# Configurer un serveur AAA externe pour le VPN



# À propos des serveurs AAA externes

Cet ASA peut être configuré pour utiliser un serveur LDAP, RADIUS ou TACACS+ externe afin de prendre en charge l'authentification, l'autorisation et la comptabilité (AAA) pour l'ASA. Le serveur AAA externe applique les autorisations et les attributs configurés. Avant de configurer l'ASA pour utiliser un serveur externe, vous devez configurer le serveur AAA externe avec les attributs d'autorisation ASA appropriés et, à partir d'un sous-ensemble de ces attributs, affecter des autorisations spécifiques aux utilisateurs individuels.

## Comprendre l'application des politiques aux attributs d'autorisation

L'ASA prend en charge plusieurs méthodes d'application des attributs d'autorisation d'utilisateur, également appelés droits ou autorisations d'utilisateur, aux connexions VPN. Vous pouvez configurer l'ASA pour obtenir les attributs utilisateur de n'importe quelle combinaison de :

- une politique d'accès dynamique (DAP) sur l'ASA
- un serveur d'authentification et/ou d'autorisation RADIUS ou LDAP externe
- une stratégie de groupe sur l'ASA

Si l'ASA reçoit des attributs de toutes les sources, les attributs sont évalués, fusionnés et appliqués à la politique d'utilisateur. En cas de conflit entre les attributs, les attributs du DAP prévalent.

L'ASA applique les attributs dans l'ordre suivant :

1. Attributs DAP sur l'ASA : introduits dans la version 8.0(2), ces attributs prévalent sur tous les autres. Si vous définissez un signet ou une liste d'URL dans DAP, il remplace un signet ou une liste d'URL défini dans la politique de groupe.
2. Attributs de l'utilisateur sur le serveur AAA externe : le serveur renvoie ces attributs une fois l'authentification ou l'autorisation de l'utilisateur réussie. Ne les confondez pas avec les attributs définis pour les utilisateurs individuels dans la base de données AAA locale sur l'ASA (comptes d'utilisateurs dans ASDM).

3. *Stratégie de groupe configurée sur l'ASA* : si un serveur RADIUS renvoie la valeur de l'attribut de classe RADIUS IETF-Class-25 (OU = group-policy) pour l'utilisateur, l'ASA place l'utilisateur dans la stratégie de groupe du même nom et applique les attributs de la stratégie de groupe qui ne sont pas renvoyés par le serveur.

   Pour les serveurs LDAP, n'importe quel nom d'attribut peut être utilisé pour définir la stratégie de groupe pour la session. La carte d'attributs LDAP que vous configurez sur l'ASA associe l'attribut LDAP à l'attribut Cisco IETF-Radius-Class.

4. Stratégies de groupe affectées par le profil de connexion (également appelé groupes de tunnels) : le profil de connexion contient les paramètres préliminaires pour la connexion et comprend une stratégie de groupe par défaut appliquée à l'utilisateur avant l'authentification. Tous les utilisateurs se connectant à l'ASA appartiennent initialement à ce groupe, qui fournit tous les attributs manquants dans les attributs d'utilisateur renvoyés par le serveur AAA ou dans la stratégie de groupe affectée à l'utilisateur.

5. Stratégie de groupe par défaut affectée par l'ASA (DfltGrpPolicy) : les attributs par défaut du système fournissent les valeurs manquantes dans le DAP, les attributs d'utilisateur, la stratégie de groupe ou le profil de connexion.

# Lignes directrices relatives à l'utilisation de serveurs AAA externes

Les ASA appliquent les attributs LDAP en fonction du nom de l'attribut, et non de l'ID numérique. Les attributs RADIUS sont appliqués par ID numérique, et non par nom.

Pour ASDM version 7.0, les attributs LDAP comprennent le préfixe cVPN3000. Pour les versions 7.1 et ultérieures d'ASDM, ce préfixe a été supprimé.

