

Gestión de certificados en el panel empresarial de Cisco

Objetivo

Un certificado digital certifica la propiedad de una clave pública por el sujeto designado del certificado. Esto permite que las partes que confían en ellas dependan de las firmas o afirmaciones hechas por la clave privada que corresponde a la clave pública certificada. Tras la instalación, Cisco Business Dashboard genera un certificado autofirmado para proteger la Web y otras comunicaciones con el servidor. Puede elegir reemplazar este certificado por el firmado por una autoridad de certificación (CA) de confianza. Para ello, deberá generar una solicitud de firma de certificado (CSR) para que la CA la firme.

También puede optar por generar un certificado y la clave privada correspondiente completamente independiente del Panel. Si es así, puede combinar el certificado y la clave privada en un archivo de formato de estándares criptográficos de clave pública (PKCS) nº 12 antes de la carga.

Cisco Business Dashboard sólo admite certificados con formato .pem. Si obtiene otros formatos de certificado, debe volver a convertir el formato o solicitar el certificado de formato .pem de la CA.

En este artículo se proporcionan instrucciones sobre cómo administrar certificados en Cisco Business Dashboard Network Manager.

Versión de software aplicable

- CBD ([Ficha técnica](#)) | 2.2 ([Descargar la última](#))

Gestión de certificados en Cisco Business Dashboard

Generar una CSR

Paso 1. Inicie sesión en la GUI de administración de su Cisco Business Dashboard y luego elija **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

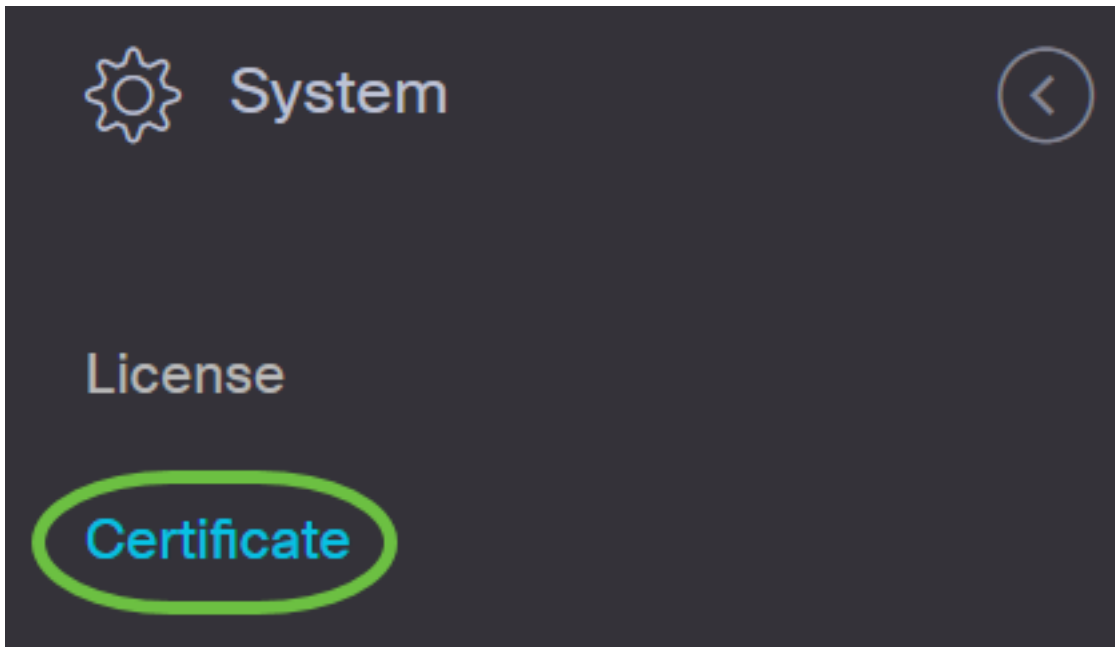


Administration



System





Paso 2. En la ficha *CSR*, introduzca los valores adecuados en los campos proporcionados en el formulario que se muestra. Estos valores se utilizarán para construir la CSR y se incluirán en el certificado firmado que reciba de la CA. Haga clic en Crear.

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

El archivo CSR se descargará automáticamente en el ordenador.

Paso 3. (Opcional) Para descargar una copia del certificado actual, haga clic en el botón **Descargar**.

