map objects.

15.2 Enabling alarms processing

In order for an operator to be able to deal with alarms, the alarms processing functionality must first be enabled in the TecomC4 system settings:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.

2. Tick the **Alarms Processing** extension.
    - If you expand the extension details by pressing the expand button, you can also set the options for alarm escalation:
        - **ACK Escalation Time** – the time (in seconds) within which an alarm must be acknowledged before being escalated, if the following option is enabled
        - **Timed Alarm Escalation Enabled** – whether to enable escalation of alarms if not acknowledged within the time set above

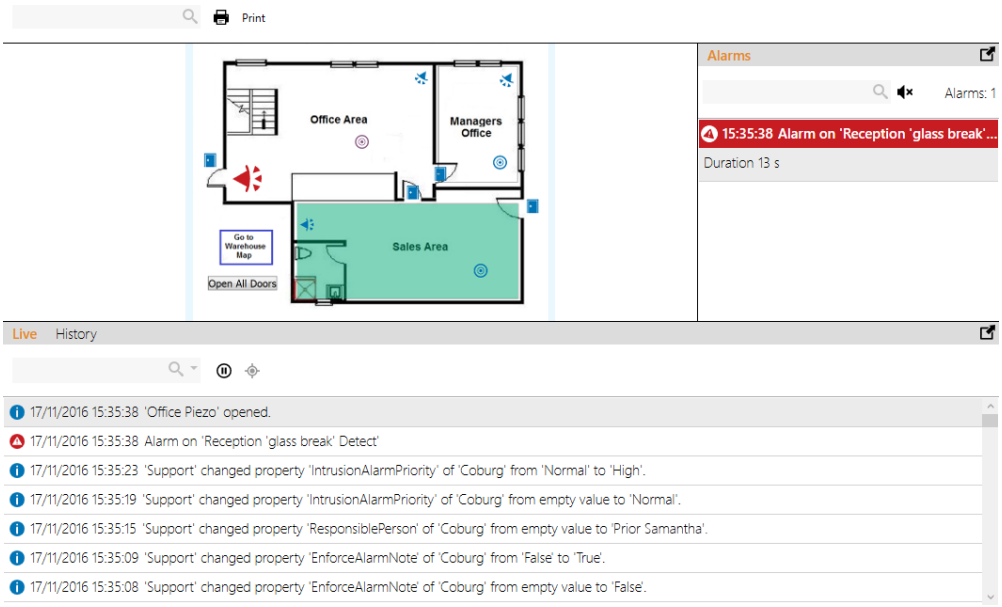
15.3 Dealing with alarms

Operators of the TecomC4 security system are typically not required to deal with all events. They typically only deal with critical events, such as alarms and errors reported by devices. Dealing with alarms combines the recording of critical events with the recording of actions required for their resolution. Dealing with alarms can be done from the alarm pane on the Monitor panel.

The following process describes how to deal with alarms:

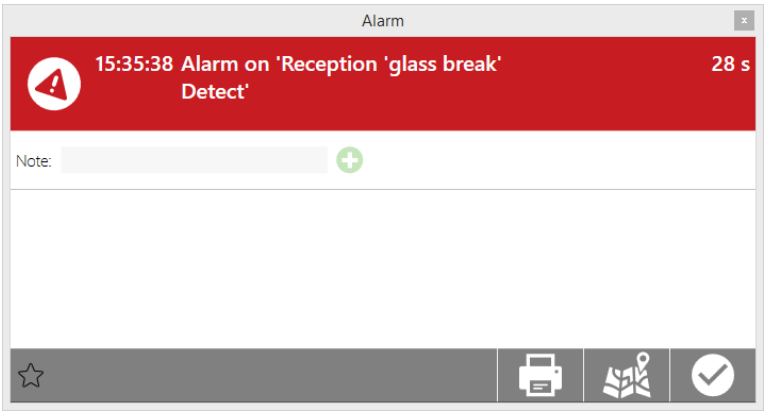
1. A critical event occurs in the system. The alarms pane is automatically displayed and a new entry describing the critical event appears in the list. Inputs in alarm will flash colour and pulse in size.

    For example:



    An audible alert also sounds to draw attention to the occurrence of the alarm. To mute the audible alert, click the **Mute** button. Click the button again to resume the audible alert.

2. Click the event in the alarms pane to open the alarm details window.



3. Click the **Accept alarm** button to register that you have acknowledged the event and will deal with it. After the alarm is confirmed, the entry in the alarms pane is greyed out to show other operators that the alarm is already being dealt with. A note about the time of alarm acknowledgement with the name of the operator responsible for it is automatically recorded. Every alarm can be acknowledged only once.

   The alarm window displays the following information:

   - **Duration** – The duration of the alarm starting from the first occurrence of the alarm even.
   - **Count** – The alarm count. If the same alarm event occurs at the same device while dealing with the previous alarm event, these alarm events are grouped into one alarm and the alarm count increases. If the operator turned off the alarm's audible alert after the alarm occurred, another occurrence of the alarm is only signalled by a short beep instead of the standard alarm audible signal.
   - **Note** – If necessary, notes can be entered for the alarm, such as the method of resolving the alarm and the result of reviewing the critical situation. To add a note, click the **Add** button. It may be required to enter a note before the alarm can be resolved. This can be set for each region on the *Assets* tab of the Regions panel by ticking Enforce Alarm Note. See the “Adding region assets” section on page 49.
   - **Accepted by** – The time and name of the operator that acknowledged the alarm.
   - **In** – The region in which the alarm occurred.
   - **Responsible persons** – The person responsible for the region in which the alarm occurred. This can be set for each region on the *Assets* tab of the Regions panel by selecting a Responsible person and a Deputy. See the “Adding region assets” section on page 49.
   - **Persons count** – The number of persons present in the region in which the alarm occurred. The counting persons in regions functionality must be enabled. See the “Counting persons in regions” section on page 50.

You can perform the following actions in the alarm window:

- Click the **Print** button to print a report on the alarm.
- Click the **Go to map** button to open a map showing the device from which the alarm event originated.
- If the alarm occurred on a device element linked with a camera, you can click the **Camera** button to watch the video feed from the camera. See the “Linking cameras to devices” section on page 45 for instructions on linking a camera to a device.
- Click the Star button to star the alarm. Starred alarms can be seen on the Alarms panel in the Starred Alarms section. See the “Viewing alarms history” section on page 116.

4. After the critical situation is resolved, click the **Resolve alarm** button in the alarm window. A note will be added to the alarm about the time of alarm resolution and the name of the operator responsible for it. The alarm will be removed from the alarms pane of the Monitor panel. If it is the last alarm in the window, the alarms pane will close automatically. If the alarm has been resolved by another operator in the meantime, the **Resolve alarm** button disappears to prevent the alarm from being resolved again.

   Note: If a note is required before the resolution of the alarm, the **Resolve alarm** button will be greyed out until a note is added.

Default types (i.e. priorities) for each event are set in the TecomC4 system. If necessary, these types can be modified to match customer needs. See the “Changing event types” section on page 126 for instructions on changing event types.

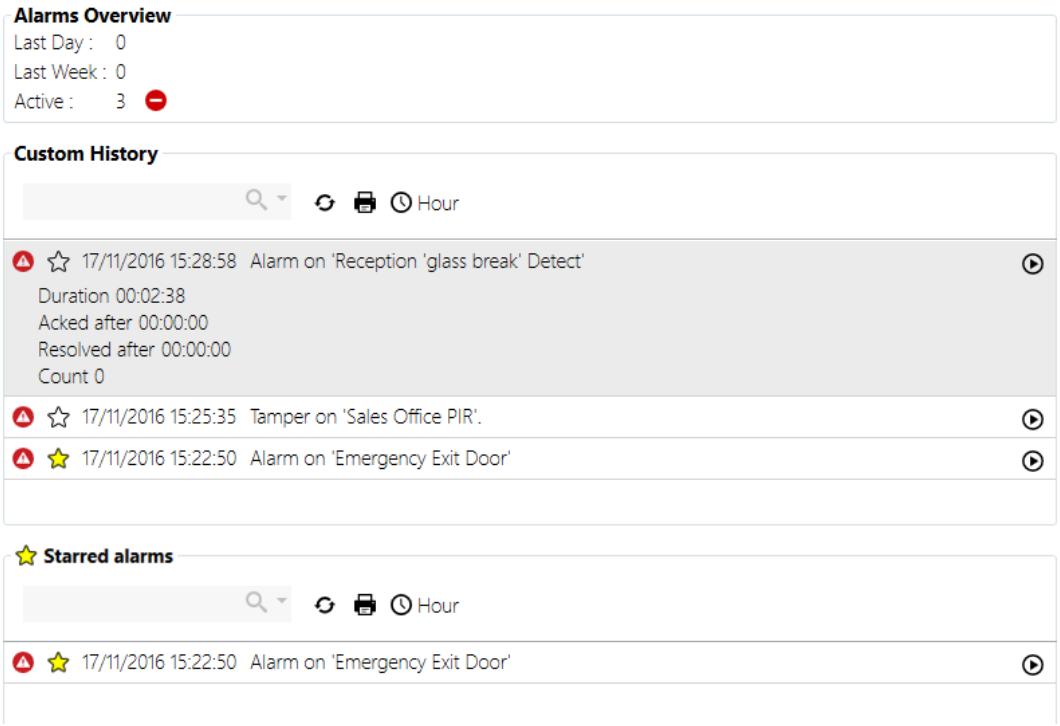
Note: If supported by both the device and the driver, the receipt of an alarm in TecomC4 also mutes the alarm on the device. When the alarm is resolved, it will also be resolved on the device.

15.4 Viewing alarms history

Operators deal with current alarm situations in the Monitor panel. However, it is sometimes necessary to review the resolution of an alarm. Resolved alarms can be reviewed on the Alarms panel.

The Alarms panel can be opened by clicking the **Navigation** button and selecting **Alarms** from the Security menu.

The Alarms panel looks like this:



The **Alarms Overview** section contains an overview of resolved and active alarms for the recent period. Click the **Cancel** button to cancel all active alarms.

In the **Custom History** section, you can view the list of alarms currently being dealt with.

In the **Starred Alarms** section, you can view the list of starred alarms. This section will only be displayed if there are starred alarms.

