Using Metis Security

Using the Metis role-based security model makes it possible to limit which functions or data are accessible for groups of users. Using Metis security is optional – by default, all users have access to all data and the full range of features included in your license. This document describes how you can control Metis security and define your own user access rights.

Users

Roles

Security

Understanding Users, Roles and Security

In Metis each user's access rights are controlled by the Security Roles assigned to that user. Each user can have any number of roles and the actual access rights will be the combined permissions of all roles. By default all users in Metis is assigned the built-in Administrator role, which has unrestricted access. Security settings on a specific Assessment or Person can specified, to control which roles have access to it, and if that access allows modification or is read-only.

Controlling access rights

Controlling access to Metis features

Using the security areas in Metis it is possible to limit which Metis features each user is allowed to use. For example you can set up a role that only has access to work with assessments. You may also set up a special role for an external consultant that only is allowed to view analyses and reports without the possibility to change anything.

Controlling access to data

It is also possible to control which data each user has access to. For example it is possible to set up Metis so that only the employees in the sales department have access to the sales department data. Furthermore it is possible to control security settings on individual assessments or persons, if they should not be accessible for all users. For example you could limit access to assessments related to upper management, or give an external consultant access to specific persons and assessments only.

Creating Security Roles

In order to control security, you must define Security Roles with the desired access rights, and assign these roles to your Metis users.

A role can represent any grouping in the real world: A job function (e.g. ”Sales consultants” or ”HR managers”), an organizational unit (e.g. ”Accounting” or ”IT”), a geographic region (e.g. ”Denmark” or ”Europe”) or any combination of these (e.g. ”HR Consultants in Copenhagen” or ”European Sales Managers”).

When defining a Security Role, you must give it a descriptive name and a detailed description to help you remember the purpose of the role. In addition you specify:

1. What Metis features the role has access to (security areas)
2. What access rights other roles have to this role's data (Default access rights)

Security Areas

For each role it is possible to define which Metis features the role has access to. This is done through Security Areas, representing different features and functionality in the Metis system. For example there are security areas for “Login”, “Assessments”, “Persons” and “Reports”. Any user must have “Login” access in order to be able to log into Metis.

Default access rights

For each role it is possible to define the default access rights to objects created by this role. For example, if the role is “HR consultants in UK”, you will set to what extent other roles are allowed to access assessments and persons created by this role. You can specify access rights for each other role in the system. The role itself always has full permission to all objects created by that role.

For each other role, access rights can be set to one of the following levels:

- None: The specified role does not have permission to see the objects at all
- Read: The specified role has permission to see the objects but not modify them
- Write: The specified role has permission to modify the objects, but not delete the.
- Full control: The specified role has full permissions for the objects, including delete and changing security.

For example you can set up a role called “Copenhagen Office”. Now all users with that role will have full access to each other’s objects, and you can define that the “Headquarters” role has read access, and all other roles cannot see the data at all.

If no default access rights are specified, then all roles will have full access to the objects created.

Setting object security

It is possible to set security on assessments or persons, to specify which roles have access, and specify if that access is read, write or full control. This is done by selecting one or more objects in the Person List or Assessment List and clicking the “Security” button.

This shows a dialog where it is possible to specify the access level for each role. Similar to default access rights it is possible to set the following access levels: None, Read, Write and Full Control. For example a specific assessment may be changed so no roles except ”HR Management” have access to it.