NewgenONE OmniDocs Service

Administration Guide

Version: 11.3

Disclaimer

This document contains information proprietary to Newgen Software Technologies Limited. The user may not disclose or use any proprietary information or use any part of this document without written permission from Newgen Software Technologies Limited.

Newgen Software Technologies Limited makes no representations or warranties regarding any software or to the contents or use of this manual. It also specifically disclaims any express or implied warranties of merchantability, title, or fitness for any particular purpose. Even though Newgen Software Technologies Limited has tested the hardware and software and reviewed the documentation, it does not guarantee or implies that this document is error-free or accurate regarding any particular specification. As a result, this product is sold as it is and the user, the purchaser, is assuming the entire risk as to its quality and performance. Further, Newgen Software Technologies Limited reserves the right to revise this publication and make changes in its content without any obligation to notify any person, of such revisions or changes. Newgen Software Technologies Limited authorizes no Newgen agent, dealer, or employee to make any modification, extension, or addition to the above statements.

Newgen Software Technologies Limited has attempted to supply trademark information about company names, products, and services mentioned in this document. The trademarks indicated in this document were derived from various sources.

Newgen Software Technologies Limited.
Newgen Software, Registered Office, New Delhi
E-44/13
Okhla Phase-II
India
Phone: +91 1146 533 200
info@newgensoft.com

Table of Contents

1 Preface

This administration guide describes how to manage the different services of OmniDocs such as Java Transaction Server (JTS), Storage Management Server (SMS), LDAP, Alarm Mailer, and Thumbnail Manager.

NOTE:

The NewgenONE OmniDocs 11.3 product documentation is available at the following locations:

- Newgen Internal Doc Portal – For Newgen employees.
- Newgen Partner Portal – For Newgen partners.

1.1 Revision history

Revision Date	Description
July 2024	Initial publication

1.2 Documentation feedback

To provide feedback or any improvement suggestions on technical documentation, write an email to docs.feedback@newgensoft.com

To help capture your feedback effectively, share the following information in your email.

- Document name
- Version
- Chapter, topic, or section
- Feedback or suggestions

2 Introduction to OmniDocs

OmniDocs is an **Enterprise Document Management** platform for creating, capturing, managing, delivering, and archiving large volumes of documents. It provides a highly scalable, unified repository for securely storing and managing documents in an enterprise. It provides access to enterprise documents directly and through integration with business applications.

OmniDocs offers a centralized repository for enterprise documents and supports rights-based archival. It manages the complete lifecycle of documents through record retention, storage, and retrieval policies. It also supports exhaustive document and folder searches based on date, indexes, and general parameters as well as Full-Text Search (FTS) on image and electronic documents.

The very basic operation of the system is to access documents from a remote site and work on them, without archival and retrieval hassles. In an enterprise-wide scenario, the **Document Management System (DMS)** can be centralized with the robust and efficient “OmniDocs”. Further, this **DMS** can also be accessed from any part of the world through OmniDocs Web.

3 OmniDocs Service Administration

The OmniDocs Service Administration (OSA) is used for remote administration of the Java Transaction Server (JTS), Storage Management Server (SMS) and LDAP service, Alarm Mailer, Thumbnail Manager, and Listener.

The JTS, SMS, and Listener listen on a port called the Admin Port in addition to the client ports (for OmniDocs client's request). The OSA manages these servers by connecting to their Admin Port.

LDAP Service, Alarm Mailer, and the Thumbnail Manager do not have the additional Admin Port and hence these services can be managed on the local computer where the OSA is installed.

3.1 Getting Started

To login into the OmniDocs Service Administration module:

1. Start the OmniDocs Service Administration module.
2. When the application is launched, the **Login** dialog box appears.

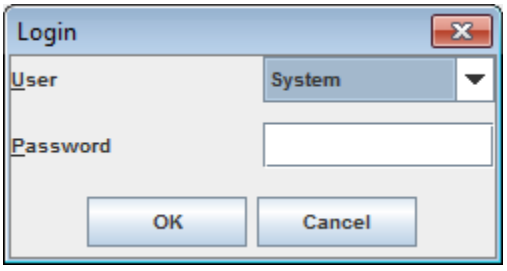


Figure 3.1

3. Select the username from the **User** dropdown list and specify the **Password**.
4. Click on **OK** to login.

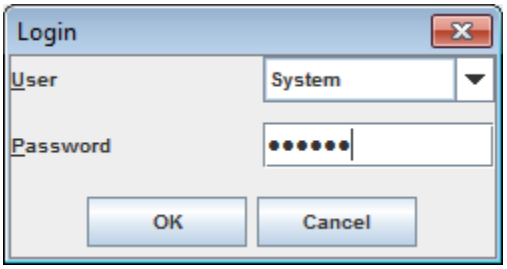


Figure 3.2

5. OmniDocs Service Administration screen appears, displaying the list of all registered servers.

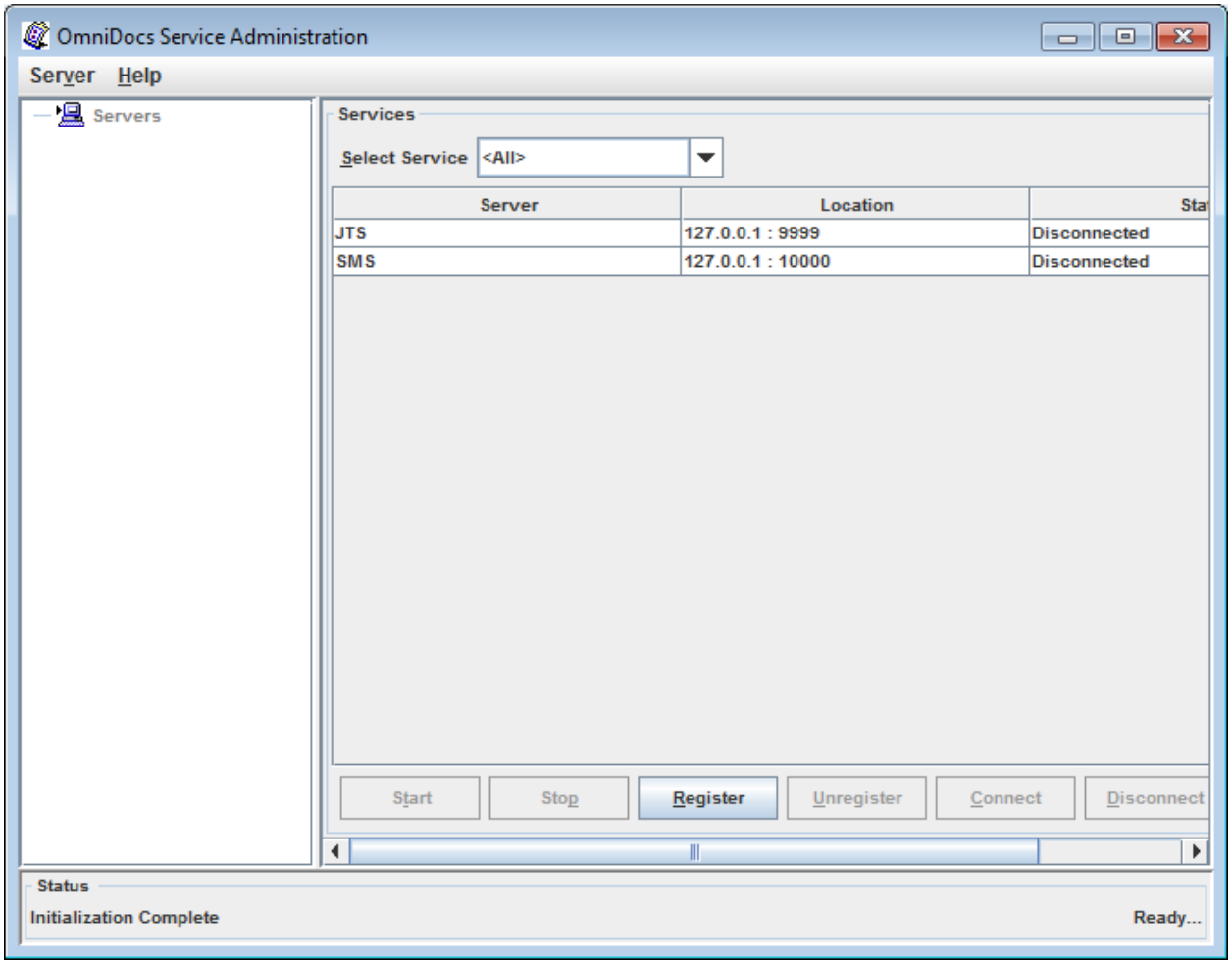


Figure 3.3

There are no registered servers when the screen is invoked for the first time. The steps to register the servers are:

1. Register the server.
2. Connect to the specific server (applicable only for JTS, SMS, and Listener)
3. Once the OSA is connected to the server, various operations like **Start**, **Stop** and **Manage** can be performed on the selected server.

NOTE:

The OSA must be first disconnected from the server and only then it can be unregistered (applicable only for JTS, SMS, and Listener).

For LDAP service, Alarm Mailer, and Thumbnail manager, there is no need to connect to these services. These services can be directly managed on the host machine.

3.1.1 Registering a Server

To Register a Server:

1. Click the **Register** button.
2. The **Register New Server** dialog box appears.

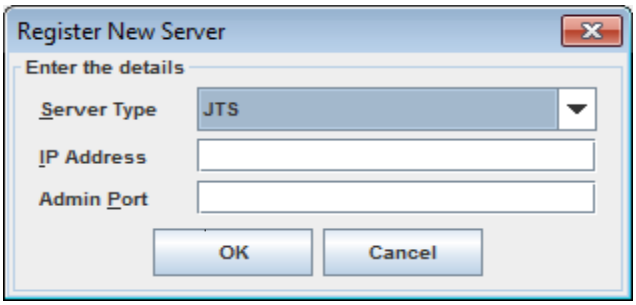


Figure 3.4

(Similar dialog box applies to SMS and Listener services also)

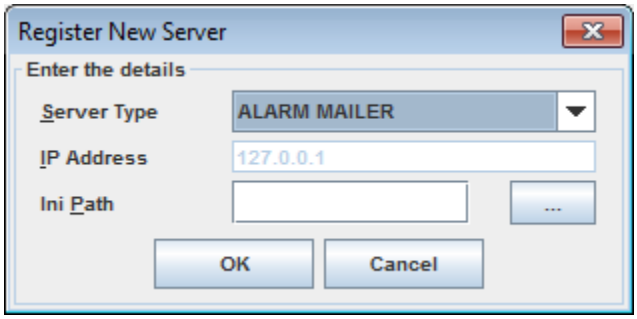
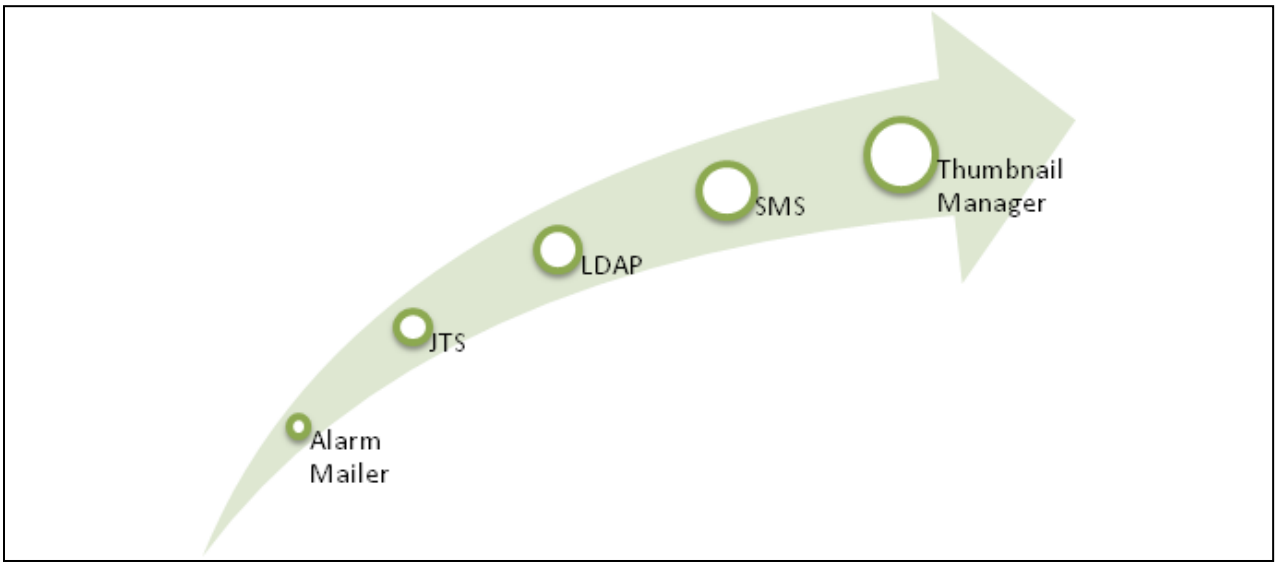


Figure 3.5

(Similar dialog box applies to Thumbnail Manager and LDAP services also)

3. Select the type of the server from the **Server Type** dropdown list. It can be:



4. Specify the IP address of the server in the **IP Address** textbox.
5. Specify the Admin Port in the **Admin Port** textbox (applicable only for JTS, SMS, and Listener).
6. Specify the path of the INI file of the service in the **Ini Path** textbox. The path can also be specified by clicking the '…' button, which opens a file open dialog box from where the required INI File can be selected (this is applicable only for Alarm Mailer, Thumbnail Manager, and LDAP services).

NOTE:

Once the server is registered it is displayed in the list and is in a disconnected state (applicable only for JTS and SMS).

7. A filter can be performed on the server (Alarm Mailer, JTS, LDAP, Listener, SMS, and Thumbnail Manager).

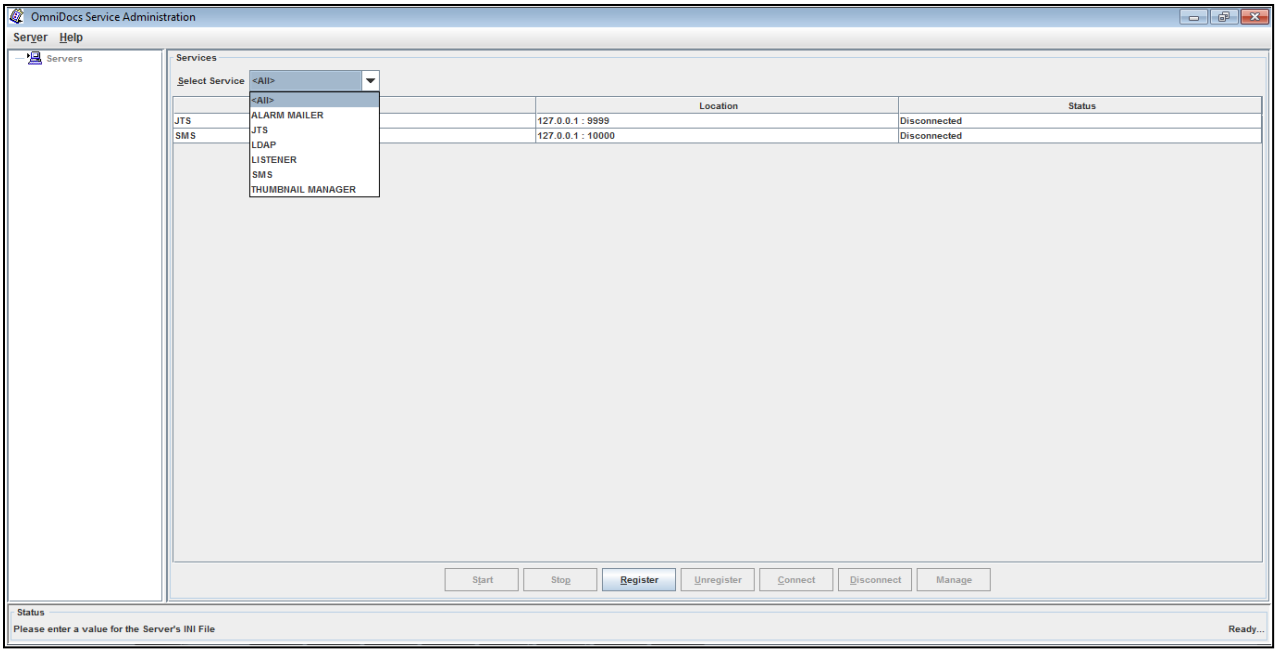


Figure 3.6

8. Select **All** option from **Select Service** dropdown list, to display all the servers.
9. Select **JTS** option from **Select Service** dropdown list, to display only the JTS servers on the list.
10. Select **Alarm Mailer** option from **Select Service** dropdown list, to display only the Alarm Mailers on the list.
11. Select **LDAP** option from **Select Service** dropdown list, to display only the LDAP services on the list.
12. Select **Listener** option from **Select Service** dropdown list, to display only the Listeners on the list.
13. Select **Thumbnail Manager** option from **Select Service** dropdown list, to display only the Thumbnail managers on the list.
14. Select **SMS** option from **Select Service** dropdown list box, to display only the SMS servers on the list.

3.1.2 Connecting to the Server

To connect to the server

1. Select the server from the Select Service list box.
2. Click the **Connect** button to connect the OSA with the selected server.

NOTE:

Once the OSA connects with a server the start/stop operations can be performed on that server from the server screen. Only JTS, SMS, and Listener services need to be connected to the OSA for their management. The Alarm Mailer, Thumbnail Manager, and LDAP services are managed directly on the host machine and therefore there is no need to connect to them.

3.1.3 Managing the Server

To perform operations other than **start**/**stop**, the server needs to be managed.

To manage the connected server:

1. Select the connected server from the list of registered servers.
2. Click the **Manage** button. An entry of the connected server along with its IP Address is displayed on the **Servers** list box of the Repository view.

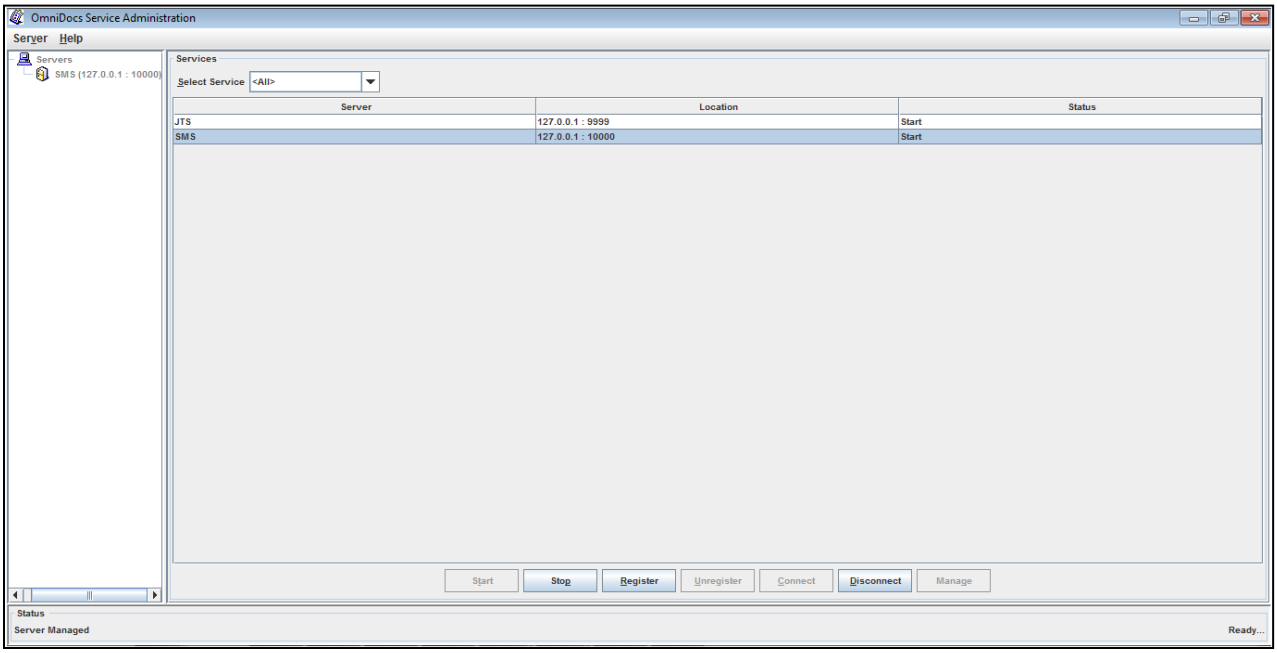


Figure 3.7

3. Select the **SMS** server from the list of servers in the Repository view.

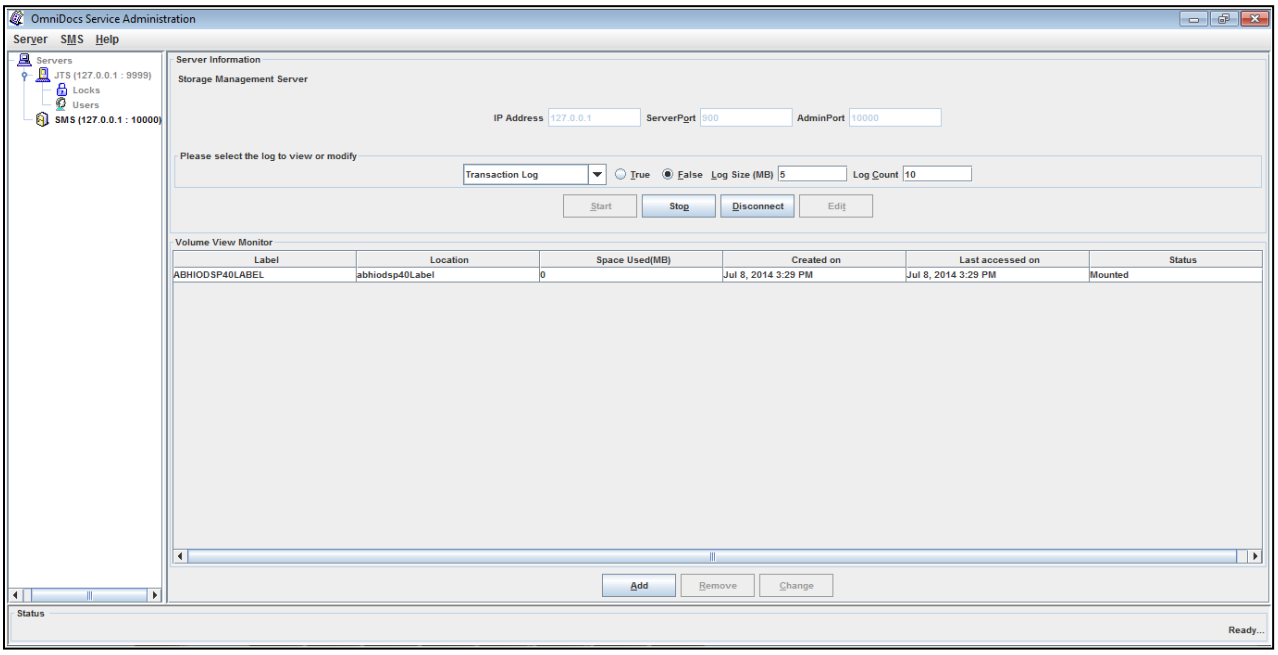


Figure 3.8

NOTE:

Once a server is managed, all the server operations can be performed on it.

3.1.4 SMS Server Operations

To perform operations on the SMS server

1. Click the **SMS** server from the **Servers** list.
2. Server information such as the **IP Address**, **Server Port**, and the **Admin Port** are displayed.

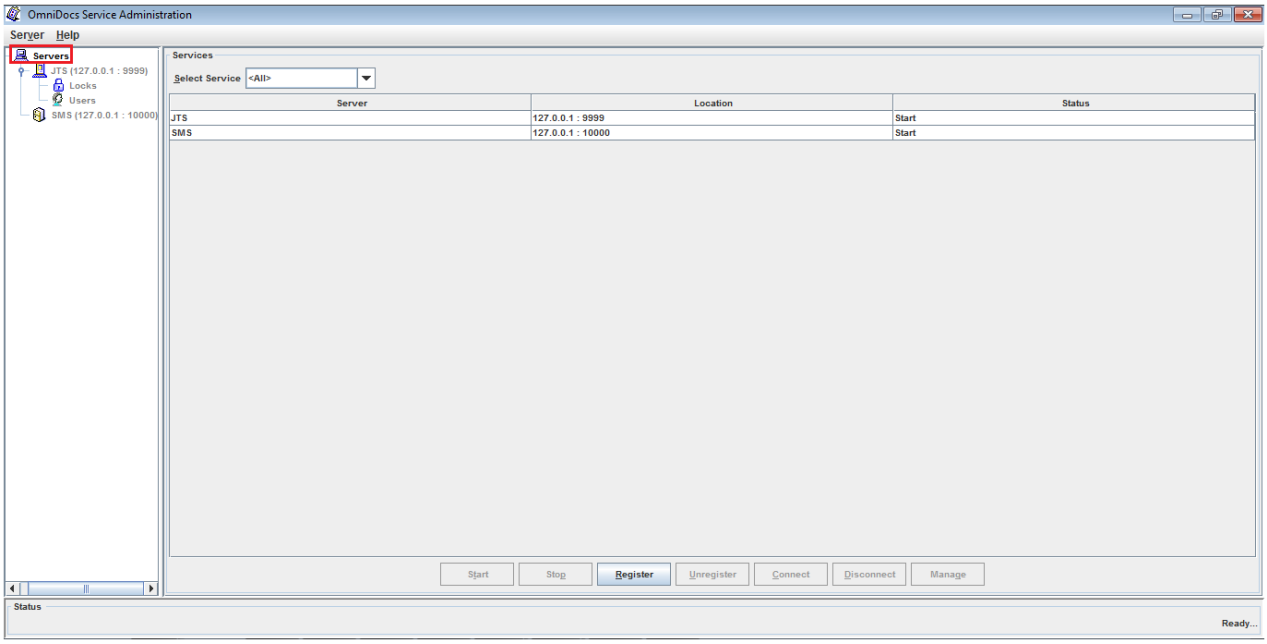


Figure 3.9

3. Select the **SMS** server from the list of servers in the Repository view.
4. If you wish to stop SMS server operations then click the **Stop** button to stop the server.

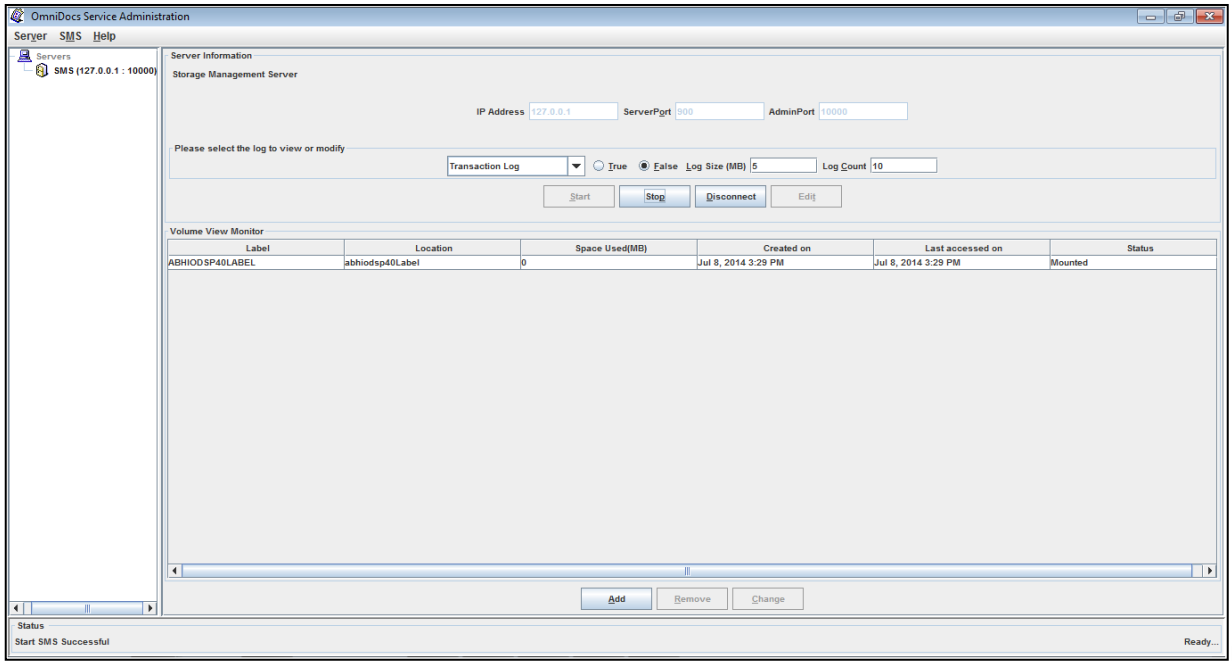


Figure 3.10

NOTE:

Once the server is stopped, Start, Remove and Change buttons gets enabled.

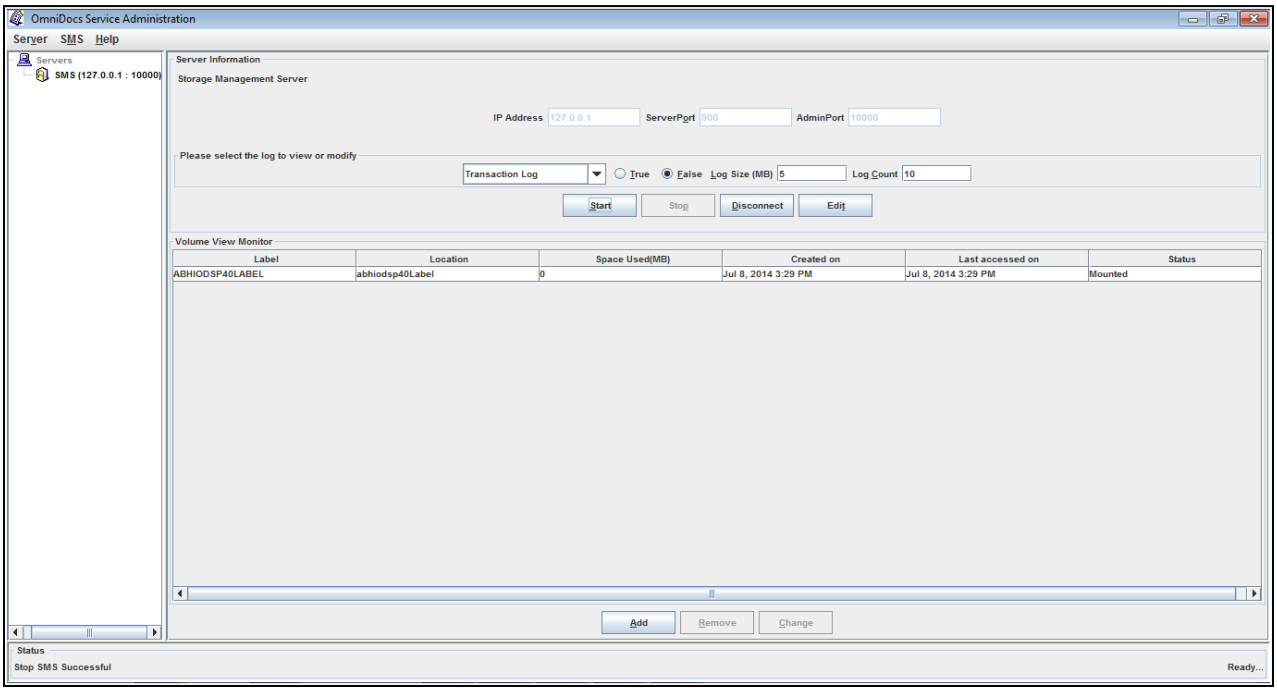


Figure 3.11

5. Click the **Disconnect** button to disconnect directly from the SMS.
6. A **Confirm** message box is invoked prompting whether, or not, you wish to disconnect from the SMS server.

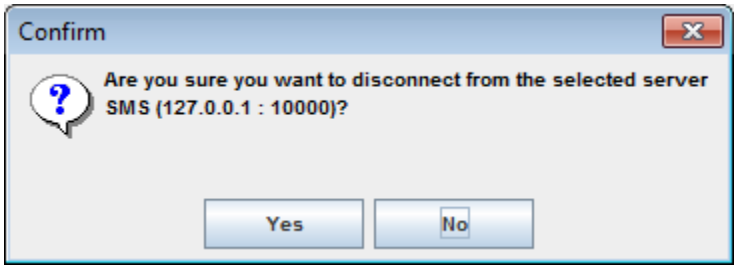


Figure 3.12

- Click **Yes** button to disconnect from the connected server. Or,
- Click **No** button to stop the disconnection process.

7. Click **Edit** to edit the **SMS Port**.

NOTE:

The Edit button is a toggle button, which changes to Update.

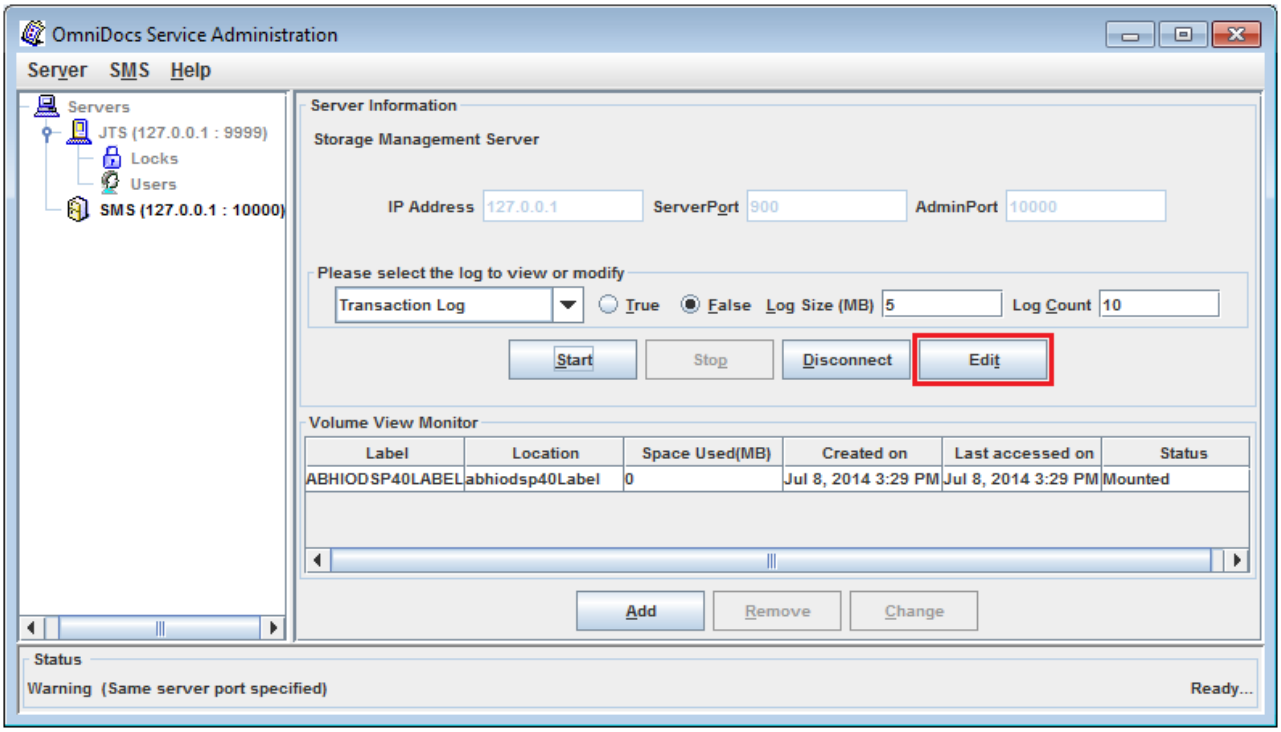


Figure 3.13

8. Make the required changes and click **Update**. A screen with updated information appears.

NOTE:

Clicking on Update updates the server port.

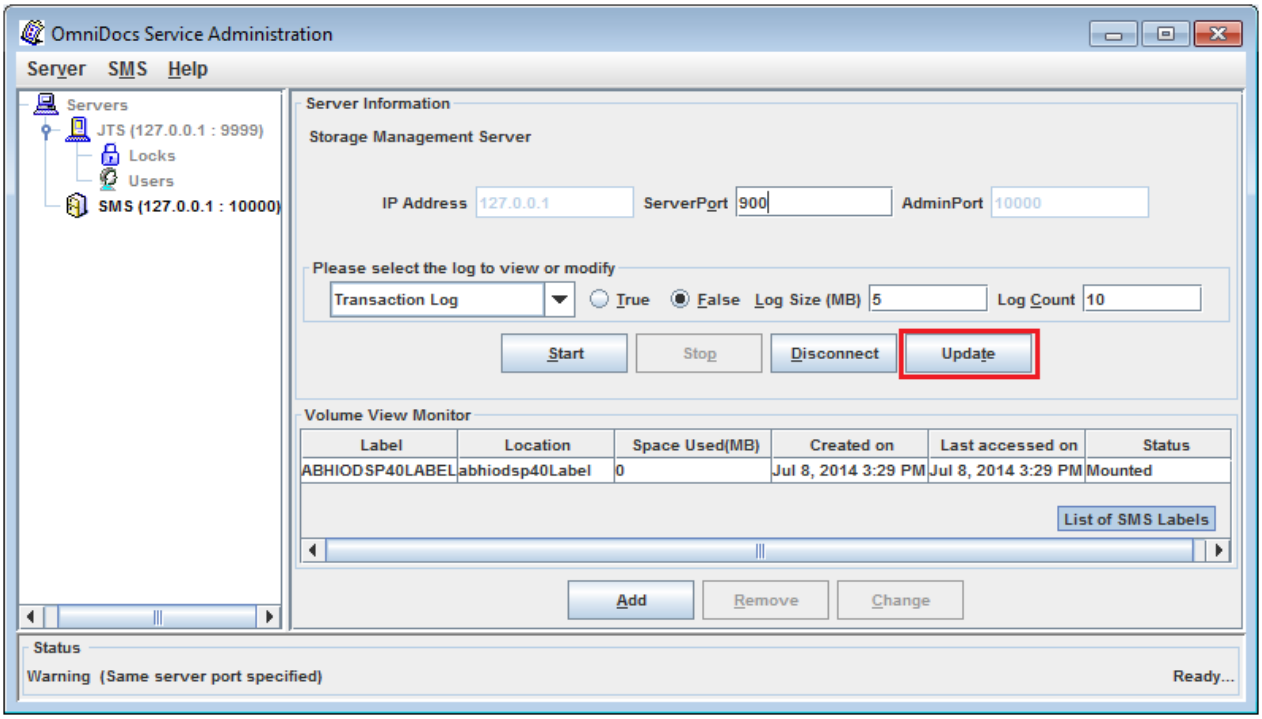


Figure 3.14

NOTE:

The status **Mounted** implies that the selected label exists on the specified directory path of the hard disk.

3.1.5 Adding Label

To add a label:

1. Visit the Server Information page.

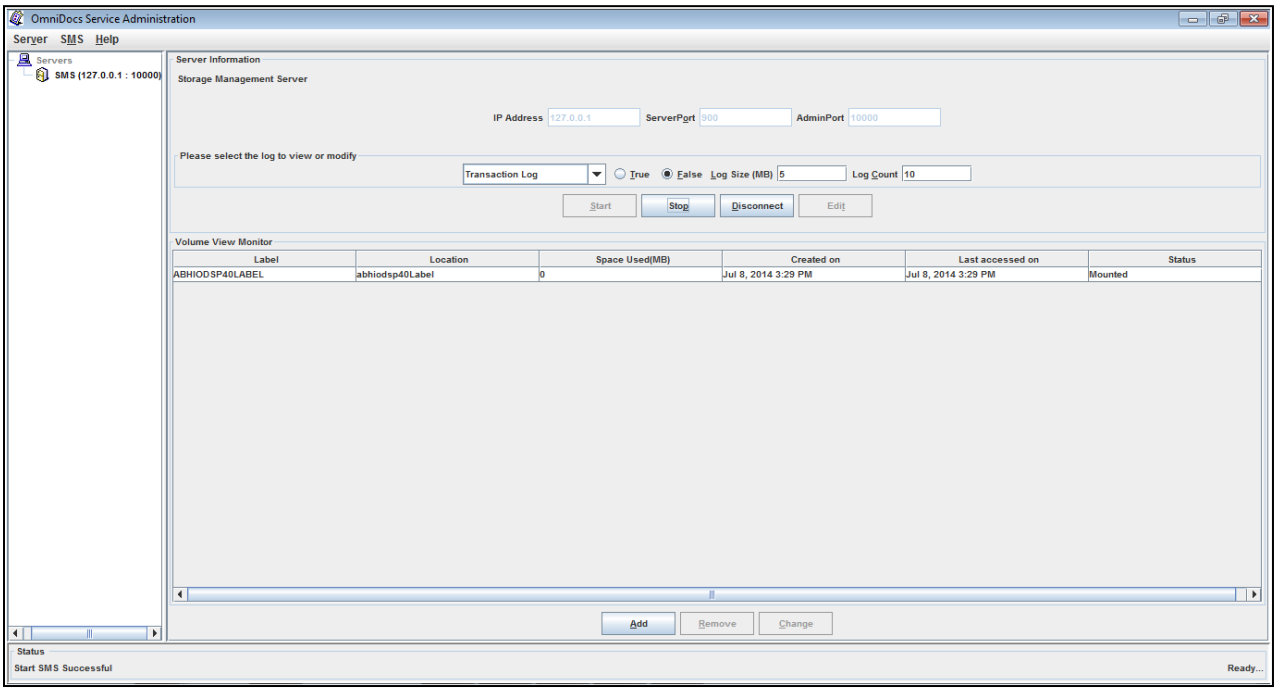


Figure 3.15

2. Click the **Add** button.
3. The **Add a Label** dialog box is invoked.

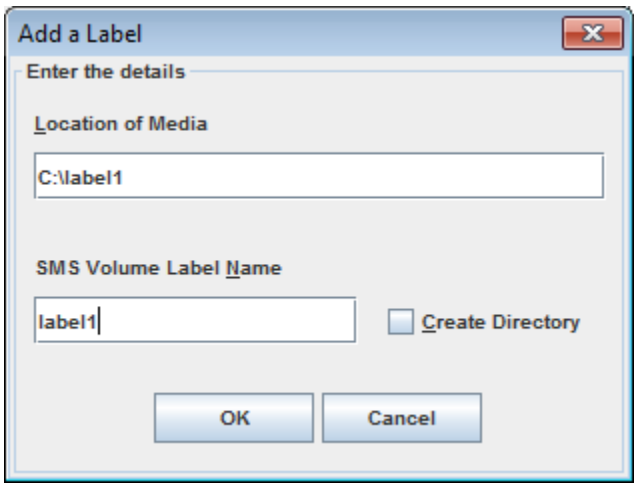


Figure 3.16

4. Specify the location where the label has to be created in the **Location of Media** textbox.

5. Specify the name of the label in the **SMS Volume Label Name** textbox.
6. Select the option **Create Directory** to create the directory in the specified location.
7. Click the **OK** button to create the label at the specified location.
8. Or, Click the **Cancel** button to close the **Add a Label** dialog box.

NOTE:

If there exists no path as that specified in the **Location of Media** and the **Create Directory** option is not checked then the specified label is not created.

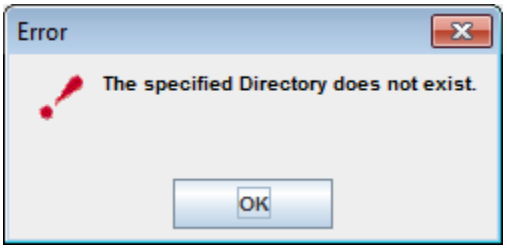


Figure 3.17

3.1.6 Removing Label

To remove the label:

1. Visit the Server Information page.

NOTE:

To enable the option of "Remove" & "Change" stop the SMS server from OSA.

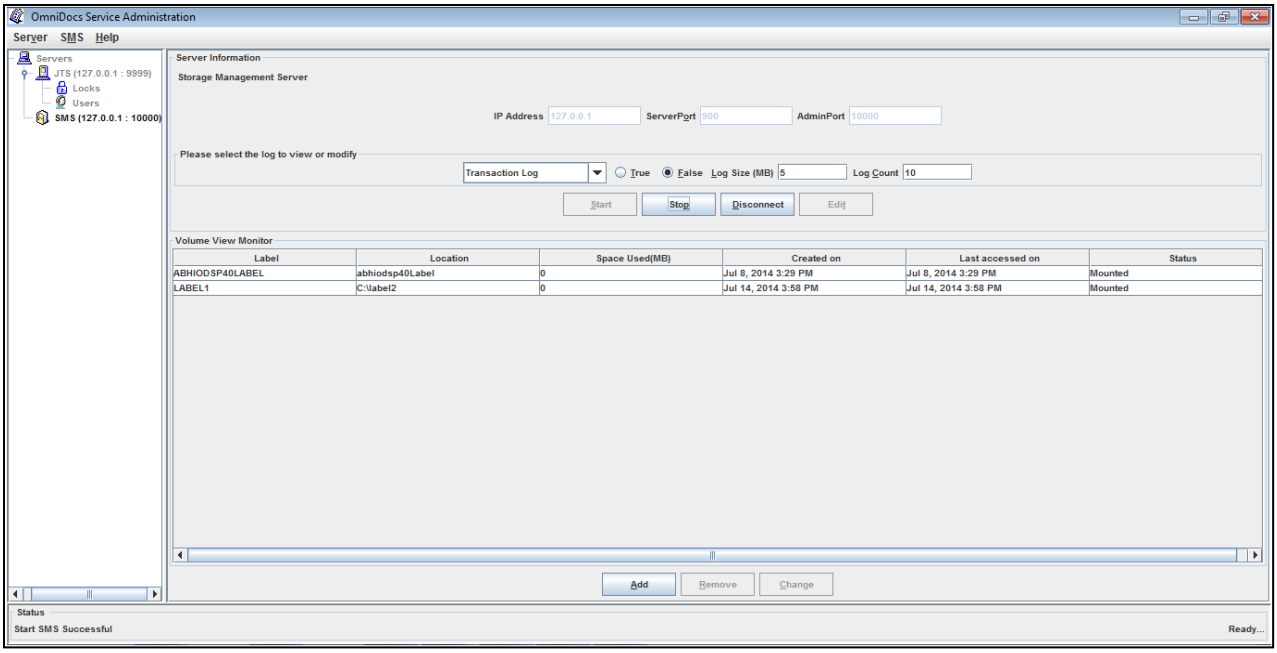


Figure 3.18

2. Select the label that needs to be removed from the list.
3. If the label is running, click **Stop**, to stop the label.
4. Click **Remove** button.

NOTE:

A message box is promptings you to confirm whether you want to remove the selected label from the list.

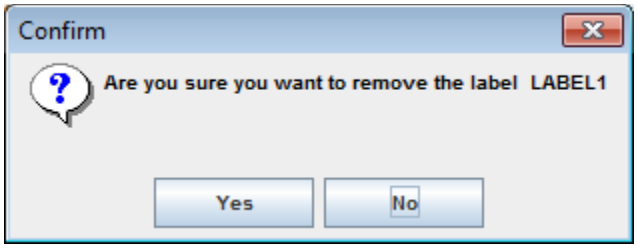


Figure 3.19

5. Click **Yes** button to remove the selected label from the list.
6. Click **No** button to avoid removing the selected label from the list.

3.1.7 Changing the Label

To change the label:

1. Visit the Server Information page.

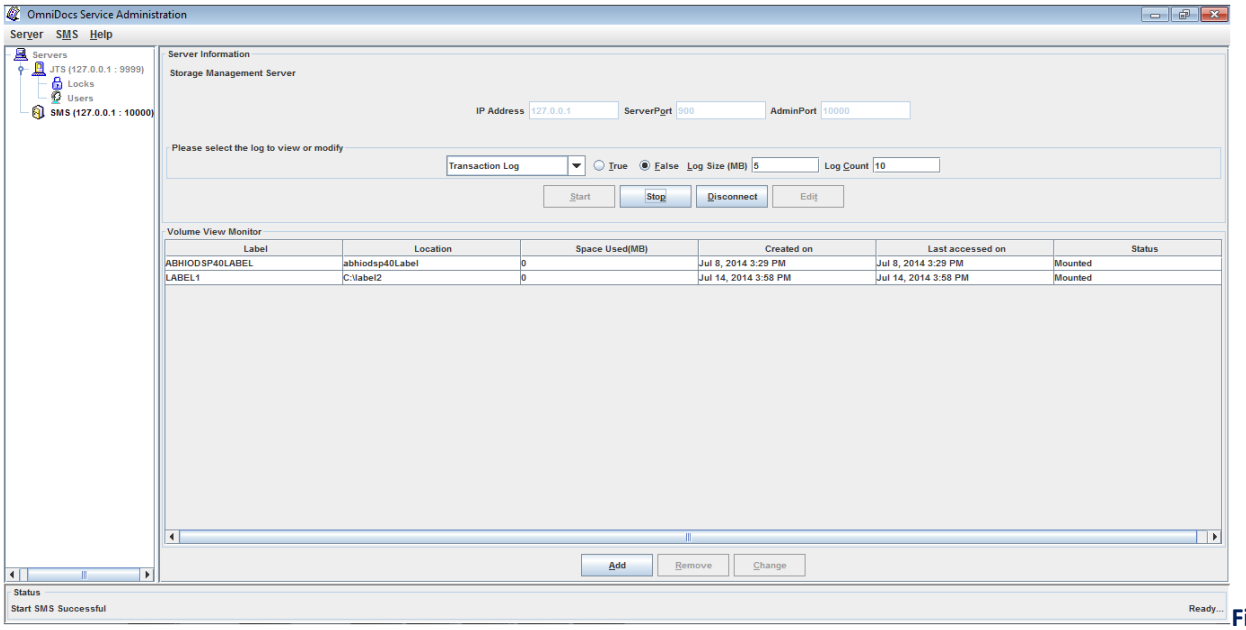


Figure 3.20

2. Select the required label, which needs to be changed from the list.

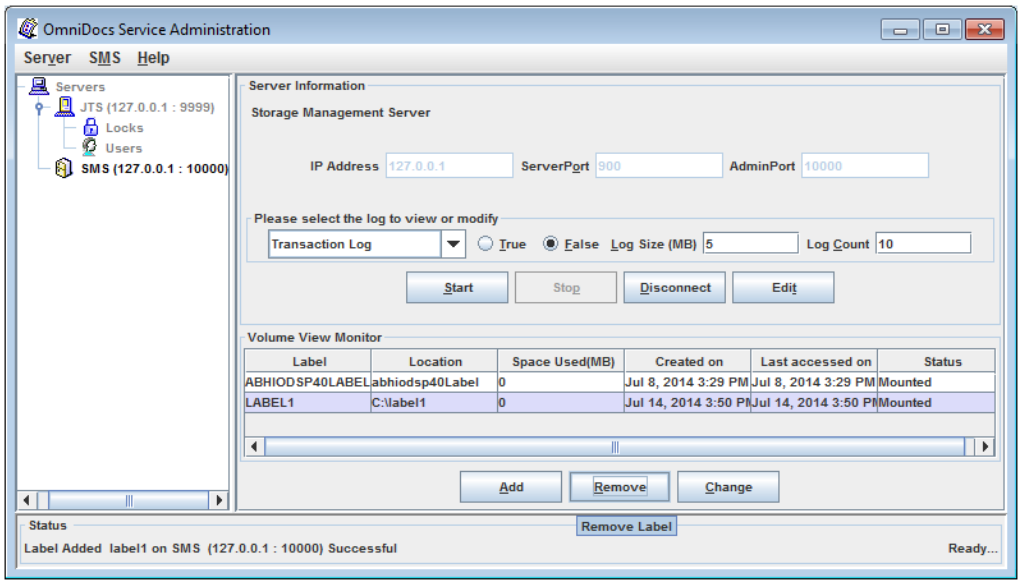


Figure 3.21

3. If the label is running, then click **Stop**.
4. Click the **Change** button. Set Label Property dialog box is invoked.

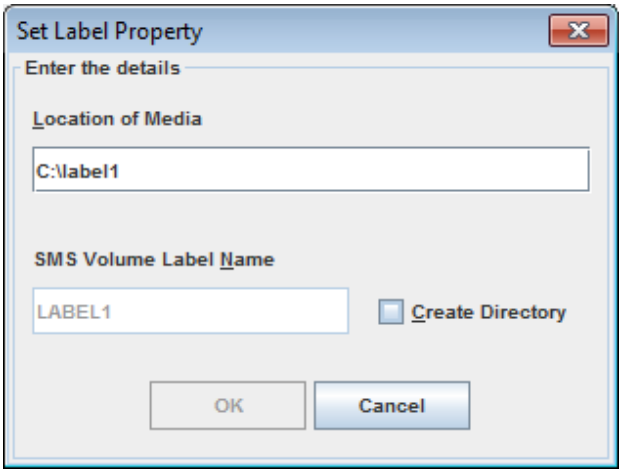


Figure 3.22

5. The only editable mode is the **Location of Media**, which displays the location where the specific label is located.
6. If you wish to change the path of the location of media, you do so by typing the path name in the **Location of Media** textbox.
7. Click the **OK** button to close the **Set Label Property** dialog box and to save the changes made. The following Confirm dialog box is evoked.
8. Click **Yes** to confirm, else, click **No**.

NOTE:

Click the **Cancel** button to quit from changing the label.

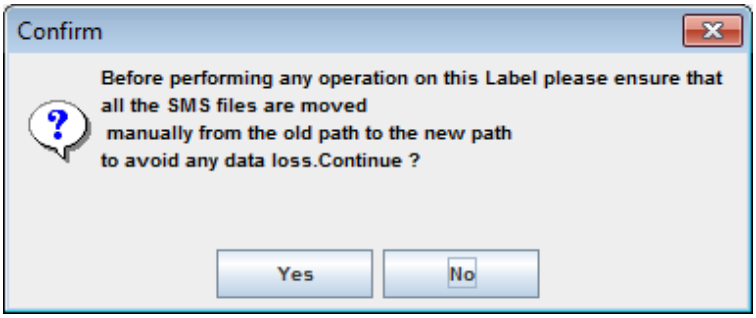


Figure 3.23

3.2 JTS Server Operations

To start operations on the JTS server

1. Select the **JTS** option from the **Select Service** dropdown list.
2. A list of all registered JTS servers is displayed.

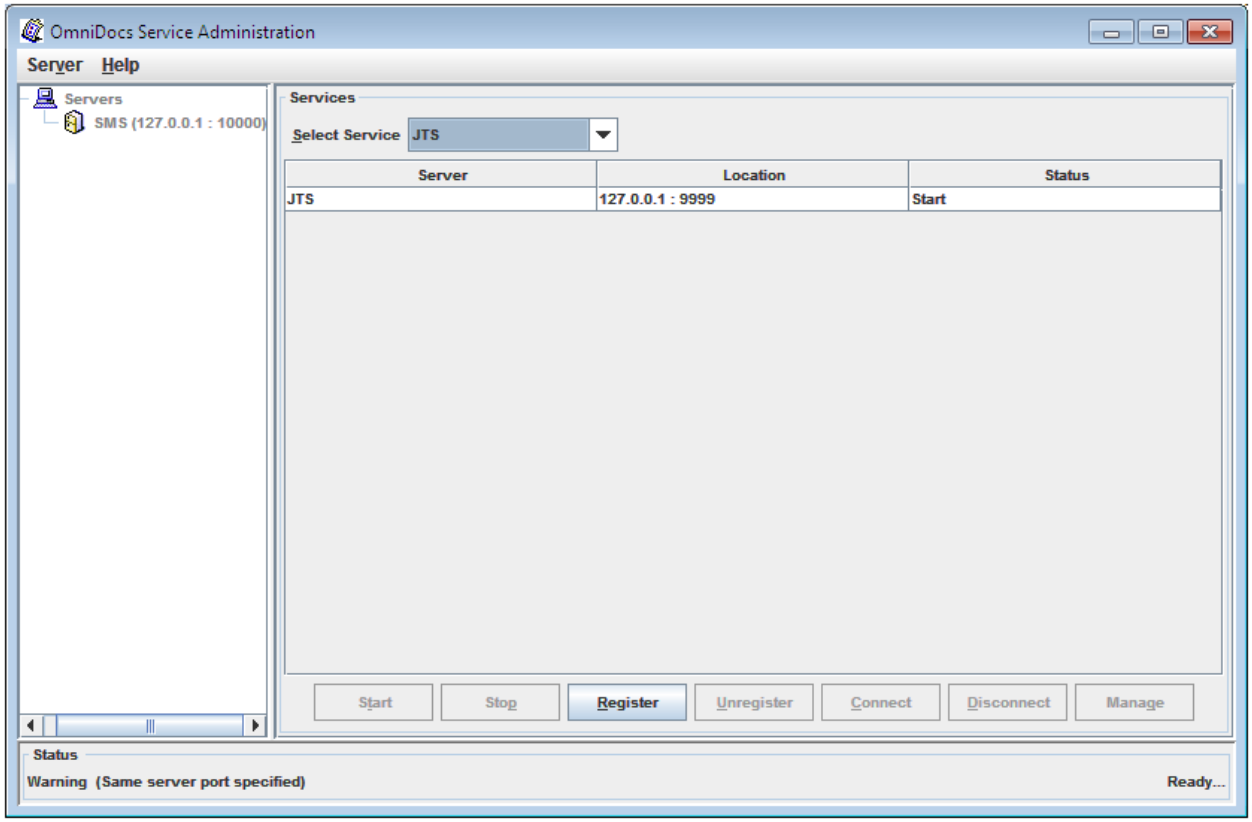


Figure 3.24

3.2.1 Registering JTS server

To register the JTS server

1. Click the **Register** button.
2. The **Register** dialog box is invoked.

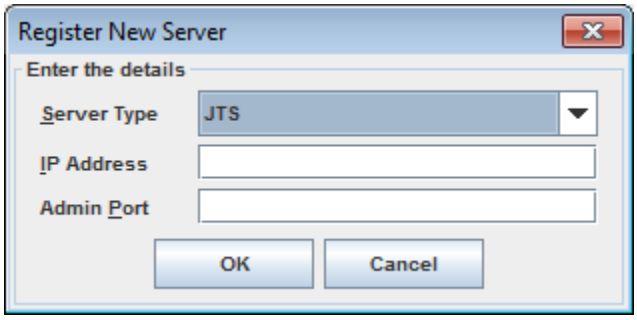


Figure 3.25

3. Enter IP Address and Admin Port Details.
4. Click **OK** to register, else click **Cancel**.

NOTE:

Once the server is registered it is displayed in the list and is in a disconnected state.

