

Configuration du protocole SNMP (Simple Network Management Protocol) sur les routeurs VPN RV320 et RV325

Objectif

Le protocole SNMP (Simple Network Management Protocol) est un protocole de couche application utilisé pour gérer et surveiller le trafic réseau. Le protocole SNMP conserve tous les enregistrements d'activité des différents périphériques du réseau afin de vous aider à trouver rapidement la source des problèmes sur le réseau, le cas échéant. Dans la gamme de routeurs VPN RV32x, vous pouvez activer SNMPv1/v2c, SNMPv3 ou les deux simultanément pour obtenir les performances souhaitées du réseau.

L'objectif de ce document est d'expliquer comment configurer SNMP sur la gamme de routeurs VPN RV32x.

Périphérique applicable

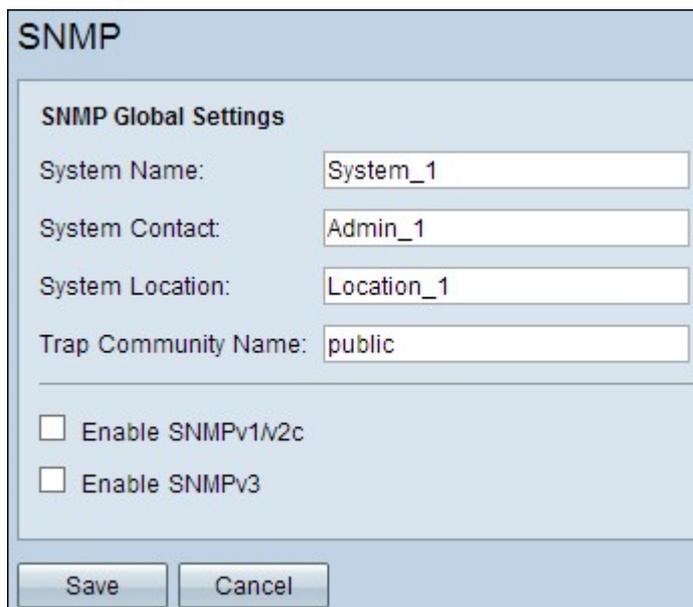
Routeur VPN double WAN · RV320
Routeur VPN double WAN Gigabit · RV325

Version du logiciel

•v 1.1.0.09

Configuration SNMP

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **System Management > SNMP**. La page *SNMP* s'ouvre :



SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Étape 2. Entrez le nom d'hôte dans le champ *Nom du système*.

Étape 3. Entrez le nom ou les informations de contact de la personne responsable du routeur dans le champ *Contact système*.

Étape 4. Entrez l'emplacement physique du routeur dans le champ *Emplacement du système*.

Note: Les informations entrées dans les champs *Contact système* et *Emplacement système* ne modifient pas le comportement du périphérique. Vous pouvez les saisir comme vous le souhaitez pour mieux gérer vos périphériques (par exemple, il peut être souhaitable d'inclure un numéro de téléphone dans le champ *Contact système*).

Étape 5. Entrez le nom de communauté de déROUTement auquel l'agent appartient dans le champ *Nom de communauté de déROUTement*. Un déROUTement est un message envoyé par le périphérique lorsqu'un événement spécifique se produit. Le nom de la communauté de déROUTement peut comporter jusqu'à 64 caractères alphanumériques. Le nom de communauté de déROUTement par défaut est *public*.

Étape 6. Cliquez sur **Save** pour enregistrer les paramètres.

Configuration SNMPv1/SNMPv2c

SNMPv1 est la première version du protocole SNMP et est désormais considéré comme non sécurisé. SNMPv2c est une version améliorée de SNMP. Il offre davantage de sécurité que SNMPv1 et améliore la gestion des erreurs.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

