# AAA サーバとしての無線ドメイン サービス AP の設定例

## 目次



## 概要

このドキュメントでは、次の機能を実行するアクセス ポイント（AP）を設定する設定例について説明します。

- Wireless Domain Services（WDS; ワイヤレス ドメイン サービス）を提供するアクセス ポイント
- Authentication, Authorization, and Accounting（AAA; 認証、認可、アカウンティング）サーバの役割を実行するアクセス ポイント

WDS に参加しているインフラストラクチャ AP とクライアント デバイスを認証する外部 RADIUS サーバを配置していない場合、このような構成を使用できます。

## 前提条件

### 要件

この設定を行う前に、次の要件が満たされていることを確認します。

- WDS に関する基本的な知識
- 現行の Extensible Authentication Protocol（EAP）セキュリティ方式に関する知識

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco IOS® ソフトウェア リリース 12.3(7)JA1 が稼働する Cisco Aironet 1200 シリーズ AP

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

### 表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

## 背景説明

WDS は、Cisco Structured Wireless-Aware Network（SWAN）の一部です。 WDS は、ワイヤレス LAN（WLAN）クライアントのモビリティを拡張したり、WLAN の導入や管理を簡素化する Cisco IOS ソフトウェアの機能を集めたものです。

WDS は、高速セキュア ローミング、レイヤ 3 モビリティ、無線管理など、さまざまな機能が基盤になっています。

これらの機能の詳細については、「WDS、高速安全ローミング、無線管理、および Wireless Intrusion Detection Services の設定」を参照してください。

WDS の主な目的の一つは、認証サーバがクライアントを最初に認証したときに、ユーザのクレデンシャルをキャッシュすることです。 その後の認証では、WDS は、キャッシュされている情報に基づいてクライアントの認証を行います。 これを実現するための要件は、次のとおりです。

- いずれか 1 つの AP が WDS AP として設定されている必要があります。
- その他の AP は、WDS AP と通信を行うインフラストラクチャ AP として設定されている必要があります。
- WDS AP は、WDS のユーザ名とパスワードを使用して認証サーバへの認証を行い、関係を確立する必要があります。

この認証サーバは、インフラストラクチャ AP およびクライアントの認証が初めて実行されるときに、これらのデバイスのクレデンシャルを検証します。 認証サーバには、外部 RADIUS サーバか、WDS AP のローカル RADIUS サーバのいずれかを使用できます。

WDS とインフラストラクチャ AP は、Wireless LAN Context Control Protocol（WLCCP）というマルチキャスト プロトコルで通信しています。 このマルチキャスト メッセージはルーティングできません。 そのため、WDS と、関連するインフラストラクチャ AP は、同じ IP サブネットワーク内および同じ LAN セグメント上に存在している必要があります。

このドキュメントでは、WDS AP のローカル RADIUS サーバ機能を使用して、クレデンシャルの検証を実行する方法について説明します。

## 設定

### WDS AP の設定

この項では、このドキュメントで説明する機能の設定に必要な情報を提供します。

AP を、AAA サーバ機能を備えた WDS AP として機能するように設定するには、最初に、AP でローカル RADIUS サーバ機能を有効にする必要があります。

