

ASA AnyConnectセキュアモバイルクライアント認証の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[背景説明](#)

[設定](#)

[AnyConnect の証明書](#)

[ASA での証明書のインストール](#)

[単一の認証と証明書の検証のための ASA 設定](#)

[テスト](#)

[デバッグ](#)

[二重認証と証明書の検証のための ASA 設定](#)

[テスト](#)

[デバッグ](#)

[二重認証とプレフィルのための ASA 設定](#)

[テスト](#)

[デバッグ](#)

[二重認証と証明書のマッピングのための ASA 設定](#)

[テスト](#)

[デバッグ](#)

[トラブルシューティング](#)

[有効な証明書がない](#)

[関連情報](#)

はじめに

このドキュメントでは、証明書検証と二重認証を使用するASA AnyConnectセキュアモバイルクライアントアクセスの設定について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- ASA コマンドライン インターフェイス (CLI) 設定および Secure Socket Layer (SSL) VPN 設定に関する基本的な知識
- X509 証明書に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Cisco Adaptive Security Appliance (ASA) ソフトウェア、バージョン 8.4 以降
- Cisco AnyConnect セキュア モビリティ クライアント 3.1 がインストールされた Windows 7

外部認証局 (CA) を使用して、以下を生成することを想定しています。


- ASA(AnyConnect.pfx)用のPublic Key Cryptography Standard #12(PKCS #12)Base64エンコード証明書
- AnyConnect の PKCS #12 証明書

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

背景説明

このドキュメントでは、証明書検証に二重認証を使用する適応型セキュリティ アプライアンス (ASA) Cisco AnyConnect セキュア モビリティ クライアントのアクセスの設定例について説明します。AnyConnect ユーザとして、プライマリおよびセカンダリ認証の正しい証明書およびクレデンシャルを提供して VPN アクセスを取得する必要があります。また、プレフィル機能による証明書マッピングの例も示します。

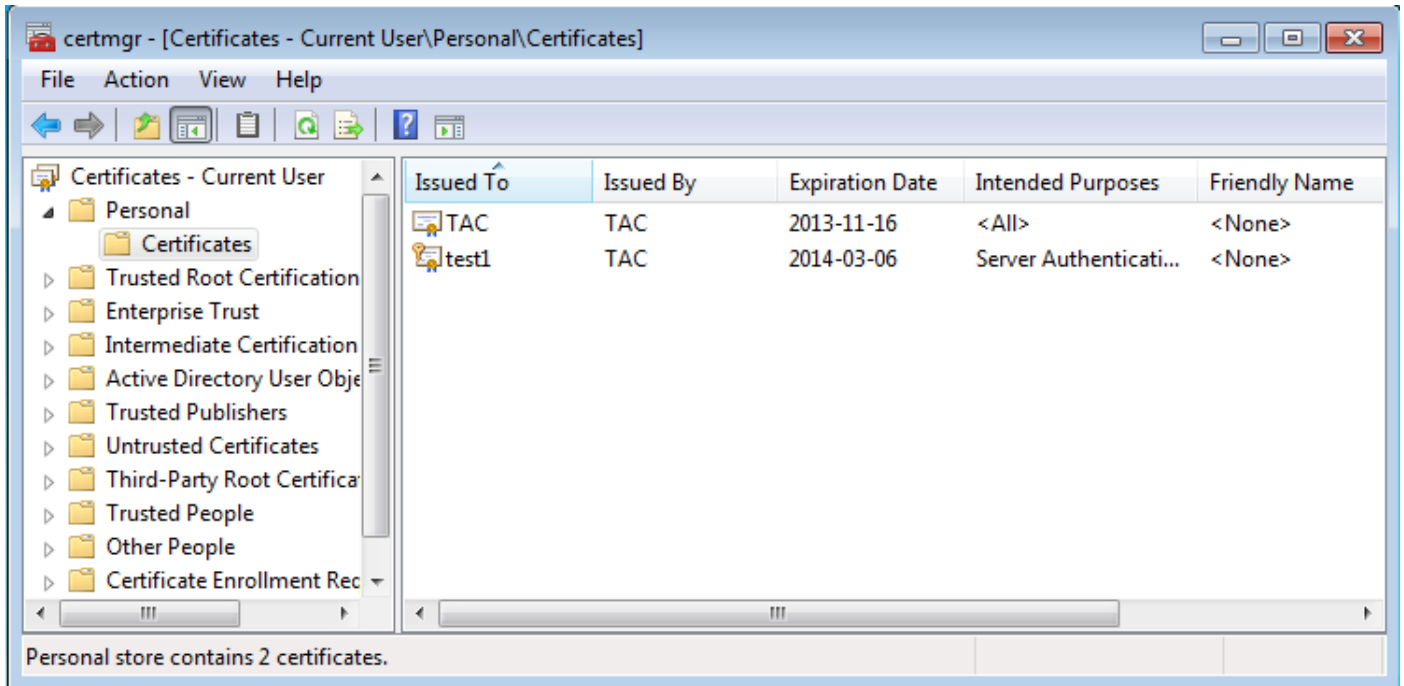
設定

 注：このセクションで使用されているコマンドの詳細を調べるには、[Command Lookup Tool](#) (登録ユーザ専用) を使用してください。シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

AnyConnect の証明書

サンプル証明書をインストールするには、anyconnect.pfx ファイルをダブルクリックし、その証明書を個人用証明書としてインストールします。

インストールを確認するには、Certificate Manager (certmgr.msc) を使用してください。



デフォルトでは、AnyConnectはMicrosoftユーザストアで証明書を検索しようとしています。AnyConnectプロファイルを変更する必要はありません。

ASA での証明書のインストール

次の例は、ASA が Base64 PKCS #12 証明書をインポートする仕組みを示します。

<#root>

```
BSNS-ASA5580-40-1(config)# crypto ca import CA pkcs12 123456
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

```
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggiOMIIIIsDCCBa8GCSqGSIb3DQEH
```

...

<output omitted>

...

