Rational. Directory Server

IBM

Product Manual

IBM Rational Directory Server

Product Manual

Release 5.0

Before using this information, be sure to read the general information under Appendix E, "Notices"on page 112.

Table of contents

1   *About this manual*

This manual describes the IBM® Rational® Directory Server (RDS). The RDS is a powerful solution for the centralized database that can be used by the enterprise to store and retrieve the large volume of data.

Purpose of this manual

This manual is intended to provide the information to the users who are new to the directory service concepts. This manual will enable the user to understand and start using the IBM Rational Directory Server with much ease.

What is a directory service?

The directory service allows you to maintain the data in an organized way. For example, the telephone directory holds the data about the individual (name, address, telephone number, etc.). The data is stored using a directory service. The directory can hold millions of entries depending on the directory service software. This number may be more than one server can reasonably be expected to hold. The directory service consists of at least one directory server and one client program. The client program can be used to access the information stored in the directory server.

Characteristics of a directory service

- **Hierarchical naming structure**

  This model uniquely identifies the names that have different origins but the same names without any ambiguity.

- **Extended search capability**

  This provides the robust search on individual attributes of entries.

- **Distributed data model**

  A directory service enables data to be distributed across multiple servers.

- **Shared access**

  The directory service enables shared access among applications.

How the data is maintained in a directory service

The data is maintained using the schema. The schema defines the structure and contents of any information resource. As a data catalog for a directory service, a schema identifies the entries (people, groups, application, etc.) and the types of attributes for those entries. The schema also maintains the integrity of the data stored in the directory by enforcing constraints on the size and format of data values. For more information on RDS schema, refer to *"RDS schema definition" on page 8*.

Contacting IBM Rational Software Support

If the self-help resources have not provided a resolution to your problem, you can contact IBM® Rational® Software Support for assistance in resolving product issues.

Note If you are a heritage Telelogic customer, a single reference site for all support resources is located at http://www.ibm.com/software/rational/support/telelogic/

Prerequisites

To submit your problem to IBM Rational Software Support, you must have an active Passport Advantage® software maintenance agreement. Passport Advantage is the IBM comprehensive software licensing and software maintenance (product upgrades and technical support) offering. You can enroll online in Passport Advantage from http://www.ibm.com/software/lotus/passportadvantage/howtoenroll.html

- To learn more about Passport Advantage, visit the Passport Advantage FAQs at http://www.ibm.com/software/lotus/passportadvantage/brochures_faqs_quickguides.html.

- For further assistance, contact your IBM representative.

To submit your problem online (from the IBM Web site) to IBM Rational Software Support, you must additionally:

- Be a registered user on the IBM Rational Software Support Web site. For details about registering, go to http://www.ibm.com/software/support/.

- Be listed as an authorized caller in the service request tool.

Submitting problems

To submit your problem to IBM Rational Software Support:

1. Determine the business impact of your problem. When you report a problem to IBM, you are asked to supply a severity level. Therefore, you need to understand and assess the business impact of the problem that you are reporting.

   Use the following table to determine the severity level.

Severity	Description
1	The problem has a *critical* business impact: You are unable to use the program, resulting in a critical impact on operations. This condition requires an immediate solution.
2	This problem has a *significant* business impact: The program is usable, but it is severely limited.
3	The problem has *some* business impact: The program is usable, but less significant features (not critical to operations) are unavailable.
4	The problem has *minimal* business impact: The problem causes little impact on operations or a reasonable circumvention to the problem was implemented.

2. Describe your problem and gather background information, When describing a problem to IBM, be as specific as possible. Include all relevant background information so that IBM Rational Software Support specialists can help you solve the problem efficiently. To save time, know the answers to these questions:

   • What software versions were you running when the problem occurred?

     To determine the exact product name and version, use the option applicable to you:

     • Start the IBM Installation Manager and select **File** > **View Installed Packages**. Expand a package group and select a package to see the package name and version number.
     • Start your product, and click **Help** > **About** to see the offering name and version number.

- What is your operating system and version number (including any service packs or patches)?
- Do you have logs, traces, and messages that are related to the problem symptoms?
- Can you recreate the problem? If so, what steps do you perform to recreate the problem?
- Did you make any changes to the system? For example, did you make changes to the hardware, operating system, networking software, or other system components?
- Are you currently using a workaround for the problem? If so, be prepared to describe the workaround when you report the problem.

3. Submit your problem to IBM Rational Software Support. You can submit your problem to IBM Rational Software Support in the following ways:

- **Online**: Go to the IBM Rational Software Support Web site at https://www.ibm.com/software/rational/support/ and in the Rational support task navigator, click **Open Service Request.** Select the electronic problem reporting tool, and open a Problem Management Record (PMR), describing the problem accurately in your own words.

  For more information about opening a service request, go to http://www.ibm.com/software/support/help.html

  You can also open an online service request using the IBM Support Assistant. For more information, go to http://www.ibm.com/software/support/isa/faq.html.

- **By phone**: For the phone number to call in your country or region, go to the IBM directory of worldwide contacts at http://www.ibm.com/planetwide/ and click the name of your country or geographic region.

- **Through your IBM Representative**: If you cannot access IBM Rational Software Support online or by phone, contact your IBM Representative. If necessary, your IBM Representative can open a service request for you. You can find complete contact information for each country at http://www.ibm.com/planetwide/.

Conventions used in this Guide

| Typeface	Description
Italic	Used for book titles and terminology.
Bold	Used for items that you can select and menu paths, also used for emphasis.
`Courier`	Used for commands, file names, and directory paths. Represents command syntax to be entered verbatim. Signifies computer output that displays on-screen.
`Courier Italic`	Represents values in a command string that you supply. For example, (`drive:\username\commands`).

2   *IBM Rational Directory Server (RDS)*

Introduction

The RDS is a single enterprise directory solution designed for user authentication and administration for IBM® Rational® Solutions for Enterprise Lifecycle Management tools. RDS is based on Lightweight Directory Access Protocol (LDAP version 3). The RDS allows you to define and administer user information at one place, eliminating the need for authenticating the user information multiple times for the same users.

The RDS comes with the Graphical User Interface (GUI) based client application IBM® Rational® Directory Administration (RDA). The RDA can be installed along with the RDS or separately. For information on installation instruction and procedure, refer to *IBM Rational Directory Server Installation Guide.*

The RDA allows you to perform day-to-day administrative tasks such as create user, create group, enable/disable users, perform user/group search, migrate users and groups, etc. with more ease. For more information on RDA features and usage, refer to chapter <u>RDA at a Glance</u>
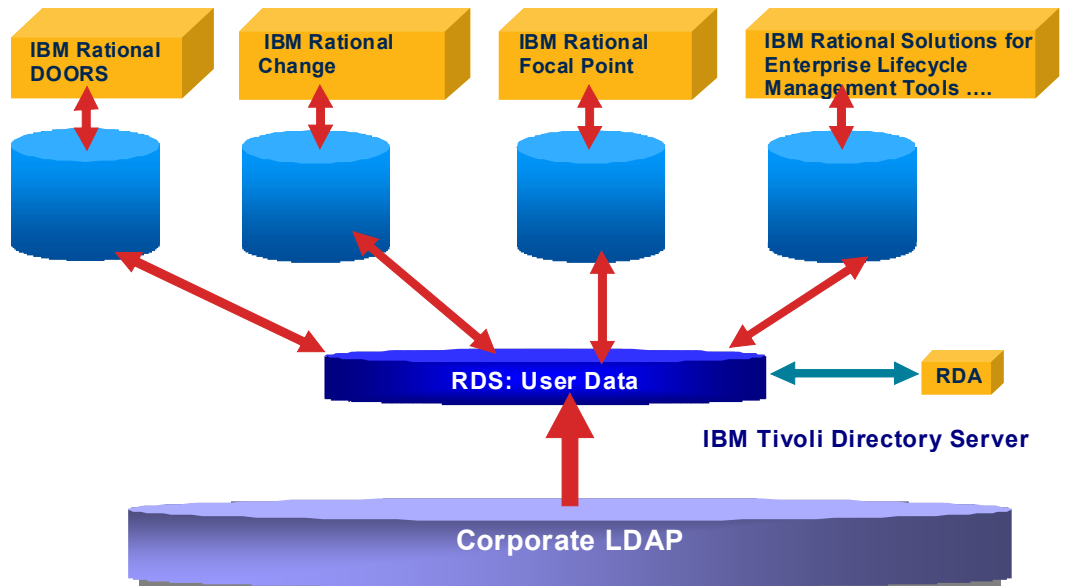
RDS schema definition

The RDS schema is based on the LDAP tree structure. The RDS uses the LDAP hierarchical structure for maintaining the user information as shown in the following diagram.
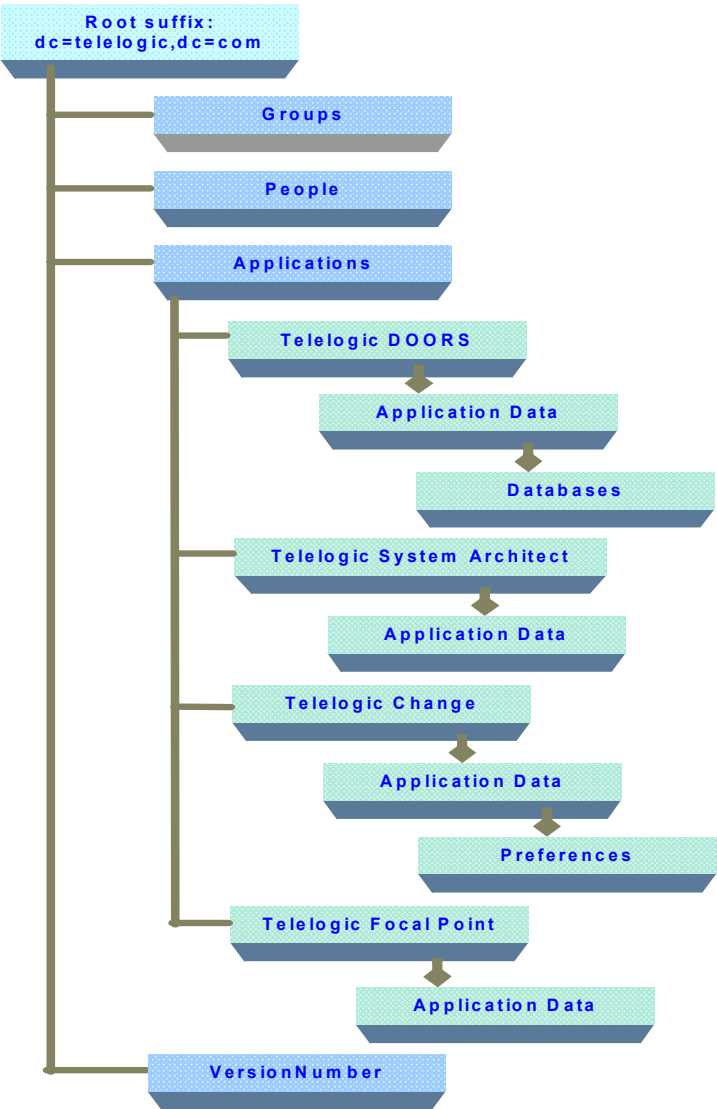
In the preceding diagram, notice that the entries are formed in a hierarchical structure. The top level of the tree is the Root suffix from which all other entries are formed.

User management

The user management deals with creating users and passwords along with assigning access to the data, etc. in a directory service. In RDS, the user entries are created under **People** organization unit (OU). These entries represents Telelogic Person objects under (RDS). The RDS contains the default admin user *tdsadmin*.

The default admin user *tdsadmin* acts as a super user and has full permission to read/write the entire schema.
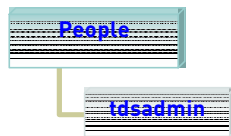
Group management

The groups allow you to set up an access rights for multiple users. You can set up an access to some data of application by assigning access rights to the group in a single operation, instead of having to assign access rights to each user, one by one.

The group acts as a reference to the various entries in the directory under one common head. The **Group** OU represents the RDS groups. This OU is defined under the root suffix which can be used to define shared groups for IBM Rational Solutions for Enterprise Lifecycle Management tools.

The following diagram shows the RDS group entries maintained in the schema**.**
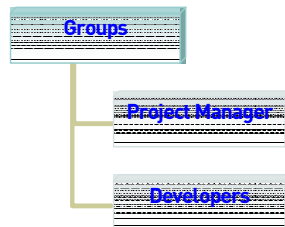
IBM Rational DOORS Group Management

The IBM® Rational® DOORS® database specific groups are maintained under each database OU as shown in the following diagram.

```
                    Applications
                         │
                    Telelogic DOORS
                         │
                    Application Data
                         │
                      Databases
                         │
           PDR (/Example DOORS Database Instance)
                         │
            Database Managers (/ Example Group)
```
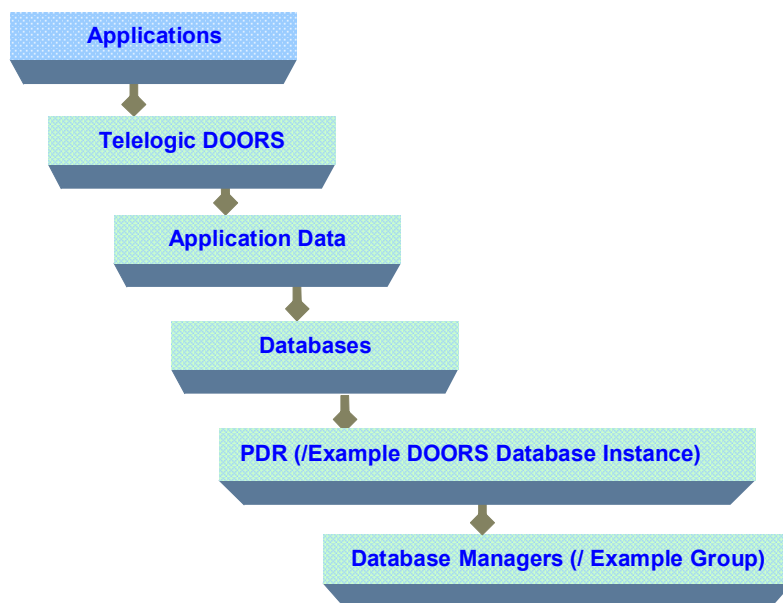
Directory Server Administration

This section describes some of the utilities used for the directory server administration on Windows, Solaris, and Linux platforms.

Administration user

The RDS also creates a *tdsadmin* user for the administrator to perform day-to-day administration functions such as creating users, groups and roles, setting the password policy for the users, adding users to groups and roles, migrating users to RDS, etc.

Note The *tdsadmin* user should be configured in the IBM Rational Solutions for Enterprise Lifecycle Management Server applications as *RDS Administrator.*

3 *Rational Directory Server Administration (RDA)*

Introduction

The RDA is a client application that allows you to perform and manage administrative tasks with much ease. The graphical interface enables the administrators to perform day-to-day tasks such as creating users, creating groups, creating roles, migrating users and groups, setting up the password policy, performing user and group search, etc. more effectively.

This chapter includes the following sections:

- Launching RDA
- Standalone mode features
- Corporate Mode Integration
- Common features across modes
- Managing licenses
- OS Authentication

RDA at a Glance

This chapter walks you through the essential features of RDA and provides a brief overview of various tasks that can be performed using the tool. RDA can be launched in following modes:

- **a.** Standalone Mode
- **b.** Corporate LDAP backbone Support Mode
- **c.** Operating Support (OS) Support Mode

Each mode provides some essential features that enable you to perform your day-to-day administration tasks easily and efficiently.

Launching RDA

This section describes how to start the RDA application. You can launch the RDA on a web browser from any machine by providing the appropriate URL.

The RDA is supported on following browsers:

- On Windows, the RDA is supported on Internet Explorer and Mozilla browsers.

- On UNIX, the RDA is supported on Mozilla browsers.

To access RDA, the **RDA web server** must be running. The RDA web server starts automatically during installation. If the web server is not started automatically, run the following command to **start** the web server.

```
<RDS_Install_Dir>\WebAccessServer\Start_RDAWebServer.bat
```

For example:

In Windows:

```
C:\Program Files\IBM\Rational\RDS_5.0\WebAccessServer\
Start_RDAWebServer.bat
```

In UNIX:

```
<RDS_Home>/RDSUtility
```

```
$ <RDS_Home>/WebAccessServer/Start_RDAWebServer.sh
```


To start the RDA, do the following:

1. Open the browser and type the following URL

   ```
   http://<hostname>:8080/webrda/rda.
   ```

   For example:

   ```
   http://rdsserver:8080/webrda/rda
   ```

Note The <hostname> refers to the name of the server where the RDS is installed.

2. The **RDS Login** dialog box appears.

3. On the **Login** dialog box, type the details as:

4. On the **Login** dialog box, type the following details.

Field name	Description
RDS URL	This specifies the LDAP URL. The URL should include a valid server name and a port number that was given at the time of RDS installation. For example: `ldap://dirserv:1636`. To open the RDS in secure mode, you can include the letter "s" in the ldap URL (where the "`s`" refers to the secure port), followed by a valid server name and a port number. For example: `ldaps://dirserv:1636`.
RDS Admin	This specifies the admin user name for RDS. The admin user *tdsadmin* is set by default by the RDS installer.
Password	This specifies the admin password set at the time of RDS installation.

5. Click **Login**.
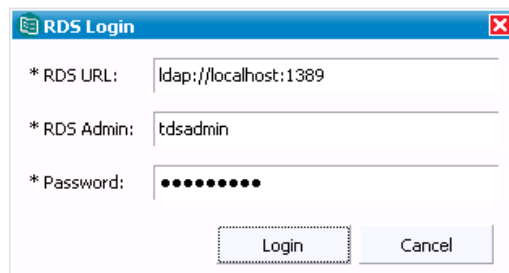
Standalone mode features

This section provide brief information on Standalone mode options that can be used for performing various administrative tasks such as managing users, groups, roles, setting up the password policy, migrating data, etc.

This section describes the following Standalone mode features.

- Managing users and groups
- Managing roles
- RDS password policy

Managing users and groups

Managing users and groups is part of the security feature of RDS. Defining users and groups allows the administrator to keep track of the people using the system and control their access to the system.

Managing users and groups in RDA involves various tasks such as creating users and groups, modifying the user and group details, searching for users and groups, enabling or disabling users, resetting the password for the users, etc.

The user-friendly options of the RDA allow you to perform all your tasks quickly and comfortably. The following example shows how users and groups are created in RDA.

To create a new user account, do the following:

1. Select the **Create User** option by doing any of the following:

    - On the **Action** menu, point to **New**, and then click **Create User**
    - Click on Create Users icon on the toolbar
    - In the console tree, right-click **Users** point to **New**, and then click **Create User**

2. On the **New User Registration** dialog box, type the user details. Refer the sample screen shot.

    Note The fields marked with the asterisk (*) are mandatory. The **User Logon Name** should be a unique name. If you enter the name that already exists, it will display an error message.

3. Click **Next.**

4. Click **Next**.

5. Type the password for the user in the **Password** box.

6. Type the same password in the **Confirm Password** box.

Note The password dialog box will not be displayed in the OS Authentication mode, as the RDS does not store passwords of the OS users.

7. Set the password option for the user by selecting any of the following options:

| Password options	Description
User must change the password at next logon	When you set this option, the user will be asked to change the password whenever the user logs in.
User can change the password	When you check this option, user can choose to change the password at the time of logon or anytime they want.

8. Click **Next**. The **Enter the Two Factor Authentication Configuration Details** dialog box is displayed.

You can enable the RDS users for the Two Factor Authentication to allow them to connect to the Radius server. This classifies the user as a secured user for the Radius server. Once this is done, whenever the user logs into the DOORS, the user will be prompted for the RDS credentials first and then the Radius server password. For more information on Two Factor Authentication see, **Configuring Two Factor security settings**.

To enable the Two Factor Authentication:

a. Click the check box against the **Enable two factor authentication** field.

This enables the **Radius User Name** field.

b. Type the user name in the **Radius User Name** box.

c. Click the check box against the **May use the password command line switch** option. This is optional.
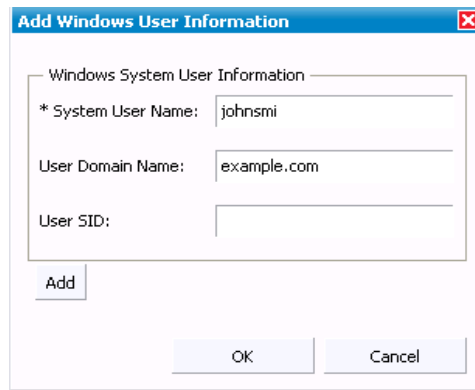
When this option is checked, user is enabled for a blank password authentication for DOORS from command line.
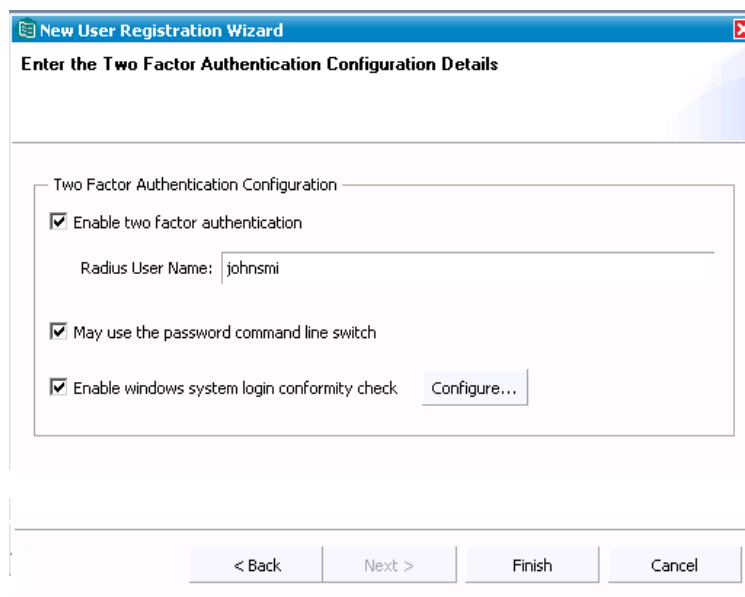
d. Click the check box against the **Enable windows system login conformity check** option and then click **Configure**.

