

Cisco Identity Services Engine に関する Cisco ワイヤレス LAN コントローラの 汎用設定

セキュア アクセスを実現するハウツーガイドシリーズ

作成者: Hosuk Won

日付: 2012 年 8 月

目次

3850 スイッチの有線 C3PL 設定	3
全体設計	3
3850 スイッチの C3PL 設定手順	4
スイッチの HTTP サーバを設定する	5
3850 スイッチの有線 C3PL 設定	24
Cisco ワイヤレス LAN コントローラの汎用設定	44
Cisco WLC の初期設定	44
ワイヤレス LAN コントローラのブートストラップを行う	44
Cisco WLC の DHCP プロキシ	45
WLC の SNMP を設定する	46
Cisco ISE を RADIUS サーバとして使用するよう WLC を設定する	47
RADIUS フォールバック オプションの設定	50
ポスチャアセスメント用の Airespace ACL を作成する	51
すべてのトラフィックを許可する Airespace ACL を追加する	53
従業員およびゲスト VLAN 用の動的インターフェイスを作成する	53
802.1X および中央 Web 認証の SSID の追加	56
従業員用の 802.1X WLAN を追加する	56
ワイヤレス中央 Web 認証用のオープン SSID を追加する	58
ワイヤレス認証に関する Cisco ISE の設定	61
ワイヤレス認証要求を受け入れるように Cisco ISE を設定します。	61
Apple の Captive Network Assistant (CNA)	63
CNA をバイパスするように WLC を設定する:	63
キャプティブ バイパス CLI を有効にする	63
付録 A: 参考資料	64
Cisco TrustSec システム:	64
デバイス設定ガイド:	64

3850 スイッチの有線 C3PL 設定

この設定例は、新しい C3PL 構文を使用して Cisco 3850 スイッチの有線アクセスレイヤ認証を設定する方法を示しています。Cisco Catalyst 3850 は、単一の Cisco IOS XE ソフトウェアをベースとしたプラットフォームで有線およびワイヤレスのサービスを可能にする、最初のスタックブル アクセス スイッチング プラットフォームです。スタック上のステートフル スイッチオーバー (SSO) に基づく高可用性、きめ細かい QoS、セキュリティ、Flexible NetFlow (FNF) などの多彩な機能を有線/ワイヤレス ネットワークでシームレスに実現します。また、有線/ワイヤレスの機能が単一の Cisco IOS ソフトウェア イメージに統合されているため、ネットワーク内でそれらの機能を有効にする場合に、ユーザが認定または認証しなければならないソフトウェアの数を削減できます。コマンドライン インターフェイス (CLI) 管理で使用するコンソール ポートが 1 つになるため、有線/ワイヤレス サービスの管理に必要なタッチ ポイント数を削減でき、その結果、ネットワーク複雑化の軽減、ネットワーク運用の簡易化、インフラストラクチャ管理の TCO の低減を実現できます。

IOS XR がインストールされた 3850 ではレガシーの認証マネージャ構文を使用できますが、このドキュメントに記載した例では主に新しい構文を取り上げます。また、このドキュメントでは、有線に関連する設定についてだけ説明します。新しい構文には多くの利点がありますが、特に顕著なのは、802.1X と MAB を同時に実行することができ、この 2 つの異なる認証プロセスを順に実行する必要がないことです。順に実行する場合は、802.1X 認証が失敗してからでないと、MAB を開始することも、RADIUS が使用可能でない場合にサービス テンプレートを使用してインターフェイスに対する事前設定済みの ACL を制御することもできません。レガシー プラットフォームでは、802.1X と MAB を順に実行するため、特定の MAB エンドポイントは速やかに IP アドレスを取得することができませんでした。802.1X と MAB を同時に処理することで、エンドポイントは DHCP で割り当てられる IP アドレスを速やかに取得できます。またレガシー プラットフォームでは、デバイスのネットワーク アクセスを認証前の段階で制限するようインターフェイスにスタティック ACL を適用すると、RADIUS サーバが使用できない間に接続するデバイスに対してはその ACL が適用されるため、RADIUS サーバが到達可能になるまでは Denial of Service (DoS) が発生します。サービス テンプレートを導入することで、RADIUS サーバが到達不能な場合など、特定の条件に一致するときにネットワーク アクセスを提供する別の ACL をインターフェイスに適用できます。

全体設計

次の図は、コンポーネントの全体的なレイアウトを示します。ユーザには、従業員ユーザと請負業者ユーザの 2 種類があります。従業員ユーザは Active Directory を使用して認証され、請負業者ユーザは ISE の内部データベースを使用してローカルで認証されます。また、請負業者ユーザには 3850 スイッチのサービス テンプレート機能を使用して VLAN 40 が割り当てられます。ここでは Cisco Identity Services Engine (ISE) 内でのさまざまな個人所有デバイス持ち込み (BYOD) ポリシーやポストチャ ポリシーの詳細については説明しませんが、この設定はそのような操作のベースラインになります。このドキュメントでは、C3PL 構文を使用した 3850 スイッチの有線設定用のベースライン設定についてだけ説明します。ワイヤレス ネットワークでの 3850 の導入やその他の ISE 設定については、ISE の対応するハウツー ドキュメントを参照してください。

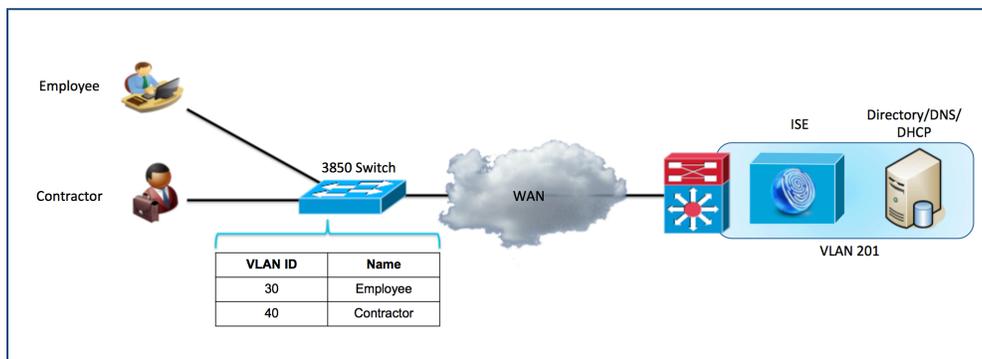


図 1.

コンポーネント

- Cisco ISE 1.2.0.899
- IOS XE バージョン 03.02.02.SE を実行する Cisco 3850
- AD/DNS/DHCP サーバとして機能する Microsoft Windows 2008

3850 スイッチの C3PL 設定手順

この設定例は、BYOD やポスチャ アセスメントなどの高度なアイデンティティ機能の基盤を提供するため、Cisco 3850 スイッチの認証を ISE と統合する方法を示しています。このドキュメントに記載した例では、主に 3850 の有線アクセス設定用の C3PL コマンドライン インターフェイスを取り上げています。

クラスベースのポリシー言語 (C3PL) を有効にする

セッション認識型ネットワークには、以前サポートされていた認証コマンドおよびポリシー コマンドの多くに代わる新しい Cisco IOS コマンドが導入されています。これらの新しいコマンドは、セッション認識型ネットワークをサポートする Cisco Common Classification Policy Language (C3PL) 表示モードを有効にした後でだけ使用できます。

注: 既存の認証マネージャ コマンドが使用されている場合、それらは C3PL 形式に変換されます。これが望ましくない場合は、この手順を開始する前に認証マネージャ コマンドが使用されていないことを確認してください。

ステップ 1 新しいスタイルの表示オプションを設定します。

次のコマンドを実行して、認証コマンドを新しいスタイルで表示します。

```
3850#authentication display new-style
```

出力例

```
3850#authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.
```

- ```
(1) If you save the config in this mode, it will be written
to NVRAM in NEW-style config, and if you subsequently
reload the router without reverting to legacy config and
saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
will only become IPv6-capable once you have entered new-
style config manually, or have reloaded with config saved
in 'authentication display new' mode.
```

```
3850#
```

**注:**簡単に言うと、CPL ベースのコマンドを入力し始めた後は、レガシー スタイルの設定モードに戻すことができなくなります。C3PL コマンドを入力したときに、警告が表示されます。レガシー モードに戻すには、**authentication display legacy** を入力してください。

## スイッチの HTTP サーバを設定する

**ステップ 1** スwitchの DNS ドメイン名を設定します。

Cisco IOS® ソフトウェアでは、デバイスの DNS ドメイン名を事前に定義しておかないと、証明書または自己生成キーを作成してインストールすることができません。次を入力します。

```
3850(config)#ip domain-name example.com
```

**ステップ 2** 次を入力して、HTTPS で使用するキーを生成します。

```
3850(config)#crypto key generate rsa general-keys modulus 2048
```

**注:** Web リダイレクト中に証明書の不一致エラーが発生しないように、ローカル証明書ではなく、信頼できる認証局が発行した証明書を使用することを推奨します。このトピックについては、このドキュメントでは説明しません。

**ステップ 3** スwitchの HTTP サーバを有効にします。

HTTP/HTTPS のキャプチャとリダイレクトを実行するには、スイッチの HTTP サーバを有効にする必要があります。次を入力します。

```
3850(config)#ip http server
3850(config)#ip http secure-server
```

**注:** ステップ 2 でキーを生成する前に **ip http secure-server** コマンドを実行しないでください。誤った順序でコマンドを実行すると、サイズの小さな証明書をスイッチが自動的に生成します。この証明書を使用すると、HTTPS トラフィックをリダイレクトするときに望ましくない動作が発生する原因になります。AireOS がインストールされた WLC と異なり、3850 シリーズのワイヤレスでは HTTPS 要求のリダイレクトがサポートされますが、エンドポイントはリダイレクト中にスイッチの自己署名証明書を信頼するように求められます。

ステップ 1 他のスイッチ管理機能の HTTP および HTTPS を無効にします(オプション)。

```
3850(config)#ip http active-session-modules none
3850(config)#ip http secure-active-session-modules none
```

**注:**これにより、3850 のワイヤレス設定への管理アクセスだけでなく、NCS Prime Infrastructure から設定への管理アクセスも無効になります。

## 手順 1 グローバル AAA コマンドを設定する

ステップ 1 アクセススイッチの認証、認可、およびアカウントिंग(AAA)を有効にします。

デフォルトでは、Cisco スイッチの AAA サブシステムは無効になっています。AAA サブシステムを有効にする前は、必要なコマンドはいずれも設定で使用できません。次を入力します。

```
3850(config)#aaa new-model
3850(config)#aaa session-id common
```

**注:**このコマンドによって、AAA のネットワークセキュリティ サービスから提供されるサービス(例えばローカル ログインの認証と認可、方式リストの定義と適用など)が有効になります。詳細については、『Cisco IOS Security Configuration Guide』を参照してください。

ステップ 2 802.1X の認証方式を作成します。

認証方式は、802.1X の認証要求に対してどの RADIUS サーバのグループを使用するかをスイッチに指示するために必要です。

```
3850(config)#aaa authentication dot1x default group radius
```

ステップ 3 802.1X の認可方式を作成します。

ステップ 2 で作成した認証方式によって、ユーザ/デバイスのアイデンティティ(ユーザ名/パスワードまたは証明書)を RADIUS サーバで検証できるようになります。しかし、有効なクレデンシャルだけでは不十分です。認可も必要です。認可は、ネットワークへのアクセスが実際に許可されるユーザまたはデバイスと、実際に許可されるアクセスレベルを定義するものです。

```
3850(config)#aaa authorization network default group radius
```

ステップ 4 802.1X のアカウントING方式を作成します。

RADIUS アカウントING パケットは非常に有用であり、ISE の多くの機能に必要です。これらのタイプのパケットは、RADIUS サーバ(Cisco ISE)がインターフェイスやエンドポイントの正確な状態を確実に認識するのに役立ちます。アカウントING パケットがないと、Cisco ISE は認証と認可の通信しか認識できません。アカウントING パケットは、認可済みセッションの長さ、クライアントの帯域幅使用量に関する情報を提供します。

```
3850(config)#aaa accounting dot1x default start-stop group radius
```

ステップ 5 定期的な RADIUS アカウントING アップデートを設定します。

Cisco ISE は、定期的な RADIUS アカウントING パケットを使用して、ネットワーク上でどのセッションがアクティブのままになっているかを追跡できます。このコマンドは、15 分ごとに定期的なアップデートを送信します。

```
3850(config)#aaa accounting update periodic 15
```

## 手順 2 グローバル RADIUS コマンドを設定する

RADIUS サーバの可用性をプロアクティブにチェックする方法を設定します。この演習では、スイッチが RADIUS サーバ (Cisco ISE) に定期的なテスト認証メッセージを送信します。スイッチはサーバからの RADIUS 応答を待機します。成功メッセージは必要ありません。サーバが稼働していることがわかればよいので、認証が失敗してもそれで十分です。

**ベスト プラクティス:** ISE 1.2 には、特定の条件下で認証を抑制する機能があります。ここでは、その機能を使用して、RADIUS キープアライブ メッセージを抑制します。手順については、このドキュメントの末尾を参照してください。

### ステップ 1 RADIUS グループに Cisco ISE サーバを追加します。

このステップでは、radius-test アカウントを使用して、Cisco ISE の各ポリシー サービス ノード (PSN) をスイッチ設定に追加します。PSN ごとに繰り返します。

```
3850(config)#radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username
radius-test idle-time 5 key cisco123
```

**注:** サーバは、通常のプロセスで発生する認証または認可に加えて、5 分に 1 回、応答があるかどうか予防的に検査されます。ISE の古いバージョンにはログ抑制機能がないため、ISE 1.2 導入環境以外ではこの値は頻繁すぎる可能性があります。その場合は、この値を 60 分以上に増やしてください。

### ステップ 2 デッド条件を設定します。

Cisco ISE サーバの RADIUS 応答をプロアクティブにチェックするようにスイッチが設定されました。次に、サーバがアライブかデッドかを判定するためにスイッチのカウンタを設定します。ここでは、RADIUS サーバからの応答を 10 秒間待機し、そのテストを 3 回試行した後でサーバをデッドと見なすように設定します。30 秒以内に Cisco ISE サーバから有効な応答が得られない場合、そのサーバはデッドと見なされます。また、deadtime はスイッチがサーバをデッドと見なす期間を定義します。ここでは、15 分に設定します。

```
3850(config)#radius-server dead-criteria time 10 tries 3
3850(config)#radius-server deadtime 15
```

**注:** 高可用性については、導入モードの項で詳しく説明します。

### ステップ 3 認可変更 (CoA) を有効にします。

前のステップでは、スイッチからの RADIUS メッセージの送信先となる RADIUS サーバの IP アドレスを定義しました。しかし、次のように (やはりグローバル設定モードの) 別のリストで認可変更 (RFC 3576) 操作を実行できるサーバを定義します。

```
3850(config)#aaa server radius dynamic-author
3850(config-locsvr-da-radius)#client 192.168.201.88 server-key cisco123
3850(config-locsvr-da-radius)#auth-type any
```

### ステップ 4 次に、ベンダー固有属性 (VSA) を有効にします。

```
3850(config)#radius-server attribute 6 on-for-login-auth
3850(config)#radius-server attribute 8 include-in-access-req
3850(config)#radius-server attribute 25 access-request include
3850(config)#radius-server attribute 31 mac format ietf upper-case
3850(config)#radius-server attribute 31 send nas-port-detail mac-only
```

**ステップ 5** スイッチが常に正しいインターフェイスから RADIUS 要求のトラフィックを送信するようにします。

多くの場合、スイッチには複数の IP アドレスが関連付けられています。したがって、常に管理通信が特定のインターフェイスを介して発生するように設定することを推奨します。このインターフェイス IP アドレスは、Cisco ISE ネットワーク デバイス オブジェクトで定義された IP アドレスと一致する必要があります。

**Cisco のベスト プラクティス:** ネットワーク管理のベスト プラクティスとしては、すべての管理通信にループバック アダプタを使用し、そのループバック インターフェイスを内部のルーティング プロトコルにアダプタイズします。

```
3850(config)#ip radius source-interface vlan 201
```

### 手順 3 ローカル アクセス コントロール リストとローカル サービス テンプレートを設定する

スイッチの特定の機能 (URL リダイレクトなど) では、ローカルに設定されたアクセス コントロール リスト (ACL) を使用する必要があります。作成されたこれらの ACL には、すぐに使用されるものと、導入のかなり後の段階まで使用されないものがあります。この項の目標は、可能なすべての導入モデルに一括して対応するようにスイッチを準備し、繰り返し行われるスイッチ設定の運用コストを抑えることです。

サービス テンプレートは、3850 スイッチの新機能です。これは、ISE 認可プロファイルと似ていますが、スイッチ上にローカルに配置できます。これは、C3PL イベントに基づいて適用できる VLAN、名前付き ACL、タイマー、および URL リダイレクト文字列の集まりです。ここでは、設定済みのどの RADIUS サーバも到達不能である場合に 802.1X または MAB 要求を処理するために適用されるサービス テンプレートをローカルで作成します。

**ステップ 1** Web 認証を伴う URL リダイレクトで使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended REDIRECT-ACL
3850(config-ext-nacl)#deny udp any host 192.168.201.72 eq 53
3850(config-ext-nacl)#deny udp any eq bootpc any eq bootps
3850(config-ext-nacl)#deny ip any host 192.168.201.88
3850(config-ext-nacl)#permit ip any any
```

**ステップ 2** 認証の前にインターフェイスに対する初期 ACL として使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended DEFAULT-ACL
3850(config-ext-nacl)#permit udp any host 192.168.201.72 eq 53
3850(config-ext-nacl)#permit udp any eq bootpc any eq bootps
3850(config-ext-nacl)#deny ip any any
```

**ステップ 3** どの RADIUS サーバも到達不能な場合に使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended PERMIT-ANY
3850(config-ext-nacl)#permit ip any any
```

**ステップ 4** どの RADIUS サーバも到達不能な場合に使用するために、「CRITICAL」という名前の次のサービス テンプレートを追加します。

```
3850(config)#service-template CRITICAL
3850(config-service-template)#description Apply When none of the RADIUS servers are reachable
3850(config-service-template)#access-group PERMIT-ANY
```

注: サービス テンプレートは、ダウンロード可能 ACL (DACL) と同じように ISE に一元的に配置して認可時にダウンロードできますが、上記のテンプレートの目的はどの ISE ノードも使用可能でないときに使用することであり、つまりサービス テンプレートをダウンロードする手段がないため、ここではローカル サービス テンプレートを作成しています。

## 手順 4 グローバル 802.1X コマンドを設定する

ステップ 5 スwitch の 802.1X をグローバルに有効にします。

802.1X をグローバルに有効にしても、実際にはどの WLAN やインターフェイスでも認証は有効になりません。

```
3850(config)#dot1x system-auth-control
```

ステップ 6 ダウンロード可能 ACL を有効にして、機能するようにします。

ダウンロード可能アクセスコントロールリスト (dACL) は、Cisco ISE 導入環境における非常に一般的な適用メカニズムです。dACL がスイッチで正しく機能するには、次のようにして IP デバイスのトラッキングをグローバルに有効にする必要があります。

