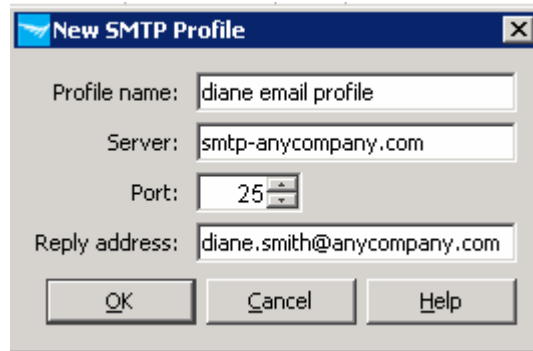


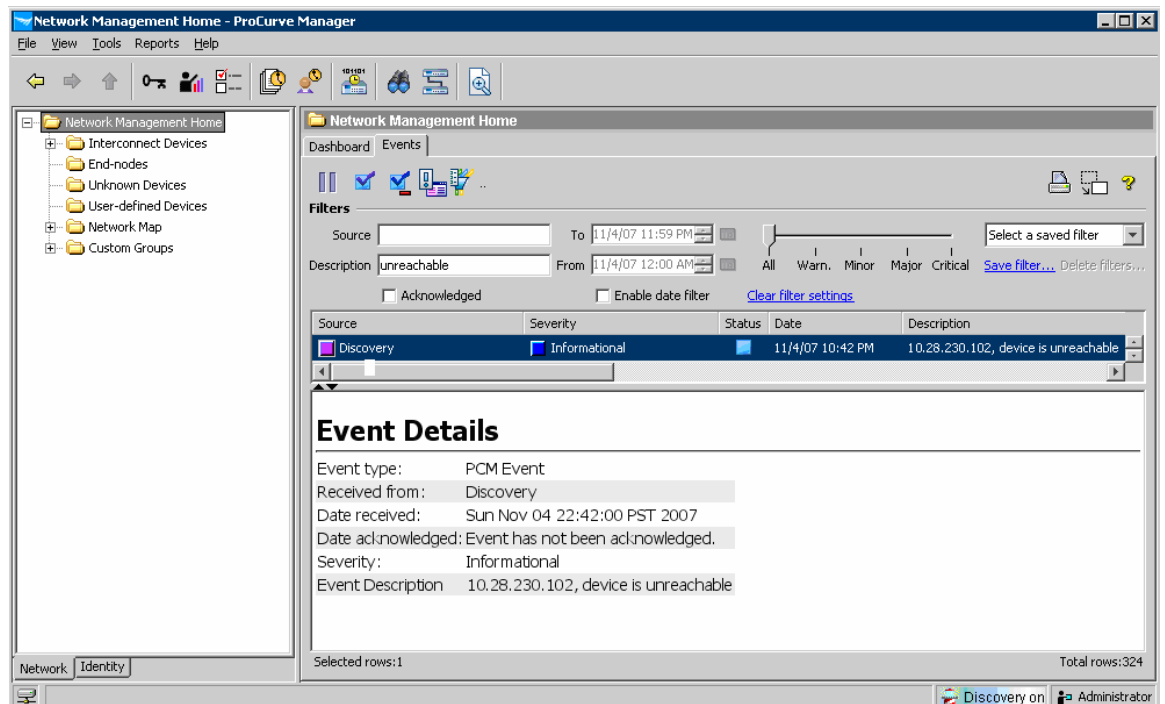
Creating a PCM policy to send an email alert when a device goes down, or becomes unreachable


This Configuration Example describes the steps necessary to create an email alert when PCM+ discovers that a device is no longer reachable and unable to send a trap. This situation may be caused by the device being down or because network connectivity between the device and the PCM server has been interrupted.

