

在WAP125和WAP581上配置SNMPv3

目标

简单网络管理协议第3版(SNMPv3)是一种安全模型，其中为用户和用户所在的组设置了身份验证策略。安全级别是安全模型中允许的安全级别。安全模型和安全级别的组合确定在处理SNMP数据包时使用的安全机制。

在SNMP中，管理信息库(MIB)是包含对象标识符(OID)的分层信息数据库，它充当可通过SNMP读取或设置的变量。MIB以树状结构组织。托管对象命名树中的子树是视图子树。MIB视图是一组视图子树或一组视图子树的组合。创建MIB视图以控制SNMPv3用户可以访问的OID范围。SNMPv3视图配置对于限制用户仅查看受限MIB至关重要。WAP最多可以有16个视图，包括两个默认视图。

本文档旨在向您展示如何收集、查看和下载WAP125和WAP581上的CPU/RAM活动。

适用设备

- WAP125
- WAP581

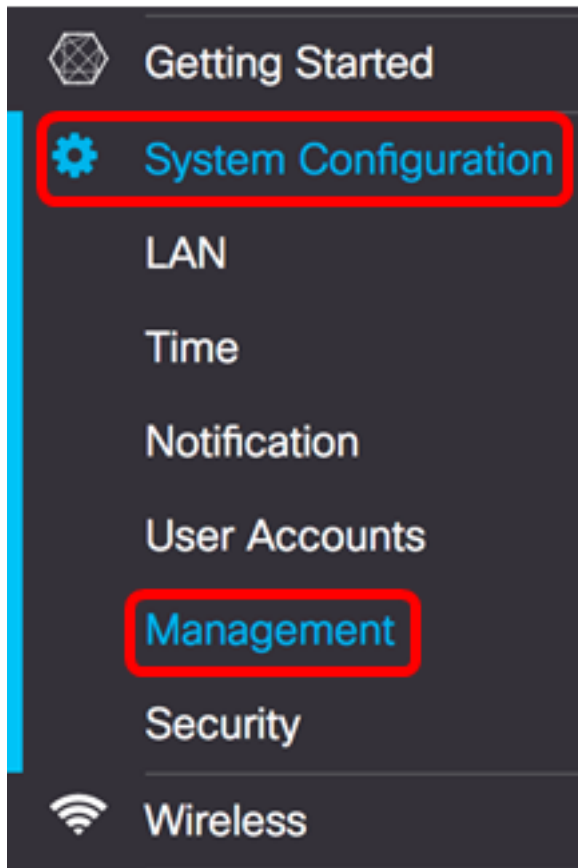
软件版本

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

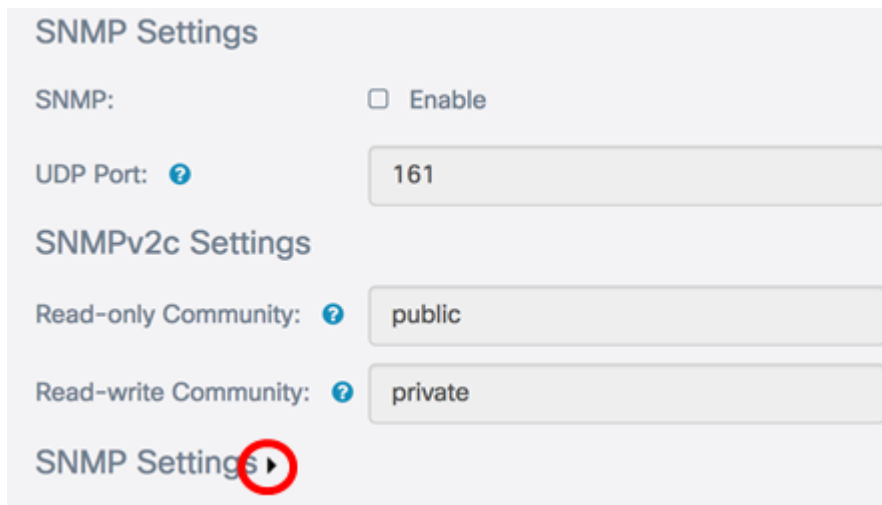
配置SNMPv3设置

配置SNMPv3视图

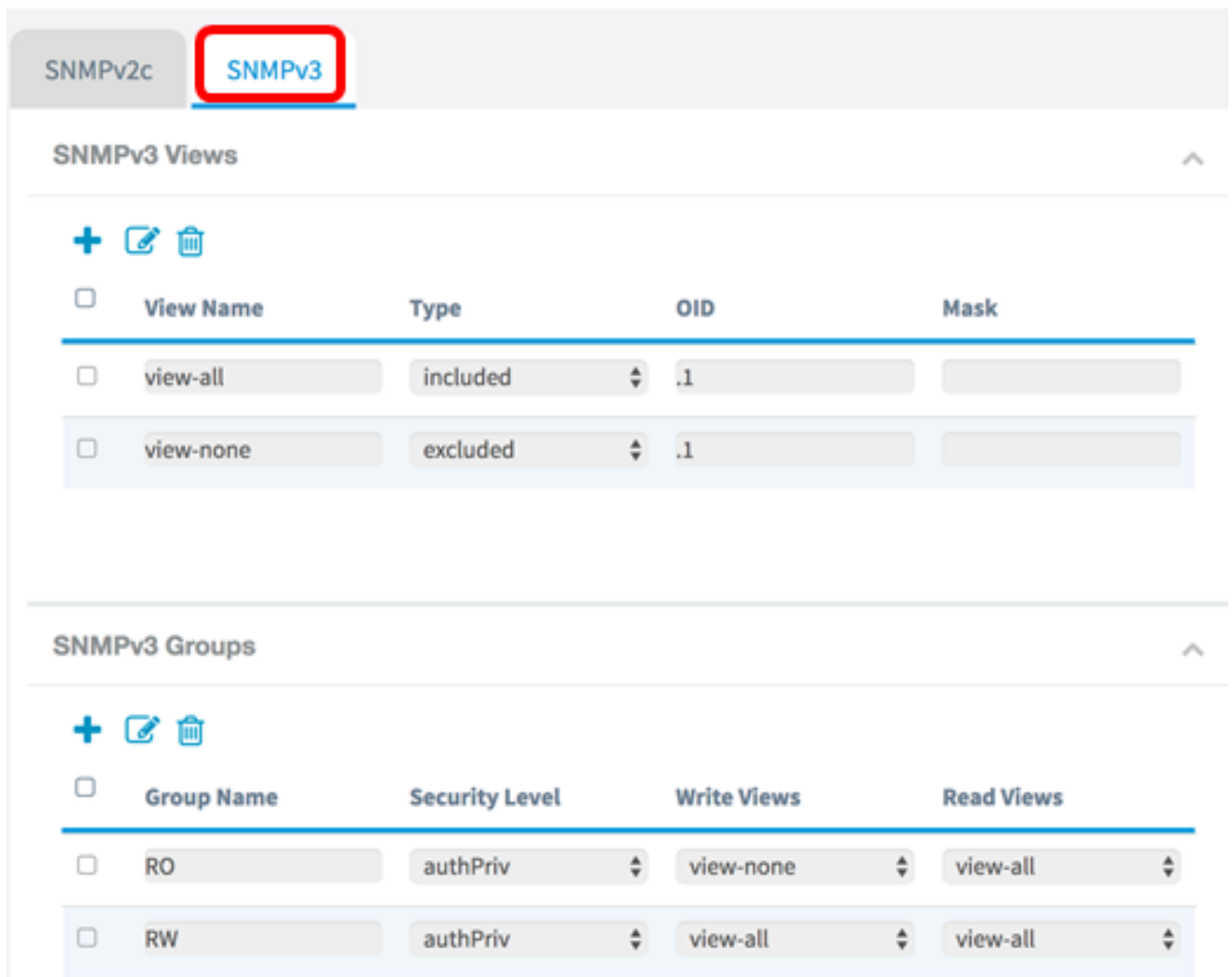
步骤1. 登录到基于Web的实用程序，然后选择**System Configuration > Management**。



