



## VPN の外部 AAA サーバの設定

- [外部 AAA サーバについて \(1 ページ\)](#)
- [外部 AAA サーバ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 \(3 ページ\)](#)
- [Active Directory/LDAP VPN リモート アクセス許可の例 \(19 ページ\)](#)

### 外部 AAA サーバについて

この ASA は、外部の LDAP、RADIUS、TACACS+ サーバを使用して、ASA の認証、認可、アカウントリング (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、ユーザ認可属性 (ユーザ権利またはユーザ権限とも呼ばれる) 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 (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。

2. AAA サーバ上のユーザ属性：ユーザ認証や認可が成功すると、サーバ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に設定されている属性（ASDM のユーザ 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 サーバからユーザに対して RADIUS CLASS 属性 IETF-Class-25（OU=*group-policy*）の値が返された場合、ASA はそのユーザを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、サーバから返されないものを適用します。

LDAP サーバでは、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せん。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、サーバから返されるユーザ属性、ユーザ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

AnyConnect 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証明書（または2つのユーザ証明書）が必要であるため、この機能では AnyConnect Start Before Logon (SBL) を使用できません。

ユーザ名の事前入力フィールドでは、2つ目の（ユーザ）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名は、常にクライアントから受信した2つ目の（ユーザ）証明書から取得されます。

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）証明書は、事前入力および証明書由来のユーザ名のプライマリおよびセカンダリユーザ名による解析対象です。