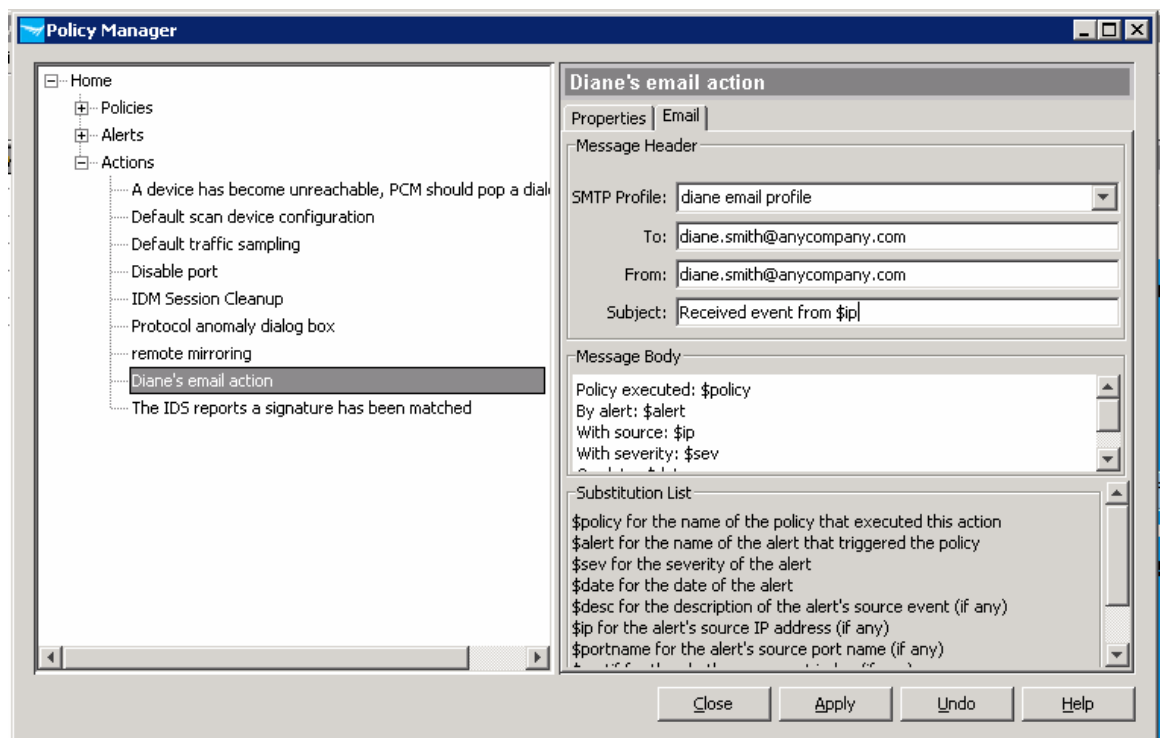
1. Go to the Preferences window and create or verify your SMTP profile is valid.



2. To set the Policy Manager action type of sending an email, the alert to trigger the action must be defined. The trigger is a specific discovery event log message of “device is unreachable,” which PCM generates when it can no longer hear a device, and turns that device indicator **red** in the Interconnected Devices column. This event can only be seen from the Network Management Home events tab, since it is generated internally by PCM, and not by a specific device.