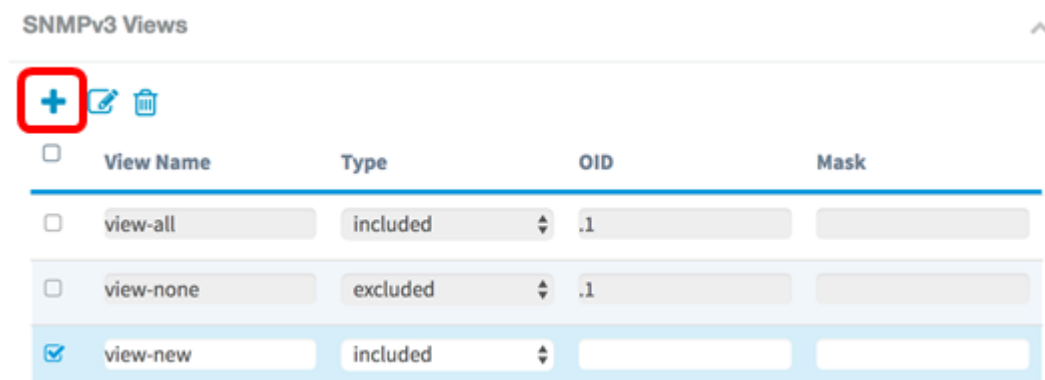
步骤2.单击“SNMP设置”右箭头。



步骤3.单击SNMPv3选项卡。



步骤4. 单击+按钮在SNMPv3视图下创建新条目。



步骤5. 在“查看名称”字段中，输入标识MIB视图的名称。

注意：在本示例中，view-new被创建为View Name。默认情况下，View-all和view-none都会创建，并包含系统支持的所有管理对象。不能修改或删除。

SNMPv3 Views

View Name	Type	OID	Mask
view-all	included	.1	
view-none	excluded	.1	
view-new	included		

步骤6.从Type下拉列表中，选择是排除还是包括视图的选项。

- included — 包括子树或子树系列中的视图（来自MIB视图）。
- excluded — 从MIB视图中排除子树或子树系列中的视图。

SNMPv3 Views

View Name	Type	OID	Mask
view-all	included	.1	
view-none	excluded	.1	
view-new	<input checked="" type="checkbox"/> included <input type="checkbox"/> excluded		

步骤7.在OID字段中，为要包括或排除在视图中的子树输入OID字符串。每个数字用于定位信息，并且每个数字对应于OID树的特定分支。OID是MIB层次结构中受管对象的唯一标识符。顶级MIB对象ID属于不同的标准组织，而低级对象ID由关联组织分配。供应商可以定义专用分支，以包括自己产品的托管对象。MIB文件将OID编号映射为可读格式。要将OID编号转换为对象名称，请单击[此处](#)。

注意：在本例中，使用1.3.6.1.2.1.1。

SNMPv3 Views

View Name	Type	OID	Mask
view-all	included	.1	
view-none	excluded	.1	
view-new	included	1.3.6.1.2.1.1	

步骤8.在Mask字段中输入OID掩码。Mask字段用于控制在确定OID所在的视图时应视为相关的OID子树的元素，最大长度为47个字符。格式为16个二进制八位数，每个二进制八位数包含两个十六进制字符，用句点或冒号分隔。要确定掩码，请计数OID元素的数量，并将这些位数设置为1。此字段仅接受十六进制格式。以示例OID 1.3.6.1.2.1.1为例，它有七个元素，因此，如果在第一个二进制八位数中设置七个连续的1后跟一个0，在第二个二进制八位数中设置

全零，则将FE:00作为掩码。

注意：在本例中，使用FE:00。

SNMPv3 Views

<input type="checkbox"/>	View Name	Type	OID	Mask
<input type="checkbox"/>	view-all	included	.1	
<input type="checkbox"/>	view-none	excluded	.1	
<input checked="" type="checkbox"/>	view-new	included	1.3.6.1.2.1.1	FE:00

