# Oracle System Administrator Fundamentals – It's All about Controlling What Users Can See and Do

Jim Childerston
*Cline Consulting and Training Solutions, LLC*

### Introduction

In this presentation, we will look at basic system administration from a functional point of view. "Gatekeeper" to sensitive data, the system administrator controls access via responsibilities, user roles, custom menus, and request groups. The system administrator works closely with the database administrator (DBA) to register custom reports and programs and set up access to custom applications. This whitepaper presentation includes screenshots, step-by-step instructions, and helpful tips to provide you with a strong foundation in system administration.

### The System Administrator's Job

Control

As a System Administrator, you are responsible for controlling user access to the applications and minimizing user frustration. Your agenda includes:

- New users - You will define new apps users, and give them usernames, passwords and responsibilities.
- Security - You will control the apps, forms, functions, and reports accessible to each user.
- Monitoring – To improve system performance you will gather data concerning who does what and when.
- Profiles – You will set system profile values at the user, responsibility, application and site levels to control the appearance and behavior of the applications.
- Concurrent Processing – You will monitor, manage, and control concurrent processing for optimum system performance.

Liaison

You provide the interface between end users and database administrators. DBAs are responsible for maintaining the data that users input, update and delete when they use Oracle Applications. This data manipulation cannot be seen by end users. For this reason DBAs are said to manage the back end of the system. The division between user applications and the underlying database structures results in the need for a person who can communicate with the DBA and administer the user interface or applications side of the system. As the System Administrator, you are the liaison who manages the front end that users see and use.

### Responsibilities

A responsibility is a level of security that lets users access the applications, functions and data required to perform their jobs. Each responsibility allows access to:

- A specific application or applications, such as Oracle General Ledger or Accounts Payable.
- A set of books.
- Specific menu paths.
- A restricted list of functions a user can perform
- A list of programs and reports that a user can submit.

Each user has at least one responsibility and several users can share the same responsibility. A system administrator can assign users any of the standard responsibilities provided with Oracle Applications, or create new custom responsibilities.

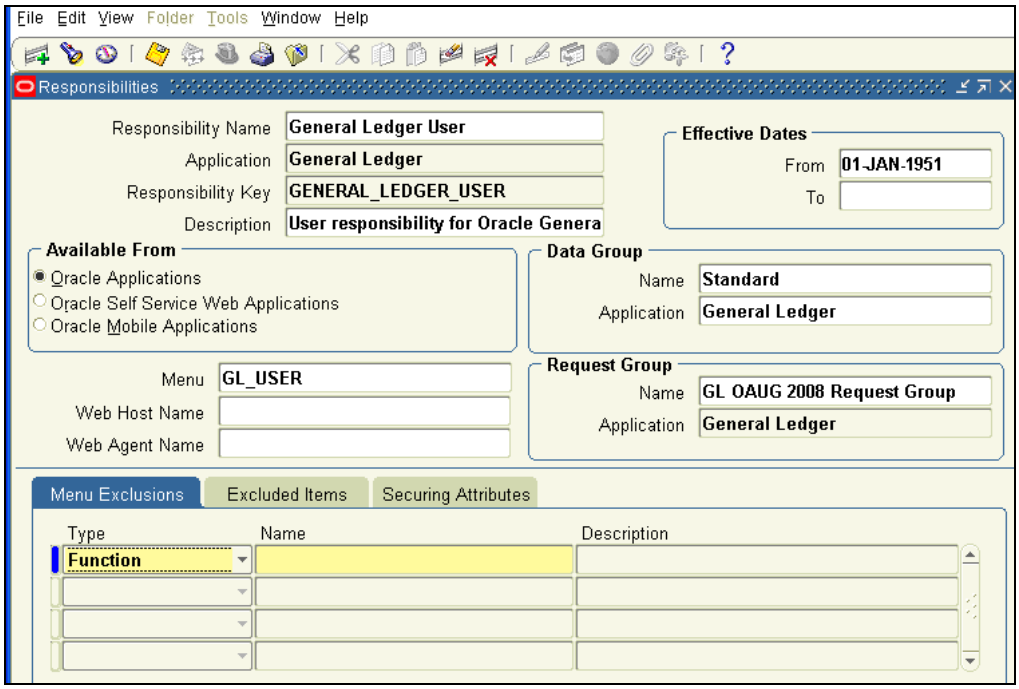
Pre-defined Responsibilities

All applications are installed with pre-defined responsibilities which should be listed in the reference guide for each Oracle Application product. The major components that define a responsibility (data groups, request security groups, menus, and functions) are also pre-defined. Responsibilities and their attributes can be viewed using the System Administrator responsibility: Navigate: Security>Responsibility>Define, then query by the name of the responsibility. Another way to find a list of responsibilities is to request a report titled "Active Responsibilities," which lists every Application, each assigned responsibility, security group, users, and start date.