To display a detailed overview of an alarm, you can double-click on an alarm entry in the Custom History or Starred Alarms section, or click the **Details** button to display a detailed overview of the alarm with the following additional information:

1. **Notes** – notes added by the operators while dealing with the alarm. To add more notes to the alarm, click the **Add** button.
2. **Events** – events from devices related to the alarm are shown. Events from the occurrence of the alarm up to its resolution are shown.
3. Click the **Print** button to print a complex alarm report.
4. Click the **Star** button to star the alarm.
5. Click the **Back** button to return to the basic view of the list of alarms.

15.5 Video wall

A video wall is a display window designed to display images from camera systems. It can be used to display a live camera feed, to play recorded footage from connected recorders or to control rotary cameras.

15.5.1 Live video display

You can open a live camera feed by selecting a camera in the Devices tree and right-clicking it to open its context menu and selecting the **Commands > Show Live Video** menu item. The TecomC4 system allows the opening of a live feed from several cameras at the same time (but only from cameras of the same type in the Devices tree).

The camera feed is opened in the **CCTV Wall** panel. When more than one camera is opened, various panel display modes are available.

By default, the Full+3 mode is selected, where the recently opened camera is displayed in a large window and other possible cameras in three small windows. Click the **Enlarge** button to move a camera from a small window to the main window. Click the **Close** button to close the camera feed.

You can switch the display mode by clicking the **Full+3**, **2x2** and **3x3** tabs.

You can use the F11 key to display the CCTV Wall panel in full screen. You can exit the full screen view by pressing F11 again.

The following controls may also be available depending on the connected camera device's options:

- – Activate the TecomC4 client computer’s microphone and transmit sound to the camera. Click again to disable the transmission of sound.
- – Adjust the volume of the sound signal from the camera.
- – Mute and restore the playback of sound from the camera.
- – Save the current video frame to a file.
- **Stream name** – Use this option to select the camera stream to play, which can decrease the data rate transmitted over the network or improve the quality of the displayed video.

15.5.2 Playing back video footage

You can play back recorded video by selecting a camera in the Devices tree and right-clicking it to open its context menu and selecting the **Commands > Show Recorded Video** menu item. Enter the date and time from which the playback of video footage should start.

The CCTV Wall panel is displayed where you can control video footage playback with the following controls (their function may be limited by the communication protocol of the camera system):

- – Use the slider bar to move the video footage in time
- – Use the arrows to control playback direction, stopping or frame-by-frame playback
- Playrate 1 – Use the **Playrate** menu to set the playback speed
- – Use the slider to set the volume of the sound being played back
- – Mute and restore the playback of sound in the footage

- – Save the recording from the recorder to the TecomC4 client computer
- – Save the current video frame to a file

15.6 Access guard

The Access Guard functionality allows an operator to monitor the card usage of up to two doors at once. Access Guard also allows for random alcohol testing of users.

15.6.1 Enabling access guard

The access guard functionality can be enabled in the TecomC4 system settings:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Access Guard** extension.
    - If you expand the extension details by pressing the expand button, you can set the **RandomCheckProbability**, which specifies the percentage probability that a user will be flagged for checking their alcohol level.

15.6.2 Access Guard panel

The Access Guard panel can be opened by clicking the **Navigation** button and selecting **Access Guard** from the Visualization menu.

You can add up to two doors in the Access Guard panel. To add a door, follow these steps:

1. Click the **Add** button to display the Devices tree in a new window.
2. Select a door from the Devices tree and click the **OK** button to add it to the Access Guard panel.

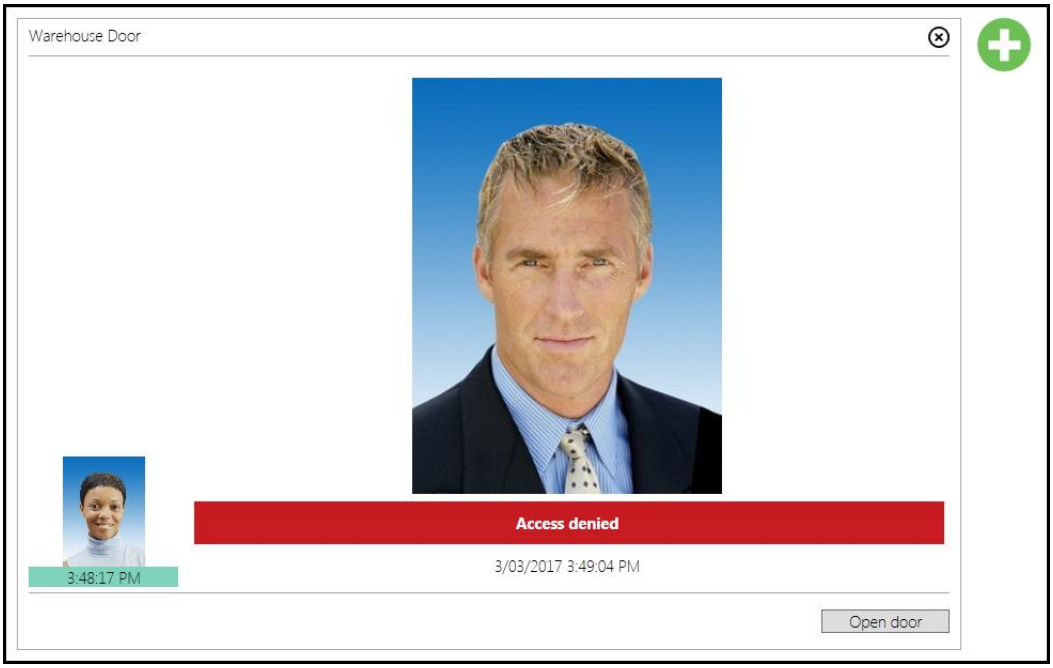
The door will appear in a new pane within the Access Guard panel. You can click on the **Remove** ⊗ button to remove the relevant door.

If a user tries to use their card at the card reader associated with a door, then a large image of the user's photo will appear in the relevant door's pane. The operator can check that the user's photo matches the user.

Note: If the user does not have a photo on their *Contact* tab on the Persons panel, then a generic person icon will appear instead.

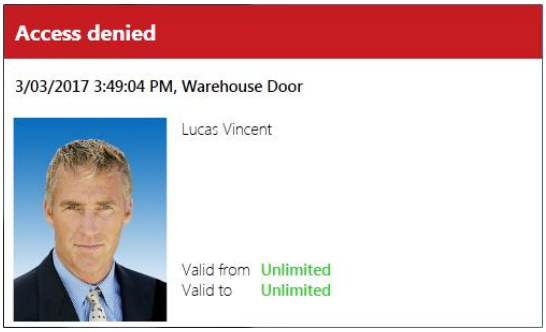
Photos of the previous four users to attempt to access the door are shown in a column to the left of the photo of the last user to attempt access, in chronological order from top to bottom.

If the user has not been assigned an access level that has access to the door, then their photo will be shown with the message "Access denied". For example:

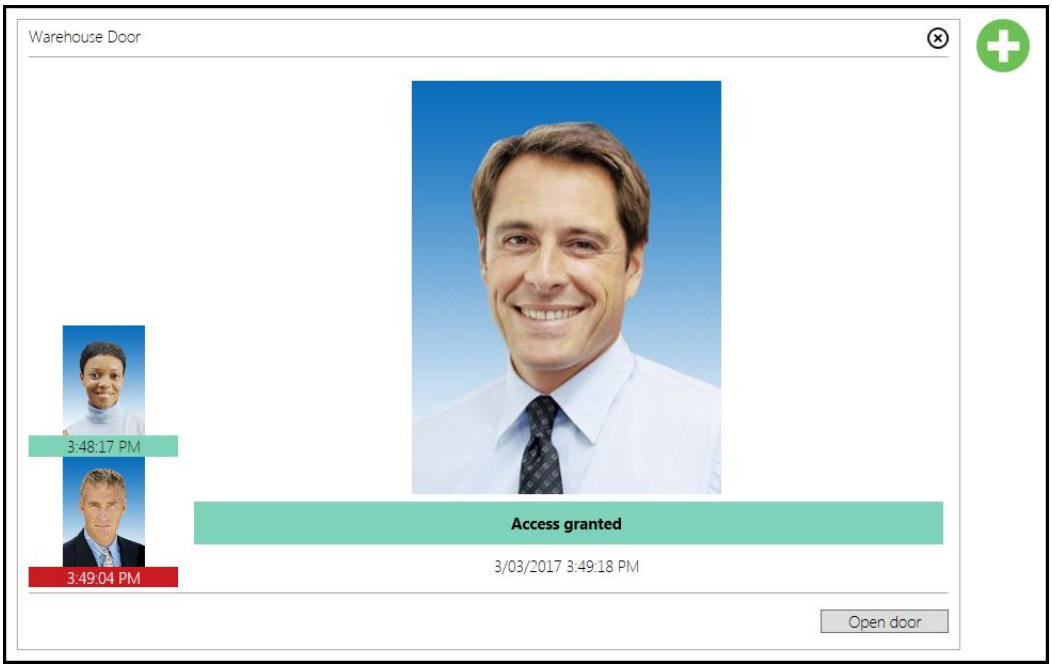


If necessary, you can click on the **Open door** button to open the door.

