WAP125およびWAP581でのSNMPv3の設定

目的

Simple Network Management Protocol Version 3(SNMPv3)は、ユーザとユーザが存在するグループに対して認証戦略を設定するセキュリティモデルです。セキュリティレベルは、セキュリティモデル内で許可されるセキュリティレベルです。セキュリティモデルとセキュリティレベルの組み合わせによって、SNMPパケットを処理するときに使用されるセキュリティメカニズムが決まります。

SNMPでは、Management Information Base（MIB；管理情報ベース）は、オブジェクト識別子(OID)を含む階層構造の情報データベースで、SNMPを介して読み取りまたは設定が可能な変数として機能します。MIBはツリー状の構造で構成されています。管理オブジェクトのネーミング・ツリー内のサブツリーは、ビュー・サブツリーです。MIBビューは、一連のビューサブツリーまたはビューサブツリーのファミリの組み合わせです。MIBビューは、SNMPv3ユーザがアクセスできるOID範囲を制御するために作成されます。SNMPv3ビューの設定は、限定されたMIBだけを表示するようにユーザを制限するために不可欠です。WAPには、2つのデフォルトビューを含め、最大16のビューを設定できます。

このドキュメントの目的は、WAP125およびWAP581でCPU/RAMアクティビティを収集、表示、ダウンロードする方法を示すことです。

該当するデバイス

- WAP125
- WAP581

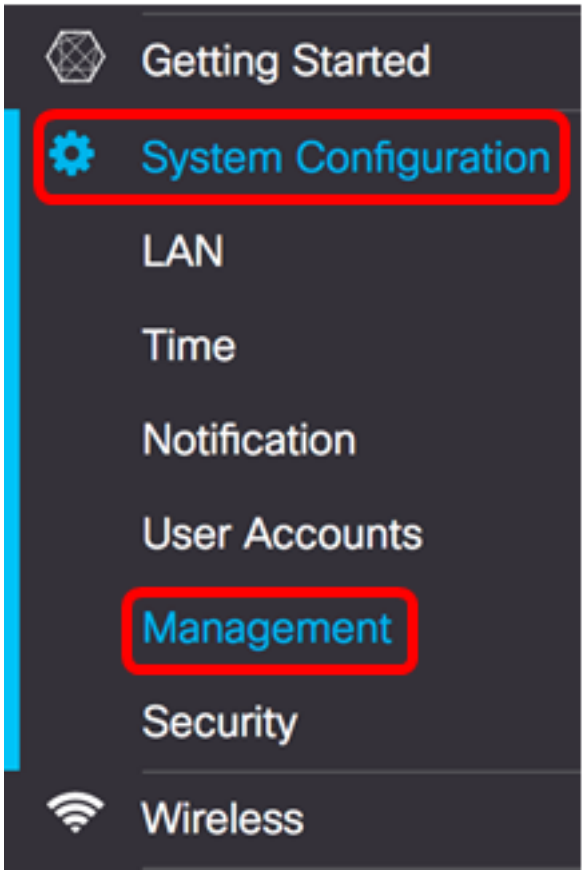
[Software Version]

