oneeducation

System Common Functionality (v4 Client)

last updated for the Spring 2016 release

CAPITA

Revision History

Version	Published on
Spring 2016 (3.59) - 1.0	12/04/2016

Doc Ref

System Common Functionality (v4 Client) Handbook/Spring 2016/2016-04-12

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.

Contents

01 | System (v4 Client) - Common Functionality

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.

Some of these processes and functions are shared between the One modules in both v4 Client and v4 Online.

The *One System (v4 Online) Common Functionality* handbook is available on the **One Publications** website (www.onepublications.com) to assist you with the following common processes in v4 Online:

- Alerts
- Linked Documents
- Memo
- Reports Manager
- SQL Mail Merge
- UDF Manager.

Using this Handbook

This handbook is intended for One Administrators and users of the One v4 Client system. It details the processes that are common to many of the modules in the v4 Client.

A number of reference guides have been produced to assist you with the processes in One. This handbook explains, in more details, the common processes described in the reference guides.

The following common functionality in the v4 Client is described in this handbook:

- Access Control List
- Alerts
- Data Panels
- Linked Documents
- Linked Reports
- Memo
- Quick Reports
- SQL Mail Merge
- UDF Manager.

Additional Resources:

The *One System (v4 Online) Common Functionality* handbook is available on My Account and on the **One Publications** website (www.onepublications.com) to assist you with the common processes in v4 Online.

Reference Guides

A number of reference guides have been produced to assist you with the processes in One v4 Client. Where a reference guide is available, it is displayed as an additional resource.

> **Additional Resources:**
>
> *RG_Equipment* available on <u>My Account</u> and the **One Publications** website (www.one publications.com).

My Account

The *One Reference Guides* document is available in the **Sticky Items** section of the **<u>My Account</u>** 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). Click on the **Resource No.** link to view the latest version of the reference guide.

To access the reference guides via My Account:

1. Select the **Knowledge Base** tab to display the **Knowledge Base | Popular Searches** page.

2. Select the **Sticky Items** link to display the **Search Results** page. The *One Reference Guides* document is available in the **Documents** list.

> **NOTE:** *Please ensure you are always working from the latest version.*

All of the reference guides are available on My Account. Enter the Resource_ID number in the **Search** box to view a reference guide.

One Publications

The reference guides are also available on the **One Publications** website (www.onepublications.com). Each release is given a different number to enable you to access the website. The number is available in the Release Notes document that is posted with each new release.

To access the reference guides via **One Publications**:

1. Open the latest version of the **One Publications** website (www.onepublications.com/<*123456*/>) to display the **Documentation Centre** page.

2. Select the **Reference Guides** tab to display the list of One modules.

3. Click the **One Reference Guides** link to display the *One Reference Guides* list. This document contains the names of all the reference guides, with their Resource_ID for My Account.

4. Select a module to display the latest version of all related reference guides.

02 | **One v4 Client**

Common Functionality in One v4 Client

There are a number of common functions in One v4 Client:

- Access Control List
- Alerts
- Data Panels
- Linked Documents
- Linked Reports
- Memo
- Quick Reports
- SQL Mail Merge
- UDF Manager.

Access Control List (ACL)

Access Control Lists (ACLs) can be set for B2B:Student, Person Details, Communication Log, Activities, Provision, Equipment, Exclusions, Involvements, Risks, Early Years Maintain Provider, SEN2 Returns, Service Level Agreements (SLAs), Adoption, Fostering, Case Notes and Provision.

Default ACLs can also be applied to service teams via **Focus | Services | CSS Service Team Administration**. ACLs defined for a service team are inherited by all associated entities (e.g. involvements). If a service team's default ACL is updated, then the new ACL cascades to all involvements and related communication log items, unless the ACL has been customised locally at record level.

The following three levels of access can be applied:

- Read Summary
- Read Details
- Write.

Additional Resources:

RG_ACL_ACL Definition available on <u>My Account</u> and the **One Publications** website (www.one publications.com).

Setting Access Control Lists (ACLs)

To set an ACL for a user:

1. In the v4 Client, select an area you wish to set the ACL, e.g. **Person Details**.
2. Click the **Set ACL** button to display the **Access Control List Definition** dialog.

3. On the **ACL Editor** panel, enter a **Description**.

4. Set the **Access Priority** to **Favour Deny** or **Favour Allow** (default).

   This dictates access rights, either downgrading or upgrading a user's permissions depending on which group or post the user is logged on as. For example:
   **Favour Deny**: If user A is a social worker and has been granted individual access to an area but the post of social worker has been denied access, user A as a social worker is denied access.
   Favour Allow: If user A is a social worker and has been denied individual access to an area but the role of social worker has been granted access, user A as a social worker is allowed access.

   For more information, see *Access Priority* on page 6.

5. On the **ACL Membership** panel, click the **Users**, **Posts**, **Groups** and **Service Teams** buttons to select your membership from the related browse.

   The person creating the ACL is automatically given full access to the ACL.
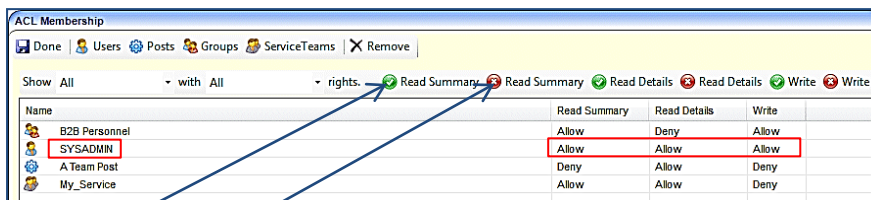
6. Select Allow or Deny access for each type of membership. Each access level must be applied separately. The following access levels are applied:

   - To allow **Read Summary**, **Read Details** and **Write** gives full access to the data.

   - To allow **Read Summary** and **Read Details** but deny **Write** access, gives read-only access to the data, but prevents editing.

   - To deny **Read Summary** denies access to any **Summary** pages, e.g. provision or involvements.

   - To deny **Read Summary** and **Read Details** access but allow **Write**, denies the user access to view the data, but enables the data to be updated at system level.

7. When all members have been granted the required ACL, click the **Done** button to return to the previous page.

8. Click the **Save** button on the focus page where you are setting up the ACL.

> **Additional Resources:**
>
> *RG_ACL_ACL Definition* available on My Account and the **One Publications** website (www.one publications.com).

Setting Default Access Control Lists (ACLs)

To set a default ACL for a service team:

1. Select **Focus | Services | CSS Service Team Administration | Service Team** to display the **CSS Service Team Definition [<*Service Team*>]** 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**.

4. Set the **Access Priority** to **Favour Deny** or **Favour Allow** (default).

   This dictates access rights, either downgrading or upgrading a service team's permissions. For example:
   Favour Allow – any allow permissions allow access.
   Favour Deny – any deny permissions prevent access.

   For more information, see *Access Priority* on page 6.

5. On the **ACL Membership** panel, click the **Service Teams** button to select your membership from the **CSS Service Teams** browse.

   If required, individual users, posts and groups can be added to the service team membership.

   The person creating the ACL is automatically given full access to the ACL.
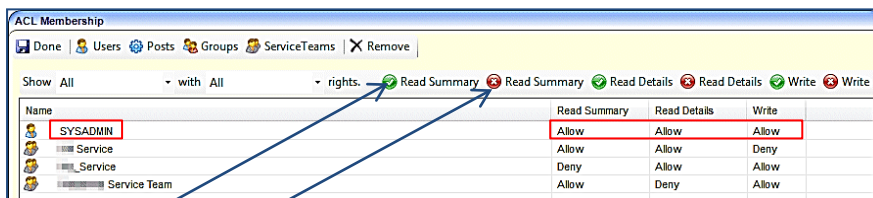
6. Select Allow or Deny access for each service team. Each access level must be applied separately. The following access levels are applied:

   - To allow **Read Summary**, **Read Details** and **Write** gives full access to the data.

   - To allow **Read Summary** and **Read Details** but deny **Write** access, gives read-only access to the data, but prevents editing.

   - To deny **Read Summary** denies access to any **Summary** pages, e.g. provision or involvements.

   - To deny **Read Summary** and **Read Details** access but allow **Write**, denies the user access to view the data, but enables the data to be updated at system level.

7. When all service teams have been granted the required ACL, click the **Done** button to return to the previous page.

8. Click the **Save** button on the focus page where you are setting up the ACL Defaults.

> **Additional Resources:**
>
> *RG_ACL_ACL Definition* available on My Account and the **One Publications** website (www.one publications.com).

Access Priority

Access priorities are **Favour Deny** or **Favour Allow**. These dictate the access rights, either downgrading or upgrading a user's permissions, depending upon which group or post the user is logging on as. **Favour Allow** is the default selection. The following scenarios are based on access to a person record.

Favour Allow

Logon ID	Summary	Read	Write	Access for the User
Group/Post User	✗ ✓	✗ ✓	✗ ✓	The user is allowed full access to the record.
Group/Post User	✓ ✗	✓ ✓	✓ ✗	The user is allowed full access to the record.
Group/Post User	✓ ✗	✓ ✗	✗ ✗	The user has read-only access.
Group/Post User	✗ ✗	✗ ✓	✗ ✓	The record is not available for selection.

Favour Deny

Group/Post User	✓ ✗	✓ ✗	✓ ✗	The record is not available for selection.
Group/Post User	✓ ✗	✓ ✓	✓ ✗	The record is not available for selection.
Group/Post User	✓ ✓	✓ ✓	✗ ✗	The user has read-only access. If read access is also denied, a message is displayed denying access to the record.

Alerts

Alerts are created to advise or warn users of changes in field values within a record.

In the case of the death of a person (child, student or adult), One <u>automatically</u> generates a system warning that <u>displays on the person's record</u>.

A number of predefined alerts are included in the One installation. Predefined alerts are <u>always</u> active and <u>cannot</u> be edited or deleted.

There are three types of alerts:

- ■Trigger alerts are created where data is persistent, such as a base closure or the death of a student. The trigger fires every time a user accesses the record.

- ■SQL alerts are created on the basis of a user enquiry to a particular focus, e.g. a user may select an option to view the details of a student.

- ■Scheduled alerts set a date, time and frequency when an alert will be executed.

These alerts are displayed as an email, a pop-up message or a workflow message on the system administrator's **My Home Page**.

An **Alerts** button is available in many areas of One v4 Client. This enables you to store alerts against individual records. These alerts create a pop-up message each time the record is accessed.

> **Additional Resources:**
>
> *RG_Administration_System Alerts*
> *RG_Administration_Creating Trigger Alerts*
> *RG_Administration_Creating SQL Alerts*
> *RG_Administration_Creating Scheduled Alerts*
> available on My Account and the **One Publications** website (www.one publications.com).

Trigger Alerts

Trigger alerts are created if the data is persistent, such as a base closure or the death of a student. The trigger fires every time a user accesses the record.

Trigger alerts work on changes to nominated database tables and fields. The generic term for this type of alert is a *database trigger*. A trigger alert is based on Field Selection or SQL. This type of alert cannot operate on a list of fields and a free form SQL statement at the same time. Retrospective Action can also be applied to a trigger alert.

