Configure ASA AnyConnect Secure Mobility Client Authentication

Contents

Introduction

This document describes a configuration for ASA AnyConnect Secure Mobility Client access that uses double authentication with certificate validation.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA command-line interface (CLI) configuration and Secure Socket Layer (SSL) VPN configuration
- Basic knowledge of X509 certificates

Components Used

The information in this document is based on these software versions:

- Cisco Adaptive Security Appliance (ASA) software, version 8.4 and later

- Windows 7 with Cisco AnyConnect Secure Mobility Client 3.1

It is assumed that you used an external Certificate Authority (CA) in order to generate:

- A public-key cryptography standard #12 (PKCS #12) base64-encoded certificate for ASA (AnyConnect.pfx)
- A PKCS #12 certificate for AnyConnect

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

This document describes a configuration example for Adaptive Security Appliance (ASA) Cisco AnyConnect Secure Mobility Client access that uses double authentication with certificate validation. As an AnyConnect user, you must provide the correct certificate and credentials for the primary and secondary authentication in order to get VPN access. This document also provides an example of certificate mapping with the pre-fill feature.

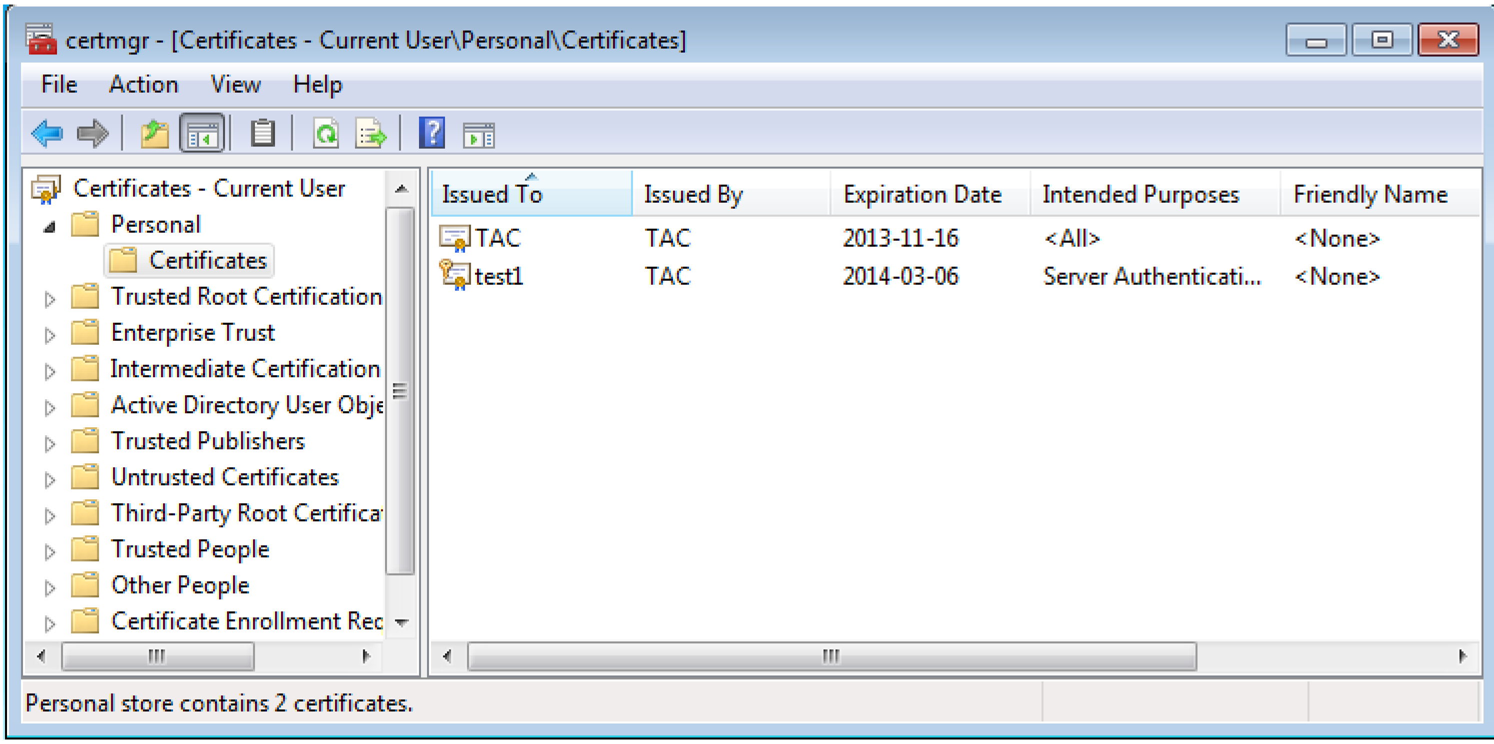
Configure

> **Note**: Use the Command Lookup Tool in order to obtain more information on the commands used in this section. Only registered Cisco users can access internal Cisco tools and information.

Certificate for AnyConnect

In order to install an example certificate, double-click the AnyConnect.pfx file, and install that certificate as a personal certificate.

Use the Certificate Manager (certmgr.msc) in order to verify the installation:


certmgr - [Certificates - Current User\Personal\Certificates]
File
Action
View
Help
Certificates - Current User
Personal
Certificates
Trusted Root Certification
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certifica
Trusted People
Other People
Certificate Enrollment Rec

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
TAC	TAC	2013-11-16	<All>	<None>
test1	TAC	2014-03-06	Server Authenticati...	<None>

Personal store contains 2 certificates.

By default, AnyConnect tries to find a certificate in the Microsoft user store; there is no need to make any changes in the AnyConnect profile.

Certificate Installation on ASA

This example shows how ASA can import a base64 PKCS #12 certificate:

<#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:
MIIJAQIBAzCCCMcGCSqGSIb3DQEHAaCCCLgEggi0MIIIsDCCBa8GCSqGSIb3DQEH
...
<output ommitted>
...
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBSkrOIeT1HARHbLF1FFQvSvBAhu0j9bTtZo
3AICCAA=
quit


INFO: Import PKCS12 operation completed successfully
```

Use the **show crypto ca certificates** command in order to verify the import:

```
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
```

Note: The Output Interpreter Tool supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output. Only registered Cisco users can access internal Cisco tools and information.

ASA Configuration for Single Authentication and Certificate Validation

ASA uses both authentication, authorization, and accounting (AAA) authentication and certificate authentication. Certificate validation is mandatory. AAA authentication uses a local database.

This example shows single authentication with certificate validation.

<#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
```

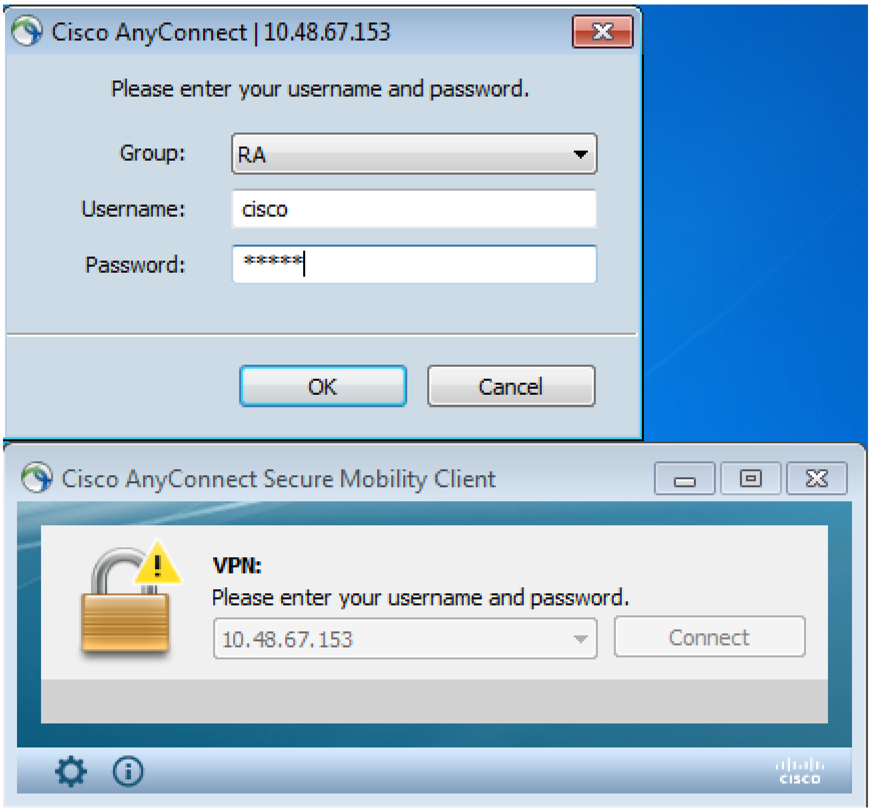
```
tunnel-group RA webvpn-attributes
 authentication aaa certificate

 group-alias RA enable
```

