

在RV220W和RV120W的用户帐户配置

客观

设备提供用户帐户为了管理和查看设置。用户可以从不同的组或属于逻辑组共享的SSL VPN认证域、LAN和服务访问规则，并且虚度光阴超时设置。用户管理定义了用户的哪种类型能使用某种设备，并且那如何可以执行。限制可能在每日定时或星期之前变化。

本文目标将配置与管理在RV220W和RV120W的用户帐户。

可适用的设备

- RV220W
- RV120W

软件版本

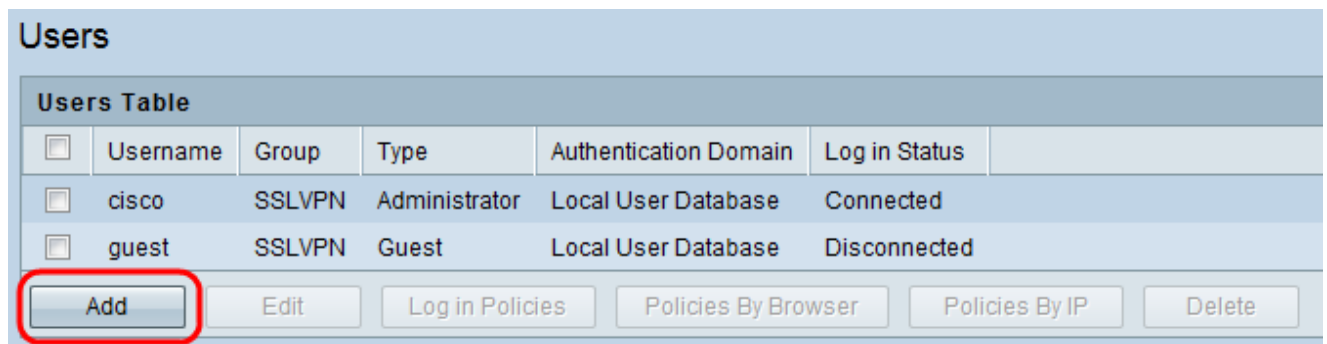
- v1.0.4.17

添加/编辑/删除用户帐户

添加用户帐户

这允许您创建/添加路由器的多个用户。

步骤1. 登陆到Web配置工具并且选择**管理> Users Management>用户**。用户页打开：



The screenshot shows the 'Users' management page. At the top, there is a 'Users Table' with the following columns: Username, Group, Type, Authentication Domain, and Log in Status. Below the table, there are several buttons: 'Add', 'Edit', 'Log in Policies', 'Policies By Browser', 'Policies By IP', and 'Delete'. The 'Add' button is circled in red.

<input type="checkbox"/>	Username	Group	Type	Authentication Domain	Log in Status
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Connected
<input type="checkbox"/>	guest	SSLVPN	Guest	Local User Database	Disconnected

步骤2. 点击**添加**，并且**用户配置**页打开：

User Configuration

User Configuration

Username:

First Name:

Last Name:

User Type:

Select Group:

Password:

Confirm Password:

Idle Timeout: Minutes

Note:支持10个VPN用户。保证您允许您在表里添加的所有的足够量的IP地址用户。

步骤3.输入在用户名字段能将添加的帐户的首选用户名。

步骤4.输入名和姓在各自名字和姓氏字段。

User Type:

Select Group:

Password:

步骤5.从用户类型下拉列表选择期望用户类型：

- SSL VPN用户—，如果使用，SSL VPN用户能登录到网络VPN客户端。
- 管理员—管理员用户获得读和对设备管理器的写访问，因此他们能更改配置数据。
- 客户—客户帐户获得对设备管理器的只读访问。