3.2.2 Connecting OSA to JTS

To connect the JTS server:

1. Select the server that needs to be connected from the servers displayed on the list.

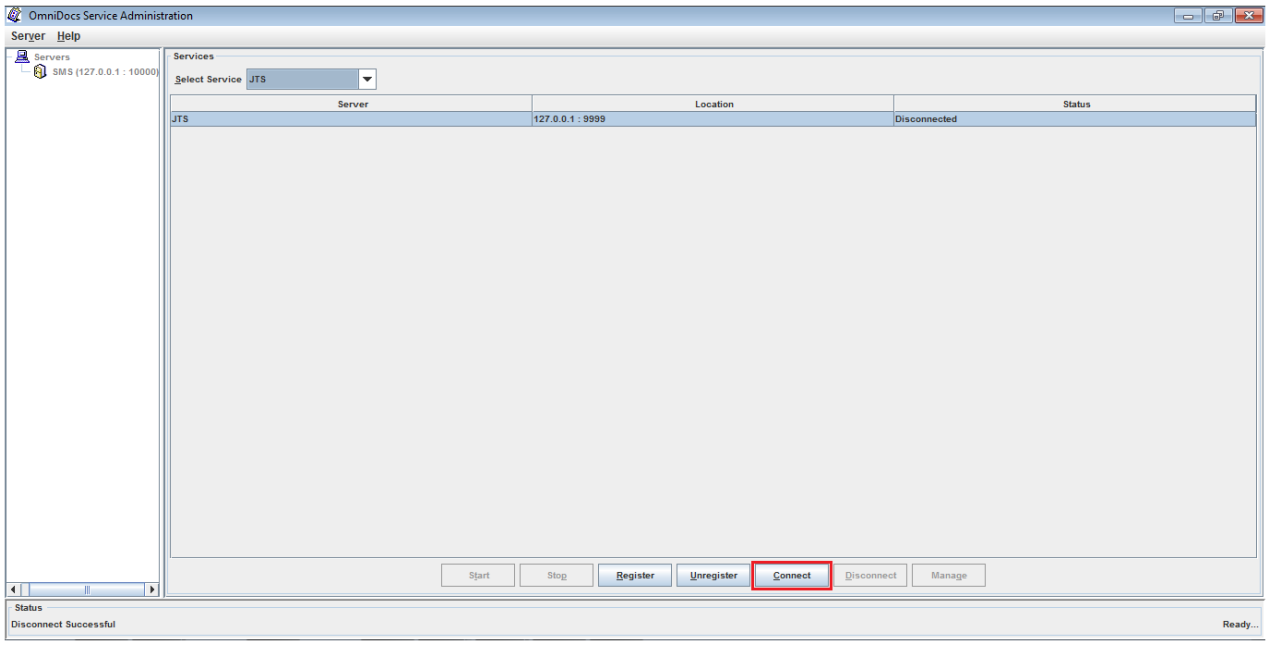


Figure 3.26

2. Click the **Connect** button. OSA gets connected with the JTS.

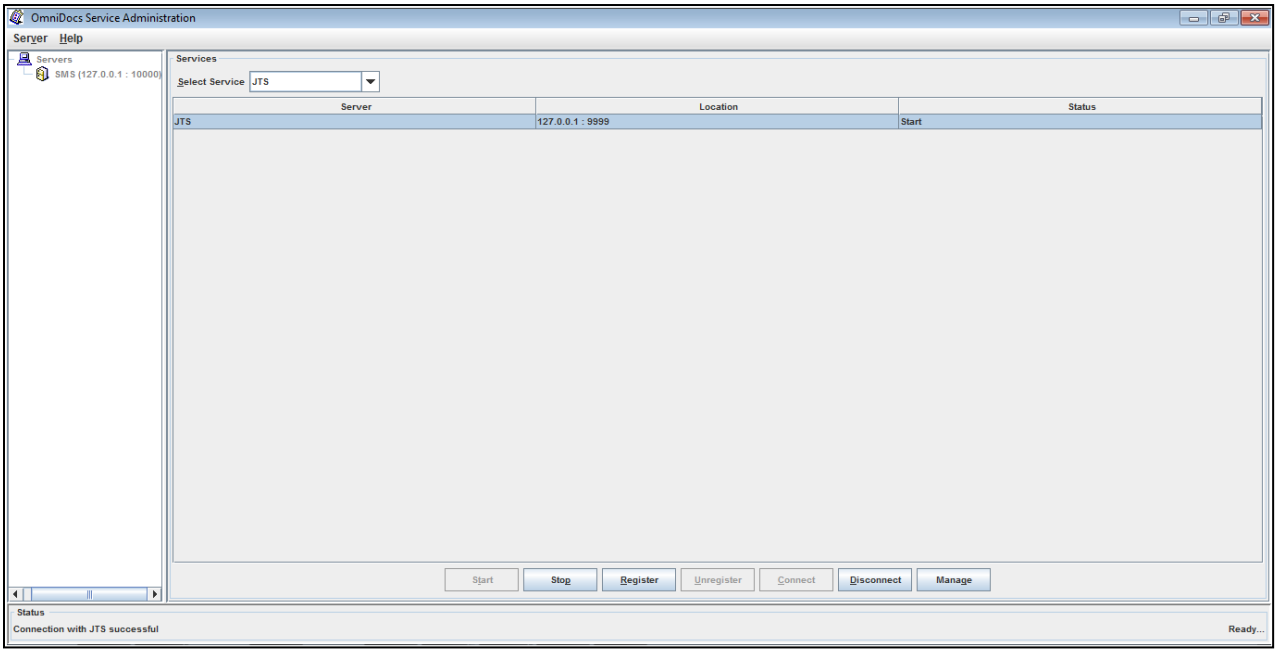


Figure 3.27

3.2.3 Managing JTS

Only when the JTS is managed, all the server operations (other than Start and Stop) can be performed on it. To manage the connected server:

1. Select the connected server from the list of registered servers.
2. Click the **Manage** button.

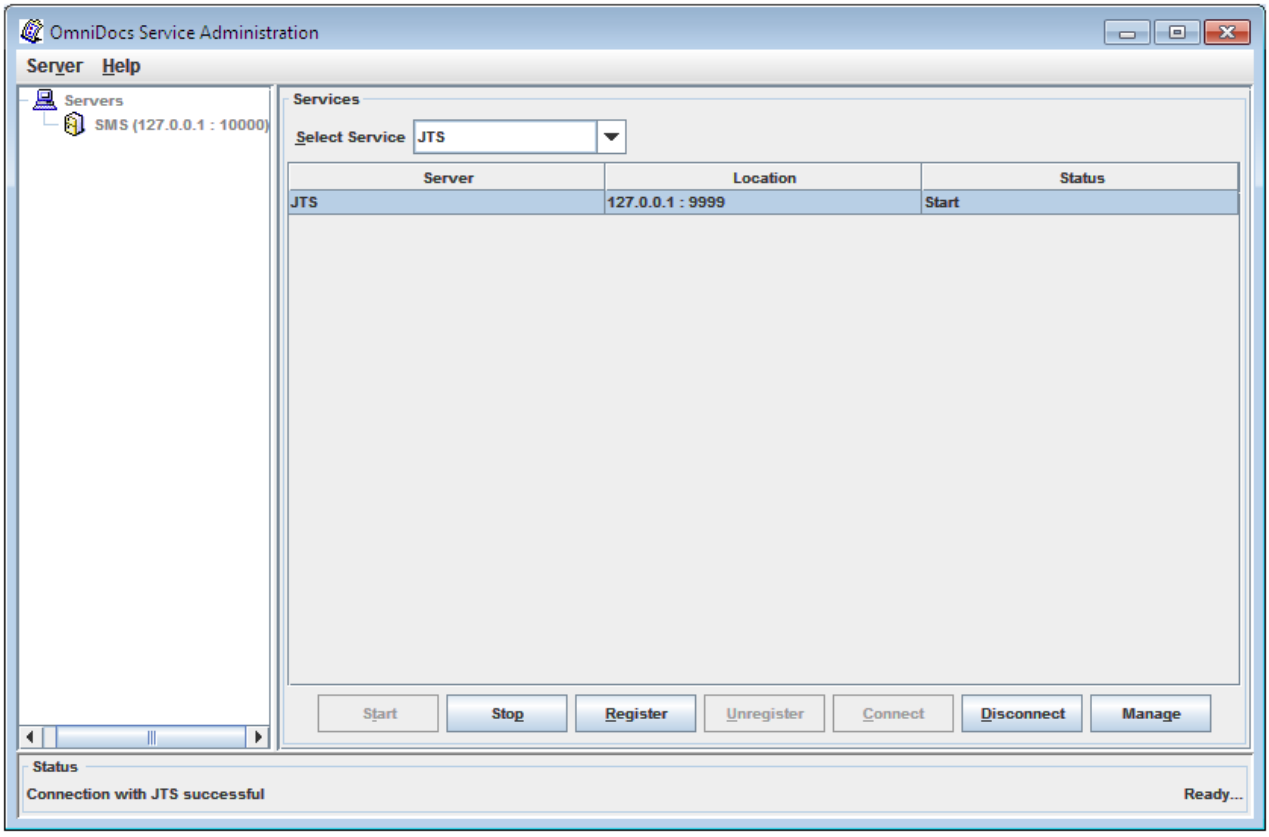


Figure 3.28

3. An entry of the connected server along with its IP Address is displayed in the **Servers** tree in the repository view.

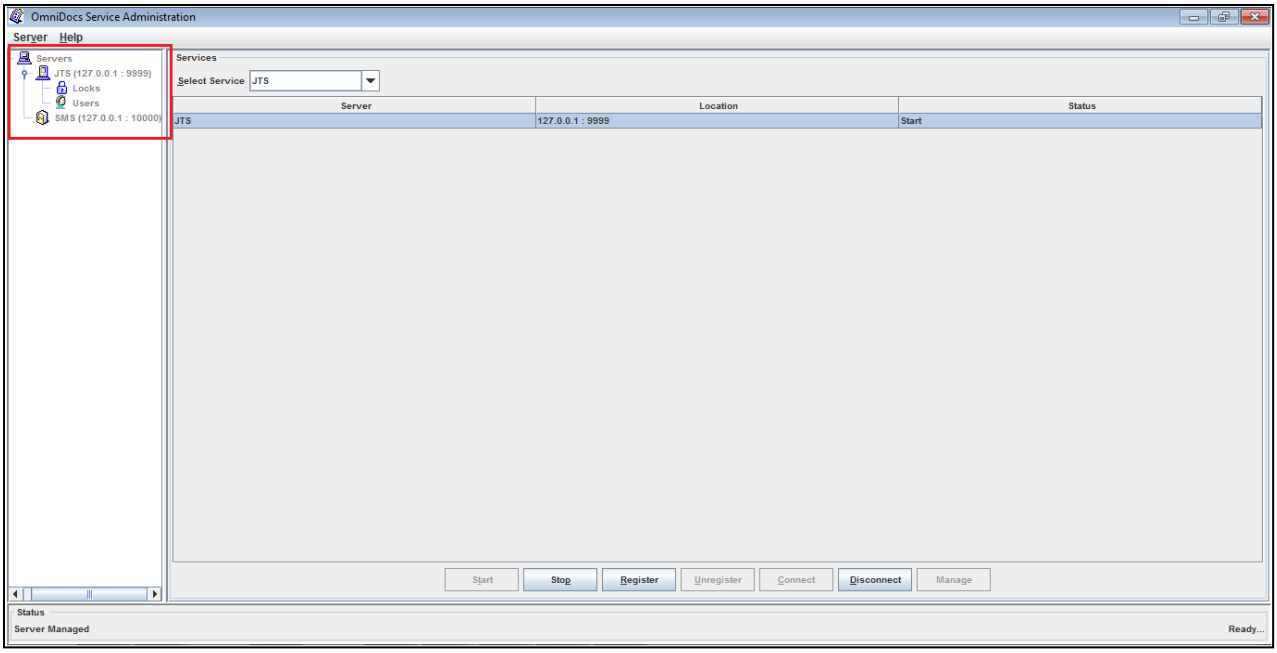


Figure 3.29

4. Select the **JTS** from the repository view.
5. The following screen is invoked displaying the JTS server information.

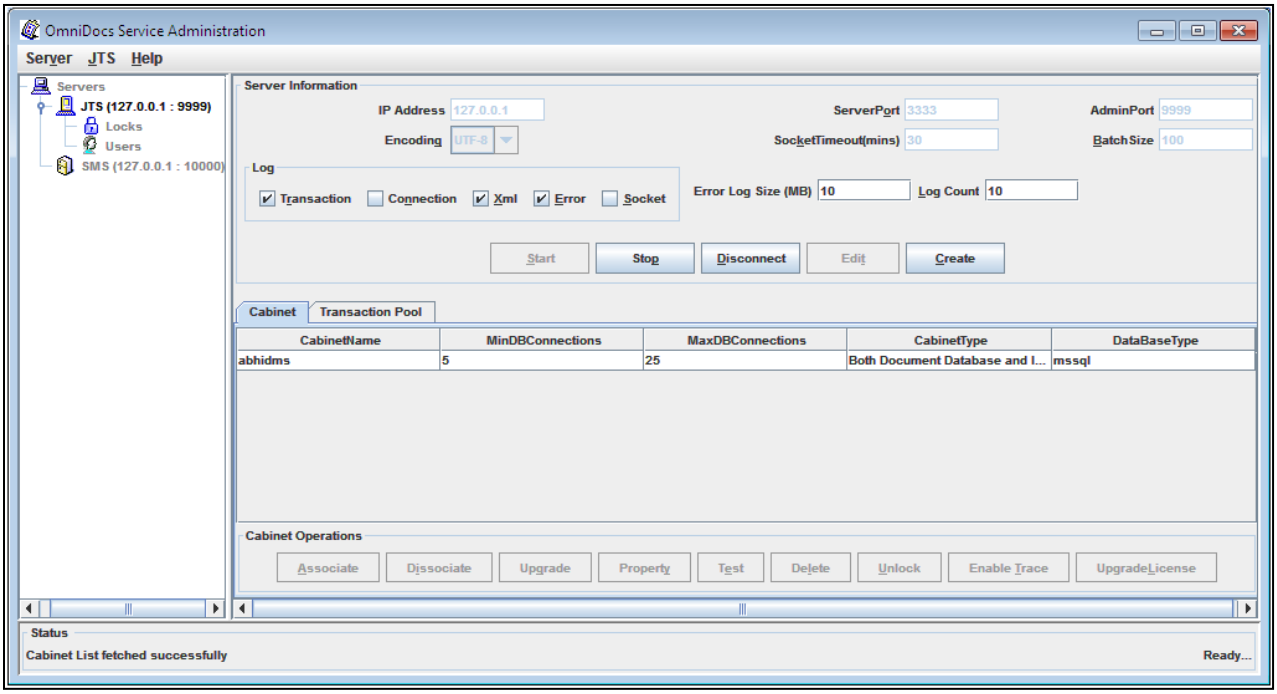


Figure 3.30

Server Port	Server Port signifies the port at which the JTS would listen to the OmniDocs client's request.
Socket Timeout	Socket Timeout signifies the time after which the OmniDocs Client would be timed out.
Batch Size	Batch Size signifies the maximum number of records that have to be fetched for a request.

3.2.4 Editing JTS Properties

To edit the properties of the JTS server:

1. Select the Server.
2. Click **Stop**.
3. Click **Edit**.

NOTE:

Edit is a toggle button and changes to Update.

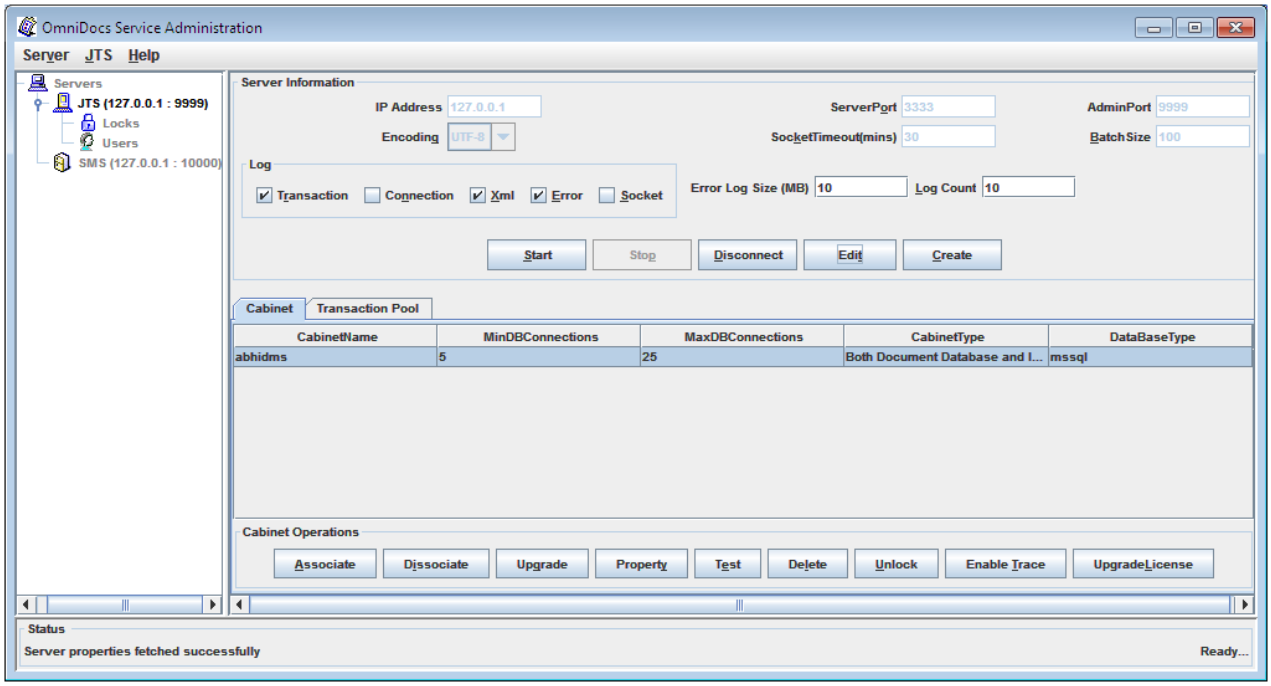


Figure 3.31

The editable modes are:

Server Port	Enter the Server Port Number of the System.
Transaction log	Select this checkbox to generate the Transaction Log.
Connection log	Select this checkbox to generate Connection Log.
Batch Size	The system takes the entered value and crates a batch of that size.
SocketTimeout (mins)	Enter the SocketTimeout Duration in minutes.
Error Log Size (MB)	The system takes the entered value and creates an error log of that size.
Log Count	The system takes the entered value and creates error logs equal to the count.
XML Log	Select this checkbox to generate XML log.
Error Log	Select this checkbox to generate an error log.
Socket Log	Select this checkbox to generate a Socket log.

4. Make the changes as per the requirement.

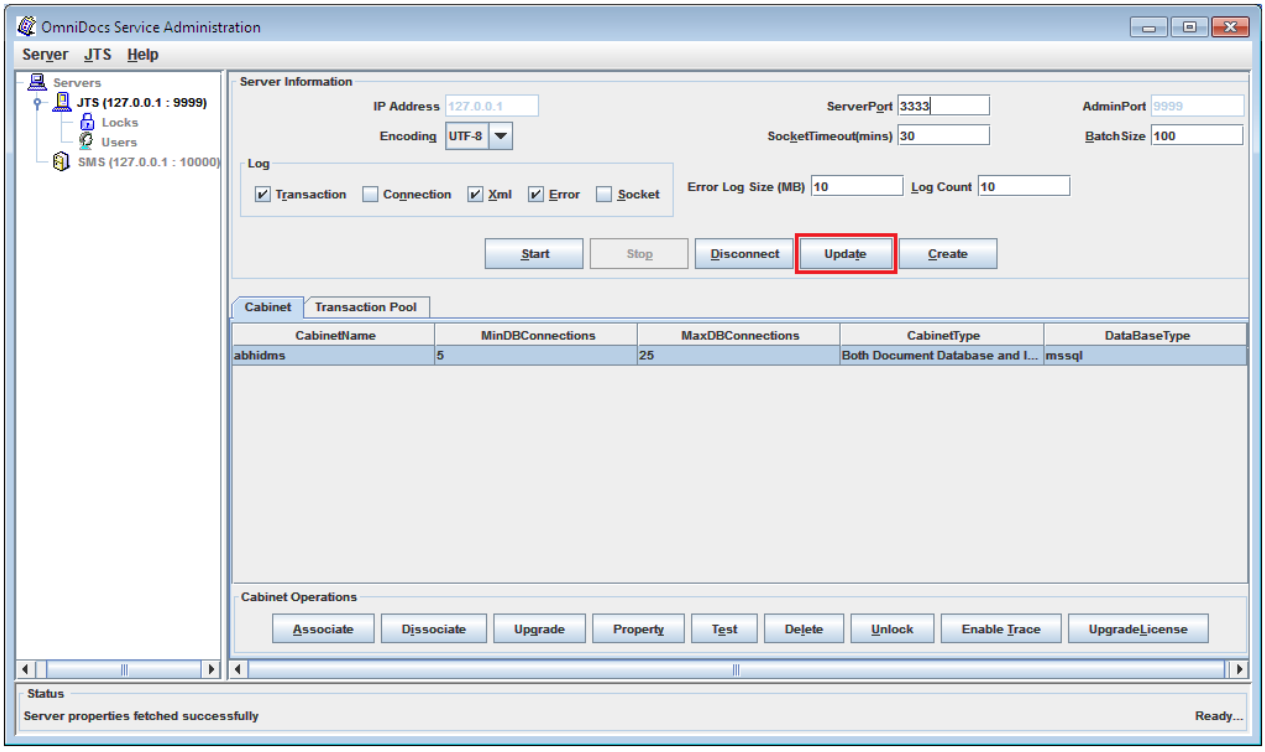


Figure 3.32

5. Click the **Update** button to save the changes made.

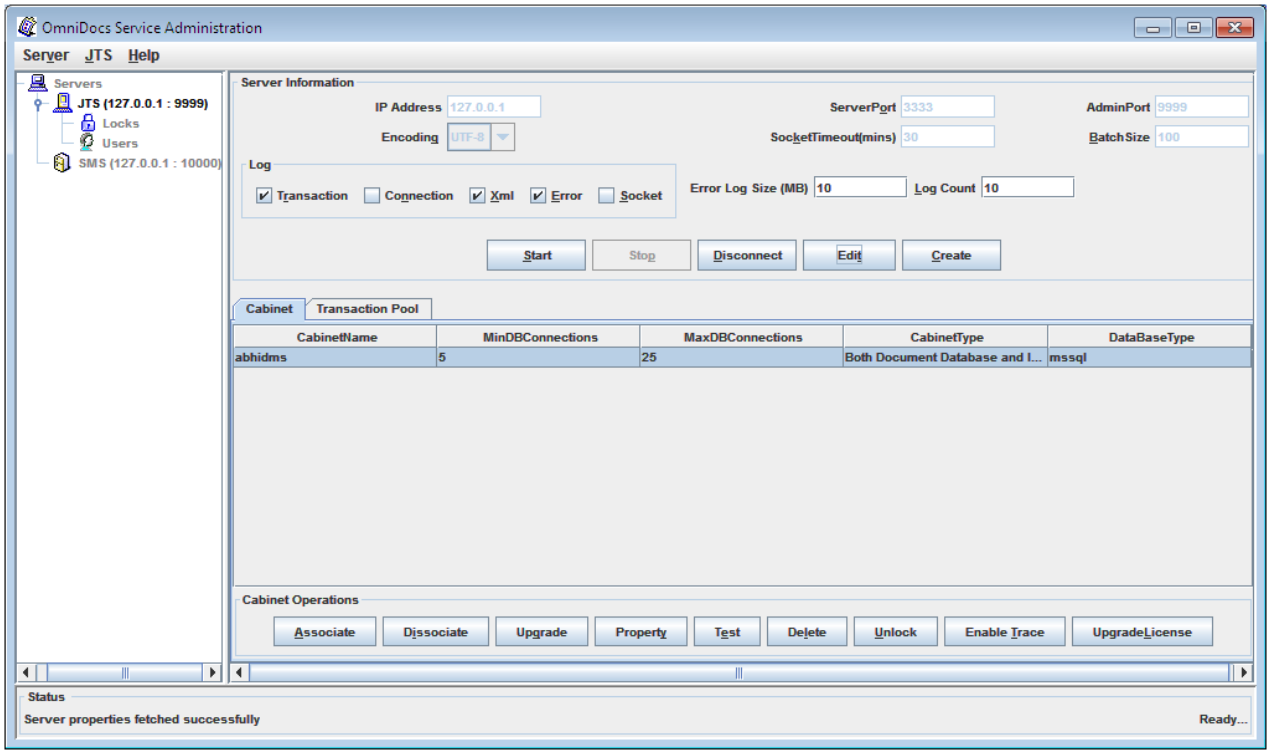


Figure 3.33

OmniDocs provides the following features:

- Option to generate XML log files.
- Enable or Disable Trace option.
- Manipulate the value of Error Log Size.
- Unlock button on the JTS properties screen of the OmniDocs Service Administration (OSA).

These features help to:

- Optimize the function of OSA.
- Rectifying errors in operations.
- Reduce time in identifying the properties.
- Increase the speed of processing tasks using the OmniDocs server.

There are various features which when added to the JTS properties screen of the OSA in OmniDocs, helps optimize and increase the speed of operations of the OmniDocs server. These features are:-

- Option to generate XML log files to record all the
- Error Log Size textbox to define the maximum size of

actions that you perform on the OmniDocs server

- Enable Trace or Disable Trace toggle button on the Cabinet Operations frame to generate trace files of all SQL statements run at the database

the error log file

- Unlock button on the Cabinet Operations frame to unlock a locked user account

The figure below shows the screen with new features added to the JTS properties screen of the OSA:

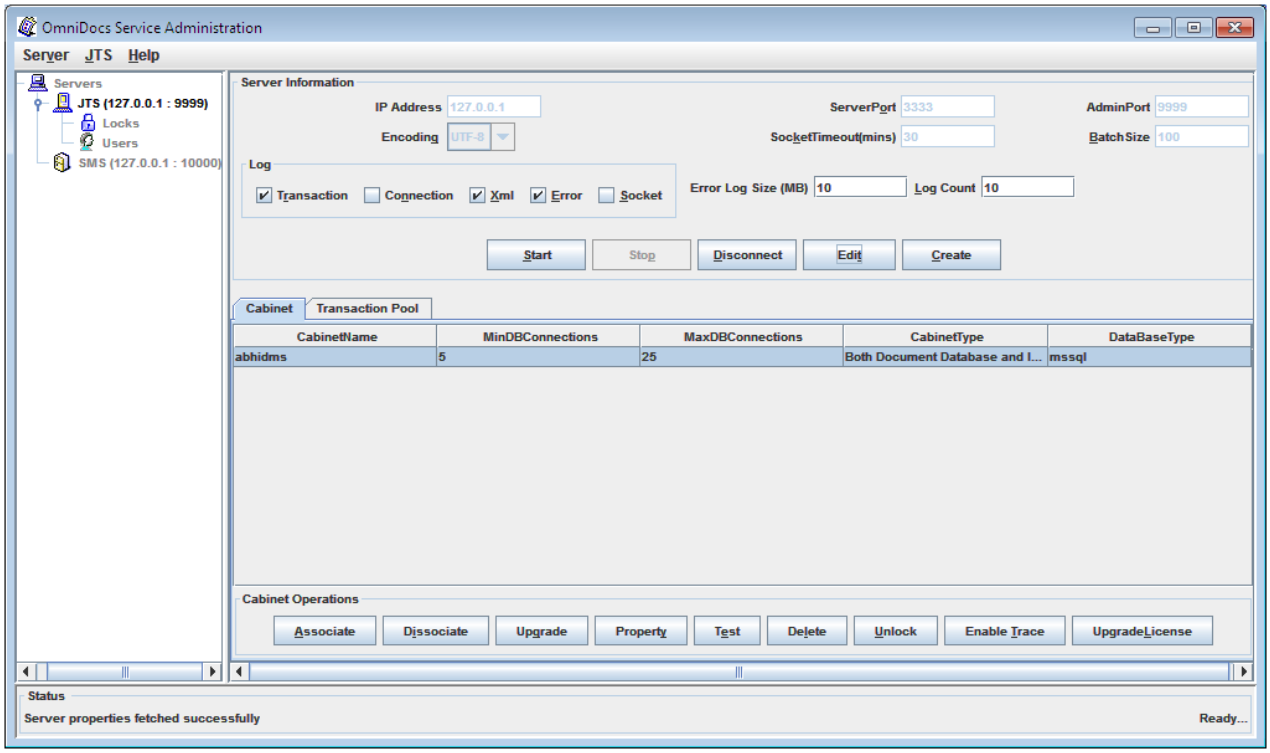


Figure 3.34

Generating XML Log Files

The Xml option on the Log frame of the JTS properties screen enables you to generate or prevent generating an XML log file named xml.log. The XML log file consists of code in the form of XML tags and maintains a record of all actions performed on the OmniDocs server. You need to set the value of the XML log file to 'true' to enable the generation of the XML log file.

You select the Xml option on the Log frame to generate the XML log file of all operations performed on the OmniDocs server. The record of all operations on the XML log file helps identify errors in an operation and rectify the errors which help reduce the time needed for errors identification and rectification. With the continuous generation of the logs of operations performed on the OmniDocs

server, the size of the log file increases, and the log file occupies more storage space. The generation of logs reduces the speed of operation of the server computer. You clear the Xml option on the Log frame to prevent the generation of logs of the operations performed on the server computer.

To generate XML logs of all operations performed on the server:

1. Select the Xml option on the Log frame of the JTS properties screen of the OSA.
2. The **Edit** button, which is a toggle button present on the lower section of the Server Information frame of the JTS properties screen and was unavailable, is made available.
3. The name of the **Edit** toggle button is changed to **Update** when the toggle button is made available. The figure below shows the Update toggle button on selecting the Xml option:

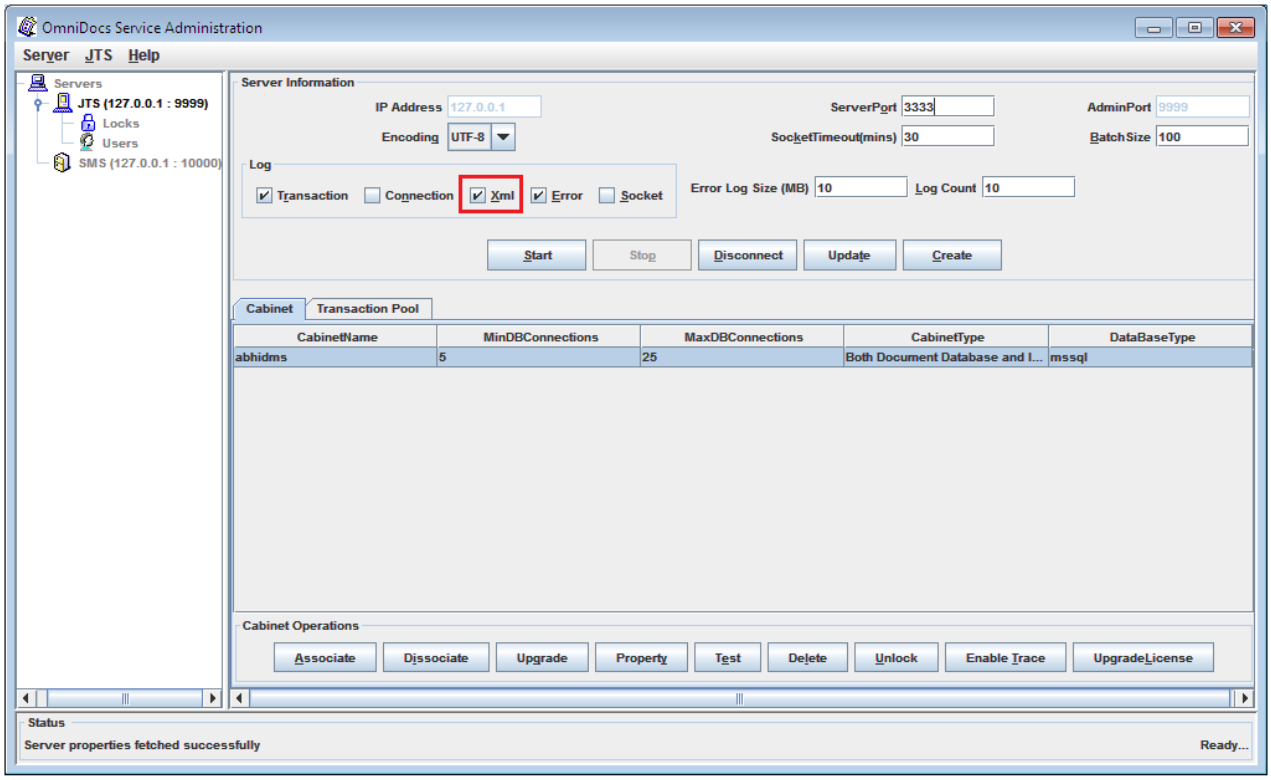


Figure 3.35

4. Click the **Update** button to save the changes made.
5. The Update toggle button changes to the Edit button and remains unavailable.

Steps to prevent generating XML logs of all operations performed on the server using the OSA:

1. Clear the Xml option on the Log frame of the JTS properties screen of the OSA.
2. The Edit toggle button, which was unavailable, changes to Update button and is made available.
3. Click the **Update** button to save the changes made.
4. The Update toggle button changes to the Edit button and remains unavailable.
5. The generating of XML logs of all operations performed on the server is terminated.

Defining Size of Error Log File

OmniDocs provides the Error Log Size textbox on the Server Information frame of the JTS Properties screen to enable you to type the maximum size of the error log file, err.log, present on the server computer. This helps to control the size of the error log file and prevents the err.log file from occupying more storage space of the CPU and increases the speed of operation of the server computer. If the size of the error log file increases, then defined on the Error Log Size textbox, the earlier error log records are deleted and replaced by current error log records to enable the error log file to remain within defined limits of size.

Steps to type or modify the size of the error.log file present on the server computer:

1. Enter the file size in **Error Log Size** textbox on the Server Information frame of the **JTS Properties** screen.
2. **Edit toggle** button, which was unavailable, changes to **Update** button and is made available.
3. The figure below shows the Update toggle button after you type the size of the error.log file:

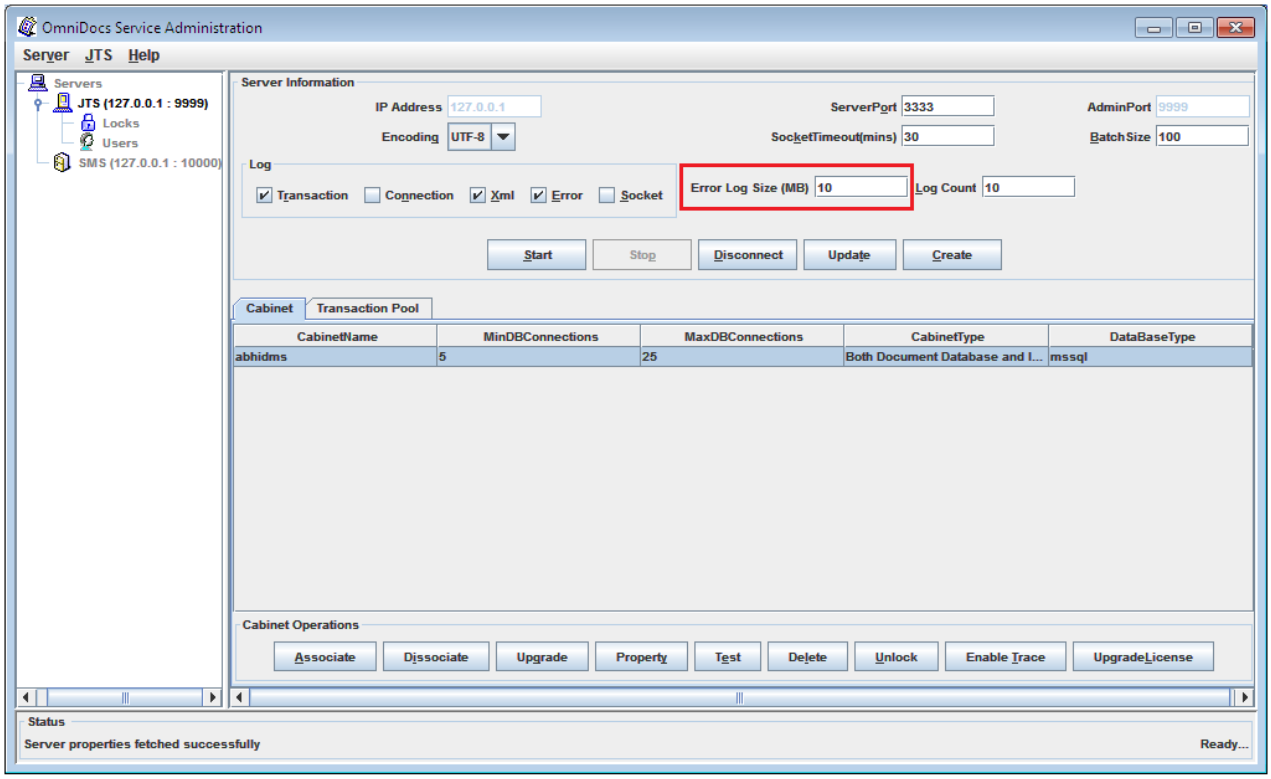


Figure 3.36

4. Click the **Update** button to save the changes made.
5. The Update toggle button changes to the Edit button and remains unavailable.

Generating Trace Files

OmniDocs provides Enable Trace or Disable Trace toggle button on the Cabinet Operations frame to generate a trace file with the extension .trc to maintain a record of all SQL statements run at the database for a cabinet. The trace file helps analyze the time needed to process a SQL statement and helps reduce the time for processing a SQL statement and optimizes the processing speed of the server computer.

Steps to generate a trace file for a cabinet:

1. Select a cabinet from the list of cabinets shown on the Cabinet tab of the JTS Properties screen.
2. **Disable Trace** toggle button, which is unavailable changes to **Enable Trace** button and is made available.

3. The figure below shows the Enable Trace button after selecting a cabinet:

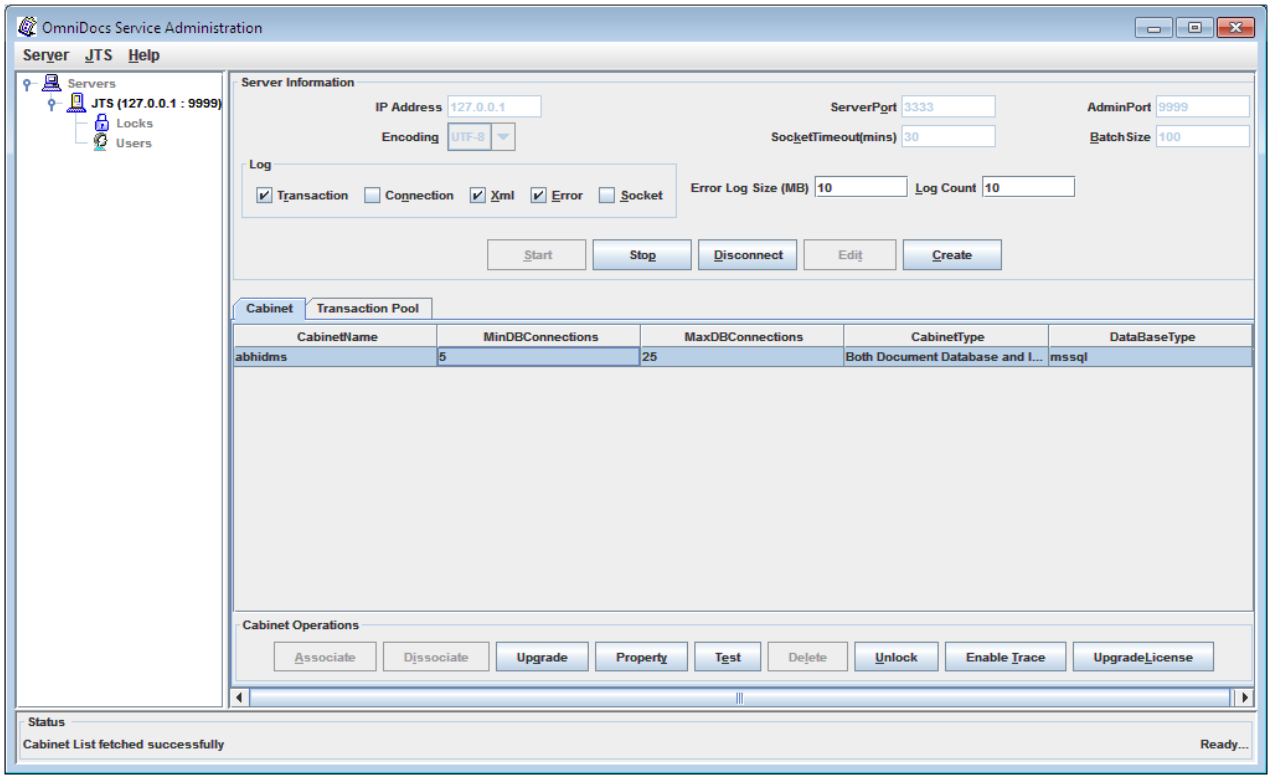


Figure 3.37

4. Click **Enable Trace** toggle button to generate trace files for the cabinet that you select on the Cabinet tab.
5. Enable Trace toggle button changes to the Disable trace toggle button and remains available.

The continuous generating of trace files for cabinets that you select from the cabinets listed on the Cabinet tab occupies more memory and CPU spaces and reduces the speed of processing SQL statements on the server.

Steps to prevent generating of trace files for cabinets that you selected from the list on the Cabinet tab:

1. Click the **Disable Trace** button available state.
2. The Disable Trace button is made unavailable.

Using Unlock Button to Unlock a Locked User Account

OmniDocs provides the Unlock button on the Cabinet Operations frame of the JTS Properties screen to enable you to unlock a locked user account. You use the Unlock button of the OSA to unlock a locked account for the Supervisor. The Supervisor can unlock all other locked user accounts.

To unlock a locked user account:

1. Click the name of the cabinet shown on the list of cabinets on the Cabinet Tab of the JTS Properties screen of the OSA.
2. The Unlock button, which was unavailable, is made available.
3. Click the **Unlock** button.
4. The **Unlock User** dialog box appears.

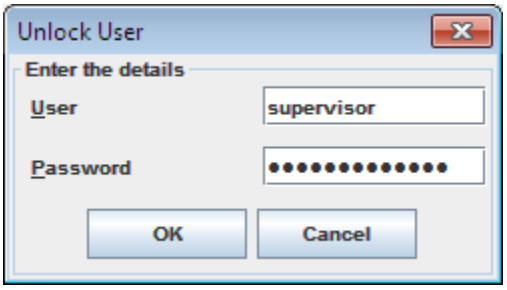


Figure 3.38

5. Type the user name and the password of the user account that is locked.
6. Click **OK** to unlock the user account, else click **Cancel** to exit from the Unlock User dialog box.

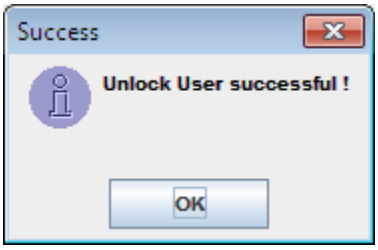


Figure 3.39

3.2.5 Creating a Cabinet

Cabinet Creation can be done in two ways:

- By using Superuser like ‘sa’ (SQL) or ‘sys’ (Oracle).
- By using a normal user with cabinet creation rights.

To create a cabinet using Superuser:

1. Click **Create** button.
2. **Create Cabinet** dialog box is invoked.

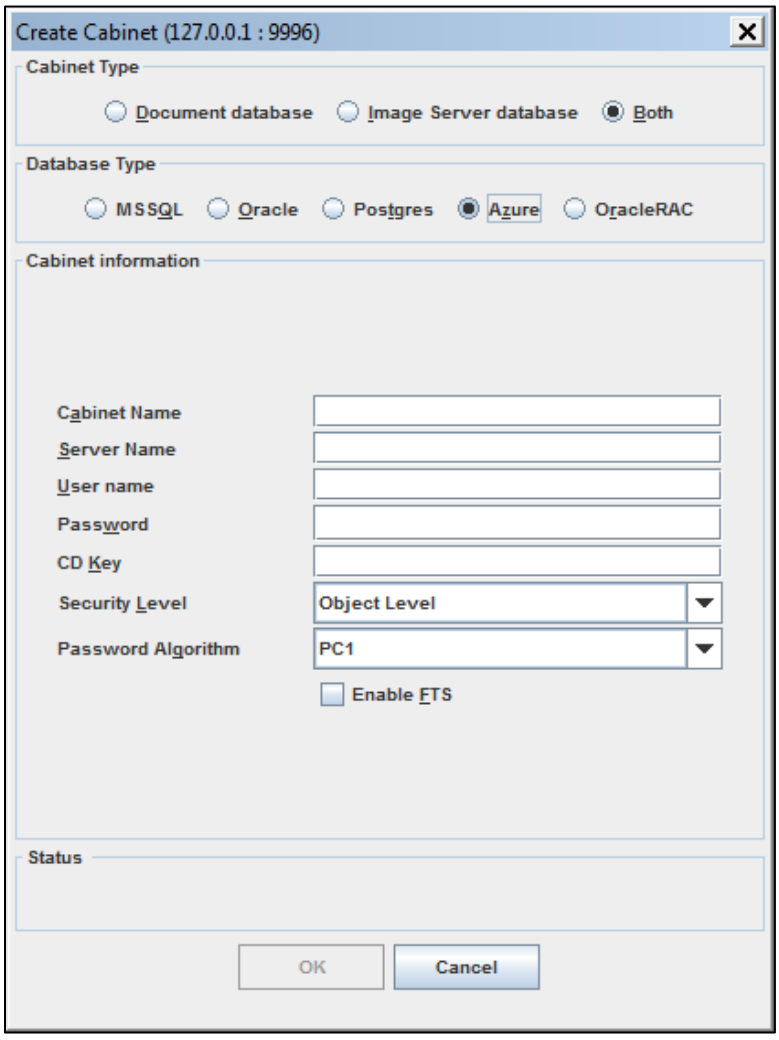


Figure 3.40

3. Select the cabinet type that needs to be created from the Cabinet Type area.

4. The Cabinet can be a **Document database**, **an Image server database,** or both.
5. Select the required **Database Type** from the options available in the Database Type area.
6. The types of databases available are **MSSQL**, **Oracle**, **PostgreSQL,** and **Azure**.

3.2.6 Creating an MSSQL Database Cabinet

Using Superuser

To create an MSSQL database cabinet:

1. Select the **MSSQL** database option from the **Database Type**.

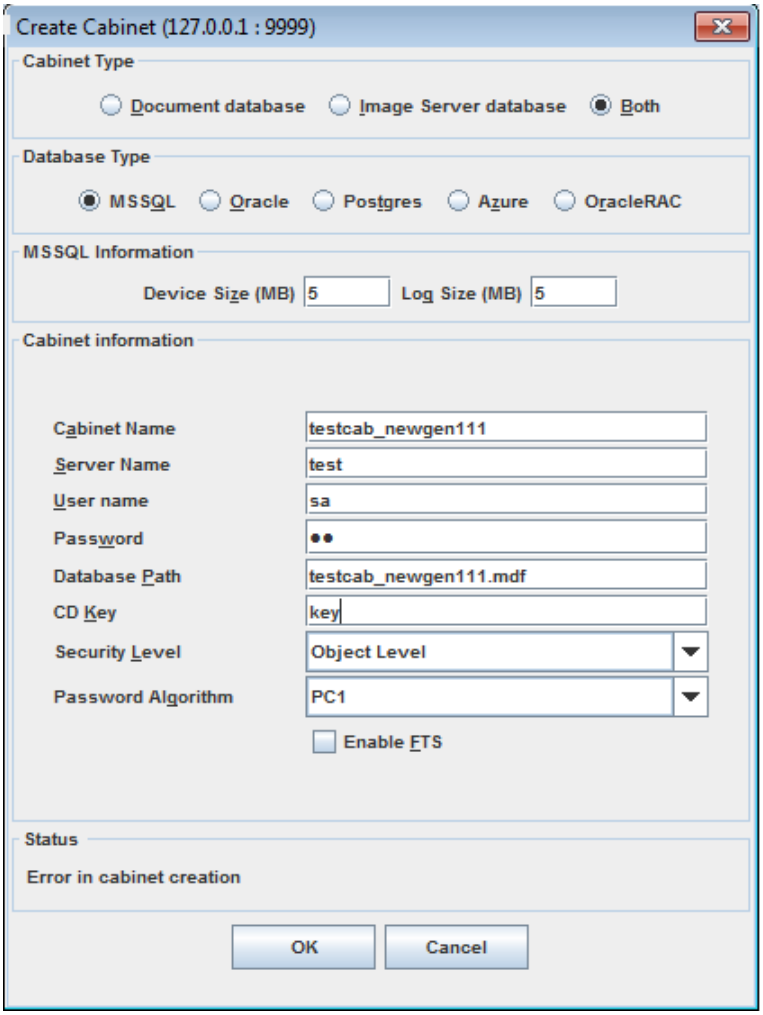


Figure 3.41

2. Select the **Enable FTS** option in the MSSQL information area to enable the FTS.

3. Specify the initial database size in **Device Size** textbox.
4. Specify the initial log size in **Log Size** textbox.
5. Specify the cabinet information in the various textboxes of the Cabinet Information area:
   a. Specify the cabinet name in the **Cabinet Name** textbox.
   b. Specify the server name (name of the machine where the MSSQL server is running) in the **Server Name** textbox.
   c. Specify the username in the **User name** textbox.
   d. Specify the password in the **Password** textbox.
   e. Specify the path where the database information is to be stored in the **Database Path** textbox.

NOTE:

The database (DAT) file is formed on the computer that we specify in the Server Name textbox i.e. the computer where the MSSQL Server is installed.

---

   f. Specify the CD key in the **CD Key** textbox.
   g. Select the required security level from the **Security Level** dropdown list. Right now, there is one level of security:

• **Object Level Security**	This means that all the rights and privileges are assigned to all the objects of OmniDocs.
• **Cabinet Level Security**	This means that all the rights and privileges are assigned at the Cabinet-level.

6. Click **OK** button to create the cabinet as per the requirements.
   Else, click **Cancel** button to close the **Create Cabinet** dialog box.

Using Normal user to create MSSQL 2008 cabinet:

NOTE:

For Creating a cabinet, avail the services of a DBA (Database Administrator) or of someone who has prior experience in creating an MSSQL cabinet.

Use **SQL Server Management Studio** and perform the following steps:

1. Select the particular SQL Server on the left panel and expand it.

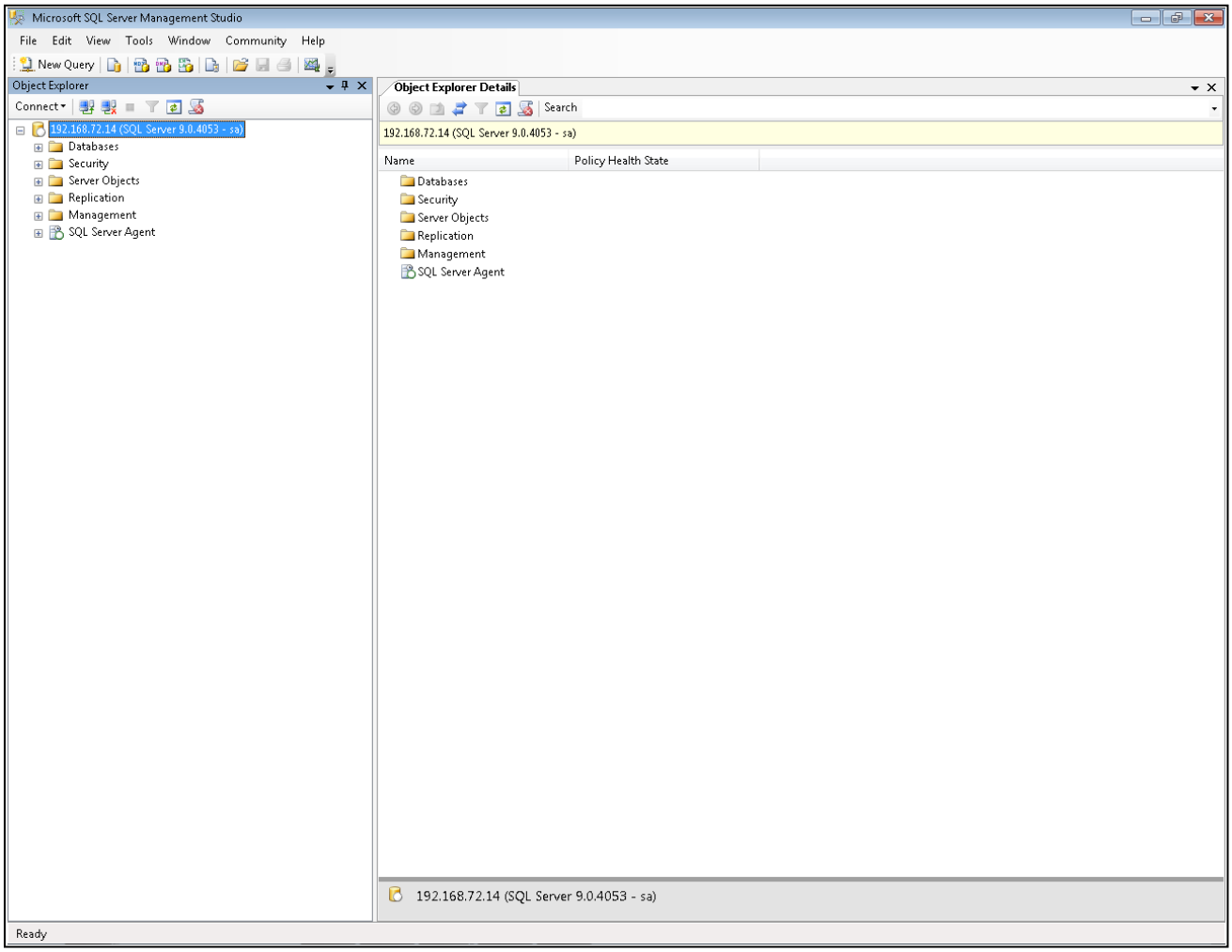


Figure 3.42

2. Expand **Security**.

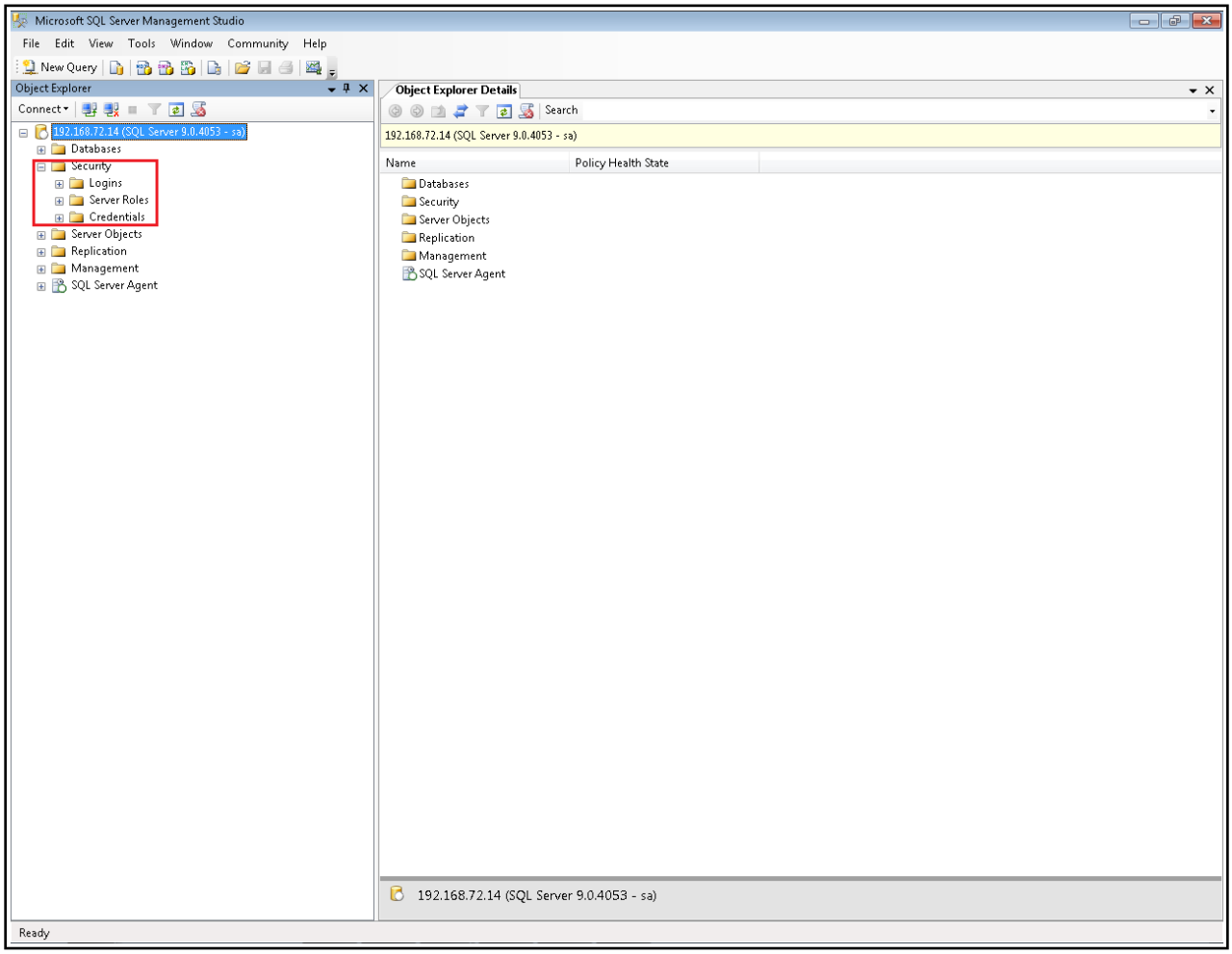


Figure 3.43

3. Select **Logins** and then do a right-click on it. Click on **New Login** from the pop-up menu.

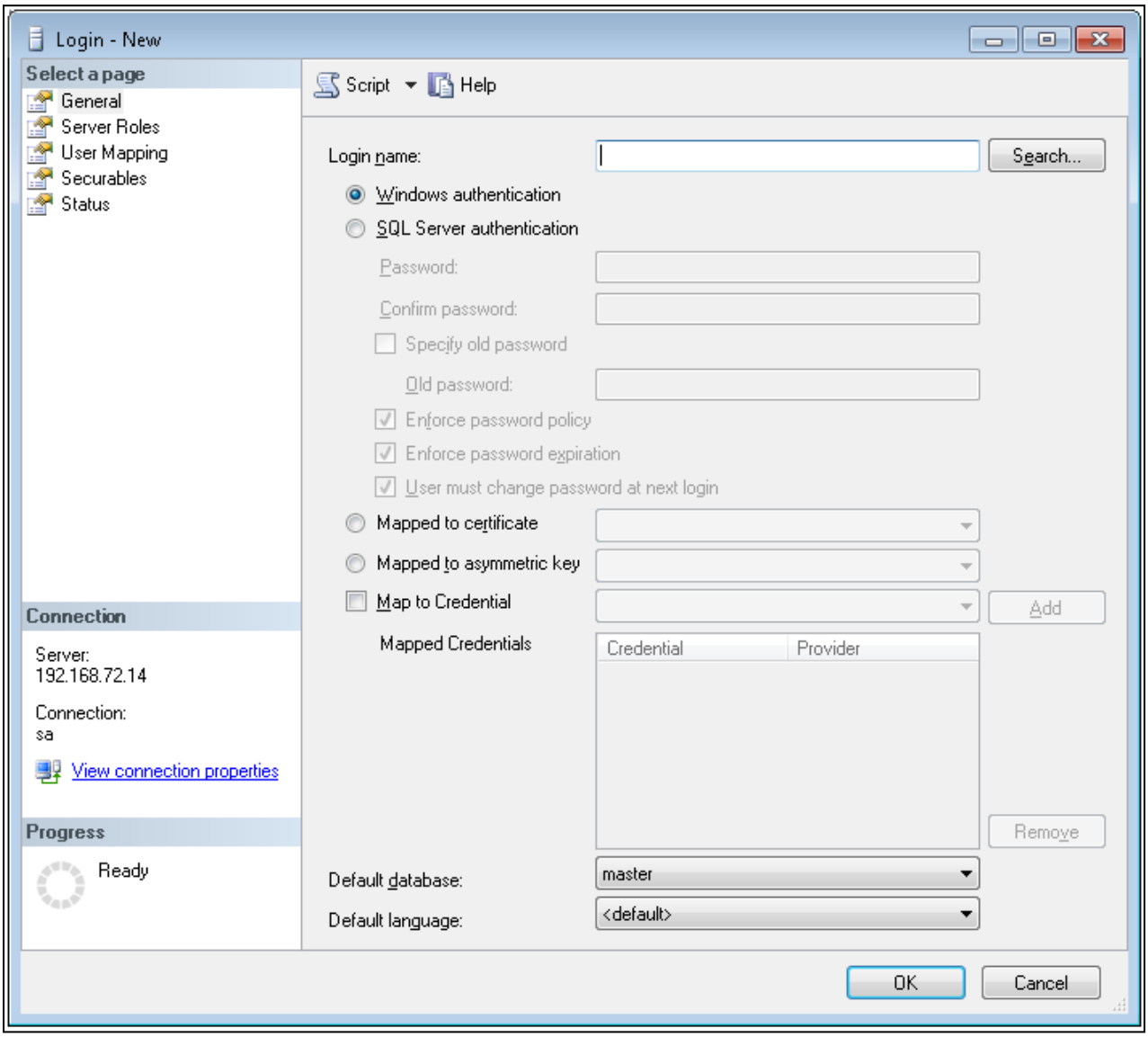


Figure 3.44

4. In the Login- New window, specify the **Login name**, select **SQL Server Authentication** and enter the password. The Default database should be master. Click **OK**.

