



# Install PostgreSQL

---

This chapter provides information about installing and setting up PostgreSQL.

- [Install PostgreSQL Database, on page 1](#)
- [Set Up PostgreSQL Listening Port, on page 3](#)
- [User Access Restriction Recommendations, on page 4](#)

## Install PostgreSQL Database

### Before you begin

- Cisco recommends that a PostgreSQL DBA install and maintain the PostgreSQL server.
- Read the security recommendations for the PostgreSQL database in section [About Security Recommendations](#).
- For information on supported versions, see [External Database Setup Requirements](#).

### Procedure

---

**Step 1** Enter these commands to sign in to the database server as a Postgres user:

```
>su - postgres  
>psql
```

**Step 2** Create a new database user. The example below creates a new database user called *tcuser*:

```
#CREATE ROLE tcuser LOGIN CREATEDB;
```

**Note** If you deploy PostgreSQL version 8.4.x, you must configure the database user as a superuser at this point in the procedure, for example:

```
#ALTER ROLE tcuser WITH SUPERUSER;
```

**Step 3** Create the database. If your database contains ASCII characters only, create the database with SQL\_ASCII encoding. If your database contains non-ASCII characters, create the database with UTF8 encoding.

The example below creates an SQL\_ASCII database called *tcadb*.

```
#CREATE DATABASE tcmadb WITH OWNER tcuser ENCODING 'SQL_ASCII';
```

**Step 4** Configure user access to the database. Edit the `install_dir/data/pg_hba.conf` file to allow the `postgres` user and the new `tcuser` user to access the database. For example:

#	TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
	host	tcmadb	tcuser	10.89.99.0/24	password
	host	dbinst	mauser	10.89.99.0/24	password
	local <sup>1</sup>	all	all		Trust OR MD5

<sup>1</sup> For Unix domain socket connections only.

**Step 5** Enter these commands to define passwords for the `postgres` and `tcuser` users:

```
#ALTER ROLE postgres WITH PASSWORD 'mypassword';
#ALTER ROLE tcuser WITH PASSWORD 'mypassword';
```

**Note** You are required to enter a password for the database user when you configure an external database entry on the IM and Presence Service.

**Step 6** If you are running the PostgreSQL version 8.3.7 or a later 8.3.x release, change the permission of the `tcuser` to superuser to allow this user access to the database. Enter this command:

```
#ALTER ROLE tcuser WITH SUPERUSER;
```

**Step 7** Configure the connections to the database from remote hosts. Edit the `listen_addresses` parameter in the `install_dir/data/postgresql.conf` file. For example:

```
listen_addresses = '*'
```

**Step 8** If you are running PostgreSQL version 9.1.1, or higher, you must set the following values in the `postgresql.conf` file:

```
escape_string_warning = off
standard_conforming_strings = off
```

**Step 9** Stop and restart the PostgreSQL service, for example:

```
/etc/rc.d/init.d/postgresql-8.3 stop
/etc/rc.d/init.d/postgresql-8.3 start
```

**Note** The commands to stop and start the PostgreSQL service may vary between PostgreSQL releases.

**Step 10** Enter these commands to sign in to the new database as the `postgres` user and enable PL/pgSQL:

```
>psql tcmadb -U postgres
```

**Note** The following example, up to the semicolon, should be entered as one line.

```
#CREATE FUNCTION plpgsql_call_handler () RETURNS LANGUAGE_HANDLER AS '$libdir/plpgsql'
LANGUAGE C;

#CREATE TRUSTED PROCEDURAL LANGUAGE plpgsql HANDLER plpgsql_call_handler;
```

### Troubleshooting Tips

Do not turn on the following configuration items in the `install_dir/data/postgresql.conf` file (by default these items are commented out):

```
client_min_messages = log
log_duration = on
```

---

### Related Topics

[About Security Recommendations](#)

## Set Up PostgreSQL Listening Port



---

**Note** This section is optional configuration.

By default, the PostgreSQL database listens on port 5432. If you want to change this port, you must edit the PGPORT environment variable in `/etc/rc.d/init.d/postgresql` with the new port number.



---

**Note** The PGPORT environment variable overrides the 'Port' parameter value in the `/var/lib/pgsql/data/postgresql.conf` file, so you must edit the PGPORT environment variable if you want the PostgreSQL database to listen on a new port number.

---

### Procedure

**Step 1** Edit the PGPORT environment variable in `/etc/rc.d/init.d/postgresql` with the new port, for example:

```
IE: PGPORT=5555
```

**Step 2** Enter these commands to stop and start the PostgreSQL service:

```
# /etc/rc.d/init.d/postgresql start
# /etc/rc.d/init.d/postgresql stop
```

**Step 3** Confirm that the PostgreSQL database is listening on the new port using this command:

```
'lsof -i -n -P | grep postg'
postmaste 5754 postgres 4u IPv4 1692351 TCP *:5555 (LISTEN)
```

**Tip** For IPv6 servers, enter `postmaste 5754 postgres 4u IPv6 1692351 TCP *:5555 (LISTEN)`

**Step 4** To connect to the database after you have changed the port, you must specify the new port number in the command using the `-p` argument. If you do not include the `-p` argument in the command, the PostgreSQL database attempts to use the default port of 5432, and the connection to the database fails.

For example:

```
psql tcadb -p 5555 -U tcuser
```

## User Access Restriction Recommendations

We strongly recommend that you restrict user access to the external database to only the particular user and database instance that the IM and Presence Service uses. You can restrict user access to the PostgreSQL database in the `pg_hba.conf` file located in the `<install_dir>/data` directory.



### Caution

Do not configure 'all' for the user and database entries because potentially this could allow any user access to any database.

When you configure user access to the external database, we also recommend that you configure password protection for the database access using the 'password' method.



### Note

You are required to enter a password for the database user when you configure a database entry on IM and Presence Service.

The following are examples of a secure user access configuration, and a less secure user access configuration, in the `pg_hba.conf` file.

Example of a secure configuration:

# TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
host	dbinst1	tcuser1	10.89.99.0/24	password
host	dbinst2	mauser1	10.89.99.0/24	password

Example of a less secure configuration:

# TYPE	DATABASE	USER	CIDR-ADDRESS	METHOD
host	dbinst1	tcuser1	10.89.99.0/24	trust
host	dbinst2	all	10.89.99.0/24	password

Notes on the example of a less secure configuration:

- The first entry contains no password protection for the database.
- The second entry allows any user to access the database “dbinst2”.

### Related Topics

[Install PostgreSQL Database](#), on page 1

[PostgreSQL documentation](#)