

ASA 8.x:Windows用のAnyConnect SSL VPN CACスマートカードの設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[Cisco ASA の設定](#)

[導入に関する考慮事項](#)

[認証、許可、アカウンティング \(AAA\) 設定](#)

[LDAP サーバの設定](#)

[証明書の管理](#)

[キーの生成](#)

[ルート CA 証明書のインストール](#)

[ASA の登録と ID 証明書のインストール](#)

[AnyConnect VPN の設定](#)

[IP アドレスプールの作成](#)

[トンネルグループおよびグループ ポリシーの作成](#)

[トンネルグループ インターフェイスおよびイメージの設定](#)

[証明書の照合ルール \(OCSP が使用される場合\)](#)

[OCSP の設定](#)

[OCSP レスポンド証明書の設定](#)

[OCSP を使用するための CA の設定](#)

[OCSP ルールの設定](#)

[Cisco AnyConnect Client の設定](#)

[Cisco Anyconnect VPN Client のダウンロード - Windows](#)

[Cisco Anyconnect VPN Client の起動 - Windows](#)

[新規接続](#)

[リモート アクセスの開始](#)

[付録 A : LDAP マッピングおよび DAP](#)

[シナリオ1 : リモートアクセス許可ダイヤルインを使用したActive Directoryの強制 : アクセスの許可/拒否](#)

[Active Directory の設定](#)

[ASA の設定](#)

[シナリオ2 : グループメンバーシップを使用したアクセスの許可/拒否によるActive Directoryの適用](#)

[Active Directory の設定](#)

[ASA の設定](#)

[シナリオ3 : 複数のmemberOf属性のダイナミックアクセスポリシー](#)

[ASA の設定](#)

[付録 B : ASA CLI 設定](#)

[付録 C : トラブルシューティング](#)

[AAA および LDAP のトラブルシューティング](#)

[例1 : 正しい属性マッピングを使用した接続の許可](#)

[例2 : 誤って設定されたCisco属性マッピングによる接続の許可](#)

[DAP のトラブルシューティング](#)

[例1:DAPで許可される接続](#)

[例2:DAPとの接続の拒否](#)

[認証局および OCSP のトラブルシューティング](#)

[付録 D : MS 内の LDAP オブジェクトの確認](#)

[LDAP Viewer](#)

[Active Directory サービス インターフェイス エディタ](#)

[付録 E](#)

[関連情報](#)

はじめに

このドキュメントでは、認証用の Common Access Card (CAC) を使用して Windows 用の AnyConnect VPN リモート アクセスを実現する、Cisco 適応型セキュリティ アプライアンス (ASA) 上でのサンプル設定について説明します。

このドキュメントでは、Cisco ASA と Adaptive Security Device Manager (ASDM) 、 Cisco AnyConnect VPN Client、Microsoft Active Directory (AD) および Lightweight Directory Access Protocol (LDAP) の設定について扱います。

このガイドの設定では、Microsoft AD および LDAP サーバを使用します。またこのドキュメントでは、OCSP、LDAP 属性マップ、ダイナミック アクセス ポリシー (DAP) などの高度な機能についても扱います。

前提条件

要件

Cisco ASA、Cisco AnyConnect Client、Microsoft AD/LDAP、および公開キー インフラストラクチャ (PKI) についての基本的な理解があれば、完全な設定を理解するために有益です。AD グループ メンバシップ、ユーザ プロパティ、および LDAP オブジェクトについて理解していれば、証明書属性と AD/LDAP オブジェクトの間での許可プロセスの関連付けに役立ちます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- ソフトウェア バージョン 8.0(x) 以降が稼働する Cisco 5500 シリーズ適応型セキュリティ アプライアンス (ASA)
- ASA 8.x 用の Cisco Adaptive Security Device Manager (ASDM) バージョン 6.x

- Cisco AnyConnect VPN Client (Windows 版)

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな (デフォルト) 設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

Cisco ASA の設定

このセクションでは、ASDM を使用した Cisco ASA の設定について扱います。ここでは、SSL AnyConnect 接続を経由した VPN リモート アクセス トンネルを配備するために必要なステップについて説明します。認証には CAC 証明書が使用され、証明書内のユーザ プリンシパル名 (UPN) 属性が、許可のために Active Directory に取り込まれます。

導入に関する考慮事項

- このガイドでは、インターフェイス、DNS、NTP、ルーティング、デバイス アクセス、ASDM アクセスなどの基本的な設定については扱いません。ネットワーク オペレータはこれらの設定をよく理解しているものとします。

詳細は、『[マルチファンクション セキュリティ アプライアンス](#)』を参照してください。

- 赤色で強調表示されているセクションは、基本的な VPN アクセスのために必要な必須の設定です。たとえば、VPN トンネルは CAC カードで設定でき、OCSP チェック、LDAP マッピング、ダイナミック アクセス ポリシー (DAP) チェックを行う必要はありません。DoD では OCSP チェックが規定されていますが、OCSP を設定しなくてもトンネルは機能します。
- 青色で強調表示されているセクションは、設計にセキュリティを追加するために含めることができる高度な機能です。
- ASDM と AnyConnect/SSL VPN は、同じインターフェイスの同じポートを使用できません。一方または他方のポートを変更してアクセスすることを推奨します。たとえば、ASDM をポート 445 にし、AC/SSL VPN は 443 のままにします。ASDM への URL アクセスは、8.x で変更されました。https://<ip_address>:<port>/admin.html を使用してください。
- 必要な ASA イメージは最低 8.0.2.19 で、ASDM 6.0.2 です。
- AnyConnect/CAC は Vista でサポートされています。
- ポリシーを強制するための LDAP およびダイナミック アクセス ポリシーのマッピングの例については、[付録 A を参照してください](#)。
- LDAP オブジェクトを MS でチェックする方法については、「[付録 D](#)」を参照してください。
- ファイアウォール設定のためのアプリケーション ポートのリストについては、『[関連情報](#)』を参照してください。

認証、許可、アカウントिंग (AAA) 設定

Common Access Card (CAC) 内の証明書の使用は、DISA 認証局 (CA) サーバまたは自分の組織の CA サーバを通じて認証されます。証明書はネットワークへのリモート アクセス用に有効である必要があります。認証に加えて、Microsoft Active Directory または Lightweight Directory Access Protocol (LDAP) の使用が許可されている必要もあります。米国国防総省 (DoD) では、ユーザプリンシパル名 (UPN) 属性を許可用に使用することを求めています。これは証明書の Subject Alternative Name (SAN) セクションの一部です。UPN または EDI/PI は、1234567890@mil のフォーマットである必要があります。これらの設定では、ASA 内の AAA サーバを LDAP サーバと一緒に許可用に構成する方法を示しています。LDAP オブジェクト マッピングの追加の設定については、[付録 A](#) を参照してください。

LDAP サーバの設定

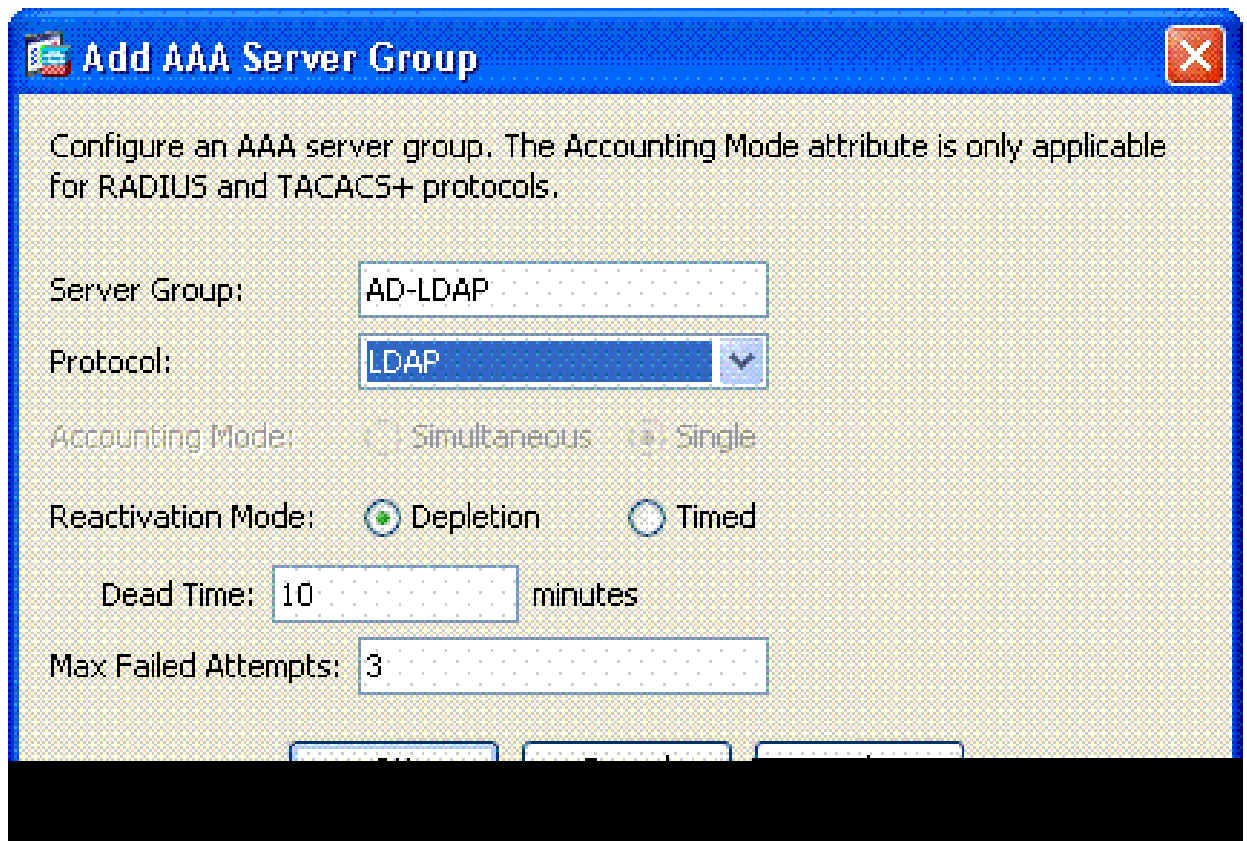
次のステップを実行します。

1. [Remote Access VPN] > [AAA Setup] > [AAA Server Group] を選択します。
2. AAA サーバグループ テーブルで、[Add 3] をクリックします。
3. サーバグループ名を入力し、プロトコル オプション ボタンで [LDAP] を選択します。図 1 を参照してください。
4. 選択されたグループ テーブルで、[Add] をクリックします。作成したサーバが前のテーブルで強調表示されていることを確認します。
5. AAA サーバの編集ウィンドウで、次の手順を実行します。図 2 を参照してください。

注：このタイプの接続にLDAP/ADが設定されている場合は、Enable LDAP over SSLオプションを選択します。

- a. LDAP が配置されるインターフェイスを選択します。このガイドでは、インターフェイスの内側であることを示しています。
- b. サーバの IP アドレスを入力します。
- c. [Server Port] を入力します。デフォルトの LDAP ポートは 389 です。
- d. [Server Type] を選択します。
- e. [Base DN] を入力します。これらの値は AD/LDAP 管理者に問い合わせてください。

図1



- f. [Scope] オプションで、該当する回答を選択します。これはベース DN によって異なります。AD/LDAP 管理者に連絡して支援を求めてください。
- g. [Naming Attribute] に、userPrincipalName と入力します。これは AD/LDAP サーバ内でユーザ許可に使用する属性です。
- h. [Login DN] に管理者 DN を入力します。

注：ユーザには、ユーザオブジェクトとグループメンバーシップを含むLDAP構造を表示または検索する管理者権限または権限があります。

- i. [Login Password] に管理者のパスワードを入力します。
- j. LDAP 属性は [None] のままにします。

図 2

注：このオプションは、後で設定で使用して、認可のために他のAD/LDAPオブジェクトを追加します。

k. [OK] を選択します。

6. [OK] を選択します。

証明書の管理

ASA に証明書をインストールするには、2つのステップがあります。最初に、必要な CA 証明書

(ルートおよび追加の認証局)をインストールします。次に、ASA を特定の CA に登録し、ID 証明書を取得します。DoD PKI では、Root CA2、Class 3 Root、ASA の登録先の CA## 中間証明書、ASA ID 証明書、および OCSP 証明書を使用します。ただし OCSP を使用しない場合は、OCSP 証明書をインストールする必要はありません。

注：ルート証明書と、デバイスのID証明書の登録方法を取得するには、セキュリティ POCに連絡してください。ASA のリモート アクセスの場合、SSL 証明書で十分です。デュアル SAN 証明書は必要ありません。

注：ローカルマシンにもDoD CAチェーンがインストールされている必要があります。証明書は Internet Explorer を使用して Microsoft 証明書ストアから表示できます。DoD は、すべての CA を自動的にマシンに追加するバッチ ファイルを提供しています。詳細については、お客様の PKI POC にお問い合わせください。

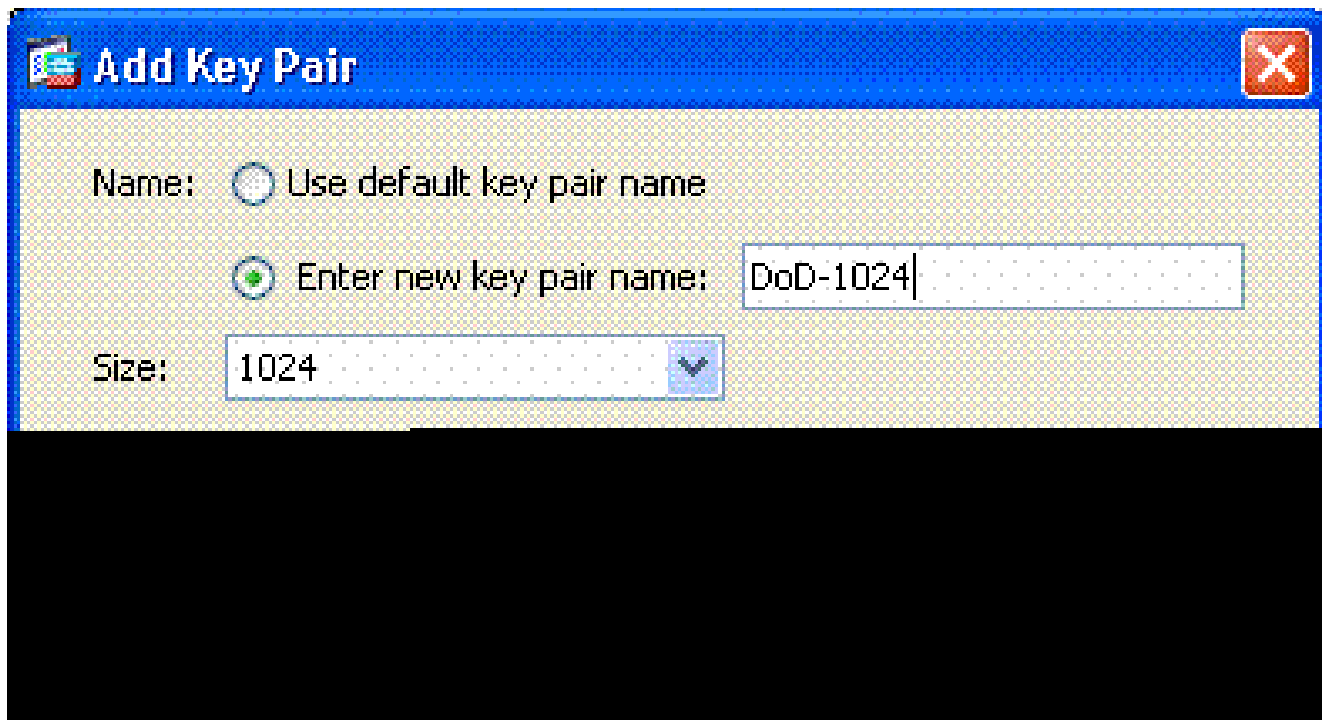
注：ユーザ認証に必要なCAは、DoD CA2とクラス3のルート、およびASA証明書を発行したASA IDとCA中間証明書のみです。現行のすべての CA 中間証明書は CA2 および Class 3 Root チェーンに該当するため、CA2 および Class 3 Root が追加される限り信頼されます。

キーの生成

次のステップを実行します。

1. [Remote Access VPN] > [Certificate Management] > [Identity Certificate] > [Add] を選択します。
2. [Add a new id certificate] を選択し、キー ペア オプションの [New] を選択します。
3. [Add Key Pair] ウィンドウで、キー名に DoD-1024 と入力します。新しいキーを追加するオプション ボタンをクリックします。図 3 を参照してください。

図 3



4. キーのサイズを選択します。
5. [Usage] は [General Purpose] のままにします。
6. [Generate Now] をクリックします。

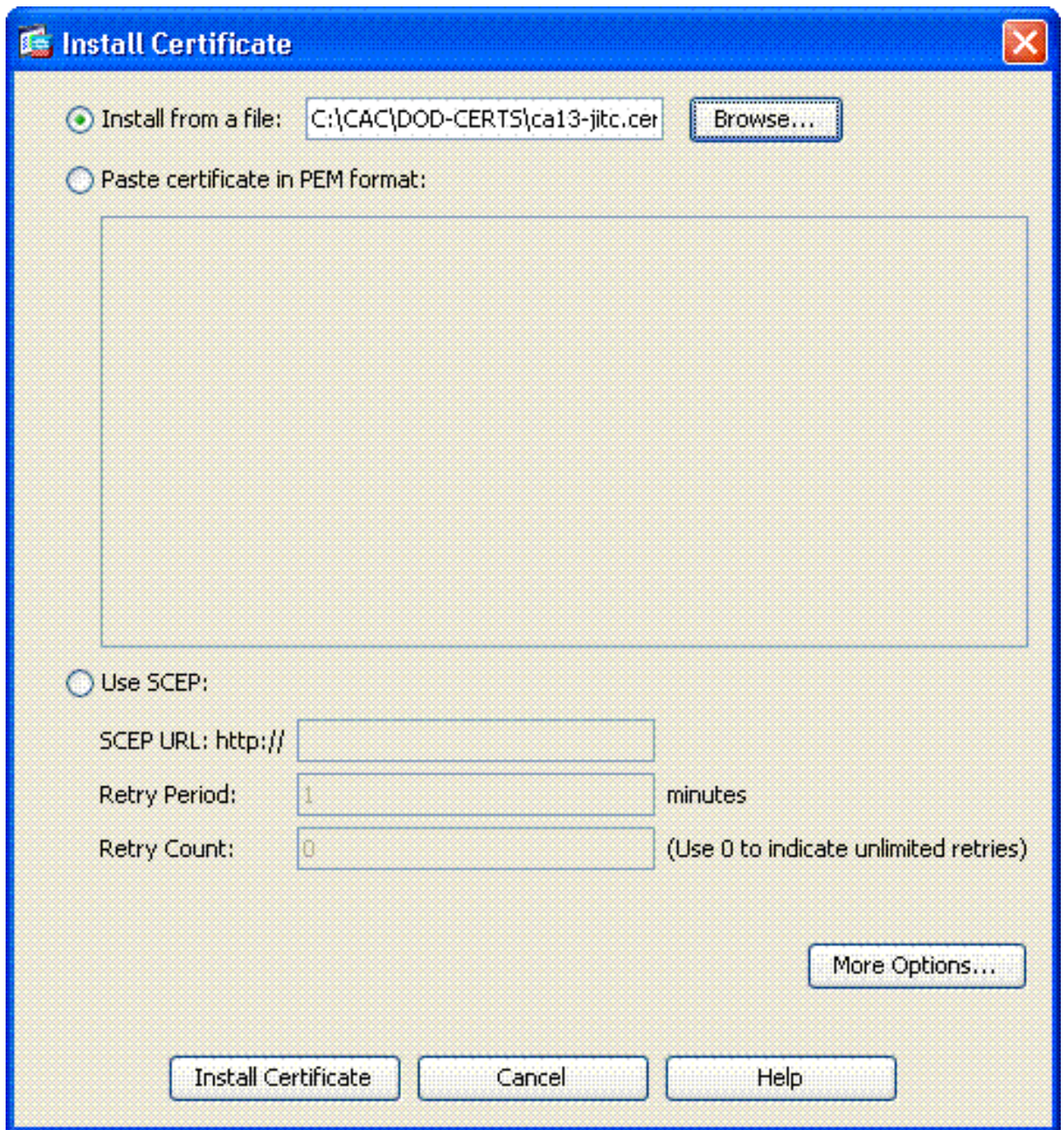
注: DoDルートCA 2は2048ビットキーを使用します。この CA を使用できるようにするには、2048 ビットのキーペアを使用する 2 番目のキーを生成する必要があります。上記の手順を使用して、2 番目のキーを追加してください。

ルート CA 証明書のインストール

次のステップを実行します。

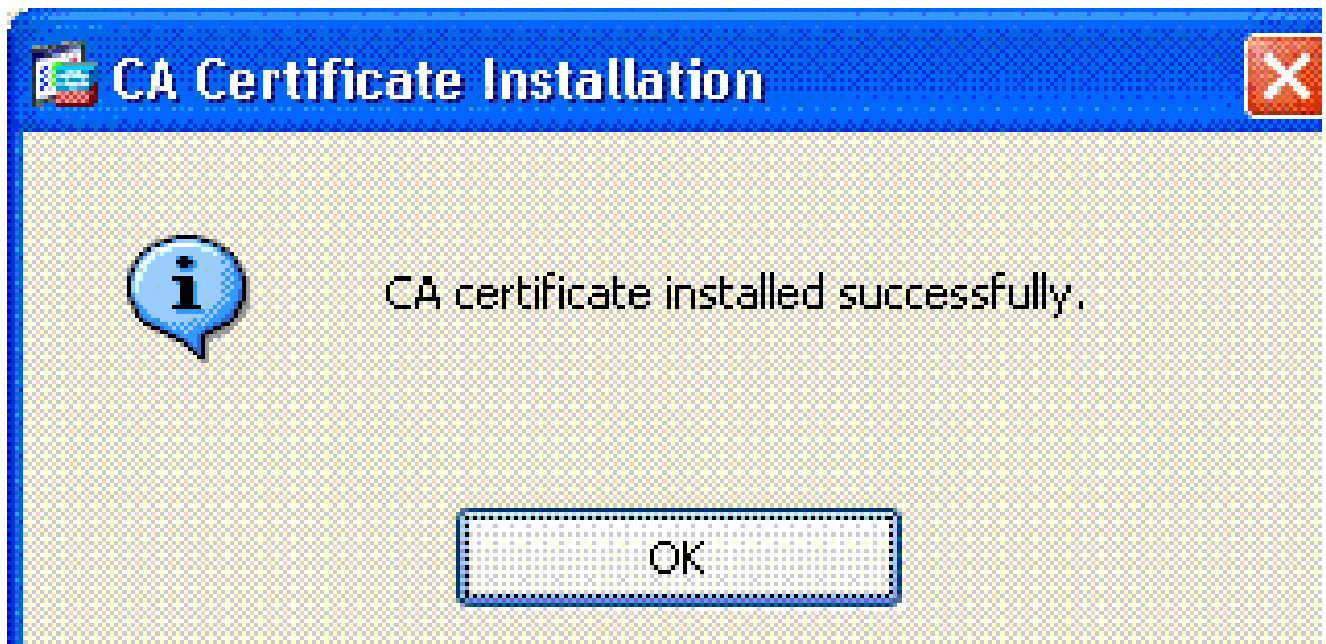
1. [Remote Access VPN] > [Certificate Management] > [CA Certificate] > [Add] を選択します。
2. [Install from File] を選択し、証明書を参照します。
3. [Install Certificate] を選択します。

図4：ルート証明書のインストール



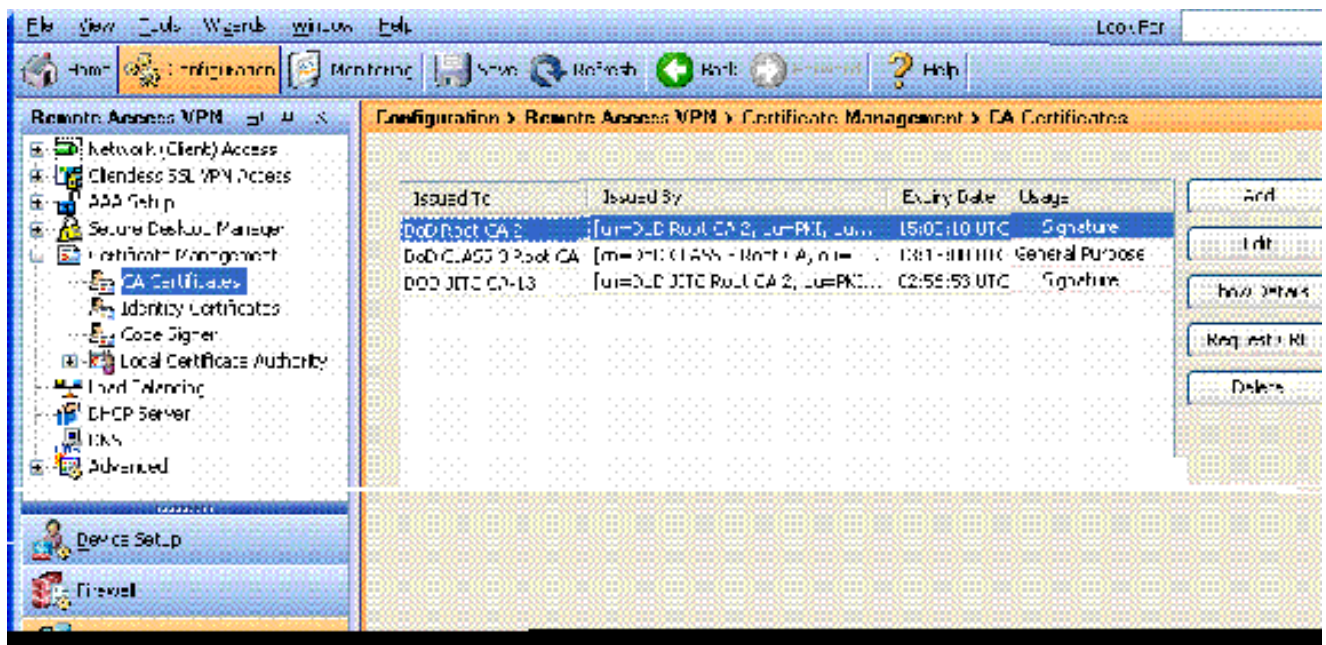
4. このウィンドウが表示されます。図 5 を参照してください。

図 5 :



注：インストールするすべての証明書について、手順1～3を繰り返します。DoD PKIでは、ルートCA 2、クラス3ルート、CA##中間、ASA ID、およびOCSPサーバのそれぞれの証明書が必要です。OCSPを使用しない場合、OCSP証明書は不要です。