步骤9. 单击 **Save**。

现在，您应该已成功配置WAP125上的SNMPv3视图。

配置SNMPv3组

步骤1. 单击**+**按钮在SNMPv3组下创建新条目。

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all

步骤2. 在Group Name字段中输入用于标识组的名称。RO和RW的默认名称不能重复使用。组名最多可包含32个字母数字字符。

注意：在本例中，使用CC。

<input type="checkbox"/>	Group Name	Security Level	Write Views	Read Views
<input type="checkbox"/>	RO	authPriv	view-none	view-all
<input type="checkbox"/>	RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/>	CC	noAuthNoPriv	view-none	view-none

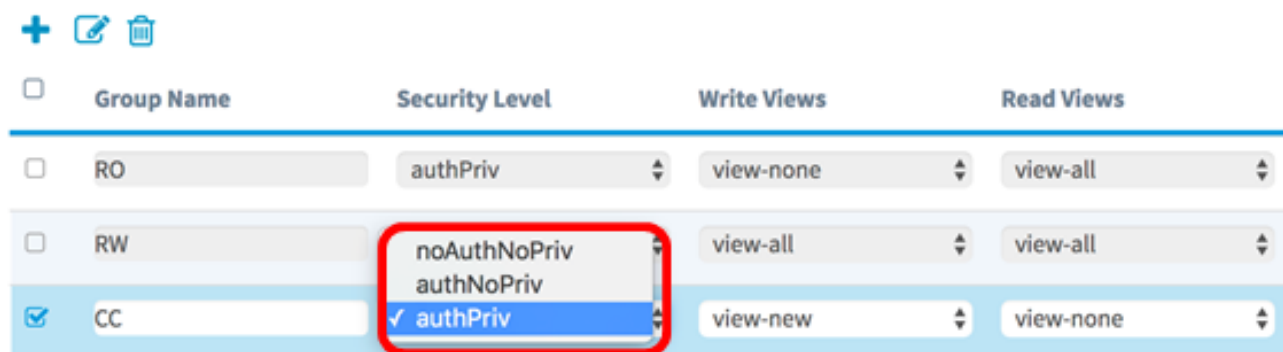
步骤3. 从Security Level下拉列表中，选择适当的身份验证级别。

- noAuthNoPriv — 不提供身份验证和数据加密（无安全）。
- authNoPriv — 提供身份验证，但无数据加密（无安全）。身份验证由安全散列身份验证(SHA)密码提供。

- authPriv — 身份验证和数据加密。身份验证由SHA密码提供。数据加密由DES密码提供。

注意：在本例中，使用authPriv。

SNMPv3 Groups

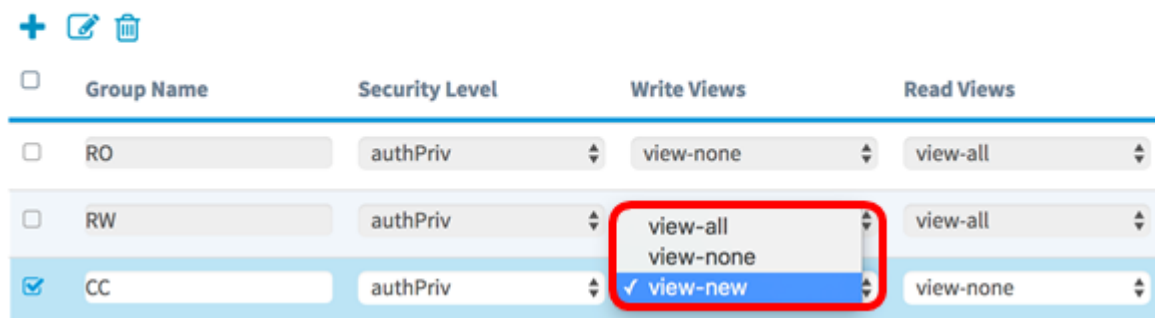


Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/> CC	authPriv	view-new	view-none