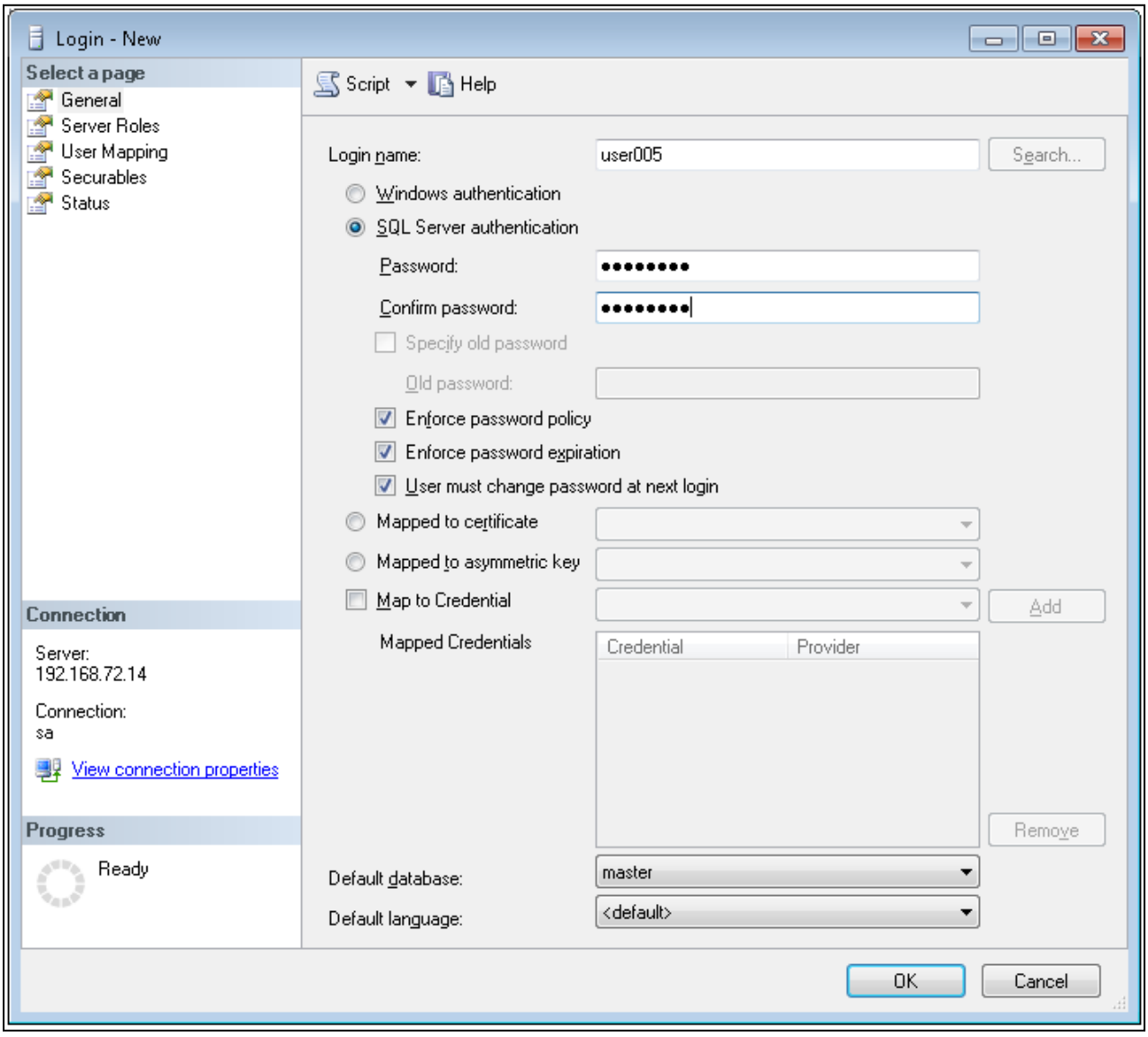


Figure 3.45

5. On the left panel expand **Databases** (corresponding to the particular SQL server) then expand **System databases** then expand **master** database then expand **Security** then Select **Users** and do a right-click on it.

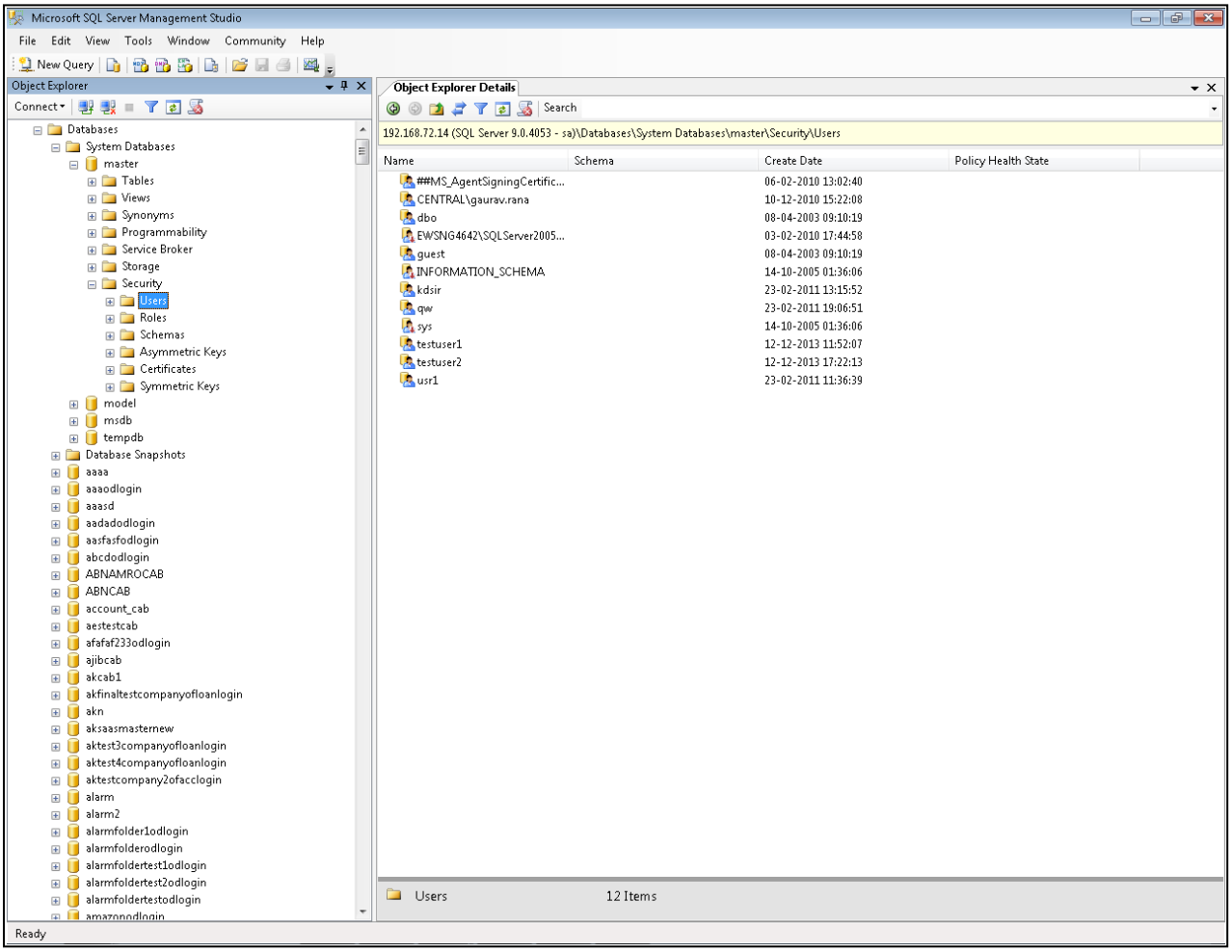


Figure 3.46

6. Perform the steps below:

   i. Click on **New User**.

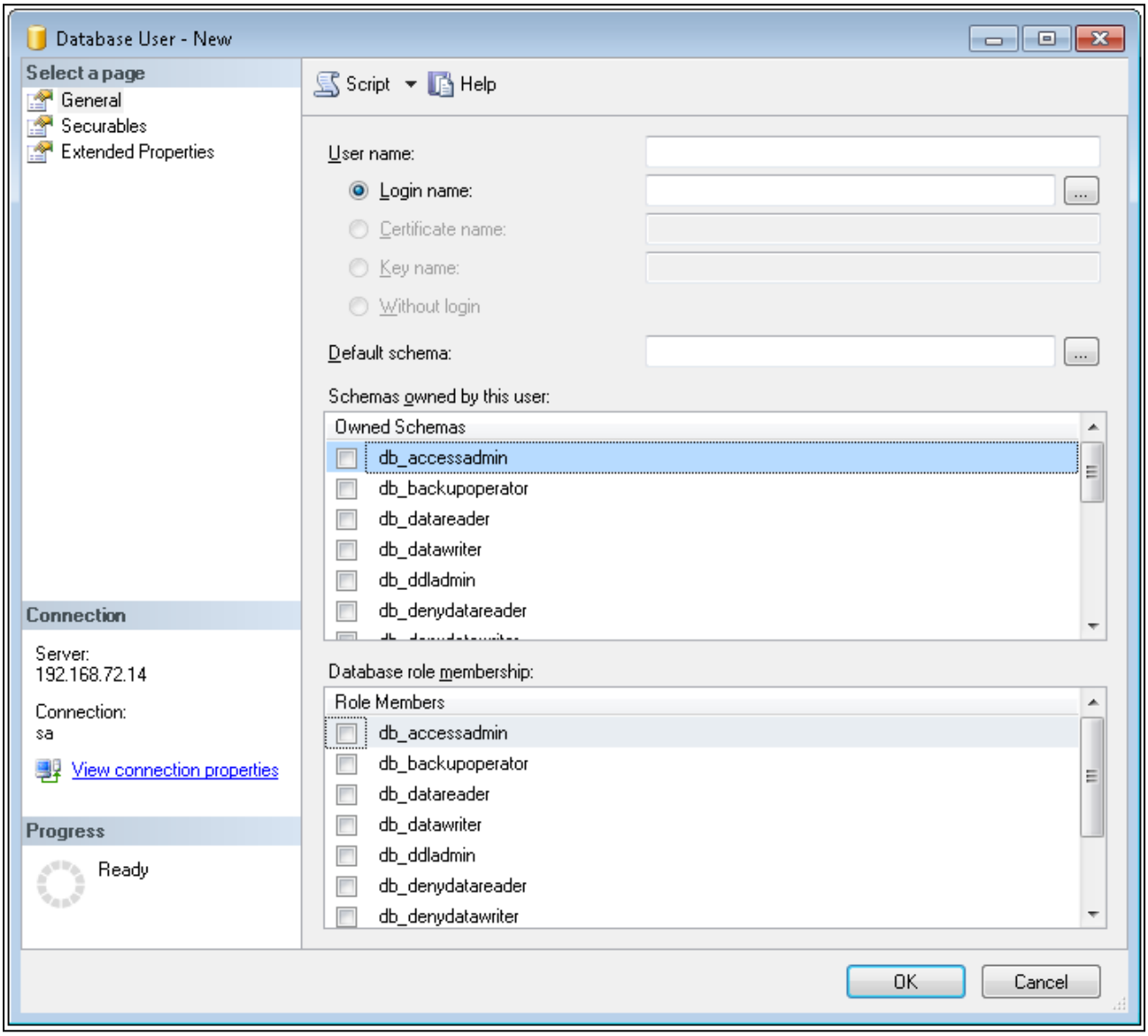


Figure 3.47

ii. In the Database User- New window, browse the above-created user for **Login Name** and click **OK**.

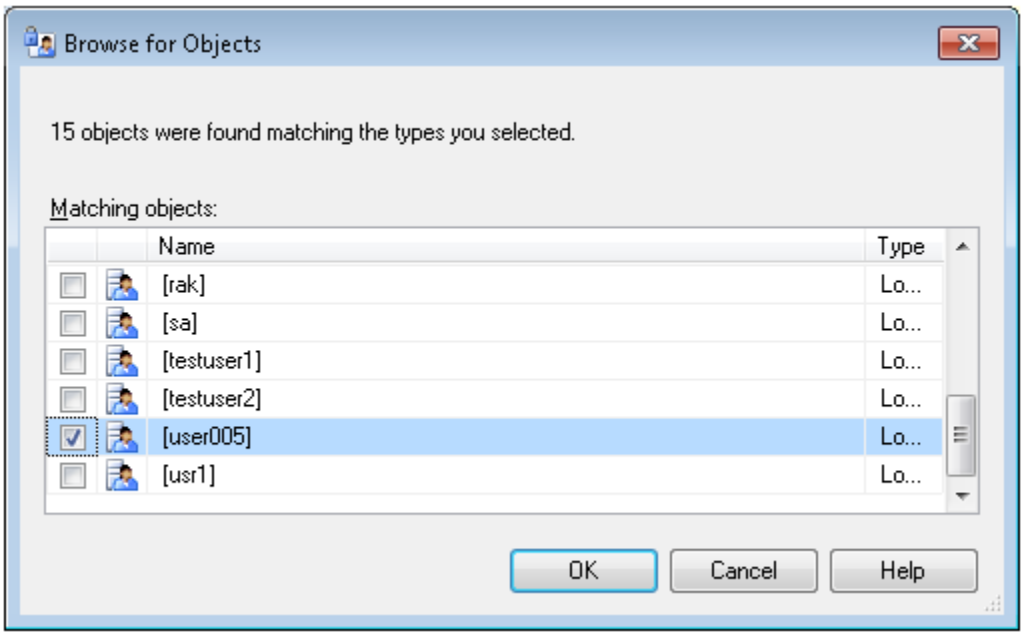


Figure 3.48

7. On the left panel, expand **Databases** (corresponding to the particular SQL server) and then **System Databases**, expand the **master database**, expand **Security**, select **Schema** and do a right-click on it.

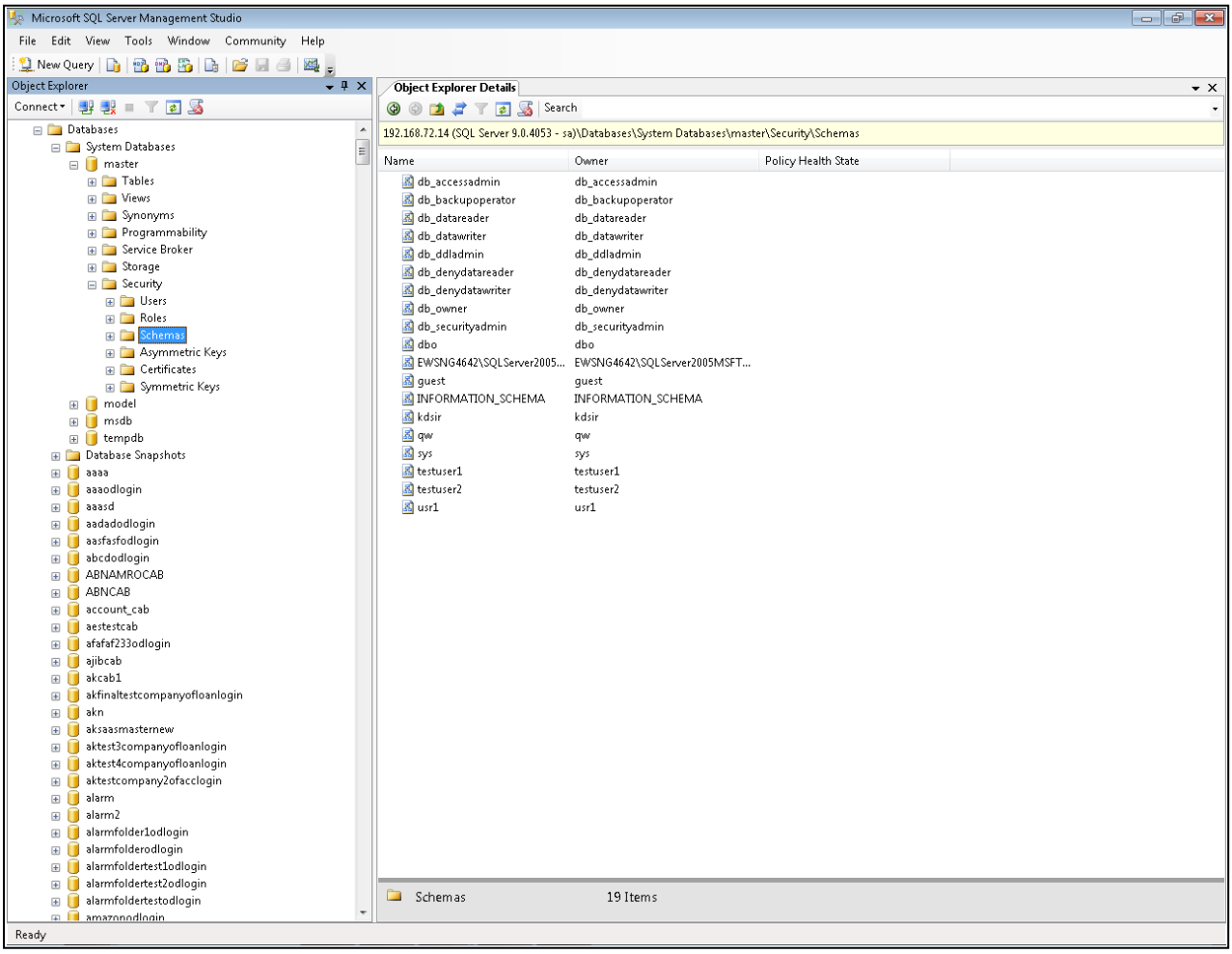


Figure 3.49

8. Perform the steps below:

   i. Click on **New Schema**.

   ii. A Schema- New window will open up. Enter the name of the above-created user in the fields **Schema name** and **Schema owner name** and Click **OK**.

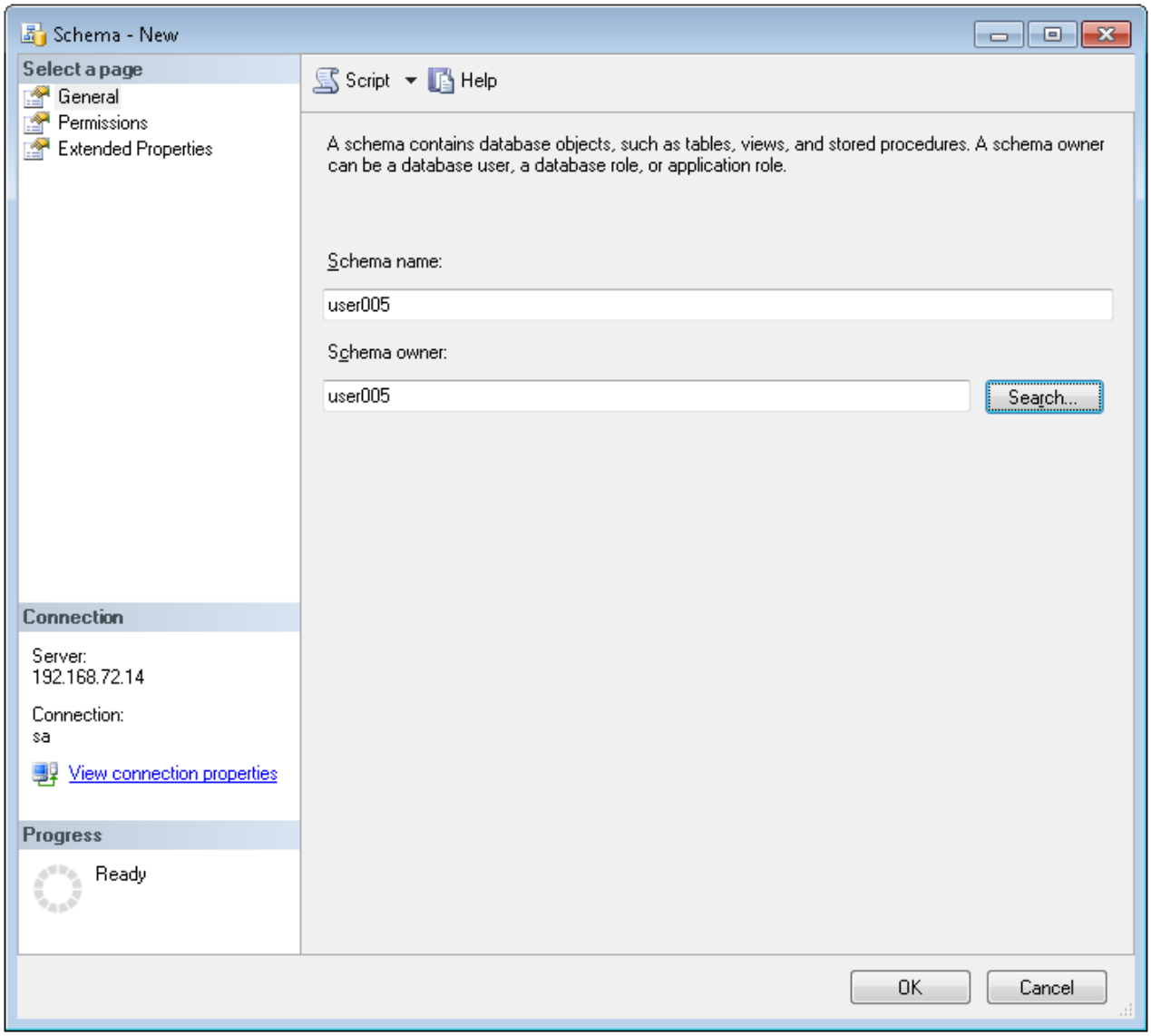


Figure 3.50

9. On the left panel expand **Databases** (corresponding to the particular SQL server) -> **System databases->Master database->Security->Users**. Select the User created above, right-click on it and then select **Properties**.

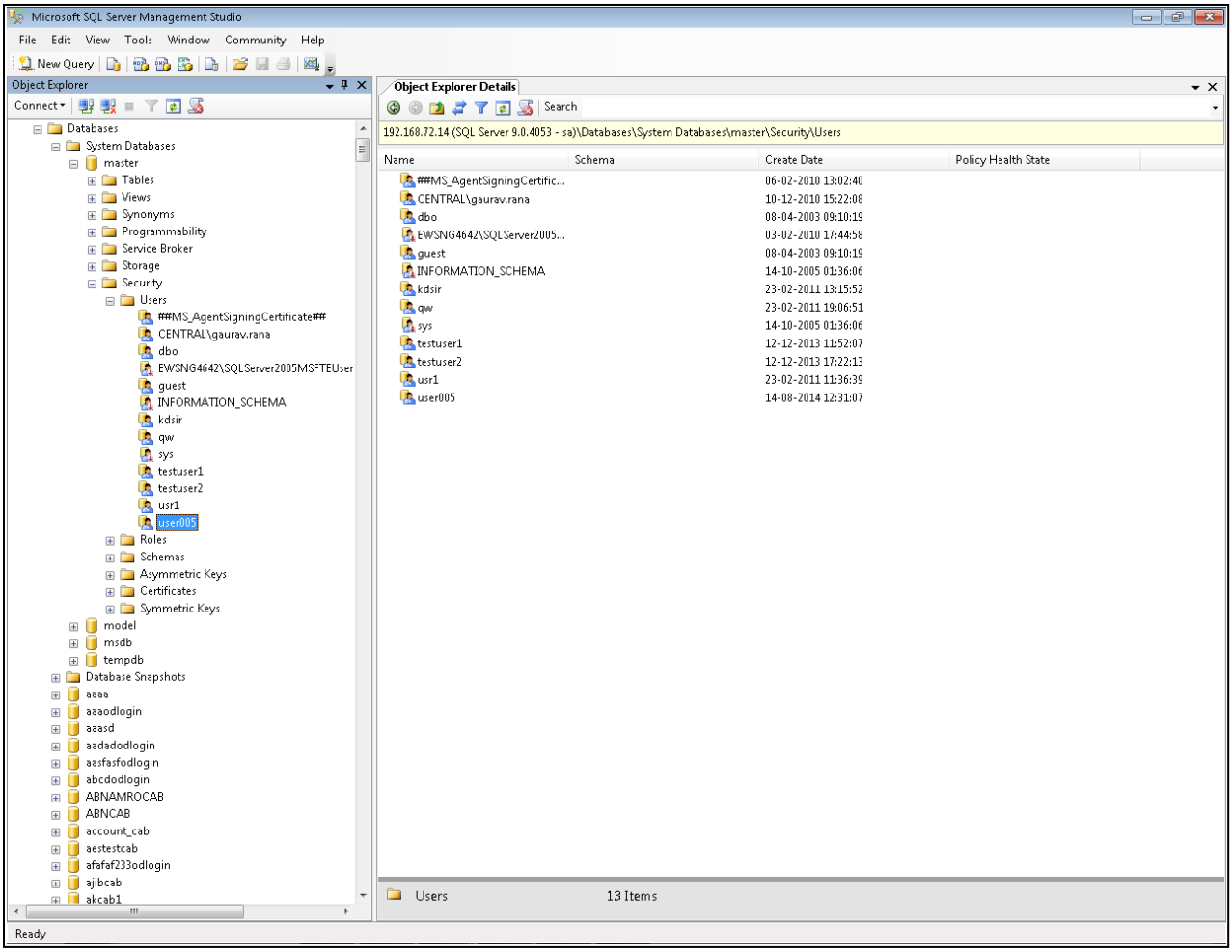


Figure 3.51

10. Perform the steps below:

i. Click on **Properties**.

ii. A Database User window opens, select the above-created schema as the default schema for the user.

iii. Click **OK**.

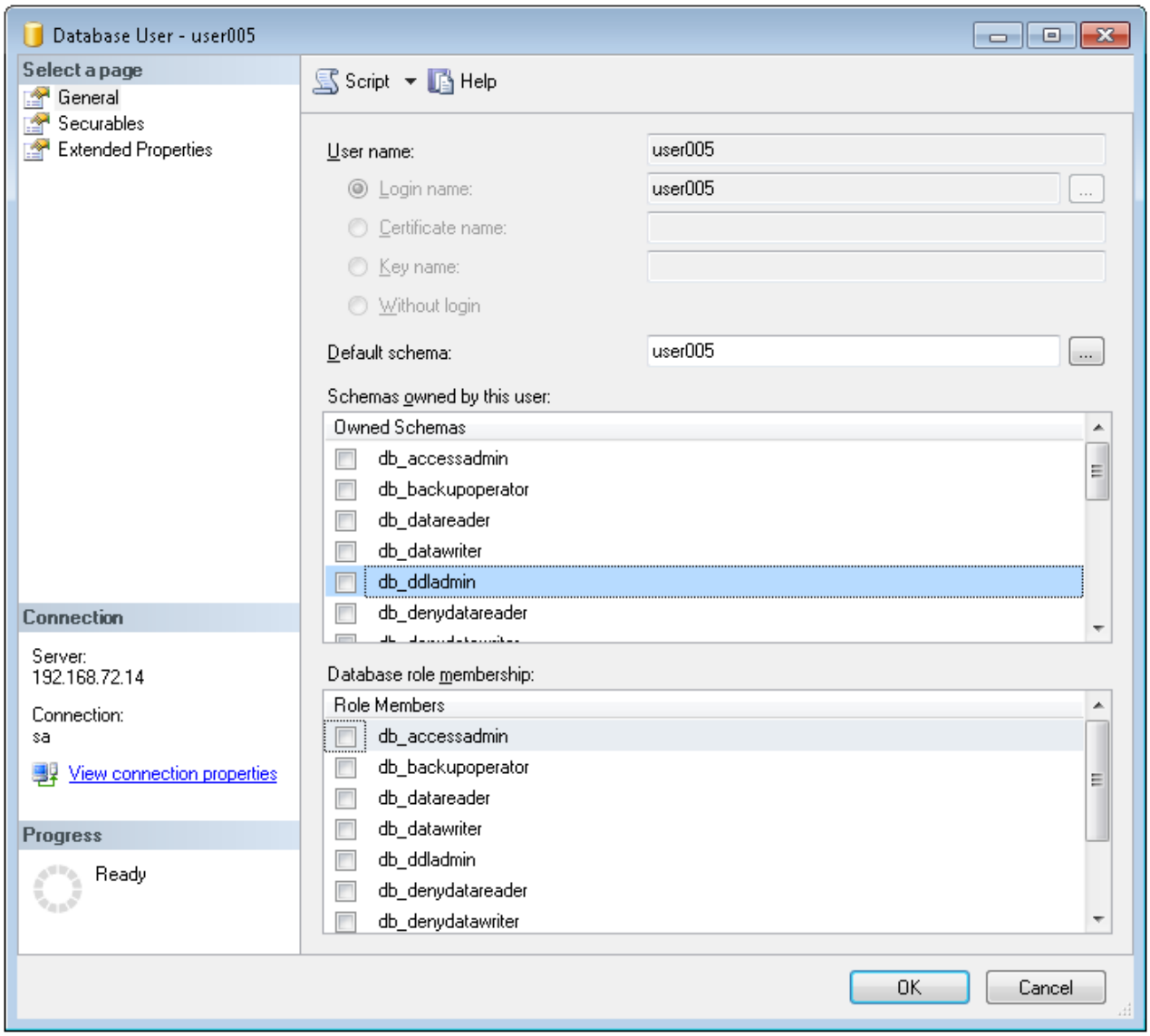


Figure 3.52

11. Perform the steps below:

i. Select **Master Database**.

ii. Right-click and select **Properties** from the pop-up menu.

iii. A new window opens.

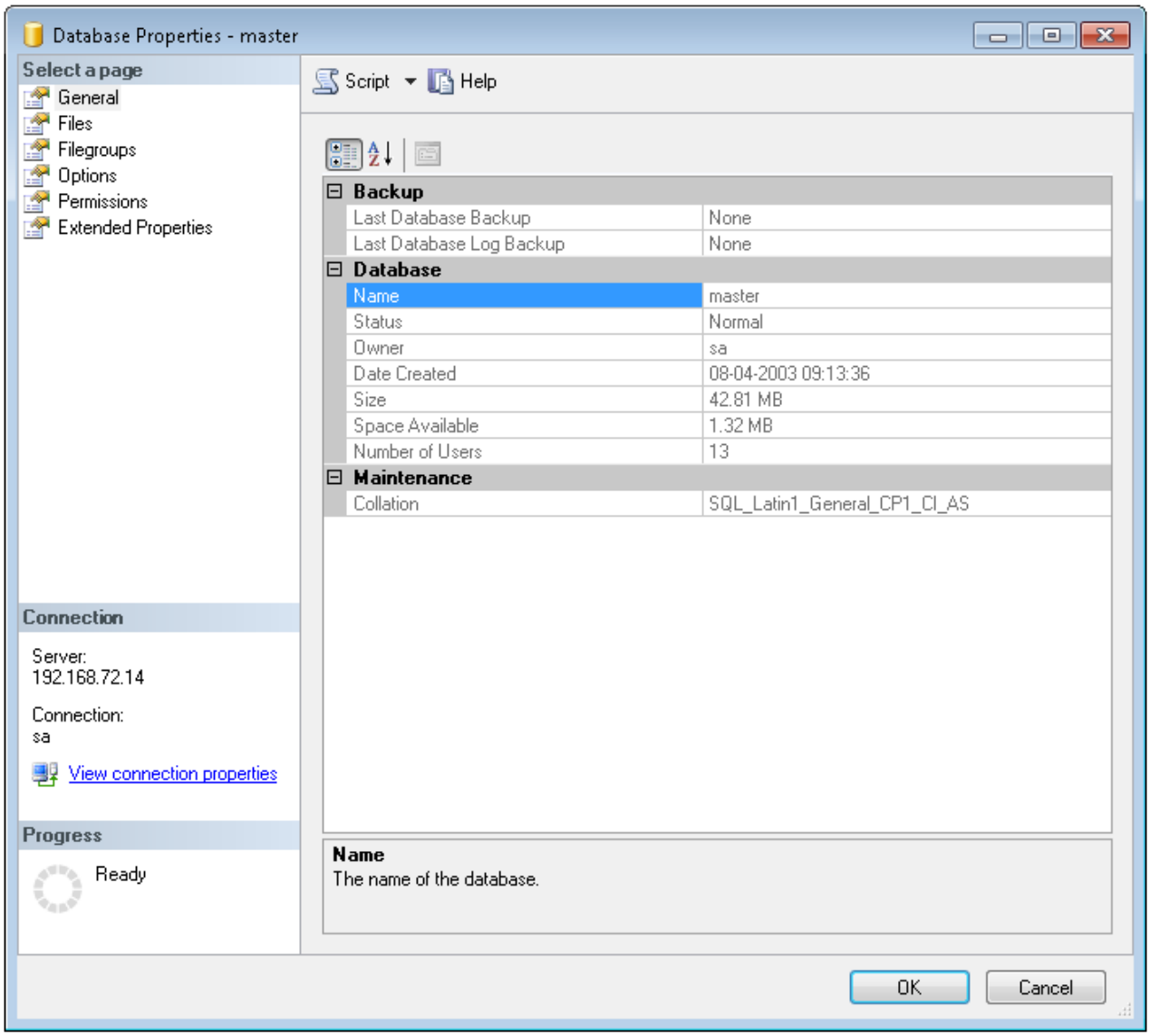


Figure 3.53

12. Perform the steps below:

i. Click on the **Permissions tab** then select the newly created user from the list of users.

ii. Now assign **Create database** and **Create procedure** permission to the user.

iii. Click **OK**.

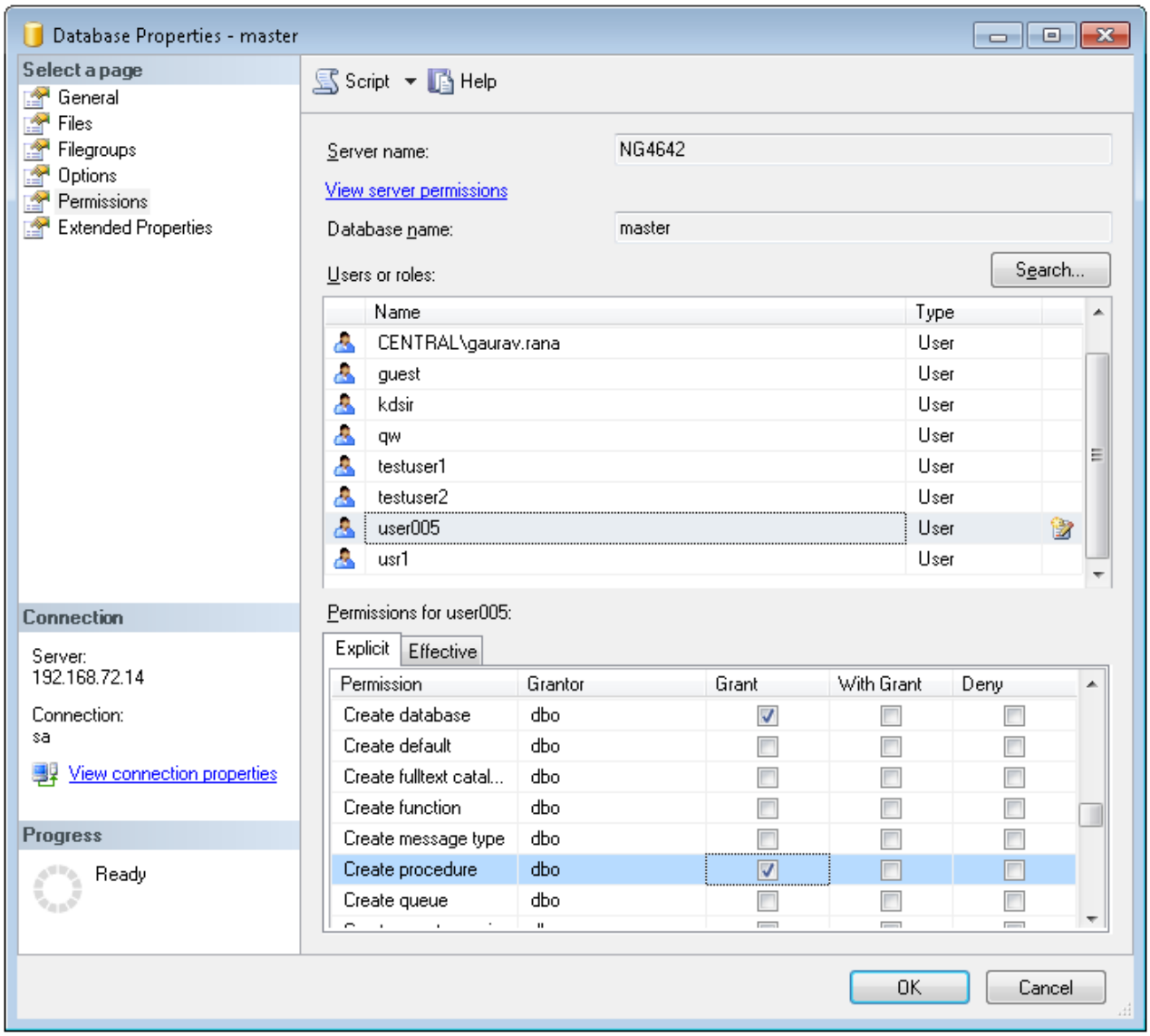


Figure 3.54

13. Now cabinets should be created using the above-created database user, instead of “sa”

Using Normal user to create MSSQL 2012 cabinet

NOTE:

For Creating a cabinet, avail the services of a DBA (Database Administrator) or a user who has prior experience in creating an MSSQL cabinet.

Use **SQL Server Management Studio** and perform the following steps:

1. Select the particular SQL Server on the left panel and expand it.

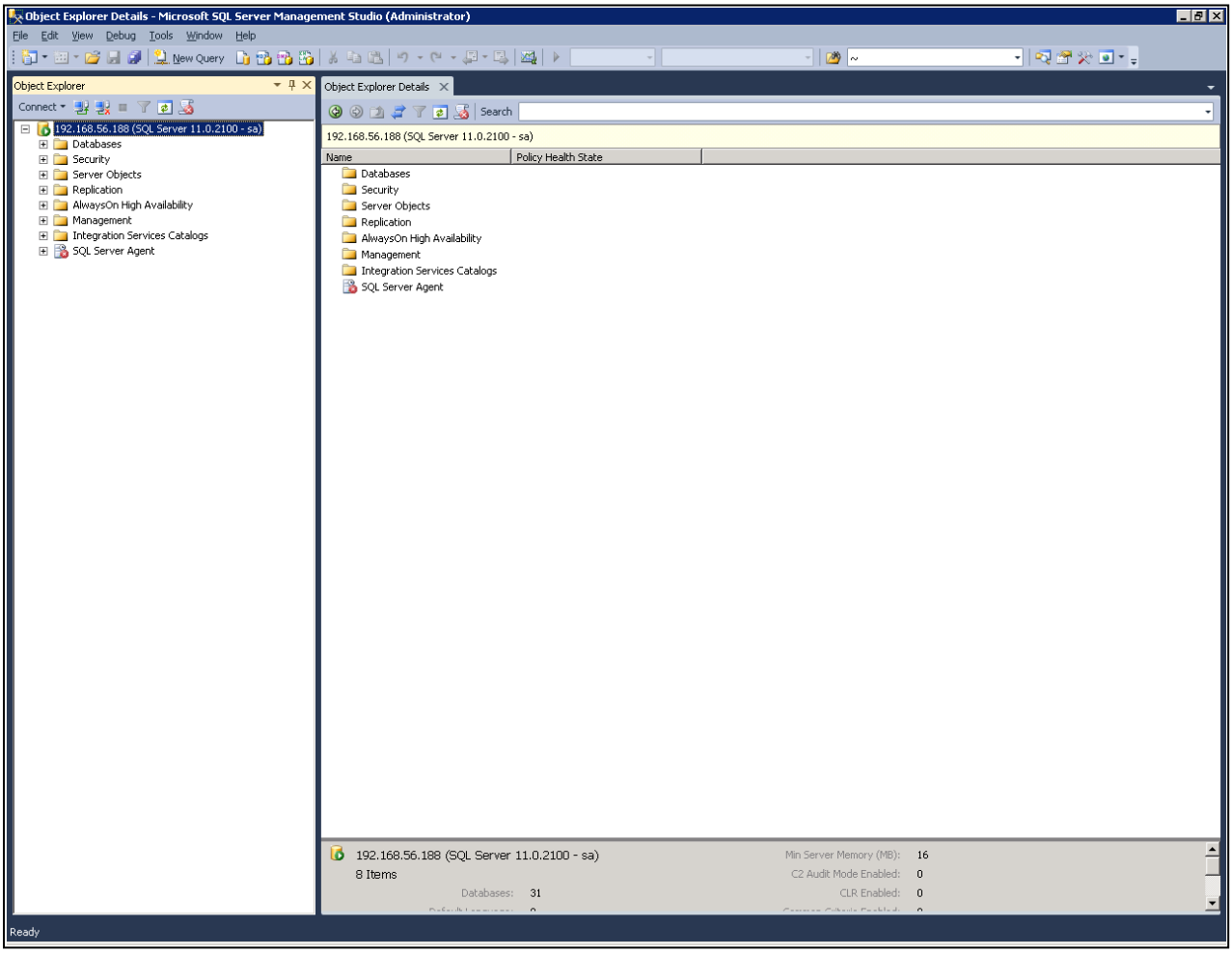


Figure 3.55

2. Expand **Security**.

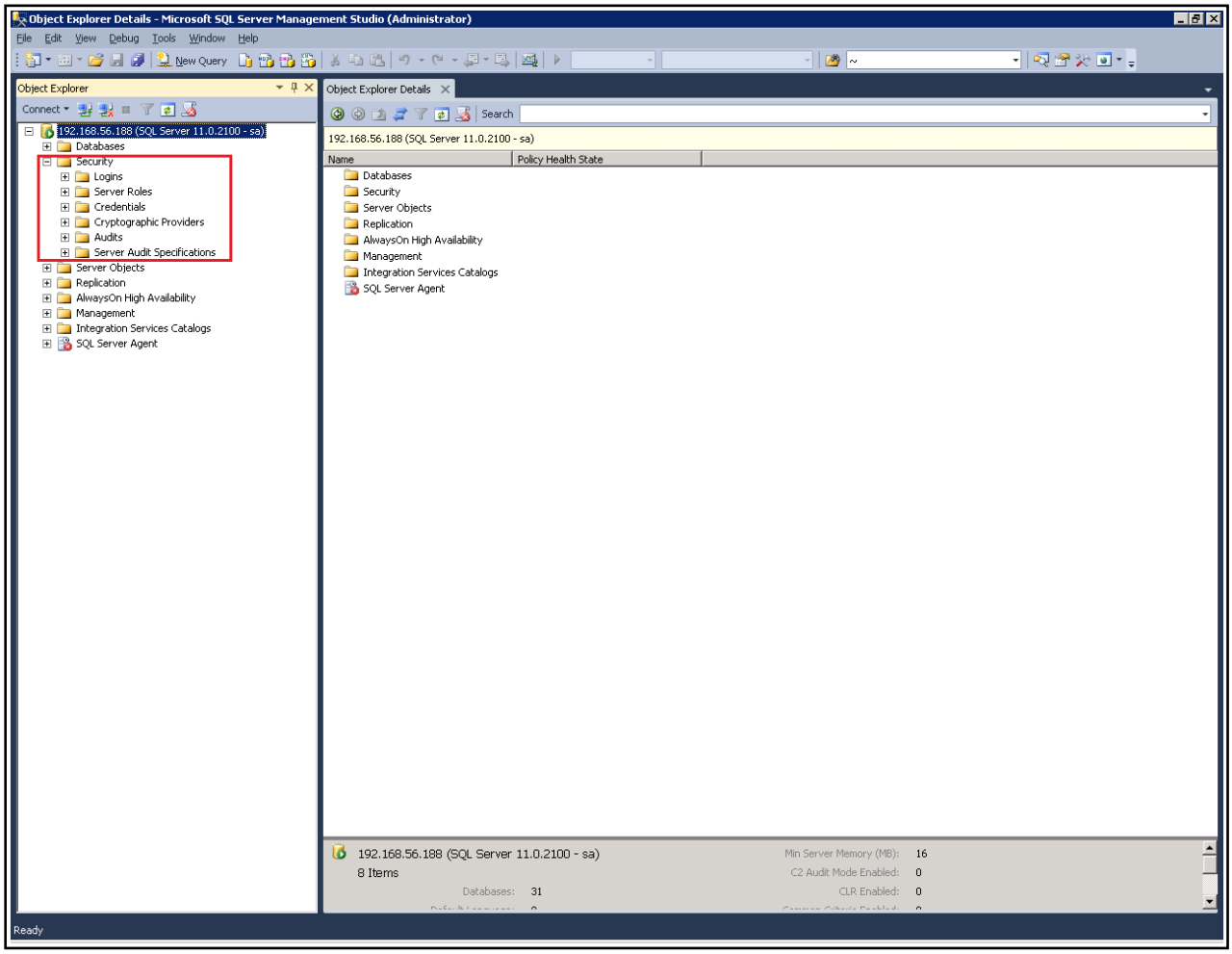


Figure 3.56

3. Select Login and then do a right-click on it. Click on **New Login** from the pop-up menu.

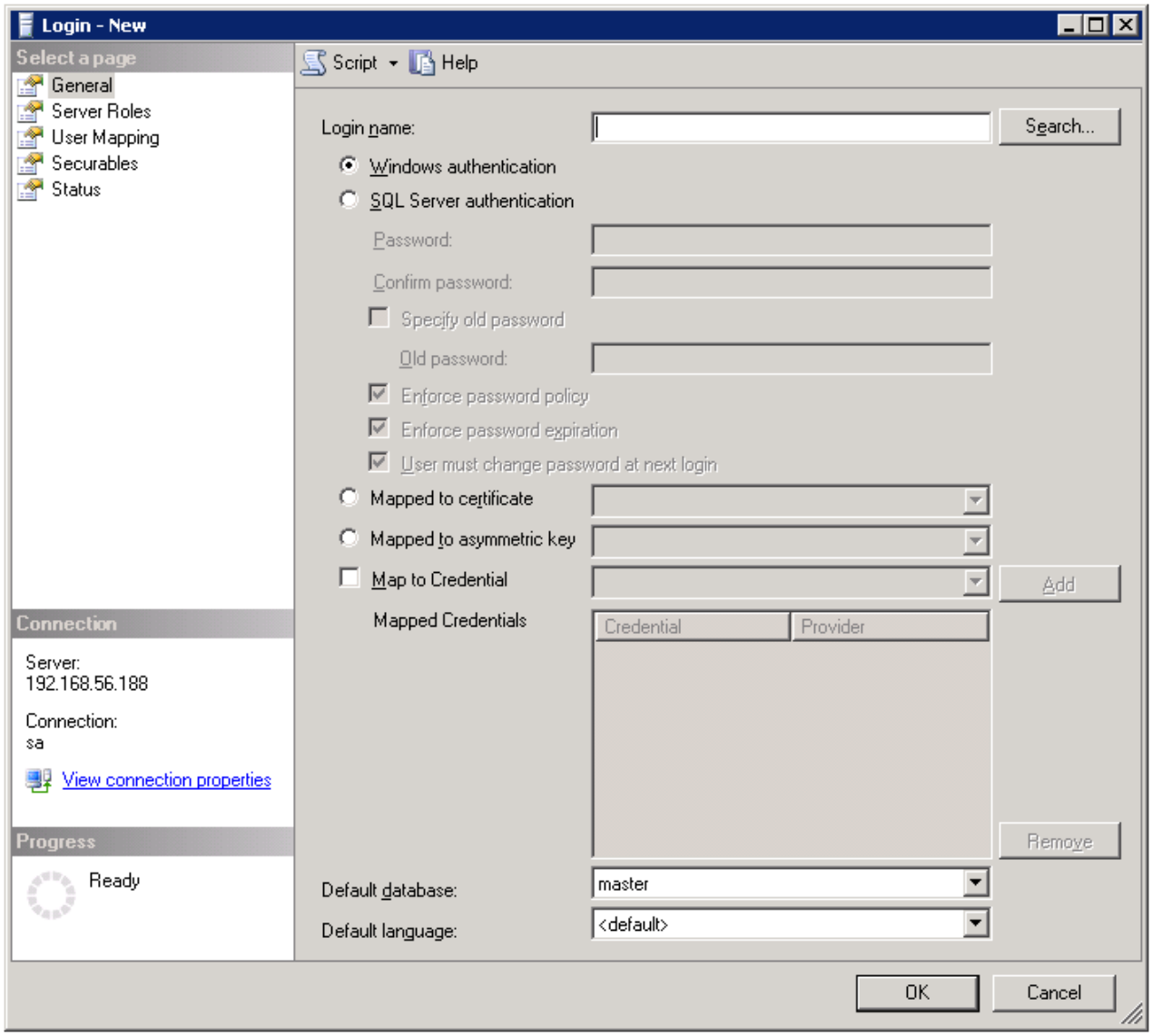


Figure 3.57

4. In the Login- New window, enter the **Login name**, select **SQL Server Authentication,** and enter the **password**. The default database should be **master.** Click **OK**.

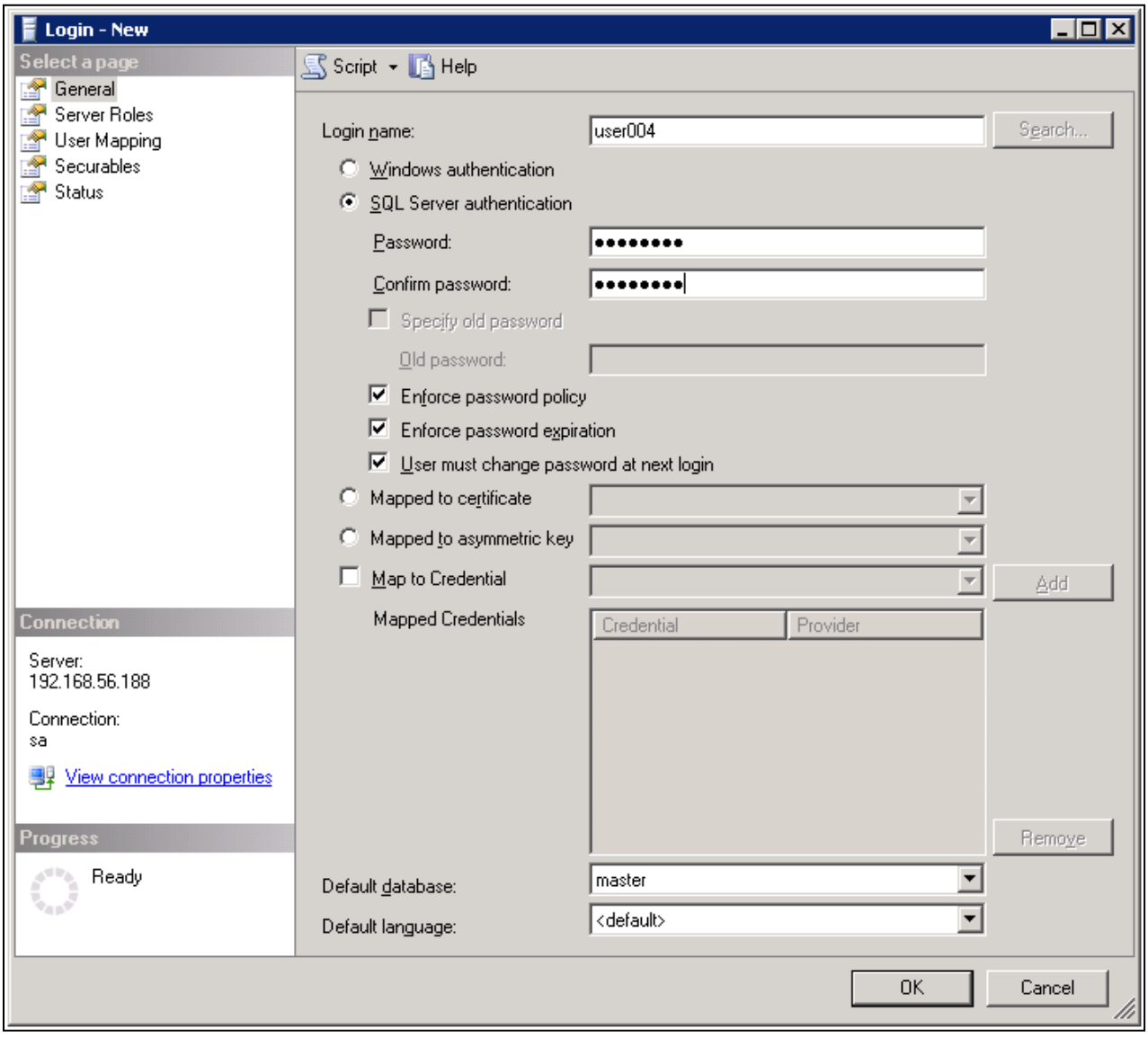


Figure 3.58

5. On the left panel expand **Databases** (corresponding to the particular SQL server) -> **System databases->master**-> **Security** and Select and right-click on **Users**.

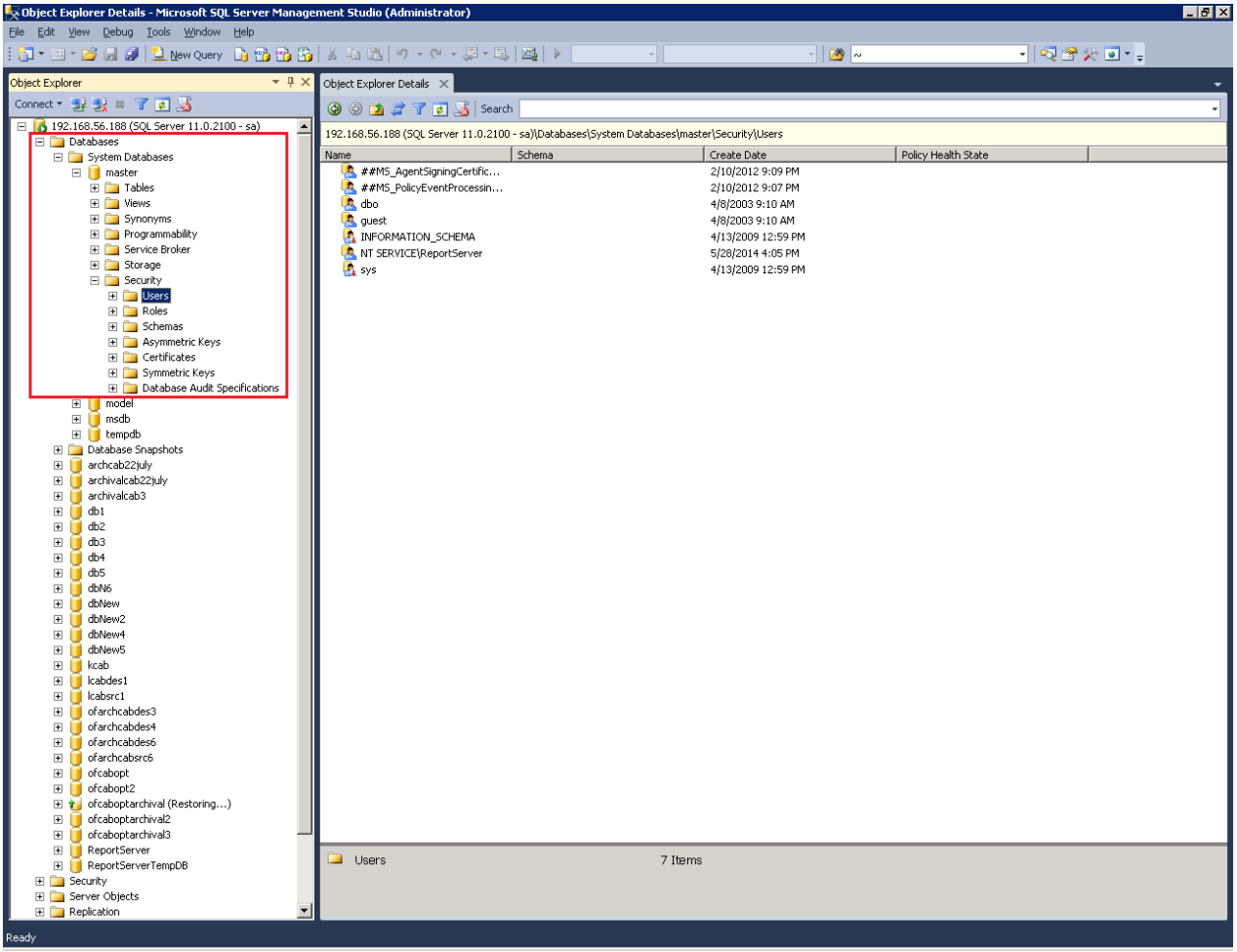


Figure 3.59

6. Perform the steps below:

   i. Click on **New User**.

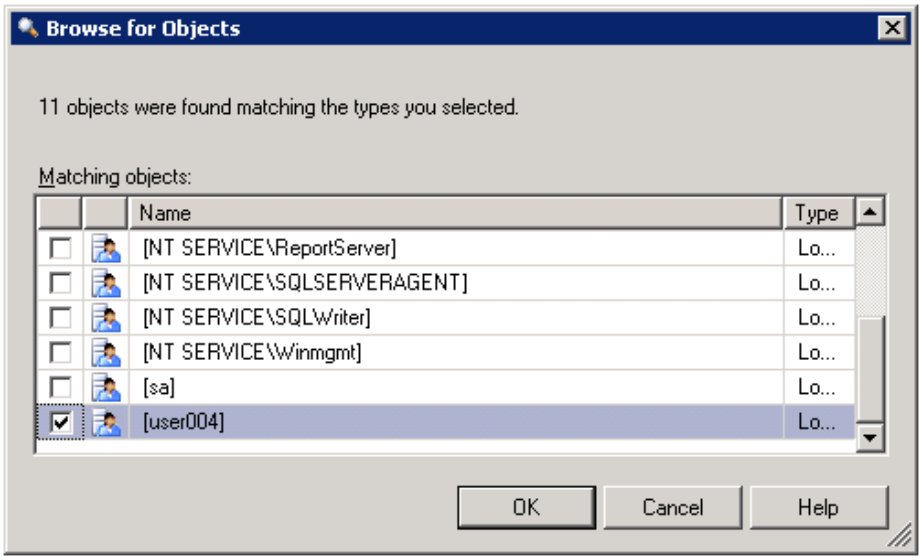


Figure 3.60

   ii. In the new window, browse the user-created above for Login Name and click **OK**.

