Generate CA and EE Certificates Using OpenSSL

For supported software information, click here.

To generate CA and EE certificates on a VOS device, use OpenSSL on any Linux system to perform the procedures described in this article.

Generate a CA Certificate

1. Create a file called versa-ras-ca.conf, and copy the following configuration text into the file, making the following changes:
   • Delete the first and last lines shown below.
   • For the name, surname, givenName, initials, and dnQualifiers fields, enter the desired values.

```
---------- start of versa-ras-ca.conf(do not copy this line) ----------
[ req ]
prompt = no
distinguished_name = my dn

[ my dn ]
# The bare minimum is probably a commonName
           commonName = RAS-CA
          countryName = US
         localityName = San Jose
     organizationName = Versa Networks Inc
organizationalUnitName = VPN
   stateOrProvinceName = CA
        emailAddress = ras-ca@versa-networks.com
               name = <givenName>
            surname = <surname>
          givenName = <givenName>
           initials = <initials>
         dnQualifier = <dsQualifier>

[ my server exts ]
keyUsage = nonRepudiation, digitalSignature, keyEncipherment, keyCertSign, cRLSign
extendedKeyUsage = serverAuth, clientAuth
basicConstraints = CA:true
subjectKeyIdentifier=hash
authorityKeyIdentifier=keyid:always,issuer:always
---------- end of versa-ras-ca.conf(do not copy this line) ----------
```

2. Generate an RSA key-pair for the CA certificate:

```
openssl genrsa -out versa-ras-ca.key 2048
```

3. Create the CA certificate:

```
openssl req -x509 -config versa-ras-ca.conf -extensions 'my server exts' -nodes -days 365 -newkey
rsa:2048 -keyout versa-ras-ca.key -out versa-ras-ca.pem
```

4. Verify the newly generated CA certificate:

```
openssl x509 -in versa-ras-ca.pem -text -noout
```

Generate an EE Certificate

1. Create a file called versa-ras-ee.conf, and copy the following configuration text into the file, making the following changes:
   • Delete the first and last lines shown below.
   • Change req_distinguished_name to the desired distinguished name.
   • In the commonName and subjectAltName fields, enter the IP address of the interface to use to establish the IPsec connection with the RACs.

```
---------- start of versa-ras-ee.conf(do not copy this line) ----------
[req]
default_bits          = 2048
default_md            = sha1
encrypt_key           = no
string_mask           = utf8only
distinguished_name    = req_distinguished_name
req_extensions        = v3_req
prompt                = no

[req_distinguished_name]
countryName           = US
stateOrProvinceName   = CA
localityName          = Fremont
organizationName      = Versa Networks Inc.
commonName            = 70.70.70.15

[ usr_cert ]
subjectKeyIdentifier   = hash
authorityKeyIdentifier = keyid,issuer
basicConstraints       = CA:FALSE
copy_extensions        = copy
subjectAltName         = email:copy

[v3_req]
basicConstraints       = CA:false
keyUsage               = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage       = serverAuth, clientAuth
subjectAltName         = IP:70.70.70.15
---------- end of versa-ras-ee.conf(do not copy this line) ----------
```

2. Create a file called versa-ras-ca.srl that contains the text string 1000.
3. Generate an RSA key-pair for the end-entity certificate:

   ```
   openssl genrsa -out versa-ras-ee.key 2048
   ```

4. Generate a certificate request for the end-entity certificate:

   ```
   openssl req -new -out versa-ras-ee.csr -newkey rsa:2048 -nodes -sha256 -keyout versa-ras-ee.key -config
   versa-ras-ee.conf -extensions v3_req
   ```

5. Sign the end-entity certificate using the CA certificate:

   ```
   openssl x509 -req -days 365 -in versa-ras-ee.csr -out versa-ras-ee.pem -CA versa-ras-ca.pem -CAkey
   versa-ras-ca.key -extfile ./versa-ras-ee.conf -extensions v3_req
   ```

6. Check the end-entity certificate:

   ```
   openssl x509 -in versa-ras-ee.pem -text -noout
   ```

Supported Software Information

Releases 20.2.2 and later support all content described in this article.

Additional Information

Configure Versa SASE Clients
Configure the Versa Secure Access Service