
Libreswan

The Libreswan Project <https://libreswan.org/>

Libreswan is an Internet Key Exchange (IKE) implementation for Linux, FreeBSD, NetBSD and OpenBSD. It supports IKEv1 and IKEv2 and has support for most of the extensions (RFC + IETF drafts) related to IPsec, including IKEv2, X.509 Digital Certificates, NAT Traversal, and many others.

Libreswan was forked from Openswan 2.6.38, which was forked from FreeS/WAN 2.04. See the CREDIT-ITS files for contributor acknowledgments.

It can be downloaded from:

```
1 https://download.libreswan.org/
```

A Git repository is available at:

```
1 https://github.com/libreswan/libreswan/
```

License

The bulk of libreswan is licensed under the GNU General Public License version 2; see the LICENSE and CREDIT.* files. Some smaller parts have a different license.

Installing

A pre-built Libreswan package is available on the following OS distributions: RHEL, Fedora, CentOS, Ubuntu, Debian, Arch, Apline, OpenWrt and FreeBSD. On NetBSD the package sources are in wip/libreswan.

Unless a source-based build is truly needed, it is often best to use the pre-built version of the distribution you are using.

Installing from Source

Requirements

There are a few packages required for Libreswan to compile from source:

For Debian/Ubuntu

```
1 apt-get install net-tools make build-essential \
2   libnss3-dev pkg-config libevent-dev libunbound-dev \
3   bison flex libsystemd-dev libcurl4-nss-dev \
4   libpam0g-dev libcap-ng-dev libldns-dev xmlto
```

For Fedora/CentOS-Stream/RHEL/AlmaLinux/RockyLinux etc.

```
1 dnf install audit-libs-devel bison curl-devel flex \
2   gcc ldns-devel libcap-ng-devel libevent-devel \
3   libseccomp-devel libselinux-devel make nspr-devel \
4   nss-devel pam-devel pkgconfig systemd-devel \
5   unbound-devel xmlto
```

Alpine Linux:

```
1 aph add mandoc mandoc-doc apk-tools-doc bison \
2   bison-doc bsd-compat-headers coreutils coreutils-doc \
3   curl-dev curl-doc flex flex-doc gcc gcc-doc git git-doc \
4   gmp-dev gmp-doc ldns-dev ldns-doc libcap-ng-dev \
5   libcap-ng-doc libevent-dev linux-pam-dev linux-pam-doc \
6   make make-doc musl-dev nspr-dev nss-dev nss-tools \
7   pkgconfig sed sed-doc unbound-doc unbound-dev \
8   xmlto xmlto-doc
```

FreeBSD:

```
1 pkg install gmake git pkgconf nss libevent unbound bison \
2   flex ldns xmlto gcc
```

NetBSD:

```
1 pkgin install git gmake nss unbound bison flex ldns xmlto pkgconf
```

OpenBSD:

```
1 pkg_add gmake nss libevent libunbound bison libldns xmlto \
2   curl git llvm%16
```

Building for RPM based systems

Install requirements for rpm package building:

```
1 dnf install rpm-build rpmdevtools
```

The `packaging/` directory is used to find the proper spec file for your distribution. Simply issue the command:

```
1 make rpm
```

You can also pick a specific spec file. For example, to build for CentOS8, use:

```
1 rpmbuild -ba packaging/centos/8/libreswan.spec
```

Building for DEB based systems

The packaging/debian directory is used to build deb files. Simply issue the command:

```
1 make deb
```

Building from scratch into /usr/local

GNU Make is used:

```
1 gmake
2 sudo gmake install
```

If you want to build without creating and installing manual pages, run:

```
1 gmake base
2 sudo gmake install-base
```

Starting Libreswan

The install will detect the init system used (systemd, upstart, sysvinit, openrc) and should integrate with the linux distribution. The service name is called “ipsec”. For example, on CentOS Stream 9, one would use:

```
1 systemctl enable ipsec.service
2 systemctl start ipsec.service
```

If unsure of the specific init system used on the system, the “ipsec” command can also be used to start or stop the ipsec service. This command will auto-detect the init system and invoke it:

```
1 ipsec start
2 ipsec stop
```

Status

For a connection status overview, use:

```
1 ipsec trafficstatus
```

For a brief status overview, use:

```
1 ipsec briefstatus
```

For a machine readable global status, use:

```
1 ipsec globalstatus
```

Configuration

Most of the libreswan configuration is stored in `/etc/ipsec.conf` and `/etc/ipsec.secrets`. Include files may be present in `/etc/ipsec.d/`. See the respective man pages for more information.

NSS initialisation

Libreswan uses NSS to store private keys and X.509 certificates. The NSS database should have been initialised by the package installer. If not, the NSS database can be initialised using:

```
1 ipsec initnss
```

PKCS#12 certificates (.p12 files) can be imported using:

```
1 ipsec import /path/to/your.p12
```

See `README.NSS` and `certutil --help` for more details on using NSS and migrating from the old Openswan `/etc/ipsec.d/` directories to using NSS.

Upgrading

If you are upgrading from older Libreswan versions, Libreswan 5.x you might need to adjust your config files, although great care has been put into making the configuration files full backwards compatible.

See ‘`man ipsec.conf`’ for the list of options to find any new features.

You can run `make install` on top of your old version - it will not overwrite your `/etc/ipsec.*` configuration files. The default install target installs in `/usr/local`. Ensure you do not install libreswan twice, one from a distribution package in `/usr` and once manually in `/usr/local`.

Note that for rpm based systems, the NSS directory changed from `/etc/ipsec.d` to `/var/lib/ipsec/nss/`

Help

Mailing lists:

The mailing lists, including archives are at <https://lists.libreswan.org/>

Wiki:

Libreswan's wiki is at https://libreswan.org/wiki/Main_Page. It contains documentation, interoper guides and other useful information.

IRC:

Libreswan developers and users can be found on IRC, on [#libreswan](https://libera.chat)

Bugs

Bugs can be reported on the mailing list swan-dev@lists.libreswan.org or using our bug tracking system, at:

```
1 https://github.com/libreswan/libreswan/issues
```

Security Information

All security issues found that require public disclosure will receive proper CVE tracking numbers (see <https://www.mitre.org/>) and will be co-ordinated via the vendor-sec / oss-security lists. A complete list of known security vulnerabilities is available at:

```
1 https://libreswan.org/security/
```

Please contact security@libreswan.org or:

```
1 https://github.com/libreswan/libreswan/security
```

if you suspect you have found a security issue or vulnerability in libreswan. Encrypted email can be received encrypted to the libreswan OpenPGP key. We strongly encourage you to report potential security vulnerabilities to us before disclosing them in a public forum or in a public security paper or conference.

Development

Those interested in the development, patches, and beta releases of Libreswan can join the development mailing list swan-dev@lists.libreswan.org or talk to the development team on IRC in [#libreswan](https://libera.chat)

on `irc.libera.chat`

For those who want to track things a bit more closely, the `swan-commits@lists.libreswan.org` mailing list will mail all the commit messages when they happen. This list is quite busy during active development periods.

Documentation

The most up to date documentation consists of the man pages that come with the software. Further documentation can be found at:

```
1 https://libreswan.org/
```

and the wiki at:

```
1 https://libreswan.org/wiki/
```