Application Visibility and Control 機能リリース 7.4 ～ 8.8 導入ガイド

最終更新日:2018 年 7 月

Application Visibility and Control リリースアップデート

特定の AVC 機能に関する情報および設定を取得するには、該当するアップデートフェーズを参照してください。

フェーズ 1:**AVC** 7.4	■ NBAR2 エンジンによる 1039 のアプリケーションの分類および制御。 ■ 16 の AVC プロファイルおよびプロファイルごとの 32 のルールのサポート。 ■ WLAN ごとに 1 つの AVC プロファイルをサポート。同じプロファイルを複数の WLAN でサポートできます。 ■ WLAN にマッピングされた AVC プロファイルには、マークまたはドロップアクションのルールがあります。 ■ 分類されたすべてのアプリケーションをコントローラにグラフィック表示。 ■ WLC で 1 つの NetFlow エクスポータとモニタを設定できます。 ■ PAM ライセンスを使用した PI での AVC NetFlow モニタリング。
フェーズ 2:**AVC** 7.5	■ AVC フェーズ 2 でのプロトコルパック 4.1 のサポート。 ■ その他のアプリケーションのサポート:合計 1056 のアプリケーション ■ プロトコルパックを動的にロードしてアプリケーションを更新するためのサポート。
フェーズ 3:**AVC** 8.0	■ プロトコルパック 9.0 ■ NBAR エンジンリリース 3.1 ■ クライアントの AAA AVC プロファイルオーバーライド。 ■ WLAN でのユーザごとのアプリケーションレート制限。 ■ ユーザおよびデバイスごとの AVC プロファイルとローカルポリシー分類の統合。 ■ アップストリームおよびダウンストリーム トラフィックの AVC 指向性 QoS DSCP マーキング。 ■ 1105 のアプリケーションのサポート。

フェーズ 4：**AVC** 8.2	■ プロトコルパック 14.0 ■ NBAR エンジン 23 ■ 1273 のアプリケーションのサポート ■ サードパーティ製 Netflow コレクタのサポート ■ 2 つのフローコレクタのサポート ■ フローコレクタでの 17 のデータフローレコードのサポート
フェーズ 5：**AVC** 8.3	■ プロトコルパック 19.1 ■ NBAR エンジンバージョン 23 ■ 1317 のアプリケーションのサポート
フェーズ 6：AVC 8.8	■ プロトコルパック 37 ■ NBAR エンジンバージョン 31 ■ 1408 のアプリケーションのサポート ■ デフォルト DSCP 値の拡張 ■ Wi-Fi 通話のサポート **Flex Connect AVC Wave-2 AP** ■ プロトコルパック 37 ■ NBAR2 エンジン 31 ■ 1408 のアプリケーションのサポート ■ デフォルト DSCP 値の拡張 ■ Wi-Fi 通話のサポート

Application Visibility and Control：フェーズ 1

Network Based Application Recognition（NBAR）は、ワイヤレスネットワークでのアプリケーション制御を可能にし、管理性と生産性を向上させます。また、エンドツーエンドのソリューションとして Cisco の Application Visibility and Control（AVC）を拡張します。これにより、ネットワーク内のアプリケーションの完全な可視化が提供され、管理者は同時にアプリケーションの制御もできます。

NBAR は Cisco IOS ベースのプラットフォームで利用できるディープパケット インスペクション テクノロジーで、ステートフル L4 - L7 分類をサポートしています。NBAR2 は NBAR に基づくもので、NBAR を使用するすべての IOS 機能で共通のフローテーブルが必要になるなどの要件があります。NBAR2 がアプリケーションを認識し、その情報を QoS、NetFlow、ファイアウォールなどの他の機能に渡すことで、この分類に基づくアクションが実行されます。

NBAR の主な使用例として、キャパシティプランニング、ネットワーク使用量のベースライン化、および帯域幅を消費するアプリケーションのより的確な把握があります。アプリケーション使用状況の傾向分析により、ネットワーク管理者はネットワーク インフラストラクチャのアップグレードを計画し、ネットワーク輻輳時に帯域幅を大量に消費するアプリケーションから重要なアプリケーションを保護してユーザエクスペリエンスを向上させ、優先順位付けと解除を行い、特定のアプリケーション トラフィックをドロップすることができます。

NBAR は、ローカル、メッシュ、およびフレックスモード AP 上の 2500、5500、7500、8500、WiSM2 シリーズ コントローラでサポートされます（中央スイッチング専用に設定された WLAN の場合）。

NBAR のサポートされる機能

NBAR はその機能として、次のタスクを実行できます。

1. 分類：アプリケーション/プロトコルの識別。
2. AVC：分類されたトラフィックを可視化し、ドロップまたはマーク（DSCP）アクションによってトラフィックを制御するオプションも提供します。
3. NetFlow：Cisco Prime Assurance Manager（PAM）などの NetFlow コレクタに最新の NBAR 統計情報を提供します。

Application Visibility and Control：フェーズ 2

AVC のフェーズ 2 では、プロトコルパックのサポートが追加されました。プロトコルパックは、コントローラ上のイメージを置き換えることなくシグニチャのサポートを更新できるソフトウェアパッケージです。プロトコルパックは、新しいプロトコルサポートが追加されたときに動的にロードできます。プロトコルパックには、メジャーとマイナーの 2 種類があります。

- メジャープロトコルパックには、マイナー プロトコル パック新しいプロトコル、更新プログラム、およびバグフィックスのサポート機能が含まれています。
- 通常、マイナープロトコルパックに新しいプロトコルパックのサポートは含まれていません。
- それぞれのプロトコルパックは、特定のプラットフォームタイプ、ソフトウェアバージョン、リリースが対象になります。プロトコルパックは、CCO からソフトウェアタイプ「NBAR2 Protocol Pack」を使用してダウンロードできます。

特定の NBAR エンジンバージョンのプロトコルパックがリリースされています。たとえば、WLC 7.5 には NBAR エンジン 13 が付属しているため、そのプロトコルパックはエンジン 13 向けに記述されています（pp-unified-wng-152-4.S-13-4.1.1.pack）。プロトコルパックは、プラットフォーム上のエンジンのバージョンが、プロトコルパックで要求されるバージョン以上（上記の例では 13）である場合にロード可能です。したがって、たとえば 3.7（バージョン 13）用の PP4.1 は、3.7（バージョン 13）および 3.8 上にロードできますが、3.8 用の PP4.1 を 3.7 にロードすることはできません。エンジンに完全に一致するプロトコルパックを使用することを強くお勧めします。

AVC フェーズ 2 では、プロトコルパックを CCO から直接ダウンロードできます（エンジン XE 3.7 用のプロトコルパック 4.1.1）。プロトコルパックファイル「pp-AIR-7.5-13-4.1.1.pack」（形式：pp-AIR-{release}-{engine version}-M.m.r.pack）は、コントローラ コード バージョン 7.5 と同じ場所に配置されます。これは、コントローラ ソフトウェア バージョン 7.5 でリリースされている唯一のテスト済みおよびサポート対象プロトコルパックです。

注：ダウンロード用に他のシスコデバイス向けのプロトコルパックが用意されている以下のリンクからプロトコルパックをダウンロードした場合、そのプロトコルパックは機能する可能性はありますが、サポートされません。
https://software.cisco.com/download/home/282600534/type/284509011/release/24.0.0 を参照してください。

リリースでサポートされているプロトコルの完全な一覧は、次のリンクに掲載されています。

http://www.cisco.com/en/US/docs/ios-xml/ios/qos_nbar/prot_lib/config_library/nbar-prot-pack-library.html

注:AVC フェーズ 2 では、ダウンロード可能な NBAR プロトコルパックは、ローカル、メッシュ、およびフレックスモード AP 上の 5500、7500、8500、WiSM2 コントローラでサポートされます（中央スイッチング専用に設定された WLAN の場合）。2500 シリーズ コントローラは、プロトコルパックをサポートしません。

注:AVC フェーズ 6（リリース 8.8）では、3504、5520、および 8540 シリーズのコントローラで最新の NBAR2 とプロトコルパックがサポートされます。リリース 8.8 の PP は、Wave 2 COS ベースの AP のみをサポートします。NBAR/AVC の仕様

- WLC 上の NBAR/AVC フェーズ 2 では、1317（リリース 8.3）のさまざまなアプリケーションに対して分類およびアクションを実行できます。
- 分類されたアプリケーションに対して、ドロップまたはマークの 2 つのアクションを実行できます。
- WLC では最大 16 の AVC プロファイルを作成できます。
- 各 AVC プロファイルには最大 32 のルールを設定できます。
- 同じ AVC プロファイルを複数の WLAN にマッピングできます。ただし、1 つの WLANが保持できるのは、1 つの AVC プロファイルのみです。
- WLC では、NetFlow エクスポータとモニタを 1 つだけ設定できます。
- GUI では上位 10 のアプリケーションについてのみ、NBAR/AVC 統計情報が表示されます。CLI を使用してすべてのアプリケーションを表示できます。
- NBAR/AVC は、中央スイッチング専用に設定された WLAN でサポートされます。
- WLAN にマッピングされた AVC プロファイルにマークアクション用のルールが設定されている場合、そのアプリケーションは、WLAN 上で設定された QOS プロファイルをオーバーライドする AVC ルールで設定された、QOS プロファイルに従って優先されます。
- WLC 上の NBAR エンジンでサポートまたは認識されないアプリケーションは、未分類のトラフィックのバケットでキャプチャされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドはサポートされません。
- AVC プロファイルは、WLAN ごとに設定できますが、ユーザごとに適用することはできません。
- NBAR/AVC は vWLC および SRE WLC ではサポートされていません。

WLAN 上の AVC および QoS のインタラクション

コントローラの AVC/NBAR2 エンジンは、特定の WLAN の QoS 設定と相互運用します。NBAR2 機能は DSCP 設定に基づいています。同じ WLAN に AVC と QoS が設定されている場合、アップストリーム方向とダウンストリーム方向でパケットは次のように処理されます。

アップストリーム

1. 内部 DSCP の有無にかかわらずパケットがワイヤレス側（ワイヤレスクライアント）から送信されます。
2. AP が、WLAN に設定されている（QoS ベースの設定）CAPWAP ヘッダーに DSCP を追加します。
3. WLC が CAPWAP ヘッダーを削除します。
4. コントローラ上の AVC モジュールが、AVC プロファイルに設定された **marked** 値で DSCP を上書きして送信します。

ダウンストリーム

1. 有線側の内部 DSCP 値の有無にかかわらずパケットがスイッチから送信されます。
2. AVC モジュールが内部 DSCP 値を上書きします。
3. コントローラが、WLAN QoS 設定（802.1p 値の 802.11e による）と、NBAR が上書きした内部 DSCP 値を比較します。WLC は、小さいほうの値を選択し、それを DSCP の CAPWAP ヘッダーに格納します。
4. WLC が、外部 CAPWAP および AVC 内部 DSCP 設定で、QoS WLAN が設定された AP にパケットを送信します。
5. AP は CAPWAP ヘッダーを削除し、AVC DSCP 設定を含むパケットを送信します。AVC がアプリケーションに適用されていない場合、そのアプリケーションには WLAN の QoS 設定が適用されます。

アンカー/外部コントローラのセットアップによる AVC の動作

アンカーおよび外部コントローラの設定では、基本的にアプリケーション制御が必要な場所で AVC を設定する必要があります。アンカー/外部セットアップではほとんどの場合、アンカーコントローラで AVC を有効にします。AVC プロファイルの適用は、アンカーコントローラの WLAN で行われます。アンカーコントローラのリリースが 7.4 以上である場合は、上記のセットアップが機能します。

AVC プロトコルパック（フェーズ 2）のロード

コマンドライン インターフェイスを使用したプロトコルパックのロードのみがサポートされます。次の例で、プロトコルパックをロードするコマンドを示します。

```
(Cisco Controller) >transfer download datatype avc-protocol-pack

(Cisco Controller) >transfer download start

Mode.....FTP

Data Type.....AVC Protocol Pack

FTP Server IP.....A.B.C.D

FTP Server Port.....21

FTP Path...../

FTP Filename..... pp-unified-wng-152-4.S-13-4.1.1.pack

FTP Username..... cisco

FTP Password.....*********

Starting transfer of AVC Protocol Pack

This may take some time.

Are you sure you want to start? (y/N)
```

Y

```
(5508-60-Active) >transfer download datatype avc-protocol-pack

(5508-60-Active) >transfer download filename pp-adv-asr1k-152-4.S-13-4.1.1.pack

(5508-60-Active) >transfer download start

Mode..................................... TFTP
Data Type................................ AVC Protocol Pack
TFTP Server IP........................... 10.70.0.59
TFTP Packet Timeout...................... 6
TFTP Max Retries......................... 10
TFTP Path.....................................
TFTP Filename............................ pp-adv-asr1k-152-4.S-13-4.1.1.
pack

Starting tranfer of AVC Protocol Pack

This may take some time.
Are you sure you want to start? (y/N)
```

351509

ダウンロードプロセスは時間がかかる場合があります。

```
TFTP AVC Protocol Pack transfer starting.

TFTP receive complete... Loading Protocol Pack.

INFO, deactivation XDR was bypassed as batch config was identified

% INFO NBAR : engine deactivation
AVC Protocol Pack installed.
```

351510

show コマンドを使用して、現在ロードされているプロトコルパックを表示する
(Cisco Controller) >show avc protocol-pack version

AVC Protocol Pack Name: Advanced Protocol Pack

AVC Protocol Pack Version: 1.0

show コマンドを使用して、現在の Nbar2 エンジンのバージョンを表示する
(Cisco Controller) >show avc engine version

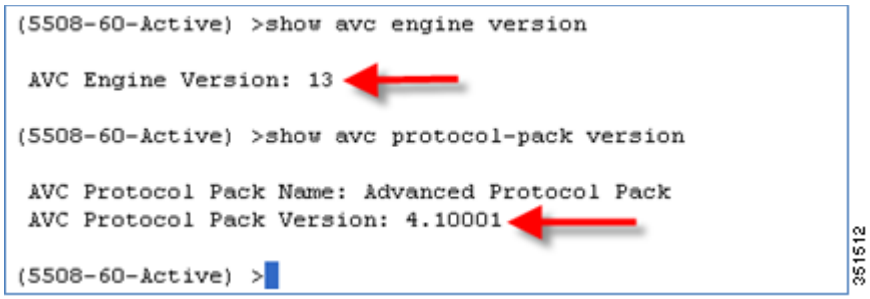
AVC Engine Version: 13

プロトコルパックをインストールする前は、次のようにデフォルトパックが表示されます。

```
(5508-60-Active) >show avc engine version

 AVC Engine Version: 13

(5508-60-Active) >show avc protocol-pack version

 AVC Protocol Pack Name: Advanced Protocol Pack
 AVC Protocol Pack Version: 1.0

(5508-60-Active) >
```

351511

プロトコルパックをインストールすると、AVC パックのバージョンが 4.10001 と表示されます。



debug コマンド

(Cisco Controller) >debug avc events enable

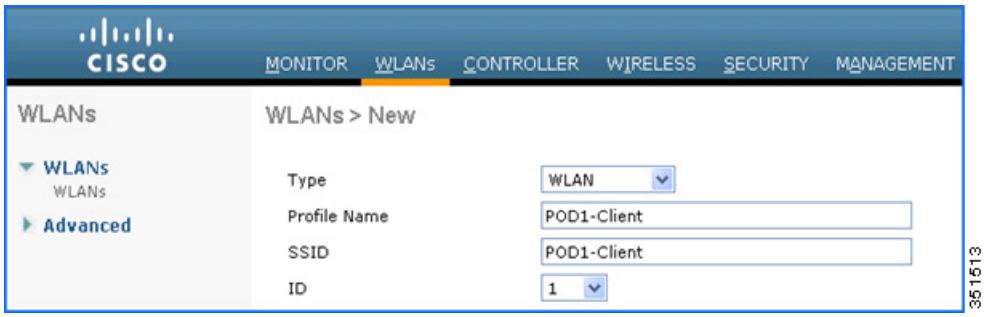
(Cisco Controller) >debug avc error enable

アプリケーション可視性の設定

次の手順を実行します。

1. 有線ラップトップで Web ブラウザを開きます。WLC の IP アドレスを入力します。
2. 命名規則を使用して「POD1-Client」などの OPEN WLAN を作成し、その WLAN の [QOS] タブで [Application Visibility] を有効化します。この WLAN を管理インターフェイスにマッピングします。

   アプリケーションの可視性を有効にするには、[WLAN ID]、[QOS] タブの順にクリックし、[Application Visibility] の [enable] オプションをオンにして [Apply] をクリックします。

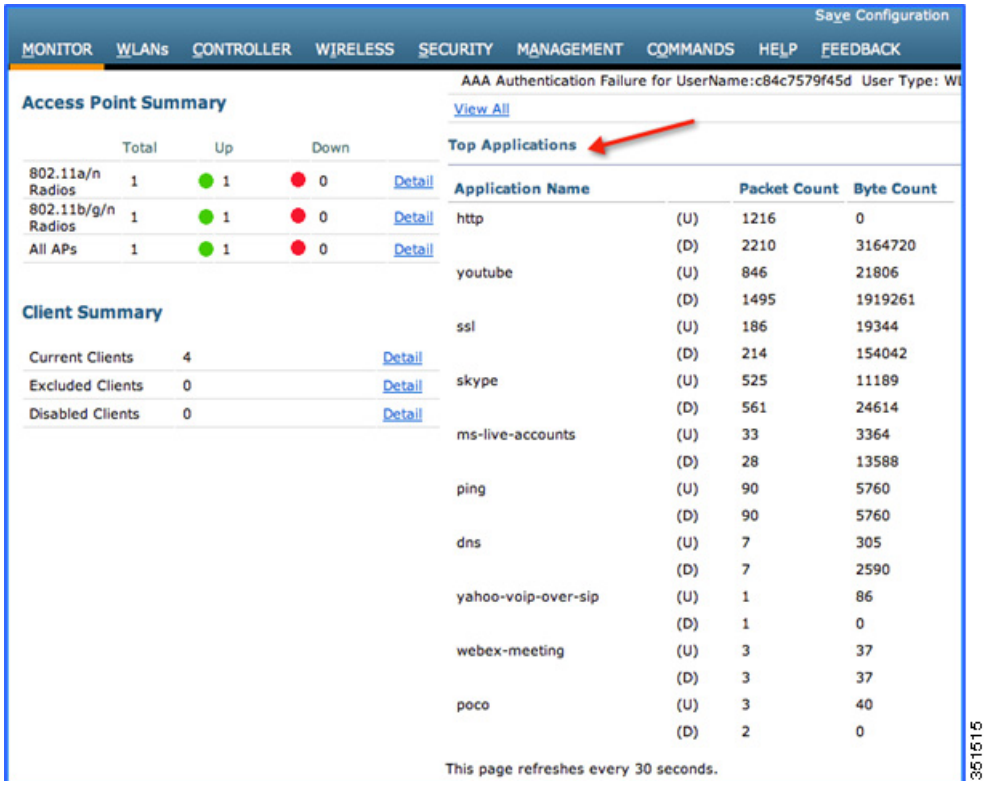


3. 特定の WLAN でアプリケーションの可視性を有効にすると、関連付けられているワイヤレスクライアントから、Cisco Jabber/Web Ex Connect、Skype、Yahoo Messenger、HTTP、HTTPS/SSL、Microsoft Messenger、YouTube、Ping、トレースルートなどの（すでにインストールされている）アプリケーションを使用するさまざまなタイプのトラフィックが開始されます。ワイヤレスクライアントからトラフィックが開始されると、クライアント単位および WLAN 単位ですべての WLAN のさまざまなトラフィックの可視性をグローバルに確認できます。これにより、管理者はネットワーク帯域幅の使用状況やネットワーク内のトラフィックのタイプについて、クライアント単位、WLAN 単位、およびグローバルに確認できます。

   上述のように、トラフィックの可視性をモニタリングできます。

- すべての WLAN を対象にグローバルに
- 個々の WLAN
- 個々のクライアント

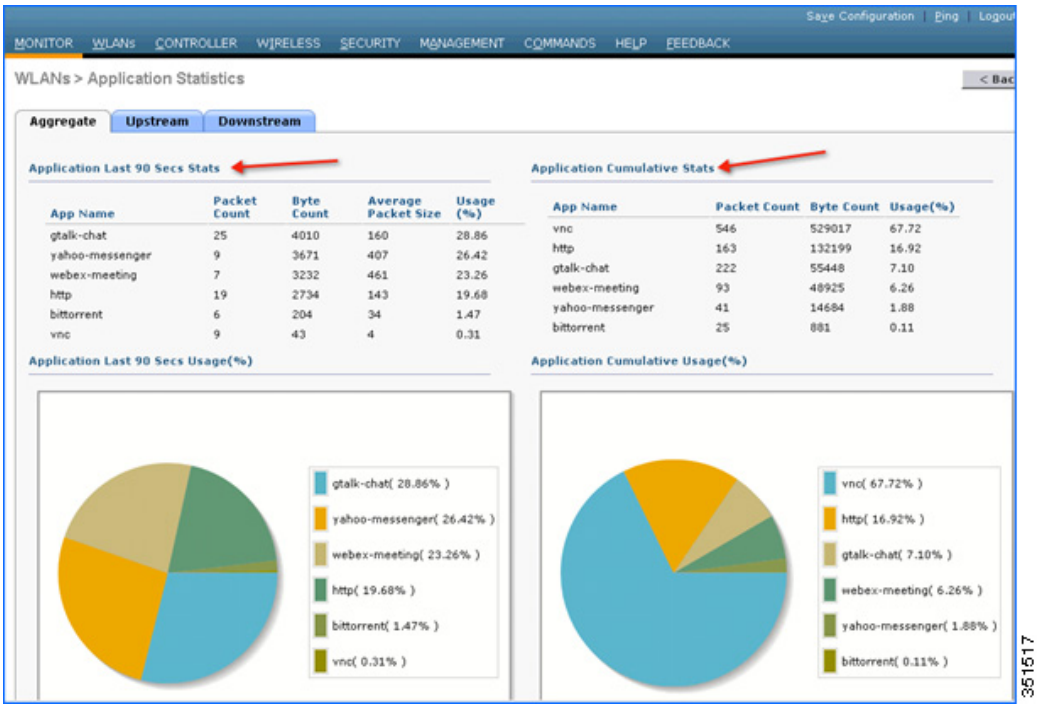
4. WLC 上のすべての WLAN の可視性をグローバルに確認するには、クリックして下にスクロールします。



注：モニタ画面に、WLC で実行されている NBAR エンジンによって分類された、すべての WLAN のアプリケーションが一覧表示されます。過去 90 秒のアップストリーム（U）およびダウンストリーム（D）の両方向で上位 10 のアプリケーションが、このページに表示されます。

5. WLAN ごとに詳細を確認する場合は、[Monitor] > [Applications] に移動します。このページには、AVC の可視性が有効になっているすべての WLAN が一覧表示されます。

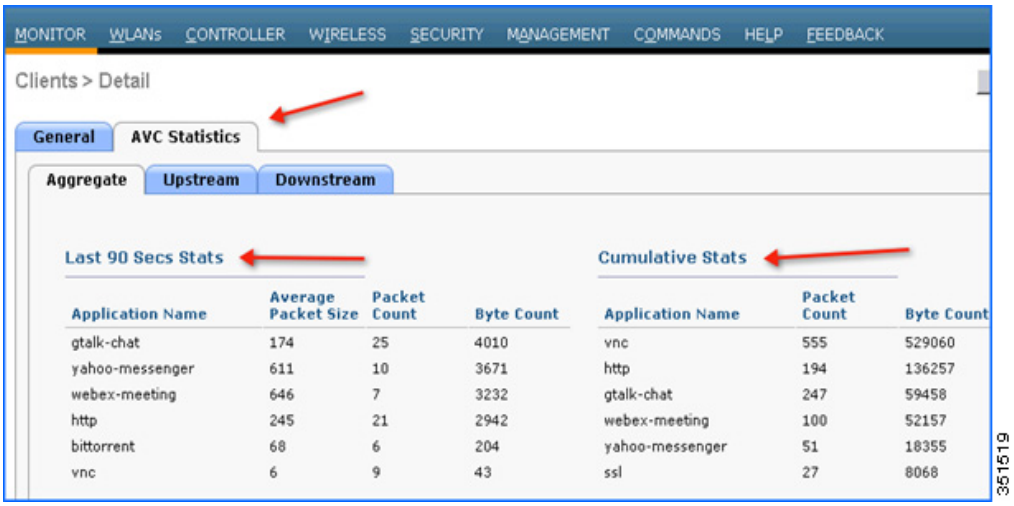
このページで個々の WLAN ID をクリックすると、下の画面に特定の WLAN で実行されている上位 10 のアプリケーションに関する集約データが表示されます。



注: このページでは、WLAN ごとのより詳細な可視性が提供され、過去 90 秒の上位 10 のアプリケーションと、上位 10 のアプリケーションの累積統計情報が表示されます。上の画面には、特定の WLAN のアップストリームデータとダウンストリームデータを含む集約トラフィックが一覧表示されます。同じページで WLAN ごとのアップストリーム統計情報とダウンストリーム統計情報を個別に表示するには、[Upstream] タブと [Downstream] タブをクリックします。

6. AVC の可視性が有効になっている特定の WLAN で、クライアントごとの上位 10 のアプリケーションについてより詳細に表示するには、[Monitor] > [Clients] に移動し、そのページに表示される個々のクライアント MAC エントリをクリックします。

上記ページに表示される個々のクライアント MAC エントリをクリックすると、2 つのタブがあるクライアント詳細ページが開きます。1 つは一般情報のタブで、もう 1 つは [AVC Statistics] というタブです。その特定のクライアントの上位 10 のアプリケーションに関する NBAR 統計情報を表示するには、[AVC Statistics] タブをクリックします。



注: このページでは、アプリケーションの可視性が有効になっている WLAN に関連付けられたクライアントごとの詳細な統計情報が提供され、過去 90 秒の上位 10 のアプリケーションと、上位 10 のアプリケーションの累積統計情報が表示されます。上の画面では、クライアントごとの集約トラフィック（アップストリーム統計情報とダウンストリーム統計情報を含む）が一覧表示されています。同じページでクライアントごとのアップストリーム統計情報とダウンストリーム統計情報を個別に表示するには、[Upstream] タブと [Downstream] タブをクリックします。

AVC プロファイルの設定

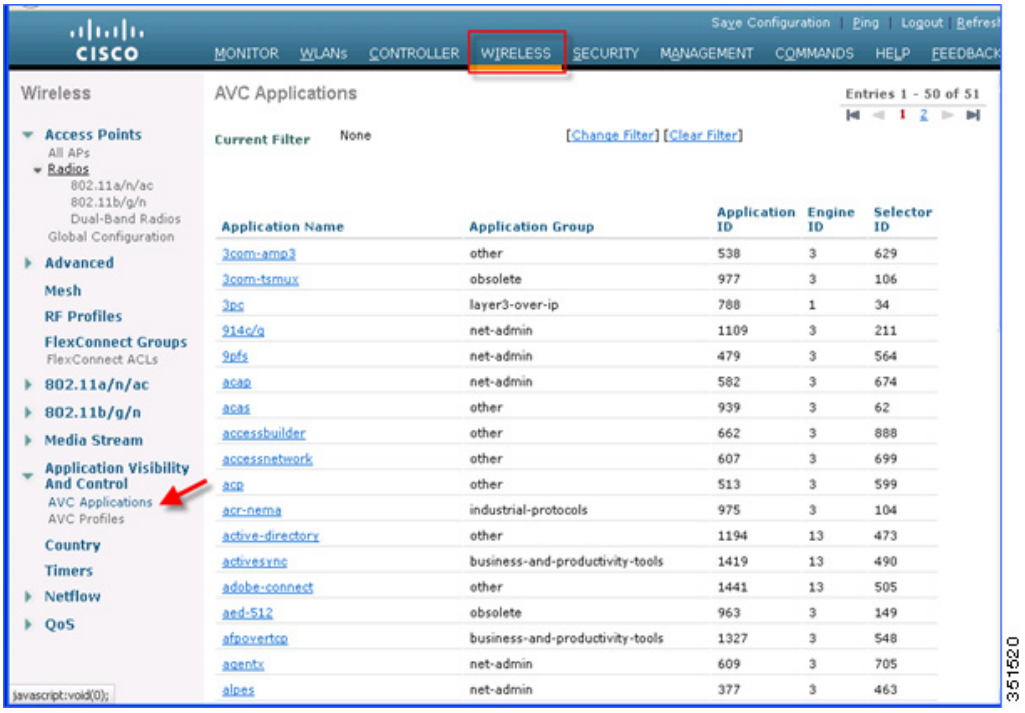
次の手順を実行します。

1. WLC の NBAR 機能は、ネットワーク内で実行されているアプリケーションの可視性を提供するだけでなく、管理者が AVC プロファイルを作成してネットワーク内で実行されているアプリケーションを制御できるようにします。認識されたアプリケーションで次のアクションを実行する AVC プロファイルを設定できます。

   a. アクションドロップ（そのアプリケーションのトラフィックはドロップされる）

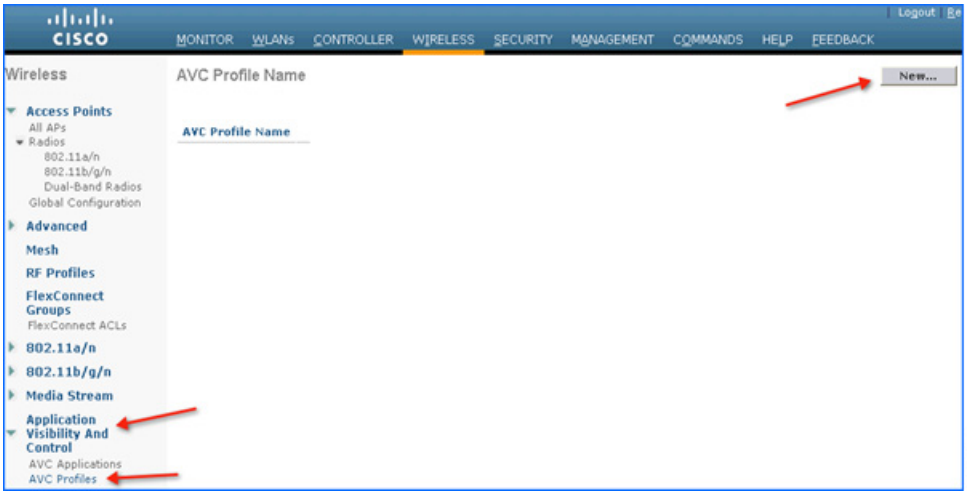
   b. アクションマーク（WLC で使用可能なさまざまな QOS プロファイルで特定のアプリケーションをマークするか、管理者がそのアプリケーションの DSCP 値をカスタム定義できる）

