



# Security Certificates for the SRC Software



Published: 2013-06-05

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, California 94089  
USA  
408-745-2000  
www.juniper.net

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*Security Certificates for the SRC Software*

Copyright © 2013, Juniper Networks, Inc.  
All rights reserved.

The information in this document is current as of the date on the title page.

#### YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

#### END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

# Table of Contents

	About the Documentation . . . . .	vii
	Documentation and Release Notes . . . . .	vii
	Supported Platforms . . . . .	vii
	Documentation Conventions . . . . .	vii
	Documentation Conventions . . . . .	viii
	Documentation Feedback . . . . .	ix
	Requesting Technical Support . . . . .	x
	Self-Help Online Tools and Resources . . . . .	x
	Opening a Case with JTAC . . . . .	xi
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Software Features Overview . . . . .</b>	<b>3</b>
	SRC Component Overview . . . . .	3
<b>Chapter 2</b>	<b>Security Digital Certificates . . . . .</b>	<b>9</b>
	Digital Certificates Overview . . . . .	9
	Before You Use Digital Certificates . . . . .	9
<b>Part 2</b>	<b>Administration</b>	
<b>Chapter 3</b>	<b>Managing Digital Certificates . . . . .</b>	<b>13</b>
	Manually Obtaining Digital Certificates (SRC CLI) . . . . .	13
	Obtaining Digital Certificates through SCEP (SRC CLI) . . . . .	14
	Removing a Certificate Request . . . . .	16
	Removing a Certificate . . . . .	16
<b>Chapter 4</b>	<b>Routine Monitoring . . . . .</b>	<b>19</b>
	Viewing Information About Security Certificates (SRC CLI) . . . . .	19
	Viewing Information About Security Certificates (C-Web Interface) . . . . .	19
<b>Chapter 5</b>	<b>Management Commands . . . . .</b>	<b>21</b>
	Commands to Manage Digital Certificates . . . . .	21
<b>Part 3</b>	<b>Index</b>	
	Index . . . . .	25



# List of Tables

	<b>About the Documentation . . . . .</b>	<b>vii</b>
	Table 1: Notice Icons . . . . .	viii
	Table 2: Notice Icons . . . . .	viii
	Table 3: Text Conventions . . . . .	viii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>Software Features Overview . . . . .</b>	<b>3</b>
	Table 4: Descriptions of SRC Components . . . . .	3



# About the Documentation

- Documentation and Release Notes on page vii
- Supported Platforms on page vii
- Documentation Conventions on page vii
- Documentation Feedback on page ix
- Requesting Technical Support on page x

## Documentation and Release Notes

---

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at <http://www.juniper.net/techpubs/>.

If the information in the latest release notes differs from the information in the documentation, follow the product Release Notes.

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

## Supported Platforms

---

For the features described in this document, the following platforms are supported:

- C Series

## Documentation Conventions

---

Table 1 on page viii defines notice icons used in this guide.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

## Documentation Conventions

Table 1 on page viii defines the notice icons used in this guide. Table 3 on page viii defines text conventions used throughout this documentation.

Table 2: Notice Icons





Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 3: Text Conventions

Convention	Description	Examples
<b>Bold text like this</b>	<ul style="list-style-type: none"> <li>Represents keywords, scripts, and tools in text.</li> <li>Represents a GUI element that the user selects, clicks, checks, or clears.</li> </ul>	<ul style="list-style-type: none"> <li>Specify the keyword <b>exp-msg</b>.</li> <li>Run the <b>install.sh</b> script.</li> <li>Use the <b>pkgadd</b> tool.</li> <li>To cancel the configuration, click <b>Cancel</b>.</li> </ul>

Table 3: Text Conventions (*continued*)

