Configurar o Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) nos roteadores VPN RV320 e RV325

Objetivo

O SNMP (Simple Network Management Protocol) é um protocolo da camada de aplicação usado para gerenciar e monitorar o tráfego da rede. O SNMP mantém todos os registros de atividade de vários dispositivos na rede para ajudá-lo a encontrar rapidamente a origem dos problemas na rede quando necessário. Na série RV32x VPN Router, você pode habilitar SNMPv1/v2c, SNMPv3 ou ambos ao mesmo tempo para ter o desempenho desejado da rede.

O objetivo deste documento é explicar como configurar o SNMP no RV32x VPN Router Series.

Dispositivo aplicável

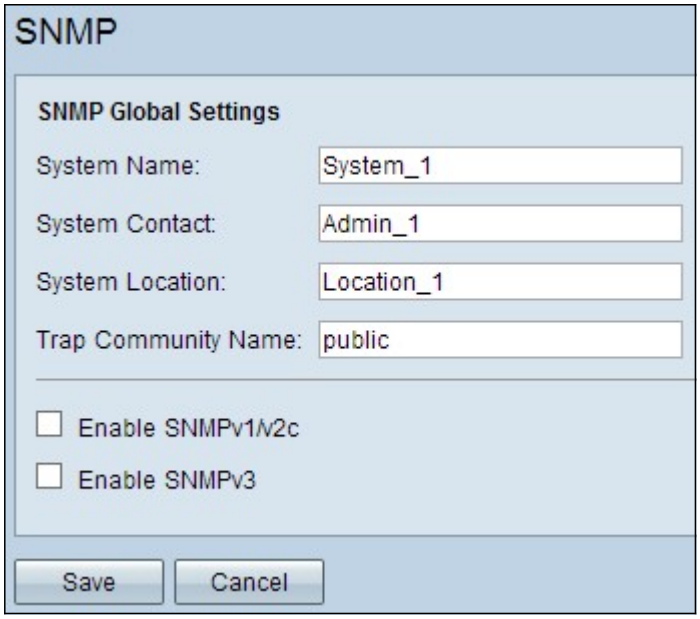
RV320 Roteador VPN WAN duplo
Roteador VPN WAN duplo RV325 Gigabit

Versão de software

•v1.1.0.09

Configuração SNMP

Etapa 1. Faça login no utilitário de configuração da Web e escolha **Gerenciamento do sistema > SNMP**. A página *SNMP* é aberta:



Etapa 2. Insira o nome do host no campo *System Name (Nome do sistema)*.

Etapa 3. Insira o nome ou as informações de contato da pessoa responsável pelo roteador no campo *Contato do sistema*.

Etapa 4. Insira a localização física do roteador no campo *System Location (Local do sistema)*.

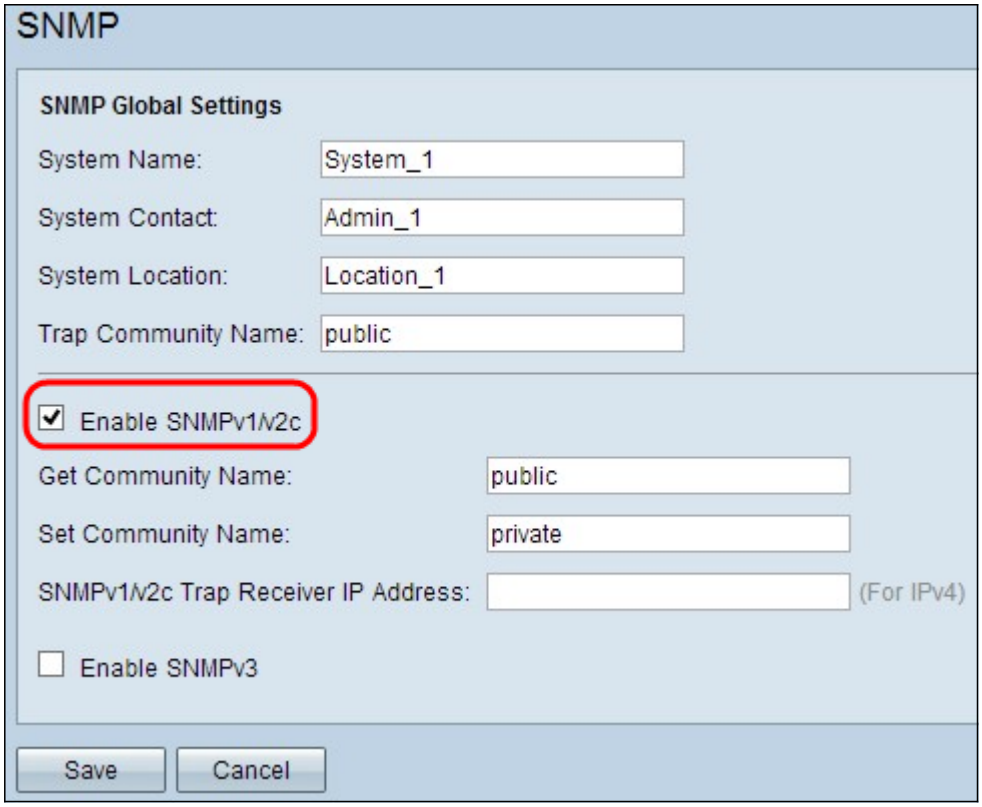
Note: As informações inseridas nos campos *Contato do sistema* e *Localização do sistema* não modificam o comportamento do dispositivo. Você pode inseri-los conforme desejado para ajudar a gerenciar melhor seus dispositivos (por exemplo, você pode achar desejável incluir um número de telefone no campo *Contato do sistema*).

