Configurez les configurations de Protocole SNMP (Simple Network Management Protocol) sur un routeur de gamme RV34x

Objectif

Le Protocole SNMP (Simple Network Management Protocol) est utilisé pour la Gestion de réseau, le dépannage, et la maintenance. Le SNMP enregistre, des mémoires, et partage les informations avec l'aide du logiciel deux principal : un système d'administration de réseaux (NMS) ce fonctionne sur des périphériques de gestionnaire et un agent qui s'exécute sur des périphériques gérés. Le routeur de gamme RV34x prend en charge des versions 1, 2, et 3. SNMP.

SNMP v1 est la version originale du SNMP que les manques certaine fonctionnalité et travaille seulement aux réseaux TCP/IP, alors que SNMP v2 est une itération améliorée de v1. SNMP v1 et v2c devrait seulement être choisi pour les réseaux qui utilisent SNMPv1 ou SNMPv2C. SNMP v3 est le plus nouveau niveau du SNMP et aborde plusieurs des questions de SNMP v1 et v2c. En particulier, il adresse plusieurs des failles de la sécurité de v1 et de v2c. SNMP v3 permet également à des administrateurs pour se déplacer à une norme commune SNMP.

Cet article explique comment configurer des configurations SNMP sur le routeur de gamme RV34x.

Périphériques applicables

- Gamme RV34x

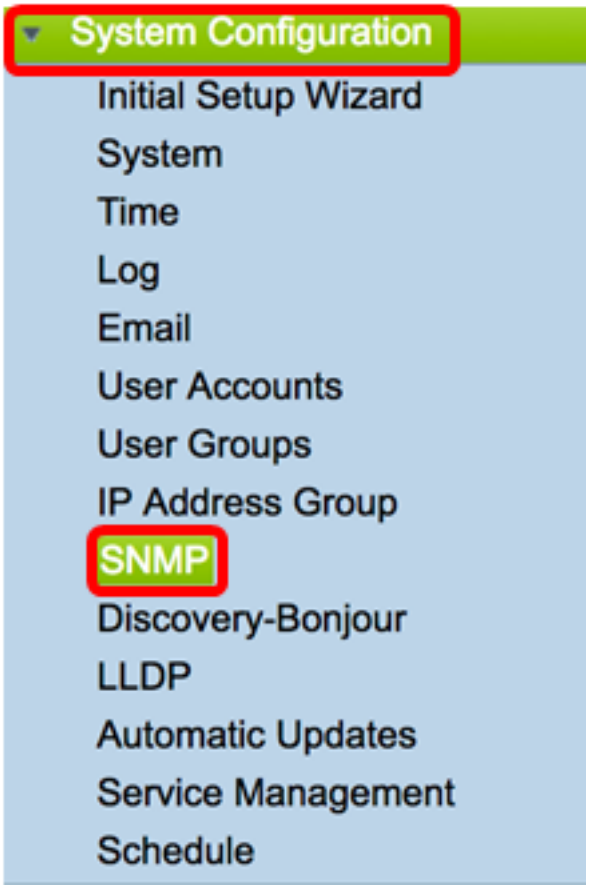
Version de logiciel

- 1.0.1.16

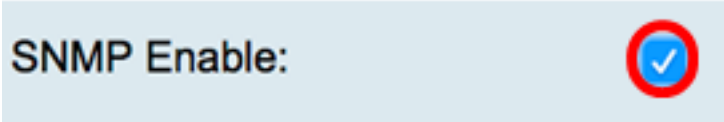
Configurez les configurations SNMP sur le routeur de gamme RV34x

Configurez les configurations SNMP

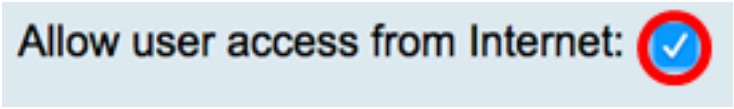
Étape 1. Ouvrez une session à l'utilitaire basé sur le WEB du routeur et choisissez la **configuration système > le SNMP**.



