Configurez le SNMPv3 sur le WAP125 et le WAP581

Objectif

La version 3 (SNMPv3) de protocole SNMP est un modèle de Sécurité dans lequel une stratégie d'authentification est installée pour un utilisateur et le groupe dans lesquels l'utilisateur réside. Le niveau de Sécurité est le niveau de sécurité permis dans un modèle de Sécurité. Une combinaison d'un modèle de Sécurité et d'un niveau de Sécurité détermine quel mécanisme de sécurité est utilisé en manipulant un paquet SNMP.

Dans le SNMP, le Management Information Base (MIB) est une base de données hiérarchique de l'information contenant les identifiants d'objet (OID) qui agit en tant que variable qui peut être lue ou placée par l'intermédiaire du SNMP. Le MIB est organisé dans une structure comme une arborescence. Un sous-arbre dans l'objet géré nommant l'arborescence est un sous-arbre de vue. Une vue MIB est une combinaison d'un ensemble de sous-arbres de vue ou d'une famille des sous-arbres de vue. Des vues MIB sont créées pour contrôler la plage OID que les utilisateurs SNMPv3 peuvent accéder à. La configuration des vues SNMPv3 est essentielle pour limiter un utilisateur pour visualiser seulement le MIB limité. Un WAP peut avoir jusqu'à 16 points de vue comprenant les deux vues par défaut.

L'objectif de ce document est de t'afficher comment recueillir, visualiser, et télécharger l'activité CPU/RAM sur le WAP125 et le WAP581.

