

Zertifikatsverlängerung für SD-WAN-Controller über manuelle Methode aktivieren

Inhalt

[Einleitung](#)

[Verfügbare Methoden](#)

[Anforderungen](#)

[Verlängerungsprozess](#)

[Cisco \(empfohlen\)](#)

[Manuell \(PnP\)](#)

[Häufige Probleme](#)

[Zeit stimmt nicht überein](#)

[Verbindung kann nicht hergestellt werden](#)

Einleitung

In diesem Dokument werden die Schritte zur Verlängerung des SD-WAN-Zertifikats auf den Controllern mithilfe der Cisco- oder manuellen Methode beschrieben.

Verfügbare Methoden

Für die Controller-Zertifikatsautorisierung stehen vier verschiedene Optionen zur Verfügung.

- Cisco (empfohlen) - Halbautomatisierter Prozess, der das Cisco Plug and Play (PnP)-Portal verwendet, um die vom vManage generierte CSR zu signieren und automatisch herunterzuladen und zu installieren.
- Manuell - Manuelle Zertifikatssignatur über Cisco PnP.
- Symantec - Manuelle Drittanbieter-Zertifikatssignatur über Symantec/Digicert.
- Enterprise Root Certificate - Manuelles Zertifikatszeichen durch eine private Root Certificate Authority (CA).


In diesem Dokument werden nur die Schritte für die Cisco-Methoden (empfohlen) und Manual (Manuell) beschrieben.



Achtung: Die in diesem Dokument behandelten Zertifikate haben nichts mit dem Webzertifikat für vManage zu tun.

Anforderungen

- Einen PC/Laptop.
- Ein Netadmin-Konto für die vManage-GUI und für jeden Controller (vManage, vSmart und vBond).
- Zugriff auf den CA-Server.
- Für Cisco (empfohlen) oder Manual: ein gültiges Konto/Kennwort für das PnP-Portal.
- Für Cisco (empfohlen) muss vManage über einen Internetzugang verfügen.
- Alle Controller benötigen einen gültigen NTP-Server, und/oder alle Controller müssen das richtige Datum und die richtige Uhrzeit aufweisen.
- Kommunikation zwischen vBond und vSmart mit vManage.

 Hinweis: Die Zertifikatsinstallation in vManage hat keine Auswirkungen auf Ihre Kontroll- oder Datenebene. Für das Zertifikat im vSmart können die Steuerverbindungen betroffen sein. Die Kontrollebene funktioniert dank OMP graceful timer weiter. Um eine Zertifikatänderung durchzuführen, müssen Sie ein Wartungsfenster für die Aktivität planen.

Verlängerungsprozess

Hierbei handelt es sich um ein Verfahren auf hoher Ebene:

1. Identifizieren Sie die in der grafischen Benutzeroberfläche von vManage verwendete Option zur Autorisierung von Controller-Zertifikaten.
2. Erstellen einer neuen CSR-Anfrage über die Benutzeroberfläche von vManage
3. Erstellen Sie ein neues Zertifikat.
4. Laden Sie das Zertifikat herunter.
5. Installieren Sie das Zertifikat.

Cisco (empfohlen)

1. Navigieren Sie zu vManage > Administration > Settings > Certificate Authority Server.
 - Vergewissern Sie sich, dass die richtige Option ausgewählt ist.
 - Wählen Sie die Dauer des Zertifikats aus.

Administration Settings

Controller Certificate Authorization

Manual

Certificate Signing by: Cisco (Recommended) Symantec Manual Enterprise Root Certificate

Sync Root Certificate (Please sync root cert to all connected devices before saving Cisco PKI mechanism)

Validity Period

1 Year

Certificate Retrieve Interval

60 min

Save

Cancel

2. Blättern Sie nach unten zu Smart Account-Anmeldeinformationen, und stellen Sie ein gültiges Benutzer-/Kennwort vor. Die Anmeldedaten müssen Zugriff auf den Smart Account haben, in dem das SD-WAN-Overlay konfiguriert ist, wie im Bild gezeigt.

Administration Settings

Smart Account Credentials

Username

egarcial@cisco.com

Password

.....

Save

Cancel

3. Navigieren Sie zu vManage > Configuration > Certificates > Controllers.

- Wählen Sie die Auslassungszeichen (..) auf dem Controller (vBond, vSmart oder vManage).
- Wählen Sie CSR erstellen aus.