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

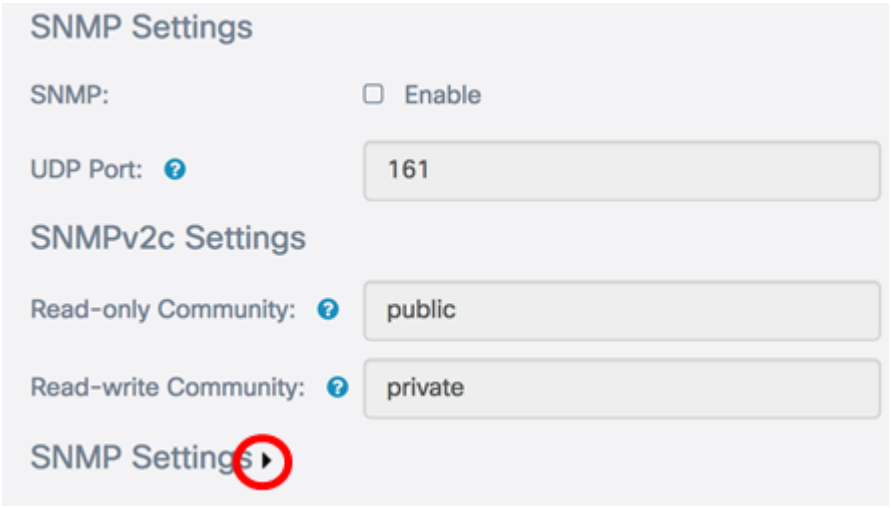
SNMPv3の設定

SNMPv3ビューの設定

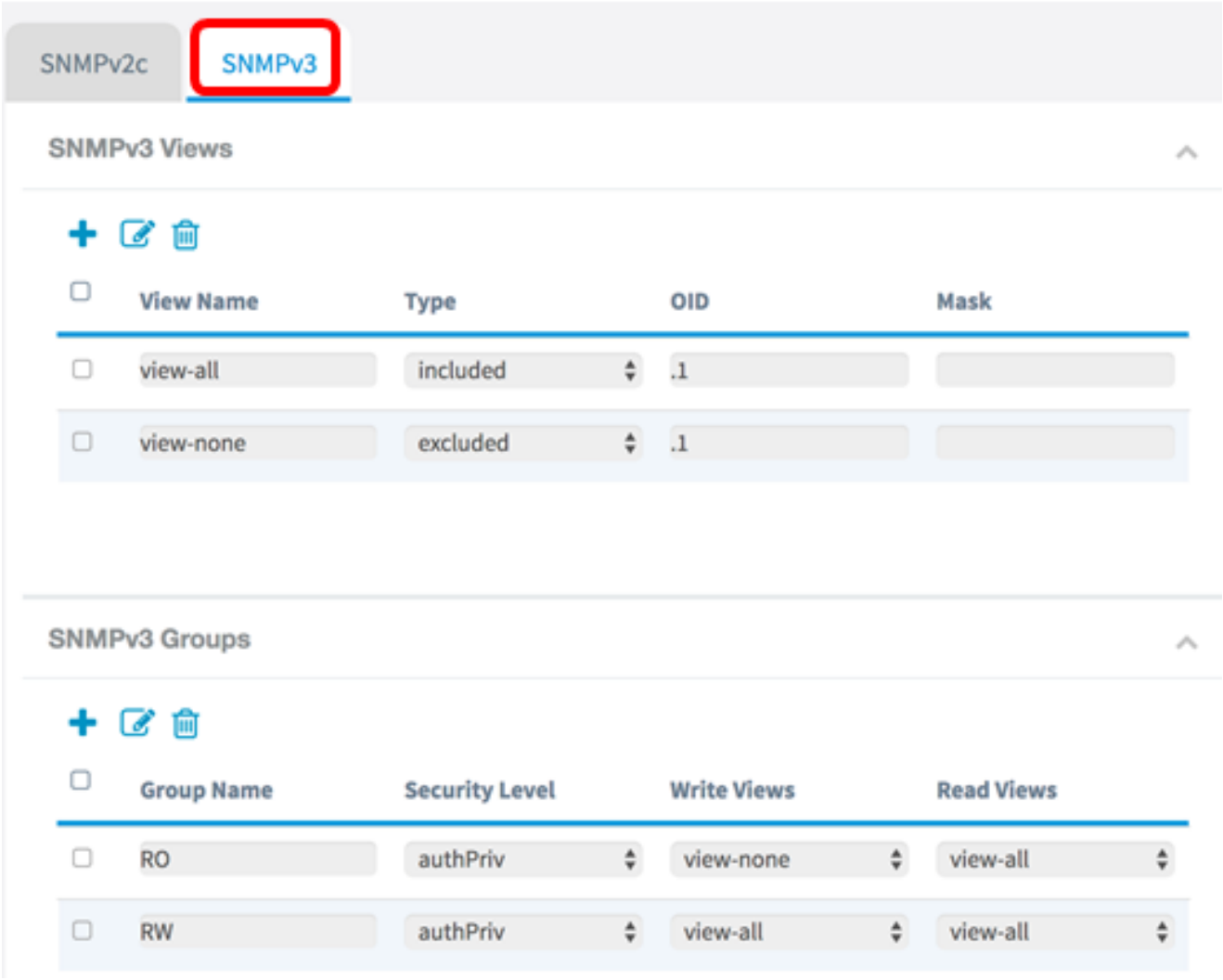
ステップ1:Webベースのユーティリティにログインし、[**System Configuration**] > [**Management**]を選択します。



