

# Configuration des paramètres SNMP (Simple Network Management Protocol) sur un routeur de la gamme RV34x

## Objectif

Le protocole SNMP (Simple Network Management Protocol) est utilisé pour la gestion, le dépannage et la maintenance du réseau. SNMP enregistre, stocke et partage des informations à l'aide de deux logiciels clés : un système de gestion de réseau (NMS) qui s'exécute sur des périphériques de gestion et un agent qui s'exécute sur des périphériques gérés. Le routeur de la gamme RV34x prend en charge SNMP versions 1, 2 et 3.

SNMP v1 est la version originale de SNMP qui ne dispose pas de certaines fonctionnalités et fonctionne uniquement sur les réseaux TCP/IP, tandis que SNMP v2 est une version améliorée de v1. Les protocoles SNMP v1 et v2c doivent être choisis uniquement pour les réseaux qui utilisent SNMPv1 ou SNMPv2c. SNMP v3 est la norme SNMP la plus récente et répond à de nombreux problèmes de SNMP v1 et v2c. En particulier, il répond à de nombreuses vulnérabilités de sécurité de v1 et v2c. SNMP v3 permet également aux administrateurs de passer à une norme SNMP commune.

Cet article explique comment configurer les paramètres SNMP sur le routeur de la gamme RV34x.

## Périphériques pertinents

- Gamme RV34x

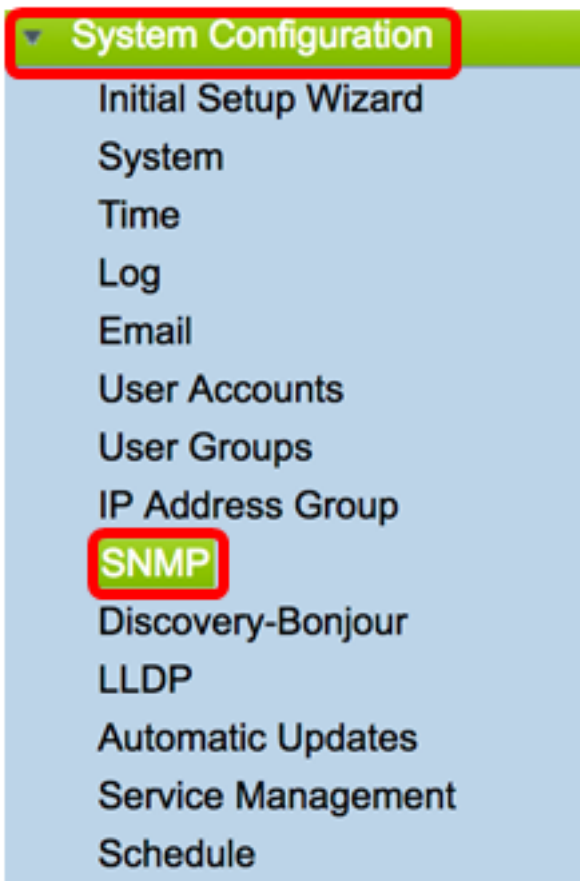
## Version du logiciel

- 1.0.1.16

## Configuration des paramètres SNMP sur le routeur de la gamme RV34x

### Configuration des paramètres SNMP

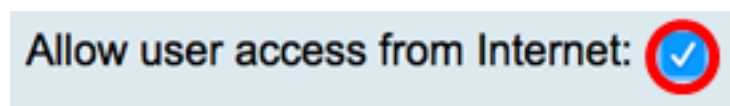
Étape 1. Connectez-vous à l'utilitaire Web du routeur et sélectionnez **Configuration système > SNMP**.



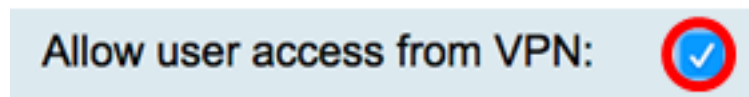
Étape 2. Cochez la case **SNMP Enable** pour activer SNMP.



Étape 3. (Facultatif) Cochez la case **Activer l'accès utilisateur à partir d'Internet** pour autoriser l'accès utilisateur autorisé en dehors du réseau via des applications de gestion telles que Cisco FindIT Network Management.



Étape 4. (Facultatif) Cochez la case **Autoriser l'accès utilisateur à partir d'un VPN** pour autoriser l'accès autorisé à partir d'un VPN.

