Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Contents

Overview .................................................. 4-3
RADIUS Overview ....................................... 4-3
  Authentication Protocols .............................. 4-4
  Dynamic or User-Based Settings ..................... 4-4
IDM Overview ............................................ 4-5
Data Store Overview ................................... 4-6
  Local Database ........................................ 4-7
  AD (Windows Domain) ................................. 4-7
  LDAP Server .......................................... 4-8
  Proxy RADIUS Server ................................. 4-9
Configure the NAC 800 as a RADIUS Server ........ 4-11
  Specify the Quarantine Method (802.1X) .......... 4-12
Configure Authentication Settings .................... 4-14
  Configure Authentication to the NAC 800's Local
  Database ............................................. 4-14
  Configure Authentication to a Windows Domain .... 4-16
  Configure Authentication to an LDAP Server ...... 4-20
  Configure Authentication to a Proxy RADIUS Server 4-29
Test Authentication Settings .......................... 4-34
Add NASs as 802.1X Devices .......................... 4-39
Apply Changes .......................................... 4-43
Restart the RADIUS Server ............................. 4-43
Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Contents

Manage Digital Certificates for RADIUS ........................................ 4-47
  Install the CA Root Certificate on the NAC 800 .................... 4-48
  Install a Server Certificate for RADIUS ................................. 4-49
    Create a Self-Signed Certificate ................................. 4-50
    Install a CA-Signed Certificate Using a Request
      Generated on the NAC 800 ................................. 4-52
    Install a CA-Signed Certificate Using a Request
      Generated on Behalf of the NAC 800 .................... 4-57
  Manage Certificates on Endpoints ................................. 4-61
  Disable Server Validation on Endpoints ............................ 4-61
Overview

As explained in Chapter 1: “Overview of the ProCurve NAC 800,” a ProCurve NAC 800 can fulfill a variety of functions, among them checking endpoint integrity and authenticating endpoints as a RADIUS server. In this chapter, you learn how to configure a NAC 800 that acts only as a RADIUS server.

ProCurve Identity Driven Manager (IDM), a plug-in to ProCurve Manager (PCM) Plus, helps you to quickly and easily configure the NAC 800’s RADIUS capabilities from a centralized location. This chapter focuses on setting up the NAC 800 in a network that includes IDM. See Chapter 5: “Configuring the RADIUS Server—Without Identity Driven Manager” to learn how to configure the NAC 800 to provide RADIUS services without IDM.

This chapter focuses on configuring a stand-alone NAC 800 that is functioning as a combination server (CS)—the typical setting for a RADIUS-only NAC 800.

In one circumstance only might you use a cluster deployment instead: you are adding a RADIUS-only NAC 800 to a system that already enforces endpoint integrity with a cluster configuration. In this case, the RADIUS-only NAC 800 would be an ES in a new cluster that enforces 802.1X quarantining and no endpoint integrity. You would configure most of the settings described in this chapter in the MS’s Web browser interface. However, you would create digital certificates through the RADIUS-only NAC 800’s root command line.

RADIUS Overview

The RADIUS protocol regulates communications between Network Access Servers (NASs) and authentication servers. The NASs are the points of access for endpoints—for example, switch ports or wireless access points (APs). They are also called the server’s clients. In your network, the NAC 800 is the authentication server.

When an end-user attempts to connect to a NAS, the NAS sends an authentication request to the NAC 800, its RADIUS server. The NAC 800 decides whether the end-user can connect. The NAC 800 bases this decision on whether the end-user submits valid credentials as well as—using IDM policies—the time and location of the access attempt.
Authentication Protocols

An authentication server receives an endpoints’ credentials via an authentication protocol. With 802.1X, the authentication protocol is always EAP, and the NAC 800 and the endpoint negotiate the method. The NAC 800 supports these EAP methods:

- Protected EAP (PEAP) with:
  - MS-CHAPv2
  - Generic Token Card (GTC)
- Transport Layer Security (TLS)
- Tunneled TLS (TTLS) with:
  - MS-CHAPv2
  - Generic Token Card (GTC)
- Lightweight EAP (LEAP)—not recommended

The NAC 800 first suggests PEAP with MS-CHAPv2.

An endpoint requires a client that supports at least one of the listed EAP methods. For example, a Windows XP workstation has an 802.1X client available to all network connections, and this client supports EAP-TLS and PEAP with MS-CHAPv2. Older workstations might require the installation of a vendor client for 802.1X authentication.

### Table 4-1. Port Authentication Methods and Authentication Protocols

<table>
<thead>
<tr>
<th>Port/Wireless Authentication Method</th>
<th>Selection Method for Authentication Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>NAC 800 and endpoint negotiation—NAC suggests PEAP with MS-CHAPv2 first.</td>
</tr>
</tbody>
</table>

Dynamic or User-Based Settings

Dynamic or user-based settings allow you to customize users’ network access according to identity and are an important component of the ProCurve Adaptive Edge Architecture (AEA). The RADIUS server is responsible for matching an authenticated user to the correct settings for that user.

Dynamic settings supported on the NAC 800 include:

- Virtual local area network (VLAN) assignments
- Access control lists (ACLs)
- Rate limits
Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Overview

IDM is required for configuring these settings on the NAC 800.

In fact, IDM enables you to capitalize on all of the NAC 800’s RADIUS capabilities—and to configure the NAC 800 as part of a centralized management solution.

**Note**

If you are using the NAC 800 to test endpoint integrity, you also use IDM to set up dynamic VLAN assignments according to an endpoint’s integrity posture.

**IDM Overview**

IDM detects and assumes management of the NAC 800 just as it does any RADIUS server. Because the IDM agent is installed on the NAC 800 at factory defaults, you only need to perform three tasks to integrate the NAC 800 with IDM:

- Configure the same read-only Simple Network Management Protocol version 2 (SNMPv2) community name on the IDM server and the NAC 800. (See “Configure MS or CS SNMP Settings” on page 3-24 of Chapter 3: “Initial Setup of the ProCurve NAC 800.”)

- On the IDM server, add the NAC 800’s IP address to this file: C:\Program Files\Hewlett-Packard\PNM\server\config\access.txt.

- On the NAC 800, specify the IP address of the server that runs PCM Plus with IDM. (See “Specify the Quarantine Method (802.1X)” on page 4-12.)

After detecting the NAC 800, IDM places it in its ProCurve Network Access Controllers folder and treats the device much like any RADIUS server:

- IDM deploys policies to the NAC 800, which include:
  - Times and locations for network access
  - Profiles for authenticated users, which include dynamic VLAN assignments, ACLs, and rate limits

**Note**

When IDM deploys a policy to a NAC 800, the NAC 800 stores the associated configuration. In other words, although IDM manages policies, once it has deployed them the NAC 800 always enforces them whether it can reach the IDM server or not.

- IDM tracks end-users that send authentication requests to the NAC 800.
In addition, IDM provides these services for NAC 800s:

- A tool for adding user accounts to the NAC 800's local database
- Access to the NAC 800's Web browser interface
- Profiles for authenticated users based on their endpoint integrity posture (pass, fail, infected, or unknown)

For more information on IDM and how it interacts with the NAC 800, see “IDM” on page 2-49 of Chapter 2: “Management Options for the ProCurve NAC 800.”

**Note**

To function with the NAC 800, IDM's version number must be 2.2 auto-update 2. The NAC 800's IDM agent version must match the IDM version.

The NAC 800 includes the IDM agent at its factory default settings; you do not need to install it. If the IDM agent is upgraded, the release notes will instruct you how to upgrade the agent on the NAC 800.

To check the current IDM agent version, log in to the NAC 800 as root and enter:

```
more /root/version
```

**Data Store Overview**

The NAC 800 can search one of several locations, or data stores, for a user's credentials:

- A local database of users
- A Windows domain controller, which runs Active Directory (AD)
- A Lightweight Directory Access Protocol (LDAP) server:
  - OpenLDAP
  - Novell eDirectory
- Another RADIUS server (via a proxy request)

You choose the data store when you configure the NAC 800’s (or cluster’s) end-user authentication method. (See “Configure Authentication Settings” on page 4-14.)
Local Database

You can store user accounts as entries in a database on the NAC 800 itself. IDM simplifies adding entries to the local database. You simply enable local authentication on the NAC 800's IDM realm. Then, whenever you add a user to IDM, the user is automatically added to the local database of all NAC 800s in the realm.

