Enable Transport Layer Security (TLS)

Enable TLS between Callisto UCM and Cisco UCM to encrypt their connection and achieve a high security level.

Download certificate from Callisto

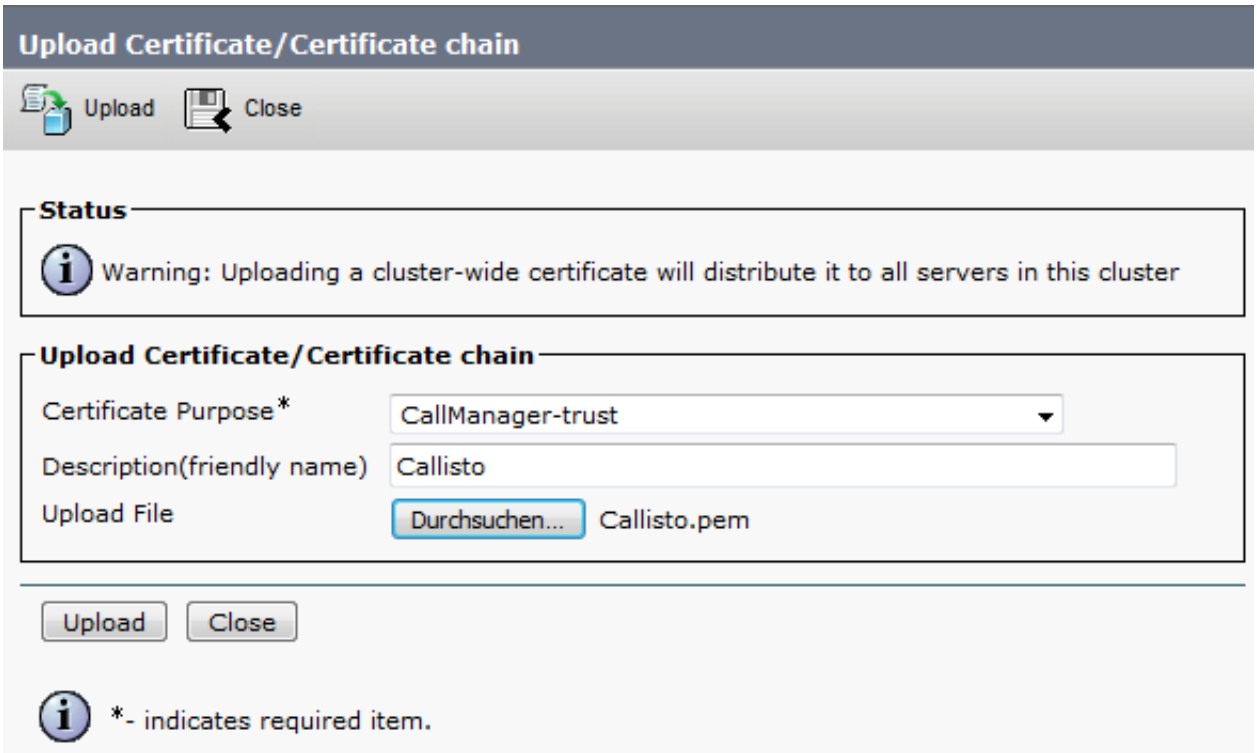
In the Callisto web interface, go to System > System Parameters > SSL Configuration (Top right corner) > Downlad PEM.
If there are no certificates yet, create a new self signed certificate… and download it.

Head back to System Parameters and make sure that the box under Miscellaneous > Secure SIP (TLS, SRTP) is checked.

Upload certificate to Cisco UCM

Open the Cisco UCM interface in your web browser and select Cisco Unified OS Administration in the Navigation in the top right corner.