Install Certificate

WAN Edge List Controllers TLS Proxy

Send to vBond

Search

Total Rows: 3

Operation Status	Controller Type	Hostname	System IP	Site ID	Certificate Serial	Expiration
CSR Generated	vBond	--	--	--	No certificate installed	--
vBond Updated	vSmart	vSmart_206_egarcial	10.10.10.3	1	150FB2DD940112BEA5...	
vBond Updated	vManage	vmanage_206_egar...	10.10.10.1	1	70783C76A1B6B233D5...	

- View CSR
- View Certificate
- Generate CSR
- Reset RSA
- Invalidate

4. Fünf bis zwanzig Minuten sind erforderlich, damit der Prozess abgeschlossen werden kann.

Überprüfen Sie, ob die Installation in GUI vManage > Configuration > Certificates > Controllers korrekt war.

Install Certificate

WAN Edge List Controllers TLS Proxy

Send to vBond

Search

Total Rows: 3

Controller Type	Hostname	System IP	Expiration Date	uuid	Operation Status	Site ID
vBond	vBond_206_egarcial	10.10.10.2	25 Dec 2024 2:00:42 PM CST	96f5b...	Installed	1
vSmart	vSmart_206_egarcial	10.10.10.3	20 Dec 2024 3:18:21 PM CST	f0269...	vBond Updated	1
vManage	vmanage_206_egar...	10.10.10.1	20 Dec 2024 3:01:02 PM CST	1f585...	vBond Updated	1

Manuell (PnP)

1. Navigieren Sie zu vManage > Administration > Settings > Certificate Authority Server

- Vergewissern Sie sich, dass die richtige Option ausgewählt ist.

2. Navigieren Sie zu vManage > Configuration > Certificates > Controllers.

- Wählen Sie die Auslassungszeichen (...) auf dem Controller aus (vBond, vSmart oder vManage).
- Wählen Sie CSR erstellen aus.
- Kopieren und speichern Sie den gesamten Text in einer temporären Datei.

3. Greifen Sie auf das PnP-Portal zu, wählen Sie Ihr SD-WAN-Overlay aus, und navigieren Sie zu den Zertifikaten, wie im Bild gezeigt.

The screenshot shows the Cisco Software Central interface. At the top, there is a navigation bar with the Cisco logo and a search icon. Below the navigation bar, the main content area is titled 'Plug and Play Connect'. On the right side, there is a section for 'Account and Virtual Account' with two dropdown menus: 'CISCO SDWAN' and 'SDWAN', both highlighted with red boxes. Below this, there is a breadcrumb trail: 'Cisco Software Central > Plug and Play Connect'. The main content area has several tabs: 'Devices', 'Controller Profiles', 'Network', 'Certificates' (highlighted with a red box), 'Manage External Virtual Account', 'Event Log', and 'Transactions'. Below the tabs, there is a toolbar with buttons: '+ Add Profile...', 'Edit Selected...', 'Delete Selected...', 'Make Default...', and 'Show Log...'. Below the toolbar, there is a table with the following columns: 'Profile Name', 'Controller Type', 'Default', 'Description', 'Used By', and 'Download'. The table contains one record: 'VBOND-LAB-MX' with 'VBOND' as the Controller Type, a checkmark in the Default column, 'VBOND-LAB-MX' as the Description, '32' in the Used By column, and a 'Provisioning File' link in the Download column. At the bottom right of the table, it says 'Showing 1 Record'.

4. Klicken Sie im Abschnitt Zertifikate auf Neues Zertifikat generieren, und geben Sie alle Informationen ein.

- Geben Sie auf Zertifikatsignierungsanforderung die in Schritt 2 generierte CSR ein.

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | **[Certificates](#)** | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

Generate Certificate

STEP **1**

Identify Certificate

STEP **2**

Review & Submit

STEP **3**

Results

Identify Certificate

Enter Certificate details and click Next to proceed to the next step

- * Certificate Name
- * Certificate Signing Request

```

ggEKAoIBAQCk7hIAfeJB+u4PFLeru5adulhrGNeLWoNmPIQ47PEpSyJ8Aw466z+5
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
rHFZ2W8q6rgu1i9f9c3eWogQE4j4s6TNWqqhWDA8btVkkefo+4M6UW+hQbuJkkr
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
mFgeolVugR28pHq2yksVSaEKmy21ZGZcXsMMckcuHu0Tdx63/dsk68ZnDLJngexa
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
IBw9Pmu3h7bvqE1UValzoAhaSMgft+OBAAEqTQ2G/EuWcGK2W0cVmOSh1V5+7j/
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
FE4VLW9j6dXlWehPqeJtcN+*k2/k25qQZmp/gGhp
-----END CERTIFICATE REQUEST-----