**Note**

You must *always* include a password for users that are added to the local database through IDM. (The NAC 800 does not accept NULL passwords.)

Advantages of using the local database configured through IDM include:

- The database is always available to the NAC 800.
- The database is under the control of administrators with access to IDM.
- Local databases on multiple NAC 800s are always identical because you configure them centrally.
- You can use any of these protocols to authenticate users:
  - EAP-TLS
  - EAP-TTLS with MS-CHAPv2 (or GTC)
  - PEAP with MS-CHAPv2 (or GTC)

Disadvantages of using the local database include:

- You must have access to IDM to add entries to the database.
- Although IDM can automatically add users, you must set passwords for the user accounts before they are added to the NAC 800's local database.

AD (Windows Domain)

Many organizations manage users as a part of a Windows domain, and Microsoft AD already stores user entries. Rather than duplicate these entries, the NAC 800 can simply join the domain and request information from AD when necessary to authenticate a user.

See “Configure Authentication to a Windows Domain” on page 4-16 to learn how to configure this option.

Advantages of using the Windows domain and AD as the data store include:

- IDM can synchronize with a Windows domain and automatically import users in specific groups. When you add the NAC 800 to the domain, you enable the NAC 800 to authenticate these users without adding passwords to the user accounts in IDM.
- Changes to an object in AD are automatically available to all NAC 800s.
Disadvantages of using the Windows domain include:

- You must know an administrator username and password for the Windows domain; otherwise, you cannot configure the NAC 800 to join the domain.
- If your NAC 800 loses connectivity to the domain controller (the server running AD), it cannot authenticate users.
  
  Having multiple domain controllers mitigates this disadvantage.
- Your network must use one of these authentication methods:
  - MS-CHAPv1 or MS-CHAPv2
  - EAP-TTLS with MS-CHAPv2
  - PEAP with MS-CHAPv2

  If you need to use a different method, use the NAC 800’s local database.

**LDAP Server**

Just as the NAC 800 can join a Windows domain and access AD, it can bind to an LDAP server and search a directory. For example, your organization might already have a directory that authenticates users and authorizes them for various types of network access.

The NAC 800 can bind to these LDAP servers:

- OpenLDAP
  
  See “Configure Authentication to an OpenLDAP Server” on page 4-21.

- Novell eDirectory
  
  See “Configure Authentication to a Novell eDirectory Server” on page 4-26.

Advantages of using LDAP servers as the data store include:

- IDM can import users from an LDAP server. When you also bind the NAC 800 to the LDAP server, you enable the NAC 800 to authenticate these users without adding passwords to the user accounts in IDM.
- Changes to a directory object are automatically available to all NAC 800s.

Disadvantages of using the LDAP servers include:

- You must know the username and password for the root account of the directory database in question; otherwise, you cannot configure the NAC 800 to bind to the directory.
Overview

- If your NAC 800 loses connectivity to the LDAP server, it cannot authenticate users.

  Specifying multiple LDAP servers mitigates this disadvantage. See Chapter 7: “Redundancy and Backup for RADIUS Services.”

Proxy RADIUS Server

The NAC 800 can proxy access requests to one or more RADIUS servers. The NAC 800 acts as a RADIUS client to the proxy server, and the proxy server looks up credentials and authenticates the user.

The NAC 800 can proxy all requests, or it can only proxy requests that meet certain criteria, such as having a particular domain suffix.

Proxying requests is primarily intended for NAC 800s that implement endpoint integrity. The existing RADIUS server handles authentication, and the NAC 800 handles the endpoint integrity.

However, you might choose the proxy option for a RADIUS-only NAC 800 in this situation: you want to use IDM, but your existing RADIUS server does not support the IDM agent. The NAC 800 will proxy authentication requests to the existing server, which checks user credentials. When the NAC 800 receives an access response from the proxy server, it will modify the response according to policies configured through IDM.

To configure proxying, you must log in as root to the NAC 800’s (CS’s or ES’s) command line and edit this file: `/etc/raddb/proxy.conf`. See “Configure Authentication to a Proxy RADIUS Server” on page 4-29.

Advantages of using a proxy server for at least some requests include:

- You do not have to duplicate user accounts already stored on another RADIUS server.
- You can gain the advantages of IDM in a network with existing RADIUS servers that do not support the IDM agent.

Disadvantages of using the proxy server include:

- The existing RADIUS server must still handle authentication requests, so the NAC 800 does not relieve that burden.
Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Overview

- The EAP method must allow the username to be transmitted in plaintext. IDM requires access to the username. If the proxy server and supplicant always transmit the username in encrypted form, IDM cannot determine the correct policy to apply.
  
  For example, EAP-TTLS might exhibit this problem.

  An example of an EAP method that works with proxying is Microsoft’s implementation of PEAP.

- If your NAC 800 loses connectivity to the proxy server, it cannot authenticate users.

  Specifying multiple proxy servers mitigates this disadvantage.

- Manual configuration creates opportunities for errors.
Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Configure the NAC 800 as a RADIUS Server

You must complete these tasks to set up the ProCurve NAC 800 as a RADIUS server in a network with IDM:

1. Configure your network’s NASs—including, as necessary, switches, wireless APs, and Wireless Edge Services Modules—to use the NAC 800 as their RADIUS server.

   The NAC 800 can be the NASs’ primary or secondary server.

   Refer to your devices’ documentation for instructions on completing this task.

   PCM Plus also offers a Secure Access Wizard for completing this step on ProCurve devices. See the ProCurve Identity Driven Management User’s Guide.

2. Complete initial configuration of the NAC 800.

   See Chapter 3: “Initial Setup of the ProCurve NAC 800.”

   In particular, set the NAC 800’s SNMPv2 community name to the name configured on the PCM Plus with IDM server.

   If you are adding the RADIUS-only NAC 800 to an existing system of NAC 800s, create a cluster for 802.1X enforcement and add the new NAC 800 as an ES. Otherwise, simply set the NAC 800 as a CS.

3. On the PCM Plus with IDM server (called the IDM server for the rest of this chapter), add the NAC 800’s IP address to the list of devices allowed to access the server.

   Follow these steps:
   a. On the IDM server, open C:\Program Files\Hewlett-Packard\PNM\server\config.access.txt.

      Open the file in a text-based editor such as Notepad or Wordpad.

   b. Add the NAC 800’s IP address or hostname on its own line.

   c. Save and close the file.

4. On the NAC 800, select 802.1X for the quarantine method.

   See “Specify the Quarantine Method (802.1X)” on page 4-12.
5. On the NAC 800, set the IDM server address.
   See “Specify the Quarantine Method (802.1X)” on page 4-12.

6. On the NAC 800, configure the authentication settings, which determine, for example, where the database of usernames and passwords is stored.
   See “Configure Authentication Settings” on page 4-14.

7. On the NAC 800, add your network's NASs—switches, APs, and Wireless Edge Services Modules—as 802.1X devices.
   See “Add NASs as 802.1X Devices” on page 4-39.

8. On the NAC 800, apply your configuration changes.
   The RADIUS server automatically restarts. See “Apply Changes” on page 4-43.

9. Complete all other configurations, including creating policies for dynamic settings and endpoint integrity, with IDM. Deploy policies to the NAC 800.
   See the ProCurve Identity Driven Manager User's Guide.

Specify the Quarantine Method (802.1X)

To act as a RADIUS server, the ProCurve NAC 800 must implement the 802.1X quarantine method. (However, you can disable the actual quarantining by disabling endpoint testing. See Chapter 6: "Disabling Endpoint Integrity Testing.")

Follow these steps:

1. Select Home > System configuration > Quarantining.

2. If you have a multiple NAC 800 deployment (MS and multiple ESs), choose the cluster that includes the RADIUS server ESs. For a CS, the default and only cluster is automatically selected.

3. In the Quarantine method area, select 802.1X.
Figure 4-1. Home > System configuration > Quarantining

4. In the **Basic 802.1X settings** area and the **IDM server IP address** field, enter the IP address of the server that runs PCM Plus with IDM.

5. Select **Local** for the **RADIUS server type**.
Configure the NAC 800 as a RADIUS Server

Note

The Quarantine subnets field only applies if the NAC 800 enforces endpoint integrity. This setting allows the NAC 800 to respond to DNS requests from endpoints in quarantine VLANs. You should have already set up the quarantine VLANs in IDM.

You have now enabled the NAC 800 to make access control decisions as a RADIUS server. Next you must configure the RADIUS server’s authentication settings.