```
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkr0IeT1HARHbLF1FFQvSvBAhu0j9bTtZo
```

```
3AICCAA=
```

```
quit
```

```
INFO: Import PKCS12 operation completed successfully
```

show crypto ca certificates コマンドを使用してインポートを確認します。

```
BSNS-ASA5580-40-1(config)# show crypto ca certificates
```

```
CA Certificate
```

```
Status: Available
```

```
Certificate Serial Number: 00cf946de20d0ce6d9
```


```
Certificate Usage: General Purpose
```

```
Public Key Type: RSA (1024 bits)
```

Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=TAC
ou=RAC
o=TAC
l=Warsaw
st=Maz
c=PL
Subject Name:
cn=TAC
ou=RAC
o=TAC
l=Warsaw
st=Maz
c=PL
Validity Date:
start date: 08:11:26 UTC Nov 16 2012
end date: 08:11:26 UTC Nov 16 2013
Associated Trustpoints: CA

Certificate

Status: Available
Certificate Serial Number: 00fe9c3d61e131cda9
Certificate Usage: General Purpose
Public Key Type: RSA (1024 bits)
Signature Algorithm: SHA1 with RSA Encryption
Issuer Name:
cn=TAC
ou=RAC
o=TAC
l=Warsaw
st=Maz
c=PL
Subject Name:
cn=IOS
ou=UNIT
o=TAC
l=Wa
st=Maz
c=PL
Validity Date:
start date: 12:48:31 UTC Nov 29 2012
end date: 12:48:31 UTC Nov 29 2013
Associated Trustpoints: CA

 注:[アウトプットインタープリタツール](#)では、特定のshowコマンドがサポートされています。
。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。シ
スコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

単一の認証と証明書の検証のための ASA 設定

ASA は、認証、承認、アカウントिंग (AAA) の認証と証明書の認証の両方を使用します。証明書の検証は必須です。AAA の認証ではローカル データベースを使用します。

次の例は、証明書の検証による単一の認証を示しています。

```
<#root>
```

```
ip local pool POOL 10.1.1.10-10.1.1.20  
username cisco password cisco
```

```
webvpn  
  enable outside  
  AnyConnect image disk0:/AnyConnect-win-3.1.01065-k9.pkg 1  
  AnyConnect enable  
  tunnel-group-list enable
```

```
group-policy Group1 internal  
group-policy Group1 attributes  
  vpn-tunnel-protocol ssl-client ssl-clientless  
  address-pools value POOL
```

```
tunnel-group RA type remote-access  
tunnel-group RA general-attributes  
  
  authentication-server-group LOCAL
```

```
default-group-policy Group1
```

```
authorization-required
```


```
tunnel-group RA webvpn-attributes
```

```
  authentication aaa certificate
```

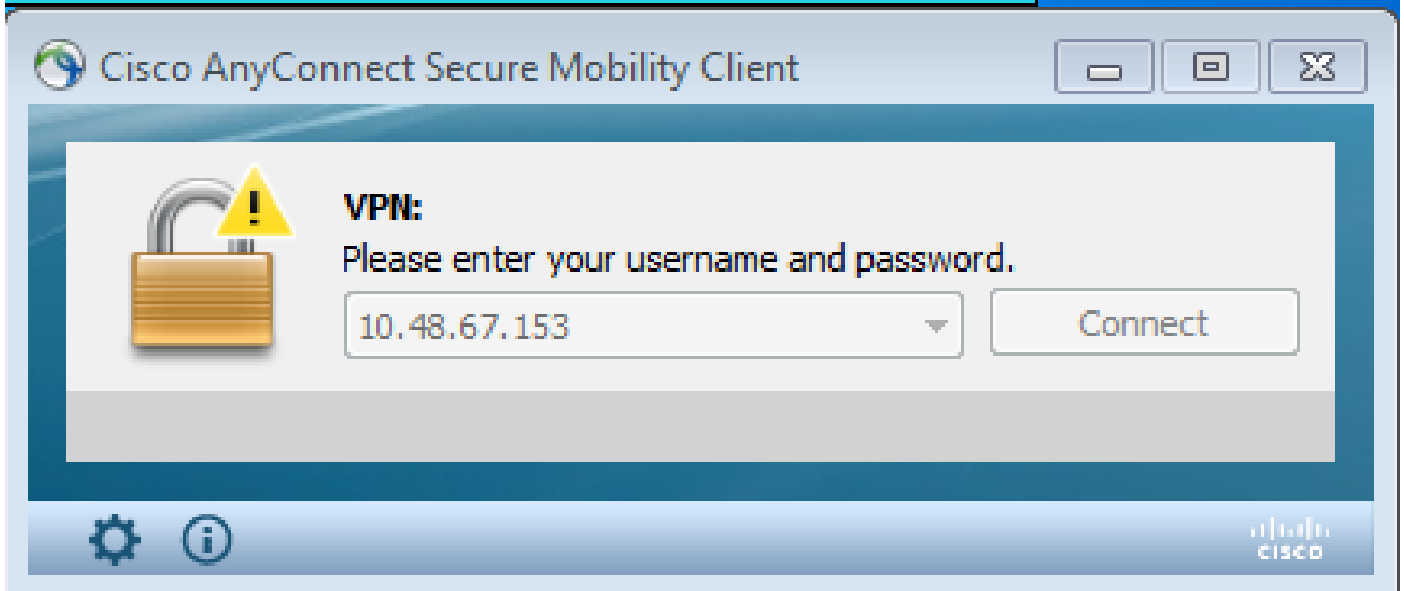
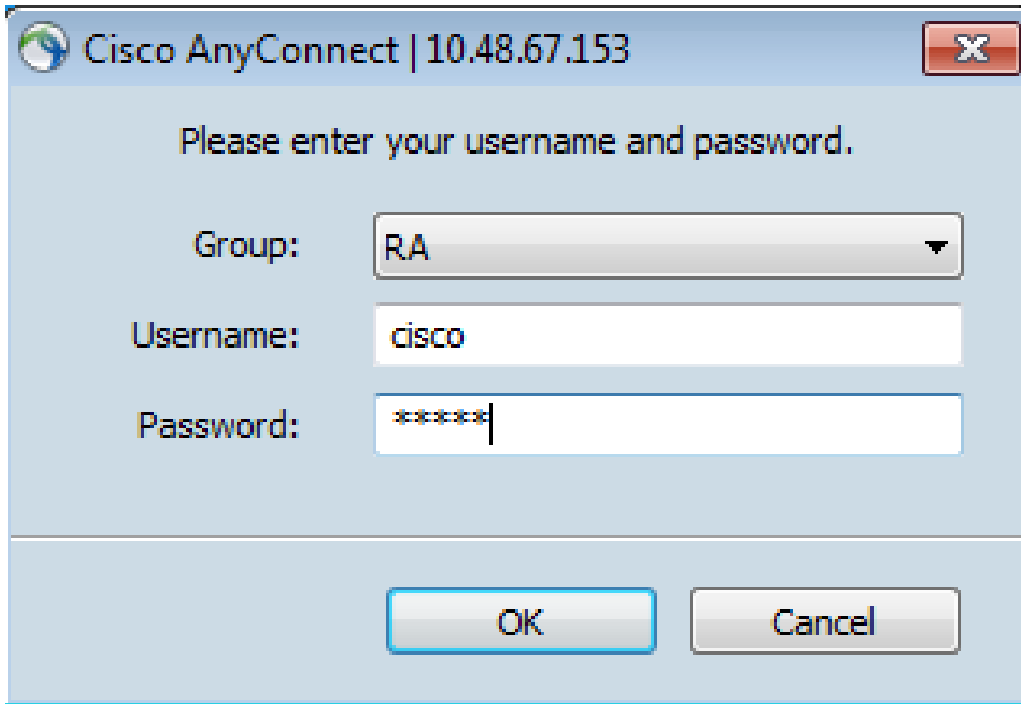
```
group-alias RA enable
```

この設定に加え、証明書名 (CN) などの特定の証明書フィールドからのユーザ名による Lightweight Directory Access Protocol (LDAP) 承認を実行できます。その後、追加の属性を取得して、VPN セッションに適用できます。認証と証明書の承認の詳細については、「[カスタムスキーマおよび証明書による ASA Anyconnect VPN および OpenLDAP の承認の設定例](#)」を参照してください。

テスト

 注:[アウトプットインタープリタツール](#)では、特定のshowコマンドがサポートされています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

この設定をテストするには、ローカル クレデンシャル (ユーザ名 cisco とパスワード cisco) を提供します。次の証明書が存在する必要があります。



ASA で show vpn-sessiondb detail anyconnect コマンドを入力します。

<#root>

