

# 証明書ハンドシェイク障害による ASA のスマート ライセンスの障害

## 目次

[概要](#)

[問題](#)

[Syslog と デバッグ出力](#)

[解決策](#)

[確認](#)

[関連情報](#)

## 概要

この資料に tools.cisco.com をホストする Webサーバを SHA-2 認証に移行されたかに 2016 年 3 月 18 日発生した変更を当てる方法を記述されています。後その移行は、ASA のいくつかのデバイス ID トークンを登録するときまたは既存の許可を更新するように試みる間、( tools.cisco.com でスマートなソフトウェアに認可する接続しませんホストされる ) ポータル。これは認証関連の問題であるために判別されました。具体的には、別の中間物によって ASA に認証局 ( CA ) 署名される示される ASA より新しい認証は期待し、前もって積みました。

## 問題

ポータルを認可するスマートなソフトウェアに ASA を登録する試みが行われるとき登録は接続か通信障害と失敗します。提示ライセンス登録およびコール ホーム テスト プロファイル license コマンドはこれらの出力を示します。

```
ASA# show license registration
```

```
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Registration Status: Retry In Progress.  
Registration Start Time: Mar 22 13:25:46 2016 UTC  
Last Retry Start Time: Mar 22 13:26:32 2016 UTC.  
Next Scheduled Retry Time: Mar 22 13:45:31 2016 UTC.  
Number of Retries: 1.  
Last License Server response time: Mar 22 13:26:32 2016 UTC.  
Last License Server response message: Communication message send response error
```

```
ASA# call-home test profile License
```

```
INFO: Sending test message to https://tools.cisco.com/its/service/oddce/services/DDCEService...  
ERROR: Failed: CONNECT_FAILED(35)
```

ただし、ASA は tools.cisco.com を解決し、TCPポート 443 で TCP PING と接続できます。

## Syslog と デバッグ出力

試みられた登録の後の ASA の Syslog 出力はこれを示します:

```
%ASA-3-717009: Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:  
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, issuer name:  
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US . [%ASA-3-717009:](#)  
Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 513FB9743870B73440418699FF, subject name:  
**cn=Symantec Class 3 Secure Server CA - G4**,ou=Symantec Trust Network,o=Symantec  
Corporation,c=US, issuer name: 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 .

詳細については別の登録を試みる間、これらのデバッグを実行して下さい。 Secure Socket Layer  
エラーは見られません。

[%ASA-3-717009:](#) Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:  
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, issuer name:  
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US . [%ASA-3-717009:](#)  
Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 513FB9743870B73440418699FF, subject name:  
**cn=Symantec Class 3 Secure Server CA - G4**,ou=Symantec Trust Network,o=Symantec  
Corporation,c=US, issuer name: 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 .

具体的には、このメッセージはその出力の一部として見られます:

[%ASA-3-717009:](#) Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 250CE8E030612E9F2B89F7058FD, subject name:  
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, issuer name:  
ou=Class 3 Public Primary Certification Authority,o=VeriSign\, Inc.,c=US . [%ASA-3-717009:](#)  
Certificate validation failed. No suitable trustpoints found to validate  
certificate serial number: 513FB9743870B73440418699FF, subject name:  
**cn=Symantec Class 3 Secure Server CA - G4**,ou=Symantec Trust Network,o=Symantec  
Corporation,c=US, issuer name: 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 .

デフォルト ASA v 設定では、サブジェクト名に「ロードされ、発行される認証が cn=Verisign ク  
ラス 3 セキュアサーバ CA - G3" ある\_SmartCallHome\_ServerCA と呼ばれるトラストポイントが  
あります。

```
ASAv# show crypto ca certificate
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 6ecc7aa5a7032009b8cebc2d491
```