Configure Authentication Settings

To check 802.1X credentials, the NAC 800 draws on user accounts stored in one of several locations:

- Its own local database configured through IDM (see “Configure Authentication to the NAC 800’s Local Database” on page 4-14)
- A Windows Domain (see “Configure Authentication to a Windows Domain” on page 4-16)
- An OpenLDAP server (see “Configure Authentication to an OpenLDAP Server” on page 4-21)
- A Novell eDirectory server (see “Configure Authentication to a Novell eDirectory Server” on page 4-26)
- Another RADIUS server (see “Configure Authentication to a Proxy RADIUS Server” on page 4-29)

While not typical for a RADIUS-only NAC 800, this option is supported.

Configure Authentication to the NAC 800’s Local Database

Follow these steps to enable the NAC to authenticate users against its own local database:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12. You should see the screen illustrated in Figure 4-2.
Figure 4-2. Home > System configuration > Quarantining—802.1X quarantine method

3. Add user accounts to the local database through IDM. 
   You must complete two steps on the IDM server:
   a. Modify the NAC 800’s domain and select **Enable Local Authentication for ProCurve NAC devices**.
   b. Add users to the realm.
      IDM automatically configures on the NAC 800 any user that you add to the NAC 800’s realm. You must, however, configure passwords for those users.
      See the *ProCurve Identity Driven Management User’s Guide* for more detailed instructions in completing these steps.

4. You are now ready to specify your network’s NASs. (See “Add NASs as 802.1X Devices” on page 4-39.)

**Configure Authentication to a Windows Domain**

The Windows Domain authentication method allows the NAC 800 to check end-user credentials against credentials stored in AD.

The NAC 800 joins the domain. Then, when it receives an authentication request from an end-user, the NAC 800 uses NT LAN Manager (NTLM) to query a domain controller (a server that runs AD) and check the end-users’ credentials.

To set up the Windows domain authentication method successfully, you must ensure that:

- Endpoints and NASs meet requirements for NTLM authentication:
  - End-users are members of the domain.
  - For 802.1X authentication, endpoints support PEAP or TTLS with MS-CHAPv2 as the inner method.

**Note**

If your NASs or endpoints do not support the correct authentication methods, the NAC 800 cannot authenticate end-users directly against AD. You must either proxy authentication requests to another RADIUS server or select local authentication in IDM to duplicate user accounts on the NAC 800’s local directory.
The NAC 800 (the CS or ESs) can join the domain:

- You need the username and password of an account with the right to add devices to the domain (an administrator account).
- The NAC 800's hostname must be fully qualified with your domain's name—for example, `nac.mydomain.com`, not `nac`.
  
  See “Edit MS or CS Network Settings” on page 3-18 of Chapter 3: “Initial Setup of the ProCurve NAC 800” for instructions on changing the hostname.
- The NAC 800 requires a valid DNS server address (which allows it to resolve the domain controller's FQDN).
  
  To specify the DNS server, see “Edit MS or CS Network Settings” on page 3-18 of Chapter 3: “Initial Setup of the ProCurve NAC 800.”
- Your network's DNS servers must have forward lookup entries for the NAC 800 and for the domain controller. It must also have the correct reverse lookup zones.
- The NAC 800's clock is synced with the domain controller's clock.
  
  Default Windows server settings require the NAC 800's time to be within five minutes of the domain controller's time to prevent replay attacks. Either verify that both devices receive their clock from an NTP server, or change the settings on the domain controller.

Follow these steps to configure end-user authentication against a Windows domain:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12. You should see the screen illustrated in Figure 4-3.
2. Select Windows domain for the End-user authentication method.

The Windows domain settings and Test Windows domain settings areas are displayed.
Figure 4-4. Home > System configuration > Quarantining—Windows domain authentication method

Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager
Configure the NAC 800 as a RADIUS Server
3. In the **Domain name** field, enter the FQDN of your domain. For example: **MyCompany.com**

**Note**

In a domain with subdomains, the NAC 800 must join the parent domain (rather than one of the subdomains). For example, you must specify **MyCompany.com**, not **hq.MyCompany.com**.

4. In the **Administrator user name** field, enter the username of an account with the right to join the NAC 800 to the domain.

5. In the **Administrator password** field, enter the password for the user specified in previous step.

6. In the **Re-enter administrator password** field, enter the password again.

7. In the **Domain controllers** field, specify the FQDN of your domain controller (or controllers).

   Domain controllers are servers that run AD. Separate FQDNs with a comma (no space).

**Note**

In a network with multiple domain controllers, you should generally specify all of the controllers. If you do not, you might see an error when you test the settings because the NAC 800 bound itself to a different domain controller than the one specified.

8. To verify that the NAC 800 can successfully join the domain, click the **test settings** button.

   See “Test Authentication Settings” on page 4-34 for more information on setting up the test.

9. You are now ready to specify your network's NASs. (See “Add NASs as 802.1X Devices” on page 4-39.)

**Configure Authentication to an LDAP Server**

Your network might already have a directory that stores user accounts and rights. You can configure your NAC 800 to authenticate users against these LDAP-compliant servers:

- OpenLDAP
- Novell eDirectory
You must configure the NAC 800 to perform these functions:

- **Bind to the LDAP server**
  
  To complete the binding, the server submits a distinguished name (DN) and password to the LDAP server. You must specify the DN and password of an object with administrative rights. In addition, you must specify the base DN. The base DN serves as the starting point for LDAP searches and is typically the top level of the tree. The administrator object must be under the specified base DN.

- **Search the LDAP server's directory to check the user's credentials and group memberships**
  
  - With the user login filter, the NAC 800 looks up the account that matches the name submitted by the end-user.
  
  - To check the end-user's password, the NAC 800 requests the password attribute for the account.

By default, the NAC 800 and the LDAP server communicate in plaintext messages. You should configure the NAC 800 to complete TLS authentication with the LDAP server, which increases security in several ways:

- The LDAP server verifies its identity to the NAC 800 with a secure digital certificate—which ensures that it receives user account information to authorized devices only.

- TLS creates an encrypted tunnel between the NAC 800 and the LDAP server—which protects users' information from eavesdroppers.

**Configure Authentication to an OpenLDAP Server.** If your network stores user accounts in OpenLDAP, follow these steps to configure the NAC 800's authentication settings:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12. You should see the screen illustrated in Figure 4-5.
Configure the NAC 800 as a RADIUS Server

2. Select OpenLDAP for the End-user authentication method.

The OpenLDAP settings and Test OpenLDAP settings areas are displayed.
3. In the **Server** field, enter the hostname or IP address of the OpenLDAP server. For example:

10.1.10.10
Configure the NAC 800 as a RADIUS Server

Optionally, append a colon and port number to the IP address to specify the port used by your OpenLDAP server. For example:

10.1.0.10:646

If you do not specify the port, the NAC 800 behaves as follows:
- Uses port 389 if the connection is not secure
- Uses port 636 if the connection is secure

Step 9 on page 4-25 explains how to choose a secure connection.

---

**Note**

If you specify a hostname, remember to check the NAC 800's DNS server. See “Edit MS or CS Network Settings” on page 3-18 of Chapter 3: “Initial Setup of the ProCurve NAC 800.”

4. In the **Identity** field, enter the DN of an object in the directory with administrative rights.

Enter the name in standard LDAP format. For example:

`cn=Manager,dc=MyCompany,dc=com`

5. In the **Password** field, enter the password for the object specified in the previous step.

6. In the **Re-enter password** field, enter this password again.

7. In the **Base DN** field, enter the DN for the object at which the NAC 800 begins searches—almost always the DN of the top level of the tree.

   For example:

   `dc=MyCompany,dc=com`

   The administrator specified in the **Identity** field should be under the base DN.

8. Typically, leave the **Filter** and **Password attribute** fields at their default settings.

   As explained in the introduction to “Configure Authentication to an LDAP Server” on page 4-20, the user filter and password attribute help the NAC 800 perform searches within the directory. Your settings must match up with attribute names used in your OpenLDAP installation, and the syntax must follow LDAP syntax.
Configure the NAC 800 as a RADIUS Server

The default filter is shown in Figure 4-6; it tells the NAC 800 to search for an entry in which the “uid” attribute equals whatever username is submitted in an authentication request. (The “Stripped-User-Domain” portion of the filter allows the NAC 800 to remove an appended domain name, which may be necessary to match the uid as stored in the directory.)

Note

Depending on how your directory is constructed, you might need to change “uid” to “cn.”

