# 在RV016、RV042、RV042G和RV082 VPN路由器的一般防火墙设置

## 客观

防火墙保护一个内部网络免受一个外部网络例如互联网。防火墙对网络安全是重要的。几个不同的设置是可用的能enable (event)或禁用根据您的安全需要的特定服务。

此条款目标如何将显示enable (event)或禁用在RV016、RV042、RV042G和RV082 VPN路由器的一般防火墙设置。

## 可适用的设备

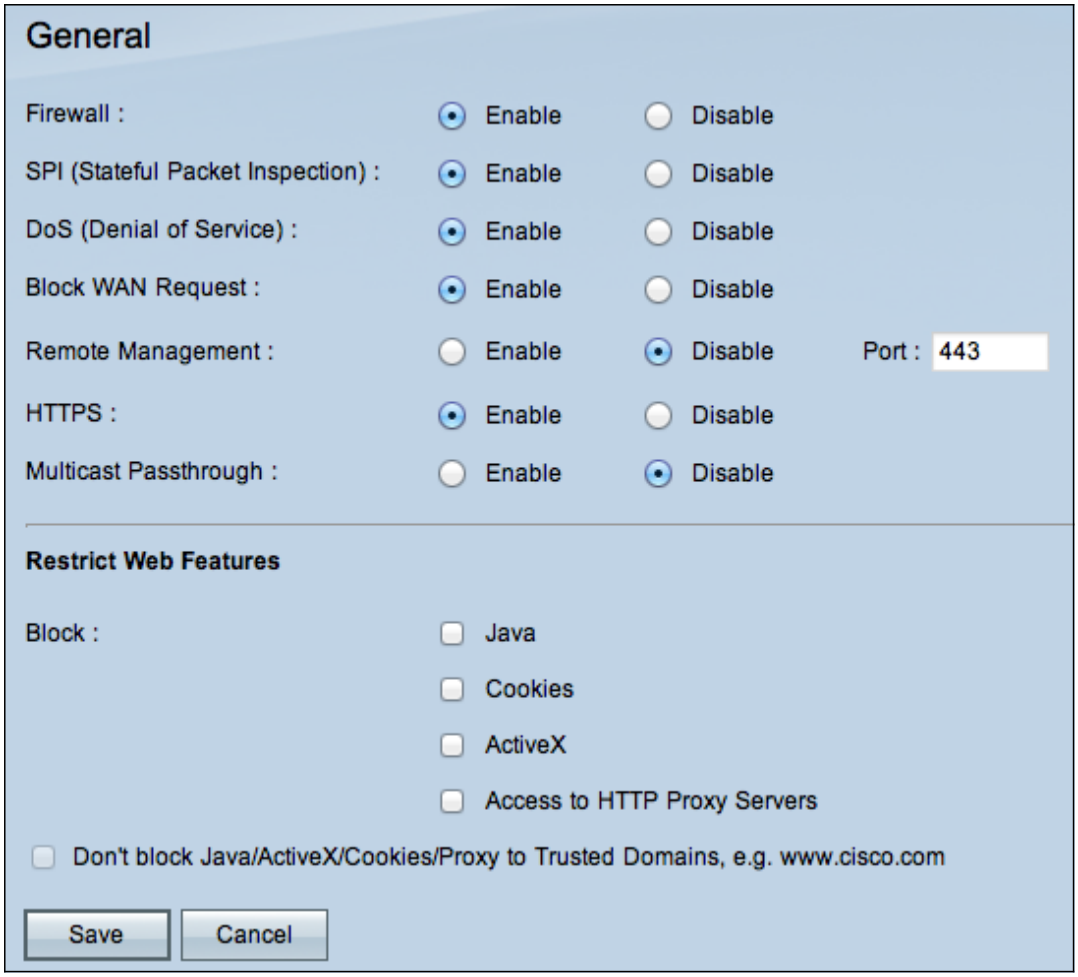
- RV016
- RV042
- RV042G
- RV082

## 软件版本

- v4.2.1.02

## 一般防火墙设置

步骤1.登陆路由器配置工具并且选择**防火墙>General**。*一般*页打开：




步骤2.点击**Enable (event)**或**禁用**单选按钮对enable (event)或根据用户需求禁用在防火墙的可用的设置。

以下字段被描述如下：

•防火墙—当此功能是启用的，路由器将执行在通过此路由器的所有数据流的深度信息包检验并且丢弃不跟随预定义的协议工作情况的信息包。

•SPI (有状态的信息包检验) —路由器的防火墙使用有状态的信息包检验(SPI)查看数据流在防火墙。它监控网络连接状态例如TCP流和UDP通信。 防火墙区分不同的连接类型的合法信息包，并且匹配已知激活连接由防火墙允许仅的信息包，所有其他被拒绝。