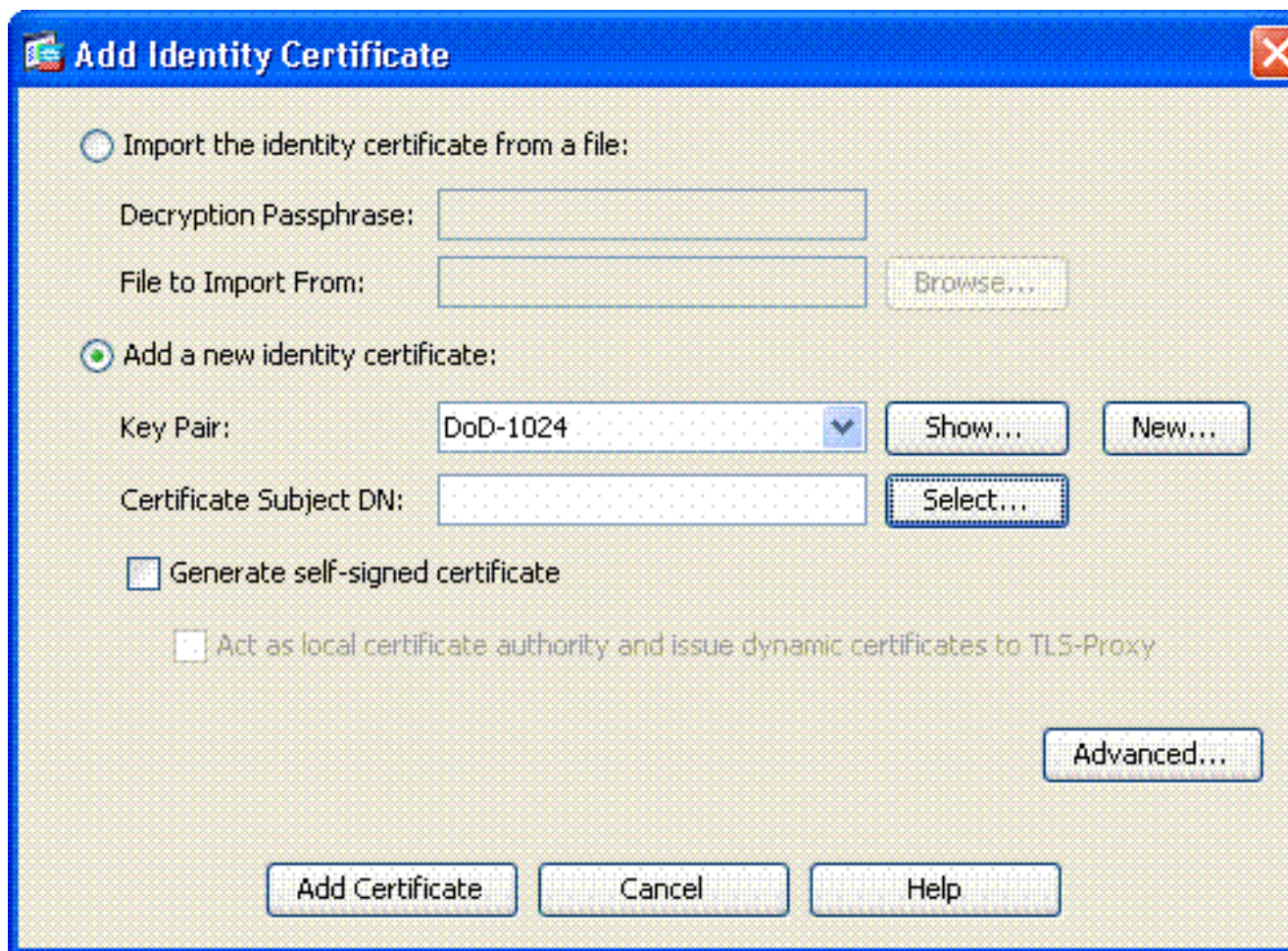
図6：ルート証明書のインストール



ASA の登録と ID 証明書のインストール

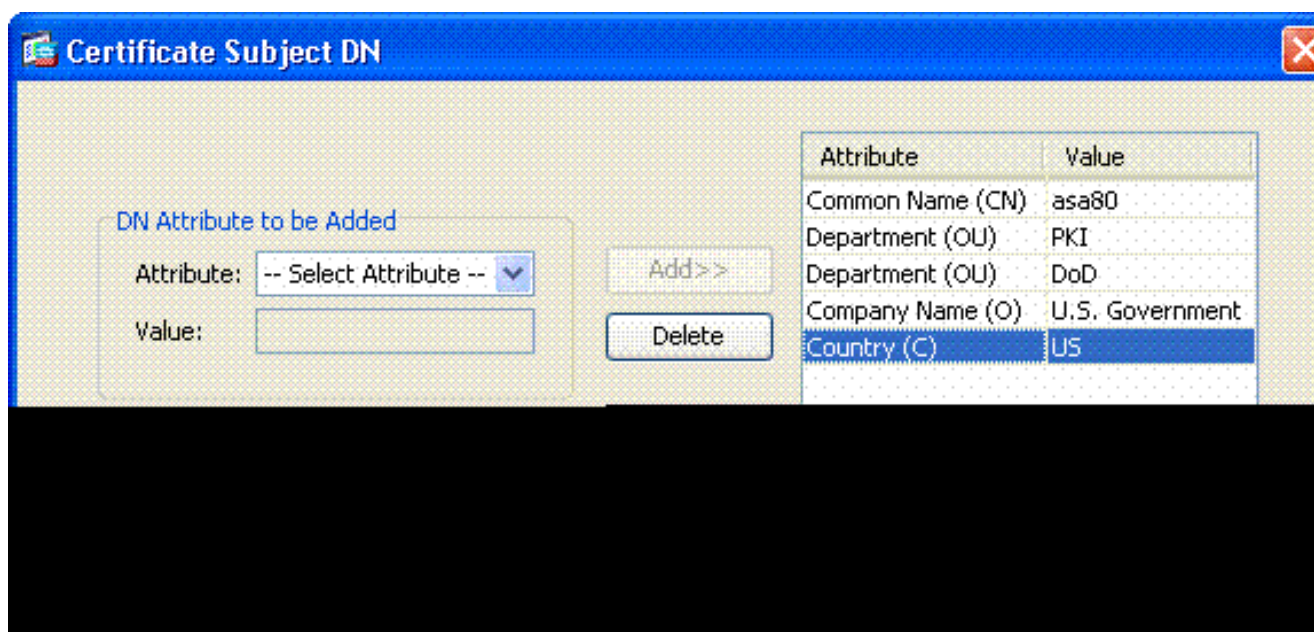
1. [Remote Access VPN] > [Certificate Management] > [Identity Certificate] > [Add] を選択します。
2. [Add a new id certificate] を選択します。
3. DoD-1024 キーペアを選択します。図7を参照してください。

図7:ID証明書のパラメータ



4. [Certificate Subject DN] ボックスに移動し、[Select] を選択します。
5. [Certificate Subject DN] ウィンドウで、デバイスの情報を入力します。図 8 の例を参照してください。

図8:DNの編集



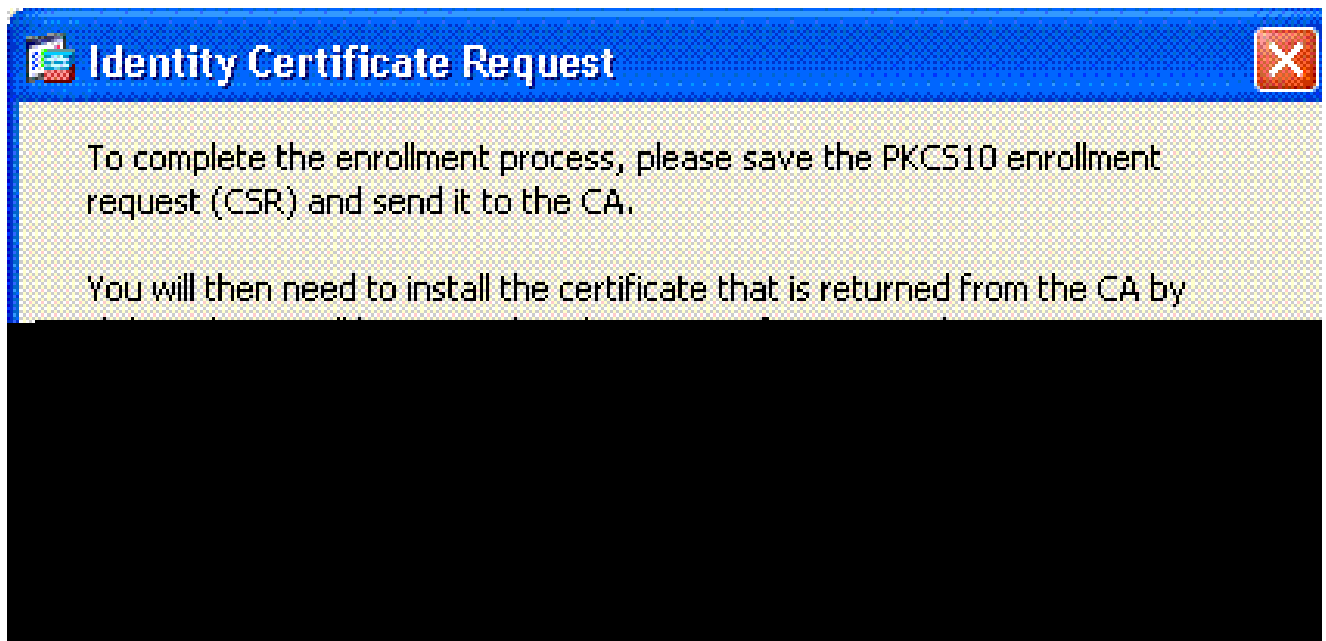
6. [OK] を選択します。

注：サブジェクトDNを追加するときは、システムに設定されているデバイスのホスト名を使用していることを確認してください。必須フィールドについては PKI POC から聞き取ることができます。

7. [Add Certificate] を選択します。

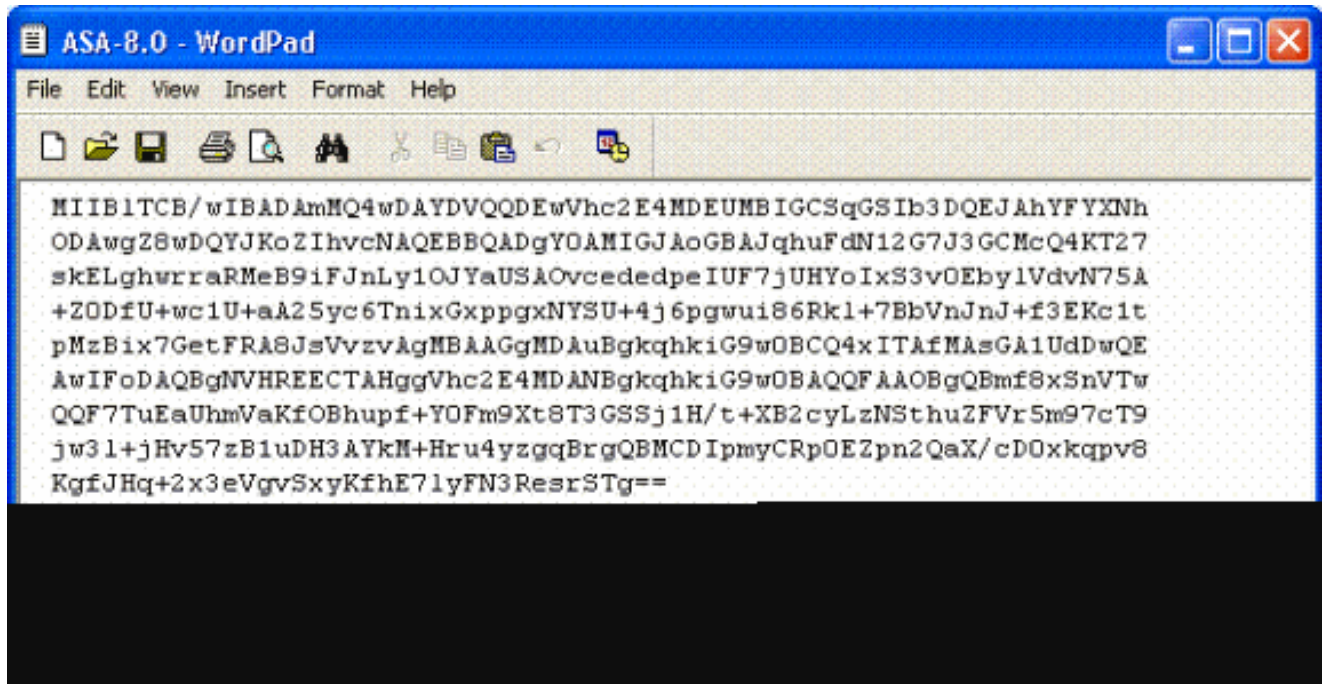
8. 要求を保存するディレクトリを選択するには、[Browse] をクリックします。図 9 を参照してください。

図9：証明書要求



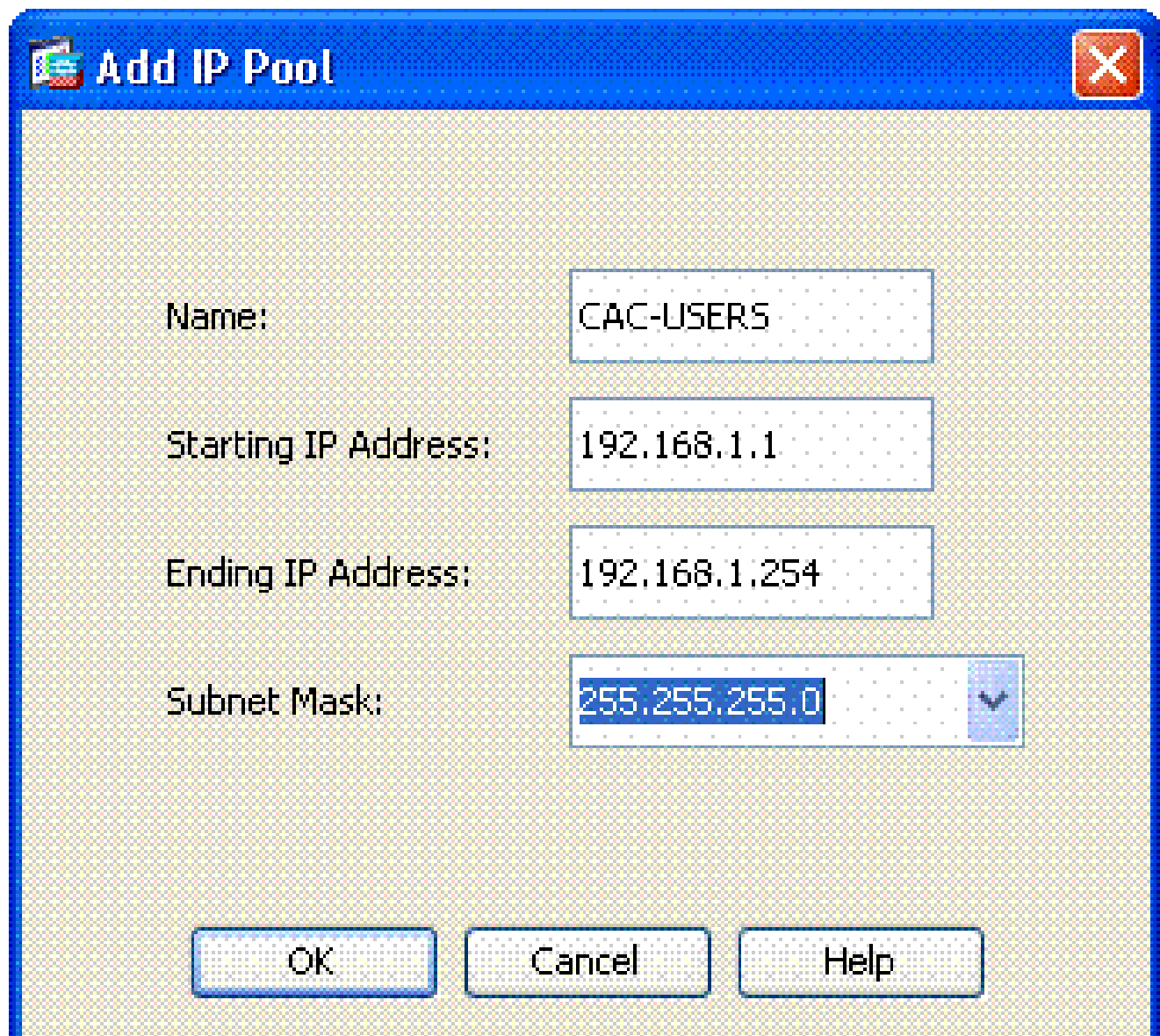
9. ファイルを WordPad で開き、適切なドキュメントに要求をコピーして、お客様の PKI POC に送信します。図 10 を参照してください。

図10：登録要求



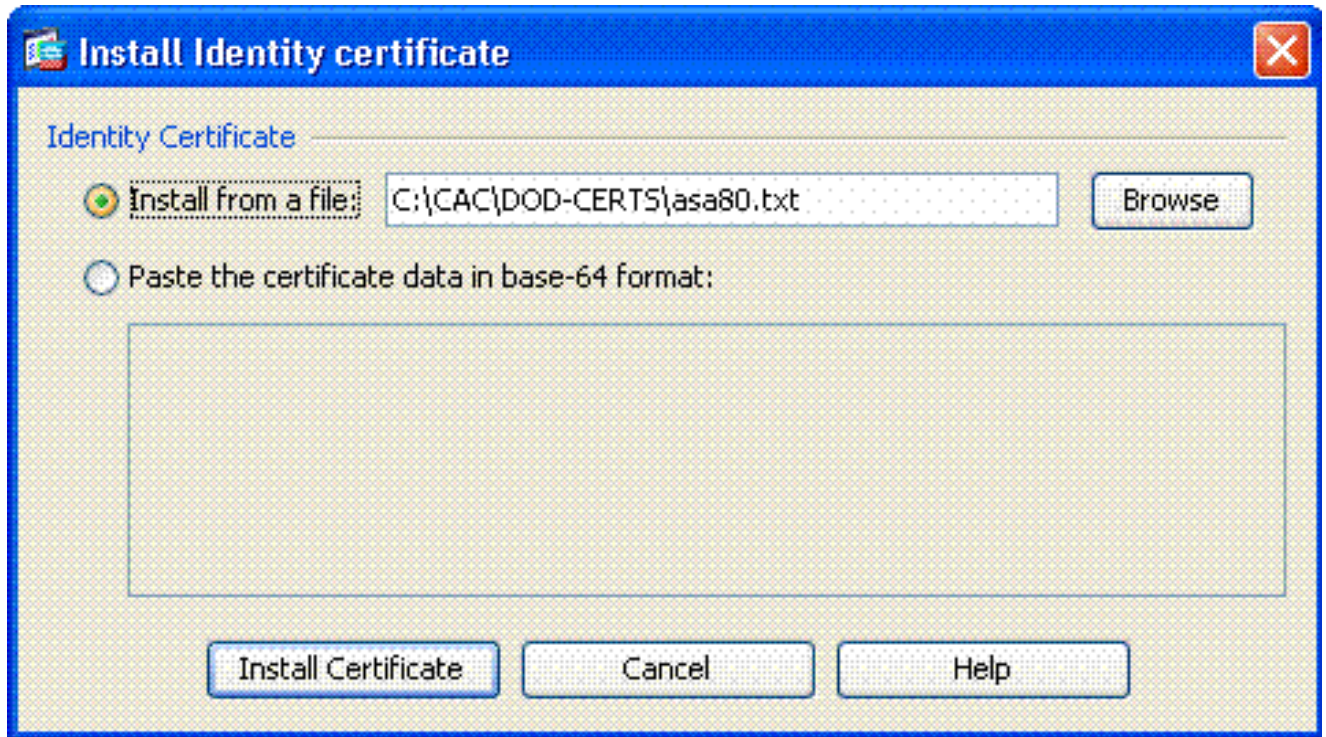
10. CA 管理者から証明書を受け取ったら、[Remote Access VPN] > [Certificate Management] > [ID Certificate] > [Install] を選択します。図 11 を参照してください。

図11:ID証明書のインポート



11. 証明書のインストール ウィンドウで、ID 証明書を参照し、[Install Certificate] を選択します。図 12 の例を参照してください。

図12:ID証明書のインストール



注：発行された証明書とキーペアを保存するために、ID証明書トラストポイントをエクスポートすることをお勧めします。これによって ASA 管理者は、RMA またはハードウェア障害の場合に証明書およびキーペアを新しい ASA にインポートすることができます。詳細は、『[トラストポイントのエクスポートおよびインポート](#)』を参照してください。

注：フラッシュメモリに設定を保存するには、SAVEをクリックします。

AnyConnect VPN の設定

ASDM で VPN パラメータを設定するには 2 つのオプションがあります。最初のオプションは SSL VPN ウィザードを使用することです。これは VPN 設定が初めてのユーザにとって、使いやすいツールです。2 つ目のオプションは、手動で各オプションを設定することです。この設定ガイドでは、手動による方法を使用します。

注:ACクライアントをユーザに提供する方法は2つあります。

1. Cisco の Web サイトからクライアントをダウンロードし、マシンにインストールすることができます。
 2. Web ブラウザ経由で ASA にアクセスすると、クライアントをダウンロードできます。
-

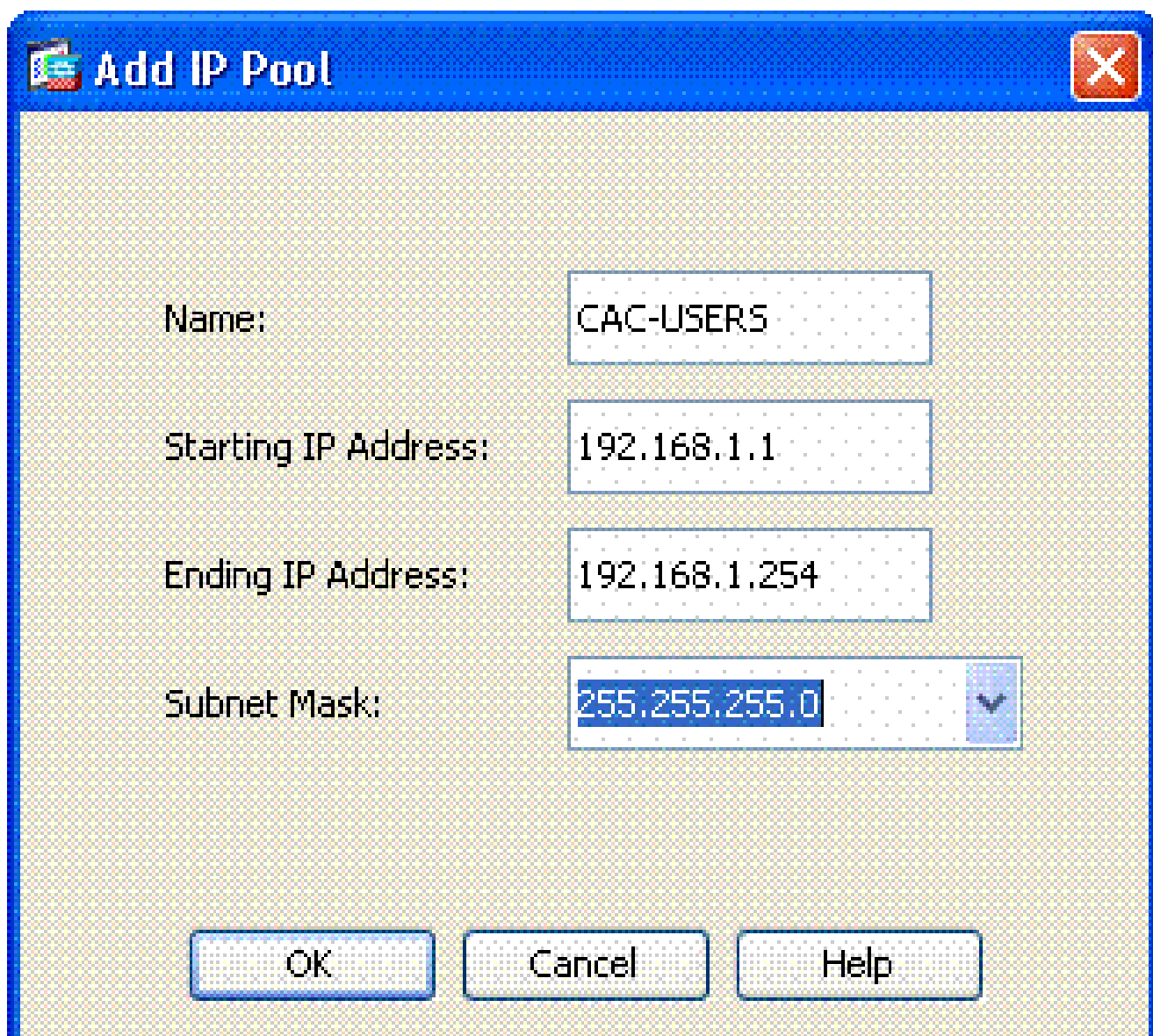
注：たとえば、<https://asa.test.com>です。このガイドでは 2 番目の方法を使用します。AC クライアントがクライアントマシンに完全にインストールされたら、AC クライアントをアプリケーションから起動します。

IP アドレス プールの作成

DHCP などの他の方法を使用する場合、これはオプションです。

1. [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Address Pools] を選択します。
2. [Add] をクリックします。
3. [Add IP Pool] ウィンドウで、IP プールの名前、開始および終了 IP アドレスを入力し、サブネットマスクを選択します。図 13 を参照してください。

図13:IPプールの追加



The screenshot shows a dialog box titled "Add IP Pool". The dialog contains the following fields and values:

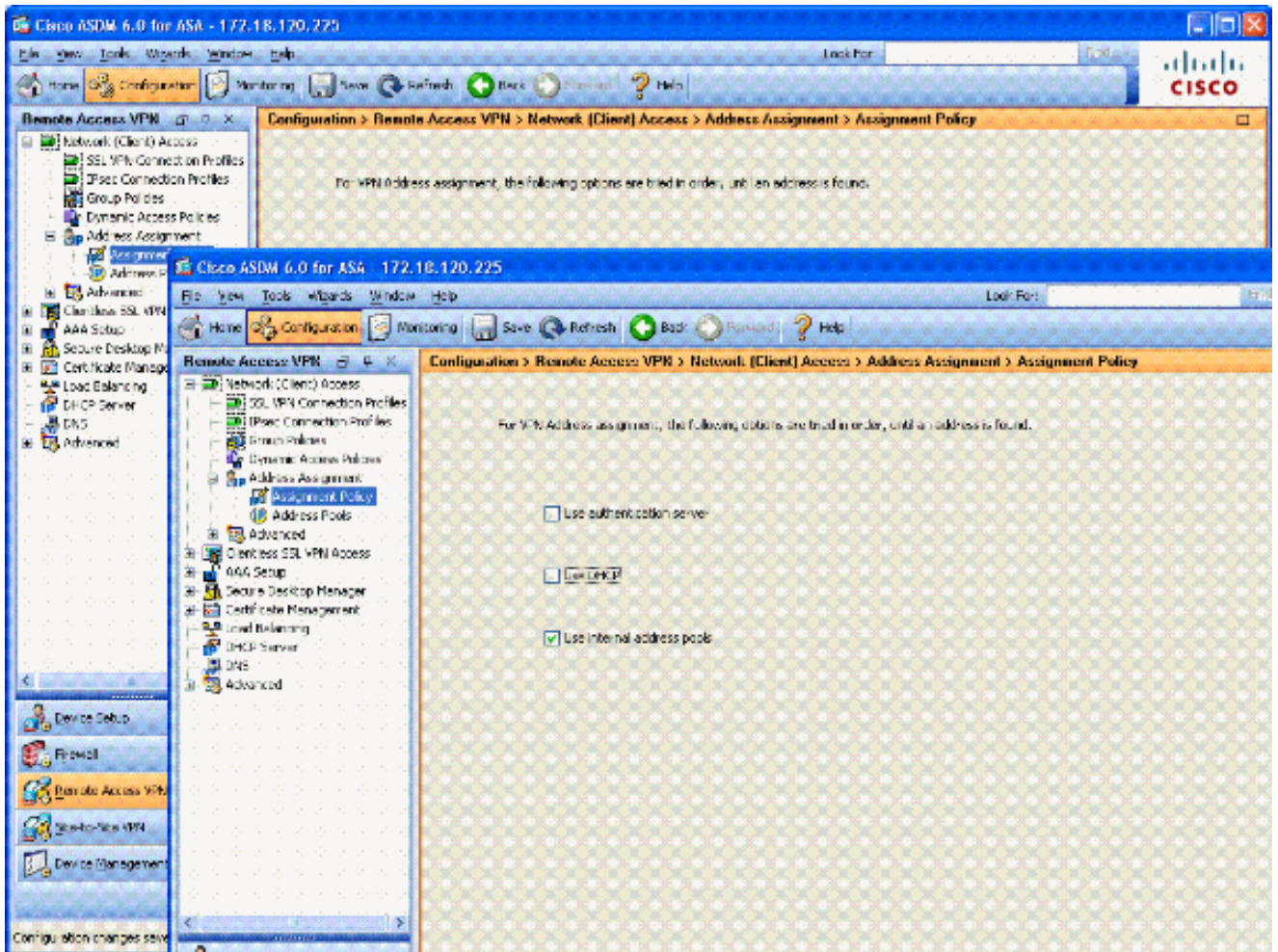
Field	Value
Name:	CAC-USERS
Starting IP Address:	192.168.1.1
Ending IP Address:	192.168.1.254
Subnet Mask:	255.255.255.0

At the bottom of the dialog, there are three buttons: "OK", "Cancel", and "Help".