Custom Responsibilities

Custom responsibilities can be defined using the System Administrator responsibility: Navigate: Security>Responsibility>Define. Points to consider when you define your responsibilities include

- Name custom responsibilities using descriptive company abbreviations.
- Start with a pre-defined menu which exceeds the desired functionality of your custom responsibility.
- Limit the functionality available with the pre-defined menu by excluding menus and functions.




By assigning the same menu hierarchy to different responsibilities and excluding different functions and menus, you can streamline responsibilities to better fit the roles of the end users and you can secure access to forms and functions that should not be viewed.

## Menus

Delivered Menus

Every pre-defined responsibility contains pre-defined menus and functions. If you cannot create the custom responsibility you need by applying exclusions to pre-defined menus and functions, you may build a custom menu for that responsibility using pre-defined forms (i.e., form functions) and their associated menus of subfunctions. However, we recommend that you do not modify a pre-defined form.

Creating Custom Menus

When defining a new menu structure create a logical, hierarchical listing of functions to make it easier to exclude functions when customizing the menu structure for different responsibilities. Create a logical, hierarchical menu that leads users through their application forms. Use the Menus form (Application>Menu) to define menus

pointing to functions that you want to make available to a new responsibility. Assign the menu structure to a new responsibility using the Responsibilities form.

Defining a New Custom Menu Structure

Before undertaking the design of a new menu structure you should run a report titled "Function Security Menu Report." This will produce a list of the full menu names of a responsibility, any excluded menu items, and the rules that exclude them. Use this report to find out if there are any existing menu structures you can modify or use as a model for your new menu.

Build your menu structure using an org chart model. Start at the bottom and work your way up. Define the lowest–level menus first. A menu must be defined before it can be selected as an entry on another menu. Assign menus and functions to higher–level menus. Assign menus and functions to a top–level menu (root menu). Document your menu structure by printing a Menu Report.

Note that you should start with a blank Menus form (blank screen). A menu saved under a different name overwrites the original menu (there is no "Save As" feature).

Entries cannot be copied from one menu definition to another. When you change a menu's name, the menu entries are not affected. The menu's definition exists under the new name. Other menus calling the menu by its old menu name automatically call the same menu by its new (revised) name.

Menu Compilation

You should compile your menus after you make changes to the menu data. A request for this concurrent program is automatically submitted after you make changes using the Menus form. The Compile Security (FNDSCMPI) concurrent program is used to compile menus so that the system can more quickly check if a particular function is available to a particular responsibility/menu.

After you apply a patch that includes menu changes, you should also run this concurrent program. You can do this through the AD Administration utility. The readme file included with the patch will include instructions to recompile the menus if necessary.

Preserving Custom Menus Across Upgrades

Use unique names to make your custom menus survive upgrades. For example, you can start the menu's name with the application short name of a custom application. If you define a custom application named Custom Accounts Payable, whose application short name is ZZZCAP define your custom menu name ZZZCAP_OAUG_MENU_ONE.

Remember that the Oracle Applications standard menus may be overwritten with upgrade versions. Therefore, if you attached your custom menu as a submenu to one of the pre-defined Oracle Applications menus, recreate the attachment to it following an upgrade. An alternative is to attach a standard Oracle Applications menu as a submenu to your custom menu; the link from your custom menu to the standard menu should survive the upgrade.

Special Function for Oracle HRMS, Oracle Sales and Marketing

In most Oracle Applications products, you can open multiple forms from the Navigator window without closing the form you already have open. However, when you define a new responsibility whose custom menu accesses Oracle Sales and Marketing forms, or Oracle HRMS task flows, you must include the function Disable Multiform, Multisession as an entry on the responsibility's top–level menu.

