

ASA 8.X : Exemple de configuration d'inscription SCEP AnyConnect

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Informations générales](#)

[Aperçu des modifications requises](#)

[Configurations XML pour activer la caractéristique d'Anyconnect SCEP](#)

[Configurez l'ASA pour prendre en charge SCEP Protocol pour AnyConnect](#)

[Test AnyConnect SCEP](#)

[Mémoire de certificat sur Microsoft Windows après demande SCEP](#)

[Dépannez](#)

[Informations connexes](#)

[Introduction](#)

La fonctionnalité d'inscription SCEP est introduite dans le client autonome AnyConnect 2.4. Dans ce processus, vous modifiez le profil d'AnyConnect XML pour inclure une configuration liée SCEP et pour créer un profil spécifique de stratégie de groupe et de connexion pour l'inscription de certificat. Quand un utilisateur d'AnyConnect se connecte à ce groupe spécifique, AnyConnect envoie une demande d'inscription de certificat au serveur CA, et le serveur CA automatiquement reçoit ou refuse la demande.

[Conditions préalables](#)

[Conditions requises](#)

Aucune spécification déterminée n'est requise pour ce document.

[Composants utilisés](#)

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

- Dispositifs de sécurité adaptatifs dédiés de la gamme Cisco ASA 5500 cette version de logiciel 8.x de passage
- Version 2.4 du Cisco AnyConnect VPN

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Informations générales

Le but de l'inscription automatique SCEP pour AnyConnect est de fournir un certificat au client d'une manière sécurisée et extensible. Par exemple, les utilisateurs n'ont pas besoin de demander un certificat d'un serveur CA. Cette fonctionnalité est intégrée dans le client d'AnyConnect. Les Certificats sont fournis aux clients basés sur les paramètres de certificat mentionnés dans le fichier des profils XML.

Aperçu des modifications requises

La caractéristique d'inscription d'AnyConnect SCEP exige de certains paramètres de certificat d'être définis dans le profil XML. Un profil de stratégie de groupe et de connexion est créé sur l'ASA pour l'inscription de certificat, et le profil XML est associé avec cette stratégie. Le client d'AnyConnect se connecte au profil de connexion qui utilise cette stratégie spécifique et envoie une demande d'un certificat avec les paramètres qui sont définis dans le fichier XML. L'Autorité de certification (CA) automatiquement reçoit ou refuse la demande. Le client d'AnyConnect récupère des Certificats avec le protocole SCEP si l'élément de <CertificateSCEP> est défini dans un profil de client.

L'authentification de certificat client doit échouer avant que les essais d'AnyConnect pour récupérer automatiquement les nouveaux Certificats, ainsi si vous aient déjà un certificat valide installé, l'inscription ne se produit pas.

Quand les utilisateurs ouvrent une session au groupe spécifique, ils sont automatiquement inscrits. Il y a également une méthode manuelle disponible pour la récupération de certificat dans laquelle des utilisateurs sont présentés avec un bouton de **certificat d'obtenir**. Ceci fonctionne seulement quand le client a l'accès direct au serveur CA, pas par le tunnel.

Référez-vous au [guide de l'administrateur de Cisco AnyConnect VPN Client](#), pour en savoir plus de [version 2.4](#).

Configurations XML pour activer la caractéristique d'Anyconnect SCEP

Ce sont les importants éléments qui doivent être définis dans le fichier XML d'AnyConnect. Référez-vous au [guide de l'administrateur de Cisco AnyConnect VPN Client](#), pour en savoir plus de [version 2.4](#).

- <AutomaticSCEPHost> — Spécifie le profil de nom d'hôte et de connexion ASA (groupe de

tunnel) pour lequel la récupération de certificat SCEP est configurée. La valeur doit être dans le format du nom de domaine complet du nom de profil ASA \ connexion ou de l'adresse IP du nom de profil ASA \ connexion.

- <CAURL> — Identifie le serveur SCEP CA.
- <CertificateSCEP> — Définit comment le contenu du certificat est demandé.
- <DisplayGetCertButton> — Détermine si le GUI d'AnyConnect affiche le bouton de certificat d'obtenir. Il permet à des utilisateurs de demander manuellement le renouvellement ou le ravitaillement du certificat.

Voici un profil d'exemple :

