在Windows上安裝安全終結點所需的根證書清單故障排除

目錄

簡介

本文描述如何檢查高級惡意軟體防護(AMP)安裝由於證書錯誤而失敗時安裝的所有證書頒發機構。

採用元件

- 安全聯結器（前身為適用於終端的AMP）6.3.1及以上版本
- 從Windows 7開始

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

問題

如果用於Windows的AMP端點聯結器出現問題，請檢查此位置下的日誌。

<#root>

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

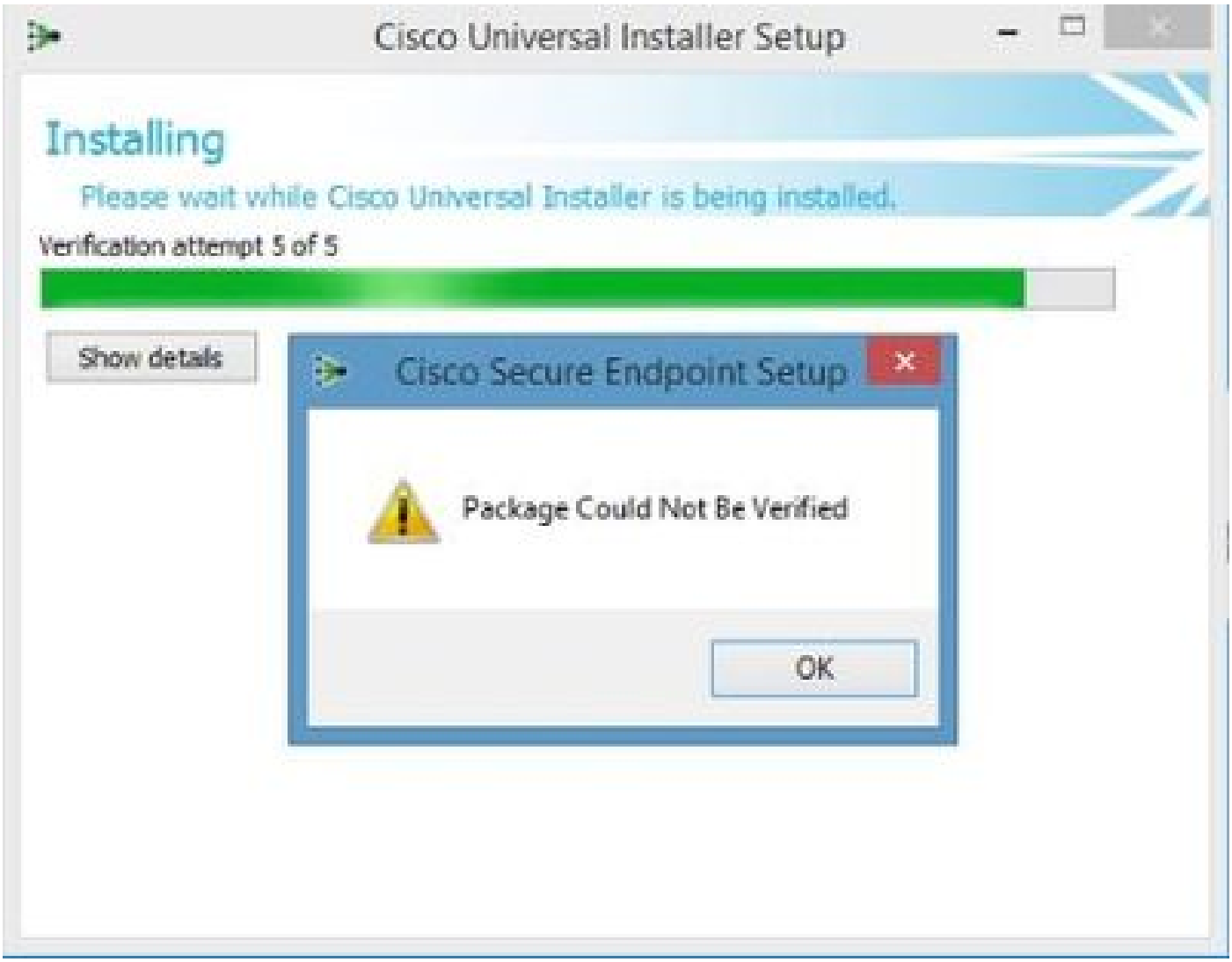
如果您看到此消息或類似消息。

<#root>

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

<#root>

Package could not be verified



確保已安裝所有必要的RootCA證書。

解決方案

步驟 1.以管理許可權開啟PowerShell並運行命令。

<#root>

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

結果顯示儲存在電腦中的已安裝RootCA證書的清單。

步驟 2.將步驟1中獲得的指紋與下表1中列出的指紋進行比較：

指紋	使用者名稱/屬性
3B1EFD3A66EA28B16697394703A72CA340A05BD5	CN=Microsoft Root Certificate Authority 2010, O=Microsoft Corporation，L=Redmond， S=Washington， C=US

D69B561148F01C77C54578C10926DF5B856976AD	CN=GlobalSign， O=GlobalSign，OU=GlobalSign根CA - R3
D4DE20D05E66FC53FE1A50882C78DB2852CAE474	CN=Baltimore CyberTrust Root、OU=CyberTrust、O=Baltimore、C=IE
D1EB23A46D17D6892564C2F1F1601764D8E349	CN=AAA Certificate Services，O=Comodo CA Limited， L=Salford，S=大曼徹斯特， 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=US
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. — 僅供授權使用", OU=VeriSign Trust Network，O="VeriSign， Inc.", C=US
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy Class 2 Certification Authority， O="The Go Daddy Group，Inc.", C=美國
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=USERTRUST Network，L=澤西市， S=新澤西， C=美國
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商業根CA 1

表1.Cisco Secure Connector所需的證書清單。

步驟 3.以PEM格式從發行者下載電腦儲存中不存在的證書。

提示：您可以在Internet上通過指紋搜尋證書。它們唯一地定義證書。

步驟 4.從「開始」選單開啟mmc控制檯。

步驟 5.導航到檔案>新增/刪除管理單元…… >證書>新增>電腦帳戶>下一步>完成>確定。

步驟 6.在受信任的根憑證授權機構下開啟憑證。按一下右鍵Certificates資料夾，然後選擇All Tasks > Import...，然後按照嚮導進行匯入，直到證書出現在Certificates資料夾中。

步驟 7.如果要匯入更多證書，請重複步驟6。

步驟 8.匯入所有證書後，檢查面向終端的AMP聯結器安裝是否成功。如果不是，請再次檢查immpro_install.log檔案中的日誌。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。