Cisco Identity Services Engine を使用したオンボーディングとプロビジョニング

セキュア アクセスを実現するハウツー ガイド シリーズ

日付:2012 年 4 月

作成者:Imran Bashir

目次

概要

モバイル デバイスが急増し、個人所有デバイス持ち込み（BYOD）のサポートが企業に期待されている状況により、新しいセキュリティ要件が生じています。このような要件では、ネットワーク サービスを保護する、データを保護する、エンタープライズのニーズとユーザの需要とのバランスをとる、といった条件を満たす必要があります。このアプリケーション ノートは、Identity Services Engine に組み込まれているいくつかのセキュリティ機能（デバイス登録やネイティブ サプリカントのプロビジョニングなど）について取り上げます。お客様はこれらの機能を使用して、BYOD に関する要件に対処することができます。

このハウツー ガイドでは、オンボーディング用にシステムを設定する方法について説明します。具体的には、ネイティブ サプリカントのプロビジョニング、プッシュされるサプリカント プロファイルのタイプ、およびアクセスを区別するポリシーを記述する方法が含まれています。

表 1 に、サポートされているプラットフォーム、ダウンロードの後のサプリカント プロファイルの場所、およびプロファイルを参照または消去するための該当する場所を示します。

表 1. 対応プラットフォーム

Device	証明書のストア	証明書情報	Version
iPhone/iPad/iPod	デバイス証明書ストア（設定プロファイル）	[設定（Settings）] → [全般（General）] → [プロファイル（Profile）] を選択して参照できます。	5.0 以上
Android	デバイスの暗号化された証明書ストア	参照できません。ただし、[設定（Settings）] → [ロケーションとセキュリティ（Location & Security）] → [ストレージのクリア（Clear Storage）]（すべてのデバイス証明書とパスワードを消去する）を選択して、消去することができます。	3.2 以上
[Windows]	ユーザの証明書ストア	MMC 用証明書スナップインを起動して参照できます。	WindowsXP - SP3 Windows Vista - SP? Windows7 - すべてのバージョン
MacOS-X	キーチェーン	アプリケーションを起動 → [ユーティリティ（Utilities）] → [キーチェーンアクセス（Keychain Access）] を選択して参照できます。	MacOS-X 10.6 および 10.7

注: MACOS-X 10.8 には次の注意点があります。
[セキュリティとプライバシー環境設定(security & Privacy Preference)] ペインの [MAC App Storeと確認済みの開発者(MAC App Store and identified developers)] オプションを選択した時点では、SPW(Supplicant MAC and)はインストールされていません。
SPW プロファイル/証明書をインストールするときに、ポップアップが複数回表示されます。

注: このマニュアルでは、推奨される導入方法と、お客様の環境で必要とされるセキュリティのレベルに応じたいくつかの異なるオプションについて説明します。これらの方法は、正常なプロジェクトの展開を保証するベスト プラクティスによって規定された Cisco TrustSec の展開に関する例であり、段階的な手順を示しています。
証明書およびサプリカント プロファイルのプロビジョニングについて関心がある場合は、『BYOD-Using_Certificates_for_Differentiated_Access』のハウツー ガイドを参照してください。

警告: このドキュメントは、ユーザが最初から最後まで手順をたどるように作成されています。セクションをとばすと、予期しない結果が生じることがあります。

シナリオの概要

このドキュメントでは、個人用デバイスのセルフサービス オンボーディングについて説明します。ここでは、従業員が新しいデバイスを登録し、そのユーザとデバイスに対してネイティブ サプリカントが自動的にプロビジョニングされ、デバイスを企業ネットワークへ接続するために事前に設定されているサプリカント プロファイルを使用してインストールされます。また、ユーザ、デバイス タイプ、場所、および時間に基づいてユーザ/デバイスへのアクセスを区別するよう、Cisco ISE ポリシーを設定することができます。

シングル SSID またはデュアル SSID を使用するよう、ワイヤレス用のデバイス オンボーディングを設定することができます。それぞれの場合の登録およびオンボーディングの流れは次のとおりです。

このドキュメントで使用しているシナリオを説明するために、iPad でのネイティブ サプリカントのプロビジョニングおよび認証の例を見てみましょう。

デュアル SSID のワイヤレス BYOD のセルフ登録

お客様のネットワークでは 2 つの SSID が設定されています。1 つは ゲスト/BYOD のための OPEN（BYOD-Open）で、もうひとつはセキュアな企業アクセス用（BYOD-Dot1x）です。

従業員はゲスト SSID（BYOD-Open）に関連付けられます。

ブラウザを開くと、Cisco ISE CWA（中央 Web 認証）のゲスト ポータルにリダイレクトされます。

従業員は、標準のゲスト ポータルに企業のユーザ名とパスワードを入力します。

Cisco ISE は企業の Active Directory または他の企業の ID ストアに対してユーザを認証し、Employee Device Registration Portal へリダイレクトすることについて承認する認可ポリシーを提供します。

Device Registration Portal ではデバイス ID に対応するデバイス MAC アドレスが事前に入力されており、従業員はオプションの説明を入力して、（必要な場合には）Acceptable User Policy を承認することができます。

従業員は承認を選択してダウンロードを開始し、サプリカント プロビジョニング ウィザードのインストールを開始します。

Cisco ISE Policy Services Node は OTA を使用し、新しいプロファイルを iPad へ送信します。この中には、iPad の MAC アドレスや従業員の AD ユーザ名が埋め込まれている（設定されている場合）発行された証明書や、Wi-Fi のサプリカント プロファイル（802.1X の認証に対して MSCHAPv2 または EAP-TLS の使用を強制します）が含まれています。

これで、認証用 MSCHAPv2 または EAP-TLS を使用して企業ワイヤレス ネットワークに関連付けるよう iPad が設定されました。Cisco ISE 認可ポリシーは証明書の属性を使用してネットワーク アクセスを強制実行します（たとえば、企業アセットではない場合は制限されたアクセスを提供する、など）。

Cisco ISE は認可変更（CoA）を開始し、（シングル SSID の iPad はEAP-TLS を使用して自動的に再接続しますが、デュアル SSID の Employee は企業の SSID に手動で接続しなければならない場合に）従業員を企業の SSID（BYOD-Dot1x）にもう一度関連付けして、MSCHAPv2 または EAP-TLS（サプリカントに設定されている認証メソッド）を介して認証します。

シングル SSID のワイヤレス BYOD のセルフ登録

1. お客様のネットワークは、PEAP および EAP-TLS（証明書を使用する場合）の両方をサポートできるようなセキュアな企業アクセス用に、シングル SSID（BYOD-Dot1x）で設定されています。
2. 従業員は企業 SSID（BYOD-Dot1x）に関連付けられます。
3. サプリカントに、REAP 認証用の EMPLOYEE のユーザ名およびパスワードを入力します。
4. Cisco ISE は企業の Active Directory または他の企業の ID ストアに対してユーザを認証し、Employee Device Registration Portal へリダイレクトすることについて承認する認可ポリシーを提供します。

5. 従業員はブラウザを開くと、Employee Device Registration Portal にリダイレクトされます。
6. Device Registration Portal ではデバイス ID に対応するデバイス MAC アドレスが事前に入力されており、従業員はオプションの説明を入力して、(必要な場合には) Acceptable User Policy を承認することができます。
7. 従業員は承認を選択してダウンロードを開始し、サプリカント プロビジョニング ウィザードのインストールを開始します。
8. Cisco ISE Policy Services Node は OTA を使用し、新しいプロファイルを iPad へ送信します。この中には、iPad の MAC アドレスや従業員の AD ユーザ名が埋め込まれている(設定されている場合)発行された証明書や、Wi-Fi のサプリカント プロファイル(802.1X の認証に対して MSCHAPv2 または EAP-TLS の使用を強制します)が含まれています。
9. これで、認証用に MSCHAPv2 または EAP-TLS を使用して企業ワイヤレス ネットワークに関連付けるよう iPad が設定されました(シングル SSID の iPad はEAP-TLS を使用して自動的に再接続しますが、デュアル SSID の従業員は企業の SSID に手動で接続する必要があります)。Cisco ISE 認可ポリシーは証明書の属性を使用してネットワーク アクセスを強制します(たとえば、企業アセットではない場合は制限されたアクセスを提供する、など)。
10. Cisco ISE は認可変更(CoA)を開始し、従業員を企業の SSID(BYOD-Dot1x)にもう一度関連付けして、MSCHAPv2 または EAP-TLS(サプリカントに設定されている認証メソッド)を介して認証します。

アーキテクチャ図

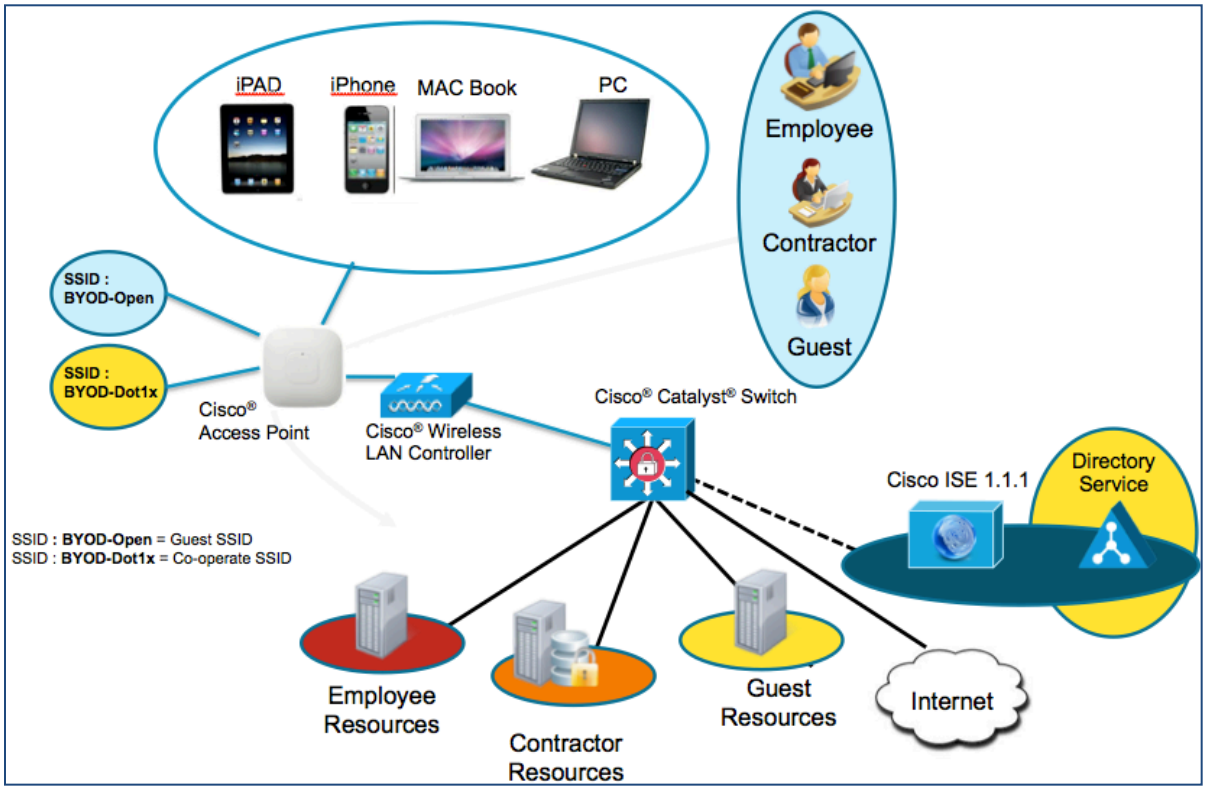


図 1. ネットワーク図

コンポーネント

表 2 このドキュメントで使用されるコンポーネント

コンポーネント	ハードウェア	テストの対象機能	Cisco IOS® ソフトウェア リリース
Cisco Identity Services Engine（ISE）	1121/3315、3355、3395、VMware のいずれか	統合 AAA、ポリシー サーバ、およびサービス（ゲスト、プロファイラ、ポスチャ）	ISE 1.1.1
ワイヤレス LAN コントローラ（WLC）	5500 シリーズ 2500 シリーズ WLSM-2	プロファイリングおよび認可変更（CoA）	ユニファイド ワイヤレス 7.2.???
Apple iOS および Google Android	Apple および Google	該当なし	Apple iOS 5.0 Google Android 2.3

注:ワイヤレスはセントラル スイッチング モードでのみテストされています。

Cisco ISE の設定

この項では、ハウツー ガイドに記載されている使用例を実装するのに必要なステップについて説明します。ここでは、ユーザ グループの作成などの基本的な設定から、PEAP-MSCHAPv2、認証、および認可ポリシーに応じたサプリカント プロファイルの作成などの高度な設定までを対象とします。

BYOD のユーザ認識フロー

ユーザのオンボーディング（「オンボーディング」とはアセットを登録し、企業ネットワークへアクセスできるようにするためにアセットサプリカントをプロビジョニングするためのプロセスを表す用語）の一環として、ID ストアを選択し、オンボーディング（BYOD）フローへ転送されるリソースを定義することができます。次の例は、ID ソース順序の一部として、Active Directory の他に Cisco Identity Services Engine のローカル ストアで定義されているユーザについて示しています。

ここでは、ベスト プラクティスのオンボーディングの一環として、Active Directory を ID ソースとして使用し、どのユーザ グループが自身のデバイスをオンボーディングできるかを定義します。次の手順では、ID ソース順序の一部として、Active Directory、および Cisco ISE のローカル ユーザ データベースで定義されているユーザを示します。

ユーザ グループは、特定の Cisco ISE サービスおよび機能へのアクセスを許可する共通の権限セットを共有する個々のユーザまたはエンドポイントの集合です。たとえば、ユーザ パスワードの変更管理者グループに属している場合は、他のユーザの管理パスワードを変更できます。

ユーザ グループの設定

ステップ 1 [管理（Administration）] → [ID の管理（Identity Management）] → [グループ（Groups）] の順に移動します。

