

ASA als SSL-gateway voor AnyConnect-clients configureren met meervoudige certificaatverificatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Beperkingen](#)

[Selectie van certificaten op Windows v/s niet-Windows-platforms](#)

[Connection Flow voor meervoudige certificaatverificatie](#)

[Configureren](#)

[Meervoudige certificaatverificatie via ASDM configureren](#)

[ASA instellen voor meerdere certificaatverificatie via CLI](#)

[Verifiëren](#)

[Geïnstalleerde certificaten op de ASA via CLI bekijken](#)

[Geïnstalleerde certificaten op de client bekijken](#)

[Machinecertificaat](#)

[Gebruikerscertificaat](#)

[Problemen oplossen](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u een adaptieve security applicatie (ASA) kunt configureren als de Secure Socket Layer (SSL) poort voor Cisco AnyConnect Secure Mobility Clients die op meerdere certificaten gebaseerde verificatie gebruikt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Basiskennis van de ASA CLI-configuratie en SSL VPN-configuratie
- Basiskennis van X509-certificaten

Gebruikte componenten

De informatie in dit document is gebaseerd op deze softwareversies:

- Software voor Cisco adaptieve security applicatie (ASA), versie 9.7(1) en hoger
- Windows 10 met Cisco AnyConnect Secure Mobility Client 4.4

Opmerking: Download het AnyConnect VPN-clientpakket (**AnyConnect-win*.pkg**) van de Cisco [Software Download](#) ([alleen geregistreerde](#) klanten). Kopieer de AnyConnect VPN-client naar het FastHub van de ASA, dat naar de externe gebruikerscomputers moet worden gedownload om de SSL VPN-verbinding met de ASA op te zetten. *Raadpleeg* het [gedeelte AnyConnect-client](#) van de ASA-configuratiehandleiding voor meer informatie.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Achtergrondinformatie

Voorafgaand aan softwareversie 9.7(1) ondersteunt ASA één op certificaat gebaseerde authenticatie, wat betekent dat gebruikers of de machine voor één enkele verbinding geauthentiseerd kunnen worden maar niet allebei.

Meervoudige op certificaat gebaseerde verificatie geeft de mogelijkheid om de ASA het machine- of apparaatcertificaat te laten valideren, om er zeker van te zijn dat het apparaat een door het bedrijf afgegeven apparaat is, naast het echtheidscertificaat van de gebruiker om VPN-toegang toe te staan.

Beperkingen

- Meervoudige certificatie van certificaten beperkt momenteel het aantal certificaten tot precies twee.
- AnyConnect-client dient ondersteuning te bieden voor meerdere certificatie. Als dat niet het geval is, gebruikt de poort een van de bestaande authenticatiemethoden of faalt hij de verbinding. AnyConnect versie 4.4.040/30 of hoger ondersteunt op meerdere certificaten gebaseerde verificatie.
- Voor Windows Platform wordt het machinecertificaat verzonden tijdens de eerste SSL-handdruk gevolgd door een gebruikerscertificaat onder het Aggregate Auth Protocol. Twee certificaten van Windows Machine Store worden niet ondersteund.
- Meervoudige certificaatauthenticatie negeert de voorkeuren **voor automatische certificaatselectie** onder het XML-profiel **in te schakelen**, wat betekent dat de client alle combinaties probeert om beide certificaten voor eensluidend te verklaren totdat deze onjuist zijn. Dit kan een aanzienlijke vertraging tot gevolg hebben terwijl AnyConnect probeert verbinding te maken. Daarom wordt aangeraden om voor meerdere gebruikers/machines-certificaten op de clientmachine te gebruiken.
- AnyConnect SSL VPN ondersteunt alleen op RSA gebaseerde certificaten.

- Slechts het op SHA256, SHA384 en SHA512 gebaseerde certificaat wordt tijdens de totale periode ondersteund.

