Doc Ref
System Managing Users, Groups & Permissions Handbook/Autumn 2016/2016-12-07
© Capita Business Services Ltd 2016. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, translated or transmitted without the express written consent of the publisher. Microsoft® and Windows® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

www.capita-one.co.uk

Contacting the Service Desk
You can log a call with the Service Desk via the Customer Service tool available on My Account.

Providing Feedback on Documentation
We always welcome comments and feedback on the quality of our documentation including online help files and handbooks. If you have any comments, feedback or suggestions regarding the module help file, this handbook (PDF file) or any other aspect of our documentation, please email:

onepublications@capita.co.uk

Please ensure that you include the document name, version and aspect of documentation on which you are commenting.
Changing a Password in v3 Client ................................................................. 20
Changing a Password in v4 Client ................................................................. 20
Changing a Password in v4 Online ................................................................. 20
Self Service Password Resets ....................................................................... 21

05 | Creating Users in Bulk ............................................................................. 22
   Introduction .................................................................................................. 22
   Creating user accounts in bulk .................................................................... 22

06 | Managing Groups in v3 .......................................................................... 24
   Introduction .................................................................................................. 24
   Creating a Group .......................................................................................... 24
   Adding Users to a Group ............................................................................. 24

07 | Managing Groups in v4 .......................................................................... 26
   Introduction .................................................................................................. 26
   Creating a user group ................................................................................... 26
   Adding users to a group .............................................................................. 26
   Viewing user details .................................................................................... 27
   Removing users from a group ...................................................................... 27
   Adding a group administrator ...................................................................... 27
   Removing a group administrator ................................................................. 28
   Viewing a user group's details ..................................................................... 28

08 | Managing Permissions ............................................................................. 29
   Permissions .................................................................................................. 29
   User Group Processes .................................................................................. 29
   Assigning Permissions to a Group via a Business Process ......................... 30
      Permit/Deny Permissions .......................................................................... 31
      Invalid Requests ...................................................................................... 32
      Interdependencies ..................................................................................... 32
   User Group Permissions .............................................................................. 33
   Assigning Permissions to Data Items .......................................................... 33
   Assigning Permissions to All Secured Data Items ...................................... 35
      Assigning Permit Read Permissions ......................................................... 35
      Assigning Permit Read/Write Permissions ................................................. 36
      Assigning Read-Only and Read/Write Permissions ................................. 37
   Report Permissions ...................................................................................... 37
      Assigning Permissions to Reports Related Business Processes ............... 38
      Assigning Permissions to the Report Definition Repository .................. 38
   Access Control Lists (ACL) ........................................................................ 42
   Access Levels .............................................................................................. 42
   Access Priority ............................................................................................ 43
   Setting ACL Defaults .................................................................................. 44
   Setting an ACL for an Entity ...................................................................... 45
   Data Panels ................................................................................................. 47
Introduction ..................................................................................................................... 47
Using the Data Panels Button .......................................................................................... 47

09 | Appendix ........................................................................................................ 49

Reference Material ........................................................................................................ 49
Reference Guides (v4 Client) .......................................................................................... 49
Reference Guides (v4 Online) ........................................................................................ 49

Index .............................................................................................................................. 50
System – Managing Users, Groups and Permissions

Overview

One v4 is a Management Information System that is used for a Local Authority’s day-to-day administration, management and the monitoring of performance data. Each module can operate independently, as free-standing software solutions to meet the needs of separate departments.

One can generate many Government returns and statistics required by the Department for Education (DfE) and the Welsh Government (WG).

Data held in the SIMS system can also be accessed by the equivalent One product, enabling transfer of data between schools and central departments.

The One v4 system is divided into two separate areas:

- v4 Client
- v4 Online

Licence keys are required for all areas of the v4 Client and v4 Online.

The v3 Client is used for some administrative purposes.

One v3 Client

The v3 Client can be used for a number of v4 system administration functions. This area is where the System Administrator can define users, both individual and groups, and manages the datasets used by One, enabling the user to carry out the various processes in One v4 Client and One v4 Online.

System Administration is accessed via One Module Launcher | Tools | System Administration.

These v3 system administration functions are now available in the v4 Client.

One v4 Client

The v4 Client is where the System Administrator define users, both individual and groups, enabling the user to carry out the various processes in One v4 Client and One v4 Online.

System Administration is accessed via Tools | Administration | User Management.

The v4 Client has a strong emphasis on guiding the practitioner through the One business processes. Where appropriate, data held in different One modules, e.g. Exclusions, Special Educational Needs (SEN) and Children’s Social Services (CSS), is auto-populated throughout the v4 Client, thus facilitating dynamic information sharing.

The v4 Client is separated into the following areas on the Focus tab:

- Adoption
- Analysis Reporting
- Aspects Management
- Bases
- Contact Record
System – Managing Users, Groups and Permissions

- Data Management
- Early Years
- Enquiries
- Fostering
- Governors
- ICS Forms
- Manage Cases
- CP-IS
- People
- Results Management
- Services
- Enquiries
- Early Years
- Staff
- Health Centres
- Hearing and Visual Impairment
- Equipment Inventory.

The v4 Client is separated into the following areas on the Tools tab:

- Administration
- Audit Trail
- Change Password
- Permissions
- Team Structure
- Year Settings
- FID
- PRIME
- Lock/Unlock System
- Data Management (Archiving)
- V3 Migration
- Activity Log
- Set Mandatory Field.

One v4 Online

One v4 Online enables individual practitioners, services and the local authorities to share data electronically, resulting in a more joined-up approach by practitioners from different disciplines to coordinate and deliver services that best support the needs of local children and families. It enables more efficient processes to be adopted, as well as providing a greater degree of flexibility for the user to access the information they need, when they need it.
The following areas are available in One v4 Online:

- A&T Application
- A&T Back Office
- A&T Preferences
- Administration
- Applications
- B2B: Student
- Bases
- Citizen Portal Admin
- CSS (including SEN, Hearing and Visual Impairment)
- Exclusions
- Governors
- Music Tuition (Courses)
- Portal Back Office
- Prof. Portal Admin
- Training Manager
- Transport Back Office

Licence keys are required for all areas of v4 Online. System Administration is accessed via Administration | System Admin.

**Using this Handbook**

This handbook is intended for Administrators and System Administrators of the One system. Administrators control users access to the One suite of modules, in both v4 Client and v4 Online.

The Administrator must assign membership of a dataset and a user group to each user in One v3 or One v4 Client, before access to One v4 is possible. Permissions and the specific level of access are applied to the group of which users are members. Passwords are set up by an Administrator, but a user can change their password if required.

This handbook explains these processes in detail.

**Reference Guides**

A number of reference guides are available to help with the processes in One v4. Where a reference guide is available, it is displayed as an additional resource.

<table>
<thead>
<tr>
<th>Additional Resources:</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>RG_Equipment</em> available on the One Publications website (<a href="http://www.onepublications.com">www.onepublications.com</a>) and also via My Account.</td>
</tr>
</tbody>
</table>

**Accessing Reference Guides via My Account**

The *One Reference Guide* document is available in the *Sticky Items* section of the *My Account* home page. This lists the available reference guides and their resource numbers. The list highlights newly added reference guides, and guides that have been updated (updated reference guides may have a new resource number).
To access the reference guides via My Account:

1. Select the **Knowledge Base** tab to display the **Knowledge Base** page.
2. Under the **Popular Searches** list, click the **Sticky Items** link.
3. Enter **One Reference Guides** in the **Search for** field, then click the **Find** button to display the **One Reference Guides PDF**
4. Click the **Resource No.** link in the PDF to view the latest version of the reference guide.

**NOTE:** Please ensure you are always working from the latest version.
Managing Users in v3

Introduction

In v4 Client and v4 Online, access to different areas of One is not controlled at the individual user level, but at the group level. Therefore, each user must be assigned to at least one user group to use the One software. However, group members must first be created as individual users in the v3 or v4 client. The following chapter describes managing users in the v3 Client. Users can also be managed in the v4 Client.