4. [OK] を選択します。
5. [Remote Access VPN] > [Network (Client) Access] > [Address Assignment] > [Assignment Policy] を選択します。

- 適切な IP アドレス割り当て方法を選択します。このガイドでは、内部アドレスプールを使用します。図 14 を参照してください。

図14:IPアドレス割り当て方法



- [APPLY] をクリックします。

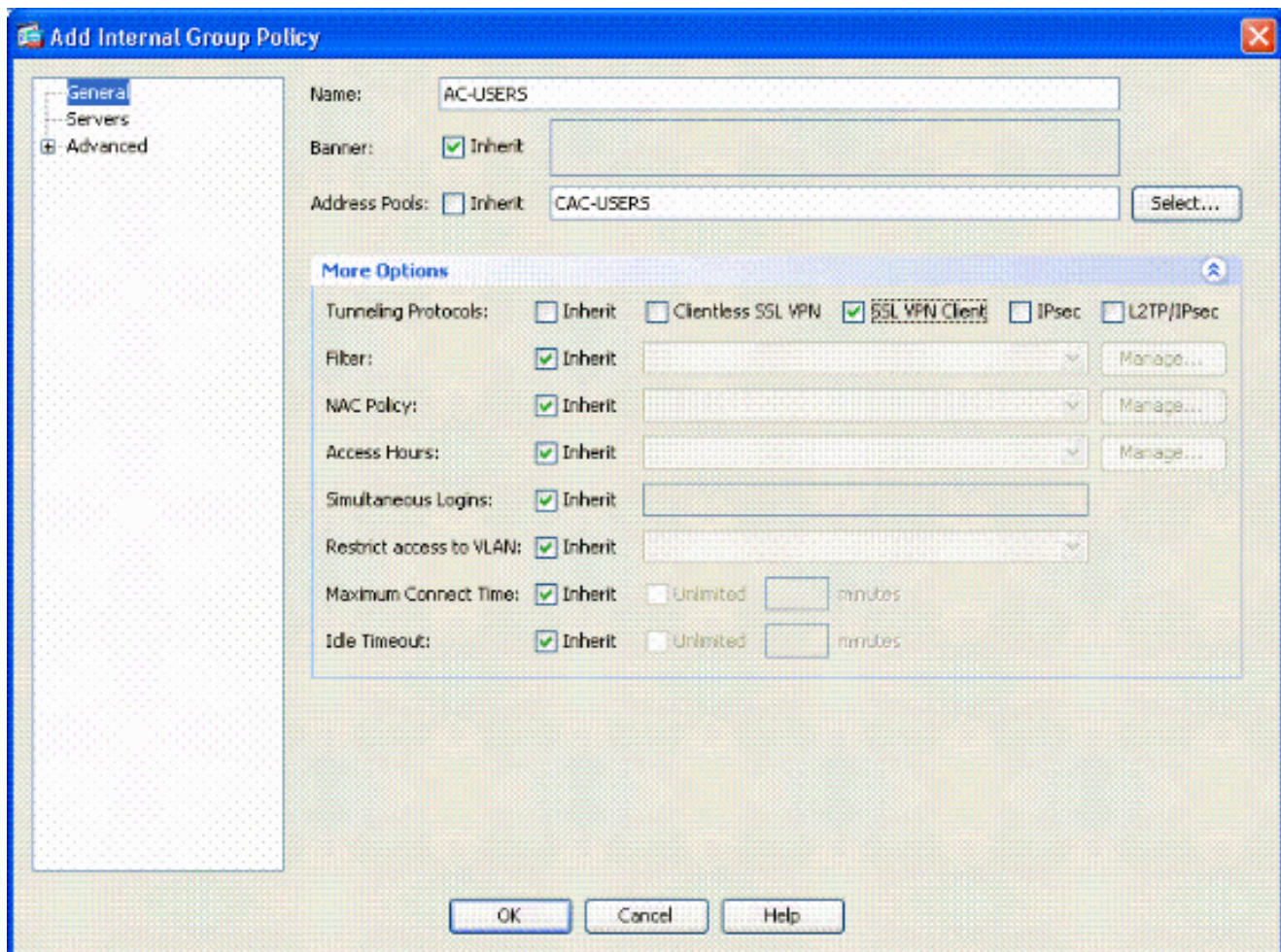
トンネルグループおよびグループポリシーの作成

グループポリシー

注：新しいポリシーを作成しない場合は、デフォルトの組み込みグループポリシーを使用できます。

- [Remote Access VPN] > [Network (Client) Access] > [Group Policies] を選択します。
- [Add] をクリックして、[Internal Group Policy] を選択します。
- [Add Internal Group Policy] ウィンドウで、[Name] テキストボックスにグループポリシーの名前を入力します。図 15 を参照してください。

図15：内部グループポリシーの追加

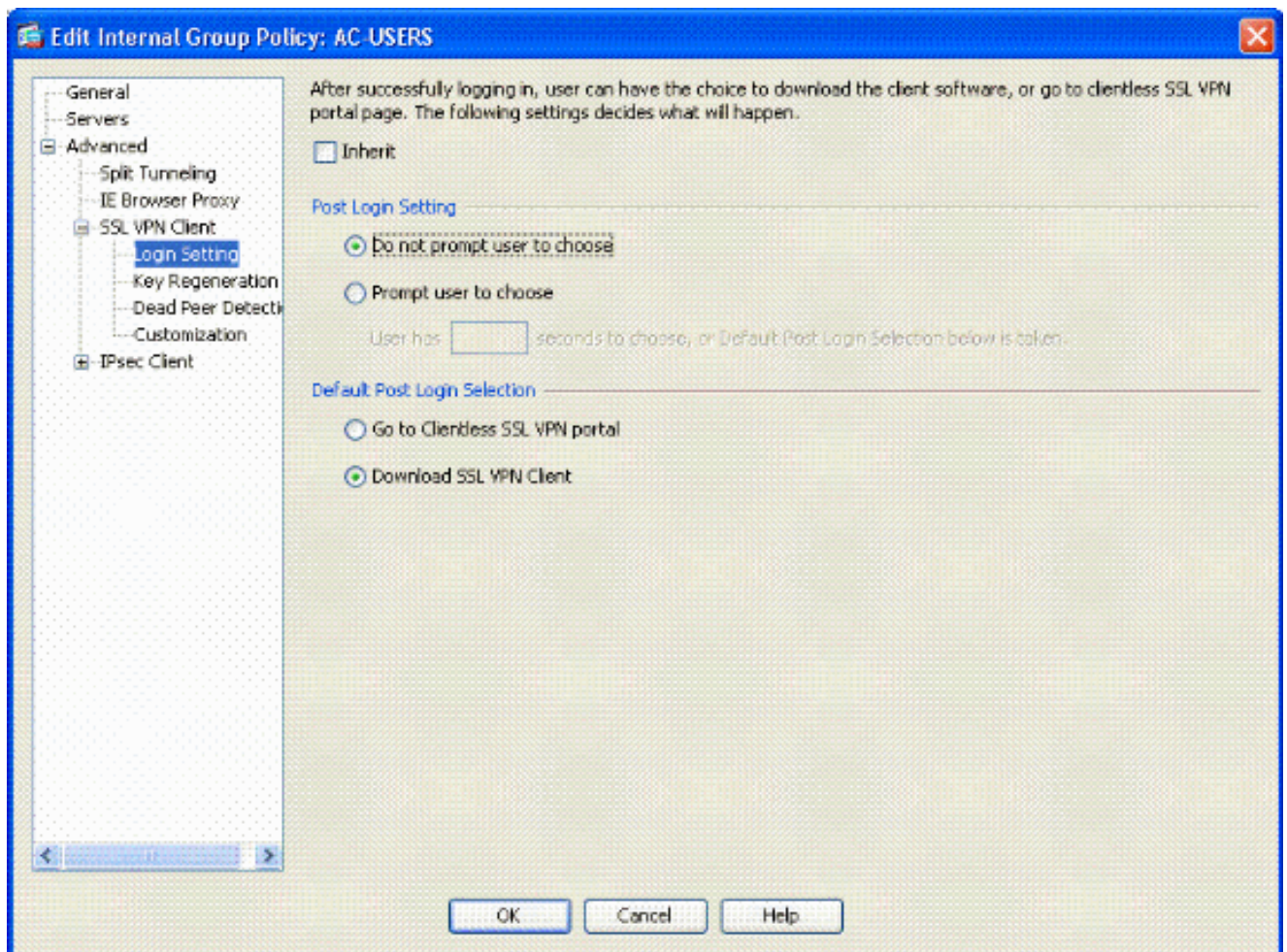


- a. [General] タブの [Tunneling Protocols] で [SSL VPN Client] オプションを選択します（Clientless SSL などの他のプロトコルを使用しない場合）。
- b. [Servers] セクションで、[inherit] チェックボックスのチェックを外し、DNS サーバおよび WINS サーバの IP アドレスを入力します。該当する場合は DHCP の範囲を入力します。
- c. [Servers] セクションで、デフォルト ドメインの [inherit] チェックボックスを選択解除し、適切なドメイン名を入力します。
- d. [General] タブで、アドレスプール セクションの [inherit] チェックを選択解除し、前の手順で作成されたアドレスプールを追加します。IP アドレス割り当てに別の方法を使用する場合、これを [inherit] のままにして、適宜変更します。
- e. 他のすべての設定タブは、デフォルト設定のままにします。

注：エンドユーザにACクライアントを提供する方法は2つあります。1つの方法は、Cisco.com にアクセスして AC クライアントをダウンロードすることです。別の方法は、ユーザが接続を試行したときに ASA でクライアントをユーザにダウンロードすることです。この例では後者の方法を示します。

4. 次に、[Advanced] > [SSL VPN Client] > [Login Settings] を選択します。図 16 を参照してください。

図16：内部グループポリシーの追加



- a. [Inherit] チェックボックスを選択解除します。
- b. [Post Login Setting] は、ご使用の環境に合ったほうを選択します。
- c. [Post Login Selection] は、ご使用の環境に合ったほうを選択します。
- d. [OK] を選択します。

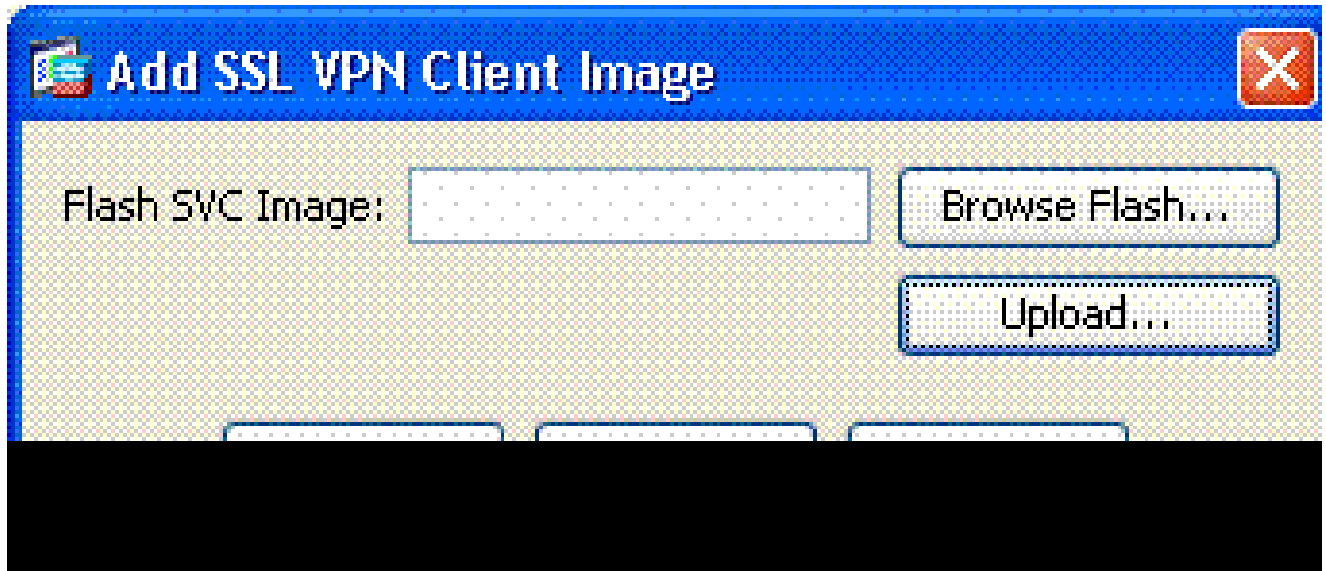
トンネルグループ インターフェイスおよびイメージの設定

注：新しいグループを作成しない場合は、デフォルトの組み込みグループを使用できます。

1. [Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profile] を選択します。
2. [Enable Cisco AnyConnect Client.....] を選択します。
3. [Would you like to designate an SVC image?]という質問を示すダイアログ ボックスが表示されます。
4. [Yes] を選択します。

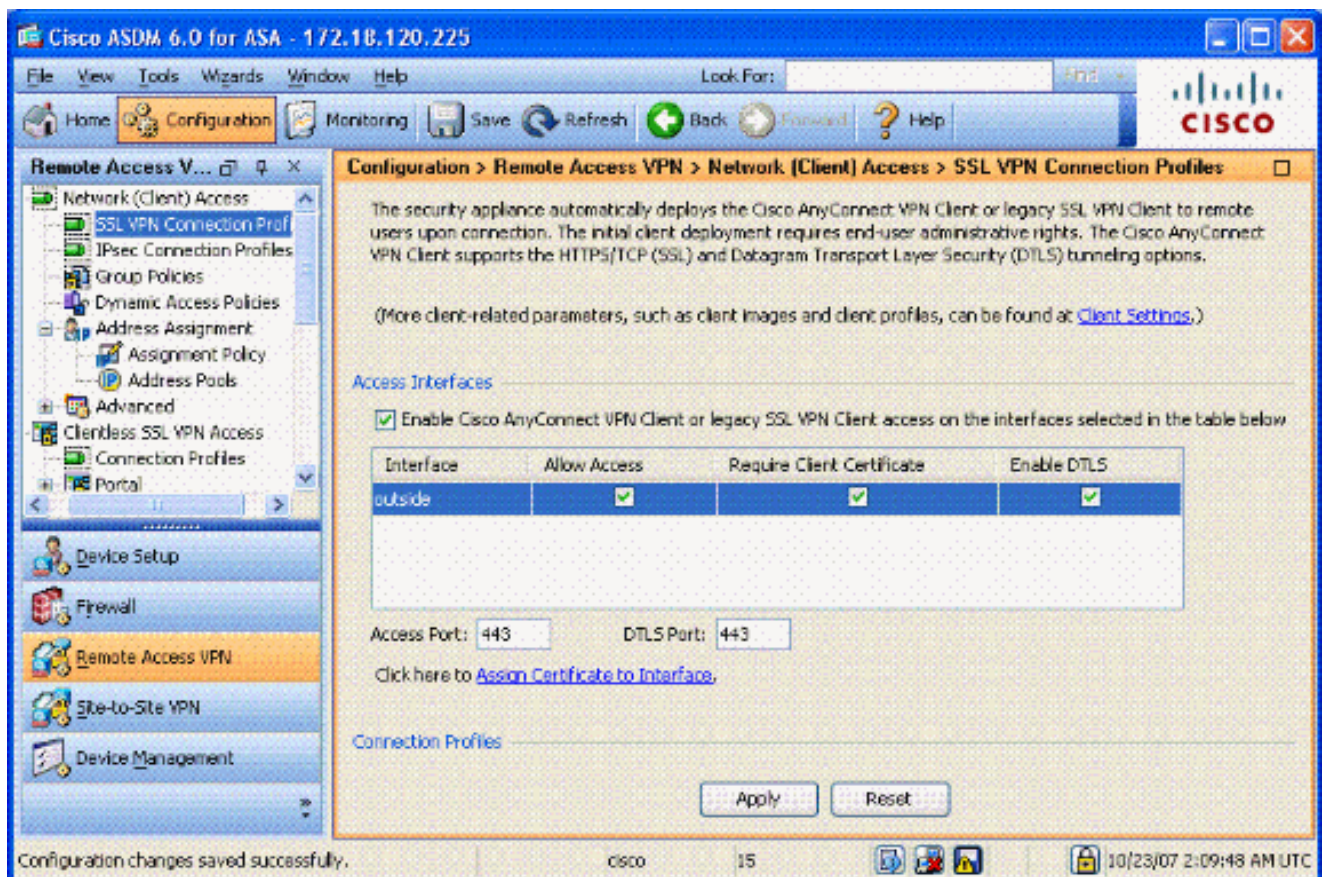
5. 画像がすでに存在する場合、Browse Flash で使用する画像を選択します。画像が使用できない場合、[Upload] を選択してローカル コンピュータ上のファイルを参照します。図 17 を参照してください。ファイルはCisco.comからダウンロードできます。Windows、MAC、およびLinuxのファイルがあります。

図17:SSL VPNクライアントイメージの追加



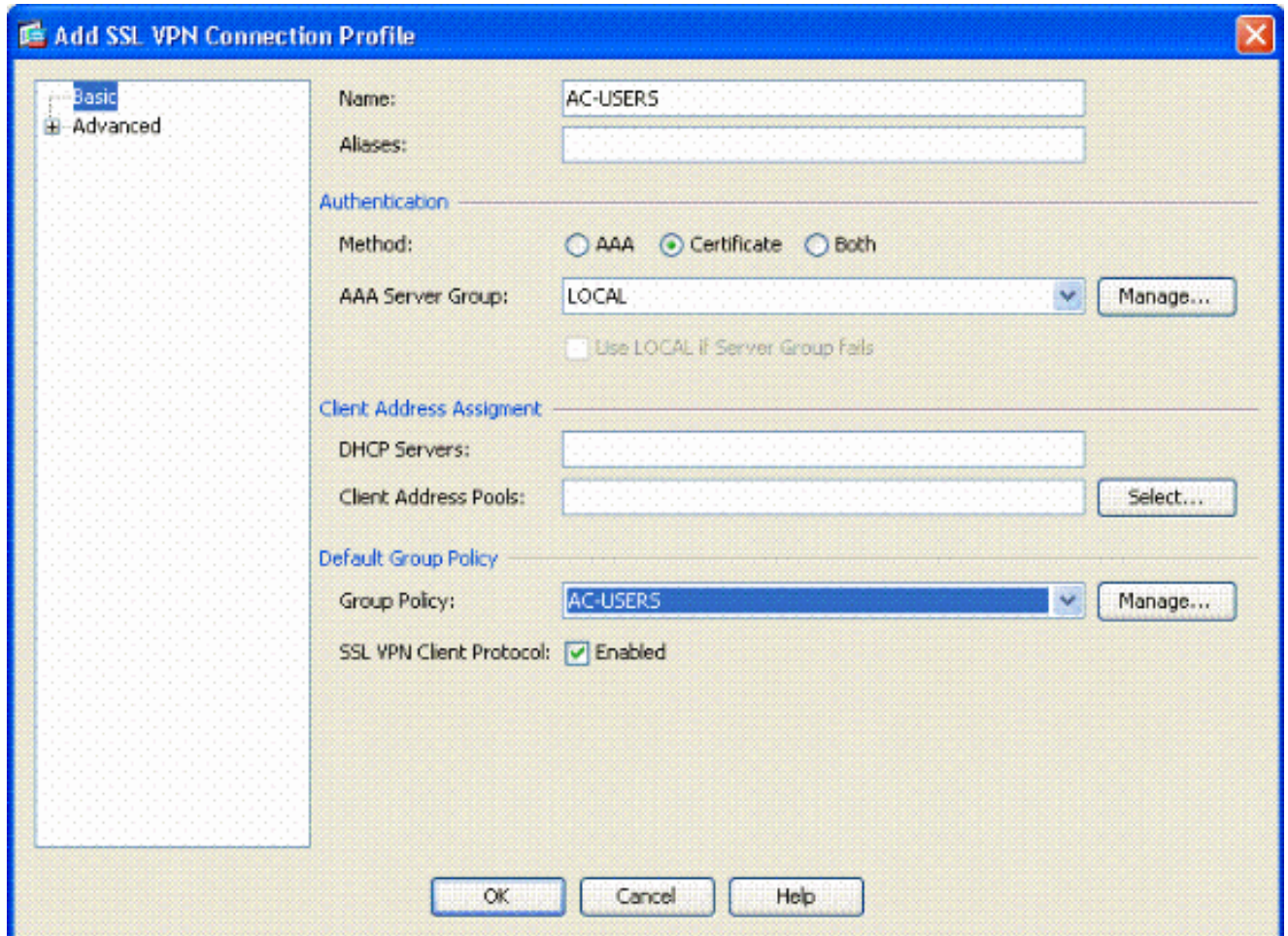
6. 次に、[Allow Access]、[Require Client Cert] をオンにし、オプションで [Enable DTLS] をオンにします。図 18 を参照してください。

図18 : アクセスの有効化



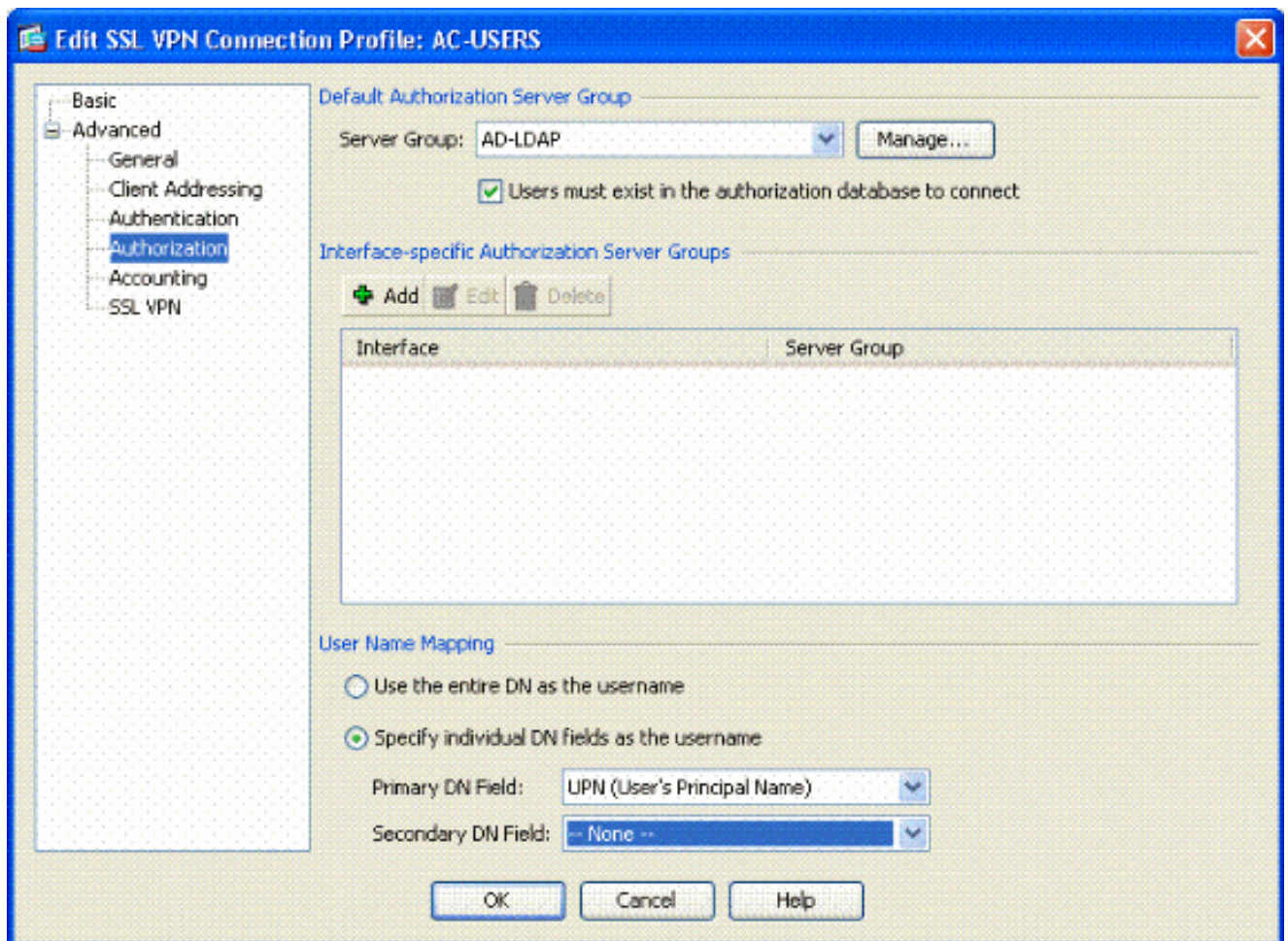
7. [APPLY] をクリックします。
8. 次に、接続プロファイルおよびトンネルグループを作成します。[Remote Access VPN] > [Network (Client) Access] > [SSL VPN Connection Profile] を選択します。
9. [Connection Profiles] セクションで、[Add] をクリックします。

図19：接続プロファイルの追加



- a. グループに名前を付けます。
 - b. 認証方法で [Certificate] を選択します。
 - c. 以前作成したグループポリシーを選択します。
 - d. [SSL VPN Client] がオンになっていることを確認します。
 - e. 他のオプションはデフォルトのままにします。
10. 次に、[Advanced] > [Authorization] を選択します。詳細については、図 20 を参照してください。

