Release Notes:
Version 1.0.22 Software
for the ProCurve Network Access Controller 800

Release 1.0.22 supports the ProCurve Network Access Controller 800 (J9065A)

These release notes include information on the following:

If Using IDM with the ProCurve Network Access Controller 800 Version 2.2 is Required

IDM version 2.2 (or greater) is required for use with the ProCurve NAC 800. Also, the IDM agent software supplied with version 2.2 must be installed. IDM 2.2 is available on the ProCurve Web site. Click here to go to the software download page.

ProCurve NAC Implementation Start-up Service Required for Endpoint Integrity Checking

Endpoint Integrity Agents require that an initial Implementation Service be provided by a ProCurve certified service provider or purchased through ProCurve. For more information, see Networking services on the ProCurve Web site.

Licenses Required for Endpoint Integrity Checking

A ProCurve Network Access Controller Agent license is required to perform endpoint integrity checks. Licenses are available in quantities of 100, 250, 1,000, and 5,000. Contact your ProCurve sales representative for information on obtaining the licenses you need.

Publication Number

Part Number 5991-2124
September 2007B

Applicable Product

ProCurve Network Access Controller 800 (J9065A)

Trademark Credits

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation. Windows Vista is either a registered trademark or trademark of Microsoft Corporation in the United States and/or other countries. Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

Warranty

See the Customer Support/Warranty booklet included with the product.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
http://www.procurve.com

Contents

Software Management

Manual Updates

Known Software Issues and Feature Limitations

(This page intentionally left blank)

Software Management

Software Updates

Check the ProCurve Networking Web site frequently for free software updates for the various ProCurve products you may have in your network.

Downloading Documentation and Software from the Web

You can download the latest product documentation from ProCurve Networking's Web site. Software updates for the ProCurve NAC 800 are available through the product's Web browser interface. An Internet connection is required.

To Download Product Documentation:

You will need the Adobe® Acrobat® Reader to view, print, and/or copy the product documentation.

1. Go to ProCurve Networking's Web site at **http://www.procurve.com**.
2. Click on **Technical support**, then **Product manuals**.
3. Click on the name of the product for which you want documentation.
4. On the resulting Web page, double-click on a document you want.
5. When the document file opens, click on the disk icon  in the Acrobat® toolbar and save a copy of the file.

To Download a Software Version:

1. Log on to the ProCurve NAC 800 Web browser interface, `https://<IP-Address>`.
2. Click on **System configuration** and then **Management server**.
3. Scroll to the bottom of the page and click on **check for upgrades**. The NAC 800 uses the Internet to check for available updates. If updates are available, follow the prompts.

Manual Updates

The following sections contain updated or new information for the ProCurve Network Access Controller 800 documentation.

ProCurve Network Access Controller 800 Hardware Installation Guide, June, 2007

LEDs and the LCD

The ProCurve Network Access Controller 800 has LEDs that indicate its status and its network connections. In addition, an LCD display provides system status information and may be used with the built-in, six-button keypad to set up and configure the unit.

Figure 1. ProCurve Network Access Controller 800 LEDs and LCD

The unit performs a power on self test (POST) when power is supplied or the system is reset. All of the LEDs turn on when the test begins, and then begin normal operation as described below.

Table 1. ProCurve NAC 800 LEDs

LEDs	State	Meaning
Power (green)	On	The unit is receiving power.
	Off	The unit is NOT receiving power.
Fault (orange)	Off	The normal state; indicates that there are no fault conditions on the unit.
	Blinking[1]	A fault has occurred on the unit.
	On	On briefly at the beginning of the self test after the unit is powered on or reset. If on for a prolonged time, the unit has encountered a fatal hardware failure, or has failed its self test. See "Diagnosing with the LEDs" for more information.
Locator (blue)	On	The Locator LED is used to locate a specific unit in a group of equipment, typically a rack. To turn the LED On or Off, use a console or secure shell (SSH) session to the **Application Main Menu > Diagnostics > Locator LED**. The LED remains On until it is manually turned Off.
	Off	The normal state.
Speed	Off	The the port is operating at 10 Mbps or there is no connection.
	Green	The port is operating at 100 Mbps.
	Amber	The port is operating at 1000 Mbps.
Link /Activity	On	Indicates the port is enabled and receiving a link beat signal.

[1] The blinking behavior is an on/off cycle once every 1.6 seconds, approximately.

Diagnosing with the LEDs

Table 2 shows LED patterns on the unit that indicate problem conditions.