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] | saml}
```

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。

## 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
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 \(5 ページ\)](#)
- [Cisco-AV-Pair 属性の構文 \(18 ページ\)](#)
- [Cisco-AV-Pair の ACL 例 \(19 ページ\)](#)



(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として定義されている LDAP サーバは、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、VPN3000 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	はい	はい	はい	文字列	シングル	time-range の名前 (Business-Hours など)
Allow-Network-Extension-Mode	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
Authenticated-User-Idle-Timeout	はい	はい	はい	整数	シングル	1 ~ 35791394 分

## 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
Authorization-Required	はい			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	はい	はい	はい	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	はい	はい	はい	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	はい	はい	はい	文字列	[マルチ (Multi) ]	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	はい	はい	はい	整数	シングル	0 = ディセーブル 1 = イネーブル
Cisco-LEAP-Bypass	はい	はい	はい	整数	シングル	0 = ディセーブル 1 = イネーブル
Client-Intercept-DHCP-Configure-Msg	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
Client-Type-Version-Limiting	はい	はい	はい	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	はい	はい	はい	整数	シングル	10 ~ 300 秒
DHCP-Network-Scope	はい	はい	はい	文字列	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
DN-Field	はい	はい	はい	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		はい	はい	文字列	シングル	アクセス リスト ID
Firewall-ACL-Out		はい	はい	文字列	シングル	アクセス リスト ID
Group-Policy		はい	はい	文字列	シングル	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。 <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				ブール	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。エントリー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	はい	はい	はい	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	はい	はい	はい	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	はい	はい	はい		シングル	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。 <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	はい	はい	はい	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。
IETF-Radius-Framed-IP-Address	はい	はい	はい	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。
IETF-Radius-Framed-IP-Netmask	はい	はい	はい	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	はい	はい	はい	整数	シングル	Seconds
IETF-Radius-Service-Type	はい	はい	はい	整数	シングル	1 = Login 2 = Framed 5 = リモート アクセス 6 = Administrative 7 = NAS プロンプト
IETF-Radius-Session-Timeout	はい	はい	はい	整数	シングル	Seconds
IKE-Keep-Alives	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル



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	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Authentication	はい	はい	はい	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 with Expiry 7 = Kerberos または Active Directory
IPsec-Auth-On-Rekey	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Backup-Server-List	はい	はい	はい	文字列	シングル	サーバアドレス (スペース区切り)
IPsec-Backup-Servers	はい	はい	はい	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リストを使用する
IPsec-Client-Firewall-Filter-Name	はい			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	はい	はい	はい	整数	シングル	0 = 必須 1 = オプション
IPsec-Default-Domain	はい	はい	はい	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)。
IPsec-ExtAuthOnRekey		はい	はい	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	はい	はい	はい	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	はい	はい	はい	整数	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Mode-Config	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
IPsec-Over-UDP-Port	はい	はい	はい	整数	シングル	4001 ~ 49151、デフォルトは 10000。
IPsec-Require-CP	はい	はい	はい	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 = Policy pushed CPP 4 = サーバからのポリシー
