

Configuring Secure Connections Between the SAE and JUNOS Routing Platforms

You can use TLS to protect communication between the SAE and JUNOS routing platforms.

To complete the handshaking protocol for the TLS connection, the client (JUNOS routing platform) and the server (SAE) must exchange and verify certificates. You need to create a client certificate and a server certificate. Both certificates must be signed by a certificate authority (CA). JUNOS software supports VeriSign, Inc. (<http://www.verisign.com>). You must then install both certificates on the SAE and on the JUNOS routing platform.

You can use the C-Web interface 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 Topics**
- Configuring Secure Connections Between the SAE and JUNOS Routing Platforms
 - Configuring the SAE to Manage JUNOS Routing Platforms (C-Web Interface)
 - Configuring the SAE to Use TLS
 - Adding the Server Certificate on the Routing Platform
 - Creating a Client Certificate for the Router

Published: 2009-09-18