コントローラおよび AP 設定の設定

この章は、次の内容で構成されています。

不正 AP トレーシングに対する SNMP クレデンシャルの設定

[SNMP Credentials] ページでは、クレデンシャルを指定して不正アクセス ポイントのトレーシングに使用できます。番号ベースのエントリを使用しても特定のエントリを確認できない場合は、このオプションを使用します。スイッチ クレデンシャルが Prime Infrastructure に追加されていない場合は、このページの SNMP クレデンシャルを使用してスイッチに接続できます。

SNMP クレデンシャルを設定するには、次の手順に従います。

ステップ 1 [Administration] > [System Settings] の順に選択します。

ステップ 2 左側のサイドバーのメニューから [SNMP Credentials] を選択します。[SNMP Credentials] ページが表示されます。

ステップ 3 現在の SNMP エントリの詳細を表示または編集するには、[Network Address] リンクをクリックします。詳細については、「グローバル SNMP の設定」（P.2-6）を参照してください。

（注） デフォルトのネットワーク アドレスは 0.0.0.0 であり、ネットワーク全体を示します。SNMP クレデンシャルはネットワークごとに定義されるため、ネットワーク アドレスのみを指定できます。0.0.0.0 は SNMP クレデンシャルのデフォルトであり、SNMP クレデンシャルが定義されていないときに使用されます。デフォルトのコミュニティ ストリングは、読み取りと書き込みの両方において *private* です。事前に設定された SNMP クレデンシャルを独自の SNMP 情報で更新する必要があります。

ステップ 4 新しい SNMP エントリを追加するには、[Select a command] ドロップダウン リストから [Add SNMP Entries] を選択し、[Go] をクリックします。詳細については、「新しい SNMP クレデンシャル エントリの追加」（P.2-9）を参照してください。

CLI セッションのプロトコル設定

Autonomous アクセス ポイントやコントローラのコマンドライン インターフェイス（CLI）テンプレートなどの多くの Prime Infrastructure 無線機能、および移行テンプレートでは、Autonomous アクセス ポイントまたはコントローラで CLI コマンドを実行する必要があります。これらの CLI コマンドは、Telnet または SSH セッションを確立して入力できます。CLI セッション ページでは、セッション プロトコルを選択できます。SSH がデフォルトです。

（注） CLI テンプレートでは、質問に対して回答する操作（コマンドに対して「*Yes*」または「*No*」で回答する、*Enter キーを押して続行する*、など）は不要です。Prime Infrastructure によって自動的に実行されます。

CLI セッションのプロトコルを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから、[CLI Session] を選択します。

ステップ 3　デフォルトのコントローラ セッション プロトコルには、SSH が選択されています。Telnet を選択するには、該当のオプション ボタンを選択します。

ステップ 4　デフォルトの Autonomous アクセス ポイント セッション プロトコルには、SSH が選択されています。Telnet を選択するには、該当のオプション ボタンを選択します。

ステップ 5　デフォルトでは、[Run Autonomous AP Migration Analysis on discovery] オプション ボタンは [No] に設定されています。Autonomous AP を検出し、移行分析を実行する場合は、[Yes] を選択し、[Save] をクリックします。

アップグレード後のコントローラのリフレッシュ

[Controller Upgrade Settings] ページを使用すると、コントローラ イメージに変更があるたびに設定を自動的に復元できるように、コントローラのアップグレード後に自動リフレッシュすることができます。自動リフレッシュを実行するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバー メニューから、[Controller Upgrade Settings] を選択します。

ステップ 3　[Auto refresh After Upgrade] チェックボックスをオンにすると、コントローラのイメージに変更があるたびに設定は自動的に復元されます。

ステップ 4　save config トラップを受信したときの Prime Infrastructure の動作を決定します。このチェックボックスをオンにすると、デバイスに存在して Prime Infrastructure には存在しない追加の設定を保持するか削除するかを選択できます。設定は、Prime Infrastructure によって管理されているすべてのコントローラに適用されます。

[Configure] > [Controllers] > [Properties] > [Settings] ページの [Auto Refresh on Save Config Trap] チェックボックスを選択した場合、この設定は上記のグローバル設定よりも優先されます。

自動更新の実行には最大 3 分かかります。

ステップ 5　[Save] をクリックします。

save config トラップを Prime Infrastructure が受信するたびに、このチェックボックスはオンになります。このチェックボックスをオンにすると、Prime Infrastructure の動作が決定されます。