```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (2048 bits)
```

```
Signature Algorithm: SHA1 with RSA Encryption
```

```
Issuer Name:
```

```
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
```

```
Subject Name:
```

```
cn=VeriSign Class 3 Secure Server CA - G3
```

```
ou=Terms of use at https://www.verisign.com/rpa (c)10
```

```
ou=VeriSign Trust Network
```

```
o=VeriSign\, Inc.
```

```
c=US
```

```
OCSP AIA:
```

```
URL: http://ocsp.verisign.com
```

```
CRL Distribution Points:
```

```
[1] http://crl.verisign.com/pca3-g5.crl
Validity Date:
  start date: 00:00:00 UTC Feb 8 2010
  end   date: 23:59:59 UTC Feb 7 2020
Associated Trustpoints: _SmartCallHome_ServerCA
```

ただし、前の syslog で、ASA は「cn=Symantec クラス 3 セキュアサーバ CA と問い合わせられる中間物が署名するポータルを認可するスマートなソフトウェアから認証を- G4" 得ることを示します。

注: サブジェクト名は類似したですが、2 つの違いがあります; Verisign 対始まりの Symantec および G3 対端に G4。

## 解決策

ASAv はチェーンを検証するために適切な中間物やルート証明が含まれている trustpool をダウンロードする必要があります。

バージョン 9.5.2 および それ 以降では、ASAv に 10:00 PM デバイス 現地時間に trustpool によって設定される自動インポートがあります:

```
ASAv# sh run crypto ca trustpool
crypto ca trustpool policy
auto-import
ASAv# sh run all crypto ca trustpool
crypto ca trustpool policy
revocation-check none
crl cache-time 60
crl enforcenextupdate
auto-import
auto-import url http://www.cisco.com/security/pki/trs/ios_core.p7b
auto-import time 22:00:00
```

これが初期インストールであり、Domain Name System ( DNS ) がその当時の上にルックアップおよびインターネット接続まだなかったら場合、自動インポートは成功しないし、手動で完了する必要があります。

より古いバージョンで、9.4.x のような、trustpool 自動インポートは手動でインポートされるデバイスおよび必要で設定されません。

あらゆるバージョンで、このコマンドは trustpool および関連した認証をインポートします:

```
ASAv# crypto ca trustpool import url http://www.cisco.com/security/pki/trs/ios_core.p7b
Root file signature verified.
You are about to update the current trusted certificate pool
with the 17145 byte file at http://www.cisco.com/security/pki/trs/ios_core.p7b
Do you want to continue? (y/n)
Trustpool import:
  attempted:  14
  installed:  14
  duplicates: 0
  expired:    0
  failed:     0
```

## 確認

trustpool が 10:00 PM 現地時間の後まで手動コマンド、または待っていることによってインポー

トされる、このコマンドは trustpool にインストール済み認証があることを確認します:

```
ASAv# show crypto ca trustpool policy
14 trustpool certificates installed
Trustpool auto import statistics:
  Last import result: FAILED
  Next scheduled import at 22:00:00 UTC Wed Mar 23 2016
Trustpool Policy
  Trustpool revocation checking is disabled
  CRL cache time: 60 seconds
  CRL next update field: required and enforced
  Automatic import of trustpool certificates is enabled
  Automatic import URL: http://www.cisco.com/security/pki/trs/ios_core.p7b
  Download time: 22:00:00
  Policy Overrides:
    None configured
```

注: 前で DNS が操作上自動的に試みた、従ってまだ失敗されるように最後の自動インポート結果を示します最後ではなかったのが最後の自動アップデート インポートを失敗しました出力して下さい。ただし、手動 trustpool アップデートは動作し、( インストールされる 14 の認証をなぜ示すか ) である trustpool アップデートに成功しました。

trustpool がインストールされていた後ポータルを認可するスマートなソフトウェアの ASAv を登録するために、トークン登録 コマンドは再度実行することができます。

```
ASAv# license smart register idtoken id_token force
```

ASAv がポータルを認可するスマートなソフトウェアに既に登録されていたが許可 更新が失敗した場合、それらはまた手動で試みることができます。

```
ASAv# license smart renew auth
```

## 関連情報

- [スマートなライセンス 証明書管理](#)
- [Trustpool 認証の設定オート インポート](#)
- [テクニカルサポートとドキュメント - Cisco Systems](#)