For more information, see the following sections:

A trigger alert must have a recipient added before it can be activated. For more information, see

A trigger alert must have an action defined before it can be activated. For more information, see

A saved alert will not work until it is activated. For more information, see

> **Additional Resources:**
>
> *RG_Administration_Creating Trigger Alerts* available on My Account and the **One Publications** website (www.one publications.com).

Creating a Trigger Alert Using Field Selection

A trigger alert can be created using field selection. This type of alert cannot operate on a list of fields and a free form SQL statement at the same time.

To create a new trigger alert using field selection:

1. Select **Tools | Administration | Alert Definition** to display the **Maintain Alert** page.

2. Click the **New** button to display the **Alert Definition [New Alert Definition]** page. The **Alert Definition ID** is a system generated number that is automatically populated.

3. Select the **Trigger Alert Type**. Selecting a trigger alert deactivates the **SQL Alert** panel and the **Scheduled Alert** panel.

4. Enter a **Reason for Alert**.

5. Enter a **Description**.

    An alert cannot be made active until it has been saved.

    You cannot create a predefined alert; they are included in the One installation.

6. On the **Trigger Alert** panel, select an **Alert Based On** context. The **Database Trigger** and the table name are automatically populated.

7. Select the **Field Selection** tab to display all of the fields according to the context selected in **Alert Based On**.

8. Select the check boxes of the fields to be the subject of the alert. You can **Select All** or **De-Select All**. If more than one field is selected, the alert will trigger only when <u>all</u> conditions are true. If you want the alert to trigger when any <u>one</u> of the conditions is true, you must create separate alerts.

9. If required, specify the parameters for **Only When Changed From** and **Only When Changed To**, e.g. **From** *True* **To** *False*.

    You can view the SQL that One generates for this trigger via the **View Trigger SQL** panel.

10. Click the **Save** button. The alert cannot be activated until a recipient has been added and an action has been defined.

> **More Information:**
>
> *Adding a Recipient* on page *14*.
> *Defining an Action* on page *18*.

Creating a Trigger Alert Using SQL

> **Important Note:** If an SQL script is used in an alert, this should only be carried out by a system administrator who is fully aware of its implications. Capita cannot accept responsibility for data problems caused as a result of not following this advice.

A trigger alert can be created using SQL. This type of alert cannot operate on a free form SQL statement and a list of fields at the same time.

To create a new trigger alert using SQL:

1. Select **Tools | Administration | Alert Definition** to display the **Maintain Alert** page.
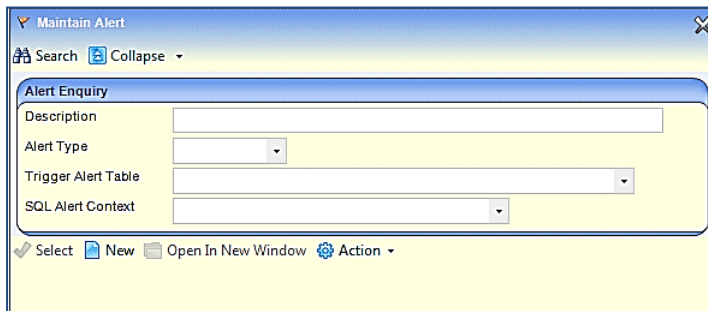
2. Click the **New** button to display the **Alert Definition [New Alert Definition]** page. The **Alert Definition ID** is a system generated number that is automatically populated.

3. Select the **Trigger Alert Type**. Selecting a trigger alert deactivates the **SQL Alert** panel and the **Scheduled Alert** panel.
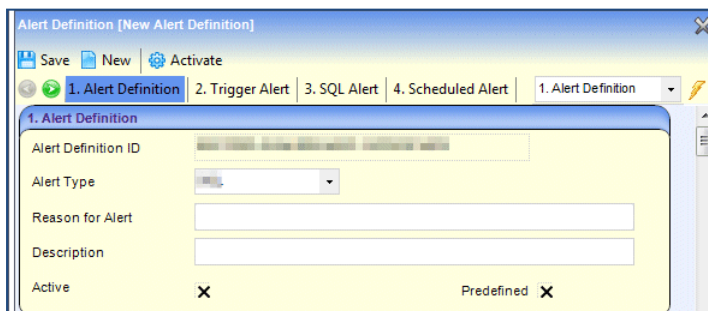
4. Enter a **Reason for Alert**.

5. Enter a **Description**.

   An alert cannot be made active until it has been saved.

   You cannot create a predefined alert; they are included in the One installation.

6. On the **Trigger Alert** panel, select an **Alert Based On** context. The **Database Trigger** and the table name are automatically populated.

7. Select the **SQL** tab to display information on how to write the SQL.

8. Enter the SQL. This can only be a `Select` statement.

9. Click the **Verify SQL** button. If the SQL statement is correct, the following message displays at the bottom of the screen: *SQL is valid*.

   To view the SQL that will be generated by One for the trigger, scroll down to the **View Trigger SQL** panel and click the **View Trigger SQL button**.
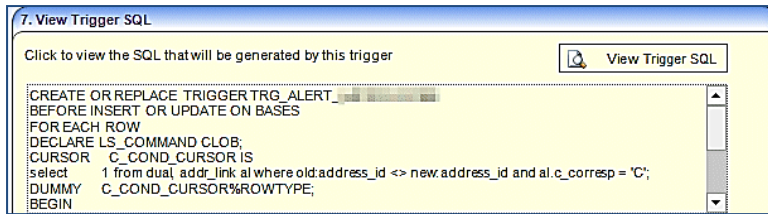
10. Click the **Save** button. The alert cannot be activated until a recipient has been added and an action has been defined.

    > **More Information:**
    >
    > *Adding a Recipient* on page *14*.
    > *Defining an Action* on page *18*.

Creating a Trigger Alert Using Retrospective Action

Retrospective action can be used with field selection <u>and</u> SQL. However, it <u>cannot</u> operate on a list of fields and a free form SQL statement at the same time. Retrospective action is only applied when the alert is activated.

To create an alert using retrospective action:

1. After the trigger alert has been created using field selection <u>or</u> SQL, select the **Retrospective Action** tab. **Alert Based On**, **Database Trigger** and the table name are automatically populated.
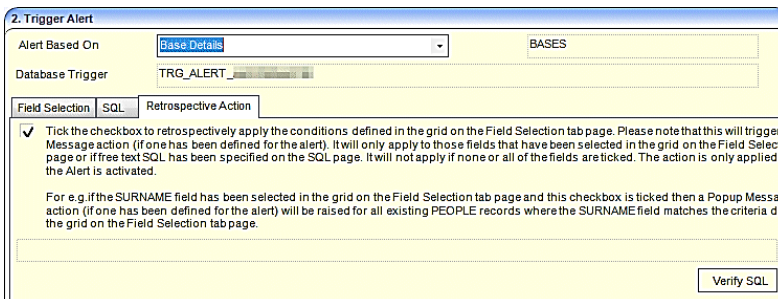
2. Select the check box to retrospectively apply the conditions defined on the **Field Selection** tab or the **SQL** tab.

3. Click the **Verify SQL** button. If the SQL statement is correct, the following message displays at the bottom of the screen: *Retrospective SQL is valid*.

   If you wish, you can view the SQL that One generates for this trigger via the **View Trigger SQL** panel.
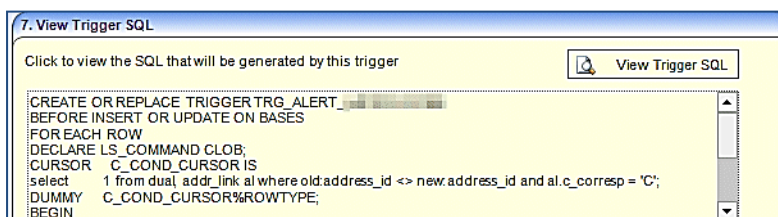

4. Click the **Save** button.

SQL Alerts

> **Important Note:** If an SQL script is used in an alert, this should only be carried out by a system administrator, who is fully aware of its implications. Capita cannot accept responsibility for data problems caused as a result of not following this advice.

SQL alerts are created and initiated on the basis of a user enquiry to a particular focus. For example, the user may select an option to view the details of a student. As a result of this enquiry, an SQL statement is run against the database.

An SQL alert must have a recipient added before it can be activated. For more information, see *Adding a Recipient* on page *14*.

An SQL alert must have an action defined before it can be activated. For more information, see *Defining an Action* on page *18*.

A saved alert will not work until it is activated. For more information, see *Activating an Alert* on page *20*.

> **Additional Resources:**
>
> *RG_Administration_Creating SQL Alerts* available on My Account and the **One Publications** website (www.one publications.com).

Creating an SQL Alert

To create a new SQL alert:

1. Select **Tools | Administration | Alert Definition** to display the **Maintain Alert** page.
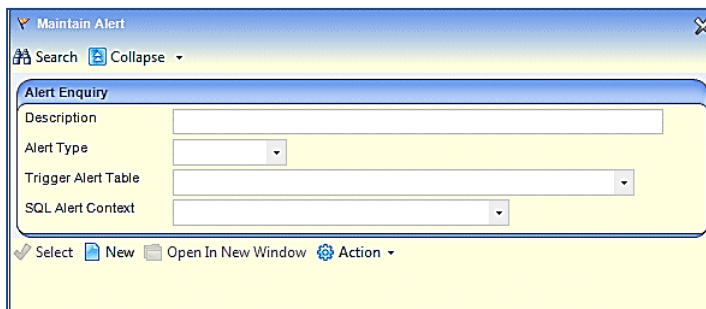
2. Click the **New** button to display the **Alert Definition [New Alert Definition]** page. The **Alert Definition ID** is a system generated number that is automatically populated.

3. Select the **SQL Alert Type**. Selecting an SQL alert deactivates the **Trigger Alert** panel and the **Scheduled Alert** panel.
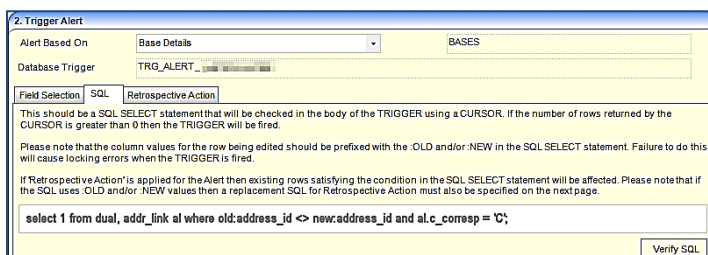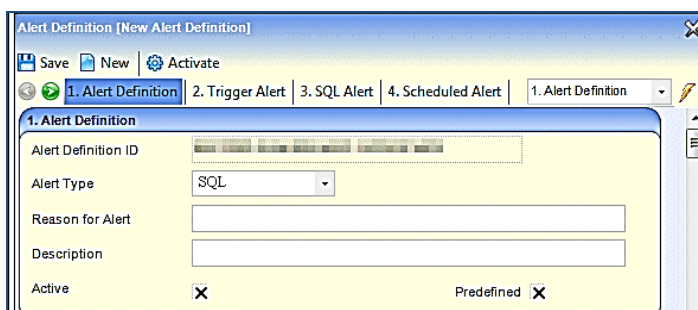

4. Enter a **Reason for Alert**.

5. Enter a **Description**.

An alert cannot be made active until it has been saved.