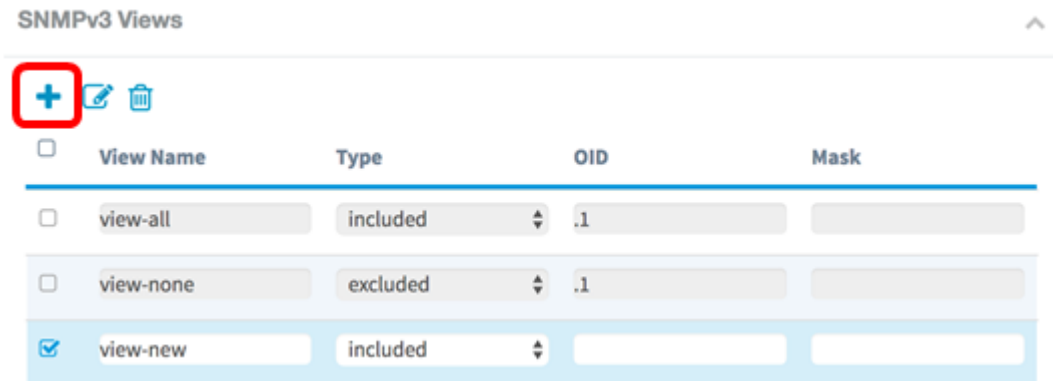
ステップ2:[SNMP Settings]の右**矢印をクリ**ックします。



ステップ3:[SNMPv3]タブ**をクリック**します。

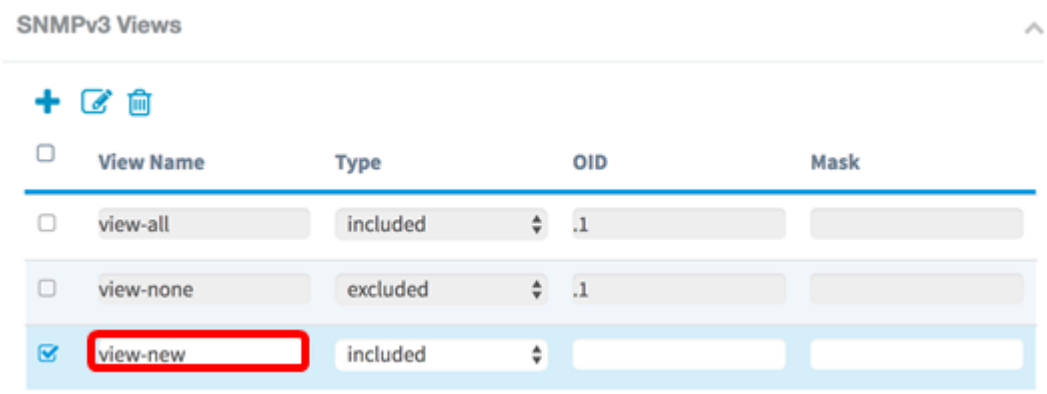


ステップ4:[+]ボタンをクリックして、[SNMPv3 Views]に新しいエントリを作成します。



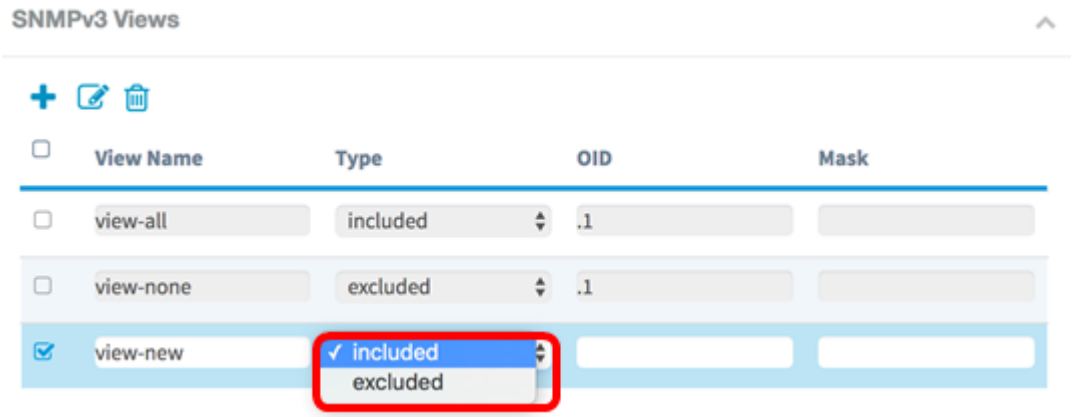
ステップ5:[View Name]フィールドに、MIBビューを識別する名前を入力します。

注：この例では、view-newがビュー名として作成されます。View-allおよびview-noneはデフォルトで作成され、システムでサポートされているすべての管理オブジェクトが含まれます。これらは変更や削除はできません。



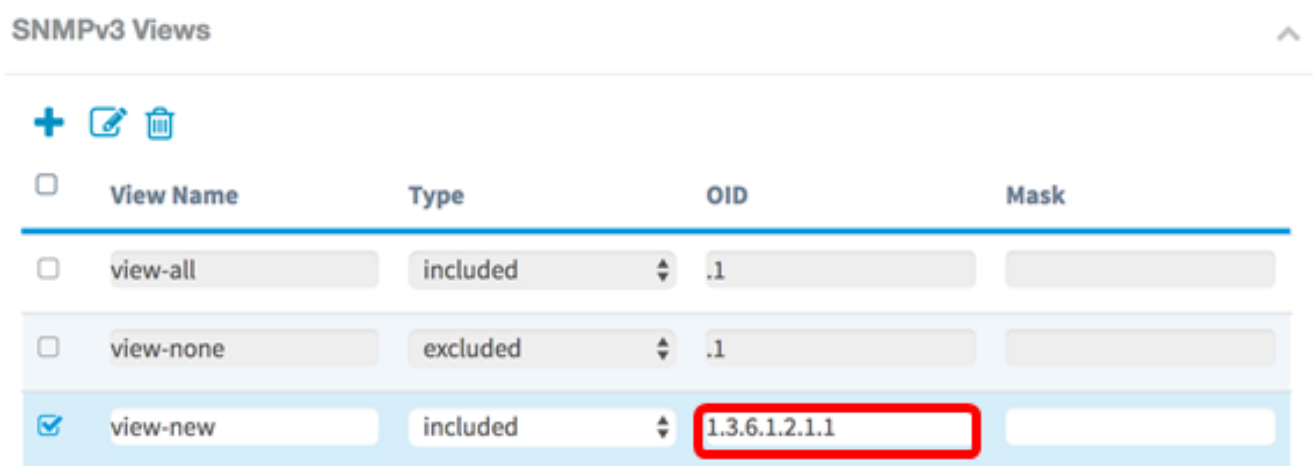
ステップ6:[Type（タイプ）]ドロップダウンリストから、ビューを除外するか含めるかを選択します。

