Windows에서 보안 엔드포인트 설치에 필요한 루트 인증서 목록 문제 해결

목차

소개

이 문서에서는 인증서 오류로 인해 AMP(Advanced Malware Protection) 설치가 실패할 경우 설치된 모든 인증 기관을 확인하는 방법에 대해 설명합니다.

사용되는 구성 요소

- Security Connector(이전의 AMP for Endpoints) 6.3.1 이후
- Windows 7 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

문제

Windows용 AMP for Endpoints Connector에 문제가 발생하면 이 위치에서 로그를 확인하십시오.

<#root>

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

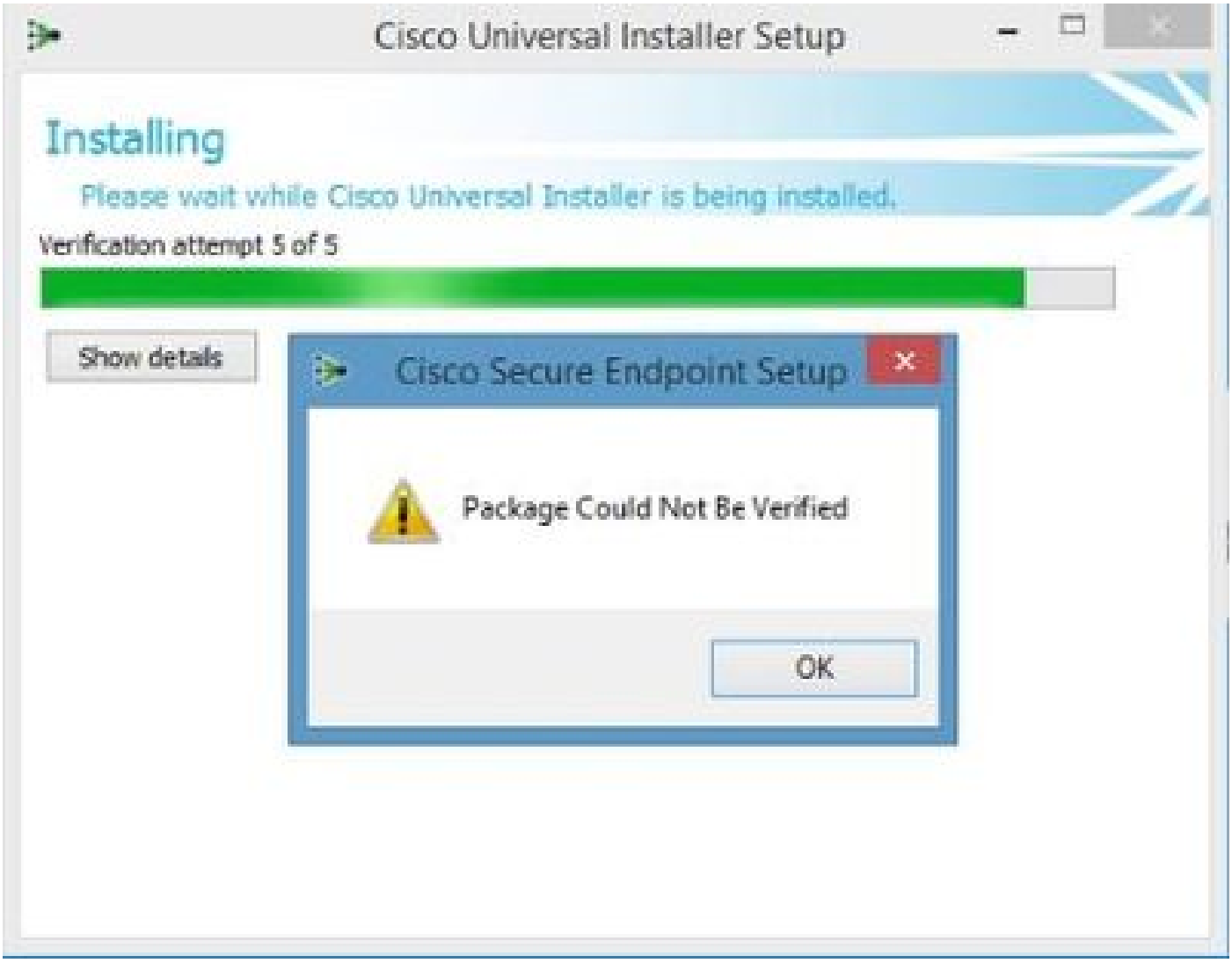
또는 유사한 메시지가 표시되는 경우

<#root>

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

<#root>

```
Package could not be verified
```



필요한 모든 RootCA 인증서가 설치되어 있는지 확인합니다.

솔루션

1단계. 관리자 권한으로 PowerShell을 열고 명령을 실행합니다.

<#root>

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

그러면 시스템에 저장된 설치된 RootCA 인증서의 목록이 표시됩니다.

2단계. 1단계에서 얻은 썸프린트와 아래 표 1에 나열된 썸프린트를 비교합니다.

지문	주체 이름/특성

3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation, L=Redmond, S=Washington, C=US
D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign, O=GlobalSign, OU=GlobalSign 루트 CA - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Baltimore CyberTrust 루트, 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 루트 CA, OU=루트 CA, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E3370EB58A	OU=Starfield Class 2 인증 기관, O="Starfield Technologies, Inc.", C=US
A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert 전역 루트 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. - 인증된 사용 전용", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy Class 2 인증 기관, 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 인증 기관, 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

표 1. Cisco Secure Connector에 필요한 인증서 목록입니다.

3단계. PEM 형식의 발급자로부터 머신 저장소에 없는 인증서를 다운로드합니다.

팁: 인터넷의 지문으로 인증서를 검색할 수 있습니다. 인증서를 고유하게 정의합니다.

4단계. 시작 메뉴에서 mmc 콘솔을 엽니다.

5단계. File(파일) > Add/Remove Snap-in... > Certificates(인증서) > Add(추가) > Computer Account(컴퓨터 계정) > Next(다음) > Finish(마침) > OK(확인)로 이동합니다.

6단계. 신뢰할 수 있는 루트 인증 기관에서 인증서를 엽니다. Certificates 폴더를 마우스 오른쪽 버튼으로 클릭하고 All Tasks(모든 작업) > Import...를 선택한 다음 Certificates(인증서) 폴더에 나타날 때까지 마법사를 따라 인증서를 가져옵니다.

7단계. 가져올 인증서가 더 있는 경우 6단계를 반복합니다.

8단계. 모든 인증서를 가져온 후 AMP for Endpoints Connector 설치가 성공적인지 확인합니다. 그렇지 않은 경우 impro_install.log 파일에서 다시 로그인을 확인합니다.

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.