Location Intelligence
Infrastructure Asset Management

Confirm®

System Administration

v26.30a.AM

Information in this document is subject to change without notice and does not represent a commitment on the part of the vendor or its representatives. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, without the written permission of Confirm.

© 2026 Confirm. All rights reserved.

Products named herein may be trademarks of their respective manufacturers and are hereby recognized. Trademarked names are used editorially, to the benefit of the trademark owner, with no intent to infringe on the trademark.

Open Source Attribution Notice

The Confirm suite of products contain the following open source software:

- Feature Data Objects v 3.5.0, which is licensed under GNU Lesser General Public License, Version 2.1, February 1999 with the unRAR restriction. The license can be downloaded from: **http://fdo.osgeo.org/licenceAndGovernance.html**. The source code for this software is available from **http://fdo.osgeo.org/content/fdo-350-downloads**
- MrSID software (specifically the mrsid32.dll) is used under license and is Copyright © 1995-2002, LizardTech, Inc., 1008 Western Ave., Suite 200, Seattle, WA 98104. All rights reserved. MrSID is protected by U.S. Patent No. 5,710,835. Foreign patents are pending. Unauthorized use or duplication prohibited.

  Patented technology in the Software was developed in part through a project at the Los Alamos National Laboratory, funded by the U.S. Government and managed by the University of California. The U.S. Government has reserved rights in the technology, including a non-exclusive, nontransferable, irrevocable, paid-up license to practice or have practiced throughout the world, for or on behalf of the United States, inventions covered by the patent, and has other rights under 35 U.S.C. § 200-212 and applicable implementing regulations.

  For further information, contact Lizardtech.

- NodaTime, version number 1.3.10, which is licensed under the Apache license, version number 2.0. The license can be downloaded from http://www.apache.org/licenses/LICENSE-2.0 . The source code for this software is available from http://nodatime.org/.
- Chromium Embedded Framework, version 3, which is licensed under the New BSD License. The license can be downloaded from http://opensource.org/licenses/BSD-3-Clause. The source code for this software is available from http://code.google.com/p/chromiumembedded/downloads/list.
- Xilium.CefGlue, version 3, which is licensed under the MIT License (with portions licensed under the New BSD License). The licenses can be downloaded from http://opensource.org/licenses/MIT and http://opensource.org/licenses/BSD-3-Clause. The source code for this software is available from http://xilium.bitbucket.org/cefglue/.
- D3 Data Driven Documentation, version 3.4.1, which is licensed under the New BSD License. The license can be downloaded from from https://github.com/mbostock/d3/blob/master/LICENSE. The source code for this software is available from http://d3js.org/.
- OpenLayers, version 8.1, which is licensed under the BSD 2-Clause Licence. The license which can be downloaded from https://github.com/openlayers/openlayers/blob/master/LICENSE.md The source code for this software is available from https://github.com/openlayers/openlayers.
- Proj4js, version 1+, which is licensed under the Apache License, Version 2, January 2004. The license can be downloaded from http://www.apache.org/licenses/LICENSE-2.0.html. The source code for this software is available from http://trac.osgeo.org/proj4js/.
- requireJS, version 2.1.2, which is licensed under the MIT License or the New BSD License. The license can be downloaded from https://github.com/jrburke/requirejs/blob/master/LICENSE. The source code for this software is available from http://requirejs.org/.
- Apache Cordova, version 11.1.0, which is licensed under the Apache License, Version 2, January 2004. The license can be downloaded from http://www.apache.org/licenses/LICENSE-2.0.html. The source code for this software is available from http://phonegap.com/download/.
- Xilium.CefGlue, version 75.1, which is unlicensed. The source code for this software is available from https://gitlab.com/xiliumhq/chromiumembedded/cefglue.

- Chromium Embedded Framework, version 75.0, which is licensed according to the following criteria:

  Copyright (c) 2008-2014 Marshall A. Greenblatt. Portions Copyright (c) 2006-2009 Google Inc. All rights reserved.

  Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

  * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

  * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

  * Neither the name of Google Inc. nor the name Chromium Embedded Framework nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

  THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

  The source code for this software is available from http://opensource.spotify.com/cefbuilds/index.html#

October 02, 2026

Table of Contents

System Administration

Introduction 7

File Explorer 8

Import Data 9

Scheduled Tasks 10

Task Progress and Cancellation 13

Security 15

- Change Password 15
- User Security 16
- Group Security 28
- Work Groups 31
- Data Security Keys 34
- Data Security Groups 35
- User Logs 35
- Connector Logs 36
- Security Settings 37
- General System Settings 39
- General User Settings 41
- Security Seed Numbers 42

System Configuration 43
User Reset 43
Internal Messages Cleardown 43
Officer Location Cleardown 43
System Registration 44
Database Schema Check 44
Database Settings 45
Confirm client Settings 45
Connector Settings 45
Mapped Drive Settings 46
Task Processor Settings 47
ConfirmConnect® Settings 48
ConfirmWorkzone Settings 50
Confirm Web Log Settings 51
Settings 52
Local Settings 57
Relicense 57
ConfirmConnect® Profile 58
ConfirmConnect® Registration 59
Mail Merge Manager 60
Import Transformations 63
Finance Year 66
Comment Library 66
Document Links System Settings 67
Import Anything System Settings 69
Terminology System Settings 71

Entity History 73
Entity History Report 73
Entity History Cleardown 75
Entity History System Settings 76

All System Settings 79

All Seed Numbers 80

System Administration

In this section

Introduction	7
File Explorer	8
Import Data	9
Scheduled Tasks	10
Task Progress and Cancellation	13
Security	15
System Configuration	43
Entity History	73
All System Settings	79
All Seed Numbers	80

Introduction

The System Administration folder contains the tools for setting up User securities, System Settings, Seed Numbers, and for database administration.

System Administration is split into several folders:

'Security'

This folder contains details of Users, Work Groups and Security Groups. Defaults can be set to regulate whether, and how often, Users will change their passwords, how many times a user may attempt to login at one time, and whether and under what circumstances User sessions will be logged.

'System Configuration'

This folder contains details of the modules that are active in this version of Confirm, the database settings and local PC settings. There are also utilities for resetting rogue User sessions and checking the structure of the database with a Database Schema Check.

'Entity History'

This folder contains the reports and settings for configuring Entity History recording.

'All System Settings'

This folder contains copies of all of the screens which contain settings which can be used to alter the behaviour of Confirm. These screens are also available in their appropriate folder e.g. the Feature System Settings will also appear in the Feature Lookups folder. The options available depend on the current User's permissions and the modules activated.

'All Seed Numbers'

This folder contains copies of all of the screens which contain Seed Numbers. Seed Numbers are required for creating many items in Confirm where a unique number is needed e.g. Jobs. These screens are also available in their appropriate folder e.g. the Job Seed Numbers will also appear in the Maintenance Lookups folder. The options available depend on the current User's permissions and the modules activated.

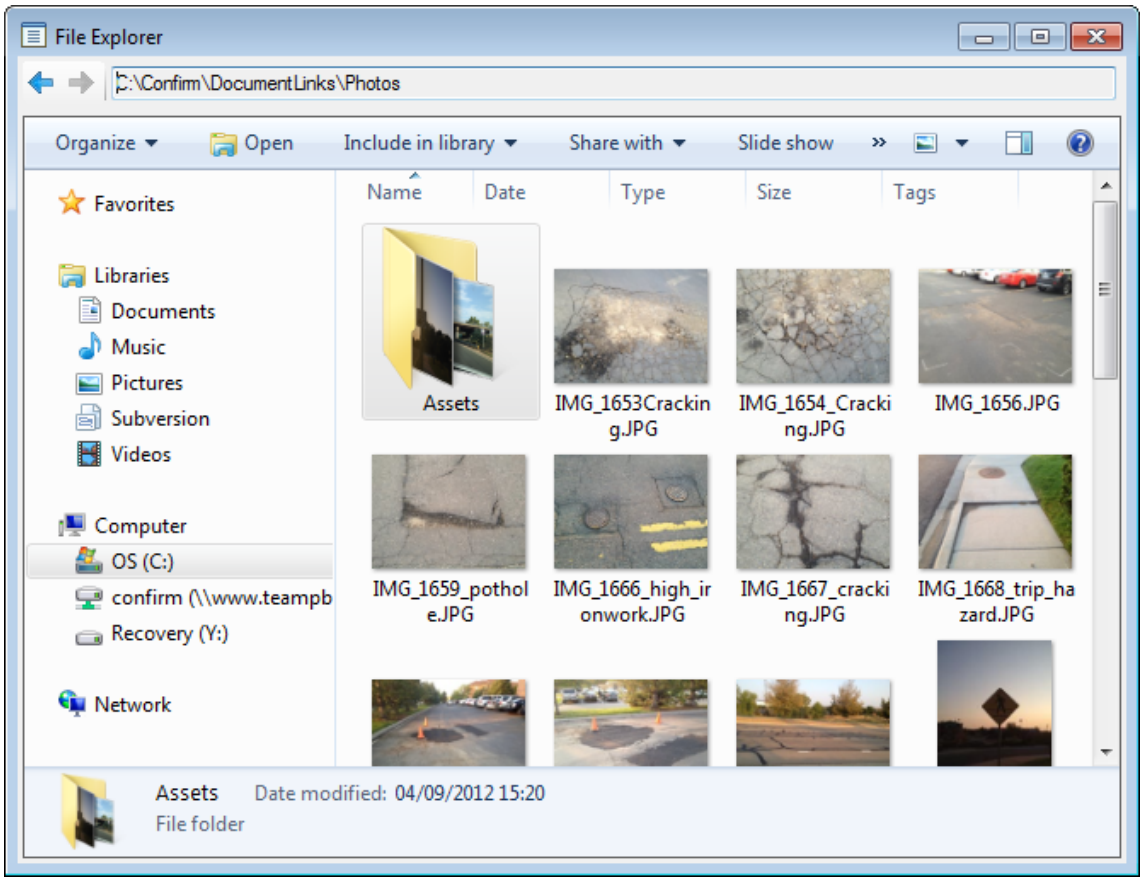
File Explorer

On Windows 7, Server 2008 or above, this menu option will open a Windows File Explorer within Confirm so that users can browse to files stored on their local or network drives.

Note: Older versions of Windows cannot open this screen and will inform the user that their operating system does not meet the required version.

Permissions and access are determined by the operating system and are not controlled through Confirm.

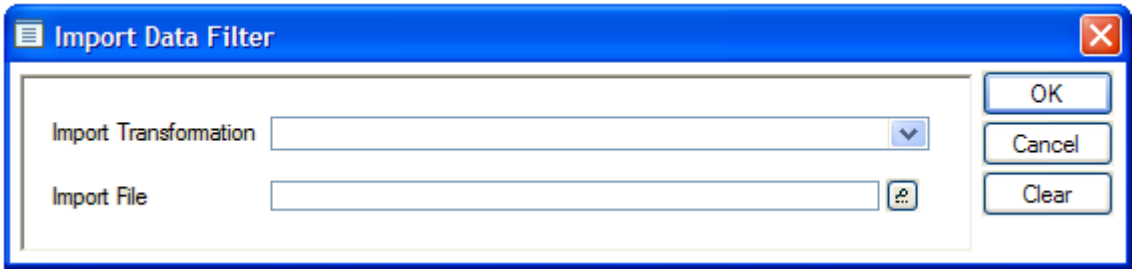
Note: For Citrix users the explorer will show the files and network driver of the server where Confirm is running.



Import Data

The Import Data utility provides the ability to load several different types of records into the Confirm database in a wide variety of file formats.

Importing data through this utility is equivalent to submitting a file to the Import Anything Agent. However, the utility will display messages on screen rather than create a .err file. It will also not move the file once processed, so if a file is imported from a folder being polled by the Import Anything Agent, the Agent will still process the file.



An Import Transformation may be selected – this will determine how the file is pre-processed and the Stylesheet to be applied. See **Import Transformations** for information on how to configure these.

If no Import Transformation is selected, the import file must be in the format the Import Anything Agent processes after a Transformation has been applied – for example a .tmp file generated by the Test button on the Import Transformations screen. For the Import Anything Agent, this is a comma delimited format, but for convenience this screen allows an equivalent tab delimited file to be supplied.

The file to be imported can then be chosen. The file pick button will default to the same folder as the last time the current User imported a file with this utility.

For full details on file structure and content, please refer to the specification section:

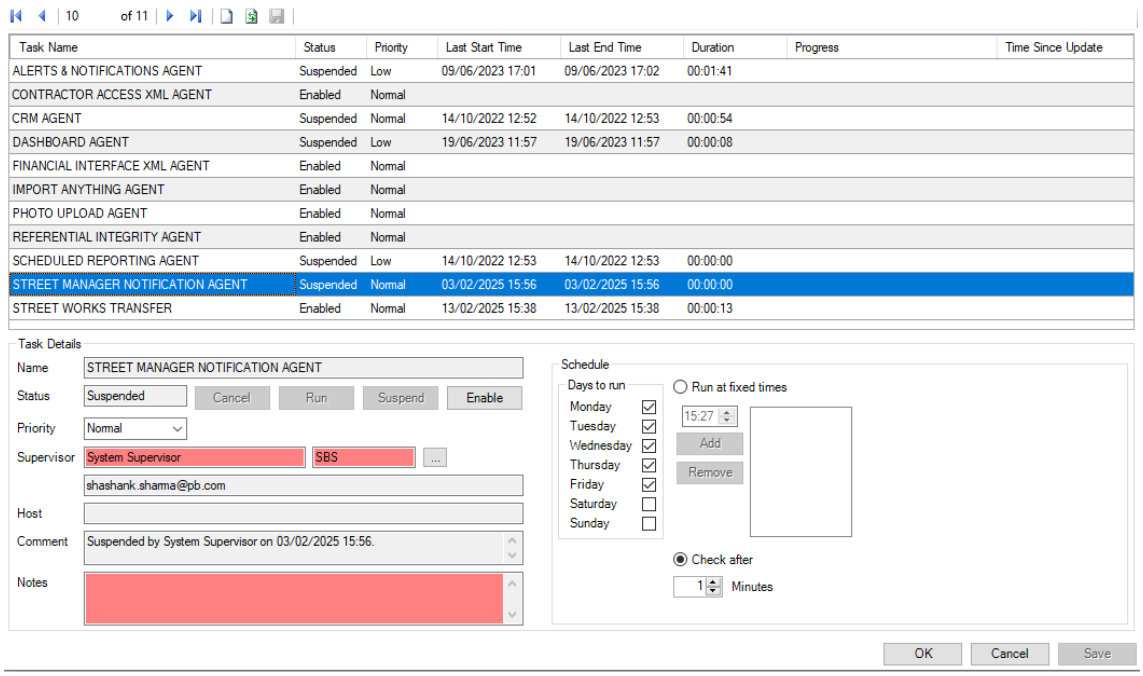
- **Confirm - Import Specification - Import Anything (LJM-59-129)**

Scheduled Tasks

This screen allows the user to view the current status of Agent tasks and edit their schedule. It also gives the user the ability to cancel a task that has not completed in a timely fashion.

When the screen first opens it will show the latest details for each Agent task. One row will be shown for each task.

The screen will automatically refresh every ten seconds and can also be manually refreshed using the button on the screen.



Task Name: The name of the task.

Status: The current status of the task. The status can be one of the following:

Queued: Denotes that task has been queued and will be picked up by Confirm Task Processor for processing in the next cycle.

Running: Denotes that the task is currently being processed.

Failed: Denotes that the task failed to be processed last time. The associated reason is shown in the Comment. A task at this status will be run again when it is next due according to its schedule.

Enabled: Denotes that the task is available to be run and will be run according to its schedule.

Suspended: Denotes that a task will not be run again until it is enabled.

Pending: Denotes that the task will be run on the next cycle regardless of its schedule.

Cancelling: Denotes that a cancellation request for the task has been sent to Task Processor.

For details on transition from one status to other refer **Agent Status Life cycle** page.

Priority: This column defines the priority in which tasks will be queued for processing. The available priorities in descending order are Critical, High, Normal and Low. Default priority of any task is Normal, and can be edited.

Last Start Time: The last date and time that the task was started.

Last End Time: The last date and time that the task finished.

Duration: If the task is currently processing this column displays how long it has been running for.

If the task run has finished the column will display how long the last run took to process.

The Duration values are shown in an hh:mm:ss format.

Progress: Displays percentage progress of a Running task.

Dashboard Agent and Scheduled Reporting Agent will also display the current report under process along with its start time.

Note: The progress update may not be continuous but in steps. For details, refer **Task Progress and Cancellation**.

Time Since Update: The time elapsed since progress was last updated, in HH:MM:SS format. This column is refreshed every 30 seconds and updated even if a small progress has been made to signify Agent is active. Applicable to queued and running tasks only.

For running agents, it's time since progress was last made. For queued agents, it's time since it was added to the queue.

Host: It displays name of the Task Processor machine running the task in the format [Host Info : <TaskProcessorMachineName>:<ProcessId of task>:<ThreadId of task>]. This information is useful in-case of multiple Task Processors serving the database. ProcessId and ThreadId may not be available for all Agent tasks.

Comment: Displays current comments for the task.

Comments cannot be edited by the User.

Supervisor: A Supervisor can be allocated to a task using the Supervisor pick button. The task will then send an e-mail to the Supervisor's e-mail address (as defined in the User Security screen) if any problems occur while processing.

Notes: Allows user notes to be entered against a task.

Cancel Button: Sends cancellation request for the Running task and updates the status as Cancelling. Task Processor then finishes the current state and skips further execution of the task. Once cancellation is complete, the status is set to Enabled. Cancel button also saves any unsaved on-screen changes.

Only tasks that are at Running status can be cancelled.

Note: Task cancelling may take up to a minute. For details, refer **Task Progress and Cancellation**.

Run Button: Sets the status to 'Pending' the Task Processor will schedule this task on its next cycle.

Suspend Button: Suspends the task so the Task Processor will not run it until it has been Enabled.

Enable Button: Enables the task so the Task Processor will run it according to its schedule.

Schedule

The schedule for the currently selected task can be viewed and edited in the Schedule section.

Days to run:	Allows the user to edit which days of the week a task will be scheduled to run.
Run at fixed times:	To schedule the task to run at fixed times, select this option. Use the time picker and the Add and Remove buttons to build a list of run times.
Check after:	Select this option for the task to run at fixed intervals.

Adding tasks

New tasks can be added and scheduled using the 'New' button. Note that only one task of each type can be added.

Task Progress and Cancellation

Task progress

Each Agent task has certain checkpoints which reports if an agent task has progressed to that checkpoint. Scheduled Tasks screen refreshes every 10 seconds and updates progress for agent tasks which have passed a checkpoint. Based on agent task and data to process in the agent task, task may take more time to reach a checkpoint and hence report progress in steps and not continuous. Task progress has been incorporated to give user the feedback whether a running task is making progress or has stuck. It is useful in case of long running agents where administrator may want to take a decision (like Cancel) to relinquish occupied resources for that task.

For reference, task progress and cancellation level for each agent task is given at the bottom of this page in a table.

Task Cancellation

Each Agent task has certain cancellation checkpoints where a running task can exit (or cancel) if cancellation has been issued. This has been done to safely stop the running task and maintain data in consistent state. However, if the Agent task takes longer than a minute to reach the next cancellation checkpoint, Task Processor forces the Agent task to terminate. This terminate behaviour applies to certain agents, which are listed below:

- Alerts and Notifications Agent
- Contractor Access XML Agent
- CRM Agent
- Enquiry FPN Delivery
- Financial Interface XML Agent
- Import Anything Agent
- Scheduled Reporting Agent
- Dashboard Agent
- Street Works Transfer
- Connector Agent

Agent task cancellation is intended to be done in case of long running, non-responding agent task or to cancel any unintended agent run. The Task Processor ensures that on reset, Agents exits gracefully.

For reference, task progress and cancellation level for each agent task is given at the bottom of this page in a table.

Task progress and cancellation levels:

Agent Task	Progress and Cancellation Level
Alerts & Notifications	Reports progress for each alert processed.
Connector	Reports progress for each file processed.
Contractor Access XML	Reports progress for each export file produced and each import file processed. **Note:** Since progress is reported at the per file level, there may be an interval of several minutes between updates if large files are involved.
CRM	Reports progress for each individual Enquiry processed.
Enquiry FPN Delivery	Reports progress for each Enquiry Penalty processed.

Agent Task	Progress and Cancellation Level
Financial Interface XML	Reports progress for export, followed by import. While importing files, reports progress for each file imported. **Note:** Since progress for export is reported for full export, there may be an interval of several minutes before progress is reported for importing files.
Full Text Index	Reports progress in percentage for the number of records processed
Import Address Agent	Reports progress in percentage for the number of transformations and files processed.
Import Anything	Reports progress at a detailed level during the importing of each file.
Photo Upload	Reports progress for each photo processed.
Referential Integrity	Reports progress for each entity record (feature, job, defect, enquiry, Street Works) update.
Scheduled Reporting	Reports progress for each Scheduled Report processed. **Note:** Since progress is reported at the per report level, there may be an interval of several minutes between updates if the retrieval of a specific reports take a long time.
Street Works Transfer	Reports progress for each entity type like Notice, restriction, FPN etc. and each record processed for each entity type.
Full Text Index	Reports progress in percentage for the number of records processed.

Security

The Security folder contains the tools for setting up Users and defining their rights within Confirm. These rights will be set in terms of program folders and forms they may view and edit (Group Security), and in terms of data they may view (Work Groups and Data Security Groups).

Users are set up under User Security, assigned a security Group, and a Work Group, inheriting from those groups the rights allocated to them.

There is one User already set up within Confirm - the System Supervisor. This User has complete rights within Confirm, and these rights should not be restricted in any way. System Supervisor is usually the only User with right to the complete Security folder. Other Users should only see the Change Password icon in the Security folder.

Change Password

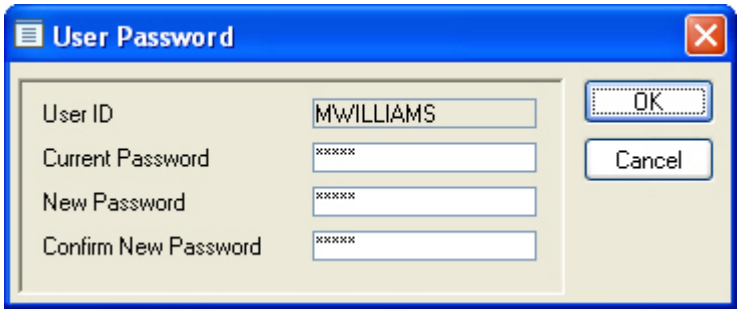
Change password allows a User to change their password.

They may do this because they wish to, or they may be required, by Confirm to change their password at regular intervals. The requirement to change password, and how often, is set in the **Security Settings** on page 37.

If the Security Settings are set to require the user to change password, they will be warned that their password has expired:



Clicking OK to the message will display the User Password screen:



The User password screen can also be displayed by selecting 'Change Password' from the Security folder on the Confirm Explorer.

User ID:	Will default to the User Id of the user who has logged in, or is attempting to login. The field is not editable.
Current Password:	Type in the current password.

New Password:	Type in a new password. **Note:** There may be a minimum password length. This is set in the **Security Settings** on page 37.
Confirm New Password:	Type the new password again.

Click OK to change the password. The User will be warned if the new password is unsuitable (it is not long enough) and will be asked to try again.

Note: If Active Directory authentication is used, User Password will use the Current and New Password values to change the Active Directory password of the user.

Note: Single Sign On users cannot change their password from this screen and these fields have been disabled. To reset or change password, please visit the Platform Universal login page.