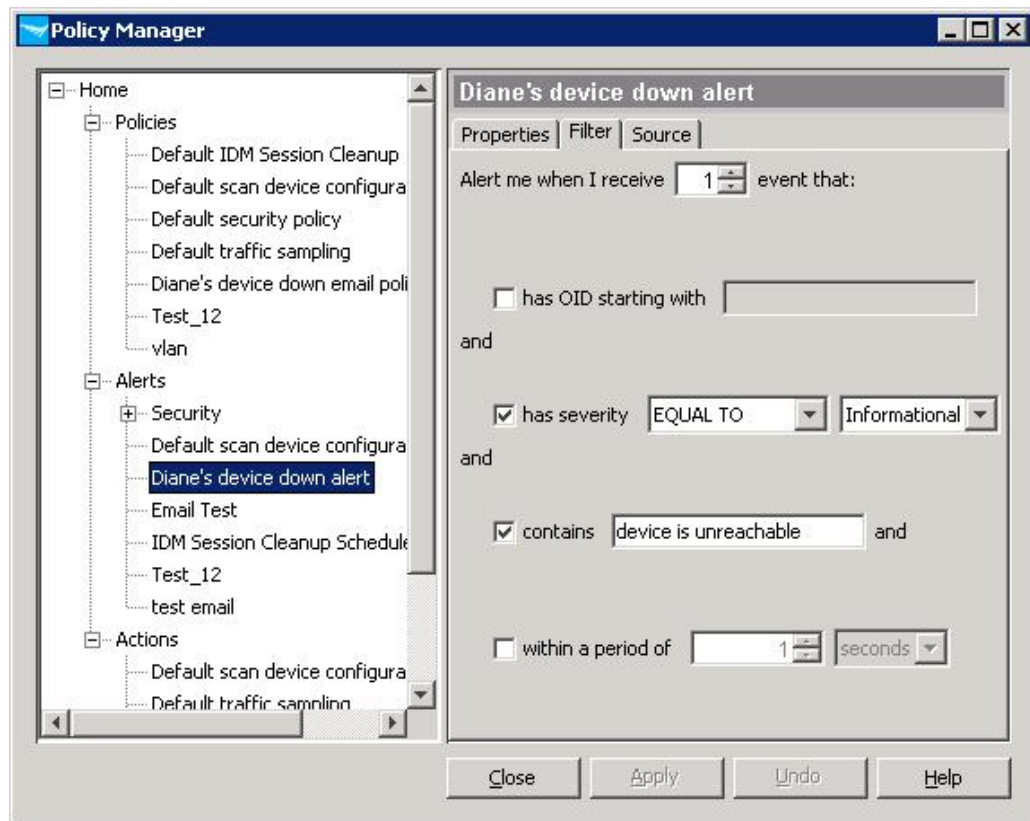


3. From PCM, click the Policy Manager icon  in the toolbar to launch the Policy Configuration Manager window.
4. Highlight on Actions in the left panel and click on the “new” button.
5. Select the Action type from the pull-down menu, “*Policy Manager: send email*” and give this action a name (e.g. Diane’s email action).
6. Select the Email tab and choose your SMTP profile (that was created in step 1) from the pull-down menu.
7. Enter the email address of a person you want to receive the alert and the email address of the person reporting the alert.
8. Click Apply to save the changes.



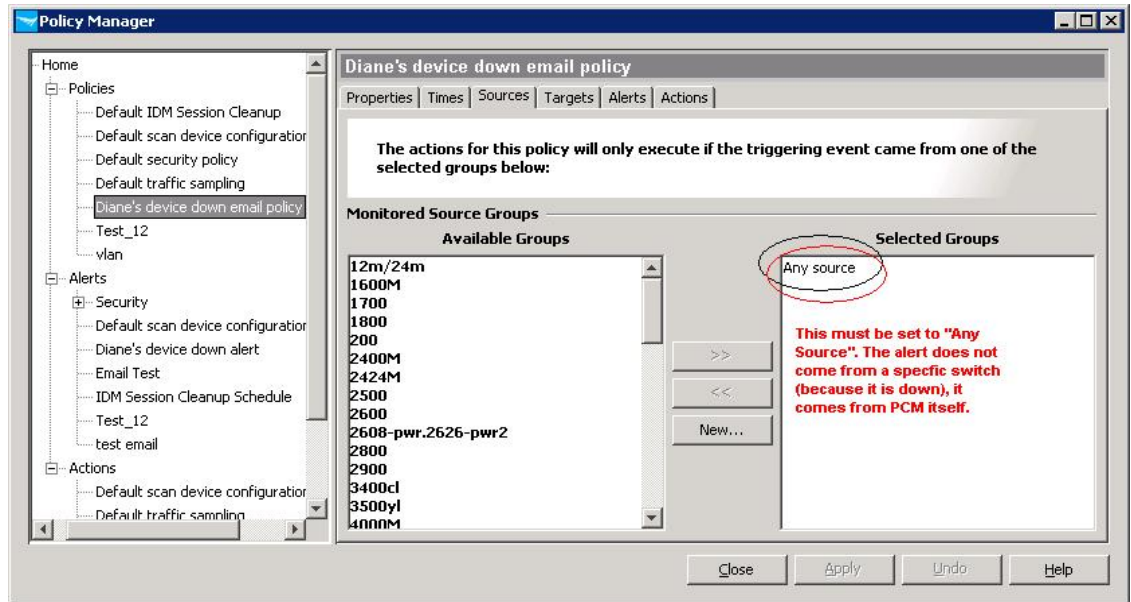
9. In Policy Manager highlight on Alerts in the left panel and click on the “new” button.
10. Select the Alert type from the pull-down menu, “*Policy Manager: Event-based alert*” and name this alert (e.g. Diane’s device down alert).

11. Click the Filter tab to enter the event filter criteria.
12. Choose the following filtering options: Click the **has severity** checkbox, then use the pull down menus to select the operator “*Equal to,*” and the severity level “*Informational.*”
13. Click the **contains** checkbox and enter the text, *device is unreachable*. (This is the actual text of the event and must be exactly correct).



