Oracle® Database

Real Application Security Administration Console (RASADM) User's Guide

12*c* Release 2 (12.2)

E85615-01

June 2017

Real Application Security Administration

Oracle Database Real Application Security Administration (RASADM) lets you create Real Application Security data security policies using a graphical user interface.

If you are familiar with Real Application Security concepts and understand the design and flow for creating data security policies, briefly scan through the first 5 topics, then continue to topics 6 and 7 for an overview of the home page layout and how to get started. See topic 8 for information about documentation accessibility.

Installation and Configuration of Real Application Security Administration (RASADM)

Perform prerequisites, installation and configuration tasks, then run the RASADM application.

This section includes the following sections:

Prerequisites

Before you install RASADM, make sure that both the Oracle Database instance and Application Express are up and running.

The following prerequisites are required:

- Oracle Database release 12.1.0.1 and later
- Application Express release 5.0 and later

Installation

You can download RASADM from OTN, install it to create the RASADM schema and the RASADM APEX workspace, which sets up APEX security features. The installation creates a schema user named RASADM. It configures the external principal store (LDAP) if the LDAP host is provided..

Perform the following steps to install RASADM:

1. Download RASADM from OTN (Oracle Real Application Security (RAS) Download).
2. Unzip the downloaded zip file into a directory that you select.
3. In the unzipped directory, change directories to the `installer` directory.
4. Connect `AS SYSDBA` into SQL*Plus and run the following PL/SQL script to install RASADM:

```
SQL> @rasadm_ins.sql
```

When you run the installation script, the following output displays:

```
.
. Oracle RASADM installation
.........................................
.
. Creating schema user with privileges
.

RASADM provides data realm preview capability. If enabled, the administrator
will be able to view the data in any user table in the database.
Enable data preview capability? [No]

Enter a password for the RASADM admin user(admin): password
. Creating APEX workspace and admin user.
.
. Importing APEX application
.
Enter LDAP host name if you use external user and group (press ENTER if not):hostname
. Post configuration
.
. Done. Please review rasadm_ins.log for any errors.
.....................................
.
```

The installation script does the following:

1. Creates a schema user named RASADM with a locked account and expired password and grants the user limited privileges, which are required to compile certain APIs.
2. The data realm preview capability will be granted to the RAS role `RASADM_POLICY_ADMIN`, which in-turn is granted to the administrator.
3. Uses the Application Express Administrator's UI to create the RASADM workspace and imports the RASADM application code into the RASADM workspace, and then sets some Application Express security features.
4. Configures the external principal store (LDAP). If the LDAP host is provided, a network ACL is created to grant the RASADM user `CONNECT` and `RESOLVE` privileges on the given LDAP host and port. The RASADM user can also choose to configure external principal store (LDAP) from the RASADM UI, after the installation. In that case, it is the RASADM administrator's responsibility to grant the network ACL manually to the data set.

> **Note:**
>
> To uninstall RASADM, as the system administrator, run `rasadm_unins.sql`.

Configuration

You must configure the `admin` user who can log into RASADM as part of user management and then perform Application Express and workspace configuration, which performs SSL setup.

The following sections describes the configuration tasks:

- User Management
- Application Express Instance Level Configuration

User Management

This is the `admin` user who can log into RASADM. The RASADM run-time user is a Real Application Security user with password, who can directly logon to the database. The user must have a Real Application Security role granted (`RASADM_POLICY_ADMIN` or `RASADM_USER_ADMIN` or both roles) in order to access RASADM.

RAS provides two administrative roles - `RASADM_POLICY_ADMIN` and `RASADM_USER_ADMIN`.

The `RASADM_POLICY_ADMIN` is a Real Application Security role, which has the privileges to perform Policy Administration; for example, a Real Application Security user with this role can create policies, privileges, privilege classes, namespaces, and regular and dynamic roles. The user cannot create Real Application Security users.

The `RASADM_USER_ADMIN` is a Real Application Security role, which has the privileges to perform User Management; for example, a Real Application Security user with this role

can create users, and regular and dynamic roles. The user cannot use the rest of the features provided by RASADM.

However, both roles have the privileges to view reports on all pages.

The RASADM user can be created using Real Application Security Admin API (in PL/SQL) at the database.

The RASADM expects two kinds of users. One who can perform only Policy Administration tasks and the other who can perform both Policy and User Administration. The former needs to be granted with `RASADM_POLICY_ADMIN` Real Application Security role and the latter needs to be granted both `RASADM_POLICY_ADMIN` and `RASADM_USER_ADMIN` Real Application Security roles.

> **See Also:**
>
> Real Application Security Admin API (in PL/SQL) for the syntax and required privileges in *Oracle Database Real Application Security Administrator's and Developer's Guide*.

This section includes the following topics:

- Enabling Data Realm Preview Capability
- Creating RASADM Run-Time User
- Implementing the Password Policy

Enabling Data Realm Preview Capability

You must be sure to enable `Data Realm Preview Capability` to a user with `RASADM_POLICY_ADMIN` Real Application Security role outside of the installation script, if the option chosen is `No` during installation, execute the following as `SYS` user.

You should explicitly grant `SELECT` privilege on the table to the `RASADM_DB_POLICY_ADMIN` role on which you want the preview capability, else you can grant `SELECT ANY TABLE` system privilege to the `RASADM_DB_POLICY_ADMIN` role.

In addition, to bypass the Security Checks of a Real Application Security Policy you can grant `EXEMPT ACCESS POLICY` privilege to the `RASADM_DB_POLICY_ADMIN` role.

You can also grant the above mentioned privileges to any user defined Database role, which then has to be granted to `RASADM_POLICY_ADMIN` Real Application Security Role.

Creating RASADM Run-Time User

Only the `SYS` administrator can create additional RASADM direct logon application users by running the following PL/SQL scripts that create this `admin` user with the Real Application Security role `RASADM_POLICY_ADMIN` or `RASADM_USER_ADMIN` or both roles.

The two types of users that the `SYS` administrator can create are:

- An Administrator user who can perform both Policy Administration and User Administration.

```
-- Create runtime user to perform both Policy and User Administration for RASADM
DECLARE
  rg_list XS$ROLE_GRANT_LIST;
BEGIN
  xs_principal.create_user(name=>'admin');
  sys.xs_principal.set_password('admin', 'welcome1',
XS_PRINCIPAL.XS_SALTED_SHA1);
  rg_list :=
XS$ROLE_GRANT_LIST(XS$ROLE_GRANT_TYPE('RASADM_POLICY_ADMIN'),XS$ROLE_GRANT_TYPE('
RASADM_USER_ADMIN'));
  xs_principal.grant_roles('admin', rg_list);
END;
/
```

- An Administrator user who can perform only Policy Administration.

```
-- Create runtime user to perform both Policy Administration for RASADM
DECLARE
  rg_list XS$ROLE_GRANT_LIST;
BEGIN
  xs_principal.create_user(name=>'admin');
  sys.xs_principal.set_password('admin', 'welcome1',
XS_PRINCIPAL.XS_SALTED_SHA1);
  rg_list := XS$ROLE_GRANT_LIST(XS$ROLE_GRANT_TYPE('RASADM_POLICY_ADMIN'));
  xs_principal.grant_roles('admin', rg_list);
END;
/
```

Implementing the Password Policy

You must implement a password policy for `admin` users.

