Security Level Management

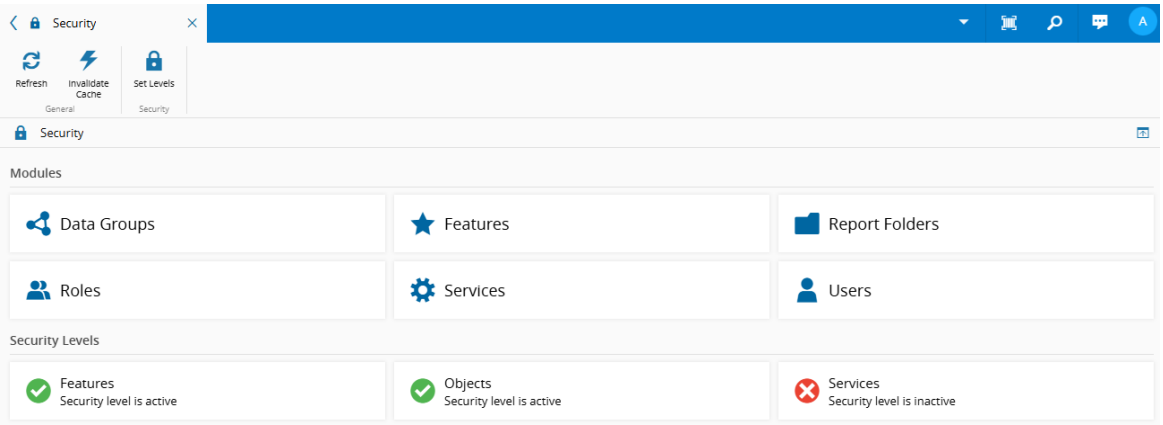
Security Overview

The **Security** section in MES allows you to manage user accounts and group them into roles. Each role is assigned a specific set of permissions, determining what users can see or do within the system - such as accessing specific entities within the MES or performing operations. In addition to granting and restricting access, it is also possible to define its granularity. These layers are configured through the **Set Levels** button on the top ribbon. For more information, see Security Levels.

Security Page

The Security Page is available within the **Administration** menu and is divided into **Modules** and **Security Levels**:

- **Modules** - used to create users and assign them to roles. Each role grants access to specific Features, Data Groups, Report Folders, and Services - either preconfigured or already system-defined.
- **Security Levels** - controls the desired security granularity. It is possible to use only the Features level, limiting access to them, or increase the detail using Data Groups (for objects) and Services.



Info

For more information, see the Security section of the User Guide.

The creation of entities within **Modules** and the association between them can be consulted in the User Guide:

- Data Groups
- Features
- Report Folders
- Roles
- Services
- Users

Connecting the Entities

To access MES, a User must be created. This is the first step when using the security module. For users who intend to perform operations such as checking in a **Resource** or executing a **Maintenance Activity Order**, it is always necessary to create an **Employee** associated with that user. The relation between User and **Employee** is 1:1.

The second step is to define the set of users who perform the same function in the **Facility** and who, as such, will have the same privileges in terms of access to entities and operations in the MES. This set of users represents a **Role** in MES.

It is at the role level that access to features, data groups, services and report folders is assigned. All users within a given role inherit these accesses. Some examples of roles could be Operator, Process Engineer, or Quality Technician.

Subsequently, the roles will be configured when creating entities in MES, meaning that certain operations can only be performed by users assigned to that specific role. Some examples are described below:

- When defining a maintenance activity within the **Maintenance Plan**, it is necessary to configure an execution role. Therefore, only users within the configured role will be allowed to execute the **Maintenance Activity Order**.
- When defining a **Change Set**, it is possible to configure the role or set of roles that will be responsible for approving it.
- When defining a **Protocol**, it is necessary to create a workflow with several states, where each state is associated with a role. Users assigned to this role are responsible for performing all operations within that protocol state.

> **Note**
>
> The administrator role (defined in the configuration entry `/Cmf/System/Configuration/AdministrationRole/`) cannot override the roles configured on these entities.