步骤6.选择您要从挑选组下拉列表添加用户的组。

Note:关于如何创建组的更多信息请参见在RV220W和RV120的条款管理组配置。

步骤7.输入您希望使用用户帐户在密码字段的密码。

步骤8.再输入同一个密码在确认密码字段。

步骤9.在会话时间前进入时间(以分钟)由于非活动在空闲超时字段。DEFAULT值10分钟。

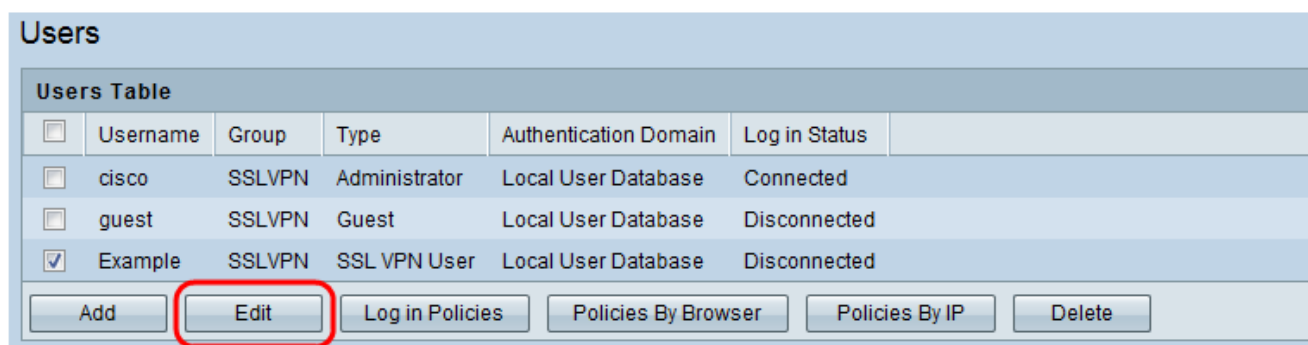
步骤10.点击“Save”应用设置。

Edit a User帐户

这允许您编辑在路由器创建的用户，在为了做期望变动前。

步骤1.登陆到Web配置工具并且选择**管理> Users Management>用户**。用户页打开：

Step 2.检查期望条目的复选框。



Users					
Users Table					
<input type="checkbox"/>	Username	Group	Type	Authentication Domain	Log in Status
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Connected
<input type="checkbox"/>	guest	SSLVPN	Guest	Local User Database	Disconnected
<input checked="" type="checkbox"/>	Example	SSLVPN	SSL VPN User	Local User Database	Disconnected

Buttons: Add, Edit, Log in Policies, Policies By Browser, Policies By IP, Delete

步骤3.点击**编辑**，并且**用户配置**页打开：

User Configuration

User Configuration

Username:

First Name:

Last Name:

User Type:

Select Group:

Check to Edit Password:

Enter Your Password:

New Password:

Confirm New Password:

Idle Timeout: Minutes

步骤4.输入在用户名字段能将添加的帐户的首选用户名。

步骤5.输入名和姓在各自名字和姓氏字段。

步骤6.从用户类型下拉列表选择期望用户类型：

- SSL VPN用户—，如果使用，SSL VPN用户能登录到网络VPN客户端。
- 管理员—管理员用户获得读和对设备管理器的写访问，因此他们能更改配置数据。
- 客户—客户帐户获得对设备管理器的只读访问。

