CVR100W VPN路由器的基本无线设置

目标

无线局域网(WLAN)利用无线通信将无线设备连接到LAN。例如，咖啡馆的Wi-Fi热点。无线网络非常有用，因为它降低了布线成本，而且易于设置。

本文介绍如何在CVR100W VPN路由器上配置基本无线设置，包括网络安全配置。有关高级无线设置，请参阅“Advanced Wireless Configuration on the CVR100W VPN Router(CVR100W VPN路由器上的*高级无线配置)”一文*。

适用设备

·CVR100W VPN路由器

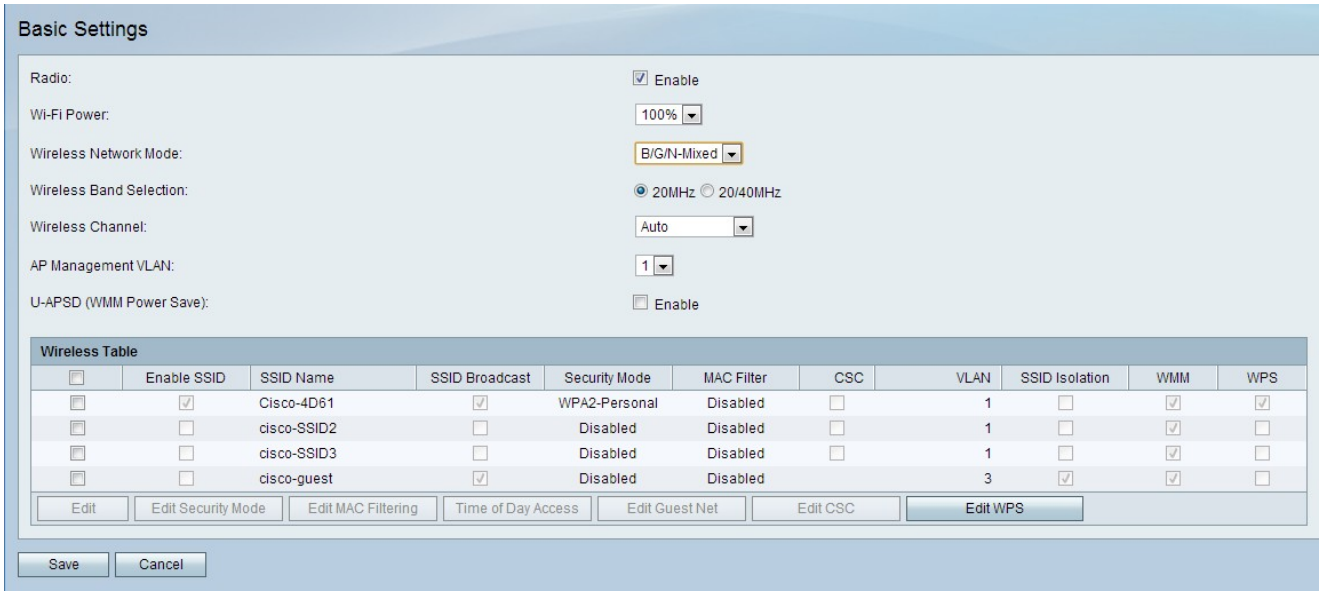
软件版本

•1.0.1.19

基本设置配置

常规设置

步骤1.登录Web配置实用程序并选择Wireless > **Basic Settings**。“*基本设置*”页打开：



步骤2.选中Radio（无线电）字段中的**Enable**复选框以启用无线电。

步骤3.从Wi-Fi电源下拉列表中选择wi-fi电源。此wi-fi功率控制wi-fi无线电的发射器功率。此功能有助于减小或增加信号范围。此功能用于节省电源。

·100% — 此选项可实现100%无线电发射器功率。

·50% — 此选项可实现50%的无线电发射器功率。

步骤4.从Wireless Network Mode下拉列表中选择无线模式。此选项基于网络中设备的无线功能。

·B/G/N-Mixed — 网络由无线 — B、无线 — G和无线 — N设备组成。

·仅B — 网络仅包含无线B设备。

·仅G-Only — 网络仅包含无线G设备。

·仅N — 网络仅包含Wireless-N设备。

·B/G-Mixed — 网络由无线B和无线G设备组成。

·G/N混合 — 网络由无线 — G和无线 — N设备组成。

步骤5.如果网络模式由Wireless-N设备组成，请在Wireless Band Selection（无线频段选择）字段中点击与无线信号所需带宽对应的单选按钮。带宽越高，表示信号可以承载的数据量越大。

·20 MHz — 无线信号的标准频率。

·20/40 MHz — 自动使用20 MHz和40 MHz信号。40 MHz信号提供更多带宽，但易受更多干扰。仅当连接的无线设备与40 MHz频率兼容时，才使用此选项。

步骤6.从Wireless Channel下拉列表中为无线电选择无线信道。选择邻居网络当前未使用的信道。如果多个无线电使用同一信道，则可能会发生干扰。

步骤7.从AP Management VLAN下拉列表中，选择管理VLAN。管理VLAN是用于从远程位置管理设备的VLAN。

步骤8.（可选）要启用非计划自动节电传送(U-APSD)，请在U-APSD字段中选**中启**用。U-APSD是允许无线电节能的功能。但是，U-APSD可能会降低无线电的吞吐量性能。

