多重 認証ベースの認証を使用している AnyConnect クライアントのための SSL ゲートウェイで ASA を設定して下さい

目次

概要

この資料に多重 認証ベースの認証を使用する Cisco AnyConnect セキュア モビリティ クライアントのための Secure Sockets Layer （ SSL ）ゲートウェイで（ ASA ）適応型セキュリティ アプライアンス（ ASA ）ソフトウェア設定する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- ASA CLI 設定および SSL VPN 設定の基本的な知識
- X509 証明書に関する基本的な知識

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアのバージョンに基づくものです。

- Cisco 適応型セキュリティ アプライアンス (ASA) ソフトウェア、バージョン 9.7(1) およびそれ 以降
- Cisco AnyConnect セキュア モビリティ クライアント 4.4 が付いている Windows 10

  注: シスコの「ソフトウェア ダウンロード」ページ (登録ユーザ専用) から、AnyConnect VPN Client パッケージ (anyconnect-win*.pkg) をダウンロードします。 AnyConnect VPN Client を ASA のフラッシュ メモリにコピーします。これは、ASA との SSL VPN 接続を確立するためにリモート ユーザ コンピュータにダウンロードされます。 詳細については、ASA のコンフィギュレーション ガイドの「AnyConnect Client のインストール」セクションを参照してください。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

ソフトウェア バージョン 9.7(1) 前に、ASA サポート単一証明書はユーザかマシンは意味する単一の接続試みのための両方を、認証することができることを基づかせていませんでした認証。

多重 認証によって基づく認証は ASA をマシンを検証してもらう機能を与えますまたはデバイス証明書は VPN アクセスを許可するためにユーザの ID証明の認証に加えて、デバイスを確認するために団体発行されたデバイス、です。

制限事項

- 多重 認証認証は丁度 2 に現在証明書の数を制限します。
- AnyConnect クライアントは多重 認証認証のサポートを示す必要があります。 それからゲートウェイがレガシー 認証方式の 1 つをまたは使用するか、それが事実でなかったら接続を失敗して下さい。 AnyConnect バージョン 4.4.04030 または それ 以降は複数の証明書によって基づく認証をサポートします。
- Windows プラットフォームに関しては、マシン認証は集約 auth プロトコルの下のユーザ許可証に先行している最初の SSL ハンドシェイクの間に送信 されます。Windows マシン記憶装置からの 2 つの証明書はサポートされません。
- 多重 認証認証無視は意味する XML プロファイルの下で失敗するまで両方の証明書を認証するためにクライアントはすべての組合せを試すことを**自動証明書選択**プリファレンスを**イネーブルにします**。 これは Anyconnect が接続することを試みる間、かなり遅延をもたらすかもしれません。 それ故に、クライアントマシンの複数のユーザ/マシン認証の場合には一致する証明書を使用することを推奨します。
- Anyconnect SSL VPN は RSA ベースの証明書だけをサポートします。
- SHA256、SHA384 および SHA512 によって基づく証明書だけ集約 auth の間にサポートされます。