步骤7.选择您希望用户被添加到从挑选组下拉列表的组。

Note:关于如何创建组的更多信息请参见在RV220W和RV120的条款 [管理组配置](#)。

步骤8.输入您希望使用用户帐户在密码字段的密码。

步骤9.再输入同一个密码在确认密码字段。

步骤10.在会话时间前进入时间(以分钟)由于非活动在空闲超时字段。DEFAULT值10分钟。

步骤11.点击“Save”应用设置。

删除用户帐户

删除用户帐户在路由器用户表里允许您删除以前被创建的所有用户。

步骤1.登陆到Web配置工具并且选择**管理> Users Management>用户**。用户页打开：

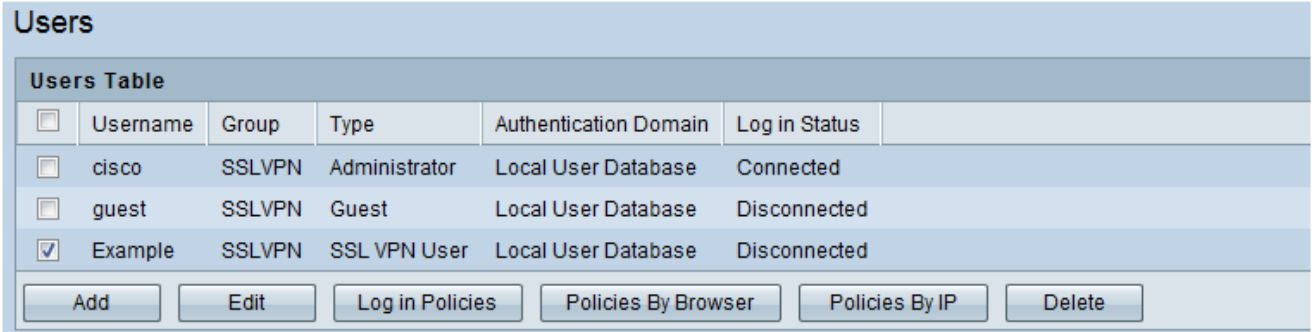
Step 2.检查期望条目的复选框。

步骤3.点击**删除**，并且用户帐户被删除。

在用户帐户的洛金策略

此功能允许用户限制或允许不同类型的登录到设备。这可以认为安全措施，保持设备的访问一样有限尽可能。

步骤1.登陆到Web配置工具并且选择**管理> Users Management>用户**。用户页打开：



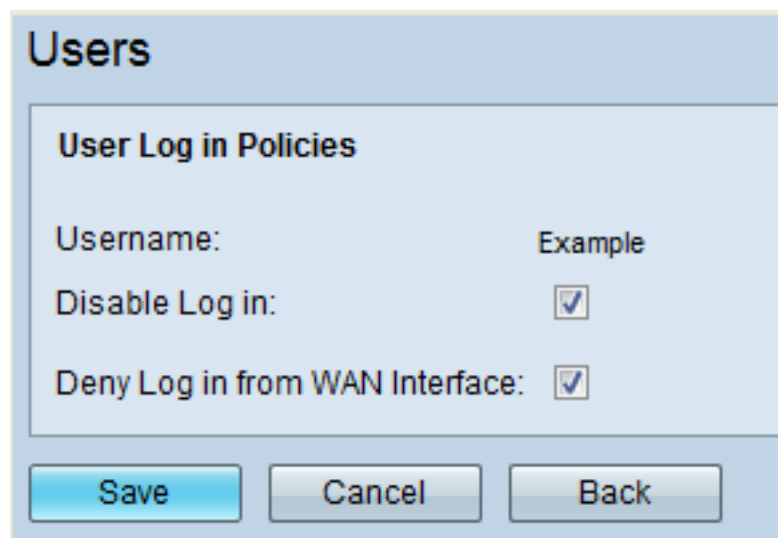
The screenshot shows a web interface for managing users. At the top, there is a header "Users". Below it is a table titled "Users Table" with the following columns: Username, Group, Type, Authentication Domain, and Log in Status. There are three rows of data. The first row has a checkbox, "cisco", "SSLVPN", "Administrator", "Local User Database", and "Connected". The second row has a checkbox, "guest", "SSLVPN", "Guest", "Local User Database", and "Disconnected". The third row has a checked checkbox, "Example", "SSLVPN", "SSL VPN User", "Local User Database", and "Disconnected". Below the table are several buttons: "Add", "Edit", "Log in Policies", "Policies By Browser", "Policies By IP", and "Delete".

<input type="checkbox"/>	Username	Group	Type	Authentication Domain	Log in Status
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Connected
<input type="checkbox"/>	guest	SSLVPN	Guest	Local User Database	Disconnected
<input checked="" type="checkbox"/>	Example	SSLVPN	SSL VPN User	Local User Database	Disconnected

Buttons: Add, Edit, Log in Policies, Policies By Browser, Policies By IP, Delete

Step 2.检查期望条目的复选框。

步骤3.点击“Login”“Policies”，并且Policies页的用户登录打开：



The screenshot shows a configuration window titled "Users". Inside, there is a section "User Log in Policies" with the following settings:

- Username: Example
- Disable Log in:
- Deny Log in from WAN Interface:

At the bottom, there are three buttons: "Save", "Cancel", and "Back".

