Secure Client Communications for Cisco DCNM Servers

This section describes how to configure HTTPS on Cisco Data Center Network Manager Servers.

Note You must enable SSL/HTTPS on the Cisco DCNM before you add a CA signed SSL certificate. Therefore, perform the procedure in the below mentioned order.

This section includes the following topics:

Enabling SSL/HTTPS on Cisco DCNM in Federation on RHEL or Windows

To enable SSL/HTTPS on RHEL or Windows for Cisco DCNM in Federation, perform the following:

Procedure

Step 1 Configure the primary server with a self signed SSL certificate.

Note In a CA signed certificate, each server has their own certificate generated. Ensure that the certificate is signed by the signing certificate chain which is common for both the servers.

Step 2 On the secondary server, perform one of the following:

- While executing the installer, choose HTTPS upfront and select to run in the HTTPs mode.
- While silent installation, choose HTTPs while you execute the installer.