High level design for

Permissions, Roles & Controls Management

Version: 1.0

Revision History

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Version | Prepared By | Date | Reviewed By | Date | Remarks |
| 1.0 | Umesh Nimbalkar | 8-Dec-17 |  |  |  |
|  |  |  |  |  |  |

Table of content

[1. Introduction to CASPER Permissions, Roles & Controls 3](#_Toc500597348)

[2. Assigning roles & controls to the CASPER user 4](#_Toc500597349)

[2.1. Identifying user type 4](#_Toc500597350)

[2.2. Various roles in CASPER 4](#_Toc500597351)

[2.3. Role of user administrators in CASPER 5](#_Toc500597352)

[2.4. Mechanism of roles and controls assignments to CASPER user 7](#_Toc500597353)

[2.5. Managing user assignments 8](#_Toc500597354)

[2.6. Managing Exceptions in given design construct 10](#_Toc500597355)

[3. Assigning & executing permissions in CASPER 11](#_Toc500597356)

[3.1. Permissions in CASPER 11](#_Toc500597357)

[3.2. Assigning permissions to role in CASPER 15](#_Toc500597358)

[3.3. Technical Approach for Assigning permissions to role in CASPER 17](#_Toc500597359)

[3.4. Applying permissions & controls to each task of CASPER user 19](#_Toc500597360)

[3.5. Technical approach for applying permissions & controls to each task of CASPER user 19](#_Toc500597361)

# Introduction to CASPER Permissions, Roles & Controls

Each of the user activity CASPER user will perform based on permissions he/she has. These permissions are also tightly interlinked with controls which works on filtering appropriate data to perform that activity.

Role represents group of permissions.

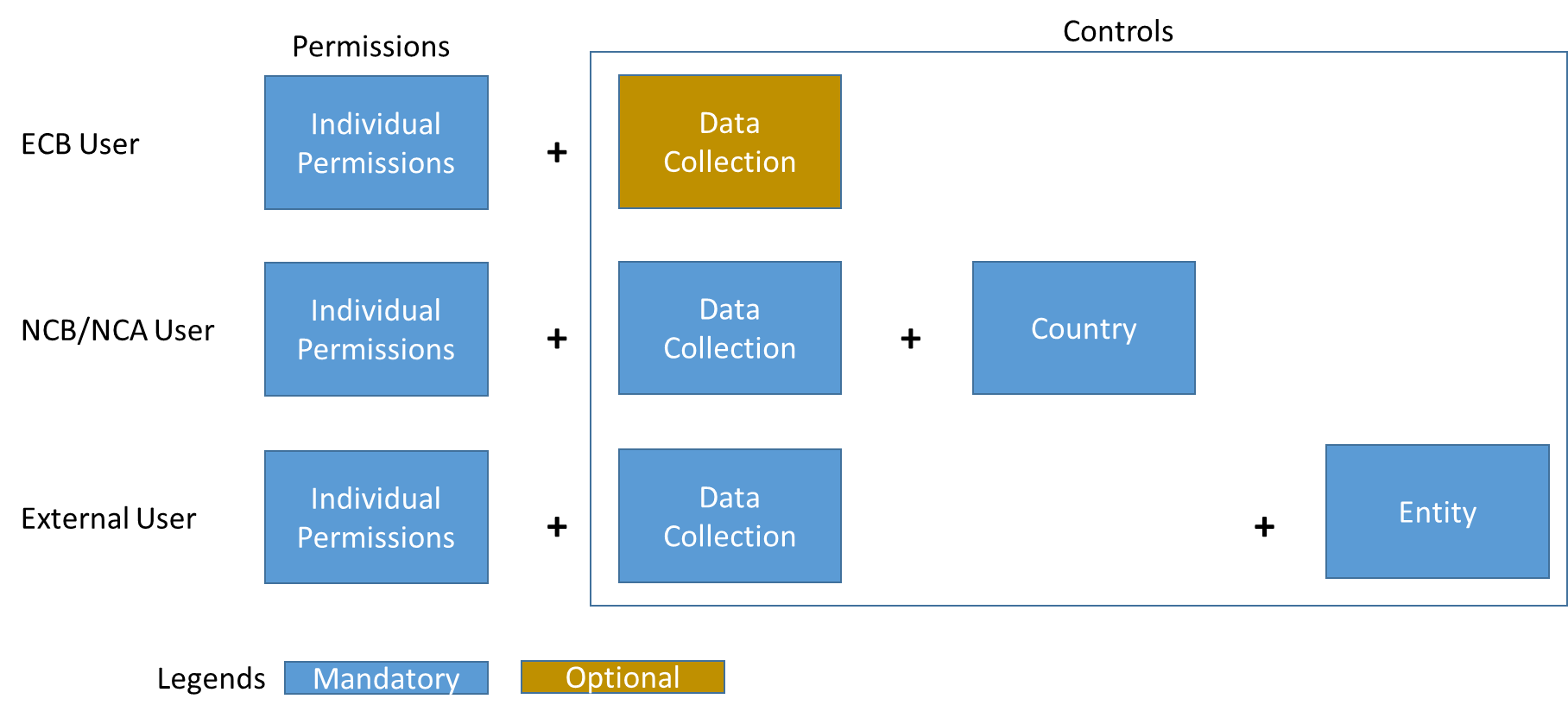
**Example of Permissions:**

* As a collection designer, user can add new Entity Group. So if this permission is given, then only user can add entity group.

**Example of Controls:**

* As a collection designer, specific user can do data collection preparation only for specific data collection.
* As a NCB data submitter, user can only submit data for entities of its countries.

Together with permissions & controls, CASPER will perform access management.



Next sections explains how permissions & controls are designed and implemented in CASPER

# Assigning roles & controls to the CASPER user

Roles (group of permissions) and controls are assigned to CASPER user using “Assign Roles to user” screen.

Below sub-topics further elaborates how this will be done:

## Identifying user type

There will be 4 types of Users in ECB.

Following way those will be identified in CASPER.

|  |  |  |  |
| --- | --- | --- | --- |
| User Type | Entry Via | Identification Logic | Remarks |
| ECB User | IAM | * Employee Type = “ESCB” * Country != “EU” | Non-ESCB users also are in IAM as per IAM design document.  Assumption: CASPER do not plan to onboard “non ESCB user” via IAM |
| NCB/NCA User | IAM | * Employee Type = “ESCB” * Country != “EU” |
| External users:   * EU Institutes * Companies representing Reporting entities * Individual entities | iWelcome | To be defined in release 2.0 |  |

## Various roles in CASPER

CASPER roles are driven by IAM roles as they are configured in IAM.

Business will be able to introduce any new role in IAM. Once role is introduced, this role will be reflected in CASPER based on IAM synchronization in CASPER.