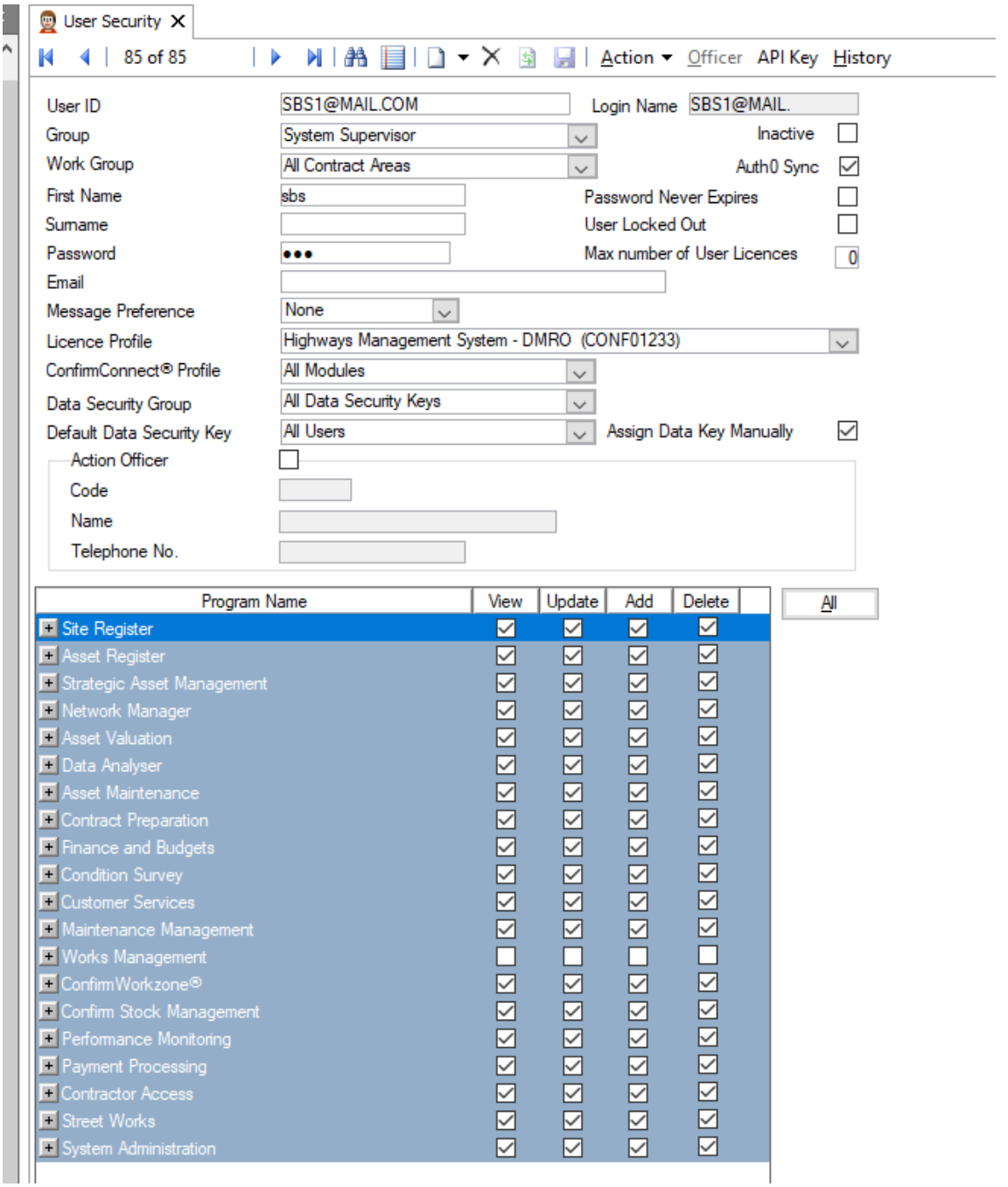
User Security

Users in Active Directory may also be managed through this screen – see **Active Directory User Management** for further details.

Each user of Confirm must be created as a User. They must be given a User ID and Password. Confirm can be set to track Users, and Action Officers may be linked to Users.

Users can share rights by belonging in the same Groups and Work Groups. Although Users inherit the program rights from the security Group, these program rights can be edited for individual Users.

Users may also have their rights determined by Data Security Groups and Data Security Keys. User's rights for using ConfirmConnect® modules will be determined on the basis of the Confirm-Connect® Profile selected on this screen.



Used ID: Enter the User ID that the User will supply when logging into Confirm. Up to 320 alphanumeric characters.

Login Name: Up to 10 alphanumeric characters.

Note: Both User ID and Login name must be unique for each user.

Group: Select a security group from the drop down list.

The drop down references the Group Security library.

On click of Save button, a message will appear asking whether you wish to copy the privileges from the specified group. Click -

- Yes - User inherits the ConfirmConnect® profile and program rights from the security group (these will appear at the bottom of the form).
- No - Leaves the program rights unchanged. In this case the program rights can be individually set for this user.

- Cancel - Cancels the save action.

Inactive:	If a User will no longer be using Confirm, tick this flag to hide their account by default on screens and lookups when a User field is displayed. Ticking 'Inactive' will automatically set the 'User Locked Out' setting to prevent the User from logging in to Confirm again. If the User is linked to an Action Officer, ticking the 'Inactive' flag will automatically set the 'Inactive' flag on that linked Action Officer.
Auth0 Sync:	When a user is created or updated with a valid email address as the User ID, they will be created in Auth0 if the tenant has been migrated to Auth0. The Auth0 sync option is checked when the Auth0 user creation or update is successful. 'Auth0 Sync flag' will not be ticked for contractor user For more details, visit Auth0 Configuration page
Work Group:	Select a Work Group from the drop down list. The drop down references the Work Group library.
First Name/ Surname:	Use these fields to enter the full name of the User. Up to 20 characters are allowed in each field.
Password:	Enter a password. Up to 128 alphanumeric characters. Minimum may be set in Security Settings. Anything typed in this field will appear as a series of asterisks **Note:** Active Directory password rules take precedence if the user has an Active Directory account. **Note:** Password field is disabled for Single Sign On users.
Password never Expires:	Check this to override the "Password Maximum Age" set in Security Settings. In this way, this user can be exempt from a requirement to change their password every so many days. **Note:** If no Maximum Password Age is set in the Security Settings, then the 'Password Never Expires' check box has no function.
User Locked out:	This box is checked when the User has been locked out as a result of repeated login attempts. If a User is locked out they will see a message telling them they have been locked out, and advising them to contact the System Administrator. To allow the User back into Confirm, uncheck this in their User record and save the change.
Max No User Licences:	Enter a number to set the maximum number of licences a user can consume at any one time. For each licence, user can log on to the Confirm client and Confirm Web interface simultaneously. Setting this to zero will set no limit.
Email:	Enter an email address. This can be the internal address - or the full internet address. The address is used with the Message Transfer Agents, where the appropriate modules are active.

Message Preference:	This field configures how the Task Processor will send Alert messages to this User. The field is only available if one or more of the Alerts modules is present. Select from one of the following values: • None - No Alert messages will be sent to this User. • Email - Alert messages for this User will be sent to their Email address. • Internal - Alert messages for this User will be viewable within Confirm via the Internal Messages screen. • Both - Alert messages for this User will be sent via email and also viewable on the Internal Messages screen.
Licence Profile:	Set the Licence Details (System Registration Details) that will be used for this User. This will determine which modules the user has access to. **Note:** If a Licence Override has been specified on the **Database Settings** screen, this Licence Profile entry will be ignored.
ConfirmConnect® Profile:	Set a ConfirmConnect® Profile for this User. This will grant the rights for accessing ConfirmConnect® modules for this user.
Data Security Group:	Set a Data Security Group for this User. This will default to the Work Group Data Security Group but can be changed.
Default Data Security Key:	The default Data Security Key that will be assigned to all new records that require Data Security Key fields, created by this User.
Assign Data Key Manually:	Check this to indicate if the User can view and alter the Data Security Key for a new or existing record that the User has rights to.

Action Officers can be created directly from the User screen by ticking the 'Action Officer' checkbox. For new Users, the checkbox will default from the **'General System Settings'** setting 'Prompt for the creation of an Action Officer with a new User'.

For an existing User with an associated Action Officer, the 'Action Officer' checkbox and related fields will be inactive.

Code:	Enter a unique Code for the Action Officer.
Name:	This will default to the First Name and Last Name of the User record but can be changed.
Telephone Number:	Enter a Telephone Number for the Action Officer.

Note: Irrespective of User Security, a Contractor User is not able to add a new User. They are also not able to see any User except themselves in the User Security screen.

Note: When Active Directory users are managed in Confirm, updates to users will also cause updates in Active Directory. see **Active Directory User Management** for further details.

Officer button

Use this to launch the full Action Officer screen.

Copy button

Click on the Copy button to create a new User based on the existing one. Enter personal details for the new User and save.

As well as inheriting the security privileges of the copied User, the new User will also have the same User Menu, Shortcuts, Dashboard and Home Page.

Action button

The Action button provides the following options.

Clear Dashboard

This button will clear the selected User's Dashboard setting, so that the Dashboard will not load automatically when that User opens Confirm.

This can be used if problems with the User's Dashboard cause difficulties when loading Confirm. This button does not permanently block the Dashboard, it only clears the User's auto-loading Dashboard setting.

Clear ConfirmWorkzone® Preferences

This button will clear the selected User's preferences in ConfirmWorkzone®.

This can be used if a User's preferences result in a very large volume of data being retrieved, causing difficulties logging into ConfirmWorkzone.

The next time the User logs into ConfirmWorkzone® they will be prompted to specify preferences just as if they were logging in for the first time.

Clear User

In order to delete a User from Confirm all child records within all database assets need to be cleared. The 'Clear' button can be used to remove these child records (such as settings) from the current database asset for the currently selected User record.

Note: If any non-child references exist within the current database asset such as Job Status Logs, the User is not able to be cleared.

This button is only enabled if the current User has 'Delete' privileges for the User screen.

Sync button

Use this to Synchronise user details between Confirm and Active Directory. This button is only displayed when Active Directory user management is enabled. See **Active Directory User Management**.

API Key button

Click on the API Key button to generate/regenerate the API Key that can be used to authenticate a Web API request, using 'Basic' HTTP Authentication. Authenticating with an API key will not use a license.

The API Key, along with the User ID, are supplied in the Web API request itself instead of having a separate authenticate request beforehand.

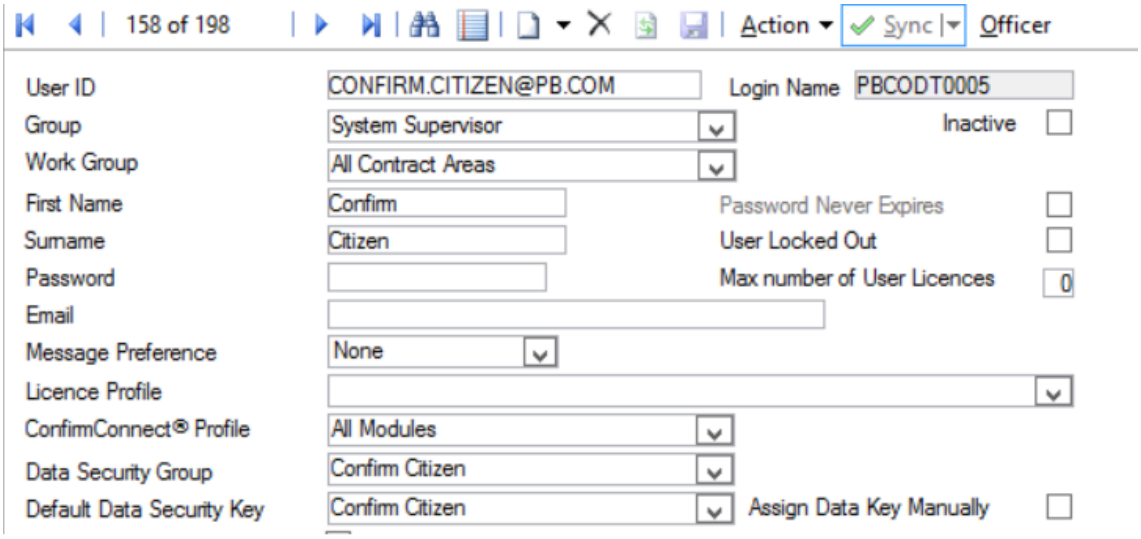
Active Directory user management

Confirm User Security will manage Active Directory users when Active Directory user management is enabled and used via Confirm Configuration Service.

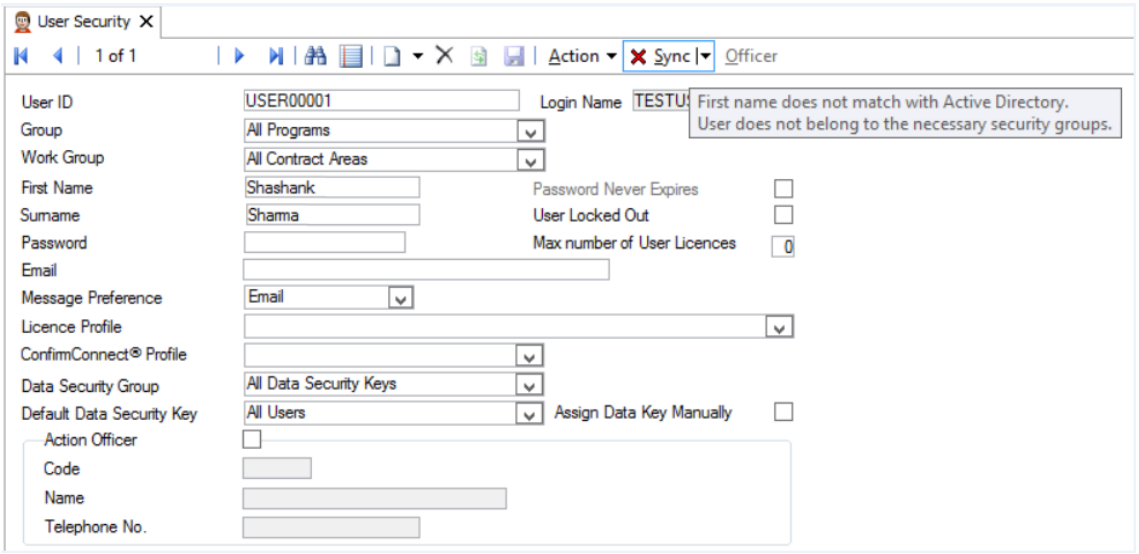
Creating/Updating users in Active Directory from Confirm

A System Administrator can use Confirm's user security screen to create users in Active Directory. When the System Administrator enters the Username in the User ID field and tabs out to a different field, there are following scenarios:

- The User exists neither in Confirm nor in Active Directory: Once the details are entered and the user hits Save, the user details are attempted to be saved in Active Directory. If successful, the screen shows a green tick on a grey-ed Sync menu as shown in the screen below.



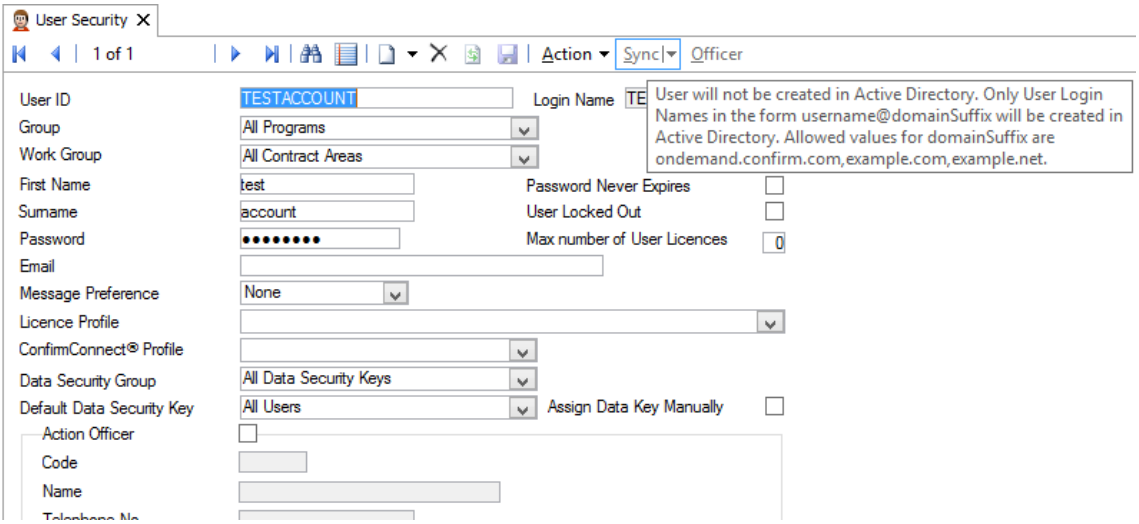
- The user exists in Confirm, but not in Active Directory or it exists at both the places but with differing attributes (i.e. first name, surname or display name are different, or the user does not belong to all the security groups for the tenant). In this case, the Sync menu is showed as enabled with a red cross. A tool-tip describes the difference between the user attributes (as shown below).



When a new user is created, the User ID field value needs to adhere to a specific pattern for the user to be successfully created in Active Directory. The pattern depends on the value of the

'Confirm Login Corresponds To' field in the **Security Settings** screen. If it is set to samAccount-Name, then the User ID must begin with a configured prefix followed by five digits. If it is set to userPrincipalName, then the User ID must be in the form of an email address ending in one of a list of configured domains. Please contact Confirm for more details on how to configure Active Directory User Management.

Note: Even if the User ID does not conform to the pattern, a user can still be created as a local user in Confirm. For such a user, the Sync menu will show up as disabled with a tool tip message explaining the expected User ID pattern.

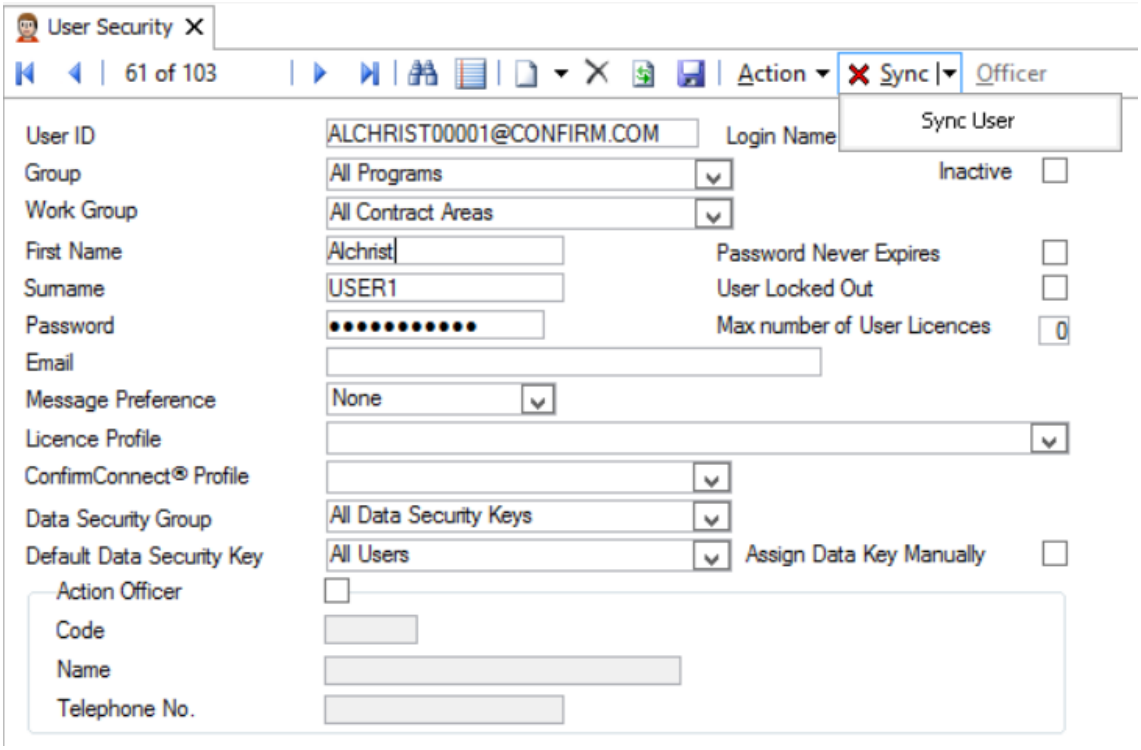


System Administrator can click on the Sync menu and then click Sync User option. This will attempt to override the user first name, surname and display name in AD and map the user to the configured security groups in AD. Note that when a user does not exist in AD, but exists in Confirm, the User gets created in AD as part of the Sync User operation. However, in that case, the System Administrator needs to re-enter the password for that user (existing Confirm password of the user cannot be transferred to AD since passwords, once saved, cannot be retrieved again but can only be validated for authentication. This is true for Confirm as well as Active directory).

Note: A display name in Active Directory is set to the first name and surname separated by a space.

Note: Password change will be required whenever a new user is created or an existing user's password is edited by System Administrator in Confirm user security screen.

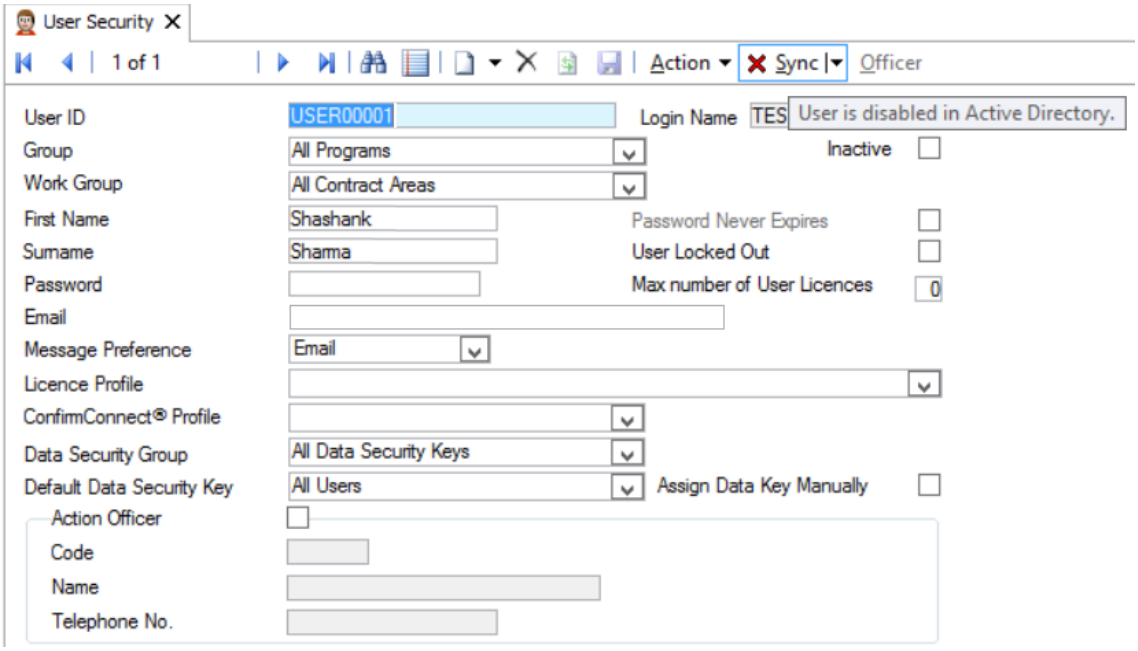
Note: If users want to change their own password, they should use the **Change Password** screen.



Note: As a part of updating an existing user, if the system administrator updates the password in Confirm user security screen, it resets the Active Directory password of the user to the new value entered on the user security screen.

Enabling a disabled Active Directory User from Confirm

If an Active directory user account is disabled, the Sync menu shows up as enabled with a red cross and a tool tip message (as shown in the screen show below).