```
BSNS-ASA5580-40-1(config-tunnel-general)# show vpn-sessiondb detail AnyConnect  
Session Type: AnyConnect Detailed
```

```
Username      :
```

```
cisco
```

```
Index        : 10
```

```
Assigned IP  :
```

```
10.1.1.10
```

```
Public IP    : 10.147.24.60
```

```
Protocol     : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
```

```
License      : AnyConnect Premium
```

```
Encryption  : RC4 AES128          Hashing      : none SHA1
```

Bytes Tx : 20150 Bytes Rx : 25199
Pkts Tx : 16 Pkts Rx : 192
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Group1 Tunnel Group : RA
Login Time : 10:16:35 UTC Sat Apr 13 2013
Duration : 0h:01m:30s
Inactivity : 0h:00m:00s
NAC Result : Unknown
VLAN Mapping : N/A VLAN : none

AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1

AnyConnect-Parent:

Tunnel ID : 10.1
Public IP : 10.147.24.60
Encryption : none TCP Src Port : 62531
TCP Dst Port : 443 Auth Mode :

Certificate

and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client Type : AnyConnect
Client Ver : 3.1.01065
Bytes Tx : 10075 Bytes Rx : 1696
Pkts Tx : 8 Pkts Rx : 4
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:

Tunnel ID : 10.2
Assigned IP : 10.1.1.10 Public IP : 10.147.24.60
Encryption : RC4 Hashing : SHA1
Encapsulation: TLSv1.0 TCP Src Port : 62535
TCP Dst Port : 443 Auth Mode :

Certificate

and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 28 Minutes
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 3.1.01065
Bytes Tx : 5037 Bytes Rx : 2235
Pkts Tx : 4 Pkts Rx : 11
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:

Tunnel ID : 10.3
Assigned IP : 10.1.1.10 Public IP : 10.147.24.60
Encryption : AES128 Hashing : SHA1
Encapsulation: DTLSv1.0 UDP Src Port : 52818
UDP Dst Port : 443 Auth Mode :

Certificate


and userPassword

Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client Type : DTLS VPN Client
Client Ver : 3.1.01065
Bytes Tx : 0 Bytes Rx : 21268

```
Pkts Tx      : 0
Pkts Tx Drop : 0
Pkts Rx      : 177
Pkts Rx Drop : 0
```

```
NAC:
Reval Int (T): 0 Seconds
SQ Int (T)   : 0 Seconds
Hold Left (T): 0 Seconds
Redirect URL :
Reval Left(T): 0 Seconds
EoU Age(T)   : 92 Seconds
Posture Token:
```

デバッグ

 注：debug コマンドを使用する前に、『debug コマンドの重要な情報』を参照してください。

この例では、証明書がデータベースにキャッシュされておらず、対応する CA が見付き、正しいキー使用方法 (ClientAuthentication) が使用され、証明書が正常に認証されました。

<#root>

```
debug aaa authentication
debug aaa authorization
debug webvpn 255

debug webvpn AnyConnect 255
```

```
debug crypto ca 255
```

debug webvpn 255 コマンドなどの詳細な debug コマンドを使用すると、実稼働環境で多くのログが生成され、ASA への負荷が大きくなる場合があります。一部の WebVPN デバッグは、わかりやすくするために除去されています。

<#root>

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x0000000012cfc50
CERT API thread wakes up!
CERT_API: process msg cmd=0, session=0x0934d687
CERT_API: Async locked for session 0x0934d687
CRYPTO_PKI:
```

```
Checking to see if an identical cert is
```

```
already in the database
```

```
...
CRYPTO_PKI: looking for cert in handle=0x00007ffd8b80ee90, digest=
ad 3d a2 da 83 19 e0 ee d9 b5 2a 83 5c dd e0 70 | .=.....*.\..p
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND
CRYPTO_PKI:
```


Cert not found in database

```
.  
CRYPTO_PKI:  
Looking for suitable trustpoints  
...  
CRYPTO_PKI: Storage context locked by thread CERT API  
CRYPTO_PKI:  
Found a suitable authenticated trustpoint CA  
.  
CRYPTO_PKI(make trustedCerts list)CRYPTO_PKI:check_key_usage: ExtendedKeyUsage  
  OID = 1.3.6.1.5.5.7.3.1  
CRYPTO_PKI:  
check_key_usage:Key Usage check OK
```

```
CRYPTO_PKI:  
Certificate validation: Successful, status: 0
```

```
. Attempting to  
  retrieve revocation status if necessary  
CRYPTO_PKI:Certificate validated. serial number: 00FE9C3D61E131CDB1, subject name:  
cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PL.  
CRYPTO_PKI: Storage context released by thread CERT API  
CRYPTO_PKI: Certificate validated without revocation check
```