You can identify an Oracle Sales and Marketing form by the OSM prefix contained in the form's function name.

You should not include the Disable Multiform, Multisession function on menus that do not include either Oracle Sales and Marketing or Oracle HRMS forms. To include the Disable Multiform, Multisession function on a menu: • Add a Function menu entry to the top–level menu (i.e., the menu referenced by your new responsibility). Select the function whose User Function Name and Function Name are: Disable Multiform, Multisession FND_FNDSCSGN_DISABLE_MULTIFORM.

**Registering Custom Reports/Programs**

Sometimes you may need to develop and implement your own custom programs to address specialized processing needs. You can integrate custom programs into the Oracle Applications environment where they will be secured and managed the same way as regular Oracle Applications programs. A custom program or report is a concurrent program consisting of an executable, for example an Oracle Report program or a PL/SQL procedure, and the input parameters required by the program or procedure. The concurrent program must be associated with an existing Oracle application or custom application. Associating your custom concurrent program with a registered custom application will usually protect it during an upgrade.

How to Register a Custom Program/Report

Following the development of the program or report, the first step is to identify the executable (Navigate: Concurrent>Program>Executable), then enter the required information: Next, create the concurrent program. (Navigate: Concurrent>Program>Define). Next, identify the program parameters.

Once you've registered your custom program, associate the program with a Request Group (Navigate: Security>Responsibility>Request). Users with a responsibility associated with the Request Group can run your custom application through Standard Request Submission.

**Request Groups and Request Sets**

Reports and concurrent programs can be assembled into request groups and request sets. A concurrent program is an executable file that runs simultaneously with other concurrent programs and with online operations. Occasionally, a concurrent program processes with a large amount of data and takes a long time to run. System Administrators can use request sets and request groups to optimize system performance.

What is a request group and why do you use one?

A request group is a collection of reports or concurrent programs. The System Administrator defines request groups to control user access to reports and concurrent programs. Only a System Administrator can create a request group.

What is a request set and why do you use one?

Request sets can define run and print options and/or parameter values for a collection of reports or concurrent programs. End users and System Administrators can define request sets. The System Administrator has request set privileges beyond those of an end user.

Standard Request Submission and Request Groups

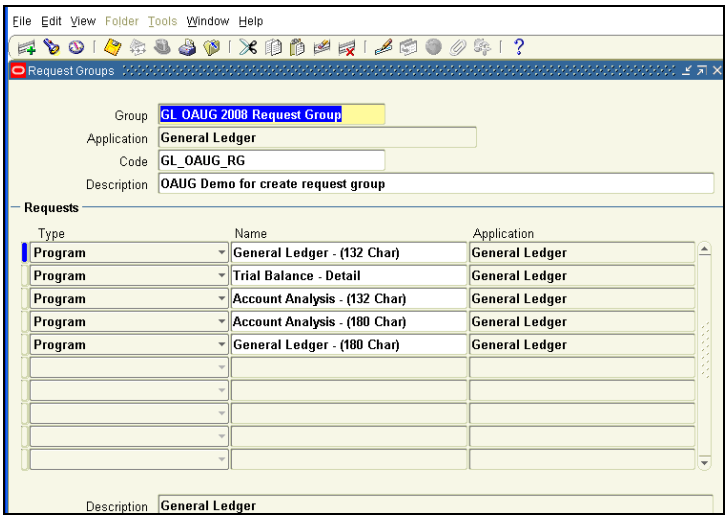
Standard Request Submission (SRS).allows you to select and run all your reports and other concurrent programs from a single, standard form. Reports and concurrent programs included in the Request Group assigned to the user's responsibility are executed via SRS.

As System Administrator you can limit the number of requests that may be active (status of Running) for an individual user. This ensures that a user cannot monopolize the request queue. For example, if a user with an Active Request Limit of 5 submits 20 requests, only 5 requests will be run at the same time. The remaining requests will be run when the number of active requests for the user drops below 5. Use the Profile Options window to set the Concurrent: Active Request Limit profile. To set a global limit for all users, set this option at the site level.

Defining a Request Group

To define a Request Group navigate to Security>Responsibility>Request. Enter the list of programs included in the group. You can add custom and/or pre-defined programs to a Request Group. The following screenshot depicts the programs and reports included in the request group GL OAUG Request Group.