Windows v/s 非 Windows プラットフォームの証明書選択

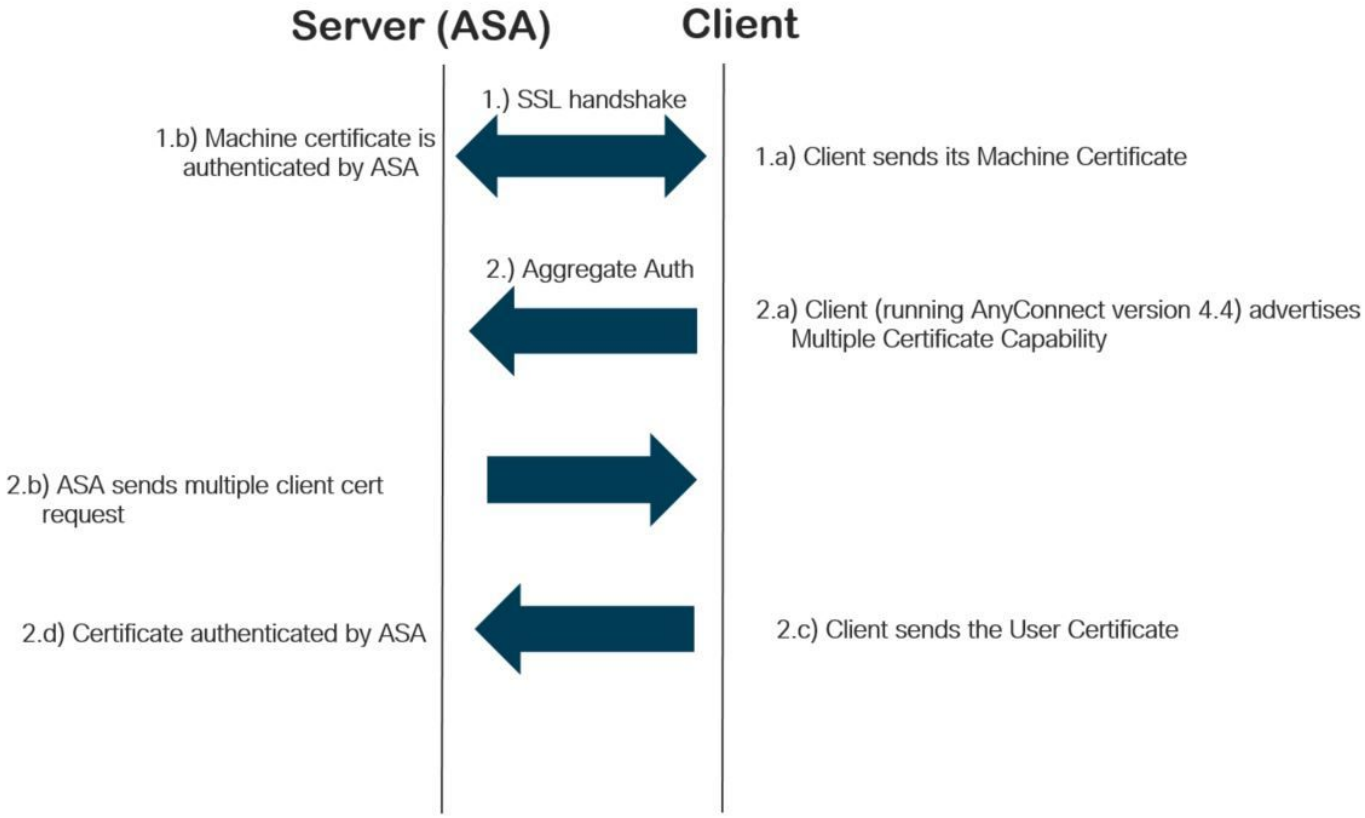
Windows の AnyConnect はマシン記憶装置（特権的プロセスによってだけアクセス可能な）およびユーザ記憶装置から区別します（ログインユーザが所有するプロセスによってだけアクセス可能な）取得される証明書の間で。 そのような違いは非 Windows プラットフォームで AnyConnect によってつけられません。

ASA は受け取った実際のタイプの証明書に基づいて ASA 管理者が、設定する接続ポリシーを実施することを選択するかもしれません。 Windows の場合、型は次のとおりである場合もあります:

- 1 台のマシンおよび 1 ユーザ、または
- 2 ユーザ。

非 Windows プラットフォームに関しては、表示は 2 つのユーザ許可証常にです。

多重 認証認証のための接続フロー



設定

ASDM によって多重 認証認証を設定して下さい

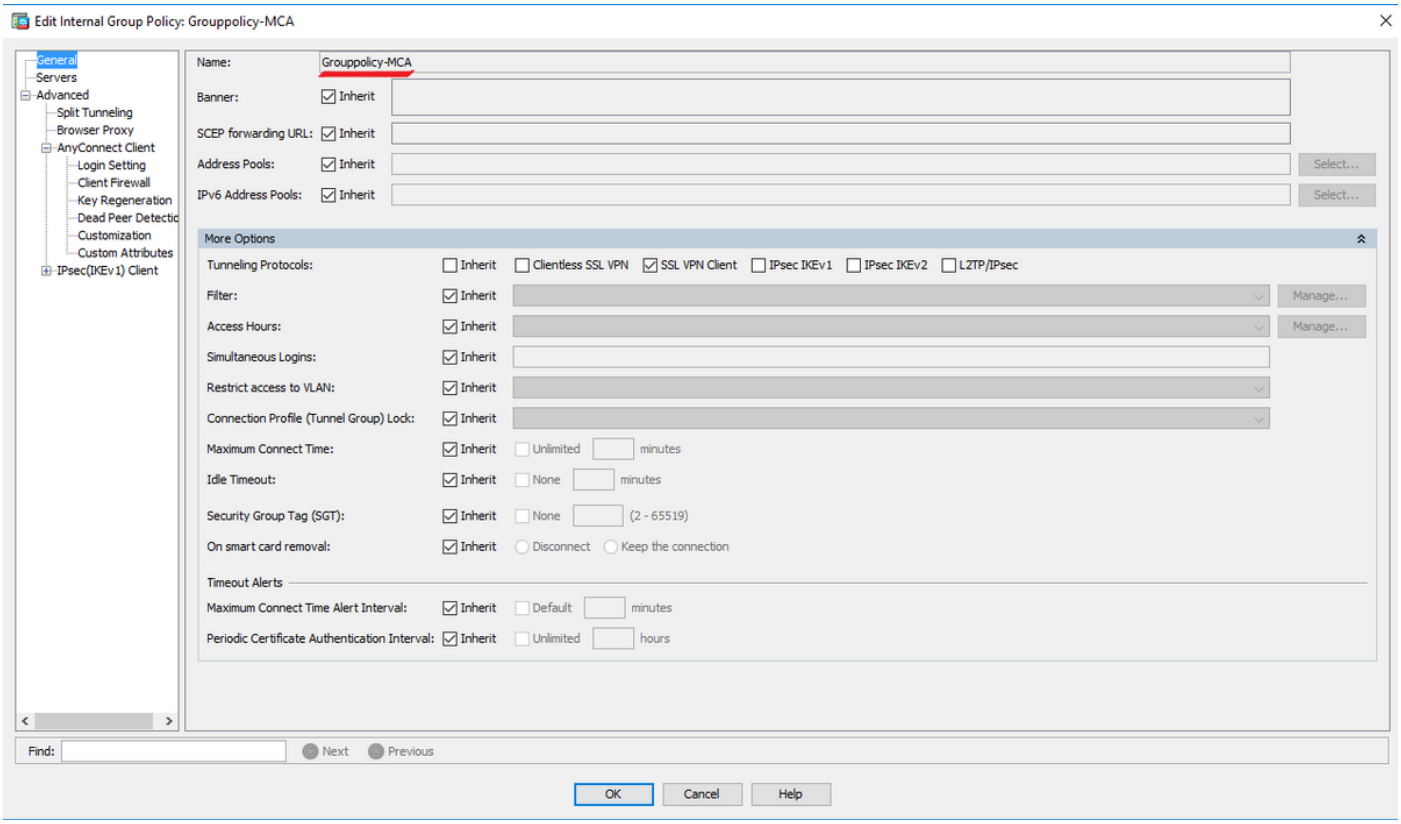
このセクションは多重 認証 認証で AnyConnect クライアントのための SSL ゲートウェイで Cisco ASA を設定する方法を記述します。

多重 認証 認証のための Anyconnect クライアントを設定するために ASDM によってこれらのステップを完了して下さい:

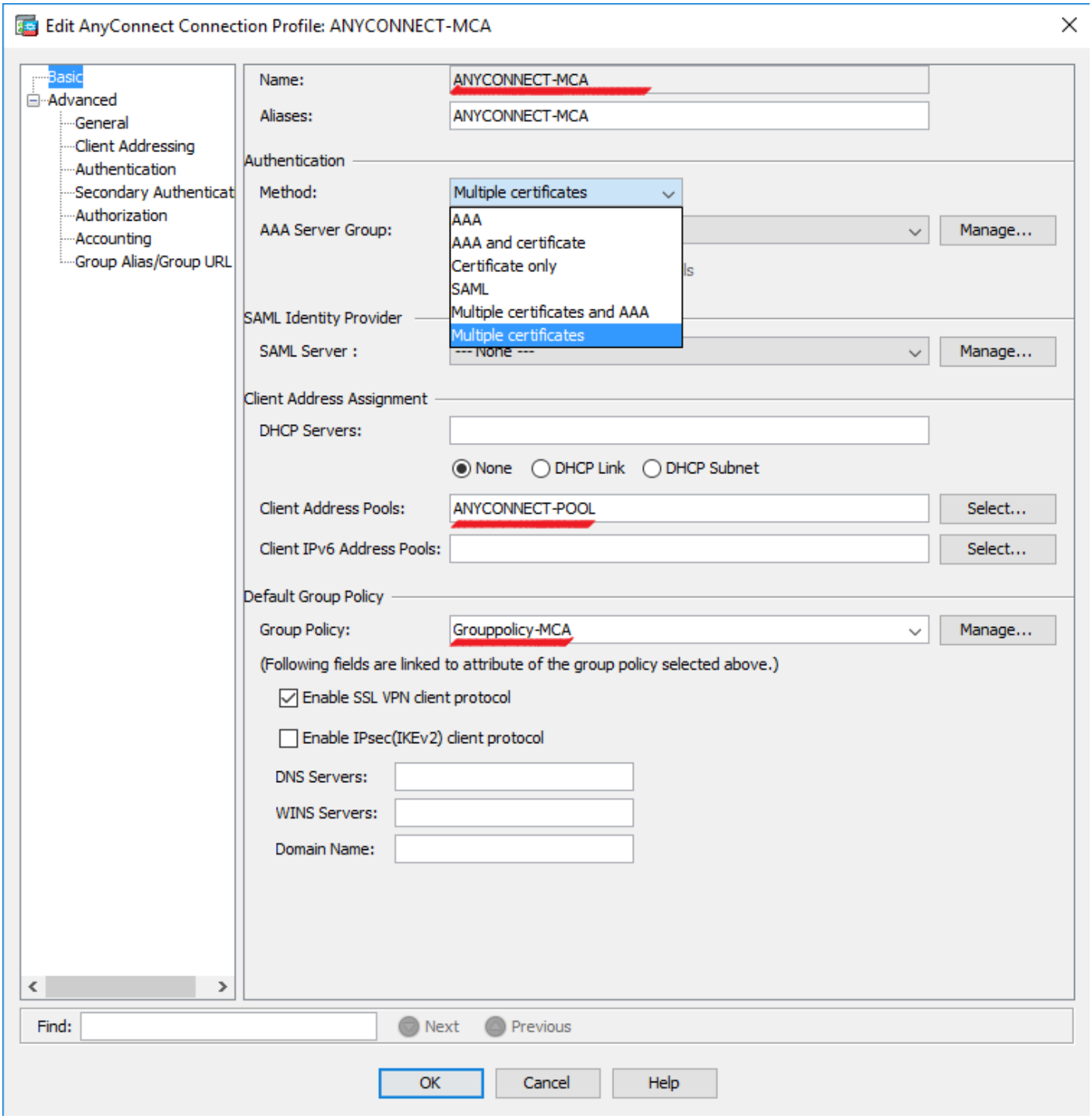
ステップ 1. ASA でユーザ向けの CA 認証およびマシン認証をインストールして下さい。

証明書のインストールに関しては設定します ASA を参照して下さい: SSL デジタル証明書のインストールと更新

ステップ 2.**設定 > リモート アクセス > グループ ポリシー**へのナビゲートはおよびグループ ポリシーを設定します。



ステップ 3.新しい接続プロファイルを設定し、多重 認証として**認証方式を**選択し、ステップ 1.で作成されるグループ ポリシーを選択して下さい。



ステップ 4 他の詳細なコンフィギュレーションに関しては、ローカルLAN 設定例を toVPN クライアントおよび AnyConnect クライアントアクセスを*参照して下さい*

CLI によって多重 認証認証のための ASA を設定して下さい

注: このセクションで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

```
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
```

確認

このセクションでは、設定が正常に機能していることを確認します。

> **注:** 特定の show コマンドがアウトプット インタープリタ ツール（登録ユーザ専用）でサポートされています。 show コマンド出力の分析を表示するには、アウトプット インタープリタ ツールを使用します。

