

Configuración de las cuentas de usuario en RV220W y RV120W

Objetivo

El dispositivo proporciona las cuentas de usuario para administrar y ver las configuraciones. Los usuarios pueden ser de diversos grupos o pertenecer a los grupos lógicos de SSL VPN que comparten el dominio de la autenticación, el LAN y las reglas de acceso del servicio, y de configuraciones del tiempo de inactividad. User Management (Administración de usuario) define que el tipo de usuarios puede utilizar un tipo determinado de recurso y cómo eso puede ser hecha. Las restricciones pueden variar por el Time Of Day o el día de la semana.

El objetivo de este documento es configurar y manejar las cuentas de usuario en el RV220W y el RV120W.

Dispositivos aplicables

- RV220W
- RV120W

Versión del software

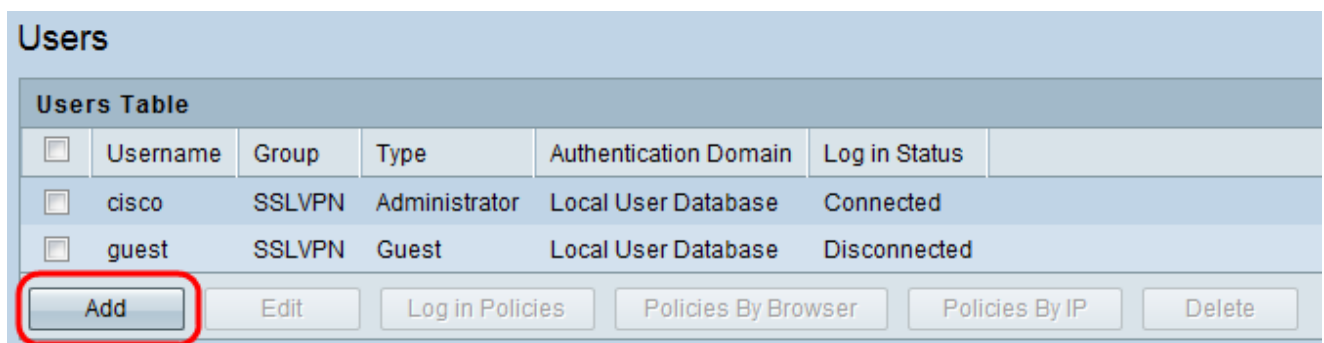
- v1.0.4.17

Agregue/edite/cancelación una cuenta de usuario

Agregue una cuenta de usuario

Esto permite que usted cree/agrega a los usuarios múltiples en un router.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:



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

Paso 2. El tecleo **agrega** y la página de la *configuración de usuario* se abre:

User Configuration

User Configuration

Username:

First Name:

Last Name:

User Type:

Select Group:

Password:

Confirm Password:

Idle Timeout: Minutes

Nota: Soportan a hasta 10 usuarios de VPN. Asegúrese le permitir una cantidad suficiente de IP Addresses para todos los usuarios que usted agrega en la tabla.

Paso 3. Ingrese un nombre de usuario preferido para que la cuenta sea agregada en el campo de nombre de usuario.

Paso 4. Ingrese el nombre y apellido en los campos respectivos del primer nombre y de último nombre.

User Type:

Select Group:

Password:

Paso 5. Elija el tipo de usuario deseado de la lista desplegable del tipo de usuario:

- Usuario de VPN SSL — Un usuario de VPN SSL puede iniciar sesión a la red si utilizan al cliente VPN.
- Administrador — Un usuario administrador consigue el acceso de lectura y escritura al administrador de dispositivo, así que pueden cambiar los datos de configuración.
- Invitado — Una cuenta de invitado consigue acceso de sólo lectura al administrador de dispositivo.

Paso 6. Elija al grupo a quien usted quiere agregar al usuario de la lista desplegable selecta del grupo.

Nota: Para más información sobre cómo crear a los grupos refiera a la *configuración de los grupos de la administración del artículo en RV220W y RV120*.