Scenarios

This section presents a series of short videos demonstrating scenarios where different roles have varying access levels in MES. These examples help illustrate how the different security layers - features, data groups, report folders and services - affect user access and behavior within the system.

Assigning Different Features to Different Roles

In this scenario, we will demonstrate the different behavior allowed when assigning different roles in the MES. Here, we compare a Supervisor and an Operator role:

Role	Allowed Features
Operator	Basic tools required for processing materials, such as dispatching/track-in materials and track-out/move-next.
Supervisor	Additional capabilities, including the ability to abort a material, place it on hold, change the step/flow of materials, record loss/bonus, among others.

Table: Different features for different roles

To check which features are assigned to each user, go to **Administration** > **Security** > **Users**, select a user, and check the Features tab. For example, the Operator role only has 16 features assigned, while the Supervisor role has full access.

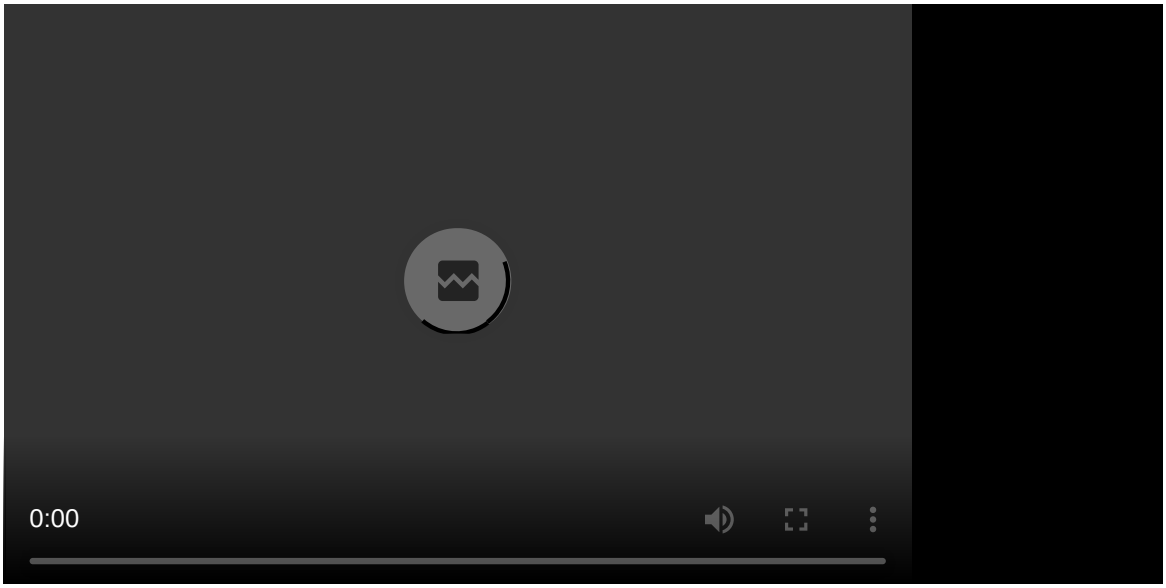
From the Operator perspective, after logging into the system, only the Business Data menu is visible in the navigation pane, with limited entities like Material and Step. When accessing a Step, the only operations available on the top ribbon are **Dispatch** and **Dispatch and Track-In**. All other operations are hidden due to lack of security feature.

If the operator performs a **Dispatch and Track-In** operation but then needs to take an action like **Abort**, they won't see the button in the top ribbon, as it is hidden due to their limited permissions. In this case, the operator must escalate the task to a Supervisor, who has the required features enabled to perform the action.

Switching to the Supervisor view, the difference becomes clear. The Supervisor sees a complete navigation pane with all MES entities visible. When opening the same step and selecting the same material, all actions (Abort, Hold, Change Flow, etc.) are visible and executable.

In this example, the Supervisor can abort the material using the **Abort** button, then proceed to **Track-In** the same material again, confirming that the operation is available only due to the security features assigned to his role.