You cannot create a predefined alert; they are included in the One installation.

6. On the **SQL Alert** panel, select a **Context** for the alert to be based on. The number of associated alerts is displayed.
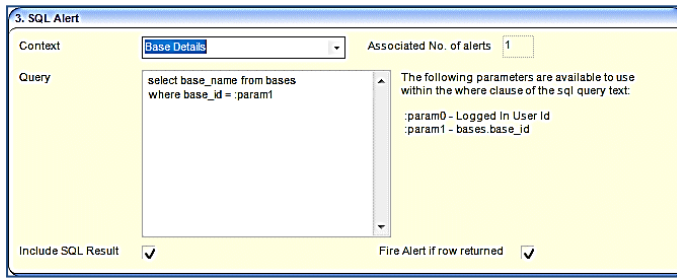
7. Enter the SQL **Query**. This can only be a `Select` statement. A number of parameters are available to use within the where clause of the SQL query text. For more information, see *Rules for Creating SQL Statements for SQL Alerts* on page *12*.

8. If required, select **Include SQL Result** to enable repetition of the SQL message in the output.

9. If required, select **Fire Alert if Row Returned** to fire a message regardless of the values returned.

10. Click the **Save** button. The alert cannot be activated until a recipient has been added and an action has been defined.

> **More Information:**
>
> *Adding a Recipient* on page *14*.
> *Defining an Action* on page *18*.

Rules for Creating SQL Statements for SQL Alerts

When adding a query on the **SQL Alert** panel, the following general rules apply:

- Any statement that does not begin with the word `Select` (including any comment markers) is treated as invalid.
- A comment must be entered as: */* … */* or **- -** (two minus characters), but is invalid if placed on the first line.
- A second statement inserted by the use of a semi-colon is ignored, although the statement may be interpreted as valid.
- The user may use parameters; these are values that One understands based on the user's focus. These parameters are made available via the **Context** selected and must adhere to the convention: :param*n* where *n* is the relevant number.
- One displays an error message if the number of the parameter value exceeds the numbers of parameters available within the context. For example, `:param3` where there are only two parameters available.
- It is only possible to retrieve a parameter when it is placed in the `Where` clause of the SQL statement.
- It is possible to create sub-selects (SQL statement where a `Select` statement exists in the `Where` clause).
- One does not save any invalid SQL statements. The user must correct the statement or abandon it.

Where an SQL Query is not validated by One, the following Oracle error message is displayed at the bottom of the page: ORA-00942: table or view does not exist.

Scheduled Alerts

Important Note: If an SQL script is used in an alert, this should only be carried out by a system administrator, who is fully aware of its implications. Capita cannot accept responsibility for data problems caused as a result of not following this advice.

The scheduled alert functionality is linked to the configuration tool which determines the frequency of checking for background tasks, e.g. the job scheduler. The **Frequency of Checking Background Tasks** field is set via the CCS Enterprise Server Configuration Utility; this should be set lower than the scheduled alert frequency. For more information, see *V4 Scheduled Tasks* technical guide available on the One Publications website *(*www.onepublications.com*)*.

Scheduled alerts set a date, time and frequency when an alert is to be executed. It is <u>not</u> possible to schedule pop-up messages or to include parameters in the **SQL Query** field of a scheduled alert.

A scheduled alert must have a recipient added before it can be activated. For more information, see *Adding a Recipient* on page *14*.

A scheduled alert must have an action defined before it can be activated. For more information, see *Defining an Action* on page *18*.

A saved alert will not work until it is activated. For more information, see *Activating an Alert* on page *20*.

Additional Resources:

RG_Administration_Creating Scheduled Alerts available on My Account and the **One Publications** website (www.onepublications.com).

Creating a Scheduled Alert

To create a new scheduled alert:

1. Select **Tools | Administration | Alert Definition** to display the **Maintain Alert** page.
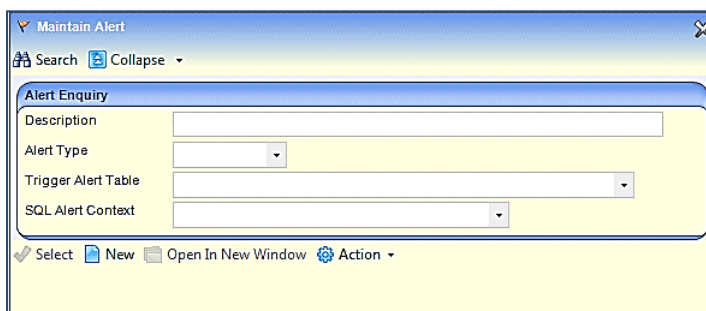
2. Click the **New** button to display the **Alert Definition [New Alert Definition]** page. The **Alert Definition ID** is a system generated number that is automatically populated.
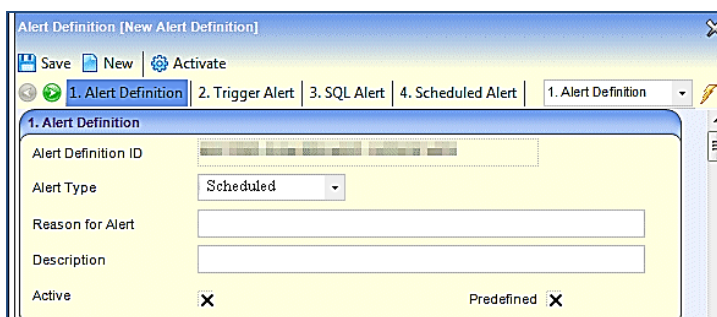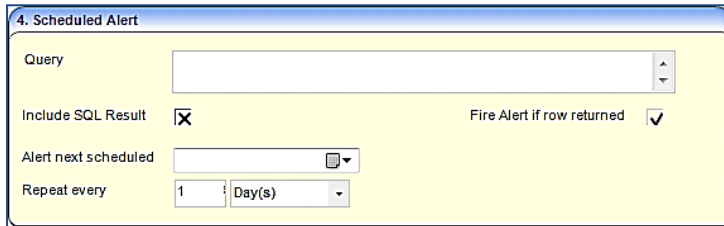
3. Select **Scheduled Alert Type**. Selecting a scheduled alert deactivates the **Trigger Alert** panel and the **SQL Alert** panel.

4. Enter a **Reason for Alert**.

5. Enter a **Description**.

    An alert cannot be made active until it has been saved.

    You cannot create a predefined alert; they are included in the One installation.

6. On the **Scheduled Alert** panel enter the SQL **Query**. This can only be a `Select` statement. You cannot include parameters in the SQL **Query**. For more information, see *Rules for Creating SQL Statements for Scheduled Alerts* on page *14*.

7. If required, select **Include SQL Result** to enable repetition of the SQL message in the output.

8. If required, select **Fire Alert if Row Returned** to fire a message regardless of the values returned.

9. Enter the date and time for **Alert next scheduled**.

10. Enter a number to **Repeat every** Minute(s), Hour(s), Day(s), Week(s) or Month(s).

11. Click the **Save** button.

Rules for Creating SQL Statements for Scheduled Alerts

When adding a query on the **Scheduled Alert** panel, the following general rules apply:

- Any statement that does not begin with the word `Select` (including any comment markers) is treated as invalid.

- A comment must be entered as: */* … */* or **--** (two minus characters), but is invalid if placed on the first line.

- A second statement inserted by the use of a semi-colon is ignored, although the statement may be interpreted as valid.

- It is possible to create sub-selects (SQL statement where a `Select` statement exists in the `Where` clause).

- One does not save any invalid SQL statements. The user must correct the statement or abandon it.

Where an SQL query is not validated by One, the following Oracle error message is displayed at the bottom of the page:

    ORA-00942: table or view does not exist.

Adding a Recipient

All alerts must have at least one recipient. The recipient type and the mechanisms for delivering an alert (email, pop-up or workflow) are defined on the **Recipient List** panel. The type of recipient determines the action type.

The action type (email, pop-up or workflow) must correspond with the action type selected on the **Action** panel. For more information, *Defining an Action* on page *18*.

It is not possible to assign all actions to all recipients. In some instances, the button to add a recipient type is disabled as the action type options are restricted. The following recipient types can be added to an alert:

- Users
- Groups
- People
- Bases
- Posts
- Query
- Email.

The recipient list <u>cannot</u> be saved until at least one action has been defined.

A **Remove** button is available to make any changes to the recipient list.

More Information:

Adding Users on page *15.*
Adding Groups on page *15.*
Adding People on page *16.*
Adding Bases on page *16.*
Adding Posts on page *17.*
Adding Queries on page *17.*
Adding Emails on page *18.*

Adding Users

To add a user to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add Users** button to display the **User Browser** dialog.
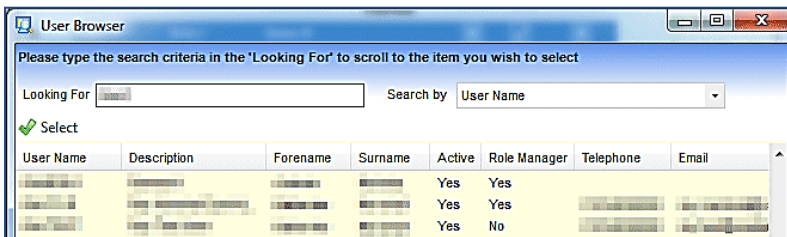
3. Highlight the required user and click the **Select** button to add the user to the **Recipient List** panel. Use the **Ctrl** key to select multiple users.

4. Select the required check boxes to send the alert by **Email**, **Pop-up** or **Workflow**. You can select all three options.

Adding Groups

To add a group to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add Groups** button to display the **Select a Group** dialog.

3. Highlight the required group and click the **Select** button to add the group to the **Recipient List** panel. Use the **Ctrl** key to select multiple groups.
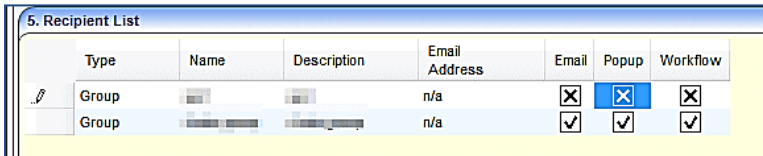
4. Select the required check boxes to send the alert by **Email**, **Pop-up** or **Workflow**. You can select all three options.

Adding People

To add people to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add People** button to display the **Person Enquiry** dialog.
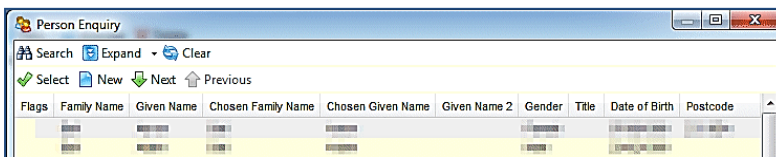
3. Highlight the required person and click the **Select** button to add the person to the **Recipient List** panel. Use the **Ctrl** key to select multiple people.

You can only send an alert to a person by **Email**. Therefore, the **Email** check box is automatically selected and cannot be changed.

Adding Bases

To add a base to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add Bases** button to display the **Base Enquiry** dialog.

3. Highlight the required base and click the **Select** button to add the base to the **Recipient List** panel. Use the **Ctrl** key to select multiple bases.

