Cisco Identity Services Engine を備えたネットワーク アクセス デバイス プロファイル

安全なアクセスの詳細ガイド シリーズ

目次

Cisco Systems © 2015

第 1 章 ネットワーク アクセス デバイス プロファイル

ネットワーク アクセス デバイス プロファイルについて

Cisco Identity Services Engine（ISE）2.0 により、シスコ以外の一部のネットワーク アクセス デバイス（NAD）がサポートされます。ISE は、MAB、ゲスト、BYOD、ポスチャなどのフローを有効にするために ISE が使用する NAD の機能と要件を*ネットワーク アクセス デバイス プロファイル*で処理します。

ISE 2.0 には多くの組み込み NAD プロファイルが付属しており、これらは [ネットワーク リソース（Network Resources）] の一覧に表示されます。

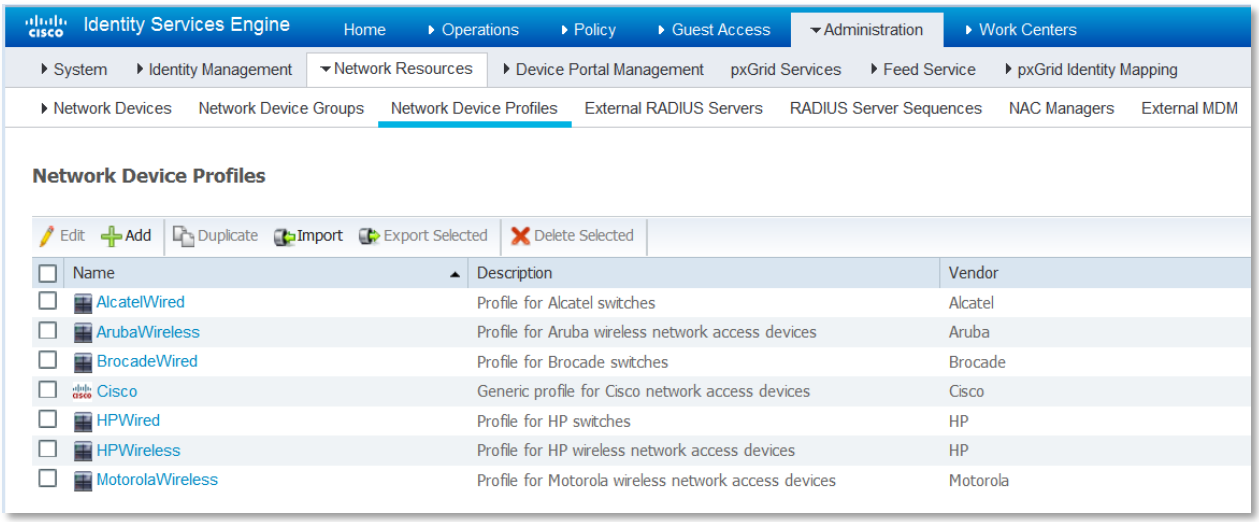

図 1. 組み込み NAD プロファイル

カスタムのネットワーク アクセス デバイス プロファイル

このガイドでは、組み込みプロファイルが十分でない場合のカスタム NAD プロファイルの作成方法について説明します。NAD プロファイルによって有効になる ISE フローの数は、NAD の機能によって異なります。

☞ ゲスト、BYOD、ポスチャなどの複雑なフローの場合、デバイスは RFC 5176、「認可変更」（CoA）、ISE ポータルへのリダイレクト、およびクライアント ID（MAC または IP アドレス）を URL パラメータとして渡すための URL リダイレクト メカニズムをサポートする必要があります。NAD でこれらの機能がサポートされていないと、複雑なフローは機能しません。

第 2 章 カスタム プロファイルを作成するためのステップ

概要

新しい NAD プロファイルを定義する前に、デバイスに関するいくつかの情報を特定しておく必要があります。通常は、NAD プロファイルを作成する前に、デバイスの新しい RADIUS ディクショナリをインポートする必要があります。CoA/URL リダイレクトをサポートするために、デバイスのファームウェアを新しいバージョンにアップグレードする必要がある場合もあります。また、通常はデバイスの設定変更を行い、特定の機能、特に URL リダイレクトを設定または有効化する必要があります。完了したら、新しい NAD プロファイルを ISE で作成し、適切なデバイスに割り当てます。最後に、新しいプロファイルを使用するために新しい認証プロファイルと ISE ポリシーを設定します。

推奨される手順

情報の収集

ステップ 1 NAD の *管理マニュアル*を参照します（多くの場合探している情報があります）
ステップ 2 存在する場合にはどの RADIUS ディクショナリが必要かを特定し、ISE にインポートします
ステップ 3 どの属性が MAB、SSID、VLAN の設定、ACL（該当する場合）に使用されているかを特定します
ステップ 4 RADIUS CoA がサポートされているかどうかと、CoA 要求でどの属性が要求されるかを特定します
ステップ 5 URL リダイレクトがサポートされているかどうかと、どの属性と URL パラメータが使用されるかを特定します

デバイス設定

ステップ 6 NAD ファームウェアが十分なレベルであることを確認し、必要な場合にはアップグレードします
ステップ 7 NAD で必要な設定変更を行います（CoA/URL リダイレクトに対して）

プロファイルの作成と割り当て

ステップ 8 上記から得た情報を使用して新しい NAD プロファイルを作成します
ステップ 9 新しいプロファイルを 1 つ以上の NAD に割り当てます

ポリシーの設定

ステップ 10 新しい認証プロファイルを作成します
ステップ 11 新しい NAD プロファイルを活用するように ISE ポリシーを設定します
ステップ 12 期待される動作を確認します

これらのステップについては、以降の章で詳しく説明します。

第 3 章 RADIUS ディクショナリ

ディクショナリをインポートする必要があるかどうかの確認

NAD のマニュアルを参照して、NAD がどの RADIUS ディクショナリを使用するかを特定します。ほとんどの NAD には、標準の IETF RADIUS 属性に加えて多数のベンダー固有の属性を提供する、ベンダー固有の RADIUS ディクショナリがあります。MAB、CoA、URL リダイレクト、ACL、VLAN、SSID などの機能は、すべて潜在的に RADIUS 属性を使用し、この属性が IETF ではなくベンダー固有（VSA）である場合もあります。

RADIUS ディクショナリのインポート

デバイスが VSA を使用する場合は、通常、NAD プロファイルに割り当てる前に ISE に RADIUS ディクショナリをインストールする必要があります。ISE には、*freeradius* 形式で RADIUS ディクショナリ ファイルをインポートする機能があります。この機能は、*[ポリシー要素（Policy Elements）]→[ディクショナリ（Dictionaries）]→[システム（System）]→[Radius]→[RADIUS ベンダー（RADIUS Vendors）]* にあります。