Selectie van certificaten op Windows v/s niet-Windows-platforms

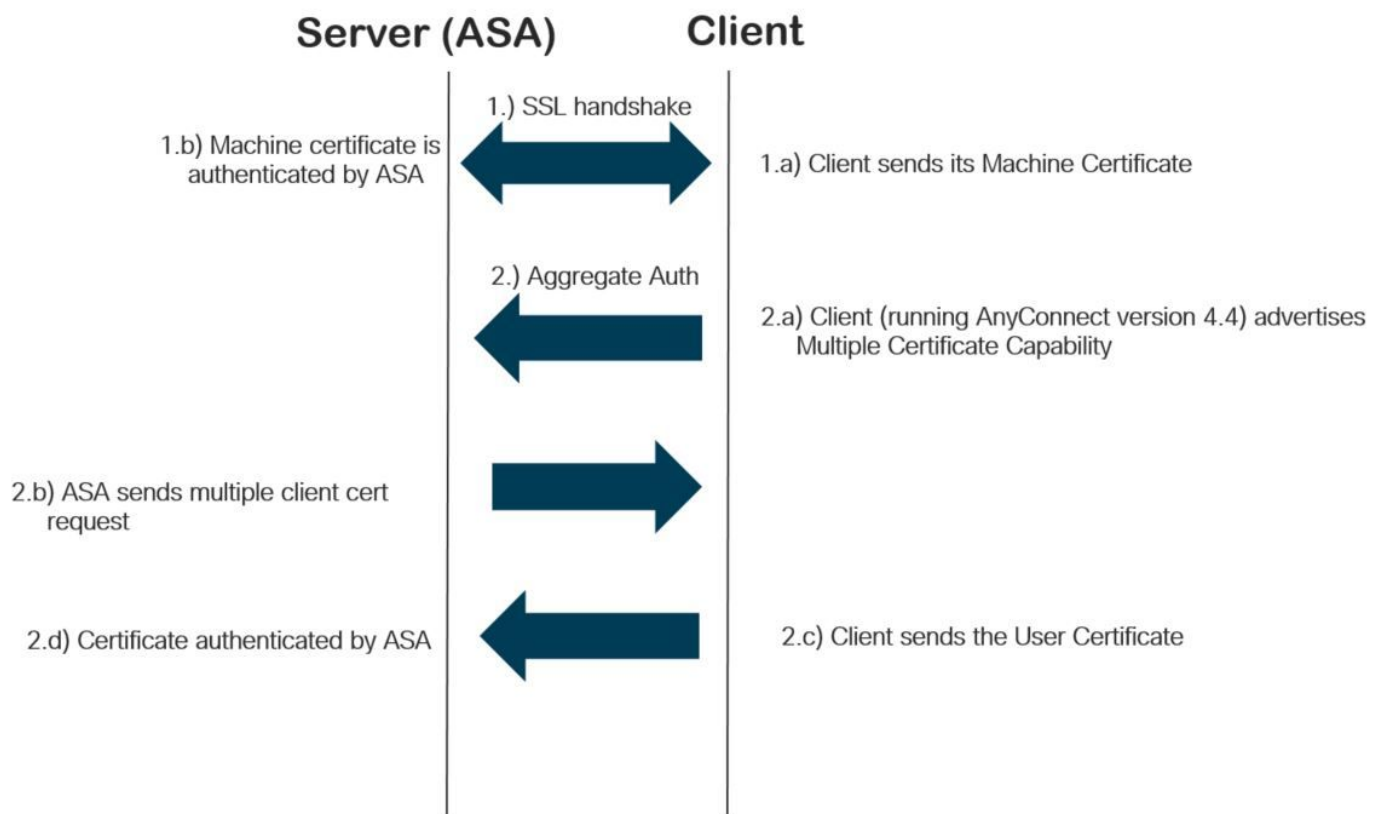
AnyConnect op Windows maakt een onderscheid tussen certificaten die worden opgehaald uit de machinewinkel (alleen toegankelijk via geprivilegieerde processen) en de gebruikerswinkel (alleen toegankelijk via processen die eigendom zijn van de ingelogde gebruiker). Een dergelijk onderscheid wordt niet gemaakt door AnyConnect op niet-Windows platforms.

ASA kan ervoor kiezen een door de ASA-beheerder ingesteld verbindingsbeleid af te dwingen op basis van de werkelijk ontvangen typen certificaten. Voor Windows kunnen de volgende typen worden gebruikt:

- één machine en één gebruiker, of
- Twee gebruikers.