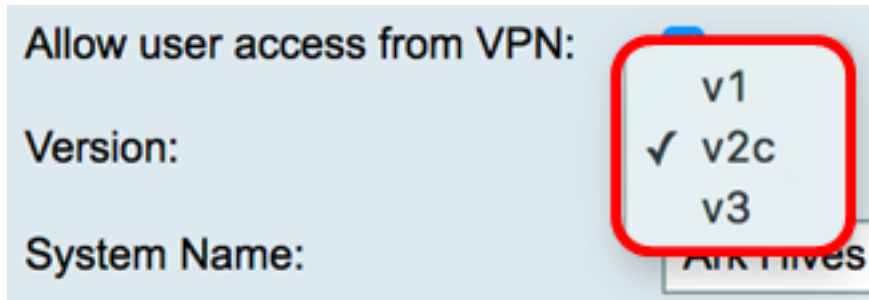


Étape 5. Dans le menu déroulant Version, sélectionnez une version SNMP à utiliser sur le réseau. Les options sont les suivantes :

- v1 - Option la moins sécurisée. Utilise du texte clair pour les chaînes de communauté.
- v2c - La prise en charge améliorée de la gestion des erreurs fournie par SNMPv2c inclut des codes d'erreur étendus qui distinguent différents types d'erreurs ; tous les types d'erreurs sont signalés via un code d'erreur unique dans SNMPv1.
- v3 - SNMPv3 est un modèle de sécurité dans lequel une stratégie d'authentification est configurée pour un utilisateur et le groupe dans lequel réside l'utilisateur. Le niveau de

sécurité est le niveau de sécurité autorisé 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 lors de la gestion d'un paquet SNMP.

**Note:** Dans cet exemple, v2c est sélectionné.



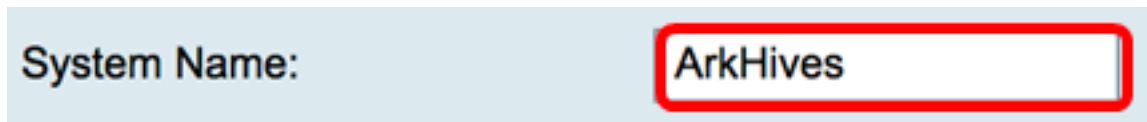
Allow user access from VPN:

Version: v1  
✓ v2c  
v3

System Name: ArkHives

Étape 6. Dans le champ *Nom du système*, saisissez un nom pour le routeur afin de faciliter son identification dans les applications de gestion de réseau.

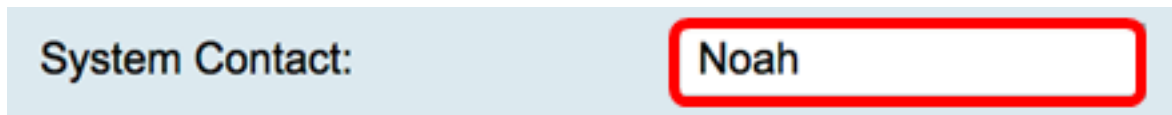
**Note:** Dans cet exemple, ArkHives est utilisé comme nom système.



System Name: ArkHives

Étape 7. Dans le champ *Contact système*, saisissez le nom d'une personne ou d'un administrateur à identifier avec le routeur en cas d'urgence.

**Note:** Dans cet exemple, Noah est utilisé comme contact système.



System Contact: Noah

Étape 8. Dans le champ *Emplacement du système*, saisissez l'emplacement du routeur. Cela facilite la recherche d'un problème pour un administrateur.

**Note:** Dans cet exemple, FloodPlains est utilisé comme emplacement système.



System Location: FloodPlains

Pour poursuivre la configuration, cliquez sur la version SNMP choisie à l'étape 5.

- [Configurer SNMP 1 ou v2c](#)
- [Configuration de SNMP v3](#)

### [Configurer SNMP 1 ou v2c](#)

Étape 1. Si SNMP v2c a été sélectionné à l'étape 5, saisissez le nom de la communauté SNMP dans le champ *Get Community*. Il crée une communauté en lecture seule qui est utilisée pour accéder aux informations de l'agent SNMP. La chaîne de communauté envoyée dans le paquet de requête envoyé par l'expéditeur doit correspondre à la chaîne de communauté sur le périphérique de l'agent. La chaîne par défaut pour la lecture seule est publique.

**Note:** Le mot de passe en lecture seule autorise la récupération des informations uniquement. Dans cet exemple, le bouton est utilisé.

Get Community:

pblick

Étape 2. Dans le champ *Set Community*, saisissez un nom de communauté SNMP. Il crée une communauté en lecture-écriture qui est utilisée pour accéder aux informations de l'agent SNMP. Seules les demandes des périphériques qui s'identifient avec ce nom de communauté sont acceptées. Il s'agit d'un nom créé par l'utilisateur. La valeur par défaut est private.

**Note:** Il est conseillé de changer les deux mots de passe en quelque chose de plus personnalisé afin d'éviter les attaques de sécurité de la part d'étrangers. Dans cet exemple, pribado est utilisé.

Set Community:

pribado

Vous devez maintenant avoir correctement configuré les paramètres SNMP v1 ou v2. Passez à la zone [Configuration des interruptions](#).

