

# Authentification double ASA AnyConnect avec la validation de certificat, le mappage, et le guide de configuration de préremplissage

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Configurez](#)

[Certificat pour AnyConnect](#)

[Installation de certificat sur l'ASA](#)

[Configuration ASA pour la validation simple d'authentification et de certificat](#)

[Test](#)

[Debug](#)

[Configuration ASA pour l'Authentification double et la validation de certificat](#)

[Test](#)

[Debug](#)

[Configuration ASA pour l'Authentification double et le préremplissage](#)

[Test](#)

[Debug](#)

[Configuration ASA pour l'Authentification double et le mappage de certificat](#)

[Test](#)

[Debug](#)

[Dépannez](#)

[Certificat valide non actuel](#)

[Informations connexes](#)

## Introduction

Ce document décrit un exemple de configuration pour l'accès de Client à mobilité sécurisé Cisco AnyConnect de l'appliance de sécurité adaptable (ASA) qui utilise l'Authentification double avec la validation de certificat. En tant qu'utilisateur d'AnyConnect, vous devez fournir le certificat et les qualifications corrects pour l'authentification primaire et secondaire afin d'obtenir l'accès VPN. Ce document fournit également à un exemple du mappage de certificat la configuration de préremplissage.

## Conditions préalables

## Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissance de base de configuration de l'interface de ligne de commande ASA (CLI) et de configuration du VPN de Protocole SSL (Secure Socket Layer)
- Connaissance de base des Certificats X509

## Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel de l'appliance de sécurité adaptable Cisco (ASA), version 8.4 et ultérieures
- Windows 7 avec le Client à mobilité sécurisé Cisco AnyConnect 3.1

On le suppose que vous avez utilisé un Autorité de certification (CA) externe afin de se produire :

- Un certificat standard de la cryptographie à clé publique #12 (PKCS #12) base64-encoded pour ASA (anyconnect.pfx)
- Un certificat PKCS #12 pour AnyConnect