Paso 7. Ingrese la contraseña que usted desea utilizar para la cuenta de usuario en el campo de contraseña.

Paso 8. Ingrese la misma contraseña otra vez en el campo de contraseña del confirmar.

Paso 9. Ingrese el tiempo (en los minutos) antes de los tiempos de la sesión hacia fuera debido a la inactividad en el campo del tiempo de inactividad. El valor predeterminado es 10 minutos.

Paso 10. **Salvaguardia del** teclado para aplicar las configuraciones.

Cuenta del Edit a User

Esto permite que usted edite a los usuarios creados en el router antes de que para realizar los cambios deseados.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:

Paso 2. Marque la casilla de verificación de la entrada deseada.

<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

Paso 3. El teclado **edita** y la página de la *configuración de usuario* se abre:

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

Paso 4. Ingrese un nombre de usuario preferido para que la cuenta sea agregada en el campo de nombre de usuario.

Paso 5. Ingrese el nombre y apellido en los campos respectivos del primer nombre y de último nombre.

Paso 6. Elija el tipo de usuario deseado de la lista desplegable del tipo de usuario:

- Usuario de VPN SSL — Un usuario de VPN SSL puede iniciar sesión a la red si utilizan al cliente VPN.
- Administrador — Un usuario administrador consigue el acceso de lectura y escritura al administrador de dispositivo, así que pueden cambiar los datos de configuración.
- Invitado — Una cuenta de invitado consigue acceso de sólo lectura al administrador de dispositivo.

Paso 7. Elija al grupo que usted quisiera que agregaran al usuario de la lista desplegable selecta del grupo.

Nota: Para más información sobre cómo crear a los grupos refiera a la *configuración de los grupos de la administración* del artículo en RV220W y RV120.

Paso 8. Ingrese la contraseña que usted desea utilizar para la cuenta de usuario en el campo de contraseña.

Paso 9. Ingrese la misma contraseña otra vez en el campo de contraseña del confirmar.

Paso 10. Ingrese el tiempo (en los minutos) antes de los tiempos de la sesión hacia fuera debido a la inactividad en el campo del tiempo de inactividad. El valor predeterminado es 10 minutos.

Paso 11 **Salvaguardia del** tecleo para aplicar las configuraciones.

Borre una cuenta de usuario

La cuenta de usuario de la cancelación permite que usted borre simplemente a cualquier usuario en la tabla de usuario del router que fuera creado antes.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:

Paso 2. Marque la casilla de verificación de la entrada deseada.

Paso 3. Se borra la **cancelación del** tecleo y la cuenta de usuario.

Directivas del login en las cuentas de usuario

Esta característica permite que un usuario restrinja o permita diversos tipos de login al dispositivo. Esto se puede considerar una medida de Seguridad, para mantener el acceso del dispositivo tan limitado como sea posible.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:

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	

Paso 2. Marque la casilla de verificación de la entrada deseada.

Paso 3. Las directivas del login del teclado y la página de las *directivas del ingreso del usuario al sistema* se abre:

Users

User Log in Policies

Username: Example

Disable Log in:

Deny Log in from WAN Interface:

Paso 4. Marque la casilla de verificación del **login de la neutralización** si usted quiere inhabilitar la capacidad de iniciar sesión de la utilidad de configuración de la red.

