Infor Quality Management Administration Guide

Publication Information

Release: Infor Quality Management 10.22.5
Publication Date: November 15, 2022
Document code: iqm_10.22.5_iqmag__en-us

Contents

About this guide

This guide describes the administrative functions of Infor Quality Management. Use this guide to set up users, user groups, reporting, BODs, user-defined fields, and system numbering parameters.

This guide describes system administrator activities unique to IQM. The Infor Mongoose framework has many other system administrator functions.

See the *Infor Mongoose System Administration Guide*.

Intended audience

This guide is for users who are responsible for administering IQM.

Related documents

You can find the documents in the product documentation section of the Infor Xtreme Support portal.

Infor Mongoose System Administration Guide

Infor Quality Management User Guide

Infor Mongoose Creating and Customizing Reports

Contacting Infor

If you have questions about Infor products, go to Infor Concierge at https://concierge.infor.com/ and create a support incident.

The latest documentation is available from docs.infor.com or from the Infor Support Portal. To access documentation on the Infor Support Portal, select **Search > Browse Documentation**. We recommend that you check this portal periodically for updated documentation.

If you have comments about Infor documentation, contact documentation@infor.com.

Chapter 1: Getting started

This section describes how to apply the IQM license and how to identify version information.

Applying the license

Your IQM license is located in a text file provided to you by Infor Support or Infor Consulting Services.

Licenses are specific to the combination of your IQM database name and your server name. If you change the name of either your IQM database or your server, your license will no longer function. You must acquire a new license from Infor.

Apply the license before you begin using IQM for the first time. You must also reapply the license after you upgrade IQM to a newer version.

1. Sign in to IQM as the sa user.
2. Select **Administration > License Management**.
3. Click the**Apply License** tab.
4. In the **License Document** field, paste the contents of the text file.
5. Click **Apply License**. After you apply the license, basic information is inserted in the form header.

   The license determines how many users can access IQM modules. If your have a concurrent user license, then the number specified for each module is the number of users that can be logged into the module at the same time. If you have a named user license, then the number specified for each module is the maximum number of users that can be assigned to the module.

Viewing version information

Infor Support might ask for version information if you contact them with an issue. IQM, SQL Server, and Mongoose each have their own version numbers.

1. Select **Administration > About Infor Quality Management**.

   The IQM and SQL Server version are displayed.
2. Select **System > Help > About**.

   The Mongoose version is displayed.

Chapter 2: Users and groups

Use the procedures described in this section to add new users and grant them permission to use the system. These functions should be performed by a system administrator.

This table shows an overview of the procedures to use to grant a user access to IQM:

Procedure	Description
Setting up password parameters	Use this procedure to specify the characteristics of user passwords. For example, you can require passwords to have at least one number. See Setting up password parameters on page 8.
Adding groups	Optionally, you can create groups. Use groups to apply permissions to multiple users simultaneously. You can create a group manually or copy an existing group. See Adding groups on page 9.
Adding users	Use this procedure to add individual users. See Adding users on page 10.
Grant licenses to users	To access IQM, users must be assigned to a license. See Licensing on page 12.
Assign permissions to users, groups, or both.	To specify the forms and features that users can access, set up permissions. You can grant permissions on a user-by-user basis, or you can assign users to groups. When a user is assigned to a group, the user inherits the permissions of the group. When a user is assigned to multiple groups, the user has access to a form if at least one of the groups has access. Permissions that you set up for an individual user override group settings. See Permissions on page 13.
Specify approval settings	Specify whether users must supply passwords when approving an IQM record. See Specifying approval settings on page 15.

Procedure	Description
Specify nonconformance and corrective action read-only settings	Specify whether users can edit a closed nonconformance record, corrective action record, or both. See Specifying nonconformance, corrective action, preventive and calibration maintenance read only settings on page 16.
Specify allowable and viewable sites	Specify the sites that users can access. See Specifying allowable and viewable sites on page 17.
Manage preferences	Specify how IQM looks and feels to each user. Managing preferences on page 17.

You can also delete orphaned user sessions.

See Deleting user sessions on page 17

Setting up password parameters

1 Select **Administration > Password Parameters**.

2 Specify this information:

Enforce Mixed Case Use
To require passwords to have at least one lowercase character and at least one uppercase character, select this check box.

Enforce Number
To require passwords to have at least one number, select this check box.

Enforce Special Character
To require passwords to have at least one special character, select this check box.

Number of Retries
Specify the number of times users can enter their passwords incorrectly before being locked out of the system.

Lockout Duration (minutes)
If users are locked out, specify the number of minutes the users must wait before trying to log in again.

Password Length Minimum
Specify the minimum number of characters that passwords must have.

Password Length Maximum
Specify the maximum number of characters that passwords must have.

Password Expiration Days
Specify the number of days the password remains valid. After the number of days you specify elapses, users must change their passwords. If passwords do not expire, specify 0.

Password Warning Days
If passwords expire, specify the number of days in advance of the expiration date that users receive a warning to change their passwords.

Password History Count
Specify the number of times users must change their password before they can reuse a password.

3 Click the **Save** button.

Adding groups

Use the Groups form to create sets of form permissions. After you create a group, create users and assign them to the group. Users inherit the permissions of any group to which they are assigned. If a user is assigned to multiple groups, the user has access to a form if at least one of the groups has access.

