Configure ASA as the SSL Gateway for AnyConnect Clients using Multiple-Certificate Based Authentication

Contents

Introduction

This document describes how to configure an Adaptive Security Appliance (ASA) as the Secure Sockets Layer (SSL) gateway for Cisco AnyConnect Secure Mobility Clients which uses Multiple-Certificate based authentication.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of ASA CLI configuration and 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 9.7(1) and later
- Windows 10 with Cisco AnyConnect Secure Mobility Client 4.4

  Note: Download the AnyConnect VPN Client package (**anyconnect-win*.pkg**) from the Cisco Software Download (registered customers only) . Copy the AnyConnect VPN client to the ASA's flash memory, which is to be downloaded to the remote user computers in order to establish the SSL VPN connection with the ASA. *Refer to* the Installing the AnyConnect Client section of the ASA configuration guide for more information.

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, make sure that you understand the potential impact of any command.

Background Information

Prior to software version 9.7(1), ASA supports single certificate based authentication, which means either user or the machine can be authenticated but not both, for a single connection attempt.

Multiple-Certificate based authentication gives the ability to have the ASA validate the machine or device certificate, to ensure the device is a corporate-issued device, in addition to authenticating the user's identity certificate to allow VPN access.

Limitations

- Multiple certificate authentication currently limits the number of certificates to exactly two.
- AnyConnect Client must indicate support for multiple certificate authentication. If that is not the case then the gateway uses one of the legacy authentication methods or fail the connection. AnyConnect version 4.4.04030 or later supports Multi-Certificate based authentication.
- For Windows Platform, machine certificate is sent during initial SSL handshake followed by User Certificate under the Aggregate auth protocol.Two certificates from Windows Machine Store is not supported.
- Multiple Certificate authentication ignores **Enable automatic Certificate Selection** preferences under the XML profile which means that client tries all the combinations to authenticate both the certificates until it fails. This may introduce considerable delay while Anyconnect tries to connect. Hence, it is recommended to use Certificate Matching in case of multiple User/Machine certificate on the client machine.
- Anyconnect SSL VPN only Supports RSA-based certificates.
- Only SHA256, SHA384, and SHA512 based certificate are supported during the aggregate auth.

Certificate Selection on Windows v/s Non-Windows

Platforms

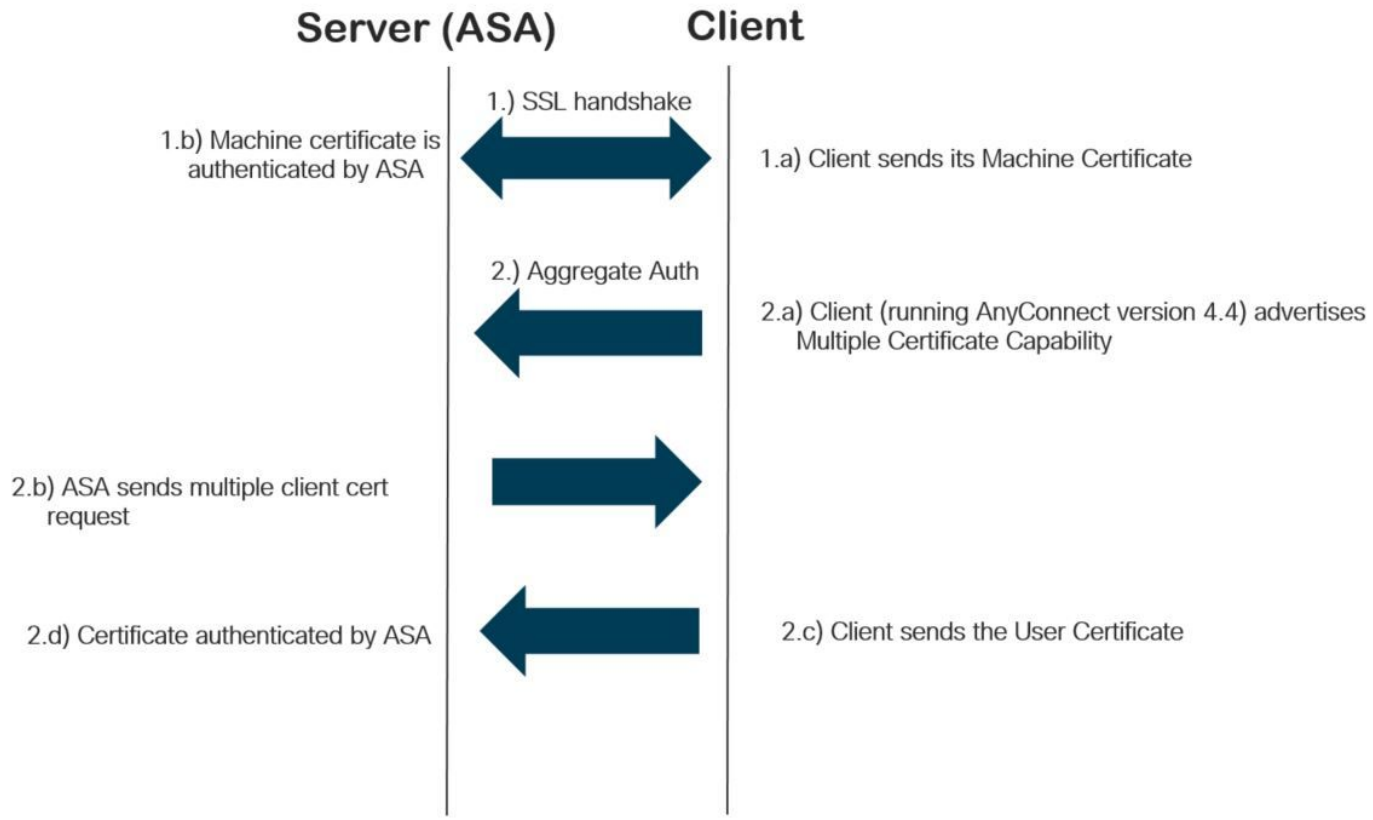
AnyConnect on Windows distinguishes between certificates retrieved from the machine store (accessible only by privileged processes) and the user store (accessible only by processes owned by the logged-in user). No such distinction is made by AnyConnect on non-Windows platforms.

