



# VPN の外部 AAA サーバーの設定

- 外部 AAA サーバーについて (1 ページ)
- 外部 AAA サーバーを使用する際のガイドライン (2 ページ)
- 複数証明書認証の設定 (2 ページ)
- VPN の LDAP 許可の設定 (4 ページ)
- Active Directory/LDAP VPN リモート アクセス許可の例 (20 ページ)

## 外部 AAA サーバーについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバーを使用して、ASA の認証、認可、アカウンティング (AAA) をサポートするように設定できます。外部 AAA サーバーは、設定されたアクセス許可と属性を適用します。外部サーバーを使用するように ASA を設定する前に、適切な ASA 許可属性を指定して外部 AAA サーバーを設定し、それらの属性のサブセットから特定のアクセス許可を個々のユーザーに割り当てる必要があります。

## 許可属性のポリシー適用の概要

ASA は、ユーザー認可属性（ユーザー権利またはユーザー権限とも呼ばれる）を VPN 接続に適用するためのいくつかの方法をサポートしています。ASA を設定して、次のいずれかの組み合わせからユーザー属性を取得できます。

- ASA のダイナミック アクセス ポリシー (DAP)
- 外部 RADIUS または LDAP 認証および許可サーバー（およびその両方）
- ASA のグループ ポリシー

ASA がすべてのソースから属性を受信すると、それらの属性は評価されて集約され、ユーザー ポリシーに適用されます。属性の間で衝突がある場合、DAP 属性が優先されます。

ASA は次の順序で属性を適用します。

1. ASA 上の DAP 属性：バージョン 8.0(2) で導入されたこの属性は、他のどの属性よりも優先されます。DAP 内でブックマークまたは URL リストを設定した場合は、グループ ポリシーで設定されているブックマークや URL リストよりも優先されます。

## ■ 外部 AAA サーバーを使用する際のガイドライン

2. AAA サーバー上のユーザー属性：ユーザー認証や認可が成功すると、サーバーからこの属性が返されます。これらの属性を、ASA のローカル AAA データベースで個々のユーザーに設定されている属性 (ASDM のユーザー アカウント) と混同しないようにしてください。
3. ASA で設定されているグループポリシー：RADIUS サーバーからユーザーに対して RADIUS CLASS 属性 IETF-Class-25 (*OU=group-policy*) の値が返された場合、ASA はそのユーザーと同じ名前のグループポリシーに配置し、そのグループポリシーの属性のうち、サーバーから返されないものを適用します。  
LDAP サーバーでは、任意の属性名を使用してセッションのグループポリシーを設定できます。ASA 上に設定された LDAP 属性マップによって、LDAP 属性が Cisco 属性 IETF-Radius-Class にマッピングされます。
4. 接続プロファイル (CLI では「トンネルグループ」と呼ばれます) によって割り当てられたグループポリシー：接続プロファイルには、接続の事前設定が含まれているほか、認証前にユーザーに適用されるデフォルトのグループポリシーが含まれています。ASA に接続しているすべてのユーザーは、最初にこのグループに所属します。このグループで、DAP、サーバーから返されるユーザー属性、ユーザーに割り当てられているグループポリシーにはない属性が提供されます。
5. ASA で割り当てられたデフォルトのグループポリシー (DfltGrpPolicy)：システムのデフォルト属性は、DAP、ユーザー属性、グループポリシー、接続プロファイルで不足している値を提供します。

## 外部 AAA サーバーを使用する際のガイドライン

ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。RADIUS 属性は、名前ではなく数値 ID によって適用されます。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ASDM バージョン 7.1 以降では、このプレフィックスは削除されています。

LDAP 属性は、RADIUS の章に記載されている RADIUS 属性のサブセットです。

## 複数証明書認証の設定

セキュアクライアント SSL クライアントプロトコルと IKEv2 クライアントプロトコルを使用して、セッションごとに複数の認証を検証できるようになりました。たとえば、マシン証明書の発行元が特定の CA と一致することでデバイスが企業から支給されたデバイスであることを確認できます。

複数証明書オプションを使用すると、証明書を通じたマシンとユーザー両方の証明書認証が可能になります。このオプションがなければ、両方ではなく一方のみの証明書認証しか行うことができません。



(注) 複数の証明書認証にはマシン証明書とユーザー証明書（または2つのユーザー証明書）が必要であるため、この機能ではセキュアクライアント Start Before Logon (SBL) を使用できません。

ユーザー名の事前入力フィールドでは、2つ目の（ユーザー）証明書のフィールドを解析し、AAA および証明書認証済みの接続で以降の AAA 認証に使用することができます。プライマリとセカンダリの両方の事前入力のユーザー名は、常にクライアントから受信した2つ目の（ユーザー）証明書から取得されます。

9.14(1) 以降、ASA では、複数証明書認証を設定し、認証または許可にユーザー名の事前入力オプションを使用する場合に、プライマリユーザー名およびセカンダリユーザー名を取得する証明書を指定できます。詳細については、[複数証明書ユーザー名の設定 \(3 ページ\)](#) を参照してください。

複数証明書認証では、2つの証明書が認証されます。クライアントから受信した2つ目の（ユーザー）証明書は、事前入力および証明書由来のユーザー名のプライマリおよびセカンダリユーザー名による解析対象です。

SAML による複数証明書認証も設定できます。

既存の認証 webvpn 属性は、複数証明書認証のオプションを含めるように変更されます。

```
tunnel-group <name> webvpn-attributes
authentication {aaa [certificate | multiple-certificate] | multiple-certificate [aaa | saml] | saml [certificate | multiple-certificate]}
```

複数証明書認証では、その接続試行を認証するために使用された証明書のフィールドに基づいてポリシー決定を行うことができます。複数証明書認証中にクライアントから受信したユーザーおよびマシンの証明書は DAP にロードされ、証明書のフィールドに基づいてポリシーを設定することができます。接続試行を許可または拒否するルールを設定できるようにダイナミック アクセス ポリシー (DAP) を使用して複数証明書認証を追加するには、『[ASA VPN ASDM Configuration Guide](#)』の適切なリリースの「Add Multiple Certificate Authentication to DAP」を参照してください。