The `admin` user's password policy is supported directly by Real Application Security.

> **See Also:**
>
> The section about the procedure for creating direct login users, creating profiles, and setting passwords in *Oracle Database Real Application Security Administrator's and Developer's Guide*.

Application Express Instance Level Configuration

Application Express and workspace configuration is the configuration that should be done at the Application Express instance level by the Application Express administrator or at the workspace level by the workspace administrator.

This configuration involves performing SSL setup. Oracle strongly recommends that SSL be used:

- Between the browser and the HTTP server

See the topics about utilizing secure sockets Layer (SSL) in *Oracle Application Express App Builder User's Guide* and requiring HTTPS in *Oracle Application Express App Builder User's Guide*.

See the HTTP Server documentation for more information about setting up SSL.

- Between the HTTP server to the database

  See the topics about configuring wallet information in *Oracle Application Express Administration Guide* and enabling the HTTP Listener to use SSL in *Oracle XML DB Developer's Guide*. See the topic about configuring secure sockets layer authentication in *Oracle Database Security Guide*.

- Between the database to LDAP

  See the topics about configuring secure sockets layer (SSL) in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory,* configuring SSL by using LDAP commands in *Oracle Fusion Middleware Administrator's Guide for Oracle Internet Directory*, and setting up LDAP directory verification in *Oracle Application Express App Builder User's Guide*.

Note:

As part of the installation script for RASADM, Application Express is modified at the Instance Level to set `Allow Real Application Security` to `Yes` under the Security Settings.

See Also:

See the chapter about managing application security in *Oracle Application Express App Builder User's Guide* for more information.

Running the RASADM Application

Based on the kind of user logging into RASADM, certain UI components like buttons will be invisible to the non-privileged user. For example, all buttons for User Management will be invisible to the user who does not have the privilege to perform these actions.

The following URL is just an example and the real URL is based on your current Application Express configuration. Make sure the correct URL is provided. Then log in as the RASADM administrator using the same password given during the installation.

To run the RASADM application, you would enter in your browser a URL like the following: https://www.example.com:8080/apex/f?p=rasadm.

Oracle recommends that you turn on HTTPS.

You can log in as the RASADM `admin` user or any user created after installation using the password given during installation.

For More Information

The Real Application Security discussion forum and Real Application Security Documentation provide more information.

See the following resources for more information:

- Real Application Security discussion forum: Database Security — General Discussion
- Real Application Security Documentation: *Oracle Database Real Application Security Administrator's and Developer's Guide*

About Data Security with Oracle Database Real Application Security

Effective security requires defining which application users, applications, or functions can have access to which data, to perform which kinds of operations.

Thus, effective security has these three dimensions:

1. Which application users (**principals**)
2. Can perform which operations (**application privileges**)
3. On which data (**data realms**)

You define (1) principals, (2) application privileges, and (3) objects (data realms) in relation to these three dimensions, respectively. Principals are users and roles, where users are application users, and a role can represent attributes of an application user, system state, or a piece of code.

Principals are granted application privileges in ACLs. These ACLs are then related to the data by defining a data security policy that protects rows and columns of table data.

Using RASADM, you create Real Application Security data security policies as follows:

1. Understand the basic elements of a data security policy described in Terminology Used in Real Application Security.
2. Understand how to join these basic elements together in a step-by-step fashion described in the Design Phase.
3. Create the data security policy using RASADM in a step-by-step fashion described in the Development Flow.

Terminology Used in Real Application Security

Defines terminology for you to better understand Real Application Security concepts used in the RASADM application.

An **application user** is an application end user identity that is known to the database. These users are schema-less and do not own any database objects or resources. The application user creates application sessions to the database through the middle tier

and can create application sessions to the database directly through the direct logon application user account. Using RASADM, you can create application users.

An **application privilege** is a named privilege to control execution of application-level operations. The operations can be on data or application artifacts, such as UI artifacts representing workflow tasks or buttons and pages in a Web application. An application privilege can imply other application privileges including `SELECT`, `INSERT`, and `DELETE` of the Real Application Security DML privilege class.

An **application role** represents a group of application users who have been granted the role. Within an access control list (ACL), privileges can be granted to a role, which has the same effect as granting those privileges to all users who have been granted the role. An application role can be only granted to application users or application roles.

A **dynamic application role** is an application role that is enabled only under certain situations, for example, when a user has logged on using SSL, or during a specific period of time, and so on. You cannot grant dynamic application roles to other application roles or users, but you can grant other application roles to dynamic application roles.

A **privilege class** is a scope for a set of application privileges. A privilege class defines a set of privileges that can be granted within access control lists (ACLs) of a data security policy.

An **access control entry (ACE)** either grants or denies application privileges to a particular principal (application user or application role).

An **access control list (ACL)** is a named list of privilege grants. Oracle Real Application Security ACL allows various constraints on the privilege grants such as ordered negative grants. If the ACL you create relies on a set of custom application privileges that you define in your own privilege class, then you can only grant privileges on that privilege class.

A **data realm** is a collection of a logical set of rows in a group of related application tables associated with ACLs. A data realm represents an application-level resource or business object and is defined using a SQL predicate. The authorization is defined in the ACL, which specifies what privileges are granted to which principles on the data set. RASADM supports the following data realm types:

- Regular - protects a data set when you specify in a SQL predicate the part of the data set to be protected and the ACL to be used to perform authorization.
- Parameterized - protects a data set when you specify in a SQL predicate a parameter to be used and in the ACL the values of that parameter to be granted permission. For example, consider `department=&DEPT_ID`, where the parameter name `DEPT_ID` follows the symbol `&`. In this case, the parameter name `DEPT_ID` is associated with different department IDs. This enables you to create the grant based on department IDs without having to create many department ID-specific data realms for each `DEPT_ID` value.
- Inherited - known as the master-detail policy uses the master object's policy to protect the detail object by pointing to the master object. You specify the parent schema and parent object (column) as master, then build the 1:1 relationship between the parent column and either the child column (detail) object or a constant value. You can build the relationship using multiple parent = child pairs.

With multiple parent = child pairs, the constant value must work with other parent = child pairs as a join condition to form the 1:1 relationship. You can optionally enter a when condition if you want to further protect child columns with the parent's object policy.