図20：許可

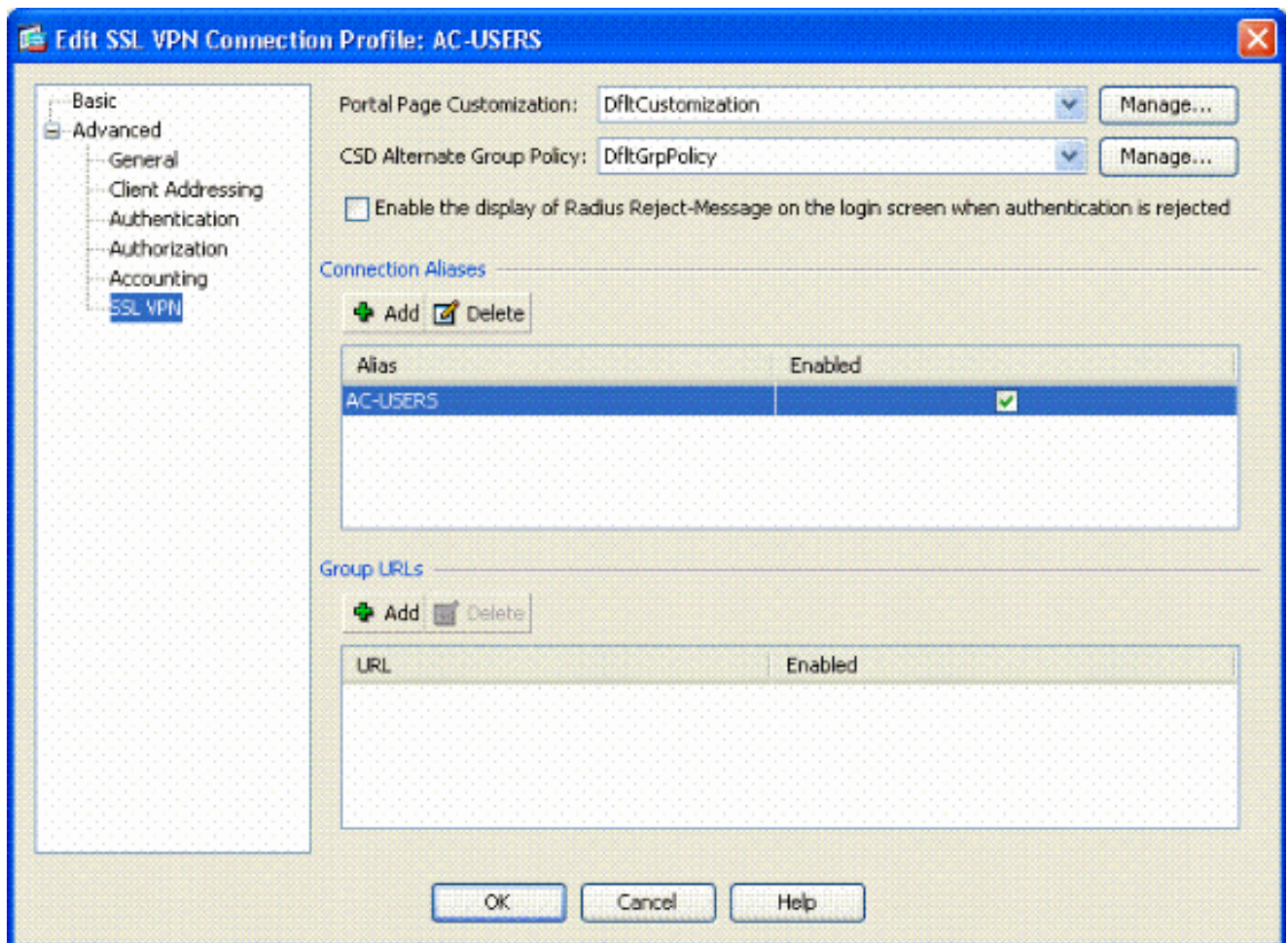


- a. 以前作成した AD-LDAP グループを選択します。
- b. [Users must exist....to connect] にチェックマークを付けます。
- c. マッピング フィールドで、プライマリについては [UPN] を、セカンダリについては [None] を選択します。

11. メニューから [SSL VPN] セクションを選択します。

12. [Connection Aliases] セクションで、次の手順を実行します。

図21：接続エイリアス



- a. [Add] を選択します。
- b. 使用するグループエイリアスを入力します。
- c. [Enabled] にチェックマークが付いていることを確認します。図 21 を参照してください。

13. [OK] をクリックします。

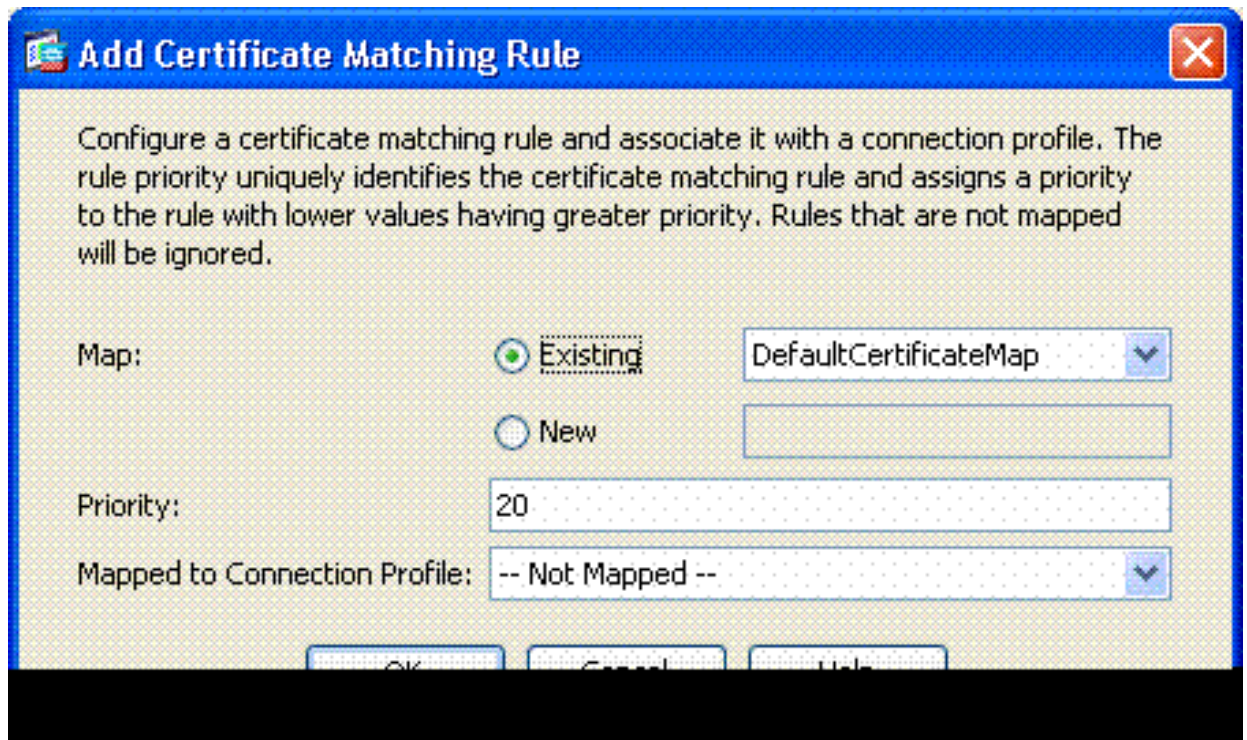
注：フラッシュメモリに設定を保存するには、Saveをクリックします。

証明書の照合ルール (OCSP が使用される場合)

1. [Remote Access VPN] > [Advanced] > [Certificate to SSL VPN Connection Profile Maps] を選択します。図 22 を参照してください。
 - a. [Certificate to Connection Profile Maps] セクションで [Add] を選択します。
 - b. [Map] セクションでは、既存のマップを DefaultCertificateMap として保持するか、あるいは IPsec 用の証明書マップをすでに使用している場合は新しいマップを作成することができます。
 - c. ルールのプライオリティはそのままにします。

- d. マップ対象グループは、[-- Not Mapped --] のままにします。図 22 を参照してください。

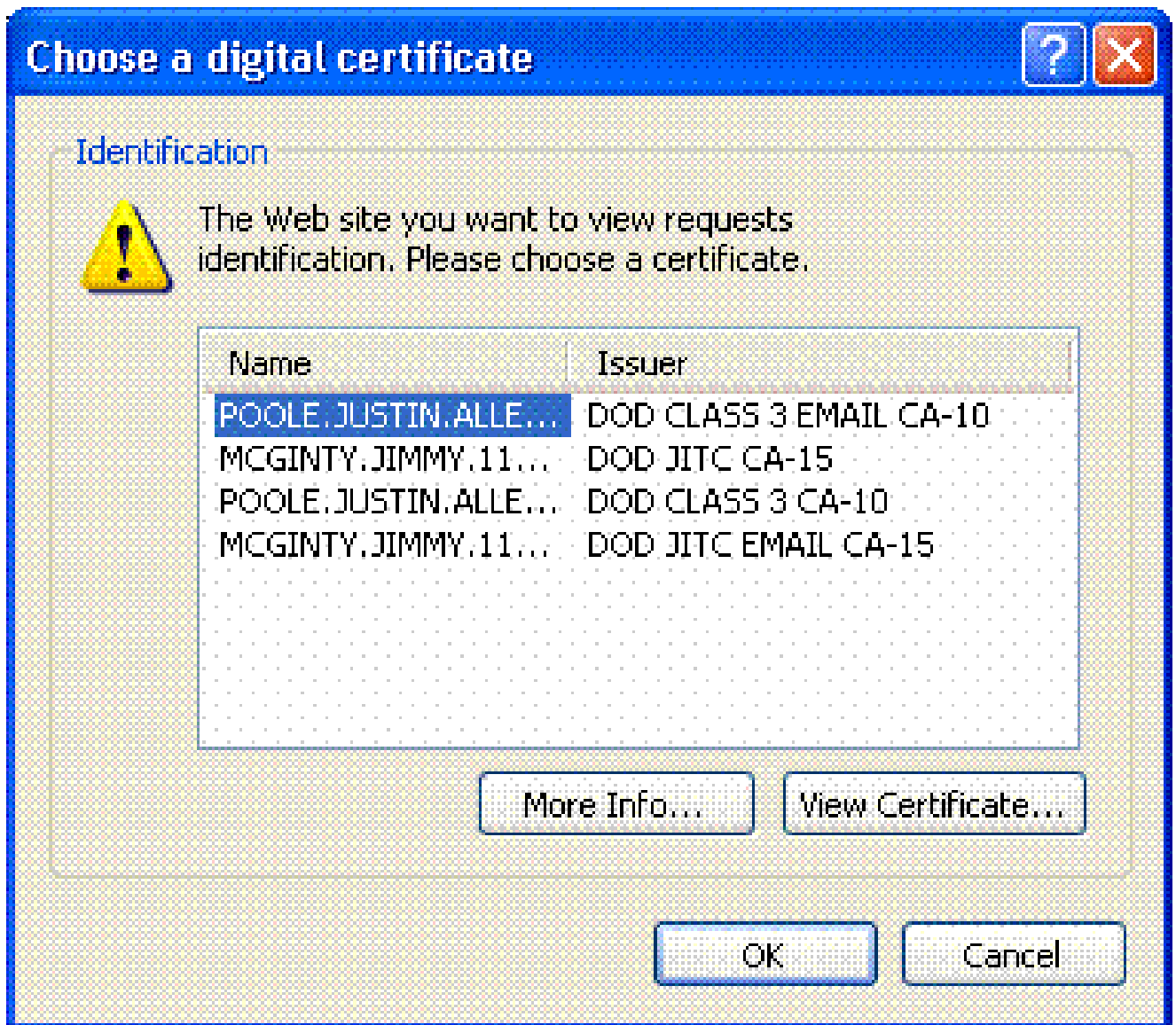
図22 : 証明書照合ルールの追加



- e. [OK] をクリックします。

2. 下の表にある [Add] をクリックします。
3. [Add Certificate Matching Rule Criterion] ウィンドウで、次の手順を実行します。

図23 : 証明書照合ルールの基準



- [Field] カラムは [Subject] のままにします。
- [Component] カラムは [Whole Field] のままにします。
- [Operator] カラムを [Does Not Equal] に変更します。
- [値]列に2つの二重引用符""を入力します。
- [OK] および [Apply] をクリックします。図 23 の例を参照してください。

OCSP の設定

OCSP の設定はさまざまであり、OCSP レスポンダベンダーによって異なります。詳細は、ベンダーのマニュアルをお読みください。

OCSP レスポンダ証明書の設定

1. OCSP レスポンダから自己生成された証明書を取得します。

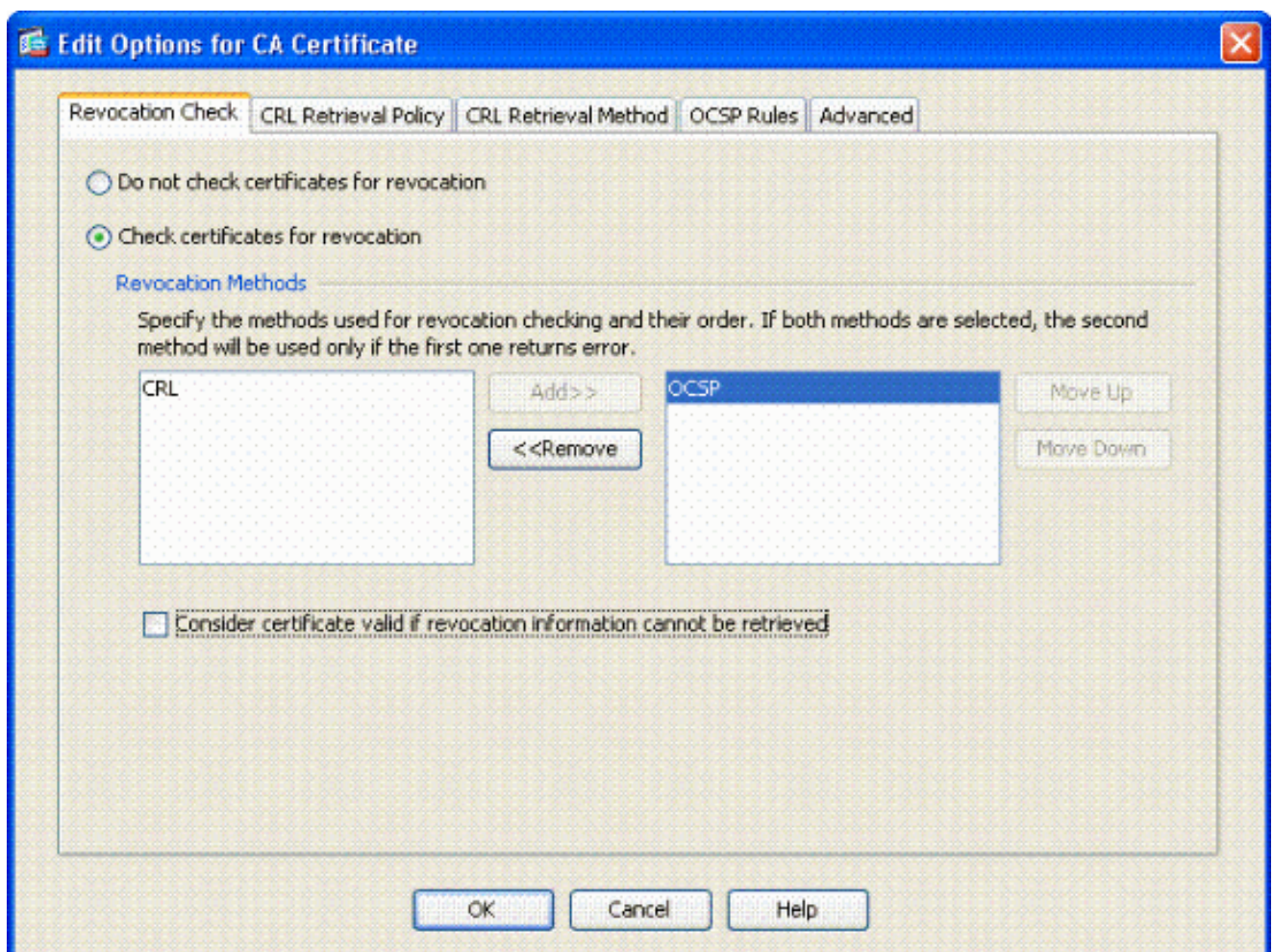
2. 以前説明した手順を実行して、OCSP サーバの証明書をインストールします。

注：OCSP証明書のトラストポイントで、Do not check certificates for revocationが選択されていることを確認します。

OCSP を使用するための CA の設定

1. [Remote Access VPN] > [Certificate Management] > [CA Certificate] を選択します。
2. OCSP を使用するように CA を設定するために、OCSP を強調表示します。
3. [Edit] をクリックします。
4. [Check certificate for revocation] がチェックされていることを確認します。
5. [Revocation Methods] セクションで、OCSP を追加します。図 24 を参照してください。

OCSP 失効チェック



6. 厳密な OCSP チェックを行う場合、[Consider Certificate valid...cannot be retrieved] のチェックマークを外してください。

注：失効にOCSPを使用するすべてのCAサーバを設定/編集します。

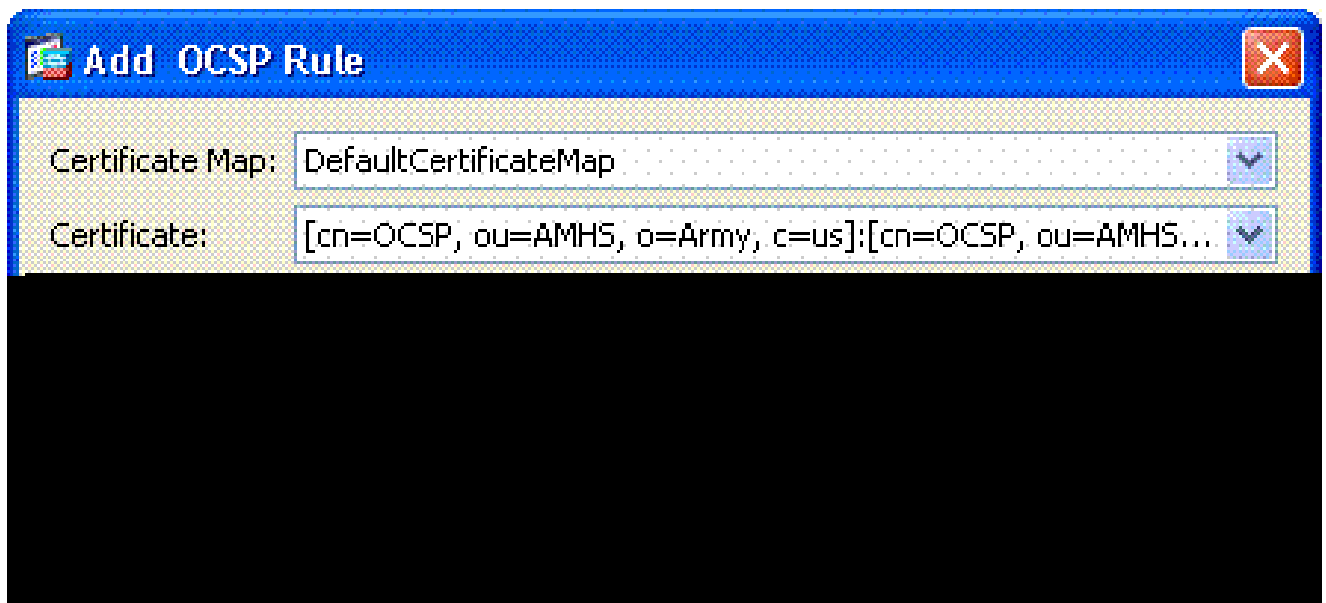
OCSP ルールの設定

注：次の手順を実行する前に、証明書グループ照合ポリシーが作成されていること、およびOCSPレスポンドが設定されていることを確認します。

注：一部のOCSP実装では、DNSのAおよびPTRレコードがASAに必要な場合があります。このチェックは、ASAが.milのサイトからのものであることを確認するために実行されます。

1. [Remote Access VPN] > [Certificate Management] > [CA Certificates 2] を選択します。
2. OCSP を使用するように CA を設定するために、OCSP を強調表示します。
3. [Edit] を選択します。
4. [OCSP Rule] タブをクリックします。
5. [Add] をクリックします。
6. [Add OCSP Rule] ウィンドウで、次の手順を実行します。図 25 を参照してください。

図25:OCSPルールの追加



- a. [Certificate Map] オプションで、[DefaultCertificateMap] を選択するか、以前作成したマップを選択します。
- b. [Certificate] オプションで、[OCSP responder] を選択します。
- c. [Index] オプションに、10 と入力します。

- d. [URL] オプションに、OCSP レスポンダの IP アドレスまたはホスト名を入力します。ホスト名を使用する場合、ASA に DNS サーバが設定されていることを確認します。
- e. [OK] をクリックします。
- f. [APPLY] をクリックします。

Cisco AnyConnect Client の設定

このセクションでは、Cisco AnyConnect VPN Client の設定について扱います。

前提条件: Cisco AnyConnect VPN Client およびミドルウェアアプリケーションがホスト PC にすでにインストールされている。ActivCard Gold および ActivClient がテスト済みである。

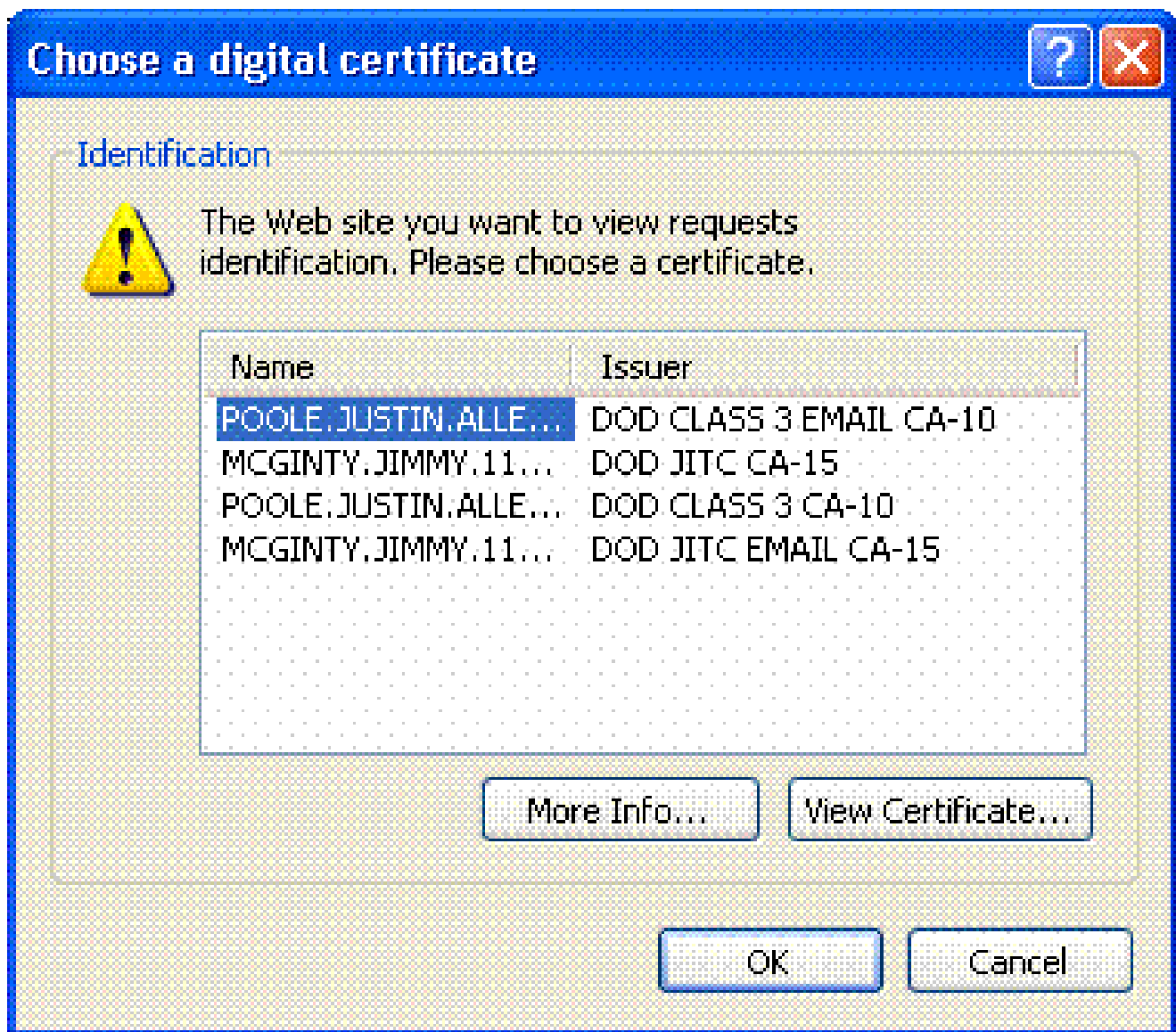
注: このガイドでは、AC クライアントの初期インストールにのみグループ URL 方式を使用します。AC クライアントのインストールが済んだら、IPsec クライアントと同じように AC アプリケーションを起動します。

注: DoD 証明書チェーンはローカルマシンにインストールする必要があります。PKI POC に問い合わせで証明書またはバッチ ファイルを取得してください。

Cisco Anyconnect VPN Client のダウンロード - Windows

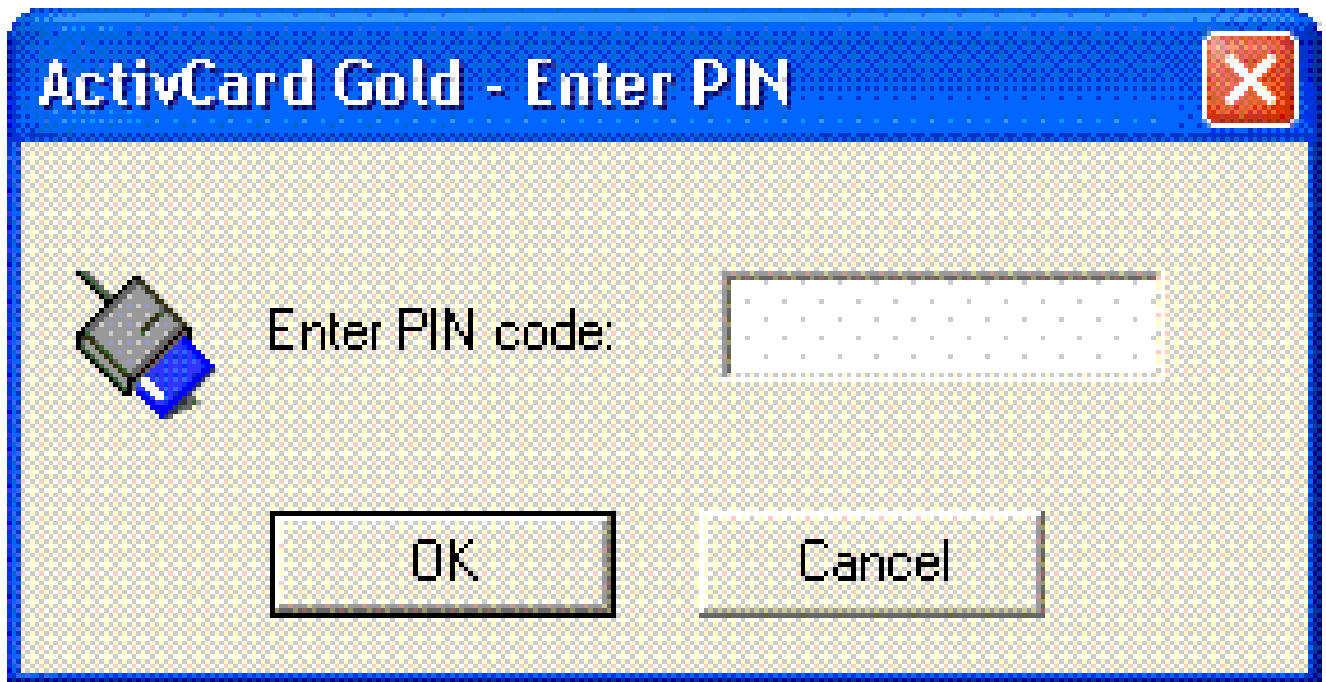
1. Internet Explorer 経由で ASA への Web セッションを起動します。アドレスは `https://Outside-Interface` という形式になります。たとえば、`https://172.18.120.225` と指定します。
2. アクセスに使用する署名証明書を選択します。図 26 を参照してください。