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectProfile xmlns="http://schemas.xmlsoap.org/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/AnyConnectProfile.xsd">
<ClientInitialization>
<UseStartBeforeLogon UserControllable="true">>false</UseStartBeforeLogon>
<AutomaticCertSelection UserControllable="true">>true</AutomaticCertSelection>
<ShowPreConnectMessage>>false</ShowPreConnectMessage>
<CertificateStore>All</CertificateStore>
<CertificateStoreOverride>>false</CertificateStoreOverride>
<ProxySettings>Native</ProxySettings>
<AutoConnectOnStart UserControllable="true">>true</AutoConnectOnStart>
<MinimizeOnConnect UserControllable="true">>true</MinimizeOnConnect>
<LocalLanAccess UserControllable="true">>false</LocalLanAccess>
<AutoReconnect UserControllable="false">>true
<AutoReconnectBehavior UserControllable="false">
ReconnectAfterResume
</AutoReconnectBehavior>
</AutoReconnect>
<AutoUpdate UserControllable="false">>true</AutoUpdate>
<RSASecurIDIntegration UserControllable="false">
Automatic
</RSASecurIDIntegration>
<WindowsLogonEnforcement>SingleLocalLogon</WindowsLogonEnforcement>
<WindowsVPNEstablishment>AllowRemoteUsers</WindowsVPNEstablishment>
<AutomaticVPNPolicy>>false</AutomaticVPNPolicy>
<PPPEXclusion UserControllable="false">Automatic
<PPPEXclusionServerIP UserControllable="false"></PPPEXclusionServerIP>
</PPPEXclusion>
<EnableScripting UserControllable="false">>false</EnableScripting>
<CertificateEnrollment>
<AutomaticSCEPHost>asa2.cisco.com/certenroll</AutomaticSCEPHost>