The **Add Windows User Information** dialog box is displayed. RDS allows you to configure Windows system login authentication for users connecting to the DOORS database. When this setting is enabled, the user authentication via DOORS confirms that the user logging into DOORS is the same user as the user logged onto the Operating System.

e. In the **Add Windows User Information** dialog box, type the following.

- In the **System User Name** box, type the user name.
- In the **User Domain Name** box, type the Windows domain name.
- The **User SID** is fetched automatically when the system user name and the domain authentication is successful.

f. Click **Add**.

**g.** Click **OK.** It takes you to the previous dialog box.

Note If the user name or domain name changes, you will have to remove and add user afresh or create user with the new user name.

9. Click **Finish** to create the user. The user is created with the confirmation message.
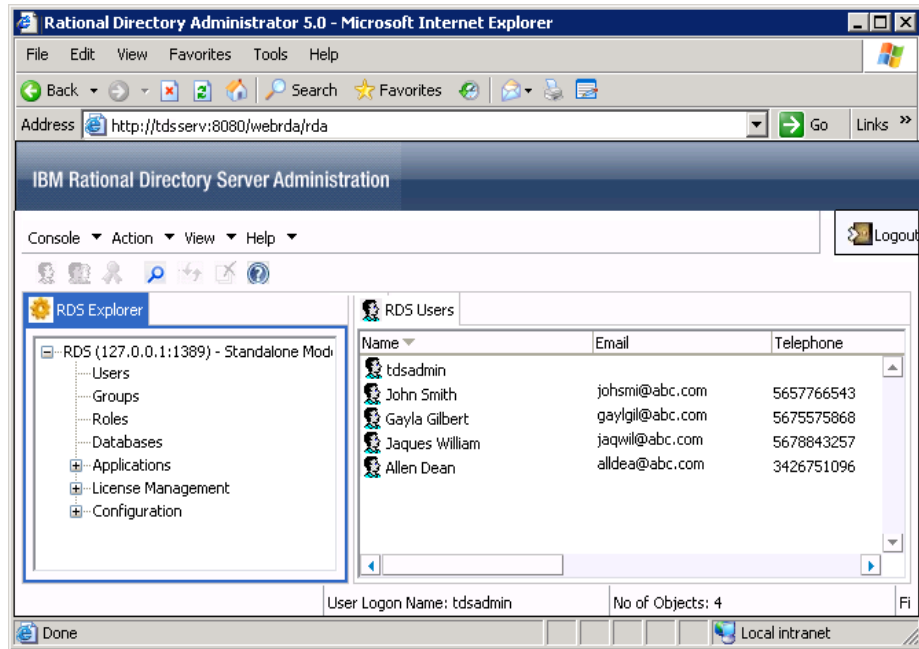
.

To create a new group, do the following:

1. Select the **Create Group** option by doing any of the following:

    -   On the **Action** menu, point to **New,** and then click **Create Groups**
    -   Click on Create Groups   icon on the toolbar
    -   In the console tree click **Groups**, right-click **RDS Groups**, point to **New** and then select **Create Group**

2. On the **Create Groups** dialog box, type the name and description for the group.
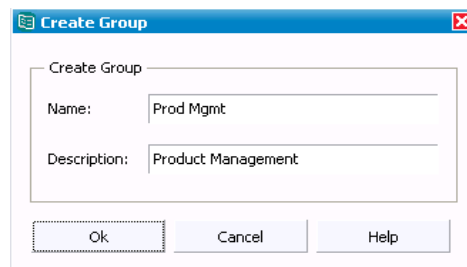
3. Click **OK.** The new group is created with the confirmation message.

Managing roles

The RDS defines the roles that can be assigned to the users. A role is an alternate to the groups, that is more efficient and easier to use. For example, the applications can identify the entries based on the defined roles instead of having to select the group and browse through the members list.

The roles are defined and administered similar to groups. Each role defines the set of privileges available to the associated users. The roles defined in RDS will have the tool specific capabilities assigned to the users.
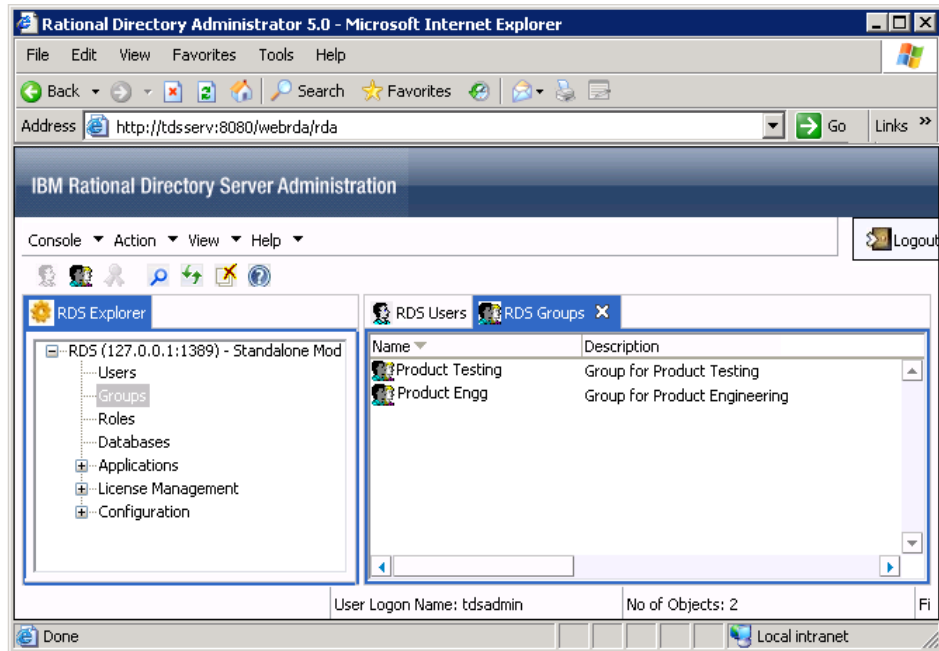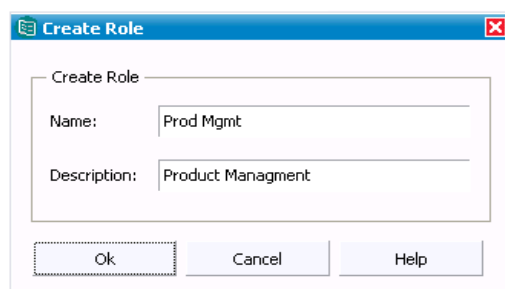
To create a role, do the following:

1. Select the **Create Role** option by doing any of the following:

    *   On the **Action** menu, point to **New**, and then click **Create Role**
    *   Click on Create Role ![icon] icon on the toolbar
    *   In the console tree click right-click **Roles**, point to **New** and then select **Create Role**

2. On the **Create Role** dialog box, type the name and description for the role.

.

3. Click **OK.** The new role is created with the confirmation message.

RDS password policy

Data security plays a vital role. To ensure maximum data security you must protect your data from an unauthorized access. This can be achieved by implementing a strong password policy which ensures that only the authorized users get access to the directory Server.

The RDS password policies helps you helps keep your data secure. This section explains the RDS password policies in detail.

The following are the password policy features that have been implemented in RDS. Each of these features are further explained in detail.

- User defined password
- Password change after first login or reset
- Password expiration
- Expiration warning
- Password syntax checking
- Password history
- Account lock out

User defined password

You can set up your password policy to either allow or not allow users to change their own passwords. The administrator can set this attribute at each individual level from RDA.

Note The *tdsadmin* user is not governed by the password policy. The *tdsadmin* password can be changed via the password change option in RDA. The password should be of atleast 8 characters in length.

Password change after first login or reset

The RDS password policy lets you decide whether users must change their passwords after the first login or after the password is reset by the administrator. The administrator can set this attribute from RDA to enable the user to change the password.

Password expiration

You can configure your password policy to expire after a given time. By default, a user password never expires. The administrator can set this attribute from RDA to enable the password to expire after a given period (for example, 30 days). This is not applicable to the *admin* user as the admin user password never expires.

Expiration warning

If you have set the password policy to expire after a given number of days, you can send users a warning before their passwords expire. This option enables IBM Rational Solutions for Enterprise Lifecycle Management tools to display a warning message to the users, specifying the number of days before the password expires.

Password history

You can set your password policy to store previously used passwords. This ensures that if a user attempts to reuse one of the old passwords the RDS has stored in history, the directory rejects the password. By default, the system remembers user's last 6 passwords.

For example, if the user changed the password for six times and if during the seventh time the user tries to use any of the last six previously entered passwords, the RDS rejects the password and user has to enter a new password.

Password syntax checking

The password syntax-checking mechanism ensures that password strings conform to the password syntax guidelines established by the password policy. By default, password syntax checking is turned off. The password policy includes following syntax.

Minimum length

The RDS allows you to specify a minimum length for user passwords. By default, the minimum password length is 6 characters.

Minimum numeric characters

You can set the password to have a minimum number of numeric characters. By default, it is set to 3 characters. For example, the user can enter the password such as "pass123".

Minimum symbolic characters

You can set the password to have a minimum number of symbolic characters such as underscores, hyphens, etc. By default, it is set to 0 characters. For example, the user can enter the password such as "pass_12".

Minimum unique characters

You can configure the password to contain minimum number of unique characters. The user password must vary the characters used in the password. For example, the user cannot have all same characters in the password such as "bbbbbb". The default is 3 characters.

Maximum character repetition

It is sometimes difficult to have all different characters in the password. You can set the password to contain a maximum number of repeated characters. The default is 3 characters. For example, the user can enter the password such as "passs1".

Account lock out

The account lockout feature protects against unauthorized users who try to access the directory server by repeatedly trying to enter a user's password. The account lockout policy works in conjunction with the password policy to provide further security. This option enables the account lockout policy.

Following are the account lockout policies implemented in RDS:

- Lockout forever
- Lockout duration
- Maximum failure attempts

Lockout forever

This attribute specifies the account will be locked out permanently until the administrator resets the user password. By default, the account will be locked out forever.

Lockout duration

This attribute specifies the length of time (in seconds) during which users will be locked out of the directory. By default, the value is set to 0. You can set the length as per your requirement.

Maximum failure attempts

This attribute specifies the number of consecutive failed login attempts after which a user will be locked out of the directory. By default, users will be locked out after a 3 failed login attempts.
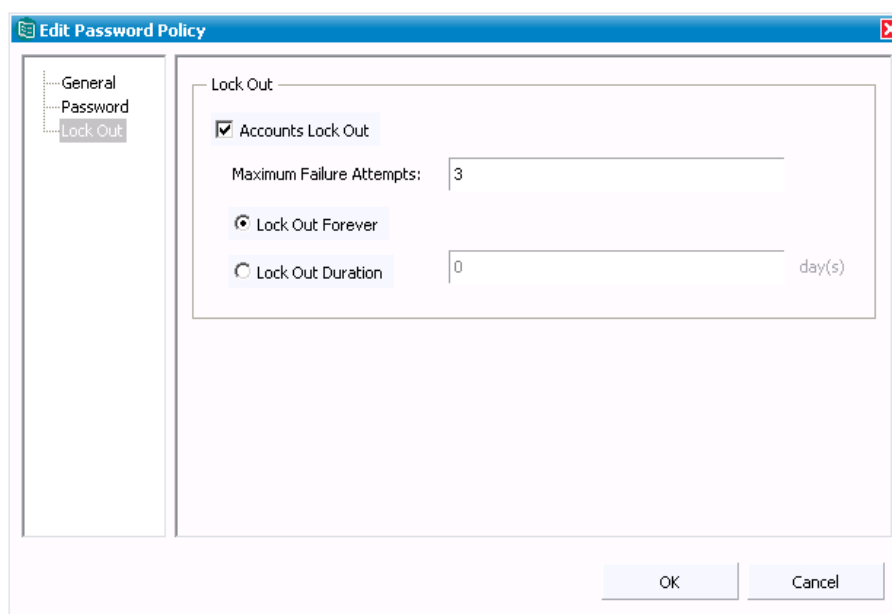
Corporate Mode Integration

The RDS corporate mode enables you to configure the RDS to integrate with the external corporate LDAP repositories. This enables your corporate backbone to serve as the user/group read-only repository for Telelogic Lifecycle Solution tools. The corporate mode enables you to access the corporate user and group information locally from the corporate partition.

About Partitions

Before you learn about the partitions, you should first understand the following:

- How do organizations maintain their data?
- When does partition come into picture??
- What is a partition?

How do organizations maintain their data?

All organizations maintain their data in a secured repository called a server. Typically, organizations store their data in a single server using a directory service.

## *When does partition come into picture?*

To enable a directory to hold large number of entries, it may be necessary to divide the directory database across multiple servers. This is when a partition comes into the picture. When you carve a single directory into manageable chunks and assign them to separate servers, you are *partitioning* the directory. The single large directory may be divided into multiple partitions. Each partition can be assigned to a separate server to handle the client load or to accommodate limits on the number of entries that can be held by a server.

What is a partition?

A directory partition is a branch or a complete sub tree of the directory information tree (DIT). A given directory tree resides in only one directory partition, and all entries within the partition must share a common ancestor knows as the *partition root*. Let us take up an example to understand it better.

The following diagram shows a directory partition based on the geographical layout with a partition root of `dc=example, dc=com`. The partitions extended by the dotted lines, extends downward from the partition root (`dc=example, dc=com`).

A directory partitioned based on geographies
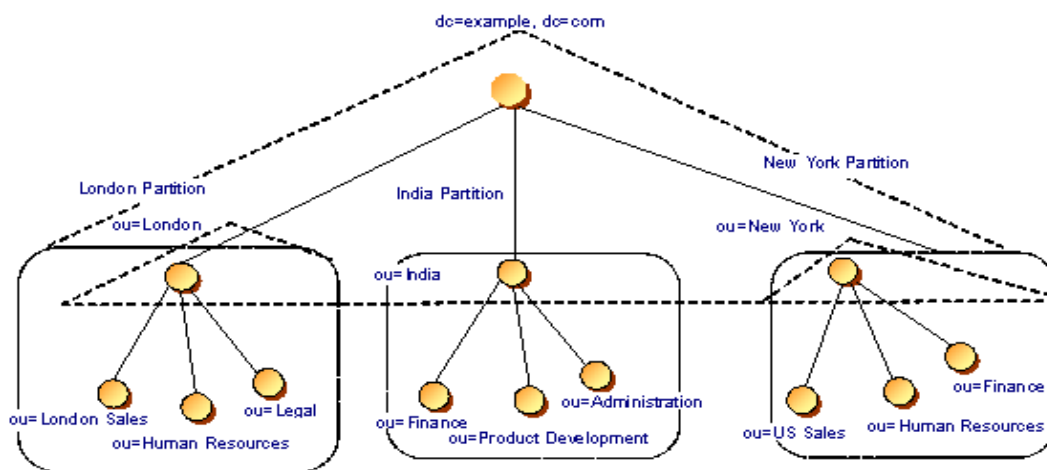
The following are the features supported by RDS corporate Mode:

- Creating partitions
- Searching for users and groups
- Deleting Partition
- Creating RDS Group

Creating partitions

By creating a partition, all corporate users are enabled as a RDS users and the authentication happens based on the corporate user identification. This makes it possible to access the corporate users and groups information locally from RDS. These users and groups are accessible to you in a read-only mode for most users for security purposes. You can create a partition using Telelogic Directory Administration tool (RDA).

You can create a Partition by doing the following:

1. On the **Action** menu, point to **New**, and then click **Create Partitions** or in the console tree click on **Configuration** and then right-click on **Corporate Partitions,** point to **New** and then click **Create Partitions.**

2. In the **Partition Creation Wizard**, type the following details.

Field name	Description
Partition Name	The name for your partition.
Partition Description	The description for the partition. You can enter a brief detail about your partition for better understanding. For example, "Partition created for the New York finance unit".
Host Name	A valid IP address of the server where the partition is created.
Port Number	A the valid port number of the server.
Enable SSL	The Secure Socket Layer (SSL) option is configured in the corporate partition.
Allow Blank Password	Can be used to authenticate a blank password when authenticating to the partition.
Configured partition is a Windows Domain Controller	Used for authenticating the connection to the Radius Server.

Note The fields marked with asterisk(*) are mandatory.

3. Click **Next.**

4. In the **Enter Corporate Admin User Details** dialog box, type the following details:

   • Under **Corporate Admin Account Information type the** admin DN and password for authenticating to the corporate server.

   The following table explains each of these options

Field name	Description	Value

Admin User DN	The Distinguished Name (DN) of the admin user. The IBM Rational Solutions for Enterprise Lifecycle Management tool uses the Admin account to lookup / search the corporate server based on the DN and the password of the admin user.
	
	The Admin user should have complete READ access to the corporate server. No write operations are performed on the corporate server.
		Example admin DN:
		`CN=John Allen,OU=Read`
		`Administrators,`
		`OU=Administrators,`
		`OU=Users, OU=New York,`
		`DC=example, DC=com.`

Admin User Password	This specifies the password for the admin user.	Enter the admin password in this field.
Admin User Confirm password	This specifies password authentication for the admin user.	Re-enter the password in the Confirm Password field. Both the passwords should match for the installation to continue.

- Under **Configure Primary Search Base**, type the primary search base for retrieving the user details from the corporate servers.

  The following table explains the option in detail:

Primary search base	Description	Example

Primary Search Base	The root search base for all RDS Lookup operations. Users / Groups referenced in RDS are located in this root node. The primary search base holds the bulk of the user population. The RDS authentication attempts to authenticate the user constructing the (DN) using the primary search base.	You provide the search base as:
		`dc=example, dc=com`
		This example search base specifies the root suffix of the corporation. The search based could be narrowed based on geography, physical distribution of the directory data etc.
		Example:
		`ou=NewYork,dc=example,dc=com`

5. Under **Corporate User Logon Attribute**, select the attribute from the list to logon to RDS.

   The following table explains the attributes:

Attribute name	Description	Example
CN	This specifies the common name (first name, last name of the user). You can select this attribute to set CN as the logon name for logging on to RDS.	You can enter the user id as **John Smith** to login into RDS from the IBM Rational Solutions for Enterprise Lifecycle Management tools.
UID	This specifies the unique identifier name for the user. You can select this attribute to set uid as the logon name for logging on to RDS.	You can enter the user id as **bjenson** to login on to RDS from the IBM Rational Solutions for Enterprise Lifecycle Management tool.

SN	This specifies the surname of the user. You can select this attribute to set surname as the logon name for logging on to RDS.	You can enter the user id as **Smith** to login into RDS from the IBM Rational Solutions for Enterprise Lifecycle Management tool
sAMAccountName	This specifies the NT login name for the user. You can select this attribute to set NT login as the logon name for logging on to RDS.	You can enter the user id as **johnsmith** to login on to RDS from the IBM Rational Solutions for Enterprise Lifecycle Management tool

6. Click **Finish** in the **Partition Creation Wizard.**

7. Click **OK** in the message box, then view information about the partition you just created.
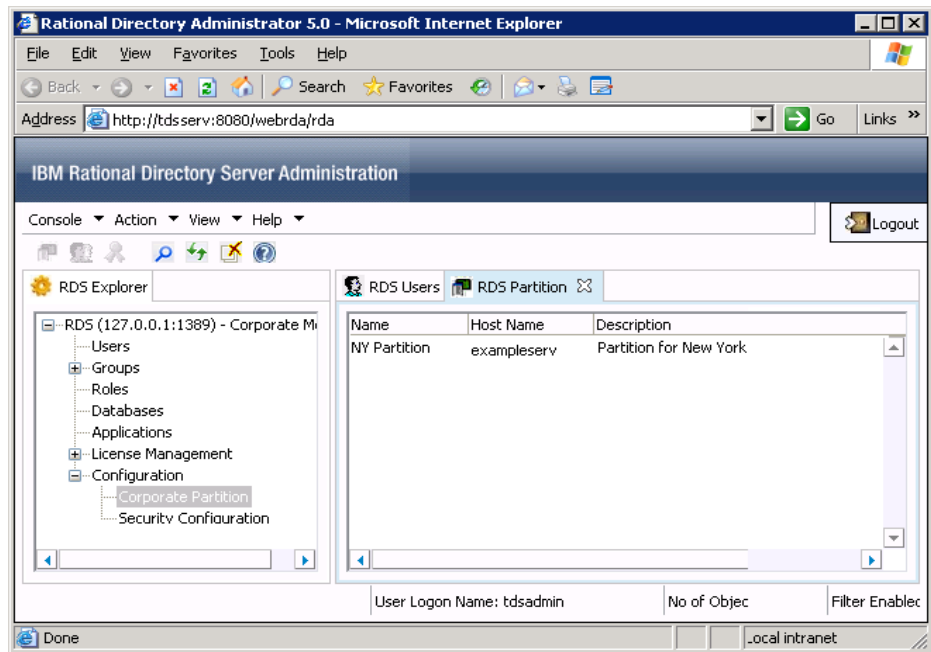
Deleting Partition

You can delete the Partitions you created in RDA using the **Delete** option. To delete the partition, right-click the Partition and select **Delete**, in the confirmation message box click **Yes**.