The password attribute (default “userPassword”) must match the name of the attribute that stores passwords in your directory. Remember the OpenLDAP directory must allow the NAC 800 “auth” access to this attribute.

Note

Be careful when altering the default settings: if you cause searches to fail, you effectively lock out all users.

9. Check the Use a secure connection (TLS) box.

The NAC 800 and the OpenLDAP server perform a TLS handshake to authenticate each other, as well as set up encryption keys to secure the connection.

ProCurve Networking recommends that you always enable this option.

10. If you checked the box in the previous step, verify that the NAC 800 has the proper certificate authority (CA) certificate.

The NAC 800 requires the CA certificate for the CA that signed the OpenLDAP server’s certificate. Save this certificate on your management station. Then click the Browse button next to New certificate to upload it to the NAC 800.

11. To verify that the NAC 800 can successfully bind to the OpenLDAP server, click the test settings button.

See “Test Authentication Settings” on page 4-34 for more information on setting up the test.

Note

You may receive a message that the test failed because the LDAP query returned no results. Do not worry: although the search did not return any results, the bind completed successfully. For information about other result messages, see Table 4-2 on page 4-38.

12. You are now ready to specify your network’s NASs. (See “Add NASs as 802.1X Devices” on page 4-39.)
Configure Authentication to a Novell eDirectory Server. If your network stores user accounts in eDirectory, follow these steps to configure the NAC 800’s authentication settings:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12. You should see the screen illustrated in Figure 4-7.

![Figure 4-7. Home > System configuration > Quarantining—802.1X quarantine method](image-url)
2. Select **Novell eDirectory** for the **End-user authentication method**.

The **Novell eDirectory settings** and **Test Novell eDirectory settings** areas are displayed.

![System configuration interface](image_url)

*Figure 4-8. Home > System configuration > Quarantining—Novell eDirectory authentication method*
3. In the **Server** field, enter the hostname or IP address of the eDirectory server. For example:

   10.1.10.10

   A hostname can include alphanumeric characters, periods, and hyphens and be up to 64 characters.

   Optionally, append a colon and port number to the IP address or hostname to specify the port used by your eDirectory server. For example:

   10.1.10.10:636

   The default LDAP port is 389, and the NAC 800 uses this port if you do not explicitly specify another. Use the 636 port when you check the **Use a secure connection (TLS)** box (recommended). See step 9 on page 4-29.

4. In the **Identity** field, enter the DN of an account with administrator rights.

   Enter the name in standard LDAP format. For example:

   `cn=Administrator,dc=MyCompany,dc=com`

5. In the **Password** field, enter the password for the account specified in the previous step.

6. In the **Re-enter password** field, enter this password again.

7. In the **Base DN** field, enter the DN for the object at which the NAC 800 begins the search.

   Typically, you should specify the top of the directory. For example:

   `dc=MyCompany,dc=com`

   The administrator specified in the **Identity** field should be under the base DN.

8. You should leave the **Filter** and **Password attribute** fields at their default settings.

   As explained in the introduction to “Configure Authentication to an LDAP Server” on page 4-20, the filter and password attribute help the NAC 800 perform searches within the directory. The values must match exactly the values used by eDirectory, and the syntax must follow LDAP syntax.

   The default filter is shown in Figure 4-8; it tells the NAC 800 to search for an account in which the “cn” attribute equals whatever username is submitted in an authentication request. (The “Stripped-User-Domain” portion of the filter allows the NAC 800 to remove an appended domain name, which may be necessary to match the cn as stored in the directory.)
The password attribute (default “nspmPassword”) must match the attribute used to store passwords in eDirectory accounts.

**Note**

Be careful when altering the default settings: if you cause searches to fail, you effectively lock out all users.

9. Check the **Use a secure connection (TLS)** box.

The NAC 800 and the eDirectory server perform a TLS handshake to authenticate each other, as well as set up encryption keys to prevent eavesdroppers from discovering credentials.

An eDirectory server, by default, requires secure connections.

10. If you checked the box in the previous step, verify that the NAC 800 has the proper CA certificate.

The NAC 800 requires the CA certificate for the CA that signed the eDirectory server’s certificate. Save this certificate on your management station. Then click the **Browse** button next to **New certificate** to upload it to the NAC 800.

11. To verify that the NAC 800 can successfully bind to the eDirectory server, click the **test settings** button.

See “Test Authentication Settings” on page 4-34 for more information on setting up the test.

12. You are now ready to specify your network’s NASs. (See “Add NASs as 802.1X Devices” on page 4-39.)

**Configure Authentication to a Proxy RADIUS Server**

If your network has an existing RADIUS server, you can configure the NAC 800 to proxy end-user authentication requests to that server.

**Note**

Check the EAP methods supported by the proxy RADIUS server. The server *must* use only those methods, such as PEAP, that include the username in plaintext.

Follow these steps:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12. You should see the screen illustrated in Figure 4-9.
Configure the NAC 800 as a RADIUS Server

2. Select **Proxy** for the End-user authentication method.
3. Specify the IP address for the proxy server (or servers).

To complete this task, you must access the NAC 800’s OS and edit the /etc/raddb/proxy.conf file.
Note

If your NAC 800 is a CS, simply alter the `proxy.conf` files on that NAC 800. However, if you have a cluster of MS and ESs, you must alter the file on each ES in this cluster.

Follow these steps:

a. Click the ok button to save your changes before you leave the Web browser session.

b. Log in as root to the NAC 800:
   i. Open a Secure Shell (SSH) or console session with the NAC 800.
   ii. When asked for your username and password, enter root and the root password (default: procurve).

c. Edit the `/etc/raddb/proxy.conf` file.
   The steps below give basic commands for editing the file with vi, a standard Linux editor built into the NAC 800. For more information on vi, see “vi Editor” on page B-4 of Appendix B: “Linux Commands.”
   i. Enter this command:
      ```bash
      vi /etc/raddb/proxy.conf
      ```
   ii. Move through the file until you find the “realm company.com” section.
   iii. Enter insert mode by pressing [i].
   iv. Delete the comment markers (#) from the five lines in the “realm company.com” section.
   v. Change “company.com” to the name of the domain of the proxy server.
   vi. For the “authhost” value, specify the proxy RADIUS authentication server. Use this syntax:
      ```
      authhost= <FQDN or IP address>:<port number>
      ```
      If you do not specify a port, the NAC 800 uses the default RADIUS authentication port (1812).
vii. If you want to implement RADIUS accounting, specify the RADIUS accounting server for the “accthost” value. Use this syntax:

```
accthost= <FQDN or IP address>:<port number>
```

If you do not specify a port, the NAC 800 uses the default RADIUS accounting port (1813).

If you do not want to implement accounting, re-insert the comment marker (#) on this line.

viii. Specify the shared secret for the “secret” value. Use this syntax:

```
secret= <shared secret>
```

This value must match exactly the secret configured on the proxy server for the NAC 800 (which should be added as a client to the proxy server).

To include special characters and spaces, enclose the secret within quotation marks (“ ”).

ix. The final configuration should resemble that shown in Figure 4-11.

x. When you are done, leave insert mode by pressing [Esc].

xi. Enter this command to save the changes:

```
:w
```

xii. Exit vi:

```
:q
```

---

**Note**

More advanced users can configure the NAC 800 to proxy various requests to different RADIUS servers depending on the domain name or EAP type included in the request. The comments in the `proxy.conf` file give guidelines; however, such configuration is not supported by ProCurve Networking.

---

4. You are now ready to specify your network’s NASs. (See “Add NASs as 802.1X Devices” on page 4-39.)

---

**Note**

If you are not comfortable using vi, you can save the file to your management station and edit it with a text editor on that device. Then copy the file back to the NAC 800 (preserving the `/etc/raddb/proxy.conf` location and filename). You can also use this option to copy the same file to multiple devices.
Test Authentication Settings

The following authentication methods require the NAC 800 to bind to a directory server:

- Windows domain (AD)
- OpenLDAP
- Novell eDirectory

After configuring one of these methods, you should test whether the NAC 800 can:

- Contact the directory
- Bind to it
- Optionally, perform a successful search

You should test the settings to eliminate problems before the NAC 800 begins to authenticate end-users on a live network.

Follow these steps:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12.

2. Complete the steps for your selected authentication method. (See “Configure Authentication Settings” on page 4-14.)

3. You should see a screen similar to the one illustrated in Figure 4-12. Find the Test <authentication method> settings area.