Below are currently configured roles in CASPER

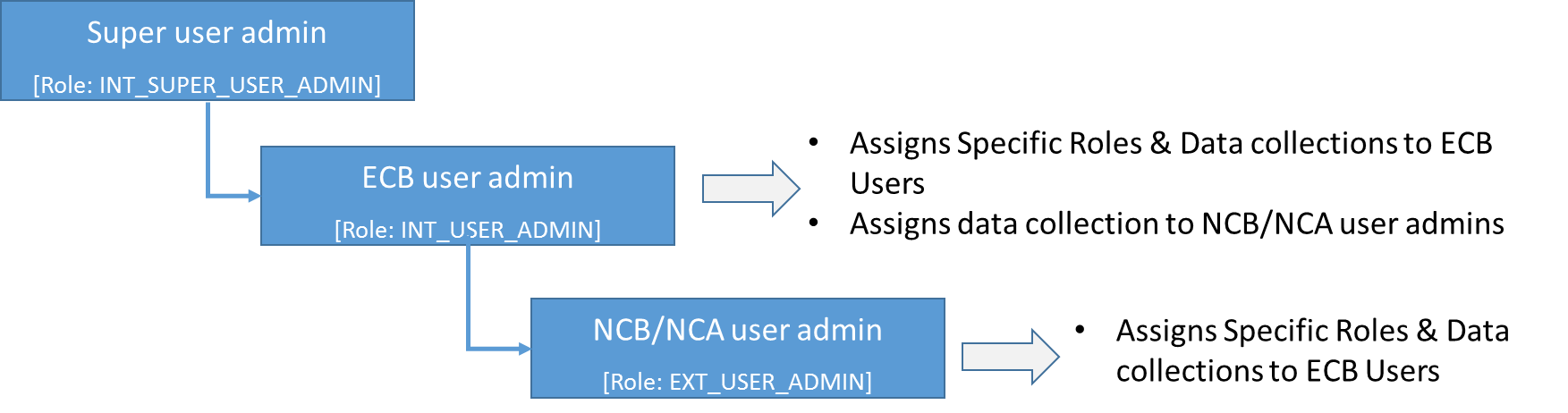
|  |  |
| --- | --- |
| Role | Role Details |
| INT\_COLLECTION\_APPROVER | ECB Data Administrator |
| INT\_COLLECTION\_DESIGNER | ECB Data Expert |
| INT\_COLLECTION\_USER | ECB Data Service Expert |
| EXT\_DATA\_SUBMITTER | NCB/NCA Data Submitter |
| EXT\_SUBMISSION\_APPROVER | NCB/NCA Manager |
| INT\_SUPER\_USER\_ADMIN | ECB Super User Admin |
| INT\_USER\_ADMIN | ECB User Administrator |
| EXT\_USER\_ADMIN | NCB/NCA User Administrator |
| INT\_TECHNICAL\_USER | Technical User for ECB integrations |
| EXT\_TECHNICAL\_USER | Technical User for NCB/NCA integrations |
| INT\_SYSTEM\_SUPPORT | ECB System Support team |

CASPER user can have one or more roles assigned in IAM.

Data Administrator assigns permissions to each role using “Roles to Permissions assignment” screen.

## Role of user administrators in CASPER

CASPER will have various types of user administrators as follows:



Details of the roles and responsibilities are follows:

|  |  |  |
| --- | --- | --- |
| User Administrator Type | Role | Roles & Responsibilities |
| Super user administrator | INT\_SUPER\_USER\_ADMIN | * Assign data collection to the ECB user admin so that he/she can further perform user management specific for that data collection |
| ECB user administrator | INT\_USER\_ADMIN | * For the assigned data collection, ECB user administrator does user management of ECB users * For the assigned data collection, ECB user administrator does user management of NCB/NCA user administrators |
| NCB/NCA user administrator | EXT\_USER\_ADMIN | * For the assigned data collection, NCB/NCA user administrator does user management of their own resources (same country users) |
| External users administration will be added in release 2.0 | | |

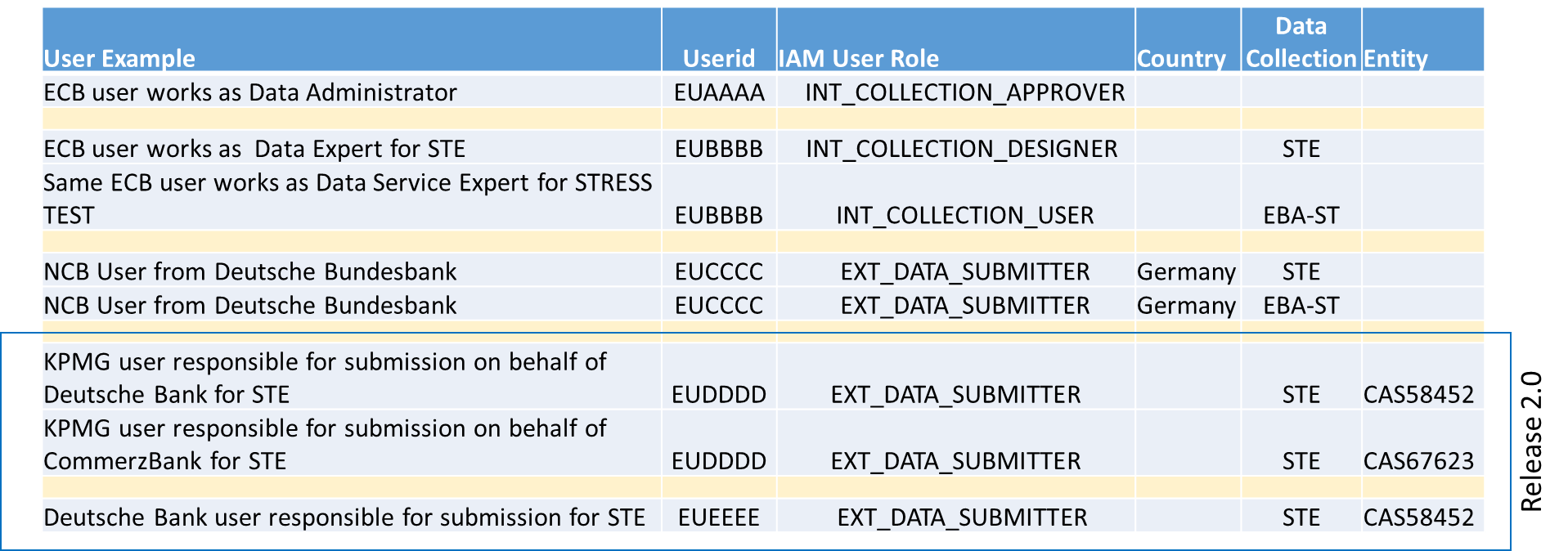
## Mechanism of roles and controls assignments to CASPER user

Each user gets one or more IAM role assigned.

Using “User Assignment” screen, user administrator assigns specific controls to the user as follows:

* CASPER role (coming from IAM)
* (Optionally) data collection for the activities which are linked to data collections
* (Only for NCA/NCBs) Country (coming from IAM. Important for limiting scope of NCAs/NCBs)
* (Only for external submitters) Entity (Release 2.0)

Demonstration example:



## Managing user assignments

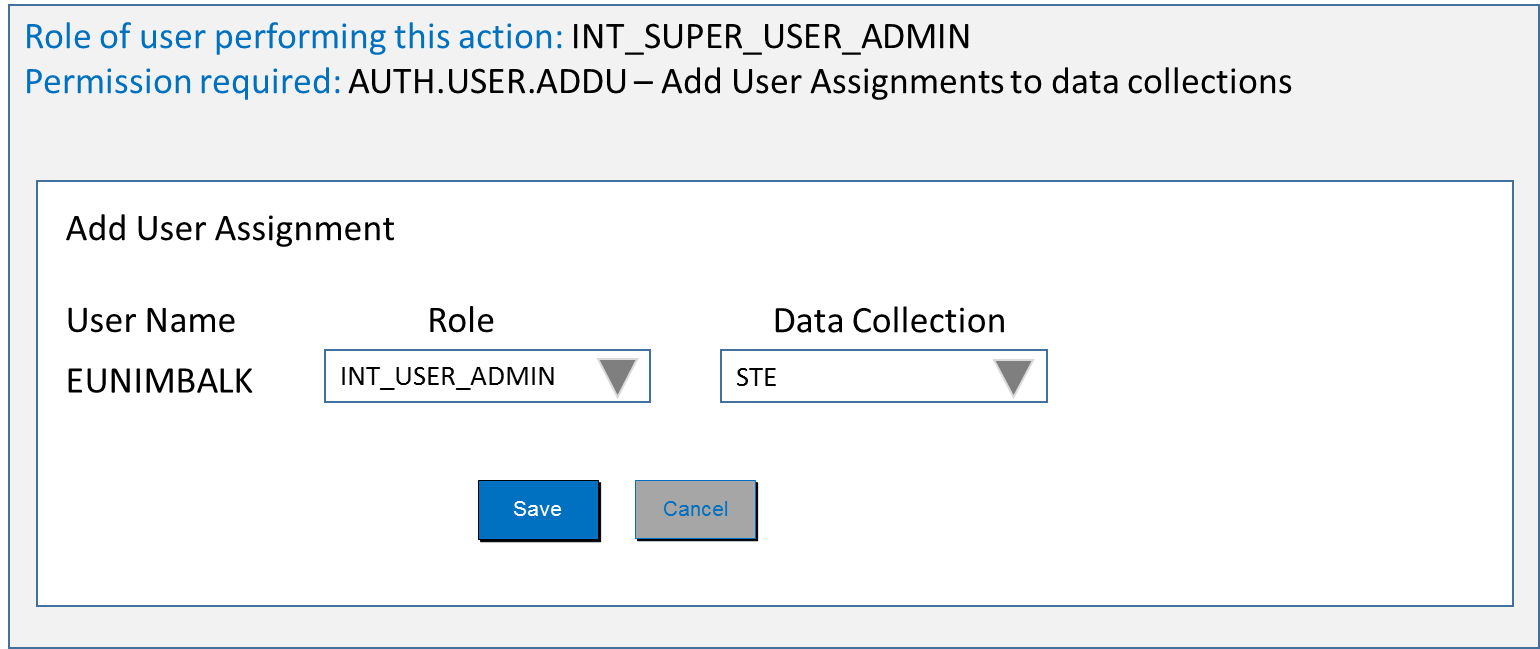
User assignment will have following behaviour based on type of user administrator as logged in user.

Following will be expected permissions assignment per user admin role

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Category | Permission code | Permission Name | INT\_SUPER\_USER\_ADMIN | INT\_USER\_ADMIN | EXT\_USER\_ADMIN |
| ECB Super User Admin | ECB User Administrator | NCB/NCA User Administrator |
| Authorisation | AUTH.PERM | Assignment of Permissions to Role | X |  |  |
| Authorisation | AUTH.USER | Manage User Assignments to data collections | X | X | X |
| Authorisation | AUTH.USER.ADDU | Add User Assignments to data collections | X | X | X |
| Authorisation | AUTH.USER.EDTU | Edit User Assignments to data collections | X | X | X |
| Authorisation | AUTH.USER.DLTU | Remove User Assignment for data collections | X | X | X |

### User assignments by Super user administrator

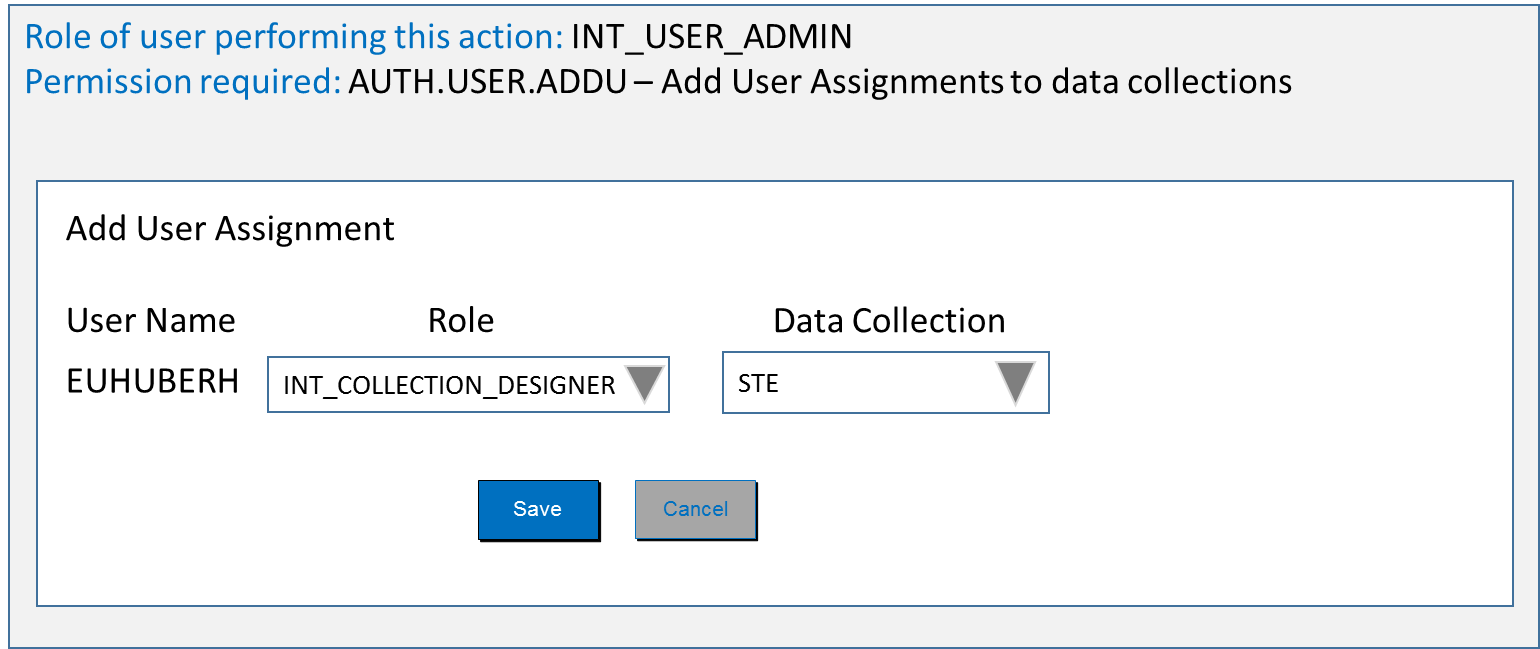
Super user will be able to provide access to ECB User Administrators for a specific data collection.