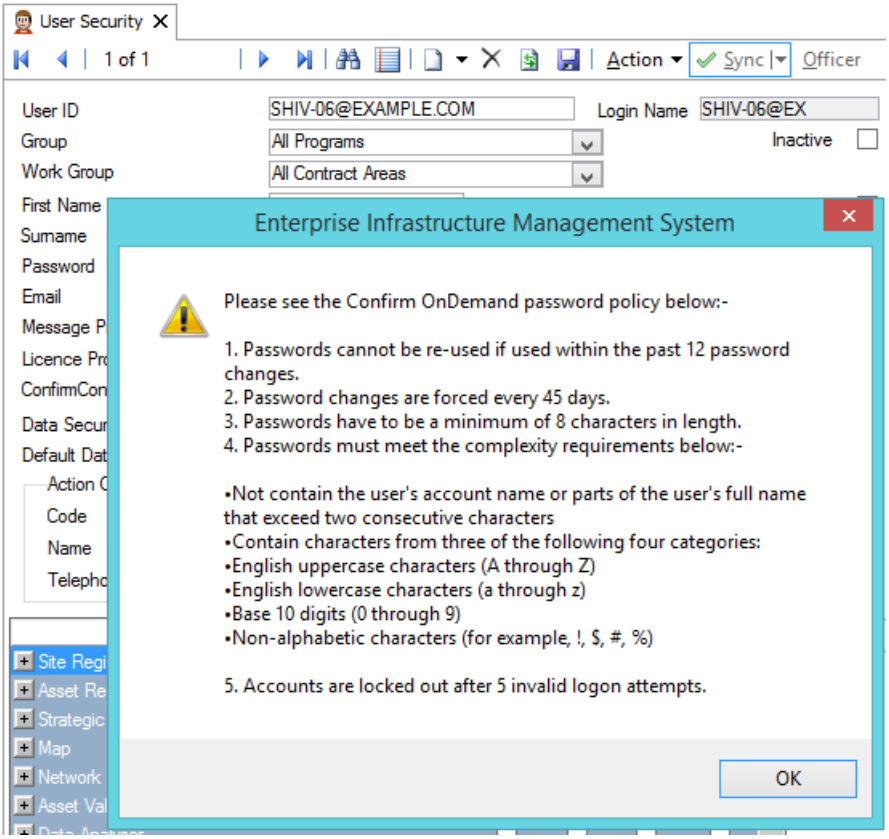


The System Administrator can use the Sync Now menu option to enable the user in Active Directory.

Errors reported while creating/updating a User in Active Directory

Certain errors can be reported while creating/updating a user in Active Directory.

For such errors, Confirm will show a dialog with the appropriate error message, but the user can still override them and create the user locally in Confirm (but they won't be created in Active Directory). However, if there is a password error (i.e. either it is blank or it does not match the configured AD password policy), then User cannot be created. The following screen shows an example of an error.



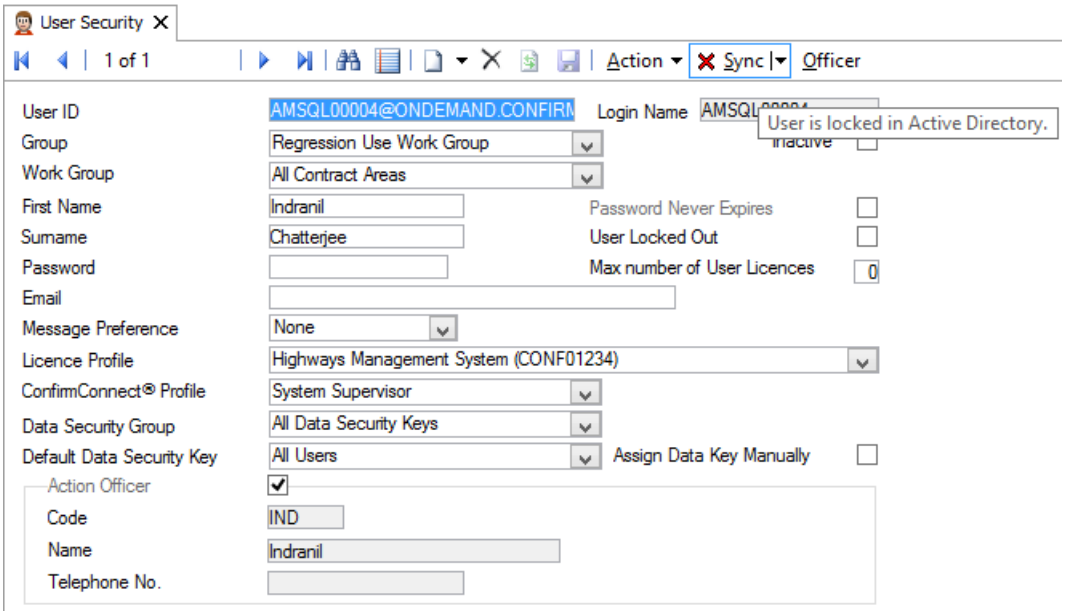
Deactivating/Deleting a user in Active Directory from Confirm

A user can either be deleted or marked inactive in Confirm. However, if Active Directory users are managed via Confirm User Security screen:

- When a User is marked as inactive in Confirm, the user gets removed from the Active directory security groups that may have been configured for the tenant profile. The user doesn't get deactivated/deleted from Active Directory. For example, is a user is deactivated in Confirm for Production tenant profile, he/she cannot access Production, but may still have access to Development or Test.
- The same User might still continue to be associated with other security groups in Active Directory.
- The behavior is same when a user gets deleted from Confirm.
- Reactivating a User in Confirm associates the user to the set of Active Directory security groups configured for the tenant profile. In case the user is not present in Active Directory, this process also creates the user.

Locking/unlocking a user in Active Directory from Confirm

A User cannot be locked in Active Directory from Confirm User Security screen. User locked in Active Directory (but not in Confirm), has the Sync menu enabled with a red cross with a tool tip message that the user is locked in Active Directory. A user can then be unlocked in Active Directory from Confirm by using the Sync User option in Sync menu.



Program Rights

The User Security and Group Security screens both have a program rights section at the bottom of the screen.

This section is set up in the same format as the Confirm Explorer Menu, containing folders and individual forms and utilities, with the same order and structure as the Confirm Explorer Menu. Some additional items are also present which are not shown on the Confirm Explorer Menu - these are described in the Security Options section below.

Rights can be assigned at the folder level which applies the rights to all sub-folders and items within that folder, or a folder can be expanded and program rights assigned to individual items within a folder. In each case View, Update, Add and Delete rights can be awarded.

View	Check this to allow Users to view the folder or form. If this is unchecked, the Update, Add and Delete boxes will uncheck also. Removing rights to view removes the folder, or form from the User's Explorer. They will no longer see the folder or icon.
Update	Check this to allow the User to edit records and save the changes, within the selected form or folder. If this is unchecked, while 'View' is checked, the User will see the records with all the fields greyed out and inactive.
Add	Check this to allow the User to add records. If this is unchecked, users will find the fields greyed out in blank forms - other than the Code field, which they can still use to enter existing codes to recall existing records.

Delete	Check this to allow Users to Delete records. If this is unchecked, Users will find the 'Delete' button inactive in the relevant forms.
Read Only	(9010 - Other Profiles - Read Only module) If the Read Only module is active in Confirm then this additional column will be shown in the Group and User screen. It shall be ticked to show which programs and utilities are available for a User to view which are active in another database profile. Example setup: • Profile A - Read Only module and Street Works are active. • Profile B - Read Only module and Customer Services are active. A User logging into Profile A would be able to have Read Only access to Customer Services. A User logging into Profile B would be able to have Read Only access to Customer Services. Items available as 'Read Only' will have the 'View' column ticked. To hide an item from a User, untick 'View'. The 'Read Only' column cannot be unticked.

Both screens have an 'All' button which awards all possible rights to the User or Group. If a User or Group will have all but a few rights, it is sometimes easier to award all rights and remove the few that are not required.

Security Options

As well as reflecting the folders, forms and utilities of the Confirm Explorer Menu, the program rights section on the User Security and Group Security screens also contains a number of other items which are special Security Options.

These items, which can be identified as those having '(Security)' on the end of the name, do not correspond to items on the Confirm Explorer Menu but control specific abilities or access, either within a particular form or more generally throughout the system.

The table below lists these Security Options and briefly describes the purpose and usage of each.

Product Area	Security Option	Description
Site Register	Can specify Workgroup for Routes	View access to this gives a User the ability to select the Work Group when creating a new Route (or Inspection Route, see below), rather than it being set to their own Work Group.
Asset Register	Can edit Central Asset Id	Update access to this gives a User the ability to edit the Central Asset Id of an existing Feature.
Asset Register	Can change Mapping Engine	View access to this gives a User the ability to change their current mapping engine by right clicking on the Map button at the top of a form or list.
Asset Register	Traffic Count Data	This controls access to the Traffic Count Survey option on the Feature screen Other button.
Asset Register	Feature Main	Update access to this controls whether a User has the ability to edit Asset Id, Feature Type, Start Date and Location of an existing Feature.

Product Area	Security Option	Description
Asset Register	Additional Tab Geography Tab Valuation Tab Smart Attributes Tab Referenced by Tab Nodes Tab	Update access to these control whether a User has the ability to edit information on these tabs on the Feature screen (subject to their privileges to update the Feature screen itself).
Asset Register	Attributes Tab	Update access to this controls whether a User has the ability to edit Attributes on the Feature screen (subject to their privileges to update the Feature screen itself). Add and Delete access to this control a User's access to the Add Attributes and Delete Attributes options on the Feature screen Action button.
Strategic Asset Management	Strategic Asset Management	Update access to this control whether a user can log in to the Strategic Asset Management application.
Map	Embedded Mapping	This controls a User's ability to interact with the map within a Street Works Wizard.
Condition Survey	Can Reset Incomplete Inspection Route	View access to this allows a User to reset an Inspection Route even when not all Features on the Inspection Route have been inspected.
Condition Survey	Can Sign-off Inspection Batch	View access to this allows a User to sign off an Inspection Batch (where applicable for the Inspection Type).
Condition Survey	Can specify Workgroup for Routes	View access to this gives a User the ability to select the Work Group when creating a new Inspection Route (or Route, see above), rather than it being set to their own Work Group.
Customer Services	Clear Links	Update access to this controls whether a User can 'Clear Links' on the Enquiry screen.
Fixed Penalty Notices	Can Accept Late Payments	This controls whether a User can enter a late payment using the 'Enter Payment' Wizard from the Offences screen.
Maintenance Management	Commit Button on Job	This controls access to the 'Commit' button on the Job screen.
Maintenance Management	Risk Assessment	This controls access to the Risk Assessments screen opened via the 'Risks' button on the Job screen.
Maintenance Management	Reassign in ConfirmConnect®	Allows a ConfirmConnect® User to Reassign Jobs assigned to them as a Job Officer.
ConfirmWorkzone®	ConfirmWorkzone® User Access	View and Update access to this control whether a User can log in to the ConfirmWorkzone® application.

Product Area	Security Option	Description
Street Works	Validation Override	This controls whether a User is able to create Street Works Notices where validation conditions or not met, or whether they are prevented from doing so.
Security	Document Links	This controls whether a User can access the Document Links screen from various Confirm screens, and whether they can Add, Update and Delete Document Link records within that screen.
Security	Additional Filtering	View access to this determines whether a User can see and use the 'More' button on various filter screens.

Group Security

Group Security sets up groups of Users who will all have the same program rights as well as the same ConfirmConnect® rights.

Program rights are defined at form or utility level, giving Users the right to 'View', 'Update', 'Add' and 'Delete'.

The program rights section of the screen is set up in the same format as the Explorer, giving folders and individual forms and utilities, in the same order and structure.

Buttons

Copy

Click on the Copy button to create a new User Security Group based on the existing one. Alter the Group Code and Name and save.

As well as inheriting the security privileges of the copied User Security Group, the new Group will also have the same User Group folder contents on the Menu.

Users

Updates all the Users in the selected Group to reflect the current rights for the Group.

This is used when a Groups rights has been modified and all the Users in the Group should be updated with the same rights.

Note: Care should be taken when using this button as any specific access rights given to Users in belonging to the Group will be reset to the default.

Program Rights

The User Security and Group Security screens both have a program rights section at the bottom of the screen.

This section is set up in the same format as the Confirm Explorer Menu, containing folders and individual forms and utilities, with the same order and structure as the Confirm Explorer Menu. Some additional items are also present which are not shown on the Confirm Explorer Menu - these are described in the Security Options section below.

Rights can be assigned at the folder level which applies the rights to all sub-folders and items within that folder, or a folder can be expanded and program rights assigned to individual items within a folder. In each case View, Update, Add and Delete rights can be awarded.

View	Check this to allow Users to view the folder or form. If this is unchecked, the Update, Add and Delete boxes will uncheck also. Removing rights to view removes the folder, or form from the User's Explorer. They will no longer see the folder or icon.
Update	Check this to allow the User to edit records and save the changes, within the selected form or folder. If this is unchecked, while 'View' is checked, the User will see the records with all the fields greyed out and inactive.
Add	Check this to allow the User to add records. If this is unchecked, users will find the fields greyed out in blank forms - other than the Code field, which they can still use to enter existing codes to recall existing records.
Delete	Check this to allow Users to Delete records. If this is unchecked, Users will find the 'Delete' button inactive in the relevant forms.
Read Only	(9010 - Other Profiles - Read Only module) If the Read Only module is active in Confirm then this additional column will be shown in the Group and User screen. It shall be ticked to show which programs and utilities are available for a User to view which are active in another database profile. Example setup: • Profile A - Read Only module and Street Works are active. • Profile B - Read Only module and Customer Services are active. A User logging into Profile A would be able to have Read Only access to Customer Services. A User logging into Profile B would be able to have Read Only access to Customer Services. Items available as 'Read Only' will have the 'View' column ticked. To hide an item from a User, untick 'View'. The 'Read Only' column cannot be unticked.

Both screens have an 'All' button which awards all possible rights to the User or Group. If a User or Group will have all but a few rights, it is sometimes easier to award all rights and remove the few that are not required.

Security Options

As well as reflecting the folders, forms and utilities of the Confirm Explorer Menu, the program rights section on the User Security and Group Security screens also contains a number of other items which are special Security Options.

These items, which can be identified as those having '(Security)' on the end of the name, do not correspond to items on the Confirm Explorer Menu but control specific abilities or access, either within a particular form or more generally throughout the system.

The table below lists these Security Options and briefly describes the purpose and usage of each.

Product Area	Security Option	Description
Site Register	Can specify Workgroup for Routes	View access to this gives a User the ability to select the Work Group when creating a new Route (or Inspection Route, see below), rather than it being set to their own Work Group.
Asset Register	Can edit Central Asset Id	Update access to this gives a User the ability to edit the Central Asset Id of an existing Feature.
Asset Register	Can change Mapping Engine	View access to this gives a User the ability to change their current mapping engine by right clicking on the Map button at the top of a form or list.
Asset Register	Traffic Count Data	This controls access to the Traffic Count Survey option on the Feature screen Other button.
Asset Register	Feature Main	Update access to this controls whether a User has the ability to edit Asset Id, Feature Type, Start Date and Location of an existing Feature.
Asset Register	Additional Tab Geography Tab Valuation Tab Smart Attributes Tab Referenced by Tab Nodes Tab	Update access to these control whether a User has the ability to edit information on these tabs on the Feature screen (subject to their privileges to update the Feature screen itself).
Asset Register	Attributes Tab	Update access to this controls whether a User has the ability to edit Attributes on the Feature screen (subject to their privileges to update the Feature screen itself). Add and Delete access to this control a User's access to the Add Attributes and Delete Attributes options on the Feature screen Action button.
Strategic Asset Management	Strategic Asset Management	Update access to this control whether a user can log in to the Strategic Asset Management application.
Map	Embedded Mapping	This controls a User's ability to interact with the map within a Street Works Wizard.
Condition Survey	Can Reset Incomplete Inspection Route	View access to this allows a User to reset an Inspection Route even when not all Features on the Inspection Route have been inspected.
Condition Survey	Can Sign-off Inspection Batch	View access to this allows a User to sign off an Inspection Batch (where applicable for the Inspection Type).
Condition Survey	Can specify Workgroup for Routes	View access to this gives a User the ability to select the Work Group when creating a new Inspection Route (or Route, see above), rather than it being set to their own Work Group.

Product Area	Security Option	Description
Customer Services	Clear Links	Update access to this controls whether a User can 'Clear Links' on the Enquiry screen.
Fixed Penalty Notices	Can Accept Late Payments	This controls whether a User can enter a late payment using the 'Enter Payment' Wizard from the Offences screen.
Maintenance Management	Commit Button on Job	This controls access to the 'Commit' button on the Job screen.
Maintenance Management	Risk Assessment	This controls access to the Risk Assessments screen opened via the 'Risks' button on the Job screen.
Maintenance Management	Reassign in ConfirmConnect®	Allows a ConfirmConnect® User to Reassign Jobs assigned to them as a Job Officer.
Confirm-Workzone®	ConfirmWorkzone® User Access	View and Update access to this control whether a User can log in to the ConfirmWorkzone® application.
Street Works	Validation Override	This controls whether a User is able to create Street Works Notices where validation conditions or not met, or whether they are prevented from doing so.
Security	Document Links	This controls whether a User can access the Document Links screen from various Confirm screens, and whether they can Add, Update and Delete Document Link records within that screen.
Security	Additional Filtering	View access to this determines whether a User can see and use the 'More' button on various filter screens.

Work Groups

Work Groups are created where it is necessary to restrict groups of Users to particular areas of data. The areas of data are defined by Contract Area. Work Groups are assigned Contract Areas they may work in, and they will be restricted to Features (and optionally, Sites) within those Contract Areas.

Data may also be restricted by Data Security Group.

Additionally, Work Groups are each assigned their own set of Seed Numbers for Orders, Inspections batches and Defects, Monitoring batches, Failures and Notices, Jobs, Customers and Enquiries.

Work Groups also set up their own Site Routes, and a Site Route created in one Work Group is not visible to Users in another Work Group.

The implications of setting up Work Groups are such that, unless you have a pressing need to segregate data in this way, the best advice is not to use more than the one 'All Contract Areas' Work Group, which is provided with the program.

Be aware that Work Group segregation will only take place for Features (and, optionally, Sites). All libraries (other than Routes), including the central SOR libraries, will still be shared.

Note: Confirm contains one Work Group by default: ALL - All Contract Areas. This Work Group should not be removed or changed. It contains the System Supervisor User.

Each Work Group has a code (up to four alphanumeric characters) and a name (up to 30 characters)

Default Data Security Group	Select a Data Security Group from the drop down list to assign the related Data Security Keys to this Work Group. The drop down list references the Data Security Group library. **Data Security Groups** on page 35
Terminology Override	This allows a Confirm terminology to be selected as the default for any User in this Work Group. This overrides the system level setting and the default terminology determined by the executable used to run Confirm. It is also possible for this setting to be overridden for individual Users on the **General User Settings** on page 41 screen.

Work Group - Contract Areas tab

Users in this Work Group will be able to view Features in the Contract Areas listed on this tab

To add or delete Contract Areas, select the Contract Areas tab, and click on the 'Detail' button to display the Work Group Contract Area form.

Add Contract Areas to the Work Group by selecting a Contract Area from the drop down in the Contract Area field.

Delete Contract Areas by selecting the record and clicking on the 'Delete' button

The Contract Area drop down references the **Contract Area** lookup

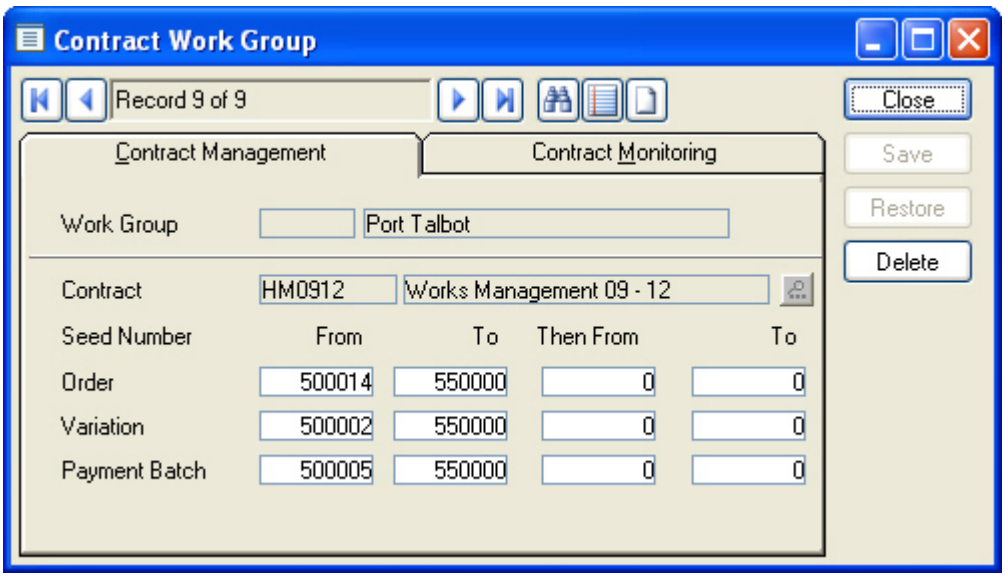
Note: When you create Contract Areas in the Contract Area Lookup, they will be automatically added to the Work Group that the User you have logged in as belongs in.

Work Group - Contract Order Pad tab

(Contract Management and Contract Monitoring modules)

The Contract Order Pad tab lists all the Contracts this Work Group will work with, and sets seed numbers for them within those Contracts

Select the Contract Order Pad tab and click on the 'Detail' button to display the Contract Work Group form:



Add Contracts to the Work Group by selecting from the Contract field pick list.

The Pick list references the Contract Library

Contract Preparation\Contract

Note: When you create Contracts, they will be automatically added to the Work Group that the User you have logged in as belongs in.

Setting Seed Numbers

Seed numbers are set, for each Contract, within each Work Group.

Contract Management Seed Numbers are set on the Contract Management tab and will be used to issue:

- Works Orders - both Routine and Non Routine Orders are numbered sequentially from the same range of numbers.
- Variations Orders
- Payment Batches

Contract Monitoring Seed Numbers are set on the Contract Monitoring tab and will be used to issue:

- Monitoring inspection batches
- Failures
- Notices

Two ranges are available allowing you to issues two batches of non-contiguous numbers.

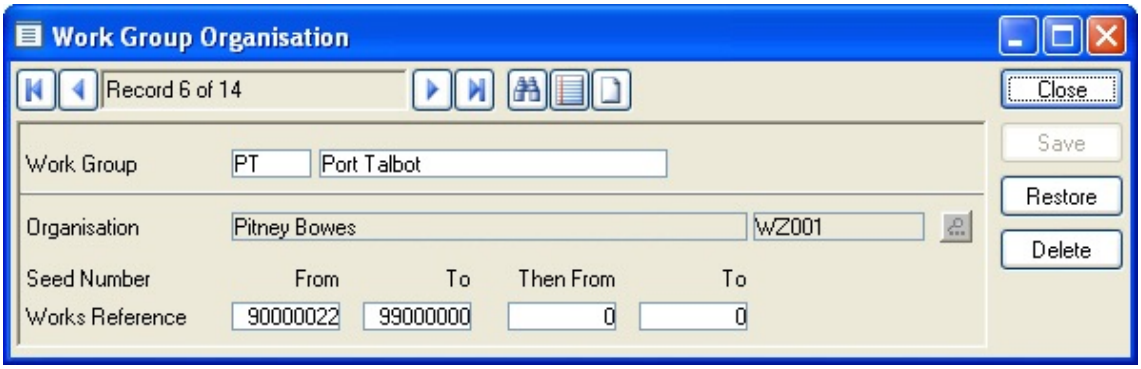
Bear in mind that:

- Only Work Groups who will be raising Orders will need Seed number for Orders (or Variations or Payments). Only Work Groups involved in Contract Monitoring will need seed numbers for Monitoring Batches, Failures and Notices
- Each Work Group must have a unique range of numbers, but if you issue one range to start with, which proves to be too few numbers, you can later come back and use the second range. You can also amend the 'To' number to make room for a range of numbers for a new Work Groups.

Each Contract has its own total range of numbers from 1 to 99999999. These numbers need to be distributed amongst the Work Groups working with that Contract.

Work Group - Organisations tab

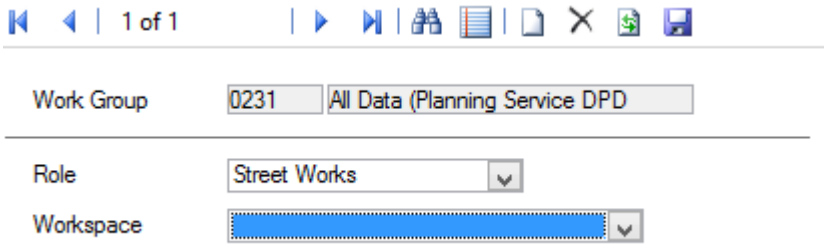
(SWR - Street Works Initiation module)



The Work Group Organisation form is used to assign seed numbers to each Organisation who will initiate Street Works Notices, and receiving Comments.