Creating RDS Group

The RDS groups are the existing local groups in RDS. These groups are displayed in the RDS Groups node. In corporate mode, RDS additionally provides you the option to create a local group and add corporate users and groups to the newly created group. Adding the corporate users to this group enables the access privileges as defined by the IBM Rational Solutions for Enterprise Lifecycle Management tools.

The group allows you to set up an access rights for multiple users. You can set up an access to a group in a single operation, instead of assigning access rights to each user, one by one.

To create a new group, do the following:

1. Select the **Create Group** option by doing any of the following:

   - On the **Action** menu, point to **New**, and then click **Create Groups**
   - Click on Create Groups [icon] icon on the toolbar
   - In the console tree click **Groups**, right-click **RDS Groups**, point to **New** and then select **Create Group**

2. On the **Create Groups** dialog box, type the name and description for the group

.
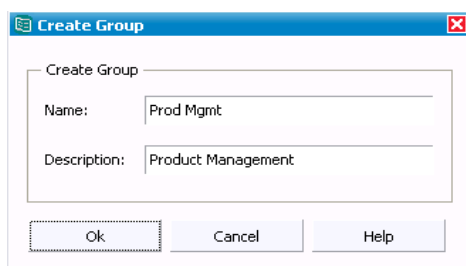
3. Click **OK.** The new group is created with the confirmation message.
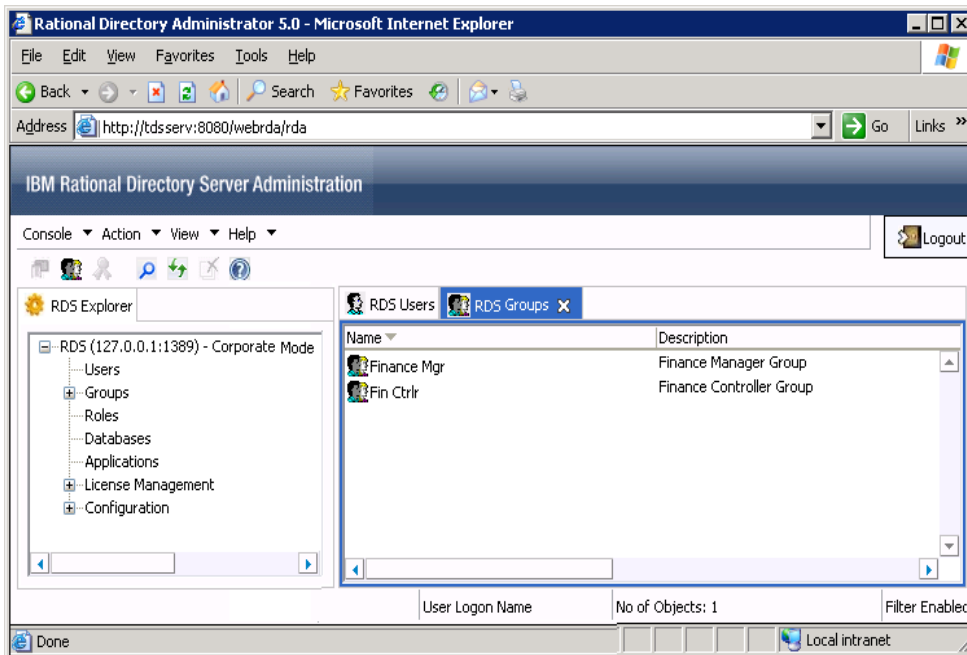
Common features across modes

This section details the features that are common in all the modes. This section includes the following features.

- Searching for users and groups
- Using the filter operation
- Applications
- Data Migration
- DOORS Migration
- Two Factor Authentication (T-FA)

Searching for users and groups

You can search for the specific user and group accounts residing under RDS using the **Find** option. In corporate mode, the users and groups residing under the corporate partition are displayed.

There are two ways of searching for a user or group account in RDA. You can either search users using a normal **Find** option or by creating your own custom query using **Custom Find** option.

To search using normal **Find**, do the following:

1. On the **Action** menu, click **Find.** You can also right-click **Users** in the console tree and click **Find** or click ![icon] icon.

2. In the **Find Users and Groups** dialog box, the option **Users** is selected by default.

3. Click **Find.** All the existing user details are displayed.

4. You can also perform your search using any of the following search criteria:
   - Search based on the user name or description starting with a particular letter
   - Wild card search

5. To search for the specific user or group, type the search value in the **Name** and **Description** box.

6. Click **Find** or press **Enter**. The user list as per the given search criteria is displayed in the **Find Results** box.
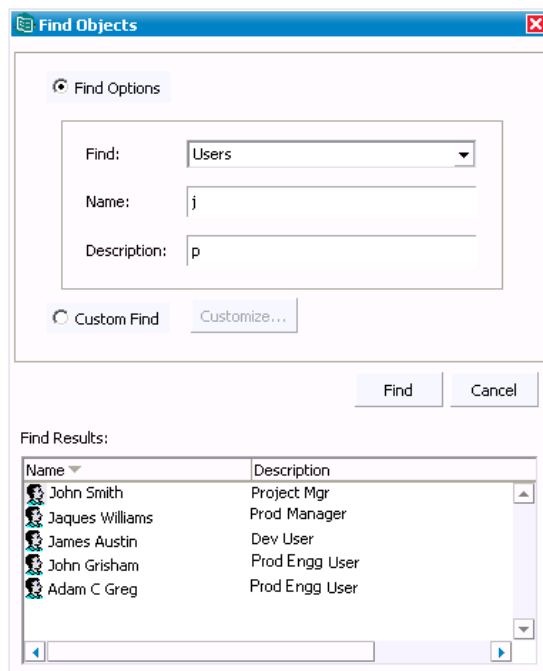
To search using **Custom Find**, do the following:

1. In the **Find Users and Groups** dialog box, select **Custom Find**

2. In the **Customize Find** dialog box, click **Field**, point to **Users**, and then select any of the options from the list.

3. Click the **Condition** list. You are provided with the various options to further refine your search criteria. Select any of the search criteria from the list. For more information on the options, refer to <u>page 61.</u>

4. In the **Value** box, enter the search value. Notice that **Add** option is activated.

5. Click **Add** or press **Enter**. The search criteria will be added in the **Condition List** box.

6. Click **Find**. The list of users as per the given search criteria is displayed in the **Find Results** box.
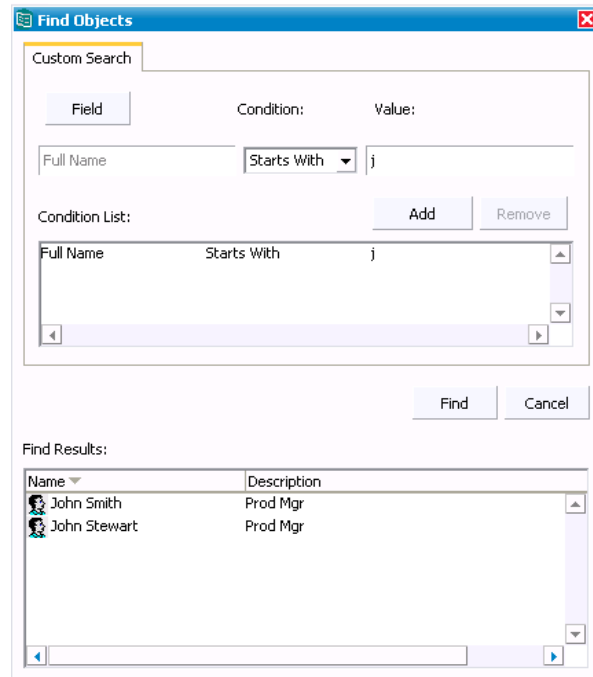
Using the filter operation

When you want to perform certain activities to only specific user accounts or groups, it is difficult to scroll through the complete list. The **Filter** option allows you to list only those users and group that you want to view. When you apply a filter, only the objects you specify in the filter are displayed in the filtered list.

The default filtering option displays all types of objects (that is, no filter is applied). However, it is possible to select only certain types of objects to be displayed, such as specific users or groups, by customizing the kind of information that is displayed within each object type.

When you customize a filter, you can select the fields and specify a filter condition and value to display specific user and group accounts. The following screen shots shows the sample user and group filter.

To filter all users and groups, do the following:

1. On the **View** menu, click **Filter Option**.

2. On the **Filter Option** dialog box, notice that the **Show all types of Objects** option is selected by default.

3. In the **Maximum number of objects to be displayed** box, enter '0' to see all users and groups or enter the maximum number of users and groups to be displayed. By default, it displays 200 objects.

.
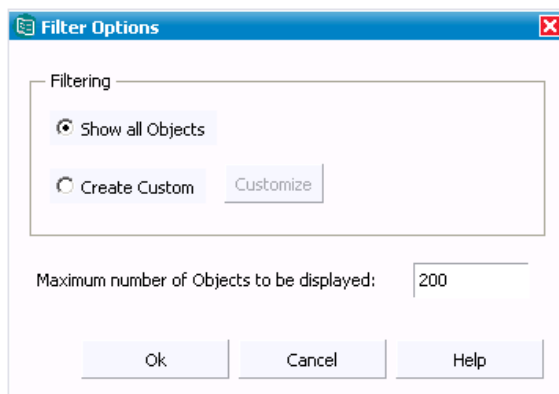
4. Click **OK**. The message will be displayed for number of users and groups retrieved. Click **OK** in the message box. The retrieved users and groups are displayed in the RDA Users and Groups tab.

Customize a filter option:

To filter users and groups based on the given criteria, do the following:

1. On the **Filter Option** dialog box, click **Create Custom** and then click **Customize**.

2. On the **Find Objects** dialog box, click **Field**, point to **Users** or **Groups**. You are provided with the following list for users and groups based on which you can create your search criteria.

    *   Full name
    *   Last name
    *   Logon name
    *   Email address
    *   Phone number
    *   Fax Number

   You can customize the group search based on the following options:

    *   Group Name
    *   Group Description

3. Click on **Users** or **Groups** and select any of the search criteria mentioned in the previous step. For example, in the sample screen shot the filter is done based on User's full name.

4. Click the **Condition** list. You are provided with the various options to further refine your search criteria. The following table explains the options:

Option name	Description	Example
Starts With	The name starting with the specific letter. You can use this option with Full Name, Last Name, and User Logon Name.	Type **A** in the **Value** box. The user names starting with this letter will be retrieved.
Ends With	The name ending with the specific letter. You can use this option with Full Name, Last Name, and User Logon Name.	Type **N** in the **Value** box. The user names ending with this letter will be retrieved.
Is (Exactly)	The exact name of the user. Your entry must be an exact match for this option to work.	Type the user name **John Smith** in the **Value** box to see the details of this user.
Is Not	The user name which you want to exclude in the list. Your entry must be an exact match for this option to work.	Type **Allen Dean** in the **Value** box; all the users except for this user will be retrieved.
Present	The user name containing this specific letter.	Enter **J** in the **Value** box; all the entries which contain the letter **J** will be retrieved.
Not Present	The user name which does not containing this specific letter.	Enter **S** in the **Value** box; the user name which does not contain the letter **S** will be retrieved.

5. In the **Value** box, enter the search value based on the condition you have selected. For example, in the sample screen shot, the search criteria selected is the **User Logon Name**, the Condition selected as **Starts With** and the Value entered is **j**.

6. Click **Add** or press **Enter**. The search criteria will be added in the **Condition List** box.

7. Click **OK**. It will take you back to the **Filter Option** dialog box.

8. Click **OK** again in the **Filter Option** dialog box. The list of users or groups as per the given search criteria appears in the **Users** and **Groups** tab.

.
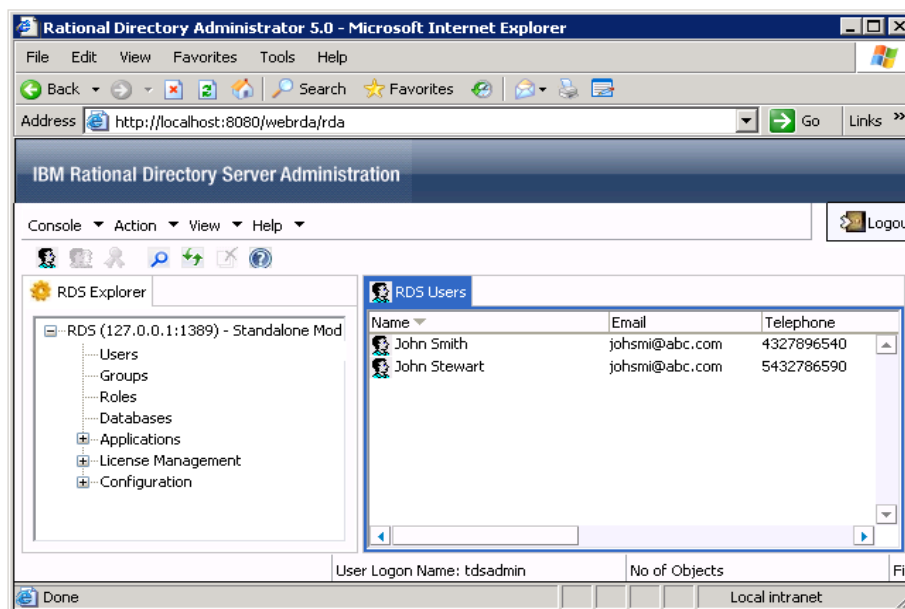
Applications

All IBM Rational Solutions for Enterprise Lifecycle Management applications registered with RDS are displayed under the **Applications** node. This allows the administrator to assign application specific roles to the users from RDA.

Managing licenses

The RDS provides you the option to assign user-based license features to users to access the IBM Rational Solutions for Enterprise Lifecycle Management tools.

The license access information is maintained in the license options file. The license option file holds the information such as the user name, features assigned to users, etc. Whenever the user is assigned a license for a particular feature of a application, this information is recorded in the license options file.

The IBM® Rational® License Server TL is configured to point to the license options file to enable the access to the users.

In standalone mode, the users must have their **NT logon name** or **UNIX logon name** configured in RDS to assign a license feature.

In corporate mode, the attribute CORPORATE_LICENSING_FEATURE_LOGON_ATTRIBUTE is configured in *RDSConfiguration.xml* file. By default, the value for this attribute is set to **samAccountName** for Active Directory Server corporate partition. For other corporate partitions such as the IBM Tivoli Directory Server, the administrator must configure this value to a valid system login name (for example, uid).

To assign license feature to users do the following:

1. On the console tree click the **License Management** and then click **License Configuration**.

2. In the **General** tab, enter the following details.

Field names	Values
License Option File	
Specify the License Options file path	Type the path for the license options file where you want the license options file to be created. For example, `c:\license.opt.`
License CVD Information	
Host Name/IP Address	Type the host name or IP address of the license server.
Port Number	Type the port number of the license server.

Note The CVD refers to Common Vendor Daemon.

3. Click **Configure**.

   The available license features are listed under **License CVD Feature Entries** area. The features that are already checked are the user-based license features. The administrator can select any other user-based licenses.

4. To select more features:

   • Select the feature and then click the **User-Based** check box.
   • Click **Save**.
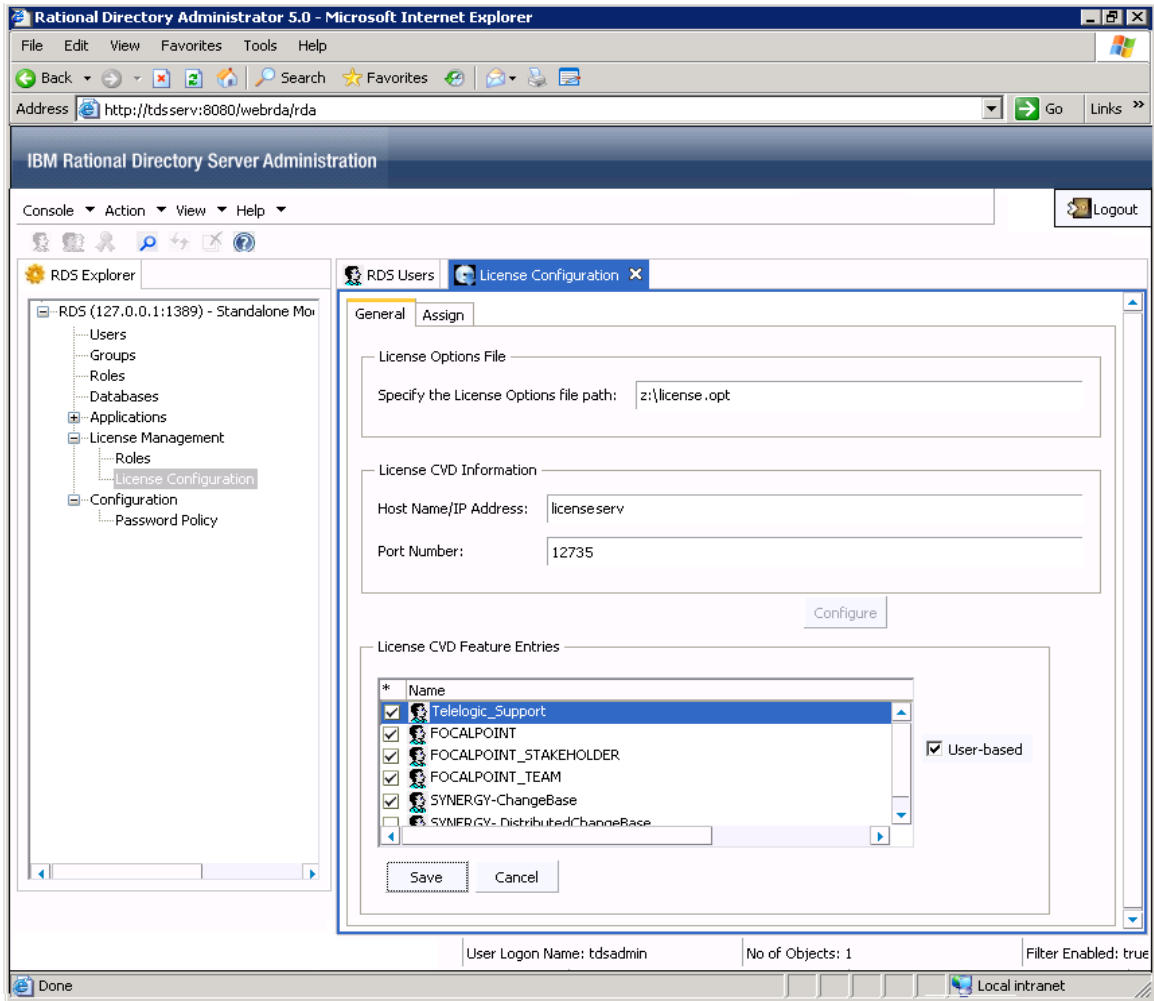
5. To assign the license feature to user, click **Assign** tab.

   The license features that you selected in the previous step are listed in this tab.

6. In the **Select the license feature** list, click the feature you want to assign.

7. Click **Add**.

   The **Find Users** dialog box is displayed. RDS provides you the facility to extract the user accounts to which you want to assign a license feature. You can retrieve the user accounts using the **Find** or the **Custom Find** options.

8. To find the users using **Find**:

   - In the **Find Users** dialog box, By default the **Users** is selected. Click **Find**.
   - All the existing users are displayed in the **Find Results** box.
   - You can also type a starting letter of user's Full Name, User Logon Name, Last Name, Description or the exact name in the **Name** and **Description** box.
   - Click **Find**.
   - The user list as per the given search criteria is displayed in the **Find Results** box.
   - Select the user and click **Assign**.

9. To find the users using **Custom Find**:

   - On **Find Users** dialog box, click **Field**, point to **Users**, and then select any of the option from the list.
   - Select the query criteria from the **Condition** drop down list.
   - In the **Value** box, enter the search value.
   - Click **Add** or press ENTER.
   - The search criteria will be added in the **Condition List** box.
   - Click **Find**.
   - The list of users as per the given search criteria will be displayed in the **Find Results** box.

10. Select the user account and click **Assign**.

    The selected user account is listed under the **License Options File Entries** list box.