You can only send an alert to a base by **Email**. Therefore, the **Email** check box is automatically selected and cannot be changed.
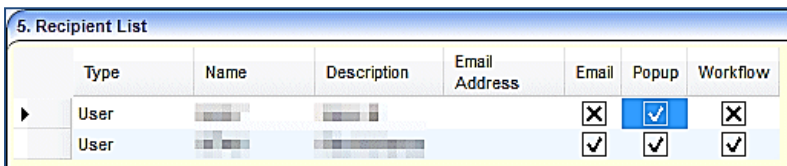
Adding Posts

To add a post to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add Posts** button to display the **Post Browser** dialog.

3. Highlight the required post and click the **Select** button to add the post to the **Recipient List** panel. Use the **Ctrl** key to select multiple posts.
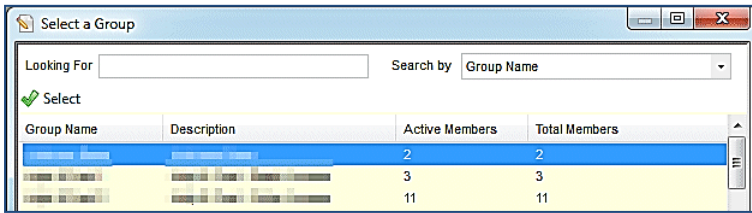

4. Select the required check boxes to send the alert by **Email**, **Pop-up** or **Workflow**. You can select all three options.

Adding Queries

This option is <u>not</u> available for trigger alerts. The correct alert type must be selected and the SQL query <u>must</u> be stated before the **Add by Query** button is activated.

To add a query to the recipient list:

1. On the **Alert Definition** page, select either an SQL or scheduled alert.

2. On the **Recipient List** panel, click the **Add By Query** button to display the **From Query** dialog. One reads the query and displays the fields that can be used.

3. Highlight the required field and click the **Select** button to add the field to the **Recipient List** panel. Use the **Ctrl** key to select multiple fields for the query.

You can only send an alert using a query by **Email**. Therefore, the **Email** check box is automatically selected and cannot be changed.

Adding Emails

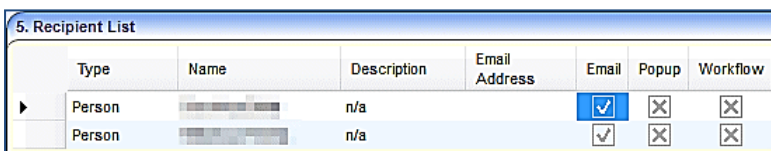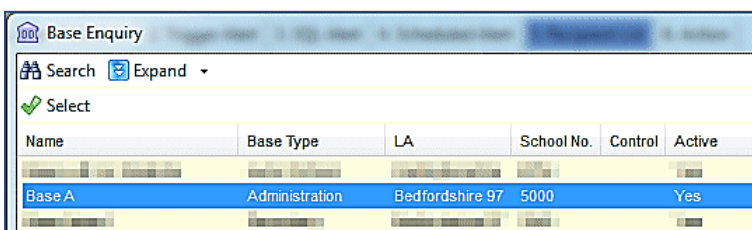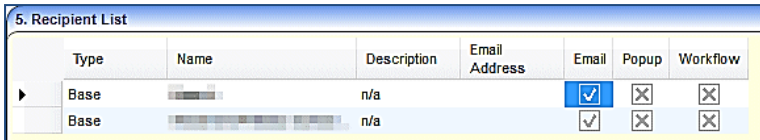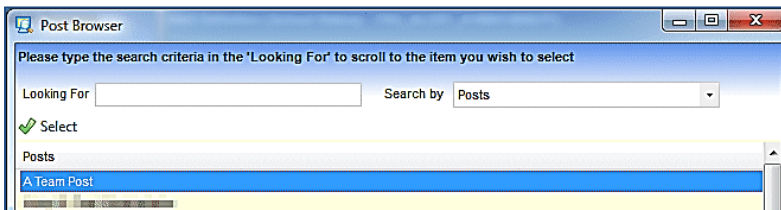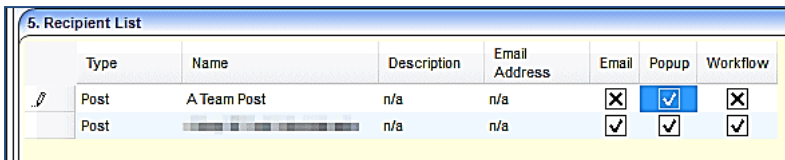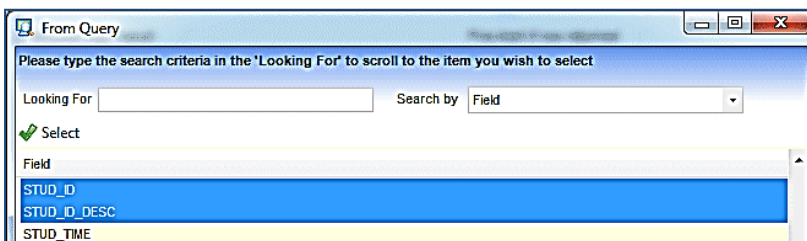To add an email address to the recipient list:

1. On the **Alert Definition** page, select the **Recipient List** panel.

2. Click the **Add Email** button to display the **Add Email Address** dialog.

3. Enter the email address to send the alert to. To add multiple email addresses, separate <u>each</u> email address with a semi colon. You can also use a distribution list.

4. Click the **OK** button to add the email addresses to the **Recipient Lis**t panel.

As this alert is sent by email, the **Email** check box is automatically selected and cannot be changed.

Defining an Action

All alerts must have at least one action defined. The action must correspond with the action selected on the **Recipient List** panel. The actions available for selection in order to transmit the alert depend on the alert type <u>and</u> the recipient type.

It is not possible to assign all actions to all recipients. In some instances, the button to add a recipient type is disabled as the action type options are restricted.

> **More Information:**
>
> *Adding a Recipient* on page *14*.

The following options are available to transmit a message:

- ■**Email** – sends an email to any nominated recipient; a distribution list can be used. The recipients must be added to the recipient list <u>before</u> the alert can be activated. If a recipient is selected as a user and is also part of a group, One dispatches the email once, as the list is filtered to accept distinct values only.

- ■**Pop-up Message** – a pop-up message box displays on the screen when an identified record is accessed. Used where a message is deemed to be relevant for a short period. A pop-up message <u>cannot</u> be used for a scheduled alert.

> **Important Note:**
>
> Upgrades for a main release include instructions to automatically delete all expired pop-up messages in the database. Once deleted One does not retain any record of the message. You may wish to review all pop-up message alerts to determine if any expired messages are to be retained for future use by setting the **Expiry Date** to null.

■**Workflow Message** – a workflow message is transmitted to a specified user. Workflow messages are displayed on the **My Home Page** as a <u>pop-up</u> box.

Before a workflow message alert can be received, a system administrator must enter the details on the **Workflow Server** tab of the Capita Children's Service Enterprise Server Configuration Utility.

> **More Information:**
>
> *Installing and Configuring One v4 Core Components* technical guide available on the **One Publications** website (www.onepublications.com).

> **Important Note:**
>
> Upgrades for a main release include instructions to automatically delete all expired workflow messages in the database. Once deleted, One does not retain any record of the message. You may wish to review <u>all</u> workflow message alerts to determine if any expired messages are to be retained for future use by setting the **Expiry Date** to null.

To define an action:

1. On the **Alert Definition** page, select the **Action** panel.

> To substitute a field into any of the above messages use the syntax @"OLD_Field Name" or @"NEW_Field name" (including the quotation marks) and the value in that field will be substituted into the message.
>
> The old value of the field replaces "OLD_Field Name" and the new value of the field replaces "NEW_Field Name", e.g. The information for @"OLD_Surname" has been updated to @"NEW_Surname" (The information for Smith has been updated to Jones).
> **NOTE**: A field cannot be substituted into a message for SQL Alerts.

The top of the panel gives advice how to use field names in the alert messages.

If you are creating an SQL alert, this can be previewed on the **Action** panel, by selecting a **Preview Action**.
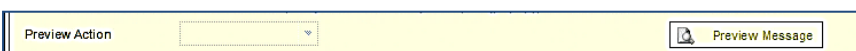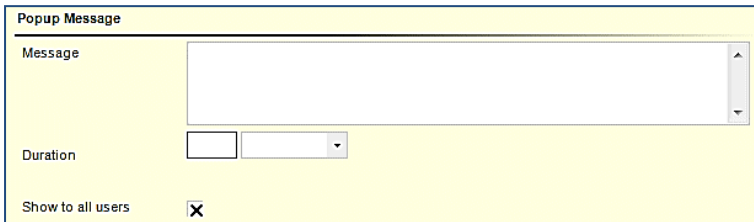
2. Click the **Preview Message** button to display the read-only SQL alert message.

3. To send the alert via email:

e-mail	
Subject	
Message	
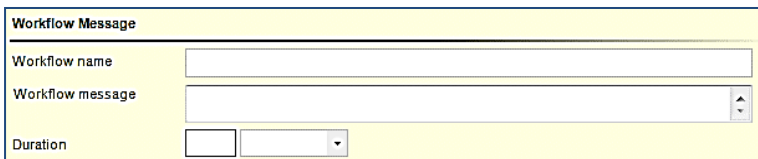
   a. Enter the **Subject** of the email.

   b. Enter the **Message** to be seen by the recipient.

4. To display the alert as a pop-up message:

Popup Message	
Message	
Duration	
Show to all users	☒

   a. Enter the **Message** details to be seen by the recipient.

   b. Define the **Duration** of the alert, i.e. the number of days, weeks, months or years.

   c. If required, select the **Show to all users** check box. Selecting this check box means that you do not need to nominate users or groups in the recipient list.

5. To transmit the email as a workflow message to a specified user:

Workflow Message	
Workflow name	
Workflow message	
Duration	

   a. Enter the **Workflow name**.

   b. Enter the **Workflow message** to be seen by the specified user.

   c. Define the **Duration** of the alert, i.e. the number of days, weeks, months or years.

6. Click the **Save** button. The following message is displayed at the bottom of the screen:

   Do you want to activate the alert?

7. Click the **Yes** button. The **Activate** button changes to **Deactivate**.

> **More Information:**
>

Activating an Alert

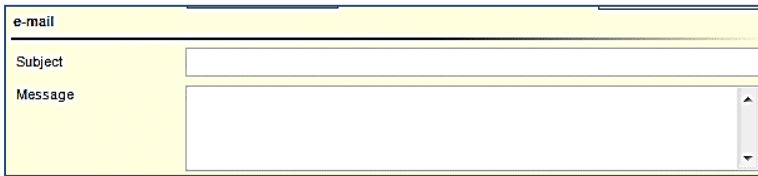Predefined alerts are <u>always</u> active and this status cannot be changed.

An alert can be activated when it is created by entering all mandatory information, selecting the required recipients and defining at least one action. Saving the alert displays the following message:

   Do you want to activate the alert?

Selecting **Yes** activates the alert immediately and the greyed out **Activate** button at the top of the page changes to **Deactivate**.