Les attributs LDAP sont un sous-ensemble des attributs Radius, qui sont répertoriés dans le chapitre Radius.

# Configurer l'authentification de plusieurs certificats

Vous pouvez désormais valider plusieurs certificats par session au moyen des protocoles client Secure Client SSL et IKEv2. Par exemple, vous pouvez vous assurer que le nom d'émetteur du certificat de machine correspond à une autorité de certification particulière et, par conséquent, que le périphérique est un périphérique émis par l'entreprise.

L'option de certificats multiples permet l'authentification de certificat de la machine et de l'utilisateur au moyen de certificats. Sans cette option, vous ne pourriez authentifier par certificat que la machine ou l'utilisateur, mais pas les deux.

**Remarque** Étant donné que l'authentification par certificats multiples nécessite un certificat d'ordinateur et un certificat utilisateur (ou deux certificats utilisateur), vous ne pouvez pas utiliser le démarrage Secure Client avant la connexion (SBL) avec cette fonctionnalité.

L'option de préremplissage du nom d'utilisateur permet à un champ du deuxième certificat (utilisateur) d'être analysé et utilisé pour l'authentification AAA ultérieure dans une connexion authentifiée par AAA et certificat.

Le nom d'utilisateur, pour le préremplissage principal comme secondaire, est toujours extrait du deuxième certificat (utilisateur) reçu du client.

À partir de la version 9.14(1), l'ASA vous permet de spécifier de quel certificat les noms d'utilisateur principal et secondaire doivent provenir lors de la configuration de l'authentification par certificats multiples et de l'utilisation de l'option de préremplissage du nom d'utilisateur pour l'authentification ou l'autorisation. Pour plus de renseignements, consultez Profil de connexion Secure Client, attributs d'authentification

Avec l'authentification par certificats multiples, deux certificats sont authentifiés : le deuxième certificat (utilisateur) reçu du client est celui à partir duquel les noms d'utilisateurs principaux et secondaires sont analysés.

Vous pouvez également configurer l'authentification par certificats multiples avec SAML.

Avec l'authentification à certificats multiples, vous pouvez prendre des décisions de politique en fonction des champs d'un certificat utilisé pour authentifier cette tentative de connexion. Les certificats utilisateur et machine reçus du client lors de l'authentification à certificats multiples sont chargés dans DAP afin de permettre la configuration de politiques fondées sur les champs du certificat. Pour ajouter l'authentification par certificats multiples à l'aide des Dynamic Access Policies (DAP) afin de pouvoir définir des règles pour autoriser ou refuser les tentatives de connexion, consultez la section *Ajouter plusieurs certificats d'authentification à DAP* dans la version appropriée du Guide de configuration ASDM du VPN ASA.

# Exemples d'autorisation d'accès à distance Active Directory/LDAP

Cette section présente des exemples de procédures pour configurer l'authentification et l'autorisation sur l'ASA à l'aide du serveur Microsoft Active Directory. Elle comprend les rubriques suivantes:


- Application de la politique aux attributs basés sur l'utilisateur, à la page 3
- Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client , à la page 5
- Appliquer l'autorisation ou le refus d'accès entrant, à la page 7
- Appliquer les règles d'heures de connexion et d'heure du jour, à la page 9


D'autres exemples de configuration disponibles sur Cisco.com comprennent les notes techniques suivantes.

- ASA/PIX : exemple de mappage des clients VPN aux stratégies de groupe de VPN à l'aide de la configuration LDAP
- PIX/ASA 8.0 : utiliser l'authentification LDAP pour affecter une stratégie de groupe à la connexion

## Application de la politique aux attributs basés sur l'utilisateur

Cet exemple affiche une bannière simple à l'utilisateur, indiquant comment vous pouvez mapper n'importe quel attribut LDAP standard à un attribut spécifique au fournisseur (VSA) bien connu, et vous pouvez mapper un ou plusieurs attributs LDAP à un ou plusieurs attributs LDAP de Cisco. Il s'applique à tout type de connexion, y compris le client VPN IPsec et Secure Client.

