# Настройте ASA как SSL шлюз для Клиентов AnyConnect, использующих Несколько серверов сертификатов Базирующаяся Аутентификация

## Содержание



## Введение

Этот документ описывает, как настроить Устройство адаптивной защиты (ASA) как шлюз Уровня защищенных сокетов (SSL) для защищенных мобильных клиентов Cisco AnyConnect Secure Mobility, который использует основанную аутентификацию Несколька серверов сертификатов.

Внесенный Шэкти Кумаром и Дхрувом Гоелем, специалистами службы технической поддержки Cisco

## Предварительные условия

### Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Базовые знания о Настройке интерфейса командной строки ASA и конфигурации VPN

SSL
- Базовые знания о сертификатах X509

### Используемые компоненты

Сведения, содержащиеся в этом документе, касаются следующих версий программного обеспечения:

- Программное обеспечение Cisco Adaptive Security Appliance (ASA), версия 9.7 (1) и позже
- Windows 10 с защищенным мобильным клиентом Cisco AnyConnect Secure Mobility 4.4

  **Примечание:** Загрузите пакет Клиента AnyConnect VPN Client (anyconnect-win*.pkg) от Загрузки Программного обеспечения Cisco (только зарегистрированные клиенты). Скопируйте VPN-клиент AnyConnect во флэш-память ASA, из которой он должен загружаться на удаленные компьютеры пользователей для установления VPN-соединения по протоколу SSL с устройством ASA. *Для получения дополнительных сведений о настройке обратитесь к разделу Установка клиента AnyConnect руководства по настройке ASA.*

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

## Общие сведения

До версии программного обеспечения 9.7 (1) ASA поддерживает основанную аутентификацию одиночного сертификата, что означает или пользователя или машину, может аутентифицироваться, но не оба, для попытки одиночного соединения.

Несколько серверов сертификатов базировалось, аутентификация дает способность иметь ASA, проверяют сертификат компьютера или сертификат устройства, чтобы гарантировать, что устройство является корпоративно выполненным устройством, в дополнение к аутентификации сертификата идентификации пользователя для предоставления доступа VPN.

## Ограничения

- Аутентификация несколька серверов сертификатов в настоящее время ограничивает количество сертификатов точно к два.

- Клиент AnyConnect должен указать на поддержку аутентификации несколька серверов сертификатов. Если это не так тогда шлюз использует один из устаревших методов аутентификации, или откажите соединение. Версия 4.4.04030 AnyConnect или более поздний Мультисертификат поддержек базировали аутентификацию.

- Для Платформы Windows сертификат компьютера передается во время начального подтверждения связи SSL, придерживавшегося Сертификатом пользователя в

соответствии с Составным подлинным протоколом. Два сертификата от Windows Machine Store не поддерживаются.

- Аутентификация Несколька серверов сертификатов игнорирует**, Включают автоматическому Сертификату** предпочтение **Selectio** под профилем XML, что означает, что клиент пробует все комбинации для аутентификации обоих сертификаты, пока это не отказывает. В то время как Anyconnect пытается соединиться, это может представить значительную задержку. Следовательно, рекомендуется использовать Сертификат, Совпадающий в случае нескольких пользователей / Сертификат компьютера на клиентском компьютере.

- VPN SSL Anyconnect только Поддержки основанные на RSA сертификаты.

- Только SHA256, SHA384 и SHA512 базировались, сертификат поддерживаются во время составной аутентификации.