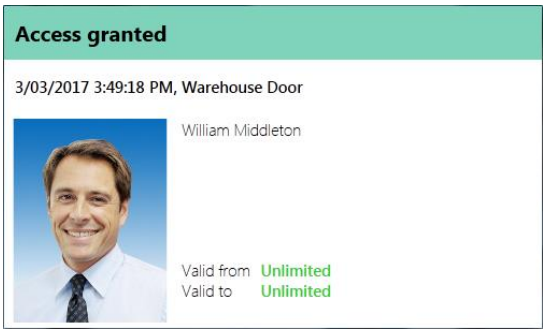
If you click on the user's photo or the message, a new window will open with more information about the user:



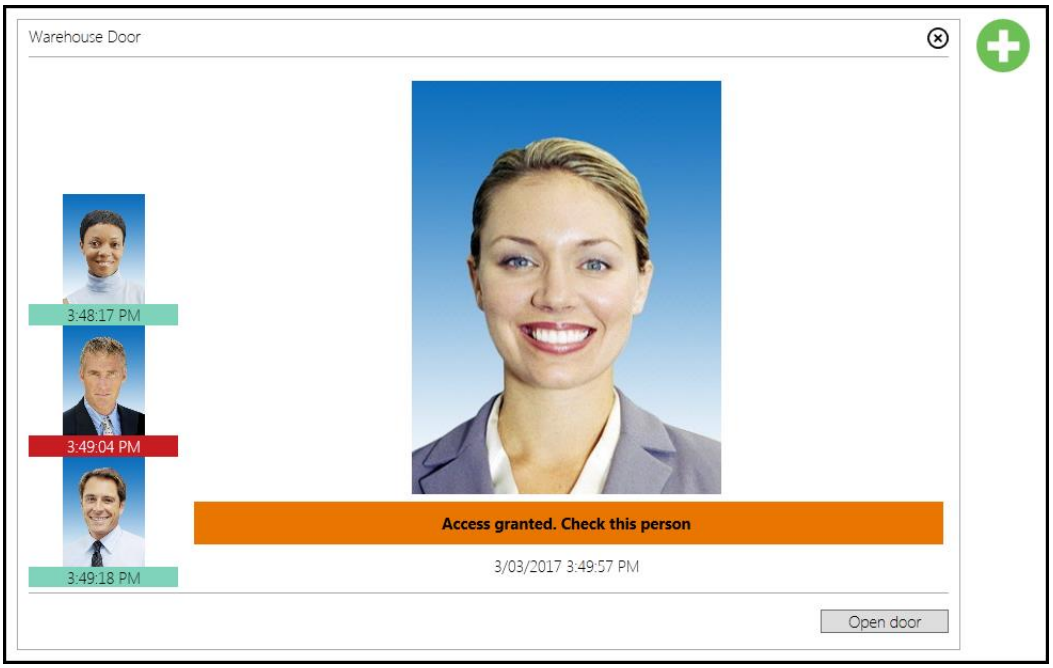
If the user has been assigned an access level that has access to the door, and the user is not flagged for a random check, then their photo will be shown with the message “Access granted”. For example:



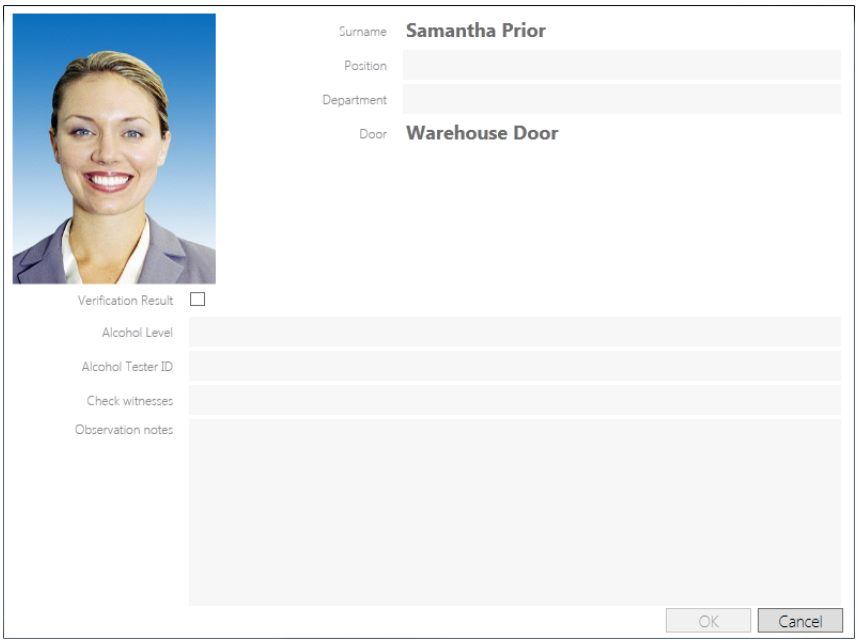
If you click on the user’s photo or the message, a new window will open with more information about the user:



At a random interval (determined by the RandomCheckProbability option specified for the Access Guard extension on the Extensions panel), a user who is granted access will be flagged for checking of their blood alcohol level. In this case, the message underneath the user's photo will say "Access granted. Check this person". For example:



If you click on the user's photo or the message, a new window will be shown where the operator can enter the results of the user's alcohol test:



The fields that can be filled in are:

- **Verification Result** – A checkbox indicating whether the user passed the alcohol test or not.
- **Alcohol Level** – The user's tested alcohol level. This field is required.
- **Alcohol Tester ID** – The ID of the alcohol tester. This field is required.

- **Check witnesses** – Witnesses to the alcohol test.
- **Observation notes** – Any additional notes on the alcohol test.

Click the **OK** button when the check is complete to close the window.

Note: Once the **OK** button has been clicked, the results of the alcohol test cannot be changed.

If the Verification Result checkbox is ticked, then the message below the photo will change to “Access granted. Passed check”. If the Verification Result checkbox is not ticked, then the message below the photo will change to “Access granted. Failed check”.

A passed or failed check will appear as an event on the *Events* tab for the relevant user in the Persons tree on the Persons panel. The event will also appear in the Live event log on the Monitor panel.

Note: Navigating away from the Access Guard panel and back again will clear all user photos for the doors.

---

16 Events

Anything that happens in the entire TecomC4 system, from a user accessing a secure area, to an operator changing permissions for a role, is recorded as an **event** in the system.

16.1 Event history

In most panels of the TecomC4 system, there is an *Events* tab from which you can view the event history of selected nodes or other relevant items.

The following tools are available to search the event history:

- There is a filter available on *Events* tabs. See the “Filtering events” section on page 125 for more information.
- **Refresh (F5)** – Refreshes the listing of events.
- **Show events including events from child nodes** – Also shows events from child nodes if applicable. If this option is active, then the button appears in blue with a blue line underneath.
- **Print** – The list of events can be printed or exported to file by means of this function. Printing of various lists can be helpful when creating reports. You can print the report or save it to Excel and use the collected data in a different way. [Wording]
- **Time** – By clicking the time filter it is possible to set the time from which events should be displayed. You can select one of the predetermined timeframes (Hour, 2 Hours, 12 Hours, Day, 2 Days or Week) or select **Custom** and specify **From** and **To** times. To display events within a different time period, enter the required value and execute the Refresh (F5) command.

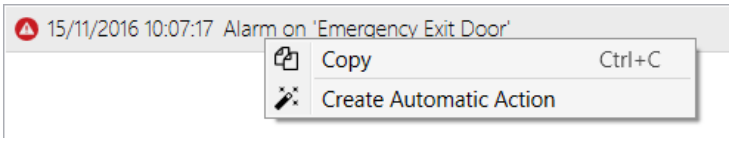
If an event message is too long to display in the TecomC4 window, then you can click the ellipsis button on the right of the event to show a tooltip containing the full text of the event message.

Each line in the event history begins with an icon indicating the type of event:

- – Info
- – Warning
- – Error
- – Alarm
- – Fire Alarm

If an event is associated with a person, device or region, you can display a window with detailed information about that entity by clicking the entity’s name within the event.

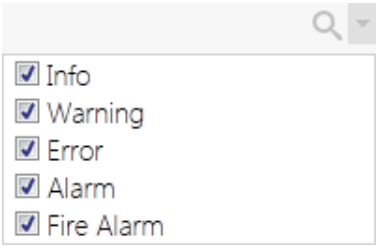
You can also right-click an event to copy it or to use it as the basis for an automatic action:



Selecting the **Create Automatic Action** menu item will cause the view to change to the Automatic Actions panel with a new automatic action created. See the “Automatic actions” chapter on page 128 for more information on automatic actions.

16.1.1 Filtering events

By default, all relevant events are shown in the *Events* tab. The tab’s form filter can be used to filter the events shown. You can also click the drop-down menu icon in order to stop showing events of certain types:



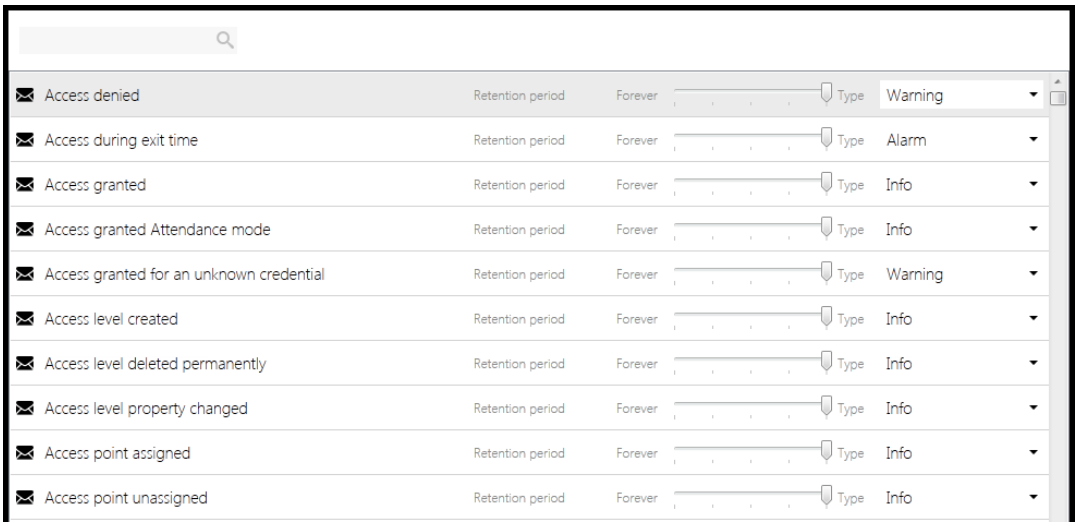
See the “Form filter” section on page 16 for more on filtering within forms.

16.2 Events panel

The Events panel shows a list of all of the events defined in the TecomC4 system.

The Events panel can be opened by clicking the **Navigation** button and selecting **Events** from the Settings menu.

The Events panel looks like this:



You can filter events by entering text in the filter above the event list.

Each event has the following attributes:

- **Name** – The event's name.
- **Retention period** – The event's retention period, which can be one of the following:
    - Forever – the event is retained indefinitely.
    - 30 days
    - 180 days
    - 365 days
    - Never – the event is not recorded in the TecomC4 database at all. The event is not shown on any relevant *Events* tabs and does not appear in the events pane on the Monitor panel. However, the event can be used as a condition in automatic actions.