IQM includes default groups. Use these groups as a model to create your own groups. You can copy the default groups to create new groups. These default groups are included:

- Calibrations Manager
- Customer Service
- Engineer
- Engineering Manager
- Facilities Manager
- HR Manager
- Maintenance Manager
- Management Review Team
- Material Review Board
- NOACCESS
- Operators
- Purchaser/Buyer
- Purchasing Manager
- QAADMIN
- READONLY
- Trainer

This form is a core form.

To add a group:

1. Select **Administration > Group**.
2. Click the **Filter-in-Place** button.
3. Specify this information:

Group Name
Specify the ID of the group.

Group Description
Specify a description of the group.

4. Click the **Save** button.
5. Set up permissions.
   See Permissions on page 13.

Copying groups

You can create a new group from an existing group.

1. Select **Administration > Groups**.
2. Open the group you are copying.
3. Click **Copy Group**.
4. Specify this information:

   Target Group Name
   Specify the name of the new group.

   Target Group Description
   Specify a description of the new group.

5. Click the **Users** tab. The users assigned to the group that you selected in step 2 are displayed.
6. Select the users to include in the new group. You can add other users to the group after you save it.
7. Click the **Group Authorizations** tab.
8. Specify permissions for the group.
   See Permissions on page 13.
9. If you have set up filters in the Row Authorizations form, use the **Row Authorizations** tab to specify permissions on filters.
   See "About row-level security" in the *Infor Mongoose Administration Guide.*
10. Click **Save**.

Adding users

Use the Users form to define the users who have access to the system.

This form is a core form. This procedure describes the basics of adding a user.

For more information about this form, select **Mongoose Administration > Mongoose Overviews & Procedures >** in the online help.

To add a user:

1 Select **Administration > Users**.
2 Click the **Filter-in-Place** button.
3 Click the **New** button.
4 Specify this information:

User Name
Specify the ID of this user.

Super User
Select this check box to grant super user privileges. Super users can access all areas of the system regardless of the individual or group permissions that are applied to the user. Super users can also view all sites.

User Description
Specify a description of the ID, such as the user's full name.

Workstation/Domain ID
If this user can log into IQM using their workstation credentials, specify the workstation credentials in this field. Specify the domain followed by the workstation user ID. For example, specify HAMPTON/LJones.

This setting is used for smart clients only. The setting does not affect the web client.

User Password
Specify the password this user supplies to access IQM.

Confirm Password
Reenter the password you specified in the User Password field.

Editing Permissions
Specify whether this user can edit forms using WinStudio. Select one of these options:

Option	Description
None	This user cannot edit forms.
Basic	This user can make minimal change to forms for the user's own purposes. This user cannot edit forms for other users. This option is recommended for most IQM users.
Full User	This user can make any modification to forms for the user's own purposes. This user cannot edit forms for other users.
Site Developer	This user can make modifications for all users.

5 Click the **Save** button.

6 To assign this user to a group, click the **Group** tab. Specify the name of the group in the Group Name column. If this is the user's primary group, select the **Primary** check box. This setting is used in conjunction with customized forms. If you customize forms by group, the user's primary group forms are loaded.
7 Use this step only if you have installed a language pack. Click the **Login Information**. In the **Default Language** field, specify the language to use as the default for the user. To ensure that the translated interface is displayed properly, the user must also set the default language in User Preferences.
8 To enable this user to send email from IQM, click the **E-mail Address** tab and specify this information:

   E-mail Type Description
   Select Primary.

   E-mail Type Address
   Specify the user's email address.

9 Click the **Save** button.

Licensing

To access forms in IQM, users must be licensed. If users are not licensed, they cannot access forms, regardless of the security settings you have set up.

You can grant licenses to these modules:

IQMCore
Use this license module to grant users access to all IQM forms. IQM forms are prefixed with vq.

Most IQM require this license only.

IQMDataCollect
Use this license to grant users access to IQM product data collection and process data collection only when additional licenses for data collection only have been purchased. Do not use this license if you have not purchased extra data collection seats. Product and process data collection are part of IQMCore.

IQMIDOs
Use this license module to allow third-party products not developed in Mongoose to access and use IQM IDOs.

MGCoreAutomation
This license allows other applications to connect to Mongoose through the IDO layer. Some integrations require the MGCoreAutomation license module in order to log in to Mongoose and collect data. Infor allows you to request automation licenses equal to 50% of the number of MGCoreTrans licenses your company buys. For example, if your company buys 100 MGCoreTrans licenses, you can request up to 50 MGCoreAutomation user licenses.

If you plan to connect custom applications to Mongoose through the IDO layer, you might need to buy additional MGCoreAutomation licenses to have enough licenses for each application connection. This license module is always assigned the session type IDO.

MGCoreTrans
Use this license module to grant users access to Mongoose forms. For IQM, assign users to this module to grant them access to Users Maintenance, Group Maintenance, Session Management, Password Parameters, E-mail Types Maintenance, Documents, Notes, and the event system modules.

MGDataViews
Use this license module to allow users to access the DataViews, DataSearch, and Critical Numbers (KPI) forms.

MGDeveloper
Use this license module if you plan to create or customize IDOs or SQL tables. This module allows the use of Mongoose forms that start with the prefix "IDO" or "SQL" that are used for development. This license module is always assigned the session type Full Client.