2. NBAR エンジンでサポートされているすべてのアプリケーションの統計情報、可視性、および制御アクション（ドロップ/マーク）を表示するには、[Wireless] > [Application Visibility And Control] > [AVC Applications] に移動します。このページには、すべてのアプリケーションとそれぞれが属しているアプリケーショングループが格納順に一覧表示されます。

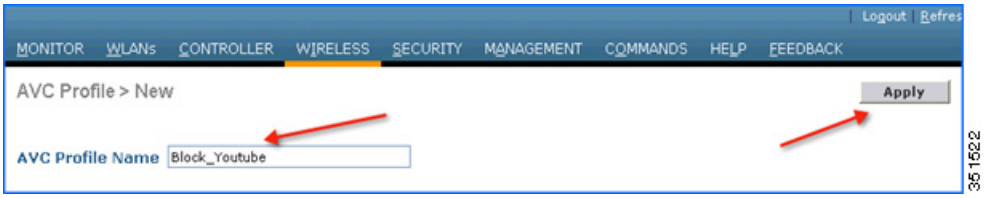


注：AVC プロファイルでアプリケーションのドロップ/マークアクションを作成する場合は、最初にアプリケーショングループを選択する必要があります。このページには、すべてのアプリケーションとそれぞれが属しているアプリケーショングループ、およびブラウザの「FIND」オプションを使用したアプリケーションの簡単なルックアップが表示されます。管理者はアプリケーションとそのグループを検索し、AVC プロファイルでこのグループを使用してドロップ/マークアクション（このガイドで説明）を設定できます。WLC の NBAR は、1054 のさまざまなアプリケーションの可視性をサポートしています。

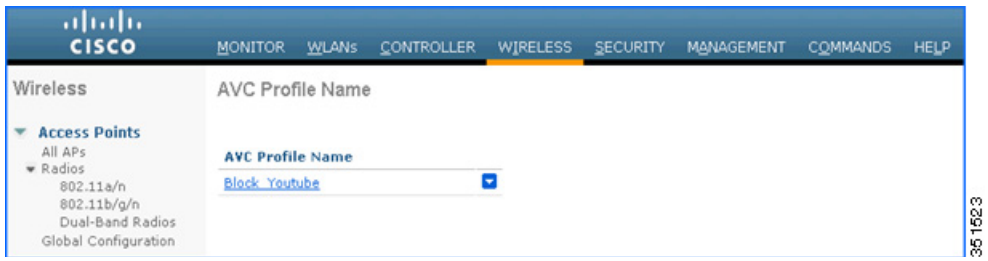
3. アクション（ドロップ/マーク）を設定するには、最初に AVC プロファイルを作成する必要があります。AVC プロファイルを設定するには、[Wireless] > [Application Visibility And Control] > [AVC Profiles] に移動し、[New] をクリックして AVC プロファイルを作成します。



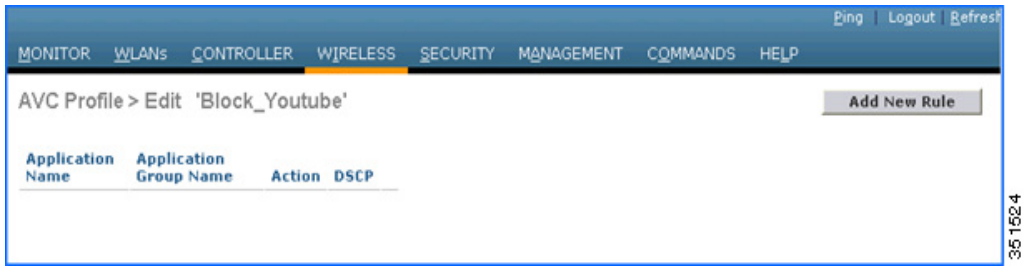
4. AVC プロファイル名を入力して [Apply] をクリックします。



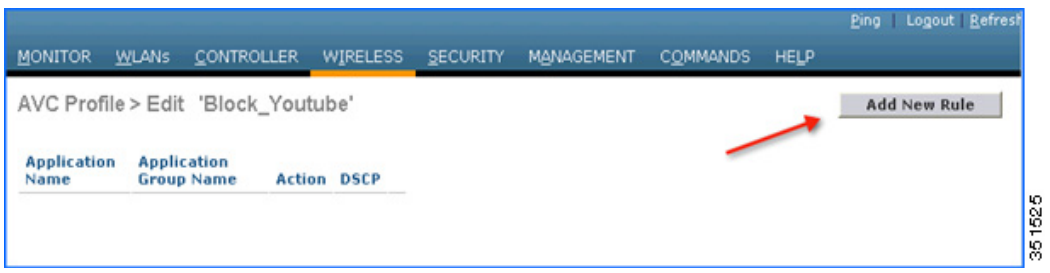
5. [Apply] をクリックすると AVC プロファイルが作成され、上記で作成したプロファイルが表示されます。これをクリックして、ドロップ/マークアクションを実行するルールを作成できます。WLC では最大 16 の AVC プロファイルを作成できます。



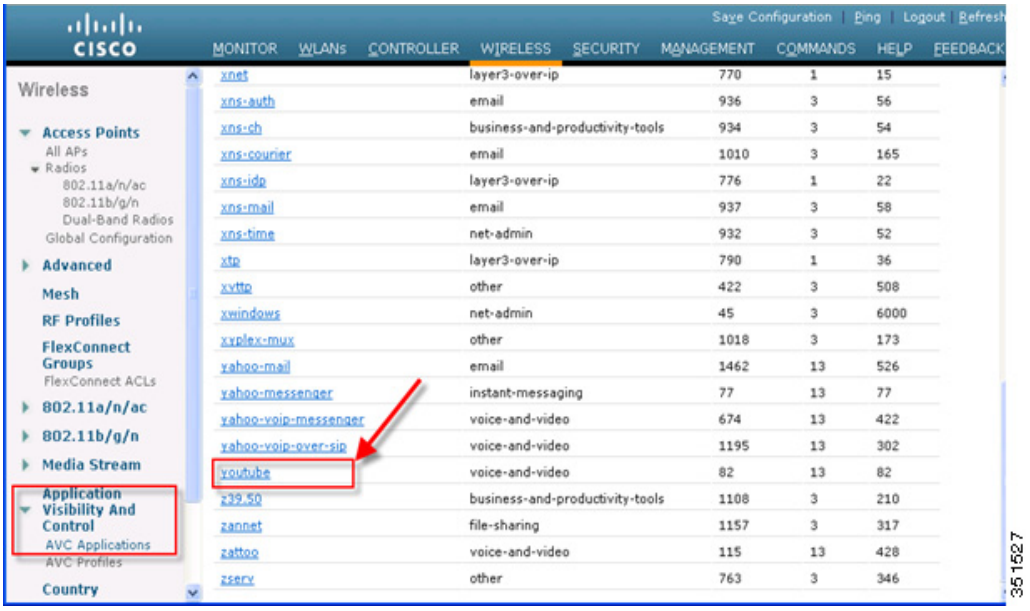
6. AVC プロファイルを作成した後は、プロファイル名をクリックして個々のプロファイルのルールを作成できます。各プロファイルで最大 32 のルールを設定できます。2 つのアクション（ドロップまたはマーク）のいずれかを実行するルールを設定できます。アプリケーション用のルールが設定されていない場合、デフォルトアクションは、WLAN で設定されている QOS ポリシーによる「許可」です。プロファイルのルールを作成するには、[Wireless] > [Application Visibility And Control] > [AVC Profiles] に移動して、先に作成したいずれかのプロファイルをクリックします。



7. [Add New Rule] をクリックすると、下記のページ（2 つ目のスクリーンショット）が表示されます。管理者はこのページの最初のドロップダウンからアプリケーショングループを選択して、そのグループに属しているアプリケーションのみに絞り込めます。次に、2 つ目のドロップダウンからアプリケーションを選択できます。2 つ目のドロップダウンでアプリケーションを選択したら、管理者はそのアプリケーションに対して実行するアクションを 3 つ目のドロップダウンから選択できます。アクションを選択したら、[Apply] をクリックします。



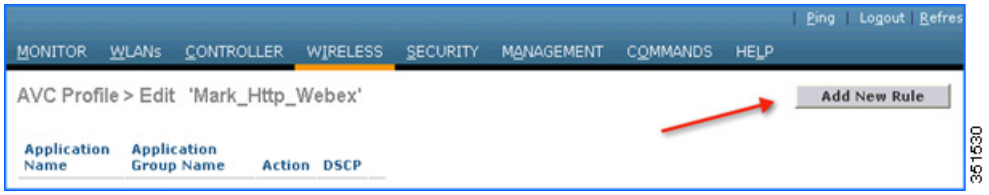
注:7.5 リリースでは、WLC は 1054 のアプリケーションを分類し、アクションを実行するオプションを提供します。アプリケーションに対してアクションを実行するには、最初に管理者はそのアプリケーションが属するアプリケーショングループを選択して、アプリケーションリストをそのアプリケーショングループのみに絞り込む必要があります。この手順が必要な理由は、1 つのドロップダウンで 1054 のアプリケーションをすべて表示することができないためです。7.5 リリースでも、[Application Names] を選択できるようになりました。また、リスト内のアプリケーション名にカーソルを合わせてクリックすると、上記のプロファイルルールを作成できます。



8. [Apply] をクリックすると、アクションルールが作成されて下の画面にキャプチャされているように表示されます。同じページで AVC プロファイルに他のルールを追加できます。1 つの AVC プロファイルで最大 32 のルールを設定できます。

9. 同じ AVC プロファイルで別のルールを設定し、別の QOS プロファイルまたはカスタム DSCP 値でトラフィックをマーキングできます。この例では、ステップ 3、4、および 5 に従って「Mark_Http_Webex」という名前の別の AVC プロファイルを作成しました。この例では、この AVC プロファイルを使用して、「Http」を低い優先順位でマーキングして、「Webex」に高い優先順位を指定するルールを作成します。

前述のステップ 6、7、8 で説明したように、AVC プロファイル名をクリックしてプロファイルのルールを作成します。[Add New Rule] をクリックします。



最初のドロップダウンからアプリケーショングループを選択し、2 つ目のドロップダウンからアプリケーション名として [Webex] を選択します。[Action] を [MARK] に設定して、QOS プロファイルとして [Platinum] を選択し、[Apply] をクリックします。

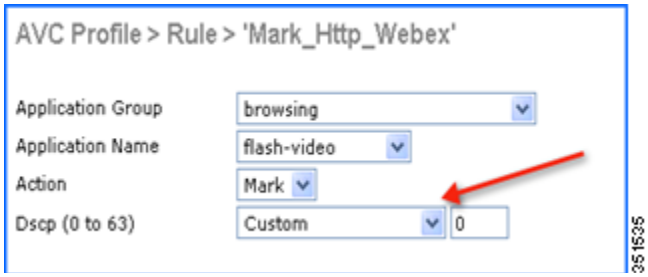
[Apply] をクリックすると、アクション ルールが作成され、下の画面にキャプチャされているように表示されます。別のアプリケーション「Http」をマーキングする別のルールを作成するには、同じページで [Add New Rule] をクリックします。

同じページで [Add New Rule] をクリックするだけで、同じプロファイルの別のルールを作成できます。最初のドロップダウンからアプリケーショングループを選択し、2 つ目のドロップダウンからアプリケーション名として [http] を選択します。次に、[Action] を [MARK] に設定し、QOS プロファイルとして [Bronze] を指定します。次に、[Apply] をクリックします。

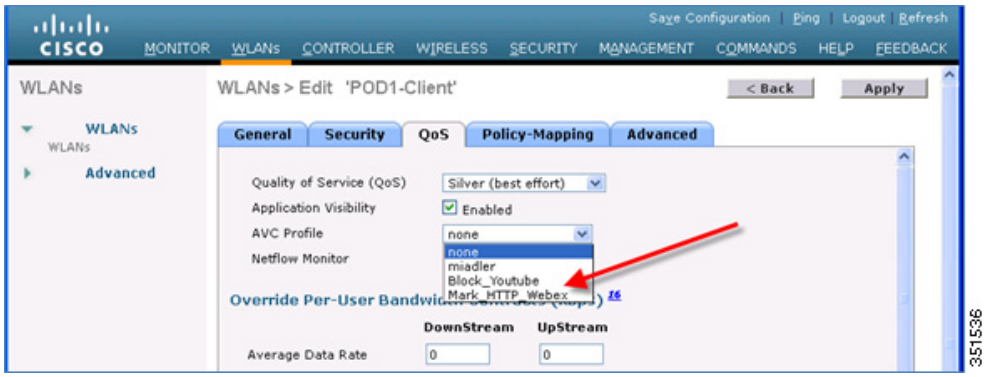
[Apply] をクリックすると、アクション ルールが作成され、下の画面にキャプチャされているように表示されます。

注：同じ AVC プロファイルに 2 つのルールが作成されます。管理者は、同じ AVC プロファイルに最大 32 のルールを設定できます。同じプロファイル内で、個別のルールに対してアクションを [MARK] または [DROP] として設定できます。単一のルールには単一のアクションのみ、つまり、[MARK] または [DROP] のいずれかを設定できます。

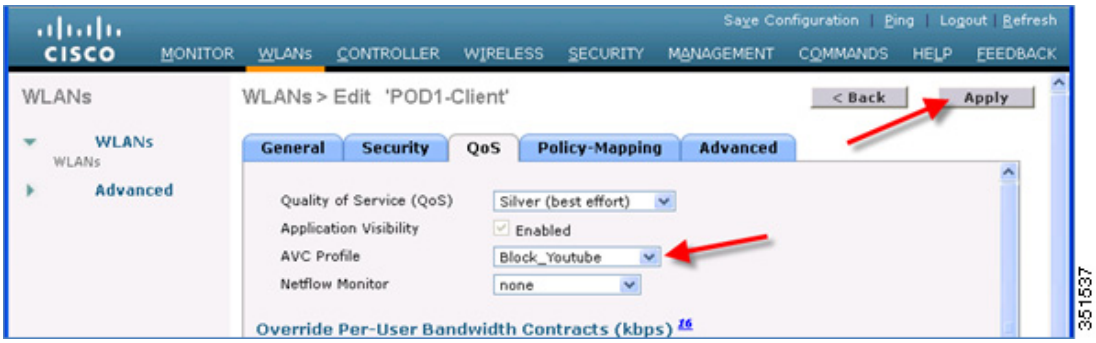
管理者は、[Action] を [MARK] に設定した場合、DSCP 値として「Platinum/Gold/Silver/Bronze」を選択する代わりに、[Custom] を選択することもできます。DSCP 値として [Custom] を選択するとテキストフィールドが表示され、管理者は 0 ～ 63 の範囲でカスタム DSCP 値を入力できます。



10. 次の手順は、WLAN にこれらの AVC プロファイルを適用することです。1 つの WLAN に AVC プロファイルを 1 つのみマッピングできます。単一の AVC プロファイルを複数の WLAN にマッピングできます。AVC プロファイルが WLAN にマッピングされ、マークアクションのルールが設定されている場合、そのアプリケーションは、WLAN 上で設定された QOS プロファイルと相互作用する AVC ルールに設定された QOS プロファイルに従って優先されます。作成されたすべての AVC プロファイルは、WLAN の [QOS] タブにある [AVC Profile] ドロップダウンに表示されます。WLAN のドロップダウンで AVC プロファイルを確認するには、[WLANs] > [WLAN ID] に移動して [QOS] タブをクリックします。作成されたすべての AVC プロファイルが、[AVC Profile] ドロップダウンに表示されます。管理者は、ネットワーク要件に従って WLAN の AVC プロファイルを選択できます。



11. たとえば、ドロップダウンから AVC プロファイル [Block_Youtube] を選択して [Apply] をクリックします。



注：アプリケーションの可視性が WLAN で有効になっていない場合に、ユーザが AVC プロファイルを選択して [Apply] をクリックすると、自動的にアプリケーションの可視性が有効になります。ただし、WLAN でアプリケーションの可視性を無効にするには、まずドロップダウンから [None] を選択して、WLAN にマッピングされている AVC プロファイルを削除する必要があります。

12. WLAN に適用された AVC プロファイルは、[Monitor] > [Applications] にも表示されます。アプリケーションの可視性が有効になっているすべての WLAN が表示されます。

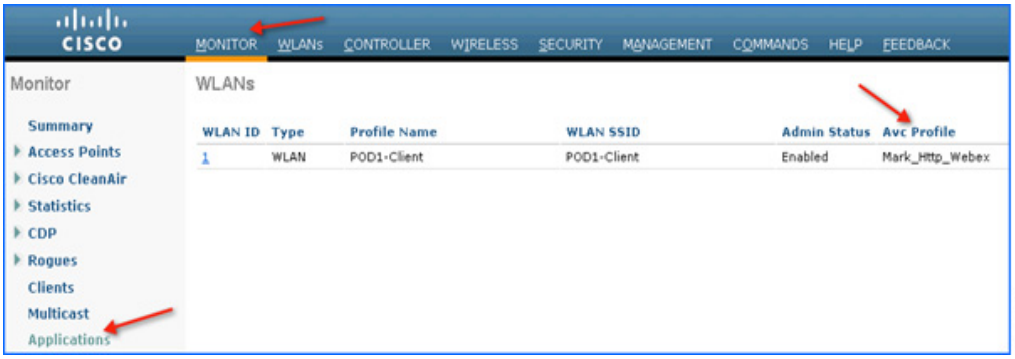
13. ワイヤレスクライアントで **www.youtube.com** を開いてみます。クライアントで YouTube のビデオを再生できないことを確認します。また、Facebook アカウントを開いたり（持っている場合）、Facebook アカウントで YouTube ビデオを開いたりしてみてください。YouTube ビデオを再生できないことが確認できます。

    YouTube をブロックする AVC プロファイルが WLAN にマッピングされているため、クライアントはブラウザ経由でも、YouTube アプリケーションを使用しても、他の Web サイトからも YouTube ビデオにアクセスすることができません。

注: すでに開いているブラウザで Youtube.com が実行されている場合、AVC プロファイルを有効にするには、ブラウザを更新してください。

14. 次に、WLAN で AVC プロファイルを変更し、NBAR 機能のマーク動作をテストします。WLAN の [QOS] タブでドロップダウンから AVC プロファイル [Mark_Http_Webex] を選択し、[Apply] をクリックします。

15. WLAN に適用された AVC プロファイルは、[Monitor] > [Applications] にも表示されます。アプリケーションの可視性が有効になっているすべての WLAN が表示されます。

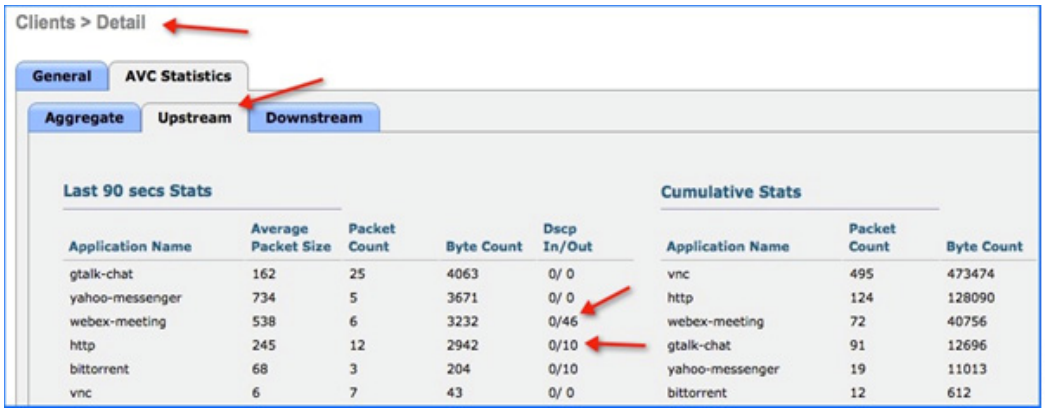


16. AVC プロファイル **Mark_Http_Webex** を WLAN に適用したら、個々の Webex アカウント（持っている場合）を開始するか、アカウントにログインし、HTTP 接続も開始して、クライアントの詳細でこれら 2 つのアプリケーションのマーキングを確認します。AVC プロファイルが WLAN にマッピングされ、マークアクションのルールが設定されている場合、そのアプリケーションは、WLAN 上で設定された QoS プロファイルをオーバーライドする AVC ルールに設定された QoS プロファイルに従って優先されます。

    この例では、WLAN がデフォルトの QOS プロファイル **SILVER** にマッピングされますが、アプリケーション Webex および HTTP を別の QOS プロファイルでマーキングするために、AVC プロファイルが作成されてこの WLAN にマッピングされています。アプリケーション Webex のトラフィックは **PLATINUM** プロファイルでマーキングされ、すべての HTTP アプリケーションのトラフィックは **BRONZE** プロファイルでマーキングされます。AVC プロファイルのルールに一致しない他のアプリケーションは、WLAN に設定されている QOS プロファイル（この例では SILVER）でマーキングされます。

17. クライアントトラフィックのマーキング統計情報を確認するには、[Monitor] > [Clients] に移動し、そのページに表示される個々のクライアント MAC エントリをクリックします。

上記ページに表示される個々のクライアント MAC エントリをクリックすると、2 つのタブがあるクライアント詳細ページが開きます。1 つは一般情報のタブで、もう 1 つは [AVC Statistics] というタブです。AVC プロファイルのマーキング動作を確認するには、[AVC Statistics] タブをクリックして、さらに [UPSTREAM] タブをクリックします。

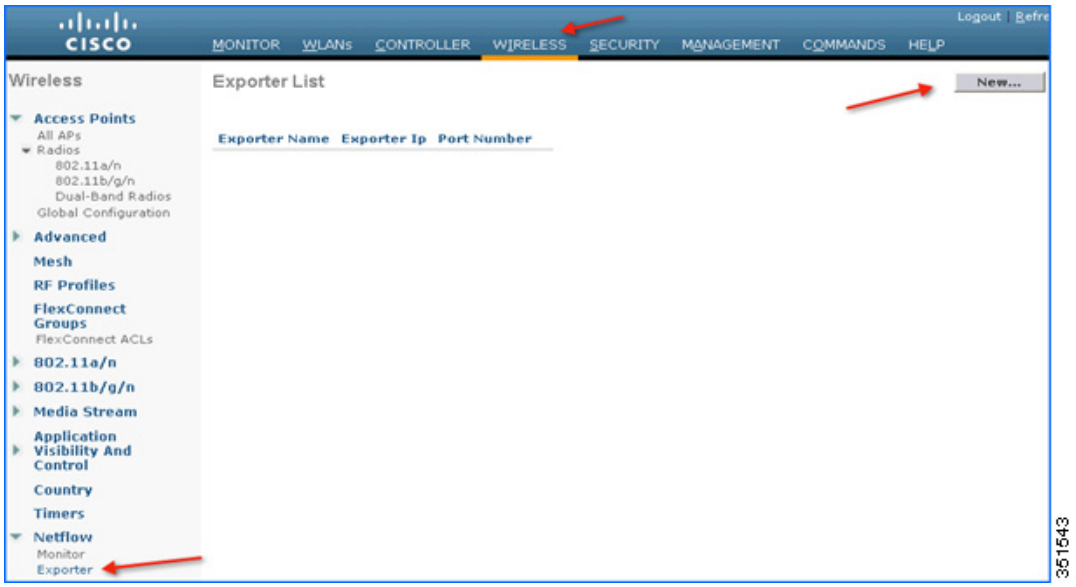


上記の出力で、Webex アプリケーションは Platinum QOS プロファイルが設定されているために OUT DSCP 値が 46 になり、HTTP アプリケーションは Bronze プロファイルが設定されているために OUT DSCP 値が 10 であることを確認してください。

NBAR NetFlow モニタの設定

WLC で生成されたすべての統計情報を収集するように、NetFlow モニタを WLC で設定することもできます。これらの統計情報は NetFlow コレクタにエクスポートできます。次の例では、Cisco Performance Application Manager（PAM）を NetFlow コレクタとして使用しています。PAM は Cisco Prime Infrastructure で稼働するライセンス付きのアプリケーションです。

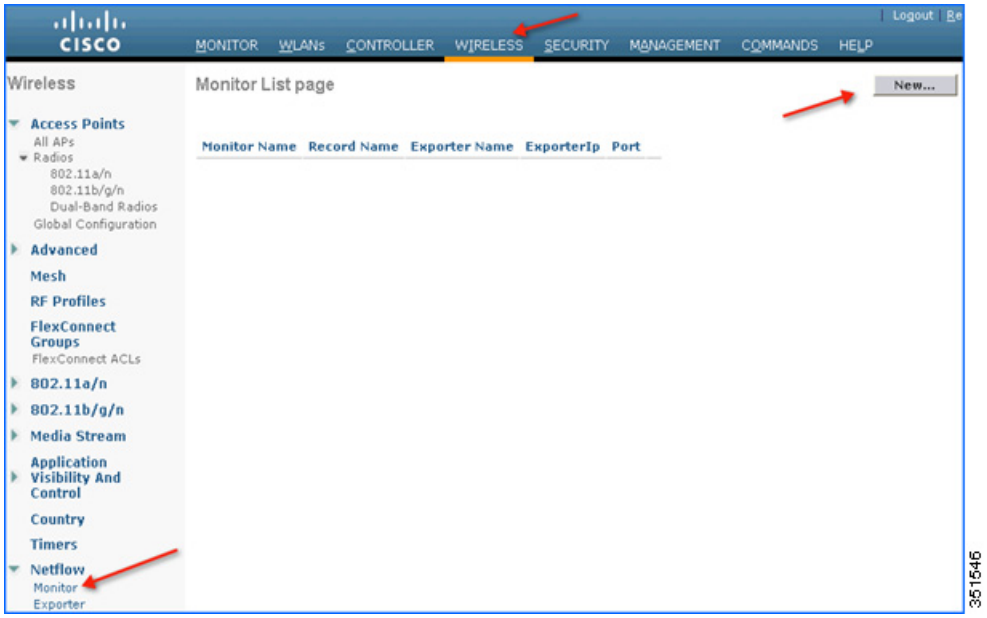
1. 最初に NetFlow エクスポータ（NetFlow コレクタ）を設定して WLC にエクスポータを追加します。この例では、Cisco PAM がエクスポータです。これは、WLC によって生成されたすべての NetFlow 統計情報を収集します。WLC にエクスポータを追加するには、[Wireless] > [NetFlow] > [Exporter] に移動して [New] をクリックします。



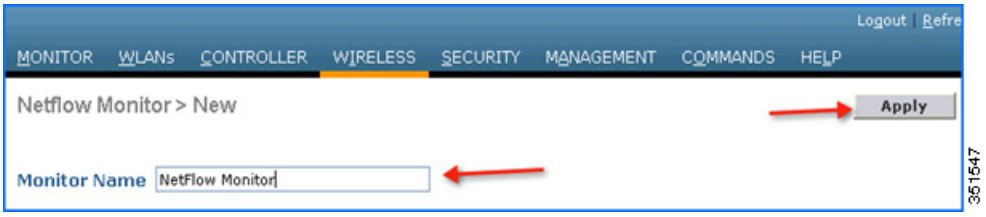
2. WLC によって生成されたすべての NetFlow 統計情報を収集する PAM の詳細として、[Exporter IP]（下記の例では 10.10.105.3）と [Port Number]（9991）を入力し、[Apply] をクリックします。

注：WLC に追加できるエクスポータは 1 つのみです。

3. WLC でエクスポータ（PAM サーバ）の詳細を追加したら、NetFlow 統計情報を保存し、同じ情報を PAM サーバにエクスポートするモニタを作成する必要があります。モニタを作成するには、[Wireless] > [NetFlow] > [Monitor] に移動して [New] をクリックします。



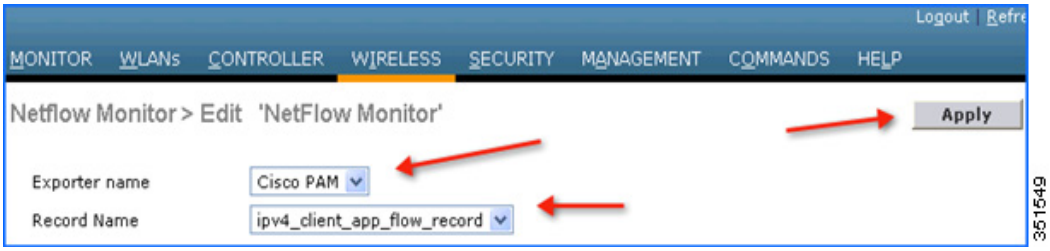
4. 任意の名前を入力して WLC でモニタエントリを作成し、[Apply] をクリックします。



5. 適用するとモニタエントリが作成されます。さらにこれを、ステップ 2 で作成したエクスポータにマッピングする必要があります。

注：WLC に追加できるモニタエントリは 1 つのみです。

6. モニタエントリをクリックしてエクスポータエントリ（Cisco PAM）にマッピングします。[Exporter name] ドロップダウンには、上記で作成した「エクスポータ」エントリが表示されます。WLC によって自動生成されたレコード「ipv4_client_app_flow_record」に、すべての NBAR 統計情報が記録されて Cisco PAM にエクスポートされます。[Record name] ドロップダウンでこのレコードエントリを選択し、[Apply] をクリックします。



7. モニタのエントリが作成され、エクスポータのエントリも同じものにマッピングする場合は、WLAN にマッピングする必要があります。エクスポータエントリを WLAN にマッピングするには、[WLANs] をクリックして特定の **WLAN ID** をクリックします。[QOS] タブをクリックし、上記で作成したモニタエントリを [NetFlow Monitor] ドロップダウンから選択して、WLAN の [Edit] ページで [Apply] をクリックします。