## 複数証明書ユーザー名の設定

ASA 9.14(1) では、認証または許可のプライマリユーザー名およびセカンダリユーザー名として ASA で使用する必要がある証明書を設定するための新しいコマンドが導入されました。認証または許可パラメータを取得するために、SSL または IKE で送信されたマシン証明書（1つの証明書）を使用するか、クライアントからのユーザー証明書（2つの証明書）を使用するかを指定できます。このオプションは、認証タイプ (**aaa**、**certificate**、または **multiple-certificate**) に関係なく、任意のトンネルグループに使用および設定できます。ただし、構成は、複数証明書認証 (**multiple-certificate** または **aaa multiple-certificate**) に対してのみ有効となります。このオプションが複数証明書認証に使用されない場合は、2つ目の証明書がデフォルトとして認証または許可に使用されます。

## 手順

---

**ステップ1** 1つ目の証明書と2つ目の証明書のどちらのプライマリユーザー名を使用するかを指定します。

**username-from-certificate-choice {first-certificate | second-certificate}**

**ステップ2** 1つ目の証明書と2つ目の証明書のどちらのセカンダリユーザー名を使用するかを指定します。

**secondary-username-from-certificate-choice {first-certificate | second-certificate}**

例 :

```
tunnel-group tgl webvpn-attributes
authentication aaa multiple-certificate
pre-fill-username client
secondary-pre-fill-username client
tunnel-group tgl type remote-access
tunnel-group tgl general-attributes
secondary-authentication-server-group LOCAL
username-from-certificate-choice first-certificate
secondary-username-from-certificate-choice first-certificate
```

---

## VPN の LDAP 許可の設定

VPN アクセスのための LDAP 認証が成功すると、ASA は LDAP 属性を返す LDAP サーバーに 対してクエリーを実行します。通常これらの属性には、VPN セッションに適用される認可データが含まれます。

この許可メカニズムとは別の異なる許可を LDAP ディレクトリ サーバーから取得することが 必要な場合があります。たとえば、認証に SDI または証明書サーバーを使用している場合、認可情報は返されません。この場合、ユーザー認可では、認証の成功後に LDAP ディレクトリの クエリーを実行するため、認証と認可は 2 つのステップで行われます。

LDAP を使用した VPN ユーザー許可を設定するには、次の手順を実行します。

## 手順

---

**ステップ1** AAA サーバー グループを作成します。

**aaa-server server\_group protocol {kerberos | ldap | nt | radius | sdi | tacacs+}**

例 :

```
hostname(config)# aaa-server servergroup1 protocol ldap
hostname(config-aaa-server-group)
```

**ステップ2** remotegrp という名前の IPsec リモート アクセス トンネル グループを作成します。

**tunnel-group groupname**

例：

```
hostname(config)# tunnel-group remotegrp
```

**ステップ3** サーバー グループと トンネル グループを関連付けます。

**tunnel-group groupname general-attributes**

例：

```
hostname(config)# tunnel-group remotegrp general-attributes
```

**ステップ4** 以前作成した認証のための AAA サーバー グループに新しい トンネル グループを割り当てます。

**authorization-server-group group-tag**

例：

```
hostname(config-general)# authorization-server-group ldap_dir_1
```

---

### 例

次に、LDAP を使用したユーザー許可を有効にするコマンドの例を示します。この例では、RAVPN という名前の IPsec リモート アクセス トンネル グループを作成し、すでに作成してある許可用の LDAP AAA サーバー グループにその新しい トンネル グループを割り当てています。

```
hostname(config)# tunnel-group RAVPN type remote-access
hostname(config)# tunnel-group RAVPN general-attributes
hostname(config-general)# authorization-server-group (inside) LDAP
hostname(config-general)#
```

この設定が完了したら、次のコマンドを入力して、ディレクトリ パスワード、ディレクトリ 検索の開始点、ディレクトリ 検索の範囲など、追加の LDAP 許可 パラメータを設定できます。

```
hostname(config)# aaa-server LDAP protocol ldap
hostname(config-aaa-server-group)# aaa-server LDAP (inside) host 10.0.2.128
hostname(config-aaa-server-host)# ldap-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-group-base-dn DC=AD,DC=LAB,DC=COM
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)# ldap-login-dn AD\cisco
hostname(config-aaa-server-host)# ldap-login-password cisco123
hostname(config-aaa-server-host)# ldap-over-ssl enable
```

## ASA LDAP 構成の定義

```
hostname (config-aaa-server-host) # server-type microsoft
```

## ASA LDAP 構成の定義

このセクションでは、LDAP AV-pair 属性のシンタックスの定義方法について説明します。次の情報が含まれています。

- [LDAP 許可でサポートされている Cisco 属性](#) (6 ページ)
- [Cisco-AV-Pair 属性の構文](#) (19 ページ)
- [Cisco-AV-Pair の ACL 例](#) (20 ページ)



(注) ASA は、数値の ID ではなく属性名に基づいて LDAP 属性を適用します。一方、RADIUS 属性には、名前ではなく数値の ID が使用されます。

認可では、権限または属性を使用するプロセスを参照します。認証または認可サーバーとして定義されている LDAP サーバーは、権限または属性（設定されている場合）を適用します。

ASDM バージョン 7.0 の LDAP 属性には、cVPN3000 プレフィックスが含まれています。ソフトウェアバージョン 7.1 以降では、このプレフィックスは削除されています。

## LDAP 許可でサポートされている Cisco 属性

このセクションでは、ASA 5500、VPN 3000 コンセントレータ、および PIX 500 シリーズ ASA で使用される全属性のリストを示します。この表には、VPN 3000 コンセントレータおよび PIX 500 シリーズ ASA での属性サポート情報も含まれています。これは、このようなデバイスの組み合わせを使用するネットワークを設定するために役立ちます。

表 1: ASA が LDAP 許可でサポートする Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Access-Hours	Y	Y	Y	文字列	シングル	time-range の名前 (Business-Hours など)
Allow-Network-Extension-Mode	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	Y	Y	Y	整数	シングル	1 ~ 35791394 分