Work Group - Map Workspace tab

(0425 - Map module)



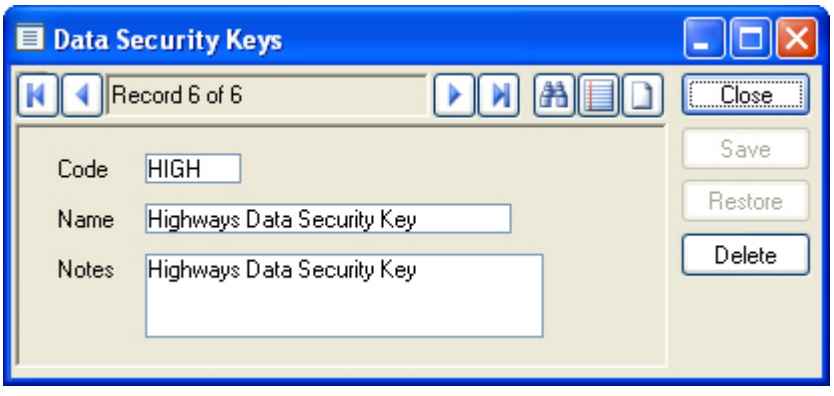
The Work Group Map Workspace form is used to assign Map Workspaces to a Workgroup so that users are automatically given a workspace when they launch the corresponding screen.

Role:	Selecting a Role from this drop down will assign the chosen **Workspace** to the corresponding Confirm screen. Roles and their corresponding screens: • Street Works - Applies to All Street Works screens containing a Map • NSG - Applies to NSG Manager • Map - Applies to Map
Workspace:	Select a Workspace from this list. Only those Workspaces with the chosen **Role** will be shown.

Data Security Keys

Data Security Keys are used to supplement the form security by determining whether a User can view or update specific records within various forms that the User has access to.

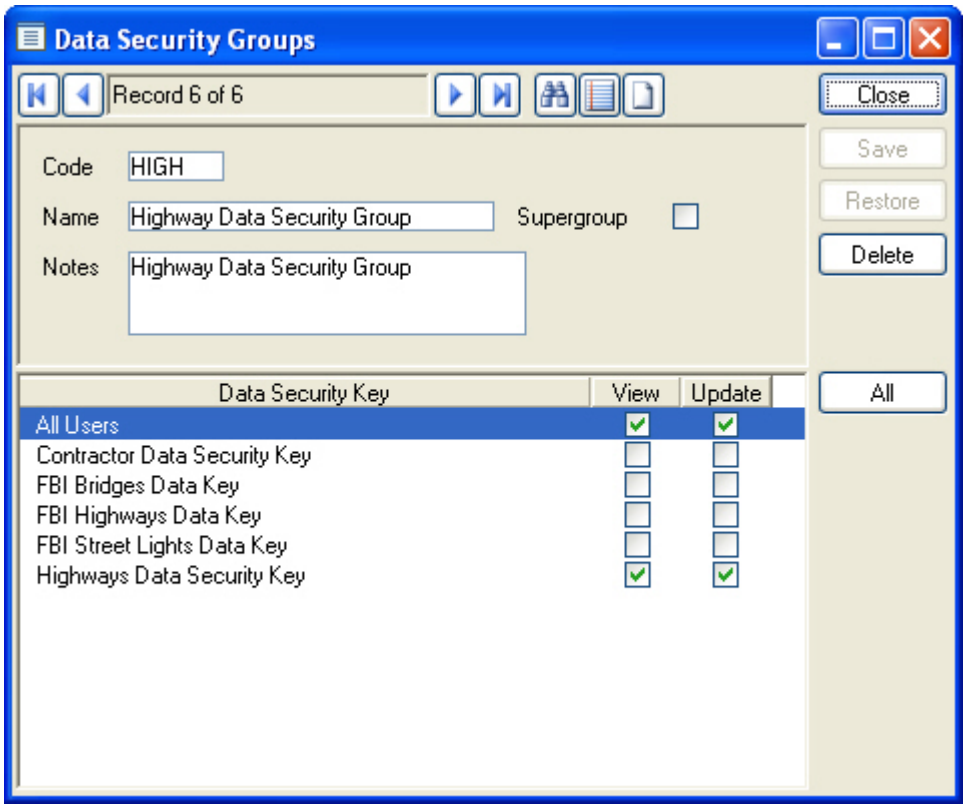
Note: The 'All Users' Data Key is created by Confirm. This is the one Data Key that will always be available to all Users.



Code:	Up to six alphanumeric characters.
Name:	Up to 50 characters.
Notes:	An optional field for a short description of the Data Security Key.

Data Security Groups

Data Security Groups are used to define data groups and their access to records within Confirm. Each Confirm User is associated with a Data Security Group. The User is therefore granted access to the records allocated to that Data Security Group.



Code:	Up to six alphanumeric characters.
Name:	Up to 50 characters.
Notes:	An optional field for a description of the Data Security Group.
Supergroup:	At least one Data Security Group in Confirm must be flagged as a 'Super-group'. Supergroups will be automatically assigned full privileges ('View' and 'Update' ticked) to all Data Security Keys.

The bottom section of the Data Security Group form automatically displays all of the Data Security Keys that have been previously created.

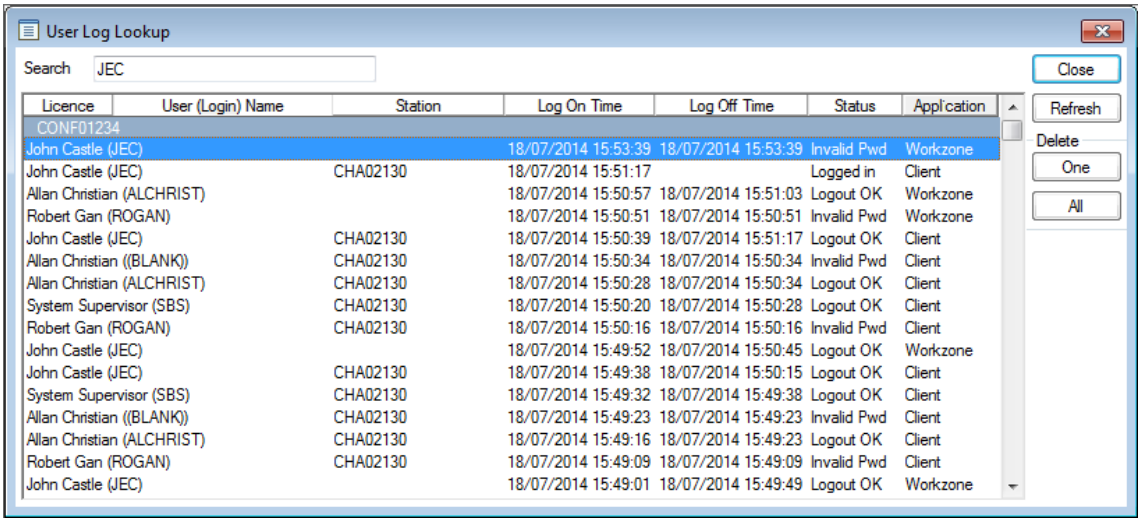
Data Security Keys are assigned to the Data Security Group by ticking the 'View' and/or 'Update' check boxes where applicable for the relevant Data Security Keys.

The absence of a Data Key for a User's Data Security Group means that the User will not be able to see data with this key attached (it will not exist as far as they are concerned).

Note: The 'All Users' Data Key is created by Confirm. This is the one Data Key that will always be available to all Users. Confirm will not allow it to be unavailable for any Data Security Group. Every Data Security Group will always have 'View' and 'Update' access to it.

User Logs

The 'User Log' screen displays login details for Confirm. These can be viewed / deleted.



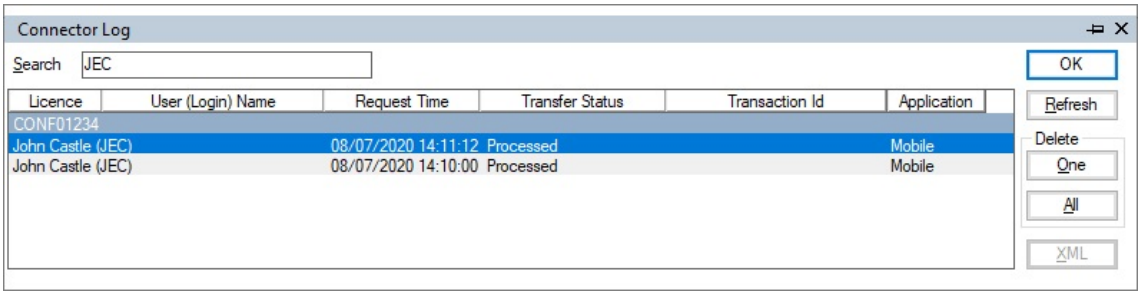
Records will only be created if 'All' or 'Failed' has been selected for the User Log in the **Security Settings** on page 37.

The User log provides a list of Users who have logged in, or made failed attempts to log in, since the log was created or last cleared.

To clear the log, click the Delete 'All' button. Login records can be deleted manually from the list by selecting the required record and clicking the Delete 'One' button.

Connector Logs

The 'Connector Log' screen displays logged Confirm Connector requests. These can be viewed / deleted.



All successful Connector transactions will be logged, grouped by the Licence number that the Connector connected to. The log displays the User supplied in the XML request as well as the Time that the request was processed.

The 'Transfer Status' column has the following possible values:

'Processed' - The Connector request was successfully processed. These records are for information only.

'Processed (with Warnings)' - The Connector request was partially processed and Transfer Warnings have been recorded. The 'XML' button will be enabled which can be used to view the details. The User will first be prompted for a filename to save the XML and then ask 'Do you wish to launch the saved file?' answering Yes will run the file in the application associated with the XML file extension.

Application will either be Connector or Mobile. Mobile covers log entries created when authentication fails in ConfirmConnect as well as Mobile Connector requests.

Note: Mobile Connector requests can come from ConfirmConnect, but the API is published so requests can come from other sources including the Mapping Interface.

Connector Requests that totally fail validation will not be logged. The Connector will display the cause of the fault. On a Confirm device the fault will also be displayed.

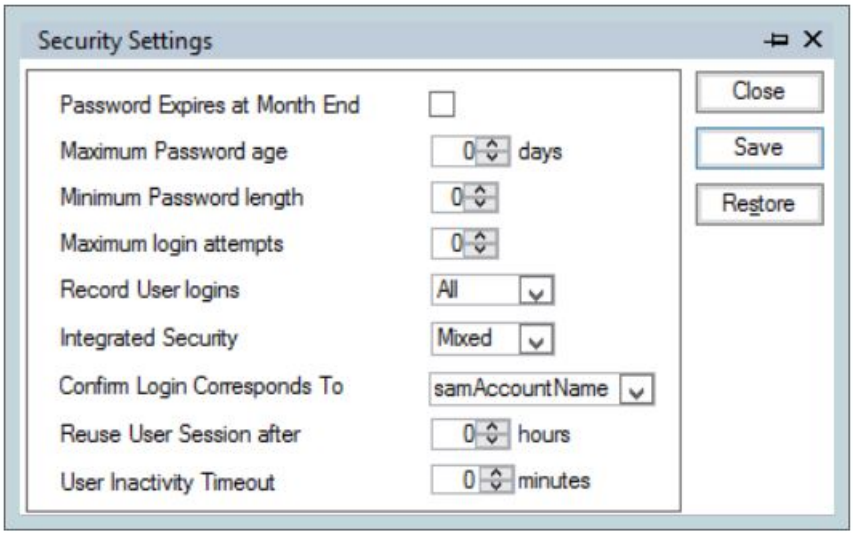
The Transaction Id column will display the value from the Connector Request XML if supplied. When supplied, the Connector will perform duplication check before importing any data. If a duplicate Transaction Id already exists in the database the import will be rejected and the Connector will display an error.

Note: Unlike the User Log, the recording of Connector logs is not dependant on any system settings.

Security Settings

Confirm can be configured with Security defaults.

Note: The default entry of zero (0) indicates that no restriction is set.



Password Expires at Month End:	Check this to require Users to change their Password at the end of each month. **Note:** Users who have 'Password never Expires' checked in their User Security record will be excluded from the requirement to change their password.
Maximum Password Age:	This field will only be editable if 'Password Expires at Month End is not checked. Sets the length of time (in days) before Users will be required to change their password. When the current password expires the user will be prompted to change their password and the User Password form will be displayed. **Note:** Users who have 'Password never Expires' checked in their User Security record will be excluded from the requirement to change their password.
Minimum Password Length:	The minimum length (in characters) for a password. **Note:** Maximum length for a password is fixed at 128 characters

Maximum Login Attempts:	Enter a number to impose a limit on the number of times a User may attempt to login before being locked out of the system.
Record User Logins:	The system can maintain a log of all User logins, with dates and times of login in and login out again. The drop down menu gives three choices: 'None' - No log will be kept 'All' - All logins will be recorded 'Failed' - A log will be kept of failed attempts to login only.
Integrated Security:	Integrated Security allows a User access to Confirm based on their network login details that they have already provided to the operating system. If Integrated Security is to be used, the User's Confirm 'User ID' must match their network login name. Confirm Users login details are held in the **'User Security library'**. Select the level of Integrated Security required from: 'None' - The User must login to Confirm manually using their Confirm User ID and password. 'Full' - To use the network login details to access Confirm. This option will refuse entry to Confirm to any users who's network login details do not match the 'User ID' held on a User record. 'Mixed' - To use the network login details to access Confirm, and to display the Confirm login screen if the network login details cannot be found in a Confirm user record.
Confirm Login Corresponds To:	This setting is applicable when: - Integrated Security is Set to Full/Mixed and logging in to Confirm Client OR - 'AuthProviderType' is set to ActiveDirectory in Registry and logging in to ConfirmWeb , ConfirmConnect® or ConfirmWorkzone® Once AD authentication is successful, and setting is set to value: 1. samAccountName: Network Login Name in AD will be used to verify the Confirm userID to allow login to application. This is the default setting. 2. userPrincipalName: User Principal name in AD will be used to verify the Confirm userID to allow login to application.
Reuse User Session After:	When logging in, Confirm will check the number of current sessions against the maximum specified on the User Security screen and System Registration screen. If neither maximum has been reached, the User will be logged in. If the maximum for the User (or Licence) has been reached, Confirm will attempt to automatically reuse the oldest session for that User (or Licence). A session can only be reused if it is older than the number of hours set here.
User Inactivity Timeout:	When logged in, Confirm will monitor the continuous user inactivity time. If user inactivity time exceeds the value specified here, user session will be locked and user needs to unlock the screen by entering their password on User Session Lock screen. If the value of this setting is set to 0, user's session will not be locked for inactivity.

General System Settings

The General System Settings screen allow you to set default behaviour for many areas of Confirm.

Priority	The Priority entered here will provide the default Priority for Jobs. Select a Priority from the drop down list. The drop down list references the Priority Lookup. **Asset Maintenance\Maintenance Lookups**
Routine Price Factor	The Price Factor entered here is the one the system will use when calculating Routine Maintenance. The Price Factor 'Routine Maintenance' will be entered by default and it is not recommended that you change this.
Show Sites	This option governs whether Sites will be restricted by Work Group in the same way that Features are. The drop down list offers two options: 'All' - All Sites will be seen by all Work Groups. 'By Work Group' - Site will be restricted, by Contract Area, to the Groups with rights to view those Contract Areas.
Working Day	Set the start and end time of the working day. This will be used by the system to calculate follow-ups that have been set in hours and flagged for 'Working days'. When a Follow Up is marked as being a Working Day the calculated follow up date & time will always be within these hours. Where these times are not specified the defaults used will be 00:00:00 (mid-night) to 23:59:59.
Date Tolerance	Enter the number of years before and after the current system date which a User can type into a date field in Confirm. This prevents Users from mistakenly entering invalid dates.
Week 1 is the first week in: that contains a:	(AM - Routine Maintenance 0720 & ConfirmConnect® Jobs 7030) Identify the first Week of the year to be used with Routine Works on Confirm-Connect®. Identify the the first week of the year which is in the specified month and also contains the specified day.
Time Zone	This is the Time Zone that should be used by Confirm server components, such as the Task Processor and Connector, when working out log times for various entities, e.g. Enquiry / Job status updates. **Note:** This setting does not apply to Confirm client components, such as the main client application and ConfirmConnect®. Confirm client components will always use the local time on a user's PC/Device when determining the current date/time.
Authority Detail	Enter a name, address, telephone number and fax number. This will appear as a header on print outs for Orders and Notices. Any blank fields will be ignored in the print out.
Logo Bitmap	Enter the path to a bitmap file. The bitmap will then be used as a header on Orders and Notices in place of the Authority details i.e. the Authority Name, Address & Telephone will not be displayed if a bitmap is selected.

Support Email Address	Enter the Email Address to which a Confirm Error Report Form should be sent when a User clicks the 'Email' button. If this is not set, Error Report Forms will be sent to the Confirm Confirm Support Email Address.
Present a clear sheet...	This check box is set by default and indicates that a new blank form will be displayed when a record is saved. To keep the just-saved record in the form after saving, uncheck the box.
Show visual indicator...	When set, some of the window buttons that provide a link between different parts of Confirm will provide a visual indication that there is one or more related records present. This indication may be in the form of a number representing the number of related records on buttons that link directly to another part of confirm or an icon on buttons that cause a fly-out menu to be displayed with further options. The options on the fly-out menus will be display the number of related records where appropriate. When this is not set buttons and fly-out menus will only display the name of the associated area of Confirm.
Prompt for the creation...	When set, this will default the 'Action Officer' checkbox on the User Security screen.
Hide Action Officer distance ...	Setting this will remove the Action Officer distance column, related to GPS Tracking, on the Action Officer lookup.
Restrict Action Officer assignment by Work Group	Setting this will disable the Work Group field on the Action Officer Filter on the following forms: • Programmed Inspections (Street Works) • Inspections (Street Works) • Inspection Sampling (Street Works) • Create FPN Wizard (Fixed Penalty Notices)
Suppress warning about extracting...	Tick this to not display the 'This selection may extract a large amount of data and take some time. Do you wish to continue?' message when filtering for records in Confirm. **Note:** This setting is system-wide so affects all Users.
Max Import Errors/Warnings	(Contractor Access Import) (Import Anything) Defaults to 10,000. This can be changed to set the amount of errors or warnings that will be displayed during an import.
Terminology override	This allows a Confirm terminology to be selected as the default for any User in the system. This overrides the default terminology determined by the executable used to run Confirm. It is also possible for this setting to be overridden on a per Work Group basis, and for individual Users to override this by selecting a terminology on the **General User Settings** on page 41 screen.
Highlight editable fields	Tick this to make Confirm highlight the fields on a form that can be edited. When ticked, the colour picker will open for a selection to be made. It is possible for Users to use a different colour by changing it in the **General User Settings** on page 41 screen.
Highlight currently selected field	Tick this to make Confirm highlight the field that the cursor is currently in for all Users. When ticked, the colour picker will open for a selection to be made.

	It is possible for Users to use a different colour by changing it in the **General User Settings** on page 41 screen.
Proxy server name...	It is possible to configure the Confirm client to use a Proxy Server when performing OD Batch transfers, Document Exchange or Restriction transfers. These four fields provide Confirm with the connection details for the Proxy server. The Proxy server name should contain the URL or TCP/IP address of the Proxy server. If this field is blank then Confirm will assume there is no Proxy server. The other settings will be specific to the Proxy server's configuration.
Proxy server port	IP port number for the Proxy server.
Proxy username	Username for connection to the Proxy server.
Proxy password	Password for connection to the Proxy server.

General User Settings

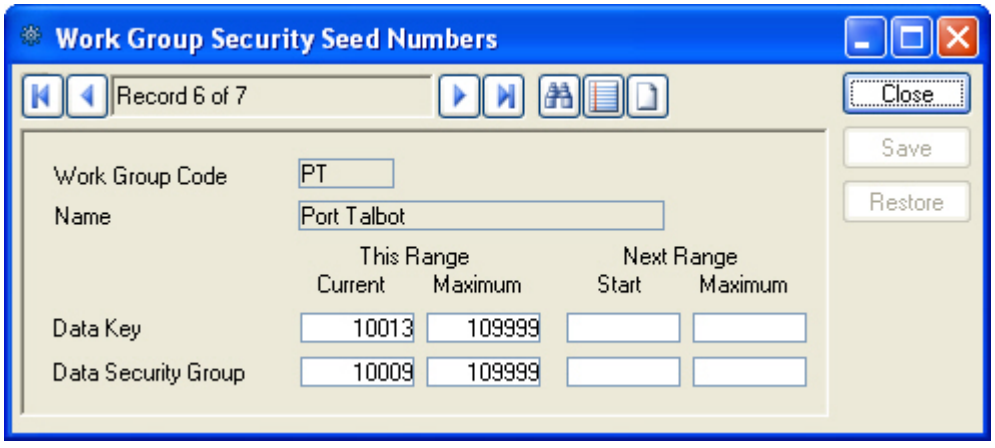
This screen is used to configure settings that apply only to the currently logged in User.

Terminology override	This allows a Confirm terminology to be selected for the currently logged in User. This overrides the setting for the User's Work Group. If a specific terminology is selected here it will be applied immediately to the application and menu, and to any subsequently opened screens.
Highlight editable fields	It is possible to have Confirm highlight all the fields that are currently editable using either a System or User specified colour. The system wide setting is set on the **General System Settings** screen and can be overridden: • 'None' - Prevent Confirm from highlighting fields. • 'Use System Setting' - Use the colour specified in the **General System Settings**. • 'Use Specified Colour' - Select from the available colours.
Highlight currently selected field	It is also possible to have Confirm highlight the field that the cursor is currently in. This is done in the same way as the Highlight editable fields setting, with both a system wide and user specific options.
Retrieve records when opening a window	The default behaviour when a Confirm window opens is for it to initially show a blank record. For a User who more often wants to retrieve existing records rather than enter new ones, this behaviour can be altered by ticking this setting. If this is done, windows will open automatically to retrieve records - either presenting a filter screen, or in the case of a lookup table with no filter, populating the screen.
Open screens as Tabs	Ticking this setting (default) will use a tabbed user interface. Un-ticking will display Confirm Data Entry Forms in classic mode. See **User Interface** for further details.
Check Internal Messages after ...	This setting is for the Internal Messages functionality. The system will check at intervals for any new Internal Messages. By default, the interval is 300 seconds (5 minutes), but this can be altered for a particular User.

If the value is set to 0 seconds, the system will check for the presence of Internal Messages when a User logs in, but there will be no subsequent checks. The User will still be able to open and refresh the Internal Messages window to see new Internal Messages.

Open Internal Messages screen on login	Check this box to automatically open the Internal Messages screen when the User first logs into the system. The changes made will apply to any screens that are opened after the settings have been saved.
Allow map rotation in ConfirmConnect®	Check this box to allow the maps in ConfirmConnect® to be rotated. Users are also able to set this via the About / Settings screen in ConfirmConnect®. When the setting is turned off then the maps will not rotate. **Note:** If set via Confirm, the user will only see the change when they sign out of ConfirmConnect® and back in again.
General Document Visibility	This setting enables users to set document visibility to "Public" or "Private" at an individual level for Non–Street Manager entities - Jobs, Defects, Enquiries, and Features. These tags are purely informational and are not imposing any security restrictions on document visibility. By default, the visibility at the user level is set to "None", but users can choose to change it to either "Public" or "Private" using the provided dropdown. When the visibility is set to "None" at the user level, the Tenant-level setting(configured in Confirm Web) will apply for tagging documents in Confirm Web and Connect. However, if the user-level setting is configured to "Public" or "Private", it will override the Tenant-level setting for document visibility in both Web and Connect.

Security Seed Numbers



Security Seed Numbers are required for each Work Group so that Data Keys and Data Security Groups can be created.

