詳細設定の使用と操作

SNMP の管理

Simple Network Management Protocol は、ネットワーク内のすべてのデバイスから情報を収集し、これらのデバイスを設定して管理するために使用される一般的なネットワーク管理プロトコルです。

Cisco Wireless リリース 8.3 以降、Cisco Mobility Express の Web インターフェイスを使用して SNMPv2c および SNMPv3 の両方を設定できます。

SNMP アクセスの設定

Cisco Mobility Express マスター AP の次の SNMP アクセス モードを設定できます。

- SNMPv2c のみ
- SNMPv3 のみ
- SNMPv2c と NMPv3 の両方
- SNMPv2c も SNMPv3 もアクセス不可

（注） Cisco Mobility Express CLI を使用しても、SNMPv1、SNMPv2c、および SNMPv3 を設定できます。

ステップ 1 **[Advanced]** > **[SNMP]** を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 次に、[SNMP Access] に移動し、適切なチェック ボックスをオンにして、特定の SNMP モードを有効にします。

デフォルト モードは v2cです（あるいはデフォルトで SNMP モードの両方が選択されているか、またはいずれも選択されていないこともあります）。

選択した SNMP アクセス モードが有効になります。

（注） Cisco Mobility Express を使用した SNMPv3 ユーザの設定については、「SNMPv3 ユーザの設定」の項を参照してください。

ステップ 3 [Read Only Community] フィールドに、特定のコミュニティ名を入力します。

デフォルト名は *public* です。

ステップ 4 [Read-Write Community] フィールドに、特定のコミュニティ名を入力します。

デフォルト名は *private* です。

ステップ 5 [SNMP Trap] ドロップダウンリストから、[Enabled] または [Disabled] を選択して SNMP トラップの受信者を設定します。このツールはログを受信し、ネットワーク デバイスから送信された SNMP トラップを表示します。

デフォルト設定では [Disabled] になっています。

ステップ 6 [SNMP Server IP] フィールドで、接続するサーバの IP アドレスを指定します。

SNMPv3 ユーザの追加

ステップ 1 **[Advanced]** > **[SNMP]** を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 [SNMP v3 Users] セクションで、[Add New SNMP v3 User] ボタンをクリックします。

[Add SNMP v3 User] ウィンドウが表示されます。

ステップ 3 [User Name] フィールドに、新しい SNMPv3 ユーザのユーザ名を入力します。

ユーザ名は次の条件を満たしている必要があります。

-
-

ステップ 4 [Access Mode] ドロップダウンリストで、[Read Only] と [Read/Write] から必要なモードを選択します。

デフォルトは [Read Only] です。

ステップ 5 [Authentication Protocol] ドロップダウンリストから、[HMAC-MD5]、[HMAC-SHA]、または [None] のいずれかを選択します。

デフォルトの認証プロトコルは **HMAC-SHA** です。

ステップ 6 [Authentication Password] フィールドと [Confirm Authentication Password] フィールドに、次のパスワード ポリシーに従って特定の認証パスワードを入力します。

（注） [Show Password] チェック ボックスを選択し、[Authentication Password] フィールドと [Confirm Authentication Password] フィールドのエントリを表示して一致していることを確認することができます。

ステップ 7 [Privacy Protocol] ドロップダウンリストで、[CBC-DES]、[CFB-AES-128]、または [None] のいずかを選択します。

デフォルトのプライバシー プロトコルは [CFB-AES-128] です。

ステップ 8 [Privacy Password] フィールドと [Confirm Privacy Password] フィールドに、次のパスワード ポリシーに従って特定のプライバシー パスワードを入力します。

（注） [Show Password] チェック ボックスを選択し、[Privacy Password] フィールドと [Confirm Privacy Password] フィールドのエントリを表示して一致していることを確認することができます。