ステップ 2 [追加（Add）] をクリックします。

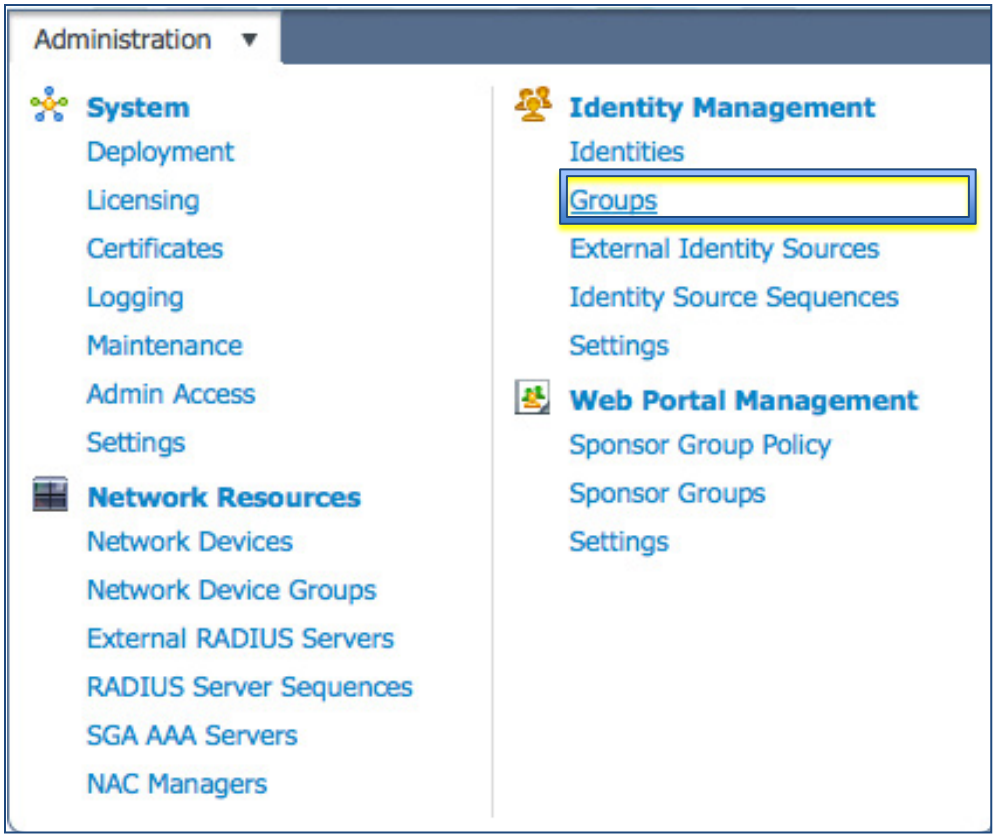


図 2. ID グループのナビゲーション

ステップ 3 ID グループを作成します。

この例では、ID グループを「**Employee**」という名前にします。

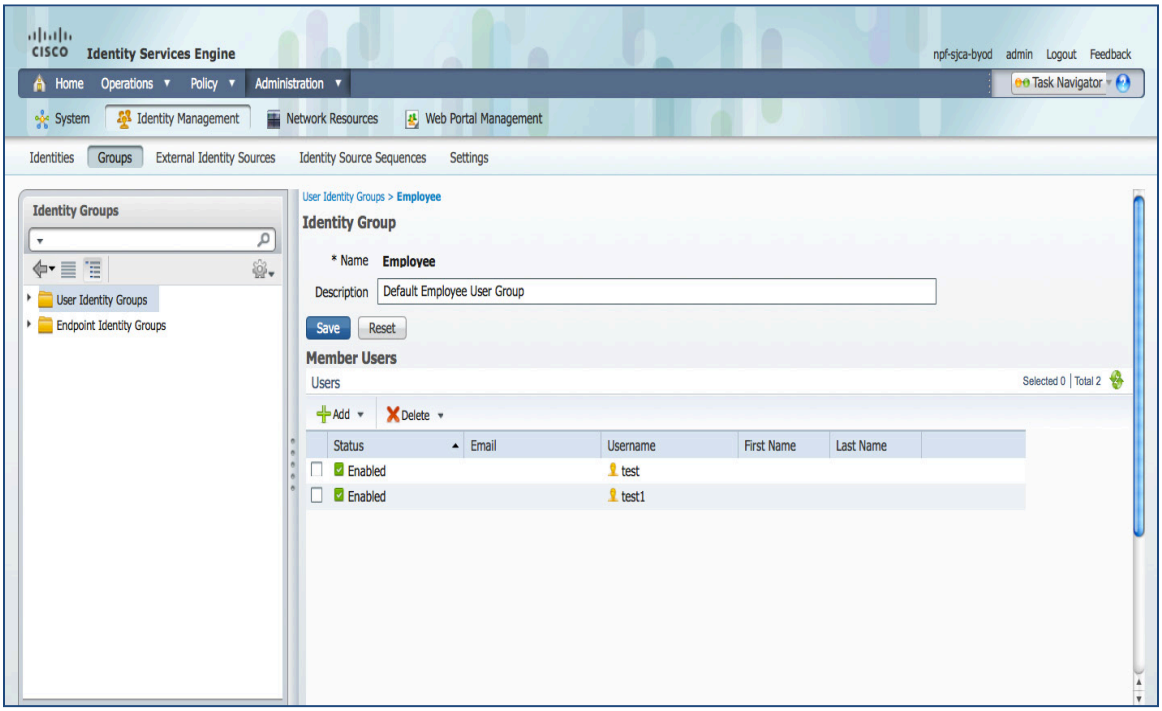


図 3. ユーザ ID グループ

Employee グループのユーザの作成

ステップ 1 [管理（Administration）] → [IDの管理（Identity Management）] → [ID（Identities）] → [ユーザ（Users）] の順に移動します。

ステップ 2 [追加（Add）] をクリックします。

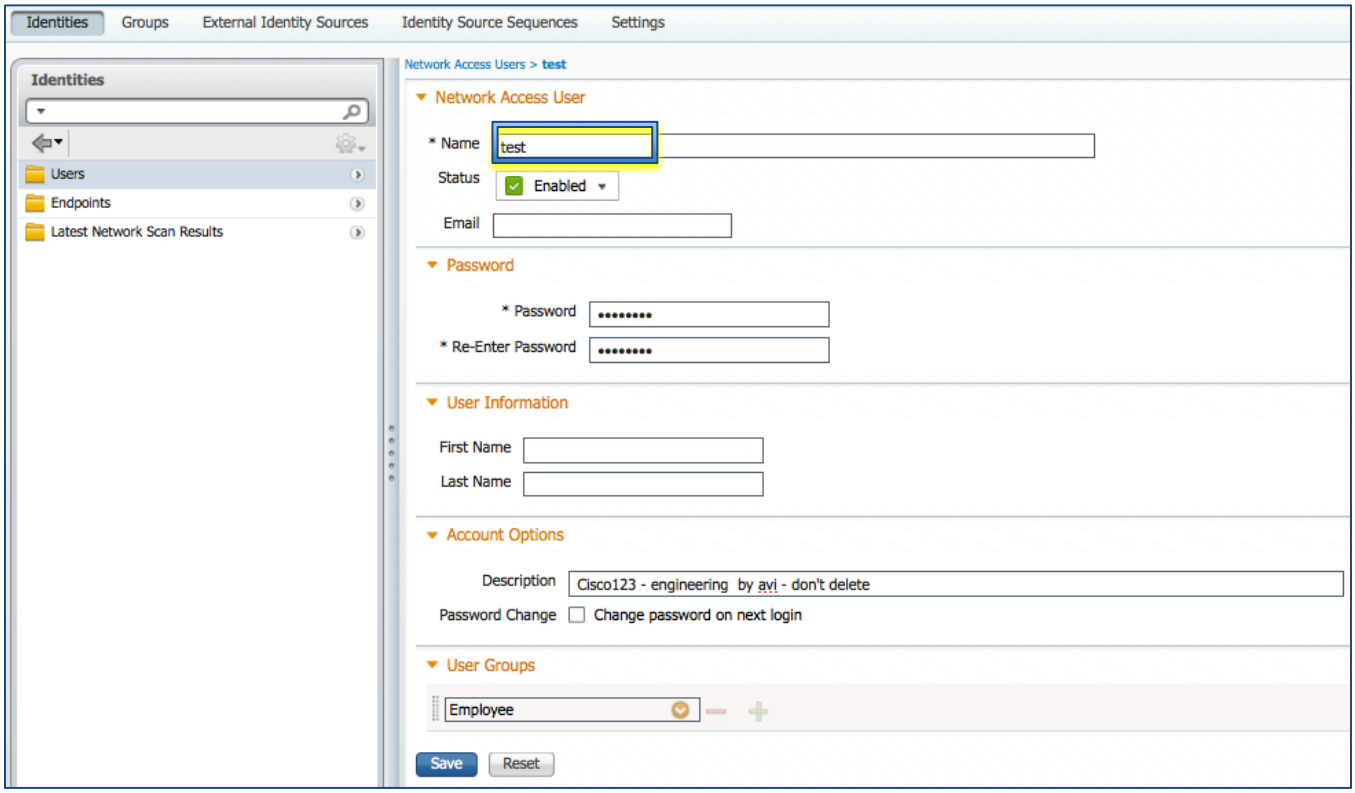


図 4.　ユーザ アカウント

ID ソース順序の作成

ID ソース順序は、Cisco ISE がそれぞれ異なるデータベース内でユーザ クレデンシャルを検索する順序を定義します。Cisco ISE は、内部ユーザ、内部エンドポイント、Active Directory、LDAP、RSA、RADIUS トークン サーバ、および証明書認証プロファイルの各データベースをサポートしています。

組織で、複数の ID ストアにクレデンシャルを保存している場合は、ID ソース順序を定義することができます。これは、Cisco ISE がデータベースの中でユーザ情報を検索する順序を表します。一致が見つかると、Cisco ISE はそれ以上の検索を行いませんが、クレデンシャルを評価し、認可結果をネットワーク アクセス デバイスへ返します。このポリシーは最初の一致ポリシーです。

ID ソース順序を作成します。

ステップ 1　[管理（Administration）] → [IDソース順序（Identity Source Sequence）] を選択します。
ステップ 2　[追加（Add）] をクリックします。

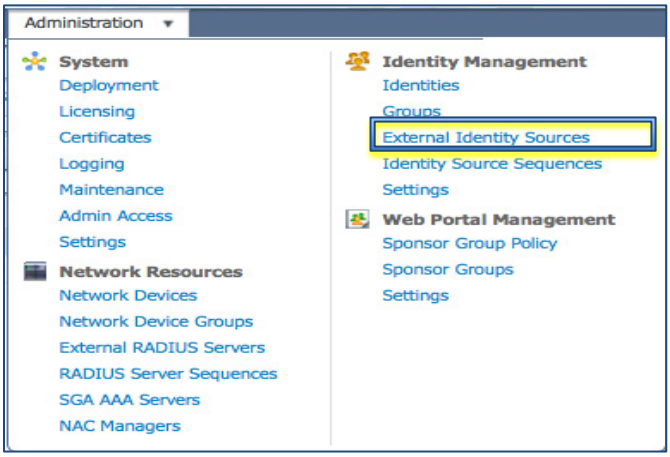


図 5. ID ソース順序のナビゲーション

ステップ 3 順序に名前を付けます。この例では、順序に「**Dot1x**」という名前を指定します。

ステップ 4 Active Directory Server（AD1）を選択し、[認証の検索リスト（Authentication Search List）] で [内部エンドポイント（Internal Endpoints）] と [内部ユーザ（Internal Users）] を選択します。

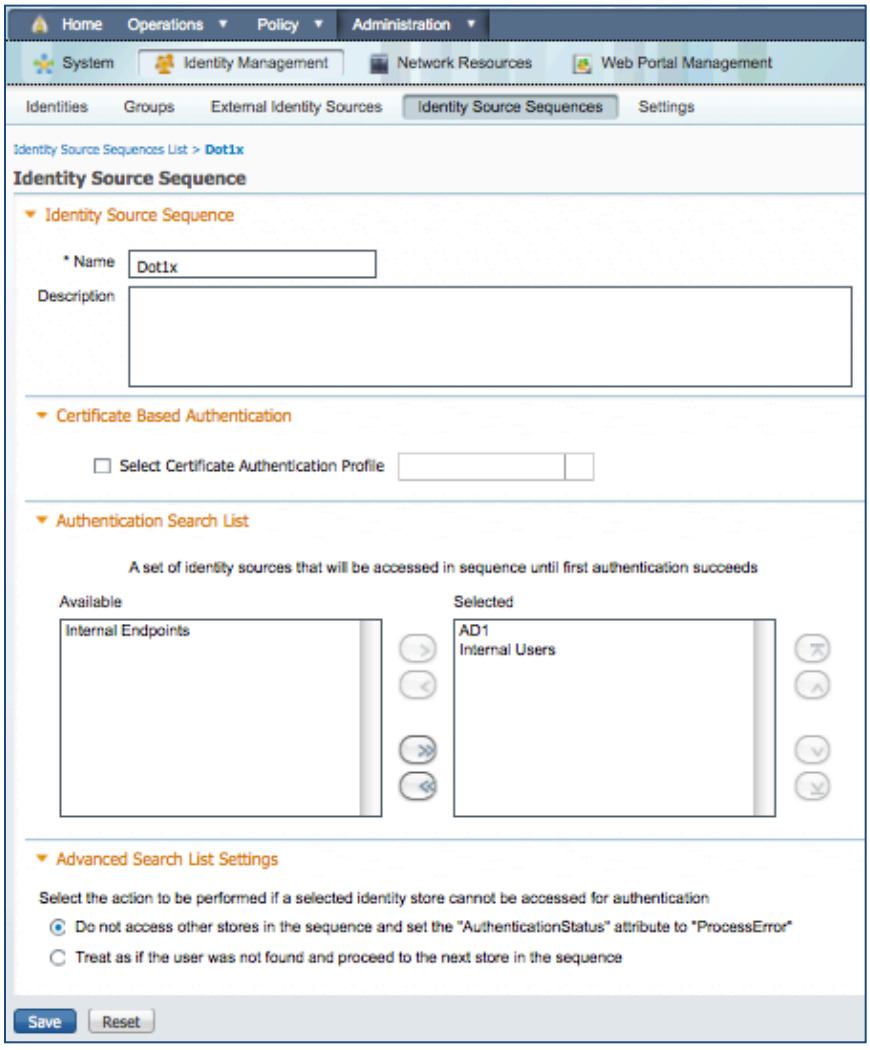


図 6. ID ソース順序（Identity Source Sequence）

デバイス ポータルの設定

デバイス ポータルの主な目的は、エンドユーザがネットワークにデバイスを自分で持ち込めるようにすることです。このポータルを使用して任意のデバイスを ISE エンドポイント データベースに入力して、ネットワーク上で許可することができますが、このポータルは、ユーザやブラウザを持っていないためにセルフプロビジョニング フローを実現できないデバイスを対象としています。このようなデバイスには、輸液ポンプ、プリンタ、ゲーム コンソールなどがあります。

デバイス ポータルの設定

ステップ 1 デバイス ポータルを有効にするには、[管理（Administration）] → [Webポータル管理（Web Portal Management）] → [設定（Settings）] → [自分のデバイス（My Devices）] → [ポータルの設定（Portal Configuration）] を選択します。

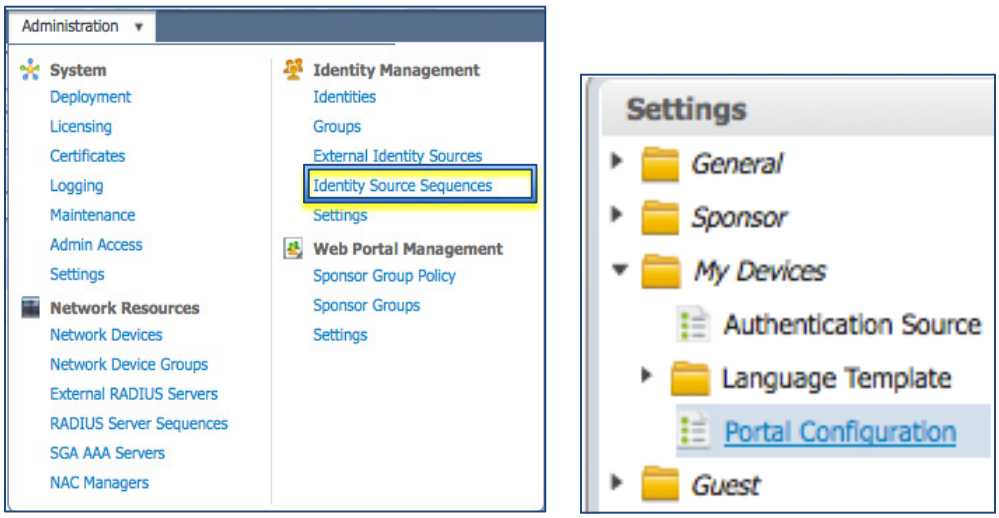


図 7. デバイス ポータルのナビゲーション

ステップ 2 デバイス ポータルはデフォルトで有効になっていますが、[自分のデバイス] のポータル管理ページへナビゲートして、有効になっていることを確認してください。

