

Configure as configurações gerais de SNMP no WAP361 e WAP150

Objetivo

O Protocolo de Gerenciamento de Rede Simples (SNMP - Simple Network Management Protocol) é um protocolo usado para gerenciamento de rede, solução de problemas e manutenção. O SNMP grava, armazena e compartilha informações com a ajuda de um software de duas chaves: um Network Management System (NMS) que é executado em dispositivos gerenciadores e em um agente que é executado em dispositivos gerenciados. O WAP361 e o WAP150 suportam SNMPv2c e SNMPv3.

O SNMPv2c é semelhante ao SNMP original por meio de segurança aprimorada e suporte para tratamento de erros. Essa melhoria inclui códigos de erro expandidos que distinguem diferentes tipos de erros; todos os tipos de erros são relatados por meio de um único código de erro em SNMPv1.

O SNMPv3 melhorou a segunda versão lançada fornecendo novos recursos de segurança como Autenticação, Privacidade, Autorização e Controle de Acesso.

Este artigo explica como configurar as configurações gerais de SNMP no WAP361 e WAP150.

Dispositivos aplicáveis

- WAP300 Series — WAP361
- WAP100 Series — WAP150

Versão de software

- 1.0.0.16

Configurações gerais SNMP

Etapa 1. Faça login no utilitário baseado na Web do ponto de acesso e escolha **SNMP > General**.



Etapa 2. Na área Configurações globais, marque a caixa de seleção **Habilitar** para habilitar o SNMP.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Etapa 3. Insira o número da porta UDP no campo *UDP Port (Porta UDP)*. O agente SNMP verifica se há solicitações de acesso nesta porta. A porta padrão é 161.

General

Global Settings

SNMP: Enable

UDP Port: (Range:1025-65535, Default: 161)

Timesaver: se você não precisa da configuração de SNMPv2, ignore esta etapa e vá para a [Etapa 11](#).

Etapa 4. Insira um nome de comunidade somente leitura no campo *Read-Only Community* com caracteres alfanuméricos de 1 a 256. O nome da comunidade é um nome definido pelo usuário que atua como um mecanismo de autenticação simples ou senha para restringir os dispositivos na rede que podem solicitar dados do agente SNMP. A string de comunidade enviada pelo remetente no pacote de solicitação deve corresponder à string de comunidade no dispositivo do agente. A string padrão para somente leitura é `cisco_public`.

Note: A senha somente leitura dá autoridade para recuperar somente informações.

SNMPv2c Settings

Read-only Community:

Read-write Community:

Etapa 5. Insira um nome de comunidade de leitura/gravação no campo *Read-write Community* com caracteres alfanuméricos que variam de 1 a 256 para operações de conjunto SNMP permitidas. Somente as solicitações dos dispositivos que se identificam com esse nome de comunidade são aceitas. O padrão é `cisco_private`. Esta é uma senha que permite recuperar informações do agente e modificar configurações nesse dispositivo de agente.

Note: Recomenda-se alterar ambas as senhas para uma senha definida pelo usuário para evitar ameaças à segurança.

SNMPv2c Settings

Read-only Community:

Read-write Community:

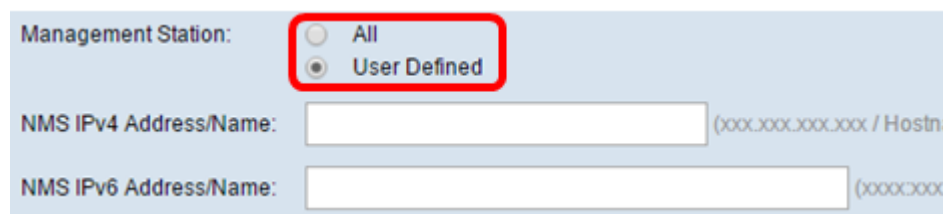
Etapa 6. Escolha entre All (Todos) ou User Defined (Definido pelo usuário) no botão de opção Management Station para escolher uma preferência de estação de gerenciamento. A estação de gerenciamento monitora e atualiza os valores na Base de Informações de

Gerenciamento (MIB).

Note: A opção selecionada como um exemplo na imagem abaixo é Definida pelo Usuário.

Tudo — Permite que todas as estações na rede acessem o Ponto de Acesso Sem Fio (WAP) através do SNMP como uma estação de gerenciamento. Se você escolher esta opção, vá para a [Etapa 8](#).

Definido pelo usuário — limita o acesso a uma estação ou grupo de estações específico.