To activate an existing alert:

1. Select **Tools | Administration | Alert Definition**, then select the alert you wish to activate to display the **Alert Definition** page.

2. Click the **Activate** button; the button changes to **Deactivate**.

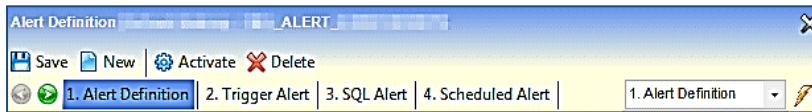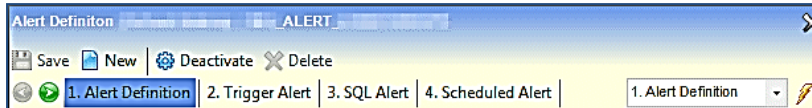The following message displays at the bottom of the page:

Alert activated successfully.

You do not need to save the alert again.

> **Note**: The **Delete** button is now inactive; you <u>must</u> deactivate an alert before you can delete it.

Deactivating an Alert

Predefined alerts <u>cannot</u> be deactivated. Trigger, scheduled or SQL alerts <u>cannot</u> be edited or deleted until the alert has been deactivated.

To deactivate an alert:

1. Select **Tools | Administration | Alert Definition**, then select the alert you wish to deactivate to display the **Alert Definition** page.
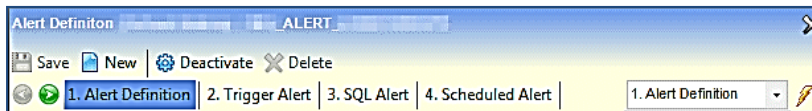
2. Click the **Deactivate** button; the button changes to **Activate**.
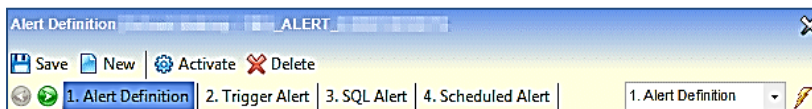
The following message displays at the bottom of the page:

Alert deactivated successfully.

You do not need to save the alert again.

> **Note**: A deactivated alert can be deleted.

Deleting an Alert

Predefined alerts <u>cannot</u> be deleted. Trigger, SQL and scheduled alerts cannot be deleted until they have been deactivated.

To delete an alert:

1. Select **Tools Administration | Alert Definition**, then select an alert from the browse list to display the **Alert Definition** page.

2. Click the **Deactivate** button; the button changes to **Activate**. The following message is displayed at the bottom of the page:

   Alert deactivated successfully.

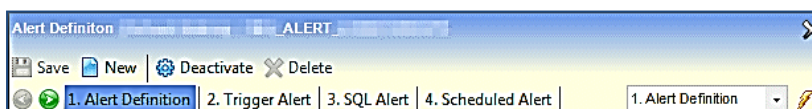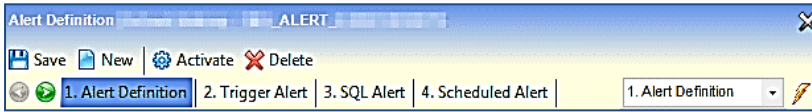3. Click the **Delete** button; the following message displays:
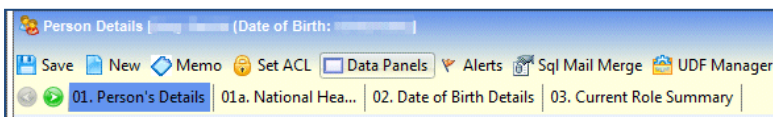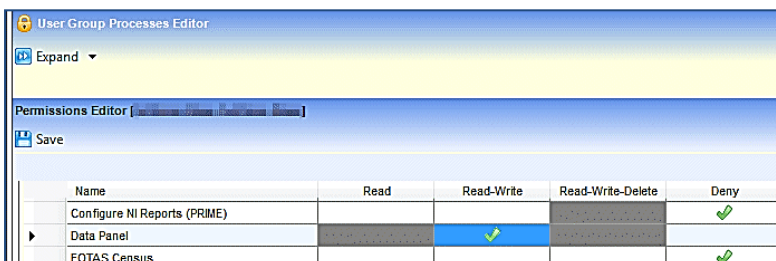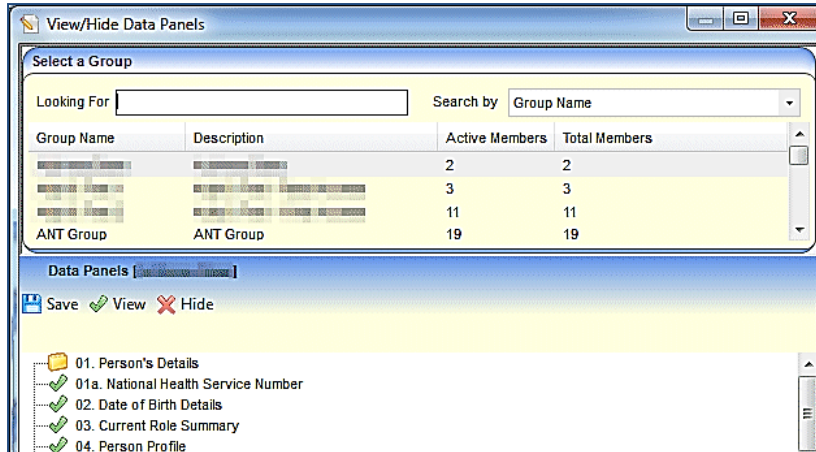
   Are you sure you want to delete this *<Alert>* for the *<Table>*?

4. Click the **Yes** button; the following message is displayed at the bottom of the page:

   Alert *<Name>* for Table *<Name>* is deleted successfully.

Data Panels

The **Data Panels** button is available in many areas of the v4 Client.

Activity Details	CSS Service Team	Exclusions
EY Enquiry	EY Maintain Provider	EY Staff
ICS Person	ICS Service Provider	Involvements
Person Details	Provider	Provision
Relocation	Staff Details	Student Details

Default data panel settings can be applied to the following areas:

- ICS Form Definitions
- Involvement Forms
- Service Teams.

Clicking the **Data Panels** button enables you to hide panels that are not used regularly. It is <u>not</u> a security measure, as data is still delivered to the panel and it is not restricted.

If the group permission for **Data Panel** is set to **Deny**, the functionality <u>can</u> be used to restrict access to sensitive data.

Access to the **Data Panels** button is granted via **Tools | Permissions | User Group Processes User Group Processes Editor | Administration**.

Hiding Data Panels

To hide a data panel:

1. Click the **Data Panels** button to display the **View/Hide Data Panels** dialog. The default setting for all panels is **View**, indicated by a green tick.

2. In the **Select a Group** panel, highlight the required group. If you want to search for a specific group, select the required **Search By** type and the **Looking For** text/number you want to search for.

3. On the **Data Panels [*Group Name*]** panel, highlight a numbered panel and click the **Hide** button. If there are a number of instances of the same panel, e.g. Contact Details, all the panels are hidden.

4. Click the **Save** button to apply the settings.

   When a member of the selected group accesses a record, the hidden panel is not displayed and the **Data Panels** buttons is no longer displayed at the top of the page.

> **Additional Resources:**
>
> *RG_Administration_Data Panels* available on My Account and the **One Publications** website (www.one publications.com).

Unhiding Data Panels

Data panels can be unhidden at any time by a system administrator.

To unhide a data panel:

1. Click the **Data Panels** button to display the **View/Hide Data Panels** dialog. Hidden panels are indicated by a red cross.

2. In the **Select a Group** panel, highlight the required group. If you want to search for a specific group, select the required **Search By** type and the **Looking For** text/number you want to search for.

3. On the **Data Panels [*Group Name*]** panel, highlight a numbered panel that is hidden and click the **View** button. If there are a number of instances of the same panel, e.g. **Contact Details**, all the panels become visible.

4. Click the **Save** button to apply the settings.

Additional Resources:

RG_Common_Data Panels available on My Account and the **One Publications** website (www.one publications.com).

Linked Documents

The **Linked Documents** feature is located on the left hand panel throughout the v4 Client. The panel displays related documents, letters, reports etc. A linked file, for example, could be related to person details, a letter generated from a timeline or a report attached to a communication log.

The maximum size for an uploaded file is 150 MB. If the selected files size is greater than the permitted upload limit, the file can be linked, but it cannot be uploaded and the following message is displayed:

> The file *filename.txt* that you are trying to upload is larger than the maximum permitted size of 150 MB.

Access to the **Linked Documents** panel is granted via **Tools | Permissions | User Group Processes | Administration**.

Adding Linked Documents

To add a new linked document:

1. Select an area to add a new linked document, e.g. Student Details.

2. Click the **New** button to display the **Files Linked** dialog.

3. Enter a **File Description**.

4. Click the **File Name** folder to select a file.

5. Click the **Save** button; the **Linked By**, **Linked Date**, **Update By** and **Last Updated** fields are populated.

   The following message is displayed:

   Do you want to upload the linked document now?

6. Click the **Yes** button to upload the file. After the upload is completed, a message box confirms that the linked file is saved and uploaded. The **Uploaded By** and **Uploaded Date** fields are populated.

7. Close the **Files Linked** dialog. The linked document is displayed in the **Linked Documents** panel.

> **Note:**
> *We recommend that files are linked and uploaded individually.*

Uploaded and opened files are stored in a temporary directory. When you return to the **Files Linked** window, One automatically removes copies of opened and uploaded files from the temporary directory.

> **Important Note:**
> *You must ensure that the file you are uploading is not in use.*

Linked Reports

Linked reports are displayed in the **Links** panel, below the **Reports** section.

These reports are designed and linked into multiple pages within One via **Tools | Permissions | Report Permissions**.

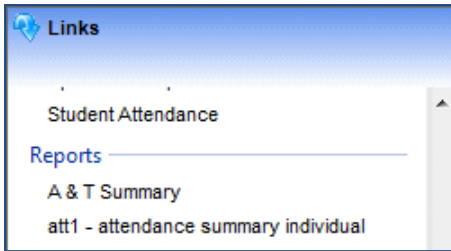When a linked report is processed, One exchanges parameter values to the linked report and validates if the parameter name value exists. If the validation is successful, the report is processed and displayed in the Report Viewer.

> **Additional Resources:**
>
> *RG_Permissions_Report Permissions*
>
> available on My Account and the **One Publications** website (www.onepublications.com).

Using Linked Reports

To run a linked report from the **Links** panel:

1. Select an area to run a new linked report, e.g. Student Details.

2. Select the required report from the **Links | Reports** link. If the parameters do not match, the following dialog displays:

> Report parameter values exist that are not provided by the client.
> Please enter parameter values manually.

3. Click the **OK** button to display the **Provide Parameter Values** dialog.

4. Enter the required values for the parameters.

5. Click the **OK** button to display the report in **Report Viewer**.

Using the Linked Reports Button

The **Linked Reports** button is found in the following modules that are embedded into the v4 Client:

- Hearing Impairment

- Visual Impairment

- Governors.

The **Linked Reports** button enables you to run a report in context of the individual record.

A system administrator must grant report permissions via **Tools | Permissions | User Group Processes | Administration**.

Permissions to run individual reports are granted via **Tools | Permissions | Report Permissions**.