Etapa 5. Insira o nome da comunidade de interceptação à qual o agente pertence no campo *Nome da comunidade de interceptações*. Uma armadilha é uma mensagem enviada pelo dispositivo quando ocorre um evento específico. O nome da comunidade de armadilhas pode ter até 64 caracteres alfanuméricos. O nome da comunidade de armadilhas padrão é *público*.

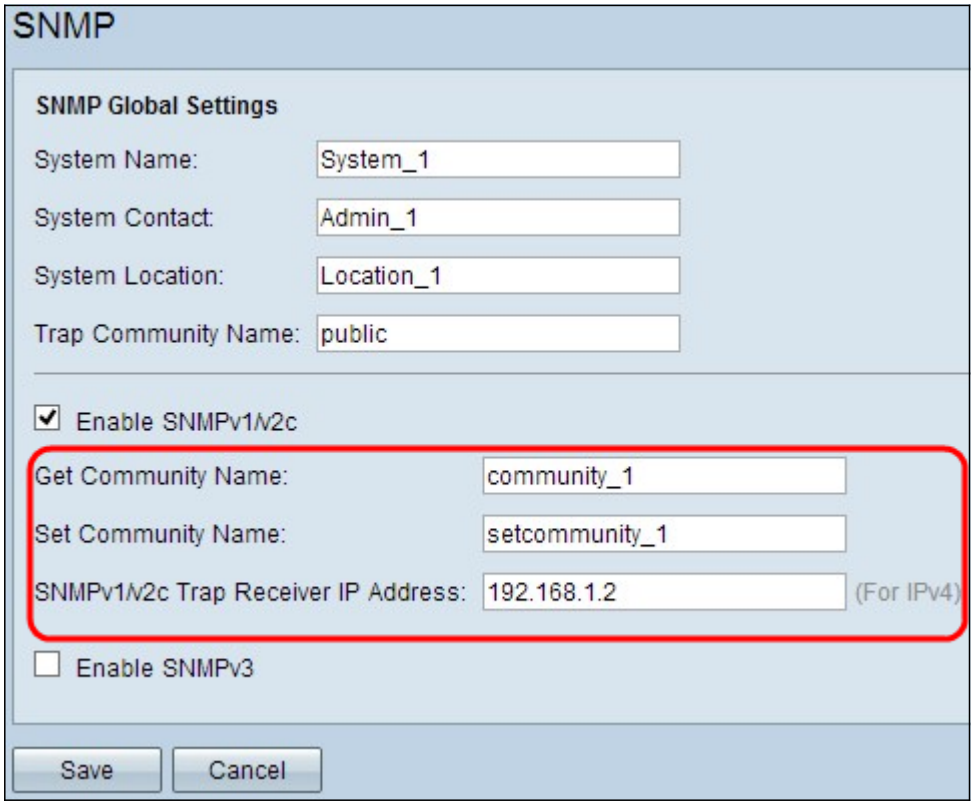
Etapa 6. Clique em **Save (Salvar) para salvar as configurações.**

Configuração SNMPv1/SNMPv2c

SNMPv1 é a primeira versão do SNMP e agora é considerado inseguro. O SNMPv2c é uma versão aprimorada do SNMP. Ele oferece mais segurança do que o SNMPv1 e melhor tratamento de erros.



Etapa 1. Marque **Habilitar SNMPv1/v2c** para habilitar SNMPv1/2c.



Etapa 2. Digite um nome de comunidade no campo *Get Community Name*. Get Community Name é a string de comunidade somente leitura para autenticar o comando SNMP Get. O comando Get é usado para recuperar as informações do dispositivo SNMP. O nome da comunidade Get pode ter até 64 caracteres alfanuméricos. O Nome da Comunidade Get padrão é *público*.

Etapa 3. Insira um nome de comunidade no campo *Definir nome da comunidade*. É a string de comunidade de leitura/gravação que autentica o comando SNMP Set. O comando Set é