The video below demonstrates how different features assigned to roles can control what users are allowed to do in the system.



Info

For more information, see How to: Create Roles, How to: Assign Roles to a User, and How to: Assign Users to a Role..

Assigning Different Data Groups to Different Roles

This scenario demonstrates how assigning different data groups can limit or grant visibility to specific entities in the MES.

Imagine two supervisors, each belonging to different business units:

- Supervisor 1 belongs to Business Unit A.
- Supervisor 2 belongs to Business Unit B.

Since Supervisor 1 from Business Unit A must not be able to perform any action on materials, resources, steps, and so on, that do not belong to his business unit (in this example, Business Unit B), it is necessary to restrict all of these entities by assigning them to different Data Groups.

Therefore, if a user is not assigned to the data group associated with a particular entity, that entity will either be hidden or masked (shown as `...`) in the interface. Furthermore, actions like dispatch or track-in will fail if attempted on an inaccessible resource. If there is no data group associated with an entity, all users will be able to view it.

From the Security page, under **Administration** > **Security** > **Users**, you can review the data groups associated with each user. For example:

- Supervisor 1 has access to Business Unit A data group.
- Supervisor 2 is assigned to Business Unit B data group.

> **Info**
>
> For more information, see Creating a Data Group and Assigning Roles to a Data Group.

If you log in as Supervisor 1:

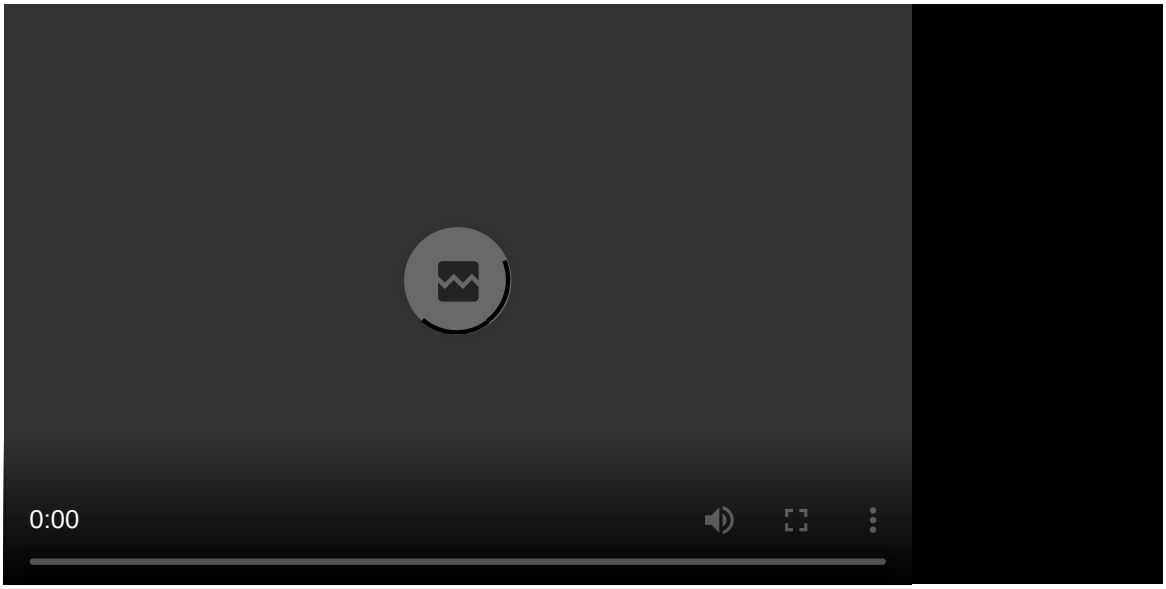
- You can view the Cookie BOM and the Baking Step because both are assigned to Business Unit A data group.
- During a **Dispatch and Track-In** operation, you only see the Oven Resource (associated with Business Unit A). The second resource, assigned to Business Unit B, appears masked by `...` and the details section is blank because, as Supervisor 1, you do not have access to the Business Unit B data group.
- Attempting to use the resource from Business Unit B will result in an error.

