Custom SSL certificates may be applied and used to support HTTPS services on the Advanced Features units. Configuring custom SSL certificates involves the following considerations:

1. Display the Default Services.
2. Disable the HTTP Service.
3. Enable the HTTPS Service.
4. Login to the GUI via HTTPS and Upload the Custom SSL Certificate (PEM file).
5. Apply the Custom SSL Certificate.

1. Display the Default Services

The default services configuration are displayed via the console interface. Use the following procedure to connect to the Advance Features unit and display the default services configuration.

1. Connect a Serial cable from a COM port on the laptop or PC to the Serial Interface on the unit.
2. Launch Putty and configure the Serial connection as follows:

Speed (baud)	115200
Data bits	8
Stop bits	1
Parity	None
Flow Control	XON/XOFF

3. Press the Return key.
4. Enter enable.
5. Enter the following command to display the default services configuration.

```
Switch# show services

Networking services configuration:

Service Name     Status        Port       Protocol   Service ACL

----------------+-------------+----------+----------+------------

http             enable        80         TCP        -

https            disable       443        TCP        -

rpc-api          disable       -          TCP        -

telnet           disable       23         TCP        -

ssh              enable        22         TCP        -
```


Copyright © 2023 Garland Technology, LLC. All rights reserved.

```
snmp             disable       161        UDP        -
```

2. Disable the HTTP Service

1. Enter the following commands to disable the HTTP service.

```
Switch# configure terminal

Switch(config)# service http disable

Switch(config)# exit

Switch# show services

Networking services configuration:

Service Name     Status        Port       Protocol   Service ACL

----------------+-------------+----------+----------+------------

http             disable       80         TCP        -

https            disable       443        TCP        -

rpc-api          disable       -          TCP        -

telnet           disable       23         TCP        -

ssh              enable        22         TCP        -

snmp             disable       161        UDP        -
```

3. Enable the HTTPS Service

1. Enter the following commands to enable the HTTPS service.

```
Switch# configure terminal

Switch(config)# service https enable

Switch(config)# exit

Switch# show services

Networking services configuration:

Service Name     Status        Port       Protocol   Service ACL

----------------+-------------+----------+----------+------------

http             disable       80         TCP        -

https            enable        443        TCP        -

rpc-api          disable       -          TCP        -
```


Copyright © 2023 Garland Technology, LLC. All rights reserved.

```
telnet          disable      23        TCP        -
ssh             enable       22        TCP        -
snmp            disable      161       UDP        -
```

4. Login to the GUI via HTTPS and Upload the Custom SSL Certificate (PEM file)

The PEM file that is uploaded onto the Advanced Features unit must contain the both key.pem and the cert.pem files. The file name must be similar to "key_AFTest.pem".

key_AFTest.pem example:

```
-----BEGIN PRIVATE KEY-----
cbhsdabsdahcbsacascakhscbdkndsjnbsdjkcvbskjdcvbskjdbvskdjvbskdvbksdbcskdcbskd
bskdbcfcc
ahscbahscbaksdhcbakshcbasdhcbakhbcahscbakhscbakshcbakshcbakhscashscacajscahscakhscb
akhscb ahscashcajshcajshcahsc&%VBGFFGBjsxncsjbdb#$%^^ujdsfbibfwfbwhfbwhbshbvskdhcvbd
-----END PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
cbhsdabsdahcbsacascakhscbdkndsjnbsdjkcvbskjdcvbskjdbvskdjvbskdvbksdbcskdcbskd
bskdbcfcc
ahscbahscbaksdhcbakshcbasdhcbakhbcahscbakhscbakshcbakshcbakhscashscacajscahscakhscb
akhscb ahscashcajshcajshcahsc&%VBGFFGBjsxncsjbdb#$%^^ujdsfbibfwfbwhfbwhbshbvskdhcvbd
-----END CERTIFICATE-----
```

1. Launch the web browser and enter the Advanced Features IP address, (https://www.xxx.yyy.zzz).
2. Login to the GUI, (admin/gtadmin1).
3. Select System Management.
4. Select Update Management.
5. Select the Select image file (Upload files to boot) Choose File.
6. Select the "key_AFTest.pem".
7. Select Upload only.
8. Select File Management.
9. Select the Boot files Tab.
10. Verify the new "key_AFTest.pem".

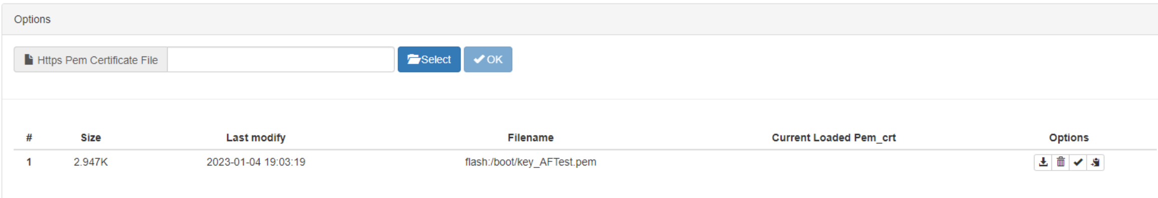
Copyright © 2023 Garland Technology, LLC. All rights reserved.

