

# Manage Certificates on the Cisco Business Dashboard

## Objective

A digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows relying parties to depend upon signatures or assertions made by the private key that corresponds to the public key that is certified. Upon installation, the Cisco Business Dashboard generates a self-signed certificate to secure web and other communication with the server. You can choose to replace this certificate with the one signed by a trusted certificate authority (CA). To do this, you will need to generate a certificate signing request (CSR) for signing by the CA.

You can also choose to generate a certificate and the corresponding private key completely independent of the Dashboard. If so, you can combine the certificate and private key into a Public Key Cryptography Standards (PKCS) #12 format file prior to upload.

The Cisco Business Dashboard only supports .pem format certificates. If you get other certificate formats, you need to convert the format or request for the .pem format certificate again from the CA.

This article provides instructions on how to manage certificates on Cisco Business Dashboard Network Manager.

## Applicable Software Version

- CBD ([Data Sheet](#)) | 2.2 ([Download latest](#))

## Manage Certificates on Cisco Business Dashboard

### Generate a CSR

Step 1. Log in to the Administration GUI of your Cisco Business Dashboard then choose **System > Certificate**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

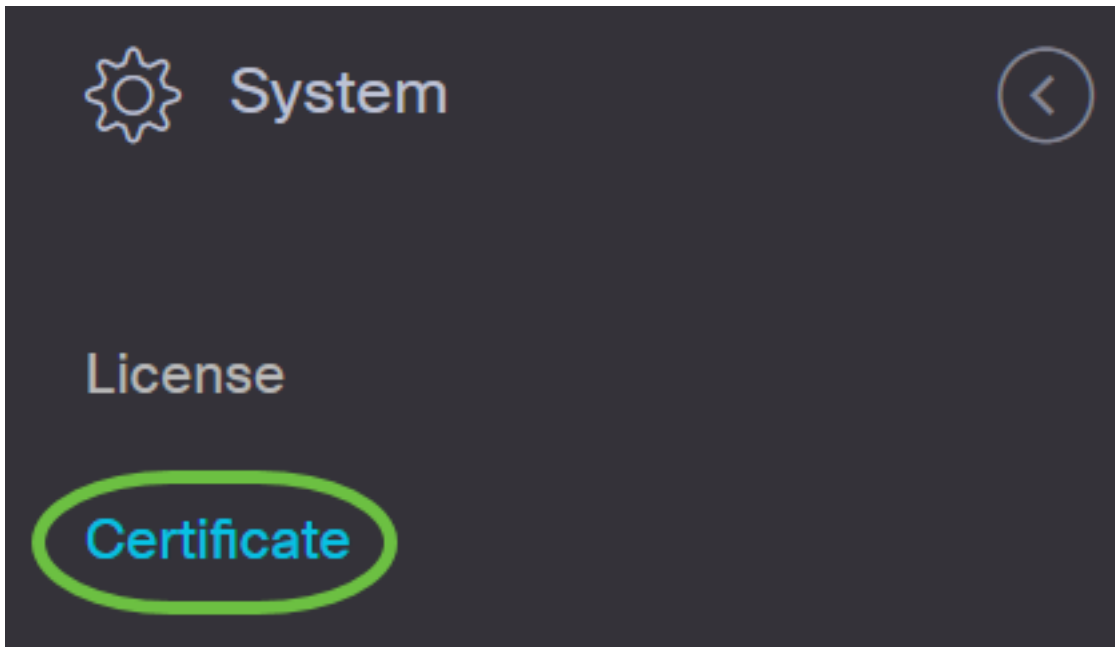


Administration



System





Step 2. In the *CSR* tab, enter appropriate values into the fields provided in the form that is displayed. These values will be used to construct the CSR, and will be contained in the signed certificate you receive from the CA. Click **Create**.

## Certificate

Current Certificate

Update Certificate

**CSR**

1

CSR:



Note: Once the CSR has been created, the downloaded file should be sent to a Certificate Authority to have a certificate is

Common Name

Test ✓

Country/region

US - United States ▼

State

CA ✓

City

Irvine ✓

Org

Cisco ✓

Org Units

Cisco Business ✓

Email

ciscocbd@cisco.com ✓

Subject Alternative Name

hostname.cisco.com ✓

3

**Create**

Clear

The CSR file will be automatically downloaded to your computer.

Step 3. (Optional) To download a copy of the current certificate, click the **Download** button.

---

Certificate

---

Current Certificate

Update Certificate

**CSR**

---

CSR: Created

Download

---

Step 4. (Optional) To update the created CSR, navigate to the *Update Certificate* tab and choose **Renew Self-signed Cert** option. Makes the desired changes to the fields and click **Save**.