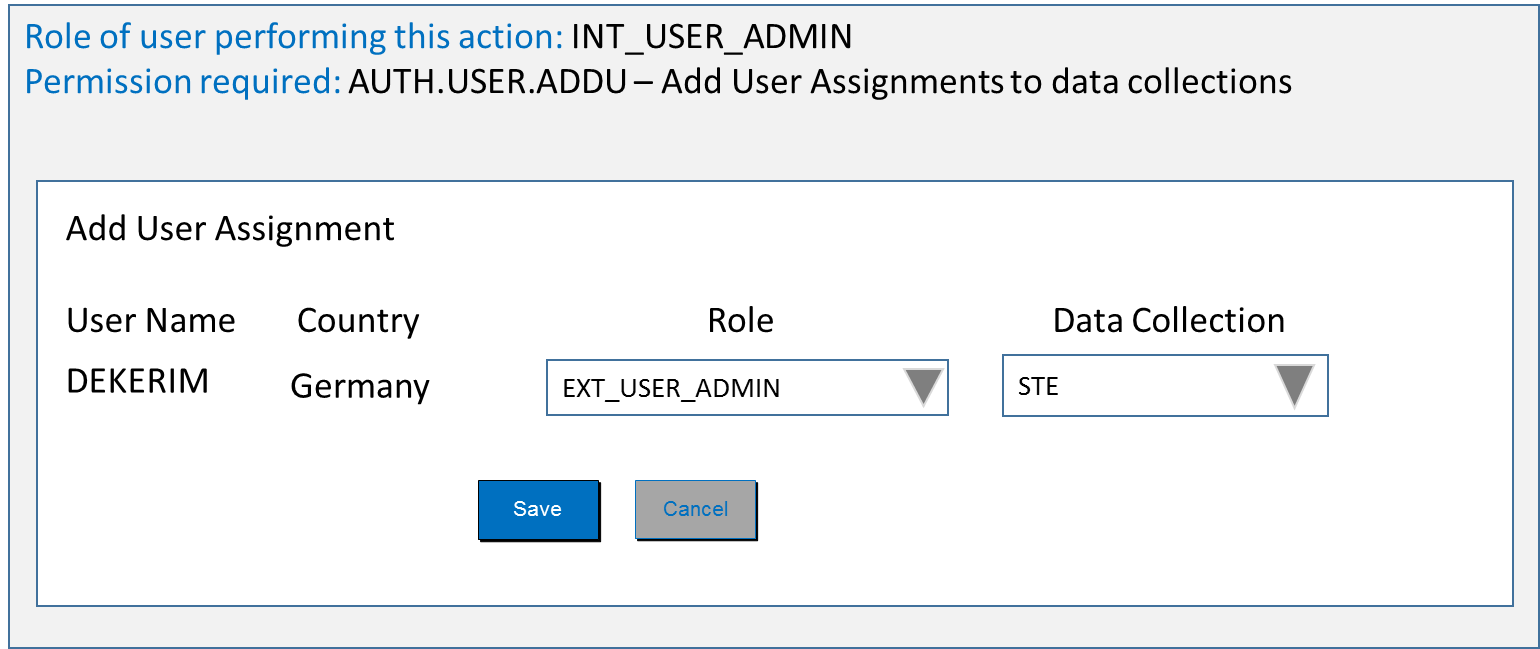
Super user admin can also provide individual accesses (e.g. assigning Data designer role to ECB user) if wish. But this is not desired activity by super user admin.

### User assignments by ECB user administrator

ECB user administrator will be able to assign specific role to the other ECB users for a specific data collection.



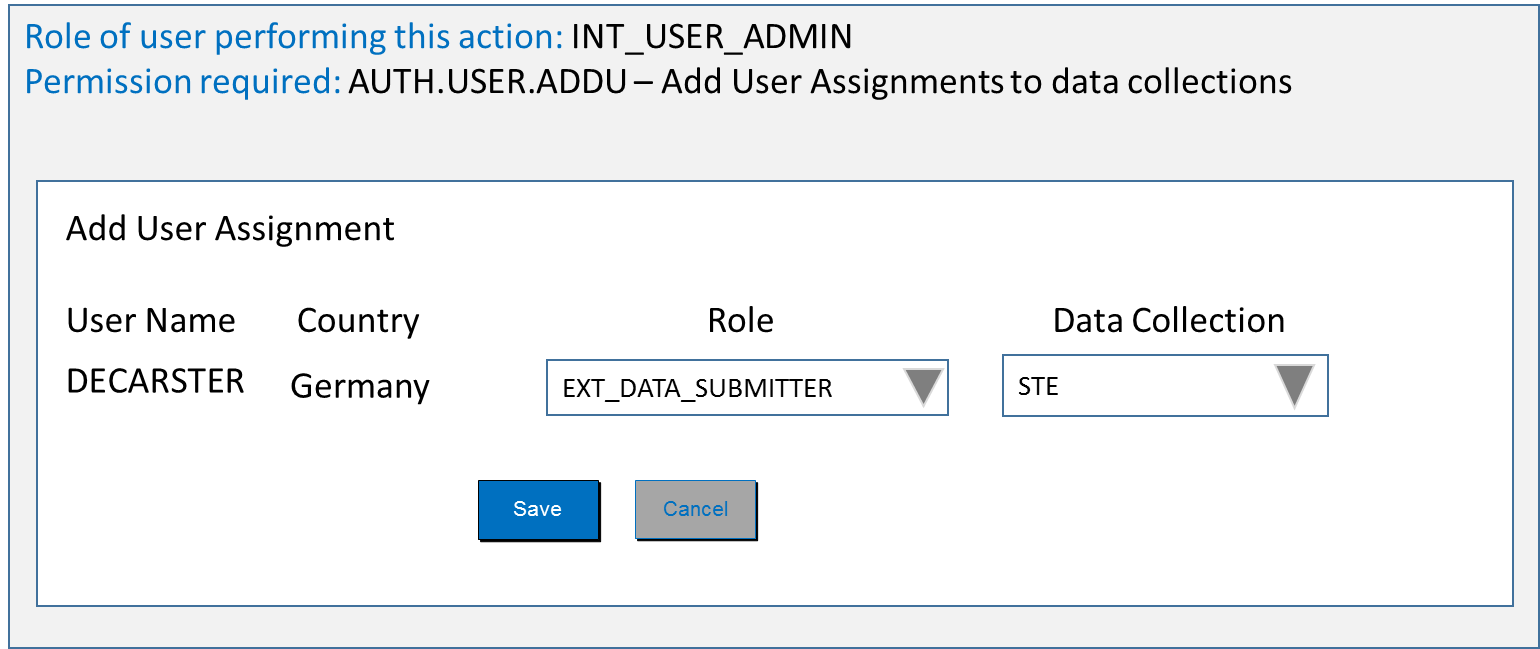
Similarly ECB user administrator will also be able to assign User admin role to the NCB/NCA users for a specific data collection.



ECB user admin can also provide individual accesses to NCB/NCA users (e.g. assigning Data designer role to NCB/NCA user) if wish. But this is not desired activity by ECB user admin.

### User assignments by NCB/NCA user administrator

NCB/NCA user administrator will be able to assign specific role to the other ECB users for a specific data collection.



## Managing Exceptions in given design construct

* 1. NCB/NCAs are responsible for submitting data for the entities which has country same as that NCB/NCA. But there can be an exception in few data collections. E.g. Malta entity submission is done by Italian NCB.

In this scenario, each Malta entity should have country as Italy and also there should be additional attribute like “Original Country” and there Malta can be put.

# Assigning & executing permissions in CASPER

In section 2, we assumed that specific group of permissions are already assigned to specific CASPER role and then how user administrators are able to assign those roles to specific users.

