Merative™ Social Program Management

Authorisation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. Merative does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

This document is intended to provide guidance to help you in your preparations for GDPR readiness. It provides information about features of this offering, and aspects of the product's capabilities, that may help your organisation with GDPR requirements. This information is not an exhaustive list, due to the many ways that clients can choose and configure features, and the large variety of ways that the product can be used in itself and with third-party applications and systems.

The GDPR and authorisation

Authorisation to access personal data is a key concept of the GDPR and is related to several articles, of which examples are:

- Article 5(1)f of the GDPR states that personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing.

- Article 29 states that the processor and any person acting under the authority of the controller or of the processor, who has access to personal data, shall not process those data except on instructions from the controller, unless required to do so by Union or Member State law.

- Article 32(4) states that the controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.

Social Program Management (SPM) and authorisation

SPM provides a powerful and flexible authorisation framework in a default installation. In SPM, authorisation is the process of granting or refusing a user access to functional elements of an application.

The functional element can be anything to which a unique identifier can be attached, such as:

- A server process call.
- An element of the application that requires security checking.

Users, roles and groups

The security information associated with an application is organised into security profiles. A security profile consists of a security role, one or more security groups, and the associations between security identifiers (SIDs) and securable elements of an application.

Every authorised user is configured with a security role and the roles are associated with a number of security groups. Each security group is associated with a number of security identifiers. The security identifier represents the securable elements of SPM, for example, a method or a field.

Such a data structure makes it possible to authorise every user against any secured element of an application. Therefore, it is a powerful and flexible method of providing authorisation to SPM users.

Security identifiers (SIDs)

Every secured element in SPM is given a security identifier (SID) that is unique across the entire application. The analysis of what elements must be securable is a manual process that is done by a developer or a security administrator.

There are a number of types of SIDs that include the following types:

- Function identifiers (FIDs)
- Field level security identifiers
- User-defined SID types

Function identifiers (FIDs)

Function identifiers (FIDs) are a specialised type of security identifier (SID). When a method is made publicly accessible by setting the stereotype as façade in the model, an FID is generated for the method and security is automatically switched on.

Different security roles can be given access to different FIDs. For example, a caseworker role can have access to the searchPerson operation on the Person façade, while a system administrator may not.

Field level security identifiers

The field level SID allows authorisation to be applied to specific fields on a publicly accessible method. At runtime, if a user does not have access rights to view the field to be displayed, the contents of the field are displayed as a number of asterisks (***).

For example, personal data fields can be given an SID of “PersonalDataRights”, and only the users who have been granted access to that SID will have permission to view the data, for example, a caseworker and not an administrator.

For more information about Field Level SIDs, see the “Cúram Modelling Reference” guide in the Knowledge Center.

User-defined security identifiers

The authorisation process is sufficiently flexible to accommodate securable elements of an SPM application. Developers have the ability to define new *types* of SIDs. The *curam.util.security.Authorisation.isSIDAuthorised()* server interface method enables authorisation to be invoked directly on the new user-defined SID types.

For example, a particular resource that contains personal data might need to be secured. A new SID and security group could be created, for example, “PersonalDataResource” and “PersonalDataGroup” respectively. A caseworker role might be deemed to have the authority to access the secured resource and can then be associated with the newly created security group.

Access to the new resource is secured by wrapping access to the resource in a call to the *curam.util.security.Authorisation.isSIDAuthorised()* method. The method determines if the resource can be accessed based on the SID of the resource and the role of the current user.

For more information about user-defined SIDs, see the “Customising Authorisation” section in the Knowledge Center.

You can see an example of user-defined SIDs in a default installation on the *product* entity. It contains very fine-grained permissions, with each product instance relating to four SIDs. The permissions are split across read, write, maintain, and approval SIDs.

For more information about the product access security example, see the “Product Access Security Settings” guide in the Knowledge Center.

Dynamic Evidence Security

Security groups and security identifiers are generated when a dynamic evidence type is created. Three security identifiers are generated for each dynamic evidence type, one each for create, modify, and view operations. You can manage the groups and identifiers through the SPM administration application; for more information, see the “Cúram Administration” guide.

Security groups can be added to user roles to give access rights for the maintenance of individual dynamic evidence types. For example, specific users can be given rights to view evidence types that are deemed to contain personal data.

For more information about dynamic evidence security, see the “Administering dynamic evidence” guide in the Knowledge Center.

Sensitivity

All users, participants, participant notes, and case notes are assigned a sensitivity level. The default sensitivity level is 1.

Users are permitted to modify and view the secured data only if their sensitivity level is either equal to or higher than the data’s sensitivity level. For example, if a user with a sensitivity level of 3 wants to access or modify an activity that concerns a participant, the participant’s sensitivity level must be equal to or less than 3.

Where a case has multiple case members, the sensitivity level of all case members involved is considered. The following criteria applies:

- The user has full access rights if they have a sensitivity level equal to, or greater than the case participant with the highest sensitivity level.
- If the primary client and the user have the same sensitivity level but other case members on the case have a higher sensitivity level, the system allows the user access to view the case. However, the user is unable to modify any aspect of the case.
- If the user does not have the appropriate sensitivity level to access the primary client’s data, access to the case’s data is denied or the data is masked.

For more information about sensitivity security, see the “Cúram Organization Administration” guide in the Knowledge Center.

Location Based Security

Location based security may also be used to restrict a user's case and client access based on a combination of the location security set up for the organisation. If configured, a user may only access cases in his or her location or sub-locations.

For example, a caseworker in an organisation in Dublin may not have the permission to access cases in Cork.

Location Based Security for the application is configured by setting the location data security level on an organisation’s home page. The security level can be:

- *Off* - there are no restrictions on users viewing and maintaining case and client information.
- *On* - users will be able to view and maintain cases and client information in their own location and sub-locations.

- *Restricted View* - users will be able to see that a case or client exists in other locations but will not be able to view and maintain case or client details outside of their own location.
- *Read Only* - users can view and maintain cases in their own location and sub-locations. Users will also be able to view client and case information in other locations, but not maintain them.

For more information about location based security, see the “Cúram Location Administration” guide in the Knowledge Center.

Further information

For more information about authorisation, see the Security" guide.

For more information about customising authorisation, see "Customising Authorisation" in the Security" guide guide.

For more information about field level security, see the "Cúram Modelling Reference" guide.

For more information about product access security, see the "Product Access Security Settings" guide.

For more information about dynamic evidence security, see the "Administering dynamic evidence" guide.

For more information about sensitivity levels, see the "Cúram Organisation Administration Guide".

For more information about location-based security, see the "Location Administration Guide".

For more information about configuring security through the Social Program Management administration application, see the "Administration Guide".