

# Log-instellingen op de RV130 en RV130W configureren

## Doel

De loginstellingen definiëren de logboekregels en uitvoerbestemmingen voor foutmeldingen, berichten over autorisatieschending en overtrekgegevens, aangezien er verschillende gebeurtenissen op het netwerk worden vastgelegd. De loginstellingen kunnen ook aangeven welke systeemberichten worden vastgelegd op basis van de voorziening die het bericht heeft gegenereerd en het ernst ervan.

Remote log-servers kunnen het beheer van netwerken vereenvoudigen door te centraliseren waar berichten worden vastgelegd en gearhiveerd voor een betere organisatie. Als gevolg hiervan gaan ze niet verloren als de router wordt gereset of de stroom wordt gedreven.

Het doel van dit document is uit te leggen hoe u loginstellingen kunt configureren op de RV130 en de RV130W.

## Toepasselijke apparaten

•RV130

RV130W

## Softwareversie

·v1.0.1.3

## Loginstellingen configureren

Stap 1. Meld u aan bij het hulpprogramma voor webconfiguratie en kies **Beheer > Vastlegging > Loginstellingen**. Het venster *Loginstellingen* wordt geopend:

Log Settings

Log Configuration

Log Mode:  Enable

Log Severity for Local Log and Email:  Emergency  Alert  Critical  Error  Warning  Notification  Information  Debugging

Email Alert:  Enable

WAN up/down  Site-to-Site IPsec VPN tunnel up/down  CPU overload  System startup

Remote Log Server Table

Remote Log Server	Log Severity	Enable
No data to display		

Add Row Edit Delete

Save Cancel

Stap 2. Selecteer in het veld *Logmodus* het aanvinkvakje **Enable** om het inloggen op het apparaat in te schakelen.

**Log Settings**

**Log Configuration**

Log Mode:  Enable

Log Severity for Local Log and Email:  Emergency  Alert  Critical  Error  Warning  Notification  Information  Debugging

Email Alert:  Enable

WAN up/down  Site-to-Site IPsec VPN tunnel up/down  CPU overload  System startup

**Remote Log Server Table**

<input type="checkbox"/>	Remote Log Server	Log Severity
<input type="checkbox"/>	No data to display	

Add Row Edit Delete

Save Cancel

Stap 3. Controleer de gewenste selectievakjes in het veld *Log Severity for Local Log and Email* die overeenkomen met de categorieën van gebeurtenissen die u wilt registreren.

**Log Settings**

**Log Configuration**

Log Mode:  Enable

Log Severity for Local Log and Email:  Emergency  Alert  Critical  Error  Warning  Notification  Information  Debugging

Email Alert:  Enable

WAN up/down  Site-to-Site IPsec VPN tunnel up/down  CPU overload  System startup

**Remote Log Server Table**

<input type="checkbox"/>	Remote Log Server	Log Severity
<input type="checkbox"/>	No data to display	

Add Row Edit Delete

Save Cancel

De beschikbare opties zijn als volgt gedefinieerd en worden in volgorde van hoogste tot laagste prioriteit vermeld:

- Noodgeval — Het bericht wordt geregistreerd als een apparaat is uitgeschakeld of onbruikbaar is. Het bericht wordt normaal uitgezonden naar alle processen.
- Waarschuwing — Het bericht wordt vastgelegd als er een ernstig defect aan het apparaat optreedt, bijvoorbeeld als alle functies van het apparaat niet meer werken.
- Kritisch — Het bericht wordt geregistreerd als er kritieke apparaatstoring is, zoals twee poorten die niet goed functioneren terwijl de resterende poorten prima werken.
- Fout — Bericht wordt vastgelegd als er een fout in een apparaat is, zoals één poort die offline is.
- Waarschuwing — Het bericht wordt geregistreerd als een apparaat goed werkt, maar er treedt een operationeel probleem op.
- Kennisgeving — Het bericht wordt geregistreerd als een apparaat correct functioneert, maar een systeembericht optreedt.
- Informatie — Het bericht wordt geregistreerd als er een voorwaarde die geen foutvoorwaarde is op het apparaat bestaat, maar kan aandacht of speciale behandeling

vereisen.