```
3850(config)#ip device tracking
```

注: Windows 7 では、まれにデバイスが ARP に応答しない場合があります。その場合は、`ip device tracking use SVI` コマンドを使用する必要があります。

## 手順 5 制御クラスを設定する

制御クラスは、制御ポリシーのアクションを実行する条件を定義します。制御ポリシーのアクションを実行するためには、条件のすべてが true と評価される、いずれかが true と評価される、あるいはいずれも true と評価されない、のいずれかを定義します。制御クラスは、制御ポリシーで指定されたイベントに基づいて評価されます。

注: このスイッチで C3PL タイプのコマンドを使用するのが今回初めての場合は、スイッチの設定を消去しない限りレガシー モードに戻れないことを示す警告が表示されます。

ステップ 1 どの RADIUS サーバも使用できない場合の制御クラスを設定します。

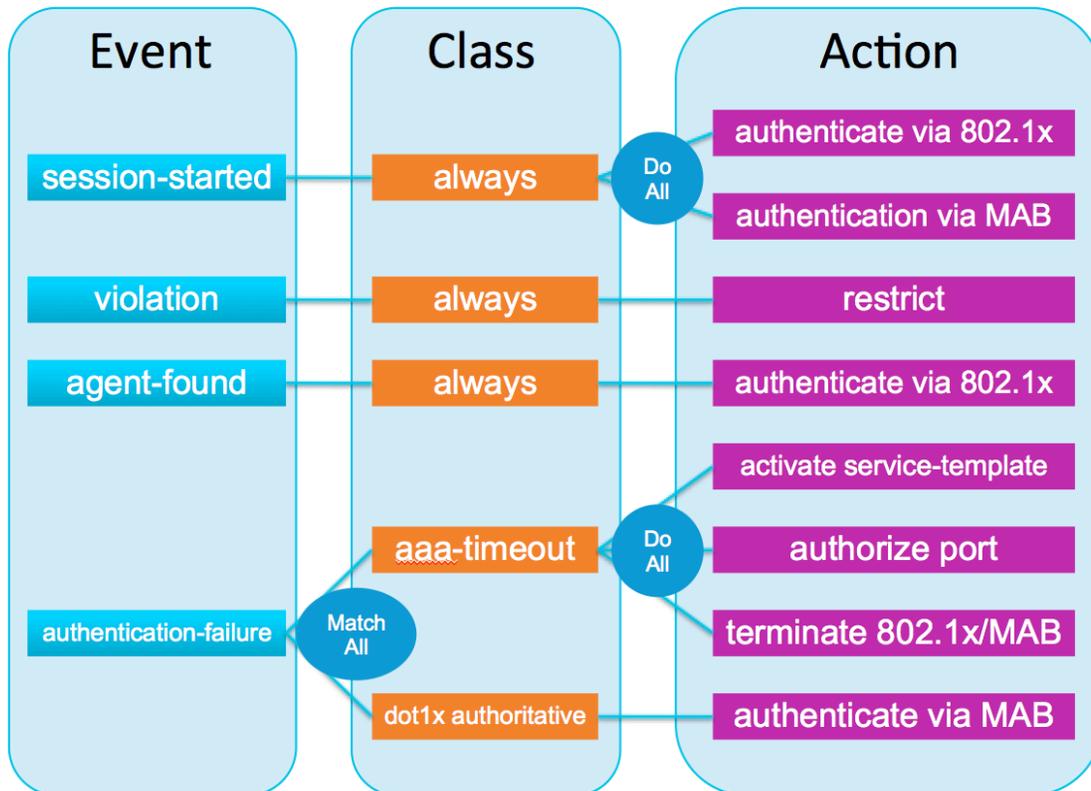
```
3850(config)#class-map type control subscriber match-any AAA-DOWN
3850(config-filter-control-classmap)#match result-type aaa-timeout
```

ステップ 2 セッションの 802.1X 認証が失敗した場合の制御クラスを設定します。

```
3850(config)#class-map type control subscriber match-all DOT1X-FAILED
3850(config-filter-control-classmap)#match method dot1x
3850(config-filter-control-classmap)#match result-type method dot1x authoritative
```

## 手順 6 制御ポリシーを設定する

制御ポリシーは、指定されたイベントと条件に対応してシステムが実行するアクションを決定します。これには、制御クラスを1つ以上のアクションに関連付ける1つ以上の制御ポリシールールが含まれます。ポリシールールで設定できるアクションは、指定するイベントのタイプに応じて異なります。制御ポリシーは、一般に加入者IDの認証およびセッションでのサービスのアクティブ化を制御し、インターフェイスに適用されます。次の図は、制御ポリシーに含まれるイベント、クラス、およびアクションの関係を示しています。



ここでは、前の項で作成した制御クラスを使用して制御ポリシーを作成し、最後にそれを一連のインターフェイスに適用します。

ステップ 1 すべての 802.1X/MAB 対応インターフェイスに適用される制御ポリシーを設定します。

```
3850(config-service-template)#policy-map type control subscriber DOT1X-DEFAULT
```

ステップ 2 セッション開始時のアクションを設定します。

次の設定によって、802.1X と MAB を同時に実行できるようになります。

```
3850(config-event-control-policymap)#event session-started match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 authenticate using dot1x priority 10
3850(config-action-control-policymap)#20 authenticate using mab priority 20
```

### ステップ 3 ポリシー違反が発生した場合のアクションを設定します。

違反が発生した場合は、次の設定によって既存のセッションがそのまま維持され、違反イベントがログに記録されます。

```
3850(config-action-control-policymap)#event violation match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 restrict
```

### ステップ 4 エンドポイントでサブリカントが検出されると、スイッチは 802.1X を使用してエンドポイントを確認しようとします。

```
3850(config-action-control-policymap)#event agent-found match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 authenticate using dot1x
```

### ステップ 5 使用可能な RADIUS サーバの不在または認証の失敗が原因となって 802.1X 認証が失敗した場合について、それに対するアクションを設定します。

これは 2 つの部分に分かれます。1 つ目の失敗は、認証要求を処理するために使用できる RADIUS サーバが存在しない場合です。この場合は、ポリシーによって「CRITICAL」という名前のローカル サービス テンプレートがアクティブ化され、permit-all ACL と、必要に応じて特定の VLAN が適用されます。2 つ目の失敗は、802.1X の認証が失敗した場合であり、この場合は MAB が実行されます。

```
3850(config-action-control-policymap)#event authentication-failure match-all
3850(config-class-control-policymap)#10 class AAA-DOWN do-all
3850(config-action-control-policymap)#10 authorize
3850(config-action-control-policymap)#20 activate service-template CRITICAL
3850(config-action-control-policymap)#30 terminate dot1x
3850(config-action-control-policymap)#40 terminate mab
3850(config-action-control-policymap)#20 class DOT1X-FAILED do-all
3850(config-action-control-policymap)#10 authenticate using mab
```

---

注:ここでは未知の MAC アドレスに対しても ACCESS-ACCEPT を送信する中央 WebAuth が使用されるため、MAB の失敗は発生しません。このため、上記の設定では MAB の失敗イベントを定義していません。

---

## 手順 7 インターフェイスへの制御ポリシーの適用

### ステップ 1 インターフェイスの範囲に対して制御ポリシーを適用します。

```
3850(config)#interface range gigabitEthernet 1/0/1 - 48
3850(config-if-range)#description DOT1X Enabled Ports
3850(config-if-range)#switchport mode access
3850(config-if-range)#service-policy type control subscriber DOT1X-DEFAULT
```

### ステップ 2 残りのインターフェイスに特定の 802.1X 設定を適用します。

802.1X 設定の多くの部分は C3PL 形式に組み込まれていますが、引き続きレガシー形式を使用するいくつかのコマンドは個別に入力する必要があります。

```
3850(config-if-range)#spanning-tree portfast
3850(config-if-range)#authentication periodic
3850(config-if-range)#authentication timer reauthenticate server
3850(config-if-range)#mab
3850(config-if-range)#ip access-group DEFAULT-ACL in
3850(config-if-range)#access-session host-mode multi-auth
3850(config-if-range)#no access-session closed
3850(config-if-range)#dot1x timeout tx-period 10
3850(config-if-range)#access-session port-control auto
3850(config-if-range)#no shutdown
```

## 3850 の設定例

```
hostname 3850
!
aaa new-model
aaa session-id common
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting update periodic 15
!
aaa server radius dynamic-author
 client 192.168.201.88 server-key Cisco123
 auth-type any
!
vlan 10
 name USER
vlan 11
 name VOICE
!
interface vlan 10
 ip address 192.168.10.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
interface vlan 11
 ip address 192.168.11.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
!
ip device tracking
!
ip domain-name example.com
!
crypto key generate rsa general-keys modulus 2048
!
dot1x system-auth-control
!
ip http serverw
ip http secure-server
ip http secure-active-session-modules none
ip http active-session-modules none
!
ip access-list extended DEFAULT-ACL
 permit udp any host 192.168.201.72 eq domain
 permit udp any eq bootpc any eq bootps
 deny ip any any
ip access-list extended PERMIT-ANY
 permit ip any any
ip access-list extended REDIRECT-ACL
 deny udp any host 192.168.201.72 eq domain
 deny udp any eq bootpc any eq bootps
 deny ip any host 192.168.201.88
 permit ip any any
!
service-template CRITICAL
 description Apply When none of the RADIUS servers are reachable
 access-group PERMIT-ANY
!
class-map type control subscriber match-any AAA-DOWN
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X-FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
policy-map type control subscriber DOT1X-DEFAULT
 event session-started match-all
```

```
10 class always do-all
 10 authenticate using dot1x priority 10
 20 authenticate using mab priority 20
event violation match-all
10 class always do-all
 10 restrict
event agent-found match-all
10 class always do-all
 10 authenticate using dot1x
event authentication-failure match-all
10 class AAA-DOWN do-all
 10 authorize
 20 activate service-template CRITICAL
 30 terminate dot1x
 40 terminate mab
20 class DOT1X-FAILED do-all
 10 authenticate using mab
!
ip radius source-interface Vlan201
snmp-server community cisco123 RO
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 MAC 形式 ietf の大文字
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 10 tries 3
radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username radius-test idle-
time 5 key cisco123
radius-server deadtime 15
!
interface GigabitEthernet x/y/z
description DOT1X Enabled Ports
switchport access vlan 30
switchport mode access
ip access-group DEFAULT-ACL in
authentication periodic
authentication timer reauthenticate server
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
service-policy type control subscriber DOT1X-DEFAULT
access-session port-control auto
no shutdown
!
```

## ISE の設定

ISE 1.2 では、サービス テンプレートを設定し、それを認可時に 3850 スイッチに適用できます。サービス テンプレートは、エンドポイントが 802.1X、MAB、WebAuth、または CoA で認証された後の認可の一部として適用できる VLAN、ACL、URL リダイレクト ACL などの認可の集まりです。サービス テンプレートは、ISE だけでなく、スイッチ上でローカルに設定することもできます。ISE のサービス テンプレートが認可の一部として適用されるときに、そのサービス テンプレートがスイッチ上に存在しない場合は、スイッチが ISE からサービス テンプレートを取得します。この操作は、IOS プラットフォームと ISE との間における dACL の動作に似ています。ISE が 3850 スイッチと統合するための設定は、サービス テンプレート以外に存在しません。このドキュメントでは BYOD に関するポリシーについて説明しますが、基盤となるサービスで BYOD を有効にするための設定については、BYOD のハウツー ガイドを参照してください。これには、CA サーバ、外部 ID ソース、およびサブリカント プロビジョニング ポリシーの設定が含まれます。

### 手順 1 アイデンティティシーケンスを作成する

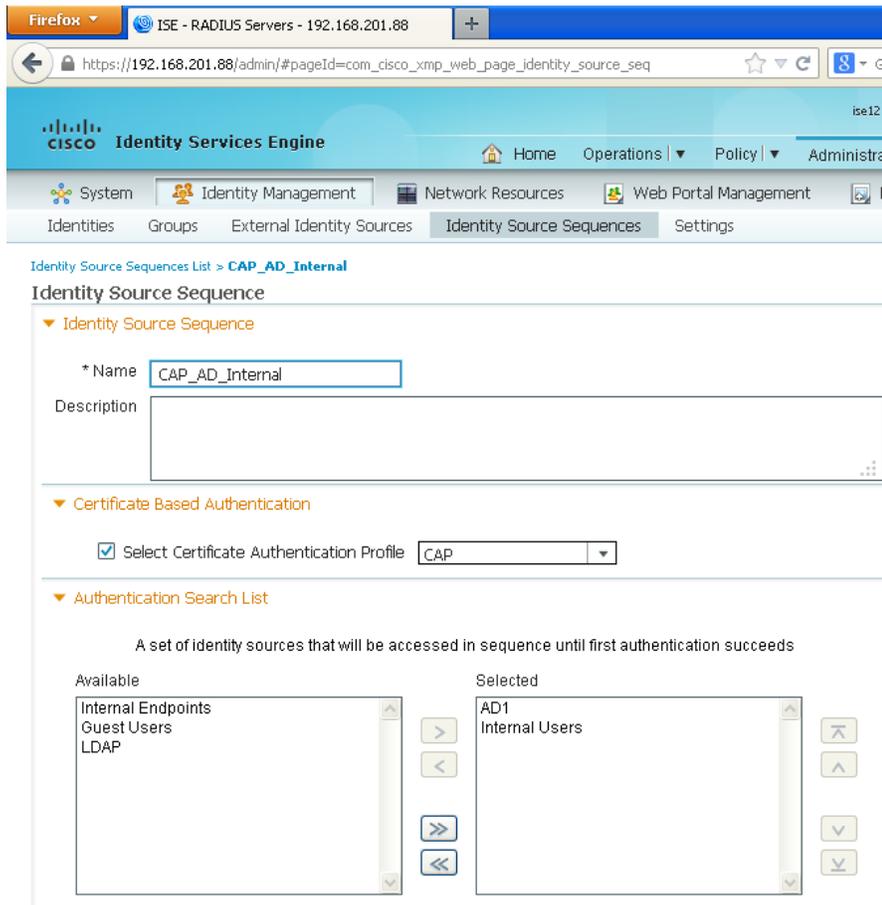
ここでは、スイッチからの認証要求を処理するアイデンティティシーケンスを作成します。このシーケンスによって、証明書、AD、または内部ユーザ データベースを使用してエンドポイントが認証されます。

ステップ 1 ISE プライマリ管理ノードにログインします。

ステップ 2 [管理 (Administration)] → [ID の管理 (Identity Management)] → [ID ソース 順序 (Identity Source Sequences)] に移動します。

ステップ 3 [追加 (Add)] をクリックします。

ステップ 4 「CAP\_AD\_Internal」という名前のシーケンスを作成します。



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The browser address bar shows the URL: `https://192.168.201.88/admin/#pageId=com_cisco_xmp_web_page_identity_source_seq`. The page title is "Identity Source Sequences List > CAP\_AD\_Internal". The main content area is titled "Identity Source Sequence" and contains the following configuration fields:

- Identity Source Sequence**
  - \* Name: CAP\_AD\_Internal
  - Description: (Empty text area)
- Certificate Based Authentication**
  - Select Certificate Authentication Profile: CAP
- Authentication Search List**
  - A set of identity sources that will be accessed in sequence until first authentication succeeds
  - Available: Internal Endpoints, Guest Users, LDAP
  - Selected: AD1, Internal Users

ステップ 5 [保存 (Save)] をクリックします。

## 手順 1 ユーザグループを作成してユーザを割り当てる

この例では、請負業者ユーザは ISE の内部データベースを使用して認証され、従業員ユーザは証明書または AD ユーザ アカウントを使用して認証されます。請負業者ユーザ用の ISE ユーザグループを作成します。

- ステップ 1 [管理 (Administration)] → [IDの管理 (Identity Management)] → [グループ (Groups)] → [ユーザIDグループ (User Identity Groups)] に移動します。
- ステップ 2 [追加 (Add)] をクリックします。
- ステップ 3 グループ名として「Contractor」を入力し、[送信 (Submit)] をクリックします。
- ステップ 4 [管理 (Administration)] → [IDの管理 (Identity Management)] → [ID (Identities)] → [ユーザ (Users)] に移動します。
- ステップ 5 [追加 (Add)] をクリックします。
- ステップ 6 ユーザ名として「contractor1」を入力し、パスワードを入力します。
- ステップ 7 ユーザグループとして [Contractor] を選択し、[送信 (Submit)] をクリックします。

## 手順 2 ポリシー セットを有効にする

管理者は、ISE 1.2 のポリシー セット機能を使用して複雑なアイデンティティ ポリシーを作成できます。このドキュメントでは、各 WLAN にマッピングする 2 つのポリシー セットを作成し、各ポリシー セット内で基礎となるポリシーを作成します。これにより、ISE のポリシー 構造によって個々の使用事例にどのようにポリシーが適用されるかが明確になります。

- ステップ 1 ポリシー セット機能を有効にするには、[管理 (Administration)] → [システム (System)] → [設定 (Settings)] → [ポリシーセット (Policy Sets)] に移動します。
- ステップ 2 [有効 (Enabled)] を選択して [保存 (Save)] をクリックします。

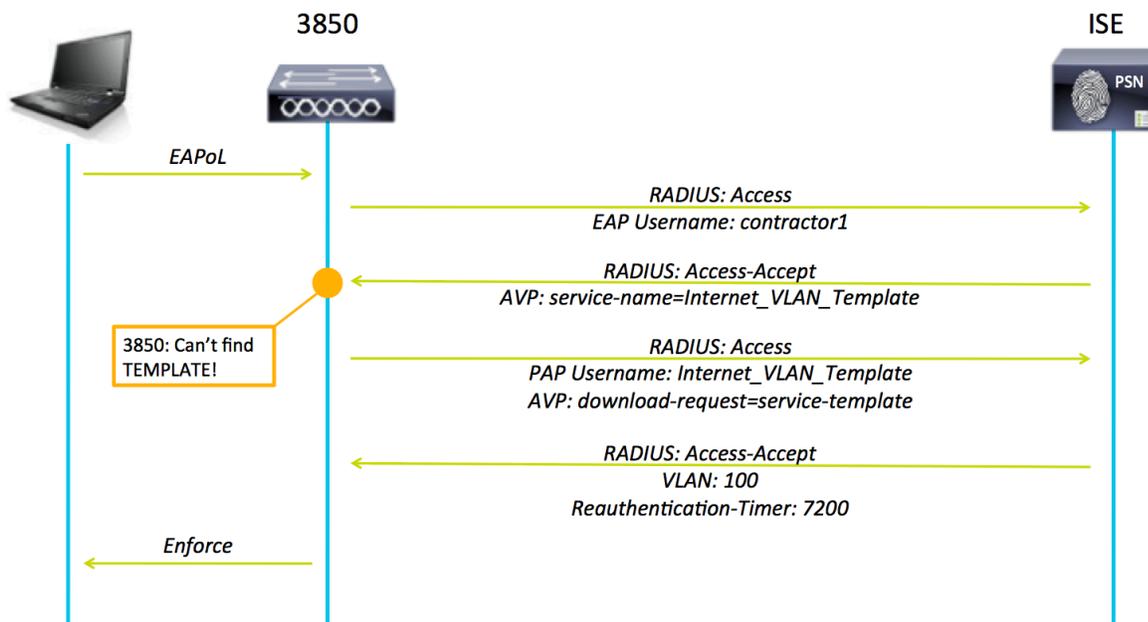
---

**注:** ポリシー セット機能を有効にした後でクラシック モードに戻す場合は、ポリシーを作成し直す必要があります。ただし、この機能を有効にすると、初期ポリシーがデフォルトのポリシー セットにコピーされます。

---

### 手順 3 認可プロファイルを設定する

ここでは、2つの認可プロファイルを作成します。1つ目は通常の認可プロファイルで、認証の成功時に dACL のフルアクセス許可をそのインターフェイス用にスイッチにプッシュします。2つ目の認可プロファイルは、請負業者ユーザに対して使用され、一連の認可属性を含むサービス テンプレートをプッシュします。実際のテンプレートは ISE に配置されるため、スイッチは最初のユーザ認証後にテンプレートの内容をダウンロードするための別の要求を送信します。サービス テンプレートの操作を示す次の図を参照してください。



ステップ 1 [ポリシー (Policy)] → [ポリシー要素 (Policy Elements)] → [許可 (Authorization)] → [許可プロファイル (Authorization Profiles)] に移動します。

ステップ 2 [追加 (Add)] をクリックし、次のパラメータを指定して Permit\_ACL 認可プロファイルを作成します。

| 名前                   | Permit_ACL           |
|----------------------|----------------------|
| 一般的なタスク              | DAACL 名 (DAACL Name) |
| DAACL 名 (DAACL Name) | PERMIT_ALL_TRAFFIC   |

ステップ 3 [保存(Save)] をクリックします。

ステップ 4 [追加(Add)] をクリックし、次のパラメータを指定して Internet\_VLAN\_Template プロファイルを作成します。

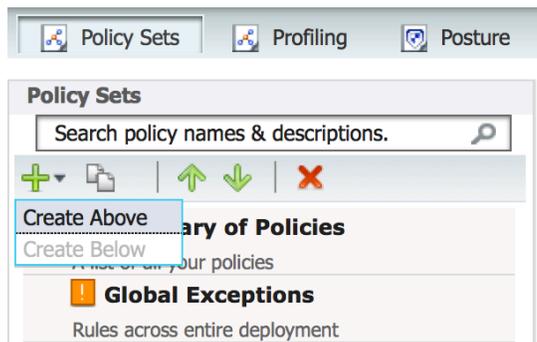
| 名前                                                 | Internet_VLAN_Template |
|----------------------------------------------------|------------------------|
| サービス テンプレート<br>(Service Template)                  | オン                     |
| 一般的なタスク                                            | VLAN                   |
| VLAN                                               | 40                     |
| RADIUS:セッションタイム<br>アウト(RADIUS:Session-<br>Timeout) | 7200                   |

ステップ 5 [保存(Save)] をクリックします。

#### 手順 4 ポリシーを設定する

ステップ 1 [ポリシー(Policy)] → [ポリシーセット(Policy Set)] に移動します。

ステップ 2 左ペインの [+] 記号をクリックし、[上を作成(Create Above)] をクリックします。



ステップ 3 名前を「DOT1X」とし、次のパラメータを指定してポリシー セットを定義します。

| Status                              | Name  | Description | Conditions   |
|-------------------------------------|-------|-------------|--------------|
| <input checked="" type="checkbox"/> | DOT1X |             | Wired_802.1X |

▼ Authentication Policy

|                                     |                            |                                            |                           |
|-------------------------------------|----------------------------|--------------------------------------------|---------------------------|
| <input checked="" type="checkbox"/> | Default Rule (If no match) | : Allow Protocols : Default Network Access | and use : CAP_AD_Internal |
|-------------------------------------|----------------------------|--------------------------------------------|---------------------------|

▼ Authorization Policy

| Status                              | Rule Name  | Conditions (identity groups and other conditions)           | Permissions                 |
|-------------------------------------|------------|-------------------------------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> | Employee   | if AD1:ExternalGroups EQUALS example.com/Users/Domain Users | then PermitAccess           |
| <input checked="" type="checkbox"/> | Contractor | if <b>Contractor</b>                                        | then Internet_VLAN_Template |
| <input checked="" type="checkbox"/> | Default    | if no matches, then                                         | DenyAccess                  |

ステップ 4 [送信 (Submit)] をクリックします。

## 手順 5 RADIUS テスト メッセージを抑制するように ISE を設定する

収集フィルタを設定して、モニタリング サーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。抑制を無効にすることもできます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

**注:** 収集フィルタの数は 20 個までに制限することを推奨します。

ステップ 1 ISE プライマリ管理ノードにログインします。

ステップ 2 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] に移動します。

ステップ 3 左ペインの [収集フィルタ (Collection Filters)] をクリックします。

ステップ 4 右ペイン上部の [追加 (Add)] をクリックします。

The screenshot shows the Cisco ISE Administration console. The top navigation bar includes System, Identity Management, Network Resources, Web Portal Management, and Feed Service. Below this, there are tabs for Deployment, Licensing, Certificates, Logging (selected), Maintenance, Backup & Restore, Admin Access, and Settings. The main content area is titled 'Logging' and has a left sidebar with options: Local Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, Debug Log Configuration, and Collection Filters (selected). The right pane shows 'Collection Filter List > User Name' and a 'Collection Filters' form. The form has three fields: '\* Attribute' set to 'User Name', '\* Value' set to 'radius-test', and '\* Filter Type' set to 'Filter Failed'. There are 'Save' and 'Reset' buttons at the bottom of the form.

- ステップ 5 [属性 (Attribute)] プルダウン メニューから [ユーザ名 (User Name)] を選択します。
- ステップ 6 [値 (Value)] に「radius-test」と入力します。
- ステップ 7 [フィルタタイプ (Filter Type)] プルダウン メニューから [すべてフィルタ (Filter All)] を選択します。
- ステップ 8 [保存 (Save)] をクリックします。

## 検証

### 手順 1 従業員デバイスを認証する

ADドメインの一部である Windows PC が接続すると、ISE はそのデバイスを認証し、インターフェイスに対して認可します。「show access-session interface」コマンドを使用して、インターフェイス上の認証および認可情報を検証できます。