<CAURL PromptForChallengePW="false">
http://10.11.11.1/certsrv/mscep/mscep.dll
</CAURL>
<CertificateSCEP>
<Name_CN>cisco</Name_CN>
<Company_O>Cisco</Company_O>
<DisplayGetCertButton>>true</DisplayGetCertButton>
</CertificateSCEP>
</CertificateEnrollment>
</ClientInitialization>
<ServerList>
<HostEntry>
<HostName>asa2.cisco.com</HostName>
</HostEntry>
</ServerList>
</AnyConnectProfile>
```

[Configurez l'ASA pour prendre en charge SCEP Protocol pour](#)

AnyConnect

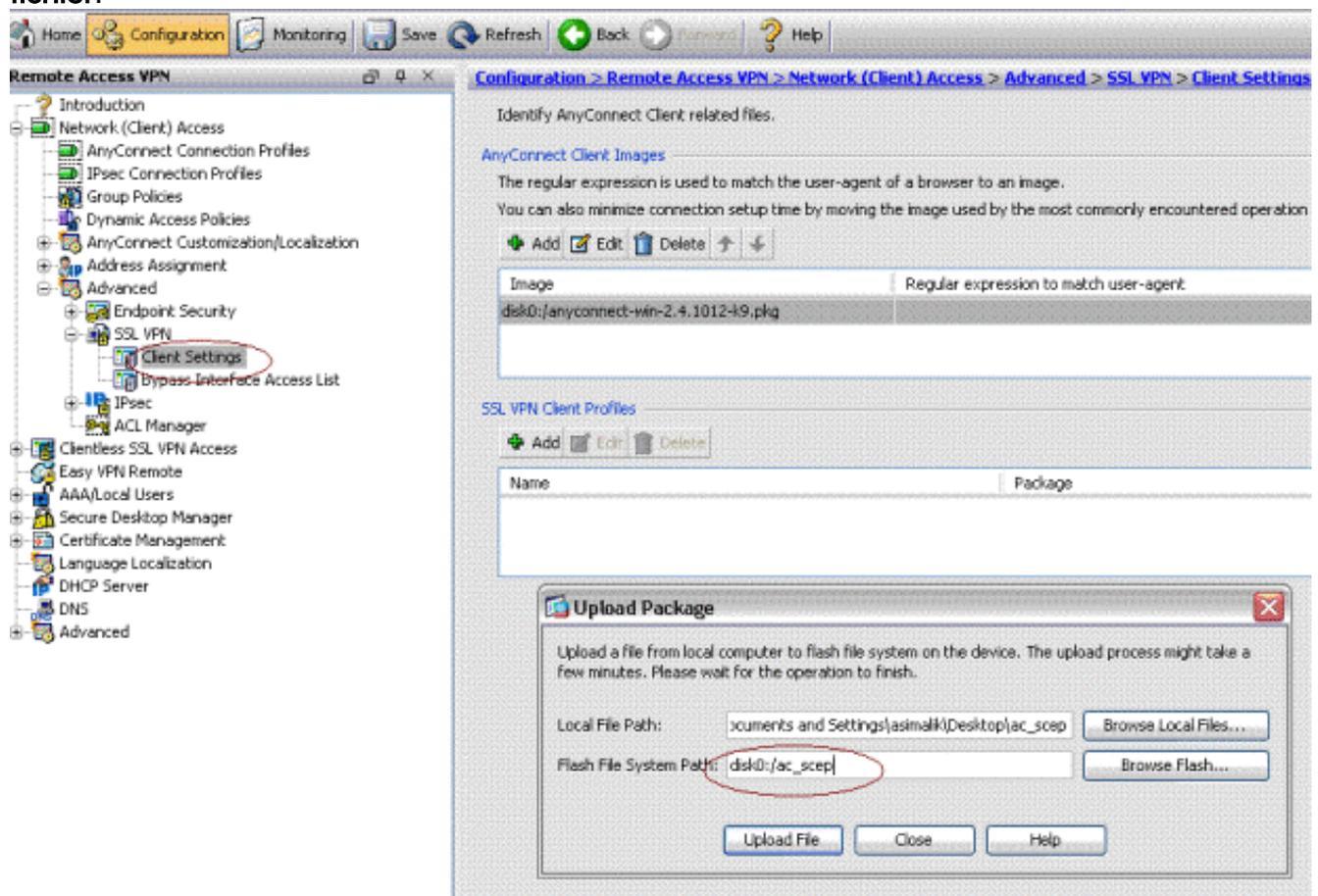
Afin de permettre d'accéder à une autorité d'enregistrement privée (RA), l'administrateur ASA doit créer un pseudonyme qui a un ACL qui limite la connexion réseau latérale privée au RA désiré. Afin de récupérer automatiquement un certificat, les utilisateurs se connectent et authentifient au ce alias.

Procédez comme suit :

1. Créez un pseudonyme sur l'ASA pour indiquer le groupe configuré par particularité.
2. Spécifiez le pseudonyme dans l'élément de <AutomaticSCEPHost> dans le profil de client de l'utilisateur.
3. Reliez le profil de client qui contient la section de <CertificateEnrollment> au groupe configuré par particularité.
4. Placez un ACL pour que le groupe configuré par particularité limite le trafic au RA latéral privé.

Procédez comme suit :

1. Téléchargez le profil XML à l'ASA. Choisissez l'**Accès à distance VPN > accès de réseau (client) > avancé > des configurations de VPN SSL > de client**. Sous des profils de client de VPN SSL, cliquez sur Add. Le clic **parcourent des fichiers locaux** afin de sélectionner le fichier des profils, et le clic **Browse Flash** afin de spécifier le nom du fichier instantané. Cliquez sur Upload le fichier.