ステップ 3 [追加（ADD）] をクリックします。

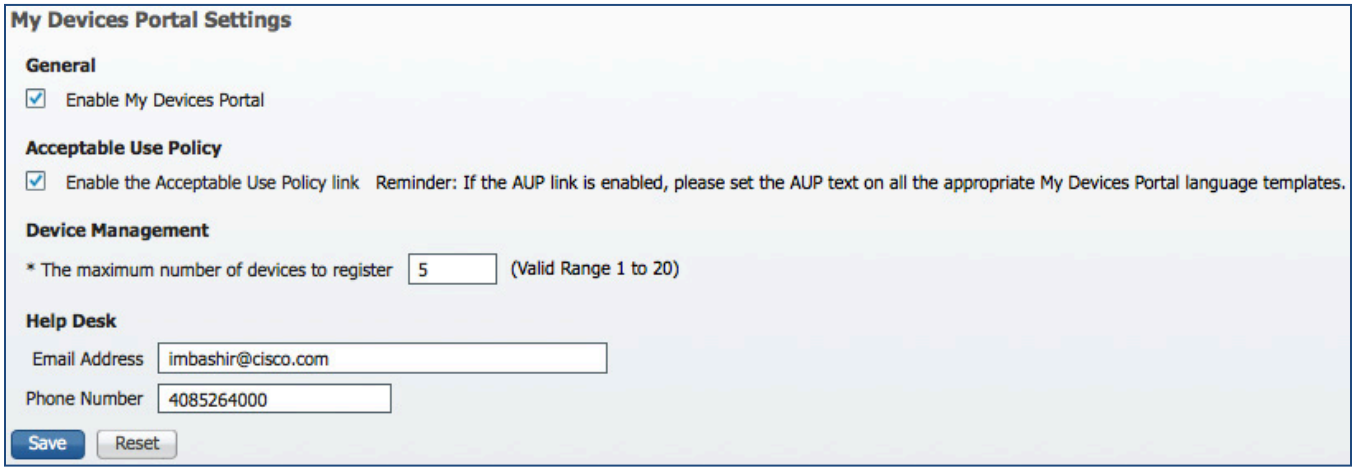


図 8. デバイス ポータルの設定

デバイス ポータルの ID ソース順序の作成

ID ソース順序を設定します。これは、デバイス ポータルへログインするための認証の順序を定義するものです。

ステップ 1 [管理（Administration）] → [ID管理（Identity Management）] → [IDソース順序（Identity Source Sequence）] を選択します。

ステップ 2 [追加（Add）] をクリックします。

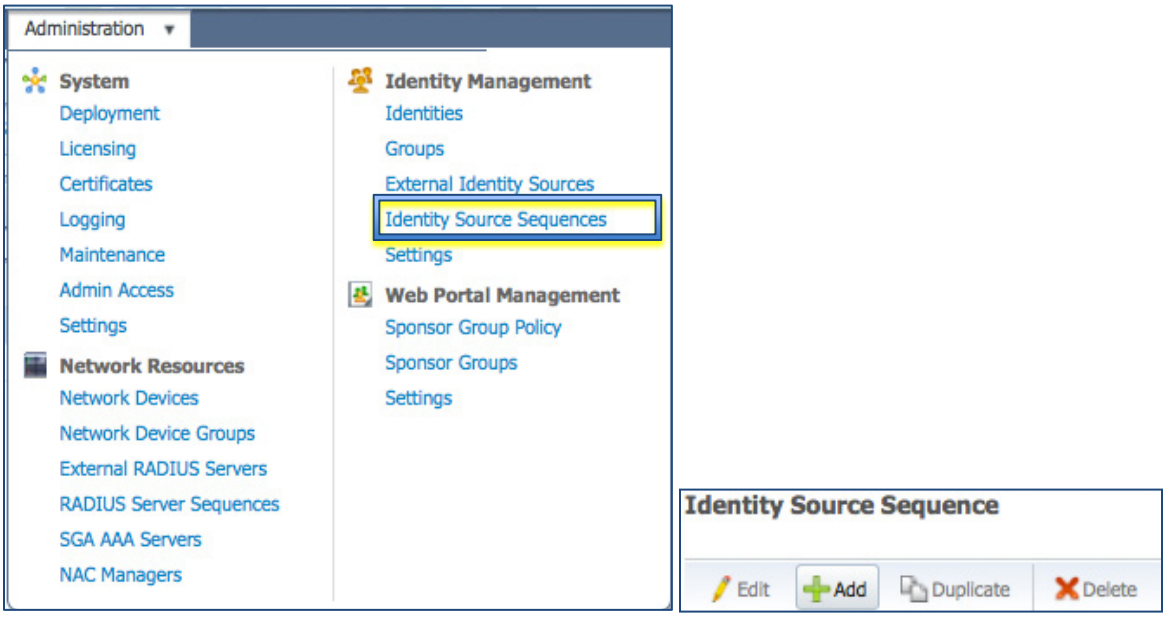


図 9. ID ソース順序のナビゲーション

ステップ 3 デバイス ポータルの ID ソース順序を設定します。

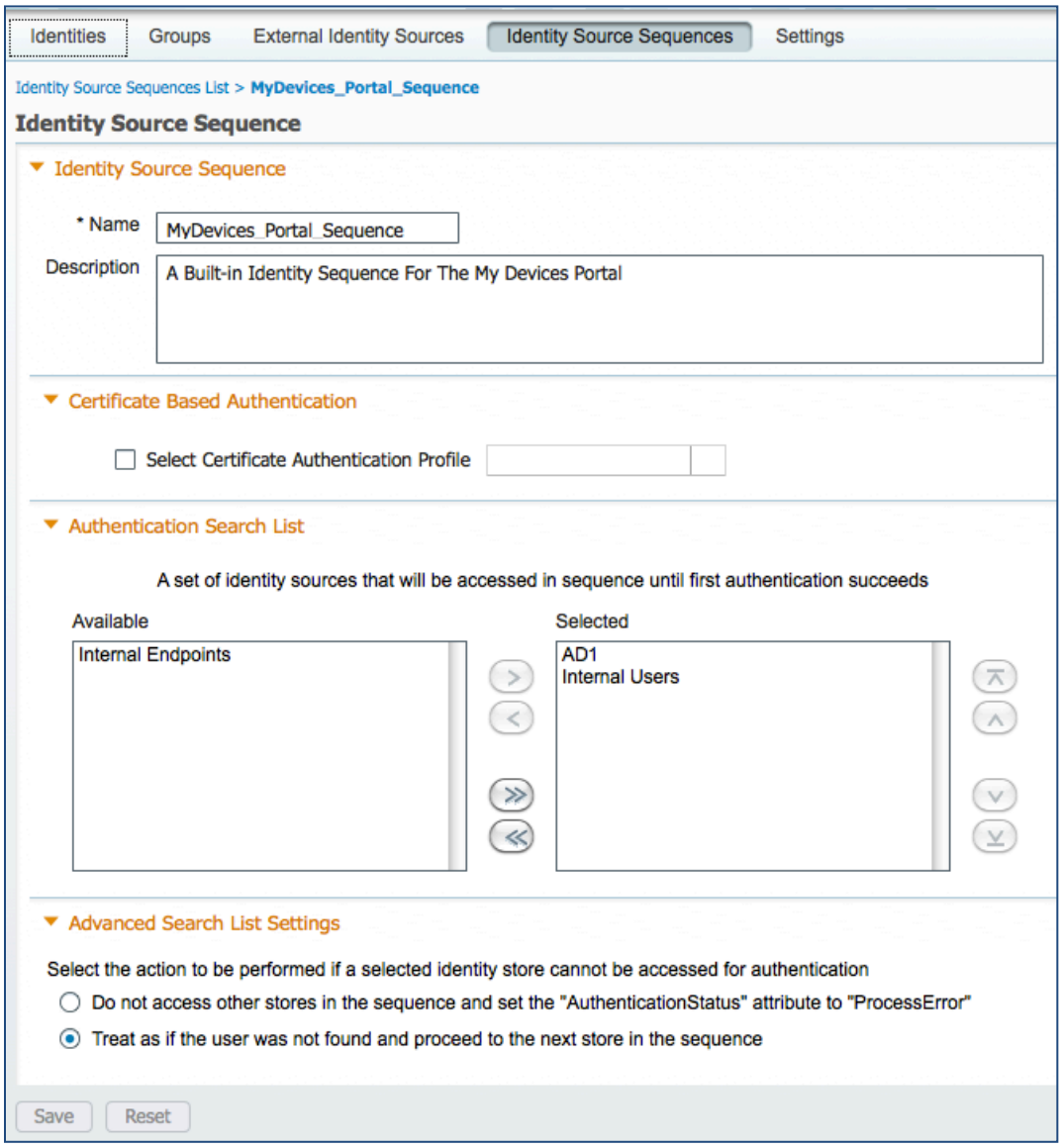


図 10. ID ソース順序の設定

ゲスト ポータル順序の設定

ゲスト ポータルは企業ユーザの認証にも使用するので、デフォルトのゲスト ポータル順序に Active Directory を追加することが重要です。

ゲスト ポータル順序の設定

ステップ 1 [管理（Administration）] → [ID管理（Identity Management）] → [IDソース順序（Identity Source Sequence）] を選択します。

ステップ 2 [**Guest_Portal_Sequence**] を編集します。

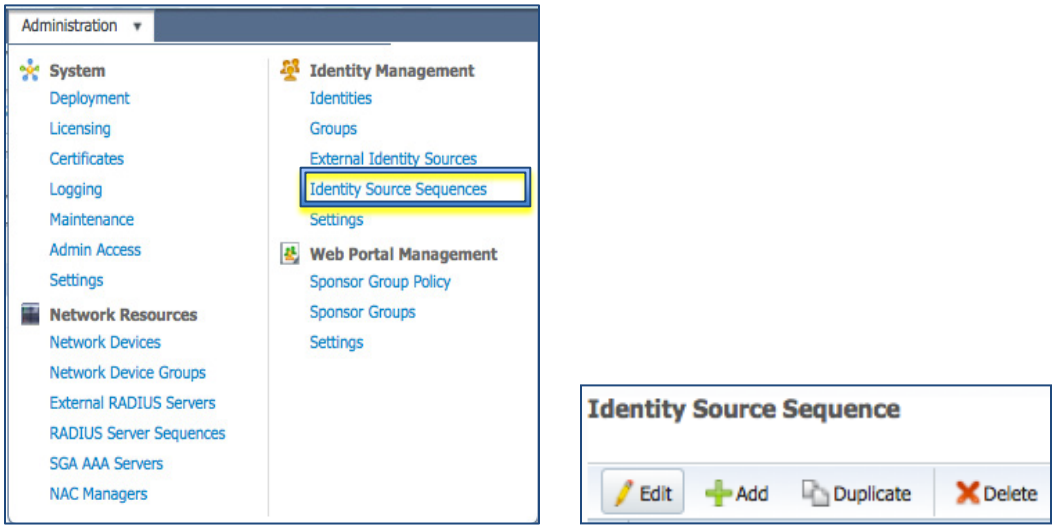


図 11. ID ソース順序のナビゲーション

ステップ 3 [**Guest_Portal_Sequence**] に Active Directory を追加します。

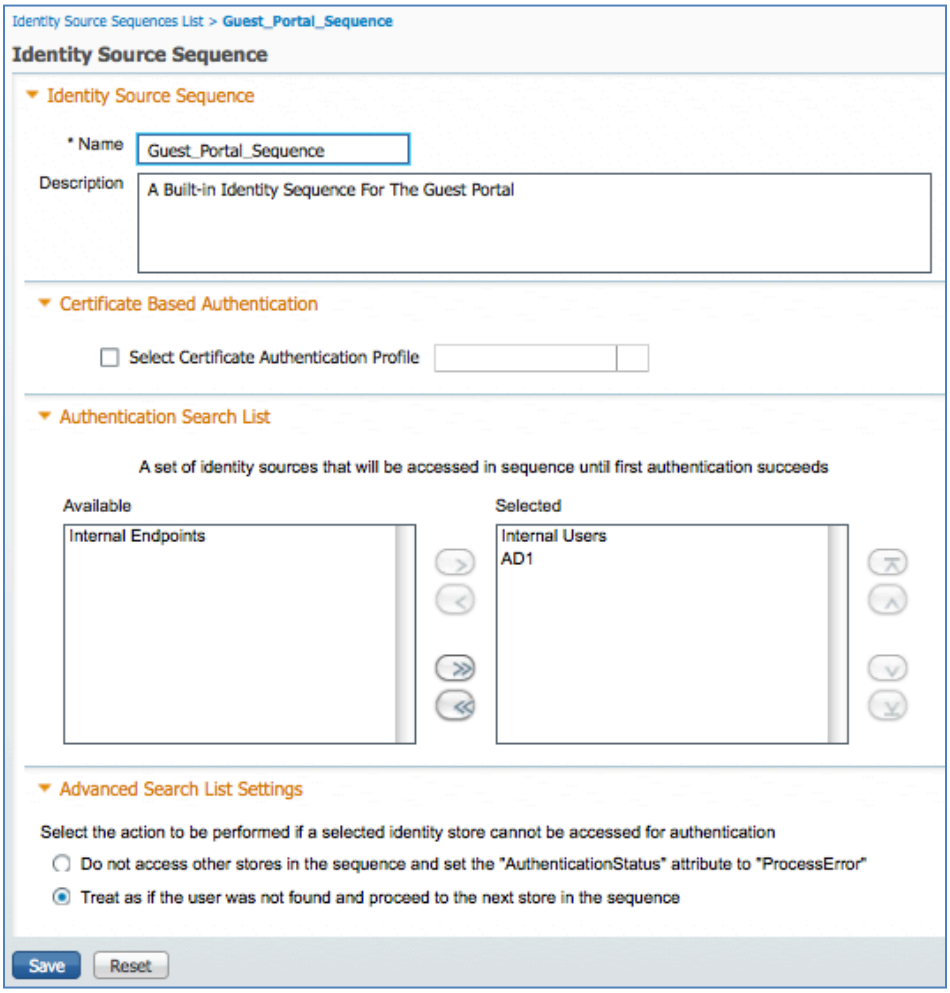


図 12. ID ソース順序の設定 - ゲスト ポータル

クライアント プロビジョニング ポリシーの作成

Cisco Identity Services Engine では、内部ネットワークにユーザがアクセスするときに使用するログイン セッションのタイプを分類する場合に、さまざまな要素を調べます。ここでクライアント プロビジョニング ポリシーを使用してサプリカント プロファイルを作成し、エンド ポイント（iPhones、iPad、Windows、MAC OS X など）を設定します。