ステップ 9 [Apply] をクリックして新しい SNMPv3 ユーザを作成します。

新たに追加した SNMP v3 ユーザが [SNMP Setup] ウィンドウの [SNMP v3 Users] テーブルに表示されます。

（注） 最大 7 つの SNMPv3 ユーザを追加できます。

SNMPv3 ユーザの編集

ステップ 1 **[Advanced]** > **[SNMP]** を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 詳細を変更する SNMPv3 ユーザが含まれている行で [edit_icon.gif] アイコンをクリックします。

[SNMPv3 Users] テーブル内の特定の行が編集可能になります（または、[Edit SNMPv3 User] ウィンドウが表示されます）。

ステップ 3 [SNMPv3 Users] テーブルで、特定の変更をインラインします（または、[Edit SNMPv3 Users] ウィンドウに表示します）。

ステップ 4 [Apply] をクリックします。

[SNMP v3 Users] テーブルが更新され、更新したエントリがこのテーブルに表示されます。

SNMPv3 ユーザの削除

ステップ 1 **[Advanced]** > **[SNMP]** を選択します。

[SNMP Setup] ウィンドウが表示されます。

ステップ 2 削除する SNMPv3 ユーザが含まれている行で [X] アイコンをクリックします。

警告メッセージが表示されます。

ステップ 3 ポップアップ ウィンドウで [Yes] をクリックします。

[SNMP v3 Users] テーブルが更新され、削除したエントリがこのテーブルから削除されます。

システム メッセージ ロギングの設定

システム メッセージ ロギング機能は、syslog サーバと呼ばれるリモート サーバにシステム イベントのログを記録します。各システム イベントは、イベントの詳細を含む Syslog メッセージをトリガーします。

システム メッセージ ロギング機能が有効な場合、コントローラは、コントローラに設定された syslog サーバに syslog メッセージを送信します。

始める前に

次の手順を開始する前に、ネットワークで syslog サーバをセットアップします。

ステップ 1 [Advanced] > [Logging] の順に選択します。

[Logging Setup] ウィンドウが表示されます。

ステップ 2 [Syslog Logging] ドロップダウン リストから [Enable] を選択します。デフォルトでは無効になっています。

システム メッセージ ロギング機能が有効になります。

ステップ 3 [Syslog Server IP] フィールドに、syslog メッセージの送信先サーバの IPv4 アドレスを入力します。

ステップ 4 syslog サーバに対する syslog メッセージのフィルタリングの重大度レベルを設定します。[Logging Level] ドロップダウン リストから、次のいずれかの重大度レベル（重大度が高い順）を設定します。

- **[Emergencies (Highest severity)]**
- **[アラート（Alerts）]**
- **[Critical]**

- **[Errors (Default)]**
- 警告
- 通知
- **[Informational]**
- **[Debugging (Lowest severity)]**

syslog レベルを設定すると、重大度がそのレベル以上であるメッセージのみが、syslog サーバに送信されます。

ステップ 5 syslog サーバに送信する syslog メッセージのファシリティを設定するには、[Syslog Facility] ドロップダウン リストから次のいずれかのオプションを選択します。

- [Kernel] = ファシリティ レベル 0
- [User Process] = ファシリティ レベル 1
- [Mail] = ファシリティ レベル 2
- [System Daemons] = ファシリティ レベル 3
- [Authorization System] = ファシリティ レベル 4
- [Syslog] = ファシリティ レベル 5（デフォルト値）
- [Line Printer] = ファシリティ レベル 6
- [USENET] = ファシリティ レベル 7
- [Unix-to-Unix Copy] = ファシリティ レベル 8
- [Cron] = ファシリティ レベル 9
- [FTP Daemon] = ファシリティ レベル 11
- [System Use 12] = ファシリティ レベル 12
- [System Use 13] = ファシリティ レベル 13
- [System Use 14] = ファシリティ レベル 14
- [System Use 15] = ファシリティ レベル 15
- [Local Use 0] = ファシリティ レベル 16
- [Local Use 1] = ファシリティ レベル 17
- [Local Use 2] = ファシリティ レベル 18
- [Local Use 3] = ファシリティ レベル 19
- [Local Use 4] = ファシリティ レベル 20
- [Local Use 5] = ファシリティ レベル 21
- [Local Use 6] = ファシリティ レベル 22
- [Local Use 7] = ファシリティ レベル 23
- [Authorization System (Private)] = ファシリティ レベル 24