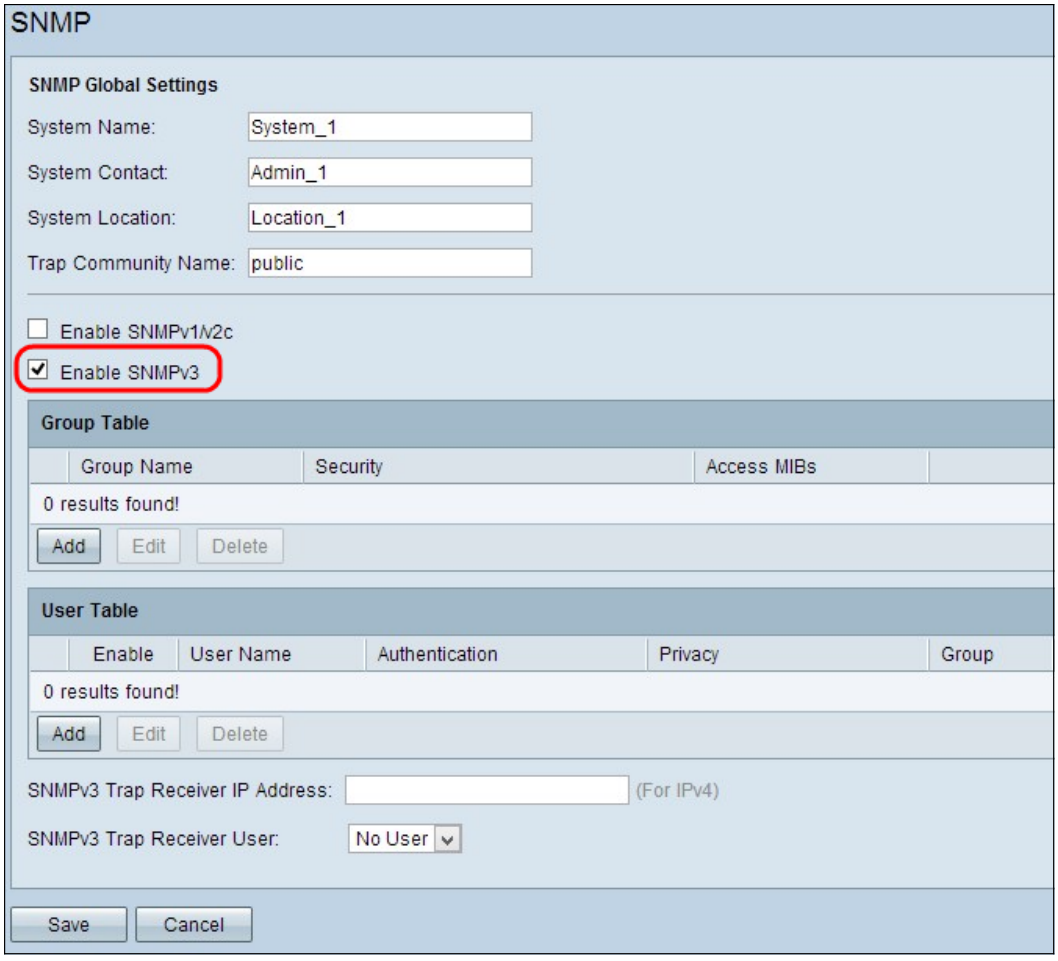
usado para modificar ou definir as variáveis no dispositivo. O campo Definir nome da comunidade pode ter até 64 caracteres alfanuméricos. O nome da comunidade do conjunto padrão é *privado*.

Etapa 4. Insira o endereço IP ou o nome de domínio do servidor específico em que o software de gerenciamento SNMP é executado no campo *Endereço IP* do *Receptor de Interceptação* SNMPv1/v2c. Uma mensagem de trap é enviada ao administrador do servidor para notificar o administrador se ocorrer algum erro ou falha.

Etapa 5. Clique em **Save (Salvar) para salvar as configurações.**

Configuração do SNMPv3

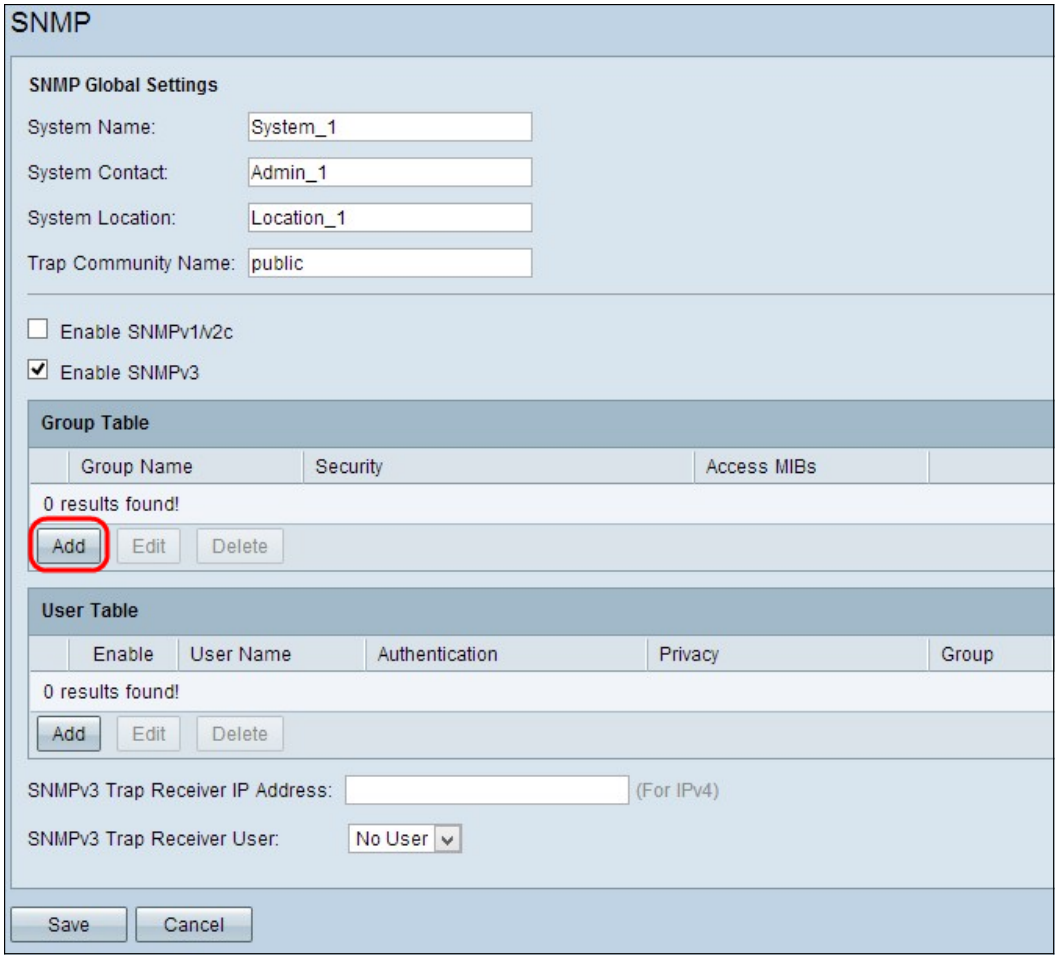
SNMPv3 é a versão mais recente do SNMP e fornece o mais alto nível de segurança entre as três versões SNMP. Também fornece configuração remota.



