配置在一个RV34x系列路由器的简单网络管理协议(SNMP)设置

客观

简单网络管理协议(SNMP)使用网络管理，排除故障和维护。SNMP在两关键软件帮助下记录，存储，并且共享信息：该网络管理的系统(NMS)在管理器设备和在可管理的设备运行的代理程序运行。RV34x系列路由器支持SNMP版本1， 2和3。

SNMP v1是缺乏某一功能和在TCP/IP网络只运作SNMP的原始版本，而SNMP v2是v1的被改进的迭代。应该为使用SNMPv1或SNMPv2C的网络只选择SNMP v1和v2c。SNMP v3是SNMP最新的标准并且解决许多SNMP v1和v2c的问题。特别是，它针对许多从v1和v2c的安全漏洞。SNMP v3也允许管理员移动向一个共同性SNMP标准。

此条款说明如何配置在RV34x系列路由器的SNMP设置。

可适用的设备

- RV34x系列

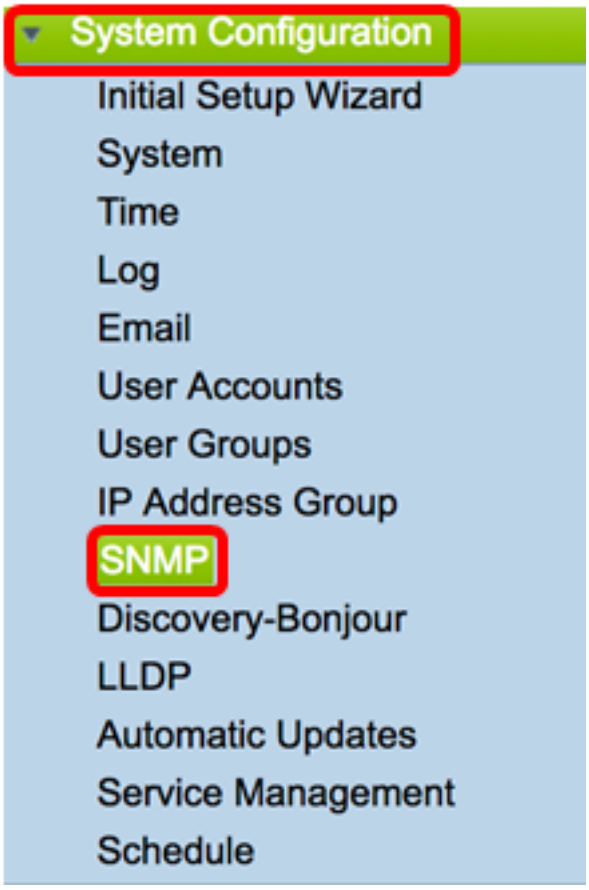
软件版本

- 1.0.1.16

配置在RV34x系列路由器的SNMP设置

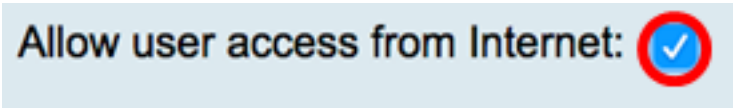
配置SNMP设置

步骤1.登陆到路由器的基于Web的工具并且选择**系统配置> SNMP**。

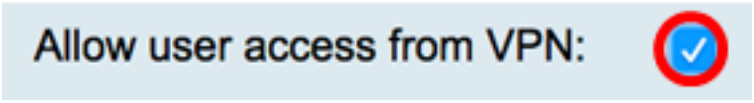


Step 2.检查**SNMP Enable复选框**对enable (event) SNMP。

第3.步(可选的)检查**Enable (event)允许从Internet复选框的用户访问**通过管理应用允许授权用户用户访问网络的外部例如Cisco FindIT网络管理。



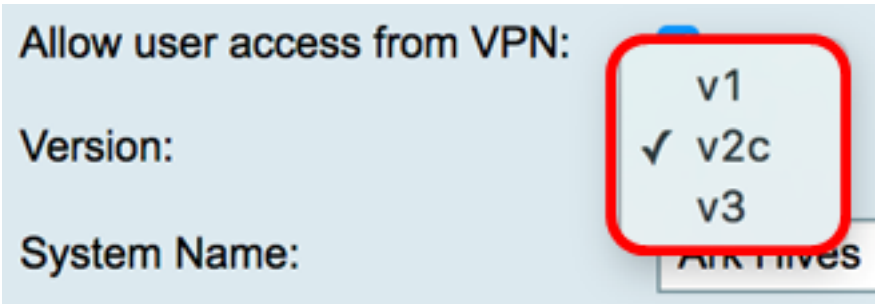
第4.步(可选的)检查**从**准许的**VPN**复选框的**允许用户访问**授权了从VPN的访问。



