

Gérer les certificats sur le tableau de bord Cisco Business

Objectif

Un certificat numérique certifie la propriété d'une clé publique par l'objet nommé du certificat. Cela permet aux parties de confiance de dépendre des signatures ou des assertions faites par la clé privée qui correspond à la clé publique qui est certifiée. Lors de l'installation, le tableau de bord Cisco Business génère un certificat auto-signé pour sécuriser les communications Web et autres avec le serveur. Vous pouvez choisir de remplacer ce certificat par celui signé par une autorité de certification (CA) de confiance. Pour ce faire, vous devez générer une demande de signature de certificat (CSR) pour la signature par l'autorité de certification.

Vous pouvez également choisir de générer un certificat et la clé privée correspondante complètement indépendante du tableau de bord. Si c'est le cas, vous pouvez combiner le certificat et la clé privée dans un fichier au format PKCS (Public Key Cryptography Standards) n° 12 avant le téléchargement.

Le tableau de bord Cisco Business ne prend en charge que les certificats au format .pem. Si vous obtenez d'autres formats de certificat, vous devez convertir à nouveau le format ou la demande du certificat au format .pem à partir de l'autorité de certification.

Cet article explique comment gérer les certificats sur Cisco Business Dashboard Network Manager.

Version logicielle applicable

- DBC ([fiche technique](#)) | 2.2 ([Télécharger la dernière version](#))

Gérer les certificats sur le tableau de bord Cisco Business

Générer une requête de signature de certificat (CSR)

Étape 1. Connectez-vous à l'interface utilisateur d'administration de votre tableau de bord Cisco Business, puis sélectionnez **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

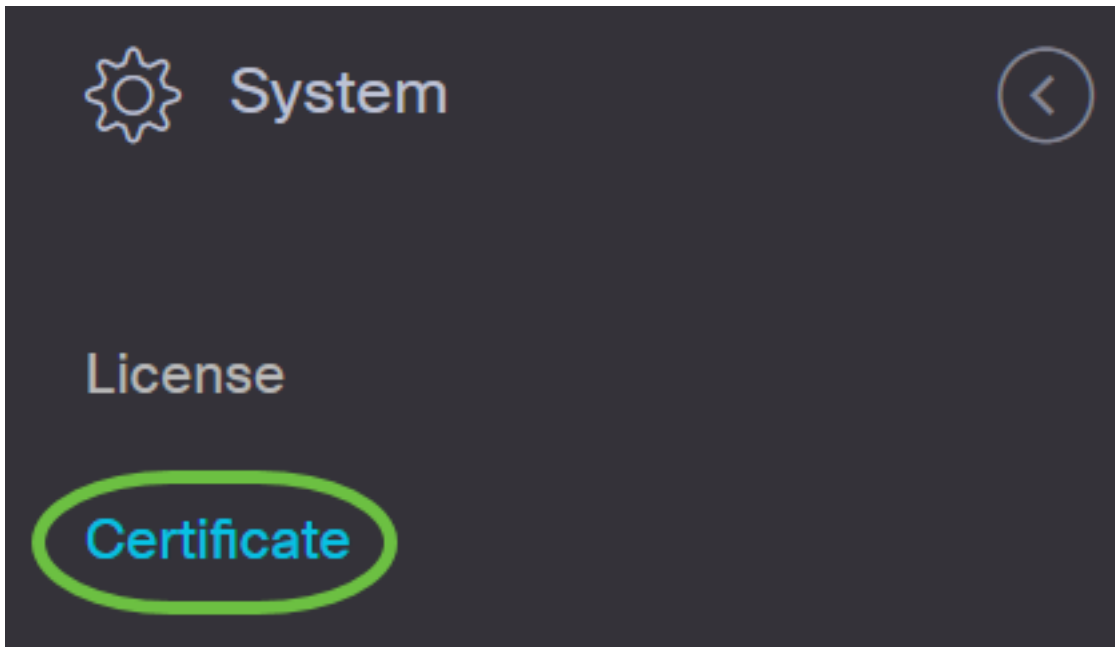


Administration



System





Étape 2. Dans l'onglet *CSR*, saisissez les valeurs appropriées dans les champs fournis dans le formulaire affiché. Ces valeurs seront utilisées pour construire le CSR et seront contenues dans le certificat signé que vous recevez de l'AC. Cliquez **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

Le fichier CSR sera automatiquement téléchargé sur votre ordinateur.

Étape 3. (Facultatif) Pour télécharger une copie du certificat actuel, cliquez sur le bouton **Télécharger**.

Certificate

Current Certificate

Update Certificate

CSR

CSR: Created

A blue rectangular button with the text "Download" in white, circled in green.