Cisco ISE はネイティブ サプリカント プロビジョニング（NSP）を使用して、オペレーティング システムごとのプロビジョニング ポリシーを区別します。各ポリシーには「ネイティブ サプリカント プロファイル」が含まれており、接続で PEAP、EAP-TLS、またはどのワイヤレス SSID を使用するかを定義します。また、クライアント プロビジョニング ポリシーは、使用するプロビジョニング ウィザードを参照します。もともと、iPad 用にプロビジョニングされるサプリカントは、Android デバイス用にプロビジョニングされるものとは異なります。エンドポイントに対してプロビジョニングするパッケージを決定するために、ここでは Cisco ISE でクライアント プロビジョニング ポリシーを使用して、オペレーティング システムごとにサプリカント プロファイルをプロビジョニング ウィザードへバインドします。

クライアント プロビジョニング ポリシーの作成

ステップ 1 ネイティブ サプリカント プロファイルを作成します。[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] に移動します。

ステップ 2 [クライアントプロビジョニング（Client Provisioning）] → [リソース（Resources）] をクリックします。

ステップ 3 [追加（ADD）] をクリックします。

図 13. クライアント プロビジョニン リソースのナビゲーション

ネイティブ サプリカント プロファイルの名前指定

ステップ 1 オペレーティング システムを選択します。

注: すべてのオペレーティング システムに対して 1 つのサプリカント プロファイルを設定できます。ただし、このドキュメントで後述しますが、オペレーティング システムごとに異なるプロビジョニング方法を指定することもできます。

ステップ 2 [接続タイプ（Connection Type）] として [有線（Wired）] または [ワイヤレス（Wireless）] を選択します。

ステップ 3 ワイヤレス LAN コントローラの設定に従って、企業のワイヤレス SSID を入力します。

ステップ 4 [許可されているプロトコル（Allowed Protocols）] に、ここでは「**PEAP**」を選択します。

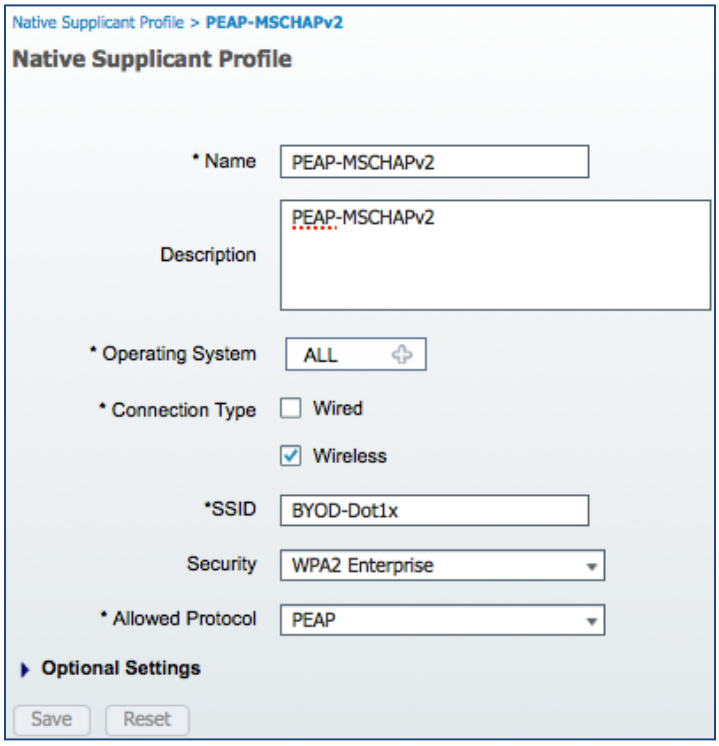


図 14. クライアント プロビジョニン リソースのナビゲーション

クライアント プロビジョニング ポリシー（CPP）の作成

この手順では、iOS および Android デバイス用のネイティブ サプリカントを設定するためのクライアント プロビジョニング ポリシーを作成します。さらに、Windows および Mac OS X のサプリカントに対する CPP を作成することもできます。

ステップ 1 Windows および MAC OS X 用のサプリカント ウィザードをダウンロードします。

ステップ 2 [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] → [クライアントプロビジョニング（Client Provisioning）] → [リソース（Resources）] を選択します。

ステップ 3 右側の [追加（ADD）] をクリックします。

ステップ 4 [Ciscoサイトのエージェントリソース（Agent resources from Cisco site）] を選択します。

この例では、WinSPWizard 1.0.0.15 および MacOsXSPWizard 1.0.0.999 を選択しました。

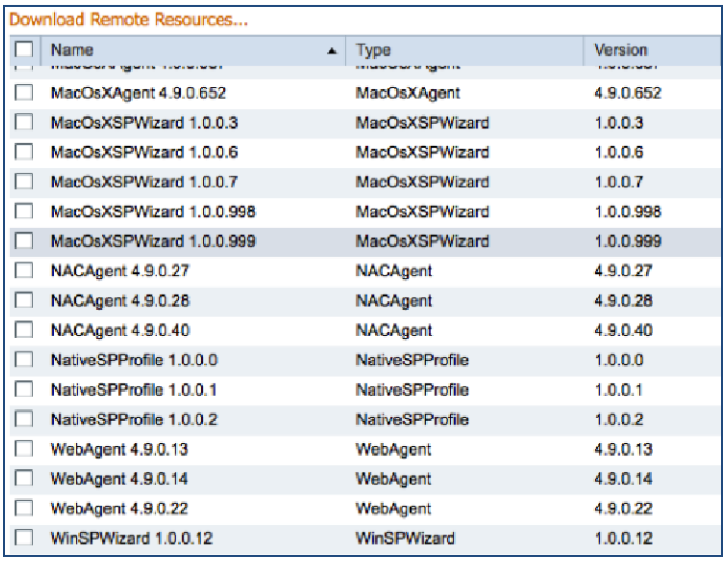


図 15. ネイティブ サプリカント ウィザード A

ステップ 5 最新のサプリカント ウィザードを選択します。

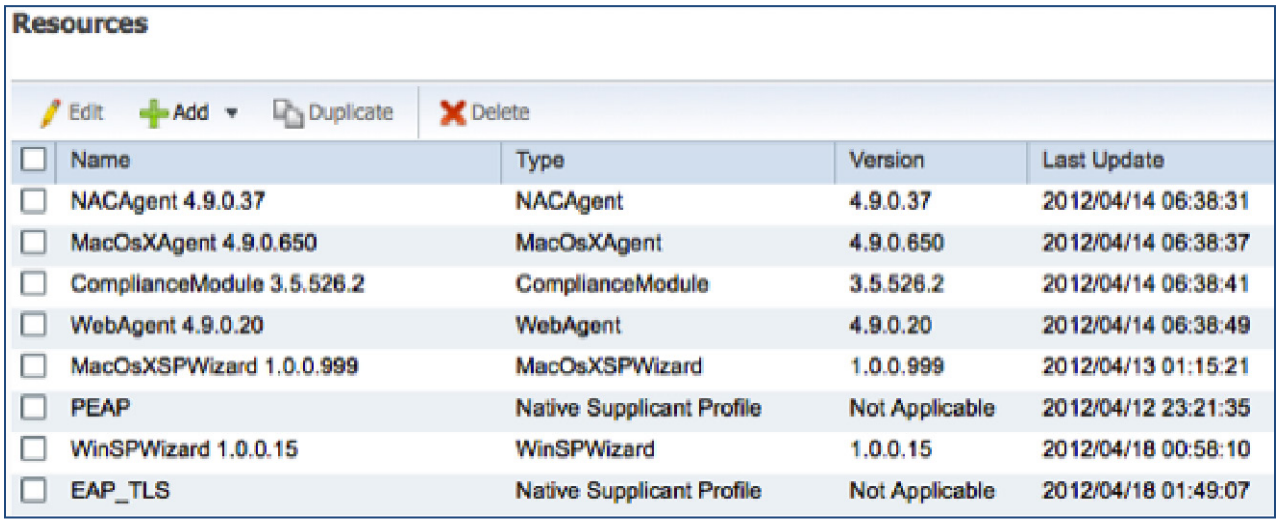


図 16. ネイティブ サプリカント ウィザード B

Apple iOS 用のクライアント プロビジョニング ポリシーの作成

ステップ 1 [ポリシー(Policy)] → [クライアント プロビジョニング(Client Provisioning)] を選択します。
ステップ 2 右側の [アクション(Actions)] → [新規ポリシーを上に挿入(Insert new Policy above)] をクリックします。
ステップ 3 Apple iOS CPP ポリシーを作成します。

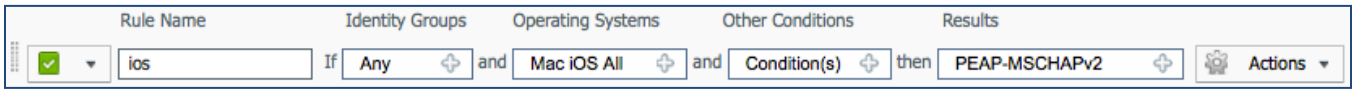


図 17. Apple iOS のクライアント プロビジョニング ポリシー

ステップ 4　Android CPP ポリシーを作成します。

図 18.　Android のクライアント プロビジョニング ポリシー

ステップ 5　（オプション）：MAC OS X CPP ポリシーを作成します。

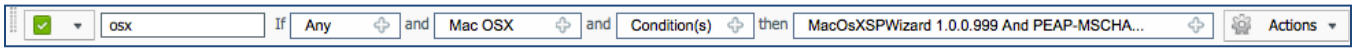


図 19.　OS X のクライアント プロビジョニング ポリシー

ステップ 6　（オプション）：Windows CPP ポリシーを作成します。

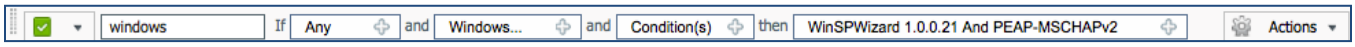


図 20.　Windows のクライアント プロビジョニング ポリシー

注：Windows と OS X には追加のサプリカント プロビジョニング プロファイルがあります。これはサプリカントと証明書のプロビジョニングを行うための Java ベースのウィザードで、アップデートの一部として cisco.com からダウンロードできます。

ポリシーの設定

この設定シナリオでは、ワイヤレス LAN コントローラ内に複数の ACL を作成します。これは BYOD サプリカントおよび証明書のプロビジョニング用に選択されたクライアントをリダイレクトするために、後で使用し、デバイスがブラックリストに登録されている場合は拒否します。

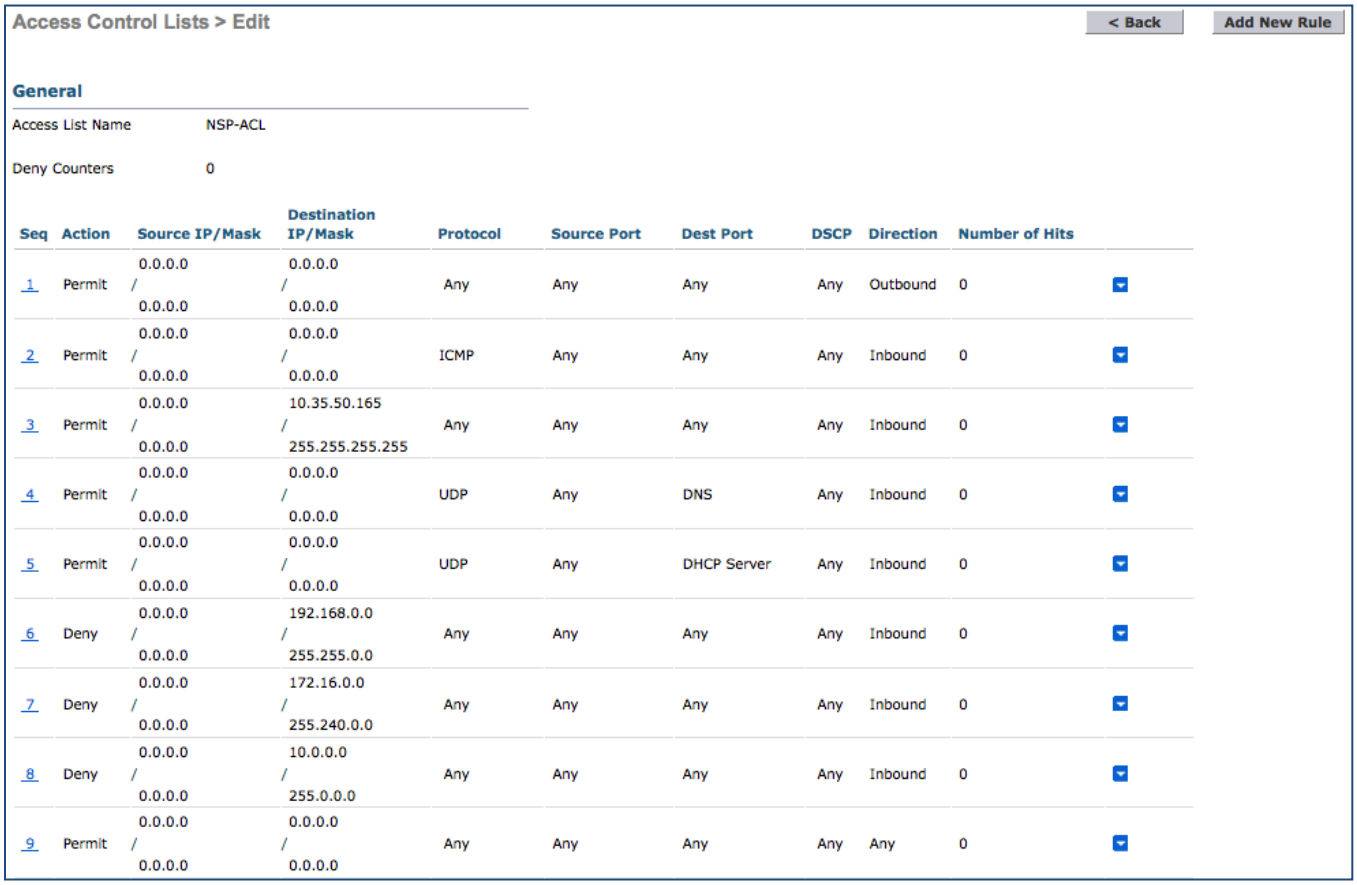
```
The Cisco Identity Services Engine IP address = 10.35.50.165
Internal Corporate Networks = 192.168.0.0, 172.16.0.0 (to redirect)
```

サプリカント プロビジョニング ACL の設定

この設定シナリオでは、ワイヤレス LAN コントローラ内に 1 つの ACL を作成します。これは BYOD サプリカントおよび証明書のプロビジョニング用に選択されたクライアントをリダイレクトするために、後で使用します。

ステップ 1　[セキュリティ（Security）] → [アクセスコントロールリスト（Access Control Lists）] に移動します。
ステップ 2　「NSP-ACL」という名前の新しい ACL を追加します。

図 1:クライアントを BYOD フローへリダイレクトするためのアクセス コントロール リスト



Access Control Lists > Edit

< Back | Add New Rule

General

Access List Name NSP-ACL

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	0
2	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	ICMP	Any	Any	Any	Inbound	0
3	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	0
4	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DNS	Any	Inbound	0
5	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	UDP	Any	DHCP Server	Any	Inbound	0
6	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
7	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0
8	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	0
9	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	0

図 21.