<b>Bold text like this</b>	Represents text that the user must type.	<b>user@host# set cache-entry-age</b> <i>cache-entry-age</i>
Fixed-width text like this	Represents information as displayed on your terminal's screen, such as CLI commands in output displays.	<pre> nic-locators {   login {     resolution {       resolver-name /realms/       login/A1;       key-type LoginName;       value-type SaeId;     }   } </pre>
Regular sans serif typeface	<ul style="list-style-type: none"> <li>Represents configuration statements.</li> <li>Indicates SRC CLI commands and options in text.</li> <li>Represents examples in procedures.</li> <li>Represents URLs.</li> </ul>	<ul style="list-style-type: none"> <li><b>system ldap server{</b> <b>stand-alone;</b></li> <li>Use the <b>request sae modify device failover</b> <b>command</b> with the force option</li> <li><b>user@host# ...</b></li> <li><a href="http://www.juniper.net/techpubs/software/management/sdx/api-index.html">http://www.juniper.net/techpubs/software/management/sdx/api-index.html</a></li> </ul>
<i>Italic sans serif typeface</i>	Represents variables in SRC CLI commands.	<b>user@host# set local-address</b> <i>local-address</i>
Angle brackets	In text descriptions, indicate optional keywords or variables.	Another runtime variable is <gfwif>.
Key name	Indicates the name of a key on the keyboard.	Press Enter.
Key names linked with a plus sign (+)	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<i>Italic typeface</i>	<ul style="list-style-type: none"> <li>Emphasizes words.</li> <li>Identifies book names.</li> <li>Identifies distinguished names.</li> <li>Identifies files, directories, and paths in text but not in command examples.</li> </ul>	<ul style="list-style-type: none"> <li>There are two levels of access: <i>user</i> and <i>privileged</i>.</li> <li><i>SRC-PE Getting Started Guide</i>.</li> <li><i>o=Users, o=UMC</i></li> <li>The <i>/etc/default.properties</i> file.</li> </ul>
Backslash	At the end of a line, indicates that the text wraps to the next line.	<pre> Plugin.radiusAcct-1.class=\ net.juniper.smgmt.sae.plugin\ RadiusTrackingPluginEvent </pre>
Words separated by the   symbol	Represent a choice to select one keyword or variable to the left or right of this symbol. (The keyword or variable may be either optional or required.)	diagnostic   line

## Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to [techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at

<https://www.juniper.net/cgi-bin/docbugreport/> . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

## Requesting Technical Support

---

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

## Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://www.juniper.net/alerts/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://tools.juniper.net/SerialNumberEntitlementSearch/>

## Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.



## PART 1

# Overview

- [Software Features Overview on page 3](#)
- [Security Digital Certificates on page 9](#)



## CHAPTER 1

# Software Features Overview

- [SRC Component Overview on page 3](#)

## SRC Component Overview

---

The SRC software is a dynamic system. It contains many components that you use to build a subscriber management environment. You can use these tools to customize and extend the SRC software for your use and to integrate the SRC software with other systems. The SRC software also provides the operating system and management tools for C Series Controllers.

[Table 4 on page 3](#) gives a brief description of the components that make up the SRC software.

**Table 4: Descriptions of SRC Components**

Component	Description
<b>Server Components</b>	
Service activation engine (SAE)	<ul style="list-style-type: none"><li>• Authorizes, activates, and deactivates subscriber and service sessions by interacting with systems such as Juniper Networks routers, cable modem termination system (CMTS) devices, RADIUS servers, and directories.</li><li>• Collects accounting information about subscribers and services from routers, and stores the information in RADIUS accounting servers, flat files, and other accounting databases.</li><li>• Provides plug-ins and application programming interfaces (APIs) for starting and stopping subscriber and service sessions and for integrating with systems that authorize subscriber actions and track resource usage.</li></ul>
Subscriber Information Collector (SIC)	Used in conjunction with the MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SIC listens for RADIUS accounting events from IP edge devices (accounting clients) and stores them in the Session State Registrar (SSR), or forwards them to a remote AAA server, allowing the SRC software to gain increased subscriber awareness. Additionally, the SIC can optionally edit accounting events before routing them.
Juniper Policy Server (JPS)	Acts as a policy decision point (PDP) and policy enforcement point (PEP) that manages the relationships between application managers and CMTS devices in a PCMM environment.

Table 4: Descriptions of SRC Components *(continued)*

Component	Description
Network information collector (NIC)	Collects information about the state of the network and can provide a mapping from a given type of network data to another type of network data.
Redirect Server	Redirects HTTP requests received from IP Filter to a captive portal page.
3GPP Gateway	The SRC Third-Generation Partnership Project (3GPP) gateway is a Diameter-based component in the SRC software, which provides integration with 3GPP Policy and Charging Control environments, to provide fixed-mobile convergence (FMC). The SRC 3GPP gateway provides Gx-based integration with the Policy and Charging Rules Function (PCRF). The SRC 3GPP gateway uses the Gx interface to mediate between the PCRF and Juniper Networks routers like the E Series Broadband Services routers and MX Series routers. The Gx interface on the SRC 3GPP gateway communicates with the PCRF using the Diameter protocol.
Web Application Service	The SRC software includes a Web application server that hosts the Web Services Gateway and the Volume Tracking Application (SRC VTA). In production environments, this application server is designed to host only these applications. However, you can load your own applications into this server for testing or demonstration purposes.
Web Services Gateway	<p>Allows a gateway client—an application that is not part of the SRC network—to interact with SRC components through a Simple Object Access Protocol (SOAP) interface.</p> <p>The Web Services Gateway provides the Dynamic Service Activator which allows a gateway client to dynamically activate and deactivate SRC services for subscribers and to run scripts that manage the SAE.</p>
<b>Repository</b>	
Directory	<p>The SRC software includes the Juniper Networks database, which is a built-in Lightweight Directory Access Protocol (LDAP) directory for storing all SRC data including services, policies, and small subscriber databases.</p> <p>For large subscriber databases, you must supply your own directory.</p>
Session State Registrar (SSR)	The SSR is a stateless, highly reliable and highly available database cluster. When used in conjunction with an MX Series router running the packet-triggered subscribers and policy control (PTSP) solution, the SSR stores the IP edge attachment subscriber sessions data learned from IP edge devices in the centralized SSR database.