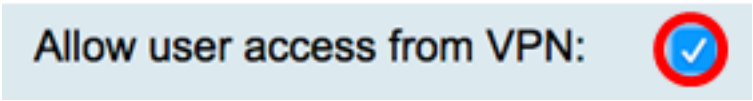
Étape 2. Cochez la case d'**enable SNMP** pour activer le SNMP.



Le contrôle (facultatif) d'étape 3. l'**enable permettent l'accès client de la** case d'**Internet** pour permettre l'accès client autorisé en dehors du réseau par des applications d'administration telles que la Gestion de réseau de Cisco FindIT.



Le contrôle (facultatif) d'étape 4. l'**accès client d'autoriser de la** case **VPN** à laisser a autorisé l'accès d'un VPN.

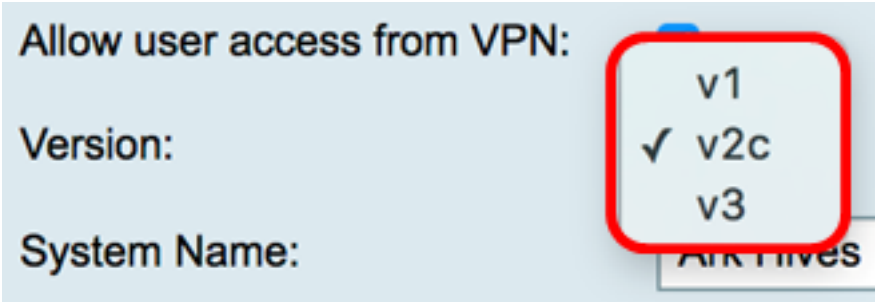


Étape 5. Du menu déroulant de version, choisissez une version SNMP pour l'utiliser sur le réseau. Les options sont :

- v1 — Mineurs ont sécurisé l'option. Utilise le plaintext pour des chaînes de la communauté.
- v2c — Le support amélioré de traitement des erreurs fourni par SNMPv2C inclut codes d'erreur développés qui distinguent différents types d'erreurs ; tous les types d'erreurs sont signalés par code d'erreur simple dans SNMPv1.
- v3 — SNMPv3 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

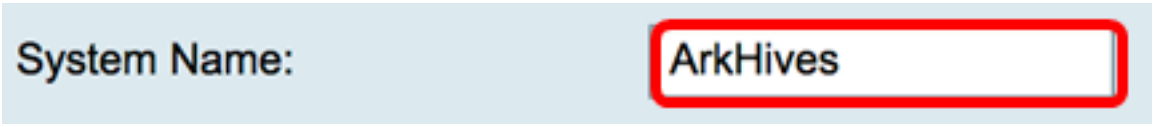
Sécurité est le niveau de sécurité permis dans un modèle de Sécurité. Une combinaison d'un modèle de Sécurité et d'un niveau de Sécurité détermine quel mécanisme de sécurité est utilisé en manipulant un paquet SNMP.

Remarque: Dans cet exemple, v2c est choisi.



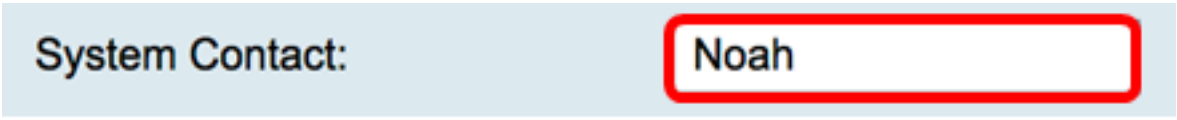
Étape 6. Dans le domaine de *nom de système*, écrivez un nom pour le routeur pour une identification plus facile dans les applications d'administration réseau.

Remarque: Dans cet exemple, ArkHives est utilisé comme nom de système.



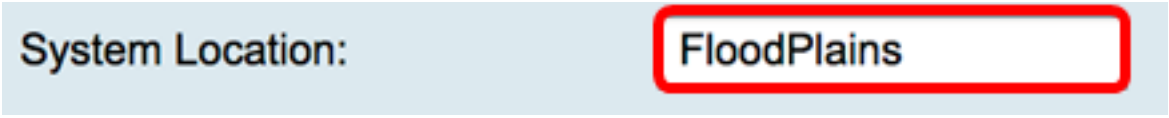
Étape 7. Dans le domaine de *personne-ressource du système*, écrivez un nom d'une personne ou d'un administrateur pour l'identifier avec le routeur en cas d'urgence.

