# OpenDJ Installation Guide

Version 4.8.1-SNAPSHOT

Mark Craig

ForgeRock AS
201 Mission St., Suite 2900
San Francisco, CA 94105, USA
+1 415-599-1100 (US)
www.forgerock.com

## Abstract

This guide shows you how to install OpenDJ directory services. The OpenDJ project offers open source LDAP directory services in Java.

# Table of Contents

# Preface

This guide shows you how to install, upgrade, and remove OpenDJ software. Unless you are planning a throwaway evaluation or test installation, read the *Release Notes* before you get started.

If you want only to try OpenDJ server software, and you do not plan to store any real or important data that you want to keep, then you need not read this entire guide. Instead, try *Installing OpenDJ With the QuickSetup Wizard*.

## 1 Who Should Read this Guide

This guide is written for anyone installing OpenDJ who plans to maintain directory services for client applications. Basic OpenDJ installation, especially using Java WebStart, can be simple and straightforward, particularly if you are already acquainted with directory services. Upgrading a running directory service without a single point of failure that can cause downtime requires at least a little thought and planning. Also, even in the case of basic installation, you may find yourself wanting more background about what you are doing.

This guide covers the install, upgrade, and removal (a.k.a. uninstall) procedures that you theoretically perform only once per version. This guide aims to provide you with at least some idea of what happens behind the scenes when you perform the steps.

You do not need to be an LDAP wizard to learn something from this guide, though a background in directory services and maintaining server software can help. You do need some background in managing servers and services on your operating

system of choice. You can nevertheless get started with this guide, and then learn more as you go along.

# 2 Formatting Conventions

Most examples in the documentation are created in GNU/Linux or Mac OS X operating environments. If distinctions are necessary between operating environments, examples are labeled with the operating environment name in parentheses. To avoid repetition file system directory names are often given only in UNIX format as in `/path/to/server`, even if the text applies to `C:\path\to\server` as well.

Absolute path names usually begin with the placeholder `/path/to/`. This path might translate to `/opt/`, `C:\Program Files\`, or somewhere else on your system.

Command line, terminal sessions are formatted as follows:

```
$ echo $JAVA_HOME
/path/to/jdk
```

Command output is sometimes formatted for narrower, more readable output even though formatting parameters are not shown in the command. In the following example, the query string parameter `_prettyPrint=true` is omitted and some of the output is replaced with an ellipsis (`...`):

```
$ curl https://bjensen:hifalutin@opendj.example.com:8443/users/newuser
{
  "_rev" : "000000005b337348",
  "_id" : "newuser",
  ...
}
```

Program listings are formatted as follows:

```
class Test {
    public static void main(String [] args)  {
        System.out.println("This is a program listing.");
    }
}
```

# 3 Accessing Documentation Online

Open Identity Platform core documentation, such as this document, aims to be technically accurate and complete with respect to the software documented.

Core documentation therefore follows a three-phase review process designed to eliminate errors:

- Product managers and software architects review project documentation design with respect to the readers' software lifecycle needs.
- Subject matter experts review proposed documentation changes for technical accuracy and completeness with respect to the corresponding software.
- Quality experts validate implemented documentation changes for technical accuracy, completeness in scope, and usability for the readership.

The review process helps to ensure that documentation published for a Open Identity Platform release is technically accurate and complete.

Fully reviewed, published core documentation is available at https://doc.openidentityplatform.org/. Use this documentation when working with a Open Identity Platform release.

You can find pre-release draft documentation at the online community resource center. Use this documentation when trying a nightly build.

# 4 Joining the Open Identity Platform Community

Visit the community resource center where you can find information about each project, download nightly builds, browse the resource catalog, ask and answer questions on the forums, find community events near you, and of course get the source code as well.

Chapter 1

# Installing OpenDJ With the QuickSetup Wizard

If you want only to try OpenDJ server software, and you do not plan to store any real or important data that you want to keep, then read only this chapter, or just try out installation without reading any further.

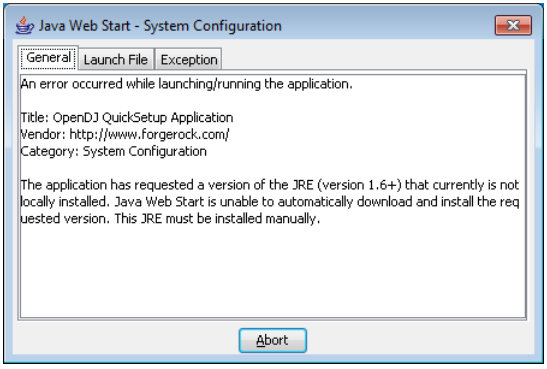
Download OpenDJ software from one of the following locations.

- The ForgeRock Enterprise Downloads page has the latest stable, supported release of OpenDJ and the other products in the ForgeRock identity stack.
- The Nightly Builds page posts links to the latest nightly builds of OpenDJ software. Note that these builds are the working version from the trunk and are not for use in a production environment.
- The Community Archives page includes stable community builds for previous releases of OpenDJ software.

QuickSetup uses Java WebStart to let you perform an installation of OpenDJ directory server starting with a click in your web browser, which can be a great way to try OpenDJ directory server for the first time, or to do a quick test installation.

## Note

OpenDJ directory server relies on Java 6 or later, so if your browser picks up an old installation of Java 5 for example, installation can fail. You might see an application error message such as this:

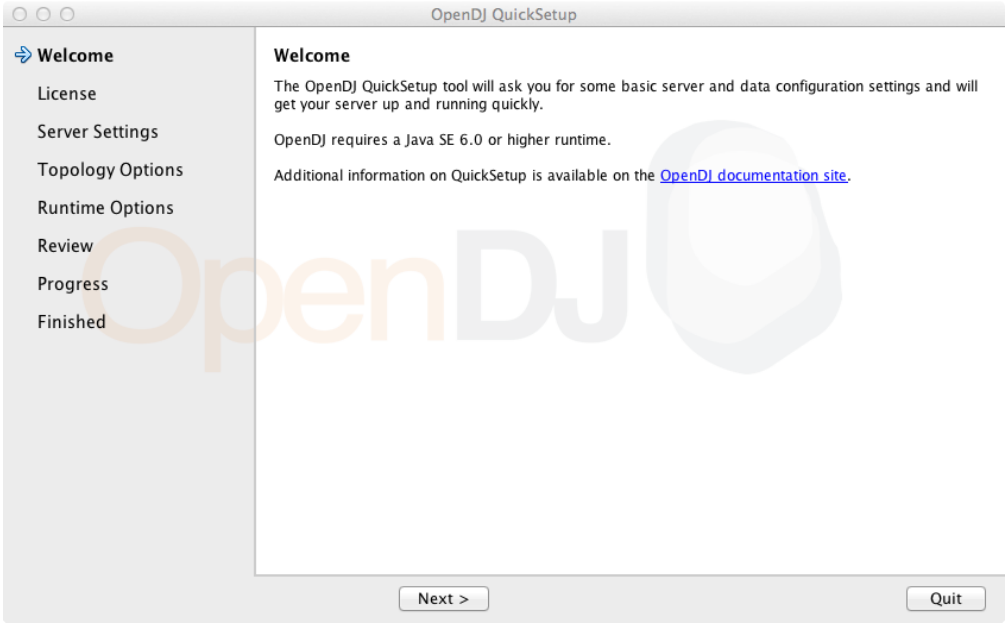


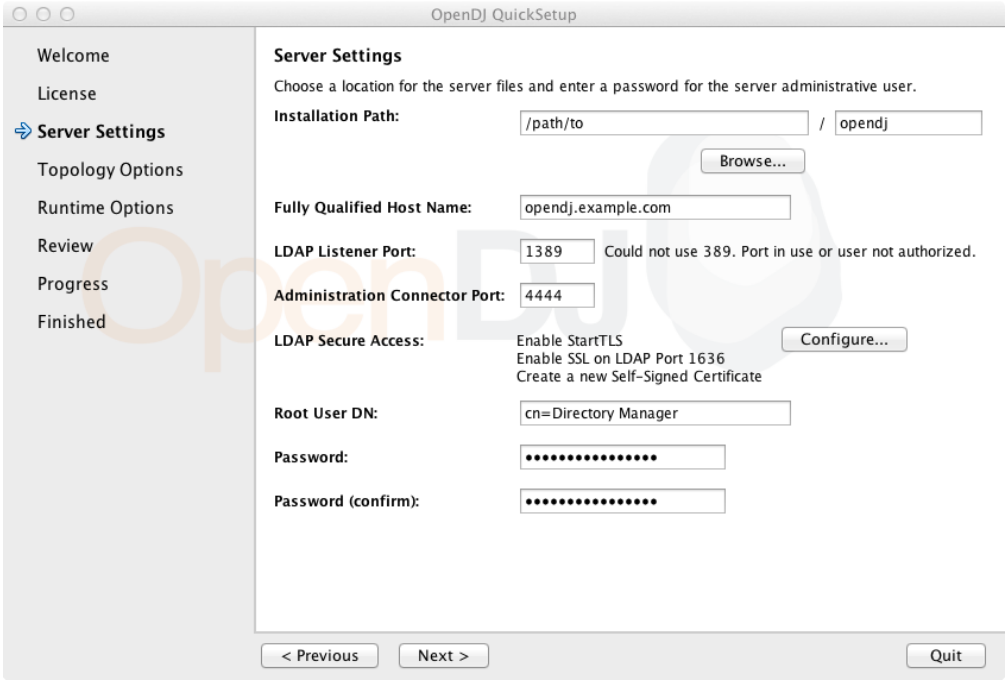

If the WebStart installation does not work in your browser, copy the WebStart URL, ending in `QuickSetup.jnlp`, from the OpenDJ download page. Next, pass the link as an argument to the **javaws** command in a terminal window to start the installer.

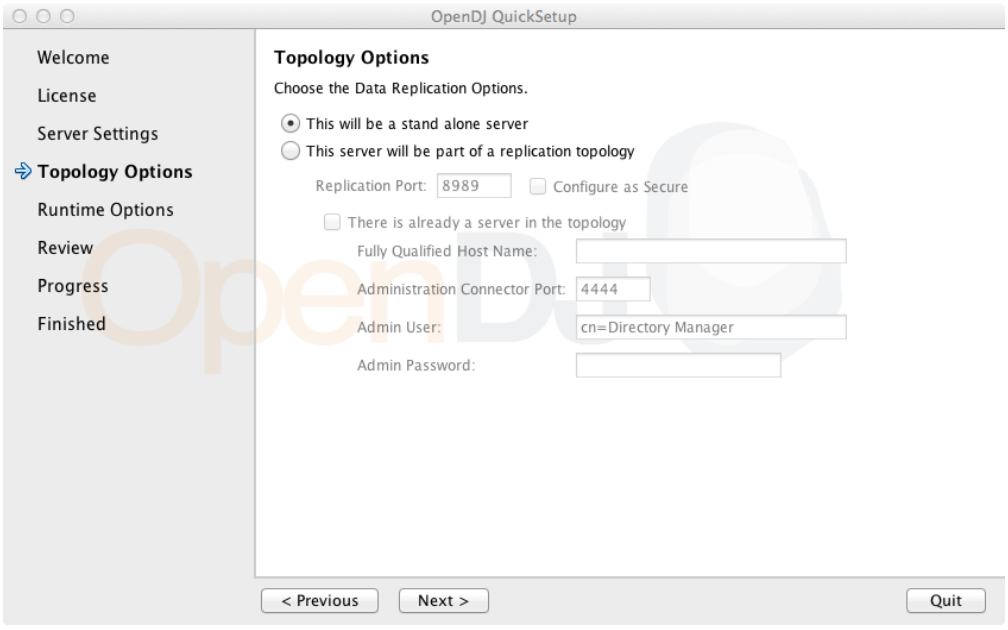
```
$ export PATH=/path/to/java/bin:$PATH
$ javaws URL-to-QuickSetup-Installer
```

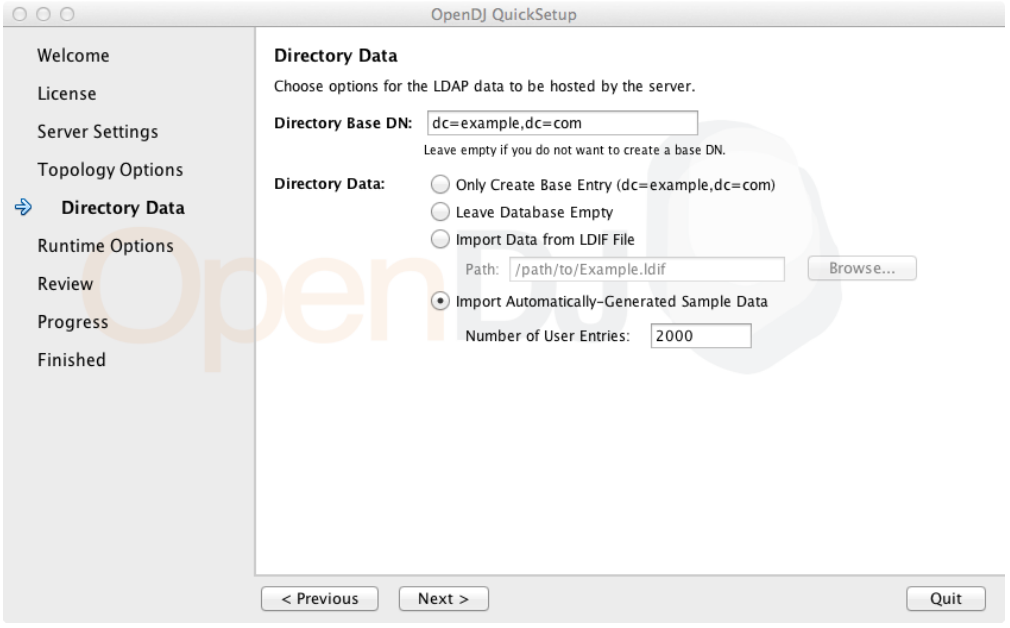
The WebStart installer corresponds to what you start if you download OpenDJ-4.8.1-SNAPSHOT.zip, unzip the file, and then run **opendj/setup** (UNIX), **opendj\setup.bat** (Windows), or **opendj/QuickSetup.app** (Mac OS X).