The Request Group must then be assigned to a responsibility. Navigate to Security>Responsibility>Define, then query the responsibility to which the request group will be assigned. Enter the Request Group Name and Application in the Request Group region and save.

Test your new Request Group. To do so, switch to the responsibility to which the Request Group is assigned. Navigate to SRS and view the list of available programs or reports.

### Responsibilities and Request Security Groups

When a request group is assigned to a responsibility, it becomes a *request security group*. Users can run only the reports, concurrent programs, and request sets that are in their responsibility's request security group. If you do not include the Submit Requests form on the menu for a responsibility, you do not need to assign a request security group to the responsibility. If a request security group is not assigned to a responsibility, then users working under that responsibility cannot run any reports, request sets, or other concurrent programs in SRS.

### Users

The methods by which the System Administrator controls user access to the applications are rapidly changing. . Oracle User Management is used by system administrators to define the access and control policies required by their organizations. Local Administrators use the policies to manage a subset of the organization's users and end users perform some self service tasks. The new features provided by Oracle User Management have been available as optional features since the release of version 11.5.10. Customers can choose to use any or all of these user management features. The primary difference between old and new features governing the control of user access is the concept of User Roles and Role Based Access Control (RBAC) as opposed to responsibilities. If customers choose not to use the roles functionality, they can still use any or all of the following features in Oracle User Management in release 11.5.10:

<u>Registration Processes</u>

Registration Processes enable organizations to provide end-users with a method for requesting various levels of access to the system, based on their eligibility. This simplifies the system administrator's job by providing streamlined flows for account maintenance and role assignments. Registration processes also allow you to specify approval routing rules, notifications, identify verification and eligibility criteria. Oracle User Management supports three types of Registration Processes:

1. Self-Service Account Requests - provides a method for persons to request a new user account. For example, a customer may need to register before they can purchase an item using an online account. Once the customer has completed the registration process, they will have a user account as well as the role(s) needed to access some portion of the website. This type of registration process also offers identity verification, which confirms the identity of the requester (via an email notification that requires a response) before the registration request is processed. If the recipient does not reply within a predetermined amount of time the request is rejected automatically.

2. Requests for Additional Access - provides an Access Request Tool for existing users to request additional roles. Users can only request additional roles that have been defined as appropriate based on their current roles. For example, you can configure Oracle User Management so that all users with 'Employee' role are eligible to sign up for a 'Sales Representative' role, while customers are not eligible to sign up for this role. However, everyone can sign up for iRecruitment to view job postings. An administrator assigning a role to a user is essentially fulfilling a registration request on behalf of the user, thereby invoking a Request for Additional Access Registration process, if defined.
3. Account Creation by Administrators - provides administrators (including delegated administrators) the ability to create user(s). Each account creation registration process can be made available to select administrators.

Registration processes have several advantages. They streamline the registration process for both end users requesting new or additional access, as well as for administrators. They enable applications to use the same infrastructure to meet their varied registration requirements giving you a uniform administration experience across all applications in the suite.

You can define specialized registration processes (including separate user interfaces) that capture specific information required as part of your organization's policies. Each registration process requires the following information:

- The type of registration.
- The role(s) assigned after the user successfully completes the process.
- A description of the purpose of the registration process.
- An optional registration user interface for collecting account or additional information.
- A workflow for approval, confirmation, rejection, and identity verification notifications.
- The Approval Management Transaction Type. A transaction type represents a set of approval routing rules that are interpreted at runtime.
- The set of users eligible to sign up for additional access (only applicable for Request for Additional Access Registration Processes).

Delegated Administration

Delegated Administration provides traditional System Administrators with the ability to delegate some of the user management privileges to people who are closer to the actual end users of the system. These local administrators manage a subset of the user population, and only assign the set of access privileges relevant to their functional area.

Access control in Oracle Application allows administrators to be designated at any level, internally within the enterprise as well as externally. Clients could internally designate administrators at division or even department levels, and then delegate administration of external users to people within those (external) organizations.

Delegation policies, or data security policies, are a set of policies defined as part of delegated administration known as Administration Privileges. Administration Privileges determine what users and roles the delegated administrator can manage. There are three aspects to administration privileges: roles, users, and organization. Each privilege is granted separately, yet the three work together to provide the complete set of abilities for the delegated administrator. These privileges can be defined along with the role definition in the Role & Role Inheritance user interface in Oracle User Management.