    Warning: Changing an event's retention period to Never means that you will never see the event appear within TecomC4.
- **Type** – The event's type, which can be one of the following:
    - Info
    - Warning
    - Error
    - Alarm
    - Fire Alarm

Alarm and Fire Alarm events will be shown on the Monitor and Alarms panels.

For example, the **Access Denied** event, whose type is **Warning** by default, can be changed to have an **Alarm** type so that it appears on the Monitor and Alarms panels.

16.2.1 Changing event types

Each event has a **type**, indicating the severity of the event and the attention it warrants by an operator. The possible types are **Info**, **Warning**, **Error**, **Alarm** and **Fire Alarm**. Events of Alarm and Fire Alarm type are displayed in the Monitor and Alarms panels.

The TecomC4 system allows you to change event types for events:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Events** to open the Events panel.
2. You can set the required type for each event by expanding the **Type** drop-down list on the right of the selected event and selecting the required type from the list. If you select multiple events at once, then a value set for any selected event is also propagated to the other selected events.

16.3 Deleting old events

The TecomC4 system is designed to keep all information created in the system for an unlimited time. It may sometimes be necessary for the information to be stored only for a specified time, with older information being regularly deleted from the system.

To enable the deletion of old events, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Clean audit logs** extension.

Once the functionality is enabled, you can set a retention period for each event in the system. Events older than the specified retention period will be deleted automatically. By default, all events have a retention period of Forever, meaning that they will never be deleted.

Set the retention period for events by following these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Events** to open the Events panel.
2. You can set the retention period for each event by sliding the Retention Period indicator.

   If you select multiple events at once, then a value set for any selected event is also propagated to the other selected events.

Warning: The deletion of events using the **Clean audit logs** extension is irreversible and results in the loss of event data, so this functionality should only be used after careful analysis.

---

17 Automatic actions

Automatic actions can be created which are executed based on specific times or the occurrence of events within the TecomC4 system. This allows you to define logical relationships between security devices in the system and automate processes.

Some examples of automatic actions, of varying complexity, are:

- Open all doors if there is a fire alarm.
- Lock all doors if a duress button is pressed.
- Disarm an area when a user swipes their card at the area's entry point, without the user having to manually disarm the area.
- Activate air-conditioning if there are more than 10 people in an area.
- Notify a person by SMS or email when there is an alarm.

An automatic action consists of two main parts:

1. A set of conditions on the basis of which the automatic action is subsequently performed. These conditions can be event-based (i.e. when a TecomC4 event occurs) or time-based (i.e. at a specific time).

   Event-based conditions can be restricted by additional conditions on the particular security devices within the system or particular users associated with the events. For example, the condition for an alarm event can be restricted to a particular input.

   If there are multiple events defined then the automatic action will be triggered if any of the events occur. If there are restrictions defined, such as devices that events may occur on, then one of the events must occur on one of the defined restrictions. For example, if you define three event conditions and two devices, then the automatic action will be executed if at least one of the three events occurs and it occurs on at least one of the two devices.

2. A set of actions that are performed when the conditions are met. If any of the conditions are met then all of the actions are performed.

   Actions can be performed on a variety of entities:

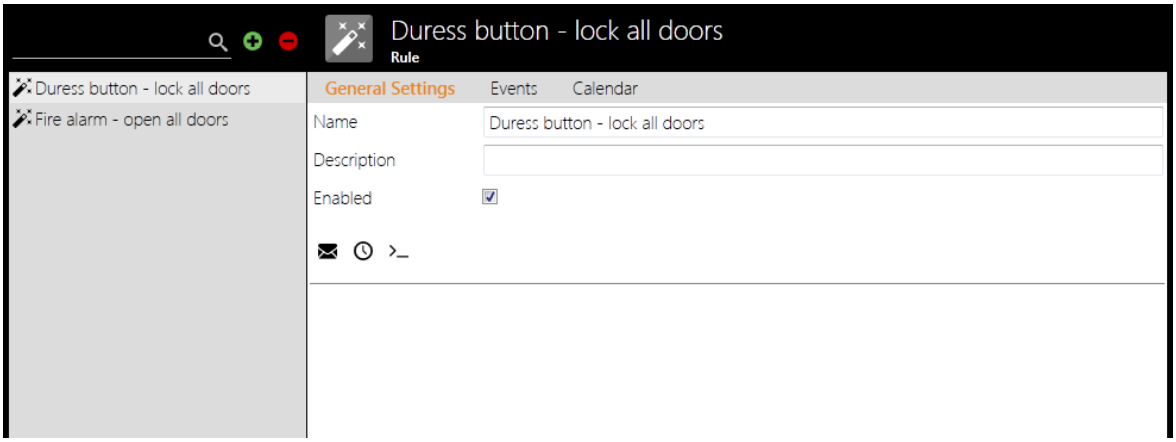
   - Devices – automatic device remote control is possible.
   - Counters – a counter value can be increased or decreased based on the occurrence of certain events and its threshold values can be evaluated.
   - Timers – an event in the system can start a timer and the system can notify if another specified event does not occur before the specified time elapses.
   - Sending an email or SMS – a person can be notified of an event.

Automatic actions are defined on the Automatic Actions panel.

17.1 Automatic Actions panel

Automatic actions are defined on the Automatic Actions panel, which can be opened by clicking the **Navigation** button and selecting **Automatic Actions** from the Settings menu.

The Automatic Actions panel looks like this:



The record list shows the list of automatic actions.

The list of automatic actions can be filtered by typing text in the record filter.

The record form has the following tabs:

- **General Settings** – Name and description of the selected automatic action, a checkbox indicating whether the automatic action is enabled, a toolbar for adding conditions to the automatic action and the detailed definition of the selected automatic action.
- **Events** – shows all events associated with the selected automatic action. See the “Events” chapter on page 124 for more information about the *Events* tab.
- **Calendar** – Defined timeframes for which the selected automatic action is active.

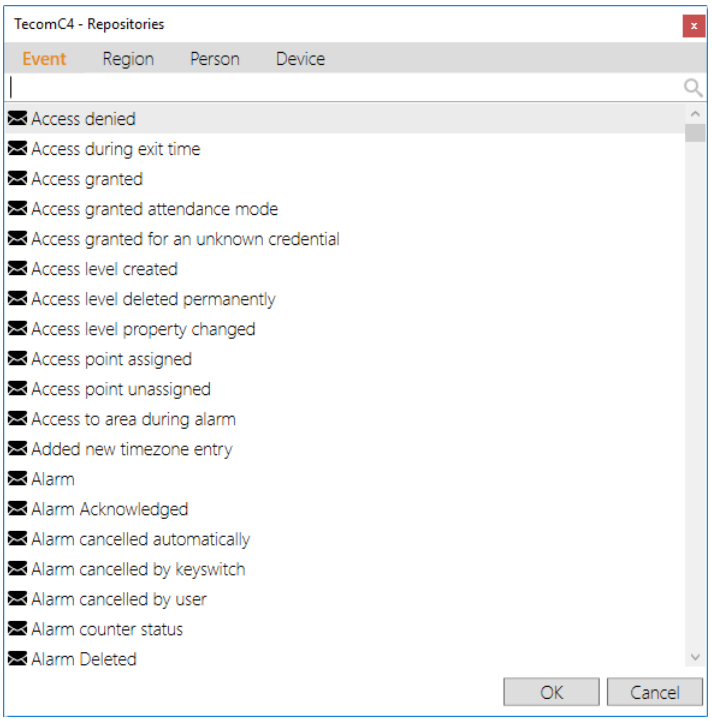
17.2 Creating an automatic action

To create a new automatic action, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Automatic Actions** to open the Automatic Actions panel.
2. Click the **Add** button next to the record filter to create a new automatic action.
3. Enter the name of the automatic action and an optional description on the *General Settings* tab.
4. You can now add event-based and/or time-based conditions.

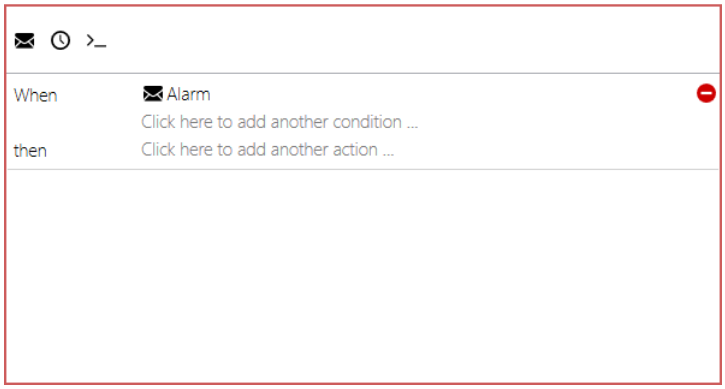
To add a condition based on an event received in the TecomC4 system:

a. Click the **Add event issued automatic action** button. A new window will open with a list of all the events that can occur within the TecomC4 system:



Select the event that the automatic action will be based on and click the **OK** button.

The form will change to look similar to this:



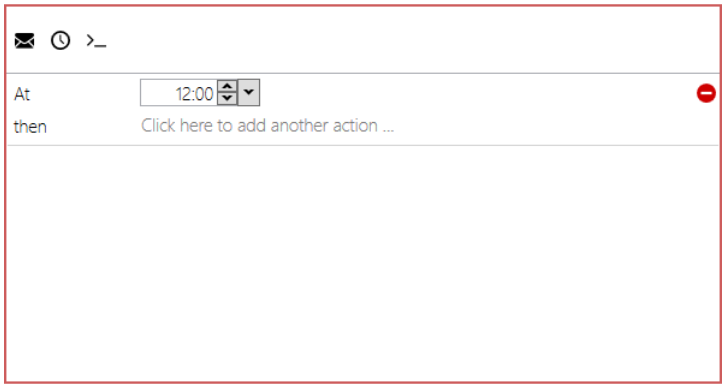
b. Click the **Click here to add another condition ...** field to add more events to the condition or restrict the condition to apply to a specific device, region or person. When you click the field a new window will open with tabs for events, regions and persons and devices. Select another event or select the desired entity that the condition relates to and click the **OK** button.