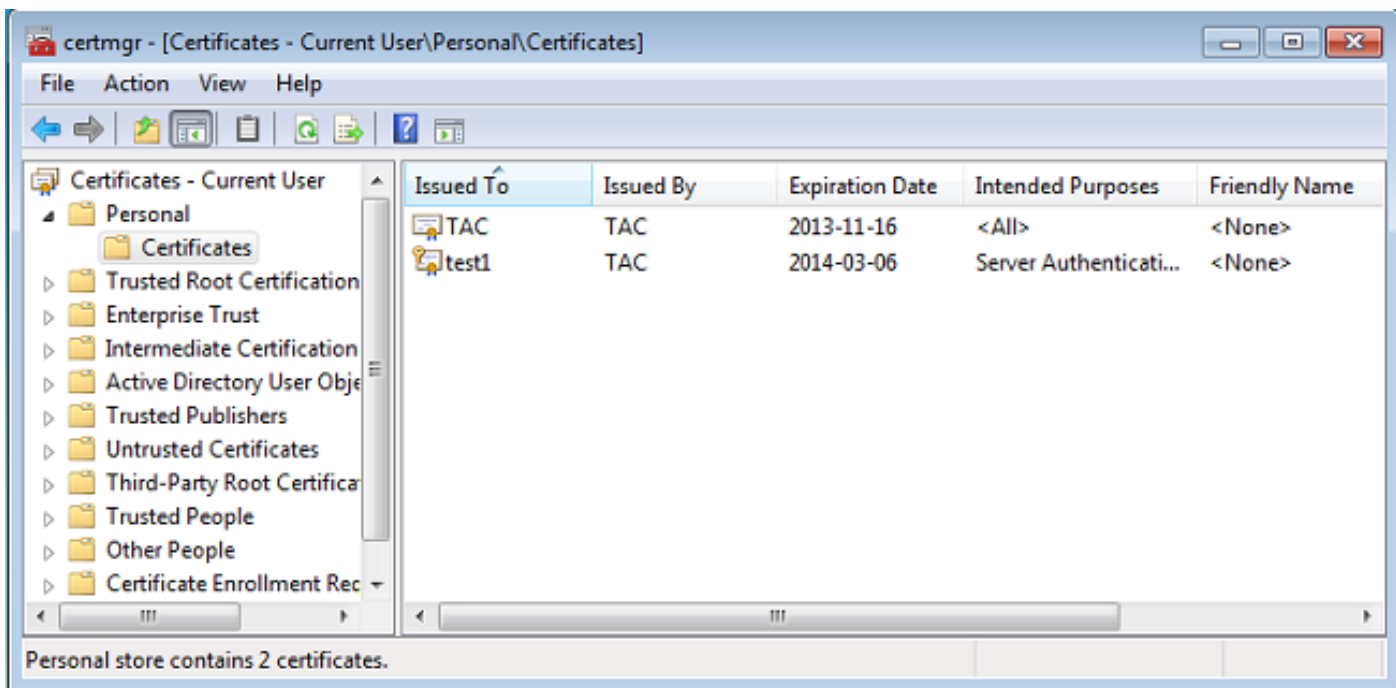
## Configurez

Remarque: Utilisez l'[Outil de recherche de commande](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

### Certificat pour AnyConnect

Afin d'installer un certificat d'exemple, double-cliquer le fichier anyconnect.pfx, et installez ce certificat comme certificat personnel.

Utilisez le gestionnaire de certificat (certmgr.msc) afin de vérifier l'installation :



Par défaut, essais d'AnyConnect pour trouver un certificat dans la mémoire d'utilisateur de Microsoft ; il n'y a aucun besoin de n'apporter aucune modification dans le profil d'AnyConnect.

## Installation de certificat sur l'ASA

Cet exemple affiche comment l'ASA peut importer un certificat base64 PKCS #12 :

```
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 omitted>

...

```
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBskrOIeTlHARHbLF1FFQvSvBAhu0j9bTtZo
```

```
3AICCAA=
```

```
quit
```

**INFO: Import PKCS12 operation completed successfully**

Employez la commande de **show crypto ca certificat** afin de vérifier l'importation :

```
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 omitted>

...

```
83EwMTAhMAkGBSsOAwIaBQAEFCS/WBskrOIeTlHARHbLF1FFQvSvBAhu0j9bTtZo
```

```
3AICCAA=
```

```
quit
```

**INFO: Import PKCS12 operation completed successfully**

Remarque: [L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse

de sortie de commande show.

## Configuration ASA pour la validation simple d'authentification et de certificat

L'ASA utilise l'authentification d'Authentification, autorisation et comptabilité (AAA) et l'authentification de certificat. La validation de certificat est obligatoire. L'authentification d'AAA utilise une base de données locale.