System Configuration

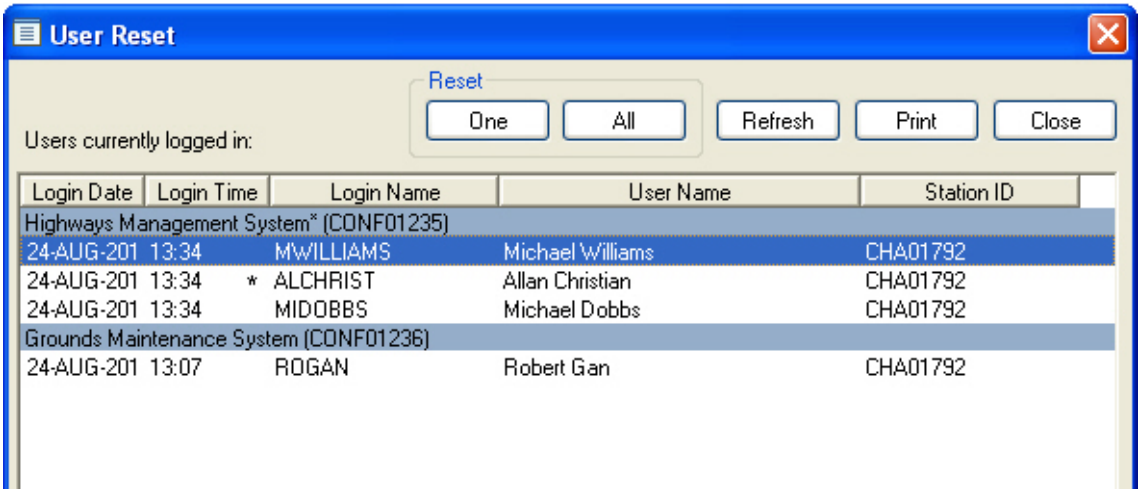
The System Configuration folder provides system details of the active modules and the database settings. These will have been set by Confirm and should not normally be altered in any way.

Also provided are tools for resetting Users, and for running a Database Schema Check, which will highlight any problem in the underlying database structure.

User Reset

The User reset allows you to view all the users currently logged in, and to log out users. This would normally be done when 'rogue' users are in the list, i.e. users who logged out incorrectly, and still appear in the list even though they are not in Confirm. Their presence in the list may be preventing other, legitimate users from login into Confirm on the grounds that all the user licences have been used up.

The active licence and the User currently logged in will be highlighted with a '*'.



Reset

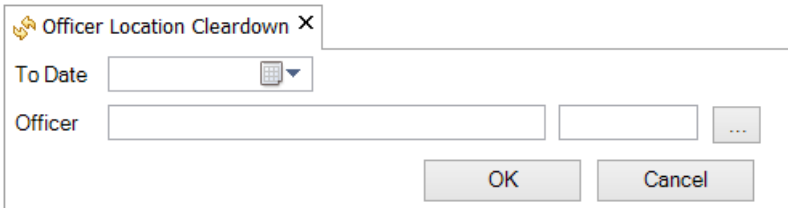
One:	Select a User in the list and click the 'One' button to remove this User from the list.
All:	Click the 'All' button to remove all Users from the list.

Internal Messages Cleardown

The Internal Messages Cleardown utility is used to permanently delete old messages of specified users from the database so they do not show on the Internal Messages screen. Please refer to the Alerts and Notifications manual for further information.

Officer Location Cleardown

The Officer Location Cleardown utility allows to permanently delete historical Location data of officers from the database.



To Date	All the Officer Location records prior to the mentioned date will be deleted.
Officer	Select Officer whose Location data is to be deleted.

System Registration

The System Registration details all the information related to your licence on Confirm, ConfirmConnect®, and ConfirmWorkzone®. The licence number, the number of users and datasets, the licence expiry date, and details of the Confirm modules that are 'switched on' in your version of Confirm. The ConfirmConnect® section shows the number of devices as well as the number of licences per ConfirmConnect® modules that are purchased in your version.

You cannot change any of these details without authorisation from Confirm , since to save changes a valid Access Code must be entered.

You may print out these details by clicking on the 'Print' button in the System Registration form.

The System Registration screen has an Export button to copy Licence and module details:

- To the clipboard
- To an XML file

This can be used to send these details to Confirm to make it easier to make changes to Licence configuration and issue new Access Codes.

The screen has a corresponding Import button which can be used to enter (paste) details supplied by Confirm without having to tick individual modules. A user with read only privileges to the System Registration screen cannot edit details using the paste button.

Database Schema Check

The Database Schema Check examines the schema of the database, and compares it to the expected schema for the current version of Confirm.

It will report errors such as columns missing from the database or defined as the wrong data type. These errors can cause the software to crash or can have serious performance implications. Any errors should be reported to Confirm.

It will also report warnings such as additional optional columns in tables. These may be valid differences introduced intentionally to a particular database in which case your database administrator should be aware of them. If unexpected warnings are reported, or if there is any doubt, these should also be reported to Confirm.

It is recommended that a Database Schema Check is carried out prior to any Confirm upgrade to detect issues that might impact the successful upgrade of the database schema. It is also recommended that a Database Schema Check is carried out after any Confirm upgrade to ensure the schema has been upgraded correctly.

Database Settings

The Database Setting form is used to set up the link between the software (the Confirm program which is installed on an individual PC) and the database (which will be centrally stored and available to all users).

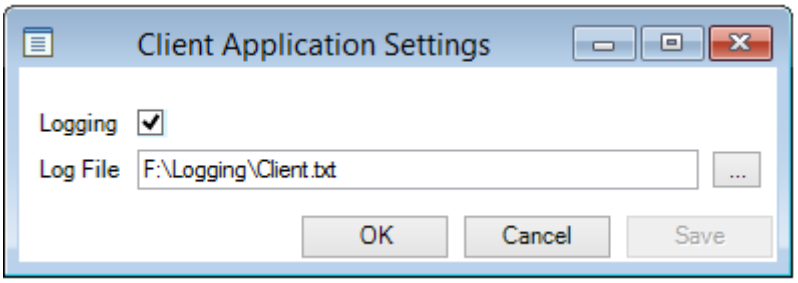
Note: If a Licence Override is specified on this screen then the this licence will be used for all users logging in via this Profile Name and any **Licence Profile** specified against the user will be ignored.

Note: If logged into an Oracle 12c database and connection details are added/edited for an Oracle 19c database, then an error will occur but you are now able to continue with the save.

Note: If logged into an Oracle 19c database then it is not possible to add or edit connection details for an Oracle 12c database.

Confirm client Settings

This screen contains settings which are used by the Confirm client. The settings displayed on this screen are all stored in the Confirm database and are used when the client is connected to the database.



Logging: When ticked, the Confirm client will write progress messages and all errors to the log file.

Note: Even when this is not ticked, logging information will still be written to file if an error occurs (provided a log file is supplied).

Log File: Supply the path and filename which will be used to store database logging information during the running of the Confirm client.

Connector Settings

This screen contains settings which are used by the Confirm Connector. The settings displayed on this screen are all stored in the Confirm database and are used when a request is processed.

In previous Confirm versions, these settings were only stored in the registry of the server running the Connector. If the settings are blank and the Connector is used, the settings from the server running the Connector will be saved into the database.



Logging: When ticked, the Confirm Connector will write progress messages and all errors to the log file. This is ticked by default.

Log File: Supply the path and filename which will be used to store logging information during the running of the Confirm Connector.

Dump Data: When ticked, additional debugging information will be added into the log file as set via the Log File setting and additional IN and OUT files will be created for each request/response. The IN and OUT files are created in sub-folders by year, month and day, e.g. …\2013\01\21\...IN.log. This can create a large number of files very quickly, so it is advised to only use this when troubleshooting problems. This is unticked by default.

Timeout: This value is used to produce a Time Out error when the Connectors processing does not complete within the time allocated.

The default for this setting is 1800 seconds (30 minutes) but can be changed if required. If this value is not set then a default of 30 minutes is used.

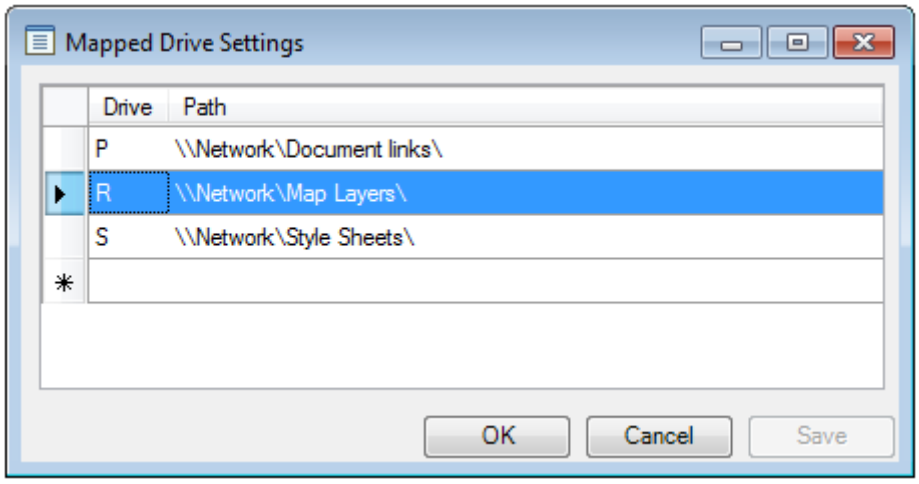
For further information about the installation and configuration of the Confirm Connector, please refer to the installation guide provided.

Mapped Drive Settings

The Mapped Drive Settings screen allows drive letters to be assigned to UNC paths which can then be used by ConfirmConnect® and Confirm Task Processor.

This allows the Confirm Task Processor and ConfirmConnect® to access these network locations without needing to map a drive letter on the server.

For Example: The **Document Links System Settings** screen has its **Document Store Folder** mapped to "P:\Photos\". A "P" drive is mapped on this screen which has a Path set to "\\Network\Document Links\". This allows ConfirmConnect® to read the full path as "\\Network\Document Links\Photos\"



Drive: Select the Drive letter you wish to associate a UNC path to.

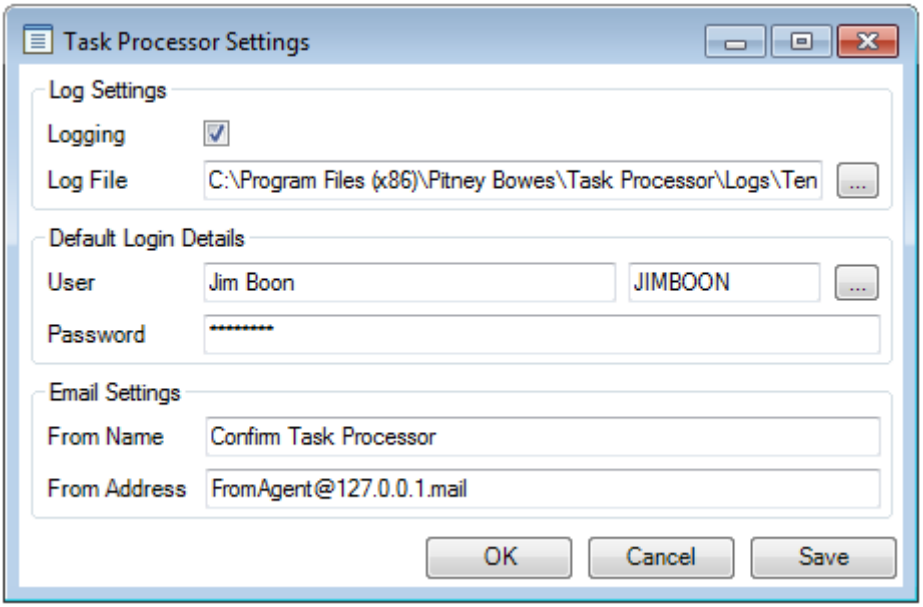
Path: Enter the UNC path for the Drive letter.

To delete an existing record select the entire row (as highlighted in the screenshot) and press delete key on the keyboard.

Note: It is recommended to restart IIS on the ConfirmConnect® server for changes to take effect.

Task Processor Settings

This screen contains settings which are used by the Task Processor. The settings displayed on this screen are all stored in the Confirm database and are used when Agent Tasks are connected to the database.



Logging: When ticked, the Confirm Task Processor will write progress messages and all errors to the log file.

Note: Even when this is not ticked, logging information will still be written to file if an error occurs (provided a log file is supplied).

Log File:	Supply the path and filename which will be used to store database logging information during the running of the Confirm Task Processor.
User:	The default user which the Confirm Task Processor will use to log in to the Confirm database. A valid User and Password must be entered for the Task Processor to operate.
Password:	The password for the user specified in the User field.

Email Settings specifies the sender details which will be mentioned in the mail sent via Task processor. This is applicable for all mails sent in case of agent errors, scheduled reports and email alerts.

From Name:	The sender's name as required to be seen by the mail recipient .
From Address:	The sender's email address as required to be seen by the mail recipient.

ConfirmConnect® Settings

This screen contains system settings which are used with Confirm Mobile devices.

Frequency of storing GPS information:	Determines how long the Mobile device should wait in between storing GPS positions.
Distance Tolerance for logging GPS information:	Determines how far an Action Officer must travel (in metres) in order for a new GPS location to be stored.
Tracking Frequency:	Determines how long the Mobile device should wait in between sending GPS location updates to Confirm.
Default Defect From Enquiry:	When ticked, Defects created from Enquiries have their Description and Location defaulted from the Enquiry Subject, Number and Location.
Notes field mandatory on all “Not Assessed” Observations on Asset and Condition Surveys	When ticked observations on Asset and Condition Survey must either have an assessed condition entered, or if set to a not assessed condition must have notes entered.
Capture Job Costs	Determines whether Cost Capture will occur for Jobs. Select from: • None • Productive Time Only: Costs will only be logged when Jobs are Completed / Paused and at the End of Day • All Costs: As above but Travel / Break time is also recorded when Jobs are Started / Resumed
Capture Survey Costs	Determines whether Cost Capture will occur for Asset / Condition Survey Tasks. Select from: • None • Productive Time Only: Costs will only be logged when Surveys are Completed / Paused and at the End of Day • All Costs: As above but Travel / Break time is also recorded when Surveys are Started / Resumed

SOR Required for Cost Capture	When ticked, an SOR must always be specified on the Cost Capture screen
Cost Code mandatory when new Defect creates and commits Works Order	Tick this to make the Cost Code mandatory when creating Defects in Confirm-Connect® that will result in a Works Order being created and committed. Whether a Works Order is created and committed is decided by the 'Device Creation of Orders' field of the Priority for the new Defect.
Routine Works earliest Due Date Tolerance	Routine Maintenance tasks appear if the earliest due date on any of the Regime Items is within this value. The Default value is 30 days.
Job future Start Date Tolerance:	Supply the number of days in the future which will be used by Confirm to restrict the Jobs being sent to the mobile device. The restriction is based on the Job Estimated Start date. If a Job does not have a Start date then it will be transferred to the device. Setting of 1 means Jobs for Today. Setting of 0 means no restriction will be applied to the Start Date. **Note:** If an officer downloads tasks on their device after the End of Day time (from General System Settings), then the next day's work will be downloaded as well.
Enquiry Future Scheduled Date Tolerance:	Supply a number of days which will be used by Confirm to restrict the Enquiries scheduled in ConfirmWorkzone being sent to the mobile device based on the Enquiry scheduled date.
Filter Features by Attribute Type	Select an Attribute Type. This will add a filter option in ConfirmConnect that will allow filtering of your Tasks and Features returned by What's Going on Here results . **Note:** Changing this value will require ConfirmConnect users to sign out and back in before the new value will take effect. **Note:** If the ConfirmConnect user does not have data security access to the chosen Attribute Type, the Attribute Filter option will not appear.
Order Features on What's Going on Here by Attribute Type	Select a Feature Attribute Type. This is used to determine the order in which What's Going on Here results for Features with Geometry are displayed on top of one another. The Attribute Values are used to determine the order (display order has no effect). High values will be placed on top of any lower values. e.g. 5 will be placed on top of 4 or lower.
Start of Day: Inspection Type	Select a 'Condition Survey' Inspection Type from the list so that an extra option on the ConfirmConnect menu will appear, named as per the given Inspection Type Name, in order for Users to be able to perform a 'Start of Day' Inspection.
Default Custom Maps Folder	Select a folder that contains the custom map file(s) to be downloaded to ConfirmConnect. This is the default location and can be overridden on a per profile basis from the **ConfirmConnect Profile** screen. **Note:** it is possible to use each of the following options: • **UNC path**, for example: \\servername\sharename\maps\confirmconnect\sqlite • **Drive Mapping**, for example: Default Custom maps folder is set to "Z:\confirmconnect\sqlite". A drive letter is then mapped, on the ConfirmConnect server, as Z: which points to "\\servername\sharename\maps".

- **Mapped Drive Setting** a drive letter is configured to the UNC path of "\\servername\sharename". The Default Custom Maps Folder is then set to "Z:\confirmconnect\sqlite". This approach removes the need to map a drive on the ConfirmConnect web server.

Run Works Order Discrepancy Data Source	Enable this option to force automatic Job committal, from Defects raised by ConfirmConnect, to use the Works Order Validation data source specified on the **Contract Management System Settings** screen. **Note:** Only Error messages will be displayed back to the ConfirmConnect user. If the Data source is configured to show a warning, this will not appear on the users transfer list.

ConfirmWorkzone Settings

This screen contains settings which are used by ConfirmWorkzone. The settings displayed on this screen are all stored in the Confirm database and are used by the application.

Calculate Travel Time	When ticked, ConfirmWorkzone will automatically calculate the travel time between Scheduled Jobs. If Calculate Travel Time is unticked, or it's not possible to retrieve the Calculated Travel Time data (e.g. because a Task doesn't have coordinates), then ConfirmWorkzone will use the Default Travel Time value (see below). **Note:** When Calculate Travel Time is ticked, it is not possible to manually edit the travel times in ConfirmWorkzone.
Consecutive Interval	The interval between Scheduled Jobs where ConfirmWorkzone expects that there would not be a return to Depot. Where the interval is exceeded then the Travel Time calculation will be based on a return to Depot taking place.
Default Travel Time	The default travel time for Jobs and Enquiries, where the automatic travel time calculation has not been used (Calculate Travel Time setting is unticked or there is no coordinate data available to calculate travel time automatically).
Refresh Rate	Configure the frequency with which ConfirmWorkzone will poll the database for new or updated Jobs. The polling is carried out every 5 minutes by default.
Earliest Cut Off	If specified, ConfirmWorkzone will treat this number of days before the current date as a cut off for downloading Jobs or Enquiries. • Jobs whose Estimated Start and End Date and Due Date are all before the cut off date will not be downloaded. • Enquiries whose earliest Target Date of any Outstanding Commitment on the Enquiry is before the cut off date will not be downloaded. **Note:** If the Enquiry does not have any Outstanding Commitments, then the Followup (by) Date of the Enquiry will be used instead of the Commitment Target Date. This can be used if a system has large numbers of historical Jobs which are no longer required but have not been closed, to prevent them cluttering ConfirmWorkzone.

Latest Cut Off	If specified, ConfirmWorkzone will treat this number of days after the current date as a cut off for downloading Jobs and Enquiries. • Jobs whose Estimated Start and End Date and Due Date are all after the cut off date will not be downloaded. • Enquiries whose earliest Target Date of any Outstanding Commitment on the Enquiry is after the cut off date will not be downloaded. **Note:** If the Enquiry does not have any Outstanding Commitments, then the Followup (by) Date of the Enquiry will be used instead of the Commitment Target Date. This can be used if a system has a large number Jobs which do not need attention until later, to prevent them cluttering ConfirmWorkzone.
Hide Job Item Values	When ticked, ConfirmWorkzone will not display the Value of any Job Items.
Work Types	Only Jobs whose Work Type is ticked in this list will be displayed in the ConfirmWorkzone task list. This does not affect tasks displayed on the ConfirmWorkzone schedule.
External Map Name	The name of the external map system as it will appear on the link in ConfirmWorkzone and on the web Job and Defect screens
External Map URL	The URL of an external map system that can be linked to via ConfirmWorkzone and the web Job and Defect screens. The URL must be able to take a latitude and longitude as parameters. Use the placeholders {lat} and {lon} to specify where the parameters belong in the URL. For example, to configure a link to Google Street View, use the following URL: https://www.google.com/maps?q=&layer=c&cbll={lat},{lon}
Enquiry Default Duration	Default duration of the Enquiry task as used by ConfirmWorkzone, where the **Enquiry SubjectDefault Duration**has not been set.

Confirm Web Log Settings

This screen contains settings which are used by the Confirm web interface. The settings displayed on this screen are stored within the Confirm database and are used by the application.

Logging:	When ticked, the Confirm web interface will write progress messages and all errors to the log file. This is ticked by default
Log File:	Supply the path and filename which will be used to store database logging information during the running of the Confirm on the web.

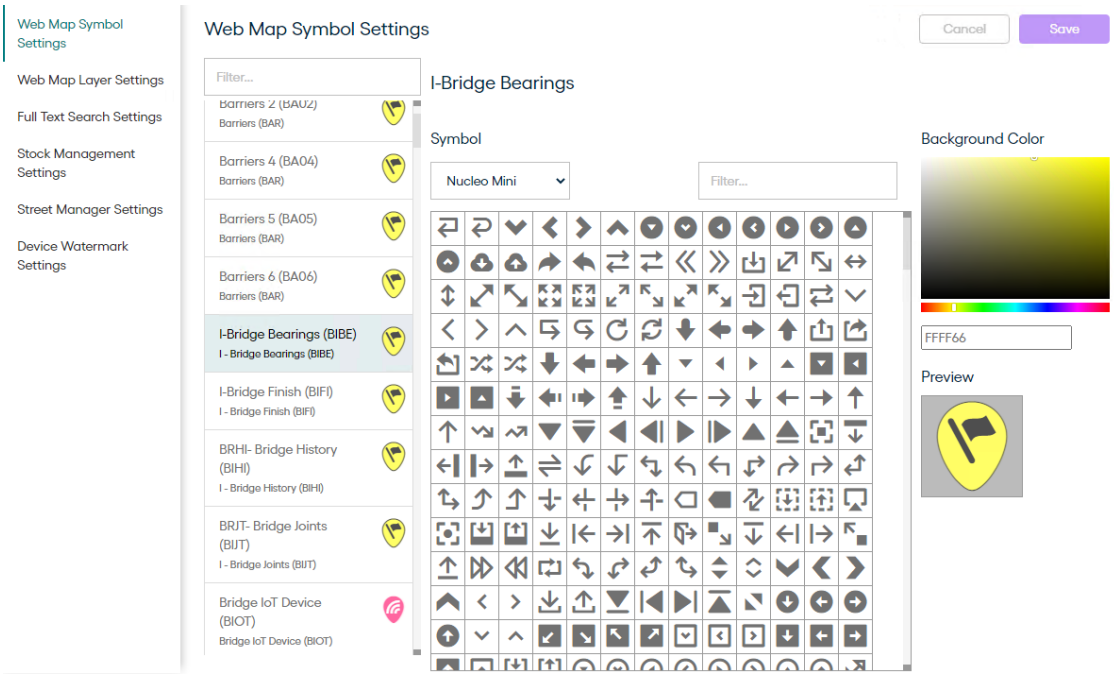
Strategic Asset Management Settings

Export File:	When ticked, the Strategic Asset Management will generate the output generated after Get Data or Refresh Data operation.
Export File Path:	Supply the path which will be used to generate the CSV output after Get Data or Refresh Data operation. File will be generated as ConfirmToSAM_DataSync_[timestamp].csv

Settings

Web Map Symbol Settings

Gives the ability to set custom symbols for Features displayed in the What's Going on Here functionality in ConfirmConnect®. This allows the user to set a symbol and background colour of the icon. The foreground or symbol colour will be automatically set to provide the best contrast for the chosen background colour.



Note: A default symbol has been pre-selected for all Feature Types, should there be a need to reset to this default symbol, filter for location_flag-diagonal-33 in the Nucleo Mini font and the default colour is hex number #ffff66.

Search

Text based filter for the Feature Type list.