## Выбор сертификата на Windows v/s Платформы Не-Windows

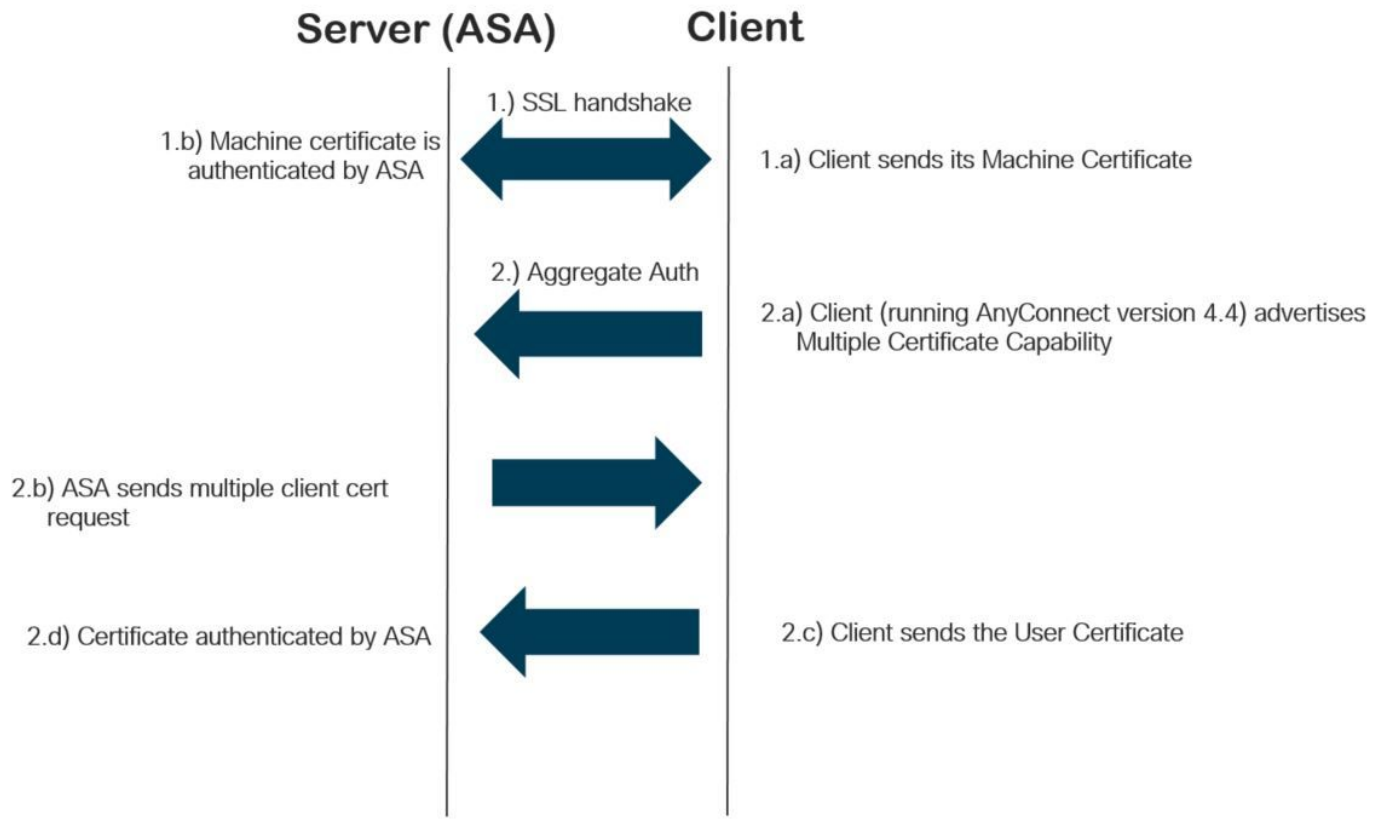
AnyConnect на Windows различает сертификаты, полученные из хранилища машины (доступный только привилегированными процессами) и пользовательского хранилища (доступный только процессами, принадлежавшими вошедшию в систему пользователь). Никакое такое различие не сделано AnyConnect на платформах не-Windows.

ASA может принять решение принудить политику установления соединений, настроенную администратором ASA, на основе фактических типов полученных сертификатов. Для Windows типы могут быть:

- Одна машина и один пользователь, или
- Два пользователя.

Для платформ не-Windows индикация всегда является двумя сертификатами пользователя.