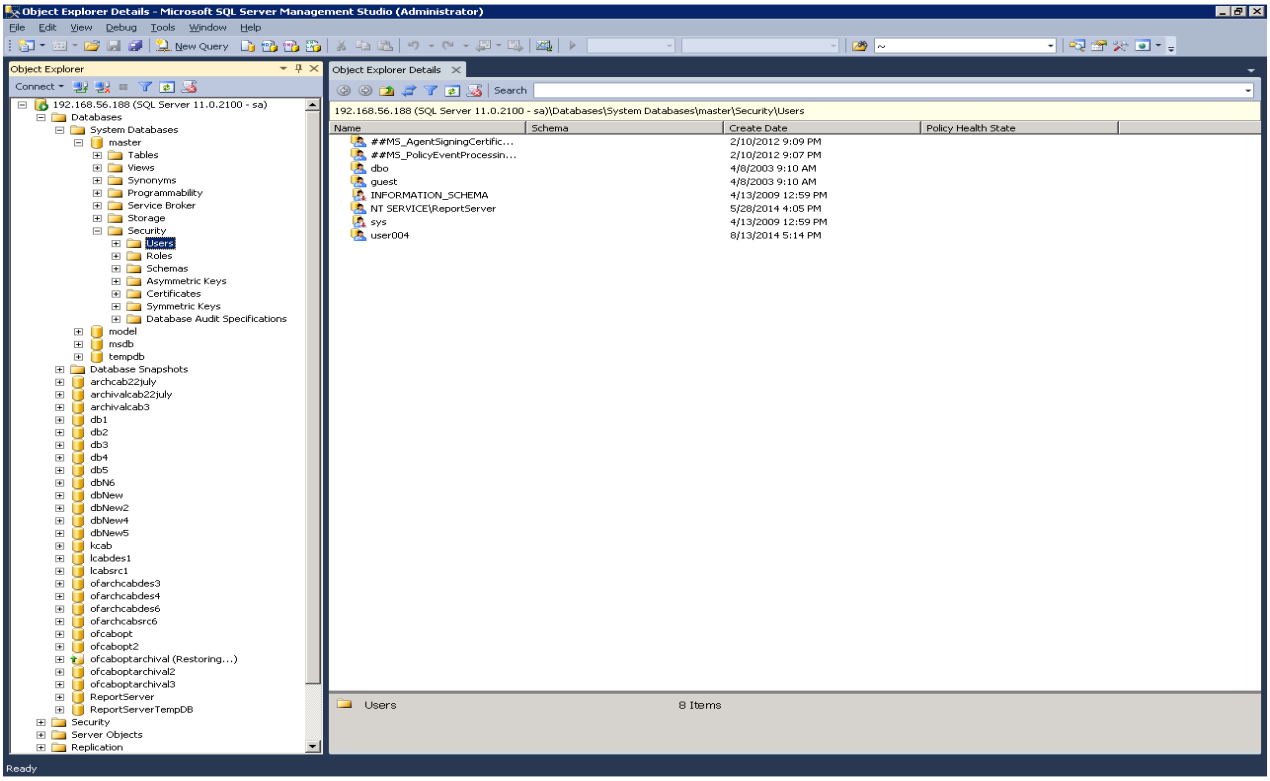


Figure 3.61

7. On the left panel expand **Databases** (corresponding to the particular SQL server) ->**System databases->master database->Security** and then select and right-click on **Schema**.

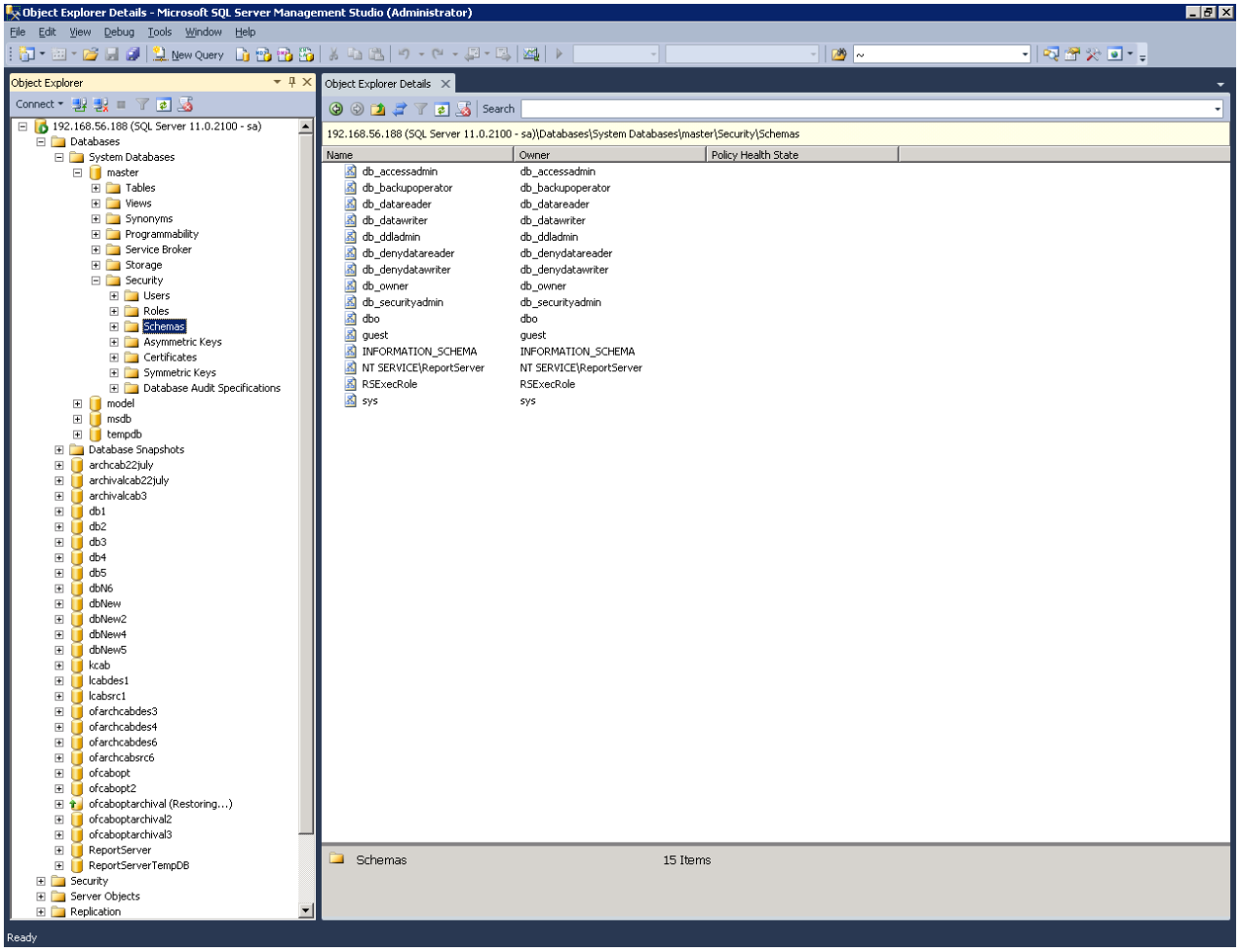


Figure 3.62

8. Perform the steps below:

   i. Click on **New Schema**.

   ii. A **Schema-New** window will open

   iii. Enter the **Schema name** and **Schema owner** name.

   - You can search for a **Schema owner** by clicking on **Search** button.

   iv. Click **OK** to create the new schema. This schema gets added to the list of Schemas.

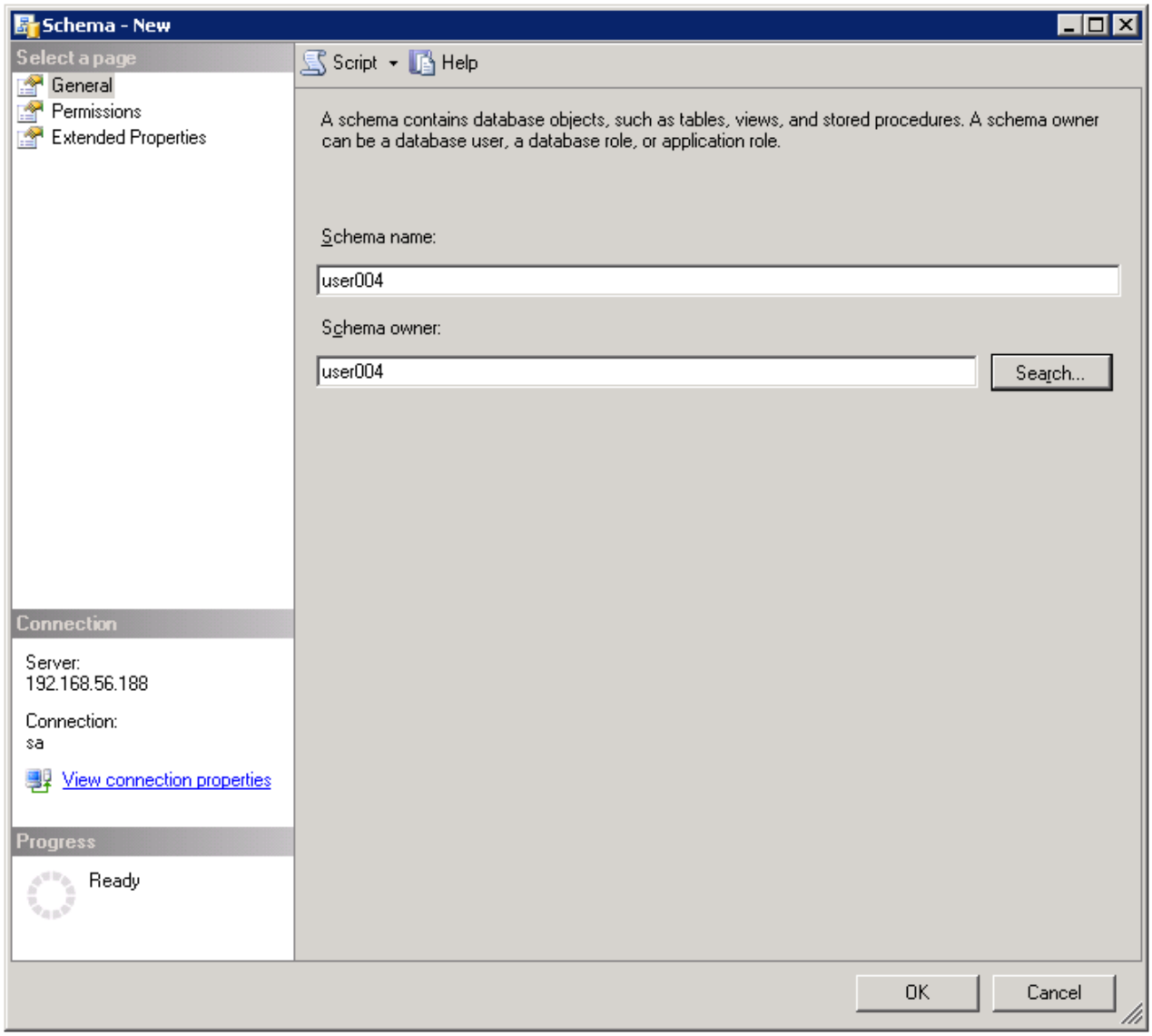


Figure 3.63

9. On the left panel expand **Databases** (corresponding to the particular SQL server) ->**System databases**->**master** database->**Security->Users**. Select and right-click on the User. Select **Properties**.

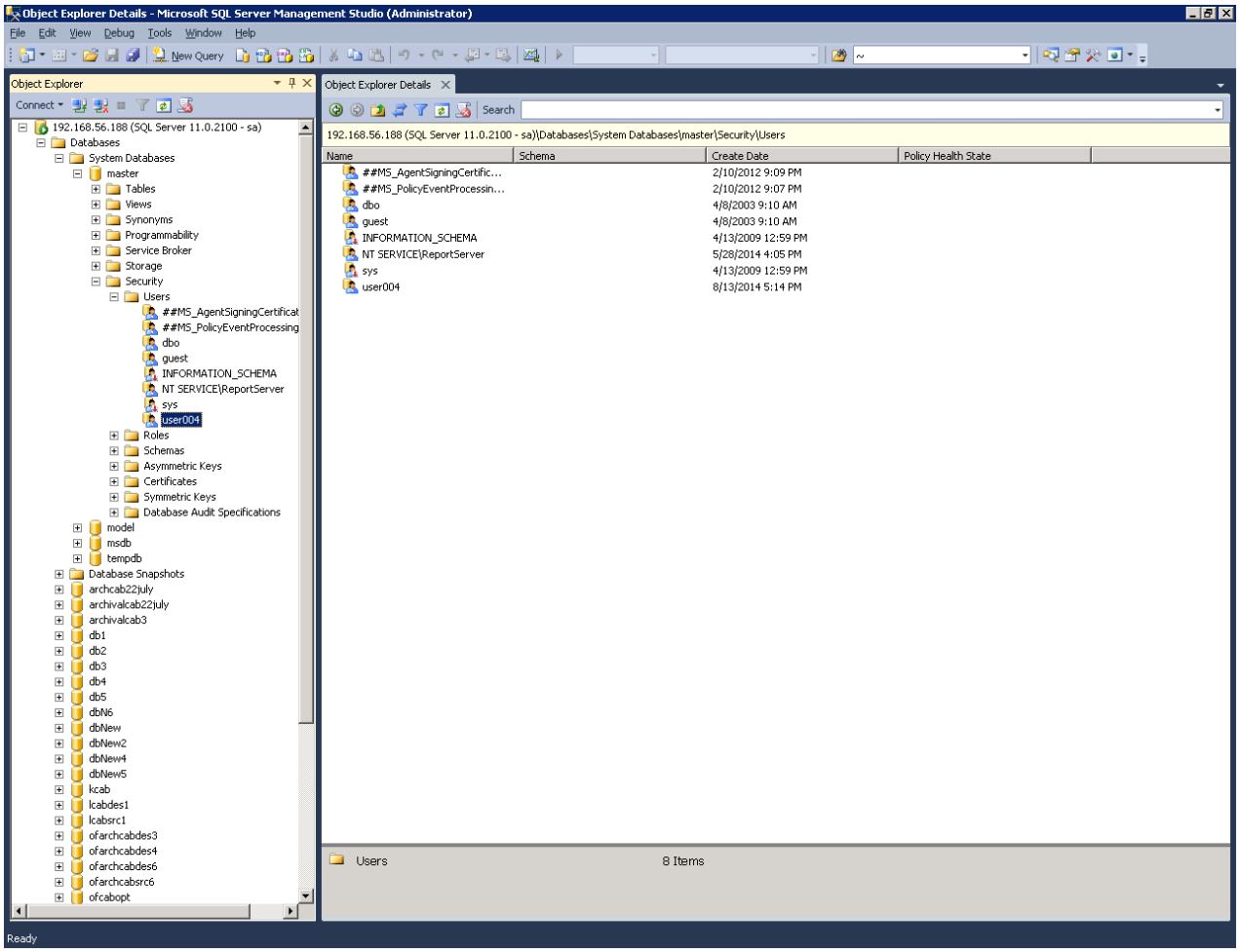


Figure 3.64

10. Click on **Properties**. A new window opens. Select the above-created schema as the default schema for the user.
11. Click **OK**.

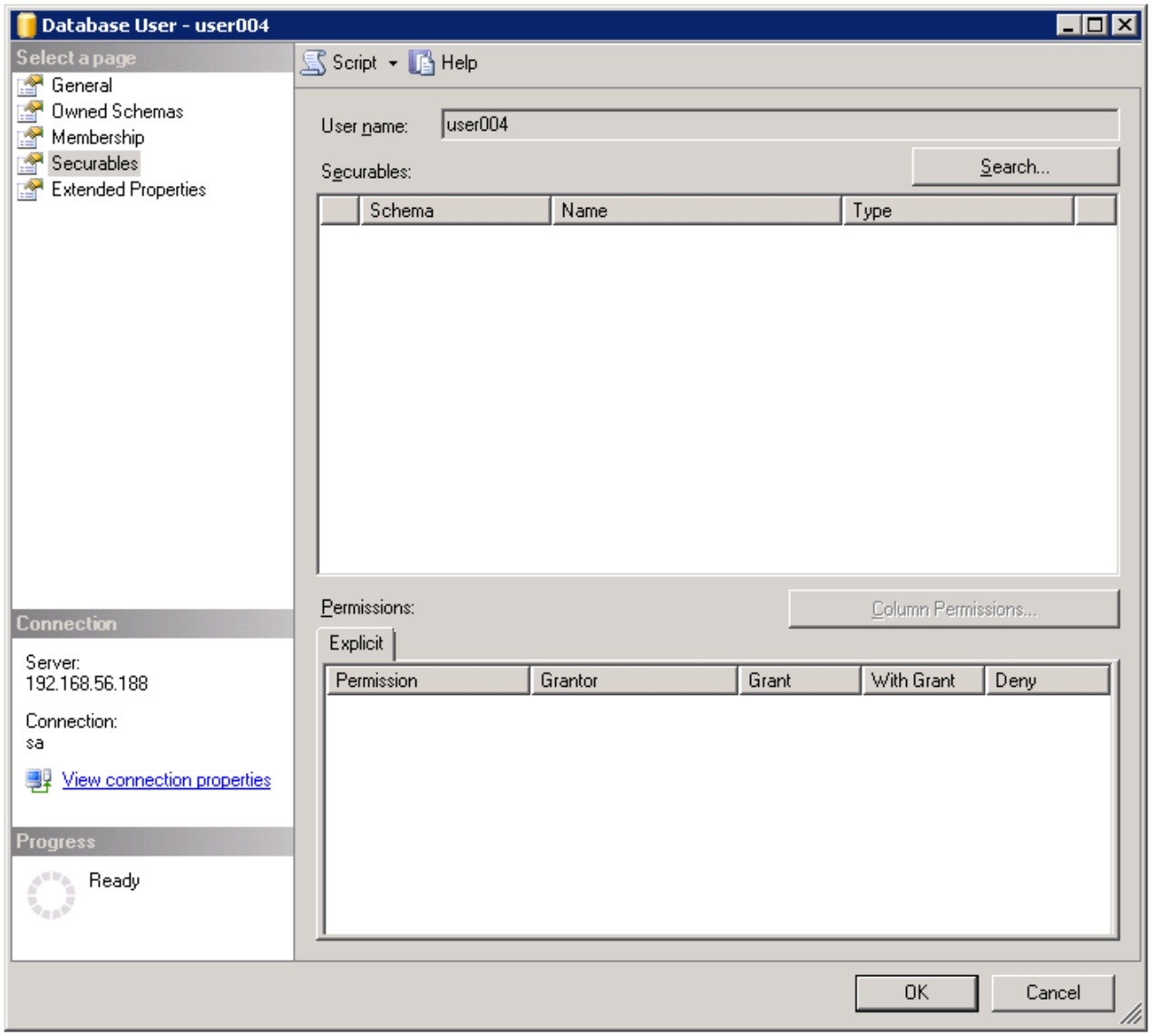


Figure 3.65

12. Perform the steps below:

i. Select **Master Database** and right-click.

ii. Click on the **properties** of the pop-up menu.

iii. A new window opens.

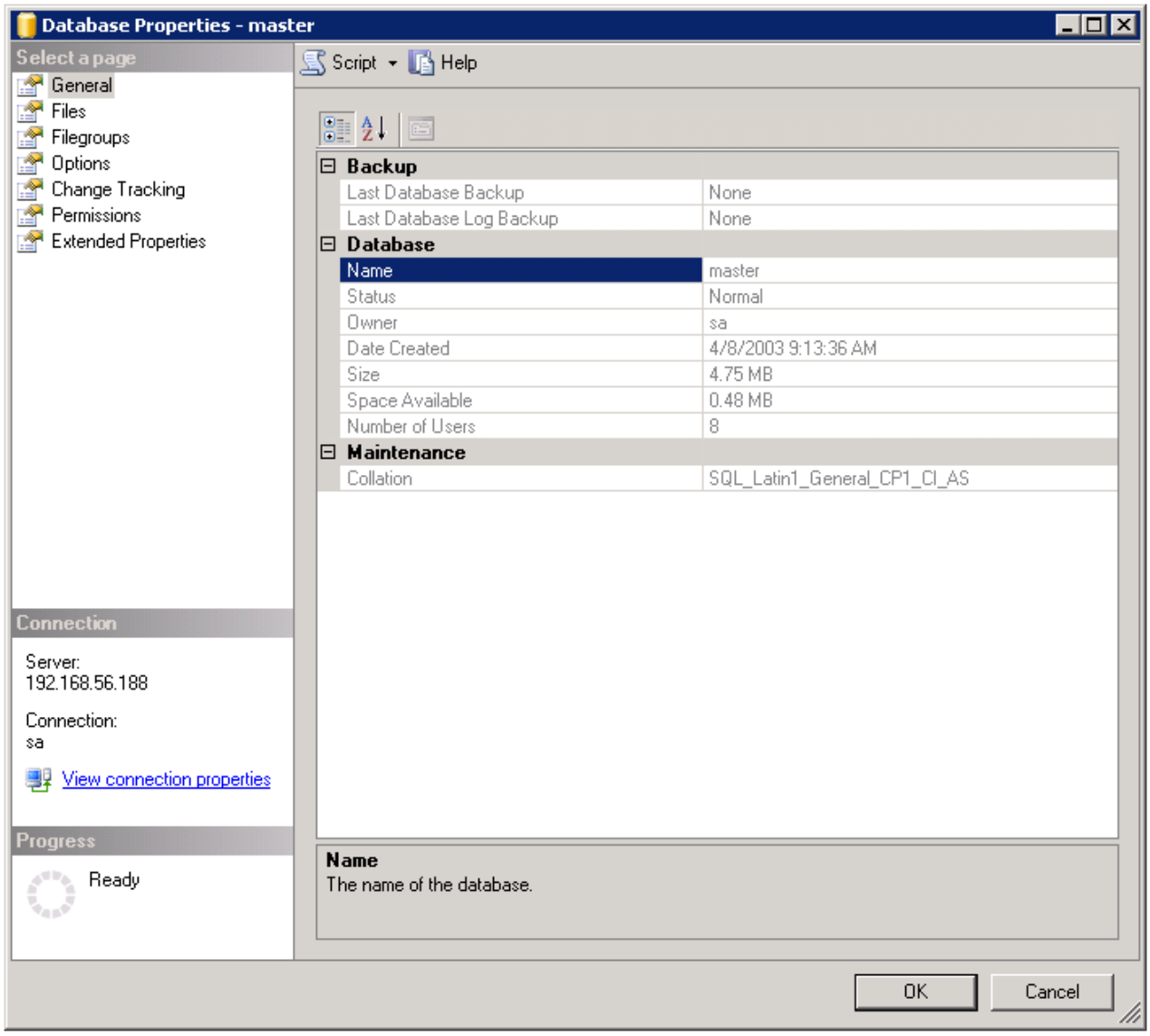


Figure 3.66

13. Perform the steps below:

i. Click on **Permissions tab.**

ii. Then select the newly created user from the list of users.

iii. Now assign Create database and Create procedure permission to the user.

iv. Click **OK**.

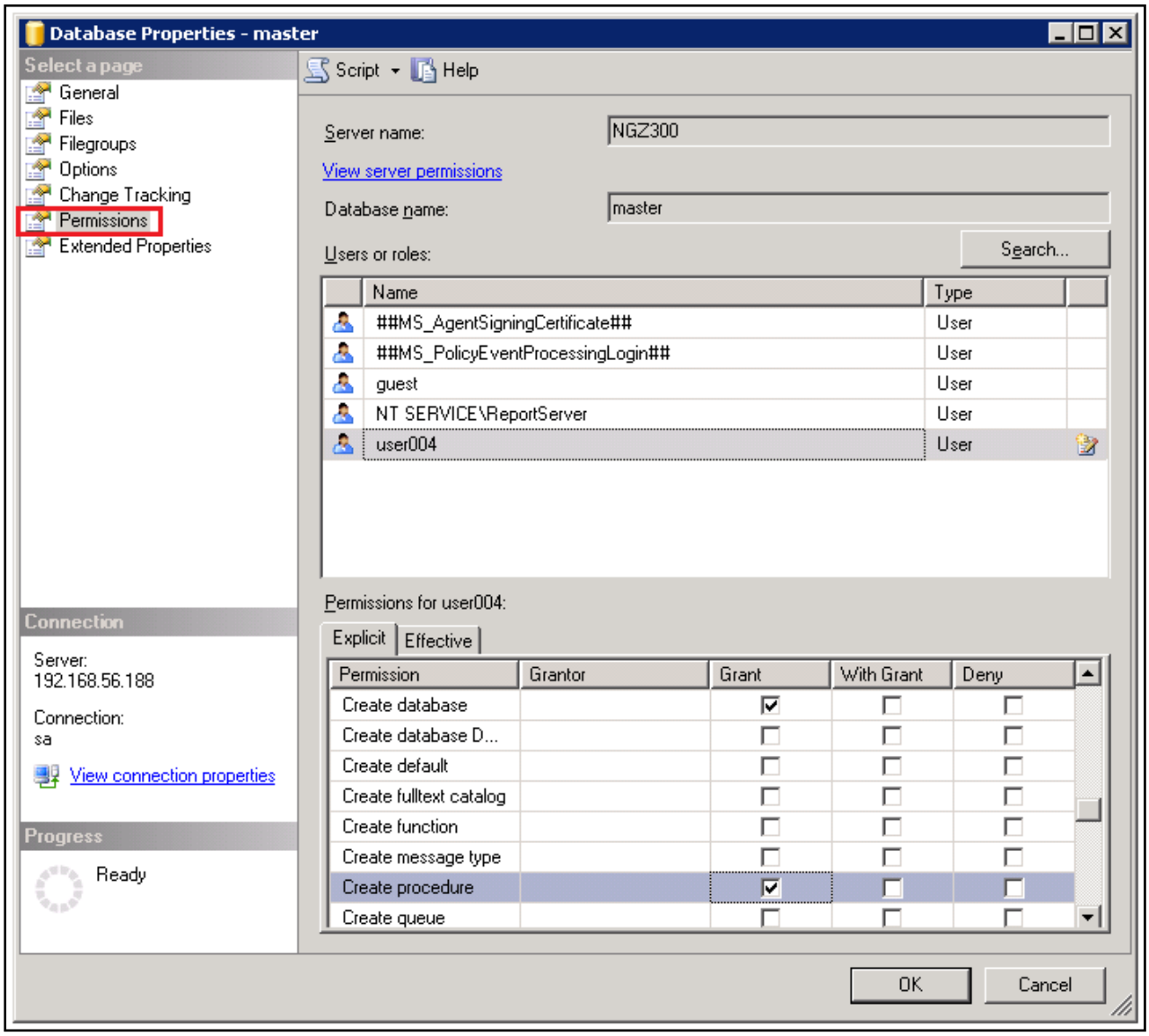


Figure 3.67

14. Now cabinets should be created using the above-created database user, instead of “sa”.

3.2.7 Creating Oracle Database Cabinet

Cabinet Creation can be done in two ways:

A. By using **Superuser** like '**sys**' (Oracle).

B. By using a **normal user** with cabinet creation rights.

The two ways are explained below:

A. Creating Cabinet using Superuser

To create an Oracle database cabinet:

1. Select the **Oracle** database option from the **Database Type** area.

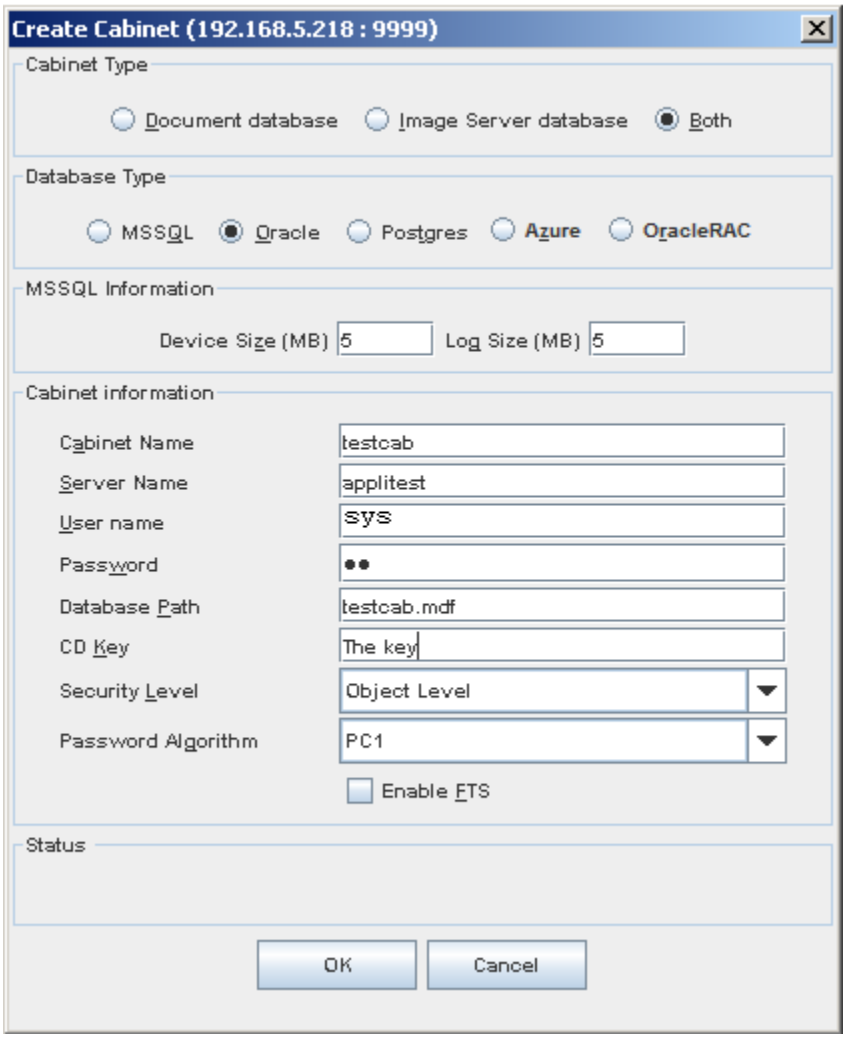


Figure 3.68

2. Check the **Enable FTS** option under the Oracle Information area to enable the FTS.
3. Specify the Oracle Service Name in **Service Name** textbox.
4. Specify the Oracle Port in **Port** textbox.
5. Specify the cabinet details under the Cabinet Information:
    i. Specify the cabinet name in the **Cabinet Name** textbox.
    ii. Specify the server IP Address in the **Server IP** textbox.
    iii. Specify the username in the **User name** textbox.
    iv. Specify the password in the **Password** textbox.
    v. Specify the path where the database information is to be stored in the **Database Path** textbox.
    vi. Specify the CD key for user licenses in the **CD Key** textbox.
    vii. Select the required security level from the **Security Level** dropdown list.
    viii. Click the **OK** button to create the cabinet as per the requirements.
    ix. Or, Click the **Cancel** button to close the **Create Cabinet** dialog box at any stage of creating the Cabinet.

B. Creating Cabinet using Normal User

Case 1

In case, if client does not create the tablespace and cabinet user and is expected to create them from the product end using the createDB script, the database user should possess the following minimum privileges:

a. CREATE TABLESPACE
b. CREATE USER
c. CREATE PROCEDURE (With Admin Option)
d. CREATE SEQUENCE (With Admin Option)
e. CREATE SESSION (With Admin Option)
f. CREATE TABLE (With Admin Option)
g. CREATE TRIGGER (With Admin Option)
h. CREATE VIEW (With Admin Option)

i. CTXSYS package object rights for CTX_DDL (With Admin Option)

Case 2:

1. Minimum Privileges for an Existing Tablespace and User:

If the client has already created the tablespace and the user and provides these existing user credentials in the Database user and cabinet user fields through OSA, the minimum privileges required for the provided DB user include:

a. CREATE PROCEDURE
b. CREATE SEQUENCE
c. CREATE SESSION
d. CREATE TABLE
e. CREATE TRIGGER
f. CREATE VIEW
g. CREATE JOB
h. CREATE TYPE
i. CTXSYS package object rights for CTX_DDL

NOTE:

For Creating a cabinet, avail the services of an Oracle DBA (Database Administrator) or of someone who has prior experience in creating an Oracle cabinet.

A normal user should be given the following rights to be able to create a cabinet:

- Cabinet Creation Rights
- Administration Rights

To create Oracle 11g Cabinet, Perform the following steps using **Enterprise Manager Console**.

1. Enter the Login Details in the “Oracle Enterprise Manager 11g” login screen.
2. Connect as SYSDBA for this operation.

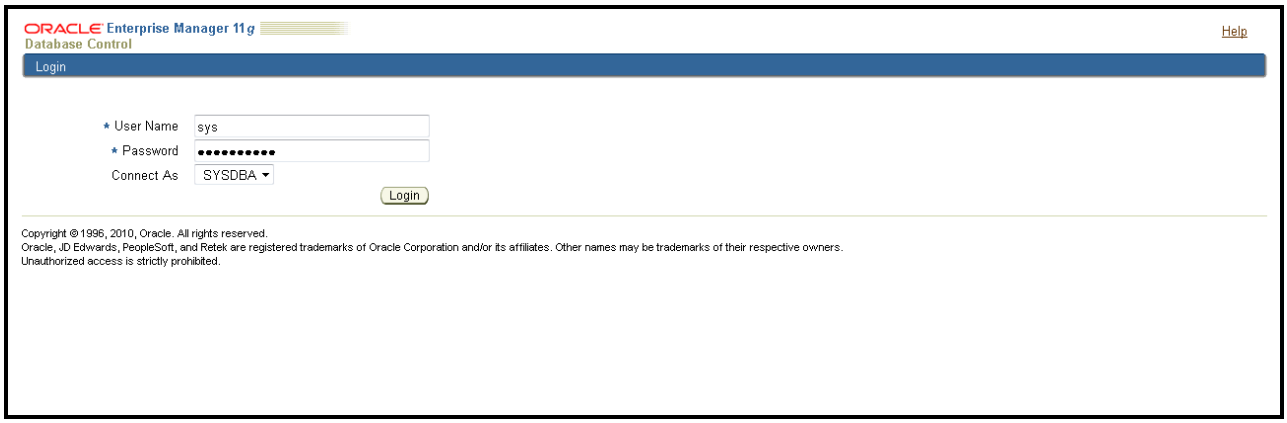


Figure 3.69

3. From the **Security** section, select **Users**.

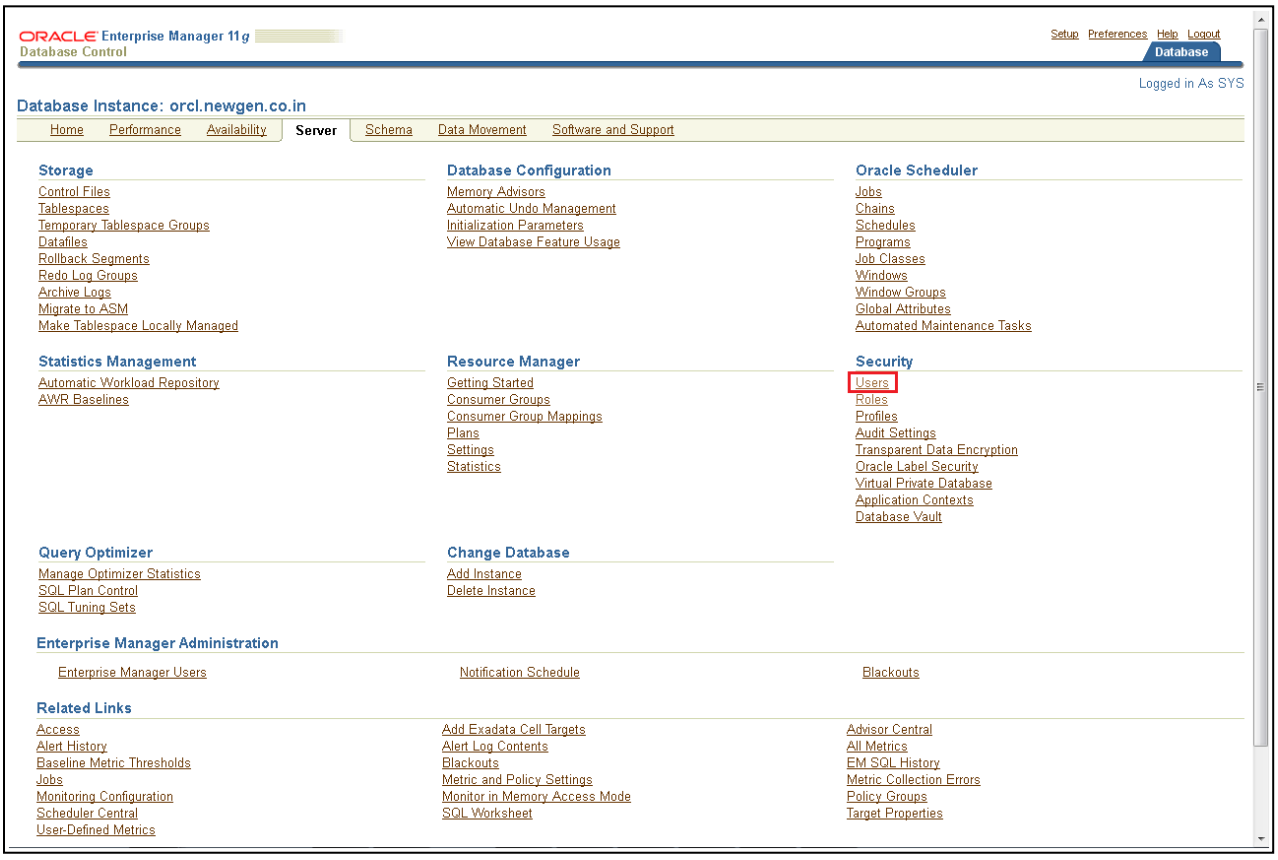


Figure 3.70

4. Users screen appears.
5. Click on **Create** button.

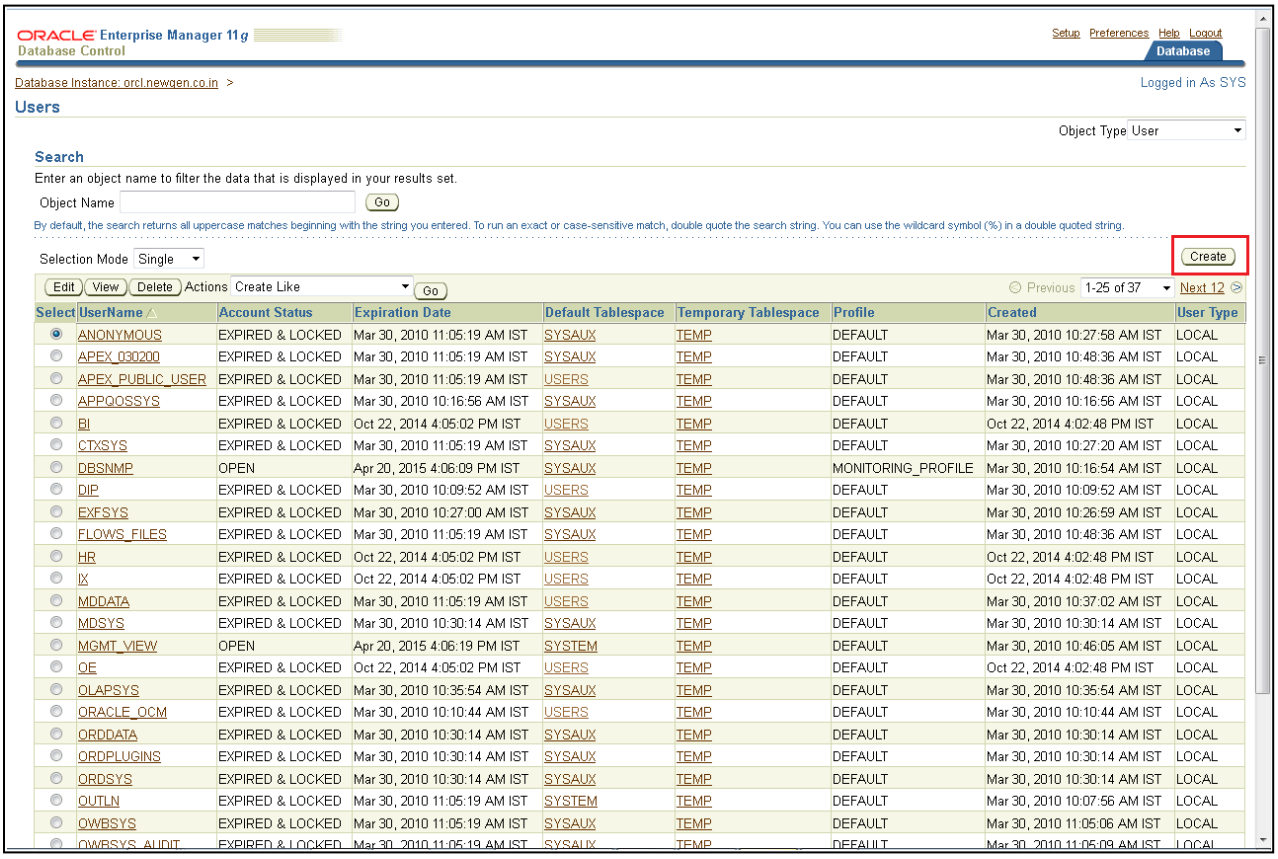


Figure 3.71

6. In the **General** tab, provide **Name** and **Password** of the user.

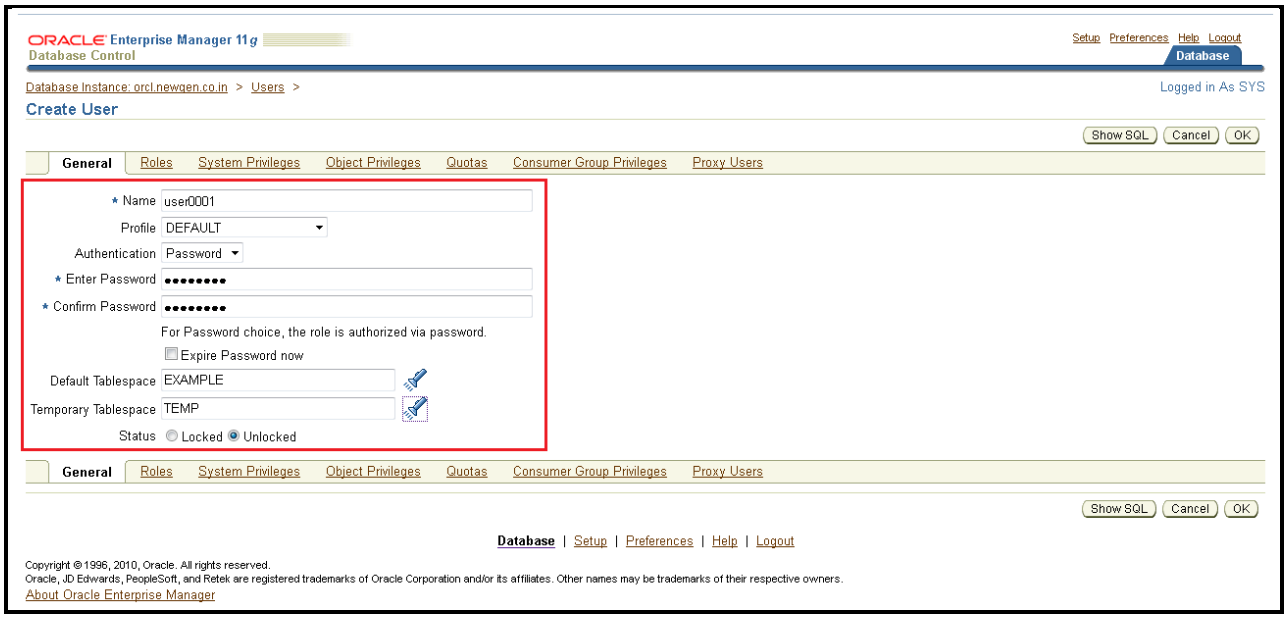


Figure 3.72

7. In **Default Tablespace** and **Temporary Tablespace**, search and select the required tablespace.

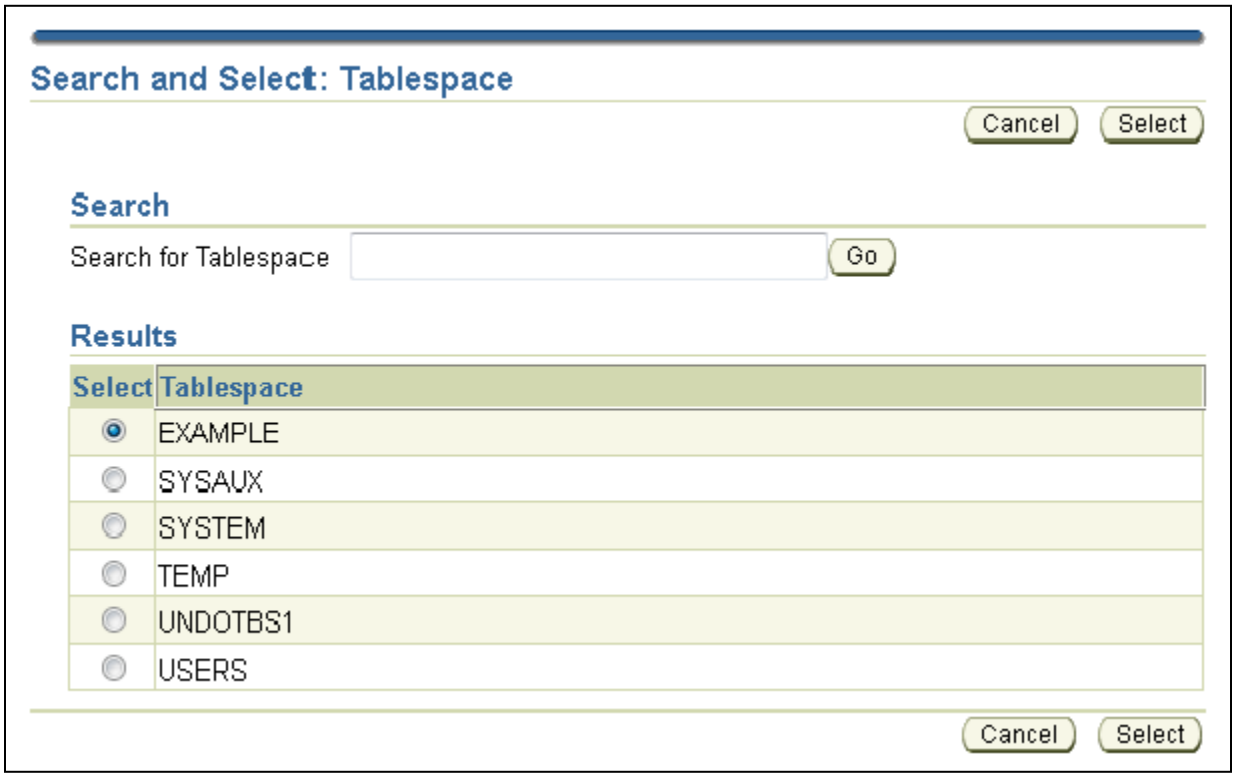


Figure 3.73

8. Select the **System Privileges** tab.
9. Click on **Edit List**.

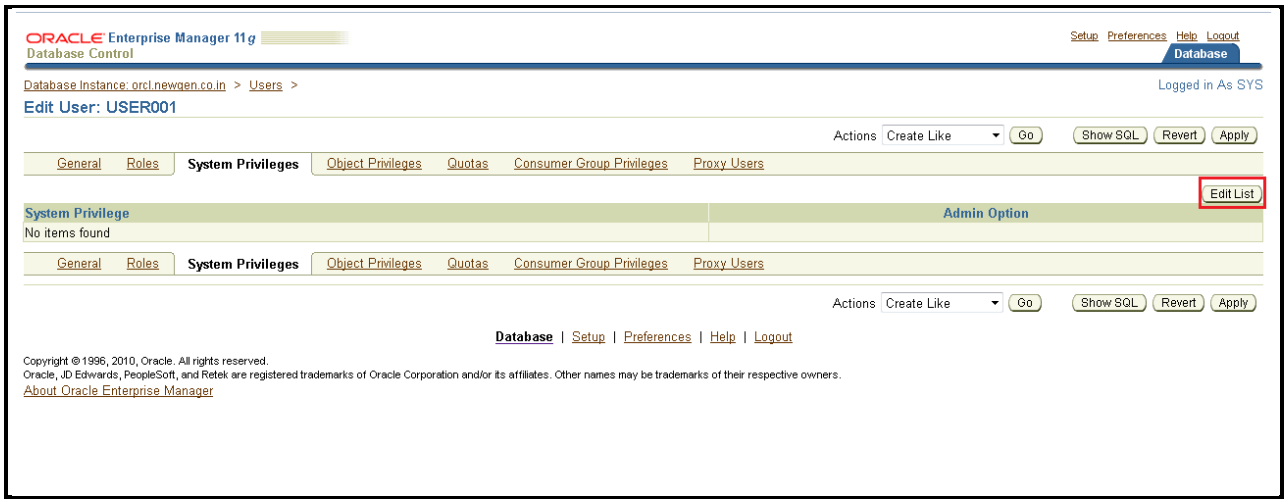


Figure 3.74

10. **Modify System Privilege** screen appears.

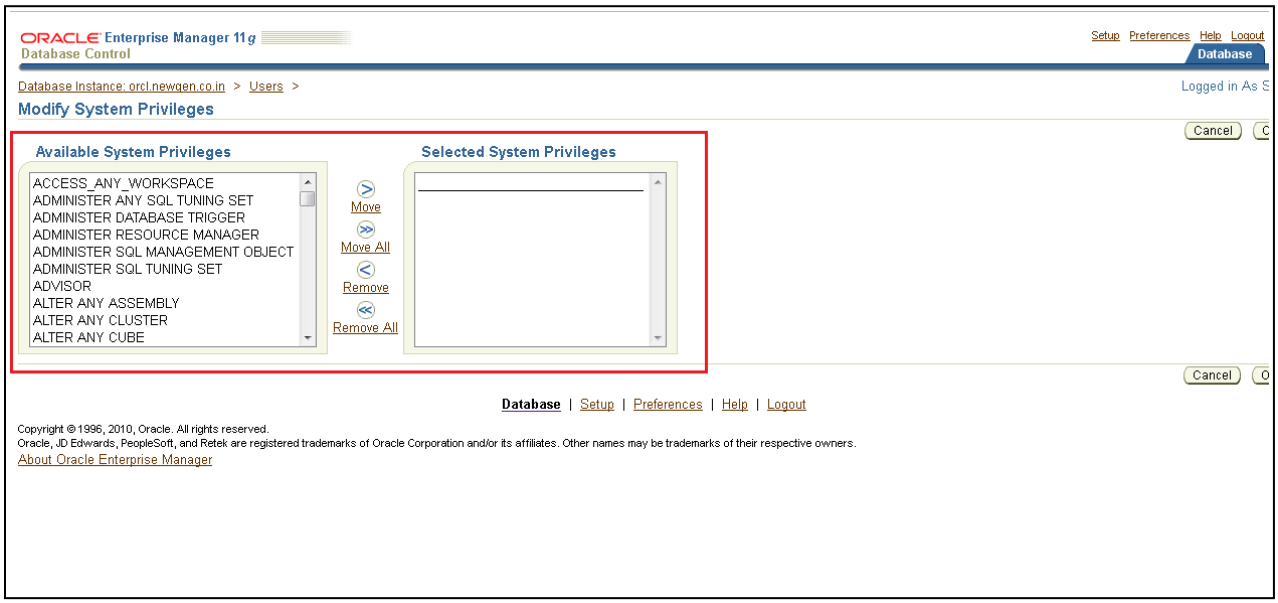


Figure 3.75

11. From **Available System Privileges**, move the following privileges to **Selected System Privileges**.
    a. CREATE PROCEDURE
    b. CREATE ANY TYPE-- WITH ADMIN OPTION

c. CREATE TABLESPACE

d. CREATE USER

e. CREATE PROCEDURE (With Admin Option)

f. CREATE SEQUENCE (With Admin Option)

g. CREATE SESSION (With Admin Option)

h. CREATE TABLE (With Admin Option)

i. CREATE TRIGGER (With Admin Option)

j. CREATE VIEW (With Admin Option)

k. CREATE JOB (With Admin Option)

l. CREATE TYPE (With Admin Option)

m. CTXSYS package object rights for CTX_DDL (With Admin Option)

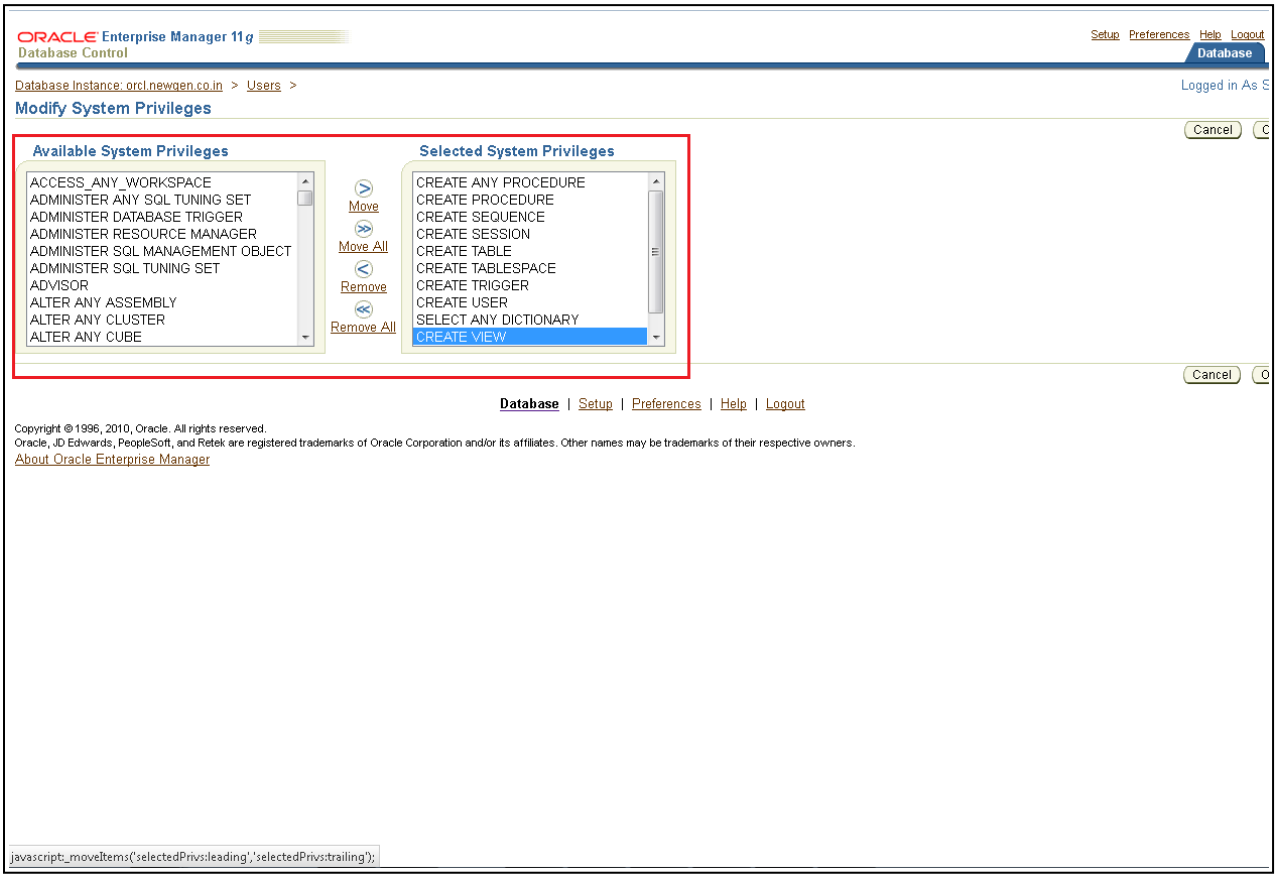


Figure 3.76

12. Once the necessary Privileges from Available System Privileges are moved to Selected System Privileges, click on **OK** button. The command returns to the System Privileges tab. Here, all the selected privileges are enlisted in the System Privileges list.

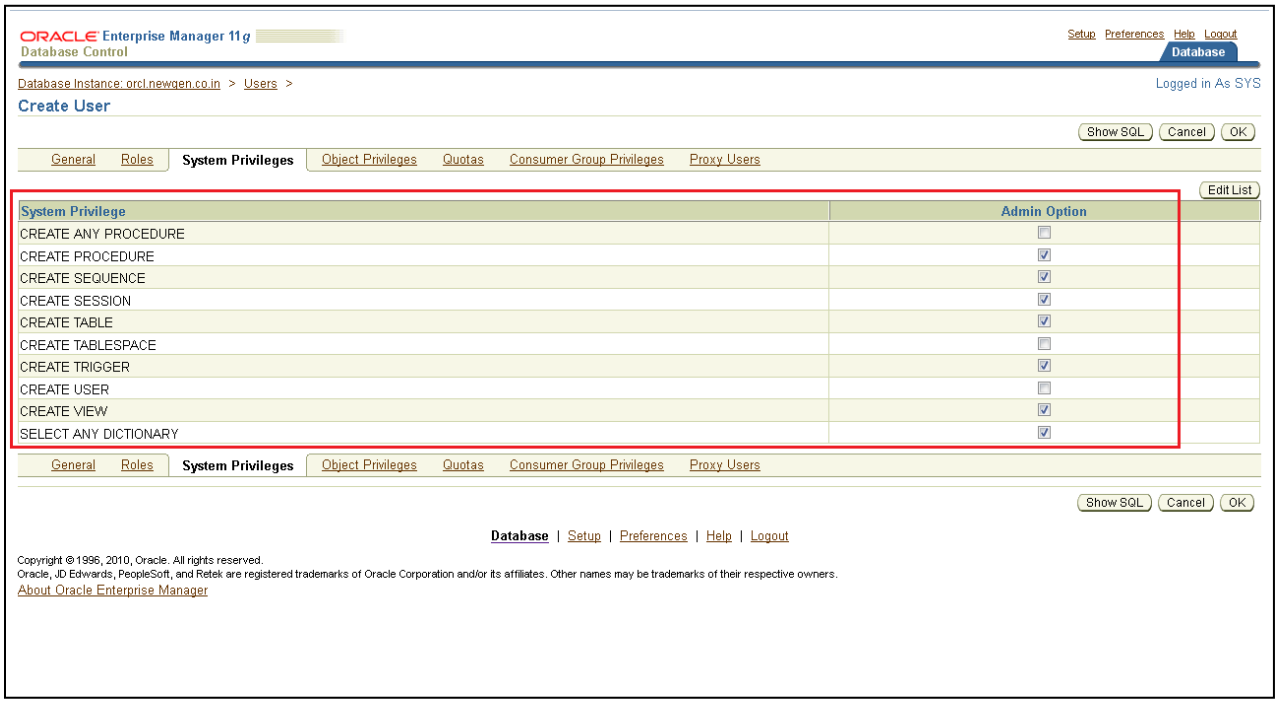


Figure 3.77

13. Select the **Object Privileges** tab.
14. From **Select Object Type** dropdown button, select the **Package** option.

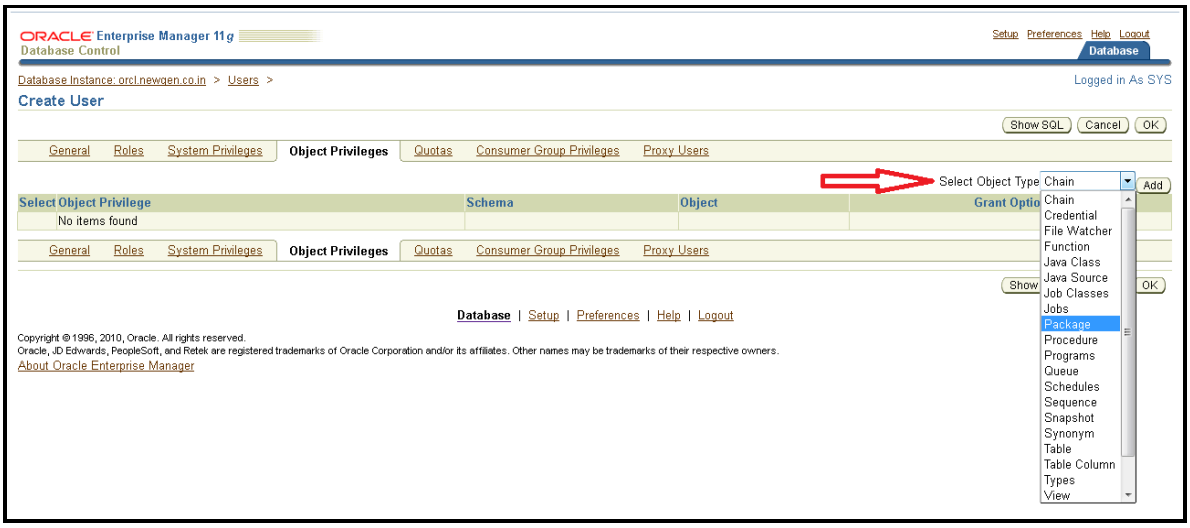


Figure 3.78

15. **Add Package Object Privileges** screen appears.