1. Check in the table for the LED pattern you see on your unit.
2. Refer to the corresponding diagnostic tip on the next few pages.

Table 2. LED Error Indicators

LED Pattern Indicating Problems		Problem	Solution
Power	**Fault**		
Off with power cord plugged in	[1]	The unit is not plugged into an active AC power source.	1. Verify the power cord is plugged into an active power source and to the unit. Ensure these connections are snug. 2. Try power cycling the unit by unplugging and plugging the power cord back in. 3. If the Power LED is still not on, verify the AC power source works by plugging another device into the outlet. Or try plugging the unit into a different outlet or try a different power cord. If the power source and power cord are OK and this condition persists, the power supply may have failed. Call your ProCurve authorized LAN dealer, or use the electronic support services from ProCurve to get assistance. See the Customer Support/ Warranty card for more information.
On, but unit not operating; LCD backlight is off, but message is displayed.	Off	The unit has been shutdown from the LCD menu or the Application Main Menu (4. Shutdown).	Press and hold the button on the ✔ on the keypad for eight seconds or power cycle the unit by unplugging and then replugging the power cord.
On	Prolonged On	A hardware failure has occurred. All the LEDs will stay on indefinitely.	Try power cycling the unit. If the fault indication reoccurs, the unit may have failed. Call your ProCurve authorized LAN dealer, or use the electronic support services from ProCurve to get assistance. See the Customer Support/Warranty card for more information.
On	Blinking[2]		

[1] This LED is not important for the diagnosis.
[2] The blinking behavior is an on/off cycle once every 1.6 seconds, approximately.

ProCurve Network Access Controller 800 Users' Guide, June 2007

Importing the NAC 800 Server Certificate for Use by IAS

If the NAC 800's self-signed certificate fails to copy to the IAS server, you can manually export it off the NAC 800 using the keytool utility and an SCP application such as PSCP. You can then manually copy the certificate to the IAS server and install in as a trusted root certificate.

See "Installing a Self-signed Certificate as a Trusted Root on Endpoints and Servers" on page 7 to learn how to use keytool and PSCP to export certificates.

Creating and Replacing SSL Certificates

Note

All of the steps in these sections—"Creating a New Self-signed Certificate" and "Using an SSL Certificate from a Known Certificate Authority (CA)"— should be performed on the MS and each ES.

The MS will present the SSL certificate when you access its Web browser interface. The ESs will use their certificates to communicate with the IAS plug-in (if you have selected that option for 802.1X quarantining), as well as with endpoints during integrity testing.

The "Creating a New Self-signed Certificate" section in the user's guide is missing steps step 7 to step 12. The section below is the corrected text for that section.

The "Using an SSL Certificate from a Known Certificate Authority (CA)" section in the user's guide is missing steps step 2, step 3, and step 16. "Using an SSL Certificate from a Known Certificate Authority (CA)" on page 8 is the corrected text for that section.

Creating a New Self-signed Certificate

You can create a self-signed certificate on the NAC 800 itself. For the NAC 800 to use the certificate for HTTPS, the certificate must be stored in **/usr/local/nac/keystore/compliance.keystore** and added as a trusted root certificate to the **/usr/local/java/jre/lib/security/cacerts** keystore.

Follow these steps to generate the self-signed certificate:

1. Log in as root to the NAC 800 via an SSH or console session.
2. Remove the existing keystore by entering the following at the command line:

```
rm -f /usr/local/nac/keystore/compliance.keystore
```

3. The same command generates the private/public keypair and encloses the public key in the self-signed certificate. Enter the following at the command line:

   ```
   keytool -genkey -keyalg RSA -alias <key_alias>
   -keystore /usr/local/nac/keystore/compliance.keystore
   ```

   Where:

   <key_alias> is the name for the private key/public key and certificate within the keystore file

4. The keytool utility prompts you for the following information:
   - **Keystore password**—You must enter **changeit** for the password.
   - **First and Last Name**—Enter the fully-qualified domain name (FQDN) of the NAC 800. This fully-qualified name includes the host name and the domain name—for example, **MyNAC.procurve.com**. (For testing purposes on a single machine, the FQDN is **localhost**.)
   - **Organizational unit**—Enter the appropriate value.
   - **Organization**—Enter the name of your organization.
   - **City or locality**—Enter the city or location.
   - **State or province**—Enter the unabbreviated state or province.
   - **Two-letter country code**—Enter a two-letter country code. The code for the United States is **US**.
5. Review the information you entered. Enter **yes** if it is correct. (Press **[Return]** to make a change.)
6. The keytool utility prompts you for **Key password for <key_alias>**. Do not enter a password; press **[Return]** to use the same password that was given for the keystore password.
7. Export the self-signed certificate to a file with this command:

