FortiNAC - Installing SSL Certificates

Version F 7.2.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 21, 2023
FortiNAC F 7.2.0 Installing SSL Certificates
49-922-769106-20211216

TABLE OF CONTENTS

Overview

This document provides the steps to install SSL certificates in a single FortiNAC appliance using the Administration UI.For other configurations, refer to the applicable document below:

- Install SSL Certificates Using the Admin UI (Single Appliance)
- Install SSL Certificates Using the Admin UI (Appliances managed by Manager)

Certificate Targets

SSL certificates are required in order to secure FortiNAC communications.The following are secured using a similar procedure via the Administration UI:

- Admin UI
- Captive Portal
- FortiNAC agents
- Local RADIUS Server (FortiNAC version 8.8 and above)
  - Local RADIUS Server (EAP)
  - RADIUS Endpoint Trust (EAP-TLS)

See Keystore for SSL/TLS Communications in Appendix for instructions for the following.

- LDAP servers
- FortiClient EMS integrations
- Nozomi systems integrations

Considerations

- User needs to already have determined FortiNAC hostnames, which will be secured by the certificates (certificates required on all FortiNAC appliances)
- Hostname used for the Portal can be different than the actual hostname of the appliance.This is beneficial when using a combination of internal and external certificates. Setting the Portal hostname differently also prevents revealing the actual appliance hostname to users interacting with the Portal.

Certificate Formats Types and Templates

- Acceptable certificate formats: PEM, DER, PKCS#7/P7B
- Required format when installing certificates via CLI*: PEM
- Local domain certificates: Use Web Service template

- Public certificates: Use Apache Mod or similar
  *If conversion is required, see Appendix section SSL File Conversion Tool Chart.

Procedure Overview

Step 1: Determine FortiNAC Certificate Targets to Secure

Step 2: Obtain a Valid SSL Certificate from a Certificate Authority (CA)

Step 3: Upload the Certificates to FortiNAC

Step 4: Activate Portal Certificates

Required when securing the Captive Portal.

Step 5: Configure Certificate Expiration Warning Alarms

Create alarms to notify when FortiNAC's SSL Certificate is approaching its expiration date.

Step 6: Apply Certificates to Secondary Server (High Availability configurations)

- Option 1: Admin UI Method – Requires a failover to the Secondary Server. A maintenance window may be required.
- Option 2: CLI Method – A maintenance window is not required.

Step 1: Determine FortiNAC Certificate Targets to Secure

SSL certificates can be installed in one or more Certificate Targets in FortiNAC. Determine use cases so the appropriate certificates can be acquired. Different certificates can be installed for different targets. Not all targets may be used.

Refer to the Deployment Guide (Create and Install SSL Certificates) for details on specific use cases.

SSL Certificates can be issued from the following Certificate Authorities (CA):

- Corporate Owned Internal CA (Internal)
  - Certificates issued from within the organization. You may act as your own Certificate Authority (CA) and use your own internal certificate, as long as all systems in your domain use the same certificate.
  - Certificate types: Individual & SAN (Subject Alternative Name)*
- Third party public (External)
  - Certificates issued from Certificate Authorities like GoDaddy, DigiCert, GlobalSign, etc.
  - Certificate types: Individual, SAN* & Wildcard

* SAN certificates can be used to secure multiple host names and/or IP addresses. For example, in a Layer 2 HA environment the virtual, Primary, and Secondary appliance host names and their corresponding IP addresses can all be secured with one certificate.

Certificate Target	Function	Certificate to Use
Admin UI	Access to the FortiNAC UI (https://<FortiNAC FQDN>:8443/)	Internal or External
Persistent Agent	Persistent Agent communication	Internal (Recommended) or External
Portal	Captive Portal access and Dissolvable Agent communication	External
Local RADIUS Server (EAP)	For use when FortiNAC is acting as the 802.1x EAP termination point.	Internal or External (avoid wildcard certificates)
RADIUS Endpoint Trust	Client-side certificate validation (EAP-TLS)	Internal or External (avoid wildcard certificates)

Step 2: Obtain a Valid SSL Certificate

A Certificate Signing Request (CSR) is issued and submitted to the Certificate Authority (examples are GoDaddy, DigiCert and GlobalSign). Depending upon the type of certificate, the CSR may be generated in FortiNAC, or from another source. The CA then issues the certificates based on the CSR.

Note: FortiNAC does not have the ability to issue certificates.