16. In the **Select Package Objects** section, click on **Torch** symbol.

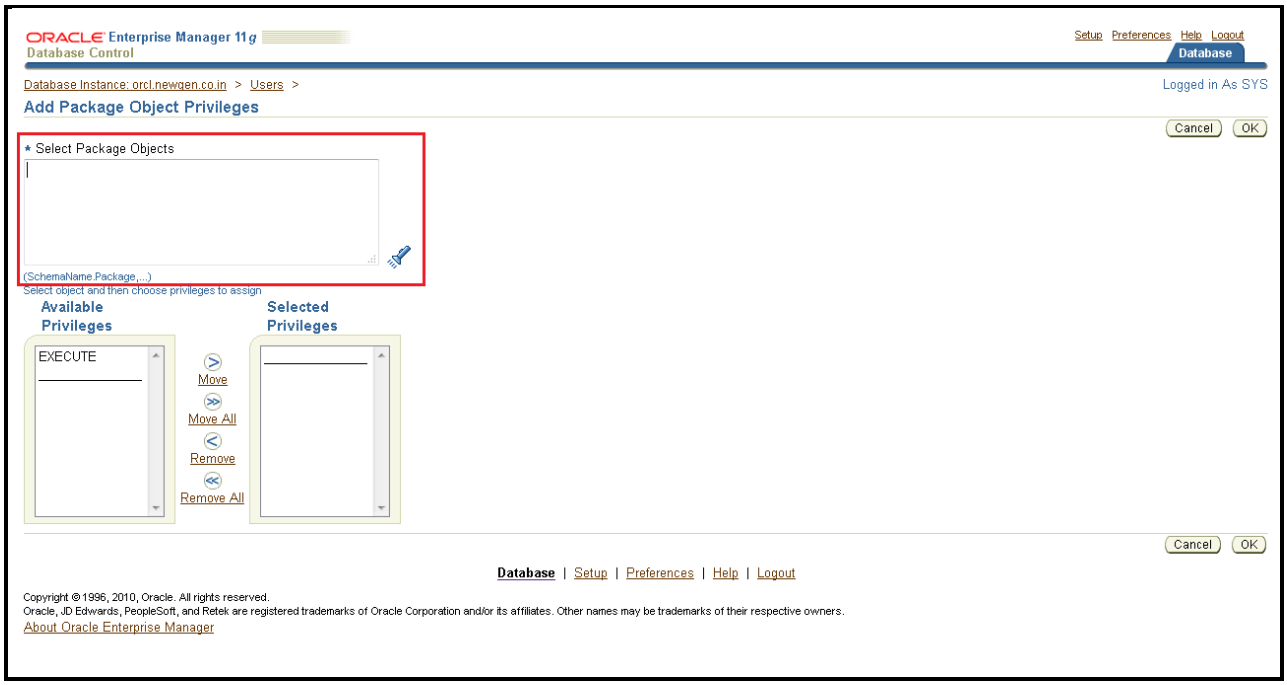


Figure 3.79

17. **Select Package Objects** dialog box appears.

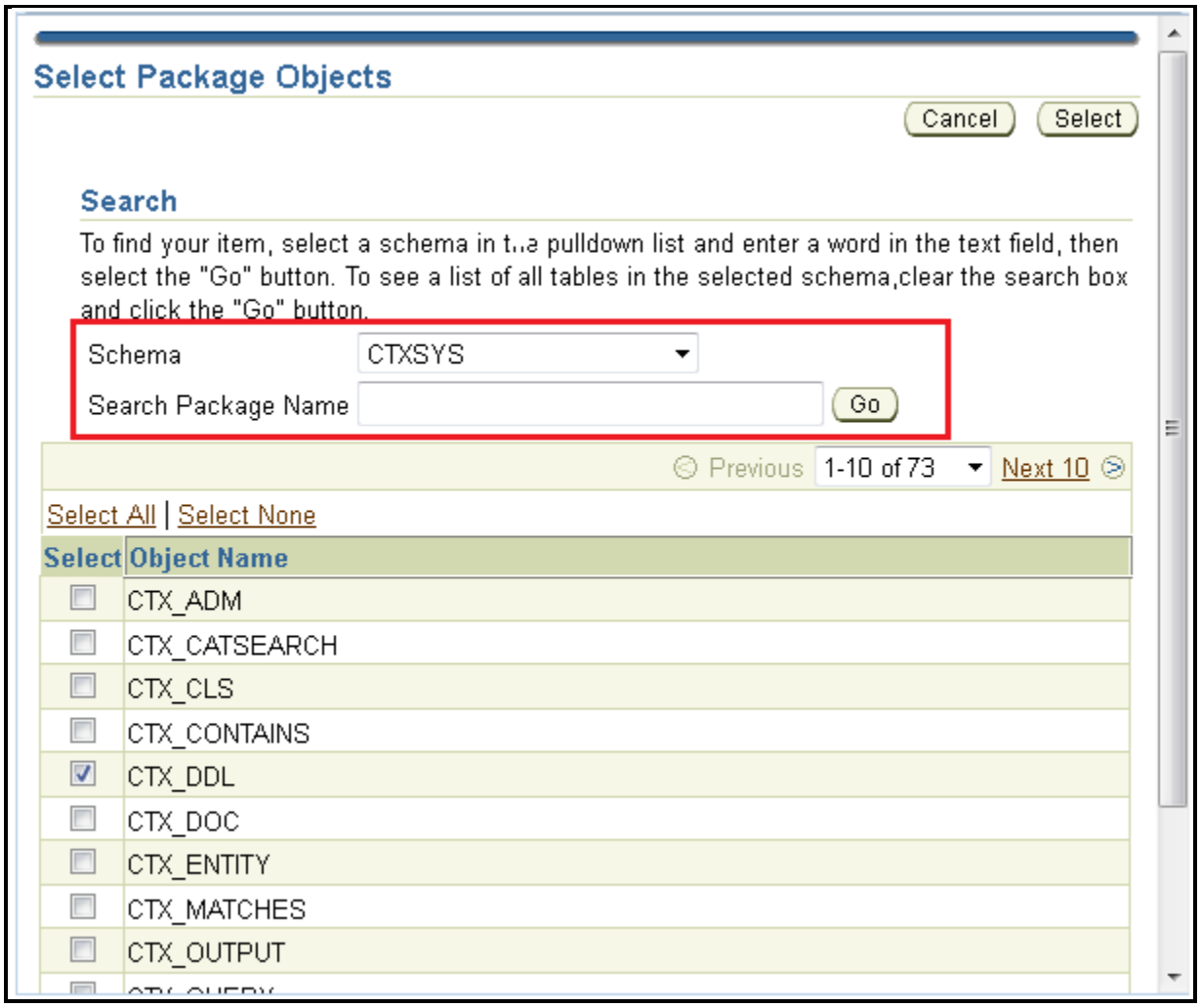


Figure 3.80

18. From the dropdown list (available in front of the Schema option), select **CTXSYS**.
19. From the Package Name list present below, select **CTX_DDL**.
20. Click on **Select** to save the changes made and then close the dialog box.
21. Else, click **Cancel** to close the Dialog Box, without saving the changes made.
22. **Add Package Object Privileges** screen appears.
23. From the **Available Privileges**, select **EXECUTE** and move it to **Selected Privileges**.
24. Click **OK** to save the changes made and get back to the Object Privileges Screen.

    Else, click **Cancel** to get back to the Object Privileges screen, without saving the made changes.

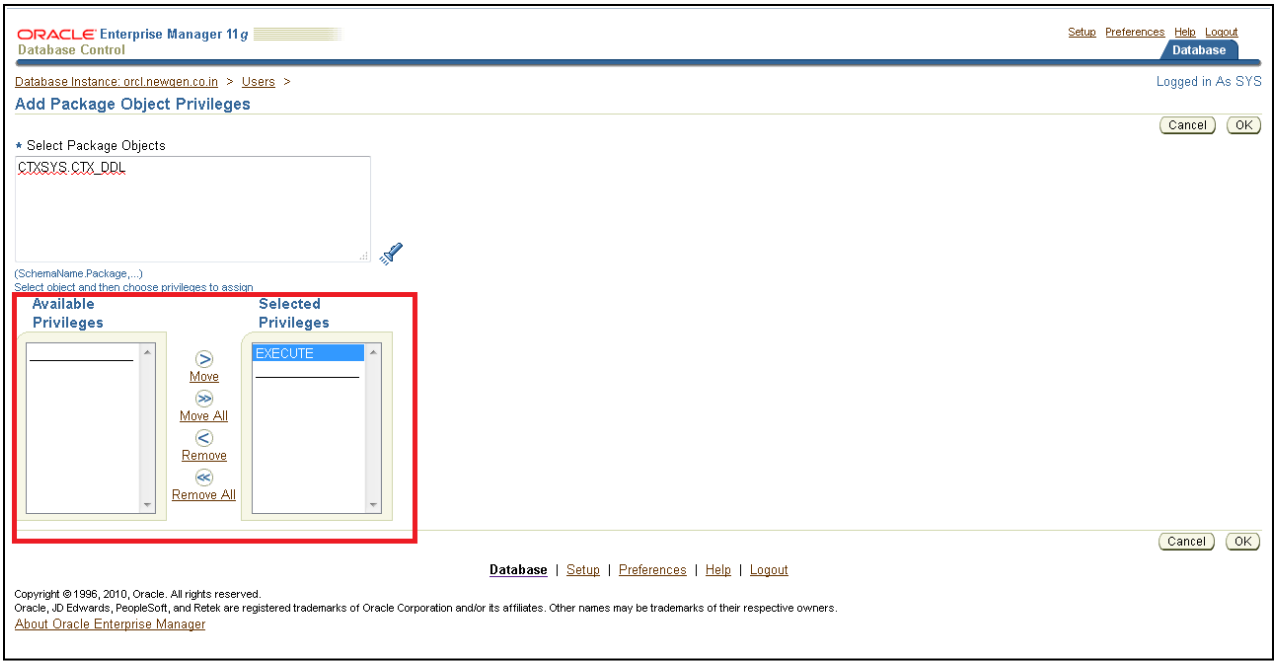


Figure 3.81

25. **Object Privileges** tab appears.

26. Click **OK** to save the changes made.

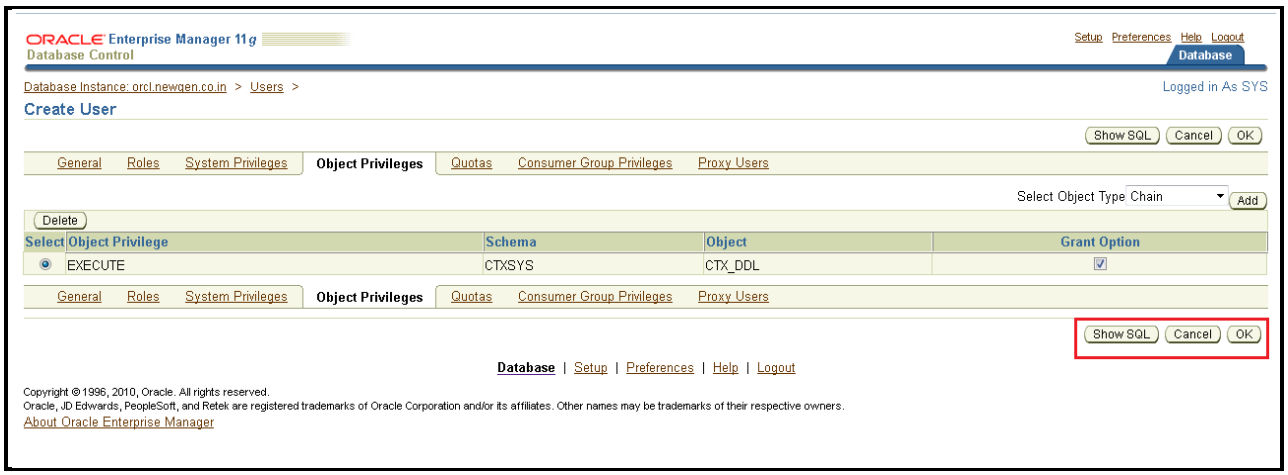


Figure 3.82

27. **Users** Screen appears.

28. Select the required user from the list of **UserName** and click on **Create** to create the Oracle user.

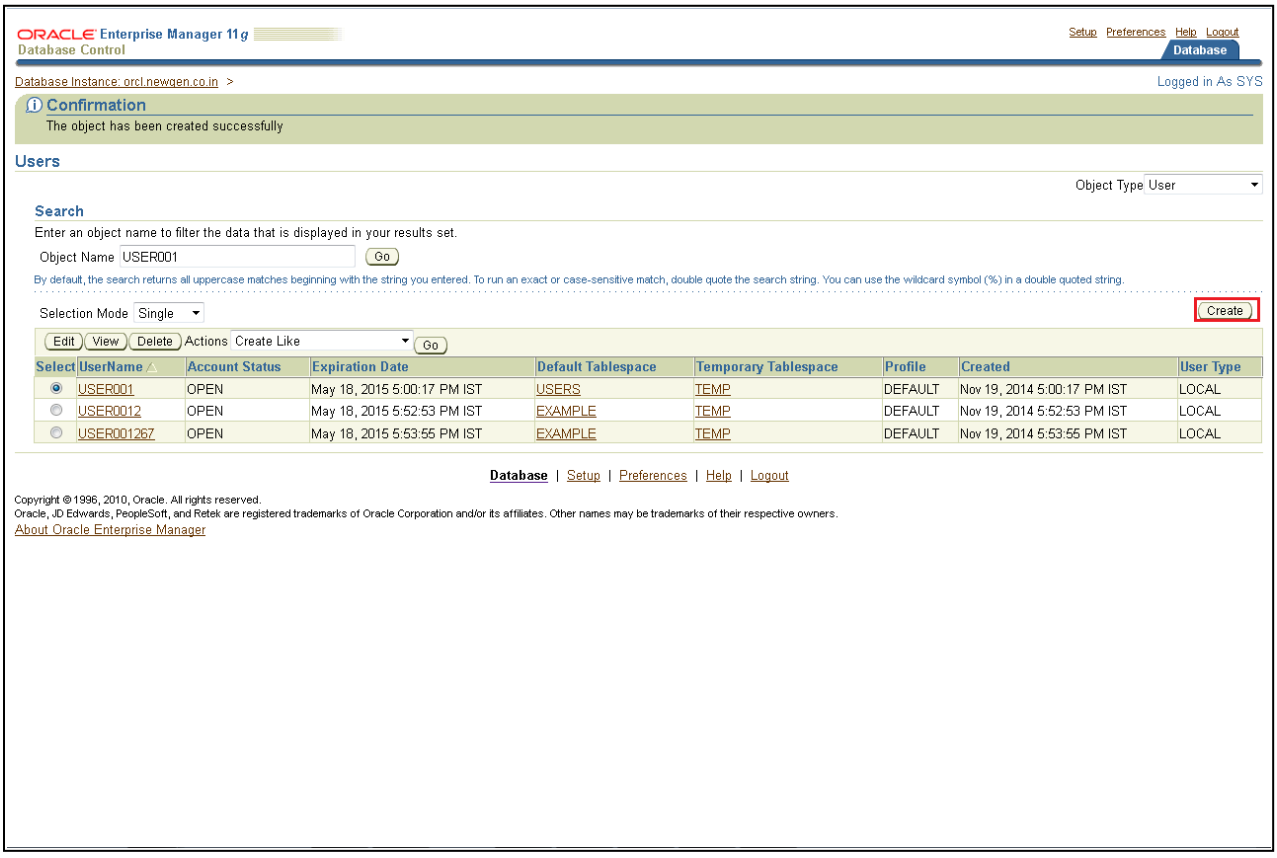


Figure 3.83

29. Use the above-created user for creating cabinets.

3.2.8 Creating a PostgreSQL Database Cabinet

Using Superuser

To create a PostgreSQL database cabinet:

1. Select the **PostgreSQL** database option from the **Database Type**.

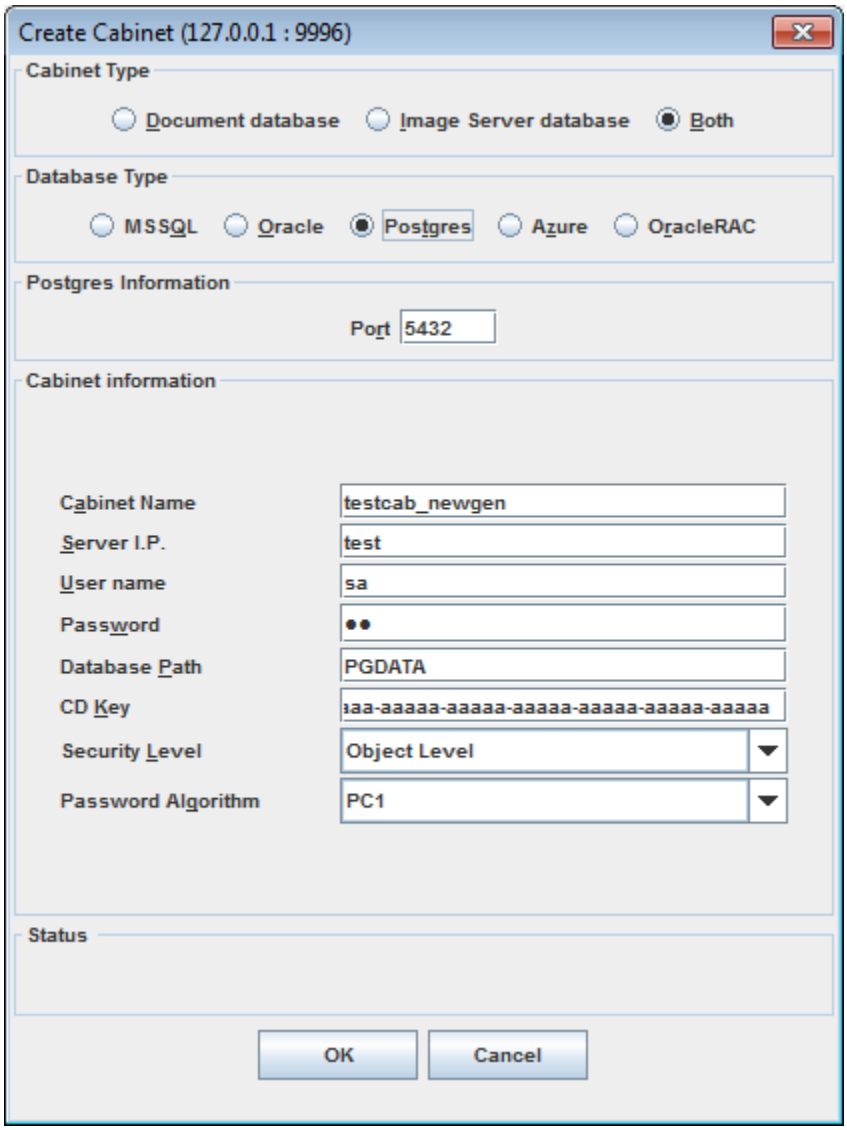


Figure 3.84

2. Select the **Enable FTS** option in the PostgreSQL information area to enable the FTS.
3. Specify the initial database size in **Device Size** textbox.
4. Specify the initial log size in **Log Size** textbox.

5. Specify the cabinet information in the various textboxes of the Cabinet Information area:
    i. Specify the cabinet name in the **Cabinet Name** textbox.
    ii. Specify the server name (name of the machine where the PostgreSQL server is running) in the **Server Name** textbox.
    iii. Specify the username in the **User name** textbox.
    iv. Specify the password in the **Password** textbox.

NOTE:

The database (DAT) file is formed on the computer that we specify in the Server Name textbox i.e. the computer where the PostgreSQL Server is installed.

---

    v. Specify the CD key in the **CD Key** textbox.
    vi. Select the required security level from the **Security Level** dropdown list. Right now, there are two levels of security:
        - **Object Level Security**: This means that all the rights and privileges are assigned to all the objects of OmniDocs.
        - **Cabinet Level Security**: This means that all the rights and privileges are assigned at the Cabinet-level.
6. Click the **OK** button to create the cabinet as per the requirements.

    Else, click **Cancel** button to close the **Create Cabinet** dialog box.

Using a Normal User: Use **pgAdmin** and perform the following steps:

1. Select the particular PostgreSQL Server on the left panel and expand it.

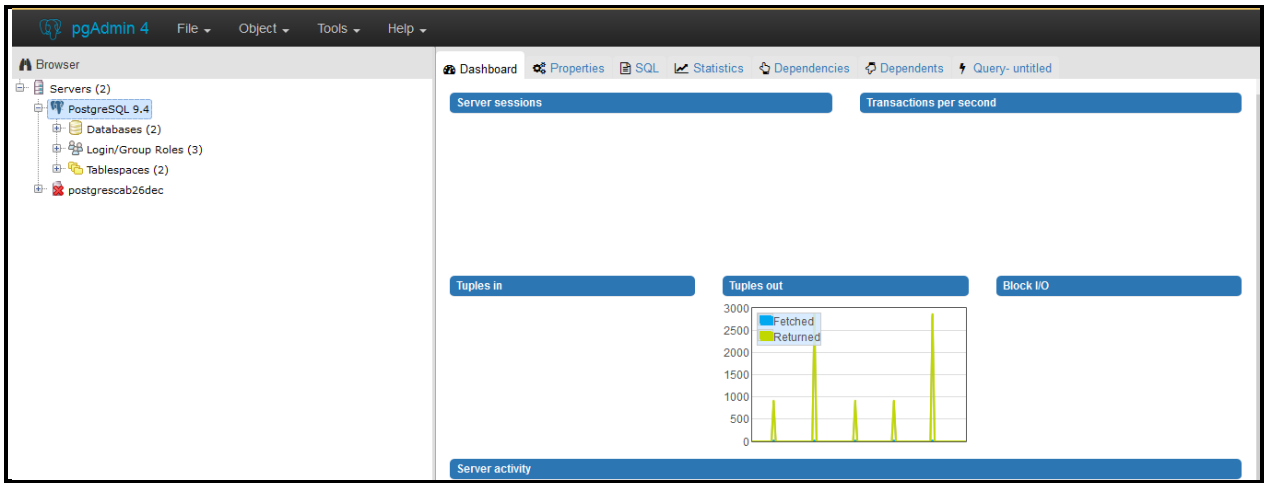


Figure 3.85

2. Expand **Login/Group Role**

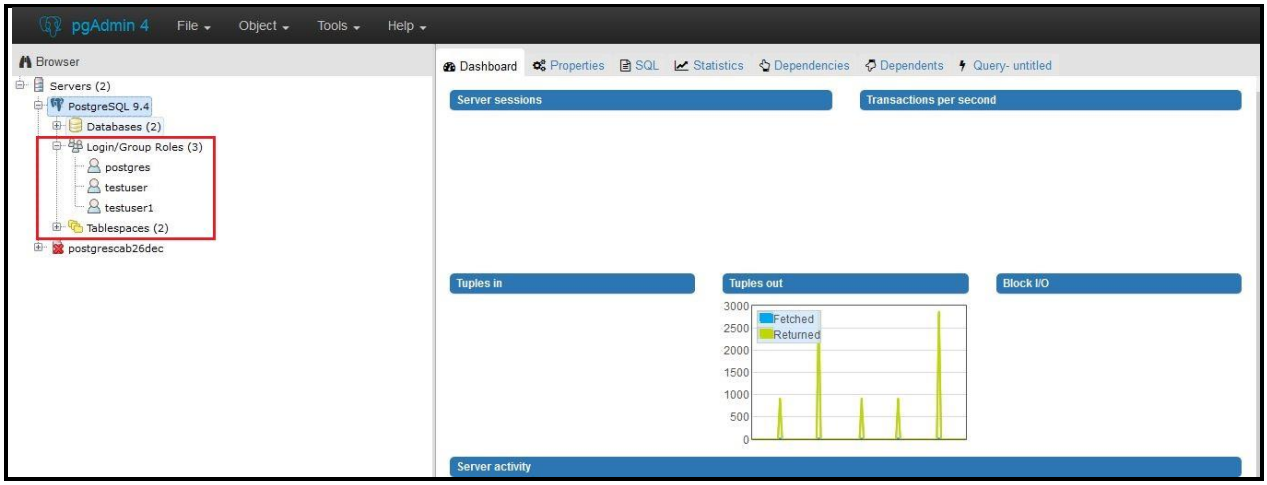


Figure 3.86

3. Select **Logins/Group Roles** and then do a right-click on it. Click on **Create -> Login/Group Role** from the pop-up menu.

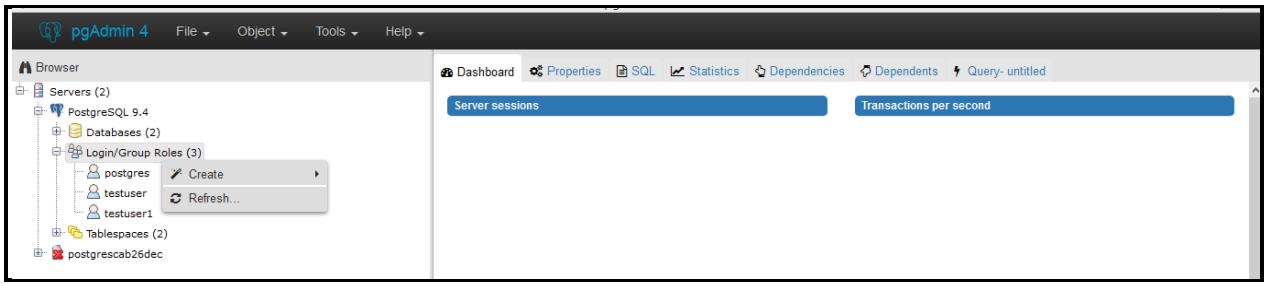


Figure 3.87

4. In the Create-Login/Group Role - New window, specify the **Name and Comments**.

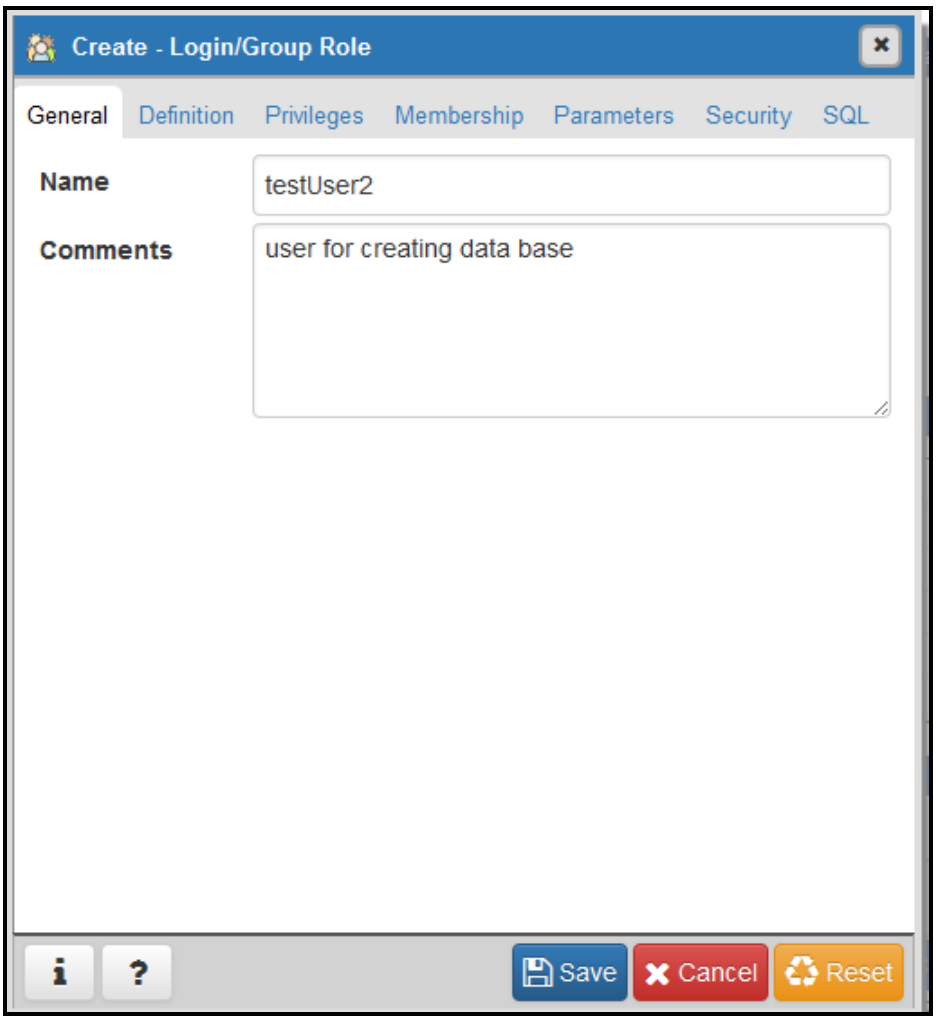


Figure 3.88

5. Click on **Definition** Tab. Specify the **Password** of the user, **Account expiry** date, and **Connection limit**.

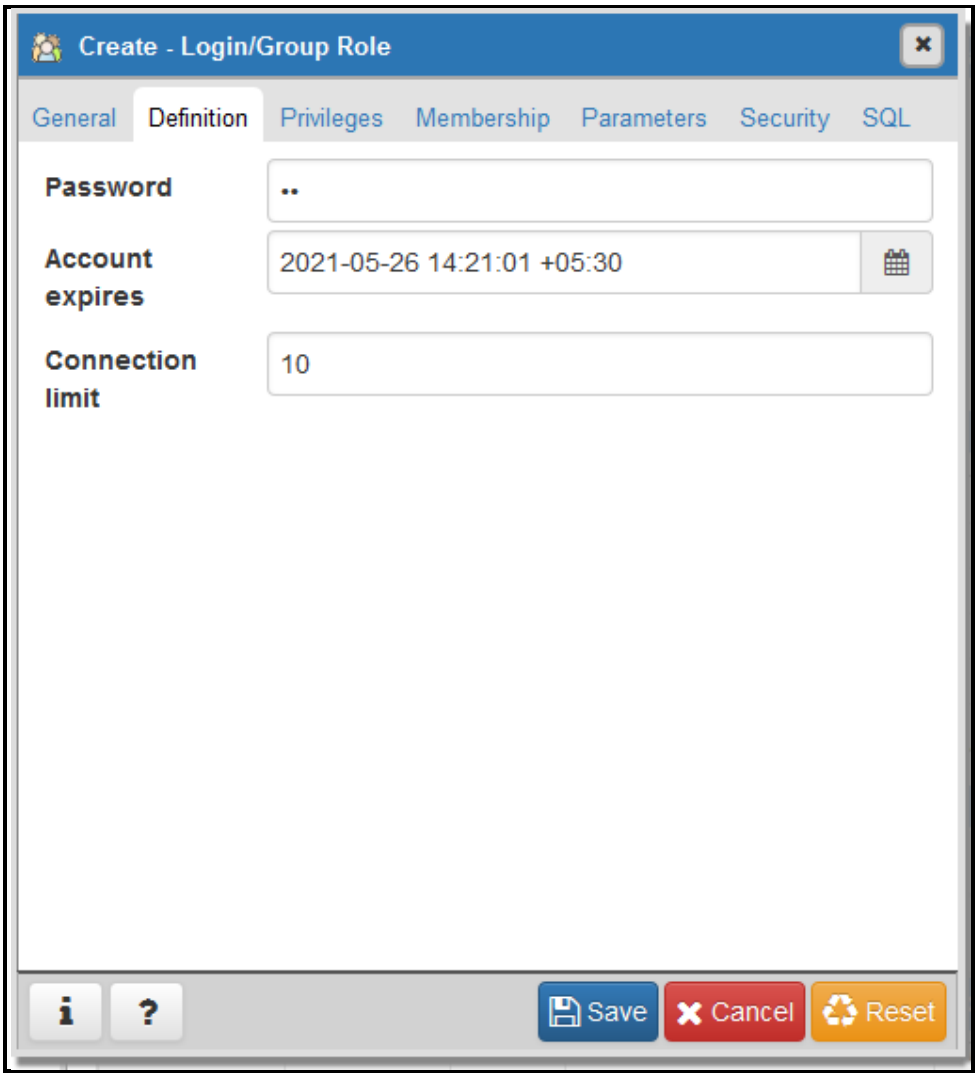


Figure 3.89

6. Click on **Privileges** Tab and specify the below privileges:

    - Can Login – yes
    - Create Data Base- Yes

Figure 3.90

7. In the Create-Login/Group Role - New window, click on **Membership** Tab, select the "**postgres"** Role from **Roles** Dropdown list.

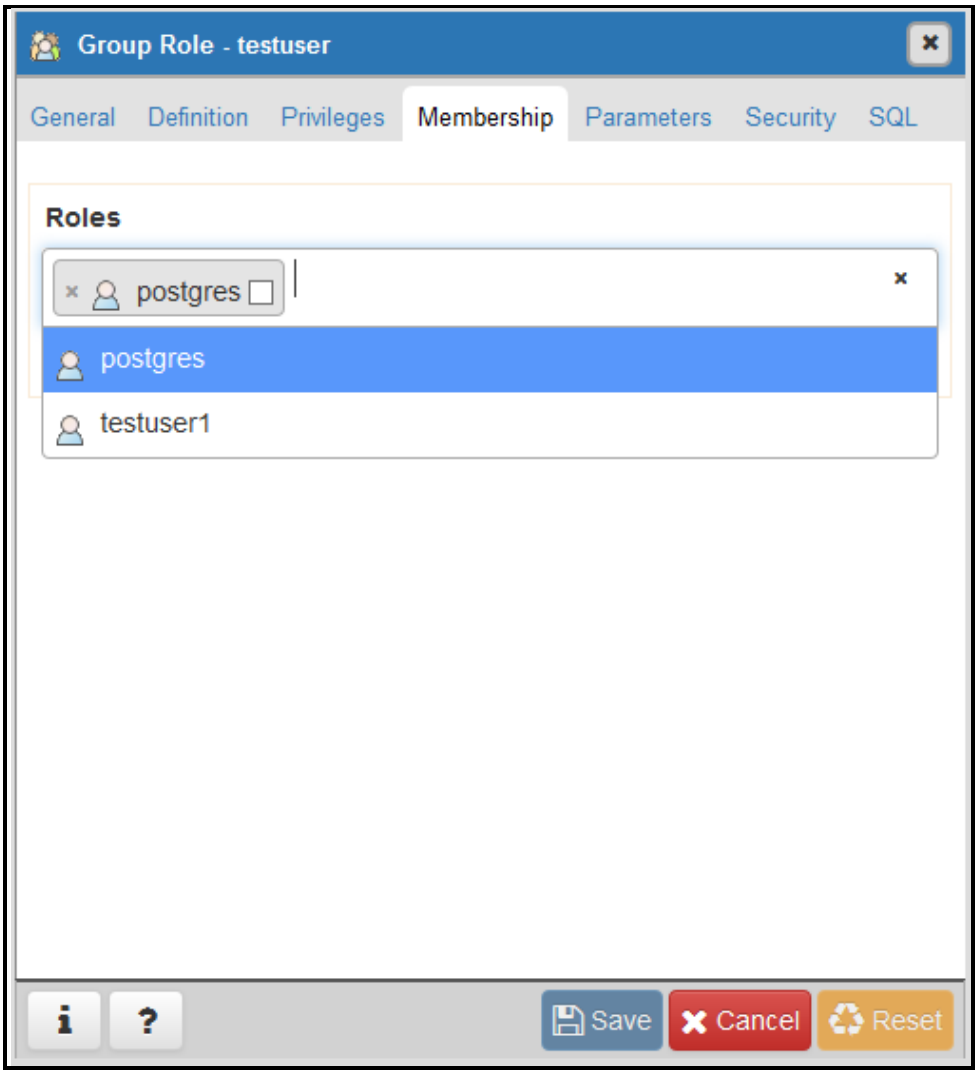


Figure 3.91

8. In the Create-Login/Group Role - New window, Click on **Save** Button. User will be created successfully and it will show in the left panel Login/Group Role.

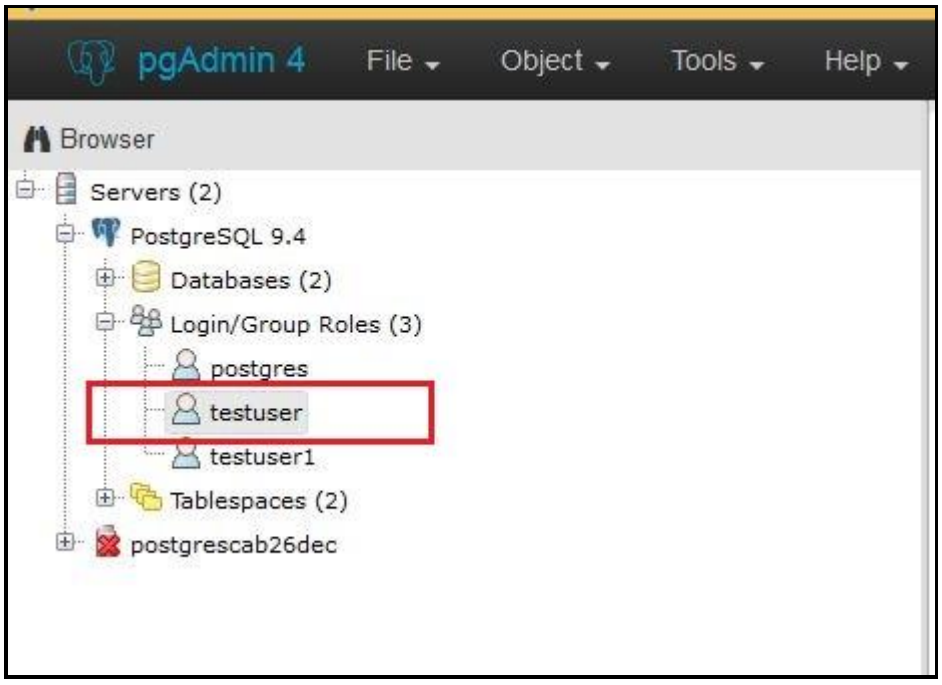


Figure 3.92

9. Now cabinets should be created using the above-created database user.

NOTE:

For Creating a cabinet, avail the services of a DBA (Database Administrator) or of someone who has prior experience in creating a PostgreSQL cabinet.

3.2.9 Creating a Microsoft Azure Database Cabinet

Using Superuser

To create a **Microsoft Azure** database cabinet:

1. Select the **Azure** database option from the **Database Type**.

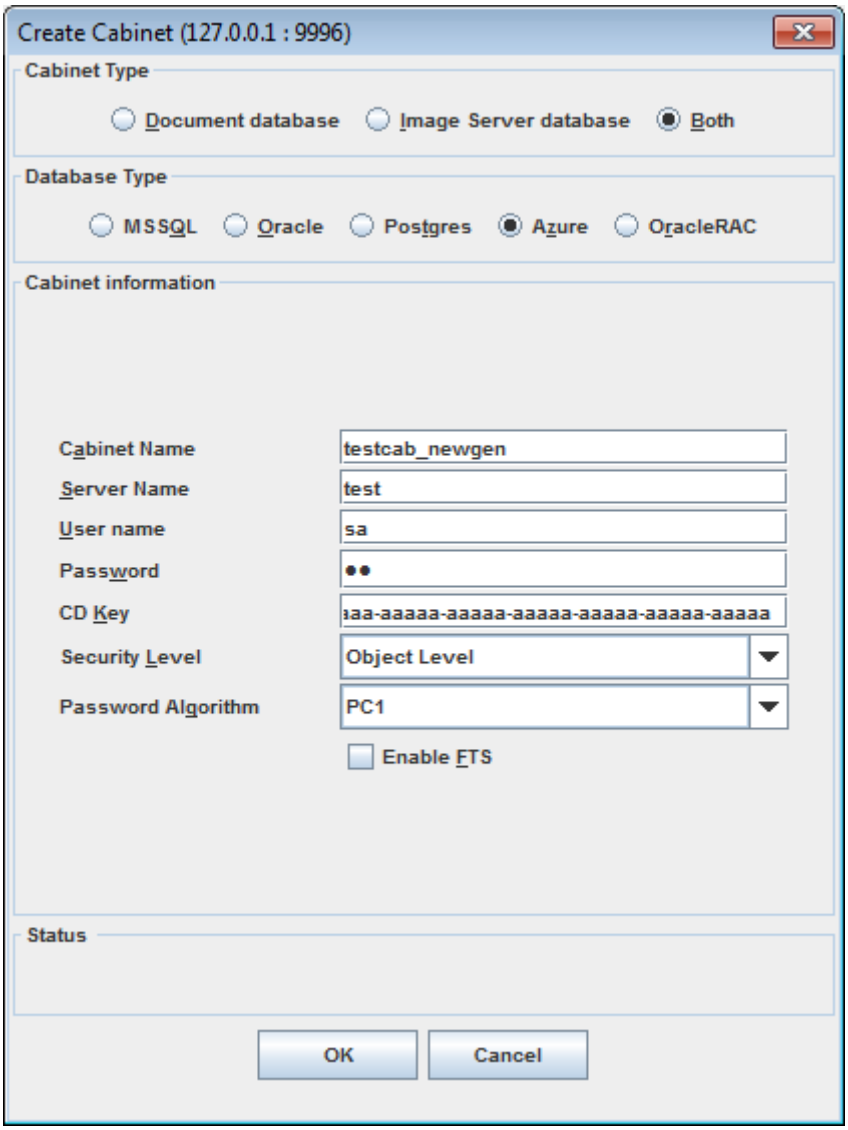


Figure 3.93

2. Select the **Enable FTS** option in the Azure information area to enable the FTS.
3. Specify the initial database size in **Device Size** textbox.
4. Specify the initial log size in **Log Size** textbox.

5. Specify the cabinet information in the various textboxes of the Cabinet Information area:
    i. Specify the cabinet name in the **Cabinet Name** textbox.
    ii. Specify the server name (name of the machine where the Azure server is running) in the **Server Name** textbox.
    iii. Specify the username in the **User name** textbox.
    iv. Specify the password in the **Password** textbox.

NOTE:

The database (DAT) file is formed on the computer that we specify in the Server Name textbox i.e. the computer where the Azure Server is installed.

---

    v. Specify the CD key in the **CD Key** textbox.
    vi. Select the required security level from the **Security Level** dropdown list. Right now, there are two levels of security:
        - **Object Level Security**: This means that all the rights and privileges are assigned to all the objects of OmniDocs.
        - **Cabinet Level Security**: This means that all the rights and privileges are assigned at the Cabinet-level.
6. Click the **OK** button to create the cabinet as per the requirements.

    Else, click **Cancel** button to close the **Create Cabinet** dialog box.

3.2.10 Creating an Oracle RAC Database Cabinet

For the cabinet creation on Oracle RAC, we need to provide the RAC net services name as a part of the JDBC URL unlike the IP, Port, and Service name for a standalone Oracle server.

We have a separate option in OSA for creating the cabinet on Oracle RAC, named OracleRAC. You have to choose the OracleRAC option and then provide the RAC net services name.

Steps to create a cabinet:

1. In Create Cabinet dialog box, select **Database Type** as **OracleRAC**.

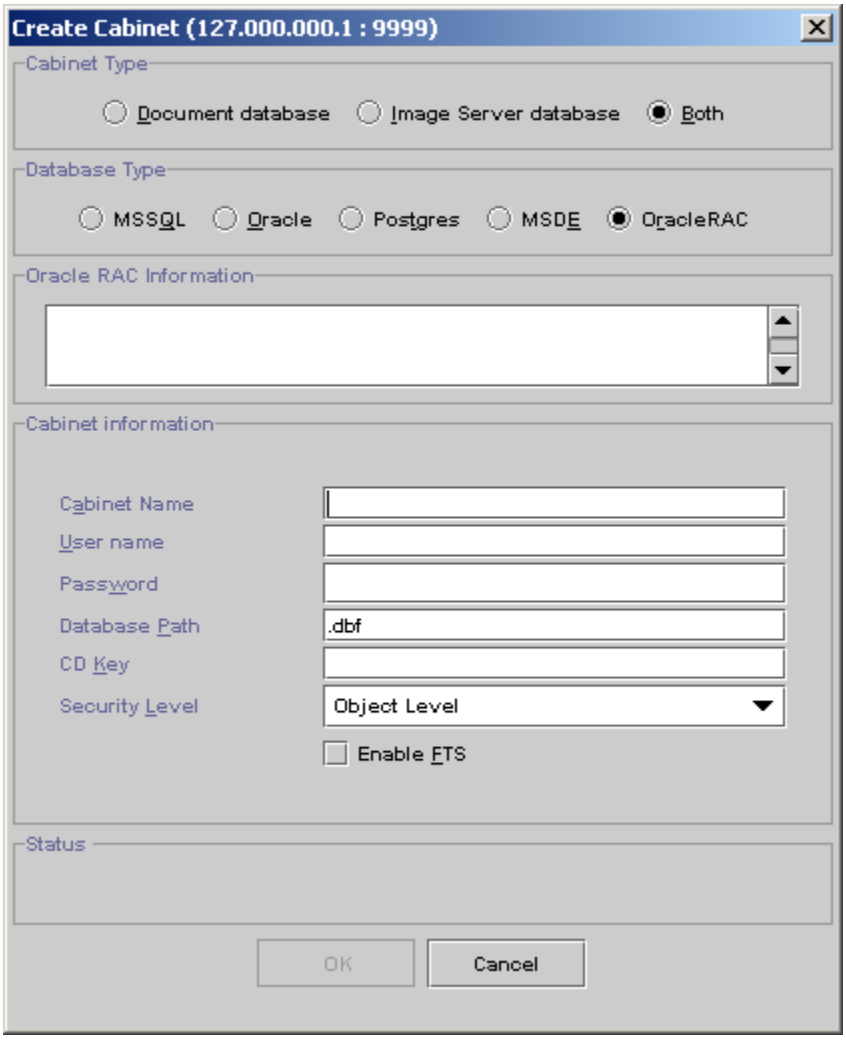


Figure 3.94

2. In **Oracle RAC Information** textbox, copy the TNS (provide RAC net services name) and paste it into the panel.

   Example: If the TNS entry is defined by:

```
FCCON =
(DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.18)(PORT = 1728))
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.11)(PORT = 1728))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = fccon)
    )
  )
```

   We have to copy the entry starting from **DESCRIPTION**, i.e., copy only the following part and paste it in the **Oracle RAC Information** textbox.

```
(DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.138)(PORT = 1726))
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.141)(PORT = 1726))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = fccon)
    )
  )
```

3. Fill in the other details accordingly and click on **OK**.

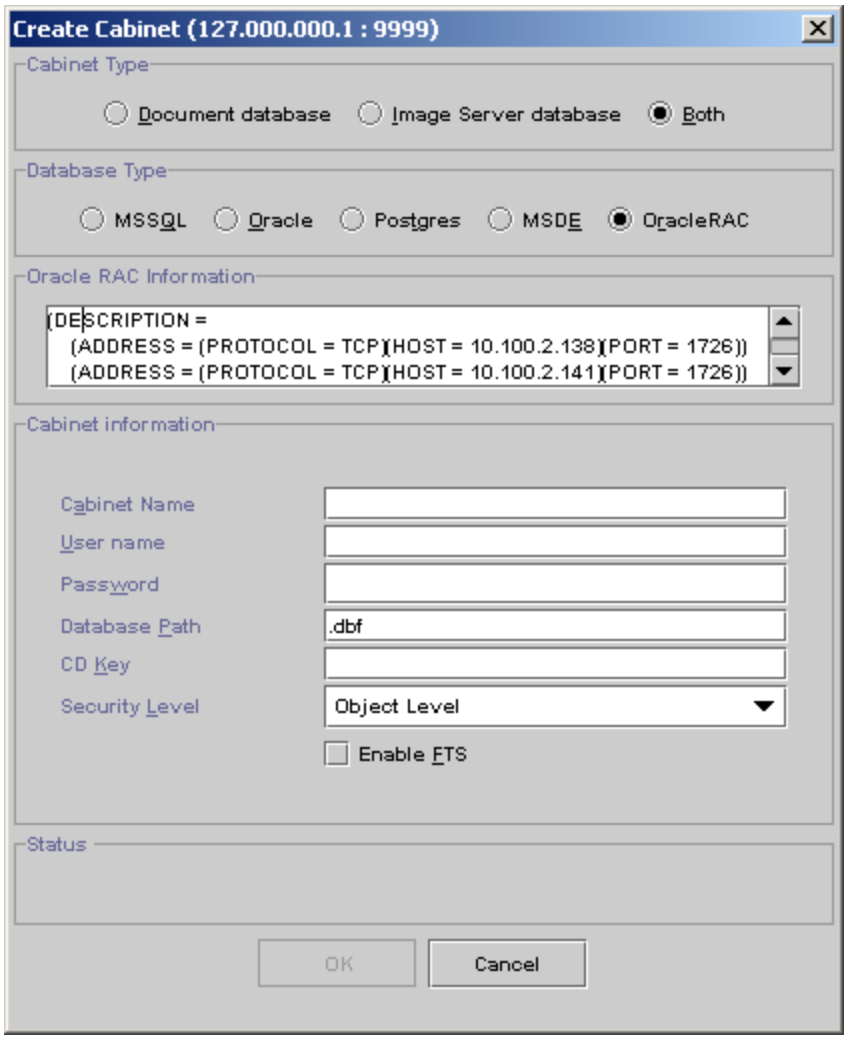

Create Cabinet (127.000.000.1 : 9999)
Cabinet Type
Document database
Image Server database
Both
Database Type
MSSQL
Oracle
Postgres
MSDE
OracleRAC
Oracle RAC Information
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.138)(PORT = 1726))
(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.141)(PORT = 1726))
Cabinet information
Cabinet Name
User name
Password
Database Path
.dbf
CD Key
Security Level
Object Level
Enable FTS
Status
OK
Cancel

Figure 3.95

Associating Cabinet

1. Open Associate a Cabinet dialog box.

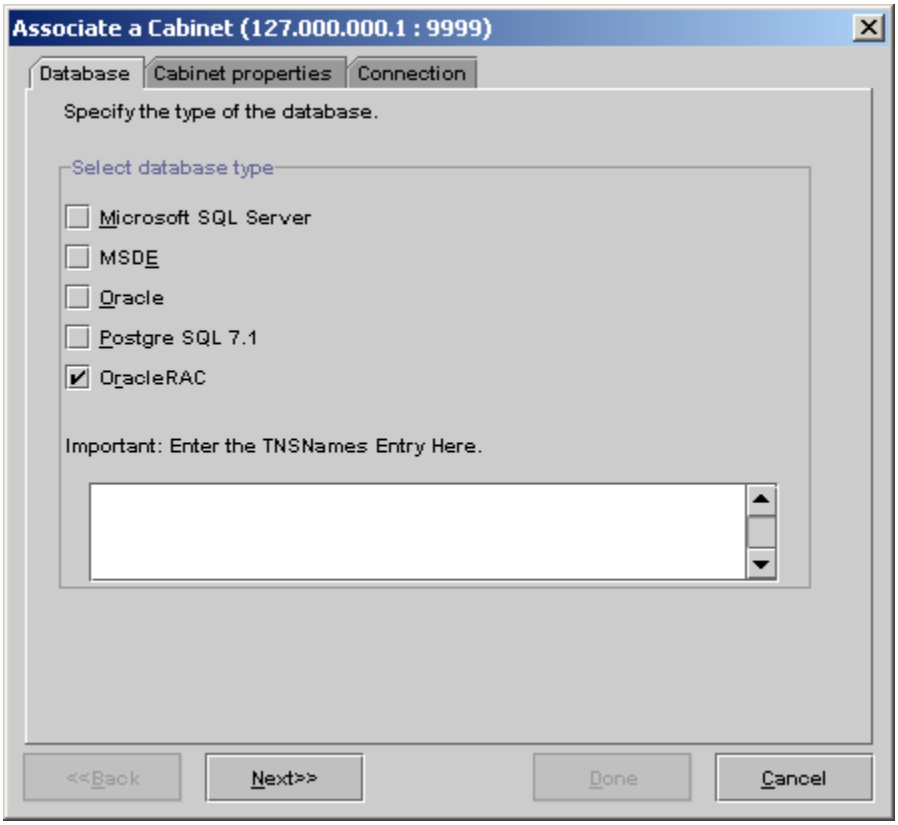


Figure 3.96

2. In **Important: Enter the TNSNames Entry Here** textbox, copy the above-given entry.

```
(DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.138)(PORT = 1726))
    (ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.141)(PORT = 1726))
    (LOAD_BALANCE = yes)
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = fccon)
    )
  )
```

3. Click on **Next**.

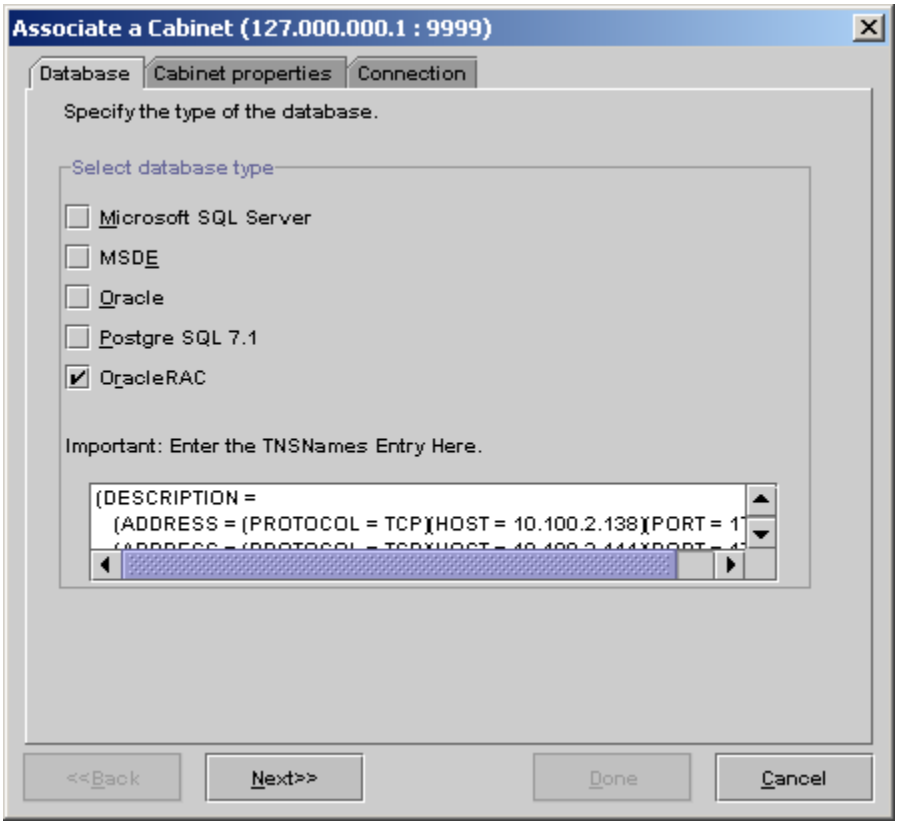


Figure 3.97

4. Cabinet properties tab appears.

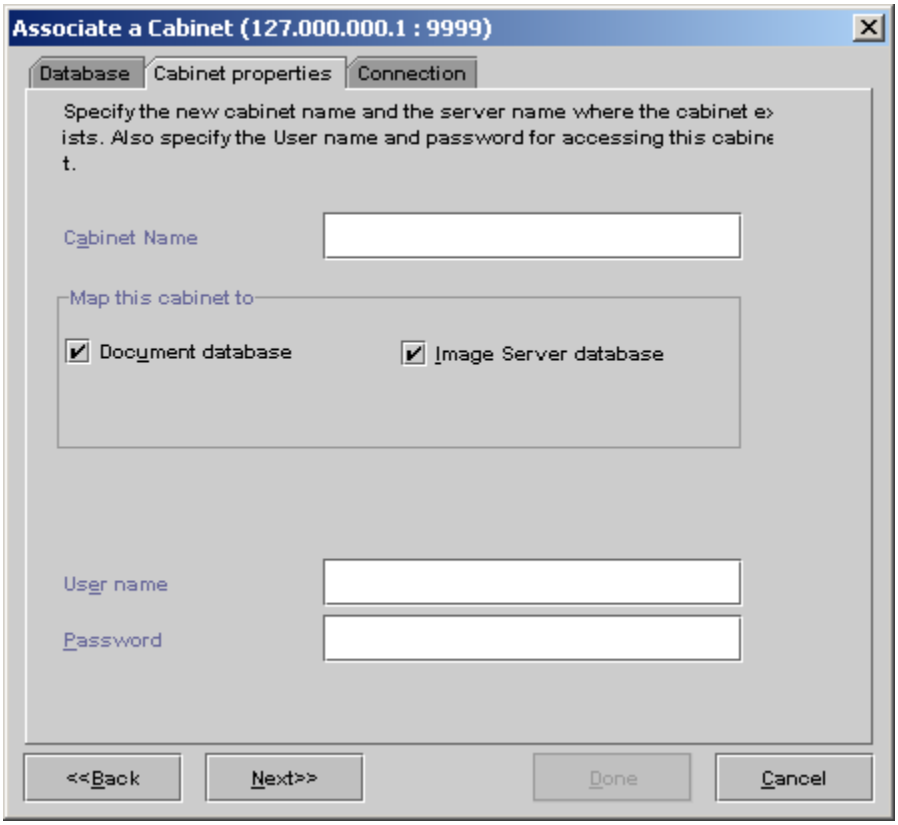


Figure 3.98

5. Enter the **Cabinet Name**, **User name,** and **Password**.
6. Click on **Next** to go to the Connection tab. Here, specify the Connection relative details and click on **DONE** to save the specified details.

Creating Data Source

Follow OmniDocs installation manual for the data source creation for different application servers, and provide the **JDBC-Connection URL** as below (depending on the RAC net services name).

Example: For the above RAC net services name, below will be the JDBC-URL:

jdbc:oracle:thin:@(DESCRIPTION =(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.138)(PORT = 1726))(ADDRESS = (PROTOCOL = TCP)(HOST = 10.100.2.141)(PORT = 1726))(LOAD_BALANCE = yes)(CONNECT_DATA =(SERVER = DEDICATED)(SERVICE_NAME = fccon)))

3.2.11 Associating a Cabinet

The JTS server must be stopped before associating a cabinet.

A cabinet can be associated in three ways:

A. Using Superuser

B. Using Normal user to associate an MSQL 2008 cabinet

C. Using Normal user to associate an MSSQL 2012 cabinet

A. **Using Superuser**

Cabinet Association can be done in two ways:

a. By using **Superuser** like '**sa'** (SQL) or '**sys'** (Oracle).

b. By using a **normal user** with cabinet creation rights.