This section will cover:

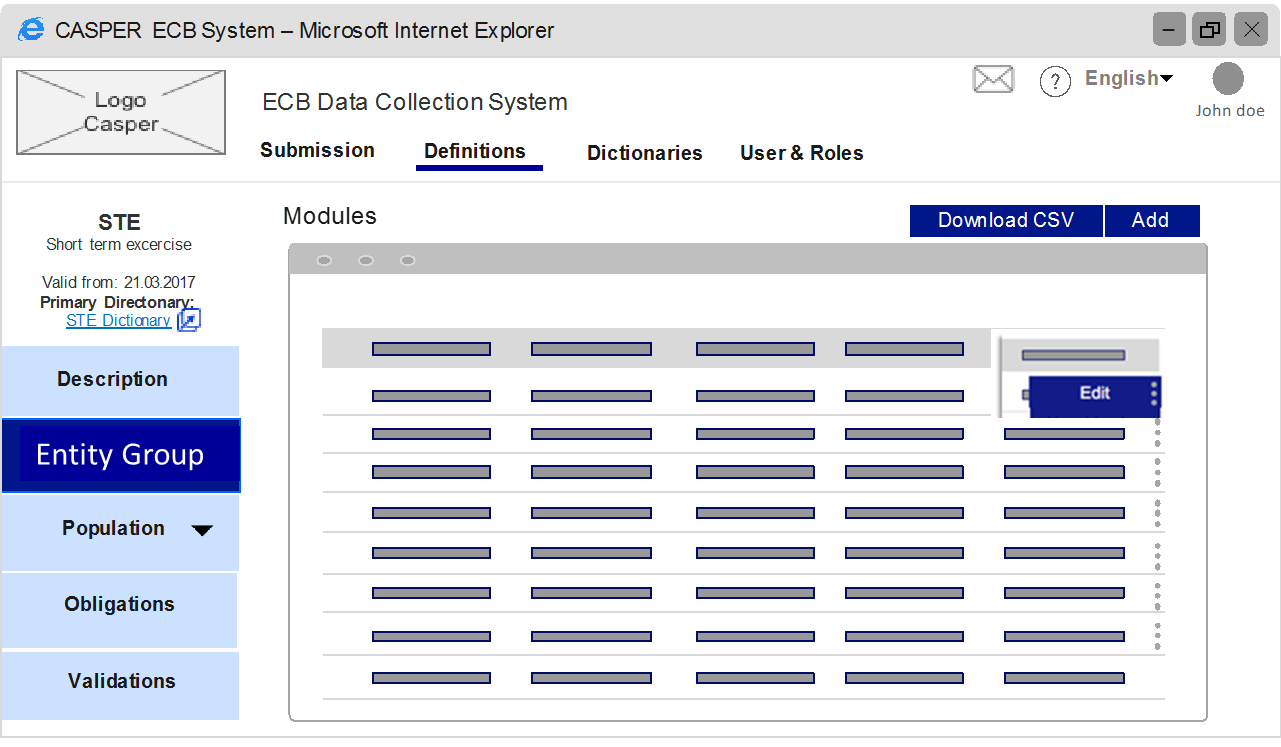
* Introduction to permissions in CASPER
* How permissions are assigned to specific role
* How permissions controls CASPER user’s access to specific task

## Permissions in CASPER

User will be performing specific task in CASPER only if he/or she is having permissions to do so. These tasks can be controlled at 4 levels.

[Technically CASPER will be able to handle nth level, as actual permission execution is always happens at macro level. For the simplicity, we limit to 4 levels]

For the demonstration, consider below re-presentation, where user wants to perform activities related to “Manage entity group” and those activities are mainly view, add and edit.



To perform this task, user need to:

* click on “Definitions” from top navigation
* then list of data collections will appear, from where he/she select appropriate data collection
* then user will be able to see left hand navigation where he can see “Manage Entity Group”. User clicks on this menu
* then user see list of entity groups which exists for that data collection.
* User can add new entity group or can edit existing one.

**Which roles can do these tasks**?

* If the user is data collection designer, then only he/she will be able to see definitions
* ECB Data Administrator can also perform this operation
* whereas ECB Data Service Expert & others will not be able to these tasks

**What permissions are required to perform these tasks?**

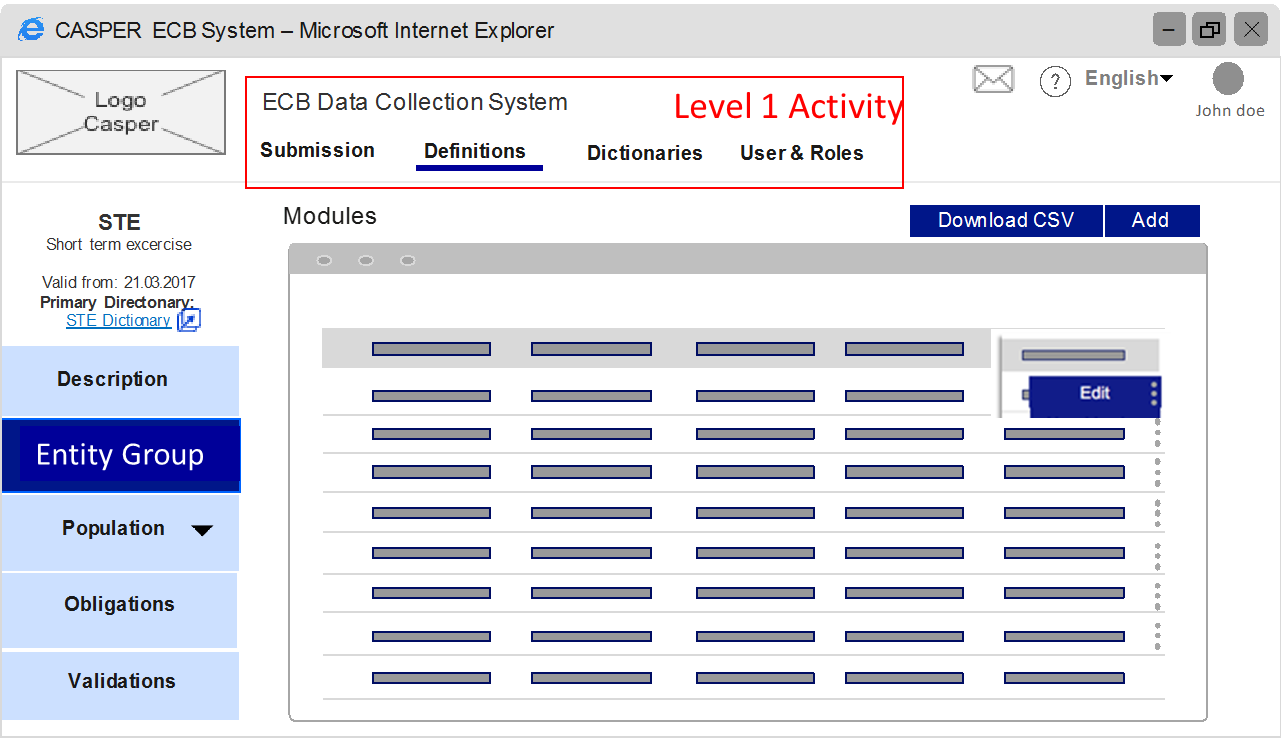
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Category | Permission code | Permission Name | INT\_COLLECTION\_APPROVER | INT\_COLLECTION\_DESIGNER | INT\_COLLECTION\_USER |
| ECB Data Administrator | ECB Data Expert | ECB Data Service Expert |
| 1 | 2 | 3 |
| Collection preparation | DTDF | Data Definitions | X | X |  |
| Collection preparation | DTDF.ENGR | Manage Entity Group | X | X |  |
| Collection preparation | DTDF.ENGR.ADDG | Add Entity Group | X | X |  |
| Collection preparation | DTD.EGR.EDTG | Edit Entity Group | X | X |  |

**How permissions are executed?**

1. **Level 1 Activity control by applying permissions**

If the user having “*DTDF - Data Definitions*” permission via any role, he/she will be able to see “definitions” menu in top navigation.

For others this menu will not appear itself.