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Authorization-Required	Y			整数	シングル	0 = しない 1 = する
Authorization-Type	Y			整数	シングル	0 = なし 1 = RADIUS 2 = LDAP
Banner1	Y	Y	Y	文字列	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。
Banner2	Y	Y	Y	文字列	シングル	クライアントレス SSL VPN、クライアント SSL VPN、および IPSec クライアントのバナー文字列。
Cisco-AV-Pair	Y	Y	Y	文字列	マルチ	次の形式のオクテット文字列：  [Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]  詳細については、「Cisco AV ペア属性のシンタックス」のセクションを参照してください。
Cisco-IP-Phone-Bypass	Y	Y	Y	整数	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	Y	Y	Y	整数	シングル	0 = ディセーブル 1 = イネーブル
Client-Intercept-DHCP-Configure-Msg	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	Y	Y	Y	文字列	シングル	IPsec VPN クライアントのバージョン番号を示す文字列
Confidence-Interval	Y	Y	Y	整数	シングル	10 ~ 300 秒
DHCP-Network-Scope	Y	Y	Y	文字列	シングル	IP アドレス

## ■ LDAP 許可でサポートされている Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
DN-Field	Y	Y	Y	文字列	シングル	有効な値 : UID、OU、O、CN、L、SP、C、EA、T、N、GN、SN、I、GENQ、DNQ、SER、use-entire-name。
Firewall-ACL-In		Y	Y	文字列	シングル	アクセスリスト ID
Firewall-ACL-Out		Y	Y	文字列	シングル	アクセスリスト ID
Group-Policy		Y	Y	文字列	シングル	<p>リモートアクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-RADIUS-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。</p> <ul style="list-style-type: none"> <li>• グループ ポリシー名</li> <li>• OU= グループ ポリシー名</li> <li>• OU= グループ ポリシー名 :</li> </ul>
IE-Proxy-Bypass-Local				プール	シングル	0 = ディセーブル 1 = イネーブル
IE-Proxy-Exception-List				文字列	シングル	DNS ドメインのリスト。エントリは改行文字シーケンス (\n) で区切る必要があります。
IE-Proxy-Method	Y	Y	Y	整数	シングル	1 = プロキシ設定を変更しない 2 = プロキシを使用しない 3 = 自動検出 4 = ASA 設定を使用する
IE-Proxy-Server	Y	Y	Y	整数	シングル	IP アドレス

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IETF-Radius-Class	Y	Y	Y		シングル	<p>リモート アクセス VPN セッションのグループ ポリシーを設定します。バージョン 8.2 以降では、IETF-Radius-Class の代わりにこの属性を使用します。次の 3 つの形式のいずれかを使用できます。</p> <ul style="list-style-type: none"> <li>• グループ ポリシー名</li> <li>• OU= グループ ポリシー名</li> <li>• OU= グループ ポリシー名 :</li> </ul>
IETF-Radius-Filter-Id	Y	Y	Y	文字列	シングル	ASA で定義されたアクセスリスト名。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETFRadiusFamIPAddr	Y	Y	Y	文字列	シングル	IP アドレス。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETFRadiusFamIPMask	Y	Y	Y	文字列	シングル	IP アドレス マスク。これらの設定は、VPN リモート アクセス クライアント、IPSec クライアント、および SSL クライアントの設定に適用されます。
IETF-Radius-Idle-Timeout	Y	Y	Y	整数	シングル	秒
IETF-Radius-Service-Type	Y	Y	Y	整数	シングル	<p>1 = ログイン 2 = フレーム化 5 = リモート アクセス 6 = 管理可能 7 = NAS プロンプト</p>
IETFRadiusSessionTimeout	Y	Y	Y	整数	シングル	秒
IKE-Keep-Alives	Y	Y	Y	ブール	シングル	<p>0 = ディセーブル 1 = イネーブル</p>

## ■ LDAP 許可でサポートされている Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IPsec-Allow-Passwd-Store	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Authentication	Y	Y	Y	整数	シングル	0 = なし 1 = RADIUS 2 = LDAP (認可のみ) 3 = NT ドメイン 4 = SDI (RSA) 5 = 内部 6 = RADIUS (期限付き) 7 = Kerberos または Active Directory
IPsec-Auth-On-Rekey	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	Y	Y	Y	文字列	シングル	サーバー アドレス (スペース区切り)
IPsec-Backup-Servers	Y	Y	Y	文字列	シングル	1 = クライアントが設定したリストを使用する 2 = クライアントリストをディセーブルにして消去する 3 = バックアップ サーバー リストを使用する
IPsec-Client-Firewall-Filter-Name	Y			文字列	シングル	クライアントにファイアウォール ポリシーとして配信するフィルタの名前を指定します。
IPsec-Client-Firewall-Filter-Optional	Y	Y	Y	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	Y	Y	Y	文字列	シングル	クライアントに送信する1つのデフォルト ドメイン名を指定します (1 ~ 255 文字)。
Pre-Extend-Auth-On-Rekey		Y	Y	文字列	シングル	文字列

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
IPsec-IKE-Peer-ID-Check	Y	Y	Y	整数	シングル	1 = 必須 2 = ピア証明書でサポートされる場合 3 = チェックしない
IPsec-IP-Compression	Y	Y	Y	整数	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	Y	Y	Y	整数	シングル	4001 ~ 49151、デフォルトは 10000。
RequiredFirewallPolicy	Y	Y	Y	整数	シングル	0 = なし 1 = リモート FW Are-You-There (AYT) で定義されているポリシー 2 = ポリシーがプッシュされた CPP 4 = サーバーからのポリシー
IPsec-Sec-Association	Y			文字列	シングル	セキュリティアソシエーションの名前
IPsec-Split-DNS-Names	Y	Y	Y	文字列	シングル	クライアントに送信するセカンダリドメイン名のリストを指定します (1 ~ 255 文字)。
IPsec-Split-Tunneling-Policy	Y	Y	Y	整数	シングル	0 = すべてをトンネリング 1 = スプリット トンネリング 2 = ローカル LAN を許可
IPsec-Split-Tunnel-List	Y	Y	Y	文字列	シングル	スプリットトンネルの包含リストを記述したネットワークまたはアクセスリストの名前を指定します。
IPsec-Tunnel-Type	Y	Y	Y	整数	シングル	1 = LAN-to-LAN 2 = リモート アクセス