To associate a selected cabinet:

1. Click **Associate** button.
2. **Associate a Cabinet** dialog box is invoked.
3. **Associate a Cabinet** dialog box has three tabs:
   - Database tab
   - Cabinet properties tab
   - Connection tab

Using the Database tab

1. Click the **Database** tab (Database tab is shown by default when you click the **Associate** button).

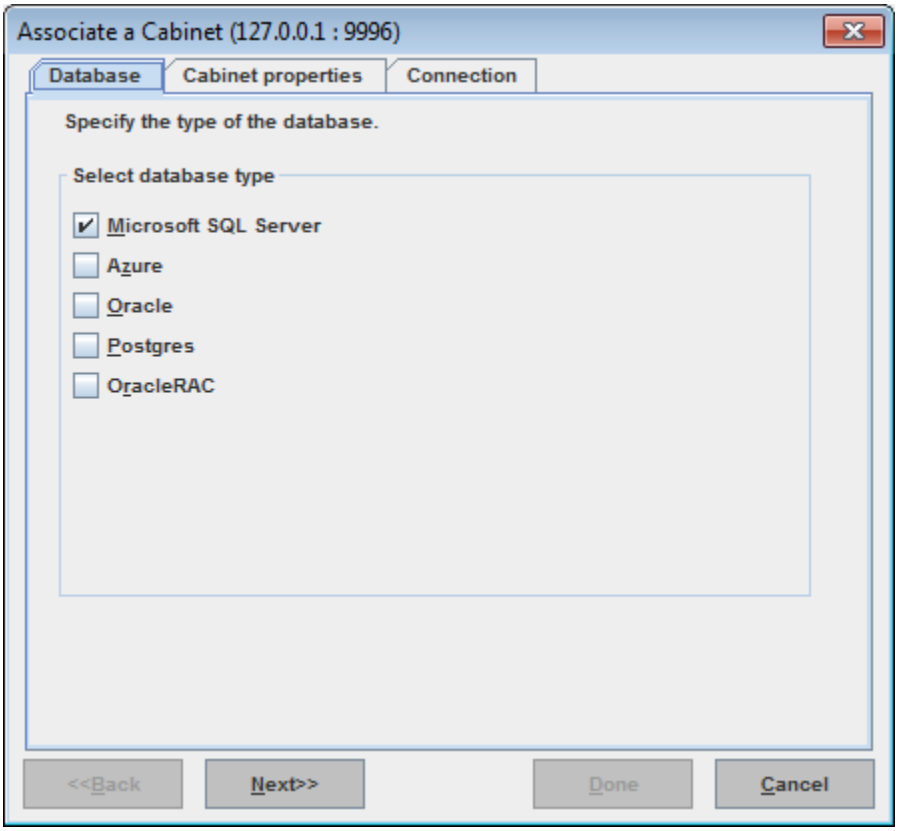


Figure 3.99

2. Select the required database type from the options available.
3. Select the **Microsoft SQL Server** option to associate the selected cabinet with the SQL database.

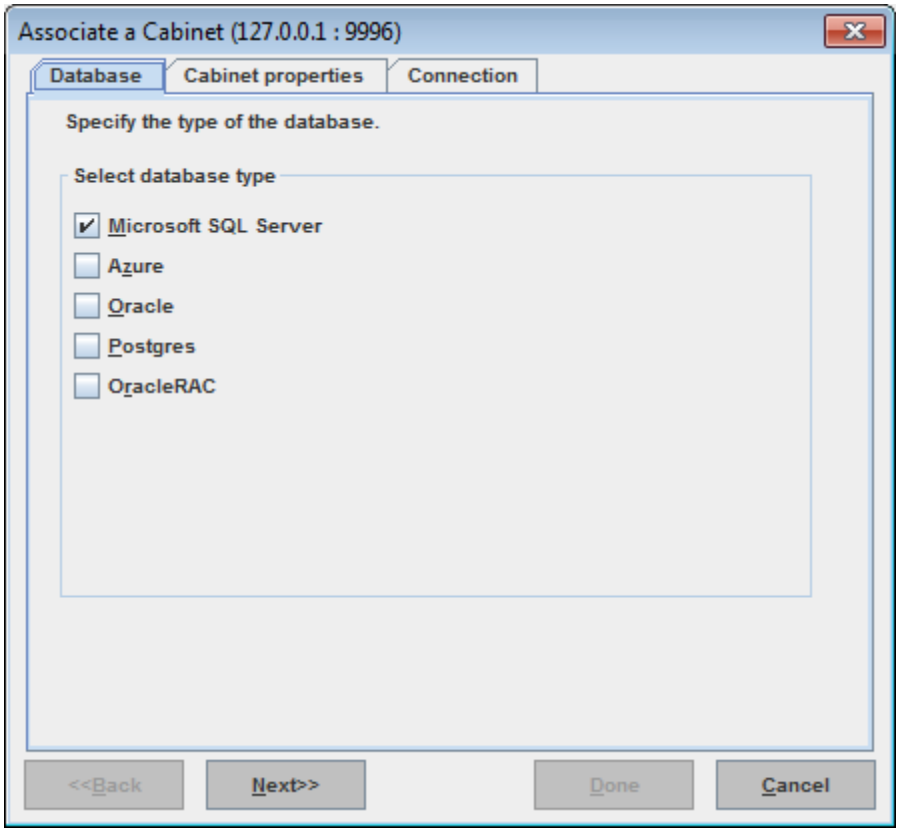

Associate a Cabinet (127.0.0.1 : 9996)
Database
Cabinet properties
Connection
Specify the type of the database.
Select database type
Microsoft SQL Server
Azure
Oracle
Postgres
OracleRAC
<<Back
Next>>
Done
Cancel

Figure 3.100

Using Cabinet Properties Tab

1. Click the **Cabinet properties** tab. The **Cabinet properties** tab page appears.

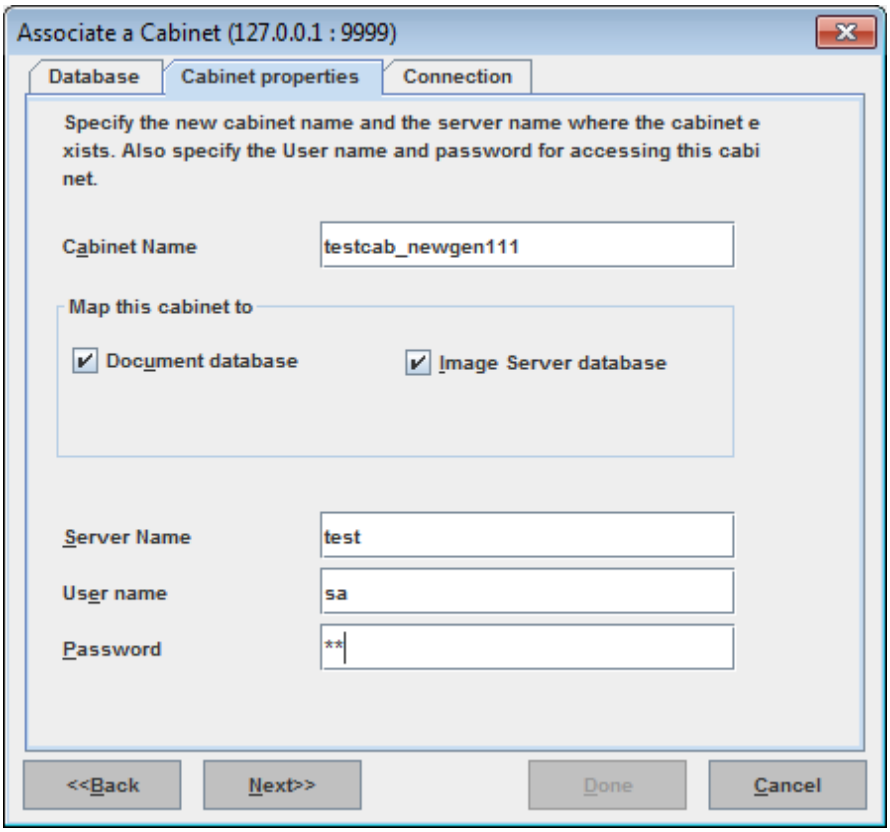


Figure 3.101

2. Specify the cabinet name in the **Cabinet Name** textbox.

NOTE:

The cabinet name should be the same as that of the cabinet name given while creating the cabinet.

---

3. Select the option **Document database**, if the database is a Document database.
4. Or, select the option **Image Server database**, if the database is an Image Server Database.

NOTE:

Both the checkboxes Document Database and Image Server Database have to be checked to associate a cabinet on which both Image Server and database operations are to be performed.

---

5. Specify the Server name in **Server Name** textbox.

6. Specify the user name in the **User name** textbox.
7. Specify the password in the **Password** textbox.
8. Click the **Back** button to go to the previous screen.
9. Or, click the **Next** button to proceed.

Using Connection tab

1. Click the **Connection** tab. The Connection tab page appears.

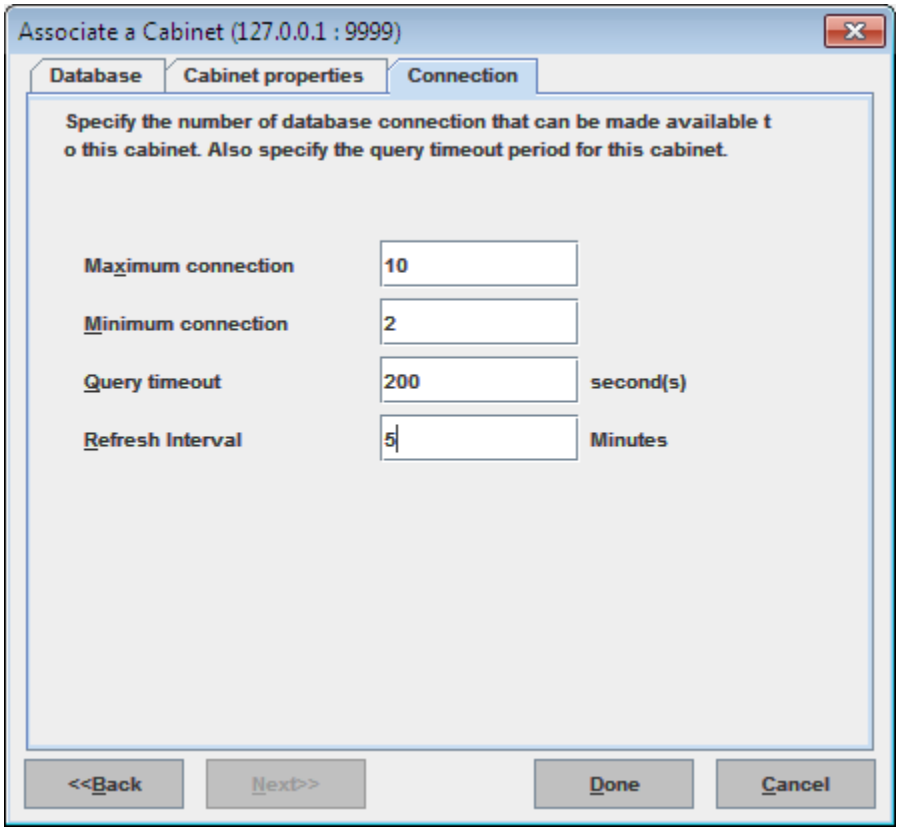


Figure 3.102

2. Specify the maximum number of connections that the JTS should maintain with the database in the **Maximum connection** textbox.
3. Specify the minimum number of connections that the JTS should maintain with the database in the **Minimum connection** textbox.
4. Specify the query time out for the selected cabinet in the **Query timeout** textbox.

5. Click the **Done** button to associate the selected cabinet or click the **Cancel** button to close the **Associate a Cabinet** dialog box without associating.
6. Click the **Back** button to go to the previous screen.

B. **Using Normal user to associate an MSQL 2008 cabinet**

1. Select the particular **SQL Server** on the left panel and expand it.

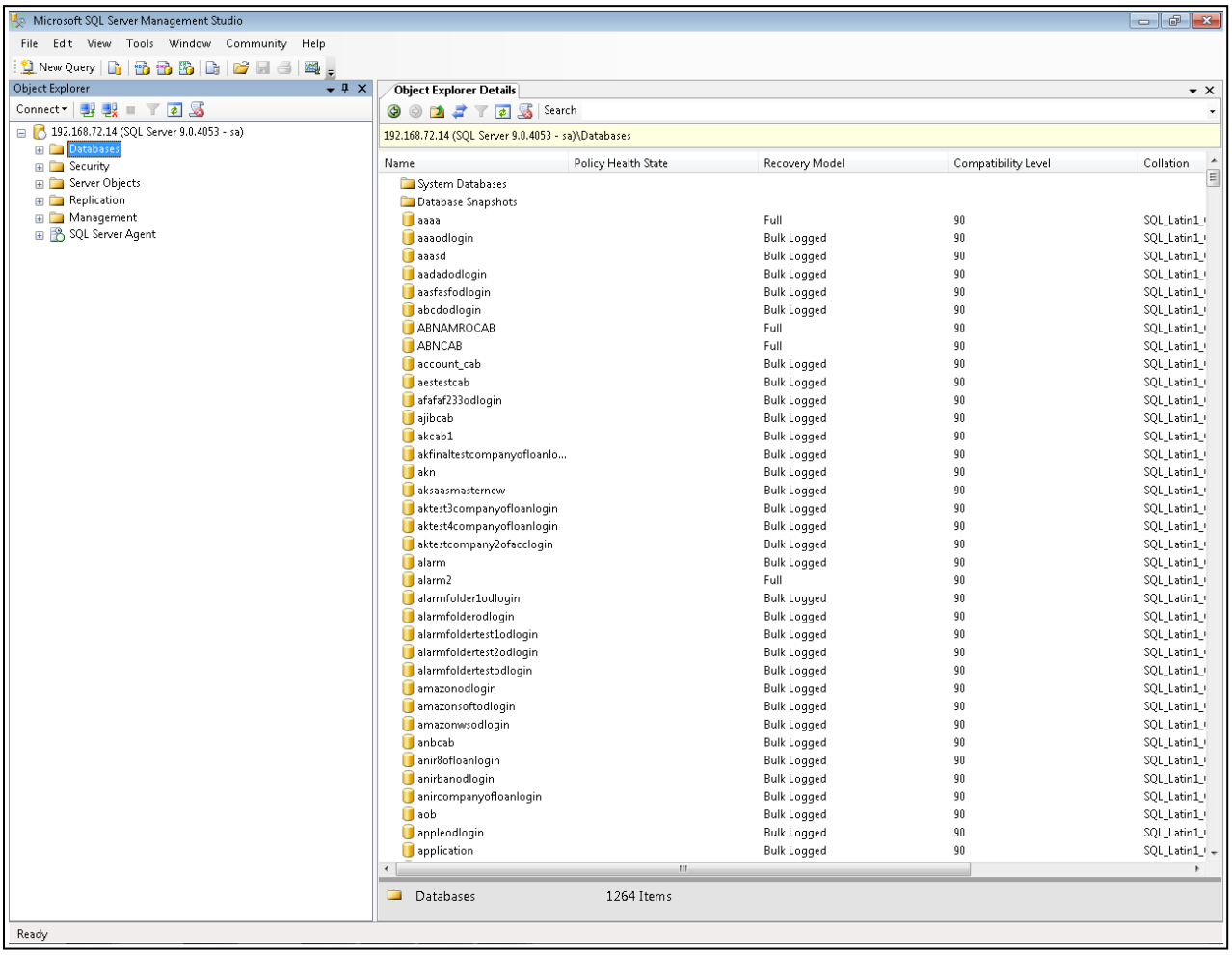


Figure 3.103

2. Expand **Security** then Select **Login.** Right-click on **Login** and select **New Login**.

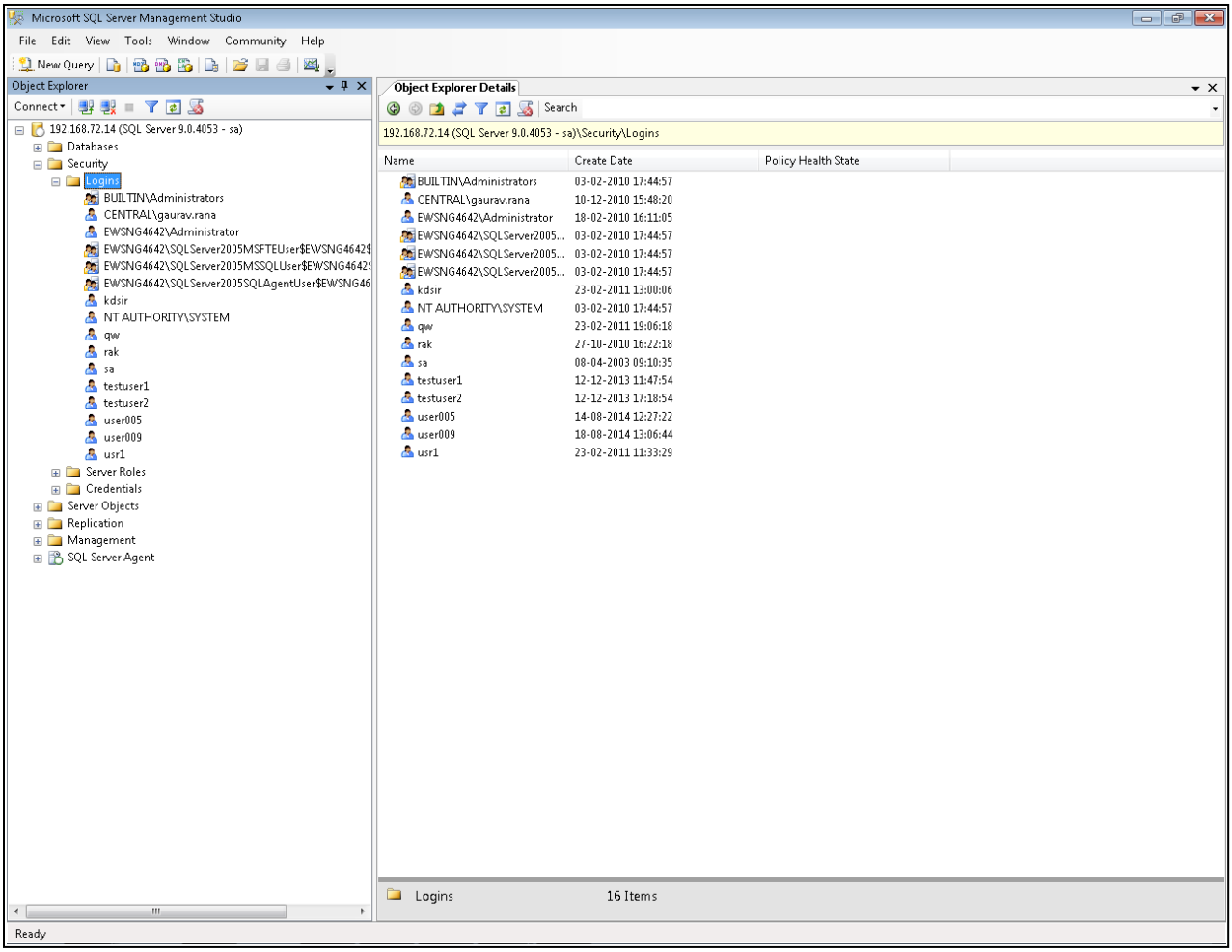


Figure 3.104

3. Perform the steps below:

   i. In the Login – New window, enter the name, select **SQL Server Authentication,** and enter the **password**.

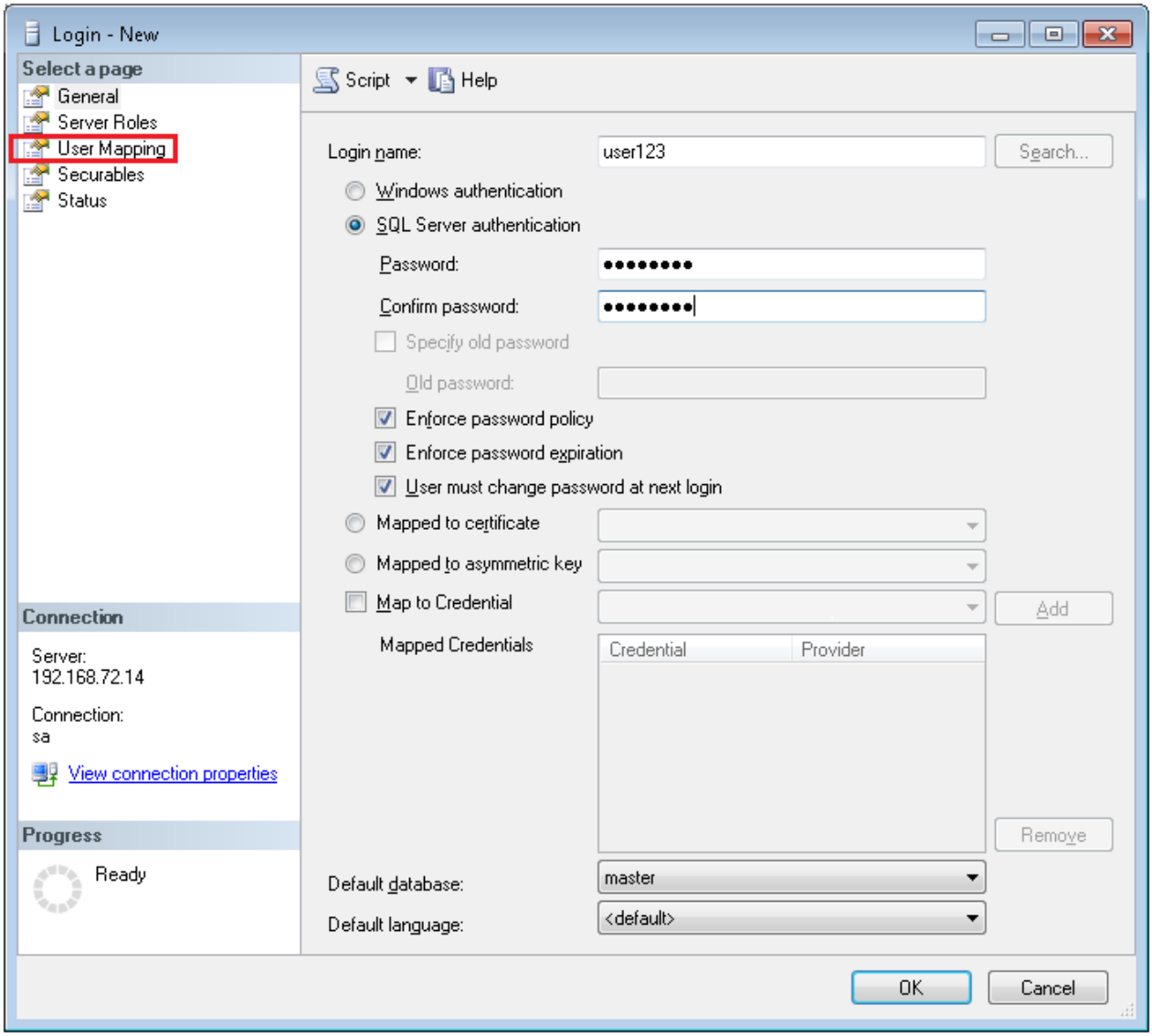


Figure 3.105

4. Perform the steps below:
   i. From the above window select the **UserMapping** tab.
   ii. Select the cabinet from the given lists and click on the **Map checkbox** so that it is checked.
   iii. From the bottom panel check on the **db_ddladmin**, **db_datareader**, **db_datawriter** checkboxes, and then click **OK**.

NOTE:

Check on the db_owner also along with db_ddladmin, db_datareader, db_datawriter, if FTS has to be used.

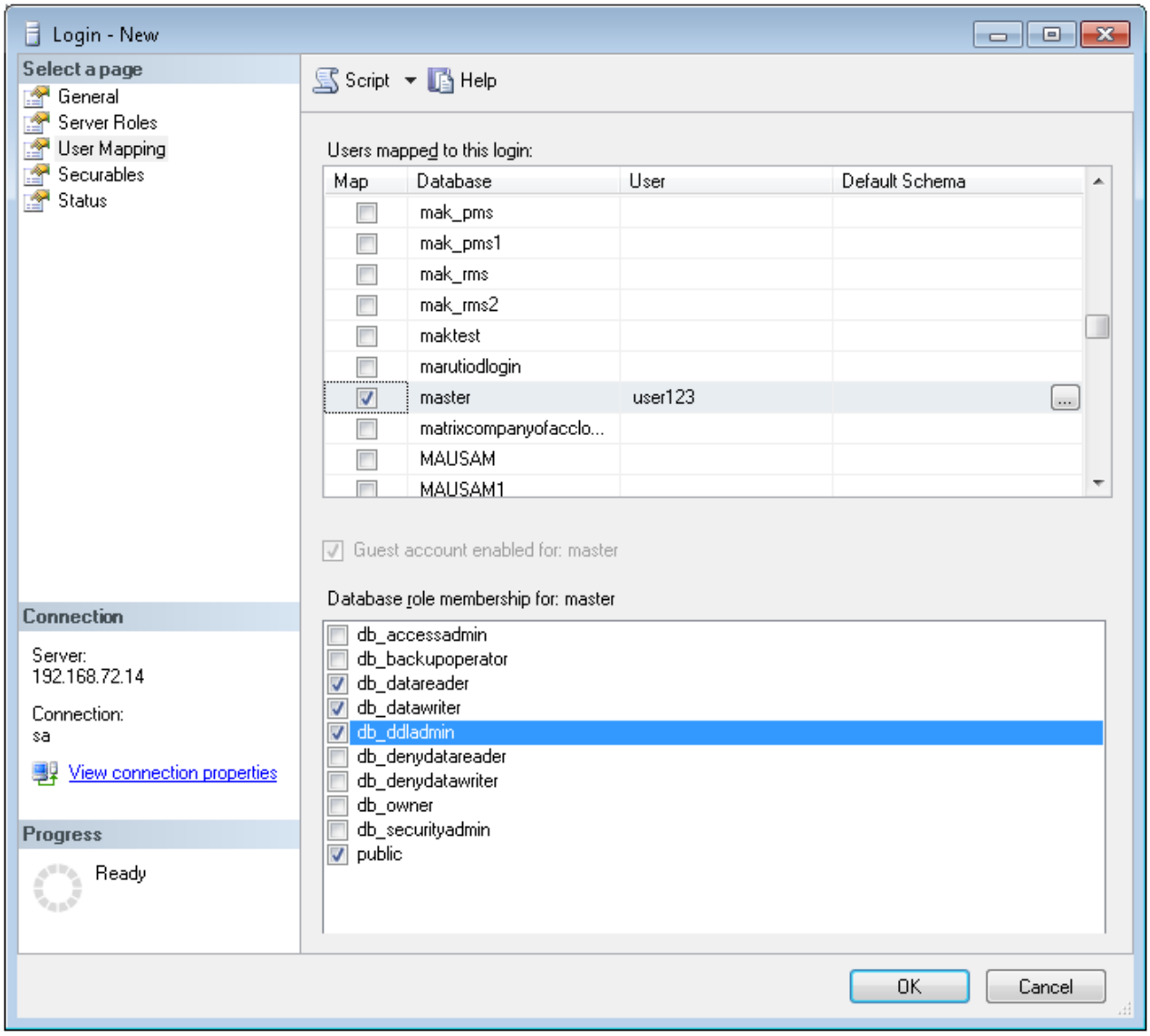


Figure 3.106

5. Run the following script.

   SELECT 'GRANT EXECUTE ON ' + RTRIM(NAME) + ' TO **USER**' FROM SYSOBJECTS WHERE XTYPE IN ('P', 'FN')

NOTE:

Replace the USER with the name of the user created above.

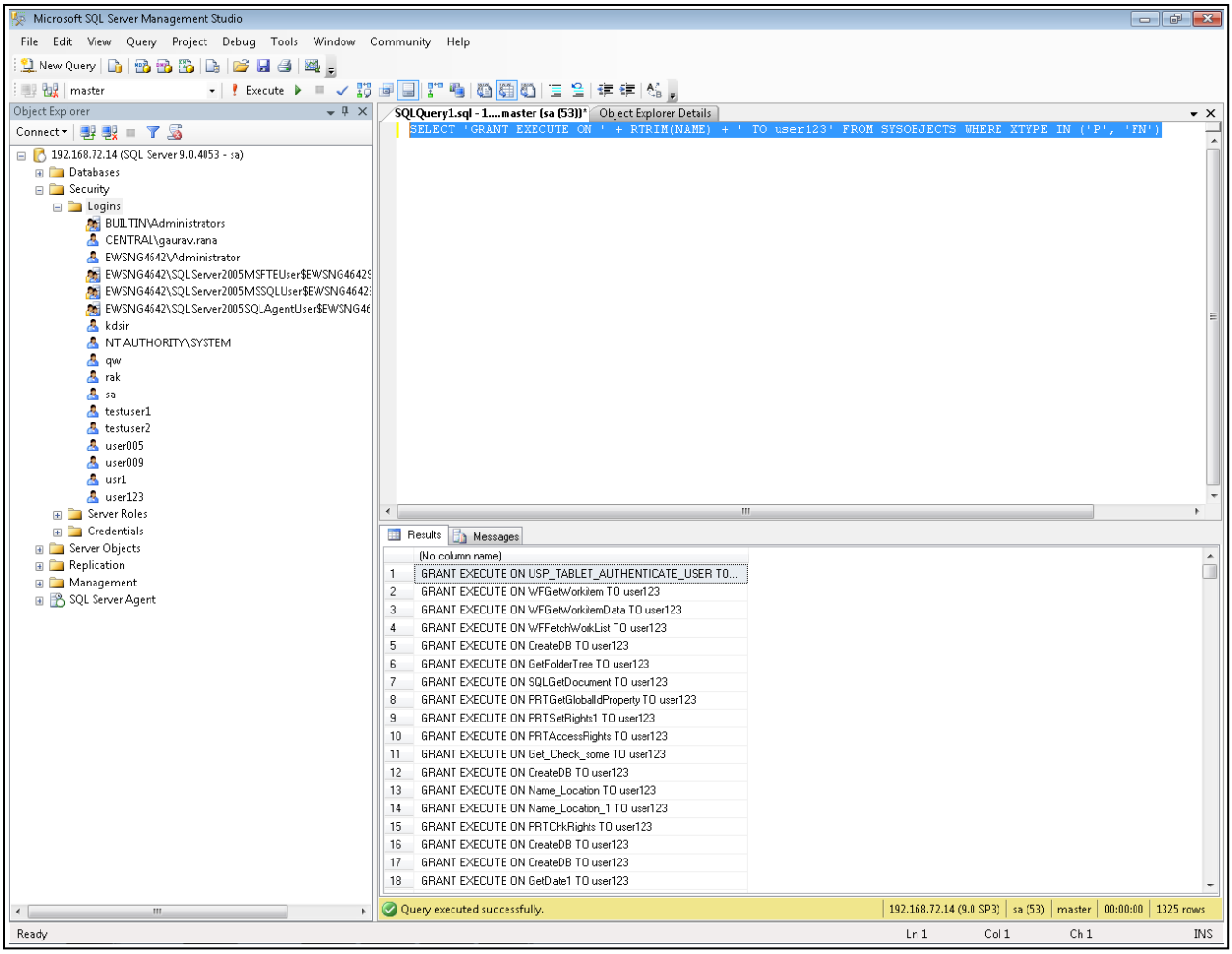


Figure 3.107

6. Copy the output of the above script and run the output as a script. This will assign the **EXEC** permission to the user created above on all procedures and functions.

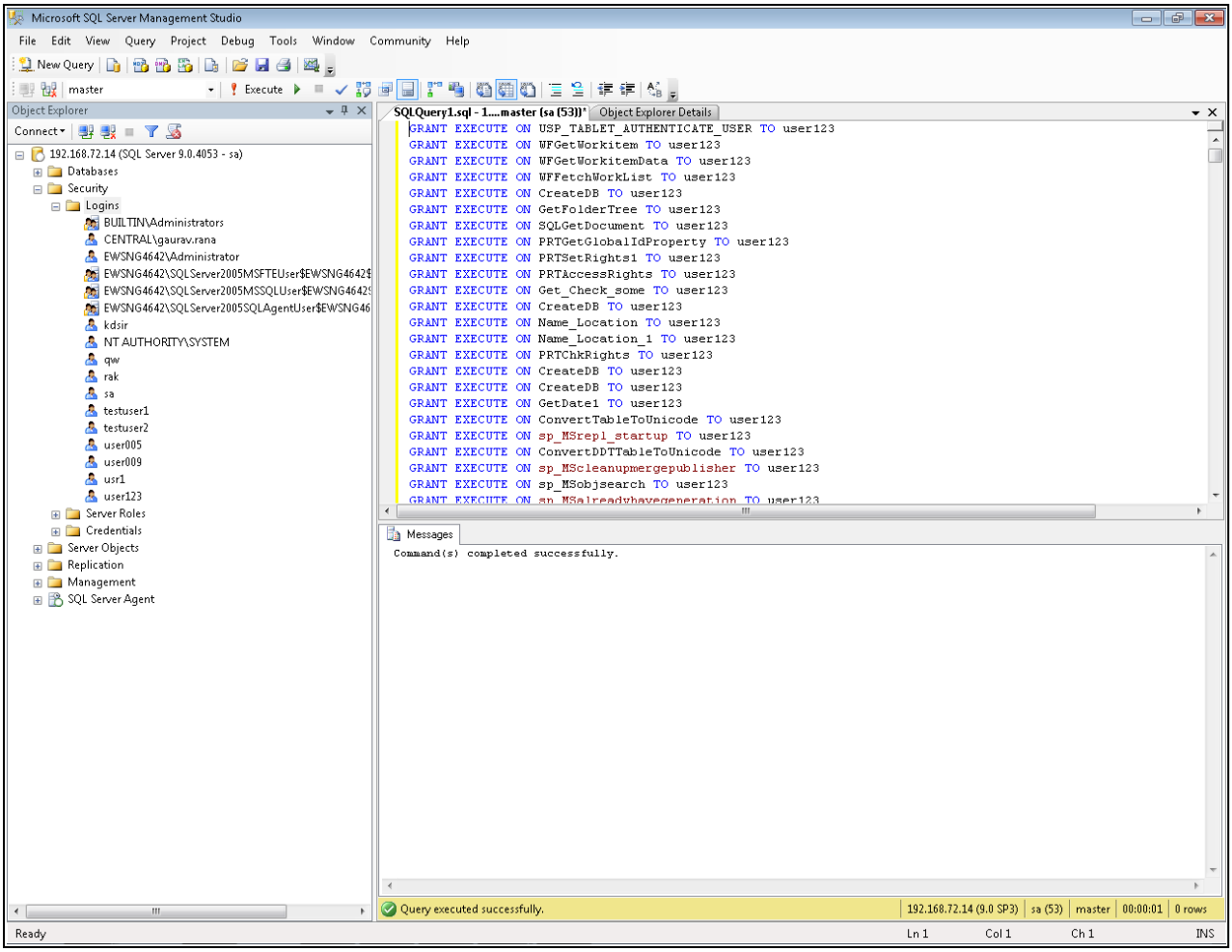


Figure 3.108

7. Use the above created user for associating a cabinet.

C. **Using Normal user to associate an MSSQL 2012 cabinet**

1. Select the particular **SQL Server** on the left panel and expand it.

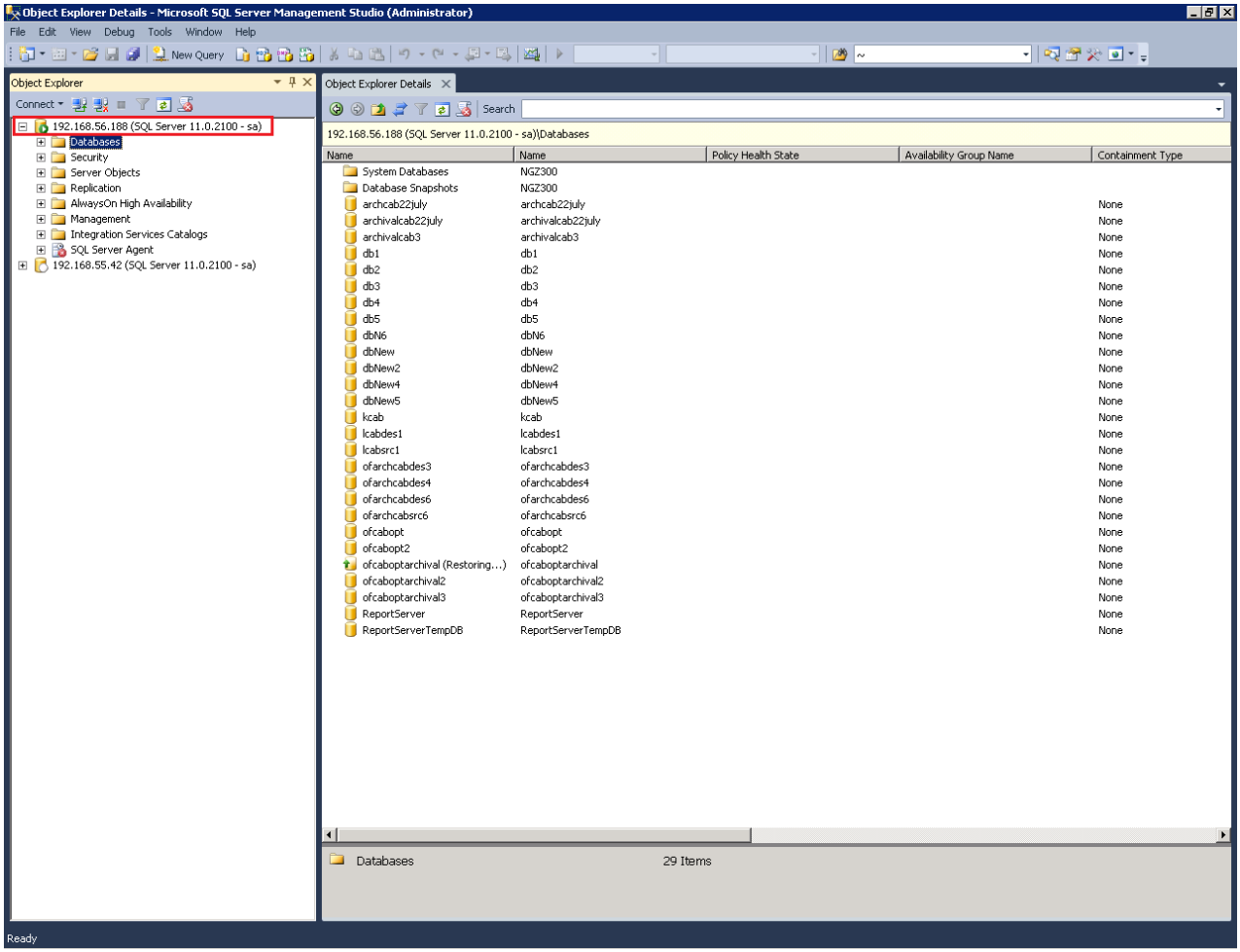


Figure 3.109

2. Expand **Security** then Select **Logins** and right-click.

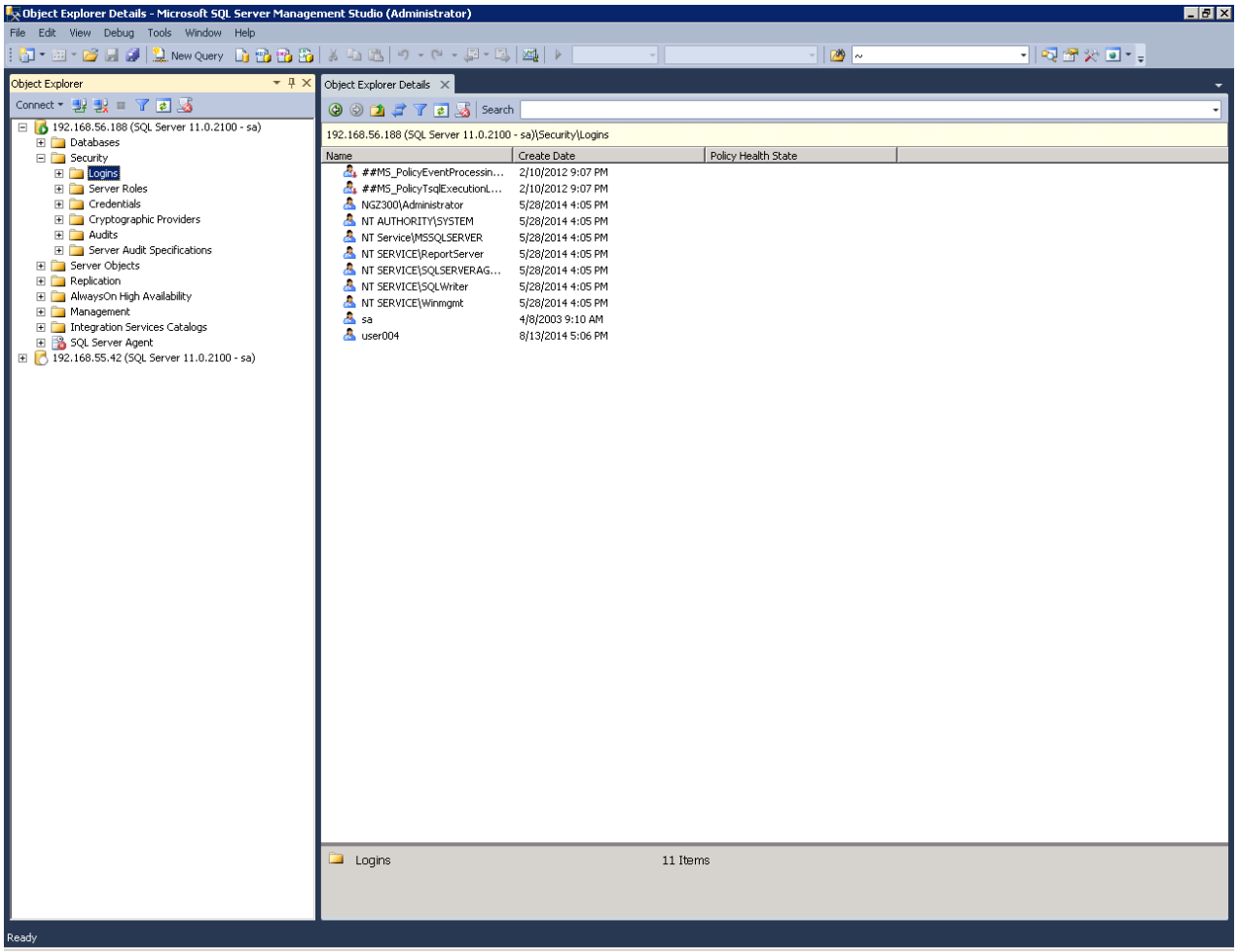


Figure 3.110

3. Perform the steps below:

   i. Click on **New Login** from the popup menu.

   ii. In the Login-New window, enter the Login name, select **SQL Server authentication,** and enter the **password**.

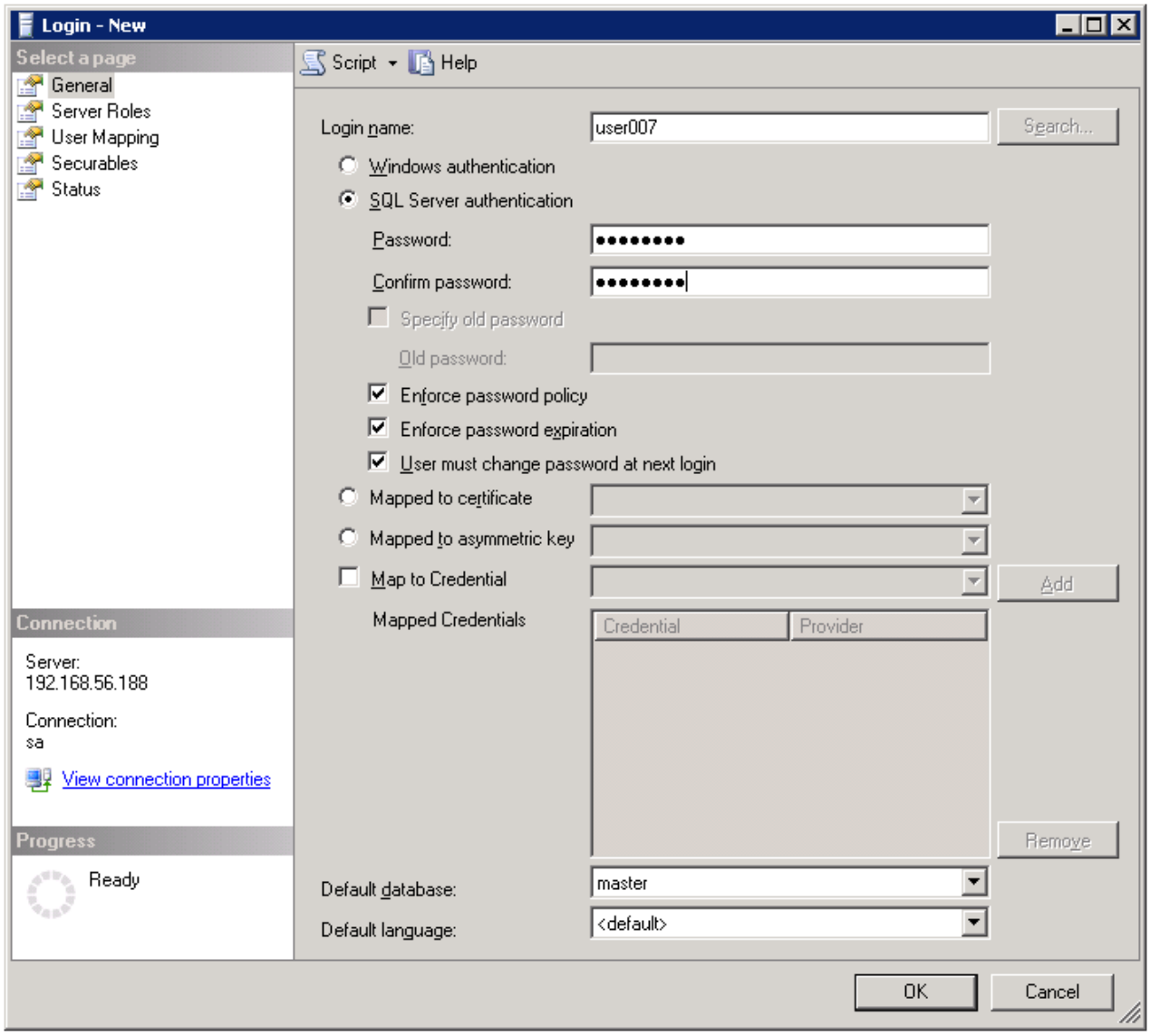


Figure 3.111

4. Perform the steps below:

   i. From the above window select the **UserMapping** tab.

   ii. Select the cabinet from the given lists and click on the **Map** checkbox so that it is checked.

iii. From the bottom panel check on the **db_ddladmin**, **db_datareader**, **db_datawriter** checkboxes.

iv. Click **OK**.

NOTE:

Check on the db_owner also along with db_ddladmin, db_datareader, db_datawriter if FTS has to be used.

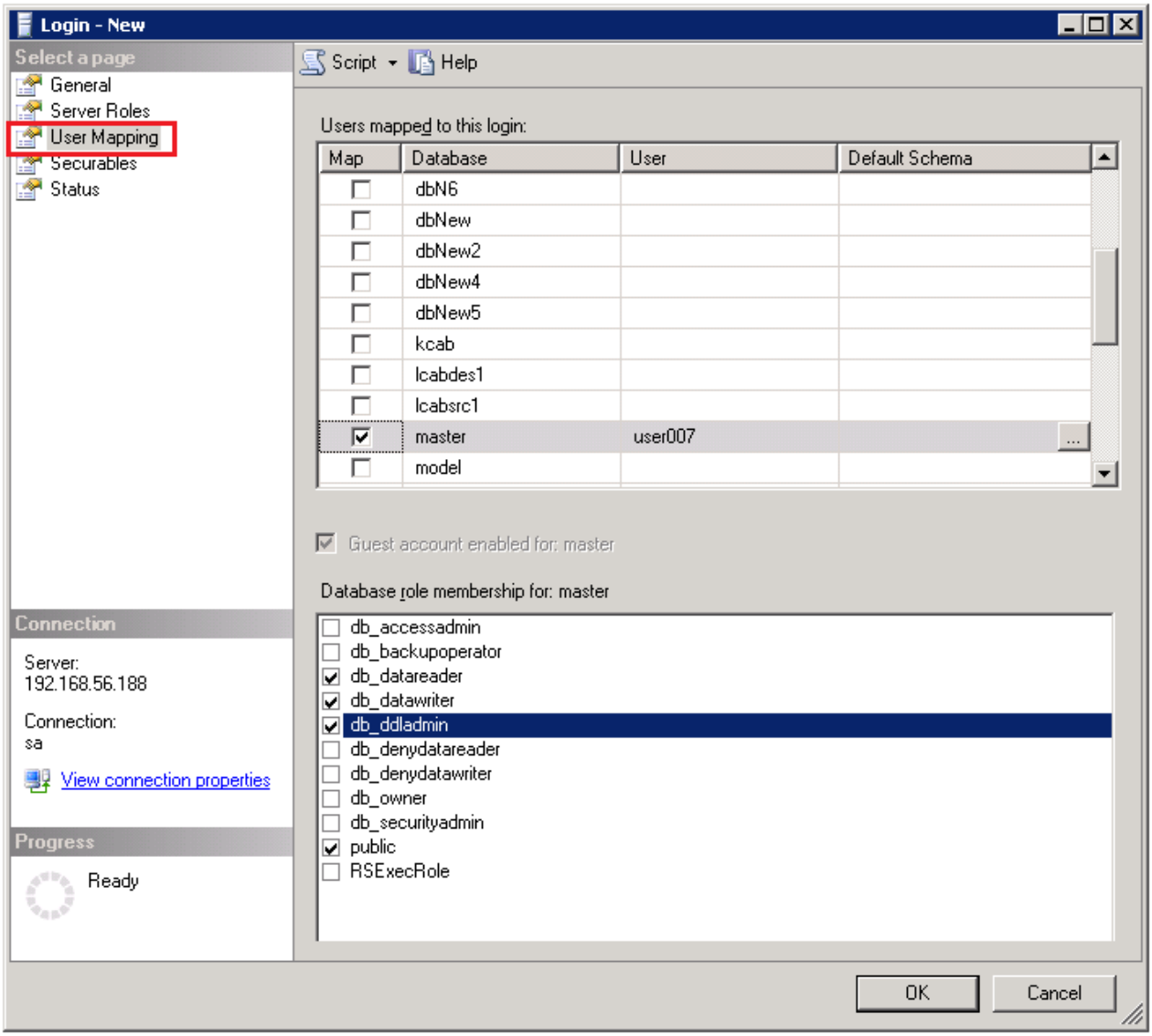


Figure 3.112

5. Run the following script.

```
SELECT 'GRANT EXECUTE ON ' + RTRIM (NAME) + ' TO USER' FROM SYSOBJECTS WHERE XTYPE IN ('P', 'FN')
```

NOTE:

Replace the USER with the name of the user created above.

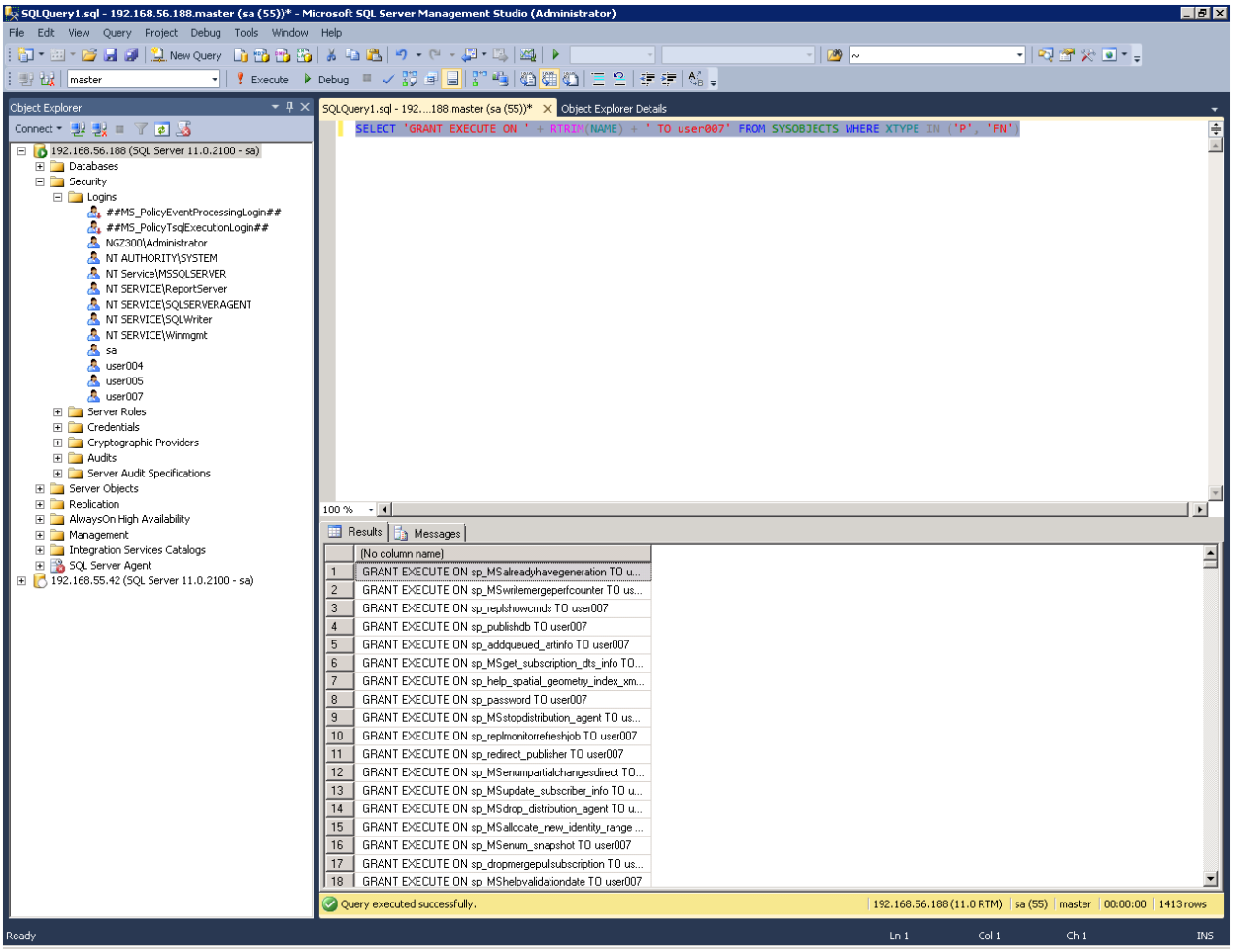


Figure 3.113

6. Copy the output of the above script and run the output as a script, this will assign the **EXEC** permission to the user created above on all procedures and functions.

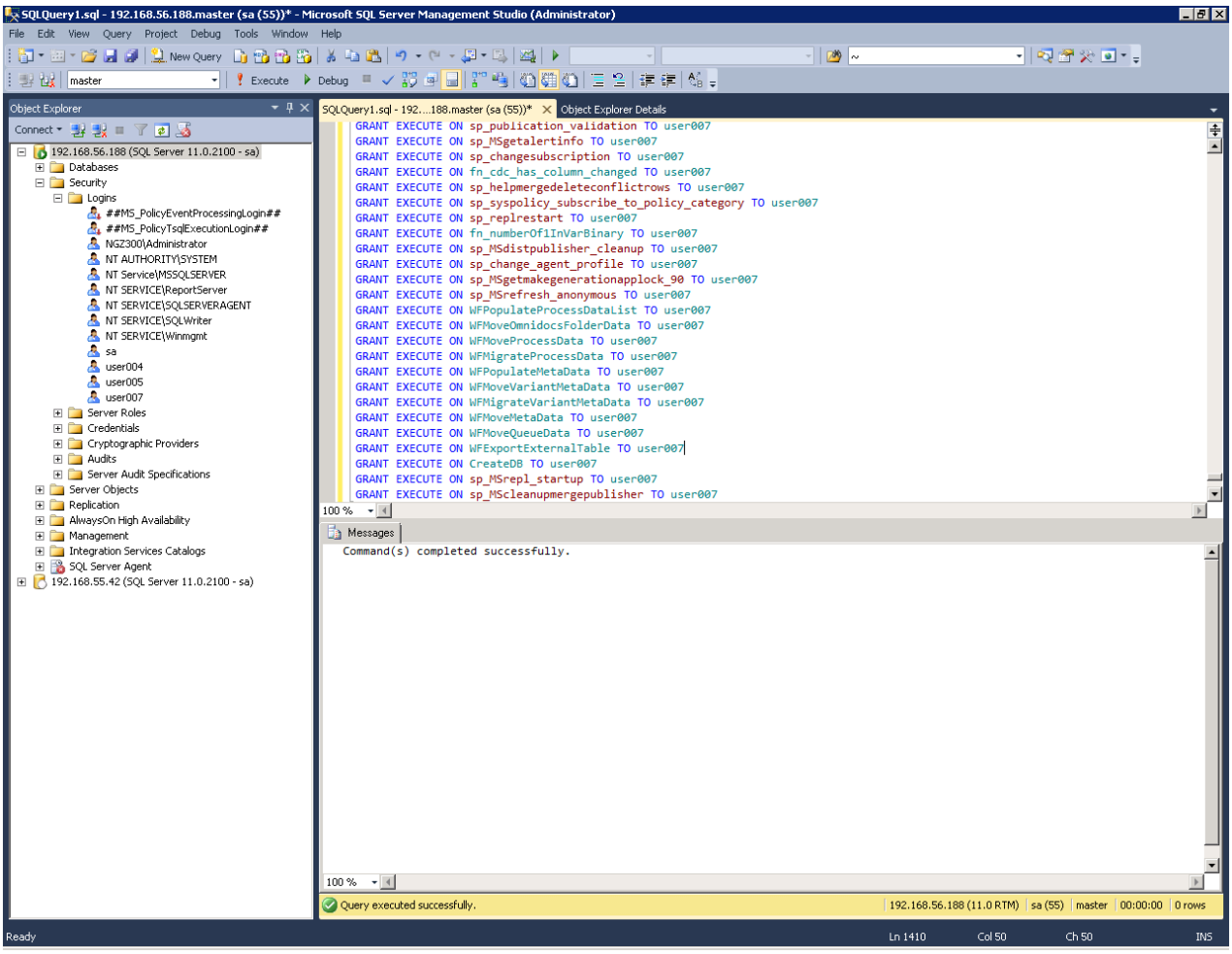


Figure 3.114

7. Use the above created user for associating a cabinet.

3.2.12 Disassociating a Cabinet

To disassociate a cabinet:

1. Select the cabinet that needs to be disassociated from the list.
2. Click the **Disassociate** button.
3. A **Confirm** message box is invoked prompting whether you want to remove the association with the selected cabinet.

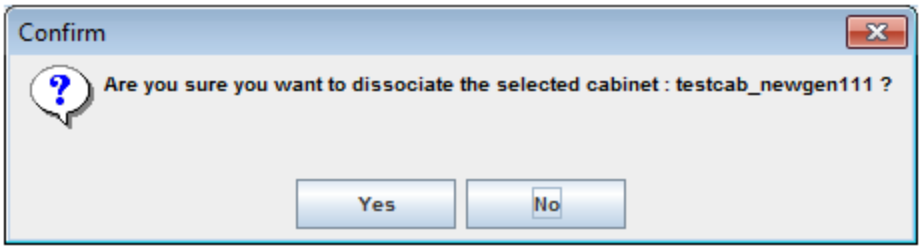


Figure 3.115

- Click the **Yes** button to remove the disassociation with the selected cabinet, or
- Click the **No** button to avoid the disassociation process.

NOTE:

Here "Disassociate" means removing the entry of the selected cabinet from JTS. The disassociation of the cabinet can be performed only when the server is stopped.

3.2.13 Upgrading cabinet

In case of the cabinet upgrade, the user has the option to install the application without the automatic configuration and associate the cabinet with any previous version.

To upgrade the selected cabinet:

1. Associate the cabinet.
2. Select the cabinet which is to be upgraded.
3. Click the **Upgrade** button.

NOTE:

Upgrading a cabinet implies:

- Executing an SQL statement (other than those, which return a result set,) on a cabinet. This may be a DDL or a DML (which includes updates, deletion, etc).
- Any number of queries can be simultaneously executed in a file. An important thing to note is that all the SQL statements must end with a comma ' ,'
- Stored procedures can also be compiled on a cabinet.