11. Click the **Include** check box and then click **Submit**.
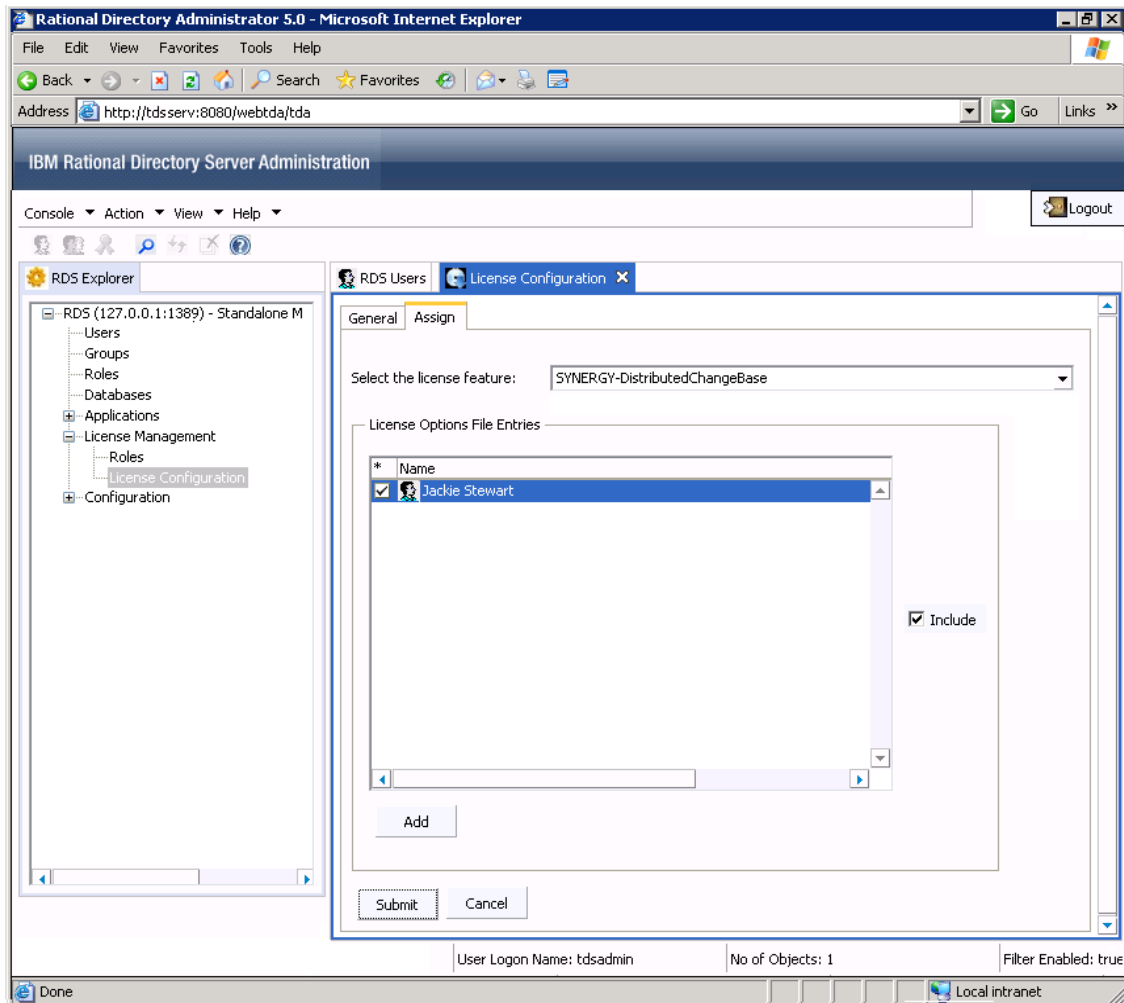
The user is assigned the selected license feature. The user, whenever logs on to the particular IBM Rational Solutions for Enterprise Lifecycle Management tool, will be able to access the assigned license features for that tool. For example, the user *Jackie Stewart* has been assigned the *Focal Point* license feature. Whenever this user log on to the *Focal Point* application, he will have the access to the features of this tool.

Two Factor Authentication (T-FA)

The Two-factor authentication (T-FA) is a security process wherein the user provides two means of identification to authenticate to the server. This feature is supported only by DOORS product to connect to the Radius Server.

You can configure the Rational Directory Server (RDS) to enable Two-factor authentication (T-FA) to integrate with the Radius Server.

Configure Two-Factor Authentication

You need to first setup a Two-Factor Authentication settings to establish the connection to the Radius server.

To configure the security settings:

1. In the console tree, click **Configuration** and then click the **Security Configuration**.

2. In the **Two Factor Authentication Configuration** tab, type the following details.

Field name	Description	Example Values
Hostname/IP Address	Hostname or IP address of the Radius server.	ExampleServer
Port Number	Port number of the Radius server. Default port is 1812.	1234
Shared Key	Security key that is given at the time of a Radius Server installation.	ExampleRadius
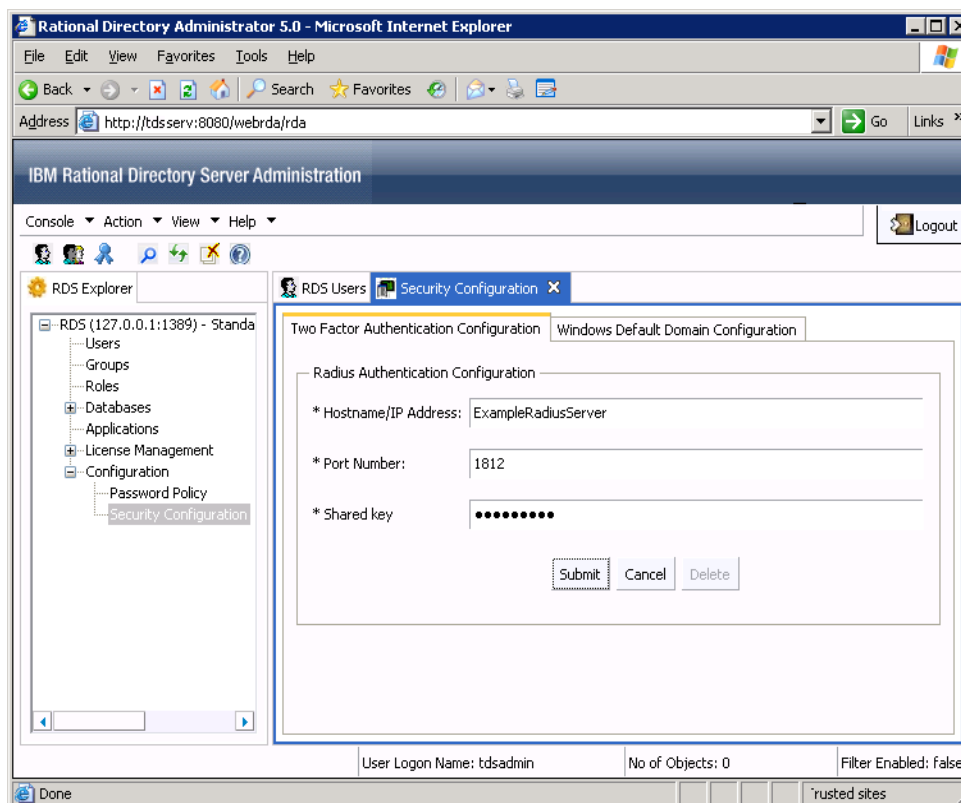
You can also configure the default Windows System Domain for the Radius server. This is optional.

3. To configure the default Windows System Domain:

    a. Click **Windows Default Domain Configuration** tab.

b. Type the Domain name in the **Default Domain Name** box.
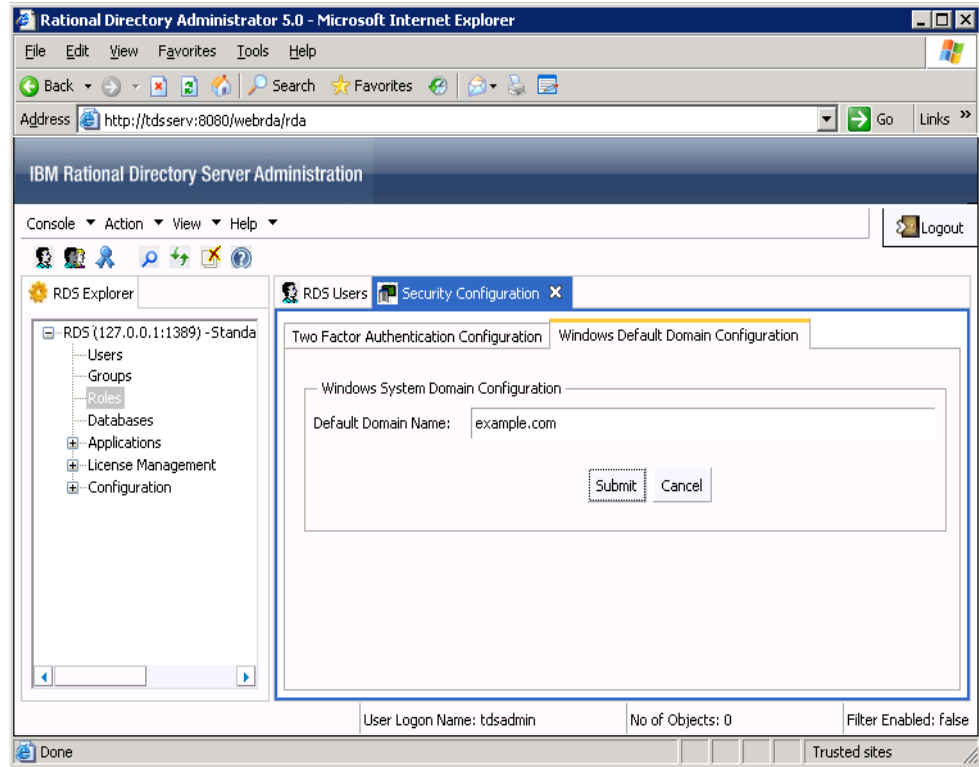
4. Submit.

Note Once you have configured the security settings, you can enable the Two Factor Authentication for the RDS users to connect to the Radius server. For detailed information on enabling the users for T-FA see, Managing users and groups.

Enable Two Factor Authentication for DOORS Database

You can enable the Two-Factor Authentication for the DOORS databases that reside under RDS. In this case, the user and the corresponding DOORS database to which the user has access to, have to be enabled as Two Factor Authentication.

Once you classify the user and the corresponding DOORS database as T-FA enabled, whenever the user logs into the DOORS database, the user will be prompted for RDS credentials followed by the Radius server password.

Note The communication between RDS and the Radius server happens through T-FA, and not directly from DOORS.

To enable the DOORS database for T-FA:

1. In the console tree, expand the **Databases** node, and then click the DOORS database.

   The Database Configuration tab appears in the right pane.

2. In the **Database Configuration** tab, do the following:

   a. Click the check box against the **Enable two factor authentication** field.

   b. Click the check box against the **Enable radius authentication** field.

   c. In the **Authentication prompt** box, type the message. For example, "Enter the password for Radius Server."

   The message you type in the box, appears when the user logs into the DOORS database; prompting the user to enter the Radius server password for Two factor authentication.

   d. Click the check box against the **Enable system login conformity check** field, to enable system login authentication.

   The **Add Windows User Information** dialog box is displayed. You can configure Windows system login authentication for users connecting to the DOORS database.

   When this setting is enabled, the user authentication via DOORS confirms that the user logging into DOORS is the same user as the user logged into the Operating System.

   e. In the **Add Windows User Information** dialog box, type the following.

   • In the **System User Name** box, type the user name.

- In the **User Domain Name** box, type the Windows domain name.
- The **User SID** is fetched automatically when the system user name and the domain authentication is successful.
- Click **Add**.
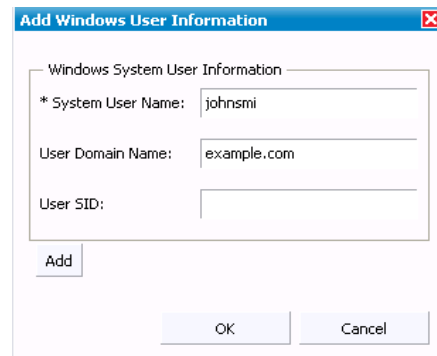
f. Click **OK.** It takes you to the previous dialog box.

g. Click **Disable the password command line switch by default** check box.

This disables the blank password authentication from the command line for DOORS.

h. Click **Submit**.
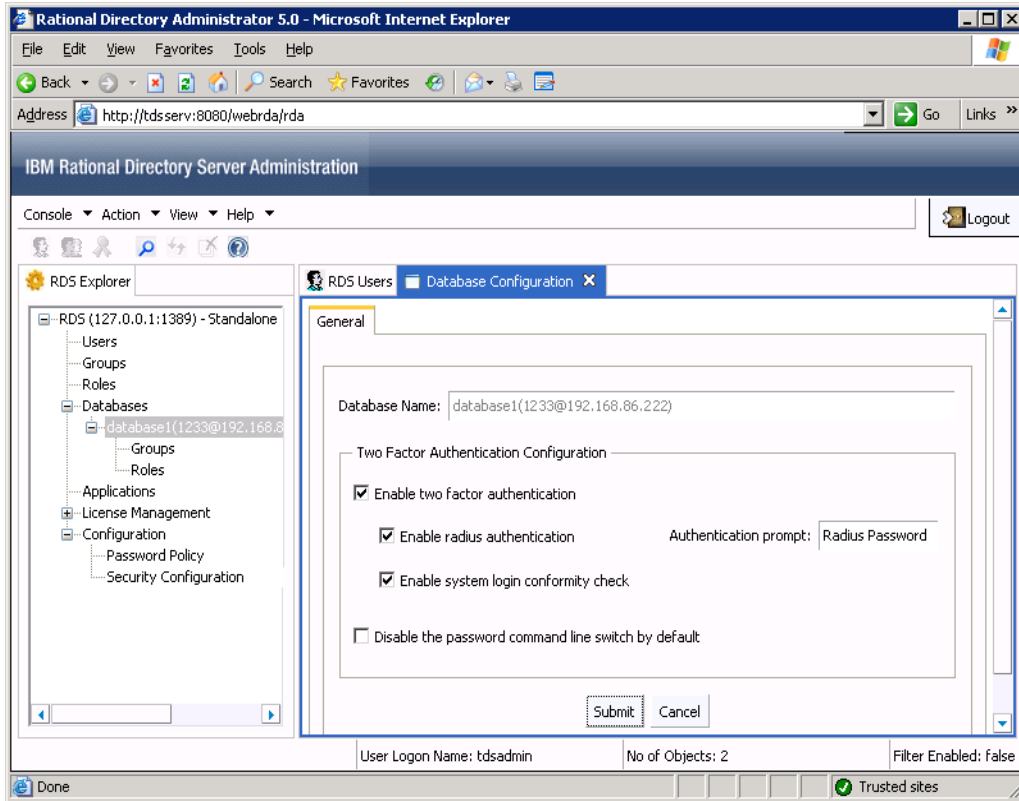
Modify Two Factor Authentication settings for users

You can view and modify the T-FA settings enabled for a specific user.

To modify the T-FA settings for users:

1. In the Console tree, click **Users**.

   All existing users are displayed in the right pane.

2. Right-click the user and then click **Properties**.

3. In the **Properties** dialog box, click the **Security Settings** tab.

   The Two-Factor Authentication settings for the user is displayed.

4. In the **Two Factor Configuration Authentication** area, you can modify the following settings:

   a. Click the check box against the **Enable two factor authentication** option to enable or disable the settings.

   b. Modify the existing user name.

   You can click in the **Radius User Name** box and type the user name.

    c. Click the check box against the **May use the password command line switch** option to enable or disable the password from command line.
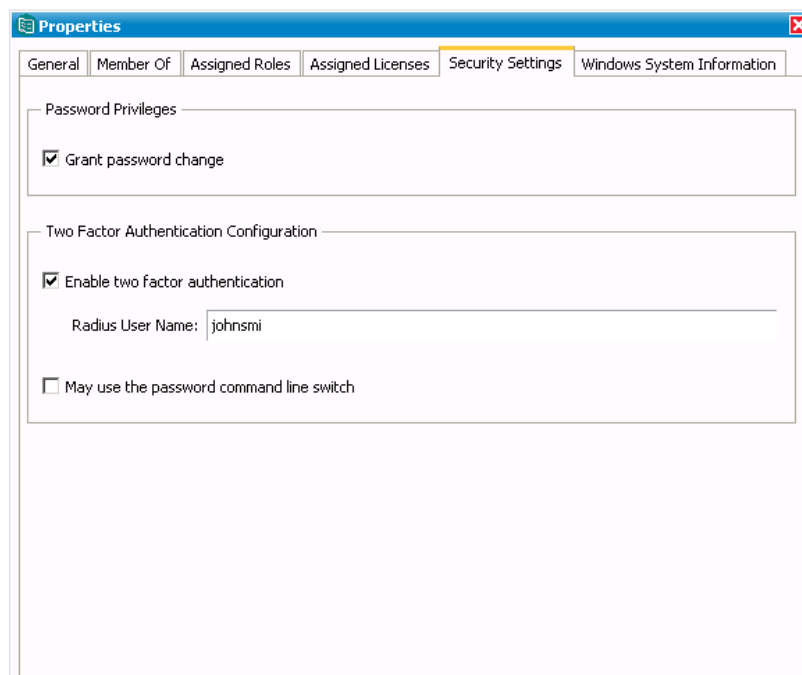
  5. To modify the Windows system information:

    a. In the **Properties** dialog box, click the **Windows System Information** tab.

       The System User Name and User Domain name are displayed.

    b. Select the user name and then Click **Edit**.

    c. In the **Add Windows System User Information** dialog box, modify the following:

      • Type new user name in the **System User Name** box.
      • Type the domain name in the **User Domain name** box.
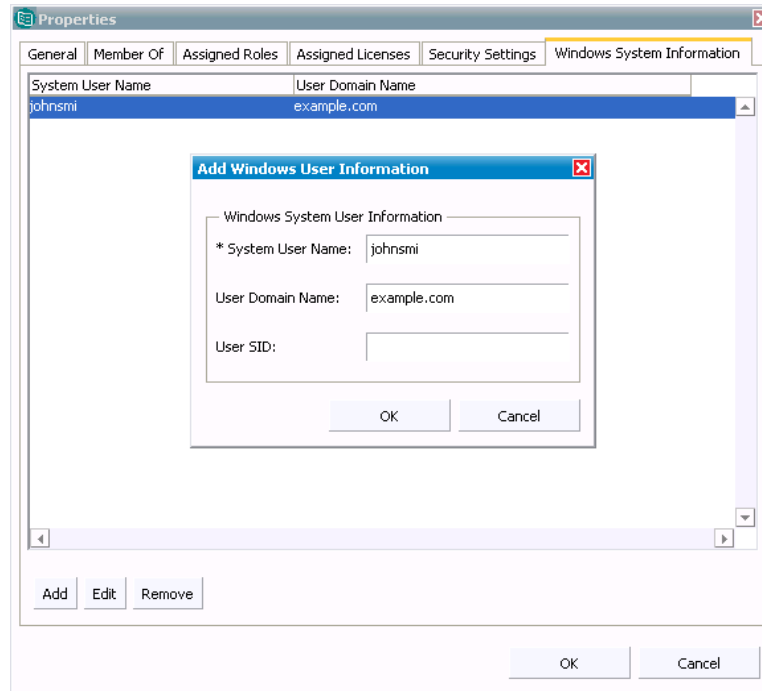
- Click **OK**.

6. To add the Windows System User Information for a specific user:

   - In the **Windows System User Information** tab, click **Add**.
   - Type new user name in the **System User Name** box.
   - Type the domain name in the **User Domain name** box.
   - Click **OK**.

7. To remove the Windows System User Information for a specific user:

   - In the **Windows System User Information** tab, select the System user name and click **Remove**.

OS Authentication

The Operating System Authentication mode enables you to configure the RDS to allow user authentication against the OS or Windows configured domain logon name and password. The users are authenticated against the OS hosting the RDS and the user names are mapped to the OS logon name. Once the user authentication is successful, the users are provided access to the IBM Rational Solutions for Enterprise Lifecycle Management tools.

Even though the users gain access to IBM Rational Solutions for Enterprise Lifecycle Management tools using their OS login, the IBM Rational Solutions for Enterprise Lifecycle Management tools still have the facility to authorize these users. In other words, RDS enables authorities of authorization to IBM Rational Solutions for Enterprise Lifecycle Management tools. This feature makes it possible for users to access resources over the network without having to repeatedly supply their credentials.

For example, the user **John Smith** has the OS logon name as "johnsmith". In order to access the IBM Rational Solutions for Enterprise Lifecycle Management tools with his OS logon name, he can logon to RDS as johnsmith. The RDS will then authenticate the user name against the OS logon name and if successful, the user *johnsmith* will have access to the IBM Rational Solutions for Enterprise Lifecycle Management tools based on the authorization granted.

This mode allows you to perform the activities similar to the Stand-Alone mode i.e., you can create users, perform search operations, add other relevant details for the existing users, etc. Refer to online help for more details on each of these options.

The users created in this mode should be the OS users. This will enable RDA / IBM Rational Solutions for Enterprise Lifecycle Management tools to display the user list facilitating appropriate tool specific privilege grant.

Note RDS supports specific settings for IBM® Rational® System Architect® and IBM® Rational® Synergy tools. Refer to *IBM Rational Directory Server Administration Guide* for more details. User creation in OS Mode does not take in the user password as RDS does not store passwords of OS users.

4 *Data Migration*

Data migration is the process of transferring data from one repository to another. The repositories usually have different formats and constraints. The migration needs to be performed in a specific format to maintain data integrity.

Generally, the steps for migrating the data involve:

1. Extracting the data from the source repository

2. Transforming the data into a format that the target repository accepts

3. Validating the data values against the target to avoid duplication of data

4. Loading the data into target repository

RDS Migration

The RDS supports the migration of user and group data from

- Existing TLS repositories into RDS

- Existing RDS repository into the current repository

The following diagram shows the data migration sequence followed for migration.
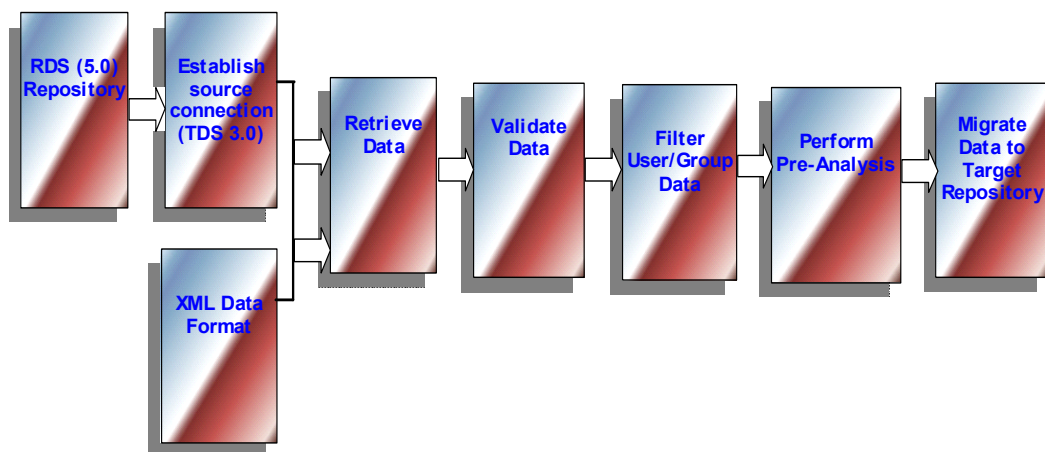
RDS migration allows two kinds of data migration:

- Migration of data from previous TDS repository (such as TDS 3.0, 4.2, 4.3) to current repository.

