

# Intermediate CA configuration file

[View this file as plain text.](#)

```
# OpenSSL intermediate CA configuration file.
# Copy to `/root/ca/intermediate/openssl.cnf`.

[ ca ]
# `man ca`
default_ca = CA_default

[ CA_default ]
# Directory and file locations.
dir                = /root/ca/intermediate
certs              = $dir/certs
crl_dir            = $dir/crl
new_certs_dir      = $dir/newcerts
database           = $dir/index.txt
serial             = $dir/serial
RANDFILE           = $dir/private/.rand

# The root key and root certificate.
private_key         = $dir/private/intermediate.key.pem
certificate         = $dir/certs/intermediate.cert.pem

# For certificate revocation lists.
crlnumber           = $dir/crlnumber
crl                = $dir/crl/intermediate.crl.pem
crl_extensions      = crl_ext
default_crl_days    = 30

# SHA-1 is deprecated, so use SHA-2 instead.
default_md          = sha256

name_opt            = ca_default
cert_opt            = ca_default
default_days        = 375
preserve            = no
policy              = policy_loose

[ policy_strict ]
# The root CA should only sign intermediate certificates that match.
# See the POLICY FORMAT section of `man ca`.
countryName         = match
stateOrProvinceName = match
organizationName    = match
organizationalUnitName = optional
commonName          = supplied
```

```
emailAddress          = optional

[ policy_loose ]
# Allow the intermediate CA to sign a more diverse range of certificat
# See the POLICY FORMAT section of the `ca` man page.
countryName           = optional
stateOrProvinceName   = optional
localityName          = optional
organizationName       = optional
organizationalUnitName = optional
commonName             = supplied
emailAddress           = optional

[ req ]
# Options for the `req` tool (`man req`).
default_bits          = 2048
distinguished_name    = req_distinguished_name
string_mask            = utf8only

# SHA-1 is deprecated, so use SHA-2 instead.
default_md             = sha256

# Extension to add when the -x509 option is used.
x509_extensions        = v3_ca

[ req_distinguished_name ]
# See <https://en.wikipedia.org/wiki/Certificate\_signing\_request>.
countryName            = Country Name (2 letter code)
stateOrProvinceName    = State or Province Name
localityName           = Locality Name
0.organizationName     = Organization Name
organizationalUnitName = Organizational Unit Name
commonName             = Common Name
emailAddress           = Email Address

# Optionally, specify some defaults.
countryName_default    = GB
stateOrProvinceName_default = England
localityName_default   =
0.organizationName_default = Alice Ltd
organizationalUnitName_default =
emailAddress_default    =

[ v3_ca ]
# Extensions for a typical CA (`man x509v3_config`).
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ v3_intermediate_ca ]
# Extensions for a typical intermediate CA (`man x509v3_config`).
```

```
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid:always,issuer
basicConstraints = critical, CA:true, pathlen:0
keyUsage = critical, digitalSignature, cRLSign, keyCertSign

[ usr_cert ]
# Extensions for client certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = client, email
nsComment = "OpenSSL Generated Client Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = clientAuth, emailProtection

[ server_cert ]
# Extensions for server certificates (`man x509v3_config`).
basicConstraints = CA:FALSE
nsCertType = server
nsComment = "OpenSSL Generated Server Certificate"
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer:always
keyUsage = critical, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth

[ crl_ext ]
# Extension for CRLs (`man x509v3_config`).
authorityKeyIdentifier=keyid:always

[ ocsp ]
# Extension for OCSP signing certificates (`man ocsp`).
basicConstraints = CA:FALSE
subjectKeyIdentifier = hash
authorityKeyIdentifier = keyid,issuer
keyUsage = critical, digitalSignature
extendedKeyUsage = critical, OCSPSigning
```

[Comments](#) 

[← Previous](#)

**Version 1.0.4** — Last updated on 2015-12-09.

© [Copyright](#) 2013-2015, [Jamie Nguyen](#). Created with Sphinx using a custom-built theme.