Périphériques applicables

- WAP125
- WAP581

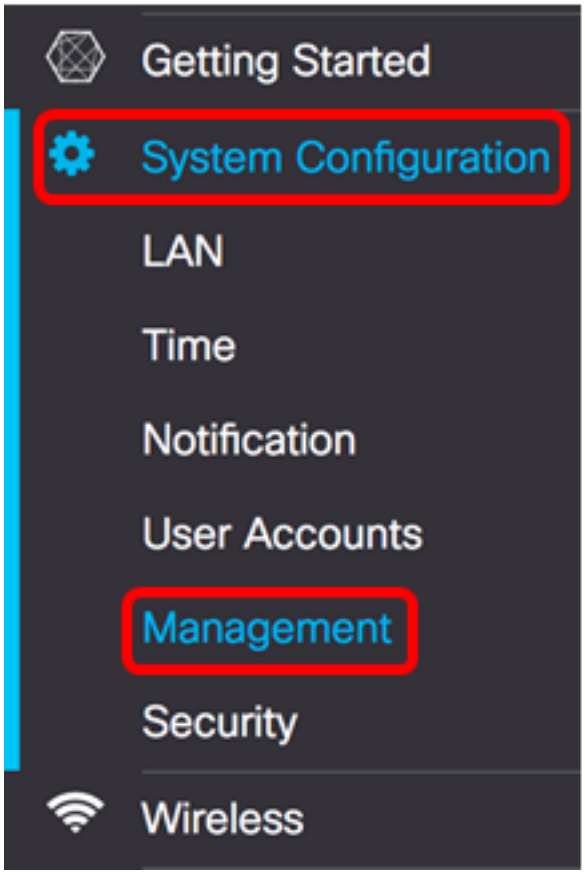
Version de logiciel

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

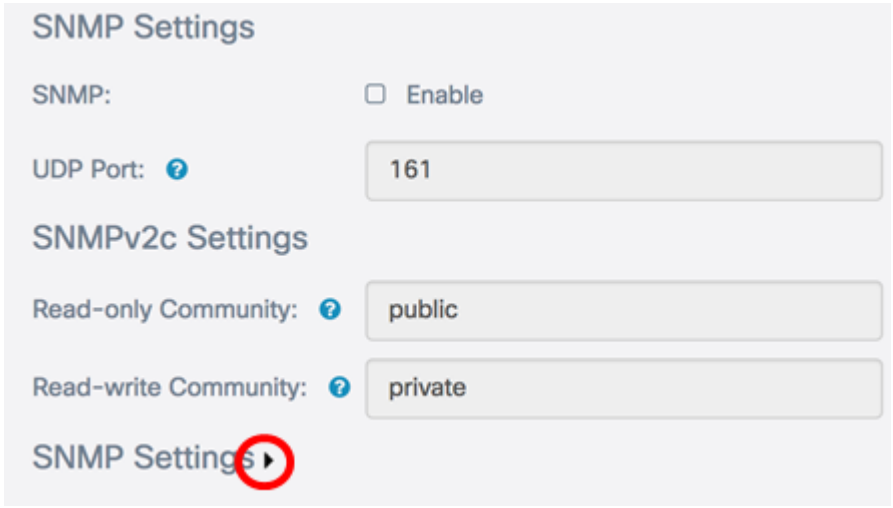
Configurez les configurations SNMPv3

Configurez les vues SNMPv3

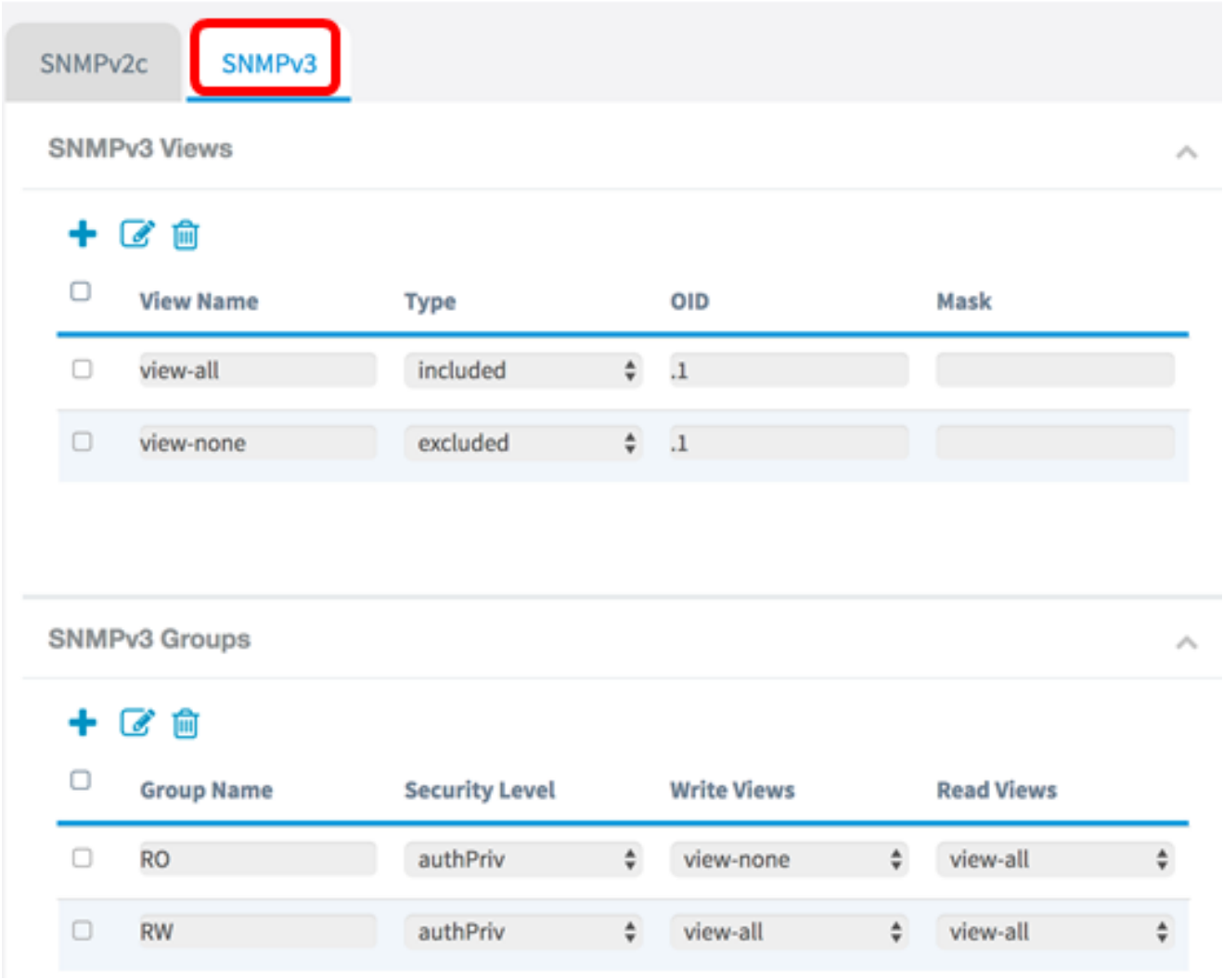
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB et choisissez la **configuration système > la Gestion**.



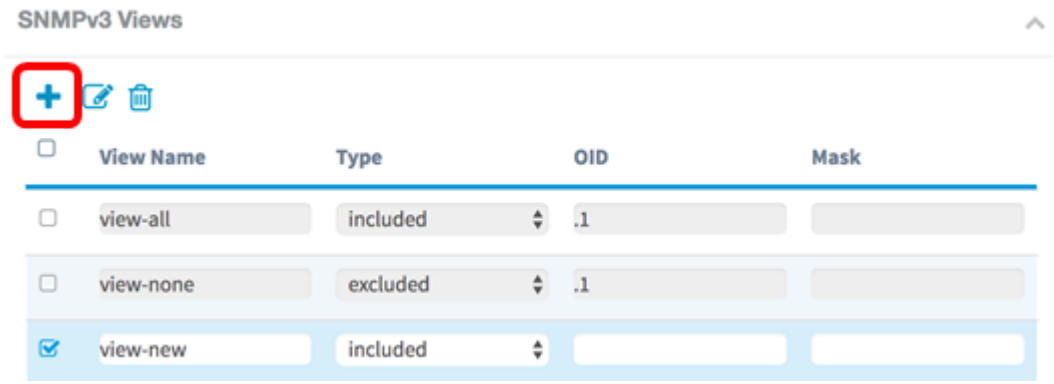
Étape 2. Cliquez sur la flèche à droite de **configurations SNMP**.



Étape 3. Cliquez sur l'onglet **SNMPv3**.