- Migration of data using XML data file format.

Directory server migration

This option allows you to transfer all user and group data from previous RDS repositories (such as TDS 3.0, 4.2, 4.3, and 5.0) to the RDS 5.0 repository. The data migration will not modify the existing user and group information or enhance or lower user preferences. In other words, the data will be migrated to the target repository without making any changes to the user information.

The data migration from one RDS repository to another is made easier with its in-built Pre-Analysis tool and filter features. These features not only make the data migration faster but also allow you to migrate quality data. This saves you time on manual analysis. We will learn about these features in detail later.

RDS migration provides following types of data migration:

Migration type	Definition
User Migration	The users from a source repository are migrated to the target repository.
Group Migration	The groups from a source repository are migrated to the target repository.
User Migration from a specific group	The users from a specific group are migrated from a source repository to the target repository. You can also create a temporary group in the source repository with the set of users you want to migrate to the target repository.
DOORS Migration Support	The DOORS-specific users/groups information is migrated from the XML data file to the target repository.

Note The migration steps for all four options specified above are same.

Let us take the example of a User migration.

To migrate users using Directory Server option, do the following:

1. On the **Console** menu, click **Migration**.
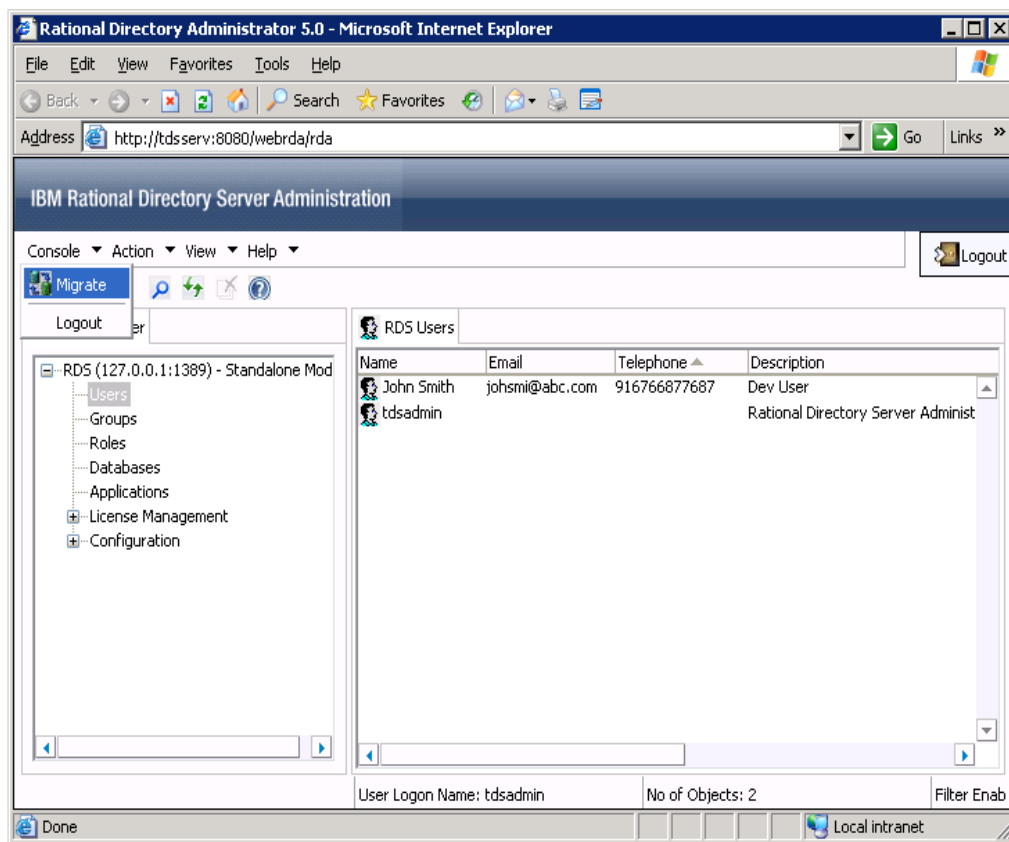
2. On the **Migration** Wizard, enter the following details:

Field name	Description
Select the migration Source	Select the migration source as **Directory Server** from the list.
Server Name/ IP Address	Enter a valid server name or IP address of the source repository (for example, IP address of TDS 3.0, 4.2, 4.3 or RDS 5.0 repository).

Field name	Description
Port Number	Enter a valid port number. The port number should contain only the numbers.
Admin DN	The admin Distinguished Name (DN) attribute name is used in User Authentication operations. Enter a valid admin DN.
Password	The password given at the time of RDS installation. Enter a password for the admin user.

Note To migrate the data from TDS 4.2, 4.3, and RDS 5.0 to the current repository (RDS 5.0), the Admin DN should be given as:

`uid=tdsadmin,ou=people,dc-=telelogic,dc=com.`

3. Click **Next**. On the **Select the migration type** dialog box, select **User migration**.

4. Click **Next.** The **Select the Filter Options** dialog box is displayed with the following options

Options	Description
Apply Filter	This option allows you to filter the records that you want to migrate by specifying the search criteria.
Specify the number of records	This option allows you to move data in chunks. If you are migrating the data for the first time, It is recommended that you move data in parts. Based on your migration experience you can choose to move data in bulk. This option is selected by default with minimum number of records as 100.
All Records	This option allows you to move all records in one shot. You can select this option to migrate all records in one go.

5. Choose any of the above mentioned options. Lets take the example of **Apply Filter** option.

> **Filter Option:** The filter feature allows you to list only those users and groups that you want to migrate. You can select certain types of objects, such as specific users or groups by specifying a filter condition and a value.

6. Select **Apply Filter** and click **Filter Options**. The **Find Objects** dialog box is displayed.

7. On the **Find Users** dialog box, click **Field,** point to **Users.** You are provided with the following options based on which you can customize your search criteria.

- Full name
- Last name
- User logon name
- Email address
- Telephone number
- Fax number
- Synergy user name
- System user name
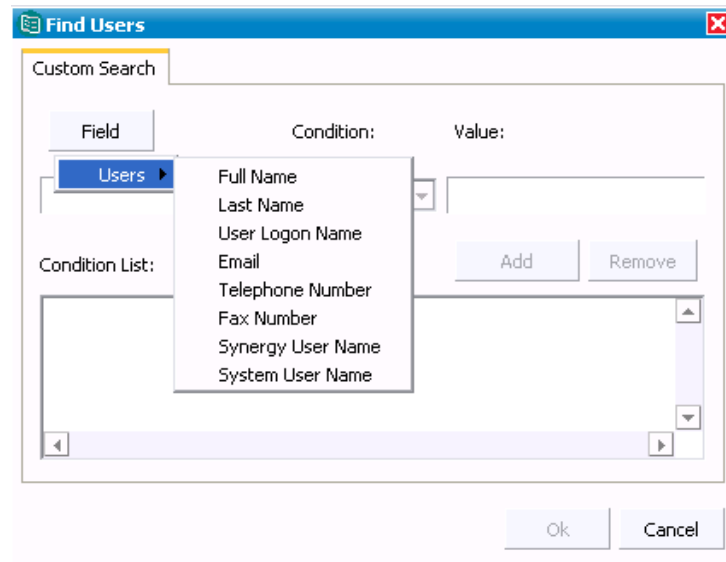
8. Select any of the search criteria mentioned in the previous step. For example, in the sample screen shot, the filter is based on the Full Name.
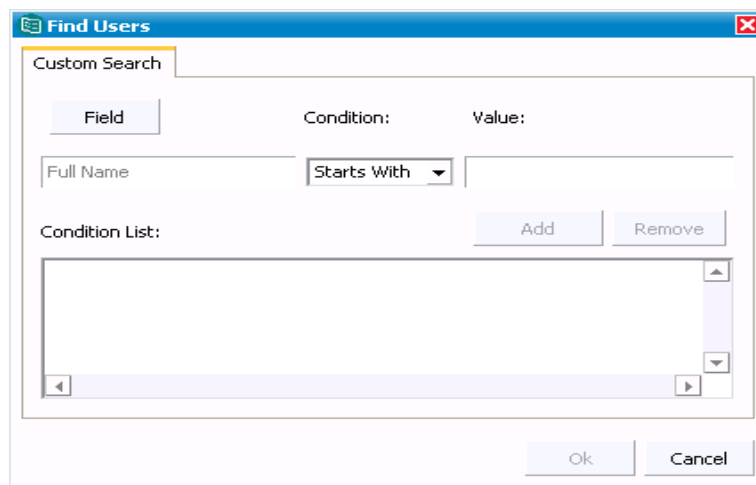
9. Click the **Condition** list. You are provided with the various options to further refine your search criteria.
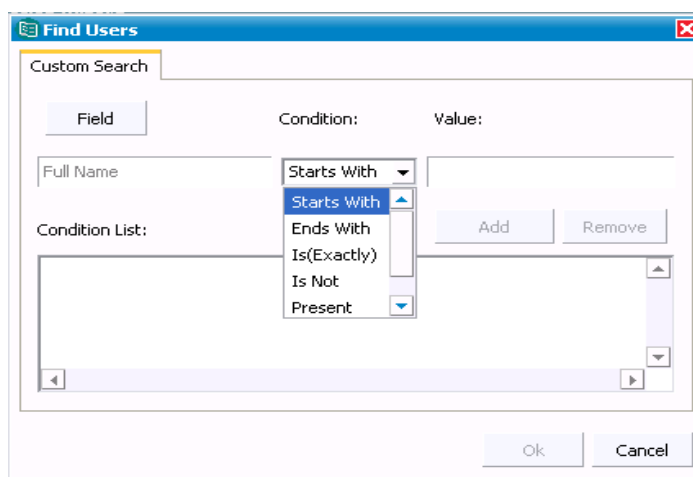
The following table explains each option:

Option name	Description	Example
Starts With	The name starting with the specific letter. You can use this option with Full Name, Last Name, and User Logon Name.	Type **A** in the **Value** box. The user names starting with this letter will be retrieved.
Ends With	The name ending with the specific letter. You can use this option with Full Name, Last Name, and User Logon Name.	Type **N** in the **Value** box. The user names ending with this letter will be retrieved.
Is (Exactly)	The exact name of the user. Your entry must be an exact match for this option to work.	Type the user name **John Smith** in the **Value** box to see the details of this user.
Is Not	The user name which you want to exclude in the list. Your entry must be an exact match for this option to work.	Type **Allen Dean** in the **Value** box; all the users except for this user will be retrieved.
Present	The user name containing this specific letter.	Enter **J** in the **Value** box; all the entries which contain the letter **J** will be retrieved.
Not Present	The user name which does not containing this specific letter.	Enter **S** in the **Value** box; the user name which does not contain the letter **S** will be retrieved.

10. Select any of the specified search conditions.

11. In the **Value** box, enter the search value based on the condition you have selected.

    For example, in the sample screen shot, the search criteria selected is the **Full Name**, the Condition selected as **Starts With** and the **Value** entered is **a**. Refer the preceding table for the details on other options.

12. Click **Add** or press **ENTER**. The search criteria will be added in the **Condition** box.
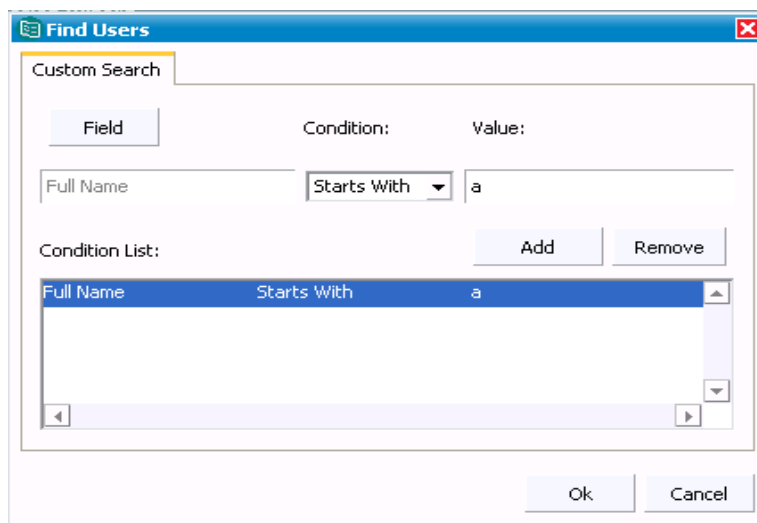
Note To remove the search condition from the list, select the search condition that you want to remove, and then click **Remove.**

13. Click **OK.** It will take you back to the **Migration Wizard** dialog box.

14. Click **Finish**. The Migration analysis process is started by the in-built Pre-Analysis tool mentioned.

Pre-Analysis tool: This tool analyses each record against the target repository and provides you with three types of lists such as **Definitive records, Conflicting records, Duplicate records** in Standalone mode.

RDS additionally displays the **Unmapped records** in the corporate mode. The Unmapped records are specific to the DOORS migration. Refer to "DOORS Migration" on page 71 for more information.

Definitive Records: The records that have no discrepancies with the target repository fall under this category. You can directly migrate these records to the new repository.

15. All records are selected by default. Click **Migrate** to move these records into the target repository.
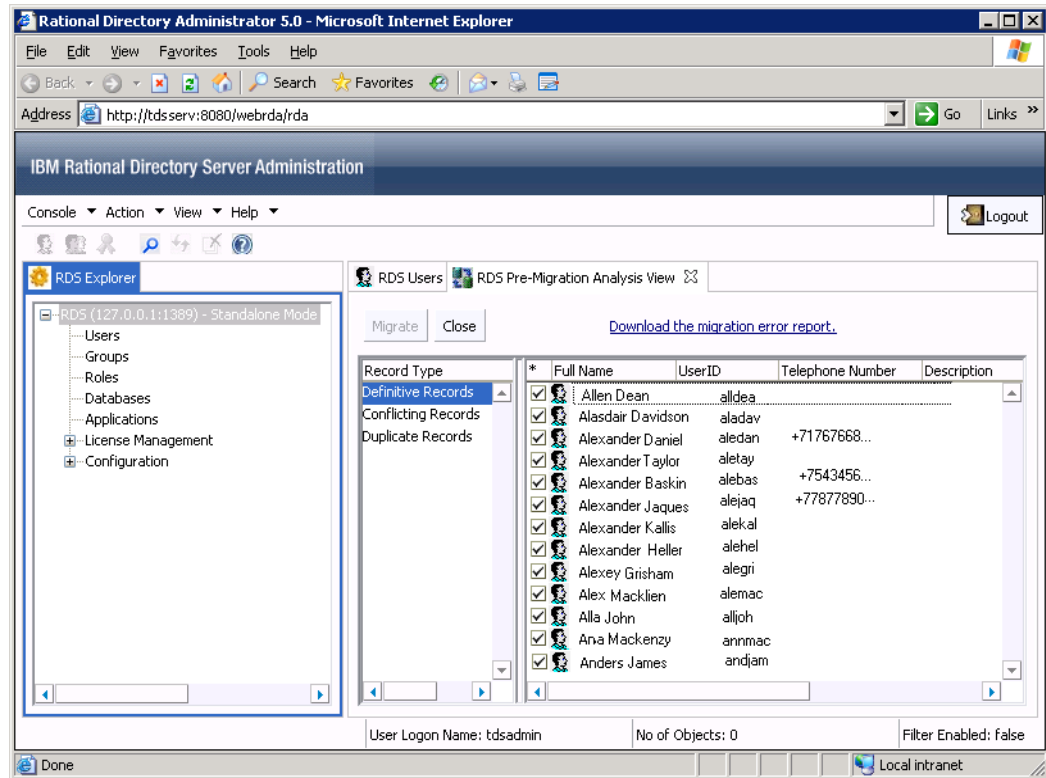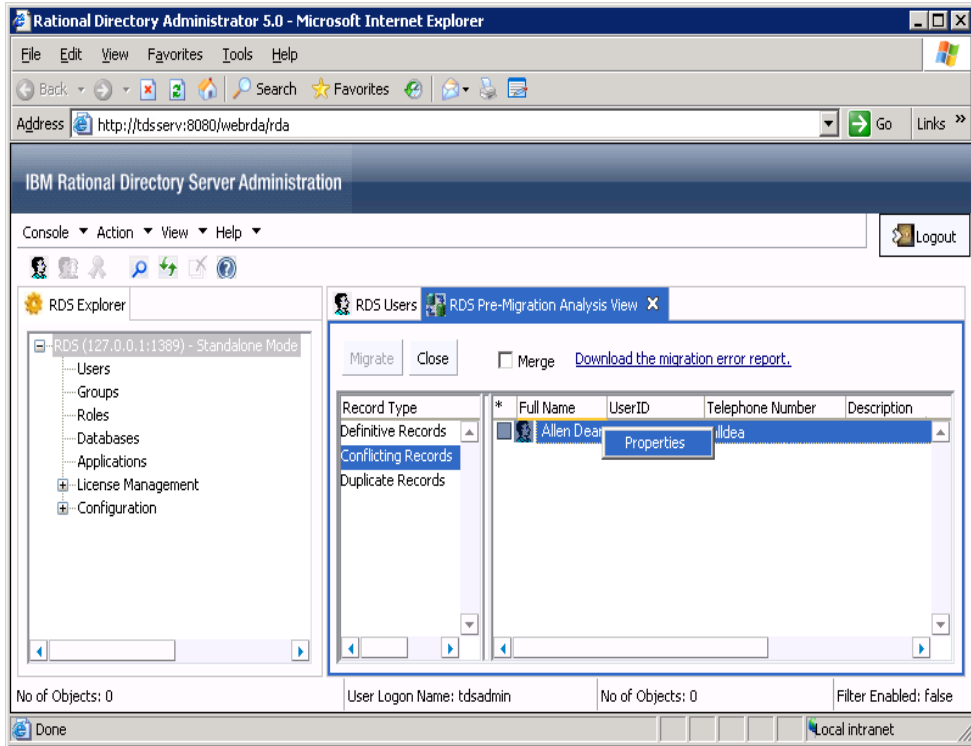

Note If there are any failed records, the details of that is recorded in the error log file. Click **Download the migration error report** option to see the error log.

16. Click Refresh ⚡ icon to see the migrated users in the **RDS Users** tab.

17. Click **Conflicting Records.** The conflicting user records are displayed in the right pane.

Conflicting Records: The records that have one or more fields having the same details as of the record in the target repository are listed in this category. You can view the conflicting information using the **Properties** option.
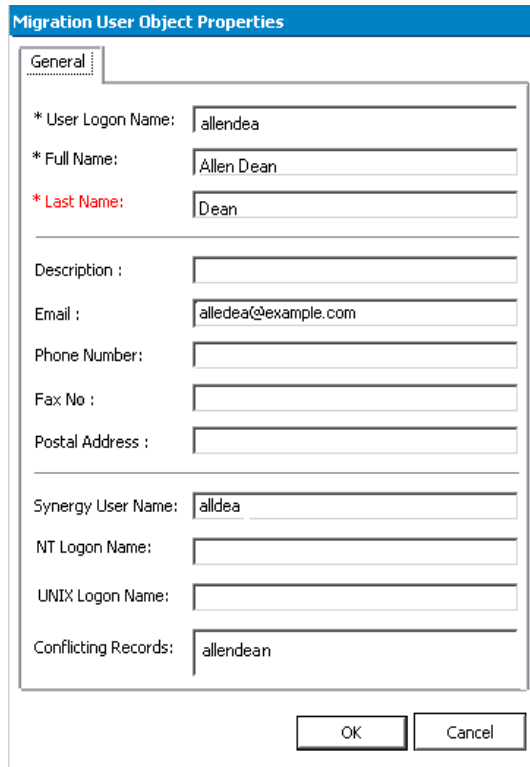
18. Double-click or right-click the user record and click **Properties.**

19. The **Migration User Object Properties** dialog box is displayed. Notice the following details:

The **Last Name** field is shown in red. This means that the user record matching this last name exist in the target repository with some other user name.