図26：正しい証明書の選択



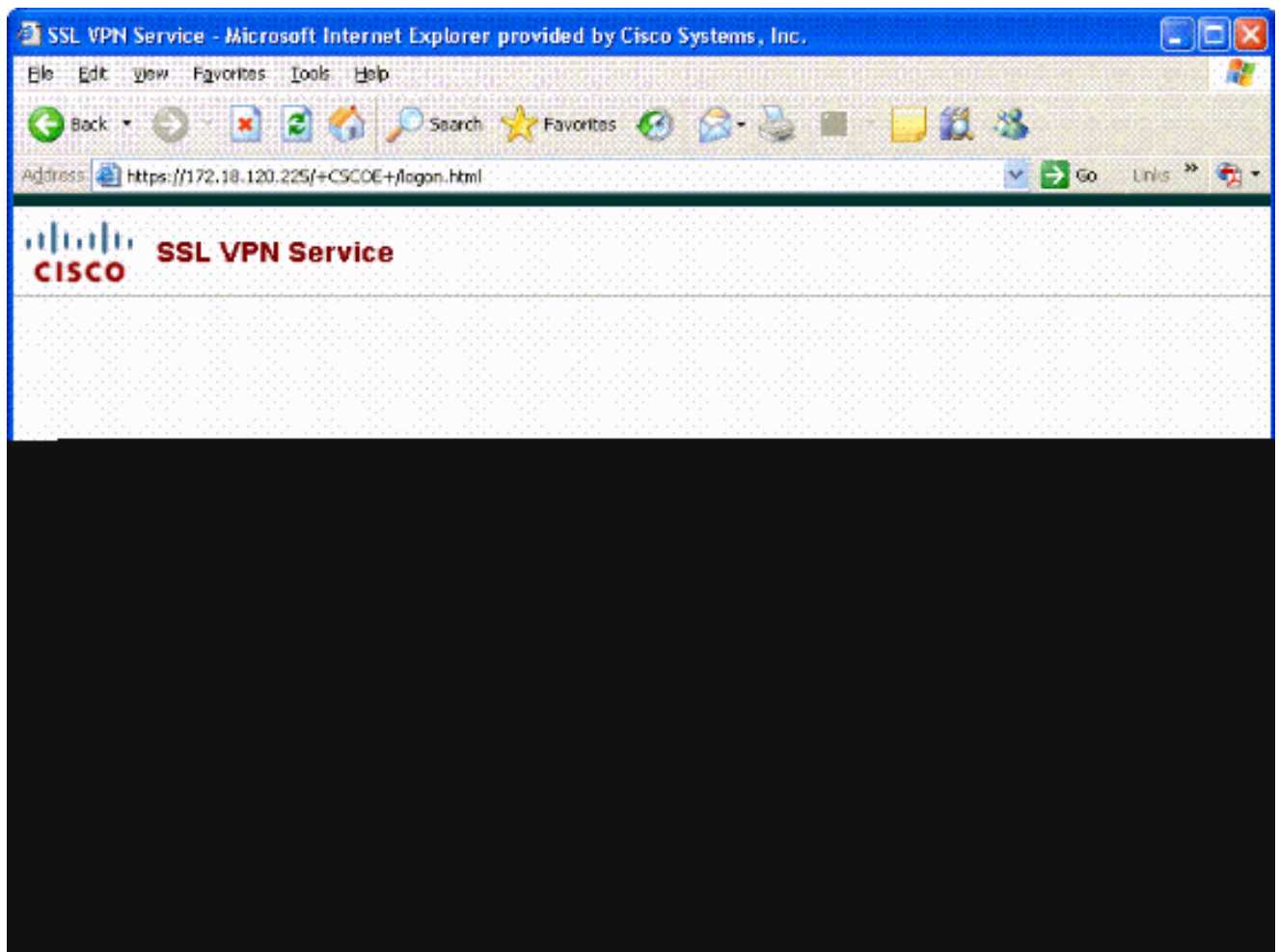
3. プロンプトが表示されたら、PIN を入力します。

図27：暗証番号の入力



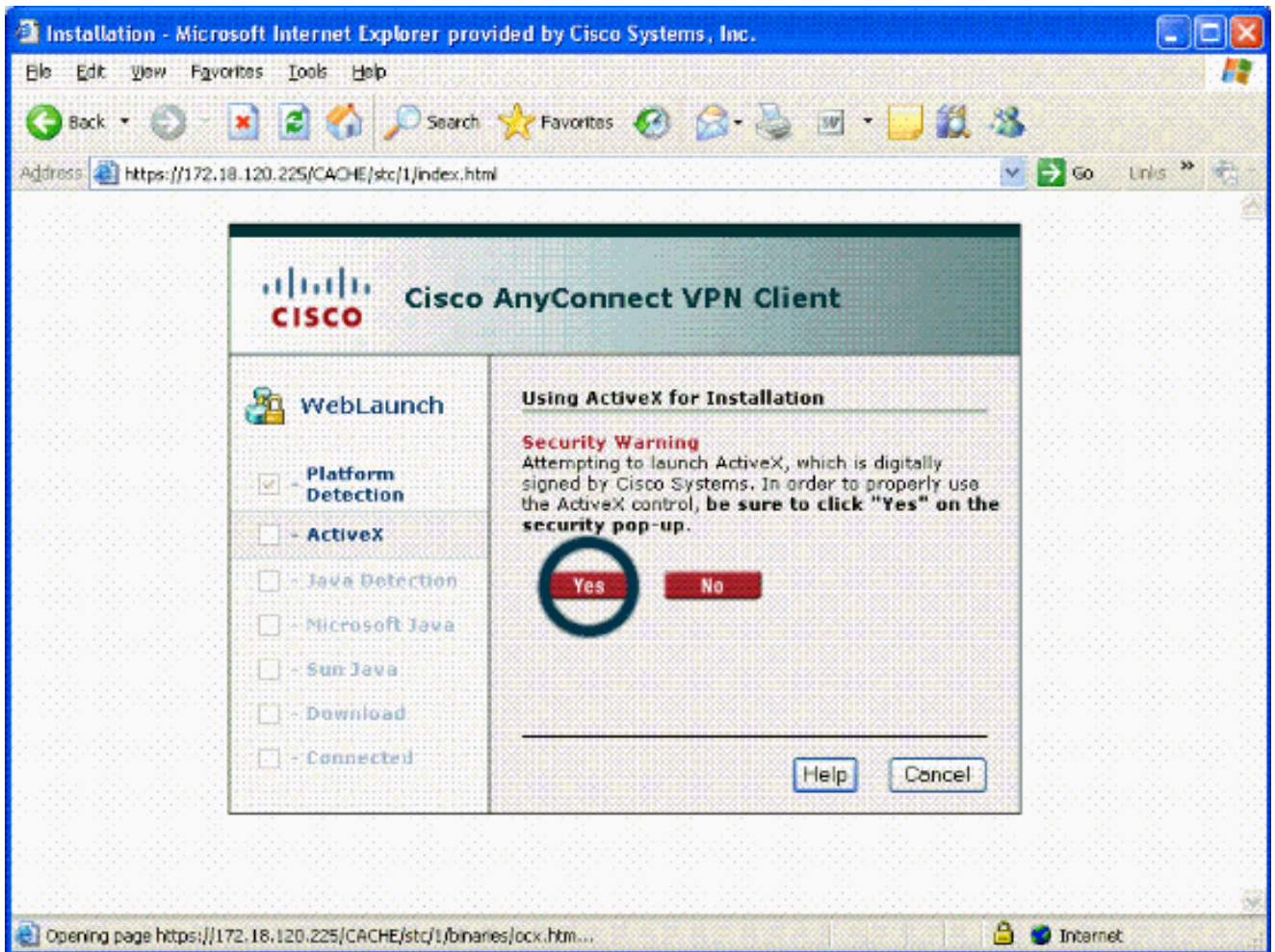
4. [Yes] を選択してセキュリティ警告に同意します。
5. SSL ログイン ページで、[Login] を選択します。クライアント証明書がログインに使用されます。図 28 を参照してください。

図28:SSLログイン



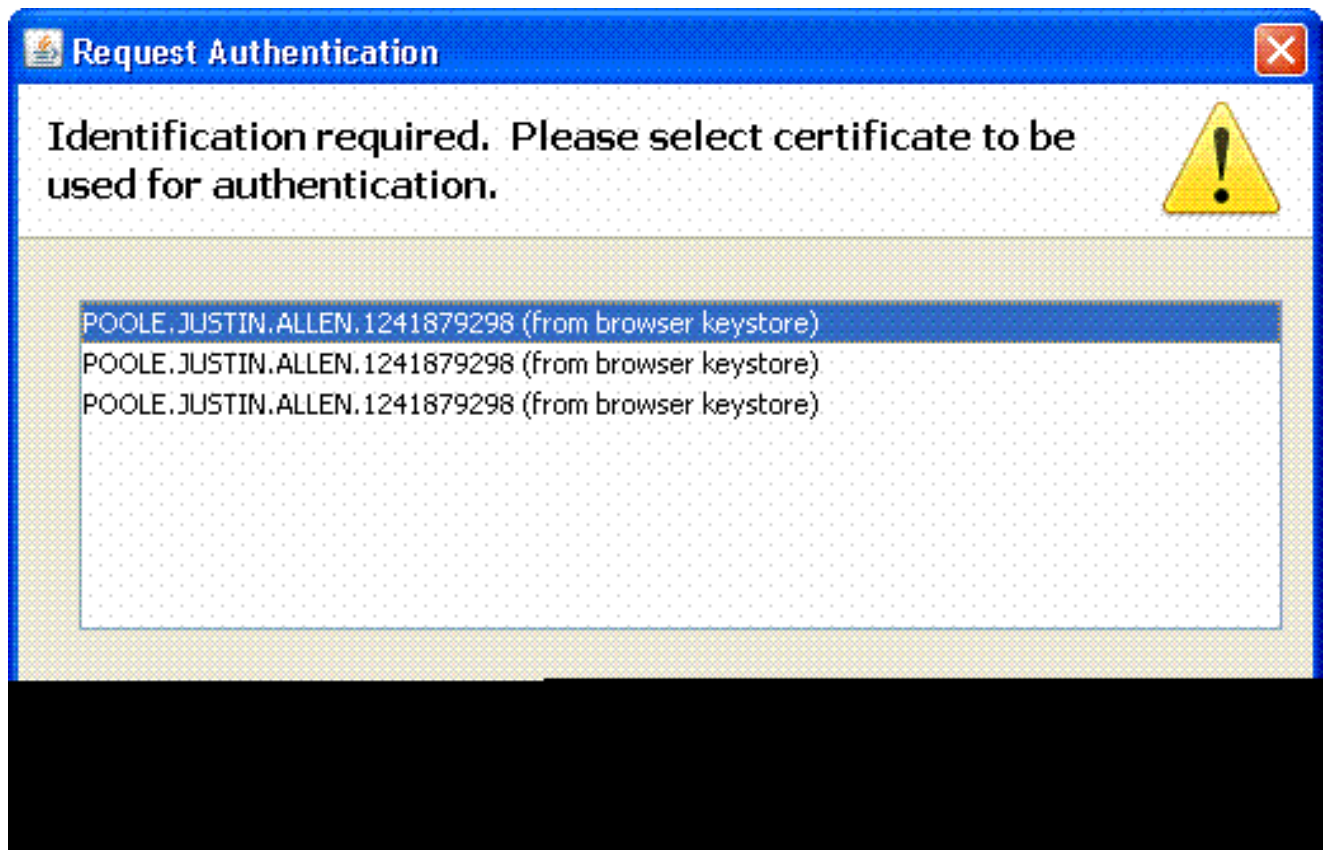
6. AnyConnect はクライアントのダウンロードを開始します。図 29 を参照してください。

図29:AnyConnectのインストール



7. 使用する適切な証明書を選択します。図 30 を参照してください。AnyConnect はインストールを続行します。ASA 管理者は、クライアントを永続的にインストールするか、ASA 接続のたびにインストールすることができます。

図30：証明書



Cisco Anyconnect VPN Client の起動 - Windows

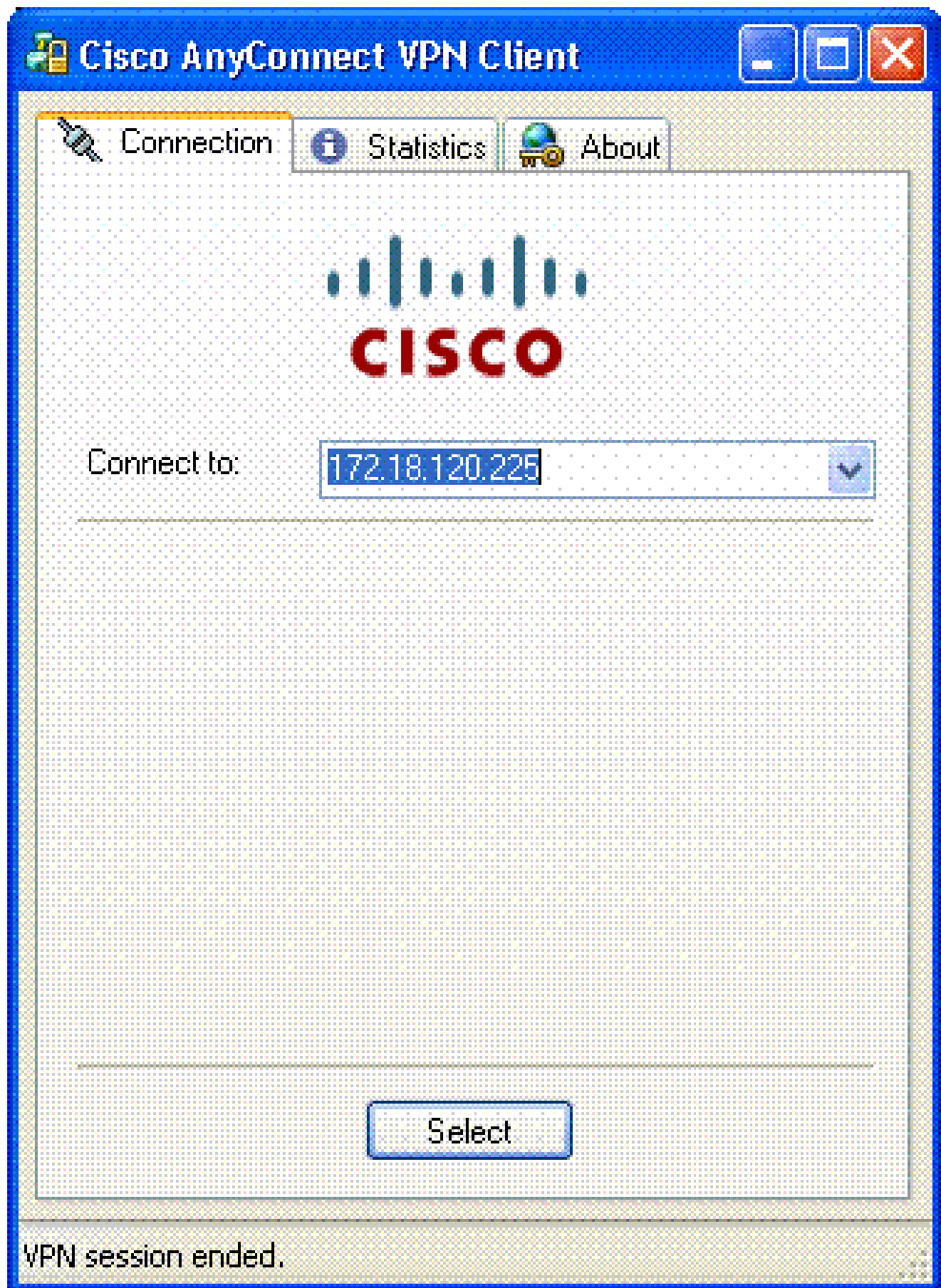
ホスト PC から、[Start] > [All Programs] > [Cisco] > [AnyConnect VPN Client] を選択します。

注：オプションのAnyConnectクライアントプロファイル設定については、付録Eを参照してください。

新規接続

1. AC ウィンドウが表示されます。図 34 を参照してください。

図34：新しいVPN接続



2. AC が接続を自動的に試行しない場合、適切なホストを選択します。
3. プロンプトが表示されたら、PIN を入力します。図 35 を参照してください。

図35：暗証番号の入力



リモート アクセスの開始

接続先となるグループおよびホストを選択します。

証明書が使用されるため、[Connect] を選択して VPN を確立します。図 36 を参照してください。

図36：接続



Connection



Statistics



About



Connect to:

172.18.120.225



Group:

AC-USERS



Username:

Password:

Connect

Please enter your username and password.

注：接続には証明書が使用されるため、ユーザ名とパスワードを入力する必要はありません。

注：オプションのAnyConnectクライアントプロファイル設定については、付録Eを参照してください。

付録 A：LDAP マッピングおよび DAP

ASA/PIX リリース 7.1(x) 以降では、LDAP マッピングと呼ばれる機能が導入されました。これは Cisco 属性と LDAP オブジェクトまたは属性の間のマッピングを提供する高度な機能で、LDAP スキーマ変更が不要になります。CAC 認証を実装する場合、これはリモート アクセス接続への追加のポリシー適用をサポートすることができます。これらは LDAP マッピングの例です。AD/LDAP サーバを変更するには、管理者権限が必要であることに注意してください。ASA 8.x ソフトウェアでは、ダイナミック アクセス ポリシー (DAP) 機能が導入されました。DAP は CAC と一緒に機能して、複数の AD グループを参照したり、ポリシーや ACL などをプッシュしたりすることができます。

シナリオ1：リモートアクセス許可ダイヤルインを使用したActive Directoryの強制 ：アクセスの許可/拒否

この例では AD 属性 msNPAllowDailin を Cisco 属性 cVPN3000-Tunneling- Protocol にマッピングします。

- AD属性値：TRUE =許可、FALSE =拒否
- Cisco属性値：1 = FALSE、4(IPSec)または20(4 IPSEC + 16 WebVPN)= TRUE、

ALLOW 条件について、次のようにマップします。

- TRUE = 20

DENY ダイヤルイン条件の場合、次のようにマップします。

- FALSE = 1

注:TRUEとFALSEはすべて大文字にしてください。詳細は、『[セキュリティアプライアンス ユーザ許可のための外部サーバの設定](#)』を参照してください。

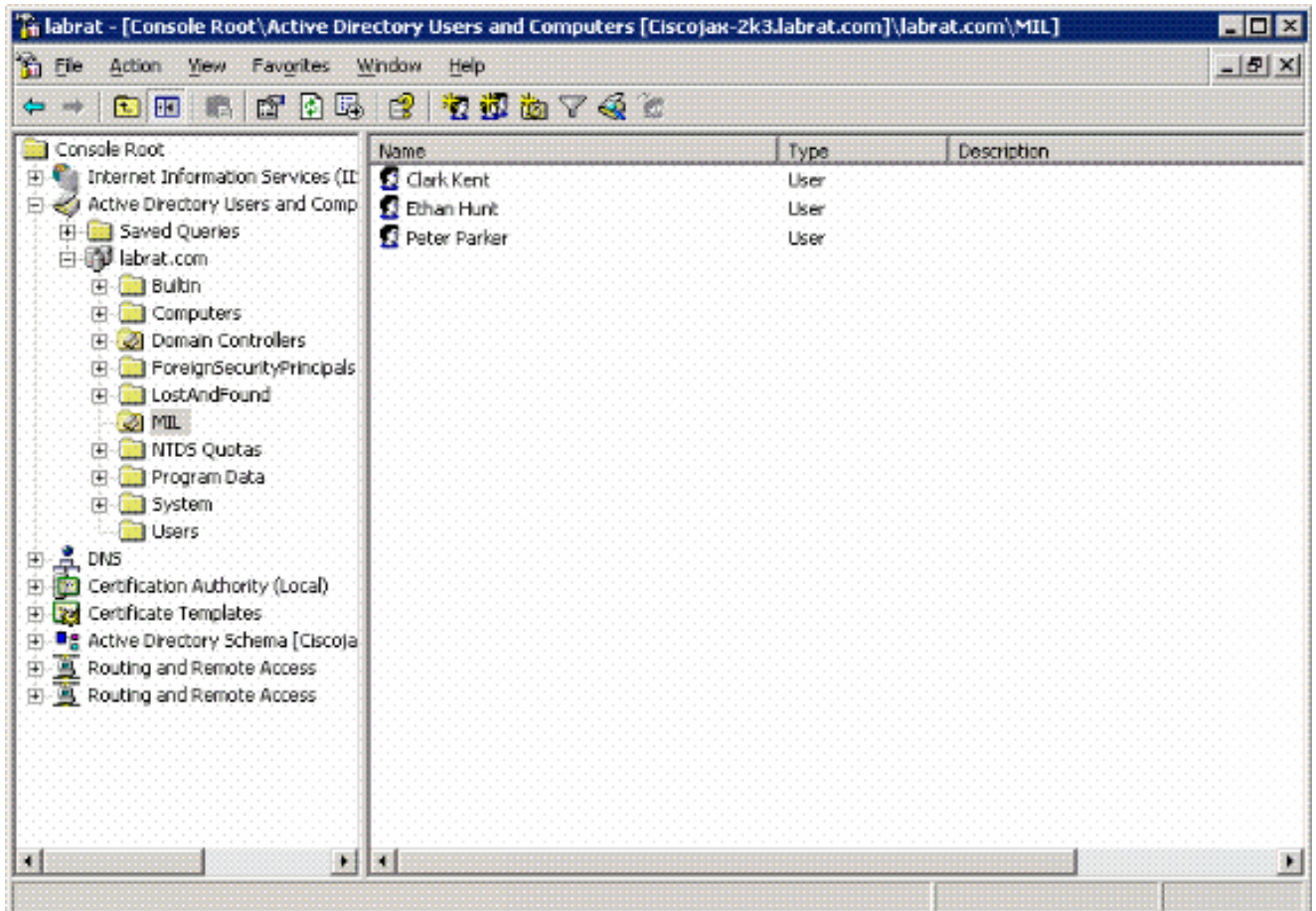
Active Directory の設定

1. Active Directory サーバで、[Start] > [Run] をクリックします。
2. 開いたテキスト ボックスに dsa.msc と入力して、[Ok] をクリックします。これで Active Directory 管理コンソールが起動します。
3. Active Directory 管理コンソールでプラス記号をクリックして、Active Directory のユーザお

よびコンピュータを展開します。

4. プラス記号をクリックして、ドメイン名を展開します。
5. ユーザのOUが作成されている場合は、すべてのユーザを表示するためにOUを展開します。すべてのユーザがUsersフォルダに割り当てられている場合は、それらのユーザを表示するためにフォルダを展開します。図 A1 を参照してください。