MORE INFORMATION:
- Managing Groups in v3 on page 24
- Managing Users in v4 on page 10
- Managing Groups in v4 on page 26

Creating a User

Creating users is done by an administrator in One v3. To create a new user:

1. From the One Module Launcher screen, select Tools | System Administration | Users tab.
2. Click the Add button to display the User Details sub-tab.
3. Enter a Login ID; this is the User Identifier (ID) when logging in to One.
4. Enter a User Name; this is the name of the person.
   - The Active check box is selected by default. A user cannot be deleted from One; they must be made inactive.
   - The number of Failed Logins displays if the user enters an incorrect password. For example, if a user has incorrectly entered their password once in v4 Client and twice in v4 Online the field displays as 1 / 2.
5. If required, enter a Telephone number.
6. If required, enter an E-Mail Address. An e-mail address must be entered if you wish the user to be synchronised to Outlook.
7. Select the required check the box if the user is to be a:
   - **System Admin** - This gives access to all System Administration areas in v4 Client and all Administration areas in v4 Online.
   - **Role Manager** - A Role Manager is able to add people to the Role table; this is particularly relevant for Base Contacts.
Managing Users in v3

- **Reports Manager** - This role enables a user to set up new reports and gives access to any reports. This overrides any field level security.

8. Enter a **Password**. The user is prompted to change this password the first time they log in. For more information, see [Password Strength](#) on page 17.

9. If the user needs a mapping assigned, click the **Mappings** button. For more information, see [Mapping a User](#) on page 6.

10. To assign a signature, click the **Signature** button. For more information, see [Adding a Signature](#) on page 7.

11. Click the **Save** button.

**Mapping a User**

Users **must** be mapped to a person to gain access to involvement records, activities, risks and the CSS service team workload. It also ensures workflow messages work correctly, as these are linked to the person and not the User ID. All ICS users **must** be mapped to a person. Each user must only be mapped to one person; this is usually themselves. PULSE users do not need to be mapped.

To map a user:

1. From the **One Module Launcher** screen, select **Tools | System Administration | Users** tab.

2. From the user list on the left-hand side, select the user to whom you wish to assign a mapping.

3. On the **User Details** sub-tab, click the **Mappings** button to display the **User Mappings** dialog.

4. Click the **Person** browse button to display the **Select a Person** dialog.

5. Enter the search criteria, then click the **Search** button to display the **Select a Person** browse list.

6. Highlight a record and click the **Select** button to return to the **User Mappings** dialog; the mapped person displays in the **Mapping Details** panel.

7. Click the **Save** button to save the mapping.
Adding a Signature

A signature, in graphic format, can be added to a user. The purpose of adding a signature to the database is to allow an authentic looking signature to be included in Crystal letters that are to be batch printed.

To add a signature:

1. From the **One Module Launcher** screen, select **Tools | System Administration | Users** tab.
2. From the user list on the left-hand side, select the user you wish to add a signature to.
3. Click the **Signature** button to display the **User Signature** dialog; the following message displays:
   
   No signature attached.
4. Click the **Attach Signature** button to display the **Select a Photo** dialog.
5. Locate the required signature graphic file; the graphic may be in .bmp, .gif or .jpg format.
6. Click the **Open** button to insert the signature into the display panel.

7. Click the **Close** button to return to the **User Details**.
8. Click the **Save Changes** button.

Choosing a Group

A user must be allocated to a group to be able to use v4 Client and v4 Online. For more information, see **Creating a Group** on page 24.

To choose a group:

1. From the **One Module Launcher** screen, select **Tools | System Administration | Users** tab.
2. From the user list on the left-hand side, select the user you wish to assign to a group.

3. Click the **Choose Group** button to display the **Choose Groups Belonged To** dialog.
4. In the Groups Not Belonged To panel, select the group to which you wish to add the user. Use the Looking For: field to jump to a specific group.

5. Click the right single-chevron to add the group to the Groups Belonged To panel.

6. Click the Save button to return to the User Details sub-tab, the Group Name browse is populated.

7. Click the Save Changes button at the top of the page to save the record.

More Information:
Creating a Group on page 24.

Choosing a Dataset
A user must belong to a dataset to be able to use v4 Client and v4 Online.
To choose a dataset:
1. From the One Module Launcher screen, select Tools | System Administration | Users tab.
2. From the user list on the left-hand side, select the user you wish to assign to a dataset.

3. Click the Choose Datasets button to display the Choose Dataset Belonged To dialog.

4. In theDatasets Not Belonged To panel, select the dataset to which you wish to add the user. Use the Looking For: field to jump to a specific dataset.

5. Click the right single-chevron to add the dataset to the Datasets Belonged To panel.

6. Click the Save button to return to the User Details sub-tab, the Datasets browse is populated.
7. Click the **Save Changes** button at the top of the page to save the record.

**NOTE:** Users can only be assigned to one dataset in the live instance. It is possible to have multiple datasets in the test instance.
03 Managing Users in v4

Introduction

In v4 Client and v4 Online, access to different areas of One is not controlled at the individual user level, but at the group level. Groups are made up of users who have been created in either the v3 or v4 Client. Therefore, each user must be assigned to at least one user group to use the One software. The following chapter describes managing users in the v4 Client.

User accounts are created and maintained in the v4 Client via Tools | Administration | User Management | User Accounts. You must be a One system administrator or a One user with the appropriate permissions to administer user accounts. User names must be unique and can only contain alphanumeric characters with no spaces.

For auditing purposes, once a user is created, they cannot be deleted, they can only be made inactive.

For all new user accounts, the user is prompted to change their password the first time they try to log into One.

The following table summarises the information that can be recorded when creating a new user account.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
<th>Mandatory</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>A unique user name for the account. The user must enter this to log in to the system. Must be at least one alphanumeric character in length.</td>
<td>Yes</td>
</tr>
<tr>
<td>User Description</td>
<td>Additional text to describe the user account. This is displayed when searching for accounts and in the title bar when viewing account details. Must be at least one alphanumeric character long.</td>
<td>Yes</td>
</tr>
<tr>
<td>Active</td>
<td>Checked by default. Only active users can log in to the One system. Both active and inactive users can be edited by an administrator.</td>
<td>Yes – must be a tick (to make the user active) or an x (to make them inactive).</td>
</tr>
<tr>
<td>System Admin</td>
<td>Deselected (x) by default. If selected, the user has full ability to administer the One environment.</td>
<td>Yes – must be a tick (to make the user a system administrator) or an x (to keep them as a standard user).</td>
</tr>
<tr>
<td>E-Mail Address</td>
<td>The user’s email address.</td>
<td>No</td>
</tr>
<tr>
<td>Field name</td>
<td>Description</td>
<td>Mandatory</td>
</tr>
<tr>
<td>------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------</td>
</tr>
<tr>
<td>Domain User ID</td>
<td>The UPN (User Principal Name) of Windows Active Directory you want to associate with the Capita One user account. Currently, the details entered here are not used within One. However, from the One Autumn 2015 Release, this UPN can be used to validate against your Windows Active Directory (AD). The entered value must be the name of an AD user in an e-mail address format. The username is followed by an “at” sign (@) followed by the name of the domain with which the user is associated. For example: ‘<a href="mailto:john.smith@capitala.com">john.smith@capitala.com</a>’.</td>
<td>No</td>
</tr>
<tr>
<td>Telephone</td>
<td>The user’s telephone number.</td>
<td>No</td>
</tr>
<tr>
<td>Password</td>
<td>The user’s password. Must be at least 10 alphanumeric characters long and meet the password requirements. For more information about password requirements, see Password Strength on page 17.</td>
<td>Yes</td>
</tr>
<tr>
<td>Mapped Person</td>
<td>Enables you to associate the user to a person already in the One database. For example, you can associate the user name to a member of a service team so that the user can view Involvements, Activities and Risks. <strong>NOTE:</strong> A person in One can only be mapped to one user account. If you attempt to associate a user account to a person who is already mapped to another user account, a warning is displayed at the bottom of the screen and you cannot save the user account details until you either remove the person from the mapping for the current user or remove the mapping that already exists.</td>
<td>No</td>
</tr>
<tr>
<td>Mapped Base</td>
<td>Enables you to associate the user to a base recorded in the One database.</td>
<td>No</td>
</tr>
</tbody>
</table>

**Creating a user**

One administrators and One users with the appropriate permissions can create new users. To create a new user in the v4 Client:

1. Select **Tools | Administration | User Management | User Accounts** to display the **User Accounts Enquiry** page.
2. In the **User Accounts Enquiry** panel, click the **New** button to display the **User Account Details [New User]** page.
3. In the **User Account Details** panel, enter the required **User Name** and **User Description**.
4. Ensure the **Active** and **System Admin** options are ticked or crossed as required.
5. Enter any optional information.
6. Enter a **Password** for the user. For more information, see **Password Strength** on page 17.