•Dos (拒绝服务) —当此功能是启用的，路由器将防止来自互联网的DOS (拒绝服务)攻击。DOS攻击造成您的路由器CPU是繁忙的，以便不能为定期数据流提供服务。

•块广域网请求—当这是启用的，路由器将忽略自互联网的ping请求，因此将看起来被隐藏。这帮助通过隐瞒网络端口提供安全，因此侵入者没容易地有对网络的访问。

•远程管理—当此功能是启用的时，路由器允许Web配置工具从互联网被获取。输入对在广域网端的主机将被打开的端口号。默认设置是443。此端口，当用户建立远程连接时，必须指定。

•HTTPS —当启用， Web配置工具可以通过HTTPS会话被获取从广域网端而不是正常HTTP。这将有Ssl encryption算法的保护的您的远程Web会话。如果HTTPS功能残疾用户不能通过使用QuickVPN连接。如果禁用，它使用较少安全HTTP连接。

•组播转接—如果IGMP代理在路由器当前运行，当组播转接被启用路由器将允许IP组播数据流自互联网进来。

**Note:** 要禁用防火墙，必须从默认值更改管理员密码。*SPI* (有状态的信息包检验)， *DoS* (拒绝服务)，*块广域网请求*和*远程管理*字段变灰。

第 3 步：在限制Web功能地区中，请检查任一或所有复选框限制对应的功能。

•Java — Java是网站的编程语言。要阻拦Java，请检查**Java**复选框。 如果拒绝Java，则您不也许能访问此编程语言写的互联网网站，因此继续和阻拦Java程序是安全的，如果设备被连接到路由器不需要访问用Java创建的网站。 另一方面，网络罪犯使用Java作为他们的攻击的一个总体部分，是确定OS并且发起一次OS指定的攻击，当您访问由malware传染的网站时。例如，当您访问一个被删改的网站时，要求您执行其功能的JAR (Java Archive文件)文件被触发，但是秘密地用于确定计算机的OS。

•Cookie —，当用户与他们时，呼应Cookie是互联网网站存储在PC和使用的数据。要阻拦Cookie，请检查**Cookie**复选框。如果希望阻拦Cookie，则网站不能保存任何早先访问信息，当从设备获取。好处是有恶意的Cookie (第三方跟踪Cookie)没有被保存，形成安全风险。