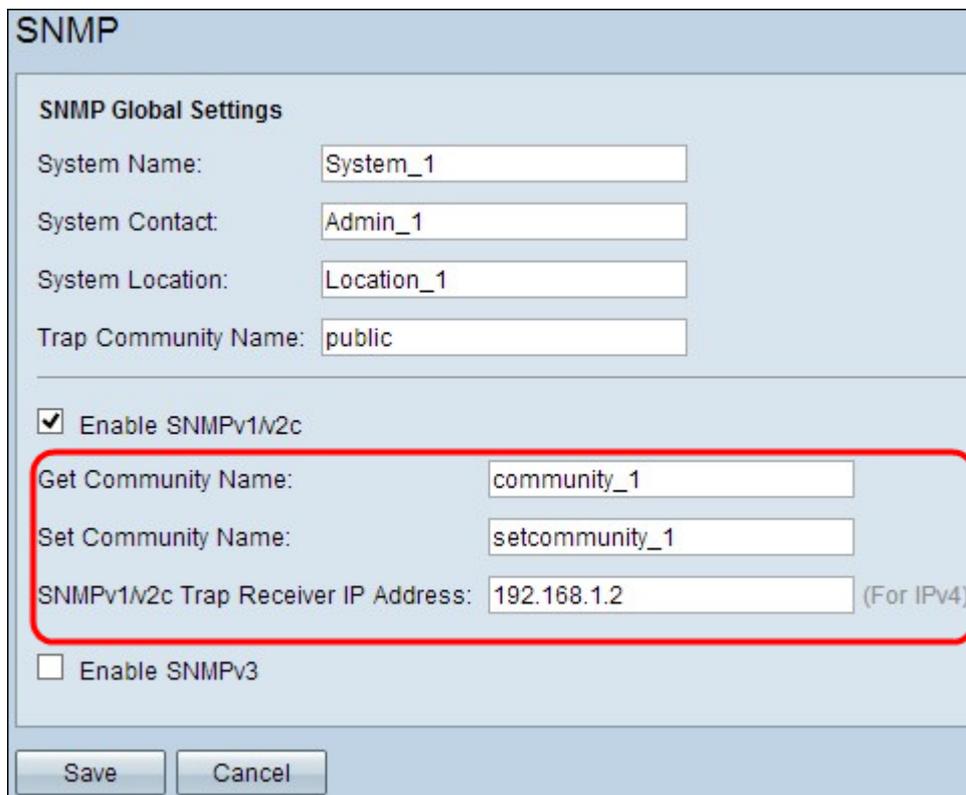
Get Community Name:

Set Community Name:

SNMPv1/v2c Trap Receiver IP Address: (For IPv4)

Enable SNMPv3

Étape 1. Cochez **Enable SNMPv1/v2c** pour activer SNMPv1/2c.

The image shows a configuration window titled "SNMP". It is divided into two main sections. The top section, "SNMP Global Settings", contains four text input fields: "System Name" (System_1), "System Contact" (Admin_1), "System Location" (Location_1), and "Trap Community Name" (public). The bottom section contains two checkboxes: "Enable SNMPv1/v2c" (checked) and "Enable SNMPv3" (unchecked). Below the "Enable SNMPv1/v2c" checkbox, there are three text input fields: "Get Community Name" (community_1), "Set Community Name" (setcommunity_1), and "SNMPv1/v2c Trap Receiver IP Address" (192.168.1.2) with a "(For IPv4)" label. A red rectangular box highlights these three fields. At the bottom of the window are "Save" and "Cancel" buttons.

Étape 2. Entrez un nom de communauté dans le champ *Get Community Name*. Get Community Name est la chaîne de communauté en lecture seule permettant d'authentifier la commande SNMP Get. La commande Get permet de récupérer les informations à partir du périphérique SNMP. Le nom de communauté Get peut comporter jusqu'à 64 caractères alphanumériques. Le nom de communauté Get par défaut est *public*.

Étape 3. Entrez un nom de communauté dans le champ *Définir un nom de communauté*. Il s'agit de la chaîne de communauté accessible en lecture/écriture pour authentifier la commande SNMP Set. La commande Set permet de modifier ou de définir les variables du périphérique. Le nom de communauté défini peut comporter jusqu'à 64 caractères alphanumériques. Le nom de communauté défini par défaut est *privé*.

Étape 4. Entrez l'adresse IP ou le nom de domaine du serveur spécifique sur lequel le logiciel de gestion SNMP s'exécute dans le champ *Adresse IP du récepteur de déroulement SNMPv1/v2c*. Un message de déroulement est envoyé à l'administrateur à partir du serveur pour l'avertir de toute erreur ou erreur.

Étape 5. Cliquez sur **Save** pour enregistrer les paramètres.

