System Logs Configuration on RV220W and RV120W

Objective

The log messages are subsystem events that occur during the operation of the running device. The device saves these messages in the system.log file. The device determines which subsystem messages to log by its configured logging level. The logging level designates that the device logs emergency, alert, critical, error, and warning messages for the subsystem. The GSS also logs notification, informational, and debugging messages.

With the help of the logs, a user can determine the type of traffic that comes in to the LAN, and alert the user when someone on the LAN tries to access a blocked WAN address. Logs also help with identifying port scans, attacks, and administrative logins.

This document explains how to view logs on the RV220W.

Applicable Devices

- RV220W
- RV120W

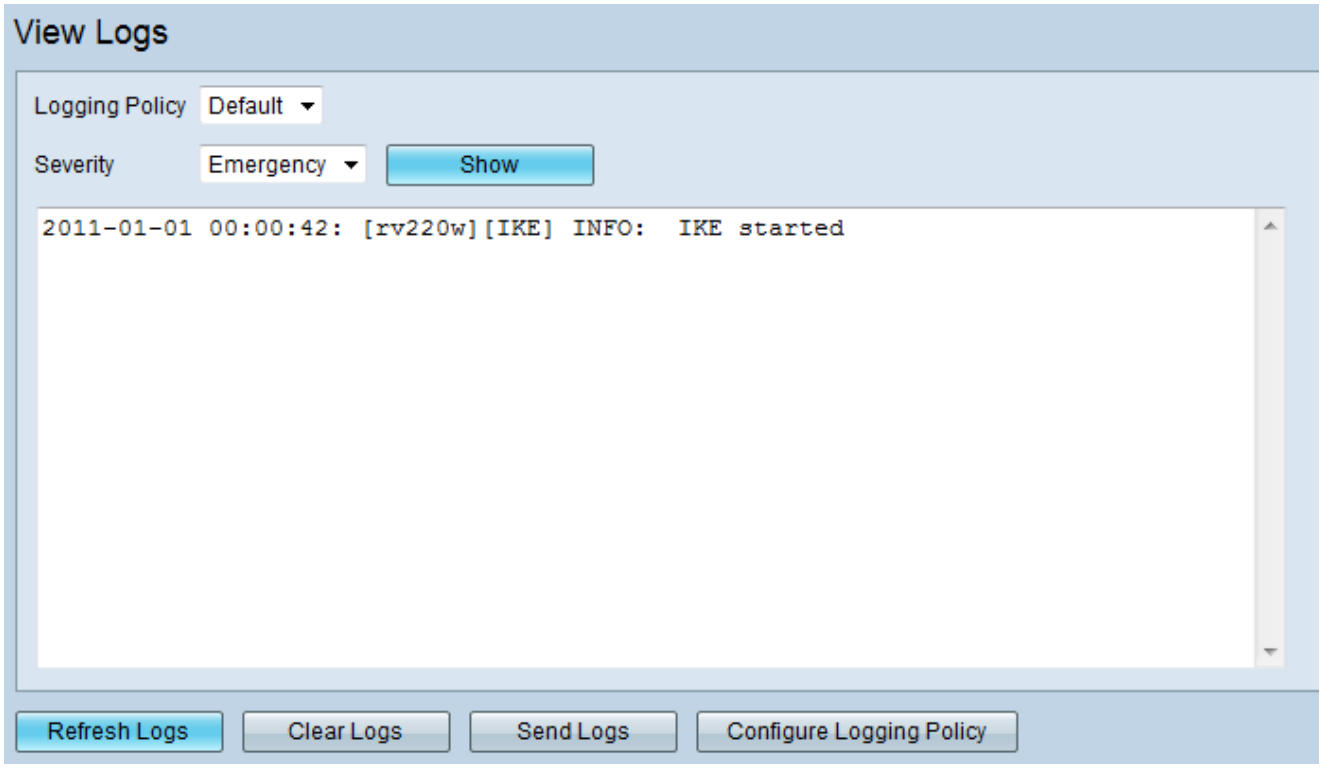
Software Version

- v1.0.4.17

System Logs Configuration

View System Logs

Step 1. Log in to the web configuration utility and choose **Status > View Logs**. The *View Logs* page opens:



Step 2. Choose the appropriate Logging Policy from the drop-down list:

• Default — Shows the default logging message according to the default policy defined.