Voor niet-Windows-platforms zijn er altijd twee gebruikerscertificaten.

Connection Flow voor meervoudige certificaatverificatie



Configureren

Meervoudige certificaatverificatie via ASDM configureren

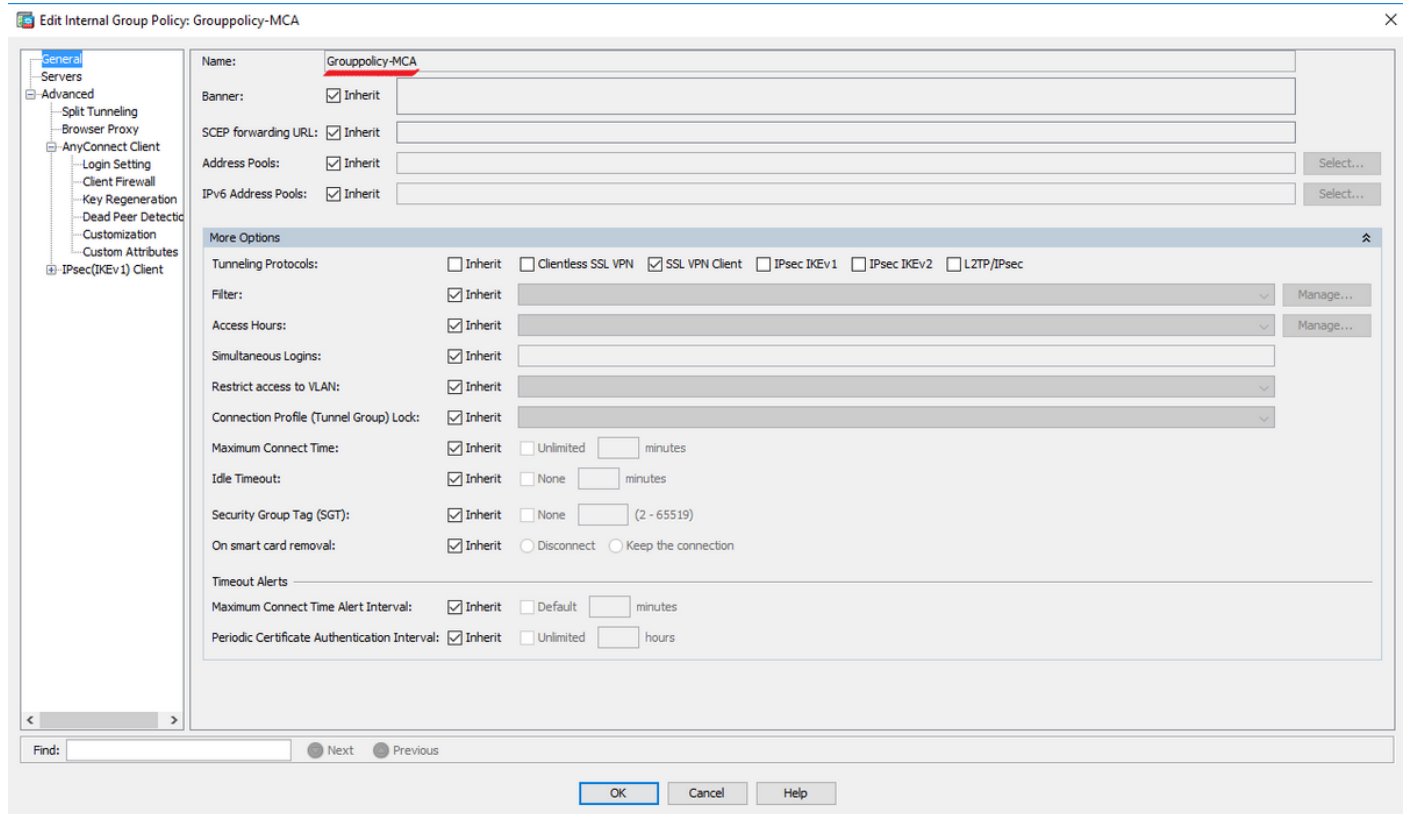
In deze sectie wordt beschreven hoe u Cisco ASA kunt configureren als de SSL-poort voor AnyConnect-clients met meervoudige certificatie.