このチェックボックスをオンにすると、ユーザはデバイスに存在して Prime Infrastructure には存在しない追加の設定を保持するか削除するかを選択できます。

設定は、Prime Infrastructure によって管理されているすべてのコントローラに適用されます。[Controller] > [Properties] ページの save config トラップの処理に関する設定は、このグローバル設定よりも優先されます。

コントローラのイメージに変更がある場合、コントローラの設定は自動的に復元されます。

不正 AP へのスイッチ ポートの追跡

[Administration] > [System Settings] > [Rogue AP Settings] ページで、不正アクセス ポイントがそれぞれ接続されているネットワーク スイッチ ポートを Prime Infrastructure が自動的に識別するようにできます。

不正 AP 自動トレースを設定するには、次の手順を実行します。

ステップ 1　[Administration] > [System Settings] の順に選択します。

ステップ 2　左側のサイドバーのメニューから [Rogue AP Settings] を選択します。[Rogue AP Settings] ページが表示されます。

ステップ 3　[Enable Auto Switch Port Tracing] チェックボックスをオンにして、Prime Infrastructure が、不正アクセス ポイントが接続されているスイッチ ポートを自動的にトレースできるようにします。次に、次の内容を含む自動ポート トレーシング用のパラメータを指定します。

- 不正の AP からのポートへのトレース間で待機する時間（分）
- Found On Wire 不正 AP をトレースするかどうか
- どの重大度（[Critical]、[Major]、または [Minor]）を含めるかどうか

ステップ 4　[Enable Auto Containment] チェックボックスをオンにして、Prime Infrastructure が重大度で不正 AP を自動的に含めるようにします。次に、次の内容を含む自動封じ込め用のパラメータを指定します。

- ポート トレーシングで Found On Wire 不正 AP を除外するかどうか
- 封じ込めにどの重大度（[Critical]、[Major]）を含めるかどうか
- 封じ込めレベル（最大 4 つの AP）

ステップ 5　[OK] をクリックします。

スイッチ ポート トレーシングの設定

現在、Prime Infrastructure では、コントローラから情報を取得することによって、不正アクセス ポイントを検出できます。不正アクセス ポイント表には、ネイバー リストにないフレームから検出された BSSID アドレスが記載されています。指定された期間の終わりに、不正アクセス ポイント表の内容が、CAPWAP Rogue AP Report メッセージでコントローラに送信されます。この方法で、Prime Infrastructure はコントローラから受信した情報を収集します。この機能拡張により、検出された不正なアクセス ポイントに対応し、今後発生する攻撃を回避できます。トレース情報は不正アクセス ポイントの Prime Infrastructure ログだけで使用でき、不正クライアントのログには使用できません。

不正アクセス ポイントに接続した不正クライアントの情報を使用して、ネットワークで不正アクセス ポイントに接続したスイッチ ポートを追跡します。

危険性のない不正アクセス ポイントまたは削除された不正アクセス ポイントにトレーシングを設定しようとすると、警告メッセージが表示されます。

スイッチ ポート トレーシングで、v3 を使用してスイッチ ポートを正常にトレースするには、すべての OID を SNMP v3 のビューに含める必要があり、SNMP v3 グループ内の VLAN ごとに VLAN の内容を作成する必要があります。

スイッチ ポート トレーシングの設定については、「スイッチ ポート トレーシングの設定」（P.7-4）を参照してください。

[Switch Port Trace] ページでは、回線上で検出された不正アクセス ポイントに対するトレースを実行できます。

不正アクセス ポイントを適切にトレースして組み込むには、以下の情報を正しく指定する必要があります。

- レポート AP : 不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- AP CDP ネイバー : シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル : トレース対象のすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。個々のスイッチだけを追加するのではなく、ネットワーク アドレスをベースに項目を追加できます。正しい write コミュニティ ストリングを指定して、スイッチ ポートを有効または無効にする必要があります。トレーシングの場合は、read コミュニティ ストリングで十分です。
- スイッチ ポートの設定 : トランキング スイッチ ポートを正しく設定する必要があります。スイッチ ポートのセキュリティは無効にする必要があります。
- シスコ イーサネット スイッチだけがサポートされています。
- スイッチ VLAN 設定を適切に行う必要があります。
- CDP プロトコルがすべてのスイッチ上で有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内でスイッチに接続される必要があります。デフォルトのホップ カウントは 2、最大ホップ カウントは 10 です。
- SNMPv3 を選択している場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成します。