Granting licenses to users

1. Select **Administration > License Module Users**.
2. Select the module to license.
3. For each user, select the **Include** check box to license the user to the module.
4. Click the **Save** button.

Permissions

When you set up permissions, you must consider the architecture of IQM. In IQM, most main forms have subforms. For example, Product Maintenance has a Product Teams subform. To grant full access to a particular form, you must grant permission to both the main form and to all of the subforms. Use Application User Maintenance to automatically grant permission to subforms when you grant permission to a main form.

Group permissions

If you assigned users to groups, the users inherit the permissions of the group.

If you assign a user to more than one group, the user has access to a form if at least one of the groups has access. For example, GROUP A allows access to Product Maintenance and GROUP B does not allow access to Product Maintenance. If a user is assigned to both GROUP A and GROUP B, then the user can access Product Maintenance.

User permissions

You can set up user permissions individually. If a user is also assigned to a group, the permissions that you set up for an individual user override the group permissions.

Permission types

You can set up these permissions:

Delete Privilege
Use this privilege to specify whether or not a user or group can delete a record using the specified form.

Edit Privilege
Use this privilege to specify whether or not a user or group can edit the form in WinStudio Designer.

Execute Privilege
Use this privilege to grant or deny access to all other privileges. If users are denied the Execute privilege, then they cannot perform any action on the form.

Insert Privilege
Use this privilege to specify whether or not a user or group can create a record using the specified form.

Read Privilege
Use this privilege to specify whether or not a user or group can view records using the specified form. If you assign users only the Read privilege, they cannot edit or create records using the specified form.

Update Privilege
Use this privilege to specify whether or not a user or group can edit an existing record using the specified form.

Bulk Update Privilege
Use this privilege to specify whether or not a user or group can edit multiple records at the same time, such as through importing a spreadsheet.

Specifying permissions

1. Select **Administration > Application User Maintenance**.
2. Perform one of these tasks:
   - To set up permissions for a group, specify the ID of the group in the Group ID field. Then, click **Group Authorizations**.
   - To set up permissions for a user, select the user in the primary collection. If the user is not listed in the primary collection, click the **New** button and select the user from the drop down window. You can select an existing user only. After you select the user, click **User Authorizations**.
3. All main forms are listed. To set up permissions, perform one of these steps:
   - To grant privileges to a form and its subforms, select the **Include Subforms** check box. Then, specify the privileges for the form. To grant or deny all privileges for the form and its subforms, select the appropriate row and then click **Toggle Row Authorizations** until the permission you want is displayed. Or, click the drop-down button for each privilege to set the permission.
   - To grant privileges to a main form only, clear the **Include Subforms** check box. Then, specify the privileges for the form. To grant or deny all privileges for the form, select the appropriate row and then click **Toggle Row Authorizations** until the permission you want is displayed. Or, click the drop-down button for each privilege to set the permission.

- To grant privileges for all forms and subforms, select the **Include Subforms** check box. Then, click the **Toggle All Authorizations** button until the permissions you want are displayed.
- To grant privileges for all main forms, clear the **Include Subforms** check box. Then, click the **Toggle All Authorizations** button until the permissions you want are displayed.
- To grant privileges to selected subforms, select the row for the main form. Then, click the **Subform Authorizations** button. Use the toggle buttons to grant permission to all privileges, or click the drop-down button for each privilege to set the permission.
- To grant privileges to form components, select the row for the main form. Then, click the **Component Authorizations** button. Use the toggle buttons to grant permission to all privileges, or click the drop-down button for each privilege to set the permission.

4 Click the **Save** button.

Setting permissions on the Users form or the Groups form

We do not recommend setting user or group authorizations directly from the Users form or Groups form.

When you click the **User Authorizations** button on the Users form or the **Group Authorizations** button on the Groups form, all IQM forms and subforms are listed. The relationships between the forms and the subforms are not indicated. Therefore, it is difficult to grant full access to a particular area of IQM.

We highly recommend that you use Application User Maintenance to set up permissions.

Specifying approval settings

Use Application User Maintenance to specify whether users must supply their IQM password when changing the status to approved in an approval list.

You can set up approval settings on an entity-by-entity basis. The user must have the same Approved By role in each entity. For example, if user BETH is an internal approver in Entity A, then BETH must also be an internal approver if BETH is added to Entity B.

To specify approval settings:

1. Select **Administration > Application User Maintenance**.
2. Select the user in the primary collection, or click the **New** button to add a user to the collection.
3. Specify this information:

   IQM Authorization
   To require the user to enter the IQM password when approving an item, select this check box. To allow the user to approve an item without entering the IQM password, clear this check box.

   Approved by
   Specify how this user ID is related to your organization. In the Approved By cell, specify Internal for employees, Customer, or Supplier.

   Entity ID
   Specify the entity in which the individual can approve items.

Employee ID
If you selected Internal in the Approved by cell, this field is active. Specify the employee ID associated with the user ID. The name of the employee is inserted in the Name field.

Customer ID
If you selected Customer in the Approved by cell, this field is active. Specify the customer ID associated with the user ID.

Customer Contact No
If you selected Customer in the Approved by cell, this field is active. After you specify the customer ID, specify the contact number associated with the user ID.