·Debugging — Biedt alle gedetailleerde debugging berichten.

**Opmerking:** De opties voor de ernst van het logbestand die op lagere prioriteitsniveaus worden geplaatst, worden automatisch met de opties voor de ernst van het logbestand met hogere prioriteitsniveaus geselecteerd en gecontroleerd. Als u bijvoorbeeld **Error** logs kiest, worden naast Error logs ook Emergency-, Alert- en Critical logs opgenomen.

Stap 4. In het veld *E-mailwaarschuwing* vinkt u het aanvinkvakje **Enable** aan zodat uw apparaat e-mailwaarschuwingen kan versturen voor specifieke gebeurtenissen of gedragingen die gevolgen kunnen hebben voor de prestaties en beveiliging, of voor foutopsporingsdoeleinden.

The screenshot shows the 'Log Settings' configuration page. Under the 'Log Configuration' section, the 'Log Mode' is set to 'Enable'. The 'Log Severity for Local Log and Email' section has checkboxes for Emergency, Alert, Critical, Error, Warning, Notification, Information, and Debugging, all of which are checked. The 'Email Alert' checkbox is also checked and highlighted with a red rectangle. Below it, there are checkboxes for 'WAN up/down', 'Site-to-Site IPsec VPN tunnel up/down', 'CPU overload', and 'System startup', which are currently unchecked. The 'Remote Log Server Table' section is empty, showing 'No data to display' and buttons for 'Add Row', 'Edit', and 'Delete'. At the bottom, there are 'Save' and 'Cancel' buttons.

**Opmerking:** Om e-mailmeldingen volledig te kunnen configureren, moeten uw e-mailinstellingen ook op het apparaat worden geconfigureerd. Raadpleeg [E-mailinstellingen op de RV130 en RV130W](#) voor meer informatie.

Stap 5. (Optioneel) Als *Email Alert* is ingeschakeld in Stap 4, controleer dan de aankruisvakjes die overeenkomen met de gebeurtenissen waarvoor u e-mailberichten wilt ontvangen.

This screenshot is similar to the previous one, but with the checkboxes for 'WAN up/down', 'Site-to-Site IPsec VPN tunnel up/down', 'CPU overload', and 'System startup' checked and highlighted with a red rectangle. The rest of the configuration remains the same.

De beschikbare opties zijn als volgt gedefinieerd:

·WAN omhoog/omlaag — Verstuur een e-mailwaarschuwing als de WAN-link omhoog of omlaag is.

·IPsec VPN-tunnel van site-to-site omhoog/omlaag — Hiermee wordt een e-mailwaarschuwing verzonden wanneer een VPN-tunnel tot stand is gebracht, een VPN-tunnel is omlaag of de VPN-tunnelonderhandeling mislukt.

·CPU-overbelasting — Verstuur een e-mailwaarschuwing als het CPU-gebruik gedurende meer dan een minuut hoger is dan de opgegeven drempel en verstuur een andere e-mailwaarschuwing wanneer het gebruik gedurende meer dan een minuut terugloopt naar normale niveaus.

·Opstarten van het systeem — Verstuur elke keer dat het systeem wordt opgestart een e-mailwaarschuwing.

## Remote-logservers toevoegen/bewerken

Stap 1. Klik in de tabel *met de externe logserver* op **Rij toevoegen**.