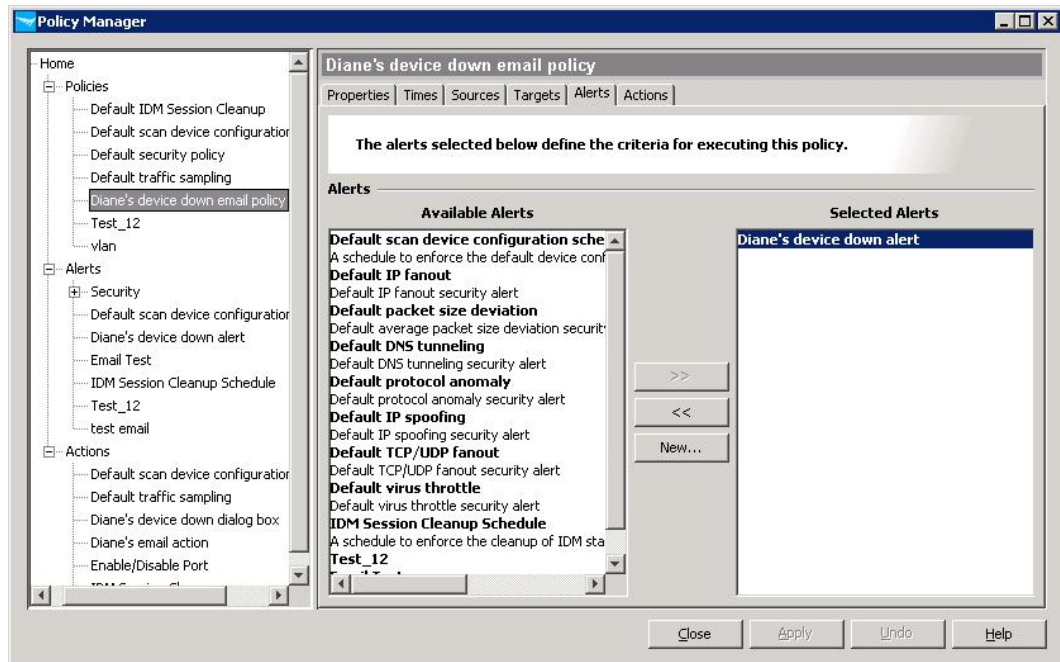
14. Click the Source tab to set Alert Source criteria. Click the radio button for “*Alert source as event source*”.
15. Click Apply to save the changes.
16. In Policy Manager, highlight on Policies and click on the “new” button.
17. Name the policy (e.g. Diane’s device down email policy).
18. Click the Times tab to configure the time periods that will be applied for your policy.

19. Click the Sources Tab to configure the device groups from which an event trigger will be applied.
20. The Selected Groups **MUST ONLY HAVE “Any Source”**. Do not select or move any other groups over from the Available Groups side.