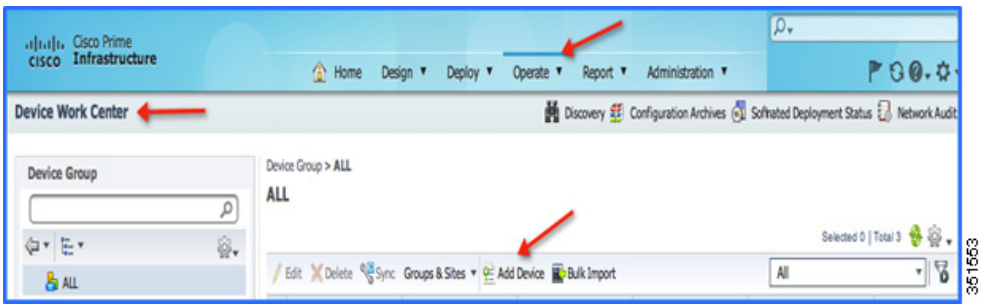
注：設定されているエクスポータポートが 9991 であることを確認してください。

8. 次にブラウザで新しいタブを開き、Cisco Prime Infrastructure サーバにログインして個々の WLC を PAM に追加します。

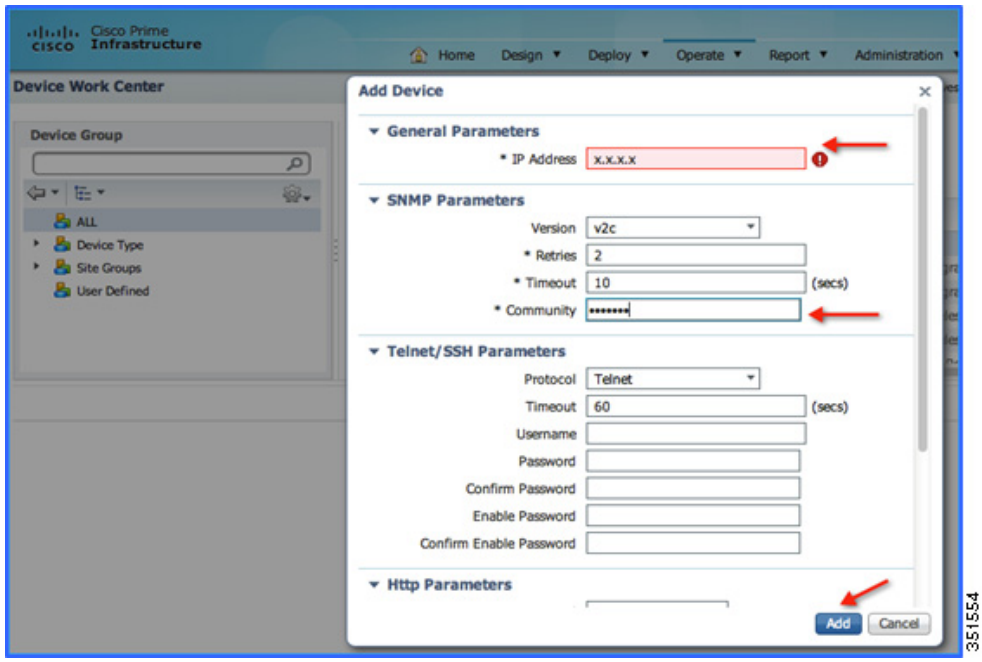
   ユーザ名：XXXXXX

   パスワード：XXXXXXX

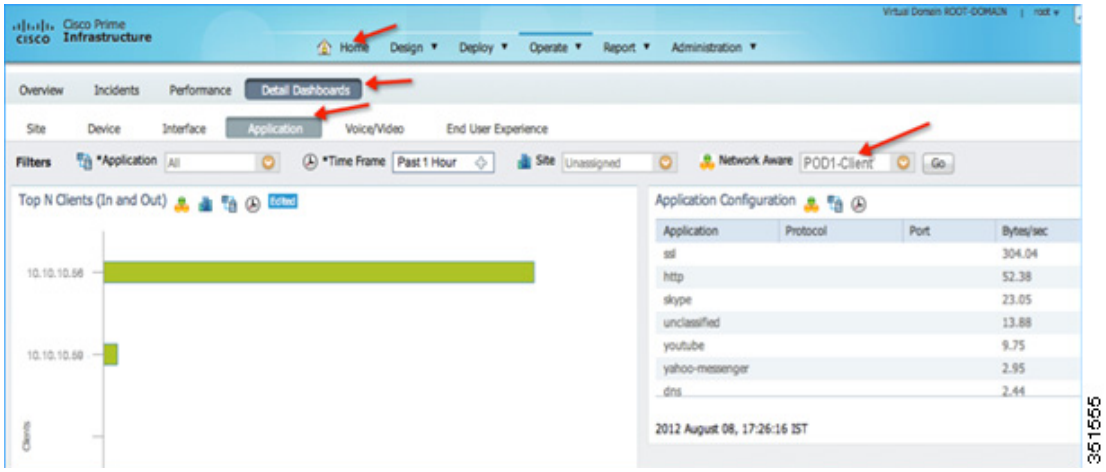
9. Cisco PAM で WLC を追加します。Cisco PAM に WLC を追加するには、Cisco PAM にログインして [Operate] > [Device Work Center] に移動し、Lifecycle テーマの [Add Device] をクリックします。



10. 個々の WLC の詳細、つまり WLC の管理 IP アドレス（例：WLC-POD4 = 10.10.40.2）、および**コミュニティストリング**として public を入力し、[Add] をクリックします。

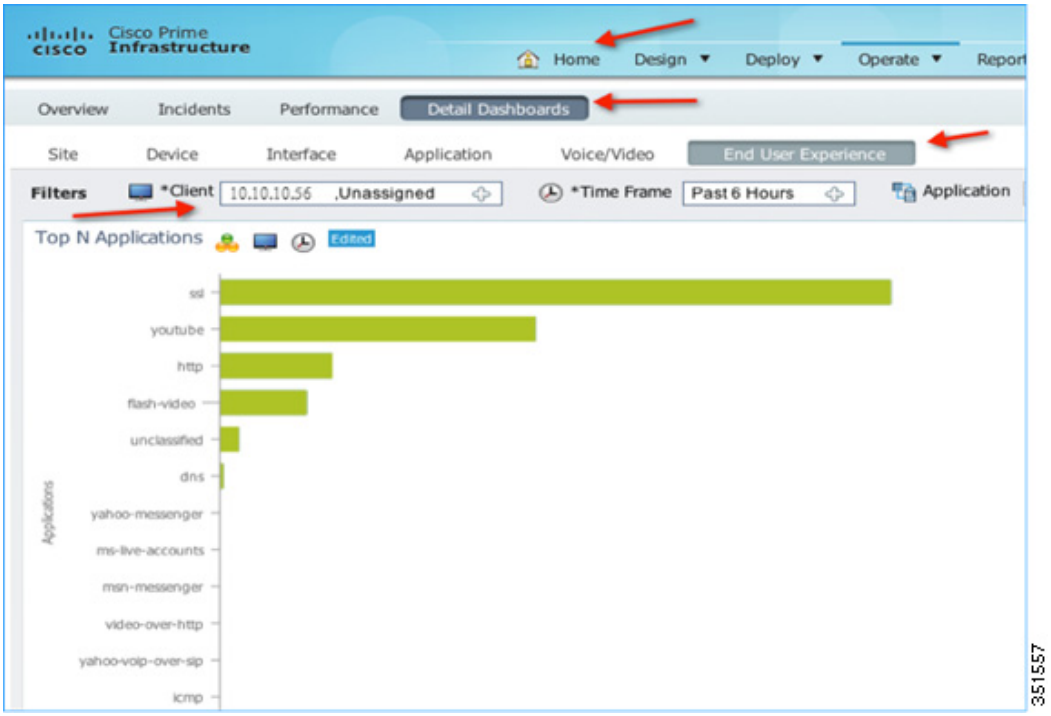


11. WLC を追加したら、ワイヤレスクライアントからのトラフィックを開始します。WLAN ごとのクライアント数とクライアントごとの使用状況を表示することができます。クライアント別の使用状況を確認するには、[Home] > [Detail Dashboards] > [Application] に移動します。ここで、[Application Box] を [All]、[Site] を [Unassigned]、[Network Aware] を [Wireless] > [PODX-Client] としてフィルタリングし、[Go] をクリックします。

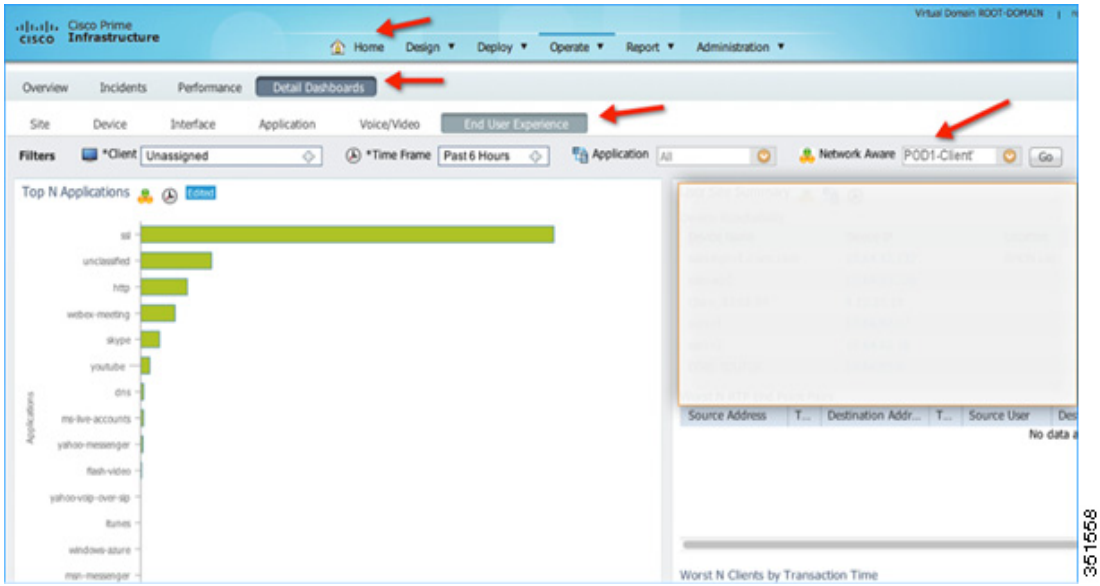


注：[Network Aware] でフィルタリングした WLAN「POD1-Client」のクライアント数を確認できます。 また、同じ画面で両方のクライアントによって使用されるアプリケーションも確認できます。

12. 特定のクライアントによるアプリケーションの使用状況を確認するには、[Home] > [Detail Dashboards] > [End User Experience] > [Under Filter] に移動して、クライアント IP を選択します。



13. WLAN ごとにアプリケーションの使用状況を確認するには、[Home] > [Detail Dashboards] > [End User Experience] > [Under Filter] に移動して、[Network Aware] で **WLAN**（この例では [POD1-Client]）を選択します。[実行（Go）] をクリックします。



CUWN リリース 8.0 の AVC フェーズ 3

このリリースでは、次を含む AVC 機能セットに対してさまざまな機能強化が行われました。

- クライアントの AAA AVC プロファイルオーバーライド。
- WLAN でのユーザごとのアプリケーションレート制限。
- AVC プロファイルと、ユーザおよびデバイスごとのローカルポリシー分類の統合。
- アップストリームおよびダウンストリーム トラフィックの AVC 指向性 QoS DSCP マーキング。
- プロトコルパック 9.0 および NBAR エンジンリリース 3.1 による 1105 のアプリケーションのサポート。

クライアントの AAA AVC プロファイルオーバーライド

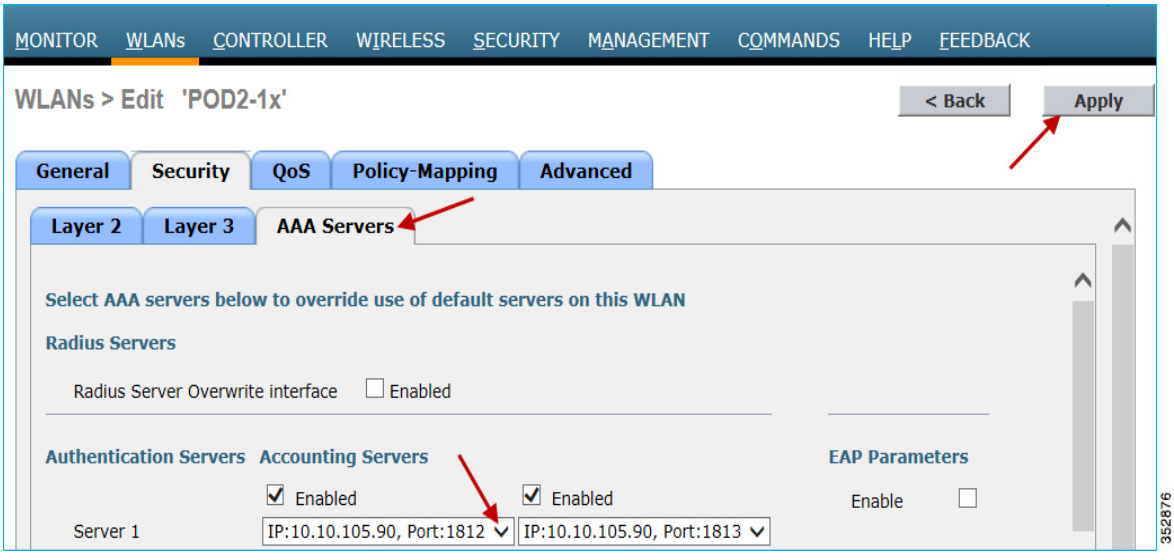
リリース 7.4、7.5、および 7.6 で前述したように、WLAN に AVC プロファイルを設定すると、その WLAN に接続されているすべてのクライアントが同じ AVC プロファイルを継承します。AAA AVC プロファイルオーバーライドを許可する価値提案は、さまざまなクライアント（異なるユーザとしてログイン）が、同じ WLAN に接続されていても異なる AVC プロファイルを取得できることです。

クライアントまたはユーザプロファイルの AAA 属性は、AAA サーバ（Cisco ACS や ISE など）で設定できます。AAA 属性は一般的な Cisco AV ペアとして定義され、AAA で文字列と値のペアとして定義できます。この属性は、L2/L3 認証中に WLC によって処理され、WLAN 上の設定によってオーバーライドされます。

ユーザロールごとにアプリケーションの可視性を設定する手順

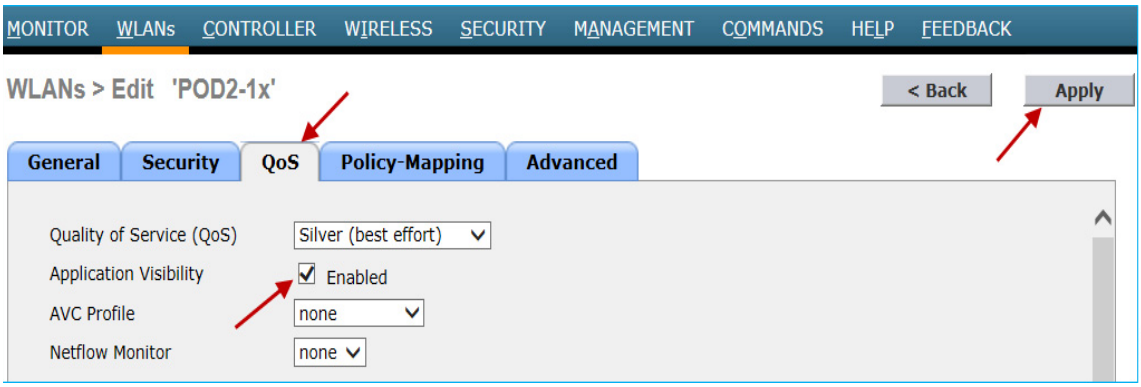
次の手順を実行します。

1. WPA2/802.1x 認証用の L2 セキュリティ設定で WLAN を作成して設定します。ユーザまたは管理者によって dot1x 認証用の AAA サーバがすでに設定されていると仮定し、[Authentication Servers] ドロップダウンリストから AAA サーバを選択して [Apply] をクリックします。



以下に示すように、[Advanced] タブをクリックして「AAA オーバーライド」を有効にします。

2. アプリケーションの可視性を有効にするには、[WLAN ID] をクリックし、[QoS] タブで [Application Visibility] の [Enabled] チェックボックスをオンにします。[Apply] をクリックします。

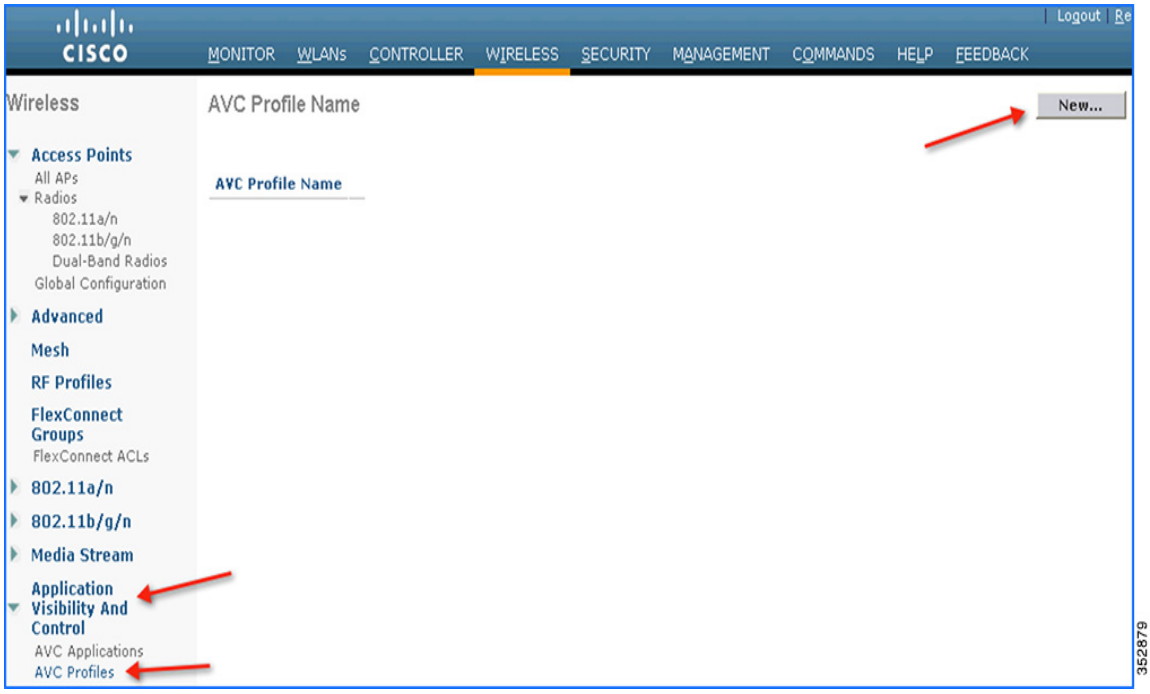


AVC プロファイルの AAA 設定

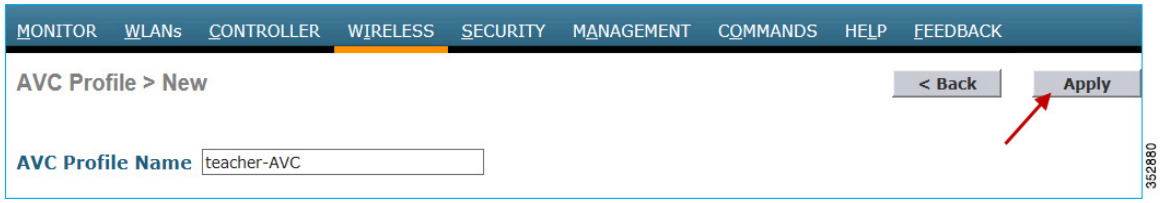
AAA AVC プロファイルは、Cisco AV ペアとして定義されます。文字列は **avc-profile-name** として定義されており、この値を WLC 上にある AVC プロファイルに設定する必要があります。

次の手順を実行します。

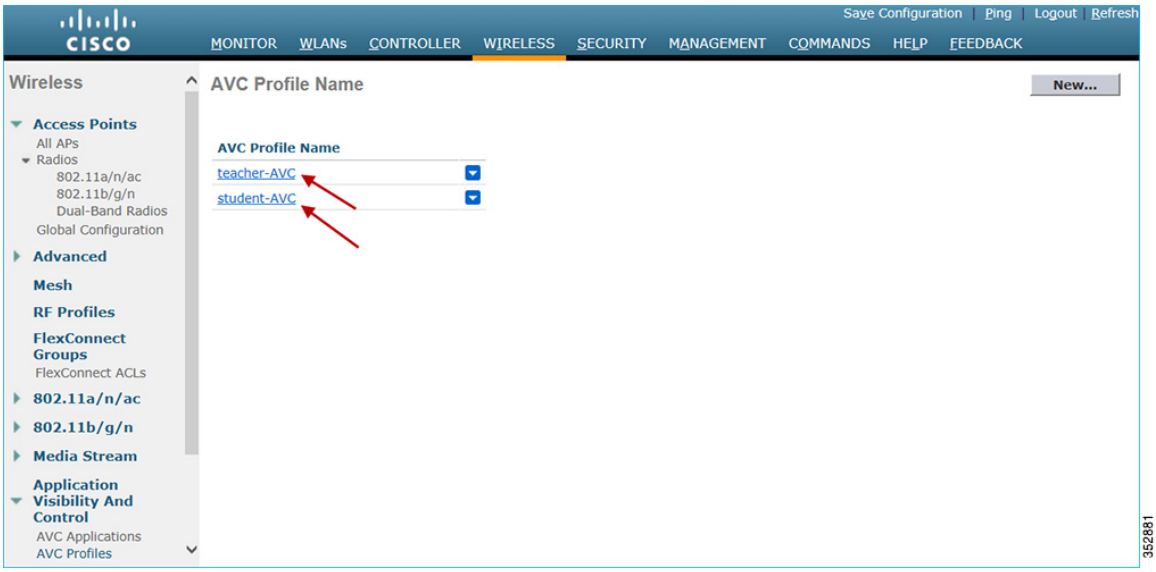
1. AAA サーバ経由でユーザごとに AVC プロファイルを適用するには、[Wireless] > [Application Visibility And Control] > [AVC Profiles] に移動して [New] をクリックし、AVC プロファイルを作成します。この設定例では、teacher-AVC と student-AVC を作成します。ユーザ（ロール）teacher の特定のトラフィック（YouTube など）をマーキングして、ユーザ（ロール）student の特定のアプリケーション/トラフィック（YouTube、Facebook など）をブロック/ドロップします。ネットワーク要件に応じて独自の AVC プロファイルを作成できます。



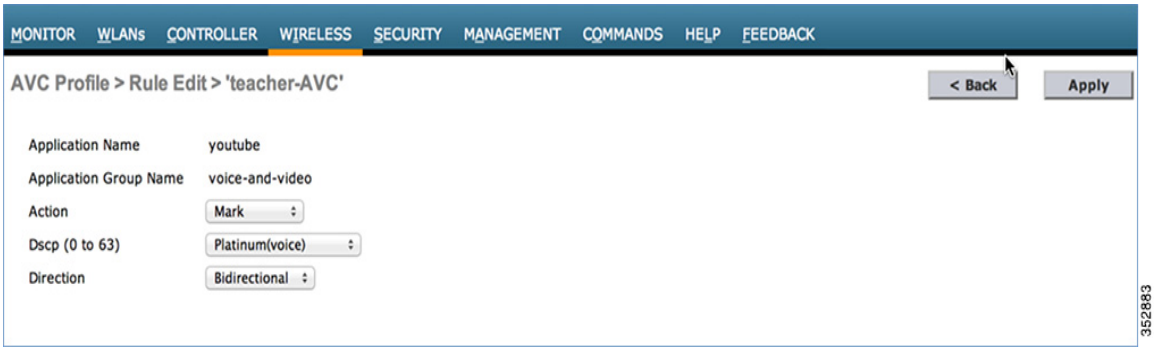
2. AVC プロファイル名を入力して [Apply] をクリックします。同様に、別のプロファイルを作成します。



3. AVC プロファイルを作成すると、上記の作成済みプロファイルが表示されます。これをクリックして、GUI でドロップ/マーク/レート制限のアクションを実行するルールを作成できます。WLC では、最大 16 個の AVC プロファイルを作成できます。



4. AVC プロファイルを作成した後は、プロファイル名をクリックして個々のプロファイルのルールを作成できます。各プロファイルで最大 32 のルールを設定できます。ルールは、ドロップ、マーク、レート制限という 3 つのアクションのいずれかを実行するように設定できます。アプリケーションのルールが設定されていない場合、デフォルトアクションは、WLAN で設定されている QOS ポリシーによる「許可」です。プロファイルのルールを作成するには、[Wireless] > [Application Visibility And Control] > [AVC Profiles] に移動して、いずれかの**プロファイル**をクリックします。



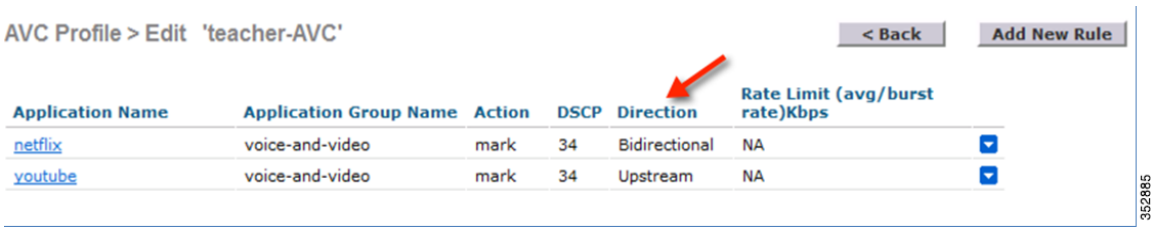
注:WLC はプロトコルパック 11.0 で 1105 のアプリケーションを分類し、アクションを実行するためのオプションを提供します。アプリケーションに対してアクションを実行するには、最初に管理者はそのアプリケーションが属するアプリケーショングループを選択して、アプリケーションリストをそのアプリケーショングループのみに絞り込む必要があります。この手順が必要な理由は、1 つのドロップダウンで 1105 のアプリケーションをすべて表示することができないためです。管理者は、[Action] を [MARK] に設定した場合、DSCP 値として「Platinum/Gold/Silver/Bronze」を選択する代わりに、[Custom] を選択することもできます。DSCP 値として [Custom] を選択するとテキストフィールドが表示され、管理者は 0 ～ 63 の範囲でカスタム DSCP 値を入力できます。

8.0 より前のリリースでは、DSCP マーキングはトラフィックの双方向にのみ適用されます。ただし、リリース 8.0 では、「Direction」という追加の設定パラメータが使用可能となり、方向（つまり、次に示すように [Upstream] または [Downstream]）に対するマーキングを指定できます。

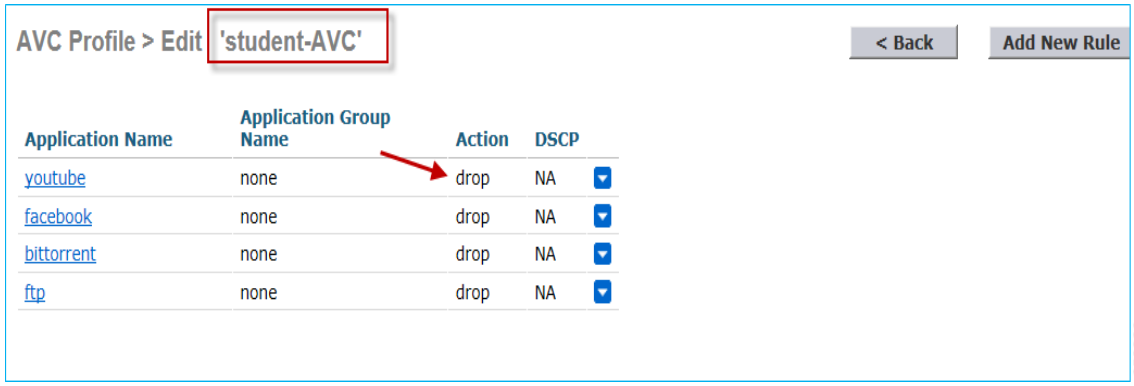
5. 適切なマーキングを選択したら、[Apply] をクリックします。アクション ルールが作成され、下の画面にキャプチャされているように表示されます。同じページで、同じ AVC プロファイルに他のルールを追加できます。1 つの AVC プロファイルで最大 32 のルールを設定できます。

同じ AVC プロファイルで別のルールを設定し、別の QoS プロファイルまたはカスタム DSCP 値で特定の方向のトラフィックをマーキングできます。

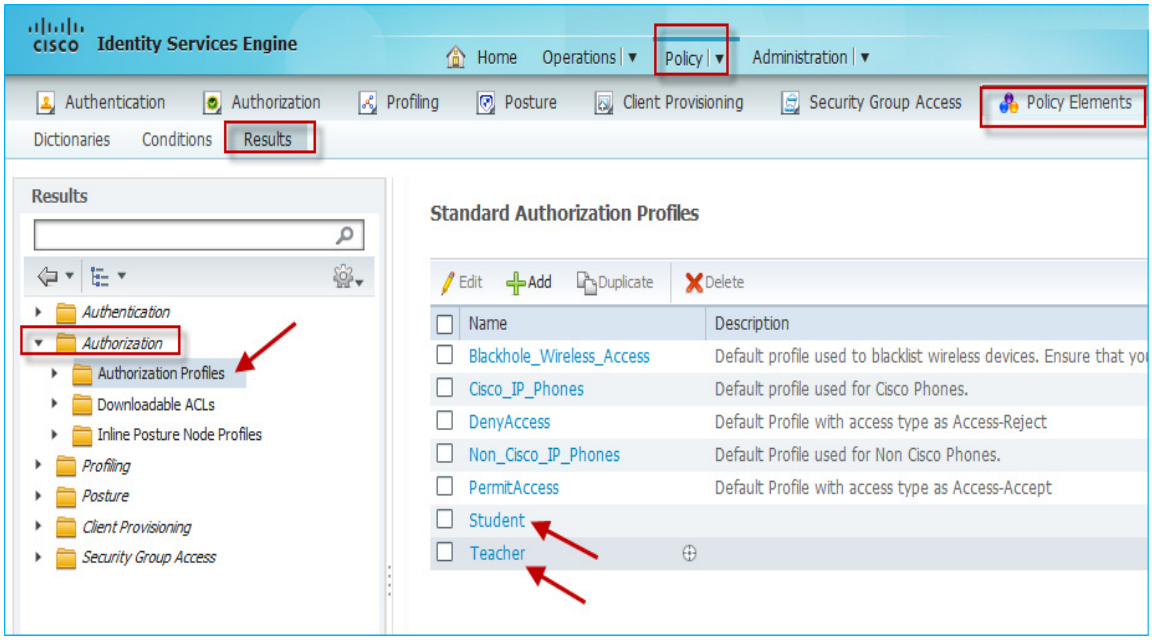
ここでは、Netflix と YouTube を AVC プロファイル「teacher-AVC」の DSCP 34（Gold）、およびそれぞれ [Bidirectional] と [Upstream] に設定された方向でマーキングするように設定しました。