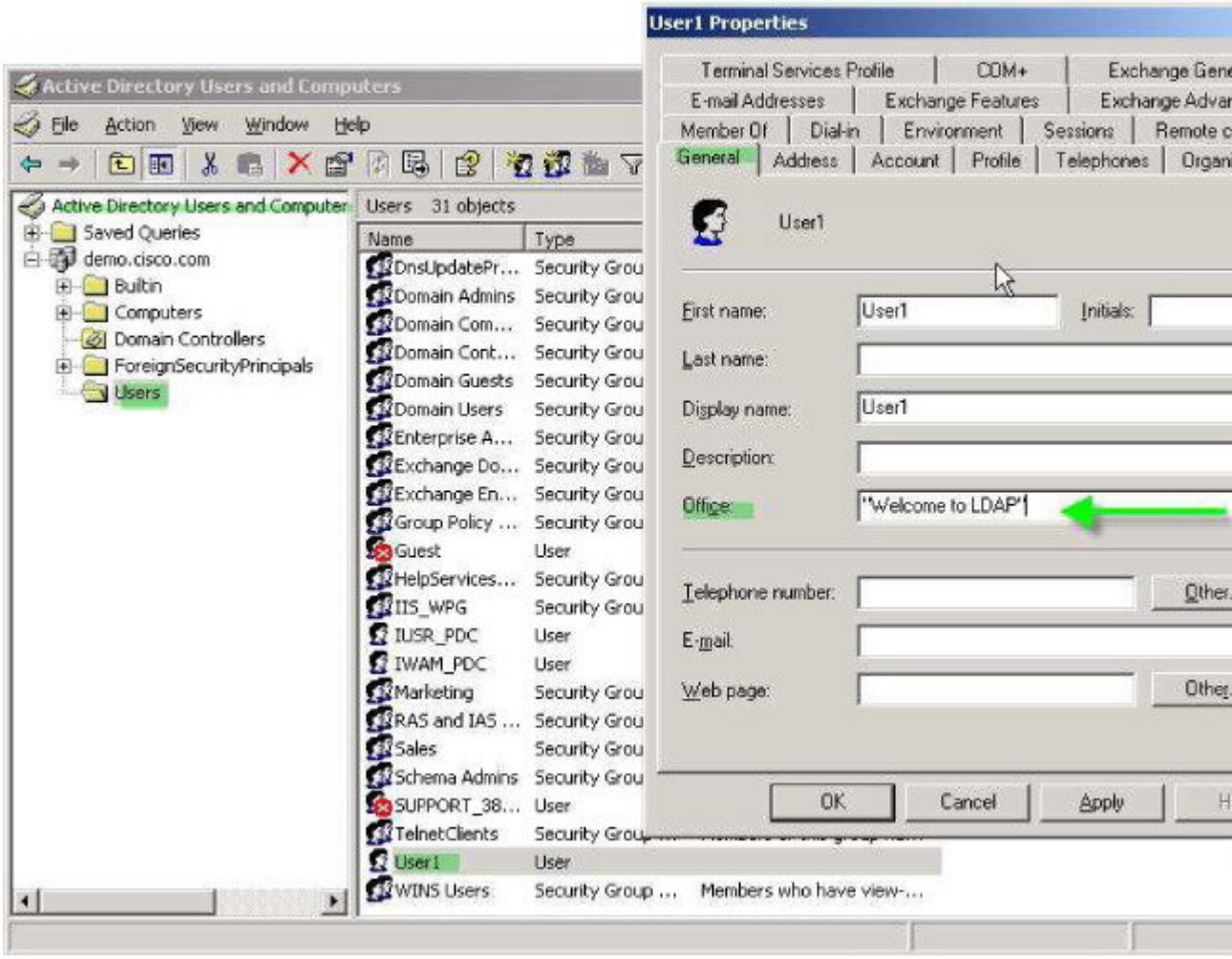
Pour appliquer une bannière simple à un utilisateur configuré sur un serveur LDAP AD, utilisez le champ Office sous l'onglet General (Général) pour saisir le texte de la bannière. Ce champ utilise l'attribut nommé

PhysicalDeliveryOfficeName. Sur l'ASA, créez une carte d'attributs qui associe physicalDeliveryOfficeName à l'attribut Cisco Banner1.