Configuration SNMPv3

SNMPv3 est la dernière version du protocole SNMP et offre le plus haut niveau de sécurité parmi les trois versions du protocole SNMP. Il fournit également une configuration à distance.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

Group Name	Security	Access MIBs
0 results found!		

User Table

Enable	User Name	Authentication	Privacy	Group
0 results found!				

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Étape 1. Cochez **Enable SNMPv3** pour activer SNMPv3.

Gestion de groupe SNMPv3

La gestion de groupe SNMPv3 vous permet de créer des groupes avec différents niveaux d'accès au périphérique. Vous pouvez ensuite mapper les utilisateurs dans ces groupes selon vos besoins.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

Group Name	Security	Access MIBs
0 results found!		
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>

User Table

Enable	User Name	Authentication	Privacy	Group
0 results found!				
<input type="button" value="Add"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>		

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Étape 1. Cliquez sur **Add** dans la table Group pour ajouter un nouveau groupe dans la table SNMPv3 Group Management. La page *SNMPv3 Group Management* s'ouvre :

SNMP

SNMPv3 Group Management

Group Name:

Group1

Security Level:

No Authentication, No Privacy

MIBs

- | | | |
|---|--|------------------------------------|
| <input type="checkbox"/> 1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.2 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.3 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.4 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.5 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.6 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.7 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.8 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.10 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.11 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.31 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.47 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.48 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.49 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.50 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.2.1.88 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.4.1 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |
| <input type="checkbox"/> 1.3.6.1.6.3 | <input checked="" type="radio"/> Read Only | <input type="radio"/> Read / Write |

Étape 2. Entrez le nom du groupe dans le champ *Nom du groupe*.

SNMP

SNMPv3 Group Management

Group Name:

Group1

Security Level:

No Authentication, No Privacy

No Authentication, No Privacy

Authentication, No Privacy

Authentication, Privacy

MIBs

1

1.3.6.1.2.1

Read Only

Read / Write

1.3.6.1.2.1.1

Read Only

Read / Write

1.3.6.1.2.1.2

Read Only

Read / Write

1.3.6.1.2.1.3

Read Only

Read / Write

1.3.6.1.2.1.4

Read Only

Read / Write

1.3.6.1.2.1.5

Read Only

Read / Write

1.3.6.1.2.1.6

Read Only

Read / Write

1.3.6.1.2.1.7

Read Only

Read / Write

1.3.6.1.2.1.8

Read Only

Read / Write

1.3.6.1.2.1.10

Read Only

Read / Write

1.3.6.1.2.1.11

Read Only

Read / Write

1.3.6.1.2.1.31

Read Only

Read / Write

1.3.6.1.2.1.47

Read Only

Read / Write

1.3.6.1.2.1.48

Read Only

Read / Write

1.3.6.1.2.1.49

Read Only

Read / Write

1.3.6.1.2.1.50

Read Only

Read / Write

1.3.6.1.2.1.88

Read Only

Read / Write

1.3.6.1.4.1

Read Only

Read / Write

1.3.6.1.6.3

Read Only

Read / Write

Étape 3. Choisissez le type de sécurité dans la liste déroulante *Niveau de sécurité*. Les types de sécurité sont décrits comme suit :

- No Authentication, No Privacy : les utilisateurs de ce groupe ne seront pas tenus de définir un mot de passe d'authentification ou un mot de passe de confidentialité. Les messages ne seront pas chiffrés et les utilisateurs ne seront pas authentifiés

·Authentication, No Privacy : les utilisateurs doivent définir un mot de passe d'authentification, mais pas un mot de passe de confidentialité. Les utilisateurs seront authentifiés lors de la réception des messages, mais ceux-ci ne seront pas chiffrés.

·Authentication Privacy : les utilisateurs doivent définir à la fois un mot de passe d'authentification et un mot de passe de confidentialité. Les utilisateurs seront authentifiés lors de la réception des messages. Les messages seront également chiffrés à l'aide du mot de passe de confidentialité.

