Probleemoplossing Lijst met basiscertificaten die vereist zijn voor de installatie van beveiligde endpoints in Windows

Inhoud

Inleiding

Dit document beschrijft hoe u alle geïnstalleerde certificeringsinstanties kunt controleren wanneer de installatie van Advanced Malware Protection (AMP) mislukt als gevolg van een certificaatfout.

Gebruikte componenten

- Security Connector (voorheen AMP voor endpoints) 6.3.1 en hoger
- Windows 7 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Probleem

Als u problemen ondervindt met AMP for Endpoints Connector voor Windows, controleert u logbestanden onder deze locatie.

<#root>

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

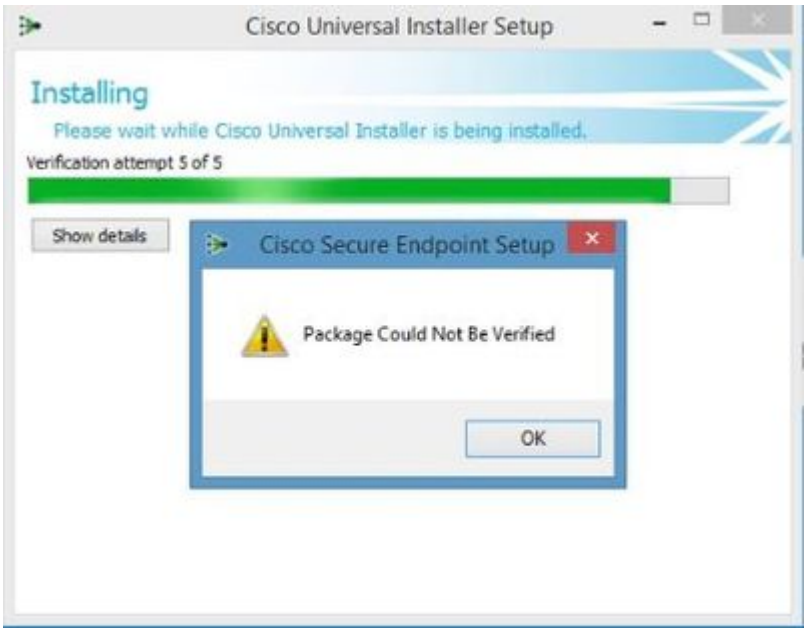
Als je dit of een vergelijkbaar bericht ziet.

<#root>

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

<#root>

```
Package could not be verified
```



Zorg ervoor dat alle benodigde RootCA-certificaten zijn geïnstalleerd.

Oplossing

Stap 1. Open PowerShell met beheerdersrechten en voer de opdracht uit.

<#root>

```
Get-ChildItem -Path Cert:LocalMachine\Root
```

Het resultaat toont een lijst van geïnstalleerde RootCA-certificaten die in een machine zijn opgeslagen.

Stap 2. Vergelijk de thumbprints die bij Stap 1 zijn verkregen met de thumbnails die in tabel 1 hieronder worden vermeld:

duimafdruk	Onderwerpnaam / kenmerken
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign, O=GlobalSign, OU=GlobalSign Root CA - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Baltimore CyberTrust Root, OU=CyberTrust, O=Baltimore, C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Greater Manchester, C=GB
B1BC968BD4F49D622A89A81F2150152A41D829C	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E370B58A	OU=Starfield Class 2 certificeringsinstantie, O="Starfield Technologies, Inc.", C=US
A895D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert Global Root CA,

	OU=www.digicert.com, O=DigiCert Inc, C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Class 3 Public Primary Certification Authority, O="VeriSign, Inc.", C=US
5FB7E063E259DBAD0C4C9AE6D38F1A61C7DC25	CN=DigiCert Hoge Verzekering 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. - Alleen voor geautoriseerd gebruik", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EE4	OU=Go Daddy Class 2 certificeringsinstantie, O="The Go Daddy Group, Inc.", C=US
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert Assure ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
DFB16CD493C973A2037D3FC83A4D7D775D05E4	CN=DigiCert Trusted Root G4, OU=www.digicert.com, O=DigiCert Inc, C=US
CA3AFBCF1240364B44B216208880483919937CF7	CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM
2B8F1B57330DBBA2D07A6C51F70E90DDAB9AD8E	CN=USERTrust RSA Certificeringsinstantie, O=The USERTRUST Network, L=Jersey City, S=New Jersey, C=US
F40042E2E5F7E8EF819FED15519AECE42C3BFA2	CN=Microsoft Identity Verification Root Certificate Authority 2020, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
DF717EAA4AD94EC9558499602D48DE5FBCF03A25 router	CN=US, O=IdenTrust, CN=IdenTrust Commercial Root CA 1

Tabel 1. Lijst met vereiste certificaten voor Cisco Secure Connector.

Stap 3. Download certificaten die niet aanwezig zijn in de machinewinkel van de uitgevers in het PEM-formaat.

> **Tip**: u kunt het certificaat via de thumbprint op het internet doorzoeken. Zij geven een unieke definitie van het certificaat.

Stap 4. Open de **mmc**-console in het menu Start.

Stap 5. Navigeer naar **Bestand > Magnetisch toevoegen/verwijderen... > Certificaten > Toevoegen > Computer-account > Volgende > Voltooien > OK**.

Stap 6. Open **Certificaten** onder **Trusted Root-certificeringsinstanties**. Klik met de rechtermuisknop op **de** map **Certificaten**, selecteer vervolgens **Alle taken > Importeren...** en volg de wizard om het certificaat te importeren totdat het in de map **Certificaten** verschijnt.

Stap 7. Herhaal stap 6 als u meer certificaten hebt om te importeren.

Stap 8. Nadat u alle certificaten hebt geïmporteerd, controleert u of de installatie van de AMP voor Endpoints Connector is geslaagd. Als dit niet het geval is, controleer dan opnieuw het bestand impro_install.log in.

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.