步骤9.单击“保**存**”。

编辑无线表

步骤1.选中Wireless Table（无线表）中要编辑的网络的复选框。

步骤2.单击“**编辑**”以编辑指定的网络。

步骤3.选中**Enable SSID** 复选框以启用网络。服务集标识符(SSID)是无线网络的名称。

步骤4.在SSID Name字段中，输入网络名称。网络上的所有设备都使用此SSID相互通信。

步骤5.选中SSID Broadcast**复选框**以启用无线广播。启用SSID广播后，CVR100W VPN路由器的可用性会通告给附近的无线设备。

步骤6.（可选）要编辑安全模式，请参阅编辑安全模式。

步骤7.（可选）要编辑MAC过滤器，请参阅编辑MAC过滤。

步骤8.（可选）要启用Cisco Simple Connect(CSC)，请选中**CSC**复选框。CSC可轻松设置无线网络，并允许将无线设备轻松连接到网络。无线设备使用CSC获取网络的SSID和密码，这允许自动连接到网络。要编辑CSC，请参阅编辑CSC。

注意：Cisco Simple Connect的VLAN不能与当前或其他SSID的VLAN相同。

步骤9.从VLAN下拉列表中选择与网络关联的VLAN。

步骤10.选中**SSID Isolation**复选框，以防止指定网络上的设备相互通信。

步骤11.选**中WMM**以在网络上启用Wi-Fi多媒体(WMM)。WMM用于增强无线设备上的多媒体流。启用WMM时，通过无线连接发送的多媒体流量会获得更高的优先级。

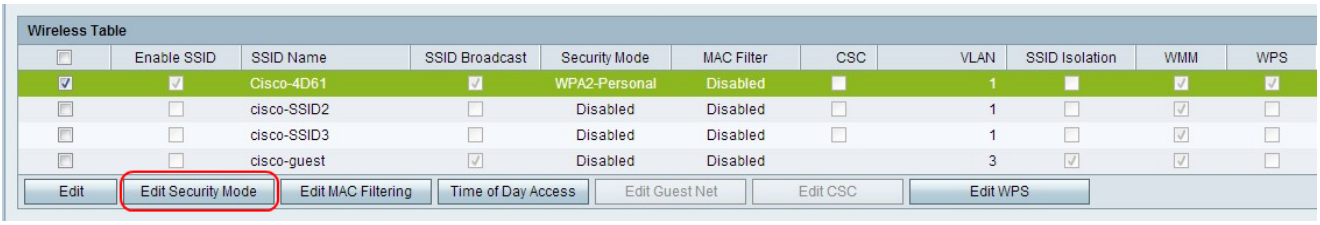
步骤12.选**中WPS**，将指定的网络指定为Wi-Fi保护设置(WPS)网络。WPS是允许轻松安全地配置网络的功能。此功能允许设备轻松连接到网络。