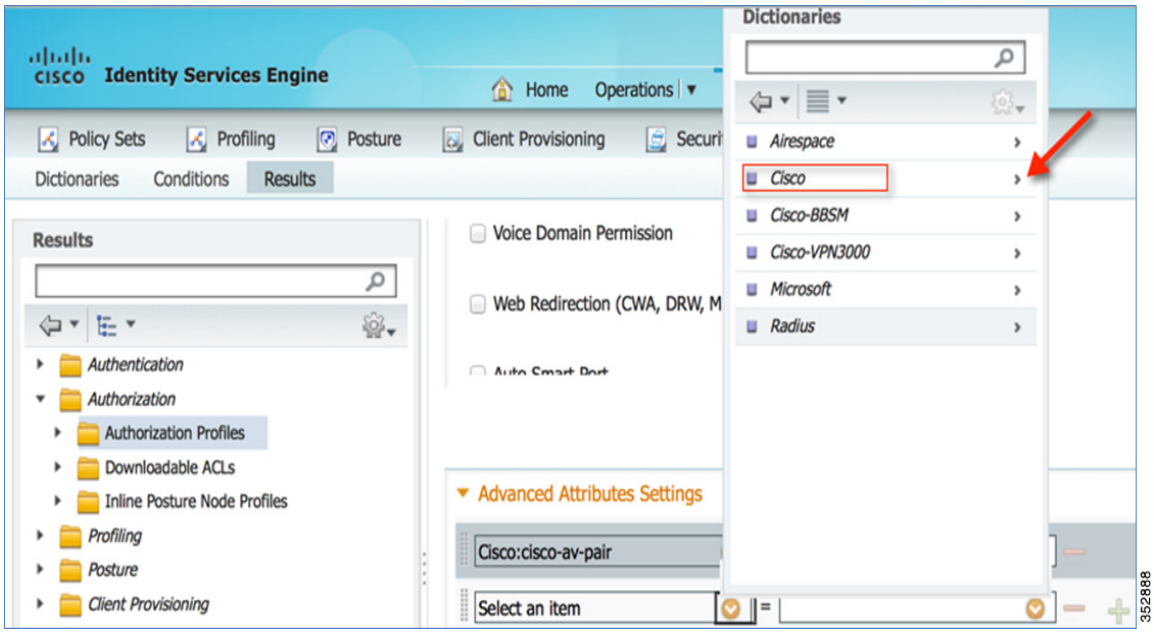
6. 同様に次の例では、ロールタイプが異なる（この設定では student）もう 1 つの AVC プロファイル（student-AVC）が表示されます。これは、Facebook、YouTube、および BitTorrent のトラフィックをドロップするように設定されています。

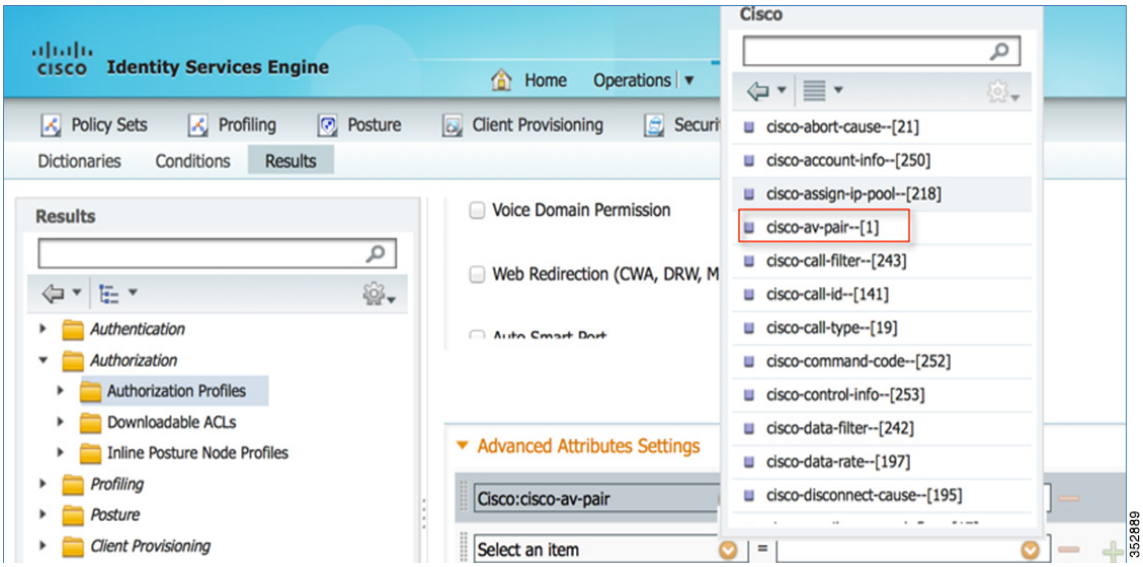


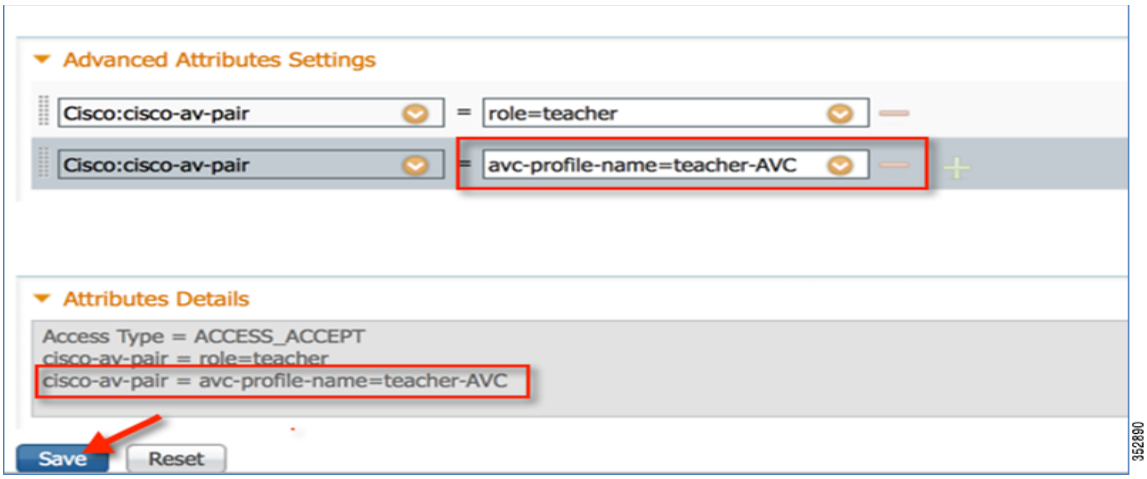
7. ここでは、ユーザまたは管理者によって、AAA サーバ（ISE/ACS/Open Radius）にユーザ（teacher と student）、デバイス（WLC）、および認証プロファイルがすでに設定されていることを前提とします。WLC で設定された AVC のプロファイルに一致するように AAA サーバを設定するには、ISE メインメニュー バーから、[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。次の例のスクリーンショットのように、設定済みのプロファイル（Student と Teacher）が表示されます。



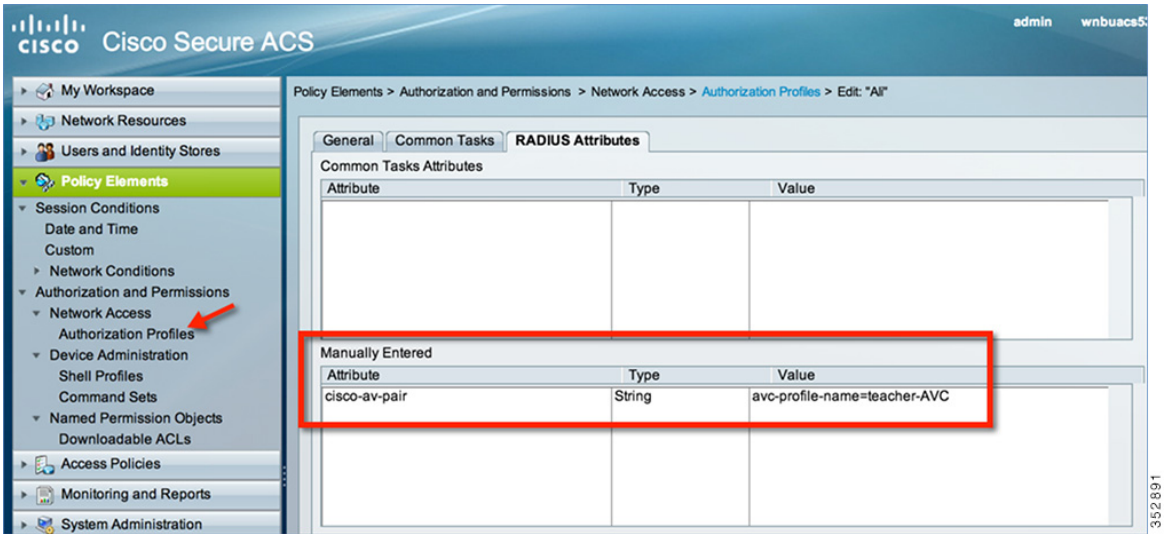
8. 以下に示すように、ロール Teacher 用に作成した認証プロファイルをクリックし、[Advanced Attributes Settings] で **cisco-av-pair=avc-profile-name=WLC で作成した AVC プロファイル名**を追加して AVC プロファイル名を設定します。







Cisco ACS を使用している場合は、[Policy Elements] > [Authorization and Permissions] > [Network Access] > [Authorization Profiles] に移動します。文字列値 **avc-profile-name=WLC で作成した AVC プロファイル名**に一致する **cisco-av-pair** を追加します。



同様に、student の認証プロファイルも設定します。設定が完了したら、teacher のクレデンシャルでワイヤレスクライアントを 802.1x WLAN に接続できます。Netflix と YouTube にアクセスできるようになります。

student ロールでワイヤレスクライアントを同じ 802.1x WLAN に接続しても、クライアントで YouTube のビデオを再生することはできません。また、クライアントで Facebook ページにアクセスして Facebook アカウントから YouTube ビデオを開こうとしても、YouTube ビデオは再生されません。

YouTube と Facebook の両方が AVC プロファイル「Student-AVC」でブロックされているため、student ロールのクライアントではブラウザ経由でも、YouTube アプリケーションを使用しても、他の Web サイトからも YouTube ビデオにアクセスできず、Facebook にアクセスすることもできません。

一方、クライアントが Teacher クレデンシャルを使ってログインした場合は、トラフィックがマーキングされるだけで、アプリケーションはドロップされません。

ポリシーが適用されているかどうかを確認するには、WLC の CLI プロンプトで次のコマンドを実行します。

`show client detail` ***`mac_address`*** を実行し、下にスクロールして適用されているプロファイルを確認します。

```
(POD2-WLC) >show client detail 18:20:32:bd:52:b7
Client MAC Address.................................. 18:20:32:bd:52:b7
Client Username .................................... teacher1
AP MAC Address...................................... 3c:ce:73:38:24:70
AP Name............................................. POD2-AP3600
AP radio slot Id.................................... 1
Client State........................................ Associated
Client NAC OOB State................................ Access
Wireless LAN Id..................................... 1
Hotspot (802.11u)................................... Not Supported
BSSID............................................... 3c:ce:73:38:24:7f
Connected For ...................................... 8288 secs
Channel............................................. 64
IP Address.......................................... 10.10.21.200
Gateway Address..................................... 10.10.21.1
Netmask............................................. 255.255.255.0
Association Id...................................... 1
Authentication Algorithm............................ Open System
Reason Code......................................... 1
Status Code......................................... 0
Client CCX version.................................. No CCX support
Re-Authentication Timeout........................... 686
QoS Level........................................... Silver

--More-- or (q)uit
Avg data Rate....................................... 0
Burst data Rate..................................... 0
Avg Real time data Rate............................. 0
Burst Real Time data Rate........................... 0
802.1P Priority Tag................................. disabled
CTS Security Group Tag.............................. Not Applicable
KTS CAC Capability.................................. No
WMM Support......................................... Enabled
  APSD ACs.......................................... BK  BE  VI  VO
Power Save.......................................... ON
Current Rate........................................ m7
Supported Rates..................................... 6.0,9.0,12.0,18.0,24.0,36.0,
    ................................................ 48.0,54.0
Mobility State...................................... Local
Mobility Move Count................................. 0
Security Policy Completed........................... Yes
Policy Manager State................................ RUN
Policy Manager Rule Created......................... Yes
Audit Session ID.................................... 0a0a1402000000006752afa3c3
AAA Role Type....................................... teacher
Local Policy Applied................................ none
IPv4 ACL Name....................................... none
FlexConnect ACL Applied Status...................... Unavailable
```

352892

AVC を通じたアプリケーションのレート制限

このリリースでは、WLC の CLI で次のコマンドを実行して、レート制限するアプリケーションを 3 個だけ設定できます。

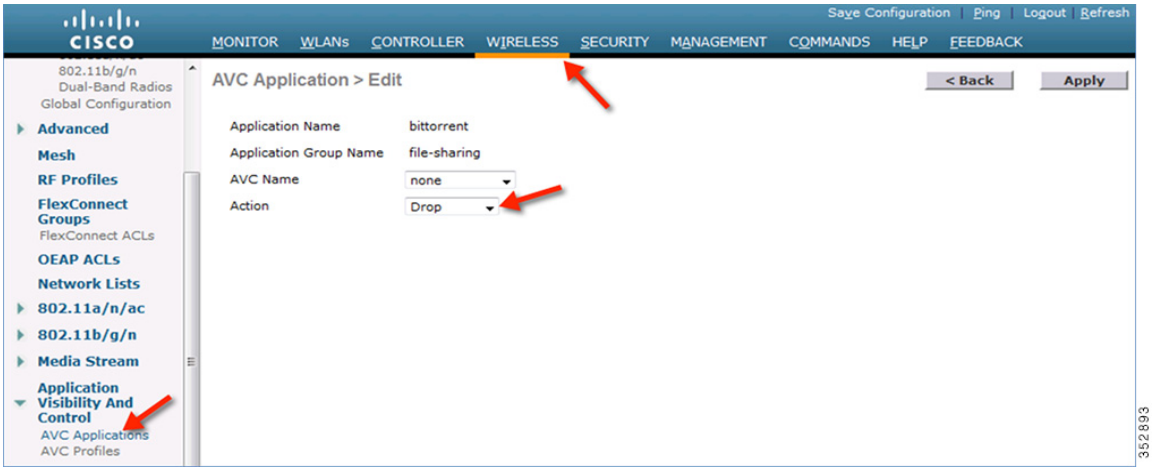
(WLC) >config avc profile <prof-name> {add|remove} rule application <app-name> {drop|mark <dscp-value>|ratelimit <avg_rate> <burst_rate>}

注:最小レート制限値は、0 Kbps ～ 2147483647 Kbps の範囲で設定できます。

次の設定例は、BitTorrent アプリケーションを使用する場合のプロファイル「student-AVC」で実行されます。

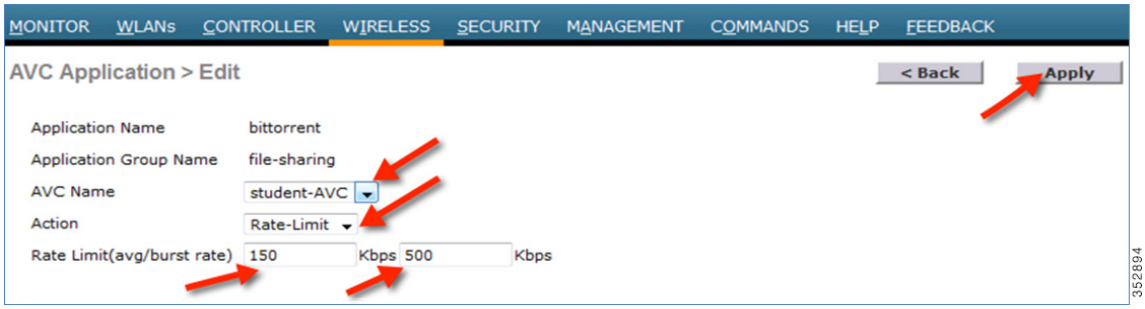
(WLC) >config avc profile student-AVC rule add application bittorrent ratelimit 150 500

同様に WLC の GUI でも、レート制限を適用するアプリケーションを選択し、[Action] ドロップダウンリストから [Rate-Limit] を選択してレート制限を設定できます。

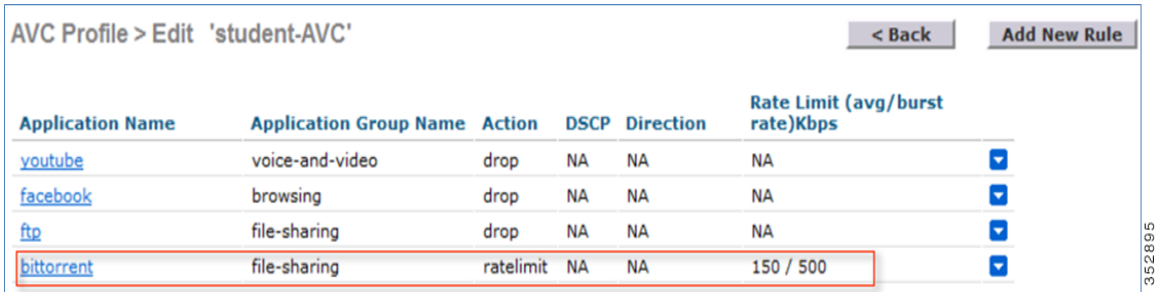


これにより、ユーザはレート制限する必要がある目的のアプリケーションに対して、平均レートとバーストレートを設定できるようになります。0 ～ 2147483647 の任意の値を Kbps 単位で割り当てることができます。レート制限が設定されたら、ユーザは [AVC Name] でレート制限の適用先を選択し、[Apply] をクリックします。

この例では、BitTorrent アプリケーションが、150 Kbps に設定された平均レート、および 500 Kbps に設定されたバーストレートでレート制限され、これが AVC プロファイルの student-AVC に適用されます。



BitTorrent アプリケーションの [Action] 列に [ratelimit] と表示され、レート制限の平均レート値とバーストレート値が示されます。



NBAR の仕様（AVC フェーズ 3）

- NBAR エンジン 13 および PP 11.0 は、1105 のさまざまなアプリケーションをサポートできます。
- ドロップ、マーク、レート制限の 3 つのアクションは、分類されたどのアプリケーションにも使用可能です。
- WLC では、最大 16 個の AVC プロファイルを作成できます。

- 各 AVC プロファイルには最大 32 のルールを設定できます。
- 同じ AVC プロファイルを複数の WLAN にマッピングできます。ただし、1 つの WLANが保持できるのは、1 つの AVC プロファイルのみです。
- WLC には、NetFlow エクスポータおよびモニタを 1 つずつのみ設定できます。
- NBAR 統計情報は GUI の上位 30 のアプリケーションについてのみ表示されます。CLI を使用すると、すべてのアプリケーションの統計情報を表示できます。
- NBAR は、中央のスイッチング用に設定されている WLAN でのみサポートされます。
- WLAN にマッピングされた AVC プロファイルにマークアクションのルールがある場合、そのアプリケーションは、WLAN に設定された QoS プロファイルをオーバーライドする AVC ルールに設定された QoS プロファイルに準じます。
- 方向マーキングは、特定のアプリケーションの双方向、アップストリームまたはダウンストリームのいずれかにのみ適用できます。
- 現在、レート制限は、3 つのアプリケーションにのみ適用できます。
- WLC 上の NBAR エンジンによってサポートまたは認識されていないアプリケーションは、UNCLASSFIED トラフィックのバケット配下でキャプチャされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドは 8.0 リリースでサポートされています。
- AVC プロファイルを WLAN ごとに設定し、ユーザ単位で適用できます。
- NBAR は vWLC および SRE WLC ではサポートされていません。

ローカルポリシーにアタッチされる AVC プロファイル

リリース 8.0 では、AVC プロファイルを特定のデバイスタイプのクライアントのローカルポリシーにマッピングできます。各ローカルポリシーを、AAA オーバーライドに基づく異なる AVC/mDNS プロファイル名を使用して設定し、同じ WLAN 上のプロファイルで許可されていないサービスをポリシーが使用することを制限できます。

WLC のプロファイリングとポリシーエンジンの概要

シスコには、現在、ISE を通じてデバイス ID、オンボーディング、ポスチャ、およびポリシーを提供する豊富な機能セットが用意されています。WLC のこの新しい機能では、HTTP、DHCP などのプロトコルに基づいてデバイスのプロファイリングを実行し、ネットワーク上のエンドデバイスを識別します。デバイスベースのポリシーを設定し、ネットワーク上のユーザ単位またはデバイスポリシー単位でそれらを適用できます。WLC では、ユーザ、デバイスエンドポイント、およびデバイスごとに適用可能なポリシーに基づく統計情報も表示されます。

BYOD（Bring Your Own Device）では、この機能がネットワーク上のさまざまなデバイスの理解に影響します。この機能を使うことで、WLC 自身で小規模に BYOD を実装できます。

範囲と目的

ここでは、AireOS 8.0 コードを実行している Cisco WLC でプロファイリングとポリシーを設定して実装します。

プロファイリングとポリシーの適用は、2 つの異なるコンポーネントとして設定します。WLC での設定は、ネットワークに参加するクライアントに固有の定義済みパラメータに基づいています。対象のポリシー属性は次のとおりです。

a. Role：ユーザが属するユーザタイプまたはユーザグループを定義します。

   たとえば、学生、従業員など

b. Device：デバイスのタイプを定義します。

たとえば、Windows マシン、スマートフォン、iPad や iPhone などの Apple デバイス

c. Time of day：エンドポイントがネットワーク上で許可される時間を設定で定義できます。

d. EAP Type：クライアントが接続されている EAP 方式を確認します。

上記のパラメータはポリシー一致属性として設定できます。WLC でエンドポイントごとに上記のパラメータとの一致が検出されると、ポリシーが適用されます。ポリシーの適用は次のようなセッション属性に基づいています。

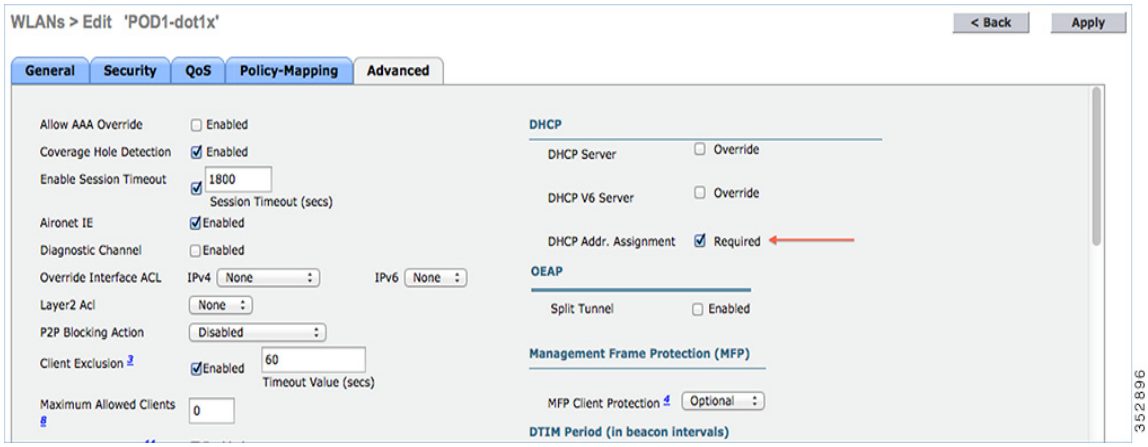
- VLAN
- ACL
- セッションタイムアウト
- QoS
- スリープ状態のクライアント
- FlexConnect ACL
- AVC プロファイル（8.0 リリースで追加）
- mDNS プロファイル（8.0 リリースで追加）

ユーザはこれらのポリシーを設定して、指定したポリシーをエンドポイントに適用できます。ワイヤレスクライアントは、MAC OUI、DHCP、および HTTP ユーザエージェントに基づいてプロファイリングされます（HTTP プロファイリングを成功させるためには有効なインターネットが必要）。WLC は、これらの属性と事前定義の分類プロファイルを使用してデバイスを識別します。

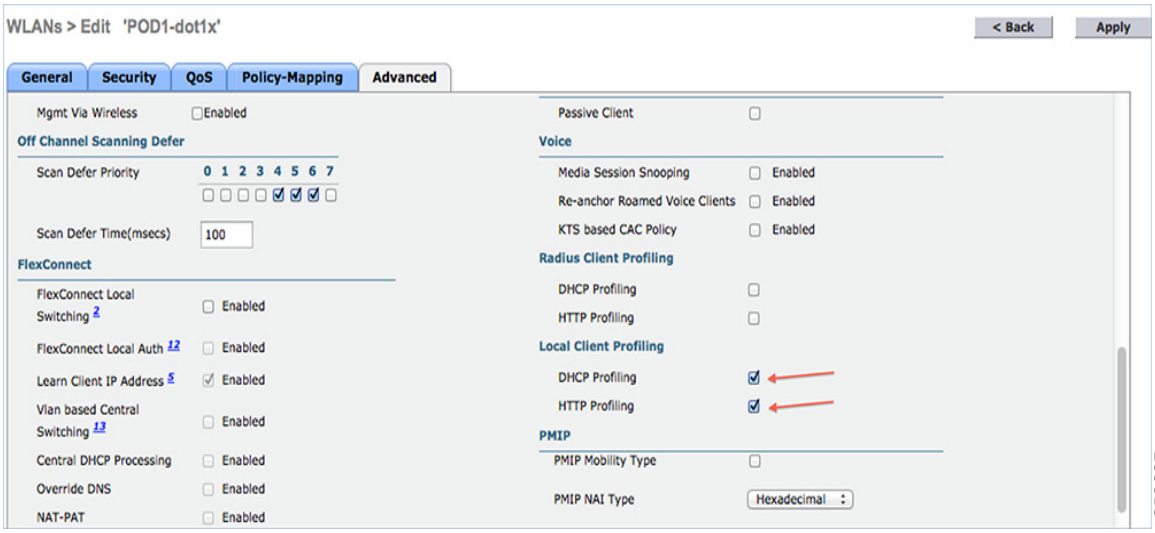
プロファイリングおよびポリシーの設定

次の手順を実行します。

1. WLAN でデバイスプロファイリングを設定するには、ネイティブプロファイリングとポリシーを実装する対象となる特定の WLAN に移動して、[Advanced] タブをクリックします。[Allow AAA Override] が有効になっている場合は、無効にします。[DHCP] 領域で、[DHCP Addr. Assignment] の [Required] チェックボックスをオンにします。

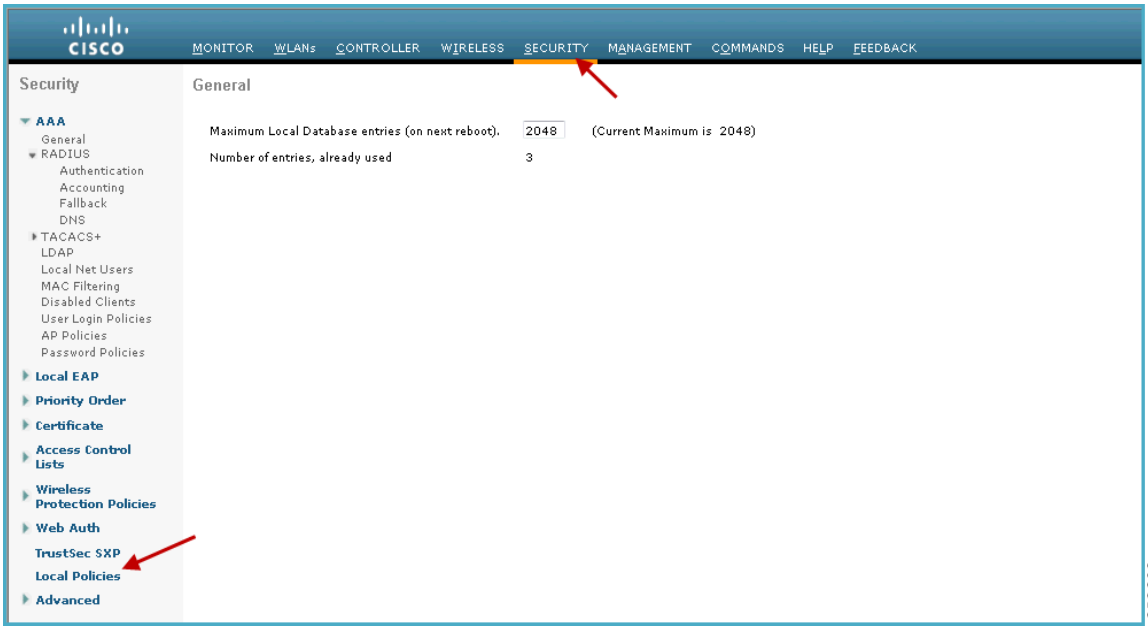


2. DHCP の [Required] オプションを有効にした後は、下にスクロールし、[Local Client Profiling] 領域で、[DHCP Profiling] と [HTTP Profiling] を有効にして（無効になっている場合）[Apply] をクリックします。



WLC GUI から WLAN でポリシーを作成

3. プロファイルを設定したら、ローカルポリシーの作成と WLAN での適用に進みます。WLC メニューバーで、[Security] > [Local Policies] に移動すると、ポリシーリストが表示されます。



