# Installation

## [Install From the Debian Package](https://backstage.forgerock.com/docs/opendj/3/install-guide/#install-deb)

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

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

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

### Install the OpenDJ directory server package:

**$ sudo dpkg -i opendj\_3.0.0-1\_all.deb**

Selecting previously unselected package opendj.

(Reading database ... 185569 files and directories currently installed.)

Unpacking opendj (from opendj\_3.0.0-1\_all.deb) ...

Setting up opendj (3.0.0) ...

Adding system startup for /etc/init.d/opendj ...

/etc/rc0.d/K20opendj -> ../init.d/opendj

/etc/rc1.d/K20opendj -> ../init.d/opendj

/etc/rc6.d/K20opendj -> ../init.d/opendj

/etc/rc2.d/S20opendj -> ../init.d/opendj

/etc/rc3.d/S20opendj -> ../init.d/opendj

/etc/rc4.d/S20opendj -> ../init.d/opendj

/etc/rc5.d/S20opendj -> ../init.d/opendj

Processing triggers for ureadahead ...

ureadahead will be reprofiled on next reboot

The Debian package installs OpenDJ directory server in the /opt/opendj directory, generates service management scripts, adds documentation files under /usr/share/doc/opendj, and adds man pages under /opt/opendj/share/man.

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

### 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

### (Optional) Check OpenDJ directory server status:

$ **service opendj status**

$opendj status: > Running.

$ **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 3.0.0

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:

# [Managing Data Replication](https://backstage.forgerock.com/docs/opendj/3/admin-guide/index.html#chap-replication)

OpenDJ uses advanced data replication with automated conflict resolution to help ensure your directory services remain available during administrative operations that take an individual server offline, or in the event a server crashes or a network goes down. This chapter explains how to manage OpenDJ directory data replication. In this chapter you will learn to:

* Set up replication as part of initial installation using OpenDJ control panel, or at any time using command-line tools
* Understand how replication operates in order to configure it appropriately
* Enable, initialize, and stop data replication
* Configure standalone directory servers and replication servers, or break a server that plays both roles into two standalone servers
* Configure replication groups, read-only replicas, assured replication, subtree replication, and fractional replication for complex deployments
* Configure and use change notification to synchronize external applications with changes to directory data
* Recover from situations where a user error has been applied to all replicas

## [Enabling Replication](https://backstage.forgerock.com/docs/opendj/3/admin-guide/index.html#enable-repl)

You can start the replication process by using the **dsreplication enable** command:

***$* /opt/opendj/bin*/*dsreplication \**

**enable \**

**--adminUID admin \**

**--adminPassword password \**

**--baseDN dc=tl=com \**

**--host1 opendj-1 \**

**--port1 4444 \**

**--bindDN1 "cn=Directory Manager" \**

**--bindPassword1 password \**

**--replicationPort1 8989 \**

**--host2 opendj-2 \**

**--port2 4444 \**

**--bindDN2 "cn=Directory Manager" \**

**--bindPassword2 password \**

**--replicationPort2 8989 \**

**--trustAll \**

**--no-prompt**

Establishing connections ..... Done.

Checking registration information ..... Done.

Updating remote references on server opendj.example.com:4444 ..... Done.

Configuring Replication port on server opendj2.example.com:4444 ..... Done.

Updating replication configuration for baseDN dc=example,dc=com on server

opendj.example.com:4444 ..... Done.

Updating replication configuration for baseDN dc=example,dc=com on server

opendj2.example.com:4444 ..... Done.

Updating registration configuration on server

opendj.example.com:4444 ..... Done.

Updating registration configuration on server

opendj2.example.com:4444 ..... Done.

Updating replication configuration for baseDN cn=schema on server

opendj.example.com:4444 ..... Done.

Updating replication configuration for baseDN cn=schema on server

opendj2.example.com:4444 ..... Done.

Initializing registration information on server opendj2.example.com:4444 with

the contents of server opendj.example.com:4444 ..... Done.

Initializing schema on server opendj2.example.com:4444 with the contents of

server opendj.example.com:4444 ..... Done.

Replication has been successfully enabled. Note that for replication to

work you must initialize the contents of the base DN's that are being

replicated (use dsreplication initialize to do so).

See

/var/.../opends-replication-7958637258600693490.log

for a detailed log of this operation.

# [Configuring Password Policies](https://backstage.forgerock.com/docs/opendj/3/admin-guide/#configure-pwp)

You configure server-based password policies by using the **dsconfig** command. Notice that server-based password policies are part of the server configuration, and therefore not replicated. Alternatively, you can configure a subset of password policy features by using subentry-based password policies that are stored with the replicated server data. This section covers both server-based and subentry-based password policies.

## [Procedure 10.1. To Adjust the Default Password Policy](https://backstage.forgerock.com/docs/opendj/3/admin-guide/#default-pwp)

You can reconfigure the default password policy, for example, to enforce password expiration, check that passwords do not match dictionary words, and prevent password reuse. This default policy is a server-based password policy.

### Enable the appropriate password validator:

**$ sudo /opt/opendj/bin/dsconfig \**

**set-password-validator-prop \**

**--port 4444 \**

**--hostname opendj-1 \**

**--bindDN "cn=Directory Manager" \**

**--bindPassword password \**

**--validator-name Dictionary \**

**--set enabled:true \**

**--set check-substrings:true \**

**--set min-substring-length:4 \**

**--trustAll \**

**--no-prompt**

### Apply the changes to the default password policy:

**$ sudo /opt/opendj/bin/dsconfig \**

**set-password-policy-prop \**

**--port 4444 \**

**--hostname opendj-1 \**

**--bindDN "cn=Directory Manager" \**

**--bindPassword password \**

**--policy-name "Default Password Policy" \**

**--set max-password-age:90d \**

**--set min-password-age:4w \**

**--set password-history-count:7 \**

**--set password-validator:Dictionary \**

**--trustAll \**

**--no-prompt**

### Check your work:

**$ sudo /opt/opendj/bin/dsconfig \**

**get-password-policy-prop \**

**--port 4444 \**

**--hostname opendj-1 \**

**--bindDN "cn=Directory Manager" \**

**--bindPassword password \**

**--policy-name "Default Password Policy"**

Property : Value(s)

------------------------------------------:--------------------------

account-status-notification-handler : -

allow-expired-password-changes : false

allow-user-password-changes : true

default-password-storage-scheme : Salted SHA-1

deprecated-password-storage-scheme : -

expire-passwords-without-warning : false

force-change-on-add : false

force-change-on-reset : false

grace-login-count : 0

idle-lockout-interval : 0 s

last-login-time-attribute : -

last-login-time-format : -

lockout-duration : 0 s

lockout-failure-count : 0

lockout-failure-expiration-interval : 0 s

max-password-age : 12 w 6 d

max-password-reset-age : 0 s

min-password-age : 4 w

password-attribute : userpassword

password-change-requires-current-password : false

password-expiration-warning-interval : 5 d

password-generator : Random Password Generator

password-history-count : 7

password-history-duration : 0 s

password-validator : Dictionary

previous-last-login-time-format : -

require-change-by-time : -

require-secure-authentication : false

require-secure-password-changes : false