

Configuração de LAN e Acesso Web de Gerenciamento Remoto no RV130 e RV130W

Para assistir a um vídeo que mostra como configurar o gerenciamento remoto e de LAN, visite <https://youtu.be/9R0Rd5bS1W8>

Objetivo

Os clientes conectados à interface LAN ou WAN do roteador podem acessar o utilitário de configuração da Web do roteador. A configuração do Acesso à Web de LAN/VPN pode permitir que os clientes na Rede Local se conectem ao roteador com segurança através do Secure Socket Layer. A configuração do Acesso via Web para Gerenciamento Remoto pode permitir que clientes de fora da rede corporativa se conectem ao roteador através de seu Endereço IP. O Acesso via Web de Gerenciamento Remoto pode ser útil se um administrador quiser acessar ou configurar o roteador de um local remoto.

O objetivo deste documento é mostrar como configurar a LAN e o Acesso via Web de Gerenciamento Remoto nos roteadores RV130 e RV130W.

Dispositivos aplicáveis

RV130

RV130W

Versão de software

•v1.0.1.3

Configuração de acesso à Web para gerenciamento remoto e LAN/VPN

Etapa 1. Inicie a sessão no utilitário de configuração da Web e escolha **Firewall > Basic Settings**. A página *Basic Settings* é aberta:

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"/> 0 . 0 . 0 . 0 - 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

Etapa 2. No campo *LAN/VPN Web Access*, marque as caixas de seleção correspondentes aos tipos desejados de protocolos de Acesso à Web. Os protocolos são usados para se conectar ao dispositivo a partir de membros da interface 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)

As opções disponíveis são definidas da seguinte forma:

·HTTP — Os clientes podem se conectar a sites da Web internos por meio do protocolo HTTP padrão. Os elementos HTML dos seus sites são enviados diretamente para o dispositivo cliente. A conexão a sites da Web via HTTP é mais rápida que a conexão HTTPS.

HTTPS — usando o HyperText Transfer Protocol Secure (HTTPS), os clientes podem se conectar a sites internos somente quando os certificados digitais instalados no site forem autenticados com o servidor Web associado a ele. Isso evita ataques de intermediários entre o cliente e o site. Marcar esta opção também fornece criptografia bidirecional entre o cliente e o site.

Note: Marque apenas a caixa de seleção **HTTP** se as páginas da Web no seu domínio não tiverem os certificados SSL necessários instalados. Marque apenas a caixa de seleção **HTTPS** se todas as páginas da Web do seu domínio tiverem os certificados SSL instalados. Você pode marcar as duas caixas de seleção para HTTP e HTTPS se quiser versatilidade em como seus clientes acessam o roteador.

Etapa 3. No campo *Remote Management*, marque a caixa de seleção **Enable** para habilitar o acesso remoto dos administradores ao utilitário de configuração da Web do dispositivo. Por padrão, o Gerenciamento remoto está desabilitado. Se estiver desmarcada, vá para a Etapa 8.

Note: Quando o Gerenciamento remoto está ativado, o roteador pode ser acessado por qualquer pessoa que saiba seu endereço IP. É importante alterar a senha padrão do dispositivo antes de habilitar esse recurso.

Etapa 4. No campo *Acesso Remoto*, selecione um botão de opção desejado correspondente

ao tipo de protocolo de Acesso Remoto. O protocolo será usado para conectar dispositivos de uma rede remota (WAN) diretamente ao roteador. O HTTPS é mais seguro que o HTTP e é a opção 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)

As opções disponíveis são definidas da seguinte forma.

·HTTP — Os clientes podem se conectar a sites da Web internos por meio do protocolo HTTP padrão. Os elementos HTML dos seus sites são enviados diretamente para o dispositivo cliente. A conexão a sites da Web via HTTP é mais rápida que a conexão HTTPS.

HTTPS — usando o HyperText Transfer Protocol Secure (HTTPS), os clientes podem se conectar a sites internos somente quando os certificados digitais instalados no site forem autenticados com o servidor Web associado a ele. Isso evita ataques de intermediários entre o cliente e o site. Marcar esta opção também fornece criptografia bidirecional entre o cliente e o site.

Etapa 5. No *campo Remote Upgrade*, marque a caixa de seleção **Enable** para permitir que os administradores atualizem o dispositivo de uma 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)

Etapa 6. No campo *Allowed Remote IP Address*, escolha quais endereços IP terão acesso remoto ao dispositivo. Clique no botão de opção **Any IP Address** para permitir a conexão de qualquer dispositivo remoto ou clique no botão de opção abaixo dele para inserir manualmente um intervalo de endereços IP permitidos.

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)

Etapa 7. Insira a porta na qual o acesso remoto é permitido. A porta padrão é 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)

Note: Ao acessar remotamente o roteador, você deve inserir a porta de gerenciamento remoto como parte do endereço IP. Por exemplo: <https://<remote-ip>:<remote-port>> ou <https://168.10.1.11:443>.

Etapa 8. Clique em **Salvar** para salvar suas configurações.

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)
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	

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.