Cet exemple affiche l'authentification simple avec la validation de certificat.

```
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

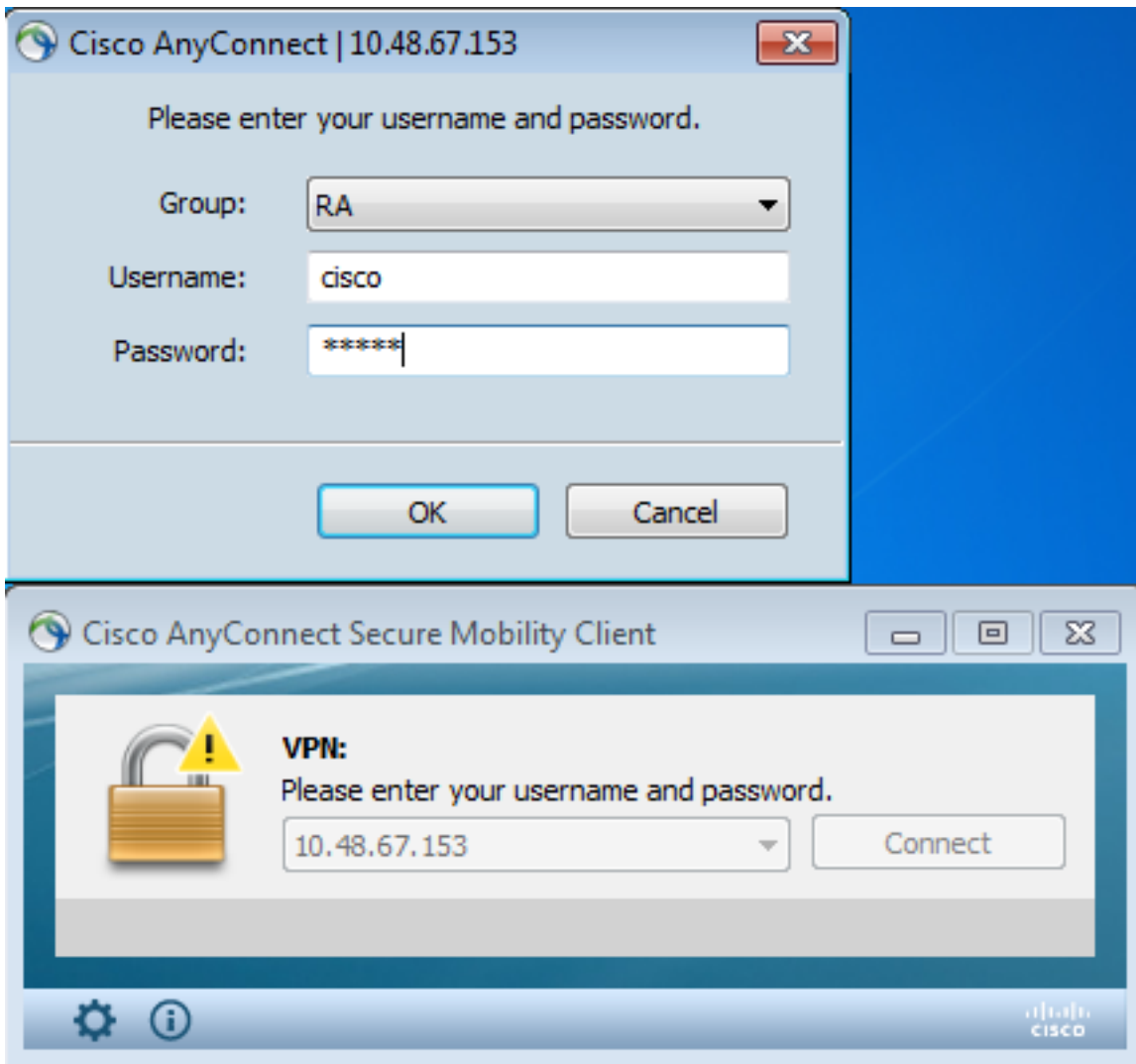
tunnel-group RA type remote-access
tunnel-group RA general-attributes
  authentication-server-group LOCAL
  default-group-policy Group1
  authorization-required
tunnel-group RA webvpn-attributes
  authentication aaa certificate
  group-alias RA enable
```

En plus de cette configuration, il est possible d'exécuter l'autorisation de Protocole LDAP (Lightweight Directory Access Protocol) avec le nom d'utilisateur d'un champ spécifique de certificat, tel que le nom de certificat (NC). Des attributs supplémentaires peuvent alors être récupérés et appliqués à la session VPN. Pour plus d'informations sur l'autorisation d'authentification et de certificat, référez-vous au « [Anyconnect VPN ASA et à l'autorisation d'OpenLDAP avec le schéma fait sur commande et délivrez un certificat l'exemple de configuration.](#) »

### Test

Remarque: [L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Afin de tester cette configuration, fournissez les qualifications locales (nom d'utilisateur Cisco avec le mot de passe cisco). Le certificat doit être présent :



Sélectionnez la commande d'anyconnect de détail de VPN-sessiondb d'exposition sur l'ASA :

```
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 : <b>Certificate</b>

**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 : <b>Certificate</b>

**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**

Remarque: Référez-vous aux [informations importantes sur les commandes de débogage](#) avant d'utiliser les commandes de **débogage**.

Dans cet exemple, le certificat n'a pas été caché dans la base de données, un CA correspondant a été trouvé, l'utilisation principale correcte a été utilisée (ClientAuthentication), et le certificat a été validé avec succès :

```
debug aaa authentication
debug aaa authorization
debug webvpn 255
debug webvpn anyconnect 255
debug crypto ca 255
```

Les commandes de débogage détaillées, telles que la commande du **debug webvpn 255**, peuvent générer beaucoup de logs dans un environnement de production et placer une charge lourde sur une ASA. Un certain webvpn met au point ont été retirés pour la clarté :

```
CERT_API: Authenticate session 0x0934d687, non-blocking cb=0x0000000012cfc50
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
```

C'est la tentative de trouver un groupe de tunnels étant assorti. Il n'y a aucune règle spécifique de mappage de certificat, et le groupe de tunnels que vous fournissez est utilisé :

