Solucionar problemas de la lista de certificados raíz necesarios para la instalación de terminales seguros en Windows

Contenido

Introducción

Este documento describe cómo comprobar todas las autoridades de certificados instaladas cuando falla la instalación de la protección frente a malware avanzado (AMP) debido a un error de certificado.

Componentes Utilizados

- Security Connector (anteriormente AMP para terminales) 6.3.1 en adelante
- Windows 7 en adelante

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Si tiene problemas con AMP para Endpoints Connector for Windows, consulte los registros en esta ubicación.

<#root>

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

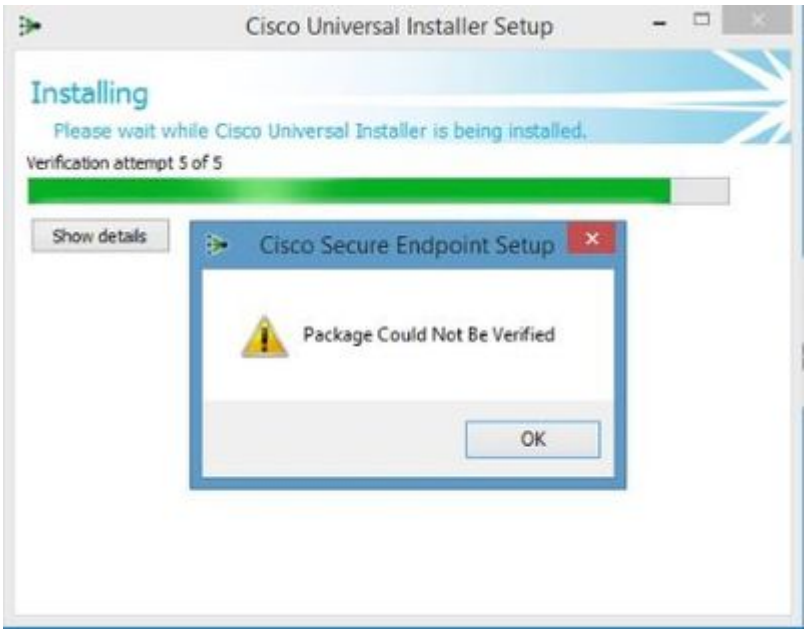
Si ve este mensaje o uno similar.

<#root>

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

<#root>

```
Package could not be verified
```



Asegúrese de que tiene instalados todos los certificados RootCA necesarios.

Solución

Paso 1. Abra PowerShell con privilegios administrativos y ejecute el comando.

<#root>

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

El resultado muestra una lista de los certificados RootCA instalados almacenados en un equipo.

Paso 2. Compare las huellas digitales obtenidas en el paso 1 con las enumeradas en la tabla 1 a continuación:

Huella digital	Nombre del asunto/Atributos
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=Raíz de CyberTrust de Baltimore, OU=CyberTrust, O=Baltimore, C=IE
D1EB23A46D17D68FD92564C2F1F1601764D8E349	CN=AAA Certificate Services, O=Comodo CA Limited, L=Salford, S=Greater Manchester, C=GB
B1BC968BD4F49D622AA89A81F2150152A41D829C	CN=CA raíz GlobalSign, OU=CA raíz, O=GlobalSign nv-sa, C=BE
AD7E1C28B064EF8F6003402014C3D0E370EB58A	OU=Autoridad de certificación Starfield Clase 2, O="Starfield Technologies, Inc.", C=EE. UU.

A8985D3A65E5E5C4B2D7D66D40C6DD2FB19C5436	CN=DigiCert Global Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
742C3192E607E424EB4549542BE1BBC53E6174E2	OU=Autoridad de certificación principal pública de clase 3, O="VeriSign, Inc.", C=EE. UU.
5FB7E0633E259DBAD0C4C9AE6D38F1A61C7DC25	CN=CA raíz de alta garantía de DigiCert, OU=www.digicert.com, O=DigiCert Inc, C=US
4EB6D578499B1CCF5F581EAD56BE3D9B6744A5E5	CN=VeriSign Class 3 Public Primary Certification Authority - G5, OU="(c) 2006 VeriSign, Inc. - Para uso exclusivo autorizado", OU=VeriSign Trust Network, O="VeriSign, Inc.", C=EE. UU.
2796BAE63F1801E277261BA0D77770028F20EEE4	OU=Go Daddy Class 2 Certification Authority, O="The Go Daddy Group, Inc.", C=EE. UU.
0563B8630D62D75ABBC8AB1E4BDFB5A899B24D43	CN=DigiCert Assured ID Root CA, OU=www.digicert.com, O=DigiCert Inc, C=US
DFB16CD4931C973A2037D3FC83A4D7D75D05E4	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=La red USERTRUST, L=Jersey City, S=Nueva Jersey, C=EE. UU.
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

Tabla 1. Lista de certificados necesarios para Cisco Secure Connector.

Paso 3. Descargue los certificados que no estén presentes en el almacén del equipo de los emisores en formato PEM.

> **Sugerencia**: Puede buscar el certificado por la huella digital en Internet. Definen el certificado de forma única.

Paso 4. Abra la consola **mmc** desde el menú Inicio.

Paso 5. Vaya a **Archivo > Agregar o quitar complemento... > Certificados > Agregar > Cuenta de equipo > Siguiente > Finalizar > Aceptar**.

Paso 6. Abra **Certificados** en **Entidades de certificación raíz de confianza**. Haga clic con el botón derecho en la carpeta **Certificates**, luego seleccione **All Tasks > Import...** y siga el asistente para importar el

certificado hasta que aparezca en la carpeta **Certificates**.

Paso 7. Repita el paso 6 si tiene más certificados para importar.

Paso 8. Después de importar todos los certificados, compruebe si la instalación del conector de AMP para terminales se ha realizado correctamente. Si no es así, vuelva a marcar los registros en el archivo immpro_install.log.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).