4. [Local Policy List] で、[New] をクリックして、ポリシー名を作成します。この例では、**teacher-LP** をポリシー名として使用していますが、任意の名前を使用して独自のポリシーを定義することもできます。

ポリシー名を設定したら、[Role]、[EAP Type]、[Device Type] を照合するポリシーを作成できます。また、一致条件に関連する必要なアクションを定義できます。

ここでは、[User Role] と [Device Type] を [Match Criteria] に使用していますが、必要に応じて任意のタイプを使用できます。

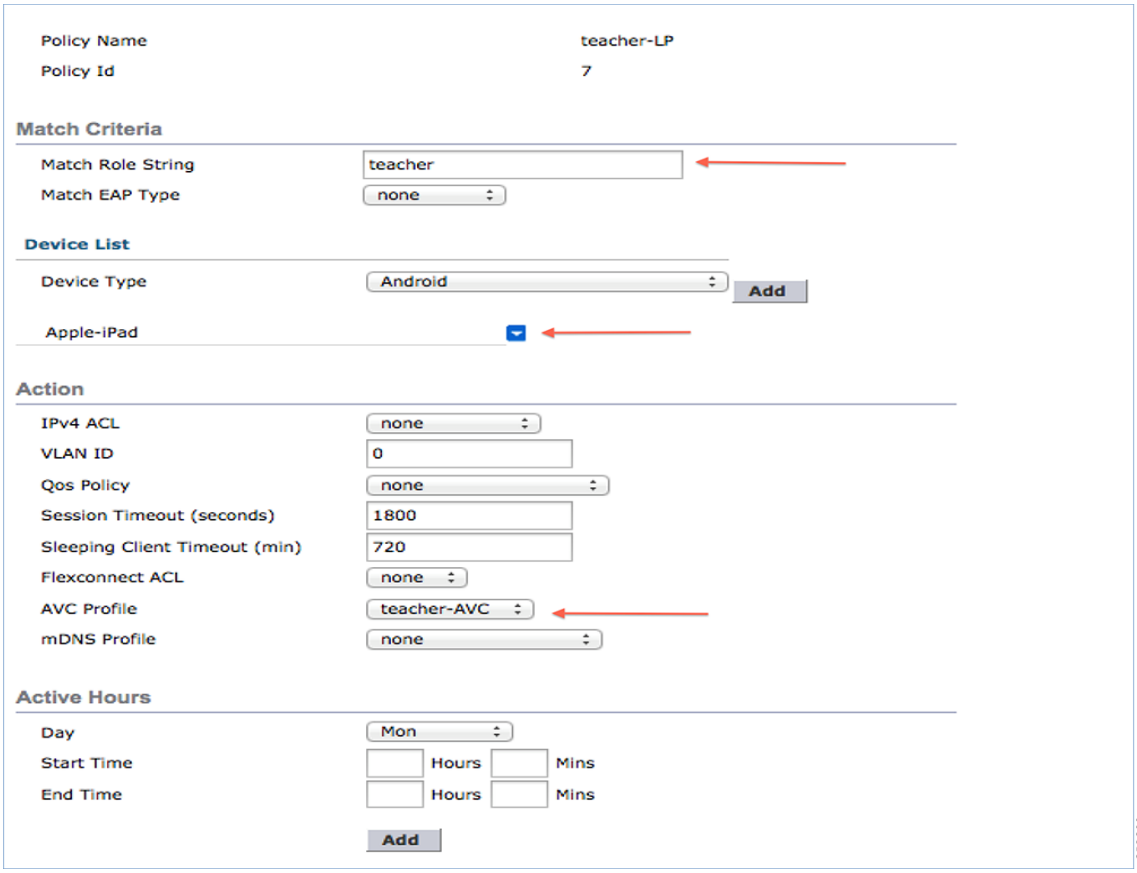
注:[Match Role string] が AAA で定義されたロール名と同じであることを確認してください。この例では、「teacher」と定義されています。

5. [User Role] を入力し、[Apply] をクリックします。ここではロール名「teacher」が例として使用されています。
6. ユーザデバイスに基づいてポリシーを適用するには、[Device List] 領域で、ポリシーを適用するデバイスタイプを [Device Type] ドロップダウンリストから選択し、[Add] をクリックします。

ここで、[Match Criteria] に対し、デバイスタイプとして [Apple-iPad] を使用しています。Apple-iPhone やその他の Apple デバイスも同様に [Device Type] ドロップダウンリストから追加できます。

注:デバイスタイプを照合しない場合は、[Device Type] オプションを設定しないでください。

7. 適切なアクションを適用するには、[Action] のパラメータから選択して、ポリシーを適用します。最後のセクションで定義されている AVC プロファイルを選択します。

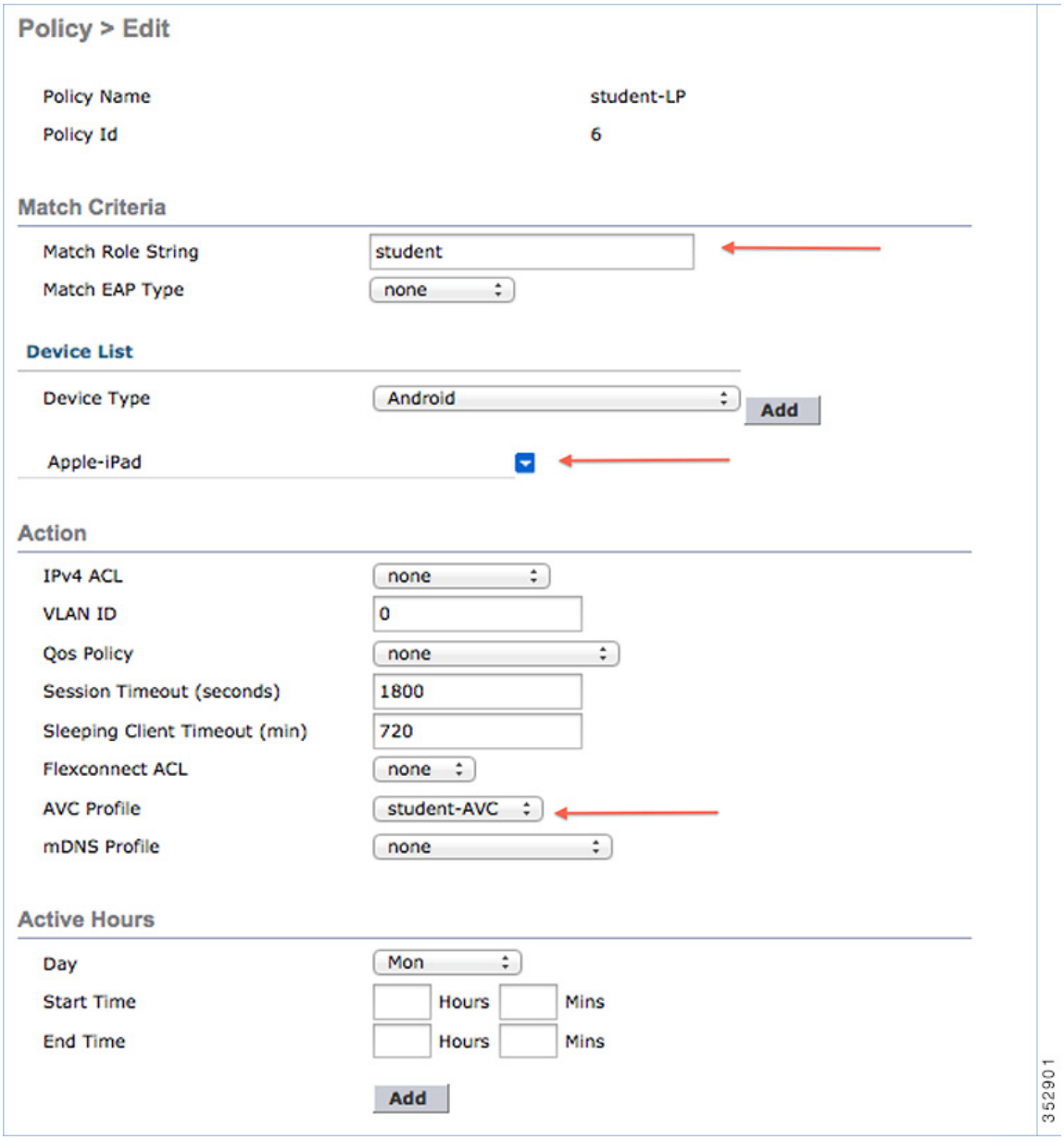


8. ユーザは、1 つ以上のローカルポリシーを作成し、「student-LP」の学生に適用できます。

注：[Match Role string] が AAA/Radius サーバで定義されたロール名と同じであることを確認してください。

ユーザデバイスに基づいてポリシーを適用するには、[Device List] 領域の [Device Type] ドロップダウンリストから、ポリシーを適用するデバイスタイプ（Apple-iPad）を選択し、[Add] をクリックします。

適切なアクションを適用するには、[Action] 領域のパラメータから選択して、ポリシーを適用します。最後のセクションで定義されている AVC プロファイル（student-AVC）を選択します。

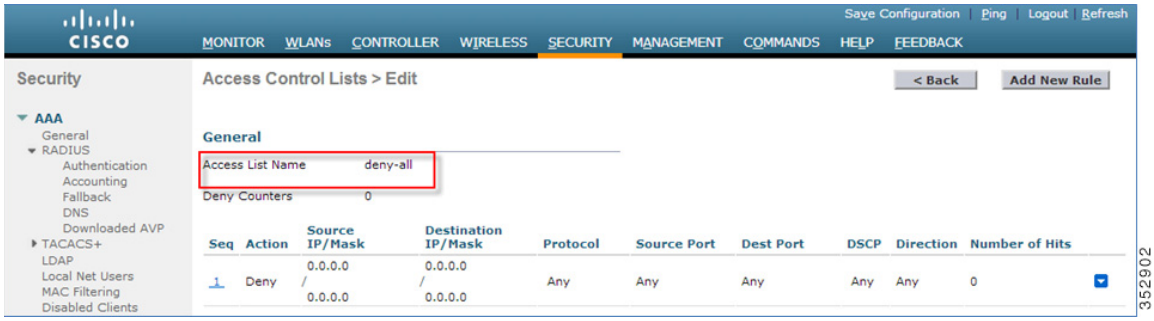


9. その他のデバイスのデフォルトのローカルポリシーを作成します。

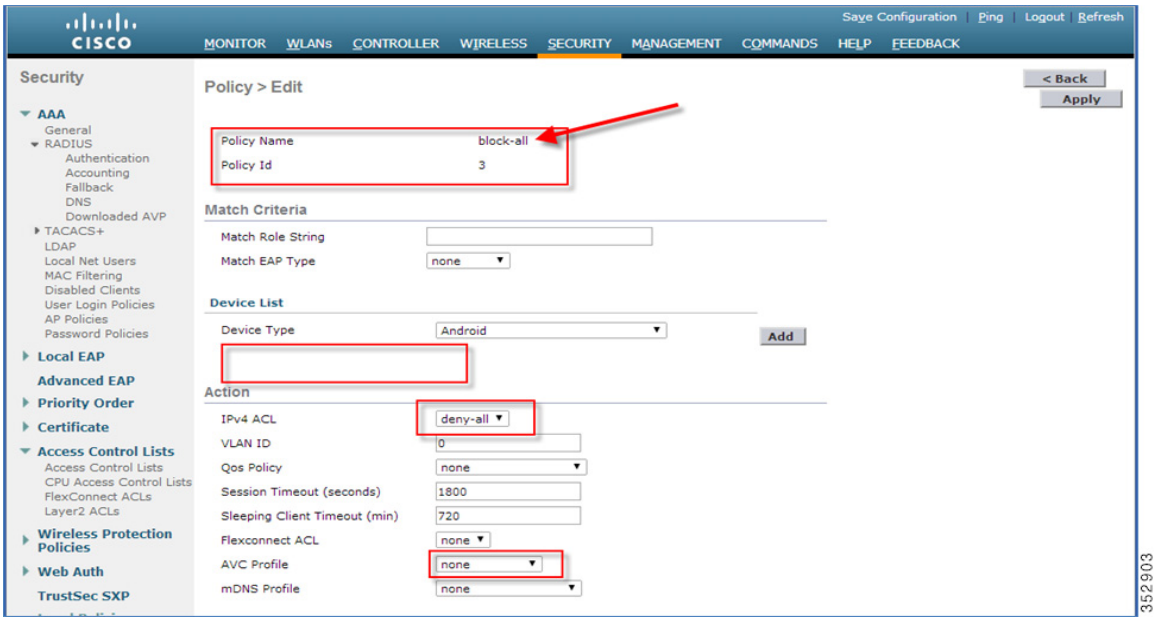
   ローカルポリシーに他の ACL が適用されていない場合、すべてのポリシーの最終フィルタ機能が [Allow all] なので、Apple-iPad 以外のすべてのデバイスはアプリケーションにアクセスできます。

   Apple-iPad を除くすべてのデバイスのすべてのアプリケーションをブロックするには、最後の手段として、[deny all] ACL を作成してローカルポリシーに適用し、WLAN にそのポリシーを適用します。次のスクリーンショットの設定例を参照してください。

   すべての IPv4 フローをブロックする ACL を作成します。



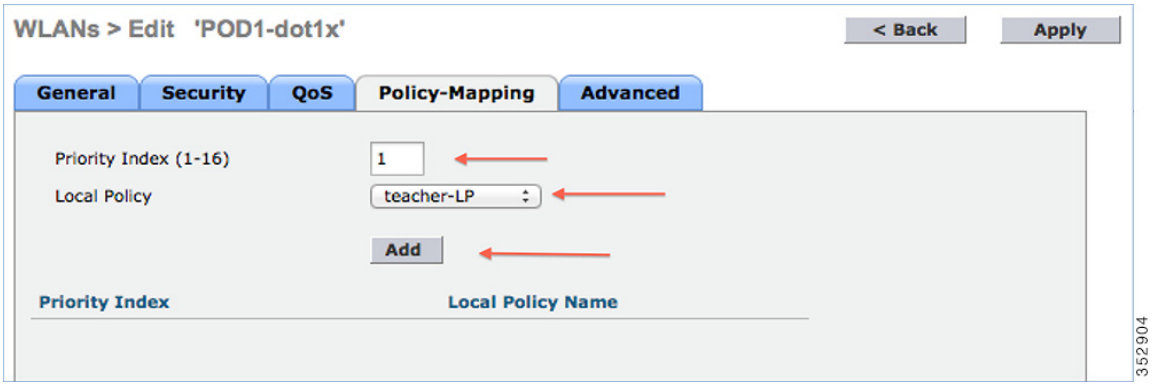
ローカルポリシー **Block-all** を作成して [deny all] ACL をこれに適用します。デバイスロールやプロファイルは選択しないでください。



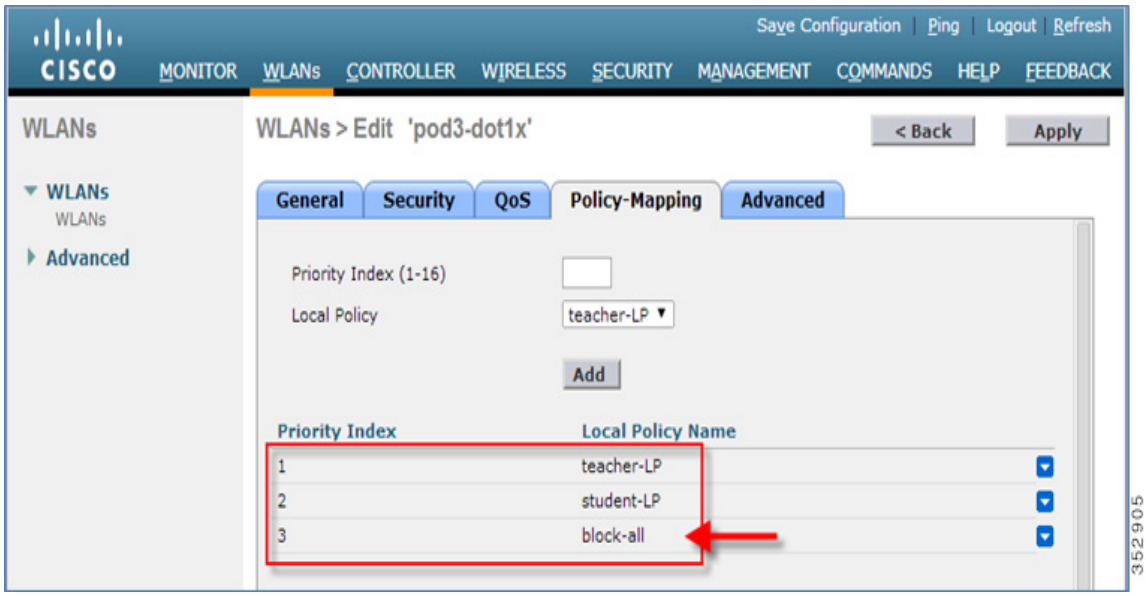
WLAN でのポリシーのマッピング

1. WLC メニューバーから [WLANs] に移動し、ポリシーを設定したい [WLAN ID] をクリックします。WLAN の [Edit] メニューから [Policy-Mapping] タブをクリックします。

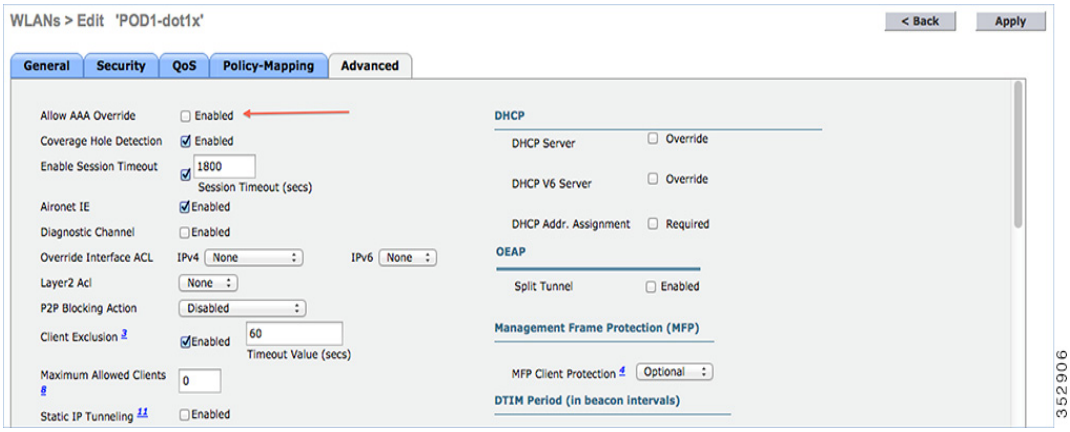
[Priority Index] で、1 ～ 16 から任意の値を設定します。[Local Policy] ドロップダウンリストから、すでに作成したポリシーを選択します。WLAN にポリシーを適用するには、[Add] をクリックします。ポリシーが WLAN にマッピングされ、[Policy Name] の下に表示されます。



2. 適切なポリシーを WLAN の [Policy-Mapping] に追加します。

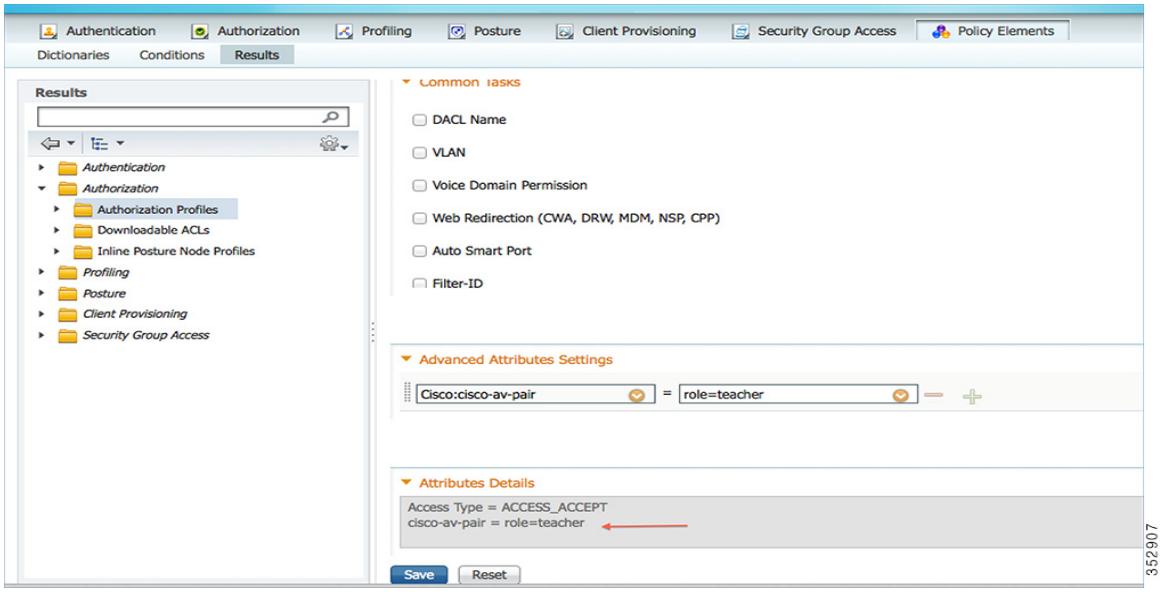


3. [Advanced] タブで、[Allow AAA Override] が有効になっている場合は無効にします。

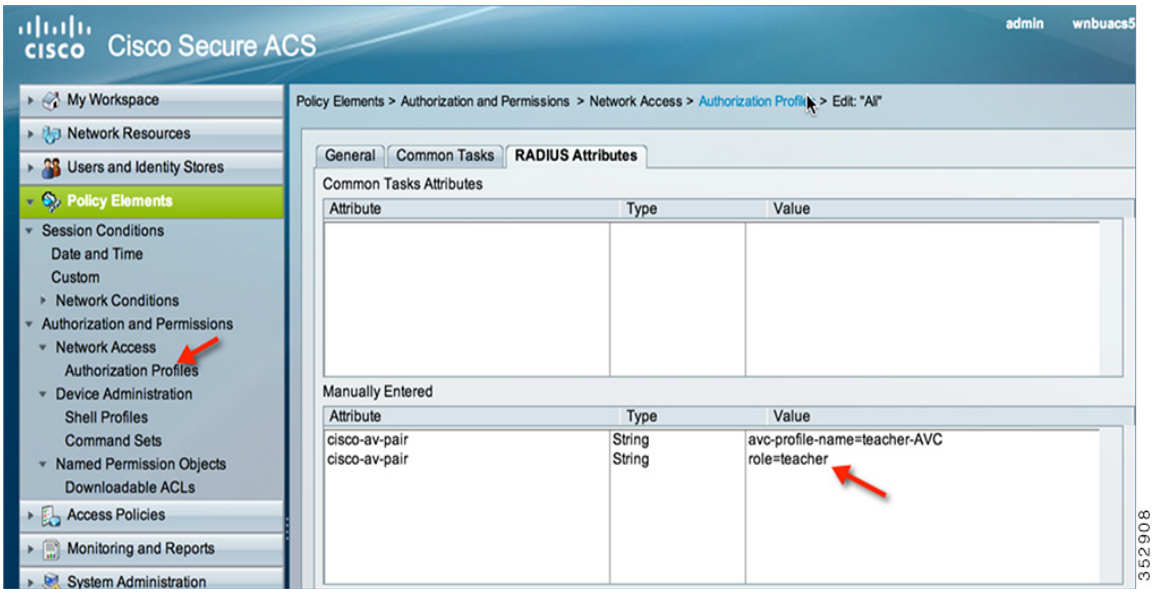


4. AAA ロールが正しく設定されていることを確認します。つまり、AAA サーバでのロール名はローカルポリシーで定義されている [Role String] と一致する必要があります。下記は、Cisco ISE サーバと Cisco ACS の例です。

ISE:

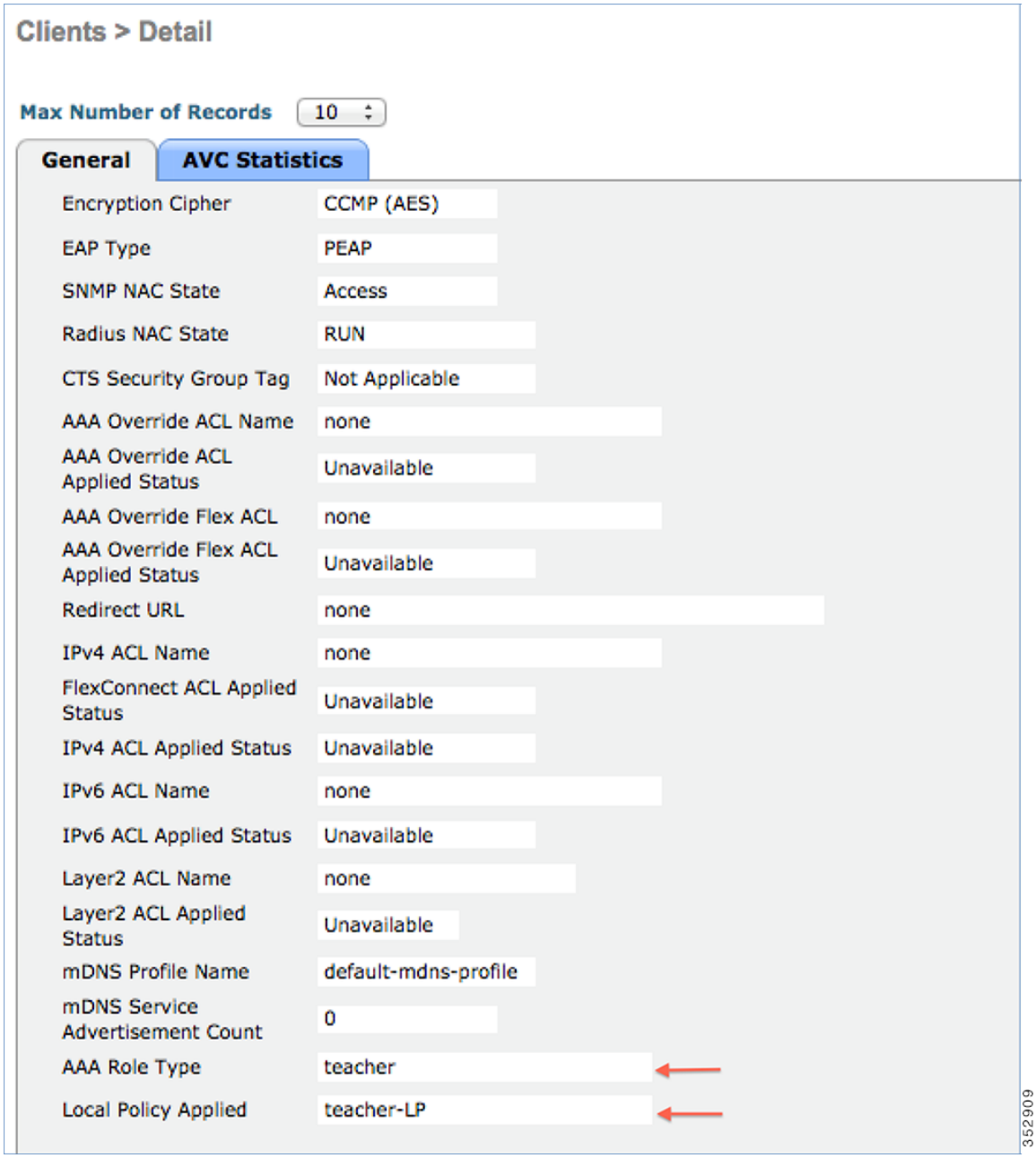


ACS：



Apple iPad を介して teacher のクレデンシャルで SSID に関連付けたクライアントは、インターネット、および AVC プロファイル設定ごとに異なるアプリケーションにアクセスできます。ユーザが Apple iPad 以外のデバイスから接続しようとしても、インターネットにアクセスすることはできません。

WLC の GUI でポリシーの適用を確認するには、[Monitor] > [Clients] に移動し、[Client MAC address] をクリックします。



WLC の CLI プロンプトでポリシーの適用を確認するには、次のコマンドを実行します。

show client detail *mac_address* を実行し、一番下までスクロールして適用されているプロファイルを確認します。

```
AAA Role Type..................................... teacher
Local Policy Applied.............................. teacher-LP
IPv4 ACL Name..................................... none
FlexConnect ACL Applied Status.................... Unavailable
IPv4 ACL Applied Status........................... Unavailable
IPv6 ACL Name..................................... none
IPv6 ACL Applied Status........................... Unavailable
Layer2 ACL Name................................... none
Layer2 ACL Applied Status......................... Unavailable
Client Type....................................... SimpleIP
mDNS Status....................................... Enabled
mDNS Profile Name................................. default-mdns-profile
No. of mDNS Services Advertised.................. 0
Policy Type....................................... WPA2
Authentication Key Management..................... 802.1x
Encryption Cipher................................. CCMP (AES)
Protected Management Frame ....................... No
Management Frame Protection....................... No
EAP Type.......................................... PEAP
Interface......................................... management
```

352910

WLC で AVC ポリシーの適用を確認する方法は次のとおりです。

AVC Profile Name: ..... teacher-AVC

student のクレデンシャルで SSID への接続を試行すると、適用されている別のポリシー（student-AVC）が表示されます。クライアントデバイスが Apple iPad でない場合は、ネットワークにアクセスできません。

ネイティブプロファイリングに関する制限事項

- WGB 背後の有線クライアントはプロファイリングされず、ポリシーアクションは実行されません。
- WLAN ごとに設定できるポリシーは 16 のみで、グローバルに 64 のポリシーを割り当てることができます。
- ポリシーアクションは、L2 または L3 認証が完了するか、デバイスから HTTP トラフィックが送信されてデバイスがプロファイリングされた場合に実行されます。特定のシナリオでは、プロファイリングおよびポリシーアクションが 1 つのクライアントで複数回発生します。
- このリリースでは、IPv4 クライアントのプロファイリングのみがサポートされます。
- WGB 有線クライアントでは HTTP プロファイリングがサポートされていないため、WGB 有線クライアントのプロファイリングはサポートされません。

