RADIUS の設定

- RADIUS の概要，1 ページ
- RADIUS の設定の制限，3 ページ
- ACS 上での RADIUS の設定，4 ページ
- RADIUS の設定（GUI），5 ページ
- RADIUS の設定（CLI），11 ページ
- コントローラによって送信される RADIUS 認証属性，17 ページ
- Access-Accept パケットで受け付けられる認証属性（Airespace），20 ページ
- RADIUS アカウンティング属性，28 ページ

RADIUS の概要

Remote Authentication Dial-In User Service（RADIUS）とは、ネットワークへの管理アクセス権を取得しようとするユーザに対して中央管理されたセキュリティ機能を提供する、クライアント/サーバ プロトコルです。 このプロトコルは、ローカル認証や TACACS+ 認証と同様に、バックエンドのデータベースとして機能し、認証サービスおよびアカウンティング サービスを提供します。

- **認証**：コントローラにログインしようとするユーザを検証するプロセス。

  コントローラでRADIUS サーバに対してユーザが認証されるようにするには、ユーザは有効なユーザ名とパスワードを入力する必要があります。 複数のデータベースを設定する場合は、バックエンド データベースを試行する順序を指定できます。

- **アカウンティング**：ユーザによる処理と変更を記録するプロセス。

  ユーザによる処理が正常に実行される度に、RADIUS アカウンティング サーバでは、変更された属性、変更を行ったユーザのユーザ ID、ユーザがログインしたリモート ホスト、コマンドが実行された日付と時刻、ユーザの認可レベル、および実行された処理と入力された値の説明がログに記録されます。 RADIUS アカウンティング サーバが接続不能になった場合、ユーザはセッションを続行できなくなります。

RADIUS では、転送にユーザ データグラム プロトコル（UDP）を使用します。 RADIUS では、1 つのデータベースが保持されます。そして、UDP ポート 1812 で受信認証要求がリッスンされ、UDP ポート 1813 で受信アカウンティング要求がリッスンされます。 アクセス コントロールを要求するコントローラは、クライアントとして動作し、サーバから AAA サービスを要求します。コントローラとサーバ間のトラフィックは、プロトコルで定義されるアルゴリズムと、両方のデバイスにおいて設定される共有秘密キーによって暗号化されます。

複数の RADIUS アカウンティングおよび認証サーバを設定できます。 たとえば、1 台の RADIUS 認証サーバを中央に配置し、複数の RADIUS アカウンティング サーバを異なる地域に配置できます。 同じタイプのサーバを複数設定すると、最初のサーバで障害が発生したり、接続不能になったりしても、コントローラは、必要に応じて 2 台目や 3 台目あるいはそれ以降のサーバへの接続を自動的に試行します。

管理ユーザが RADIUS サーバを使用して認証される場合、PAP プロトコルだけが使用されます。Web 認証ユーザの場合、PAP、MSCHAPv2 および MD5 セキュリティ メカニズムがサポートされます。

RADIUS サーバのサポート

- RADIUS 認証サーバおよびアカウンティング サーバは、それぞれ最大 17 台まで設定できます。
- 冗長性を保つために複数の RADIUS サーバが設定されている場合、バックアップが適切に機能するようにするには、すべてのサーバでユーザ データベースを同一にする必要があります。
- ワンタイム パスワード（OTP）は、RADIUS を使用しているコントローラでサポートされます。 この設定では、コントローラがトランスペアレント パススルー デバイスとして動作します。 コントローラは、クライアント動作をチェックせずにすべてのクライアント要求を RADIUS サーバに転送します。 OTP を使用する場合は、クライアントが正しく機能するためにはコントローラへの接続を 1 つ確立する必要があります。 現在、コントローラには、複数の接続を確立しようとしているクライアントを修正するチェック機能はありません。
- RADIUS サーバで読み取り専用コントローラ ユーザを作成するには、サービス タイプをコールバック NAS プロンプトではなく NAS プロンプトに設定します。 サービス タイプをコールバック NAS プロンプトに設定すると、ユーザ認証は失敗しますが、NAS プロンプトに設定されることで、コントローラへの読み取り専用アクセスがユーザに与えられます。

  また、コールバック管理サービス タイプでは、ユーザにコントローラへのロビー アンバサダー権限が与えられます。
- RADIUS サーバが WLAN 単位でマッピングされている場合は、コントローラがその WLAN 上のグローバル リストに含まれている RADIUS サーバを使用しません。

Radius ACS サポート

- CiscoSecure Access Control Server（ACS）とコントローラの両方で、RADIUS を設定する必要があります。

- RADIUS は、CiscoSecure ACS バージョン 3.2 以降のリリースでサポートされます。 実行しているバージョンに対応する CiscoSecure ACS のマニュアルを参照してください。

プライマリおよびフォールバック RADIUS サーバ

プライマリ RADIUS サーバ（最も低いサーバインデックスを持つサーバ）は、コントローラの最優先サーバであるとみなされます。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（低い方から 2 番目の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。

RADIUS DNS

完全修飾ドメイン名（FQDN）を使用できます。これにより、必要に応じて IP アドレスを変更できます（たとえば、ロード バランシングの更新）。 サブメニューの [DNS] が [Security > AAA > RADIUS] メニューに追加されます。これを使用して、DNS から RADIUS IP 情報を取得できます。DNS クエリーはデフォルトでは無効になっています。