ステップ 6 [Apply] をクリックします。

RF パラメータの最適化

ネットワークの Wi-Fi のパフォーマンスを最大化するため、無線周波の信号のカバレッジと品質を最適化できます。

ステップ 1 [RF Optimization] ドロップダウン リストから [Enabled] を選択します。

ステップ 2 ネットワークの予想される [Client Density] と [Traffic Type] が表示されます。

低、標準または高密度のクライアント タイプが選択された場合に設定された値については、RF パラメータの最適化設定 を参照してください。

ステップ 3 [Apply] をクリックします。

ローミングの最適化

ローミングの最適化について

ローミングの最適化は、遠隔地のアクセスポイントに長時間アソシエートし続けているクライアントや、接続が不安定な Wi-Fi ネットワークに接続を試みるアウトバウンド クライアントの問題を解決します。最適化されたローミングでは、クライアントのデータ パケットとデータ レートに基づいて、クライアントの関連付けを解除することができます。クライアントは、RSSI アラーム条件が満たされ、現在のデータ レートが最適化ローミング データ レートのしきい値を下回っている場合にアソシエート解除されます。データ レート オプションを無効にして、RSSI のみをクライアントのアソシエート解除に使用するようにできます。

また、最適化されたローミングは、着信クライアントの RSSI を RSSI しきい値と照合して、クライアントの RSSI が低いときのクライアント関連付けも防ぎます。このチェックで、クライアントに有効な接続がない限り、クライアントの Wi-Fi ネットワークへの接続が阻止されます。クライアントはビーコンを受信して Wi-Fi ネットワークに接続できても、信号が弱いために安定した接続をサポートできない場合がよくあります。

ローミングの最適化を使用することによって、無線に対してクライアント カバレッジ レポート間隔を設定することもできます。

最適化されたローミングは、次のシナリオに有益です。

- クライアントを積極的に切断することによってスティッキー クライアントの問題に対処する。
- データ RSSI パケットを積極的に監視する。
- 設定されたしきい値よりも RSSI が低い場合はクライアントの関連付けを解除する。

ローミングの最適化の制約事項

- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。
- BSS 遷移が 802.11v 対応クライアントに送信され、切断タイマーの期限が切れる前にそのクライアントが他の BSS に遷移していない場合、そのクライアントは強制的に切断されます。802.11v 対応クライアントのデフォルトにより、BSS 遷移が有効になります。

設定の最適化されたローミング

始める前に

- GUI を介して最適化されたローミングを設定できるようにするには、[Expert View] に切り替えていることを確認します。
- 802.11a/b ネットワークを無効にするまで、ローミングの最適化の間隔を設定できません。

ステップ 1 **[Advanced]** > **[RF Optimization]** を選択します。

[RF Optimization] ページが表示されます。

ステップ 2 [Optimized Roaming] ノブを有効にします。

最適化されたローミングを設定するためのさまざまなオプションが表示されます。これには、データ レート チェックやカバレッジ ホール検出と緩和（CHDM）から取得したデフォルトの RSSI しきい値などが含まれています。

ステップ 3 [2.4 GHz Interval] テキスト ボックスと [5.0 GHz Interval] テキスト ボックスに、アクセス ポイントがマスター AP にクライアント カバレッジ統計を報告する間隔の値を指定します。

間隔の範囲は 5 ～ 90 秒（デフォルト）です。報告間隔を小さく設定すると、ネットワークはカバレッジ レポート メッセージによって過負荷になることがあります。

クライアント カバレッジの統計情報には、データ パケット RSSI、カバレッジ ホールの検出および軽減（CHDM）の事前アラーム障害、再送信要求と現在のデータ レートが含まれます。