## ■ LDAP 許可でサポートされている Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
L2TP-Encryption	Y			整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPCCompresion	Y			整数	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	Y	Y	Y	文字列	シングル	IP アドレス
PFS-Required	Y	Y	Y	プール	シングル	0 = しない 1 = する
Port-Forwarding-Name	Y	Y		文字列	シングル	名前の文字列 (例 : 「Corporate-Apps」)
PPTP-Encryption	はい			整数	シングル	ビットマップ： 1 = 暗号化が必要 2 = 40 ビット 4 = 128 ビット 8 = ステートレスが必要 例： 15 = 40/128 ビットで暗号化/ステートレスが必要
PPTP-MPPCCompresion	Y			整数	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Primary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
Privilege-Level				整数	シングル	ユーザー名の場合、0 ~ 15

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Required-Client-Firewall-Vendor-Code	Y	Y	Y	整数	シングル	1 = シスコ (Cisco Integrated Client を使用) 2 = Zone Labs 3 = NetworkICE 4 = Sygate 5 = シスコ (Cisco Intrusion Prevention Security Agent を使用)
Required-Client-Firewall-Description	Y	Y	Y	文字列	シングル	—
Required-Client-Firewall-Product-Code	Y	Y	Y	整数	シングル	シスコ製品： 1 = Cisco Intrusion Prevention Security Agent または Cisco Integrated Client (CIC)  Zone Labs 製品： 1 = Zone Alarm 2 = Zone AlarmPro 3 = Zone Labs Integrity  NetworkICE 製品： 1 = BlackIce Defender/Agent  Sygate 製品： 1 = Personal Firewall 2 = Personal Firewall Pro 3 = Security Agent
Require-HW-Client-Auth	Y	Y	Y	プール	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	Y	Y	Y	整数	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	Y	Y	Y	文字列	シングル	IP アドレス
Secondary-WINS	Y	Y	Y	文字列	シングル	IP アドレス
SEP-Card-Assignment				整数	シングル	未使用

## ■ LDAP 許可でサポートされている Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
Simultaneous-Logins	Y	Y	Y	整数	シングル	0 ~ 2147483647
Strip-Realm	Y	Y	Y	ブール	シングル	0 = ディセーブル 1 = イネーブル
TACACS-Authtype	Y	Y	Y	整数	シングル	—
TACACS-Privilege-Level	Y	Y	Y	整数	シングル	—
Tunnel-Group-Lock		Y	Y	文字列	シングル	トンネルグループの名前または「none」
Tunneling-Protocols	Y	Y	Y	整数	シングル	1 = PPTP 2 = L2TP 4 = IPSec (IKEv1) 8 = L2TP/IPSec 16 = WebVPN. 32 = SVC 64 = IPsec (IKEv2) 8 および 4 は相互排他値 (0~11、16~27、32~43、48~59 は有効値)。
Use-Client-Address	Y			ブール	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	Y			文字列	シングル	IP アドレス/ホスト名
User-Auth-Server-Port	Y	Y	Y	整数	シングル	サーバー プロトコルのポート番号
User-Auth-Server-Secret	Y			文字列	シングル	サーバーのパスワード
WebVPN-ACL-Filters		Y		文字列	シングル	Webtype アクセスリスト名
WebVPNApplyACLFirst	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性 は必須ではありません。

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPNDirSupportEnable	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル バージョン 8.0 以降では、この属性は必須ではありません。
WebVPNEnableFunctions				整数	シングル	使用しない (廃止)
WebVPNExchangeServerAddress				文字列	シングル	使用しない (廃止)
WebVPNExchangeServerNETBIOS-Name				文字列	シングル	使用しない (廃止)
WebVPNFileAccessEnable	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSendForwardingEnable	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNFileServerEntry-Enable	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNForwardedPorts		Y		文字列	シングル	ポート転送リスト名
WebVPN-Homepage	Y	Y		文字列	シングル	URL (たとえば <a href="http://www.example.com">http://www.example.com</a> )
WebVPNMacShiftInVal1	Y	Y		文字列	シングル	例については、次の URL にある『SSL VPN Deployment Guide』を参照してください。 <a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpndeployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpndeployment_guide/deploy.html</a>
WebVPNMacShiftInVal2	Y	Y		文字列	シングル	例については、次の URL にある『SSL VPN Deployment Guide』を参照してください。 <a href="http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpndeployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpndeployment_guide/deploy.html</a>
WebVPNPortForwarding-Auto-Download-Enable	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル

## ■ LDAP 許可でサポートされている Cisco 属性

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPNPortForwarding-Enable	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNPortForwarding-Exchange-Proxy-Enable	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNPortForwarding-HTTP-Proxy-Enable	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSingleSignOn-Server-Name	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCClientDPD	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCCompresion	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Enable	Y	Y		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCGatewayDPD	Y	Y		整数	シングル	0 = ディセーブル n = デッドピア検出値 (30 ~ 3600 秒)
WebVPNSVCKeepalive	Y	Y		整数	シングル	0 = ディセーブル n = キープアライブ値 (15 ~ 600 秒)
WebVPNSVCKeepEndle	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNSVCKeyMtd	Y	Y		整数	シングル	0 = なし 1 = SSL 2 = 新規トンネル 3 = 任意 (SSL に設定)

属性名	VPN 3000	ASA	PIX	構文/タイプ	シングルまたはマルチ値	有効な値
WebVPNServicePeriod	Y	Y		整数	シングル	0 = ディセーブル n = 分単位の再試行間隔 (4 ~ 10080 分)
WebVPNServiceRapidEnt	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNURLEntryEnt	Y	Y		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-URL-List		Y		文字列	シングル	URL リスト名

## ACL でサポートされる URL タイプ

URL は部分的な URL でもかまいません。また、サーバーを表すワイルドカードや、ポートが含まれていてもかまいません。

次の URL タイプがサポートされています。

すべての URL	https://	post://	ssh://
cifs://	ica://	rdp://	telnet://
citrix://	imap4://	rdp2://	vnc://
citrixs://	ftp://	smart-tunnel://	
http://	pop3://	smtp://	

## Cisco-AV-Pair (ACL) 使用のガイドライン

- リモート IPsec トンネルおよび SSL VPN Client (SVC) トンネルにアクセスリストを適用するには、Cisco-AV-Pair エントリにプレフィックス ip:inac1# を追加して使用してください。
- SSL VPN クライアントレス（ブラウザモード）トンネルにアクセスリストを適用するには、Cisco-AV-Pair エントリにプレフィックス webvpn:inac1# を追加して使用してください。
- Webtype ACL では、ASA が送信元となるため、送信元を指定しないでください。