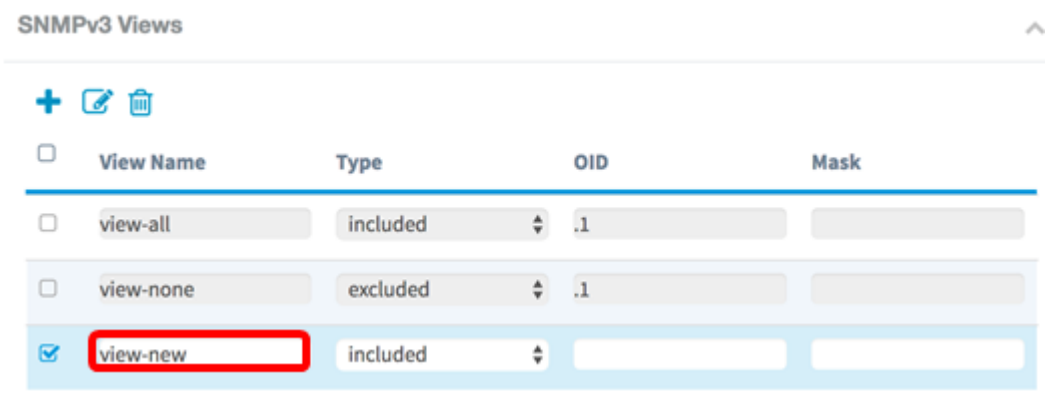


Étape 4. Cliquez sur **+** bouton pour créer une nouvelle entrée sous les vues SNMPv3.



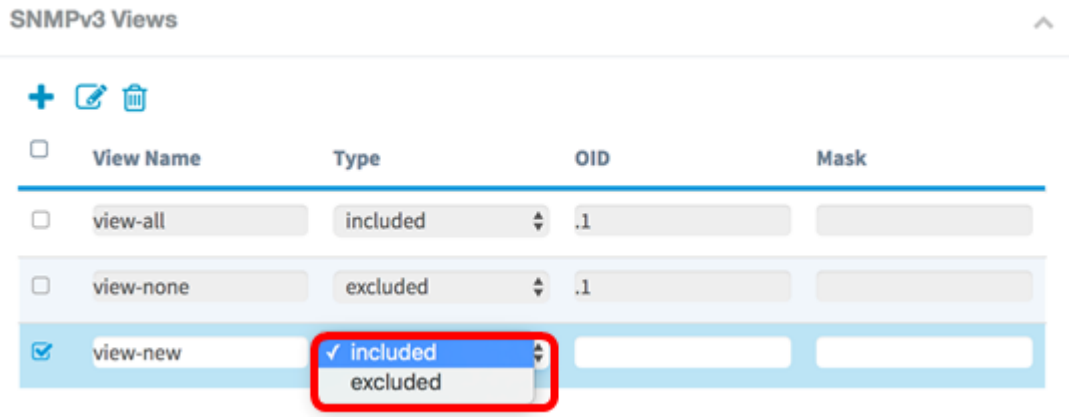
Étape 5. Dans la zone d'*identification de vue*, écrivez un nom qui identifie la vue MIB.

Remarque: Dans cet exemple, vue-nouveau est créé comme le nom de vue. Vue-tout et vue-aucuns sont créés par défaut et contiennent tous les objets de Gestion pris en charge par le système. Ceux-ci ne peuvent pas être modifiés ni supprimés.



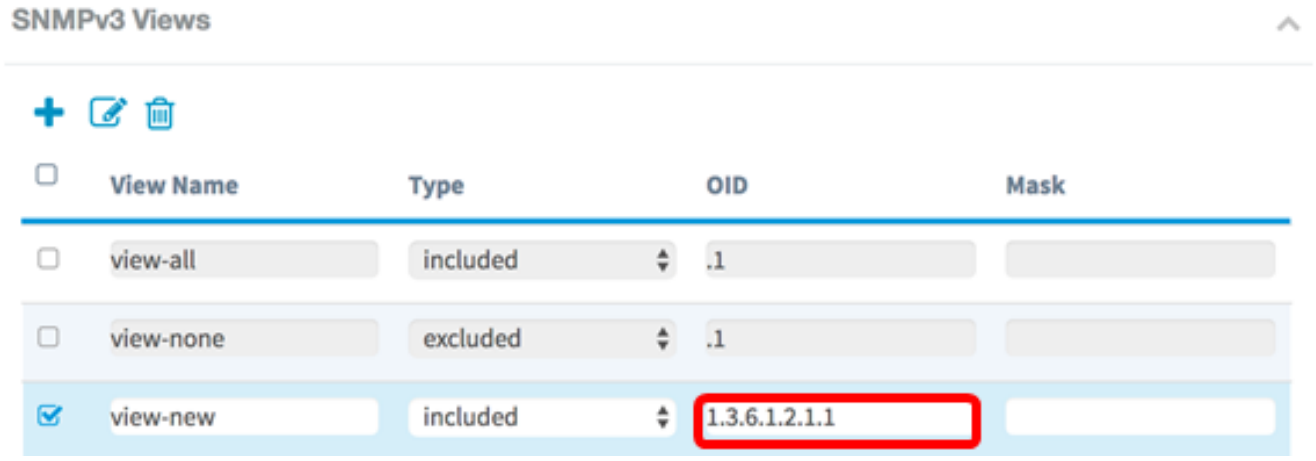
Étape 6. De la liste déroulante de type, choisissez une option si exclure ou inclure la vue.

- inclus — Inclut la vue dans le sous-arbre ou la famille des sous-arbres de la vue MIB.
- exclu — Exclut la vue dans le sous-arbre ou la famille des sous-arbres de la vue MIB.