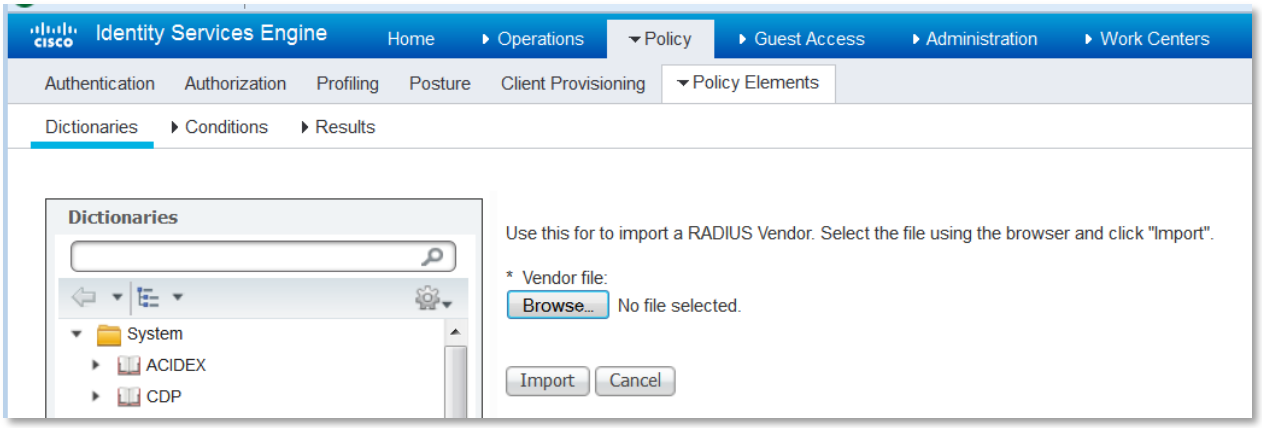

図 2. RADIUS ディクショナリのインポート

正常にインポートされると、新しいディクショナリが RADIUS ディクショナリ ベンダーの一覧に表示されます。

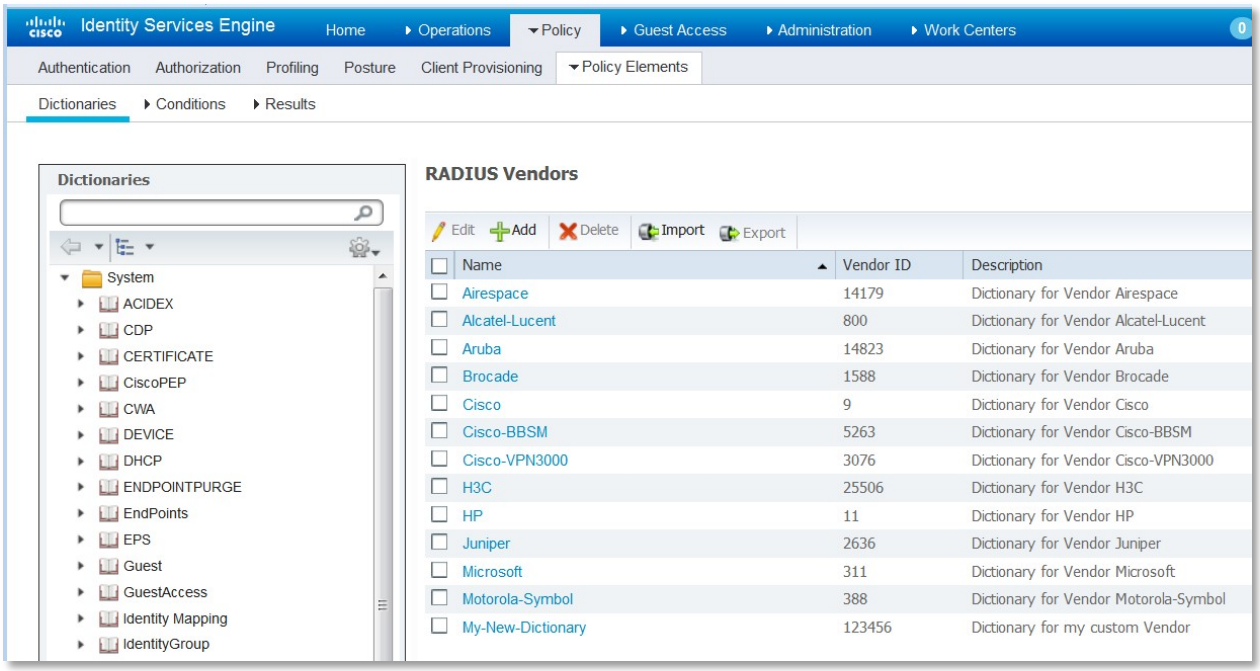

図 3. 新しくインポートされたディクショナリ

第 4 章 カスタム プロファイルの定義

新しいプロファイル エントリの作成

必要な情報を集め、RADIUS ディクショナリをインストールしたら、[新しいネットワーク デバイス プロファイル（New Network Device Profile）] をクリックして新しい NAD プロファイルを作成します。NAD プロファイルの新しい名前と説明を作成します。名前はポリシー条件とトラブルシューティングに役立ち、レポートに表示されます。新しいプロファイルに固有のアイコンを割り当てて、他のプロファイルと区別しやすくすることができます。