For example, if the condition was an Alarm event, then you could restrict the condition to apply to a specific input by selecting it from the Devices tree on the *Devices* tab.

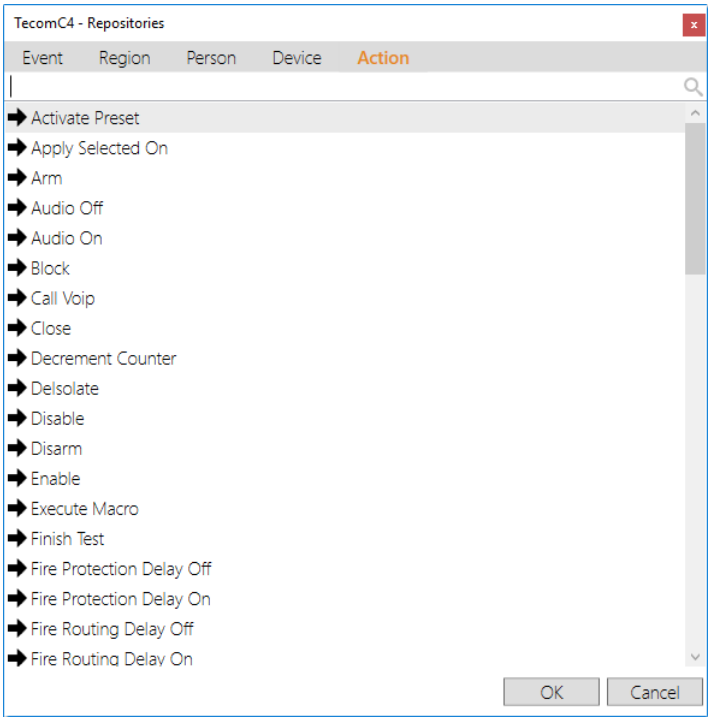
Unnecessary conditions can be removed by clicking the **Delete** button to the right of the condition.

To add a condition for a specific time:

a. Click the **Add time issued automatic action** button and specify the time to run the automatic action, in HH:MM format.

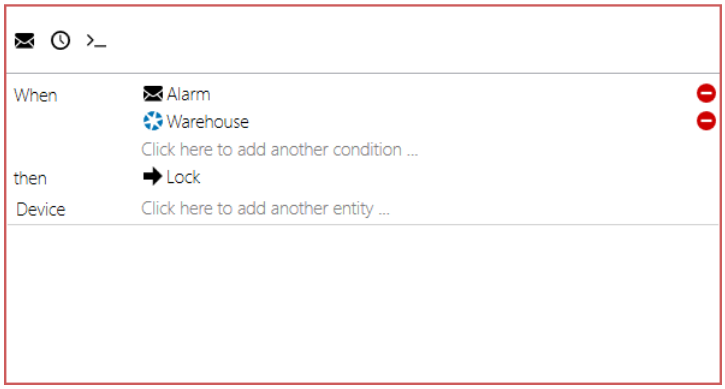


5. Now click the **Click here to add another action ...** field to choose an action to be performed when the condition is fulfilled. A new window will open with the available actions.



Select the desired action and click the **OK** button.

An entity where the action is to be performed (such as a device) also needs to be defined for the action. To do this, click the **Click here to add another entity ...** field.



A new window will open with tabs for devices, regions and persons, from which you can select the appropriate entity to perform the action on (e.g. the device to perform a command on). Select the desired entity and click the **OK** button.

For example, if the action was to Arm, then you could select an area from the Devices tree on the *Devices* tab to be armed.

Additional fields may appear depending on what the action is. For example, if the action is to Send Mail, then additional Subject and Text fields will appear that must be filled in.

6. Another action can be added by repeating step 5 as many times as required.

If the definition of the automatic action is valid and has been successfully interpreted, the red validation frame shown while editing the automatic action will disappear. The automatic action is now in effect and will be performed whenever the input conditions are fulfilled.

Note: The email address of the person selected as an automatic action email recipient must be entered in TecomC4. Likewise, the phone number of the person selected as an automatic action SMS recipient must be entered in C4.

If the automatic action needs to be temporarily suspended, uncheck the **Enabled** option on the *General Settings* tab. You can also browse the events of the selected automatic action on the *Events* tab.

You can use the *Calendar* tab to assign timeframes to the automatic action, which defines time periods for the automatic action to apply. The principle of creating timeframes is identical to the access level timeframes described in the “Creating an access level” section on page 77.

To delete the selected automatic condition entirely, click the **Delete** button next to the record filter.

17.3 Editing automatic action scripts

Each automatic action can also be modified by directly editing its script. Editing the script should only be done by a skilled and trained operator.

1. Click the **View source code** >_ button.
2. The automatic action script appears and can be edited manually.
3. If necessary, you can add a new variable to the script by clicking the **Add variable to code** ••• button.

The system continuously verifies script syntax and changes are saved only if the script syntax is correct. If the script remains simple, you can click the **View in wizard** button to restore the wizard form of the script. If the script is too complex, this option is greyed out and further changes to the automatic action can only be made by editing the script itself.

18 Advanced system properties

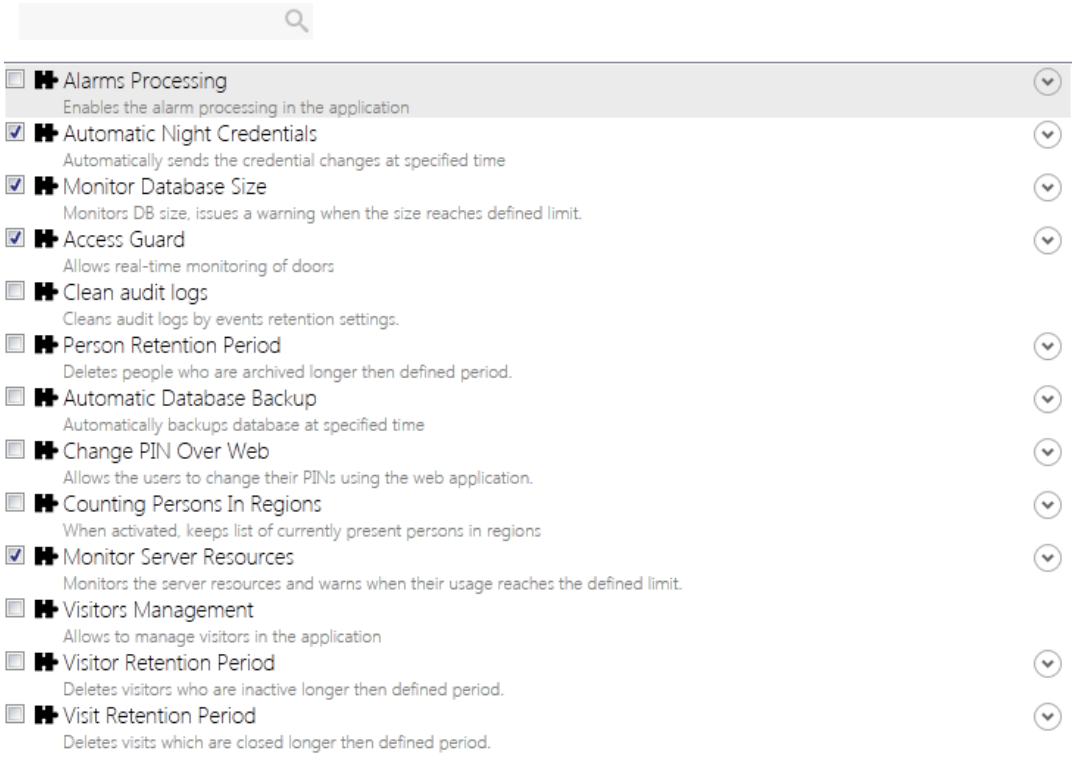
18.1 Extensions

Extended functionality for TecomC4, such as **Alarms Processing** and **Counting Persons in Regions**, can be enabled from the Extensions panel.

18.1.1 Extensions panel

The Extensions panel can be opened by clicking the **Navigation** button and selecting **Extensions** from the Settings menu.

The Extensions panel looks like this:



Tick the checkbox next to an extension to enable it in the TecomC4 system. You can click the down arrow on the right of an extension to see more options for the selected extension.

The available extensions and their options are:

- **Alarms Processing** – enables alarm processing in TecomC4. Alarms will appear in the Monitor and Alarms panels. You can set the following options:
  - **ACK Escalation Time** – the time (in seconds) within which an alarm must be acknowledged before being escalated, if the following option is enabled.
  - **Timed Alarm Escalation Enabled** – whether to enable escalation of alarms if not acknowledged within the time set above.

- **Automatic Night Credentials** – automatically send any credential and access changes to devices at a specified time. You can set the following option:
    - **Credentials Sending Time** – the time that credentials should be sent, in HH:MM:SS format.
- **Monitor Database Size** – TecomC4 can monitor the size of the TecomC4 database and issue a warning in the information bar when the size reaches the specified limit. You can set the following option:
    - **Database Size Threshold (GB)** – the database size at which the operator will be warned.
- **Access Guard –** allows for real-time monitoring of doors. See the “Access guard” section on page 119 for more information. You can set the following option:
    - **RandomCheckProbability** – the percentage probability that a user who is granted access will be flagged for checking their alcohol level.
- **Clean audit logs** – TecomC4 can delete old events according to the events’ retention period. See the “Deleting old events” section on page 127 for more information.
- **Person Retention Period** – deletes persons who have been archived for longer than the specified period. You can set the following option:
    - **Retention** – the period after which to delete archived persons, in DD.HH:MM:SS format.
- **Automatic Database Backup** – performs a daily backup of the TecomC4 database. See the “Database backup and restore” section on page 147 for more information. You can set the following options:
    - **Backup Time** – the time that the backup should be performed each day, in HH:MM:SS format.
    - **Directory** – the directory on the TecomC4 server where the database backup file should be saved.
- **Change PIN over web** – allows users to change their PINs using TecomC4’s web interface. You can set the following option:
    - **Pin length** – required PIN length when changed over the web.
- **Counting Persons in Regions** – enables functionality in TecomC4 to count persons in regions. See the “Counting persons in regions” section on page 50 for detailed information. You can set the following option:
    - **Soft Antipassback Enabled** – logs an event if a user enters the same region a second time without having previously exited the region.