   ```
   keytool -export -alias <key_alias> -keystore
   /usr/local/nac/keystore/compliance.keystore -file <filename>
   ```

   Where:

   <key_alias> is the name for the private key/public key and certificate within the keystore

   <filename> is the name under which the certificate will be saved
8. When prompted, enter the password for the keystore (**changeit**).
9. Install the certificate as a trusted root certificate in the **/usr/local/java/jre/lib/security/cacerts** keystore:

   ```
   keytool -import -alias <CA_alias> -keystore
   /usr/local/java/jre/lib/security/cacerts -file <filename>
   ```

   Where:

   <CA_alias> is a name that identifies the self-certificate you just created

   <filename> is the name under which you saved the self-certificate in the previous step
10. When prompted, enter the password for the keystore (**changeit**).

11. If you are prompted, enter **yes** to trust the certificate.
12. Restart the HTTPS server with this command:
    - **On an MS**—`service nac-ms restart`
    - **On an ES**—`service nac-es restart`

Installing a Self-signed Certificate as a Trusted Root on Endpoints and Servers

The NAC 800 presents its self-signed certificate to endpoints accessing its HTTPS server. Because the certificate is self-signed, the endpoint will not trust it until you install the certificate on the endpoint as a trusted root CA certificate. You might also need to install the certificate on an IAS server.

Follow these steps:

1. Log in as root to the NAC 800.
2. If you created a new self-signed certificate, you have already exported the certificate to a file (see step 7 on page 6). Make a note of the filename and move to step 3 on page -8.

   Otherwise, complete these steps:

   a. View the certificate in the compliance.keystore:

   ```
   keytool -list -v -keystore /usr/local/nac/keystore/compliance.key-
   store -storepass changeit
   ```

   Figure 2 shows the example output when you use the **-v** (verbose) option. The certificate in this example is the factory default self-signed certificate.

```
Keystore type: jks
Keystore provider: SUN
Your keystore contains 1 entry
Alias name: procurvenac800                    <-- Alias
Creation date: Jun 29, 2007
Entry type: keyEntry
Certificate chain length: 1
Certificate[1]:
Owner: CN=Hewlett-Packard Company, OU=procurve, O=Hewlett-Packard
Company, L=Palo Alto,
ST=California, C=US
Issuer: CN=Hewlett-Packard Company, OU=procurve, O=Hewlett-Packard
Company, L=Palo Alto,
ST=California, C=US
Serial number: 46854158
Valid from: Fri Jun 29 10:28:56 PDT 2007 until: Wed Mar 24 10:28:56
PDT 2010
Certificate fingerprints:
MD5: 10:18:BA:0D:3B:E8:0B:13:A4:34:F8:86:55:EC:07:A8
SHA1: 79:5B:59:58:60:BA:02:EB:D1:B6:26:D6:F1:79:B1:FF:D4:7D:BC:46
```

Figure 2. Viewing Certificates with Keytool

b. Make a note of the alias.

c. Export the certificate to a file:

```
keytool -export -alias <alias> -keystore
/usr/local/nac/keystore/compliance.keystore -file <filename> -store-
pass changeit
```

Where:

<alias> is the name for the private key/public key and certificate within the keystore

<filename> is the name under which the certificate will be saved

3. Follow these steps to save the certificate file off the NAC 800 to a server or station that runs PSCP:

a. Access the command line for the endpoint that runs PSCP (click **Start** > **Run** and enter **cmd**) and move to the directory in which PSCP is installed.

b. Enter this command:

```
pscp root@<IP address>:<filename> <filename_endpoint>
```

Where:

<IP address> is the IP address of the NAC 800

<filename> is the name you chose for the certificate

<filename_endpoint> is the name under which the certificate will be saved on the endpoint

c. When prompted, enter the NAC 800's root password.

4. You can now copy the certificate to other devices and install it as a trusted root CA certificate.

The exact steps for installing the certificate depend on the station or server OS and your environment. For example, in a Windows domain, you can publish the certificate in Active Directory. Check the appropriate documentation for instructions.

Using an SSL Certificate from a Known Certificate Authority (CA)

You can install a certificate signed by a CA on the NAC 800, which the NAC 800 will use for HTTPS. The certificate must be installed in **/usr/local/nac/keystore/compliance.keystore**. If the CA that signs the certificate is your own CA or a less well-known CA, its root certificate must be added to the **/usr/local/java/jre/lib/security/cacerts** keystore. Table 3 lists well-known CAs for which certificates are installed in the **cacerts** keystore at factory defaults.