Supplier ID
If you selected Supplier in the Approved by cell, this field is active. Specify the supplier ID associated with the user ID.

Supplier Contact No
If you selected Supplier in the Approved by cell, this field is active. After you specify the supplier ID, specify the contact number associated with the user ID.

4 Click the **Save** button.

Specifying nonconformance, corrective action, preventive and calibration maintenance read only settings

By default, a user cannot edit a closed nonconformance or corrective action or preventive or calibration maintenance record. You can override this default setting.

To override this setting:

1. Select **Administration > Application User Maintenance**.
2. Select the user in the primary collection. If the user is not listed in the primary collection, click the **New** button and select the user from the drop-down list. You can select an existing user only. You cannot add new users in this form.
3. To allow the user to edit a closed nonconformance record, select the **Nonconformance read only override** check box.
4. To allow the user to edit a closed corrective action record, select the **Corrective action read only override** check box.
5. To allow the user to edit a closed preventive maintenance record, select the **Preventive Maintenance read only override** check box.
6. To allow the user to edit a closed calibration maintenance record, select the **Calibration Maintenance read only override** check box.
7. Click the **Save** button.

Specifying allowable and viewable sites

A site that a user can access is referred to as an allowable site. Users can use allowable sites in records and reports.

A viewable site is available for selection in the site ID list. For example, if users only occasionally work at a particular site, they can choose to remove that site from their viewable sites.

Users can use My Viewable Sites to override the viewable site settings that the system administrator sets up.

1. Select **Administration > User Site Maintenance**.
2. Select the user.
3. Click the **Site ID** arrow and select the user's allowable site. You can insert more than one site.
4. To display the site ID in site ID drop-down lists for the user, select the **Viewable** check box.
5. To designate the site as the default site for the user, select the **Default** check box. For records saved at the site level, the default site is inserted in the Site ID field when the user accesses the maintenance window. For records saved at the entity level, the default entity is inserted in the Entity ID field when the user access the maintenance window. Users can select a different site or entity on individual records. You can specify only one default site ID.
6. Click the **Save** button.

Managing preferences

When users personalize IQM, their personalization preferences are stored. Administrators can use the Preferences Maintenance form to manage the preferences that users have set up.

1. Select **Administration > Preferences Maintenance**.
2. Select the user whose preferences you want to view.
3. Edit the preference values as necessary. Take extreme caution when editing these settings. Editing these settings could result in IQM not behaving as anticipated.
4. Click the **Save** button.

Deleting user sessions

We recommend that you periodically delete orphaned user sessions. A user session can be orphaned if a user does not sign out of IQM correctly.

1. Select **Administration > Session Management**.
2. Select the sessions to delete. Currently active sessions are also listed. Use caution when deleting sessions.
3. Click **Delete Selected Sessions**.

Chapter 3: Customizing reports

To customize a report, complete these steps:

1. Make copies of the report and dialog forms.
2. Make a copy of the report task.
3. Copy the report links to My Reports.
4. Edit the report.

You must use the Design mode of WinStudio client to customize reports. You can customize the report for a specific user, group, or for all users.

Copying standard report forms

To copy a report, you must copy the report itself and the report dialog.

1. In the WinStudio client, select **System > Form > Definition > Design**.
2. In the For User/Group field, specify the user or group for whom you are customizing the report.
3. Select **System > Form > Definition > Copy**.
4. In the **Source Form** field, specify the ID of the report form that you are copying.
5. In the **Target Form** field, specify the ID of your customized report.
6. Accept the default settings for all other fields.
7. Click **OK**.
8. Select **System > Form > Definition > Copy**.
9. In the **Source Form** field, specify the ID of the report dialog that you are copying.
10. In the **Target Form** field, specify the ID of the customized report dialog that you are creating.
11. Accept the default settings for all other fields.
12. Click OK.

Copying standard report tasks

1. Select **System > Form > Open > Background Task Definition**.
2. Click **Filter in Place**.

3 In the collection, locate the task for the report that you are customizing. The task name matches the name of the report.
4 Right-click the line number of the task and select **Copy**.
5 In the copy, edit the task name and executable to match the name of your custom report.
6 Accept the default settings for all other fields.
7 Click **Save**.

Copying report links

1 Select **Administration > Report Customization**.
2 Click **Filter in Place**.
3 Select the report that you copied.
4 Right-click and select **Copy Report**.
5 Specify this information:

   New Report Name
   Specify the name of your new report.

   New Dialog Path
   Specify the name of the dialog that you created.

   New Report Path
   Specify the name of the report that you created.

6 Click **Ok**.

Editing the report format

1 Select **System > Form > Definition > Design**.
2 Locate the copy of the report that you made in the "Copying a standard report" procedure.
3 Click **OK**.
4 Customize the report. See the information about report template type forms in the *Infor Mongoose Creating and Customizing Reports* guide.
5 Click the **Save** button.

Chapter 4: User-defined fields

Several windows in the application feature user defined fields. You can use these fields to enter customized information specific to your business practices. This information is stored in the database.

By default, user defined fields are labeled "User Defined Field" with a number. You can customize these labels to be more descriptive. You can specify different labels for different languages.

In certain user defined fields, you enter free-form text. In other user defined fields, you select a value from a list. You can specify the values that are valid for selection.

