简单网络管理协议(SNMP)在AP541N接入点的用户配置

客观

简单网络管理协议(SNMP)是用于管理网络设备的网络管理协议。它在实现您迅速解决网络问题的网络帮助记录，存储和共享多种设备的信息。SNMP使用管理信息基础(MIB)存储可用的信息以分层的方式。

本文解释如何配置AP541N接入点的SNMP用户。默认情况下SNMP没有任何用户。

可适用的设备

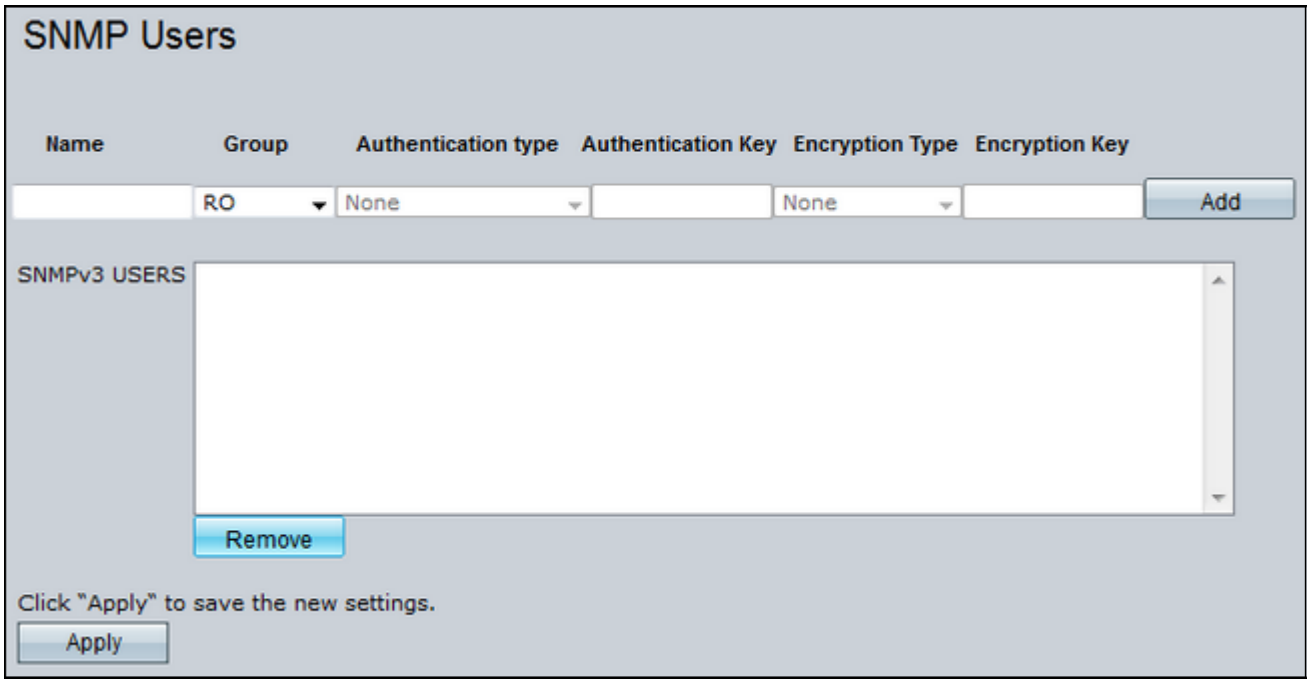
•AP541N接入点

软件版本

•AP541N-K9-2.0(4)

SNMP用户配置

步骤1.登陆到Web配置工具并且选择**SNMP > Users**。*SNMP*用户页打开：



步骤2.输入SNMP用户的名字在名称字段。示例-用户3， user4。

步骤3.从组下拉列表选择特定用户的组。

Note:关于SNMP组的更多信息，请参见*在AP541N接入点的*条款*简单网络管理协议(SNMP)组配置*。

- RO —表明此组的用户没有认证和数据加密SNMP消息的。用户访问读访问默认值所有MIB视图。
- RWAuth —表明此组的用户没有认证，但是SNMP消息的数据加密。用户读了和对默认值的写访问所有MIB视图。
- RWPriv —表明此组的用户有认证和加密SNMP消息的。用户读了和对默认值的写访问所有MIB视图。