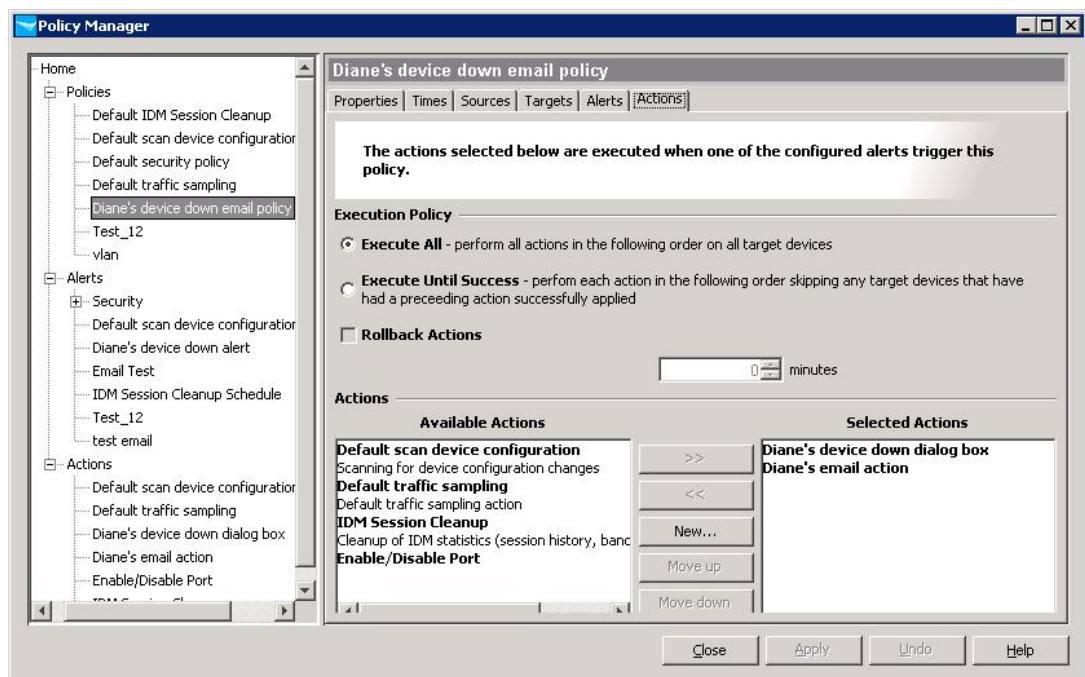


21. Click the Targets Tab to configure the device groups to which the policy action will be applied.
22. Click the radio button for “No targets for this policy.”

23. Click the Alerts tab to configure the alerts that will trigger the policy execution.
24. Highlight and move the custom Alert you created in Step 9 (e.g. Diane's device down alert) over to the Selected Alerts column on the right.

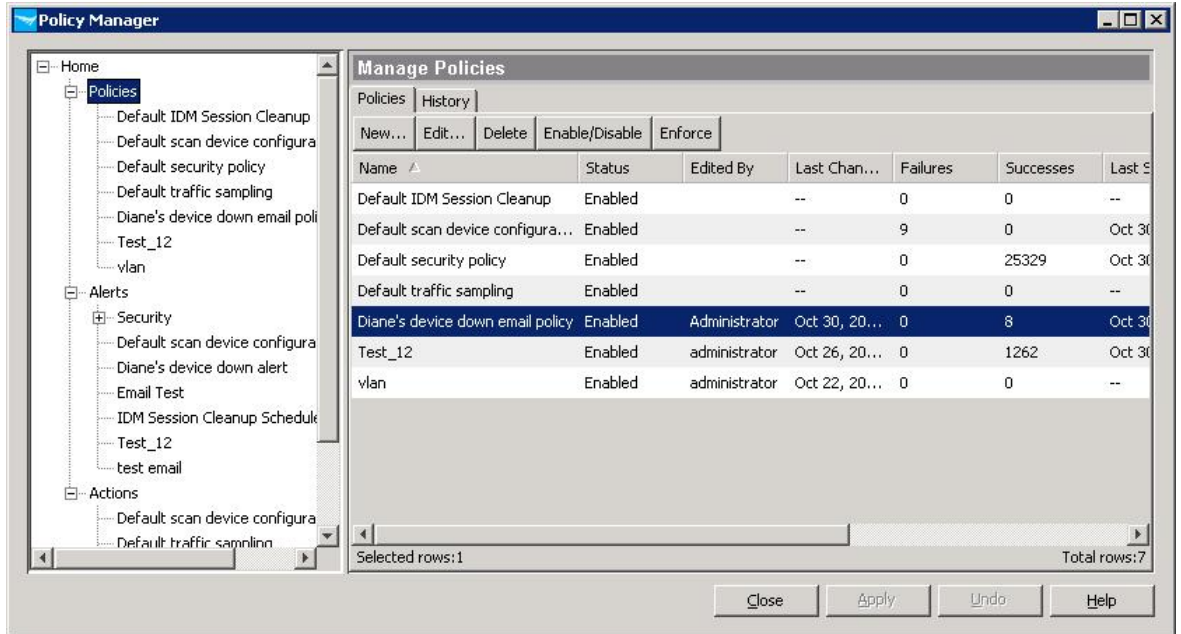


25. Click the Actions tab to configure the actions the policy will take when it is executed.
26. Highlight and move the custom action you created in Step 4 (e.g. Diane's email action) over to the Selected Actions column on the right. You may have to expand the window to see the actions.



27. Click Apply to save the changes.

28. Verify the new policy is enabled.



29. The new policy is enabled and will send an email alert when PCM Discovery reports a device is unreachable.

For more information, see the Using Policy Manager Features section of the ProCurve Manager *Network Administrator's Guide*.

To find out more about
ProCurve Networking
products and solutions,
visit our web site at

www.procurve.com



© 2007 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

November 2007