Business Unit, Calibration Major Location, Calibration Minor Location, Major Location, and Minor Location each have separate code maintenance forms. Use these forms to maintain the codes for these fields, regardless of the label you use for these areas.

Specifying user defined field labels

ENU is the default language for user defined fields. Set up field labels for ENU first.

To specify user defined field labels:

1. Select **Administration > User Defined Field Labels**.
2. By default, all user defined field labels are displayed. To view user defined field labels for a particular module, click the Module down arrow and select the module to view.
3. In the Language field, specify ENU.
4. In the Label field, specify the field label to use.
5. Click the **Save** button.

Specifying user defined field labels for other languages

The label list for languages is built from the label list provided for ENU.

To specify user defined field labels for languages other than ENU:

1. Select **Administration > User Defined Field Labels**.

2. By default, all user defined field labels are displayed. To view user defined field labels for a particular module, click the Module down arrow and select the module to view.
3. In the Language field, specify the language. If you have not yet set up user defined field labels for the language, you are prompted to create them from ENU. Click Yes to create the labels.
4. In the Label field, specify the field label to use.
5. Click the **Save** button.

Specifying user defined values

For some user-defined fields, you can specify which codes are valid for selection. For example, in Device Maintenance, you define the values to use for User Defined Field 1.

To specify the values to use:

1. Right-click in the user-defined field and select **Add**.
2. Specify the code and the description.
3. Click the **Save** button.

Chapter 5: Next system IDs

When you create a record in most areas of IQM, the record is saved with an ID number. Use Next System IDs to specify prefixes and suffixes for your IDs for each application that uses system IDs.

If you use multiple entities and multiple sites, specifying unique prefixes or suffixes can help you identify which records belong to a particular entity or site. You can also use Next System IDs to specify which ID number to use when the next record in a module is saved.

Specifying next system IDs

1. Select **Administration > Edit Next System ID**. Each application that uses system IDs is listed. Modules where IDs are stored at the entity or site level are listed one time for each entity or site. In addition to Entity ID and Site ID, this information is displayed:

   Module ID
   This is the area in the application where the ID is used.

   Table Name
   This is the name of the database table where the ID is stored.

   Application
   This is the name of the window where the ID is used.

   Current ID
   This is the ID with the largest integer. When you next save a record, this number is increased by one.

2. Specify this information:

   Change To
   To change the next number used, specify a new number in this field. Specify a number that is one less than the next number you want to use. For example, if the value in the Current ID field is 10, and you want to use 15 as the next ID, specify 14 in the Change To field.

   Prefix
   Specify a prefix to use in conjunction with the ID.

   Suffix
   Specify a suffix to use in conjunction with the ID.

3 Click the **Save** button.

Chapter 6: Sending email

To send email, specify the application path in Application Global Maintenance. Then, use Email Configuration Maintenance to specify email settings for each form in IQM.

Specifying the IQM application path

If you intend to include links to IQM records in email that you send from IQM, specify the application path where IQM is located. This path is used to generate the URL links included in the email body.

1 Select **Administration > Application Global Maintenance**.
2 Click the **General** tab.
3 Specify this information:

   Click Once Application Path
   If you are using the one-click client, specify the location of the application. Use this format:

   ```
   http://myservername.domain.com/ClientDeploy/mongoose.application
   ```

   Note: Note that the client is only supported for automatic data collection, form customization, and certain administrative functions.

   Web Application Path
   If you are using the web application, specify the location of the application. Use this format:

   ```
   http://myservername.domain.com/WSWebClient/default.aspx
   ```

4 Click the **Save** button.

Setting up email from IQM forms

Use this procedure to specify the information to include in email sent from an IQM form. Repeat this procedure for each form from which you intend to send email.

1 Select **Administration > Email Configuration Maintenance**.

2 In the primary collection, select the form to set up. When you select a form, the ID and Description of the form are inserted in the header.

3 In the **Include Links** field, specify whether to include hyperlinks to IQM records in the email. Select one of these options:

Option	Description
None	Select this option if you do not want to include links in emails.
Both	Select this option to send links in emails sent from either the web client or the one-click client. IQM supports the use of the one-click client for automatic data collection and certain administrative functions, such as specifying the license key.
Web Client	Select this option to include links in emails sent from the web client.
One Click Client	Select this option to include links in emails sent from the one-click client. Because IQM does not support the one-click client for most functions, we recommend that you do not select this option.

If you select the **Include Links** check box, ensure that you have set up the IQM application path in Application Global Maintenance.

4 In the **Subject String Name** field, specify the text to use as the subject line. By default, the sEmailSubjectString name for the application is used. You can edit the value returned for the string name.

5 Click the **Subject** tab. All of the information that can be included in the subject line is displayed.

6 Specify this information:

Include in Subject
Select this check box to include the information in the subject line.

Label String Name
Optionally, change the label that is used for the information.

7 Use the up and down arrows to arrange the order of the fields.

8 Click the **Details** tab. All of the information that can be included in the email body is displayed.

9 Specify this information:

Include in Output
To include the information in the body of the e-mail, select the Include in **Output** check box.

Include in Link Filter
Using the default settings is recommended. This check box is selected if the information in the object is included in the URL link. For example, primary keys are often included in the link. To hide the information in the URL, clear the check box. E-mail recipients can still open the individual record you send.

Label String Name
Optionally, change the label that is used for the information.