Fonts

Select from a list of available font types.

Search Symbols

Text based filter for the grid of symbols available for the selected Font.

For Example: Entering the text 'tree' will limit the symbols to those containing 'tree' in their name.

Note: Hovering the cursor over a symbol will display a tooltip containing its name.

Colour Picker

Select the desired colour. The text field beneath the colour picker allows the entry of a hex number should a specific colour be required.

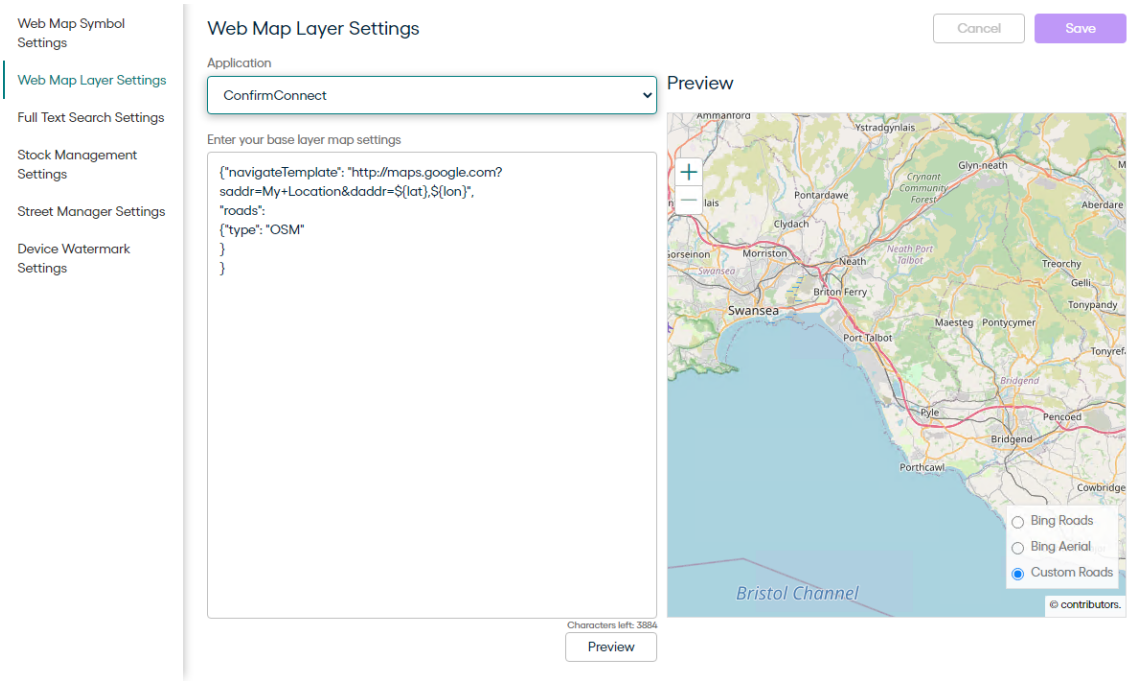
Preview:

Displays the chosen Symbol for the currently selected Feature Type.

Web Map Layer Settings

This page provides the ability to configure background map layers for Confirm Customer Services, ConfirmConnect® and ConfirmWorkzone® which can be used to replace the default Bing maps, along with the preview of the map layer.

The map preview displays Bing layer, if the extents of the custom layer cannot be determined, with an option to switch to custom and aerial views (if available).



Note: The page removes the need to request SQL from Confirm to apply these settings. It will ensure that the entered text is within the database limit of 4000 characters and will use simple parsing to validate JSON text.

This will apply to all users of ConfirmConnect® who do not currently have a settings.js file loaded on their device.

Projections

ConfirmConnect®, ConfirmWorkzone®, and Confirm web are capable to transform all data coming from Confirm into your specified coordinate system, so that it can be displayed properly on the map. The popular visualisation system (EPSG:3785) used by Google and Bing is included as a

standard. But for other coordinate systems, the definition needs to be provided, which is required for all map service types.

The definition for a coordinate system should be provided on Web Map Settings as follows:

"projection":	This is the EPSG code of the coordinate system that you want to use. E.g. "EPSG:27700" is the EPSG code for British National Grid.
"projectionDef":	ConfirmConnect® uses the Proj4 format for coordinate system definitions. You can find the Proj4 definition for your coordinate system here: **http://spatialreference.org/**. For example, **http://spatialreference.org/ref/epsg/27700/proj4/** gives: +proj=tmerc +lat_0=49 +lon_0=-2 +k=0.9996012717 +x_0=400000 +y_0=-100000 +ellps=airy +datum=OSGB36 +units=m +no_defs **Note:** Enter this on a single line in the projectionDef parameter.

Grid Shift

Some countries apply a grid shift in order to provide high accuracy coordinate conversions from default GPS coordinate systems into their own native coordinate systems. For example, in the UK the Ordnance Survey base maps use the OSTN15 grid. See the **Ordnance Survey** website for details.

In order for ConfirmConnect®, ConfirmWorkzone®, and Confirm web to accurately plot entities on map where this type of conversion is required, Confirm needs to be notified of the grid used so the grid shift file can be included. These files have not all been included by default due to their initial size and potential performance implications.

The OSTN02, OSTN15 & A66 National grid shift files have been included with ConfirmConnect®, ConfirmWorkzone® and Confirm Web, if you use OS background maps, you will need to include an additional **projectionDef** value. Append '+nadgrids=ostn15' onto the end of the current line, for example:

+proj=tmerc +lat_0=49 +lon_0=-2 +k=0.9996012717 +x_0=400000 +y_0=-100000 +ellps=airy +datum=OSGB36 +units=m +no_defs +nadgrids=ostn15

Note: For A66, use +nagrids=A66_National

GDA2020

Confirm supports the new GDA2020 coordinate reference system.

A GDA94 projection can be converted to a GDA2020 projection by adding another projectionDef value which is “+towgs84=-0.06155,0.01087,0.04019,-0.0394924,-0.0327221,-0.03289790,0.009994”.

For example:

The projection definition for MGA zone 55 from spatialreference.org is:

"+proj=utm +zone=55 +south +ellps=GRS80 +towgs84=0,0,0,0,0,0,0 +units=m +no_defs"

Which can be converted to GDA2020 as follows:

"+proj=utm +zone=55 +south +ellps=GRS80 +towgs84=-0.06155,0.01087,0.04019,-0.0394924,-0.0327221,-0.03289790,0.009994 +units=m +no_defs"

Note: Note: Enter this in a single line in the projectionDef parameter.

Full Text Search Settings

Confirm web interface supports full text search for Enquiry search and customer address. This enables faster search of Enquiry and customer address in the web interface.

Before enabling the full text search, Confirm Database need to be configured

Configuring SQL Server for enabling full text search

The instructions mentioned **here** must be followed, to enable full text index feature in SQL server.

Note: Ensure the windows service 'SQL Full-text Filter Daemon Launcher' is running and it's startup type is set to Automatic.

Configuring Oracle Server for enabling full text search

The instructions mentioned **here** must be followed, to enable full text index feature in Oracle database.

In Oracle, for every schema user (that needs to use full text search) in the asset_type table, following things are needed:

1. The database user needs to be given the role of CTXAPP (to allow them to create/manage full text preferences/indexes.
2. Execute permissions need to be given for the oracle text packages CTXSYS.CTX_CLS, CTXSYS.CTX_DDL, CTXSYS.CTX_DOC, CTXSYS.CTX_OUTPUT, CTXSYS.CTX_QUERY, CTXSYS.CTX_REPORT, CTXSYS.CTX_THES, CTXSYS.CTX_ULEXER.

Once the database configuration has been done, the following settings need to be enabled in the to enable full text search in the web interface:

1. The 'Address' checkbox needs to be selected to enable full text search for customer address.
2. The 'Enquiry' checkbox needs to be selected to enable full text search for Enquiry.

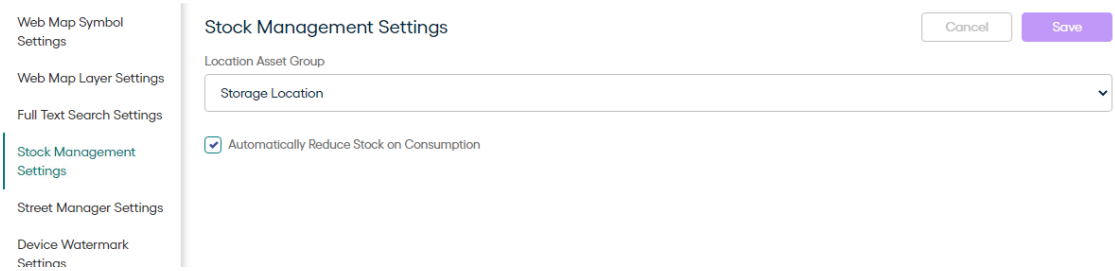
This will add the Full Text Index agent in the Scheduled Tasks. The Full Text index agent creates and maintains the full text index on Enquiries and customer address

After the index has been created, full text search functionality will be used in the web interface for searching Enquiries and customer address.

If the 'Enquiry'/'Address' checkbox is deselected, the full text search is disabled for Enquiry/Address and the corresponding index will be deleted.

Stock Management Settings

This page is used to configure Stock Management.



Location Feature Group

Set which Confirm Feature Group will be used for Stock Management. This allows any Features, of a Feature Type within this group, to be available as locations.

Automatically Reduce Stock on Consumption

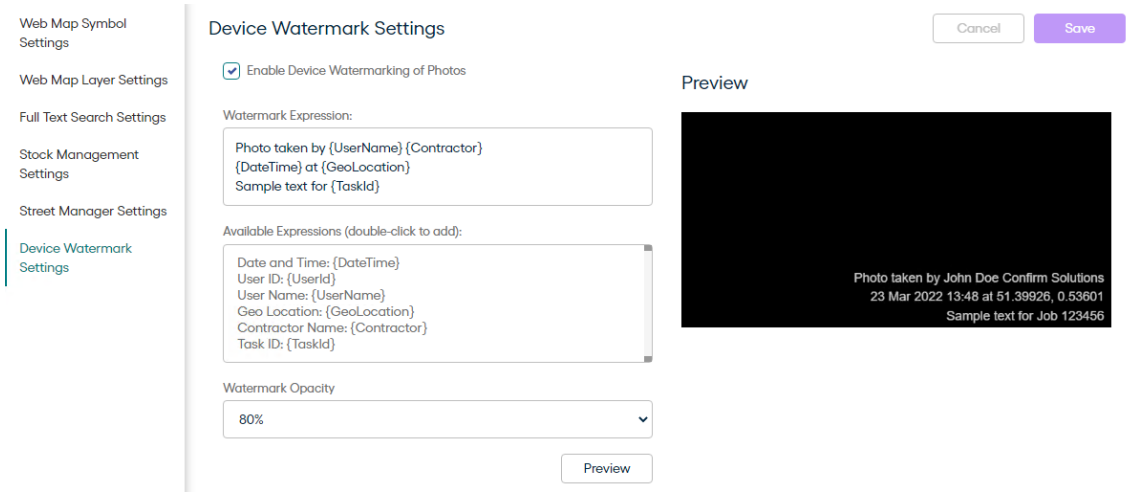
Set whether Inventory levels should be decreased when Jobs are completed in ConfirmConnect.

Street Manager Settings

Street Manager Settings screen is used to configure Confirm to interact with Street Manager. All the fields on the screen have in-line help, refer to the page for further information.

Device Watermark Settings

This page is used to configure how photos are watermarked within ConfirmConnect.



Enable Device Watermarking of Photos

When checked, ConfirmConnect will watermark all photos that are taken on a device using the expression defined on this settings screen.

Watermark Expression

This field is used to configure a watermark using a combination of static text and/or dynamic expressions that will be calculated at the time of taking a photo in ConfirmConnect. The result will be stamped on the photo as a watermark.

Available Expressions

This list contains all the available expressions that can be added to the Watermark Expression above. Each expression can be added to the watermark expression field by a double-click. Altern-

atively the expression code can be typed into the watermark expression field manually. Each expression will be evaluated at the time a photo is taken in ConfirmConnect.

Note: Geolocation data can be added to the watermark using the {GeoLocation} expression. This data will be displayed in Latitude/Longitude using Decimal coordinates.

Watermark Opacity

Set the Opacity of the text shown on the image.

Note: Text has a subtle dark border to allow it to be visible on lighter images.

Preview

Click the "Preview" button to show an example of how the watermark might look based on the current values in the Watermark Expression field.

Local Settings

The Local Settings program allows local machine configuration settings to be edited.

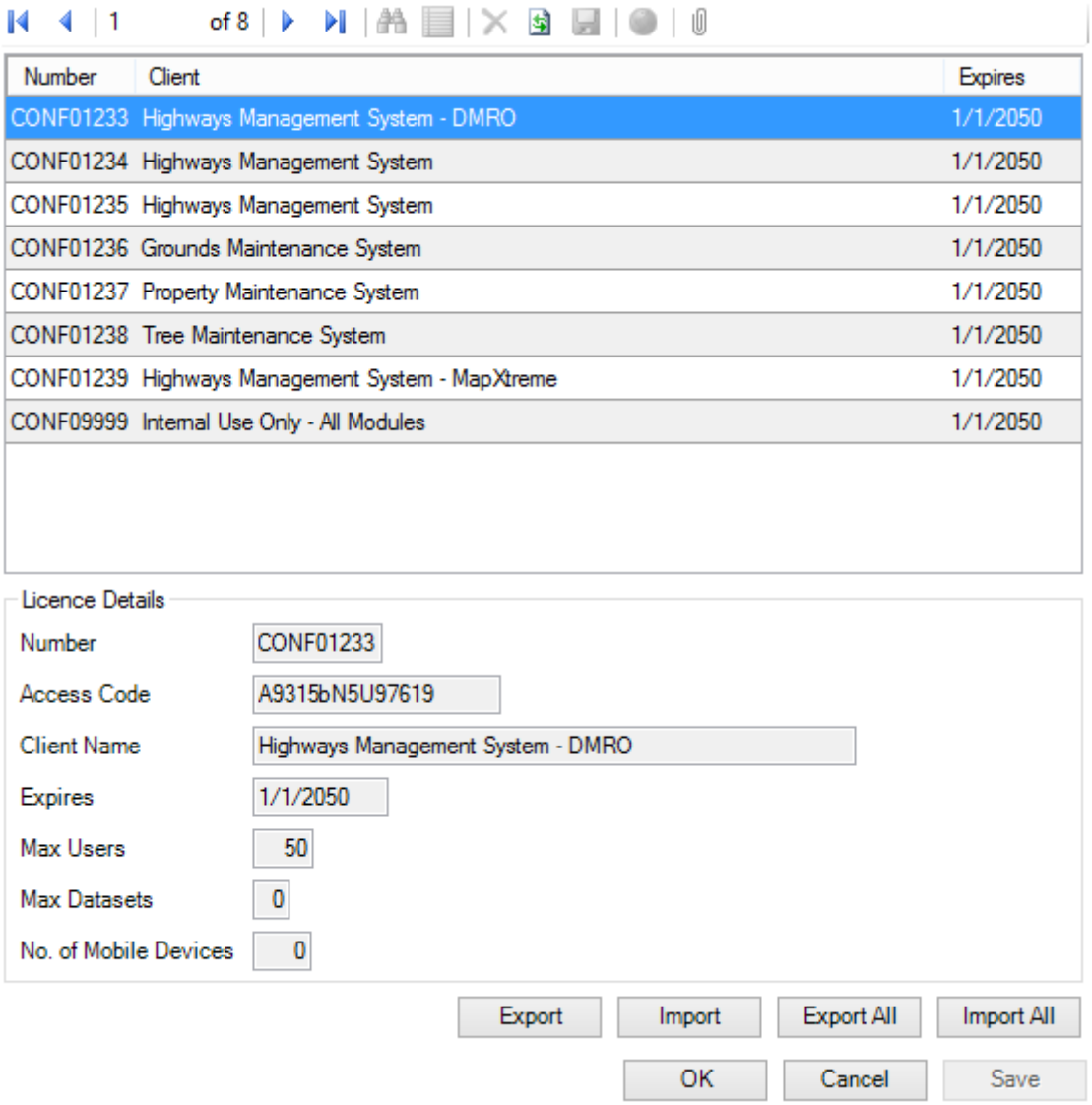
It updates the Registry and security access to it should be restricted.

This will have been set up by Confirm, and should not be changed other than on Confirm advice.

Relicense

The relicensing utility enables the user to export licence details from one database into an XML file and then this XML can be used to import the licences into another database.The utility can be used to assign test licences to a copy of a live database so that the live database can then be used as test database.

It also enables the user to view the licence details on the screen.



Export: When clicked, will export the licence details of the selected licence from the screen into an XML file.

Import: When clicked, will import the details of the licence(s) from the XML file supplied into the Database. This will overwrite the details any existing matching licences.

Export All: When clicked, will export the details of all the licences currently residing in the database to a single XML file. This can be used to backup all the licences and then later be imported into a fresh database.

Import All: When clicked, will ask for an XML to be imported. The user must be sure before using this function as it will delete all existing licences that are not included in the XML file. Once the import is complete then the user must exit the application and login again.

ConfirmConnect® Profile

The ConfirmConnect® Profile screen allows the administrator to create new profiles for ConfirmConnect® Users. Purchased modules can be assigned to a profile which in turn can be assigned to a user or a users group for easy deployment.

Setting the Custom Maps Folder will override the 'Default Custom Maps Folder' Setting on the **ConfirmConnect Settings** screen and will be the location that the custom map file(s) are downloaded from, for each User that has this Profile.

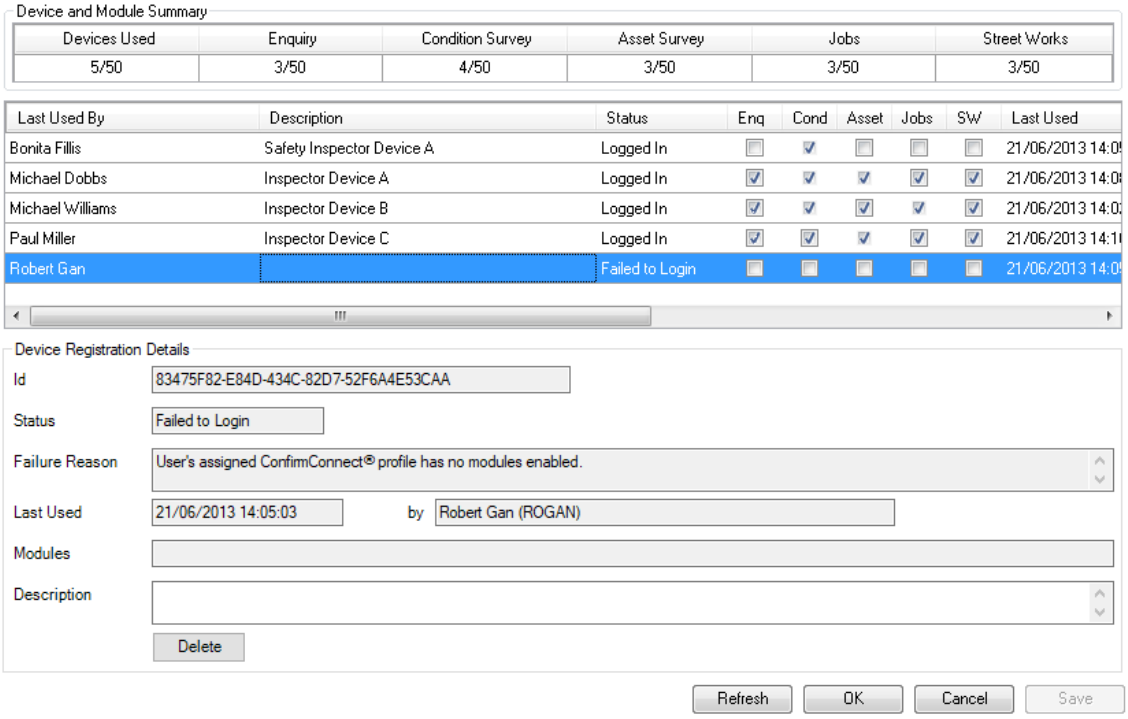
ConfirmConnect® Registration

When a ConfirmConnect® device signs in successfully for the first time it is registered within Confirm.

When a user attempts to sign in, their ConfirmConnect® profile is checked and the required modules are requested. If the required modules are available they are assigned accordingly, if not the sign in process is cancelled and an error message is returned.

The ConfirmConnect® Registration utility enables an administrator to view all registered devices and additional information such as device status and module usage so that sign in issues can be resolved efficiently.

All the information displayed is read only with the exception of device descriptions and the ability to delete a device which is explained later.



Device and Module Summary

This section provides a summary information which includes:

Devices Used:	Lists how many devices have been registered followed by how many in total can be registered at any one time. Suspended devices are not counted as registered devices.
Enquiry/Condition Survey/Asset Survey/Jobs and Street Works	The subsequent columns list how many module licenses have been used followed by the total number of concurrent licenses for each module type.

Device Registration Details

Each device is represented by a row in the main table. The table can be ordered by any of the columns by clicking on the column header.

To display full details for a device in the Device Registration Details panel click its row in the main table.

Clicking on the refresh button refreshes both the summary information and the main table of devices.

ID:	Unique installation ID for the device created when ConfirmConnect® is installed. The ID can be found for each device by clicking on the 'About' screen within ConfirmConnect®.
Status:	The current status for the selected device.
Failure Reason	The current sign in failure reason if one occurred is displayed here. A failure reason is cleared once the user has signed in successfully.
Last Used / By:	Date and time that the device last interacted with the ConfirmConnect® service and the user name that was used.
Modules:	When a device signs in a list of module types that have been assigned are displayed here.
Description:	A free format description to assist device identification. This information can be edited for each device.

Delete

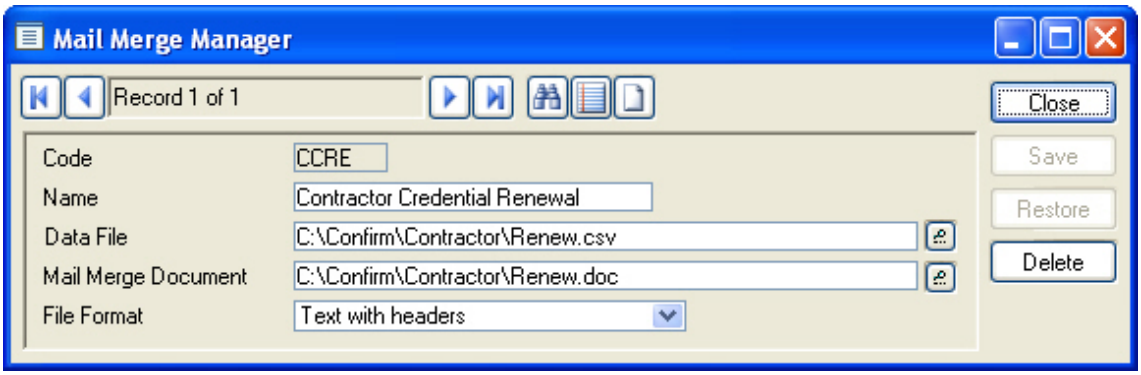
When a device is no longer required, it can be deleted from device registration screen and a device licence will be released. Should a device be deleted by mistake, whilst it is still signed in, the user will receive a forced sign out event when they next attempt a transfer.

Note: A forced sign out event will remove any draft and completed work, which has not been transferred, from the device.

In the event that there are no remaining device licences available when logging in to ConfirmConnect® with a new device, an attempt will be made to free up an unused licence. This is defined as the device holding the oldest licence that has been logged out for more than 2 days.

Mail Merge Manager

The Mail Merge Manager stores details of the mail merges that have been created in Confirm.



Mail Merges may be viewed and amended from this Mail Merge manager, but not created

Mail Merges are set up from the area to which they relate, so that a Credential Renewal Mail Merge is created from the 'Mail' button on the Credential Type Lookup form.

Mail Merges may also be set up from most forms, lists and reports.

