

Stratusphere™

How to place a signed certificate on the Stratusphere™ Hub

Instructions:

1. Log into the console of the Stratusphere™ Hub using `root/sspassword` as credentials.
2. Move into the backend folder which has a existing certificate:

```
cd /var/empty/backend
```
3. Backup the original certificate. The “.keystore” file is not visible unless you use the “ls -al” command.

```
mv .keystore .keystore.orig
```
4. You now have to generate a new public/private key pair. Run the command below to do so. When prompted for the password, use “changeit”. The command will then prompt the user for “first and last name”, please use the Fully Qualified Domain Name (FQDN) of the Stratusphere™ Hub. The command will then prompt for additional information such as Organizational Unit, Organization Name, City, State and Country Code. Use the same password “changeit” or hit ENTER for <tomcat> password.

```
/usr/java/default/bin/keytool -keysize 2048 -genkey -alias tomcat -keyalg RSA -keystore /var/empty/backend/.keystore
```
5. You now have to generate the Certificate Signing Request (CSR) that you need to provide to VeriSign, RapidSSL or any internal certificate authority. When prompted for a password, use “changeit”.
 - a.

```
/usr/java/default/bin/keytool -certreq -keyalg RSA -alias tomcat -file /var/empty/backend/hub.csr -keystore /var/empty/backend/.keystore
```
6. Copy this `hub.csr` file to the `/home/friend` folder and use WinSCP to download it to your desktop. To connect to the Stratusphere™ Hub using WinSCP use the `friend/sspassword` credentials to connect. Alternatively you can also use “cat” to copy it out of the console itself.

```
cp /var/empty/backend/hub.csr /home/friend/hub.csr
```

OR

```
cat /var/empty/backend/hub.csr
```
7. Use this CSR to get your certificate from your Certificate Source such as VeriSign, RapidSSL, or an internal certificate authority. Depending on your certifying authority, you will receive a X.509 certificate for your server along with an Intermediate CA Certificate. Save these two certificates as `hub.crt` and `intermediate.crt` and use WinSCP to upload them to the Hub. Use `friend/sspassword` as credentials within WinSCP to copy the certificate to the Hub’s

/home/friend folder. Then log into the console of the Stratusphere™ Hub again using root/sspassword to login as root.

8. If and only if, you received an Intermediate CA Certificate from your certifying authority then execute the following command, otherwise skip to next item:
 - a. `/usr/java/default/bin/keytool -importcert -keystore /var/empty/backend/.keystore -file /home/friend/intermediate.crt`
9. Execute the following command to import the certificate into the keystore:
 - a. `/usr/java/default/bin/keytool -import -alias tomcat -keystore /var/empty/backend/.keystore -trustcacerts -file /home/friend/hub.crt`
10. Make sure you provide the right permissions for the new keystore file for the service that needs to access it:
 - a. `chown vsservice /var/empty/backend/.keystore`
11. Restart the backend service to read the new certificate and be ready to accept new connections.
 - a. `sv restart tnt-backend`
Note: Access the UI from the web browser and see if it works without warnings. If it fails, replace /var/empty/backend/.keystore with /var/empty/backend/.keystore.orig and restart backend.