If you log in as Supervisor 2:

- You cannot see the Cookie BOM, as it is assigned to Business Unit A and, as Supervisor 2, you do not have access to this data group.
- In the BOM Context, you see that the Mixing Step has a BOM associate but you are not able to see the name (only `...`) due to lack of access to the corresponding data group.

If there are Smart Tables that do not have a data group associated and are visible to all users, some entities may appear restricted if they are associate with a data group for which you do not have access.

The following video explains the above scenarios.



Assigning Different Services to Different Roles

This scenario illustrates how services can provide a more granular level of control than features. We will demonstrate this by showing how even if a user has the feature to edit roles, they might still be restricted from specific operations - such as assigning users to roles - based on service-level permissions.

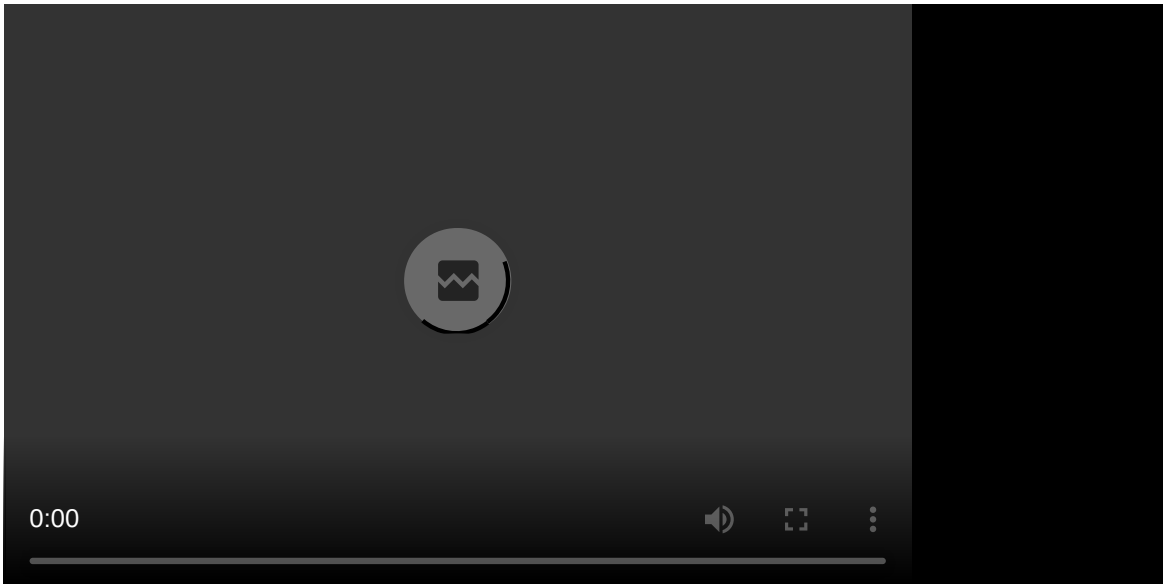
Suppose you have a role, such as CM Engineer, that is allowed to edit roles via the `Role.Edit` feature. This feature allows editing of all components in a role - users, services, features, and report folders. However, you want to limit certain users from assigning or removing members from a role, while still allowing them to modify the role's features or services.

In this case, simply removing the `Role.Edit` feature would be too broad. Instead, if you navigate to **Administration** > **Security** > **Services**, you see that you have a greater level of detail in the existing services, and you can remove the specific services responsible for managing members:

- Add Roles To User
- Add Roles To Users
- Add User Roles To Users
- Add Users To Role

Now, if you select a user without these four specific services, you will still have the option to Assign Users to Role because the `Role.Edit` feature was not removed. However, if you attempt to perform this operation, the system will throw an error because the CM Engineer does not have the necessary services to Assign Users to Role. And this is proof that services operate at a more granular level than features.