Table 3. CAs Trusted at Factory Defaults

CA	
AddTrust	Sonera
Comodo	Starfield
Cybertrust	Thawte
Entrust	UserTrust
Equifax Secure	Valicert
GeoTrust	VeriSign
Go Daddy	

Follow these steps to generate a certificate request, submit it to a CA, and install the CA-signed certificate:

1. Log in as root to the NAC 800 via an SSH or console session.
2. Remove the existing keystore by entering the following at the command line:

   ```
   rm -f /usr/local/nac/keystore/compliance.keystore
   ```

3. Generate the private/public keypair for the certificate by entering following at the command line:

   ```
   keytool -genkey -keyalg RSA -alias <key_alias>
   -keystore /usr/local/nac/keystore/compliance.keystore
   ```

   Where:

   <key_alias> is the name for the private/public keypair

4. The keytool utility prompts you for the following information:
   - **Keystore password**—You must enter **changeit** for the password.
   - **First and Last Name**—Enter the fully-qualified domain name (FQDN) of the NAC 800. This fully-qualified name includes the host name and the domain name—for example, **MyNAC.procurve.com**. (For testing purposes on a single machine, the FQDN is **localhost**.)
   - **Organizational unit**—Enter the appropriate value.
   - **Organization**—Enter the name of your organization.
   - **City or locality**—Enter the city or location.
   - **State or province**—Enter the unabbreviated state or province.
   - **Two-letter country code**—Enter a two-letter country code. The code for the United States is **US**.
5. Review the information you entered. Enter **yes** if it is correct. (Press **[Return]** to make a change.)
6. The keytool utility prompts you for **Key password for <key_alias>**. Do not enter a password; press **[Return]** to use the same password that was given for the keystore password.

7. Generate a certificate request. Enter the following at the command line:

   ```
   keytool -certreq -alias <key_alias> -keystore
   /usr/local/nac/keystore/compliance.keystore -file <filename>
   ```

   Where:

   <key_alias> is the name for the private key/public key and certificate within the keystore (set in step step 3)

   <filename> is the name under which the certificate request will be saved

8. When prompted, enter the password for the keystore (**changeit**).
9. Transfer the certificate request off the NAC 800. Follow these steps to transfer the request to a management station that runs PSCP:
   a. Access the command line for the station that runs PSCP (click **Start** > **Run** and enter **cmd**) and move to the directory in which PSCP is installed.
   b. Enter this command:

      ```
      pscp root@<IP address>:<filename> <filename_station>
      ```

      Where:

      <IP address> is the IP address of the NAC 800

      <filename> is the name you chose for the certificate request

      <filename_station> is the name under which the certificate request will be saved on the management station
   c. When prompted, enter the NAC 800's root password.
10. Submit the certificate request to your CA.
11. After the CA sends you the certificate, transfer it to the NAC 800:
    a. Save the certificate to the management station that runs PSCP.
    b. Access the command line for the station (click **Start** > **Run** and enter **cmd**) and move to the directory in which PSCP is installed.
    c. Enter this command:

       ```
       pscp <cert_filename> root@<IP address>:<cert_filename_nac>
       ```

       Where:

       <IP address> is the IP address of the NAC 800

       <cert_filename> is the name of the certificate file

       <cert_filename_nac> is the name under which the certificate will be saved on the NAC 800
    d. When prompted, enter the NAC 800's root password.

e. If your CA is not listed in Table 3, obtain the CA root certificate and transfer it to the NAC 800 with this command:

```
pscp <ca_filename> root@<IP address>:<ca_filename_nac>
```

Where:

<IP address> is the IP address of the NAC 800

<ca_filename> is the name of the CA root certificate file

<ca_filename_nac> is the name under which the CA root certificate will be saved on the NAC 800

Enter the NAC 800's root password when prompted.

12. Log in as root to the NAC 800.
13. Complete this step if your CA is not listed in Table 3:
    a. Import the CA certificate as a trusted certificate by entering the following from the command line:

```
keytool -import -alias <CA_alias> -keystore
/usr/local/java/jre/lib/security/cacerts -file <ca_filename_nac>
```

Where:

<CA_alias> is a name that identifies your CA

<ca_filename_nac> is the name under which you saved the CA root certificate in step step 11-step e.

    b. When prompted, enter the password for the keystore (**changeit**).
    c. If you are prompted, enter **yes** to trust the certificate.
14. Import the CA-signed certificate:

```
keytool -import -alias <key_alias> -keystore
/usr/local/nac/keystore/compliance.keystore
-trustcacerts -file <cert_filename_nac>
```

Where:

<key_alias> is the name for the private/public keypair that you set in step step 3

<cert_filename_nac> is the name under which you saved the certificate in step step 11-step c.

