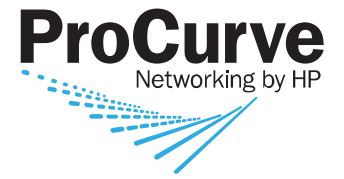


ProCurve Networking

ProCurve NAC 800 Local Authentication Directory (LAD) Configuration



Technical Brief



Introduction	3
Local Authentication Directory (LAD)	3
Configuring LAD	3
Registering ProCurve NAC 800 to IDM	3
Enabling LAD	3
Creating Users in LAD	4
Creating a User	4
Importing Users	4
Configuring Devices and Testing Authentication	5
Adding RADIUS Clients	5
LAD Authentication	5

Introduction

This paper provides instructions for users who wish to configure Local Authentication Directory (LAD) for RADIUS authentication. It includes steps for configuring LAD and creating users in Identity Driven Manager (IDM). IDM Access Policy has been designed to work with the LAD RADIUS server for authentication. The LAD leverages the free RADIUS in ProCurve Network Access Controller (NAC) 800, and provides authentication of users connecting to the network via local area network (LAN) and wireless technology.

Local Authentication Directory (LAD)

LAD is a user directory and feature of IDM, which is a plug-in for ProCurve Manager Plus (PCM+). LAD is local to ProCurve NAC 800. It also is for small environments, and provides the ability to use a local user's database for authentication when network environments do not have a user directory.

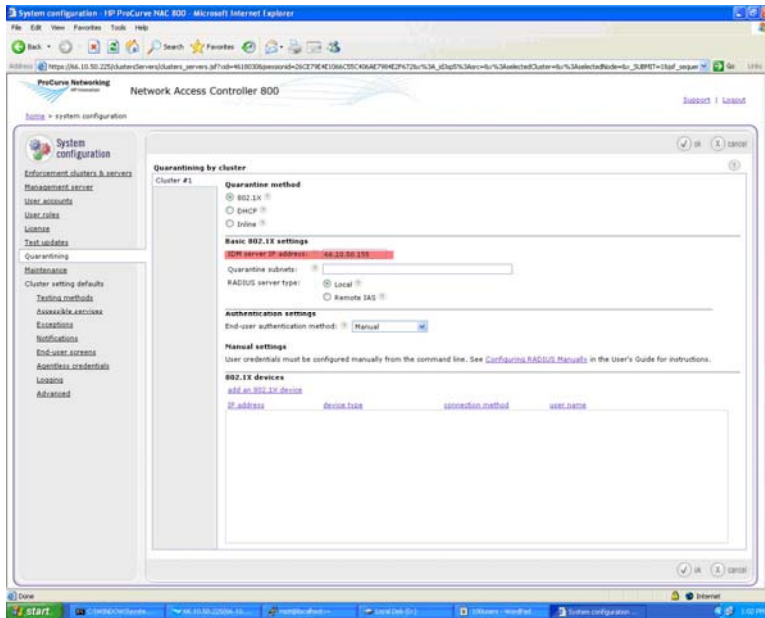
Configuring LAD

Note: Install the latest PCM auto-updates packages available on ProCurve's website.

Registering ProCurve NAC 800 to IDM

Follow these steps to register the ProCurve NAC 800 in the IDM to enable LAD in IDM.

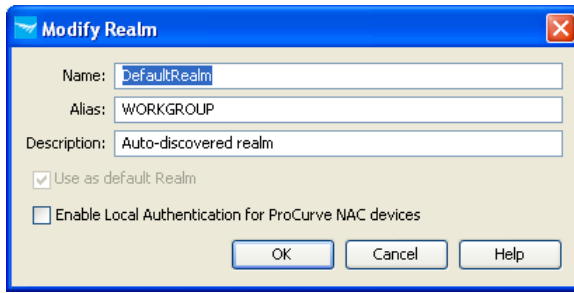
1. On the main web page of ProCurve NAC 800, go to the System configuration -> quarantining menu option, as shown in the figure below.
2. Enter the IDM server IP address (highlighted in red below) and apply the changes. ProCurve NAC 800 will appear under the default realm in IDM.



Enabling LAD

Use the following steps to enable LAD in IDM.

1. Select the realm under which the ProCurve NAC 800 is listed. By default, it will be under "DefaultRealm" in IDM.
2. Right-click the realm and under properties check the "Enable Local Authentication for ProCurve NAC devices" box to enable LAD. Once enabled, the IDM server will display a PCM event "Event Description Reporting Entity: IDM LAD Server Enabling LAD".



To disable LAD, uncheck the “Enable Local Authentication Directory” checkbox in realm properties.