## Cisco-AV-Pair (ACL) 使用のガイドライン

表 2: ASA でサポートされるトークン

トークン	構文のフィールド	説明
ip:inac1# Num =	該当なし (識別子)	(ここで、Num は一意の整数です) すべての AV ペアアクセス制御リストを開始します。リモート IPsec トンネルと SSL VPN (SVC) トンネルにアクセスリストを適用します。
webvpn:inac1# Num =	該当なし (識別子)	(ここで、Num は一意の整数です) すべてのクライアントレス SSL AV ペアアクセス制御リストを開始します。クライアントレス (ブラウザモード) トンネルにアクセスリストを適用します。
deny	アクション	アクションを拒否します。(デフォルト)。
許可	アクション	アクションを許可します。
icmp	プロトコル	インターネット制御メッセージプロトコル (ICMP)
1	プロトコル	インターネット制御メッセージプロトコル (ICMP)
IP	プロトコル	インターネットプロトコル (IP)
0	プロトコル	インターネットプロトコル (IP)
TCP	プロトコル	伝送制御プロトコル (TCP)
6	プロトコル	伝送制御プロトコル (TCP)
UDP	プロトコル	User Datagram Protocol (UDP)
17	プロトコル	User Datagram Protocol (UDP)
any	ホストネーム	すべてのホストにルールを適用します。
host	ホストネーム	ホスト名を示す任意の英数字文字列。
log	ログ	イベントが発生すると、フィルタログメッセージが表示されます。(permit and log または deny and log の場合と同様)。
lt	演算子	値より小さい
gt	演算子	値より大きい
eq	演算子	値と等しい
neq	演算子	値と等しくない
range	演算子	この範囲に含まれる。range の後に 2 つの値を続けます。

## Cisco-AV-Pair 属性の構文

Cisco Attribute Value (AV) ペア (ID 番号 26/9/1) を使用すると、アクセスリストを RADIUS サーバー (たとえば Cisco ACS) から、または LDAP サーバーから LDAP 属性マップ経由で適用できます。

Cisco-AV-Pair ルールの構文は次のとおりです。

*[Prefix] [Action] [Protocol] [Source] [Source Wildcard Mask] [Destination] [Destination Wildcard Mask] [Established] [Log] [Operator] [Port]*

表 3: AV-Pair 属性の構文ルール

フィールド	説明
操作	ルールに一致する場合に実行するアクション (deny または permit)。
接続先	パケットを受信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード <b>any</b> で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。
接続先ワイルドカードマスク	宛先アドレスに適用されるワイルドカードマスク。
ログ	FILTER ログメッセージを生成します。重大度レベル 9 のイベントを生成するには、このキーワードを使用する必要があります。
演算子	論理演算子 : greater than、less than、equal to、not equal to。
ポート	TCP または UDP ポートの番号 (0 ~ 65535)。
プレフィックス	AV ペアの固有識別子。（例：ip:inac1#1=（標準アクセスリスト用）または webvpn:inac1#（クライアントレス SSL VPN アクセスリスト用））。このフィールドは、フィルタが AV ペアとして送信された場合にだけ表示されます。
プロトコル	IP プロトコルの番号または名前。0 ~ 255 の整数値、または <b>icmp</b> 、 <b>igmp</b> 、 <b>ip</b> 、 <b>tcp</b> 、 <b>udp</b> のいずれかのキーワード。
送信元	パケットを送信するネットワークまたはホスト。IP アドレス、ホスト名、またはキーワード <b>any</b> で指定します。IP アドレスを使用する場合、続いて Source Wildcard Mask を指定する必要があります。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。
送信元ワイルドカードマスク	送信元アドレスに適用されるワイルドカードマスク。ASA がソースまたはプロキシの役割を果たすため、このフィールドはクライアントレス SSL VPN には適用されません。

## Cisco-AV-Pair の ACL 例

このセクションでは、Cisco AVペアの例を示し、その結果の許可または拒否のアクションについて説明します。



(注) inacl# の各 ACL # は固有である必要があります。ただし、これらは連続している（たとえば 1、2、3、4）必要はありません。たとえば、5、45、135 でもかまいません。

表 4: Cisco AVペアとそのアクション許可/拒否の例

Cisco-AV-Pair の例	アクションの許可または拒否
ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log	フルトンネル IPsec または SSL VPN クライアントを使用した、2つのホスト間の IP トラフィックを許可します。
ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log	フルトンネル IPsec または SSL VPN クライアントのみを使用した、すべてのホストから特定のホストのポート 80 への TCP トラフィックを許可します。
webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share	指定 URL へのクライアントレス SSL VPN トラフィックを許可し、特定サーバーへの SMTP トラフィックを拒否し、指定サーバーへのファイル共有アクセス (CIFS) を許可します。
webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log	クライアントレス SSL VPN について、非デフォルトポート 2323 および 2222 で Telnet アクセスを拒否し、SSH アクセスを許可します。これらのポートを使用して通過する他のアプリケーション トラフィックも同様に許可または拒否します。
webvpn:inacl#1=permit url ssh://10.86.1.2webvpn:inacl#35=permit tcp 10.86.1.5 eq 22 logwebvpn:inacl#48=deny url telnet://10.86.1.2webvpn:inacl#100=deny tcp 10.86.1.6 eq 23	クライアントレス SSL VPN でのデフォルトポート 22 への SSH アクセスを許可し、ポート 23 への Telnet アクセスを拒否します。この例は、これらの ACL で適用される Telnet または SSH Java プラグインを使用していることを前提とします。

## Active Directory/LDAP VPN リモート アクセス許可の例

この項では、Microsoft Active Directory サーバーを使用している ASA で認証および認可を設定するための手順の例を示します。説明する項目は次のとおりです。

- ユーザー ベースの属性のポリシー適用 (21 ページ)
- セキュアクライアントトンネルのスタティック IP アドレス割り当ての適用 (23 ページ)
- ダイヤルイン許可または拒否アクセスの適用 (25 ページ)
- ログオン時間と Time-of-Day ルールの適用 (27 ページ)