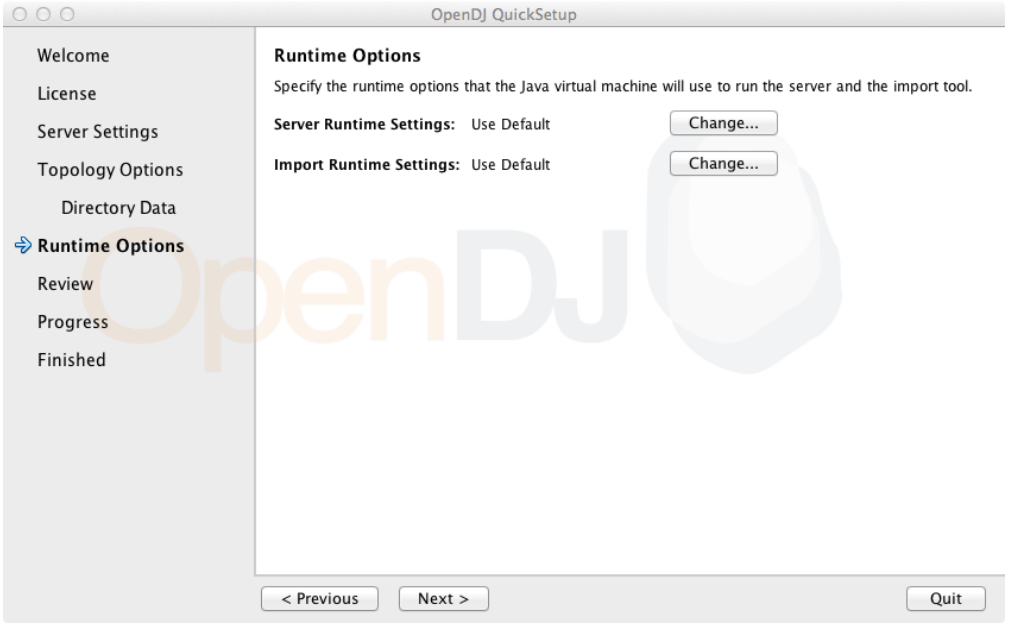
Java WebStart launches the the QuickSetup wizard, and soon the Welcome screen appears.

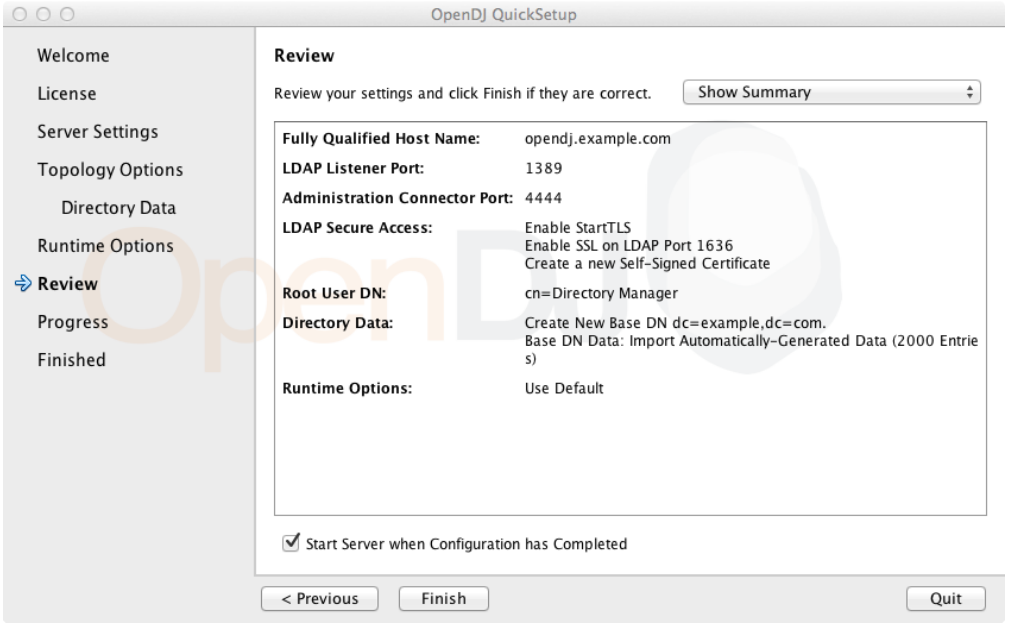

OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Runtime Options
Review
Progress
Finished
Welcome
The OpenDJ QuickSetup tool will ask you for some basic server and data configuration settings and will get your server up and running quickly.
OpenDJ requires a Java SE 6.0 or higher runtime.
Additional information on QuickSetup is available on the OpenDJ documentation site.
Next >
Quit
OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Runtime Options
Review
Progress
Finished
License
Please read the following License Agreement.
You must accept the terms of the agreement before continuing with the installation.
READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING THE FORGEROCK SOFTWARE, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT DOWNLOAD OR INSTALL THE FORGEROCK SOFTWARE.
1. Software License.
1.1. Development Right to Use. If Company intends to or does use the ForgeRock Software only for the purpose(s) of developing, testing, prototyping and demonstrating its application software, then ForgeRock hereby grants Company a nonexclusive, nontransferable, limited license to use the ForgeRock Software only for those purposes, solely at Company's facilities and only in a non-production environment. ForgeRock may audit Company's use of the ForgeRock Software to confirm that a production license is not required upon reasonable written notice to Company. If Company intends to use the ForgeRock Software in a live environment, Company must purchase a production license and may only use the ForgeRock Software licensed thereunder in accordance with the terms and conditions of that subscription agreement.
1.2. Restrictions. Except as expressly set forth in this ForgeRock Software License Agreement (the "Agreement"), Company shall not, directly or indirectly: (a) sublicense, resell, rent, lease, distribute or otherwise transfer rights or usage in the ForgeRock Software, including without limitation to Company
Click to accept
< Previous
Next >
Quit

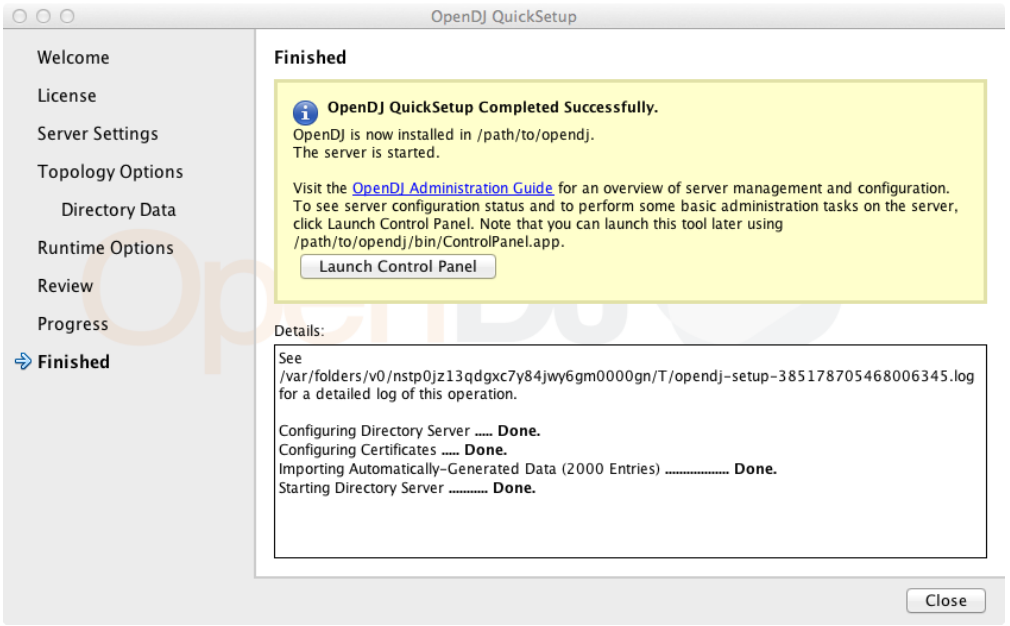

OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Runtime Options
Review
Progress
Finished
Server Settings
Choose a location for the server files and enter a password for the server administrative user.
Installation Path:
/path/to
/
opendj
Browse...
Fully Qualified Host Name:
opendj.example.com
LDAP Listener Port:
1389
Could not use 389. Port in use or user not authorized.
Administration Connector Port:
4444
LDAP Secure Access:
Enable StartTLS
Enable SSL on LDAP Port 1636
Create a new Self-Signed Certificate
Configure...
Root User DN:
cn=Directory Manager
Password:
Password (confirm):
< Previous
Next >
Quit

