RADIUS Server

Contents

Overview ......................................................... 11-2
RADIUS Authentication ........................................ 11-3
  Configuring the Internal RADIUS Server ................. 11-4
    Choosing the Authentication Type for 802.1X/EAP .... 11-5
    Specifying the RADIUS Server’s Digital Certificate ... 11-8
    Choosing the Source for User Credentials ............... 11-9
    Configuring the Local RADIUS Database ................. 11-12
    Using LDAP for the Data Source ......................... 11-20
    Specifying a Domain Proxy RADIUS Server .............. 11-27
    Specifying Global RADIUS Settings ..................... 11-30
    Adding RADIUS Clients .................................. 11-31
    Starting and Stopping the RADIUS Server ............... 11-32
    Enabling Authentication to the Internal Server on a WLAN .... 11-33
RADIUS Accounting ............................................. 11-36
  Enabling Accounting to the Internal RADIUS Server on a WLAN ... 11-38
  Viewing the Internal RADIUS Server’s Accounting Logs ...... 11-41
Overview

A Remote Access Dial In User Service (RADIUS) server provides centralized authentication (and sometimes accounting) for a network. The RADIUS protocol regulates communications between network access servers (NASs) and RADIUS servers.

The NASs are devices such as switches and Wireless Edge Services xl Modules, which provide network access to stations. First, however, they can force the stations to authenticate themselves.

Although the NAS enforces authentication, it does not decide whether a particular station is authenticated. Instead it submits an authentication request for the station to the RADIUS server. The RADIUS server decides whether a station can connect to the network according to the user's credentials and the policies configured on the server.

The Wireless Edge Services xl Module acts as a NAS when it enforces 802.1X, Web authentication (Web-Auth), or MAC authentication. In addition to forwarding authentication requests to an external RADIUS server, the module can make decisions with its internal server. In this second case, the module acts as the NAS and as the RADIUS server.

You learned about configuring settings for an external RADIUS server in Chapter 4: Wireless Local Area Networks (WLANs). In this chapter, you will learn how to configure the module's internal RADIUS server.

The Wireless Edge Services xl Module's internal RADIUS server can provide the following services:

- authenticating users who attempt to connect to a wireless LAN (WLAN) that requires authentication to a RADIUS server
- responding to authentication requests from network access servers (NASs) in the wired network
- creating accounting logs of user activity on a WLAN
RADIUS Authentication

The Wireless Edge Services xl Module’s RADIUS authentication server fulfils these roles:

- decides whether a user can connect to a WLAN that enforces one of these types of security:
  - 802.1X
  - Web authentication (Web-Auth)
  - MAC authentication
- makes the decision based on credentials stored in one of these locations:
  - user accounts configured on the module itself
  - user accounts on a Lightweight Directory Access Protocol (LDAP) server, such as Novell eDirectory
- specifies policies (such as a dynamic virtual LAN (VLAN) assignment) for authenticated users

For 802.1X authentication, the module’s internal RADIUS server supports these Extensible Authentication Protocol (EAP) methods:

- EAP-Transport Layer Security (TLS)
- EAP-Tunneled TLS (TTLS) with Message Digest 5 (MD5)
- EAP-TTLS with Password Authentication Protocol (PAP)
- Protected EAP (PEAP) with Generic Token Card (GTC)
- PEAP with Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2)

All of these methods are suitable for a wireless network. That is, they not only enable a wireless user to authenticate securely, they also help the Wireless Edge Services xl Module and the station to generate a unique encryption key for the association. This key can be either for Wired Equivalent Privacy (WEP) or the more secure Wi-Fi Protected Access (WPA).