Lors de l'authentification, l'ASA récupère la valeur de physicalDeliveryOfficeName du serveur, associe la valeur à l'attribut Cisco Banner1 et affiche la bannière à l'utilisateur.

### Procédure

**Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Propriétés puis l'onglet **General** (Général) et saisissez le texte de la bannière dans le champ Office (Bureau), qui utilise l'attribut AD/LDAP physicalDeliveryOfficeName.




**Étape 2** Créez une correspondance d'attributs LDAP sur l'ASA.

Créez la carte Bannière et faites correspondre l'attribut AD/LDAP PhysicalDeliveryOfficeName à l'attribut Cisco Bannière1 :

```
hostname(config)# ldap attribute-map Banner
```

```
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

**Étape 3** Associez la carte d'attributs LDAP au serveur AAA.

Passez en mode de configuration d'hôte de serveur aaa pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP et associez la bannière de carte d'attributs que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

**Étape 4** Testez l'application de la bannière.

# Appliquer l'affectation d'adresse IP statique pour les tunnels Secure Client

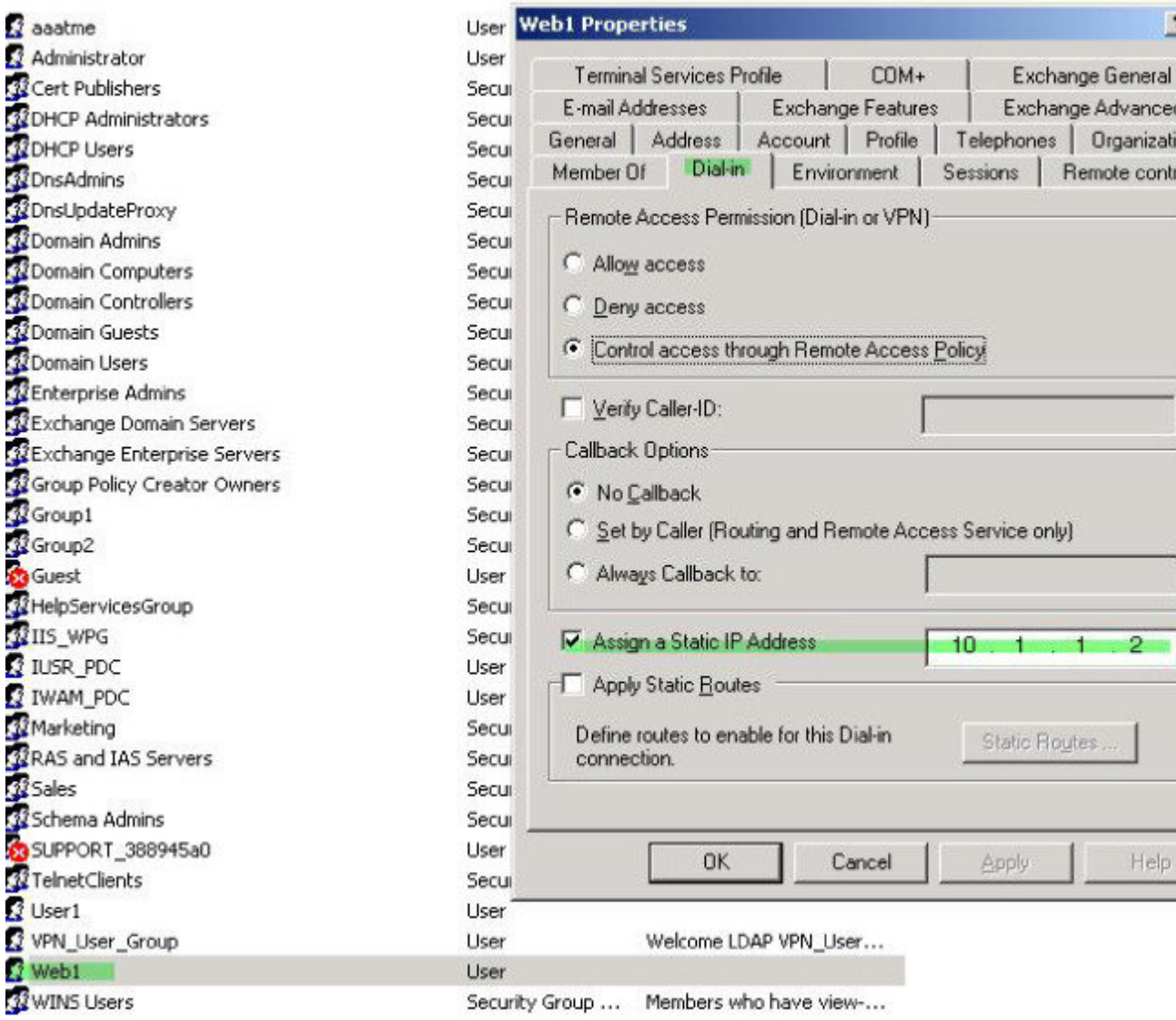
Cet exemple s'applique aux clients de tunnel complet, tels que le client IPsec et les clients VPN SSL.

Pour appliquer les affectations d'adresses IP statiques Secure Client, configurez l'utilisateur Web1 Secure Client pour qu'il reçoive une adresse IP statique, saisissez l'adresse dans le champ Assign Static IP Address (affecter une adresse IP statique) de l'onglet Dial-in (Accès distant) sur le serveur LDAP AD (ce champ utilise l'attribut msRADIUSFramedIPAddress), puis créez une carte d'attributs qui mappe cet attribut à l'attribut Cisco IETF-Radius-Framed-IP-Address.