次に、図 17 での **NSP-ACL** について説明します。

1. サーバからクライアントへのすべてのアウトバウンド トラフィックを許可します。
2. トラブルシューティング用に、クライアントからサーバへの ICMP インバウンド トラフィックを許可します(これはオプションです)。
3. Web ポータル、サプリカント、および証明書のプロビジョニング フロー用に、クライアントからサーバ、および ISE へのすべてのインバウンド トラフィックを許可します。
4. 名前解決用に、クライアントからサーバへの DNS インバウンド トラフィックを許可します。
5. IP アドレス用に、クライアントからサーバへの DHCP インバウンド トラフィックを許可します。
6. (企業ポリシーに応じて)ISE へリダイレクトするために、クライアントからサーバ、および企業リソースへのすべてのインバウンド トラフィックを拒否します。
7. (企業ポリシーに応じて)ISE へリダイレクトするために、クライアントからサーバ、および企業リソースへのすべてのインバウンド トラフィックを拒否します。
8. (企業ポリシーに応じて)ISE へリダイレクトするために、クライアントからサーバ、および企業リソースへのすべてのインバウンド トラフィックを拒否します。
9. 残りのトラフィックをすべて許可します(オプション)。

ブラックリスト ACL の作成

ワイヤレス LAN コントローラで、「**BLACKLIST-ACL**」という名前の ACL を作成します。これは、ブラックリストに登録されているデバイスに対してアクセスを制限するために、後でポリシーで使用します。

図 2：ブラックリスト ACL

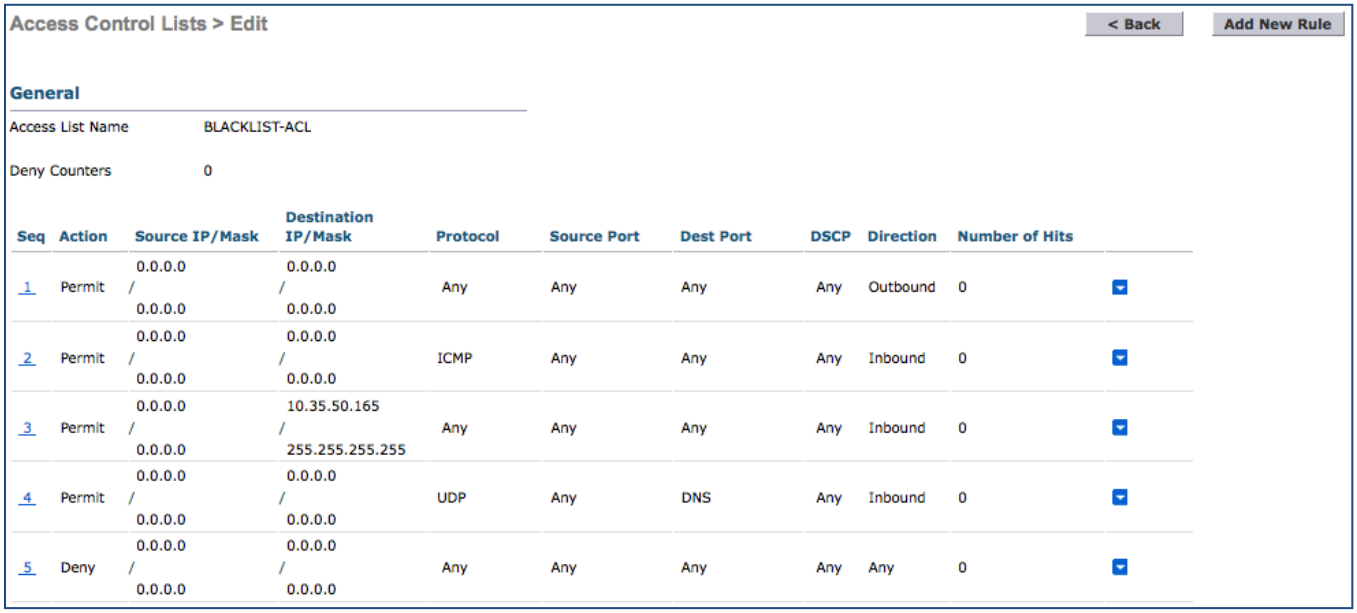


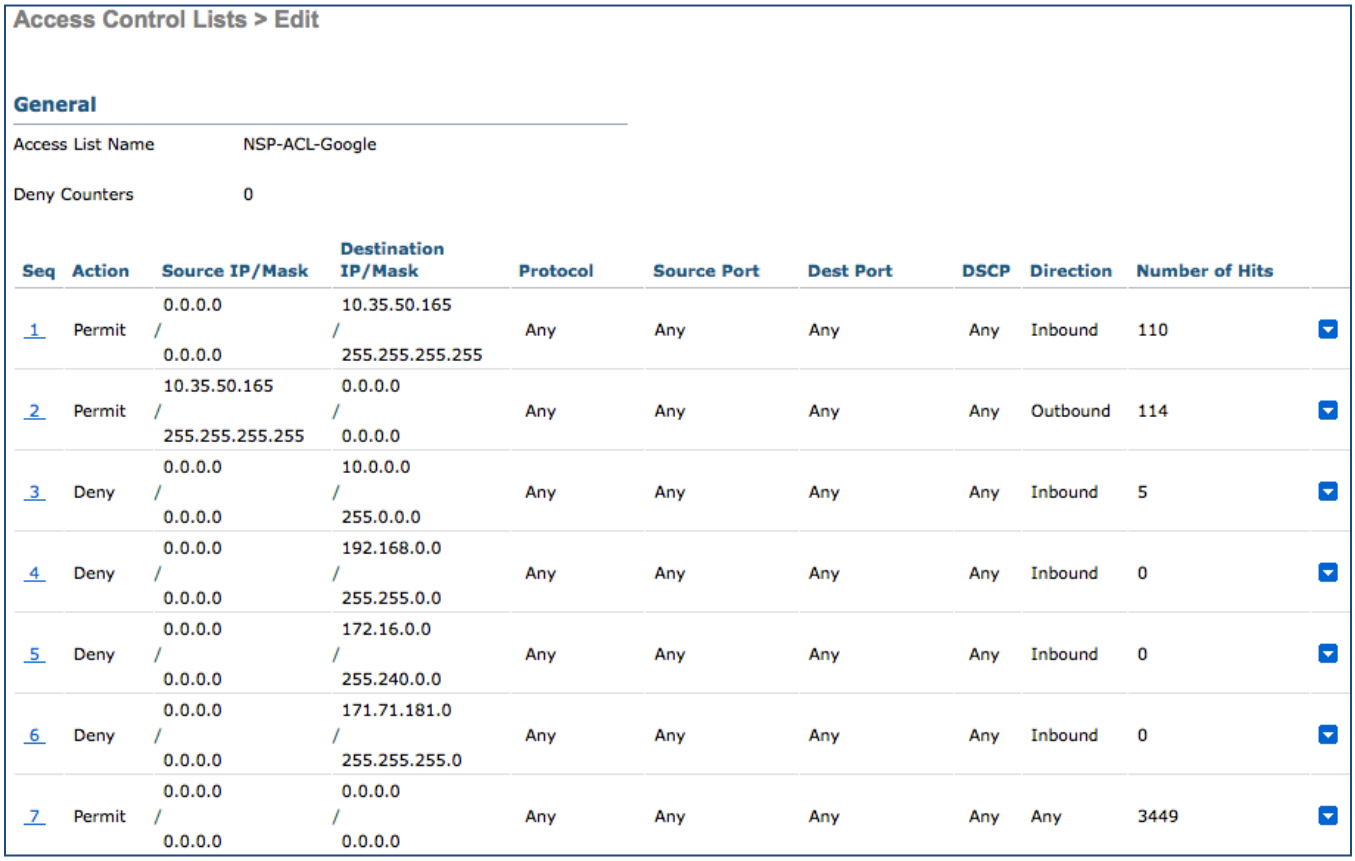
図 22.

次に、図 18 の **BLACKLIST-ACL** について説明します。

1. サーバからクライアントへのすべてのアウトバウンド トラフィックを許可します。
2. トラブルシューティング用に、クライアントからサーバへの ICMP インバウンド トラフィックを許可します（これはオプションです）。
3. ブラックリスト Web ポータル ページ用に、クライアントからサーバ、および ISE へのすべてのインバウンド トラフィックを許可します。
4. 名前解決用に、クライアントからサーバへの DNS インバウンド トラフィックを許可します。
5. 残りのトラフィックをすべて拒否します（オプション）。

ステップ 3 ワイヤレス LAN コントローラで、「**NSP-ACL-Google**」という名前の ACL を作成します。これは、Android デバイスをプロビジョニングするために、後でポリシーで使用されます。

図 3：Google アクセス ACL



Access Control Lists > Edit

General

Access List Name NSP-ACL-Google

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits
1	Permit	0.0.0.0 / 0.0.0.0	10.35.50.165 / 255.255.255.255	Any	Any	Any	Any	Inbound	110
2	Permit	10.35.50.165 / 255.255.255.255	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Outbound	114
3	Deny	0.0.0.0 / 0.0.0.0	10.0.0.0 / 255.0.0.0	Any	Any	Any	Any	Inbound	5
4	Deny	0.0.0.0 / 0.0.0.0	192.168.0.0 / 255.255.0.0	Any	Any	Any	Any	Inbound	0
5	Deny	0.0.0.0 / 0.0.0.0	172.16.0.0 / 255.240.0.0	Any	Any	Any	Any	Inbound	0
6	Deny	0.0.0.0 / 0.0.0.0	171.71.181.0 / 255.255.255.0	Any	Any	Any	Any	Inbound	0
7	Permit	0.0.0.0 / 0.0.0.0	0.0.0.0 / 0.0.0.0	Any	Any	Any	Any	Any	3449

図 23.

次に、上記の図の **NSP-ACL-Google** について説明します。

1. ISE へのすべてのインバウンド トラフィックを許可します（この手順はオプションです）。
2. ISE からのすべてのアウトバウンド トラフィックを許可します（この手順はオプションです）。
3. 企業の内部サブネットへのすべてのインバウンド トラフィックを拒否します（企業ポリシーに応じて設定できます）。
4. 企業の内部サブネットへのすべてのインバウンド トラフィックを拒否します（企業ポリシーに応じて設定できます）。
5. 企業の内部サブネットへのすべてのインバウンド トラフィックを拒否します（企業ポリシーに応じて設定できます）。
6. 残りのすべてのトラフィックを許可します（これは、Google Play サブネットのみに制限されますが、Google Play サブネットは場所によって異なる可能性がありますので注意してください）。

注：必要な場合は、トラブルシューティング用に ICMP などの行を追加することができます。

注：play.google.com のみを許可する方法の詳細については、「付録 B」を参照してください。必要に応じて、トラブルシューティングのために ICMP などの行を追加することができます。

認証ポリシーの設定

複合認証ポリシーの設定

複合認証条件についてレビューします。これはポリシーの設定において後で使用します。これらのビルトイン ポリシーをレビューして、ポリシーが修正されていない状態で存在していることを確認し、後で新しいポリシーから参照できるようにします。

ステップ 1 [ポリシー(Policy)] → [条件(Conditions)] → [認証(Authentication)] → [複合条件(Compound Conditions)] をクリックします。

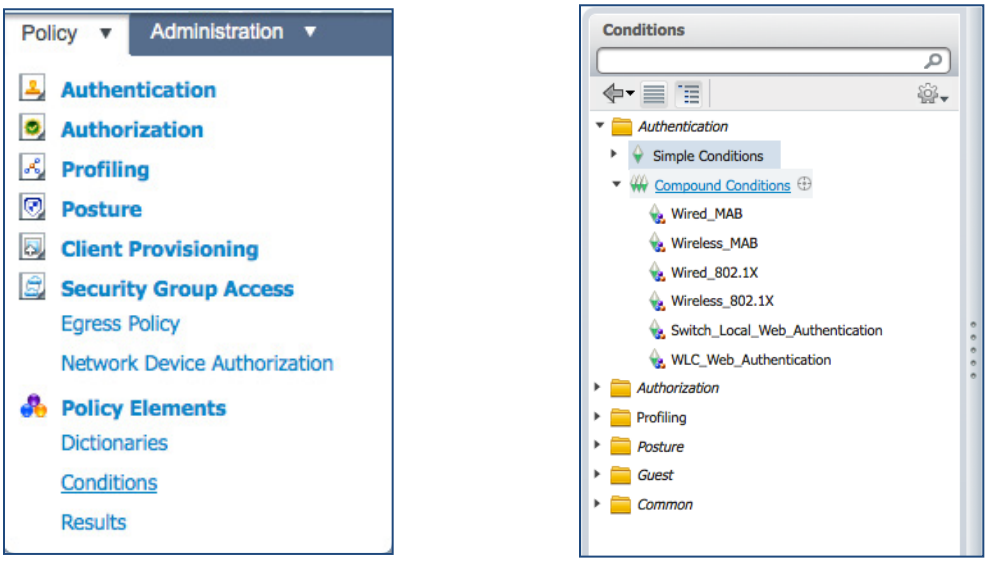


図 24. 注:ワイヤレスはセントラル スイッチング モードでのみテストされています。

ステップ 2 「**Wireless_MAB**」という名前の複合条件をレビューします。

```
"Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Wireless - IEEE 802.11"
```

図 4 ワイヤレス MAB

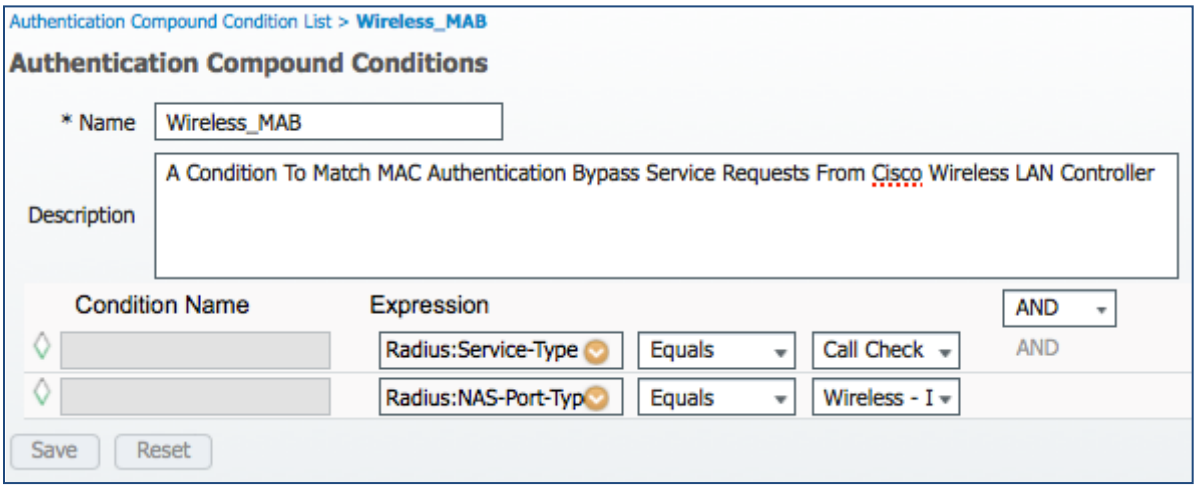
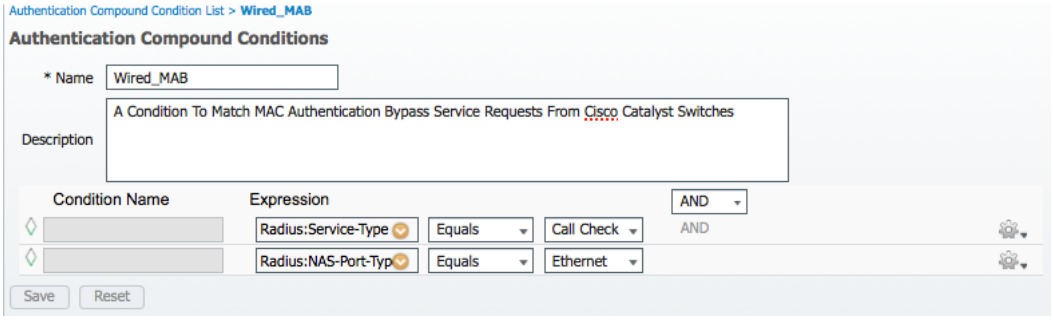


図 25.