注意：要在CVR100W VPN路由器上配置WPS，请参阅CVR100W VPN路由器上的“*WiFi Protected Setup(WPS)”一文*。

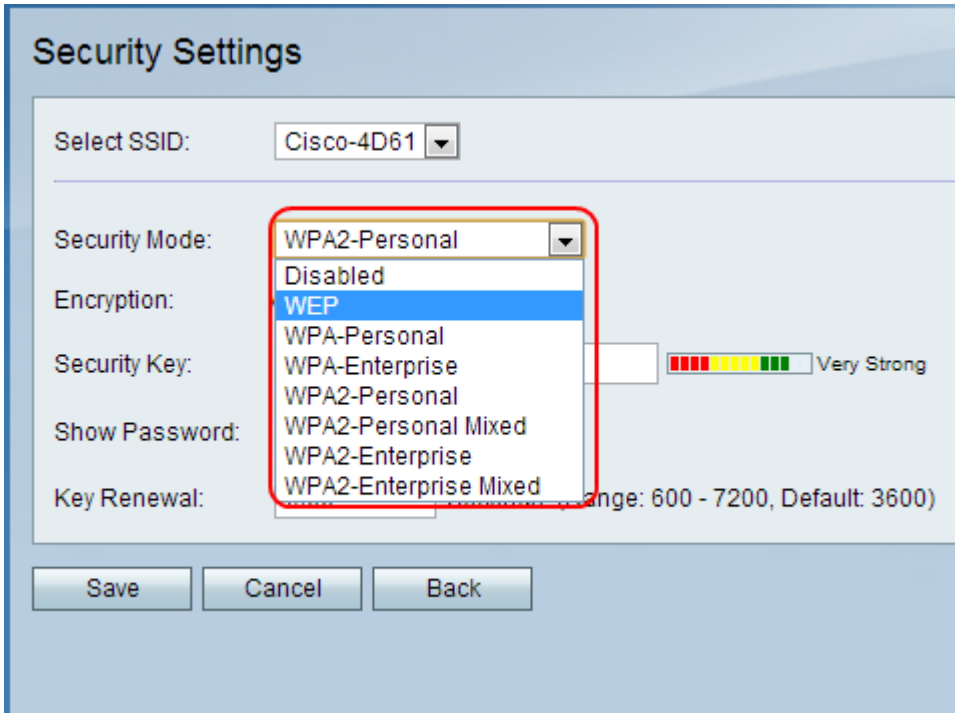
步骤13.单击“保**存”**。

编辑安全模式

步骤1.选中Wireless Table（无线表）中要编辑的网络的复选框。



步骤2.单击**Edit Security Mode**以编辑指定网络的安全。系统将*打开“安全设置”*页。



步骤3.（可选）要更改要为其配置安全的SSID，请从Select SSID下拉列表中选择所需的SSID。

步骤4.从Security Mode下拉列表中选择要配置的安全模式。

·禁用安全性 — 此选项禁用CVR100W VPN路由器上的安全性。

·WEP安全 — 有线等效保密(WEP)是用于保护无线网络的算法。WEP用于提供比WPA安全性低的基本加密方法。当连接的网络设备不支持WPA时，使用WEP。

·WPA — 个人安全 — Wi-Fi保护访问(WPA)是无线网络的安全标准。WPA-Personal是WPA的一个版本，用于由几个用户组成的网络。WPA-Personal提供每个用户用于访问无线网络的共享密钥。WPA是通过密钥加密方法临时密钥完整性协议(TKIP)和高级加密标准(AES)引入的。

·WPA — 企业安全— WPA — 企业是WPA的一个版本，建议在包含大量用户的网络中使用。RADIUS服务器控制用于访问网络的身份验证。每个连接的用户都有访问无线网络的唯一密钥。WPA是通过密钥加密方法临时密钥完整性协议(TKIP)和高级加密标准(AES)引入的。

·WPA2 — 个人安全— WPA2是WPA的增强功能，它提供比WPA更高的安全性。WPA2-Personal是WPA2的一个版本，用于用户较少的网络。WPA2 — 个人比WPA2 — 个人混合更安全。WPA2-Personal提供每个用户用于访问无线网络的共享密钥。

·WPA2 — 个人混合安全— WPA2 — 个人混合是WPA2的一个版本，用于用户较少的网络。WPA2 — 个人混合支持不能使用WPA2的旧设备向后兼容。WPA2 — 个人混合是安全性较低的连接。

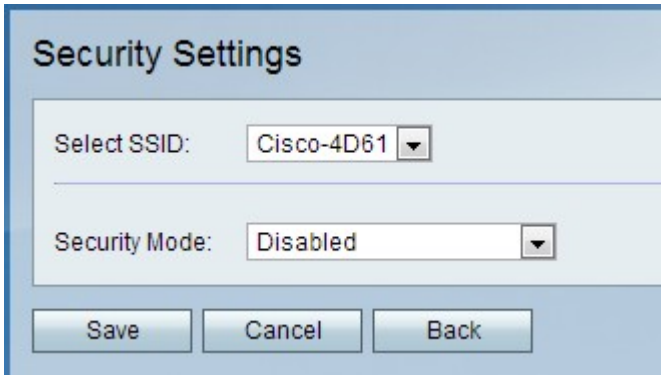
·WPA2 — 企业安全— WPA2 — 企业是WPA2的一个版本，用于拥有大量用户的网络。WPA2-Enterprise比WPA2-Enterprise混合更安全。用于获取访问的身份验证由RADIUS服务器控制。这意味着每个连接的用户将获得访问无线网络的唯一密钥。

·WPA2 — 企业混合安全— WPA2 — 企业混合是WPA2的版本，用于拥有大量用户的网络。WPA2 — 企业混合支持不能使用WPA2的旧设备向后兼容。WPA2 — 企业混合提供的连接比WPA2 — 企业不安全。用于获取访问的身份验证由RADIUS服务器控制。这意味着每个连接的用户将获得访问无线网络的唯一密钥。

