

# Mise à jour du nouveau bundle de certificats racine approuvés WSA - Avril 2017

## Contenu

[Introduction](#)

[Informations générales](#)

[Mettre à jour la description](#)

[Qu'est-ce que cela signifie pour les utilisateurs WSA ?](#)

## Introduction

Ce document décrit en détail la mise à jour d'avril 2017 des ensembles racine de confiance Cisco et ses effets sur l'appareil de sécurité Web Cisco (WSA).

## Informations générales

Afin de maintenir la sécurité de nos produits au plus haut niveau ; L'équipe des services cryptographiques Cisco est heureuse d'annoncer la publication de la prochaine version des bundles racine de confiance Cisco. Cette modification aura un effet sur WSA. Les bundles seront automatiquement mis à jour sur toutes les versions prises en charge de Cisco AsyncOS pour le Web, et aucune action n'est requise de la part des administrateurs WSA.

## Mettre à jour la description

Ces bundles reflètent les dernières mises à jour des bundles dérivés des magasins racine approuvés en amont en novembre 2016.

Les modifications les plus importantes apportées aux ensembles racine de confiance Cisco sont les suivantes :

- Suite à la décision des grands magasins de confiance ([Google](#), [Apple](#), [Mozilla](#)) de les supprimer, les nouveaux Cisco Trusted Root Bundles ne contiennent plus de racines de WoSign/StartCom. S'ils soumettent à nouveau de nouvelles racines à des magasins racine en amont, nous reviendrons sur la décision de les retirer des ensembles de confiance.
- Le nouveau Cisco Root CA 2099 a été ajouté à tous les bundles pour prendre en charge les nouveaux chipsets ACT2.
- L'ancienne racine VeriSign a été remplacée dans le bundle Core par la nouvelle racine qui enchaîne correctement les certificats VeriSign mPKI.
- DST Root CA X1 a été supprimé du bundle Core uniquement, car Cisco n'émet plus de racines de cette chaîne.

## Qu'est-ce que cela signifie pour les utilisateurs WSA ?

- Cisco WSA télécharge de nouveaux ensembles de certificats racine qui utilisent notre processus de mise à jour. Aucune action n'est nécessaire de la part des administrateurs WSA.
- Si WSA est configuré pour utiliser le décryptage, les requêtes vers les sites qui ont des certificats SSL signés par **WoSign/StartCom**, seront par défaut abandonnées par WSA, car les certificats d'autorité de certification racine de ce fournisseur ne seront pas approuvés par WSA après la mise à jour.
- Sinon, WSA appliquera l'action configurée dans **Proxy HTTPS > Gestion de certificat non valide > Autorité racine non reconnue / Émetteur**. Cette action est DROP par défaut et Cisco recommande de ne pas modifier l'action par défaut Autorité racine non reconnue.

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.