- **Monitor Server Resources** – a warning will appear in the information bar of all connected TecomC4 clients if the TecomC4 server's memory usage (from all applications; not just TecomC4) reaches a specified limit. You can set the following option:
    - **Percentage** – percentage of total memory used at which to show the memory warning.
- **Visitors Management** – enables the visitor management functionality in TecomC4. See the "Visitor management" chapter on page 139 for detailed information.
- **Visitor Retention Period** – deletes visitors that have been inactive for longer than the specified period. You can set the following option:
    - **Retention** – the period after which inactive visitors will be deleted, in DD.HH:MM:SS format.
- **Visits Retention Period** – deletes visits that have been closed for longer than the specified period. You can set the following option:
    - **VisitRetention** – the period after which closed visits will be deleted, in DD.HH:MM:SS format.

18.2 Sending emails

The TecomC4 system can be connected to an email server so that you can send emails from within TecomC4.

To connect to an email server, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Right-click the root Installation node to open its context menu. Select **Add > External Notification > Mail Sender Bus Controller** from the context menu.
3. Enter the parameters for the email server. Consult the email server administrator if required. In addition to the driver settings available on all bus controllers, you can configure the following parameters:
    - **From Address** – From address for emails sent by the system.
    - **IP Address** – IP address of the email server.
    - **Port** – Port number for communicating with the email server.
    - **Account** – Account on the email server to use for sending emails.
    - **Password** – Password of the account above.
    - **Timeout** – Timeout period for connecting to the email server, in HH:MM:SS format.
    - **Enable SSL** – A checkbox indicating whether SSL communication is enabled with the email server.

4. Start communication with the email server by right-clicking the new mail sender bus controller device in the Devices tree to open its context menu and selecting **Commands > Start**.

When the connection to the email server is established, TecomC4 is capable of sending emails to any person who has an email address defined in their contact information.

You can send emails either directly to persons from the Persons panel or via automatic actions. See the “Automatic actions” chapter on page 128 for more information on automatic actions.

To send an email directly from the Persons panel, right-click the intended email recipient in the Persons tree to open its context menu and select the **Send E-mail** menu item. The Send E-mail menu item may be under the **Send** menu if SMS communication is also set up.

18.3 Sending SMS messages

The TecomC4 system can be connected to a GSM gateway to that you can send SMS notifications from within TecomC4.

To connect to a GSM gateway, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Devices** to open the Devices panel.
2. Right-click the root Installation node to open its context menu. Select **Add > External Notification > SMS Gateway Bus Controller** from the context menu.
3. Enter the parameters for the GSM gateway. Refer to the GSM gateway’s installation manual if required. In addition to the driver settings available on all bus controllers, you can configure the following parameters:
    - **Bits Per Second** – Bit rate for communication with the GSM gateway.
    - **Communication Port** – Communication port on the TecomC4 server that the GSM gateway is connected to. The port must be specified as COM+number (e.g. COM1).
    - **PIN Code** – PIN code for the SIM card in the GSM gateway. It is recommended that no PIN code be set for the SIM card because the TecomC4 system might use all permitted attempts to enter the PIN code and the SIM card will be blocked.
4. Start communication with the email server by right-clicking the new SMS gateway bus controller device in the Devices tree to open its context menu and selecting **Commands > Start**.

When the connection to the GSM gateway is established, TecomC4 is capable of sending SMS messages to any person who has a mobile phone (i.e. cell phone) defined in their contact information.

You can send messages either directly to persons from the Persons panel or via automatic actions. See the “Automatic actions” chapter on page 128 for more information on automatic actions.

To send an SMS message directly from the Persons panel, right-click the intended message recipient in the Persons tree to open its context menu and select the **Send SMS** menu item. The Send SMS menu item may be under the **Send** menu if email communication is also set up.

18.4 Displaying a camera feed automatically

In certain situations, a live video camera feed should automatically be displayed to a TecomC4 operator. This can be particularly useful when dealing with emergencies, where an immediate view of the area can speed up an assessment of how serious an issue is.

You can set up an automatic camera feed by following these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Client Camera Pop-up** extension.

Once the functionality is enabled, you can create an automatic action with the desired conditions for automatically displaying a camera feed. See the “Creating an automatic action” section on page 129 for information on creating an automatic action.

When adding actions to the automatic action, select **Show Live Video On Client Computer**. Select the required camera from the Devices tree in the Camera field of the automatic action. Select the required operator to whom the camera feed will be displayed from the Persons tree in the User field of the automatic action.

If the condition is fulfilled, a live feed from the specified camera is automatically displayed on all TecomC4 clients where the operator is logged in (regardless of which part of the application the operator is currently working with).

Note: The operator for whom the camera is to be displayed must have the View permission for the specified camera.

---

19 Visitor management

TecomC4 provides visitor management functionality to enable visitors to move around a secure installation. The functionality provides for registration of visits and management of visitors.

The management of visitors is based on the following steps:

1. Enabling visitor management
2. Configuring a reception
3. Registering a new visit

You can also modify visitor data.

19.1 Enabling visitor management

The visitor management functionality must first be enabled in the TecomC4 system settings:

3. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
4. Tick the **Visitors Management** extension.
5. You can also tick the **Visitor Retention Period** extension to delete visitors that have been inactive for longer than the specified period.
    - If you expand the extension details by pressing the expand button, you can set the **Retention**, which specifies the period after which inactive visitors will be deleted.
6. You can also tick the **Visits Retention Period** extension to delete visits that have been closed for longer than the specified period.
    - If you expand the extension details by pressing the expand button, you can set the **VisitRetention**, which specifies the period after which closed visits will be deleted.

When visitor management is enabled, the following new menu items will appear in the navigation menu (if the operator has permission to view the relevant panels):

- **Receptions** under the Settings menu
- **Visits** under the new Visitors menu
- **Visitors** under the Administration menu

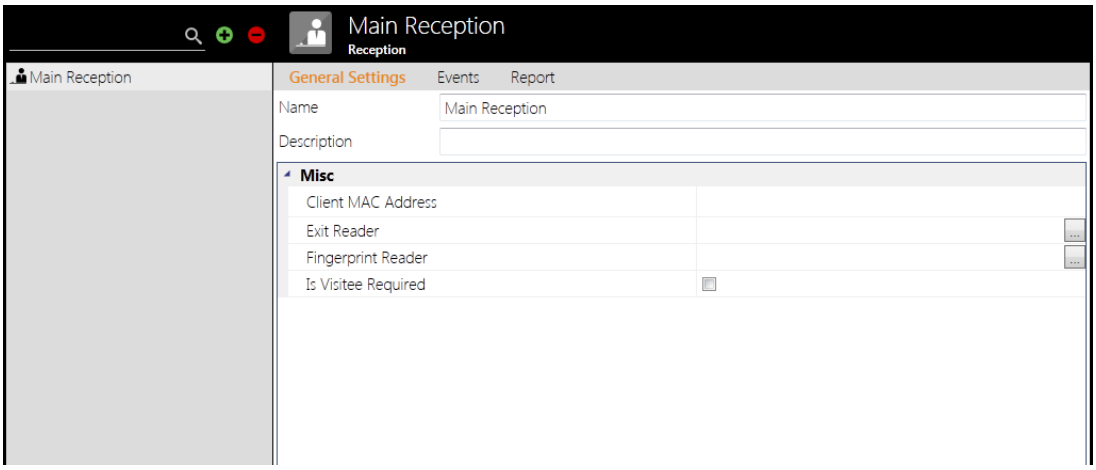
19.2 Configuring receptions

Receptions are used to centralise visitor management within TecomC4. Individual receptions are not authorized to see each other's visits.

One predefined reception (Main Reception) exists in the TecomC4 system. Receptions are configured on the Receptions panel.

19.2.1 Receptions panel

The **Receptions** menu item on the Settings menu opens the Receptions panel. The Receptions panel looks like this:



The record list shows a list of receptions.

The record filter can be used to filter receptions in the record list.

The record form has the following tabs:

- General Settings
- Events
- Reports

The tabs are described in the following sections.

19.2.1.1 Receptions panel: General Settings tab

The *General Settings* tab shows the name and optional description of the reception. It also contains settings for the reception.

19.2.1.2 Receptions panel: Events tab

The *Events* tab shows all events associated with the selected reception. See the “Events” chapter on page 124 for more information about the *Events* tab.

19.2.1.3 Receptions panel: Reports tab

The *Reports* tab can be used to create reports about the reception.

19.2.2 Creating a reception

To create a new reception, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Receptions** to open the Receptions panel.
2. Click the **Add** button next to the record filter to create a new reception.
3. Enter a name and optional description for the new reception.

4. Set the following properties for the new reception:
    - **Client MAC Address** – it is possible to set the default reception for a particular TecomC4 client computer. Enter the MAC address of the computer.
    - **Exit Reader** – exit reader to be used at the end of the visit.
    - **Fingerprint Reader** – fingerprint reader for the visit.
    - **Is Visitee Required** – tick this option to require a note of whom a visitor is visiting when a visit is registered.

A reception can be deleted by clicking the **Delete** button. A dialog box will be shown asking you to confirm the deletion.

Note: Operators in TecomC4 can only create a new reception if the **Create new reception** privilege is enabled. See the “Roles panel: Permissions tab” section on page 83 for more information.

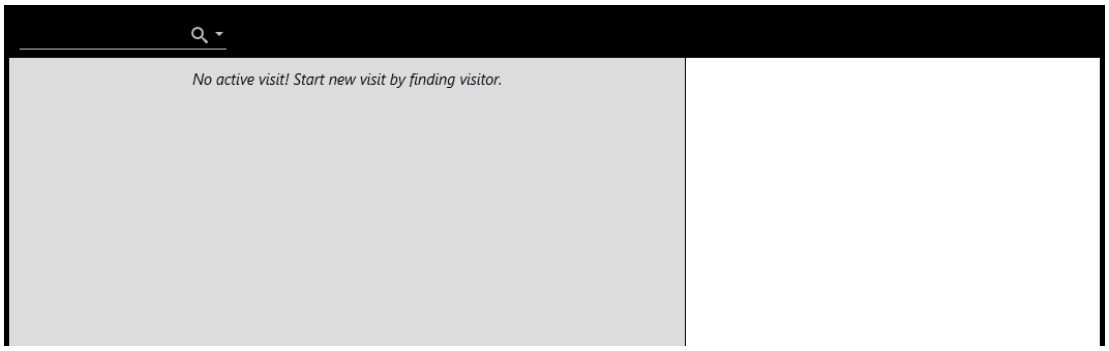
19.3 Registering a visit

Visitors are registered at the company reception. To register visitors, a receptionist records every visitor event and assigns a credential and access level to the visitor.