（注） アクセス ポイントは、次の条件に基づいてクライアント統計情報をマスター AP に送信します。

- 間隔がデフォルトで 90 秒に設定されている場合。
- カバレッジホールの検出（CHD）の赤色アラームにより、最適化されたローミングに障害が発生している間のみに間隔が設定されている場合（たとえば、10 秒）。

ステップ 4 [2.4 GHz Data Rates] スライダーと [5.0 GHz Data Rates] スライダーを操作して、クライアントのしきい値データ レートを設定します。

次のデータ レートが使用可能です。

- 2.4 GHz：1、2、5.5、6、9、11、12,、18、24、36、48、54

• 5 GHz：6、9、12、18、24、36、48、54

コントローラ ツールの使用

（注） この機能は、読み込み/書き込み権限を持つ管理ユーザ アカウントのみで利用できます。

[Controller Tools] ページでは、コントローラの次の操作を実行できます。

- コントローラの再起動。

  コントローラの再起動 （8 ページ）を参照してください。
- コントローラ コンフィギュレーションのクリアと工場出荷時状態へのコントローラのリセット。コントローラ コンフィギュレーションのクリアとコントローラのリセット （8 ページ）を参照してください。
- コントローラ コンフィギュレーションのエクスポートとインポート。「コントローラ コンフィギュレーションのエクスポートとインポート （9ページ）」を参照してください。

コントローラの再起動

コントローラは、[Advanced] > [Controller Tools] を選択し、[Restart Controller] をクリックすることで、いつでも再起動（またはリブート）できます。

コントローラ コンフィギュレーションのクリアとコントローラのリセット

この手順によって、Cisco Mobility Express ワイヤレス LAN コントローラは工場出荷時の設定にリセットされます。

ステップ 1 [Advanced] > [Controller Tools] を選択します。

これにより、[Controller Tools] ページが開きます。

ステップ 2 [Clear Candidate Configuration] をクリックします。

これにより、現在の Cisco Mobility Express コントローラ設定が消去され、工場出荷時の値に設定がリセットされて、Cisco Mobility Express ワイヤレス LAN コントローラがリブートします。

次のタスク

Cisco Mobility Express コントローラがリブートしたら、初期設定ウィザードの起動に進みます。

コントローラ コンフィギュレーションのエクスポートとインポート

コントローラ設定のエクスポート

現在のコントローラ設定は、いつでも .TXT ファイル形式にエクスポートできます。

現在の設定をエクスポートするには、[Advanced] > [Controller Tools] を選択し、[Configuration File] の下にある [Export Configuration] をクリックします。

設定ファイルは HTTPS を介し、Mobility Express の UI が表示されているデバイス上に保存されます。デフォルトでは、ダウンロード フォルダ内に *configuration.txt* として保存されます。

コントローラ設定のインポート

以前に .TXT ファイル形式で保存した設定ファイルから設定をインポートできます。これを行うには、[Advanced] > [Controller Tools] を選択し、[Configuration File] の下にある [Import Configuration] をクリックして必要なファイルを参照し、選択します。

インポートによって、ネットワーク内のコントローラ対応のすべての AP がリブートします。AP がオンラインに戻ると、マスター AP 選定プロセスが開始され、マスター AP は新たにインポートされたコントローラ コンフィギュレーションでオンラインになります。

マスター AP 選定プロセスの詳細については、Cisco Mobility Express コントローラのフェールオーバーとマスター AP の選定プロセスを参照してください。

コントローラ コンフィギュレーションの保存

アクセス ポイントには、揮発性のあるアクティブな RAM と不揮発性の RAM（NVRAM）の 2 種類のメモリがあります。通常動作時は、Cisco Mobility Express コントローラの現在の設定は、マスター AP の RAM 上にあります。再起動時には、揮発性 RAM は完全に消去されますが、NVRAM 上のデータは保持されます。

RAM 上にある Cisco Mobility Express コントローラの設定は、マスター AP の NVRAM にいつでも保存できます。これにより、最後に保存した設定を使用してコントローラを再起動できます。