Étape 4. (Facultatif) Pour mettre à jour le CSR créé, accédez à l'onglet *Mettre à jour le certificat* et choisissez l'option **Renouveler le certificat auto-signé**. Effectue les modifications souhaitées dans les champs et cliquez sur **Enregistrer**.

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

Vous avez maintenant généré une demande de service de contact sur votre tableau de bord Cisco Business. Vous pouvez maintenant envoyer le fichier CSR téléchargé à l'autorité de certification.

Télécharger un certificat signé de l'autorité de certification

Une fois que vous avez reçu le CSR signé de la CA, vous pouvez le télécharger sur le tableau de bord.

Étape 1. Connectez-vous à l'interface utilisateur d'administration de votre tableau de bord Cisco Business, puis sélectionnez **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

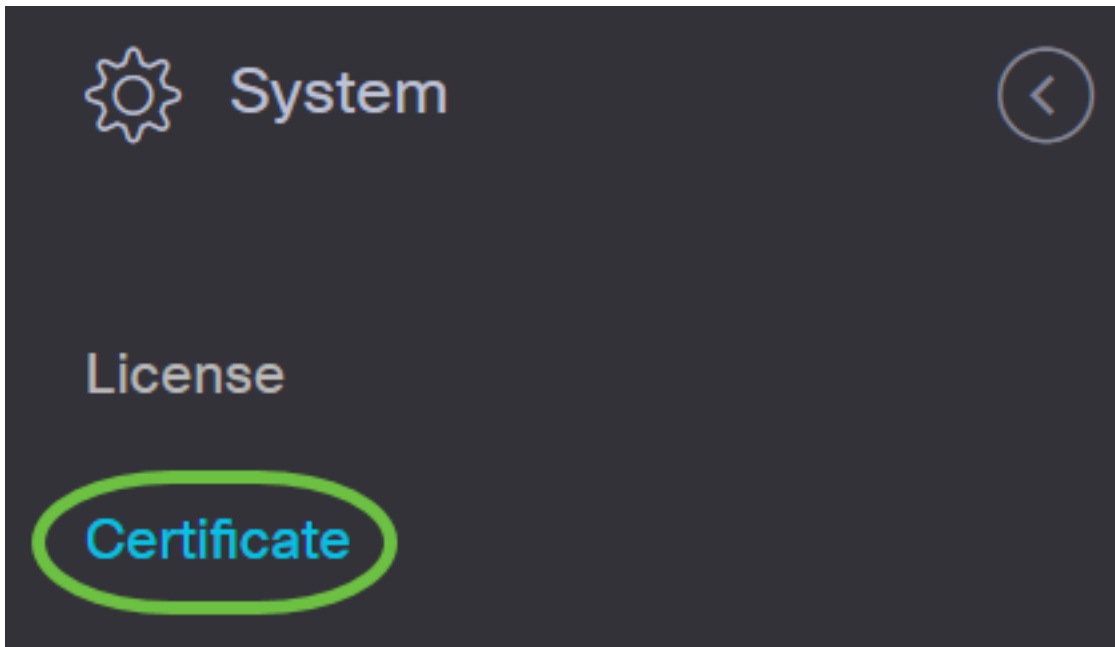


Administration

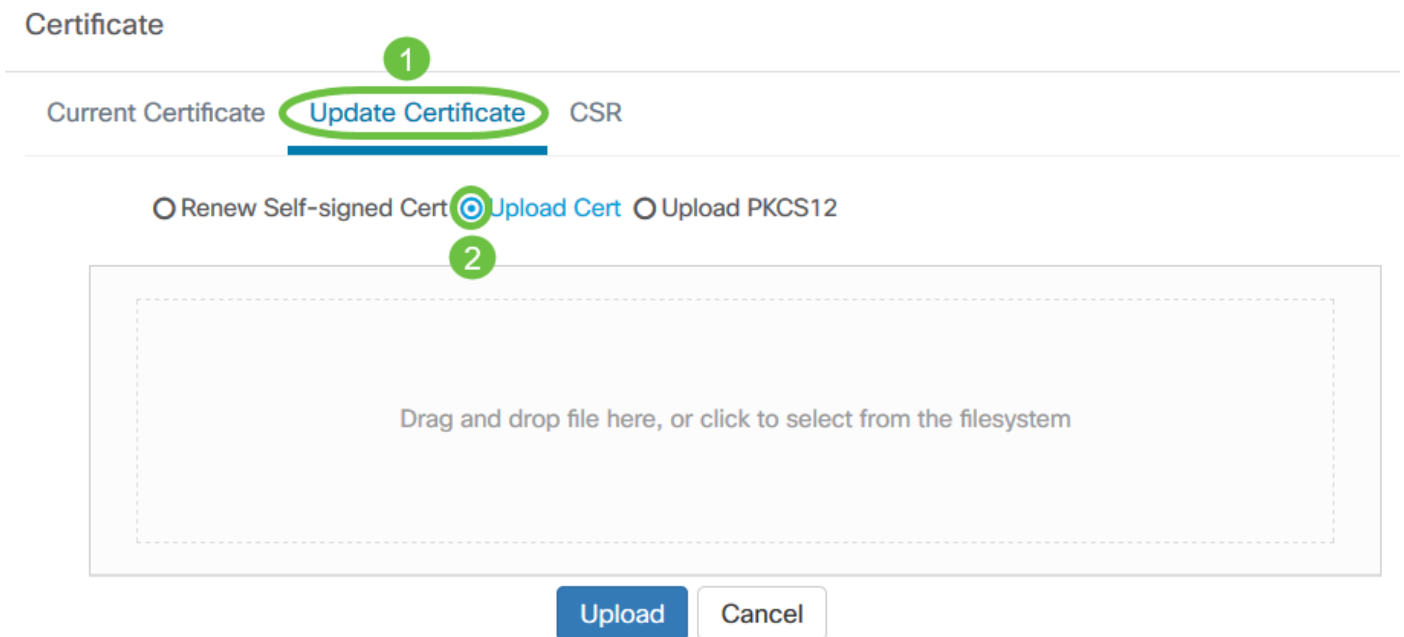


System





Étape 2. Dans l'onglet *Mettre à jour le certificat*, sélectionnez la case d'option **Télécharger le certificat**.



Note: Vous pouvez également télécharger un certificat avec la clé privée associée au format PKCS#12 en sélectionnant la case d'option **Upload PKCS12**. Le mot de passe pour déverrouiller le fichier doit être spécifié dans le champ *Mot de passe* fourni.

Certificate

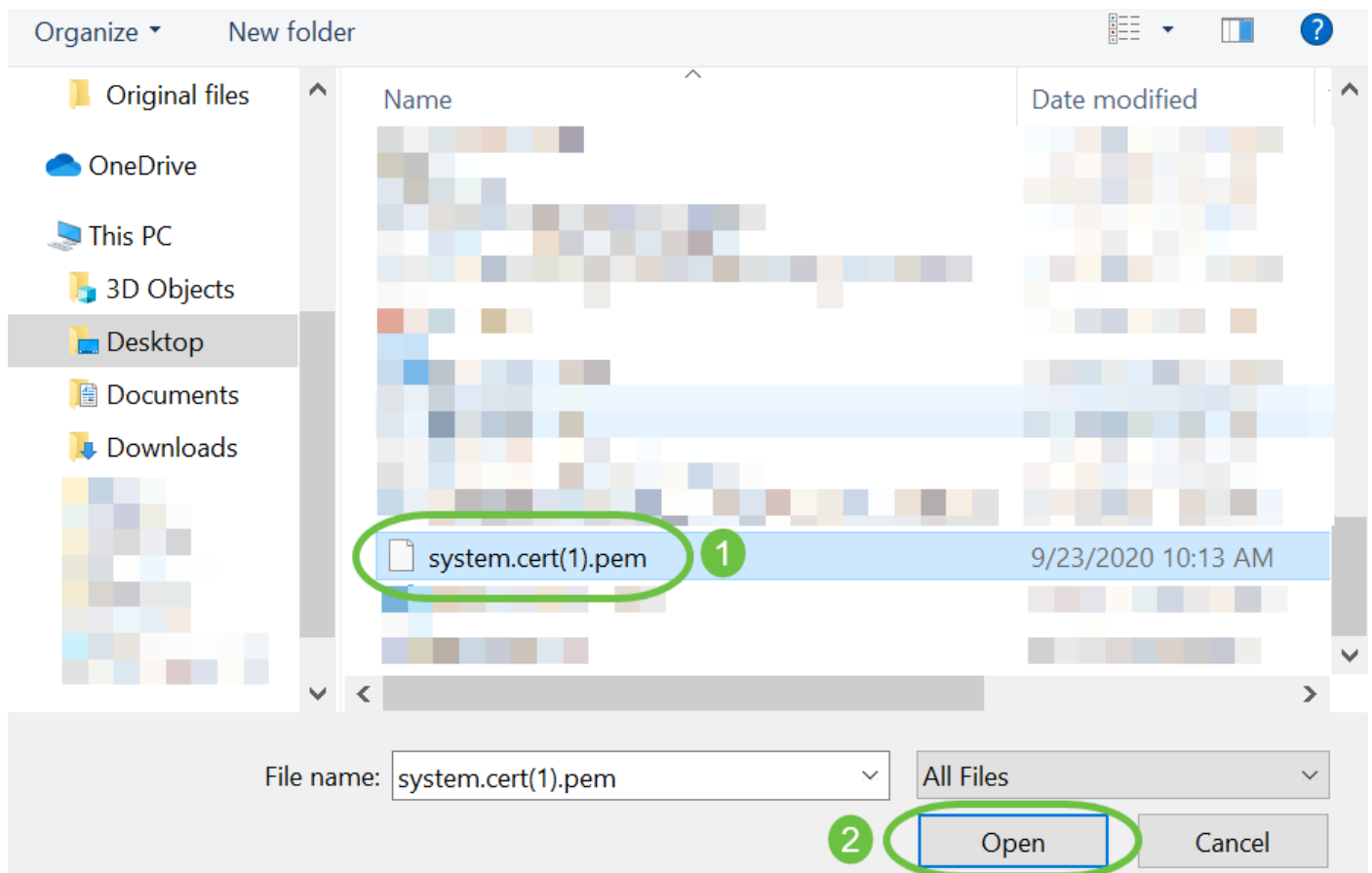
Current Certificate **Update Certificate** CSR