```
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)
```

Ce sont le SSL et la session générale met au point :

```
%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.
```

## Configuration ASA pour l'Authentification double et la validation de certificat

C'est un exemple de l'Authentification double, où le serveur primaire d'authentification est LOCAL, et le serveur secondaire d'authentification est LDAP. La validation de certificat est encore activée.

Cet exemple affiche la configuration de LDAP :

```
%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.
```

Voici l'ajout d'un serveur secondaire d'authentification :

```
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
```

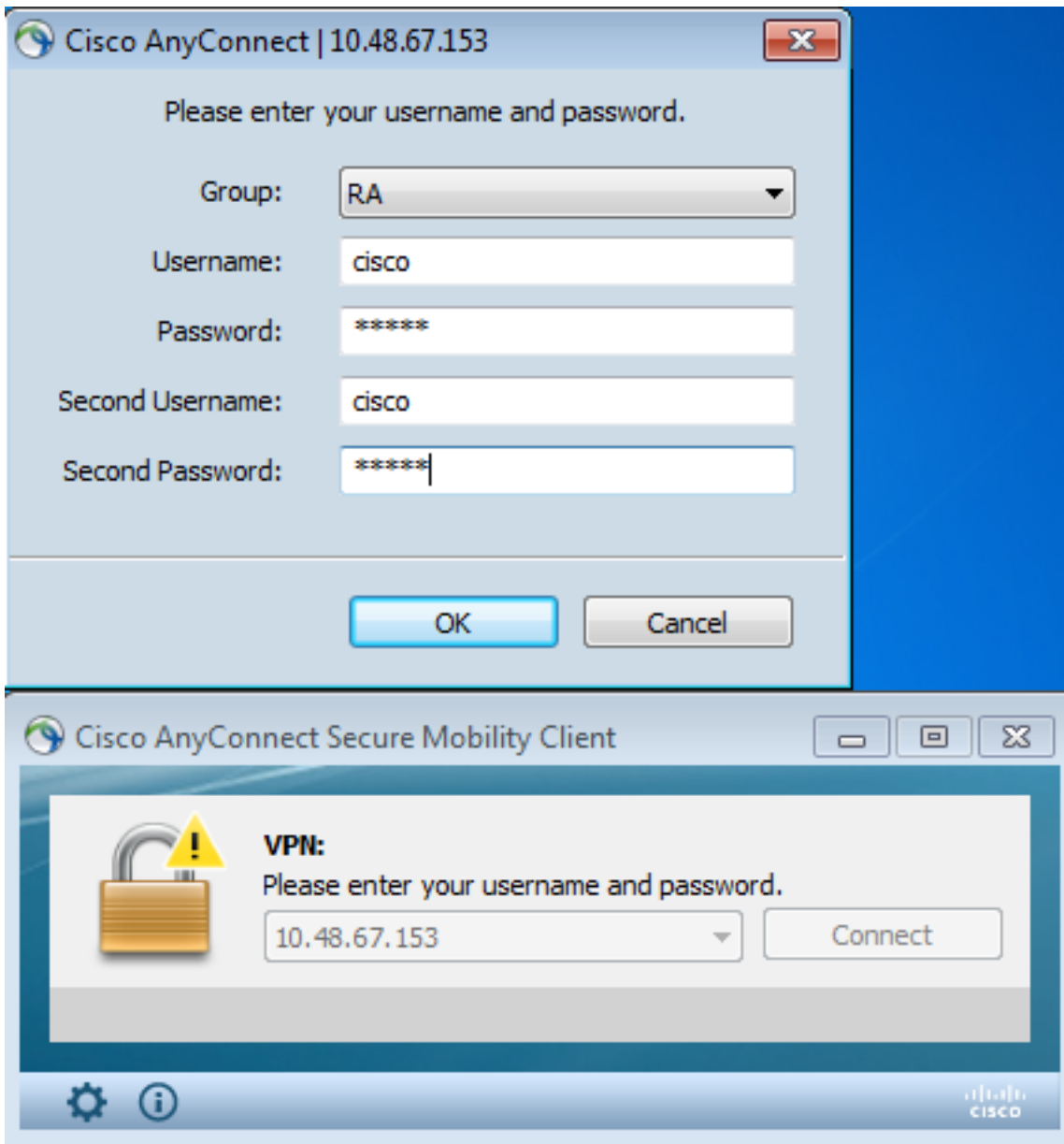
Vous ne voyez pas des « GENS DU PAYS d'authentification-serveur-groupe » dans la configuration parce que c'est une valeur par défaut.

N'importe quel autre serveur d'AAA peut être utilisé pour le « authentification-serveur-groupe. » Pour le « secondaire-authentification-serveur-groupe, » il est possible d'utiliser tous les serveurs d'AAA excepté un serveur d'International de dynamics de Sécurité (SDI) ; dans ce cas, le SDI a pu encore être le serveur primaire d'authentification.

## Test

Remarque: [L'Output Interpreter Tool](#) (clients [enregistrés](#) seulement) prend en charge certaines **commandes show**. Utilisez l'Output Interpreter Tool afin de visualiser une analyse de sortie de commande show.

Afin de tester cette configuration, fournissez les qualifications locales (nom d'utilisateur Cisco avec le mot de passe cisco) et les qualifications de LDAP (nom d'utilisateur Cisco avec le mot de passe du LDAP). Le certificat doit être présent :



Sélectionnez la commande d'anyconnect de détail de VPN-sessiondb d'exposition sur l'ASA.

Les résultats sont semblables à ceux pour l'authentification simple. Référez-vous à la [« configuration ASA pour la validation simple d'authentification et de certificat, test. »](#)

## Debug

Les debugs pour la session et l'authentification de webvpn sont semblables. Référez-vous à la [« configuration ASA pour la validation simple d'authentification et de certificat, debug. »](#) Une procédure d'authentification supplémentaire apparaît :

