在WAP361和WAP150上配置常规SNMP设置

目标

简单网络管理协议(SNMP)是用于网络管理、故障排除和维护的协议。SNMP记录、存储和共享信息，借助两键软件：在管理器设备上运行的网络管理系统(NMS)和在受管设备上运行的代理。WAP361和WAP150支持SNMPv2c和SNMPv3。

SNMPv2c通过改进的安全和错误处理支持与原始SNMP类似。这种改进包括扩展的错误代码，可区分不同类型的错误；所有类型的错误都通过SNMPv1中的一个错误代码报告。

SNMPv3通过提供新的安全功能（如身份验证、隐私、授权和访问控制）改进了第二版。

本文介绍如何在WAP361和WAP150上配置常规SNMP设置。

适用设备

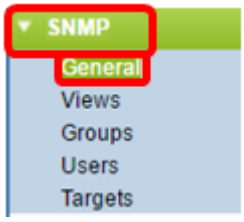
- WAP300系列 — WAP361
- WAP100系列 — WAP150

软件版本

- 1.0.0.16

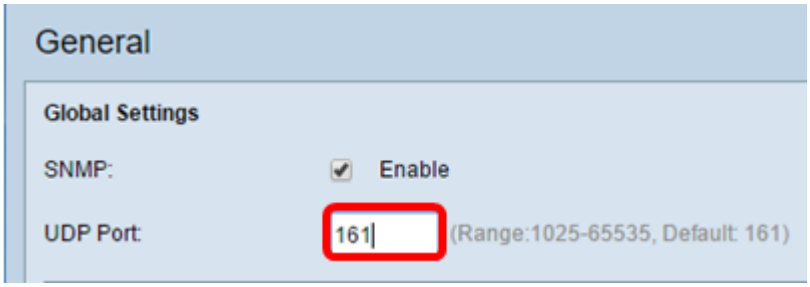
SNMP常规设置

步骤1.登录到基于Web的接入点实用程序并选择SNMP > **General**。



步骤2.在Global Settings区域，选中**Enable**复选框以启用SNMP。

步骤3.在UDP Port字段中输入UDP*端口*号。SNMP代理检查此端口的访问请求。默认端口为161。



节省时间：如果您不需要SNMPv2配置，请跳过此步骤，然后跳至步骤11。

步骤4.在只读社区字段中输入只读社区名称，其中包含从1到256的字母数字字符。社区名称是用户定义的名称，用作简单的身份验证机制或密码，以限制网络上可向SNMP代理请求数据的设备。请求数据包中的发送方发送的社区字符串必须与代理设备上的社区字符串匹配。只读的默认字符串是cisco_public。

注意：只读密码授予仅检索信息的权限。

步骤5.在读写社区字段中输入读写社区名称，其中字母数字*字符范围*为1到256，以用于允许的SNMP设置操作。仅接受来自使用此社区名称标识自己的设备的请求。默认值为cisco_private。此密码允许从代理检索信息和修改该代理设备上的设置。