步骤4.从“写入视图”下拉列表中，选择对新组的所有管理对象(MIB)的写入访问。这定义了组可对MIB执行的操作。此列表还将包括在WAP上创建的任何新SNMP视图。

注意：在本例中，使用view-new。

SNMPv3 Groups



Group Name	Security Level	Write Views	Read Views
RO	authPriv	view-none	view-all
RW	authPriv	view-all	view-all
<input checked="" type="checkbox"/> CC	authPriv	view-new	view-none

步骤5.从“读取视图”下拉列表中选择新组的所有管理对象(MIB)的读取访问权限。下面提供的默认选项以及在WAP上创建的任何其他视图。

- view-all — 这允许组查看和读取所有MIB。
- view-none — 这会限制组，使任何人都无法查看或读取任何MIB。
- view-new — 用户创建的视图。

注意：在本例中，使用view-none。



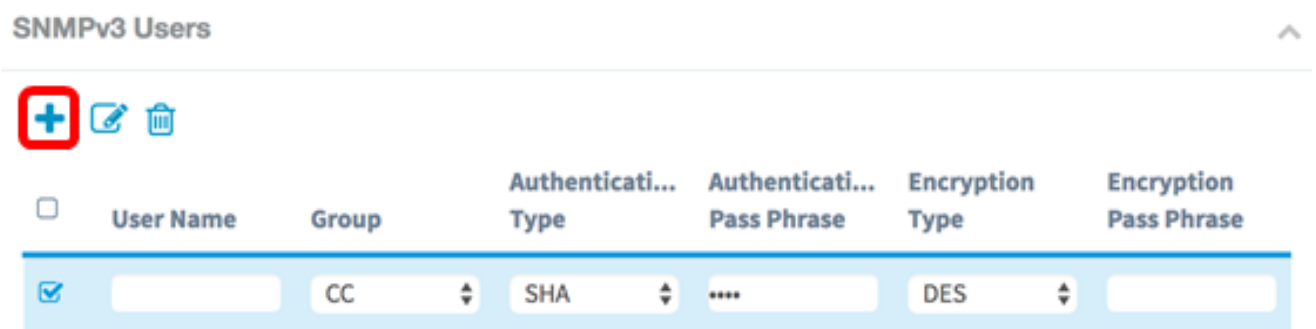
步骤6. 单击 **Save**。

您现在应该已成功配置SNMPv3组。

配置SNMPv3用户

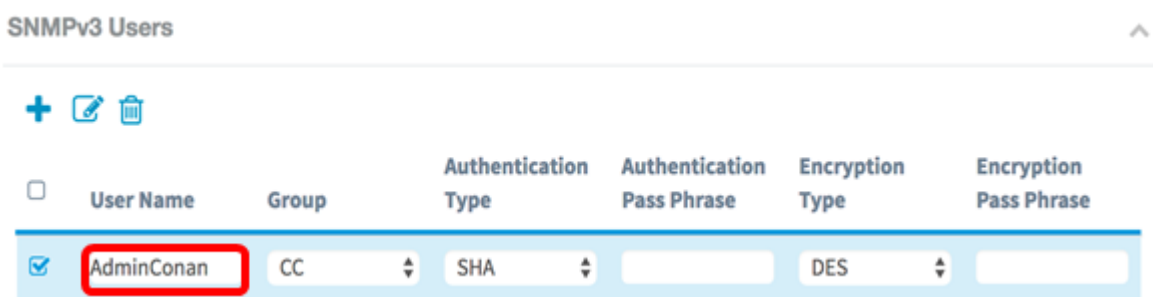
SNMP用户由其登录凭证（用户名、密码和身份验证方法）定义，并与SNMP组和引擎ID关联运行。只有SNMPv3使用SNMP用户。具有访问权限的用户与SNMP视图关联。

