Fehlerbehebung: Liste der Root-Zertifikate, die für die Installation sicherer Endgeräte unter Windows erforderlich sind

Inhalt

[Einleitung](#)
[Verwendete Komponenten](#)
[Problem](#)
[Lösung](#)

Einleitung

In diesem Dokument wird beschrieben, wie alle installierten Zertifizierungsstellen überprüft werden, wenn die Installation von Advanced Malware Protection (AMP) aufgrund eines Zertifikatfehlers fehlschlägt.

Verwendete Komponenten

- Security Connector (ehemals AMP für Endgeräte) 6.3.1 und höher
- Windows 7 und höher

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Wenn Sie Probleme mit AMP für Endgeräte Connector für Windows haben, überprüfen Sie die Protokolle unter diesem Speicherort.

<#root>

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

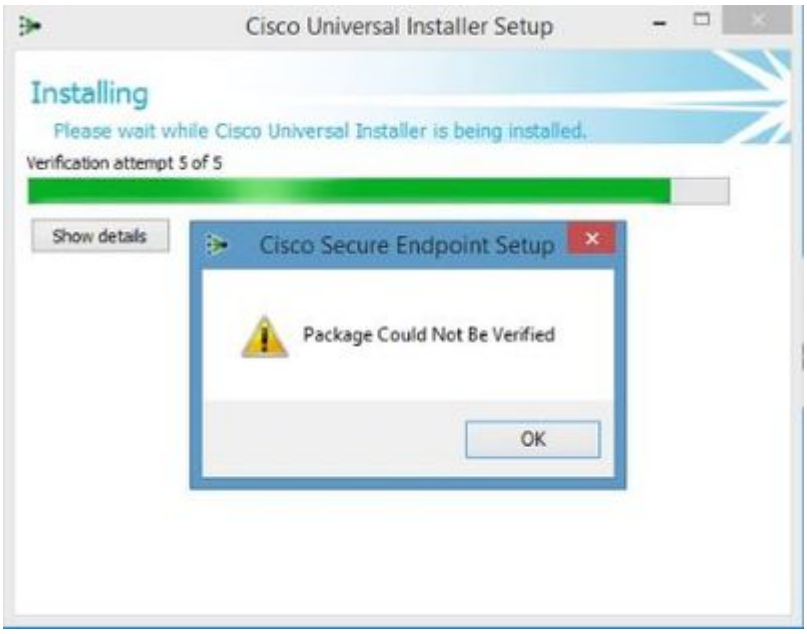
Wenn diese oder eine ähnliche Meldung angezeigt wird.

<#root>

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

<#root>

```
Package could not be verified
```



Stellen Sie sicher, dass alle erforderlichen RootCA-Zertifikate installiert sind.

Lösung

Schritt 1: Öffnen Sie PowerShell mit Administratorberechtigungen, und führen Sie den Befehl aus.

<#root>

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

Das Ergebnis zeigt eine Liste der installierten RootCA-Zertifikate, die auf einem Computer gespeichert sind.

Schritt 2: Vergleichen Sie die in Schritt 1 ermittelten Fingerabdrücke mit den in Tabelle 1 aufgeführten:

Daumenabdruck	Betreffname/Attribute
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
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=GlobalSign Root CA, OU=Root CA, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E3370EB58A	OU=Starfield Class 2 Certification Authority, O="Starfield Technologies, Inc", C=USA
A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	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
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. - Nur zur autorisierten Verwendung", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc", C=US
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
DDFB16CD4931C973A2037D3FC83A4D7D775D05E4	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
2B8F1B57330DBBA2D07A6C51F70EE90DDAB9AD8E	CN=USERTrust RSA Certification Authority, O=The USERTRUST Network, 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

Tabelle 1. Liste der erforderlichen Zertifikate für Cisco Secure Connector.

Schritt 3: Laden Sie Zertifikate, die nicht im Computerspeicher vorhanden sind, von den Ausstellern im PEM-Format herunter.

> **Tipp:** Sie können das Zertifikat nach dem Fingerabdruck im Internet durchsuchen. Sie definieren das Zertifikat eindeutig.

Schritt 4: Öffnen Sie die **mmc**-Konsole über das Startmenü.

Schritt 5: Navigieren Sie zu **Datei > Snap-In hinzufügen/entfernen... > Zertifikate > Hinzufügen > Computerkonto > Weiter > Fertig stellen > OK**.

Schritt 6: Öffnen Sie **Zertifikate** unter **Vertrauenswürdige Stammzertifizierungsstellen**. Klicken Sie mit der rechten Maustaste auf den Ordner **Zertifikate,** wählen Sie dann **Alle Aufgaben > Importieren...** und folgen Sie dem Assistenten, um das Zertifikat zu importieren, bis es im Ordner **Zertifikate** angezeigt wird.

Schritt 7. Wiederholen Sie Schritt 6, wenn Sie weitere Zertifikate importieren möchten.

Schritt 8: Überprüfen Sie nach dem Importieren aller Zertifikate, ob die Installation von AMP für Endpoints-Connector erfolgreich war. Ist dies nicht der Fall, überprüfen Sie erneut die Protokolle in der Datei immpro_install.log.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.