SNMP

SNMPv3 Group Management

Group Name:

Security Level: ▼

MIBs

<input type="checkbox"/> 1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.2	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.3	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.4	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.5	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input checked="" type="checkbox"/> 1.3.6.1.2.1.6	<input type="radio"/> Read Only	<input checked="" type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.7	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.8	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.10	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.11	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.31	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.47	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.48	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.49	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.50	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.2.1.88	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.4.1	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write
<input type="checkbox"/> 1.3.6.1.6.3	<input checked="" type="radio"/> Read Only	<input type="radio"/> Read / Write

Étape 4. Activez les cases à cocher pour sélectionner la base MIB (Management Information Base) spécifique à laquelle vous souhaitez que le groupe ait accès. Les MIB sont utilisées pour définir les informations nécessaires du système géré. Il est représenté par iso.org.dod.internet.mgmt.mib. En définissant des MIB spécifiques, vous pouvez autoriser des groupes à accéder à différentes parties du périphérique.

Étape 5. Cliquez sur la case d'option spécifique pour chaque MIB cochée pour choisir le niveau d'autorisation disponible pour le groupe. Les niveaux d'autorisation sont définis comme suit :

·Lecture seule : les utilisateurs de ce groupe pourront lire à partir de la base MIB, mais ne la modifieront pas.

·Lecture/Écriture : les utilisateurs de ce groupe pourront lire à la fois à partir de la base MIB et la modifier.

Étape 6. Faites défiler la page vers le bas et cliquez sur **Enregistrer** pour enregistrer les paramètres. Ceci ajoute le groupe à la table de groupe.

The screenshot shows the SNMP configuration page. Under 'SNMP Global Settings', there are input fields for System Name (System_1), System Contact (Admin_1), System Location (Location_1), and Trap Community Name (public). There are checkboxes for 'Enable SNMPv1/v2c' (unchecked) and 'Enable SNMPv3' (checked). Below is the 'Group Table' with one group: 'Group1' with security 'Authentication,Privacy' and access MIBs 1.3.6.1.2.1[W], 1.3.6.1.2.1.1[R], 1.3.6.1.2.1.4[W], 1.3.6.1.2.1.5[R], and 1.3.6.1.2.1.6[W]. The 'Edit' button is circled in red. Below is the 'User Table' with 0 results found and buttons for Add, Edit, and Delete. At the bottom, there are fields for 'SNMPv3 Trap Receiver IP Address' and 'SNMPv3 Trap Receiver User' (set to 'No User').

Étape 7. (Facultatif) Si vous souhaitez modifier le groupe configuré, cliquez sur la case d'option du groupe souhaité, puis cliquez sur **Modifier** et modifiez le ou les champs respectifs.

Étape 8. (Facultatif) Pour supprimer le groupe configuré, cliquez sur la case d'option souhaitée du groupe, puis cliquez sur **Supprimer**.

Gestion des utilisateurs SNMPv3

Les utilisateurs SNMP sont les utilisateurs distants pour lesquels les services SNMP sont exécutés.

Remarque : vous devez ajouter un groupe à la table de groupe avant de pouvoir ajouter un utilisateur dans la table d'utilisateurs.

SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Group Table

	Group Name	Security	Access MIBs
<input type="radio"/>	Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]

User Table

	Enable	User Name	Authentication	Privacy
0 results found!				

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Étape 1. Cliquez sur **Ajouter** dans la table des utilisateurs pour ajouter un nouvel utilisateur dans la table de gestion des utilisateurs SNMPv3. La page *SNMPv3 User Management* s'ouvre :

SNMP

SNMPv3 User Management

Enable :

User Name:

Group:

Authentication Method: MD5 SHA None Authentication Password:

Privacy Method: DES AES None Privacy Password:

Étape 2. Cochez **Enable** pour activer la gestion utilisateur pour SNMP.

Étape 3. Entrez un nom d'utilisateur dans le champ *Nom d'utilisateur*.

Étape 4. Choisissez le groupe souhaité dans la liste déroulante *Groupe*. Le nouvel utilisateur est ajouté à ce groupe spécifique.

Étape 5. Cliquez sur la case d'option spécifique pour choisir une méthode d'authentification. Les méthodes d'authentification sont décrites comme suit :

- MD5 — Message Digest Algorithm-5 (MD5) est une fonction de hachage hexadécimal à 32 chiffres.
- SHA — Secure Hash Algorithm (SHA) est une fonction de hachage de 160 bits considérée comme plus sécurisée que MD5.

