

Sage SalesLogix Security	Web	LAN
Ownership		
<p>Determines what records a user can see in each table.</p> <p>Campaigns and accounts are the only tables with an “Owner” field. If a user can access a particular account, the user can also see all contact, opportunity, ticket, contract, return, and defect records that relate to that account.</p> <p>Most companies use either <i>Team</i> ownership or <i>Individual</i> ownership, not necessarily both. For example, if your company uses teams, you can see only accounts that are owned by your team(s). Lee is on the Midwest team, so he can see all accounts with Owner set to "Midwest." If your company uses individual ownership, you can see accounts that you own and that are owned by other users that you're allowed to see. Lee is on Dan's user team, so Lee can see all accounts with Owner set to "Lee" and "Dan."</p> <p>Companies also use owner types of <i>Everyone</i> and <i>Everyone (View Only)</i> when they want everyone to be able to see a particular record regardless of team or user.</p> <p>Departments are another way to organize team ownership. When you add new users to SalesLogix, you can select the department(s) to which each user belongs. Then within teams, you can simply add the entire department to the team instead of adding all department users individually. Any user in the department can access any accounts owned by the department's team(s).</p>	✓	✓
Field Security		
<p>Determines what fields a user can see or edit in each table.</p> <p>Field security is applied to a user through a field security profile, which includes a list of all tables and fields in the database and designates which fields are set to No Access, Read Only, or Read/Write. By default, SalesLogix includes three system profiles that you can use:</p> <ul style="list-style-type: none"> • Read Only Default – All fields are set to Read Only. • Read/Write Default – All fields are set to Read/Write EXCEPT the Owner field (seccodeid) in the Account table, which is Read Only. • Team Owner Profile– All fields in all tables are set to Read/Write. <p>The ability to change the Owner field is typically reserved for one user (like the team owner) because if someone accidentally (or maliciously) changes the Owner field for an account, all other team members also lose access to it, and they would need to contact the administrator to change it.</p> <p>You can create custom security profiles per user. For example, you may want to set all fields to Read/Write except the Credit Score field (Read Only) and save it as the “Field Sales” profile to apply to all Level 1 sales reps. Users can also have different security profiles on different teams. Security profiles apply to individually-owned accounts and team-owned accounts, but when an account Owner is set to “Everyone,” no security profile prevails.</p>	✓	✓
Feature Security		
<p>Determines what Create and Delete operations a user can perform.</p> <p>Feature security includes the following entities: Account, Campaign, Contact, Contract, Defect, Lead, Opportunity, Return, SalesDashboard, and Ticket.</p>		✓
Function Security		
<p>Determines what menu items a user can access.</p> <p>By default, new users are restricted from accessing the File > Subscribe to Account and Edit > Account Unsubscribe menus, as well as the Tools > Literature Fulfillment, Customize, Macros, Manage, and Maintenance menus. Most companies like to reserve the Manage menu for power users or sales managers because it includes access to features like managing products and pricing, sales quotas, pick list items, and more.</p>		✓

Sage SalesLogix Security	Web	LAN
Administrative Roles		
<p>Determines what interface items a user can see inside the LAN Administrator.</p> <p>If a SalesLogix user has access to the LAN Administrator (either via an installation on the sales person's computer or via remote access to the Administrative workstation), the user can log on with his or her standard SalesLogix credentials and perform administrative functions like managing currency, library items, or users. By default, three administrative roles are available to use:</p> <ul style="list-style-type: none"> • Sales Admin – Access to create Remote user databases, territory realignment, users, and more • DB Admin – Access to the Database Manager and more • Librarian – Access to the Library and SpeedSearch indexes 		✓
Secured Actions/Roles		
<p>Determines what interface items a user can see when applied to a web role.</p> <p>Secured actions are the web client's equivalent of Feature Security, Function Security, and Administrative Roles rolled into one spot. You can access secured actions and roles inside of the Web Administrator in Sage SalesLogix version 7.5.3 or higher when you log on as "admin" or a user with an "Administrator" role.</p> <p>A secured action can be applied to almost any interface item inside the Application Architect. Secured actions are then grouped into roles, which are then applied to users. Out-of-the-box as of v7.5.4, you can find the following roles (A = Add, E = Edit, V = View, D = Delete):</p> <ul style="list-style-type: none"> • Account Management** – Includes secured actions for Account (A, E, V, D*). • Administrator – Includes secured actions for: Packages, Product, Group*, Lead, Administration/Deduplication/, and Administration/View. Use caution for assigning a user to the out-of-the-box "Administrator" role because the user gets access to the following features: Users, Teams, Departments, Roles, Competitors, Lead Sources, Products, Packages, Pick Lists, Literature Items, Qualifications, Secured Actions, Integration Setup, and Library Management. If you want to isolate a particular function without giving access to all features—like a web librarian, for example—create custom admin roles. • Contact Management** – Includes secured actions for Contact (A*, E, V, D*). • Data Quality Manager – Includes all secured actions for Administration/Deduplication: CheckDuplications, CheckHistory, ProcessDuplications. • Integration Contract Lock Price – Includes all secured actions for Product/LockPricing* and SalesOrders/LockPricing. • Opportunity Management* – Includes secured actions for Opportunity (A, E, V, D*). • Order and Quote Processor – Includes secured actions for Contact (A*, V), Account (A, V), and SalesOrder: (A, E*, V, D*). • Service/Support – Includes all secured actions for Contract (A, E*, V, D*), Ticket (A, E*, V, D*), Defect (A, E*, V, D*), and Return (A, E*, V, D*), • Standard User – Includes all secured actions for Account (A, E, V, D*), Contact (A*, E, V, D*), Opportunity (A, E*, V, D*), SalesOrder (A, E*, V, D*), Lead, Campaign (A, E*, V, D*), Contract (A, E*, V, D*), Defect (A, E*, V, D*), Return (A, E*, V, D*), Ticket (A, E*, V, D*), Packages/View, Product/View, and Group*. You should assign all users to the Standard User role upon installing or upgrading to v7.5.4. <p>* The secured action in v7.5.4 is not assigned to an interface item and is logged as a defect. ** The role in v7.5.4 is not assigned to secured actions and is logged as a defect.</p>	✓	