IPsec-Sec-Association	はい			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	はい	はい	はい	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	はい	はい	はい	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	はい	はい	はい	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	はい	はい	はい	整数	シングル	1 = LAN-to-LAN 2 = リモートアクセス

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
L2TP-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 15 = 40/128 ビットで暗号化/ステートレスが必要
L2TP-MPPC-Compression	はい			整数	シングル	0 = ディセーブル 1 = イネーブル
MS-Client-Subnet-Mask	はい	はい	はい	文字列	シングル	IP アドレス
PFS-Required	はい	はい	はい	ブール	シングル	0 = しない 1 = する
Port-Forwarding-Name	はい	はい		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-MPPC-Compression	はい			整数	シングル	0 = ディセーブル 1 = イネーブル
Primary-DNS	はい	はい	はい	文字列	シングル	IP アドレス
Primary-WINS	はい	はい	はい	文字列	シングル	IP アドレス
Privilege-Level				整数	シングル	ユーザ名の場合、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	はい	はい	はい	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	はい	はい	はい	文字列	シングル	—
Required-Client-Firewall-Product-Code	はい	はい	はい	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	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
Require-Individual-User-Auth	はい	はい	はい	整数	シングル	0 = ディセーブル 1 = イネーブル
Secondary-DNS	はい	はい	はい	文字列	シングル	IP アドレス
Secondary-WINS	はい	はい	はい	文字列	シングル	IP アドレス
SEP-Card-Assignment				整数	シングル	未使用

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	はい	はい	はい	整数	シングル	0 ~ 2147483647
Strip-Realm	はい	はい	はい	ブール	シングル	0 = ディセーブル 1 = イネーブル
TACACS-Authtype	はい	はい	はい	整数	シングル	—
TACACS-Privilege-Level	はい	はい	はい	整数	シングル	—
Tunnel-Group-Lock		はい	はい	文字列	シングル	トンネル グループの名前または「none」
Tunneling-Protocols	はい	はい	はい	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	はい			ブール	シングル	0 = ディセーブル 1 = イネーブル
User-Auth-Server-Name	はい			文字列	シングル	IPアドレス/ホスト名
User-Auth-Server-Port	はい	はい	はい	整数	シングル	サーバ プロトコルのポート番号
User-Auth-Server-Secret	はい			文字列	シングル	サーバのパスワード
WebVPN-ACL-Filters		はい		文字列	シングル	Webtype アクセス リスト名
WebVPN-Apply-ACL-Enable	はい	はい		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
WebVPN-Client-Support-Enable	はい	はい		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。
WebVPN-Enable-functions				整数	シングル	使用しない (廃止)
WebVPN-Exchange-Server-Address				文字列	シングル	使用しない (廃止)
WebVPN-Exchange-Server-NETBIOS-Name				文字列	シングル	使用しない (廃止)
WebVPN-File-Access-Enable	はい	はい		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Enable	はい	はい		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-File-Server-Entry-Enable	はい	はい		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Forwarded-Ports		はい		文字列	シングル	ポート転送リスト名
WebVPN-Homepage	はい	はい		文字列	シングル	URL (たとえば <a href="http://www.example.com">http://www.example.com</a> )
WebVPN-Mac-Substit-Via1	はい	はい		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_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a>
WebVPN-Mac-Substit-Via2	はい	はい		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_vpn_deployment_guide/deploy.html">http://www.cisco.com/en/US/docs/security/asa/asa80/asdm60/ssl_vpn_deployment_guide/deploy.html</a>
WebVPN-Port-Forwarding-Auto-Download-Enable	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル

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
WebVPN-Port-Forwarding-Enable	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-Exchange-Proxy-Enable	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Port-Forwarding-HTTP-Proxy-Enable	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-Single-Sign-On-Server-Name	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Client-DPD	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Compression	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Enable	はい	はい		ブール	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Gateway-DPD	はい	はい		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)