## Поток соединения для аутентификации несколька серверов сертификатов




# Настройка

## Настройте Аутентификацию Несколька серверов сертификатов через ASDM

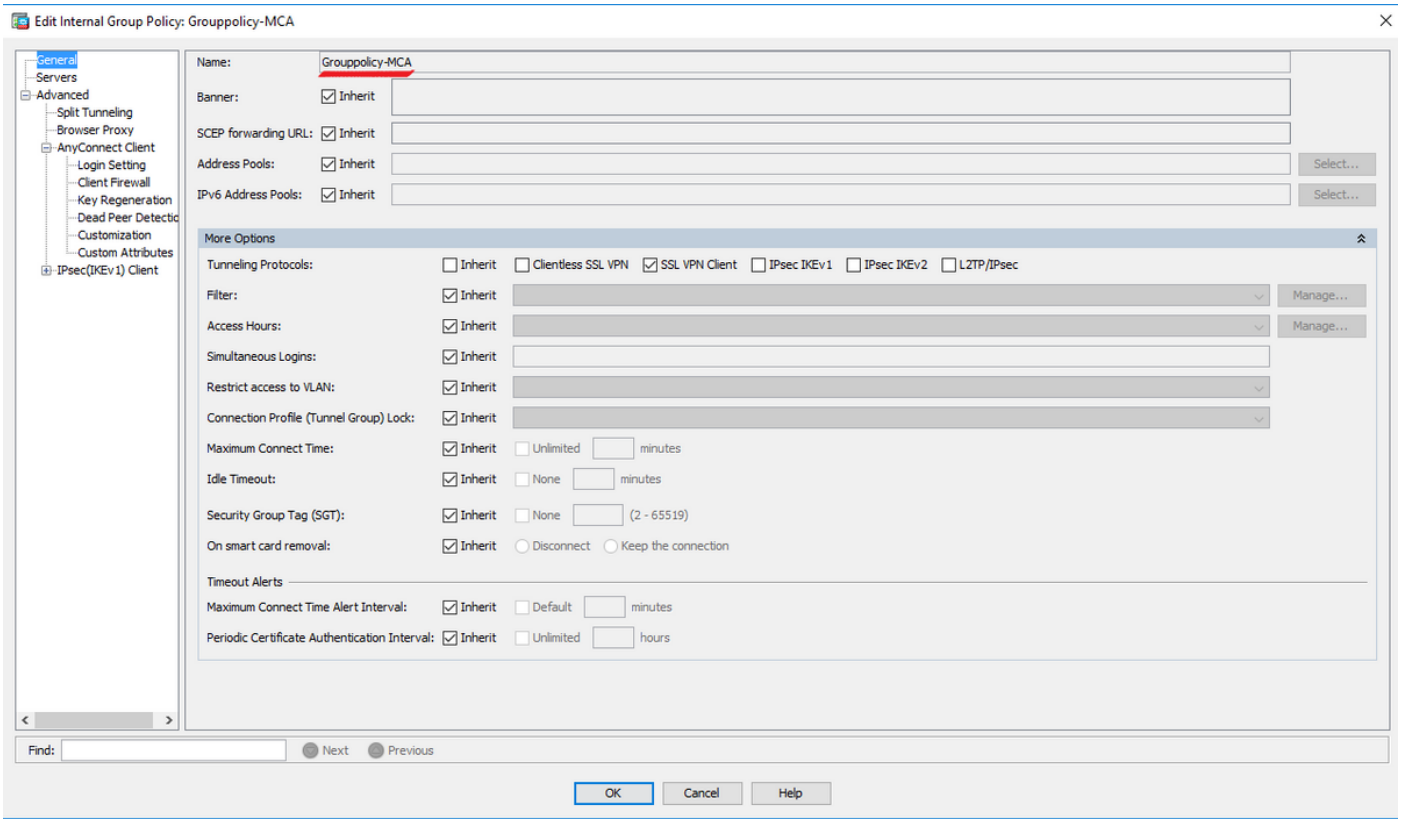
В этом разделе описывается настроить Cisco ASA как шлюз SSL для Клиентов AnyConnect с аутентификацией несколька серверов сертификатов.

Выполните эти шаги через ASDM для устанавливания клиентов Anyconnect для Аутентификации Несколька серверов сертификатов:

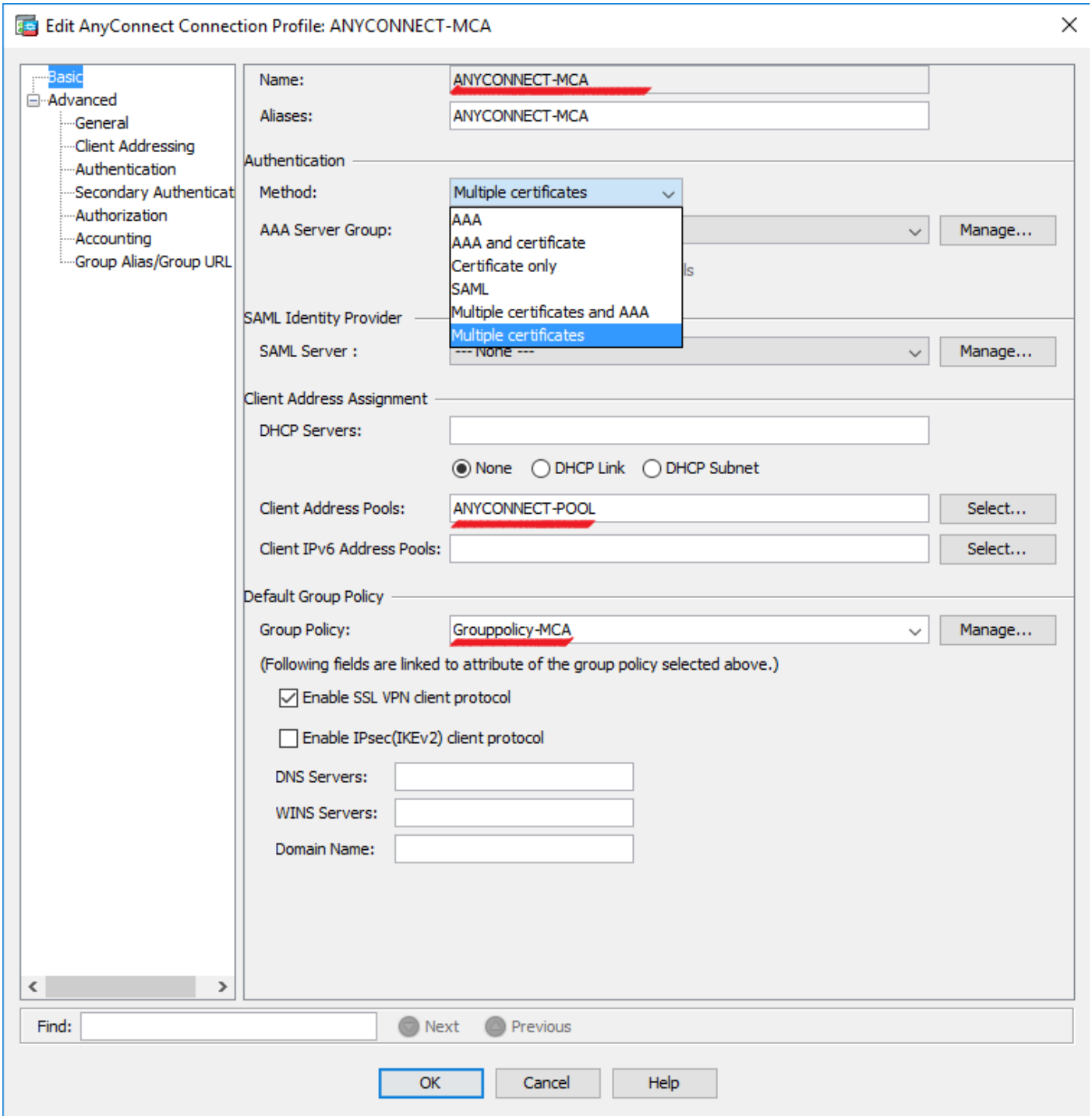
Шаг 1. Установите сертификат CA для Пользователя и Сертификатов компьютера на ASA.

Поскольку установка сертификата относится для Настройки ASA: Установка Цифрового сертификата SSL и Обновление

Шаг 2. Перейдите к **Конфигурации> Удаленный доступ> Групповая политика** и настройте Групповую политику.




Шаг 3. Настройте Профиль нового соединения и выберите **Authentication Method** как Несколька серверов сертификатов и выберите Group-Policy, созданный в шаге 1.




Шаг 4. . Для другой подробной конфигурации *обратитесь toVPN* Клиента и Доступ клиента AnyConnect к Примеру конфигурации Локальной сети

## Настройте ASA для Аутентификации Несколька серверов сертификатов через CLI

**Примечание:** Чтобы получить подробные сведения о командах в данном документе, используйте Средство поиска команд (только для зарегистрированных клиентов).

```
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
```

# Проверка

Воспользуйтесь данным разделом для проверки правильности функционирования вашей конфигурации.

