ネットワーク アドミッション コントロールの設定

この章には、次の項があります。

用途、要件、および制約

ネットワーク アドミッション コントロール（NAC）は、実稼働状態でのネットワーク アクセスの条件として、エンドポイントにおける準拠性チェックと脆弱性チェックを実行することによって、ワーム、ウイルス、危険なアプリケーションの侵入や感染から企業ネットワークを保護します。これらのチェックは、ポスチャ検証と呼ばれます。ポスチャ検証を設定すると、IPSec セッションを確立するアンチウイルス ファイル、パーソナル ファイアウォール ルール、または侵入防止ソフトウェアが最新の状態であることを確認できます。ポスチャ検証では、リモート ホストで実行されているアプリケーションが、最新の修正プログラムによって更新されていることも確認できます。NAC は、IPSec や他のアクセス方式が提供するアイデンティティベースの検証を補完します。これは、ホーム PC など、ネットワーク ポリシーの自動適用の対象になっていないホストから企業ネットワークを保護する場合に特に便利です。

（注）　NAC をサポートするように設定されている場合、セキュリティ アプライアンスが Cisco Secure Access Control Server のクライアントとして機能するため、ネットワーク上に少なくとも 1 台の Cisco Secure Access Control Server をインストールして NAC 認証サービスを提供する必要があります。ASA による NAC のサポートは、リモート アクセス IPSec と L2TP over IPSec セッションに限られます。ASA 上の NAC は、WebVPN、VPN 以外のトラフィック、IPv6、およびマルチモードをサポートしません。

Access Control Server への接続の設定

次の各項の説明では、少なくとも 1 台の Access Control Server をネットワークに追加して NAC をサポートしていると想定します。

- Access Control Server グループの設定（P.9-2）
- ACS グループへの ACS の追加（P.9-4）
- ACS Server Group を NAC Authentication Server として割り当てる（P.9-6）

Access Control Server グループの設定

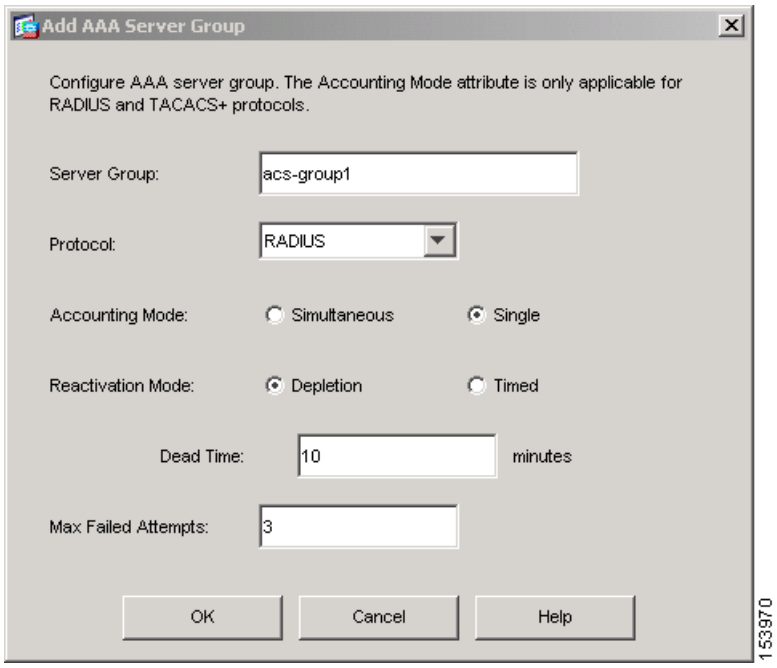
Access Control Server がネットワーク上に 1 台しかない場合でも、Access Control Server グループを設定する必要があります。

Access Control Server グループを設定する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Server Groups を選択し、AAA Server Groups テーブルの右側の **Add** をクリックします。

AAA Server Groups ウィンドウが開きます（図 9-1）。

図 9-1　Add AAA Server Group ウィンドウ



ステップ 2　次の説明に従って、このウィンドウのアトリビュートに値を割り当てます。

- **Server Group**：サーバ グループの名前を入力します。

（注） RADIUS サーバが Class アトリビュート（#25）を返すように設定されている場合、セキュリティ アプライアンス は、そのアトリビュートを使用してグループ名を認証します。RADIUS サーバ上で、アトリビュートは OU=*groupname* という形式を取ります。ここで *groupname* は、セキュリティ アプライアンス 上の Server Group で指定したサーバ グループ名です。