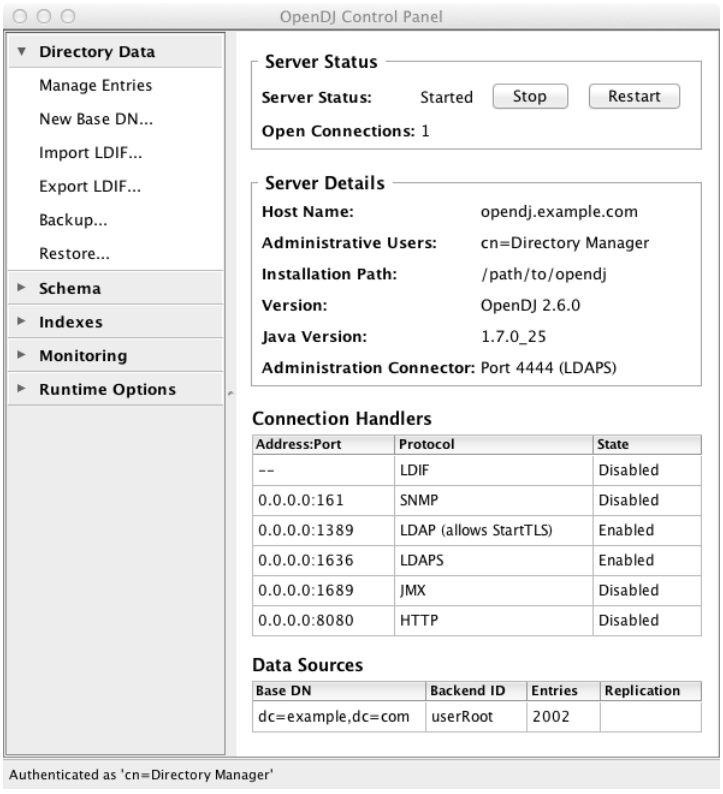

OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Runtime Options
Review
Progress
Finished
Topology Options
Choose the Data Replication Options.
This will be a stand alone server
This server will be part of a replication topology
Replication Port:
8989
Configure as Secure
There is already a server in the topology
Fully Qualified Host Name:
Administration Connector Port:
4444
Admin User:
cn=Directory Manager
Admin Password:
< Previous
Next >
Quit


OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Directory Data
Runtime Options
Review
Progress
Finished
Directory Data
Choose options for the LDAP data to be hosted by the server.
Directory Base DN:
dc=example,dc=com
Leave empty if you do not want to create a base DN.
Directory Data:
Only Create Base Entry (dc=example,dc=com)
Leave Database Empty
Import Data from LDIF File
Path:
/path/to/Example.ldif
Browse...
Import Automatically-Generated Sample Data
Number of User Entries:
2000
< Previous
Next >
Quit


OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Directory Data
Runtime Options
Review
Progress
Finished
Runtime Options
Specify the runtime options that the Java virtual machine will use to run the server and the import tool.
Server Runtime Settings:
Use Default
Change...
Import Runtime Settings:
Use Default
Change...
< Previous
Next >
Quit


OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Directory Data
Runtime Options
Review
Progress
Finished
Review
Review your settings and click Finish if they are correct.
Show Summary
Fully Qualified Host Name: opendj.example.com
LDAP Listener Port: 1389
Administration Connector Port: 4444
LDAP Secure Access: Enable StartTLS
Enable SSL on LDAP Port 1636
Create a new Self-Signed Certificate
Root User DN: cn=Directory Manager
Directory Data: Create New Base DN dc=example,dc=com.
Base DN Data: Import Automatically-Generated Data (2000 Entries)
Runtime Options: Use Default
Start Server when Configuration has Completed
< Previous
Finish
Quit


OpenDJ QuickSetup
Welcome
License
Server Settings
Topology Options
Directory Data
Runtime Options
Review
Progress
Finished
Finished
OpenDJ QuickSetup Completed Successfully.
OpenDJ is now installed in /path/to/opendj.
The server is started.
Visit the OpenDJ Administration Guide for an overview of server management and configuration.
To see server configuration status and to perform some basic administration tasks on the server, click Launch Control Panel. Note that you can launch this tool later using /path/to/opendj/bin/ControlPanel.app.
Launch Control Panel
Details:
See /var/folders/v0/nstp0jz13qdgxc7y84jwy6gm0000gn/T/opendj-setup-385178705468006345.log for a detailed log of this operation.
Configuring Directory Server ..... Done.
Configuring Certificates ..... Done.
Importing Automatically-Generated Data (2000 Entries) ..... Done.
Starting Directory Server ..... Done.
Close




To launch OpenDJ Control Panel again later, you can run one of the following, depending on your host system.

- (Mac OS X) **opendj/bin/ControlPanel.app**
- (UNIX) **opendj/bin/control-panel**
- (Windows) **opendj\bat\control-panel.bat**

Chapter 2

# Installing OpenDJ From the Command Line

This chapter covers command-line installation with additional information on setup options.



**Procedure 2.1. To Prepare For Installation**

1. Make sure you have the correct Java environment installed, as described in the *Release Notes* section on *Java Environment* requirements.

   If your default Java environment is not appropriate, set `OPENDJ_JAVA_HOME` to the path to the correct Java environment, or set `OPENDJ_JAVA_BIN` to the absolute path of the **java** command. The latter environment variable is

useful for example if you have both 32-bit and 64-bit versions of the Java environment installed, and want to make sure you use the 64-bit version.

2. Download OpenDJ software from one of the following locations.

   - The ForgeRock Enterprise Downloads page has the latest stable, supported release of OpenDJ and the other products in the ForgeRock identity stack.
   - The Nightly Builds page posts links to the latest nightly builds of OpenDJ software. Note that these builds are the working version from the trunk and are not for use in a production environment.
   - The Community Archives page includes stable community builds for previous releases of OpenDJ software.

   The following server software is available.

   OpenDJ-4.8.1-SNAPSHOT.zip

   Cross-platform OpenDJ directory server installation files

   opendj_4.8.1-SNAPSHOT-1_all.deb

   OpenDJ directory server native package for Debian and related Linux distributions.

   opendj-4.8.1-SNAPSHOT-1.noarch.rpm

   OpenDJ directory server native package for Red Hat and related Linux distributions.

   OpenDJ-4.8.1-SNAPSHOT-DSML.war

   Cross-platform OpenDJ DSML gateway web archive

   opendj-rest2ldap-servlet-4.8.1-SNAPSHOT-servlet.war

   Cross-platform OpenDJ REST LDAP gateway web archive

3. If you plan to install OpenDJ DSML gateway or OpenDJ REST LDAP gateway, make sure you have an appropriate application server installed.

4. If you plan to configure SSL or TLS to secure network communications between the server and client applications, get a properly signed digital certificate that your client applications recognize, such as one that fits with your organization's PKI or one provided by a recognized certificate authority.

To use the certificate during installation, the certificate must be located in a key store provided with Java (JKS, JCEKS, PKCS#12), or on a PKCS#11 token. To import a signed certificate into a key store, you can use the Java **keytool** command.

See *Preparing For Secure Communications* in the *Administration Guide* for examples.

#### Procedure 2.2. To Install OpenDJ Directory Server

1. Unzip `OpenDJ-4.8.1-SNAPSHOT.zip` in the file system directory where you want to install the server.

   Unlike the web-based Quick Setup install, the **setup** command uses the directory where you unzipped the files as the installation directory, and does not ask you where to install OpenDJ. Therefore, if you want to install elsewhere on the file system, unzip the files in that location.

