Prerequisites for TLS/SSL connections

If you specified the https protocol in the **TNaaS Authority Connector Host** box when configuring the authority, you will need the following files to complete the installation process:

- PEM encoded file containing the X.509 certificate to be used for TLS/SSL
- PEM encoded file containing the private key of the X.509 certificate

Copy these files to the local hard drive of the TNaaS Authority Connector host.

Ensure that the files are readable by root. As a best practice, Resilient recommends setting the minimum privileges on the PEM/CRT files.
sudo chmod 400 *file_name.extension*

Installing the TNaaS Authority Connector

To install the TNaaS Authority Connector, complete the following steps.

1. Download the TNaaS Authority Connector from the Administrative Console.
2. Log onto the TNaaS Authority Connector host.
3. Copy the ZIP file containing the TNaaS Authority Connector scripts onto the TNaaS Authority Connector host.
4. Open a terminal prompt.
5. Extract the contents of the ZIP file.
   unzip *file_name*.**zip**
6. If you are not already logged in as a user with **sudo ALL** privileges, switch to one.
   su *sudo_ALL_user_name*
7. Execute the **tnaas-authority** shell script using **sudo**.
   sudo bash tnaas-authority.sh
   [-c *path*/*cert_file_name.extension* **-k** *path*/*prikey_file_name.extension***]**
   where the **-c** and **-k** flags are required only if you specified the https protocol in the **Custom REST Service URL** box when configuring the authority.
8. If the web server starts successfully, you will see the following message:
   Bottle v0.13-dev server starting up (using
   CherryPyServer(keyfile='*prikey_file_name.extension***', certfile='***cert_file_name.extension***'))...**
   Listening on http[s]://*host_name***:***port_number***/**
   Hit Ctrl-C to quit.
9. After receiving the message that the web server is up and running, log into the Administrative Console, perform the [TNaaS Authority Test](#) to make sure the authority connector is functioning configured and functioning correctly and then switch your the authority from **OFF** to **ON** to use them in policies.