A **data security policy** protects data realms by associating them with ACLs. Database records, both at the row and column level, can be protected using the fine-grained access control. The data security policy performs the following two functions:

- Data realm authorization.

  Data realm authorization specifies the data that you want to protect in a data realm of one or more rows and associates each data realm with one access control list (ACL). The ACL specifies which kinds of access by means of application privileges are granted or denied to particular principals. This controls access to rows of the data realm to form what is called a data realm authorization. A given ACL protects a given data realm and controls access to particular application users or application roles (called principals).

- Column authorization.

  Column authorization optionally applies additional application privileges to protect a particular column. This is useful in cases where you need to add column authorization security for sensitive column data in which to associate additional custom application privileges.

In summary, the application user who logs in will only be allowed to perform operations including DML on records within the data realm, including individual rows of data, based on the application privileges in its associated ACLs. Thus, the data security policy is composed of data realm authorization and column authorization that protects the data realm by only allowing access to application users who have application privileges in the associated ACLs.

An **authorization service** checks if a privilege is granted to a user.

Session **namespace** attributes are collections of attribute-value pairs under an application namespace with an associated access control policy. Often, an application needs to use the same namespace across different application sessions. You can create a namespace template to define and initialize a namespace. A namespace template defines the namespace and its properties. It is used to initialize the namespace in an application session.

An **application session** is an application users' session that corresponds to application users' security contexts, roles, and namespace attributes, in the database.

Design Phase

The design phase involves identifying all tasks an application performs that require application privileges to control data access.

For example, during the design phase, the application policy designer must identify:

1. The set of application-level operations that require access control.
2. The rows and columns of tables and views that can be accessed as part of the application-level operations.

3. The set of actors or principals (users and roles) that can perform these operations.
4. The runtime application session attributes that identity rows of a table or views. These attribute names are used within the predicates that selects the rows to be authorized, and their values are set during the execution of the application.

Development Flow

In the development phase, as the RASADM administrator, you use RASADM to develop your data security policies.

Follow these steps to develop your data security policies:

1. Create the corresponding application users and roles. If using an external directory server, create the application users and roles or user groups in the directory server. Follow this procedure to create these principals natively in the database:
    a. Create the application roles and grant application roles to application roles, if needed. See Creating Application Roles.
    b. Create the application users and grant application roles to the application users. See Creating Application Users.
    c. Configure the directory server to fetch the users and role, when principals from external stores are used. See Configuration.
    d. For users and roles in the external Directory Server, manage parameter settings for using RASADM with a Directory Server. See Manage Settings.
2. Create each privilege class that you plan to use to develop the security policies for your application. Each privilege class consists of one or more appropriate privileges that you define and can reference in an ACL and also grant them to the application users and application roles. Each privilege class authorizes by means of ACLs the required application-level operations of a data security policy. See Creating Application Privilege Classes.
3. Create one or more session namespaces that can be used across different application sessions. This consists of defining for a session namespace its set of properties (application attributes) and its associated access control policy or ACL that you can choose from a list or create. See Creating Namespaces.
4. Create the data security policy by associating each data realm with an ACL, so as to create both data realm authorization and column authorization as needed. This process consists of four parts:
    a. Policy Information - You choose the object to be protected and the privilege class to protect it as well as specify the policy name and select the policy owner. See Step 3 in Creating Data Security Policies.
    b. Column Level Authorization - You choose the name of the column to be protected and select the privilege to be granted to access the column, which is associated with the privilege class you selected in Step 3a. See Step 4 in Creating Data Security Policies.
    c. Data Realm Authorization - You create a SQL predicate to represent the data realm to be protected and add each to a data realm grant list. Then you choose or create the ACL to protect the data realm. Next, create privilege

grants to be added to a privilege grants list consisting of each principal and whether it is allowed authorization or denied authorization by selecting the appropriate privilege. See Step 5 in Creating Data Security Policies.

d. Apply Policy - You can apply, remove, enable, or disable the data security policy you are creating and choose to specify certain apply options, allowing the owner of the table or view to bypass this data security policy, and whether to enforce statement types for this policy. See Step 6 in Creating Data Security Policies.

Real Application Security Administration Home Page

The Real Application Security Administration **Home** page provides an overview of data security policy activity.

It includes the following topics:

- Introduction
- Policy Modification Report
- Auditing Report

Introduction

Provides an overview of Real Application Security Administration.

Provides the steps to follow to create a data security policy.

Policy Summary Report

The Policy Summary Report consists of two reports.

It includes:

- Users and Roles Report
- Data Security Report

Users and Roles Report

Shows how many application users and role entities are created from external stores and in the database.

Click the **Count** link to view an entity's summary report.

Data Security Report

Shows how many data security entities are created, including data security policies, data realms, and privilege classes.

Click the **Count** link to view an entity's summary report.

Policy Modification Report

The **Policy Modification Report** consists of five reports.

It includes:

- Modification Count Report
- Data Securities Policies Report
- Privilege Grants to Data Realms Report
- Application Roles in Database Report
- Application Users in Database Report

Modification Count Report

Shows how many modifications there are for each entity for each time period.

Data Securities Policies Report

Shows for each policy, when it was modified and created, its name and description, target object, and current status.

Click **Next** to view the next set of records.

Privilege Grants to Data Realms Report

Shows for each data realm, when it was modified and created, the policy name, the data realm name to which the ACL was granted, and the ACL that was granted to the data realm.

Click **Next** to view the next set of records.

Application Roles in Database Report

Shows for each principal type, role or dynamic role, when it was modified and created, the role name, description, and type.

Click **Next** to view the next set of records.

Application Users in Database Report

Shows for each user, when it was modified and created, the user name, description, and status.

Click **Next** to view the next set of records.

Auditing Report

The Auditing Report consists of two reports.

It includes:

- Audit Policies

- Audit Policies Enabled

Audit Policies

Shows the name of the audit policy and other important information.

Shows the condition associated with the audit policy, the auditing option defined in the audit policy, the evaluation option (`STATEMENT`, `SESSION`, or `INSTANCE`) associated with the audit policy's condition, and whether the audit policy is a common audit policy (`YES`) or local (`NO`) or `NULL` in non-CDBs. Click **Next** to view the next set of records.

Audit Policies Enabled

Shows the database user name for whom the policy is enabled and other important information.

Shows if the audit policy is enabled for all users the value is `ALL USERS`; name of the audit policy; the enabled option (`BY`, `EXCEPT`, or `DISABLED`) of the audit policy; indicates whether the audit policy is enabled for auditing successful events (`YES`) or not (`NO`); and indicates whether the audit policy is enabled for auditing unsuccessful events (`YES`) or not (`NO`). Click **Next** to view the next set of records.

