

Configuração do Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) em RV215W

Objetivo

O SNMP (Simple Network Management Protocol) é um protocolo da camada de aplicação usado para gerenciar e monitorar uma rede. O SNMP é usado por administradores de rede para gerenciar o desempenho da rede, detectar e corrigir problemas de rede e coletar estatísticas de rede. Uma rede gerenciada por SNMP consiste em dispositivos gerenciados, agentes e um gerenciador de rede. Dispositivos gerenciados são dispositivos capazes do recurso SNMP. Um agente é o software SNMP em um dispositivo gerenciado. Um gerenciador de rede é uma entidade que recebe dados dos agentes SNMP. O usuário deve instalar um programa de gerenciador SNMP v3 para exibir notificações SNMP.

Este artigo explica como configurar o SNMP no RV215W.

Dispositivos aplicáveis

RV215W

Versão de software

•1.1.0.5

Configuração SNMP

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

SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level:

Authentication Algorithm Server: MD5 SHA

Authentication Password:

Privacy Algorithm: DES AES

Privacy Password:

Trap Configuration

IP Address: (Hint: 192.168.1.100 or fec0::64)

Port: (Range: 162 or 1025 - 65535, Default: 162)

Community:

SNMP Version:

Save

Cancel

Informações do sistema SNMP

SNMP System Information

SNMP: Enable

Engine ID: 80000009033CCE738E0126

SysContact:

SysLocation:

SysName:

Etapa 1. Marque **Enable** no campo SNMP para permitir a configuração SNMP no RV215W.

Note: A ID do mecanismo do agente do RV215W é exibida no campo ID do mecanismo. As IDs do mecanismo são usadas para identificar agentes em dispositivos gerenciados de forma exclusiva.

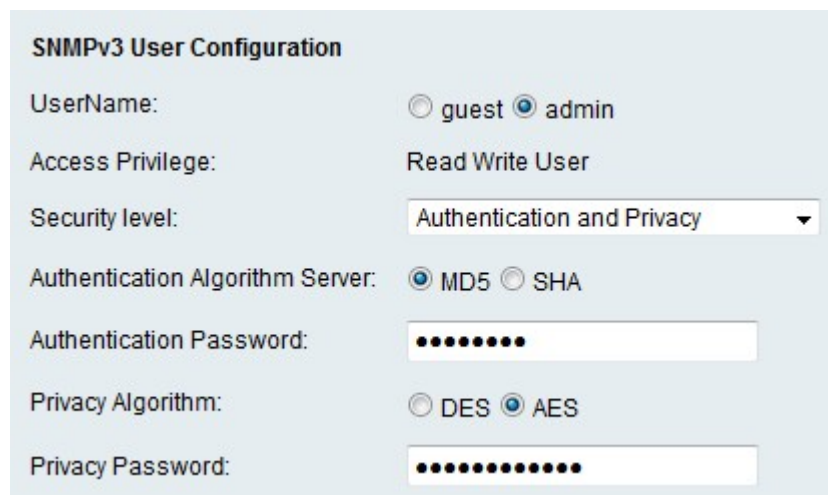
Etapa 2. Insira um nome para o contato do sistema no campo SysContact. É prática comum incluir informações de contato para o contato do sistema.

Etapa 3. Insira a localização física do RV215W no campo SysLocation.

Etapa 4. Insira um nome para a identificação do RV215W no campo SysName.

Etapa 5. Click **Save**.

Configuração do usuário SNMPv3



SNMPv3 User Configuration

UserName: guest admin

Access Privilege: Read Write User

Security level: Authentication and Privacy

Authentication Algorithm Server: MD5 SHA

Authentication Password: ●●●●●●●●

Privacy Algorithm: DES AES

Privacy Password: ●●●●●●●●●●

Etapa 1. Clique no botão de opção que corresponde à conta desejada a ser configurada no campo Nome de usuário. O privilégio de acesso do usuário é exibido no campo Privilégio de acesso.

Convidado — Um usuário convidado só tem privilégios de leitura.

Admin — Um usuário administrador tem privilégios de leitura e gravação.

Etapa 2. Na lista suspensa Nível de segurança, escolha a segurança desejada. A autenticação é usada para autenticar e permitir que os usuários visualizem ou gerenciem os recursos SNMP. A privacidade é outra chave que pode ser usada para aumentar a segurança no recurso SNMP.

Nenhuma autenticação e nenhuma privacidade — nenhuma senha de autenticação ou privacidade é necessária para o usuário.

Autenticação e Sem privacidade — Somente a autenticação é exigida pelo usuário.

Autenticação e privacidade — a autenticação e uma senha de privacidade são exigidas pelo usuário.

Etapa 3. Se o nível de segurança incluir autenticação, clique no botão de opção que corresponde ao servidor desejado no campo Servidor do algoritmo de autenticação. Este algoritmo é uma função de hash. As funções de hash são usadas para converter chaves em uma mensagem de bit designada.

MD5 — Message-Digest 5 (MD5) é um algoritmo que recebe uma entrada e produz um resumo de mensagem de 128 bits da entrada.

SHA - O Secure Hash Algorithm (SHA) é um algoritmo que recebe uma entrada e produz

um resumo de mensagem de 160 bits da entrada.

Etapa 4. Insira uma senha para os usuários no campo Authentication Password (Senha de autenticação).

Etapa 5. Se o nível de segurança incluir privacidade, clique no botão de opção que corresponde ao algoritmo desejado no campo Privacy Algorithm (Algoritmo de privacidade).

DES — Data Encryption Standard (DES) é um algoritmo de criptografia que usa o mesmo método para criptografar e descriptografar uma mensagem. O algoritmo DES processa mais rápido que o AES.

AES — O AES (Advanced Encryption Standard) é um algoritmo de criptografia que usa métodos diferentes para criptografar e descriptografar uma mensagem. Isso torna o AES um algoritmo de criptografia mais seguro do que o DES.

Etapa 6. Insira uma senha de privacidade para os usuários no campo Senha de privacidade.

Passo 7. Click **Save**.

Configuração de armadilha

As interceptações são mensagens SNMP geradas usadas para relatar eventos do sistema. Uma armadilha forçará um dispositivo gerenciado a enviar uma mensagem SNMP ao gerenciador de rede que notifica o gerenciador de rede de um evento do sistema.



The screenshot shows a 'Trap Configuration' form with the following fields and values:

Field	Value	Hint/Range
IP Address:	192.168.1.100	(Hint: 192.168.1.100 or fec0::64)
Port:	162	(Range: 162 or 1025 - 65535, Default: 162)
Community:	community1	
SNMP Version:	v1	

Etapa 1. Insira o endereço IP para o qual as notificações de interceptação (trapping) serão enviadas no campo IP address (Endereço IP).

Etapa 2. Insira o número da porta do endereço IP para o qual as notificações de armadilha serão enviadas no campo Porta.

Etapa 3. Digite a string de comunidade à qual o gerenciador de armadilhas pertence no campo Comunidade. Uma string de comunidade é uma string de texto que atua como uma senha. É usado pelo SNMP para autenticar mensagens enviadas entre um agente e um gerenciador de rede.

Note: Esse campo só é aplicável se a versão de interceptação SNMP não for a versão 3.

Etapa 4. Na lista suspensa Versão SNMP, escolha a versão do gerenciador SNMP para as mensagens de interceptação SNMP.

v1 — Usa uma string de comunidade para autenticar mensagens de interceptação.

v2c — Usa uma string de comunidade para autenticar mensagens de interceptação.

v3 — Usa senhas criptografadas para autenticar mensagens de interceptação.

Etapa 5. Click **Save**.