禁用安全

在CVR100W VPN路由器上，为了在设置测试网络时易于使用，可能会禁用无线安全。

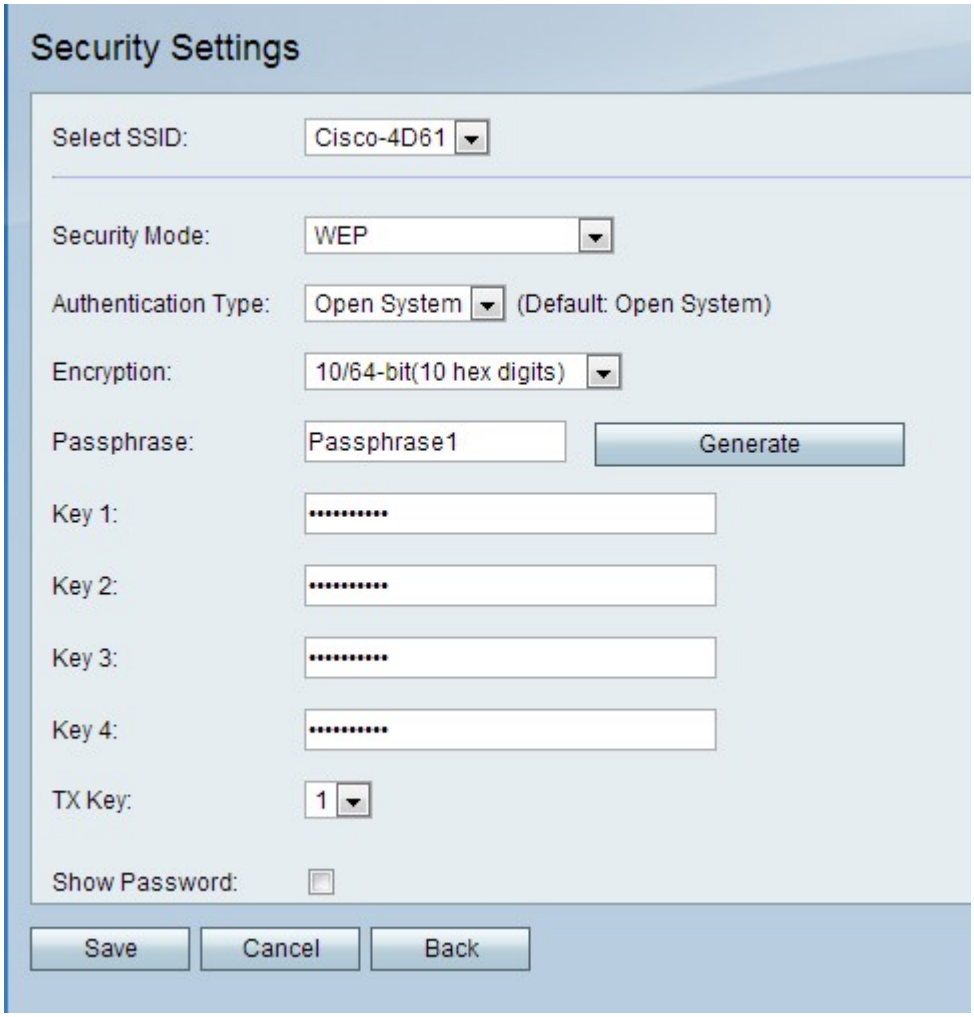
注意：不建议禁用安全。



步骤1.从Security Mode下拉列表中选择**Disabled**。无线网络的安全性已禁用。

步骤2.单击“保**存**”。

配置WEP安全



步骤1.从Security Mode下拉列表中选择**WEP**。

步骤2.从Authentication Type下拉列表中，选择无线网络的身份验证类型。

·开放系统 — 任何网络设备都可与接入点关联，但通过接入点传递流量需要WEP密钥。

·共享密钥 — 需要WEP密钥才能与接入点关联。它还用于通过接入点传递流量。

步骤3.从Encryption下拉列表中，选择WEP密钥的加密方法。

·10/64位（10个十六进制数字） — 提供40位密钥。

·26/128位（26个十六进制数字） — 提供104位密钥。此选项更安全。

步骤4.在Passphrase字段中，输入大于8个字符的密码。密码短语有助于使网络安全设置更易于记忆。

步骤5.单击**Generate**在Key 1、Key 2、Key 3和Key 4字段中创建密钥。

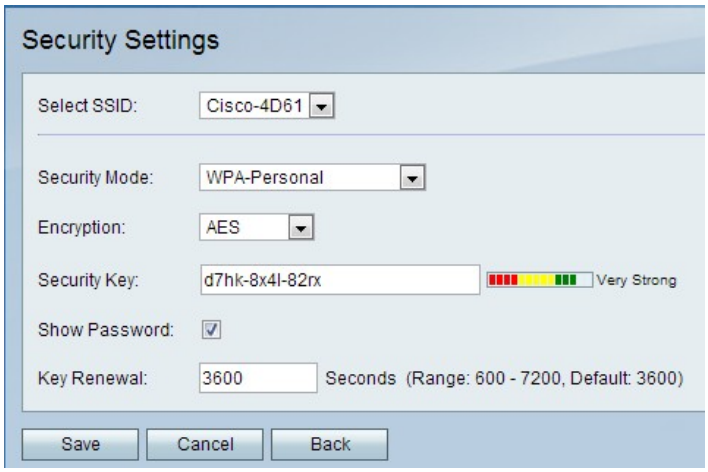
注意：您还可以在密钥1、密钥2、密钥3和密钥4字段中手动输入密钥。

步骤6.从TX Key下拉列表中，选择用户访问无线网络必须输入的密钥。

步骤7.（可选）选中Show **Password复**选框以显示密钥的字符串。

步骤8.单击“保**存**”。

配置WPA — 个人安全



步骤1.从Security Mode下拉列表中选择**WPA-Personal**。

步骤2.从Encryption下拉列表中，为WPA密钥选择加密方法。

·TKIP/AES — 当连接到无线网络的设备不全都支持AES时，选择此选项。

·AES — 如果连接到无线网络的所有设备都支持AES，则此选项是首选的。

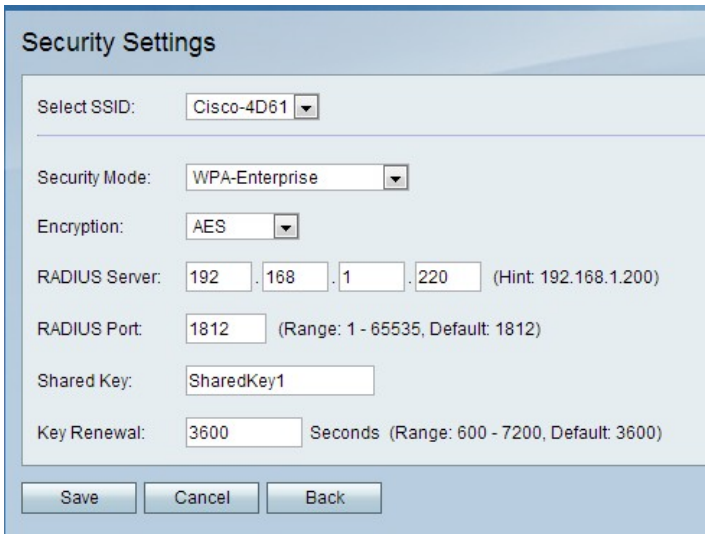
步骤3.在Security Key字段中输入安全密钥。安全密钥是由字母和数字组成的密码短语。设备使用安全密钥连接到网络。