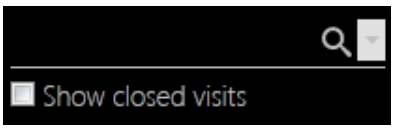
Visits are registered on the Visits panel.

19.3.1 Visits panel

The **Visits** menu item on the Visitors menu opens the **Visits** panel. The Visits panel looks like this:



The record list shows the visits list. The visits list can be filtered by typing text in the record filter or by selecting a pre-determined filter option from the filter drop-down menu :



The filter options available are:

- **Show closed visits** – show closed visits.

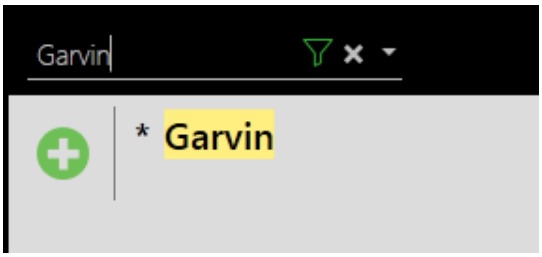
When you enter text in the record filter, the text can be used as the basis for registering a new visitor.

Each visit in the record list contains the name, the visitor's company, the visitee, and the Check In and Check Out times.

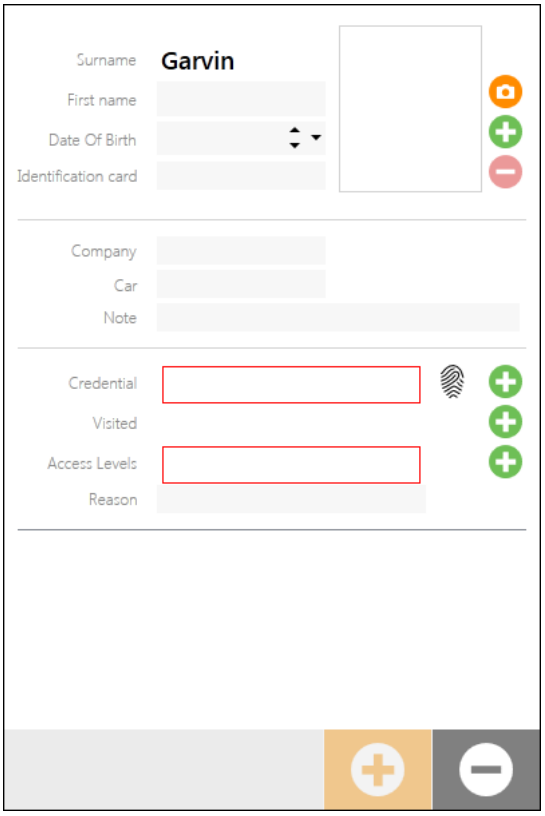
19.3.2 Registering a visit

To register a new visitor, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Visitors > Visits** to open the Visits panel.
2. Enter the visitor's name in the record filter. The names of previous visitors matching the entered text will appear in the record list. If the visitor does not exist in the list, then a visitor with the name matching the entered text will be added.



3. Click the **Register visit** button next to the name of the visitor.
4. The record form will display the new visitor information:



Enter the visitor's contact details in the record form:

- Click the **Add** button to assign a photo or click the **Delete** button to delete the visitor's existing photo. The supported photo formats are .png, .jpg, .jpeg and .gif. It is also possible to capture the photo by means of the web camera if available when you click the **Take photo** button.
- If a fingerprint reader device is present in TecomC4 and has been assigned to the relevant reception, then you can click the **Fingerprint** button next to the Credential field to add a fingerprint credential for the visitor. Alternatively, click the **Add** button to assign the visitor a card. See the "Configuring card decks" section on page 66 for more information on cards.
- You can click the **Add** button next to the Visited field to select the person the visitor is going to visit. This field may be mandatory depending on the reception settings.
- You can click the **Add** button next to the Access Levels field to select the access level for the visitor. This will determine which parts of the secure installation the visitor can enter. See the "Configuring user access levels" chapter on page 71 for more information on access levels.

5. If the visitor is an unwanted person, a red bar appears at the bottom and it is up to the receptionist to decide whether the visitor will be allowed entry.

See the "Modifying visitor data" section on page 145.

6. Click the **Confirm visit** button to confirm the visitor's data and register the new visitor. Click the **Cancel visit** button to cancel the registration of the new visitor.

The visit event history can be viewed in the Receptions panel on the *Events* tab of the relevant reception.

Note: It is not recommended to allow visitors to have access to private company premises, but only to public premises (passages, dayrooms etc.).

Note: The created visitor is remembered in the system and their contact details do not need to be filled in again at their next visit.

Note: Operators in TecomC4 can only create a new visitor if the **Create new visitor** privilege is enabled. See the "Roles panel: Permissions tab" section on page 83 for more information.

19.3.3 Ending a visit

To finish a visit, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Visitors > Visits** to open the Visits panel.

2. Find the relevant visit in the record list and click the **End visit** button next to the visit.

If an exit card reader is set for the reception, then the visit is finished automatically when the visitor's assigned card is read on the exit card reader.

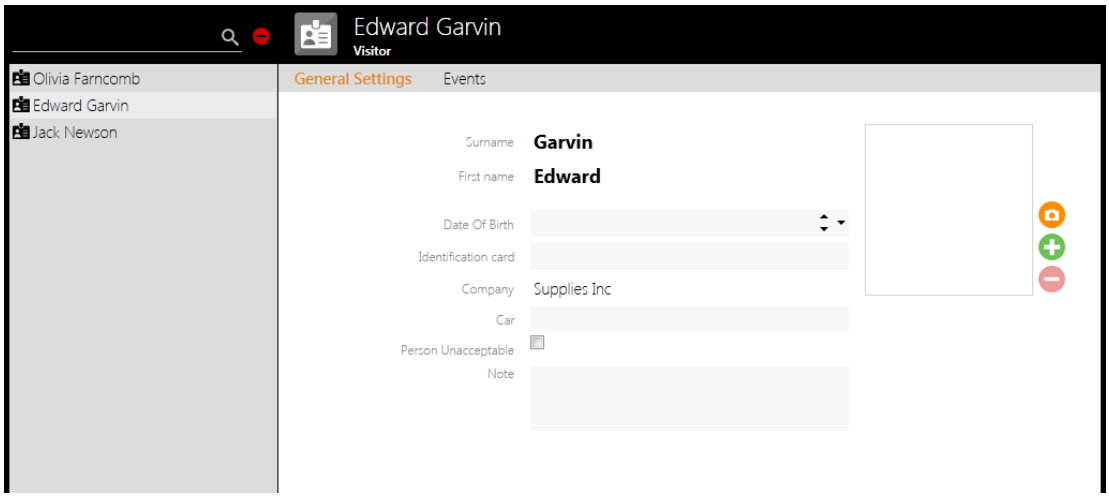
After the visit is finished, the assigned card will become available again.

19.4 Modifying visitor data

Visitor data can be modified directly in the data about each visit or on the Visitors panel. All visitors are registered in the Visitors panel.

19.4.1 Visitors panel

The **Visitors** menu item on the Administration menu opens the Visitors panel. The Visitors panel looks like this:



The record list shows a list of visitors.

The record filter can be used to filter visitors in the record list.

The record form has the following tabs:

- General Settings
- Events

The tabs are described in the following sections.

19.4.1.1 Visitors panel: General Settings tab

The *General Settings* tab shows the contact information for the visitor.

19.4.1.2 Visitors panel: Events tab

The *Events* tab shows all events associated with the selected visitor. See the "Events" chapter on page 124 for more information about the *Events* tab.

19.4.2 Modifying visitor data

To modify visitor data, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Administration > Visitors** to open the Visitors panel.
2. Find the relevant visitor in the record list and modify their details.

To delete a visitor, select the visitor in the list of visitors and click the **Delete** button next to the record filter above the list.

To flag a visitor as an unwanted person, tick the **Person Unacceptable** checkbox. You can also fill the **Reason** field as to why the person is unwanted.

In the list of visitors, unwanted persons are indicated by the unwanted status icon.

This indication is only for information and does not deny the visitor's entry to the building. When creating a new visit, the receptionist is warned of such a visitor by the red bar and it is up to the receptionist to decide whether the visitor will be allowed to enter the building.

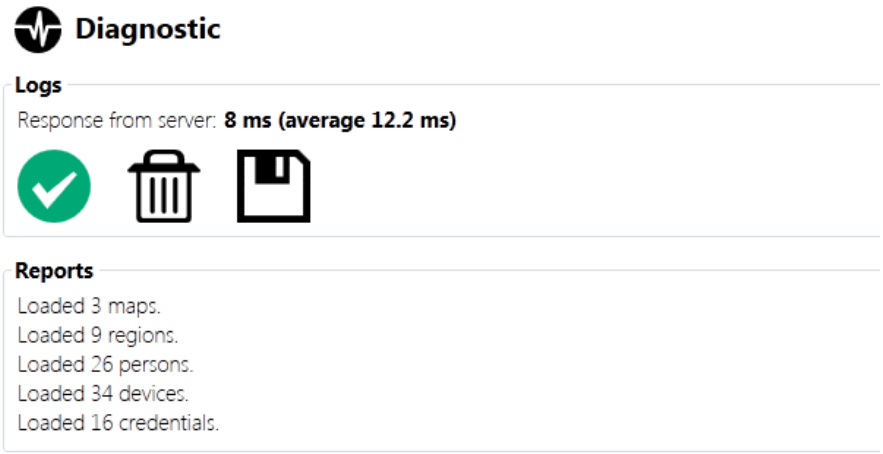
20 System maintenance

20.1 System diagnostics

The Diagnostic panel shows diagnostics about the TecomC4 system.

20.1.1 Diagnostic panel

The Diagnostic panel can be opened by clicking the **Navigation** button and selecting **Diagnostic** from the Help menu.