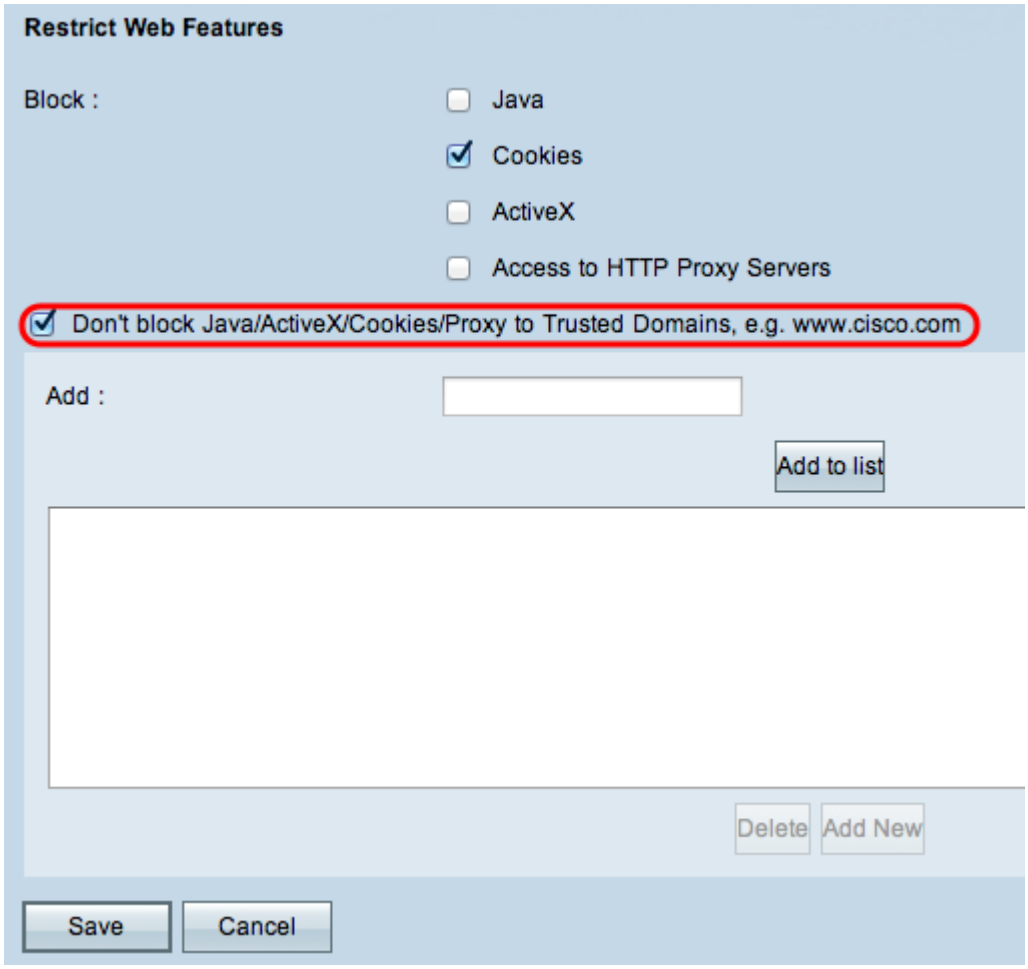
•ActiveX — ActiveX是能使用开发应用程序或控制小的程序类似附加程序使用在互联网网站微软视窗的软件组件。如果允许ActiveX，可帮助改进您的经验，当您访问时;它允许网站运行动画和其他相似的程序。另一方面，有一个潜伏风险，如果访问包含网络罪犯开发的有恶意的ActiveX软件能造成对计算机的损伤的网页。要阻拦ActiveX，请检查**ActiveX**复选框。如果阻拦ActiveX，您可以有问题，如果要访问使用ActiveX实行的某些互联网网站。

•访问到代理HTTP服务器—如果希望通过代理服务器冲浪匿名和拒绝对代理服务器的访问，请检查**访问到代理HTTP服务器**复选框。HTTP代理服务器躲藏起来从终端用户详细资料黑客。因为中间人和您直接地，不如此访问互联网他们工作。然而，如果本地用户访问广域网代理服务器，他们可能能在路由器阻拦的路由器和访问互联网网站的内容过滤器附近查找方式。