CLI によって ASA のインストール済み証明書を表示して下さい

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
```

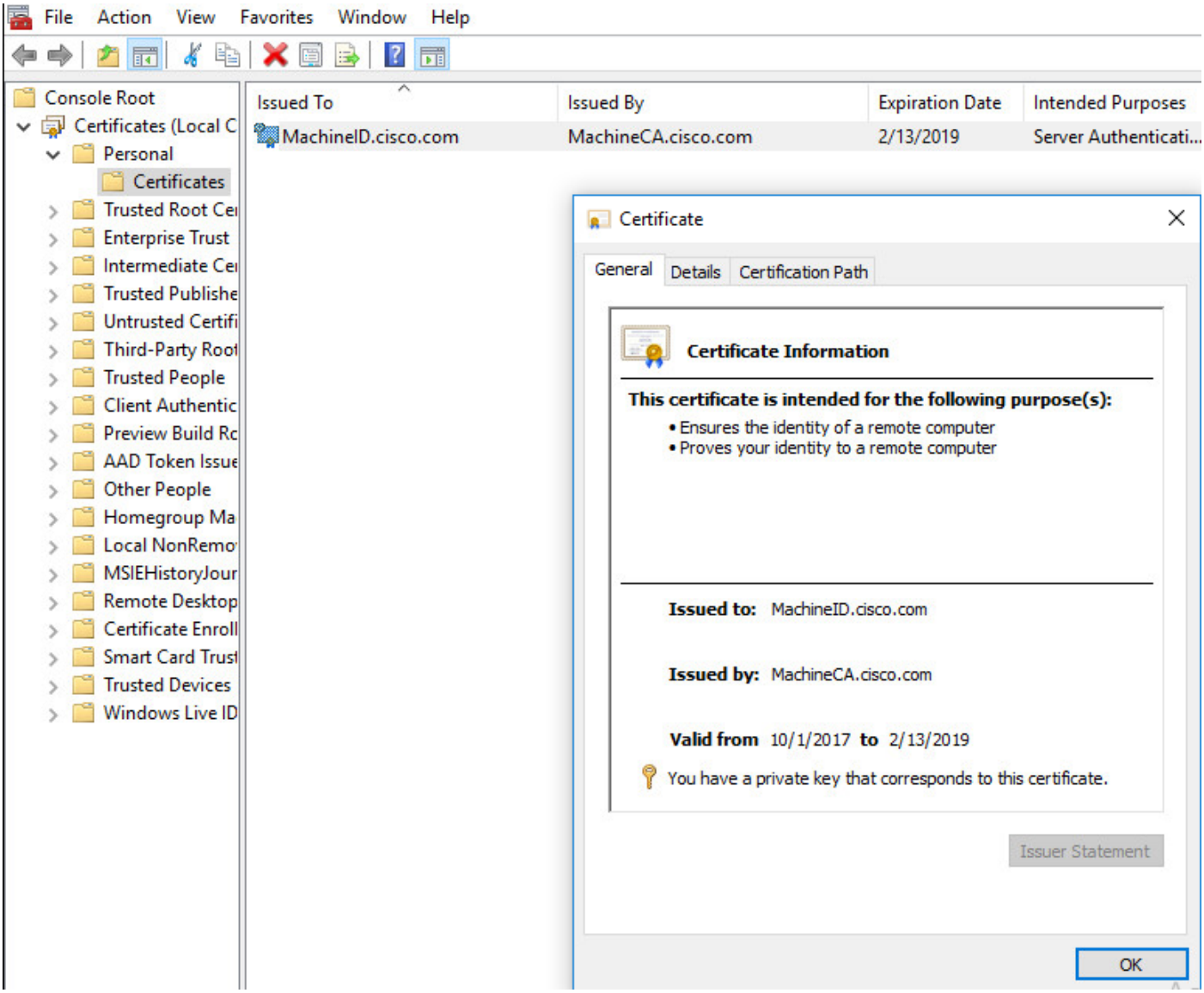
```
CA Certificate