Certificate

Current Certificate

Update Certificate

CSR

CSR: Created

Download

Paso 4. (Opcional) Para actualizar la CSR creada, navegue a la pestaña *Update Certificate* y elija la opción **Renew Self-signed Cert.** Realice los cambios deseados en los campos y haga clic en **Guardar.**

Certificate

1

Current Certificate **Update Certificate** CSR

2 Renew Self-signed Cert Upload Cert Upload PKCS12

Common Name ✓

Country/region ▾

State ✓

City ✓

3 Org ✓

Org Units ✓

Start Date - End Date

Email ✓

Subject Alternative Name ✓

4

Ya ha generado correctamente una CSR en su panel empresarial de Cisco. Ahora puede enviar el archivo CSR descargado a la CA.

Cargar un certificado firmado desde la CA

Una vez que reciba la CSR firmada de la CA, ahora puede cargarla en el panel.

Paso 1. Inicie sesión en la GUI de administración de su Cisco Business Dashboard y luego elija **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

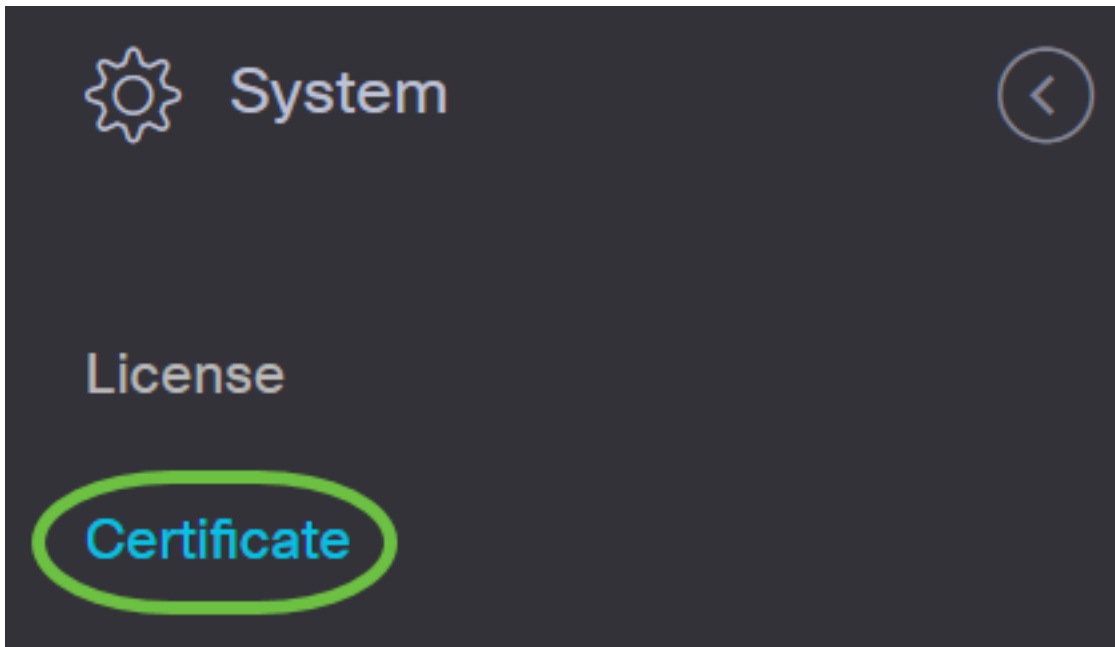


Administration

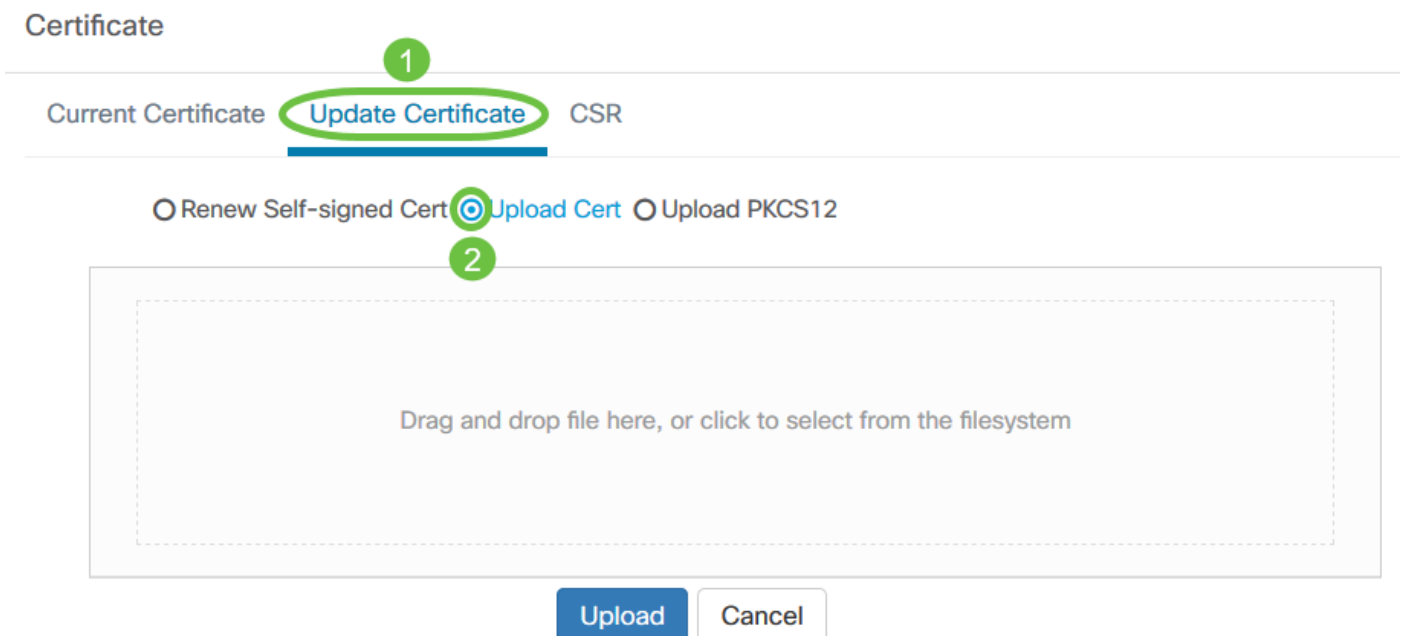


System





Paso 2. En la pestaña *Actualizar certificado*, elija el botón de opción **Cargar certificado**.



Nota: Alternativamente, puede cargar un certificado con la clave privada asociada en formato PKCS#12 eligiendo el botón de opción **Cargar PKCS12**. La contraseña para desbloquear el archivo debe especificarse en el campo *Password* proporcionado.

Certificate

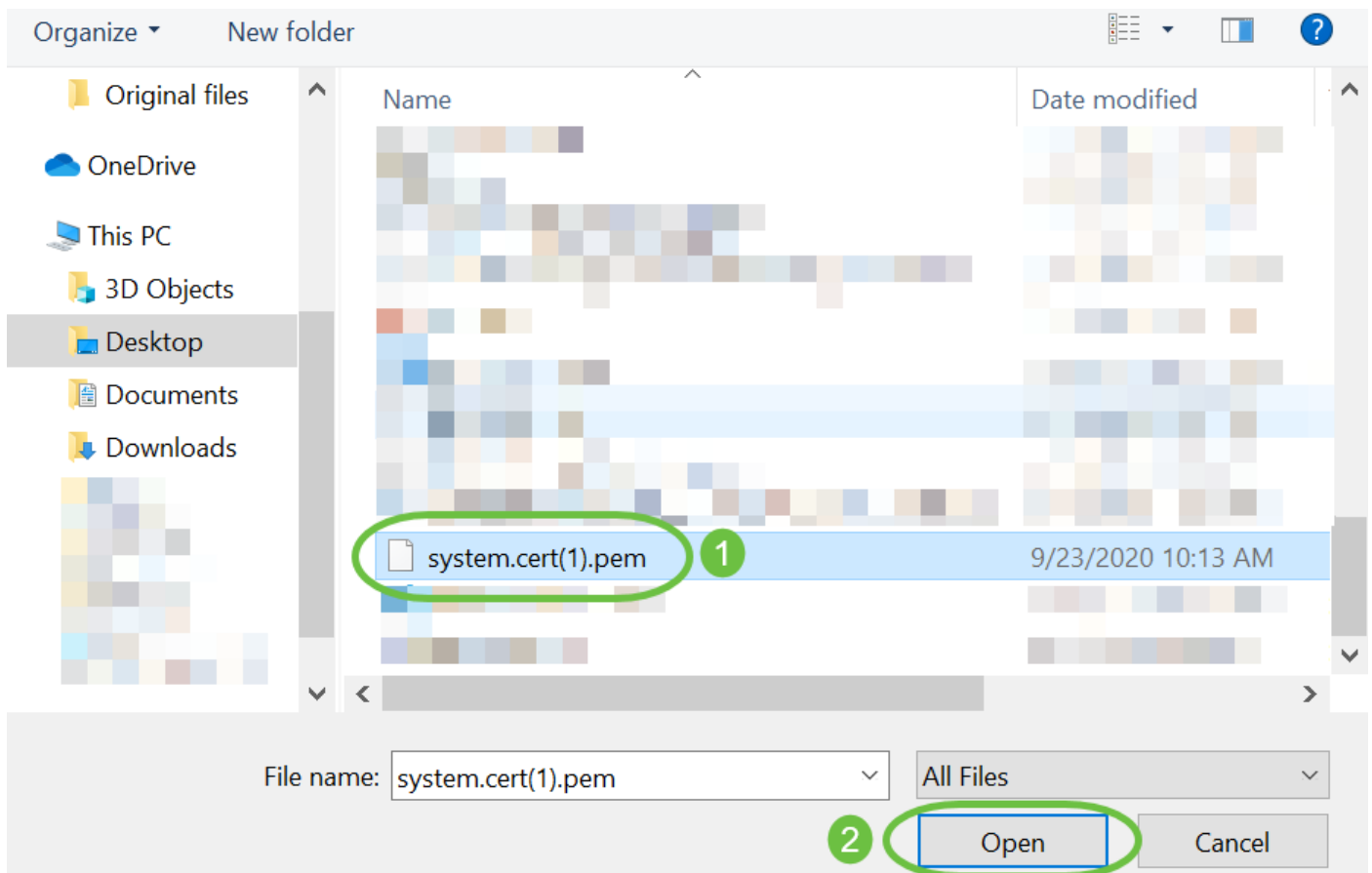
Current Certificate **Update Certificate** CSR