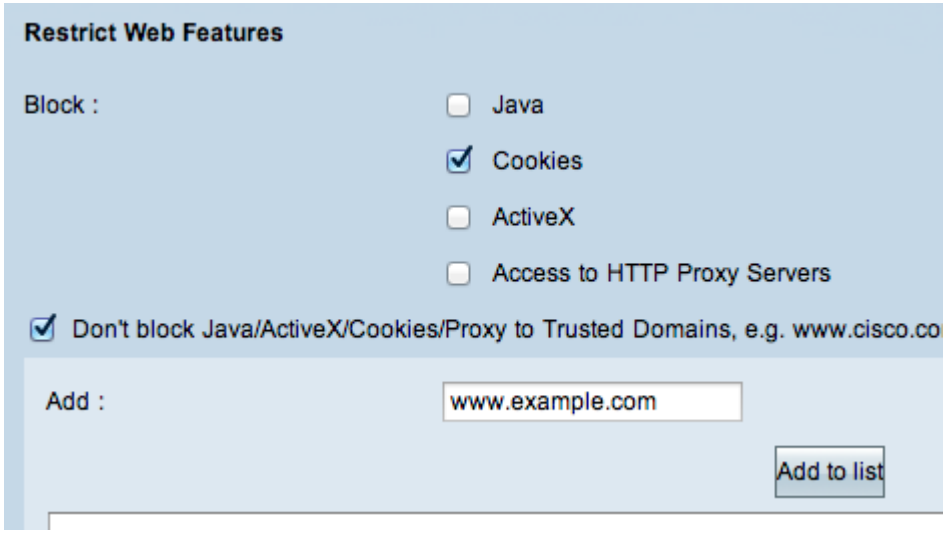
步骤4.点击**"Save"**为了保存设置。

## 添加可信的域

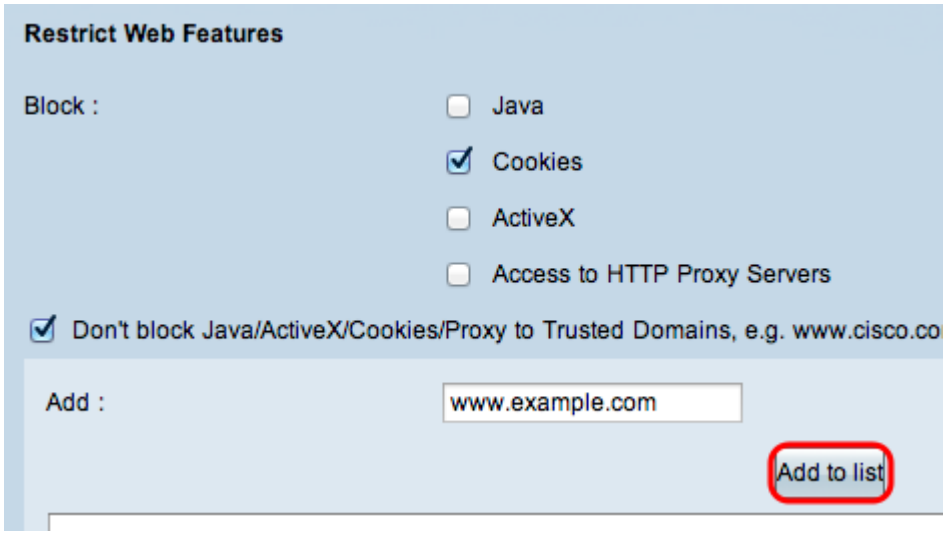
即使其中一个Web功能可能被阻拦，用户能允许这些功能为指定的可信的域被启用。




第 1 步：检查不**阻拦Java/ActiveX/Cookie/代理到可信的域**按钮。如果用户选择阻拦其中任一个在第3步的Web功能*一般防火墙设置*，这只将是可用的。