Remarque: Pour cet exemple, Noé est utilisé en tant que personne-ressource du système.



Étape 8. Dans le *champ System Location*, entrez un emplacement du routeur. Ceci facilite localisant un problème beaucoup pour un administrateur.

Remarque: Pour cet exemple, des zones inondables est utilisés comme emplacement de système.



Pour procéder à la configuration, cliquez sur en fonction la version SNMP qui a été choisie dans l'étape 5.

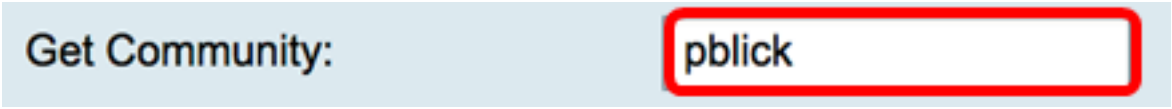
- Configurez SNMP 1 ou v2c
- Configurez SNMP v3

Configurez SNMP 1 ou v2c

Étape 1. Si SNMP v2c était choisi dans l'étape 5, écrivez le nom de communauté SNMP dans le domaine de la *Communauté d'obtenir*. Il crée la communauté à accès en lecture seule qui est utilisée pour accéder aux informations pour l'agent SNMP. La chaîne de la communauté introduite le paquet de demandes envoyé par l'expéditeur doit apparier la

chaîne de la communauté sur le périphérique d'agent. La chaîne par défaut pour en lecture seule est publique.

Remarque: Le mot de passe en lecture seule donne l'autorité pour récupérer les informations seulement. Dans cet exemple, le pblick est utilisé.



Étape 2. Dans le domaine de *set community*, écrivez un nom de communauté SNMP. Il crée la communauté en lecture/écriture qui est utilisée pour accéder aux informations pour l'agent SNMP. Demande seulement aux périphériques qui s'identifient avec ce nom de communauté sont reçus. C'est un nom créé par l'utilisateur. Le par défaut est privé.

Remarque: Il est recommandé de changer les les deux les mots de passe à quelque chose plus personnalisée afin d'éviter l'attaque de Sécurité à partir des étrangers. Dans cet exemple, le pribado est utilisé.

Vous devriez avoir maintenant avec succès configuré les configurations v1 ou v2 SNMP. Poursuivez à la région de configuration de déroutement.

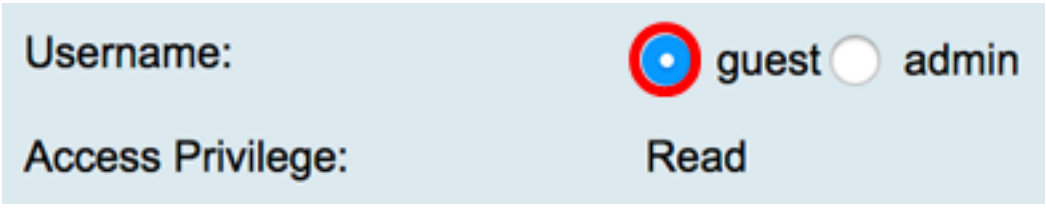
Configurez SNMP v3

Étape 1. Si SNMP v3 était choisi, cliquez sur une case d'option dans la région de nom d'utilisateur pour choisir un privilège d'accès. Les options sont :

- invité — Privilèges en lecture seule
- admin — Lisez et écrivez les privilèges

Remarque: Pour cet exemple, l'invité est choisi.