RADIUS の設定の制限

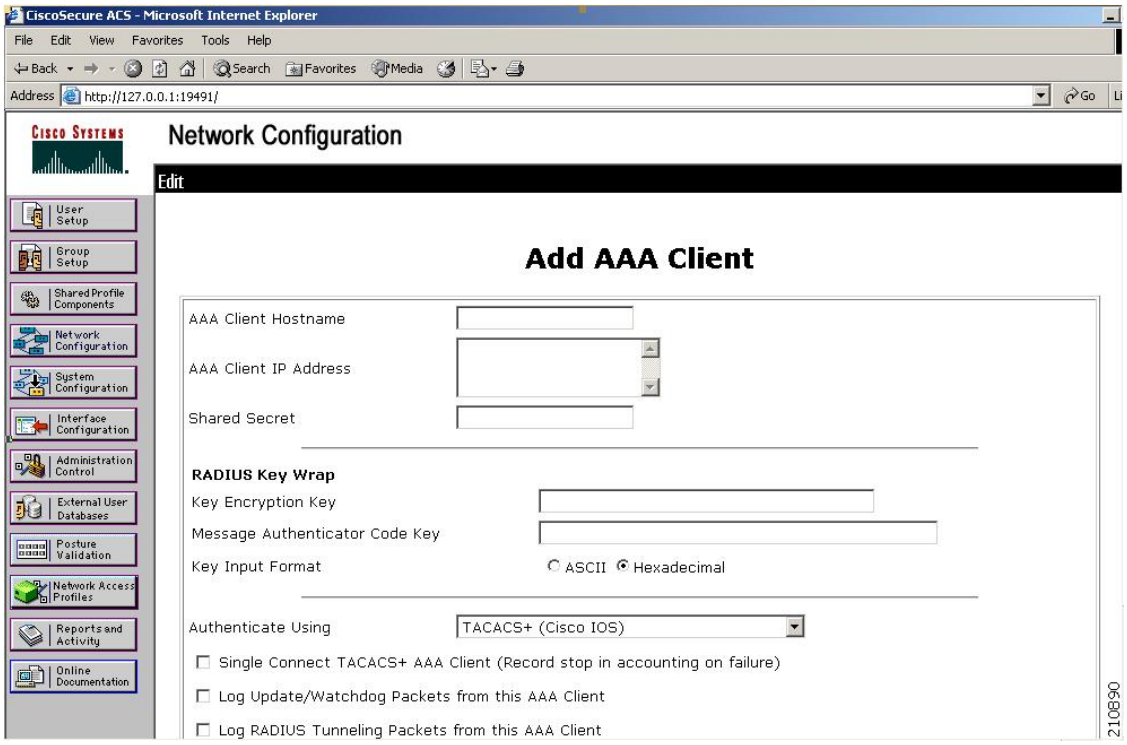
- RADIUS サーバのセッション タイムアウト値を最大 65535 秒に設定できます。 コントローラは、65535 秒を超える RADIUS サーバのセッション タイムアウト値の設定をサポートしません。
- RADIUS サーバに設定されているセッション タイムアウト値が 24 日間を超えている場合は、RADIUS セッション タイムアウト値は、WLAN を介してローカルに設定されたセッション タイムアウト値をオーバーライドしません。

ACS 上での RADIUS の設定

ステップ 1 ACS のメイン ページで、[Network Configuration] を選択します。

ステップ 2 [AAA Clients] の下の [Add Entry] を選択し、使用しているコントローラをサーバに追加します。 [Add AAA Client] ページが表示されます。

図 1：***CiscoSecure ACS の [Add AAA Client] ページ***



ステップ 3 [AAA Client Hostname] テキスト ボックスに、コントローラの名前を入力します。

ステップ 4 [AAA Client IP Address] テキスト ボックスに、コントローラの IP アドレスを入力します。

ステップ 5 [Shared Secret] テキスト ボックスに、サーバとコントローラ間の認証に使用する共有秘密キーを入力します。

（注） 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 6 [Authenticate Using] ドロップダウン リストから [RADIUS (Cisco Airespace)] を選択します。

ステップ 7 [Submit + Apply] をクリックして、変更内容を保存します。

ステップ 8 ACS のメイン ページで、[Interface Configuration] を選択します。

ステップ 9 [RADIUS (Cisco Aironet)] を選択します。 [RADIUS (Cisco Aironet)] ページが表示されます。

ステップ 10 [User Group] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにします。

ステップ 11 [Submit] をクリックして変更を保存します。

ステップ 12 ACS のメイン ページで、左のナビゲーション ペインから [System Configuration] を選択します。

ステップ 13 [Logging] を選択します。

ステップ 14 [Logging Configuration] ページが表示されたら、ログ記録するすべてのイベントを有効にし、変更内容を保存します。

ステップ 15 ACS のメイン ページで、左のナビゲーション ペインから [Group Setup] を選択します。

ステップ 16 [Group] ドロップダウン リストから、以前に作成したグループを選択します。

（注） この手順では、ユーザが割り当てられることになるロールに基づいて、ACS のグループにすでにユーザが割り当てられていることを想定しています。

ステップ 17 [Edit Settings] をクリックします。 [Group Setup] ページが表示されます。

ステップ 18 [Cisco Aironet Attributes] の [Cisco-Aironet-Session-Timeout] チェックボックスをオンにし、編集ボックスにセッション タイムアウト値を入力します。

ステップ 19 RADIUS 認証を使用したコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定します。読み取り専用アクセスが必要な場合は、Service-Type 属性（006）を [Callback NAS Prompt] に設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] に設定してください。 この属性を設定しない場合、認証プロセスはコントローラ上での認可エラーなしで正常に完了しますが、認証を再試行するようにプロンプトが表示されることがあります。

（注） ACS 上で Service-Type 属性を設定する場合は、必ずコントローラの GUI の [RADIUS Authentication Servers] ページ上にある [Management] チェックボックスをオンにします。

ステップ 20 [Submit] をクリックして変更を保存します。

RADIUS の設定（GUI）

ステップ 1 [Security] > [AAA] > [RADIUS] を選択します。

ステップ 2 次のいずれかの操作を行います。

- RADIUS サーバを認証用に設定する場合は、[Authentication] を選択します。
- RADIUS サーバをアカウンティング用に設定する場合は、[Accounting] を選択します。

（注） 認証およびアカウンティングの設定に使用されるページでは、ほとんど同じテキスト ボックスが表示されます。 そのため、ここでは [Authentication] ページを例にとって、設定の手順を一度だけ示します。 同じ手順に従って、複数のサービスまたは複数のサーバを設定できます。

[RADIUS Authentication（または Accounting）Servers] ページが表示されます。
このページには、これまでに設定されたすべての RADIUS サーバが表示されます。

- 既存のサーバを削除するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Remove] を選択します。
- コントローラが特定のサーバに到達できることを確認するには、そのサーバの青いドロップダウンの矢印の上にカーソルを置いて、[Ping] を選択します。

ステップ 3 [Acct Call Station ID Type] ドロップダウン リストから、Access-Request メッセージで RADIUS サーバに送信されるオプションを選択します。 次のオプションを使用できます。

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID
- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

（注） AP Name:SSID、AP Name、AP Group、Flex Group、AP Location、および VLAN ID オプションは、リリース 7.4 で追加されました。

AP Ethernet MAC Address および AP Ethernet MAC Address:SSID は 7.6 リリースで追加されました。

ステップ 4 [Auth Call Station ID Type] ドロップダウン リストから、Access-Request メッセージで RADIUS サーバに送信されるオプションを選択します。 次のオプションを使用できます。