20.1.2 Diagnostic panel: Logs

The **Logs** section of the Diagnostic panel shows the response time of the TecomC4 client to the TecomC4 server. It also has a toolbar for dealing with logs.

Log files serve the purpose of troubleshooting application issues, the cause of which would otherwise require a time-consuming diagnostic process. Under normal operation of the security system, logs can be disabled, in which case only unexpected exceptions and application errors are logged.

You can disable logging by clicking the green symbol, which will change to the red symbol.

If diagnosis of the system is necessary, logging can be enabled by clicking the red symbol. This enables extended logging, which requires more disk space. After the issue analysis is completed, it is recommended to disable logging again by clicking the green symbol again.

In some cases, it is useful to clear existing logs by clicking the **Delete** icon before the simulation of a recurrent error. Log files can be saved to a zip file on the local computer by clicking the **Save** icon.

20.1.3 Diagnostic panel: Reports

The **Reports** section of the Diagnostic panel shows a summary of the number of maps, regions, persons, devices and credentials in the TecomC4 system.

20.1.4 Diagnostic panel: Interactive window

The **Interactive Window** section contains an interactive console. The console is in experimental mode and it is not recommended that you use it.

20.2 Monitoring database size

TecomC4 can monitor its database size and notify the operator if the size exceeds a specified limit, so that appropriate changes can be made to the system to ensure continued operation of TecomC4.

To enable database size monitoring, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Monitor Database Size** extension.
    - If you expand the extension details by pressing the expand button, you can set the **Database Threshold Size (GB)**, which specifies the time of the daily database backup in HH:MM:SS format, and the directory

Upon exceeding the specified value, TecomC4 will display a warning in the information bar.

20.3 Database backup and restore

The entire TecomC4 database can be backed up daily to a location on the TecomC4 server computer. TecomC4 will maintain three rolling backups, with new backups overwriting the oldest backups.

20.3.1 Setting up database backup

To enable the daily database backup, follow these steps:

1. Click the **Navigation** button to open the navigation menu. Select **Settings > Extensions** to open the Extensions panel.
2. Tick the **Automatic Database Backup** extension.
    - If you expand the extension details by pressing the expand button, you can set the **Backup Time**, which specifies the time for the daily backup in HH:MM:SS format, and the **Directory** where the database backup file will be saved.

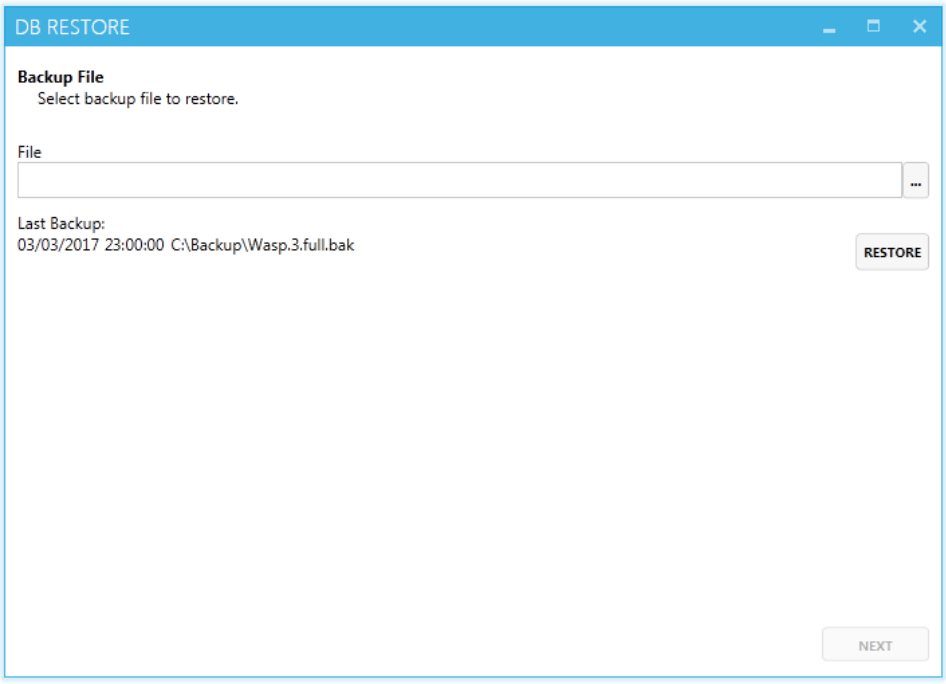
    Note: The directory must be accessible by the account that runs the TecomC4 service on the TecomC4 server computer. This account is called C4Service in a default installation.
3. After the first scheduled backup time, verify that the first backup file (which will have a name of the form `Wasp.n.full.bak`, where `n` is a number) is present in the specified location.

20.3.2 Restoring the database

If required, you can restore the TecomC4 database by using the **Database Restore** program provided with TecomC4. The program is installed on the TecomC4 server computer when TecomC4 is installed.

To restore the TecomC4 database, follow these steps:

1. Start the Database Restore program, by navigating to **Programs > Gamanet a.s > Database Restore** within Windows.
2. The Database Restore program window has a File field, where you can enter the path to a database backup file, or use the **Browse** ... button to open a file open dialog window. Once the File field is populated, you can click the **Next** button to continue.



   Alternatively, if there are existing database backup files in the backup directory designated in the Automatic Database Backup extension, then the most recent backup file appears below the File field. You can click the **Restore** button next to the most recent database backup file to continue.
3. The program will display a summary of the proposed database restore. Confirm the restore by clicking the **Next** button. A progress bar will be displayed as the database backup is restored.
4. The program will display a summary. Click the **Finish** button to close the program.

Appendix A: Challenger10 devices and commands

The following table lists all of the Challenger10 devices and the commands that can be run on them. It also shows each device's possible child devices. Child devices in italics are grouped together in the table since they have the same commands and possible child devices.

Information on the commands can be found in the "Challenger10 commands" section on page 42.

Table 7: Challenger10 devices and commands

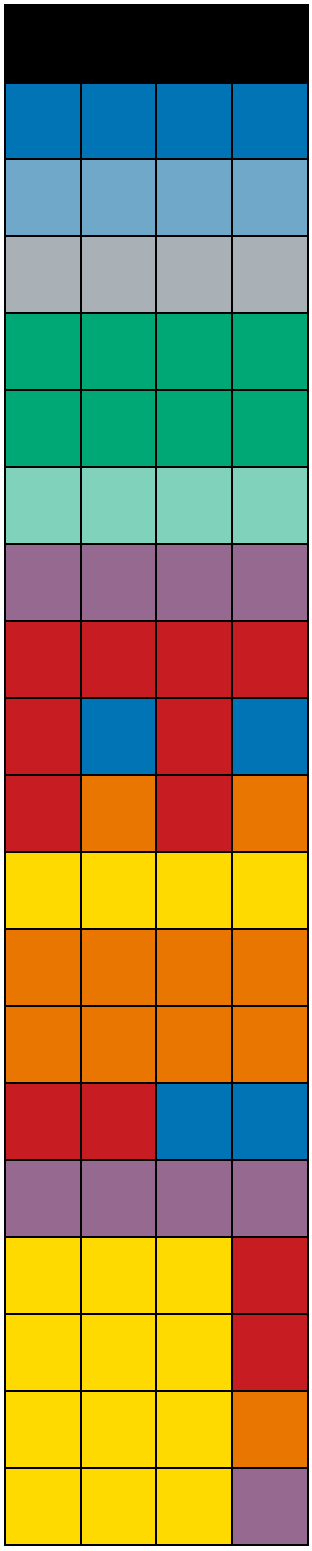
Device	Commands	Possible child devices
Bus controller	Start Stop	Panel
Panel	Isolate Isolate Timed DeIsolate Send All Credentials Send Panel Access Changes	Door Access Controller Lift Access Controller Standard DGP Expander *Detectors* *Fire Detectors* Area *Doors* Film Camera Output *Generics* Automation Zone Automation Floor Lift Door
Door Access Controller	Isolate Isolate Timed DeIsolate	*Detectors* *Fire Detectors* *Doors (4DC)* Output
Lift Access Controller	Isolate Isolate Timed DeIsolate	*Detectors* *Fire Detectors* Output Lift
Standard DGP Expander	Isolate Isolate Timed DeIsolate	*Detectors* *Fire Detectors* Output

Device	Commands	Possible child devices
Detectors: Detector Centre Detector Dual Detector Glass Break Detector Infra Detector Magnetic Detector Panic Button Shock Detector	Reset Isolate Isolate Timed DeIsolate	–
Fire Detectors: Fire Detector Ceiling Fire Detector Floor Fire Detector Input Manual Call Point Max Temperature Detector Thermo Differential Detector	Reset Isolate Isolate Timed DeIsolate	–
Area	Arm Disarm	–
Doors: Door Ramp	Open	Card Reader With Keypad
Card Reader With Keypad	Isolate Isolate Timed DeIsolate	–
Film Camera	–	–
Output	On Off	–
Generics: Communication Path Expander Module	–	–
Automation Zone Automation	On Off Trigger Level	–
Floor Lift Door	Lock Unlock	–
Doors (4DC): Door Ramp	Open Open Timed Lock Unlock Enable Disable	Card Reader With Keypad (4DC)

Device	Commands	Possible child devices
Lift	Enable Disable	Card Reader With Keypad (4DC) Lift Door
Lift Door	Lock Unlock	–
Card Reader With Keypad (4DC)	–	–

Appendix B: Device status colours

See the “Device status colours” section on page 40 for information about device status colours. The table on that page shows status colours applicable to Challenger10. The complete table of possible device status colours for all devices is as follows:



Black – unknown/communications stopped/offline

Blue – normal status/disarmed

Pale blue – processing

Grey – isolated

Green – locked

Green – armed

Cyan – partially armed

Violet – activated

Red – rearmed

Red/Blue – alarm

Red/Orange – tamper

Yellow – test

Orange – failure

Orange – disconnected

Red/blue – alarm precondition

Violet – not ready to arm

Yellow/Red – alarm during test

Yellow/Red – alarm precondition during test

Yellow/orange – tamper during test

Yellow/violet – activated during test

Index

E

F

H

I

L

M

N

O

P

R

S

T

U

V