2. Run the **setup --cli** command found in the `opendj` directory.

   This command starts the setup program in interactive mode on the command line, prompting you for each option. Alternatively, use additional **setup** options to specify values for the options you choose during interactive mode, thus scripting the installation process. See **setup --help** and the notes below.

   To perform a non-interactive, silent installation, provide all the options to configure OpenDJ, and then also use the `-n` or `--no-prompt` option.

   The **setup** command without the `--cli` option runs the Quick Start GUI installer with your local version of software, as does Java WebStart with a remote version of the software.

```
$ /path/to/opendj/setup --cli
READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING
THE FORGEROCK SOFTWARE, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO
BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE
TERMS, DO NOT DOWNLOAD OR INSTALL THE FORGEROCK SOFTWARE.

...

Please read the License Agreement above.
You must accept the terms of the agreement before continuing with the
installation.
Accept the license (Yes/No) [No]:Yes

What would you like to use as the initial root user DN for the Directory
Server? [cn=Directory Manager]:
Please provide the password to use for the initial root user:
Please re-enter the password for confirmation:

Provide the fully-qualified directory server host name that will be used when
```

```
generating self-signed certificates for LDAP SSL/StartTLS, the administration
connector, and replication [opendj.example.com]:

On which port would you like the Directory Server to accept connections from
LDAP clients? [1389]:

On which port would you like the Administration Connector to accept
connections? [4444]:

Do you want to create base DNs in the server? (yes / no) [yes]:

Provide the base DN for the directory data: dc=example,dc=com
Options for populating the database:

    1)  Only create the base entry
    2)  Leave the database empty
    3)  Import data from an LDIF file
    4)  Load automatically-generated sample data

Enter choice [1]: 3

Please specify the path to the LDIF file containing the data to import: \
/path/to/Example.ldif

Do you want to enable SSL? (yes / no) [no]:

Do you want to enable Start TLS? (yes / no) [no]:

Do you want to start the server when the configuration is completed? (yes /
no) [yes]:


Setup Summary
=============
LDAP Listener Port:            1389
Administration Connector Port: 4444
LDAP Secure Access:            disabled
Root User DN:                  cn=Directory Manager
Directory Data:                Create New Base DN dc=example,dc=com.
Base DN Data: Import Data from LDIF File (/path/to/Example.ldif)

Start Server when the configuration is completed


What would you like to do?

    1)  Set up the server with the parameters above
    2)  Provide the setup parameters again
    3)  Print equivalent non-interactive command-line
    4)  Cancel and exit

Enter choice [1]:

See /var/.../opendj-setup...log for a detailed log of this operation.

Configuring Directory Server ..... Done.
Importing LDIF file /path/to/Example.ldif ........... Done.
Starting Directory Server ........... Done.

To see basic server configuration status and configuration you can launch \
/path/to/opendj/bin/status
```

Some notes on the options follow.

Initial root user DN

The root user Distinguished Name identifies a user who can perform all administrative and other operations allowed for the server, called root user due to the similarity to the UNIX root. The default, `cn=Directory Manager`, is a well-known name. If you have reason to be paranoid, you might opt for a different name.

Initial root user password

The root user will use simple, password-based authentication. Later you can limit clear text access to avoid snooping, but for now use a strong password here unless this is a throwaway server.

Fully-qualified directory server host name

OpenDJ uses fully-qualified host name in self-signed certificates and for identification when you use replication. If you are installing a single server temporarily for evaluation, and are not concerned about replication and whether self-signed certificates can be trusted, then you can use an FQDN such as `localhost.localdomain`. Otherwise, use an FQDN that other hosts can resolve to reach your server.

LDAP port

The default for LDAP is 389. If you are working as a user who cannot open port 389, setup suggests 1389 by default.

Administration port

This is the service entrance used to configure the server, run tasks, and so forth. The default is 4444.

Create base DNs

You need a base Distinguished Name, such as `dc=example,dc=com`, to add directory data. If you already have LDIF, the base DN you want is the distinguished name suffix common to all entries in your LDIF. You can provide more than one base DN if your data belongs in more than one suffix.

Import LDIF

LDAP data interchange format is the standard text format for expressing LDAP data. If you have LDIF already, one reason you might not want to import the data at the same time you install is because your data uses

attributes not defined in the default schema, and so you will wait to add schema definitions before you import.

If you have a huge data set to import, you no doubt should also increase the import cache size, which you can do by passing a Java properties file. You might also prefer to perform data import offline.

Enable SSL and TLS

Enabling Secure Sockets Layer or Transport Layer Security lets you protect the network traffic between directory clients and your server.

SSL

SSL requires its own, separate port for LDAPS traffic. The default port for LDAPS is 636. If you are working as a user who cannot open port 636, setup suggests 1636 by default.

TLS

TLS lets you use StartTLS to negotiate a secure connection between a client and server, starting from the same server port you configured for LDAP.

X.509 certificates

The digital certificate you need for SSL and TLS can be self-signed and created on the fly. Trouble is, client applications view self-signed certificates like fake IDs, and so do not trust them. Self-signed certificates facilitate testing, but are not intended for production use.

Start the server

If you do not start the server during installation, you can use the **/path/to/opendj/bin/start-ds** command later.

3. Run the **status** command to make sure your OpenDJ server is working as expected.

```
$ /path/to/opendj/bin/status

>>>> Specify OpenDJ LDAP connection parameters

Administrator user bind DN [cn=Directory Manager]:

Password for user 'cn=Directory Manager':

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                opendj.example.com
Administrative Users:     cn=Directory Manager
Installation Path:        /path/to/opendj
Version:                  OpenDJ 4.8.1-SNAPSHOT
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol : State
-------------:----------:---------
--           : LDIF     : Disabled
0.0.0.0:161  : SNMP     : Disabled
0.0.0.0:636  : LDAPS    : Disabled
0.0.0.0:1389 : LDAP     : Enabled
0.0.0.0:1689 : JMX      : Disabled

          --- Data Sources ---
Base DN:     dc=example,dc=com
Backend ID:  userRoot
Entries:     160
Replication: Disabled
```

### Note

You can install OpenDJ in unattended and silent fashion, too. See the procedure, Procedure 2.5, “To Install OpenDJ Directory Server With a Properties File”.

#### Procedure 2.3. To Install From the Debian Package

On Debian and related Linux distributions such as Ubuntu, you can install OpenDJ directory server from the Debian package.

1. (Optional) Before you install OpenDJ, install a Java runtime environment if none is installed yet.

```
$ sudo apt-get install default-jre
```

2. Install the OpenDJ directory server package.

```
$ sudo dpkg -i opendj_4.8.1-SNAPSHOT-1_all.deb
Selecting previously unselected package opendj.
(Reading database ... 185569 files and directories currently installed.)
Unpacking opendj (from opendj_4.8.1-SNAPSHOT-1_all.deb) ...

Setting up opendj (4.8.1-SNAPSHOT) ...
$
```

   The .deb installs OpenDJ directory server in the directory `/opt/opendj`.

   The files are owned by root by default, making it easier to have OpenDJ listen on ports 389 and 636.

