

Konfigurieren des Simple Network Management Protocol (SNMP) auf RV320- und RV325-VPN-Routern

Ziel

Simple Network Management Protocol (SNMP) ist ein Protokoll auf Anwendungsebene, das zur Verwaltung und Überwachung des Netzwerkverkehrs verwendet wird. SNMP speichert alle Aktivitätsprotokolle verschiedener Geräte im Netzwerk, damit Sie bei Bedarf schnell die Ursache von Problemen im Netzwerk finden können. In der RV32x VPN Router-Serie können Sie SNMPv1/v2c, SNMPv3 oder beide gleichzeitig aktivieren, um die gewünschte Netzwerkleistung zu erzielen.

In diesem Dokument wird erläutert, wie SNMP auf den RV32x VPN-Routern der Serie RV32x konfiguriert wird.

Anwendbares Gerät

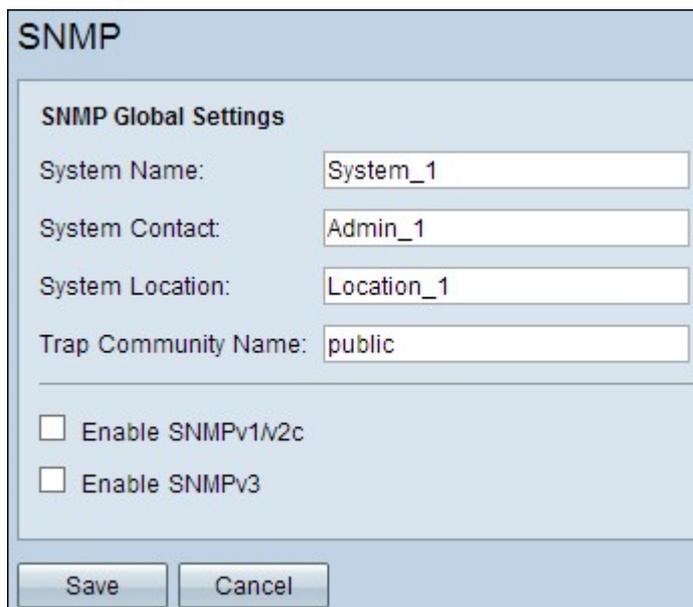
- RV320 Dual-WAN VPN-Router
- RV325 Gigabit Dual-WAN VPN-Router

Softwareversion

- v1.1.0.09

SNMP-Konfiguration

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Systemverwaltung > SNMP** aus. Die Seite *SNMP* wird geöffnet:



SNMP

SNMP Global Settings

System Name:

System Contact:

System Location:

Trap Community Name:

Enable SNMPv1/v2c

Enable SNMPv3

Schritt 2: Geben Sie den Hostnamen im Feld *Systemname* ein.

Schritt 3: Geben Sie im Feld *Systemkontakt* den Namen oder die Kontaktinformationen der für den Router zuständigen Person ein.

Schritt 4: Geben Sie im Feld *Systemstandort* den physischen Standort des Routers ein.

Hinweis: Die in die Felder *Systemkontakt* und *Systemstandort* eingegebenen Informationen ändern das Verhalten des Geräts nicht. Sie können diese nach Wunsch eingeben, um die Geräte optimal zu verwalten (es ist beispielsweise ratsam, im Feld *Systemkontakt* eine Telefonnummer einzugeben).

Schritt 5: Geben Sie den Namen der Trap-Community ein, zu dem der Agent im Feld *Trap Community Name* gehört. Ein Trap ist eine Nachricht, die vom Gerät gesendet wird, wenn ein bestimmtes Ereignis auftritt. Der Name der Trap-Community kann bis zu 64 alphanumerische Zeichen enthalten. Der Standardname der Trap-Community ist *public*.

Schritt 6: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SNMPv1/SNMPv2c-Konfiguration

SNMPv1 ist die erste SNMP-Version und gilt jetzt als unsicher. SNMPv2c ist eine verbesserte Version von SNMP. Es bietet mehr Sicherheit als SNMPv1 und verbesserte Fehlerbehandlung.

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

Schritt 1: Aktivieren Sie **SNMPv1/v2c aktivieren**, um SNMPv1/2c zu aktivieren.

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

Schritt 2: Geben Sie im Feld *Get Community Name* einen Community-Namen ein. Get Community Name ist der schreibgeschützte Community-String, der den SNMP Get-Befehl authentifiziert. Mit dem Befehl Get werden die Informationen vom SNMP-Gerät abgerufen. Der Get-Community-Name kann bis zu 64 alphanumerische Zeichen enthalten. Der Standardname Get-Community ist *öffentlich*.