- **Protocol**：これが RADIUS か LDAP サーバ グループかを指定します。Access Control Server グループの **RADIUS** を選択します。
- **Accounting Mode**：（RADIUS および TACACS+ プロトコルのみ）**Simultaneous** をクリックすると、セキュリティ アプライアンス が課金データをグループ内のすべてのサーバに送信するように設定され、**Single** をクリックすると、課金データが 1 つのサーバだけに送信されます。
- **Reactivation Mode** : **Depletion** をクリックすると、サーバに障害が起こった場合、グループ内のすべてのサーバが非アクティブになった後でサーバが再度アクティブ化して接続されます。**Timed** をクリックすると、ダウンタイムが 30 秒経過した後、障害が起こったサーバが再度アクティブ化されます。
- **Dead Time**：（Depletion モードの場合のみ）グループ内の最後のサーバが無効になってから、すべてのサーバを再度有効にするまでの分数を入力します。
- **Max Failed Attempts** : 1 ～ 5 の範囲の整数を入力して、セキュリティ アプライアンス が何度接続を試みて失敗した後に、サーバの無応答、非アクティブを宣言するかを設定します。

ステップ 3　**OK** をクリックします。

AAA Server Groups テーブルに追加したグループが、Configuration > Properties >AAA Setup > AAA Server Groups テーブルに表示されます。

サーバをグループに追加するには、次の項の手順を実行します。

ACS グループへの ACS の追加

1 つ以上の Access Control Servers を ACS グループに追加する手順は、次のとおりです。

ステップ 1　Configuration > Properties > AAA Setup > AAA Server Groups を選択します。

AAA Server Groups テーブルに、このセキュリティ アプライアンスに設定されたグループが表示されます。

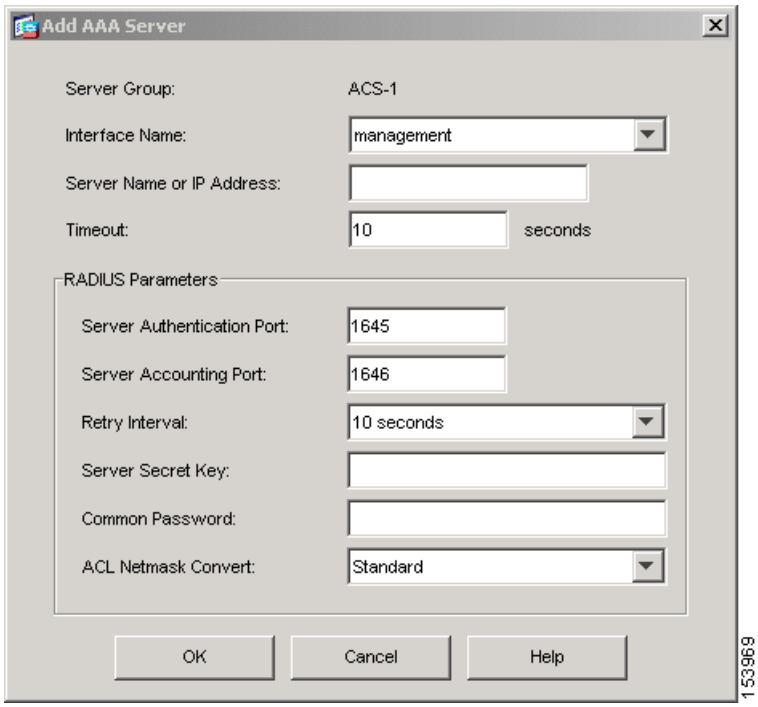
ステップ 2　前の項で作成した ACS グループを選択します。

グループが強調表示され、選択したグループ テーブルの Servers に、そのグループに含まれるサーバが表示されます。

ステップ 3　選択したグループ テーブルで、Servers の右側の **Add** をクリックします。

Add AAA Server ウィンドウが開きます（図 9-2）。

図 9-2　Add AAA Server ウィンドウ



ステップ 4　ACS に設定した値と同じ値を、このウィンドウのアトリビュートに値を割り当てます。アトリビュートの説明を以下に示します。

- **Server Group**：表示のみ。ACS サーバを追加するサーバ グループの名前が表示されます。
- **Interface Name**：セキュリティ アプライアンスがサーバへの接続に使用するネットワーク インターフェイスを選択します。
- **Server Name or IP Address**：AAA サーバの名前と IP アドレスを入力します。
- **Timeout**：タイムアウト間隔を秒数で入力します。セキュリティ アプライアンスは、この時間が期限切れになると、AAA サーバへの要求を放棄します。設定の中にスタンバイ AAA サーバが存在する場合に、プライマリ サーバへの接続がタイムアウトすると、セキュリティ アプライアンス が要求をバックアップ サーバに送信します。
- **Server Authentication Port**：ユーザ認証に使用するサーバのポート番号を入力します。デフォルト ポートは 1645 です。

（注）　最新の RFC では、RADIUS を UDP ポート番号 1812 に設定すべきだとしているので、このデフォルトは 1812 への変更が必要になる場合があります。