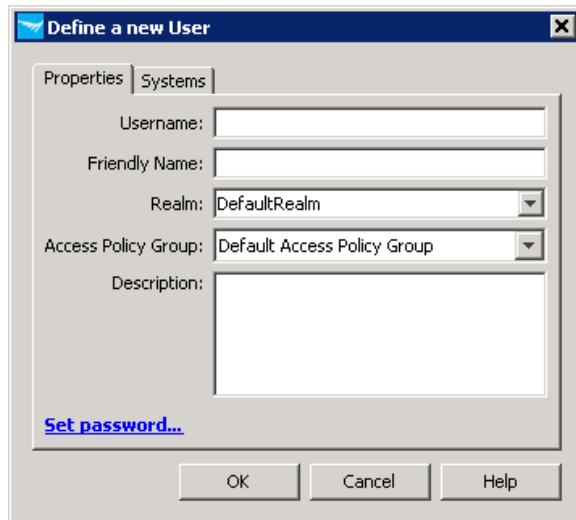
Note: This checkbox is not visible for all realms. For a checkbox to be visible, the following conditions should be met:

- The realm must have at least one IDM agent that is a ProCurve NAC 800.
- The RADIUS service must be installed and running on the ProCurve NAC 800.

Creating Users in LAD

Creating a User

1. In DefaultRealm, go to the “Users” tab and select the “Add User” toolbar button.
2. Enter a username and password in the “Add User” dialog box and apply the changes.



Importing Users

IDM also supports importing users to LAD, but it only supports an XML file import. The “IDM User Import” tool is available from the “Tools” menu in IDM.

Here is the format of the XML file:

```
<DirData>
  <Domain name="DEFAULTREALM">
    <User name="LadUsr1" password="idm" description="XML Import" displayName="LadUsr1" />
    <User name="LadUsr2" password="idm" description="XML Import" displayName="LadUsr2" />
  </Domain>
</DirData>
```

Note: Change the domain name in the XML file where the ProCurve NAC 800 resides; by default it resides in “DefaultRealm”.

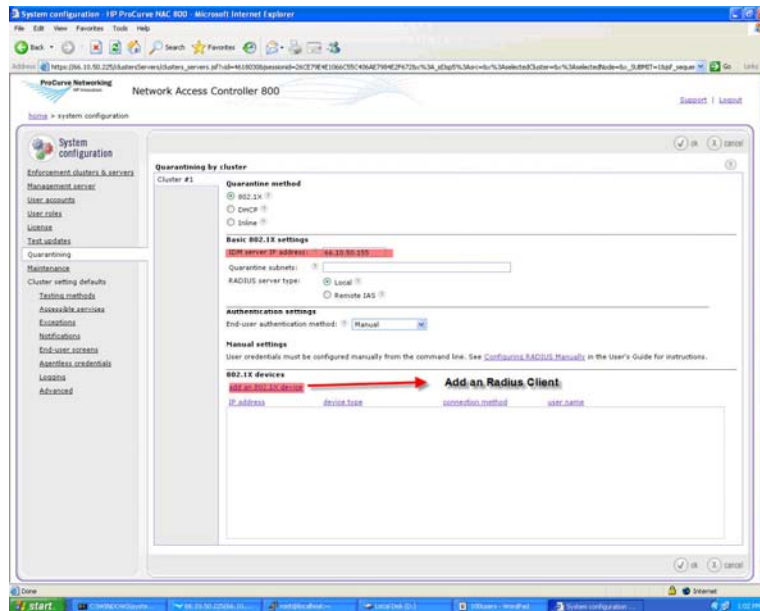
Configuring Devices and Testing Authentication

When the above instructions have been completed, refer to the sections below to configure RADIUS clients and test LAD user authentication.

Adding RADIUS Clients

Use the following steps to add 802.1X clients in ProCurve NAC 800:

1. On the main web page of ProCurve NAC 800, go to the System Configuration -> quarantining menu option.
2. Select the "add an 802.1X device" option, as highlighted in red in the figure below. (Note: SNMP community string of 802.1X device is required.)



LAD Authentication

Use the following steps to perform an 802.1X authentication using LAD. Windows XP and Vista supplicants are supported.

1. Perform a PEAP 802.1X authentication using Windows XP or Vista supplicant.
2. If the authentication is a success or failure, a user login/failed event will be reported in the IDM events tab and IDM dashboard.

Note: By default, MD5 authentication is disabled in ProCurve NAC 800; using PEAP authentication is recommended. Use the default access policy group and default access profile to test the LAD user authentication. Session Accounting (AAA) needs to be enabled in RADIUS clients for session start and session end events in the IDM server.

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

www.procurve.com



© 2008 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.

4AA1-8772ENW, April 2008