

Manually Obtaining Digital Certificates

You can manually add digital certificates, or you can use SCEP to help manage how you obtain certificates.

For information about using SCEP to obtain certificates, see Obtaining Digital Certificates through SCEP .

To manually add a signed certificate:

1. Create a certificate signing request.

```
user@host> request security generate-certificate-request subject subject  
password password
```

where:

- **subject** is the distinguished name of the SRC host; for example `cn=cseries1,ou=pop,o=Juniper,l=kanata,st=Ontario,c=Canada`.
- **password** is the password received from the certificate authority for the specified subject.

By default, this request creates the file `/tmp/certreq.csr` and encodes the file by using Privacy-Enhanced Mail (pem) encoding.

2. Copy the file generated to another system, and submit the certificate signing request file generated to the certificate authority.

You can transfer the file through FTP by using the `file copy` command.

```
user@host> file copy source_file ftp:// username @ server [: port ]/  
destination_file
```

The remote system prompts you for your password.

3. When you receive the signed certificate, copy the file back to the system to the `/tmp` directory.

You can transfer the file through FTP, as shown in Step 2.

4. Add the certificate to the SRC configuration.

```
user@host> request security import-certificate file-name file-name identifier  
identifier
```

where

- **file-name** is the name of the certificate file in the `/tmp` folder. The file has one of the following extensions:
 - CER—Windows extension
 - PEM—Privacy-Enhanced Mail encoding

- DER—Binary encoding
- BER—Binary encoding
- identifier is the name of the certificate.

For example, to import the file `sdx.cer` that is identified as `web`:

```
user@host> request security import-certificate file-name sdx.cer identifier web
```

5. Verify that the certificate is part of the SRC configuration.

```
user@host> show security certificate
web subject:CN=host
```

If there are no certificates on the system, the CLI displays the following message:

```
user@host> show security certificate
No entity certificates in key store
```

- Related Topics**
- Before You Use Digital Certificates
 - Removing a Certificate Request
 - Overview of Digital Certificates
 - Commands to Manage Digital Certificates