2. Installez une stratégie de groupe de **certenroll** pour l'inscription de certificat. Choisissez l'**Accès à distance VPN > accès > stratégie de groupe de client réseau**, et cliquez sur

Add.

Edit Internal Group Policy: certenroll

Name:

Banner: Inherit

More Options

Tunneling Protocols: Inherit Clientless SSL VPN SSL VPN Client IPsec

Web ACL: Inherit Manage...

Access Hours: Inherit Manage...

Simultaneous Logins: Inherit

Restrict access to VLAN: Inherit

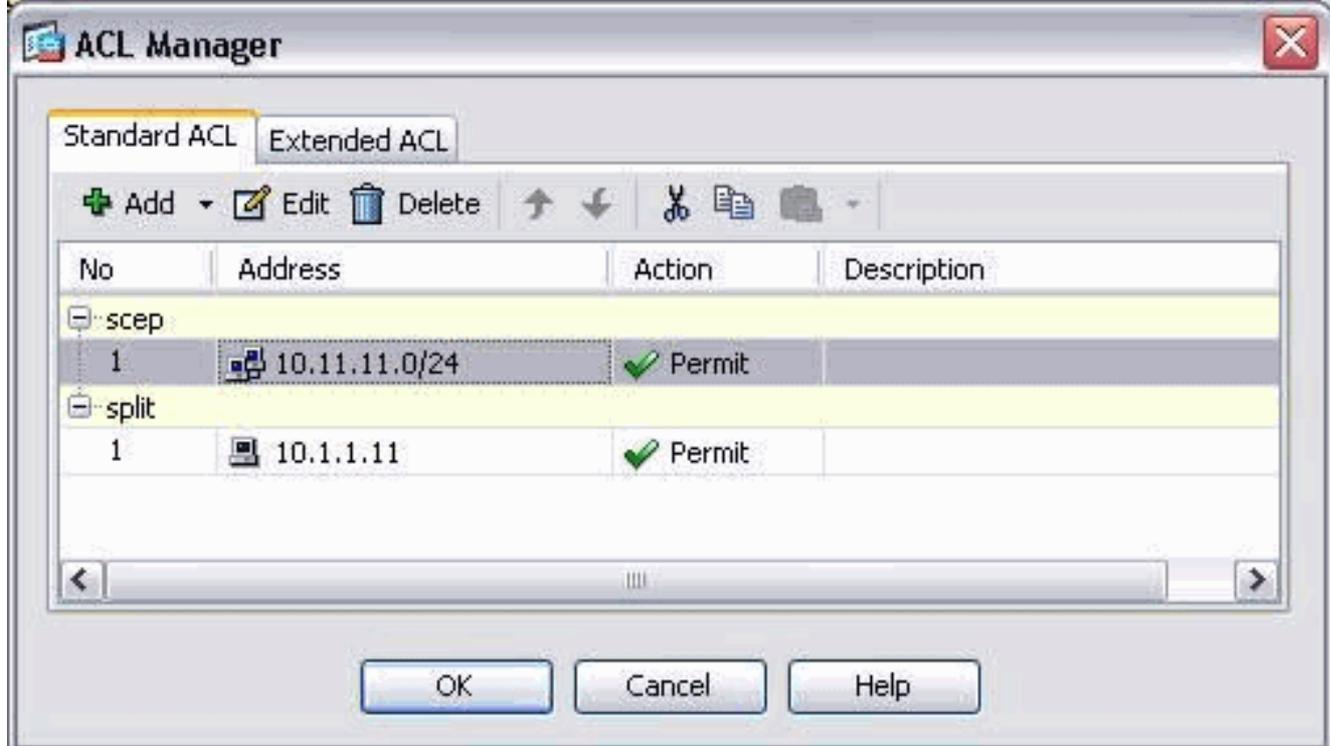
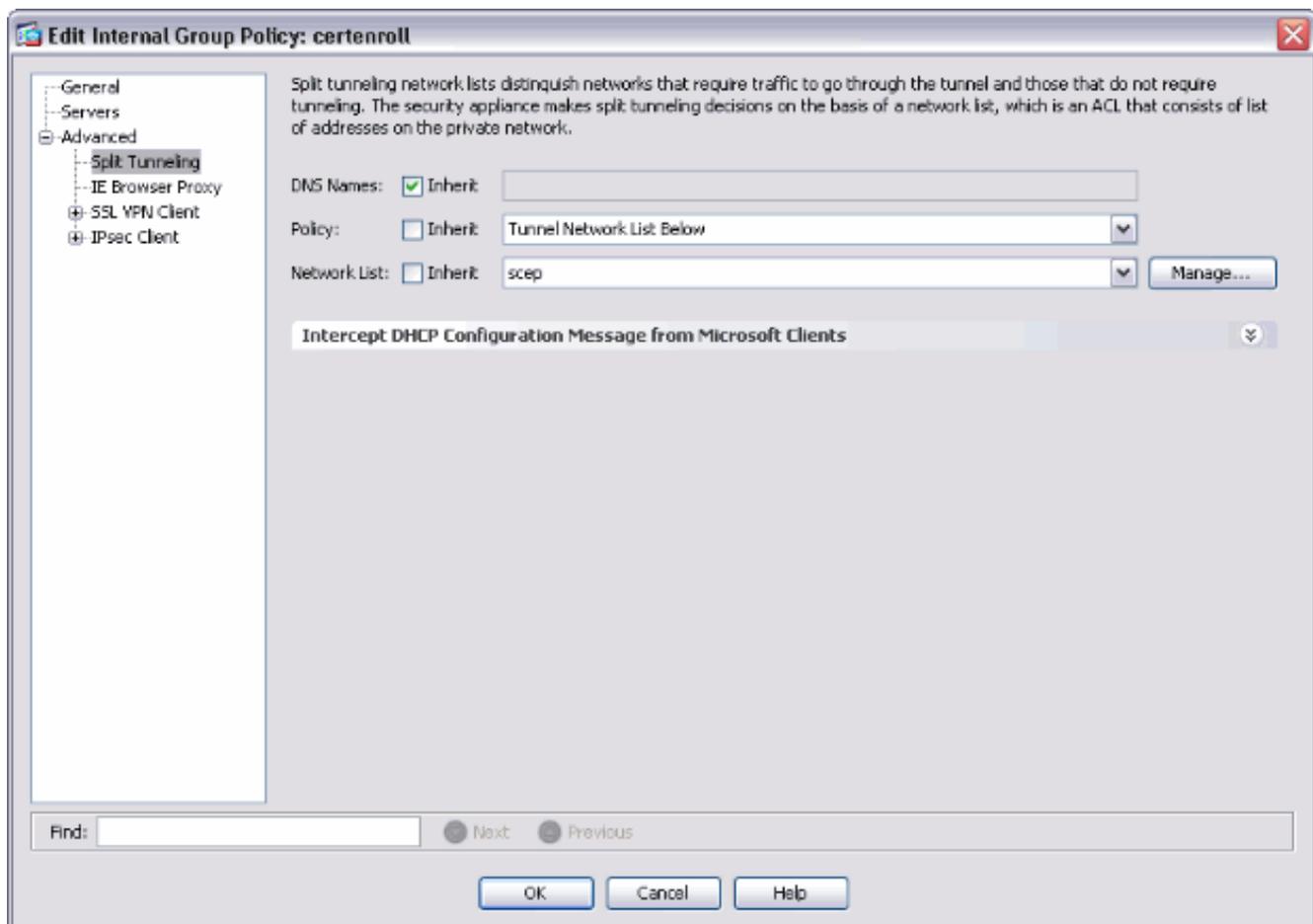
Connection Profile (Tunnel Group) Lock: Inherit

Maximum Connect Time: Inherit Unlimited minutes

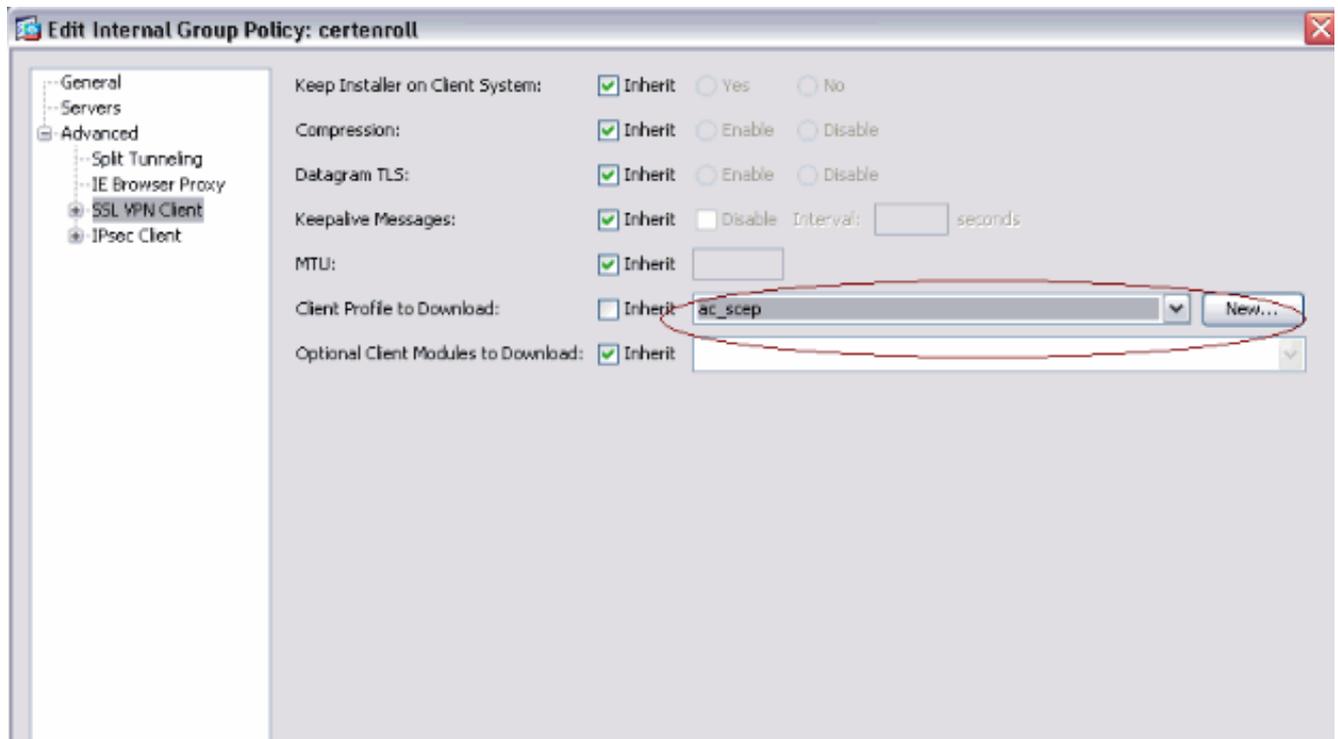
Idle Timeout: Inherit Unlimited minutes

Find: Next Previous

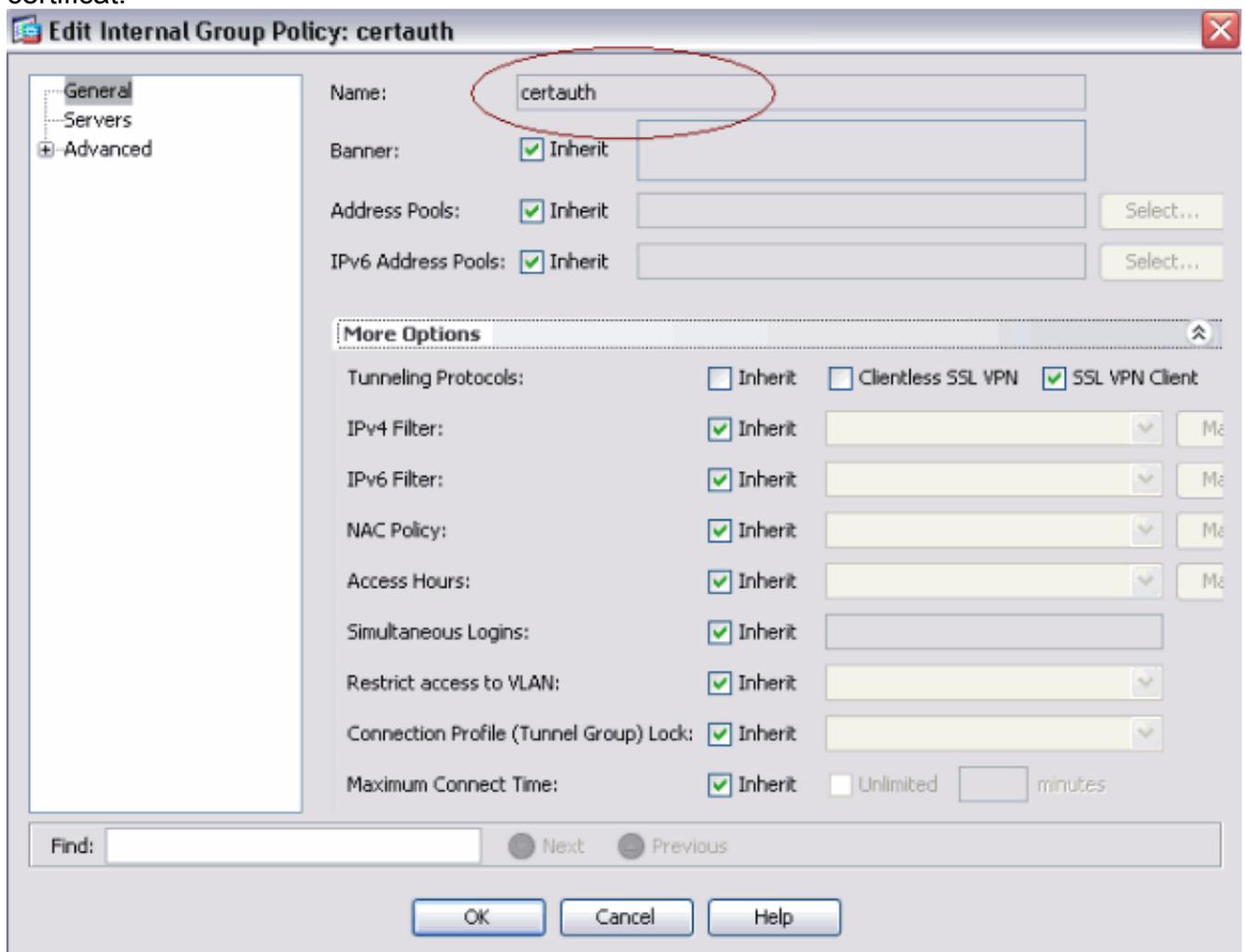
Ajoutez un tunnel partagé pour le serveur CA. Développez **avancé**, et puis sélectionnez la **Segmentation de tunnel**. Choisissez la **liste des réseaux de tunnel ci-dessous** du menu de stratégie, et le clic **parviennent** afin d'ajouter la liste de contrôle d'accès.



Le client choisi de VPN SSL, et choisissent le profil pour le certenroll du profil de client pour télécharger le menu.



3. Créez un autre groupe appelé le **certauth** pour l'authentification de certificat.