Étape 7. Dans le domaine *OID*, écrivez une chaîne OID pour le sous-arbre pour inclure ou l'exclure de la vue. Chaque nombre est utilisé pour localiser les informations et chaque nombre correspond à un branchement spécifique de l'arborescence OID. Les OID sont des identifiants uniques des objets gérés dans la hiérarchie MIB. Les object id MIB de haut niveau appartiennent à différentes organisations de normalisation, alors que des object id plus élémentaires sont alloués par des organismes associés. Des branchements privés peuvent être définis par des constructeurs pour inclure les objets gérés pour leurs propres Produits. La liste des fichiers MIB OID numérote au format lisible pour l'homme. Pour traduire le nombre OID au nom d'objet, a cliquez ici.

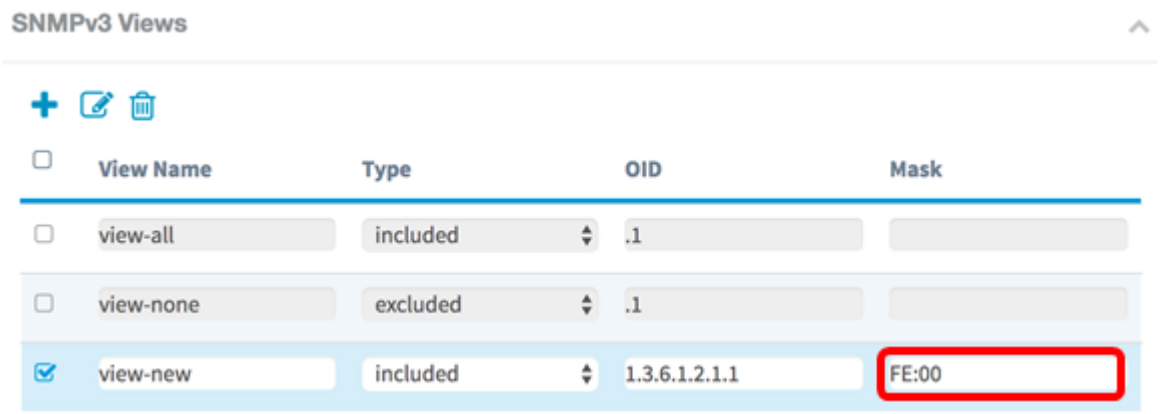
Remarque: Dans cet exemple, 1.3.6.1.2.1.1 est utilisés.



Étape 8. Écrivez un masque OID dans le domaine de *masque*. Le champ de *masque* est

utilisé pour contrôler les éléments du sous-arbre OID qui devrait être considéré en tant qu'approprié quand vous déterminez la vue dans laquelle un OID est, et le maximum est 47 caractères de longueur. Le format est 16 octets de longueur et chaque octet contient deux caractères hexadécimaux séparés par une période ou des deux points. Pour déterminer le masque, comptez le nombre d'éléments OID et placez que beaucoup de bits à un. Seulement des formats hexadécimaux sont reçus dans ce domaine. Considérez l'exemple OID 1.3.6.1.2.1.1, il a sept éléments, ainsi si vous réglé sept 1s consécutifs suiviez par un 0 dans le premier octet et tous zéros dedans le second, vous obtenez FE:00 comme masque.

Remarque: Dans cet exemple, FE:00 est utilisé.

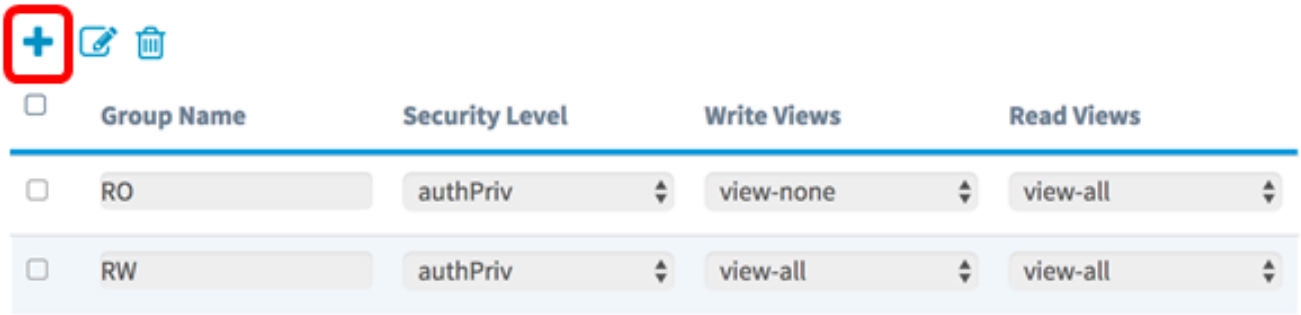


Étape 9. Clic Save.

Vous devriez avoir maintenant avec succès configuré les vues SNMPv3 sur le WAP125.