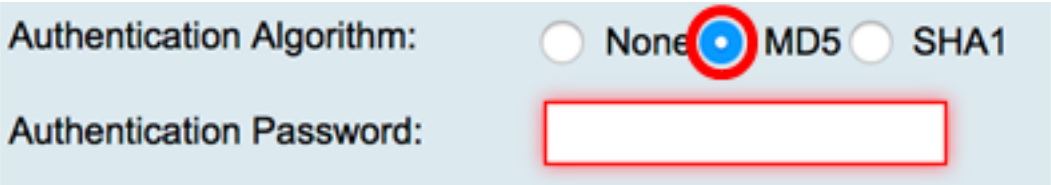
La région de privilège d'accès affiche le type de privilège selon la case d'option cliquée sur.



Étape 2. Cliquez sur une case d'option dans la région d'algorithme d'authentification pour choisir une méthode que l'agent SNMP l'utilisera pour authentifier. Les options sont :

- Aucun — Aucune authentification de l'utilisateur n'est utilisée.
- MD5 — L'algorithme 5 de message-digest utilise une valeur de hachage 128-bit pour l'authentification. Exige le nom d'utilisateur et mot de passe.
- SHA1 — Le Secure Hash Algorithm (SHA-1) est un algorithme de hachage à sens unique qui produit un condensé 160-bit. SHA-1 calcule plus lent que le MD5, mais est plus sécurisé que le MD5.

Remarque: Pour cet exemple, le MD5 est choisi.



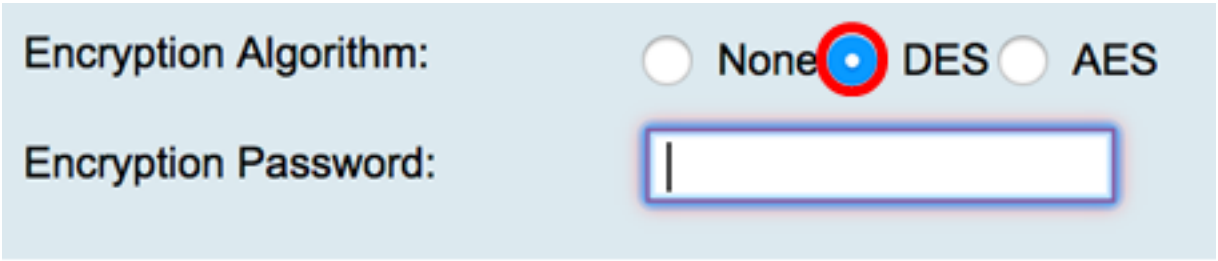
Remarque: Si vous n'en choisissiez aucun, ignorez à la région de configuration de déroutement.

Étape 3. Dans le domaine de *mot de passe d'authentification*, entrez un mot de passe.

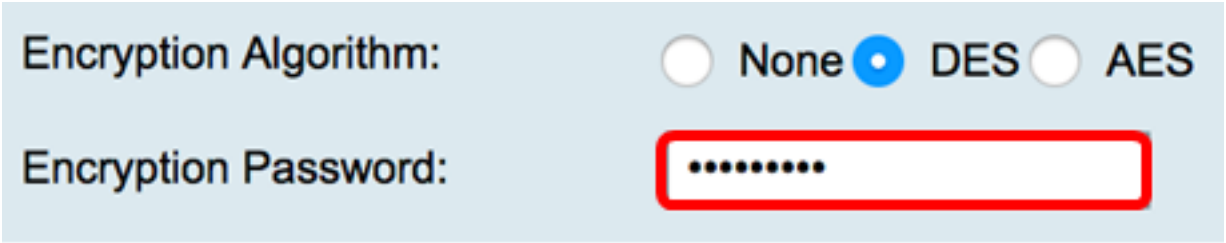
Étape 4. (facultative) dans la région d'algorithme de chiffrement, cliquent sur en fonction une case d'option pour choisir comment les informations SNMP seront chiffrées. Les options sont :

- Aucun — Aucun cryptage n'est utilisé. Si cette étape est choisie, ignorez à la région de configuration de déroutement.
- DES — Le Norme de chiffrement de données (DES) est une méthode de cryptage 56-bit qui n'est pas très sécurisée, mais peut être exigé pour ascendant la compatibilité.
- AES — Norme AES (Advanced Encryption Standard). Si ceci est choisi, un mot de passe de cryptage est exigé.