To run a linked report from the **Linked Reports** button:

1. Click the **Linked Reports** button to display the reports browse.

2. From the browse drop-down, select the required report.

3. Click the **Run** button to display the **Report Parameters** dialog.
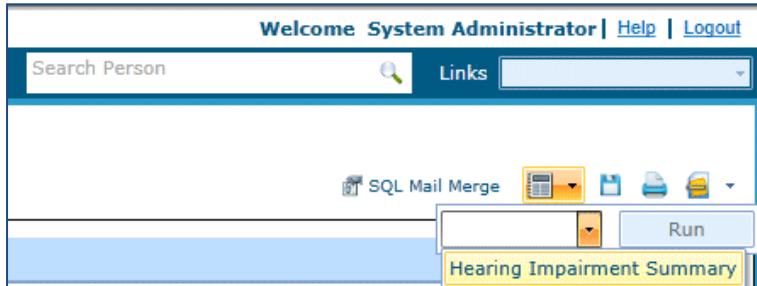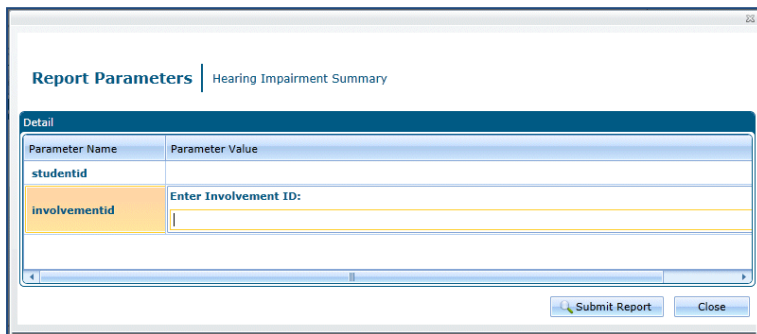

4. Select a **Parameter Value** field and enter the required value.

5. Click the **Submit Report** button. The SAP Crystal report opens in a new browser window.

The toolbar at the top of the report enables you to navigate through the report.

	Click the **Group Tree** button to display the **Group Tree** panel. This panel lists all of the records contained in the report.
	1. Click the **Print Report** button to display the **Print** dialog. 2. Select the required printing options. 3. Click the **Print** button.
	The **Drill Up** button is not used in Capita One Crystal reports.
	1. Click the **Export this Report** button to display the **Export** dialog. 2. Select a file format. 3. Select the page range to be printed. 4. Click the **Export** button to display the **Save As** dialog. 5. Enter a **File name**. 6. Select *RPT File (*.rpt)* as the **Save as Type**. 7. Click the **Save** button.
	To search for text in the report: 1. Enter the text in the **Search for text field**. 2. Click the **Search for text** button. The results are highlighted.
	Click the **Go to Previous Page** and **Go to Next Page** buttons to navigate through the report, page by page.

1 of 1+ ⏷	To navigate to a particular page: 1. Enter a page number in the **Page Navigation** field. 2. Click the **Enter** button on your desktop. 3. Click the drop-down to access the **Go to First Page** and **Go to Last Page** navigation options.
100% ⏷	Select the drop-down on the **Zoom** field and select a zoom factor between 25% and 400 %.

Additional Resources:

RG_Online_Common_Reports
RG_Permissions_Report Permissions

available on <u>My Account</u> and the **One Publications** website (<u>www.onepublications.com</u>).

Report Viewer

The Report Viewer is accessed when a Crystal report is opened via the **Links | Reports** panel.

The toolbar at the top of the page enables you to navigate through the report.

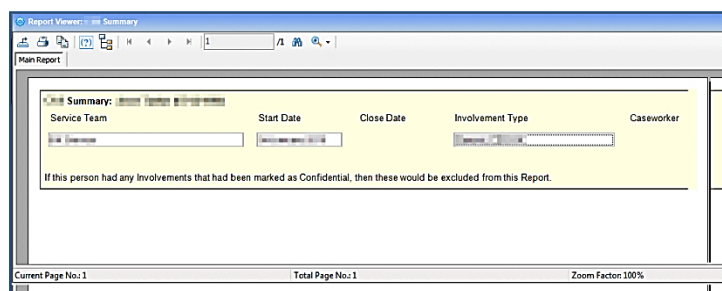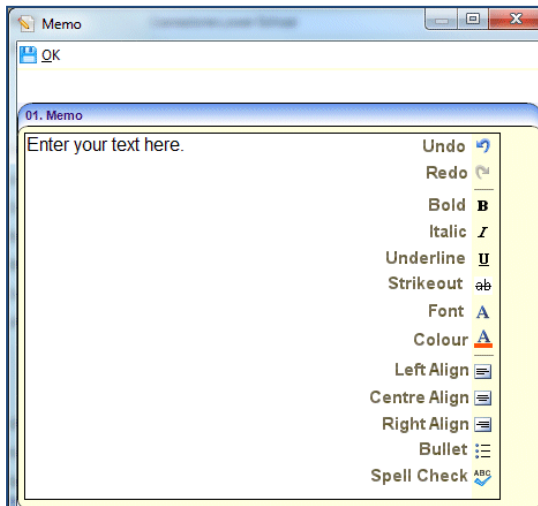|	
📤	Click the **Export Report** button to display the **Export Report** dialog. Select a location, enter a **File name**, then click the **Save** button to save the (*.rpt).
🖨	Click the **Print Report** button to display the **Print** dialog. If required, make changes to the printing options on the **General** tab and the **Layout** tab.
📋	Use the **Ctrl** key and the mouse to select sections of the report. Click the **Copy** button then paste the items stored on the clipboard.
(?)	The **Toggle Parameter Panel** button is not used with Capita One Crystal reports.
🗂	Click the **Toggle Group Tree** button to display the **Group Tree** panel. This panel lists all of the records contained in the report.
◀ ▶	Click the **Go to Previous Page** and **Go to Next Page** buttons to navigate through the report, page by page.
⏮ ⏭	Click the **Go to First Page** and **Go to Last Page** buttons to navigate to the beginning and the end of the report.
2 /3	The **Go to Page** button displays the current page number and the total number of pages contained in the report. To navigate to a particular page, type the number in the box and click the **Enter** button.
🔍	Click the **Find Text** button to display the **Find Text** dialog. Enter the text you are looking for in the **Find What:** field. You must start your search from the beginning of the report.
🔍⏷	Click the **Zoom** button and select a zoom factor between 25% and 400%. You can also zoom in on the whole page or customise your own zoom level.

Memo

The **Memo** functionality enables you to record relevant information relating to the current record. The **Memo** button displays at the top of many pages in v4 Client. **The Memo dialog can be expanded to full screen, edited, then returned to its previous size.**

Creating a Memo

To create a new memo:

1. Click the **Memo** button to display the **Memo** dialog. Hover over the icons to display the tooltips.

2. Enter the text, and format as required.

3. Click the **OK** button to close the **Memo** dialog.

4. Click the **Save** button to save the record. The **Memo** icon changes from blue to red to inform the next user that a memo has been recorded against the record.

> **Note:**
>
> *All free text fields with more than 1,000 characters are converted to memos, with the same functionality as above.*

Quick Reports

The **Quick Reports** panel enables you to use Microsoft Word templates, in XML format, to extract data via individual pages or exemplars. At run-time, the output can be to Word or Adobe PDF. Once a report has been created or imported, the template is specific to your computer.

Templates can be designed as letters or forms. A template can be created independently in Word by selecting a blank report template. Data items for each field are used in the construction of a quick report template.

A number of quick reports are available in One via the **My Documents\Capita ICS\My Report Templates** folder. The majority of these quick reports are for use with ICS Exemplars, some are for use in the Communication Log, a few are available for Early Years. These templates can be customised by adding or removing data items according to your requirements.

One uses entities to link a template to the area where the quick report can be run. For example, the *Parent Notification* report template is accessed via **Quick Reports | Communication Log Correspondence** (*CCS-Entity-CommLogCorrespondence.Parent Notification.ReportTemplate*).

The Capita One quick reports are accessed via the **Links | Communication Log Quick Reports** panel, under the following headings:

- Communication Log Correspondence
- Attendance Monitoring Correspondence
- Penalty Notice Correspondence
- Parent Contract Correspondence
- Court Order Correspondence
- Exclusions Correspondence
- Involvements Correspondence
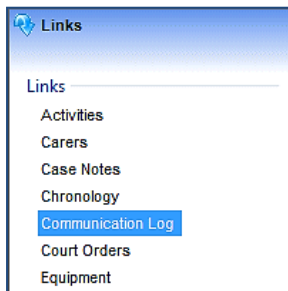- Relocations Correspondence.

> **Additional Resources:**
>
> *RG_Administration_Using Quick Reports*
>
> available on My Account and the **One Publications** website (www.onepublications.com).

Using Capita One Quick Reports

To create a quick report utilising CSS specific entities:

1. In v4 Client, select **Focus | People | Person/Students** to display the **Enquiry** page.

2. Select a person/student and click **Communication Log** in the **Links** panel to display the communication log for that person.

   Any existing communication logs are displayed in the browse list.

3. Select a communication log to display the **Communication Log Details** page; the **Quick Reports** panel is displayed on the right, with the Capita One report templates listed below.

4. Double-click on an individual report template to view its data items and content.

> **Note:**
>
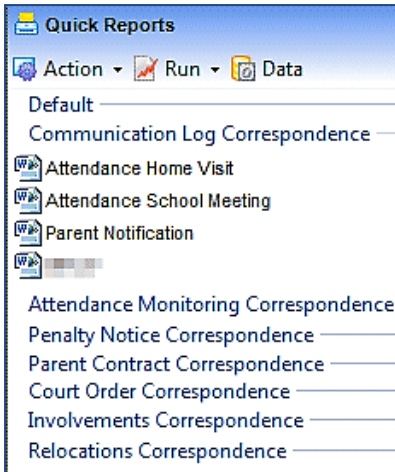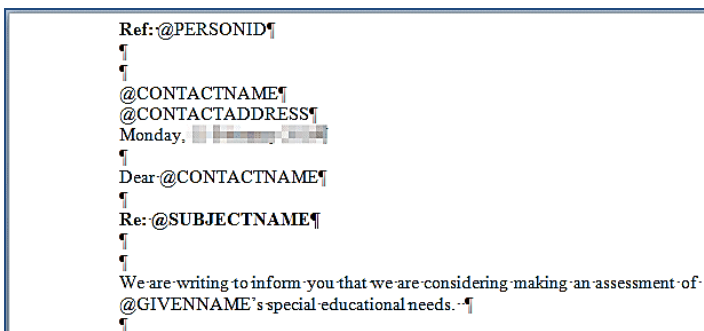> Do not run a report until the communication log details have been saved.

5. Populate the **Communication Log Details** panels.

6. Click the **Save** button.

   The communication log details <u>must</u> be saved before you run a Capita One quick report. You must also check that other related panels have been populated, e.g. Attendance Details for use in the Attendance Home Visit quick report.

7. In the **Quick Reports** panel, highlight the required quick report.

8. Click the **Run** button and select **Run as Word** or **Run as PDF** to display the **Save Report As** dialog.

9. If required, alter the **File Name**.

   A Word documents automatically saves as an XML file.
   A PDF automatically saves as a PDF file.

