

# JUNIPER NETWORKS STRM TECHNICAL NOTE

## USING A TRUSTED CERTIFICATE

February 2008

By default, STRM provides an untrusted SSL certificate. You can replace the untrusted SSL certificate with a trusted certificate. This document provides information for replacing the untrusted SSL certificate with a trusted certificate.



**Note:** You cannot replace the provided certificate with another untrusted (self-signed) certificate.

To replace the SSL certificate on your Console:

**Step 1** Obtain a trusted certificate from your certificate authority.



**Note:** Make sure the Administration Console is closed while performing the below procedure.

**Step 2** Log in to your system, as root.

**Step 3** Copy the obtained certificates to your system:

```
cd <directory>
cp <private key filename> /etc/httpd/conf/certs/cert.key
cp <public key filename> /etc/httpd/conf/certs/cert.cert
```

Where:

<directory> indicates the directory used to generate the certificate.

<private key filename> indicates the name of the private key file. The private key file must be named cert.key.

<public key filename> indicates the name of the public key file. The public key file must be named cert.cert.

**Step 4** If you require an intermediate certificate:

a Obtain the intermediate certificate from your certificate authority.

b Copy the certificate to the following:

```
/etc/httpd/conf/certs/intermediate.ctr
```

c Open the following file:

```
/etc/httpd/conf.d/ssl.conf
```

d Locate the following line:

- ```
#SSLCACertificateFile /usr/share/ssl/certs/ca-bundle.ctr
```
- e Replace the line with the following:
- ```
SSLCACertificateFile /etc/httpd/conf/certs/intermediate.ctr
```
- f Save and exit the file.

For more information on installing an intermediate certificate, see the documentation from your certificate authority.

- Step 5** Enter the following command:

```
/opt/qradar/bin/install_ssl_cert.sh /etc/httpd/conf/certs/cert.cert
```

The following message appears:

```
Installing a new SSL certificate in the QRadar system ...
  Changing the SSL certificate configuration variable...
  Restarting the Apache
Shutting down httpd
Starting httpd
  Restarting HostContext
[Q]Shutting down hostcontext service
[Q]Shutting hostcontext service
Successfully done.
```

- Step 6** Restart the host context process on all non-Console systems in your deployment:

```
service hostcontext restart
```

**Juniper Networks, Inc.**  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA

Copyright © 2008 Juniper Networks, Inc. All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Part Number 530-023923-01