Getting Started

From the Real Application Security Administration **Home** page, you can begin to develop a data security policy for securing an application.

You can navigate to following tabs to perform tasks:

> **Note:**
>
> Names are case sensitive for all Real Application Security entities that are created using the RASADM application.

- **Policies** - Create, update, and delete data security policies including adding and deleting data realms and column authorizations; and for each defined policy, set its status to enable it, disable it, apply it, or remove it.
- **Privileges** - Create, update, and delete privilege classes, including adding application privileges to or deleting application privileges from a privilege class.
- **Namespaces** - Create, update, and delete namespaces, including adding application attributes to a namespace or deleting application attributes from a namespace.
- **Users** - Create, update, and delete application users, including granting application roles to application users and revoking application roles from application users.
- **Roles** - Create, update, and delete application roles and dynamic application roles, including for application roles, adding role grants to or deleting role grants

from an application role; and for dynamic application roles, adding object privilege grants to or deleting object privilege grants from a dynamic application role.

- **Settings** - Update parameter settings for using Real Application Security Administration with a Directory Server.

Using Real Application Security Administration, you can perform the following tasks for developing a data security policy for securing an application:

1. Manage Application Users
2. Manage Application Roles and Dynamic Application Roles
3. Manage Application Privilege Classes
4. Manage Data Security Policies to Secure Data Rows and Columns in the Application
5. Manage Namespaces
6. Manage Settings

The topics that follow describe in detail how to perform each of these tasks using Real Application Security Administration.

Manage Application Users

From the **Users** tab, the RASADM user creates, updates, or deletes application users that are known to the database. The application user creates application sessions to the database through the middle tier and can create application sessions to the database directly through the direct logon application user account.

Managing application users includes the following topics:

- Creating Application Users
- Updating Application Users
- Deleting Application Users

Creating Application Users

From the **Users** tab, create each application user you need to add to your data security policy for this application.

To create an application user:

1. Click the **Users** tab.

> **Note:**
>
> Steps 2 to 5 are not applicable for the user without `RASADM_USER_ADMIN` Real Application Security role.

2. On the **Users** page, click **Create**.

> **Note:**
>
> The **Create** button would be invisible for a user without `RASADM_USER_ADMIN` Real Application Security role.

3. On the **Manage User** page in the **Application User** section, enter information in the following fields. A red asterisk denotes a required field.
   - **User Name** - Enter the name of the application user. Names are case sensitive.
   - **Description** - Enter a brief description about this application user.
   - **Default Schema** - Click (**^**) to select the schema for this application user to access.
   - **Roles Default Enabled** - Choose whether the default application roles are enabled (`Yes`) or not (`No`).
   - **Status** - Choose whether the application user is to be active or inactive.
   - **Start Date** - Click the calendar icon to select an effective start date for this application user or leave the field blank. No start date means this application user is always effective.
   - **End Date** - Click the calendar icon to select an effective end date for this application user or leave the field blank. No end date means this application user is always effective. If you specify a start date, you must specify an end date.

   In the **Roles Grants** section, select application roles to be granted to the application user. An application role must already have been created to select it. A red asterisk denotes a required field. Enter information in the following fields:
   - **Role** - Click (**^**) to select an application role to be granted to this application user.
   - **Start Date** - Click the calendar icon to select an effective start date for this role grant or leave the field blank. No start date means this role grant is always effective.
   - **End Date** - Click the calendar icon to select an effective end date for this role grant or leave the field blank. No end date means this role grant is always effective. If you specify a start date, you must specify an end date.

   Click **Add** to grant the role.

   To grant more application roles to this application user, choose another role, and if needed select the start date and end date, and then click **Add**, and so forth.

   To delete one or more application roles from this user, select each one and then click **Delete**.
4. Click **Apply Changes** to create this application user.
5. Repeat Steps 1 through 4 for each application user you need to add to your data security policy for this application.

Updating Application Users

From the **Users** tab, make updates to application users in your application. The RASADM user can grant more application roles to or delete some application roles from the application user.

To update information for an application user:

1. Click the **Users** tab.
2. Select the name of the application user in the **User** column you want to update.
3. On the **Manage User** page, make your updates.

   To grant more application roles to the application user, choose another role, and if needed enter the start date and end date, and then click **Add**.

   To delete one or more application roles from an application user, select each one to be deleted in the **Direct Role Grants** section, and then click **Delete**.

   If an application user has indirectly been granted one or more application roles, these application roles are listed in the **Indirect Role Grants** section along with the name of the root role and the grant path.

> **Note:**
>
> All the buttons except **Cancel** will be invisible to a user without `RASADM_USER_ADMIN` Real Application Security role.

4. Click **Apply Changes** to save your changes.

> **See Also:**
>
> Creating Application Users for information about the fields on the **Manage User** page.

Deleting Application Users

From the **Users** tab, delete any application users that are no longer needed for this application.

To delete an application user:

1. Click the **Users** tab.
2. In the **User** column of the **Users** page, click the name of the application user you want to delete.
3. In the **Application User** section of the **Manage User** page, click **Delete**.

> **Note:**
>
> The **Delete** Button is invisible to a user without `RASADM_USER_ADMIN` Real Application Security role.

Manage Application Roles and Dynamic Application Roles

From the **Roles** tab, create and grant regular and dynamic application roles. An application role can be granted to an application user or another application role. A dynamic application role cannot be granted to other application users or application roles; it is enabled only under certain situations..

Managing application roles and dynamic application roles includes the following topics:

- Creating Application Roles
- Updating Application Roles
- Deleting Application Roles

Creating Application Roles

Create the application roles and dynamic roles you need for the data security policy for this application.

To create an application role:

1. Click the **Roles** tab.
2. On the **Roles** page, click **Create Role**.
3. On the **Manage Role** page in the **Application Role** section, enter information in the following fields. A red asterisk denotes a required field.
   - **Role Name** - Enter the name of the application role. Names are case sensitive.
   - **Description** - Enter a brief description for this application role.
   - **Role Type** - Choose `REGULAR` or `DYNAMIC`. **Role Type**: `Regular` = application role, `Dynamic` = dynamic application role.
     - **REGULAR**

       Enabled by Default - Choose whether to enable this application role upon creation (`Yes`) or not to enable it (`No`) (the default) upon creation.

       Start Date - Click the calendar icon to select an effective start date for this application role or leave the field blank. No start date means this application role is always effective.

       End Date - Click the calendar icon to select an effective end date for this application role or leave the field blank. No end date means this application role is always effective. If you specify a start date, you must specify an end date.

– **DYNAMIC**

Duration - Enter the duration (in minutes) of the dynamic application role.