Etapa 1. Marque **Habilitar SNMPv3** para habilitar SNMPv3.

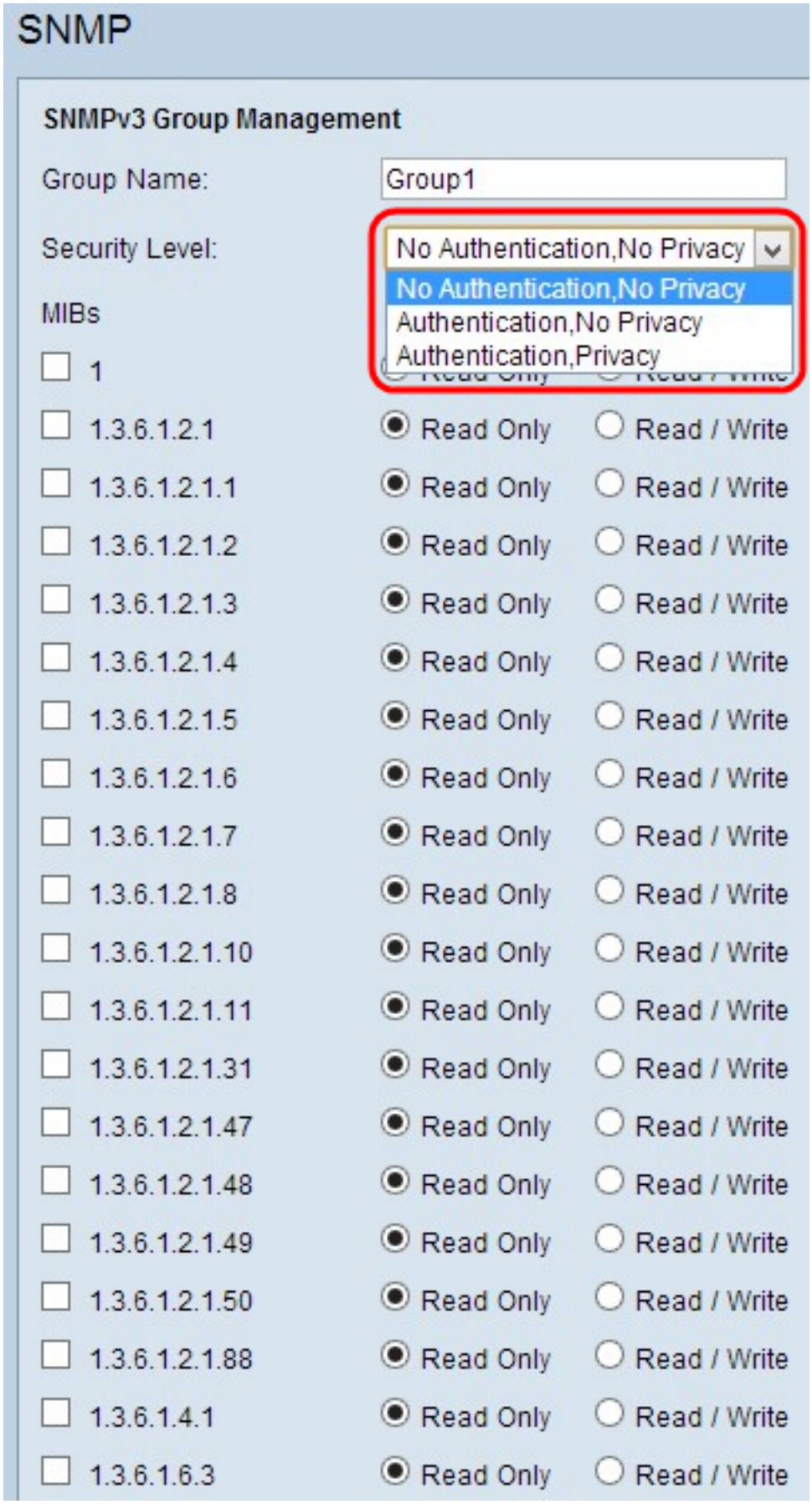
Gerenciamento de grupo SNMPv3

O gerenciamento de grupo SNMPv3 permite criar grupos com diferentes níveis de acesso ao dispositivo. Em seguida, você pode mapear usuários nesses grupos conforme julgar apropriado.



Etapa 1. Clique em **Add** na Tabela de grupos para adicionar um novo grupo na tabela SNMPv3 Group Management. A página *Gerenciamento de grupo SNMPv3* é aberta:

Etapa 2. Digite o nome do grupo no campo *Nome do grupo*.