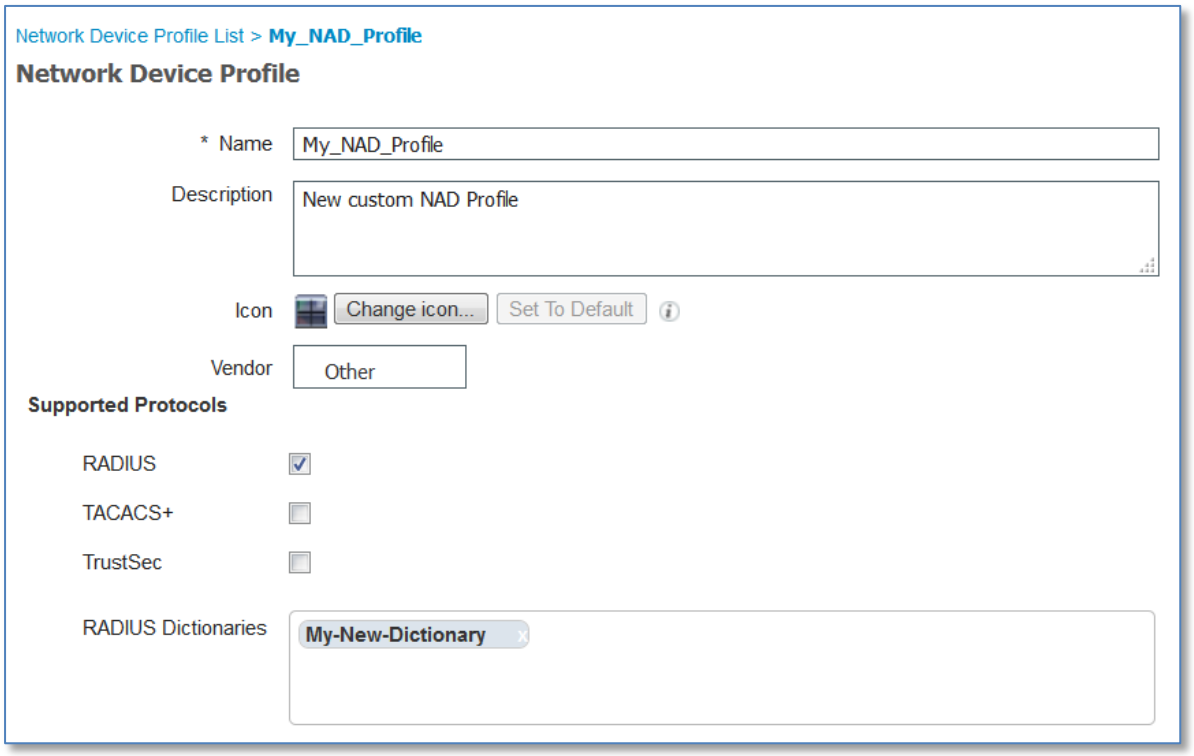

図 4. 新しい NAD プロファイル

ベンダーについて、いずれかの組み込みプロファイルと似たデバイス用の NAD プロファイルを作成する場合、つまり、同じベンダーでいくつかの違いがある別のモデルを使用する場合は、既存の NAD プロファイルを複製してカスタマイズすることが最善です。複製されたプロファイルには元のプロファイルの設定がコピーされているため、最初から定義するのではなく、この設定を微調整するだけで済みます。現在のもので十分な場合には、新しい RADIUS ディクショナリを定義する必要がない場合もあります。

ただし、NAD ベンダーが既存のものと一致しない場合には、[ベンダー（Vendor）] フィールドを [その他（Other）] に設定し、その特性をすべて入力する必要があります。

サポートされるプロトコル

デバイスが RADIUS、TACACS+、TrustSec をサポートする場合には、各ボックスにマークを付けます。実際に使用するプロトコルにのみマークを付ける必要があります。

RADIUS ディクショナリ

デバイスがサポートする RADIUS ディクショナリを割り当てます。通常は、前のステップで事前にインポートしたディクショナリです。

(注)一部のデバイスは複数のベンダー ディクショナリをサポートするため、1 つ以上のディクショナリを割り当てることができます。

フロー タイプ条件

有線 MAB や 802.1x などのさまざまなフローのためにデバイスが使用する属性と値を [フロー タイプ条件(Flow Type Conditions)] セクション([認証/認可(Authentication/Authorization)] の下)に入力します。これは、ISE が使用される属性に応じてデバイスに適したフロー タイプを検出するために必要です。MAB 用の IETF 標準がないため、ベンダーごとに異なる値が Service-Type に使用されています。デバイスの管理者ガイドに記載されていない場合には、この値を特定するためにスニファ トレースを使用する必要がある場合があります。

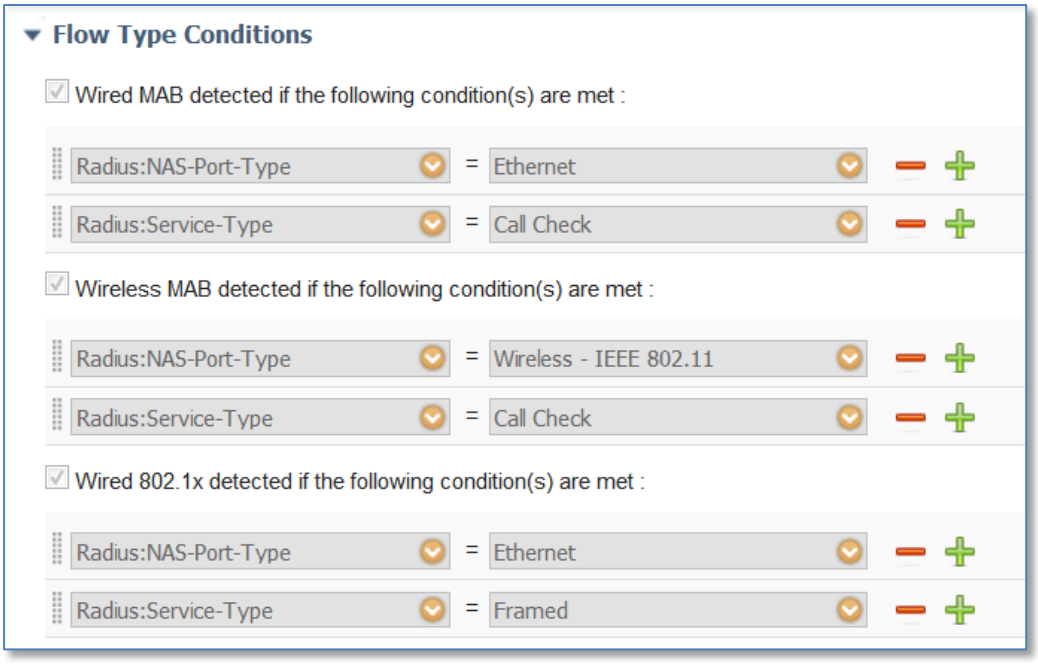

図 5. フロー タイプ条件

属性のエイリアシング

このセクションでは、デバイス固有の属性名を共通名にマップして、ポリシー ルールを簡素化することができます。現在は、「SSID」のみが定義されています。デバイスにワイヤレス SSID の概念がある場合には、使用される属性に対してこれを設定します。