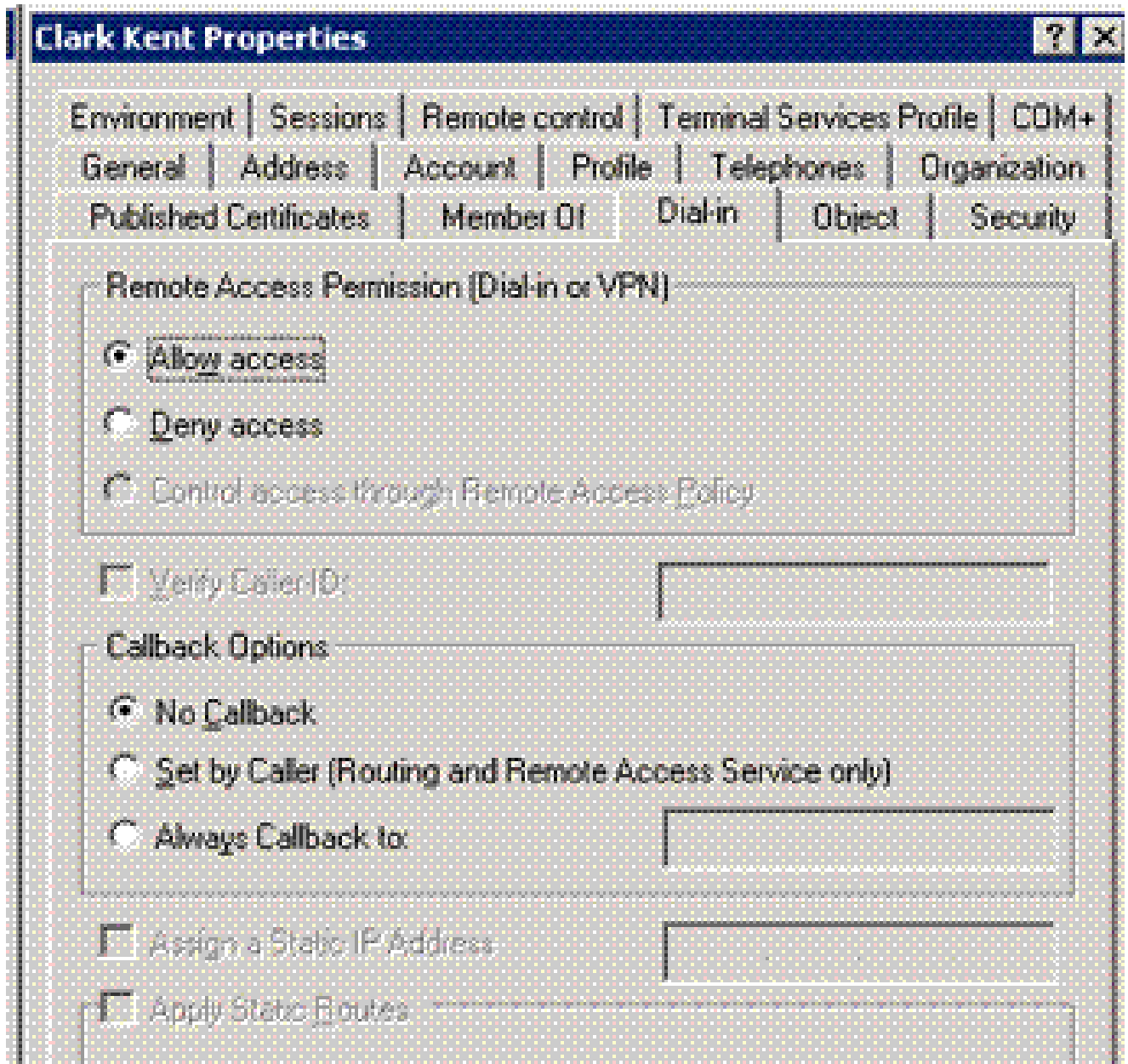
図A1: Active Directory管理コンソール



6. 編集するユーザをダブルクリックします。

ユーザのプロパティ ページで [Dial-in] タブをクリックし、[Allow] または [Deny] をクリックします。図 A2 を参照してください。

図A2 : ユーザのプロパティ



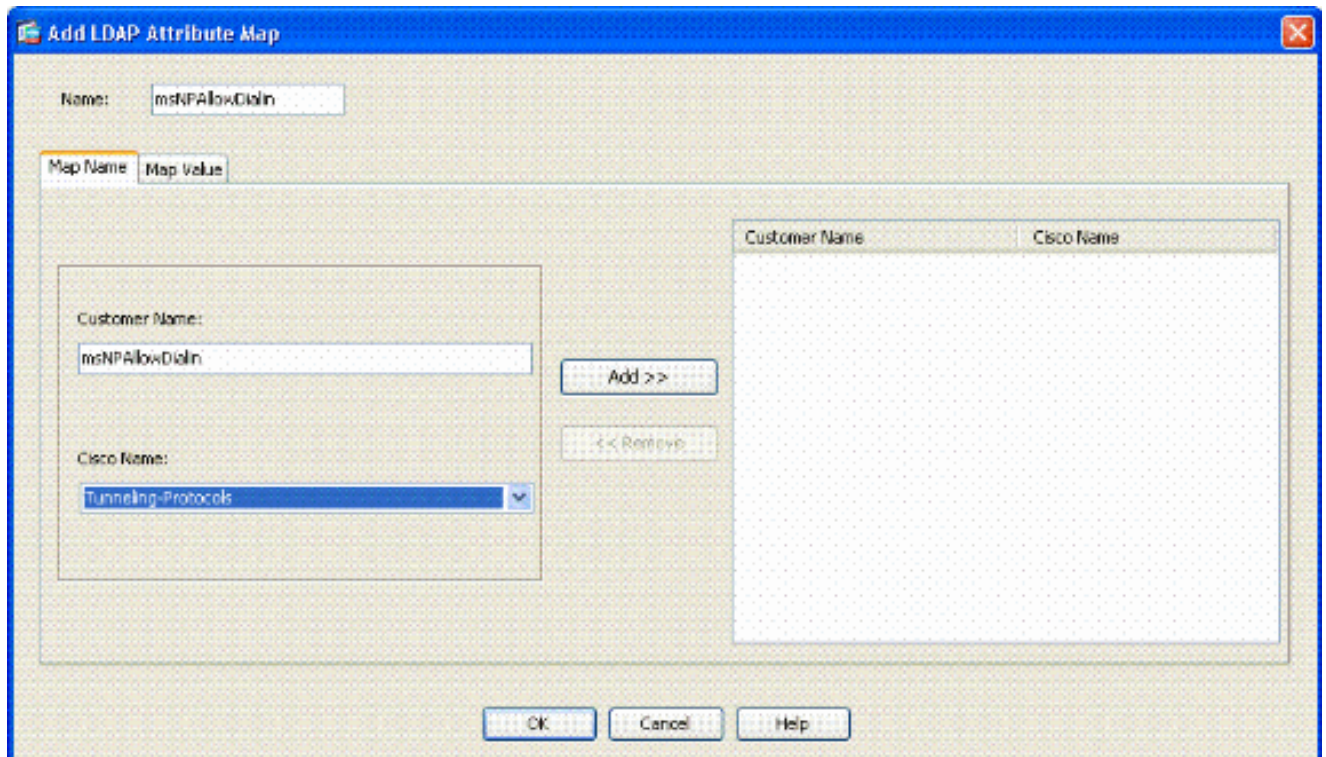
7. 次に [OK] をクリックします。

ASA の設定

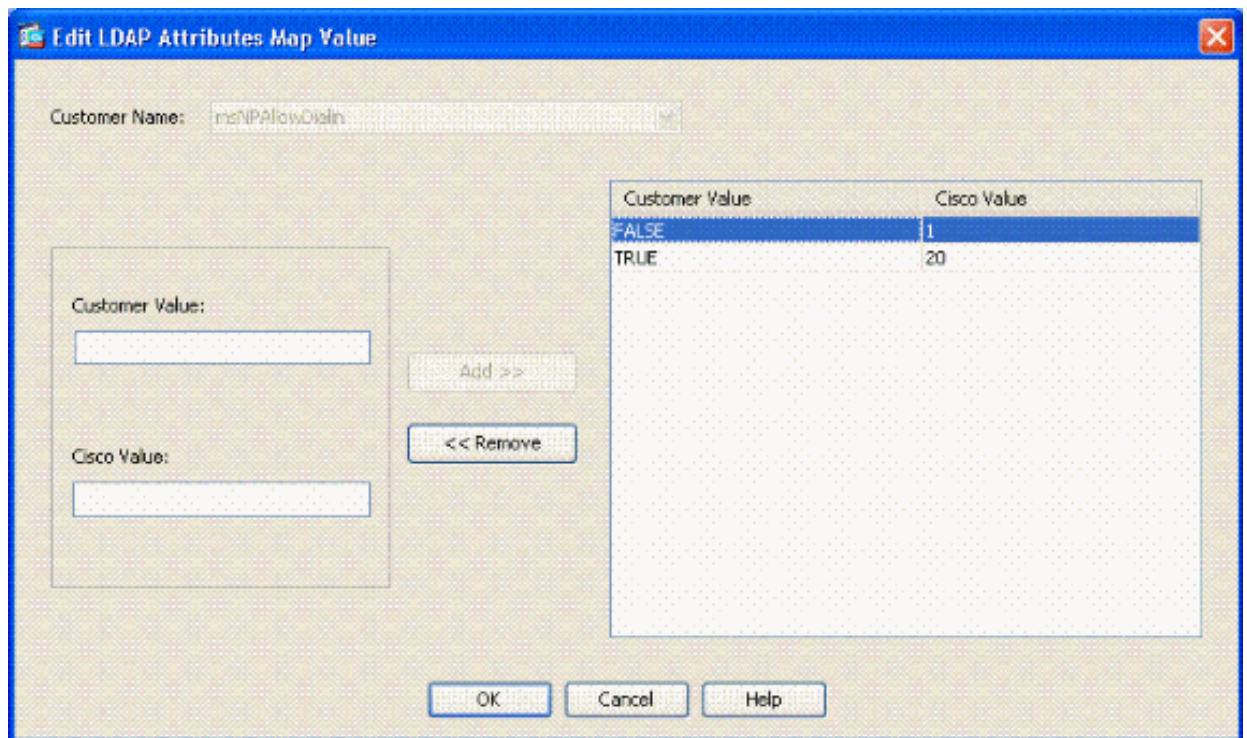
1. ASDM で、[Remote Access VPN] > [AAA Setup] > [LDAP Attribute Map] を選択します。
2. [Add] をクリックします。
3. Add LDAP Attribute Map ウィンドウで、次の手順を実行します。図 A3 を参照してください

。

図A3:LDAP属性マップの追加



- a. 「名前」テキストボックスに名前を入力します。
- b. [Map Name] タブの [Customer Name] テキストボックスに msNPAllowDialin と入力します。
- c. [Map Name] タブの [Cisco Name] ドロップダウン オプションで [Tunneling-Protocols] を選択します。
- d. [Add] をクリックします。
- e. [Map Value] タブを選択します。
- f. [Add] をクリックします。
- g. [Add Attribute LDAP Map Value] ウィンドウの [Customer Name] テキストボックスに TRUE と入力し、[Cisco Value] テキストボックスに 20 と入力します。
- h. [Add] をクリックします。
- i. [Customer Name] テキストボックスに FALSE と入力し、[Cisco Value] テキストボックスに 1 と入力します。図 A4 を参照してください。



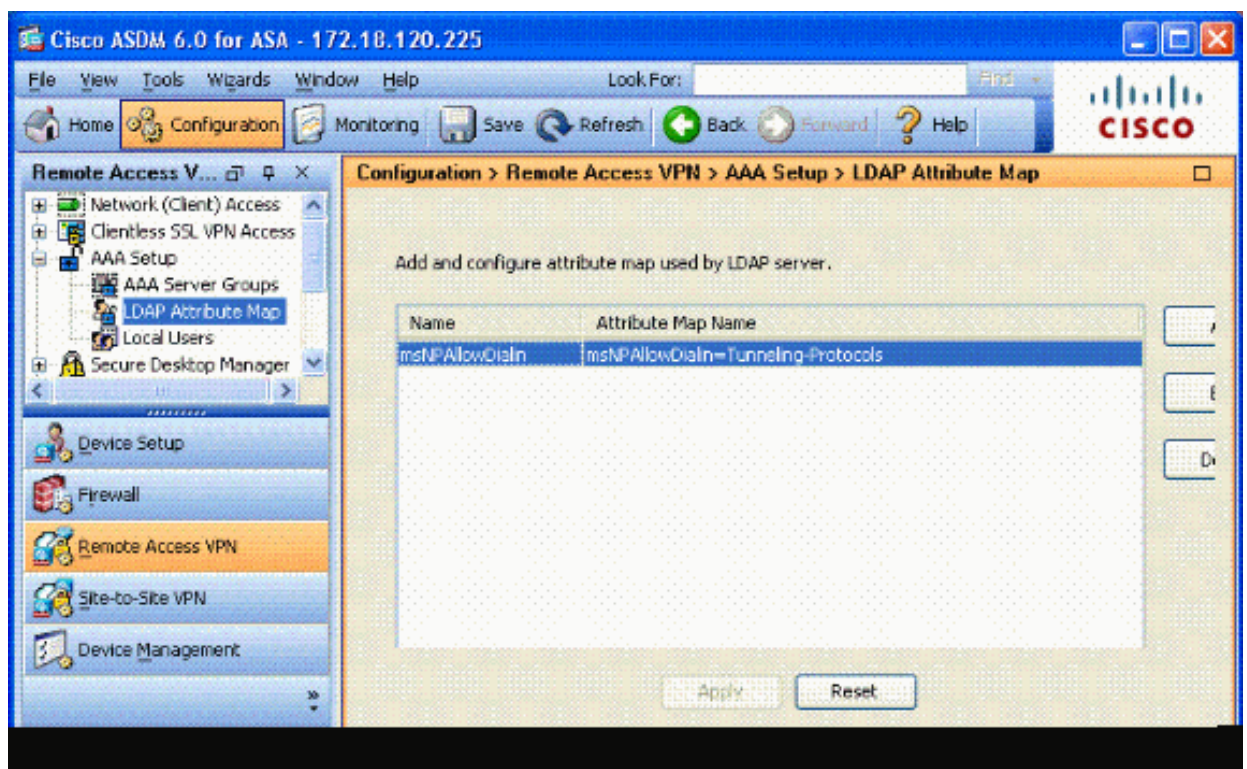
j. [OK] をクリックします。

k. [OK] をクリックします。

l. [APPLY] をクリックします。

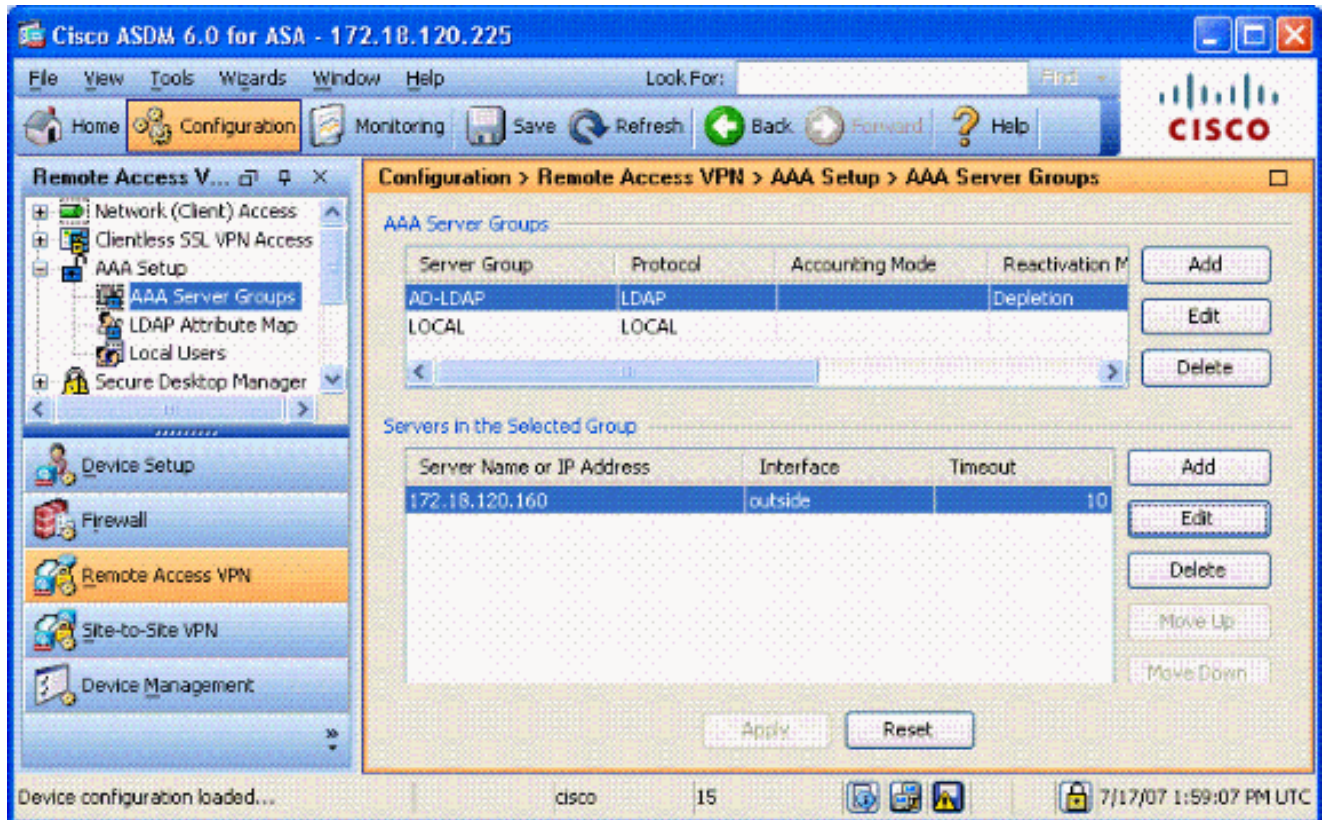
m. 設定は図 A5 のようになります。

図A5:LDAP属性マップの設定



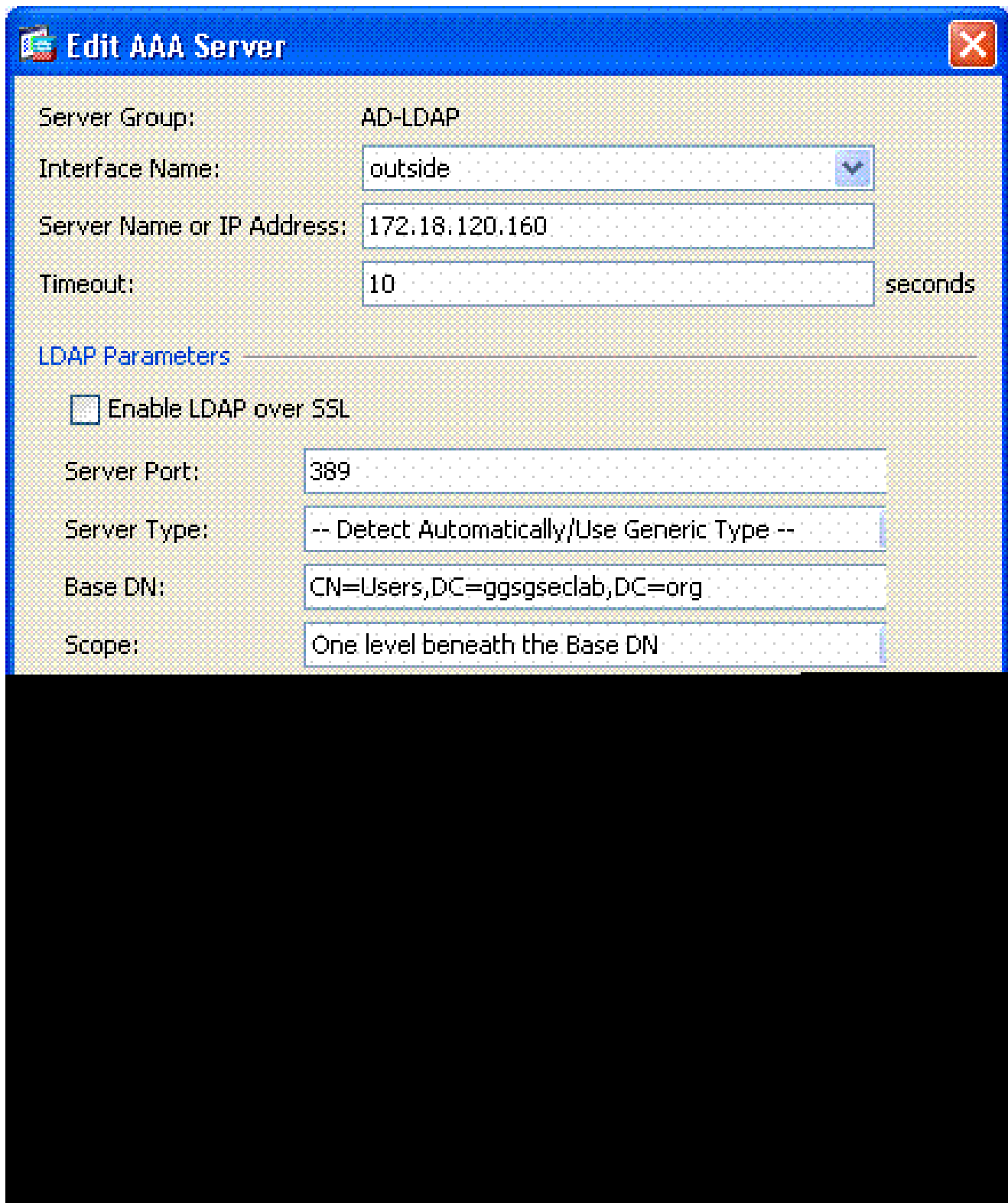
4. [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] を選択します。図 A6 を参照してください。

図A6:AAAサーバグループ



5. 編集するサーバグループをクリックします。[Servers in the Selected Group] セクションからサーバの IP アドレスまたはホスト名を選択して、[Edit] をクリックします。
6. [Edit AAA Server] ウィンドウの [LDAP Attribute Map] テキストボックスで、作成された LDAP 属性マップをドロップダウンメニューから選択します。図 A7 を参照してください。

図A7:LDAP属性マップの追加



Edit AAA Server

Server Group: AD-LDAP

Interface Name: outside

Server Name or IP Address: 172.18.120.160

Timeout: 10 seconds

LDAP Parameters

Enable LDAP over SSL

Server Port: 389

Server Type: -- Detect Automatically/Use Generic Type --

Base DN: CN=Users,DC=gsgseclab,DC=org

Scope: One level beneath the Base DN

7. [OK] をクリックします。

注：LDAPバインディングと属性マッピングが正しく機能しているかどうかを確認するには、テスト中にLDAPデバッグをオンにします。トラブルシューティング コマンドについては付録 C を参照してください。

シナリオ2：グループメンバーシップを使用したアクセスの許可/拒否によるActive

Directoryの適用

この例では、グループメンバシップを条件として設定するために、LDAP 属性 memberOf を使用してトンネリングプロトコル属性にマッピングします。このポリシーを機能させるには、次の条件が必要です。

- ALLOW 条件のメンバになる ASA VPN ユーザについて、すでに存在するグループを使用するか、新しいグループを作成します。
- DENY 条件のメンバになる ASA 以外のユーザについて、すでに存在するグループを使用するか、新しいグループを作成します。
- LDAP Viewer 内で、グループの DN が正しいことを確認します。「付録 D」を参照してください。DN が正しくない場合、マッピングは正しく動作しません。

注：このリリースでは、ASAはmemberOf属性の最初の文字列だけを読み取ることができ、ことに注意してください。作成された新しいグループがリストの先頭になるようにしてください。他のオプションは、特殊文字を名前の前に配置して、AD が特殊文字を最初に参照できるようにすることです。この制約を回避するには、複数のグループを参照する 8.x ソフトウェアの DAP を使用してください。

注：ユーザが拒否グループの一部であるか、memberOfが常にASAに送り返されるように別の1つ以上のグループの一部であることを確認してください。FALSE 拒否条件を指定する必要はありませんが、そうすることがベスト プラクティスです。既存のグループ名にスペースが含まれる場合は、次の方法で属性を入力します。

CN=Backup Operators,CN=Builtin,DC=gsgsec1ab,DC=orgです。

注：DAPを使用すると、ASAはmemberOf属性の複数のグループを参照し、それらのグループに基づいて許可を行うことができます。DAP のセクションを参照してください。

マッピング

- AD 属性の値：
 - memberOf CN=ASAUUsers,CN=Users,DC=gsgsec1ab,DC=org
 - memberOf CN=TelnetClients,CN=Users,DC=labrat,DC=com
- Cisco属性値：1 = FALSE、20 = TRUE、

ALLOW 条件について、次のようにマップします。

- memberOf CN=ASAUUsers,CN=Users,DC=gsgsec1ab,DC=org= 20

DENY 条件について、次のようにマップします。

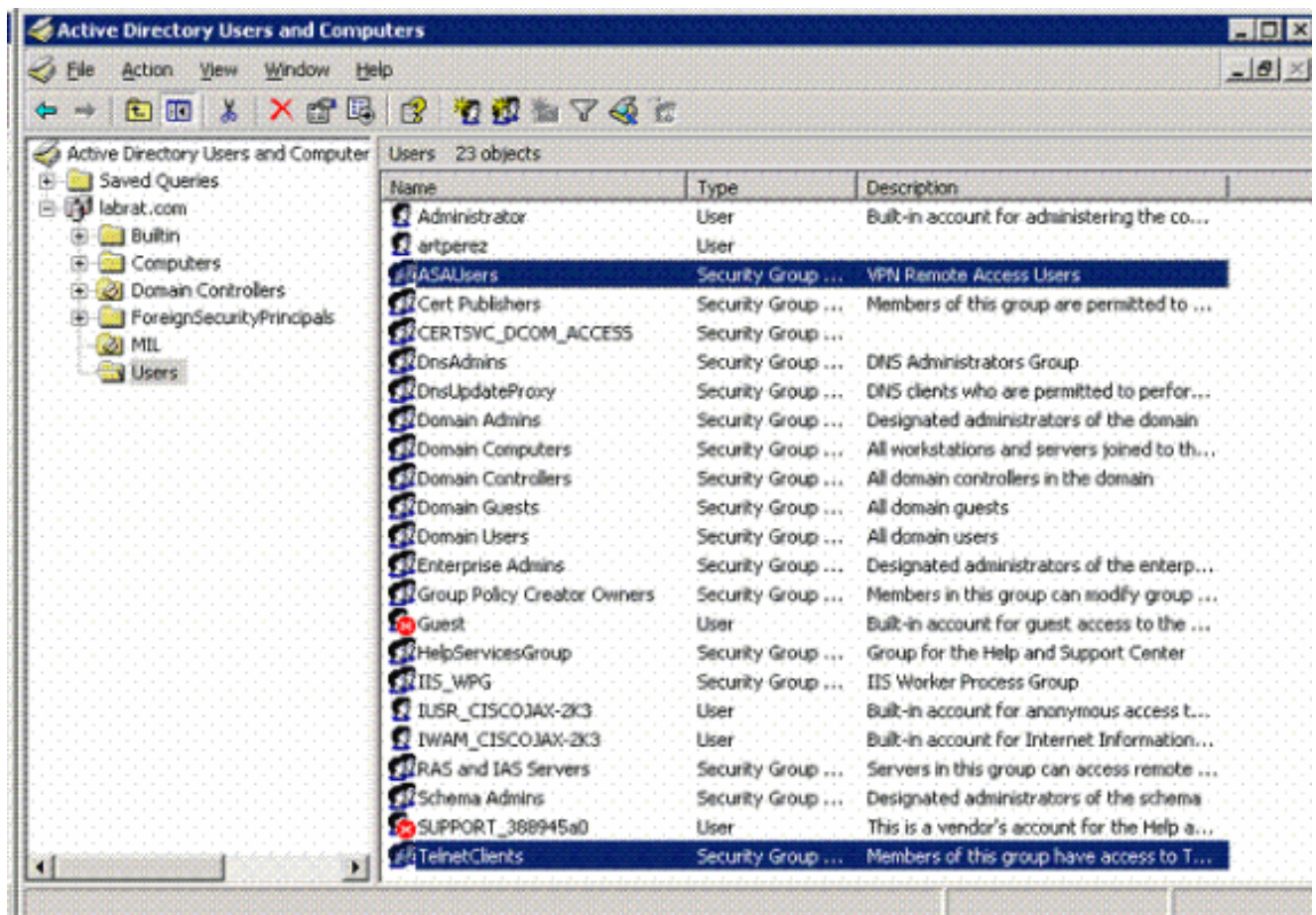
- memberOf CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org = 1

注：今後のリリースでは、接続を許可および拒否するためのCisco属性が追加されます。Cisco属性についての詳細は、『[セキュリティアプライアンスユーザ許可のための外部サーバの設定](#)』を参照してください。

Active Directory の設定

1. Active Directory サーバで、[Start] > [Run] を選択します。
2. 開いたテキストボックスに dsa.msc と入力して、[Ok] をクリックします。これで Active Directory 管理コンソールが起動します。
3. Active Directory 管理コンソールでプラス記号をクリックして、Active Directory のユーザおよびコンピュータを展開します。図 A8 を参照してください。

図A8:Active Directoryグループ



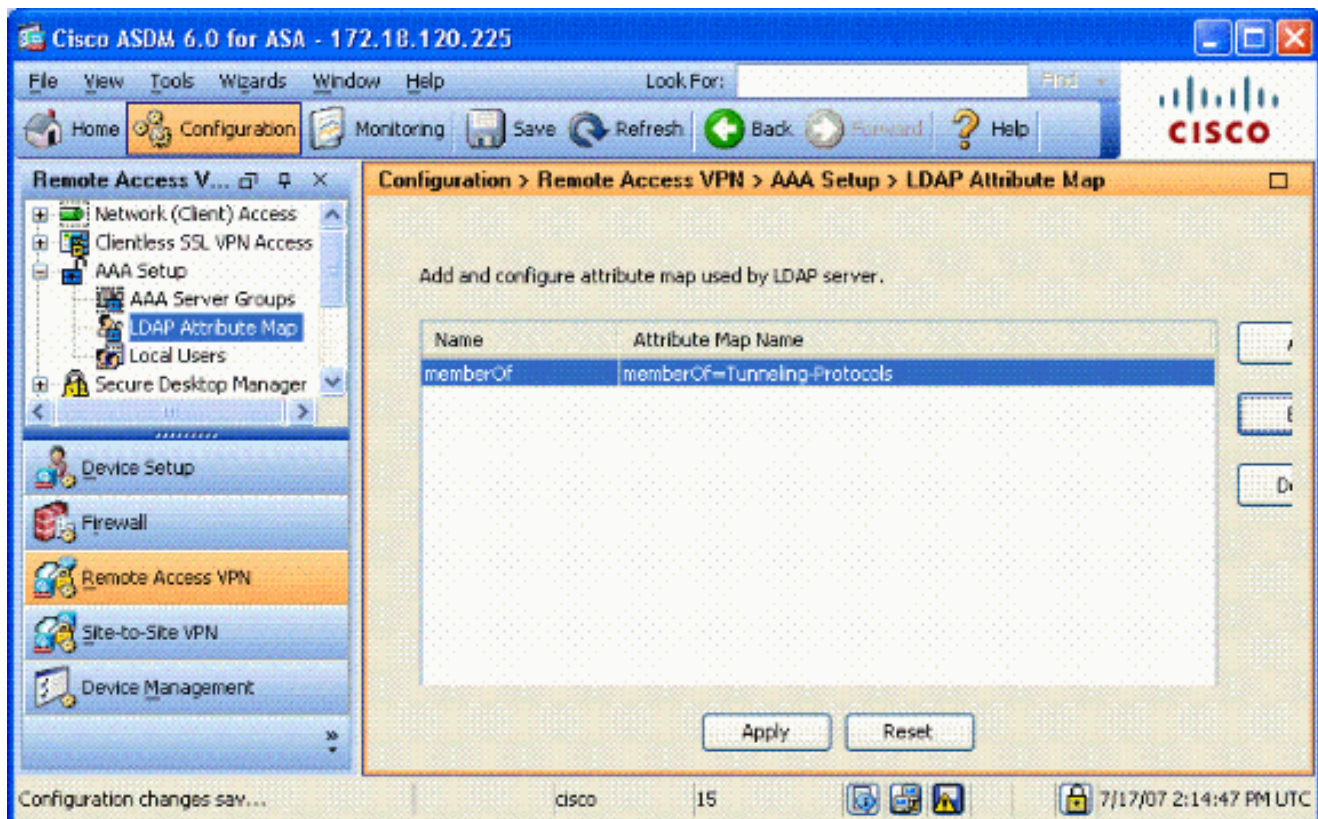
4. プラス記号をクリックして、ドメイン名を展開します。
5. [Users] フォルダを右クリックし、[New] > [Group] を選択します。
6. グループ名を入力します。例：ASAUUsers。
7. [OK] をクリックします。

8. [Users] フォルダをクリックし、上記で作成したグループをダブルクリックします。
9. [Members] タブを選択して、[Add] をクリックします。
10. 追加するユーザの名前を入力して、[Ok] をクリックします。