- **Server Accounting Port**：ユーザ課金に使用するサーバ ポートを入力します。デフォルト ポートは 1646 です。
- **Retry Interval**：サーバにクエリを送信し、応答がない場合に、再接続を試みるまでの秒数を入力します。秒数は、1 ～ 10 の範囲で入力します。デフォルト値は 10 秒です。
- **Server Secret Key**：暗号化に使用する、たとえば C8z077f のようなサーバ秘密鍵（「共有秘密鍵」とも呼ばれます）を入力します。この秘密鍵では、大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。セキュリティ アプライアンスは、Access Control Server への認証に、サーバ秘密鍵を使用します。ここで設定したサーバ秘密鍵は、Access Control Server で設定されたサーバ秘密鍵と一致する必要があります。最大フィールド長は、64 文字です。
- **Common Password**：グループの共通パスワードを入力します。パスワードは、大文字と小文字が区別されます。フィールドには、アスタリスクだけが表示されます。RADIUS サーバを許可ではなく認証に使用するよう定義する場合は、共通パスワードを設定しないでください。

  RADIUS 認証サーバでは、接続しようとする各ユーザのパスワードとユーザ名が必要です。パスワードはここに入力します。RADIUS 許可サーバの管理者は、このパスワードをセキュリティ アプライアンス経由で接続する各ユーザに関連付けて RADIUS サーバを設定する必要があります。この情報は、必ず RADIUS サーバの管理者に提供してください。このセキュリティ アプライアンス経由で RADIUS 許可サーバにアクセスするすべてのユーザの共通パスワードを入力します。

  このフィールドを空白のままにすると、各ユーザのユーザ名がパスワードになります。セキュリティ上の予防措置として、RADIUS 許可サーバを絶対に認証に使用しないでください。共通パスワードを使用したり、ユーザ名をパスワードとして使用したりすることは、各ユーザが強力なパスワードを持つことに比べて安全性が大きく劣ります。

（注）　RADIUS プロトコルではパスワード フィールドが必須であり、RADIUS サーバによっても要求されますが、ユーザはパスワードを知る必要がありません。

- **ACL Netmask Convert**：セキュリティ アプライアンスが、ダウンロード可能なアクセス リストで受け取ったネットマスクを処理する方法を選択します。セキュリティ アプライアンスは、ダウンロード可能なアクセス リストに、標準のネットマスク表現が含まれていると想定します。

ワイルドカード マスクには、無視するビット位置に 1 が、一致するビット位置に 0 が入っています。ACL Netmask Convert リストは、ダウンロード可能なアクセス リストの RADIUS サーバ上での設定方法の違いによる影響を最小限に抑えます。

Detect Automatically を選択すると、使用されているネットマスク表現のタイプをセキュリティ アプライアンスが判定します。ワイルドカード ネットマスク表現が検出された場合は、標準のネットマスク表現に変換されます。しかし、一部のワイルドカードは明確な検出が困難であるため、この設定を使用すると、ワイルドカード ネットマスク表現が、標準のネットマスク表現と誤解される場合があります。

Standard を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、標準ネットマスク表現だけが入っていると想定します。セキュリティ アプライアンスは、ワイルドカード ネットマスク表現を変換しません。

Wildcard を選択すると、セキュリティ アプライアンスは、RADIUS サーバから受け取ったダウンロード可能なアクセス リストに、ワイルドカード ネットマスク表現だけが含まれていると想定し、アクセス リストがダウンロードされたときにすべてを標準ネットマスク表現に変換します。