第 4 步：如果要禁用能力从Web配置工具，登陆请检查功能失效洛金复选框。

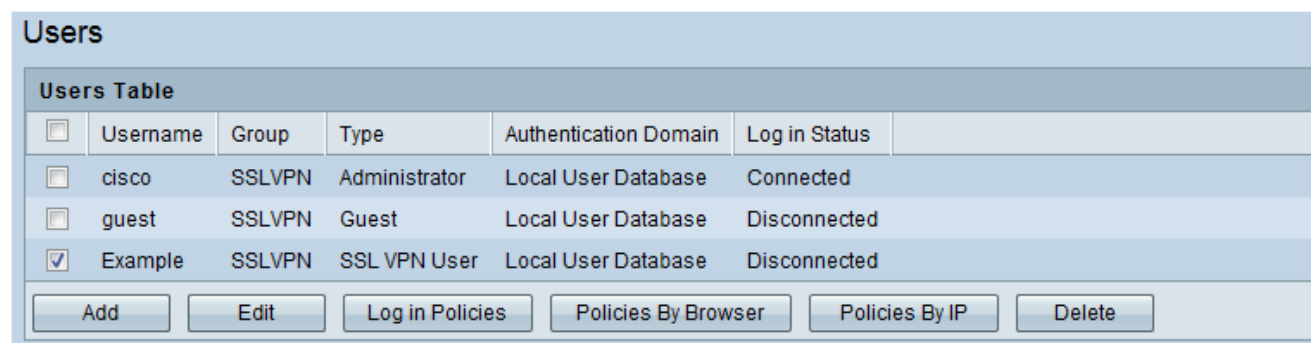
第 5 步：如果要禁用从广域网接口的登录权限请检查从广域网接口复选框的拒绝洛金。

步骤6.点击“Save”应用设置。

由浏览器的策略在用户帐户

此特定的功能允许您定义特定浏览器，用户能从那些被定义的浏览器然后允许或限制登录。

步骤1.登陆到Web配置工具并且选择管理> Users Management>用户。用户页打开：



The screenshot shows the "Users" management page. It features a table with the following columns: Username, Group, Type, Authentication Domain, and Log in Status. Below the table are several action buttons: Add, Edit, Log in Policies, Policies By Browser, Policies By IP, and Delete.

Users Table					
<input type="checkbox"/>	Username	Group	Type	Authentication Domain	Log in Status
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Connected
<input type="checkbox"/>	guest	SSLVPN	Guest	Local User Database	Disconnected
<input checked="" type="checkbox"/>	Example	SSLVPN	SSL VPN User	Local User Database	Disconnected

Step 2.检查期望条目的复选框。

Users

Users Table						
<input type="checkbox"/>	Username	Group	Type	Authentication Domain	Log in Status	
<input type="checkbox"/>	cisco	SSLVPN	Administrator	Local User Database	Connected	
<input type="checkbox"/>	guest	SSLVPN	Guest	Local User Database	Disconnected	
<input checked="" type="checkbox"/>	Example	SSLVPN	SSL VPN User	Local User Database	Disconnected	

步骤3.由浏览器点击“Policies”，并且由客户端浏览器页的用户策略打开：

Users

User Policy By Client Browser

Username:

Deny Log in from Defined Browsers:

Allow Log in only from Defined Browsers:

Defined Browsers

<input type="checkbox"/>	Source Address Type
<input type="checkbox"/>	0 results found

步骤4.从以下选择期望单选按钮：

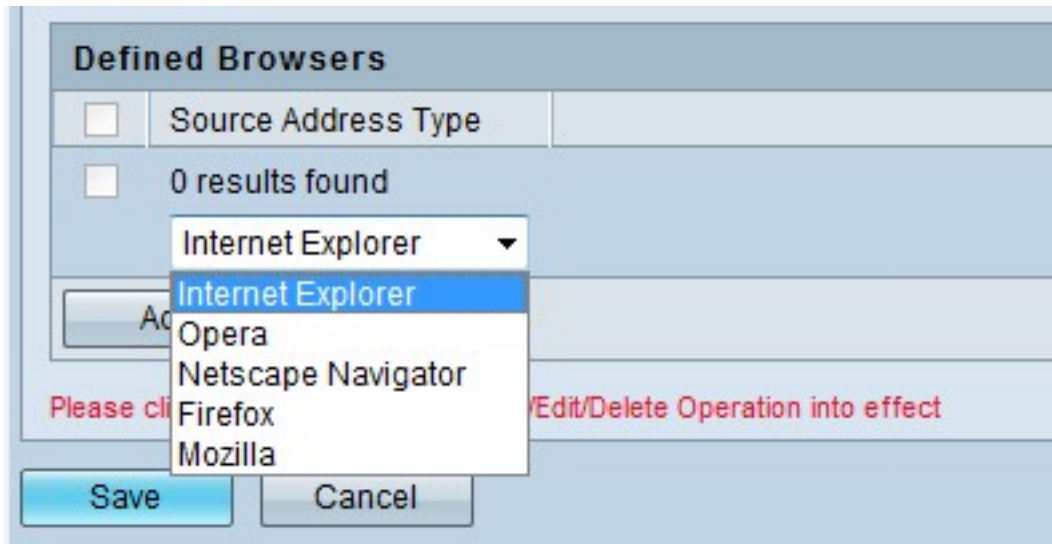
- 拒绝从被定义的浏览器的洛金—洛金从被定义的浏览器被拒绝，在下一步被配置。
- 允许仅洛金从被定义的浏览器—洛金从在下一步被配置的被定义的浏览器仅允许。