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
```

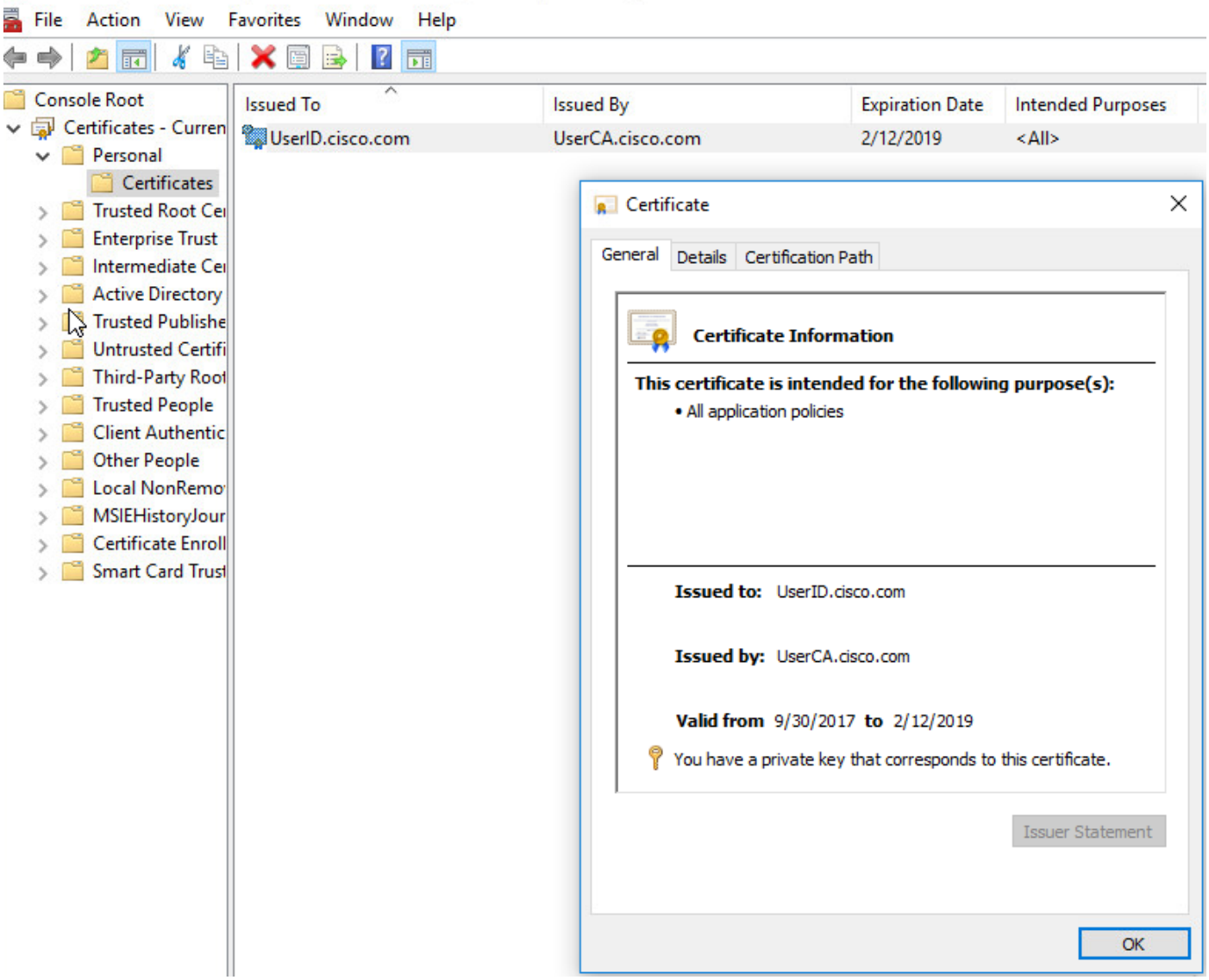
クライアントのインストール済み証明書を表示して下さい

インストールを確認するために、認証マネージャ（certmgr.msc）を使用して下さい:

マシン認証


File Action View Favorites Window Help
Console Root
Certificates (Local C
Personal
Certificates
Trusted Root Cer
Enterprise Trust
Intermediate Cer
Trusted Publishe
Untrusted Certifi
Third-Party Root
Trusted People
Client Authentic
Preview Build Rc
AAD Token Issue
Other People
Homegroup Ma
Local NonRemo
MSIEHistoryJour
Remote Desktop
Certificate Enroll
Smart Card Trust
Trusted Devices
Windows Live ID
Issued To
Issued By
Expiration Date
Intended Purposes
MachineID.cisco.com
MachineCA.cisco.com
2/13/2019
Server Authenticati...
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

ユーザ証明書



接続を確認するこのコマンドを実行して下さい:

```
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
```

トラブルシューティング

このセクションでは、設定のトラブルシューティングに役立つ情報を提供します。

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

> **注意**： ASA では、さまざまなデバッグ レベルを設定できます。 デフォルトでは、レベル 1 が使用されます。 デバッグ レベルを変更すると、デバッグの冗長性が高くなる場合があります。 特に実稼働環境では、注意して実行してください。

- Debug crypto ca メッセージ 127
- Debug crypto ca トランザクション 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.
```

- **デバッグ集約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
```

- **デバッグ集約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
```

関連情報

- Cisco ASA シリーズ用のリリース ノート、9.7(x)
- Cisco AnyConnect セキュア モビリティ クライアント 管理者ガイド、リリース 4.4
- AnyConnect VPN クライアントのトラブルシューティング ガイド - 一般的な問題
- テクニカル サポートとドキュメント