The **Conflicting Records** field displays the user id (allendean) of the record creating the conflict.
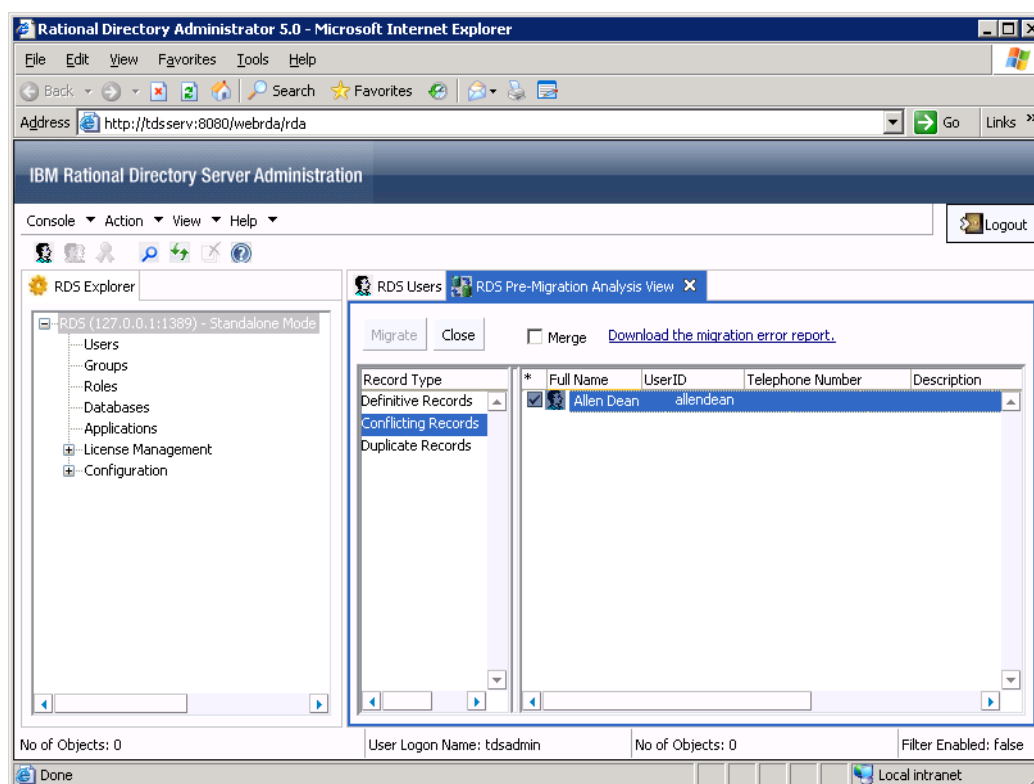
20. Click **OK** to return to the **Conflicting Records** pane.

21. To migrate the record as it is, select the record by clicking the check box provided against the record, click **Migrate**.

22. Click **Duplicate Records.** The duplicate user records are displayed in the right pane.

Duplicate Records: The records which already exist in the target repository are listed under this category. In other words, the listed records hold the same user id as in the target repository.
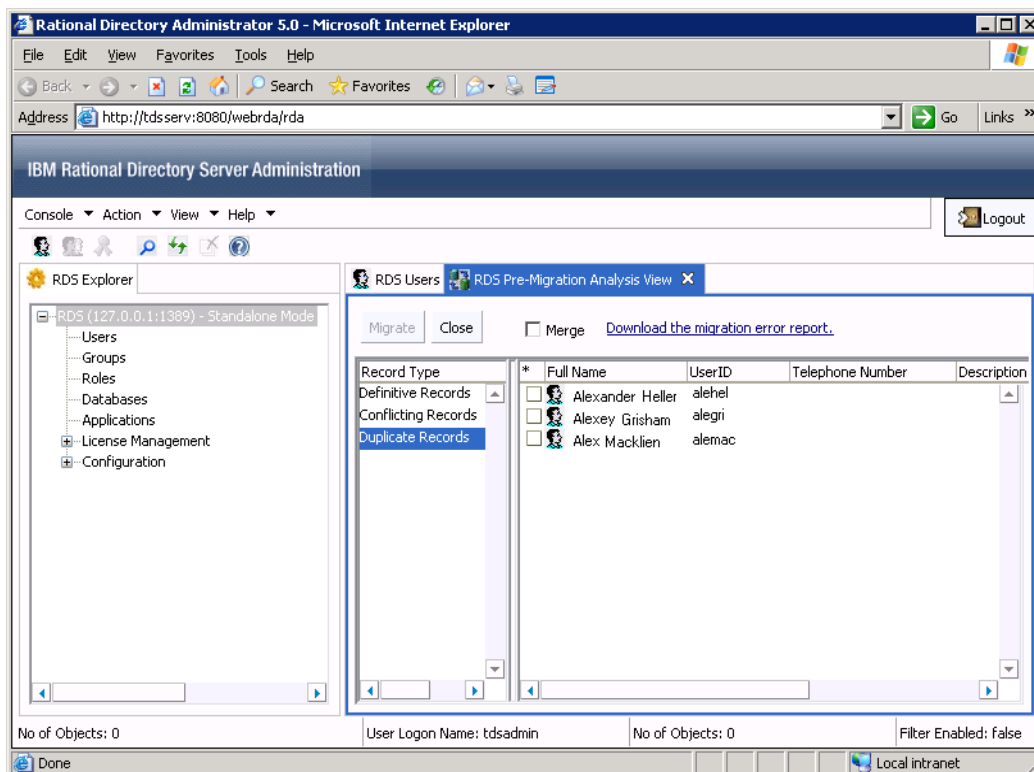
23. Double-click or right-click the user record and click **Properties** to view the details. You cannot migrate these records as it already exist in the target repository with the same user id.

24. After migration, restart the RDS server.

Note Follow step 1 to step 24 for **Group Migration** and **User Migration from specific group** options.

Migration using XML data file

This option allows you to migrate users and groups data from IBM Rational Solutions for Enterprise Lifecycle Management tools into RDS using the XML data file.

The XML file format to be used for migration is defined in the **XML schema definition (XSD).** The XSD file defines the user and group attributes to be used for creating the XML file. For more information on RDS XML schema definition format refer to Appendix A,"User schema definition format" on page 99.

The XML data provided by the IBM Rational Solutions for Enterprise Lifecycle Management tools should be used for migration. The XML file containing the user and group data should align to the XML schema definition (XSD). Refer to Appendix C, "Example : RDS user migration XML format" on page 108 and Appendix D, "Example : RDS group migration XML format" on page 110 for the sample XML file.

Note The group migration process is similar to the user migration. For group migration, create the XML file based on the group schema definition given in the section Appendix B, "Group schema definition format" on page 103. The DOORS groups will be migrated based on the Database Name as defined in the migration XSD file.

To migrate users using XML data file, do the following:

1. On the **Console** menu, click **Migration**.

2. On the **Migration Source Selection** dialog box, click **User Migration** or **Group Migration**. By default, the **User Migration** option is selected.

3. Click **Next**.

4. Click **Browse** and select the XML file you want to migrate.

5. Click **Upload** to upload the XML file to the server.

6. Click **Finish**.

   The Migration analysis process is started by the in-built Pre-Analysis tool. Rest of the steps are similar to the Directory Server User Migration explained earlier in this manual. Follow the step 15 to step 24 to complete the migration.

.

Note If any of the records fail during the migration process, the error will be logged in the error log file. The migration process will continue with the next record. Click **Down the migration error report** option to see the error log.

5 *DOORS Migration*

RDS supports the DOORS data migration through various configurations. The DOORS user and group data can be migrated into RDS using the XML data file. The XML file format to be used for migration is defined in the **XML schema definition (XSD).** The XSD file defines the user and group attributes to be used for creating the XML file.

The DOORS database instances are migrated to RDS based on the database name as defined in the migration XSD file. The group migration migrates the groups as the database groups and the user migration associates the users to the defined database.

DOORS Data Migration with RDS in Standalone mode

The following migration configurations are supported by RDS.

| RDS mode	DOORS configuration	Migration synopsis
Stand-Alone mode	DOORS using local database	• All Users/Groups information are stored in the local DOORS database server. These information can be migrated to RDS using the XML data file.
		• The migrated users retain the database access privileges/roles.
		• The logon user name and password remain the same for the migrated users.

RDS mode	DOORS configuration	Migration synopsis
Stand-Alone mode	DOORS using corporate database	• The Users/Groups information are stored in the corporate LDAP used by DOORS. • The DOORS generated XML data file must be used for data migration. • The DOORS specific access privileges are preserved for the migrated users. • The DOORS groups are migrated as local database groups within RDA.
Stand-Alone mode	DOORS using TDS 3.0, 4.2, 4.3 and RDS 5.0.	• Online migration to move users and groups can be performed from TDS 3.0, 4.2, 4.3 and RDS 5.0 repository. • DOORS generated XML data files can then be migrated for user specific database access privileges. • The groups are migrated as local database groups.

The following section explains the migration procedure for following configurations.

- DOORS using local database
- DOORS using corporate database

To migrate DOORS database, do the following:

1. On the **Console** menu, click **Migrate**.
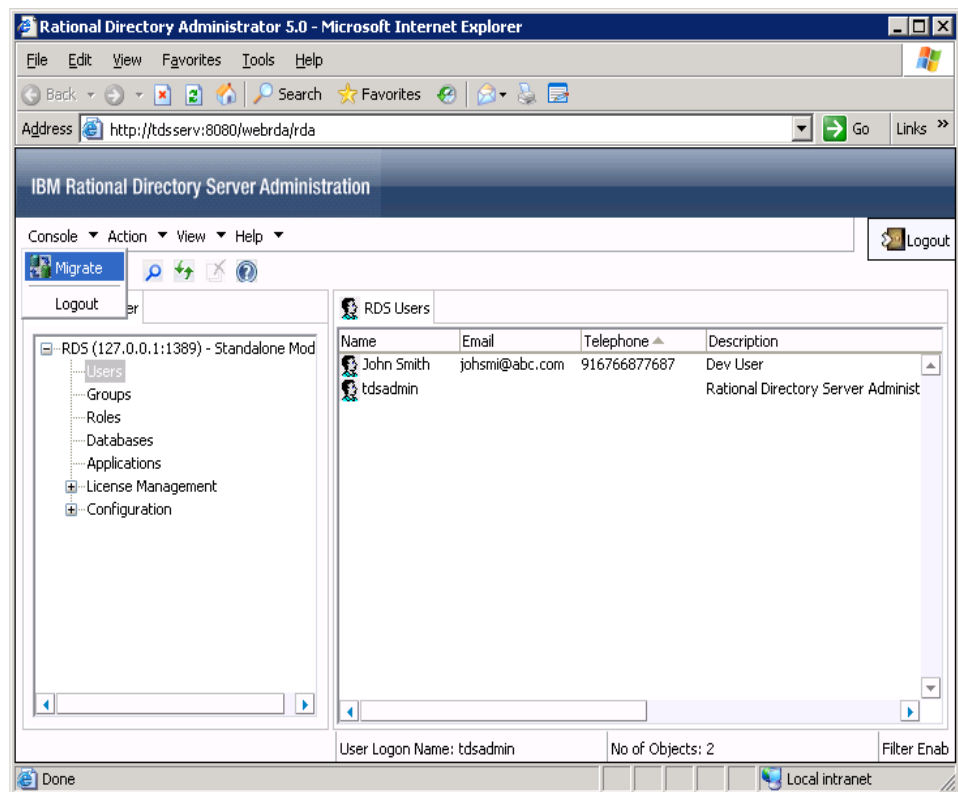
2. On the **Migration Source Selection** dialog box, select **User Migration** or **Group Migration** option to begin the migration. By default, the **User Migration** option is selected.

3. Click **Browse** and select the XML file to migrate. The XML file can contain user/group information from the DOORS Local Database or the corporate LDAP repository.

4. Click **Finish**.

   The migration pre-analysis process is started by the in-built pre-analysis tool.
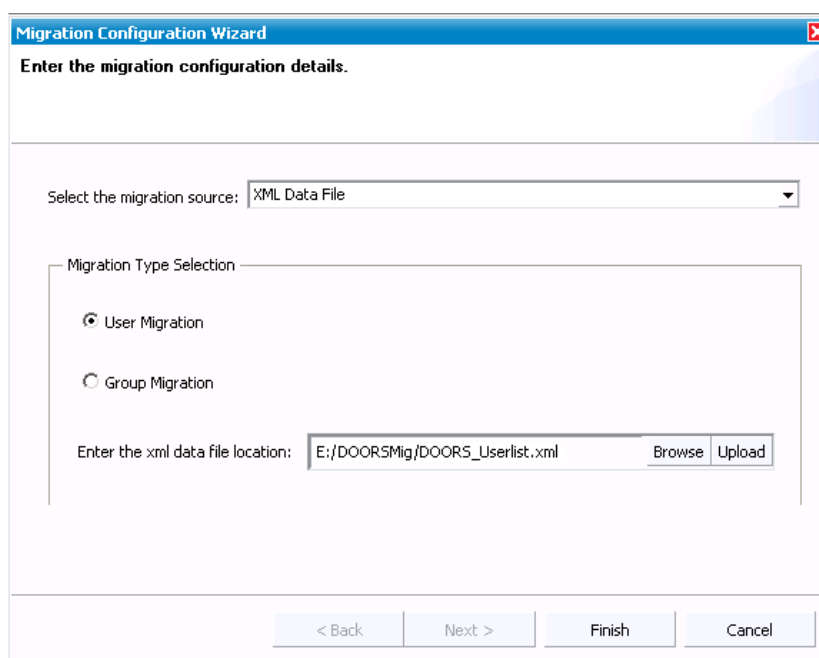
Pre-Analysis phase: The pre-analysis phase analyses each record against the target repository and classifies the data as Definitive, Conflicting and Duplicate. At this stage, the administrator user is allowed to perform the migration manually for each of the above category.

Definitive Records: The records which are clear of any conflicts or duplicate data are listed under this category. The administrator can directly migrate these records to the new repository.

Conflicting Records: The records that have one or more fields having the same details as of the record in the target repository are listed in this category.

The administrator can perform any of the following tasks.

- Discard the record
- Appropriately modify conflicting information
- Merge the user record

Duplicate Records: The records which already exist in the target repository. In other words, the listed records hold the same user id as in the target repository. These records cannot be migrate as it already exist in the target repository.

The administrator can perform any of the following tasks

- Ignore the record
- Merge the user record with existing matching records

Note The merge option ensures that the user properties such as access permissions, etc. of the same users belonging to different databases get merged into RDS. This prevents the migration of duplicate users into the target repository.

5. The Definitive records are selected by default. Click **Migrate** to move these records into the target repository.
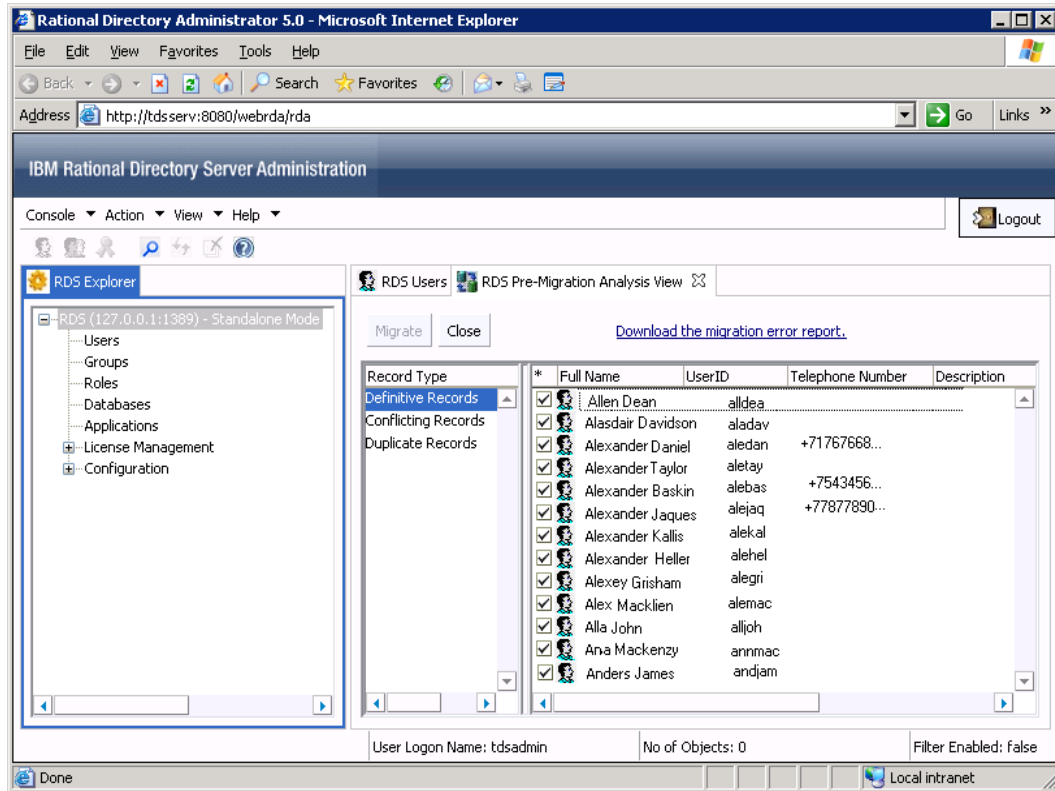
Note If there are any failed records, the details of that is recorded in the error log file. Click **Download the migration error report** option to see the error log file.

6. Click Refresh ✦ icon to see the migrated users in the RDS Users Tab.

7. Click **Conflicting Records.** You can see the conflicting information using the **Properties** option.

8. Double-click or right-click the user record and click **Properties.**

9. The **Migration User Object Properties** dialog box is displayed. Notice the following details:

- The **Last Name** field is shown in red. This means that the user record matching this last name exist in the target repository with some other user name.

- The **Conflicting Records** field displays the user id (allendean) of the record creating the conflict.

10. Click **OK** to return to the **Conflicting Records** pane.

11. To migrate the record as it is, select the check box next to the name, and then click **Migrate.**

12. To merge the user information for a record, select the check box next to the name, then select the **Merge** check box. Click **Migrate** to complete the operation.
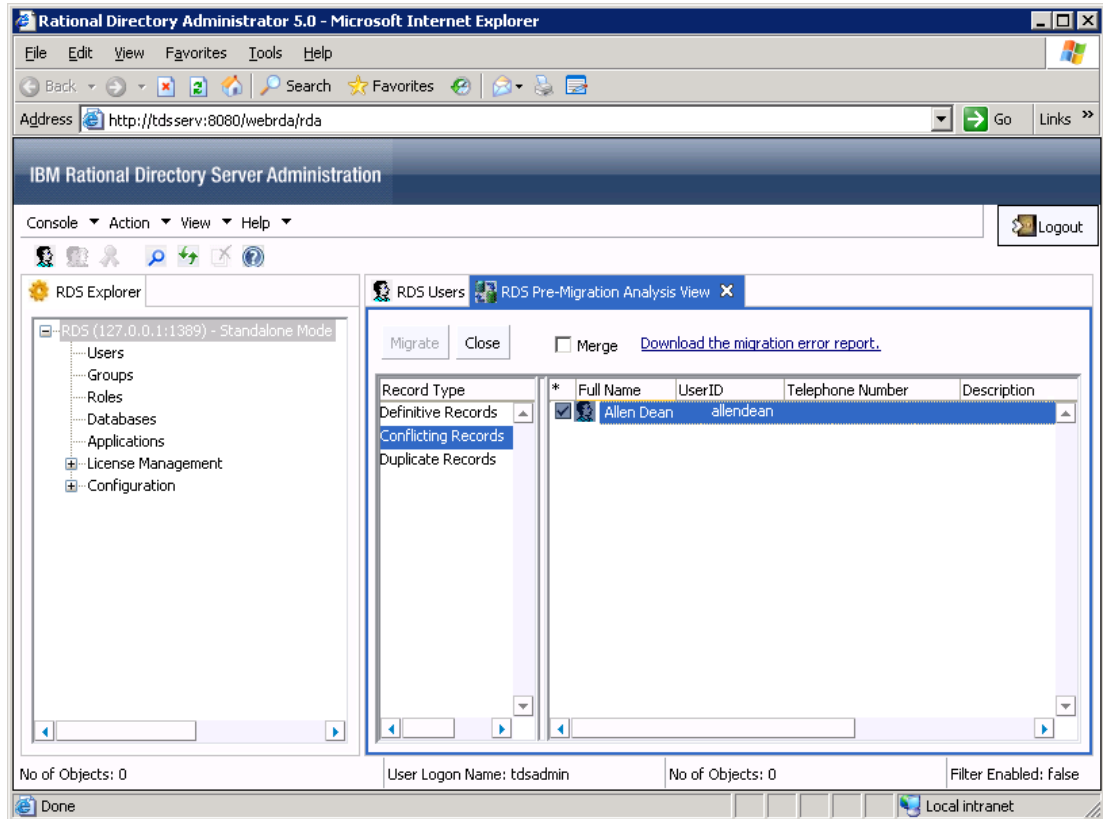
13. Click **Duplicate Records.** You can see the conflicting information using the **Properties** option.
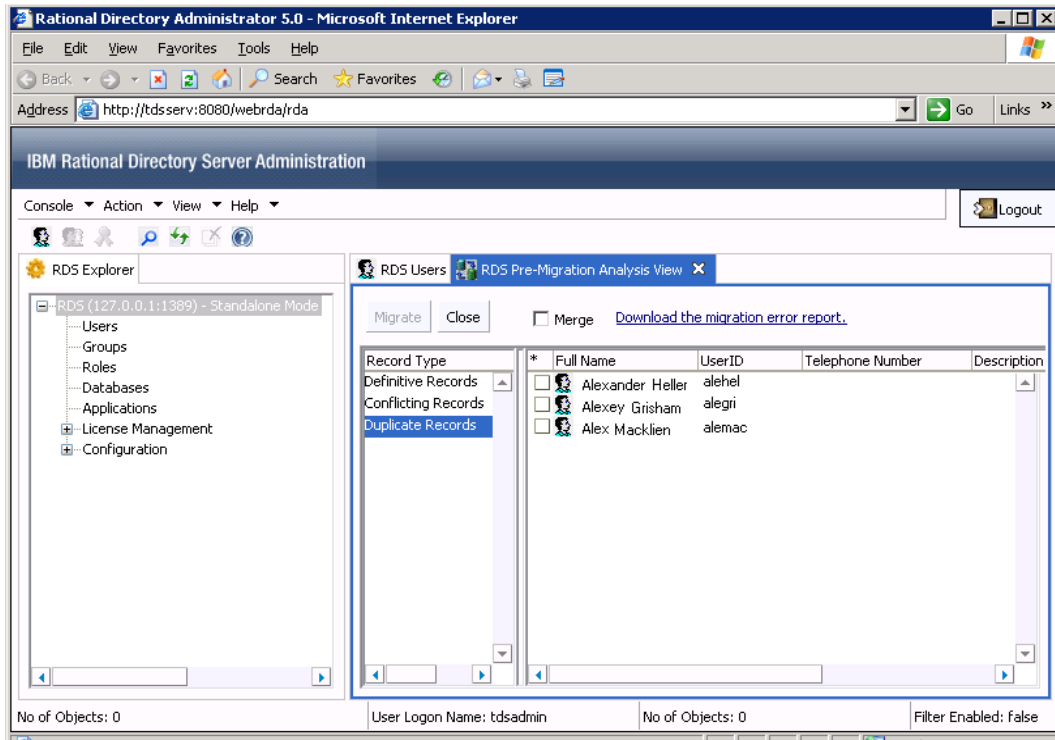
14. Double-click or right-click the record and then click **Properties** to view the details.