Scope - Enter the scope attribute of the dynamic application role. **Session**, the default, means the enabled dynamic application role is still enabled when you detach the session and attach to the session again, unless you explicitly specify that it be disabled in the session reattach. **Request** means that the dynamic application role is disabled after the session is detached.

In the **Role Grants** section, select application roles to be granted to the application role. A role must already have been created to grant it. A red asterisk denotes a required field. Enter information in the following fields:

- **Role** - Click (**^**) to select an application role to be granted to this application role.
- **Start Date** - Click the calendar icon to select an effective start date for this role grant or leave the field blank. No start date means this role grant is always effective.
- **End Date** - Click the calendar icon to select an effective end date for this role grant or leave the field blank. No end date means this role grant is always effective. If you specify a start date, you must specify an end date.

Click **Add** to grant the role.

To grant more application roles to this application role, choose another application role, and if needed select the start date and end date, and then click **Add**, and so forth.

To delete one or more granted application roles from this application role, select each role to be deleted and click **Delete**.

4. Click **Apply Changes** to create the application role.
5. Repeat Steps 1 through 4 for each application role you need to add to your data security policy for this application.

> **See Also:**
>
> Terminology Used in Real Application Security for more information about application role and dynamic application role.

Updating Application Roles

From the **Roles** tab, grant more application roles to an application role or delete one or more application roles from an application role. Check the **Indirect Role Grants** section if an application role has indirectly been granted one or more application roles.

To update information for an application role:

1. Click the **Roles** tab.

2. In the **Role** column of the **Roles** page, select the name of the application role you want to update.
3. On the **Manage Role** page, make your updates.

   To grant more application roles to the application role, choose another application role, and if needed select the start date and end date, and then click **Add**.

   To delete one or more granted application roles from an application role, select each one to be deleted in the **Role Grants** section, and then click **Delete**.

   If an application role has indirectly been granted one or more application roles, these application roles are listed in the **Indirect Role Grants** section along with the name of the root role and the grant path.
4. Click **Apply Changes** to save your changes.

> **See Also:**
>
> Creating Application Roles for information about the fields on the **Manage Role** page.

Deleting Application Roles

From the **Roles** tab, delete the roles that you no longer need in your data security policy for this application.

To delete an application role:

1. Click the **Roles** tab.
2. In the **Role** column of the **Roles** page, click the name of the application role you want to delete.
3. In the **Application Role** section of the **Manage Role** page, click **Delete**.

Manage Application Privilege Classes

From the **Privileges** tab, create, update, and delete application privilege classes. An application privilege is a named privilege to control execution of application-level operations. Create application privilege classes to add to your data security policy for this application.

Managing application privileges includes the following topics:

- Creating Application Privilege Classes
- Updating Application Privilege Classes
- Deleting Application Privilege Classes

Creating Application Privilege Classes

From the **Privileges** tab, create each application privilege class you need to add to your data security policy for this application.

To create application privilege classes:

1. Click the **Privileges** tab.
2. On the **Privileges** page, click **Create**.
3. On the **Manage Privilege** page in the **Privilege Class** section, enter information in the following fields. A red asterisk denotes a required field.
   - **Privilege Class Schema** - Click (^) to select the schema name.
   - **Privilege Class Name** - Enter a name for the privilege class. Names are case sensitive.
   - **Description** - Enter a brief description for the privilege class.

   In the **Application Privileges** section, enter information in the following fields. A red asterisk denotes a required field.
   - **Privilege Name** - Enter the name of the privilege.
   - **Description** - Enter a brief description for this privilege.
   - **Implied Privileges** - Select one or more DML privileges listed to be implied privileges. When the application privilege is granted to a principal, its implied privileges are also granted.

   Click **Add** to add the application privilege to this application privilege class.

   Repeat this step to add additional application privileges to this application privilege class.
4. Click **Apply Changes** to create the application privilege class.
5. Repeat Steps 1 through 4 for each privilege class you need to add to your data security policy for this application.

Updating Application Privilege Classes

From the **Privileges** tab, add new application privileges to the application privilege class or delete one or more application privileges from the application privilege class.

To update information for an application privilege class:

1. Click the **Privileges** tab.
2. In the **Privilege Class** column of the **Privileges** page, select the name of the privilege class you want to update.
3. On the **Manage Privilege** page, make your updates.

   To add a new application privilege to this privilege class, enter the privilege name, a brief description of the privilege, select the DML privileges to be implied privileges for this application privilege, and then click **Add**.

   To delete one or more application privileges from the privilege class, select each one to be deleted in the **Application Privileges** section, and then click **Delete**.
4. Click **Apply Changes** to save your changes.

> **See Also:**
>
> Creating Application Privilege Classes for information about the fields on the **Manage Privilege** page.

Deleting Application Privilege Classes

From the **Privileges** tab, delete the application privilege class from your data security policy for this application.

To delete an application privilege class:

1. Click the **Privileges** tab.
2. In the **Privilege Class** column of the **Privileges** page, click the name of the privilege class you want to delete.
3. In the **Privilege Class** section of the **Manage Privilege** page, click **Delete**, and then click **OK** to delete the privilege class.

Manage Data Security Policies to Secure Data Rows and Columns in the Application

From the **Policies** tab, create, update, or delete data security policies that secure data rows and columns for tables or views for this application.

Managing data security policies includes the following topics:

- Creating Data Security Policies
- Updating Data Security Policies
- Deleting Data Security Policies

Creating Data Security Policies

From the **Policies** tab, create the data security policy to secure data rows and columns for tables or views for this application.

To create a data security policy:

1. Click the **Policies** tab.
2. On the **Policies** page, click **Create**.
3. **Policy Information**. Enter information in the following fields. A red asterisk denotes a required field.
    - **Policy Owner** - Click (**^**) to select a policy owner.
    - **Policy Name** - Enter a name for the data security policy. Names are case sensitive.
    - **Description** - Enter a brief description for the data security policy.

- **Privilege Class** - Click (^) to select a privilege class. Or click **NEW** to create a new privilege class, or click **MODIFY** to update the selected privilege class.
- **Protected Object's Schema** - Click (^) to select the name of the object's schema to be protected.

> **Note:**
>
> Only the authorized schemas are shown in the list of values. You must grant the `SELECT` privilege on the target object if a specific schema is not shown.

- **Protected Object** - Click (^) to select the object to be protected.

Click **Next** to continue after entering information in the **Policy Information** section.

4. **Column Authorization**. Enter the following information to create a column authorization:
   - **Column** - Click (^) to select the name of the column to be protected.
   - **Privilege** - Click (^) to select a privilege to be applied to the column. The privilege must already have been created. The list of privileges that appear are those associated with the **Privilege Class** you selected on the **Policy Information** page in Step 3.

   Click **Add** to add the column authorization to the **Column Authorization Created** list. Repeat this step to add additional column authorizations.