RAM 上にあるコントローラの現在の設定を NVRAM に保存するには、Cisco Mobility Express Web インターフェイスの右上にある [Save Configuration] をクリックし、[Ok] をクリックします。

設定が正常に保存されたら、同一であることを伝えるメッセージが表示されます。

CMX クラウド プレゼンス分析の使用

Cisco Connected Mobile Experiences Cloud（Cisco CMX Cloud）は現場での分析を実現する Software as a Service（SaaS）製品です。Cisco Mobility Express の Web インターフェイスを使用して、Cisco CMX Cloud ソリューションを設定できます。

Cisco Mobility Express と統合された Cisco CMX Cloud ソリューションは、次の機能を提供します。

- カスタム ポータルを通じ、訪問者のための安全なゲスト アクセス ソリューションの設定を可能にします。

（注） CMX Connect 設定はゲスト アクセス用の WLAN レベルで実行されます。

- すべての Wi-Fi のデバイスの検出を容易にします。
- 滞留時間、新規訪問者とリピート訪問者、ピーク タイムなど、Wi-Fi デバイスのプレゼンスに関する分析を提供します。
- ロケーションベースのコンテンツを提供するゲストポータルページやモバイルアプリケーションに訪問者を直接取り込むこともできます。

CMX プレゼンス分析の前提条件

- 有効な CMX サーバ URL と対応する CMX サーバ トークンが必要です。CMX クラウド アカウントを登録するには、www.cmxcisco.com にアクセスしてください。詳細については、http://support.cmxcisco.com/hc/en-us を参照してください。

（注） サーバ URL フィールドの URL に /visitor/login が追加されていることを確認します。

- CMX クラウド用の WLAN が作成されます。詳細については、「**ワイヤレス設定の指定**」の章の「**WLAN の追加**」の項を参照してください。

CMX プレゼンス分析の有効化

始める前に

有効な CMX サーバの URL と対応するトークンが必要です。

ステップ 1 **[Advanced]** > **[CMX]** を選択します。

[CMX] ウィンドウが表示されます。

ステップ 2 [CMX Status] ドロップダウン ボックスで、[Enabled] を選択します。

ステップ 3 [CMX Server URL] フィールドに有効な CMX サーバの URL を入力します。

ステップ 4 [CMX Server Token] フィールドに有効な CMX サーバのトークンを入力します。

ステップ 5 [Apply] をクリックします。

DNS アクセス制御リスト

DNS アクセス制御リスト（ACL）機能が Cisco Mobility Express でサポートされるようになりました。これにより、ドメインベースのフィルタリングが Flex モードで実行可能になります。今後は承認なしに URL を選択して許可できるようになります。この機能により、事前認証と事後認証の両方を対象に、URL ルールで設定された FQDN に対応する複数の IP を学習できます。

この機能は次のように URL リストをサポートします。

- IPv4 および IPv6
- ワイルドカード照合：32 個 の URL ルールから、最大 20 文字のワイルドカード照合が可能。
- 事後認証に対応した許可/拒否ルール。
- FQDN を使用した ACL の設定。
- ACL 名ごとに設定可能な 32 個の URL ルール。

（注） この機能拡張により、上記の機能は事後認証にも適用できます。

コントローラは、WLAN、AP グループ、AP ごとに ACL 名で設定するか、AAA サーバから返される名前で設定します。AP データパスは DNS 要求や応答をモニタし、設定された DNS 名の IP アドレスを学習し、学習した IP アドレスのトラフィックを許可します。

ACL アクションが DNS 応答を**許可**すると、IP アドレスはスヌーピングされたリストに追加されます。認証後の ACL では、URL アクションが**拒否**の場合、AP は DNS 応答を変更し、IP アドレス 0.0.0.0 をクライアントに送信します。

Wave 2 AP でサポートされている DNS ACL には、次の 2 つのタイプがあります。

- 事前認証または Web 認証 DNS ACL：これらの ACL の URL は、クライアント認証フェーズの前に**許可**に設定されています。クライアントの URL ルールが**許可**に設定されている