步骤4.（可选）要显示密钥的字符串，请选中**Show Password**复选框。

步骤5.在Key Renewal字段中，输入CVR100W VPN路由器在生成新密钥之前使用密钥的时间（以秒为单位）。

步骤6.单击“保**存**”。

配置WPA-Enterprise安全



步骤1.从Security Mode下拉列表中选择**WPA-Enterprise**。

步骤2.从Encryption下拉列表中，为WPA密钥选择加密方法。

·TKIP/AES — 当连接到无线网络的设备不全都支持AES时，选择此选项。

·AES — 如果连接到无线网络的所有设备都支持AES，则此选项是首选的。

步骤3.在RADIUS Server字段中，输入RADIUS服务器的IP地址。

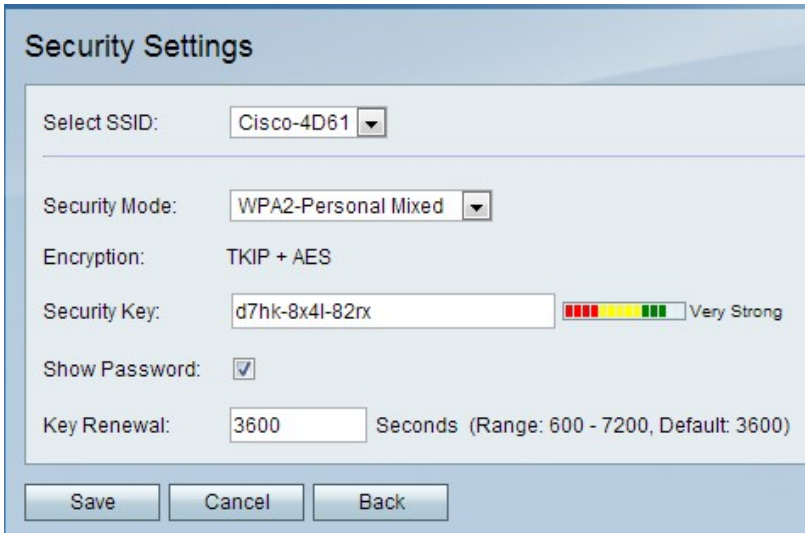
步骤4.在RADIUS Port字段中，输入用于访问RADIUS服务器的端口号。

步骤5.在Shared Key字段中，输入无线用户的预共享密钥。预共享密钥是所有用户使用的密钥。预共享密钥功能是新增的安全功能。

步骤6.在Key Renewal字段中，输入CVR100W VPN路由器在生成新密钥之前使用密钥的时间（以秒为单位）。

步骤7.单击**“保存”**。

配置WPA2 — 个人/WPA2 — 个人混合安全



步骤1.从Security Mode下拉列表中，选择**WPA2-Personal**或WPA2-**Personal Mixed**。

注意：当无线网络上的所有设备都支持AES时，使用WPA2 — 个人。当网络上的设备不全都支持AES时，会使用WPA2 — 个人混合。安全方法使用的加密类型显示在Encryption字段中。

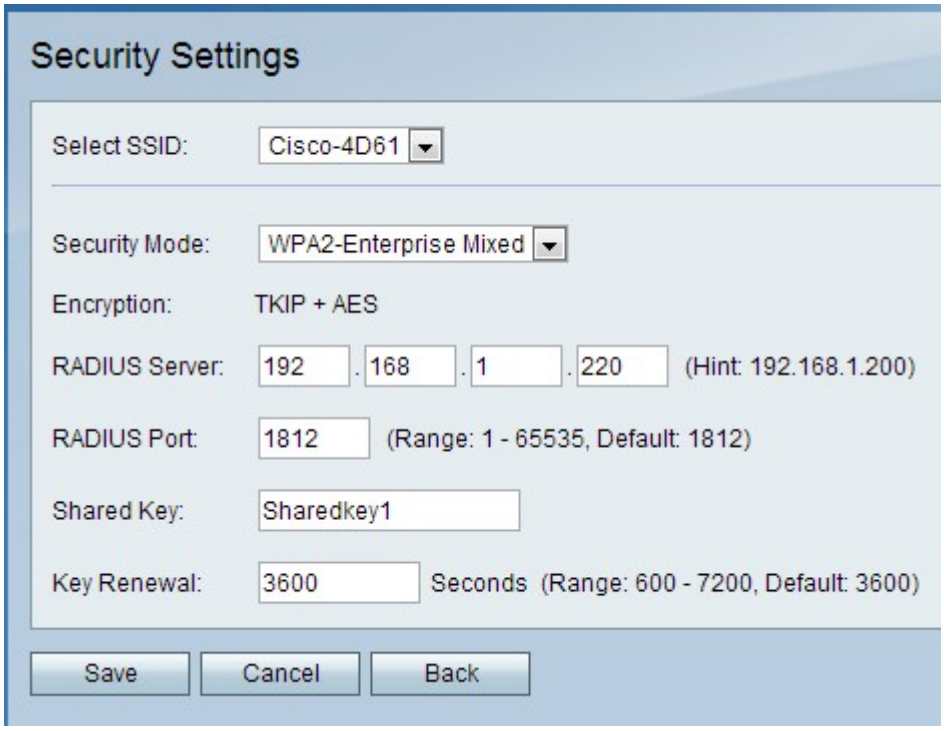
步骤2.在Security Key字段中，输入安全密钥。安全密钥是由字母和数字组成的密码短语。设备使用安全密钥连接到网络。

