

# Configuración de LAN y acceso web de gestión remota en los RV130 y RV130W

Para ver un vídeo que muestra cómo configurar LAN y la administración remota, visite <https://youtu.be/9R0Rd5bS1W8>

## Objetivo

Los clientes que están conectados a la interfaz LAN o WAN del router pueden acceder a la utilidad de configuración web del router. La configuración de LAN/VPN Web Access puede permitir que los clientes de la red de área local se conecten al router de forma segura a través de Secure Socket Layer. La configuración de Remote Management Web Access puede permitir que los clientes externos a la red corporativa se conecten al router a través de su dirección IP. Remote Management Web Access puede ser útil si un administrador desea acceder o configurar el router desde una ubicación remota.

El objetivo de este documento es mostrarle cómo configurar LAN y Remote Management Web Access en los routers RV130 y RV130W.

## Dispositivos aplicables

- RV130
- RV130W

## Versión del software

- v1.0.1.3

## Configuración de LAN/VPN y acceso web de gestión remota

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Firewall > Basic Settings**. Se abre la página *Basic Settings*:

## Basic Settings

IP Address Spoofing Protection:	<input checked="" type="checkbox"/> Enable
DoS Protection:	<input checked="" type="checkbox"/> Enable
Block WAN Ping Request:	<input checked="" type="checkbox"/> Enable
LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> - <input type="text" value="0"/>
Remote Management Port	<input type="text" value="443"/> (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input type="checkbox"/> Enable
SIP ALG	<input type="checkbox"/> Enable
<hr/>	
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
<hr/>	
Block Java:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> <input checked="" type="radio"/> Auto <input type="radio"/> Manual Port: <input type="text"/>

Save

Cancel

Paso 2. En el campo *LAN/VPN Web Access*, marque las casillas de verificación correspondientes a los tipos deseados de protocolos de acceso Web. Los protocolos se utilizan para conectarse al dispositivo desde los miembros de la interfaz LAN.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	<input type="text" value="443"/> (Range: 1 - 65535, Default: 443)

Las opciones disponibles se definen de la siguiente manera:

·HTTP: los clientes pueden conectarse a sitios web internos a través del protocolo estándar de transferencia de hipertexto (HTTP). Los elementos HTML de los sitios web se envían directamente al dispositivo cliente. La conexión a sitios web a través de HTTP es más rápida que HTTPS.

·HTTPS: mediante el protocolo de transferencia de hipertexto seguro (HTTPS), los clientes pueden conectarse a sitios web internos solo cuando los certificados digitales instalados en el sitio web están autenticados con el servidor web asociado. Esto evita cualquier ataque de intermediarios entre el cliente y el sitio web. Al marcar esta opción también se proporciona cifrado bidireccional entre el cliente y el sitio web.

**Nota:** Marque solamente la casilla de verificación **HTTP** si las páginas web de su dominio no tienen instalados los certificados SSL requeridos. Marque solamente la casilla de verificación **HTTPS** si todas las páginas web de su dominio tienen instalados los certificados SSL. Puede marcar ambas casillas para HTTP y HTTPS si desea versatilidad en la forma en que sus clientes acceden al router.

Paso 3. En el campo *Administración remota*, marque la casilla de verificación **Enable** para habilitar el acceso remoto de los administradores a la utilidad de configuración web del dispositivo. De forma predeterminada, la gestión remota está desactivada. Si no se marca, vaya al paso 8.

**Nota:** Cuando la gestión remota está activada, cualquier persona que conozca su dirección IP puede acceder al router. Es importante cambiar la contraseña predeterminada del dispositivo antes de activar esta función.

Paso 4. En el campo *Acceso remoto*, seleccione el botón de opción que desee que

corresponda al tipo de protocolo de acceso remoto. El protocolo se utilizará para conectar dispositivos de una red de área extensa (WAN) remota directamente al router. HTTPS es más seguro que HTTP y es la opción recomendada.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)

Las opciones disponibles se definen de la siguiente manera.

·HTTP: los clientes pueden conectarse a sitios web internos a través del protocolo estándar de transferencia de hipertexto (HTTP). Los elementos HTML de los sitios web se envían directamente al dispositivo cliente. La conexión a sitios web a través de HTTP es más rápida que HTTPS.

·HTTPS: mediante el protocolo de transferencia de hipertexto seguro (HTTPS), los clientes pueden conectarse a sitios web internos solo cuando los certificados digitales instalados en el sitio web están autenticados con el servidor web asociado. Esto evita cualquier ataque de intermediarios entre el cliente y el sitio web. Al marcar esta opción también se proporciona cifrado bidireccional entre el cliente y el sitio web.

Paso 5. En el campo *Remote Upgrade*, marque la casilla de verificación **Enable** para permitir que los administradores actualicen el dispositivo desde una WAN remota.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)

Paso 6. En el campo *Allowed Remote IP Address*, elija qué direcciones IP tendrán acceso remoto al dispositivo. Haga clic en el botón de opción **Any IP Address** para permitir que cualquier dispositivo remoto se conecte, o haga clic en el botón de opción que se encuentra debajo para introducir manualmente un intervalo de direcciones IP permitidas.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input checked="" type="radio"/> Any IP Address <input type="radio"/> 0 . 0 . 0 . 0 - 0
Remote Management Port	443 (Range: 1 - 65535, Default: 443)

Paso 7. Introduzca el puerto en el que se permite el acceso remoto. El puerto predeterminado es 443.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input type="radio"/> Any IP Address <input checked="" type="radio"/> 192 . 168 . 1 . 75 - 100
Remote Management Port	443 (Range: 1 - 65535, Default: 443)

**Nota:** Al acceder de forma remota al router, debe introducir el puerto de gestión remota como parte de la dirección IP. Por ejemplo: **https://<remote-ip>:<remote-port>**, o **https://168.10.1.11:443**.

Paso 8. Haga clic en **Guardar** para guardar la configuración.

LAN/VPN Web Access:	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Remote Management:	<input checked="" type="checkbox"/> Enable
Remote Access:	<input type="radio"/> HTTP <input checked="" type="radio"/> HTTPS
Remote Upgrade:	<input checked="" type="checkbox"/> Enable
Allowed Remote IP Address:	<input type="radio"/> Any IP Address <input checked="" type="radio"/> 192 . 169 . 1 . 75 - 100
Remote Management Port	443 (Range: 1 - 65535, Default: 443)
IPv4 Multicast Passthrough:(IGMP Proxy)	<input checked="" type="checkbox"/> Enable
IPv4 Multicast Immediate Leave:(IGMP Proxy Immediate Leave)	<input type="checkbox"/> Enable
SIP ALG	<input type="checkbox"/> Enable
UPnP	<input checked="" type="checkbox"/> Enable
Allow Users to Configure	<input checked="" type="checkbox"/> Enable
Allow Users to Disable Internet Access	<input type="checkbox"/> Enable
Block Java:	<input type="checkbox"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> Auto <input type="radio"/> Manual Port: <input type="text"/>
<input checked="" type="button"/> Save <input type="button"/> Cancel	

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).