- IP Address
- System MAC Address
- AP MAC Address
- AP MAC Address:SSID
- AP Name:SSID

- AP Name
- AP Group
- Flex Group
- AP Location
- VLAN ID
- AP Ethernet MAC Address
- AP Ethernet MAC Address:SSID

ステップ 5 [Use AES Key Wrap] チェックボックスをオンにし、AES キー ラップ保護を使用して RADIUS からコントローラへのキーの転送を有効にします。 デフォルト値はオフです。 この機能は、FIPS を使用するユーザにとって必要です。

ステップ 6 [MAC Delimiter] ドロップダウン リストから、Access-Request メッセージで RADIUS サーバに送信されるオプションを選択します。 次のオプションを使用できます。

- Colon
- Hyphen
- Single-hyphen
- None

ステップ 7 [Apply] をクリックします。 次のいずれかの操作を行います。

- 既存の RADIUS サーバを編集するには、そのサーバのサーバ インデックス番号をクリックします。 [RADIUS Authentication（または Accounting）Servers > Edit] ページが表示されます。
- RADIUS サーバを追加するには、[New] をクリックします。 [RADIUS Authentication（または Accounting）Servers > New] ページが表示されます。

ステップ 8 新しいサーバを追加している場合は、[Server Index（Priority）] ドロップダウン リストから数字を選択し、同じサービスを提供するその他の設定済みの RADIUS サーバに対してこのサーバの優先順位を指定します。

ステップ 9 新しいサーバを追加している場合は、[Server IP Address] テキスト ボックスに RADIUS サーバの IP アドレスを入力します。

（注） Auto IPv6 は、RADIUS サーバではサポートされていません。 RADIUS サーバを設定するときには Auto IPv6 アドレスを使用しないでください。 固定 IPv6 アドレスを代わりに使用してください。

ステップ 10 [Shared Secret Format] ドロップダウン リストから [ASCII] または [Hex] を選択し、コントローラと RADIUS サーバ間で使用される共有秘密キーの形式を指定します。 デフォルト値は [ASCII] です。

ステップ 11 [Shared Secret] テキスト ボックスと [Confirm Shared Secret] テキスト ボックスに、コントローラとサーバ間で認証に使用される共有秘密キーを入力します。

（注） 共有秘密キーは、サーバとコントローラの両方で同一である必要があります。

ステップ 12 新しい RADIUS 認証サーバを設定して AES キー ラップを有効にすると、コントローラと RADIUS サーバ間の共有秘密の安全性を高めることができます。そのための手順は次のとおりです。

（注） AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

a) [Key Wrap] チェックボックスをオンにします。
b) [Key Wrap Format] ドロップダウン リストから [ASCII] または [HEX] を選択して、AES キー ラップ キーの形式を Key Encryption Key（KEK）または Message Authentication Code Key（MACK）に指定します。
c) [Key Encryption Key (KEK)] テキスト ボックスに、16 バイトの KEK を入力します。
d) [Message Authentication Code Key (MACK)] テキスト ボックスに、20 バイトの KEK を入力します。

ステップ 13 新しいサーバを追加している場合は、[Port Number] テキスト ボックスに、インターフェイス プロトコルに対応する RADIUS サーバの UDP ポート番号を入力します。 有効な値の範囲は 1 ～ 65535 で、認証用のデフォルト値は 1812、アカウンティング用のデフォルト値は 1813 です。

ステップ 14 [Server Status] テキスト ボックスから [Enabled] を選択してこの RADIUS サーバを有効にするか、[Disabled] を選択して無効にします。 デフォルト値はイネーブルです。

ステップ 15 新しい RADIUS 認証サーバを設定している場合は、[Support for RFC 3576] ドロップダウン リストから [Enabled] を選択して RFC 3576 を有効にするか、[Disabled] を選択してこの機能を無効にします。RFC 3576 では、ユーザ セッションの動的な変更を可能にするよう RADIUS プロトコルが拡張されています。 デフォルト値は [Enabled] です。 RFC 3576 では、ユーザの切断およびユーザ セッションに適用される許可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。 Disconnect メッセージはユーザ セッションをただちに終了させ、CoA メッセージはデータ フィルタなどのセッション認証属性を変更します。

ステップ 16 [Server Timeout] テキスト ボックスに、再送信の間隔を秒単位で入力します。 有効な範囲は 2 ～ 30 秒で、デフォルト値は 2 秒です。
[Key Wrap] チェックボックスをオンにします。

（注） 再認証が繰り返し試行されたり、プライマリ サーバがアクティブで接続可能なときにコントローラがバックアップ サーバにフォールバックしたりする場合には、タイムアウト値を増やすことをお勧めします。

ステップ 17 [Network User] チェックボックスをオンにしてネットワーク ユーザ認証（またはアカウンティング）を有効にするか、オフにしてこの機能を無効にします。 デフォルト値はオンです。 この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS 認証（アカウンティング）サーバと見なされます。 WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。

ステップ 18 RADIUS 認証サーバを設定している場合は、[Management] チェックボックスをオンにして管理認証を有効にするか、オフにしてこの機能を無効にします。 デフォルト値はオンです。 この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。

ステップ 19 [IPSec] チェックボックスをオンにして IP セキュリティ メカニズムを有効にするか、オフにしてこの機能を無効にします。 デフォルト値はオフです。

（注） IPSec は IPv6 ではサポートされません。 サーバの IP アドレスに IPv4 を使用した場合にのみ使用してください。

ステップ 20 ステップ *17* で IPSec を有効にした場合は、次の手順に従って追加の IPSec パラメータを設定します。

a) [IPSec] ドロップダウン リストから、IP セキュリティで使用する認証プロトコルとして、[HMAC MD5] または [HMAC SHA1] のいずれかのオプションを選択します。 デフォルト値は [HMAC SHA1] です。
Message Authentication Code（MAC; メッセージ認証コード）は、秘密キーを共有する 2 者間で送信される情報を検証するために使用されます。 HMAC（Hash MAC）は暗号ハッシュ関数に基づくメカニズムです。 任意の反復暗号ハッシュ関数との組み合わせで使用できます。 HMAC でハッシュ関数として MD5 を使用するのが HMAC MD5 であり、SHA1 を使用するのが HMAC SHA1 です。 また、HMAC では、メッセージ認証値の計算と検証に秘密キーを使用します。