15. When prompted, enter the password for the keystore (**changeit**).
16. Restart the HTTPS server with this command:
    - **On an MS**—`service nac-ms restart`
    - **On an ES**—`service nac-es restart`

Known Software Issues and Feature Limitations

Software Issues

The issues known to exist with this software version are listed below. The number in parentheses is an internal tracking number.

- **Basic 802.1X Settings (9073)** — When you switch the end-user quarantine method your changes to the Basic 802.1X settings are erased.

  Workaround: Re-enter the Basic 802.1X settings.

- **iptables not Updating (8855)** — When using inline mode, and IP addresses in the Exceptions List, iptables does not update after the endpoint disconnects.

  Workaround: Use resolved names instead of IP addresses in the Exceptions List.

- **SSH not Supported for Nortel Switch (9009)** — SSH support for Nortel switches is not supported in this release.

- **MAC OS X Endpoints** — DHCP mode with endpoint enforcement is not supported in environments with OS X endpoints. OS X 10.4 and earlier do not accept static routes from DHCP acknowledgement responses. When this support is added to OS X in the future, then endpoint enforcement will function properly with OS X endpoints.

- **Inline Failover (9064)** — Using inline mode with multiple ESs for failover or load balancing is not available in this release

- **CatOS User Name in Enable Mode** (8988) — If you have a CatOS switch configured to run in enable mode with a user name, the expect script supplied with the NAC 800 will not run.

  Workaround: Do not use a user name with your switch, or modify the expect script in the console to include the user name.

  To modify the expect script in the NAC 800 console:

  NAC 800 Home window>>System configuration>>Quarantining menu option

  1.Click edit next to an 802.1X device. (You can also perform these steps while you are adding an 802.1X device.)

  2. Click the plus sign next to **Show scripts**.

  3. Add the correct expect script syntax to the text box for enable mode user name. See your switch documentation for more information on the correct syntax.

  4. Click **ok**.

- **Moving ESs between Clusters (9080)** — If you add an ES to the wrong cluster, you must reset the system in order to move it to the correct cluster.

Caution:

When a system is reset, the database is cleared, and the property files are restored to their defaults.

To move an ES to a different cluster:

1. Disconnect the ES by shutting it down or removing the network cable.
2. Log in to the NAC 800 MS console.
3. Navigate to

   NAC 800 Home window>>System configuration>>Enforcement clusters & servers.

4. Click delete next to the ES you want to remove.
5. Start the ES and log in as root using SSH or directly with a console session.
6. Enter the following command at the ES command line:

   resetSystem.py

7. Return to the NAC 800 MS console.
8. Click **Add an Enforcement server** in the Enforcement clusters & servers area. The Add Enforcement server window appears.
9. Select a cluster from the Cluster drop-down list.
10. Enter the IP address for this Enforcement server in the IP address text box.
11. Enter the fully qualified hostname to set on this server in the Host name text box.
12. Enter one or more DNS resolver IP addresses, separated by a commas, semicolons, or spaces in the DNS IP addresses text box. For example, 10.0.16.100,10.0.1.1

Note:

Enter the password to set for the root user of the ES server's operating system in the Root password text box.

13. Re-enter the password to set for the root user of the ES server's operating system in the Re-enter root password text box.
14. Click ok.
15. Click ok.

- **iptables Wrapper Script (9171)** — To avoid creating conflicts between `iptables` and the `nac-es` service, do not run the following commands manually:

  ```
  /etc/init.d/iptables
  service iptables start
  service iptables stop
  service iptables restart
  ```

  The `nac-es` service must be shutdown before making changes to the `iptables` firewall. This script ensures that errors are not introduced by making changes when `nac-es` is running.

  Use the following commands to control `iptables` from the command line:

  To stop iptables:

  ```
  fw_control stop
  ```

  To start iptables:

  ```
  fw_control start
  ```

  To restart iptables:

  ```
  fw_control restart
  ```

  To save iptables config:

  ```
  fw_control save
  ```

  To get iptables status (iptables -L):

  ```
  fw_control status
  ```

  Note:

  Note that this last command can be used even if the nac-es service is running since it makes no changes to the iptables rules.