7. If required, map the user to a person, base or both.

8. If required, assign the user to user groups.

9. If required, make the user an administrator of any required groups.

10. Click the **Save** button.

You should now provide the user with their user name and password details. They are prompted to change their password the first time they try to log in to One.

### MORE INFORMATION:
- Mapping a user to a Person on page 12
- Mapping a user to a Base on page 12
- Adding a user to a group on page 14
- Making a user a group administrator on page 14
- Password Strength on page 17

---

### Mapping a user to a Person

A user can be mapped to a person already recorded in the One database. Users **must** be mapped to a person to gain access to involvement records, activities, risks and the CSS service team workload. It also ensures workflow messages work correctly, as these are linked to the person and not the User ID. All ICS users **must** be mapped to a person. Each user must only be mapped to one person; this is usually themselves. PULSE users do not need to be mapped.

**NOTE:** A person in the One database can only be mapped to a single user at a time. If you attempt to map a second user to a person, an error message displays at the bottom of the page. Double click the error message to display the details of the user to whom the person is already mapped. You must remove the existing mapping before you can create the new mapping.

You can create the mapping when first creating the user or by editing an existing user. Follow the same procedure to edit an existing mapping.

1. In the v4 Client, select **Tools | Administration | User Management | User Accounts** to create a new user or open an existing user account. For more information, see **Viewing user details** on page 15.

2. In the **User Account Details** panel of the **User Account Details** page, click the **Select**... button adjacent to the **Mapped Person** field to display the **Person Enquiry** dialog.

3. Enter your search criteria and click the **Search** button to display a list of people who meet the criteria.

4. Highlight the required person in the list and click the **Select** button to associate them with the user account. The **Person Enquiry** dialog closes automatically.

5. On the **User Account Details** page, click the **Save** button.

---

### Mapping a user to a Base

A user can be mapped to a base already recorded in the One database. This is used throughout one, for example to link a governor to a base. You can create the mapping when first creating the user or by editing an existing user. Follow the same procedure to edit an existing mapping.

1. In the v4 Client, select **Tools | Administration | User Management | User Accounts** to create a new user or open an existing user account. For more information, see **Viewing user details** on page 15.
2. In the **User Account Details** panel of the **User Account Details** page, click the **Select…** button adjacent to the **Mapped Base** field to display the **Base Enquiry** dialog.

3. Enter your search criteria and click the **Search** button to display a list of bases that meet the criteria.

4. Highlight the required base in the list and click the **Select** button to associate the base with the user account. The **Base Enquiry** dialog closes automatically.

5. On the **User Account Details** page, click the **Save** button.

### Removing a user mapping

To remove the association between a One user account and a person or base, complete the following procedure:

1. In the v4 Client, select **Tools | Administration | User Management | User Accounts** to create a new user or open an existing user account. For more information, see [Viewing user details](#) on page 15.

2. In the **User Account Details** panel of the **User Account Details** page, click the **Clear Selection** button adjacent to the **Mapped Person** or **Mapped Base** field as required.

3. Click the **Save** button.

### Resetting a user password

If a user forgets their password and does not have an email associated with their One account and so cannot reset the password themselves, a One administrator can reset the user’s password. The administrator can also choose to force the user to reset the password the next time the user logs into One.

1. Open the required user account. For more information, see [Viewing user details](#) on page 15.

2. Enter a new **Password**.

3. Click the **Save** button to display a confirmation dialog.

4. If you want to force the user to reset their password when they next log in, click the **Yes** button. If you do not want to force the user to reset their password when they next log in, click the **No** button.

**MORE INFORMATION:**
- [Password Strength](#) on page 17
- [Self Service Password Resets](#) on page 21

### Changing a user’s Active status

By default, when a user is created, they have a status of active (a tick (✓) against the **Active** check box). This means they can log in and use One as normal, based on the permissions that a system administrator has granted them. If a user is made inactive (an ‘x’ in the **Active** check box, then they cannot log into One, however, system administrators can continue to manage the user as normal.

1. Open the required user account. For more information, see [Viewing user details](#) on page 15.

**IMPORTANT NOTE:** By default, the search only returns active users. If the user is already inactive and you want to make them active, when searching for the user, you must ensure the **Active** check box has an ‘x’ against it.
2. In the User Account Details panel, click the **Active** check box until it displays the required status. A tick (✓) indicates the user is active. A cross (x) indicates the user is inactive.
3. Click the **Save** button to update the user’s status.

**Adding a user to a group**

In most cases, One user should be added to at least one user group to inherit the permissions assigned to the group. To add an existing user to a group:

1. In the v4 Client, select **Tools | Administration | User Management | User Accounts** to create a new user or open an existing user account. For more information, see Viewing user details on page 15.
2. In the Member of Groups panel of the User Account Details page, click the **Add** button to display the Select Group(s) dialog.
3. Click the check box in the Select column for each group to which you want to add the user. You can filter the list by entering search criteria in the User Group Name or User Group Description fields and clicking the Search button.
4. Click the Select button to add the user to the group and close the dialog. The groups of which the user is a member are displayed in the Member of Groups panel.

**Viewing group details**

To view the details of any group of which a user is a member or an administrator:

1. Open the required user account. For more information, see Viewing user details on page 15.
2. In the Member of Groups panel, select the group whose details you wish to view.
3. Click the View button to display the group details.

**Removing a user from a group**

To remove a user from a user group:

1. Open the required user account. For more information, see Viewing user details on page 15.
2. In the Member of Groups panel, select the group from which you wish to remove the user.
3. Click the Remove button.
4. Click the Save button.

**Making a user a group administrator**

In Local Authorities with many users and groups, it can be useful to create group administrators who can manage the membership of specific groups but do not have other system administrator rights.

To be a group administrator, a user must be part of a user group with the correct access to the User Accounts and User Groups business process, which are part of the Administration main business process. The following table summarises the capabilities granted by each level of access:

<table>
<thead>
<tr>
<th>Business Process</th>
<th>Read</th>
<th>Read-Write</th>
<th>Read-Write-Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts</td>
<td>✓ - Minimum level, can view but not edit user details.</td>
<td>✓ - Can view and edit user details.</td>
<td>N/A</td>
</tr>
</tbody>
</table>
Business Process | Read | Read-Write | Read-Write-Delete
--- | --- | --- | ---
User Groups | ✓ - Minimum level, can view but not edit group details. | ✓ - Can add users to and remove users from the groups they administer. | ✓ - Group administrators can manage group membership and also delete the groups they administer.

To add a user as a group administrator:

1. Open the required user account. For more information, see Viewing user details on page 15.
2. In the Permitted to Administer Groups panel of the User Account Details page, click the Add button to display the Select Group(s) dialog.
3. Click the check box in the Select column for each group you want the user to administer. You can filter the list by entering search criteria in the User Group Name or User Group Description fields and clicking the Search button.
4. Click the Select button. The dialog closes automatically.
5. Click the Save button.

Removing group administrator rights from a user

To remove a user’s group administrator rights:

1. Open the required user account. For more information, see Viewing user details on page 15.
2. In the Permitted to Administer Groups panel of the User Account Details page, select the group from which you wish to remove the user as an administrator.
3. Click the Remove button.
4. Click the Save button.

Viewing user details

To search for and view a user’s details:

1. In the v4 Client, select Tools | Administration | User Management | User Accounts to display the User Accounts Enquiry page.

   **IMPORTANT NOTE:** By default, the search only returns active users. To find inactive users, you must ensure the Active check box has an ‘x’ against it.

2. If required, enter any search criteria in the User Accounts Enquiry panel.
3. Click the Search button to display a list of all the users that match your search criteria. If you did not enter any search criteria, all users are returned.
4. In the list of users, double-click the name of the user to display their details in the User Account Details [User Name] page.

   The User Account Details page has two panels of read-only information that can be used for auditing purposes, the Login Information panel and the Last Updated Details panel.