第 5 步：从版本下拉菜单，请选择SNMP版本使用在网络。选项是：

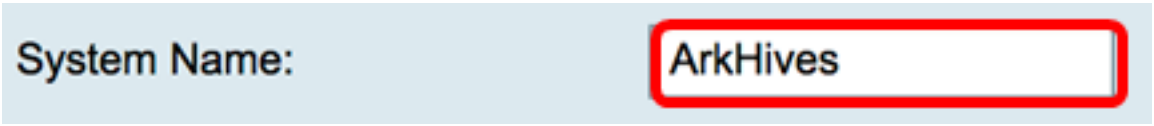
- v1 —最少安全选项。使用明文社区字符串。
- v2c — SNMPv2C提供的改进的错误处理技术支持包括区分不同种类的错误的膨胀错误代码;错误的所有类型通过在SNMPv1的一个单一错误错误代码报告。
- v3 — SNMPv3是认证策略为用户和组设置用户位于的安全模式。安全等级是允许的安全级别在安全模式内的。安全模式和安全等级的组合确定使用哪安全机制，当处理SNMP信息包时。

Note:在本例中， v2c被选择。



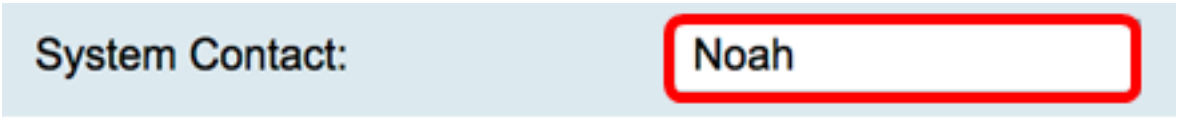
第6.步。在*系统名称*名称字段，请输入一个名字对于更加容易的证明的路由器在网络管理应用程序。

Note:在本例中， ArkHives使用作为系统名称。



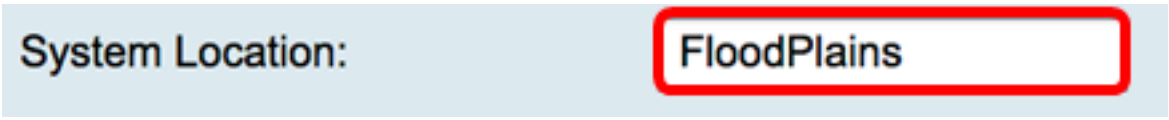
第 7 步：在*System Contact字段*，请输入单个或管理员的名字用路由器紧急情况下识别。

Note:对于此示例，诺亚使用作为系统触点。



第8.步。在*System Location字段*，请输入路由器的位置。这使找出问题容易对管理员。

Note:对于此示例，洪泛区使用作为系统位置。



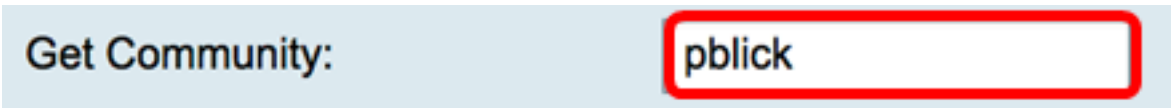
要继续进行配置，请点击在第5.步被选择的SNMP版本。

- 配置SNMP 1或v2c
- 配置SNMP v3

配置SNMP 1或v2c

第 1 步：如果SNMP v2c在第5步被选择了，请输入SNMP团体名字在*获得Community字段*。它创建用于访问SNMP代理程序信息的只读属性。在请求信息包发送的社区字符串发送由发送方必须匹配在代理程序设备的社区字符串。 只读的默认字符串是公共。

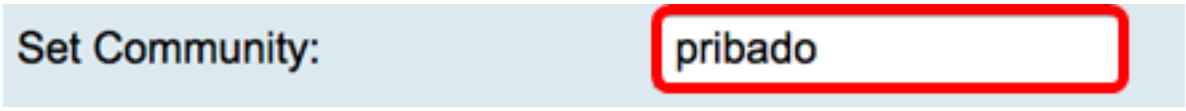
Note:只读密码产生权限检索仅信息。在本例中，使用pblick。



Step 2.在*Set community*字段，请输入SNMP团体名字。它创建用于访问SNMP代理程序信息的读写属性。从识别自己与此属性名称被接受的设备只请求。这是一个用户建立的名字。默认值是专用的。