- **802.1X and Windows Vista Endpoints (9225)** — In 802.1X mode, Vista wireless endpoints may not get an IP address in the correct VLAN. This is an issue in the Vista product that Microsoft is investigating.

  Workaround: Perform a manual `ipconfig /release` and then `ipconfig /renew`.

- **Test Results Page Cached in Safari Browser (9236)** — In some cases after an endpoint is retested, an end-user may see test results from a previous test because the Safari browser has stored the test results in its cache.

  Workaround: If the end-user believes the test results are in error, clear the browser cache and select Retest.

Windows Vista

Windows Vista is now listed as an unsupported operating system.

To allow Windows Vista operating system endpoints to access to your network without being tested:

NAC 800 Home window>>NAC policies

1. Select one of the following:
   - **Add a NAC policy** (see figure 3)
   - The name of an existing NAC policy, for example: **High security**.
2. Select the **Windows Vista, Windows ME, Windows 95** check box in the **Operating systems** area.
3. Click **ok** to save the changes and return to the **NAC policies** window.

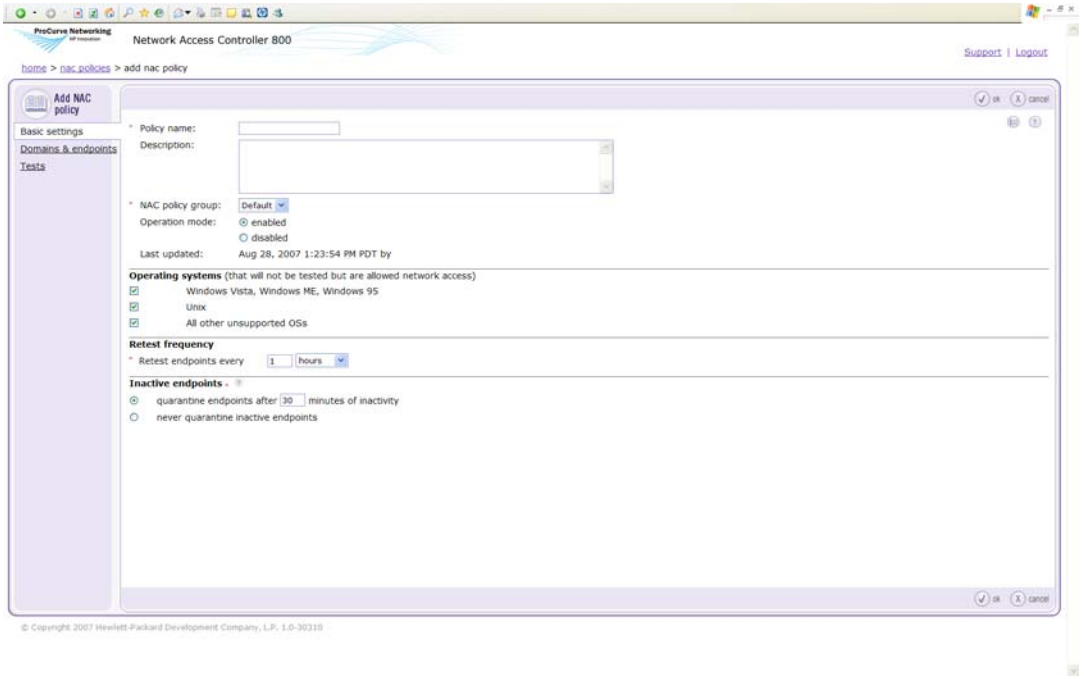

Figure 3. Add NAC policy window

Recovering Quickly from a Network Failure

Normally, most networks recover quickly from a problem. However, if you have a network with a very large number of endpoints (around 3,000 endpoints per ES), and your network goes down, performing the following steps will help ensure that your endpoints can reconnect as quickly as possible:

1. Place all of the clusters that have a large number of endpoints in allow all mode:
   a. Select **System configuration**.
   b. Click a cluster name.
   c. Select the **allow all** radio button.
   d. Click **ok**.
2. Leave the cluster in allow all mode for a full test cycle. If your test cycle is to retest endpoints every two hours, leave the cluster in allow all mode for two hours. To check the length of your test cycle:
   a. Select **NAC policies**.
   b. Click a policy name.
   c. Select the **Basic settings** menu option.
   d. In the **Retest frequency** area, check the **Retest endpoints every X hours** text field.

NOTE: The retest frequency can be different for each policy.

3. Move the clusters back to normal mode:
   a. Select **System configuration**.
   b. Click a cluster name.
   c. Select the **normal** radio button.
   d. Click **ok**.