Lors de l'authentification, l'ASA récupère la valeur de msRADIUSFramedIPAddress du serveur, la mappe à l'attribut Cisco IETF-Radius-Framed-IP-Address et fournit l'adresse statique à Web1.

### Procédure

**Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue Properties (Propriétés), puis l'onglet **Dial-in** (Accès distant), cochez la case **Assign Static IP Address** (affecter une adresse IP statique) et saisissez l'adresse IP 10.1.1.2.




**Étape 2** Créez une mise en correspondance d'attributs pour la configuration LDAP affichée.

Mappez l'attribut AD msRADIUSFramedIPAddress utilisé par le champ d'adresse statique avec l'attribut Cisco IETF-Radius-Framed-IP-Address :

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

**Étape 3** Associez la carte d'attributs LDAP au serveur AAA.

Entrez en mode de configuration d'hôte de serveur AAA pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP, puis associez la carte d'attributs static_address que vous avez créée précédemment :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

```
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

**Étape 4** Vérifiez que la commande **vpn-address-assignment** est configurée pour spécifier AAA en affichant cette partie de la configuration :

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

**Étape 5** Établissez une connexion à l'ASA avec Secure Client. Observez que l'utilisateur reçoit l'adresse IP configurée sur le serveur et mappée à l'ASA.