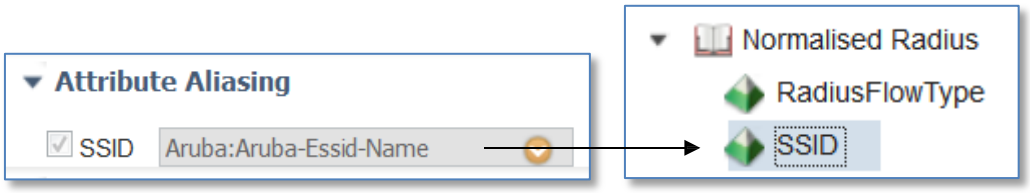

図 6. 属性のエイリアシング（SSID）

属性のエイリアシングにより、NAD プロファイルがベンダー固有の属性を共通属性にマップして、ポリシー ルールがフレンドリ名を使用できるようになります。これにより属性の選択が容易になり、さまざまなベンダー デバイスに必要な認証/認可ポリシー ルールの数が減り、潜在的なエラーが少なくなります。たとえば、フローに関与するワイヤレス SSID を、関与する NAD のタイプに応じて、Airespace-Wlan-ID、Aruba-ESSID-Name、Called-Station-ID に含めることができます。「正規化された Radius」ディクショナリでこれを利用可能な「SSID」属性にマップすることができます（[ポリシー（Policy）] > [ポリシー要素（Policy Elements）] > [ディクショナリ（Dictionaries）] > [正規化された Radius（Normalised Radius）] > [SSID]）。

ホスト ルックアップ

このセクションでは、デバイスが MAB 用に使用する属性とプロトコルを定義することができます。2.0 より前では、これは [許可されているプロトコル（Allowed Protocols）] ページのチェックボックスのさまざまな不明瞭な組み合わせで行っていて、複数の許可されているプロトコルのエントリが必要になる可能性がありました。現在は、ホスト ルックアップは NAD プロファイルにカプセル化され、設定が簡素化されました。

[許可されているプロトコル（Allowed Protocols）] ページで [ホスト ルックアップの処理（Process Host Lookup）] オプションが有効化されている場合、ホスト ルックアップ要求が NAD プロファイル設定（特に [ホスト ルックアップ（MAB）（Host Lookup（MAB））] の設定）に基づいて処理されます。

（シスコ以外の）さまざまなベンダーが、MAB 認証の際に RADIUS *Calling-Station-ID* とパスワードの属性をさまざまな方法で入力します。Cisco NAD が MAB を行うには、[ホスト ルックアップの処理（Process Host Lookup）] オプションを有効化するだけで十分です。ただし、別のベンダーのデバイスの場合は、NAD プロファイルを作成する際に [ホスト ルックアップ（MAB）（Host Lookup（MAB））] セクションで適切なオプションを有効化する必要があります。

前述のとおり、MAB の標準はないので、使用される属性とプロトコルはベンダーごとに異なります。このセクションの正しい設定を特定するには、デバイスの管理者ガイドまたは MAB のスニファトレースを参照してください。

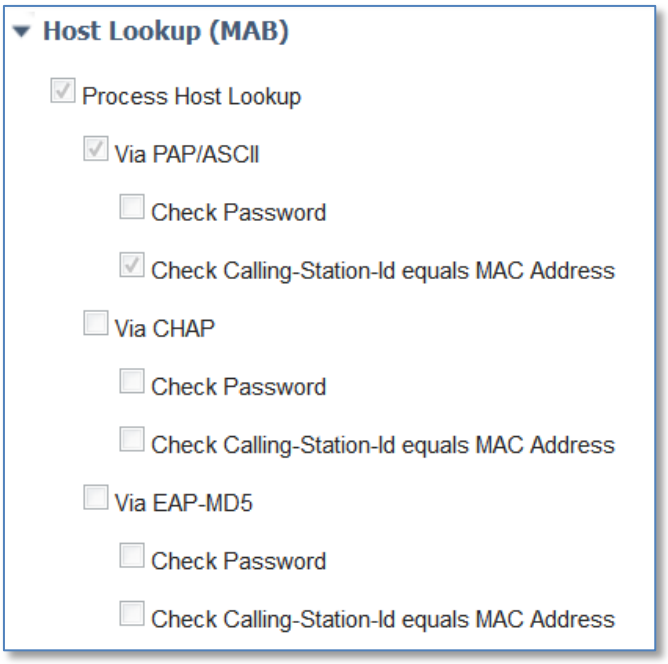

図 7. ホスト ルックアップ（MAB）

権限

このセクションは、VLAN または ACL の設定にデバイスが使用する属性を定義します。IETF 標準属性またはベンダー固有の属性が使用できます。これらは通常、デバイスの管理者ガイドで公開されています。

VLAN 権限の場合、複数の RADIUS 属性値ペア、または単一の RADIUS 属性（Aruba-User-VLAN など）を指定できます。

ACL 権限の場合、現在の NAD プロファイルに関連する NAD で名前付き ACL を設定するために使用される、単一の RADIUS 属性を指定できます。

（注）[認証プロファイル（Authorization Profile）] ページの [共通タスク（Common Tasks）] セクションに表示されるオプションは、[NAD プロファイル権限（NAD Profile Permission）] セクションで設定した属性によって異なります。

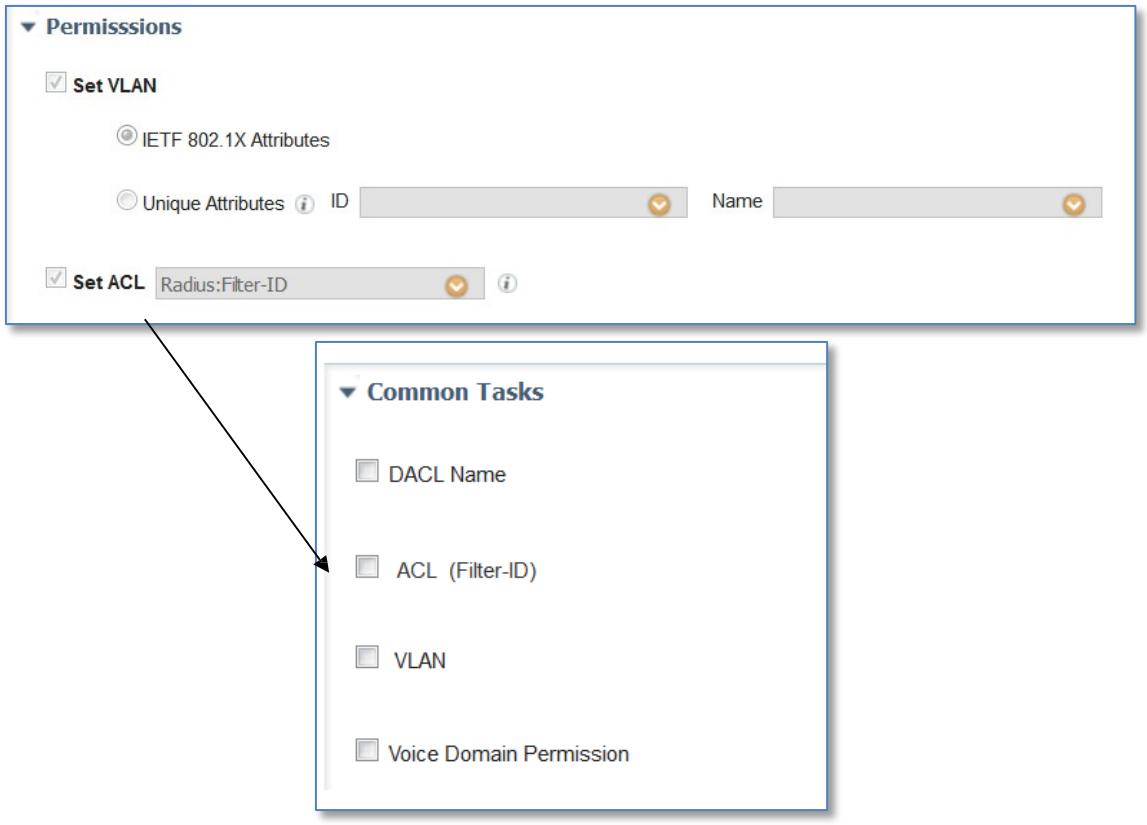

図 8. 権限と共通タスクに対する関係

認可変更(CoA)