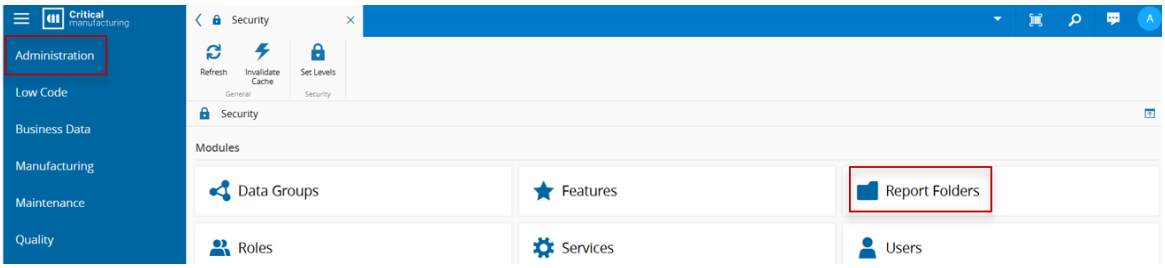
The following video shows how it is possible to restrict more specific operations using the service level, instead of just using the feature level.



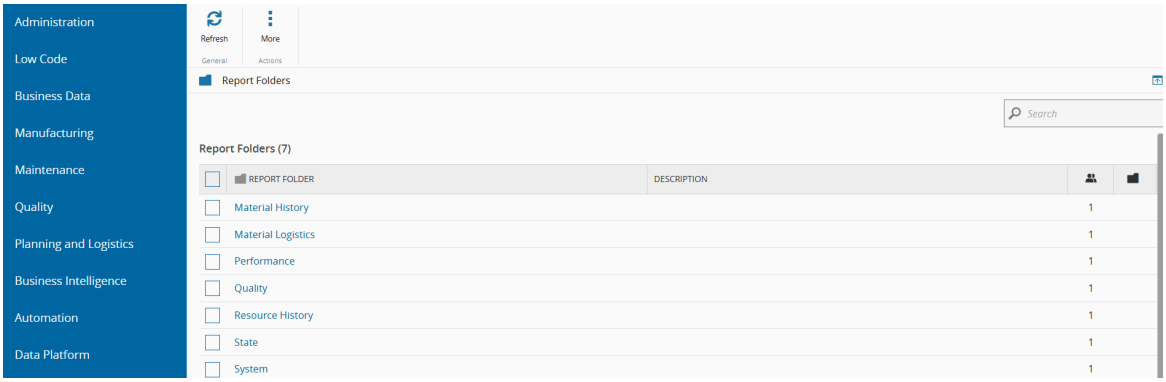
Assigning Different Report Folders to Different Roles

This scenario demonstrates how access to Report Folders in the Business Intelligence section of the MES can be controlled through role-based assignments.

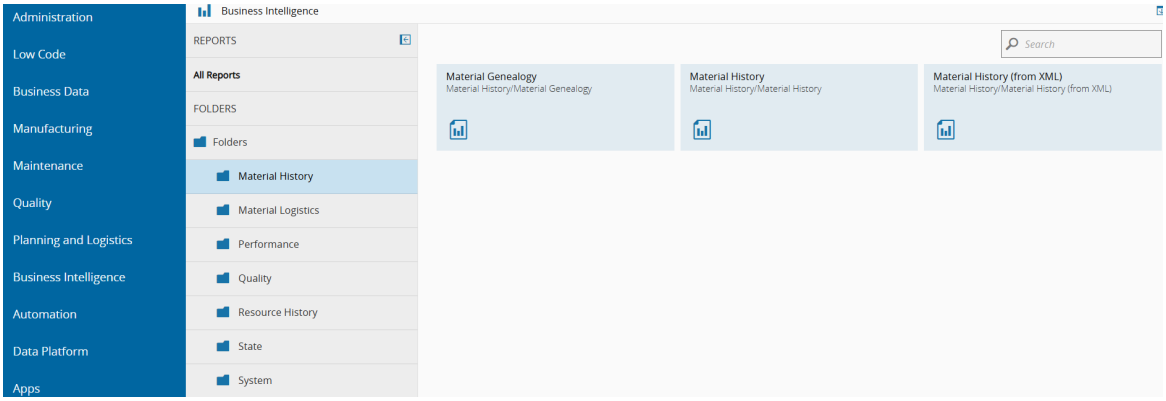
To access the list of Report Folders, navigate to **Administration** > **Security**, and select the Report Folders option under the **Modules** section.