## Certificate

1 **Update Certificate** CSR

2  Renew Self-signed Cert  Upload Cert  Upload PKCS12

Common Name	Test2 ✓
Country/region	US - United States ▾
State	CA ✓
City	Irvine ✓
Org	Cisco ✓
Org Units	Cisco Business ✓
Start Date - End Date	Sep 21 2020 ~ Oct 21 2020
Email	ciscobd@cisco.com ✓
Subject Alternative Name	hostname.cisco.com ✓

3

4 **Save** Cancel

You have now successfully generated a CSR on your Cisco Business Dashboard. You can now send the downloaded CSR file to the CA.

### Upload a Signed Certificate from the CA

Once you receive the signed CSR from the CA, you can now upload it to the Dashboard.

Step 1. Log in to the Administration GUI of your Cisco Business Dashboard then choose **System > Certificate**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

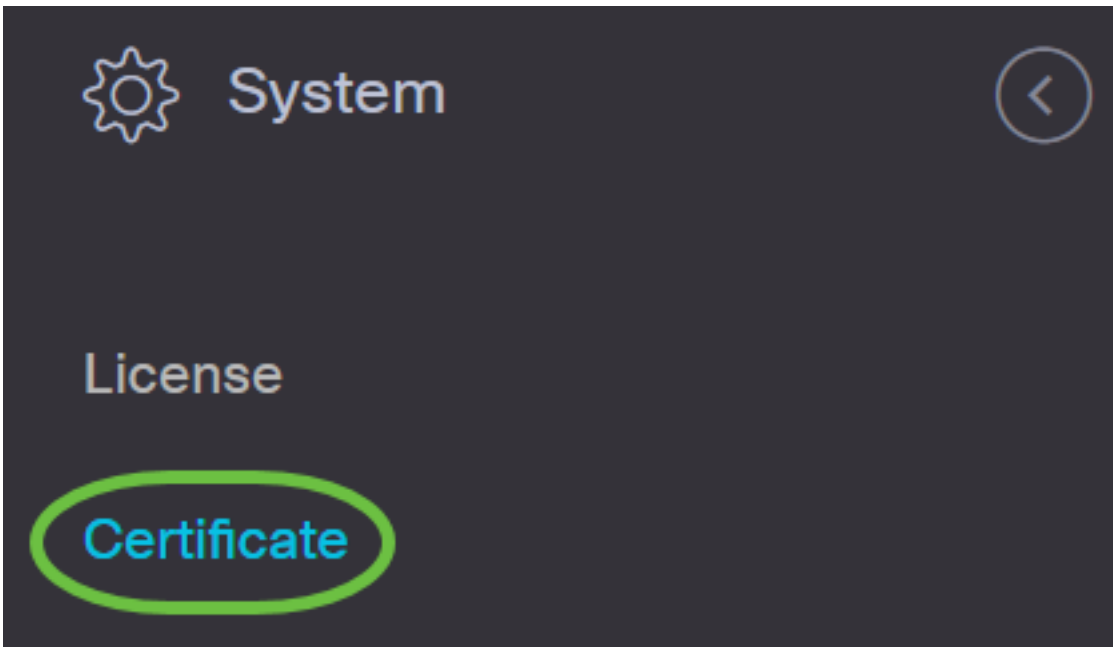


Administration



System





Step 2. In the *Update Certificate* tab, choose the **Upload Cert** radio button.

Certificate

---

Current Certificate **Update Certificate** CSR

---

Renew Self-signed Cert  **Upload Cert**  Upload PKCS12

2

Drag and drop file here, or click to select from the filesystem

**Note:** Alternatively, you can upload a certificate with the associated private key in PKCS#12 format by choosing the **Upload PKCS12** radio button. The password to unlock the file should be specified in the *Password* field provided.