次の例では、一致するトンネルグループを見つけようとしています。特定の証明書マッピングルールがないため、指定したトンネルグループが使用されます。

<#root>

```
CRYPTO_PKI: Attempting to find tunnel group for cert with serial number:  
00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,  
c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.  
CRYPTO_PKI:
```

```
No Tunnel Group Match for peer certificate
```

```
.  
CERT_API: Unable to find tunnel group for cert using rules (SSL)
```

次に示すのは、SSL および一般的なセッションのデバッグです。

<#root>

```
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client  
outside:10.147.24.60/64435  
%ASA-7-717025:  
Validating certificate chain containing 1 certificate(s).
```

%ASA-7-717029:

Identified client certificate

within certificate chain. serial
number: 00FE9C3D61E131CDB1, subject name:

cn=test1,ou=Security,o=Cisco,l=Krakow,
st=PL,c=PL

%ASA-7-717030:

Found a suitable trustpoint CA to validate certificate

%ASA-6-717022:

Certificate was successfully validated

. serial number:

00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,
c=PL.

%ASA-6-717028: Certificate chain was successfully validated with warning,
revocation status was not checked.

%ASA-6-725002: Device completed SSL handshake with client outside:

10.147.24.60/64435

%ASA-7-717036:

Looking for a tunnel group match based on certificate maps

for

peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.

%ASA-4-717037:

Tunnel group search using certificate maps failed for peer
certificate

: serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,
l=Warsaw,st=Maz,c=PL.

%ASA-6-113012:

AAA user authentication Successful : local database : user = cisco

%ASA-6-113009:

AAA retrieved default group policy (Group1) for user = cisco

%ASA-6-113008: AAA transaction status ACCEPT : user = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.grouppolicy = Group1

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username1 = cisco

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.username2 =

%ASA-7-734003: DAP: User cisco, Addr 10.147.24.60:

Session Attribute aaa.cisco.tunnelgroup = RA

%ASA-6-734001: DAP: User cisco, Addr 10.147.24.60, Connection AnyConnect: The

following DAP records were selected for this connection: DfltAccessPolicy
%ASA-6-113039: Group <Group1> User <cisco> IP <10.147.24.60> AnyConnect parent
session started.

二重認証と証明書の検証のための ASA 設定

ここで示すのは、プライマリ認証サーバがローカルで、セカンダリ認証サーバが LDAP の二重認証の例です。証明書の検証は、引き続き有効です。

次の例は、LDAP 設定を示しています。

```
aaa-server LDAP protocol ldap
aaa-server LDAP (outside) host 10.147.24.60
  ldap-base-dn DC=test-cisco,DC=com
  ldap-scope subtree
  ldap-naming-attribute uid
  ldap-login-password *****
  ldap-login-dn CN=Manager,DC=test-cisco,DC=com
server-type openldap
```

次に示すのは、セカンダリ認証サーバの追加です。

```
<#root>
```

```
tunnel-group RA general-attributes

  authentication-server-group LOCAL
  secondary-authentication-server-group LDAP

default-group-policy Group1

authorization-required


tunnel-group RA webvpn-attributes

authentication aaa certificate
```

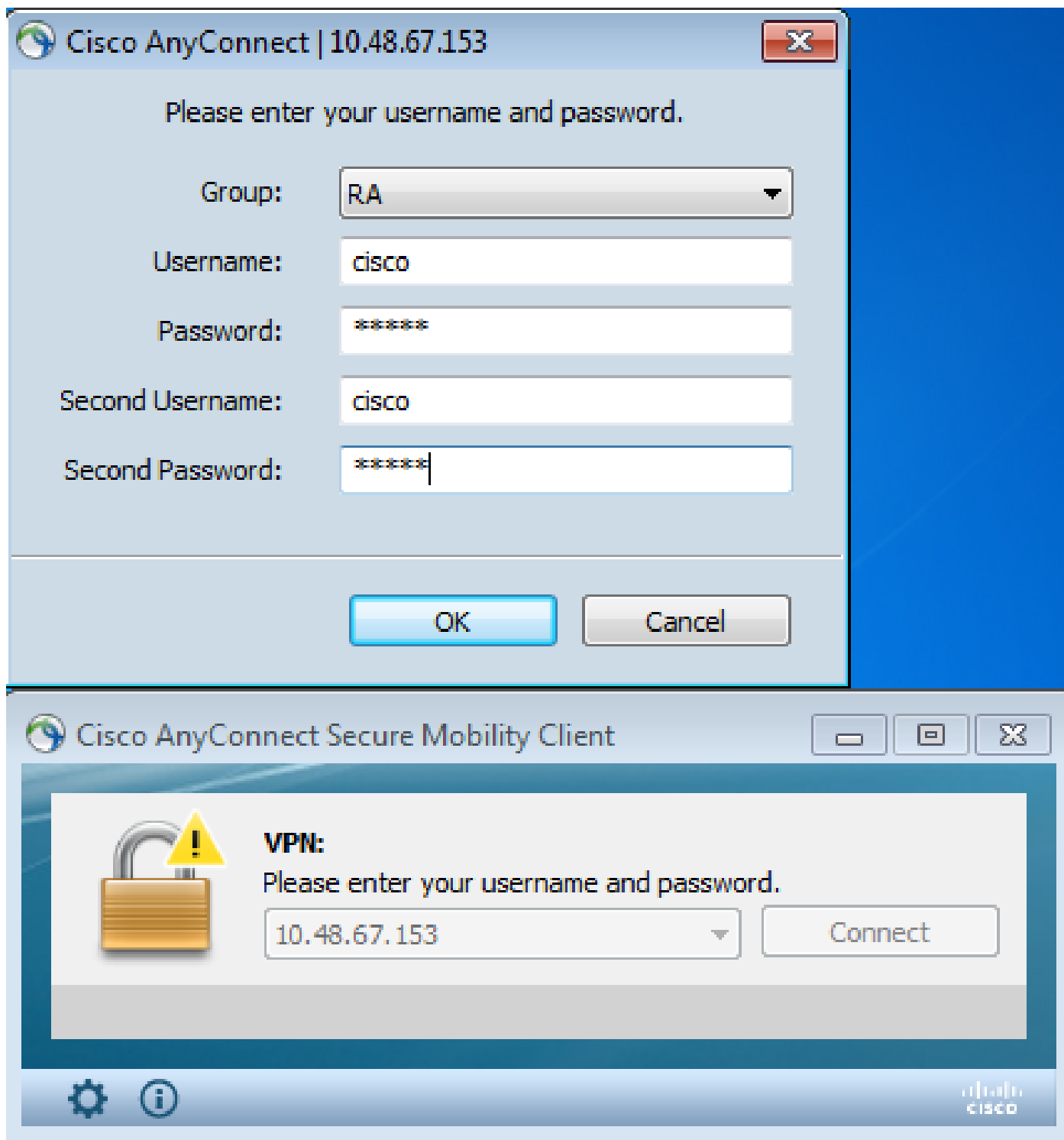
「authentication-server-group LOCAL」は、デフォルト設定であるため、設定には表示されません。

