Dépannage de la liste des certificats racine requis pour l'installation de Secure Endpoint sous Windows

Table des matières

Introduction

Ce document décrit comment vérifier toutes les autorités de certification installées lorsque l'installation d'Advanced Malware Protection (AMP) échoue en raison d'erreurs de certificat.

Composants utilisés

- Connecteur de sécurité (anciennement AMP for Endpoints) 6.3.1 et versions ultérieures
- Windows 7 et versions ultérieures

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Problème

Si vous rencontrez des problèmes avec AMP for Endpoints Connector pour Windows, consultez les journaux à cet emplacement.

<#root>

C:\ProgramData\Cisco\AMP\immpro_install.log

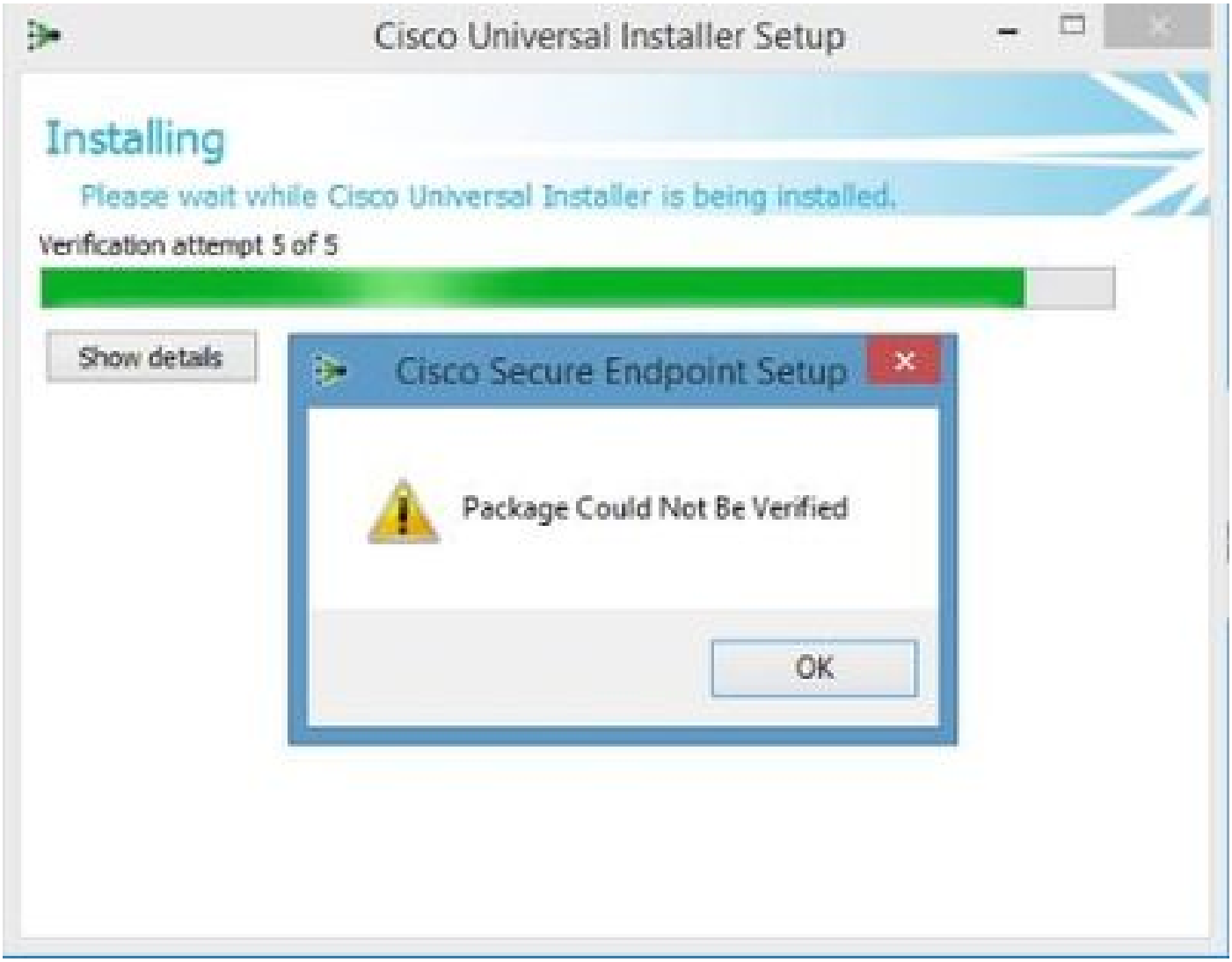
Si ce message ou un message similaire s'affiche.

