Create a keystore or trusted store .

Integration Server stores its private keys and SSL certificates in keystore files and the trusted roots for the certificates in truststorefiles. Keystores and truststores are secure files with industry-standard file formats.

**Keystore File**

Integration Server uses a special file called a keystoreto store SSL certificates and keys. A keystore file contains one or more pairs ofa private key and signed certificate for its corresponding public key. The keystore should be strongly protected with a password, and stored (either on the file system or elsewhere) so that it is accessible only to administrators.

Now specify the password which are available are used in while creating certificates



**Truststore File**

Integration Server uses a truststore to store its trusted root certificates, which are the public keys for the signing CAs. Although a truststore can contain the trusted roots for entire certificate chains, there is no requirement for the organization ofcertificates within an Integration Server truststore. It simply functions as a database containing all the public keys for CAs within a specified trusted directory.



Once we create the keystore and truststore itrepresent like this.



Now under the ports create an https port by standardport: 443. Select the keystore and truststore that was created and save it.





Now let us connect the integration server with the port 443 where it ask about userid and password since we specified usage as SSL authentication.



Since we specified during importing the certificate as user group as Administrator so after specifying the member of the group with its userid and password we can connect the server.