> **Примечание:** Средство интерпретации выходных данных (только зарегистрированные клиенты) поддерживает **некоторые команды show**. **Используйте Средство интерпретации выходных данных, чтобы просмотреть анализ выходных данных команды show.**

## Обзорные Установленные Сертификаты на ASA через CLI

### show crypto ca certificate

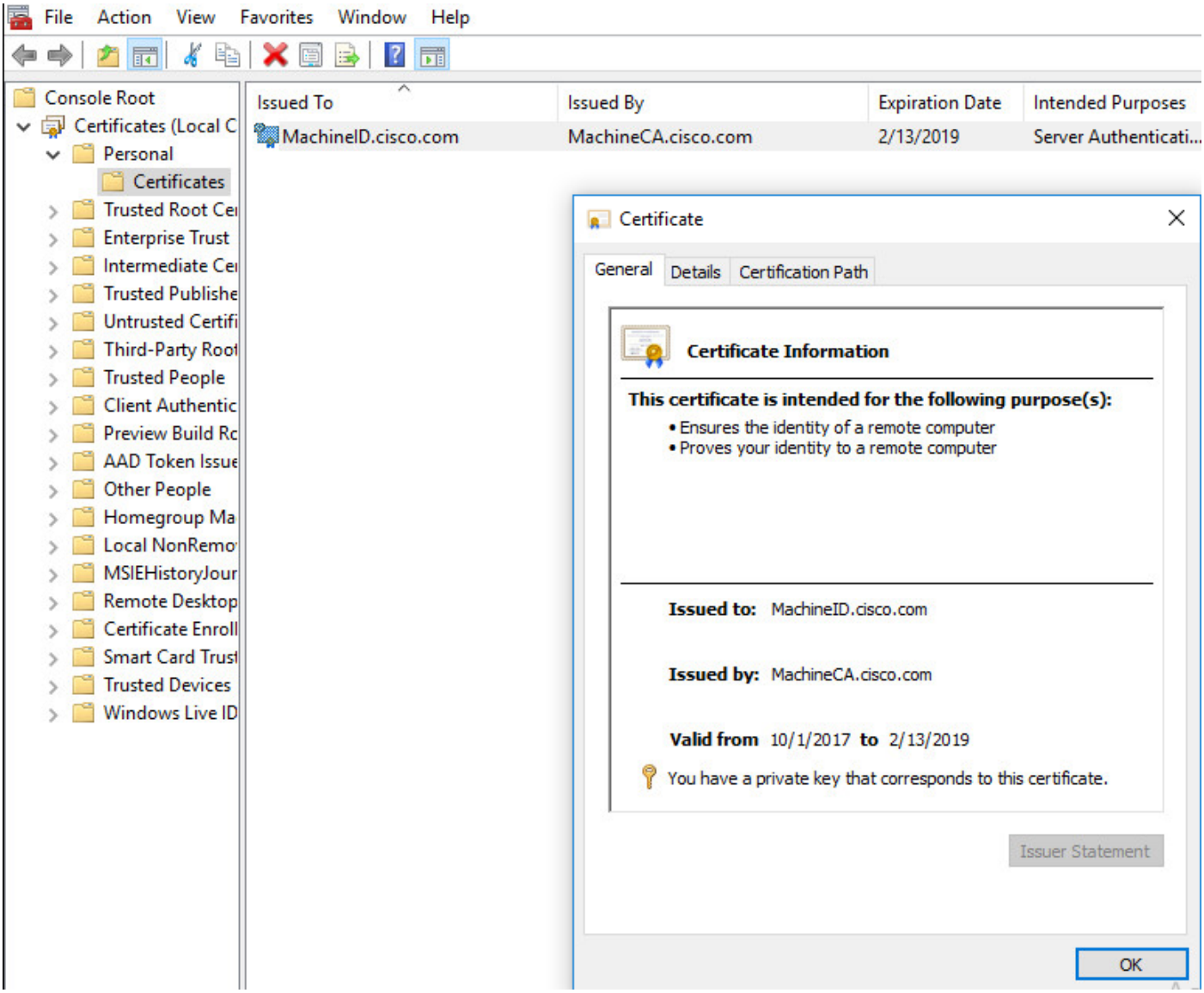
```
GCE-ASA(config)# show crypto ca certificate

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
```