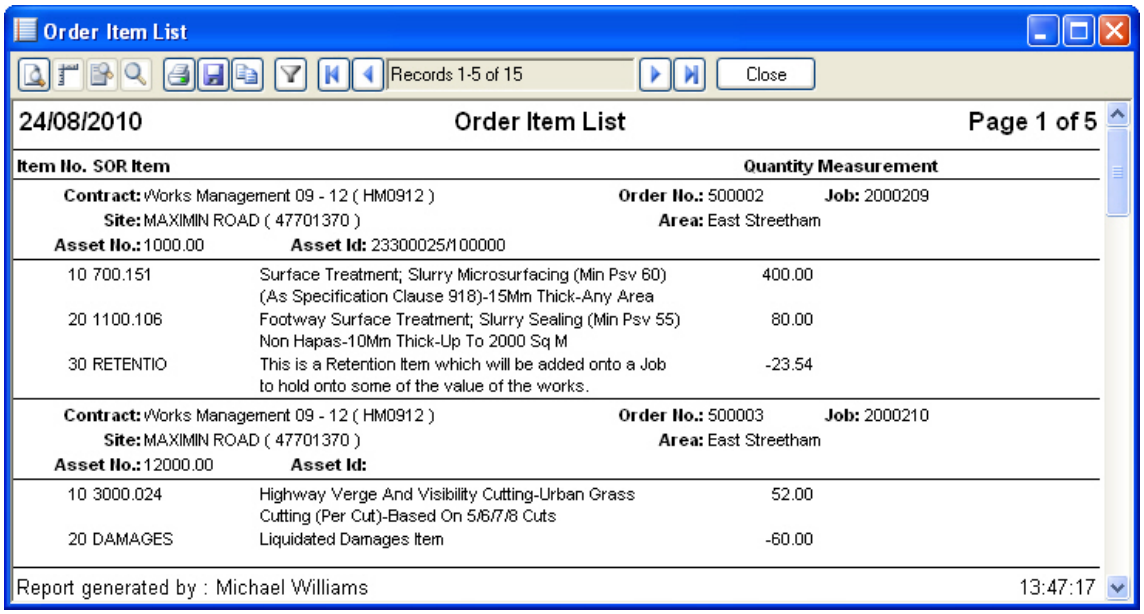
Contract Preparation\Contractor Standing Lists\Standing list Lookups

Creating a Mail Merge

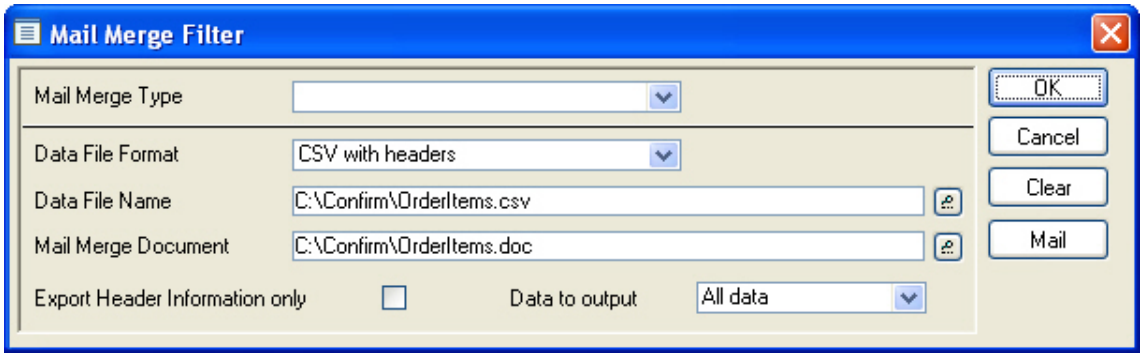
Set up a Mail Merge

These instructions are based on Word 2007/2010 as the word processor.

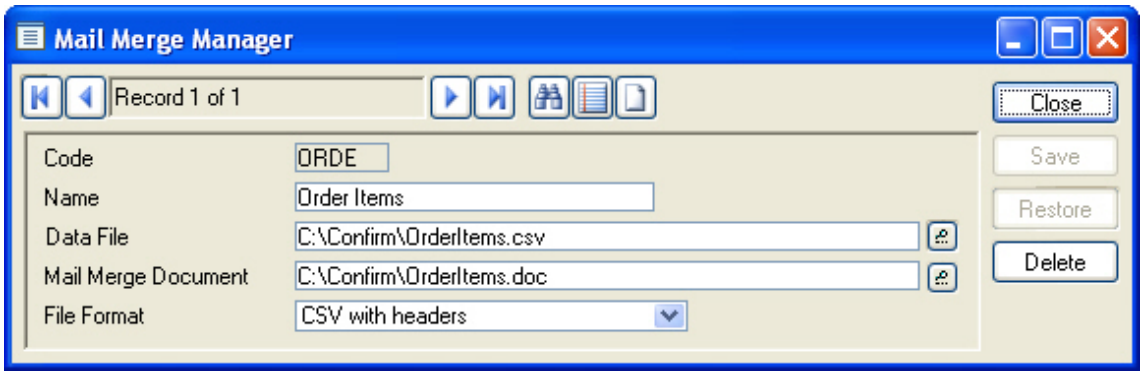
1. Open Word and save a blank document with an appropriate name and in the correct location. This document will form that basis of the merge document.
2. Close Word.
3. In Confirm, select records by recalling them into a form, or creating a list or report. In this example an Order Item List has been created from the List button in the Order Details screen:



4. Select 'Mail Merge' from the File menu. The Mail Merge Filter is displayed:



5. Where no mail merge has been created for this entity before, the Mail Merge Type field will not be available. To create a Mail Merge Type, click on the 'Mail' button to display the Mail Merge Manager:



6. Use the Mail Merge Manager to set up a mail merge format for the selected entity:

   Code: Up to 4 alphanumeric characters

   Name: Up to 30 characters

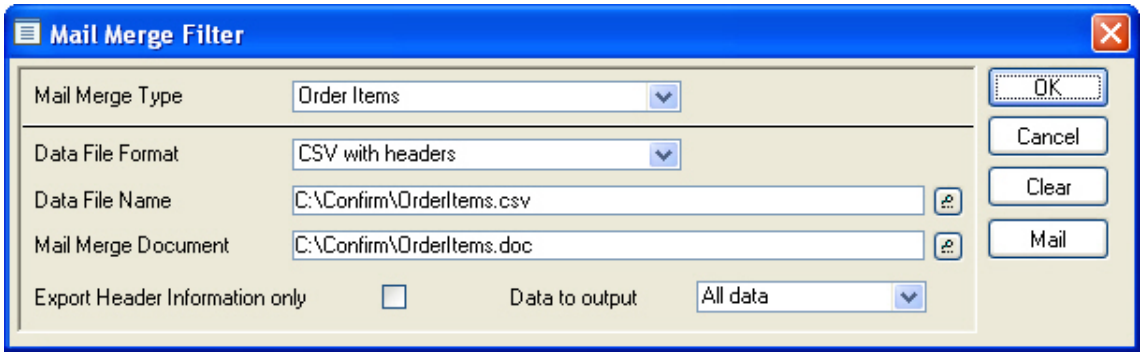
   Data File: Enter the full path and name of the data file. The path may be selected using the pick button. The file is created when a merge is carried out, in the location, and with the name, entered here.

   Note: The data file will hold the headers, and the field data, from the selected records, and will be used to provide merge fields, and populate them, in the word processor.

   Mail Merge document: Enter the full path and name of the mail merge document. This is the file created in Word at step 1 above. This file must already be present and may be picked from the folder where it was stored using the pick button at the end of the field.

   File Format: Select the file format for the Data File entered in the Data File field. In this example a text file is being used, and this provides the simplest transfer format for data.

7. Save and close the Mail Merge Manager. The Mail Merge Filter is re-displayed:



8. The Mail Merge Type drop down list will now be available, and will display all Mail Merge Types appropriate to the currently selected data. In this example, the Order Item list is still displayed; therefore the drop down list will offer the Order Item Mail Merge Type.
9. Select the required Mail Merge type. The remaining fields in the Mail Merge filter are populated from the Mail Merge Type record. These may be edited.

   Export Header Information only: Select this to export only field headers. This may be appropriate at the set-up stage if the data is not to be output.

Data to output: 'Current Record only' - Where data is displayed in a form, the export for mail merge may be limited to only the currently displayed record.

'All data' - To merge all the currently selected records.

10. Click OK.
11. The word processor will be launched and the mail merge document will be opened in the word processor.
12. To set-up mail merge document in Word use the 'Mailings' menu option in the toolbar. Use the 'Select Recipients' option and select the data file created by Confirm.
13. Once the data has been selected, use the merge fields from the 'Insert Merge Field' drop down to insert into the document. The finished document may be viewed with the text of the selected records inserted, by clicking on the 'Preview Results' button in the toolbar. Select 'Finish & Merge' button to print the document.
14. Close Word.

The mail merge is now configured and can be used at any time by a User to generate the documents with data from Confirm. These steps must be followed for each new Mail Merge Type that is set up.

Running a Mail Merge

Once Mail Merge Types have been created and saved, all the relevant files, paths and directories are set and the merge will be carried out automatically when records are recalled and that Mail Merge Type selected in the Mail Merge Manager.

To merge records in an existing Mail Merge Type:

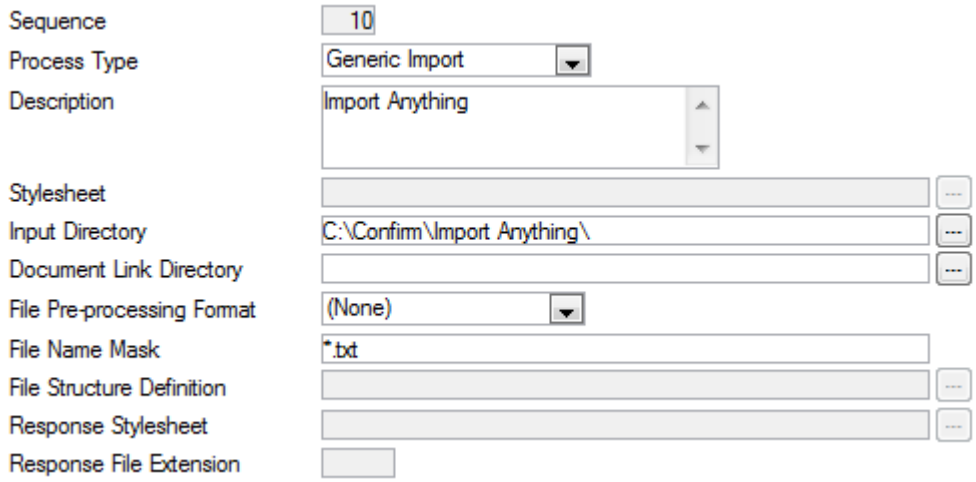
1. Select the required records by recalling them into the form, list or report.
2. Select Mail Merge from the File menu, or press Ctl+M on the keyboard.
3. In the Mail Merge Manager select the Mail Merge Type required in the Mail Merge Type field.

   Note: If this field is not available it is because no Mail Merge Type exists for the entity type currently selected.

4. Click OK. The word processor is launched and the selected records are merged to the word processor document specified in the Mail Merge Manager.

Import Transformations

Import Transformations define the parameters for locating data import files and for converting them into a format suitable for import into Confirm.



Sequence: A unique numerical identifier will be suggested by the system but can be changed if desired.

Contractor: (Contractor Access Agent module)

This will only be visible if opened from the Contractor 'Import' button and will display the currently displayed Contractor.

Process Type: Select from:

'Contractor XML Import' - For importing Contractor data with the Contractor Access XML Agent e.g. Payment Requests and Job Status updates. This will only be displayed if opened from the Contractor 'Import' button.

'Financial XML Agent' - For importing Order commit authorisation data from an external Financial system with the Financial XML Agent.

'Generic Import' - For importing Defects, Jobs, Features, Inventory, Performance Monitoring inspection results and Asset Valuation Logs with the Import Anything Agent or the equivalent Import Data option on the menu.

'EToN Import' - For importing non-standard Street Works EToN data with the EToN Hub module.

'Connector Agent' - For importing data with the Confirm Connector invoked by the Task Processor. The Task Processor will then pole the supplied directory for files to pass to the Connector.

'Import Address' - For importing or updating address records in Confirm system.

Description: A free text field for a description of the transformation.

Stylesheet: This field is only enabled when ‘File Pre-processing Format’ is not set to (None) or ‘Process Type’ is set to ‘EToN Import’. Enter or find the location of the Stylesheet (.XSL) that will be used to convert the import file into the required Confirm format. This is not required if import files are in Confirm format.

Please see the **Import Preprocessing** section below for further details.

Input Directory: Enter the location of the directory where the import file(s) can be found.

Document Link Directory: If a directory is specified here the import file will be copied to this location and a document link created to it. The file can then be accessed directly from the relevant Confirm screen. This is applicable to Inspection Batches, Defects and Jobs imported with the Import Anything Agent.

File Pre-processing Format: Select the field delimiter being used in the import file. The system will use this to convert the import file to XML format and then apply a Stylesheet to convert it to Confirm format.

Note: Set this to '(None)' if import files are in Confirm format, and to 'XML' if import files are XML files to be converted to Confirm format using a Stylesheet.

Note: Tab and comma delimited files are assumed to have an end of record denoted by the Carriage Return and Line Feed characters. Pipe delimited files are assumed to have an end of record denoted by tilde (~).

File Name Mask: You may restrict the selection of files from the Input Directory by specifying the name, or part name of the files to be used. Wildcards may be used. The File Name Mask defaults to *.* meaning all files in the Input Directory will be processed.

File Structure Definition: (EToN Hub module)

EToN Import transformations have to convert EToN text files into XML so that they can be transformed by the EToN Agent. An XML structure definition file tells the EToN Agent the structure of the file it is transforming.

Response Sylesheet: Only available with the 'Connector Agent' Process Type. The response given by the Connector can then be passed through the supplied Stylesheet.

Response File Extension: Only available with the 'Connector Agent' Process Type. Provide the file extension for the response files so that they can be processed by the stylesheet suppled above.

Test: When a Stylesheet is being used to transform data into Confirm format, this button can be used to test that the settings specified are correct and the Stylesheet is correctly constructed. The Test button will examine each file in the Input Directory matching the File Name Mask, and generate test file(s) as follows.

If File Pre-processing Format is set to 'XML' then the Stylesheet will be applied directly to the XML import file and the result created as a .TMP file.

If any other File Pre-processing Format is being used, an .XML file will be generated by applying the Pre-processing Format to the import file. The Stylesheet will then be applied to this and the result created as a .TMP file.

In either case, the .TMP file contains the data that would be imported into Confirm so its content can be checked against the Import Specification for the relevant Agent.

Note: The Test button will not proceed with processing if more than 10 files are found. This is a safety measure in case the wrong Input Directory is chosen.

Note: If the File Name Mask is one that includes .XML and .TMP files (such as *.* which includes both of these), clicking the Test button a second time will attempt to process any .XML and .TMP files present. The Task Processor will also attempt to process these files if they are left in the import folder.

Note: A history of changes made to Import Transformation records will automatically be recorded. Click on the History button to see the full Entity History Report for the current record.

Import Preprocessing

The import file is processed, depending on its format, as follows:

Text files requiring transformation

These are transformed into XML. An example is used to explain how a delimited text file is converted into XML and the XML notation used for this process.

The following is an example of a supplied Pipe Delimited text file, to be converted into XML, with two rows:

Order1|Job5|50|1.5|75.00

Order2|Job8|100|3|300.00

This file is converted into the following XML:

```
<table>
  <tr>
    <td>Order1</td>
    <td>Job5</td>
    <td>50</td>
    <td>1.5</td>
    <td>75.00</td>
  </tr>
  <tr>
    <td>Order2</td>
    <td>Job8</td>
    <td>100</td>
    <td>3</td>
    <td>300.00</td>
  </tr>
</table>
```

XML

XML files, either produced by the above process or supplied, are transformed into SBSCSV format by the stylesheet held on the XSL Transform record.

Text files in SBSCSV format

These files, either produced by the above process or supplied, are processed by the import utility against which the preprocessor is running.

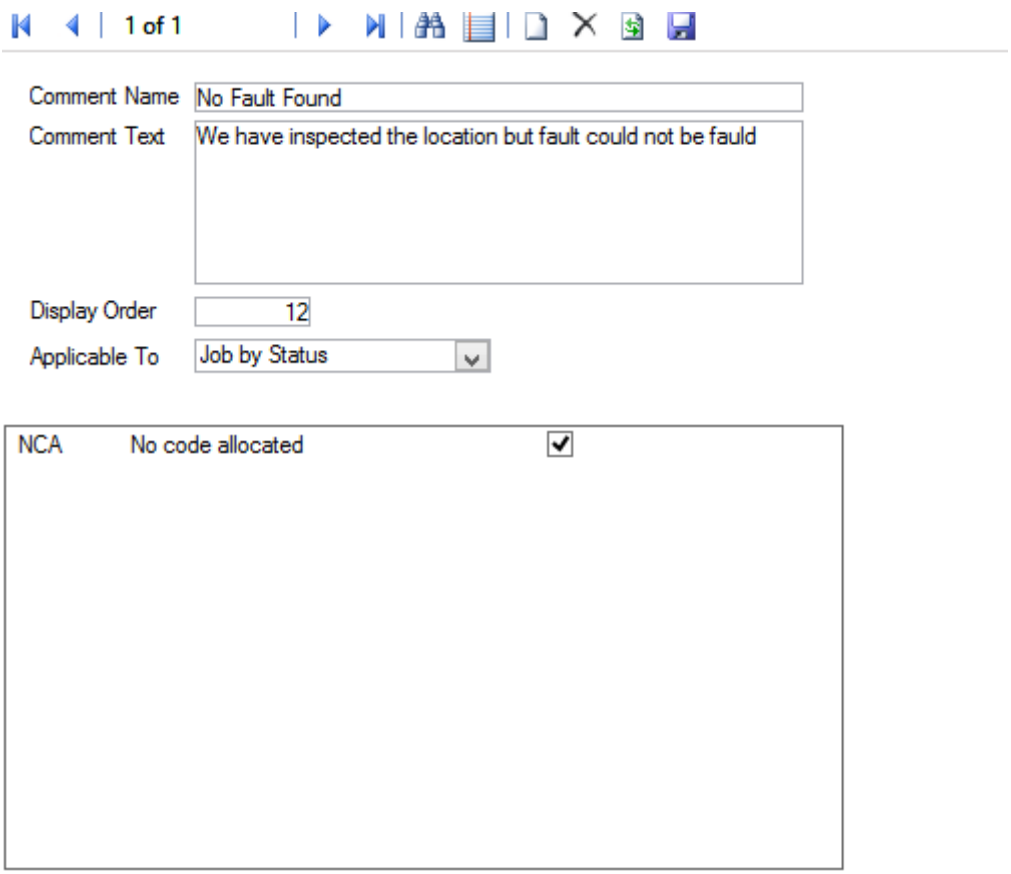
Finance Year

The Finance Year library stores Finance Years with start and end dates for use throughout Confirm.

Please refer to the Finance and Budgets manual for details.

Comment Library

The Comment Library allows a list of standard Comments to be created and maintained. A standard Comment can be pasted into Comments, Descriptions, or Notes fields throughout the system.



Comment Name: An optional field to help identify a Comment.

Comment Text: A free text Notes field.

Display Order: Order in which a Comment will appear in the lookup list. By default this value is set to 999999 but can be changed to a lower value to make the Comment appear higher in the list.

Applicable To: Restricts the applicability of a standard Comment.

All - Comment can be applied to any field.

Job - Comment will be available only on Job related screens.

Enquiry - Comment will be available only on Enquiry related screens.

Enquiry by Status - Comment will be available only if an Enquiry's Status is one of those ticked.

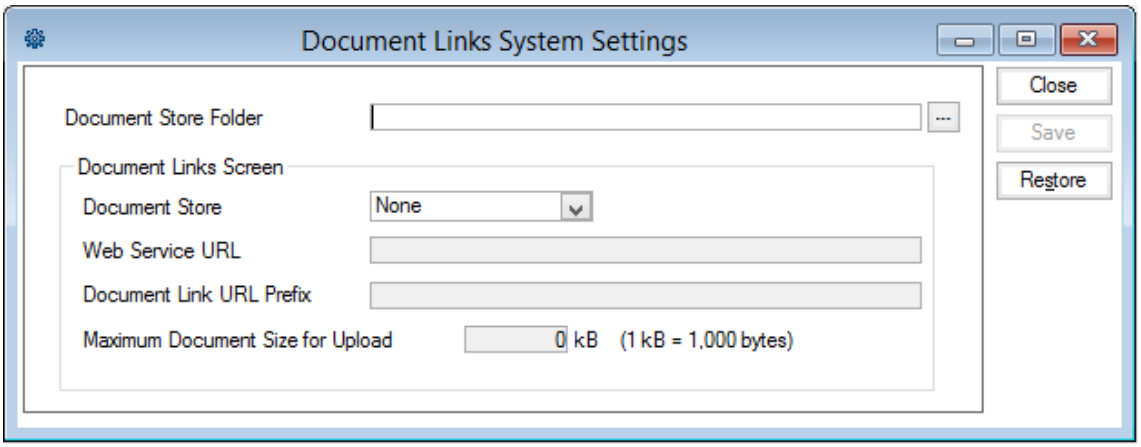
Job by Status - Comment will be available only if a Job's Status is one of those ticked.

Street Works - Comment will be available only on Street Works related screens.

Defect - Comment will be available only on Defect related screens.

Although the Comment Library Lookup filters the list based on Applicability, the entire list of Comments can be viewed by clicking the 'Show All' button.

Document Links System Settings



Document Store Folder

This setting is used to specify the directory path to the Folder that will be used as a central document store. This will be the location that all photos uploaded from mobile devices will be transferred to, and will also be the location that other linked documents can be uploaded to from the Document Links screen, if a Document Store setting of Folder is chosen. It can be in the form of a file path (e.g. C:\Documents\) or a UNC path (e.g. \\ServerName\Documents\).

When uploading photos from a mobile device via the Confirm Connector the Document Store Folder will refer to a path on the machine hosting the Confirm Connector, so a setting of C:\FBIImages would be a directory in the root of the Confirm Connector machines hard drive.

Uploaded Photographs will be attached to entities as document links and any uploaded documents or photos will have the Document Location prefixed with either $Document$, for photos uploaded during a transfer, or $Document Store$ for documents uploaded manually to a 'Folder' document store. When launching documents the prefix values will automatically be replaced with the Document Store Folder value.

Note: If this setting is left blank then any transfers from handheld devices with photos will fail.

Note: If this setting is ever modified then the Confirm Connector must be re-started for it to use the new path.

Document Store

This is used to specify where files should be transferred to when choosing to upload a file to a document store in the Document Links screen. The options are:

- None
- Folder
- Web (PUT)
- Web (POST)

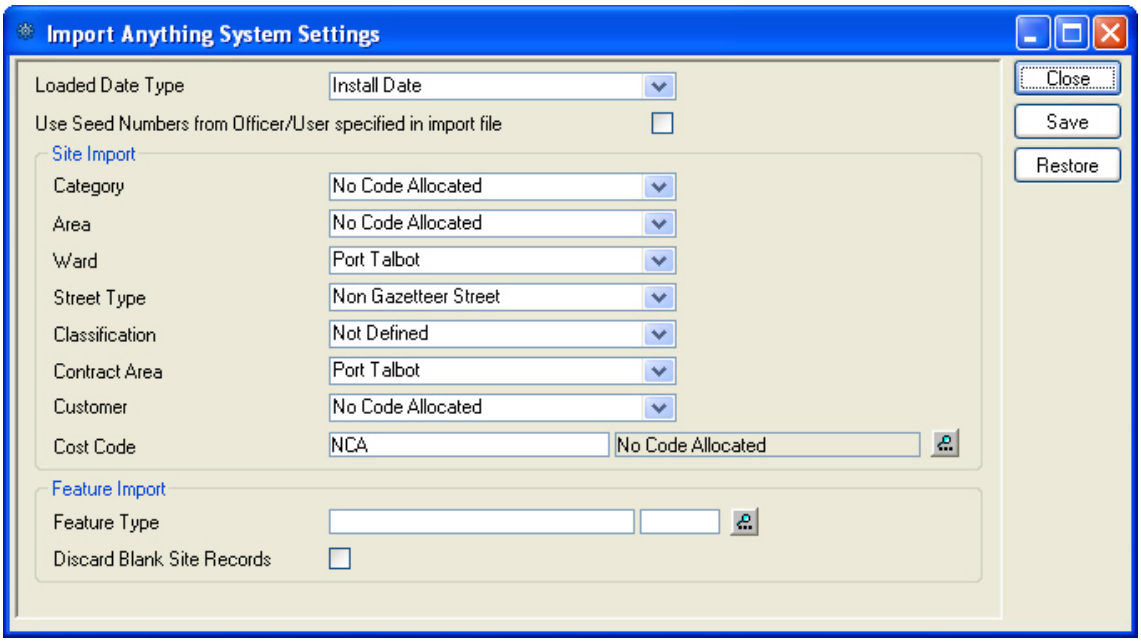
'Folder' will upload document files to a Document Store Folder, or rather to a Year/Month subfolder structure within it. The subfolder structure is determined from the Document Date at the time of upload. A subfolder is created for each year, and within that a subfolder for each month.