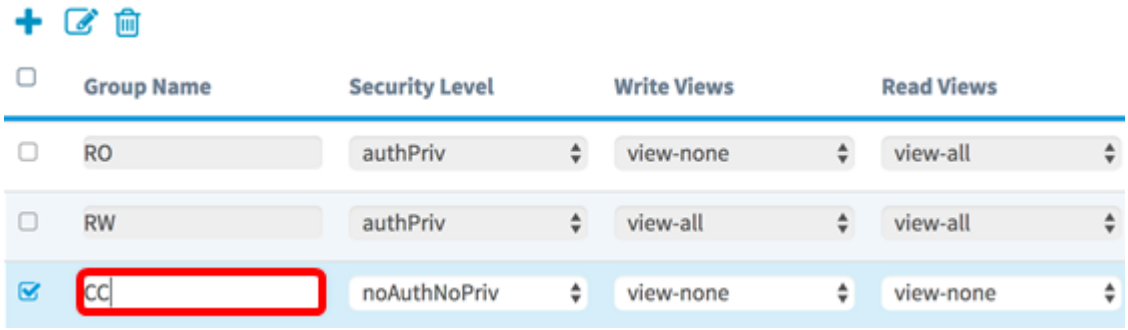
Configurez les groupes SNMPv3

Étape 1. Cliquez sur **+** bouton pour créer une nouvelle entrée sous les groupes SNMPv3.



Étape 2. Écrivez un nom utilisé pour identifier le groupe dans la zone d'*identification de groupe*. Les noms par défaut du RO et du RW ne peuvent pas être réutilisés. Les noms de groupe peuvent contenir jusqu'à 32 caractères alphanumériques.

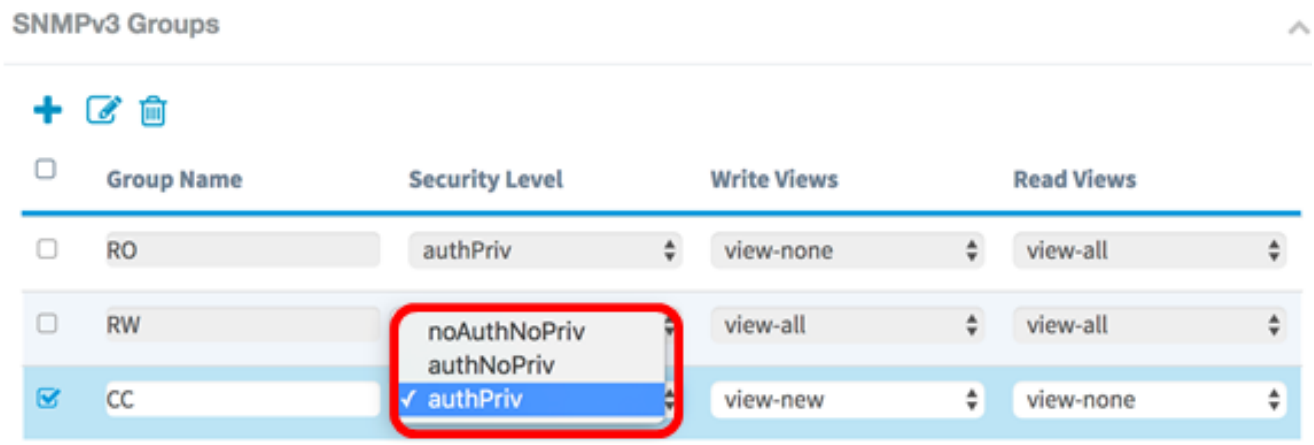
Remarque: Dans cet exemple, le cc est utilisé.



Étape 3. De la liste déroulante de niveau de Sécurité, choisissez un niveau approprié de l'authentification.

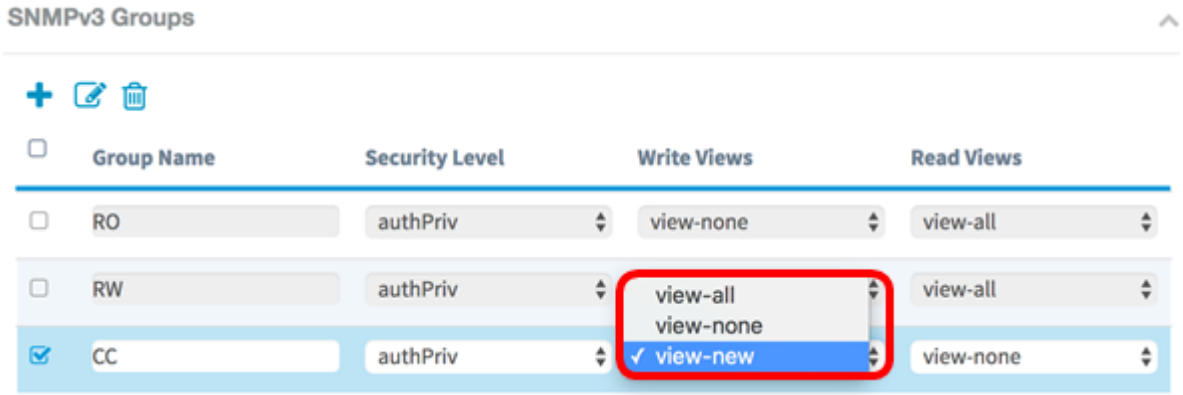
- noAuthNoPriv — Ne fournit aucune authentification et aucun chiffrement de données (aucune Sécurité).
- authNoPriv — Ne fournit l'authentification mais aucun chiffrement de données (aucune Sécurité). L'authentification est fournie par un mot de passe d'authentification de Secure Hash (SHA).
- authPriv — Authentification et chiffrement de données. L'authentification est fournie par un mot de passe de SHA. Le chiffrement de données est fourni par mot de passe DES.