次の手順を実行します。

1. GUI を使用して AP にログインします。Summary Status ページが表示されます。
2. AP の左側のメニューから [Security] > [Server Manager] の順に選択します。
3. Corporate Servers で、RADIUS サーバとして機能させる AP の IP アドレスと共有秘密を入力します。この場合、WDS AP は RADIUS サーバとして動作するので、WDS AP の IP アドレスを入力します。 この例では、10.0.0.1 の IP アドレスを使用しています。 これはローカル RADIUS サーバであるため、この例のように、1812 と 1813 を認証ポートとアカウンティング ポートとして使用する必要があります。
4. [Apply] をクリックします。
5. [Default Server Priorities for EAP Authentication] で、WDS AP の IP アドレスを [Priority 1] として選択します。[Apply] をクリックします。これで、ローカル RADIUS サーバが、インフラストラクチャ AP とクライアントの認証で最初に選択されるようになります。
6. 左側のメニューから [Security] > [Local Radius server] の順に選択します。General Set-up をクリックして、ローカル RADIUS サーバのパラメータを設定します。Local Radius Server Authentication Settings で LEAP にチェック マークを付け、Apply をクリックします。Network Access Servers の下で WDS AP の IP アドレスと共有秘密パスワードを入力します。 この例では、共有秘密パスワードに「**test123**」を使用しています。[Apply] をクリックします。
7. Individual Users の下で、WDS AP と通信を行うすべてのインフラストラクチャ AP とクライアントのユーザ名とパスワードを入力します。[Apply] をクリックします。この例では、WDS AP に登録するように設定するインフラストラクチャ AP のユーザとパスワードを入力しています。 この例では、ユーザ名に「**infrastructureAP1**」、パスワードに「**Cisco**」を使用しています。 同じユーザ名とパスワードを設定する必要があります。

AP のローカル RADIUS サーバ機能の設定が完了したら、AP の WDS 機能を有効にする必要があります。

次の手順を実行します。

1. AP の左側のメニューから [Wireless Services] > [WDS] の順に選択します。
2. [General Set-up] をクリックします。
3. General Set-up ページの Use this AP as Wireless Domain Services にチェック マークを付けます。[Wireless Domain Services Priority] フィールドに「254」と入力します。 [Apply] をクリックします。
4. インフラストラクチャの認証を有効にします。WDS ページで Server Groups をクリックします。Server Group Name フィールドに、インフラストラクチャ AP の認証を行うときの名前を入力します。 この例では、[Server Group Name] に「Infrastructure」を使用しています。Group Server Priorities ドロップダウン リストから、ローカル RADIUS サーバの IP アドレスを選択します。WDS AP は、このサーバを使用してインフラストラクチャ AP の認証を実行します。Use Group For の下にある Infrastructure Authentication を選択します。[Apply] をクリックします。

これで、WDS AP が AAA サーバとして機能するようになりました。 インフラストラクチャ AP のいずれか 1 つを設定して、WDS AP に登録します。

**注:** このドキュメントで使用されているコマンドの詳細を調べるには、Command Lookup Tool（登録ユーザ専用）を使用してください。

## インフラストラクチャ AP の設定

このセクションでは、WDS AP に登録するために必要なインフラストラクチャ AP の設定について説明します。 クライアントはインフラストラクチャ AP に関連付けられます。 インフラストラクチャ AP は、WDS AP にクライアントの認証を実行するように要求します。

WDS のサービスを使用するインフラストラクチャ AP を追加するには、次の手順を実行します。

1. 左側のメニューから [Wireless Services] > [AP] の順に選択します。
2. Participate in SWAN Infrastructure で Enable を選択します。
3. WDS Discovery で Auto Discovery を選択します。
4. WDS のユーザ名とパスワードを該当するフィールドに入力します。[Apply] をクリックします。ユーザ名とパスワードは、ローカル RADIUS サーバに存在するものである必要があります。 WDS のメンバーになる予定のすべてのデバイスの WDS のユーザ名とパスワードを認証サーバに指定しておく必要があります。

WDS AP の設定と、WDS AP へのインフラストラクチャ AP の設定が完了すると、WDS Status タブの AP Information エリアにインフラストラクチャ AP が REGISTERED の状態で表示されます。 これは、[Wireless Services] > [WDS] メニュー項目の下にあります。

WDS AP またはインフラストラクチャ AP のいずれかで認証の設定に誤りがあると、AP が ACTIVE および REGISTERED で表示されない場合があります。 エラーが発生したり、認証が失敗したりする場合は、認証サーバの統計情報を確認してください。 認証サーバの統計情報で、[Security] > [Local Radius Server] > [Statistics] を選択します。