注意：建议将两个密码都更改为用户定义的密码以避免安全威胁。

步骤6.在管理站单选按钮中选择全部或用户定义，以选择管理站首选项。管理站监控并更新管理信息库(MIB)中的值。

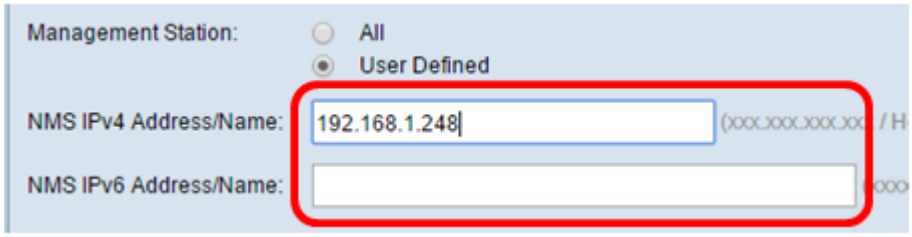
注意：在下图中作为示例选择的选项是“用户定义”。

All — 允许网络中的所有站点通过SNMP作为管理站访问无线接入点(WAP)。如果选择此项，请继续步骤8。

用户定义 — 限制对特定站点或站组的访问。

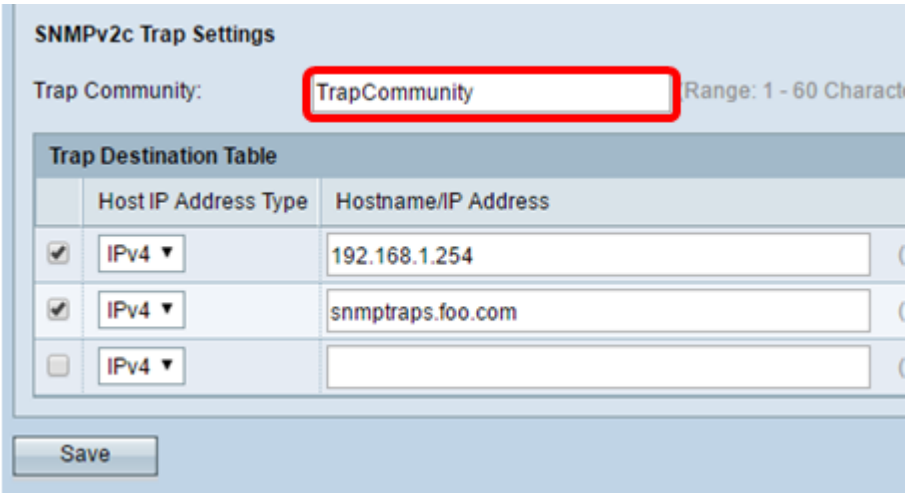
步骤7.分别在NMSIPv4地址/名称和*NMS IPv6地址/名称*字段中，输入可执行、获取和设置对受管设备的请求的IPv4或IPv6地址、DNS主机名或NMS子网。NMS是指执行监控和控制受管设备的应用的管理站。

注意：NMS IPv4地址192.168.1.241用作下图中的示例。



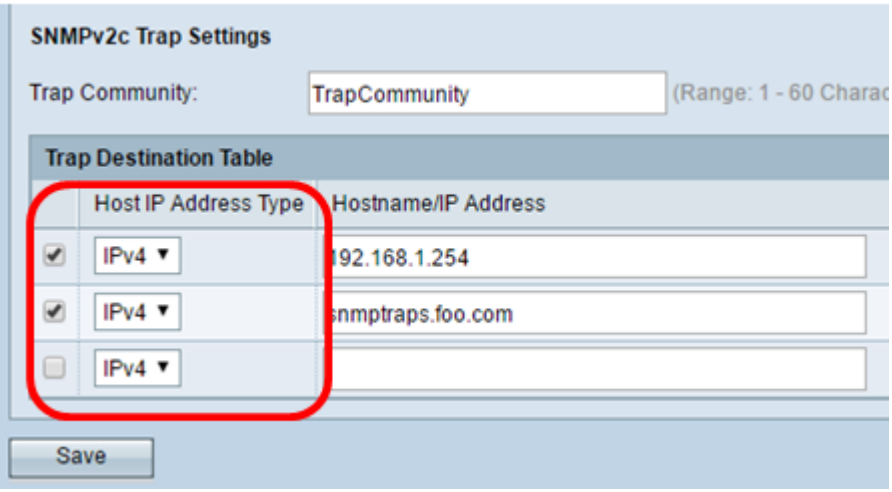
步骤8.在Trap Community字段中输入与SNMP陷阱关联的*全局社*区名称。有效范围为1到60个字母数字和特殊字符。在下图中，以TrapCommunity为例。

