# **Configure Log Settings on the RV130 and RV130W**

## Objective

Log settings define the logging rules and output destinations for error messages, authorization violation messages, and trace data as various events are recorded on the network. Log settings can also specify which system messages are logged based on the facility that generated the message and its severity level.

Remote log servers can make managing networks easier by centralizing where messages are logged and archived for improved organization. As a result, they are not lost if the router is reset or power cycled.

The objective of this document is to explain how to configure log settings on the RV130 and the RV130W.

#### **Applicable Devices**

- RV130
- RV130W

### **Software Version**

### **Configuring Log Settings**

Step 1. Log in to the web configuration utility and choose **Administration** > **Logging** > **Log Settings**. The *Log Settings* window opens:

<sup>•</sup> v1.0.1.3

Log Settings							
Log Configuration							
Log Mode:	Enable						
Log Severity for Local Log and Email:	t 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 Lo	og Server Log Severity Enal	ale					
No data to display							
Add Row Edit E	Delete						
Save Cancel							

Step 2. In the Log Mode field, check the Enable check box to enable logging on the device.

Log Settings						
Log Configuration						
Log Mode:	V 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				
No data to display						
Add Row Edit De	Add Row Edit Delete					
Save Cancel						

Step 3. Check the desired check boxes in the *Log Severity for Local Log and Email* field that correspond to the categories of events you would like to be logged.

Log Settings					
Log Configuration					
Log Mode:	🗹 Enable				
Log Severity for Local	Log and Email: 🛛 🗹 Emergency	y 🗹 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	r Table				
	Remote Log Server	Log Severity			
📃 🗌 No data to disp	blay				
Add Row Edit Delete					
Save Can	ncel				

The available options are defined as follows and listed in order of highest to lowest priority:

• Emergency — Message is logged if a device is down or unusable. The message is normally broadcast to all processes.

• Alert — Message is logged if there is a serious device malfunction, such as a case in which all device features stop working.

• Critical — Message is logged if there is critical device malfunction, such as two ports not functioning properly while the remaining ports work fine.

• Error — Message is logged if there is an error within a device, such as a single port being offline.

• Warning — Message is logged if a device is functioning properly, but an operational problem occurs.

• Notification — Message is logged if a device is functioning properly, but a system notice occurs.

• Information — Message is logged if a condition that is not an error condition exists on the device, but may require attention or special handling.

• Debugging — Provides all detailed debugging messages.

**Note:** Selecting log severity options placed at lower priority levels will automatically include and check any log severity options with higher priority levels. For example, choosing **Error** logs automatically includes Emergency, Alert, and Critical logs in addition to Error logs.

Step 4. In the *Email Alert* field, check the **Enable** check box to allow your device to send email alerts for specific events or behaviors that may impact performance and security, or for debugging purposes.

Log Settings						
Log Configuration						
Log Mode:	Enable					
Log Severity for Local Log and Email:	Emergence	cy 🗹 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				
No data to display						
Add Row Edit Delete						
Save Cancel						

**Note:** In order to fully configure Email Alerts, your email settings must also be configured to the device. Refer to *Email Settings on the RV130 and RV130W* for more information.

Step 5. (Optional) If *Email Alert* is enabled in Step 4, check the check boxes that correspond to the events you would like to receive email alerts for.

I	Log Settings					
	Log Configuration					
	Log Mode:	C Enable				
	Log Severity for Local Log and Email:	Emergency 🗹 Alert 🗹 Critical 🖉 Error 🖤 Warning 🖤 Notification 🖤 Information 📝 Debugging				
	Email Alert:	C 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				
	No data to display					
	Add Row Edit Delete					
	Save Cancel					

The available options are defined as follows:

• WAN up/down — Sends an email alert if the WAN link is up or down.

• Site-to-Site IPsec VPN tunnel up/down — Sends an email alert when a VPN tunnel is established, a VPN tunnel is down, or the VPN tunnel negotiation fails.

• CPU overload — Sends an email alert if the CPU utilization is higher than the specified threshold for over a minute and sends another email alert when the utilization drops back to normal levels for

over a minute.

• System startup — Sends an email alert each time the system is booted up.

#### **Add/Edit Remote Log Servers**

Step 1. In the *Remote Log Server* table, click Add Row.

Remote Log Server Table					
	Remote Log Server	Log Severity			
No data to display					
Add Rov	v Edit	Delete			

A new row appears with new fields and options available:

Remote Log Server Table					
		Remote Log Server	Log Severity	Enable	
		1.1.1.1	🖉 Emergency 🖉 Alert 🖉 Critical 🖉 Error 🖉 Warning 🖉 Notification 🖉 Information 🗖 Debugging		
4	Add Row Edit Delete				

Step 2. Under the *Remote Log Server* column, enter the IP address of the log server that will collect the logs in the field of the row.

Remote Log Server Table							
	Remote Log Server	Log Severity	Enable				
	192.168.1.100	Emergency Alert Critical Error Warning Notification Information Debugging					
Add Row	Add Row Edit Delete						
Save	Save Cancel						

Step 3. Under the *Log Severity* column, check the desired severity of the logs for the corresponding remote log server.

Remote Log Server Table						
	Remote Log Server	Log Severity	Enable			
	192.168.1.100	Emergency 🗹 Alert 🗹 Critical 🗹 Error 🗹 Warning 🗹 Notification 🗹 Information 🗹 Debugging				
Add Row	Edit Delete					
Save	Save Cancel					

Step 4. Under the *Enable* column, check the check box to enable the logging settings for the corresponding remote log server.



Step 5. To edit the information for a particular remote log server, select the entry by checking its corresponding check box and clicking the **Edit** button.



Note: You must click Save after creating a new row to be able to edit it.

Step 6. Click Save to save your settings.

If you would like to view the logs, navigate to **Status** > **View Logs** in the web configuration utility. The *View Logs* page opens and displays the *System Log Table*:

View Logs			
System Log Table			Showing 1 - 20 of 374 20 👻 per page
Filter: Log Severity matches Emergency Alert Critical Error Warnin	g 🗹 Notification 🗹 Informat	tion 🗹 Debugging 🛛 Go	
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	wI0: Disconnected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
5 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
6 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
7 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
8 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
9 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
10 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
11 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
12 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
13 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
14 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
15 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
16 2014-09-18 12:19:40 PM	info	w10: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
17 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
18 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
19 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
20 2014-09-18 12:19:40 PM	info	wI0: Connected WDS link with a4:18:75:e1:75:72 (Manual Mode)	
Refresh Logs Clear Logs Save Logs			I∢ ≺ Page 1 of 19 ▶ ▶1