ステップ 5　**OK** をクリックします。

選択したグループ テーブルの Servers に、追加したサーバが表示されます。

ACS サーバをサーバ グループに追加したら、次の項の手順に従って、サーバ グループをグループ ポリシーに割り当てます。

ACS Server Group を NAC Authentication Server として割り当てる

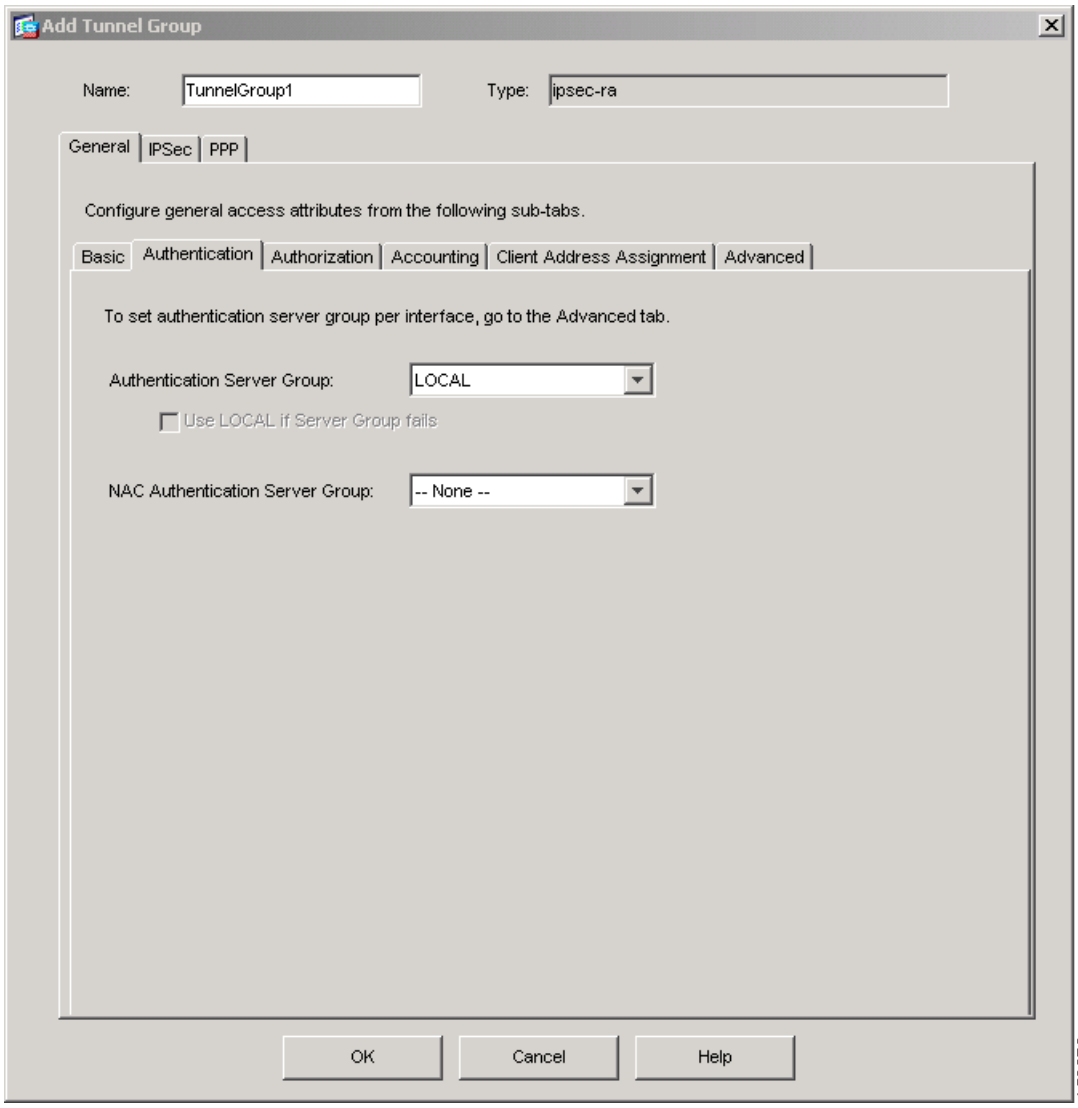
ACS Server Group を デフォルト トンネル グループの NAC Authentication Server として追加するか、または NAC のサポートを設定する代替トンネル グループに追加します。手順は次のとおりです。

ステップ 1　Configuration > VPN > General > Tunnel Group を選択します。

ステップ 2　DefaultRAGroup というトンネル グループをダブルクリックするか、リモート アクセス用に設定され、NAC サポートを設定する代替のトンネル グループ（Type は「ipsec-ra」）をダブルクリックするか、**Add** > **IPSec for Remote Access** をクリックして新しいトンネル グループを追加します。

ステップ 3　General タブ > Authentication タブをクリックします（図 9-3）。

図 9-3　General タブ > Authentication タブ



ステップ 4　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Authentication Server Group**：LOCAL グループ（デフォルト設定）などの利用可能な認証サーバ グループを一覧表示します。None も選択可能です。None または Local 以外のオプションを選択すると、Use LOCAL if Server Group Fails チェックボックスが利用できるようになります（Advanced タブでは、各インターフェイスに認証サーバ グループを割り当てられます）。
- **Use LOCAL if Server Group fails**：このアトリビュートをオンにすると、Authentication Server Group アトリビュートによって指定されたグループに障害が発生した場合、LOCAL データベースにフォールバックできます。フォールバックを無効にするには、このアトリビュートをオフにします。
- **NAC Authentication Server Group**：NAC をサポートするように設定された、少なくとも 1 台のサーバで構成される ACS グループを選択します。このセキュリティ アプライアンスに設定され、リモート アクセス トンネルで利用できる RADIUS タイプのすべてのサーバ グループ名が一覧表示されます。