Étape 6. Entrez un mot de passe pour l'authentification dans le champ *Mot de passe d'authentification*. Le mot de passe d'authentification est le mot de passe qui est partagé à l'avance entre les périphériques. Lorsqu'ils échangent du trafic, ils utilisent le mot de passe spécifique pour authentifier le trafic.

Étape 7. Cliquez sur la case d'option spécifique pour choisir la méthode de chiffrement souhaitée dans le champ *Privacy Method*.

- DES : Data Encryption Standard (DES) est une méthode de cryptage 56 bits. Il est considéré comme non sécurisé, mais peut être nécessaire lorsque le périphérique est utilisé conjointement avec d'autres périphériques qui ne prennent pas en charge AES.
- AES - Advanced Encryption Standard (AES) utilise une méthode de cryptage 128 bits, 192 bits ou 256 bits. Il est considéré comme plus sûr que DES.

Étape 8. Entrez un mot de passe pour la confidentialité dans le champ *Privacy Password*. Le mot de passe de confidentialité est le mot de passe utilisé pour chiffrer les messages.

Étape 9. Cliquez sur **Save pour enregistrer les paramètres**. L'utilisateur est ajouté à la table des utilisateurs.

The screenshot shows the configuration interface for SNMPv3. At the top, there is a checkbox labeled "Enable SNMPv3" which is checked. Below this is the "Group Table" section, which contains a table with columns for Group Name, Security, and Access MIBs. The table has one row for "Group1" with Security set to "Authentication,Privacy" and Access MIBs listed as 1.3.6.1.2.1[W], 1.3.6.1.2.1.1[R], 1.3.6.1.2.1.4[W], 1.3.6.1.2.1.5[R], and 1.3.6.1.2.1.6[W]. Below the table are "Add", "Edit", and "Delete" buttons. The "User Table" section is below, with columns for Enable, User Name, Authentication, Privacy, and Group. The first row is highlighted with a red circle and contains: Enable (checked), User Name "USER1", Authentication "SHA", Privacy "AES", and Group "Group1". Below the table are "Add", "Edit", and "Delete" buttons. At the bottom, there are two input fields: "SNMPv3 Trap Receiver IP Address:" with a text box and "(For IPv4)" label, and "SNMPv3 Trap Receiver User:" with a dropdown menu showing "USER1".

Enable SNMPv3

Group Table			
Group Name	Security	Access MIBs	
<input type="radio"/> Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]	

Add Edit Delete

User Table				
Enable	User Name	Authentication	Privacy	Group
<input checked="" type="radio"/>	USER1	SHA	AES	Group1

Add Edit Delete

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Save Cancel

Étape 10. (Facultatif) Pour modifier l'utilisateur configuré, cliquez sur la case d'option de l'utilisateur souhaité, puis cliquez sur **Modifier** et modifiez le champ correspondant.

Étape 11. (Facultatif) Pour supprimer l'utilisateur configuré, cliquez sur la case d'option de l'utilisateur souhaité, puis cliquez sur **Supprimer**.

Enable SNMPv1v2c

Get Community Name:

Set Community Name:

SNMPv1v2c Trap Receiver IP Address: (For IPv4)

Enable SNMPv3

Group Table			
Group Name	Security	Access MIBs	
<input type="radio"/> Group1	Authentication,Privacy	1.3.6.1.2.1[W] 1.3.6.1.2.1.1[R] 1.3.6.1.2.1.4[W] 1.3.6.1.2.1.5[R] 1.3.6.1.2.1.6[W]	

Add Edit Delete

User Table					
Enable	User Name	Authentication	Privacy	Group	
<input type="radio"/>	<input checked="" type="checkbox"/>	USER1	SHA	AES	Group1

Add Edit Delete

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Save Cancel

Étape 12. Entrez l'adresse IP du récepteur d'interruptions SNMPv3 dans le champ *Adresse IP du récepteur d'interruptions SNMPv3*.

Étape 13. Choisissez l'utilisateur de déroulement respectif dans la liste déroulante *SNMPv3 Trap Receiver User*. Il s'agit de l'utilisateur qui reçoit le message de déroulement lorsqu'un événement de déroulement se produit.

Étape 14. Cliquez sur **Save** pour enregistrer les paramètres.