Risoluzione dei problemi relativi all'elenco dei certificati radice necessari per l'installazione dell'endpoint sicuro in Windows

Sommario

[Introduzione](#)

[Componenti usati](#)

[Problema](#)

[Soluzione](#)

Introduzione

In questo documento viene descritto come controllare tutte le autorità di certificazione installate quando l'installazione di Advanced Malware Protection (AMP) non riesce a causa di un errore del certificato.

Componenti usati

- Security Connector (in precedenza AMP for Endpoints) 6.3.1 in avanti
- Windows 7 e versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Problema

Se si verificano problemi con AMP for Endpoints Connector for Windows, controllare i registri in questo percorso.

<#root>

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

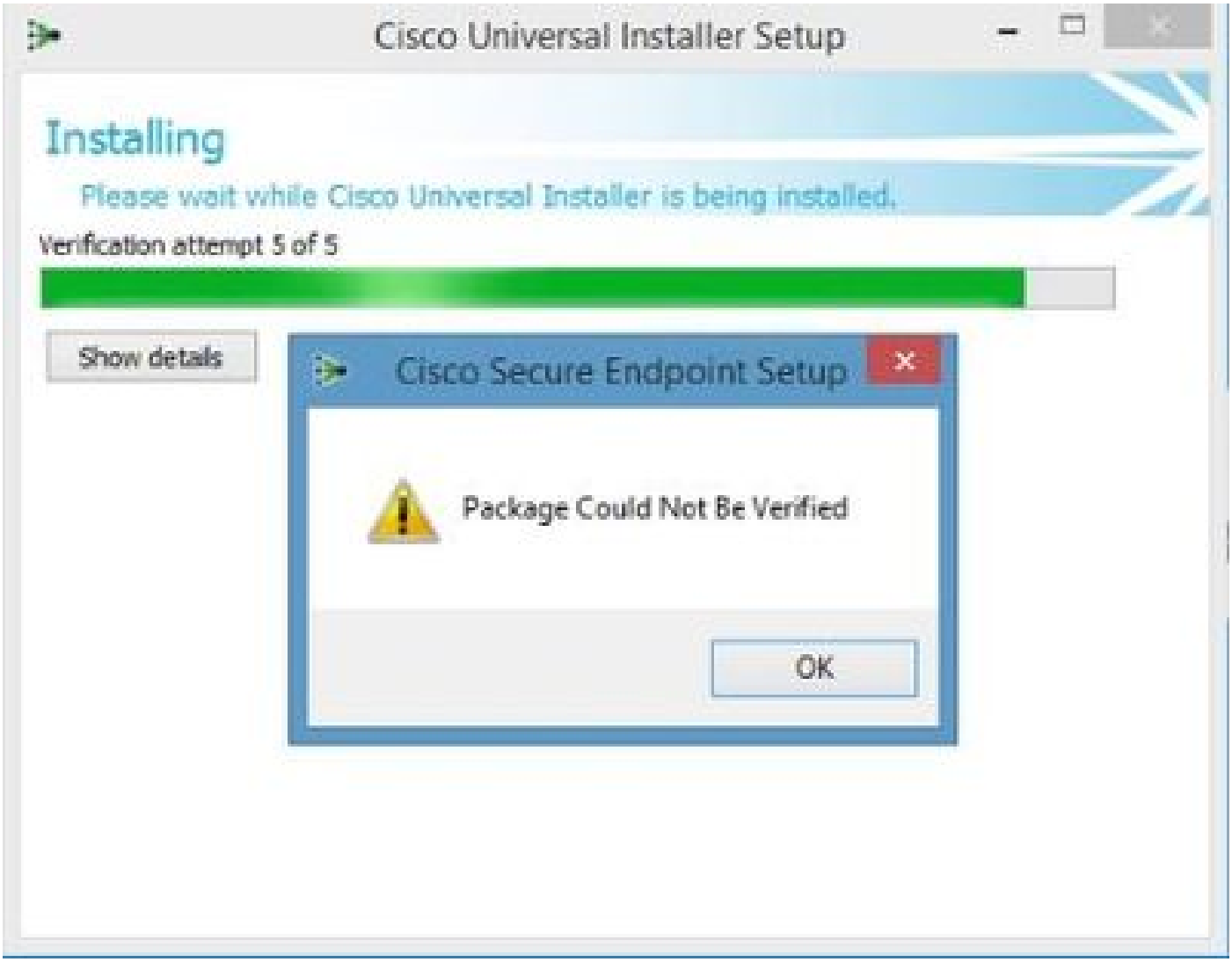
Se viene visualizzato questo messaggio o un messaggio simile.

<#root>

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

<#root>

```
Package could not be verified
```



Verificare che siano installati tutti i certificati RootCA necessari.

Soluzione

Passaggio 1. Aprire PowerShell con privilegi amministrativi ed eseguire il comando.

<#root>

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

Il risultato mostra un elenco di certificati RootCA installati archiviati in un computer.

Passaggio 2. Confrontare le miniature ottenute nel passo 1 con quelle elencate nella tabella 1 riportata di seguito:

Identificazione personale	Nome soggetto/Attributi
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign, O=GlobalSign, OU=GlobalSign CA radice - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Radice CyberTrust di Baltimora, OU=CyberTrust, O=Baltimora, C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Greater Manchester, C=GB
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=GlobalSign CA radice, OU=CA radice, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E3370EB58A	OU=Autorità di certificazione classe 2 Starfield, O="Starfield Technologies, Inc.", C=US
A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Classe 3 Autorità di certificazione primaria pubblica, O="VeriSign, Inc.", C=US
5FB7E0633E259DBAD0C4C9AE6D38F1A61C7DC25	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. - For authorized use only", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D7770028F20EEE4	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=IT
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert ID garantito CA radice, OU=www.digicert.com, O=DigiCert Inc, C=US
DDFB16CD4931C973A2037D3FC83A4D7D775D05E4	CN=DigiCert Root G4, OU=www.digicert.com, O=DigiCert Inc,

	C=US
CA3AFBCF1240364B44B216208804839199 37CF7	CN=QuoVadis Root CA 2, O=QuoVadis Limited, C=BM
2B8F1B57330DBBA2D07A6C51F70E90DDAB9AD8E	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
DF717EAA4AD94EC958499602D48DE5FBCF03A25	CN=US, O=IdenTrust, CN=IdenTrust Commercial Root CA 1

Tabella 1. Elenco dei certificati richiesti per Cisco Secure Connector.

Passaggio 3. Scaricare i certificati non presenti nell'archivio del computer dagli emittenti nel formato PEM.

Suggerimento: è possibile eseguire la ricerca nel certificato tramite l'identificazione personale su Internet. Definiscono in modo univoco il certificato.

Passaggio 4. Aprire la console mmc dal menu Start.

Passaggio 5. Selezionare File > Aggiungi/Rimuovi snap-in... > Certificati > Aggiungi > Account computer > Avanti > Fine > OK.

Passaggio 6. Aprire Certificati in Autorità di certificazione radice attendibili. Fare clic con il pulsante destro del mouse sulla cartella Certificati, quindi selezionare Tutte le attività > Importa e seguire la procedura guidata per importare il certificato fino a quando non viene visualizzato nella cartella Certificati.

Passaggio 7. Ripetere il passaggio 6 se si dispone di più certificati da importare.

Passaggio 8. Dopo aver importato tutti i certificati, verificare che l'installazione di AMP for Endpoints Connector abbia esito positivo. In caso contrario, controllare nuovamente i log nel file immpro_install.log.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).