- included:MIBビューのサブツリーまたはサブツリーファミリのビューを含みます。
- excluded：サブツリーまたはサブツリーファミリのビューをMIBビューから除外します。



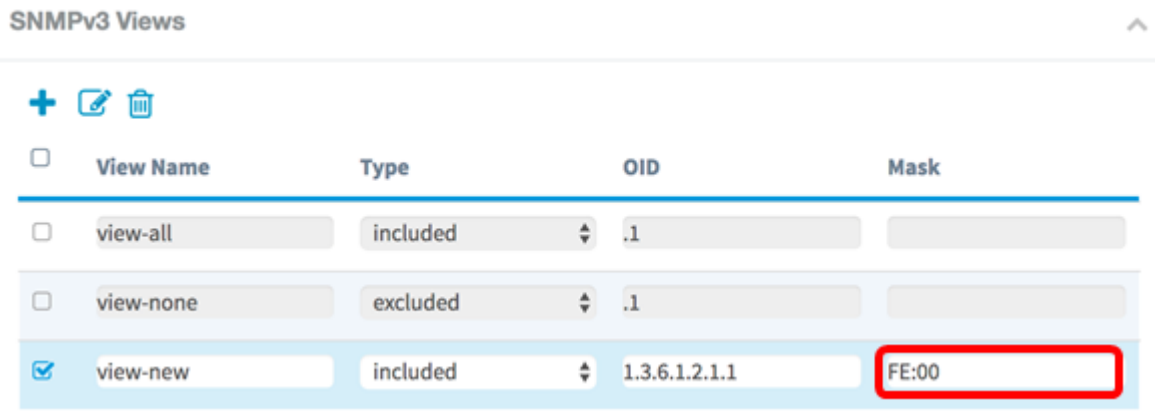
ステップ7:[*OID*]フィールドに、ビューに含める、またはビューから除外するサブツリーのOID文字列を入力します。各番号は情報の検索に使用され、各番号はOIDツリーの特定のブランチに対応します。OIDは、MIB階層内の管理対象オブジェクトの一意の識別子です。最上位のMIBオブジェクトIDは異なる標準組織に属し、下位のオブジェクトIDは関連付けられた組織によって割り当てられます。ベンダーが独自の製品の管理対象オブジェクトを含むようにプライベートブランチを定義できます。MIBファイルは、OID番号を人間が読み取り可能な形式にマッピングします。OID番号をオブジェクト名に変換するには、ここをクリックします。

注：この例では、1.3.6.1.2.1.1が使用されています。



ステップ8:[Mask]フィールドにOIDマスクを*入力*します。*Mask*フィールドは、OIDが存在するビューを決定する際に関連していると見なされるOIDサブツリーの要素を制御するために使用され、最大長は47文字です。形式は16オクテットで、各オクテットにはピリオドまたはコロンで区切られた2つの16進数文字が含まれます。マスクを決定するには、OID要素の数をカウントし、その多くのビットを1に設定します。このフィールドでは、16進形式のみが使用できます。例のOID 1.3.6.1.2.1.1には7つの要素があるため、最初のオクテットに7つの連続した1が1つ、2番目のオクテットにすべての0が続く場合、マスクとしてFE:00が取得されます。