   The following table summarises the read-only details:

<p>| Login Information panel |</p>
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
### Login Information panel

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Failed Logins</td>
<td>The number of failed login attempts since the last successful login. This number is reset each time the user successfully logs in.</td>
</tr>
<tr>
<td>Machine</td>
<td>The numbers to the left of the dash are the IP address of the machine on the local network. The Windows network name of the computer from which the last login attempt (either successful or unsuccessful) was made is to the right of the dash.</td>
</tr>
<tr>
<td>OS User</td>
<td>The Windows user account from which the Capita One user logged in, this is not populated if the user has logged in from v4 Online.</td>
</tr>
<tr>
<td>Fail Time</td>
<td>The date (DD-MM-YYYY) and time (HH:MM) that the last failed login attempt occurred.</td>
</tr>
</tbody>
</table>

### Last Updated Details panel

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User ID</td>
<td>The One user ID for the selected user.</td>
</tr>
<tr>
<td>Created By</td>
<td>The One user that created the currently selected user account.</td>
</tr>
<tr>
<td>Created On</td>
<td>The date (DD-MM-YYYY) and time (HH:MM:SS) on which the currently selected user account was created.</td>
</tr>
<tr>
<td>Last Updated By</td>
<td>The One user that most recently updated the currently selected user account.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date (DD-MM-YYYY) and time (HH:MM:SS) on which the currently selected user account was most recently updated. Updates include changes to the user’s personal details as well as changes to groups of which the user is a member.</td>
</tr>
</tbody>
</table>
Managing Passwords

Introduction

Passwords are created by the System Administrator in v3 or v4 Clients. You can set a password expiry period and set up automatic account locking if too many incorrect logins are attempted.

Password Strength

In order to ensure that passwords for One user accounts are sufficiently secure, One enforces the following password strength requirements:

- Must contain between 10 and 128 characters
- Must contain one uppercase, one lowercase, one numeric and one special character
- Must not be the same as the username
- New password cannot be the same as the previous 10 passwords
- New password cannot numerically increment the existing password, e.g. if the existing password is Lack!ngEntropy29, the new password cannot be Lack!ngEntropy30.

These rules are not configurable within the One software. The rules apply to any passwords created within any of the following One interfaces:

- v3 Client
- v4 Client
- v4 Online
- modules hosted in the Provider portal
- modules hosted in the Professional Portal
- modules hosted in the Citizen Portal
- System Portal
- Transport v4

Password Expiry

You can set a password expiry value to automatically force users to change their passwords after a set number of days. When setting the expiry period, you can also choose accounts that should not be forced to change their password periodically.

Setting Password Expiry in the v3 Client

To configure the Password Expiry in the v3 Client:

1. Select Tools | System Administration | Passwords
2. Select the Passwords expire automatically radio button to display the number of days selector and the Except For panel.
3. Enter the number of days or use the arrows to change the frequency that passwords should be changed for all users.

If the expiry limit is changed, all users' passwords (except for those whom an exception has been made) will expire \( nn \) calendar days after their last change of password. If any users have not previously changed their password, their password will expire \( nn \) calendar days after their next login.

4. If required, on the Except For panel, click the Choose button to select users whose passwords should never expire.

5. Click the Save button at the top of the page to save the changes.

**Setting Password Expiry in the v4 Client**

To configure the password expiry in the v4 Client:

1. In the v4 Client, select Tools | Administration | User Management | Password Management to display the Password Management page.

2. In the Password Expiry panel, select the Expire passwords periodically check box.

3. In the Password expiry periods (In days) is field, enter the number of days after which a user will be forced to change their password.

4. If required, add users whose passwords should not be automatically expired:
   a. In the Users excluded from password expiry section, click the Add button to display the Add User Accounts dialog.
b. Search for the required users and click the check box in the Select column adjacent to the names or users to exclude.

c. Click the Select button to exclude the selected accounts and close the dialog.

5. Click the Save button.

**Account Locking**

Account locking enables you to set the number of times that a user can try to log in using the wrong password before the account is locked. If an account is locked, then the user must contact a One administrator to reset their password and unlock the account.

**NOTE:** If a user attempts to exceed the maximum number of logins in the A&T public facing application, a time lock of 20 minutes is applied.

**Setting Account Locking in the One v3 Client**

The **Account Locking** default option is **No locking of accounts when incorrect passwords are entered**.

To set the number of failed attempts before an account is locked:

1. Select the **Lock accounts after a number of incorrect passwords have been entered** radio button to display the number of attempts selector. Before you can change the number of attempts the following message displays:
Managing Passwords

If you enable account locking, you are advised to create at least one alternative System Administrator level account, with a non-standard user name, in case the default SYSADMIN account becomes locked.

2. Enter the number or use the arrows to change the default number, up to 100.
3. Click the Save button at the top of the page to save the changes.

Setting Account Locking in the One v4 Client
To set the number of failed attempts before an account is locked:

1. In the v4 Client, select Tools | Administration | User Management | Password Management to display the Password Management page.
2. In the Account Locking panel, select the Enforce Account Locking check box.
3. Enter the required number in the User accounts will be locked where the number of incorrect attempts is field.
4. Click the Save button.

Changing a Password
Users can change their passwords at any time in the v3 Client, v4 Client or v4 Online. The password changes are automatically updated throughout the One system.

Changing a Password in v3 Client
1. On the One Module Launcher screen, select Tools | Change Password to display the Change Password dialog.
2. Enter a new password, and then click the Continue button.
3. Confirm the new password.
4. Click the Save button.

Changing a Password in v4 Client
1. On the My Home Page screen, select Tools | Change Password to display the Change Password dialog.
2. Enter the Old Password.
3. Enter a New Password.
4. Enter the new password again in the Confirm New Password field.
5. Click the OK button.

Changing a Password in v4 Online
1. On the Login screen, enter your User Name.
2. Enter your old Password.
3. Click the Change Password button to display the Change Password dialog.
4. Enter the Old Password.
5. Enter the New Password.
6. Enter the new password again in the Confirm New Password field.
7. Click the OK button.
Self Service Password Resets

One users who have a valid email recorded against their account can reset a forgotten password from the v4 Client login dialog via the Forgotten your password button or from the v4 Online login page via the Forgotten your password link. After clicking the reset button or link the users receives a temporary password via email. When they log in with the temporary password, they are forced to create a new password.

If no email address is recorded for the user, then the user is asked to contact their system administrator when they try to reset their password.

**IMPORTANT NOTE:** In order for the self-service password reset facility to work, the One email service must be configured by a system administrator. For more information, refer to the Installing the Email Service chapter of the Installing and Configuring One v4 Core Components technical guide, available from the One Publications website ([www.onepublications.com](http://www.onepublications.com)).

For a user to reset their password:

1. Open the v4 Client or the v4 Online login page.
2. Click the Forgotten your password button/link to display the Reset Password confirmation dialog.
3. Click the Yes button to reset your password. A confirmation dialog is displayed and an email is sent to the email address associated with the user’s account.
4. Obtain the temporary password from the email.
5. Log into the v4 Client or v4 Online with the temporary password and follow the on-screen prompts to create a new password.
Creating Users in Bulk

Introduction

The batch create users facility, available in the One v4 client, enables you to create user accounts for bases (e.g. a school or a nursery) so that they can interact with the One software. For example, when first setting up your Provider Self Service portals, you can quickly create an administrator account for each provider. The account details can then be shared with the appropriate person at each provider so that they can finish the set up process and manage their portal.

Users created via the batch process have an automatically generated username, which is a number that combines the LA number and the school number. If there is no school number for a base, then no user account can be created for it. To help organization, each user account can have a suffix appended, for example you might add ‘P’ to indicate that the account is intended to be used for the Provider Self Service portal. This also means that you can create multiple users for the same base by running the routine multiple times, changing the suffix each time.

Users created with the batch process also have a password automatically assigned to them. Each account has a unique password based on their LA and school number. User account passwords cannot be viewed in the One software (even by administrators), therefore a Microsoft Excel spreadsheet, called Batch Create User Password.xls, is available that displays the user passwords based on the LA number and school number you enter. The passwords can then be copied from the spreadsheet and disseminated to the users at the providers. Contact the One Service Desk to obtain the spreadsheet.

The batch create users functionality is accessed via Tools | Administration | User Management | Batch Create Users.

Creating user accounts in bulk

One administrators can create One user accounts in bulk via Tools | Administration | User Management | Batch Create Users. The routine automatically maps the created users to the respective Base for which they were created. Users created via the batch create process are managed the same way as any other One user. You must assign the bases to user groups before you can run the batch create process. However, the group memberships can be edited as normal after the users are created.

IMPORTANT NOTE: Only bases with an LA number and school number recorded against them can have a user account created for them. If you cannot create a user account for a specific base, ensure there is an LA number and a school number and then run the batch create process again.

To use the batch create users process:

1. In the v4 Client, select Tools | Administration | User Management | Batch Create Users to display the Batch Create Users [Base Population] page.
2. In the Base Population panel, select the All LA Bases radio button to return all the available bases.
   Alternatively, select the Only LA Bases for Base Type radio button and select a base type from the drop-down to return only bases of the selected type.
3. Click the Search button to display a list of bases that meet the search criteria.
4. In the list of bases, select the check box in the Select column for each base for which you want to create a user.
5. If required, enter a **User Name Suffix** in the **User Account Parameters** panel. The suffix is added to the automatically generated user name and description.