10 Use the up and down arrows to arrange the order of the fields.

11 Click the **Save** button.

Chapter 7: Working with BODs

Use BODs to integrate IQM with an ERP. When IQM is integrated with an ERP, the ERP serves as the system of record (SOR). All data shared between the two systems are owned by the ERP.

To set up IQM to send and receive BODs:

On the BOD Maintenance tab in Application Global Maintenance, specify the Tenant ID and Message Bus Logical ID for IQM. When you set up the integration in Infor ION, this information is used to identify the IQM application. The BOD Maintenance tab lists all of the BODs IQM sends and receives.

In SOA Code Maintenance, review the mapping between BOD codes and the IQM application. IQM receives common codes, such as territories. The SOA Code Maintenance form shows where these codes are displayed in the application.

After IQM sends BODs to the ERP, use the SOR Response form to review the acknowledgement information sent back from the ERP. This form shows whether the information sent by IQM was accepted.

In addition, several BOD-related forms are found in the core framework.

Specifying BOD settings

Use BOD settings to specify the tenant ID and logical ID for the IQM database. BODs are processed with Infor ION. You can use BODs to integrate IQM with an ERP.

1. Select **Administration > Application Global Maintenance**.
2. Specify this information:

   Tenant ID
   Specify the tenant ID to use for your integration. Contact your Infor representative for the value to specify in this field. If you specified this information during the IQM installation process, the value you specified is displayed.

   Message Bus Logical ID
   The logical ID is made up of lid://infor.visual plus an instance ID of your choosing. If you specified this information during the IQM installation process, the value you specified is displayed.

   Do not allow delete of SOR records

   If IQM is integrated to an ERP or other system, select this check box to keep the IQM database and the integrated databases in sync.

When you select this check box, users cannot delete records that were created using BODs. Currently, IQM is the system of record for the InspectionOrder BOD, which maps to Lot Maintenance and Lot Maintenance History. Selecting this check box prevents users from deleting Lot Maintenance records and Lot History Maintenance records. If a user attempts to delete a Lot Maintenance or Lot History Maintenance record, a message is displayed informing the user that the record cannot be deleted.

If you clear this check box, a message is displayed warning you that your IQM and other system databases could become out of sync. Click **Yes** in the message to clear the check box. Click **No** to select the check box. It is highly recommended that you select the check box. If the IQM and other system databases become out of sync, issues can arise in the database.

3 The table displays the BODs that are imported into IQM and the BODs that IQM sends. You cannot edit this information.
4 Click the **Save** button.

Viewing SOA code types

The SOA Code Maintenance form shows all code types that can be used in BODs. Not all of these codes are used in the BODs sent and received in IQM. You cannot edit the code types.

Only a system administrator should use this form.

1. Select **Administration > Codes > SOA Maintenance**.
2. In the primary collection, select a code type. All codes for the code type are displayed.
3. Optionally, click the **Replication** tab to view the current mapping for the code type. The **Target IDO Name** field shows the IDO used to maintain the information displayed in the table. For example, for territory codes the IDO name vqTerritoryCodes is displayed.

Viewing acknowledgment BODs

When IQM sends a BOD to an ERP, the ERP returns an acknowledgment BOD. The SOR Response form shows details from the acknowledgment BOD. The acknowledgment BOD indicates whether the ERP successfully processed the information sent from IQM.

1. To view all acknowledgment BODs, select **Administration > SOA Response**. You can also access the SOR Response form from an individual form in IQM. For example, if you access SOR Response from Contacts Maintenance, then only the ContactPartyMaster acknowledgments are displayed.
2. Review this information:

   Entity ID
   If the information is specific to an entity, the ID of the entity is displayed.

   Site ID
   If the information is specific to a site, the ID of the site is displayed.

Original Document ID
The document ID of the process BOD that IQM sent to the ERP system of record is displayed. This is the BOD being acknowledged by the ERP.

Original Create Date
The date and time that IQM sent the process BOD are displayed.

Original Component ID
The ID of the component that sent the process BOD is displayed. This value is always IQM.

Original LID
The lid of the system that sent the process BOD is displayed. This is the value specified on the BOD Maintenance tab in Application Global Maintenance.

Verb
The type of verb sent by IQM is displayed. This value is always Process.

Noun
The BOD noun sent by IQM is displayed.

Creation Date
The date that the acknowledgment BOD was sent by the SOR is displayed.

Sender Component ID
The ID of the component that sent the acknowledgment BOD is displayed.

Sender LID
The lid of the system that sent the acknowledgment BOD is displayed.

Response Code
The response from the system that sent the acknowledgment BOD is displayed. This value is Accepted, Rejected, or Modified.

Reason Code
If the acknowledgment BOD included a reason code, this code is displayed.

Reason
If the acknowledgment BOD included a reason, the reason is displayed.

Chapter 8: Individual privacy

Use the Individual Privacy program to help your company comply with the European Union General Data Protection Regulation (GDPR). The intent of GDPR is to give individuals more control over their personal data. Upon request, an organization is required to provide a copy of an individual's personal data that the organization has stored in their databases.

You can use the Individual Privacy program to complete these tasks:

- Search for the name of an individual data subject in your database
- Generate the Individual Privacy report that can be sent to the data subject
- Redact a data subject's information
- Monitor Individual Privacy program usage

Terminology

These terms are used in the Individual Privacy documentation:

Data subjects

Data subjects are individuals about whom you store data. Data subjects can request a copy of their data and request that their data be removed.

