

# Gestire certificati su Cisco Business Dashboard

## Obiettivo

Un certificato digitale certifica la proprietà di una chiave pubblica da parte del soggetto specificato del certificato. In questo modo le relying party possono dipendere da firme o asserzioni effettuate dalla chiave privata corrispondente alla chiave pubblica certificata. Al momento dell'installazione, Cisco Business Dashboard genera un certificato autofirmato per proteggere le comunicazioni Web e di altro tipo con il server. È possibile scegliere di sostituire questo certificato con quello firmato da un'Autorità di certificazione (CA) attendibile. A tale scopo, è necessario generare una richiesta di firma del certificato (CSR) per la firma da parte della CA.

È inoltre possibile scegliere di generare un certificato e la chiave privata corrispondente in modo completamente indipendente dal dashboard. In questo caso, è possibile combinare il certificato e la chiave privata in un file in formato PKCS (Public Key Cryptography Standards) #12 prima del caricamento.

Cisco Business Dashboard supporta solo certificati in formato .pem. Se si ottengono altri formati di certificato, è necessario convertire nuovamente il formato o la richiesta del certificato in formato .pem dalla CA.

In questo documento viene spiegato come gestire i certificati in Cisco Business Dashboard Network Manager.

## Versione del software applicabile

- CBD ([data sheet](#)) | 2.2 ([scarica la versione più recente](#))

# Gestisci certificati su Cisco Business Dashboard

## Genera un CSR

Passaggio 1. Accedere alla GUI di amministrazione di Cisco Business Dashboard, quindi scegliere **Sistema > Certificato**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

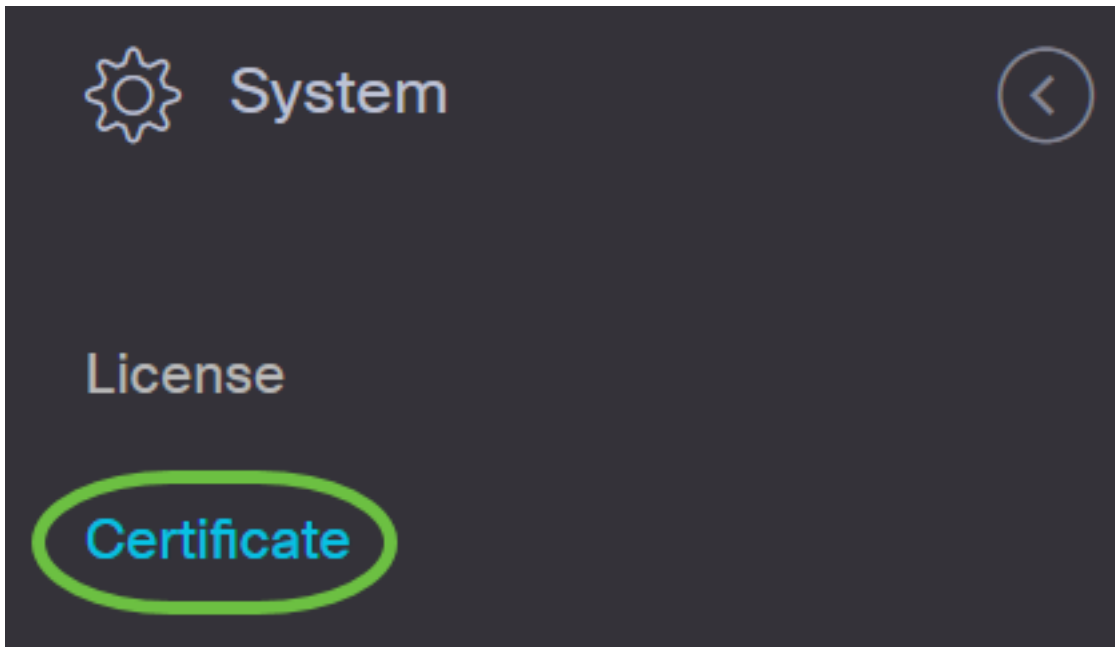


Administration



System





Passaggio 2. Nella scheda *CSR* immettere i valori appropriati nei campi disponibili nel modulo visualizzato. Questi valori verranno utilizzati per costruire il CSR e saranno contenuti nel certificato firmato ricevuto dalla CA. Fare clic su **Crea**.

## 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 ✓

2

**Create**

Clear

3

Il file CSR verrà scaricato automaticamente nel computer.

Passaggio 3. (Facoltativo) Per scaricare una copia del certificato corrente, fare clic sul pulsante **Scarica**.

---

Certificate

---

Current Certificate

Update Certificate

**CSR**

---

CSR: Created

[Download](#)

---

Passaggio 4. (Facoltativo) Per aggiornare il CSR creato, passare alla scheda *Aggiorna certificato* e scegliere l'opzione **Rinnova certificato autofirmato**. Apporta le modifiche desiderate ai campi e fare clic su **Salva**.