步骤1. 单击**+**按钮在SNMPv3 Users下创建新条目。



步骤2. 在“用户名”字段中，创建表示SNMP用户的用户名。

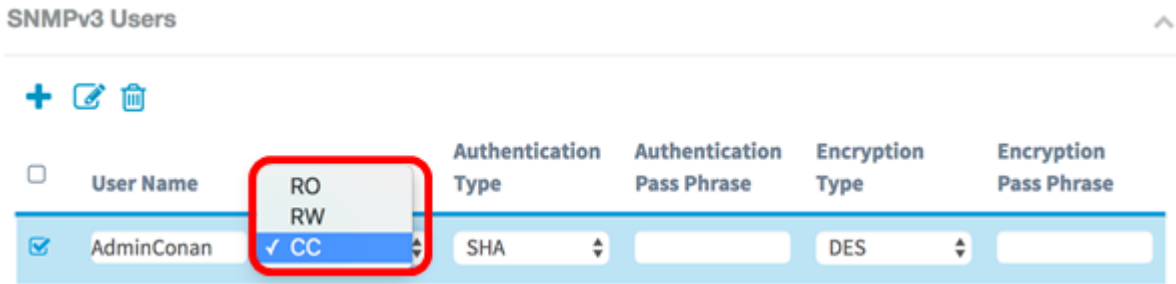
注意：在本例中，使用AdminConan。



步骤3. 从Group下拉列表中，选择要映射到用户的组。选项有：

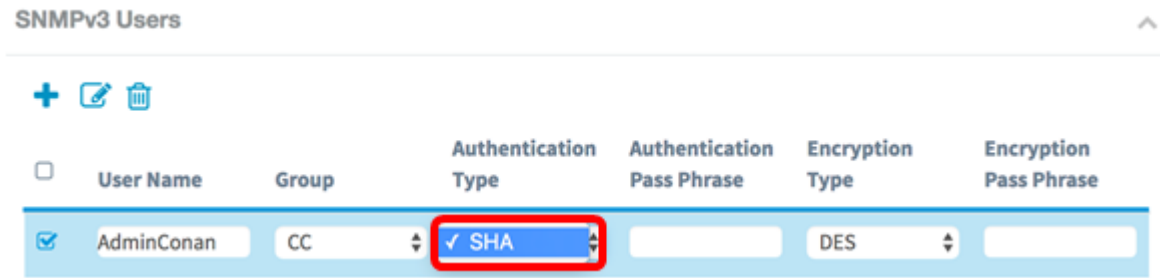
- RO — 只读组，默认创建。此组允许用户仅查看配置。
- RW — 读/写组，默认创建。此组允许用户查看配置并进行必要的更改。
- CC - CC，用户定义的组。仅当已定义组时，才会显示用户定义的组。

