

# 加强您的无线网络的五个提示

## 客观

无线电是创建一个无线网络无线访问访问接入点(WAP)的物理组件。在WAP的无线电设置和无线路由器控制无线电的工作情况并且确定设备传输的信号。当Wi-Fi网络是方便的时，它可能变得易受攻击对无线客户端用完带宽的和增长的安全风险，当没有适当地保护。推荐有被添加的安全的以下设置：

- 启用数据封装
- 允许仅已知设备连接到网络用媒体访问控制(MAC)过滤
- 有规律地更改无线网络密码
- Enable (event)内置防火墙
- 隐藏服务集标识(SSID)

此条款打算提供是有用的在巩固您的无线网络的提示。

## 可适用的设备

- RV系列
- 无线访问访问接入点
- Cisco Unified通信

## 加强您的无线网络

### 启用数据封装

无线网络设备典型地支持某种加密能安全地连接到无线网络。若情况许可，使用Wi-Fi保护访问(WPA)或Wi-Fi受保护的访问2 (WPA2)，他们提供更好的安全高级加密标准(AES)加密方法。在启用数据加密的步骤每个设备轻微有所不同。对于[enable \(event\)无线安全一个指南在无线路由器，请点击此处。](#)对于[enable \(event\)无线安全一个指南在接入点，请点击此处。](#)

### 允许有MAC过滤的仅已知设备

MAC地址过滤让您列出在无线客户端的MAC地址下被联络到您的网络，有效建立一份知道设备清单。您能根据您的需求然后准许或拒绝对网络的设备访问。MAC地址不在列表从情况自动地被排除。在启用MAC地址过滤的步骤每个设备轻微有所不同。对于过滤在[无线路由器的enable \(event\) MAC一个指南，请点击此处。](#)对于过滤在[无线访问访问接入点的enable \(event\) MAC一个指南，请点击此处。](#)

### 有规律地更改无线网络密码

设置无线网络密码是巩固无线网络的简便的方法。他们经常需要与在网络的其他无线访问访问接入点同步，无缝的无线连接的。无线网络密码典型地需要有规律地更改保证仅被核准的设备被连接到网络。在设置无线网络密码的步骤每个设备轻微有所不同。[对于关于怎样的一个指南配置在路由器的无线设置，请点击此处。](#)对于在更改密码的一个指南在[接入点，请点击此处。](#)

### Enable (event)内置防火墙

许多无线路由器，例如RV130W无线N VPN路由器，有防止恶意流量进入您的网络的内置防火墙。在启用防火墙的步骤每个设备轻微有所不同。对于在启用[防火墙的一个指南在路由器，请点击此处。](#)

## 隐藏SSID

当搜索无线网络时，禁用SSID广播使您的网络无形对设备。类似设置，因为连接在设备，将必须手工被配置一个无线密码，隐藏SSID使连接到您的无线网络更加困难。在禁用SSID广播的步骤每个设备轻微有所不同。对于在禁用[SSID广播的一个指南在接入点，请点击此处。](#)对于在禁用[SSID广播的一个指南在无线路由器，请点击此处。](#)