その他の設定例については、Cisco.com にある次のテクニカル ノートを参照してください。

- ・『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』
- ・『PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login』

## ユーザー ベースの属性のポリシー適用

この例では、ユーザー向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性 (VSA) にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。IPsec VPN クライアントやセキュアクライアントなど、どの接続タイプにも適用されます。

AD LDAP サーバー上で設定されたユーザーに簡易バナーを適用するには、[General] タブの [Office] フィールドを使用してバナー テキストを入力します。このフィールドでは、physicalDeliveryOfficeName という名前の属性を使用します。ASA で、physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングする属性マップを作成します。

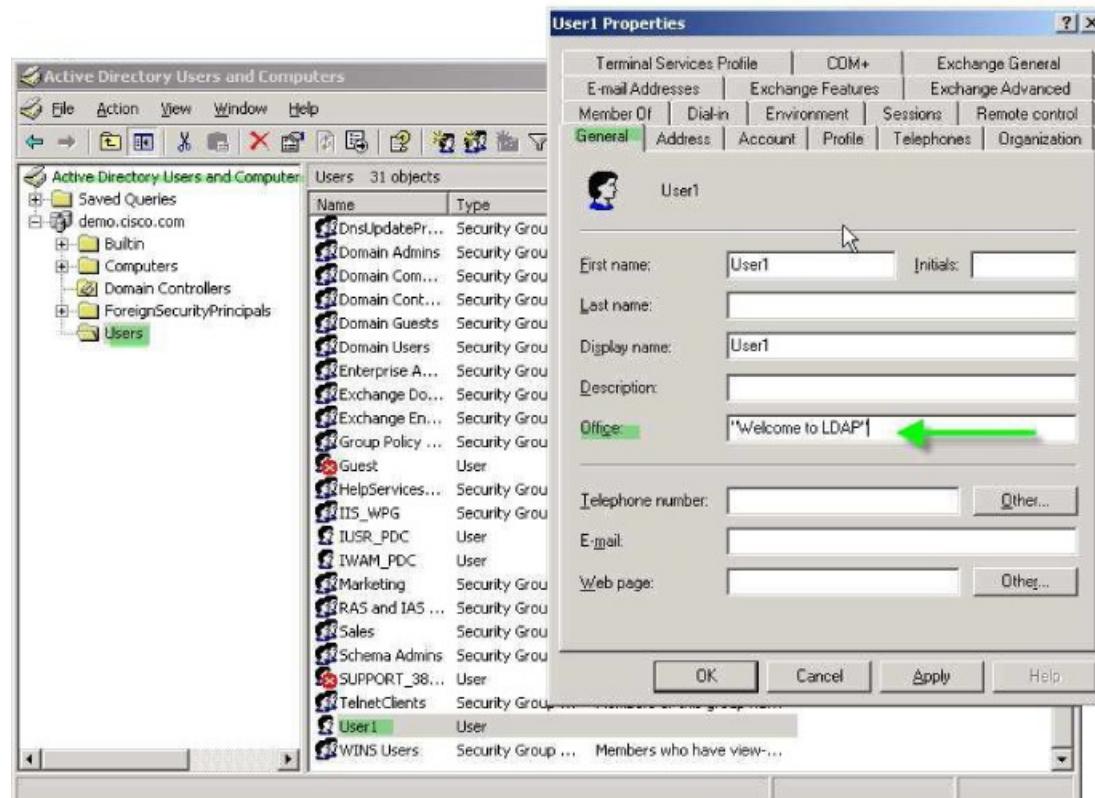
認証時、ASA はサーバーから physicalDeliveryOfficeName の値を取得し、その値を Cisco 属性 Banner1 にマッピングしてユーザーにバナーを表示します。

### 手順

---

**ステップ1** ユーザー名を右クリックして、[Properties] ダイアログボックスの [General] タブを開き、AD/LDAP 属性 physicalDeliveryOfficeName を使用する [Office] フィールドにバナー テキストを入力します。

## ■ ユーザー ベースの属性のポリシー適用



330370

### ステップ2 ASA で LDAP 属性マップを作成します。

Banner というマップを作成し、AD/LDAP 属性 physicalDeliveryOfficeName を Cisco 属性 Banner1 にマッピングします。

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

### ステップ3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバーグループ MS\_LDAP のホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始し、以前作成した属性マップ Banner を関連付けます。

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

### ステップ4 バナーの適用をテストします。

## セキュアクライアント トンネルのスタティック IP アドレス割り当ての適用

この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネルクライアントに適用されます。

スタティック セキュアクライアント クライアントユーザー Web1 をスタティック IP アドレスを受信するように設定して、そのアドレスを AD LDAP サーバーの [ダイヤルイン (Dialin) ] タブの [スタティック IP アドレスの割り当て (Assign Static IP Address) ] フィールド（このフィールドで msRADIUSFramedIPAddress 属性が使用される）に入力し、この属性を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングする属性マップを作成します。