Note: Policies except default need to be configured manually.

Step 3. Choose the appropriate option from the Severity drop-down list:

• Emergency — Choose this to find logs when the system is unusable with an emergency state. Like an "urgent" condition which affects multiple apps/servers/sites. All tech will be notified when this happens.

• Alert — Choose this to find logs when immediate action was needed. This needs to be corrected immediately therefore notify staff. An example of this would be the loss of a primary ISP connection.

• Critical — Choose this to find logs when the device was in critical condition. These logs can be fixed right away but these logs indicate primary failure of system. An example of this would be the loss of the backup ISP connection. These logs are directed at the global level.

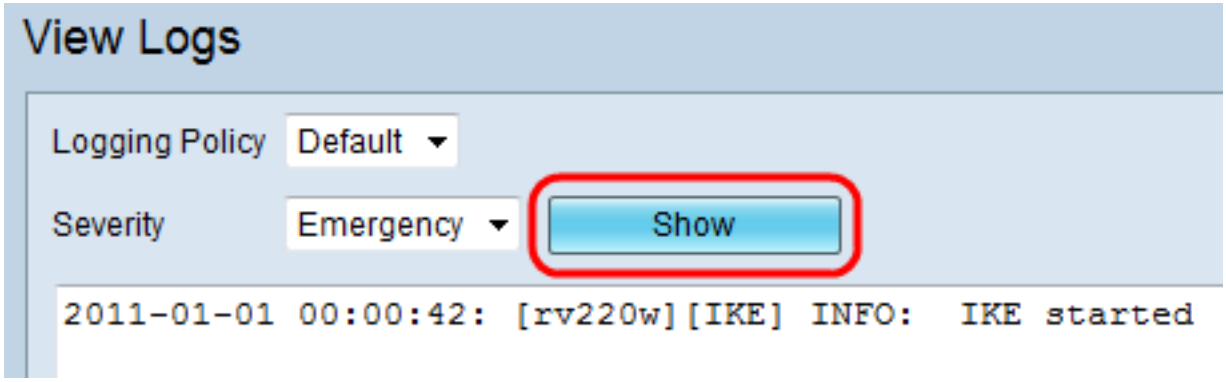
• Error — Choose this to find logs pertaining to error conditions. These logs indicate an upcoming serious problem, but are in a category that does not require immediate attention. These log messages can be described as non-urgent failures and need to be relayed to developers or admins. Each error log needs to be taken care of within a given time.

• Warning — Choose this to find logs with warning conditions. This is a forewarning of potential problems, but not a response to an actual warning. It is a warning that indicates that a component or application is not in an ideal state. These messages are not an error, but indication that an error will occur if action is not taken, such as when the file system is 85% full.

• Notification — Choose this to find logs which are normal but have significant conditions. These logs are not like error conditions. The solution set to these log messages is to summarize them in an email and email your admins or developers to spot a potential problem, but an immediate action is not required.

• Information — Choose this to find logs which have informational messages only. These log messages contain non-critical information for the admin and can be further harvested for reporting issues.

• Debugging — Choose this to find logs which have debugging messages only. These logs are useful to developers for debugging the application, but not useful amidst operations.



Step 4. Click **Show** to get the appropriate severity logs records.

Step 5. Choose the appropriate log options from the bottom of the page:

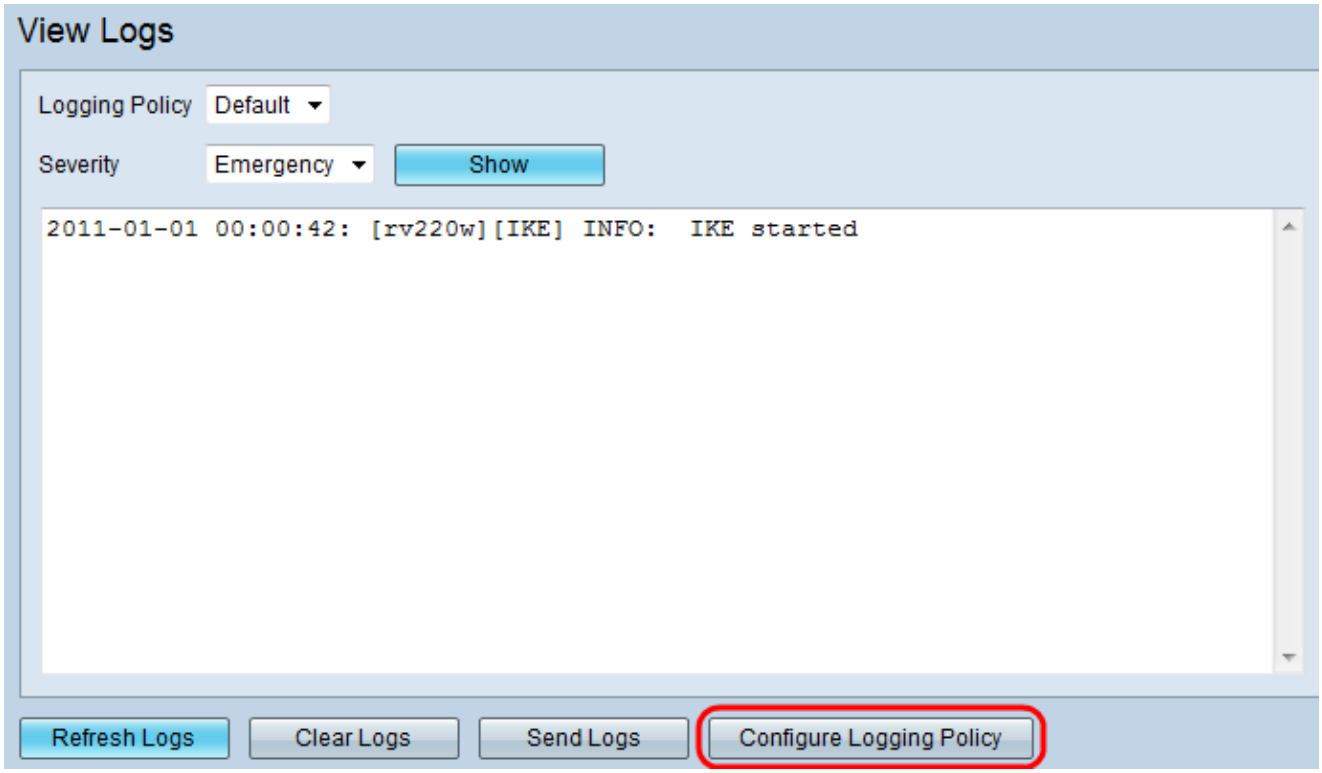
• Refresh Logs — Refreshes the logs and restarts capturing logs from then.

• Clear Logs — Clears all the logs.

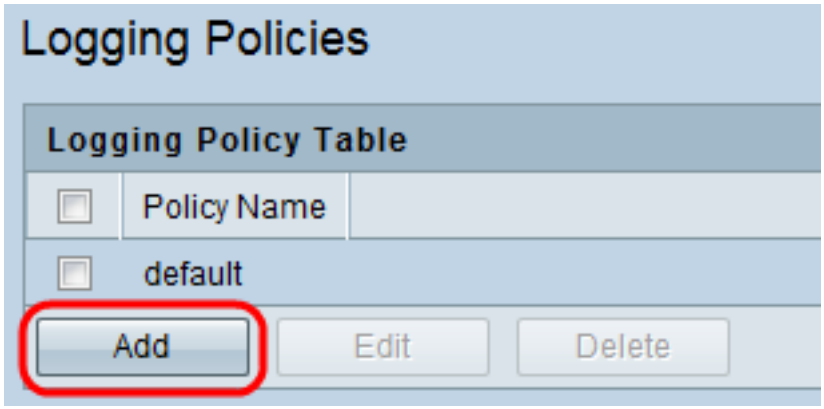
• Send Logs — Sends logs to the configured email address.