Data controller

Data controllers are entities that hold data about data subjects. Because your IQM database can hold information about data subjects, your company is a data controller.

GDPR compliance overview

This table shows on overview of how you can use IQM to help you to comply with components of the GDPR:

Product Capability	**GDPR Reference**	**What We Do**
Access	GDPR, Article 15	Data Controllers can access data on behalf of the Data Subjects and generate reports to provide information to the Data Subject as required.

Product Capability	GDPR Reference	What We Do
Rectification of Inaccuracies	GDPR, Article 16	Data Controllers can update data on behalf of the Data Subjects.
Permanent Erasure	GDPR, Article 17	Data Controllers can permanently erase or remove Data Subject data through removal processes within the application.
Restriction of & Objection to Processing	GDPR, Articles 18 and 21	Data Controller can inactive Data Subject information and through security measures prevent the processing of Data Subject information.
Data Portability (Machine-Readable Formats)	GDPR, Article 20	Data Controller can print reports or export Data Subject data in machine readable format - csv.
Automated decision-making	GDPR, Article 22	Not a function or purpose of IQM.
Data Return or Deletion	GDPR, Article 28	Data Controller can return data in printed or machine reportable format and delete Data Subject data.
Technical & Organizational Security Measures	GDPR, Article 25	Data Controller can secure application access by user login and passwords are encrypted
Consent	GDPR, Article 7	There is no data processing activity that requires consent.

Manual redaction

The Individual Privacy program is a tool that you can use to help you redact personal data from your database. However, the program does not search all areas of the database that could contain personal information. You may need to manually delete data through the standard IQM interface.

Individual Privacy program security

You can restrict access to the Individual Privacy program through Application User Maintenance. We recommend that you limit the number of users who can access the program.

Individual Privacy program limitations

The Individual Privacy program searches for a data subject's name in the FIRST_NAME, LAST_NAME, MIDDLE_NAME, and username columns as described in the "Finding data subject information" topic. If a data subject's name is stored in any other database column, you must search for and remove the data subject's name manually.

The Individual Privacy program redacts only the data displayed in the table in "Data Redaction" No other data is redacted.

The Individual Privacy program does not search for nor redact information in these areas:

- Database User IDs
- Primary keys, such as employee IDs, customer IDs, and vendor IDs
- Notations
- Specifications
- Document Attachments
- User-defined fields
- Custom tables or custom columns in standard tables
- BOD in-box and out-box database tables

In addition to the areas in the list, other areas of the IQM database could contain personal information that you must search for and redact manually.

Data redaction and family information in Employee Maintenance

The Individual Privacy program does not search for information on the **Family** tab in **Employee Maintenance**. If you redact the Employee's information, then the data in the **Family** tab is also redacted. If you want to redact only information in the **Family** tab and retain the remainder of the employee's information, you must manually redact the information in the **Family** tab.

Data privacy best practices

To help you comply with GDPR, we recommend these best practices:

- Do not use an individual's name or other personal information as the primary key for an employee, customer, vendor, or other document. Primary keys must be retained in the database and cannot be redacted.
- Ifyou store document attachments that contain personal data, we recommend that you designate that the attachments contain personal data. For example, you could use a code in the file name or store the attachments in a dedicated folder.

Finding data subject information

The Individual Privacy program contains a field where you enter a data subject's name. You can specify all or part of the name.

When you click **Refresh** or tab out of the **Individual ID** field, the program searches for the data subject's name. This table shows the database tables that the program searches and the database columns that are searched. The table is organized by data group:

Data Group	Database Table	Database Columns
Contact	VQ_CONTACT	FIRST_NAME MIDDLE_NAME LAST_NAME
Employee	VQ_EMPLOYEE	FIRST_NAME MIDDLE_NAME LAST_NAME
User	UserNames	Username
User	UserEmail	Username

No other database tables are searched.

The search results are displayed in the table and are sorted by Data Group. You can sort the table by any of the columns, and you can filter the table by data group.

After you run a search, you can generate a report about a data subject and redact a data subject's information.

Searching for a data subject

1. Select **Admin > Individual Privacy**.
2. In the **Individual ID** field, specify the search text. You can enter all or part of the data subject's name.
3. Press **Tab** or click the **Refresh** button. The Individual Privacy program searches for your text in the FIRST_NAME, MIDDLE_NAME, LAST_NAME, and Username columns in tables that store these types of data: Contact, Employee, User. For a complete list of the tables that are searched, see Finding data subject information on page 32.

   The search results are inserted in the table sorted by Data Group. You can use the Data Group check boxes to filter the results. To sort the table by a different column, click the column's header.

   To export the results to Microsoft Excel, right-click and select **To Excel**.

Individual Privacy report

The Individual Privacy report contains this information:

- The data group where the data subject's data was found
- The primary key of the document that contains the data subject's data
- The data subject's name
- The data subject's address
- The data subject's phone number
- The data subject's email

You can generate the report for more than one data subject. If the data subject's information is used on multiple documents in your database, you can include multiple documents in the report.

Generating the Individual Privacy report as a PDF

You can generate the report in PDF format and send it to the data subject.

