



Knowledge Base Article #PG728

Importing a Customer Certificate for the PolicyGuru® Solution Web Interface

Overview

By default, the PolicyGuru® Solution uses a self-signed certificate for the web interface. The certificate and key are found in the `/opt/ngp/config/security/server.p12` truststore. This is identified in `/opt/ngp/jboss-as-7.2.0.Final/standalone/configuration/standalone-full.xml` in this section:

```
<subsystem xmlns="urn:jboss:domain:web:1.4" default-virtual-server="default-host" native="false">
    <connector name="http" protocol="HTTP/1.1" scheme="http" socket-binding="http" redirect-port="8443"/>
    <connector name="https" protocol="HTTP/1.1" scheme="https" socket-binding="https" secure="true">
        <ssl key-alias="<alias>"
password="<password_used_to_create_the_truststore>" certificate-key-file="/opt/ngp/config/security/server.p12" protocol="TLSv1" verify-client="false" ca-certificate-file="/opt/ngp/config/security/server.p12" ca-certificate-password="<password_used_to_create_the_certificate>" keystore-type="PKCS12" truststore-type="PKCS12"/>
```

You can import a customer certificate to use instead of the default self-signed certificate, as long as the following requirements are met:

- The PolicyGuru Solution requires TLSv1 as the protocol.
- The keystore type must be PKCS12, and the key and certificate must be in the same file, because this is what the application providing the webserver supports.

You can use the **openssl** tool to convert the certificate to meet these requirements if it is in another format such as PEM.

The PolicyGuru Mediation Server uses **JBoss** middleware to provide the web interface functionality, including use of a certificate. Customer-provided certificates can be imported using standard **JBoss** procedures. This document describes one way to accomplish that goal.

The instructions below describe how to import a customer certificate that meets these requirements using the existing truststore name and values that are referenced in the **standalone-full.xml** file. You can choose to create a new truststore and use different values for the alias and use different passwords. If you do, update the corresponding entries in the **standalone-full.xml** file.

Importing the Certificate

To import a customer certificate

1. Stop the **ngp** service on the Mediation Server:

```
service ngp stop 5
```
2. SSH to the Mediation Server and **cd /opt/ngp/config/security/**
3. Make a backup copy of **server.p12**.



Knowledge Base Article #PG728

4. Copy the customer certificate file and private key file to the Mediation Server. The instructions below assume they are placed in **cd /opt/ngp/config/security/**. If you place them elsewhere, such as in **tmp**, use the full path in the conversion and import command.

5. Convert and import the certificate into the **server.p12** truststore:

```
openssl pkcs12 -export -out server.p12 -name <alias> -inkey  
<privateKey>.key -in <certificate>.crt
```

Where **<privateKey>.key** is the name of the private key file, **<alias>** is the alias from the **standalone-full.xml** file, and **<certificate>.crt** is the name of the certificate file. Do not include the angle brackets in the command.

6. Use the following command to view and verify the contents of the truststore:

```
keytool -list -v -storetype pkcs12 -keystore server.p12
```

7. Verify that the alias and password values in **standalone-full.xml** match the passwords used to create the key and certificate.

8. Start the **ngp** service:

```
service ngp start
```

9. Log in via the web interface to verify that the new certificate allows access.

Last Update: 5/1/2017



SecureLogix Corporation

13750 San Pedro, Suite 820 • San Antonio, Texas 78232
(210) 402-9669 • www.securelogix.com

Support (877) SLC-4HELP • EMAIL support@securelogix.com • <http://support.securelogix.com>

ETM, We See Your Voice, SecureLogix, SecureLogix Corporation, the SecureLogix Emblem, and the SecureLogix Diamond Emblem are registered trademarks or registered trademarks and registered service marks of SecureLogix Corporation in the U.S.A. and other countries. PolicyGuru is a registered trademark of SecureLogix Corporation in the U.S.A. All other trademarks mentioned herein are believed to be trademarks of their respective owners.

© Copyright 2015 SecureLogix Corporation. All Rights Reserved. This product is protected by one or more of the following patents:
US 6,249,575 B1, US 6,320,948 B1, US 6,687,353 B1, US 6,718,024 B1, US 6,760,420 B2, US 6,760,421 B2, US 7,133,511 B2,
US 7,231,027 B2, US 7,440,558 B2, US 8,150,013 B2, CA 2,354,149, DE 1,415,459 B1, FR 1,415,459 B1, and GB 1,415,459 B1.