Voltooi deze stappen via ASDM om AnyConnect-klanten voor verificatie met meerdere certificaten in te stellen:

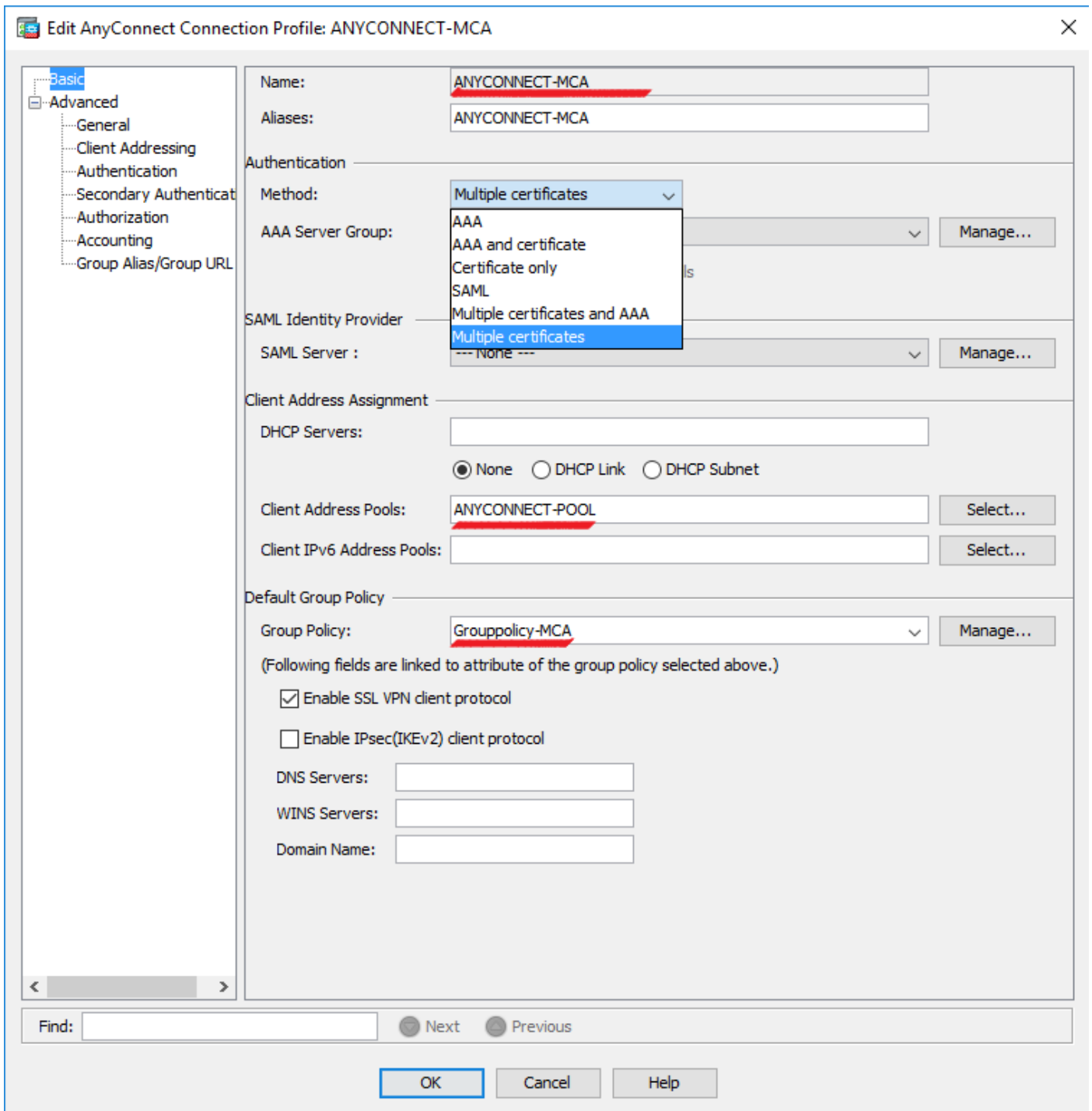
Stap 1. Installeer CA-certificaat voor gebruiker- en machinecertificaten op de ASA.