If a certificate has already been generated, skip this step and proceed to section Upload the Certificate Received from the CA.

To generate a CSR:

1. Navigate to **System > Certificate Management.**
2. Click **Generate CSR**.
3. Select the certificate target to generate the CSR. This will be the same target in which the resulting certificate files will be installed.

Certificate Target	**Admin UI**: Generates CSR for the Administration User Interface. **Local RADIUS Server (EAP)**: For use when FortiNAC is acting as the 802.1x EAP termination point. For details see Local RADIUS Server. **Persistent Agent**: Generates CSR for Communications between FortiNAC and the Persistent Agent. **Portal**: Generates a CSR to secure the Captive Portal and Dissolvable Agent communications. **RADIUS Endpoint Trust**: Endpoint Trust Certificate used by FortiNAC to validate the client-side certificate when Local RADIUS Server is configured and EAP-TLS is used for authentication. For details see section Local RADIUS Server of the Administration Guide in the Fortinet Document Library.

4. Enter the **Common Name (Fully-Qualified Host Name).** This is the Host Name to be secured by the certificate. If generating a wildcard CSR, enter the desired domain specifying the wildcard in the Common Name Field (e.g. *.Fortinetnetworks.com).
5. Whether or not you are securing a single name or multiple names, enter the Common Name in the **Subject Alternative Name** list with any other SANs. Some browsers only check the SAN list and no longer check the CN for name comparison.
6. Enter the remaining information for the certificate in the dialog box.
7. Click **OK** to generate the CSR.

   Note: The Private Key that corresponds with the CSR is stored on the appliance. Once the SSL Certificate is uploaded, to view the Private Key, click the Details button and select the Private Key tab.
8. Copy **ALL** the text, even **including** “----BEGIN CERTIFICATE REQUEST-----” and “-----END CERTIFICATE REQUEST-----”

9. Paste it into a text file, and save the file with a .txt extension. Note the location of this file on your PC.

   Important: Make sure there are no spaces, characters or carriage returns added to the Certificate Request.

10. Click **Close** to exit the "Certificate Generated" screen.

11. Send the Certificate Request file to the CA to request a Valid SSL Certificate. Note the following before submitting:

    - **Acceptable certificate formats:** PEM, DER, PKCS#7/P7B
    - **Required format when installing certificates via CLI***: PEM
    - **Local domain certificates**: Use Web Service template
    - **Public certificates**: Use Apache Mod or similar
    - **Agent versions prior to 3.1.5 are not compatible with SHA2.** Contact Support to verify appropriate SHA version based on current deployment.
    - **Do not generate a new CSR for the same target after submitting request to CA**. Generating more than one certificate request for a single target will overwrite the previous private key stored in the temporary location with a new private key. Certificates obtained using the initial certificate request would then be invalid as the private key no longer matches.

*If conversion is required, see Appendix section SSL File Conversion Tool Chart.

Step 3: Upload the Certificate to FortiNAC

Once the certificates are received from the CA, upload them to the applicable FortiNAC certificate targets (Admin UI, Captive Portal, Persistent Agent, RADIUS).

- If the certificate files were a result of a CSR generated by FortiNAC, the files must be installed on FortiNAC for the target used to generate the CSR.
- If the Certificate was generated elsewhere, then a private key must be provided with the certificate. Important: The private key cannot be password protected and must be in RSA format. To verify, see related KB article Convert SSL private key to RSA format.

  Tip: If using the same certificate for multiple targets (Admin UI, Portal, Persistent Agent, etc), first install certificate in a target that’s easy to validate (such as the Admin UI). Once validated, the files can be copied to the other targets.

Upload the valid SSL certificate to the appliance when the certificate file is returned from the CA. Certificate files can be returned to you in one of several configurations. Depending upon the CA, one or multiple certificate files may be returned.

1. Save the file(s) received from the CA to your PC.
2. Select **System > Certificate Management.**
3. Click **Upload Certificate.**
4. Select the target where the certificate will be uploaded. If the certificate files were a result of a CSR generated by FortiNAC, the files must be installed on FortiNAC for the target used to generate the CSR.