   For example, in Figure 4-12, you can see the Test Novell eDirectory settings area.
4. If you are configuring a CS, you can skip this step. Otherwise, you must select an ES from the **Server to test from** drop-down menu.

In a multiple NAC 800 deployment, ESs (not the MS) bind to the LDAP server when they need to authenticate end-users. When you test settings, you must choose for which ES you are testing them.
5. You now have two options:
   - Test the bind operation only.
     Click the test settings button.
     This test verifies that:
     - The NAC 800 can reach the domain controller or LDAP server.
     - The administrator username and password are correct.

   Note
   If you choose this option, you may receive a message that the test failed because the LDAP query returned no results or multiple results. Do not worry: although the search didn't return results, the bind completed successfully. See Table 4-2 for results that do indicate a problem.

   - Test the bind operation and look up an end-user’s credentials:
     i. Check the Verify credentials for an end-user box.
     ii. Enter the username for a valid user in the User name field.
     iii. Enter the user’s password in the Password field.
     iv. Re-enter the password in the Re-enter password field.
     v. Click the test settings button.
     This test verifies that:
     - The NAC 800 can reach the domain controller or LDAP server.
     - The administrator username and password are correct.
     - For authentication through an LDAP server, the filter and password attribute are correct.
     - The end-user credentials that you entered are correct.

   Note
   When you first test a configuration with the Verify credentials for an end-user option, choose an end-user username and password that you are certain are correct (for example, the administrator password). In that way, you verify that the configuration itself functions correctly.

   Later, if a particular user has difficulty connecting, you can use the Verify credentials for an end-user option to check the user’s credentials.

6. The Operation in progress screen is displayed.

   Figure 4-13 shows the screen for testing Windows domain authentication settings.
Configure the NAC 800 as a RADIUS Server

You might see, instead, the screen shown in Figure 4-14.

Figure 4-13. Home > System configuration > Quarantining > test settings button

This screen is displayed when you have edited previously configured authentication settings. To test the new settings, the NAC 800 must temporarily write them over the old settings, which—if the NAC 800 is the RADIUS server for an active network—can briefly interrupt service.

Click the no button to cancel the test (in which case you should also wait before applying your new settings).

Click the yes button to proceed with the test.

Note that proceeding with the test only temporarily overwrites the old settings. You must still click the ok button in the Home > System configuration > Quarantining screen to save the new settings.

7. When the test completes, you are returned to the Home > System configuration > Quarantining screen. The message at the top of the screen indicates the result. Refer to Table 4-2 for help interpreting the message.
Table 4-2. Authentication Settings Test Results

<table>
<thead>
<tr>
<th>Message</th>
<th>Result</th>
<th>Possible Cause of Failure</th>
</tr>
</thead>
</table>
| LDAP settings successfully validated. | • The NAC 800 successfully bound to the LDAP server.  
• The NAC 800 successfully validated the test credentials. | |
| Test failed: LDAP query returned no results. | • The NAC 800 successfully bound to the LDAP server.  
• You didn’t ask to verify credentials. | |
| Test failed: LDAP query returned more than one result. | • The NAC 800 successfully bound to the LDAP server.  
• You didn’t ask to verify credentials. | |
| Test failed: [LDAP: error code 48 - Inappropriate Authentication]. | The NAC 800 failed to bind to the LDAP server. | The bind password is incorrect. |
| Test failed: could not authenticate identity. | The NAC 800 failed to bind to the LDAP server. | • The bind username is incorrect.  
• The base DN is incorrect. |
| Test failed: [LDAP: error code 32 - NDS error: no such entry (-601)] | The NAC 800 failed to bind to the LDAP server. | • The bind username is incorrect.  
• The base DN is incorrect. |
| Test failed: [LDAP: error code 13 - Confidentiality Required] | The NAC 800 failed to bind to the LDAP server. | The LDAP server requires TLS, but this option is not selected. |
| Test failed: connection error (Connection refused). | The NAC 800 failed to bind to the LDAP server. | The LDAP server requires TLS, but this option is not selected. |
| Test failed: could not verify server’s certificate signature. | The NAC 800 failed to bind to the LDAP server. | The CA certificate for TLS authentication does not match the LDAP server’s CA certificate. |
| Test failed: end-user <username> not found. | • The NAC 800 successfully bound to the LDAP server.  
• The NAC 800 failed to validate the test credentials. | • The test username is incorrect.  
• The base DN is incorrect.  
• The filter specifies the wrong attribute name. |
| Test failed: password for end user <username> is invalid. | • The NAC 800 successfully bound to the LDAP server.  
• The NAC 800 failed to validate the test credentials. | The test password is incorrect. |
Configure the NAC 800 as a RADIUS Server

A NAS is the device to which end-users connect—typically, a switch or an AP. The NAS enforces port authentication on end-user ports, forwarding users’ authentication requests to a RADIUS server.

You must add each NAS that uses the NAC 800 as its RADIUS server to the NAC 800’s list of 802.1X devices.

**Note**

The NASs are often called RADIUS clients. The Web browser interface, however, as well as this guide, will refer to them as 802.1X devices.

Follow these steps to add the 802.1X devices:

1. Complete the steps listed in “Specify the Quarantine Method (802.1X)” on page 4-12.
2. Complete the steps for your selected authentication method. (See “Configure Authentication Settings” on page 4-14.)
3. You should see a screen similar to that illustrated in Figure 4-15.

---

### Table: Test Failure Messages

<table>
<thead>
<tr>
<th>Message</th>
<th>Result</th>
<th>Possible Cause of Failure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test failed: Attribute &lt;attribute name&gt; not found.</td>
<td>- The NAC 800 successfully bound to the LDAP server.</td>
<td>The password attribute is incorrect.</td>
</tr>
<tr>
<td></td>
<td>- The NAC 800 failed to validate the test credentials.</td>
<td></td>
</tr>
</tbody>
</table>

Test failed: Attribute `<attribute name>` not found.

- The NAC 800 successfully bound to the LDAP server.
- The NAC 800 failed to validate the test credentials.

Add NASs as 802.1X Devices
Configuring the RADIUS Server—Integrated with ProCurve Identity Driven Manager
Configure the NAC 800 as a RADIUS Server

Figure 4-15. Home > System configuration > Quarantining—802.1X quarantine method

4. Click the add an 802.1X device link. The Add 802.1X device screen is displayed.
5. Enter the 802.1X device’s IP address in the **IP address** field.
   
   For example, endpoints connect to an edge switch that has 10.1.1.152 for its management IP address. Enter:
   
   10.1.1.152

6. Enter a character string in the **Shared secret** field.
   
   This string and the RADIUS server secret configured on the 802.1X device must match exactly. (See your device's documentation for information on configuring this secret. Or use PCM Plus’s Secure Access Wizard, described in the *ProCurve Identity Driven Manager User’s Guide*.)

   The secret can include alphanumeric and special characters.

7. Enter the same character string in the **Re-enter shared secret** field.

8. Optionally, give the 802.1X device a descriptive name by entering a string in the **Short name** field.
   
   The name is displayed in logs and can include alphanumeric and special characters.

9. From the **Device type** drop-down menu, choose the type of 802.1X device (that is, its manufacturer and OS).
   
   The drop-down menu includes several common devices, but the NAC 800 supports any device that can act as a standard RADIUS client. If your device is not listed, select **Other**.

10. Options for connecting to the selected device are displayed.
Connecting to the 802.1X device is necessary for implementing endpoint integrity: the NAC 800 must force the 802.1X to re-authenticate the endpoint after its endpoint integrity posture has changed, so that the new VLAN assignment can take effect. See “How the NAC 800 Quarantines Endpoints” on page 1-35 of Chapter 1: “Overview of the ProCurve NAC 800” for more information.
If you are using the NAC 800 as a RADIUS server only, the connection settings do not matter.

Leave the settings at the defaults, or for the ProCurve Wireless Edge Services xl Module, ProCurve 420 AP, and ProCurve 530 AP, fill in only the community name.

11. Click the **ok** button.

12. To apply and save the 802.1X device configuration, you must also click the **ok** button in the **Home > System configuration > Quarantining** screen.

### Apply Changes

Whenever you alter the configuration for the 802.1X and RADIUS settings (including adding an 802.1X device), you must apply and save the changes. When you apply the changes, the CS's internal RADIUS server, or the RADIUS servers on all ESs in the cluster, automatically restart.