注：この例では、FE:00が使用されています。



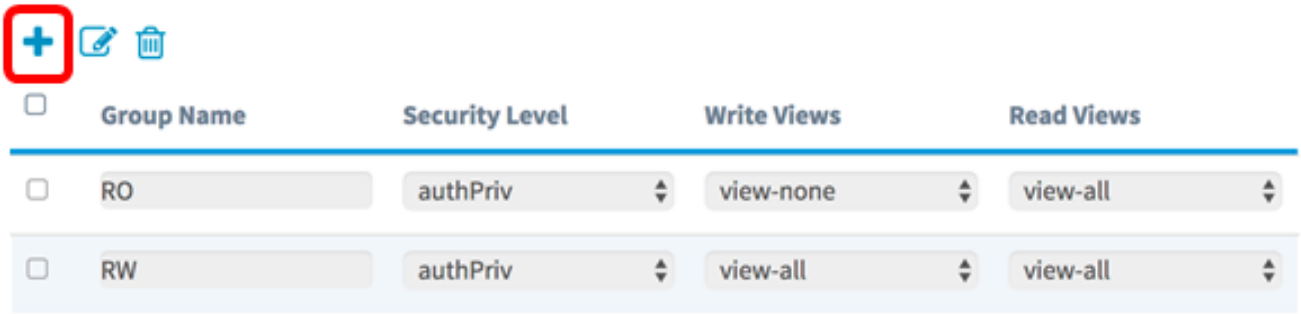
ステップ9：をクリックします 

。

これで、WAP125のSNMPv3ビューが正常に設定されました。

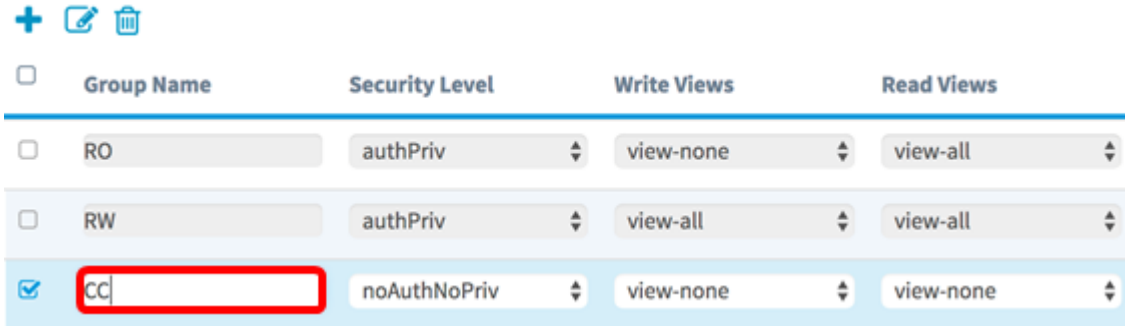
SNMPv3グループの設定

ステップ1:[+]ボタン**をクリック**して、[SNMPv3 Groups]に新しいエントリを作成します。



ステップ2:[Group Name]フィールドに、グループの識別に使用する名前を入力します。ROおよびRWのデフォルト名は再利用できません。グループ名には、最大32文字の英数字を使用できます。

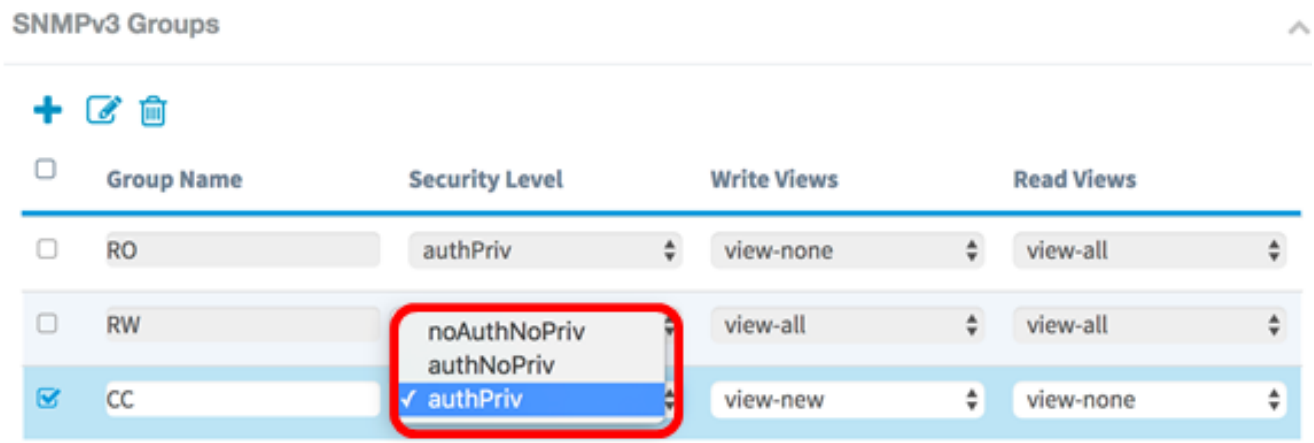
注：この例では、CCが使用されています。



ステップ3:[Security Level]ドロップダウンリストから、適切なレベルの認証を選択します。

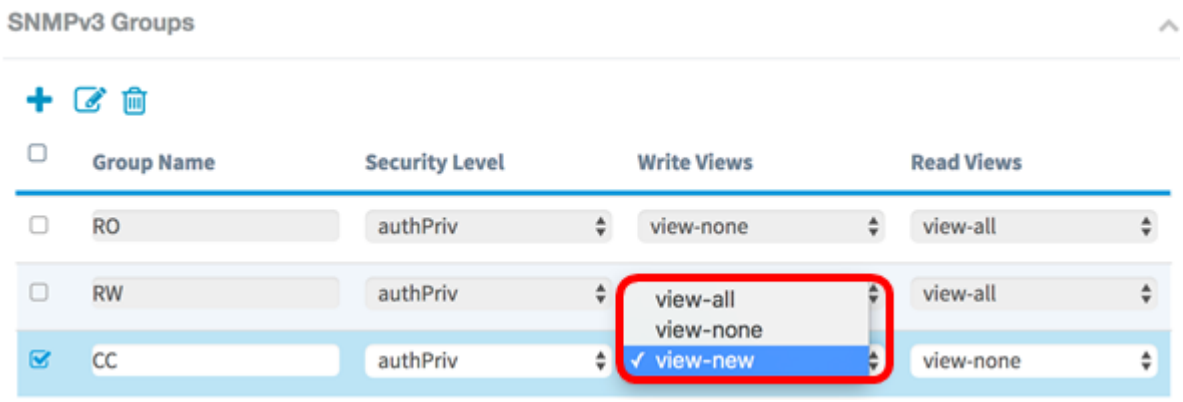
- noAuthNoPriv：認証なし、データ暗号化なし（セキュリティなし）を提供します。
- authNoPriv：認証を提供しますが、データ暗号化は提供しません（セキュリティは提供されません）。 認証は、セキュアハッシュ認証(SHA)パスフレーズによって提供されます。
- authPriv：認証とデータ暗号化。認証はSHAパスフレーズによって提供されます。データ暗号化は、DESパスフレーズによって提供されます。