The ASA may choose to enforce a connection policy, configured by the ASA administrator, based on the actual types of certificates received. For Windows, the types can be:

- One machine and one user, or
- Two user.

For non-Windows platforms, the indication is always two user certificates.

Connection Flow for Multiple Certificate Authentication



Configure

Configure Multiple Certificate Authentication via ASDM

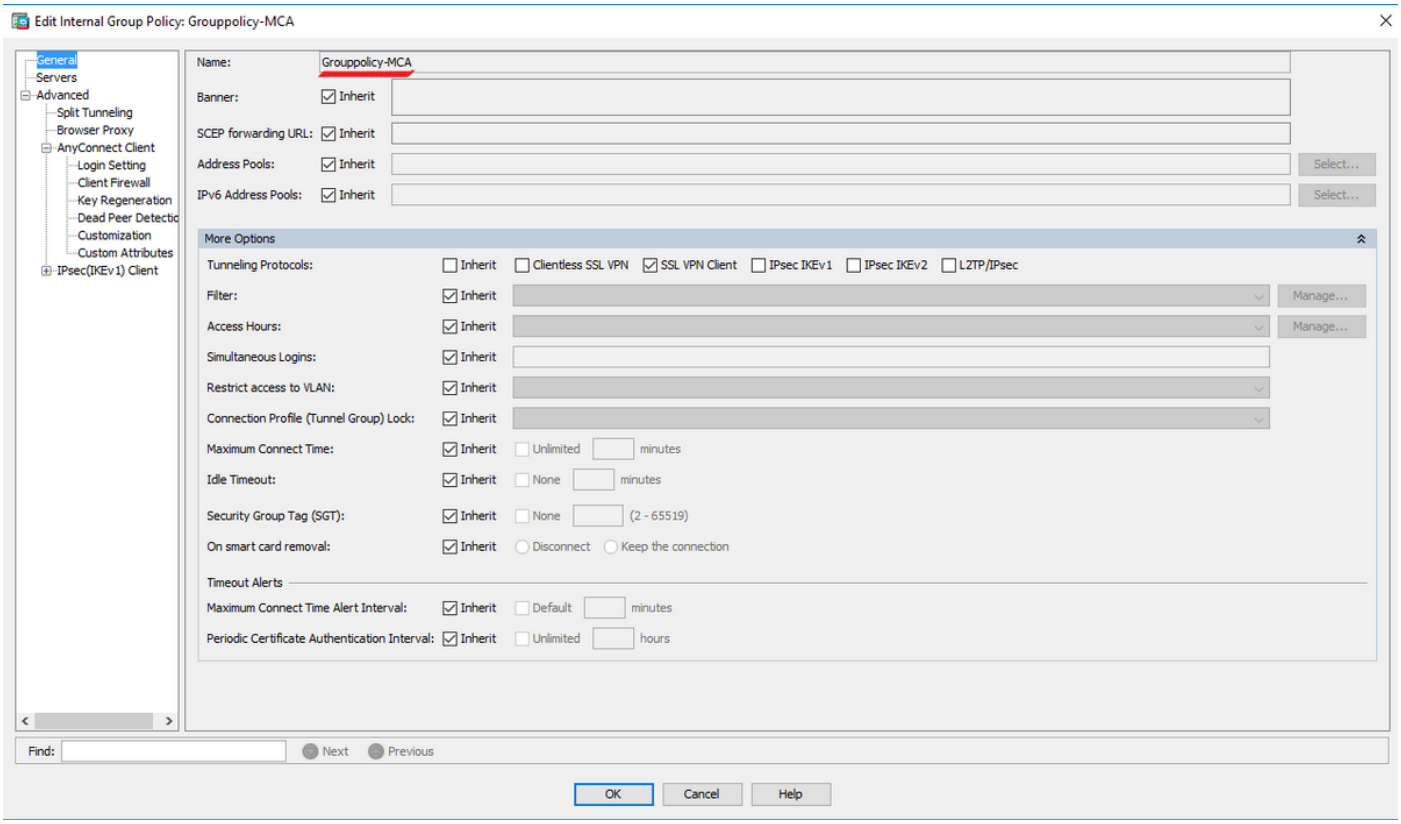
This section describes how to configure the Cisco ASA as the SSL gateway for AnyConnect Clients with multiple-certificate authentication.