---

4. A **Select Operation** message box is invoked.

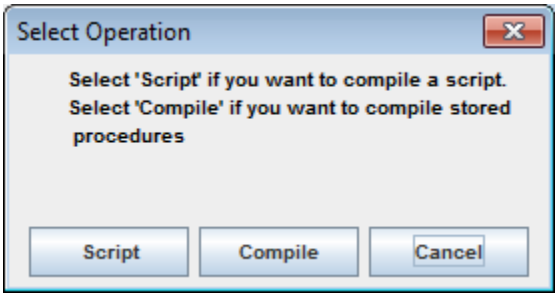


Figure 3.116

5. Click the **Script** button to compile a script.
6. **Select the script** dialog box is invoked.

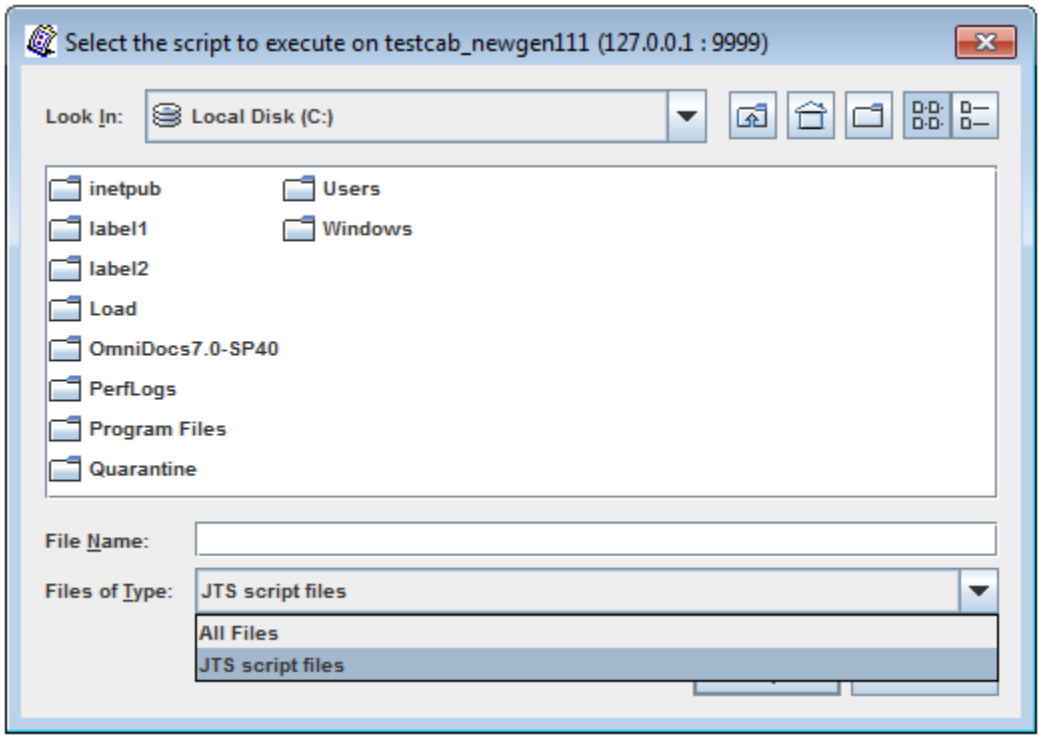


Figure 3.117

i. Select the required path where the script is located, from the **Look in** dropdown list. A list of all the files with extension jts is displayed.

ii. The name of the selected file is displayed in the **File Name**; you can also specify the file name in **File Name**.

iii. Select the type of file from the **Files of Type** dropdown list.

NOTE:

The **Files of Type** dropdown list consists of one option 'JTS script files'.

---

iv. Click the **Compile** button to run the required script.

v. Click the **Cancel** button to close the dialog box.

7. Click the **Compile** button on the **Select Operation** message box.
8. If you are logged in as the Supervisor, then **Compiled Stored Procedures** dialog box is invoked.

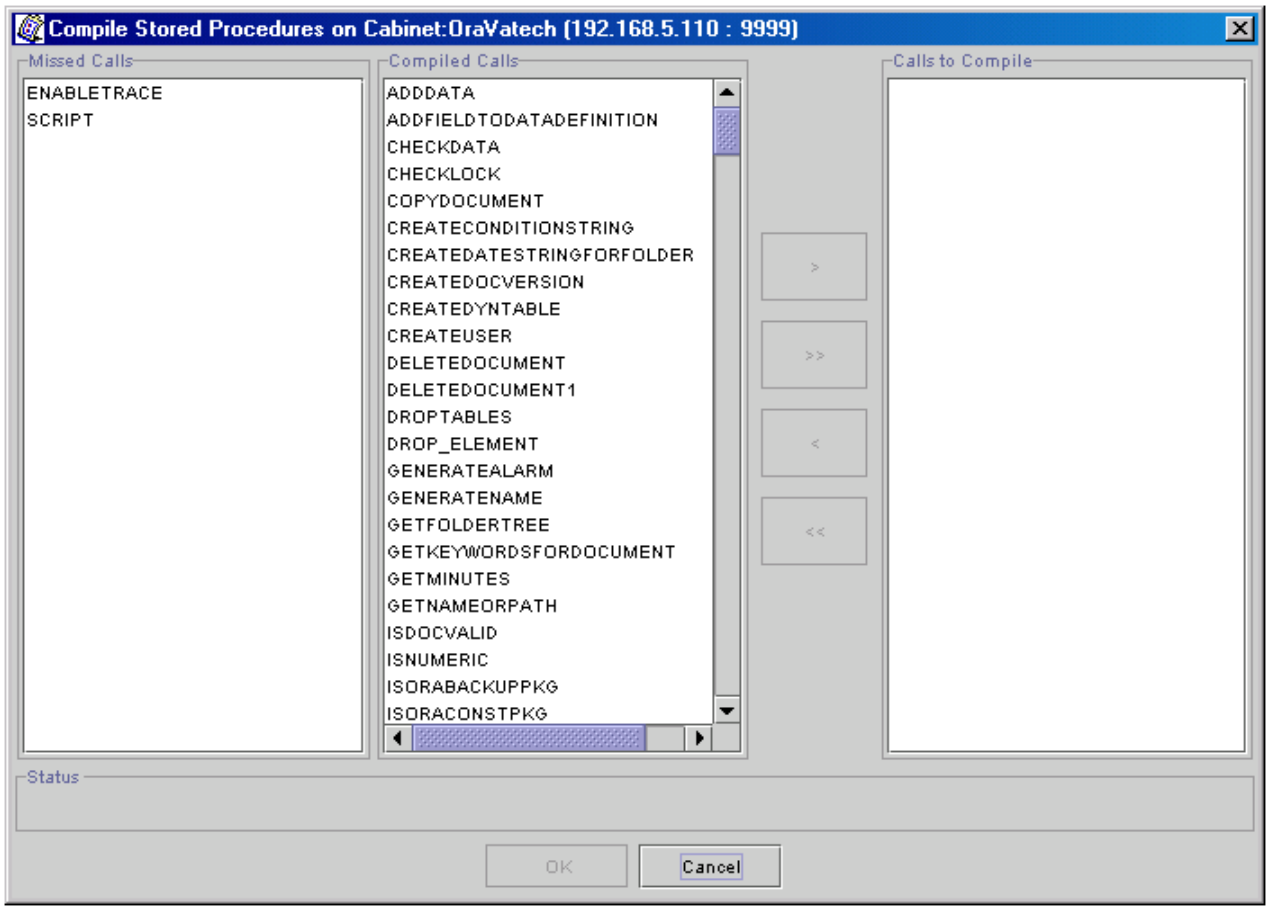


Figure 3.118

The **Compiled Calls** pane displays the list of all the compiled procedures of the selected cabinet.

To recompile the procedures:

a. Select the required procedure from the **Compiled Calls** left pane and click the > button, to add the procedure in the **Calls to Compile** list on the right pane.

b. To recompile all the calls, click **>>**. The entire list is added to **Calls to Compile** list on the right side.

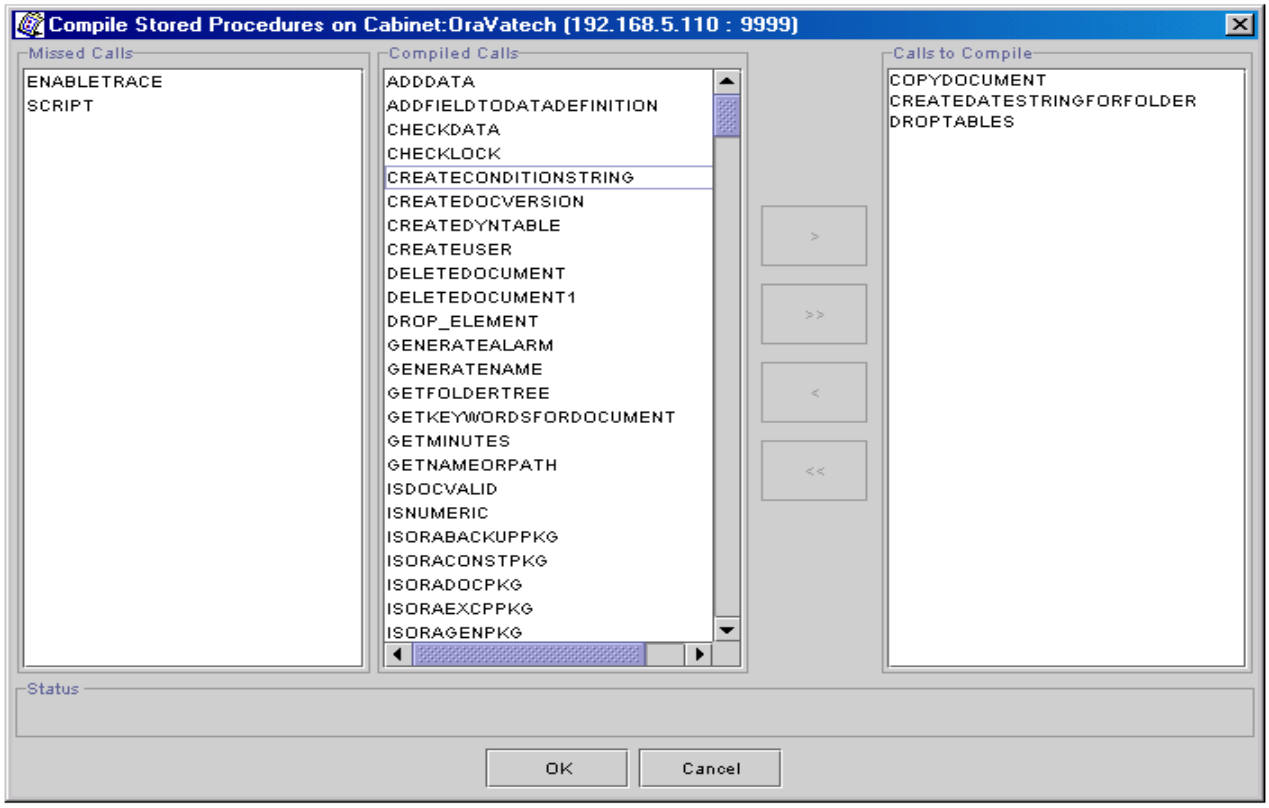


Figure 3.119

To move the calls from the **Calls to Compile** list to the **Compiled Calls** list:

a. Select the call that does not need to be compiled, from the **Calls to Compile** list.

b. Click the **<** button to move the call to the **Complied Calls** list on the left pane.

c. To move all the calls from the **Calls to Compile** list to the **Compiled Calls** list, click <<.

d. Click the **OK** button to close the **Calls to Compile** list.

e. Click the **Cancel** button to close the dialog box.

9. If you are logged in as System, then the operation is slightly different.

10. Refer to steps 6-7 for further information.

11. After upgrading the cabinet, data source creation is required. Refer to DataSource Creation (JBoss/WildFly/WebLogic/WebSphere) section of OmniDocs Post Deployment Guide.
12. After creating the data source, register the cabinet. Refer Registration of Cabinet section of OmniDocs Post Deployment Guide.

3.3 Viewing Properties of the Cabinet

To view properties of the cabinet:

1. Select a cabinet and click the **Property** button.

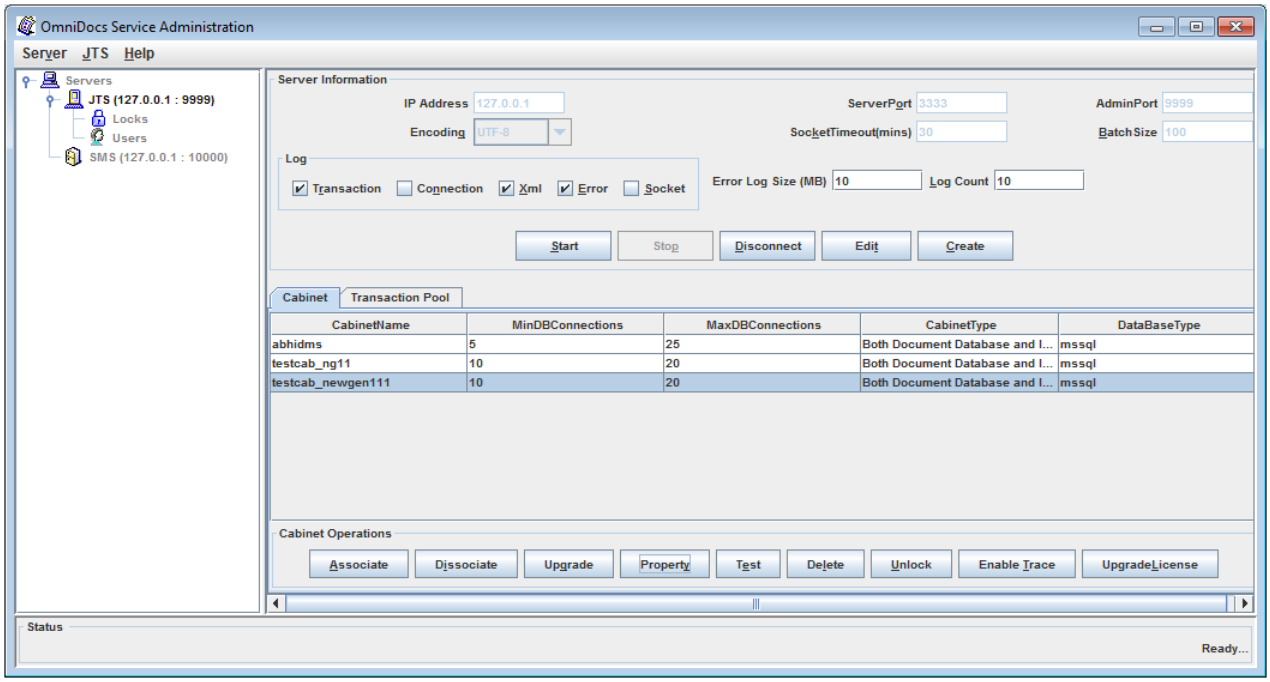


Figure 3.120

2. The **Cabinet Properties** dialog box is invoked.

   Cabinet Properties dialog box consists of three tabs:

   - Database tab
   - Cabinet properties tab
   - Connection tab

Database tab

The database tab displays the cabinet database type. It also displays the Server Port and the Service Name in case of an Oracle Cabinet and the Server Port in case of a Postgres Cabinet.

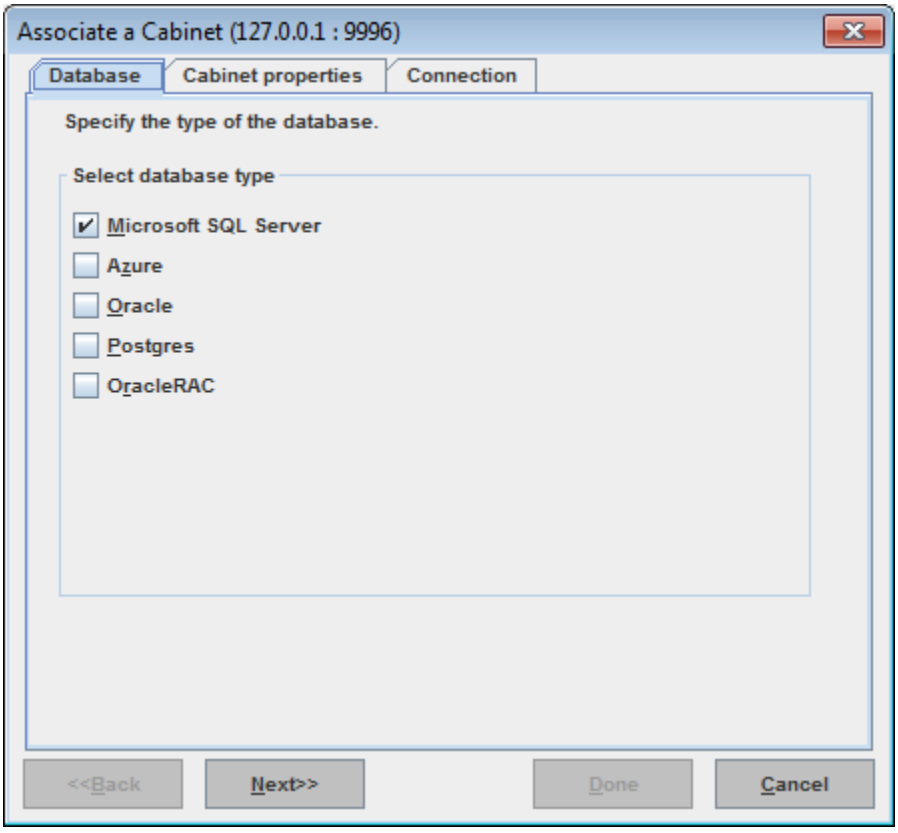


Figure 3.121

Cabinet properties tab

The Cabinet properties tab displays the cabinet name, the mapped status of the selected cabinet, the server name, the user name, and the password.

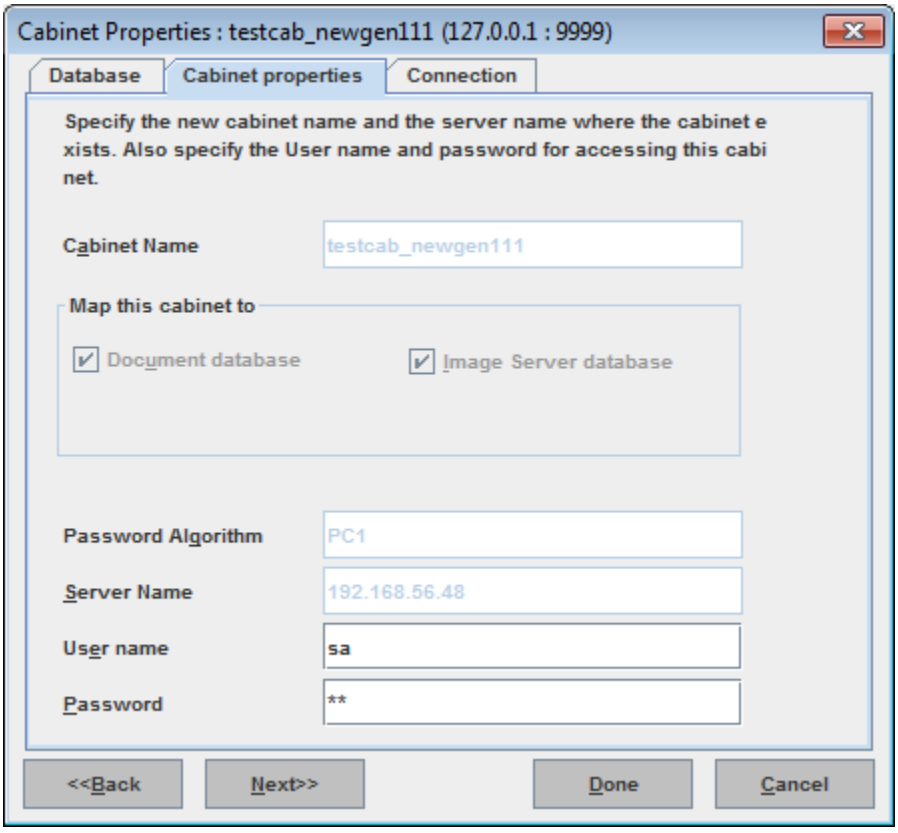


Figure 3.122

Connection tab

The Connection tab is in editable mode.

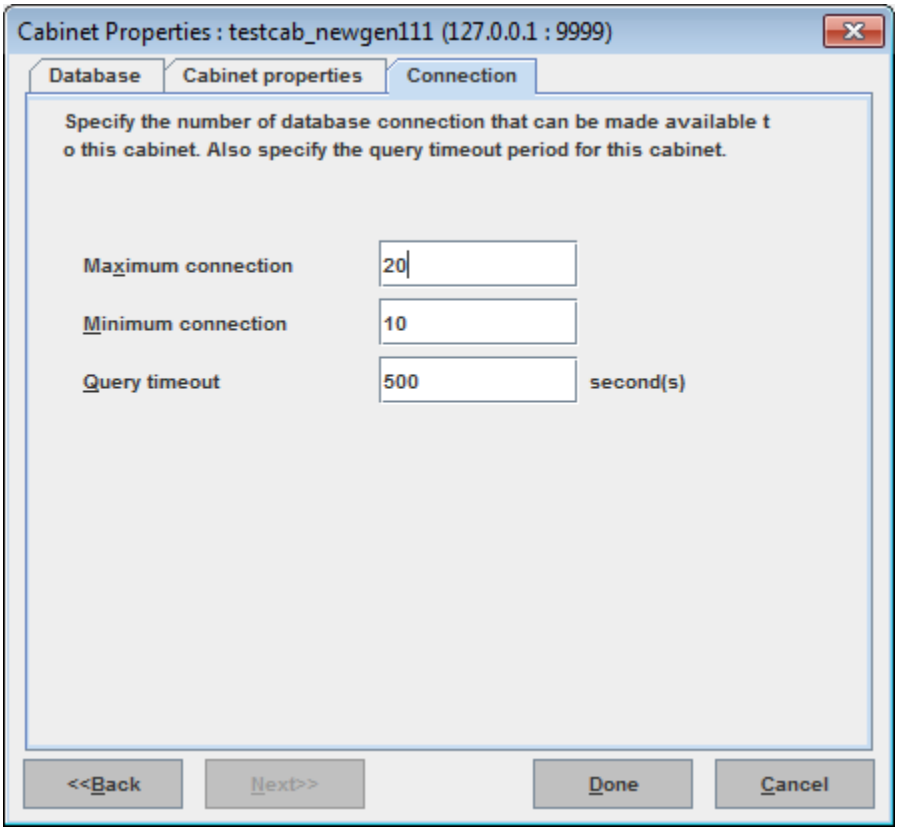


Figure 3.123

Properties of the cabinet can be changed when the server is not running.

You can edit the following:

- Maximum connection
- Minimum connection
- Query timeout

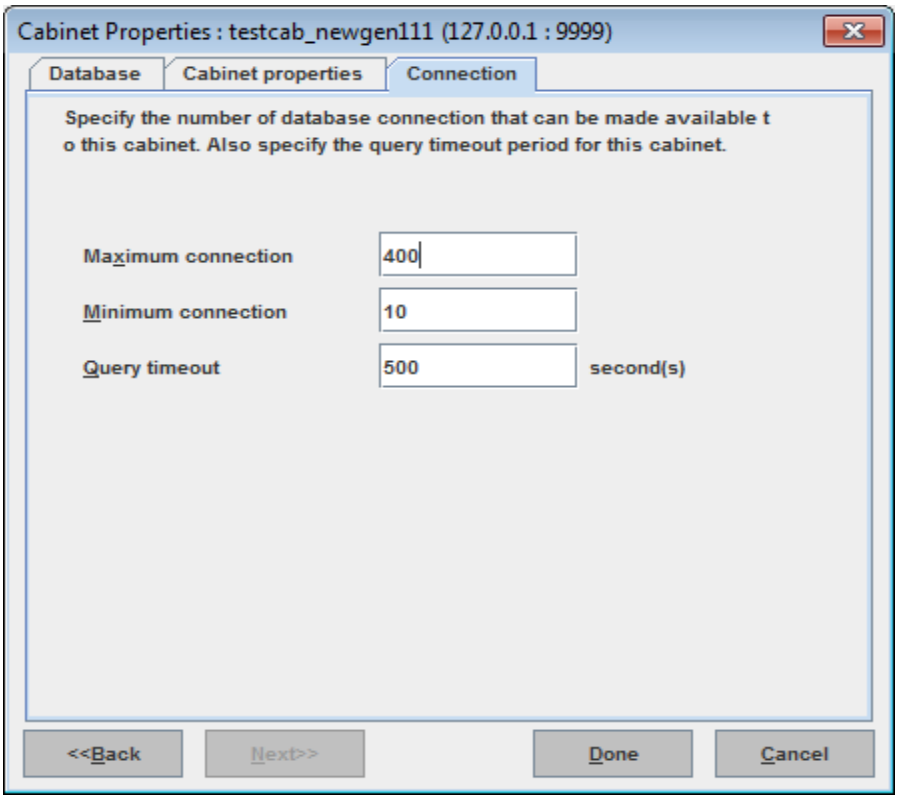


Figure 3.124

3. Click the **Back** button to go to the previous screen.
4. Click **Cancel** button to close **Cabinet Properties** dialog box without saving the changes made.
5. Click **Done** button to close the **Cabinet Properties** dialog box while saving the changes made. The changes done are immediately reflected.

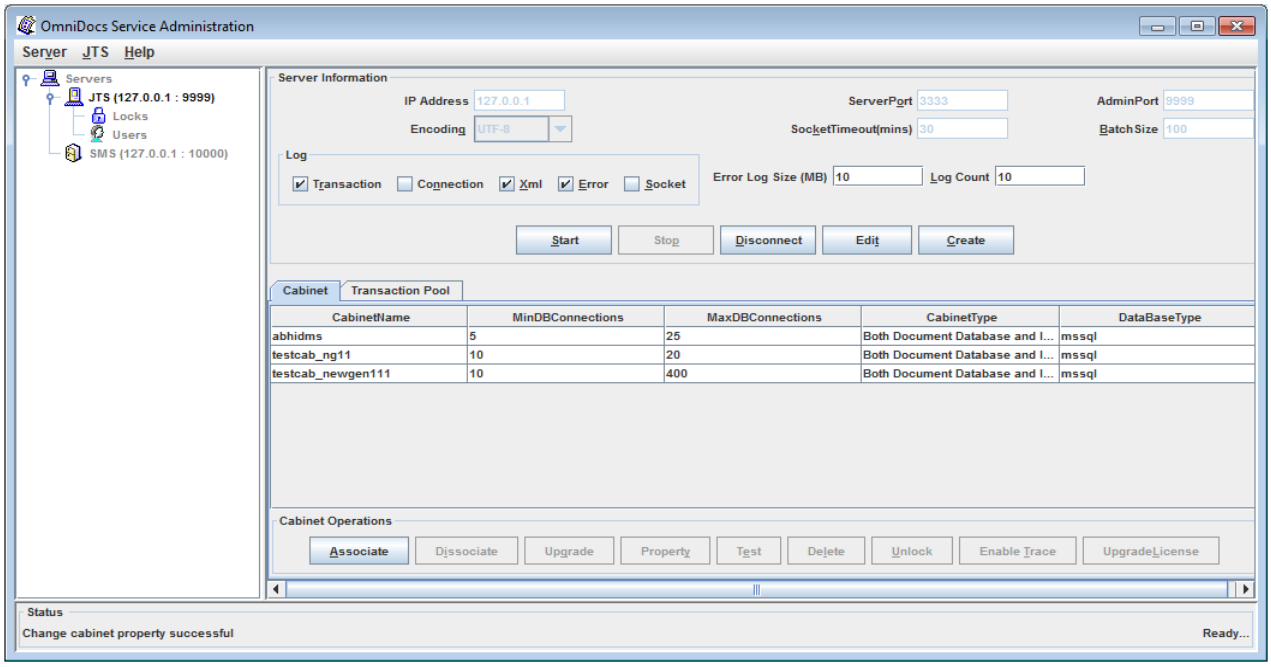


Figure 3.125

3.4 Testing the cabinet

Testing the cabinet implies testing the validity of the JTS's database connection.

To test the cabinet:

1. Select the Server which you want to test.
2. Click **Test**.
3. A message box is invoked displaying the result of the connection test for the selected cabinet.

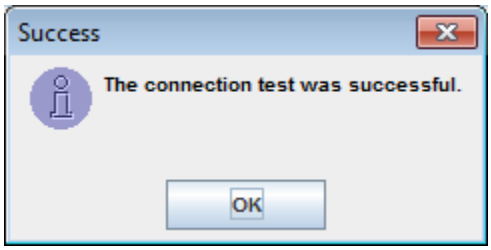


Figure 3.126

3.5 Viewing Locks

The Lock view displays all the locks that have been applied on objects (folders, documents, forms, and versions) by the user of the specified cabinet.

To view the locks of the selected cabinet:

1. Select the Locks.

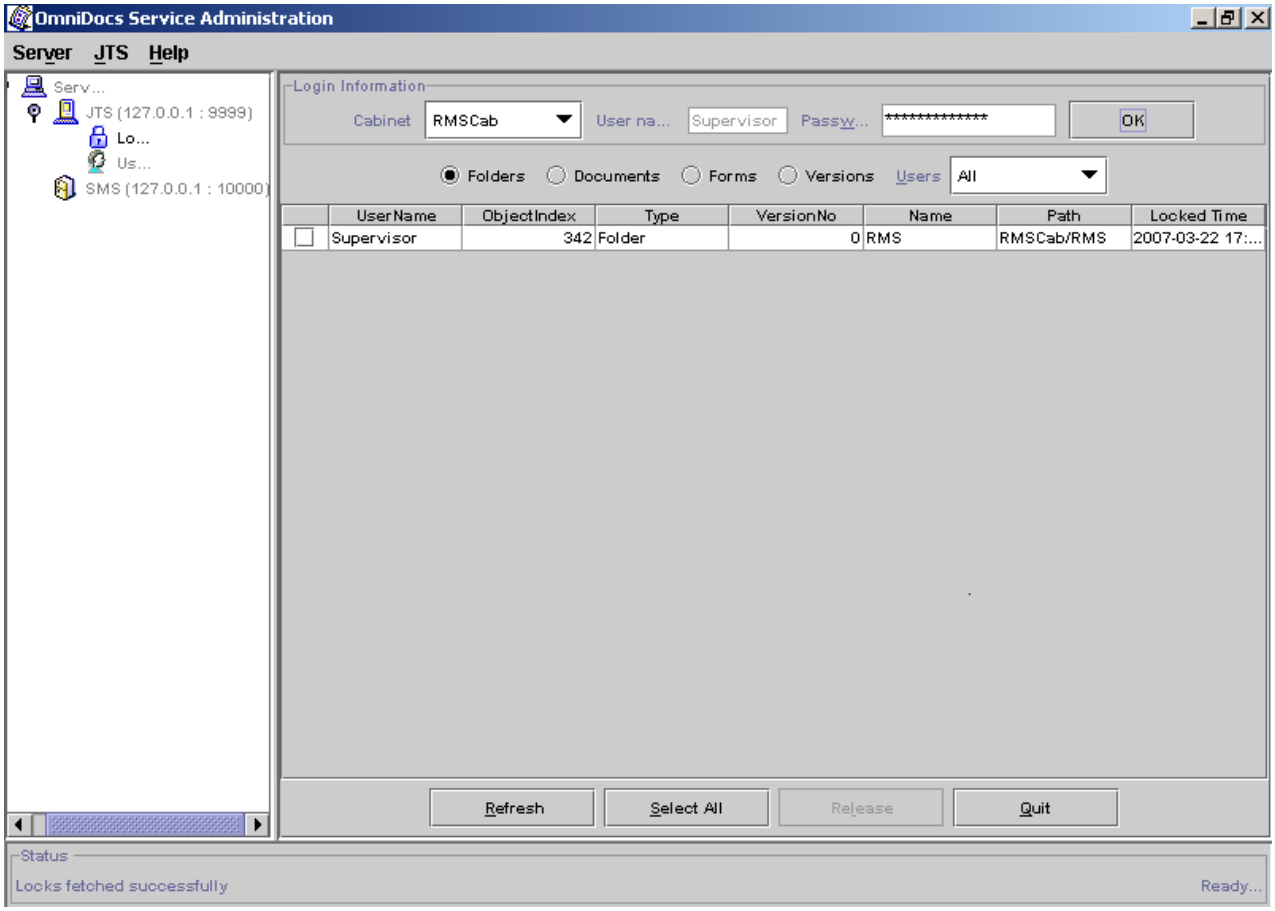


Figure 3.127

2. Select the required cabinet from the **Cabinet** dropdown list.

NOTE:

JTS can have multiple cabinets associated with it.

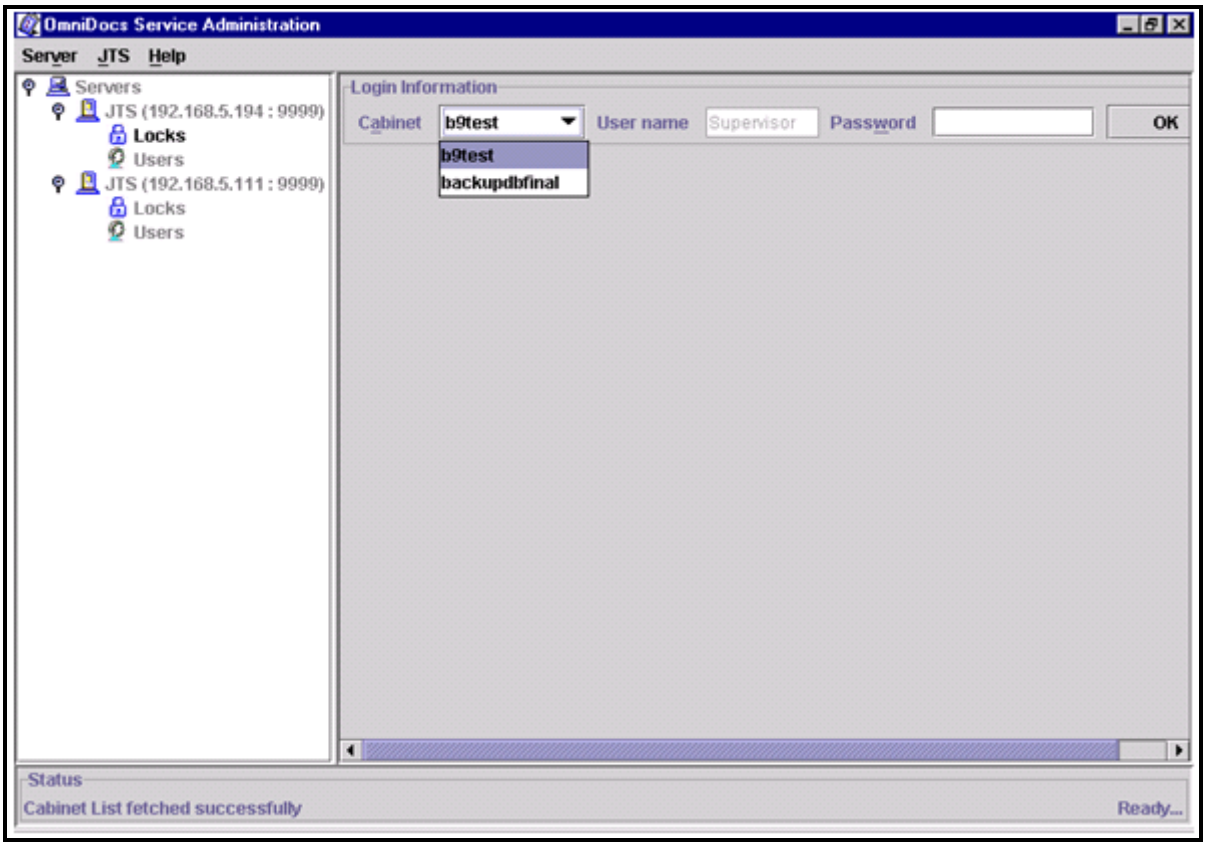


Figure 3.128

3. Specify the password for logging, in **Password**.

NOTE:

Only the Supervisor can change the locks of a cabinet. This is the reason, only the Supervisor user is shown. The login password is the same as the cabinet password.

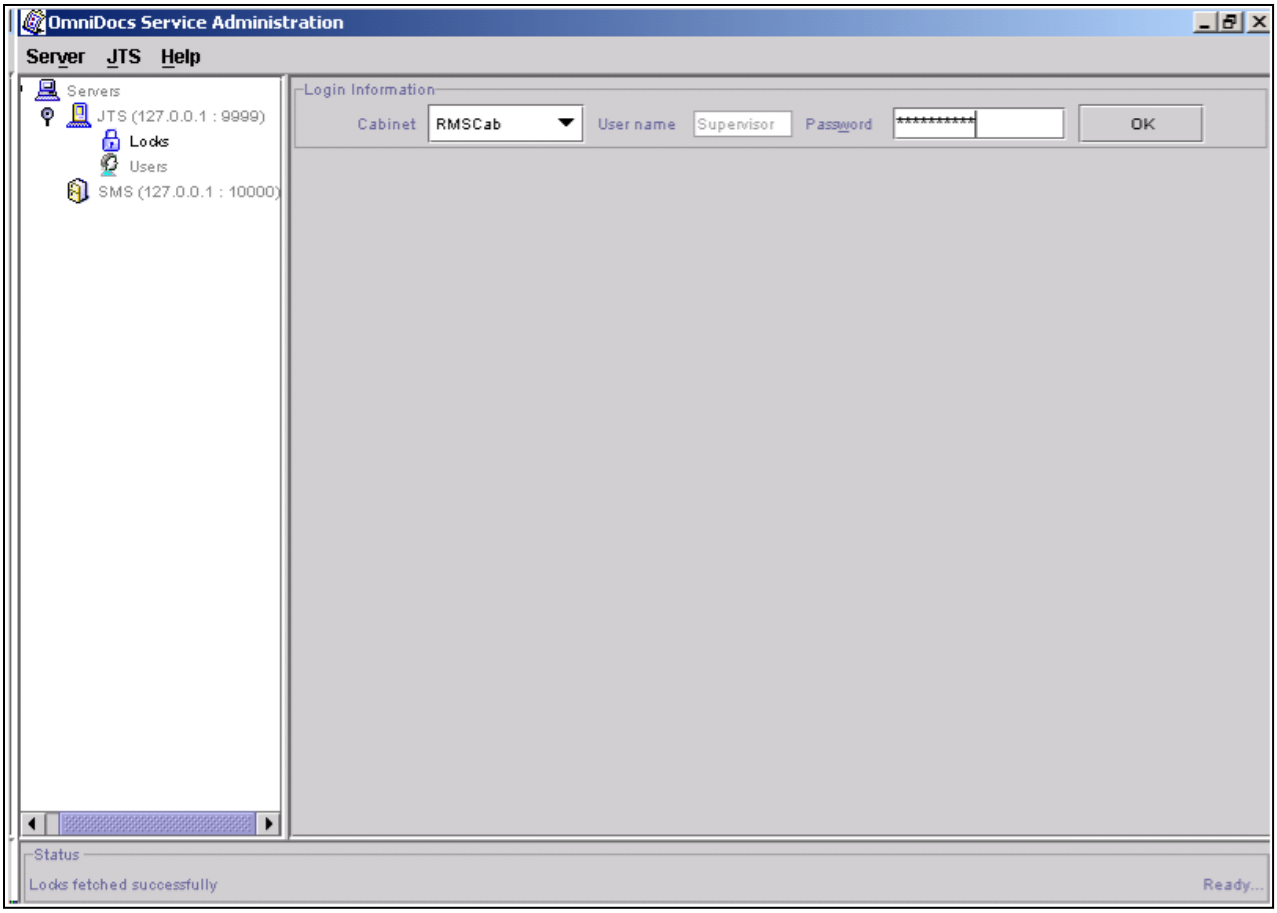


Figure 3.129

4. Click the **OK** button to view the locks of the selected cabinet.

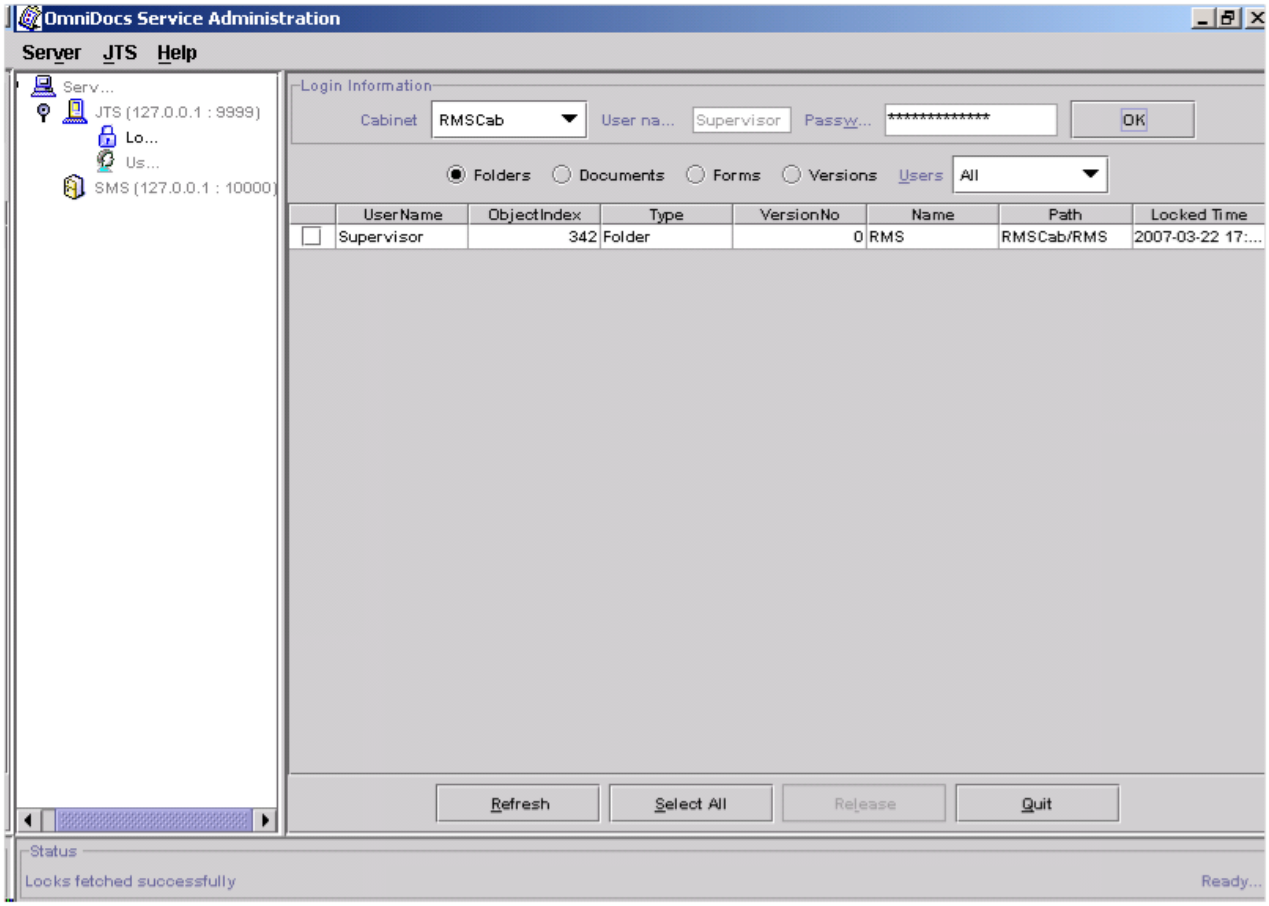


Figure 3.130

5. Select the **Folders** option to view the locks associated with folders.
6. Select the **Documents** option to view the locks associated with the document.
7. Select the **Forms** option to view the locks associated with forms.
8. Select the **Version** option to view the locks associated with the Versions of a document.

To view the locks by specific users

1. Select the required user from the **Users** dropdown list.

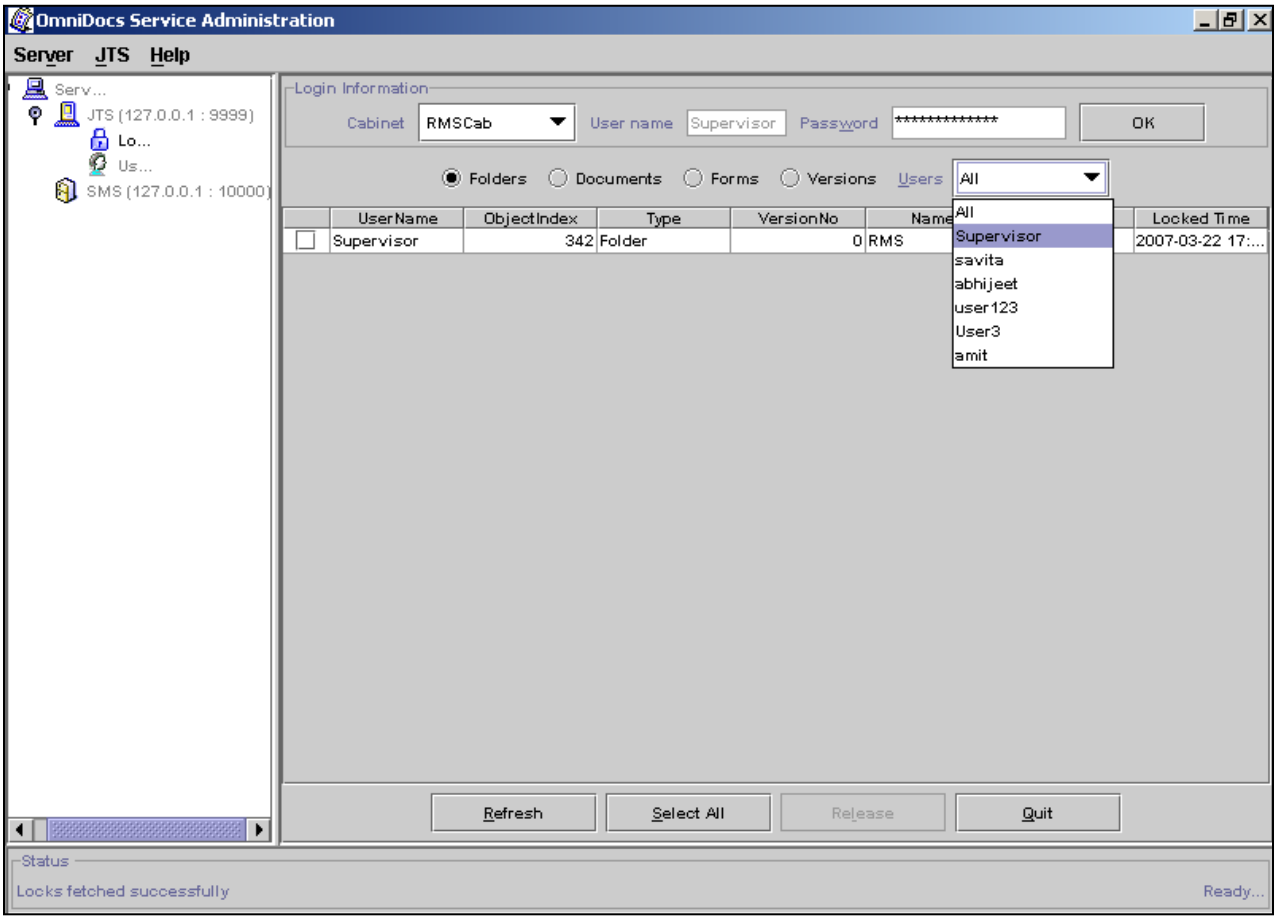


Figure 3.131

2. The locks associated by the selected user on the selected options (folders, documents, forms, and versions) are displayed below.

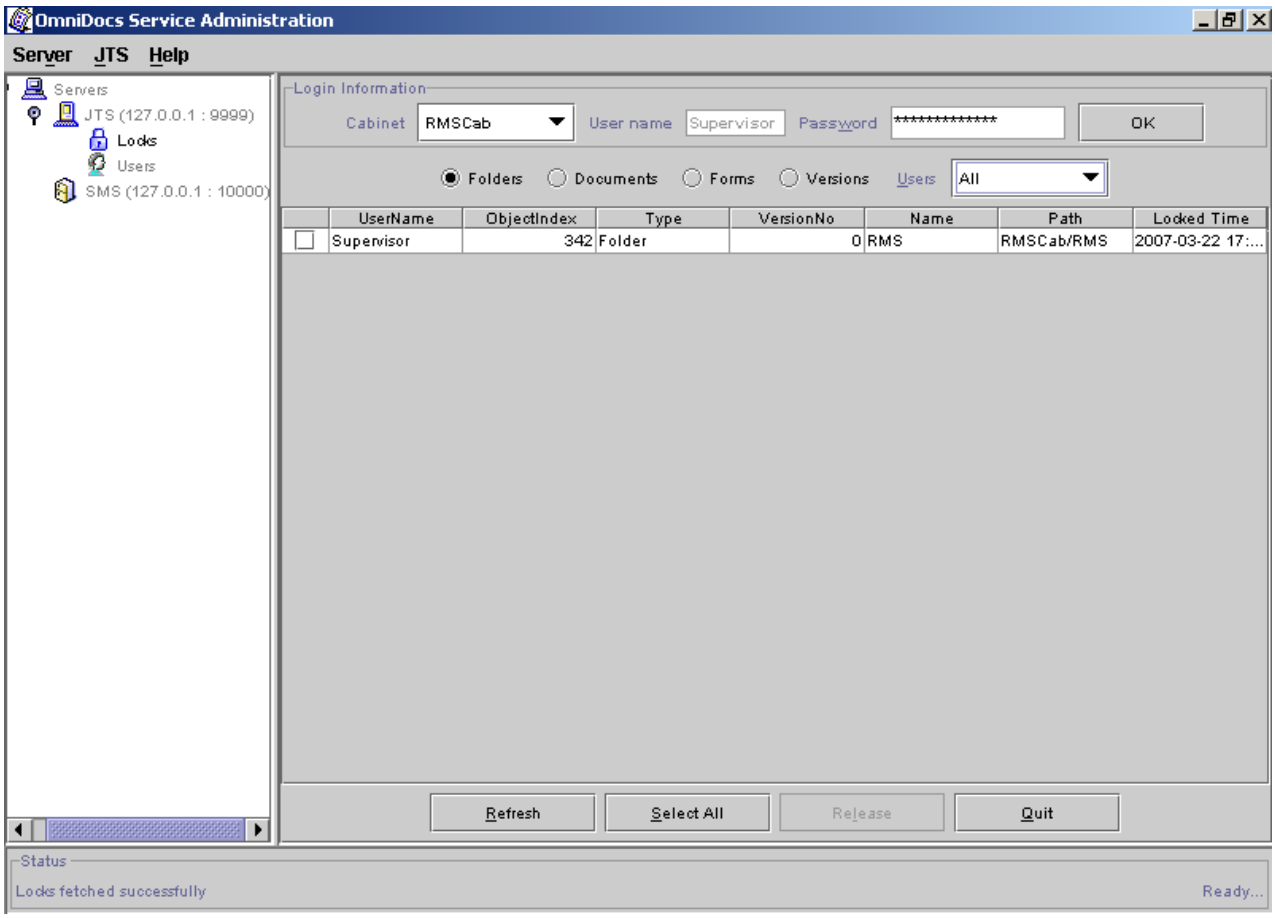


Figure 3.132

3. Check the locks that have to be released in the **Select column**.
4. To select all the locks, click **Select All**.

NOTE:

Select All is a toggle button, which changes to Deselect All.

---

5. Click **Release** button to release all the selected locks.
6. Click **Refresh** button to refresh the screen.
7. Click **Quit** button to log out from the cabinet.

3.6 Viewing Users

To view the users who are currently logged into a cabinet:

1. Select **Users**.

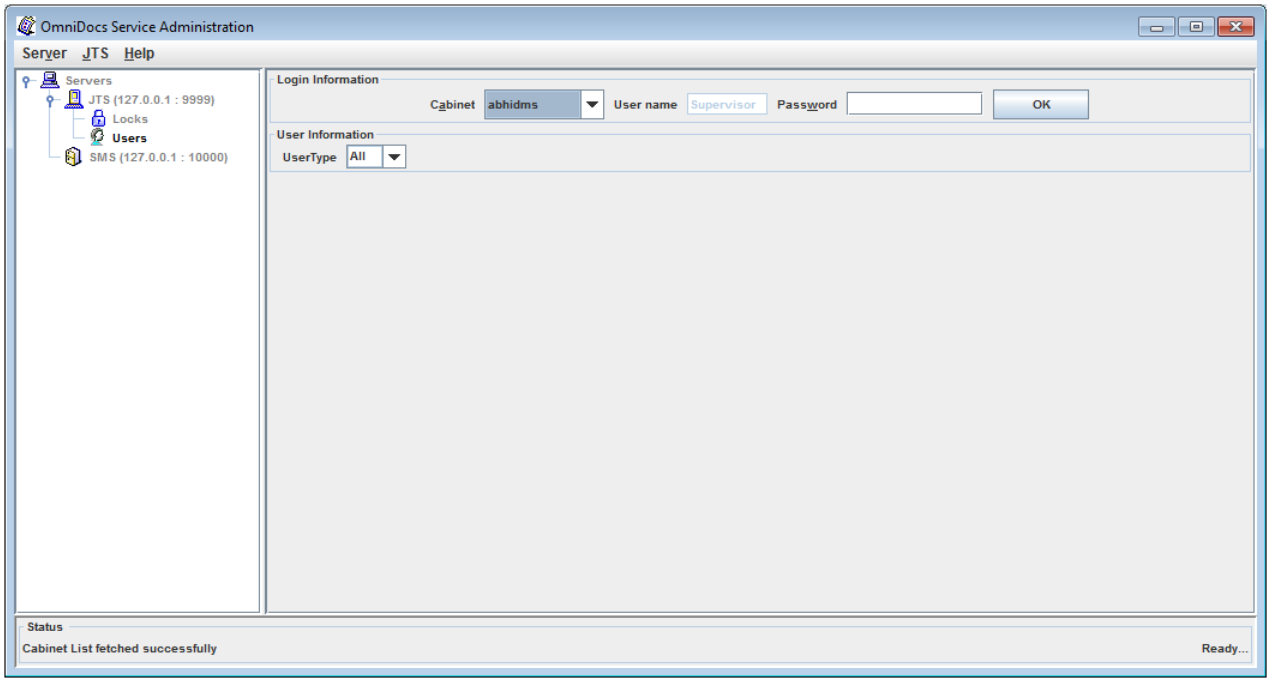


Figure 3.133

2. Select the required cabinet whose login users are to be seen from the **Cabinet** dropdown list.

   Concept:

   - The JTS can have multiple cabinets associated with it.
   - Each cabinet can have users connected to it. Therefore, the cabinet whose login users are required has to be selected from the Cabinet dropdown list.

3. Specify the password for the Supervisor of the cabinet in **Password** edit box.

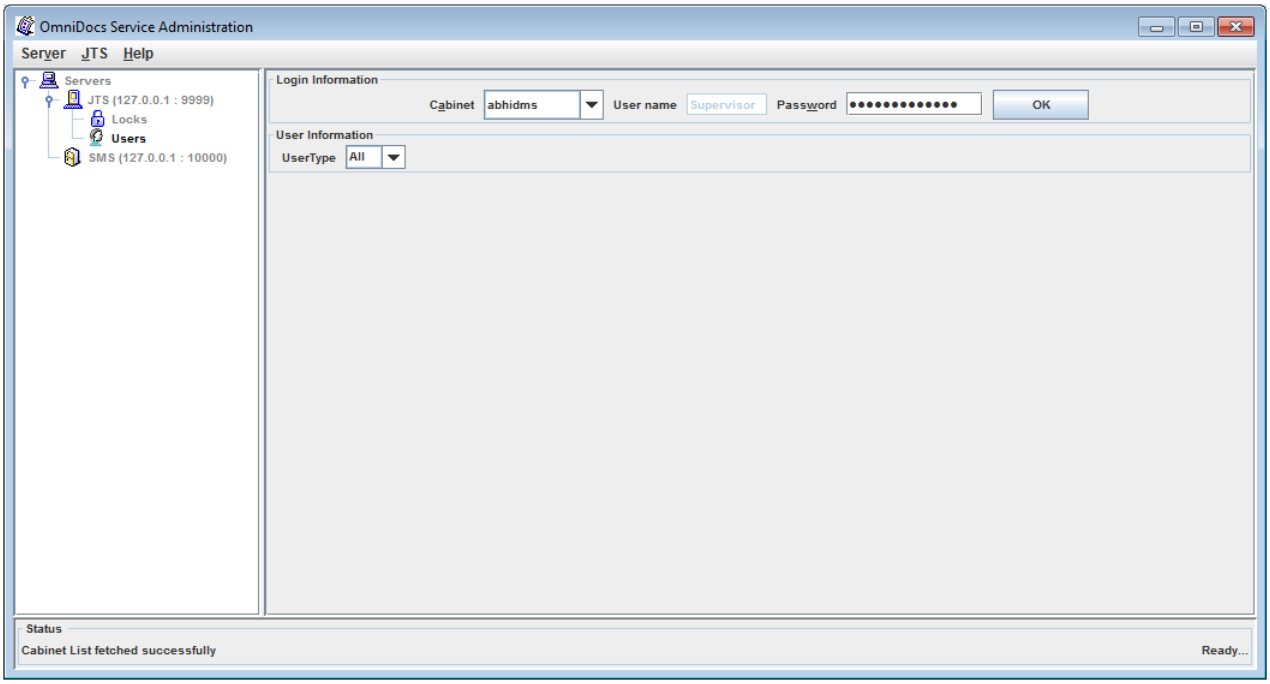


Figure 3.134

4. Click **OK** button to proceed. A list of all the users connected to the specified cabinet is displayed.

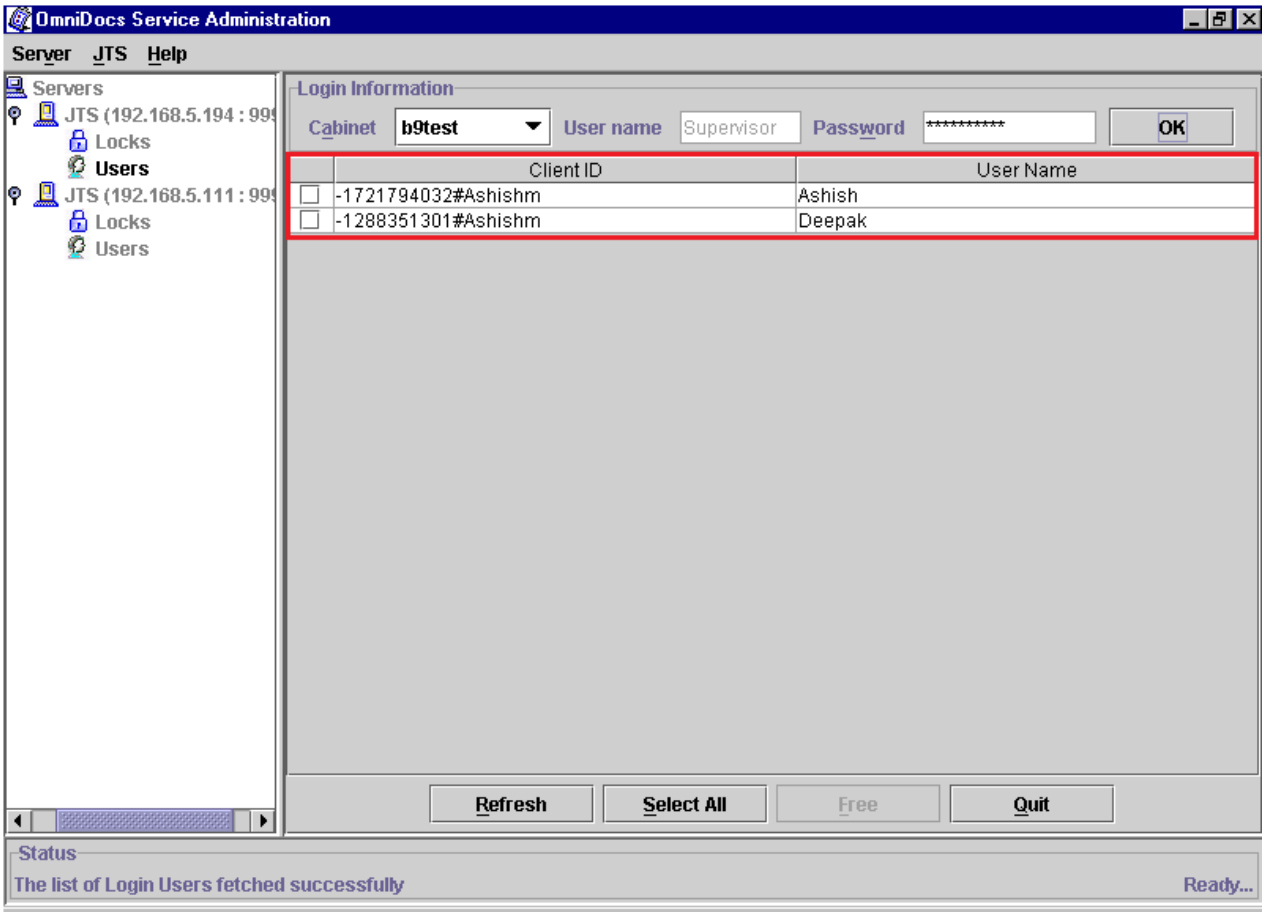


Figure 3.135

To disconnect the selected users:

1. Select the users that need to be disconnected.
2. Click the **Select All** button to select all the users connected with the cabinet.