WebVPN-SVC-Keepalive	はい	はい		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)
WebVPN-SVC-Keepalive-Enable	はい	はい		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPN-SVC-Key-Method	はい	はい		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)

## ACL でサポートされる URL タイプ

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
WebVNSVC-Key-Period	はい	はい		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)
WebVNSVC-Key-Enable	はい	はい		整数	シングル	0 = ディセーブル 1 = イネーブル
WebVPNURL-Entry-Enable	はい	はい		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://
citrixxs://	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:inacl#` 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:inacl#` 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。



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:inacl# Num =	該当なし (識別子)	(ここで、 <i>Num</i> 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:inacl# Num =	該当なし (識別子)	(ここで、 <i>Num</i> 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)
任意	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 (たとえば Cisco ACS) から、または LDAP サーバから 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 (Destination)	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。
Destination Wildcard Mask	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 (Port) ]	TCP または UDP ポートの番号 (0 ~ 65535)。
[プレフィックス (Prefix) ]	AV ペアの固有識別子。(例 : ip:inacl#1= (標準アクセスリスト用) または webvpn:inacl# (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。
ソース (Source)	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。
Source Wildcard Mask	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
<code>ip:inacl#1=deny ip 10.155.10.0 0.0.0.255 10.159.2.0 0.0.0.255 log</code>	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。
<code>ip:inacl#2=permit TCP any host 10.160.0.1 eq 80 log</code>	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。
<code>webvpn:inacl#1=permit url http://www.example.comwebvpn:inacl#2=deny url smtp://serverwebvpn:inacl#3=permit url cifs://server/share</code>	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、特定サーバへの SMTP トラフィックを拒否し、指定サーバへのファイル共有アクセス (CIFS) を許可します。
<code>webvpn:inacl#1=permit tcp 10.86.1.2 eq 2222 logwebvpn:inacl#2=deny tcp 10.86.1.2 eq 2323 log</code>	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。
<code>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</code>	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。

- [ユーザベースの属性のポリシー適用 \(20 ページ\)](#)
- [特定のグループポリシーへの LDAP ユーザの配置 \(22 ページ\)](#)
- [AnyConnect 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](#)』

## ユーザベースの属性のポリシー適用

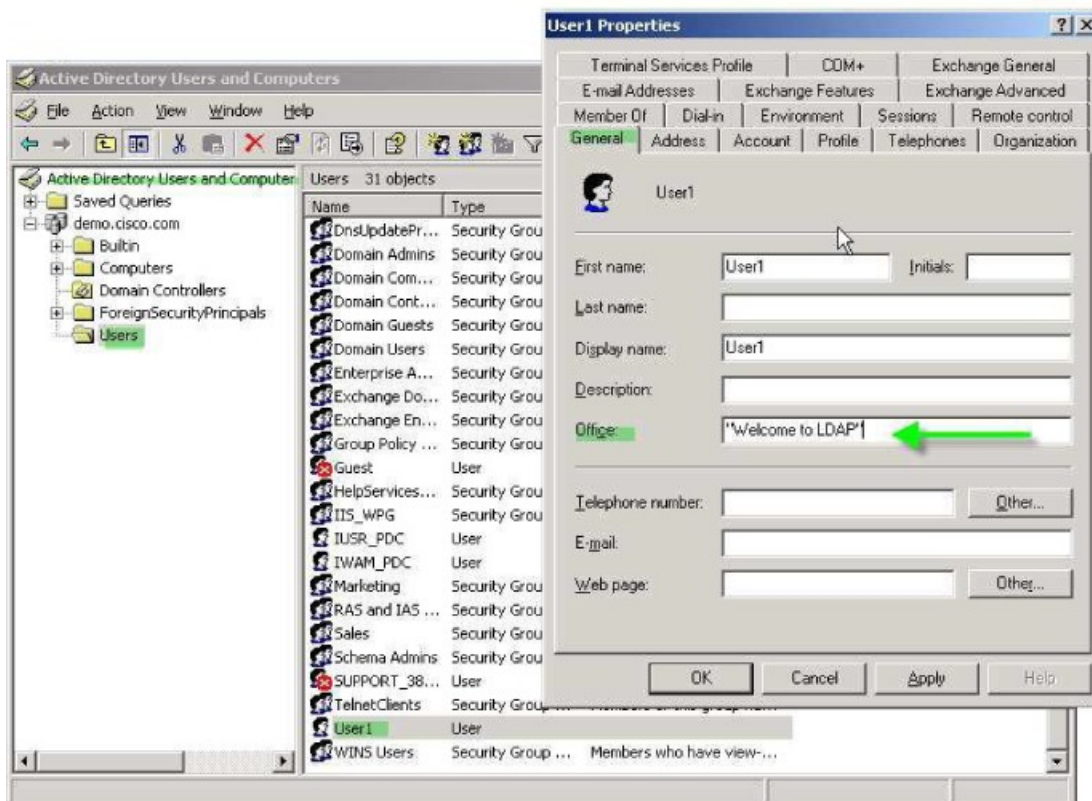
この例では、ユーザ向けの簡易バナーを表示して、標準の LDAP 属性を既知のベンダー固有属性 (VSA) にマッピングする方法と 1 つ以上の LDAP 属性を 1 つ以上の Cisco LDAP 属性にマッピングする方法を示します。この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。

AD LDAP サーバ上で設定されたユーザ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にバナーを表示します。

### 手順

- 
- ステップ 1** ユーザ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。



**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 サーバに関連付けます。

AAA サーバグループ MS\_LDAP のホスト 10.1.1.2 の AAA サーバ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。

## 特定のグループポリシーへの LDAP ユーザの配置

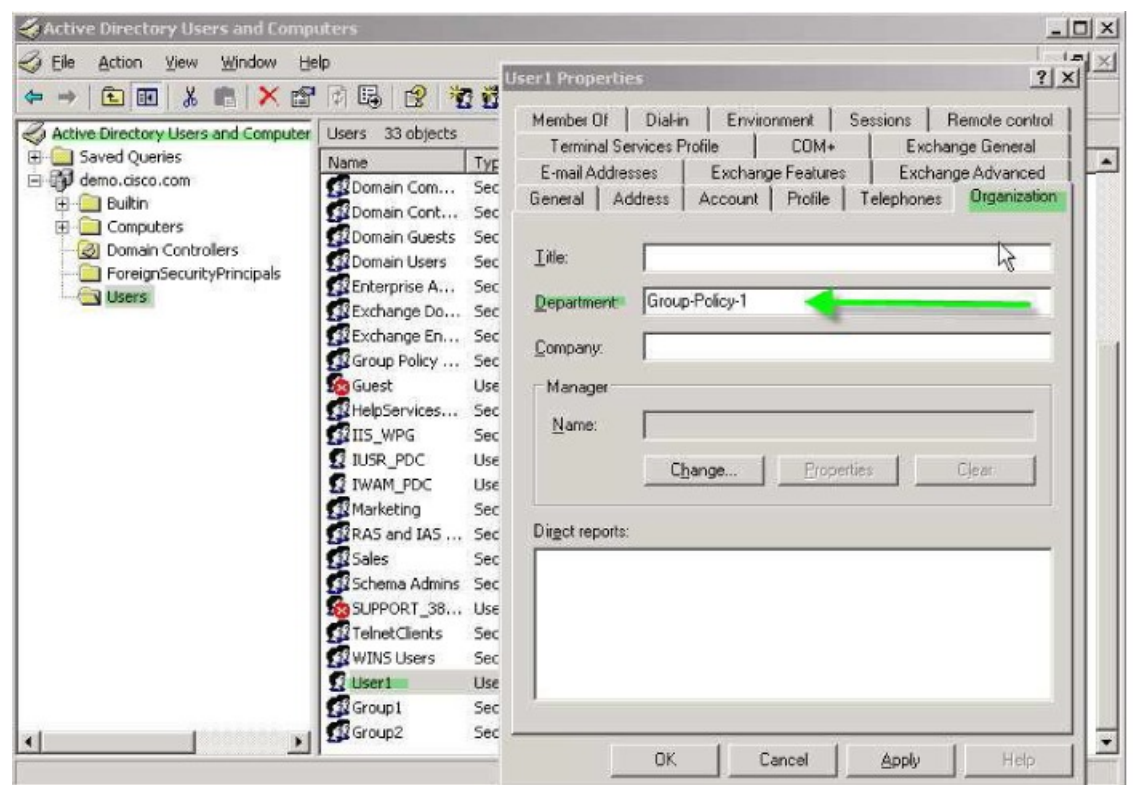
この例は、IPsec VPN クライアント、AnyConnect SSL VPN クライアント、クライアントレス SSL VPN など、どの接続タイプにも適用されます。この例では、User1 はクライアントレス SSL VPN 接続経由で接続します。

LDAP ユーザを特定のグループポリシーに配置するには、[Organization] タブの [Department] フィールドを使用してグループポリシーの名前を入力します。次に、属性マップを作成し、[Department] を Cisco 属性である IETF-Radius-Class にマッピングします。

認証時、ASA はサーバから [Department] の値を取得し、その値を IETF-Radius-Class にマッピングして、User1 をグループポリシーに配置します。

### 手順

- ステップ 1** ユーザ名を右クリックして、[Properties] ダイアログボックスの [Organization] タブを開き、[Department] フィールドに「**Group-Policy-1**」と入力します。



- ステップ 2** LDAP コンフィギュレーションの属性マップを定義します。

AD 属性 Department を Cisco 属性 IETF-Radius-Class にマッピングします。