VLAN Tagging

In some cases, such as when the DHCP server is in a separate VLAN than the span/mirror port, the mirrored port traffic is 802.1q tagged. In this case, in order for NAC 800 to recognize the traffic, the following workaround must be performed.

1. Set up the virtual interface:
   a. Log in to each ES that is monitoring a port using SSH or directly with a console session.
   b. Enter the following command at the command line:

```
cd /etc/sysconfig/network-scripts
```

c. For 802.1X mode:
   i. Enter the following at the command line:

      ```
      cp ifcfg-eth1 ifcfg-eth1.1
      ```

   ii. Open the `ifcfg-eth1.1` file with a text editor such as `vi`.
   iii. Change the following line:

      ```
      DEVICE=eth1
      ```

      To:

      ```
      DEVICE=eth1.1
      ```

d. For DHCP mode:
   i. Enter the following at the command line:

      ```
      cp ifcfg-eth0 ifcfg-eth0.1
      ```

   ii. Open the `ifcfg-eth0.1` file with a text editor such as `vi`.
   iii. Change the following line:

      ```
      DEVICE=eth0
      ```

      To:

      ```
      DEVICE=eth0.1
      ```

e. Append the following line to the bottom of the file:

   ```
   VLAN=yes
   ```

f. Modify the `IPADDR` line if needed.
g. Save and exit the file.
h. Restart the network interface by entering the following at the command line:

   ```
   service network restart
   ```

2. Change the interface the EDAC listens on:
   a. Log in to the MS using SSH or directly with a keyboard.

b. For 802.1X mode, enter the following command at the command line:

```
setProperty.py –c <cluster name> Compliance.ObjectManager.NACMode-
TcpdumpInterface=eth1:1
```

c. For DHCP mode, enter the following command at the command line:

```
setProperty.py –c <cluster name> Compliance.ObjectManager.DDHCPMod-
eDHCPInterface=eth1:1
```

3. Verify the change:
   a. Log in to each ES using SSH or directly with a keyboard.
   b. Enter the following command at the command line:

```
ifconfig
```

   c. Verify that the virtual interface you created is listed.
   d. Open the following file:

```
var/log/nac/nac-es.log
```

   e. Verify that the EDAC is using the virtual interface you created. The log should contain a line similar to the following:

```
[070509-MDT 10:53:11.366 DeviceActivityCapture-INFO ] Listening on:
eth1:1
```

DNS/Windows Domain Authentication and Quarantined Endpoints

In order to satisfy the following scenarios:

- A guest user gets redirected
- A user is redirected if their home page is the Intranet
- The only host that is resolved is the domain controller (DC); and no other intranet hosts are resolved.
- Windows domain authentication can take place from quarantine with minimal configuration

Perform the following steps:

1. Configure the domain suffixes in the quarantine areas to a placeholder, such as the following:

```
quarantine.bad
```

2. Enter the full domain controller hostnames in the System configuration>>Accessible services area (for example, `dc01.mycompany.com, dc02.mycompany.com`).
3. Ensure that each ES has a valid, fully qualified domain name (FQDN) and that the domain portion matches the domain for the registered Windows domain.
4. Ensure that each ES is configured with one or more valid DNS servers that can fully resolve (both **A** and **PTR** records) each ES.
5. Ensure that the following ports on the domain controller/active directory (DC/AD) servers are available from quarantine:
   - 88
   - 389
   - 135-139
   - 1025

   The NAC 800 will then lookup the Kerberos and LDAP services, and resolve those services within its own DNS server used for quarantined devices.

   For example:

```
_kerberos._tcp.Default-First-Site-Name._sites.dc._msdcs.lvh.com. 86400 IN
 SRV 0 100 88 dc01.lvh.com
_ldap._tcp.Default-First-Site-Name._sites.dc._msdcs.lvh.com. 86400 IN SRV 0
 100 389 dc01.lvh.com
```

   When a browser is configured with an Intranet site as its home page, it will get redirected as shown in the following example process:

   -> `lookup intranet.mycompany.com`

   <- `get` an NXDomain (since `dc01.mycompany.com` is in the forwarders, all other `mycompany.com` hostnames get an NXDomain; that is the way `named` works).

   -> `lookup intranet.mycompany.com.quarantine.bad`

   <- `get` NAC 800 IP address

   When the end-user logs in, they will be able to authenticate from quarantine even if credentials are not cached:

   -> `lookup` the `_kerberos` and `_ldap` service location

   <- `receive dc01.mycompany.com & dc02.mycompany.com`

   -> `lookup` the dc01 IP address

   <- `receive` the dc IP address forwarded through NAC 800 `named` to the real DNS server (since `dc01.mycompany.com` is in the accessible services list).