Schritt 3: Geben Sie im Feld *Community-Namen festlegen* einen Community-Namen ein. Es ist der Read/Write Community String, der den SNMP Set-Befehl authentifiziert. Mit dem Befehl Festlegen werden die Variablen auf dem Gerät geändert oder festgelegt. Der Community-Name festlegen kann bis zu 64 alphanumerische Zeichen enthalten. Der Standardname Set Community Name ist *private*.

Schritt 4: Geben Sie die IP-Adresse oder den Domännennamen des spezifischen Servers ein, auf dem die SNMP-Managementsoftware im Feld *IP-Adresse des SNMPv1/v2c Trap Receivers* ausgeführt wird. Eine Trap-Meldung wird vom Server an den Administrator gesendet, um den Administrator zu benachrichtigen, wenn ein Fehler oder Fehler auftritt.

Schritt 5: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

SNMPv3-Konfiguration

SNMPv3 ist die neueste Version von SNMP und bietet die höchste Sicherheitsstufe unter den drei SNMP-Versionen. Es bietet auch Remote-Konfiguration.

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:

Schritt 1: Aktivieren Sie **SNMPv3 aktivieren**, um SNMPv3 zu aktivieren.

SNMPv3-Gruppenverwaltung

Mit der SNMPv3-Gruppenverwaltung können Sie Gruppen mit unterschiedlichen Zugriffsebenen für das Gerät erstellen. Sie können Benutzer dann nach Bedarf diesen Gruppen zuordnen.

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:

Schritt 1: Klicken Sie in der Gruppentabelle auf **Hinzufügen**, um in der Tabelle für die SNMPv3-Gruppenverwaltung eine neue Gruppe hinzuzufügen. Die Seite *SNMPv3 Group Management* wird geöffnet:

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 |

Schritt 2: Geben Sie im Feld *Gruppenname* den Namen der Gruppe ein.

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

Schritt 3: Wählen Sie den Sicherheitstyp aus der Dropdown-Liste *Sicherheitsstufe* aus. Die Sicherheitstypen werden wie folgt beschrieben:

- Keine Authentifizierung, kein Datenschutz - Benutzer in dieser Gruppe müssen kein Authentifizierungskennwort festlegen oder ein Datenschutzkennwort festlegen. Nachrichten werden nicht verschlüsselt und Benutzer werden nicht authentifiziert

·Authentifizierung, Keine Privatsphäre - Benutzer müssen ein Authentifizierungskennwort festlegen, aber kein Datenschutzkennwort. Benutzer werden authentifiziert, wenn Nachrichten empfangen werden, die Nachrichten werden jedoch nicht verschlüsselt.

·Authentifizierungsschutz - Benutzer müssen sowohl ein Authentifizierungskennwort als auch ein Datenschutzkennwort festlegen. Benutzer werden authentifiziert, wenn Nachrichten empfangen werden. Die Nachrichten werden ebenfalls mit dem Datenschutzkennwort verschlüsselt.

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

Schritt 4: Aktivieren Sie die Kontrollkästchen, um die spezifischen Management Information Base (MIBs) auszuwählen, auf die die Gruppe zugreifen soll. MIBs werden verwendet, um die erforderlichen Informationen für das verwaltete System zu definieren. Sie wird als iso.org.dod.internet.mgmt.mib dargestellt. Durch Festlegen bestimmter MIBs können Gruppen Zugriff auf verschiedene Teile des Geräts erhalten.

Schritt 5: Klicken Sie auf das entsprechende Optionsfeld für jede aktivierte MIB, um die für die Gruppe verfügbare Berechtigungsstufe auszuwählen. Die Berechtigungsstufen sind wie folgt definiert:

- Read Only (Nur Lesen): Benutzer in dieser Gruppe können die MIB lesen, sie jedoch nicht ändern.
- Lesen/Schreiben - Benutzer in dieser Gruppe können sowohl von der MIB lesen und ändern.

Schritt 6: Blättern Sie nach unten, und klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Damit wird die Gruppe der Gruppentabelle hinzugefügt.

The screenshot shows the SNMP configuration interface. It includes sections for Global Settings, Group Table, and User Table. The Group Table has one entry, 'Group1', with a radio button selected. The 'Edit' button for this group is circled in red. The User Table is currently empty.

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 checked="" 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	Group
0 results found!				

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Schritt 7: (Optional) Wenn Sie die konfigurierte Gruppe ändern möchten, klicken Sie auf das Optionsfeld der gewünschten Gruppe und dann auf **Bearbeiten** und ändern Sie die entsprechenden Felder.