NOTE:

Select All is a toggle button, which changes to Deselect All.

---

3. Click the **Free** button to disconnect the selected users from the cabinet.
4. Click the Refresh button to refresh the screen.
5. Click **Quit** to logout from the cabinet

3.7 Ways of Logging

The following two users can log in to the OmniDocs Service Administration (OSA), these are:

- System and
- Supervisor

NOTE:

The **System** user needs to have a more comprehensive knowledge of JTS to perform additional operations effectively.

3.7.1 Login as System

To log-in as System:

1. Select the username “System” from the **User** dropdown list.

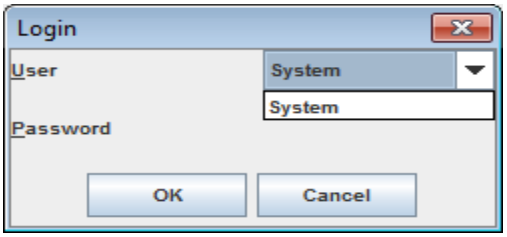


Figure 3.136

2. Specify the password in the **Password**.
3. Click the **OK** button to connect.
4. Click the **Cancel** button to close the **Login** dialog box.

3.7.2 Login as Supervisor

To log in as Supervisor:

1. Select the username “Supervisor” from the **User** dropdown list.

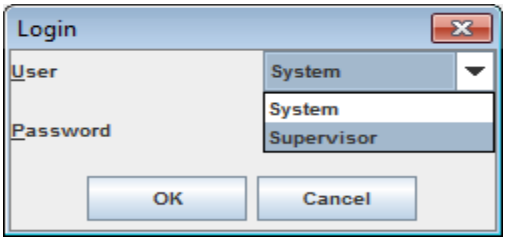


Figure 3.137

2. Specify the password in the **Password**.
3. Click the **OK** button to connect.
4. Click the **Cancel** button to close the **Login** dialog box.

3.8 Thumbnail Manager Operations

The Thumbnail Manager is a utility that does the following activities:-

- It creates Thumbnails for documents of the registered cabinets.
- It also listens on a port for requests to create thumbnails for specified documents.

NOTE:

Follow steps written in "How to configure Thumbnail Manager.docx" available in the Thumbnail Manager Folder of the OD Installation Folder.

To perform operations on the Thumbnail Manager:

1. Click **Thumbnail Manager** from the **Servers** list in the left pane of the OSA screen.

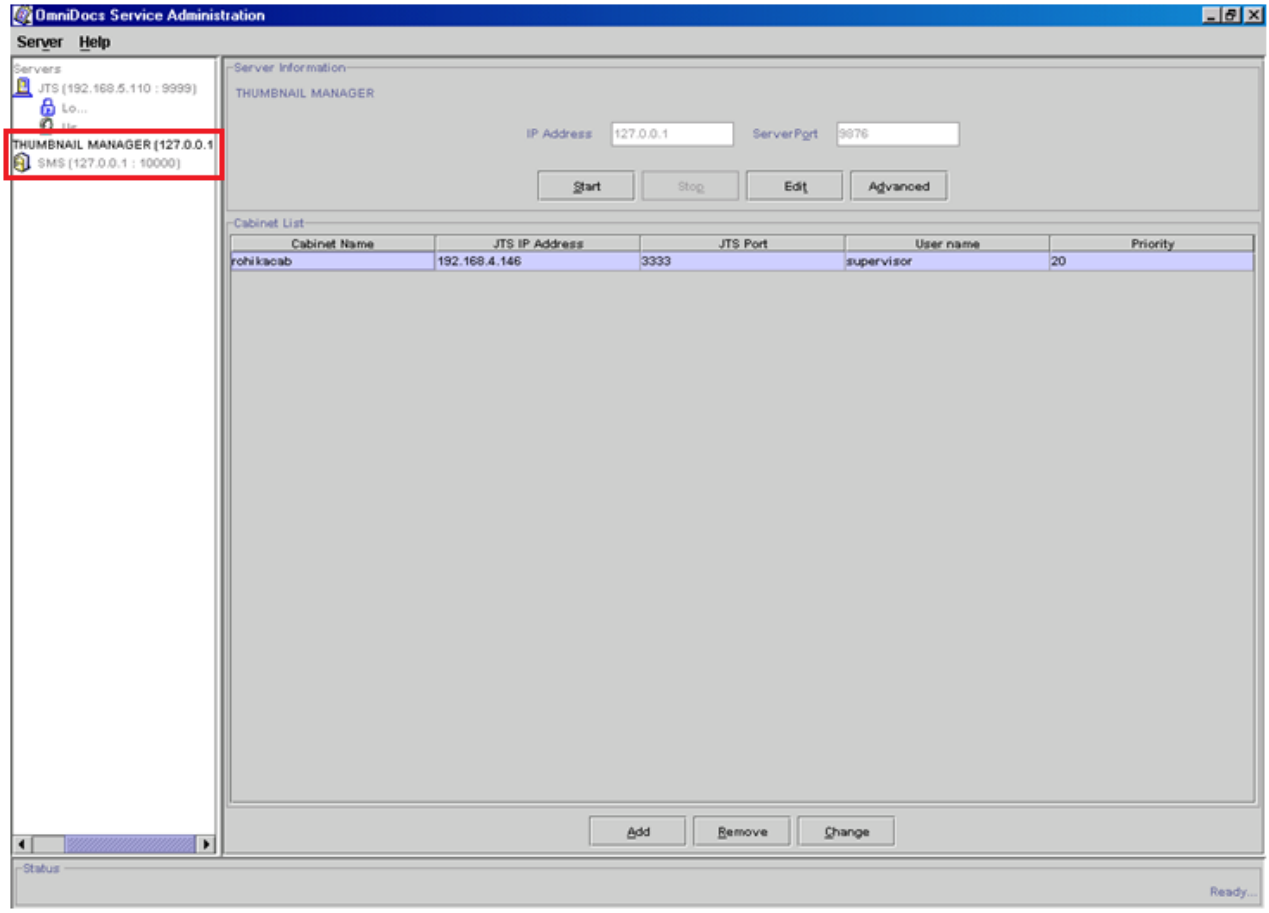


Figure 3.138

2. Server information contains:
    - IP Address
    - Server Port
3. Click the **Stop** button to stop the server.
4. Once the server is stopped, the following buttons get enabled.
    - Start
    - Edit
    - Remove
    - Advanced
    - Change
5. Click the **Edit** button to edit the **Server Port**.

NOTE:

Edit is a toggle button, which changes to Update button.

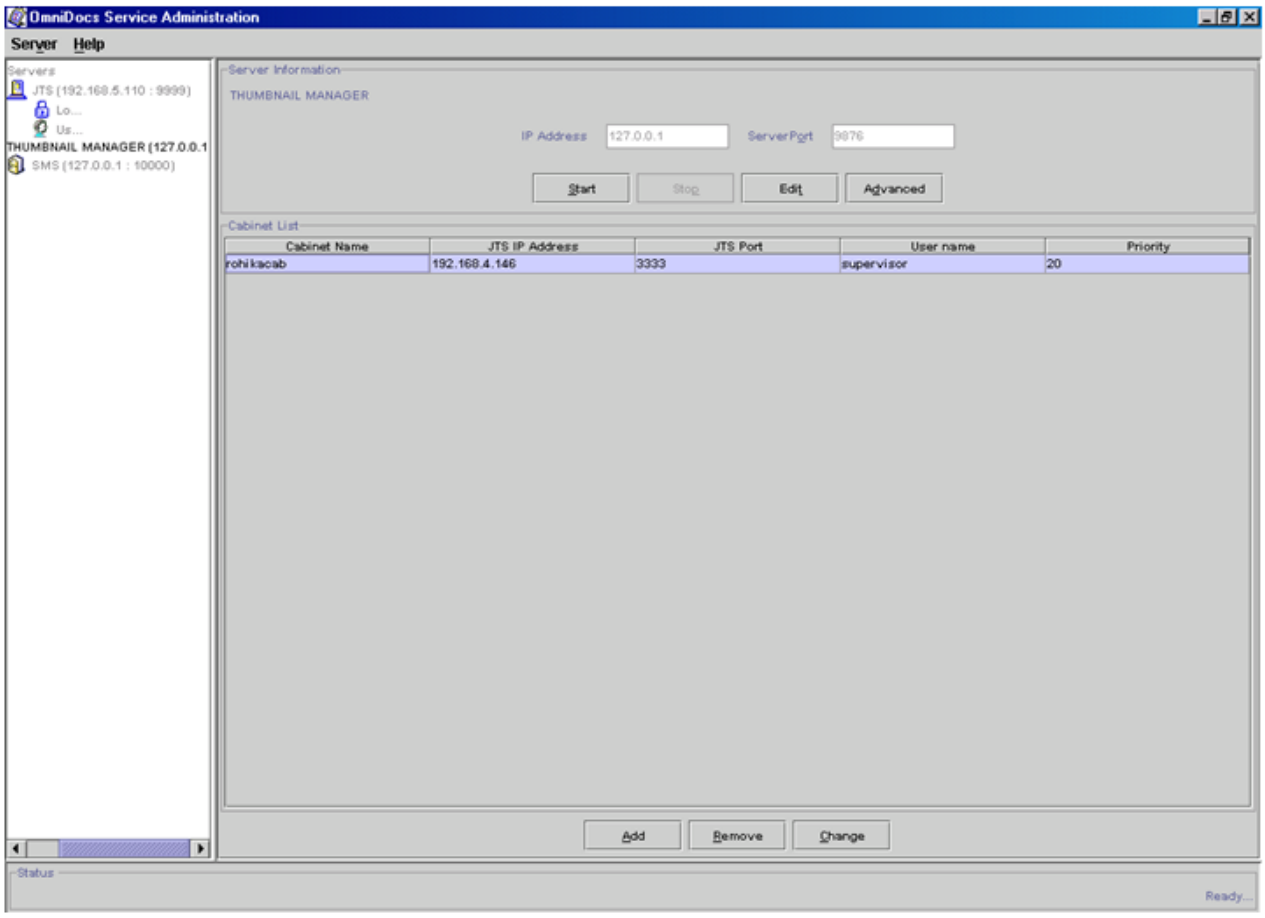


Figure 3.139

6. Make the required changes.
7. Click **Update**.
8. Click the **Advanced** button.
9. Advanced dialog box appears.

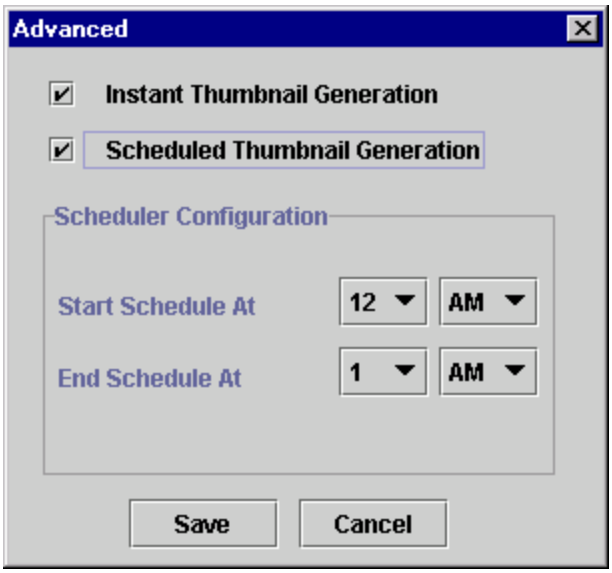


Figure 3.140

- Select **Instant Thumbnail Generation** checkbox to generate Thumbnails instantly.

  This feature is applicable in the case of OmniDocs Web. When an image document is added to OmniDocs Web, the thumbnails of the only first page (of that document) are generated instantly.
- Select **Scheduled Thumbnail Generation** checkbox to generate Thumbnails according to the scheduled time.
- Specify Start schedule time in **Start Schedule At** combo box.
- Specify End schedule time in **End Schedule At** combo box.
- Click the **Save** button to save the required changes.

  Else, click the **Cancel** button.

3.8.1 Adding a Cabinet

To add a Cabinet:

1. Click the **Add** button.
2. The **Add Cabinet** dialog box is invoked.

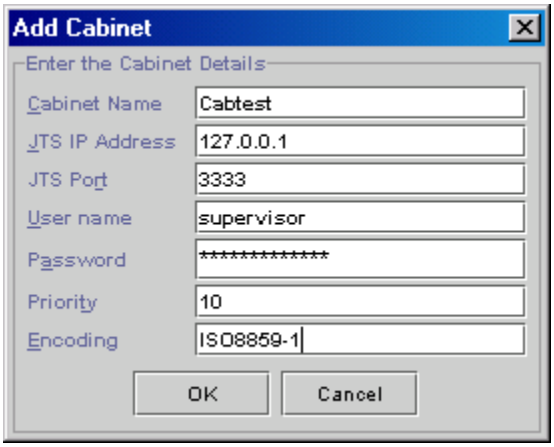


Figure 3.141

3. Specify the Cabinet name in the **Cabinet Name** textbox.
4. Specify the JTS IP Address in **JTS IP Address** textbox.

   (This is the IP Address of the JTS where the cabinet is associated).
5. Specify the JTS Port in **JTS Port** textbox.

   (This is the Port of the JTS where the cabinet is associated).
6. Specify the Cabinet's user name in **User Name** textbox.

   (This is the user name with which the Thumbnail manager would log in into the JTS).
7. Specify the password in **Password** textbox.

   (This the Password for the specified user name).
8. Specify the Priority in **Priority** text field.

   (This is the Priority of the cabinet for the other cabinets registered with the Thumbnail Manager).
9. Specify the Encoding in the Encoding textbox.

   (This is used to identify the language that is used by the user).

NOTE:

To run a Thumbnail manager, the encoding used is UTF-8.

10. Click the **OK** button.
11. Click the **Cancel** button to close the **Add Cabinet** dialog box.
    - If the Thumbnail Manager is running then you can add a Cabinet.
    - If the Thumbnail Manager is not running then you can,
        - Add a Cabinet.
        - Remove a Cabinet.
        - Change the Cabinet Property.

3.8.2 Removing Cabinet

To remove the Cabinet:

1. Select the Cabinet that needs to be removed from the list.
2. Click the **Remove** button.
3. A message box is invoked prompting whether you want to remove the selected Cabinet from the list.

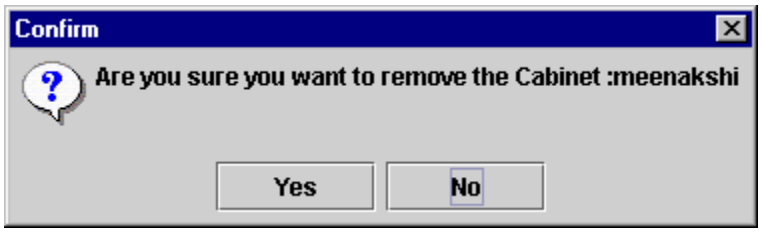


Figure 3.142

a. Click the **Yes** button to remove the selected Cabinet from the list.

b. Click the **No** button to avoid removing the selected Cabinet from the list.

3.8.3 Changing the Cabinet property

To change the property of the Cabinet:

1. Select the required Cabinet, whose user name/password needs to be changed from the list.
2. Click the **Change** button.
3. The **Change Cabinet Property** dialog box is invoked.

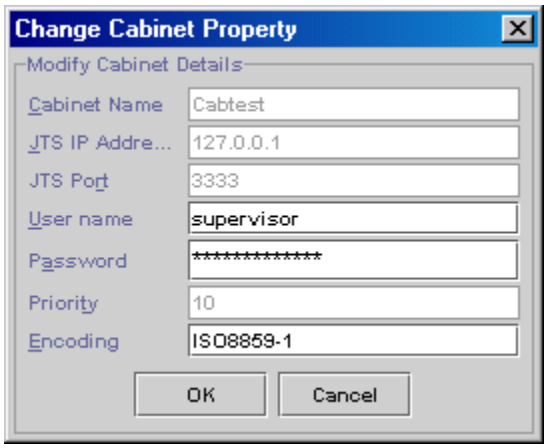


Figure 3.143

4. The only editable modes are the **User Name** and **Password**.
5. Click the **OK** button to close the **Change Cabinet Property** while saving the changes made.
6. Else, click the **Cancel** button.

3.9 Alarm Mailer Operations

Alarm Mailer is a utility that polls the JTS for alarms and dispatches them in case any alarms are set.

For performing operations on the Alarm Mailer:

1. Click the **Alarm Mailer** from the **Servers** list.

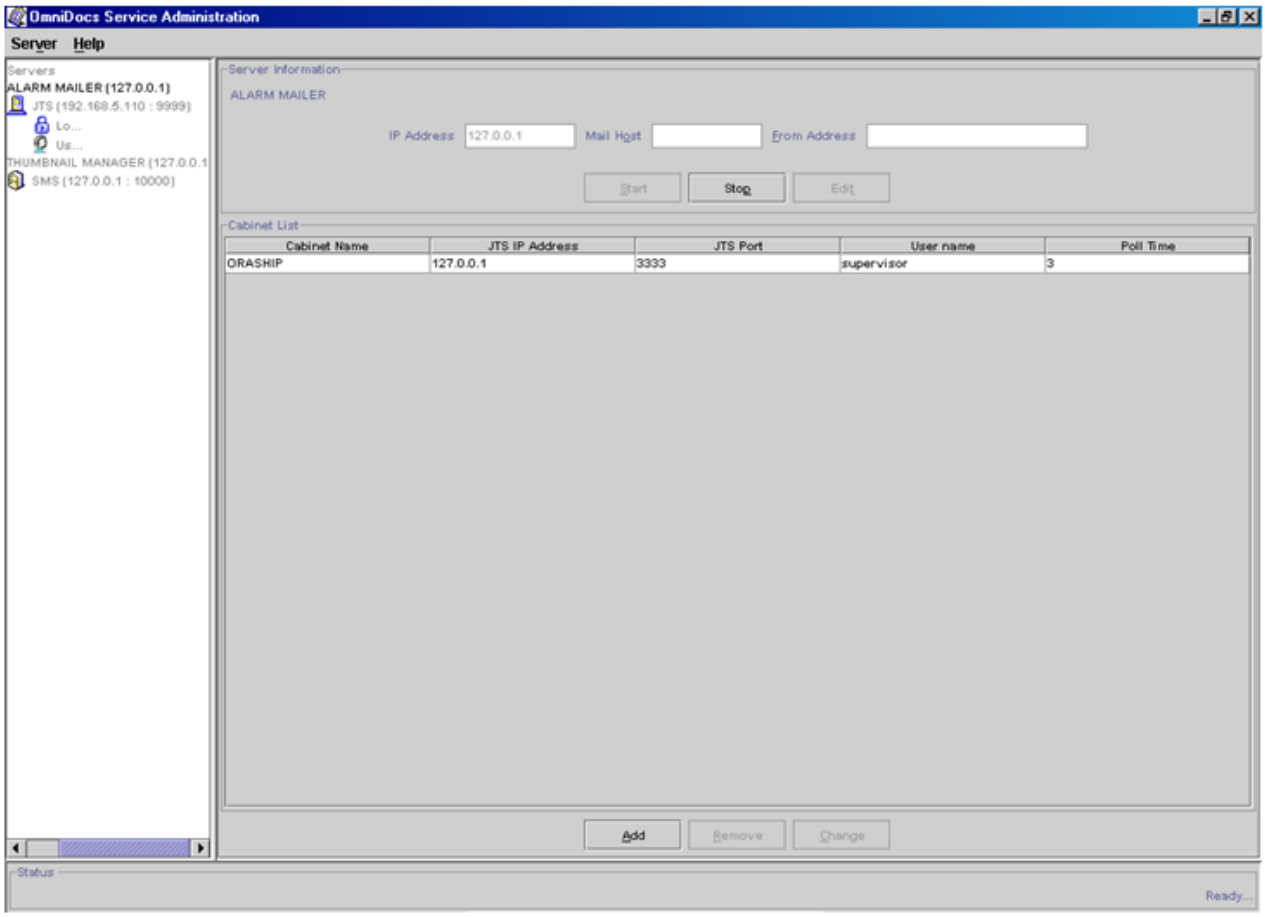


Figure 3.144

2. Displayed Server information contains:
   - IP Address
   - Mail Host
   - From Address
3. Click the **Stop** button to stop the server.
4. Once the server is stopped, the following buttons get enabled:-

- Start
- Edit
- Remove
- Change

5. Click the Edit button:
    - To edit the Mail Host
    - To edit the From Address

NOTE:

Edit is a toggle button, which changes to Update.

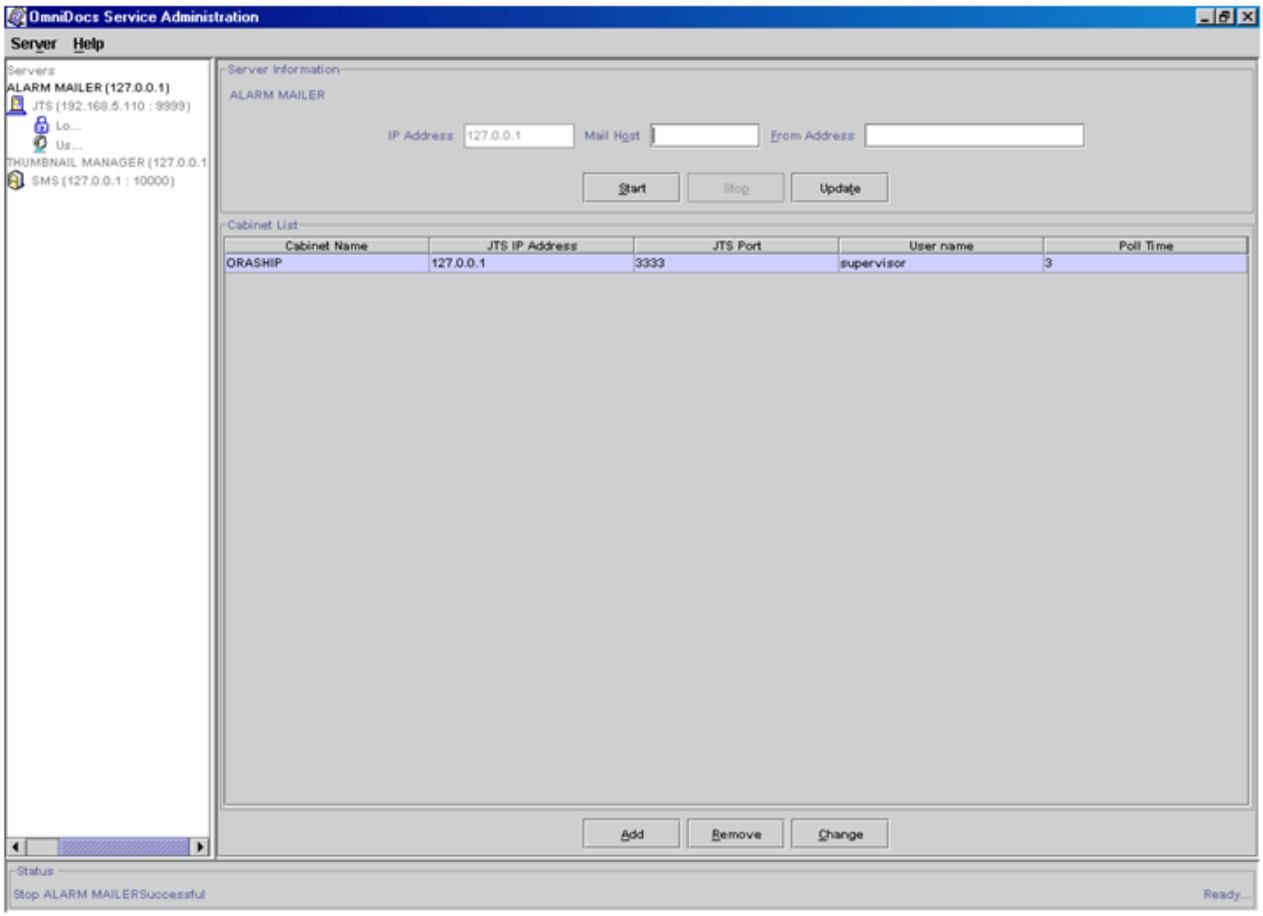


Figure 3.145

6. Make the required changes.
7. Click **Update**. The updated changes are immediately reflected.

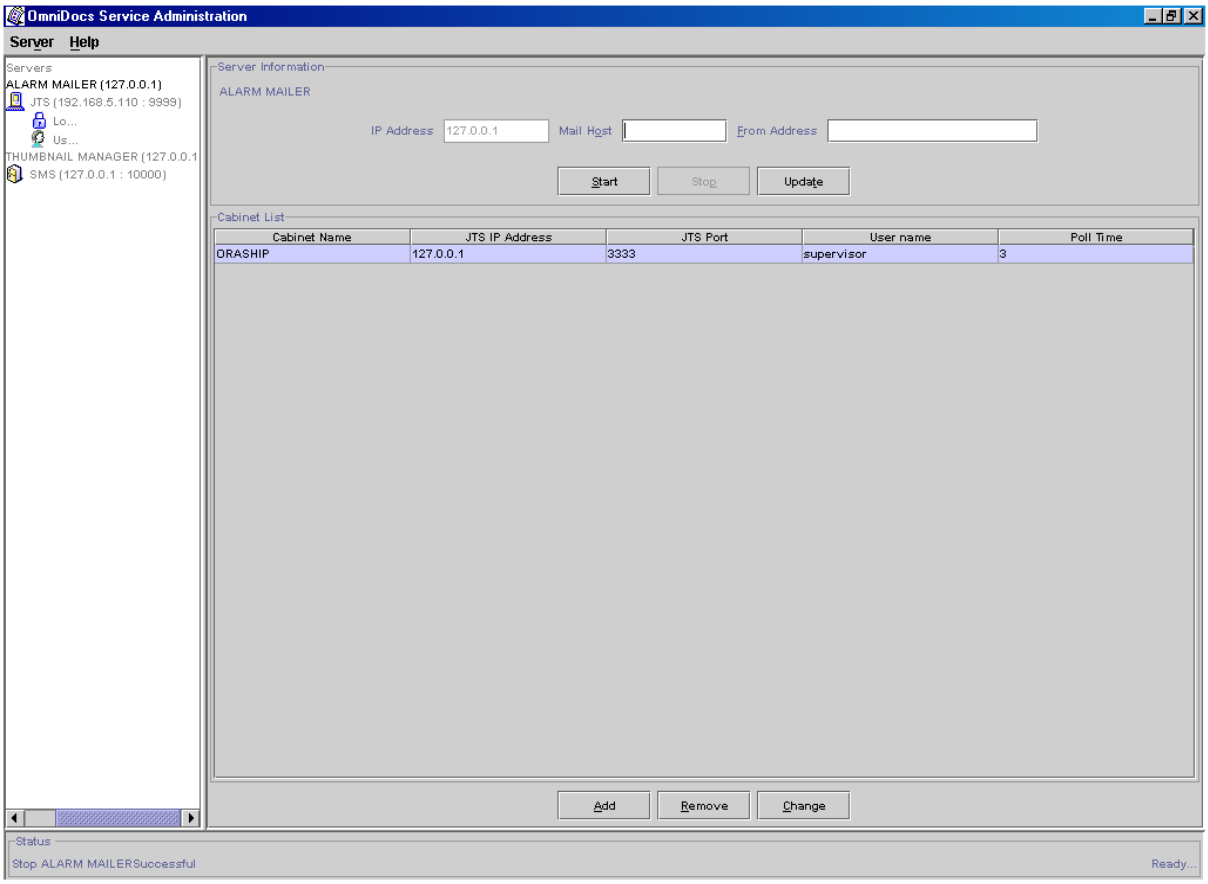


Figure 3.146

3.9.1 Adding a Cabinet

To add a Cabinet:

1. Click the **Add** button.
2. The **Add Cabinet** dialog box is invoked.

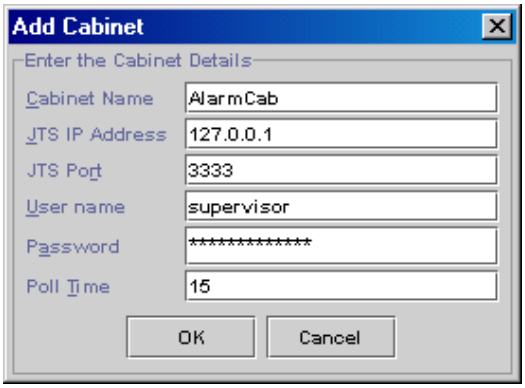


Figure 3.147

3. Specify the Cabinet name in the **Cabinet Name** textbox.
4. Specify the JTS IP Address in **JTS IP Address** textbox.

   (This is the IP Address of the JTS where the cabinet is associated).
5. Specify the JTS Port in **JTS Port** textbox.

   (This is the Port of the JTS where the cabinet is associated).
6. Specify the Cabinet's User name in **User Name** textbox.

   (This the user name with which the Alarm Mailer would log in into the JTS).
7. Specify the Password in **Password** textbox.

   (This the Password for the specified user name).
8. Specify the Poll time in **Poll Time** textbox.

   (This is the time in minutes after which the Alarm Mailer would call the JTS).
9. Click the **OK** button.
10. Click the **Cancel** button to close the **Add Cabinet** dialog box.

- If the Alarm Mailer is running from OSA, the user can add a Cabinet.
- If the Alarm Mailer is not running from OSA, the user can:
  - Add a Cabinet.

- Remove a Cabinet.
- Change the Cabinet Property.

3.9.2 Removing Cabinet

To remove the Cabinet:

1. Select the Cabinet that needs to be removed from the list.
2. Click the **Remove** button.
3. A message box is invoked prompting whether you want to remove the selected Cabinet from the list.

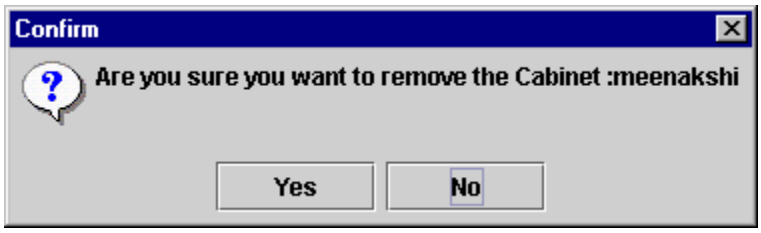


Figure 3.148

a. Click the **Yes** button to remove the selected Cabinet from the list.

b. Click the **No** button to avoid removing the selected Cabinet from the list.

3.9.3 Changing the Cabinet Property

To change the property of the Cabinet:

1. Select the required Cabinet, whose user name/password needs to be changed from the list.
2. Click the **Change** button.
3. The **Change Cabinet Property** dialog box is invoked.

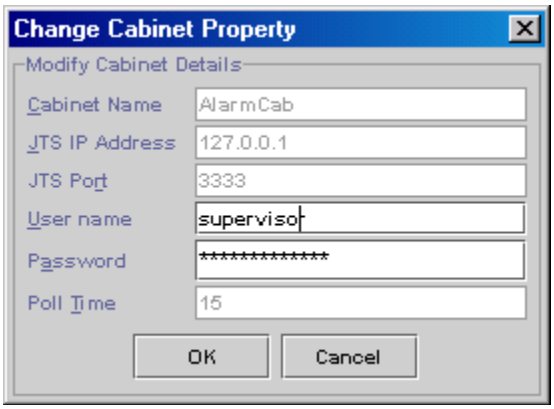


Figure 3.149

4. The only editable modes are the **User Name** and **Password**.
5. Click the **OK** button to close the **Change Cabinet Property** while saving the changes made.
6. Else click the **Cancel** button.

3.10 Menu Options

The various menu options are:

- Server Menu
- JTS Menu
- SMS Menu

3.10.1 Server Menu

Start: Starts the server

Stop: Stops the server

Register: Registers a new server.

Unregister: Unregisters the selected server.

Disconnect: Disconnects from the selected server.

Manage: Manages the selected server.

Change Password: Enables to change the password of the connected users.

Exit: Exits from the application.

3.10.2 JTS Menu

Edit: Enables editing of server port, transaction log, connection log, server time out and batch size.

Create: Enables in creating a cabinet.

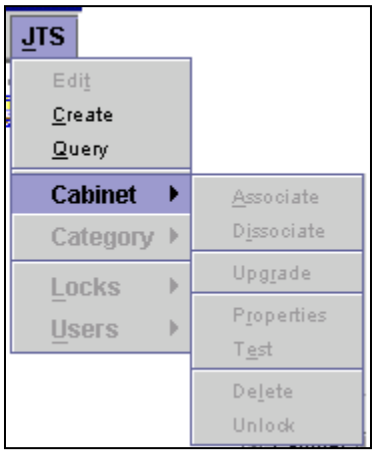


Figure 3.150

Query

Cabinet: A cabinet is a central storage unit that can be connected to a desktop through a server.

Associate: Registers the selected cabinet with JTS.

Disassociate: Unregisters the selected cabinet with JTS.

Upgrade: Upgrades the cabinet.

Properties: Enables viewing/changing the properties of the selected cabinet.

Test: Tests the database validity for the selected cabinet.

Delete: Deletes the selected cabinet along with the associated database.

3.10.3 SMS Menu

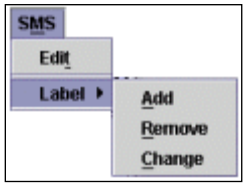


Figure 3.151

Edit: Enables to change the server port.

Label

- Add: Enables to add the SMS label.
- Remove: Enables to change the path associated with the SMS label.
- Change: Enables to change the path associated with the label.

3.11 Change Password

To change the password:

1. Click **Server** menu and then click **Change Password**.
2. The **Change Password** dialog box is invoked.

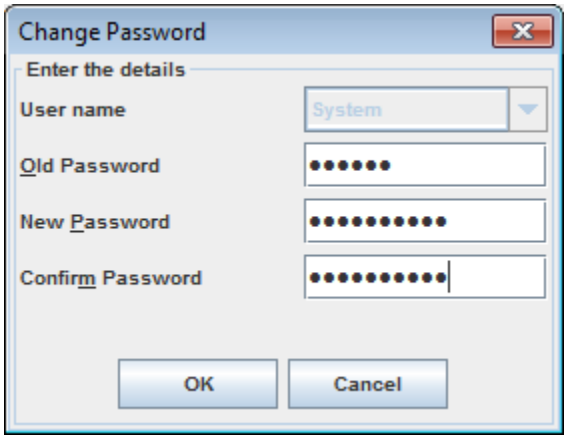


Figure 3.152

3. Enter the old password in **Old Password** textbox.
4. Enter the new password in **New Password** textbox.
5. Re-enter the new password in **Confirm Password** textbox.
6. Click **OK** button to close **Change Password** dialog box while saving the changes made.
7. Click **Cancel** button to close the **Change Password** dialog box without saving the changes made.

4 Call Interception Architecture

OmniDocs Server Architecture provides a framework to extend/customize the behavior of standard XML-based APIs. This framework can be used to perform tasks in addition to the standard behavior as a part of the same transaction. A typical example of this could be accessing/updating other tables, extending user authentication policies, validations, etc.

This chapter describes how to intercept and extend OmniDocs API. The component that is created for this is henceforth referred to as **API Hook**.

4.1 Classes and Components Required for Hook Implementation

The HookClass, HookHandler, and HookImplementer classes are required for hook implementation. These classes are provided with OmniDocs Server setup in the following jar files:

- **NGJTS.jar** file for OmniDocs JTS version.
- **omnidocs_hook.jar** file for OmniDocs J2EE version.

  Specifically, **omnidocs_hook.jar** will be at the following locations:

For OmniDocs-JBOSS Application Server Setup

In <Drive:>/<Directory in which JBOSS Application Server is installed>/server/<JBOSS Application Server Configuration for OmniDocs>/lib folder.

For OmniDocs-Oracle10G Application Server Setup

In <Drive:>/<Directory in which Oracle10g Application Server is installed>/j2ee/<OmniDocs Oc4j instance directory>/applib folder.

For OmniDocs-Sun Java System Application Server Setup

In <Drive:>/<Directory in which Sun Java Application Server is installed>/domains/domain-n/server-n/lib folder.

For OmniDocs-WebSphere Application Server Setup

In <Drive:>/<Directory in which WebSphere Application Server is installed>/AppServer/profiles/<WebSphere Application Server profile directory>/<OmniDocs Shared Library directory>.

For OmniDocs-WebLogic Application Server Setup

In <Drive:>/<Directory in which WebLogic Application Server is installed>/user_projects/domains/<Omnidocs domain directory>/Jars folder.

Steps for implementing hooks:

NGJTS.jar/omnidocs_hook.jar has the classes, **HookClass**, **HookHandler,** and **HookImplementer** in the package **com.newgen.omni.jts.srvr. HookHandler** contains an object of **HookClass**, namely **hookObject**.

HookImplementer is a singleton for reading HOOK properties files, which stores the names of all **API Hooks** that are to be executed.

The following steps need to be taken for creating a hook for a particular transaction:

1. If the name of the transaction is NGOxyz, then the name of the hook class should be HOOKxyz. For example, if the Transaction class is NGOAddUser, the corresponding hook class should be HOOKAddUser.
2. The hook class should be defined under the package name of **com.newgen.omni.jts.hook**.
3. The hook class should extend the abstract base class **com.newgen.omni.jts.srvr.HookHandler**.
4. The abstract base class, HookHandler has two abstract methods defined as
   i. abstract public String executeIn(String strInputXML);
   ii. abstract public String executeOut(String strOutputXML);
5. The user-defined hook class must provide the implementation for both methods. **executeIn()** method should be used for any processing that needs to be done before the execution of the actual OmniDocs transaction, and **executeOut()** method should be used for processing that needs to be done after execution of the actual OmniDocs transaction.

6. The minimum implementation for these two methods must be to return the input String i.e. the string passed in the input parameter.
7. To throw any error within these two methods, the **setStatus(int)** and **setMessage(String)** should be called on the object **hookObject**, e.g
   - hookObject.setStatus(-78999);
   - hookObject.setMessage("Test For Error");.

   In this case, the outputXML returned to the client will contain the error code along with the given message.

NOTE:

hookObject is the object of HookClass declared in HookHandler class and will be available by default.

---

8. Once the hook class has been created and packaged appropriately, the Hook class name must be added to the HookData.xml, which is located at the following locations:

   For OmniDocs-JTS Setup

   <Drive:>/Program Files/OmniDocs Server.

   For OmniDocs-JBOSS Application Server Setup

   In <Drive:>/<Directory in which JBOSS Application Server is installed>/bin/ngdbini folder.

   For OmniDocs-Oracle10G Application Server Setup

   In <Drive:>/<Directory in which Oracle10g Application Server is installed>/j2ee/home/ngdbini folder.

   For OmniDocs-Sun Java System Application Server Setup

   In <Drive:>/<Directory in which Sun Java Application Server is installed>/domains/domain-n/server-n/config/ngdbini folder.

   For OmniDocs-WebSphere Application Server Setup

   In <Drive:>/<Directory in which WebSphere Application Server is installed>/AppServer/profiles/<WebSphere Application Server profile directory>/ ngdbini folder.

For OmniDocs-WebLogic Application Server Setup

In <Drive:>/<Directory in which WebLogic Application Server is installed>/user_projects/domains/<Omnidocs domain directory>/ ngdbini folder.

Sample HookData.xml

```
<HookInfo>
    <!-- Hook Names that are intended to exist in the system.  -->
    <HookName>HookAddUser</HookName>
    <HookName>HookAddFolder</HookName>
</HookInfo>
```

NOTE:

Only the existence of this file at the specified locations and a corresponding entry for each Hook will result in the execution of the Hook.

9. If no hook is defined for a transaction, JTS will continue as usual.

Example: Code for HOOKAddUser class

```
package com.newgen.omni.jts.hook;
public class HOOKAddUserextendscom.newgen.omni.jts.srvr.HookHandler{
        public String executeIn(String strInputXML){
// any processing to be done here.
Connection con = hookObject.getConnection(); // to obtain Connection
                                        object passed to Hook
//hookObject.setStatus(-78999);          // to throw any error
//hookObject.setMessage("Test For Error"); // to throw any error
return strInputXML;
}
public String executeOut(String strOutputXML){
        // any processing to be done here.
        return strOutputXML;
        }
}
```

NOTE:

In case the Connection Object passed to Hookclass is being used, then only the Statements and ResultSet objects obtained using the Connection Object have to be closed. The Connection object should not be closed.

4.1.1 Steps for Deploying User's Hook Implementation

Create a jar file containing the "**.class**" files for the user-defined implementation of Hooks. Assuming that the jar thus created is named "**omni_hook.jar**".

For OmniDocs-JTS setup

1. Stop JTS.
2. omni_hook.jar should be placed in <Drive:>/Program Files/OmniDocs Server.
3. Go to command prompt
4. Type regedit.
5. Expand HKEY_LOCAL_MACHINE
6. Expand SYSTEM-> expand CurrentControlSet.
7. Expand Services.
8. Expand JTS.
9. Expand Parameters.
10. Right-click on the **AppParameters** string and select modify.
11. Then add omni_hook.jar to the classpath.

    For example,

    Djava.class.path=.;**omni_hook.jar**;jce1_2_2.jar;SecurityAPI.jar;classes12.zip;msbase.jar;mssqlserver.jar;msutil.jar;ngjts.jar;SQLTransaction.jar;ORATransaction.jar

    wrkdir=C:\PROGRAMFILES\OMNIDOCSSERVER
12. Add corresponding HookName tag in HookData.xml.
13. Start JTS.

For OmniDocs-J2EE setup

1. "**omni_hook.jar**" should be placed at the following locations:

   For OmniDocs-JBOSS setup

   In <Drive:>/<Directory in which JBOSS Application Server is installed>/server/<JBOSS Application Server Configuration for OmniDocs>/lib folder.

   For OmniDocs-Oracle10G setup

   In <Drive:>/<Directory in which Oracle10g Application Server is installed>/j2ee/<OmniDocs Oc4j instance directory>/ applib folder.

   For OmniDocs-Sun Java System Application Server setup

   In <Drive:>/<Directory in which Sun Java Application Server is installed>/domains/domain-n/server-n/lib folder.

2. Add corresponding HookName tag in HookData.xml.
3. Restart the application Server Instance.

5 Configuration File Management Architecture

One of the challenges while developing J2EE applications is the management of the Application's Configuration settings. Configuration parameters could range from logging settings, information concerning database server, user settings, etc, and could be loaded from some configuration files that reside outside the Application's deployable components.

Although J2EE provides for some externalization, through J2EE-specific constructs (data sources or via references, etc) but often that is not enough. Applications require some configurable parameters to be editable by the Application/Server Administrator and hence these files cannot be localized to the Application's deployable components, (EAR, WAR, or JAR files).

Configuration files could be loaded from the Application Server's Current Working Directory, (JVM's "user.dir" property) but the exact location of the Current Working Directory differs with application servers.

5.1 Introduction to OmniDocs Configuration File Management Architecture

OmniDocs setup on the Application server requires the following configuration files and folders to be placed in the Current Working Directory of the Application Server:

- Ngdbini : Configuration files exist in this folder.
- Mssql : Mssql Procedures exist in this folder
- Oracle : Oracle Procedures exist in this folder
- IS.ini : Configuration file

OmniDocs Configuration File Management Architecture makes use of URL resources to provide the user with the flexibility of deciding upon the location of the aforementioned configuration files.

Configuration File Management Architecture comprises of:

- OmniConfigLocator.java
- Omni_Configurations.xml

5.2 Managing OmniDocs Configurations

This section describes the how to manage OmniDocs configurations.

5.2.1 Omni_Configurations.xml

The idea of this XML file is to store the location of the configuration files and folders. This file has to be placed at the same level of "**omnishared.jar**".

NOTE:

Omnishared.jar's exact location varies for different Application Server's and the exact location can be determined from the corresponding OmniDocs Installation Manual.

"**Omni_Configurations.xml**" file has the following format:

```
<PathInfo>
<Location>
        <Name>Omni_Config_Location</Name>
        <Path></Path>
</Location>
</PathInfo>
```

First Scenario:

OmniDocs configuration files and folders have been placed at a location other than the Application Server's Current Working Directory.

The user needs to specify the location of OmniDocs configuration files and folders as the **"<Path>…</Path>"** tag's value in **"Omni_Configurations.xml" file**.

For example if IS.ini file, ngdbini, mssql, and oracle folders have been placed at the location "C:\Omni_config" then contents of this file need to be updated as follows:

```
<PathInfo>      <Location>
        <Name>Omni_Config_Location</Name>
        <Path> C:\Omni_config </Path>
</Location>
</PathInfo>
```

NOTE:

For Linux systems "/" is to be used as the path separator character, while specifying the "<Path>…</Path>" tag's value. Example: "\root\folder" is **not acceptable**. "/root/folder" is **acceptable**.

By default no value is specified for the **"<Path>…</Path>"** tag. On system start up, the Application Server's Current Working Directory will be treated as the desired location of the configuration files and folders and the absolute path of Application Server's Current Working Directory will automatically be updated to the **"<Path>…</Path>"** tag's value in **"Omni_Configurations .xml".**

While specifying the path of configuration files and folders in "**Omni_Configurations.xml**", a space character is not allowed.

Example: "c:\\New Folder\Dir" is not acceptable.

|

\/

Space exists

Second Scenario:

No value has been specified, for the **"<Path>…</Path>"** tag in **"Omni_Configurations.xml"** file.

In this case, start-up of OmniDocs application (for WebSphere AS only)/Application Server, Application Server's Current Working Directory will be treated as the desired location and the absolute path of Application Server's Current Working Directory will automatically be updated to the **"<Path>…</Path>"** tag's value in

"Omni_Configurations.xml" file. Hence in this case all folders and files must be in the Application Server's Current Working Directory.

NOTE:

This ensures backward compatibility with older versions of OmniDocs.

Third Scenario:

"Omni_Configurations.xml" file has not been placed at level, (read directory) of **"omnishared.jar".**

In case of the absence of **"Omni_Configurations.xml"** file at the level of **"omnishared.jar"**, Application Server's Current Working Directory will be treated as the desired location and the absolute path of the Application Server's Current Working Directory will automatically be updated to the **"<Path>…</Path>"** tag's value in **"Omni_Configurations.xml"** file. Hence, in this case, also, all folders and files must be in the Application Server's Current Working Directory.

6 Component Integration Framework

This section describes the following:

- Component Integration Framework for Web Module
- Component Integration Framework for Backend Module

6.1 Component Integration Framework for Web Module

To ensure easy and simplified integration of add-ons and other applications of OmniDocs the Integration Framework enhancement is launched.

This enhancement enables the application to run independently without making major changes in the OmniDocs web source code. The updating of the dependent files at the time of version release or updates is not required as a result of this enhancement. Now onwards OmniDocs web module and other web modules of other applications remain exclusive of each other.

A ComponentIntegration.xml is provided for this integration.

For an application to be integrated a <Component> tag is added in the xml as a child tag of <Components> tag.

Integration support is provided at three levels:

- OmniDocs Toolbar features
- Folder level features
- Document level features

Below is an example that shows integration with OmniDocs web using this framework:

```
<Components>
<Component Name="RMS">
<Module Type="Toolbar" Display="true">
<IconURL>http://ServerIP/RMS/images
/RMS.gif</IconURL>
<LaunchURL>http://ServerIP/RMS/login.j sp</LaunchURL>
</Module>
<Module Type="Folder" Display="true">
<DisplayName>RMSFolder</DisplayName>
<ParameterList>VolIndex=#VolIndex,DocListFolderId=#DocListFolderId,</ParameterList>
```

<LaunchURL>http://ServerIP/RMS/folder/addfolder.jsp</LaunchURL>

</Module>

<Module Type="Document" Display="true">

<DisplayName>RMSAddDoc</DisplayName>

<LaunchURL>http://ServerIP/RMS/Docum ent/adddoc.jsp</LaunchURL>

</Module>

</Component>

</Components>

Example Explanation:

1. Component Name is “RMS”.
2. There are three module types:
    - Toolbar
    - Folder
    - Document

1. The first Module is Toolbar:
    - The display attribute can be set as “true” or “false”. True is for enabling the icon and false is for disabling the icon.
    - IconUrl is the URL of the icon.
    - LaunchURL is the URL of the screen that will be launched by clicking the icon.
    - On launching the URL following parameters will be passed to the application:

Name of the Parameter	Value
CabName	Name of the cabinet.
UsrDbId	UserDbId of the user logged in.
jtsipadd	Ip address of JTS.
jtsport	Port of JTS.
CabID	Cabinet Id
DataBaseType	Type of the database (e.g., mssql, oracle, etc..)

Name of the Parameter	Value
GroupName	Group Name of the user logged in.
UserName	Name of logged-in user.
LoggedInUserIndex	User Index of the user logged in.
UserPassword	The password of the user logged in.
FromOD	Y

2. The second module is Folder:
    - The display attribute can be set as “true” or “false”. True is for enabling the link and false is for disabling the link.
    - Display name will be the name of the operation that will be displayed as the link (e.g., RMSFolder)
    - The parameters for the Folder are:
    - Vol Index: Volume Index of the folder
    - VolIndex=#VolIndex

The LHS bears the name of the parameter used in the add-on application while RHS bears the name of the parameter used in OmniDocs source code.

DocListFolderId: Index of the folder

DocListFolderId=#DocListFolderId The LHS bears the name of the parameter used in the add-on application while RHS bears the name of the parameter used in OmniDocs source code.

NOTE:

The parameter values are separated by comma (,).

FolderRights: LoggedIn user has rights on the folder.

FolderRights=#FolderRights

FolderName: The name of the folder

FolderName=# FolderName

FolderOwner: The owner who created the folder

FolderOwner=# FolderOwner

ParentFolderIndex: Index of the Parent folder.

ParentFolderIndex: Index of the parent folder.

ParentFolderIndex=#ParentFolderIndex

3. The third module type is Document.
    - The display can be set as True or False, if true the operation is visible else, hidden.
    - Display name will be the name of the operation that will be displayed as the link(e.g., RMSFolder)
    - On launching the URL following parameters will be passed to the application:

Name of the Parameter	Value
DocumentListId	Comma-separated list of selected document indexes
DocNameList	Comma-separated list of selected document names.
FolderId	Folder index of the selected folder.
FolderName	Folder name of the selected folder.
documentCreatedByAppNameList	Comma-separated list of selected document extensions.

NOTE:

The document list is sent as comma-separated values.

6.2 Component Integration Framework for Backend Module

OmniDocs Integration Framework has been devised to provide for smooth and seamless integration of applications to OmniDocs. The current implementation of the framework targets the following areas:

- Support for secondary applications on the Wrapper component.
- Support for compiling Database scripts for secondary applications.

6.2.1 Introduction to OmniDocs Integration Framework

Support for secondary applications on the Wrapper component.

To use the Wrapper Component secondary applications need to add their client- libraries to the Wrapper's classpath and update the <Wrapper_Directory>/ngdbini.

/CallRedirection.xml file to contain the name of various Transactional APIs and the fully qualified name of their corresponding Client.

To meet the aforementioned requirements and provide for smooth and seamless integration of applications to Wrapper component, OmniDocs Integration Framework makes use of "Java Extension Mechanism" and provides support for multiple "CallRedirection.xml" files.

Updating Wrapper's Classpath

The wrapper component comprises of "Wrapper_Lib" folder, which defines the classpath for Wrapper. Any jar file placed in the "Wrapper_Lib" folder will be automatically loaded to Wrapper's classpath, post restart. User doesn't need to update the "RunWrapper.bat" and "RunWrapper.sh" files nor the parameters for "NewgenWrapper" Service, (in case the Wrapper component has been deployed as a Windows Service).

Wrapper
|_ ngdbini\
|
|_Wrapper_Lib\
|
|_Other Files

Wrapper's Folder Structure

Application-specific CallRedirection.xml

<Wrapper_Directory>/ngdbini/CallRedirection.xml file contains the name of various Transactional APIs and the fully qualified name of their corresponding Client. There used to be a single "CallRedirection.xml" file that all applications were supposed to update, but with OmniDocs Integration Framework each application can have its own "CallRedirection_AppName.xml" file, where "AppName" could be any sequence of printable characters.

Wrapper
|_ ngdbini

||_ CallRedirection.xml
|
|_Wrapper_Lib\
|
|_Other Files

Wrapper's Folder Structure

Following guidelines must be followed, for all "CallRedirection_AppName.xml" files:

a) File Naming

All "CallRedirection_AppName.xml" files must have the ".xml" extension and their names must start with the "CallRedirection" string.

For example, "CallRedirection_OF.xml"

b) Location

All "CallRedirection_AppName.xml" files must reside in the ngdbini folder.

c) File Format

All "CallRedirection_AppName.xml" files must be in the given below format:

```
<Transactions>
<Transaction>
<Name>Call Name_1</Name>
<Path>Specified Path_1</Path>
</Transaction>
<Transaction>
<Name>Call Name_2</Name>
<Path>Specified Path_2</Path>
</Transaction>
<Transactions>
```

CallRedirection_AppName.xml format

NOTE:

Multiple "CallRedirection_AppName.xml" files must not have an entry for the same Transactional API.

"CallRedirection.xml" also resides at the Application Server level at the following location:

<**App_Server_User_Directory>/ngdbini** folder,

where "<**App_Server_User_Directory**>" is the Application Server's working directory, for example, in the case of JBoss Application Server "<**App_Server_User_Directory**>" would refer to "<**Drive:>/Jboss-4.0.2/bin**" directory.

Multiple "CallRedirection_AppName.xml" files and the above guidelines also apply at the Application Server level.

Support for compiling Database scripts for secondary applications.

To provide support for compiling Database Scripts of secondary applications, at the time of Cabinet creation, OmniDocs Server provides "Post.sql" file, in which database scripts are delimited using "~" character. These scripts could be used for creating the secondary applications table structure or for compiling stored procedures. All valid SQL scripts in "Post.sql" would be executed during the Cabinet creation process.

Post.sql support

Secondary applications add their SQL scripts in Post.sql using "~" as the script delimiter. All valid SQL scripts in "Post.sql" would be executed during the Cabinet creation process.

Now with OmniDocs Integration Framework, OmniDocs Server setup will no longer comprise of "Post.sql", it will henceforth be used only for providing support for secondary application.

Secondary Applications will have to place the "Post.sql" file in "<App_Server_User_Directory>/mssql/docdb" or "<App_Server_User_Directory>/oracle/docdb" folders, where "<App_Server_User_Directory>" is the Application Server's working directory, for example, in case of JBoss Application Server "<App_Server_User_Directory>" would refer to "<Drive:>/Jboss-4.0.2/bin" directory.

Only the presence of Post.sql file with valid SQL scripts, separated by the delimiter results in the functionality being included in the system.

7 Glossary

-A-

Action	Action refers to a particular task that has to be automated. For example, it can be a Leave Request, Purchase Request, Bill Approval, Loan Sanction Request, etc. Post Item is defined in the Administration Desktop.
Administration Desktop	For administering the Cabinets, Administration Desktop is maintained. Administration includes the creation of users, groups, data classes, assignment of rights, etc.
Alias	Synonyms that can be associated with a keyword
Authorize	Keywords for Cabinets are also created from the OmniDocs Desktop. But they can be authorized by Administration Desktop. The administrator authorizes the keywords made by users. Authorized Keywords cannot be modified.
Audit Trail	Audit Trail is a log on all the actions performed on the OmniDocs.

-C-

Cabinet	The cabinets are central storage units that can be connected to the desktop through a server.
Commit Type	Immediate commit type enables to saves the changes directly in the database. Delayed commit type enables you to save the changes in the scratch directory and then save them in the database as you click the Commit command button in the Volume Properties.
Compact	Compact means freeing disk space by deleting the already committed files.
Connect	Establishes the connection with the registered cabinet.

-D-

Data Class	Set of indexes that can be associated with the documents or folder for providing the unique entity to them.
Disconnect	Disconnects the registered cabinet. The documents and folders under the cabinet are not accessible if you disconnect the cabinet.
DOB Format	File format supported by Newgen OmniDocs. It saves the document image along with the data and annotations associated with it, as one file.

-E-

Everyone Group	Everyone group includes all the users created by the Administration Desktop. This group is not displayed in the group list, so you cannot modify it. But you can assign rights collectively to all the users by assigning the rights to the Everyone group.

-F-

Filter	Sorting on the related keywords by specifying the keyword with or without wild cards. (Wild card means *,#- for example avi*)
Folder	The folder is a repository for the documents.

-G-

Global Index	Global indexes are user-defined indexes or fields that could be associated with any document across the Cabinet. These indexes can be either associated with the data class or defined separately.
Group	The users can be clubbed together as a Group.

-I-

Image Server	Stores the document images in form of volume blocks.
Inbox	System folder for the Cabinet that contains all the messages and documents received by the users across the network.

-K-

Keywords	Words you would like to associate with the documents so that you can perform a search on them.

-L-

Locked	A particular user can lock a particular folder such that no other user can change the folder properties. The users can access documents present under that folder.

-M-

Mandatory	To make the data entry compulsory with an index, it can be defined as Mandatory. For example, if you are maintaining the Inventory list, the Item name and Item code indexes can be made mandatory.
Move Volume Block	Moving the contents of the volume block to another Disk.

-O-

Omni Server	Caters to the request to the OmniDocs Desktop users, brings data and document images from database and image storage respectively. It is divided into two parts: Image Server and Transaction Server.

-P-

Privileges	Specific rights assigned to the specific user by the Administrator. It enables the user to perform certain administrative functions. There are seven privileges.

-R-

Register	Registers the Cabinet for accessing the documents and folders under it.
Rights	Rights are defined as access permission for the users, for accessing an object. There are 5 rights – READ, CREATE, MODIFY, DELETE and ANNOTATE.

-S-

Supervisor	The supervisor has full rights on the Administration Desktop.
Supervisory Group	Supervisors are clubbed as a supervisory group and they are responsible for creating the objects for Cabinets.
Sites	Sites store the information on the Image Volumes and Volume Blocks.
SMS	SMS (Storage Management Server) is software that manages all kinds of storage devices used by you through a common front end.
Send Items	Send Items folder contains a copy of all the messages sent by the users across the network.

-T-

Transaction Server	Transaction Server listens to the request of the OmniDocs Desktop client and fetches the document image from the database.

Trash	The trash folder contains the deleted documents. If the documents are deleted from the trash folder, they cannot be restored.

-U-

Unauthorize	You can modify or delete only unauthorized keywords and create an alias for only Authorized keywords.
Unique Key	A unique key means the value associated with that index cannot be duplicated.
Unregister	Unregisters the selected Cabinet. After unregistering the Cabinet, it cannot be viewed on the Administration Desktop.
User	To access the Cabinets, you should be a user of that cabinet.

-V-

Volume	Volume is a logical entity that includes several Volume blocks.
Volume Block	Volume Block corresponds to a data file and provides the actual physical storage for the documents.