Raadpleeg voor installatie van het certificaat [ASA-configuratie: SSL digitale certificaatinstallatie en -vernieuwing](#)

Stap 2. Navigeer naar **Configuration > Remote Access > Group Policy** en stel het groepsbeleid in.



Stap 3. Configureer het nieuwe verbindingsprofiel en selecteer de **verificatiemethode** als meerdere certificaten en selecteer het groepsbeleid dat in stap 1 is gemaakt.



Stap 4. Raadpleeg voor andere gedetailleerde configuratie [de VPN-client en AnyConnect-clienttoegang tot het configuratievoorbeeld van lokaal LAN](#)

ASA instellen voor meerdere certificaatverificatie via CLI

Opmerking: Gebruik de [Command Lookup Tool \(alleen voor geregistreeerde gebruikers\)](#) voor meer informatie over de opdrachten die in deze sectie worden gebruikt.

```
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
```

Verifiëren

Gebruik dit gedeelte om te bevestigen dat de configuratie correct werkt.

Opmerking: De [Output Interpreter Tool \(alleen voor geregistreerde klanten\)](#) ondersteunt [bepaalde opdrachten met show](#). Gebruik de Output Interpreter Tool om een analyse te bekijken van de output van de opdracht **show**.

Geïnstalleerde certificaten op de ASA via CLI bekijken

certificaat van cryptografie

```
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

Geïnstalleerde certificaten op de client bekijken

Gebruik certificaatbeheer (certmgr.msc) om de installatie te controleren:

Machinecertificaat

File Action View Favorites Window Help

← → ↻ 📄 ✂ 📄 ✖ 📄 📄 ? 📄

Issued To	Issued By	Expiration Date	Intended Purposes
MachineID.cisco.com	MachineCA.cisco.com	2/13/2019	Server Authenticati...

Console Root

- Certificates (Local C)
 - Personal
 - Certificates
 - Trusted Root Certificates
 - Enterprise Trust
 - Intermediate Certificates
 - Trusted Publishers
 - Untrusted Certificates
 - Third-Party Root Certificates
 - Trusted People
 - Client Authentication
 - Preview Build Root Certificates
 - AAD Token Issuers
 - Other People
 - Homegroup Master Keys
 - Local Non-Removable Certificates
 - MSIEHistoryJournals
 - Remote Desktop
 - Certificate Enrollment
 - Smart Card Trust
 - Trusted Devices
 - Windows Live ID

Certificate

General Details Certification Path

Certificate Information

This certificate is intended for the following purpose(s):

- Ensures the identity of a remote computer
- Proves your identity to a remote computer

Issued to: MachineID.cisco.com

Issued by: MachineCA.cisco.com

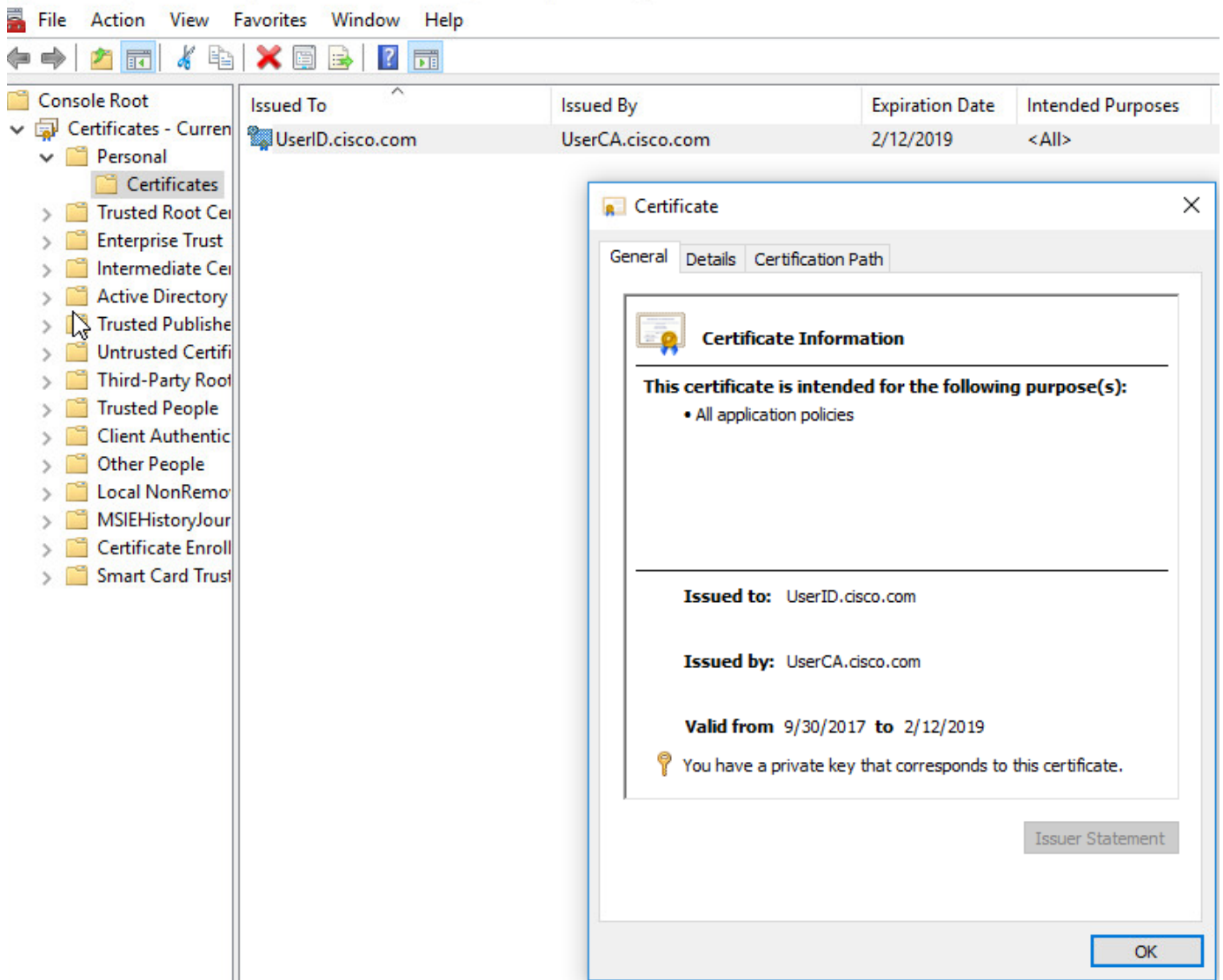
Valid from 10/1/2017 **to** 2/13/2019

🔑 You have a private key that corresponds to this certificate.

Issuer Statement

OK

Gebruikerscertificaat



Voer deze opdracht uit om de verbinding te controleren:

```
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

Problemen oplossen

Deze sectie verschaft de informatie die u kunt gebruiken om problemen met uw configuratie op te lossen.

Opmerking: Raadpleeg [Important Information on Debug Commands \(Belangrijke informatie over opdrachten met debug\)](#) voordat u opdrachten met debug opgeeft.

Voorzichtig: Op de ASA kun je verschillende debug-niveaus instellen. standaard wordt niveau 1 gebruikt. Als u het debug-niveau wijzigt, kan de breedtegraad van de insecten toenemen. Doe dit met voorzichtigheid, vooral in productieomgevingen.

- Debug crypto ca berichten 127
- Debug crypto ca transactie 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 -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
yTCCAzwggIkAgkApaQuJKNF4RowDQYJKoZIhvcNAQELBQAwWTELMakGA1UEBhMC
#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+G5u2Phr4fJI9aWFqdl1BbV9WhSTsF
EYt4G2hQ4hySySYqD4L4iV91uCT5b5Bmr5HZmSqKehg0zrDBjqxx7CLMSf2pSmQn
ABXv++cN71NWGHK91EAvNRcpCX4TdZ+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 aggregaat-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_AUTHENTICATE_CERT(1)
[462466710] Fiber waiting
Aggauth Message handler received message AGGAUTH_MSG_AUTHENTICATE_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

Gerelateerde informatie

- [Releaseopmerkingen van Cisco ASA Series 9.7\(x\)](#)
- [Cisco AnyConnect Secure Mobility Client-beheerdershandleiding, release 4.4](#)
- [AnyConnect VPN-clientprobleemoplossing - gemeenschappelijke problemen](#)
- [Technische ondersteuning en documentatie](#)