```
3850#show access-session interface GigabitEthernet 1/0/1 detail
 Interface: GigabitEthernet1/0/1
 IIF-ID: 0x106E04000000085
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.30.100
 User-Name: host/winxp.example.com
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: N/A
 Common Session ID: C0A8C9FE00000FB30B2FC0AA
 Acct Session ID: 0x00000FAA
 Handle: 0x23000003
 Current Policy: DOT1X-DEFAULT

Server Policies:

Method status list:
 Method State
 dot1x Authc Success
 mab Authc Failed

3850#
3850#
```

## 手順 2 請負業者デバイスを認証する

請負業者アカウントを含むデバイスが接続すると、ISE はサービス テンプレートを使用してそのデバイスを認証し、インターフェイスに対して認可します。

```

3850#show access-session interface GigabitEthernet 1/0/1 detail
 Interface: GigabitEthernet1/0/1
 IIF-ID: 0x108F9C000000089
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.40.100
 User-Name: contractor1
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: 7200s (server), Remaining: 7150s
 Timeout action: Reauthenticate
 Common Session ID: COA8C9FE00000FB80B3C89C0
 Acct Session ID: 0x00000FB0
 Handle: 0x92000007
 Current Policy: DOT1X-DEFAULT

Server Policies:
 Template: Internet_VLAN_Template (priority 100)
 Vlan Group: Vlan: 40

Method status list:
 Method State
 dot1x Authc Success
 mab Authc Failed

3850#
3850#

```

また、3850 が ISE のテンプレートの内容を要求したときに、「Internet\_VLAN\_Template」のユーザ名を示すイベントが ISE 内で発生します。

| Time                    | Status | Details | Repeat Count | Identity               | Endpoint ID       | IP Address     | Device Port          | Authorization Profiles |
|-------------------------|--------|---------|--------------|------------------------|-------------------|----------------|----------------------|------------------------|
| 2014-01-16 14:55:18.062 |        |         | 0            | contractor1            | 00:16:D4:2E:E8:BA | 192.168.40.100 |                      |                        |
| 2014-01-16 14:55:08.739 |        |         |              | Internet_VLAN_Template |                   |                |                      |                        |
| 2014-01-16 14:55:08.725 |        |         |              | contractor1            | 00:16:D4:2E:E8:BA | 192.168.30.107 | GigabitEthernet1/0/1 | Internet_VLAN_Tem...   |

### 手順 3 ISE が使用できない間に認証する

ネットワークの停止や ISE ノードのダウンによって ISE が使用できない間にデバイスが接続した場合は、「CRITICAL」という名前のローカル テンプレートが適用されます。このテンプレートには、すべてのネットワーク アクセスを許可する ACL が含まれており、インターフェイスにすでに適用されているスタティック ACL はこの ACL に置き換えられます。

```
3850#show access-session interface GigabitEthernet 1/0/1 detail
Interface: GigabitEthernet1/0/1
 IIF-ID: 0x108C30000000092
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.30.107
 User-Name: 0016d42ee8ba
 Status: Authorized
 Domain: UNKNOWN
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: N/A
 Common Session ID: C0A8C9FE00000FC30F981C6E
 Acct Session ID: 0x00000FC9
 Handle: 0x43000010
 Current Policy: DOT1X-DEFAULT

Local Policies:
 Template: CRITICAL (priority 150)
 Filter-ID: PERMIT-ANY

Method status list:
 Method State
 dot1x Stopped
 mab Stopped

3850#
3850#
```

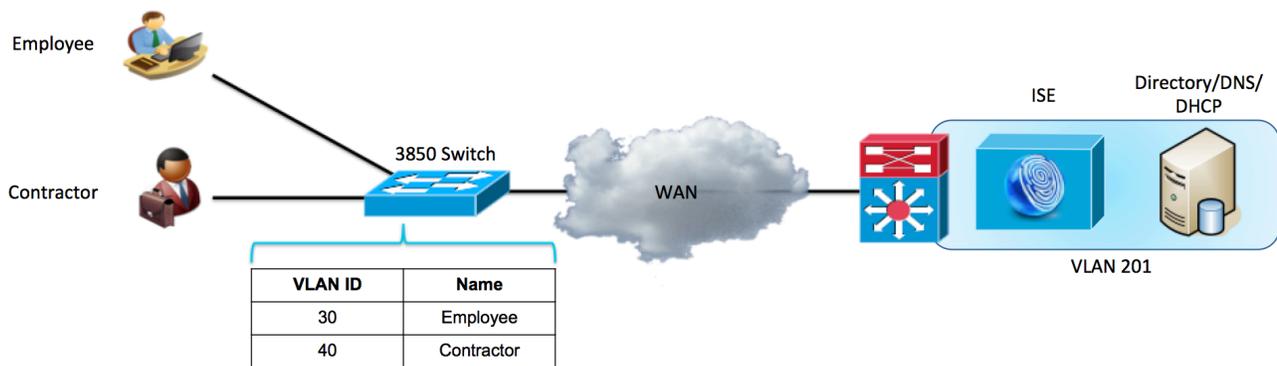
## 3850 スイッチの有線 C3PL 設定

この設定例は、新しい C3PL 構文を使用して Cisco 3850 スイッチの有線アクセスレイヤ認証を設定する方法を示しています。Cisco Catalyst 3850 は、単一の Cisco IOS XE ソフトウェアをベースとしたプラットフォームで有線およびワイヤレスのサービスを可能にする、最初のスタックブル アクセス スイッチング プラットフォームです。スタック上のステートフル スイッチオーバー (SSO) に基づく高可用性、きめ細かい QoS、セキュリティ、Flexible NetFlow (FNF) などの多彩な機能を有線/ワイヤレス ネットワークでシームレスに実現します。また、有線/ワイヤレスの機能が単一の Cisco IOS ソフトウェア イメージに統合されているため、ネットワーク内でそれらの機能を有効にする場合に、ユーザが認定または認証しなければならないソフトウェアの数を削減できます。コマンドライン インターフェイス (CLI) 管理で使用するコンソール ポートが 1 つになるため、有線/ワイヤレス サービスの管理に必要なタッチ ポイント数を削減でき、その結果、ネットワーク複雑化の軽減、ネットワーク運用の簡易化、インフラストラクチャ管理の TCO の低減を実現できます。

IOS XR がインストールされた 3850 ではレガシーの認証マネージャ構文を使用できますが、このドキュメントに記載した例では主に新しい構文を取り上げます。また、このドキュメントでは、有線に関連する設定についてだけ説明します。新しい構文には多くの利点がありますが、特に顕著なのは、802.1X と MAB を同時に実行することができ、この 2 つの異なる認証プロセスを順に実行する必要がないことです。順に実行する場合は、802.1X 認証が失敗してからでないと、MAB を開始することも、RADIUS が使用可能でない場合にサービス テンプレートを使用してインターフェイスに対する事前設定済みの ACL を制御することもできません。レガシー プラットフォームでは、802.1X と MAB を順に実行するため、特定の MAB エンドポイントは速やかに IP アドレスを取得することができませんでした。802.1X と MAB を同時に処理することで、エンドポイントは DHCP で割り当てられる IP アドレスを速やかに取得できます。また、レガシー プラットフォームでは、認証前の段階でデバイスのネットワーク アクセスを制限するためにインターフェイスにスタティック ACL を適用すると、RADIUS サーバが使用可能でない間に接続するデバイスに対してその ACL が適用されるため、RADIUS サーバが到達可能になるまで Denial of Service (DoS) が発生します。サービス テンプレートを導入することで、RADIUS サーバが到達不能な場合など、特定の条件に一致するときにネットワーク アクセスを提供する別の ACL をインターフェイスに適用できます。

### 全体設計:

次の図は、コンポーネントの全体的なレイアウトを示します。ユーザには、従業員ユーザと請負業者ユーザの 2 種類があります。従業員ユーザは Active Directory を使用して認証され、請負業者ユーザは ISE の内部データベースを使用してローカルで認証されます。また、請負業者ユーザには 3850 スイッチのサービス テンプレート機能を使用して VLAN 40 が割り当てられます。ここでは Cisco Identity Services Engine (ISE) 内でのさまざまな個人所有デバイス持ち込み (BYOD) ポリシーやポスチャ ポリシーの詳細については説明しませんが、この設定はそのような操作のベースラインになります。このドキュメントでは、C3PL 構文を使用した 3850 スイッチの有線設定用のベースライン設定についてだけ説明します。ワイヤレス ネットワークでの 3850 の導入やその他の ISE 設定については、ISE の対応するハウツー ドキュメントを参照してください。



## 使用されるコンポーネント:

Cisco ISE 1.2.0.899

IOS XE バージョン 03.02.02.SE を実行する Cisco 3850

AD/DNS/DHCP サーバとして機能する Microsoft Windows 2008

## 3850 スイッチの C3PL 設定手順

この設定例は、BYOD やポスチャアセスメントなどの高度なアイデンティティ機能の基盤を提供するため、Cisco 3850 スイッチの認証を ISE と統合する方法を示しています。このドキュメントに記載した例では、主に 3850 の有線アクセス設定用の C3PL コマンドライン インターフェイスを取り上げています。

### 手順 4 クラスベースのポリシー言語 (C3PL) を有効にする

セッション認識型ネットワークには、以前サポートされていた認証コマンドおよびポリシー コマンドの多くに代わる新しい Cisco IOS コマンドが導入されています。これらの新しいコマンドは、セッション認識型ネットワークをサポートする Cisco Common Classification Policy Language (C3PL) 表示モードを有効にした後でだけ使用できます。

**注:** 既存の認証マネージャコマンドが使用されている場合、それらは C3PL 形式に変換されます。これが望ましくない場合は、この手順を開始する前に認証マネージャコマンドが使用されていないことを確認してください。

#### ステップ 1 新しいスタイルの表示オプションを設定します。

次のコマンドを実行して、認証コマンドを新しいスタイルで表示します。

```
3850#authentication display new-style
```

## 出力例

```
3850#authentication display new-style

Please note that while you can revert to legacy style
configuration at any time unless you have explicitly
entered new-style configuration, the following caveats
should be carefully read and understood.

(1) If you save the config in this mode, it will be written
to NVRAM in NEW-style config, and if you subsequently
reload the router without reverting to legacy config and
saving that, you will no longer be able to revert.

(2) In this and legacy mode, Webauth is not IPv6-capable. It
will only become IPv6-capable once you have entered new-
style config manually, or have reloaded with config saved
in 'authentication display new' mode.

3850#
```

注:簡単に言うと、CPL ベースのコマンドを入力し始めた後は、レガシー スタイルの設定モードに戻すことができなくなります。C3PL コマンドを入力したときに、警告が表示されます。レガシー モードに戻すには、**authentication display legacy** を入力してください。

## 手順 5 スイッチの HTTP サーバを設定する

### ステップ 1 スイッチの DNS ドメイン名を設定します。

Cisco IOS® ソフトウェアでは、デバイスの DNS ドメイン名を事前に定義しておかないと、証明書または自己生成キーを作成してインストールすることができません。次を入力します。

```
3850(config)#ip domain-name example.com
```

### ステップ 2 次を入力して、HTTPS で使用するキーを生成します。

```
3850(config)#crypto key generate rsa general-keys modulus 2048
```

注:Web リダイレクト中に証明書の不一致エラーが発生しないように、ローカル証明書ではなく、信頼できる認証局が発行した証明書を使用することを推奨します。このトピックについては、このドキュメントでは説明しません。

### ステップ 3 スイッチの HTTP サーバを有効にします。

HTTP/HTTPS のキャプチャとリダイレクトを実行するには、スイッチの HTTP サーバを有効にする必要があります。次を入力します。

```
3850(config)#ip http server
3850(config)#ip http secure-server
```

注:ステップ 2 でキーを生成する前に **ip http secure-server** コマンドを実行しないでください。誤った順序でコマンドを実行すると、スイッチが小さいサイズの証明書を自動的に生成します。この証明書を使用すると、HTTPS トラフィックをリダイレクトするときに望ましくない動作が発生する原因になります。AireOS がインストールされた WLC と異なり、3850 シリーズのワイヤレスでは HTTPS 要求のリダイレクトがサポートされますが、エンドポイントはリダイレクト中にスイッチの自己署名証明書を信頼するように求められます。

#### ステップ 4 他のスイッチ管理機能の HTTP および HTTPS を無効にします (オプション)。

```
3850(config)#ip http active-session-modules none
3850(config)#ip http secure-active-session-modules none
```

**注:**これにより、3850 のワイヤレス設定への管理アクセスだけでなく、NCS Prime Infrastructure から設定への管理アクセスも無効になります。

### 手順 6 グローバル AAA コマンドを設定する

#### ステップ 5 アクセススイッチの認証、認可、およびアカウントिंग (AAA) を有効にします。

デフォルトでは、Cisco スイッチの AAA サブシステムは無効になっています。AAA サブシステムを有効にしないと、設定で必要なコマンドはいずれも使用できません。次を入力します。

```
3850(config)#aaa new-model
3850(config)#aaa session-id common
```

**注:**このコマンドによって、AAA のネットワーク セキュリティ サービスから提供されるサービス (ローカル ログインの認証と認可、認証方式リストの定義と適用など) が有効になります。詳細については、『Cisco IOS Security Configuration Guide』を参照してください。

#### ステップ 6 802.1X の認証方式を作成します。

認証方式は、802.1X の認証要求に対してどの RADIUS サーバのグループを使用するかをスイッチに指示するために必要です。

```
3850(config)#aaa authentication dot1x default group radius
```

#### ステップ 7 802.1X の認可方式を作成します。

ステップ 2 で作成した認証方式によって、ユーザ/デバイスのアイデンティティ (ユーザ名/パスワードまたは証明書) を RADIUS サーバで検証できるようになります。しかし、有効なクレデンシャルだけでは不十分です。認可も必要です。認可は、ネットワークへのアクセスが実際に許可されるユーザまたはデバイスと、実際に許可されるアクセスレベルを定義するものです。

```
3850(config)#aaa authorization network default group radius
```

#### ステップ 8 802.1X のアカウントング方式を作成します。

RADIUS アカウントング パケットは非常に有用であり、ISE の多くの機能に必要です。これらのタイプのパケットは、RADIUS サーバ (Cisco ISE) がインターフェイスやエンドポイントの正確な状態を確実に認識するのに役立ちます。アカウントング パケットがないと、Cisco ISE は認証と認可の通信しか認識できません。アカウントング パケットは、認可済みセッションの長さ、クライアントの帯域幅使用量に関する情報を提供します。

```
3850(config)#aaa accounting dot1x default start-stop group radius
```

#### ステップ 9 定期的な RADIUS アカウントング アップデートを設定します。

Cisco ISE は、定期的な RADIUS アカウントング パケットを使用して、ネットワーク上でどのセッションがアクティブのままになっているかを追跡できます。このコマンドは、15 分ごとに定期的なアップデートを送信します。