```
hostname (config) # ldap attribute-map group_policy
hostname (config-ldap-attribute-map) # map-name Department IETF-Radius-Class
```

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

AAA サーバグループ MS\_LDAP のホスト 10.1.1.2 に対して AAA サーバホスト 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 `group_policy` 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 group_policy
```

**ステップ 4** サーバの [Department] フィールドに入力されているグループポリシー `Group-policy-1` を ASA に追加し、ユーザに割り当てる必須ポリシー属性を設定します。

```
hostname(config)# group-policy Group-policy-1 external server-group LDAP_demo
hostname(config-aaa-server-group)#
```

**ステップ 5** このユーザとしてVPN接続を確立し、Group-Policy1からの属性（およびその他に適用可能な、デフォルトのグループポリシーからの属性）がセッションに継承されていることを確認します。

**ステップ 6** 特権 EXEC モードで `debug ldap 255` コマンドをイネーブルにして、ASA とサーバの間の通信をモニタします。このコマンドからの出力の例を次に示します。これは、主要なメッセージがわかるように編集済みです。

```
[29] Authentication successful for user1 to 10.1.1.2
[29] Retrieving user attributes from server 10.1.1.2
[29] Retrieved Attributes:
[29] department: value = Group-Policy-1
[29] mapped to IETF-Radius-Class: value = Group-Policy-1
```