```
- * Validity Period
- Type
- Description

5. Klicken Sie auf Senden und Fertig.

Plug and Play Connect

[Feedback](#) [Support](#) [Help](#)

[Devices](#) | [Controller Profiles](#) | [Network](#) | **[Certificates](#)** | [Manage External Virtual Account](#) | [Event Log](#) | [Transactions](#)

Generate Certificate

STEP **1** ✓

Identify Certificate

STEP **2**

Review & Submit

STEP **3**

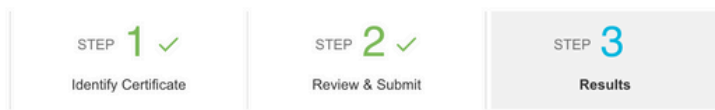
Results

Review & Submit

Certificate Name	Type	Description
VBOND-2022-DEC	SD-WAN	--

Showing 1 Record

Generate Certificate




Attempted to generate 1 Certificate

✓ Successfully requested for 1 Certificate !
It may take a few minutes to process your request. Please check the request status on Certificates tab.

[Done](#)

6. Nach wenigen Minuten ist das Zertifikat zum Download bereit.

- Zertifikatsdatei herunterladen
- Zugriff auf die vManage-Benutzeroberfläche
- Wählen Sie Installationszertifikat unter vManage > Certificate > Controllers aus.
- Wählen Sie das Zertifikat im Popup-Fenster aus.

 Hinweis Wenn Sie das Zertifikat nicht sehen oder auswählen können, stellen Sie sicher, dass Sie die Option Alle Dateien unter Format auswählen. Wenn das Formatfeld nicht angezeigt wird, verwenden Sie einen anderen Webbrowser.



Certificates

Search

Name	Size	Kind	Date Added
VBOND-2022-DEC.cer	2 KB	certificate	Today, 14:15

- All Files

Format: ✓ *.pem

Hide Options

Cancel

Open



Install Certificate

Certificate Text

 **Select a File**

```
MllFpzCCA4+gAwlBAglUTbYlXWBzQ75WYFvDABMcURHTblowDQY
JKoZlHvcNAQELBQAwOjEOMAwGA1UECgwFQ2lzY28xEDAOBgNVB
AsMB0FsYmlyZW8xZjAUBgNVBAMMDVZpcHRibGEgU3ViQ0EwHhc
NMjIxMjI2MjAwMDQyWWhcNMjIxMjI2MjAwMDQyWjCBTELMAkGA1
UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWEuETAPBgNVBAC
MCFNhbiBKb3NIMRwwGgYDVQQKDBNDaXNjbyBTeXN0ZW1zLCBjb
mMuMRUwEwYDVQQLDAxTRC1XQU4tNzNzNzNzQTA/BgNVBAMM
OHZib25kLTk2ZjVlNjVlLTQ1MzctNDk1ZC05YTk2LWJlNDZmYjdiYzA
yYy0zLnZpcHRibGEuY29tMllBijANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEApO4SAH3iQfruD3y3q7uWnbiIaxjXl1qDZj300OzxKUs
ifAMOOus
/uaEkIOxrjuMTrNiv9le0qwLZom4DUhrRxMQzNfh2kuwOVen3RUPshv
KF5yX0G3/8TqxxWdlvKuq4LtYvX
/XN3ljoEBOI+LOkzVqqoSfg2vG7VZJHn6PuDOIFvoUG7IzJK01B40y0
```

Install

Cancel

7. Das Zertifikat ist jetzt installiert.

Total Task: 1 | Success : 1

Status	Message	Device Type	Device ID	System IP	vManage IP
Success	Successfully synced vE...	vBond	96f5b65b-4537-409d...	--	10.10.10.1

Häufige Probleme

Zeit stimmt nicht überein

Für die in der Cisco Cloud gehosteten Controller ist ein NTP-Server konfiguriert.

Wenn das NTP aufgrund einer Konfigurationsänderung nicht vorhanden ist, können die Controller unterschiedliche Zeiten haben, was die Zertifikatinstallation oder die CSR-Generierung beeinträchtigen kann.

Stellen Sie sicher, dass die Controller über dieselbe Zeit verfügen.

Verbindung kann nicht hergestellt werden

Die SD-WAN-Controller müssen über die unter VPN0 konfigurierte Schnittstelle erreichbar sein.

Stellen Sie sicher, dass Layer-3- und Layer-4-Kommunikation besteht.

Wir können die Protokolle des Controllers über die Konsole überprüfen, um weitere Details über das Problem zu erhalten.

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.