---

**Note**

The RADIUS server typically takes several seconds to restart. During this period, the RADIUS server is unavailable for authenticating end-users. To avoid interrupting services, configure 802.1X quarantining settings after hours.

Follow these steps:

1. If you have not already done so, click the **ok** button in the **Home > System configuration > Quarantining** screen.

   Clicking the **ok** button writes the change to both the startup-config and running-config.

### Restart the RADIUS Server

Follow these steps should you ever need to restart the RADIUS server manually:

1. Select **Home > System configuration > Enforcement clusters & servers.**
Configure the NAC 800 as a RADIUS Server

2. Click the name of the CS or ES. The Enforcement server screen is displayed.

Note

Figure 4-19 shows the Enforcement server screen for a CS. The screen for an ES features two menu options: General and Configuration. You should select the General menu option.
3. The **Process/thread status** area lists a number of services. Click the **restart now** button for radius. The **Operation in progress** screen is displayed.
Configure the NAC 800 as a RADIUS Server

4. Within several seconds, the Operation in progress screen should close. At the top of the Enforcement server screen, this message should be displayed:

   The radius process was restarted.

**Note**

Typically, the RADIUS server restarts without a problem. If it encounters difficulties, you should restart it from the root of the OS. Follow these steps:

1. Log in as root to the NAC 800 OS:
   a. Open an SSH or console session with the NAC 800.
   b. When asked for your username and password, enter root and the root password (default, procurve).

2. Enter this command:

   ProCurve NAC 800:# service radiusd restart

3. Read any messages that display. For example, if you have altered configuration files, one of the files might have an error and fail to load.
Manage Digital Certificates for RADIUS

The following authentication methods use mutual authentication, which means that the RADIUS server (in your case, the NAC 800 CS or ES) identifies itself to endpoints with a digital certificate:

- **EAP-TLS**
- **EAP-TTLS**
- **PEAP**

At its factory default settings, the NAC 800 authenticates as a RADIUS server with a self-signed digital certificate. However, this certificate is not intended for an enterprise environment. It identifies the NAC 800 as follows:

- subject=/C=CA/ST=Province/L=Some City/O=Organization/OU=localhost/CN=Root certificate/emailAddress=root@example.com
- issuer=/C=CA/ST=Province/L=Some City/O=Organization/OU=localhost/CN=Client certificate/emailAddress=client@example.com

You should load one of the following certificates on your NAC 800:

- A self-signed certificate that specifies the NAC 800’s FQDN as its common name (CN)
- A certificate that specifies the NAC 800’s FQDN as its CN and is signed by a trusted CA

In either case, the certificate must allow the NAC 800 to use it for client and server authentication. That is, the extensions for the key usage should be “TLS Web Server Authentication” and “TLS Web Client Authentication.”

Follow these steps to set up certificates for RADIUS services:

1. If you plan to use a CA-signed certificate, install the CA root certificate on the NAC 800.
2. Obtain a server certificate and install it on the NAC 800. You must specify the certificate and private key locations in the `/etc/raddb/eap.conf` file.

   As mentioned above, you can create a self-certificate or obtain a certificate from a CA.

The following sections explain how to complete these tasks. The final sections of this chapter give you some guidelines on setting up certificates on endpoints.
You must complete these tasks by accessing the root command line for the NAC 800's OS:

1. Open a console or SSH session with the NAC 800.

2. Log in:
   - username = root
   - password = <root password>

### Install the CA Root Certificate on the NAC 800

The NAC 800 must have the CA root certificate for the CA that signed its server certificate. If supplicants authenticate with certificates (the EAP method is EAP-TLS or, less commonly, PEAP or EAP-TTLS with an inner method that requires certificates), the NAC 800 also uses this CA certificate to verify the supplicants' certificates.

Follow these steps to install the CA certificate on the NAC 800:

1. Obtain the CA certificate from your CA.
   
   Your CA should instruct you how to complete this step.
   
   The certificate must be in PEM format. (See step 4 on page 4-49 for instructions on converting a DER or PFX certificate to PEM format.)

2. Transfer the CA certificate to the NAC 800.
   
   If you have installed PSCP on your management station, you can follow these steps:
   a. Save the CA certificate to your management station.
   b. Access the command prompt on your management station and move to the directory in which PSCP is installed.
   c. Enter this command:

   **Syntax:**
   
   pscp <path\filename> root@<NAC 800 IP address>://etc/raddb/certs/demoCA/cacert.pem
   
   Replace `<path\filename>` with the directory path and filename for the CA certificate.

   For example:

   pscp myCA.pem root@10.1.1.20://etc/raddb/certs/demoCa/cacert.pem
Be very careful to enter the output file for the certificate exactly as shown above: /etc/raddb/certs/demoCA/cacert.pem.

Otherwise, you must alter the name specified for the private key file and the certificate file in the “tls” section of the /etc/raddb/eap.conf file—which can lead to errors. (See step 12 on page 4-55.)

d. When prompted, enter the NAC 800’s root password.

3. Log in as root to the NAC 800 OS.

4. If the CA certificate is not in PEM format, follow these steps:
   a. Move to the correct directory:
      ProCurve NAC 800:/# cd /etc/raddb/certs/demoCA
   b. Convert from DER format with this command:
      Syntax: openssl x509 -in <filename> -inform DER -out <filename> -outform PEM
     
      Preferably, specify cacert.pem for the second filename.

      For example, enter:
      ProCurve NAC 800:/etc/raddb/certs/demoCA# openssl x509 -in cacert.der -inform DER -out cacert.pem -outform PEM

      Convert from PFX format with this command:
      Syntax: openssl pkcs12 -in <filename>.pfx -out <filename>.pem

      You should change the filename extension to reflect the changed format. Preferably, specify cacert.pem for the filename

5. Restart the RADIUS server.
   ProCurve NAC 800:/etc/raddb/certs/demoCA# service radiusd restart

Install a Server Certificate for RADIUS

You have a variety of options for obtaining and installing the server certificate for RADIUS authentication. You can:

- Create a self-signed certificate on the NAC 800.
Obtain and install a CA-signed certificate in one of these ways:
- Create a private/public keypair and certificate request on the NAC 800 and submit the request to your CA.
- On the CA, request a certificate on behalf of the NAC 800. Make sure to save the associated private key so that you can load it to the NAC 800.

Create a Self-Signed Certificate

Follow these steps to create a self-signed certificate to be used for RADIUS authentication:

1. Log into the NAC 800 as root.
2. Configure the openssl application to issue self-signed certificates with the correct extensions for a RADIUS server. (See Appendix B, “Linux Commands” for vi commands.)
   a. Copy the default configuration file for openssl to a new location. You will make changes to the new file.
      ProCurve NAC 800:# cp /var/ssl/openssl.cnf /etc/raddb/certs/openssl.cnf
   b. Enter this command:
      ProCurve NAC 800:# cd /etc/raddb/certs
   c. Alter the new configuration file:
      ProCurve NAC 800:/etc/raddb/certs# vi openssl.cnf
   d. Press [i] to enter Insert mode.
   e. Find the “[new_oids]” section. Add this text:
      
      [radsrv]
      subjectKeyIdentifier = hash
      authorityKeyIdentifier = keyid,issuer:always
      keyUsage = digitalSignature, keyEncipherment
      extendedKeyUsage = clientAuth, serverAuth
      
   f. Press [Esc] to exit Insert mode.
   g. Save the changes and exit vi.
      :wq
3. Enter this command to generate the self-signed certificate:

**Syntax:**

```bash
openssl req -x509 -config openssl.cnf -extensions radsrv -newkey [rsa | dsa];[512 | 1024 | 2048 | 4096] -nodes -days <number> -keyout cert-srv.pem -out cert-srv.pem
```

*The -config option should specify the new configuration file that you created in step 2. (Make sure that you are in the correct directory.) Similarly the -extensions option specifies the bracketed name for the extensions that you added to that file.*

*The -newkey option generates a private/public keypair for this certificate. Choose rsa or dsa for the algorithm and then choose the key length. (4096 is not a valid option for dsa). Replace <number> with the number of days that this certificate will remain valid.*

*The -nodes option in the command above creates the private key without password protection. For greater security, leave out this option when you enter the command. You will then be prompted to enter the password.*

*After you finish step 4, edit the /etc/raddb/eap.conf file and change the private key password from whatever to the password that you entered.*

For example:

```bash
ProCurve NAC 800:/etc/raddb/certs# openssl req -x509
-config openssl.cnf -extensions radsrv -newkey rsa:2048 -nodes -days 365 -keyout cert-srv.pem -out cert-srv.pem
```

**Note**

Be very careful to enter the output files for the key and the certificate exactly as shown above: `/etc/raddb/certs/cert-srv.pem`.