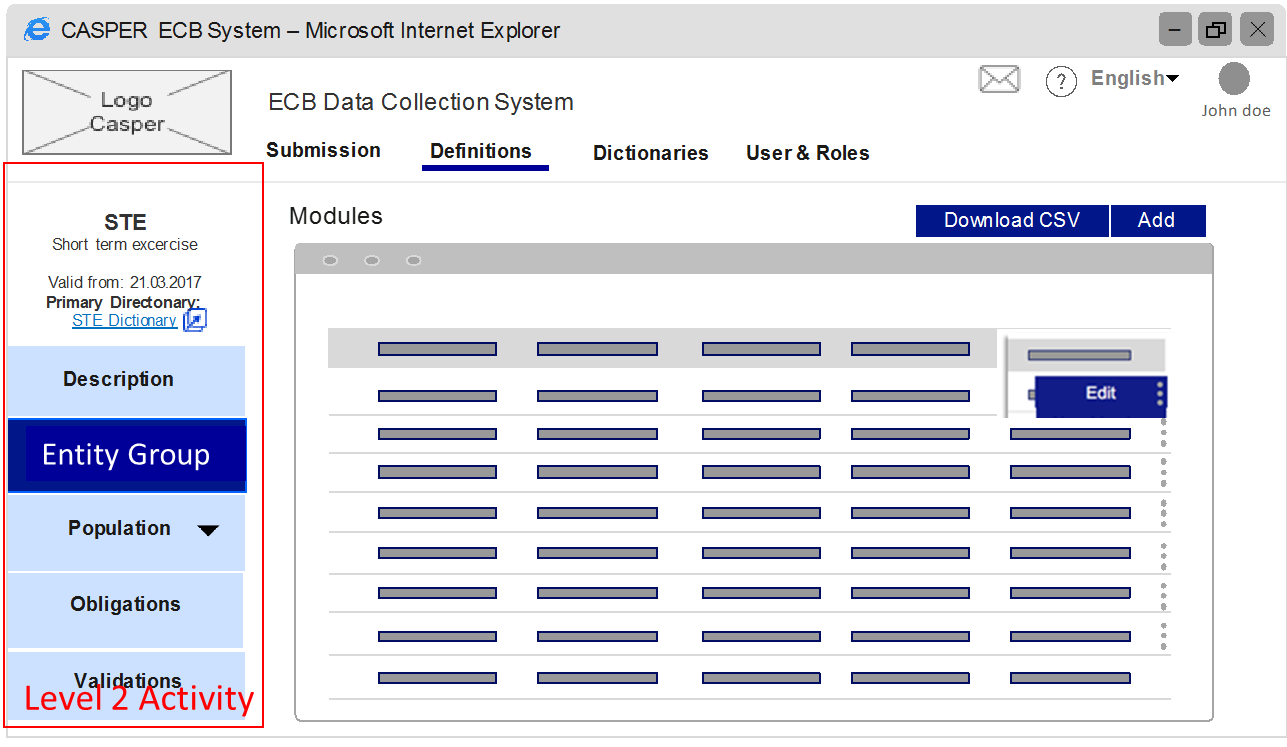


1. **Level 2 Activity control by applying permissions**

If the user having “*DTDF.ENGR - Manage Entity Group*” permission via any role, he/she will be able to see “Entity Group” menu in side navigation.

For others this menu will not appear itself.

When user is having permissions to this level, user have implicitly permission for previous level



Based on Level 2 activity, middle screen will appear for appropriate action e.g. View Entity group”. Where Level 2 is not relevant, after clicking on Level 1 itself, middle screen can appear.

1. **Level 3 Activity control by applying permissions**

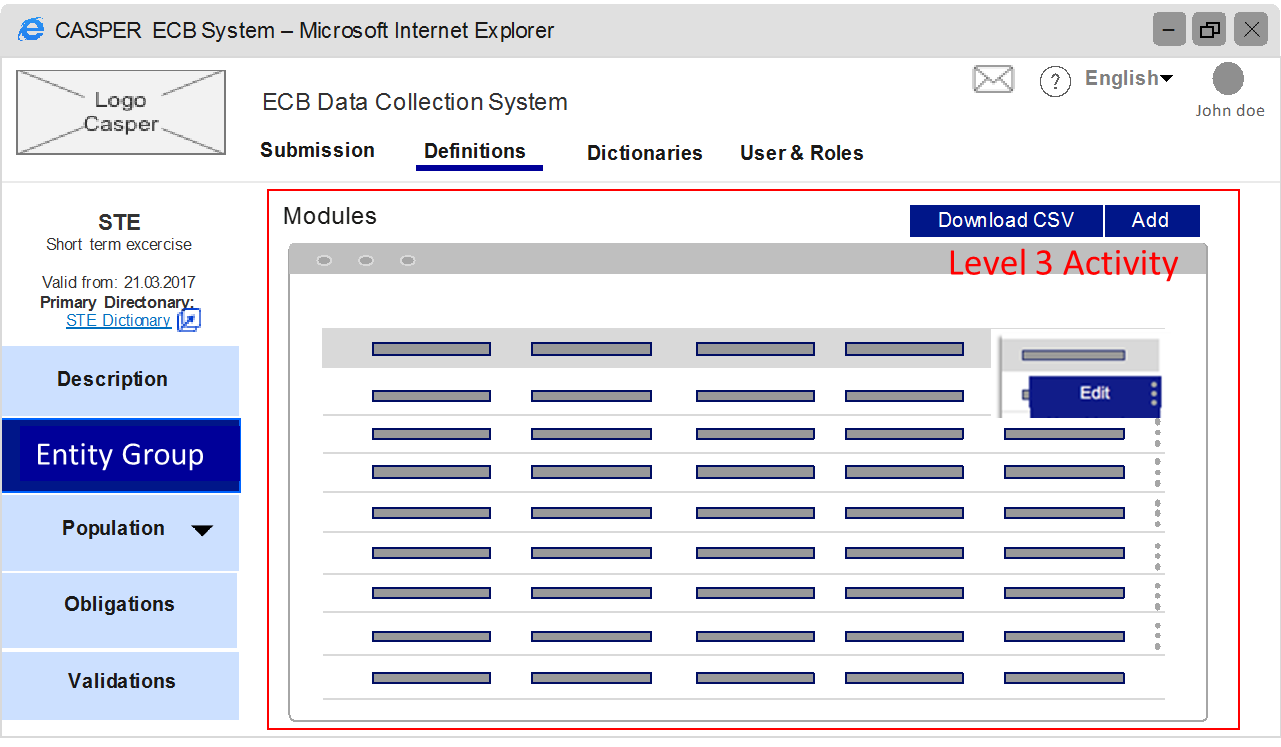
Based on Level 2, “Entity group view” screen appeared with list of already existing entitiy groups.

Now user’s activity of “Add new entity group” or “edit existing entity group” is controlled by Level 3 permissions

* If the user having “*DTDF.ENGR.ADDG- Add Entity Group*” permission via any role, he/she will be able to see “Add” button on screen.
* If the user having “*DTD.EGR.EDTG- Edit Entity Group*” permission via any role, he/she will be able to see “Edit” option for inline edit.

For others this menu will not appear itself.

When user is having permissions to this level, user have implicitly permission for previous level



1. **Level 4 Activity control by applying permissions**

Specific changes within the level3 action can be controlled by Level 4 permissions. E.g. any user can change status A to Status B, but only specific user can change status A directly to Status Z.

Those will be very rarely used in CASPER.

User having specific permissions will be able to perform this task whereas others will get either error that “You are not Authorised to perform this change” or option will not be visible, depending on the design of that screen.

When user is having permissions to this level, user have implicitly permission for previous level

## Assigning permissions to role in CASPER

ECB super user admin with permission “assign permissions to role” will be able to perform assignment.

|  |  |  |  |
| --- | --- | --- | --- |
| Category | Permission code | Permission Name | INT\_SUPER\_USER\_ADMIN |
| ECB Super User Admin |
| 6 |
| Authorisation | AUTH.PERM | Assignment of Permissions to Role | X |

Tree structure based screen will help super user admin to perform this configuration.