步骤4.从认证类型下拉列表选择认证类型使用它在自SNMPv3用户的SNMP请求。在RO组下的用户没有认证。

- MD5 —表明自SNMPv3用户的请求要求消息分类算法(MD5)认证。MD5使用导致认证的一个Hash值的一个128-bit散列函数。
- 什么都—表明认证没有对于SNMPv3用户请求是必需的。

第 5 步：如果MD5认证类型在第4步被选择，请输入键在认证密钥领域。 此enable (event)验证用户请求的SNMP代理程序。

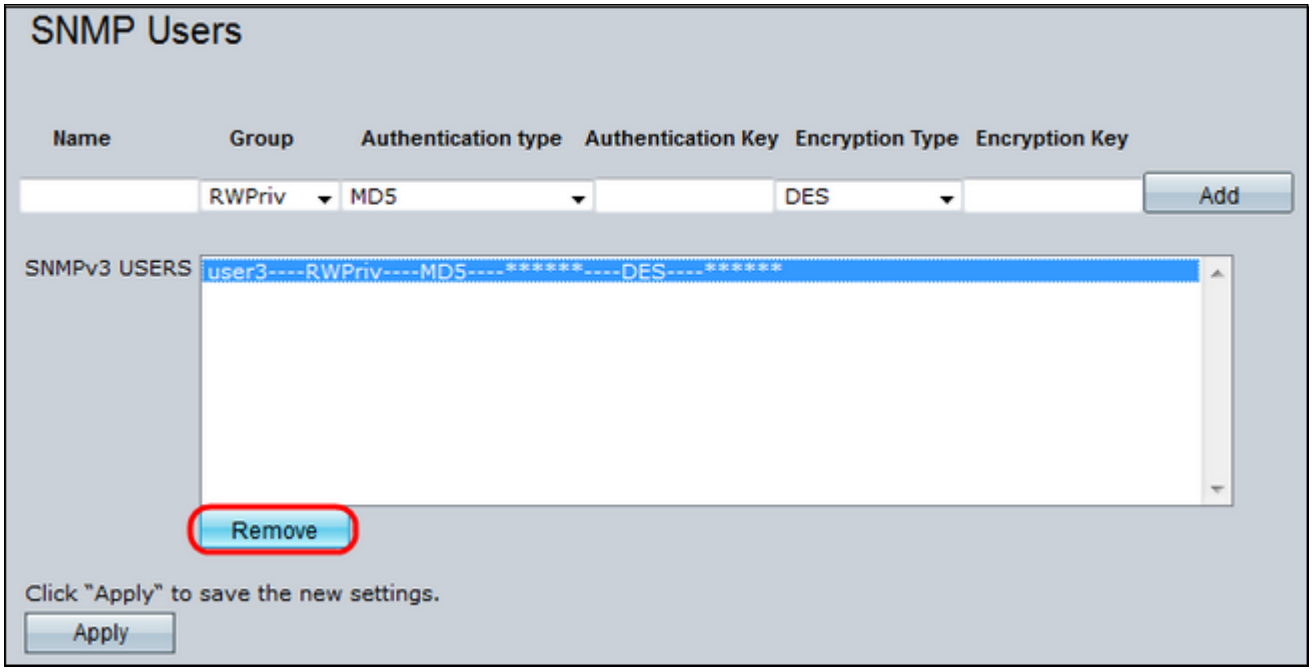
步骤6.选择加密的种类使用在自加密类型下拉列表的SNMPv3请求。

Note:在RO和RWAuth组下的用户不使用加密。

- DES —数据加密标准(DES)指示自被加密的SNMPv3用户的请求。DES是的数据加密一个用途广泛的方法使用一个专用的(秘密)键。
- 什么都—表明SNMPv3用户请求的保密性不存在。

第 7 步：如果DES加密类型在第6步被选择，请输入加密密钥在范围自8到32个字符的加密密钥领域。此键用于加密SNMPv3请求。

步骤8.点击**添加**添加用户到SNMPv3用户表。



第9.步(可选)删除用户，从SNMPv3用户列表选择其中一个用户和点击**去除**。

步骤10.点击**适用**保存设置。