# Comment puis-je générer des certificats sur le portail Cisco Device Activation (CDA) ?

## Table des matières

Réservé aux clients et partenaires externes: Ces instructions sont pourvu pour aider les clients/partenaires à effectuer eux-mêmes l'action suivante pour résoudre le problème. Si le client/partenaire rencontre des problèmes suite aux instructions, demandez-lui d'ouvrir un dossier avec l'assistance pour les licences (https://www.cisco.com/go/scm) Pour aider à résoudre. Veuillez NE PAS effectuer ces actions vous-même si vous êtes une ressource interne de Cisco en dehors de l'équipe d'assistance pour les licences.

Avant de commencer, vérifiez que vous disposez des éléments suivants :

- Compte Cisco.com actif
- L'utilisateur doit disposer d'un accès au portail CDA
- L'utilisateur doit avoir accès à la gestion des certificats

Étape 1 : cliquez sur le lien Certificate Managementk Services de développement Cisco.

Étape 2 : Cliquez sur ‘Gestion des certificats’Onglet.

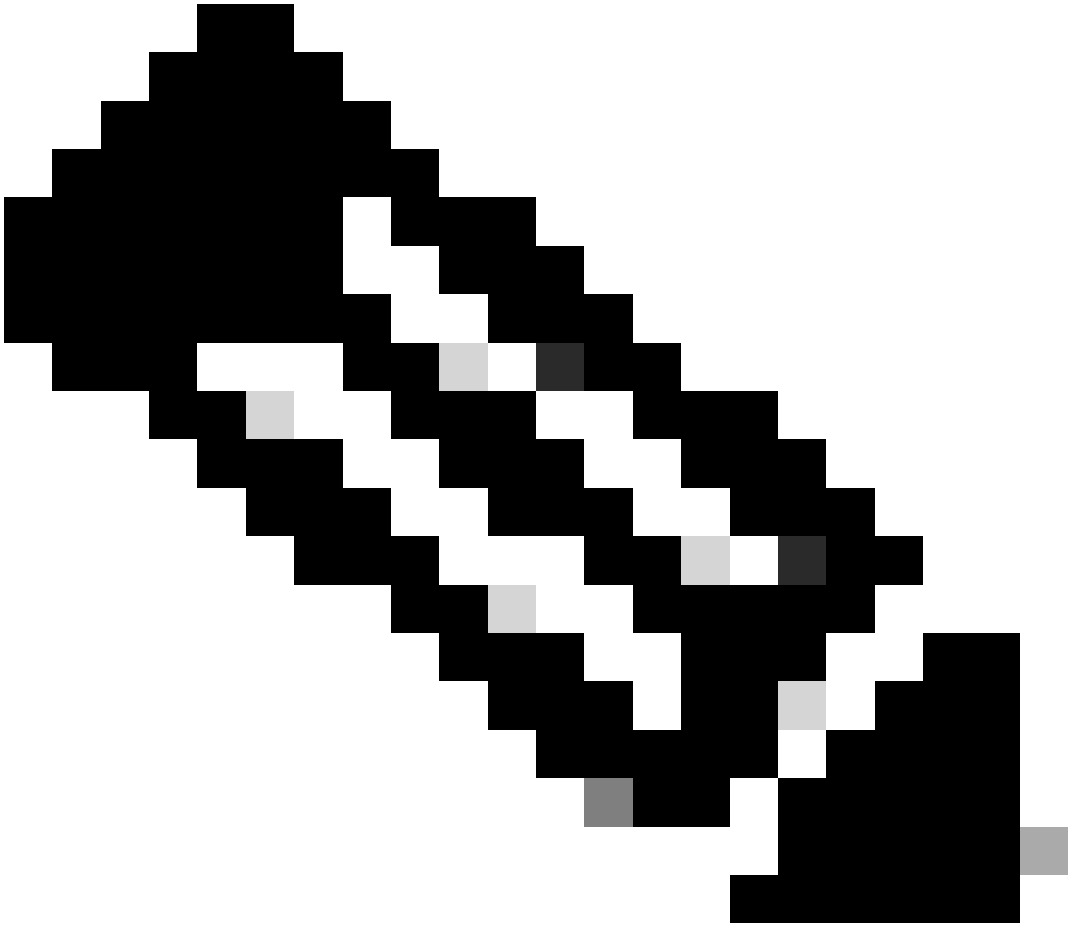
Étape 3 : Cliquez sur « Signer CSR’Onglet.

Étape 4 : Sélectionnez un produit dans l'Sélectionner un produit» dans la liste déroulante.

Étape 5 : les attributs « Encryption Type », « Sign in Duration » et « CSR File » ne sont activés que lors de la sélection du produit.

Étape 6 :  Sélectionnez le type de cryptage dans le sous l'Type de chiffrement» (SHA1/SHA256). Par défaut, la valeur sélectionnée est SHA256.

Étape 7 :  Sélectionnez la durée du certificat dans le champ ‘Durée de connexion» (180 jours/jusqu'au 31 mai)st,2025).



Remarque : lorsque le chiffrement MD5 est sélectionné, un message d'avertissement s'affiche pour confirmer la sélection du chiffrement

Étape 8 : Téléchargez le fichier CSR dans le champ Fichier CSR.

Étape 9 : Cliquez sur ‘Demande de certificat de signature’ pour signer le fichier de certificat qui a été chargé. Le fichier va maintenant être signé

Étape 10 : Une fois le certificat signé avec succès, le message « CLe certificat a été signé’ s s'affiche à l'écran. Cliquer OK.

Étape 11 : Cliquez sur ‘Télécharger’ pour télécharger le certificat signé.

Étape 12 : Sous ‘Méthode de réception des certificats’ - Saisissez une adresse e-mail dans le champ Adresse e-mail pour envoyer le certificat signé à une adresse e-mail.

Étape 14 : Cliquez sur ‘Envoyer’ pour envoyer le certificat signé à l'adresse e-mail saisie. Vous

recevrez un message de confirmation indiquant que le fichier a été envoyé à l'adresse e-mail. Le fichier téléchargé pour être signé et le fichier envoyé par e-mail portent le même nom.

Dépannage :

Si vous rencontrez un problème avec ce processus, que vous ne pouvez pas résoudre, veuillez ouvrir un dossier à l'adresse Support Case Manager (gestionnaire de dossiers de soutien)

Pour obtenir des commentaires sur le contenu de ce document, veuillez envoyer ici.

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.