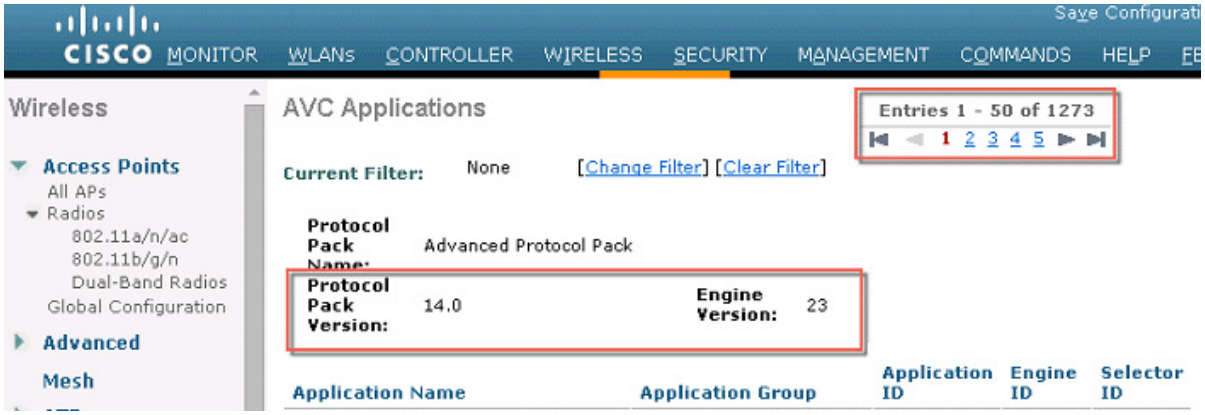
まとめ

- デフォルトでは、すべての WLAN でプロファイリングが無効になっています。
- 各 WLAN に、マッピング済みのプロファイリングポリシーを設定できます。
- 各ポリシーに、照合する Role Type、Device Type、EAP type を設定して、関連付けられているポリシーインデックスをマッピングできます。
- ポリシーインデックスは、最初に照合する必要があるポリシーを示します。
- 対応するポリシー名は、ポリシーインデックスから推定されます。
- ポリシーマッチングは最初にポリシーが一致した時点で終了し、対応するポリシーアクション属性がクライアントごとに設定されます。
- クライアントごとにポリシーを適用する順番は、セキュリティタイプに基づきます。

CUWN リリース 8.2 の AVC フェーズ 4

プロトコルパックと NBAR エンジンの更新

リリース 8.2 までは、集中型 AVC をサポートするために NBAR エンジン（16）が WLC に統合され、プロトコルパック（PP）バージョン 12 までがサポートされています。リリース 8.2 では、改善された新しい NBAR エンジン 23 とプロトコルパック 14 が導入されました。新しいバージョンを使用すると、顧客はコントローラのパフォーマンスにほとんど影響を与えずに、Netflix、Jabber、Bittorrent、YouTube など、1273 のアプリケーションをより高い精度で確実に分類できます。プロトコルパック 14 には NBAR エンジン 23 が必要であり、前の WLC リリースで以前にリリースされたバージョンの NBAR では機能しないことにも注意してください。PP バージョン 15 がリリースされて CCO に掲載された場合は、NBAR エンジン 23 で動作します。



リリース 8.2 の NetFlow サポート

IP トラフィックフローでは、一連のパケットが、送信元/宛先 IP アドレス、トランスポートポート、方向などの共通の属性を伴い、ネットワークデバイスを通過します。ワイヤレスフローのその他の共通属性としては、SSID や AP MAC があります。共通の属性を持つこれらのパケットがフローに集約され、Netflow コレクタにエクスポートされます。8.2 より前のリリースでは、コントローラがエクスポートした Netflow データは PI（Prime Infrastructure）によってのみ分析され、サードパーティ製の Netflow コレクタとの互換性はありませんでした。

リリース 8.2 では、強化された Netflow レコードエクスポータが導入されています。新しい Netflow v9 では、17 の異なるデータレコード（RFC 3954 で定義されている）が、StealthWatch などの外部のサードパーティ製 Netflow コレクタに送信されます。強化されたフローレコード データ エクスポート機能は、WLC 5520、8510、8540 に追加されています。

8.2 より前のリリースでは、コントローラの Netflow 機能によって、クライアントの IP アドレス、SSID、アプリケーションの統計情報だけが送信されていました。その場合、Cisco Prime などの互換性のある Netflow コレクタではアプリケーションの統計情報を表示できましたが、5 タプルの完全なフロー情報は得られず、5 タプルを必要とする多くのサードパーティ製 Netflow コレクタとの互換性も確保されていませんでした。

8.2 より前のリリースによって WLC がエクスポートする現行の Netflow レコードでは、次のフィールドのみサポートされています。

- applicationTag
- ipDiffServCodePoint
- octetDeltaCount

- packetDeltaCount
- postIpDiffServCodePoint
- staIPv4Address
- staMacAddress
- wtpMacAddress

リリース 8.2 で新たに導入されたフローレコードエクスポータは、次のフローデータレコードをサポートしています。

- Application Tag
- クライアントの MAC アドレス
- AP MAC アドレス
- WlanID
- 送信元 IP
- 宛先 IP
- 送信元ポート
- 宛先ポート
- プロトコル
- フロー開始時刻
- フロー終了時刻
- 方向
- パケット数
- バイト数
- VLAN ID：管理/ダイナミック
- TOS：DSCP 値
- Dot1x ユーザ名

Netflow の配置に関する考慮事項

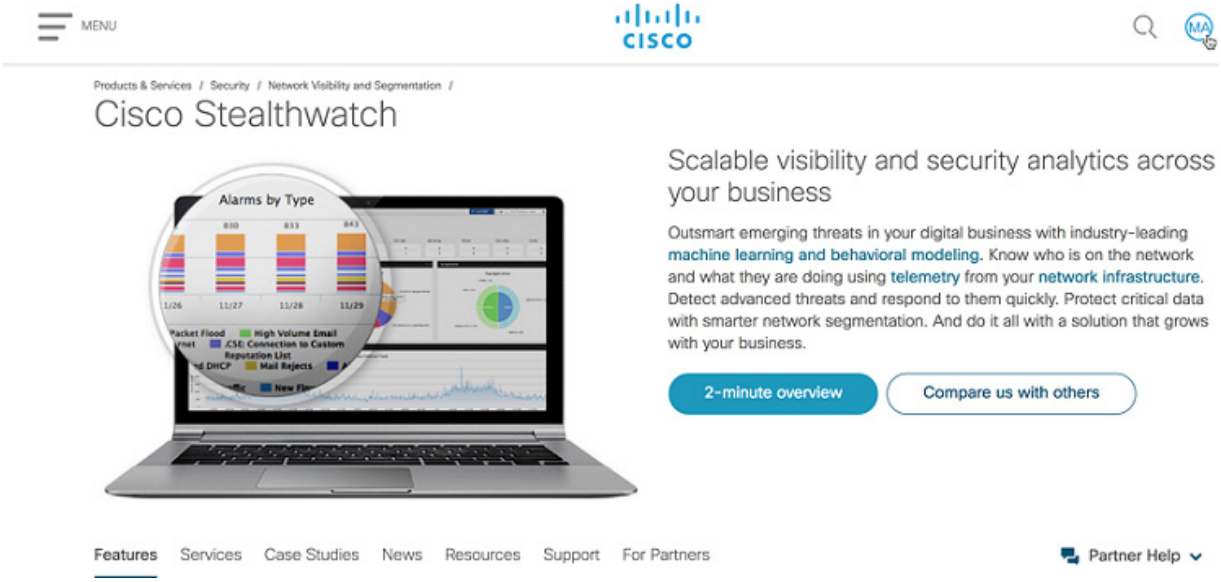
- WLC では、1 つのモニタとエクスポータのみサポートされています。
- WLC では、コントローラごとに 1 つのタイプの Netflow レコードのみ、グローバルにサポートされます。
- フローレコードは直接エクスポートされ、コントローラには表示されません。
- 現在のアプリケーションの可視性の統計情報は、引き続きコントローラに表示されます。
- モニタのパラメータの変更により、WLAN の無効化と有効化が必要になります。
- 新しいレコードは、8510、5520、および 8540 コントローラでのみサポートされます。
- 2500、5508、7500、および WiSM2 コントローラはサポートされません。
- Netflow 統計情報は 30 秒間隔で送信されます（ユーザ設定不可。現在の値は 90 秒）。

- Netflow レコードは、新しいフローレコードを持つ未分類のアプリケーションにも送信されます。
- Netflow は、その WLAN で AVC を有効にする際に送信されます。
- IPv6 トラフィックは、リリース 8.2 の Netflow ではサポートされていません。
- 初期テンプレートを送信する Netflow は、コントロールプレーンから送信されます。
- サービスポートでの Netflow のエクスポートはサポートされていません。

評価を目的とした StealthWatch ソフトウェアの入手

ソフトウェアは次に示す URL から Web ダウンロードできます:
https://www.Stealthwatch .com/stealthwatch-evaluation-application

1. Stealth Watch Evaluation にサインアップして、ソフトウェアをダウンロードします。



WLC での Netflow 設定

8.2 より前のリリースでは、WLC での Netflow 設定は、固定レコード ipv4_client_app_flow_record を Netflow モニタに関連付けることで行っていました。現在ではこの方法に加えて、ipv4_client_src_dst_flow_record という新しい固定レコードがサポートされています。これは以下に示す CLI と GUI でも使用できます。

注: コントローラで使用できる Netflow エクスポータは 1 つだけであるため、新旧のレコード形式のいずれかを使用することになります。

CLI からの設定

設定の変更内容

```
(Cisco Controller) > config flow add monitor <My_Netflow_Monitor record>
```

CLI からの設定手順

```
config flow create monitor <My_Netflow_Monitor>
config flow create exporter My_Netflow_Exporter A.B.C.D port 2055
config flow add monitor My_Netflow_Monitor exporter My_Netflow_Exporter
config flow add monitor My_Netflow_Monitor record ipv4_client_src_dst_flow_record config wlan flow 1
monitor My_Netflow_Monitor enable
```

debug コマンド

```
debug fastpath cfgtool --flowdb.dump debug fastpath dump wlandb
debug flow info enable
```

WebUI を使用した設定

次のスクリーンショットは、IP アドレス 10.10.105.22 を持ち、UDP ポート 2055 でリッスンしている、USC ボックス上の StealthWatch Netflow コレクタ VM の例を示しています。

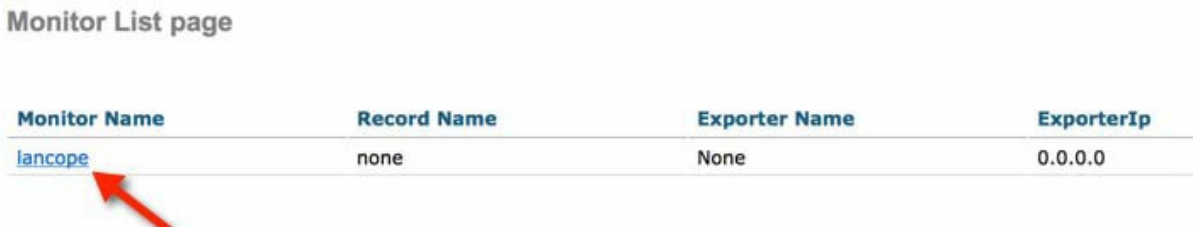
1. WLC のメインメニューから [Wireless] > [NetFlow] > [Exporter] に移動して、Netflow エクスポータを設定します。[New] をクリックします。

2. [Exporter Name]、[Exporter IP]、および [Port Number] を設定して [Apply] をクリックします。

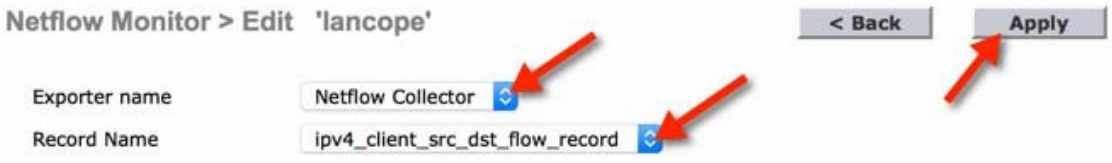
3. 次に、上記で作成した Netflow エクスポータのフローモニタを作成します。[Netflow] の下にある [Monitor] に移動します。[New] をクリックします。

4. 以下に示すように、「Stealthwatch」という名前でモニタを作成して [Apply] をクリックします。

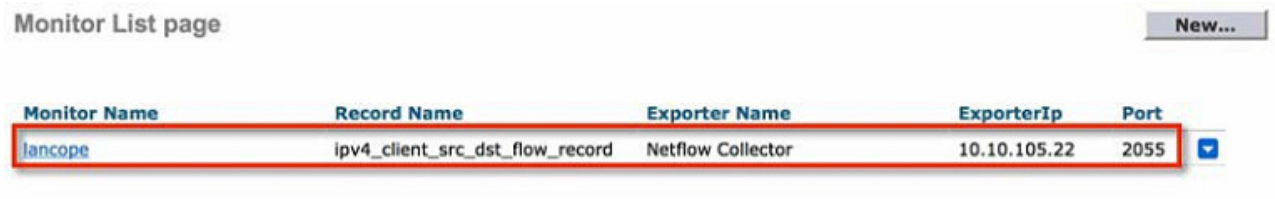
5. 作成したモニタ名をクリックします。



6. [Exporter Name] ドロップダウンメニューから [Netflow Collector] を選択し、[Record Name] リストから [ipv4_client_src_dst_flow_record] を選択します。[Apply] をクリックします。



[Wireless] > [NetFlow] > [Monitor] に次のように表示されます。



7. AVC と Netflow モニタを有効にする必要がある **WLAN** を参照します。WLAN の編集パラメータから [QoS] タブに移動して、[Application Visibility] のチェックボックスをオンにします。次に、[Netflow Monitor] を選択して [Apply] をクリックします。

NetFlow レポート

StealthWatch Netflow レポート設定は、フローコレクタと集中管理コンソールで構成されます。

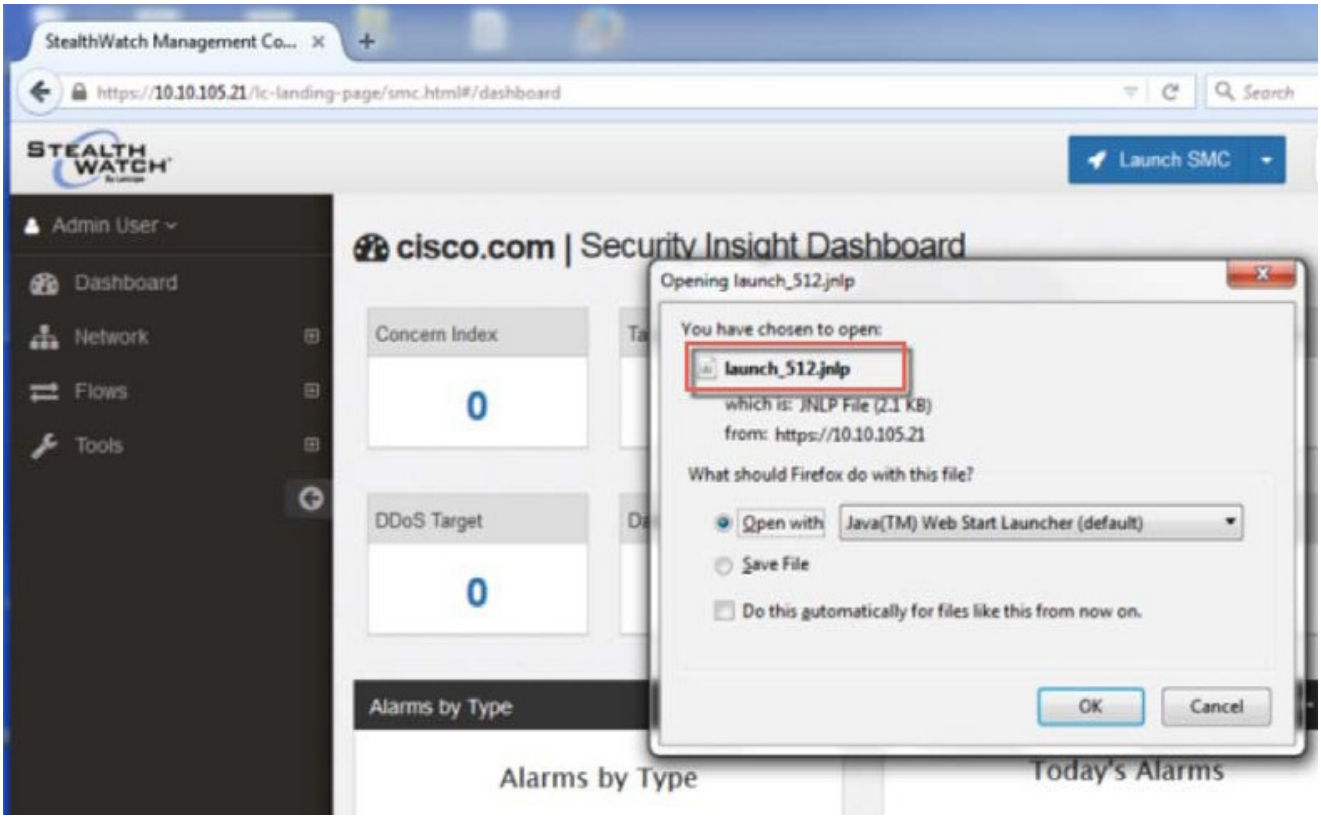
StealthWatch FlowCollector は、さまざまなソース（この場合はワイヤレス LAN コントローラ）からデータを収集し、それらを分析して通常のアクティビティのプロファイルを作成したうえで、通常のプロファイルの範囲外にあるアクティビティ用のアラーム（SMC 宛て）を生成します。

SMC は、Web ブラウザを介してシステムのさまざまなコンポーネントを管理、調整、および設定します。一元管理、およびトラフィックを視覚化したグラフによる最大 25 のフローコレクタのレポートが可能です。

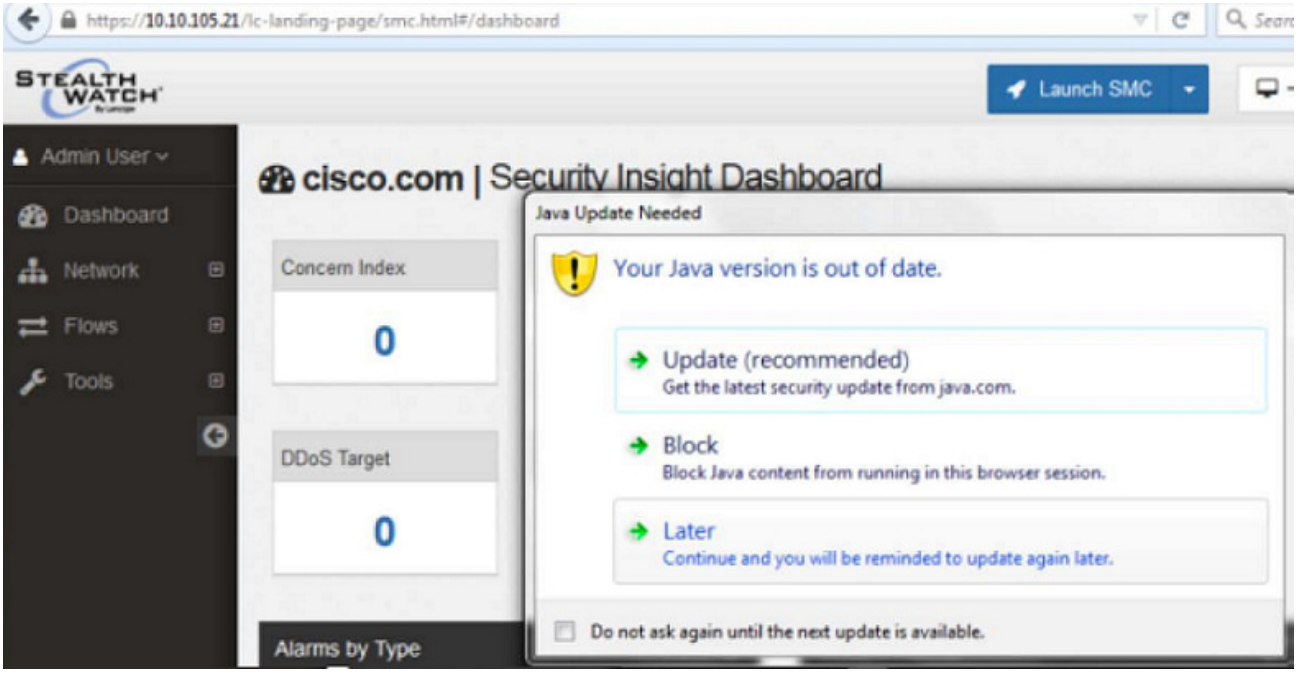
次の例は、10.10.105.22 に存在する FlowCollector（上記の WLC で設定されている）と 10.10.105.21 にある SMC を示しています。

1. ユーザ名とパスワードを使用して SMC にログインします。

2. ダッシュボードで [Launch SMC] をクリックします。アプリケーション「**launch_512**」のダウンロードを求めるプロンプトが表示されます。ローカルに保存し、前述のように起動します。



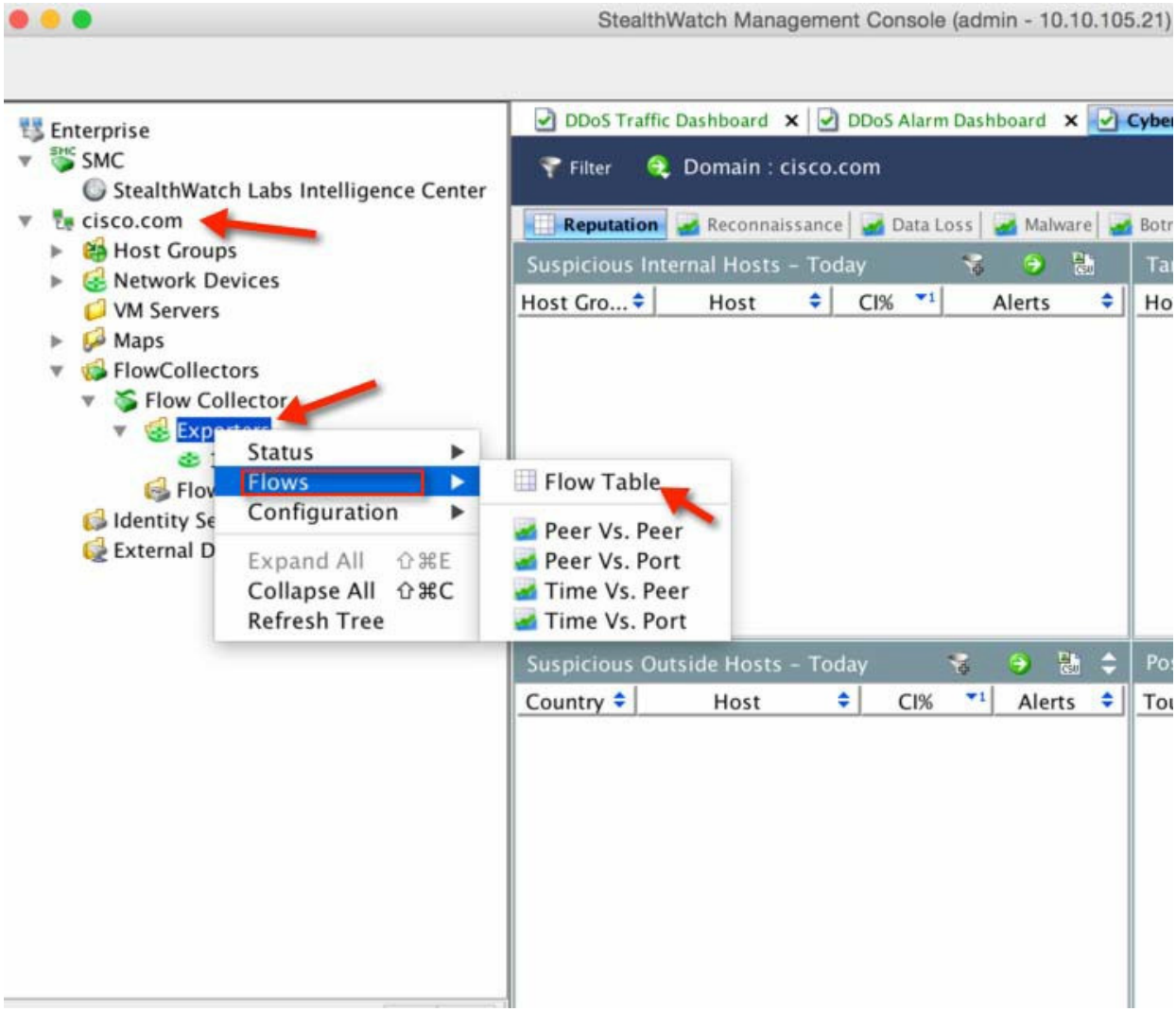
3. ポップアップウィンドウが表示されたら、次に示す手順を実行します。



4. 引き続き Stealth Watch Monitor をロードします。

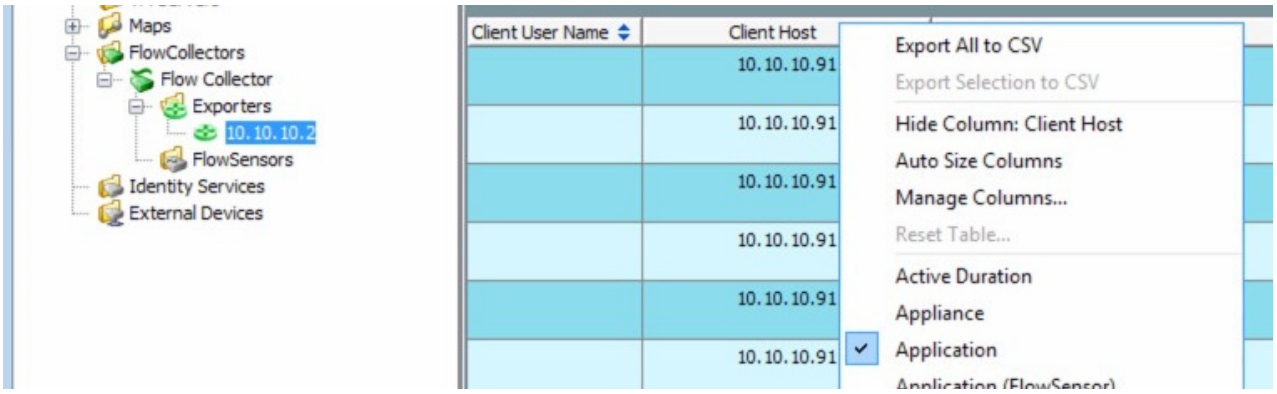
5. 設定したクレデンシャルで StealthWatch Collector Monitor にログインします。

6. ダッシュボードで [Exporters] を右クリックして [<Controller IP>] > [Flows] > [Flow Table] を選択し、クライアントフローを表示します。

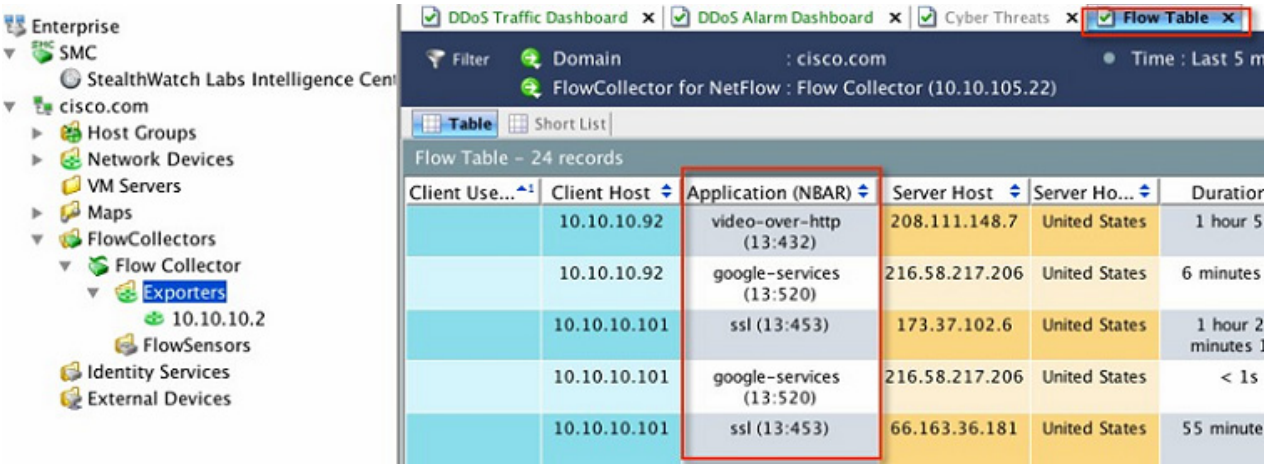


7. ここには複数のクライアントフローが表示されます。以下に示すように、列名を右クリックしてパラメータを選択すると、さまざまな属性のフローをフィルタリングできます。次に示す例では、IP アドレス 10.10.10.2 の WLC が [Application (NBAR)] 属性で選択されています。