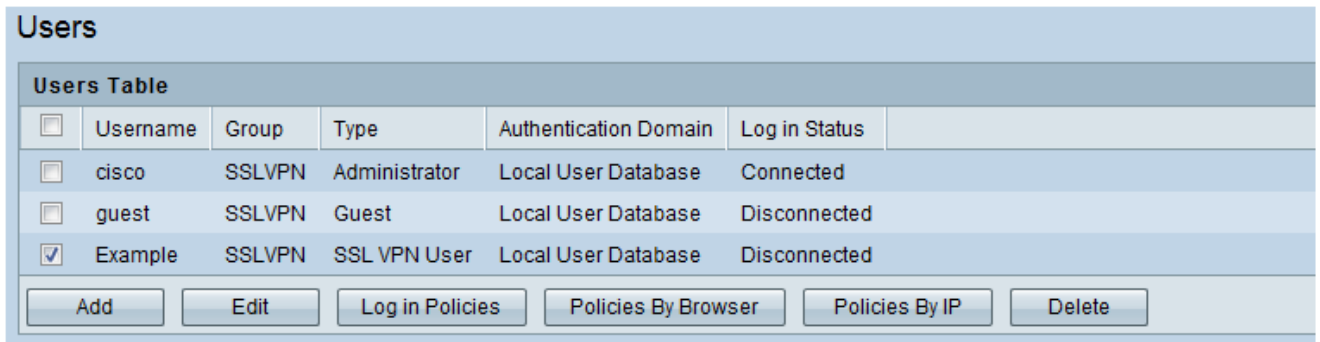
Paso 5. Marque el **login de la negación de la** casilla de verificación de la **interfaz de WAN** si usted quiere inhabilitar el permiso del login de la interfaz de WAN.

Paso 6. **Salvaguardia del teclado** para aplicar las configuraciones.

Directivas del navegador en las cuentas de usuario

Esta función particular permite que usted defina a los navegadores específicos, el usuario puede después permitir o restringir el login de esos navegadores definidos.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:



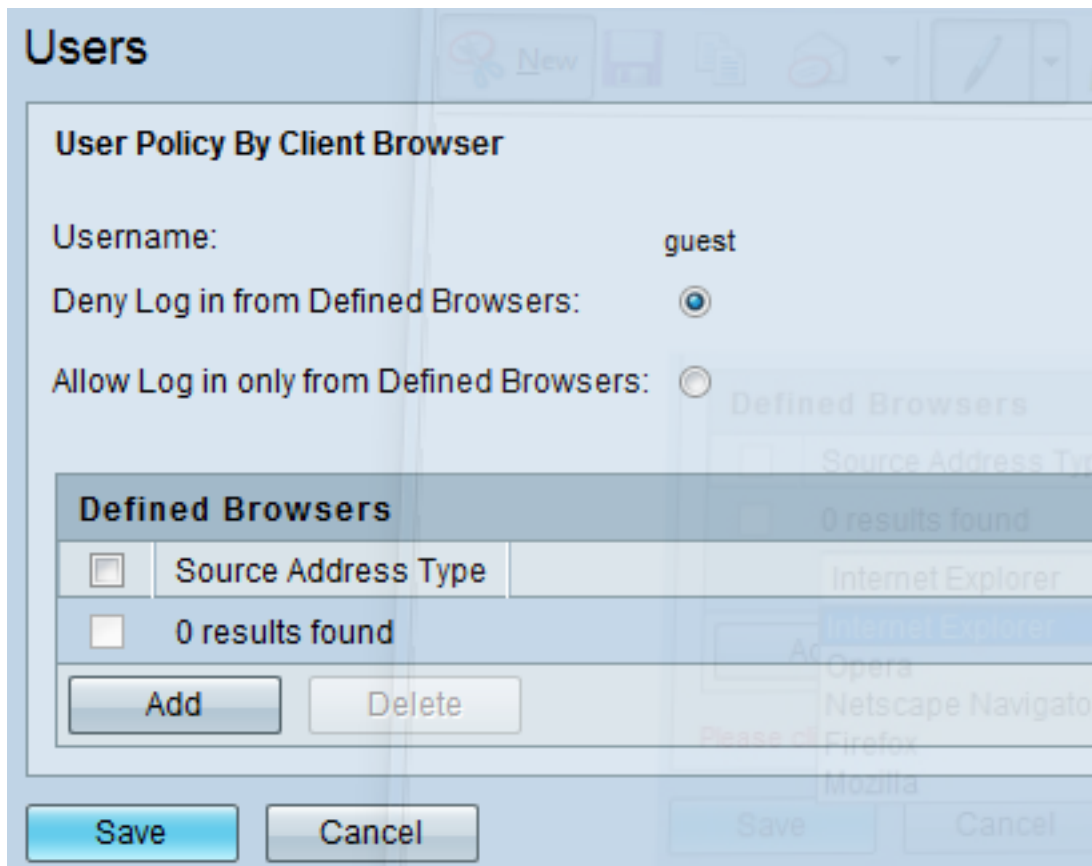
The screenshot shows the 'Users' configuration page. At the top, there is a 'Users Table' with the following columns: Username, Group, Type, Authentication Domain, and Log in Status. The table contains three rows: 'cisco' (Administrator, Local User Database, Connected), 'guest' (Guest, Local User Database, Disconnected), and 'Example' (SSL VPN User, Local User Database, Disconnected). Below the table are several buttons: 'Add', 'Edit', 'Log in Policies', 'Policies By Browser', 'Policies By IP', and 'Delete'.