10. Click the **Save** button; the populated report displays in the selected format.

    If you have selected your quick report to output to Word, then it is possible to format it.

Creating a Quick Report Template

To create your own quick report template:

1. In v4 Client, navigate to the area you wish to report on, e.g. **Focus | People | Student | School History**.

2. Check the required panels and fields have been populated.

3. If any changes have been made, click the **Save** button.

4. In the **Quick Reports** panel, select **Action | New | Template from Blank Report** to display the **New Template[CCS.UserInterface.QuickReport Manager…]** dialog.

5. Enter the name of the quick report template in the **Create Template As** field.

6. Click the **OK** button. The new report template displays in the **Quick Reports** panel.

7. Double-click to open the blank report template.

8. Give your report a heading.

9. Click the **Save** button.

   Now, you need to add the data items. For more information, see *Adding Data items to the Quick Report Template* on page *33*.

Adding Data items to the Quick Report Template

To add data item to the report template:

1. In the **Quick Reports** panel, click the **Data** button to display the **Data Selection** dialog; the dialog remains on top of your document.
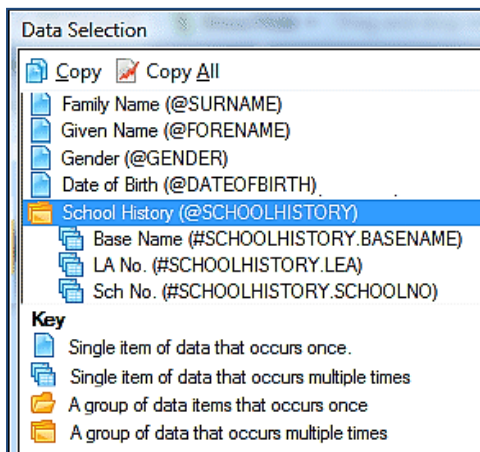

Double-click on a folder to view the data items.

The data items are in UPPERCASE.

Data items containing an @ symbol are for single items.

Data items containing a # symbol are for group items, where the data is repeated.

2. Select a data item and click the **Copy** button (**Ctrl + C** does <u>not</u> work).

   Copying a data folder copies <u>all</u> the data items in that folder.
   Clicking the **Copy All** button selects <u>every</u> data item in the **Data Selection** dialog.

3. Paste the item into your template; you can use **Ctrl + V** or right-click and select the **Paste** option.

> **Important Note:**
>
> You <u>cannot</u> 'type' the data item into your document; you <u>must</u> use **Copy** and **Paste**. If you delete any letter, including the **@** or **#** symbols, you <u>must</u> copy and paste the data item again.

Single (**@**) data items can be inserted straight onto the page.

Text can be formatted on the report template.

To convert a number of data items into a table: select all the data items, then select **Insert | Table | Convert Text to Table | Separate text at Tabs**.

Group (**#**) data items <u>must</u> be inserted into a table.

Any preceding text that is not deleted in the report template, will display on the populated report.

If there is an error in the data item on the template, the data item displays on the report output.

4. Delete all of the text <u>preceding</u> the **@** or **#** symbols. This text can be used to create headings.

5. Adjust any table cells to fit the <u>results</u> of the data items, e.g. **Start Date** and **End Date** can be narrow columns.

6. If required, make any formatting changes to the data items.

7. Click the **Save** button.

8. Close the report template.

   To run a quick report that you have created, follow steps 7 – 10 in *Using Capita One Quick Reports* on page *30*.

SQL Mail Merge

The primary function of SQL Mail merge is to create a file of exported data on the basis of an SQL Select query, typically for use in a mail merge Word document. The data may also be used for analysis in Excel, for example.

> **Note:**
>
> Only SQL statements that begin with the word `Select` are allowed. All other commands such as `Update`, `Insert` or `Delete` are prohibited and will fail validation.

Once the file is created you can export the data to a nominated file folder on the system's network or to a local machine.

Before creating SQL Mail Merge, users and user groups must be set up via **v4 Client | Tools | Administration | User Management | User Accounts/User Groups**. For more information, see the *Managing Users, Groups & Permissions* handbook available on the **One Publications** website (www.onepublications.com) via **Handbooks | System**.

The SQL Mail Merge query is set up by the system administrator in v4 Online. For more information, see *Creating SQL Mail Merge* on page *34*.

The system administrator nominates which users and user groups may initiate the query. For more information, see *Adding Users to SQL Mail Merge* on page *36* and *Adding Groups to SQL Mail Merge* on page *37*.

> **Additional Resources:**
>
> *RG_Administration_SQL Mail Merge*
> *RG_Online Administration_Creating SQL Mail Merge*
>
> available on My Account and the **One Publications** website (www.onepublications.com).
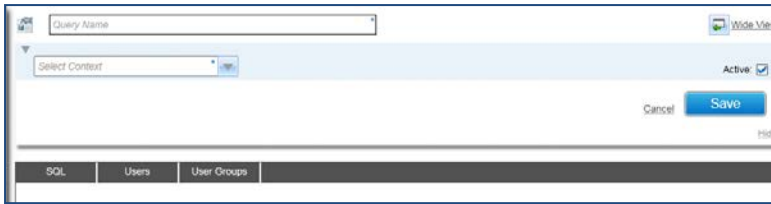
Creating SQL Mail Merge

To create a new SQL Mail Merge:

1. In One v4 Online, select **Administration | System Admin | SQL Mail Merge** to display the **SQL Mail Merge Query** page.

2. Click the **Add New Query** button to display the **Query Name** dialog.

3. Enter a **Query Name**.

4. Select a **Context**.

5. Click the **Save** button to display the **SQL Statement** field. Information is given in the **Parameters** panel displaying parameters that are available to use within the clause of the SQL statement.

6. Enter the **SQL Statement** text. Only SQL statements that begin with the word `Select` are allowed.

7. Click the **Save** button to display the SQL statement.

If required, click the **Preview** button on the **Parameter** panel to display the **SQL Mail Merge** dialog; this displays the results of the SQL query.

If required, click the **Export** button on the **Parameter** panel to display the **Save Output As** dialog; this enables you to save the files and export the queries.

Adding Users to SQL Mail Merge

To add users to the SQL Mail Merge:

1. Click the **Users** tab to display the **Users / Edit** page.
2. Click the **Edit** button to display the **Users Filter** dialog.

3. In the **Filter** field, enter the initial letter of the user name to minimise your search results.
4. Select the check boxes next to the names of the required users.
5. Click the **Save** button. The following message is displayed:

   SQL Mail Merge Users saved.

6. Close the **Users Filter** dialog to display the **Users** tab and the list of selected users.

7. Click the **Edit** button to make any necessary changes to the list of users.

Adding Groups to SQL Mail Merge

To add user groups to the SQL Mail Merge:

1. Click the **User Groups** tab to display the **User Groups / Edit** page.

2. Click the **Edit** button to display the **Groups Filter** dialog.

Clicking the plus sign next to a group displays the list of users in that group.

3. In the **Filter** field, enter the initial letter of the group name to minimise your search results.

4. Select the check boxes next to the names of the required groups.

5. Click the **Save** button. The following message is displayed:

   SQL Mail Merge Groups saved.

6. Close the **Groups Filter** dialog to display the **User Groups** tab and the list of selected users.

7. Click the **Edit** button to make any necessary changes to the user group.

Using the SQL Mail Merge Button

The **SQL Mail Merge** button is available in many areas of the v4 Client.

1. Click the **SQL Mail Merge** button at the top of the page to display the **SQL Mail Merge** dialog.

2. In the **SQL Mail Merge Details** panel, highlight the required group. If you want to search for a specific group, enter the **Looking For** text/number you want to search for.

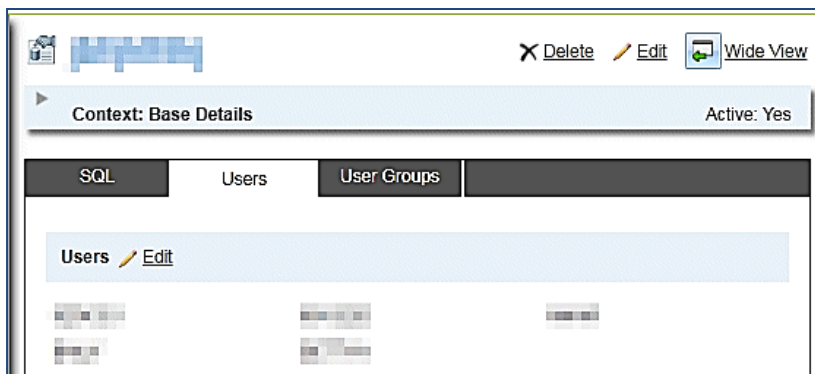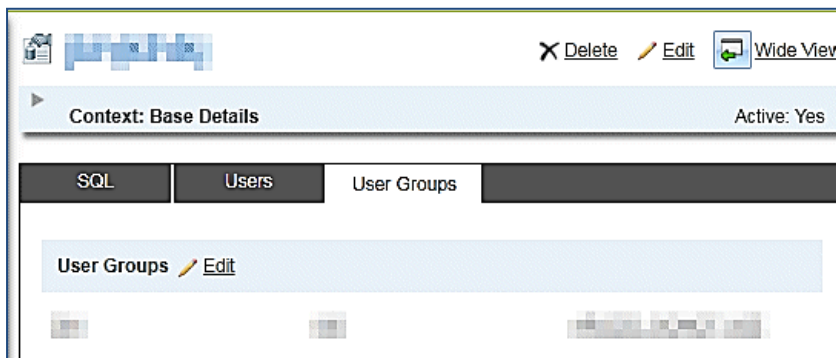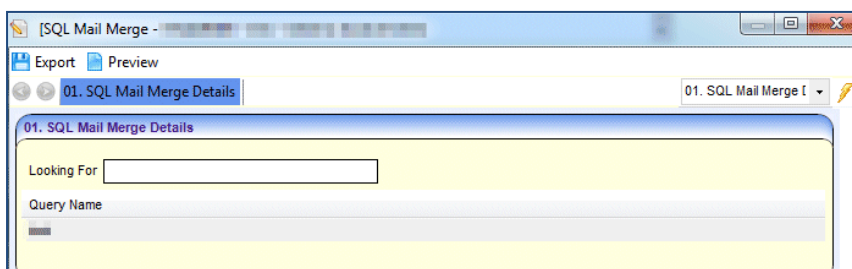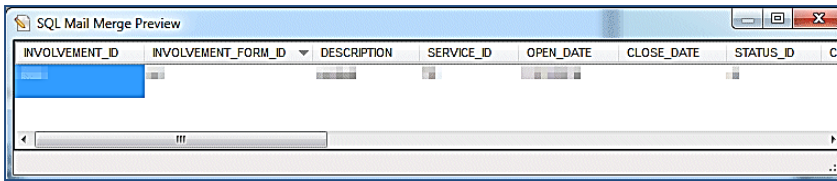3. Highlight the required SQL query and click the **Preview** button to display the **SQL Mail Merge Preview** dialog. This displays the results of the SQL Mail Merge.

Click on a column heading to sort by ascending or descending order.
Use the scroll bar to view more columns.