他の任意の AAA サーバを「authentication-server-group」として使用できます。「secondary-authentication-server-group」では、Security Dynamics International(SDI)サーバを除くすべての AAAサーバを使用できます。この場合でも、SDIをプライマリ認証サーバにできます。

テスト

 注:[アウトプットインタープリタツール](#)では、特定のshowコマンドがサポートされています。show コマンドの出力の分析を表示するには、Output Interpreter Tool を使用します。シスコの内部ツールおよび情報にアクセスできるのは、登録ユーザのみです。

この設定をテストするには、ローカル クレデンシャル (ユーザ名 cisco とパスワード cisco) および LDAP クレデンシャル (ユーザ名 cisco と LDAP のパスワード) を提供します。次の証明書が存在する必要があります。



The image shows two screenshots of the Cisco AnyConnect interface. The top screenshot is a login dialog box titled "Cisco AnyConnect | 10.48.67.153". It prompts the user to "Please enter your username and password." and contains the following fields: "Group:" with a dropdown menu set to "RA"; "Username:" with the text "cisco"; "Password:" with masked characters "*****"; "Second Username:" with the text "cisco"; and "Second Password:" with masked characters "*****". There are "OK" and "Cancel" buttons at the bottom. The bottom screenshot is the "Cisco AnyConnect Secure Mobility Client" window. It features a warning icon (a padlock with a yellow triangle) and the text "VPN: Please enter your username and password." Below this is a dropdown menu showing "10.48.67.153" and a "Connect" button. The bottom of the window has a status bar with a gear icon, an information icon, and the Cisco logo.

ASA で show vpn-sessiondb detail anyconnect コマンドを入力します。

結果は、単一の認証の場合と同様です。「[単一の認証と証明書の検証のための ASA 設定、テスト](#)」を参照してください。

デバッグ

WebVPN セッションおよび認証のデバッグは同様です。「[単一の認証と証明書の検証のための ASA 設定、デバッグ](#)」を参照してください。追加の認証プロセスが 1 つ表示されます。

```
<#root>
```

```
%ASA-6-113012:
```

```
AAA user authentication Successful : local database : user = cisco
```

```
%ASA-6-302013: Built outbound TCP connection 1936 for outside:10.147.24.60/389  
(10.147.24.60/389) to identity:10.48.67.153/54437 (10.48.67.153/54437)
```

```
%ASA-6-113004:
```

```
AAA user authentication Successful : server = 10.147.24.60 :  
user = cisco
```

```
%ASA-6-113009: AAA retrieved default group policy (Group1) for user = cisco
```

```
%ASA-6-113008: AAA transaction status ACCEPT : user = cisco
```

LDAPのデバッグには、LDAP設定によって異なる詳細が表示されます。

```
[34] Session Start  
[34] New request Session, context 0x00007ffd8d7dd828, reqType = Authentication  
[34] Fiber started  
[34] Creating LDAP context with uri=ldap://10.147.24.60:389  
[34] Connect to LDAP server: ldap://10.147.24.60:389, status = Successful  
[34] supportedLDAPVersion: value = 3  
[34] Binding as Manager  
[34] Performing Simple authentication for Manager to 10.147.24.60  
[34] LDAP Search:  
      Base DN = [DC=test-cisco,DC=com]  
      Filter  = [uid=cisco]  
      Scope   = [SUBTREE]  
[34] User DN = [uid=cisco,ou=People,dc=test-cisco,dc=com]  
[34] Server type for 10.147.24.60 unknown - no password policy  
[34] Binding as cisco  
[34] Performing Simple authentication for cisco to 10.147.24.60  
[34] Processing LDAP response for user cisco  
[34] Authentication successful for cisco to 10.147.24.60  
[34] Retrieved User Attributes:  
[34]   cn: value = John Smith  
[34]   givenName: value = John  
[34]   sn: value = cisco  
[34]   uid: value = cisco  
[34]   uidNumber: value = 10000  
[34]   gidNumber: value = 10000  
[34]   homeDirectory: value = /home/cisco  
[34]   mail: value = name@dev.local
```

```
[34] objectClass: value = top
[34] objectClass: value = posixAccount
[34] objectClass: value = shadowAccount
[34] objectClass: value = inetOrgPerson
[34] objectClass: value = organizationalPerson
[34] objectClass: value = person
[34] objectClass: value = CiscoPerson
[34] loginShell: value = /bin/bash
[34] userPassword: value = {SSHA}pndf5sfjscTPuyrhL+/QUqhK+i1UCUTy
[34] Fiber exit Tx=315 bytes Rx=911 bytes, status=1
[34] Session End
```

二重認証とプレフィルのための ASA 設定

プライマリおよびセカンダリ認証に使用されるユーザ名に、特定の証明書フィールドをマッピングできます。

```
<#root>
```

```
username test1 password cisco
```

```
tunnel-group RA general-attributes
```

```
authentication-server-group LOCAL
```

```
secondary-authentication-server-group LDAP
```

```
default-group-policy Group1
authorization-required
```

```
username-from-certificate CN
```

```
secondary-username-from-certificate OU
```

```
tunnel-group RA webvpn-attributes
```

```
authentication aaa certificate
```

```
pre-fill-username ssl-client
```

```
secondary-pre-fill-username ssl-client
```

```
group-alias RA enable
```