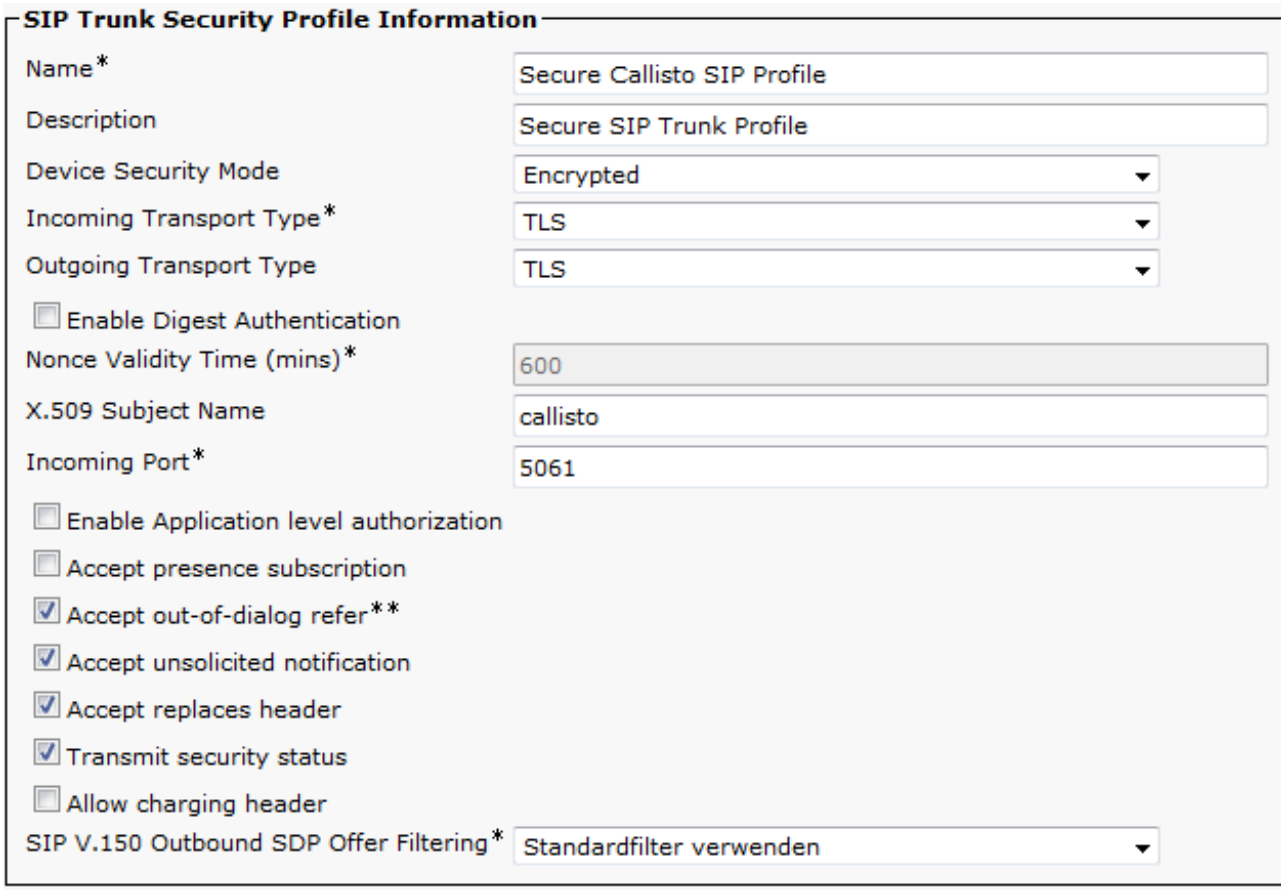
Go to Security > Certificate Management > Upload Certificate and upload the certificate that you previously downloaded from Callisto.
Choose CallManager-trust as the certificate purpose and provide a user friendly description like Callisto.



Device security profile

Select now the Cisco Unified CM Administration in the Navigation in the top right corner and head to System > Security > SIP Trunk Security Profle and then Add New.

Fill in the profile information as following:



(Name and description are examples)

If you are not already using secure connections it might be that the LBM Security Mode is set to insecure. To change this, head to System > Enterprise Parameters > Security Parameters > LBM Security Mode and change it to at least Mixed.

Create trunk

Create a new Trunk under Device > Trunk as described above under SIP tunk configuration.

Use the previously created Device Security Profile, set the Destinationport to 5061 and use the Callisto IP as Destination Address.

Now the Trunk is ready to be used as a secure connection, to do so define a new route pattern and use the created trunk as the Gateway / Route List to route the desired calls trough this trunk.