4. Close the **SQL Mail Merge Preview** dialog.

5. Highlight the required SQL query and click the **Export** button to display the **Save Output As** dialog.

6. Select a location to store your file.

7. Enter a **File name**.

8. Set the **Save as type** to *CSV files (*.csv)*.

9. Click the **Save** button.

10. Close the **SQL Mail Merge** dialog.

Additional Resources:

RG_Administration_SQL Mail Merge
RG_Online Administration_Creating SQL Mail Merge

available on <u>My Account</u> and the **One Publications** website (<u>www.onepublications.com</u>).

UDF Management

User Defined Fields (UDFs) enable you to add extra fields to accommodate data items that One does not store. UDFs can be created against all entities, e.g. Student Details, Activities, Exclusions and Hearing Impairment. A UDF can only be used once. They are created via **Tools | Administration | UDF Management**. For more information, see *Creating a UDF* on page *39*.

UDFs cannot be deleted; they can only be made inactive by removing them from the entity. For more information, see *Removing a UDF* on page *42*.

A dynamic view is created for each migrated v3 table. The view name is **VIEW_UDF_{V3_TABLE_NAME}**. For example, the BASES table has a dynamic view as VIEW_UDF_BASES.

For reporting purposes, a new UDF is included in the view by clicking the **Compile View** button at the top of the **Tools | Administration | UDF Management** page. This creates the view and displays the following message at the bottom of the page:

View VIEW_UDF_<*BASES*> is generated successfully.

Additional Resources:

RG_Administration_Managing UDFs available on <u>My Account</u> and the **One Publications** website (www.one publications.com).
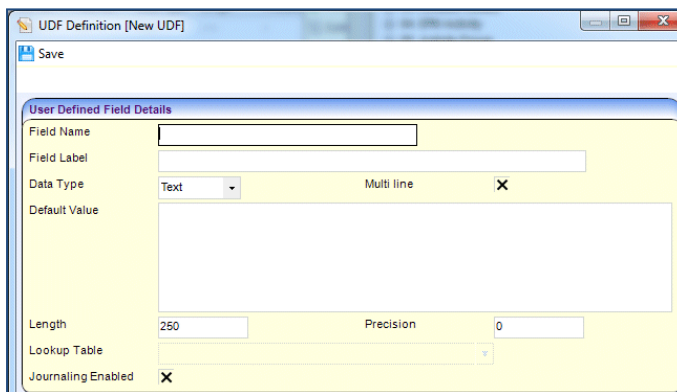

Creating a UDF

To create a new UDF:

1. Select **Tools | Administration | UDF Management** to display the **UDF Management** page.

2. On the **Entity Selector** panel, select the required **Entity Name** from the drop-down list. The **UDF List** displays any UDFs that have already been defined. UDFs that are in use display as grey text. Available UDFs display as red text.

3. Click the **Add** button to display the **UDF Definition** dialog.

4. On the **User Defined Field Details** panel, enter the following UDF details as required:

    i. **Field Name**: This is a unique code name by which the field is known in the database. It contain no spaces, an underscore can be used. It is a free text field up to 30 characters. When the UDF is saved, the file name is added to the UDF table with a prefix of 'U_' to identify the field from those fields that are supplied at the time of installation. The characters are automatically changed to UPPER CASE.

    ii. **Field Label**: This is a description that enables you to identify the UDF. It is a free text field up to 50 characters. The description may include an indication of the type of entry that is expected, e.g. *FSM? (T/F)*, which indicates that the UDF is a logical field and displays as a check box

    iii. **Data Type**: Select from **Text**, **Number**, **Date**, **Logical** or **Lookup**. The remaining fields are dependent upon the data type selected.

    iv. **Multi Line**: This check box is used only for the **Text** data type. Selecting the check box makes the **Default Value** field scrollable, enabling you to enter multiple lines of text.

    v. **Default Value**: The following default values are set:

        a. **Text** – This is a free text field enabling you to enter letters, numbers and symbols according to the **Length**.

        b. **Number** – Selecting **Number** only allows numerals to be entered into the **Default Value**. The **Default Value** is dependent on the **Length** field. Selecting **Number** activates the **Precision** field, which enables you to set the number of decimal places.

    c. **Date** –A default value is required only if you wish to set a particular date as a default date.

    d. **Logical** – This field displays in the form of a check box. The default values are T (true) or F (false).

    e. **Lookup** – Lookups do not have a default value.

vi. **Length**: The following are the maximum number of characters allowed:

    a. **Text**: If **Multi line** has been selected, then this field is user defined up to a maximum of 250 characters. If **Multi line** has not been selected, then the maximum number of characters is 179.

    b. **Number**: This is a user defined field up to 18 characters. If the **Length** is set to 10, then the **Default Value** can only be a number up to 10 digits.

    c. **Date**: This requires 10 characters. It must be in the following format: DD/MM/YYYY.

    d. **Logical**: The number of characters is automatically set to 1.

    e. **Lookup**: This is a user defined field up to 6 characters. One Lookup Codes require 4 digits.

vii. **Precision**: This applies only to the **Number** data type. It is used to record the number of decimal places to be stored in a field. The decimal point and the decimal places are included in the **Length** field.

viii.   **Lookup Table**: Select a lookup code to which you wish to link the UDF. The field displays as a dropdown from which you can select a user code and description from the relevant lookup.

ix. **Journaling Enabled**: Select this check box to make the UDF available for audit tracking. This is available for all data types.

5. Click the **Save** button to return to the **UDF Management** page. The new UDF is displayed in red on the UDF List. It remains inactive until added to an entity. For more information, see *Adding a UDF to an Entity* on page *40*.

UDF List

Field Name	Field Label	Data Type	Length	Precision	Journaling ...	Inactive
U_TERM1	Term 1	Text	80		No	No
U_NEXT_OFSTED	Next Ofsted	Date	10		No	No
U_U_EMA	EMA Base	Logical	1		No	No
NEW_UDF	Handbook	Text	250	0	Yes	Yes

Additional Resources:

RG_Administration_Managing UDFs available on My Account and the **One Publications** website (www.one publications.com).
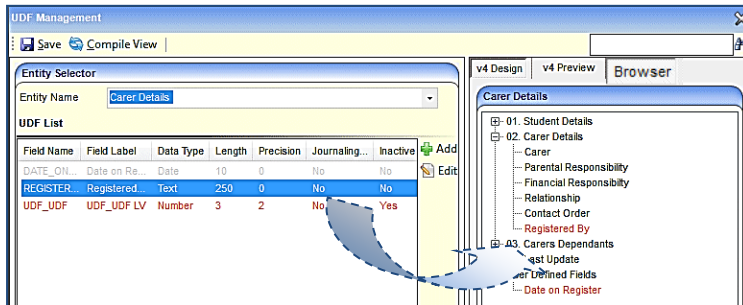
Adding a UDF to an Entity

After the UDF has been created, it is added to an entity on the **v4 Design** tab. You can preview the UDF, but you cannot enter any data. For more information, see *Previewing a UDF* on page *41*

For v4 Online entities, i.e. CIEE and G&B, a separate **Browser** tab is available to add the UDFs. You cannot preview these UDFs.
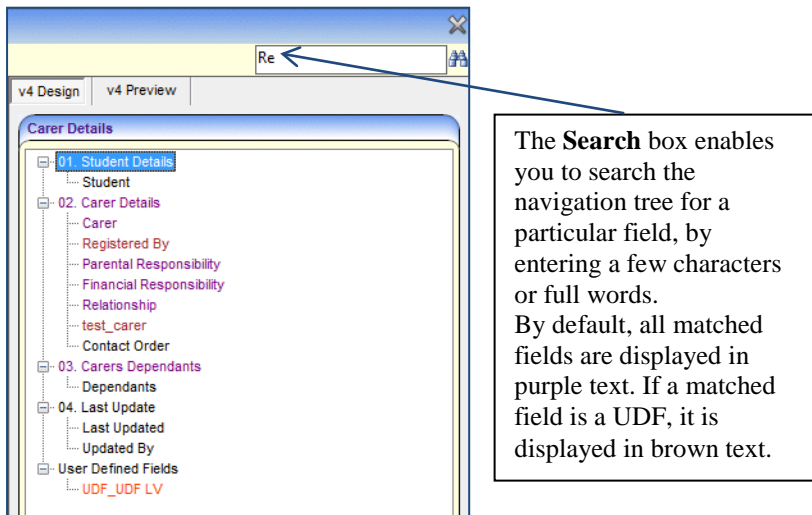
To add a UDF to an entity:

1. Select **Tools | Administration | UDF Management** to display the **UDF Management** page.

2. Select the required **Entity Name**.

3. On the **Entity Selector** panel, drag the UDF from the **UDF List** panel to the **v4 Design** tab.

   The **v4 Design** tab lists the details of the selected entity in a tree view. The tree is pre-populated with the panels relating to the selected entity.

UDFs can be placed in any panel or in the **User Defined Fields** panel at the bottom of the tree.

The **Search** box enables you to search the navigation tree for a particular field, by entering a few characters or full words.
By default, all matched fields are displayed in purple text. If a matched field is a UDF, it is displayed in brown text.

4. Click the **Save** button.

> **Additional Resources:**
>
> *RG_Administration_Managing UDFs* available on My Account and the **One Publications** website (www.one publications.com).

Previewing a UDF

The **v4 Preview** tab is available to enable you to view how the UDF will be displayed on the **Entity** page on a record. You <u>cannot</u> enter any data on this tab.

To preview a UDF:

1. Select **Tools | Administration | UDF Management** to display the **UDF Management** page.

2. On the **Entity Selector** panel, select an **Entity Name**.

3. Click the **v4 Preview** tab to display the **<Entity Details> – Preview** panel.

Some fields cannot be displayed in the **v4 Preview** tab. If this occurs, the following message is displayed on the panel:

> Control cannot be displayed in preview screen.

Removing a UDF

UDFs cannot be deleted; they can only be made inactive by removing them from the entity. If a UDF is removed from an entity, it is removed from all records for that entity; this affects all records regardless of when they were created.

To remove a UDF from an entity:

1. Select **Tools | Administration | UDF Management** to display the **UDF Management** page.
2. On the **Entity Selector** panel, select the required **Entity Name**.
3. Drag the UDF from the **v4 Design** tab to the **UDF List** panel.

The details of the UDF on the **UDF List** panel revert from grey to red text.

4. Click the **Save** button.

03 | **Appendix**

Reference Material

The following documents, referenced in this handbook, can be found with every main release:

Managing Users, Groups and Permissions Handbook

One System (v4 online) Common Functionality Handbook

V4 Linked Reports Handbook

Reference Guides (v4 Client)

The following reference guides are available on My Account and the **One Publications** website (www.onepublications.com) to help you with the v4 Client System processes:

RG_Administration_ACL Definition

RG_Administration_Creating Scheduled Alerts

RG_Administration_Creating SQL Alerts

RG_Administration_Creating Trigger Alerts

RG_Administration_Managing UDFs

RG_Administration_Quick Reports

RG_Administration_SQL Mail Merge

RG_Administration_System Alerts

RG_Administration_Data Panel Definition

RG_Permissions_Report Permissions

RG_Permissions_User Group Permissions

RG_Permissions_User Group Processes

Index