注: フローを表示するには、クライアントが AVC および Netflow 対応 SSID に接続されていることを確認してください。



ユーザが dot1x credentials を使用して接続している場合は、StealthWatch のフロー テーブル ダッシュボードにも表示されます。



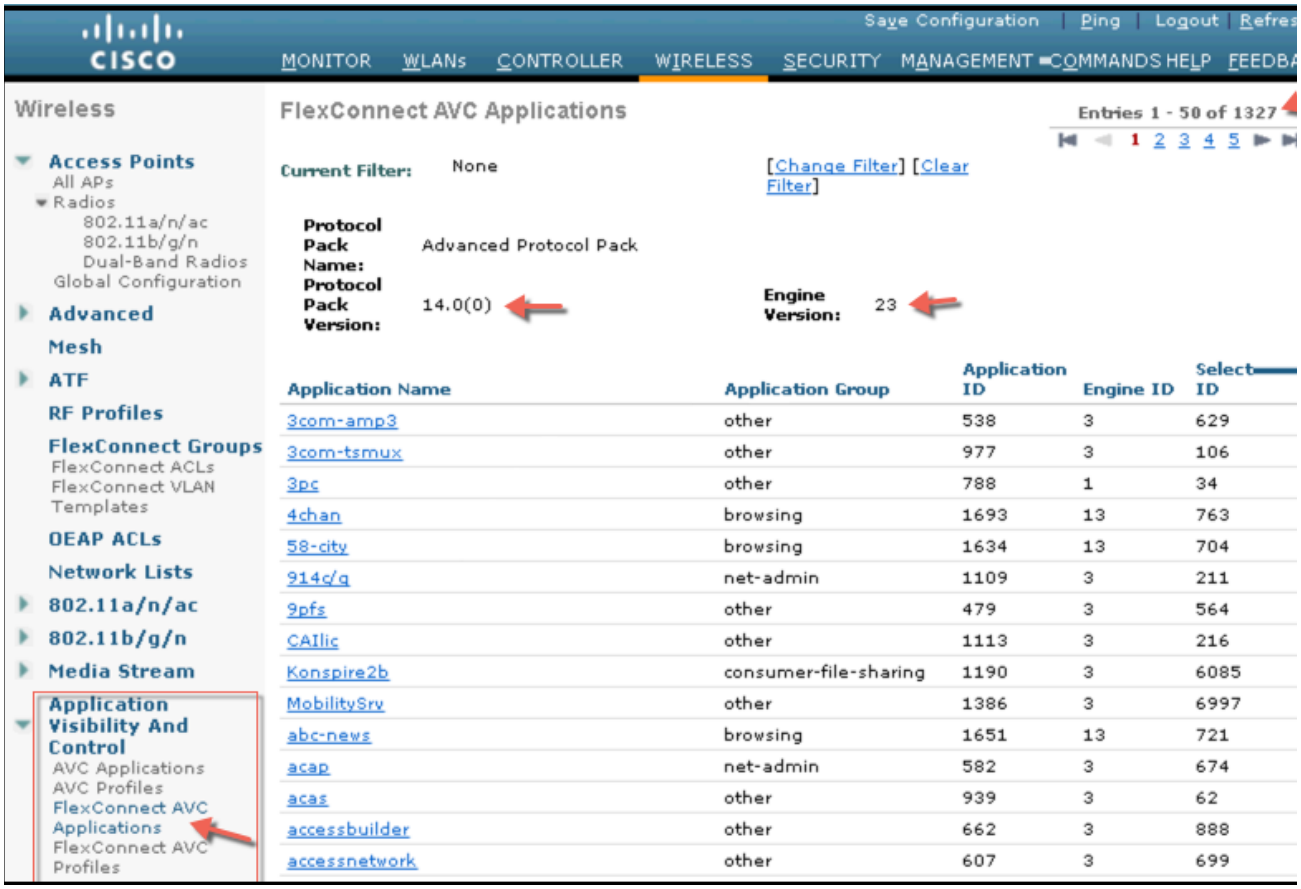
注:コントローラでプロトコルパックファイルをアップグレードする予定がある場合は、次のリンクで最新のプロトコルパックを確認できます。

https://software.cisco.com/download/home/282600534/type/284509011/release/24.0.0

CUWN リリース 8.3 の AVC フェーズ 5

FlexConnect モードバージョン 8.3 の AVC

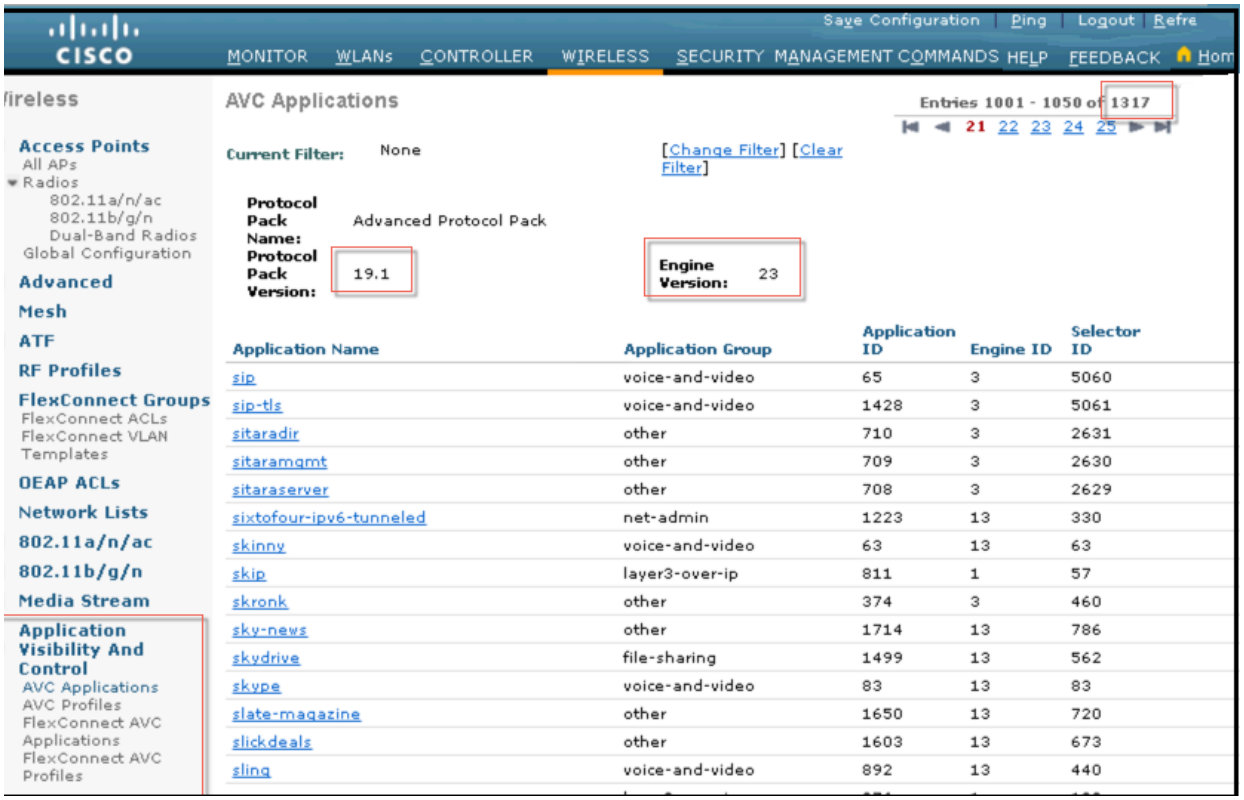
リリース 8.3 では、プロトコルパックと NBAR エンジンが Flex Connect アプリケーション向けにアップグレードされ、プロトコルパック 14 および NBAR エンジン 23 がサポートされて、サポートされるアプリケーションの合計数が 1327 になりました。



詳細については、
http://www.cisco.com/c/en/us/td/docs/wireless/controller/technotes/8-1/Flex-7500/Flex_7500_DG.html#pgfId-131717 を参照してください。

リリース 8.3 でのプロトコルパックと NBAR エンジンの更新

リリース 8.3 までは、集中型 AVC をサポートするために NBAR エンジン 23 が WLC に統合され、プロトコルパック (PP) バージョン 16 がサポートされています。リリース 8.3 では、改善された新しい NBAR エンジン 23 とプロトコルパック 19.1 が導入されました。新しいバージョンを使用すると、顧客はコントローラのパフォーマンスにほとんど影響を与えずに、Skype や Jabber など、最大 1317 のアプリケーションをより高い精度で確実に分類できます。プロトコルパック 19.1 には NBAR エンジン 23 が必要であり、前の WLC リリースで以前にリリースされたバージョンの NBAR では機能しないことにも注意してください。PP バージョン 19.1 がリリースされて CCO に掲載された場合は、NBAR エンジン 23 以上で動作します。



CUWN リリース 8.8 の AVC フェーズ 6

8.8 より前のリリースでは、WLC は NBAR エンジンバージョン 23（3.16.3）とデフォルト プロトコルパックバージョン 19.1 をサポートしていました。WLC でサポートされるアプリケーションの追加（特に新しい Wi-Fi 通話やズームなど）に対して顧客から多くの需要がありました。これらの新しいアプリケーションは、プロトコルパックバージョン 37 でサポートされています。ただし、プロトコルパック 35 は NBAR エンジン 23（3.16.3）でサポートされていないため、新しい PP 37 アプリケーションの分類に対応するには、NBAR エンジンとプロトコルパックを最新バージョンにアップグレードする必要があります。リリース 8.8 では、NBAR エンジン 31 および PP 37 が Wave-2 AP でサポートされます。

COS ベースの Wave-2 AP もアップグレードされ、FC モードの NBAR 31 および PP37 をサポートしています。

IOS AP は、最新の NBAR エンジンおよびプロトコルパックにアップグレードされません。したがって、新しいアプリケーションは FC 展開の Wave-1 AP に対して「UNKNOWN」と表示されます。

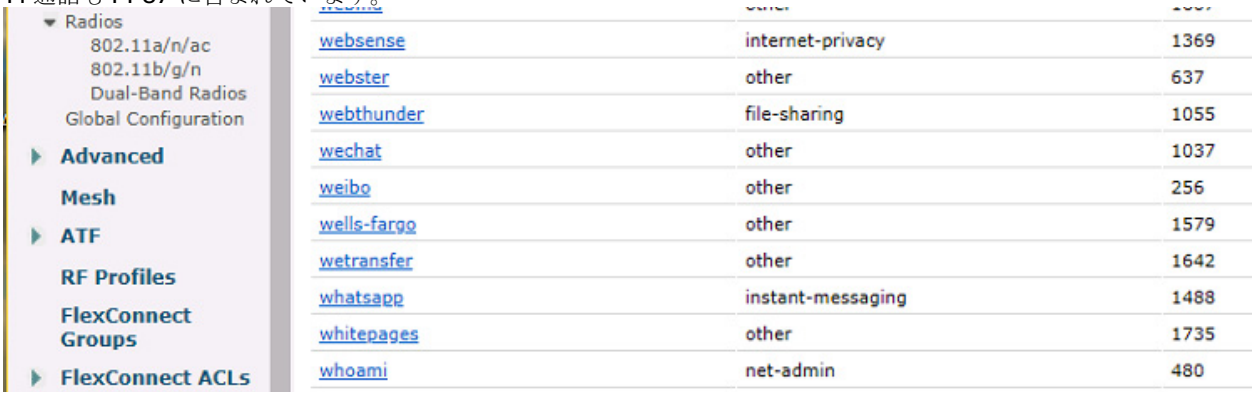
リリース 8.8 では、3504、5520、8540、および vWLC のみが、Wave-2 AP 1800、2800、3800、および 4800 シリーズで最新の PP37 と NBAR2 31 をサポートします。

AVC 拡張機能の設定手順

最新の NBAR エンジンまたはプロトコルパックのロードに必要な設定手順はありません。

ズーム通話は PP 37 に表示されています。

Wi-Fi 通話も PP37 に含まれています。



CLI を使用した 8.8 AVC 機能の管理

CLI 出力:

```
(Cisco Controller) >show avc protocol-pack version
AVC Protocol Pack Name: Advanced Protocol Pack
AVC Protocol Pack Version: 37
(Cisco Controller) >show avc engine version
AVC Engine Version: 31
(Cisco Controller) >
```

AVC プロファイル機能のデフォルト DSCP 値の概要

AVC が有効になっている 8.8 より前のリリースでは、AVC プロファイルで設定されているアプリケーションフローのすべてのアプリケーションの DSCP 値のみを上書きすることはできません。さらに、AVC プロファイルには最大 32 のアプリケーション ルールを含めることができます。

AVC プロファイルにルールが設定されていないフローの場合は、アクションが実行されず、DSCP はそのまま残ります。このままで AVC を PEP（ポリシー適用ポイント）として使用することはできません。

マネージドサービスの場合、AVC プロファイルに存在しないすべてのフローの DSCP 値（例：DSCP 0）を制御して書き直すことは不可能です。

新しい AVC 拡張機能では、AVC ルールが設定されていないすべてのアプリケーションフローの DSCP 値を上書きする「デフォルトクラス」ルールを使用できます。これは、Any/Any 条件を含む最後のルールのようなものです。その目的は、不要または制御済みの DSCP 値を持つすべてのフローからネットワークを保護することです。

現時点で AVC は、認識しているすべてのアプリケーションのマーキング、レート制限、またはドロップをサポートします。AVC では 32 のルールがサポートされます。これらのルールに設定されていないアプリケーションに対してアクションが実行されることはありません。

ローカルモードの場合、これらのルールはデータプレーンに組み込まれます。データプレーンで、これらのアプリケーションに対して、DSCP マーキングを含むアクションが実行されます。

リリース 8.8 の新機能の一環として、サポートされる 32 のルールに含まれる「デフォルトクラス」を設定できます。

既存のルールに一致しないアプリケーションには、この「デフォルトルール」が適用されます。

Flex Connect AVC の場合は、TLV タイプ TLV_FLEX_AVC_CLASS_MAP_APP_NAME_PAYLOAD のアプリケーション名と、TLV タイプ TLV_FLEX_AVC_CLASS_MAP_APP_ID_PAYLOAD のアプリケーション ID が送信されます。

リリース 8.8 では、AP に送信する「デフォルトクラス」のアプリケーション名とアプリケーション ID のサポートが強化されます。また、AP はこれらの値を処理して、それに応じてクラスマップを更新する必要があります。

リリース 8.8 での AVC のデフォルト DSCP 値に関する制限事項

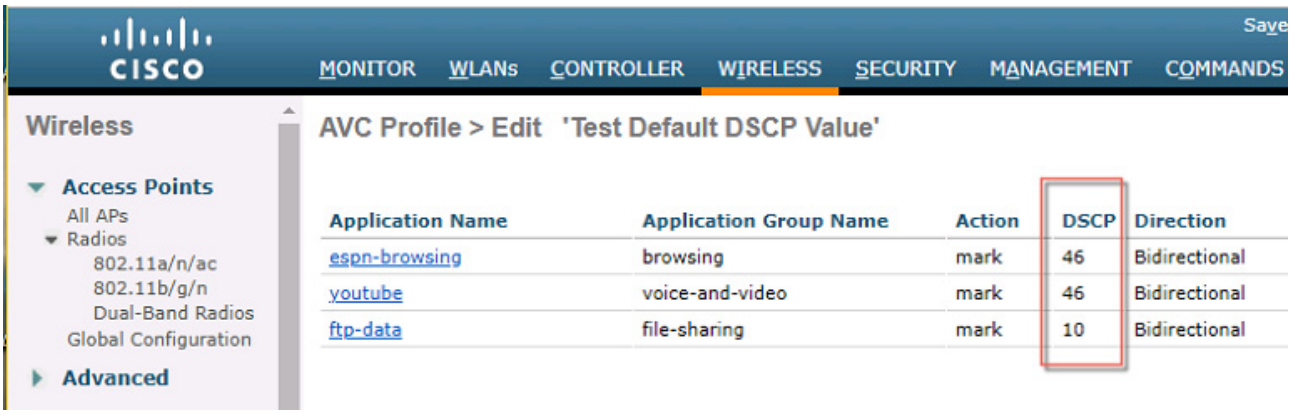
- マーキングのみがサポートされ、レート制限とドロップはサポートされません。
- デフォルト DSCP は AVC が有効な場合にのみ機能します。
- プロファイルあたり 32 のルール（「デフォルトクラス」ルールを含む）がサポートされます。デフォルトルールが設定されている場合、ユーザが設定できるルールは 31 個のみです。
- 設定されている「デフォルトクラス」のアプリケーション名は、統計情報ページおよび CLI 出力には表示されません。
- マルチキャストフローおよびブロードキャストフローはサポートされません。
- 現時点で AVC は IPv6 をサポートしていません。
- AVC ではルールをカスケーディングできないので、同じフローに対してレート制限とマーキングを実行することはできません。そのため、レート制限が実行されているフローに「デフォルト」のマーキングが行われることはありません。

注：プロファイルを WLAN に適用すると、「デフォルトクラス」の設定によって、未設定のすべてのアプリケーションの DSCP 値がすべて上書きされます。

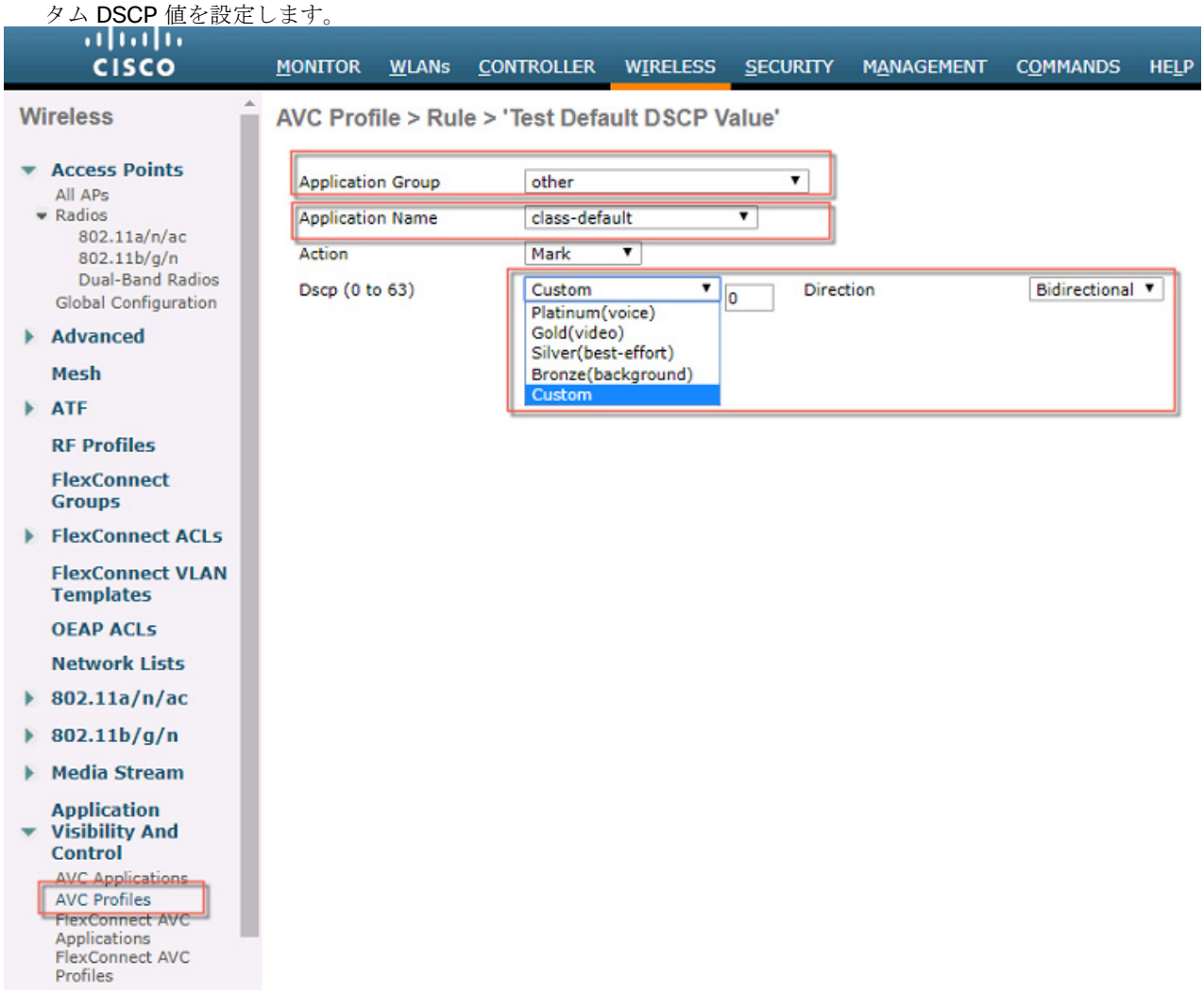
デフォルトの DSCP 設定の設定手順

この導入ガイドの前項の説明に従って、AVC プロファイルを作成、設定して WLAN に適用する手順を実行し、AVC プロファイルの作成後は次の手順を行ってください。

1. AVC プロファイルを作成すると、次の例のように表示されます。

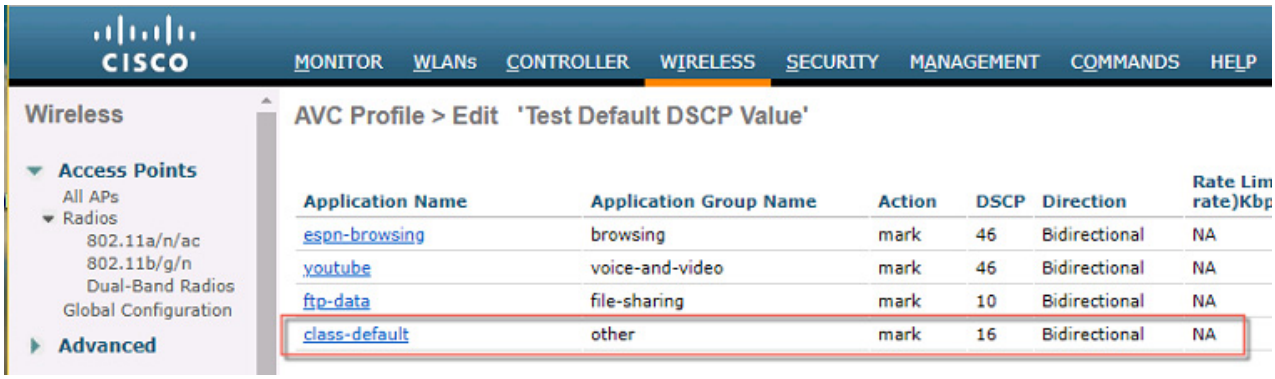


2. デフォルトクラス アプリケーションを追加するには、アプリケーショングループ「other」およびアプリケーション名「class-default」で新しいルールを作成すると同時に、必要な DSCP アクションを選択するか、次の例で示すようにカスタム DSCP 値を設定します。



注：Flex Connect モード用に作成した AVC プロファイルにも同じ手順が適用されます。

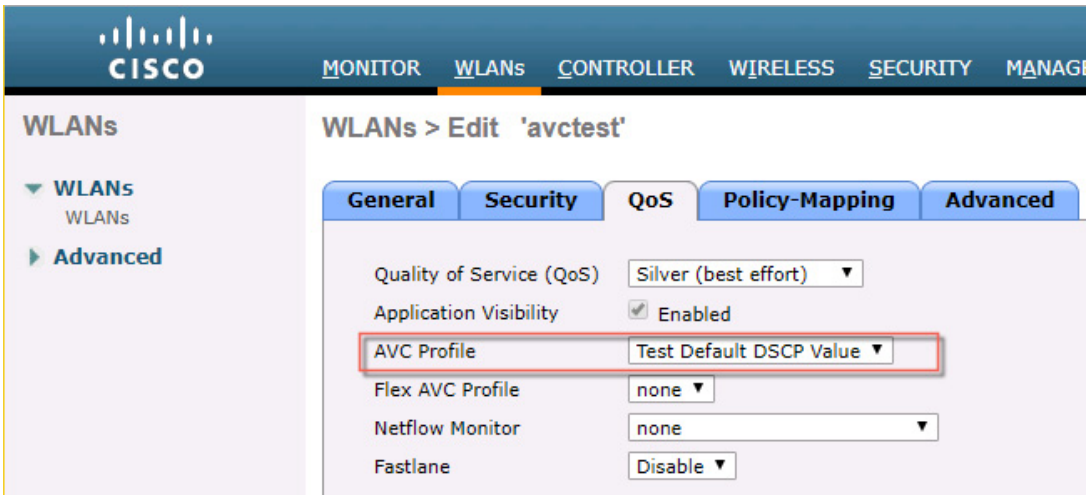
3. 新しく作成したルールをプロファイルに適用すると、プロファイルに表示されるようになります。



既存のアプリケーションリストに「class-default」アプリケーションが追加されます。

GUI に自動的に表示されます。

4. 新しく作成したプロファイルを WLAN に適用します(次の例では、作成したプロファイルが WLAN「avctest」に適用されます)。



デフォルト DSCP の CLI コンフィギュレーション コマンド:

アプリケーション名「class-default」で AVC プロファイルを作成します。

```
# config avc profile <profile_name> rule add application <application name> mark <dscp>
```

show コマンドの変更:

```
# show avc profile detailed <profile_name>
Application-Name          Application-Group-Name            Action     DSCP    DIR  AVG-RATELIMIT
BURST-RATELIMIT
  ================          ======================           ======     ====  ===== =============
=============
 default       -                                Mark      46
```

Config コマンドの例:

```
(Cisco Controller) >config avc profile temp rule add application class-default mark 16
(Cisco Controller) >show avc profile detailed temp
Application-Name  Application-Group-Name  Action DSCP   DIR  AVG-RATELIMIT -RATELIMIT  ================
======================           ======     ====  ===== =
telnet                    net-admin                          Mark      7 Bidirectional
 ping                      net-admin                          Mark      6 Bidirectional
class-default             other                              Mark     16 Bidirectional
Associated WLAN IDs       :
Associated Remote LAN IDs :
Associated Guest LAN IDs  :
(Cisco Controller) >
```

FlexConnect 向け Application Visibility and Control リリース 8.1 ～ 8.8

AVC は、ワイヤレスネットワークでのアプリケーション対応制御を可能にし、管理性と生産性を向上させます。AVC は、ASR、ISR G2 および WLC プラットフォーム上ですでにサポートされています。これはエンドツーエンドのソリューションであるため、FlexConnect AP に組み込まれている AVC のサポートもエンドツーエンドまで拡大されます。ネットワークのアプリケーションが完全に可視化されるため、管理者はアプリケーションに対してアクションを実行できます。

AVC には次のコンポーネントがあります。

- Network Based Application Recognition（NBAR2）と呼ばれる次世代ディープ パケット インスペクション（DPI）テクノロジーが、アプリケーションの識別と分類を可能にします。NBAR は、ステートフル L4 ～ L7 分類をサポートし、Cisco IOS ベースのプラットフォームで利用できるディープパケット インスペクション テクノロジーです。NBAR2 は NBAR に基づいており、NBAR を使用するすべての IOS 機能に共通のフローテーブルを提供するなどの追加の要件を満たしています。NBAR2 はアプリケーションを認識し、その情報を Quality of Service（QoS）やアクセスコントロールリスト（ACL）などの機能に渡すことで、分類に基づくアクションが実行されます。
- QoS、ドロップおよびレート制限アプリケーションを使用してマーキングを適用できます。

NBAR AVCの主な使用例として、キャパシティプランニング、ネットワーク使用量のベースライン化、帯域幅を消費するアプリケーションのより適切な把握などがあります。アプリケーションの使用状況の傾向を把握できるため、ネットワーク管理者は、ネットワーク インフラストラクチャのアップグレードを計画したり、ネットワーク上で輻輳が生じた場合に帯域幅消費の激しいアプリケーションから主要なアプリケーションを保護することで Quality of Experience を改善したりすることができます。さらに、特定のアプリケーション トラフィックの優先順位を変更したり、ドロップしたりすることもできます。

AVC は、リリース 7.4 以降のローカルモードおよび FlexConnect モード（中央スイッチング用に構成された WLAN の場合のみ）の 5520、8540、2500、5508、7500、8500、および WiSM2 コントローラでサポートされています。リリース 8.1 では、5508、7500、75100、WiSM2、および vWLC 上の FlexConnect AP で、ローカルスイッチング WLAN 向けの Application Visibility and Control がサポートされています。

- リリース 8.3 では、プロトコルパックと NBAR エンジンが Flex Connect アプリケーション向けにアップグレードされ、プロトコルパック 14 および NBAR エンジン 23 がサポートされて、サポートされるアプリケーションの合計数が 1327 になりました。
- リリース 8.8 では、プロトコルパックと NBAR エンジンが Flex Connect アプリケーション向けにアップグレードされ、プロトコルパック 37 および NBAR エンジン 31 がサポートされて、サポートされるアプリケーションの合計数が 1408 になりました。

リリース 8.6 から、AVC は 3504、5520、8540 シリーズのコントローラでサポートされ、vWLC でも FC モードの AVC のみがサポートされます。

注: AVC フェーズ 6（リリース 8.8）では、3504、5520、および 8540 シリーズのコントローラで最新の NBAR2 とプロトコルパックがサポートされ、vWLC は Flex Connect AP 向けの AVC のみをサポートします。リリース 8.8 の PP は、Wave-2 COS ベースの AP のみをサポートします。

AVC の仕様および制限

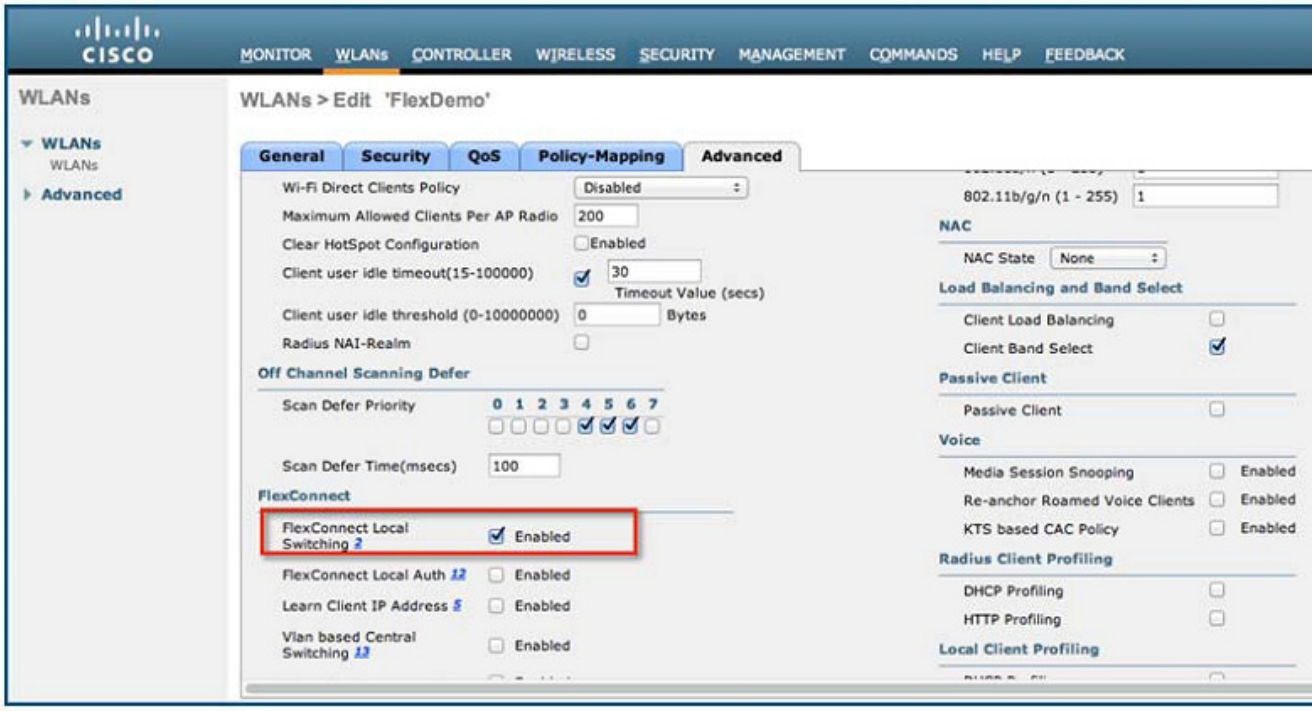
FlexConnect AP の AVC では、1000 種類以上のアプリケーションを分類し、アクションを実行できます。