Etapa 3. Escolha o tipo de segurança na lista suspensa *Nível de segurança*. Os tipos de segurança são descritos a seguir:

Sem autenticação, Sem privacidade — Os usuários neste grupo não precisarão definir uma senha de autenticação ou definir uma senha de privacidade. As mensagens não serão criptografadas e os usuários não serão autenticados

Autenticação, Sem privacidade — Os usuários serão obrigados a definir uma senha de autenticação, mas não uma senha de privacidade. Os usuários serão autenticados quando as mensagens forem recebidas, mas elas não serão criptografadas.

Authentication Privacy (Privacidade de autenticação): os usuários precisarão definir uma senha de autenticação e uma senha de privacidade. Os usuários serão autenticados quando as mensagens forem recebidas. As mensagens também serão criptografadas usando a senha de privacidade.

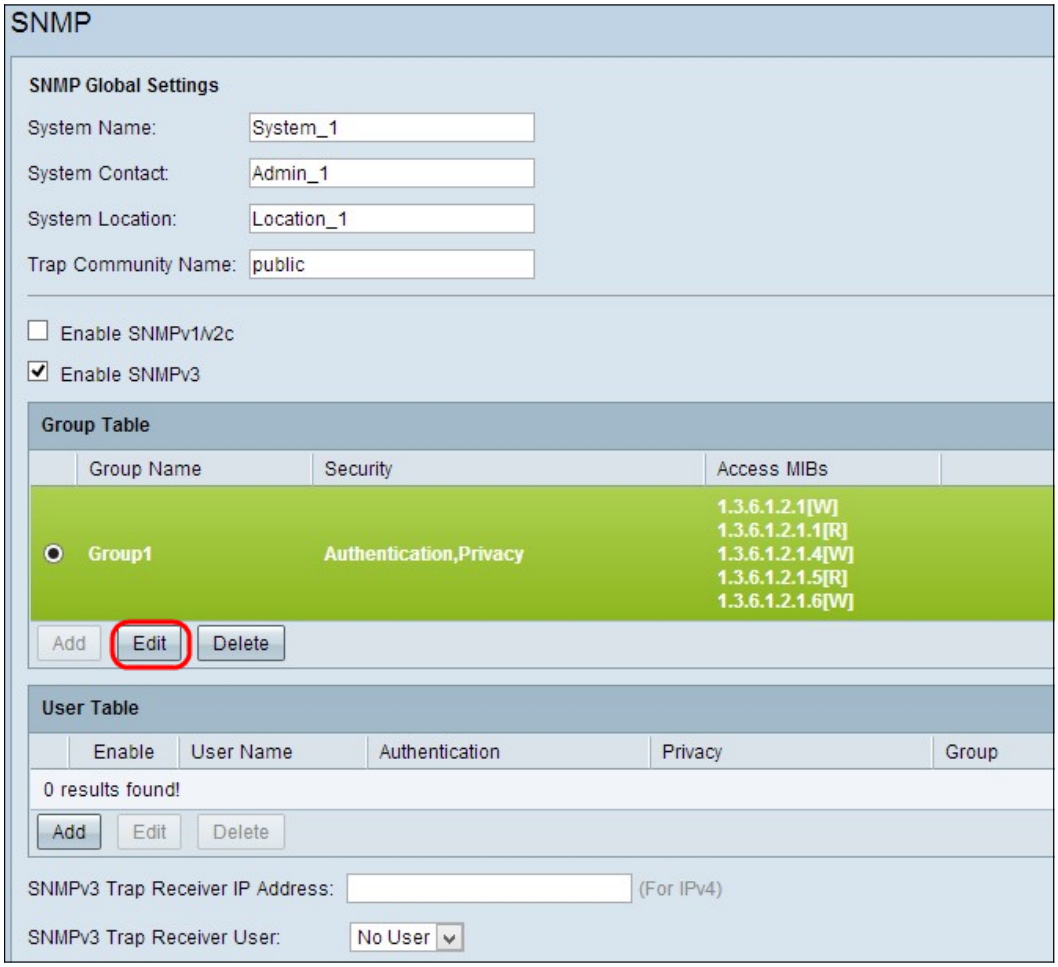
Etapa 4. Marque as caixas de seleção para selecionar as MIBs (Management Information Base, Base de informações de gerenciamento) específicas às quais você deseja que o grupo tenha acesso. As MIBs são usadas para definir as informações necessárias do sistema gerenciado. Ele é representado como iso.org.dod.internet.mgmt.mib. Ao definir MIBs específicas, você pode permitir que os grupos tenham acesso a diferentes partes do dispositivo.

Etapa 5. Clique no botão de opção específico de cada MIB marcado para escolher o nível de permissão disponível para o grupo. Os níveis de permissões são definidos da seguinte forma:

Read Only (Somente leitura) — Os usuários desse grupo poderão ler a MIB, mas não modificá-la.

Leitura/gravação — Os usuários neste grupo poderão ler a partir da MIB e modificá-la.

Etapa 6. Role para baixo e clique em **Salvar** para salvar as configurações. Isso adiciona o grupo à Tabela de grupos.