Note:更改两个密码到定制的某事为了避免从局外人的安全攻击是可行的。在本例中，使用

pribado。



您应该成功当前配置了SNMP v1或v2设置。进行对陷井配置地区。

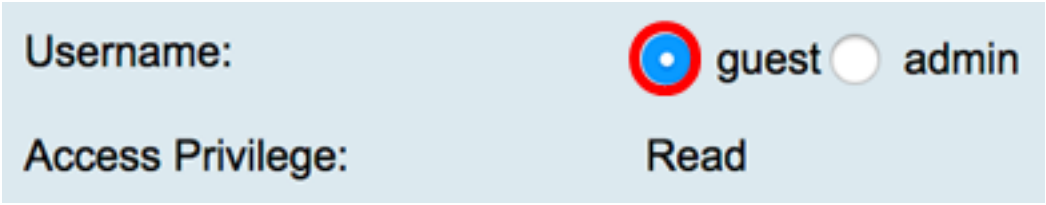
配置SNMP v3

第 1 步：如果SNMP v3被选择了，请点击一个单选按钮在用户名地区选择访问权限。选项是：

- 客户—只读权限
- Admin -读&写权限

Note:对于此示例，客户被选择。

访问权限地区根据点击的单选按钮显示权限的种类。



步骤2.点击一个单选按钮在认证算法地区选择SNMP代理程序将使用验证的方法。选项是：

- 无—没有使用用户认证。
- MD5 — message-digest算法5使用一个128-bit Hash值认证。要求用户名和密码。
- SHA1 —安全散列算法(SHA-1)是生产一160-bit摘要的一种单向散列函数算法。SHA-1比MD5计算慢，但是安全比MD5。

Note:对于此示例， MD5被选择。

Note:如果什么都没有选择，请跳过对陷井配置地区。

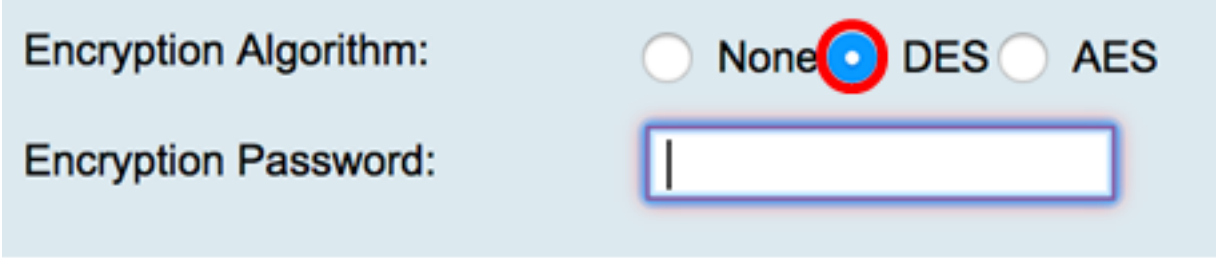
第 3 步：在*认证密码*字段，请输入密码。

第4.步(可选)在加密算法地区，点击一个单选按钮选择SNMP信息如何将被加密。选项是：

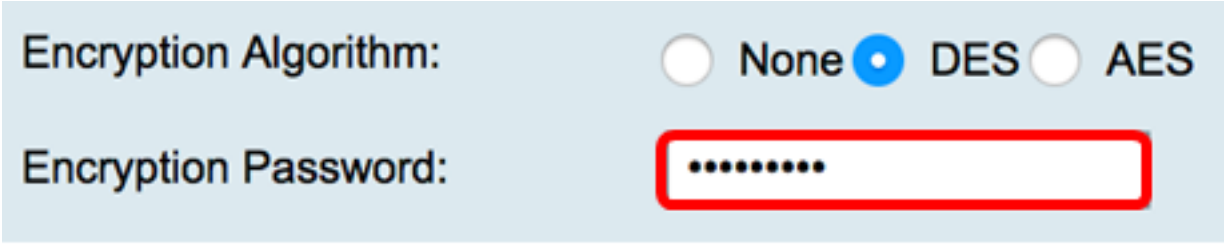
- 无—没有使用加密。如果此步骤被选择，请跳过对陷井配置地区。
- DES —数据加密标准(DES)是不安全的56位加密方法，但是可能对于向后兼容性是必需的。