   Admin UI

   Local RADIUS Server (EAP)

   Persistent Agent

   Portal

   RADIUS Endpoint Trust
5. For the Private Key, select the appropriate drop-down menu option:
   - Select **Use Private Key from Last Generated CSR** if the files received were due from generating a CSR in FortiNAC (certificate target must be the one used to generate CSR).
   - Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use. This option is for renewing an existing installed certificate.
   - Select **Upload Private Key** to upload a key stored outside FortiNAC. Click **Choose** to find and upload the private key.
6. Click the **+** button to find and select the certificate to be uploaded. Users can also upload CA certificates and CA bundles. **Note**: Repeatedly use the + button to add all the certificate files needed.

   Important: Upload any relevant intermediate certificate files needed for the creation of a complete certificate chain of authority. The Certificate Authority should be able to provide these files. Without a complete certificate chain of authority, the target functionality may produce error/warning messages.
7. Click **OK**.
8. If the Certificate was successfully installed, you will be prompted to restart the target’s services. **Note**: Only the service specific to the target is restarted. General FortiNAC operation is not interrupted.

   If unexpected behavior occurs, see Troubleshooting.

   Click **Restart**.

The browser will time out if the target is the Admin UI, though the certificate has been successfully installed. Log back in if that is the case.

9. Validate certificate is active. For example, if the certificate was installed in the Admin UI target, browse to the Administration UI

   ```
   https://<FortiNAC hostname secured by certificate>:8443
   ```

   Important: Ensure the name used in the URL is the one specified in the certificate.

   Examine the certificate details in the browser (such as the security lock icon or whichever method is offered by that browser).

   If not secure, verify all intermediate and root certificates were included. See related KB article Identify missing SSL certificates via administration UI.

   If unexpected behavior occurs, see Troubleshooting.

Copy Certificate to Other Targets

If the certificate is intended to be used for multiple targets, copy the certificate to the new target:

1. Highlight the target with the desired certificate installed.
2. Click **Copy Certificate**.
3. Select the new target from the drop-down menu.
4. Click **OK**.

Step 4: Activate Portal Certificate

Certificates for the Administration User Interface and Persistent Agent activate automatically upon installation. No further action is required.

To begin using the certificate when connecting to the Portal, do the following:

1. Navigate to **System > Settings**.
2. Expand the Security folder, and then click **Portal SSL**.
3. In the **SSL Mode** field, select Valid SSL Certificate.
4. Click **Save Settings**.

   If unexpected behavior occurs, see Troubleshooting.
5. Validate certificate is active. Browse to the Captive Portal and Examine the certificate details in the browser (such as the security lock icon or whichever method is offered by that browser).

   If not secure, verify all intermediate and root certificates were included. See related KB article Identify missing SSL certificates via administration UI.

   If unexpected behavior occurs, see Troubleshooting.

Step 5 (optional): Create Certificate Expiration Warning Alarms

Three events are enabled by default in FortiNAC:

- **Certificate Expiration Warning**: Generated when a certificate is due to expire within 30 days.
- **Certificate Expiration Warning (CRITICAL)**: Generated when a certificate is due to expire within 7 days.
- **Certificate Expired**: Generated when a certificate has expired.

You must create alarms to send emails when these events are generated. To create alarms, do the following:

1. Navigate to **Logs > Event to Alarm Mappings**.
2. Create one alarm for each event with the following settings:

   Select the **Notify Users** setting.

   Select the type of messaging (Email or SMS) and Admin group desired to be notified.

   Set the Trigger Rule to **One Event to One Alarm**.

   For detailed instructions on creating alarms, refer to section Add or Modify Alarm Mapping of the Administration Guide.

Step 6: Apply Certificates to Secondary Server

UI Method

Note: FortiNAC management processes are stopped twice using this method and may require a maintenance window.

1. Force a failover to the Secondary Server.

   a. Login to the Secondary Server CLI as root and run the following command:

   ```
   hsIsSlaveActive
   ```

   Ensure **slave is active** is returned. If **slave is inactive** is returned, do not proceed. Contact Support for assistance.

   Example:

   ```
   > hsIsSlaveActive

   Host myFortinac

   SQL version 5.6.39,

   slave is active
   ```

   b. Run the following commands to start tailing logs in the Secondary Server CLI:

   ```
   logs

   tail –F output.processManager | grep –i “Slave In Control”
   ```

   c. In a window, login to Primary Server CLI as root and run the following command to stop processes and force failover:

   ```
   shutdownNAC -kill
   ```

   After roughly 3-5 minutes, the failover should complete. The Secondary Server CLI should return **(Slave) Slave In Control Idle(false)** in the log.
2. Login to the Administration UI for the Secondary Server and install certificates using the steps in section Upload the Certificate to FortiNAC.
3. Once certificates are installed, restore control to the Primary Server. Click the **Resume Control** button in the **Summary** Dashboard panel. This will take several minutes to complete.