Schritt 8: (Optional) Wenn Sie die konfigurierte Gruppe löschen möchten, klicken Sie auf das gewünschte Optionsfeld der Gruppe und anschließend auf **Löschen**.

SNMPv3-Benutzerverwaltung

SNMP-Benutzer sind die Remote-Benutzer, für die die SNMP-Dienste ausgeführt werden.

Hinweis: Sie müssen der Gruppentabelle eine Gruppe hinzufügen, bevor Sie einen Benutzer in der Benutzertabelle hinzufügen können.

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:

Schritt 1: Klicken Sie in der Benutzertabelle auf **Hinzufügen**, um einen neuen Benutzer in der SNMPv3-Benutzerverwaltungstabelle hinzuzufügen. Die Seite *SNMPv3-Benutzerverwaltung* wird geöffnet:

SNMP

SNMPv3 User Management

Enable :

User Name:

Group:

Authentication Method: MD5 SHA None Authentication Password:

Privacy Method: DES AES None Privacy Password:

Schritt 2: Aktivieren Sie **Aktivieren**, um die Benutzerverwaltung für SNMP zu aktivieren.

Schritt 3: Geben Sie im Feld *Benutzername* einen Benutzernamen ein.

Schritt 4: Wählen Sie die gewünschte Gruppe aus der Dropdown-Liste *Gruppe* aus. Der neue Benutzer wird dieser speziellen Gruppe hinzugefügt.

Schritt 5: Klicken Sie auf das entsprechende Optionsfeld, um eine Authentifizierungsmethode auszuwählen. Die Authentifizierungsmethoden werden wie folgt beschrieben:

·MD5 - Message Digest Algorithm-5 (MD5) ist eine 32-stellige hexadezimale Hash-Funktion.

·SHA - Secure Hash Algorithm (SHA) ist eine 160-Bit-Hash-Funktion, die als sicherer gilt als MD5.

Schritt 6: Geben Sie im Feld *Authentifizierungskennwort* ein Kennwort für die Authentifizierung ein. Das Authentifizierungskennwort ist das Kennwort, das von den Geräten im Voraus gemeinsam verwendet wird. Beim Austausch von Datenverkehr wird das spezifische Kennwort zur Authentifizierung des Datenverkehrs verwendet.

Schritt 7: Klicken Sie auf das entsprechende Optionsfeld, um im Feld *Datenschutzmethode* die gewünschte Verschlüsselungsmethode auszuwählen.

·DES - Der Data Encryption Standard (DES) ist eine 56-Bit-Verschlüsselungsmethode. Sie wird als unsicher angesehen, kann jedoch erforderlich sein, wenn das Gerät zusammen mit anderen Geräten verwendet wird, die AES nicht unterstützen.

·AES - Advanced Encryption Standard (AES) verwendet eine 128-Bit-, 192-Bit- oder 256-Bit-Verschlüsselungsmethode. Sie gilt als sicherer als DES.

Schritt 8: Geben Sie im Feld *Datenschutzkennwort* ein Kennwort für die Privatsphäre ein. Das Datenschutzkennwort ist das Kennwort, das zur Verschlüsselung von Nachrichten verwendet wird.

Schritt 9: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern. Damit wird der Benutzer der Benutzertabelle hinzugefügt.

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	Group
<input type="radio"/>	<input checked="" type="checkbox"/> USER1	SHA	AES	Group1

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

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"/>	<input checked="" type="checkbox"/>	USER1	SHA	AES	Group1

Add Edit Delete

SNMPv3 Trap Receiver IP Address: (For IPv4)

SNMPv3 Trap Receiver User:

Save Cancel

Schritt 10: (Optional) Wenn Sie den konfigurierten Benutzer ändern möchten, klicken Sie auf das Optionsfeld des gewünschten Benutzers und anschließend auf **Bearbeiten** und ändern Sie das entsprechende Feld.

Schritt 11: (Optional) Wenn Sie den konfigurierten Benutzer löschen möchten, klicken Sie auf das Optionsfeld des gewünschten Benutzers und anschließend auf **Löschen**.

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

Schritt 12: Geben Sie die IP-Adresse des SNMPv3-Trap-Receiver im Feld *IP-Adresse des SNMPv3-Trap-Receiver* ein.

Schritt 13: Wählen Sie den entsprechenden Trap-Benutzer aus der Dropdown-Liste *SNMPv3 Trap Receiver User* aus. Dies ist der Benutzer, der die Trap-Meldung empfängt,

wenn ein Trap-Ereignis auftritt.

Schritt 14: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.