このセクションでは、デバイスが持つ CoA 機能を定義することができます。詳細については、デバイスのマニュアルを参照し、「RFC 5176」、「認可変更」、「CoA」などの用語に対する記述を探してください。RFC 5176 をサポートするシスコ以外のほとんどのデバイスは「プッシュ」および「切断」をサポートしますが、再認証はサポートしないため、確信がない場合には「RFC 5176」と示された 2 つのチェックボックスの有効化を試みます。

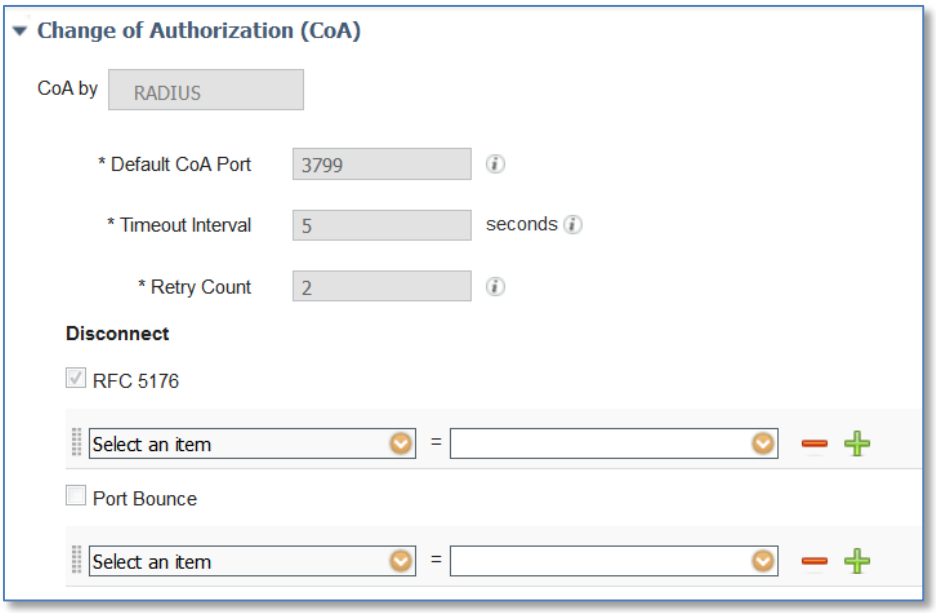

図 9. CoA 設定

RFC 5176 は CoA 要求のタイプを定義しますが、要求で必要な属性はデバイスによって異なります。一部のデバイスでは、CoA 要求で送信される属性に対して非常に細かい指定があります。

CoA 要求がデバイスから CoA「NAK」を返される場合には、次のいくつかのヒントを確認してください。

- access-request からの RADIUS User-Name 属性が CoA 要求に含まれている必要がある場合があります
- 同じ要求で送信された Calling-Station-ID と Acct-Session-ID の両方が受け入れられない場合があります（一方を送信します）
- 要求の他のベンダーの VSA が受け入れられない場合があります
- 一部のデバイスは、Event-Timestamp と上記の CoA 設定が一致する必要がある（または必要がない）ように設定することができます

一部の管理者ガイドでは属性が公開されていますが、一部では公開されておらず、属性の正しい設定を特定するために試行錯誤が必要となります。

（注）RADIUS CoA を設定する前に、[サポートされているプロトコル（Supported Protocols）] セクションで [RADIUS] オプションが選択されていることを確認します。

URL リダイレクト

このセクションでは、デバイスの URL リダイレクト機能を定義します。URL リダイレクトは、ゲスト、BYOD、ポスチャなどの複雑なフローのために必要です。ISE ポータルに対してリダイレクトできる必要があります。つまり、*ローカル Web 認証*では不十分です。

デバイスで使用されている URL リダイレクトには、静的と動的という 2 つの一般的なタイプがあります。静的では、URL をデバイスに設定する必要があります（手動）。RADIUS 属性を通じて動的にリダイレクト先を指定することはサポートされていません。通常は、デバイスの設定に ISE ポータルの URL をコピー アンド ペーストします。

もう一方のタイプは動的 URL です。このタイプでは、ISE は RADIUS 属性を使用してデバイスに動的にリダイレクト先を指定することができます。手動でデバイスを設定する必要はありません。デバイスが動的 URL をサポートしている場合は、設定を容易にするために動的 URL の使用を推奨します。

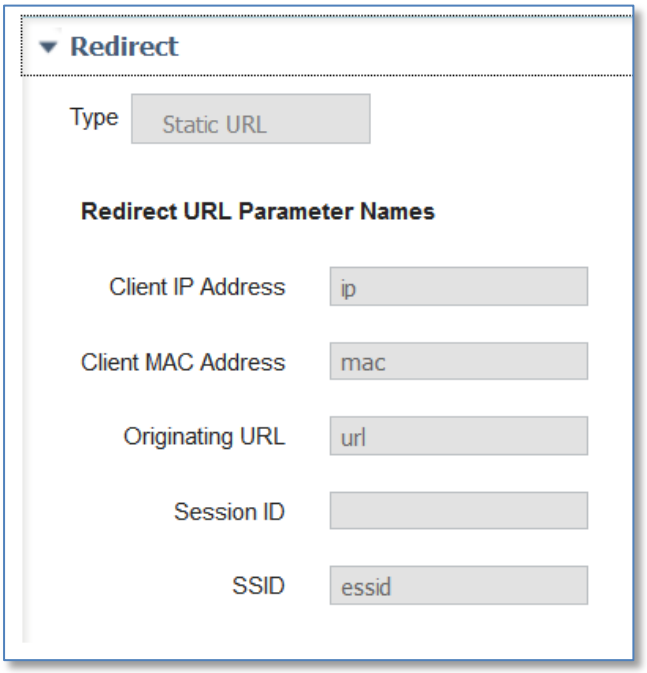

図 10. URL リダイレクト

パラメータ名とは、リダイレクト URL でデバイスによって渡される引数です。ISE にはこれらのパラメータの名前を指定して、URL からパラメータを正しく抽出できるようにする必要があります。ISE はこれらを使用してクライアントとセッション、およびクライアントが取得を試みた元の URL を特定し、リダイレクトできるようにします。