Complete these steps via ASDM to set up Anyconnect clients for Multiple-Certificate Authentication:

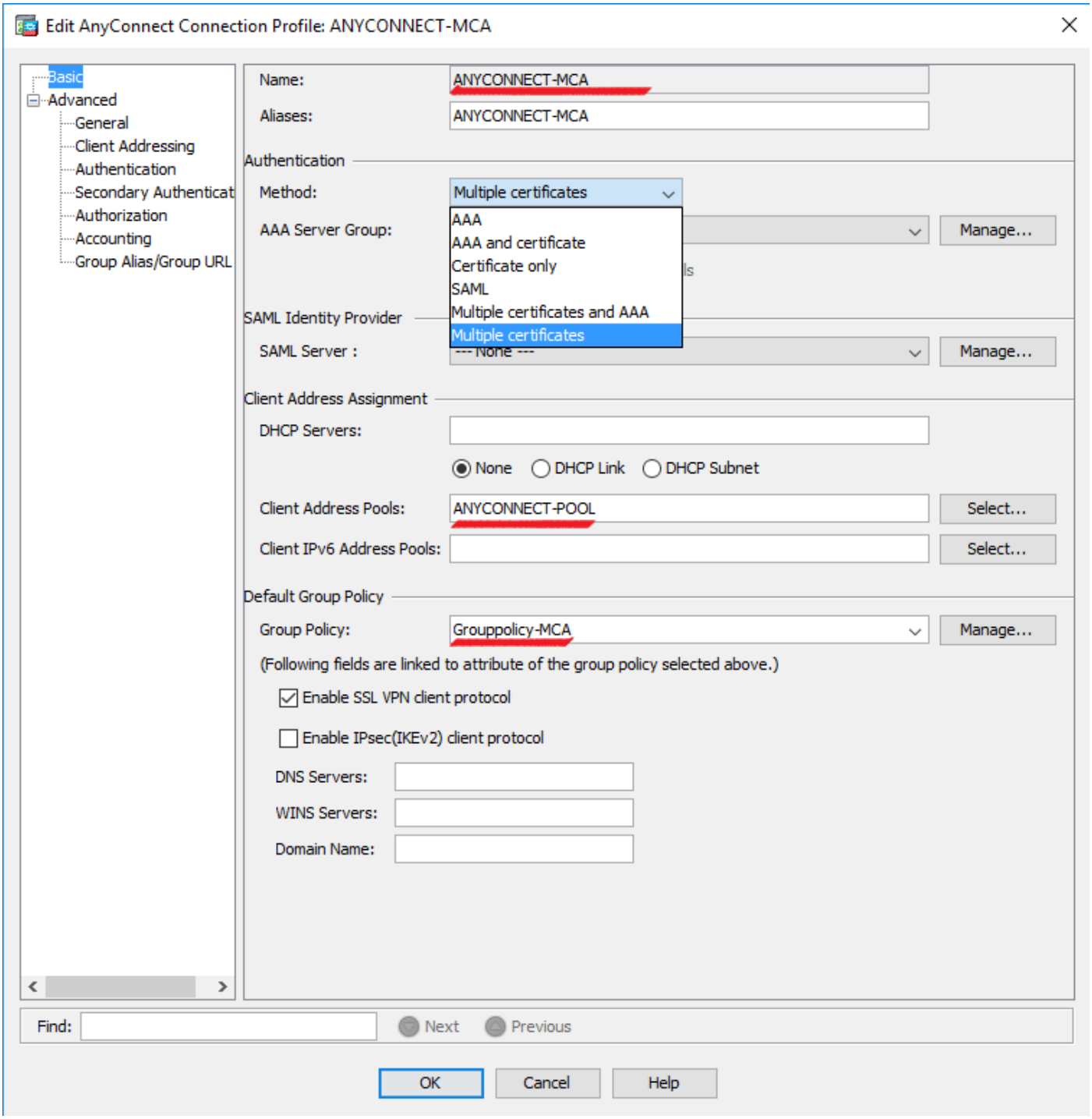
Step 1. Install CA certificate for User and Machine Certificates on the ASA.