When upper level is selected, system will select all lower levels of permissions.

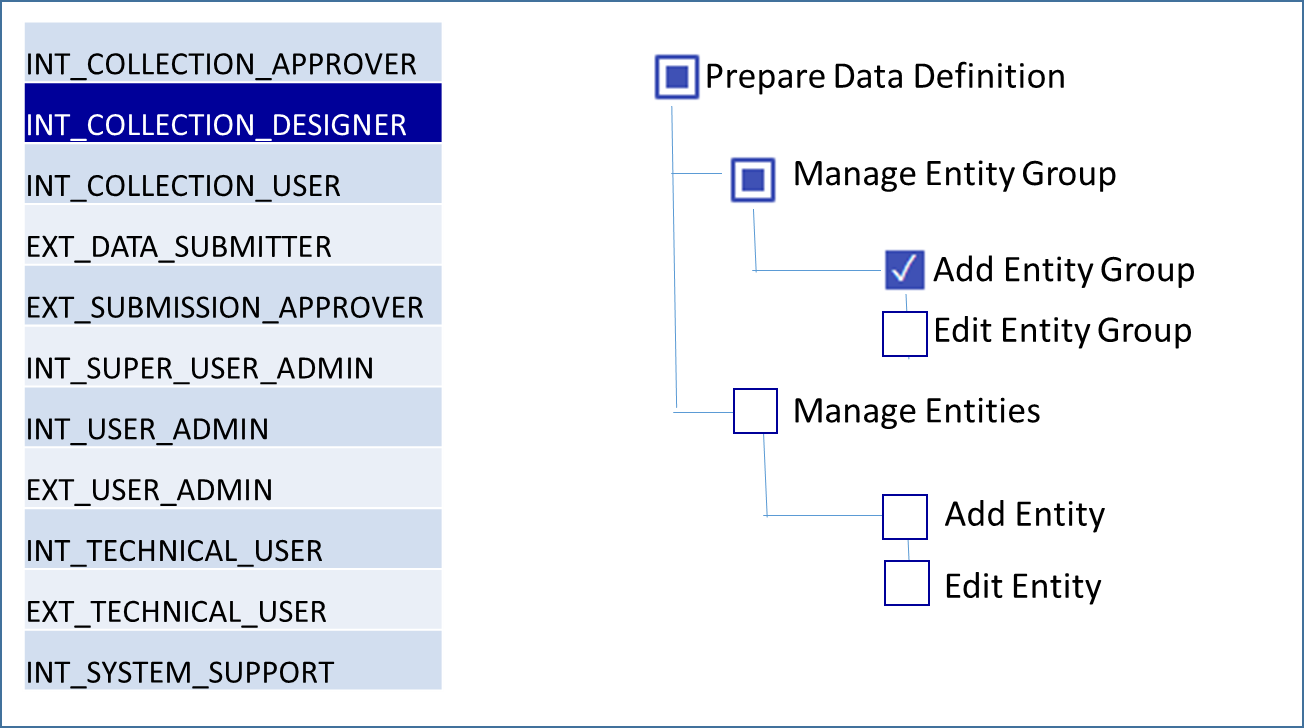
Note: Below are 2 approaches for populating role list in this screen

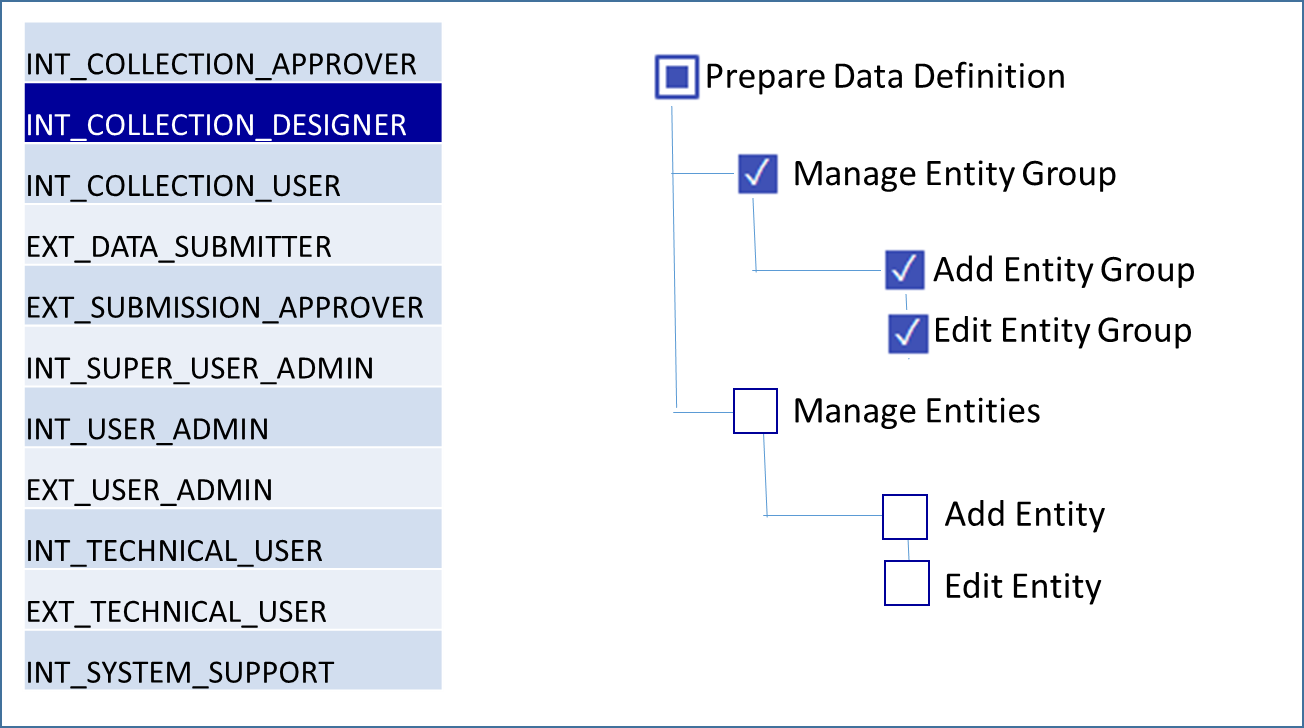
**Apporach1**: Left hand side list of roles is populated as distinct list of all roles of all users replicated from IAM (and in release 2.0 from iWelcome). So if any specific role is not used for any user, said role will not be visible for configuration. With this any new introduction of role is automatically reflected

