

Verwalten von Zertifikaten auf dem Cisco Business Dashboard

Ziel

Ein digitales Zertifikat bescheinigt, dass der benannte Subjekt des Zertifikats Eigentümer eines öffentlichen Schlüssels ist. Dies ermöglicht vertrauenden Parteien, sich auf Signaturen oder Assertionen des privaten Schlüssels zu verlassen, der dem zertifizierten öffentlichen Schlüssel entspricht. Nach der Installation generiert das Cisco Business Dashboard ein selbstsigniertes Zertifikat, um die Web- und andere Kommunikation mit dem Server zu sichern. Sie können dieses Zertifikat durch das von einer vertrauenswürdigen Zertifizierungsstelle (Certificate Authority, CA) signierte Zertifikat ersetzen. Dazu müssen Sie eine Zertifikatssignierungsanforderung (Certificate Signing Request, CSR) für die Signierung durch die Zertifizierungsstelle erstellen.

Sie können auch ein Zertifikat und den zugehörigen privaten Schlüssel völlig unabhängig vom Dashboard generieren. In diesem Fall können Sie das Zertifikat und den privaten Schlüssel vor dem Hochladen in eine Datei im Format Public Key Cryptography Standards (PKCS) #12 kombinieren.

Das Cisco Business Dashboard unterstützt nur Zertifikate im PEM-Format. Wenn Sie andere Zertifikatformate erhalten, müssen Sie das Format konvertieren oder das Zertifikat im Format .pem von der Zertifizierungsstelle erneut anfordern.

Dieser Artikel enthält Anweisungen zum Verwalten von Zertifikaten im Cisco Business Dashboard Network Manager.

Anwendbare Softwareversion

- CBD ([Datenblatt](#)) | 2.2 (Aktuelle Version herunterladen)

Verwalten von Zertifikaten auf dem Cisco Business Dashboard

CSR erstellen

Schritt 1: Melden Sie sich in der Verwaltungs-GUI Ihres Cisco Business Dashboards an, und wählen Sie dann System > Certificate.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports





System



License

Certificate

Schritt 2: Geben Sie auf der Registerkarte CSR entsprechende Werte in die Felder ein, die im angezeigten Formular enthalten sind. Diese Werte werden zum Erstellen des CSR verwendet und sind in dem signierten Zertifikat enthalten, das Sie von der Zertifizierungsstelle erhalten. Klicken Sie auf Erstellen.

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

Die CSR-Datei wird automatisch auf Ihren Computer heruntergeladen.

Schritt 3: (Optional) Um eine Kopie des aktuellen Zertifikats herunterzuladen, klicken Sie auf die Schaltfläche Herunterladen.

Certificate

Current Certificate

Update Certificate

CSR

CSR: Created

Download

Schritt 4: (Optional) Um den erstellten CSR zu aktualisieren, navigieren Sie zur Registerkarte Update Certificate (Zertifikat aktualisieren), und wählen Sie die Option Renew Self-signed Certificate (Selbstsigniertes Zertifikat erneuern). Nehmen Sie die gewünschten Änderungen an den Feldern vor, und klicken Sie auf Speichern.

Certificate

1 **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

Sie haben jetzt erfolgreich eine CSR-Anfrage für Ihr Cisco Business Dashboard erstellt. Sie können nun die heruntergeladene CSR-Datei an die CA senden.

Hochladen eines signierten Zertifikats von der Zertifizierungsstelle

Sobald Sie die signierte CSR-Anfrage von der Zertifizierungsstelle erhalten haben, können Sie sie in das Dashboard hochladen.