```
%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
```

Les debugs pour le LDAP affichent les détails qui pourraient varier avec la configuration de LDAP :

```
%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
```

## Configuration ASA pour l'Authentification double et le préremplissage

Il est possible de tracer certains champs de certificat au nom d'utilisateur qui est utilisé pour l'authentification primaire et secondaire :

```
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
```

Dans cet exemple, le client utilise le certificat : **cn=test1,ou=Security, o=Cisco, l=Krakow, st=PL, c=PL**.

Pour l'authentification primaire, le nom d'utilisateur est pris de la NC, qui est pourquoi l'utilisateur local 'test1' a été créé.

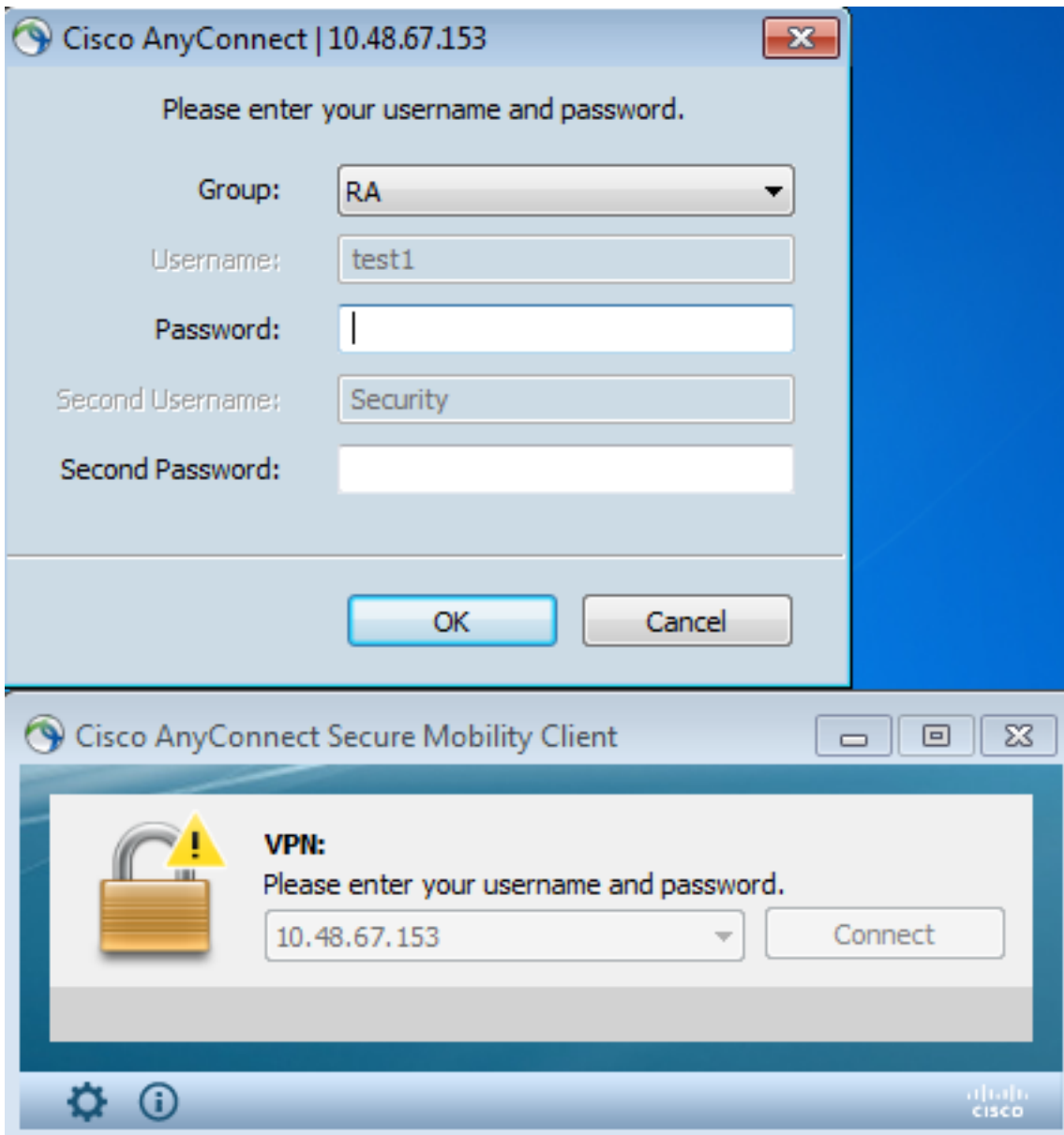
Pour l'authentification secondaire, le nom d'utilisateur est pris à partir de l'unité organisationnelle (l'OU, qui est pourquoi l'utilisateur « Sécurité » a été créé sur le serveur LDAP).

Il est également possible de forcer AnyConnect à employer des commandes de préremplissage afin de préremplir le nom d'utilisateur primaire et secondaire.

Dans un scénario de monde réel, le serveur primaire d'authentification est habituellement un AD ou un serveur LDAP, alors que le serveur secondaire d'authentification est le serveur de Rivest, de Shamir, et d'Adelman (RSA) qui utilise les mots de passe symboliques. Dans ce scénario, l'utilisateur doit fournir les qualifications AD/LDAP (que l'utilisateur connaît), un mot de passe symbolique RSA (que l'utilisateur a) et un certificat (sur l'ordinateur qui est utilisé).

## Test

Observez que vous ne pouvez pas changer le nom d'utilisateur primaire ou secondaire parce qu'il est prérempli des champs NC et OU de certificat :



## Debug

Cet exemple affiche la requête envoyée de préremplissage à AnyConnect :

```
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
```

Voici que vous voyez que l'authentification utilise les noms d'utilisateur corrects :

