

JUNIPER NETWORKS STRM TECHNICAL NOTE

USING A TRUSTED CERTIFICATE

June 2008

By default, STRM and STRM Log Management provide an untrusted SSL certificate. You can replace the untrusted SSL certificate with a trusted certificate. This document provides the following information:

- [Understanding SSL Certificates](#)
- [Replacing the Untrusted SSL Certificate](#)

Understanding SSL Certificates

Secure Sockets Layer (SSL) is the transaction security protocol used by web sites to provide an encrypted link between a web server and a browser. SSL is an industry standard and is used by web sites to protect online transactions. To be able to generate an SSL link, a web server requires an SSL certificate. SSL certificates are issued by:

- Software - This generally available software, such as Open SSL or Microsoft's Certificate Services manager, issues SSL certificates known as self-signed certificates. Self-signed certificates are not inherently trusted by browsers and although they can be used for encrypting data, there is no third-party verification process used to identify the server sending the certificate. They cause browsers to display warning messages that inform the user that the certificate has not been issued by an entity that the user has chosen to trust.
- Trusted third-party certifying authorities - These certification authorities, such as VeriSign or Thawte, use their trusted position to issue trusted SSL certificates. SSL certificates issued by trusted certification authorities do not display a warning and transparently establish a secure link between a web site and a browser.

Browsers and operating systems include a pre-installed list of trusted certification authorities, known as the Trusted Root CA store. As Microsoft and Netscape provide the major operating systems and browsers, they elect whether or not to include the certification authority into the Trusted Root CA store, thereby giving the certification authority its trusted status. STRM supports any trusted certificate where their Trusted Root CA is in the browser and java keystores.

Replacing the Untrusted SSL Certificate

You can replace the untrusted SSL certificate provided with your STRM or STRM Log Management with a certificate issued by a trusted third-party certifying authority.



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



Note: SSL certificates issued from VeriSign require an intermediate certificate. You must download the intermediate certificate from VeriSign and use it during the configuration.

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:



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

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
```

Copyright Notice

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 530-025617-01