ステップ 5　**OK** をクリックします。

NAC の有効化と NAC プロパティのグループ ポリシーへの割り当て

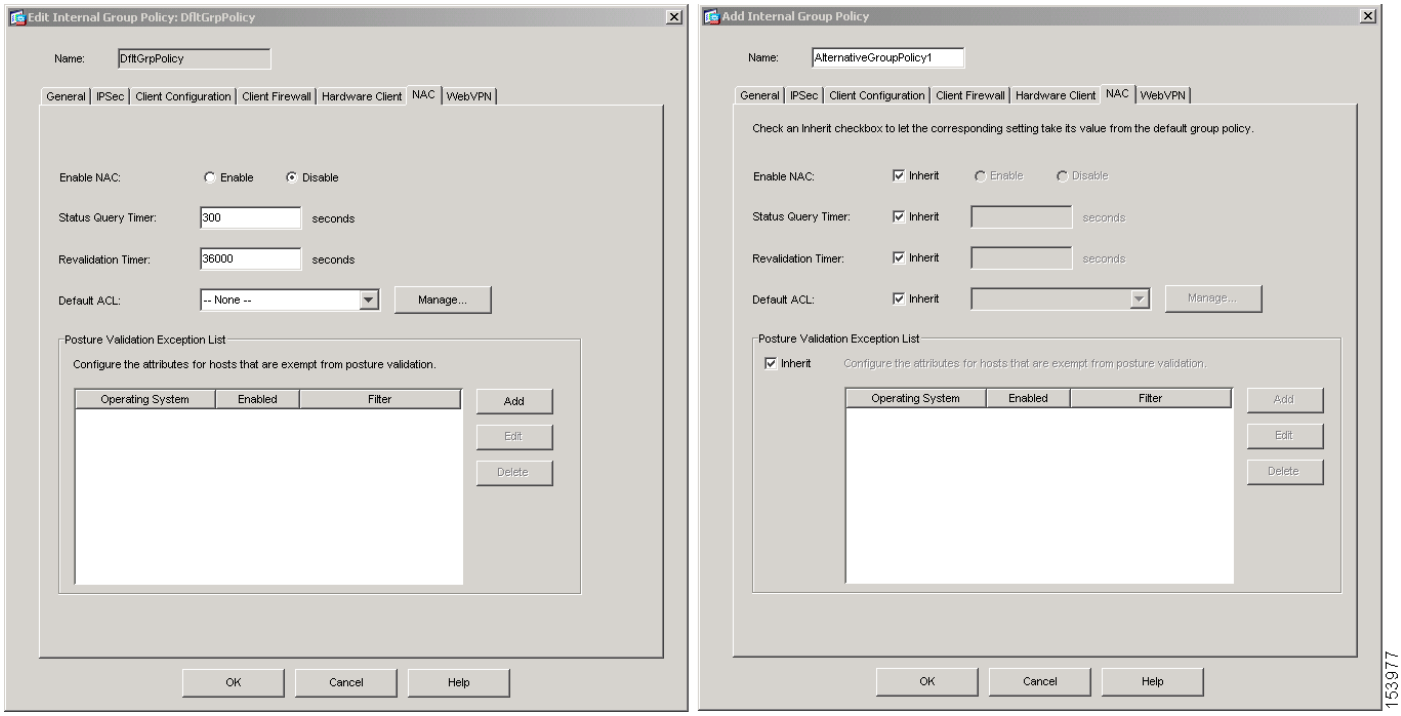
デフォルトのグループ ポリシー、または代替 IPSec グループ ポリシーで NAC を有効化し、そのデフォルト設定を表示して変更する手順は、次のとおりです。

ステップ 1　Configuration > VPN > General > Group Policy を選択します。

ステップ 2　DfltGrpPolicy というポリシーをダブルクリックするか、リモート アクセス用に設定され、NAC サポートを有効にする代替のグループ ポリシー（Tunneling Protocol は「IPSec」）をダブルクリックするか、**Add** > **Internal Group Policy** をクリックして新しいグループ ポリシーを追加します。

ステップ 3　NAC タブを開きます（図 9-4）。

図 9-4　DfltGrpPolicy の NAC タブと Alternative Group Policy



（注）　Alternative Group Policy の Inherit チェックボックスをオンにすると、デフォルトのグループ ポリシーの設定がポリシーとして使用されます。Inherit チェックボックスをオフにすると、デフォルト グループ ポリシー設定とは別個に代替グループ ポリシー設定をカスタマイズできます。

ステップ 4　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Enable NAC**：**Enable** をオンにすると、Network Admission Control プロシージャが実行されて、このグループ ポリシーに関連付けられた適格なホストが検証され、ポスチャ検証チェックに合格した場合は、それらに対して Access Control Server からダウンロードされた ACL が割り当てられます。**Disable** をオンにすると、NAC プロシージャは実行されません。

（注）　その他のアトリビュートは、NAC が有効な場合にだけ有効です。

- **Status Query Timer**：ポスチャ検証に合格するたびにセキュリティ アプライアンスがステータス クエリ タイマーを起動します。このタイマーが期限切れになると、リモート ホストに対してクエリが起動され、最後のポスチャ検証以降の変更点が問い合せられます。変更なしの応答が返された場合は、ステータス クエリ タイマーがリセットされます。ポスチャの変更を示す応答が返された場合は、無条件でポスチャの再検証が起動されます。セキュリティ アプライアンスは、再検証の間、現在のアクセス ポリシーを維持します。

