Note: To replace an expiring SSL certificate, replace the sign.crt, sign.key, gd_bundle.crt and nginx.crt in the **/usr/local/nukona/certs/configurator/** with the new ones and restart the appcenter-services.

1. Transfer the new certificate files the Mobility front-end (FE); renaming them as necessary to match the names below. If the SSL certificate provided by the certificate authority (CA) is in PFX (PKCS personal exchange) follow HOWTO106999 to extract the required certificates.

   /usr/local/nukona/certs/configurator/sign.crt
   Note: This is the PEM formatted public SSL certificate.

   /usr/local/nukona/certs/configurator/sign.key
   Note: This is the key file used to generate the certificate signing request (CSR) for the public SSL certificate and must not contain a password.

   /usr/local/nukona/certs/configurator/gd_bundle.crt
   Note: This contains a PEM formatted certificate chain, most often is just the issuing CA certificate.

2. Create the nginx.crt file using the following commands, as root:

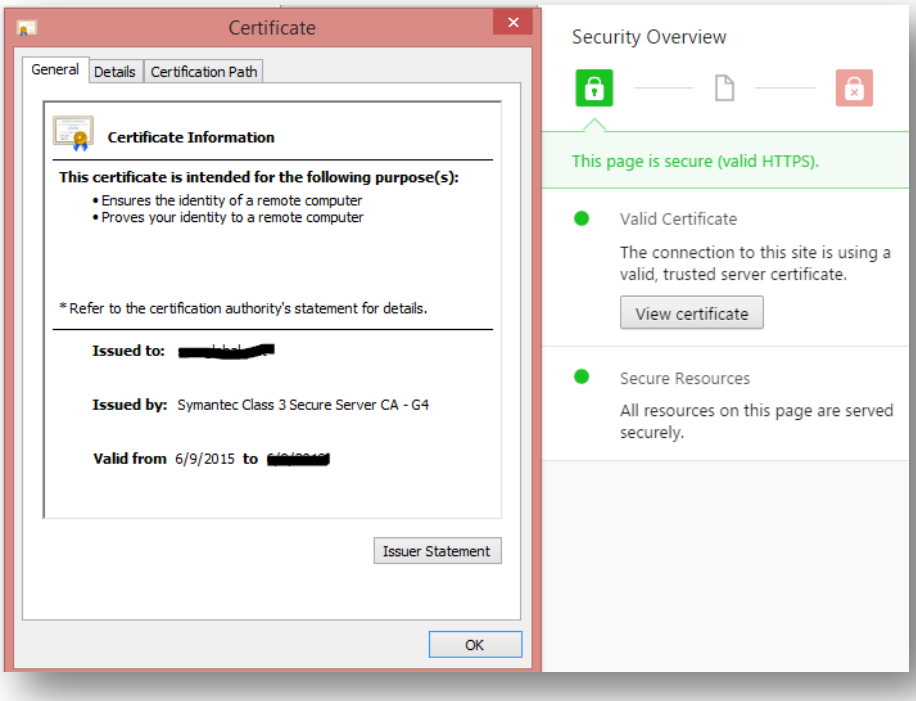
   a. copy the **sign.crt** and name the copied file **nginx.crt** using the following command:
      cp /usr/local/nukona/certs/configurator/sign.crt /usr/local/nukona/certs/configurator/nginx.crt
   b. Append the **nginx.crt** with the ssl chain from the **gd_bundle.crt** file using the following command:
      cat /usr/local/nukona/certs/configurator/gd_bundle.crt >> /usr/local/nukona/certs/configurator/nginx.crt
   c. Change the owner to **nginx** using the following command:
      chown nginx:nginx /usr/local/nukona/certs/configurator/nginx.crt

      Note: The nginx.crt file contains the PEM public formatted SSL certificate and certificate chain. This is created by taking the sign.crt file and appending the gd_bundle.crt thereto.

3. Enter the following, as root, from the FE:
   /etc/init.d/appcenter-services restart

4. Repeat the above for each FE in the environment.

5. Verify that the updated certificate is being used by navigating to the Mobility server's FQDN (Fully Qualified Domain Name) and click on the **https** symbol in the address bar. Click view details about the connection and finally click **View certificate:**


Certificate
General
Details
Certification Path
Certificate Information
This certificate is intended for the following purpose(s):
• Ensures the identity of a remote computer
• Proves your identity to a remote computer
* Refer to the certification authority's statement for details.
Issued to:
Issued by: Symantec Class 3 Secure Server CA - G4
Valid from 6/9/2015 to
Issuer Statement
OK
Security Overview
This page is secure (valid HTTPS).
Valid Certificate
The connection to this site is using a valid, trusted server certificate.
View certificate
Secure Resources
All resources on this page are served securely.