Remarque: Dans cet exemple, l'authPriv est utilisé.



Étape 4. De la liste déroulante de vues d'inscription, choisissez l'accès en écriture à tous les objets de Gestion (MIB) pour le nouveau groupe. Ceci définit l'action qu'un groupe peut exécuter sur le MIB. Cette liste inclura également n'importe quel nouveau SNMP Views qui ont été créés sur le WAP.

Remarque: Dans cet exemple, vue-nouveau est utilisé.



Étape 5. Choisissez l'accès en lecture pour tous les objets de Gestion (MIB) pour le nouveau groupe de la liste déroulante lue de vues. Les options par défaut données ci-dessous apparaît avec toutes les autres vues créées sur le WAP.

- vue-tout — Ceci laisse des groupes pour visualiser et lire tout le MIB.
- vue-aucuns — Ceci limite le groupe de sorte que personne ne puisse visualiser ou lire n'importe quel MIB.
- vue-nouveau — Vue créée par l'utilisateur.

Remarque: Dans cet exemple, vue-aucun est utilisé.

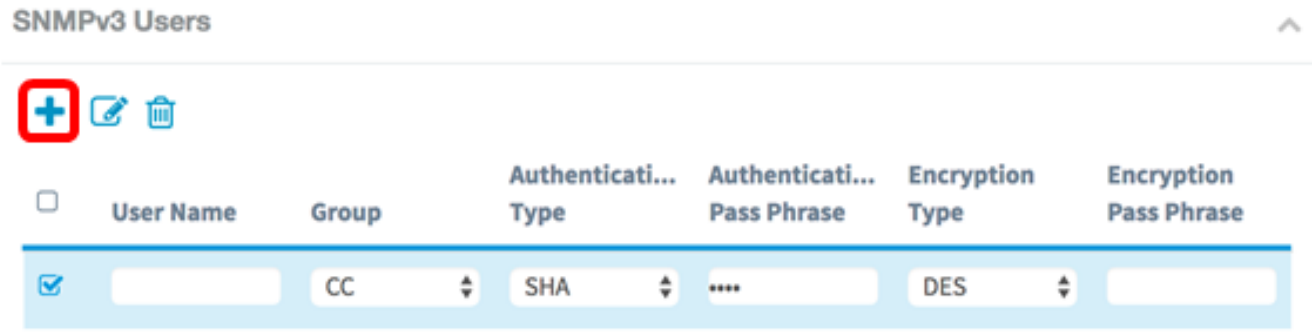
Étape 6. Clic Save.

Vous devriez avoir maintenant avec succès configuré les groupes SNMPv3.

Configurez les utilisateurs SNMPv3

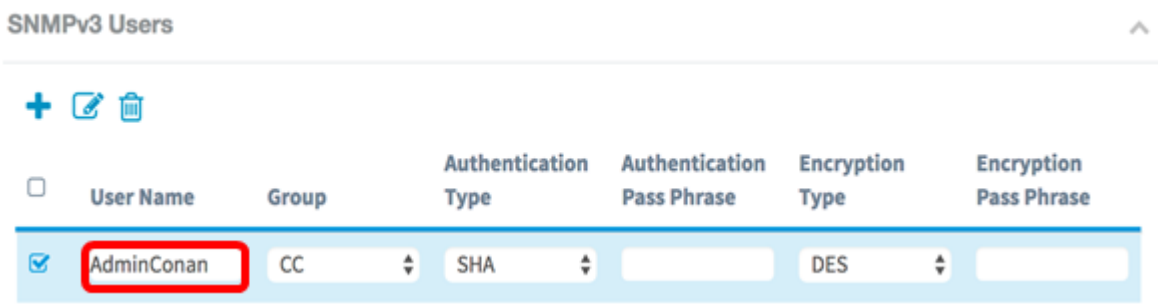
Un utilisateur SNMP est défini par ses qualifications de procédure de connexion (nom d'utilisateur, mots de passe, et méthode d'authentification) et il est actionné en association avec un ID de groupe et d'engine SNMP. Seulement SNMPv3 utilise des utilisateurs SNMP. Des utilisateurs avec des privilèges d'accès sont associés avec une vue SNMP.

Étape 1. Cliquez sur **+** bouton pour créer une nouvelle entrée sous les utilisateurs SNMPv3.



Étape 2. Dans le *champ User Name*, créez un nom d'utilisateur qui dénoterait un utilisateur SNMP.

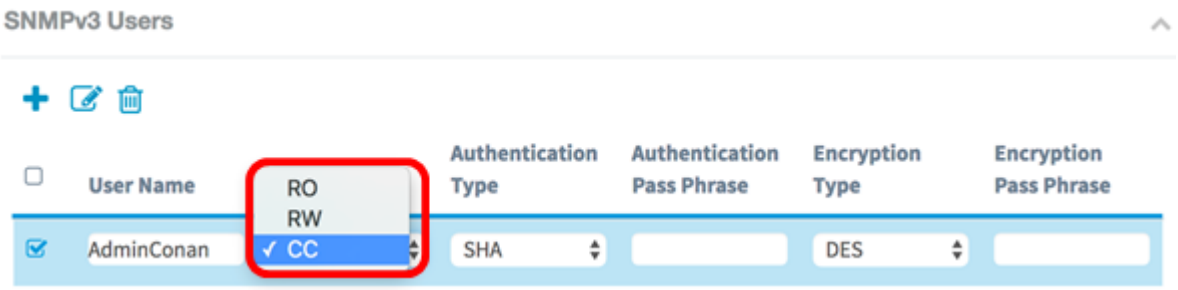
Remarque: Dans cet exemple, AdminConan est utilisé.