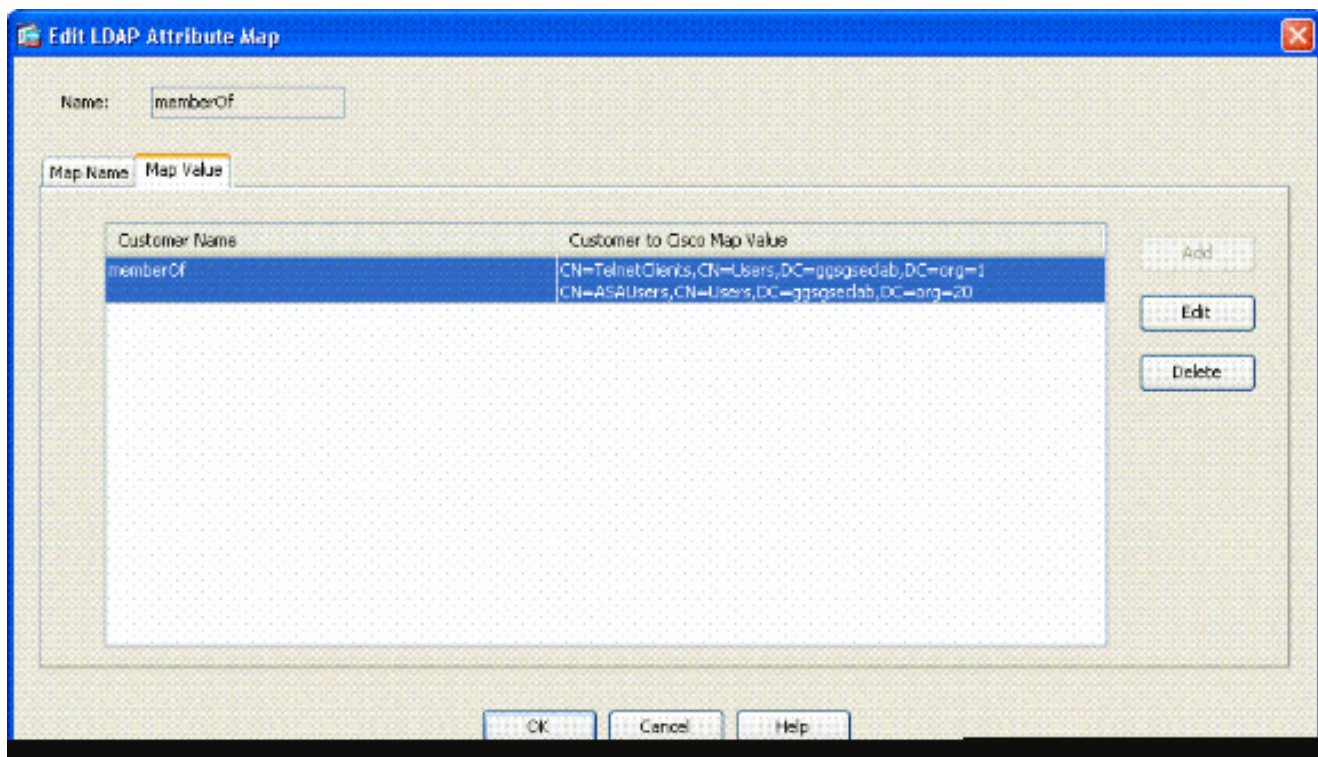
ASA の設定

1. ASDM で、[Remote Access VPN] > [AAA Setup] > [LDAP Attribute Map] を選択します。
2. [Add] をクリックします。
3. Add LDAP Attribute Map ウィンドウで、次の手順を実行します。図 A3 を参照してください。
 - a. 「名前」テキストボックスに名前を入力します。
 - b. [Map Name] タブの [Customer Name] テキストボックス c に memberOf と入力します。
 - c. [Map Name] タブの [Cisco Name] ドロップダウン オプションで [Tunneling-Protocols] を選択します。
 - d. [Add] を選択します。
 - e. [Map Value] タブをクリックします。
 - f. [Add] を選択します。
 - g. [Add Attribute LDAP Map Value] ウィンドウの [Customer Name] テキストボックスに CN=ASAUsers,CN=Users,DC=gsgseclab,DC=org と入力し、[Cisco Value] テキストボックスに 20 と入力します。
 - h. [Add] をクリックします。
 - i. [Customer Name] テキストボックスに CN=TelnetClients,CN=Users,DC=gsgseclab,DC=org と入力し、[Cisco Value] テキストボックスに 1 と入力します。図 A4 を参照してください。
 - j. [OK] をクリックします。
 - k. [OK] をクリックします。
 - l. [APPLY] をクリックします。
 - m. 設定は図 A9 のようになります。

図 A9 : LDAP 属性マップ



4. [Remote Access VPN] > [AAA Setup] > [AAA Server Groups] を選択します。
5. 編集するサーバグループをクリックします。[Servers in the Selected Group] セクションからサーバの IP アドレスまたはホスト名を選択して、[Edit] をクリックします。



6. [Edit AAA Server] ウィンドウの [LDAP Attribute Map] テキストボックスで、作成された LDAP 属性マップをドロップダウンメニューから選択します。

7. [OK] をクリックします。

注：LDAPバインディングと属性マッピングが正しく動作していることを確認するために、テスト中はLDAPデバッグをオンにします。トラブルシューティング コマンドについては付録 C を参照してください。

シナリオ3：複数のmemberOf属性のダイナミックアクセスポリシー

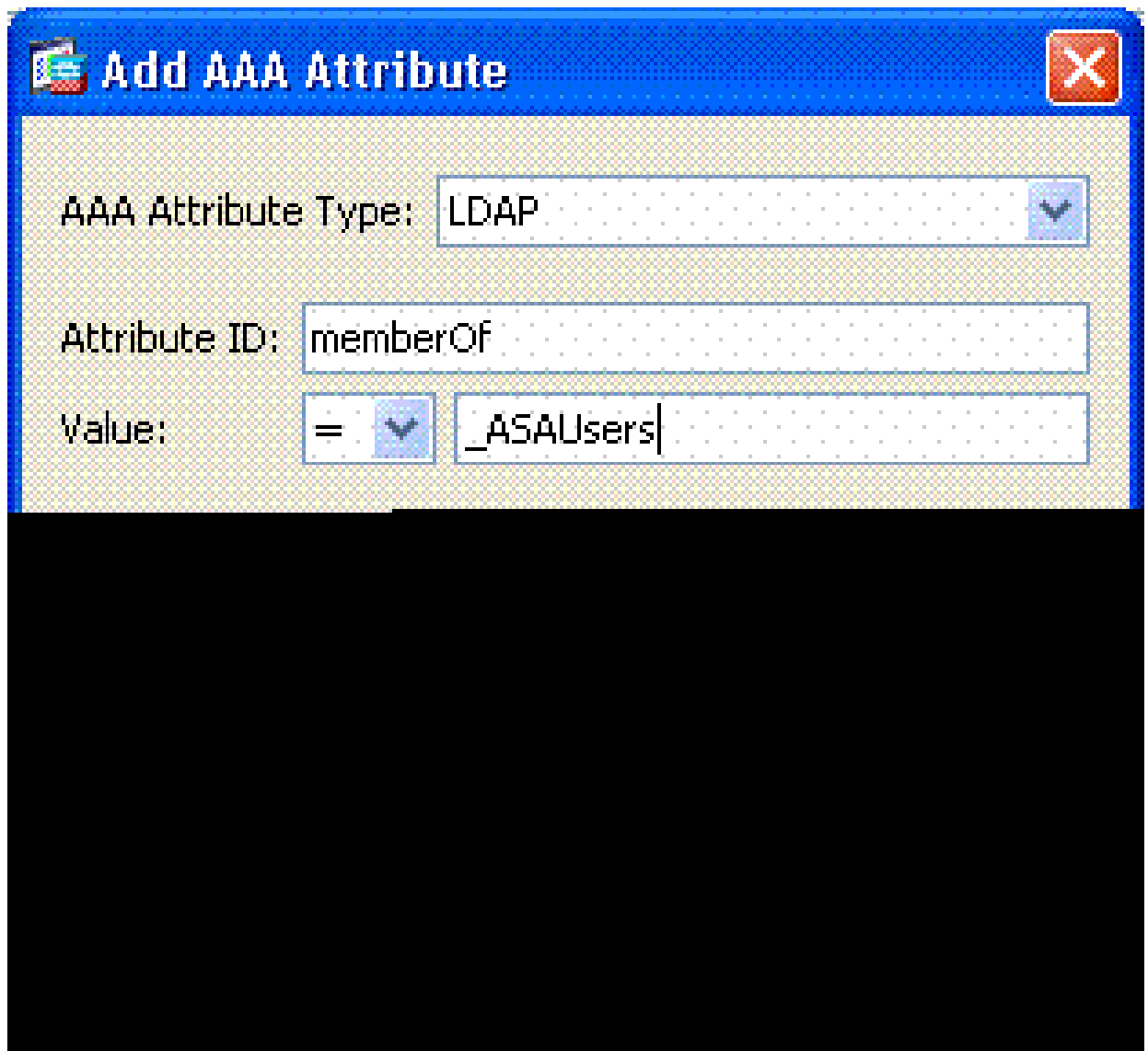
この例では、Active Directory グループ メンバシップに基づくアクセスを可能にするために、DAP を使用して複数の memberOf 属性を参照します。8.x よりも前では、ASA は最初の memberOf 属性のみを読み取っていました。8.x 以降では、ASA はすべての memberOf 属性を参照できます。

- ALLOW 条件のメンバになる ASA VPN ユーザについて、すでに存在するグループを使用するか、新しいグループ (1 つまたは複数) を作成します。
- DENY 条件のメンバになる ASA 以外のユーザについて、すでに存在するグループを使用するか、新しいグループを作成します。
- LDAP Viewer 内で、グループの DN が正しいことを確認します。「付録 D」を参照してください。DN が正しくない場合、マッピングは正しく動作しません。

ASA の設定

1. ASDM で、[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択します。
2. [Add] をクリックします。
3. [Add Dynamic Access Policy] で、次の手順を実行します。
 - a. 「名前」テキストボックスに名前を入力します。
 - b. プライオリティ セクションに、1 などの 0 より大きい数を入力します。
 - c. 選択基準で、[Add] をクリックします。
 - d. [Add AAA Attribute] で、[LDAP] を選択します。
 - e. [Attribute ID] セクションで、memberOf と入力します。
 - f. [Value] セクションで、[=] を選択し、AD グループ名を入力します。参照する各グループについてこの手順を繰り返します。図 A10 を参照してください。

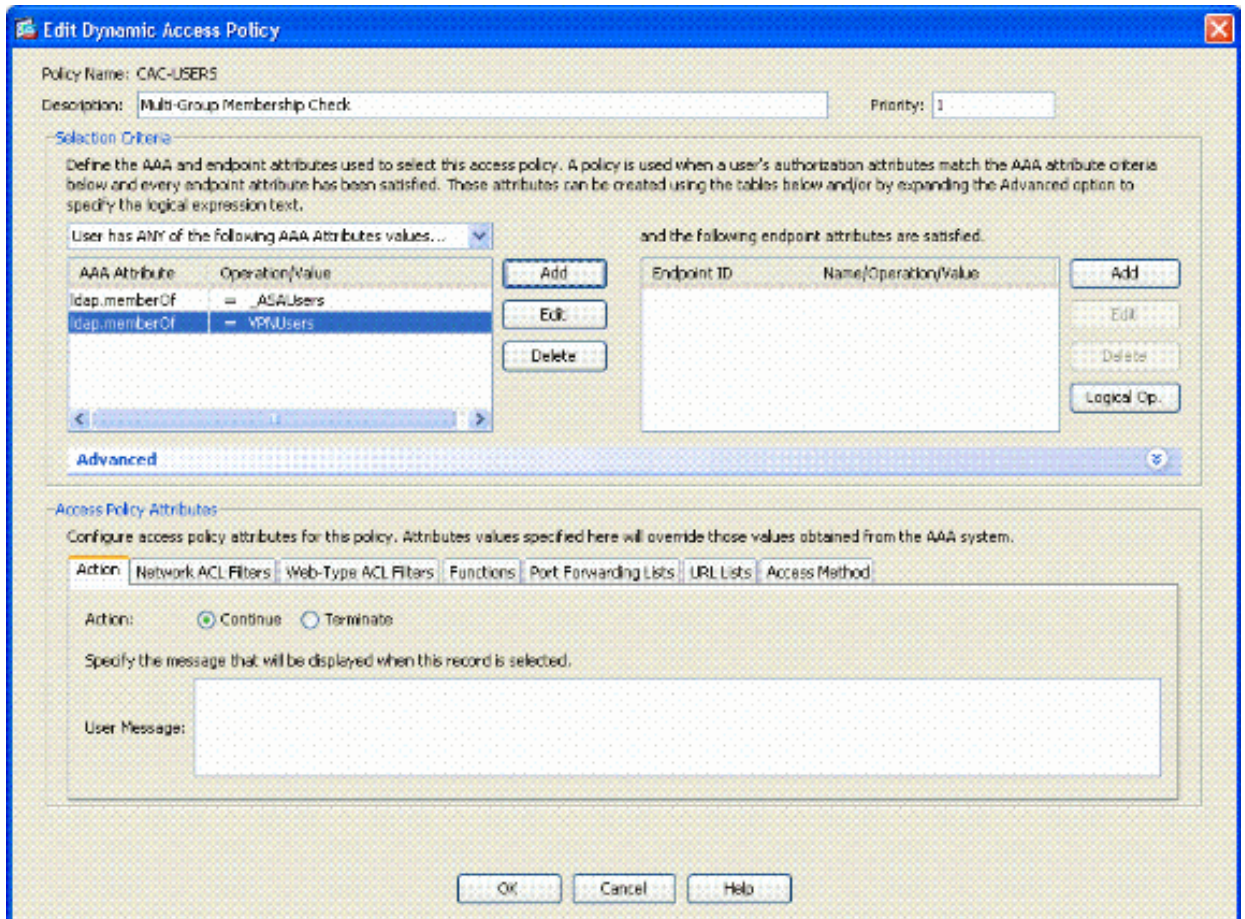
図 A10 : AAA 属性マップ



g. [OK] をクリックします。

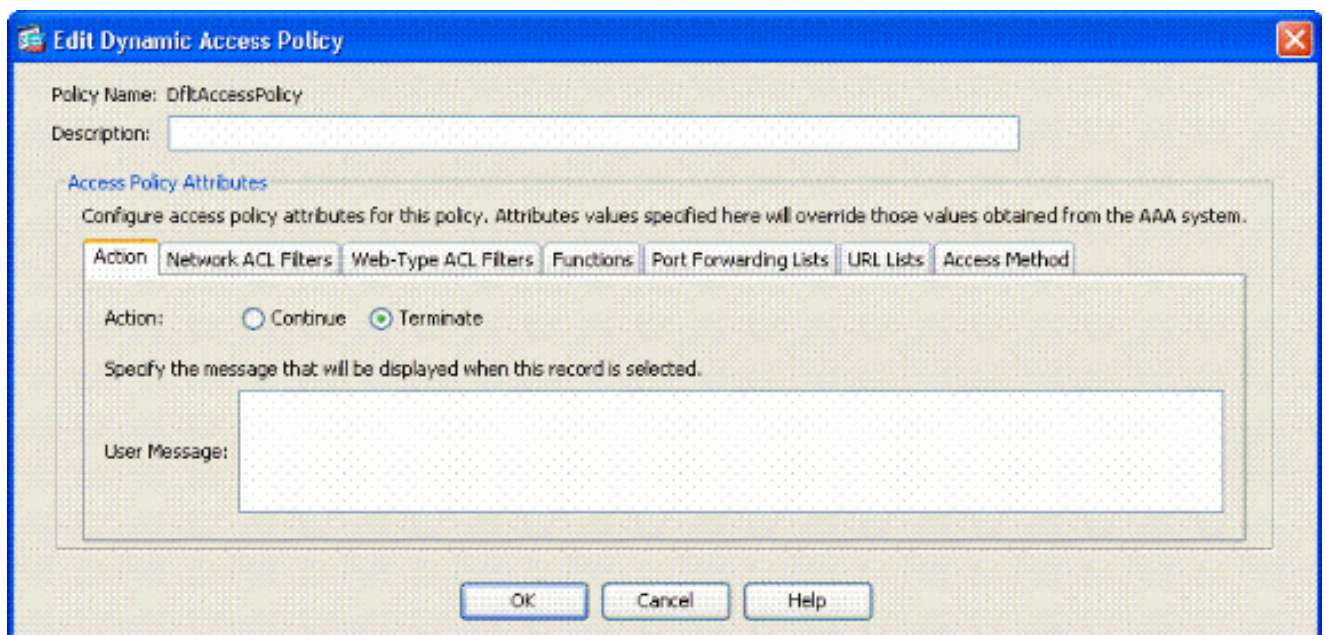
h. [Access Policy Attributes] セクションで、[Continue] を選択します。図 A11 を参照してください。

図 A11 : ダイナミック ポリシーの追加



4. ASDM で、[Remote Access VPN] > [Network (Client) Access] > [Dynamic Access Policies] を選択します。
5. [Default Access Policy] を選択し、[Edit] を選択します。
6. デフォルト アクションは [Terminate] に設定されます。図 A12 を参照してください。

図 A12 : ダイナミック ポリシーの編集



7. [OK] をクリックします。

注：デフォルトでは「続行」が選択されているため、「終了」が選択されていない場合は、どのグループにも属していなくても許可されます。

付録 B : ASA CLI 設定

ASA 5510

```
<#root>
ciscoasa#
show running-config
: Saved
:
ASA Version 8.0(2)
!
hostname asa80
domain-name army.mil
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface GigabitEthernet0/0
nameif outside
security-level 0
ip address x.x.x.x 255.255.255.128
!
interface GigabitEthernet0/1
nameif inside
security-level 100
no ip address
!
boot system disk0:/asa802-k8.bin
ftp mode passive
dns server-group DefaultDNS
domain-name army.mil
!
-----ACL's-----
access-list out extended permit ip any any
-----
pager lines 24
logging console debugging
mtu outside 1500
!
-----VPN Pool-----
ip local pool CAC-USERS 192.168.1.1-192.168.1.254 mask 255.255.255.0
-----
!
no failover
icmp unreachable rate-limit 1 burst-size 1
asdm image disk0:/asdm-602.bin
no asdm history enable
arp timeout 14400
access-group out in interface outside
route outside 0.0.0.0 0.0.0.0 172.18.120.129 1
```

```
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat
0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect
0:02:00
timeout uauth 0:05:00 absolute
!
-----LDAP Maps & DAP-----
ldap attribute-map memberOf
map-name memberOf Tunneling-Protocols
March 11, 2008 ASA - CAC Authentication for AnyConnect VPN Access
Company Confidential. A printed copy of this document is considered uncontrolled.
49
map-value memberOf CN=_ASAUsers,CN=Users,DC=gsgsec1ab,DC=org 20
ldap attribute-map msNPAAllowDialin
map-name msNPAAllowDialin Tunneling-Protocols
map-value msNPAAllowDialin FALSE 1
map-value msNPAAllowDialin TRUE 20
dynamic-access-policy-record CAC-USERS
description "Multi-Group Membership Check"
priority 1
dynamic-access-policy-record DfltAccessPolicy
action terminate
-----
!
-----LDAP Server-----
aaa-server AD-LDAP protocol ldap
aaa-server AD-LDAP (outside) host 172.18.120.160
ldap-base-dn CN=Users,DC=gsgsec1ab,DC=org
ldap-scope onelevel
ldap-naming-attribute userPrincipalName
ldap-login-password *
ldap-login-dn CN=Administrator,CN=Users,DC=gsgsec1ab,DC=org
-----
!
aaa authentication http console LOCAL
http server enable 445
http 0.0.0.0 0.0.0.0 outside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp authentication linkup linkdown coldstart
!
-----CA Trustpoints-----
crypto ca trustpoint ASDM_TrustPoint0
revocation-check ocsp
enrollment terminal
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
cr1 configure
crypto ca trustpoint ASDM_TrustPoint1
revocation-check ocsp
enrollment terminal
fqdn asa80
subject-name CN=asa80,OU=PKI,OU=DoD,O=U.S. Government,C=US
keypair DoD-1024
match certificate DefaultCertificateMap override ocsp trustpoint
ASDM_TrustPoint5 10 url http://ocsp.disa.mil
no client-types
cr1 configure
crypto ca trustpoint ASDM_TrustPoint2
```

```
revocation-check oosp
enrollment terminal
keypair DoD-2048
match certificate DefaultCertificateMap override oosp trustpoint
ASDM_TrustPoint5 10 url http://oosp.disa.mil
no client-types
cr1 configure
crypto ca trustpoint ASDM_TrustPoint3
revocation-check oosp none
enrollment terminal
cr1 configure
!
```

```
-----Certificate Map-----
```

```
crypto ca certificate map DefaultCertificateMap 10
subject-name ne ""
```

```
-----CA Certificates (Partial Cert is Shown)-----
```

```
crypto ca certificate chain ASDM_TrustPoint0
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311b3019 06035504 03131244 6f44204a 49544320 526f6f74
```

```
crypto ca certificate chain ASDM_TrustPoint1
certificate 319e
30820411 3082037a a0030201 02020231 9e300d06 092a8648 86f70d01
01050500
305c310b 30090603 55040613 02555331 18301606 0355040a 130f552e
532e2047
6f766572 6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06
0355040b
```

```
crypto ca certificate chain ASDM_TrustPoint2
certificate ca 37
3082044c 30820334 a0030201 02020137 300d0609 2a864886 f70d0101
05050030
60310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
f766e045 f15ddb43 9549d1e9 a0ea6814 b64bcece 089e1b6e 1be959a5
6fc20a76
```

```
crypto ca certificate chain ASDM_TrustPoint3
certificate ca 05
30820370 30820258 a0030201 02020105 300d0609 2a864886 f70d0101
05050030
5b310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 31163014 06035504 03130d44 6f442052 6f6f7420 43412032
301e170d
30343132 31333135 30303130 5a170d32 39313230 35313530 3031305a
305b310b
30090603 55040613 02555331 18301606 0355040a 130f552e 532e2047
6f766572
6e6d656e 74310c30 0a060355 040b1303 446f4431 0c300a06 0355040b
1303504b
```

```
49311630 14060355 0403130d 446f4420 526f6f74 20434120 32308201
crypto ca certificate chain ASDM_TrustPoint4
certificate ca 04
```

```
30820267 308201d0 a0030201 02020104 300d0609 2a864886 f70d0101
05050030
61310b30 09060355 04061302 55533118 30160603 55040a13 0f552e53
2e20476f
7665726e 6d656e74 310c300a 06035504 0b130344 6f44310c 300a0603
55040b13
03504b49 311c301a 06035504 03131344 6f442043 4c415353 20332052
6f6f7420
```

```
!
!
class-map inspection_default
match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
parameters
message-length maximum 512
policy-map global_policy
class inspection_default
inspect dns preset_dns_map
inspect ftp
inspect h323 h225
inspect h323 ras
inspect netbios
inspect rsh
inspect rtsp
inspect skinny
inspect esmtp
inspect sqlnet
inspect sunrpc
inspect tftp
inspect sip
inspect xdmcp
```

```
!
service-policy global_policy global
!
```

```
-----SSL/WEBvpn-windows-----
ssl certificate-authentication interface outside port 443
webvpn
enable outside
svc image disk0:/anyconnect-win-2.0.0343-k9.pkg 1
svc enable
tunnel-group-list enable
```

```
-----VPN Group/Tunnel Policy-----
group-policy CAC-USERS internal
ggroup-policy AC-USERS internal
group-policy AC-USERS attributes
vpn-windows-tunnel-protocol svc
address-pools value CAC-USERS
webvpn
svc ask none default svc
tunnel-group AC-USERS type remote-access
tunnel-group AC-USERS general-attributes
authorization-server-group AD-LDAP
default-group-policy AC-USERS
authorization-required
authorization-dn-attributes UPN
tunnel-group AC-USERS webvpn-windows-attributes
authentication certificate
group-alias AC-USERS enable
tunnel-group-map enable rules
```

```
no tunnel-group-map enable ou
no tunnel-group-map enable ike-id
no tunnel-group-map enable peer-ip
-----
prompt hostname context
```

付録 C : トラブルシューティング

AAA および LDAP のトラブルシューティング

- debug ldap 255 : LDAP データ交換を表示します
- debug aaa common 10 : AAA データ交換を表示します

例1 : 正しい属性マッピングを使用した接続の許可

この例は、付録 A に示すシナリオ 2 を使用した接続の成功における debug ldap および debug aaa common の出力を示します。

図C1:debug LDAPおよびdebug aaa commonの出力 : 正しいマッピング

```
AAA API: In aaa_open
AAA session opened: handle = 39
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: 172.18.120.160
AAA FSM: In AAA_SendMsg
User: 1234567890@mil
Pasw: 1234567890@mil
Resp:
[78] Session Start
[78] New request Session, context 0x26f1c44, reqType = 0
[78] Fiber started
[78] Creating LDAP context with uri=ldap:// 172.18.120.160:389
[78] Binding as administrator
[78] Performing Simple authentication for Administrator to
172.18.120.160
[78] Connect to LDAP server: ldap:// 172.18.120.160, status =
Successful
[78] LDAP Search:
Base DN = [CN=Users,DC=gsgsec1ab,DC=org]
Filter = [userPrincipalName=1234567890@mil]
Scope = [SUBTREE]
[78] Retrieved Attributes:
[78] objectClass: value = top
[78] objectClass: value = person
[78] objectClass: value = organizationalPerson
```

```
[78] objectClass: value = user
[78] cn: value = Ethan Hunt
[78] sn: value = Hunt
[78] userCertificate: value =
0..50...../.....60...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[78] userCertificate: value =
0..'0...../..t.....50...*.H.....0@1.0.....&....,d....com1.0.....
&....,d...
[78] givenName: value = Ethan
[78] distinguishedName: value = CN=Ethan
Hunt,OU=MIL,DC=labrat,DC=com
[78] instanceType: value = 4
[78] whenCreated: value = 20060613151033.0Z
[78] whenChanged: value = 20060622185924.0Z
[78] displayName: value = Ethan Hunt
[78] uSNCreated: value = 14050
[78] memberOf: value = CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org
[78] mapped to cVPN3000-Tunneling-Protocols: value = 20
[78] uSNChanged: value = 14855
[78] name: value = Ethan Hunt
[78] objectGUID: value = ..9...NJ..GU..z.
[78] userAccountControl: value = 66048
[78] badPwdCount: value = 0
[78] codePage: value = 0
[78] countryCode: value = 0
[78] badPasswordTime: value = 127954717631875000
[78] lastLogoff: value = 0
[78] lastLogon: value = 127954849209218750
[78] pwdLastSet: value = 127946850340781250
[78] primaryGroupID: value = 513
[78] objectSid: value = .....q.....mY...
[78] accountExpires: value = 9223372036854775807
[78] logonCount: value = 25
[78] sAMAccountName: value = 1234567890
[78] sAMAccountType: value = 805306368
[78] userPrincipalName: value = 1234567890@mil
[78] objectCategory: value =
[78] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
[78] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[78] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(CAC-USERS)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
```

```

User: CAC-USER
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 39, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunneling-Protocol(4107) 20 20
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunneling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "ggsgseclab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
In aaai_close_session (39)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
CAC-Test#

```

例2：誤って設定されたCisco属性マッピングによる接続の許可

この例は、付録 A に示すシナリオ 2 を使用した接続の許可における debug ldap および debug aaa common の出力を示します。

図C2:debug LDAPおよびdebug aaa commonの出力：誤ったマッピング

```

AAA API: In aaa_open
AAA session opened: handle = 41
AAA API: In aaa_process_async
aaa_process_async: sending AAA_MSG_PROCESS
AAA task: aaa_process_msg(1a87a64) received message type 0
AAA FSM: In AAA_StartAAATransaction
AAA FSM: In AAA_InitTransaction
Initiating authorization query (Svr Grp: AD-LDAP)