CLI Method

Note: This option does not require a maintenance window.

Once the certificate files are received from the CA, upload them to FortiNAC. The Certificate Authority will generally return:

- Certificate
- CA bundle containing any intermediate and root certificates to ensure authenticity of the certificate.

The certificate, the key, and bundle (containing only the intermediate and root certificates) must be in separate files.

Admin UI

1. Log into the Control Server as root. Copy the certificate files received from the CA to **/bsc/campusMgr**.
2. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle before proceeding. For instructions see KB article Create SSL Certificate Bundle with Files Returned from Certificate Authority).
3. Verify Private Key is in RSA format. Review the private key file using a text editor. Alternatively, if in Linux, the file can be viewed by running the command:

   ```
   cat <filename>
   ```

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   The Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):

   ```
   openssl rsa -in <old_file_name> -out <new_file>
   ```

   Complete SSL Certificate installation using the newly converted Private Key file.
4. Backup the existing .keystore file. Type

   ```
   cp /bsc/campusMgr/.keystore /bsc/campusMgr/.keystore.bak
   ```

5. Ensure the names of the files are the following:

   key = server.key

   certificate = server.crt

   bundle = server.ca-bundle
6. Import files to the keystore using the alias “tomcat”

   Type

   ```
   ImportCertificateWithKey -alias tomcat -cas <CA-Bundle> -key <Private-Key> -
   cert <Leaf-Certificate> -keystore /bsc/campusMgr/.keystore -v -force -import
   -storepass ^8Bradford%23
   ```

   Example

   ```
   ImportCertificateWithKey -alias tomcat -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass
   ^8Bradford%23
   ```

   "Successfully imported key and certificate chain" will display.
7. Activate Certificate by restarting the tomcat-admin service. Type

   ```
   service tomcat-admin restart
   ```

8. Validate certificate is active. Browse to the Administration UI

   ```
   https://<FortiNAC hostname secured by certificate>:8443
   ```

   Examine the certificate details in the browser (such as the security lock icon or whichever method is offered by that browser). Important: ensure the name used in the URL is the one specified in the certificate. If not secure, verify all intermediate and root certificates were included in server.ca-bundle If not secure, verify all intermediate and root certificates were included. See related KB article Identify missing SSL certificates via administration UI.

   If unexpected behavior occurs, see Troubleshooting.

Agent and Captive Portal

1. Log into the Application Server as root. Copy the key, leaf certificate and bundle files to **/bsc/siteConfiguration/apache_ssl**

   Note: If the same certificate files are used for the Admin UI, these files (server.key, server.crt and server.ca-bundle) can be copied from the Control Server. If using these files, proceed to step 5.
2. If several intermediate certificate files are received (as opposed to a single CA bundle), the files should be merged into a bundle. For instructions see KB article Create SSL Certificate Bundle with Files Returned from Certificate Authority).
3. Verify Private Key is in RSA format. Review the private key file using a text editor. Alternatively, if in Linux, the file can be viewed by running the command:

   cat <filename>

   Header should look like this: -----BEGIN RSA PRIVATE KEY-----

   If Key Header looks like this: -----BEGIN PRIVATE KEY-----

   The Key is not in the correct format and needs to be converted. Covert the file by running the following command (on a Linux server):

   ```
   openssl rsa -in <old_file_name> -out <new_file>
   ```

   Complete SSL Certificate installation using the newly converted Private Key file.
4. Ensure the names of the files are the following:

   key = server.key

   certificate = server.crt

   bundle = server.ca-bundle
5. Backup the existing .keystore file. Type

   ```
   cp /bsc/campusMgr/.keystore /bsc/campusMgr/.keystore.bak
   ```
6. If using the Persistent Agent, import files to the keystore for the Persistent Agent certificate target. Type

   ```
   ImportCertificateWithKey -alias agent -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass
   ^8Bradford%23
   ```

   "Successfully imported key and certificate chain" will display.
7. If using the Captive Portal, import files to the keystore for the captive portal certificate target. Type

   ```
   ImportCertificateWithKey -alias portal -cas server.ca-bundle -key server.key -cert
   server.crt -keystore /bsc/campusMgr/.keystore -v -force -import -storepass
   ^8Bradford%23
   ```

   "Successfully imported key and certificate chain" will display.
8. If certificates were installed in the Portal, restart apache service. Type

   ```
   service httpd restart
   ```
9. In the Administration UI, navigate to **System > Settings > Security > Certificate Managemen**t. Verify certificate details display for each target.
10. **Captive Portal**: Verify new certificate is being used by examining the certificate details in the browser (such as the security lock icon or whichever method is offered by that browser). **Important**: ensure the name used in the URL is the one specified in the certificate.