   Click **Next** to continue after entering information in the **Column Authorization** section.
5. **Data Realm Authorization**. Enter information in the following fields:
   - **Name** - Enter the name of the data realm. Names are case sensitive.
   - **Description** - Enter a brief description about this data realm.
   - **Realm Type** - Select the type of data realm:
     - **REGULAR** - Allows you to create a data realm or set of data associated with an ACL, in which the data set is defined by a SQL predicate and the authorization is defined in the ACL. The ACL specifies what privileges are granted to which principals on the data set. For a **REGULAR** data realm, specify the SQL predicate and an ACL.

       For example, if you want to create a data realm for the `DEPARTMENT` table with the ID of 60 in the `HR` schema, you would specify a SQL predicate of `DEPARTMENT_ID=60`. The defined ACL would grant the `SELECT` privilege to the principal `EMPLOYEE` for the principal store DATABASE and also grant the `VIEW_SALARY` privilege to the principal `EMPLOYEE` for the principal store `DATABASE`. This would allow only the employees for this department with the ID of 60 to view their own salary.

       ACL

       Enter the following information:

ACL Name - Click (**^**) to select an ACL name. Or, click **NEW** to create an ACL. Or select an ACL name and click **MODIFY** to modify the ACL.

- **INHERITED** - Also known as master-detail, allows you to use the master object's policy to protect the detail object by pointing to a master object, so you do not have to create another duplicate policy on the detail object. For an **INHERITED** data realm, you must choose the **Parent Schema** and **Parent Object** and optionally enter a **When Condition**. The **When Condition** is used to further filter the child table records that could meet the parent to child relationship. The parent to child relationship is defined by giving parent.column = child.column.

  For example, using the **HR** schema, if you want to create a master-detail policy between the **DEPARTMENTS** parent table and the **EMPLOYEES** child table, you would specify `HR` as the **Parent Schema**, `DEPARTMENTS` as the **Parent Object** and enter `1=1` for the **When Condition**. Then, for **Realm Inheritance**, you would select `DEPARTMENT_ID(NUMBER)` as the **Parent Column**, select `COLUMN NAME` as the **Child Type**, then select `DEPARTMENT_ID(NUMBER)` as the value, then click **Add**. The **Realm Inheritance** list will show the entry: `(HR.DEPARTMENTS) DEPARTMENT_ID= (HR.EMPLOYEES) DEPARTMENT_ID`, which establishes the parent = child pair join condition to form the 1:1 relationship.

  Enter information for the following fields:

  Parent Schema - Select the name of the parent schema as the master object.

  Parent Object - Select the name of the parent object as the master object.

  When Condition - Enter a predicate to further filter the child records that you want to be protected by the parent's object policy or use Predicate Builder to create the predicate.

  Realm Inheritance

  Enter information for the following fields:

  Parent Column - Select the parent column.

  Child Type - Select the child type. If **COLUMN NAME** is selected, click (**^**) in the adjacent field to choose the column name. If **VALUE** is selected, enter a value in the field to the right.

  Click **Add** to add this realm inheritance to the list.

  Repeat this process to add more realm inheritances to the **Realm Inheritance** list.

  Realm Inheritance - Lists the realm inheritance relationships already created.

  Data Realm Created - Lists the created data realms.

- **PARAMETERIZED** - Allows parameters to be used in the realm's SQL predicate, such as `department=&DEPT_ID`. Note the use of the symbol `&` preceding the parameter name to represent the parameter. With a parameterized data realm, multiple "value-ACL" can be given to one

parameter, which in turn, allows that parameterized data realm to be instantiated as multiple regular data realms, so you do not have to create multiple regular data realms. For a **PARAMETERIZED** data realm, you must specify the SQL predicate and an ACL.

For example, if you specify `DEPARTMENT_ID=&DEPT_ID,`. the parameter name `DEPT_ID` is associated with different department IDs, which are each granted permission. This enables you to create the grant based on department IDs without having to create many department ID-specific data realms for each `DEPT_ID` value.

ACL Parameters

Enter information for the following fields:

ACL - Click (**^**) to select an ACL name. Or, click **NEW** to create an ACL, or click **MODIFY** to update the selected ACL.

Parameter Name - Enter a parameter name or click (**^**) to select a parameter name from the list. The parameter name is automatically extracted from the predicate and appears in this list.

Parameter Type - Select the parameter type: `NUMBER` or `VARCHAR`.

Parameter Value - Enter the parameter value.

Click **Add** to add this ACL parameter to the list.

Repeat this process to add more ACL parameters to the **ACL Parameters** list.

ACL Parameters - Lists the ACL parameters that are already defined.

- **SQL Predicate** - Click (**^**) to select a SQL predicate. Or, click (**>**) to expand the **Predicate Builder** field and enter information for the following fields:
  - **Column Name** - Click (**^**) to select a column name. The list of columns from which to select are those associated with the **Protected Object** you selected on the **Policy Information** page in Step 3.
  - **Operator** - Click (**^**) to select an operator.
  - **Value** - Enter a value. The value field will auto-complete to automatically populate values for selection that match the value entered. For the parameterized data realm, once `&` is entered, the previously defined parameters are automatically populated from which you select the one you want.
  - **AND/OR** - If needed, click (**v**) and select **AND** or **OR** to further develop the SQL predicate.
  - **Predicate Construction** - As you construct the SQL Predicate, it will be constructed in this field and provide you feedback as to whether the predicate is valid and complete to assist you in this operation.

  Click **Preview** to test the SQL predicate. Inspect the query results that display. If the results are satisfactory, click **Apply** to add the predicate to the **SQL Predicate** field.

  Click **Next** to add the data realm to the **Data Realm Authorization** list.

Repeat this process to create additional data realms and to add them to the **Data Realm Created** list.

In the **Data Realm Created** list, click (**^**) or click (**v**) to reorder the evaluation order for each data realm. The first data realm in the list is evaluated first, the second one is evaluated next, and so on.

To delete one or more data realms from the **Data Realm Grant** list, select them, and click **Delete**.

ACL

To create an ACL, on the **Access Control List (ACL)** section, enter information for the following fields:

- **ACL Name** - Enter the name of the ACL. Names are case sensitive.
- **Description** - Enter a brief description for the ACL.
- **ACL Inheritance** - Click (**>**) to expand the field. Enter the following information:
  - **Parent** - Click (**^**) to select a parent ACL.
  - **Inherit Mode** - Choose **Extended** or **Constrained**.

    Extended means extending ACL inheritance (OR with ordered evaluation). This option dictates that the ACEs are evaluated from the bottom of the inheritance tree to its top, from child to parent.

    Constrained means constraining ACL inheritance (AND) requires that both the child and the parent ACL grant the application privilege so that the ACL check evaluates to `true`.