ステップ 1　[Administration] > [System Settings] > [Switch Port Trace] を選択します。

ステップ 2　次の基本設定を行います。

- [MAC address +1/-1 search]：有効にするには、チェックボックスをオンにします。

  この検索では、無線 MAC アドレスに 1 加算するか 1 減算することによって不正アクセス ポイントの有線側の MAC アドレスを得る、慣習的な MAC アドレス +1/-1 方式を使用します。

- [Rogue client MAC address search]：有効にするには、チェックボックスをオンにします。

  不正クライアントが存在していると、検索可能な MAC アドレスのリストにクライアントの MAC アドレスが追加されます。

- [Vendor (OUI) search]：有効にするには、チェックボックスをオンにします。組織固有識別子である OUI、すなわち MAC アドレスの先頭 3 バイトで検索します。

- [Exclude switch trunk ports]：スイッチ ポートのトレースからスイッチ トランク ポートを除外する場合に、このチェックボックスをオンにします。

  （注）　特定の MAC アドレスについて複数ポートをトレースする場合は、精度を向上させるために、追加のチェックが実行されます。トランク ポートのチェック、ポート上にある AP でない CDP ネイバーのチェック、およびこの MAC アドレスがこのポート上の唯一のアドレスであるかどうかのチェックを含みます。

- [Exclude device list]：トレースから追加のデバイスを除外する場合に、このチェックボックスをオンにします。スイッチ ポート トレースから除外する各デバイスをデバイス リスト テキスト ボックスに入力します。デバイス名はカンマで区切ります。

- [Max hop count]：このトレースに対するホップの最大数を入力します。ホップ カウントを大きくするほど、スイッチ ポート トレースの実行時間が長くなることに留意してください。

- [Exclude vendor list]：スイッチ ポート トレースから除外するすべてのベンダーをベンダー リスト テキスト ボックスに入力します。ベンダー名はカンマで区切ります。ベンダー リストでは、大文字と小文字が区別されません。

ステップ 3　次の高度な設定を行います。

- [TraceRogueAP task max thread]：スイッチ ポート トレーシングで、複数のスレッドを使用して不正アクセス ポイントをトレースします。このフィールドは、並列スレッドでトレースできる不正アクセス ポイントの最大数を示します。

- [TraceRogueAP max queue size]：スイッチ ポート トレーシングでは、キューを保持して、不正アクセス ポイントをトレースします。トレーシングする不正アクセス ポイントを選択すると、処理待ちのキューに入ります。このフィールドは、キューに保管できる項目の最大数を示します。

- [SwitchTask max thread]：スイッチ ポート トレーシングでは、複数のスレッドを使用して、スイッチ デバイスをクエリーします。このフィールドは、並列スレッドでクエリーできるスイッチ デバイスの最大数を示します。

（注）　これらのパラメータのデフォルト値は、通常の運用に適しています。これらのパラメータは、スイッチ ポート トレーシングと Prime Infrastructure のパフォーマンスに直接影響します。必要な場合を除き、これらのパラメータは変更しないことを推奨します。

- [Select CDP device capabilities]：有効にするには、チェックボックスをオンにします。

（注）　Prime Infrastructure では、トレーシング中にネイバーを検出するために CDP を使用します。ネイバーが検証されると、Prime Infrastructure では、[CDP capabilities] フィールドを使用して、ネイバー デバイスが有効なスイッチであるかどうかを判別します。ネイバー デバイスが有効なスイッチでない場合は、トレースされません。

ステップ 4　行った変更を保存するには [Save] をクリックします。ページを元の設定に戻すには、[Reset] をクリックします。出荷時の初期状態に設定を戻すには、[Factory Reset] をクリックします。

スイッチ ポート トレーシングの確立

スイッチ ポート トレーシングを確立するには、次の手順を実行します。

ステップ 1　Prime Infrastructure ホームページで、[Security] ダッシュボードをクリックします。

ステップ 2　[Rogue APs and Adhoc Rogues] ダッシュレットで、不正要素の過去 1 時間以内、過去 24 時間以内、および合計のアクティブ数な指定する数値 URL をクリックします。[Alarms] ウィンドウが開きます。