6. Add the bases to the required groups.
   a. Click the **Add** button to display the **Select Groups(s)** dialog.
   b. Click the check box in the **Select** column for each group to which you want to add the bases. You can filter the list by entering search criteria in the **User Group Name** or **User Group Description** fields and clicking the **Search** button.
   c. Click the **Select** button to add the user to the group and close the dialog.

7. Click the **Create User(s)** button to create the users.

8. After the users are created, enter the user details into the **Batch Create User Password.xls** spreadsheet to obtain the passwords and then send the usernames and passwords to the designated individuals at each provider.

   You can view the list of users created and any errors that occurred for the most recent running of the batch process in the **User Creation Summary** panel. The content of this panel is updated each time you run the process or if you close the page. Therefore, if you receive any errors, you should investigate them as soon as possible or make a note of them for investigation later.

   The users can now be maintained just like any other users. For more information, see **Managing Users in v4** on page 10.
Managing Groups in v3

Introduction

In v4 Client and v4 Online work is carried out by group members, rather than individual users. Users that are not assigned to a group can only log in to One and change their passwords. Users can be added to groups in the v3 Client or the in the v4 Client.

A group can be created first and then the users can be added to the group. Once groups are created in v3 or v4, the groups can be assigned permissions in the v4 Client. Any user that is a member of a group receives the permissions defined in the v4 Client.

You must be a One system administrator or designated group administrator with the appropriate permissions to administer user groups. Group names must be unique and can contain alphanumeric characters, spaces and special characters.

MORE INFORMATION:
Managing Groups in v4 on page 26

Creating a Group

To create a new group:

1. From the One Module Launcher screen, select Tools | System Administration | Groups tab.
2. Click the Add button to display the Group Details panel.
3. Enter a Group Name.
4. Enter a Description.
5. Click the Save button to save the group details.

Adding Users to a Group

Group members are created from individual users.

To choose group members:

1. From the One Module Launcher, select Tools | System Administration | Groups tab.
2. In the Active Group Members panel click the Choose button to display the Choose Group Members dialog.
3. In the **Users Not in the Group** panel, select the user you wish to add to the group. Use the **Looking For:** field to jump to a specific user.

4. Click the right single-chevron to add the user to the **Group Members** panel.

5. Click the **Save** button to return to the **Group Details** sub-tab, the **Active Group Members** browse is populated.

6. Click the **Save Changes** button at the top of the page to save the group.
Managing Groups in v4

Introduction

In v4 Client and v4 Online work is carried out by group members, rather than individual users. Users that are not assigned to a group can only log in to One and change their passwords. Users can be added to groups in the v3 Client or in the v4 Client.

A group can be created first and then the users can be added to the group. Once groups are created in v3 or v4, the groups can be assigned permissions in the v4 Client. Any user that is a member of a group receives the permissions defined in the v4 Client.

You must be a One system administrator or designated group administrator with the appropriate permissions to administer user groups. Group names must be unique and can contain alphanumeric characters, spaces and special characters.

Creating a user group

To create a new user group:

1. In the v4 Client, select Tools | Administration | User Management | User Groups to display the User Groups Enquiry page.
2. In the User Group Enquiry panel, click the New button to display the User Group Details [New User Group] page.
3. In the User Group Details panel, enter a unique User Group Name and User Group Description.
4. If required, add group members and group administrators. Alternatively, you can edit group memberships later.
5. Click the Save button.

The user group is now created, but it still must have appropriate permissions assigned to it. To assign user group processes or permissions, use the User Group Permissions and User Group Processes hyperlinks in the Links panel on the right-hand side of the screen.

Adding users to a group

After creating a group, you can add users. Any users added to the group inherit the access to group business processes and group permissions that have been assigned to the group.
1. Open the user group to which you want to add members. For more information, see Viewing a user group’s details on page 28.

2. In the Group Members panel of the User Group Details page, click the Add button to display the Add User Accounts dialog.

3. If required, enter any search criteria in the User Accounts Enquiry panel.

4. Click the Search button to display a list of all the users who match your search criteria. If you did not enter any search criteria, all users are returned.

5. Click the check box in the Select column for all the users you want to add to the group.

6. Click the Select button to add the users to the group. The Add User Accounts dialog closes automatically.

7. Click the Save button.

### Viewing user details

To view the details of any user of a specific user group or to view the details of a group’s administrators:

1. Open the user group to which you want to add members. For more information, see Viewing a user group’s details on page 28.

2. In the Group Member panel or Group Administrators panel, select the user whose details you wish to view.

3. Click the View button to display the user’s details.

### Removing users from a group

To remove users from a group:

1. Open the user group to which you want to add members. For more information, see Viewing a user group’s details on page 28.

2. In the Group Members panel of the User Group Details page, select the member of the group you want to remove.

3. Click the Remove button.

4. Click the Save button.

### Adding a group administrator

In Local Authorities with many users and groups, it can be useful to create group administrators who can manage the membership of specific groups but do not have other system administrator rights.

To be a group administrator, a user must be part of a user group with the correct access the User Accounts and User Groups business process, which are part of the Administration main business process. The following table summarises the capabilities granted by each level of access:
### Managing Groups in v4

<table>
<thead>
<tr>
<th>Business Process</th>
<th>Read</th>
<th>Read-Write</th>
<th>Read-Write-Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Accounts</td>
<td>✓ - Minimum level, can view but not edit user details.</td>
<td>✓ - Can view and edit user details.</td>
<td>N/A</td>
</tr>
<tr>
<td>User Groups</td>
<td>✓ - Minimum level, can view but not edit group details.</td>
<td>✓ - Minimum level, can add users to and remove users from the groups they administer.</td>
<td>✓ - Group administrators can manage group membership and also delete the groups they administer.</td>
</tr>
</tbody>
</table>

To add a group administrator:

1. Open the required user group. For more information, see [Viewing a user group’s details](#) on page 28.
2. In the **Group Administrators** panel, click the **Add** button to display the **Add User Accounts** dialog.
3. If required, enter any search criteria in the **User Accounts Enquiry** panel.
4. Click the **Search** button to display a list of all the users who match your search criteria. If you did not enter any search criteria, all users are returned.
5. Click the check box in the **Select** column for all the users you want to add as group administrators.
6. Click the **Select** button to add the administrators to the group. The **Add User Accounts** dialog closes automatically.
7. Click the **Save** button.

### Removing a group administrator

To remove a group administrator:

1. Open the required user group. For more information, see [Viewing a user group’s details](#) on page 28.
2. In the **Group Administrators** panel, highlight the user to wish to remove as an administrator.
3. Click the **Remove** button.
4. Click the **Save** button.

### Viewing a user group’s details

To search for and view a user’s details:

1. Select **Tools | Administration | User Management | User Groups** to display the **User Groups Enquiry** page.
2. If required, enter any search criteria in the **User Groups Enquiry** panel.
3. Click the **Search** button to display a list of all the user groups that match your search criteria. If you did not enter any search criteria, all user groups are returned.
4. In the list of user groups, double-click the name of the group to display their details in the **User Group Details [User Name]** page.
Managing Permissions

Permissions

Permissions for v4 Client and v4 Online are maintained in the v4 Client via Tools | Permissions. Permissions in v4 are linked to user groups and not individual users.

Permissions are divided into the following areas:

- User Group Processes
- User Group Permissions
- Report Permissions

User Group Processes work in tandem with User Group Permissions. A link is available in the Links panel in both areas to switch between the two methods.

Changes made in one permissions area are reflected in the other. However, User Group Permissions allows for fine tuning of permissions assigned in User Group Processes.

**IMPORTANT NOTE:** SEN Memos and sections of Children’s Social Care (ICS) require Field Level Security to be set. This level of security must be set in User Group Permissions. Permissions assigned via User Group Processes do not override Secured Data settings.

User Group Processes

The User Group Processes functionality controls the level of access a user group has to specific areas and functionality within One. A group’s permissions can be assigned broadly against a main Business Process or to any of the individual Business Processes that constitute a Main Business Process. Business Processes map to menu routes and links, which in turn are linked to a user group, rather than an individual user.

**NOTE:** User Group Processes do not include All Secured Services items. This level of security is set in User Group Permissions.

User groups are assigned read, read-write, read-write-delete or deny permissions to each Business Process.