注：この例では、authPrivが使用されています。



ステップ4:[Write Views]ドロップダウンリストから、新しいグループのすべての管理オブジェクト(MIB)への書き込みアクセス権を選択します。これは、グループがMIBで実行できるアクションを定義します。このリストには、WAPで作成された新しいSNMPビューも含まれます。

注：この例では、view-newを使用します。



ステップ5:[Read Views]ドロップダウンリストから、新しいグループのすべての管理オブジェクト(MIB)の読み取りアクセス権を選択します。次に示すデフォルトオプションは、WAPで作成された他のビューとともに表示されます。

- view-all：グループはすべてのMIBを表示および読み取ることができます。
- view-none：これはグループを制限し、誰もMIBを表示したり読み取ったりできないようにします。
- view-new：ユーザが作成したビュー。

注：この例では、view-noneを使用します。

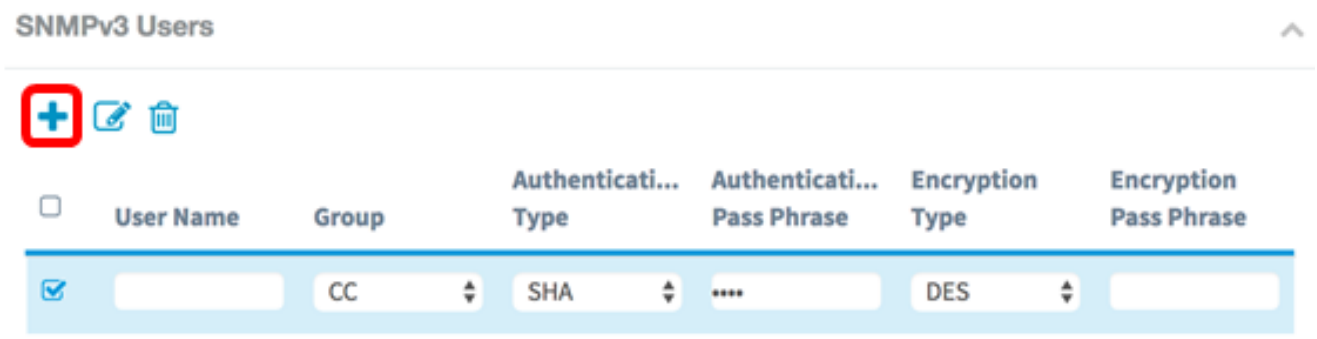
ステップ6：をクリックします Save。

これで、SNMPv3グループが正常に設定されました。

SNMPv3ユーザの設定

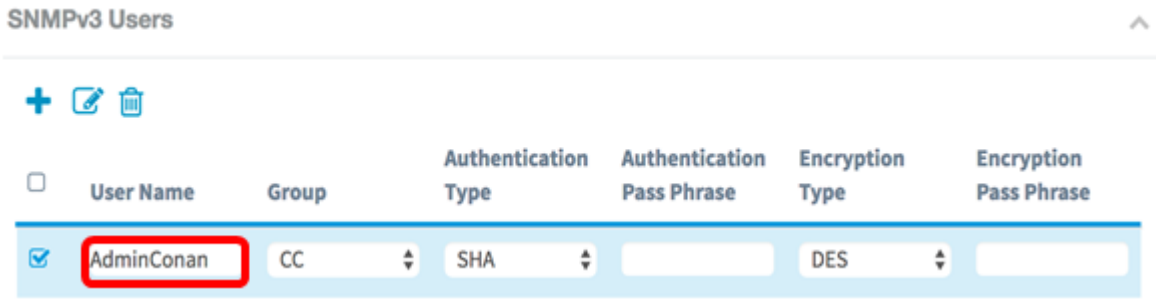
SNMPユーザは、ログインクレデンシャル（ユーザ名、パスワード、および認証方式）によって定義され、SNMPグループおよびエンジンIDと関連付けて動作します。SNMPv3だけがSNMPユーザを使用します。アクセス権限を持つユーザは、SNMPビューに関連付けられます。

