SSL Certificate How To Guide

Contents

Overview

Swivel Appliances (Virtual and Hardware) ship with a self-signed certificate which prompts users to accept a security warning when the TURing image is presented within a web browser. When a Swivel server goes into production, then a valid signed certificate from a trusted certificate authority should be installed onto the Appliance. This article describes how to install a valid certificate using the Swivel Appliance's CMI menu.

A certificate request can be made from the Swivel virtual or hardware appliance or an existing certificate can be used by importing the private AND the public key.

Applying for certificates may take some time so we advise that renewals are carried out in good time before current certificates expire.

Prerequisites

- Swivel Appliance with version 3.x with Console Management Interface (CMI)
- DNS name for the Swivel instance, usually the public IP address
- Configuration of the Swivel Appliance for basic settings
- Certificate Authority to sign a Certificate Signing Request (CSR)
- Please read and understand these instructions before attempting to install a certificate

Considerations

HA Appliances using a VIP

For HA Appliances, if a VIP (Virtual IP) is being is used then the certificate must to be bound to a hostname that is used on both Swivel servers. When you've setup a signed certificate on one Appliance then the keystore can be copied to the other Appliance.

NAT Address and Certificates

Where the Swivel Appliance or HA VIP is behind a NAT, the DNS entry used as for the IP address of the NAT is usually used as the hostname for the certificate and with a Swivel HA VIP, that certificate is imported into the Standby Appliance by transferring the /home/swivel/.keystore file - see below for details.

Webmin

The other Appliance web based interface known as Webmin uses a separate certificate for SSL communications. Since this is rarely used and then only for administrative purposes by trained administrators, the built-in self-signed certificate is utilised.

Keystore and Connector Ports

The keystore used by each port is defined as a Connector element within the Tomcat server.xml file. You can view this file from Webmin (https://<Swivel_server>:10000). Go to Servers -> Swivel and select "Edit Tomcat config file". There should be 3 "<Connector ..." entries, one each for ports 8080, 8443 and 8181 (the last is for internal use only). The entries for port="8080" and "8443" should both have the same value for keystoreFile, which should be "/home/swivel/.keystore". If one of these is different, it needs to be changed.

Import with .PFX format

When you request the SSL Certificate from the trusted Certificate Authority (CA) in a .pfx format, then it is vital that you include the private key. Also, it is recommended that you choose to include the certificates in the certification path.

You will prompted to enter a password for the .pfx file and we recommend that you use the password "lockbox" as this is the password that is currently set on the Swivel Appliance.

The .pfx file must be converted into a .jks format in order for it to be imported into the Swivel Server. Therefore, we recommend that you download the following tool which allows you to inspect keystore files and this case, convert the .pfx to a .jks file:

Keystore Explorer

1. Open an Exisiting Keystore and when prompted, enter the password which comes with the file (which should have been set to "lockbox").

2. Rename the file to "swivel" by right clicking on the file and "Rename".

3. Navigate to Tools > Change Format and select JKS.

4. The password will need updating for the keystore and the certificate. Under Tools > Set Password and enter "lockbox". Also, right click on the certificate and Set Password to "lockbox".

5. File > Save As.. ".keystore"

You must take a copy of the existing .keystore which is located under /home/swivel or perform a Backup under Backup & Restore on the CMI.

6. Using WinSCP, copy the new .keystore to /home/swivel

7. Restart Tomcat

8. Confirm that the certificate has been updated by navigating to https://<hostname:8443/proxy/SCImage?username=test (Replace <hostname> with the actual hostname for the Swivel Appliance.

Note: If you are running a HA Pair, then you only have to carry out the above steps on one server (i.e Primary) and then simply copy and replace the .keystore to the Standby.

You must ensure that the permissions are set correctly for the .keystore file. The owner and group must be "swivel" and the permissions must be 0640.

Import with a .CRT format

Once you have created the Local Certificate and generated a CSR from the Swivel Appliance and send it off to the Certificate Authority, you will receive Intermediate(s), Root and Response certificates from your trusted Certificate Authority.

Note: GoDaddy are known to provide the Root and Response certificates only as most web browsers include GoDaddy as a Trusted CA so the browser will complete the certificate chain. However, this has been known to cause issues with Mobile Provisioning and Certificate Warning messsages - please see Known Issues

1. Using an SFTP client such as WinSCP, copy the certificates to /backups/upload.

2. From the CMI, navigate to Tomcat > Certificates.

3. You must install the Intermediate certificate(s) first. Select Import New / Existing Alias > Import to New Alias and choose the Intermediate from the list. Then give it an alias such as "inter".

4. After the Intermediate(s) have been added to the keystore, you will remain on the same screen so you should select the Root certificate and give it an alias, such as "root".

5. Go back to the Import Menu and select Import to Existing Alias and select the Response (Reply) certificate. Next, you MUST choose the "swivel" alias.

6. Navigate to the Swivel Admin Console and click the padlock on the Address Bar and confirm that the certificate has been installed, the correct expiry date appears and you can see the full certificate path. Please be aware that you will see a Certificate Warning message if you are connecting to the Swivel Server via an IP address as opposed to a hostname.

If you are running a HA pair, then you can take a copy of the .keystore file that is located under /home/swivel and copy it onto the Standby Server, under /backups/upload. Use the certificate import menu as described above to import the new keystore. Finally, confirm that the certificate has been updated on the Standby Server via the Web (Swivel Admin Console).

How to Change Keystore Password

From the CMI, you must navigate to Tomcat > Certificates > Change Keystore Password.

If this option is not available, then you must update the Appliance by navigating to Administration > Update Appliance > Update Appliance.

Known Issues

GoDaddy and Comodo issue the Root and Response certificates only, without any intermediates as GoDaddy are known as a Trusted CA to most web browsers therefore the browser completes the certificate chain as it has a repository of certificates for a variety of Trusted CA's. However, due the intermediate(s) being missing, it can cause issues with Mobile Provisioning and cause Certificate Warning messages. Therefore, you must retrieve the "Go Daddy Class 2 Certification Authority" and "Go Daddy Root Certificate Authority - G2" and import them onto the Swivel Appliance.

Comodo only provide the Response certificate and the above steps must be followed. To confirm which certificates are required, click on the padlock icon in the Address Bar and view the Certificate Path.

Mozilla Firefox:

From Firefox you can navigate to Tools > Options > Advanced > Certificates > View Certificates > Authorities (tab) - then search for the Go Daddy certificates.

Google Chrome:

You can view these within Google Chrome,under Settings > Show Advanced Settings > HTTPS/SSL (Manage Certificates) > Trusted Root Certification Authorities.