<input type="checkbox"/>	Remote Log Server	Log Severity
<input type="checkbox"/>	No data to display	
<b>Add Row</b> Edit Delete		

Er wordt een nieuwe rij weergegeven met nieuwe velden en opties beschikbaar:

<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input type="checkbox"/>	1.1.1.1	<input checked="" type="checkbox"/> Emergency <input checked="" type="checkbox"/> Alert <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Error <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Notification <input checked="" type="checkbox"/> Information <input type="checkbox"/> Debugging	<input checked="" type="checkbox"/>
Add Row Edit Delete			

Stap 2. Voer in de kolom *Remote Log Server* het IP-adres in van de logserver die de logbestanden in het veld van de rij zal verzamelen.

<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input type="checkbox"/>	192.168.1.100	<input type="checkbox"/> Emergency <input type="checkbox"/> Alert <input type="checkbox"/> Critical <input type="checkbox"/> Error <input type="checkbox"/> Warning <input type="checkbox"/> Notification <input type="checkbox"/> Information <input type="checkbox"/> Debugging	<input type="checkbox"/>
Add Row Edit Delete			

Save Cancel

Stap 3. Controleer onder de kolom *Log Severity* de gewenste ernst van de logbestanden op de corresponderende externe logserver.

<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input type="checkbox"/>	192.168.1.100	<input checked="" type="checkbox"/> Emergency <input checked="" type="checkbox"/> Alert <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Error <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Notification <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Debugging	<input type="checkbox"/>
Add Row Edit Delete			

Save Cancel

Stap 4. Selecteer in de kolom *Enable* het aanvinkvakje om de loginstellingen voor de betreffende externe logserver in te schakelen.

Remote Log Server Table			
<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input type="checkbox"/>	192.168.1.100	<input checked="" type="checkbox"/> Emergency <input checked="" type="checkbox"/> Alert <input checked="" type="checkbox"/> Critical <input checked="" type="checkbox"/> Error <input checked="" type="checkbox"/> Warning <input checked="" type="checkbox"/> Notification <input checked="" type="checkbox"/> Information <input checked="" type="checkbox"/> Debugging	<input checked="" type="checkbox"/>

Add Row Edit Delete

Save Cancel

Stap 5. Als u de informatie voor een bepaalde externe logserver wilt bewerken, selecteert u het item door het bijbehorende selectievakje in te schakelen en op de knop **Bewerken** te klikken.

Remote Log Server Table			
<input type="checkbox"/>	Remote Log Server	Log Severity	Enable
<input checked="" type="checkbox"/>	192.168.1.100	Emergency, Alert, Critical, Error, Warning, Notification, Information, Debugging	Enabled

Add Row Edit Delete

Save Cancel

**Opmerking:** U moet op **Opslaan** klikken nadat u een nieuwe rij hebt gemaakt om deze te kunnen bewerken.

Stap 6. Klik op **Opslaan** om de instellingen op te slaan.

Als u de logbestanden wilt weergeven, navigeert u naar **Status > Logbestanden bekijken** in het hulpprogramma voor webconfiguratie. De pagina *Logbestanden bekijken* opent en toont de *systemlogtabel*:

View Logs

System Log Table			
Log Index	Log Time	Log Severity	Description
1	2014-09-18 12:19:40 PM	err	syslog-ng[1962]: Connection broken to AF_INET(192.168.1.100:514), reopening in 60 seconds
2	2014-09-18 12:19:40 PM	debug	syslog_bsd: start cron to do "41 0 * * mon root/sbin/bsd check "
3	2014-09-18 12:19:40 PM	debug	syslog_bsd: Start bsd_cron
4	2014-09-18 12:19:40 PM	info	w0: Disconnected WDS link with a4-18:75:e1:75:72 (Manual Mode)
5	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
6	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
7	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
8	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
9	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
10	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
11	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
12	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
13	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
14	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
15	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
16	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
17	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
18	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
19	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)
20	2014-09-18 12:19:40 PM	info	w0: Connected WDS link with a4-18:75:e1:75:72 (Manual Mode)

Refresh Logs Clear Logs Save Logs

Showing 1 - 20 of 374 20 per page Page 1 of 19

## Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.