- FlexConnect AP で稼働するプロトコルパックは、WLC 上で稼働するプロトコルパックとは異なります。
- AVC による GUI の統計情報は、デフォルトでは上位 10 のアプリケーションに対して表示されます。これを、上位 20 または 30 のアプリケーションに変更することもできます。
- FlexConnect グループ内のローミングがサポートされます。
- IPv6 トラフィックを分類することはできません。
- AVC プロファイルの AAA オーバーライドはサポートされません。
- マルチキャストトラフィックは、AVC アプリケーションではサポートされません。
- FlexConnect AVC の Netflow エクスポートはサポートされていません。

アプリケーション可視性の設定

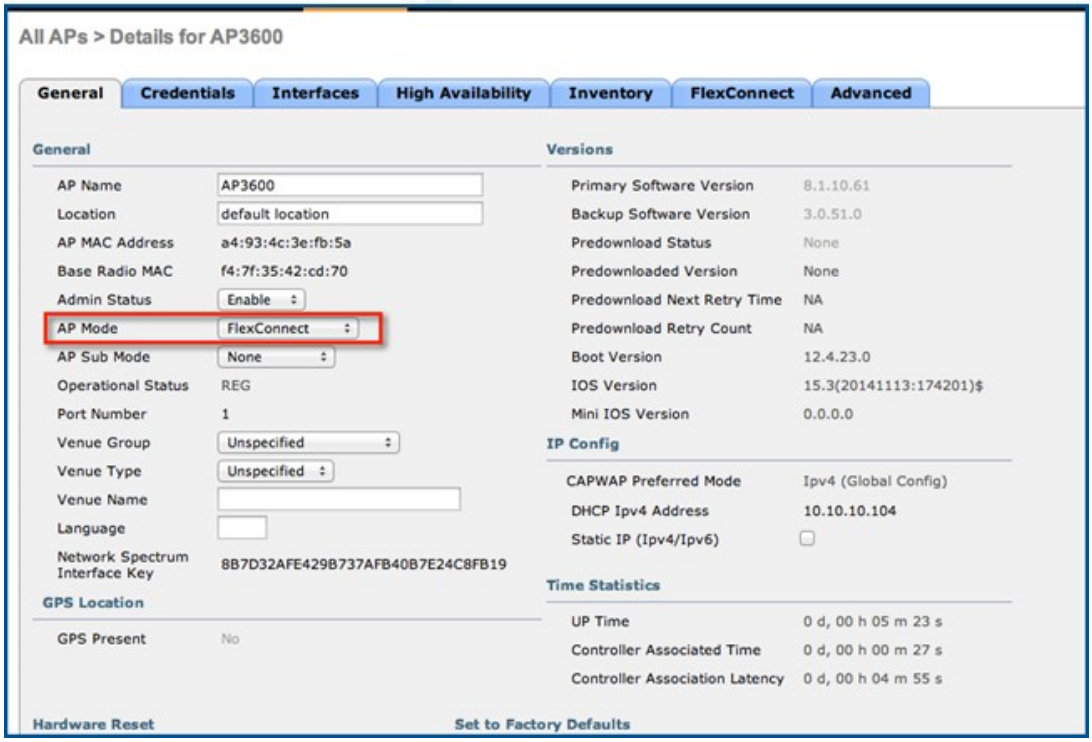
アプリケーションの可視性を設定するには、次の手順を実行します。

1. 有線ラップトップで Web ブラウザを開き、WLC の IP アドレスを入力します。
2. 命名規則を使用して、「FlexDemo」などの OPEN WLAN を作成します。
3. WLAN で [FlexConnect Local Switching] を有効にして、[Apply] をクリックします。



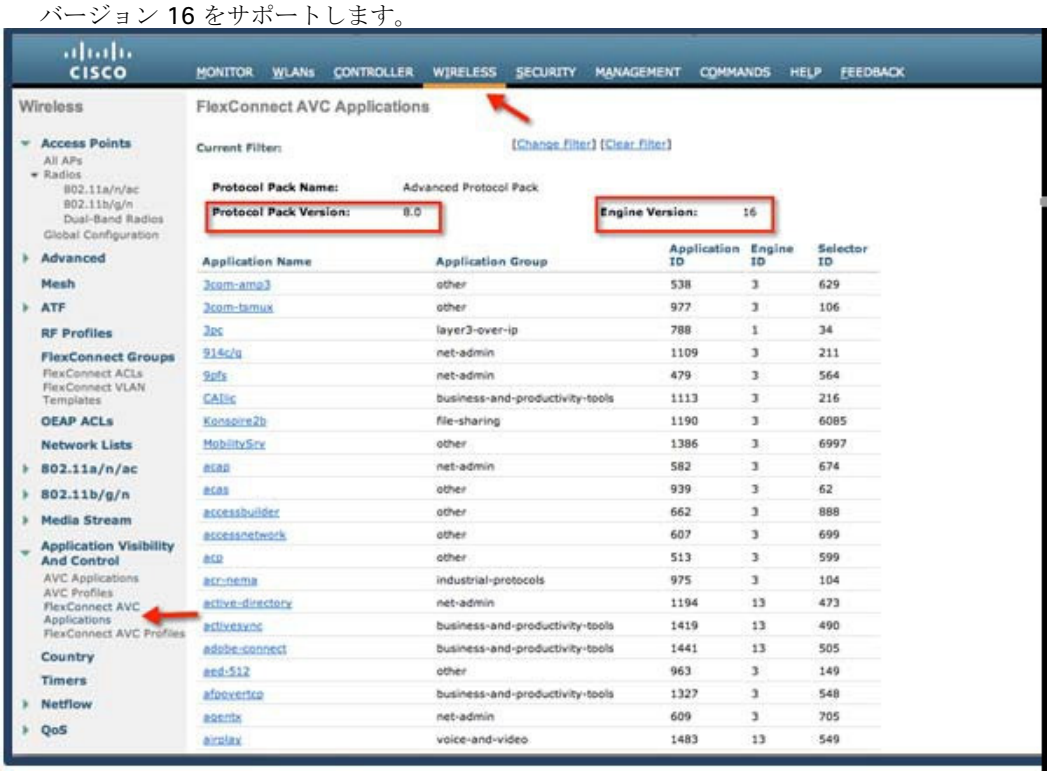
4. この WLAN に接続された AP がこの機能に対してサポートされているアクセスポイントのリスト内に存在することを確認します。

5. [AP Mode] ドロップダウンメニューで [FlexConnect] を選択して AP を FlexConnect モードに切り替え、[Apply] をクリックします。リブートしなくてもモードが FlexConnect に変わります。



6. FlexConnect グループを作成して、AP をその FlexConnect グループに追加します。次の例では、「FlexGroup」という FlexConnect グループにアクセスポイント AP3600 を追加します。

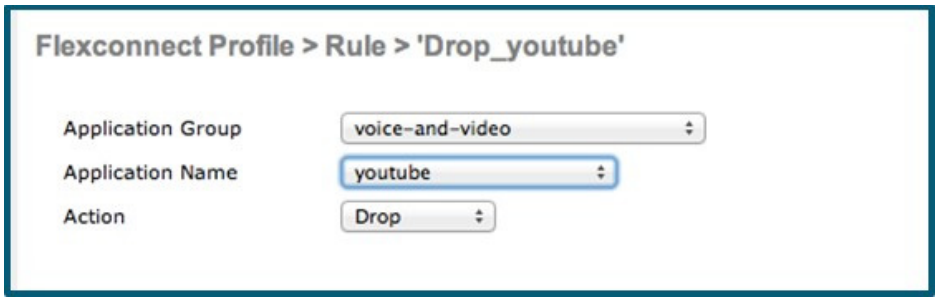
7. 識別、分類、および制御が可能なアプリケーションが、[Wireless] > [Application Visibility and Control] > [FlexConnect AVC Applications] > に一覧表示されます。アクセスポイントは、プロトコルパックバージョン 8.0 と NBAR エンジンバージョン 16 をサポートします。



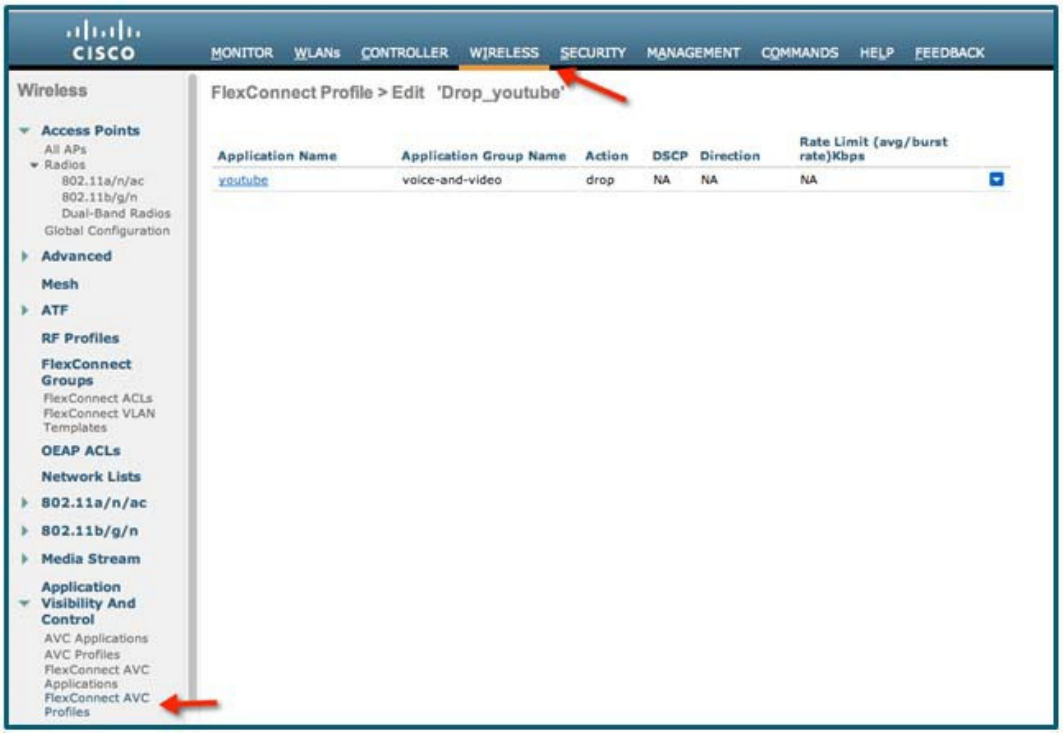
8. [Wireless] > [Application Visibility And Control] > [FlexConnect AVC Profiles] > [New] で、「Drop_youtube」という名前の AVC プロファイルを作成します。次に、[Apply] をクリックします。

新しい名前「Drop_youtube」で AVC プロファイルが作成されます。

9. プロファイル名をクリックして、[Add New Rule] をクリックします。[Application Group]、[Application Name]、および [Action] を選択して、[Apply] をクリックします。

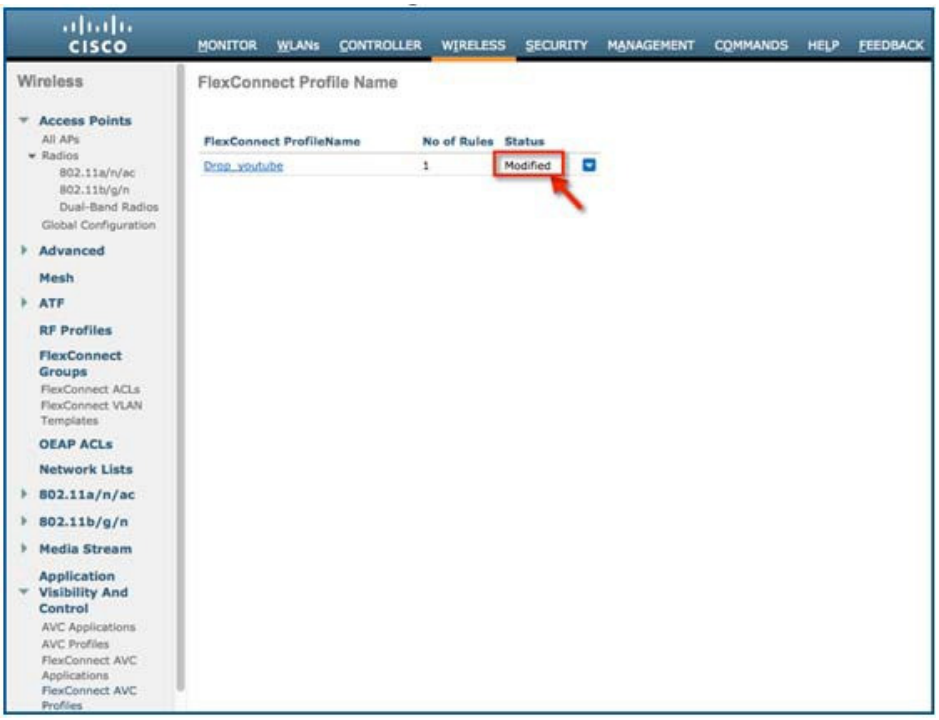


10. 次の図に示すように、ルールが追加されたことを確認します。

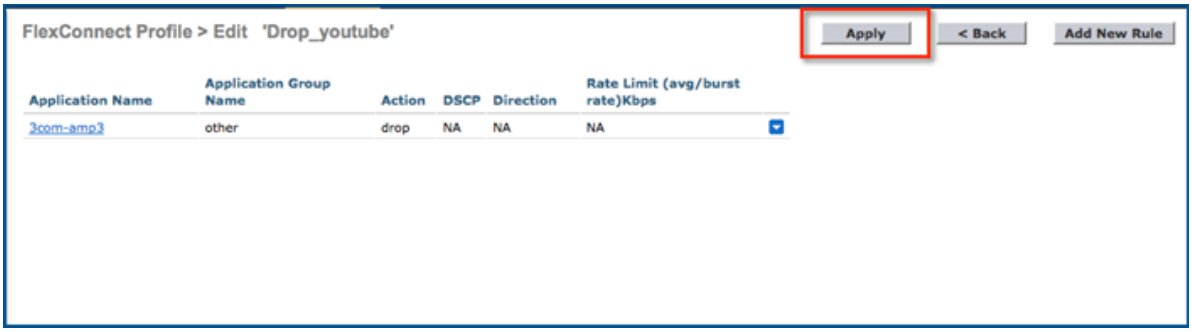


この時点の FlexConnect AVC プロファイルのステータスは、[Modified] です。

11. プロファイルを適用して有効化するには、プロファイルを選択して [Apply] をクリックします。



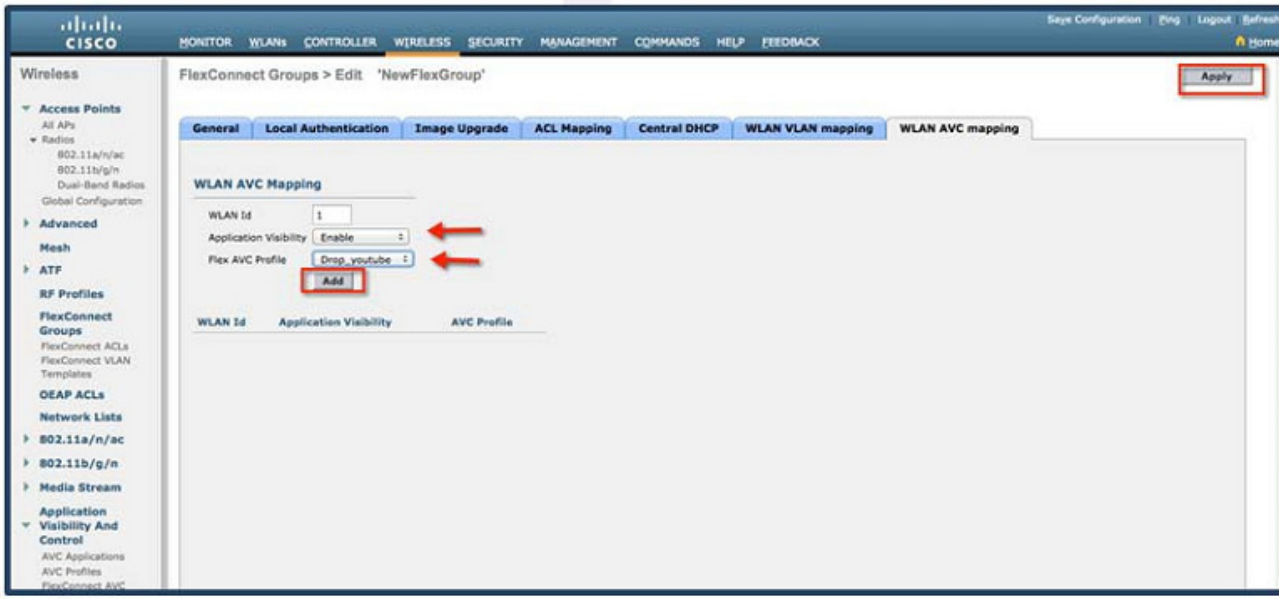
12. プロファイルを適用して有効化するには、プロファイルを選択して [Apply] をクリックします。



FlexConnect AVC プロファイルのステータスが、[Applied] に変わります。

13. [Wireless] > [FlexConnect Group] > [FlexConnect Group name] > [WLAN AVC Mapping] で、[WLAN ID] を選択してドロップダウンメニューから [Enable] を選択し、FlexConnect グループでアプリケーションの可視性を有効にします。

14. [AVC Profile] ドロップダウンメニューから、前の設定で作成したプロファイルを選択して、FlexConnect AVC プロファイルを適用します。[Add] をクリックし、[Apply] をクリックします。

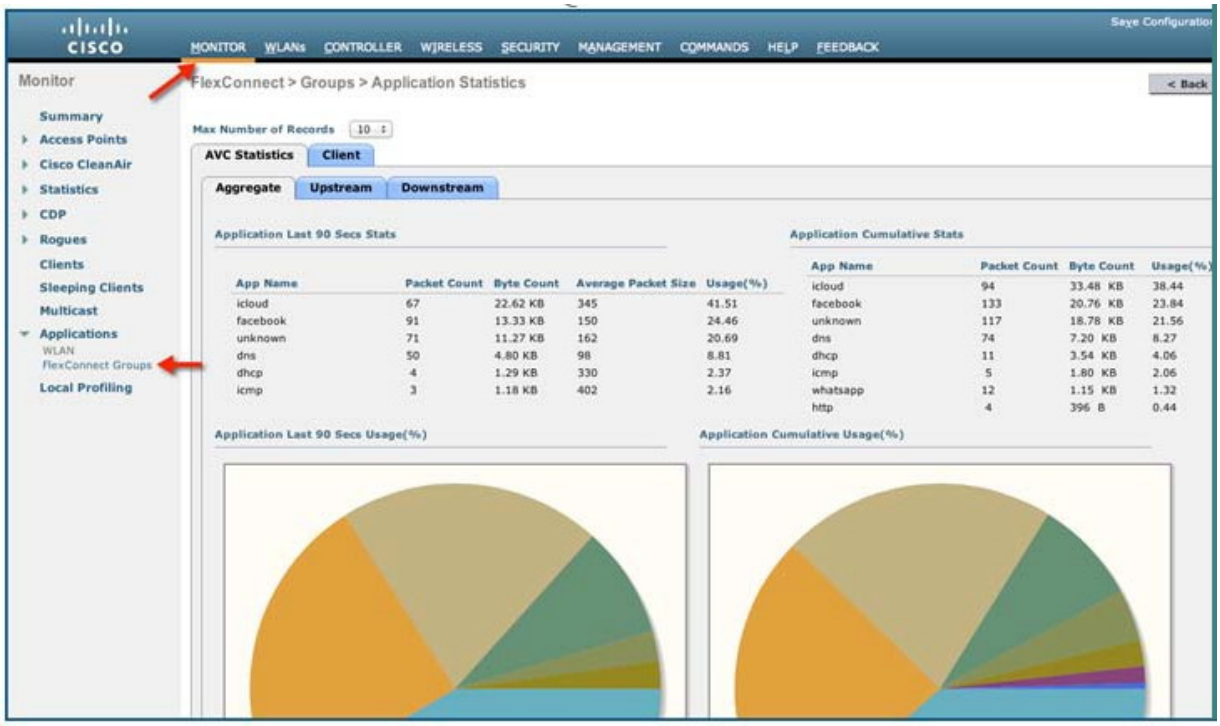


15. FlexConnect グループで AVC を有効にすると、関連付けられているワイヤレスクライアントから、Cisco Jabber/Web Ex Connect、Skype、Yahoo Messenger、HTTP、HTTPS/SSL、Microsoft Messenger、Ping、トレースルートなどの（すでにインストールされている）アプリケーションを使用するさまざまなタイプのトラフィックが開始されます。

ワイヤレスクライアントからトラフィックが開始されると、FlexConnect グループ単位およびクライアント単位でさまざまなトラフィックの可視性を確認できます。これにより、管理者はネットワーク帯域幅の使用状況やネットワーク内のトラフィックのタイプについて、クライアント単位およびブランチサイト単位で確認できます。

16. FlexConnect グループ上のすべての WLAN の可視性をグローバルにチェックするには、[Monitor] > [Applications] > [FlexConnect] > [FlexConnect Groups] をクリックし、先に作成した FlexConnect グループを選択します。

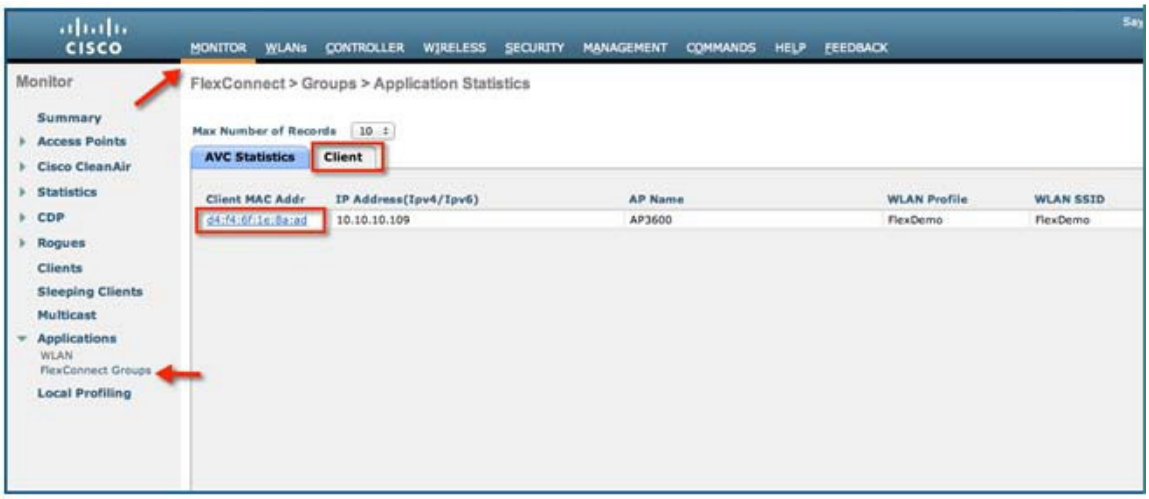
次の画面には、その特定の FlexConnect グループで実行されている上位 10 のアプリケーションに関する集約データが一覧表示されます。



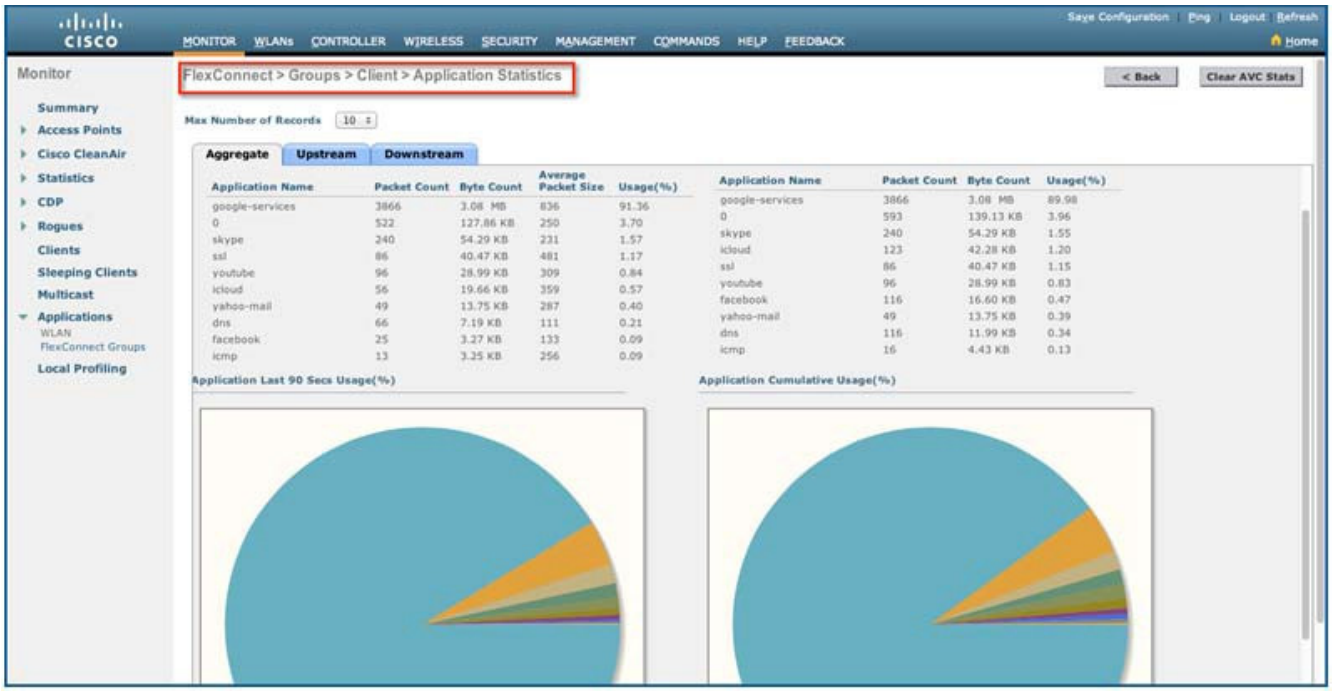
このページでは、FlexConnect グループごとのよりきめ細かな可視性が提供され、過去 90 秒の上位 10 のアプリケーションと、上位 10 のアプリケーションの累積統計情報が表示されます。同じページに FlexConnect グループごとのアップストリーム統計情報とダウンストリーム統計情報を個別に表示するには、[Upstream] タブと [Downstream] タブをクリックします。

注: このページの [Max Number of Records] フィールドを変更すると、このページに表示されるアプリケーションの数を 20 または 30 に増やすことができます。デフォルト値は 10 です。

17. AVC の可視性が有効になっている特定のローカルスイッチング WLAN で、クライアントごとの上位 10 のアプリケーションについてより詳細に表示するには、[Monitor] > [Applications] > [FlexConnect Group] > [FlexConnect Group name] > [Clients] をクリックします。次に、そのページに表示された個別のクライアント MAC エントリをクリックします。



個別のクライアント MAC エントリをクリックすると、クライアントの詳細ページが表示されます。



このページでは、WLAN 自体で、またはこの例のように FlexConnect グループで AVC の可視性が有効になっているローカルスイッチング WLAN に関連付けられたクライアントごとの詳細な統計情報が提供されます。過去 90 秒の上位 10 のアプリケーションと、上位 10 のアプリケーションの累積統計情報がページに表示されます。

18. 同じページでクライアントごとのアップストリーム統計情報とダウンストリーム統計情報を個別に表示するには、[Upstream] タブと [Downstream] タブをクリックします。

注: このページの [Max Number of Records] フィールドを変更すると、このページに表示されるアプリケーションの数を 20 または 30 に増やすことができます。デフォルト値は 10 です。

19. 特定のクライアントの AVC 統計情報をクリアするには、[Clear AVC Stats] ボタンをクリックします。

これで、ワイヤレスクライアントから YouTube を開いた場合に、そのクライアントで YouTube ビデオを再生できなくなります。また、該当する場合は、Facebook アカウントを開いて YouTube ビデオを開いてみてください。YouTube ビデオを再生できないことが確認できます。YouTube をブロックする FlexConnect AVC プロファイルが FlexConnect グループの WLAN にマッピングされているため、ブラウザ経由でも、YouTube アプリケーションを使用しても、他の Web サイトからも YouTube ビデオにアクセスすることはできません。

注: ブラウザですでに Youtube が開いている場合、AVC プロファイルを有効にするには、ブラウザを更新してください。

付録

VOD リファレンス

Cisco AVC - ユーザ単位のアプリケーション制御：http://www.youtube.com/watch?v=ESg53o3ufDQ&feature=youtu.be

Web リンクと用語

Cisco WLAN コントローラの情報：

http://www.cisco.com/en/US/products/hw/wireless/products.html

http://www.cisco.com/cisco/web/support/index.html

Cisco Prime 管理ソフトウェアの情報：

http://www.cisco.com/en/US/products/ps11686/index.html

Cisco MSE の情報：

http://www.cisco.com/en/US/products/ps9742/index.html

Cisco LAP のマニュアル：

http://www.cisco.com/en/US/products/ps10981/index.html

FlexConnect 向け Application Visibility and Control リリース 8.1 ～ 8.8