Étape 3. De la liste déroulante de groupe, choisissez un groupe pour tracer à l'utilisateur. Les options sont :

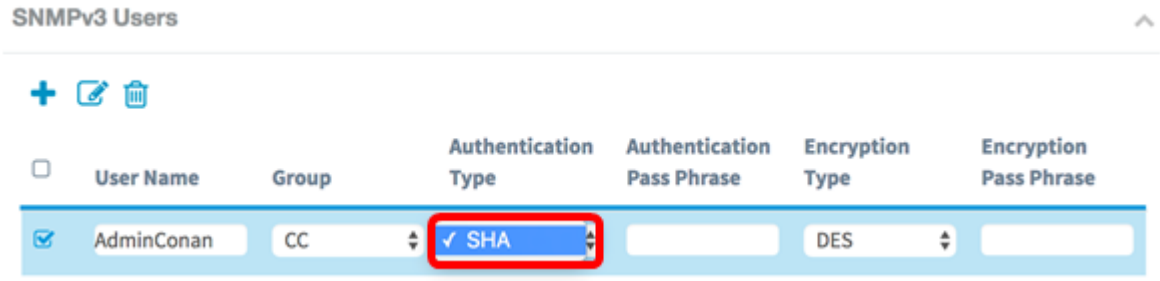
- RO — Groupe en lecture seule, créé par défaut. Ce groupe permet à un utilisateur pour visualiser seulement la configuration.
- LE RW — Groupe lecture/écriture, créé par défaut. Ce groupe permet à un utilisateur pour visualiser et apporter des modifications nécessaires à la configuration.
- Cc — Cc, un groupe défini par l'utilisateur. Le groupe défini par l'utilisateur apparaît seulement si un groupe a été défini.

Remarque: Dans cet exemple, le cc est choisi comme défini dans l'étape 2 configurez dessous les groupes SNMPv3.

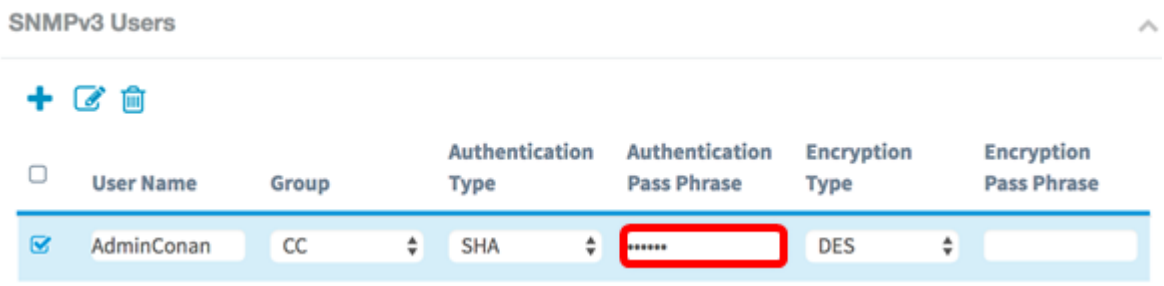


Étape 4. De la liste déroulante d'authentification, choisissez le **SHA**.

Remarque: Cette zone est greyed si le niveau de Sécurité de groupe choisi dans l'étape 3 était placé au noAuthNoPriv.



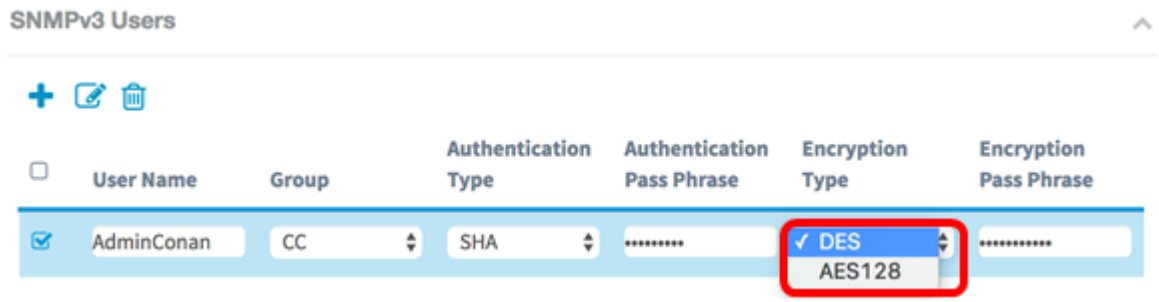
Étape 5. Dans le domaine de *mot de passe d'authentification*, entrez dans le mot de passe associé pour l'utilisateur. C'est le mot de passe SNMP qui doit être configuré pour authentifier les périphériques afin qu'ils puissent pour se connecter les uns avec les autres.