For installation of the certificate refer to [Configure ASA: SSL Digital Certificate Installation and Renewal]

Step 2. Navigate to **Configuration > Remote Access > Group Policy** and configure the Group-Policy.



Step 3. Configure the new Connection Profile and select **Authentication Method** as Multiple Certificates and select the Group-Policy created in step 1.



Step 4. For other detailed configuration, *refer to*VPN Client and AnyConnect Client Access to Local LAN Configuration Example

Configure ASA for Multiple Certificate Authentication via CLI

> **Note**: Use the Command Lookup Tool (registered customers only) in order to obtain more information on the commands used in this section.

```
ASA Version 9.7(1)
!
hostname GCE-ASA
```

```
!
! Configure the VPN Pool
ip local pool ANYCONNECT-POOL 192.168.100.1-192.168.100.254 mask 255.255.255.0
!
interface GigabitEthernet0/0
nameif outside
security-level 100
ip address 10.197.223.81 255.255.254.0
!
interface GigabitEthernet0/1
nameif inside
security-level 100
ip address 192.168.1.1 255.255.255.0
!
! Configure Objects
object network obj-AnyConnect_pool
subnet 192.168.100.0 255.255.255.0
object network obj-Local_Lan
subnet 192.168.1.0 255.255.255.0
!
! Configure Split-tunnel access-list
access-list split standard permit 192.168.1.0 255.255.255.0
!
! Configure Nat-Exemption for VPN traffic
nat (inside,outside) source static obj-Local_Lan obj-Local_Lan destination static obj-
AnyConnect_pool obj-AnyConnect_pool no-proxy-arp route-lookup
!
! TrustPoint for User CA certificate
crypto ca trustpoint UserCA
enrollment terminal
crl configure
!
! Trustpoint for Machine CA certificate
crypto ca trustpoint MachineCA
enrollment terminal
crl configure
!
!
crypto ca certificate chain UserCA
certificate ca 00ea473dc301c2fdc7
30820385 3082026d a0030201 02020900 ea473dc3 01c2fdc7 300d0609 2a864886
<snip>
3d57bea7 3e30c8f0 f391bab4 855562fd 8e21891f 4acb6a46 281af1f2 20eb0592
012d7d99 e87f6742 d5
quit


crypto ca certificate chain MachineCA
certificate ca 00ba27b1f331aea6fc
30820399 30820281 a0030201 02020900 ba27b1f3 31aea6fc 300d0609 2a864886
f70d0101 0b050030 63310b30 09060355 04061302 494e3112 30100603 5504080c
<snip>
2c214c7a 79eb8651 6ad1eabd ae1ffbba d0750f3e 81ce5132 b5546f93 2c0d6ccf
606add30 2a73b927 7f4a73e5 2451a385 d9a96b50 6ebeba66 fc2e496b fa
quit
!
! Enable AnyConnect
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.4.00243-webdeploy-k9.pkg 2
anyconnect enable
tunnel-group-list enable
!
! Configure Group-Policy
```

```
group-policy Grouppolicy-MCA internal
group-policy Grouppolicy-MCA attributes
vpn-tunnel-protocol ssl-client
split-tunnel-policy tunnelspecified
split-tunnel-network-list value split
!
! Configure Tunnel-Group
tunnel-group ANYCONNECT-MCA type remote-access
tunnel-group ANYCONNECT-MCA general-attributes
address-pool ANYCONNECT-POOL
default-group-policy Grouppolicy-MCA
tunnel-group ANYCONNECT-MCA webvpn-attributes
authentication multiple-certificate
group-alias ANYCONNECT-MCA enable
group-url https://10.197.223.81/MCA enable
```

Verify

Use this section in order to confirm that your configuration works properly.

> **Note**: The Output Interpreter Tool (registered customers only) supports certain **show** commands. Use the Output Interpreter Tool in order to view an analysis of **show** command output.

View Installed Certificates on the ASA via CLI

show crypto ca certificate

```
GCE-ASA(config)# show crypto ca certificate

CA Certificate

Status: Available
Certificate Serial Number: 00ea473dc301c2fdc7
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Subject Name:
cn=UserCA.cisco.com
o=Cisco
l=Dallas
st=Texas
c=IN
Validity Date:
start date: 15:40:28 UTC Sep 30 2017
enddate: 15:40:28 UTC Jul202020
Storage: config
Associated Trustpoints: UserCA
```