Renew Self-signed Cert Upload Cert Upload PKCS12

Password

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

Paso 3. Suelte el certificado firmado en el área de destino o haga clic en el área de destino para navegar por el sistema de archivos y luego haga clic en **Abrir**. El archivo debe estar en formato .pem.




Paso 4. Haga clic en **Cargar**.

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



Ha cargado correctamente un certificado firmado en Cisco Business Dashboard Network Manager.

Administrar certificado actual

Paso 1. Inicie sesión en la GUI de administración de su Cisco Business Dashboard y luego elija **System > Certificate**.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports

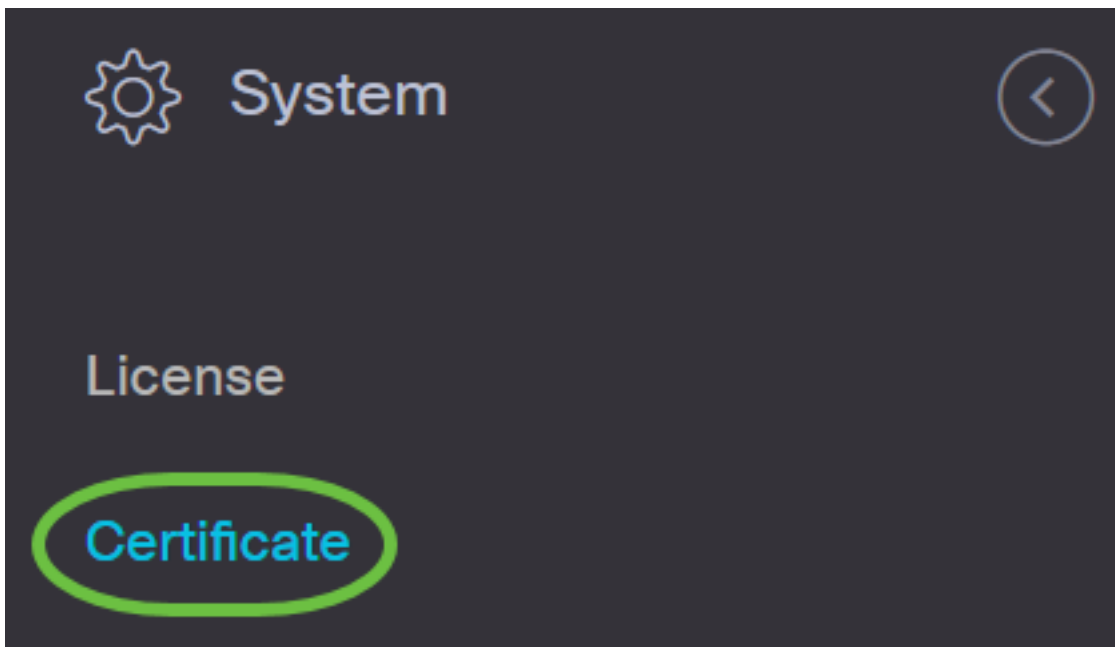


Administration



System





Paso 2. Vaya a la pestaña *Certificado actual*. El certificado actual se mostrará en formato de texto sin formato.

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)
```

Paso 3. (Opcional) Para descargar una copia del certificado actual, haga clic en el botón

Descargar.

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:
```



Ya ha gestionado correctamente el certificado actual en su panel empresarial de Cisco.