```



```
-----  
AAA FSM: In AAA_BindServer  
AAA_BindServer: Using server: 172.18.120.160  
AAA FSM: In AAA_SendMsg  
User: 1234567890@mil  
Pasw: 1234567890@mil  
Resp:  
[82] Session Start  
[82] New request Session, context 0x26f1c44, reqType = 0  
[82] Fiber started  
[82] Creating LDAP context with uri=ldap://172.18.120.160:389  
[82] Binding as administrator  
[82] Performing Simple authentication for Administrator to  
172.18.120.160  
[82] Connect to LDAP server: ldap:// 172.18.120.160:389, status =  
Successful  
[82] LDAP Search:  
Base DN = [CN=Users,DC=gsgsec1ab,DC=org]  
Filter = [userPrincipalName=1234567890@mil]  
Scope = [SUBTREE]  
[82] Retrieved Attributes:  
[82] objectClass: value = top  
[82] objectClass: value = person  
[82] objectClass: value = organizationalPerson  
[82] objectClass: value = user  
[82] cn: value = Ethan Hunt  
[82] sn: value = Hunt  
[82] userCertificate: value =  
0..50...../.....60...*.H.....0@1.0.....&....,d....com1.0.....  
&....,d...  
[82] userCertificate: value =  
0..'0...../..t.....50...*.H.....0@1.0.....&....,d....com1.0.....  
&....,d...  
[82] givenName: value = Ethan  
[82] distinguishedName: value = CN=Ethan  
Hunt,OU=MIL,DC=labrat,DC=com  
[82] instanceType: value = 4  
[82] whenCreated: value = 20060613151033.0Z  
[82] whenChanged: value = 20060622185924.0Z  
[82] displayName: value = Ethan Hunt  
[82] uSNCreated: value = 14050  
[82] memberOf: value = CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org  
[82] mapped to cVPN3000-Tunneling-Protocols: value =  
CN=ASAUsers,CN=Users,DC=gsgsec1ab,DC=org  
[82] uSNChanged: value = 14855  
[82] name: value = Ethan Hunt  
[82] objectGUID: value = ..9...NJ..GU..z.  
[82] userAccountControl: value = 66048  
[82] badPwdCount: value = 0  
[82] codePage: value = 0  
[82] countryCode: value = 0  
[82] badPasswordTime: value = 127954717631875000  
[82] lastLogoff: value = 0  
[82] lastLogon: value = 127954849209218750  
[82] pwdLastSet: value = 127946850340781250  
[82] primaryGroupID: value = 513  
[82] objectSid: value = .....q.....mY...  
[82] accountExpires: value = 9223372036854775807  
[82] logonCount: value = 25  
[82] sAMAccountName: value = 1234567890  
[82] sAMAccountType: value = 805306368  
[82] userPrincipalName: value = 1234567890@mil
```

```
[82] objectCategory: value =
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
[82] mail: value = Ethan.Hunt@labrat.com
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
[82] Fiber exit Tx=147 bytes Rx=4821 bytes, status=1
[82] Session End
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Authorization Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_AUTHORIZE, auth_status = ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_TUNN_GRP_POLICY,
AAA FSM: In AAA_InitTransaction
aaai_policy_name_to_server_id(USAFE)
Got server ID 0 for group policy DB
Initiating tunnel group policy lookup (Svr Grp: GROUP_POLICY_DB)
-----
AAA FSM: In AAA_BindServer
AAA_BindServer: Using server: <Internal Server>
AAA FSM: In AAA_SendMsg
User: CAC-USERS
Pasw:
Resp:
grp_policy_ioctl(12f1b20, 114698, 1a870b4)
grp_policy_ioctl: Looking up CAC-USERS
callback_aaa_task: status = 1, msg =
AAA FSM: In aaa_backend_callback
aaa_backend_callback: Handle = 41, pAcb = 2ae115c
AAA task: aaa_process_msg(1a87a64) received message type 1
AAA FSM: In AAA_ProcSvrResp
Back End response:
-----
Tunnel Group Policy Status: 1 (ACCEPT)
AAA FSM: In AAA_NextFunction
AAA_NextFunction: i_fsm_state = IFSM_TUNN_GRP_POLICY, auth_status =
ACCEPT
AAA_NextFunction: authen svr = <none>, author svr = AD-LDAP, user pol =
, tunn pol = CAC-USERS
AAA_NextFunction: New i_fsm_state = IFSM_DONE,
AAA FSM: In AAA_ProcessFinal
Checking time simultaneous login restriction for user 1234567890@mil
AAA FSM: In AAA_Callback
user attributes:
1 Tunnelling-Protocol(4107) 20 0
user policy attributes:
None
tunnel policy attributes:
1 Primary-DNS(4101) 4 IP: 10.0.10.100
2 Secondary-DNS(4102) 4 IP: 0.0.0.0
3 Tunnelling-Protocol(4107) 4 4
4 Default-Domain-Name(4124) 10 "gsgsec1ab.org"
5 List of address pools to assign addresses from(4313) 10
"CAC-USERS"
Auth Status = ACCEPT
AAA API: In aaa_close
AAA task: aaa_process_msg(1a87a64) received message type 3
```

```
In aaai_close_session (41)
AAA API: In aaa_send_acct_start
AAA API: In aaa_send_acct_stop
```

DAP のトラブルシューティング

- debug dap errors : DAP エラーを表示します
- debug dap trace : DAP 機能のトレースを表示します

例1:DAPで許可される接続

この例は、付録Aに示すシナリオ3を使用した接続の成功におけるdebug dap errorsおよびdebug dap traceの出力を示します。複数のmemberOf属性に注目してください。ユーザは _ASAUsers と VPNUsers の両方に属することも、いずれかのグループに属することもでき、ASA 構成によって決まります。

図C3 : デバッグDAP

```
<#root>
#
debug dap errors
debug dap errors enabled at level 1
#
debug dap trace
debug dap trace enabled at level 1
#
The DAP policy contains the following attributes for user:
1241879298@mil
-----
1: action = continue
DAP_TRACE: DAP_open: C8EEFA10
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
organizationalPerson
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
DAP_TRACE: Username: 1241879298@mil,
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
CN=1241879298,CN=Users,DC=ggsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
20070626163734.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
20070718151143.0Z
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.1 = VPNUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf.2 = _ASAUUsers
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
....+..F..5....
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
328192
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
128273494546718750
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
d.
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
9223372036854775807
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
1241879298
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
805306368
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["1"] =
"VPNUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"]["2"] =
```

```
"_ASAUUsers";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["tunnelgroup"] = "CACUSERS";
DAP_TRACE: dap_add_to_lua_tree:endpoint["application"]["clienttype"] =
"IPSec";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs: CAC-USERS
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 1 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
DAP_TRACE: Username: 1241879298@mil, DAP_close: C8EEFA10
d.
```

例2:DAPとの接続の拒否

この例は、付録 A に示すシナリオ 3 を使用した接続の失敗における debug dap errors および debug dap trace の出力を示します。

図C4 : デバッグDAP

```
<#root>
#
debug dap errors
```

```
debug dap errors enabled at level 1
```

```
#
```

```
debug dap trace
```

```
debug dap trace enabled at level 1
```

```
#
```

```
The DAP policy contains the following attributes for user:  
1241879298@mil
```

```
-----
```

```
1: action = terminate
```

```
DAP_TRACE: DAP_open: C91154E8
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.1 = top
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.2 = person
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.3 =
```

```
organizationalPerson
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectClass.4 = user
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.cn = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil,
```

```
aaa.ldap.physicalDeliveryOfficeName = NETADMIN
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.givenName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.distinguishedName =
```

```
CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.instanceType = 4
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenCreated =
```

```
20070626163734.0Z
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.whenChanged =
```

```
20070718151143.0Z
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.displayName = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNCreated = 33691
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.memberOf = DnsAdmins
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.uSNChanged = 53274
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.department = NETADMIN
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.name = 1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectGUID =
```

```
.....F..5.....
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userAccountControl =
```

```
328192
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPwdCount = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.codePage = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.countryCode = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.badPasswordTime = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogoff = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.lastLogon = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.pwdLastSet =
```

```
128273494546718750
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.primaryGroupID = 513
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userParameters = m:
```

```
d.
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectSid = ..
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.accountExpires =
```

```
9223372036854775807
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.logonCount = 0
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountName =
```

```
1241879298
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.sAMAccountType =
```

```
805306368
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.userPrincipalName =
```

```
1241879298@mil
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.objectCategory =
```

```
CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org
```

```
DAP_TRACE: Username: 1241879298@mil, aaa.ldap.msNPAAllowDialin = TRUE
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.username =
1241879298@mil
DAP_TRACE: Username: 1241879298@mil, aaa.cisco.tunnelgroup = CAC-USERS
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["1"] = "top";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["2"] =
"person";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["3"] =
"organizationalPerson";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectClass"]["4"] =
"user";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["cn"] = "1241879298";
DAP_TRACE:
dap_add_to_lua_tree:aaa["ldap"]["physicalDeliveryOfficeName"] =
"NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["givenName"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["distinguishedName"] =
"CN=1241879298,CN=Users,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["instanceType"] = "4";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenCreated"] =
"20070626163734.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["whenChanged"] =
"20070718151143.0Z";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["displayName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNCreated"] = "33691";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["memberOf"] = "DnsAdmins";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["uSNChanged"] = "53274";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["department"] = "NETADMIN";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["name"] = "1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectGUID"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userAccountControl"] =
"328192";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPwdCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["codePage"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["countryCode"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["badPasswordTime"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogoff"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["lastLogon"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["pwdLastSet"] =
"128273494546718750";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["primaryGroupID"] = "513";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userParameters"] contains
binary data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectSid"] contains binary
data
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["accountExpires"] =
"9223372036854775807";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["logonCount"] = "0";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountName"] =
"1241879298";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["sAMAccountType"] =
"805306368";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["userPrincipalName"] =
"1241879298@mil";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["objectCategory"] =
"CN=Person,CN=Schema,CN=Configuration,DC=gsgsec1ab,DC=org";
DAP_TRACE: dap_add_to_lua_tree:aaa["ldap"]["msNPAAllowDialin"] = "TRUE";
DAP_TRACE: dap_add_to_lua_tree:aaa["cisco"]["username"] =
"1241879298@mil";
DAP_TRACE: Username: 1241879298@mil, Selected DAPs:
```

```
DAP_TRACE: dap_request: memory usage = 33%
DAP_TRACE: dap_process_selected_daps: selected 0 records
DAP_TRACE: Username: 1241879298@mil, dap_aggregate_attr: rec_count = 1
```

認証局および OCSP のトラブルシューティング

- debug crypto ca 3
- コンフィギュレーション モードで logging class ca console (または buffer) debugging

これらの例では、OCSP レスポンダによる証明書検証の成功と、証明書グループ照合ポリシーの失敗を示します。

図 C3 は、検証された証明書と、動作中の証明書グループ照合ポリシーのデバッグ出力を示します。

図 C4 は、設定を誤った証明書グループ照合ポリシーのデバッグ出力を示します。

図 C5 は、無効になった証明書を持つユーザのデバッグ出力を示します。

図C5:OCSPデバッグ – 正常な証明書検証

```
CRYPTO_PKI: Found a suitable authenticated trustpoint
ASDM_TrustPoint11.
CRYPTO_PKI: Allocated OCSP data handle 0xca2d27b8
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting
to retrieve revocation status if necessary
CRYPTO_PKI: status = 0: poll revocation status
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for SSL.
CRYPTO_PKI: Processing map SSL sequence 20...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, map rule: subject-name ne "".
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.
CRYPTO_PKI: Found OCSP override match. Override URL:
http://198.154.68.90, Override trustpoint: ASDM_TrustPoint12
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()
CRYPTO_PKI: Destroying OCSP data handle 0xca2d27b8
Crypto CA thread sleeps!
CRYPTO_PKI: Attempting to find tunnel group for cert with serial
number: 0F192B, subject name:
cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
Government,c=US, issuer_name: cn=DOD JITC EMAIL CA-
15,ou=PKI,ou=DoD,o=U.S. Government,c=US.
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.
```



```
Government,c=US, map rule: subject-name ne "".  
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap  
sequence: 10.  
CRYPTO_PKI: Ignoring match on map DefaultCertificateMap, index 10 for  
WebVPN group map processing. No tunnel group is configured.  
CRYPTO_PKI: Peer cert could not be authorized with map:  
DefaultCertificateMap.  
CRYPTO_PKI: Processing map rules for SSL.  
CRYPTO_PKI: Processing map SSL sequence 20...  
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:  
= cn=MCGINTY.JIMMY.1160139435,ou=USN,ou=PKI,ou=DoD,o=U.S.  
Government,c=US, map rule: subject-name ne "".  
CRYPTO_PKI: Peer cert has been authorized by map: SSL sequence: 20.  
CRYPTO_PKI: Ignoring match on map SSL, index 20 for WebVPN group map
```

図C5 : 失敗した証明書グループ照合ポリシーの出力

図C5 : 失効した証明書の出力

```
n %PI=X-3-7E17t02h7a Certinf icaHtue cnhta,in faioled uvalidation=  
CMertifiIcLa,ted ccha=inl ais eibtrhaer tin,validid cor =noct  
oamuthori,zed.  
map rule: subject-name ne "".  
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap  
sequence: 10.  
Tunnel Group Match on map DefaultCertificateMap sequence # 10.  
Group name is CAC-USERS  
CRYPTO_PKI: Checking to see if an identical cert is  
already in the database...  
CRYPTO_PKI: looking for cert in handle=2467668, digest=  
CRYPTO_PKI: Cert record not found, returning E_NOT_FOUND  
CRYPTO_PKI: Cert not found in database.  
CRYPTO_PKI: Looking for suitable trustpoints...  
CRYPTO_PKI: Found a suitable authenticated trustpoint trustpoint0.  
CRYPTO_PKI: Certificate validation: Successful, status: 0. Attempting  
to retrieve revocation status if necessary  
CRYPTO_PKI: Attempting to find OCSP override for peer cert: serial  
number: 2FB5FC74000000000035, subject name: cn=Ethan  
Hunt,ou=MIL,dc=gsgsecclab,dc=org, issuer_name:  
cn=gsgsecclab,dc=gsgsecclab,dc=org.  
CRYPTO_PKI: Processing map rules for DefaultCertificateMap.  
CRYPTO_PKI: Processing map DefaultCertificateMap sequence 10...  
CRYPTO_PKI: Match of subject-name field to map PASSED. Peer cert field:  
= cn=Ethan Hunt,ou=MIL,dc=gsgsecclab,dc=org, map rule: subject-name  
ne "".  
CRYPTO_PKI: Peer cert has been authorized by map: DefaultCertificateMap  
sequence: 10.  
CRYPTO_PKI: Found OCSP override match. Override URL:  
http://ocsp.disa.mil, Override trustpoint: OCSP  
CRYPTO_PKI: crypto_pki_get_cert_record_by_subject()  
CRYPTO_PKI: Found a subject match  
ERROR: Certificate validation failed, Certificate is revoked, serial  
number: 2FB5FC74000000000035, subject name: cn=Ethan  
Hunt,ou=MIL,dc=gsgsecclab,dc=org  
CRYPTO_PKI: Certificate not validated
```

付録 D : MS 内の LDAP オブジェクトの確認

Microsoft Server 2003 の CD には、LDAP 構造と、LDAP オブジェクトおよび属性を表示するためにインストールできる追加のツールがあります。これらのツールをインストールするには、CD の Support ディレクトリに移動し、Tools ディレクトリを選択します。SUPTOOLS.MSI をインストールします。

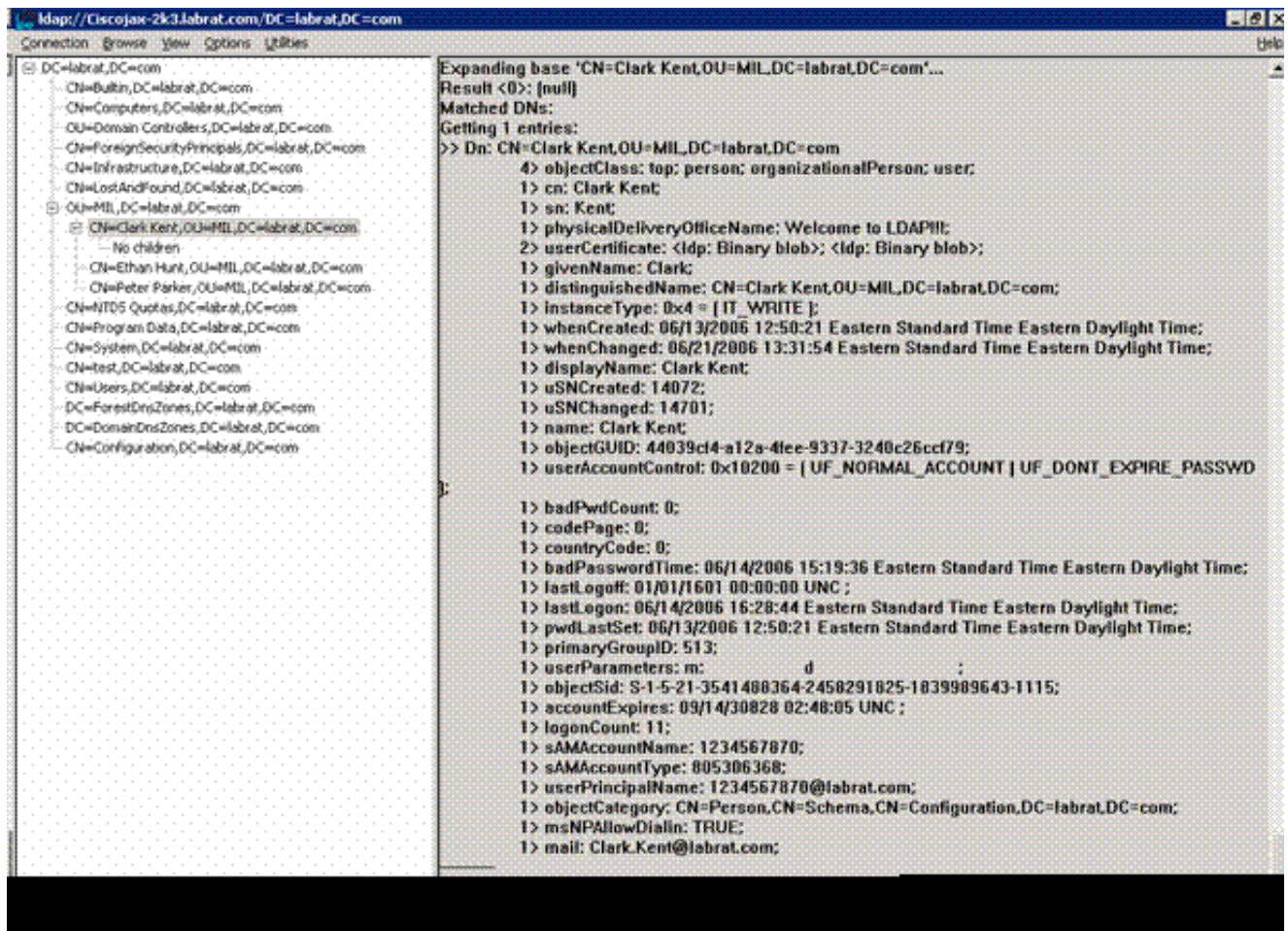
LDAP Viewer

1. インストールした後、[Start] > [Run] を選択します。
2. ldp と入力し、[OK] をクリックします。これで LDAP Viewer が始動します。
3. [Connection] > [Connect] を選択します。
4. サーバ名を入力して [OK] をクリックします。
5. [Connection] > [Bind] を選択します。
6. ユーザ名とパスワードを入力します。

注：管理者権限が必要です。

7. [OK] をクリックします。
8. LDAP オブジェクトを表示します。図 D1 を参照してください。

図D1:LDAPビューア

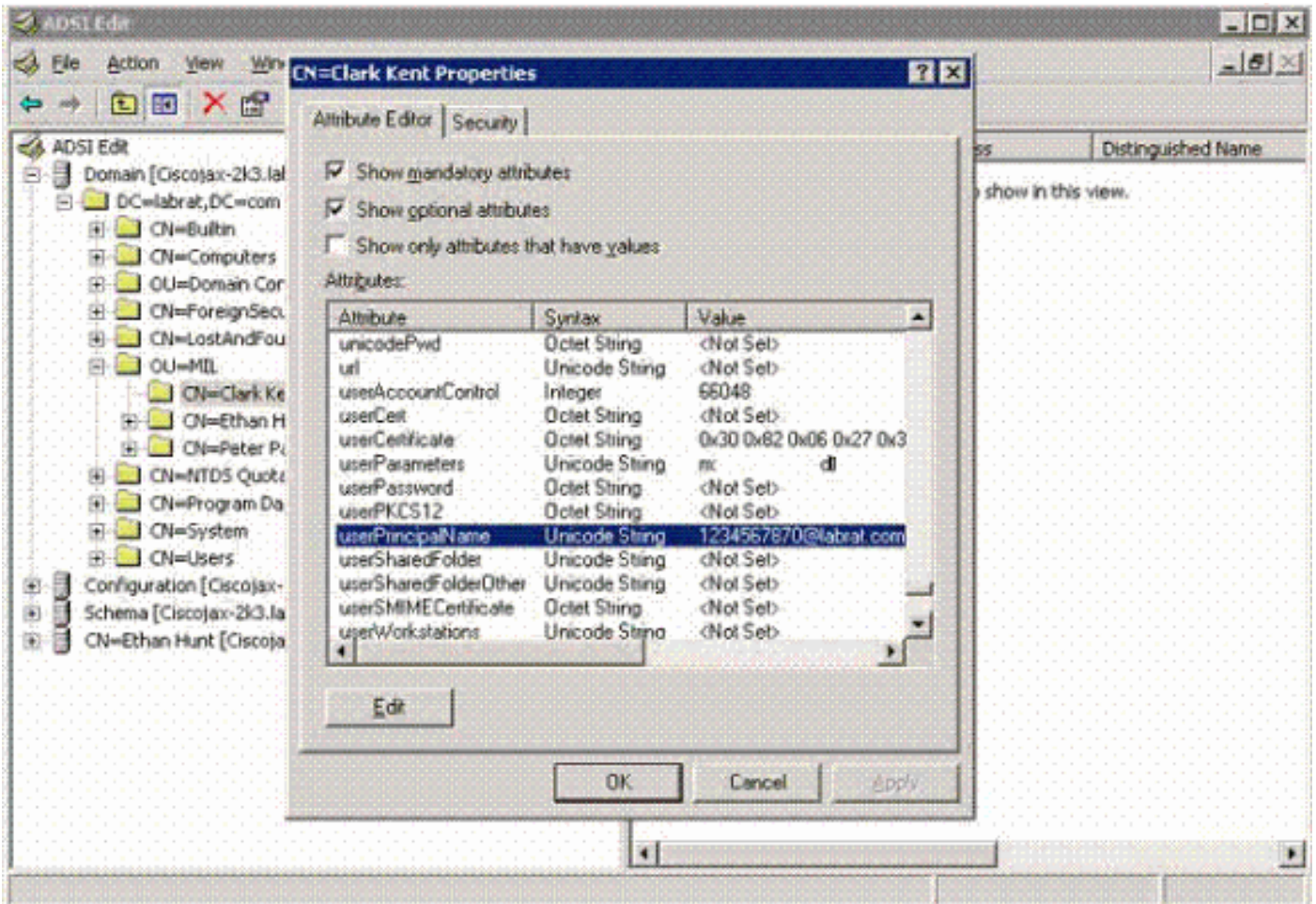


Active Directory サービス インターフェイス エディタ

- Active Directory サーバで、[Start] > [Run] を選択します。
- adsiedit.msc と入力します。これでエディタが始動します。
- オブジェクトを右クリックし、[Properties] をクリックします。

このツールは特定のオブジェクトのすべての属性を表示します。図 D2 を参照してください。

図D2:ADSI Edit



付録 E

AnyConnect プロファイルを作成してワークステーションに追加することができます。このプロファイルは、ASA ホストなどのさまざまな値や、識別名あるいは発行者などの証明書照合パラメータを参照できます。このプロファイルは .xml ファイルとして保存され、Notepad で編集できます。このファイルは各クライアントに手動で追加したり、グループ ポリシーを通じて ASA からプッシュしたりすることができます。ファイルは次の場所に保存されます。

C:\Documents and Settings\All Users\Application Data\Cisco\Cisco AnyConnect VPN Client\Profile

次のステップを実行します。

1. AnyConnectProfile.tmpl を選択し、ファイルを Notepad で開きます。
2. ファイルに対して発行者やホスト IP などの変更を行います。図 F1 の例を参照してください。
3. 完了したら、ファイルを .xml として保存します。

プロファイル管理については、Cisco AnyConnect のドキュメントを参照してください。つまり、

次のようになります。

- プロファイルには、ユーザ企業に固有の名前を付ける必要があります。例
: CiscoProfile.xml
- 会社内の個々のグループについて異なっていたとしても、プロファイル名は同じである必要があります。

このファイルは Secure Gateway 管理者によって保守され、クライアント ソフトウェアと一緒に配布されるためのものです。この XML に基づくプロファイルは、クライアントにいつでも配布できます。サポートされる配布メカニズムは、ソフトウェア配布のバンドル ファイルとしての配布か、自動ダウンロード メカニズムの一部としての配布です。自動ダウンロード メカニズムは、一部の Cisco Secure Gateway 製品でのみ使用できます。

注：管理者は、作成したXMLプロファイルをオンライン検証ツールで検証するか、ASDMのプロファイルインポート機能で検証することを強く推奨します。検証は、このディレクトリにある AnyConnectProfile.xsd を使用して実行できます。AnyConnectProfile は AnyConnect Client Profile を表すルート要素です。

これは、Cisco AnyConnect VPN クライアント プロファイル XML ファイルの例です。

```
<#root>

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">

!--- The ClientInitialization section represents global settings !--- for the client. In some cases, fo
!--
-->
-
<ClientInitialization>

!--- The Start Before Logon feature can be used to activate !--- the VPN as part of the logon sequence.
-->
<UseStartBeforeLogon UserControllable="false">>false</UseStartBeforeLogon>

!--- This control enables an administrator to have a one time !--- message displayed prior to a users
-->

<ShowPreConnectMessage>>false</ShowPreConnectMessage>
```

```

!-- This section enables the definition of various attributes !--- that can be used to refine client c
-->
-
<CertificateMatch>

!--- Certificate Distinguished Name matching allows !--- for exact match criteria in the choosing of a

- <DistinguishedName>
- <DistinguishedNameDefinition Operator="Equal" Wildcard="Disabled">
<Name>ISSUER-CN</Name>
<Pattern>DoD-Issuer-ABC</Pattern>
</DistinguishedNameDefinition>
</DistinguishedName>
</CertificateMatch>
</ClientInitialization>
-
!-- This section contains the list of hosts from which !--- the user is able to select.
-
<ServerList>

!--- This is the data needed to attempt a connection to !--- a specific host.

-->
-
<HostEntry>
<HostName>host-02</HostName>
<HostAddress>host-02.dod.gov</HostAddress>
</HostEntry>
- <HostEntry>
<HostName>host-01</HostName>
<HostAddress>192.168.1.1</HostAddress>
</HostEntry>
</ServerList>
</AnyConnectProfile>

```

関連情報

- [Certificates & CRLs specified by X.509 and RFC 3280](#)
- [OCSP specified by RFC 2560](#)
- [Public Key Infrastructure Introduction](#)
- [“Lightweight OCSP” profiled by draft standard](#)
- [SSL / TLS specified by RFC 2246](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。