---

## AnyConnect トンネルのスタティック IP アドレス割り当ての適用

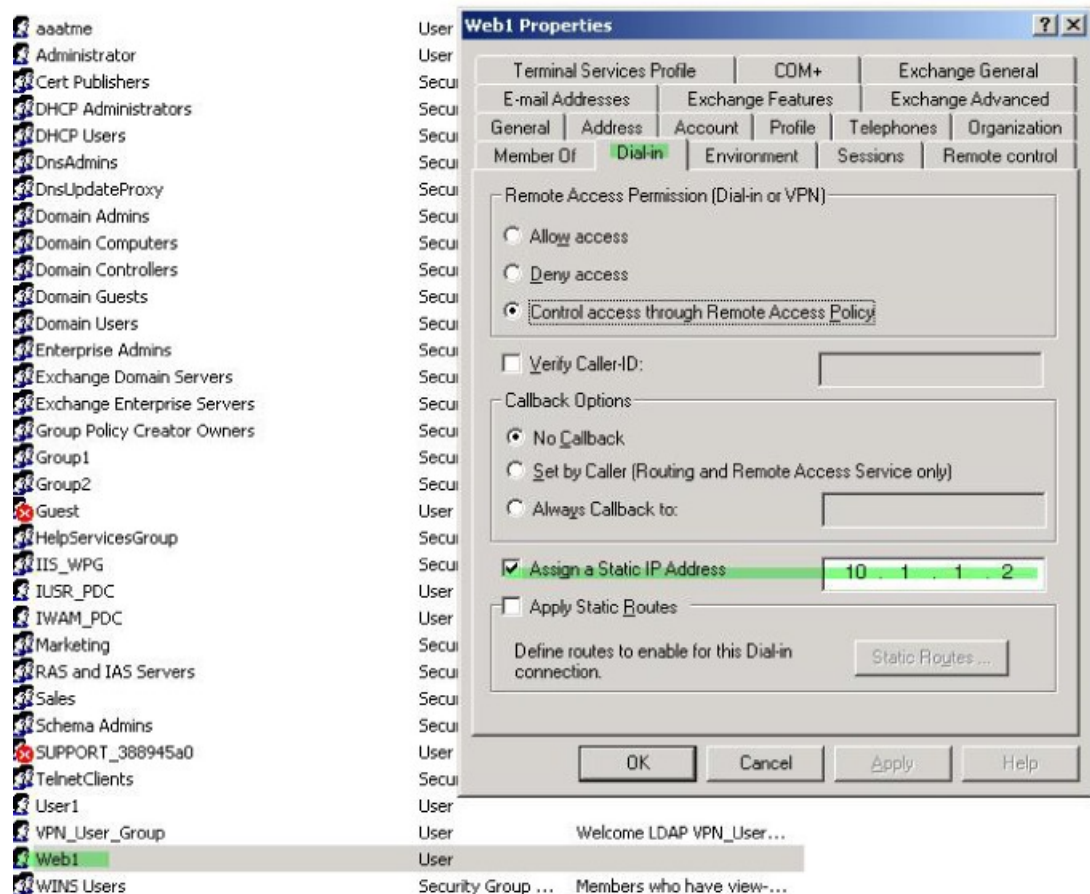
この例は、IPsec クライアントや SSL VPN クライアントなどのフルトンネルクライアントに適用されます。

スタティック AnyConnect スタティック IP 割り当てを適用するには、AnyConnect クライアントユーザ 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 サーバの [Dialin] タブの [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。



- 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 サーバに関連付けます。

AAA サーバグループ `MS_LDAP` のホスト `10.1.1.2` に対して AAA サーバ 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 AnyConnect クライアントとの接続を確立します。サーバで設定され、ASA にマッピングされた IP アドレスをユーザ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 : AnyConnect または SSL VPN クライアント

値	トンネリング プロトコル
64	IPsec (IKEv2)

<sup>1</sup> (1) IPsec と L2TP over IPsec は同時には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。