## Certificate

Current Certificate **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

ciscocbd@cisco.com ✓

Subject Alternative Name

hostname.cisco.com ✓

**4**

Save

Cancel

La creazione di un CSR in Cisco Business Dashboard è stata completata. A questo punto è possibile inviare il file CSR scaricato alla CA.

### Carica un certificato firmato dalla CA

Una volta ricevuto il CSR firmato dalla CA, è possibile caricarlo nel dashboard.

Passaggio 1. Accedere alla GUI di amministrazione di Cisco Business Dashboard, quindi scegliere **Sistema > Certificato**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

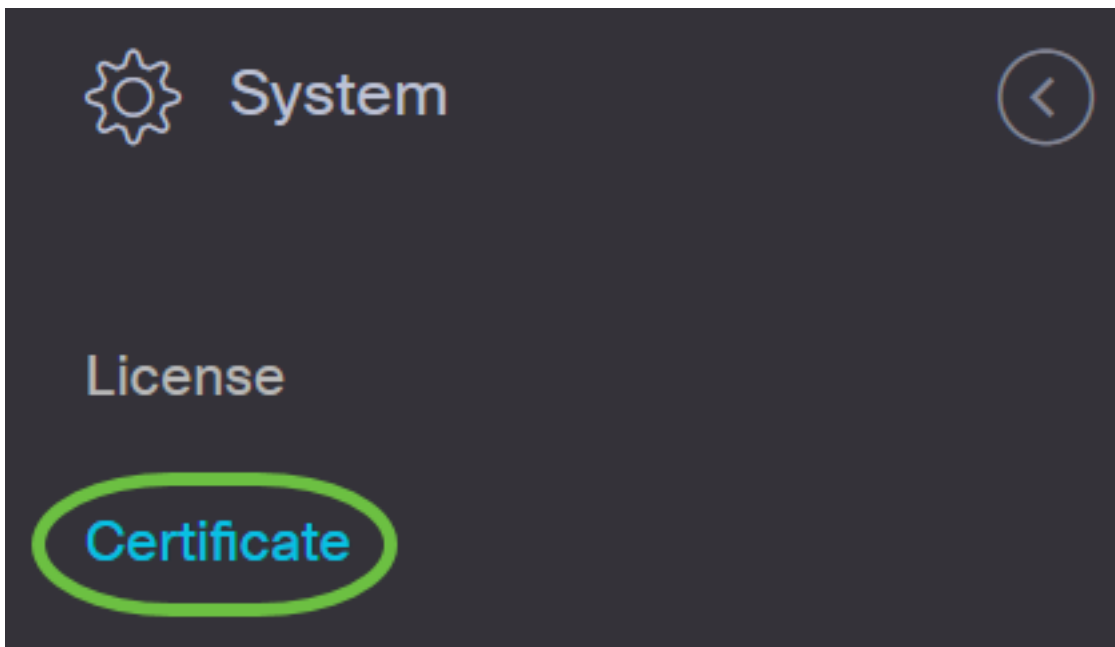


Administration

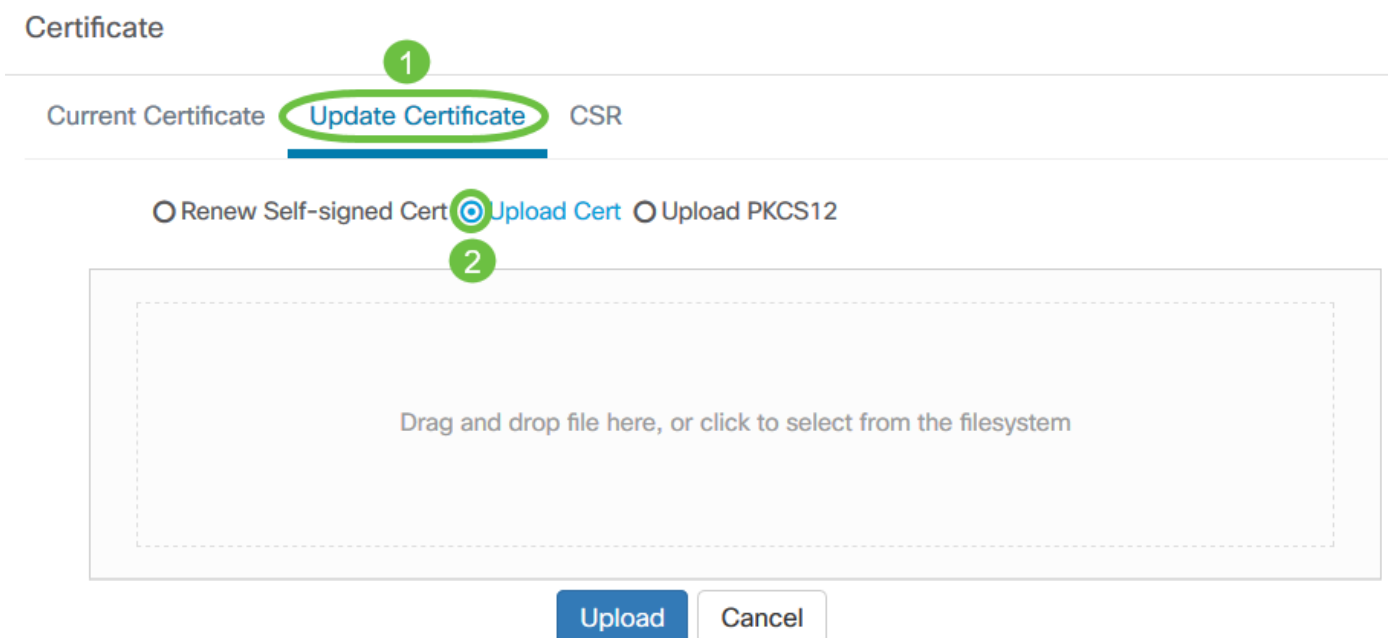


System





Passaggio 2. Nella scheda *Aggiorna certificato*, scegliere il pulsante di opzione **Carica certificato**.



**Nota:** In alternativa, è possibile caricare un certificato con la chiave privata associata in formato PKCS#12 scegliendo il pulsante di opzione **Carica PKCS12**. La password per sbloccare il file deve essere specificata nel campo *Password* fornito.



## Certificate

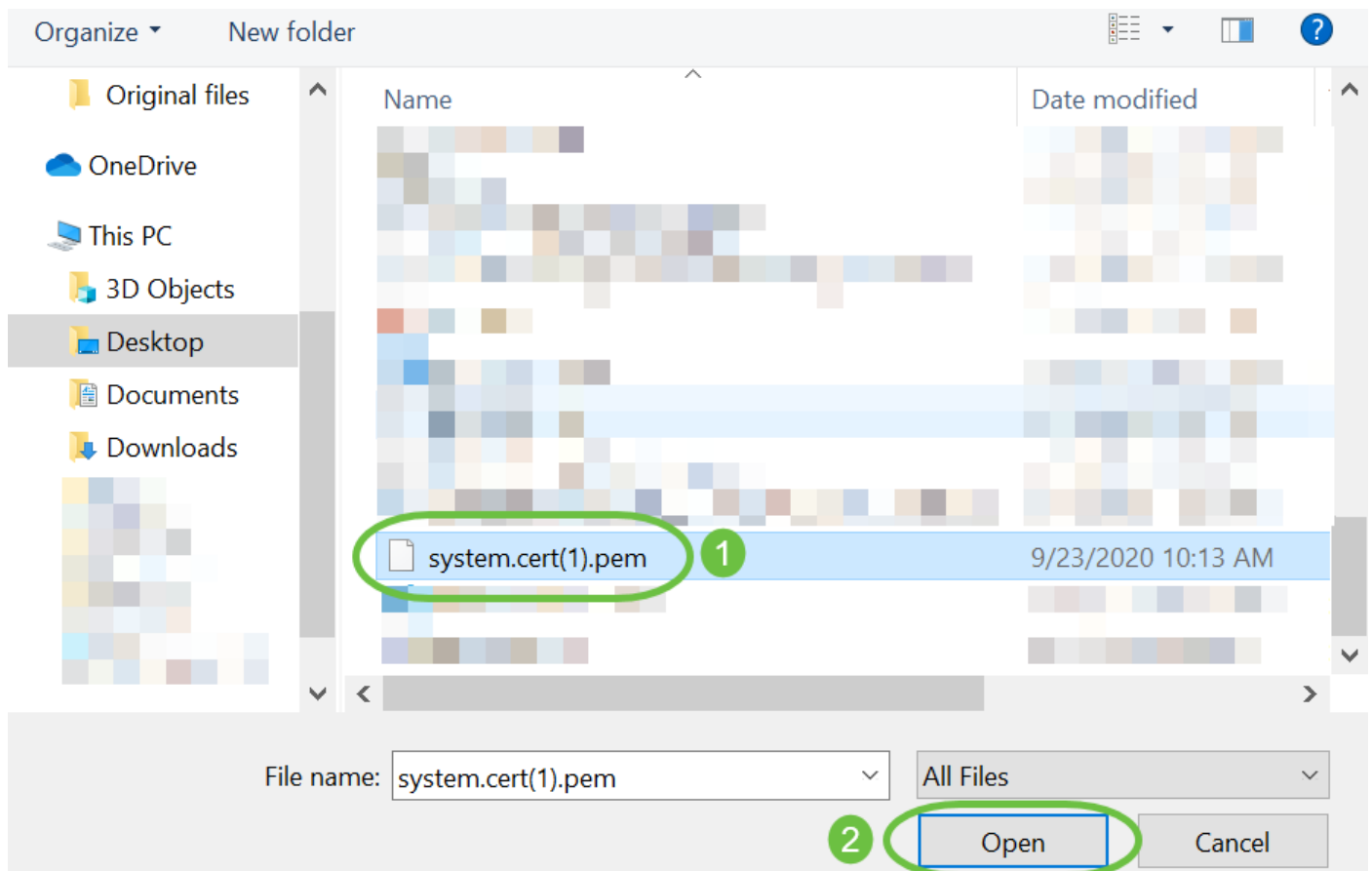
Current Certificate **Update Certificate** CSR