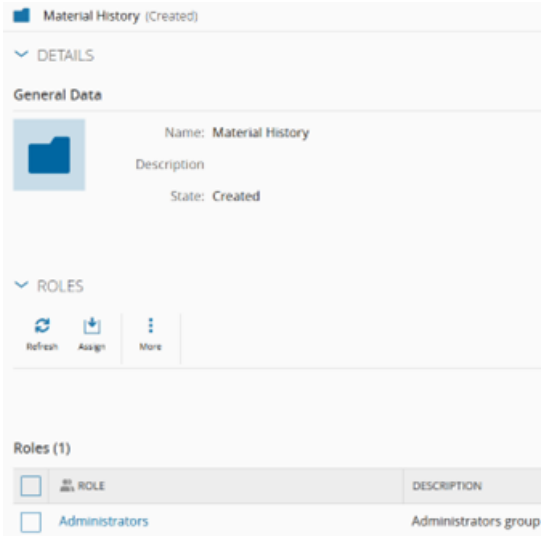
This will open the list of available report folders:



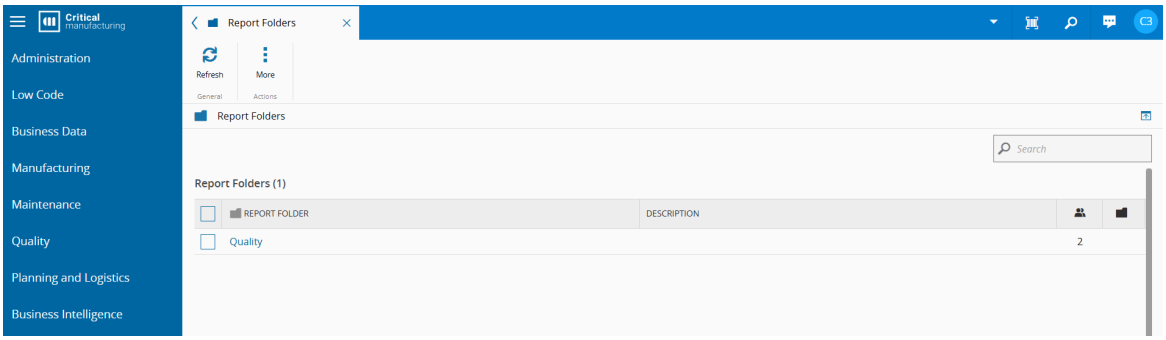
These folders correspond to the list of report folders found in the **Business Intelligence** menu.



Access to a Report Folder is restricted to users who belong to roles that have been explicitly assigned to that folder. Only these users will be able to view the folder and access the reports inside it.



If the user does not have permission to access a report, it will not appear under **Administration** > **Report Folders**. For example, if a user only has access to the Quality Reports folder, that will be the only one visible, as shown in the image below.



Additionally, if the user attempts to access a restricted report through Business Intelligence, the page will appear empty.

Exploring Data Group Access Types

This scenario highlights the difference between Read and Write access types within Data Groups, and how they affect what users can do with entities they have visibility over. For this purpose, the following roles will be used:

Role	Data Group access types
Operator BU-A	Data Group BU-A with access type = `read`
Process Engineer BU-A	Data Group BU-A with access type = `write` Data Group BU-B with access type = `read`

Start by navigating to **Administration** > **Security** > **Data Groups** and select Business Unit A. In this scenario, we added multiple roles to this data group, but only the Process Engineer and Supervisor have **Write Access**, while the Operator and Quality Engineer only have **Read Access**.