ステップ 3 「**Wired_MAB**」という名前の複合条件をレビューします。

```
“Radius:Service-Type Equals Call Check AND Radius:NAS-Port-Type Equals Ethernet”
```

図 5 有線 MAB



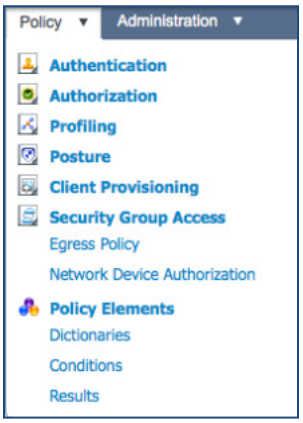
デフォルトのネットワーク アクセス結果の検証

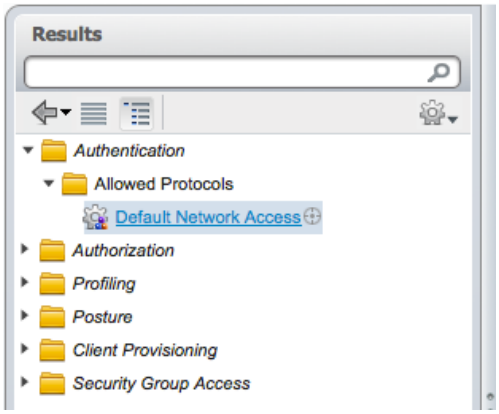
この手順では、**デフォルト ネットワーク アクセス**に設定されている現行のプロトコル設定について説明します。

ステップ 1 [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] をクリックします。

ステップ 2 [認証（Authentication）] → [許可されているプロトコル（Allowed Protocols）] → [デフォルトネットワークアクセス（Default Network Access）] をクリックします。

図 6 デフォルト ネットワーク アクセスのナビゲーション





注：プロトコル設定が次のスクリーン ショットのようになっていることを確認してください。これは、許可されているプロトコルについて、あらかじめビルドされているデフォルト ネットワーク アクセスのオブジェクトを使用するためです。デフォルトのオブジェクトが変更されていないこと、および設定が次のスクリーン ショットと一致することを確認してください。

図 7 デフォルト ネットワーク アクセス ポリシー

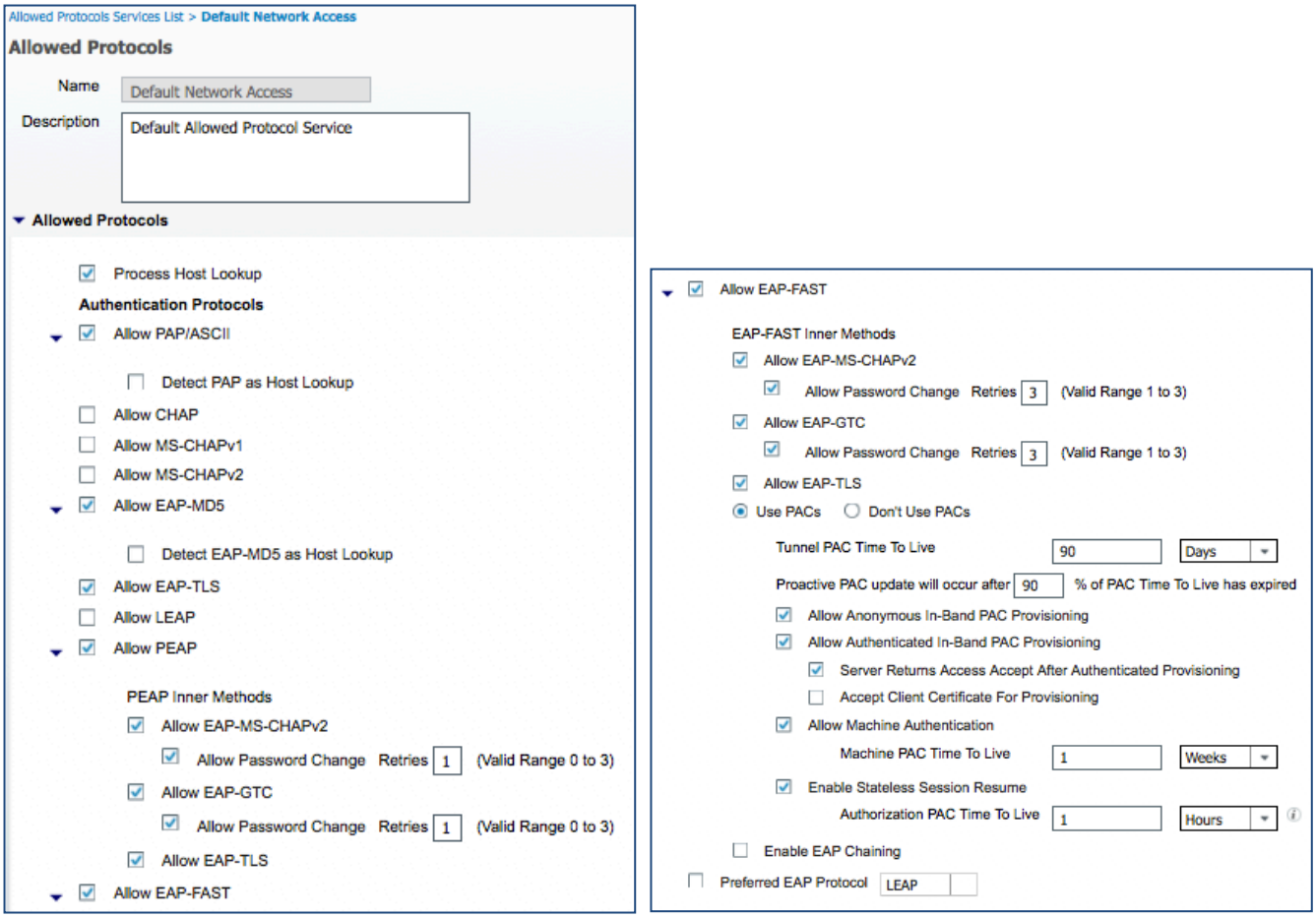


図 26.

ステップ 3 認証ポリシーの設定をレビューします。次のスクリーンショットはリファレンス用の完全なポリシー ビューで、個別のポリシーは以降の手順で設定されます。

図 8 認証ポリシーの設定

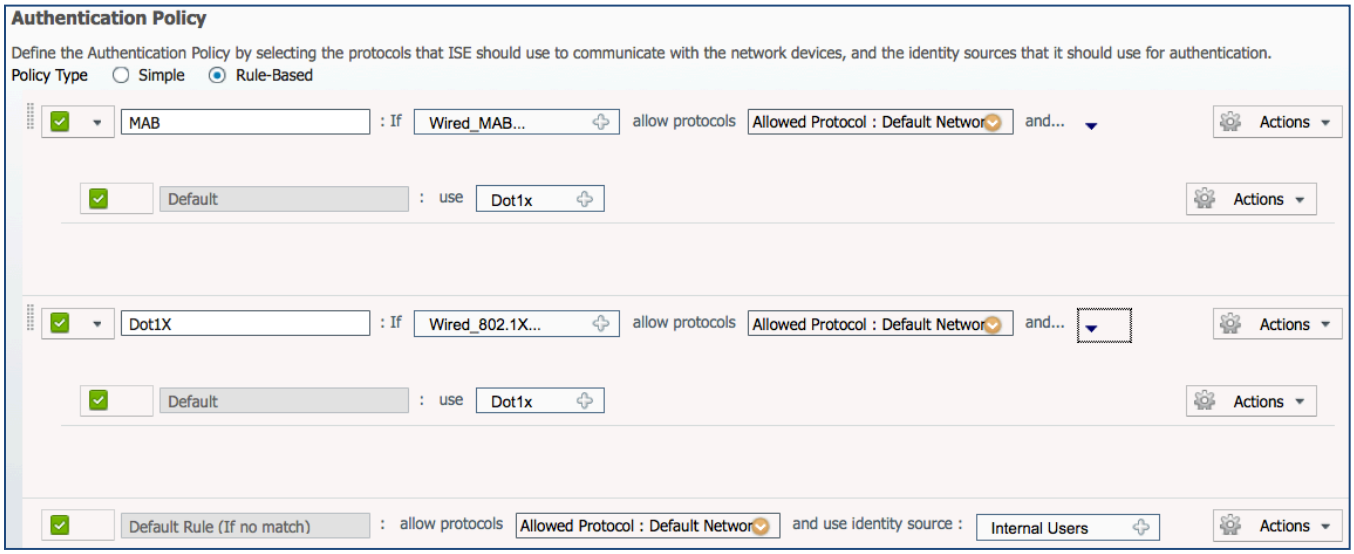
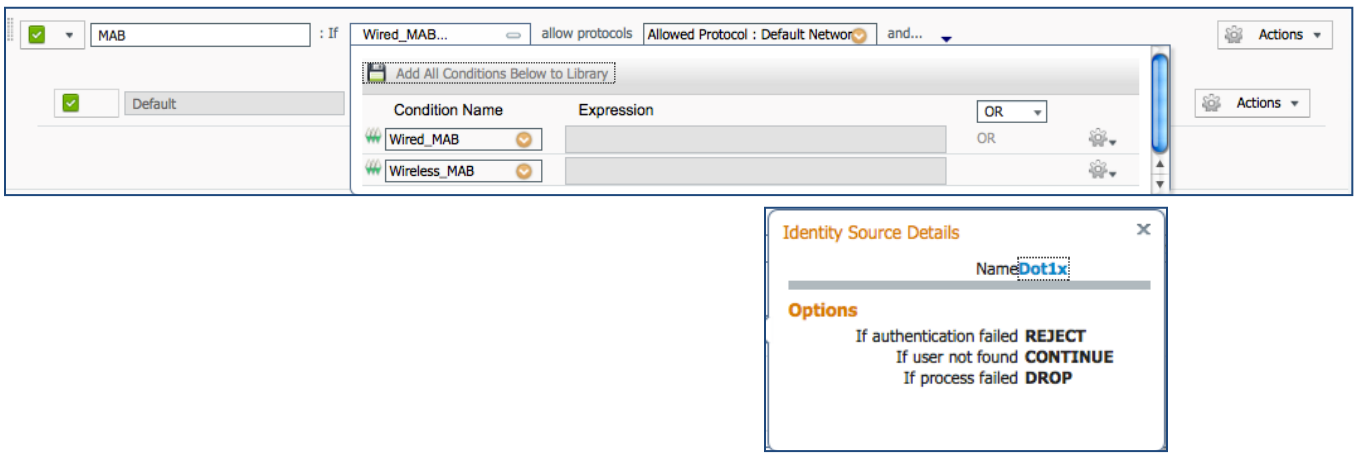


図 27.

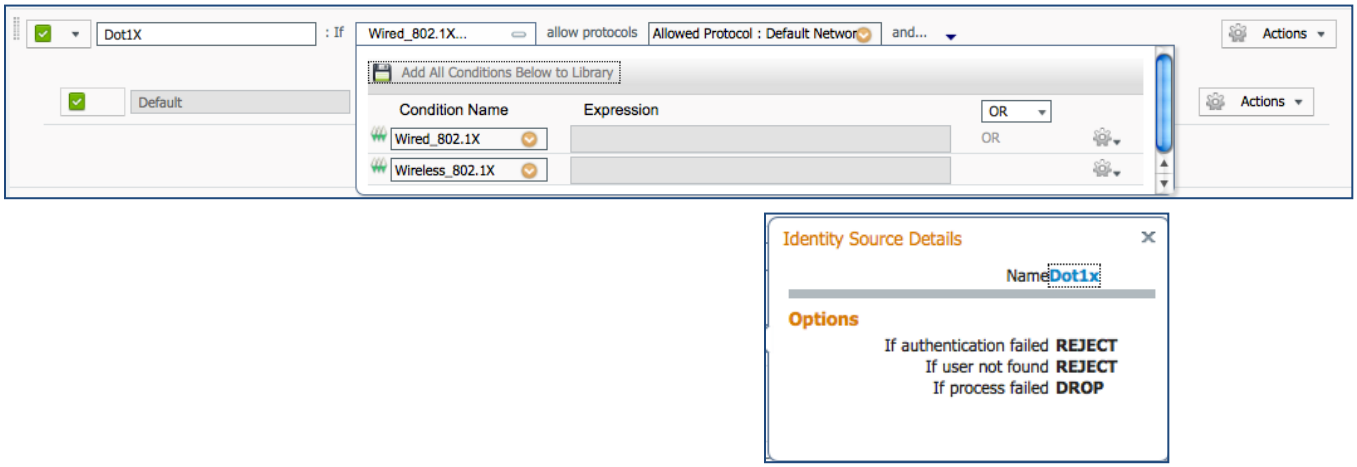
ステップ 4 MAB に対する認証ポリシー：条件（**Wired_MAB** OR **Wireless_MAB**）を追加してください。

図 9 MAC 認証バイパス ポリシー



ステップ 5　**Dot1x** に対する認証ポリシー：条件（**Wired_802.1X** OR **Wireless_802.1X**）を追加してください。

図 10 802.1X ポリシー



ステップ 6　デフォルトの認証ポリシー

図 11 デフォルトの認証ポリシー

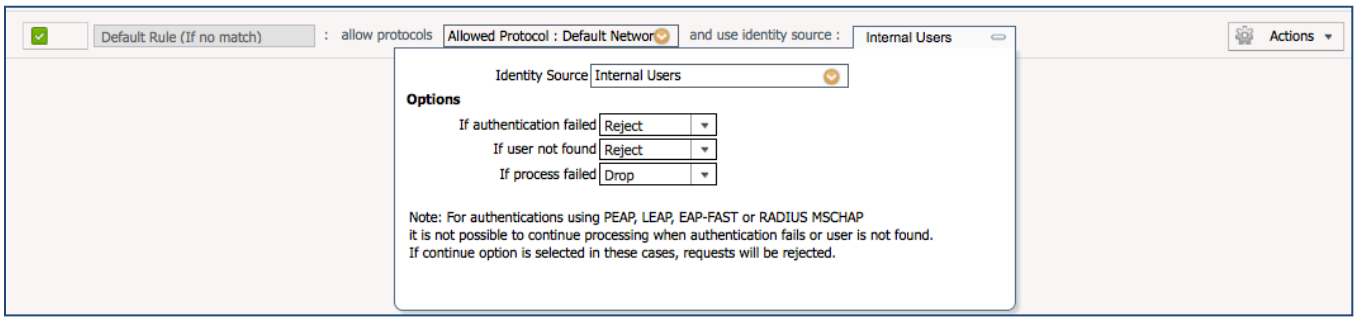


図 28.