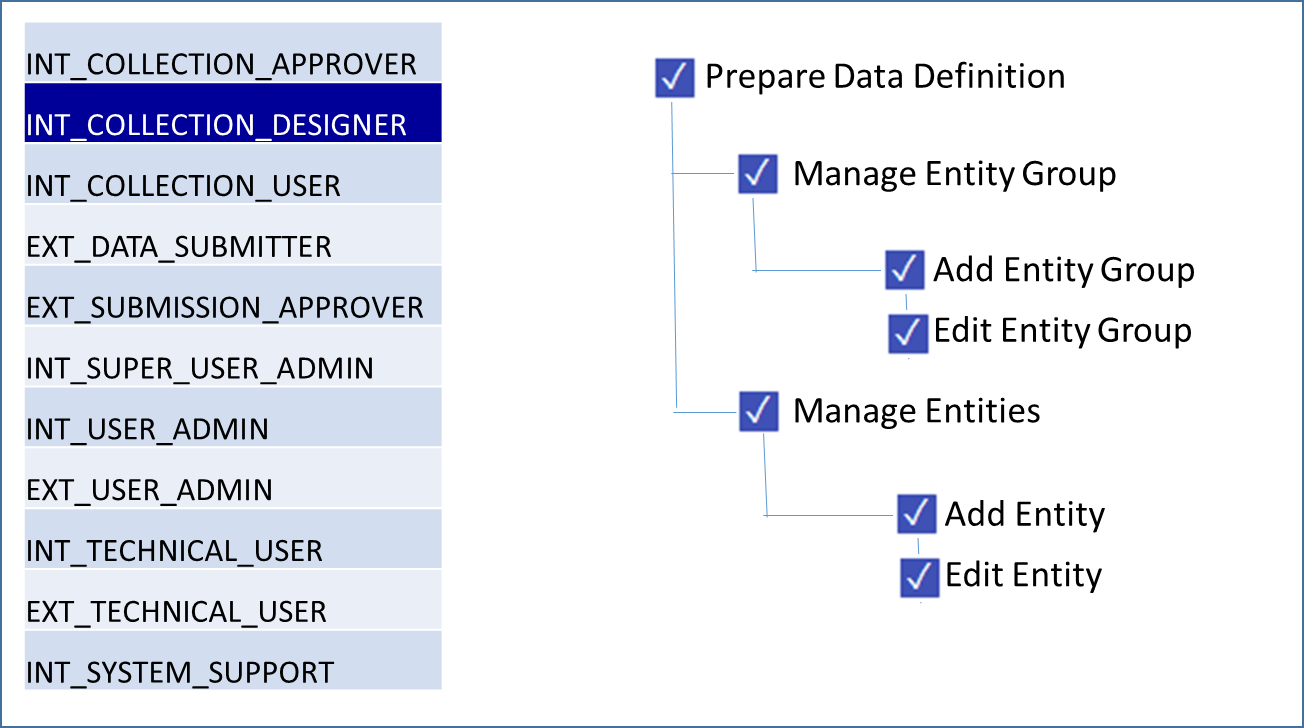
**Approach 2**: List is defined & configured in database. But in this case new role will need to be added in configuration table.

**CASPER will follow Approach 1**.

Pictorial representation of this assignment is depicted as below:







## Technical Approach for Assigning permissions to role in CASPER

Database will maintain permissions master with permission code, name, level & sequence.

* Level will be used to render tree structure
* sequence will be used to arrange items in order at same level

Example as follows:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Category | Permission code | Permission Name | Level | Sequence |
| Authorisation | AUTH | Users & Roles | 1 | 4 |
| Authorisation | AUTH.PERM | Assignment of Permissions to Role | 2 | 1 |
| Authorisation | AUTH.USER | Manage User Assignments to data collections | 2 | 2 |
| Authorisation | AUTH.USER.ADDU | Add User Assignments to data collections | 3 | 1 |
| Authorisation | AUTH.USER.EDTU | Edit User Assignments to data collections | 3 | 2 |
| Authorisation | AUTH.USER.DLTU | Remove User Assignment for data collections | 3 | 3 |

Permissions are validated based on permission code.

**Permission code will have specific format as follows:**

* Each Permission code is unique in CASPER & 2 codes cannot be the same irrespective of category, level etc.
* Each level is represented by 4 letters.
* Each level is separated by dot (.)

**Purpose of specific format:**

This format will be used for pattern based search.

e.g. User who has permission “AUTH.USER.ADDU (Add User Assignments to data collections)” will implicitly have permission for

* “AUTH (Users & Roles)” and
* “AUTH.USER (Manage User Assignments to data collections)”.

So when CASPER is checking if user has “AUTH” permission, it will scan user’s assigned roles and permissions assigned to them and check if any permission matches “AUTH%”.

Since user is having already “AUTH.USER.ADDU” permission, user has implicitly “AUTH” permission, and on top menu “Users & Roles” option will appear.

## Applying permissions & controls to each task of CASPER user

Each User is assigned with specific role and with which he/she gets specific sets of permissions. These permissions enables him/her to perform allowed tasks

Additional controls like data collection, country, entity further restricts operations of user to the allowed set of data.

Permissions are generally applied for specific operations user is going to perform like:

* View
* Add
* Edit
* Delete
* Create new version

CASPER will use permissions while rendering UI to display /hide specific operation. E.g. if no add permission attached to user role then user will not see “Add button”.

Also which performing database operations like insert, update, delete, same permissions will be checked.

## Technical approach for applying permissions & controls to each task of CASPER user

Below technical approach is explained on logical tables’ level, technical team will enhance approach with physical table details

1. “Roles to permissions” mapping will populate bridge table once ECB super user admin updates mapping.

|  |  |
| --- | --- |
| Role | Permission |
| INT\_COLLECTION\_DESIGNER | DTDF |
| INT\_COLLECTION\_DESIGNER | DTDF.ENGR |
| INT\_COLLECTION\_DESIGNER | DTDF.ENGR.ADDG |
| INT\_COLLECTION\_DESIGNER | DTDF.ENGR.EDTG |

2. Each User is assigned with specific role and with which he/she gets specific sets of permissions. Also user is linked witih specific controls for that role.

This is performed as a part of “Manage User Assignments to data collections”.

Following way this information will be available in database

Entity control will be added in release 2.0

|  |  |  |  |
| --- | --- | --- | --- |
| userid | Role | User Country | Data collection |
| EUNIMBALK | INT\_COLLECTION\_DESIGNER |  | STE |
| EUNIMBALK | INT\_COLLECTION\_USER |  | EBA-ST |
| EUHUBERHE | EXT\_USER\_ADMIN | DE | STE |
| EUHUBERHE | EXT\_DATA\_SUBMITTER | DE | STE |

3. For each screen, there will be certain set of permissions required to perform various tasks.

e.g. Manage Entity group screen will have 2 operations & will need following permissions for the same.

|  |  |
| --- | --- |
| Permission code | Permission Name |
| DTDF.ENGR.ADDG | Add Entity Group |
| DTDF.ENGR.EDTG | Edit Entity Group |

4. When the screen is triggered, Generalized function will bring result whether said permissions are allowed for the user or not.

**Function**: **IsPermissionValid** (UserID, PermissionCode, DataCollection, Country)

**Return**: Y (if permission) / N (if no permission)

**Logic**:

* 1. For each permission, **IsPermissionValid** function is triggered passing all parameters
  2. System gets all the roles assigned to the UserID passed for which said DataCollection and Country is mentioned.
     1. There are few tasks are performed in CASPER which are not DataCollection specific e.g. ECB Data Administrator.

(INT\_COLLECTION\_APPROVER) will create new data collection

In this case said user have entry for Role where data collection will be blank, so same logic works.

* + 1. For ECB users country field will be blank, so same logic works
  1. If no role is received, no further steps required and system returns “N” as permission does not exists.
  2. If one or more roles are received, System takes all the permissions assigned to all roles received from “Permissions to Role” bridge table.

In the retrieved permissions list, system checks if permission pattern exists as “PermissionId%”. So if same permission do not exists but its lower level permission is exists then also condition is satisfied.

* 1. If permission is found then system returns “Y” as permission does exists.
  2. If permission is not found then system returns “N” as permission does not exists.
  3. UI gets PermissionCode & Result as input
  4. While screen rendering, UI checks if permissionCode is “Y” then it renders action. E.g. if “Add Entity Group” permission is returned as “Y”, then “Add” button is displayed on “View Entity Group” page

With this approach, UI coding becomes simpler & their behaviour is controlled by “Y” & “N” flag based results.