Otherwise, you must alter the name specified for the private key file and the certificate file in the “tls” section of the `/etc/raddb/eap.conf` file—which can lead to errors. (See step 12 on page 4-55.)

4. You will be prompted to enter information about the NAC 800. When prompted for the CN, enter the NAC 800's FQDN.

5. Restart the RADIUS server.

```bash
ProCurve NAC 800:/etc/raddb/certs# service radiusd restart
```
Manage Digital Certificates for RADIUS

Install a CA-Signed Certificate Using a Request Generated on the NAC 800

Follow these steps to create a certificate request and install a CA-signed certificate for RADIUS authentication:

1. Log in to the NAC 800 as root.
2. Enter this command:
   ```bash
   ProCurve NAC 800:/# cd /etc/raddb/certs
   ```
3. Configure the openssl application to create certificate requests that request the correct extensions for a RADIUS server. (See Appendix B, “Linux Commands” for vi commands.) If you are using your own Windows CA, you might skip this step and use a certificate template add the correct extensions.
   a. Copy the default configuration file for openssl to a new location. You will make changes to the new file.
      ```bash
      ProCurve NAC 800:# cp /var/ssl/openssl.cnf /etc/raddb/certs/openssl.cnf
      ```
   b. Alter the new configuration file:
      ```bash
      ProCurve NAC 800:/etc/raddb/certs# vi openssl.cnf
      ```
   c. Press [i] to enter Insert mode.
   d. Find the “[new_oids]” section. Add this text:
      ```
      [radsrv_req]
      subjectKeyIdentifier = hash
      authorityKeyIdentifier = keyid,issuer:always
      keyUsage = digitalSignature, keyEncipherment
      extendedKeyUsage = clientAuth, serverAuth
      ```
   e. Press [Esc] to exit Insert mode.
   f. Save the changes and exit vi.
      ```
      :wq
      ```
4. Enter this command to generate the certificate request:

**Syntax:**

```bash
openssl req -new -config openssl.cnf -extensions radsrv_req -newkey 
[rsa | dsa];[512 | 1024 | 2048 | 4096] -nodes -keyout <key_filename> -out 
<request_filename> [-outform [DER | PEM]]
```

*The*-config option should specify the new configuration file* that you created in step 2. (Make sure that you are in the correct directory.) Similarly, the*-extensions option specifies bracketed name for the extensions that you added to that file.

*The*-newkey option generates a private/public keypair for this certificate. Choose *rsa* or *dsa* for the algorithm and then choose the key length (*4096* is not a valid option for *dsa*).

The private key for the certificate is saved with the name you enter for the <key_filename>. The certificate request is saved with the name you enter for the <request_filename>. You can choose the format (DER or PEM) for the request (default: PEM). The -nodes option in the command above creates the private key without password protection. For greater security, omit this option when you enter the command. You will then be prompted to enter the password. In step 12 on page 4-55, you will edit the `/etc/raddb/eap.conf` file and specify this password.

For example:

```bash
ProCurve NAC 800:/etc/raddb/certs# openssl req -new 
-config openssl.cnf -extensions radsrv_req -newkey 
rsa:1024 -nodes -keyout mykey.pem -out myrequest.req
```

5. You will be prompted to enter information about the NAC 800. When prompted for the Common Name (CN), enter the NAC 800’s FQDN.

6. Transfer the certificate request to a Secure Copy (SCP) server.

   If you have installed PuTTY SCP (PSCP) on your management station, you can follow these steps:
   a. Access the command prompt on your management station and move to the directory in which PSCP is installed.
   b. Enter this command:

   **Syntax:**
   ```bash
   pscp root@<NAC 800 IP address>://etc/raddb/certs/<request_filename>
   <path_filename>
   ``
   *Transfers the request off the NAC 800. Replace <request_filename> with the name you specified in step 4 on page 4-53. The request is saved on the station with the name that you specify for <path_filename>.*
Configure the RADIUS Server—Integrated with ProCurve Identity Driven Manager

Manage Digital Certificates for RADIUS

For example:

pscp root@10.1.1.20://etc/raddb/certs/myrequest.req nacrequest.req

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

7. Submit the certificate request to your CA.

Contact your CA to learn how to complete this step. You should request X.509 format (either Distinguished Encoding Rules [DER] or Privacy Enhanced Mail [PEM]). However, if necessary you can convert a certificate that uses a different format. (See step 11.)

---

**Note**

If you are using a Windows CA, have the CA issue a certificate using the RAS and IAS Server template (or another template that has key extensions for both server authentication and client authentication).

---

8. After the CA returns the server certificate to you, transfer it to the NAC 800.

If you have installed PSCP on your management station, you can follow these steps:

a. Save the certificate to your management station.

b. Access the command prompt on your management station and move to the directory in which PSCP is installed.

c. Enter this command:

For example:

pscp mycertificate.pem root@10.1.1.20://etc/raddb/certs/mycertificate.pem

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

9. Log back in to the NAC 800 as root.

10. Enter this command:

    ProCurve NAC 800:# cd /etc/raddb/certs

11. If your certificate is not the desired format, you can convert it.

---

Syntax: pscp <path\filename> root@<NAC 800 IP address>://etc/raddb/certs/<certificate_filename>

*Replace <path\filename> with the directory path and filename for the server certificate. The certificate is saved with the name that you specify for <certificate_filename>.*
Convert from DER with this command:

**Syntax:** openssl x509 -in `<certificate_filename>` -inform DER -out `<certificate_filename>` -outform PEM

*For `<certificate_filename>` enter the name for the certificate that you chose in step 8. You should change the file name extension to reflect the changed format.*

For example, enter:

```
ProCurve NAC 800:/etc/raddb/certs# openssl x509 -in mycertificate.der -inform DER -out mycertificate.pem -outform PEM
```

Convert from PFX format with this command:

**Syntax:** openssl pkcs12 -in `<certificate_filename>.pfx` -out `<certificate_filename>.pem`

*For `<certificate_filename>` enter the name for the certificate that you chose in step 8 on page 4-54. You should change the filename extension to reflect the changed format.*

12. Alter the `/etc/raddb/eap.conf` file to specify the new private key and certificate files. (See Appendix B, “Linux Commands” for vi commands.)
   a. Enter this command:

   ```
   ProCurve NAC 800:/#vi /etc/raddb/eap.conf
   ```

   b. Use the arrow keys or other vi commands to reach the “tls” section of the configuration file. (See Figure 4-21.)
Note

The NAC 800 uses the “tls” configuration for server certificates for TLS, PEAP, and TTLS.

c. Press [i].

d. If you created a password for the private key, set
   private_key_password to the same key that you chose earlier. For
   example:

   ```plaintext
   private_key_password = mypassword
   ```

e. Set private_key_file to the same as the <key filename> that you speci-
   fied in step 4 on page 4-53. Keep the default path already included in
   the configuration file (which works as long as you saved the key in
   the proper directory). For example:

   ```plaintext
   private_key_file = $(raddbdir)/certs/mykey.pem
   ```

f. Set certificate_file to the same as the <certificate filename> that you
   specified in step 8-c on page 4-54 (or step 11 on page 4-54). Keep the
default path already included in the configuration file (which works
as long as you saved the certificate in the proper directory). For
example:

   ```plaintext
   certificate_file = $(raddbdir)/certs/mycertificate.pem
   ```

g. Make sure that CA_file is set to the filename (including the correct
   path) for the CA root certificate. This certificate was installed in
   “Install the CA Root Certificate on the NAC 800” on page 4-48.

---

tls {
    
    private_key_password = whatever
    private_key_file = $(raddbdir)/certs/cert-srv.pem

    # If Private key & Certificate are located in
    # the same file, then private_key_file &
    # certificate_file must contain the same file
    # name.
    certificate_file = $(raddbdir)/certs/cert-srv.pem

    # Trusted Root CA list
    CA_file = $(raddbdir)/certs/demoCA/cacert.pem

    dh_file = $(raddbdir)/certs/dh
    random_file = $(raddbdir)/certs/random

Figure 4-21. Example radiusd.conf File——tls Section
h. Press [Esc].

i. Enter this command:

: wq

13. Restart the RADIUS server.

    ProCurve NAC 800:/# service radiusd restart

If the RADIUS server fails to restart, you have probably mistyped the filenames or private key password in step 12. Carefully recheck the configuration.

Install a CA-Signed Certificate Using a Request Generated on Behalf of the NAC 800

Follow these steps to generate a certificate for the NAC 800 on your organization's CA and to install that certificate on the NAC 800:

1. Following the instructions in your CA documentation, create the certificate request and generate the certificate (in X509 format).
   
Enter the NAC 800's FQDN for its CN. Specify the NAC 800's country, state, and so forth, as prompted.

Make sure to generate a RADIUS server certificate for the NAC. (Its key usage extensions should provide for both client and server authentication.)

2. Transfer the certificate and the private key to the NAC 800.
   
   If you have installed PSCP on your management station, you can follow these steps:
   
a. Save the certificate and private key to your management station.
   
   It is very important that you save the private key for the certificate. You will upload this key to the NAC 800 in step 3. You might have been prompted to create a password for the key. If you do, you will need to specify that password in step 6 on page 4-59.
   
b. Access the command prompt on your management station and move to the directory in which PSCP is installed.
c. Enter this command:

**Syntax:** `pscp <path\filename> root@<NAC 800 IP address>://etc/raddb/certs/<certificate_filename>`

*Replace* `<path\filename>` *with the directory path and filename for the server certificate. Replace* `<certificate_filename>` *with the name under which the certificate will be stored on the NAC 800.*

For example:

```bash
pscp mycertificate.pem root@10.1.1.20://etc/raddb/certs/mycertificate.pem
```

d. Repeat the previous command to transfer the private key file, if separate from the certificate file:

**Syntax:** `pscp <path\filename> root@<NAC 800 IP address>://etc/raddb/certs/<key_filename>`

*Replace* `<path\filename>` *with the directory path and filename for the private key. Replace* `<key_filename>` *with the name under which the private key will be stored on the NAC 800.*

For example:

```bash
pscp mycertificate.pem root@10.1.1.20://etc/raddb/certs/mykey.pem
```

**Note**

The private key and server certificate might be stored in the same file. In this case, you only need to enter the command once and you should specify the output file: `:/etc/raddb/certs/cert-srv.pem`.

This allows the NAC 800 to use the new certificate without forcing you to alter the “tls” section of the `/etc/raddb/eap.conf` file—which can lead to errors.

e. When prompted, enter the NAC 800’s root password.

3. Log in to the NAC 800 as root.

4. Enter this command:

```
ProCurve NAC 800:/# cd /etc/raddb/certs
```

5. If your certificate is not in the correct format, you can convert it.
Convert from DER format to PEM format with this command:

**Syntax:**  
openssl x509 -in `<certificate filename>` -inform DER -out `<certificate filename>` -outform PEM

For `<certificate_filename>`, enter the name for the certificate that you chose in step 2-c on page 4-58. You should change the filename extension to reflect the changed format.

For example, enter:

```
ProCurve NAC 800:/etc/raddb/certs# openssl x509 -in mycertificate.der -inform DER -out mycertificate.pem -outform PEM
```

Convert from PFX format with this command:

**Syntax:**  
openssl pkcs12 -in `<certificate filename>.pfx` -out `<certificate filename>.pem`

For `<certificate_filename>`, enter the name for the certificate that you chose in step 2-c on page 4-58. You should change the filename extension to reflect the changed format.

6. Alter the `/etc/raddb/eap.conf` file to specify the new certificate. (See Appendix B, “Linux Commands” for vi commands.)

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>You can skip this step if the new server certificate and private key are in the same file, which is named <code>cert-srv.pem</code>, and if the private key is not protected with a password.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>a. Enter this command:</td>
</tr>
<tr>
<td>ProCurve NAC 800:/# vi /etc/raddb/eap.conf</td>
</tr>
<tr>
<td>b. Use the arrow keys or other vi commands to reach the “tls” section of the configuration file. (See Figure 4-22).</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Note</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>The NAC 800 uses the “tls” configuration to authenticate itself for TLS, PEAP, and TTLS.</td>
</tr>
</tbody>
</table>
Manage Digital Certificates for RADIUS

**Figure 4-22. Example radiusd.conf File—tls Section**

```plaintext
tls {
    private_key_password = whatever
    private_key_file = ${raddbdir}/certs/cert-srv.pem

    # If Private key & Certificate are located in
    # the same file, then private_key_file &
    # certificate_file must contain the same file
    # name.
    certificate_file = ${raddbdir}/certs/cert-srv.pem

    # Trusted Root CA list
    CA_file = ${raddbdir}/certs/demoCA/cacert.pem

dh_file = ${raddbdir}/certs/dh
random_file = ${raddbdir}/certs/random
}
```

c. Press `[i]`.
d. Set **private_key_password** to equal the password you chose to protect your key. For example:

   ```plaintext
   private_key_password = mypassword
   ```
e. Set **private_key_file** to equal the `<key_filename>` you specified in step 2-d on page 4-58. Keep the default path already included in the configuration file (which works as long as you saved the key in the proper directory). For example:

   ```plaintext
   private_key_file = ${raddbdir}/certs/mykey.pem
   ```
f. Set **certificate_file** to equal the `<certificate_filename>` you specified in step 2-c on page 4-58 (or step 5 on page 4-58). Keep the default path already included in the configuration file (which works as long as you saved the certificate in the proper directory). For example:

   ```plaintext
   certificate_file = ${raddbdir}/certs/mycertificate.pem
   ```
g. Make sure that **CA_file** is set to the filename (including the correct path) for the CA root certificate. This certificate was installed in “Install the CA Root Certificate on the NAC 800” on page 4-48.
h. Press `[Esc]`.
i. Enter this command:

   ```plaintext
   :wq
   ```
7. Restart the RADIUS server.

    ProCurve NAC 800:/# service radiusd restart

    If the RADIUS server fails to restart, you have probably mistyped the password or filenames in step 6. Carefully recheck the configuration.

Manage Certificates on Endpoints

To authenticate the NAC 800 RADIUS server, endpoints require the root certificate for the CA that signed the NAC 800's server certificate. The exact steps for installing this certificate depend, of course, on the endpoint. Refer to the appropriate documentation.

Note

If you selected a well-known vendor CA to issue your NAC 800's certificate, most endpoints already have the necessary certificate.

You must also install user or computer certificates on endpoints—if you have selected an EAP method that requires supplicants to authenticate with a certificate rather than a password. Generally, you would issue those certificates using your organization's CA. Refer to the documentation for your CA service for instructions.

Disable Server Validation on Endpoints

You might want to prevent endpoints from checking the NAC 800's server certificate for several reasons:

- You do not want to bother installing new certificates on the NAC 800 for server authentication.

Caution

Because this option could allow endpoints to connect to a rogue server, ProCurve Networking does not recommend it.

- You want to help endpoints temporarily connect to the network so that they can obtain the CA certificate necessary for validating the NAC 800's certificate.

For example, a Windows station automatically receives the domain's CA root certificate when it joins the domain.

After an endpoint obtains the certificate, it should be configured to once again validate the server certificate.
Follow these steps on an endpoint to disable validation of the server on the native Windows 802.1X supplicant:

1. Select Start > Settings > Network Connections > Local Area Connection.

2. Click the Properties button.

3. Select the Authentication tab in the window that is displayed.
4. Choose your EAP type and click the **Properties** button.
5. Clear the **Validate server certificate** check box.
6. Click **OK** to close all open windows.

Follow these steps to disable validation of the server on an endpoint that uses the Microsoft Wireless Zero Configuration client:

1. Select **Start > Settings > Network Connections > Wireless Network Connection**.
Figure 4-26. Start > Settings > Network Connections > Local Area Connection

2. Click the **Properties** button.
3. Select the **Wireless Networks** tab in the window that is displayed.
4. Select the service set identifier (SSID) for your wireless network in the **Preferred networks** area and click the **Properties** button.

   If the SSID has not yet been configured on the client, you must click the **Add** button instead. Then, in addition to completing the steps below, you must configure settings such as the SSID, the authentication method, and the encryption type.

5. Select the **Authentication** tab in the window that is displayed.
6. Choose the EAP type and click the Properties button.
7. Uncheck the Validate server certificate box.
Manage Digital Certificates for RADIUS

Figure 4-29. <EAP type> Properties

8. Click OK to close all open windows.