```
3850(config)#aaa accounting update periodic 15
```

## 手順 7 グローバル RADIUS コマンドを設定する

RADIUS サーバの可用性をプロアクティブにチェックする方法を設定します。この演習では、スイッチが RADIUS サーバ (Cisco ISE) に定期的なテスト認証メッセージを送信します。スイッチはサーバからの RADIUS 応答を待機します。成功メッセージは必要ありません。サーバがアライブ状態であることがわかればよいので、認証が失敗してもそれで十分です。

**ベスト プラクティス:** ISE 1.2 には、特定の条件下で認証を抑制する機能があります。ここでは、その機能を使用して、RADIUS キープアライブ メッセージを抑制します。手順については、このドキュメントの末尾を参照してください。

### ステップ 6 RADIUS グループに Cisco ISE サーバを追加します。

このステップでは、radius-test アカウントを使用して、Cisco ISE の各ポリシー サービス ノード (PSN) をスイッチ設定に追加します。PSN ごとに繰り返します。

```
3850(config)#radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username
radius-test idle-time 5 key cisco123
```

**注:** サーバは、通常のプロセスで発生する認証または認可に加えて、5 分に 1 回、応答があるかどうか予防的に検査されます。ISE の古いバージョンにはログ抑制機能がないため、ISE 1.2 導入環境以外ではこの値は頻繁すぎる可能性があります。その場合は、この値を 60 分以上に増やしてください。

### ステップ 7 デッド条件を設定します。

Cisco ISE サーバの RADIUS 応答をプロアクティブにチェックするようにスイッチが設定されました。次に、サーバがアライブかデッドかを判定するためにスイッチのカウンタを設定します。ここでは、RADIUS サーバからの応答を 10 秒間待機し、そのテストを 3 回試行した後でサーバをデッドと見なすように設定します。30 秒以内に Cisco ISE サーバから有効な応答が得られない場合、そのサーバはデッドと見なされます。また、deadtime はスイッチがサーバをデッドと見なす期間を定義します。ここでは、15 分に設定します。

```
3850(config)#radius-server dead-criteria time 10 tries 3
3850(config)#radius-server deadtime 15
```

**注:** 高可用性については、導入モードの項で詳しく説明します。

### ステップ 8 認可変更 (CoA) を有効にします。

前のステップで、スイッチからの RADIUS メッセージの送信先となる RADIUS サーバの IP アドレスを定義しました。しかし、次のように (やはりグローバル設定モードの) 別のリストで認可変更 (RFC 3576) 操作を実行できるサーバを定義します。

```
3850(config)#aaa server radius dynamic-author
3850(config-locsvr-da-radius)#client 192.168.201.88 server-key cisco123
3850(config-locsvr-da-radius)#auth-type any
```

### ステップ 9 次に、ベンダー固有属性 (VSA) を有効にします。

```
3850(config)#radius-server attribute 6 on-for-login-auth
3850(config)#radius-server attribute 8 include-in-access-req
3850(config)#radius-server attribute 25 access-request include
3850(config)#radius-server attribute 31 mac format ietf upper-case
3850(config)#radius-server attribute 31 send nas-port-detail mac-only
```

**ステップ 10** スイッチが常に正しいインターフェイスから RADIUS 要求のトラフィックを送信するようにします。

多くの場合、スイッチには複数の IP アドレスが関連付けられています。したがって、常に管理通信が特定のインターフェイスを介して発生するように設定することを推奨します。このインターフェイス IP アドレスは、Cisco ISE ネットワーク デバイス オブジェクトで定義された IP アドレスと一致する必要があります。

**Cisco のベスト プラクティス:** ネットワーク管理のベスト プラクティスとしては、すべての管理通信にループバック アダプタを使用し、そのループバック インターフェイスを内部のルーティング プロトコルにアダプタイズします。

```
3850(config)#ip radius source-interface vlan 201
```

## 手順 8 ローカル アクセス コントロール リストとローカル サービス テンプレートを設定する

スイッチの特定の機能 (URL リダイレクトなど) では、ローカルに設定されたアクセス コントロール リスト (ACL) を使用する必要があります。作成されたこれらの ACL には、すぐに使用されるものと、導入のかなり後の段階まで使用されないものがあります。この項の目標は、可能なすべての導入モデルに一括して対応するようにスイッチを準備し、繰り返し行われるスイッチ設定の運用コストを抑えることです。

サービス テンプレートは、3850 スイッチの新機能です。これは、ISE 認可プロファイルと似ていますが、スイッチ上にローカルに配置できます。これは、C3PL イベントに基づいて適用できる VLAN、名前付き ACL、タイマー、および URL リダイレクト文字列の集まりです。ここでは、設定済みのどの RADIUS サーバも到達不能である場合に 802.1X または MAB 要求を処理するために適用されるサービス テンプレートをローカルで作成します。

**ステップ 7** Web 認証を伴う URL リダイレクトで使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended REDIRECT-ACL
3850(config-ext-nacl)#deny udp any host 192.168.201.72 eq 53
3850(config-ext-nacl)#deny udp any eq bootpc any eq bootps
3850(config-ext-nacl)#deny ip any host 192.168.201.88
3850(config-ext-nacl)#permit ip any any
```

**ステップ 8** 認証の前にインターフェイスに対する初期 ACL として使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended DEFAULT-ACL
3850(config-ext-nacl)#permit udp any host 192.168.201.72 eq 53
3850(config-ext-nacl)#permit udp any eq bootpc any eq bootps
3850(config-ext-nacl)#deny ip any any
```

**ステップ 9** どの RADIUS サーバも到達不能な場合に使用するために、次の ACL を追加します。

```
3850(config)#ip access-list extended PERMIT-ANY
3850(config-ext-nacl)#permit ip any any
```

**ステップ 10** どの RADIUS サーバも到達不能な場合に使用するために、「CRITICAL」という名前の次のサービス テンプレートを追加します。

```
3850(config)#service-template CRITICAL
3850(config-service-template)#description Apply When none of the RADIUS servers are reachable
3850(config-service-template)#access-group PERMIT-ANY
```

注: サービス テンプレートは、ダウンロード可能 ACL (dACL) と同じように ISE に一元的に配置して認可時にダウンロードできますが、上記のテンプレートの目的はどの ISE ノードも使用可能でないときに使用することであり、つまりサービス テンプレートをダウンロードする手段がないため、ここではローカル サービス テンプレートを作成しています。

## 手順 9 グローバル 802.1X コマンドを設定する

ステップ 11 スイッチの 802.1X をグローバルに有効にします。

802.1X をグローバルに有効にしても、実際にはどの WLAN やインターフェイスでも認証は有効になりません。

```
3850 (config) #dot1x system-auth-control
```

ステップ 12 ダウンロード可能 ACL を有効にして、機能するようにします。

ダウンロード可能アクセスコントロールリスト (dACL) は、Cisco ISE 導入環境における非常に一般的な適用メカニズムです。dACL がスイッチで正しく機能するには、次のようにして IP デバイスのトラッキングをグローバルに有効にする必要があります。

```
3850 (config) #ip device tracking
```

注: Windows 7 では、まれにデバイスが ARP に応答しない場合があります。その場合は、`ip device tracking use SVI` コマンドを使用する必要があります。

## 手順 10 制御クラスを設定する

制御クラスは、制御ポリシーのアクションを実行する条件を定義します。制御ポリシーのアクションを実行するためには、条件のすべてが true と評価される、いずれかが true と評価される、あるいはいずれも true と評価されない、のいずれかを定義します。制御クラスは、制御ポリシーで指定されたイベントに基づいて評価されます。

注: このスイッチで C3PL タイプのコマンドを使用するのが今回初めての場合は、スイッチの設定を消去しない限りレガシー モードに戻れないことを示す警告が表示されます。

ステップ 3 どの RADIUS サーバも使用できない場合の制御クラスを設定します。

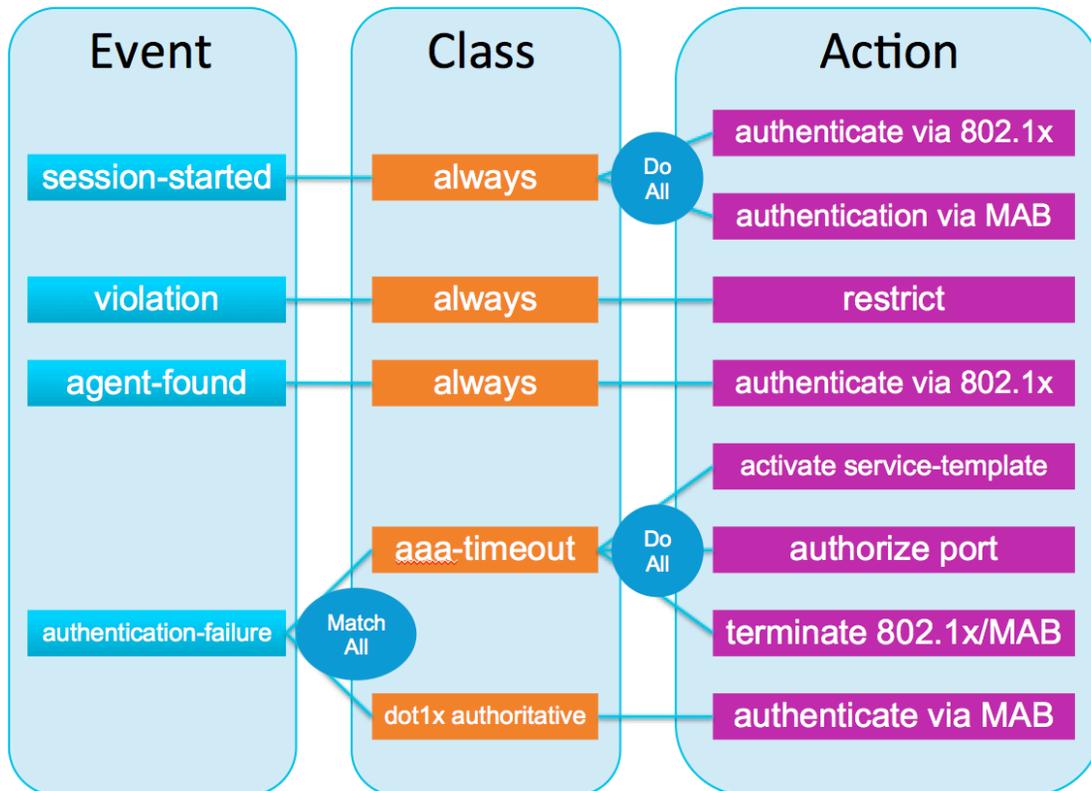
```
3850 (config) #class-map type control subscriber match-any AAA-DOWN
3850 (config-filter-control-classmap) #match result-type aaa-timeout
```

ステップ 4 セッションの 802.1X 認証が失敗した場合の制御クラスを設定します。

```
3850 (config) #class-map type control subscriber match-all DOT1X-FAILED
3850 (config-filter-control-classmap) #match method dot1x
3850 (config-filter-control-classmap) #match result-type method dot1x authoritative
```

## 手順 11 制御ポリシーを設定する

制御ポリシーは、指定されたイベントと条件に対応してシステムが実行するアクションを決定します。これには、制御クラスを1つ以上のアクションに関連付ける1つ以上の制御ポリシールールが含まれます。ポリシールールで設定できるアクションは、指定するイベントのタイプに応じて異なります。制御ポリシーは、一般に加入者IDの認証およびセッションでのサービスのアクティブ化を制御し、インターフェイスに適用されます。次の図は、制御ポリシーに含まれるイベント、クラス、およびアクションの関係を示しています。



ここでは、前の項で作成した制御クラスを使用して制御ポリシーを作成し、最後にそれを一連のインターフェイスに適用します。

ステップ 6 すべての 802.1X/MAB 対応インターフェイスに適用される制御ポリシーを設定します。

```
3850(config-service-template)#policy-map type control subscriber DOT1X-DEFAULT
```

ステップ 7 セッション開始時のアクションを設定します。

次の設定によって、802.1X と MAB を同時に実行できるようになります。

```
3850(config-event-control-policymap)#event session-started match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 authenticate using dot1x priority 10
3850(config-action-control-policymap)#20 authenticate using mab priority 20
```

### ステップ 8 ポリシー違反が発生した場合のアクションを設定します。

違反が発生した場合は、次の設定によって既存のセッションがそのまま維持され、違反イベントがログに記録されます。

```
3850(config-action-control-policymap)#event violation match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 restrict
```

### ステップ 9 エンドポイントでサブリカントが検出されると、スイッチは 802.1X を使用してエンドポイントを認証しようとします。

```
3850(config-action-control-policymap)#event agent-found match-all
3850(config-class-control-policymap)#10 class always do-all
3850(config-action-control-policymap)#10 authenticate using dot1x
```

### ステップ 10 使用可能な RADIUS サーバの不在または認証の失敗が原因となって 802.1X 認証が失敗した場合のアクションを設定します。

これは 2 つの部分に分かれます。1 つ目の失敗は、認証要求を処理するために使用できる RADIUS サーバが存在しない場合です。この場合は、ポリシーによって「CRITICAL」という名前のローカル サービス テンプレートがアクティブ化され、permit-all ACL と、必要に応じて特定の VLAN が適用されます。2 つ目の失敗は、802.1X の認証が失敗した場合であり、この場合は MAB が実行されます。

```
3850(config-action-control-policymap)#event authentication-failure match-all
3850(config-class-control-policymap)#10 class AAA-DOWN do-all
3850(config-action-control-policymap)#10 authorize
3850(config-action-control-policymap)#20 activate service-template CRITICAL
3850(config-action-control-policymap)#30 terminate dot1x
3850(config-action-control-policymap)#40 terminate mab
3850(config-action-control-policymap)#20 class DOT1X-FAILED do-all
3850(config-action-control-policymap)#10 authenticate using mab
```

---

注:ここでは未知の MAC アドレスに対しても ACCESS-ACCEPT を送信する中央 WebAuth が使用されるため、MAB の失敗は発生しません。このため、上記の設定では MAB の失敗イベントを定義していません。

---

## 手順 12 インターフェイスへの制御ポリシーの適用

### ステップ 3 インターフェイスの範囲に対して制御ポリシーを適用します。

```
3850(config)#interface range gigabitEthernet 1/0/1 - 48
3850(config-if-range)#description DOT1X Enabled Ports
3850(config-if-range)#switchport mode access
3850(config-if-range)#service-policy type control subscriber DOT1X-DEFAULT
```

#### ステップ 4 残りのインターフェイスに特定の 802.1X 設定を適用します。

802.1X 設定の多くの部分は C3PL 形式に組み込まれていますが、引き続きレガシー形式を使用するいくつかのコマンドは個別に入力する必要があります。

```
3850(config-if-range)#spanning-tree portfast
3850(config-if-range)#authentication periodic
3850(config-if-range)#authentication timer reauthenticate server
3850(config-if-range)#mab
3850(config-if-range)#ip access-group DEFAULT-ACL in
3850(config-if-range)#access-session host-mode multi-auth
3850(config-if-range)#no access-session closed
3850(config-if-range)#dot1x timeout tx-period 10
3850(config-if-range)#access-session port-control auto
3850(config-if-range)#no shutdown
```

## 3850 の設定例

```
hostname 3850
!
aaa new-model
aaa session-id common
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting dot1x default start-stop group radius
aaa accounting update periodic 15
!
aaa server radius dynamic-author
 client 192.168.201.88 server-key Cisco123
 auth-type any
!
vlan 10
 name USER
vlan 11
 name VOICE
!
interface vlan 10
 ip address 192.168.10.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
interface vlan 11
 ip address 192.168.11.1
 ip helper 192.168.201.72
 ip helper 192.168.201.88
 no shut
!
ip device tracking
!
ip domain-name example.com
!
crypto key generate rsa general-keys modulus 2048
!
dot1x system-auth-control
!
ip http serverw
ip http secure-server
ip http secure-active-session-modules none
ip http active-session-modules none
!
ip access-list extended DEFAULT-ACL
 permit udp any host 192.168.201.72 eq domain
 permit udp any eq bootpc any eq bootps
 deny ip any any
ip access-list extended PERMIT-ANY
 permit ip any any
ip access-list extended REDIRECT-ACL
 deny udp any host 192.168.201.72 eq domain
 deny udp any eq bootpc any eq bootps
 deny ip any host 192.168.201.88
 permit ip any any
!
service-template CRITICAL
 description Apply When none of the RADIUS servers are reachable
 access-group PERMIT-ANY
!
class-map type control subscriber match-any AAA-DOWN
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X-FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
policy-map type control subscriber DOT1X-DEFAULT
 event session-started match-all
```