3. Configure OpenDJ directory server by using the command **sudo /opt/opendj/setup**.

```
$ sudo /opt/opendj/setup --cli
...
To see basic server configuration status and configuration you can launch
 /opt/opendj/bin/status
```

4. (Optional) Check OpenDJ directory server status.

```
$ sudo /opt/opendj/bin/status


>>>> Specify OpenDJ LDAP connection parameters

Administrator user bind DN [cn=Directory Manager]:

Password for user 'cn=Directory Manager':

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                ubuntu.example.com
Administrative Users:     cn=Directory Manager
Installation Path:        /opt/opendj
Version:                  OpenDJ 4.8.1-SNAPSHOT
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol               : State
-------------:-----------------------:---------
--           : LDIF                   : Disabled
0.0.0.0:161  : SNMP                   : Disabled
0.0.0.0:389  : LDAP (allows StartTLS) : Enabled
0.0.0.0:636  : LDAPS                  : Enabled
0.0.0.0:1689 : JMX                    : Disabled
0.0.0.0:8080 : HTTP                   : Disabled

          --- Data Sources ---
Base DN:     dc=example,dc=com
Backend ID:  userRoot
Entries:     2002
Replication:
```

5. (Optional) If you want to run OpenDJ when the system starts, see create-rc-script.

#### Procedure 2.4. To Install From the RPM Package

On Red Hat and related Linux distributions such as Fedora and CentOS, you can install OpenDJ directory server from the RPM package.

1. Log in as superuser to install the software.

```
$ su
Password:
#
```

2. (Optional) Before you install OpenDJ, install a Java runtime environment if none is installed yet.

You might need to download an .rpm to install the Java runtime environment, and then install it using the **rpm** command.

```
# rpm -ivh jre-*.rpm
```

3. Install the OpenDJ directory server package.

```
# rpm -i opendj-4.8.1-SNAPSHOT-1.noarch.rpm
Pre Install - initial install
Post Install - initial install

#
```

The .rpm installs OpenDJ directory server in the directory `/opt/opendj`.

The files are owned by root by default, making it easier to have OpenDJ listen on ports 389 and 636.

4. Configure OpenDJ directory server by using the command **/opt/opendj/setup**.

```
# /opt/opendj/setup --cli
...
To see basic server configuration status and configuration you can launch
 /opt/opendj/bin/status
```

5. (Optional) Check OpenDJ directory server status.

```
# /opt/opendj/bin/status


>>>> Specify OpenDJ LDAP connection parameters

Administrator user bind DN [cn=Directory Manager]:

Password for user 'cn=Directory Manager':

          --- Server Status ---
Server Run Status:        Started
Open Connections:         1

          --- Server Details ---
Host Name:                fedora.example.com
Administrative Users:     cn=Directory Manager
Installation Path:        /opt/opendj
Version:                  OpenDJ 4.8.1-SNAPSHOT
Java Version:             version
Administration Connector: Port 4444 (LDAPS)

          --- Connection Handlers ---
Address:Port : Protocol               : State
-------------:-----------------------:---------
--           : LDIF                   : Disabled
0.0.0.0:161  : SNMP                   : Disabled
0.0.0.0:389  : LDAP (allows StartTLS) : Enabled
0.0.0.0:636  : LDAPS                  : Enabled
0.0.0.0:1689 : JMX                    : Disabled
0.0.0.0:8080 : HTTP                   : Disabled

          --- Data Sources ---
Base DN:     dc=example,dc=com
Backend ID:  userRoot
Entries:     2002
Replication:
```

6. (Optional) If you want to run OpenDJ when the system starts, see create-rc-script.

#### Procedure 2.5. To Install OpenDJ Directory Server With a Properties File

You can install OpenDJ directory server by using the **setup** command with a properties file.

Property names correspond to the option names, but without leading dashes. Options that take no arguments become boolean properties as in the following example.

```
enableStartTLS=true
```

If you use a properties file with multiple tools, prefix the property name with the tool name followed by a dot (.), as in the following example.

```
setup.rootUserPasswordFile=/tmp/pwd.txt
```

The following steps demonstrate use of a properties file as part of a scripted installation process.

1. Prepare your properties file.

   This procedure uses the following example properties file.

```
#
# Sample properties file to set up OpenDJ directory server
#
hostname                        =opendj.example.com
ldapPort                        =1389
generateSelfSignedCertificate   =true
enableStartTLS                  =true
ldapsPort                       =1636
jmxPort                         =1689
adminConnectorPort              =4444
rootUserDN                      =cn=Directory Manager
rootUserPassword                =password
baseDN                          =dc=example,dc=com
ldifFile                        =/net/install/dj/Example.ldif
#sampleData                     =2000
```

   If you have multiple servers to install, consider scripting creation of the properties files.

2. Prepare an installation script.

```
$ cat /net/install/dj/1/setup.sh
#!/bin/sh

unzip -d /path/to /net/install/dj/OpenDJ-4.8.1-SNAPSHOT.zip && cd /path/to/opendj
./setup --cli --propertiesFilePath /net/install/dj/1/setup.props \
  --acceptLicense --no-prompt
```

3. Run your installation script.

```
$ /net/install/dj/1/setup.sh
Archive:  /net/install/dj/OpenDJ-4.8.1-SNAPSHOT.zip
   creating: /path/to/opendj
...
  inflating: /path/to/opendj/setup
  inflating: /path/to/opendj/uninstall
  inflating: /path/to/opendj/upgrade

READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING
THE FORGEROCK SOFTWARE, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO
BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE
TERMS, DO NOT DOWNLOAD OR INSTALL THE FORGEROCK SOFTWARE.

...

Do you accept the License Agreement?yes
See /var/folders/.../opendj-setup-....log for a detailed log of this operation.

Configuring Directory Server ..... Done.
Configuring Certificates ..... Done.
Importing LDIF file /net/install/dj/Example.ldif ....... Done.
Starting Directory Server ....... Done.

To see basic server configuration status and configuration you can launch
 /path/to/opendj/bin/status
```

At this point you can use OpenDJ directory server, or you can perform additional configuration.

**Procedure 2.6. To Install OpenDJ REST LDAP Gateway**

The OpenDJ REST LDAP gateway functions as a web application in a web application container, running independently of OpenDJ. Alternatively, you can use the HTTP connection handler in OpenDJ directory server. See the procedure, *To Set Up REST Access to OpenDJ Directory Server*, for instructions.

You configure the gateway to access your directory service by editing `opendj-rest2ldap-servlet.json` where you deploy the gateway web application.

1. Deploy `opendj-rest2ldap-servlet-4.8.1-SNAPSHOT-servlet.war` according to the instructions for your application server.

2. Edit `opendj-rest2ldap-servlet.json` where you deployed the gateway web application.

   The default JSON resource for the configuration includes both connection and authentication information, and also `mappings`. The `mappings` describe how the gateway translates between JSON and LDAP representations of your data. The default `mappings` are built to work with generated example data and also the sample content in Example.ldif.

At minimum, make sure that the host name and port numbers for `primaryLDAPServers` are properly configured, that `authentication` reflects the correct simple bind credentials, and that the `mappings` for the endpoints correctly match your directory data.

For details on the configuration, see *REST LDAP Configuration*.

When connecting to directory servers over LDAPS or LDAP and StartTLS, you can configure the trust manager to use a file-based trust store for server certificates that the gateway should trust. This allows the gateway to validate server certificates signed for example by a Certificate Authority not recognized by the Java environment when setting up LDAPS or StartTLS connections. See *Preparing For Secure Communications* for an example showing how to use the **keytool** command to support a server certificate into a trust store file.