'Web (PUT)' and 'Web (POST)' will only be available if you have module 8010. The PUT and POST options provide two common protocols for transmitting files across the internet. The configuration of the remote web service would dictate which of these is used.

Web Service URL	This is to specify the location of a web service capable of receiving documents sent from Confirm. Documents will be sent to this web service when the Document Store setting is set to Web (PUT) or "Web (POST)", however, images uploaded from mobile devices will continue to be transferred to the Document Store Folder location.
Document Link URL Prefix	When a file is uploaded to a web service, the final storage location that can be used to view the file is returned to Confirm and this then becomes the new Document Location value shown on the Document Link. The Document Link URL Prefix setting specifies a path that is matched against the Document Location value returned from the web service. A match is substituted with the string '$Document URL$'. This prefix substitution feature allows easy identification of files stored in the central document store and shortens lengthy location details shown with the document link. For example, If this URL Prefix field had the value "http://www.confirm.com/Documents and a document is uploaded to a web service which returns a Document Location of http://www.confirm.com/Documents/inspections/photo.jpg then the Document Location value for that Document Link would appear as $Document URL$/inspections/photo.jpg. If no URL prefix is specified then the Document Location will appear as the full URL to the file.
Maximum Document Size for Upload	This setting is used to limit the size of files that are uploaded to a central document store. The size limit is given in 1000s of bytes, with 0 meaning no limit. Here 1kB is set to be equal to 1000 bytes. This may differ to file sizes reported elsewhere in the system, where 1024 bytes is often used to signify 1kB. Files over the specified size will not be uploaded and a message will be displayed to inform the user. This Document Upload size limit does not check any other restrictions that may be in place such as disk quotas or web service upload limits that could also cause the upload to fail; so these should be considered when setting the maximum document size.

Import Anything System Settings

The Import Anything System Settings allow you to specify a date type to be applied to the date when the file is loaded into Confirm.



Loaded Date Type:

Specify a Date Type to act as the Loaded Date. This Attribute will be set to the current date for all Features created via this import, including new versions of existing Features. The Loaded Date does not get set for existing Features that are being updated. If a value for this Date Type is supplied as a Feature Attribute in the file, it will be ignored.

The drop down list references the Date Types lookup.

Asset Register\Feature Lookups

Use Seed Numbers from... :

Check this flag to enable imported Jobs, Defects and Inspection batches to be given Seed Numbers from the Work Group of the Action Officer or User supplied, rather than the Task Processor User Work Group.

The following entities will be given the following range of Seed Numbers:

- Jobs - Work Group of the login name supplied with the Job.
- Defects - Work Group of the officer code supplied with the Defect.
- Inspection Batches - Work Group of the officer code supplied with the Inspection Feature.

If the Work Group applicable for Jobs, Defects or Inspection batches does not have a valid range of Seed Numbers then the Task Processor User's Work Group is used instead.

Street Import

Confirm will use the lookup values specified in this section if not supplied in the Site import file.

Feature Import

Feature Type:

Select a Feature Type from the drop down list, which Confirm will use if the import file does not contain a valid Feature Type. The drop down list references the Feature Types lookup.

Asset Register\Feature Lookups

Discard Blank Site Records:	Check this to discard Feature records with a blank Site Code. This prevents these records from being imported without raising an error and thus the import file being rejected.

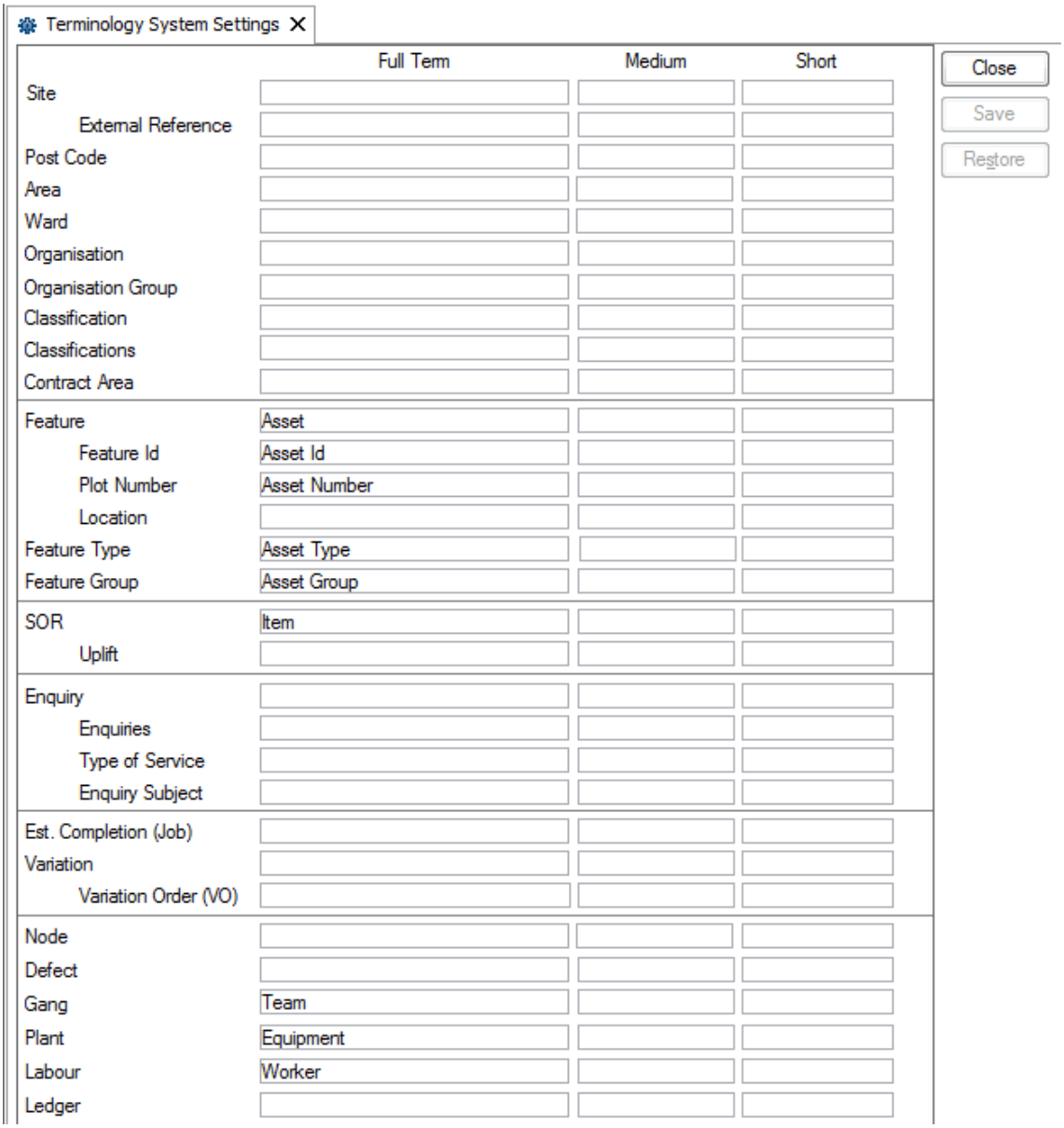
Terminology System Settings

The default terminology used on Confirm screens varies depending on User and system configuration. See **Terminology in Confirm Products** for more information.

For example 'Feature' is called 'Asset' when running Confirm Street Lighting terminology, and 'Tree' when running Confirm Arboriculture.

The Terminology System Settings screen allows these terms to be overridden. The settings do not vary according to the Confirm executable unlike the default settings.

If terms are not overridden, all Confirm executables use the default terminology.



Each default name has three columns into which the user-defined name can be entered.

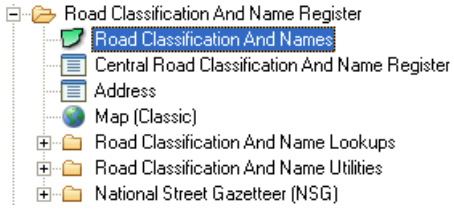
• The first column is used for the full user-defined terminology.

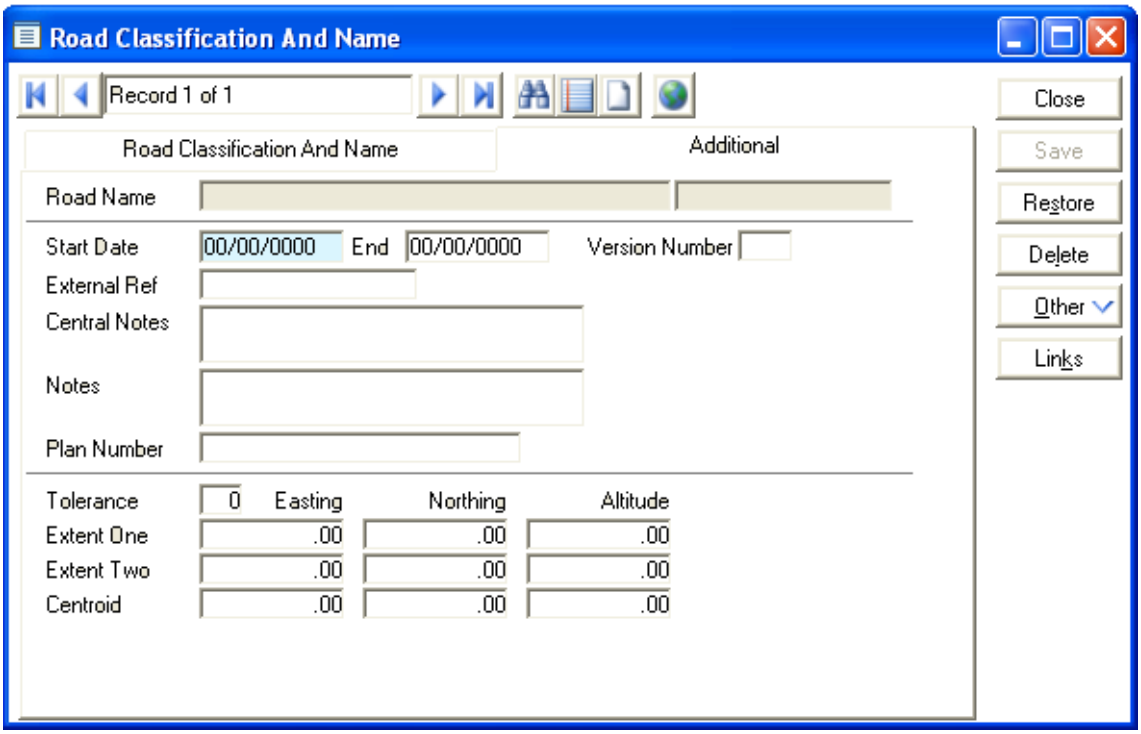
• The second column may be used for a shorter name which the system will use if it cannot fit the name in the first column into the available space.

• The third column may be used to define a fully shortened name which the system will use if it cannot fit the name in the first column, or the name in the second column, into the available space.

For example:

The changes illustrated above will result in the Site folder appearing in the Confirm Explorer as illustrated below:





Fields in the forms and filters associated with the Site (Road Classification And Names) will also be re-named in accordance with the terminology settings.

Entity History

Entity History is used to track changes made to the particular Entities where it has been enabled in Entity History Settings. It can be used to Report on the changes made, who made them, and when.

Each area of Confirm that records Entity History will have Settings particular to that Entity.

Entity History Report

Key Codes

Entity History can be recorded for the following:

Entity	Key	Module Required
Feature	Site Code / Plot Number	0115 – Audit Trails
Feature Attributes	Site Code / Plot Number / Type Code	0115 – Audit Trails
Feature Measurements		
Feature Dates		
Feature Smart Attributes		
Inventory	Site Code / Plot Number / Inv Item Id	0115 – Audit Trails
Inventory Attributes	Site Code / Plot Number / Inv Item Id / Type Code	0115 – Audit Trails
SOR Item	SOR Item Code	None
Defect	Defect Number	0500 – Condition Survey
Enquiry Customer Details	Customer Number	1200 – Customer Services
Enquiry Contact Details	Enquiry Number	1200 – Customer Services
Job	Job Number	0700 – Asset Maintenance
Job Attribute Type	Job Number / Type Code	0715 – Job Attributes
Job Status	Status Code	0700 – Asset Maintenance
Tender Bids	Tender Number / Contractor Code	0945 – Non-Term Bidding
Standing List Prerequisite	Work Band Key / Credential Code	1810 – Contractor Standing Lists
Listed Contractor	Work Band Key / Contractor Code	1810 – Contractor Standing Lists
Contractor Credentials	Contractor Code / Credential Code	1810 – Contractor Standing Lists
Consequence Type	Consequence Type Code	2300 – Risk Management
Consequence Severity	Consequence Type / Severity	2300 – Risk Management
Consequence of Failure (Matrix)	Feature Group / Risk Type / Risk Class / Failure Mode / Consequence Type / Severity	2300 – Risk Management

Entity	Key	Module Required
Feature Activity	Site Code / Plot Number / Activity Number	2300 – Risk Management
Statement Item	Organise Code / Statement Number / Statement Item Number	3400 - Street Works Register
User Security	Login Name	None
User Security - Program Rights	Login Name / Program Code	None
Note: The 'All' button on the User Security screen, and the 'Users' button on the Group Security screen, delete Program Rights and insert new ones.	For example, Key Like USER1/* returns all changes to the access for User USER1, and Key Like */JOB returns all changes to accesss to the Job screen.	
Note: Only manual changes to the 'User Locked Out' flag will be shown in the Entity History. For example, if a User is locked out by exceeding the password retry limit, this will not be shown.		
Group Security	Group Code	None
Group Security - Program Rights	Group Code / Program Code	None
Note: The 'All' button on the Group Security screen deletes Program Rights and inserts new ones.	For example, Key Like GRP1/* returns all changes to the access for Group GRP1, and Key Like */JOB returns all changes to accesss to the Job screen.	
Data Security Key	Data Key	None
Data Security Group	Data Group Key	None
Data Security Group - Access	Data Group Key / Data Key	None
	For example, Key Like 1/* returns all changes to the access for Group 1, and Key Like */1 returns all changes to accesss to Data Key 1.	
ConfirmConnect Profile	Profile Code	None
Import Transformation (includes Contractor Import and Export Transformation)	Transformation Key	None

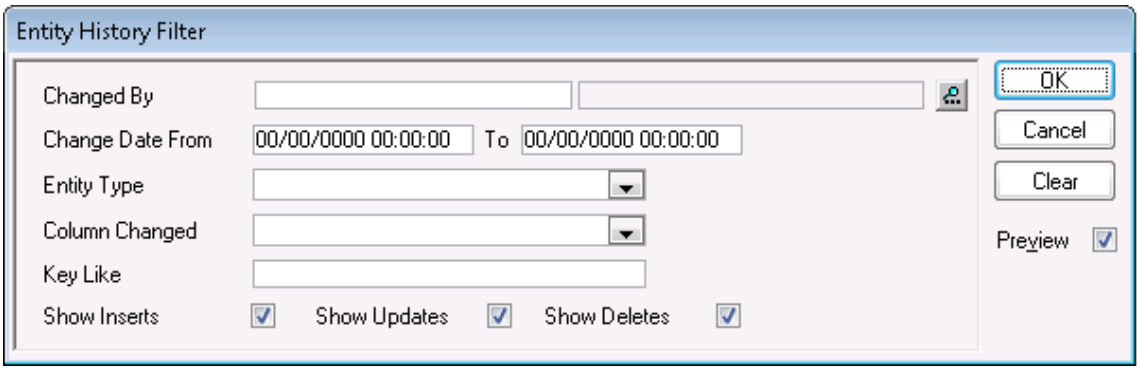
Note: Plot Number is stored without trailing zeroes. For example Entity History for a Feature with a Plot Number of 100.00 is stored with a Key value in the form 47701370/100 rather than 47701370/100.00.

Note: Entity History will only record the first 500 characters of text fields, such as Feature Location, Feature Description, Defect Notes, Attribute Notes etc.

Click on the OK button to retrieve the results.

The Entity History Report will open and display the results that met the filter criteria. Displaying all Historical Log entries associated with Entity Date along with any changes made.

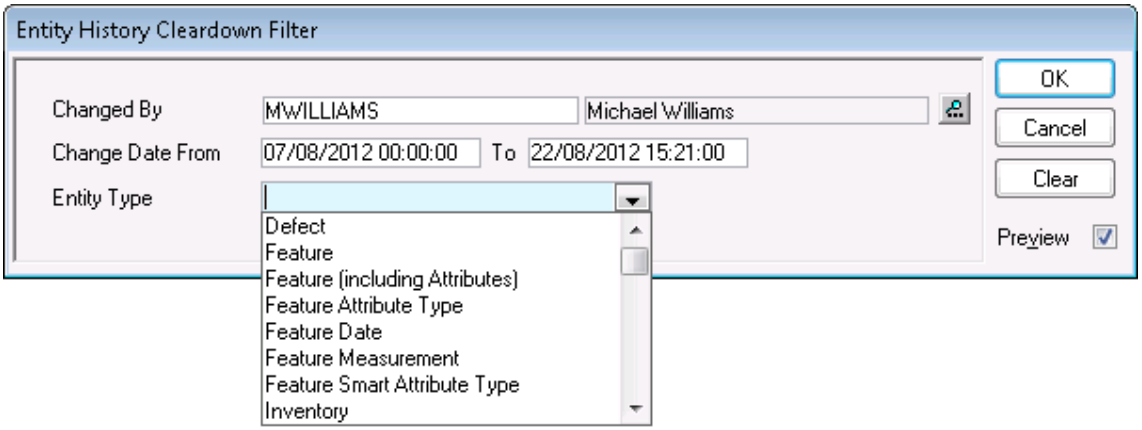
Note: For Enquiry, only 'Updates' to an existing Enquiry are recorded in Entity History.



Changed By:	Select a User from the User library. **System Administration\Security\User Security**
Change Date From \ To:	Select the date range to report on.
Entity Type:	Enter the section of data to report on. The drop down list shows the data sections as defined in the Entity History System Settings.
Column Changed:	A list of fields will be displayed which will reflect the selection made in the Entity Type field. Select from the list.
Key Like:	A free Text field in which key codes may be entered. Each code is separated by a slash. See the 'Key Codes' section for example codes.
Show Inserts:	Check this to include newly created records in the report.
Show Updates:	Check this to include changes to existing records.
Show Deletes:	Check this to include records that have been deleted from the database.

Entity History Cleardown

The Entity History Cleardown will delete Entity History records based on the parameters set in the filter.



Changed By	Restricts the Cleardown utility to clear changes made by the selected User only.
Change Date From \ To	Restricts the removal of Entity History records to only those created between the dates set. These are optional and if not provided then no date restriction will be applied.
Entity Type	Restricts the Cleardown utility to only particular Entity Types. The drop down list shows the entire list of Entities that Entity History can be recorded for.

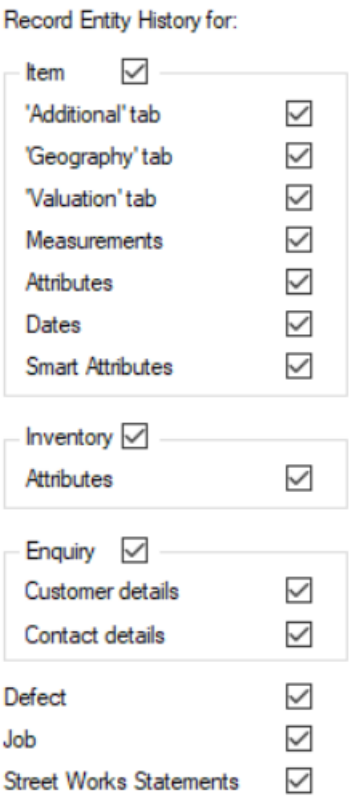
The Preview Report will display the Entity History records retrieved based on the filter criteria, and all of these displayed records will be removed from Confirm. The records will not be removed until the 'Save' button is clicked, and upon completion the Report Title will change from “Entity History Cleardown Report” to “Entity History Cleardown – Result”.

Entity History System Settings

The Entity History Settings define the Feature, Inventory, Enquiry, Job, Defect data for which changes are tracked and recorded.

Entity History will record changes made through Confirm screens and also via other means such as Import Utilities, Batch Utilities, and the results of work carried out on a mobile device.

Except for Enquiry data, which is not dependent on Features, the general settings on this screen are further controlled on a per Feature Group basis. Entity History will only be recorded for Features (or Inventory Items) in a Feature Group that has the 'Maintain History' box ticked on the Feature Group screen.



Feature:	This box must be ticked to 'activate' audit trails for Features. If only this box is checked, the data recorded in fields on the Feature tab of the Feature form will be tracked and may be reported on.
'Additional' tab:	To also record changes in fields on the Additional tab of the Feature form.
'Geography' tab:	To also record changes in fields on the Geography tab of the Feature form.
'Valuation' tab:	To also record changes in fields on the Valuation tab of the Feature form.
Measurements:	To also record changes to Measurement values on the Attributes tab of the Feature form.
Attributes:	To also record changes to Pick List and Text values on the Attributes tab of the Feature form.
Dates:	To also record changes to Date values on the Attributes tab of the Feature form.
Smart Attributes:	To also record changes to Smart Attribute values.
Inventory:	This box must be ticked to record changes to Inventory Items.
Enquiry:	This box must be ticked to 'activate' audit trails for Enquiry Customer or Contact details.
Customer Details:	Tick this to tell Confirm to record updates to any of the following Customer fields of existing Enquiry: • Forename • Surname • Address • Telephone No.

- Alternate Tel.
- Mobile Tel.
- Fax No.
- Email

Contact Details: Tick this to tell Confirm to record updates to any of the following Contact fields of existing Enquiry:

- Contact
- Email
- Telephone No.
- Alternate Tel.
- Fax No.

Attributes: To also record changes to any of the Attributes of Inventory Items.

Job: Tick this to tell Confirm to record changes to Job Attributes and any of the following fields:

- Site Code
- Plot Number
- Estimated Start Date
- Actual Start Date
- Estimated Completion Date
- Actual Completion Date
- Liability Date

Defect: Tick this to tell Confirm to record changes to any of the following Defect fields:

- Site Code
- Plot Number
- Date
- Target Date
- Observation type
- Defect type
- Priority
- Defect Notes
- Job number
- Defect Status

Street Works Statements: Tick this to record changes to any of the following fields on Statement Items:

- Charge
- Discount
- Apply Charge
- Reviewed
- Comments

All System Settings

This folder contains copies of all of the screens which contain settings which can be used to alter the behaviour of Confirm. These screens are also available in their appropriate folder e.g. the Feature System Settings will also appear in the Feature Lookups folder. The options available depend on the current User's permissions and the modules activated.

All Seed Numbers

This folder contains copies of all of the screens which contain Seed Numbers. Seed Numbers are required for creating many items in Confirm where a unique number is needed e.g. Jobs. These screens are also available in their appropriate folder e.g. the Job Seed Numbers will also appear in the Maintenance Lookups folder. The options available depend on the current User's permissions and the modules activated.