Paso 2. Marque la casilla de verificación de la entrada deseada.



This screenshot is identical to the previous one, but the 'Policies By Browser' button is highlighted with a red rectangular box.

Paso 3. Las **directivas del teclado por el navegador** y la *política de usuario por la página del buscador del cliente* se abren:



The screenshot shows the 'User Policy By Client Browser' configuration dialog. The 'Username' field is set to 'guest'. There are two radio buttons: 'Deny Log in from Defined Browsers:' (which is selected) and 'Allow Log in only from Defined Browsers:'. Below this is a 'Defined Browsers' section with a table that has one column 'Source Address Type' and shows '0 results found'. There are 'Add' and 'Delete' buttons for this section. At the bottom of the dialog are 'Save' and 'Cancel' buttons.

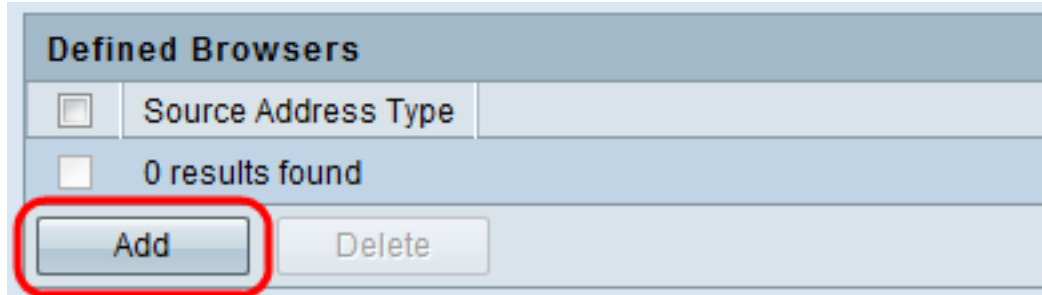
Paso 4. Elija los botones de radio deseados del siguiente:

- Niegue el login de los navegadores definidos — El login se niega de los navegadores

