Chapter 21

Managing Security Digital Certificates

This chapter describes how digital certificates are used on by the SRC software and how to obtain and delete these certificates. Topics include:

Overview of Digital Certificates

The SRC software provides support for digital certificates for use by other protocols to protect communications between the SRC software and other applications or network devices. You can manage certificates to:

- Support HTTPS connections between the SRC software and Web browsers.
- Allow BEEP TLS connections between the SRC software and JUNOS routing platforms.

You can use SRC CLI commands to manage certificates manually, or through the Simple Certificate Enrollment Protocol (SCEP).

Certificates are in the format defined in the X.509 standard for public key infrastructure. The certificate requests are in the Public Key Cryptology Standard (PKCS) #10 format.

Before You Use Digital Certificates

Before you use digital certificates, you should:

- Have a working relationship with a certificate authority (CA).
- Have a good working knowledge of how to work with certificates.
- Decide whether or not to use SCEP to assist with certificate management.
- Identify which connections should be secured by a protocol that requires digital certificates.
- Know how to use the file management commands in the CLI.

Commands to Manage Digital Certificates

You can use the following operational mode commands to manage digital certificates. Which commands you use depends on whether or not you use SCEP.

- clear security certificate
- clear certificate request
- request security generate-certificate-request
- request security enroll (SCEP)
- request security get-ca-certificate (SCEP)
- request security import-certificate
- show security certificate

For detailed information about each command, see the *SRC-PE CLI Command Reference*.

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* on page 192.

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 in Step 1 to another system, and submit the certificate signing request file generated in Step 1 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
   ```

Obtaining Digital Certificates through SCEP

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

For information about manually obtaining certificates, see *Manually Obtaining Digital Certificates* on page 191.

To add a signed certificate that you obtain through SCEP:

1. Request a CA certificate through SCEP.

   user@host> **request security get-ca-certificate url** *url* **ca_identifier** *ca_identifier*

   where:

   - url is the URL of the certificate authority (which is the SCEP server).
   - ca-identifier is the identifier that designates the authority.

For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

```
user@host> request security get-ca-certificate url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
ca-identifier SdxCA

Version: 3
Serial Number: 5721058705923989279
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
Valid From: Wed Sep 06 17:00:55 EDT 2006
Valid Until: Sat Sep 03 17:10:55 EDT 2016
Subject: CN=SdxCA
Public key: RSA
Thumbprint Algorithm: SHA1
Thumbprint: 3c 57 a9 77 af 83 3 e9 c7 1e ee e2 4a e8 ff f3 89 f4 11 a9
Do you want to add the above certificate as a trusted CA [yes,no] ? (no) y
```

2. Request that the certificate authority automatically sign the certificate request.

   user@host> **request security enroll subject** *subject* **password** *password*

   where:

   - subject is the distinguished name of the SRC host; for example cn=myhost.
   - password is the password received from the certificate authority for the specified subject.

   For example, to request a certificate from the CA authority SdxCA at a specified URL on the server security_server:

```
user@host> request security enroll url
http://security_server:8080/ejbca/publicweb/apply/scep/pkiclient.exe
identifier web ca-identifier SdxCA subject cn=myhost password mypassword

Received certificate:
Version: 3
Serial Number: 6822890691617224432
Signature Algorithm: SHA1withRSA
Issuer: CN=SdxCA
Valid From: Tue Sep 19 16:33:11 EDT 2006
Valid Until: Thu Sep 18 16:43:11 EDT 2008
Subject: CN=myhost
Public key: RSA
Do you want to install the above certificate [yes,no] ? (no) y
```

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

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

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

No entity certificates in key store

Removing a Certificate Request

To remove a certificate request:

1. Review the certificate request files on the system. These files are in the /tmp directory and have the file extension .csr.

2. Issue the clear security certificate-request command to remove a file. For example:

user@host> **clear security certificate-request certreq.csr**

Removing a Certificate

To remove a certificate:

1. Issue the show security certificate command to view information about the local certificates. For example:

```
user@host> show security certificate
web subject:CN=myhost
CAcert1 subject:CN=myhost
```

2. Issue the clear security certificate command to remove a certificate. Use the trusted option if the certificate is a CA certificate.

clear security certificate <trusted> <identifier *identifier*>

For example:

- To remove the certificate web (that is not a trusted certificate) from myhost:

  user@host>**clear security certificate web**

- To remove a trusted (CA) certificate from myhost:

  user@host>**clear security certificate trusted CAcert1**