「CWA」という名前の認可ポリシーの設定

ステップ 1　[ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] をクリックします。
ステップ 2　[許可（Authorization）] → [許可プロファイル（Authorization Profiles）] を選択します。
ステップ 3　[追加（ADD）] をクリックします。

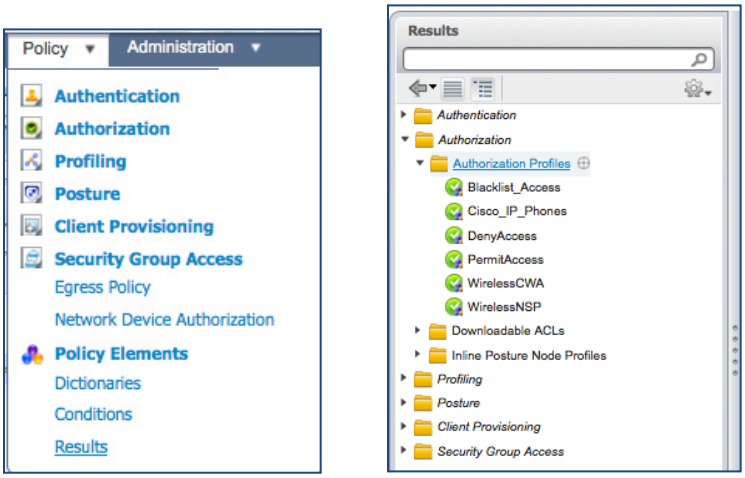


図 29. 認可プロファイルのナビゲーション

ステップ 4 「**CWA**」という名前の認可プロファイルを追加します。

中央 Web 認証（CWA）は、中央デバイスが Web ポータルとして機能できるようにします（ここでは、Cisco Identity Services Engine）。中央 Web 認証では、mac/dot1x の認証に伴ってクライアントはレイヤ 2 へシフトされます。Cisco Identity Services Engine は、Web リダイレクションを実行する必要があることをスイッチに示すための特別な属性を返します。クライアント ステーションの MAC アドレスが RADIUS サーバに知られていない場合（ただし他の基準を使用することも可能）、サーバはリダイレクション属性を返し、スイッチは（MAB を介して）ステーションを認可しますが、Web トラフィックをポータルへリダイレクトするためのアクセス リストを配置します。

ユーザがゲスト ポータルへログインすると、認可変更（CoA）を介してスイッチポートをバウンスすることが可能になり、新しいレイヤ 2 MAB 認証が発生します。ISE は、それが Web 認証ユーザであったことを覚えておいて、レイヤ 2 属性を（動的 VLAN の割り当てと同様に）ユーザに適用することができます。ActiveX コンポーネントは、クライアント PC に IP アドレスの強制リフレッシュをさせることもできます。

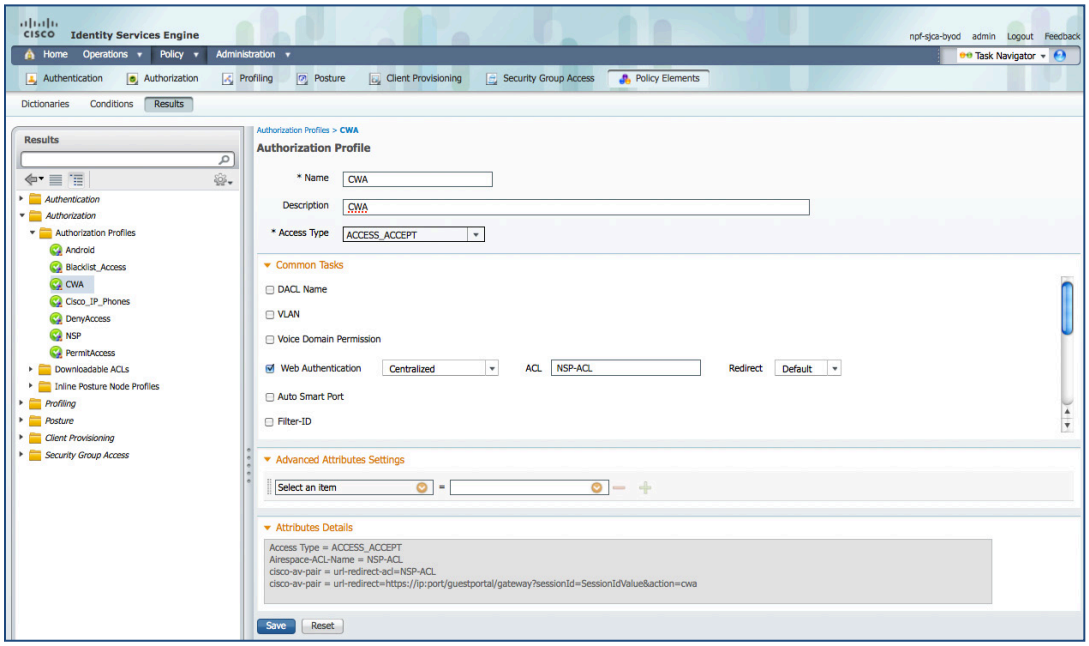


図 30. CWA の認可プロファイル

ステップ 5 「**CWA_GooglePlay**」という名前の認可プロファイルを追加します。

Android デバイスはこのプロファイルを使用して、「Cisco Network Setup Assistant」をダウンロードするために Google Play へのアクセスを可能にします。

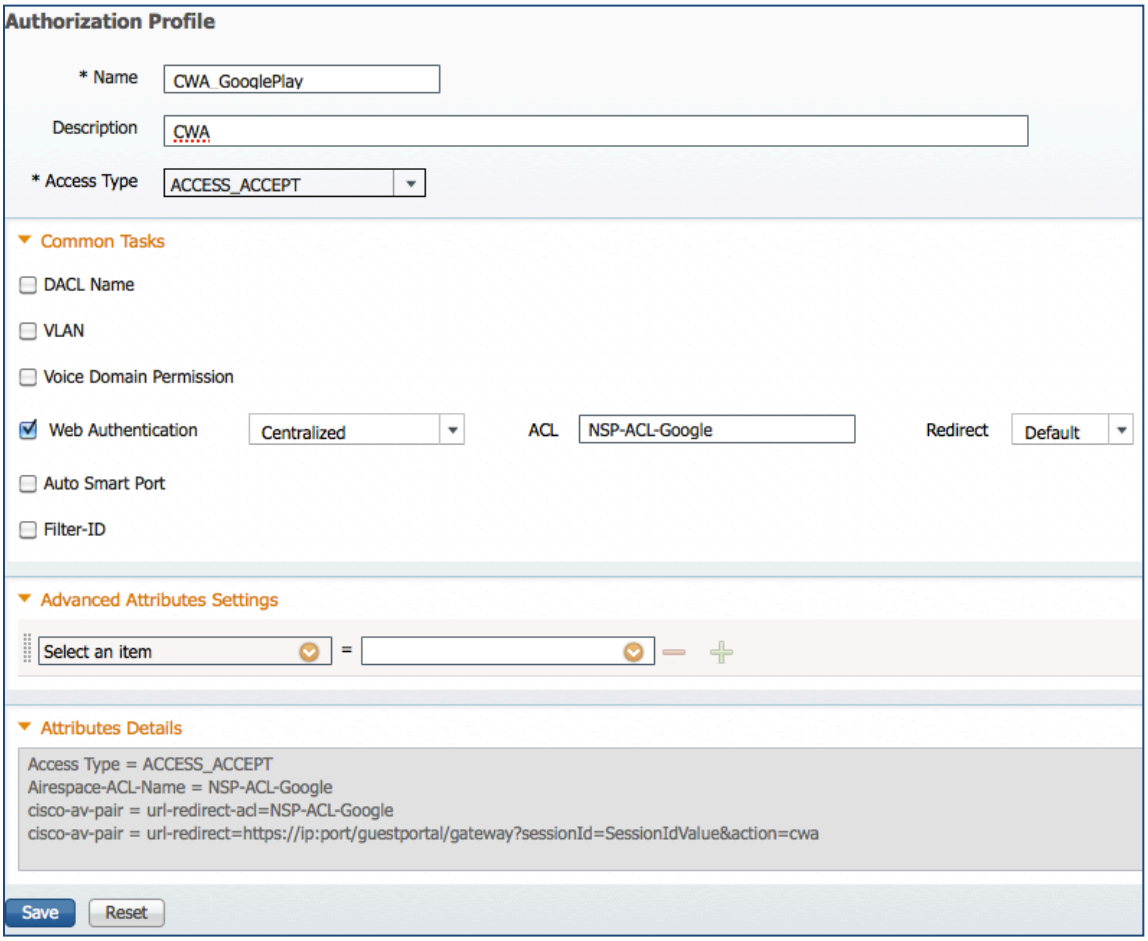


図 31. Google にアクセスするための Android 用 CWA 認可プロファイル

認可プロファイルにおけるポリシー条件のレビュー

ステップ 1 [ポリシー（Policy）] → [ポリシー要素（Policy Elements）] → [結果（Results）] → [許可（Authorization）] → [許可プロファイル（Authorization Profiles）] をクリックします。

ステップ 2 「**Blacklist_Access**」という名前のプロファイルをレビューします。

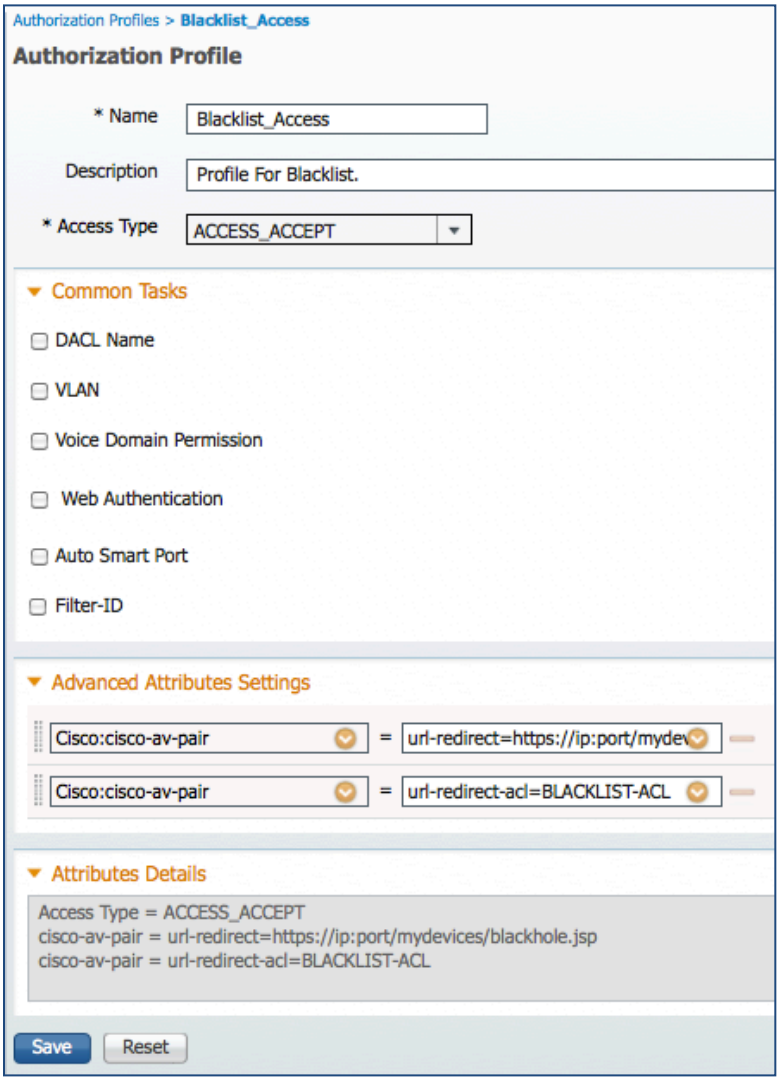


図 32.　ブラックリスト認可プロファイル

高度な属性設定（Advanced Attributes Settings）

```
Cisco:cisco-av-pair =  url-redirect=https://ip:port/mydevices/blackhole.jsp
Cisco:cisco-av-pair = url-redirect-acl=BLACKLIST-ACL
```

ステップ 3　「**NSP**」という名前の認可プロファイルを追加します。

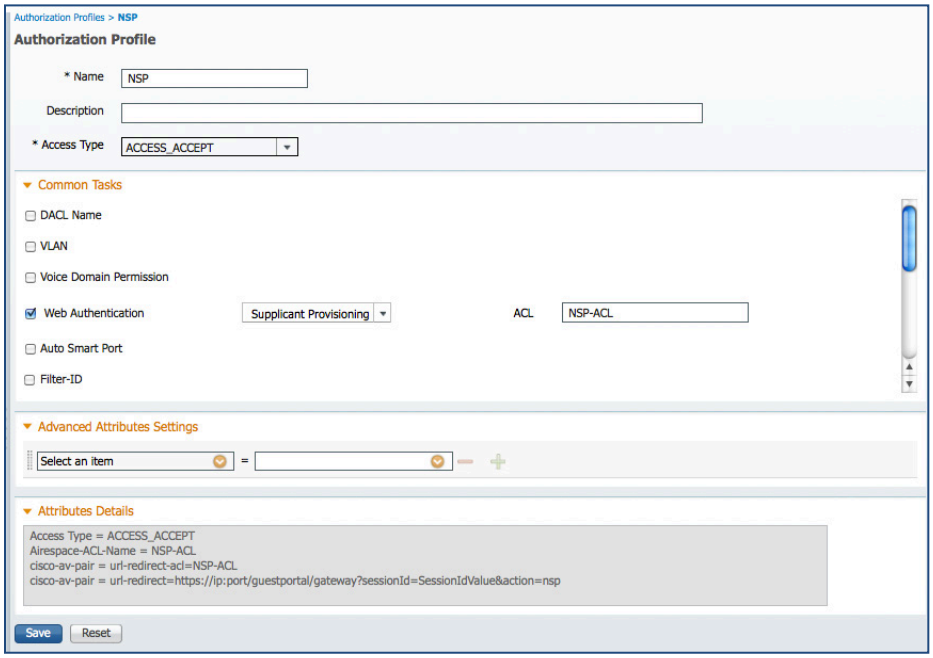
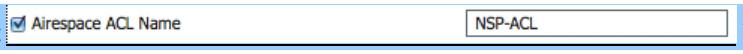