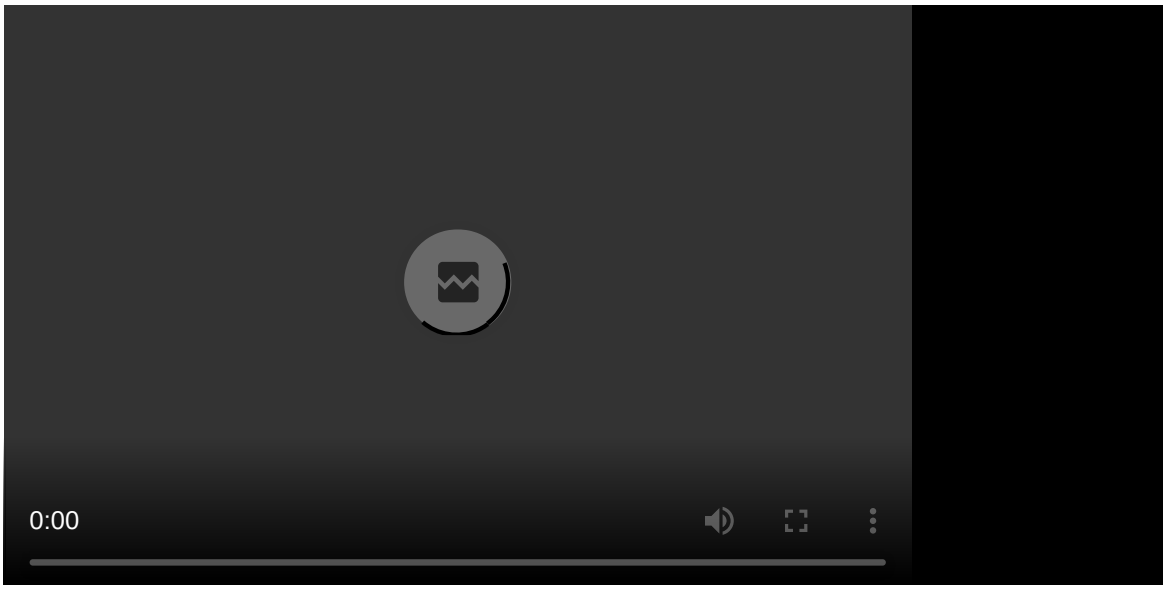
Let's first look at Operator001, with a Operator BU-A role, which has **Read Access** to the Business Unit A Data Group:

- When this user logs in and searches under **Business Data** > **Resources**, only resources belonging to Business Unit A are displayed.
- When selecting a resource, details are visible, but there is no **Edit** button - confirming that read-only access applies.

Now, consider the Process Engineer BU-A role, which has **Write Access** to the Business Unit A Data Group and **Read Access** to the Business Unit B Data Group:

- When a user with this role logs in and searches under **Business Data** > **Resources**, resources from both Business Unit A and B are display.
- When opening a resource from Business Unit A, the **Edit** button is available, because the role has the write access to this data group.
- However, opening a resource from Business Unit B, which only has read access, disables the editing functionality.

The following video demonstrates the different access that these roles have on the entities associated with each of the data groups.



Customizing Feature Details: Force Signature and Require Comment

In this scenario, we will explore how to enforce additional validation steps when executing certain features in MES - specifically by requiring users to provide a comment or enter their credentials (PIN).

Start by navigating to **Administration** > **Security** > **Features** and select a feature, such as `Resource.Edit`. On the **Edit** wizard, you will find two toggle options: **Force Signature** and **Require Comment**. Additionally, you can enter a custom message that appears when the resource is edited. For example, add the message "Insert comments justifying changes", then save the configuration.

Now, let's see how this works from the user perspective. Open a resource and attempt to edit it - for instance, by changing the Resource Type. You will see that the comment field becomes mandatory and the message you configured earlier is shown next to the information icon. After entering a justification, the system prompts for the user PIN, confirming that the operation cannot proceed without authentication.

The following video demonstrates how to use the Force Signature and Require Comment at the feature level.