Renew Self-signed Cert  Upload Cert  Upload PKCS12

Password

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

Passaggio 3. Eliminare il certificato firmato nell'area di destinazione oppure fare clic sull'area di destinazione per esplorare il file system, quindi fare clic su **Apri**. Il file deve essere in formato .pem.




Passaggio 4. Fare clic su **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



Caricamento di un certificato firmato in Cisco Business Dashboard Network Manager completato.

### Gestisci certificato corrente

Passaggio 1. Accedere alla GUI di amministrazione di Cisco Business Dashboard, quindi scegliere **Sistema > Certificato**.

# Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

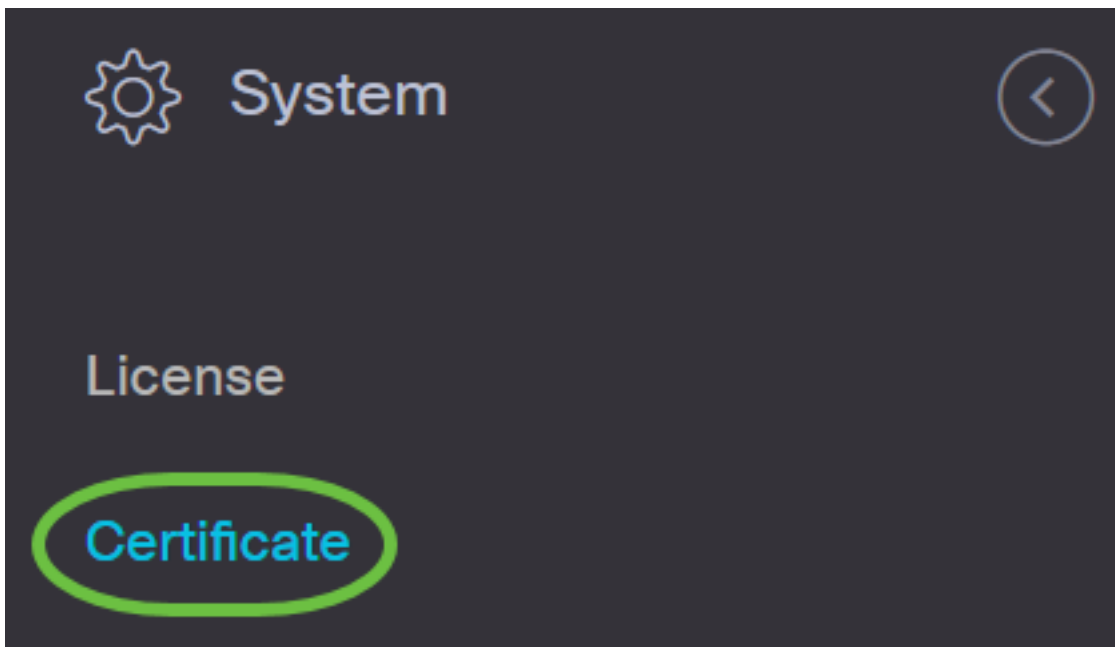


Administration



System





Passaggio 2. Passare alla scheda *Certificato corrente*. Il certificato corrente verrà visualizzato in formato testo normale.

## 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)

Passaggio 3. (Facoltativo) Per scaricare una copia del certificato corrente, fare clic sul pulsante

## Scarica.

### 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](#)

Il certificato corrente in Cisco Business Dashboard è stato gestito correttamente.

Per ulteriori informazioni sui certificati, vedere gli articoli seguenti:

- [Utilizzo di Let's Encrypt Certificates con Cisco Business Dashboard](#)
- [Utilizzo di Let's Encrypt Certificates con Cisco Business Dashboard e la convalida DNS](#)