ステップ 3　チェックボックスをオンにすることでスイッチ ポート追跡を設定する不例を選択します。

ステップ 4　[Troubleshoot] ドロップダウン リストから [Traceroute] を選択します。[Traceroute] ウィンドウが開き、Prime Infrastructure がスイッチ ポート トレースを実行します。

検索可能な MAC アドレスを 1 つ以上使用できる場合、Prime Infrastructure では CDP を使用して、検出中のアクセス ポイントから最大 2 ホップ離れて接続されているすべてのスイッチを検出します。各 CDP が検出したスイッチの MIB は、対象の MAC アドレスのいずれかが含まれているかどうかを確認するために検証されます。いずれかの MAC アドレスが見つかった場合、該当するポート番号が返され、不正スイッチ ポートとして報告されます。

[Switch Port Tracing Details] ダイアログボックスに関する追加情報については、「Switch Port Tracing Details」（P.7-6）を参照してください。

Switch Port Tracing Details

[Switch Port Tracing Details] ダイアログボックスでは、スイッチ ポートの有効化および無効化、スイッチ ポートのトレース、およびアクセス ポイント スイッチ トレースの詳細ステータスの表示を行うことができます。スイッチ ポート トレーシングの詳細については、以下のトピックを参照してください。

- スイッチ ポート トレーシングの設定：スイッチ ポート トレースの設定について説明します。
- 不正 AP トレーシングに対する SNMP クレデンシャルの設定：SNMP スイッチ クレデンシャルの設定について説明します。

[Switch Port tracing Details] ダイアログボックスで、次のいずれかを実行します。

- [Enable/Disable Switch Port(s)] をクリック：選択した任意のポートを有効または無効にします。
- [Trace Switch Port(s)] をクリック：別のスイッチ ポート トレースを実行します。
- [Show Detail Status] をクリック：このアクセス ポイントのスイッチ ポート トレースに関する詳細を表示します。
- [Close] をクリックします。

スイッチ ポート トレーシングのトラブルシューティング

スイッチ ポート トレーシング（SPT）は、ベストエフォート方式で動作します。SPT では、適切にトレースして不正 AP を組み込むために、以下の情報を必要とします。

- レポート アクセス ポイント：不正アクセス ポイントは 1 台以上の管理対象アクセス ポイントによってレポートされる必要があります。
- アクセス ポイント Cisco Discovery Protocol（CDP）ネイバー：シード スイッチを判別するために、アクセス ポイント CDP ネイバー情報が必要です。
- スイッチの IP アドレスと SNMP のクレデンシャル
  - トレースする必要のあるすべてのスイッチは管理 IP アドレスを持つ必要があり、SNMP 管理が有効にされている必要があります。
  - SNMP クレデンシャルが新しく変更される場合は、個々のスイッチを Prime Infrastructure に追加するのではなく、ネットワーク アドレスに基づき追加できます。
  - この新しい SNMP クレデンシャル機能は、read と write の両方についてデフォルトのコミュニティ ストリングを private とするデフォルト エントリ 0.0.0.0 を持ちます。
  - スイッチ ポートを有効または無効にするには、正しい write コミュニティ ストリングを指定する必要があります。トレーシングの場合、通常、read コミュニティ ストリングで十分です。
- スイッチ ポートの設定
  - トランキングされているスイッチ ポートは、トランク ポートとして正しく設定されている必要があります。
  - スイッチ ポートのセキュリティは無効にする必要があります。
- シスコ イーサネット スイッチだけがサポートされています。

（注） サポートされているスイッチは、3750、3560、3750E、3560E、および 2960 です。

- スイッチ VLAN 設定を適切に行う必要があります。
- すべてのスイッチについて CDP プロトコルが有効にされている必要があります。
- 不正アクセス ポイントとシスコ製スイッチの間にイーサネット接続が存在している必要があります。
- 不正アクセス ポイントとイーサネット スイッチの間に何らかのトラフィックが存在する必要があります。
- 不正アクセス ポイントは、最大ホップ カウントの制限内で、スイッチに接続される必要があります。デフォルト ホップは 2 です。最大ホップは 10 です。
- SNMPv3 を使用する場合は、メイン グループのための 1 個（VLAN ベースでない MIB 用に必要）の他に、コンテキスト オプションを使用して、VLAN ごとに 1 個作成してください。