この例では、クライアントは証明書cn=test1,ou=Security,o=Cisco,l=Krakow,st=PL,c=PLを使用します。

プライマリ認証では、ユーザ名が CN から取得されます。ローカル ユーザ「test1」が作成されて

いるのは、このためです。

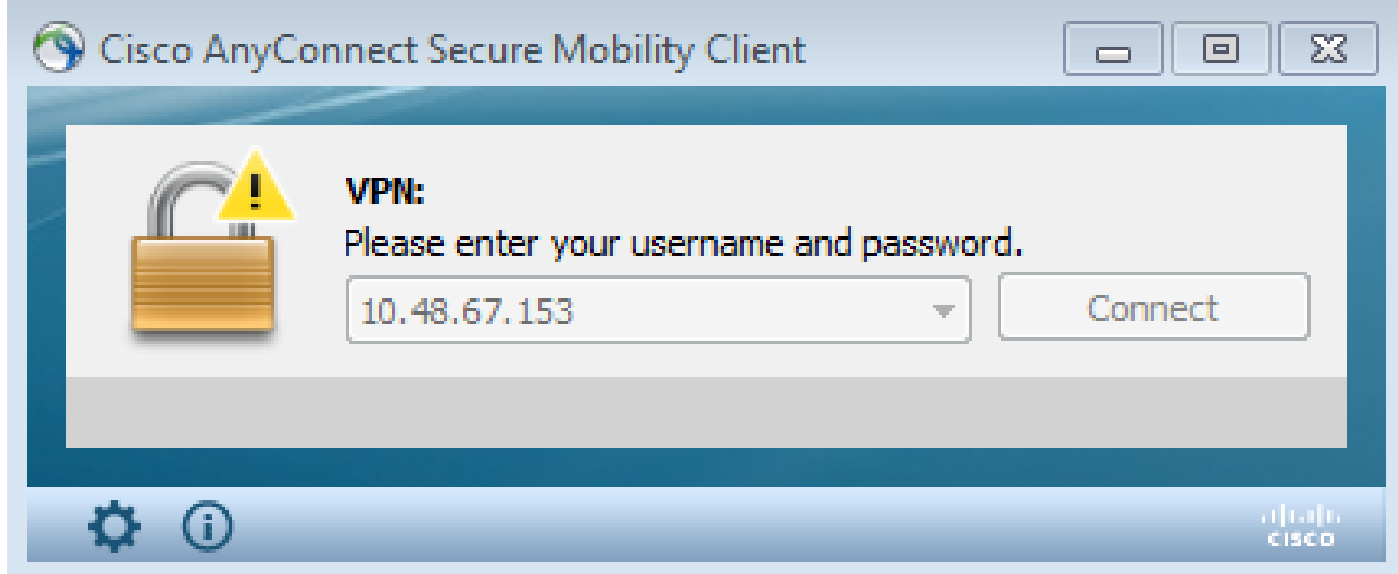
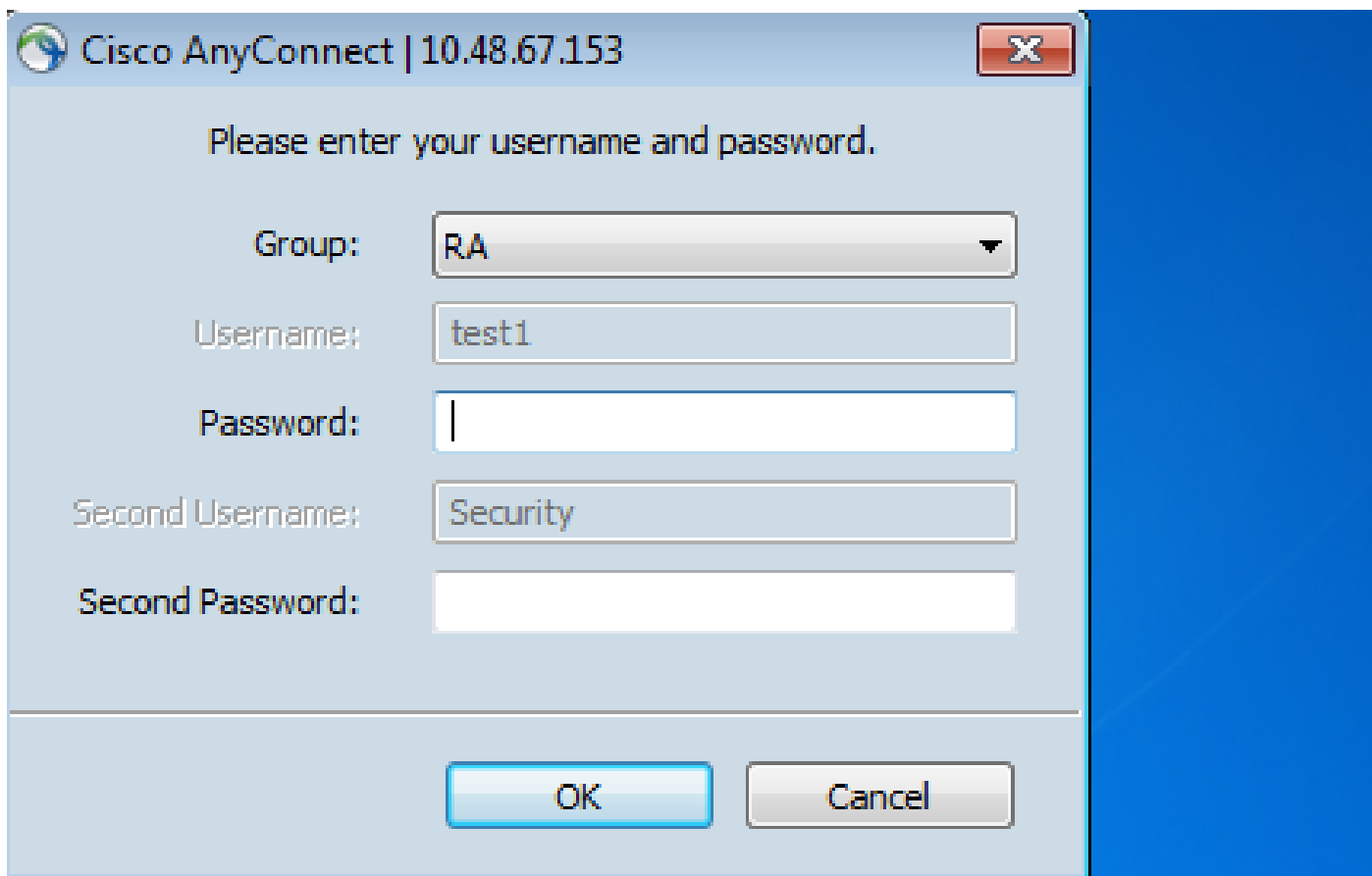
セカンダリ認証では、ユーザ名が組織ユニット (OU) から取得されます。ユーザ「Security」が LDAP サーバで作成されているのは、このためです。