```
10 class always do-all
 10 authenticate using dot1x priority 10
 20 authenticate using mab priority 20
event violation match-all
10 class always do-all
 10 restrict
event agent-found match-all
10 class always do-all
 10 authenticate using dot1x
event authentication-failure match-all
10 class AAA-DOWN do-all
 10 authorize
 20 activate service-template CRITICAL
 30 terminate dot1x
 40 terminate mab
20 class DOT1X-FAILED do-all
 10 authenticate using mab
!
ip radius source-interface Vlan201
snmp-server community cisco123 RO
radius-server attribute 6 on-for-login-auth
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 10 tries 3
radius-server host 192.168.201.88 auth-port 1812 acct-port 1813 test username radius-test idle-
time 5 key cisco123
radius-server deadtime 15
!
interface GigabitEthernet x/y/z
description DOT1X Enabled Ports
switchport access vlan 30
switchport mode access
ip access-group DEFAULT-ACL in
authentication periodic
authentication timer reauthenticate server
mab
dot1x pae authenticator
dot1x timeout tx-period 10
spanning-tree portfast
service-policy type control subscriber DOT1X-DEFAULT
access-session port-control auto
no shutdown
!
```

## ISE の設定

ISE 1.2 では、サービス テンプレートを設定し、それを認可時に 3850 スイッチに適用できます。サービス テンプレートは、エンドポイントが 802.1X、MAB、WebAuth、または CoA で認証された後の認可の一部として適用できる VLAN、ACL、URL リダイレクト ACL などの認可の集まりです。サービス テンプレートは、ISE だけでなく、スイッチ上でローカルに設定することもできます。ISE のサービス テンプレートが認可の一部として適用されるときに、そのサービス テンプレートがスイッチ上に存在しない場合は、スイッチが ISE からサービス テンプレートを取得します。この操作は、IOS プラットフォームと ISE との間における dACL の動作に似ています。ISE が 3850 スイッチと統合するための設定は、サービス テンプレート以外に存在しません。このドキュメントでは BYOD に関するポリシーについて説明しますが、基盤となるサービスで BYOD を有効にするための設定については、BYOD のハウツー ガイドを参照してください。これには、CA サーバ、外部 ID ソース、およびサブリカント プロビジョニング ポリシーの設定が含まれます。

### 手順 13 アイデンティティシーケンスを作成する

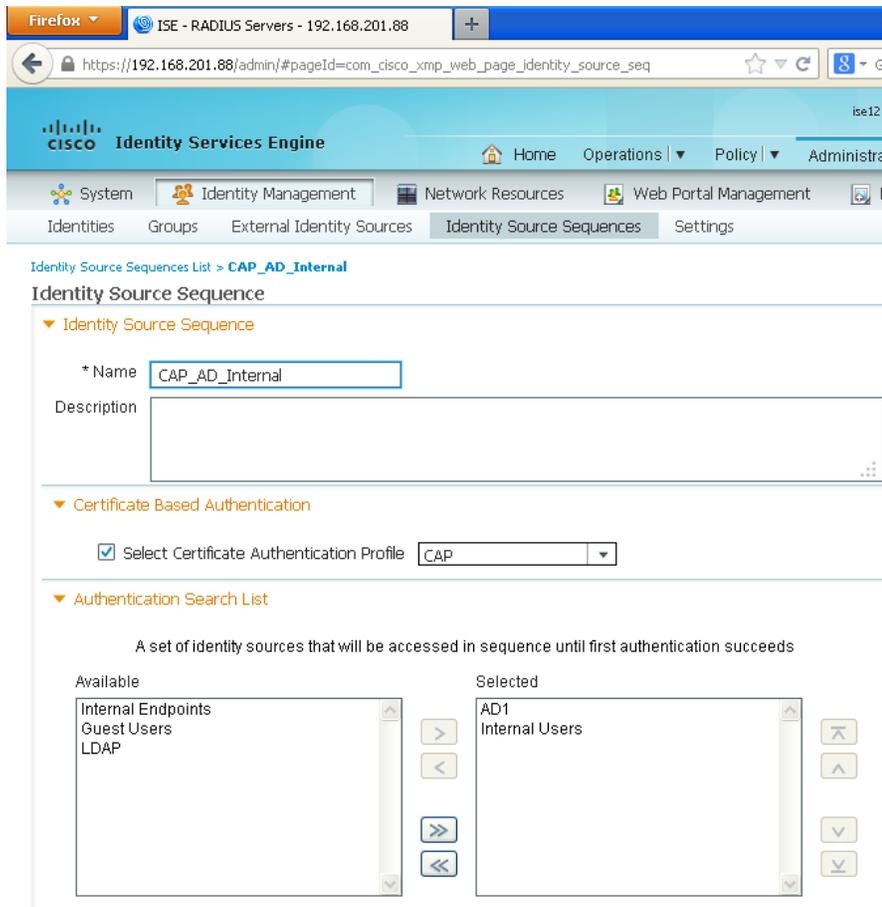
ここでは、スイッチからの認証要求を処理するアイデンティティシーケンスを作成します。このシーケンスによって、証明書、AD、または内部ユーザ データベースを使用してエンドポイントが認証されます。

ステップ 6 ISE プライマリ管理ノードにログインします。

ステップ 7 [管理 (Administration)] → [ID の管理 (Identity Management)] → [ID ソース 順序 (Identity Source Sequences)] に移動します。

ステップ 8 [追加 (Add)] をクリックします。

ステップ 9 「CAP\_AD\_Internal」という名前のシーケンスを作成します。



The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The browser address bar indicates the URL is `https://192.168.201.88/admin/#pageId=com_cisco_xmp_web_page_identity_source_seq`. The page title is "Identity Source Sequence List > CAP\_AD\_Internal". The main content area is titled "Identity Source Sequence" and contains the following configuration fields:

- \* Name:** CAP\_AD\_Internal
- Description:** (Empty text area)
- Certificate Based Authentication:**  Select Certificate Authentication Profile: CAP
- Authentication Search List:** A set of identity sources that will be accessed in sequence until first authentication succeeds. This section contains two lists: "Available" (Internal Endpoints, Guest Users, LDAP) and "Selected" (AD1, Internal Users). Navigation buttons (left, right, double left, double right) are present between the lists.

ステップ 10 [保存(Save)] をクリックします。

## 手順 14 ユーザグループを作成してユーザを割り当てる

この例では、請負業者ユーザは ISE の内部データベースを使用して認証され、従業員ユーザは証明書または AD ユーザアカウントを使用して認証されます。請負業者ユーザ用の ISE ユーザグループを作成します。

ステップ 8 [管理(Administration)] → [IDの管理(Identity Management)] → [グループ(Groups)] → [ユーザIDグループ(User Identity Groups)] に移動します。

ステップ 9 [追加(Add)] をクリックします。

ステップ 10 グループ名として「Contractor」を入力し、[送信(Submit)] をクリックします。

ステップ 11 [管理(Administration)] → [IDの管理(Identity Management)] → [ID(Identities)] → [ユーザ(Users)] に移動します。

ステップ 12 [追加(Add)] をクリックします。

ステップ 13 ユーザ名として「contractor1」を入力し、パスワードを入力します。

ステップ 14 ユーザグループとして [Contractor] を選択し、[送信(Submit)] をクリックします。

### 手順 15 ポリシー セットを有効にする

管理者は、ISE 1.2 のポリシー セット機能を使用して複雑なアイデンティティ ポリシーを作成できます。このドキュメントでは、各 WLAN にマッピングする 2 つのポリシー セットを作成し、各ポリシー セット内で基礎となるポリシーを作成します。これにより、ISE のポリシー 構造によって個々の使用事例にどのようにポリシーが適用されるかが明確になります。

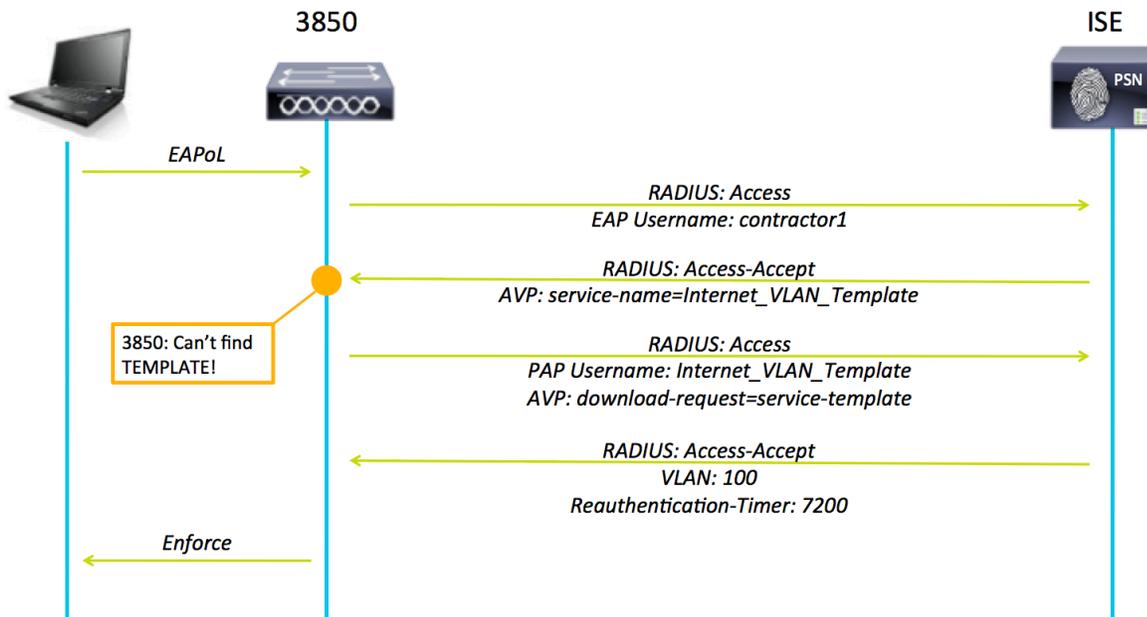
ステップ 3 ポリシー セット機能を有効にするには、[管理 (Administration)] → [システム (System)] → [設定 (Settings)] → [ポリシー セット (Policy Sets)] に移動します。

ステップ 4 [有効 (Enabled)] を選択して [保存 (Save)] をクリックします。

注: ポリシー セット機能を有効にした後でクラシック モードに戻す場合は、ポリシーを作成し直す必要があります。ただし、この機能を有効にすると、初期ポリシーがデフォルトのポリシー セットにコピーされます。

### 手順 16 認可プロファイルを設定する

ここでは、2 つの認可プロファイルを作成します。1 つ目は通常の認可プロファイルで、認証の成功時に dACL のフルアクセス許可をそのインターフェイス用にスイッチにプッシュします。2 つ目の認可プロファイルは、請負業者ユーザに対して使用され、一連の認可属性を含むサービス テンプレートをプッシュします。実際のテンプレートは ISE に配置されるため、スイッチは最初のユーザ認証後にテンプレートの内容をダウンロードするための別の要求を送信します。サービス テンプレートの操作を示す次の図を参照してください。



ステップ 6 [ポリシー (Policy)] → [ポリシー要素 (Policy Elements)] → [許可 (Authorization)] → [許可プロファイル (Authorization Profiles)] に移動します。

ステップ 7 [追加 (Add)] をクリックし、次のパラメータを指定して Permit\_ACL 認可プロファイルを作成します。

| 名前                 | Permit_ACL         |
|--------------------|--------------------|
| 一般的なタスク            | DACL 名 (DACL Name) |
| DACL 名 (DACL Name) | PERMIT_ALL_TRAFFIC |

ステップ 8 [保存 (Save)] をクリックします。

ステップ 9 [追加 (Add)] をクリックし、次のパラメータを指定して Internet\_VLAN\_Template プロファイルを作成します。

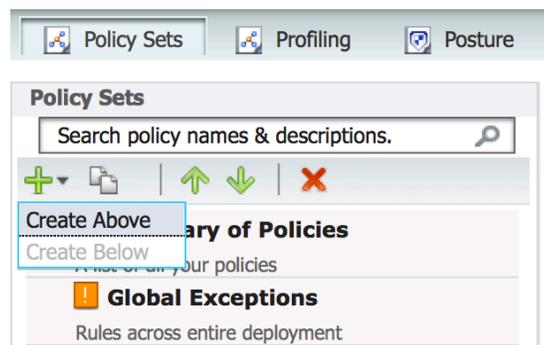
| 名前                                          | Internet_VLAN_Template |
|---------------------------------------------|------------------------|
| サービス テンプレート (Service Template)              | オン                     |
| 一般的なタスク                                     | VLAN                   |
| VLAN                                        | 40                     |
| RADIUS:セッションタイムアウト (RADIUS:Session-Timeout) | 7200                   |

ステップ 10 [保存 (Save)] をクリックします。

## 手順 17 ポリシーを設定する

ステップ 5 [ポリシー (Policy)] → [ポリシーセット (Policy Set)] に移動します。

ステップ 6 左ペインの [+] 記号をクリックし、[上を作成 (Create Above)] をクリックします。



ステップ 7 名前を「DOT1X」とし、次のパラメータを指定してポリシー セットを定義します。

| Status                              | Name  | Description | Conditions   |
|-------------------------------------|-------|-------------|--------------|
| <input checked="" type="checkbox"/> | DOT1X |             | Wired_802.1X |

▼ Authentication Policy

|                                     |                            |                                            |                           |
|-------------------------------------|----------------------------|--------------------------------------------|---------------------------|
| <input checked="" type="checkbox"/> | Default Rule (If no match) | : Allow Protocols : Default Network Access | and use : CAP_AD_Internal |
|-------------------------------------|----------------------------|--------------------------------------------|---------------------------|

▼ Authorization Policy

| Status                              | Rule Name  | Conditions (identity groups and other conditions)           | Permissions                 |
|-------------------------------------|------------|-------------------------------------------------------------|-----------------------------|
| <input checked="" type="checkbox"/> | Employee   | if AD1:ExternalGroups EQUALS example.com/Users/Domain Users | then PermitAccess           |
| <input checked="" type="checkbox"/> | Contractor | if Contractor                                               | then Internet_VLAN_Template |
| <input checked="" type="checkbox"/> | Default    | if no matches, then                                         | DenyAccess                  |

ステップ 8 [送信 (Submit)] をクリックします。

### 手順 18 RADIUS テスト メッセージを抑制するように ISE を設定する

収集フィルタを設定して、モニタリング サーバおよび外部サーバに送信される syslog メッセージを抑制できます。抑制は、異なる属性タイプに基づいてポリシー サービス ノード レベルで実行できます。抑制を無効にすることもできます。特定の属性タイプおよび対応する値を使用して複数のフィルタを定義できます。

注: 収集フィルタの数は 20 個までに制限することを推奨します。

ステップ 9 ISE プライマリ管理ノードにログインします。

ステップ 10 [管理 (Administration)] > [システム (System)] > [ロギング (Logging)] に移動します。

ステップ 11 左ペインの [収集フィルタ (Collection Filters)] をクリックします。

ステップ 12 右ペイン上部の [追加 (Add)] をクリックします。

The screenshot shows the ISE Administration console interface. At the top, there are navigation tabs for System, Identity Management, Network Resources, Web Portal Management, and Feed Service. Below these are sub-tabs for Deployment, Licensing, Certificates, Logging (which is selected), Maintenance, Backup & Restore, Admin Access, and Settings. The main content area is divided into two panes. The left pane shows a 'Logging' sidebar with options like Local Log Settings, Remote Logging Targets, Logging Categories, Message Catalog, Debug Log Configuration, and Collection Filters. The right pane is titled 'Collection Filter List > User Name' and shows a 'Collection Filters' configuration form. The form has three fields: '\* Attribute' set to 'User Name', '\* Value' set to 'radius-test', and '\* Filter Type' set to 'Filter Failed'. There are 'Save' and 'Reset' buttons at the bottom of the form.

ステップ 13 [属性(Attribute)] プルダウン メニューから [ユーザ名 (User Name)] を選択します。

ステップ 14 [値(Value)] に「radius-test」と入力します。

ステップ 15 [フィルタタイプ(Filter Type)] プルダウン メニューから [すべてフィルタ(Filter All)] を選択します。

ステップ 16 [保存(Save)] をクリックします。

## 検証

### 手順 19 従業員デバイスを認証する

ADドメインの一部である Windows PC が接続すると、ISE はそのデバイスを認証し、インターフェイスに対して認可します。「show access-session interface」コマンドを使用して、インターフェイス上の認証および認可情報を検証できます。

```
3850#show access-session interface GigabitEthernet 1/0/1 detail
 Interface: GigabitEthernet1/0/1
 IIF-ID: 0x106E04000000085
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.30.100
 User-Name: host/winxp.example.com
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: N/A
 Common Session ID: C0A8C9FE00000FB30B2FC0AA
 Acct Session ID: 0x0000FAA
 Handle: 0x23000003
 Current Policy: DOT1X-DEFAULT

Server Policies:

Method status list:
 Method State
 dot1x Authc Success
 mab Authc Failed

3850#
3850#
```

## 手順 20 請負業者デバイスを認証する

請負業者アカウントを含むデバイスが接続すると、ISE はサービス テンプレートを使用してそのデバイスを認証し、インターフェイスに対して認可します。

```

3850#show access-session interface GigabitEthernet 1/0/1 detail
 Interface: GigabitEthernet1/0/1
 IIF-ID: 0x108F9C000000089
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.40.100
 User-Name: contractor1
 Status: Authorized
 Domain: DATA
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: 7200s (server), Remaining: 7150s
 Timeout action: Reauthenticate
 Common Session ID: COA8C9FE00000FB80B3C89C0
 Acct Session ID: 0x00000FB0
 Handle: 0x92000007
 Current Policy: DOT1X-DEFAULT

Server Policies:
 Template: Internet_VLAN_Template (priority 100)
 Vlan Group: Vlan: 40

Method status list:
 Method State
 dot1x Authc Success
 mab Authc Failed

3850#
3850#

```

また、3850 が ISE のテンプレートの内容を要求したときに、「Internet\_VLAN\_Template」のユーザ名を示すイベントが ISE 内で発生します。

| Time                    | Status | Details | Repeat Count | Identity               | Endpoint ID       | IP Address     | Device Port          | Authorization Profiles |
|-------------------------|--------|---------|--------------|------------------------|-------------------|----------------|----------------------|------------------------|
| 2014-01-16 14:55:18.062 |        |         | 0            | contractor1            | 00:16:D4:2E:E8:BA | 192.168.40.100 |                      |                        |
| 2014-01-16 14:55:08.739 |        |         |              | Internet_VLAN_Template |                   |                |                      |                        |
| 2014-01-16 14:55:08.725 |        |         |              | contractor1            | 00:16:D4:2E:E8:BA | 192.168.30.107 | GigabitEthernet1/0/1 | Internet_VLAN_Tem...   |

## 手順 21 ISE が使用できない間に認証する

ネットワークの停止や ISE ノードのダウンによって ISE が使用できない間にデバイスが接続した場合は、「CRITICAL」という名前のローカル テンプレートが適用されます。このテンプレートには、すべてのネットワーク アクセスを許可する ACL が含まれており、インターフェイスにすでに適用されているスタティック ACL はこの ACL に置き換えられます。

```
3850#show access-session interface GigabitEthernet 1/0/1 detail
Interface: GigabitEthernet1/0/1
 IIF-ID: 0x108C30000000092
 MAC Address: 0016.d42e.e8ba
 IPv6 Address: Unknown
 IPv4 Address: 192.168.30.107
 User-Name: 0016d42ee8ba
 Status: Authorized
 Domain: UNKNOWN
 Oper host mode: multi-auth
 Oper control dir: in
 Session timeout: N/A
 Common Session ID: C0A8C9FE00000FC30F981C6E
 Acct Session ID: 0x00000FC9
 Handle: 0x43000010
 Current Policy: DOT1X-DEFAULT

Local Policies:
 Template: CRITICAL (priority 150)
 Filter-ID: PERMIT-ANY

Method status list:
 Method State
 dot1x Stopped
 mab Stopped

3850#
3850#
```

## Cisco ワイヤレス LAN コントローラの汎用設定

次の項では、Cisco® ワイヤレス LAN コントローラ(WLC)の汎用設定について説明します。これらの推奨設定は、すべての導入環境で使用できるベスト プラクティスとして編集されており、どの導入タイプを選択しても、導入のどの段階でも、一貫して使用できます。

### Cisco WLC の初期設定

#### ワイヤレス LAN コントローラのブートストラップを行う

次の手順では、Cisco ワイヤレス LAN コントローラの初期設定について説明します。

**ステップ 4** WLC のコンソール ポートに接続します。次の設定を参照して、WLC のブートストラップを行います。

```
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:yes
AUTO-INSTALL: process terminated -- no configuration loaded

System Name [Cisco_91:e2:64] (31 characters max):
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): *****
Re-enter Administrative Password : *****

Service Interface IP Address Configuration [static][DHCP]:dhcp

Enable Link Aggregation (LAG) [yes][NO]: no

Management Interface IP Address: 10.1.60.2
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.60.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.100.100

Virtual Gateway IP Address: 192.0.2.1

Mobility/RF Group Name: cts.local

Network Name (SSID): CTS-CORP

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:us

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: yes
```

```
Enter the NTP server's IP address: 10.1.100.100
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset. [yes][NO]: yes
```

**ベストプラクティス:** Cisco WLC の仮想ゲートウェイアドレスを 192.0.2.1 に設定することを推奨します。これは、ドメイン ネーム システム (DNS) でマッピングされる完全修飾ドメイン名 (FQDN) を使用した非ルーテッド IP にする必要があります。この FQDN/IP アドレスを、CA によって生成された証明書に追加する必要があります。これにより、ユーザが WLC の仮想ゲートウェイにリダイレクトされたときに「証明書を信頼できません (untrusted certificate)」のエラーが表示されなくなります。

**ステップ 5** WLC に接続されたポートのスイッチポートを設定します。