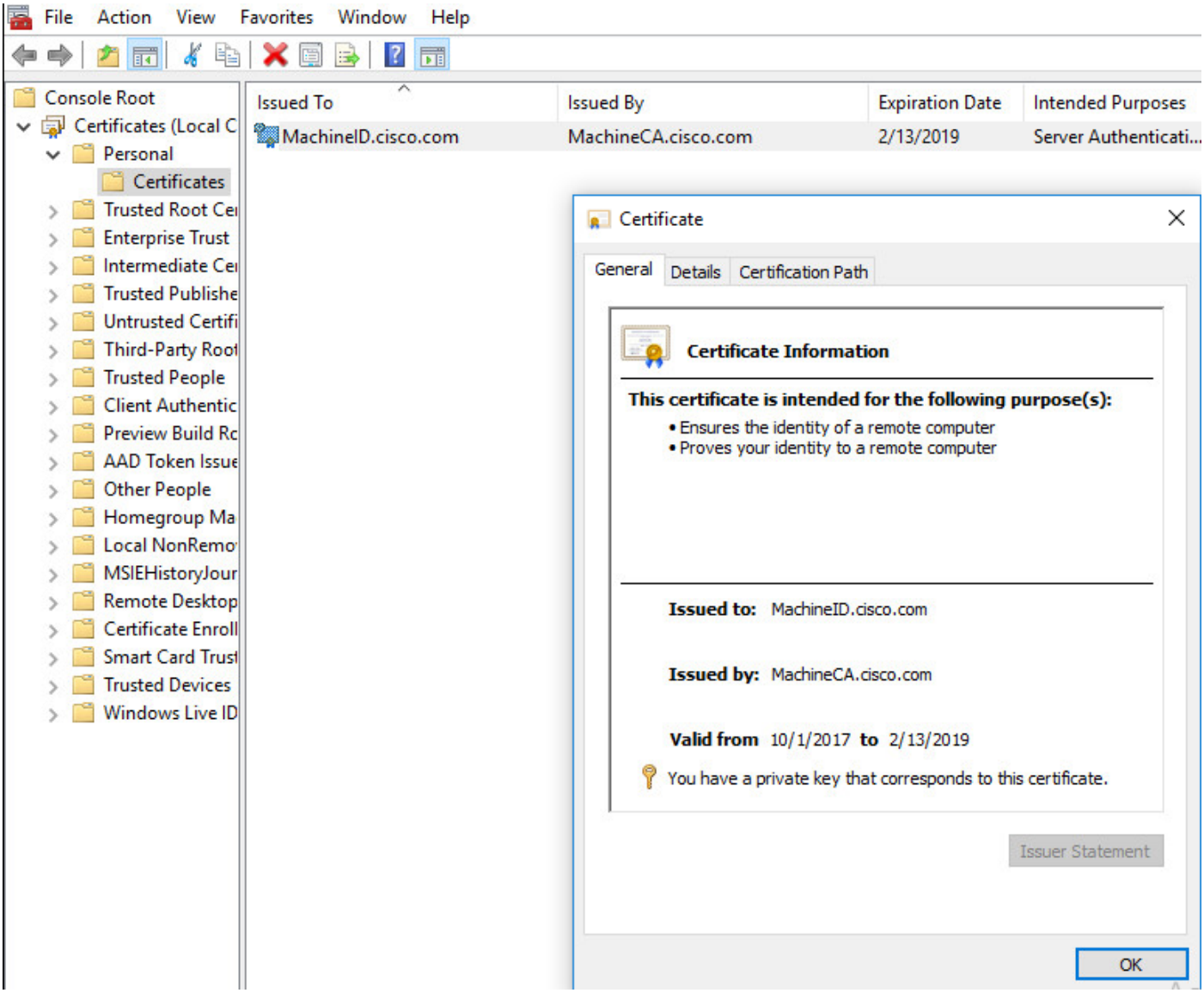
```
CA Certificate

Status: Available
Certificate Serial Number: 00ba27b1f331aea6fc
Certificate Usage: General Purpose
Public Key Type: RSA (2048 bits)
Signature Algorithm: SHA256 with RSA Encryption
Issuer Name:
cn=MachineCA.cisco.com
o=Cisco
l=Bangalore
st=Karnataka
c=IN
Subject Name:
cn=MachineCA.cisco.com
o=Cisco
l=Bangalore
st=Karnataka
c=IN
Validity Date:
start date: 15:29:23 UTC Sep 30 2017
enddate: 15:29:23 UTC Jul202020
Storage: config
Associated Trustpoints: MachineCA
```