    Note You can only merge the records as it already exist in the target repository.

15. To migrate the record, select the check box next to the name, and then select the **Merge** check box. Click **Migrate** to complete the operation.

16. Click Refresh icon to see the migrated users and groups under the Users and Groups tab.

17. After migration, restart the RDS server.

Group migration

In case of group migration, the corresponding group database is displayed under the **DOORS Database** node along with the groups and roles under that database. The created roles will have the same name as of DOORS group database name.

Each database created under **DOORS Database** node (either by migration or by DOORS installation) will have the associated access role defined in TDA. Once the access role is created for that database, other users can be given access role to that database.

Only the users who have this access role defined within database will become valid users for that particular database. For example, the user **John Smith** migrated as part of marketing database will be associated with the marketing role.

You can further add or remove the DOORS database groups using RDA. The following screen shots displays the sample DOORS group database and roles created by the migration.

The following screen shot displays the DOORS group database.
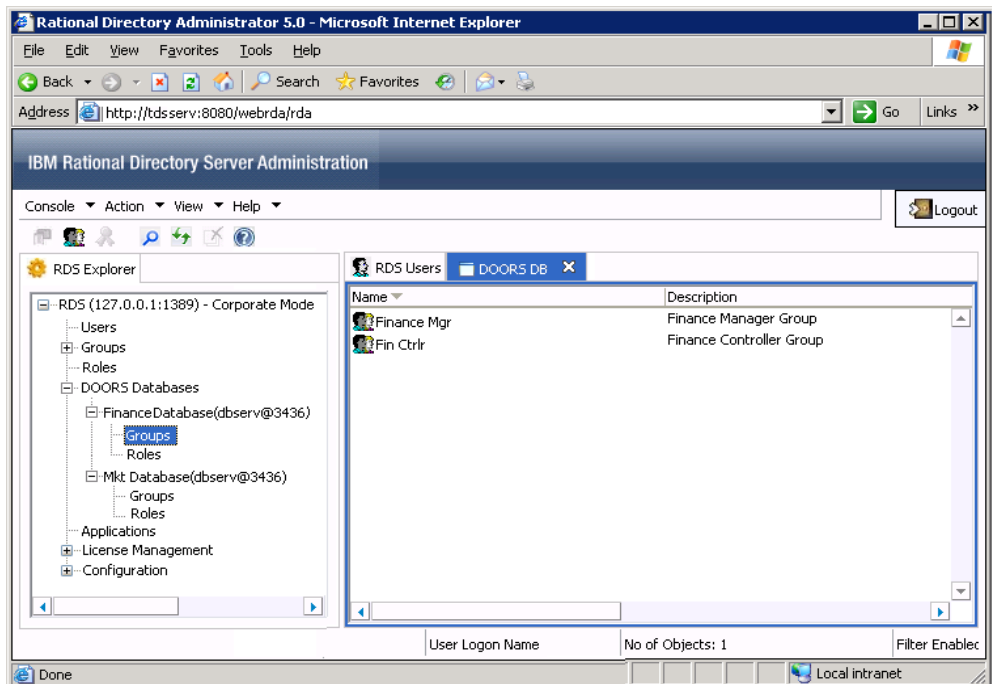
The following screen shot displays the associated roles.
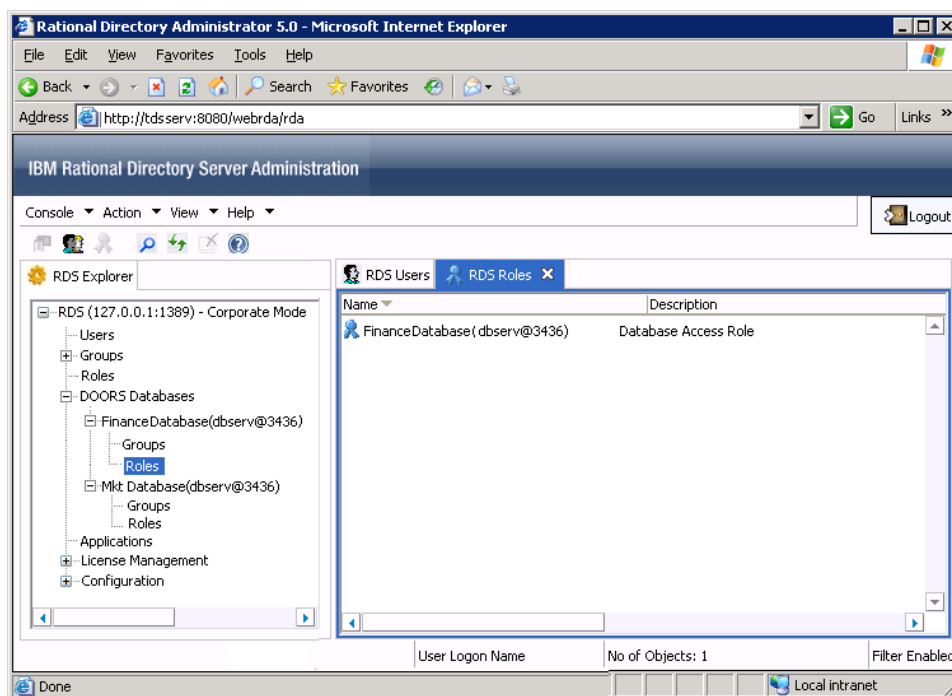
DOORS using TDS 3.0, 4.2, 4.3, or RDS 5.0

The following section explains the procedure for DOORS using TDS 3.0, 4.2, 4.3, and RDS 5.0 configuration.

To migrate the database, do the following:

1. On the **Console** menu, click **Migration**.

2. On the **Migration** Wizard, enter the details of TDS 3.0, 4.2, 4.3, or RDS 5.0 repository. Refer to step 2 of the Directory Server migration for details on the field descriptions.

3. Click **Next**. On the **Select the type of Migration** dialog box, click **User Migration or Group Migration**. Click the **DOORS Migration File** check box, and then click **Browse** to select the XML file to be migrated.
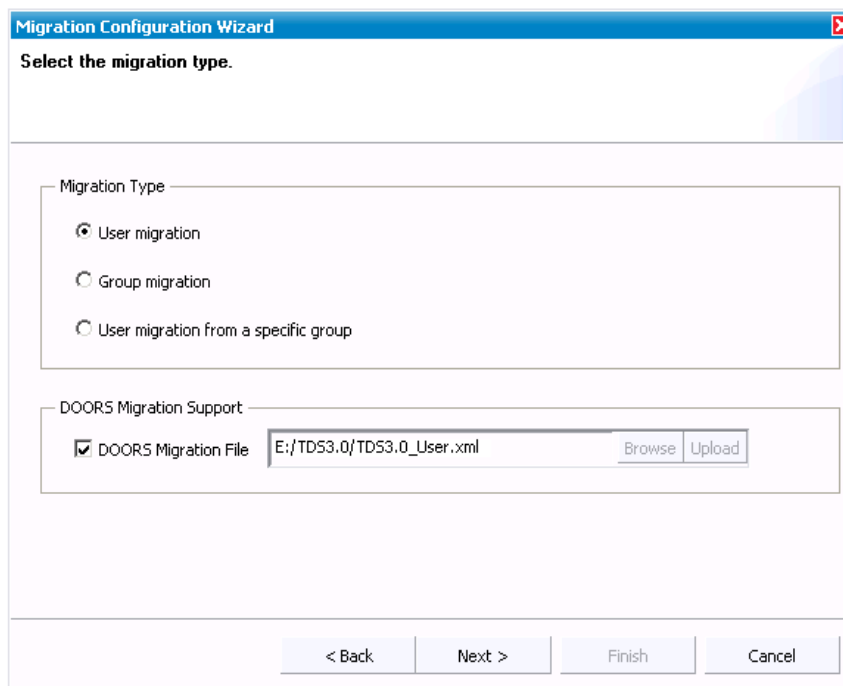
4. Click **Next.** The **Select the Filter Options** dialog box is displayed. Follow the steps from step 4 to step 16 of RDS Migration.

5. Click **Conflicting Records.** Follow the steps from step 7 to step 15 to migrate the records.

6. Click on Refresh icon to see the migrated users/group and roles in RDA.

7. After migration, restart the RDS server.

DOORS Data Migration with RDS in Corporate mode

The RDS additionally supports the DOORS data migration through various configurations. The DOORS user and group data can be migrated into RDS using the XML data file. The XML file format to be used for migration is defined in the **XML schema definition (XSD).** The XSD file defines the user and group attributes to be used for creating the XML file.

The DOORS database instances are migrated to RDS based on the database name as defined in the migration XSD file. The group migration migrates the groups as the database groups and the user migration associates the users to the defined database.

The following migration configurations are supported by RDS.

RDS mode	DOORS configuration	Migration synopsis
Corporate mode	DOORS using local database	• The users are mapped to the existing corporate users in RDS. If the mapping is successful, the selected users/groups can be migrated to the RDS.
		• The mapping is done using the best case algorithm match based on SystemLoginName, Common Name (CN), etc. For example, the System login name *"johsmi"* or CN *"John Smith"* will be mapped to user with similar details in the RDS corporate repository.
		• The user name is the partition logon name and the password is the partition password.
		• The migration preserves the DOORS access privileges of the particular user.

RDS mode	DOORS configurations	Migration synopsis
Corporate mode	DOORS using corporate database	The Users are matched against the RDS partition. If the partition matches the corporate database used by DOORS: • The users are mapped directly based on the Distinguished Name (DN) of the corporate database. • The groups are migrated as local database groups referring to corporate users. • The DOORS XML data file is used to retrieve the DOORS specific information of the mapped users. The DOORS specific access privileges are preserved for the migrated users.
		If the partition does not match the corporate database used by DOORS: • The users are migrated into RDS based on the best case algorithm mapping against systemLoginName, CN, etc. • The groups are migrated as local database groups referring to the corporate users. • The DOORS XML data file is used to retrieve the DOORS specific information of the mapped users. The DOORS specific access privileges are preserved for the migrated users.

RDS mode	DOORS configuration	Migration synopsis
Corporate mode	DOORS using TDS 3.0, 4.2, 4.3 and RDS 5.0	• Online migration to move users and group can be performed from TDS 3.0, 4.2, 4.3 and RDS 5.0 repository. • The users are matched against the partition using the best case algorithm mapping against systemLoginName, CN etc. • DOORS generated XML data files can be migrated for user specific database access privilege. • The groups are migrated as local database groups.

The following section explains the migration procedure for the following configurations.

- DOORS using local database
- DOORS using corporate database

To migrate the DOORS database, do the following:

1. On the **Console** menu, click **Migrate**.

2. Follow step 2 to step 3 of Standalone mode migration.

3. Click **Finish**. The Migration analysis process is started by the in-built Pre-Analysis tool.

Pre-Analysis phase

The pre-analysis phase analyses each record against the target repository and classifies the data as Definitive, Conflicting, Duplicate and UnMapped. At this stage, the administrator user is allowed to perform the migration manually for each of the above category.

Definitive Records: The records which are clear of any conflicts or duplicate data are listed under this category. The administrator can directly migrate these records to the new repository.

Conflicting Records: The records that have one or more fields having the same details as of the record in the target repository are listed in this category.

The administrator can perform any of the following tasks.

- Discard the record
- Appropriately modify conflicting information
- Merge the user record

Duplicate Records: The records which already exist in the target repository. In other words, the listed records hold the same user id as in the target repository. These records cannot be migrate as it already exist in the target repository.

The administrator can perform any of the following tasks.

- Ignore the record
- Merge the user record with existing matching records

UnMapped Records: The records which do not match the corporate partition are listed in this category. You can only view the details of the UnMapped records. You cannot migrate these records as they do not map to information on the corporate partition.

Note The **Merge** option ensures that the user properties such as access permissions, etc. of the same users belonging to different databases get merged into RDS. This prevents the migration of duplicate users into the target repository.

4. All records are selected by default. Click **Migrate** to move these records into the target repository.
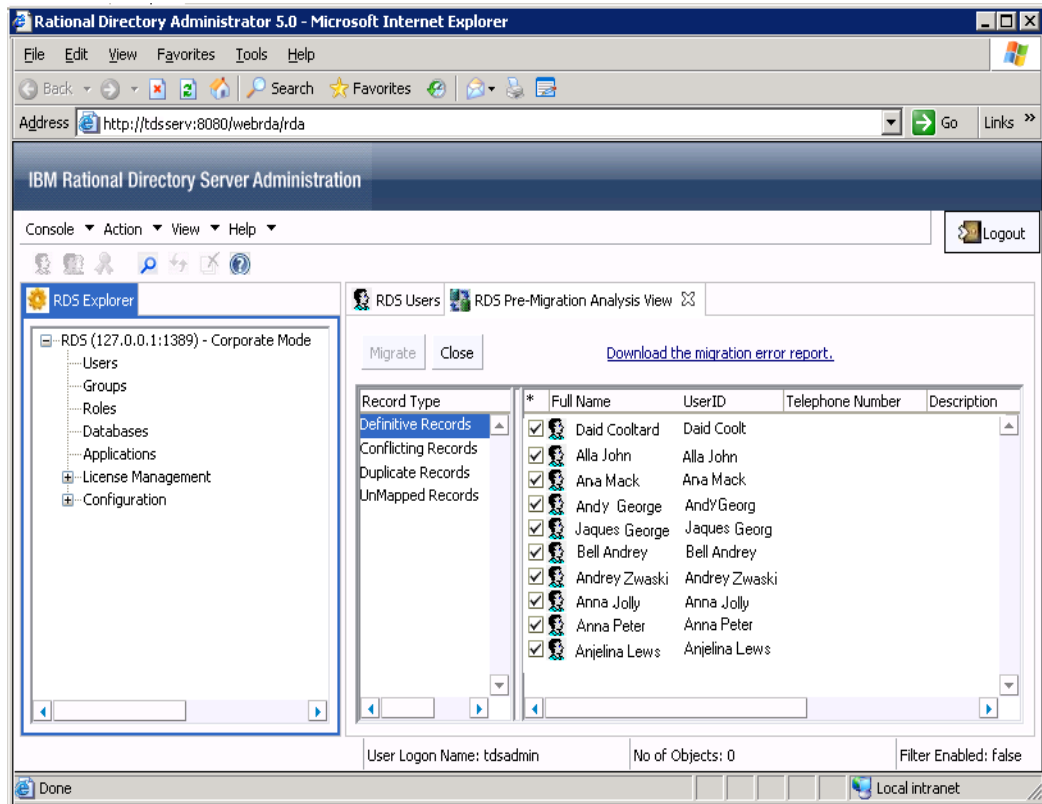
Note If there are any failed records, the details of that is recorded in the error log file. Click **Download the migration error report** option to see the error log.

5. Click **Conflicting Records.** Refer to <u>step 7</u> to <u>step 12</u>. for migrating these records.

6. Click on **Duplicate Records.** Refer to <u>step 13</u> to <u>step 15</u>. for migrating these records.

7. Click on **UnMapped Records.** The UnMapped DOORS user records are displayed in the right pane.
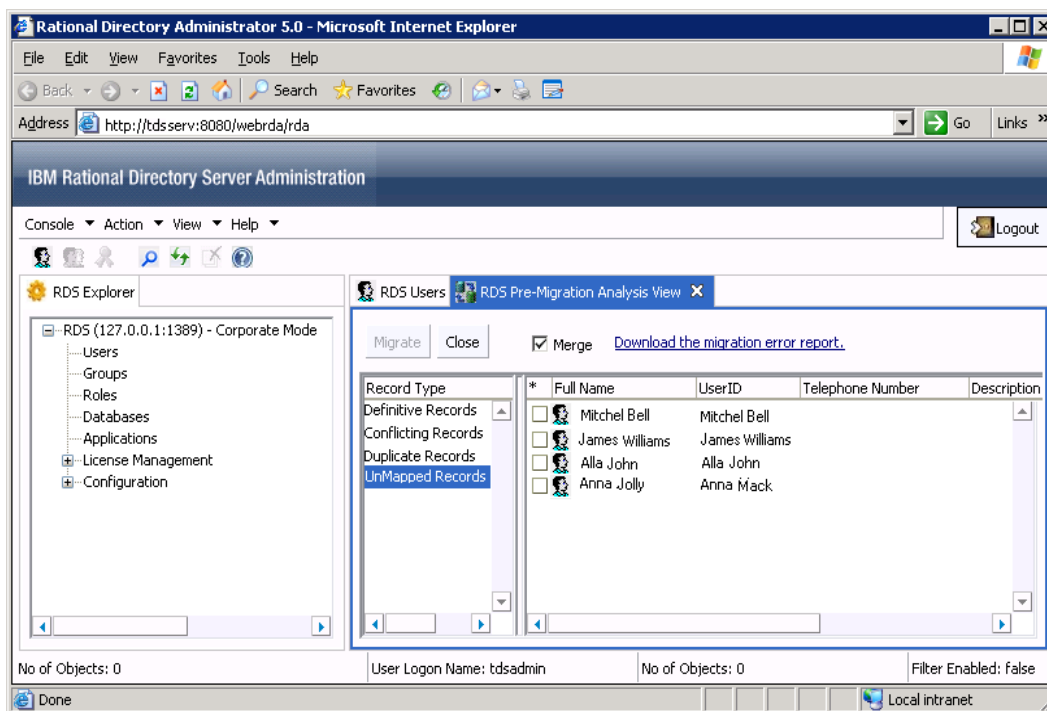
8. Double-click or right-click the record, and then click **Properties** to view the details.

9. Click Refresh [icon] icon to see the migrated users and groups under the Users and Groups tab.

10. After migration, restart the RDS server.

Group migration

In case of group migration, the corresponding group database is displayed under the **DOORS Database** node along with the groups and roles under that

database. The created roles will have the same name as of DOORS group database name.

Each database created under **DOORS Database** node (either by migration or by DOORS installation) will have the associated access role defined in TDA. Once the access role is created for that database, other users can be given access role to that database.

Only the users who have this access role defined within database will become valid users for that particular database. For example, the user **John Smith** migrated as part of marketing database will be associated with the marketing role.

You can further add or remove the DOORS database groups using TDA. The following screen shots displays the sample DOORS group database and roles created by the migration.