```
Disable interface GigabitEthernet2/46
description WLC-5500 connection
ip address 10.1.60.1 255.255.255.0
終了
```

## Cisco WLC の DHCP プロキシ

**ステップ 1** Cisco WLC は、デフォルトで Dynamic Host Configuration Protocol (DHCP) 要求をプロキシするように設定されています。Cisco ISE はエンドポイントを正確にプロファイリングするためにエンドポイントからの DHCP トラフィックを利用しているため、この機能を無効にすることを推奨します。DHCP プロキシ オプションを有効な状態のままにしておくと、Cisco WLC の DHCP 属性が変更されます。その結果、エンドポイントを正確にプロファイリングするのに役立つ貴重な情報が失われます。

**ステップ 2** [コントローラ (Controller)] → [詳細 (Advanced)] → [DHCP] に移動します。

**ステップ 3** [DHCP プロキシを有効にする (Enable DHCP Proxy)] オプションをオフにします (図 1)。

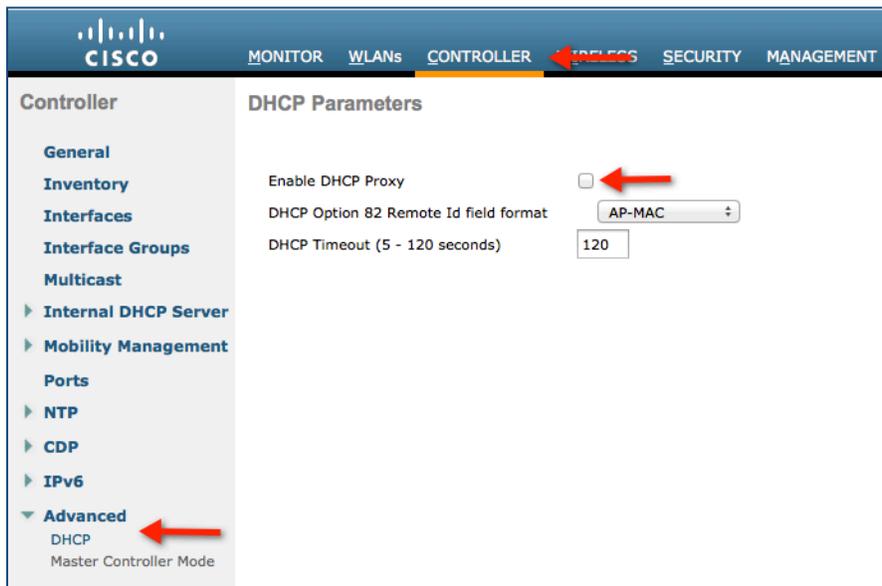


図 2. Cisco WLC の DHCP プロキシを無効化する

## WLC の SNMP を設定する

Cisco ISE は、ワイヤレス ネットワークに接続されたデバイスを識別するため、Simple Network Management Protocol (SNMP) を使用して WLC に特定の属性をクエリします。ここでは、クエリする Cisco ISE の SNMP コミュニティを設定します。

**ステップ 1** [管理 (Management)] → [SNMP] → [一般 (General)] に移動し、SNMPv2 のプロファイリングが有効になっていることを確認します (図 2)。

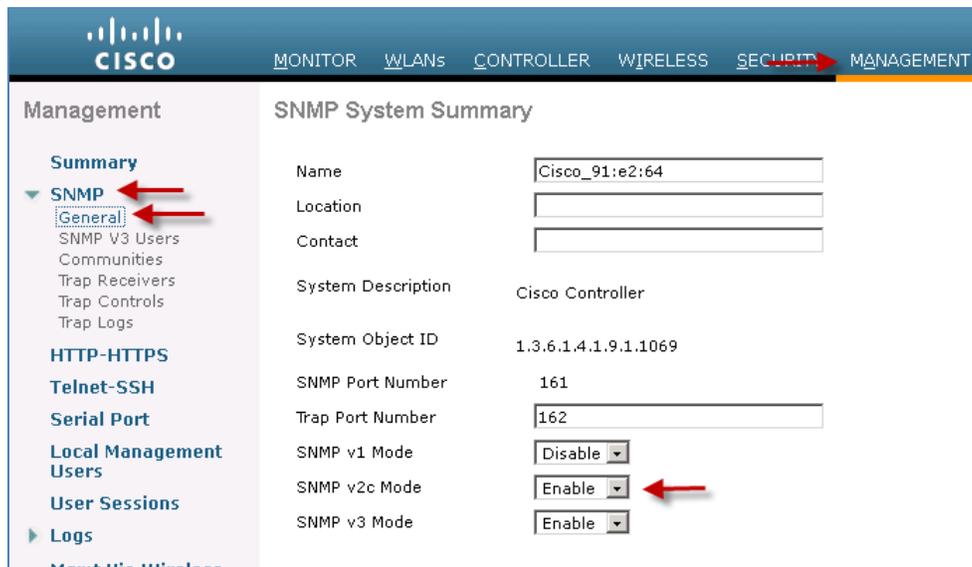


図 3. Cisco WLC の SNMP の設定

**ステップ 2** [コミュニティ (Communities)] をクリックし、表 1 の値を使用して新しいコミュニティを作成します。

**ステップ 3** 完了したら [適用 (Apply)] をクリックします。

表 1. SNMP コミュニティを作成するための値

| 属性 (Attribute)             | 値                    |
|----------------------------|----------------------|
| [コミュニティ名 (Community Name)] | RO                   |
| [IP アドレス (IP Address)]     | 10.1.100.0           |
| IP マスク                     | 255.255.255.0        |
| [アクセス モード (Access Mode)]   | [読み取り専用 (Read only)] |
| ステータス                      | [有効 (Enable)]        |

## Cisco ISE を RADIUS サーバとして使用するよう WLC を設定する

Cisco WLC は、Cisco ISE を RADIUS サーバとして使用します。次の手順では、Cisco ISE を RADIUS サーバとして使用するよう Cisco WLC を設定するプロセスについて説明します。

**ステップ 1** WLC の GUI にアクセスし、[セキュリティ(Security)] → [RADIUS] → [認証(Authentication)] に移動します。

**ステップ 2** [呼出端末 ID タイプ(Call Station ID Type)] を [システム MAC アドレス(System MAC Address)] に設定します(図 3)。

図 1 Cisco WLC の RADIUS サーバの設定



図 4. Cisco WLC の RADIUS サーバの設定

**ステップ 4** [適用(Apply)] をクリックします。

**注:** エンドポイントの IP アドレスではなく MAC アドレスを送信すると、プロファイリング サービス用に設定された Cisco ISE ポリシー サービス ノードに送信される RADIUS パケットがこの MAC アドレスを検出して分類のための属性を取得できるようになります。

**ステップ 5** 右上隅の [新規...(New...)] をクリックして、新しい RADIUS 認証サーバを追加します(図 4)。

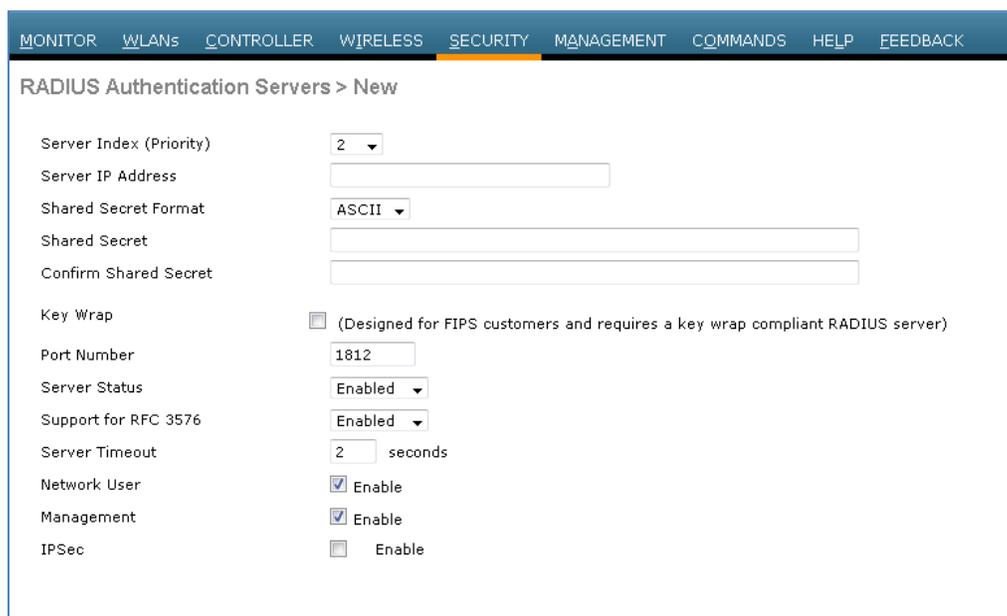
RADIUS 認証サーバの設定を表 2 に一覧表示します。

表 2. RADIUS 認証サーバの設定

| 属性(Attribute)                               | 値          |
|---------------------------------------------|------------|
| [サーバ インデックス(優先順位)(Server Index (Priority))] | 1          |
| サーバの IP アドレス                                | 10.1.100.3 |
| [共有秘密形式(Shared Secret Format)]              | ASCII      |
| [共有秘密鍵(Shared Secret)]                      | Cisco123   |

| 属性 (Attribute)                          | 値                   |
|-----------------------------------------|---------------------|
| [キー ラップ (Key Wrap)]                     | (オフ)                |
| 部品番号                                    | 1812                |
| サーバステータス (Server Status)                | [有効 (Enabled) (オン)] |
| [RFC 3576 のサポート (Support for RFC 3576)] | [有効 (Enabled) (オン)] |
| サーバタイムアウト (Server timeout)              | 2 秒                 |
| [ネットワーク ユーザ (Network User)]             | [有効 (Enabled) (オン)] |
| 管理                                      | [有効 (Enabled) (オン)] |
| IPsec                                   | (オフ)                |

図 2 RADIUS サーバの設定



MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK

RADIUS Authentication Servers > New

Server Index (Priority) 2

Server IP Address

Shared Secret Format ASCII

Shared Secret

Confirm Shared Secret

Key Wrap  (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

Port Number 1812

Server Status Enabled

Support for RFC 3576 Enabled

Server Timeout 2 seconds

Network User  Enable

Management  Enable

IPSec  Enable

図 5. RADIUS サーバの設定

**ステップ 6** [適用 (Apply)] および [設定の保存 (Save Configuration)] をクリックします。

**ステップ 7** [アカウントिंग (Accounting)] > [新規... (New...)] をクリックして、図 5 に示すように RADIUS アカウントिंग サーバを追加します。

RADIUS アカウントिंग サーバの設定を表 3 に一覧表示します。

表 3. RADIUS アカウントिंग サーバの設定

| 属性 (Attribute)                                | 値                   |
|-----------------------------------------------|---------------------|
| [サーバ インデックス (優先順位) (Server Index (Priority))] | 1                   |
| サーバの IP アドレス                                  | 10.1.100.3          |
| [共有秘密形式 (Shared Secret Format)]               | ASCII               |
| 共有秘密鍵 (Shared Secret)                         | Cisco123            |
| 部品番号                                          | 1813                |
| サーバ ステータス (Server Status)                     | [有効 (Enabled) (オン)] |
| サーバ タイムアウト (Server timeout)                   | 30 秒                |
| [ネットワーク ユーザ (Network User)]                   | [有効 (Enabled) (オン)] |
| IPSec                                         | (オフ)                |

| MONITOR                                        | WLANs                                                                                                  | CONTROLLER | WIRELESS | SECURITY | MANAGEMENT | COMMANDS | HELP | FEEDBACK |
|------------------------------------------------|--------------------------------------------------------------------------------------------------------|------------|----------|----------|------------|----------|------|----------|
| <b>RADIUS Authentication Servers &gt; Edit</b> |                                                                                                        |            |          |          |            |          |      |          |
| Server Index                                   | 1                                                                                                      |            |          |          |            |          |      |          |
| Server Address                                 | 10.1.100.3                                                                                             |            |          |          |            |          |      |          |
| Shared Secret Format                           | ASCII ▼                                                                                                |            |          |          |            |          |      |          |
| Shared Secret                                  | ●●●                                                                                                    |            |          |          |            |          |      |          |
| Confirm Shared Secret                          | ●●●                                                                                                    |            |          |          |            |          |      |          |
| Key Wrap                                       | <input type="checkbox"/> (Designed for FIPS customers and requires a key wrap compliant RADIUS server) |            |          |          |            |          |      |          |
| Port Number                                    | 1812                                                                                                   |            |          |          |            |          |      |          |
| Server Status                                  | Enabled ▼                                                                                              |            |          |          |            |          |      |          |
| Support for RFC 3576                           | Enabled ▼                                                                                              |            |          |          |            |          |      |          |
| Server Timeout                                 | 2 seconds                                                                                              |            |          |          |            |          |      |          |
| Network User                                   | <input checked="" type="checkbox"/> Enable                                                             |            |          |          |            |          |      |          |
| Management                                     | <input checked="" type="checkbox"/> Enable                                                             |            |          |          |            |          |      |          |
| IPSec                                          | <input type="checkbox"/> Enable                                                                        |            |          |          |            |          |      |          |

図 6. RADIUS アカウンティング サーバの設定

**ステップ 8** [適用 (Apply)] および [設定の保存 (Save Configuration)] をクリックします。

## RADIUS フォールバック オプションの設定

プライマリ RADIUS サーバ (最も小さいサーバ インデックスを持つサーバ) は、Cisco WLC の最優先サーバであると見なされます。プライマリ サーバが応答しなくなると、コントローラは次にアクティブなバックアップ サーバ (2 番目に小さいサーバ インデックスを持つサーバ) に切り替えます。コントローラは、プライマリ RADIUS サーバが回復して応答可能になるとそのサーバにフォールバックするように設定されているか、使用可能なバックアップ サーバの中からより優先されるサーバにフォールバックするように設定されていない限り、このバックアップ サーバを引き続き使用します。

**ステップ 1** [セキュリティ (Security)] → [AAA] → [RADIUS] → [フォールバック (Fallback)] に移動します。

**ステップ 2** [フォールバックモード (Fallback Mode)] を [アクティブ (Active)] に設定します。

**注:** [アクティブ (Active)] を選択すると、Cisco WLC は RADIUS プロブ メッセージを使用して、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行し、非アクティブとマークされたサーバがオンラインに戻ったかどうかを判断します。コントローラは、すべてのアクティブな RADIUS 要求に対して、非アクティブなすべてのサーバを無視します。[パッシブ (Passive)] を選択すると、Cisco WLC は関係のないプロブ メッセージを使用せずに、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行します。コントローラは、しばらくの間非アクティブなすべてのサーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。

**ステップ 3** [ユーザ名 (Username)] に、非アクティブ サーバ プローブで送信される名前を入力します。

**ステップ 4** [秒 (Sec.)] フィールドに、間隔の値を入力します。

この間隔は、パッシブ モードでの非アクティブ時間、およびアクティブ モードでのプローブ間隔としての意味を持ちます。有効な値の範囲は 180 ~ 3600 秒で、デフォルト値は 300 秒です。