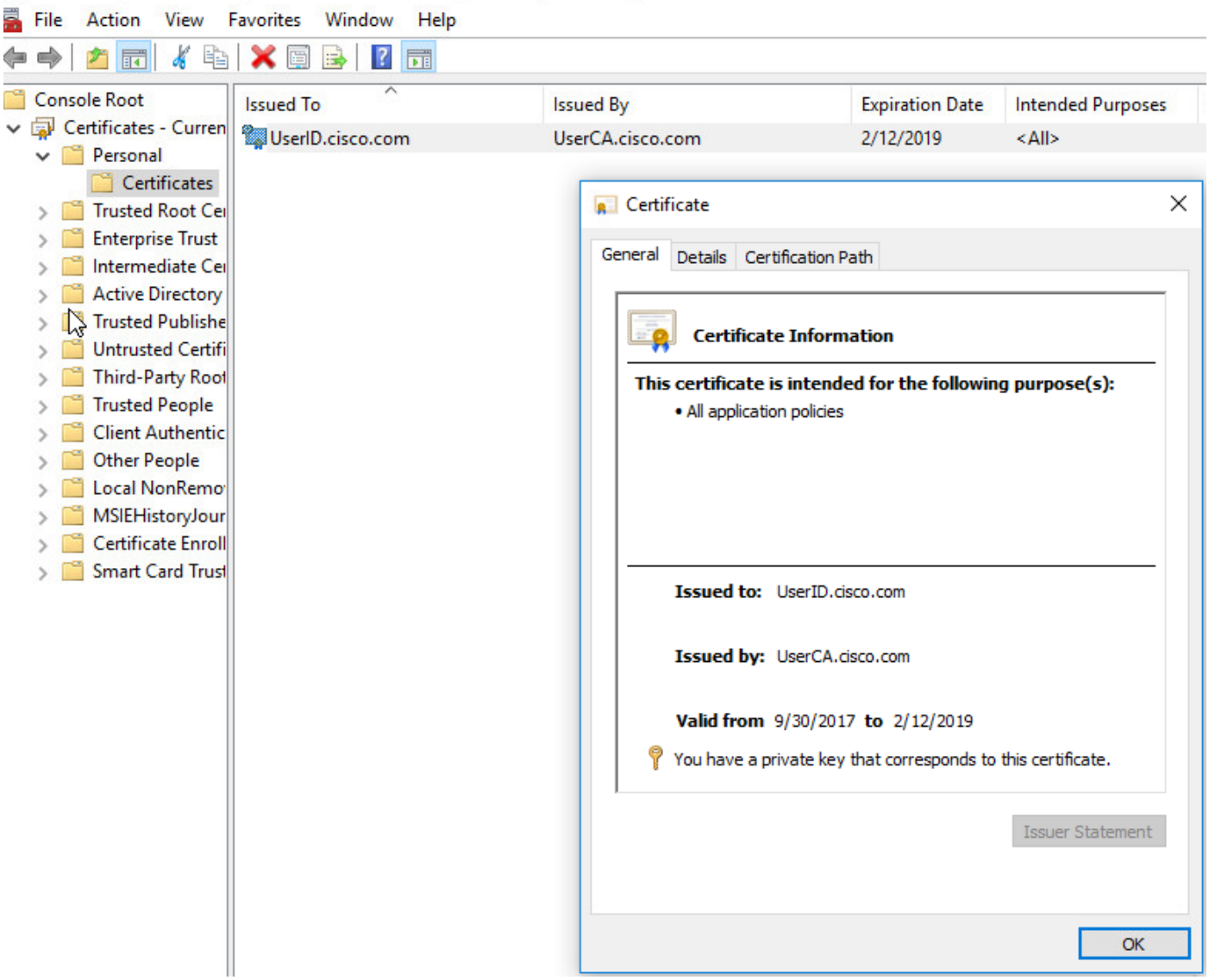
View Installed Certificates on the Client

In order to verify the installation, use the Certificate Manager (certmgr.msc):

Machine Certificate



User Certificate



Execute this command to verify the connection:

```
GCE-ASA# sh vpn-sessiondb detail anyconnect

Session Type: AnyConnect Detailed

Username : MachineID.cisco.com Index : 296
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Protocol : AnyConnect-Parent SSL-Tunnel DTLS-Tunnel
License : AnyConnect Premium
Encryption : AnyConnect-Parent: (1)none SSL-Tunnel: (1)AES128 DTLS-Tunnel: (1)AES256
Hashing : AnyConnect-Parent: (1)none SSL-Tunnel: (1)SHA1 DTLS-Tunnel: (1)SHA1
Bytes Tx : 11542 Bytes Rx : 2097
Pkts Tx : 8 Pkts Rx : 29
Pkts Tx Drop : 0 Pkts Rx Drop : 0
Group Policy : Grouppolicy-MCA Tunnel Group : ANYCONNECT-MCA
Login Time : 22:26:27 UTC Sun Oct 1 2017
Duration : 0h:00m:21s
Inactivity : 0h:00m:00s
VLAN Mapping : N/A VLAN : none
Audt Sess ID : 0ac5df510012800059d16b93
Security Grp : none
AnyConnect-Parent Tunnels: 1
SSL-Tunnel Tunnels: 1
DTLS-Tunnel Tunnels: 1
```

```
AnyConnect-Parent:
Tunnel ID : 296.1
Public IP : 10.197.223.235
Encryption : none Hashing : none
TCP Src Port : 51609 TCP Dst Port : 443
Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : win
Client OS Ver: 10.0.14393
Client Type : AnyConnect
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 5771 Bytes Rx : 0
Pkts Tx : 4 Pkts Rx : 0
Pkts Tx Drop : 0 Pkts Rx Drop : 0

SSL-Tunnel:
Tunnel ID : 296.2
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Encryption : AES128 Hashing : SHA1
Ciphersuite : AES128-SHA
Encapsulation: TLSv1.2 TCP Src Port : 51612
TCP Dst Port : 443 Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : SSL VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 5771 Bytes Rx : 446
Pkts Tx : 4 Pkts Rx : 5
Pkts Tx Drop : 0 Pkts Rx Drop : 0

DTLS-Tunnel:
Tunnel ID : 296.3
Assigned IP : 192.168.100.1 Public IP : 10.197.223.235
Encryption : AES256 Hashing : SHA1
Ciphersuite : AES256-SHA
Encapsulation: DTLSv1.0 UDP Src Port : 63385
UDP Dst Port : 443 Auth Mode : Multiple-certificate
Idle Time Out: 30 Minutes Idle TO Left : 29 Minutes
Client OS : Windows
Client Type : DTLS VPN Client
Client Ver : Cisco AnyConnect VPN Agent for Windows 4.4.01054
Bytes Tx : 0 Bytes Rx : 1651
Pkts Tx : 0 Pkts Rx : 24
Pkts Tx Drop : 0 Pkts Rx Drop : 0
```