  デフォルトで、ポスチャ検証合格からステータス クエリまでの間隔、およびそれ以降のステータス クエリの間隔は 300 秒（5 分）です。ステータス クエリ タイマーの値は、変更しない限り、デフォルトのグループ ポリシーからグループ ポリシーに継承されます。この値を変更するには、300 ～ 1800 秒（5 ～ 30 分）の範囲で数値を入力します。

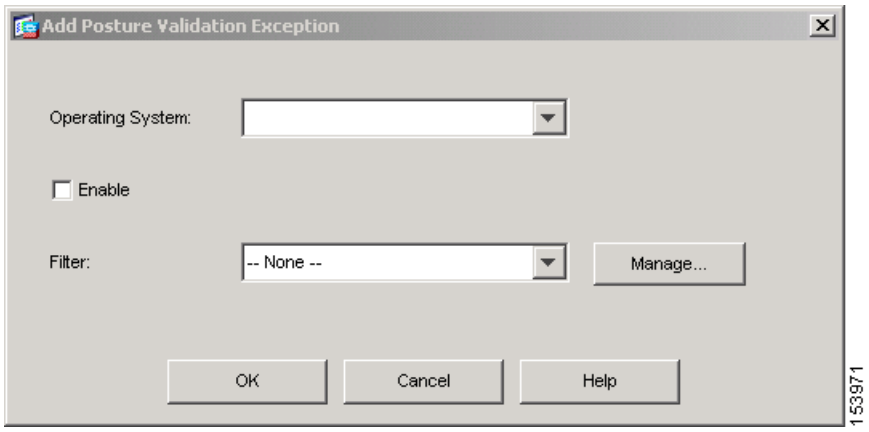
- **Revalidation Timer**：ポスチャ検証に合格するたびにセキュリティ アプライアンス が再検証タイマーを起動します。このタイマーが期限切れになると、次回のポスチャ検証が無条件で起動します。セキュリティ アプライアンスは、再検証の間、現在のアクセス ポリシーを維持します。デフォルトで、ポスチャ検証に合格してから次のポスチャ検証までの間隔は、36000 秒（10 時間）です。再検証タイマーの値は、変更しない限り、デフォルトのグループ ポリシーからグループ ポリシーに継承されます。この値を変更するには、300 ～ 86400 秒（5 分 ～ 24 時間）の範囲で数値を入力します。

- **Default ACL**：セキュリティ アプライアンスは、ポスチャ検証の前に、このアトリビュートによって識別された ACL を、NAC に適格なホストに適用します。ポスチャ検証の後、セキュリティ アプライアンスは、デフォルトの ACL の代わりに、Access Control Server からリモート ホスト用に取得した ACL を使用します。再検証に失敗した場合は、この ACL が適用されます。クライアントレス認証が有効な場合、セキュリティ アプライアンスは、Cisco Trust Agent を持たないホストにもこの ACL を適用してポスチャ検証要求に対応します。ACL を選択して NAC セッションのデフォルトの ACL として使用するか、デフォルト設定の **None** を使用してデフォルト ACL を適用しないようにします。

  ACL をドロップダウン リストに追加するには、リストに ACL の設定を表示するか、リストで ACL を変更して、**Manage** をクリックします。ACL Manager ウィンドウが開きます。手順については、P.2-14 の「ACL と ACE の管理」を参照してください。

- **Posture Validation Exception List**：Enabled カラムの Yes の値は、関連付けられたオペレーティング システムがポスチャ検証を免除されていることを示します。No の値は、設定内に免除エントリはあっても、セキュリティ アプライアンスがそれを無視していることを示します。Filter はオプションです。ポスチャ検証からのコンピュータの除外に加えて、コンピュータのオペレーティング システムが一致し、Enabled の値が Yes の場合、セキュリティ アプライアンスは Filter カラムで識別された ACL を適用して、トラフィックをフィルタリングします。リストでエントリを追加または変更するには、**Add** をクリックするか、変更するエントリをダブルクリックします。Add or Edit Posture Validation ウィンドウが開きます（図 9-5）。

図 9-5　Add Posture Validation Exception



ステップ 5　（Posture Validation Exception List を変更している場合のみ）次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Operating System**：ポスチャ検証から除外するリモート　コンピュータで実行されているオペレーティングシステムを選択するか、その名前を入力します。たとえば、**Windows XP** のように入力します。
- **Enable**：オンにすると免除が有効になります。デフォルト設定はオフで、免除リストから削除はされませんが、免除リストのエントリが無効になります。
- **Filter** は、コンピュータ上で動作しているオペレーティング システムが Operating System アトリビュートの値に一致する場合に、トラフィックに ACL を適用してフィルタリングします。フィルタを適用しない場合は、デフォルト オプションの **None** を使用します。使用する場合は、ドロップダウン リストから ACL を選択します。