3. Restart the REST LDAP gateway or the application server to make sure the changes are taken into account.

4. Make sure that your directory server is running, and then check that the gateway is connecting correctly.

   The following command reads Babs Jensen's entry through the gateway to the backend holding data from `Example.ldif`.

```
$ curl http://bjensen:hifalutin@opendj.example.com:8080/rest2ldap/users/bjensen
 ?_prettyPrint=true
{
  "_rev" : "000000002ee3b764",
  "schemas" : [ "urn:scim:schemas:core:1.0" ],
  "contactInformation" : {
    "telephoneNumber" : "+1 408 555 1862",
    "emailAddress" : "bjensen@example.com"
  },
  "_id" : "bjensen",
  "name" : {
    "familyName" : "Jensen",
    "givenName" : "Barbara"
  },
  "userName" : "bjensen@example.com",
  "displayName" : "Barbara Jensen",
  "manager" : [ {
    "_id" : "trigden",
    "displayName" : "Torrey Rigden"
  } ]
}
```

   If you generated example data, Babs Jensen's entry is not included. Try a URL such as `http://user.0:password@opendj.example.com:8080/rest2ldap/users/user.0` instead.

**Procedure 2.7. To Install OpenDJ DSML gateway**

The OpenDJ DSML gateway functions as a web application located in a web application container. The DSML gateway runs independently of OpenDJ directory server. You configure the gateway to access your directory service by editing the `ldap.host` and `ldap.port` parameters in the `WEB-INF/web.xml` configuration file.

1. Deploy `OpenDJ-4.8.1-SNAPSHOT-DSML.war` according to the instructions for your application server.
2. Edit `WEB-INF/web.xml` to ensure the values for `ldap.host` and `ldap.port` are correct.
3. Restart the web application container according to the instructions for your application server.

Chapter 3

# Tuning JVM Options

By default, OpenDJ installs with options appropriate for evaluation, not for production.

You can change JVM options for the server in the QuickStart installer, and alternatively using the Control Panel (Runtime Options > Java Settings), or with the **dsjavaproperties** command after editing the `config/java.properties` file.

Heap size

The JVM heap size by default is either 256 MB or 1 GB.

In production, use at least a 2 GB heap (-Xms2G -Xmx2G).

Server optimizations

Use -server to select the HotSpot Server VM.

32-bit vs. 64-bit

For heap sizes over 4 GB on 64-bit systems use -d64.

Garbage collection

Use -XX:+UseConcMarkSweepGC to select the CMS garbage collector for low GC pause times.

New generation size

If your directory handles high throughput, set the new generation size large enough for the JVM to avoid promoting short-lived objects into the old gen space (-XX:NewSize=512M).

Chapter 4

# Upgrading to OpenDJ 4.8.1-SNAPSHOT

This chapter covers upgrade from OpenDJ 2.4.5 and later versions.

For upgrades from earlier versions, upgrade first to at least OpenDJ 2.4.5, and then follow the procedures in this chapter. See Upgrading OpenDJ Directory Server in the OpenDJ Wiki for details on upgrading to OpenDJ 2.4.5 from earlier versions.

**Procedure 4.1. Before You Upgrade**

1. Prepare to perform the upgrade procedure as the user who owns the OpenDJ server files.

   Make sure you have the credentials to run commands as the user who owns the server.

2. Download OpenDJ software from one of the following locations.

   - The ForgeRock Enterprise Downloads page has the latest stable, supported release of OpenDJ and the other products in the ForgeRock identity stack.

   - The Nightly Builds page posts links to the latest nightly builds of OpenDJ software. Note that these builds are the working version from the trunk and are not for use in a production environment.

- The Community Archives page includes stable community builds for previous releases of OpenDJ software.

3. In order to revert if the upgrade fails, make sure you perform a full backup of your current OpenDJ installation.

   It might be most expedient to back up the file system directory where the current OpenDJ server is installed as part of the upgrade process.

   Alternatively, see *Backing Up & Restoring Data* for instructions.

#### Procedure 4.2. To Upgrade an OpenDJ Directory Server

To upgrade OpenDJ directory server installed from native packages (.deb, .rpm), use the command-line package management tools provided by the system.

The following steps describe how to upgrade OpenDJ directory server installed from the cross-platform (.zip) delivery.

1. Login as the user who owns the current OpenDJ server.

2. Stop the current OpenDJ server.

3. (Optional) If you have not already backed up the current OpenDJ server, make a back up copy of the directory where OpenDJ is installed.

4. (Optional) If OpenDJ is currently installed in a directory such as `OpenDJ-2.4.5`, you can change the directory name to `opendj` to make it easier to unpack subsequent .zip deliveries for future upgrades.

5. Unpack the new files from the .zip delivery over the current server files.

   If your directory is not named `opendj`, then you can first unpack the files, then copy everything in the `opendj` over the current server files.

6. Run the **upgrade** command to bring OpenDJ configuration and application data up to date with the new binary and script files that you copied over the current server files.

   By default, the **upgrade** command requests confirmation before making important configuration changes. You can use the `--no-prompt` option to run the command non-interactively, with the `--acceptLicense` option to accept the license terms non-interactively.

   When using the `--no-prompt` option, if the **upgrade** command cannot complete because it requires confirmation for a potentially very long or critical task, then it exits with an error and a message about how to finish making the

changes. You can add the `--force` option to force a non-interactive upgrade to continue in this case, also performing long running and critical tasks.

7. When you upgrade from OpenDJ 2.5.0-Xpress1, you must rebuild the `ds-sync-hist` ordering index before you restart the server, as indicated in the message from the upgrade tool.

```
  OpenDJ 2.5.0-Xpress1 introduced a regression in the ds-sync-hist ordering
  index. This index must be rebuilt after the upgrade has completed and before
  restarting OpenDJ. Do you wish to continue? (yes/no) [no]: yes
```

   To rebuild the index, use the **rebuild-index** command after upgrade but before starting the server as in the following example.

```
$ ./opendj/bin/rebuild-index --baseDN dc=example,dc=com --index ds-sync-hist
... msg=Rebuild of index(es) ds-sync-hist started ...
... msg=Rebuild complete. Processed XXX entries in YYY seconds...
```

8. Start the upgraded OpenDJ server.

   At this point the upgrade process is complete. See the resulting `upgrade.log` file for a full list of operations performed.

#### Example 4.1. Upgrading From OpenDJ 2.4.5

The following example upgrades an OpenDJ 2.4.5 directory server installed in `/path/to/OpenDJ-2.4.5`, backing up the current server directory in case the upgrade process fails, and changing the directory name to `/path/to/opendj` to simplify future upgrades.

```
$ cd /path/to
$ ls
OpenDJ-2.4.5
$ ./OpenDJ-2.4.5/bin/stop-ds --quiet
... msg=The backend userRoot is now taken offline
... msg=The Directory Server is now stopped
$ zip -rq OpenDJ-backup.zip OpenDJ-2.4.5
$ unzip -q ~/Downloads/OpenDJ-2.6.0.zip
$ cp -r opendj/* OpenDJ-2.4.5/
$ rm -rf opendj
$ mv OpenDJ-2.4.5 opendj
$ ./opendj/upgrade --no-prompt --acceptLicense

>>>> OpenDJ Upgrade Utility

 * OpenDJ will be upgraded from version 2.4.5.7743 to 2.6.0.9086
 * See '/path/to/opendj/upgrade.log' for a detailed log of this operation

READ THIS SOFTWARE LICENSE AGREEMENT CAREFULLY. BY DOWNLOADING OR INSTALLING
THE FORGEROCK SOFTWARE, YOU, ON BEHALF OF YOURSELF AND YOUR COMPANY, AGREE TO
BE BOUND BY THIS SOFTWARE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THESE
TERMS, DO NOT DOWNLOAD OR INSTALL THE FORGEROCK SOFTWARE.

 ...
```

```
Please read the License Agreement above.
You must accept the terms of the agreement before continuing with the
installation
Do you accept the License Agreement? yes

>>>> Preparing to upgrade

  OpenDJ 2.5.0 modified the default configuration of the 'isMemberOf' virtual
  attribute so that it is included with group entries. This was done in order
  to make it easier for users to determine which groups a 'nested' group
  belongs to.
  Do you want to make this configuration change? (yes/no) yes

  The upgrade is ready to proceed. Do you wish to continue? (yes/no) yes


>>>> Performing upgrade

  Fixing de-DE collation matching rule OID.........................   100%
  Updating password policy configurations..........................   100%
  Updating audit log publisher configuration.......................   100%
  Rename SNMP security config file.................................   100%
  Adding 'etag' virtual attribute schema...........................   100%
  Configuring 'etag' virtual attribute.............................   100%
  Configuring 'ds-pwp-password-expiration-time' virtual attribute.....   100%
  Updating certificate syntax configuration........................   100%
  Updating JPEG syntax configuration...............................   100%
  Updating country string syntax configuration.....................   100%
  Modifying filter in 'isMemberOf' virtual attribute configuration....   100%
  Updating dictionary password validator configuration.............   100%
  Updating attribute value password validator configuration..........   100%
  Adding PBKDF2 password storage scheme configuration..............   100%
  Adding 'http-config.json' configuration file.....................   100%
  Adding HTTP connection handler configuration.....................   100%
  Adding file-based HTTP access logger.............................   100%
  Adding 'emailAddress' attribute..................................   100%
  Updating subject attribute to user attribute configuration.........   100%
  Replacing schema file '02-config.ldif'...........................   100%
  Archiving concatenated schema....................................   100%

>>>> OpenDJ was successfully upgraded from version 2.4.5.7743 to 2.6.0.9086

 * See '/path/to/opendj/upgrade.log' for a detailed log of this operation
$ ./opendj/bin/start-ds --quiet
$
```