また、WDS AP の CLI から **show wlccp wds ap** コマンドを使用して設定を確認することもできます。 WDS AP への登録が正常に終了すると、WDS AP への登録の正常終了を表示する出力は、次の例のようになります。

```
WDS#show wlccp wds ap
  MAC-ADDR         IP-ADDR         STATE      LIFETIME    CDP-NEIGHBOR
  000e.d7e4.a629   10.0.0.2      REGISTERED    97          10.77.241.161
```

## クライアントの認証方式の設定

WDS にクライアントの認証方式を追加します。

次の手順を実行します。

1. WDS AP で [Wireless Services] > [WDS] > [Server Groups] の順に選択します。クライアント（クライアント グループ）の認証を行うサーバ グループを定義します。このグループは、前の手順でインフラストラクチャの認証用に設定したサーバ グループと別のものである必要があります。 この例では、[Server Group Name] に「**Clients**」を使用しています。 Priority 1 にローカル RADIUS サーバを設定します。クライアントの認証に使用する認証タイプ（LEAP、EAP、MAC など）にチェック マークを付けます。この例では、LEAP 認証を使用しています。設定を関連する SSID に適用します。
2. インフラストラクチャ AP で、次の手順を実行します。[Security] > [Encryption Manager] の順に選択してから [WEP Encryption] をクリックし、ドロップダウン メニューから

[Mandatory] を選択します。 Encryption Keys の下に、128 ビット WEP 暗号化キーを入力します。 この例では、暗号化キーに「**1234567890abcdef1234567890**」を使用しています。 [Security] > [SSID Manager] を選択し、新しい SSID を作成します。この例では、[SSID] に「**Cisco123**」を使用しています。 続いて、認証方式を選択します。インフラストラクチャ AP で [Network EAP] を選択します。

クライアントが正常に認証され、インフラストラクチャ AP に関連付けられるかどうかテストします。 クライアントは最初に起動すると、自身のクレデンシャルをインフラストラクチャ AP に渡します。 続いて、インフラストラクチャ AP は同じものを WDS AP に転送し、WDS AP でクレデンシャルが検証されます。

**注:** このドキュメントでは、クライアント アダプタの設定方法については説明しません。 クライアント アダプタの設定方法については、「Cisco Aironet ワイヤレス LAN クライアント アダプタ」を参照してください。

## 確認

ここでは、設定が正常に動作していることを確認します。

- **show wlccp wds mn**：WDS AP の CLI からこのコマンドを使用すると、クライアントの WDS AP への認証と関連付けが正常に終了したかどうかを確認できます。

```
WDS#show wlccp wds mn
  MAC-ADDR         IP-ADDR      Curr-AP          STATE
 0040.96a5.b5d4    10.0.0.15    000e.d7e4.a629  REGISTERED
```

次のデバッグ コマンドも役立ちます。

- **debug wlccp ap { mn | wds-discovery | state }** ：クライアント デバイス（**mn**）、**WDS 検出プロセス**、および WDS アクセス ポイントに対するアクセス ポイント認証（**state**）に関連するデバッグ メッセージ出力を有効にする場合に使用します。
- **debug wlccp packet** ：WDS アクセス ポイントとの間で送受信されるパケットを表示する場合に使用します。
- **debug radius local-server**：ローカル オーセンティケータに対して失敗したクライアント認証に関するエラー メッセージの表示をアクティブにします。

## トラブルシューティング

現在のところ、この設定に関する特定のトラブルシューティング情報はありません。

## 関連情報

- 無線ドメイン サービス（WDS）の設定
- Cisco Aironet クライアント アダプタ
- 無線ドメイン サービスに関する FAQ
- WLAN の設定例とテクニカル ノート
- Cisco Aironet 1200 シリーズの設定例とテクニカル ノート
- テクニカル サポートとドキュメント – Cisco Systems