  ACL をドロップダウン リストに追加するには、リストに ACL の設定を表示するか、リストで ACL を変更して、**Manage** をクリックします。ACL Manager ウィンドウが開きます。手順については、P.2-14 の「ACL と ACE の管理」を参照してください。

  Add or Edit Posture Validation でアトリビュートを設定した後、**OK** をクリックします。NAC タブでは、Posture Validation Exception List に、新しいエントリと変更されたエントリが表示されます。

ステップ 6　**OK**、**Apply** の順にクリックして、変更内容を実行コンフィギュレーションに保存します。

グローバル NAC 設定の変更

セキュリティ アプライアンスには、すべての NAC セッションに適用するデフォルトの設定が用意されています。この項の説明に従って、ネットワークで実行されているポリシーに合わせて、これらの設定を調整します。

ASA は、セキュリティ アプライアンスとリモート ホストとの間の通信を指定するアトリビュートに対して、デフォルトの設定を提供します。これらのアトリビュートは、有効期限カウンタの最大値を決定します。この値は、リモート ホスト上の Cisco Trust Agent を制限し、Cisco Trust Agent との通信のためのポート番号を指定します。

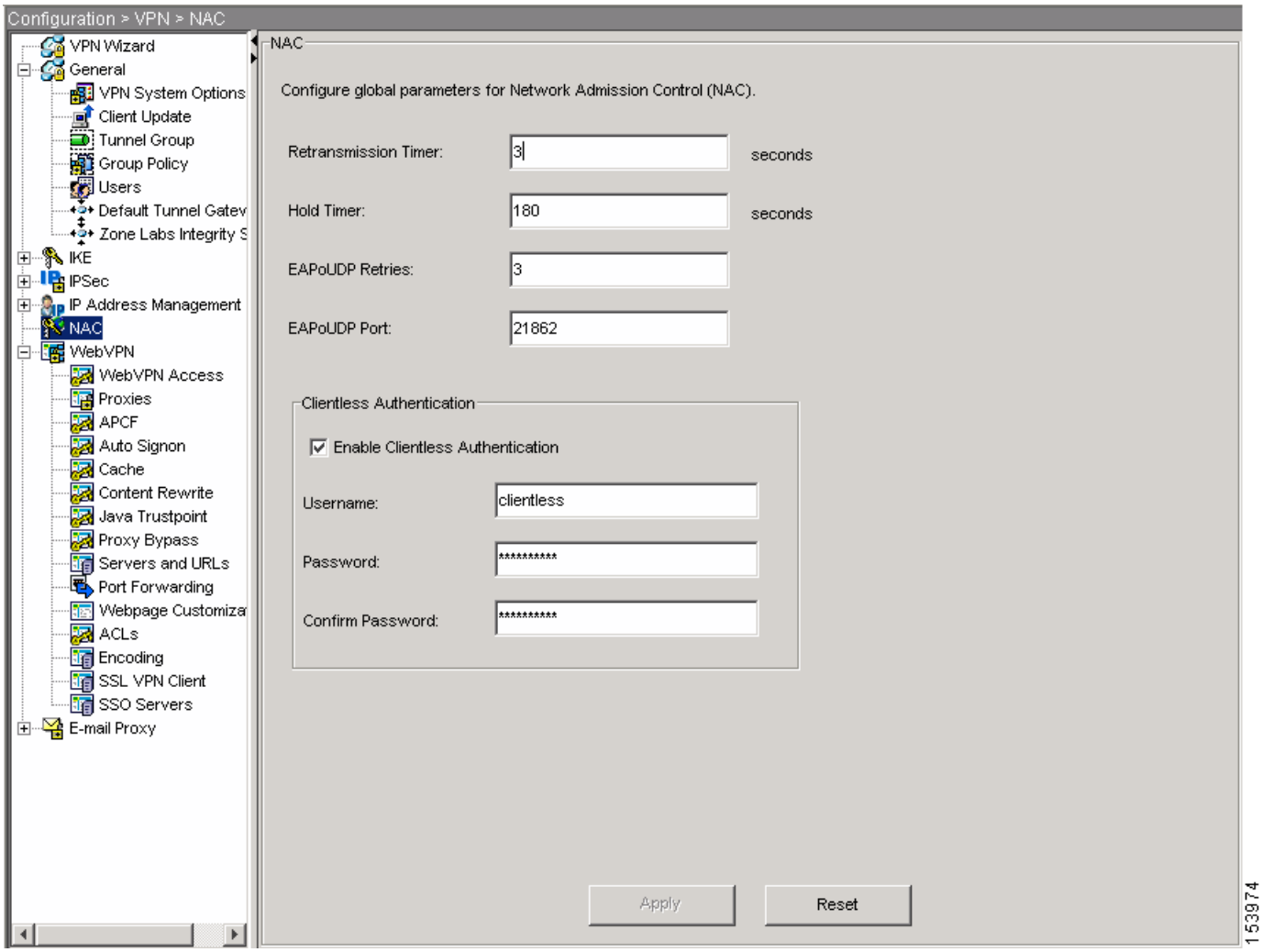
またグローバル NAC 設定では、クライアントレス認証の有効と無効を切り替えられます。この設定は、ポスチャ検証要求に応答する Cisco Trust Agent を持たないホストに対して、ポリシーを適用します。