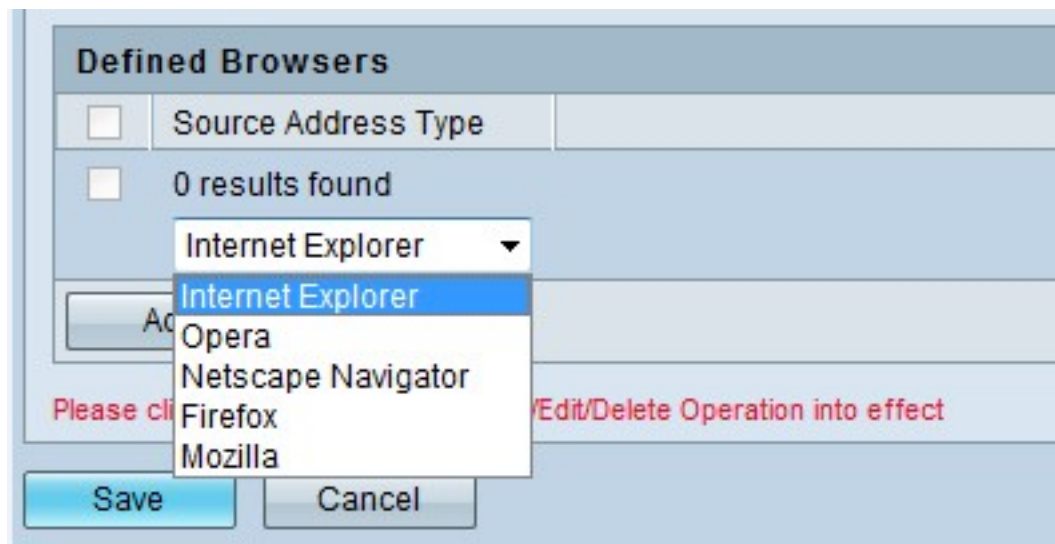
definidos, que se configuran en el siguiente paso.

- Permita el login solamente de los navegadores definidos — El login se permite solamente de los navegadores definidos que se configuran en el siguiente paso.

Nota: Configuran a los navegadores definidos en el área inferior de la página. Los botones de radio elegidos en el paso 4 permiten o inhabilitan realmente al usuario para acceder la directiva definida abajo.



Paso 5. El tecleo **agrega** para agregar a un navegador definido.



Paso 6. Elija al navegador deseado de la lista desplegable definida de los navegadores.

Paso 7. **Salvaguardia** del tecleo para aplicar las configuraciones.

Directivas por el IP en las cuentas de usuario

Esta característica permite que usted defina los IP específicos, el usuario puede después permitir o restringir el login de esos IP definidos.

Paso 1. Inicie sesión a la utilidad de configuración de la red y elija la **Administración de la administración > Users > Users**. La página de los *usuarios* se abre:

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	

Paso 2. Marque la casilla de verificación de la entrada deseada.

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	

Paso 3. Las directivas del teclado por el IP y la política de usuario por la página del IP address de la fuente se abren:

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
0 results found			

Paso 4. Elija los botones de radio deseados del siguiente:

- Niegue el login de los direccionamientos definidos — El login se niega de los direccionamientos definidos, que se configuran en el siguiente paso.
- Permita el login solamente de los navegadores definidos — El login se permite solamente de los direccionamientos definidos que se configuran en el siguiente paso.

Nota: Los direccionamientos definidos se configuran en el área inferior de la página.

Defined Addresses			
<input type="checkbox"/>	Source Address Type	Network Address / IP Address	Mask Length
<input type="checkbox"/>	0 results found		
<input type="button" value="Add"/>		<input type="button" value="Delete"/>	

Paso 5. Haga clic **agregan** y *definen la página de configuración del direccionamiento* se abre:

Defined Addresses	
Defined Address Configuration	
Source Address Type:	<input type="text" value="Defined Address Configuration"/>
Network Address / IP Address:	<input type="text" value="192.0.2.0"/>
Mask Length (0-32):	<input type="text" value="24"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Back"/>	

Paso 6. Elija el tipo deseado de la dirección de origen del menú desplegable del tipo de la dirección de origen:

- Dirección IP — Un IP address de la máquina se asigna dinámicamente.
- Configuración definida del direccionamiento — Asignan una dirección de red estáticamente al dispositivo.

Paso 7. Si la configuración definida del direccionamiento fue elegida en el paso 5, ingrese un IP Address de red en el campo de la dirección de red/del IP address.

Paso 8. Si la configuración definida del direccionamiento fue elegida en el paso 5, ingrese la longitud de la máscara de la dirección de red proporcionada en la extensión del campo de la máscara. El rango es a partir la 0 a 32.

Paso 9. **Salvaguardia del** teclado para aplicar las configuraciones.