場合、クライアントデータはローカルに切り替えられます。URL が一致するルールがない場合、すべてのパケットがコントローラに転送されます。デフォルトでは、クライアントデータが AP に設定されているどのルールにも一致しない場合、トラフィックはコントローラに送信されて、L3 認証の対象になります。

- 事後認証 DNS ACL：これらの ACL は、クライアント実行中に適用されます。事後認証の ACL 名は WLAN で設定できます。また、特定のクライアントの AAA サーバで設定されている ACL 名で上書きできます。ACL ルールアクションが**拒否**に設定されて URL は、DNS 応答で IP アドレスを取得しません。AP は DNS 応答を 0.0.0.0 で上書きしてからクライアントに送信します。

DNS アクセス制御リスト（ACL）の設定

事前認証用に DNS ACL を設定する手順が変更されました。DNS ACL を設定するには、次の手順に従います。

ステップ 1 [Advanced] > [Security Settings] の順に選択します。
[Security Settings] ページが表示されます。

ステップ 2 [新Add new ACL] をクリックします。
[Add ACL Rule] ウィンドウが表示されます。

ステップ 3 新しい ACL ルールを追加するには、次の手順に従います。

a) [ACL Type] で [IPv4] または [IPv6] を選択します。
b) [ACL Name] を入力します。
c) ポリシー ACL を有効または無効にするには、[Policy ACL] トグルボタンを使用します。
d) [Add IP Rule] ボタンをクリックします。
[Add/Edit IP ACLs] ウィンドウが表示されます。
e) [Add/Edit IP ACL] ウィンドウでは、[Action]、[Protocol]、[Source IP/Mask]、[Source Port]、[Dest. IP Address/Mask]、[Dest. Port]、[DSCP] などの詳細を入力し、[Apply] をクリックします。
f) [Add URL Rules] ボタンをクリックします。
[Add/Edit URL ACLs] ウィンドウが表示されます。
g) [Add/Edit URL ACL] ウィンドウで、[URL] と [Action] を入力します。

（注） IPv4 と IPv6 で同じ URL を追加できません。

h) [Apply] をクリックします。

[Security Settings] ページに、ACL タイプ、ACL 名、およびポリシー名が一覧表示されます。また、ポリシー名がマッピングされているかどうかも確認できます。

事前認証レベルで ACL を WLAN に適用

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 有効または無効にする WLAN の横にある [Edit] アイコンをクリックします。
[Edit WLAN] ウィンドウが表示されます。

ステップ 3 [WLAN Security] タブで、[Guest Network] を有効にします。

ステップ 4 [Rule Name(IPv4)] および [Rule Name(IPv6)] ドロップダウンリストで値を選択します。

ステップ 5 [Apply] をクリックします。

事後認証レベルで ACL を WLAN に適用

ステップ 1 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 2 有効または無効にする WLAN の横にある [Edit] アイコンをクリックします。
[Edit WLAN] ウィンドウが表示されます。

ステップ 3 [VLAN & Firewall] タブの [Enable Firewall] フィールドで、[Yes] を選択してファイアウォールを有効にします。

ステップ 4 [WLAN Post-auth ACL] セクションで、[ACL Name(IPv4)] 、[ACL Name(IPv6)] の一方または両方を選択します。

ステップ 5 [Apply] をクリックします。

WLAN での AAA オーバーライドの設定

ステップ 1 現在標準ビューになっている場合は、**エキスパートビュー**に切り替えます。

ステップ 2 [Wireless Settings] > [WLANs] の順に選択します。
[WLAN Configuration] ウィンドウが表示されます。

ステップ 3 有効または無効にする WLAN の横にある [Edit] アイコンをクリックします。
[Edit WLAN] ウィンドウが表示されます。

ステップ 4 [Advanced] タブを選択し、[Allow the AAA Override] トグルボタンを有効にします。

ステップ 5 [Apply] をクリックします。