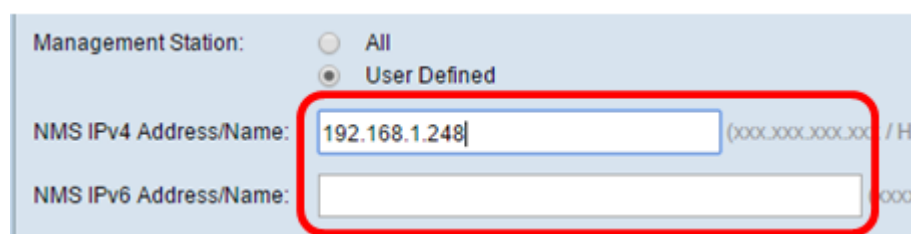
Management Station: All User Defined

NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / Hostn

NMS IPv6 Address/Name: (xxxx:xxx

Passo 7. Insira os endereços IPv4 ou IPv6, o nome de host DNS ou a sub-rede do NMS que podem executar, obter e definir as solicitações para os dispositivos gerenciados nos campos *Endereço/Nome do NMSIPv4* e *Endereço/Nome do NMS IPv6*, respectivamente. Um NMS se refere às estações de gerenciamento que executam aplicativos que monitoram e controlam dispositivos gerenciados.

Note: O endereço IPv4 do NMS 192.168.1.241 é usado como um exemplo na imagem abaixo.



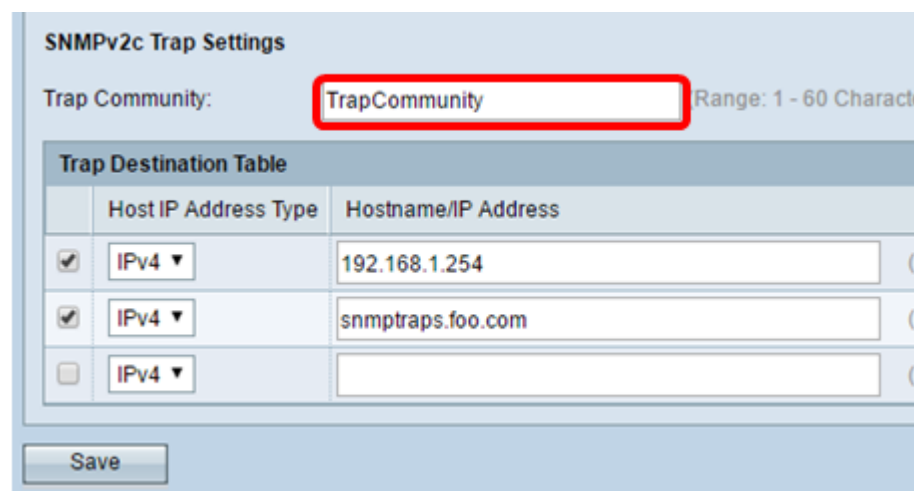
Management Station: All User Defined

NMS IPv4 Address/Name: (xxx.xxx.xxx.xxx / H

NMS IPv6 Address/Name: xxx

Etapa 8. Insira o nome da comunidade global associado a interceptações SNMP no campo *Comunidade Trap*. O intervalo válido é de 1 a 60 caracteres alfanuméricos e especiais. Na imagem abaixo, TrapCommunity é usado como exemplo.

Note: Armadilhas são notificações de agente para gerente contendo informações de agente. Armadilhas enviadas do dispositivo usam a string inserida como nome de comunidade.



SNMPv2c Trap Settings

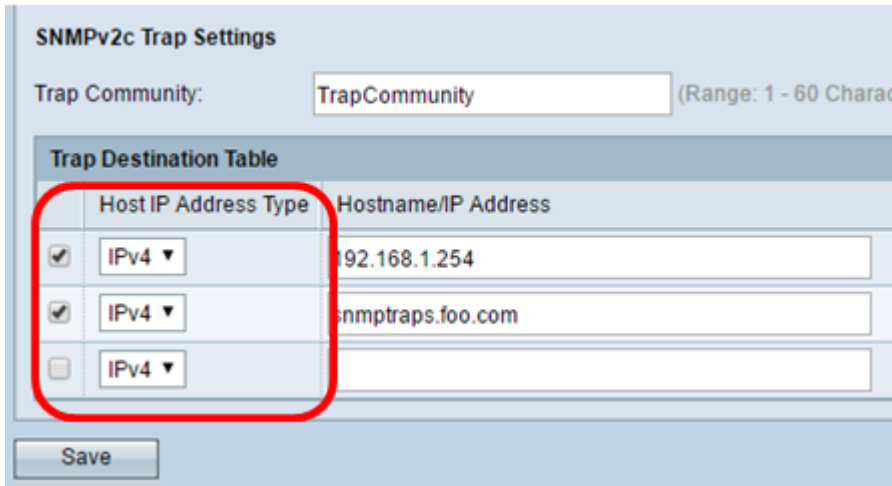
Trap Community: Range: 1 - 60 Charact

| Trap Destination Table | |
|--|---------------------|
| Host IP Address Type | Hostname/IP Address |
| <input checked="" type="checkbox"/> IPv4 | 192.168.1.254 |
| <input checked="" type="checkbox"/> IPv4 | snmptraps.foo.com |
| <input type="checkbox"/> IPv4 | |

Save

Etapa 9. Na área Trap Destination Table (Tabela de destino de interceptação), marque a caixa e escolha entre IPv4 e IPv6 na lista suspensa Host IP Address Type.

Note: No exemplo abaixo, as duas primeiras caixas foram marcadas com o IPv4 definido como o Tipo de endereço IP do host.