また、強制的に AnyConnect でプレフィル コマンドを使用して、プライマリおよびセカンダリ ユーザ名をプレフィルすることも可能です。

実際のシナリオでは、プライマリ認証サーバは、AD または LDAP サーバであるのが普通であり、セカンダリ認証サーバは、トークン パスワードを使用する Rivest、Shamir、または Adelman (RSA) サーバです。このシナリオでは、ユーザが、AD/LDAP クレデンシャル (ユーザが知っている)、RSA トークン パスワード (ユーザが知っている)、および証明書 (使用するマシンにある) を提供する必要があります。

テスト

プライマリまたはセカンダリ ユーザ名は、証明書の CN フィールドと OU フィールドからプレフィルされているため、変更できないことに注意してください。



デバッグ

次の例は、AnyConnect に送信されるプレフィル要求を示しています。

```
%ASA-7-113028: Extraction of username from VPN client certificate has been requested. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has started. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has finished successfully. [Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
```



```
[Request 5]
%ASA-7-113028: Extraction of username from VPN client certificate has been
requested. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has started.
[Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has finished
successfully. [Request 6]
%ASA-7-113028: Extraction of username from VPN client certificate has completed.
[Request 6]
```

ここでは、認証で正しいユーザ名が使用されていることがわかります。

```
<#root>
```

```
%ASA-6-113012:
AAA user authentication Successful : local database : user = test1

%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)
%ASA-6-113004:
AAA user authentication Successful : server = 10.147.24.60 :
user = Security
```


二重認証と証明書のマッピングのための ASA 設定

次に示すように、特定のトンネルグループに特定のクライアント証明書をマッピングすることも可能です。

```
crypto ca certificate map CERT-MAP 10
  issuer-name co tac

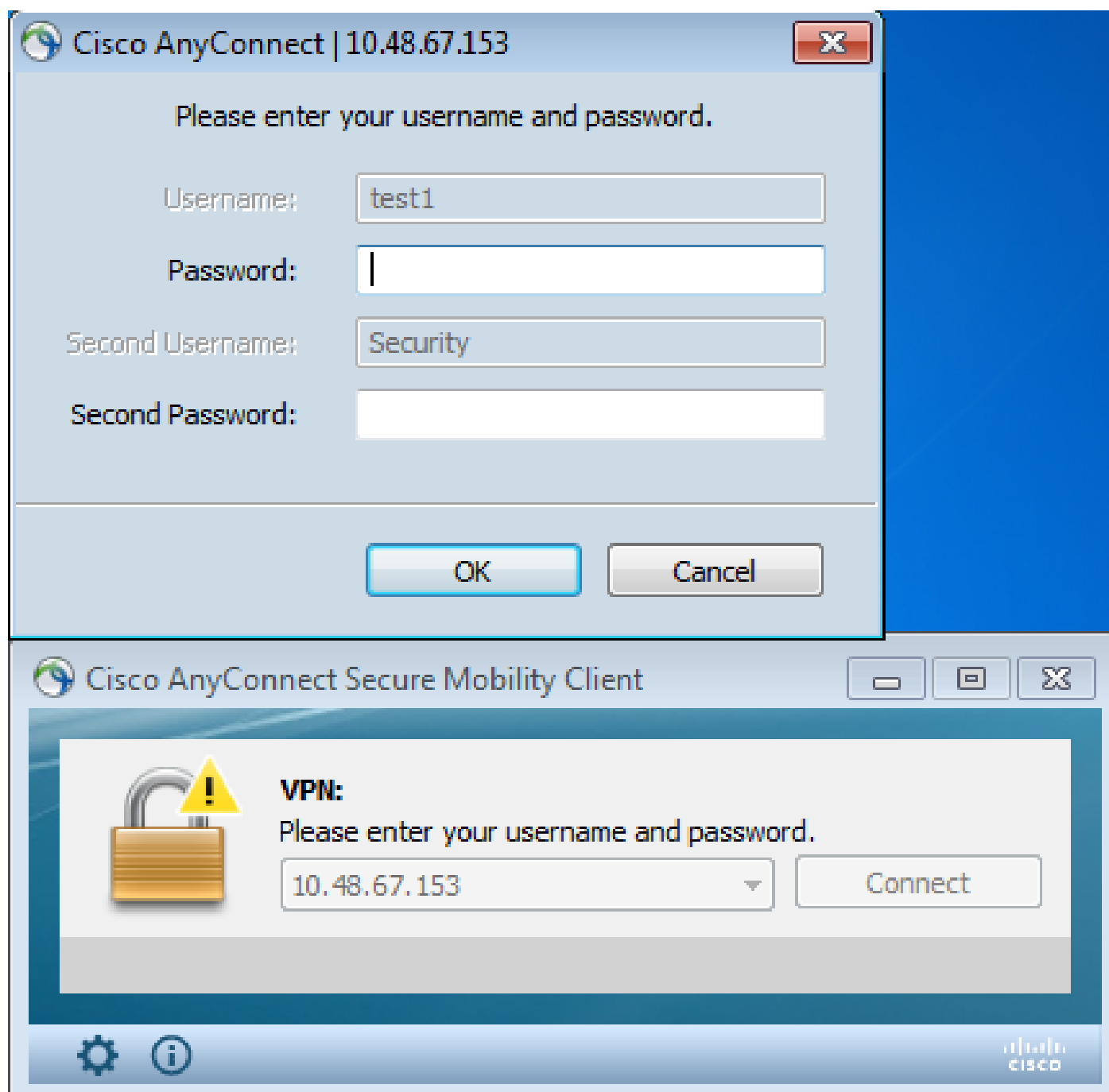
webvpn
  certificate-group-map CERT-MAP 10 RA
```

こうすると、Cisco Technical Assistance Center (TAC) CA によって署名されたすべてのユーザ証明書が、「RA」という名前のトンネルグループにマッピングされます。

 注:SSLの証明書マッピングは、IPsecの証明書マッピングとは異なる方法で設定されます。IPsecの場合、グローバルコンフィギュレーションモードで「tunnel-group-map」ルールを使用して設定されます。SSLの場合は、webvpn設定モードで「certificate-group-map」を使用して設定されます。