Not all Administrator Account Creation Registration Processes are available to all administrators. While administrators can benefit from these registration processes, designed to streamline the process of creating and maintaining user accounts, each registration process must be granted to the appropriate set of administrators.

Self-Service Requests

Release 11.5.10 provides a sample Oracle User Management Self Service registration user interface for internal employees and for new, external individuals. Organizations can extend or create their own registration user interfaces and business logic.

When users request additional access to the system, they are requesting that they be granted additional roles. A user's eligibility for receiving additional access is based on his or her current roles. An organization's employees

can request roles which further define their job functions, but customers of that organization cannot request the same roles.

Approvals

Existing users request additional role(s) through the Oracle User Management Access Request Tool (ART), depending on their eligibility. The ART is included on the Preferences menu. Eligibility defines what Roles a user can request and is defined in the Request for Additional Access Registration Process. For example, employees can be eligible to sign up for a 'Timecard Entry' role, while customers will not be eligible to sign up for this role. However, everyone can sign up for iRecruitment to access job postings.

Oracle User Management raises Workflow Business Events when a role or account is requested and when an account or role is approved or rejected. All information retrieved in the registration process and the registration context such as application ID, role code, and registration service code, are included when these events are raised.

**Role Based Access Control (RBAC)**

Role Based Access Control (RBAC) can improve existing security by organizing data security policies and existing function security using roles. Security privileges in Oracle Applications have historically been managed on an individual user basis, with different types of privileges assigned to each user directly. For example, a Customer Service Agent at your organization may have multiple responsibilities and several other types of access privileges to perform his or her job. With RBAC, users no longer need to be directly assigned the lower level permissions and responsibilities, as these can be implicitly inherited based upon the roles assigned to the user. Roles can be defined to consolidate other roles and responsibilities with lower level permissions (functions) and data security policies. This is accomplished through a one-time setup, where all the permissions are assigned to the role. The benefit is, to modify the privileges for a group of users, all you need to do is change the permissions or role inheritance hierarchies for that role. All of the users assigned to that role will instantly inherit the new permissions.

RBAC is based on a national standard that supports user access control based on the role that user plays within an organization rather than upon the user's individual identity. The benefits of implementing RBAC include reduced cost of administering user access; streamlined setup and implementation of security policies; and structured user access control based upon users' job functions.

Roles vs. Responsibilities

In Oracle User Management, responsibilities can be considered special roles that represent the set of navigation menus contained within an application. Responsibilities are associated with an application, roles determine what parts of that application (and data therein) a user can access. This represents a shift in the definition of a responsibility in Oracle Applications. Before the concept of roles, it was often necessary to create several similar responsibilities to effectively carve out data and functional security access for a group of users. This increased the overall cost of ownership as the number of responsibilities grew.

Oracle User Management follows the RBAC definition of a role as "a job function within the context of an organization with some associated semantics regarding the authority and responsibility conferred on the user assigned to the role." Roles can now be defined to determine the applications as well as the data and functions within those applications accessible to a user.

Roles vs. Groups

Oracle Applications distinguish the concepts of groups and roles to avoid confusion. A role is a job function within an organization conferred on the user assigned to the role. "Groups" represent a collection of users, and possibly other groups, that are brought together for some purpose, not necessarily for access privileges. Although a group can be brought together for some access control purpose, within the context of Application Security, only roles should represent job functions within the context of an organization. It is job function that determines access rights within an organization. Therefore, for the purpose of Application Security, the distinction between groups and roles is maintained.

One important aspect of the RBAC implementation is the ability to use the different groups already utilized within Oracle Applications. For example, Roles and Positions as defined in Oracle Human Resource Application, Group

Parties as defined in the Trading Community Architecture (TCA), and Resource Groups as defined in Resource Manager, are integrated with the RBAC model. The groups and the group memberships are maintained through the owning application. With Oracle User Management, clients can assign permissions to these externally managed groups. In the future, these groups can also be hierarchy enabled, allowing clients to assign roles and responsibilities to the groups through role inheritance. Administration of access privileges is significantly reduced because roles, permissions and responsibilities are automatically assigned to users as they change positions or groups within the company.