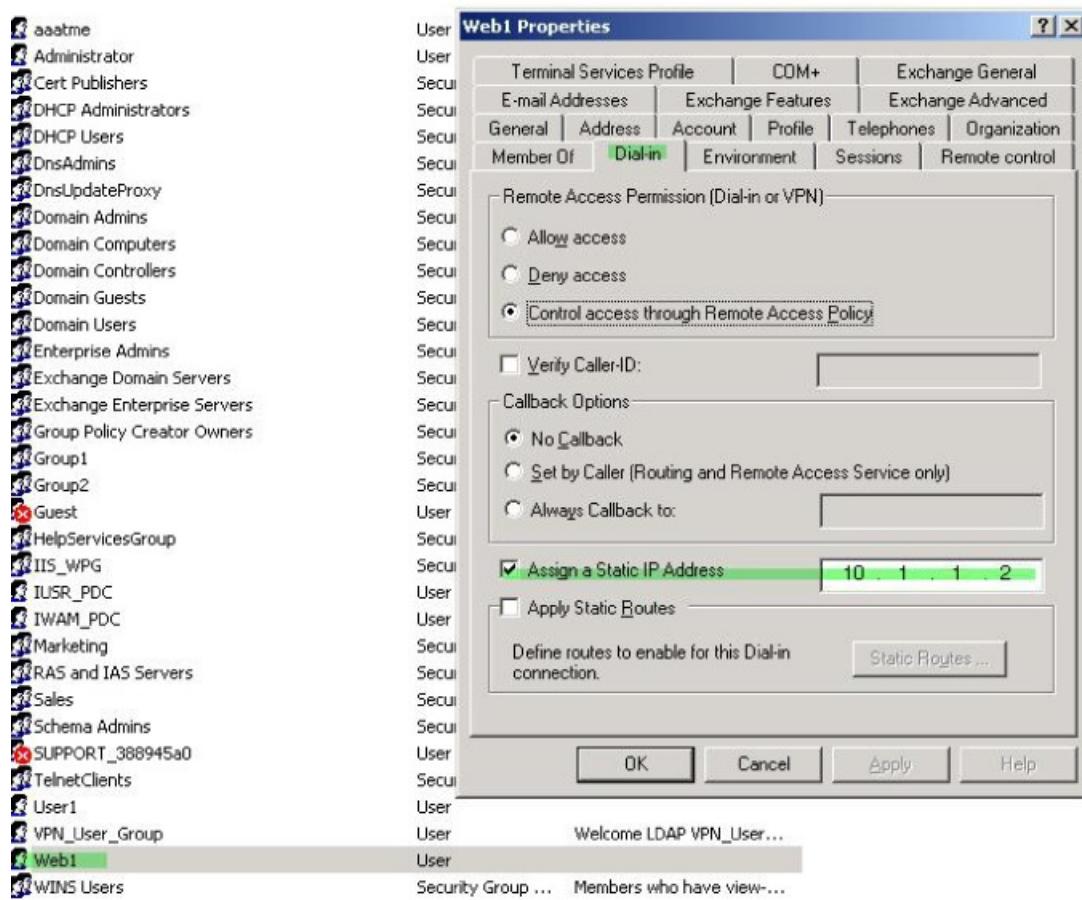
認証時に、ASA はサーバーから msRADIUSFramedIPAddress の値を取得し、その値を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングして、User1 にスタティック アドレスを渡します。

### 手順

---

**ステップ1** ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Assign Static IP Address] チェックボックスをオンにして、10.1.1.2 という IP アドレスを入力します。

## セキュアクライアントトンネルのスタティック IP アドレス割り当ての適用



330373

### ステップ2 図に示す LDAP コンフィギュレーションの属性マップを作成します。

[Static Address] フィールドで使用される AD 属性 msRADIUSFramedIPAddress を Cisco 属性 IETF-Radius-Framed-IP-Address にマッピングします。

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

### ステップ3 LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバーグループ MS\_LDAP のホスト 10.1.1.2 に対して AAA サーバー ホスト コンフィギュレーションモードを開始し、作成した属性マップ static\_address を関連付けます。

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

### ステップ4 vpn-address-assignment コマンドが AAA を指定するように設定されているかどうかを確認するために、コンフィギュレーションのこの部分を表示します。

```
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)#

```

**ステップ5** ASA とセキュアクライアントとの接続を確立します。サーバーで設定され、ASA にマッピングされた IP アドレスをユーザーが受信することを確認します。

**ステップ6** **show vpn-sessiondb svc** コマンドを使用してセッションの詳細を表示し、割り当てられたアドレスを確認します。

```
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
```

---

## ダイヤルイン許可または拒否アクセスの適用

この例では、ユーザーによって許可されるトンネリングプロトコルを指定する LDAP 属性マップを作成します。[Dialin] タブの許可アクセスと拒否アクセスの設定を Cisco 属性 Tunneling-Protocol にマッピングします。この属性は次のビットマップ値をサポートします。

値	トンネリング プロトコル
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	クライアントレス SSL
32	SSL クライアント：セキュアクライアントまたは SSL VPN クライアント
64	IPsec (IKEv2)

<sup>1</sup> (1) IPsec と L2TP over IPsec は同時にサポートされません。そのため、値 4 と 8 は相互排他値となります。

## ■ ダイヤルイン許可または拒否アクセスの適用

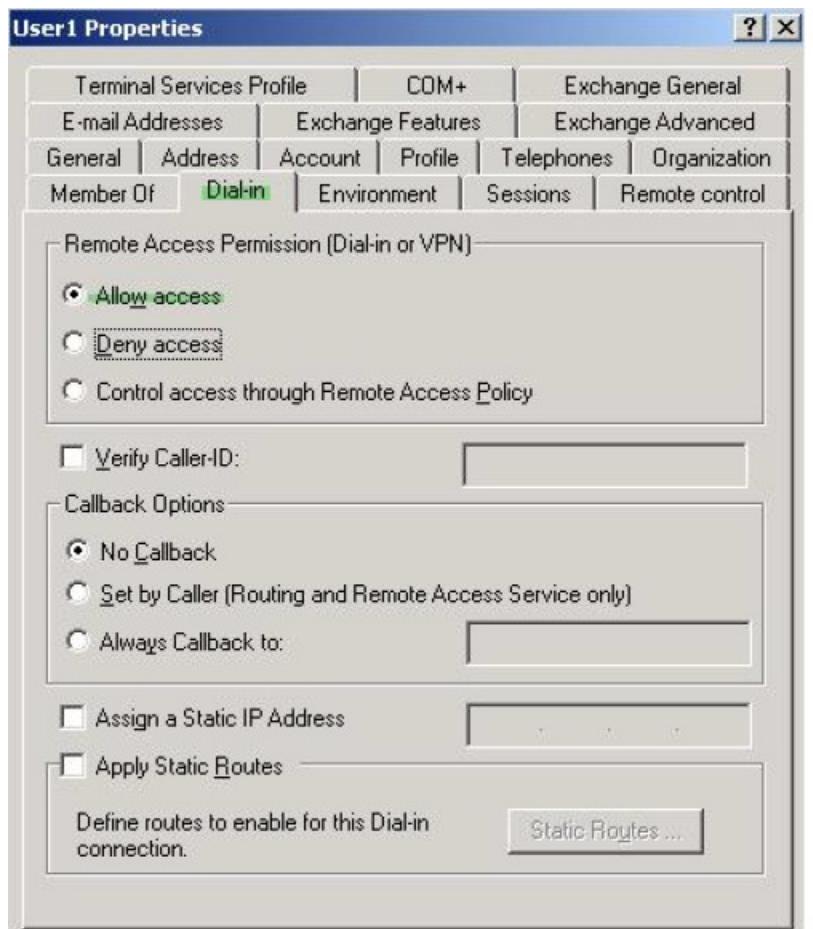
### 2 (2) 注 1 を参照。

この属性を使用して、プロトコルの [Allow Access] (TRUE) または [Deny Access] (FALSE) の条件を作成し、ユーザーがアクセスを許可される方法を適用します。