   -> `authenticate`

Mass Deployments of the Windows End Point Integrity Agent

To obtain the .msi file used by the Microsoft Windows Installer to load the Windows Endpoint Integrity Agent on an endpoint, follow the instructions below.

1. See the section "Manually Installing the Windows Agent" in chapter 5 of the *ProCurve Network Access Controller 800 Users' Guide* steps 1 and 2. You need the following URL: `https://<enforcement_server_ip>:89/setup.exe`
2. In step 3, when asked to select **Run or Save the file**, choose **Run.** If a Security Warning appears, asking if you wish to run this software, select **Run**.
3. Wait for, but DO NOT RESPOND TO, the **ProCurve NAC Endpoint Integrity Agent - InstallShield Wizard** dialog. This allows the installation to begin, but not complete. This is required to obtain the desired .msi file.
4. Open Windows Explorer and search your **Documents and Settings\<*username*>\Local Settings** folder (in most cases **C:\Documents and Settings\<*username*>\Local Settings**) for `*NAC*.msi`. This will show the folder location of the **ProCurve NAC Endpoint Integrity Agent.msi** file. Note: this path works correctly, even if the system file **Local Settings** is not displayed by Windows Explorer.
5. Make a copy of the **ProCurve NAC Endpoint Integrity Agent.msi** file for use in your normal deployment procedures when deploying the endpoint integrity agent. Following this procedure, the .msi file size is about 4.5 MB.
6. Select **Cancel** in the **ProCurve NAC Endpoint Integrity Agent - InstallShield Wizard** dialog, then confirm that you are sure you wish to cancel in the next dialog. Lastly, select **Finish** in the next dialog to completely exit the installation process.
7. Review the information in Chapter 5 to make sure that your deployment opens the appropriate ports in the network. This is not done by the .msi file installation.

IDM Information

Rate Limiting for IDM freeRADIUS Agents

Port bandwidth on a freeRADIUS authenticated port is set to 100%, regardless of what bandwidth is specified in IDM. If bandwidth is set to **no-override** in IDM, then bandwidth is left at whatever is configured for the port.

In the HP freeRADIUS dictionary (**dictionary.hp**) the attribute is incorrectly specified as **string** and should be set to **integer**. The fix is to change the datatype to **integer** as follows:

1. Locate the existing **dictionary.hp** file using the **find** or **locate** commands from the shell of the Linux system.

```
locate dictionary.hp
 or
find / -name dictionary.hp
```

2. Stop **radiusd**.

```
service radiusd stop
or
 /etc/init.d/radiusd stop
```

3. Backup the existing **dictionary.hp**.

```
cp /usr/share/freeradius/dictionary.hp /usr/share/freeradius
   /dictionary.bak
```

4. Edit the file found in step 1.

```
 vi /usr/share/freeradius/dictionary.hp
```

5. Find and change **string** to **integer** in the following lines

   From:

```
   ATTRIBUTE       HP-bandwidth-max-ingress 46 string   HP
   ATTRIBUTE       HP-bandwidth-max-egress  48 string HP
```

   To:

```
   ATTRIBUTE       HP-bandwidth-max-ingress 46 integer  HP
   ATTRIBUTE       HP-bandwidth-max-egress  48 integer HP
```

6. Restart **radiusd**.

```
service radiusd start
 or
/etc/init.d/radiusd start
```

Installing the IDM Linux Agent

1. Download the IDM agent tarball and install.sh into the same directory
2. As root, run ./install.sh from the directory.
3. Follow the prompts.

Notes:

1. If iptables is running on the host, it may need to be modified to allow traffic to/from the management server. For example,

```
iptables –I INPUT –p tcp –s <mgmt server ip address> -j ACCEPT

iptables –I INPUT –p udp –s <mgmt server ip address> -j ACCEPT
```

2. The file **access.txt** needs to be setup correctly on the management server.

IDM 2.15 Import Wizard Issue

The IDM Import Wizard does not correctly process the special characters single quotes, double quotes, and backslashes in Group and User names. As a result, the wizard hangs and must be closed. IDM continues to operate normally.

The workaround is to upgrade to IDM 2.2 and use the AD Sync feature instead of the Import Wizard, or remove the special characters single quotes, double quotes, and backslashes from Group and User names.

September 2007B
Manual Part Number
5991-2124