

Activer le renouvellement de certificat des contrôleurs SD-WAN via une méthode manuelle

Table des matières

[Introduction](#)

[Méthodes disponibles](#)

[Exigences](#)

[Processus de renouvellement](#)

[Cisco \(recommandé\)](#)

[Manuel \(PnP\)](#)

[Problèmes courants](#)

[Non-concordance temporelle](#)

[Impossible d'établir la connexion](#)

Introduction


Ce document décrit les étapes à suivre pour renouveler le certificat SD-WAN sur les contrôleurs via la méthode Cisco ou manuelle.

Méthodes disponibles

Quatre options différentes sont disponibles pour l'autorisation de certificat de contrôleur.


- Cisco (recommandé) - Processus semi-automatisé qui utilise le portail Plug-and-Play (PnP) de Cisco pour signer le CSR généré par vManage et les télécharger et les installer automatiquement.
- Manuel - Signature manuelle du certificat via Cisco PnP.
- Symantec - Signature manuelle de certificat tiers via Symantec/Digicert.
- Certificat racine d'entreprise - Signature manuelle du certificat via une autorité de certification racine privée.

Ce document décrit uniquement les étapes des méthodes Cisco (Recommandé) et Manuel.

 Attention : les certificats couverts par ce document ne sont pas liés au certificat Web pour vManage.

Exigences

- Un PC/ordinateur portable.
- Un compte Netadmin pour l'interface utilisateur graphique vManage et pour chaque contrôleur (vManage, vSmart et vBond).
- Accès au serveur AC.
- Pour Cisco (recommandé) ou Manual, un compte/mot de passe valide pour le portail Plug and Play.
- Pour Cisco (recommandé), le vManage doit disposer d'un accès Internet.
- Tous les contrôleurs ont besoin d'un serveur NTP valide et/ou tous doivent avoir la date et l'heure correctes.
- Communication entre le vBond et le vSmart vers le vManage.

 Remarque : l'installation du certificat dans vManage n'aurait aucun impact sur votre plan de contrôle ou votre plan de données. Pour le certificat dans le vSmart, les connexions de contrôle peuvent être affectées. Le plan de contrôle continue à fonctionner grâce au minuteur progressif OMP. Afin d'effectuer une modification de certificat, vous devez planifier une fenêtre de maintenance pour l'activité.

Processus de renouvellement

Il s'agit d'une procédure de haut niveau :

1. Identifiez l'option Controller Certificate Authorization utilisée dans l'interface graphique utilisateur de vManage.
2. Générez une nouvelle CSR via l'interface graphique utilisateur vManage.
3. Créer un nouveau certificat.
4. Téléchargez le certificat.
5. Installez le certificat.

Cisco (recommandé)

1. Accédez à vManage > Administration > Settings > Certificate Authority Server.
 - Vérifiez que l'option appropriée est sélectionnée.
 - Sélectionnez la durée du certificat.

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. Faites défiler jusqu'à Identifiants de compte Smart et présentez un utilisateur/mot de passe valide. Les informations d'identification doivent avoir accès au compte Smart sur lequel la superposition SD-WAN est configurée, comme illustré dans l'image.

Administration Settings

Smart Account Credentials

Username

egarcial@cisco.com

Password

.....

Save

Cancel

3. Accédez à vManage > Configuration > Certificates > Controllers.

- Sélectionnez les points de suspension (...) sur le contrôleur (vBond, vSmart ou vManage).
- Sélectionnez Generate CSR (produire CSR).

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. Cinq à vingt minutes sont nécessaires pour terminer le processus.

Vérifiez que l'installation était correcte dans l'interface graphique utilisateur vManage > Configuration > Certificates > Controllers.

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

Manuel (PnP)

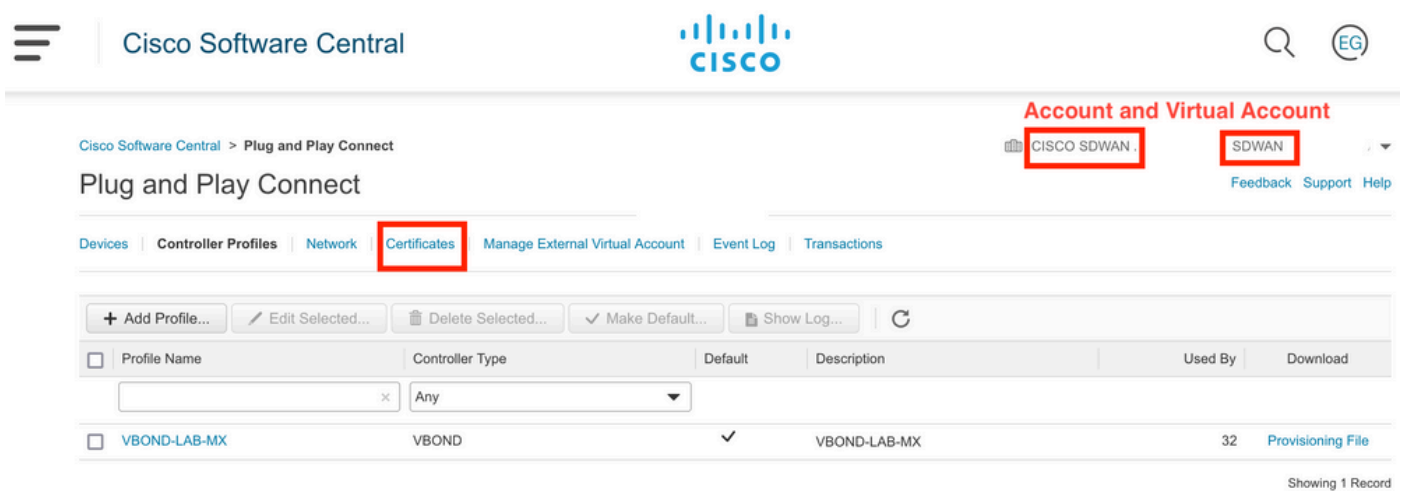
1. Accédez à vManage > Administration > Settings > Certificate Authority Server

- Vérifiez que l'option appropriée est sélectionnée.