One contains the following Business Processes:

- ACL Button Permissions
- Address Management
- Addresses
- Administration
- Admissions Applications
- Admissions Finalising Processes
- Admissions Manage Import Online Apps
- Admissions Offers and Ranks
- Admissions Online Public
- Admissions Online School/LA
- CSS Administration
- Data Importing
- Disability Details
- Early Years Administration
- Early Years Finance
- Early Years Processing
- Early Years Setup
- Exclusions
- GNB
- Governors
Assigning Permissions to a Group via a Business Process

Assigning permissions to a Business Process consists of the following stages:

- Selecting a group
- Selecting a main business process
- Assigning permissions to individual business processes.

Permissions are edited in the User Group Processes Editor, which consists of the following panels:

- Select a Group
- Permissions Editor.

At the top of the page is a Collapse/Expand button that closes and opens the Select a Group panel, enabling the Permissions Editor panel to be displayed full width.

Opening and closing the Permissions Editor panel can be set to occur automatically by clicking on the drop-down arrows and selecting Automatically Collapse or Automatically Expand, depending on the current status of the Select a Group panel.

To assign permissions to a group via a business process, complete the following procedure:

1. In the v4 Client, select Tools | Permissions | User Group Processes to display the User Group Processes Editor window.
2. On the **Select a Group** panel, enter at least one letter in the **Looking For** field.

3. Select a **Search By** option to display the group list; the list is ordered according to the **Search By** criteria.

4. Highlight a group and click the **Select** button to display the **Permissions Editor | Main Processes** panel.

5. Select a **Main Business Process** to display the related **Business Processes** list; the name of the main business process displays at the top of the list in bold.

6. Click a cell to assign **Read**, **Read-Write** or **Read-Write-Delete** permissions; the default selection for all items is **Deny**. Clicking the main business process cell assigns that permission to all the individual processes below.

   If a cell is greyed out, the options are restricted and the permission is assigned to the next level down.

7. Click the **Save** button to save the permissions.

**Permit/Deny Permissions**

**Permit/Deny** permissions (a tick and a cross in the same cell) occur if both permit and deny permissions have been assigned to the processes within the **Main Business Process**.
When a change is made to processes within the main business process, the Permit/Deny icon displays in the column of the highest level permitted.

Invalid Requests

One does not allow a Deny selection if the denial invalidates another process. For example, if the user group is given the right to process student data, One does not allow attempts to deny the same group access to bases, as bases data is interlinked with student data. A warning message (similar to the following) displays:

Invalid Request

You cannot set this process as selected, because this will invalidate another process available to the user group.

If you continue, the system will:

1. Save the changed business processes that do not cause conflict.
2. Set the remaining processes to the minimum, so that other affected processes are not invalidated.

Do you wish to continue?

Select No to return to the Permissions Editor screen and set different permissions. (The user group must be given at least Read-Only permissions to bases, when access to student data is required)

Select Yes to save the changes as per the rules in the message.

Interdependencies

A number of processes within some of the main business processes require permissions to be assigned in another main business process.

The following areas contain interdependencies:

- Bases and Student Core Data
- Core Data and Student Data
- Exclusions and Student Data
- Results Administration and Student Data
- Results Administration and Data Importing.

Additional Resources:

RG_Permissions_User Group Processes and RG_Permissions_User Group Permissions available on the One Publications website (www.onepublications.com) and also via My Account.
User Group Permissions

User Group Permissions control group access to all web services, web methods, menu routes and menu links into the One Business Processes. It is accessed via Tools | Permissions | User Group Permissions.

The User Group Permissions Editor panel enables the System Administrator to control access for individual user groups to the various areas of One v4 Client and v4 Online.

User Group Permissions are divided into the following main data groups:

- **All Secured Services** – These are the permissions to data items that are displayed within the panels.
- **All Secured Menu Routes** – These permissions allow access to the data items in the Focus and Tools menus.
- **All Secured Menu Links** – These permissions are the links from the Links panel to other areas of One.
- **All Secured Data** – These permissions are related to data item security and require a higher level of permissions at field level. For more information, see Assigning Permissions to All Secured Data Items on page 35.

Assigning Permissions to Data Items

Assigning User Group Permissions consists of the following stages:

- Selecting a group.
- Selecting a data items folder.
- Assigning permissions to individual data items for the selected group.

To assign permissions to a user group, complete the following procedure:

1. Select Tools | Permissions | User Group Permissions to display the User Group Permissions Editor page.
2. On the Select a Group panel, enter at least one letter in the Looking For field.
3. Click the Search By drop-down and select one of the options to display the user group list; the list is ordered according to the Search By criteria.

4. Highlight a record and click the Select button to display the Permissions Editor panel; the System Map folder is displayed with the four data group folders below.
Managing Permissions

All data groups are displayed in a tree view. Each main data group is indicated by a folder icon. Double click a folder or click the plus sign to expand the group. Double click an expanded folder or click the minus sign to collapse the group.

The Run, Read and Write function buttons are activated when a data group or a data item is selected. Only the Run button is activated for the All Secured Services, All Secured Menu Routes and All Secured Menu Links data items. The Read or Write buttons are activated only when All Secured Data items are selected.

**IMPORTANT NOTE:** The data items located in All Secured Services | ICSF Person | Get ICS Person Details require Read or Read/Write permissions at individual field level.

5. To assign run permissions to all the data items within a data group, highlight the data group then click the Permit Run button. Assign permissions to individual data items by selecting the required item, then clicking the Permit Run button.

6. To deny permissions to all the data items within a data group, highlight the data group then click the Deny Run button. Deny access to individual items by selecting the required item, then clicking the Deny Run button.

7. Click the Save button to save the permissions.

**Permit/Deny Permissions**

If both permit and deny permissions are assigned to the data items within the main data group, then a tick and a cross icon displays next to the main business process.
Assigning Permissions to All Secured Data Items

The All Secured Data items require a higher level of permissions at field level. The majority of these permissions are ICS (now referred to as Children's Social Care) related.

Permissions may have been assigned via Tools | Permissions | User Group Processes. However, the System Administrator may wish to permit or deny permissions to individual data items, e.g. A Case Note Detail | Case Note Code.

There are two levels of permissions:
- Read
- Read/Write.

Assigning Permit Read Permissions

To assign Permit Read permissions to all the data items in a group:
1. Click the plus sign to open the All Secure Data items folder.
2. Click the plus sign to open the required group folder.
3. Highlight the group heading.
4. Click the Read button.
5. Click the Permit Read button; all the data items in the group display the read-only icon.
6. Click the Save button to save the permissions.

To assign Permit Read permissions to individual items in a group:
1. Click the plus sign to open the All Secure Data items folder.
2. Click the plus sign to open the required group folder.
3. Highlight a data item; you can only highlight one data item at a time.
4. Click the Read button.
5. Click the Permit Read button; the selected data items in the group display the read-only icon.
6. Click the **Save** button to save the permissions.

**Assigning Permit Read/Write Permissions**

To assign **Permit Read/Write** permissions to all the data items in a group:

1. Click the plus sign to open the **All Secure Data** items folder.
2. Click the plus sign to open the required group folder.
3. Highlight the group heading.
4. Click the **Read** button.
5. Click the **Write** button.
6. Click the **Permit Read/Write** button; all the data items in the group display the read/write icon.

7. Click the **Save** button to save the permissions.

To assign **Permit Read/Write** permissions to individual items in a group:

1. Click the plus sign to open the **All Secure Data** items folder.
2. Click the plus sign to open the required group folder.
3. Highlight a data item; you can only highlight one data item at a time.
4. Click the **Read** button.
5. Click the **Write** button.
6. Click the **Permit Read/Write** button; the selected data items in the group display the read/write icon.
7. Click the **Save** button to save the permissions.

### Assigning Read-Only and Read/Write Permissions

It is not always appropriate to assign permissions to all the data items in a group. **Permissions Editor | All Secured Data** enables you to assign permissions at individual field level.

To assign Read-Only, Read-Write permissions or to Deny access within a folder:

1. Click the plus sign to open the **All Secure Data** items folder.
2. Click the plus sign to open the required group folder.
3. Highlight the group heading and click either the **Read** or **Write** button; all the data items in the group display the selected permission.
4. Select an individual data item and choose whether this field requires **Read** or **Read/Write** permissions to be assigned.
5. Click the **Permit Read**, **Deny Read**, **Permit Read/Write** or **Deny Read/Write** button, depending on your selection in step 4.
6. Repeat steps 4 and 5 for all the data items (fields) in the group; the individual data items display the assigned permissions.