Remarque: Pour cet exemple, le DES est choisi.



Étape 5. (facultative) si le DES ou l'AES était choisi, entrent un mot de passe de cryptage dans le domaine de *mot de passe de cryptage*.

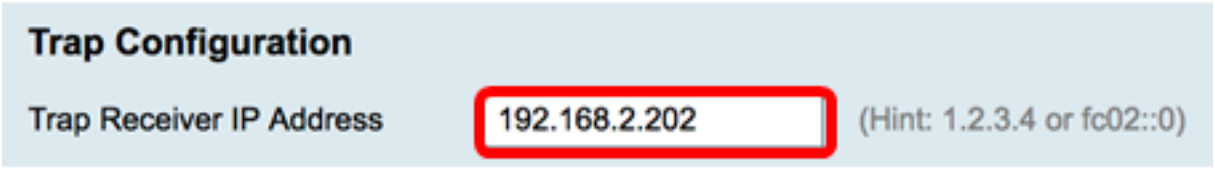


Vous devriez maintenant avoir avec succès pour configurer les configurations SNMP v3. Poursuivez maintenant à la région de configuration de déroutement.

Configuration de déroutement

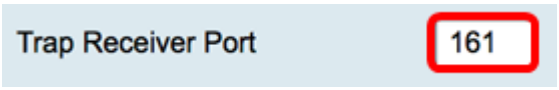
Étape 1. Dans le *champ IP Address de récepteur de déroutement*, écrivez un ipv4 ou une adresse IP d'IPv6 qui recevront les déroutements SNMP.

Remarque: Pour cet exemple, 192.168.2.202 est utilisé.