**Step 2.**在*Add字段*，请输入将被添加的域到可信的域列表。

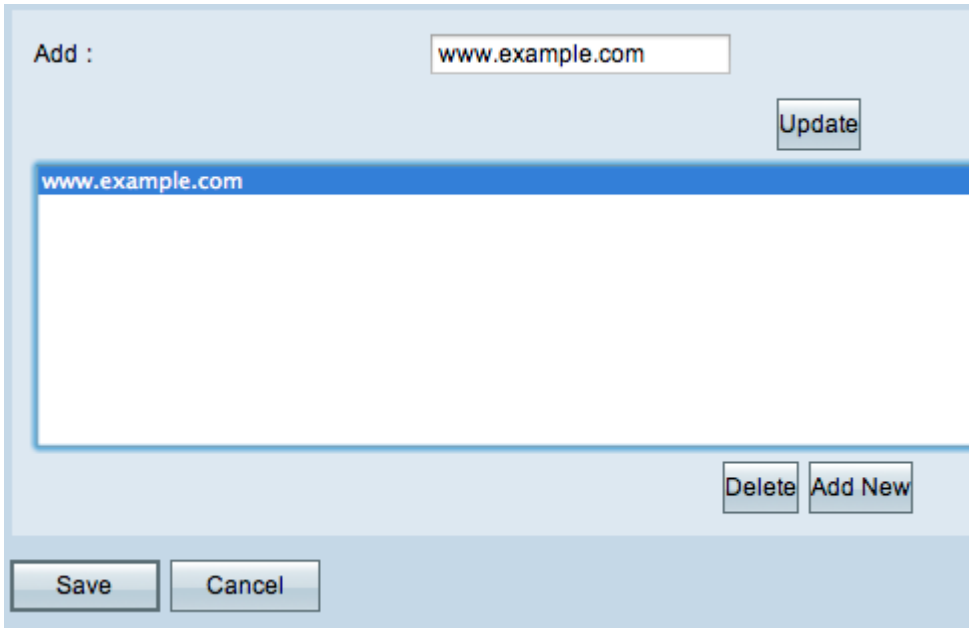



步骤3.点击**添加列出。**域被添加到委托的列表。

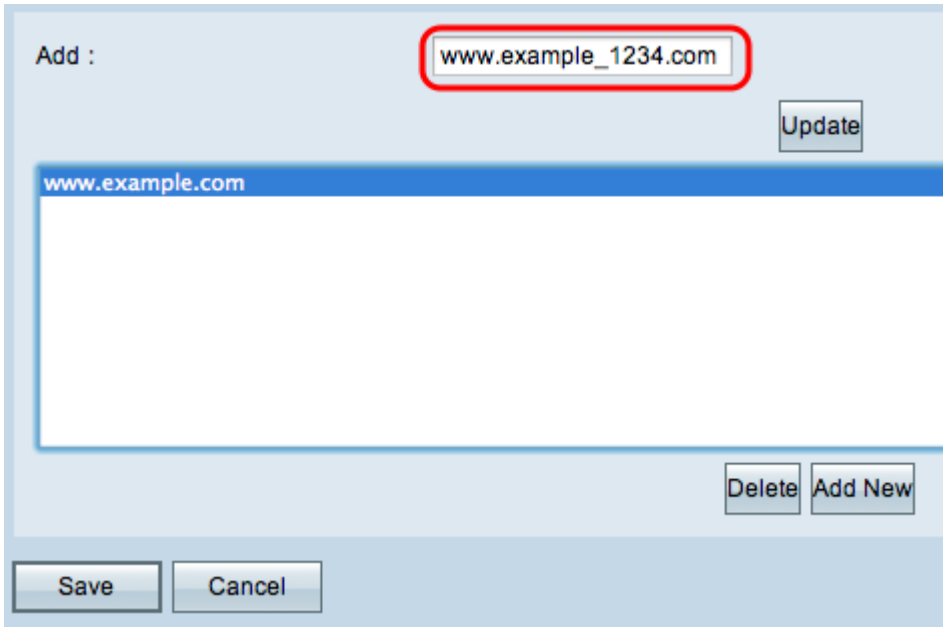
步骤4.点击**"Save"**保存更改。

## 更新可信的域

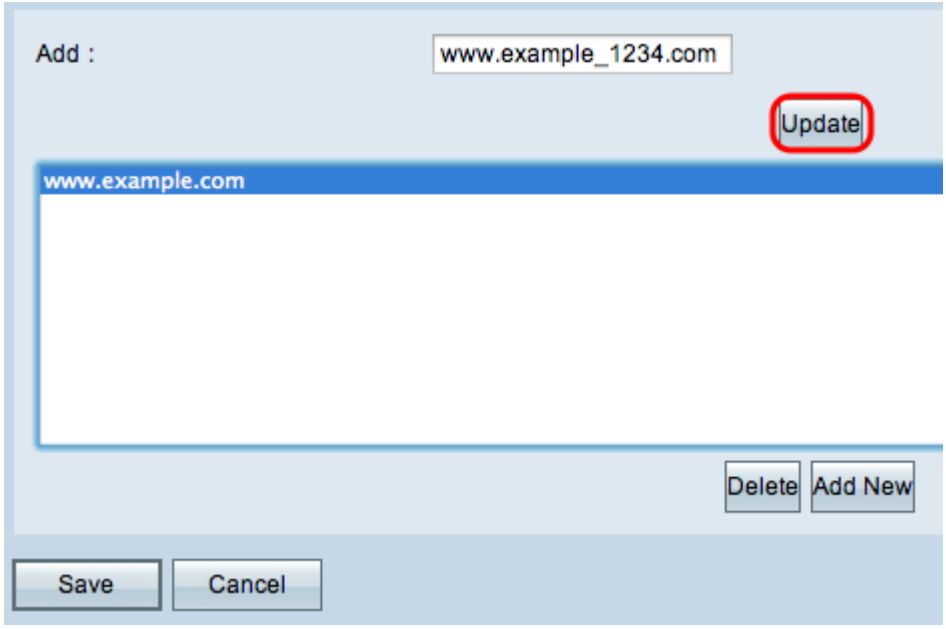
此部分指导关于怎样的用户编辑可信的域。




步骤1.选择您希望从可信的域列表编辑的域。