```
%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
```

## Configuration ASA pour l'Authentification double et le mappage de certificat

Il est également possible de tracer les certificats client spécifiques aux groupes de tunnels spécifiques, suivant les indications de cet exemple :

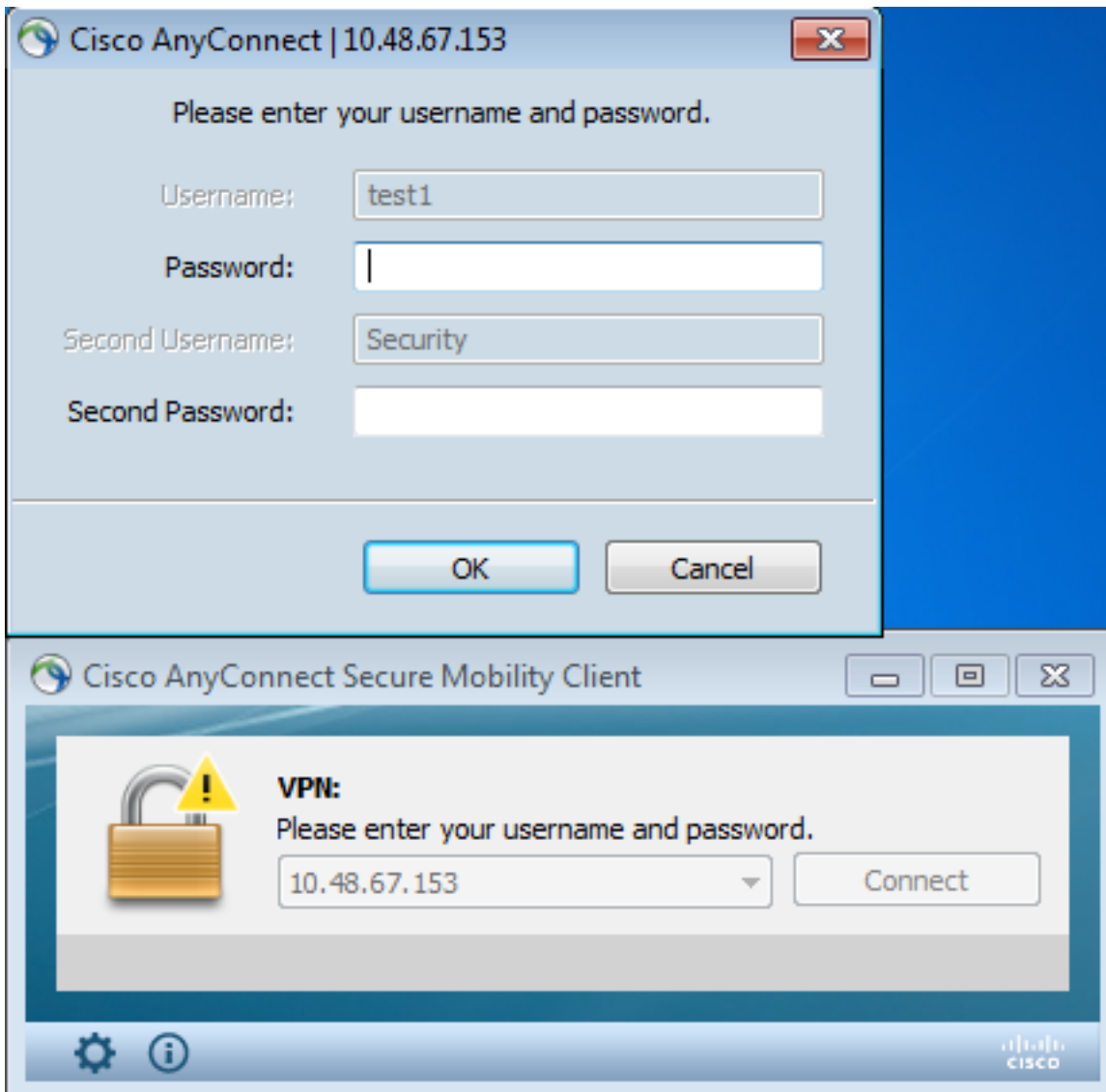
```
%ASA-6-113012: AAA user authentication Successful : local database : user = test1  
%ASA-6-302013: Built outbound TCP connection 2137 for outside:10.147.24.60/389  
(10.147.24.60/389) to identity:10.48.67.153/46606 (10.48.67.153/46606)  
%ASA-6-113004: AAA user authentication Successful : server = 10.147.24.60 :  
user = Security
```

De cette façon, tous les certificats utilisateurs signés par le centre d'assistance technique Cisco (TAC) CA sont tracées à un groupe de tunnels nommé le « RA. »

Remarque: Le mappage de certificat pour le SSL est configuré différemment que le mappage de certificat pour IPsec. Pour IPsec, il est configuré utilisant des règles de « tunnel-groupe-MAP » en mode de configuration globale. Pour le SSL, il est configuré utilisant la « certificat-groupe-MAP » sous le mode de config de webvpn.