## ポスチャ アセスメント用の Airespace ACL を作成する

ユーザがネットワークに接続すると、そのユーザは最初に検疫状態になります。この段階では、Cisco ISE にアクセスする Cisco Network Access Control (NAC) アプライアンスのエージェントからの DNS とトラフィックだけを許可します。Cisco ISE がポスチャ準拠デバイスを使用するユーザを特定すると、RADIUS 認可変更 (CoA) を使用してユーザが再認証され、ユーザのロールに適したアクセス権がユーザに提供されます。現在の WLC は名前付きの ACL だけをサポートするため、WLC の ACL を事前に定義する必要があります。

この段階でこの ACL をポスチャのリダイレクト用に定義しますが、この ACL はポスチャが有効になる適用モードに移行するまで使用されません。

**注:**ワイヤレス LAN コントローラの ACL は、レイヤ 3 およびレイヤ 4 でポリシーを適用します。Airespace ACL は、最大 64 個のルールをサポートし、インターフェイス単位またはユーザ単位で適用できます。

**ステップ 1** WLC から、[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。[新規 (New)] をクリックします。

**ステップ 2** 図 6 に示すように、ACL 名として **ACL-AGENT-REDIRECT** を使用します。

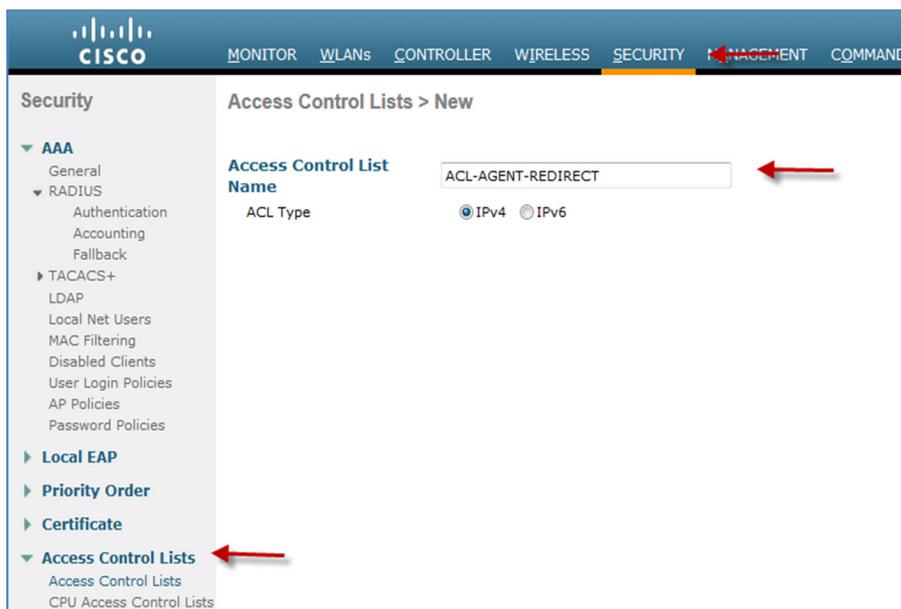


図 7. Cisco WLC への新しい ACL の追加

**注:**ユーザ セッションに適用される ACL は、WLC で事前に定義されている必要があります。Cisco ISE の認可プロファイルで使用される名前は、WLC の ACL 名と正確に一致する必要があります。

**ステップ 3** 図 7 に示すように、[ACL-AGENT-REDIRECT] ACL をクリックします。

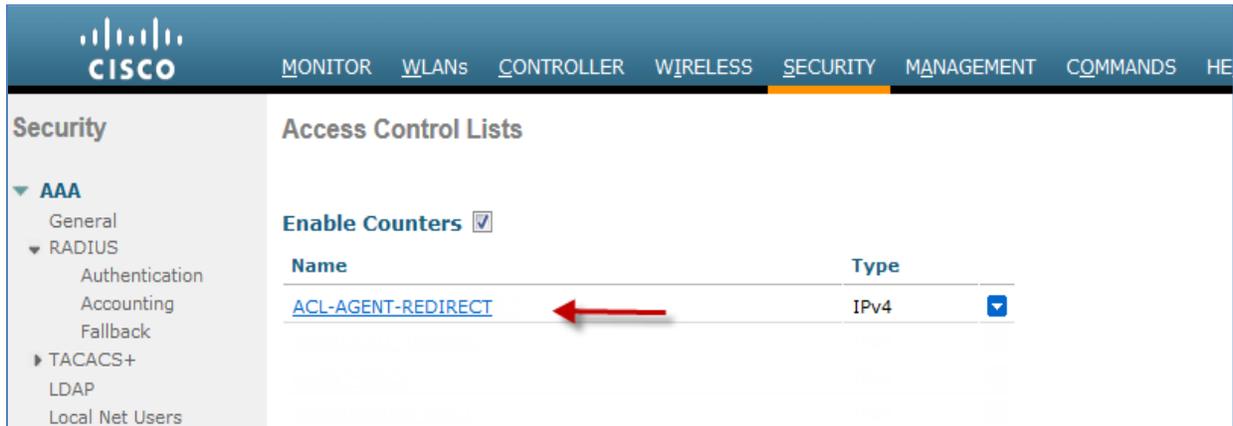


図 8. Cisco WLC の ACL へのルールの追加

**ステップ 4** [新しいルールの追加 (Add New Rule)] をクリックします。図 10 に示す値を使用します。

**ステップ 5** 値のセットごとに [適用 (Apply)] をクリックし、次のルールのために [新しいルールの追加 (Add New Rule)] を選択します。

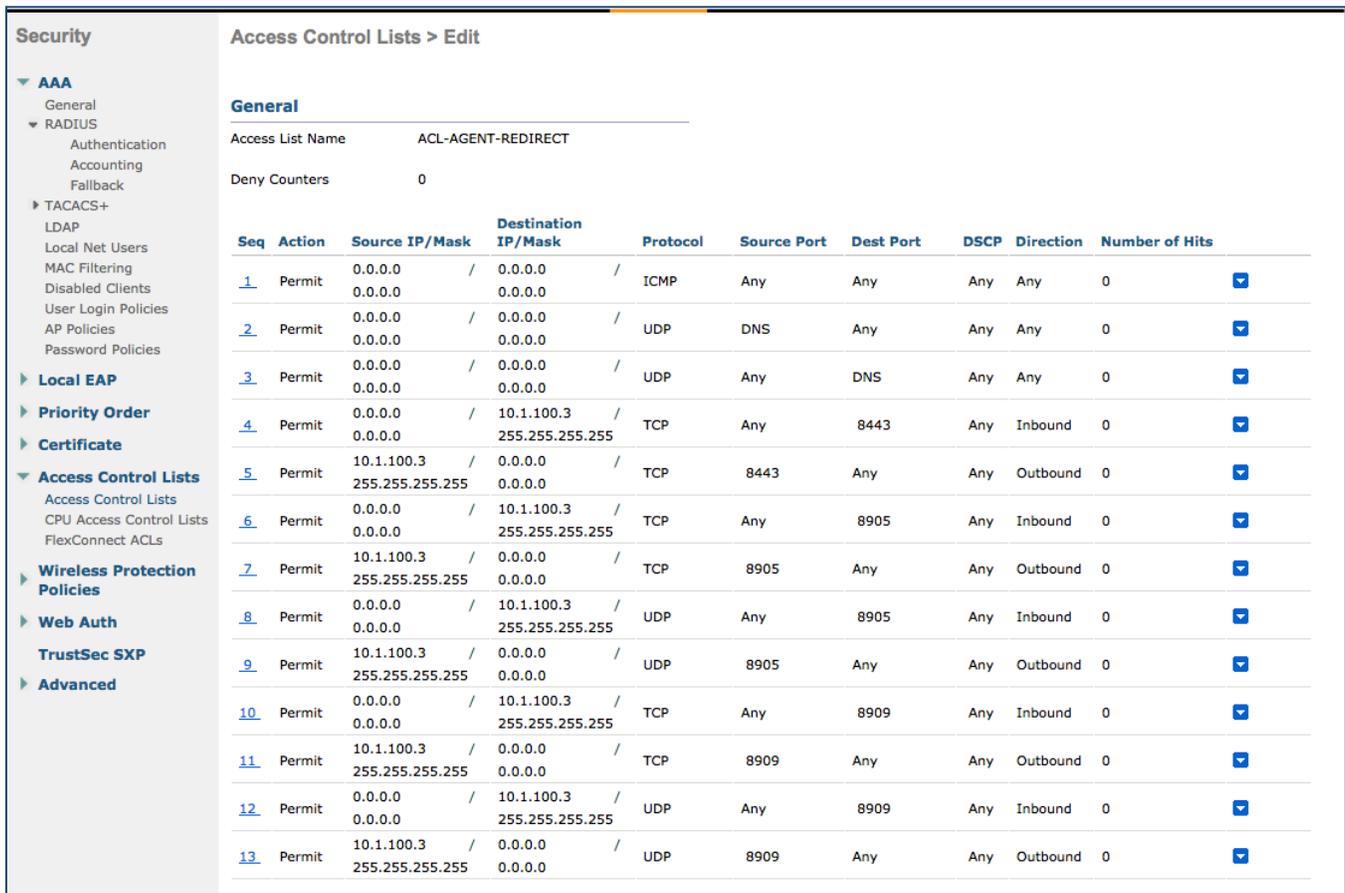


図 9. ACL-AGENT-REDIRECT アクセス リスト

**ステップ 6** ACL が正しく設定されていることを確認します。

**注:** クライアントがプリポスチャ状態 (WLC で定義されている **POSTURE\_REQ**) の場合、WLC のデフォルトの動作では DHCP/DNS 以外のすべてのトラフィックがブロックされます。(Cisco ISE のために受信される **url-redirect-acl** AV ペアで呼び出される) **PRE-POSTURE ACL** がクライアントに適用され、クライアントは ACL で特に許可されているリソースだけに到達できます。

## すべてのトラフィックを許可する Airespace ACL を追加する

すべてのトラフィックを許可する別のアクセスリストも作成します。

**ステップ 1** 「ポスチャアセスメント用の Airespace ACL を作成する」の手順に従って ACL を作成します。

表 4 に、WLC の **ACL-ALLOW** の設定を示します。

**表 4.** ワイヤレス LAN コントローラの ACL-ALLOW の設定

| ACL-ALLOW        |             |
|------------------|-------------|
| 順序 (Sequence)    | 1           |
| ソース (Source)     | 任意 (Any)    |
| 接続先              | 任意 (Any)    |
| プロトコル (Protocol) | 任意 (Any)    |
| DSCP             | 任意 (Any)    |
| 方向 (Direction)   | 任意 (Any)    |
| 操作               | 許可 (Permit) |

## 従業員およびゲスト VLAN 用の動的インターフェイスを作成する

ここでは、ワイヤレス ネットワーク用の 2 つの異なるサービス セット ID (SSID) を作成します。1 つは従業員用で、もう 1 つはゲスト用です。各 SSID は個別の動的インターフェイスにマッピングできます。次の手順では、Cisco WLC の動的インターフェイスを作成するプロセスについて説明します。

**ステップ 1** WLC の GUI から、[コントローラ (Controller)] → [インターフェイス (Interfaces)] に移動し、[新規 (New)] をクリックします (図 9)。

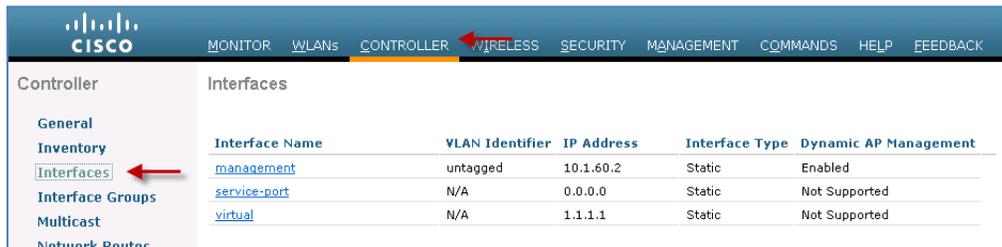


図 10. Cisco WLC への動的インターフェイスの追加

**ステップ 2** 表 5 に示す値を使用して、[適用 (Apply)] をクリックします。

表 5. 従業員用の動的インターフェイスを作成する

| 属性 (Attribute)               | 値        |
|------------------------------|----------|
| [インターフェイス名 (Interface Name)] | Employee |
| [VLAN ID]                    | 10       |

**ステップ 3** 表 6 に示す値を従業員インターフェイス用に入力します。

表 6. 従業員用の動的インターフェイスの設定

| 属性 (Attribute)        | 値             |
|-----------------------|---------------|
| ポート番号                 | 1             |
| [VLAN ID]             | 10            |
| [IPアドレス (IP Address)] | 10.1.10.2     |
| ネットマスク (Netmask)      | 255.255.255.0 |
| ゲートウェイ                | 10.1.10.1     |
| DHCP                  | 10.1.100.100  |

**ステップ 4** 手順を繰り返して、ゲスト用の動的インターフェイスを作成します (表 7 および 8 を参照)。

表 7. ゲスト用の動的インターフェイスを作成する

| 属性 (Attribute)               | 値   |
|------------------------------|-----|
| [インターフェイス名 (Interface Name)] | ゲスト |
| [VLAN ID]                    | 20  |

表 8. ゲスト用の動的インターフェイスの設定

| 属性 (Attribute)        | 値             |
|-----------------------|---------------|
| ポート番号                 | 1             |
| [VLAN ID]             | 20            |
| [IPアドレス (IP Address)] | 10.1.20.2     |
| ネットマスク (Netmask)      | 255.255.255.0 |
| ゲートウェイ                | 10.1.20.1     |
| DHCP                  | 10.1.100.100  |

ステップ 5 設定を保存します (図 10)。

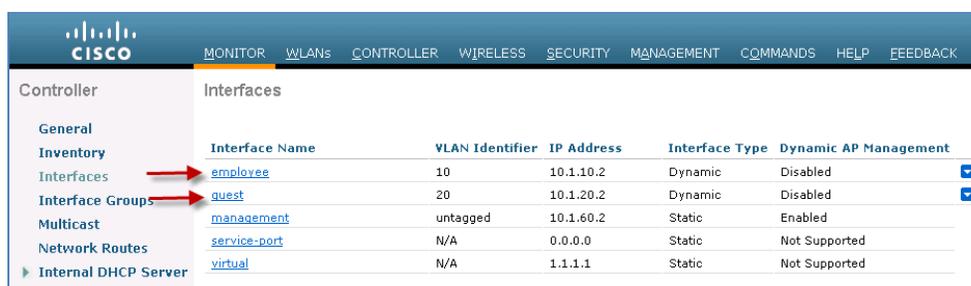


図 11. 動的インターフェイスの設定を確認する

## 802.1X および中央 Web 認証の SSID の追加

### 従業員用の 802.1X WLAN を追加する

次に、適切なセキュリティ設定で SSID を設定し、RADIUS サーバとして定義された Cisco ISE による 802.1X 認証を有効にします。

**ステップ 1** WLC から、[WLAN (WLANs)] → [WLAN ID] に移動して、ブートストラップで定義された SSID を変更します。新しい SSID を定義する場合は、[WLAN (WLANs)] → [新規作成 (Create New)] → [実行 (Go)] をクリックします (図 11)。



図 12. 802.1X WLAN の追加

**ステップ 2** WLAN 設定の [一般 (General)] タブの値を設定します (図 12)。

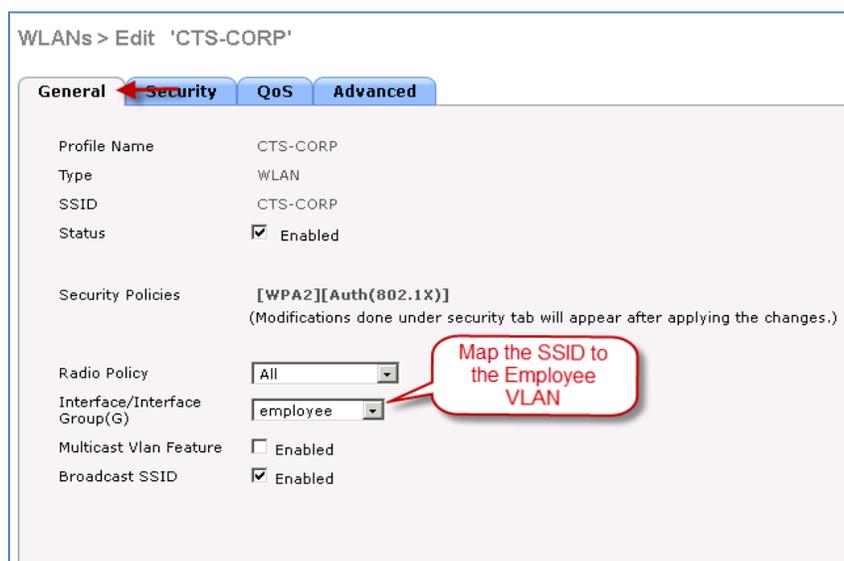


図 13. 802.1X WLAN の [一般 (General)] タブの設定

**ステップ 3** [セキュリティ(Security)] → [レイヤ2(Layer 2)] タブの値を次のように設定します(図 13)。

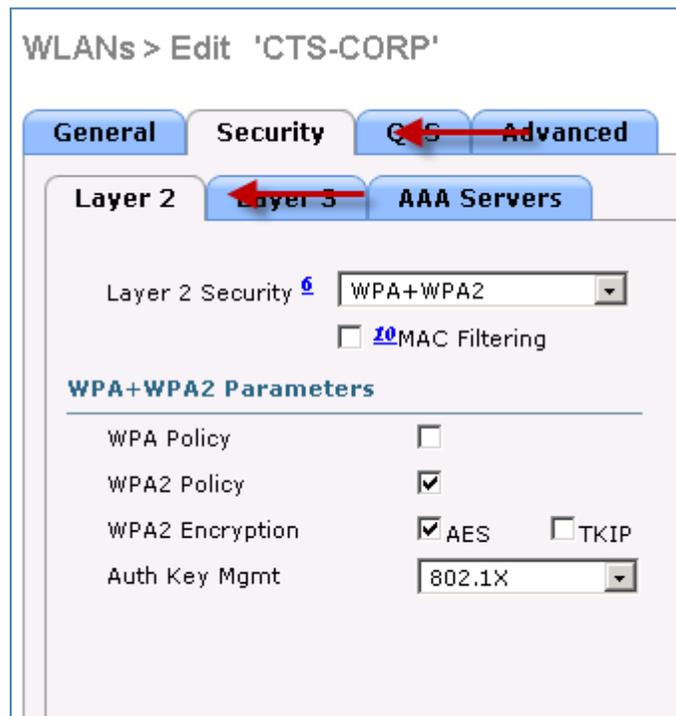


図 14. 802.1X WLAN のレイヤ 2 セキュリティの設定

**ステップ 4** [セキュリティ(Security)] → [AAAサーバ(AAA Servers)] タブの値を次のように設定します(図 14)。

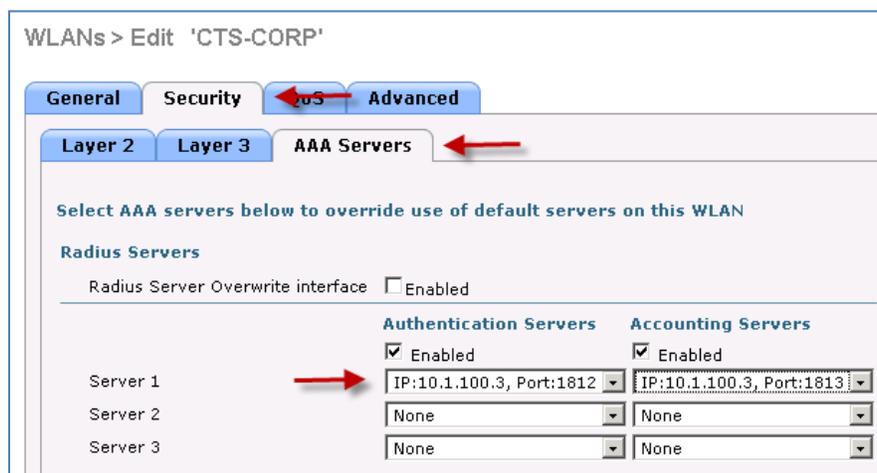
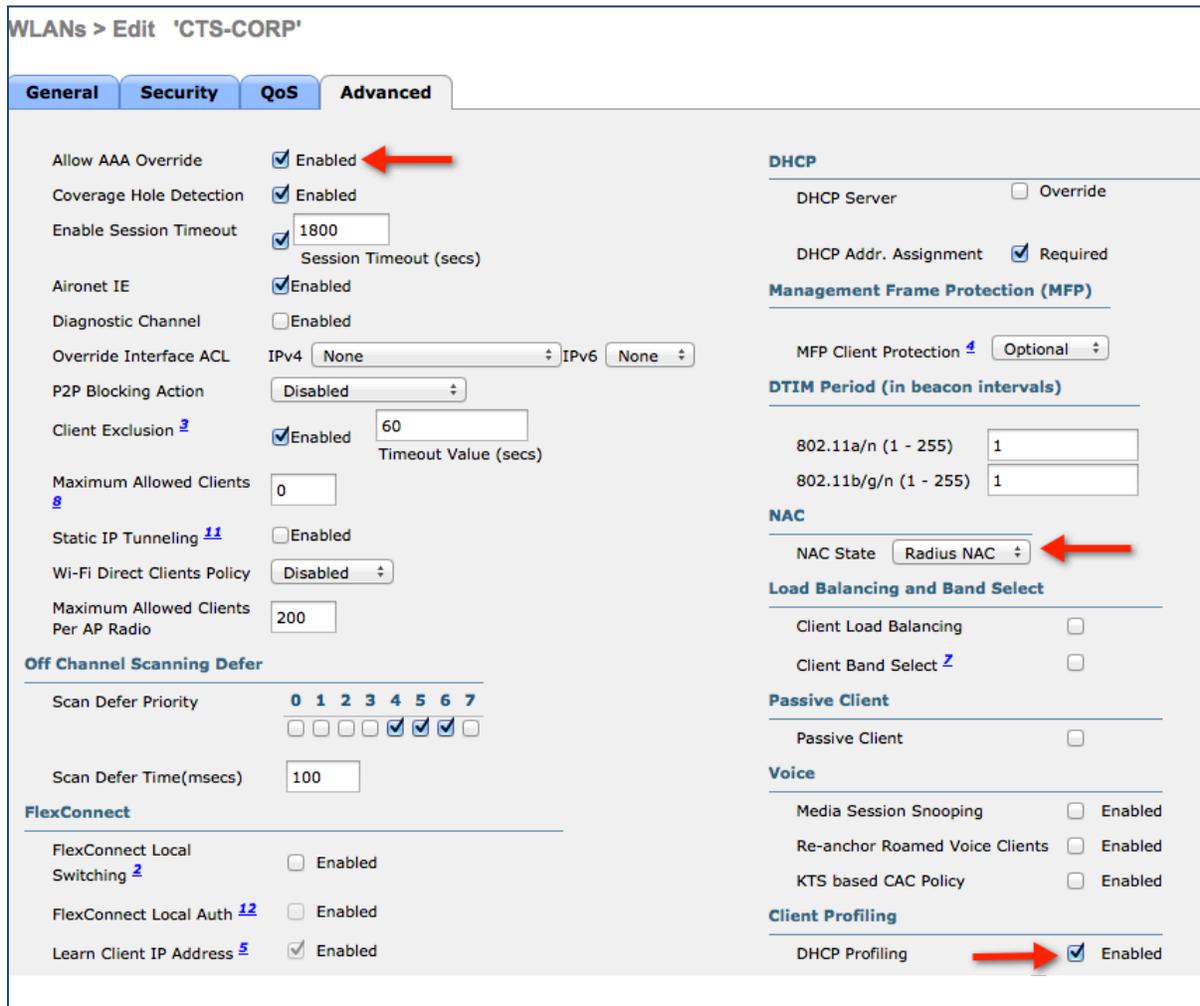


図 15. 802.1X WLAN の RADIUS サーバのマッピング

**ステップ 5** [詳細 (Advanced)] タブの値を設定します (図 15)。



WLANs > Edit 'CTS-CORP'

**General** **Security** **QoS** **Advanced**

Allow AAA Override  Enabled

Coverage Hole Detection  Enabled

Enable Session Timeout  1800  
Session Timeout (secs)

Aironet IE  Enabled

Diagnostic Channel  Enabled

Override Interface ACL IPv4  IPv6

P2P Blocking Action

Client Exclusion  Enabled  
Timeout Value (secs)

Maximum Allowed Clients

Static IP Tunneling  Enabled

Wi-Fi Direct Clients Policy

Maximum Allowed Clients Per AP Radio

**Off Channel Scanning Defer**

Scan Defer Priority  0  1  2  3  4  5  6  7

Scan Defer Time(msecs)

**FlexConnect**

FlexConnect Local Switching  Enabled

FlexConnect Local Auth  Enabled

Learn Client IP Address  Enabled

**DHCP**

DHCP Server  Override

DHCP Addr. Assignment  Required

**Management Frame Protection (MFP)**

MFP Client Protection

**DTIM Period (in beacon intervals)**

802.11a/n (1 - 255)

802.11b/g/n (1 - 255)

**NAC**

NAC State

**Load Balancing and Band Select**

Client Load Balancing

Client Band Select

**Passive Client**

Passive Client

**Voice**

Media Session Snooping  Enabled

Re-anchor Roamed Voice Clients  Enabled

KTS based CAC Policy  Enabled

**Client Profiling**

DHCP Profiling  Enabled

図 16. 802.1X WLAN の詳細設定

**注:** CoA を適用するには、RADIUS NAC の設定が必要です。これはこの段階で定義しますが、WLC にリダイレクトベンダー固有属性 (VS) を送信してプリポストチャアセスメント ACL を起動するように Cisco ISE を設定するまでは有効になりません。

**ステップ 6** [適用 (Apply)] をクリックして WLAN の設定を保存します。

## ワイヤレス中央 Web 認証用のオープン SSID を追加する

この手順では、中央 Web 認証 (CWA) 用の SSID を設定する手順について説明します。

**注:** ワイヤレス中央 Web 認証のサポートは、Cisco ワイヤレス LAN コントローラ ソフトウェア バージョン 7.2 以降でのみ利用可能です。ローカル Web 認証の設定については、『Cisco TrustSec 2.0 Design and Implementation Guide』 ([http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec\\_2.0/trustsec\\_2.0\\_dig.pdf](http://www.cisco.com/en/US/docs/solutions/Enterprise/Security/TrustSec_2.0/trustsec_2.0_dig.pdf)) を参照してください。

**ステップ 1** WLC の GUI から、[WLAN (WLANs)] → [新規作成 (Create New)] → [実行 (Go)] に移動します。

**ステップ 2** 表 9 の値を入力し、[適用 (Apply)] をクリックします。

表 9. 表 9 中央 Web 認証用の SSID の設定

| 属性 (Attribute)         | 値             |
|------------------------|---------------|
| プロファイル名 (Profile Name) | CTS-GUEST-CWA |
| SSID                   | CTS-GUEST-CWA |

ステップ 3 WLAN 設定の [一般 (General)] タブの値を設定します (図 16)。

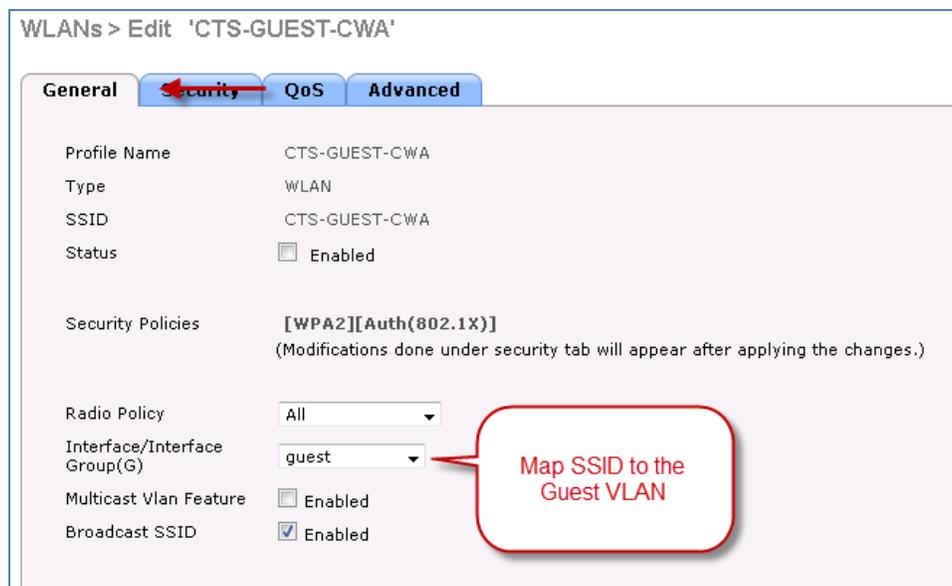


図 17. オープン SSID の [一般 (General)] タブの設定

ステップ 4 [セキュリティ (Security)] の [レイヤ 2 (Layer 2)] タブの値を設定します (図 17)。

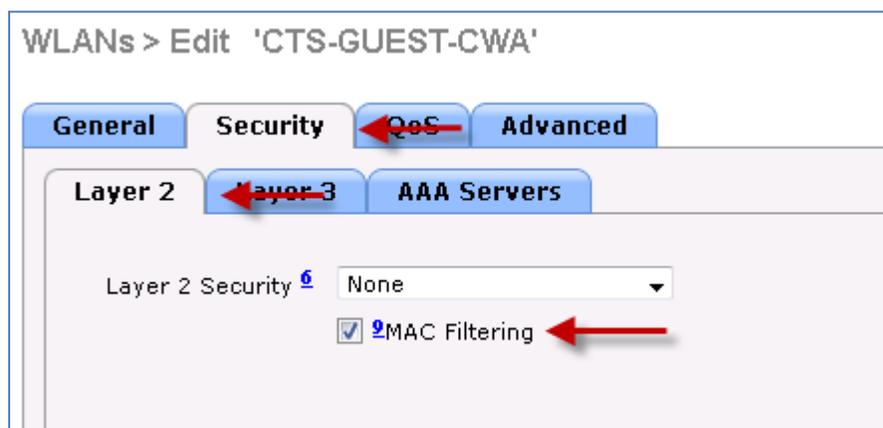


図 18. CWA を使用するオープン SSID のレイヤ 2 セキュリティの設定

**ステップ 5** [セキュリティ(Security)] タブの [AAAサーバ(AAA Servers)] の値を設定します(図 18)。

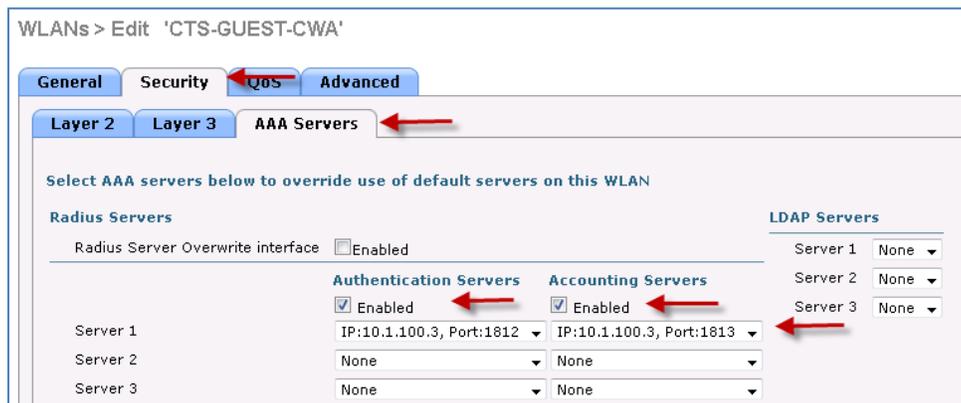


図 19. CWA を使用するオープン SSID の RADIUS サーバのマッピング

**ステップ 6** [詳細(Advanced)] タブの値を設定します(図 19)。

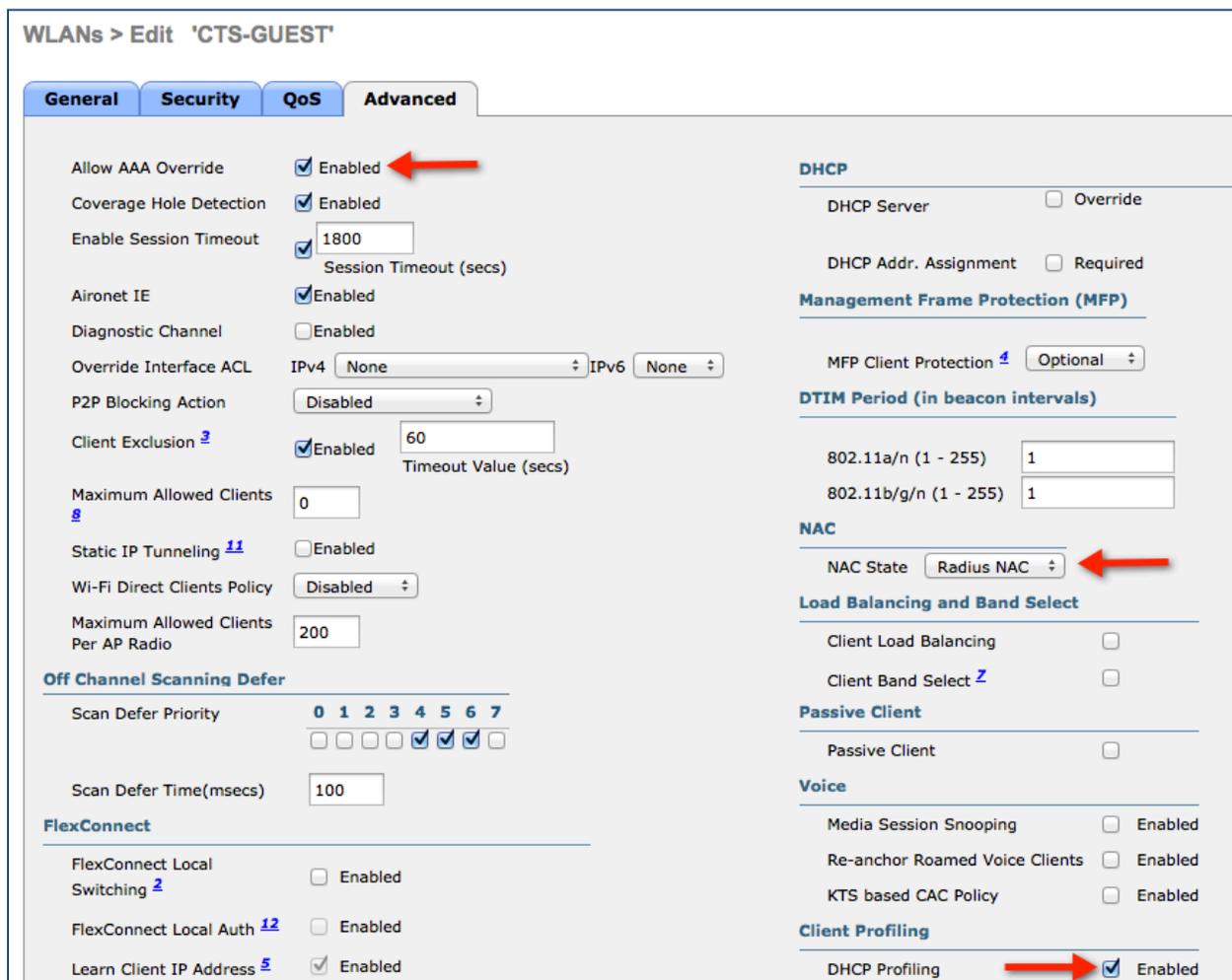


図 20. CWA を使用するオープン SSID の詳細設定

注:AAA サーバの属性を適用できるようにするため、[AAAオーバーライド(AAA Override)] を有効にすることが重要です。

ステップ7 WLC の設定を保存します。

## ワイヤレス認証に関する Cisco ISE の設定

### ワイヤレス認証要求を受け入れるように Cisco ISE を設定します。

Cisco WLC の基本設定が完了しました。次に、Cisco WLC からの RADIUS 要求を処理するように Cisco ISE を設定します。

ステップ1 『ISE Base Configurations: ISE Bootstrapping How-To Guide』に従って、Cisco WLC をネットワーク アクセス デバイスとして Cisco ISE に追加します。

ステップ2 Cisco ISE で、[ポリシー (Policy)] → [認証 (Authentication)] に移動します。

ステップ3 MAB ルールの IF 条件を展開し、[ライブラリから条件を追加する (Add Condition from Library)] を選択します (図 20)。

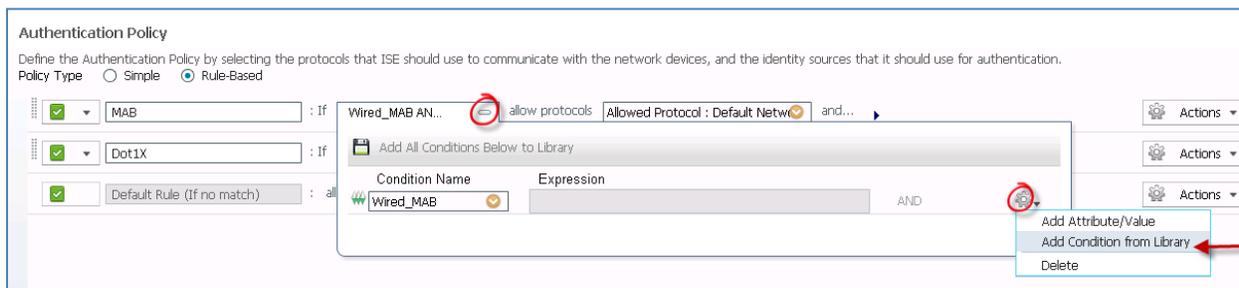


図 21. ISE 認証ルールへの条件の追加

ステップ4 [条件の選択 (Select Condition)] ドロップダウン メニューから、[複合条件 (Compound Condition)] → [Wireless\_MAB] を選択します (図 21)。

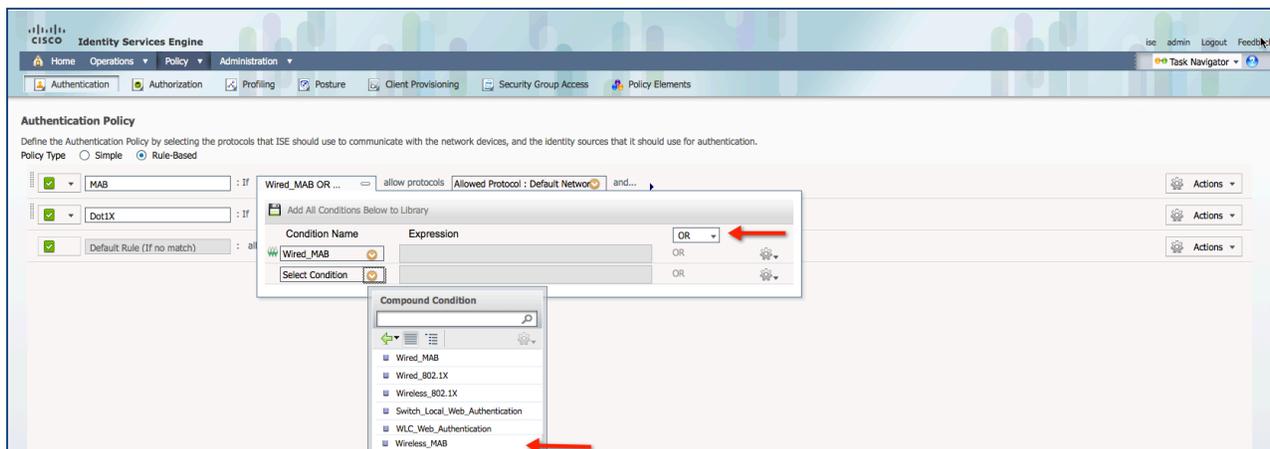


図 22. 認証ルールへの Wireless\_MAB 条件の追加

ステップ5 Dot1X ルールの IF 条件を展開し、[ライブラリから条件を追加する (Add Condition from Library)] を選択します。

**ステップ 6** [条件の選択 (Select Condition)] ドロップダウン メニューから、[複合条件 (Compound Condition)] → [Wireless\_802.1X] を選択します (図 22)。

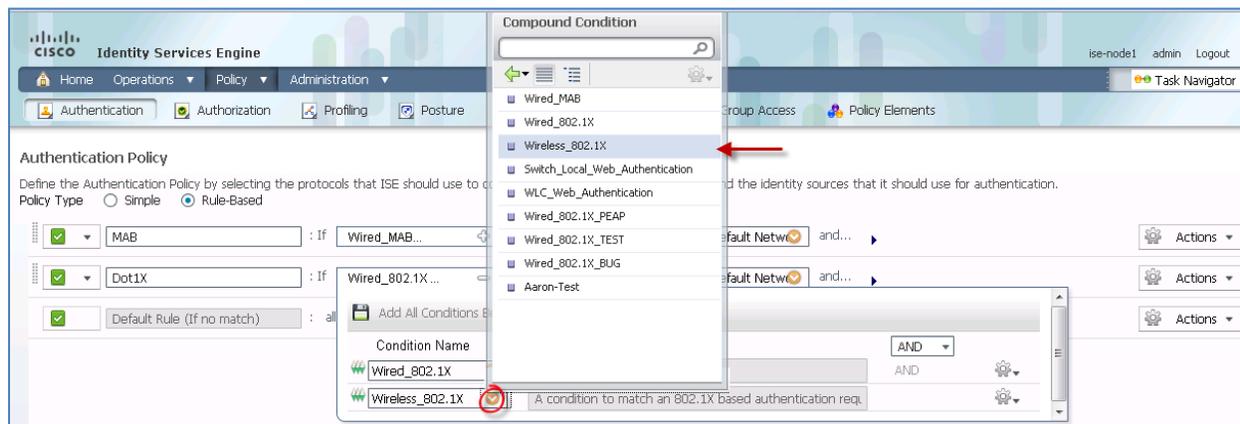


図 23. 認証ルールへの Wireless\_802.1X 条件の追加

**ステップ 7** 設定を保存します。

Cisco ISE がワイヤレス ネットワークから発信された RADIUS 要求を受け入れる準備ができました。Cisco ISE は、ワイヤレスの送信元から RADIUS 要求を受信したときに、認証プロトコルが許可されるかどうかを確認します。通常、デフォルトのネットワーク オプションでは、Cisco ISE でサポートされるすべての認証プロトコルが許可されます。Cisco ISE の次のステップでは、指定された ID ストアを照会して、受信したクレデンシャルを検証します。

## Apple の Captive Network Assistant (CNA)

Apple は、キャプティブ ポータルが存在する場合にネットワーク アクセスを容易にする iOS の機能を導入しました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することによってキャプティブ ポータルの存在を検出し、その要求を <http://www.apple.com/library/test/success.html> に転送します。

応答を受信した場合は、インターネットにアクセスできると見なされ、それ以上の操作は必要ありません。応答を受信しなかった場合は、インターネット アクセスがキャプティブ ポータルによってブロックされたと見なされ、CNA が疑似ブラウザを自動起動して管理ウィンドウでのポータル ログインを要求します。

ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。WLC バージョン 7.2 では、疑似ブラウザを表示しないようにする CLI コマンドが追加されました。

### CNA をバイパスするように WLC を設定する:

#### キャプティブ バイパス CLI を有効にする

**ステップ 1** WLC のコマンドライン インターフェイスにログインします。

**ステップ 2** キャプティブ バイパス コマンドを有効にします。

