# Security levels

1. Who can connect to the server:
   1. Checking the connection to the server according to Username and Password [1]
   2. Checking the connection to the server based on the presence or absence of AccountId [10]
   3. Examining the type of connection, the volume of authorized and unauthorized requests for a specific username (in terms of volume and time) [2]
2. Who is allowed to use service methods ? This is done by permissions . [3]
3. Who can see which fields of the database tables . This is done by Context Scopes . [4]
4. Who can see what records? This case is regulated by queries that are set in Service Methods according to the received request. [5]
5. Who can change which fields? This is done by different Context Scopes ( different DataModels set for different Scopes ) and ValueChangePreventerAttribute . It should be noted that if ValueChangePreventerAttribute is used when adding a record to the database, the mentioned fields must have default values , and only if they have default values when adding a new record, this attribute is considered. [6]
6. Who can change what records? This case is done by the logic similar to case 4 in Service Methods . This security level is performed in every Add , Edit , Delete operation. At this level, in addition to checking the Id of the record, all ForeignKeys are also checked so that they do not take values outside the legal permissions [7] . It should be noted that at this stage, according to the request received by the State, the current status is set (this operation should be done before starting any security check operation). [8] . It is also checked in this section that the DataView has not been sent to storage [9] .