AAA Override の設定

- AAA Override について，1 ページ
- AAA Override の制約事項，2 ページ
- 正しい QoS 値を取得するための RADIUS サーバ ディクショナリ ファイルの更新，2 ページ
- AAA Override の設定（GUI），4 ページ
- AAA オーバーライドの設定（CLI），4 ページ

AAA Override について

WLAN の AAA Override オプションを使用すると、WLAN で Identity ネットワーキングを設定できます。 これにより、AAA サーバから返される RADIUS 属性に基づいて、個々のクライアントに VLAN タギング、Quality Of Service (QoS)、およびアクセス コントロール リスト (ACL) を適用することができます。

IPv6 ACL の AAA オーバーライド

Cisco Identity Services Engine（ISE）、ACS などの一元化された AAA サーバによるアクセス コントロールのサポートのために、AAA Override 属性を使用して・クライアントについて IPv6 ACL をプロビジョニングできます。 この機能を使用するには、IPv6 ACL をコントローラで設定し、AAA Override 機能をイネーブルにして WLAN を設定する必要があります。 ACL がコントローラで事前に設定されていない場合、クライアントは認証解除されます。 IPv6 ACL の実際の名前付き AAA 属性は、IPv4 ベースの ACL をプロビジョニングするために使用される *Airespace ACL-Name* 属性に似た ***Airespace-IPv6-ACL-Name*** です。 AAA 属性が返すコンテンツは、コントローラで設定された IPv6 ACL の名前に一致する文字列になるはずです。

（注） リリース 7.5 から、アップストリーム AAA Override のレート制限値はダウンストリーム AAA Override のレート制限値と同じになりました。

AAA Override の制約事項

- AAA Override のためにクライアントが新しいインターフェイスに移動したあと、そのインターフェイスに ACL を適用しても、クライアントが再認証されるまで ACL は有効になりません。 この問題を回避するには、インターフェイス上ですでに設定済みの ACL にすべてのクライアントが接続するように、ACL を適用してから WLAN を有効にします。あるいは、クライアントが再認証されるように、インターフェイスを適用したあとで WLAN を一旦無効にし、再び有効にします。
- AAA サーバから返された ACL がコントローラ上にないか、 ACL が間違った名前で設定されている場合、クライアントは認証されません。
- FlexConnect のローカル スイッチングを使用すると、マルチキャストは SSID がマッピングされた VLAN にのみ転送され、上書きされた VLAN には転送されません。 したがって、IPv6 は、マルチキャスト トラフィックが不正な VLAN から転送されるため、正しく動作しません。
- インターフェイス グループが WLAN にマッピングされ、クライアントがその WLAN に接続した場合、クライアントはラウンドロビン方式で IP アドレスを取得しません。 インターフェイス グループによる AAA Override はサポートされています。
- AAA Override を許可する設定の多くは、RADIUS サーバで実行されます。RADIUS サーバでは、コントローラに返すようにする上書きプロパティで、Access Control Server（ACS）を設定する必要があります。
- コントローラでは、GUI または CLI を使用して、Allow AAA Override 設定パラメータを有効にします。 このパラメータを有効にすることにより、コントローラで RADIUS サーバから返される属性を受け入れるようになります。 次にコントローラはそれらの属性をクライアントに適用します。
- レイヤ 2 認証中に AAA Override を有効にすると、ローカル ポリシーは適用されず、Override が優先されます。
- Cisco TrustSec セキュリティ グループのタグは、WLAN で AAA ocerride を有効にするまで適用されません。

正しいQoS値を取得するためのRADIUSサーバディクショナリ ファイルの更新

Steel-Belted RADIUS（SBR）、FreeRadius、または同等の RADIUS サーバを使用している場合、AAA Override 機能を有効化した後、クライアントが正しい QoS 値を取得できないことがあります。 ディクショナリ ファイルの編集を可能にするこれらのサーバについて、正しい QoS 値（Silver = 0、Gold = 1、Platinum = 2、Bronze = 3）を反映させてファイルを更新する必要があります。 RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。

（注） この問題は、Cisco Secure Access Control Server（ACS）には適用されません。

RADIUS サーバのディクショナリ ファイルを更新するには、次の手順を実行します。

1 SBR サービス（または他の RADIUS サービス）を停止します。

2 次のテキストを、ciscowlan.dct として Radius_Install_Directory\Service フォルダに保存します。

```
################################################################################
# CiscoWLAN.dct- Cisco Wireless Lan Controllers
#
# (See README.DCT for more details on the format of this file)
################################################################################

# Dictionary - Cisco WLAN Controllers
#
# Start with the standard Radius specification attributes
#
@radius.dct
#
# Standard attributes supported by Airespace
#
# Define additional vendor specific attributes (VSAs)
#

MACRO Airespace-VSA(t,s) 26 [vid=14179 type1=%t% len1=+2 data=%s%]

ATTRIBUTE   WLAN-Id                 Airespace-VSA(1, integer)     cr
ATTRIBUTE   Aire-QoS-Level          Airespace-VSA(2, integer)     r
VALUE Aire-QoS-Level Bronze     3
VALUE Aire-QoS-Level Silver     0
VALUE Aire-QoS-Level Gold       1
VALUE Aire-QoS-Level Platinum   2

ATTRIBUTE   DSCP                    Airespace-VSA(3, integer)     r
ATTRIBUTE   802.1P-Tag              Airespace-VSA(4, integer)     r
ATTRIBUTE   Interface-Name          Airespace-VSA(5, string)      r
ATTRIBUTE   ACL-Name                Airespace-VSA(6, string)      r

# This should be last.

################################################################################
# CiscoWLAN.dct - Cisco WLC dictionary
################################################################################
```

3 （同じディレクトリにある）dictiona.dcm ファイルを開いて、「@ciscowlan.dct.」行を追加します。

4 dictiona.dcm ファイルを保存して閉じます。

5 （同じディレクトリにある）vendor.ini ファイルを開いて、次のテキストを追加します。

```
vendor-product       = Cisco WLAN Controller
dictionary           = ciscowlan
ignore-ports         = no
port-number-usage    = per-port-type
help-id              =
```

6 vendor.ini ファイルを保存して閉じます。

7 SBR サービス（または他の RADIUS サービス）を起動します。

8 SBR アドミニストレータ（または他の RADIUS アドミニストレータ）を起動します。

9 RADIUS クライアントを追加します（まだ追加されていない場合）。 [Make/Model] ドロップダウン リストから [Cisco WLAN Controller] を選択します。

AAA Override の設定（GUI）

ステップ 1 [WLANs] を選択して、[WLANs] ページを開きます。

ステップ 2 設定する WLAN の ID 番号をクリックします。 [WLANs > Edit] ページが表示されます。

ステップ 3 [Advanced] タブを選択します。

ステップ 4 [Allow AAA Override] チェックボックスをオンにして AAA Override を有効にするか、オフにしてこの機能を無効にします。 デフォルト値は [disabled] です。

ステップ 5 [Apply] をクリックします。

ステップ 6 [Save Configuration] をクリックします。

AAA オーバーライドの設定（CLI）

- 次のコマンドを入力して、WLAN 上の AAA を介したユーザ ポリシーのオーバーライドを設定します。
  config wlan aaa-override {**enable** | **disable**} *wlan-id*
  wlan-id には 1 ～ 16 の値を入力します。
- 次のコマンドを入力して、802.1X AAA インタラクションのデバッグを設定します。
  debug dot1x aaa {**enable** | **disable**}
- 次のコマンドを入力して、AAA QoS オーバーライドのデバッグを設定します。
  debug ap aaaqos-dump {**enable** | **disable**}