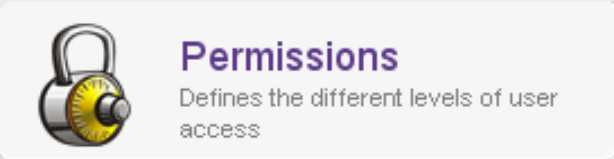
Permissions – Common Examples

Quick Reference



Permissions define the level of access for all users in the database. Each user must be linked to a permission record in order to have any access to the system or portal. Typically you should only need a few permission groups to accommodate all users, and many clients use similar permission levels to reflect their users' role and data management needs within the system.

Common Permission levels include:

FULLACCESS
Full Access users typically have access to all components of the program that are in use, as well as the ability to add, edit, duplicate, delete, and print records. They can usually edit closed records. Full Access users typically have password administrator rights as well as the ability to edit not only which contacts are assigned to permission records, but the permission records themselves. Full Access users are often the only users who are capable of editing capsule preferences (such as capsule names, custom fields, and mandatory fields).

ADMIN
Admin users may have access to some or all components of the program that are in use, but especially the Resources, Work, and Purchase modules. They are often able to add, edit, duplicate, and print records, and may have the ability to delete certain types of records and edit closed records as well. They often have access to password administrator rights, and are the people other users would contact in the event of a forgotten password (this may not apply to clients using SSO, as the Active Directory passwords are not stored in AwareManager and cannot be edited from the program).

ENG-MGR
Engineering Managers can access the modules most relevant to their day-to-day operations, usually Work and Maintenance. They often have the ability to add, edit, duplicate, delete, and print Work records, Maintenance and Equipment records, and Equipment Types. Engineers can perform more advanced Maintenance and Equipment operations, such as copying maintenance records between pieces of equipment, or generating Maintenance work orders. They sometimes also have the ability to edit and create Work Types and Work Statuses. They do not typically have access to password administrator functions, nor can they change the permission levels of other users. If the client is using mobile, they may have the ability to add, edit, assign, and close work orders from their mobile device.

ENG
Engineers typically have access to the Work and Maintenance modules, though they usually cannot delete records. They may be able to add and edit Maintenance, Equipment, and Work records, but usually do not have the ability to edit Work Types, Work Statuses, or Equipment Types. Engineers sometimes have the ability to generate Maintenance work orders. If the client is using mobile, they may have the ability to add, edit, and complete work orders from their mobile device.

PORTAL
Portal (sometimes called Tenant) users can only access the program from the tenant portal. They can search, view, and add records. Sometimes they may have limited editing capabilities. Often their ability to search is restricted to only records entered by themselves or their organization. They may be given the ability to cancel their own work requests, but they cannot delete requests. Portal users typically have no access to JXT (the main program) or mobile applications.

SECURITY
Security users primarily access the Visitors module, but may also access Work. They can add, edit, duplicate, and print records from the modules they have access to. They do not typically have password administrator abilities or the ability to delete records from the system.

Note: Each of the levels described here are general recommendations based on existing client use of the program, and should not be considered set in stone. Our permission feature is flexible enough to allow complete customization of every level of access tailored to the data security needs of each client.

For more information about customizing permission levels, please contact your client manager.