Schritt 1: Melden Sie sich in der Verwaltungs-GUI Ihres Cisco Business Dashboards an, und

wählen Sie dann System > Certificate.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play

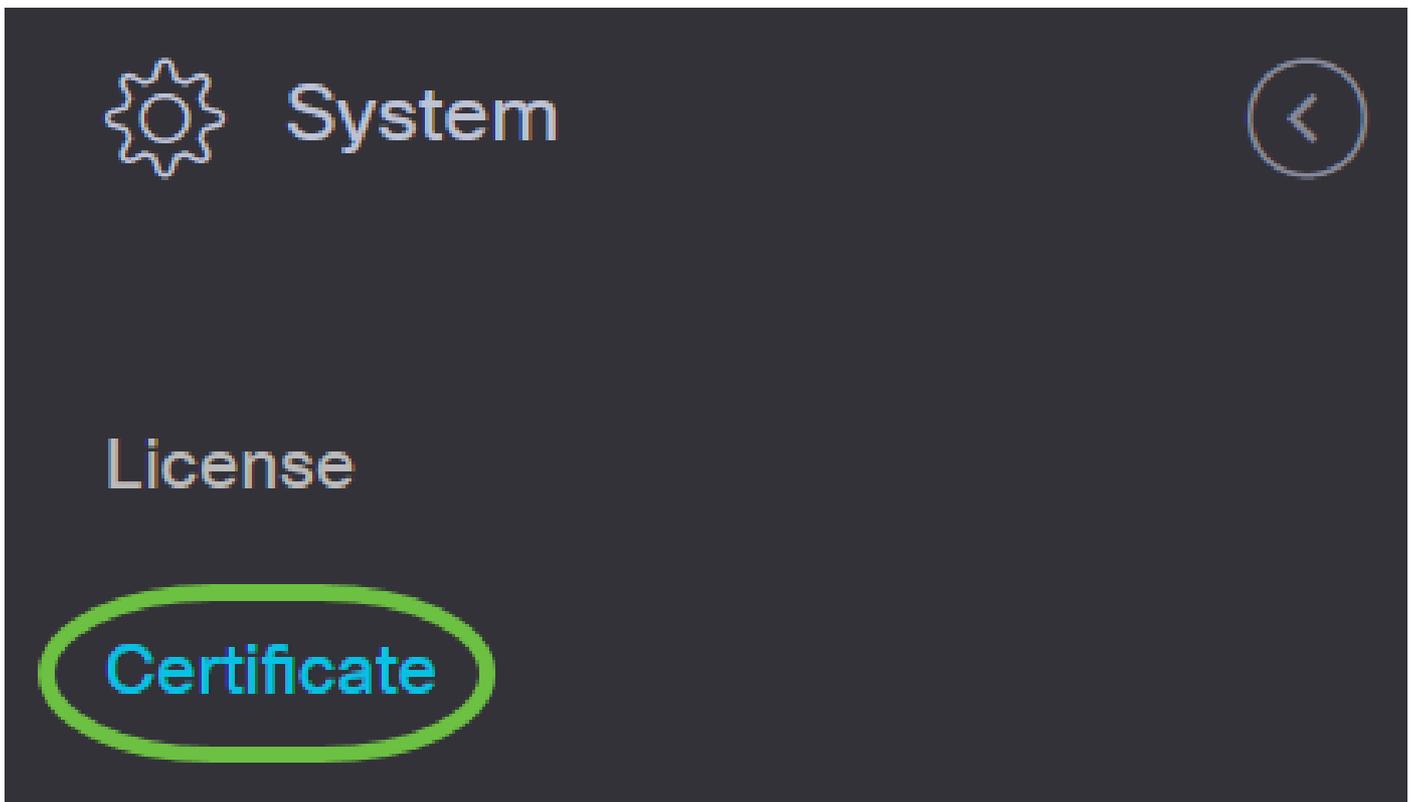


Event Log

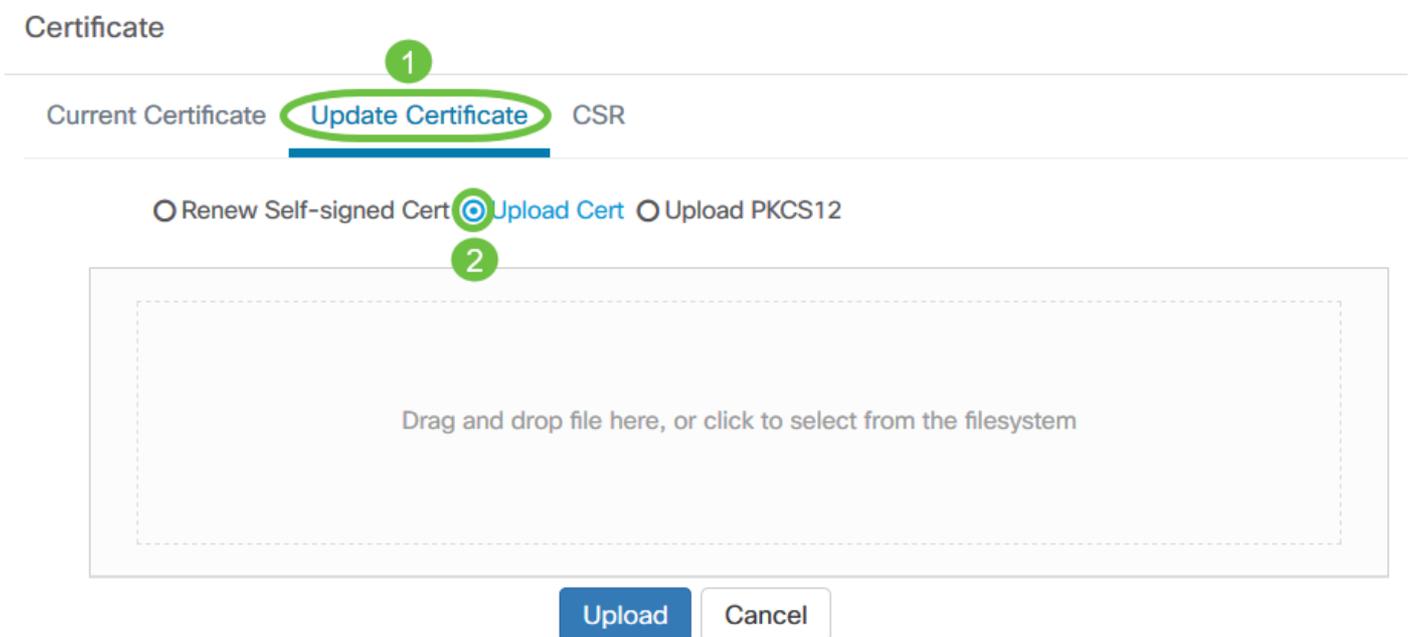


Reports





Schritt 2: Wählen Sie auf der Registerkarte Zertifikat aktualisieren das Optionsfeld Zertifikat hochladen.



Anmerkung: Alternativ können Sie ein Zertifikat mit dem zugehörigen privaten Schlüssel im PKCS#12-Format hochladen, indem Sie das Optionsfeld PKCS12 hochladen auswählen. Das Kennwort zum Entsperren der Datei muss im bereitgestellten Feld Kennwort angegeben werden.