（注）管理者ガイドには通常、これらのパラメータ名は公開されていません。公開されているものもありますが、大半はされていません。いくつかは実際にプログラム可能です。重要なのは、URL パラメータ名がデバイスが送信したものと一致する必要があるということです（パラメータ名が公開されていない場合は、特定するためにブラウザを使用する必要がある場合があります）。

（注）有線デバイスは通常、URL リダイレクトを使用できません。

ポリシー要素の作成

通常、組み込みの認証および認可（*有線/ワイヤレス MAB* や *有線/ワイヤレス 802.1X* など）を追加で作成したり、変更する必要はありません。これらは実行時に適切な NAD プロファイルを自動的に使用するためです。同様に、組み込みの *許可されているプロトコル* は既存の NAD プロファイルから適切な属性を使用して MAB を検出します。

ただし、カスタムの条件、プロトコル、またはプロファイルを作成する必要がある場合には、[ポリシー要素の作成（Policy Element Generation）] ウィザードを利用することができます。このウィザードでは、NAD プロファイルに基づいてさまざまな編集可能要素を作成できます。この要素はさらにカスタマイズすることや、ポリシーで使用することができます。

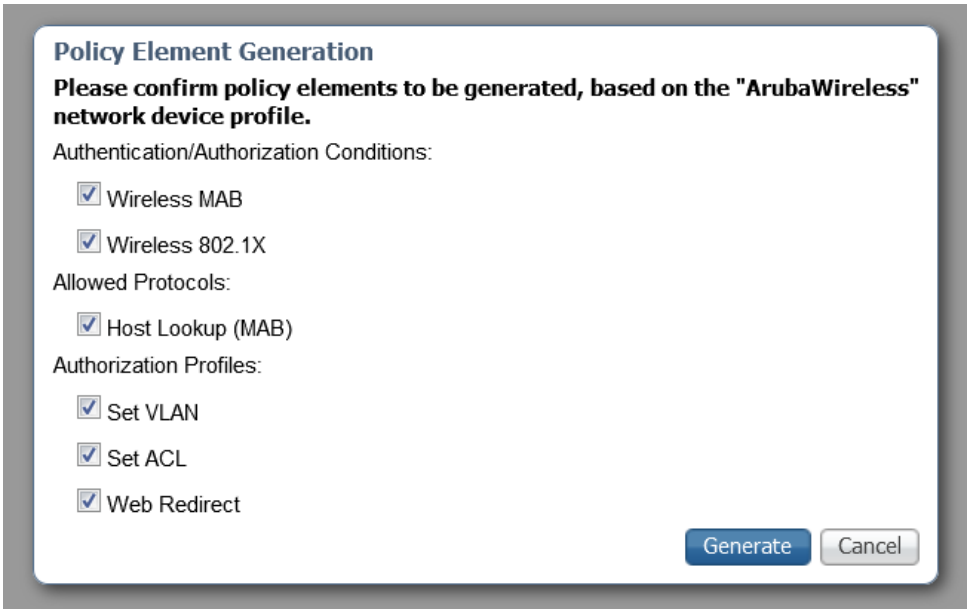

図 11. ポリシー要素の作成

サマリー

[サマリー（Summary）] セクションには、NAD プロファイル設定により有効にされるフローとサービスが表示されます。

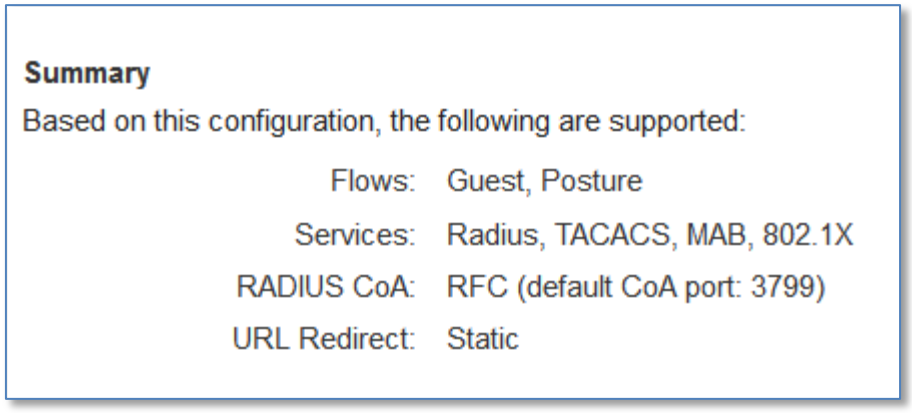

図 12. NAD プロファイルの概要

第 5 章 ネットワーク デバイス プロファイルの使用

NAD プロファイルの割り当て