ステップ1:[+]ボタンをクリックして、[SNMPv3 Users]に新しいエントリを作成します。



ステップ2:[ユーザー名]フィールドで、SNMPユーザーを示すユーザー名を作成します。

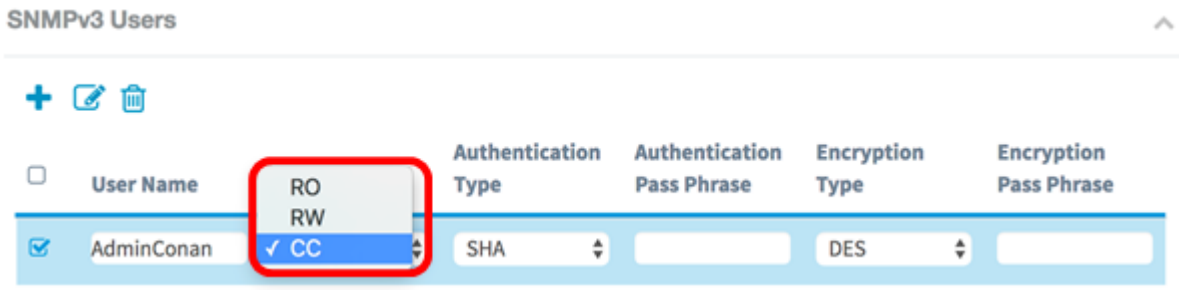
注：この例では、AdminConanが使用されています。



ステップ3:[Group]ドロップダウンリストから、ユーザにマッピングするグループを選択します。次のオプションがあります。

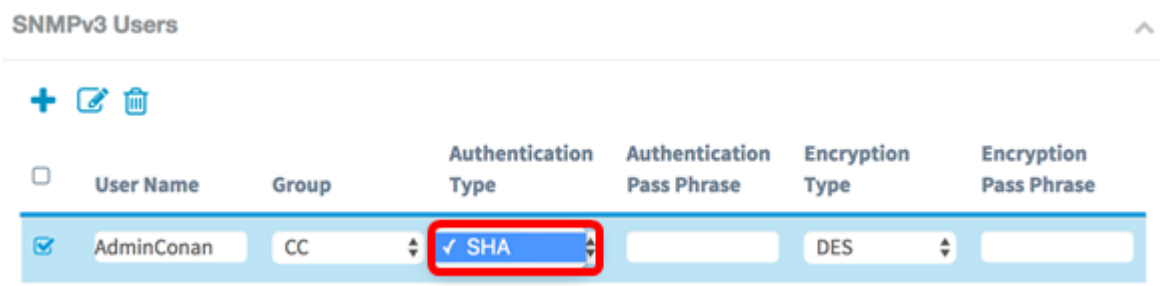
- RO：デフォルトで作成された読み取り専用グループ。このグループを使用すると、ユーザは設定のみを表示できます。
- RW：デフォルトで作成された読み取り/書き込みグループ。このグループを使用すると、ユーザは設定を表示し、必要な変更を加えることができます。
- [CC]：ユーザ定義グループのCC。ユーザ定義グループは、グループが定義されている場合にのみ表示されます。

注：この例では、[Configure SNMPv3 Groups]のステップ2で定義されているように[CC]が選択されています。

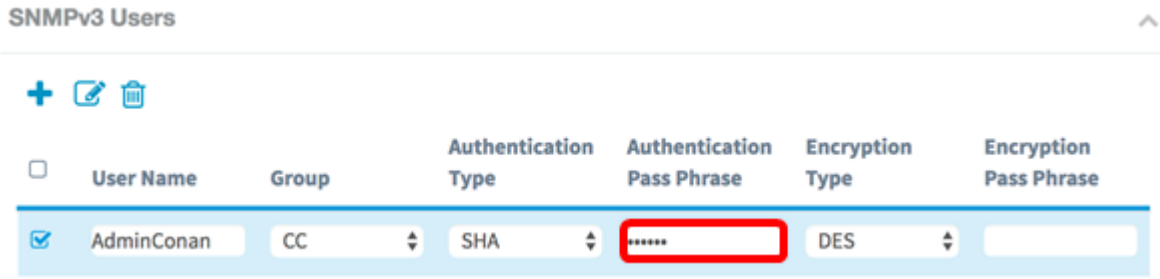


ステップ4:[Authentication]ドロップダウンリストから[SHA]を選択します。

注：ステップ3で選択したグループセキュリティレベルがnoAuthNoPrivに設定されている場合、このエリアはグレー表示されます。



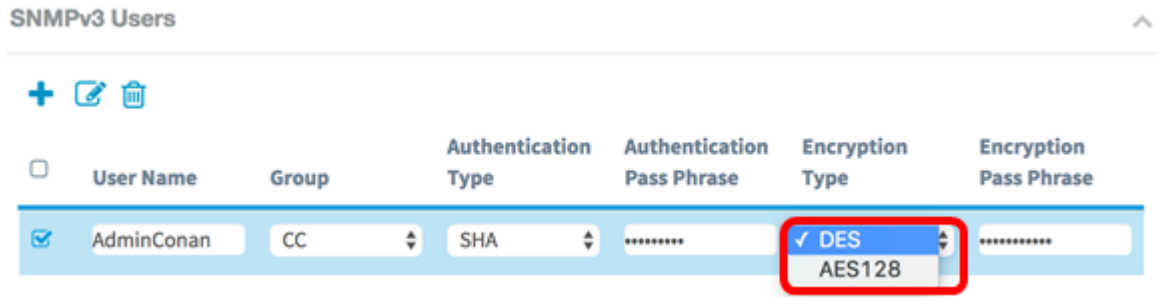
ステップ5:[*Authentication Pass Phrase*]フィールドに、ユーザーに関連するパスフレーズを入力します。これは、デバイスが相互に接続するためにデバイスを認証するように設定する必要があるSNMPパスワードです。