Renew Self-signed Cert Upload Cert Upload PKCS12

Password

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

Étape 3. Supprimez le certificat signé dans la zone cible ou cliquez sur la zone cible pour parcourir le système de fichiers, puis cliquez sur **Ouvrir**. Le fichier doit être au format .pem.




Étape 4. Cliquez sur **Upload** (charger).

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



Vous avez maintenant téléchargé un certificat signé dans Cisco Business Dashboard Network Manager.

Gérer le certificat actuel

Étape 1. Connectez-vous à l'interface utilisateur d'administration de votre tableau de bord Cisco Business, puis sélectionnez **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

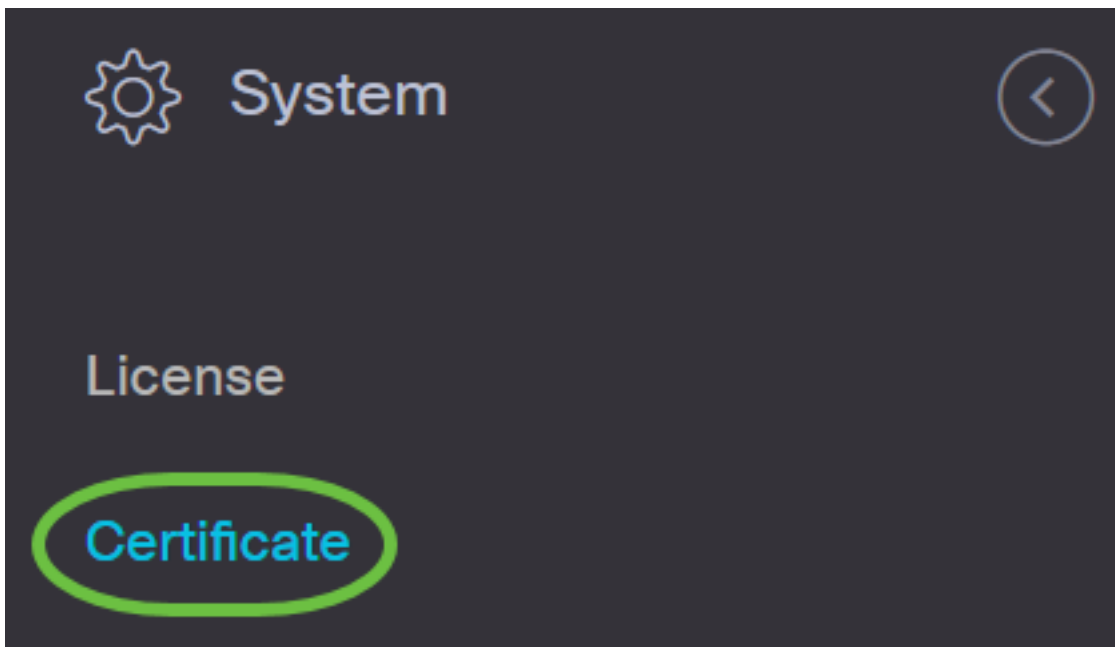


Administration



System





Étape 2. Accédez à l'onglet *Certificat actuel*. Le certificat actuel s'affiche en texte brut.

Certificate



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)
```

Étape 3. (Facultatif) Pour télécharger une copie du certificat actuel, cliquez sur le bouton **Télécharger**.

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](#)

Vous avez maintenant réussi à gérer le certificat actuel sur votre tableau de bord Cisco Business.

Pour plus d'informations sur les certificats, consultez les articles suivants :

- [Utilisation de Chiffons les certificats avec le tableau de bord Cisco Business](#)
- [Utilisation du chiffrement des certificats avec le tableau de bord Cisco Business et la validation DNS](#)