4. Créez un profil de connexion de certenroll. Choisissez l'**Accès à distance VPN > accès de client réseau > des profils de connexion d'AnyConnect**, et cliquez sur Add. Écrivez le groupe de **certenroll** dans le domaine de pseudonymes. **Remarque:** Le pseudonyme doit apparier la valeur utilisée dans le profil d'AnyConnect sous

AutomaticSCEPHost.

Add SSL VPN Connection Profile

Name: certenroll

Aliases: certenroll

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: ssl_pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: certenroll Manage...

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN Client protocol

5. Établissez un autre rapport profiler le **certauth** appelé avec l'authentification de certificat. C'est le profil réel de connexion qui est utilisé après inscription.

Edit SSL VPN Connection Profile: certauth

Name: certauth

Aliases: certauth

Authentication

Method: AAA Certificate Both

AAA Server Group: LOCAL Manage...

Use LOCAL if Server Group fails

Client Address Assignment

DHCP Servers:

Client Address Pools: ssl_pool Select...

Client IPv6 Address Pools: Select...

Default Group Policy

Group Policy: certauth Manage...

(Following field is an attribute of the group policy selected above.)

Enable SSL VPN Client protocol

6. Afin de s'assurer l'utilisation du pseudonyme est activé, contrôle permettent à l'utilisateur pour sélectionner le profil de connexion, identifié par son pseudonyme, sur la page de connexion. Autrement, DefaultWebVPNGroup est le profil de connexion.

Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles

The security appliance automatically deploys the Cisco AnyConnect VPN Client or legacy SSL VPN Client to remote users upon connection. The initial client deployment requires end-user administrative rights. The Cisco AnyConnect VPN Client supports the HTTPS/TCP (SSL) and Datagram Transport Layer Security (DTLS) tunneling options.

(More client-related parameters, such as client images and client profiles, can be found at [Client Settings](#).)

Access Interfaces

Enable Cisco AnyConnect VPN Client or legacy SSL VPN Client access on the interfaces selected in the table below

Interface	Allow Access	Enable DTLS
outside	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
inside	<input type="checkbox"/>	<input type="checkbox"/>

Access Port: 443 DTLS Port: 443

Click here to [Assign Certificate to Interface](#).

Login Page Setting

Allow user to select connection profile, identified by its alias, on the login page. Otherwise, DefaultWebVPNGroup will be the connection profile.

Connection Profiles

Connection profile (tunnel group) specifies how user is authenticated and other parameters.

[Add](#) [Edit](#) [Delete](#)

Name	Enabled	Aliases	Authentication Method
certenroll	<input checked="" type="checkbox"/>	certenroll	AAA(LOCAL)
Sales	<input checked="" type="checkbox"/>	Sales	AAA(LOCAL)
DefaultRAGroup	<input checked="" type="checkbox"/>		AAA(LOCAL)
certauth	<input checked="" type="checkbox"/>	certauth	Certificate
DefaultWEBVPNGroup	<input checked="" type="checkbox"/>	default	AAA(LOCAL)

Test AnyConnect SCEP

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Lancez le client d'AnyConnect, et connectez au profil de