Add a Logging Policy

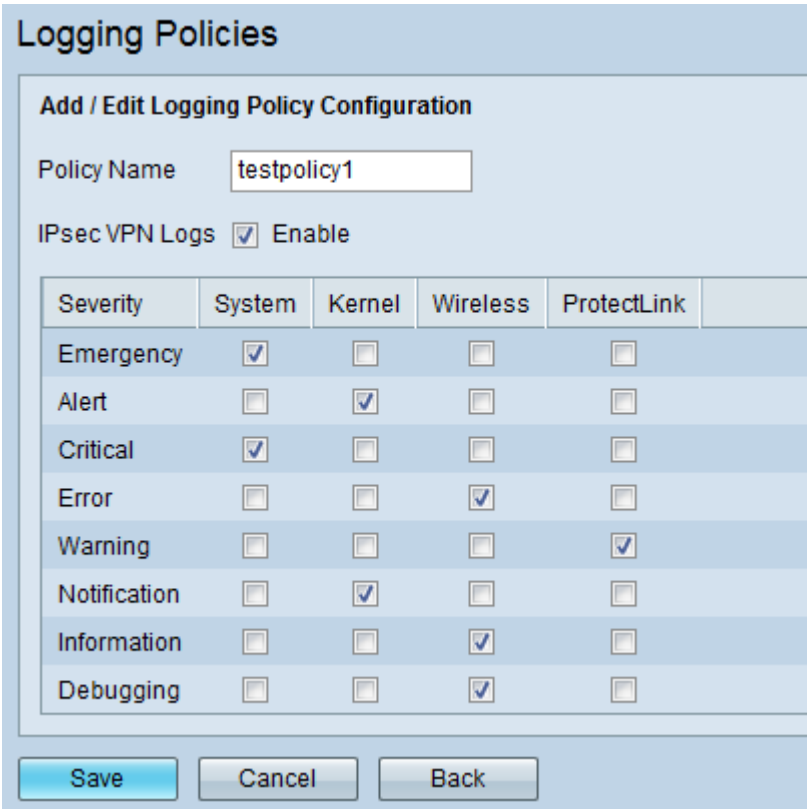
Step 1. Log in to the web configuration utility and choose **Status > View Logs**. The *View Logs* page opens:



Step 2. Click **Configure Logging Policy** and the *Logging Policy Table* page opens:



Step 3. Click **Add** and the *Add / Edit Logging Policy Configuration* page opens:



Step 4. Enter the desired policy name in the Policy Name field.

Step 5. Check the **IPsec VPN Logs** check box to enable IPsec VPN logs. These logs are related to ipsec negotiations and are related to user space logs.

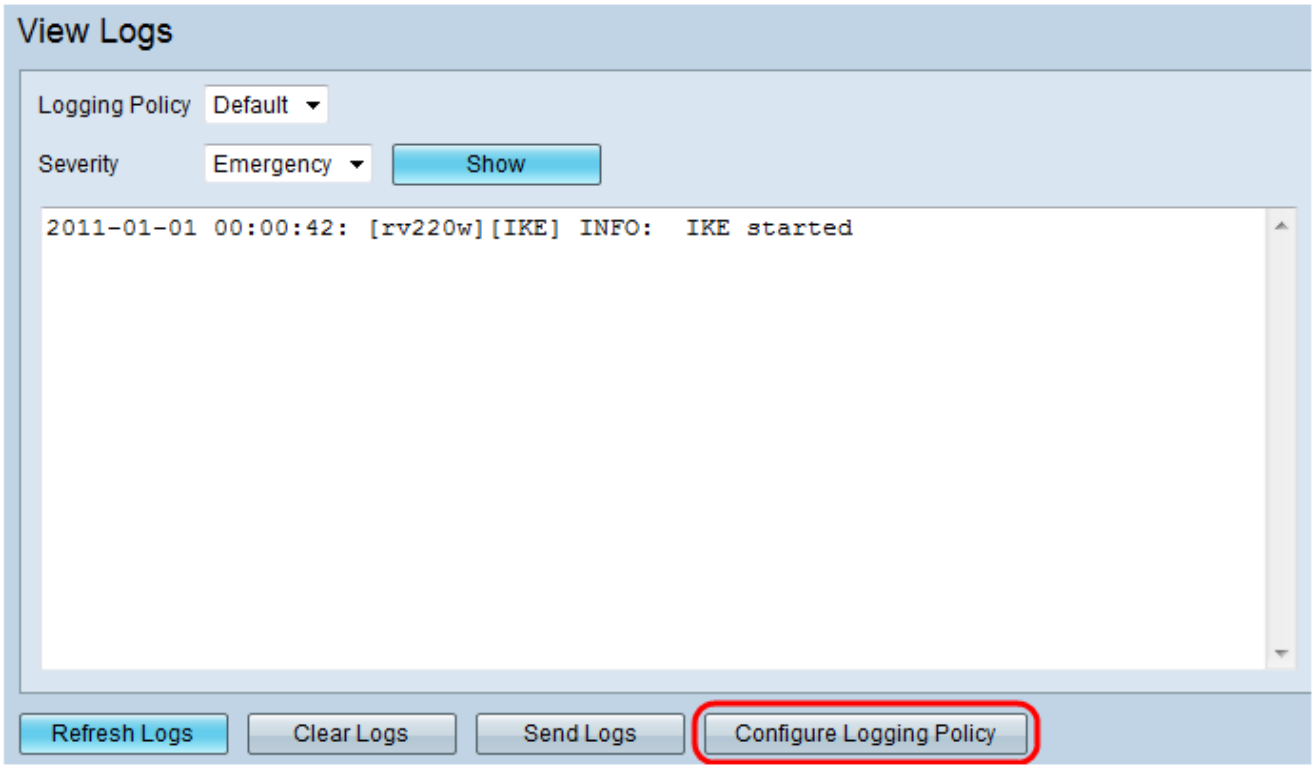
Step 6. Appropriately configure the policy as needed from the check box table:

- ProtectLink — Protectlink logs are a hosted service which integrate powerful anti-spam, URL Content Filter and Web Reputation to block standalone, blended-threat, and customer-specific attacks. These features don't allow unwanted content to pass through the router.
- Kernel — Kernel logs are those that are a part of kernel code (for example, firewall).
- System — System logs are those that are a part of user-space applications (for example, NTP and DHCP).
- Wireless — Wireless Logs are those that are related to wirless connection and negotiations.

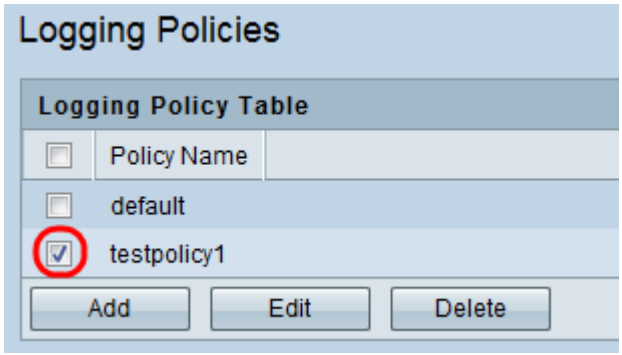
Step 7. Click **Save** to store the added policy.

Edit a Logging Policy

Step 1. Log in to the web configuration utility and choose **Status > View Logs**. The *View Logs* page opens:

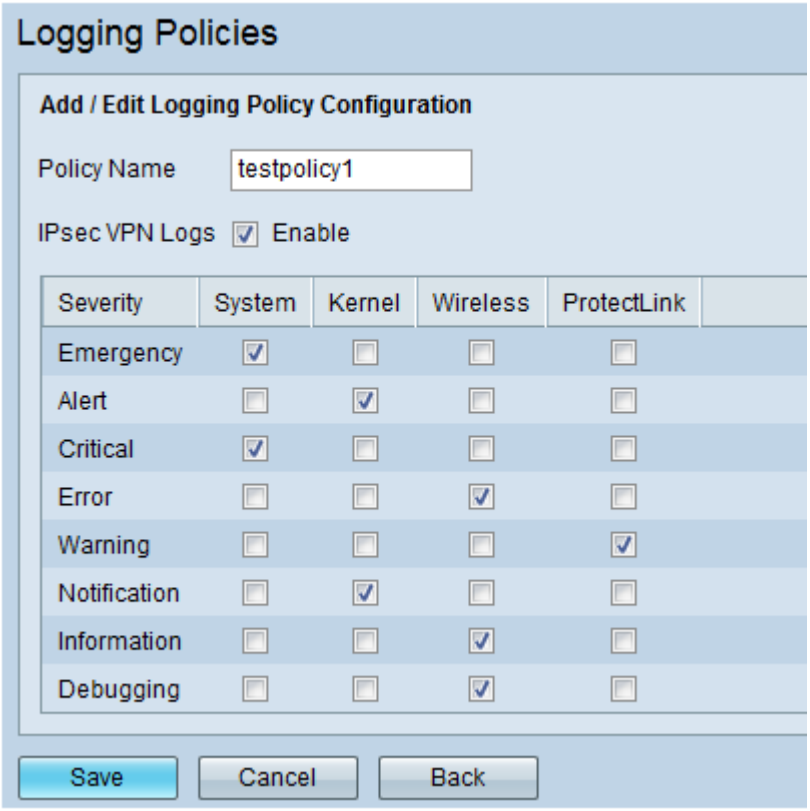


Step 2. Click **Configure Logging Policy** and the *Logging Policy Table* page opens:



Step 3. Check the check box adjacent to the policy you wish to edit.

Step 4. Click **Edit** and the *Add / Edit Logging Policy Configuration* page opens:



Step 5. Edit the policy as desired and click **Save** to store the changes made.

- ProtectLink — Protectlink logs are a hosted service which integrate powerful anti-spam, URL Content Filter and Web Reputation to block standalone, blended-threat, and customer-specific attacks. These features prevent unwanted content to pass through the router.

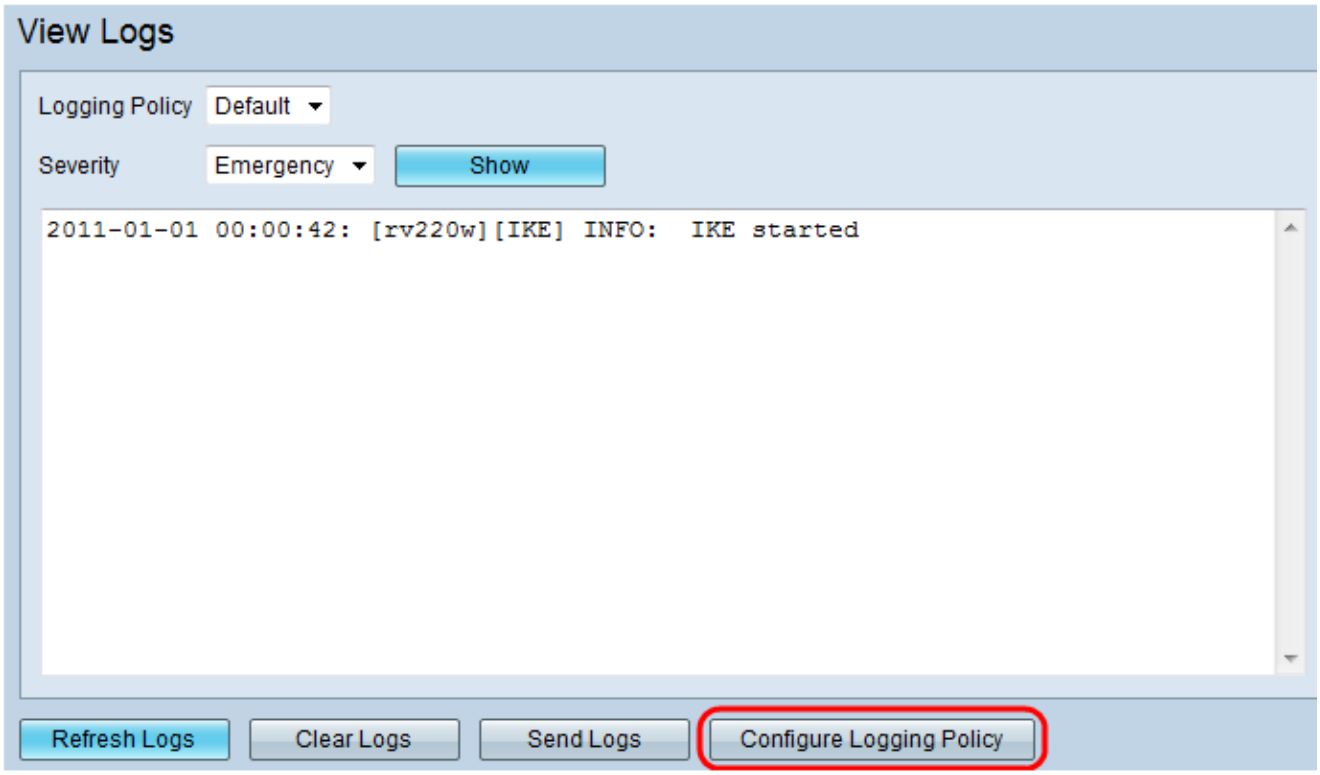
- Kernel — Kernel logs are those that are a part of kernel code (for example, firewall).