b) [IPSec Encryption] ドロップダウン リストで次のオプションのいずれかを選択して、IP セキュリティ暗号化メカニズムを指定します。

- [DES]：データ暗号化規格。プライベート（秘密）キーを使用するデータ暗号化の方法です。 DES では、56 ビットのキーを 64 ビットのデータ ブロックごとに適用します。
- [3DES]：連続して 3 つのキーを適用するデータ暗号化規格です。 これはデフォルト値です。
- [AES CBC]：高度暗号化規格。128、192、または 256 ビット長のキーを使用して 128、192、または256 ビット長のデータ ブロックを暗号化します。 AES 128 CBC では、暗号ブロック連鎖（CBC）モードで 128 ビットのデータ パスを使用します。
- [256-AES]：256 ビット長のキーを使用する高度暗号化規格。

c) [IKE Phase 1] ドロップダウン リストから [Aggressive] または [Main] のいずれかのオプションを選択して、インターネット キー交換（IKE）プロトコルを指定します。 デフォルト値は [Aggressive] です。
IKE Phase 1 は、IKE の保護方法をネゴシエートするために使用されます。 Aggressive モードでは、セキュリティ ゲートウェイの ID をクリアで送信するだけで、わずかに高速な接続が確立され、より少ないパケットでより多くの情報が渡されます。

d) [Lifetime] テキスト ボックスに値（秒単位）を入力して、セッションのタイムアウト間隔を指定します。 有効な範囲は 1800 ～ 57600 秒で、デフォルト値は 1800 秒です。

e) [IKE Diffie Hellman Group] ドロップダウン リストから [Group 1 (768 bits)]、[Group 2 (1024 bits)]、または [Group 5 (1536 bits)] のいずれかのオプションを選択して、IKE Diffie Hellman グループを指定します。 デフォルト値は [Group 1 (768 bits)] です。
Diffie Hellman 技術を 2 つのデバイスで使用して共通キーを生成します。このキーを使用すると、値を公開された状態で交換して、同じ共通キーを生成することができます。 3 つのグループのすべてで従来の攻撃に対するセキュリティが確保されますが、キーのサイズが大きいことから、Group 5 の安全性がより高くなります。 ただし、Group 1 および Group 2 のキーを使用した計算は、素数サイズがより小さいために、多少高速に実行される可能性があります。

（注） IPSec の共有秘密が設定されていない場合、デフォルトの RADIUS 共有秘密が使用されます。認証方式が PSK の場合、IPSec 共有秘密を使用するために WLANCC を有効にする必要があります。無効の場合はデフォルト値が使用されます。 [Controller] > [Inventory] で WLANCC および UCAPL の前提条件モードの状態を表示できます。

ステップ 21 [Apply] をクリックします。

ステップ 22 [Save Configuration] をクリックします。

ステップ 23 同じサーバ上または追加の RADIUS サーバ上で追加のサービスを設定する場合は、上記の手順を繰り返します。

ステップ 24 次の手順を実行して、RADIUS サーバ フォールバックの動作を指定します。

a) [Security] > [AAA] > [RADIUS] > [Fallback to open the RADIUS] > [Fallback Parameters] の順に選択し、[Fallback Parameters] ページを開きます。

b) [Fallback Mode] ドロップダウン リストから、次のオプションのいずれかを選択します。

- [Off]：RADIUS サーバのフォールバックを無効にします。 これはデフォルト値です。
- [Passive]：コントローラが、関係のないプローブ メッセージを使用することなく、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するようにします。 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、あとで 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。
- [Active]：コントローラが、RADIUS プローブ 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するようにします。 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。 プライマリ サーバが回復した ACS サーバからの応答を一旦受信すると、アクティブ フォールバック RADIUS サーバは、アクティブ プローブ認証を要求しているサーバにプローブ メッセージを送信しなくなります。

c) ステップ *b* でフォールバック モードを [Active] にした場合は、非アクティブなサーバ プローブで送信される名前を [Username] テキスト ボックスに入力します。 最大 16 文字の英数字を入力できます。 デフォルト値は「cisco-probe」です。

d) ステップ *b* でフォールバック モードを [Active] にした場合は、[Interval in Sec] テキスト ボックスにプローブ間隔値（秒単位）を入力します。 この間隔は、Passive モードでの非アクティブ時間、および Active モードでのプローブ間隔としての意味を持ちます。 有効な範囲は 180 ～ 3600 秒で、デフォルト値は 300 秒です。

ステップ 25 次の手順で、RADIUS DNS パラメータを指定します。

（注） IPv6 は RADIUS DNS ではサポートされません。

a) [Security] > [AAA] > [RADIUS] > [DNS] を選択します。 [RADIUS DNS Parameters] ページが表示されます。

b) [DNS Query] チェックボックスをオンまたはオフにします。

c) [Port Number] テキスト ボックスに、認証ポート番号を入力します。 有効な範囲は 1 ～ 65535 です。 アカウンティング ポート番号は認証ポート番号に 1 を加えた値です。 たとえば、認証ポート番号を 1812 と定義すると、アカウンティング ポート番号は 1813 です。 アカウンティング ポート番号は常に認証ポート番号から取得されます。

d) [Secret Format] ドロップダウン リストから、秘密を設定する形式を選択します。 有効なオプションは [ASCII] と [Hex] です。

e) 選択した形式に応じて秘密を入力して確定します。
（注） すべてのサーバで同じ認証ポートおよび同じ秘密を使用する必要があります。

f) [DNS Timeout] テキスト ボックスに、DNS サーバから最新の更新を取得するために DNS クエリーがリフレッシュされるまでの日数を入力します。

g) [URL] テキスト ボックスに、RADIUS サーバの完全修飾ドメイン名または絶対ドメイン名を入力します。

h) [Server IP Address] テキスト ボックスに、DNS サーバの IP アドレスを入力します。

i) [Apply] をクリックします。

ステップ 26 [Security] > [Priority Order] > [Management User] の順に選択し、複数のデータベースを設定する際の認証の順序を指定します。 [Priority Order > Management User] ページが表示されます。

ステップ 27 [Order Used for Authentication] テキスト ボックスで、コントローラが管理ユーザを認証する際にどのサーバを優先するかを指定します。 [Not Used] テキスト ボックスと [Order Used for Authentication] テキスト ボックスの間でサーバを移動するには、[>] および [<] ボタンを使用します。 希望するサーバが [Order Used for Authentication] テキスト ボックスに表示されたら、[Up] ボタンと [Down] ボタンを使用して優先するサーバをリストの先頭に移動します。
デフォルトで、ローカル データベースは常に最初に検索されます。 ユーザ名が見つからない場合、コントローラは、RADIUS に設定されている場合は RADIUS サーバへの切り換え、TACACS+ に設定されている場合は TACACS+ サーバへの切り換えを行います。 デフォルトの設定はローカル、RADIUS の順になっています。