In addition to this configuration, it is possible to perform Lightweight Directory Access Protocol (LDAP) authorization with the username from a specific certificate field, such as the certificate name (CN). Additional attributes can then be retrieved and applied to the VPN session. For more information on authentication and certificate authorization, refer to "ASA AnyConnect VPN and OpenLDAP Authorization with Custom Schema and Certificates Configuration Example."

Test

> **Note**: The Output Interpreter Tool supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output. Only registered Cisco users can access internal Cisco tools and information.

In order to test this configuration, provide the local credentials (username cisco with password cisco). The certificate must be present:



Cisco AnyConnect | 10.48.67.153

Please enter your username and password.

Group: RA

Username: cisco

Password: *****

VPN:
Please enter your username and password.

10.48.67.153

Enter the **show vpn-sessiondb detail AnyConnect** command on the ASA:

<#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 Rx      : 177
  Pkts Tx Drop : 0                      Pkts Rx Drop : 0

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

Debug

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

In this example, the certificate was not cached in the database, a corresponding CA has been found, the correct Key usage was used (ClientAuthentication), and the certificate has been validated successfully:

<#root>

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

debug webvpn AnyConnect 255


debug crypto ca 255
```

Detailed debug commands, such as the **debug webvpn 255** command, can generate many logs in a production environment and place a heavy load on an ASA. Some WebVPN debugs have been removed for clarity:

<#root>

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x00000000012cfc50
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
```

This is the attempt to find a matching tunnel-group. There are no specific certificate mapping rules, and the tunnel-group that you provide is used:

<#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)
```

These are the SSL and general session debugs:

<#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.
```

ASA Configuration for Double Authentication and Certificate Validation

This is an example of double authentication, where the primary authentication server is LOCAL, and the secondary authentication server is LDAP. Certificate validation is still enabled.

This example shows the LDAP configuration:

```
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
```

Here is the addition of a secondary authentication server:

<#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
```

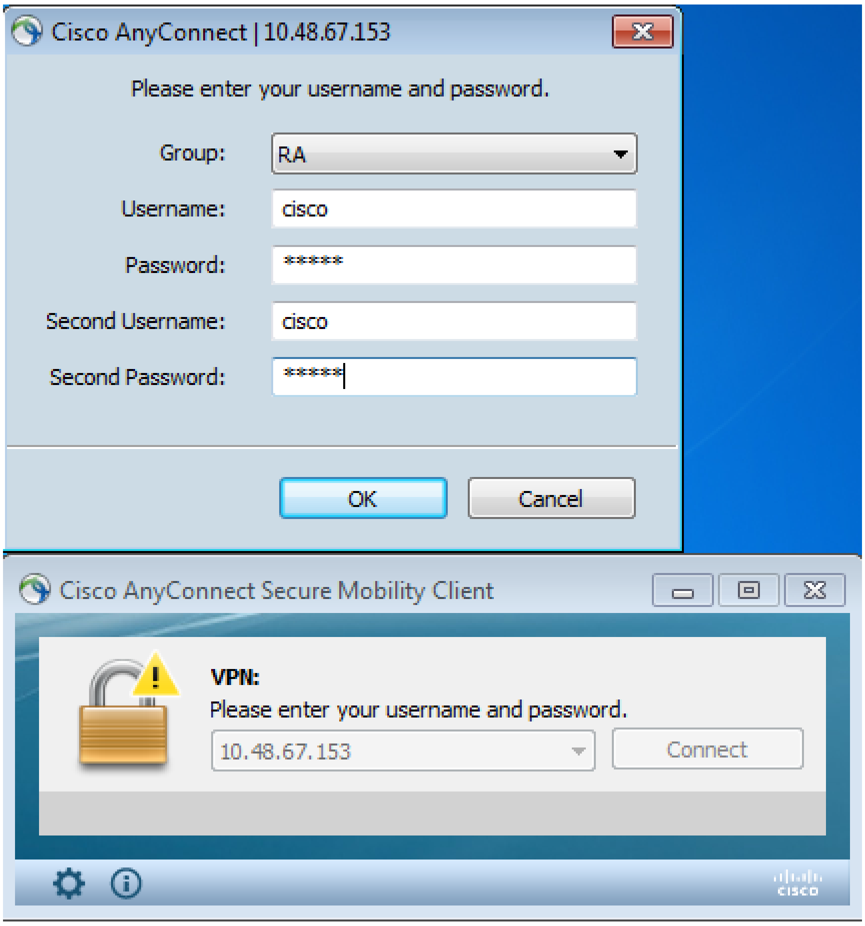
You do not see 'authentication-server-group LOCAL' in the configuration because it is a default setting.

Any other AAA server can be used for 'authentication-server-group.' For 'secondary-authentication-server-group,' it is possible to use all AAA servers except for a Security Dynamics International (SDI) server; in that case, the SDI could still be the primary authentication server.

Test

Note: The Output Interpreter Tool supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output. Only registered Cisco users can access internal Cisco tools and information.

In order to test this configuration, provide the local credentials (username cisco with password cisco) and LDAP credentials (username cisco with password from LDAP). The certificate must be present:



Cisco AnyConnect | 10.48.67.153

Please enter your username and password.

Group: RA

Username: cisco

Password: *****

Second Username: cisco

Second Password: *****

Cisco AnyConnect Secure Mobility Client

VPN:

Please enter your username and password.

10.48.67.153

Enter the **show vpn-sessiondb detail AnyConnect** command on the ASA.

Results are similar to those for single authentication. Refer to "ASA Configuration for Single Authentication and Certificate Validation, Test."

Debug

Debugs for WebVPN session and authentication are similar. Refer to "ASA Configuration for Single Authentication and Certificate Validation, Debug." One additional authentication process appears:

<#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
```

Debugs for LDAP show details that can vary with the LDAP configuration:

```
[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
```

ASA Configuration for Double Authentication and Pre-Fill

It is possible to map certain certificate fields to the username that is used for primary and secondary authentication:

<#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
```

In this example, the client uses the certificate: cn=**test1**,ou=**Security**,o=Cisco,l=Krakow,st=PL,c=PL.

For primary authentication, the username is taken from the CN, which is why local user 'test1' was created.

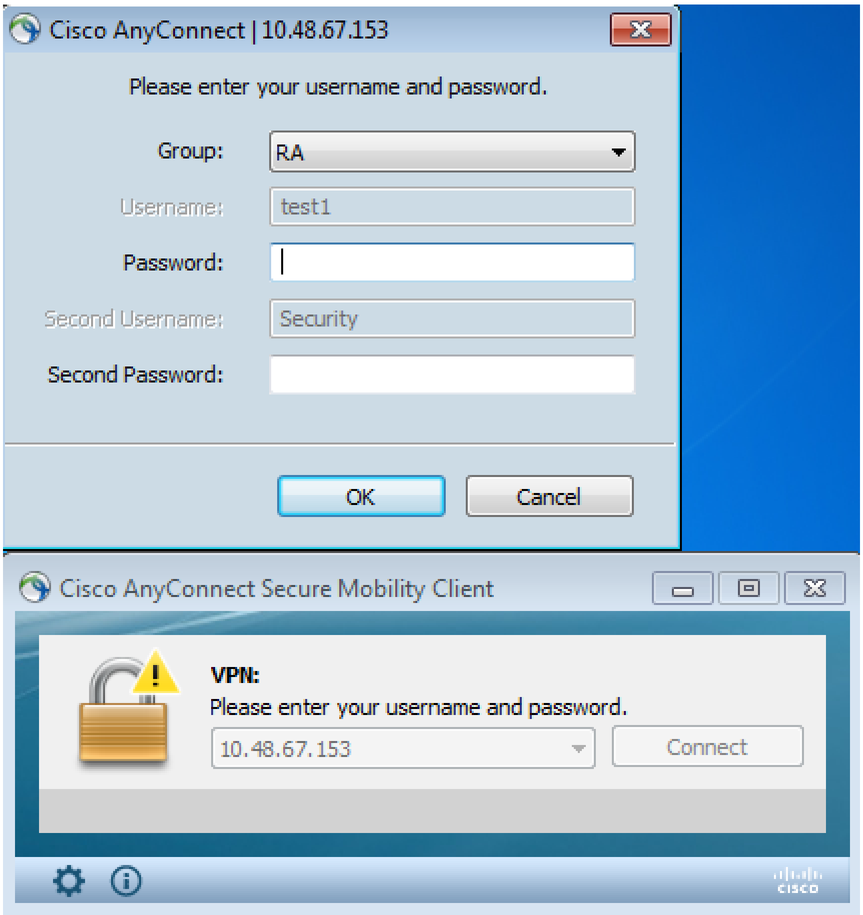
For secondary authentication, the username is taken from the organizational unit (OU, which is why user 'Security' was created on the LDAP server.

It is also possible to force AnyConnect to use pre-fill commands in order to pre-fill the primary and secondary username.

In a real world scenario, the primary authentication server is usually an AD or LDAP server, while the secondary authentication server is the Rivest, Shamir, and Adelman (RSA) server that uses token passwords. In this scenario, the user must provide AD/LDAP credentials (which the user knows), an RSA token password (which the user has) and a certificate (on the machine that is used).

Test

Observe that you cannot change the primary or secondary username because it is pre-filled from the certificate CN and OU fields:



Cisco AnyConnect | 10.48.67.153

Please enter your username and password.

Group: RA

Username: test1

Password:

Second Username: Security

Second Password:

Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

10.48.67.153

Debug

This example shows the pre-fill request sent to AnyConnect:

```
%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]
```

Here you see that authentication uses the correct usernames:

<#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
```

ASA Configuration for Double Authentication and Certificate Mapping

It is also possible to map specific client certificates to specific tunnel-groups, as shown in this example:

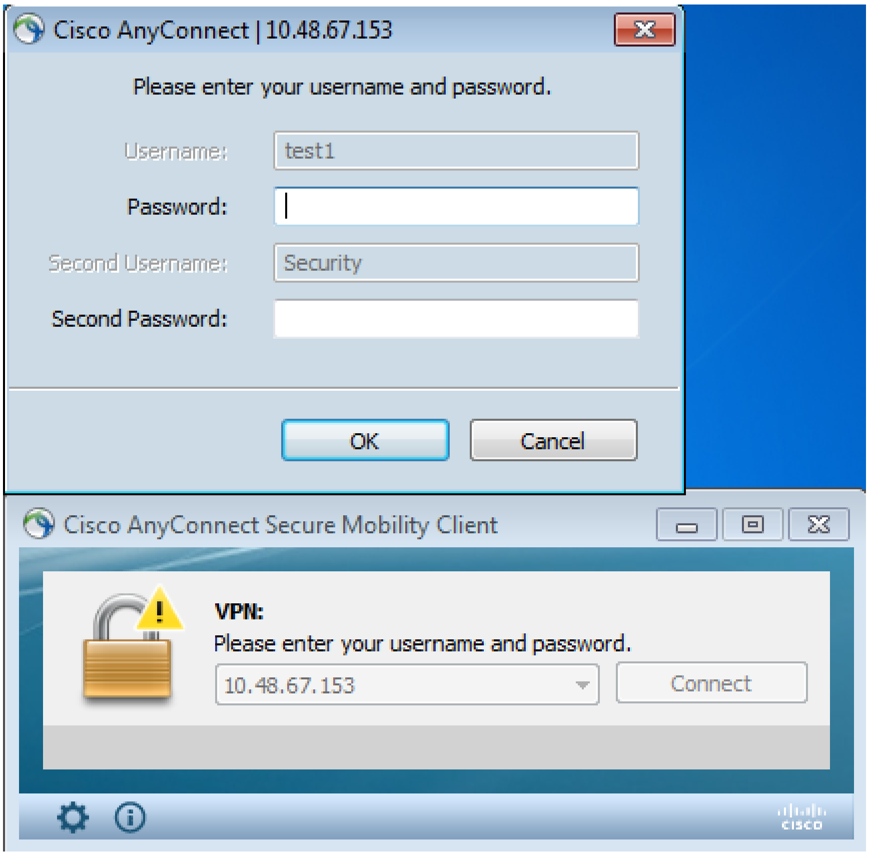
```
crypto ca certificate map CERT-MAP 10
 issuer-name co tac

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

This way, all user certificates signed by the Cisco Technical Assistance Center (TAC) CA are mapped to a tunnel-group named 'RA.'

> **Note**: Certificate mapping for SSL is configured differently than certificate mapping for IPsec. For IPsec, it is configured with 'tunnel-group-map' rules in global config mode. For SSL, it is configured with 'certificate-group-map' under webvpn config mode.

Test

Observe that, once certificate mapping is enabled, you do not need to choose tunnel-group anymore:


Cisco AnyConnect | 10.48.67.153

Please enter your username and password.

Username: test1

Password:

Second Username: Security

Second Password:

Cisco AnyConnect Secure Mobility Client

VPN:
Please enter your username and password.

10.48.67.153

Debug

In this example, the certificate mapping rule allows the tunnel-group to be found:

<#root>

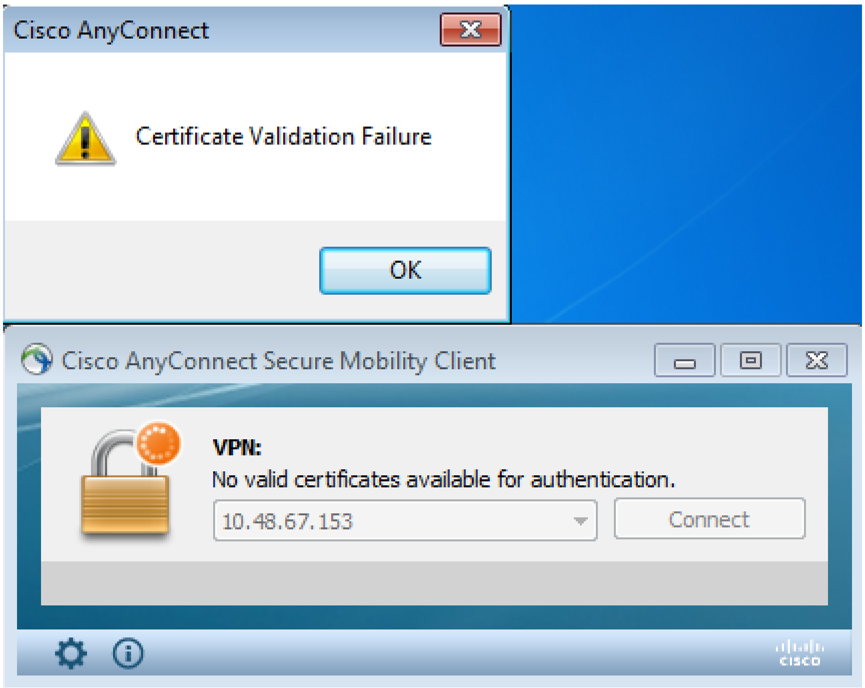
```
%ASA-7-717036:

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.
```

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Valid Certificate Not Present

After you remove a valid certificate from Windows7, AnyConnect cannot find any valid certificates:



Cisco AnyConnect

Certificate Validation Failure

Cisco AnyConnect Secure Mobility Client

VPN:

No valid certificates available for authentication.

10.48.67.153

On the ASA, it looks like the session is terminated by the client (Reset-I):

<#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
```

Related Information

- **Configure Tunnel Groups, Group Policies, and Users: Configure Double Authentication**
- **Configure an External Server for Security Appliance User Authorization**
- **Cisco Technical Support & Downloads**