Troubleshoot

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

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

> **Caution**: On the ASA, you can set various debug levels; by default, level 1 is used. If you change the debug level, the verbosity of the debugs might increase. Do this with caution, especially in production environments.

- **Debug crypto ca messages 127**
- **Debug crypto ca transaction 127**

```
CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00B6D609E1D68B9334
Subject: cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
Issuer:  cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer_name:
cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"
serial number=00 b6 d6 09 e1 d6 8b 93 34                          |  ........4

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.

CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00B6D609E1D68B9334
Subject: cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
Issuer:  cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00B6D609E1D68B9334, subject name:
cn=MachineID.cisco.com,ou=Cisco,l=Bangalore,st=Karnataka,c=IN, issuer_name:
cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=MachineCA.cisco.com,o=Cisco,l=Bangalore,st=Karnataka,c=IN"
serial number=00 b6 d6 09 e1 d6 8b 93 34                          |  ........4

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.

CRYPTO_PKI: Begin sorted cert chain
---------Certificate--------:
Serial:  00A5A42E24A345E11A
Subject: cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN
Issuer:  cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN

CRYPTO_PKI: End sorted cert chain
CRYPTO_PKI: Cert chain pre-processing: List size is 1, trustpool is not in use
CRYPTO_PKI: List pruning is not necessary.
CRYPTO_PKI: Sorted chain size is: 1
CRYPTO_PKI: Found ID cert. serial number: 00A5A42E24A345E11A, subject name:
cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN
CRYPTO_PKI: Verifying certificate with serial number: 00A5A42E24A345E11A, subject name:
```

```
cn=UserID.cisco.com,ou=TAC,o=Cisco,l=Dallas,st=Texas,c=IN, issuer_name:
cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN, signature alg: SHA256/RSA.

CRYPTO_PKI(Cert Lookup) issuer="cn=UserCA.cisco.com,o=Cisco,l=Dallas,st=Texas,c=IN" serial
number=00 a5 a4 2e 24 a3 45 e1 1a                         |  ....$.E..

CRYPTO_PKI: valid cert with warning.

CRYPTO_PKI: valid cert status.
```