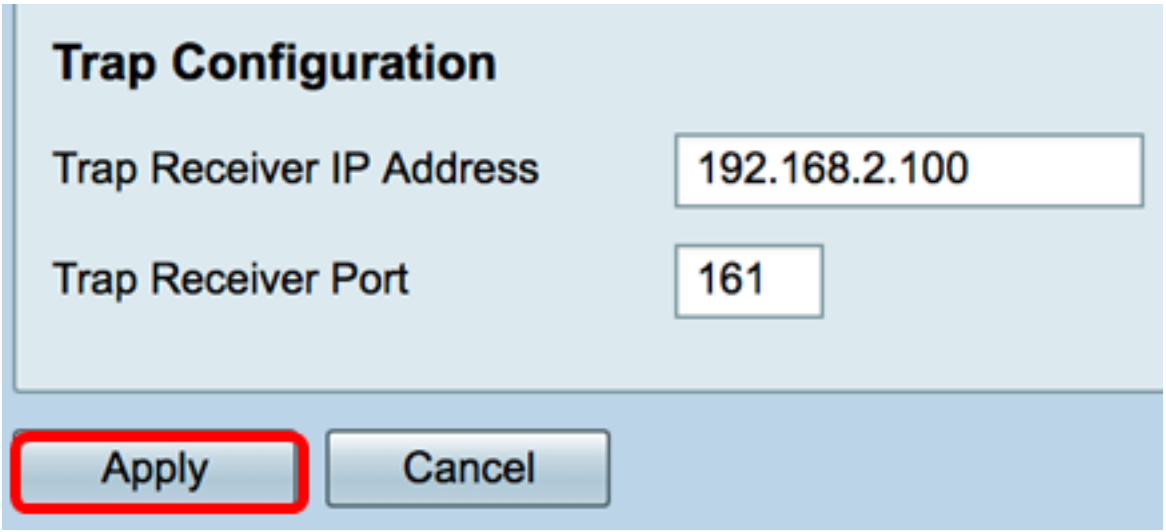


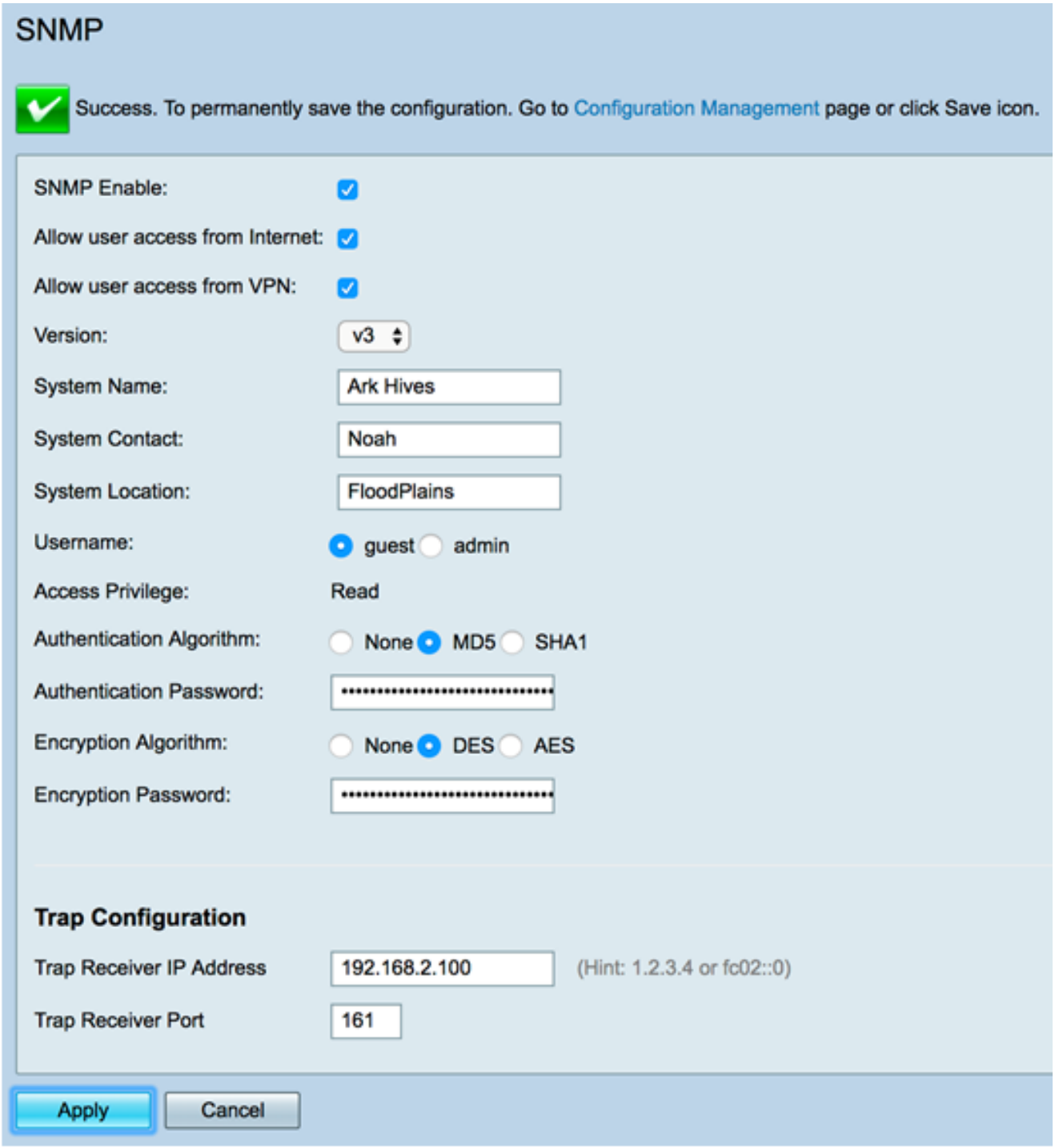
Étape 2. Introduisez un numéro de port de Protocole UDP (User Datagram Protocol) dans le domaine de *port de récepteur de déroutement*. L'agent SNMP vérifie ce port pour des demandes d'accès.

Remarque: Pour cet exemple, 161 est utilisés.



Étape 3. Cliquez sur Apply.





Étape 4. (facultative) pour sauvegarder la configuration de manière permanente, vont à la page de copie/save configuration ou cliquent sur 

l'icône à la partie supérieure de la page.

Vous devriez avoir maintenant avec succès configuré les configurations SNMP sur un routeur de gamme RV34x.