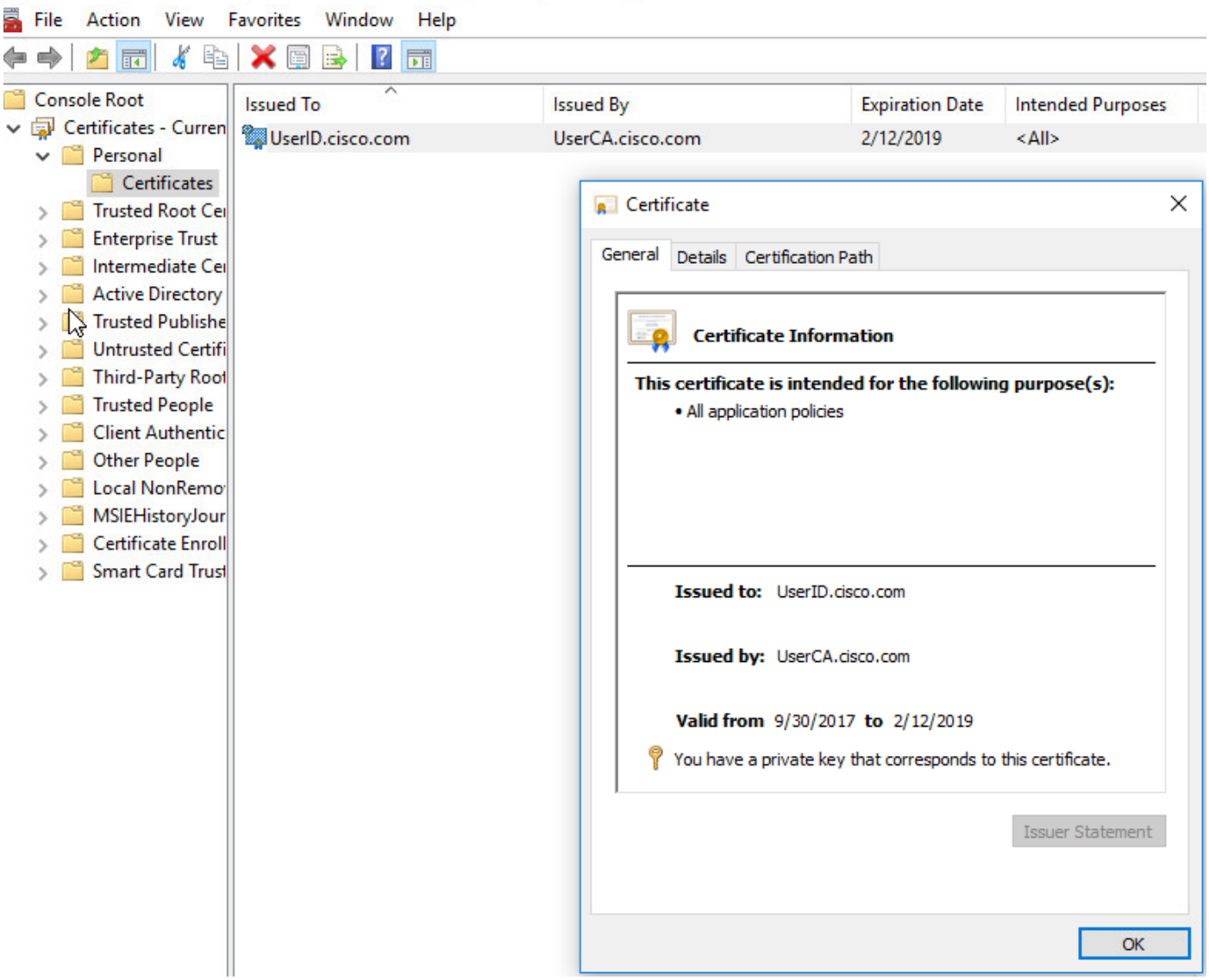
## Обзорные установленные сертификаты на клиенте

Для проверки установки используйте Менеджера сертификатов (certmgr.msc):

### Сертификат компьютера




Сертификат пользователя




Выполните эту команду для проверки соединения:

```
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 : 0ac5df5100128000059d16b93
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
```

# Устранение неполадок

Этот раздел предоставляет информацию, которую можно использовать для устранения проблем конфигурации.

> **Примечание:** Прежде чем выполнять какие-либо команды отладки , ознакомьтесь с документом "Важные сведения о командах отладки".

> **Внимание. :** На ASA можно установить различные уровни отладки; по умолчанию уровень 1 используется. При изменении уровня отладки многословие отладок могло бы увеличиться. Сделайте это с осторожностью, особенно в производственных

средах.

- Debug crypto ca обменивается сообщениями 127
- Транзакция debug crypto ca 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.
```

- Отладьте составной подлинный 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
```

- Отладьте составной подлинный 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
```

# Дополнительные сведения

- Комментарии к выпуску для серии Cisco ASA, 9.7 (x)
- Руководство администратора защищенного мобильного клиента Cisco AnyConnect Secure Mobility, выпуск 4.4
- Руководство по поиску и устранению проблем клиента AnyConnect VPN Client - типичные проблемы
- Техническая поддержка и документация