**Étape 6** Utilisez la commande **show vpn-sessiondb svc** pour afficher les détails de la session et vérifier l'adresse affectée :

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

# Appliquer l'autorisation ou le refus d'accès entrant

Cet exemple crée une mise en correspondance d'attributs LDAP qui précise les protocoles de tunnellisation autorisés par l'utilisateur. Vous associez les paramètres d'autorisation d'accès et de refus d'accès de l'onglet Dial-in à l'attribut Cisco Tunneling-Protocol, qui prend en charge les valeurs de bitmap suivantes :

| Valeur | Protocole de tunnellisation |
|---|---|
| 1 | PPTP |
| 2 | L2TP |
| 4 | IPsec (IKEv1) |
| 8 | L2TP/IPsec |
| 16 | SSL sans client |
| 32 | Client SSL—Secure Client ou client VPN SSL |
| 64 | IPsec (IKEv2) |

[1] (1) IPsec et L2TP sur IPsec ne sont pas pris en charge simultanément. Par conséquent, les valeurs 4 et 8 s'excluent mutuellement.
[2] (2) Voir note 1.

Utilisez cet attribut pour créer une condition Allow Access (TRUE) ou Deny Access (FALSE) pour les protocoles et appliquer la méthode pour laquelle l'utilisateur est autorisé à accéder.

Consultez la note technique ASA/PIX : Mappage des clients VPN avec les stratégies de groupe VPN à l'aide de l'exemple de configuration LDAP pour obtenir un autre exemple d'application de l'autorisation d'accès par numérotation ou de refus d'accès.

### Procédure

**Étape 1** Cliquez avec le bouton droit sur le nom d'utilisateur, ouvrez la boîte de dialogue des propriétés, puis l'onglet **Dial-in**, et cliquez sur le bouton radio Allow Access (autoriser l'accès).


**Remarque**
Si vous choisissez l'option Contrôle de l'accès par la stratégie d'accès à distance, aucune valeur n'est renvoyée par le serveur et les autorisations appliquées sont basées sur les paramètres de stratégie de groupe internes de l'ASA.

**Étape 2** Créez une mise en correspondance d'attributs pour autoriser une connexion IPsec et Secure Client, mais refuser une connexion SSL sans client.

a) Créez la carte tunneling_protocols :

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Mappez l'attribut AD msNPAllowDialin utilisé par le paramètre Allow Access (autoriser l'accès) avec l'attribut Cisco Tunneling-Protocols (protocoles de tunnellisation) :

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Ajoutez des valeurs de carte :

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

**Étape 3** Associez la carte d'attributs au serveur AAA.

a) Passez en mode de configuration d'hôte de serveur aaa pour l'hôte 10.1.1.2 dans le groupe de serveurs AAA MS_LDAP :

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associez la carte d'attributs tunneling_protocols que vous avez créée :

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

**Étape 4** Vérifiez que la carte d'attributs fonctionne comme configurée.

Essayez les connexions à l'aide du protocole SSL sans client, l'utilisateur doit être informé qu'un mécanisme de connexion non autorisée est la raison de l'échec de la connexion. Le client IPsec doit se connecter, car IPsec est un protocole de tunnellisation autorisé en fonction de la carte d'attributs.