- **Debug aggregate-auth xml 127**

```
Received XML message below from the client <?xml version="1.0" encoding="UTF-8"?> <config-auth
client="vpn" type="init" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
#snip#  win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<group-select>ANYCONNECT-MCA</group-select>
<group-access>https://10.197.223.81/MCA</group-access>
<capabilities>
<auth-method>single-sign-on</auth-method>
<auth-method>multiple-cert</auth-method></capabilities>
</config-auth>

Generated XML message below
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-request" aggregate-auth-version="2">
<opaque is-for="sg">
<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>136775778</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash>
</opaque>
<multiple-client-cert-request>
<hash-algorithm>sha256</hash-algorithm>
<hash-algorithm>sha384</hash-algorithm>
<hash-algorithm>sha512</hash-algorithm>
</multiple-client-cert-request>
<random>FA4003BD87436B227####snip####C138A08FF724F0100015B863F750914839EE79C86DFE8F0B9A0199E2</r
andom>
</config-auth>

Received XML message below from the client
<?xml version="1.0" encoding="UTF-8"?>
<config-auth client="vpn" type="auth-reply" aggregate-auth-version="2">
<version who="vpn">4.4.01054</version>
<device-id device-type="VMware, Inc. VMware Virtual Platform" platform-version="10.0.14393
##snip## win</device-id>
<mac-address-list>
<mac-address>00-0c-29-e4-f5-bd</mac-address></mac-address-list>
<session-token></session-token>
<session-id></session-id>
<opaque is-for="sg">

<tunnel-group>ANYCONNECT-MCA</tunnel-group>
<aggauth-handle>608423386</aggauth-handle>
<auth-method>multiple-cert</auth-method>
<auth-method>single-sign-on</auth-method>
<config-hash>1506879881148</config-hash></opaque>
```

```
<auth>
<client-cert-chain cert-store="1M">
<client-cert-sent-via-protocol></client-cert-sent-via-protocol></client-cert-chain>
<client-cert-chain cert-store="1U">
<client-cert cert-format="pkcs7">MIIG+AYJKoZIhvcNAQcCoIIG6TCCBuU
yTCCAzwwggIkAgkApaQuJKNF4RowDQYJKoZIhvcNAQELBQAwWTELMAkGA1UEBhMC
#Snip#
gSCx8Luo9V76nPjDI8PORurSFVWL9jiGJH0rLakYoGv
</client-cert>
<client-cert-auth-signature hash-algorithm-
chosen="sha512">FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJ
#snip#
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQnjMwi6D0ygT=</client-cert-auth-
signature>
</client-cert-chain>
</auth>
</config-auth>
Received attribute hash-algorithm-chosen in XML message from client
Base64 Signature (len=349):
FIYur1Dzb4VPThVZtYwxSsCVRBUin/8MwWK+G5u2Phr4fJI9aWFqd1BbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
ABXv++cN7lNWGHK91EAvNRcpCX4TdZ+6ZKpL4sClu8vZJeW2jwGmPnYesG3sttrS
TFBRqg74+1TFSbUuIEzn8MLXZqHbOnA19B9gyXZJon8eh3Z7cDspFiR0xKBu8iYH
L+ES84UNtDQjatIN4EiS8SD/5QPAunCyvAUBvK5FZ4c4TpnF6MIEPhjMwi6D0ygT
sm2218mstLDNKBouaTjB3A==
Successful Base64 signature decode, len 256
Loading cert into PKI
Waiting for certificate validation result
Verifying signature
Successfully verified signature
```

- **Debug aggregate-auth ssl 127**

```
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-no-cert: Client has not sent a certificate
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-no-cert: Resolve tunnel group (ANYCONNECT-MCA) alias (NULL) Cert or URL mapped YES
INIT-no-cert: Client advertised multi-cert authentication support
[332565382] Created auth info for client 10.197.223.235
[332565382] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-no-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
[332565382] Generating multiple certificate request
[332565382] Saved message of len 699 to verify signature
rcode from handler = 0
Sending response
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (init)
INIT-cert: Client has certificate, groupSelect ANYCONNECT-MCA
Found TG ANYCONNECT-MCA by URL https://10.197.223.81/MCA
INIT-cert: Found tunnel group (ANYCONNECT-MCA) alias (NULL) url or certmap YES
INIT-cert: Client advertised multi-cert authentication support
[462466710] Created auth info for client 10.197.223.235
[462466710] Started timer (3 mins) for auth info for client 10.197.223.235
INIT-cert: Tunnel group ANYCONNECT-MCA requires multi-cert authentication
Resetting FCADB entry
[462466710] Generating multiple certificate request
[462466710] Saved message of len 741 to verify signature
rcode from handler = 0
```

```
Sending response
/CSCOSSLC/config-auth
Processing client request
XML successfully parsed
Processing request (auth-reply)
auth-reply:[462466710] searching for authinfo
[462466710] Found auth info for client 10.197.223.235, update expire timer (3 mins)
Found tunnel group (ANYCONNECT-MCA) alias ANYCONNECT-MCA
[462466710] Multi cert authentication
[462466710] First cert came in SSL protocol, len 891
[462466710] Success loading cert into PKI
[462466710] Authenticating second cert
[462466710] Sending Message AGGAUTH_MSG_ATHENTICATE_CERT(1)
[462466710] Fiber waiting
Aggauth Message handler received message AGGAUTH_MSG_ATHENTICATE_CERT
[462466710] Process certificate authentication request
[462466710] Waiting for async certificate verification
[462466710] Verify cert callback
[462466710] Certificate Authentication success - verifying signature
[462466710] Signature verify success
[462466710] Signalling fiber
[462466710] Fiber continuing
[462466710] Found auth info
[462466710] Resolved tunnel group (ANYCONNECT-MCA), Cert or URL mapped YES
Resetting FCADB entry
Attempting cert only login
Authorization username = MachineID.cisco.com
Opened AAA handle 335892526
Making AAA request
AAA request finished
Send auth complete
rcode from handler = 0
Sending response
Closing AAA handle 335892526
[462466710] Destroy auth info for 10.197.223.235
[462466710] Free auth info for 10.197.223.235
```

Related Information

- Release Notes for the Cisco ASA Series, 9.7(x)
- Cisco AnyConnect Secure Mobility Client Administrator Guide, Release 4.4
- AnyConnect VPN Client Troubleshooting Guide - Common Problems
- Technical Support and Documentation