図 33. ネイティブ サプリカント プロビジョニング認可プロファイル

注： 

もクリックしてください。

ステップ 4 「**NSP_Google**」という名前の認可プロファイルを作成します。

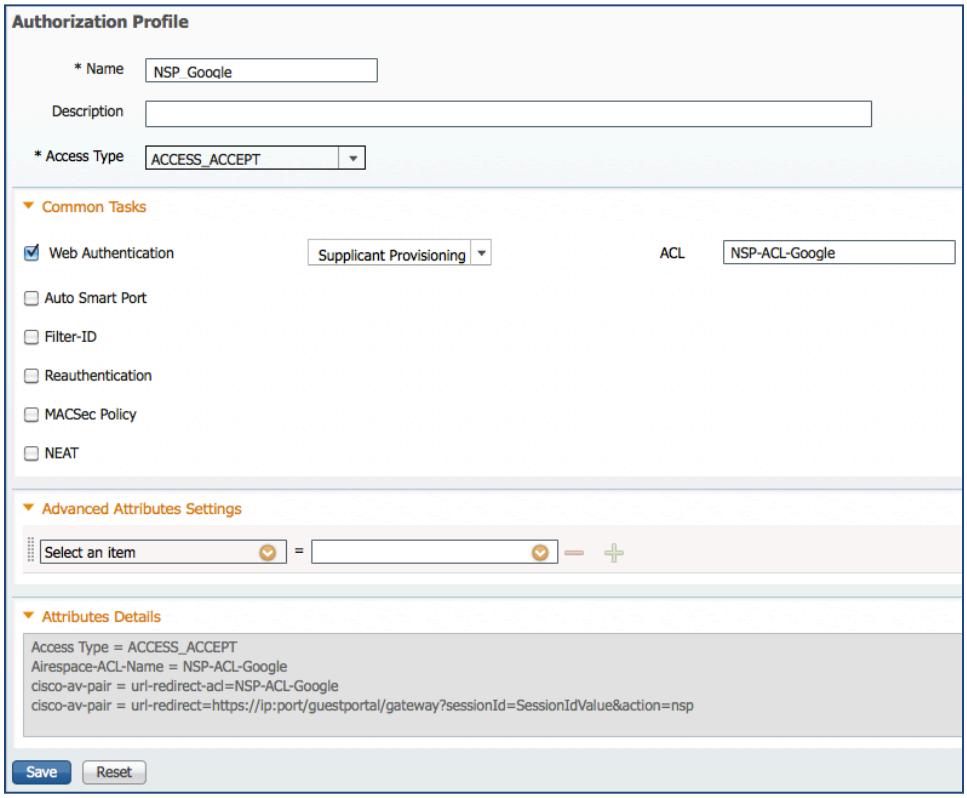
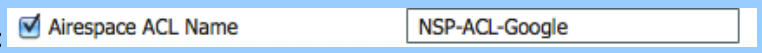


図 34. NSP_Google 認可プロファイル

注： 

もクリックしてください。

認可ポリシーの追加

ステップ 1 [ポリシー（Policy）] → [許可（Authorization）] をクリックします。
ステップ 2 [新規ルールを下に挿入（Insert New Rule Below）] をクリックします。

図 12 新規ルールの挿入

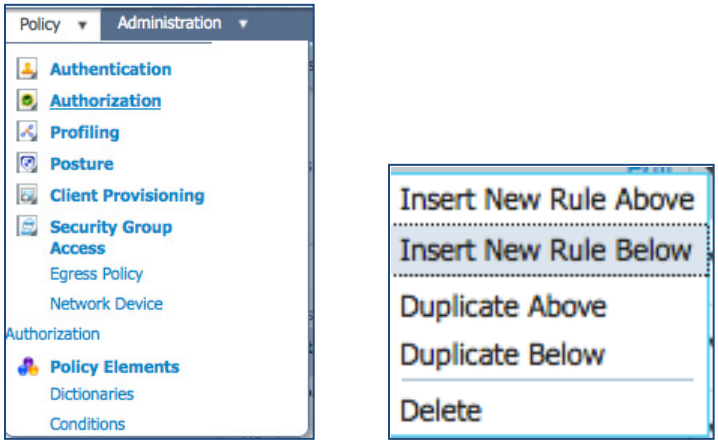


図 35. 新規ルールの挿入

ステップ 3 次の認可ポリシーを追加します。

Black List Default = This is the Default Authorization rule for blacklisting the devices, it could be customized as per company policy where devices could either be redirected to a restricted web page or even not allowed to be on the network once blacklisted.

Profiled Cisco IP Phones = Default Authorization rule for Cisco IP Phones.

Corp_Owned = This Authorization Rule is added for devices which would by-pass BYOD supplicant and certificate provisioning flows when they are classified as corporate assets "**Corp_Assets**" and coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

Android_SingleSSID = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Single SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP_Google permission to continue with the provisioning process

Android_DualSSID = This Authorization Rule is added for Android devices since they require to download the Cisco Network Setup Assistant to complete the provisioning. The rule is specific to Dual SSID setup. Once the Android device hits the "Register" button during device registration, ISE sends a Re-Auth COA to the controller. When the Android connects back to the network the session ID remains same since COA issued from ISE was Ra-Auth and NOT Session Terminate. ISE then applies the NSP_Google permission to continue with the provisioning process

CWA = Authorization rule added for Central Web Authentication.

NSP = This Authorization Rule is added for devices which will go through the BYOD supplicant and certificate provisioning flows when coming over Corporate Wireless SSID using 802.1x using protocol MSCHAPV2.

PERMIT = Devices which have completed BYOD Supplicant and Certificate provisioning, with a certificate using EAP-TLS for authentication and coming over Corporate Wireless SSID will fall under this Authorization Policy.

Default = Default Authorization Policy set as Deny Access.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions	
✓	Wireless Black List Default	if **Blacklist** AND Wireless_802.1X	then Blacklist_Access	Edit | ▾
✓	Profiled Cisco IP Phones	if **Cisco-IP-Phone**	then Cisco_IP_Phones	Edit | ▾
✓	Corp_Owned	if **Corp_Assets** AND (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then PermitAccess	Edit | ▾
✓	Android_SingleSSID	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2 AND Session:Device-OS EQUALS Android)	then NSP_Google	Edit | ▾
✓	Android_DualSSID	if (Wireless_MAB AND Session:Device-OS EQUALS Android)	then CWA_GooglePlay	Edit | ▾
✓	CWA	if Wireless_MAB	then CWA	Edit | ▾
✓	NSP	if (Wireless_802.1X AND Network Access:AuthenticationMethod EQUALS MSCHAPV2)	then NSP	Edit | ▾
✓	PERMIT	if Wireless_802.1X	then PermitAccess	Edit | ▾
✓	Default	if no matches, then DenyAccess		Edit | ▾

図 36.　認可ポリシー

すべて完了しました。

証明書およびサプリカント プロファイルのプロビジョニングについて関心がある場合は、『**BYOD-Using_Certificates_for_Differentiated_Access**』のハウツー ガイドを参照してください。

付録 A：Android および Play.Google.Com

Android がなぜ異なっているのか?

Android デバイスは、iOS デバイスや Windows とは別に扱う必要があります。これは 2 つの Android デバイスがまったく同じであることも一因ですが、Android 用のサプリカントおよび証明書を設定するにはサプリカント プロビジョニングのアプリを使用しなければならないことも原因です。

デフォルトでは、Android デバイスはどのようなソースからのアプリも承認しません。アプリは、play.google.com などの信頼できる App Store からのものであることが必須です。サプリカント プロビジョニング ウィザード（SPW）アプリをホストするよう Cisco ISE を設定することは可能ですが、エンドユーザの Android デバイスを設定して、App Store のように Cisco ISE を信頼することはできません。したがって Windows、MAC、および iOS とは異なり、Android デバイスは、BYOD およびネイティブ サプリカント プロビジョニングへ参加するためにインターネットへアクセスできることが必要です。

TrustSec のテスト中、ほとんどの場合に Google Play は TCP および UDP ポート 5228 を使用することがわかりました。ただし、これはテスト対象のすべての Android デバイスが機能するには十分ではありませんでした。インターネットの検索（「付録 C：参考資料」を参照）により、ポート8880 もオープンする必要がある場合があることがわかりました。Android の設定によっては、エンドユーザが「インターネット」または「Play Store」のオプションを指定するよう要求されることがあります。

ラボ テスト

Android オプション	オープンするネットワーク範囲	TCP および UDP のポート
Google Play オプション	74.125.00/16 173.194.0.0/16	TCP/UDP：5228 TCP/UDP：8889
インターネット オプション	74.125.00/16 173.194.0.0/16	UDP：5228 TCP：すべてのポート

付録 B：BYOD フロー

この項では、iOS および Android デバイス向けの BYOD フローについて説明します。

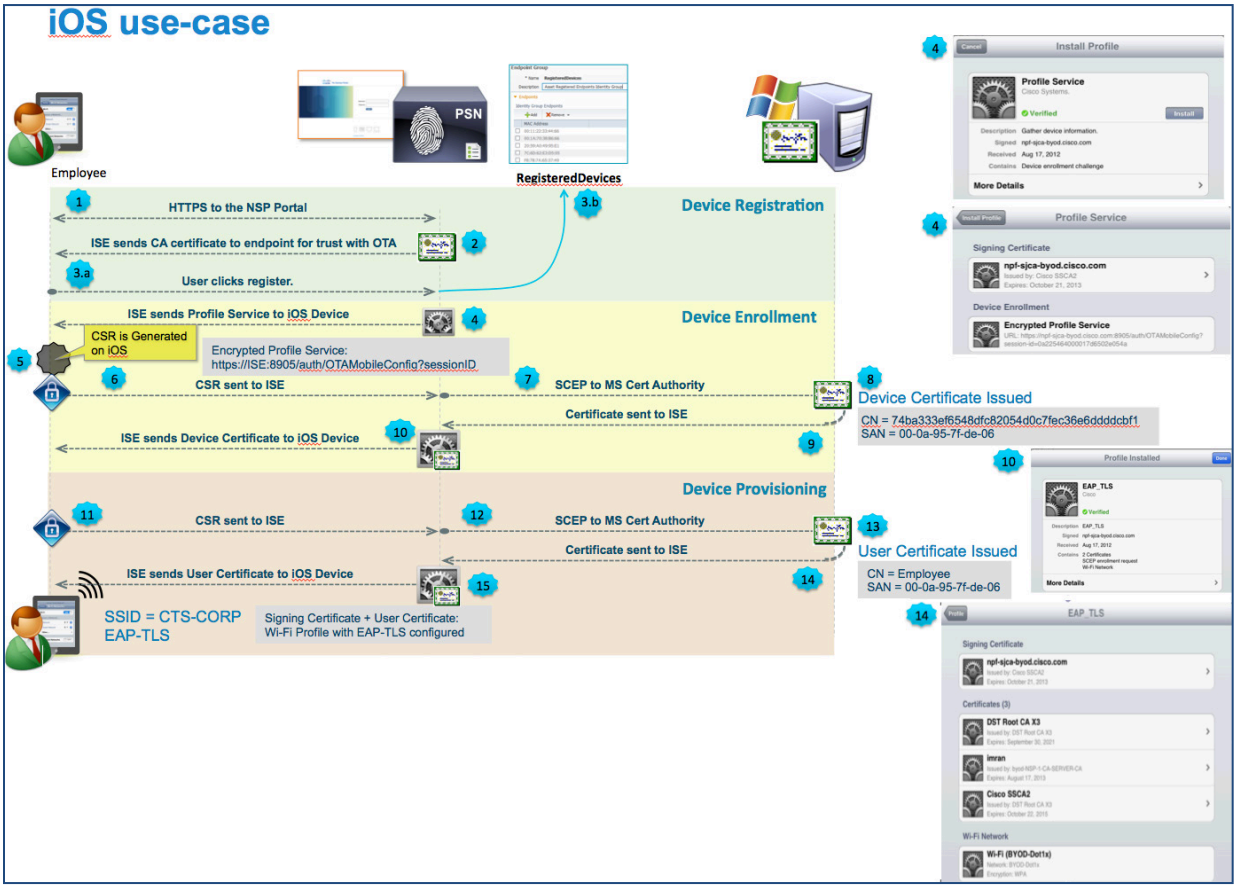


図 37. iOS および Android デバイス向けの BYOD フロー

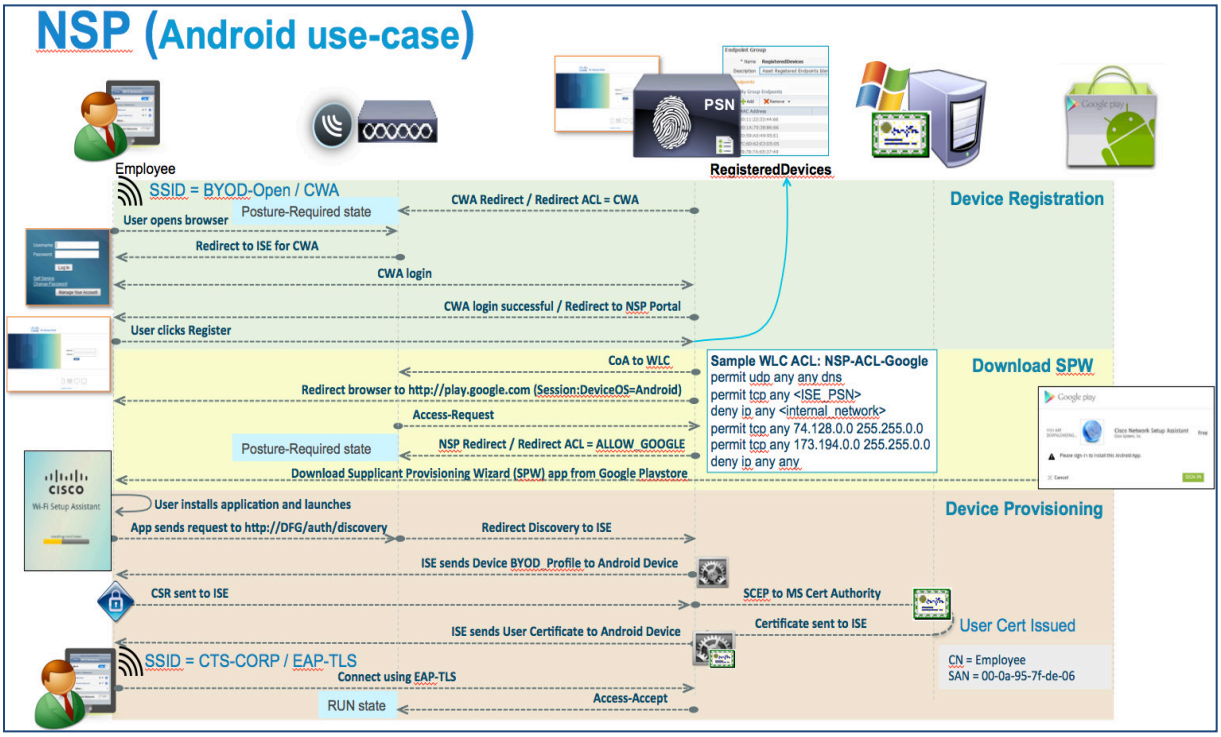


図 38. Android の使用例

付録 C：参考資料

Cisco TrustSec System

http://www.cisco.com/go/trustsec

http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing_DesignZone_TrustSec.html

デバイス設定ガイド：

Cisco Identity Services Engine ユーザ ガイド：
http://www.cisco.com/en/US/products/ps11640/products_user_guide_list.html

Cisco IOS ソフトウェア、Cisco IOS XE ソフトウェア、および Cisco NX-OS ソフトウェアの詳細については、次の URL を参照してください。

Cisco Catalyst 2900 シリーズ スイッチ：
http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000 シリーズ スイッチ：
http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html

Cisco Catalyst 3000-X シリーズ スイッチ：
http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html

Cisco Catalyst 4500 シリーズ スイッチ：
http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html

Cisco Catalyst 6500 シリーズ スイッチ：
http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html

Cisco ASR 1000 シリーズ ルータ：
http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html

Cisco Wireless LAN Controller：
http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/wlc_cg70MR1.html