Install a Signed SSL Certificate on a CSPC

Contents

Introduction

Prerequisites

Requirements

Configure

Components Used

Configurations

Import the files into the CSPC

Install

Verify

Troubleshoot

Introduction

This document describes how to install SSL certificates signed by you or a Certificate Authority (CA) in the CSPC.

Prerequisites

Requirements

- .key file (Generated while creating the csr file for you or a CA to sign)
- .crt file (This is the certificate which matches the .key file and is signed by you or CA)
- Root access to CSPC

Tip: Alternatively to the .crt file, you can provide .cer files. These can be converted to .crt files to be installed.

Configure

Components Used

- CSPC (tested versions include 2.7.x 2.8.x 2.9.x and 2.10.x)
- FTP client (such as WinSCP, Filezilla, MobaXterm, and so on.)

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configurations

Import the files into the CSPC

1. Using an FTP client, import the .crt and .key files into **/home/collectorogin**.
1.1 If you have been provided a .cer, convert the file to .crt. (Replace <name> with the name of your file).
openssl x509 -inform DER -in <name>.cer -out localhost.crt

```
openssl x509 -inform DER -in <name>.cer -out rui.crt
```

If the previous command gives an error (like unable to load certificate), which could happen in some cases, then use this command. It cannot prompt the error.

```
openssl x509 -in <name>.cer -out rui.crt
```

Install

2. Create the keystore.

```
openssl pkcs12 -export -in localhost.crt -inkey localhost.key > localhost.p12
```

3. Import to CSPC's keystore.

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -importkeystore -srckeystore localhos
```

Note: It asks for the password. It is always **cspcgxt**.

4. Verify it has been imported (two entries are present).

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore $CSPCHOME/webui/to
```

5. Delete the previous alias.

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -delete -alias tomcat -keystore $CSPC
```

6. Verify there is only one alias present

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -list -v -keystore $CSPCHOME/webui/to
```

7. Change the alias to tomcat.

```
/opt/cisco/ss/adminshell/applications/CSPC/jreinstall/bin/keytool -changealias -alias 1 -destalias tomca
```

8. Restart CSPC services.

For versions 2.7.x and 2.8.x:

```
service cspc restart
```

For versions 2.9.x and 2.10.x:

```
systemctl cspc restart
```

⚠ **Caution**: Save the .key and .crt files as upgrades to the CSPC can remove the SSL certificate and re-installation is required.

Verify

Navigate to the **CSPC log in screen** and select the lock on the left of the address bar and inspect the certificate.

Troubleshoot

Upon restarting, versions 2.9.x and 2.10.x have been reported to have issues with Tomcat. If GUI doesnt come up:
1. Confirm that tomcat services are up after restart:

```
service tomcat status
```

2. If the message shows **Active: activating (start)**, wait for five to ten minutes as service is coming up. Otherwise, start it manually:

```
service tomcat start
```

🔍 **Tip**: If you are still facing issues, please contact a lead or share in the comments.