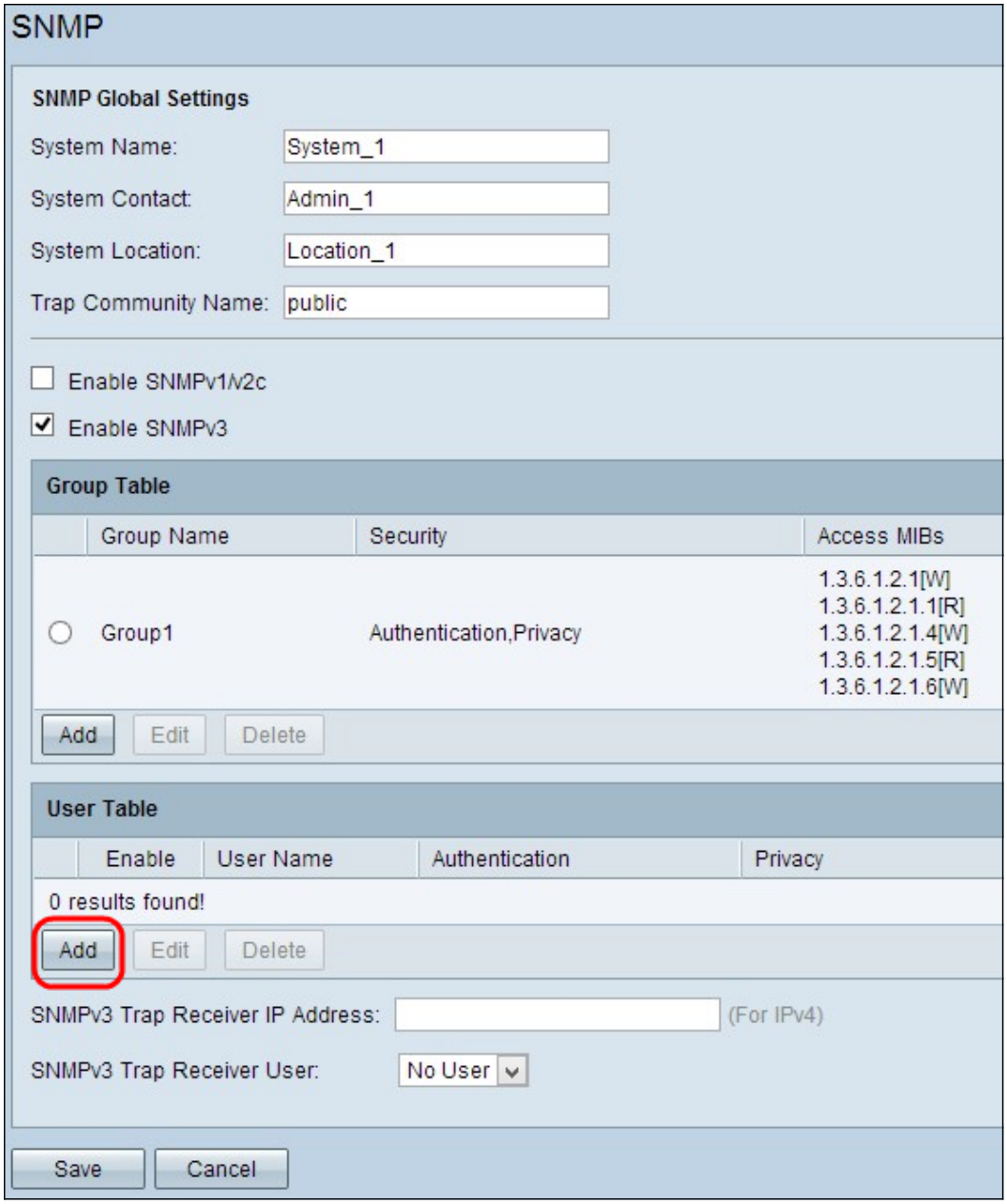
Passo 7. (Opcional) Para alterar o grupo configurado, clique no botão de opção do grupo desejado e clique em **Editar** e altere os respectivos campos.

Etapa 8. (Opcional) Para excluir o grupo configurado, clique no botão de opção desejado do grupo e clique em **Excluir.**

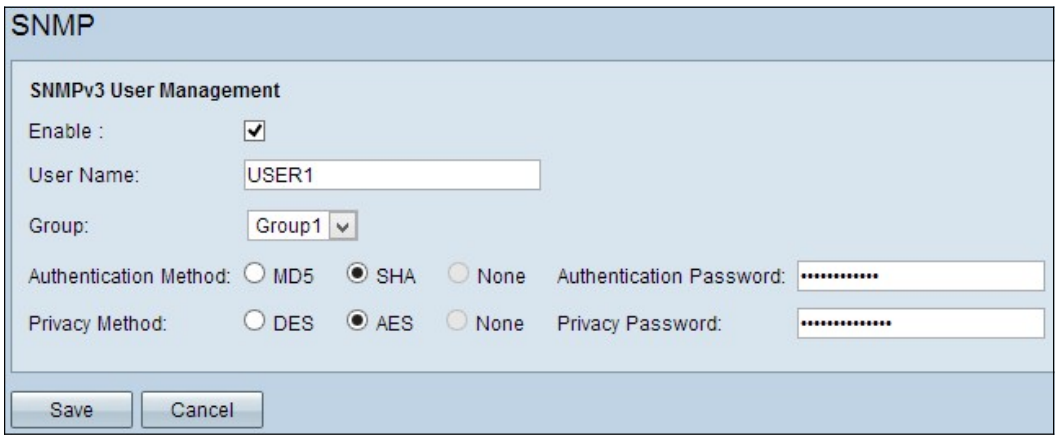
Gerenciamento de usuário SNMPv3

Os usuários SNMP são os usuários remotos para os quais os serviços SNMP são executados.

