



Secure Client Communications for Cisco DCNM Servers

- [Secure Client Communications for Cisco DCNM Servers, on page 1](#)

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 HA Environment on Virtual Appliance

To enable SSL/HTTPS on a Virtual Appliance for Cisco DCNM in HA mode, 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, locate the keystore.

Step 3 Rename the keystore located at

```
<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks
```

to

```
<DCNM_install_root>/dcm/wildfly-10.1.0.Final/standalone/configuration/fmserver.jks.old
```

Step 4 Copy the file `fmserver.jks` generated in primary server to secondary server into folders

```
<dcnm-home> /dcm/wildfly-10.1.0.Final/standalone/configuration/  
<dcnm-home>/dcm/fm/conf/cert/
```

What to do next

If you have created a self-signed certificate or imported an SSL certificate to the keystore, you must copy the new `fmserver.jks` located at

`/usr/local/cisco/dcm/wildfly-10.1.0.Final/standalone/configuration/etc/elasticsearch`. If you do not copy the `fmserver.jks` file to the `elasticsearch` directory, you will not be able to get the Alarms and Policies. As the `elasticsearch` database will be stabilizing, you cannot configure any Alarm Policy on the Cisco DCNM **Web UI Monitor > Alarms > Alarm Policies**.