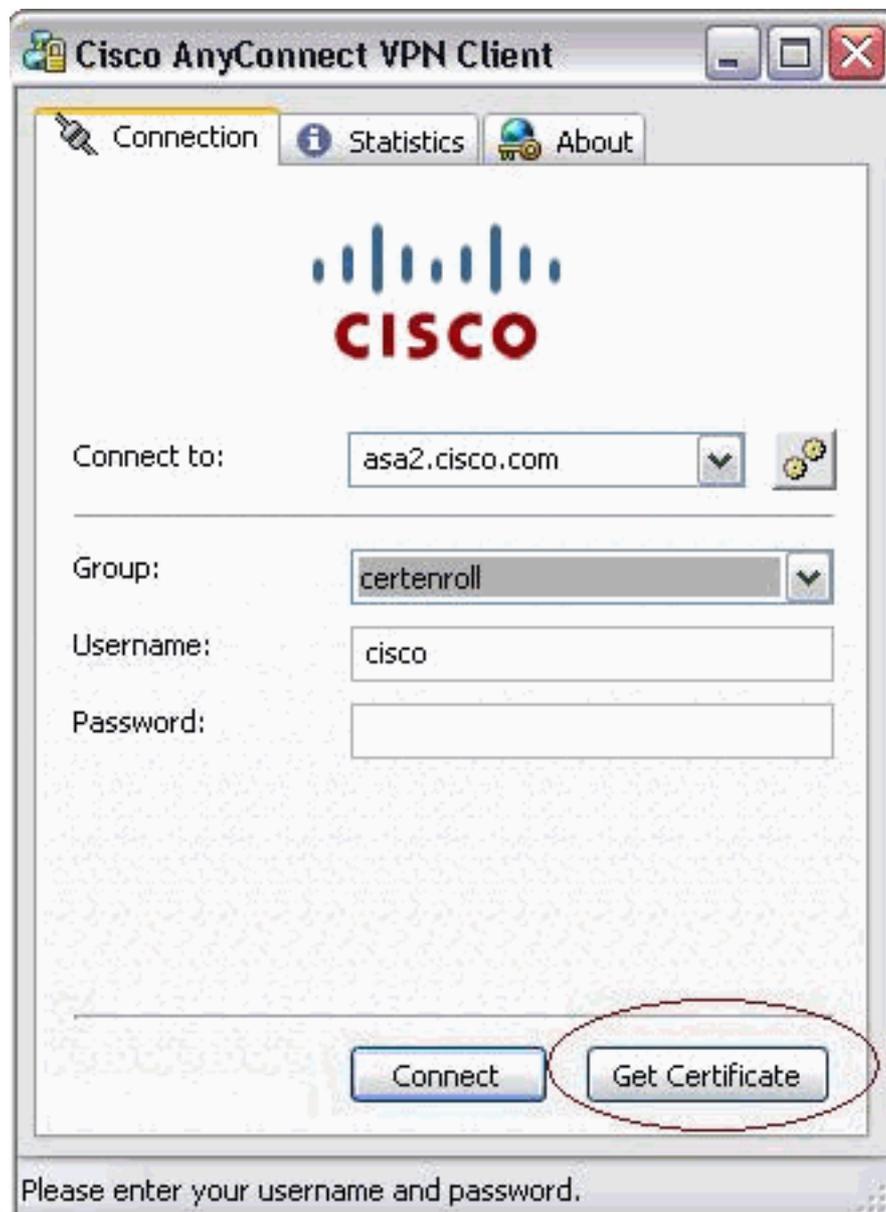
certenroll.

la demande d'inscription au serveur CA par

AnyConnect passe

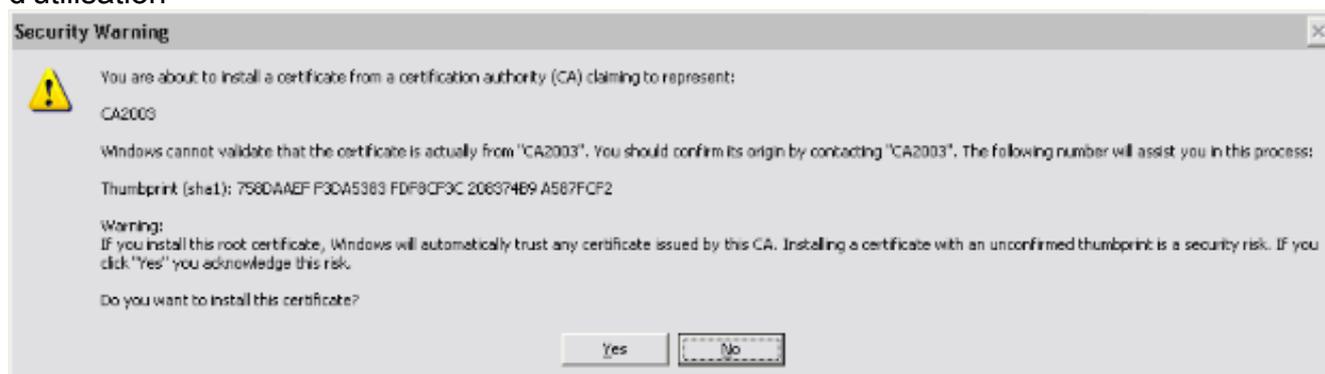


SCEP. Certificate Enrollment - Request forwarded. AnyConnect passe la demande d'inscription directement et ne passe pas par le tunnel, si le bouton de certificat



d'obtenir est utilisé.

2. Cet avertissement apparaît. Cliquez sur **oui** pour installer l'utilisateur et le certificat racine d'utilisation

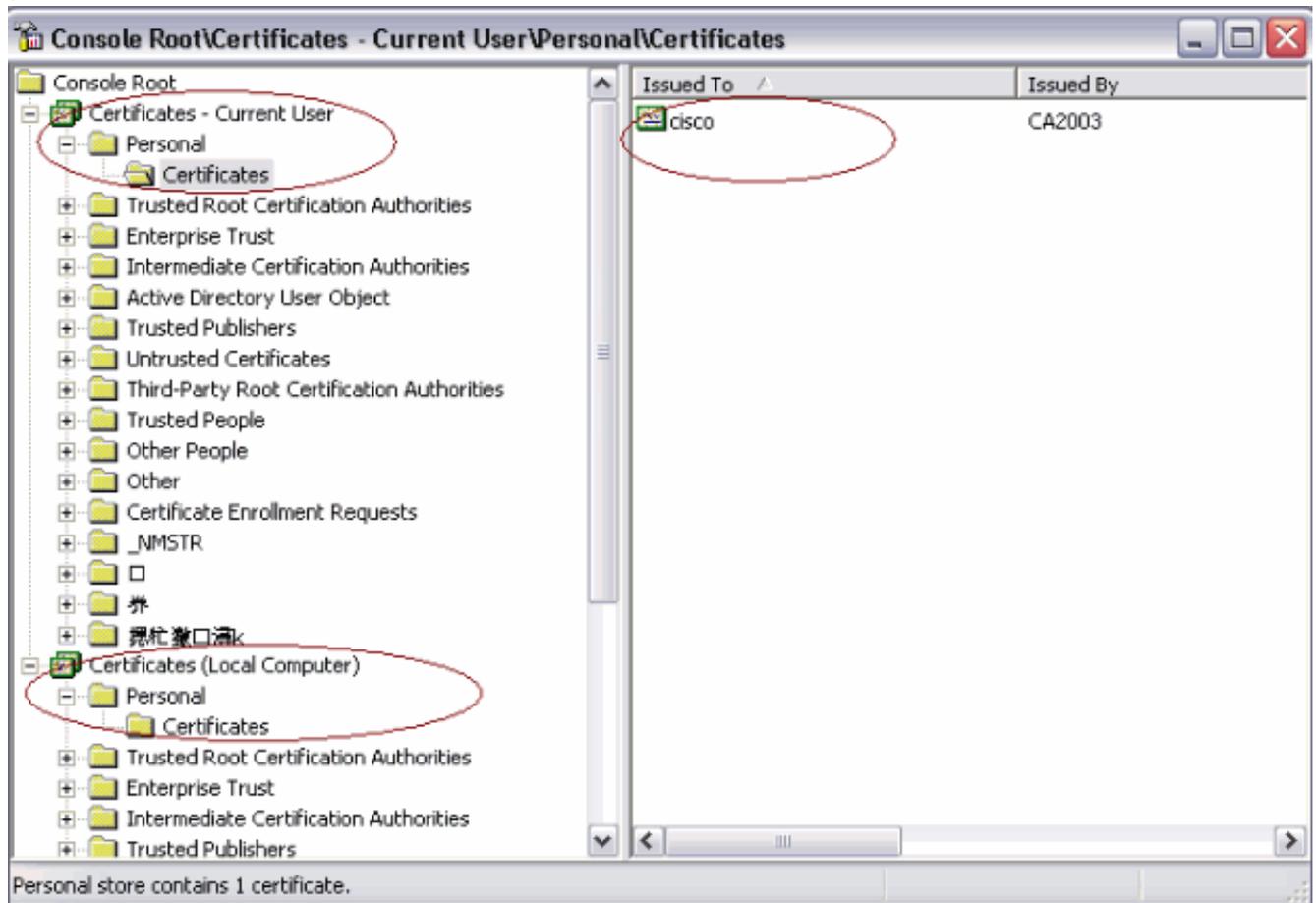


3. Une fois le certificat est inscrit, se connecte au profil de **certauth**.

[Mémoire de certificat sur Microsoft Windows après demande SCEP](#)

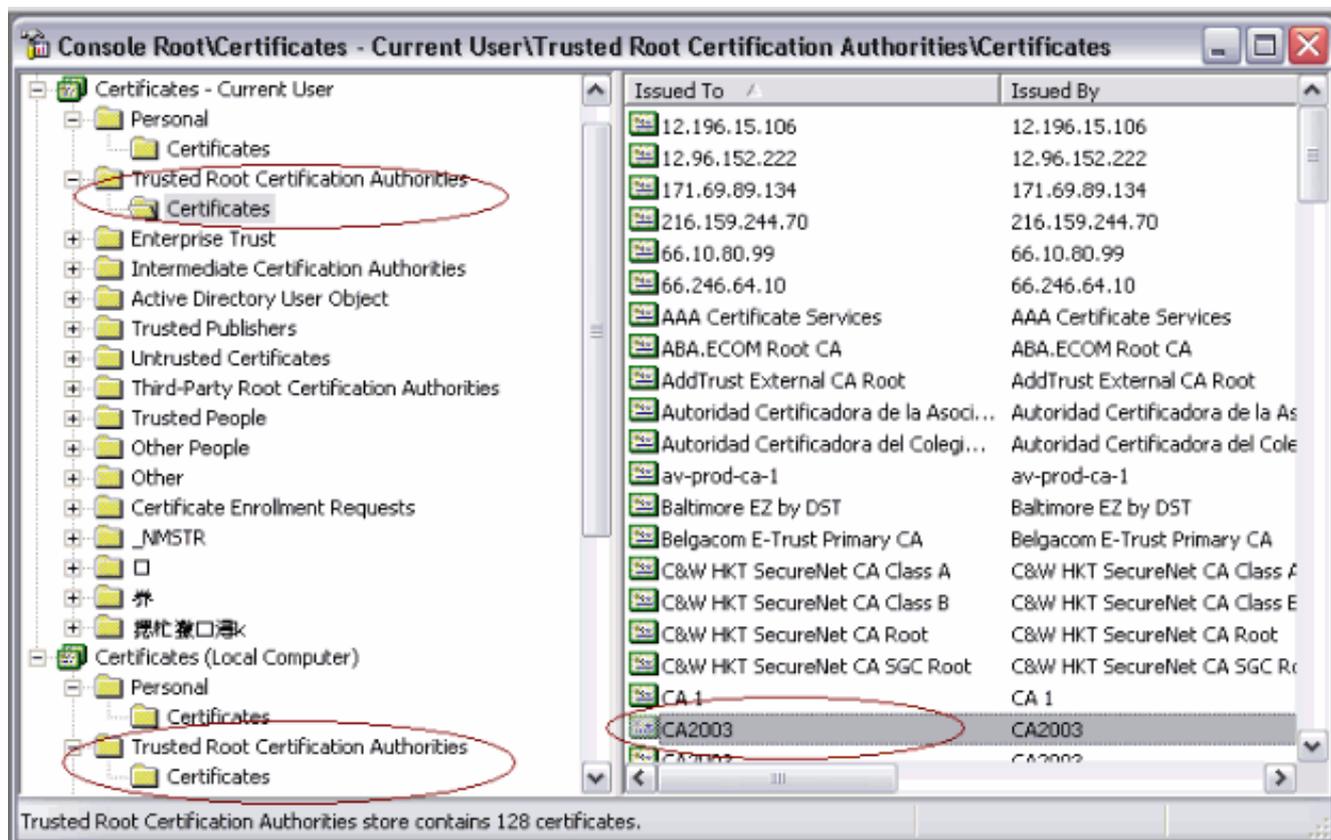
Procédez comme suit :

1. Début de clic > exécuté > MMC.
2. Cliquez sur Add/retirez le SNAP dedans.
3. Cliquez sur Add, et choisissez les **Certificats**.
4. Ajoutez les **mes** Certificats de **compte utilisateur** et de **compte d'ordinateur**. Cette image affiche le certificat utilisateur installé dans la mémoire de certificat de Windows



Cette image affiche le certificat de CA installé dans la mémoire de certificat de Windows

:



Dépannez

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

- L'inscription d'AnyConnect SCEP fonctionne seulement quand l'authentification de certificat échoue. S'il ne s'inscrit pas, vérifiez la mémoire de certificat. Si des Certificats sont déjà installés, supprimez-les et testez de nouveau.