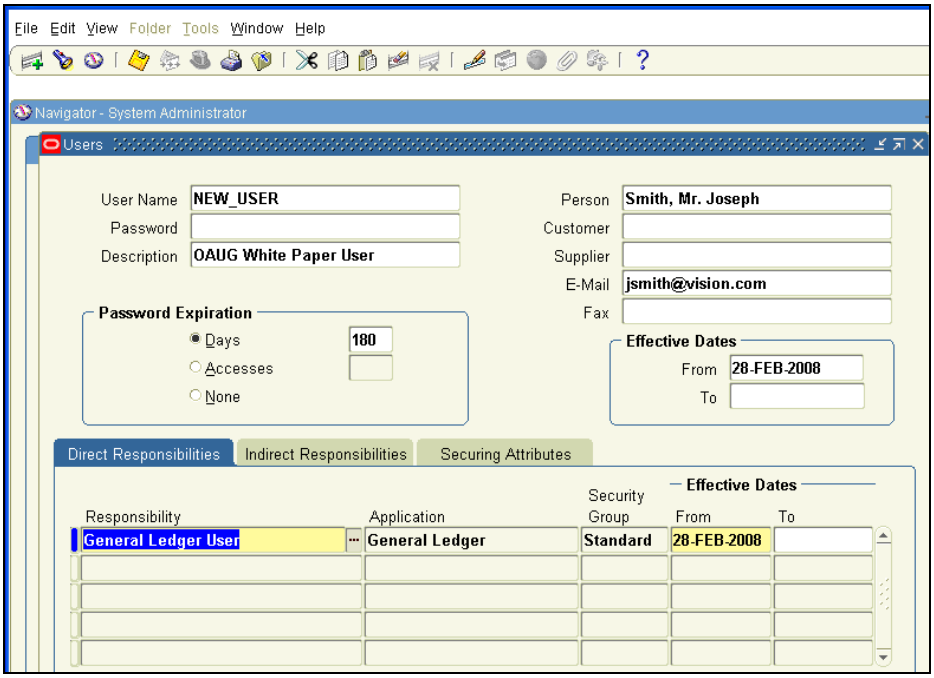
Role Inheritance Hierarchies

Roles are included in Role Inheritance Hierarchies. When roles are inherited through role inheritance hierarchies, the various permissions and responsibilities assigned to those roles are conferred to the users within the hierarchy. The RBAC model supports General Role Hierarchies, which means that any role can have multiple superior and sub-role relationships.

Role Inheritance Hierarchies are created in the Roles & Role Inheritance user interface in the Oracle User Management application. Administrators can nest roles using the Add Role feature. This nesting results in the inheritance of the sub-role by the superior role. This is also true when the administrator is creating role inheritance hierarchies for groups from other source systems (such as Resource Groups as defined in Resource Manager).

**Traditional User Set up**

To set up a new user, using the System Administrator responsibility, navigate: Security>User>Define.




Enter the username, then enter the initial password twice. Click the appropriate Password Expiration button and complete the appropriate field. As a general rule, passwords should be set to expire every 180 days. Assign the designated responsibilities and end dates, if applicable and you're done!

Use the same form to query and update existing users.

### Enabling Various Features on the Login Page

Oracle Applications provides the ability to include several optional attributes on the login page. The attributes are as follows:

- Username Hint
- Password Hint
- Cancel Button
- Forgot Password Link
- Register Here Link
- Language Images
- Sarbanes Oxley Text

These attributes are controlled via a single profile option, "Local Login Mask" FND_SSO_LOCAL_LOGIN_MASK). To display one of more of these optional attributes on the Login page, add the numeric values of all desired attributes and then set the value of the profile option to that sum of the values. The following list details the numeric values for each of the attributes:

- Username Hint = 01
- Password Hint = 02
- Cancel Button = 04
- Forgot Password Link = 08
- Register Here Link = 16
- Language Images = 32
- Sarbanes Oxley Text = 64

To display the Username Hint, the Password Hint and the Forgot Password Link attributes on the login page, the profile value should be set to 11 (01+02+08). In order to display just the language images, set the profile value to 32.

### Conclusion

Call it a role or a responsibility, it's all about controlling what users can see and do. The job of system administrator is an indispensable link in any organization's use of Oracle Applications. Serving the needs of end users, the need for security, and need for system efficiency requires diplomacy, technical and functional skills.