ステップ 28 [Apply] をクリックします。

ステップ 29 [Save Configuration] をクリックします。

RADIUS の設定（CLI）

- 次のコマンドを入力して、発信元の IP アドレス、システム MAC アドレス、AP MAC アドレス、AP イーサネット MAC アドレスが Access-Request メッセージで RADIUS サーバに送信されるかどうかを指定します。
  config radius callStationIdType {ipaddr | macaddr | ap-macaddr-only | ap-macaddr-ssid | ap-ethmac-only | ap-ethmac-ssid | ap-group-name | ap-label-address | ap-label-address-ssid | ap-location | ap-name | ap-name-ssid | flex-group-name | vlan-id}

  このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

（注） デフォルトは、システムの MAC アドレスです。

注意 IPv6 専用クライアントには発信側ステーション ID タイプを使用しないでください。

- 次のコマンドを入力して、Access-Request メッセージで RADIUS 認証サーバまたはアカウンティング サーバに送信される MAC アドレスにデリミタを指定します。
  config radius{**auth** | **acct**} **mac-delimiter** {*colon* | *hyphen* | *single-hyphen* | *none*}

  値は次のとおりです。

  - **colon** はデリミタをコロンに設定します（書式は xx:xx:xx:xx:xx:xx となります）。
  - **hyphen** はデリミタをハイフンに設定します（書式は xx-xx-xx-xx-xx-xx となります）。これはデフォルト値です。
  - **single-hyphen** はデリミタを単一のハイフンに設定します（書式は xxxxxx-xxxxxx となります）。
  - **none** はデリミタを無効にします（書式は xxxxxxxxxxxx となります）。

- 次のコマンドを入力して、RADIUS 認証サーバを設定します。

  - **config radius auth add***index server_ip_address port_number* {**ascii** | **hex**} **shared_secret**：RADIUS 認証サーバを追加します。

    このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。

  - **config radius auth keywrap** {**enable** | **disable**}：AES キー ラップを有効にします。これにより、コントローラと RADIUS サーバ間の共有秘密の安全性が高まります。 AES キー ラップは、Federal Information Processing Standards（FIPS）を使用するユーザのために設計されており、キー ラップ準拠の RADIUS 認証サーバを必要とします。

  - **config radius auth keywrap add {ascii** | **hex**} *kek mack index*：AES キー ラップ属性を設定します。

    値は次のとおりです。

    - *kek* では、16 バイトの Key Encryption Key（KEK）が指定されます。
    - *mack* では、20 バイトの Message Authentication Code Key（MACK）が指定されます。
    - *index* では、AES キー ラップを設定する RADIUS 認証サーバのインデックスが指定されます。

  - **config radius auth rfc3576 {enable** | **disable**} *index*：RFC 3576 を有効または無効にします。RFC 3576 では、ユーザ セッションの動的な変更を可能にするように RADIUS プロトコルが拡張されています。 RFC 3576 では、ユーザの切断およびユーザ セッションに適用される許可の変更のほか、Disconnect メッセージと Change-of-Authorization（CoA）メッセージがサポートされています。 Disconnect メッセージはユーザセッションをただちに終了させ、CoA メッセージはデータ フィルタなどのセッション認証属性を変更します。

  - **config radius auth retransmit-timeout***index timeout*：RADIUS 認証サーバの再送信のタイムアウト値を設定します。

  - **config radius auth mgmt-retransmit-timeout***index timeout*：RADIUS 認証サーバのデフォルト管理ログイン再送信タイムアウトを設定します。

- **config radius auth network***index***{enable | disable}**：ネットワーク ユーザ認証を有効または無効にします。 この機能を有効にすると、ここで設定するサーバはネットワークユーザの RADIUS 認証サーバと見なされます。 WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius auth management***index***{enable | disable}**：管理認証を有効または無効にします。 この機能を有効にすると、ここで設定するサーバは管理ユーザの RADIUS 認証サーバと見なされ、認証要求が RADIUS サーバに送られます。
- **config radius auth ipsec {enable | disable}** *index*：IP セキュリティ メカニズムを有効または無効にします。
- **config radius auth ipsec authentication {hmac-md5 | hmac-sha1}** *index*：IP セキュリティに使用する認証プロトコルを設定します。
- **config radius auth ipsec encryption {256-aes | 3des | aes | des | none}** *index*：IP セキュリティ暗号化メカニズムを設定します。
- **config radius auth ipsec ikedh-group {group-1 | group-2 | group-5| 2048bit-group-14}** *index*：IKE Diffie-Hellman グループを設定します。
- **config radius auth ipsec ikelifetime***interval index*：セッションのタイムアウト間隔を設定します。
- **config radius auth ipsec ikephase1{aggressive | main}***index*：Internet Key Exchange（IKE）プロトコルを設定します。
- **config radius auth ipsec ike auth-method {PSK | certificate}** *index*：IKE 認証方式を設定します。 デフォルトでは、PSK は IPSEC セッションで使用されます。
- **config radius auth ipsec ike auth-modepre-shared-key***indexhex/asciisecret*：IPSEC 事前共有キーを設定します。
- **config radius auth ipsec ike auth-mode {pre-shared-key***index hex-ascii-index shared-secret* **| certificate***index***}**：IKE 認証方式を設定します。 デフォルトでは、事前共有キーは IPSEC セッションで使用されます。
- **config radius auth {enable | disable}** *index*：RADIUS 認証サーバを有効または無効にします。
- **config radius auth delete***index*：以前に追加された RADIUS 認証サーバを削除します。

- 次のコマンドを入力して、RADIUS アカウンティング サーバを設定します。
  - **config radius acct add***index server_ip_address port#* **{ascii | hex}** *shared_secret*：RADIUS アカウンティング サーバを追加します。

    このコマンドは、 IPv4 と IPv6 の両方のアドレス形式をサポートします。
  - **config radius acct server-timeout***index timeout*：RADIUS アカウンティング サーバの再送信のタイムアウト値を設定します。