### Configuration de SNMP v3

Étape 1. Si SNMP v3 a été sélectionné, cliquez sur une case d'option dans la zone Nom d'utilisateur pour choisir un privilège d'accès. Les options sont les suivantes :

- guest : privilèges en lecture seule
- admin : privilèges de lecture et d'écriture

**Note:** Dans cet exemple, guest est sélectionné.

La zone Privilège d'accès affiche le type de privilège en fonction du bouton d'option cliqué.

Username:

guest  admin

Access Privilege:

Read

Étape 2. Cliquez sur une case d'option dans la zone Authentication Algorithm (Algorithme d'authentification) pour choisir une méthode que l'agent SNMP utilisera pour s'authentifier. Les options sont les suivantes :

- Aucun : aucune authentification utilisateur n'est utilisée.
- MD5 — Message-Digest Algorithm 5 utilise une valeur de hachage de 128 bits pour l'authentification. Nécessite le nom d'utilisateur et le mot de passe.
- SHA1 — SHA-1 (Secure Hash Algorithm) est un algorithme de hachage unidirectionnel qui produit un résumé de 160 bits. SHA-1 calcule plus lentement que MD5, mais est plus sécurisé que MD5.

**Note:** Dans cet exemple, MD5 est sélectionné.

Authentication Algorithm:  None  MD5  SHA1

Authentication Password:

**Note:** Si vous avez sélectionné Aucun, passez à la zone [Configuration des interruptions](#).

Étape 3. Dans le champ *Mot de passe d'authentification*, saisissez un mot de passe.

Authentication Algorithm:  None  MD5  SHA1

Authentication Password:

Étape 4. (Facultatif) Dans la zone Encryption Algorithm (Algorithme de chiffrement), cliquez sur une case d'option pour choisir le mode de cryptage des informations SNMP. Les options sont les suivantes :

- Aucun : aucun chiffrement n'est utilisé. Si cette étape est sélectionnée, passez à la zone [Configuration des interruptions](#).
- DES - Data Encryption Standard (DES) est une méthode de cryptage 56 bits qui n'est pas très sécurisée, mais qui peut être requise pour la compatibilité descendante.
- AES - Advanced Encryption Standard (AES). Si cette option est sélectionnée, un mot de passe de chiffrement est requis.

**Note:** Dans cet exemple, DES est sélectionné.

Encryption Algorithm:  None  DES  AES

Encryption Password:

Étape 5. (Facultatif) Si DES ou AES a été sélectionné, saisissez un mot de passe de chiffrement dans le champ *Mot de passe de chiffrement*.

Encryption Algorithm:  None  DES  AES

Encryption Password:

Vous devez maintenant configurer correctement les paramètres SNMP v3. Passez maintenant à la zone [Configuration des interruptions](#).

## [Configuration du dé routement](#)

Étape 1. Dans le champ *Adresse IP du récepteur de dé routement*, saisissez une adresse IPv4 ou IPv6 qui recevra les dé routements SNMP.

**Note:** Pour cet exemple, 192.168.2.202 est utilisé.

**Trap Configuration**

Trap Receiver IP Address  (Hint: 1.2.3.4 or fc02::0)

Étape 2. Entrez un numéro de port UDP (User Datagram Protocol) dans le champ *Port du récepteur de déroutement*. L'agent SNMP recherche les demandes d'accès sur ce port.

**Note:** Dans cet exemple, 161 est utilisé.

Trap Receiver Port

Étape 3. Cliquez sur Apply.

**Trap Configuration**

Trap Receiver IP Address

Trap Receiver Port

## SNMP



Success. To permanently save the configuration. Go to [Configuration Management](#) page or click Save icon.

SNMP Enable:	<input checked="" type="checkbox"/>
Allow user access from Internet:	<input checked="" type="checkbox"/>
Allow user access from VPN:	<input checked="" type="checkbox"/>
Version:	v3
System Name:	Ark Hives
System Contact:	Noah
System Location:	FloodPlains
Username:	<input checked="" type="radio"/> guest <input type="radio"/> admin
Access Privilege:	Read
Authentication Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> MD5 <input type="radio"/> SHA1
Authentication Password:	.....
Encryption Algorithm:	<input type="radio"/> None <input checked="" type="radio"/> DES <input type="radio"/> AES
Encryption Password:	.....

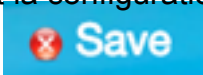
### Trap Configuration

Trap Receiver IP Address	192.168.2.100	(Hint: 1.2.3.4 or fc02::0)
Trap Receiver Port	161	

Apply

Cancel

Étape 4. (Facultatif) Pour enregistrer définitivement la configuration, accédez à la page

Copier/Enregistrer la configuration ou cliquez sur l'  icône située dans la partie supérieure de la page.

Vous devez maintenant avoir correctement configuré les paramètres SNMP sur un routeur de la gamme RV34x.