步骤3.（可选）要查看密钥的字符串，请选中**Show Password**复选框。

步骤4.在Key Renewal字段中，输入CVR100W VPN路由器在生成新密钥之前使用密钥的时间（以秒为单位）。

步骤5.单击**Save**。

配置WPA2-Enterprise/WPA2-Enterprise混合安全



步骤1.从Security Mode下拉列表中，选择**WPA2-Enterprise**或WPA2-**Enterprise Mixed**。

注意：当无线网络上的所有设备都支持AES时，使用WPA2-Enterprise。当网络上的设备不全都支持AES时，会使用WPA2 — 企业混合。安全方法使用的加密类型显示在Encryption字段中。

步骤2.在RADIUS Server字段中，输入RADIUS服务器的IP地址。

步骤3.在RADIUS Port字段中，输入用于访问RADIUS服务器的端口号。

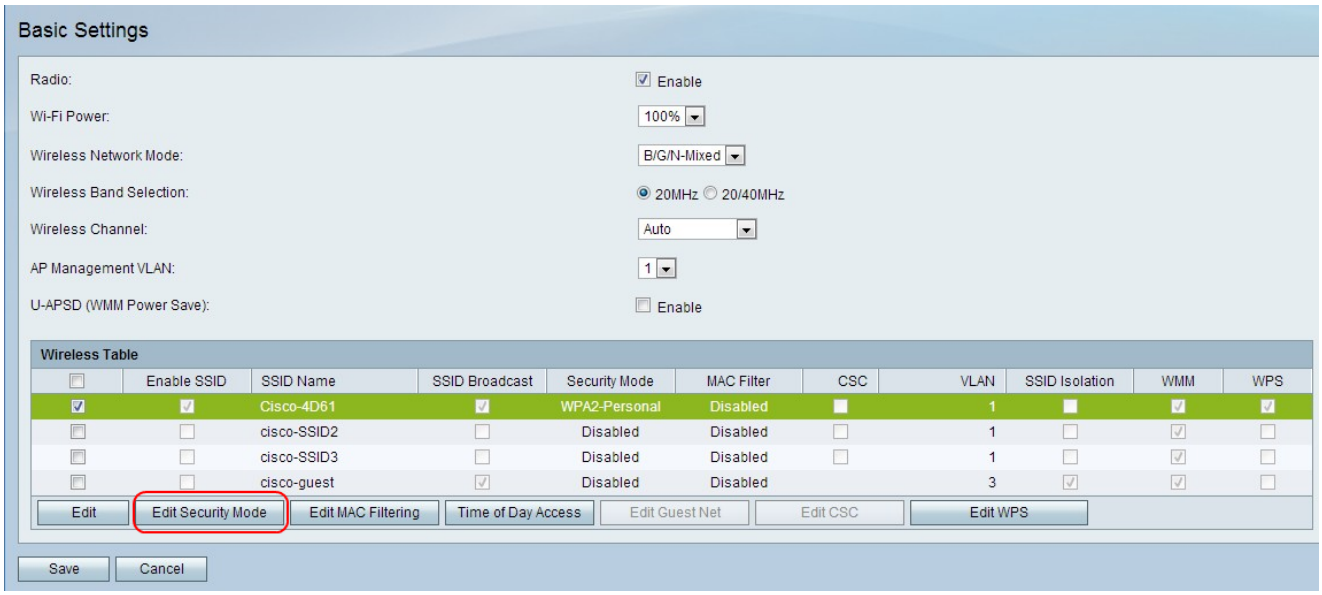
步骤4.在Shared Key字段中，输入无线用户的预共享密钥。预共享密钥是所有用户使用的密钥。预共享密钥功能是新增的安全功能。

