Addendum: TecomC4 Operators Manual

Introduction

This document outlines the changes between **TecomC4 2016** and **TecomC4 2017**, and describes the upgrade process.

Upgrade process

In order to complete the upgrade from TecomC4 2016 to TecomC4 2017, you must do the following:

1. Upgrade TecomC4. Run **TecomC4ServerSetup.exe** as administrator and follow the prompts to upgrade TecomC4.
2. Open the TecomC4 client application and log in.
3. Ensure your TecomC4 license is up to date on the **Licenses** panel. An upgrade from TecomC4 2016 to TecomC4 2017 requires a license update.
4. Install the latest Challenger10 driver in TecomC4. Upgrade the driver by navigating to the **Drivers** panel, clicking the **Updates** tab, and selecting the Challenger10 driver from the list.
5. The TecomC4 service must be restarted. The simplest way to do this is to reboot the TecomC4 server computer. Alternatively, open the **Services** snap-in in Windows on the TecomC4 server computer, locate the **TecomC4 Application Server**, right-click it and select **Restart** from the context menu.
6. Open the TecomC4 client application and log in.
7. You must resend all credentials to the Challenger10. On the **Devices** panel, right-click the Panel device of the Challenger10 and select **Commands > Clear Memory and Send All Credentials**.

New features

TecomC4 2017 (in conjunction with the latest Challenger10 driver) has the following important new features:

- Named device import
- Optional extension PIN for credential types
- Merged credentials
- Custom alarm groups
- Access level user flags

These new features are described in the following sections.

Named device import

The following new features relate to the import of named devices:

- A Challenger10 Panel  device will now have its name imported (if it has a name defined).
- If an operator has made changes to the name of a device in TecomC4, then that name will not be overwritten if you reload a Challenger10 configuration (by running the **Load configuration from device** option on the Challenger10 device in the **Devices** panel). Newly added devices will still be imported with their names.

Optional extension PIN for credential types

Note: Challenger10 ***does not support*** extension PINs for cards. To use card and PIN with Challenger10, use merged credentials instead of the extension PIN, as described in the “Merged credentials” section on page 3.

TecomC4 2017 allows the operator to enable or disable the extension PIN option for individual credential types, thus avoiding confusion when working with systems that do not support extension PINs, such as Challenger10.

The extension PIN option for a credential type can be enabled via the new **Enable PIN** check box, which can be found under the **Card number** field on the **Credential types** panel for a selected credential type.

Ticking the check box enables the extension PIN for the credential type. The extension PIN can be entered in the **Pin** field for a card of that type (cards can be selected on the **Credentials** tab of the **Persons** panel when a person is selected in the Persons tree, or on the **Cards** panel). If the **Enable PIN** check box is cleared, then the **Pin** field does not appear for cards of that type.

The **Enable PIN** option is disabled in TecomC4 2017 by default. The option should only be enabled if required.

Merged credentials

It is now possible for the TecomC4 operator to merge a card credential and a PIN credential into a single merged **Card and PIN** credential. This allows TecomC4 to explicitly pair the card and PIN for a single Challenger10 user.

To merge a card and a PIN, navigate to the **Persons** panel, select the relevant person from the Persons tree, and click the **Credentials** tab. Select a single card credential and a single PIN credential (by shift-clicking or ctrl-clicking), and click the **Merge** button. The merged credentials appear together with the label **Card + Pin**.

You will have to resolve the credential changes to the Challenger10.

Merged credentials can be unmerged by selecting the merged credentials and clicking the **Unmerge** button.

Custom alarm groups

In TecomC4 2016 with the previous Challenger10 driver, it was not possible to assign a user a specific Challenger10 alarm group, except for alarm group 3 via the **Installer mode (alarm group 3)** check box. This check box was located under an access level's Challenger10 extended properties (visible on the **General Settings** tab of the **Access levels** panel).

In TecomC4 2017 with the latest Challenger10 driver, the check box has been removed, and a new field called **Alarm Group Mode** has been added, allowing you to explicitly set the alarm group for users with the access level. There are three options for the **Alarm Group Mode**:

- *Automatic Alarm Group* – this mode is equivalent to TecomC4 2016 with the **Installer mode (alarm group 3)** check box unticked. A user with the access level will have their alarm group automatically determined by TecomC4. In this case, there are options for **User flags selection** and **User menu selection**.
- *Custom Alarm Group* – this mode allows you to explicitly set an alarm group for users with the access level. If you select this mode, then the field **Alarm Group Position** appears, allowing you to enter the alarm group number.
- *Installer Alarm Group* – this mode is equivalent to ticking the **Installer mode (alarm group 3)** check box in TecomC4 2016. That is, users with the access level will have alarm group 3 ("Master Code") in the Challenger10.

Notes:

If multiple access levels are assigned to a person and a custom alarm group is required, then all access levels assigned to the person **must** have the *Custom Alarm Group* mode and the same **Alarm Group Position** specified.

If multiple access levels are assigned to a person and the installer alarm group is required, then all access levels assigned to the person **must** have the *Installer Alarm Group* mode.

In order for a user with the selected access level to have the installer alarm group or a custom alarm group, you must assign at least one access point from the Challenger10 to the access level.

Access level user flags

The following changes have been made to the **User flags selection** option of the Challenger10 extended properties of access levels (visible on the **General Settings** tab of the **Access levels** panel):

- **Audit log only user** now has the *Area Reset* flag in addition to the *User Alarm Group* and *Alarm System Control* flags.
- **Limited user** now has had the *Area Disarm* and *Area Timed* flags removed. It therefore has the following flags: *User Alarm Group*, *Alarm System Control*, *Area Arm*, and *Area Reset*.

© 2018 UTC Fire & Security Australia Pty Ltd. All rights reserved.