Nota: É necessário adicionar um grupo à Tabela de grupos antes de adicionar um usuário à Tabela de usuários.



Etapa 1. Clique em **Adicionar** na Tabela de usuários para adicionar um novo usuário na Tabela de gerenciamento de usuário SNMPv3. A página *Gerenciamento de usuário SNMPv3* é aberta:



Etapa 2. Marque **Habilitar** para habilitar o gerenciamento de usuário para SNMP.

Etapa 3. Insira um nome de usuário no campo *Nome de usuário*.

Etapa 4. Escolha o grupo desejado na lista suspensa *Grupo*. O novo usuário é adicionado a esse grupo específico.

Etapa 5. Clique no botão de opção específico para escolher um Método de autenticação. Os métodos de autenticação são descritos a seguir:

MD5 — Message Digest Algorithm-5 (MD5) é uma função hash hexadecimal de 32 dígitos.

SHA — O Secure Hash Algorithm (SHA) é uma função de hash de 160 bits considerada mais segura do que o MD5.

Etapa 6. Insira uma senha para a autenticação no campo *Authentication Password (Senha de autenticação)*. A senha de autenticação é a senha que é compartilhada antecipadamente entre os dispositivos. Quando trocam tráfego, usam a senha específica para autenticar o tráfego.

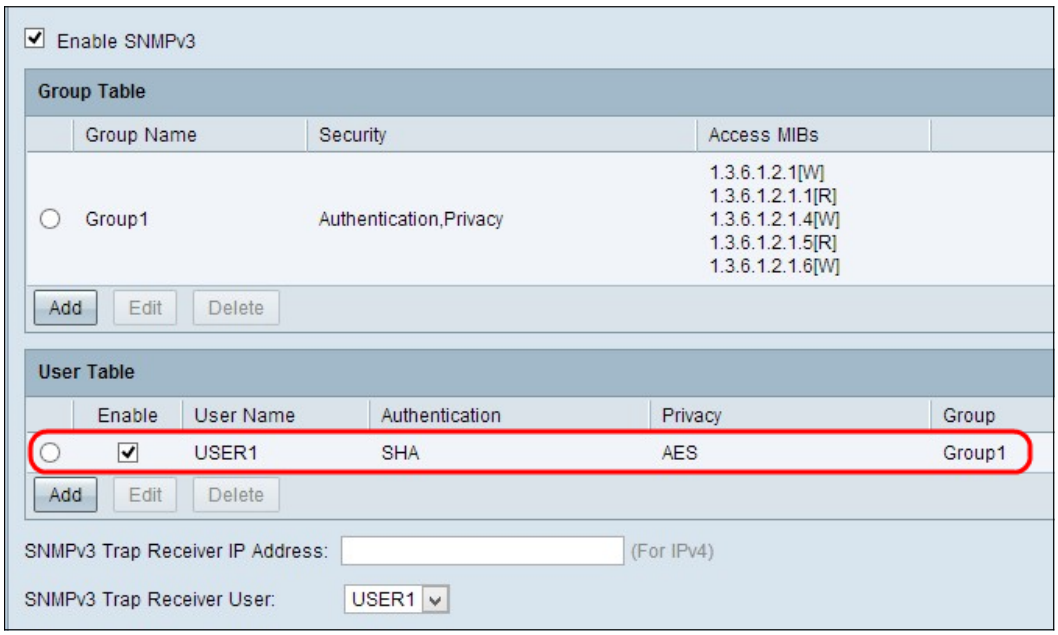
Passo 7. Clique no botão de opção específico para escolher o método de criptografia desejado no campo *Privacy Method*.

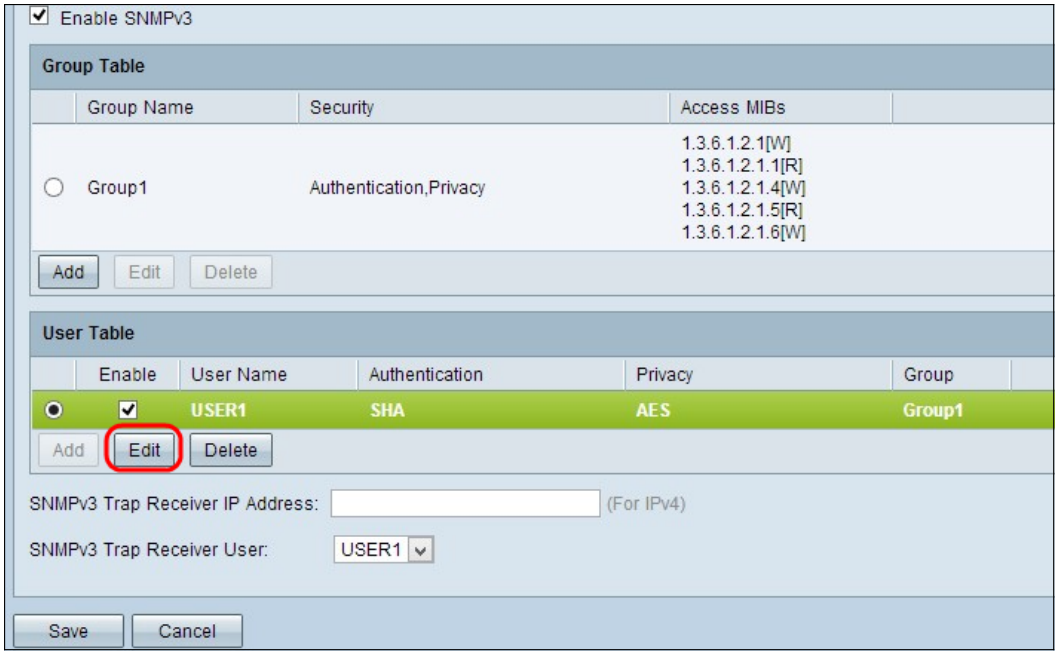
DES — Data Encryption Standard (DES) é um método de criptografia de 56 bits. Ele é considerado inseguro, mas pode ser necessário quando o dispositivo é usado em conjunto com outros dispositivos que não suportam AES.

