

TECHNICAL NOTE

USING A TRUSTED CERTIFICATE

OCTOBER 2009

By default, STRM and STRMLM provide a Self signed 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. These certificates are not inherently trusted by browsers, because they are not issued by a recognized authority. Although they can be used for encrypting data, there is no third-party assurance regarding the identity of 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 Mozilla 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. Java Runtime Environment provides a set of trusted certificated authorities, as selected by Sun Microsystems. For the purpose of establishing SSL connections between STRM components, and between the browser and Console, STRM will trust any certificate that is issued, directly or indirectly, from a trusted root CA in the browser and Java keystore.

Replacing the Untrusted SSL Certificate



You can replace the untrusted SSL certificate provided with your STRM or STRMLM 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 some vendors, such as VeriSign, require an intermediate certificate. You must download the intermediate certificate from the vendor and use it during the configuration.

To replace the SSL certificate on your Console:

- Step 1** Obtain a certificate from a trusted certificate authority.
- Step 2** Log in to your system, as root.
- Step 3** Choose one of the following options:
- If you require an intermediate certificate, see [Step 4](#).
 - If you do not require an intermediate certificate, see [Step 5](#).
- Step 4** If you require an intermediate certificate, follow the below procedure.
- a Enter the following command:
- ```
/opt/qradar/bin/install_ssl_cert.sh -i
```
- The following message and prompt appears:
- ```
This script installs a new SSL certificate
Path to private key file (SSLCertificateKeyFile):
```
- b** At the **Path to private key file** prompt, enter the directory path for your private key file. Press **Enter**.
- The following prompt appears:
- ```
Path to public key file (SSLCertificateFile):
```
- c** At the **Path to public key file** prompt, enter the directory path for your public key file. Press **Enter**.
- The following prompt appears:
- ```
Path to SSL intermediate certificate file
(SSLCACertificateFile - optional):
```
- d** At the **Path to SSL intermediate certificate file** prompt, enter the directory path for your intermediate certificate. Press **Enter**.
- The following messages and prompt appears:
- ```
You have specified the following:
SSLCertificateKeyFile of '<private certificate directory
path>'
SSLCertificateFile of '<public certificate directory path>'
SSLCACertificateFile of '<intermediate certificate directory
path>'
```

Continue and reconfigure Apache now (includes restart of httpd daemon) (Y/[N])?

- e At the prompt, enter `y` to continue. Press **Enter**.

The following messages appear.

```
Changing the SSL certificate configuration variable ...
Restarting Apache
Stopping httpd: [OK]
Starting httpd: [OK]
Restarting HostContext
[Q] Shutting down hostcontext service: [OK]
[Q] Starting hostcontext service: [OK]
Successfully done.
```

Go to [Step 6](#).

- Step 5** If you do not require an intermediate certificate, follow the below procedure:

- a Enter the following command:

```
/opt/gradar/bin/install_ssl_cert.sh -b
```

The following message and prompt appears:

```
This script installs a new SSL certificate
Path to private key file (SSLCertificateKeyFile):
```

- b At the `Path to private key file` prompt, enter the directory path for your private key file. Press **Enter**.

The following prompt appears:

```
Path to public key file (SSLCertificateFile):
```

- c At the `Path to public key file` prompt, enter the directory path for your public key file. Press **Enter**.

The following messages and prompt appears:

```
You have specified the following:
SSLCertificateKeyFile of '<private certificate directory
path>'
SSLCertificateFile of '<public certificate directory path>'
Continue and reconfigure Apache now (includes restart of httpd
daemon) (Y/[N])?
```

- d At the prompt, enter `y` to continue. Press **Enter**.

The following messages appear.

```
Changing the SSL certificate configuration variable ...
Restarting Apache
Stopping httpd: [OK]
Starting httpd: [OK]
Restarting HostContext
[Q] Shutting down hostcontext service: [OK]
[Q] Starting hostcontext service: [OK]
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.

Published: 2009-10-12