- **config radius acct network***index***{enable | disable}**：ネットワーク ユーザ アカウンティングを有効または無効にします。 この機能を有効にすると、ここで設定するサーバはネットワーク ユーザの RADIUS アカウンティング サーバと見なされます。 WLAN 上の RADIUS サーバを設定しなかった場合は、ネットワーク ユーザに対してこのオプションを有効にする必要があります。
- **config radius acct ipsec{enable | disable}** *index*：IP セキュリティ メカニズムを有効または無効にします。
- **config radius acct ipsec authentication {hmac-md5 | hmac-sha1}** *index*：IP セキュリティに使用する認証プロトコルを設定します。
- **config radius acct ipsec encryption {256-aes | 3des| aes|des|none}** *index*：IP セキュリティ暗号化メカニズムを設定します。
- **config radius acct ipsec ike dh-group {2048bit-group-14 | group-1 | group-2 | group-5}** *index*：IKE Diffie-Hellman グループを設定します。
- **config radius acct ipsec ike lifetime***interval index*：セッションのタイムアウト間隔を設定します。
- **config radius acct ipsec ike auth-mode {pre-shared-key***index hex-ascii-index shared-secret* **| certificate***index***}**：IKE 認証方式を設定します。 デフォルトでは、事前共有キーは IPSEC セッションで使用されます。
- **config radius acct ipsec ike phase1{aggressive | main}***index*：インターネット キー交換（IKE）プロトコルを設定します。
- **config radius acct {enable | disable}** index：RADIUS アカウンティング サーバを有効または無効にします。
- **config radius acct deleteindex**：以前に追加された RADIUS アカウンティング サーバを削除します。
- **config radius acct region{group | none | provincial}**：RADIUS リージョンを設定します。
- **config radius acct realm{add | delete }** *radius-index realm-string*：RADIUS アカウンティング サーバのレルムを設定します。
- **config radius auth callStationIdType {ap-ethmac-only | ap-ethmac-ssid}**：SSID の有無にかかわらず AP の無線 MAC アドレスになるように発信側ステーション ID タイプを設定します。
- **config radius auth callStationIdType***ap-label-address*：発信側ステーション ID タイプを、認証メッセージに対して、AP ラベルに表示されている AP MAC アドレスに設定します。
  config radius auth callStationIdType*ap-label-address-ssid*：発信側ステーション ID タイプを、認証メッセージに対して、<AP label MAC address>:<SSID> 形式に設定します。
- **config radius auth callStationIdTypeap-group-name**：AP グループ名を使用する発信側ステーション ID タイプを設定します。 AP が AP グループの一部でない場合、「default-group」が AP グループ名として使用されます。

- **config radius auth callStationIdTypeap-location**：AP ロケーションの発信側ステーション ID を設定します。
- **config radius auth callStationIdType** {**ap-macaddr-only** | **ap-macaddr-ssid**}：SSID の有無にかかわらず、AP の無線 MAC アドレスになるように発信側ステーション ID タイプを設定します（SSID がある場合は <AP 無線 MAC アドレス>:<SSID> 形式）。
- **config radius auth callStationIdType** {**ap-name** | **ap-name-ssid**}：SSID の有無にかかわらず、AP 名になるように発信側ステーション ID を設定します（SSID がある場合は <AP 名>:<SSID> 形式）。

（注） 発信側ステーション ID タイプが AP 名に設定されている場合、AP 名の大文字から小文字への変換は考慮されません。 たとえば AP を作成する場合に、AP 名が大文字で指定されると、発信側ステーション ID タイプの AP 名はすべて大文字で表示されます。

- **config radius auth callStationIdTypeflex-group-name**：発信側ステーション ID タイプを FlexConnect グループ名に設定します。
- **config radius auth callStationIdType** {**ipaddr** | **macaddr**}：発信側ステーション ID タイプを IP アドレス（レイヤ 3 のみ）またはシステムの MAC アドレスに設定します。
- **config radius auth callStationIdTypevlan-id**：発信側ステーション ID タイプをシステムの VLAN ID に設定します。

- 次のコマンドを入力して、RADIUS サーバのフォールバック動作を設定します。
  config radius fallback-test mode{off | passive | active}

  値は次のとおりです。

  - **off** は RADIUS サーバのフォールバックを無効にします。
  - **passive** は、コントローラが、関係のないプローブ メッセージを使用することなく、使用可能なバックアップ サーバから優先順位のより低いサーバへ復帰するようにします。当座は非アクティブなすべてのサーバを無視し、その後、RADIUS メッセージの送信が必要になったとき再試行します。
  - **active** は、コントローラが、RADIUS プローブ メッセージを使用して、使用可能なバックアップ サーバから優先順位のより低いサーバへ復帰し、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するようにします。アクティブな RADIUS 要求に対して、コントローラは単に非アクティブなすべてのサーバを無視します。プライマリ サーバが回復した ACS サーバからの応答を一旦受信すると、アクティブ フォールバック RADIUS サーバは、アクティブ プローブ認証を要求しているサーバにプローブ メッセージを送信しなくなります。

- ステップ *5* で Active モードを有効にした場合は、次のコマンドを入力して追加のフォールバック パラメータを設定します。

- **config radius fallback-test username***username*：非アクティブなサーバ プローブで送信する名前を指定します。 *username* パラメータには、最大 16 文字の英数字を入力できます。
- **config radius fallback-test interval***interval*：プローブ間隔の値（秒単位）を指定します。

- 次のコマンドを入力して、RADIUS DNS パラメータを設定します。
  - **config radius dns global***port-num* {*ascii* | *hex*} *secret*：RADIUS DNS のグローバル ポート番号と機密情報を追加します。
  - **config radius dns query***url timeout-in-days*：RADIUS サーバの FQDN、および DNS サーバから最新の更新を取得するためにリフレッシュが実行されるまでのタイムアウトを設定します。
  - **config radius dns serverip***ip-addr*：DNS サーバの IP アドレスを設定します。
  - **config radius dns** {**enable** | **disable**}：DNS クエリーを有効または無効にします。

- RADIUS 拡張送信元ポートのサポートを設定するには、次のコマンドを入力します。
  config radius ext-source-ports {**enable** | **disable**}
  複数の送信元ポートを有効にすると、未処理の RADIUS 要求の数が増えます。 1 つの送信元ポートを使用している場合は、未処理の要求の数が認証要求とアカウンティング要求のそれぞれで 255 に制限されます。

  さまざまな WLC プラットフォームでサポートされる RADIUS キューの数：
  - 5508 および WiSM2 は 8 つの RADIUS キューをサポート
  - 5520、Flex 7500 シリーズ、および 8500 シリーズは 16 の RADIUS キューをサポート