  For **Privilege Grants**, enter the following information:

  - **Principal** - Click (**<-**) to specify search criteria to find the principal, then select the principal. For search criteria, specify the **Principal Type** as `Role` or `User`, and **Principal Store** as `Database` or `External`, and then click **Search**. Select the principal from the return list. Note that the word `Database` mentioned here means the principal store for the Real Application Security application user and role.
  - **All Except** - Select this option to grant all privileges to the principal except the one specified or leave this option deselected to grant or deny only the specified privilege.
  - **Privilege** - Click (**v**) to select the application privilege.
  - **Grant Type** - Choose **Grant** to grant this application privilege to this principal or choose **Deny** to deny this application privilege from this principal.
  - **Start Date** - Click the calendar icon to select an effective start date for this privilege grant or leave the field blank. No start date means this privilege grant is always effective.
  - **End Date** - Click the calendar icon to select an effective end date for this privilege grant or leave the field blank. No end date means this privilege grant is always effective. If you specify a start date, you must specify an end date.

Click **Add** to add this privilege grant to the ACL.

Repeat this process to add another privilege grant to the ACL.

In the **Privilege Grants** list, click (**^**) or click (**v**) to reorder the evaluation order for each privilege grant. The first privilege grant in the list is evaluated first, the second one is evaluated next, and so on.

To delete one or more privilege grants from an ACL, select them and then click **Delete**.

Click **Apply Changes** to create the ACL.

> **Note:**
>
> At this point, if you click **Cancel** to cancel creating the data security policy, the ACL you just created is not associated with a data security policy. This ACL can be viewed in the ACL list during security policy creation and reused only if the next data security policy you create has the same security class. Otherwise, not using the same security class, this ACL is not listed in the ACL list and reused.

Click **Add** to add this data realm to the **Data Realm Created** list.

Click **Next** to continue after entering information in the **Data Realm Authorization** section.

6. **Apply Policy**. The **Policy Name** and **Object Name** names display for the data security policy. Enter the following information:
   - In the **Apply Policy** field, specify the policy status for this policy as either `Apply`, `Remove`, `Enable`, or `Disable`. If you select `Apply`, specify the **Apply Options**.
   - Click (**>**) to expand **Apply Options**. Enter information for the following fields:
     - **ACL Per Row** - Whether the policy is to create hidden columns. `True` or `False`, the default is `False`. A value of `True` creates the hidden columns `SYS_ACLOD`.
     - **Owner Bypass** - Whether the owner of the row can bypass the data security policy, `True` or `False`, the default is `False`.
     - **Statement Type** - Whether to enforce all statement types (`Select`, `Insert`, `Update`, `Delete`) for this policy. Deselect statement types as needed; by default all statement types are selected.

   Click **Apply Changes** to create the data security policy.

> **See Also:**
>
> For **Privilege Class**, if clicking **NEW** to create a new privilege class, refer to Creating Application Privilege Classes for information about creating a privilege class.

Updating Data Security Policies

From the **Policies** tab, update the data security policy by applying the same policy to other objects, such as a table or view to secure these data rows and columns for this application.

To update information for a data security policy:

1. Click the **Policies** tab.
2. In the **Policy** column of the **Policies** page, select the policy name you want to update.
3. On the **Policy Definition** page, make your updates.

   Note that an update you can make is to apply the same policy to other objects, such as a table or view. You can do that by clicking **ADD** next to the **Protected Objects** field on the **Policy Definition** page. After selecting the object to protect and clicking **Apply Changes**, the **Apply Policy** page displays where you can click **Apply Changes** to apply the policy on the new object. During the apply operation, a validation is performed to validate the column or realm authorization applicable to the new object. If the column authorization is not valid for this new object, RASADM does not allow you to complete the apply operation. If the realm predicate is not valid, a warning displays next to the object's name, but RASADM allows you to apply the policy.
4. Click **Apply Changes** to save your changes.

> **See Also:**
>
> Creating Data Security Policies for information about the fields on the **Policy Definition** page.

Deleting Data Security Policies

From the **Policies** tab, delete the data security policy for the table or view that is no longer needed for this application.

To delete a data security policy:

1. Click the **Policies** tab.
2. In the **Policy** column of the **Policies** page, click the policy name you want to delete.
3. In the **Policy** section of the **Policy Definition** page, click **Delete**, and then click **OK** to delete the policy.

Manage Namespaces

From the **Policies** tab, create session namespaces that your application can use across different sessions. Create a session namespace template to define the namespace and its properties to initialize the namespace in an application session.

Managing namespaces includes the following topics:

- Creating Namespaces
- Updating Namespaces
- Deleting Namespaces

Creating Namespaces

From the **Namespaces** tab, create the session namespace you need to add to your data security policy for this application.

To create a namespace:

1. Click the **Namespaces** tab.
2. On the **Namespaces** page, click **Create**.
3. On the **Manage Namespaces** page in the **Application Namespace** section, enter information in the following fields. A red asterisk denotes a required field.
    - **Namespace Name** - Enter a name for the namespace. Names are case sensitive.
    - **Description** - Enter a brief description for the namespace.
    - **ACL** - Click (**^**) to select an ACL for this namespace.

      Or click **NEW** to create an ACL or **MODIFY** to update the selected ACL, and on the **Access Control List (ACL)** page, enter or change the following information.

        – **ACL Name** - Enter the name of the ACL. Cannot change this name.

        – **Description** - Enter a brief description for the ACL.

      For **ACL Inheritance**, click (**>**). Enter the following information:

        – **Parent** - Click (**^**) to select a parent ACL.

        – **Inherit Mode** - Choose **Extended** or **Constrained**.

          Extended means Extending ACL inheritance (OR with ordered evaluation). This option dictates that the ACEs are evaluated from the bottom of the inheritance tree to its top, from child to parent.

          Constrained means constraining ACL inheritance (AND) requires that both the child and the parent ACL grant the application privilege so that the ACL check evaluates to `true`.

      For **Privilege Grants**, enter the following information:

        – **Principal** - Click (**<-**) to select a principal. Select the **Principal Type**: `Role` or `User`, **Principal Store**: `Database` or `External`, and optionally enter filter information in the **Principal Filter** field, then click **Search**. From the search results shown, click **Select** to choose the desired **Principal** name.

`Database` means the database store is to be used. Note that the word `Database` mentioned here means the principal store for the Real Application Security application user and role.

For `External`, optionally enter filter information in the **Principal Filter** field, select the **ReFetch** option and then in the **Principal Store Password** field, enter the password, then click **Search**. From the results shown, click **Select** to choose the desired **Principal** name.

