Lab 1 Setting Up the Directory Server Using the Graphical User Interface (GUI)

The graphical user interface (GUI) install uses a Java-based graphical installer that enables you to set up the directory server, load it with data, and get it running in very little time.

The installer asks some basic questions about the server configuration and then gives you the choice of leaving your database empty, loading the server with data from your own LDIF or loading the server with automatically generated sample data. The installer also enables you to configure security and replication, and, optionally, to start the server when the configuration is complete.

To setup a directory server instance using the `oud-setup` graphical user interface (GUI):

When you have installed the software, change to the `ORACLE_HOME` subdirectory.
On UNIX and Linux systems:
`$ cd OUD-base-location/ORACLE_HOME`

On Windows systems:
`C:\> cd OUD-base-location\ORACLE_HOME`

1. Ensure that your `JAVA_HOME` environment variable is set to a supported JVM installation (JRE 8 or JDK 8).

Run the `oud-setup` command to configure the directory server installation.
On UNIX and Linux systems:
`$ oud-setup`

On Windows systems:
`C:\`*`OUD-base-location`*`\`*`ORACLE_HOME`*`> oud-setup.bat`

The utility launches the graphical installer and creates the Oracle Unified Directory instance in `OUD-base-location/instance-dir`.
The default instance directory name is `asinst_1`, with subsequent instances on the same server named `asinst_2`, `asinst_3`, and so on.

On the Welcome screen, click **Next**.
The **Server Settings** screen is displayed.

2. Enter the following information:
    - **Host Name**: Enter the directory server's host name or IP address.

      The default is the local host name.
    - **LDAP Listener Port**: Enter the LDAP port for the directory server.

      The default port that is proposed is the first available port that ends with `389`. On UNIX and Linux systems,

if you run the installer as a non-root user, the default is `1389`, if available.

- **Administration Connector Port**: Enter the port that will be used for administration traffic.

  The default administration port is `4444`.

- **LDAP Secure Access**: To configure SSL, StartTLS, or both, then click **Configure**.

  Complete the following information:

  SSL Access: Select Enable SSL to indicate that the LDAPS (that is, LDAP over SSL) listener should be enabled. Enter the port number on which the directory server listens for connections.

  The default secure port that is proposed is the first available port that ends with `636`. On UNIX and Linux systems, if you run the installer as a non-root user, the default secure port is `1636`, if available.

  StartTLS Access: Select **Enable StartTLS for LDAP** to specify that the LDAP connection handler should allow clients to use the StartTLS extended operation to initiate secure communication over an otherwise insecure connection.

  Certificate: Select one of the following radio buttons to obtain the certificate that the server should use for

SSL, StartTLS, or both:

Generate Self-Signed Certificate generates a self-signed certificate that you can use to secure the communication. While this option is convenient for testing purposes, many clients will not trust the certificate by default, and you might need to configure it manually.

Use an Existing Certificate uses a certificate in an existing JKS keystore, a PKCS #12 file, or a PKCS #11 token.

- For production servers, select **Use an Existing Certificate**, and then select the Keystore Type. Enter the Keystore Path, and Keystore PIN if necessary.
  If more than one certificate is defined in the specified key store, you are asked to select one of the certificates from a drop down menu.
  Click **OK**.
- **Root User DN**: Enter the Root User DN, or keep the default, `cn=Directory Manager`.
- **Password**: Enter the root user bind password.
- **Password (confirm)**: Retype the root user bind password.

3. Click **Next**.

   The **Topology Options** screen is displayed.

4. Select one of the following:

   - **This will be a stand-alone server**.
   - **This server will be part of a replication topology**.

5. Click **Next**.

   The **Directory Data** screen is displayed.

6. Specify how to load data into your directory:

   - **Directory Base DN**: Enter the base DN for your directory.

     The default Base DN is `dc=example,dc=com`.

   - **Directory Data**: Select one of the following data options:

     Only Create Base Entry: Creates an entry with the base DN specified previously.

     Leave Database Empty: Sets up a database but does not populate any entries.

     Import Data from LDIF File: Imports LDIF data from the file specified in the Path field.

     Import Automatically-Generated Sample Data: Generates the number of sample entries specified in the Number of User Entries field.

7. Click **Next**.

   The **Oracle Components Integration** screen is displayed.

8. Select one of the following options. Some components appear in multiple options, with consecutive options adding additional components to the selection. The options are:

   - **No specific integration**: Select this option if you want a standard installation. This is the default option.
   - **Enable for DIP**: Select this option if you want this server instance to be enabled as a datastore for Oracle Directory Integration Platform (DIP) only.
   - **Enable for EBS (E-Business Suite), Database Net Services and DIP**: Select this option if you want this server instance to be enabled as a datastore for Oracle E-Business Suite (EBS), Oracle Database Net Services, and Oracle Directory Integration Platform (DIP).
   - **Enable for EUS (Enterprise User Security), EBS, Database Net Services and DIP**: Select this option if you want this server instance to be enabled as a datastore for Oracle Enterprise User Security (EUS), Oracle E-Business Suite (EBS), Oracle Database Net Services, and Oracle Directory Integration Platform (DIP).

     To enable a server instance for EUS, you must also

have enabled SSL access, as described in the Server Settings screen in Step 5 of this procedure.

The **Enable for Oracle Database Net Services** option causes this server to store the database connect identifiers.

- These naming contexts are not created if you select DIP.

  Click **Next**.

  The **Server Tuning** screen is displayed.

9. The **Server Tuning** screen enables you to tune Oracle Unified Directory server by selecting one of these options:
   - Providing the specific memory to be dedicated to the server.
   - Explicitly providing the run-time settings (JVM arguments) to be used by the server and the off-line tools (`import-ldif`, `export-ldif`, `verify-index`, and `rebuild-index`).
10. Click **Next**.

    The **Review** screen is displayed.
11. Review your configuration.

    Select **Start Server when Configuration has Completed** to start the server after the directory server has been configured.

On Windows systems, select **Start Server as a Windows service**, if desired.

To display the equivalent command-line installation, select **Show Equivalent Command-Line** from the drop down menu at the top of the panel. This option displays the non-interactive commands that are run to set up the server with the specified configuration, and can be useful for scripting purposes.

12. Click **Finish**.
13. Click **Close**.

Test whether the directory server has been set up and started successfully by searching an entry in the directory. For example:
On UNIX and Linux systems:

```
instance-dir/OUD/bin/ldapsearch -h localhost -p 1389 \
  -D "cn=directory manager" -w my-password -b
"dc=example,dc=com" \
  "(objectclass=*)"
```

On Windows systems:

```
instance-dir\OUD\bat\ldapsearch.bat -h localhost -p
1389 \
  -D "cn=directory manager" -w my-password -b
"dc=example,dc=com" \
  "(objectclass=*)"
```