Access Levels and Roles

This document explains the difference between Access Levels or visibility a user has within Devensoft's M&A Tool and the predefined Roles. User access and roles go hand in hand and provide the necessary security and flexibility that is needed for large teams with different types of users.

Access Levels

Access Levels define the type of visibility given to a user for all/some/none of the Target or Integration. The User Detail page (**Admin/User Administration**) is where Custom and Limited access is defined. Descriptions and examples for when you would assign access to a user are described below.

1. **N/A (No Access)** – a user cannot see any Targets or Integrations within the system.

2. **Executive Level** – a user has access to ALL Targets and Integrations within the system and has the Full Rights role assigned. Users can read, update, create and delete Target and Integration data. CEO, CIO, VP's and people with a similar job title are typically assigned this access.

3. **Corp Dev/Strategy** – a user with this access can potentially see All Targets and/or Integrations within the system. They can have Full Rights, Full Rights w/o Delete, Read Only or custom roles assigned to them. Typically, team members in the Corporate or Business Development/Strategy departments within an organization are assigned this type of access.

4. **Business Unit** – have access to Target or Integration data within their Business Unit. The Business Unit field is listed in their Contact Detail page AND on the Deal Detail Page, accessed via the Summary tab. Both fields must be completed for this Access Level to work. Business Unit's are usually based on geography/regional area or different divisions within a company such as consulting, manufacturing, etc.

5. **Project Specific** – means that a user can be given access to specific Targets and Integrations. The user with this type of access MUST be added to the deal team manually. If a user is not assigned as a team member, they cannot access that Target or Integration. This type of access is good for team members who should be given access to a few Targets/Integrations vs. all the Targets or Integrations within the system.

Roles

A role determines what areas within a Target or Integration a user has access to. One user may have access to ***read*** certain data while another user has access to ***read and edit*** the data. Roles can be pre-defined as explained below or customized based on a company's functional area.

1. **Read Only** – means that the user assigned to this role can read the data with the system.

2. **Full Rights w/o Delete** – a user assigned to this role has full rights to the system --they can read, update, and create data…they just can't **delete** data.

3. **Full Rights** – the user w/ this role has full rights to the system…they can read, update, create and delete data.