- AES —高级加密标准(AES)。如果这被选择，需要加密密码。

Note:对于此示例， DES被选择。



第5.步(可选)，如果DES或AES被选择了，在*加密*密码字段输入加密密码。

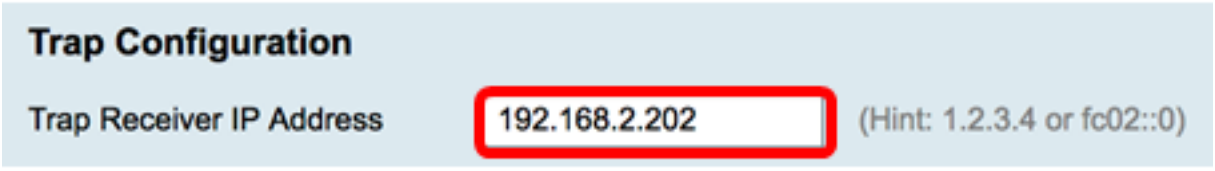


您应该顺利地当前有配置SNMP v3设置。当前进行对陷井配置地区。

设陷井配置

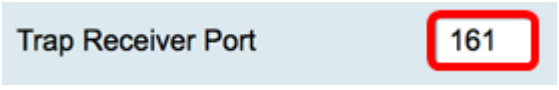
第 1 步：在*IP Address字段的陷阱接收器中*，请输入将收到SNMP陷阱的IPv4或IPv6 IP地址。

Note:对于此示例，使用192.168.2.202。

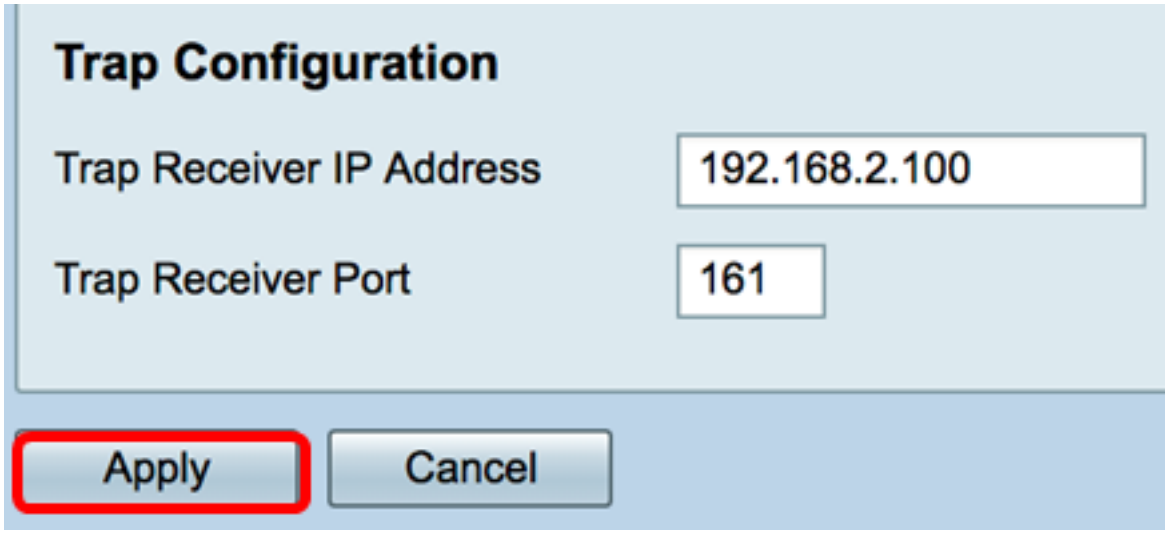


步骤2.输入用户数据报协议(UDP)端口号在*Port字段的陷阱接收器*。SNMP代理程序检查此端口访问请求。

Note:对于此示例，使用161。



步骤3.点击**适用**。



SNMP

Success. To permanently save the configuration. Go to Configuration Management page or click Save icon.

SNMP Enable:	☑
Allow user access from Internet:	☑
Allow user access from VPN:	☑
Version:	v3
System Name:	Ark Hives
System Contact:	Noah
System Location:	FloodPlains
Username:	guest admin
Access Privilege:	Read
Authentication Algorithm:	None MD5 SHA1
Authentication Password:	••••••••••••••••••••••••••••••
Encryption Algorithm:	None DES AES
Encryption Password:	••••••••••••••••••••••••••••••

Trap Configuration

Trap Receiver IP Address	192.168.2.100 (Hint: 1.2.3.4 or fc02::0)
Trap Receiver Port	161

Apply Cancel

第4.步(可选)永久保存配置，去复制/保存配置页或点击 

图标在页的上面的部分。

您应该成功当前配置了在一个RV34x系列路由器的SNMP设置。