NAC 設定を表示、変更する手順は、次のとおりです。

ステップ 1　Configuration > VPN > NAC を選択します。

ステップ 2　NAC ウィンドウが開きます（図 9-6）。

図 9-6　NAC



（注）　このウィンドウのアトリビュートは、セキュリティ アプライアンスが IPSec セッションに適用するグループ ポリシーで NAC が有効な場合にだけ有効です。

ステップ 3　次の手順に従って、このウィンドウのアトリビュートを設定します。

- **Retransmission Timer**：セキュリティ アプライアンスがリモート ホストにポスチャ検証を求める EAP over UDP 要求を送信し、応答を待ちます。このアトリビュートに割り当てられた秒数の間に応答がなければ、EAP over UDP メッセージが再送されます。デフォルトでは、再送信タイマーは 3 秒です。待ち時間の長さを変更するには、1 ～ 60 の範囲で値を入力します。
- **Hold Timer**：EAPoUDP Retries カウンタが EAPoUDP Retries の値に一致した場合、セキュリティ アプライアンスは、リモート ホストとの EAP over UDP セッションを終了して、このタイマーを再開始します。このアトリビュートが *n* 秒に等しい場合、セキュリティ アプライアンスは、リモートホストとの EAP over UDP セッションを確立します。デフォルトでは、新しいセッションを確立するまでの最大待ち時間は 180 秒です。秒数は、60 ～ 86400 （24 時間）の範囲で入力して変更します。
- **EAPoUDP Retries**：セキュリティ アプライアンスがリモート ホストに EAP over UDP メッセージを送信し、応答を待ちます。応答がなければ、EAP over UDP メッセージが再送信されます。デフォルトでは、再試行は最大 3 回行われます。この値を変更するには、1 ～ 3 の範囲で値を入力します。
- **EAPoUDP Port**：Cisco Trust Agent との EAP over UDP 通信に使用するクライアント エンドポイント上のポート番号を入力します。デフォルトのポート番号は 21862 です。この値を変更するには、1024 ～ 65535 の範囲で値を入力します。
- **Enable Clientless Authentication**：オンにすると、ポスチャ検証要求に応答する Cisco Trust Agent を持たないホストに対して、ポリシーを適用します。

  ホストが IPSec セッションの確立を試みると、セキュリティ アプライアンスはデフォルトのアクセス ポリシーを適用し、ポスチャ検証を求める EAP over UDP 要求を送信し、タイムアウトを要求します。セキュリティ アプライアンスが、クライアントレス ホストのポリシーを Access Control Server に要求するように設定されていない場合、そのクライアントレス ホストに対してすでに使用されているデフォルトのアクセス ポリシーが引き続き使用されます。

  クライアント認証が有効で、検証要求に対するリモート ホストからの応答がない場合、セキュリティ アプライアンスは、リモート ホストに代わってクライアントレス認証要求を Access Control Server に送信します。この要求には、Access Control Server 上でのクライアントレス認証用に設定されたクレデンシャルに一致するログインクレデンシャルが含まれます。Access Control Server は次にアクセス ポリシーを提供し、これがセキュリティ アプライアンスによって適用されます。

（注）　その他のアトリビュートは、**Enable Clientless Authentication** がオンの場合にだけ適用されます。

- **Username**：クライアントレス ホストをサポートするために、Access Control Server 上に設定されたユーザ名を入力します。デフォルトのユーザ名は、「clientless」です。このユーザ名を Access Control Server で変更した場合は、セキュリティ アプライアンスでも変更する必要があります。ユーザ名には、1 ～ 64 文字の ASCII 文字が入力できますが、先頭と末尾の空白、ポンド記号(#)、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< と >）は使用できません。
- **Password**：クライアントレス ホストをサポートするために、Access Control Server 上に設定されたパスワードを入力します。デフォルトのパスワードは、「clientless」です。このパスワードを Access Control Server で変更した場合は、セキュリティ アプライアンスでも変更する必要があります。パスワードには、4 ～ 32 文字の ASCII 文字が使用できます。
- **Confirm Password**：Password に入力したパスワードを再度入力して確認します。

ステップ 4　**Apply** をクリックして、変更内容を実行コンフィギュレーションに保存します。