NAD プロファイルを作成したら、[ネットワーク デバイス（Network Devices）] でデバイスに割り当てます。

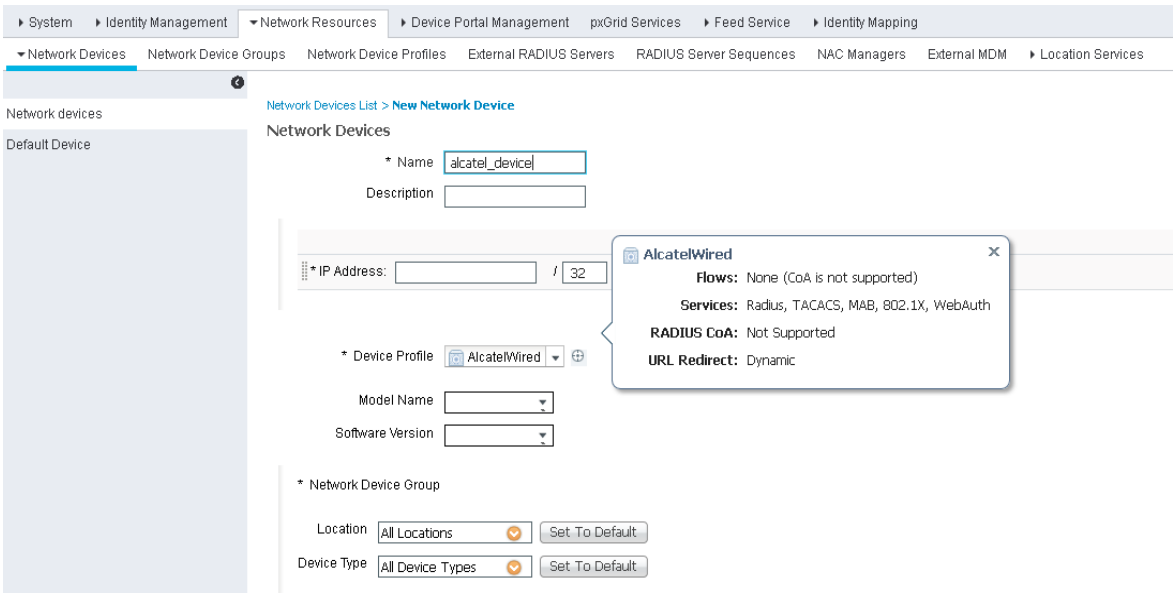

図 13. NAD プロファイルの割り当て

認証/認可の条件

ISE には、評価対象とする適切な基礎条件をスマートに選択する、組み込みの認証および認可の条件（有線/ワイヤレス MAB、802.1x）が多数あります。これは、実行時に NAD に割り当てられた NAD プロファイルを特定し、その NAD プロファイル内の情報を参照することで行われます。これにより、認証/許可条件を大幅に減らすことができます。新しい NAD プロファイルを定義できるときに、組み込みのスマートな条件をカスタマイズする必要がないこともよくあります。

いずれかの既存の条件を調べると、どの NAD プロファイルが考慮され、どの NAD プロファイルが考慮されないかがわかります。

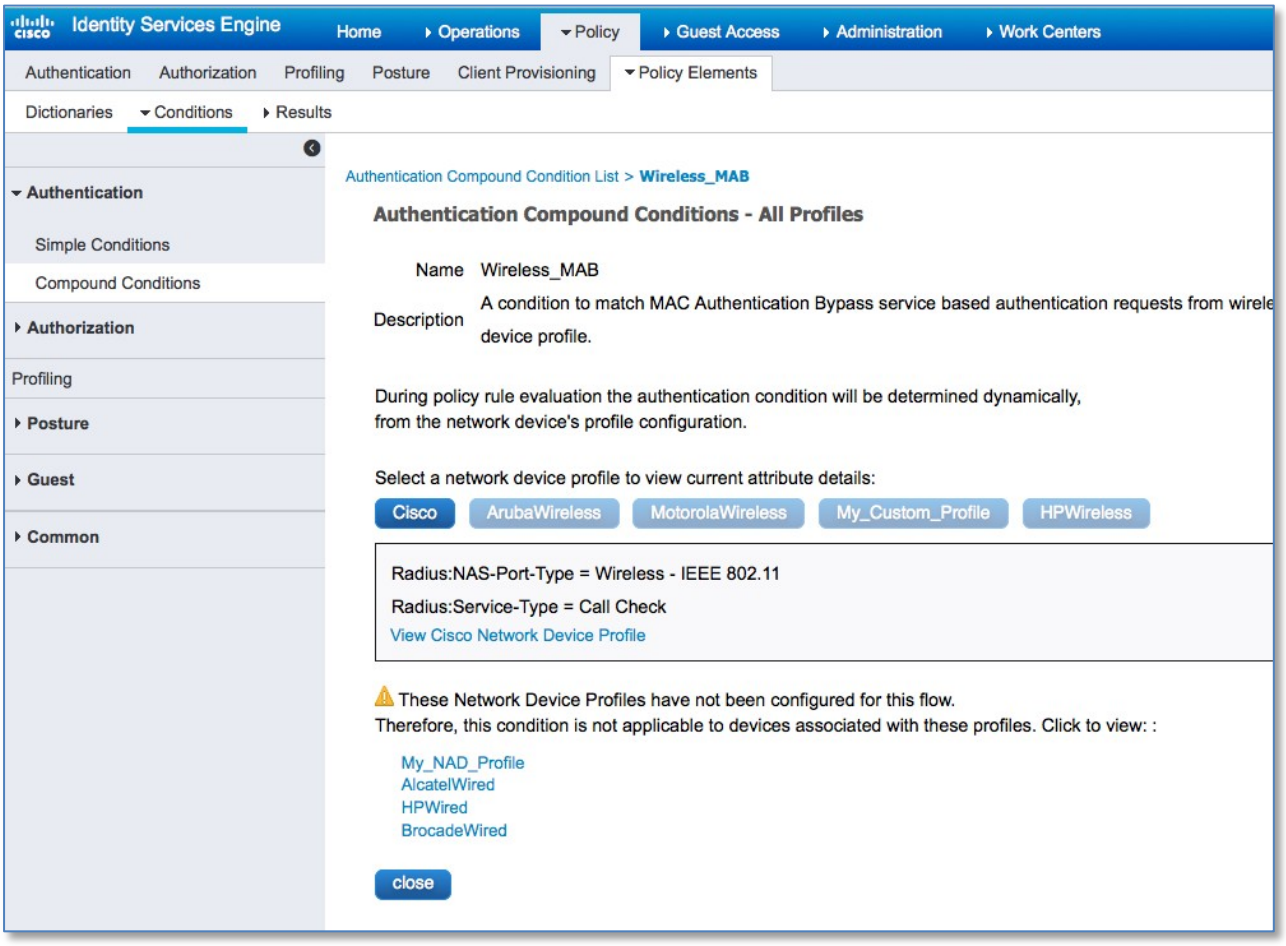

図 14. スマートな認証条件

ときには、新しいデバイス用のカスタム条件を定義する場合もあります。NAD プロファイルから [ポリシー要素の作成（Generate Policy Elements）] 機能を使用して、条件で適切な属性/値を使用してカスタム条件を作成するために役立てることができます。

認証プロファイル

通常、新しいデバイス用に 1 つ以上の認証プロファイルを作成する必要があります。プロファイルを作成するときは、[ネットワーク デバイス プロファイル（Network Device Profile）] ボックスを新しい NAD プロファイルの名前に設定します。これにより「スマート」認証が可能になり、デバイスに割り当てられた NAD プロファイルに基づいて適切なプロファイルが自動的に選択されます。