**Step 2.**在*Add字段*，请输入必需的域的更新的域名。

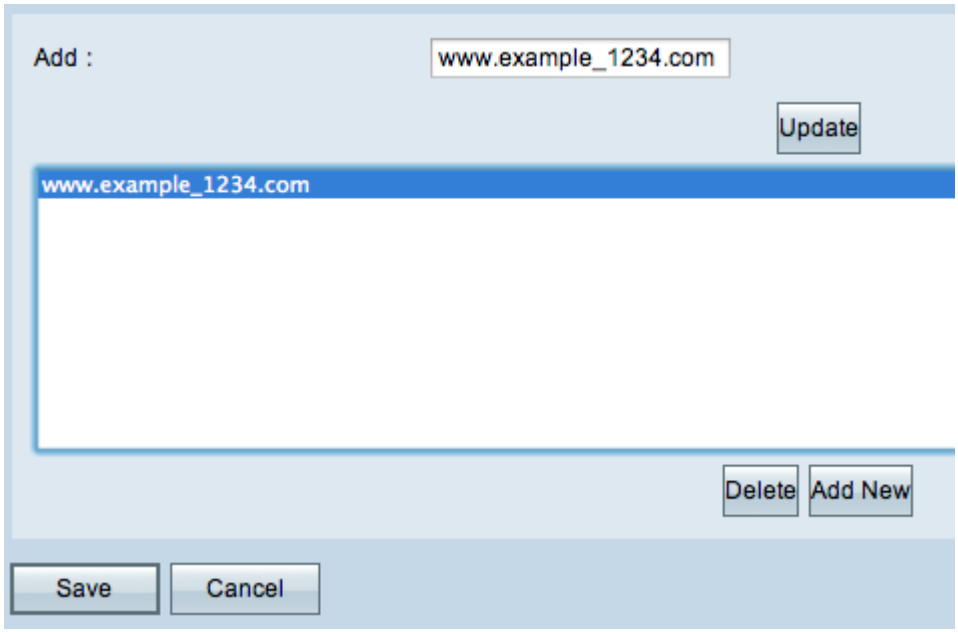



步骤3.点击**更新**。

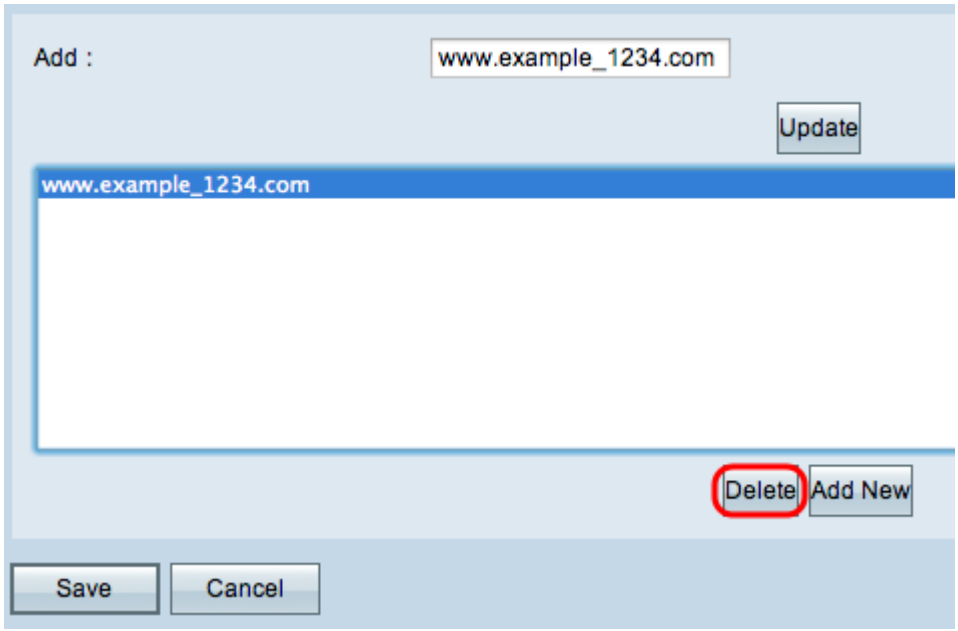
步骤4.点击**"Save"**保存更改。

## 删除可信的域

此部分指导关于怎样的用户删除可信的域。




步骤1.选择您希望删除的域。




步骤2.点击**删除**。域被删除。

步骤3.点击**“Save”**保存更改。