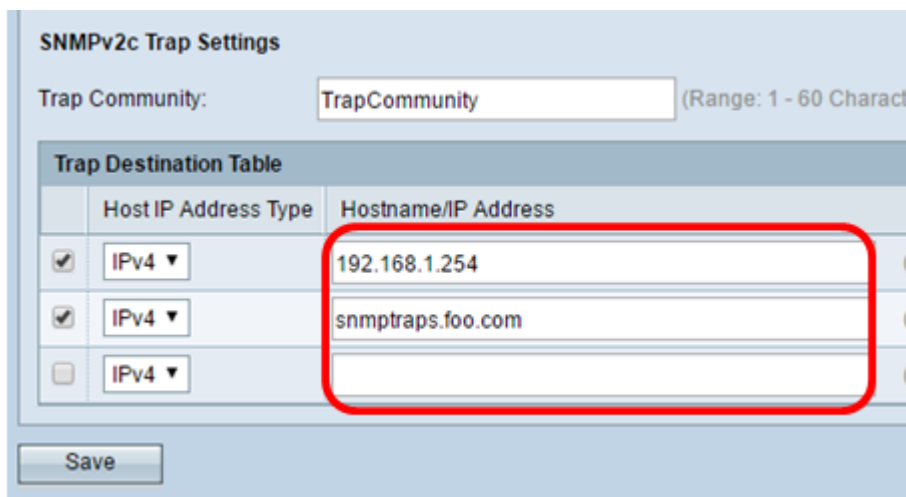
The screenshot shows the 'SNMPv2c Trap Settings' interface. At the top, there is a 'Trap Community' field with the value 'TrapCommunity'. Below it is the 'Trap Destination Table' with the following structure:

| | Host IP Address Type | Hostname/IP Address |
|-------------------------------------|----------------------|---------------------|
| <input checked="" type="checkbox"/> | IPv4 | 192.168.1.254 |
| <input checked="" type="checkbox"/> | IPv4 | snmptraps.foo.com |
| <input type="checkbox"/> | IPv4 | |

A red box highlights the first two rows of the table. At the bottom left, there is a 'Save' button.

Etapa 10. No campo *Nome do host/Endereço IP*, insira os nomes de host ou endereços IP de até três hosts para receber interceptações SNMP.

Note: Na imagem abaixo, um endereço IP e um nome de host foram inseridos como exemplos.

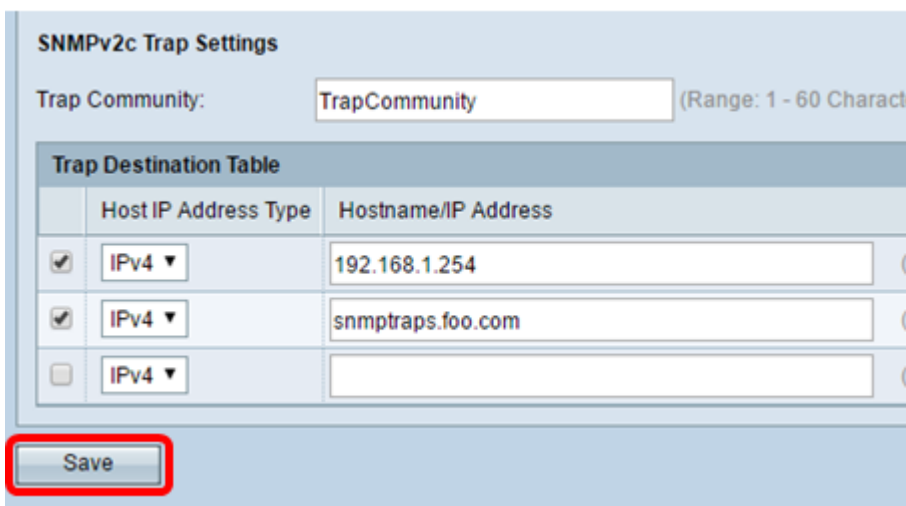


This screenshot is similar to the previous one, but the red box highlights the 'Hostname/IP Address' field in the first two rows of the 'Trap Destination Table'.

| | Host IP Address Type | Hostname/IP Address |
|-------------------------------------|----------------------|---------------------|
| <input checked="" type="checkbox"/> | IPv4 | 192.168.1.254 |
| <input checked="" type="checkbox"/> | IPv4 | snmptraps.foo.com |
| <input type="checkbox"/> | IPv4 | |

The 'Save' button is visible at the bottom left.

Etapa 11. Click **Save**.



This screenshot shows the same 'SNMPv2c Trap Settings' interface, but the 'Save' button at the bottom left is highlighted with a red box.

Você configurou com êxito as configurações gerais SNMP em seu WAP.

Para obter mais informações sobre Configurações gerais, clique nos seguintes links:

- [Configurações gerais do Protocolo de gerenciamento de rede simples \(SNMP - Simple Network Management Protocol\) nos access points WAP121 e WAP321](#)
- [Configuração de configurações gerais do Protocolo de gerenciamento de rede simples \(SNMP - Simple Network Management Protocol\) nos access points WAP551 e WAP561](#)