The following screen shot displays the DOORS Group database created by the migration.
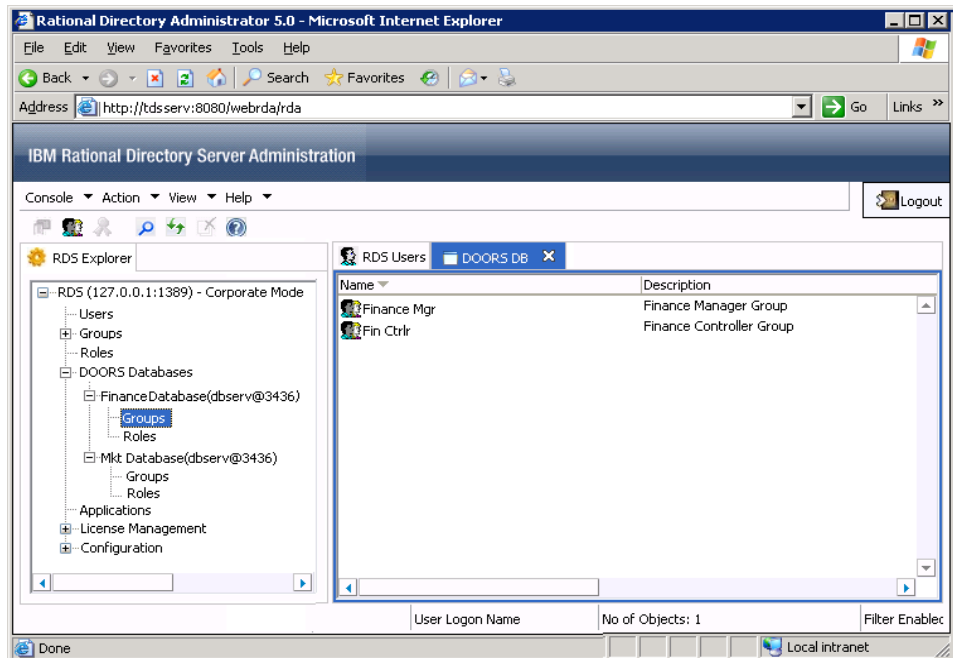
The following screen shot displays the sample associated roles created by the migration.
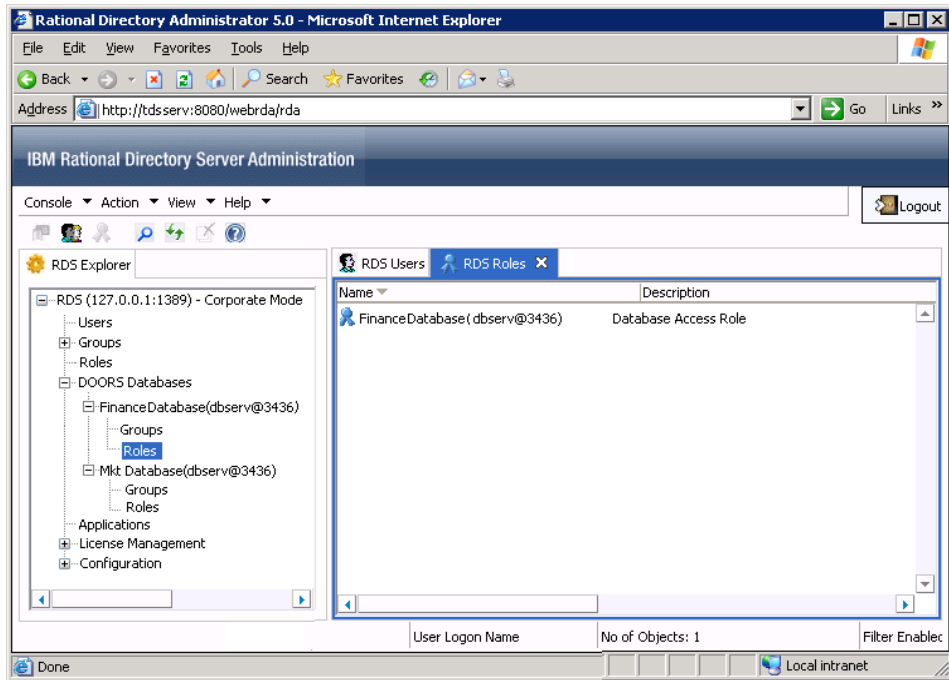
DOORS Using TDS 3.0, **4.2, 4.3, RDS 5.0**

The following section explains the migration procedure for the DOORS Using TDS 3.0, 4.2, 4.3, RDS 5.0 configuration.

To migrate DOORS database, do the following:

1. On the **Console** menu, click **Migrate** option.

2. On the **Migration** Wizard, enter the connection details of the TDS 3.0, 4.2, 4.3 or RDS 5.0 repository. Refer step 2 for the details on the field description.

3. Click **Next**.

   On the **Select the type of Migration** dialog box, click **User Migration or Group Migration**. If you want to migrate the DOORS specific data, click **DOORS Migration File** check box and then click **Browse** to select the XML file to be migrated.

4. Click **Next.** On the **Filter option** dialog box, follow the step 4 to step 13 of Directory Server Migration.

5. Click **Finish**. The Migration analysis process is started. This process is started by the in-built Pre-Analysis tool to analyses each record against the target repository. For more information on pre-analysis phase, see Pre-Analysis phase (page 87)

6. All Definitive records are selected by default. Click **Migrate** to move these records into the target repository.
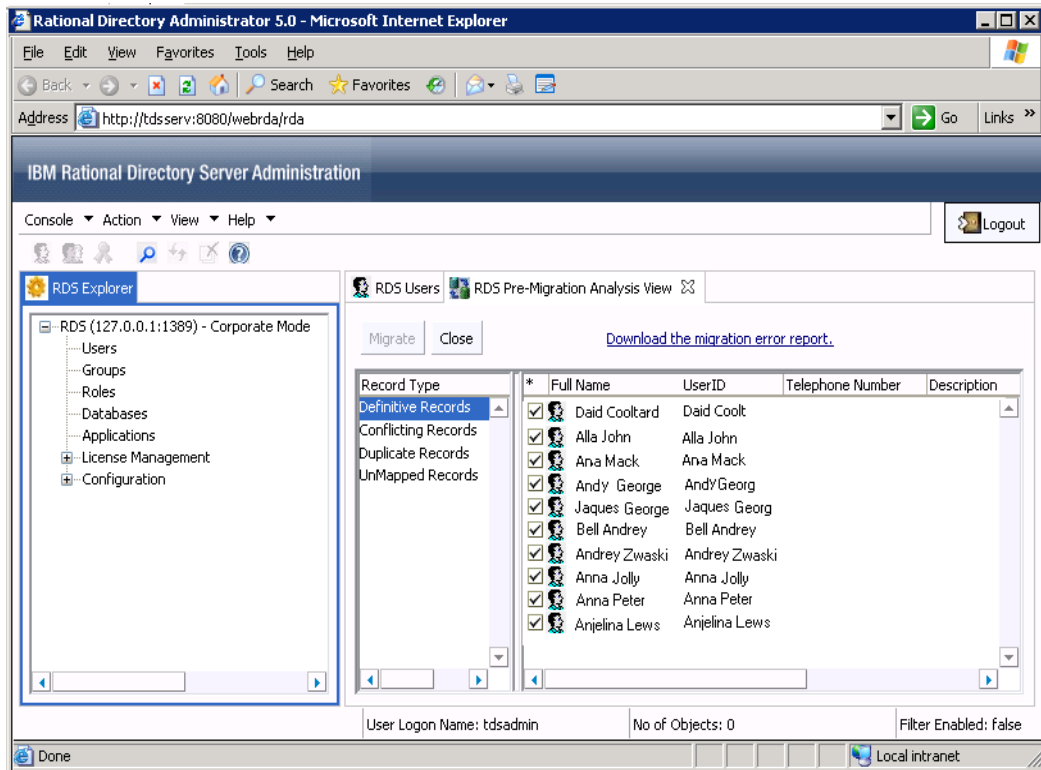
7. Once the migration is complete, the details of the migration will be displayed in the **Migration Results** screen.

Note If there are any failed records, the details of that is recorded in the error log file that you had selected in the beginning.

8. Click Refresh ✦ icon to see the migrated users in the RDS Users tab.

9. Click **Conflicting Records.** The records that have one or more fields having the same details as of the record in the target repository are listed in this category. Refer to step step 7 to step 12 for migrating the records.

10. Click on **Duplicate Records.** The records which already exist in the target repository are listed under this category. Refer to step step 13 to step 15 for details on migrating the records.

11. Click on **UnMapped Records.** The records which does not match the corporate partition are listed under this category. You can only view the details of the UnMapped records. You cannot migrate these records as they do not map to information on the corporate partition.

12. After migration, restart the RDS server.

Note In case of group migration, the corresponding group database and associated roles are created under DOORS Database node. For more details on groups and roles, refer to Group migration (page 90).

6 *Terms and Concepts*

Term	Definition
CN	Common Name consist of user's first name, last name, etc.
DIT	Directory Information Tree. The logical representation of the information stored in the directory. It mirrors the tree model used by the directory server, with the tree's root point appearing at the top of the hierarchy.
DN	The string representation of an entry's name and location in the directory.
Entry	A group of attributes and a unique distinguished name.
Object Class	Defines an entry type in the directory by defining which attributes are contained in the entry.
Object Identifier	(OID) A string representation of an object identifier consists of a list of numeric values separated by periods, e.g. "1.3.6.1.4.1.15265.2". The object identifiers are used to uniquely identify schema elements, including object classes and attribute types.
OU	Organizational Units are administrative-level containers that allow the administrators to organize groups of users together. An OU can be set up for each department. Within that department OU, there could be objects that represent users, groups, etc.
Partition	A partition is a branch or a complete sub tree of the directory information tree (DIT).
Root Suffix	The parent of one or more sub suffixes.

Term	**Definition**
Schema	Definitions describing what types of information can be stored as entries in the directory. When information that does not match the schema is stored in the directory, clients attempting to access the directory may be unable to display the proper results.
Suffix	The name of the entry in the directory tree, below which data is stored.

Appendix A: User schema definition format

The user XML file to be migrated must contain the data in the following format.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/
XMLSchema">

<xsd:element name="UserRecordSequence"
type="UserRecordSequenceType"/>

<!-- Type for a User RecordSequence  -->

<xsd:complexType name="UserRecordSequenceType">
   <xsd:choice minOccurs="0" maxOccurs="unbounded">
      <xsd:element name="UserRecord"
type="UserRecordType"/>
   </xsd:choice>

   <xsd:attribute name="DOORSUserSource">
      <xsd:simpleType>
        <xsd:restriction base="xsd:string">
             <xsd:enumeration value="Local"/>
             <xsd:enumeration value="LDAP"/>
             <xsd:enumeration value="TDS"/>
        </xsd:restriction>
      </xsd:simpleType>
   </xsd:attribute>

   <xsd:attribute name="TDSServer" type="xsd:string"/
>

   <xsd:attribute name="DoorsLdapServer" type =
"xsd:string"/>

   <xsd:attribute name="TDSMode">
```

```
    <xsd:simpleType>
      <xsd:restriction base="xsd:string">
           <xsd:enumeration value="Standalone"/>
           <xsd:enumeration value="Corporate"/>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:attribute>

  <xsd:attribute
name="DOORSLdapMatchesTDSPartition"
type="BooleanType" default="TRUE"/>

</xsd:complexType>

<!--Type for a UserRecordType element -->
<xsd:complexType name="UserRecordType">
  <xsd:all>
  <xsd:element name="uid" type="xsd:string"
minOccurs="1" maxOccurs="1"/>
  <xsd:element name="cn" type="xsd:string"
minOccurs="1" maxOccurs="1"/>
  <xsd:element name="sn" type="xsd:string"
minOccurs="1" maxOccurs="1"/>
  <xsd:element name="authPasswordInfo"
type="AuthPasswordType" minOccurs="1" maxOccurs="1"/
>
  <xsd:element name="authPasswordValue"
type="xsd:string" minOccurs="1" maxOccurs="1"/>
  <xsd:element name="tdsPasswordResetFlag"
type="BooleanType" minOccurs="0" maxOccurs="1"/>
  <xsd:element name="description" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
  <xsd:element name="telephoneNumber"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
  <xsd:element name="postalAddress"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
```

```xml
   <xsd:element name="displayName" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="mail" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="employeeNumber"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="givenName" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSUserAttribute"
type="DOORSUserAttributeType" minOccurs="0"
maxOccurs="1"/>
   <xsd:element name="tdsFullyQualifiedObjectId"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsSYNERGYUserName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsOSNTUserName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsOSPosixUserName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="systemLoginName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsCorporateDN"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSDatabaseId"
type="DOORSDatabaseIdType" minOccurs="0"
maxOccurs="1"/>
   </xsd:all>
</xsd:complexType>

<xsd:simpleType name="AuthPasswordType">
   <xsd:restriction base="xsd:string">
    <xsd:enumeration value="SHA"/>
       <xsd:enumeration value="SSHA"/>
    <xsd:enumeration value="CLEAR"/>
    <xsd:enumeration value="DOORSMD5"/>
   </xsd:restriction>
</xsd:simpleType>
```

```
<xsd:simpleType name="BooleanType">
   <xsd:restriction base="xsd:string">
      <xsd:enumeration value="TRUE"/>
       <xsd:enumeration value="FALSE"/>
   </xsd:restriction>
</xsd:simpleType>

<xsd:complexType name="DOORSUserAttributeType">
   <xsd:choice minOccurs="0" maxOccurs="unbounded">
      <xsd:element name="UserAttribute"
type="xsd:string"/>
   </xsd:choice>
</xsd:complexType>

<xsd:complexType name="DOORSDatabaseIdType">
   <xsd:choice minOccurs="0" maxOccurs="unbounded">
      <xsd:element name="DatabaseId"
type="xsd:string"/>
   </xsd:choice>
</xsd:complexType>

</xsd:schema>
```

Appendix B: Group schema definition format

The user XML file to be migrated should contain the data in the following format.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/
XMLSchema">


<xsd:element name="GroupRecordSequence"
type="GroupRecordSequenceType"/>


<!-- Type for a GroupRecordSequence  -->


<xsd:complexType name="GroupRecordSequenceType">
   <xsd:choice minOccurs="0" maxOccurs="unbounded">
      <xsd:element name="GroupRecord"
type="GroupRecordType"/>
   </xsd:choice>


   <xsd:attribute name="DOORSUserSource">
      <xsd:simpleType>
        <xsd:restriction base="xsd:string">
            <xsd:enumeration value="Local"/>
            <xsd:enumeration value="LDAP"/>
            <xsd:enumeration value="TDS"/>
        </xsd:restriction>
      </xsd:simpleType>
   </xsd:attribute>


   <xsd:attribute name="TDSServer"
type="xsd:string"/>
```

```
<xsd:attribute name="DoorsLdapServer" type =
"xsd:string"/>

<xsd:attribute name="TDSMode">
   <xsd:simpleType>
      <xsd:restriction base="xsd:string">
            <xsd:enumeration value="Standalone"/>
            <xsd:enumeration value="Corporate"/>
      </xsd:restriction>
   </xsd:simpleType>
</xsd:attribute>

<xsd:attribute
name="DOORSLdapMatchesTDSPartition"
type="BooleanType" default="TRUE"/>

</xsd:complexType>

<!--Type for a GroupRecordType element -->
<xsd:complexType name="GroupRecordType">
   <xsd:all>
   <xsd:element name="cn" type="xsd:string"
minOccurs="1" maxOccurs="1"/>
   <xsd:element name="businessCategory"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="description" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="o" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="ou" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
   <xsd:element name="owner" type="xsd:string"
minOccurs="0" maxOccurs="1"/>
```

```xsd
      <xsd:element name="UserList" type="UserListType"
minOccurs="0" maxOccurs="1"/>
         <xsd:element name="seeAlso"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSDatabaseId"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSDatabaseName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsFullyQualifiedObjectId"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsCorporateDN"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSDBHostName"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   <xsd:element name="tdsDOORSDBPortNumber"
type="xsd:string" minOccurs="0" maxOccurs="1"/>
   </xsd:all>
</xsd:complexType>

<xsd:complexType name="UserListType">
   <xsd:choice minOccurs="0" maxOccurs="unbounded">
      <xsd:element name="uid" type="xsd:string"/>
   </xsd:choice>
</xsd:complexType>

<xsd:simpleType name="BooleanType">
   <xsd:restriction base="xsd:string">
      <xsd:enumeration value="TRUE"/>
       <xsd:enumeration value="FALSE"/>
   </xsd:restriction>
</xsd:simpleType>

</xsd:schema>
```

Attributes used in the XSD file

The following table explains the attributes used in the schema definition file.

Attribute name	Definition
uid	The unique identifier name for the user. All the user logins are mapped using the unique identifier.
cn	The common name for the user. For example, the First name, Last name, etc.
sn	The surname for the user.
authPasswordInfo	The password info should contain the algorithm used for populating the password values. The RDS supports the following encryption algorithms for the password in the imported files: • Secure Hash Algorithm (SHA) • Salted Secure Hash Algorithm (SSHA) • CLEAR • DOORSMD5 (DOORS specific encryption algorithm)
authPasswordValue	The passwords used for each user login.
description	The brief description about the user.
telephoneNumber	The contact number of the user.
postalAddress	The postal address of the user.
displayName	The display name for the user. For example, for the user name John Smith, the display name could be **John Smith**.
mail	The e-mail id of the user.
employeeNumber	The employee number of the user.
tdsFullyQualifiedObjectId	The Unique User ID (UUID).

Attribute name	Definition
tdsDOORSUserAttribute	This multivalued attribute is DOORS specific user data.
tdsSYNERGYUserName	This specifies the Synergy user name.

Note The import files have to be UTF-8 encoded files. If the import files are not of UTF-8 format, non ASCII characters will not be successfully imported and appear corrupted in RDA.

DOORS specific group format definition

The following table explains the DOORS specific group attribute used in the schema definition file.

Attribute name	Definition
uid	This specifies the unique identifier name for the DOORS group.
cn	This specifies the common name for the group. For example, the First name, Last name, etc.
sn	This specifies the surname for the group.
tdsDOORSDatabaseId	This specifies the DOORS group database id.
tdsDOORSDatabaseName	This specifies the DOORS database name.

Appendix C: Example : RDS user migration XML format

The following section shows the sample user migration XML format.

```
<?xml version="1.0" encoding="UTF-8"?>
<UserRecordSequence xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance">
 <UserRecord>
            <cn>Allina sean</cn>
            <sn>Dean</sn>
            <uid>dallen</uid>
            <authPasswordInfo>DOORSMD5</authPasswordInfo>
<authPasswordValue>588c9aef7f6f2d97c9cbbb400e91e89c</
authPasswordValue>
            <displayName>Allen</displayName>
<tdsFullyQualifiedObjectId>46d3f2ec6df15296:0000000000000
002:01111111</tdsFullyQualifiedObjectId>
        </UserRecord>
<UserRecord>
            <cn>James Johnson</cn>
            <sn>Johnson</sn>
            <uid>jamesj</uid>
            <authPasswordInfo>DOORSMD5</authPasswordInfo>
<authPasswordValue>588c9aef7f6f2d97c9cbbb400e91e89c</
authPasswordValue>
            <description>Product Manager</description>
            <telephoneNumber>011 2007 04</telephoneNumber>
            <postalAddress>East Wood Street</
postalAddress>
        <displayName>James Johnson</displayName>
            <mail>james.johnson@abc.org</mail>
<tdsFullyQualifiedObjectId>46d3f2ec6df15296:0000000000000
003:00000000</tdsFullyQualifiedObjectId>
        </UserRecord>
<UserRecord>
```

```
        <uid>analew</uid>
        <cn>Ana Lewis</cn>
        <sn>Lewis</sn>
    <authPasswordInfo>DOORSMD5</authPasswordInfo>
<authPasswordValue>588c9aef7f6f2d97c9cbbb400e91e89c</
authPasswordValue>
        <description>Product Engineer</description>
        <telephoneNumber> 9112345789 </telephoneNumber>
        <postalAddress>#12, Irvine, Sweden   </
postalAddress>
        <mail>analew@abc.com </mail>
        <employeeNumber/>
        <tdsDOORSUserAttribute>
        <UserAttribute>i=k</UserAttribute>
        <UserAttribute>karse</UserAttribute>
        <UserAttribute>brian</UserAttribute>
        <UserAttribute></UserAttribute>
        </tdsDOORSUserAttribute>
<tdsFullyQualifiedObjectId>46d3f52b43693142:0000000000000
003:01111111</tdsFullyQualifiedObjectId>
        <tdsSYNERGYUserName>parcamre</tdsSYNERGYUserName>
        <tdsOSNTUserName>parcamre</tdsOSNTUserName>
        <tdsOSPosixUserName>parcamre</tdsOSPosixUserName>
</UserRecord>
<UserRecord>
        <uid>chrisj</uid>
        <cn>chris johnston </cn>
        <sn>sesh</sn>
     <authPasswordInfo>SHA</authPasswordInfo>
        <authPasswordValue>6bkkIW8mDtYleguPDVM5ZZWnieM=</
authPasswordValue>
<description>Marketing Manager</description>
        <tdsSYNERGYUserName>bill</tdsSYNERGYUserName>
        <tdsOSNTUserName>indkarse</tdsOSNTUserName>
</UserRecord>
</UserRecordSequence>
```

Appendix D: Example : RDS group migration XML format

The following section shows the sample group migration XML format.

```
<GroupRecordSequence xmlns:xsi="http://www.w3.org/
2001/XMLSchema-instance">

<GroupRecord>
   <cn>TDS </cn>
   <businessCategory> </businessCategory>
   <description>Product Manager</description>
   <o> </o>
   <ou> </ou>
   <owner> </owner>
   <UserList>
      <uid>johnsmi</uid>
      <uid>jamwill </uid>
      <uid>annjoh</uid>
      <uid>chrosc</uid>
   </UserList>

   <tdsDOORSDatabaseId>46d3f2ec6df15299</
tdsDOORSDatabaseId>
   <tdsDOORSDatabaseName>TDS_DATABASE_NODE</
tdsDOORSDatabaseName>

<tdsFullyQualifiedObjectId>46d3f2ec6df15299:00000000
0000000e</tdsFullyQualifiedObjectId>

</GroupRecord>

<GroupRecord>
   <cn>Doors </cn>
```

```
        <description>Marketing </description>
        <UserList>
            <uid>johnsmi</uid>
            <uid>jamwill </uid>
            <uid>annjoh</uid>
            <uid>chrosc</uid>
        </UserList>
        <tdsDOORSDatabaseName>DOORS_DATABASE_NODE</
    tdsDOORSDatabaseName>
    </GroupRecord>

    <GroupRecord>
        <cn> </cn>
        <description>Manager </description>
        <UserList>
            <uid>johnsmi</uid>
            <uid>jamwill </uid>
            <uid>annjoh</uid>
            <uid>chrosc</uid>
        </UserList>
    </GroupRecord>
    </GroupRecordSequence>
```

Appendix E: Notices

© Copyright 2000, 2009

U.S. Government Users Restricted Rights - Use, duplication, or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send written license inquiries to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send written inquiries to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT,

MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions. Therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

Intellectual Property Dept. for Rational Software
IBM Corporation
1 Rogers Street
Cambridge, Massachusetts 02142
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Copyright license

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at www.ibm.com/legal/copytrade.html.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product or service names may be trademarks or service marks of others.

Index