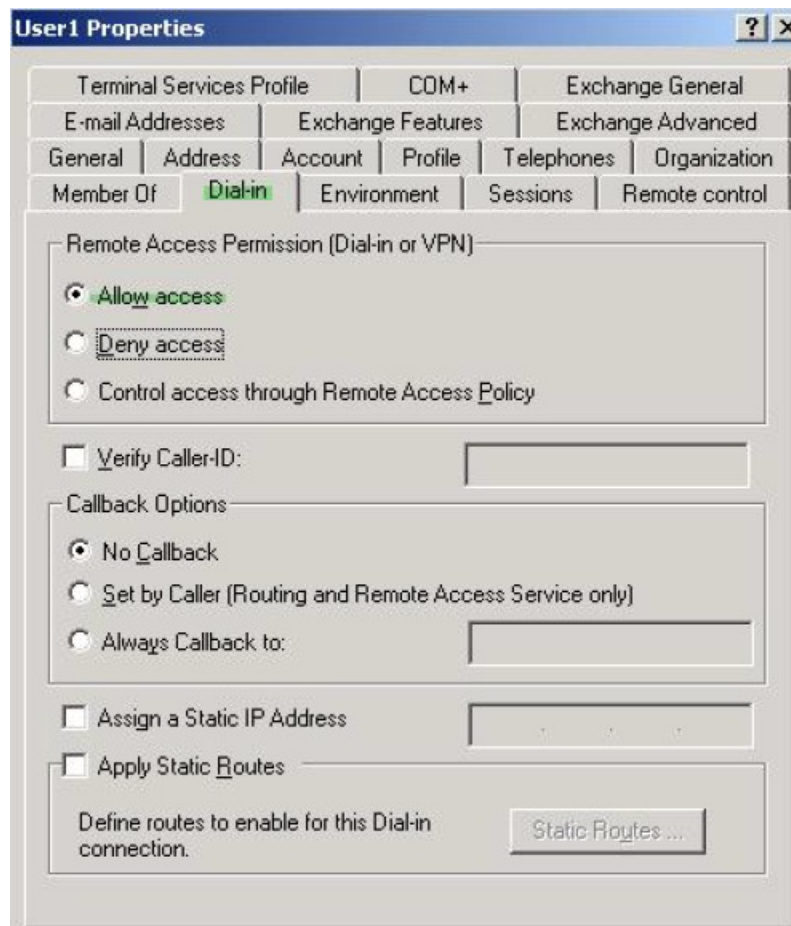
<sup>2</sup> (2) 注 1 を参照。

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 AnyConnect の両方の接続を許可するがクライアントレス SSL 接続を拒否する属性マップを作成します。

- a) マップ tunneling\_protocols を作成します。

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

- b) [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
```

- c) 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 サーバに関連付けます。

- a) AAA サーバグループ MS\_LDAP でホスト 10.1.1.2 の AAA サーバホスト 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
```

- b) 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。

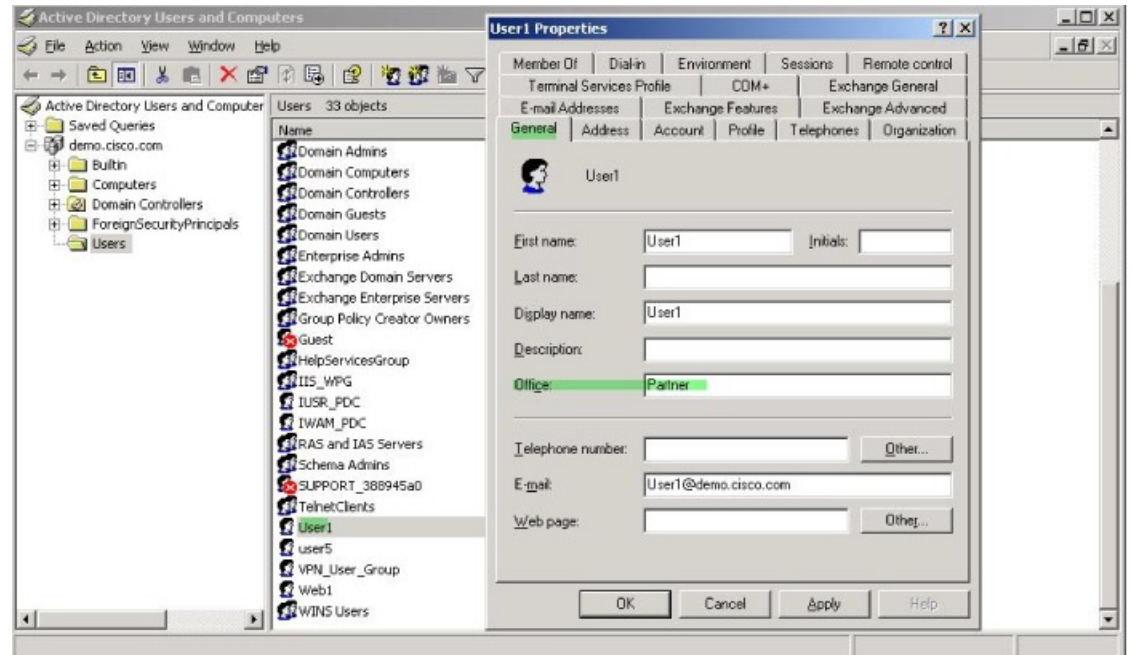
## ログオン時間と Time-of-Day ルールの適用

次の例では、クライアントレス SSL ユーザ（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。

## 手順

ステップ1 ユーザを選択して、[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 サーバに関連付けます。

AAA サーバグループ `MS_LDAP` のホスト `10.1.1.2` に対して AAA サーバ 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
```