ダイヤルイン許可アクセスまたは拒否アクセスの適用に関するその他の例については、テクニカルノート『ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example』を参照してください。

## 手順

**ステップ1** ユーザー名を右クリックして、[Properties] ダイアログボックスの [Dial-in] タブを開き、[Allow Access] オプション ボタンをクリックします。



(注)

[Control access through the Remote Access Policy] オプションを選択した場合は、サーバーから値が返されず、適用される権限は ASA の内部グループ ポリシー設定に基づいて決定されます。

**ステップ2** IPsec とセキュアクライアントの両方の接続を許可する一方で、クライアントレス SSL 接続を拒否する属性マップを作成します。

- マップ tunneling\_protocols を作成します。

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

- [Allow Access] 設定で使用される AD 属性 msNPAllowDialin を Cisco 属性 Tunneling-Protocols にマッピングします。

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

- マップ値を追加します。

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

**ステップ3** LDAP 属性マップを AAA サーバーに関連付けます。

- AAA サーバーグループ MS\_LDAP でホスト 10.1.1.2 の AAA サーバー ホスト コンフィギュレーション モードを開始します。

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

- 作成した属性マップ tunneling\_protocols を関連付けます。

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

**ステップ4** 属性マップが設定したとおりに機能することを確認します。

クライアントレス SSL を使用して接続を試みます。ユーザーには、許可されていない接続メカニズムが接続の失敗の原因であることが通知されます。IPsec クライアントの接続は成功します。これは、属性マップに従って IPsec にトンネリング プロトコルが許可されるためです。

## ログオン時間と Time-of-Day ルールの適用

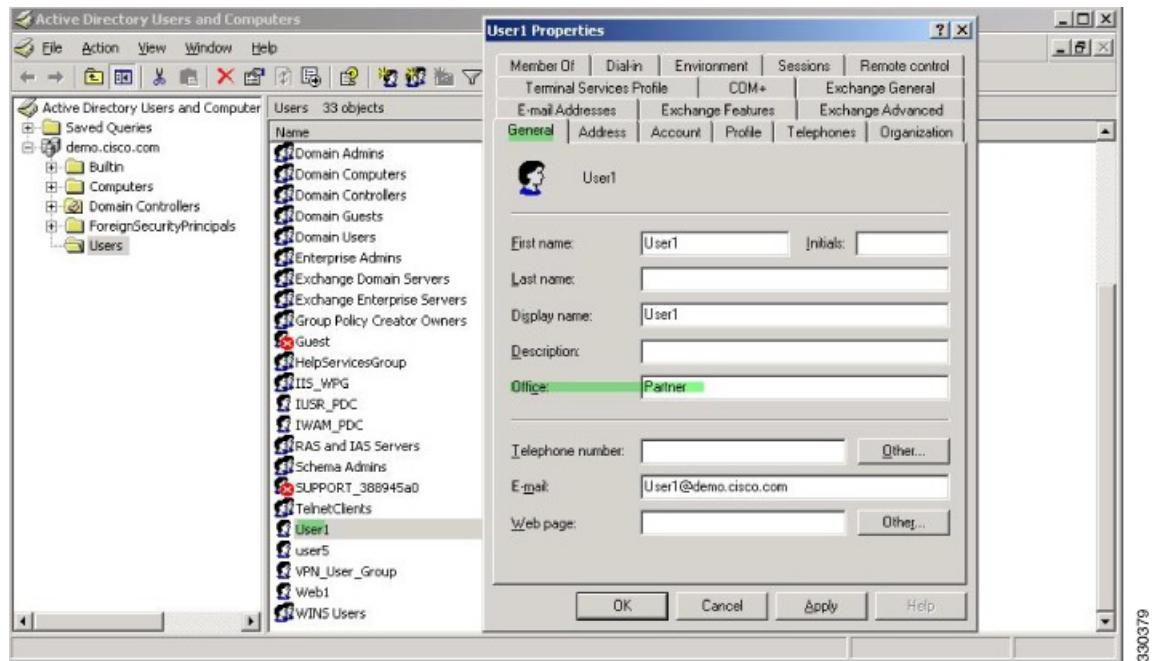
次の例では、クライアントレス SSL ユーザー（たとえばビジネス パートナー）にネットワークへのアクセスを許可する時間帯を設定して適用する方法を示します。

AD サーバー上で、[Office] フィールドを使用してパートナーの名前を入力します。このフィールドでは、physicalDeliveryOfficeName 属性が使用されます。次に、ASA で属性マップを作成し、その属性を Cisco 属性 Access-Hours にマッピングします。認証時に、ASA は physicalDeliveryOfficeName の値を取得して Access-Hours にマッピングします。

## ■ ログオン時間と Time-of-Day ルールの適用

### 手順

**ステップ1** ユーザーを選択して、[Properties] を右クリックし、[General] タブを開きます。



**ステップ2** 属性マップを作成します。

属性マップ `access_hours` を作成し、[Office] フィールドで使用される AD 属性 `physicalDeliveryOfficeName` を Cisco 属性 `Access-Hours` にマッピングします。

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

**ステップ3** LDAP 属性マップを AAA サーバーに関連付けます。

AAA サーバー グループ `MS_LDAP` のホスト `10.1.1.2` に対して AAA サーバー ホスト コンフィギュレーション モードを開始し、作成した属性マップ `access_hours` を関連付けます。

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

**ステップ4** 各値にサーバーで許可された時間範囲を設定します。

パートナー アクセス時間を月曜日から金曜日の午前 9 時から午後 5 時に設定します。

```
hostname(config)# time-range Partner
```

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

---

## ■ ログオン時間と Time-of-Day ルールの適用

## 翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。