步骤5.在Key Renewal字段中，输入CVR100W VPN路由器在生成新密钥之前使用密钥的时间（以秒为单位）。

步骤6.单击“保存”。

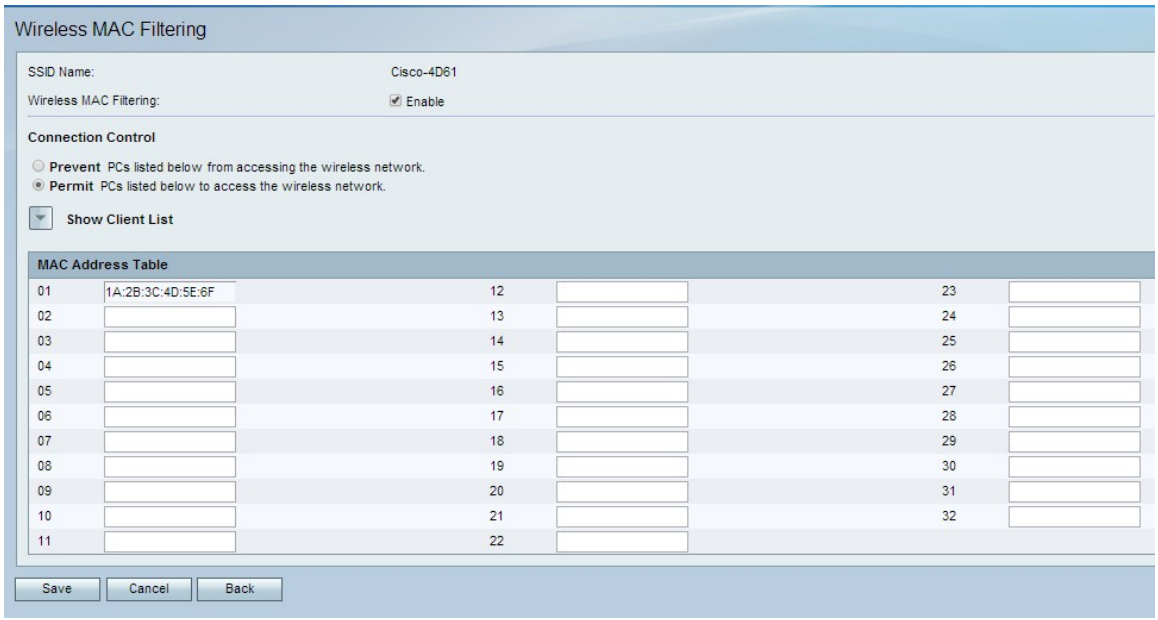
编辑MAC过滤

MAC过滤用于根据连接设备的MAC地址允许或拒绝对无线网络的访问。



步骤1.选中要编辑的网络复选框。

步骤2.单击**Edit MAC Filtering**为指定网络创建MAC访问控制列表。“*无线MAC过滤器*”页打开：



步骤3.选中**Enable**以在网络上启用MAC过滤。

步骤4.点击与Connection Control字段中所需列表类型对应的单选按钮。

·阻止PC — 阻止具有所列MAC地址的PC进入网络。

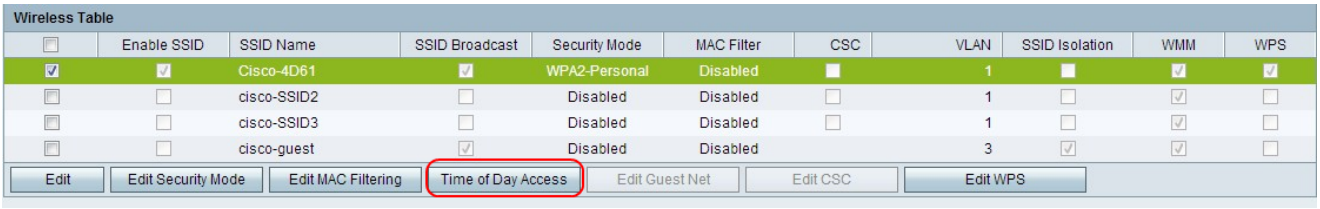
·允许PC — 允许具有所列MAC地址的PC进入网络。

步骤5.在MAC地址表中，输入所需的MAC地址。

步骤6.单击“保存”。

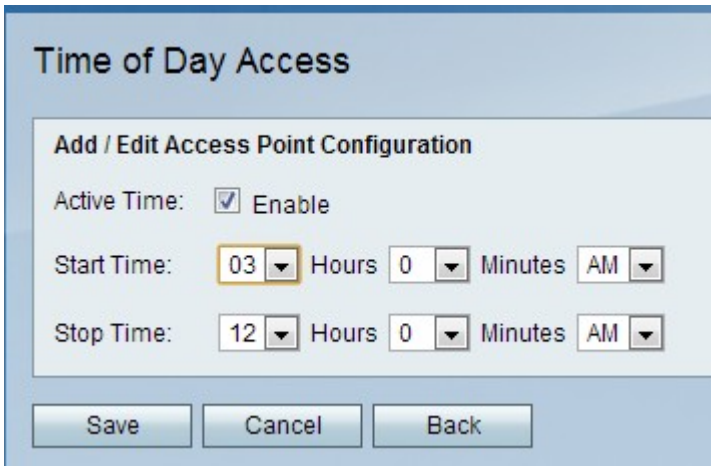
一天中的访问时间

Time of Access功能用于根据已配置的计划允许用户访问。



步骤1.选中要编辑的网络复选框。

步骤2.单击**Time of Day Access以配**置用户何时可以访问指定网络。此时*将打开"访问时*间"页：



步骤3.在Active Time字段中选中**Enable**，以启用网络的一天中的访问时间。

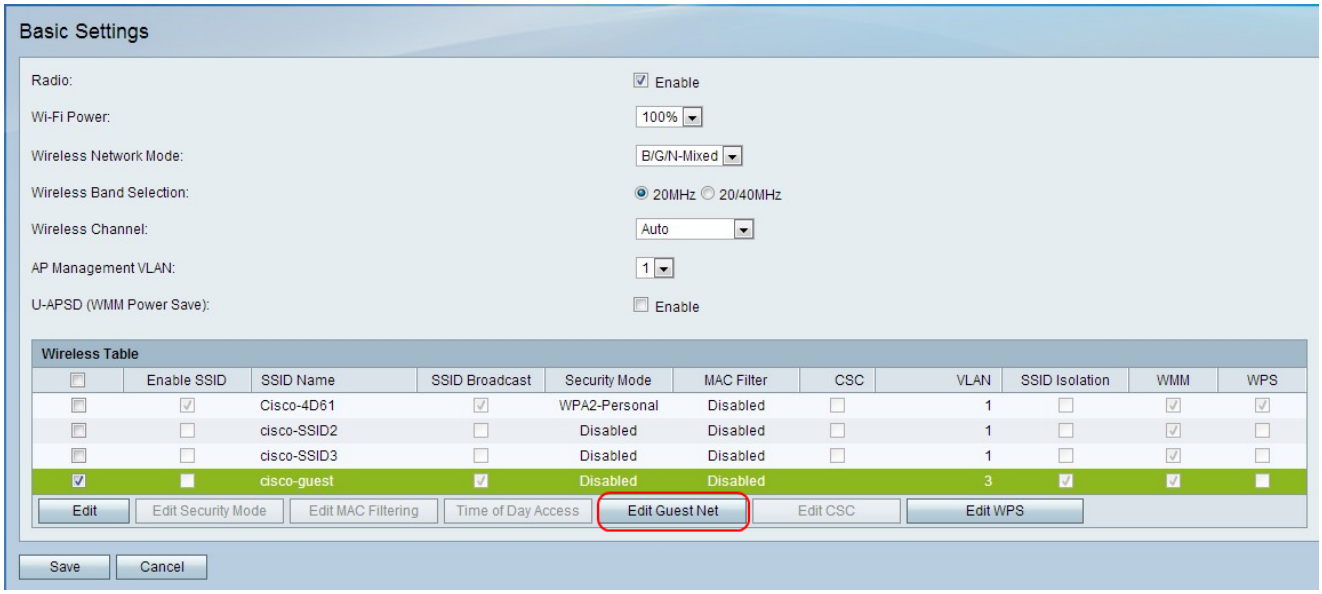
步骤4.在Start Time字段中，输入网络访问开始的时间。

步骤5.在Stop Time字段中，输入网络访问结束的时间。