2. Accédez à vManage > Configuration > Certificates > Controllers.

- Sélectionnez les points de suspension (...) sur le contrôleur (vBond, vSmart ou vManage).
- Sélectionnez Generate CSR (produire CSR).
- Copiez et enregistrez tout le texte dans un fichier temporaire.

3. Accédez au portail Plug and Play, sélectionnez votre superposition SD-WAN et accédez aux certificats, comme illustré dans l'image.



4. Dans la section Certificats, cliquez sur Générer un nouveau certificat et entrez toutes les informations.

- Dans Certificate Signing Request, entrez le CSR généré à l'étape 2.

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

ggEKAolBAQck7hIAfeJB+u4PFLeru5adulhrGNeLWoNmPIQ47PEpSyJ8Aw466z+5
 XXX
 rHFZ2W8q6rgu1i9f9c3eWogQE4j4s6TNWqqhWda8btVkkefo+4M6UW+hQbuJkkr
 XXX
 mFgeolVugR28pHq2yksVSaEKmy21ZGZcXsMMckcuHu0Tdx63/dsk68ZnDLJngexa
 XXX
 iBw9Pmu3h7bvqE1UValzoAhaSMgft+OBAAEqTQ2G/EuWcGK2W0cVmOSh1V5+7j/
 XXX
 FE4VLW9j6dXlWehPqeJtcN+*k2/k25qQZmp/gGhp
 -----END CERTIFICATE REQUEST-----
- * Validity Period
- Type
- Description

5. Cliquez sur Soumettre et Terminé.

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

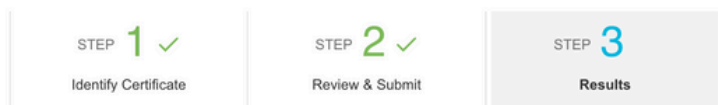
Review & Submit

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

Showing 1 Record

Cancel
Back
Submit

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. Après quelques minutes, le certificat est prêt à être téléchargé.

- Télécharger le fichier de certificat
- Accéder à l'interface graphique vManage
- Sélectionnez installer le certificat sous vManage > Certificate > Controllers.
- Sélectionnez le certificat dans la fenêtre contextuelle.

 Remarque Si vous ne pouvez pas voir ou sélectionner le certificat, assurez-vous de choisir Tous les fichiers sous l'option de format. Si la zone de format n'est pas visible, utilisez un autre navigateur Web.



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**

```
MlIFpzCCA4+gAwlBAglUTbYlXWBzQ75WYFvDABMcURHTblowDQY
JKoZlHvcNAQELBQAwOjEOMAwGA1UECgwFQ2lzY28xEDAObGNVB
AsMB0FsYmlyZW8xFjAUBgNVBAMMDVZpcHRibGEgU3ViQ0EwHhc
NMjIxMjI2MjAwMDQyWhcNMjIxMjI2MjAwMDQyWjCBTELMAkGA1
UEBhMCVVMxEzARBgNVBAGMCkNhbm3JuaWEtETAPBgNVBAC
MCFNhbiBkb3NIMRwwGgYDVQQKDBNDaXNjbyBTeXN0ZW1zLCBjb
mMuMRUwEwYDVQQLDAxTRC1XQU4tNzNzNzNzQTA/BgNVBAMM
OHZib25kLTk2ZjVlNjVlLTQ1MzctNDk0NTYtMjLWJlNDZmYjdiYzA
yYy0zLnZpcHRibGEuY29tMlIiBjANBgkqhkiG9w0BAQEFAAOCAQ8A
MlIiBjCgKGAQEApO4SAH3iQfruD3y3q7uWnbiIaxjXl1qDZj300OzxKUs
ifAMOOus
/uaEkIOxrjuMTrNiv9le0qwLZom4DUhrRxMQzNfh2kuwOVen3RUPshv
KF5yX0G3/8TqxxWdlvKuq4LtYvX
/XN3IjoEBOI+LOkzVqqoSfg2vG7VZJHn6PuDOIFvoUG7iZJK01B40y0
```

Install

Cancel

7. Le certificat est maintenant installé.

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

Problèmes courants

Non-concordance temporelle

Un serveur NTP est configuré sur les contrôleurs hébergés dans le cloud Cisco.

Si le NTP n'est pas présent en raison d'une modification de la configuration, les contrôleurs peuvent avoir des heures différentes et cela peut interférer avec l'installation du certificat ou la génération de CSR.

Assurez-vous que les contrôleurs ont la même heure.

Impossible d'établir la connexion

Les contrôleurs SD-WAN doivent être accessibles via l'interface configurée sous VPN0.

Vérifiez qu'il existe une communication de couche 3 et de couche 4.

Nous pouvons vérifier les journaux du contrôleur via la console pour plus de détails sur le problème.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.