- System — System logs are those that are a part of user-space applications (for example, NTP and DHCP).

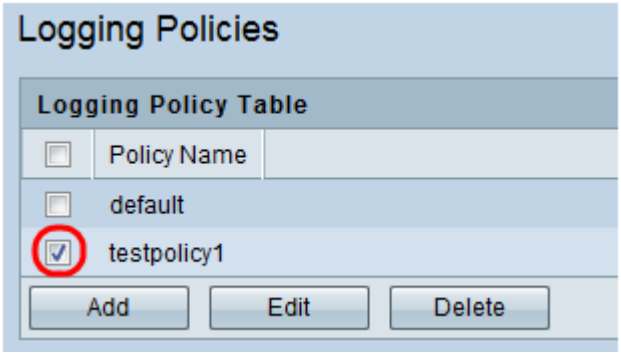
- Wireless — Wireless Logs are those that are related to wirless connection and negotiations.

Delete a Logging Policy

Step 1. Log in to the web configuration utility and choose **Status > View Logs**. The *View Logs* page opens:

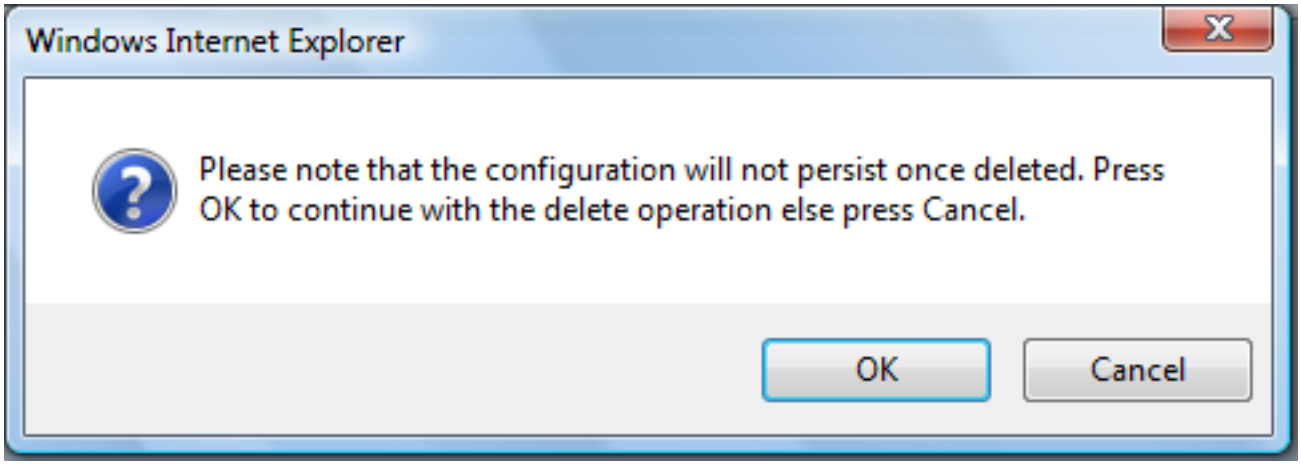


Step 2. Click **Configure Logging Policy** and the *Logging Policy Table* page opens:



Step 3. Check the check box adjacent to the policy you wish to delete.

Step 4. Click **Delete** and a warning window appears:



Step 5. Click **OK** to continue and delete the policy.