#### SRC Configuration and Management Tools

Table 4: Descriptions of SRC Components (*continued*)

Component	Description
SRC command line interface (CLI)	Provides a way to configure the SRC software on a C Series Controller from a Junos OS–like CLI. The SRC CLI includes the policies, services, and subscribers CLI, which has separate access privileges.
C-Web interface	Provides a way to configure, monitor, and manage the SRC software on a C Series Controller through a Web browser. The C-Web interface includes a policies, services, and subscribers component, which has separate access privileges.
Simple Network Management Protocol (SNMP) agent	Monitors system performance and availability. It runs on all the SRC hosts and makes management information available through SNMP tables and sends notifications by means of SNMP traps.
<b>Service Management Applications (Run on external system)</b>	
IMS Services Gateway	Integrates into an IP multimedia system (IMS) environment. The SRC software provides a Diameter protocol-based interface that allows the SRC software to integrate with services found on the application layer of IMS.
<b>SRC Programming Interfaces</b>	
NETCONF API	Allows you to configure or request information from the NETCONF server on a C Series Controller that runs the SRC software. Applications developed with the NETCONF API run on a system other than a C Series Controller.
CORBA plug-in service provider interface (SPI)	Tracks sessions and enables linking the rest of the service provider's operations support system (OSS) with the SRC software so that the OSS can be notified of events in the life cycle of SAE sessions. Hosted plug-ins only.
CORBA remote API	Provides remote access to the SAE core API. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
NIC access API	Performs NIC resolutions. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.
SAE core API	Controls the behavior of the SRC software. Applications that use these extensions to the SRC software run on a system other than a C Series Controller.

Table 4: Descriptions of SRC Components (*continued*)

Component	Description
Script services	Provides an interface to call scripts that supply custom services such as provisioning policies on a number of systems across a network.
VTA API	The Volume Tracking Application (VTA) API is a Simple Object Access Protocol (SOAP) interface that allows developers to create gateway clients and that administrators use to manage VTA subscribers and sessions. The SRC Web Services Gateway allows a gateway client—an application that is not part of the SRC network—to interact with SRC components, such as the VTA, through a SOAP interface.
<b>Authorization and Accounting Applications</b>	
AAA RADIUS servers	Authenticates subscribers and authorizes their access to the requested system or service. Accepts accounting data—time active and volume of data sent—about subscriber and service sessions. RADIUS servers run on a system other than a C Series Controller.
SRC Admission Control Plug-In (SRC ACP)	Authorizes and tracks subscribers' use of network resources associated with services that the SRC application manages.
Flat file accounting	Stores tracking data to accounting flat files that can be made available to external systems that send the data to a rating and billing system.
Volume Tracking Application	<p>The SRC Volume Tracking Application (SRC VTA) is an SRC component that allows service providers to track and control the network usage of subscribers and services. You can control volume and time usage on a per-subscriber or per-service basis. This level of control means that service providers can offer tiered services that use volume as a metric, while also controlling abusive subscribers and applications.</p> <p>When a subscriber or service exceeds bandwidth limits (or quotas), the SRC VTA can take actions including imposing rate limits on traffic, sending an e-mail notification, or charging extra for additional bandwidth consumed.</p>
<b>Demonstration Applications (available on the Juniper Networks Web site)</b>	
Enterprise Audit Plug-In	Defines a callback interface, which receives events when IT managers complete specified operations.
Enterprise Manager Portal	<p>Allows service providers to provision services for enterprise subscribers on routers running JunosE or Junos OS and allows IT managers to manage services.</p> <p>Enterprise Manager Portal can be used with NAT Address Management Portal to allow service providers to manage public IP addresses for use with NAT services on routers running Junos OS and to allow IT managers to make requests about public IP addresses through the Enterprise Manager Portal.</p>

Table 4: Descriptions of SRC Components (*continued*)

Component	Description
Monitoring Agent application	Integrates IP address managers, such as a DHCP server or a RADIUS server, into an SRC-managed network so that the SAE is notified about subscriber events. The Monitoring Agent application runs on a Solaris platform.
Residential service selection portals	Provides a framework for building Web applications that allow residential and enterprise subscribers to manage their own network services. It comes with several full-featured sample Web applications that are easy to customize and suitable for deployment. The Residential service selection portals run on a Solaris platform.
Sample enterprise service portal	Lets service providers supply an interface to their business customers for managing and provisioning services.

