

Konfiguration des LAN- und Remote-Management-Webzugangs auf der RV130 und der RV130W

Ein Video zur Konfiguration von LAN- und Remote-Management finden Sie unter <https://youtu.be/9R0Rd5bS1W8>

Ziel

Clients, die mit der LAN- oder WAN-Schnittstelle des Routers verbunden sind, können auf das Webkonfigurationsprogramm des Routers zugreifen. Durch die Konfiguration von LAN/VPN Web Access können Clients im LAN sicher über Secure Socket Layer eine Verbindung zum Router herstellen. Durch die Konfiguration von Remote Management Web Access können Clients von außerhalb des Unternehmensnetzwerks über dessen IP-Adresse eine Verbindung zum Router herstellen. Remote Management Web Access kann nützlich sein, wenn ein Administrator von einem entfernten Standort aus auf den Router zugreifen oder diesen konfigurieren möchte.

In diesem Dokument wird erläutert, wie Sie den LAN- und Remote-Management-Webzugriff auf den Routern RV130 und RV130W konfigurieren.

Unterstützte Geräte

- RV130
- RV130W

Software-Version

- v1.0.1.3

Konfiguration von LAN-/VPN- und Remote-Management-Webzugriff

Schritt 1: Melden Sie sich beim Webkonfigurationsprogramm an, und wählen Sie **Firewall > Basic Settings**. Die Seite *Grundeinstellungen* wird geöffnet:

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

Schritt 2: Aktivieren Sie im Feld *LAN/VPN Web Access* die Kontrollkästchen für die gewünschten Typen von Web Access-Protokollen. Die Protokolle werden verwendet, um über Elemente der LAN-Schnittstelle eine Verbindung zum Gerät herzustellen.

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)

Die verfügbaren Optionen sind wie folgt definiert:

- HTTP - Clients können sich über das Standard-Hypertext Transfer Protocol (HTTP) mit internen Websites verbinden. HTML-Elemente Ihrer Websites werden direkt an das Client-Gerät gesendet. Die Verbindung zu Websites über HTTP ist schneller als HTTPS.
- HTTPS - Mithilfe des HyperText Transfer Protocol Secure (HTTPS) können Clients nur dann eine Verbindung zu internen Websites herstellen, wenn die auf der Website installierten digitalen Zertifikate mit dem zugehörigen Webserver authentifiziert werden. Dadurch werden alle Man-in-the-Middle-Angriffe zwischen dem Client und der Website verhindert. Wenn Sie diese Option auswählen, wird auch eine bidirektionale Verschlüsselung zwischen dem Client und der Website bereitgestellt.

Anmerkung: Aktivieren Sie nur das Kontrollkästchen **HTTP**, wenn auf Webseiten in Ihrer Domäne nicht die erforderlichen SSL-Zertifikate installiert sind. Aktivieren Sie nur das Kontrollkästchen **HTTPS**, wenn auf allen Webseiten Ihrer Domäne die SSL-Zertifikate installiert sind. Sie können beide Kontrollkästchen für HTTP und HTTPS aktivieren, wenn Sie die Zugriffsmöglichkeiten Ihrer Clients auf den Router flexibel gestalten möchten.

Schritt 3: Aktivieren Sie im Feld "*Remote Management*" das Kontrollkästchen **Enable** (Aktivieren), um Administratoren den Remote-Zugriff auf das Webkonfigurationsprogramm des Geräts zu ermöglichen. Standardmäßig ist die Remoteverwaltung deaktiviert. Wenn das Kontrollkästchen deaktiviert ist, fahren Sie mit Schritt 8 fort.

Anmerkung: Wenn die Remoteverwaltung aktiviert ist, kann jeder Benutzer auf den Router zugreifen, der seine IP-Adresse kennt. Vor der Aktivierung dieser Funktion muss das Standardkennwort des Geräts geändert werden.

Schritt 4: Wählen Sie im Feld "*Remote Access*" eine gewünschte Optionsschaltfläche für den

Typ des Remote Access-Protokolls. Das Protokoll wird verwendet, um Geräte aus einem Remote-Wide Area Network (WAN) direkt mit dem Router zu verbinden. HTTPS ist sicherer als HTTP und stellt die empfohlene Option dar.

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)

Die verfügbaren Optionen werden wie folgt definiert.

- HTTP - Clients können sich über das Standard-Hypertext Transfer Protocol (HTTP) mit internen Websites verbinden. HTML-Elemente Ihrer Websites werden direkt an das Client-Gerät gesendet. Die Verbindung zu Websites über HTTP ist schneller als HTTPS.
- HTTPS - Mithilfe des HyperText Transfer Protocol Secure (HTTPS) können Clients nur dann eine Verbindung zu internen Websites herstellen, wenn die auf der Website installierten digitalen Zertifikate mit dem zugehörigen Webserver authentifiziert werden. Dadurch werden alle Man-in-the-Middle-Angriffe zwischen dem Client und der Website verhindert. Wenn Sie diese Option auswählen, wird auch eine bidirektionale Verschlüsselung zwischen dem Client und der Website bereitgestellt.

Schritt 5. Aktivieren Sie im Feld *Remote Upgrade* das Kontrollkästchen **Enable (Aktivieren)**, damit Administratoren das Gerät von einem Remote-WAN aus aktualisieren können.

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)

Schritt 6. Wählen Sie im Feld *Zugelassene Remote-IP-Adresse* aus, welche IP-Adressen Remote-Zugriff auf das Gerät haben sollen. Klicken Sie auf die Optionsschaltfläche **Any IP Address (Beliebige IP-Adresse)**, um die Verbindung mit einem beliebigen Remote-Gerät zuzulassen, oder auf die Optionsschaltfläche darunter, um manuell einen Bereich zulässiger IP-Adressen einzugeben.

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)

Schritt 7: Geben Sie den Port ein, auf dem der Remote-Zugriff erlaubt ist. Der Standardport ist 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)

Anmerkung: Beim Remote-Zugriff auf den Router müssen Sie den Remote-Management-Port als Teil der IP-Adresse eingeben. Beispiele: **https://<remote-ip>:<remote-port>** oder **https://168.10.1.11:443**.

Schritt 8: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.

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="checkbox"/> Manual Port: <input type="text"/>
Block Cookies:	<input type="checkbox"/> Auto <input type="checkbox"/> Manual Port: <input type="text"/>
Block ActiveX:	<input type="checkbox"/> Auto <input type="checkbox"/> Manual Port: <input type="text"/>
Block Proxy:	<input type="checkbox"/> Auto <input type="checkbox"/> Manual Port: <input type="text"/>
<input checked="" type="button"/> Save <input type="button"/> Cancel	

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.