<#root>

ERROR: Util::VerifyAll: signature verification failed : -2146762487 : A certificate chain processed, but

<#root>

Package could not be verified



Assurez-vous que tous les certificats RootCA nécessaires sont installés.

Solution

Étape 1. Ouvrez PowerShell avec des privilèges d'administration et exécutez la commande.

<#root>

Get-ChildItem -Path Cert:LocalMachine\Root

Le résultat affiche la liste des certificats RootCA installés et stockés sur une machine.

Étape 2. Comparez les empreintes obtenues à l'étape 1 avec celles répertoriées dans le tableau 1

ci-dessous :

Empreinte	Nom du sujet / Attributs
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Autorité de certification racine Microsoft 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign, O=GlobalSign, OU=Autorité de certification racine GlobalSign - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Racine CyberTrust de Baltimore, OU=CyberTrust, O=Baltimore, C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Grand Manchester, C=GB
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E370EB58A	OU=Autorité de certification Starfield Classe 2, O="Starfield Technologies, Inc.", C=US
A8985D3A65E5E5C4B2D7D66D40C6D2FB19C5436	CN=DigiCert Autorité de certification racine globale, OU=www.digicert.com, O=DigiCert Inc, C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Autorité de certification publique principale de classe 3, O="VeriSign, Inc.", C=US
5FB7EE0633E259DBAD0C4C9AE6D38F1A61C7DC25	CN=DigiCert High Assurance EV Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - Pour utilisation autorisée uniquement", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Autorité de certification Go Daddy Class 2, O="The Go Daddy Group, Inc.", C=US
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D4	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
DFB16CD4931C973A2037D3FC83A4D7D775D05E4	CN=DigiCert Racine de confiance G4,

	OU=www.digicert.com, O=DigiCert Inc, C=US
CA3AFBCF1240364B44B216208880483919937CF7	CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM
2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E	CN=USERTRUST Autorité de certification RSA, O=Le réseau USERTRUST, L=Jersey City, S=New Jersey, C=US
F40042E2E5F7E8EF8189FED15519AECE42C3BFA2	CN=Microsoft Identity Verification Root Certificate Authority 2020, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
DF717EAA4AD94EC9558499602D48DE5FBCF03A25	CN=US, O=IdenTrust, CN=IdenTrust Commercial Root CA 1

Tableau 1 . Liste des certificats requis pour Cisco Secure Connector.

Étape 3. Téléchargez les certificats qui ne sont pas présents dans le magasin de machines à partir des émetteurs au format PEM.

Conseil : Vous pouvez rechercher le certificat par l'empreinte numérique sur Internet. Ils définissent le certificat de manière unique.

Étape 4. Ouvrez la console mmc à partir du menu Démarrer.

Étape 5. Accédez à Fichier > Ajouter/Supprimer un composant logiciel enfichable... > Certificats > Ajouter > Compte d'ordinateur > Suivant > Terminer > OK.

Étape 6. Ouvrez Certificats sous Autorités de certification racine de confiance. Cliquez avec le bouton droit sur le dossier Certificates, puis sélectionnez All Tasks > Import... et suivez les instructions de l'assistant afin d'importer le certificat jusqu'à ce qu'il apparaisse dans le dossier Certificates.

Étape 7. Répétez l'étape 6 si vous avez d'autres certificats à importer.

Étape 8. Après avoir importé tous les certificats, vérifiez si l'installation d'AMP for Endpoints Connector a réussi. Si ce n'est pas le cas, vérifiez à nouveau les journaux dans le fichier immpro_install.log.

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.