AES — O AES (Advanced Encryption Standard) usa um método de criptografia de 128 bits, 192 bits ou 256 bits. Ele é considerado mais seguro que o DES.

Etapa 8. Insira uma senha para a privacidade no campo *Privacy Password (Senha de privacidade)*. A senha de privacidade é a senha usada para criptografar mensagens.

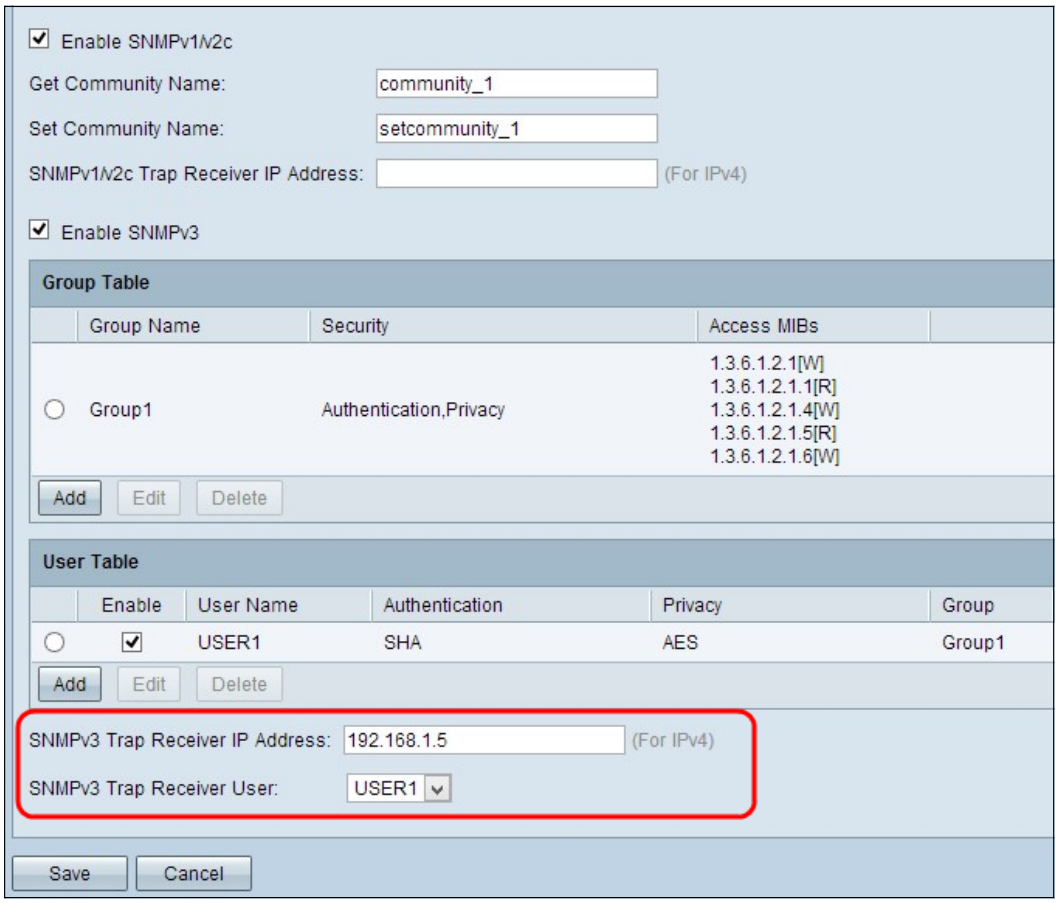
Etapa 9. Clique em **Save (Salvar) para salvar as configurações.** Isso adiciona o usuário à Tabela do usuário.





Etapa 10. (Opcional) Se desejar alterar o usuário configurado, clique no botão de opção do usuário desejado e clique em **Editar** e altere o respectivo campo.

Etapa 11. (Opcional) Se desejar excluir o usuário configurado, clique no botão de opção do usuário desejado e clique em **Excluir.**



Etapa 12. Insira o endereço IP do receptor de interceptação SNMPv3 no campo *Endereço IP do receptor de interceptação SNMPv3*.

Etapa 13. Escolha o respectivo usuário de interceptação na lista suspensa *Usuário do receptor de interceptação SNMPv3*. Esse é o usuário que recebe a mensagem de armadilha quando um evento de armadilha ocorre.

Etapa 14. Clique em **Save (Salvar) para salvar as configurações.**