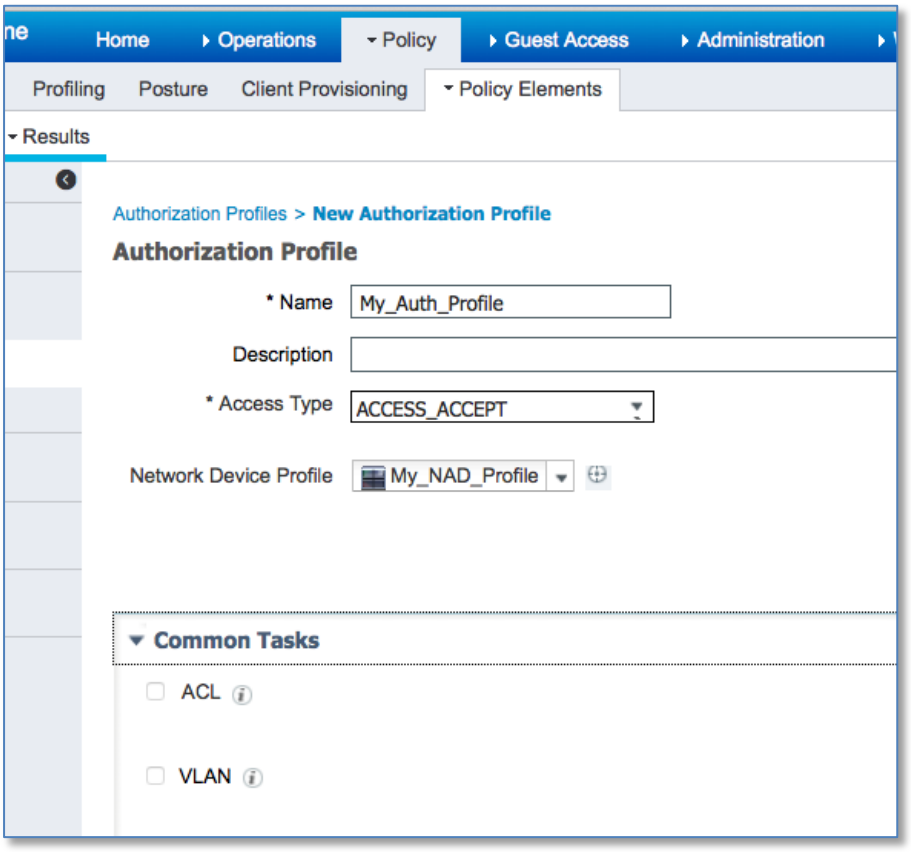

図 15. 新規の認証プロファイル

ポリシー ルールを設定するときは、認証プロファイルをそのデバイスに割り当てた NAD プロファイルに明示的に設定するか、単に VLAN または ACL を使用する場合は [任意（Any）] に設定します。

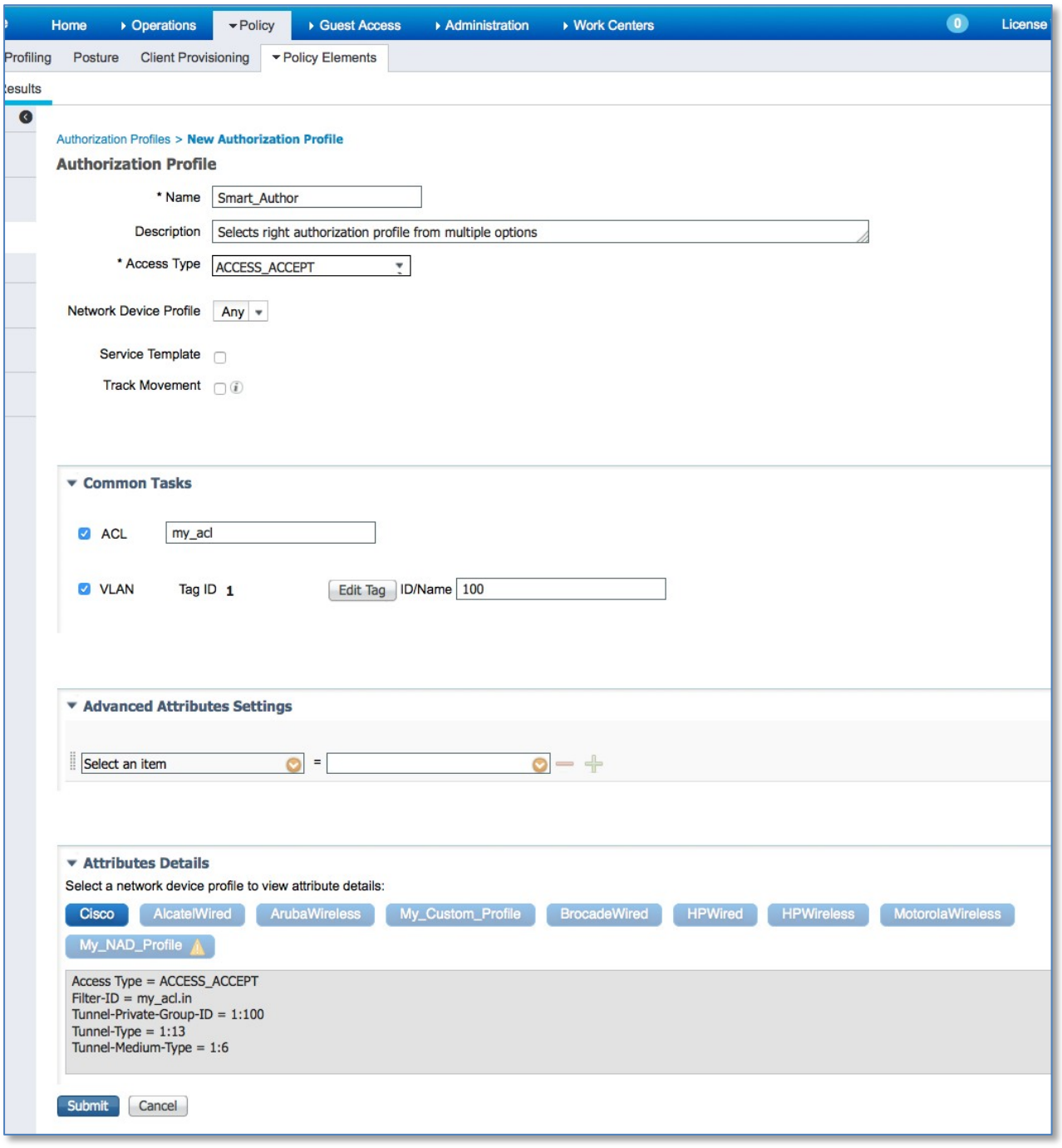

図 16. スマート認証プロファイル

動作の確認

新しい NAD プロファイルを作成して、それを使用するために ISE のポリシーを設定したら、関連するフローが予期したとおりに機能するかどうかを確認する必要があります。他の NAD プロファイルを使用しているデバイスが、引き続き予期したとおりに機能することを確認することも推奨します。ISE のモニタリング/レポートの [ステップ（STEPS）] の詳細には、どの NAD プロファイルが使用されていて、どのフロー タイプが検出されているかを把握できるように ISE 2.0 の追加情報が表示され、トラブルシューティングに役立ちます。