7. Click the **Save** button. Any changes to the **Permissions Editor** must be saved for the permissions to take effect.

**IMPORTANT NOTE:** The data items located in **All Secured Services | ICSF Person | Get ICS Person Details** require **Read** or **Read/Write** permissions at individual field level like All Secured Data items.

### Additional Resources:

- **RG_Permissions_User Group Permissions** and
- **RG_Permissions_User Group Processes** available on the One Publications website ([www.onepublications.com](http://www.onepublications.com)) and also via **My Account**.

### Report Permissions

Report Permissions are set up in the v4 Client via **Tools | Permissions | Report Permissions**.

Report Permissions enable the System Administrator to set up user groups to run both SSRS Reports (SQL Server Reporting Services) and Crystal Reports in v4 Client and v4 Online.
Assigning Report Permissions consists of the following stages:

- Assigning permissions to run the report business processes. For more information, see User Group Processes on page 29.
- Assigning permissions to run groups of reports.

After permissions have been assigned, user groups can access the v4 Client reports via the Reports link in the Links panel. The v4 Online reports can be accessed via the Reports area.

Assigning Permissions to Reports Related Business Processes

To assign permissions to the reports business processes, complete the following procedure:

1. Select Tools | Permissions | User Group Processes to display the User Group Processes Editor page.
2. On the Select a Group panel, enter at least one letter in the Looking For field.
3. Select a Search By option to display the results list based on the selected option.
4. Highlight the group and click the Select button to display the Permissions Editor | Main Processes panel.
5. Select the Administration Main Business Process to display the related business processes list; the permissions default options are set to Deny.
6. For each Report business process item, click the appropriate cells to assign Read, Read-Write or Read-Write-Delete permissions for the user group.
7. Click the Save button to save the permissions.

Assigning Permissions to the Report Definition Repository

In order to run a report, a user or group must be granted access to the report folder that contains the required report.
Reports are stored in folders within the Report Definition Repository. These folders contain the related Crystal Reports. If there are any available SSRS Reports, they are listed at the end of the Report Definition Repository list.

**NOTE:** Permissions to run reports are granted to the report folder and not to individual reports, so granting access to the folder will grant access to all reports within the folder.

To grant a group or user permission to run the reports in a specific folder, complete the following procedure:

1. Select **Tools | Permissions | Report Permissions** to display the **Report Permissions** page.

2. If you want to assign permissions to a group, ensure the **Groups** tab is selected and enter at least one letter in the **Group Name** field.

   Alternatively, if you want to assign permissions to a user, select the **Users** tab and enter at least one letter in the **User Name** field.

3. Click the **Search** button to display the group or users who meet your search criteria.
When viewing groups, you can highlight a group and click the **View Users** button to view the list of users in the selected group.

4. Select the required group or user.

5. In the panel on the left-hand side, click the plus sign to expand the **Report Definition Repository** folder and display the available report folders.
6. Select the folder to which you want to grant the selected group/user access, then click the **Grant** button; the cross changes to a tick to indicate that the permission has been assigned for the selected group or user.

There is no **Save** button on the **Report Permissions** page.
Managing Permissions

Access Control Lists (ACL)

The purpose of the ACL facility is to grant and restrict access rights to specific areas of One, where data is considered too sensitive to allow it to be viewed by non-authorised users.

Permission to view certain sensitive data, e.g. Person Details, is granted to the relevant entity by clicking the Set ACL button, located at the top of the page.

If a user or a user group has been denied access to data and they attempt to access the information, a warning message, created by the person defining the ACL, is displayed with an explanation as to why they have been denied access.

Permissions to use the ACL facility are set up by a System Administrator in the v4 Client via Tools | Permissions | User Group Processes | Main Business Process – ACL Button Permissions. For more information, see User Group Processes on page 29.

The following rules apply when an ACL is set up against a record:

- The person defining the ACL is automatically given permit access to a record.
- The person defining the ACL must specify at least one other rule (person, post, group or service team) in the ACL, otherwise the list is not saved.
- Anyone not included in the ACL definition is automatically denied access to a record.

**Warning:** When creating an ACL for any entity, only those users in the ACL (either as an individual or member of a group/role) for that entity have any access to the entity. Any other user or group is automatically denied from viewing or editing the entity.

Access Levels

There are three levels of access that can be applied: Read Summary, Read Details and Write. When ACL members are selected, allow (indicated by a tick icon) is the default setting, (deny is indicated by a cross icon).

- Clicking the buttons to allow Read Summary, Read Details and Write gives full access to the data.
- Clicking the buttons to allow Read Summary and Read Details, but to deny Write access, gives read-only access to the data; the user is not allowed to edit the data.
- Clicking the buttons to deny Read Summary refuses access to the Summary pages, therefore, it would not make sense to allow Read Details.
Clicking the buttons to deny Read Summary and Read Details, but allow Write access, denies access to see the data, but allows the data to be updated at system level, for example where the system is being updated from an external source.

**Access Priority**

The ACL function incorporates use of the following conventions when setting the access priority:

- **Favour Allow**
- **Favour Deny**

Favour Allow and Favour Deny dictate the access rights, either downgrading or upgrading a user’s permissions, depending upon which group or post the user is logging on as. Access priorities are used only to resolve conflicts between ACL permissions granted at different levels.

**Favour Allow**

Selecting the Favour Allow radio button results in those specified being granted access to a record, if a Read-Write permission has been applied to any of their Login, Post or User Group of which they are a member, even if they have been denied access to the record elsewhere in One.

The following scenarios are based on access to a Person record:

<table>
<thead>
<tr>
<th>Login ID</th>
<th>Summary</th>
<th>Read</th>
<th>Write</th>
<th>User Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group/Post User</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td>The user has full access to the record, although other members of the group/posts do not.</td>
</tr>
<tr>
<td>Group/Post User</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>The user has full access to the record, because their group/post membership elevates their access level (from read only).</td>
</tr>
<tr>
<td>Group/Post User</td>
<td>✔</td>
<td>✔</td>
<td>❌</td>
<td>The user has read-only access to the record, because that is the highest level of access to which their group membership elevates them.</td>
</tr>
<tr>
<td>Group/Post User</td>
<td>❌</td>
<td>❌</td>
<td>✔</td>
<td>The record will not be available for selection, however, it can be edited if accessed via a different area of One.</td>
</tr>
</tbody>
</table>

**Favour Deny**

Selecting the Favour Deny radio button results in those specified being denied access to a record, if a deny Read-Write permission has been applied to any of their Login, Post or User Group of which they are a member, even if they have been granted access to the record elsewhere in One.

The following scenarios are based on access to a Person record:

<table>
<thead>
<tr>
<th>Login ID</th>
<th>Summary</th>
<th>Read</th>
<th>Write</th>
<th>User Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group/Post User</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>The record will not be available for selection, because although their group/role membership has both read and write access they have been denied access at the user level/</td>
</tr>
</tbody>
</table>
Managing Permissions

## Setting ACL Defaults

The **Set ACL Defaults** button is accessed via **Focus | Services | CSS Service Teams Administration**; it enables the System Administrator to set the default access for service teams groups and users. ACLs set up for a service team are inherited by all associated entities, e.g. Involvements and Communication Log. If a service team default ACL is updated, the new ACL cascades to all related areas. ACLs customised at record level take precedence over default ACLs.

### When setting ACL defaults, the System Administrator selects between the following options to set which permissions takes precedence.

- **Favour Allow** – any allow permissions allow access; this is the default.
- **Favour Deny** – any deny permissions prevent access.

### To set the ACL defaults, complete the following procedure:

1. **Select** **Focus | Services | CSS Service Teams Administration** to display the **CSS Service Team Definition** page.
2. **Click the Set ACL Defaults button** to display the **Access Control List Definition** dialog.
3. **On the ACL Editor panel**, enter a **Description** for the ACL. The description displays when a user, who is not permitted to do so, attempts to access the ACL record. For example: **Access Denied. Please see your System Administrator.**
4. **Select the Favour Allow or Favour Deny radio button** to set the **Access Priority**.
5. **On the ACL Membership panel**, click one of the buttons to select the membership:
   - **Users** – displays the **User Selector** dialog; defined in v3 via **Tools | System Administration | Users**.

---

<table>
<thead>
<tr>
<th>Group/Post User</th>
<th>The record will not be available for selection.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group/Post User</td>
<td>The user will have read-only access.</td>
</tr>
</tbody>
</table>
Managing Permissions

- **Posts** – displays the Post Browser dialog; defined in v4 via Tools | Team Structure | Posts.