**Procedure 4.3. To Upgrade Replicated Servers**

- Upgrade each server sequentially, as described above.

**Procedure 4.4. To Upgrade OpenDJ DSML Gateway**

- Replace the gateway web application with the newer version, as for a fresh installation.

Chapter 5

# Removing OpenDJ Servers

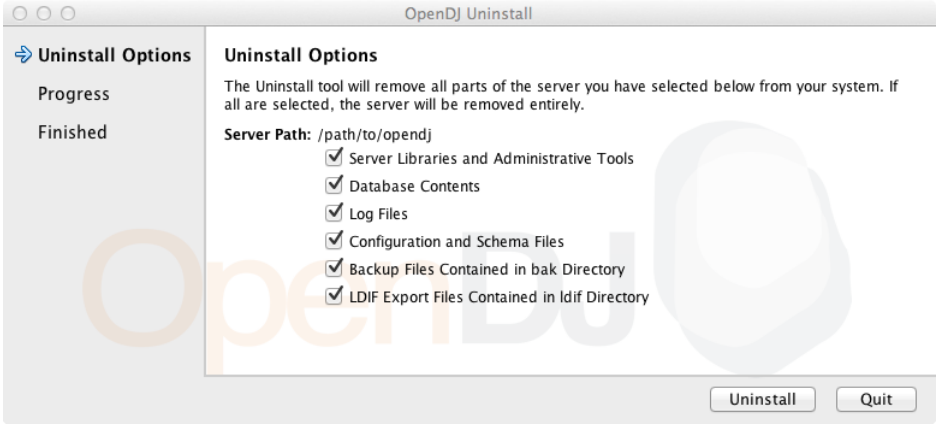
Remove OpenDJ directory server software with the **uninstall** command.

### Procedure 5.1. To Uninstall OpenDJ From the Graphical Uninstaller

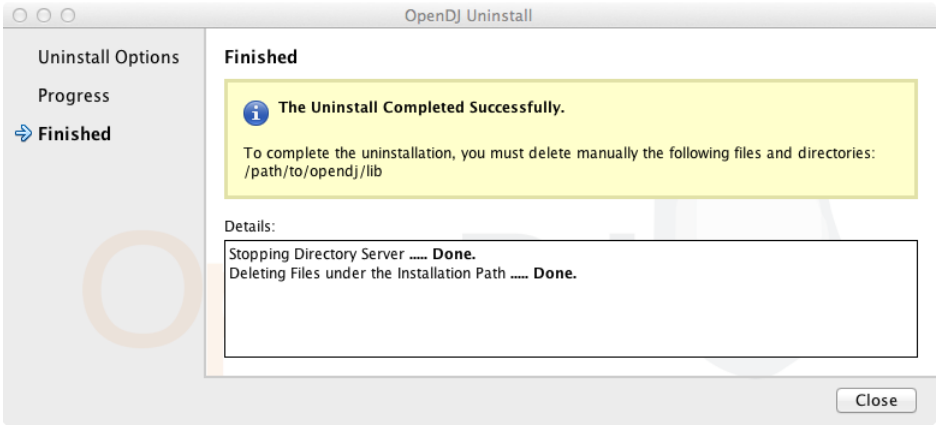
1. (UNIX) Run **opendj/uninstall**.

   (Windows) Double-click `opendj\uninstall.bat`.

   (Mac OS X) Double-click `opendj/Uninstall.app`.



2. When the process is finished, you might still have some files to remove manually.




**Procedure 5.2. To Uninstall OpenDJ On the Command Line**

1. Login as the user who installed and runs the server.

2. Run the **opendj/uninstall --cli** command.

   This command starts the removal program in interactive mode on the command line, prompting you for each option. Alternatively, use additional **uninstall** options to specify choices for the options. See **uninstall --help** for more information.

```
$ cd /path/to/opendj
$ ./uninstall --cli
Do you want to remove all components of the server or select the components to
remove?

    1)  Remove all components
    2)  Select the components to be removed

    q)  quit

Enter choice [1]:

The server is currently running and must be stopped before uninstallation can
continue.
Stop the Server and permanently delete the files? (yes / no) [yes]:

Stopping Directory Server ..... Done.
Deleting Files under the Installation Path ..... Done.

The Uninstall Completed Successfully.
To complete the uninstallation, you must delete manually the following files
and directories:
/path/to/opendj/lib
See /var/....log for a detailed log of this operation.
```

3. If the command output tells you to delete files manually, then remove those remaining files to complete the process.

```
$ rm -rf /path/to/opendj
```

**Procedure 5.3. To Uninstall the Debian Package**

When you uninstall the Debian package from the command line, OpenDJ directory server is stopped if it is running.

- Remove the package from your system.

```
$ sudo dpkg -r opendj
(Reading database ... 185725 files and directories currently installed.)
Removing opendj ...
*Stopping OpenDJ server...
Stopping Server...
[03/Jun/2013:10:00:49 +0200] category=BACKEND severity=NOTICE
 msgID=9896306 msg=The backend userRoot is now taken offline
[03/Jun/2013:10:00:49 +0200] category=CORE severity=NOTICE
 msgID=458955 msg=The Directory Server is now stopped

*OpenDJ successfully removed

$
```

  Removing the package does not remove your data or configuration. You must remove `/opt/opendj` manually to get rid of all files.

#### Procedure 5.4. To Uninstall the RPM Package

When you uninstall the RPM package from the command line, OpenDJ directory server is stopped if it is running.

- Remove the package from your system.

```
# rpm -e opendj
Pre Uninstall - uninstall
Stopping Server...
[03/Jun/2013:10:42:46 +0200] category=BACKEND severity=NOTICE
 msgID=9896306 msg=The backend userRoot is now taken offline
[03/Jun/2013:10:42:46 +0200] category=CORE severity=NOTICE
 msgID=458955 msg=The Directory Server is now stopped
Post Uninstall - uninstall
OpenDJ successfully removed.
#
```

  Removing the package does not remove your data or configuration. You must remove `/opt/opendj` manually to get rid of all files.

# Index