**Related Documentation**

- *SRC Product Description*



## CHAPTER 2

# Security Digital Certificates

- [Digital Certificates Overview on page 9](#)
- [Before You Use Digital Certificates on page 9](#)

## Digital Certificates Overview

---

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 routers running Junos OS.

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.

### Related Documentation

- [Before You Use Digital Certificates on page 9](#)
- [Commands to Manage Digital Certificates on page 21](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)
- [Viewing Information About Security Certificates \(SRC CLI\) on page 19](#)

## 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.

**Related  
Documentation**

- [Digital Certificates Overview on page 9](#)
- [Commands to Manage Digital Certificates on page 21](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)
- [Viewing Information About Security Certificates \(SRC CLI\) on page 19](#)

## PART 2

# Administration

- [Managing Digital Certificates on page 13](#)
- [Routine Monitoring on page 19](#)
- [Management Commands on page 21](#)



## CHAPTER 3

# Managing Digital Certificates

- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)
- [Removing a Certificate Request on page 16](#)
- [Removing a Certificate on page 16](#)

### Manually Obtaining Digital Certificates (SRC CLI)

---

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 \(SRC CLI\)” on page 14](#).

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 Documentation

- [Before You Use Digital Certificates on page 9](#)
- [Removing a Certificate Request on page 16](#)
- [Digital Certificates Overview on page 9](#)
- [Commands to Manage Digital Certificates on page 21](#)

---

## Obtaining Digital Certificates through SCEP (SRC CLI)

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 \(SRC CLI\)” on page 13](#).

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

**Related  
Documentation**

- [Before You Use Digital Certificates on page 9](#)
- [Removing a Certificate Request on page 16](#)
- [Digital Certificates Overview on page 9](#)
- [Commands to Manage Digital Certificates on page 21](#)

---

## 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
```

**Related  
Documentation**

- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)

---

## 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 CAcert 1
```

**Related  
Documentation**

- [Removing a Certificate Request on page 16](#)
- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)

- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)



## CHAPTER 4

# Routine Monitoring

- [Viewing Information About Security Certificates \(SRC CLI\) on page 19](#)
- [Viewing Information About Security Certificates \(C-Web Interface\) on page 19](#)

### Viewing Information About Security Certificates (SRC CLI)

---

**Purpose** View information about security certificates that reside on the system.

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

**Meaning** If no security certificates reside on the system, the CLI return a message to that effect:

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

For information about managing security digital certificates, see [“Digital Certificates Overview” on page 9](#)

**Related Documentation** • [Viewing Information About Security Certificates \(C-Web Interface\) on page 19](#)

### Viewing Information About Security Certificates (C-Web Interface)

---

**Purpose** View messages generated during SRC software startup.

**Action** 1. Click **Monitor>Security>Certificate**.  
The Certificate pane appears.



2. To display authority certificates, select the **Trusted** check box.

3. Click **OK**.

The Certificate pane displays the security certificates.

For information about managing security digital certificates, see [“Digital Certificates Overview” on page 9](#)

#### Related Documentation

- [Viewing Information About Security Certificates \(SRC CLI\) on page 19](#)

## CHAPTER 5

# Management Commands

- [Commands to Manage Digital Certificates on page 21](#)

## 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**

### Related Documentation

- [Manually Obtaining Digital Certificates \(SRC CLI\) on page 13](#)
- [Obtaining Digital Certificates through SCEP \(SRC CLI\) on page 14](#)
- For detailed information about each command, see the *SRC PE CLI Command Reference*



## PART 3

# Index

- [Index on page 25](#)



# Index

## B

BEEP TLS connections.....9

## C

conventions

notice icons.....viii

text.....viii

customer support.....x

contacting JTAC.....x

## D

digital certificates. *See* security

directory

description.....4

directory server.....4

documentation

comments on.....ix

## H

HTTPS connections.....9

## L

LDAP (Lightweight Directory Access Protocol). *See*  
directory; directory server

## M

manuals

comments on.....ix

## N

notice icons.....viii

## S

security

digital certificates.....9

clearing certificates.....16, 21

clearing requests.....16

prerequisites.....9

requesting certificates.....13, 21

requesting certificates through SCEP.....14

viewing certificates.....21

security certificates

information, viewing

C-Web interface.....19

SRC CLI.....19

SRC components

description.....3

support, technical *See* technical support

## T

technical support

contacting JTAC.....x

text conventions.....viii