- 次のコマンドを入力して、変更を保存します。
  save config
- 次のコマンドを入力して、複数のデータベースを設定する際の認証の順序を設定します。
  config aaa auth mgmt*AAA_server_type AAA_server_type*

  ここで、*AAA_server_type is* は local、radius、または tacacs となります。

  現在の管理認証サーバの順序を表示するには、show aaa auth コマンドを入力します。
- 次のコマンドを入力して、RADIUS の統計情報を表示します
  - **show radius summary**：RADIUS サーバ、および AP イーサネット MAC 設定による統計情報の概要を表示します。
  - **show radius auth statistics**：RADIUS 認証サーバの統計情報を表示します。
  - **show radius acct statistics**：RADIUS アカウンティング サーバの統計情報を表示します。
  - **show radius rfc3576 statistics**：RADIUS RFC 3576 サーバの概要を表示します。

- 次のコマンドを入力して、アクティブなセキュリティ アソシエーションを表示します。

- **show ike {brief | detailed}***ip_or_mac_addr*：アクティブな IKE セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。
- **show ipsec {brief | detailed}***ip_or_mac_addr*：アクティブな IPSec セキュリティ アソシエーションの簡単な概要または詳しい要約を表示します。

- 次のコマンドを入力して、1 台または複数の RADIUS サーバの統計情報をクリアします。
  clear stats radius {**auth** | **acct**} {*index* | **all**}
- 次のコマンドを入力して、コントローラが RADIUS サーバに到達できることを確認します。
  ping*server_ip_address*

コントローラによって送信される RADIUS 認証属性

次の表は、Access-Request パケットおよび Access-Accept パケットで、コントローラと RADIUS サーバ間で送信される RADIUS 認証属性を示しています。

表 *1*：*Access-Request* パケットで送信される認証属性

属性 ID	説明
1	User-Name
2	Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type[1]
12	Framed-MTU
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier
33	Proxy-State
60	CHAP-Challenge
61	NAS-Port-Type
79	EAP-Message
243	TPLUS-Role

[1] RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。

表 *2* : ***Access-Accept*** パケットで受け付けられる認証属性（シスコ）

属性 ID	説明
1	Cisco-LEAP-Session-Key
2	Cisco-Keywrap-Msg-Auth-Code
3	Cisco-Keywrap-NonCE
4	Cisco-Keywrap-Key
5	Cisco-URL-Redirect
6	Cisco-URL-Redirect-ACL

（注） シスコ固有の属性 Auth-Algo-Type および SSID はサポートされません。

表 *3* : ***Access-Accept*** パケットで受け付けられる認証属性（標準）

属性 ID	説明
6	Service-Type RADIUS 認証を使用してコントローラへの読み取り専用アクセスまたは読み取りと書き込みアクセスを指定するには、RADIUS サーバで Service-Type 属性（6）を設定する必要があります。読み取り専用アクセスが必要な場合は [Callback NAS Prompt] を設定し、読み取りと書き込みの両方の権限が必要な場合は [Administrative] を設定してください。
8	Framed-IP-Address
25	Class
26	Vendor-Specific
27	Timeout
29	Termination-Action
40	Acct-Status-Type
64	Tunnel-Type
79	EAP-Message
81	Tunnel-Group-ID

（注） メッセージ認証はサポートされていません。

表 *4*：***Access-Accept*** パケットで受け付けられる認証属性（***Microsoft***）

属性 ID	説明
11	MS-CHAP-Challenge
16	MS-MPPE-Send-Key
17	MS-MPPE-Receive-Key
25	MS-MSCHAP2-Response
26	MS-MSCHAP2-Success

表 *5*：***Access-Accept*** パケットで受け付けられる認証属性（***Airespace***）

属性 ID	説明
1	VAP-ID
3	DSCP
4	8021P-Type
5	VLAN-Interface-Name
6	ACL-Name
7	Data-Bandwidth-Average-Contract
8	Real-Time-Bandwidth-Average-Contract
9	Data-Bandwidth-Burst-Contract
10	Real-Time-Bandwidth-Burst-Contract
11	Guest-Role-Name
13	Data-Bandwidth-Average-Contract-US
14	Real-Time-Bandwidth-Average-Contract-US
15	Data-Bandwidth-Burst-Contract-US
16	Real-Time-Bandwidth-Burst-Contract-US

Access-Accept パケットで受け付けられる認証属性（Airespace）

この項では、Cisco WLC で現在サポートされている RADIUS 認証の Airespace 属性について説明します。

VAP ID

この属性は、クライアントが属する WLAN の WLAN ID を示します。 RADIUS Access Accept に WLAN-ID 属性が指定されている場合、システムでは認証後に WLAN-ID（SSID）がクライアントステーションに適用されます。 WLAN ID は、Cisco WLC によって IPsec 以外のすべての認証のインスタンスで送信されます。 Web 認証では、Cisco WLC が AAA サーバからの認証応答で WLAN-ID 属性を受信し、これが WLAN の ID に一致しない場合、認証が拒否されます。 DotIX/Mac フィルタリングも拒否されます。 AAA サーバからの応答に基づく拒否は、SSID Cisco-AVPair サポートが原因です。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           WLAN ID (VALUE)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 1
- Vendor length – 4
- Value –クライアントが属する WLAN の ID。

QoS-Level

この属性は、スイッチングファブリック内、および無線経由のモバイルクライアントのトラフィックに適用される QoS レベルを示しています。 この例は、QoS-Level 属性フォーマットの要約を示しています。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                           QoS Level                           |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）

- Length – 10
- Vendor-Id – 14179
- Vendor type – 2
- Vendor length – 4
- Value – 3 オクテット：
  - 3 – Bronze（バックグラウンド）
  - 0 - Silver（ベストエフォート）
  - 1 – Gold（ビデオ）
  - 2 – Platinum（音声）

Diffserv コード ポイント（DSCP）

DSCP は QoS レベルに基づく Diffserv の提供に使用できるパケット ヘッダー コードです。 この属性は、クライアントに適用される DSCP 値を定義します。 RADIUS Access Accept に値が指定されている場合、DSCP 値によって、WLAN プロファイルで指定された DSCP 値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                        DSCP (VALUE)                           |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 3
- Vendor length – 4
- Value – クライアントに適用される DSCP 値。