注意：在本示例中，CC按照步骤2中“配置SNMPv3组”的定义选择。

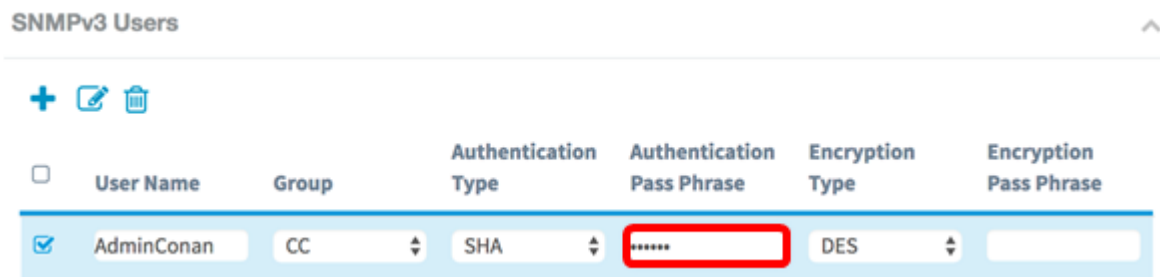


步骤4.从Authentication下拉列表中，选择SHA。

注意：如果步骤3中选择的组安全级别设置为noAuthNoPriv，则此区域将灰显。



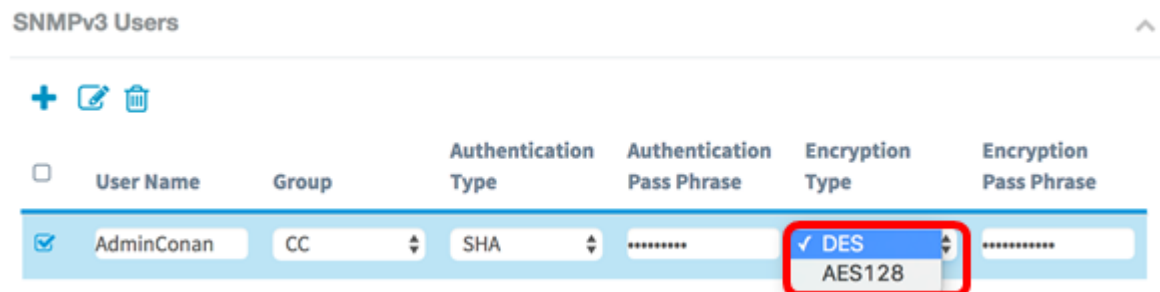
步骤5.在Authentication Pass Phrase字段中，输入用户的关联密码。这是必须配置的SNMP密码，以便对设备进行身份验证，以便它们彼此连接。



步骤6.从Encryption Type下拉菜单中，选择加密方法来加密SNMPv3请求。选项有：

- DES — 数据加密标准(DES)是使用64位共享密钥的对称分组密码。
- AES128 — 使用128位密钥的高级加密标准。

注意：在本例中，选择DES。



步骤7.在Encryption Pass Phrase字段中，输入用户的关联密码。这用于加密发送到网络中其他设备的数据。此密码还用于解密另一端的数据。通信设备中的密码必须匹配。密码长度可以介于8到32个字符之间。

SNMPv3 Users						
	User Name	Group	Authentication Type	Authentication Pass Phrase	Encryption Type	Encryption Pass Phrase
<input checked="" type="checkbox"/>	AdminConan	CC	SHA	*****	DES	*****

步骤8.单击 **Save**。

现在，您应该已在WAP125上成功配置SNMPv3用户。

配置SNMPv3目标

SNMP目标是指发送的消息和向其发送代理通知的管理设备。每个目标都由目标名称、IP地址、UDP端口和用户名标识。

SNMPv3将SNMP目标通知作为通知消息发送到SNMP管理器，而不是陷阱。这可确保目标传输，因为陷阱不使用确认，而是通知。

步骤1.单击**+**按钮，在SNMPv3 Targets下创建新条目。

注意：总共可以配置多达16个目标。

SNMPv3 Targets		
	IP Address	UDP Port
<input checked="" type="checkbox"/>		

步骤2.在IP Address字段中，输入将发送所有SNMP陷阱的目标IP地址。这通常是网络管理系统地址。这可以是IPv4或IPv6地址。

注意：在本例中，使用192.168.2.165。

SNMPv3 Targets		
	IP Address	UDP Port
<input checked="" type="checkbox"/>	192.168.2.165	

步骤3.在UDP Port字段中输入用户数据报协议(UDP)的端口号。SNMP代理检查此端口的访问请求。默认值为161。有效范围为1025到65535。

注意：在本例中，使用161。

SNMPv3 Targets

+ ✎ 🗑

<input type="checkbox"/>	IP Address	UDP Port	Users
<input checked="" type="checkbox"/>	192.168.2.165	161	AdminConan

步骤4.从Users下拉列表中选择要与目标关联的用户。此列表显示在“用户”(Users)页面上创建的所有用户的列表。

注意：选择AdminConn作为用户。

SNMPv3 Targets

+ ✎ 🗑

<input type="checkbox"/>	IP Address	UDP Port	Users
<input checked="" type="checkbox"/>	192.168.2.165	161	<input checked="" type="checkbox"/> AdminConan

步骤5.单击 [Save](#)。

现在，您应该已在WAP125和WAP581上成功配置SNMPv3目标。