- **Groups** – displays the Group Selector dialog; defined in v3 via Tools | System Administration | Groups.

- **Service Teams** – displays the CSS Service Teams dialog; defined in v4 via Focus | Services | CSS Service Teams Administration.

6. If required, use the **Show** and **with** drop-downs to filter the membership lists.

7. Highlight a row (you can highlight more than one row at a time, by holding down the **Shift** or **Ctrl** key), then click one of the **Read Summary**, **Read Details** or **Write** buttons according to the access level you wish to assign the ACL.

8. Click the **Done** button to return to the **CSS Service Team Definition** page.

9. You must click the **Save** button at the top of the page to save the ACL details.

**Setting an ACL for an Entity**

To define the access to a specific entity, you must access the entity to which you wish to add an ACL and then use the **Set ACL** button to grant permissions.

In order to use the **Set ACL** buttons, a System Administrator must assign permissions in the v4 Client via Tools | Permissions | User Group Processes | Main Business Process – ACL Button Permissions. For more information, see User Group Processes on page 29.

The **Set ACL** button is available in the following areas of One:

- Activity
- Communication Log
- Equipment
- Equipment Loan
- Exclusions
- Early Years Service Provision
- Early Years Service Level Agreement
- Early Years SLA Base Link
- ICS Adoption Case Note
- ICS Adoption Placement
- ICS Case Note
- ICS Form Definition
- ICS Form Instance
- ICS Fostering Case Note
- ICS Person
- Involvements
- Person Details
- Provision
- Risks
- SEN Returns
- Service Teams Administration

To set an ACL complete the following procedure:

1. Select one of the areas above where the **Set ACL** button is displayed.
2. Click the Set ACL button to display the Access Control List Definition dialog.

3. On the ACL Editor panel, enter a Description for the ACL. The description displays when a user, who is not permitted to do so, attempts to access the ACL record. For example: Access Denied. Please see your System Administrator.

4. Select the Favour Allow or Favour Deny radio button to set the Access Priority.

5. On the ACL Membership panel, click one of the buttons to select the membership:
   - **Users** – displays the User Selector dialog; defined in v3 via Tools | System Administration | Users.
   - **Posts** – displays the Post Browser dialog; defined in v4 via Tools | Team Structure | Posts.
   - **Groups** – displays the Group Selector dialog; defined in v3 via Tools | System Administration | Groups.
   - **Service Teams** – displays the CSS Service Teams dialog; defined in v4 via Focus | Services | CSS Service Teams Administration.

6. If required, use the Show and with drop-downs to filter the membership lists.

7. Highlight a row (you can highlight more than one row at a time, by holding down the Shift or Ctrl key), then click one of the Read Summary, Read Details or Write buttons according to the access level you wish to assign the ACL.

8. Click the Done button to return to the main screen.

9. To save the Access Control List, you must click the Save button on the screen from which you launched the ACL.
Data Panels

Introduction
The Data Panels functionality gives the System Administrator the ability to hide panels that are used infrequently. It is not strictly a security measure, but it can be used to restrict access to panels that show sensitive data.

In order to use the Data Panels buttons, a System Administrator must assign Read, Read-Write, Read-Write-Delete permissions in the v4 Client via Tools | Permissions | User Group Processes | Main Business Process – Administration. For more information, see User Group Processes on page 29.

Using the Data Panels Button
The View/Hide Data Panels button is available in many areas of One v4 Client. It enables you to hide panels that may contain sensitive data from specified groups.

To view or hide data panels:
1. Click the Data Panels button to display the View/Hide Data Panels dialog.
2. On the Select a Group panel, enter at least one letter in the Looking For field.
3. Select the Search By option to display the group list; the list is ordered according to the Search By criteria.
4. Highlight a group to display the existing Data Panels and their permissions. The default for all panels is View.
5. Select the panel number that is to be hidden; you can only hide one panel at a time.
6. Click the **Hide** button. If a panel is a repeating panel, e.g. **Details of Main Carer**, then all instances are hidden.

7. Repeat steps 5 and 6 until all the required panels have been selected.

8. Click the **Save** button.

9. Click the cross at the top of the dialog to return to the main screen.
09 | Appendix

Reference Material

The following documents, referenced in this handbook, can be found on the One Publications website (www.onepublications.com).

V4 Linked Reports Handbook
One System Handbook
Permissions Changes and Additions

Reference Guides (v4 Client)

The following reference guides are available from the One Publications website (www.onepublications.com) and also via My Account, to help you with the v4 System processes:

RG_Permissions_Report Permissions
RG_Permissions_User Group Permissions
RG_Permissions_User Group Processes

Reference Guides (v4 Online)

The following reference guides are available from the One Publications website (www.onepublications.com) and also via My Account, to help you with the v4 System processes:

RG_Online_Administration_Login_Logout
RG_Online_Common_Reports
RG_Permissions_Report Permissions
RG_Permissions_User Group Permissions
RG_Permissions_User Group Processes
Index

Access Control Lists ............................................................ 42
Account Locking ............................................................ 19, 20
ACLs ................................................................. 42
Access Levels ............................................................ 42
Access Priority ............................................................ 43
ACL Button ............................................................. 45
ACL Defaults ............................................................ 44
Favour Allow ............................................................. 43
Favour Deny ............................................................. 43
Setting an ACL .......................................................... 45
Appendix
Reference Guides (v4 Client) ................................................... 49
Reference Guides (v4 Online) ............................................... 49
Reference Material ....................................................... 49
Creating a Group .......................................................... 24
Creating a User ............................................................ 5
Choosing a Dataset .......................................................... 8
Choosing a Group .......................................................... 7
Mapping a User ........................................................... 6
Data Items ................................................................. 33
Data Items (All Secured) ..................................................... 35
Data Panels ................................................................. 47
Data Panels Button .......................................................... 47
Introduction ................................................................. 47
Data Panels Button ........................................................... 47
Introduction ................................................................. 1
Managing Groups
Adding Users to a Group ..................................................... 24
Creating a Group .......................................................... 24
Introduction ................................................................. 24, 26
Managing Permissions
ACLS ................................................................. 42
Data Panels ................................................................. 47
Permissions ................................................................. 29
Report Permissions .......................................................... 37
User Group Permissions ..................................................... 33
User Group Processes ....................................................... 29
Managing Users
Creating a User ............................................................ 5
Introduction ................................................................. 5, 10
Mappings ................................................................. 6
Signature ................................................................. 7
Mapping a User ........................................................... 6
Overview ................................................................. 1
v3 Client ................................................................. 1
v4 Client ................................................................. 1
v4 Online ................................................................. 2
Passwords ................................................................. 17
Account Locking ........................................................... 19, 20
Changing a Password ....................................................... 20
Changing a Password in v3 Client ........................................ 20
Changing a Password in v4 Client ........................................ 20
Changing a Password in v4 Online ...................................... 20
Password Expiry .......................................................... 17
Permissions ................................................................. 29
Assigning Read and Read/Write Permissions
.................................................................................. 37
Assigning Read Permissions ................................................... 35
Assigning Read/Write Permissions ........................................... 36
Interdependencies ............................................................ 32
Invalid Requests ............................................................. 32
Permit/Deny Permissions ..................................................... 31, 34
Report Permissions .......................................................... 37
User Group Permissions ..................................................... 33
User Group Processes ....................................................... 29
Permit/Deny Permissions ..................................................... 34
Reference Guides ........................................................... 3
My Account ................................................................. 3
Reference Guides (v4 Client) ................................................... 49
Reference Guides (v4 Online) ................................................... 49
Reference Material .......................................................... 49
Report Permissions .......................................................... 37
Assigning Permissions - Business Processes
.................................................................................. 38
Assigning Permissions - Report Definition
Repository ................................................................. 38
Signature ................................................................. 7
User Group Processes
Assigning Permissions via a Business Process
.................................................................................. 30
User Group Permissions ..................................................... 33
All Secured Data Items ...................................................... 35
All Secured Menu Links ..................................................... 33
All Secured Menu Routes ..................................................... 33
All Secured Services ......................................................... 33
Assigning Permissions ...................................................... 33
User Group Processes ....................................................... 29
Using this Handbook .......................................................... 3
V3 Client ................................................................. 1
V4 Client ................................................................. 1
V4 Online ................................................................. 2
System Managing Users, Groups & Permissions Handbook