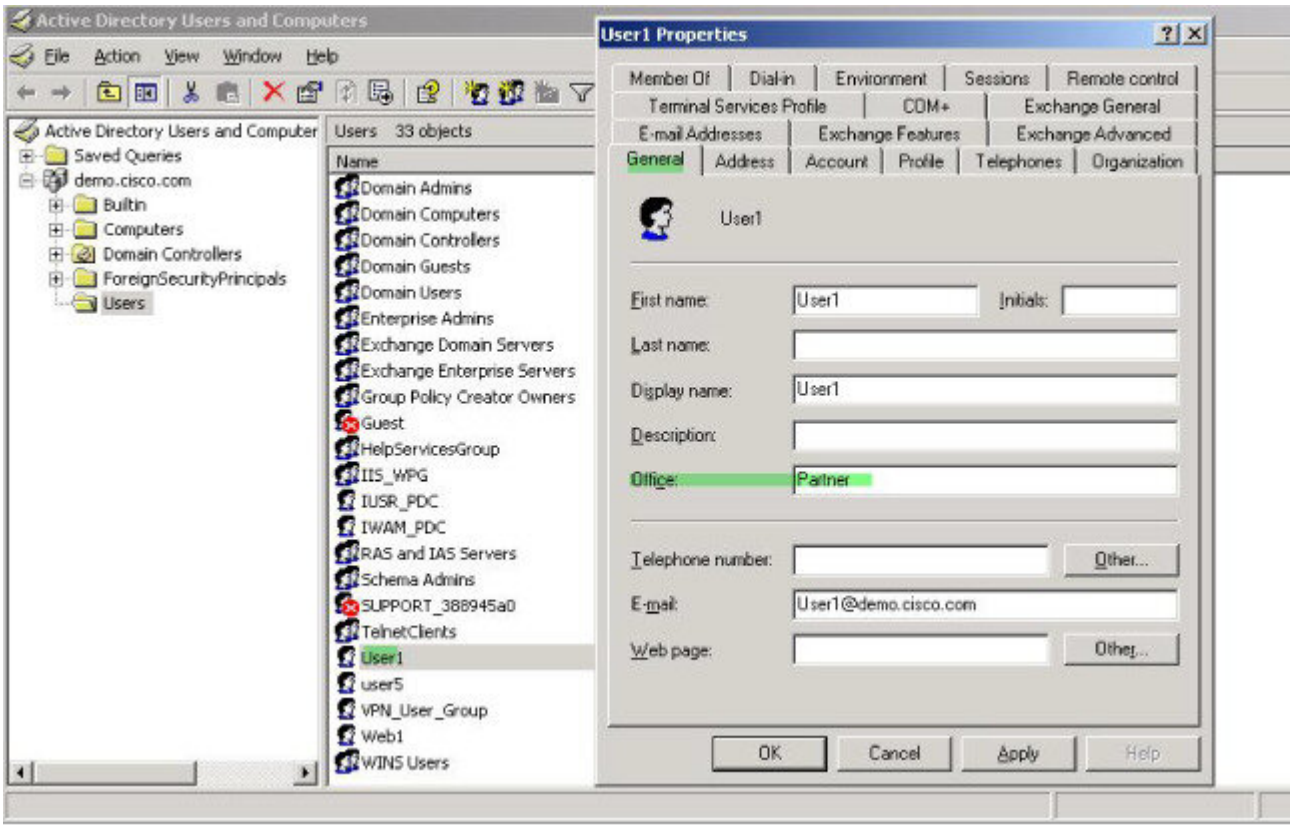
# Appliquer les règles d'heures de connexion et d'heure du jour

L'exemple suivant montre comment configurer et appliquer les heures pendant lesquelles un utilisateur SSL sans client (comme un partenaire commercial) est autorisé à accéder au réseau.

Sur le serveur AD, utilisez le champ Office (Bureau) pour saisir le nom du partenaire, qui utilise l'attribut physicalDeliveryOfficeName. Nous créons ensuite une carte d'attributs sur l'ASA pour faire correspondre cet attribut à l'attribut Cisco Access-Hours. Lors de l'authentification, l'ASA récupère la valeur de physicalDeliveryOfficeName et l'associe à Access-Hours.

### Procédure

**Étape 1** Sélectionnez l'utilisateur, cliquez avec le bouton droit sur **Properties (Propriétés)** puis ouvrez l'onglet **General** (Général) :




**Étape 2** Créez une carte d'attributs.

Créez la carte d'attributs access_hours et faites correspondre l'attribut AD physicalDeliveryOfficeName utilisé par le champ Office à l'attribut Cisco Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

**Étape 3** Associez la carte d'attributs LDAP au serveur AAA.

Entrez dans le mode de configuration de l'hôte du serveur aaa pour l'hôte 10.1.1.2 du groupe de serveurs AAA MS_LDAP et associez la carte d'attributs access_hours que vous avez créée.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

**Étape 4** Configurez les plages de temps pour chaque valeur autorisée sur le serveur.

Configurez les heures d'accès du partenaire de 9 h à 17 h du lundi au vendredi :

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```

À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d’incohérence, la version anglaise du présent contenu prévaudra.