注意：陷阱是从代理到管理器的通知，包含代理信息。从设备发送的陷阱使用作为团体名称输入的字符串。



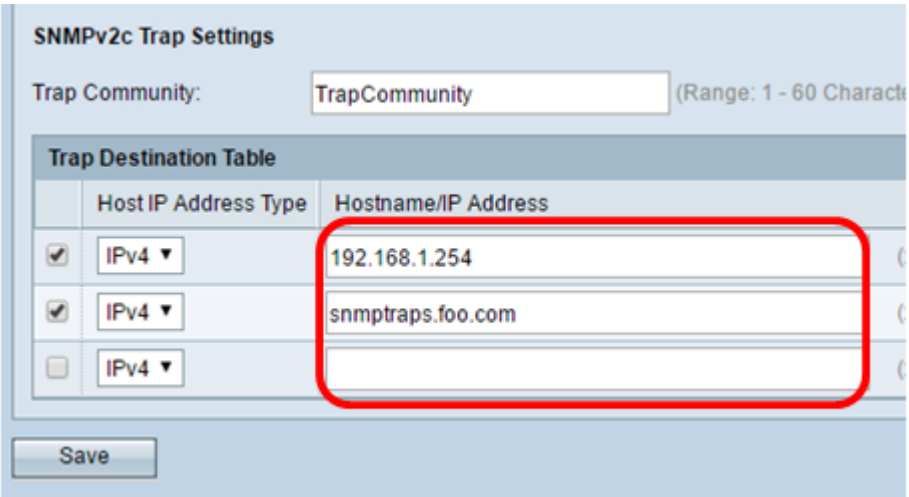
步骤9.在Trap Destination Table区域，选中该框并在Host IP Address Type下拉列表中选择IPv4和IPv6。

注意：在以下示例中，前两个框已选中，两个IPv4均设置为主机IP地址类型。

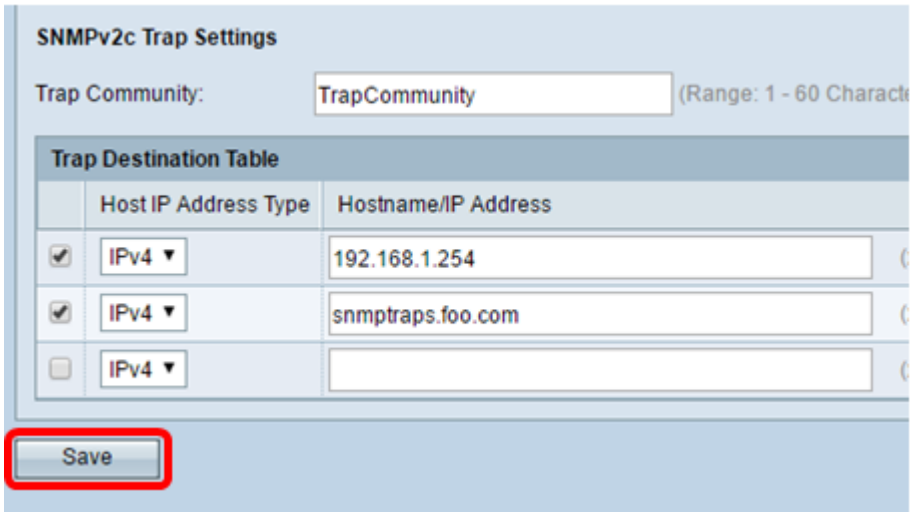


步骤10.在Hostname/*IP Address*字段中，输入最多三台主机的主机名或IP地址以接收SNMP陷阱。

注意：在下图中，输入IP地址和主机名作为示例。



步骤11.单击“保**存**”。



您已成功在WAP上配置SNMP常规设置。

有关General Settings Simple Network Management Protocol的详细信息，请点击以下链接：

- WAP121和WAP321接入点上的简单网络管理协议(SNMP)常规设置
- WAP551和WAP561接入点上的简单网络管理协议(SNMP)常规设置配置