```
> config network web-auth captive-bypass enable
```

**ステップ 3** コントローラの設定を保存します。

```
> save config
```

**ステップ 4** この変更を適用するには、コントローラを再起動する必要があります。

```
> reset system in 00:01:01
```

## 付録 A: 参考資料

---

### Cisco TrustSec システム:

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

[http://www.cisco.com/en/US/solutions/ns340/ns414/ns742/ns744/landing\\_DesignZone\\_TrustSec.html](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 User Guides:

[http://www.cisco.com/en/US/products/ps11640/products\\_user\\_guide\\_list.html](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 ソフトウェアの各リリースの詳細については、次の URL を参照してください。

Cisco Catalyst 2900 シリーズ スイッチの場合:

[http://www.cisco.com/en/US/products/ps6406/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps6406/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 3000 シリーズ スイッチの場合:

[http://www.cisco.com/en/US/products/ps7077/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps7077/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 3000-X シリーズ スイッチの場合:

[http://www.cisco.com/en/US/products/ps10745/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps10745/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 4500 シリーズ スイッチの場合:

[http://www.cisco.com/en/US/products/hw/switches/ps4324/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps4324/products_installation_and_configuration_guides_list.html)

Cisco Catalyst 6500 シリーズ スイッチの場合:

[http://www.cisco.com/en/US/products/hw/switches/ps708/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/hw/switches/ps708/products_installation_and_configuration_guides_list.html)

Cisco ASR 1000 シリーズ ルータの場合:

[http://www.cisco.com/en/US/products/ps9343/products\\_installation\\_and\\_configuration\\_guides\\_list.html](http://www.cisco.com/en/US/products/ps9343/products_installation_and_configuration_guides_list.html)

Cisco ワイヤレス LAN コントローラの場合:

<http://www.cisco.com/en/US/docs/wireless/controller/7.2/configuration/guide/cg.html>