Certificate

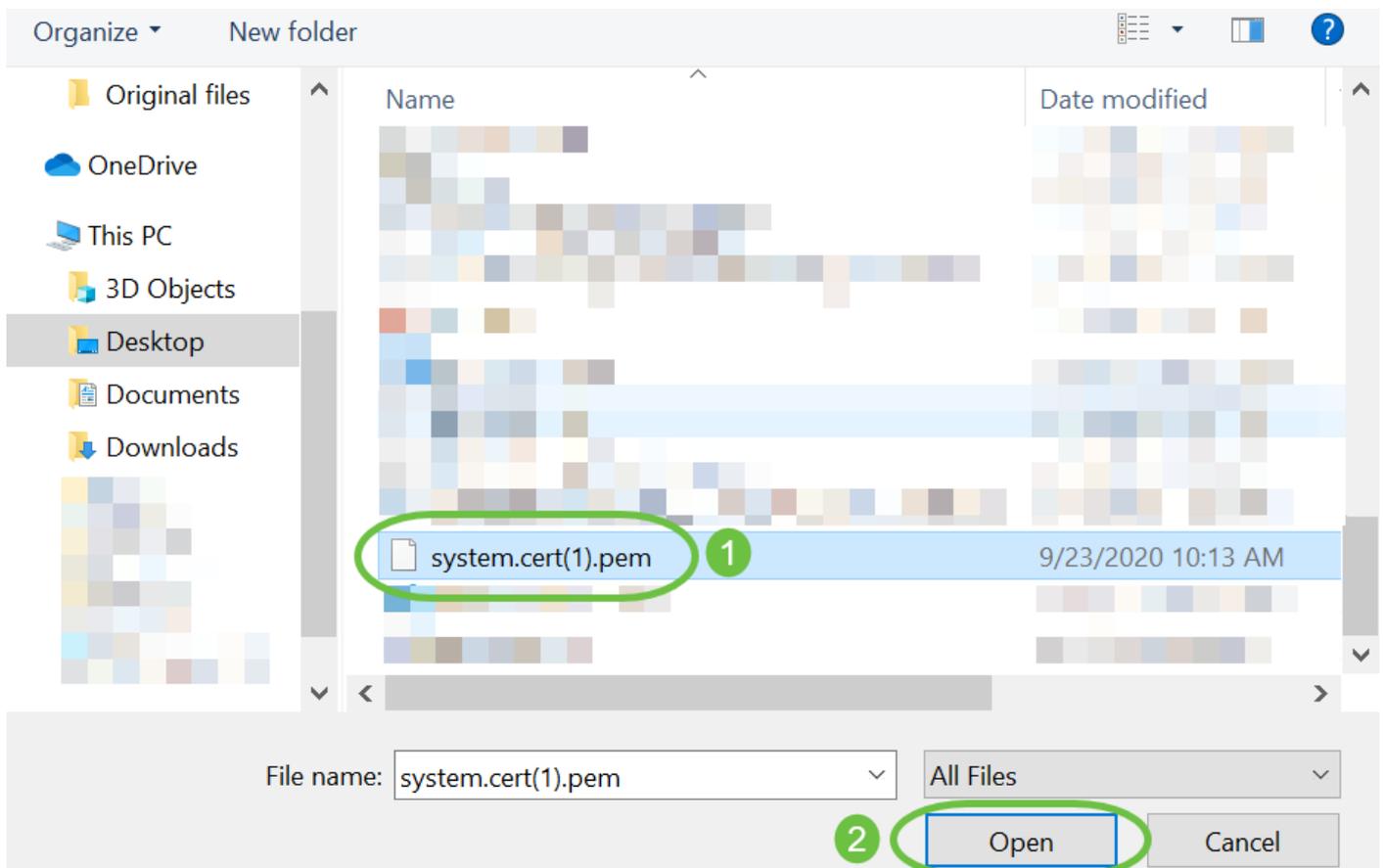
Current Certificate **Update Certificate** CSR

Renew Self-signed Cert Upload Cert Upload PKCS12

Password

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

Schritt 3: Legen Sie das signierte Zertifikat im Zielbereich ab, oder klicken Sie auf den Zielbereich, um das Dateisystem zu durchsuchen, und klicken Sie dann auf Öffnen. Die Datei sollte das Format .pem haben.



Schritt 4: Klicken Sie auf Hochladen.

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



Sie haben jetzt erfolgreich ein signiertes Zertifikat in den Cisco Business Dashboard Network Manager hochgeladen.

Aktuelles Zertifikat verwalten

Schritt 1: Melden Sie sich in der Verwaltungs-GUI Ihres Cisco Business Dashboards an, und wählen Sie dann System > Certificate.

Cisco Business Dashboard



Dashboard



Network



Inventory



Port Management



Network Configuration



Network Plug and Play



Event Log



Reports





System



License

Certificate

Schritt 2: Navigieren Sie zur Registerkarte Aktuelles Zertifikat. Das aktuelle Zertifikat wird im Nur-Text-Format angezeigt.

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)

Schritt 3: (Optional) Um eine Kopie des aktuellen Zertifikats herunterzuladen, klicken Sie auf die Schaltfläche Herunterladen.

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](#)

Sie haben jetzt das aktuelle Zertifikat in Ihrem Cisco Business Dashboard erfolgreich verwaltet.

Weitere Informationen zu Zertifikaten finden Sie in den folgenden Artikeln:

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

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.