- **All Except** - Select this option to grant all privileges to the principal except the one specified or leave this option deselected to grant or deny only the specified privilege.
- **Privilege** - Click (**v**) to select an application privilege.
- **Grant Type** - Choose **Grant** to grant this application privilege to this principal or choose **Deny** to deny this application privilege from this principal.
- **Start Date** - Click the calendar icon to select an effective start date for this privilege grant or leave the field blank. No start date means this privilege grant is always effective.
- **End Date** - Click the calendar icon to select an effective end date for this privilege grant or leave the field blank. No end date means this privilege grant is always effective. If you specify a start date, you must specify an end date.

Click **Add** to add the privilege grant to the ACL.

Repeat this process to create another privilege grant to add to the ACL.

In the **Privilege Grants** list, click (**^**) or click (**v**) to reorder the evaluation order for each privilege grant. The first privilege grant in the list is evaluated first, the second one is evaluated next, and so on.

To delete one or more privilege grants from an ACL, select them, and then click **Delete**.

- **Event Handler** - Indicate whether an event handler is needed, `No` or `Yes`. If you indicate `Yes`, click (^) to select the **Handler Schema**, **Handler Package**, and **Handler Function**.

In the **Application Attributes** section, you can add namespace attributes and their default values. Enter information in the following field.

- **Attribute** and **Default Value** - Click **Add** to add a namespace attribute and its default value. Enter the attribute name in the **Attribute** column and its default value in the **Default Value** column. Select the **Attribute Event**: `None`, `First Read`, `Modify`, or `First Read and Modify`. Then click **Add** to add this application attribute.

Click **Add** to add another namespace attribute name and its default value.

4. Click **Apply Changes** to create the namespace.
5. Repeat Steps 1 through 4 for each namespace you need to add to your data security policy for this application.

> **See Also:**
>
> For the **Event Handler**, if answering `Yes` that the event handler is needed, refer to the section on components of namespace template in *Oracle Database Real Application Security Administrator's and Developer's Guide* for information about the namespace handler and how to create it using PL/SQL.

Updating Namespaces

From the **Namespaces** tab, make updates to any existing namespace by either adding an event handler if it did not have one previously or by adding or deleting application attributes.

To update information for a namespace:

1. Click the **Namespaces** tab.
2. In the **Application Namespace** column of the **Namespaces** page, click the namespace name you want to update.
3. On the **Manage Namespace** page, make your updates.

   If you had previously indicated no event handler was needed and now one is needed, select `Yes`, then click (^) to select the **Handler Schema**, **Handler Package**, and **Handler Function**.

   Click **Add** to add another application attribute. Enter the attribute name and its default value. Repeat this process to add each additional attribute and its default value.

   To delete one or more application attributes, select each one to be deleted in the **Application Attributes** section, and then click **Delete**.
4. Click **Apply Changes** to save your changes.

> **See Also:**
>
> Creating Namespaces for information about the fields on the **Manage Namespace** page.

Deleting Namespaces

From the **Namespaces** tab, delete the session namespace you no longer need in your data security policy for this application.

To delete a namespace:

1. Click the **Namespaces** tab.
2. In the **Application Namespace** column of the **Namespaces** page, click the namespace name you want to delete.

3. In the **Application Namespace** section of the **Manage Namespace** page, click **Delete**, and then click **OK** to delete the namespace.

Manage Settings

From the **Settings** tab, update the parameter settings for using Real Application Security Administration with a Directory Server.

Managing parameter settings for either the LDAP user or the LDAP group includes the following topics:

- Updating Parameter Settings for the LDAP User
- Updating Parameter Settings for the LDAP Group

Updating Parameter Settings for the LDAP User

From the **Settings** tab, update the parameter settings for the LDAP user.

To update information for these parameter settings:

1. Click the **Settings** tab.
2. In the **Name** column of the **Settings** page, select the group name that is already entered; for example, select the `LDAP_USER`.
3. On the **Manage Settings** page, make your updates.

> **Note:**
>
> Change these settings carefully because an incorrect setting in the **Parameters** section can adversely affect the connection to the Directory server.

The name of the LDAP group displays in the **Settings** section. You can make updates to the following fields in the **Settings** and **Parameters** sections:

- **Description** - Description for the user name.
- **Host** - Name of the host on which the Directory server is running.
- **Port** - Directory server port number.
- **User** - User entity location in the directory information tree (DIT)
- **Base** - Naming context used to store the user entry in the Directory server.
- **Name Attribute** - Name attribute and value pair.
- **ID Attribute** - ID attribute and value pair. The **ID attribute** should be an attribute of the LDAP entry, which is specified by the `base`. It should globally identify the user. Normally, a GUID is used. For Oracle Internet Directory (OID), it should be `orclguid`; for Microsoft Active Directory (AD), it should be `objectGUID`.
- **Description Attribute** - Description attribute and value pair.

- **SSL Wallet Location** - Path to the wallet on the file system, such as, `file:/home/mywallet`. The word `file:` must be used as a prefix.
- **SSL Authentication Mode** - Modes values are: 1 for no authentication required, 2 for one way authentication required, or 3 for two way authentication required.

4. Click **Apply Changes** to save your changes.

Updating Parameter Settings for the LDAP Group

From the **Settings** tab, update the parameter settings for the LDAP group.

To update information for these parameter settings:

1. Click the **Settings** tab.
2. In the **Name** column of the **Settings** page, select the group name that is already entered; for example, select the `LDAP_GROUP`.
3. On the **Manage Settings** page, make your updates.

> **Note:**
>
> Change these settings carefully because an incorrect setting in the **Parameters** section can adversely affect the connection to the Directory server.

The name of the LDAP group displays in the **Settings** section. You can make updates to the following fields in the **Settings** and **Parameters** sections:

- **Description** - Description for the group name.
- **Host** - Name of the host on which the Directory server is running.
- **Port** - Directory server port number.
- **User** - Group entity location in the directory information tree (DIT).
- **Base** - Naming context used to store the group entry in the Directory server.
- **Name Attribute** - Name attribute and value pair.
- **ID Attribute** - ID attribute and value pair. The **ID attribute** should be an attribute of the LDAP entry, which is specified by the `base`. It should globally identify the group. Normally, a GUID is used. For Oracle Internet Directory (OID), it should be `orclguid`; for Microsoft Active Directory (AD), it should be `objectGUID`.
- **Description Attribute** - Description attribute and value pair.
- **SSL Wallet Location** - Path to the wallet on the file system, such as, `file:/home/mywallet`. The word `file:` must be used as a prefix.
- **SSL Authentication Mode** - Modes values are: 1 for no authentication required, 2 for one way authentication required, or 3 for two way authentication required.

4. Click **Apply Changes** to save your changes.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Database Real Application Security Administration Console (RASADM) User's Guide, 12*c* Release 2 (12.2)
E85615-01