## Certificate

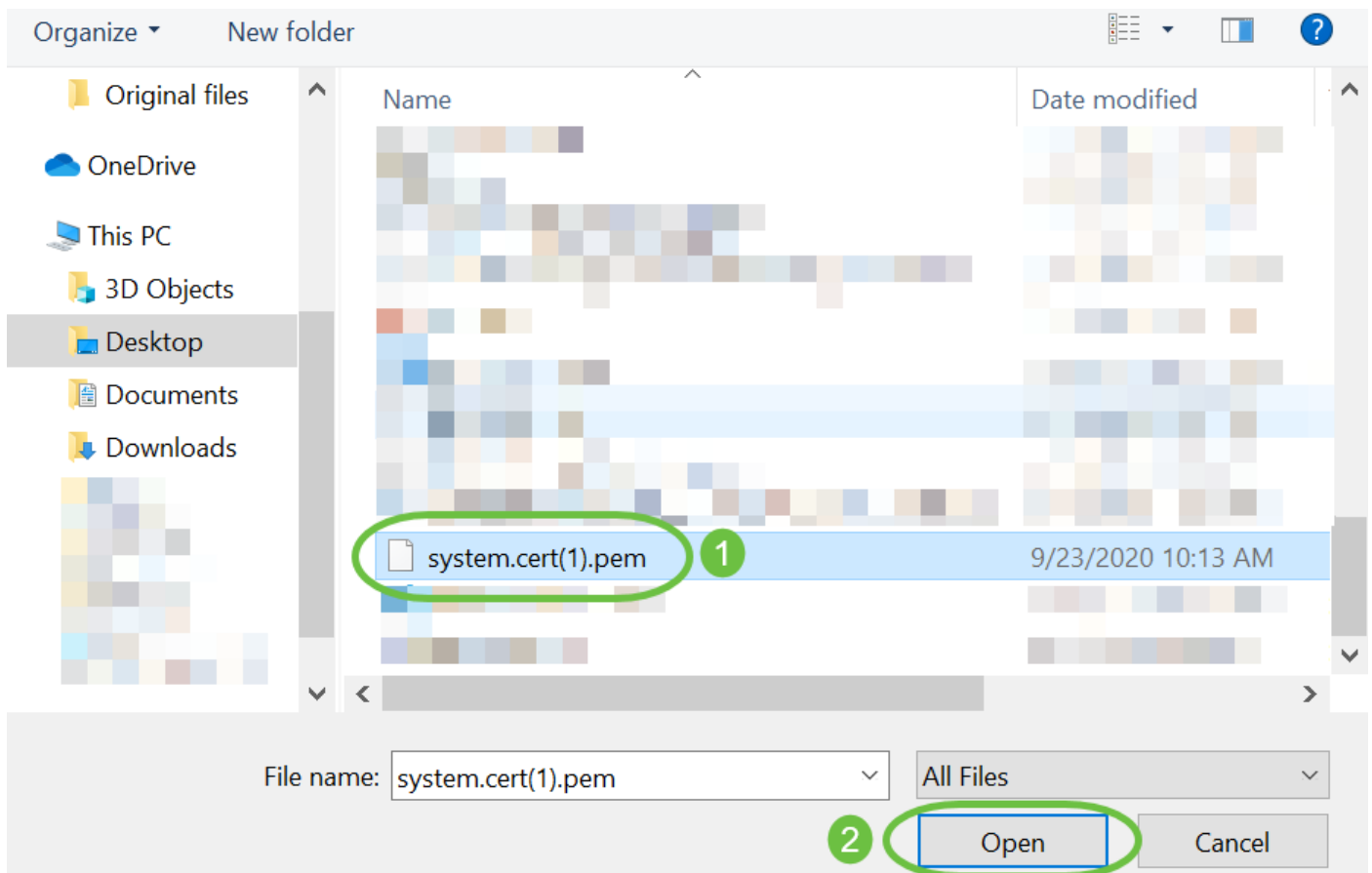
Current Certificate **Update Certificate** CSR

Renew Self-signed Cert  Upload Cert  Upload PKCS12

Password

Drag and drop file here, or click to select from the filesystem

Step 3. Drop the signed certificate on the target area, or click the target area to browse the file system then click **Open**. The file should be in .pem format.




Step 4. Click **Upload**.

## Certificate

Current Certificate   **Update Certificate**   CSR

Renew Self-signed Cert    Upload Cert    Upload PKCS12

Drag and drop file here, or click to select from the filesystem

 system.cert(1).pem 8.47KB



You have now successfully uploaded a signed certificate to the Cisco Business Dashboard Network Manager.

### Manage Current Certificate

Step 1. Log in to the Administration GUI of your Cisco Business Dashboard then choose **System > Certificate**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