Note:被定义的浏览器在页的底下区域被配置。在第4步enable (event)实际上选择的单选按钮或禁用用户访问如下被定义的策略。

Defined Browsers

<input type="checkbox"/>	Source Address Type
<input type="checkbox"/>	0 results found

步骤5.点击添加添加一个被定义的浏览器。



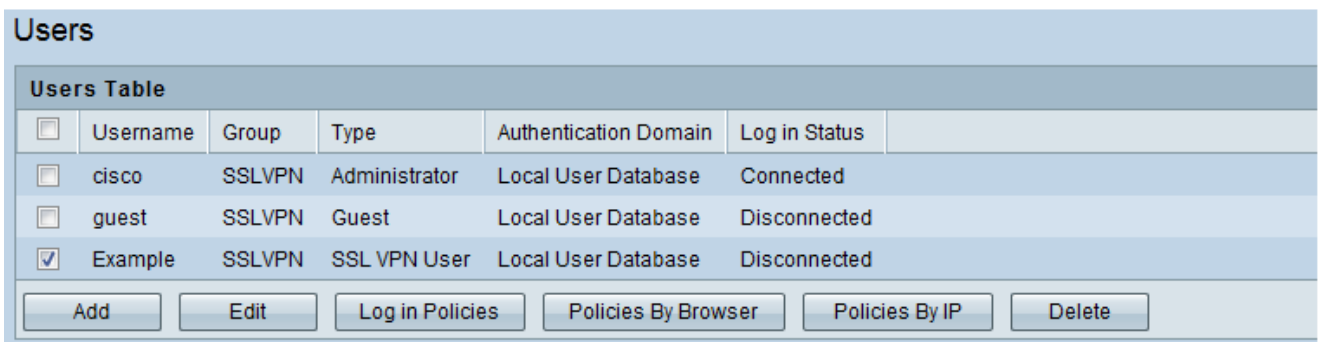
步骤6.从被定义的浏览器下拉列表选择期望浏览器。

步骤7.点击“Save”应用设置。

由IP的策略在用户帐户

此功能允许您定义特定IP，用户能从那些被定义的IP然后允许或限制登录。

步骤1.登陆到Web配置工具并且选择**管理> Users Management>用户**。用户页打开：



Step 2.检查期望条目的复选框。



步骤3.由IP点击“Policies”，并且由来源IP地址页的用户策略打开：

Users

User Policy By Source IP Address

Username:

Deny Log in from Defined Addresses:

Allow Log in only from Defined Addresses:

Defined Addresses

<input type="checkbox"/>	Source Address Type	Network Address / IP Address	Mask Length
<input type="checkbox"/>	0 results found		

步骤4.从以下选择期望单选按钮：

- 拒绝从被定义的地址的洛金—洛金从被定义的地址被拒绝，在下一步被配置。
- 允许仅洛金从被定义的浏览器—洛金从在下一步被配置的被定义的地址只允许。

Note:被定义的地址在页的底下区域被配置。

Defined Addresses

<input type="checkbox"/>	Source Address Type	Network Address / IP Address	Mask Length
<input type="checkbox"/>	0 results found		

步骤5.点击**添加**并且定义了地址配置页打开：

Defined Addresses

Defined Address Configuration

Source Address Type:

Network Address / IP Address:

Mask Length (0-32):

步骤6.从源地址类型下拉菜单选择期望源地址类型：

- IP地址—机器的IP地址动态地分配。
- 被定义的地址配置—网络地址静态分配到设备。

步骤7.若被定义地址配置在第5步在网络地址/IP地址字段被选择了，输入网络IP地址。

步骤8.若被定义地址配置在第5步在掩码长度域被选择了，输入提供的网络地址的掩码长度。范围是从0到32。

步骤9.点击“**Save**”应用设置。