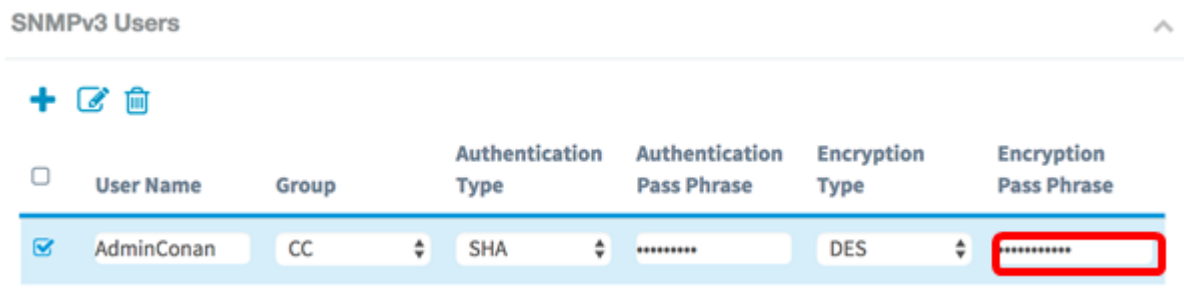
ステップ6:[Encryption Type]ドロップダウンメニューから、SNMPv3要求を暗号化する暗号化方式を選択します。次のオプションがあります。

- DES:Data Encryption Standard（DES；データ暗号規格）は、64ビットの共有秘密キーを使用する対称ブロック暗号です。
- AES128:128ビットキーを使用するAdvanced Encryption Standard（AES；高度暗号化規格）。

注：この例では、DESが選択されています。



ステップ7:[*Encryption Pass Phrase*]フィールドに、ユーザーに関連付けられたパスフレーズを入力します。これは、ネットワーク内の他のデバイスに送信されるデータを暗号化するために使用されます。このパスワードは、もう一方の端のデータを復号化するためにも使用されます。パスフレーズは、通信デバイスで一致している必要があります。パスフレーズの長さは8 ~ 32文字です。



ステップ8：をクリックします Save。

これで、WAP125のSNMPv3ユーザが正常に設定されたはずです。

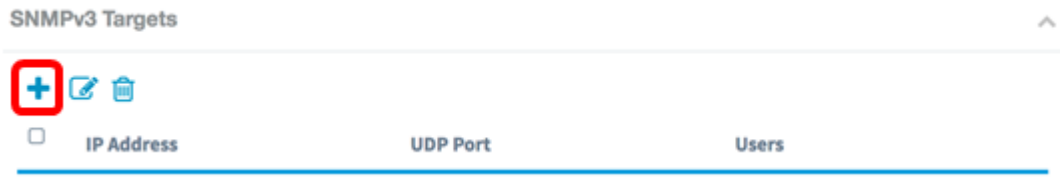
SNMPv3ターゲットの設定

SNMPターゲットは、送信されるメッセージと、エージェント通知の送信先となる管理デバイスの両方を参照します。各ターゲットは、ターゲット名、IPアドレス、UDPポート、およびユーザ名で識別されます。

SNMPv3は、SNMPターゲット通知をトラップではなくSNMPマネージャにインフォームメッセージとして送信します。これにより、トラップは確認応答を使用しませんが、インフォームは使用するため、ターゲット配信が保証されます。

ステップ1:[+]ボタン**をクリック**して、[SNMPv3 Targets]に新しいエントリを作成します。

注：最大16個のターゲットを設定できます。



ステップ2:[*IP Address*]フィールド*に、すべてのSNMPトラップが送信される対象*のIPアドレスを入力します。これは通常、ネットワーク管理システム(NMS)のアドレスです。これは、IPv4アドレスまたはIPv6アドレスのいずれかです。

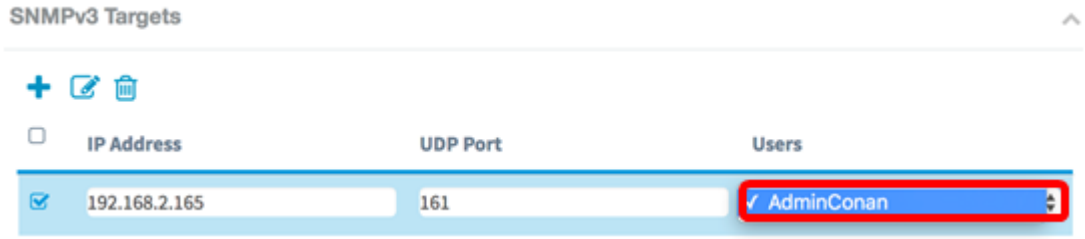
注：この例では、192.168.2.165が使用されています。

ステップ3:[UDPポート]フィールドにユーザデータグラムプロトコル(UDP)ポート*番号を入力*します。SNMPエージェントは、このポートでアクセス要求をチェックします。デフォルトは161です。有効な範囲は1025 ~ 65535です。

注：この例では、161が使用されています。

ステップ4:[Users]ドロップダウンリストから、ターゲットに関連付けるユーザを選択します。このリストには、[ユーザ(Users)]ページで作成されたすべてのユーザのリストが表示されます。

注：ユーザとして[AdminConan]が選択されます。



ステップ5：をクリックします 

。

これで、WAP125およびWAP581でSNMPv3ターゲットが正しく設定されたはずです。