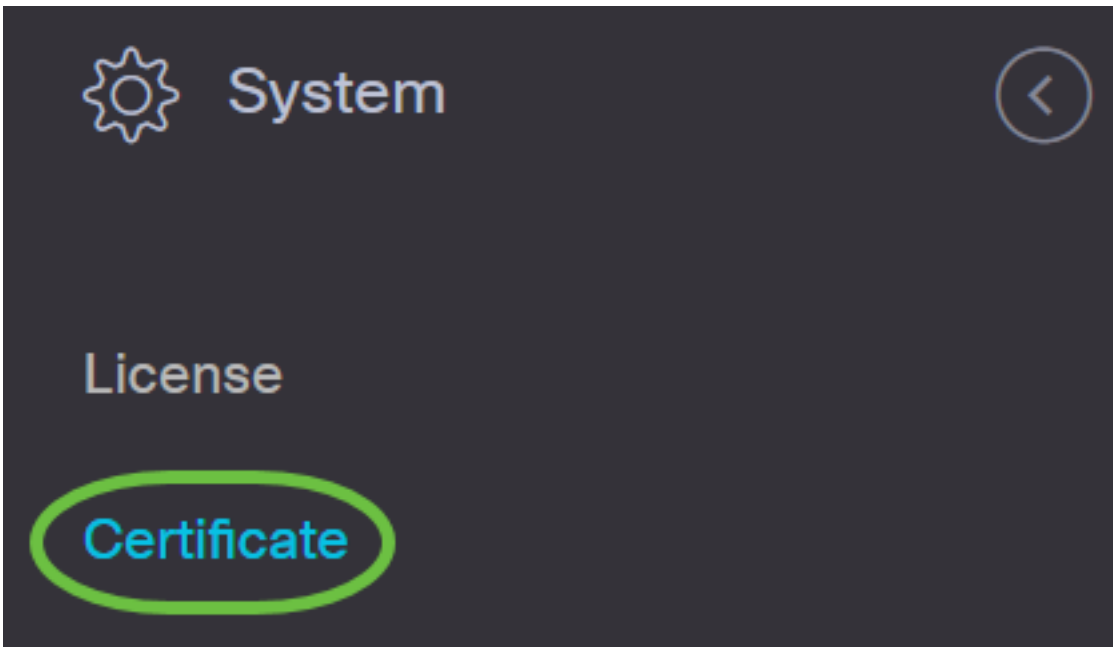


Administration



System





Step 2. Navigate to the *Current Certificate* tab. The current certificate will be displayed in plain text format.

## Certificate

[Current Certificate](#) [Update Certificate](#) [CSR](#)

### Certificate Detail

#### Certificate:

##### Data:

Version: 3 (0x2)

##### Serial Number:

6a:78:e1:66:cb:6a:b9:fe:d3:1a:e2:c2:3d:60:12:f1

Signature Algorithm: sha256WithRSAEncryption

Issuer: C=GB, ST=Greater Manchester, L=Salford, O=Sec

##### Validity

Not Before: Aug 11 00:00:00 2020 GMT

Not After : Mar 18 23:59:59 2021 GMT

Subject: CN=cbd.sbcenter.net

##### Subject Public Key Info:

Public Key Algorithm: rsaEncryption

Public-Key: (2048 bit)

Step 3. (Optional) To download a copy of the current certificate, click the **Download** button.

## Certificate

Current Certificate

Update Certificate

CSR

```
14:C0:60:6C:4A:45:A5:E3:79:EC:69:89:BB:D7:96:80:
5D:12:49:19:20:C0:93:AD
Signature Algorithm: sha256WithRSAEncryption
8b:19:a4:75:dd:13:e7:d0:0f:37:c2:eb:ee:8d:34:c4:65:99:
0e:f9:54:cf:ca:c4:92:84:48:e7:ba:a4:13:a7:66:39:8b:03:
cd:79:ae:35:2a:48:86:ff:be:b3:ac:ee:50:00:1f:62:9e:c0:
7b:89:00:86:70:ce:82:45:56:25:4e:7b:0b:44:74:7b:76:8a:
98:cd:a4:55:24:09:12:a9:de:a6:cc:39:22:6e:f1:e3:8c:50:
eb:4f:46:79:16:7e:ef:20:70:17:b9:9e:e2:34:1e:0f:00:4a:
7f:0d:c3:62:df:fe:23:fd:be:9d:e6:37:f5:31:bf:1c:09:50:
5d:6e:bf:02:42:df:a0:04:b9:0f:df:79:72:73:0e:4e:9c:7f:
97:f8:da:77:9b:59:6a:b2:23:8d:eb:f1:41:4a:d2:8d:0d:f0:
78:8e:71:78:d6:55:48:9d:75:ae:13:00:8a:8f:14:68:d1:cd:
6e:2c:70:75:28:94:f8:d8:36:da:7f:17:a6:73:7b:d7:72:f9:
69:8b:f9:87:4d:30:ef:8e:8a:09:8d:f0:03:05:42:82:5e:96:
28:42:a6:02:9c:8f:a5:4d:fe:e3:fb:f8:61:3d:86:53:39:21:
61:3c:4d:76:fb:ff:a9:3f:99:4f:60:ed:51:20:30:6d:b4:0d:
```

[Download](#)

You have now successfully managed the current certificate on your Cisco Business Dashboard.

For more information on certificates, check out the following articles:

- [Using Let's Encrypt Certificates with Cisco Business Dashboard](#)
- [Using Let's Encrypt Certificates with Cisco Business Dashboard and DNS Validation](#)