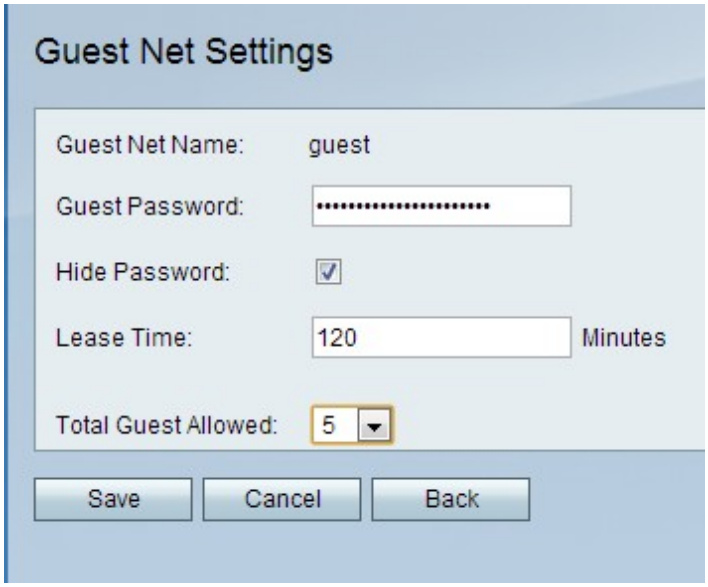
步骤6.单击"保**存**"。

编辑访客网络

访客网络是专为临时用户设计的网络的一部分。这用于允许访客访问网络，而无需公开私有Wi-Fi密钥。访客网络可以配置为限制用户的访问时间和带宽使用。



步骤1.单击**Edit Guest Network**以配置访客网络。“访*客网络设置*”页打开：



步骤2.在Guest Password字段中，输入用户将用于进入访客网络的密码。

步骤3.（可选）要在页面上隐藏密码，请选中Hide Password字段中的复选框。

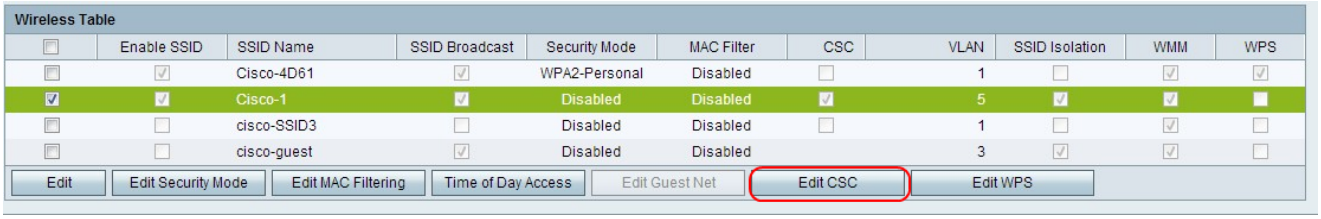
步骤4.在Lease Time字段中，输入允许用户保持与访客网络连接的时间（以分钟为单位）。

步骤5.从Total Guest Allowed下拉列表中，选择允许的访客总数。

步骤6.单击“保**存**”。

编辑CSC

CSC可轻松设置无线网络，并允许将无线设备轻松连接到网络。无线设备使用CSC获取网络的SSID和密码，这允许自动连接到网络。



步骤1.选中要编辑的网络复选框。

步骤2.单击“**编辑CSC”**以编辑Cisco Simple Connect。

步骤3.选中CSC复选框。

步骤4.从VLAN下拉列表中选择用于CSC的VLAN。

注意：Cisco Simple Connect VLAN不能与当前或其他SSID VLAN相同。要创建新的VLAN，请参阅“CVR100W路*由器上的VLAN成员身份”一文*。

注意：CSC只能对SSID1使用无线分发系统(WDS)。请参阅CVR100W路由器上的*无线分发系统(WDS)文章*。

步骤5.单击**Save**。