1. Select **Administration > Individual Privacy**.
2. In the **Individual ID** field, specify the search text. You can enter all or part of the data subject's name.
3. Press **Tab** or click the **Refresh** button.
4. Select the **Selected** check box for the individuals to include in the report.
5. Click the **Print** button.

Generating the Individual Privacy report as a CSV file

You can export privacy information to Microsoft Excel as a CSV file.

1. Select **Administration > Individual Privacy**.
2. In the **Individual ID** field, specify the search text. Make the search text specific so that only the individuals for whom you are providing privacy information are returned in the search results. Alternatively, you can edit the Excel file after you export the information.
3. Press **Tab** or click the **Refresh** button.
4. Right-click and select **To Excel**.

Data redaction

Caution: If you redact a data subject's data, the data cannot be recovered.

When you redact a data subject's data with the Individual Privacy program, text strings are replaced by Xs and dates are set to null. For columns that do not allow null values, the value is reset to the default value for the column.

If your search for a data subject yielded multiple results, you must redact all of the results to remove thedata subject's information from the database. For example, if a data subject's name is found in the First Name or Last Name fields in Contacts Maintenance and in Employee Maintenance, two lines are displayed for the data subject in the Individual Privacy table. To redact the data subject's data from both documents, you must select both lines in the table before selecting Redact Personal Information from the right-click menu.

This table shows the data that you can redact with the Individual Privacy program:

Interface location	Database table	Redacted columns
Contact Maintenance	VQ_CONTACT	

Interface location	Database table	Redacted columns
		FIRST_NAME
		LAST_NAME
		MIDDLE_NAME
		MIDDLE_INITIAL
		SALUTATION
		HONORIFIC
		COUNTRY_DIAL_CODE
		PHONE
		PHONE_EXT
		FAX
		MOBILE
		EMAIL_ADDRESS
		ADDRESS_LINE_1
		ADDRESS_LINE_2
		ADDRESS_LINE_3
		CITY
		STATE
		ZIP
		COUNTRY
		GENDER_CODE
		MARITAL_STATUS
		BIRTH_DATE
		OTHER_ADDRESS
		HOME_PHONE
		HOME_FAX
		HOME_EMAIL_ADDRESS
		HOME_ADDR_LINE_1
		HOME_ADDR_LINE_2
		HOME_ADDR_LINE_3
		HOME_CITY
		HOME_STATE
		HOME_COUNTRY
		HOME_ZIP
		URL_TWITTER
		URL_FACEBOOK
		URL_MYSPACE
		URL_LINKEDIN

Interface location	Database table	Redacted columns
		URL_HYVES HOME_COUNTRY_DIAL_CODE HOME_MOBILE OTHER_NUMBER
Employee Maintenance	VQ_EMPLOYEE	FIRST_NAME LAST_NAME MIDDLE_INITIAL ADDRESS_LINE_1 ADDRESS_LINE_2 ADDRESS_LINE_3 CITY ZIP STATE WORK_EMAIL_ADDRESS HOME_EMAIL_ADDRESS WORK_PHONE OTHER_NUMBER HOME_PHONE SOCIAL_SECURITY BIRTH_DATE
	VQ_EMPLOYEE_FAMILY	FIRST_NAME LAST_NAME MIDDLE_INITIAL RELATIONSHIP GENDER BIRTH_DATE SOCIAL_SECURITY
	VQ_EMPLOYEE_HISTORY	COMPANY_OR_SCHOOL START_DATE END_DATE REASON_FOR_LEAVING MAJOR DEGREE
Users	UserNames	UserDesc
	UserEmail	EmailAddress

Redacting data

Caution: If you redact a data subject's data, the data cannot be recovered.

1 Select **Admin > Individual Privacy**.
2 In the **Individual ID** field, specify the search text. You can enter all or part of the data subject's name.
3 Press **Tab** or click the **Refresh** button.
4 Select the rows that contain the data that you want to redact.
5 Right-click and select **Redact Personal Information**.
6 A message is displayed that states that all personal data for the selected rows will be removed. Click **Yes** to continue.
   The data is redacted, and the rows are removed from the Individual Privacy table.

Data redaction and BODs

If you are integrated to another application through BODs, an updated BOD is sent when you redact information. If you are integrated to Infor VISUAL, employee and contact data that you redact in IQM is also redacted in VISUAL.

If you use the Individual Privacy Program in VISUAL, you must manually trigger a BOD update to send the information to IQM.

Data redaction and third-party products

The Individual Privacy program works with IQM only. If you use third-party products with IQM, you must work with the provider of the product to redact private data.

Monitoring usage of the Individual Privacy program

You can view a history of the actions that users have taken in the Individual Privacy Program. You can view this information:

- The primary key of the document on which an action wasperformed,
- The actiontaken
- The user who performed theaction
- The date that the action was performed You can print the information to a report.

You can print the information to a report

1 Select **Administration > Individual Privacy**.
2 Click the **Privacy History** button.

3 Click the **Refresh** button. All actions are displayed, sorted by Data Group.

4 Use these filters to limit the information that is displayed in the table:
   - To filter the list by date, specify a date range in the **Start Date** and **End Date** fields.
   - To filter the list by data group, use the check boxes in the Data Group section.

5 To sort the table by a different column, double-click the columns' header.

6 To generate a report that includes the information in the table, click the **Print**button.