## Test

Observez que, une fois mappage de certificat est activé, vous n'avez besoin de choisir le groupe de tunnels plus :



## Debug

Dans cet exemple, la règle de mappage de certificat laisse le groupe de tunnels à trouver :

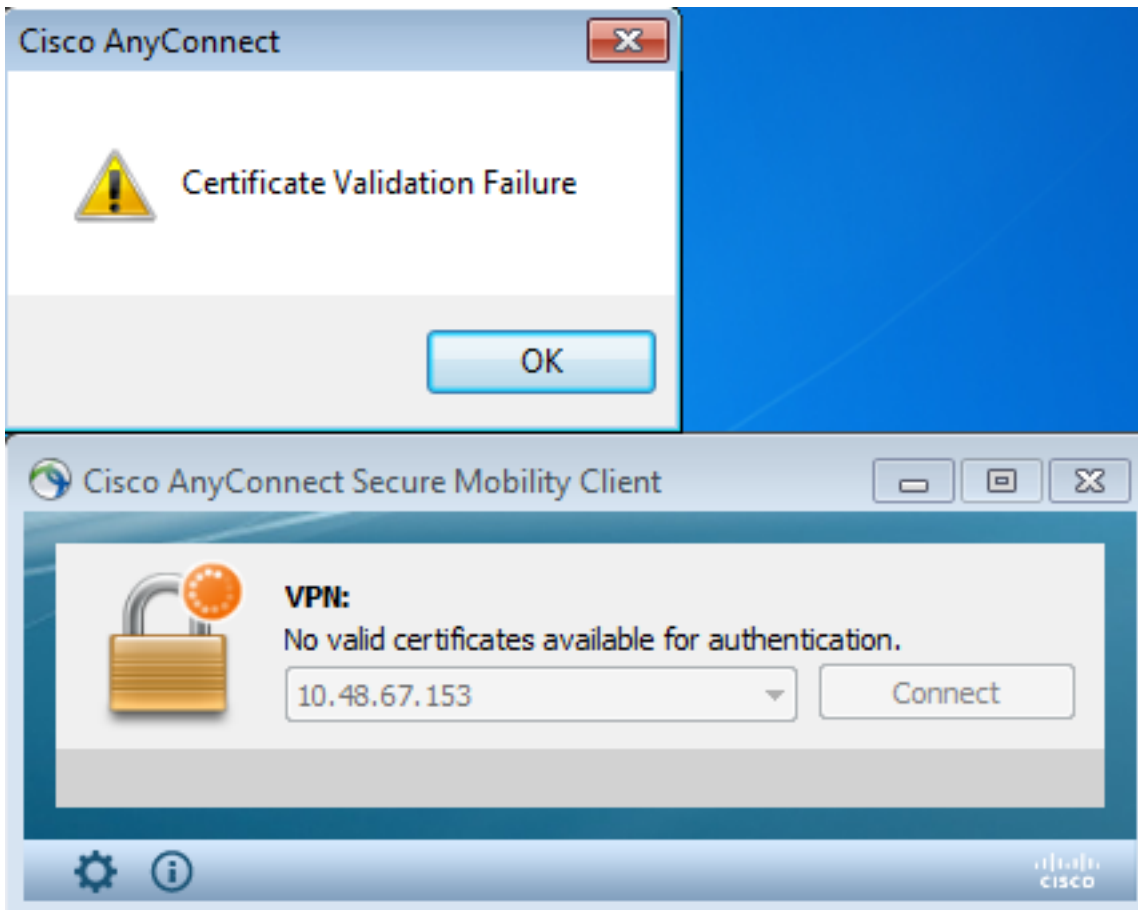
```
%ASA-7-717036: Looking for a tunnel group match based on certificate maps for peer certificate with serial number: 00FE9C3D61E131CDB1, subject name: cn=test1, ou=Security,o=Cisco,l=Krakow,st=PL,c=PL, issuer_name: cn=TAC,ou=RAC,o=TAC,l=Warsaw,st=Maz,c=PL.  
%ASA-7-717038: Tunnel group match found. 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.
```

## Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

### Certificat valide non actuel

Après que vous retiriez un certificat valide de Windows7, AnyConnect ne peut trouver aucun Certificats valides :



Sur l'ASA, il ressemble à la session est terminé par le client (remise-Je) :

```
%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
```

## [Informations connexes](#)

- [Configurer le tunnel Groupes, les stratégies de groupe, et les utilisateurs : Configurer l'Authentification double](#)
- [Configurer un serveur externe pour l'autorisation d'utilisateur de dispositifs de sécurité](#)

- [Support et documentation techniques - Cisco Systems](#)