If unexpected behavior occurs, see Troubleshooting.

Troubleshooting

Related KB Articles

Private Key error when installing renewed SSL certificate

Invalid private key error while installing SSL certificate

Convert SSL private key to RSA format

Export SSL certificate and private key from keystore

Create SSL Certificate Bundle with Files Returned from Certificate Authority

Identify missing SSL certificates via administration UI

'One or more certificates are invalid' error

Error when updating Portal SSL mode or portal SSL certificate

If something is wrong with the uploaded certificate files, FortiNAC will display an error and will not apply the certificate.

Common Causes for Certificate Upload Errors

- The wildcard name (e.g., *.yourcompany.com) was placed in the Fully- Qualified Host Name Field in the Portal SSL view under System > Settings > Security. To correct, change the entry to the true Fully-Qualified Host Name and click Save Settings.
- There are extra spaces, characters, and/or carriage returns above, below, or within the text body of any of the files.
- The certificate was not generated with the current key and there is mismatch.

  This can happen if the OK button in the Generate CSR screen had been clicked after saving the Certificate Request. Each time OK is clicked on the Generate CSR screen, a new CSR and private key are created, overwriting any previous private key.

  To confirm the certificate and key match, use the following tool: https://www.sslshopper.com/certificate-key-matcher.html

If the key and certificate do not match, generate a new CSR and submit for a new certificate.

Contact Support for further assistance.

Appendix

Keystore for SSL/TLS Communications

When using SSL or TLS security protocols for communications between FortiNAC and some servers (such as LDAP directory, Fortinet EMS and Nozomi servers) a security certificate may be required. The need for the certificate is dependent upon the configuration of the directory. In most cases, FortiNAC automatically imports the certificate it needs. However, if this is not the case, import the certificate. For instructions, see section Create a keystore for SSL or TLS of the Administration Guide.

SSL File Conversion Tool Chart

The following commands are in Linux. Use these commands to convert files either on a separate Linux machine or on the FortiNAC appliance.

Function	Linux Syntax

Convert DER/Binary to PEM Format	`openssl x509 -inform der -in <filename> -out <newfilename>`
	Example converting certificate.cer:
	`openssl x509 -inform der -in certificate.cer -out certificate.pem`

Convert P7B/PKCS#7 to PEM Format	`openssl pkcs7 -print_certs -in <filename> -out <newfilename>`
	Example converting certificate.p7b:
	`openssl pkcs7 -print_certs -in certificate.p7b -out certificate.cer`

Convert PFX/PKCS#12 to PEM Format (requires PFX file password)	`openssl pkcs12 -in <filename> -out <newfilename> -nodes`
	Example converting certificate.pfx:
	`openssl pkcs12 -in certificate.pfx -out certificate.cer -nodes`

Convert PKCS8 Private Key to RSA Format	`openssl rsa -in <filename> -out <newfilename>` Example converting to RSA Private key:

Function	Linux Syntax
	`openssl rsa -in server.key.norsa -out server.key`
Decrypt Private Key (requires Private Key file password)	`openssl rsa -in <filename> -out <newfilename>` Example decrypting Private Key: openssl rsa –in serer.key.encrypted -out server.key

Renew a Certificate

SSL Certificates must be renewed periodically or they expire. However, the existing certificate must be used until the new one arrives. Some Certificate Authorities allow managing certificates such that it can be renewed without generating a new request file. In these cases, the private key will remain the same and the new certificate can be imported when it arrives.

1. Save the file(s) received from the CA to your PC.
2. Select the target where the certificate will be uploaded.
3. Select **Reuse Private Key from Existing Certificate** to use the private key for the certificate currently in use.
4. Upload new certificate files.

   Troubleshooting:

   Private Key error when installing renewed SSL certificate
5. Copy certificate to other targets as necessary. See Copy Certificate to Other Targets.