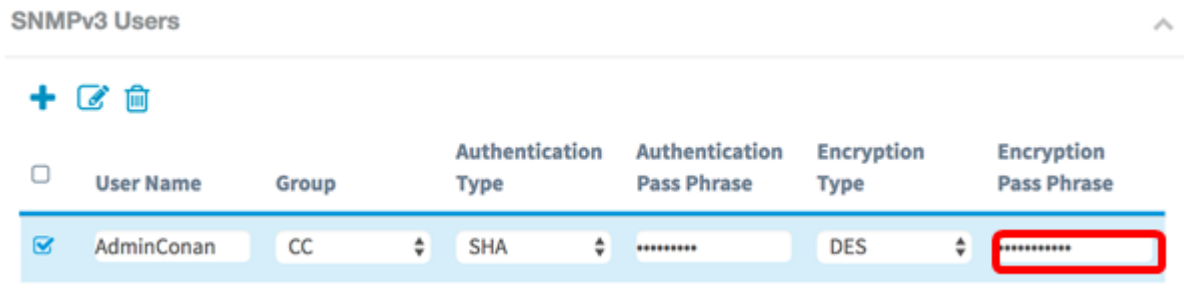
Étape 6. Du menu déroulant de type de cryptage, choisissez une méthode de cryptage pour chiffrer les demandes SNMPv3. Les options sont :

- DES — Le Norme de chiffrement de données (DES) est un chiffre par bloc symétrique qui utilise une clé secrète partagée 64-bit.
- AES128 — Advanced Encryption Standard qui utilise une clé 128-bit.

Remarque: Dans cet exemple, le DES est choisi.



Étape 7. Dans le domaine de *mot de passe de cryptage*, entrez dans le mot de passe associé pour l'utilisateur. Ceci est utilisé pour chiffrer les données transmises aux autres périphériques dans le réseau. Ce mot de passe est également utilisé pour déchiffrer les données sur l'autre extrémité. Le mot de passe doit s'assortir dans les périphériques de communication. Le mot de passe peut s'étendre de huit à 32 caractères de longueur.



Étape 8. Clic Save.

Vous devriez avoir maintenant avec succès configuré les utilisateurs SNMPv3 sur le WAP125.

Configurez les cibles SNMPv3

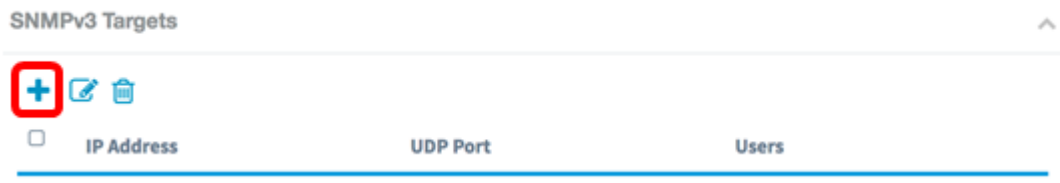
Une cible SNMP se rapporte au message envoyé et au périphérique de Gestion auxquels des notifications d'agent sont envoyées. Chaque cible est identifiée par le nom cible, l'adresse IP, le port UDP, et le nom d'utilisateur.

SNMPv3 envoient des notifications de cible SNMP comme informent des messages au SNMP Manager plutôt que des déroutements. Ceci s'assure que la livraison de cible puisque

les déroutements ne les utilisent pas reconnaissent mais informe font.

Étape 1. Cliquez sur **+** bouton pour créer une nouvelle entrée sous les cibles SNMPv3.

Remarque: Un total de jusqu'à 16 cibles peuvent être configurées.



Étape 2. Dans le *champ IP Address*, écrivez l'adresse IP de cible où tous les déroutements SNMP seront envoyés. C'est typiquement l'adresse de système d'administration de réseaux. Ceci peut être un ipv4 ou ipv6 addres.

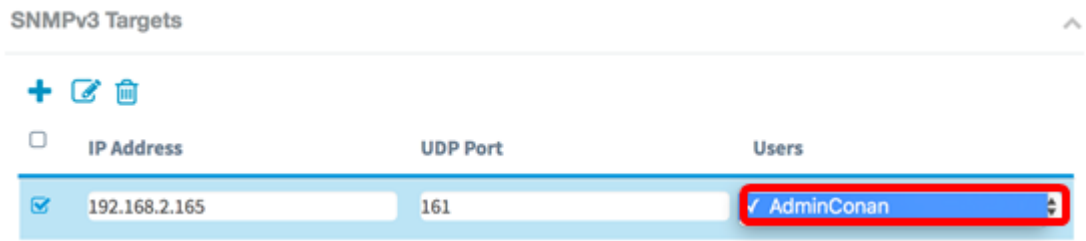
Remarque: Dans cet exemple, 192.168.2.165 est utilisé.

Étape 3. Introduisez un numéro de port de Protocole UDP (User Datagram Protocol) dans le domaine de *port UDP*. L'agent SNMP vérifie ce port pour des demandes d'accès. Le par défaut est 161. La plage valide est à partir de 1025 à 65535.

Remarque: Pour cet exemple, 161 est utilisés.

Étape 4. Choisissez l'utilisateur pour s'associer avec la cible de la liste déroulante d'utilisateurs. Cette liste affiche une liste de tous les utilisateurs créés à la page d'utilisateurs.

Remarque: AdminConan est choisi en tant qu'utilisateur.



Étape 5. Clic Save.

Vous devriez avoir maintenant avec succès configuré les cibles SNMPv3 sur le WAP125 et le WAP581.