5. Apply the Custom SSL Certificate

1. Select Security.

2. Select Https Pem_crt.

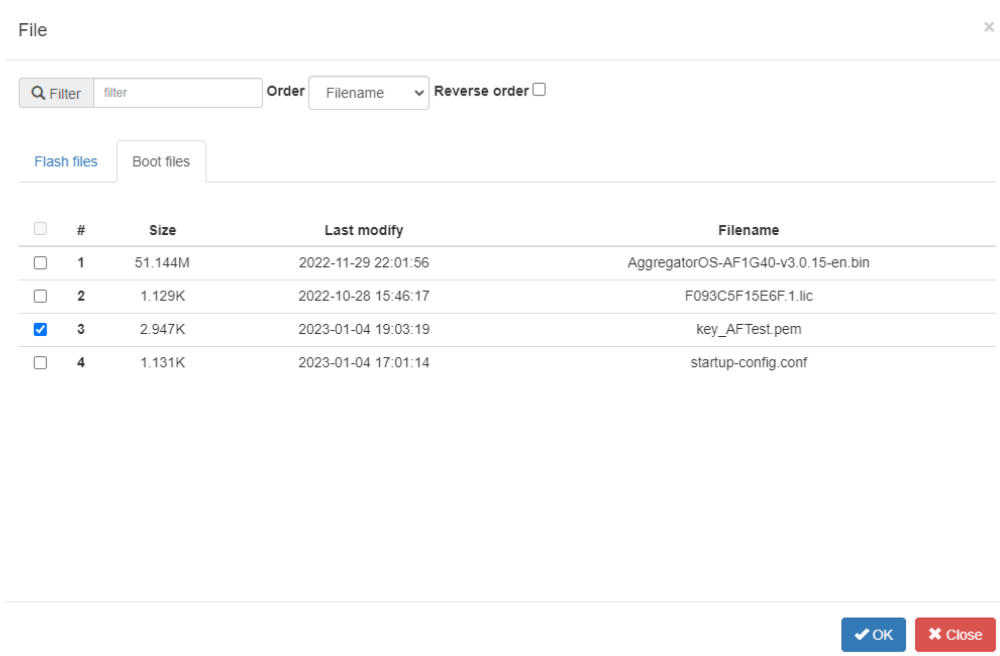
   The key_AFTest.pem *will be displayed.*

3. 

Select Select.

4. Select the Boot files Tab.

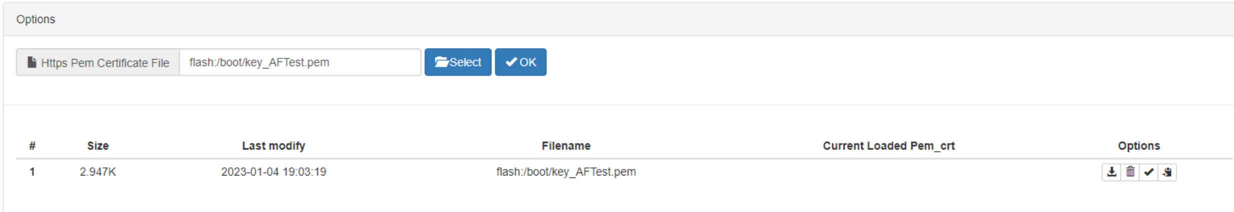
5. Select the pem file “key_AFTest.pem”.



6. Select OK.

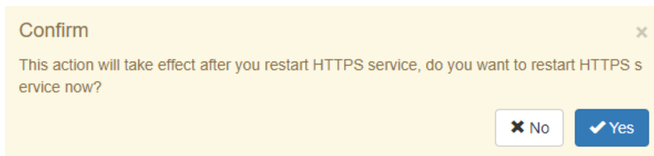
7. Verify the Https Pem Certificate File, new “key_AFTest.pem”.

Copyright © 2023 Garland Technology, LLC. All rights reserved.



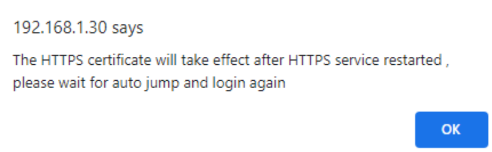
8. Select OK.

The Confirm message will be displayed.



9. Select Yes.

The HTTPS restart message will be displayed.



8. Select OK.

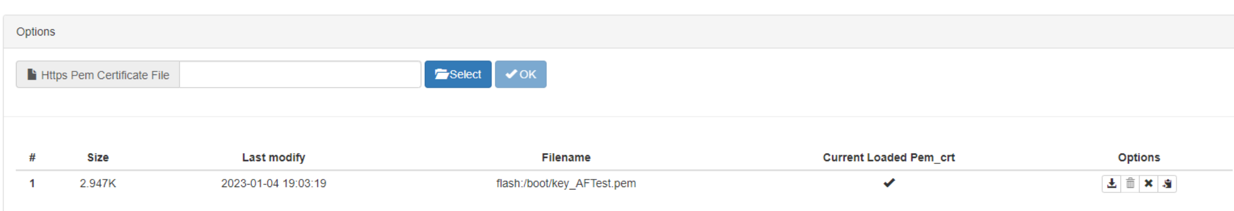
The GUI will refresh.

9. Login to the GUI, (admin/gtadmin1).

10. Select Security.

11. Select Https Pem_crt.

12. Verify the Current Loaded Pem_crt.



13. Select the Download icon to download the pem file.

Copyright © 2023 Garland Technology, LLC. All rights reserved.

14. Select the Cancel icon to cancel the current loaded pem file. This will cause the GUI to be restarted back to the login display.
15. Select the Backup icon to create a .pem_BAK file.
16. Select the Delete icon to delete the pem file. However, the pem file must be canceled before delete is allowed.

Copyright © 2023 Garland Technology, LLC. All rights reserved.