Issuing a Self-Signed Certificate

FortiNAC issues its own certificate. This option is not as secure, but can be used in the event there are no certificates issued by a third party or internal Certificate Authority that are available.

Important: This type of certificate cannot be used for the Persistent Agent certificate target (for Persistent Agent communication) or the Portal target when using Dissolvable Agents.

To generate a Self-Signed Certificate:

1. Select **System > Certificate Management**.
2. Click GenerateCSR.
3. Select the certificate target.

   Admin UI: Generates CSR for the Administration User Interface.

   Persistent Agent: Not recommended when using Self-Signed Certificates.

   Portal: Not recommended when using Self-Signed Certificates.
4. Select Use Result as Self-Signed Certificate
5. Enter the Common Name (Fully-Qualified Host Name). This is the Host Name to be secured by the certificate.

6. Click **OK**.
7. Import the certificate to the endstations accessing this target (Admin UI, Persistent Agent or Portal) in order to establish trust. There are various methods to do this. See Import Self-Signed Certificates.

Import Self-Signed Certificates

1. Export certificate from FortiNAC to use for other browsers.

   Note: Exporting the certificate may not be possible with Internet Explorer

   Export using FireFox:

   To export certificate to use for other browsers:

   a. Browse to https://<appliance name>:8443

   The message "Your connection is not secure" displays.

   b. Click the padlock or "i" next to the URL

   c. Click the > next to the host name

   d. Click **More Information**

   e Under the Details tab click the Export button.

   f. Save as PEM.

   Export using FortiNAC CLI:

   a. Login to the FortiNAC Server or Control Server as root.

   b. Export the certificate to a file. Type

   ```
   echo -n | openssl s_client -connect <appliance name>:8443 | sed -ne '/-BEGIN
   CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert
   ```

   Example:

   ```
   echo -n | openssl s_client -connect qa6-74.Fortinetnetworks.com:8443 | sed -ne '/-
   BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > server.cert

   depth=0 CN = qa6-74.Fortinetnetworks.com

   verify error:num=18:self signed certificate

   verify return:1

   depth=0 CN = qa6-74.Fortinetnetworks.com

   verify return:1

   DONE
   ```

   c. Download certificate file from FortiNAC. This can be done in various ways:

   FortiNAC CLI:

   - Upload file to a FTP server

     ftp <destination ip or name>
   - Use SCP and copy to another endstation

     scp server.cert root@<destination IP address or hostname>:/<path>

     WinSCP or similar program: Specify SCP for transfer protocol
2. Import the certificate to the browser.

   FireFox:

a. Browse to https://<appliance name>:8443

The message "Your connection is not secure" displays.

b. Click **Advanced**

c. Click **Add Exception**

d. Click **Confirm Security Exception**

e. Close the browser completely and reopen. The URL should now display as secure.

Internet Explorer (IE):

a. Browse to https://<appliance name>:8443

b. Under start menu, in search bar type **certmgr.msc**.

c. Navigate to folder **Trusted Root Certification Authorities\Certificates**.

d. Click **Action > All Tasks > Import**

e. Browse and select the filename of the certificate.

f. Click **Open**

g. Click **Next**

h. Ensure Place all certificates in Certificate store Trusted Root Certification Authorities is selected

i. Click **Next**

j. Click **Finish**

k. When prompted to install certificate, click **Yes**

"The import was successful" should display.

Close the browser completely and reopen. The URL should now display as secure.

Generate New Self-Signed Certificate

Certificate alias 'server' certificate expiring. Delete the certificate and generate a new one.

1. Shut down management processes.

```
shutdownNAC
```

```
shutdownNAC -kill
```

2. Delete the certificate. Type

```
keytool -delete -alias server -keystore /bsc/campusMgr/.keystore -storepass
^8Bradford%23
```

3. Generate new certificate. Type

```
keytool -genkey -alias server -keyalg RSA -keysize 2048 -validity 3650 -dname
'CN=bradfordnetworks.com,OU=Bradford Networks,O=bni,L=Concord,ST=NH,C=US' -keypass
^8Bradford%23 -keystore /bsc/campusMgr/.keystore -storepass ^8Bradford%23
```

4. Distribute the certificate to the application servers and NCM (if they exist). Type

```
/bsc/campusMgr/bin/internal/exchange-server-certs
```

5. Start processes. Type

```
startupNAC
```