テスト

証明書マッピングを有効にした後は、トンネルグループを選択する必要がなくなる点に注意してください。



デバッグ

次の例では、証明書マッピングのルールによりトンネルグループが見つかります。

```
<#root>
```

```
%ASA-7-717036:
```

```
Looking for a tunnel group match based on certificate maps
```

```
for  
peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,
```

```
ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,  
l=Warsaw,st=Maz,c=PL.  
%ASA-7-717038:
```

Tunnel group match found. Tunnel Group: RA

, Peer certificate:

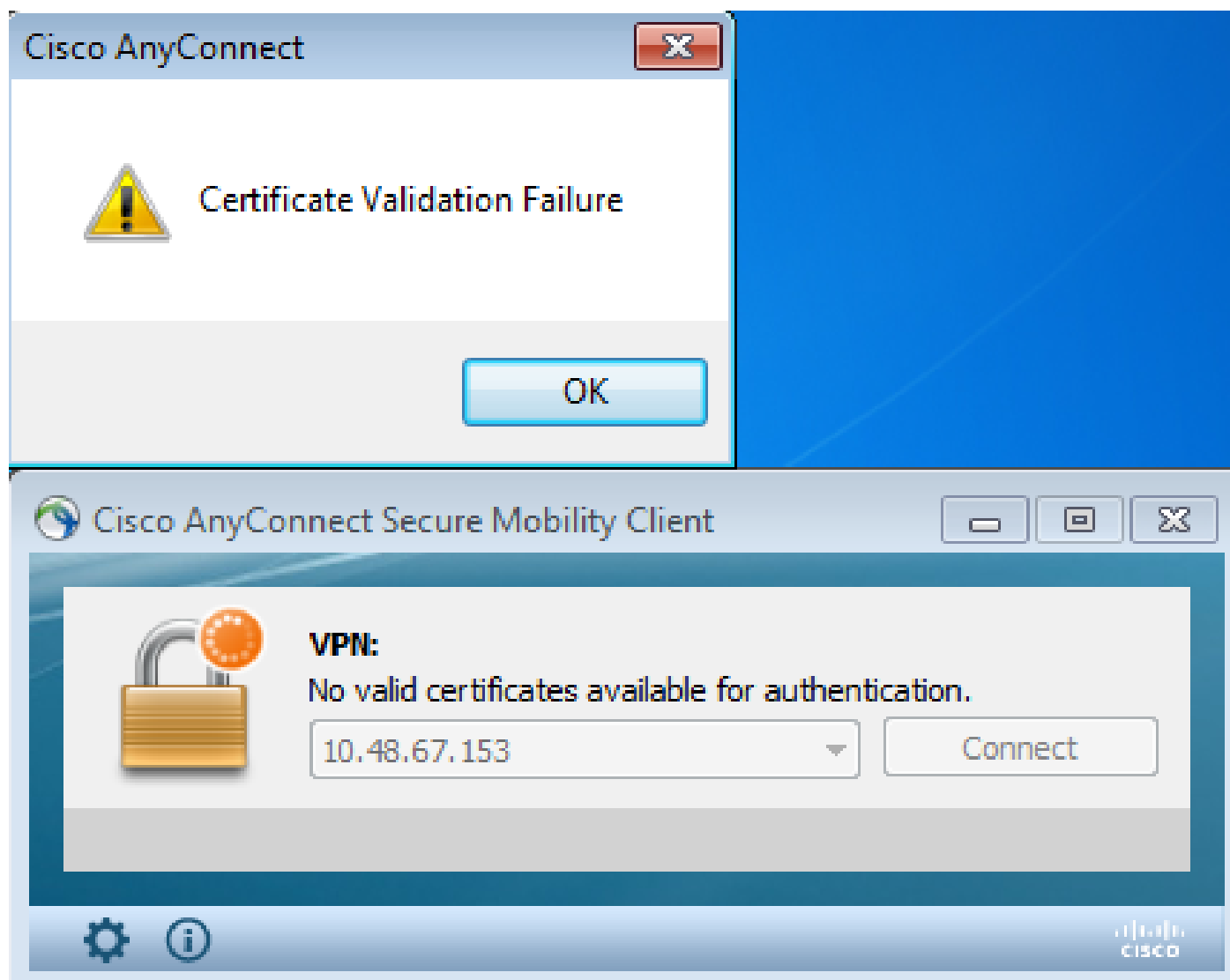
```
serial number: 00FE9C3D61E131CDB1, subject name: cn=test1,ou=Security,o=Cisco,  
l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.
```

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

有効な証明書がない

Windows7 から有効な証明書を削除した後、AnyConnect で、有効な証明書が見つかりません。



ASA では、クライアント (Reset-I) がセッションを終了したように見えます。

<#root>

```
%ASA-6-302013: Built inbound TCP connection 2489 for outside:10.147.24.60/52838
(10.147.24.60/52838) to identity:10.48.67.153/443 (10.48.67.153/443)
%ASA-6-725001: Starting SSL handshake with client outside:10.147.24.60/52838 for
TLSv1 session.
%ASA-7-725010: Device supports the following 4 cipher(s).
%ASA-7-725011: Cipher[1] : RC4-SHA
%ASA-7-725011: Cipher[2] : AES128-SHA
%ASA-7-725011: Cipher[3] : AES256-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725008: SSL client outside:10.147.24.60/52838 proposes the following 8
cipher(s).
%ASA-7-725011: Cipher[1] : AES128-SHA
%ASA-7-725011: Cipher[2] : AES256-SHA
%ASA-7-725011: Cipher[3] : RC4-SHA
%ASA-7-725011: Cipher[4] : DES-CBC3-SHA
%ASA-7-725011: Cipher[5] : DHE-DSS-AES128-SHA
%ASA-7-725011: Cipher[6] : DHE-DSS-AES256-SHA
%ASA-7-725011: Cipher[7] : EDH-DSS-DES-CBC3-SHA
%ASA-7-725011: Cipher[8] : RC4-MD5
%ASA-7-725012: Device chooses cipher : RC4-SHA for the SSL session with client
outside:10.147.24.60/52838
%ASA-6-302014:

Teardown TCP connection 2489 for outside:10.147.24.60/52838 to
identity:10.48.67.153/443 duration 0:00:00 bytes 1448 TCP Reset-I
```

関連情報

- [トンネルグループ、グループポリシー、およびユーザの設定：二重認証の設定](#)
- [セキュリティアプライアンスユーザ認証用の外部サーバの設定](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。