802.1p Tag Type

クライアントから受信した 802.1p VLAN タグ（アクセス プライオリティを定義する）。 このタグはクライアントとネットワーク間のパケットの QoS レベルにマッピングされます。 この属性は、クライアントに適用される 802.1p プライオリティを定義します。 RADIUS Access Accept に値が指定されている場合、802.1p 値によって、WLAN プロファイルで指定されたデフォルトが上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
```

```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                      802.1p (VALUE)                           |

+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 4
- Vendor length – 3
- Value – クライアントに適用される 802.1p プライオリティ。

VLAN Interface Name

この属性は、クライアントが関連付けられる VLAN インターフェイスを示します。 Interface-Name 属性形式の要約を次に示します。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          |  Vendor type  | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|    Interface Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 5
- Vendor length – >0
- Value – クライアントが割り当てられるインターフェイスの名前を含む文字列

（注） この属性は、MAC フィルタリングが有効になっている場合、またはセキュリティ ポリシーとして 802.1X または WPA が使用されている場合にのみ機能します。

ACL-Name

この属性は、クライアントに適用される ACL 名を示します。 ACL-Name 属性形式の要約を次に示します。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        ACL Name...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – >7
- Vendor-Id – 14179
- Vendor type – 6
- Vendor length – >0
- Value – クライアントに対して使用する ACL の名前を含む文字列

Data Bandwidth Average Contract

この属性は、レート制限値です。 TCP などの非リアルタイム トラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。 この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Data Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均データレート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Data Bandwidth Average Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 7
- Vendor length – 4
- Value – 値（Kbps 単位）

Real Time Bandwidth Average Contract

この属性は、レート制限値です。 UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。 この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均リアルタイム レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Real Time Bandwidth Average Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 8
- Vendor length – 4
- Value – 値（Kbps 単位）

Data Bandwidth Burst Contract

この属性は、レート制限値です。 TCP などの非リアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。 この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Data Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバースト データ レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Data Bandwidth Burst Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 9
- Vendor length – 4
- Value – 値（Kbps 単位）

Real Time Bandwidth Burst Contract

この属性は、レート制限値です。 UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。 この値は、有線から無線へのダウンストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバースト リアルタイム レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Real Time Bandwidth Burst Contract...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 10
- Vendor length – 4
- Value – 値（Kbps 単位）

Guest Role Name

この属性は、認証ユーザに適用される帯域幅コントラクト値を提供します。 RADIUS Access Accept に値が指定されている場合、ゲスト ロールに定義された帯域幅コントラクト値によって、WLAN に指定された帯域幅コントラクト値（QoS 値に基づく）が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        GuestRoleName ...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 11
- Vendor length – ゲスト ロール名の長さに基づく変数
- Value – 英数字の文字列

Data Bandwidth Average Contract Upstream

この属性は、レート制限値です。 TCP などの非リアルタイム トラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。 この値は、無線から有線へのアップストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Data Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均データ レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Data Bandwidth Average Contract Upstream...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 13
- Vendor length – 4
- Value – 値（Kbps 単位）

Real Time Bandwidth Average Contract Upstream

この属性は、レート制限値です。 UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Average Contract を示します。 この値は、無線から有線へのアップストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Average Contract 値によって、WLAN または QoS プロファイルで指定された平均リアル タイム レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Real Time Bandwidth Average Contract Upstream...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 14
- Vendor length – 4
- Value – 値（Kbps 単位）

Data Bandwidth Burst Contract Upstream

この属性は、レート制限値です。 TCP などの非リアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。 この値は、無線から有線へのアップストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Data Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバースト データ レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Data Bandwidth Burst Contract Upstream...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 15
- Vendor length – 4
- Value – 値（Kbps 単位）

Real Time Bandwidth Burst Contract Upstream

この属性は、レート制限値です。 UDP などのリアルタイム トラフィック用にクライアントに適用される Data Bandwidth Burst Contract を示します。 この値は、無線から有線へのアップストリーム方向にのみ当てはまります。 RADIUS Access Accept に値が指定されている場合、Real Time Bandwidth Burst Contract 値によって、WLAN または QoS プロファイルで指定されたバースト リアルタイム レート値が上書きされます。 フィールドは左から右に伝送されます。

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |  Length       |            Vendor-Id
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
     Vendor-Id (cont.)          | Vendor type   | Vendor length |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|        Real Time Bandwidth Burst Contract Upstream...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

- Type – 26（ベンダー固有）
- Length – 10
- Vendor-Id – 14179
- Vendor type – 16
- Vendor length – 4
- Value – 値（Kbps 単位）

RADIUS アカウンティング属性

次の表に、コントローラから RADIUS サーバに送信されるアカウンティング要求の RADIUS アカウンティング属性を示します。

表 *6*：アカウンティング要求のアカウンティング属性

属性 ID	説明
1	User-Name
4	NAS-IP-Address
5	NAS-Port
8	Framed-IP-Address
25	Class
30	Called-Station-ID（MAC アドレス）
31	Calling-Station-ID（MAC アドレス）
32	NAS-Identifier
40	Accounting-Status-Type
41	Accounting-Delay-Time（ストップおよび中間メッセージのみ）
42	Accounting-Input-Octets（ストップおよび中間メッセージのみ）
43	Accounting-Output-Octets（ストップおよび中間メッセージのみ）
44	Accounting-Session-ID
45	Accounting-Authentic
46	Accounting-Session-Time（ストップおよび中間メッセージのみ）
47	Accounting-Input-Packets（ストップおよび中間メッセージのみ）
48	Accounting-Output-Packets（ストップおよび中間メッセージのみ）
49	Accounting-Terminate-Cause（ストップおよび中間メッセージのみ）
52	Accounting-Input-Gigawords
53	Accounting-Output-Gigawords
55	Event-Timestamp
64	Tunnel-Type
65	Tunnel-Medium-Type
81	Tunnel-Group-ID

属性 ID	説明
	IPv6-Framed-Prefix
190	IPv6-Framed-Address

次の表に Accounting-Status-Type 属性（40）のさまざまな値の一覧を示します。

表 *7*：*Accounting-Status-Type* 属性の値

属性 ID	説明
1	Start
2	Stop
3	Interim-Update （注） クライアントの WLAN で RADIUS サーバ アカウンティング - 暫定アップデート機能が有効になっていない場合でも、各クライアントの認証時に RADIUS 中間アカウンティング アップデートが送信されます。
7	Accounting-On
8	Accounting-Off
9-14	トンネリングのアカウンティング用に予約
15	Failed 用に予約