- L'inscription SCEP ne fonctionne pas à moins que la commande **extérieure du port 443 d'interface de certificat-authentification SSL** soit utilisée. Référez-vous à ces pour en savoir plus d'id de bogue Cisco : L'ID de bogue Cisco [CSCtf06778](#) (clients [enregistrés](#) seulement) — AnyConnect SCEP s'inscrivent ne fonctionne pas avec par le CERT 2 authentiques de groupe Inscription de l'ID de bogue Cisco [CSCtf06844](#) (clients [enregistrés](#) seulement) — AnyConnect SCEP ne fonctionnant pas avec l'ASA par CERT de groupe authentique
- Si le serveur CA est sur l'extérieur de l'ASA, veuillez à permettre cheveu-goupiller avec la commande **intra-interface d'autorisation du même-Sécurité-traffic**. Ajoutez également l'extérieur et les commandes access-list nat suivant les indications de cet exemple :


```

nat
(outside) 1

```

access-list natoutside extended permit ip 172.16.1.0 255.255.255.0 host 171.69.89.87 Là où 172.16.1.0 est le groupe et 171.69.89.87 d'AnyConnect est l'adresse IP du serveur CA.

- Si le serveur CA est sur l'intérieur, veuillez à l'inclure dans la liste d'accès de tunnel partagé pour la stratégie de groupe de **certenroll**. Dans ce document, on le suppose que le serveur CA est sur l'intérieur.


```

group-policy certenroll attributes
split-tunnel-policy tunnelspecified
split-tunnel-network-list value scep

```

access-list scep standard permit 171.69.89.0 255.255.255.0

Informations connexes

- [Guide de l'administrateur de Cisco AnyConnect VPN Client, version 2.4](#)
- [Support et documentation techniques - Cisco Systems](#)