Table 11-1 summarizes the characteristics of these different EAP types.
Table 11-1. EAP Methods

<table>
<thead>
<tr>
<th>EAP Type</th>
<th>Characteristics</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>The wireless station and the module’s RADIUS server exchange digital certificates in a three-step TLS handshake.</td>
</tr>
<tr>
<td>EAP-TTLS with MD5</td>
<td>• The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.</td>
</tr>
<tr>
<td></td>
<td>• Inside the secure tunnel, the wireless station submits a username and a hashed (MD5) password.</td>
</tr>
<tr>
<td>EAP-TTLS with PAP</td>
<td>• The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.</td>
</tr>
<tr>
<td></td>
<td>• Inside the secure tunnel, the wireless station sends a PAP request.</td>
</tr>
<tr>
<td>PEAP with GTC</td>
<td>• The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.</td>
</tr>
<tr>
<td></td>
<td>• Inside the secure tunnel, the wireless station submits a GTC packet with its username and a password.</td>
</tr>
<tr>
<td>PEAP with MS-CHAP v2</td>
<td>• The module’s RADIUS server authenticates itself with a digital certificate and creates a secure TLS tunnel with the wireless station.</td>
</tr>
<tr>
<td></td>
<td>• Inside the secure tunnel, the wireless station submits a username and a password using the MS-CHAP v2 protocol.</td>
</tr>
</tbody>
</table>

Configuring the Internal RADIUS Server

You must complete the following steps to configure the internal RADIUS server to authenticate users that connect to a WLAN:

1. Select the authentication type.
2. Specify the internal RADIUS server’s digital certificate.
3. Select the source for policies and credentials:
   • If you select the local database, create groups and user accounts.
   • If you select a LDAP-compliant server, configure the LDAP settings and create a group.
4. Restart the RADIUS server.
5. Specify the internal server (loopback address) as the RADIUS server for one or more WLANs.
Depending on your environment, you might also need to complete these tasks:

- **Specify proxy RADIUS servers to which the local RADIUS server forwards queries**—This step allows the Wireless Edge Services xl Module to relay authentication requests in certain domains to external servers.

- **Specify RADIUS clients, which query the local RADIUS server**—This step allows the module to authenticate users who connect to different NASs—in both the wired and wireless network.

Whenever you make a change to the RADIUS settings, the Web browser interface will ask you to restart the RADIUS server. (See Figure 11-1).

**Figure 11-1. Restarting the RADIUS Server**

Click the **Yes** button.

**Choosing the Authentication Type for 802.1X/EAP**

For 802.1X authentication, you must select the EAP method with which the RADIUS server authenticates users. Users’ wireless client utilities must be configured for the same EAP method. Table 11-2 lists the available options, including the requirements for each. Refer to this table when you add the user’s account.
Table 11-2. Internal RADIUS Server EAP Methods

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Server Credentials</th>
<th>Station Credentials</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>Digital certificate</td>
<td>Digital certificate</td>
</tr>
<tr>
<td>EAP-TTLS with MD5</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-TTLS with PAP</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-PEAP with GTC</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
<tr>
<td>EAP-PEAP with MSCHAPv2</td>
<td>Digital certificate</td>
<td>Password</td>
</tr>
</tbody>
</table>

**Note**

You do not have to select any particular protocol to use the module’s internal RADIUS server for Web-Auth or MAC authentication.

To select the method, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
Figure 11-2. Choosing the EAP Method

2. From the **802.1x EAP/Auth Type** drop-down menu, select a method. Select **all** to allow users to authenticate with any of the supported methods.

3. Next, choose your server’s digital certificates (explained in the section below). Or click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.
Specifying the RADIUS Server’s Digital Certificate

As an authentication server, the Wireless Edge Services xl Module requires various certificates:

■ a server certificate

   No matter which EAP type you select, the internal RADIUS server must authenticate itself using a digital certificate.

   By default, the module identifies itself to users with the server certificate in the default-trustpoint. This certificate is installed on the module when it ships and is self-signed with the name Hewlett-Packard.

   Alternatively, the module can authenticate itself with one of these certificates:
   • a self-signed certificate that you create on the module
   • a digital certificate signed by a trusted certificate authority (CA) and installed on the module

■ a CA certificate

   The Wireless Edge Services xl Module uses the public key in the CA certificate to verify certificates signed by that CA.

   For example, for EAP-TLS, the RADIUS server checks users’ digital certificates. So the server needs the CA certificate for the CA that signed the users’ digital certificates.

On the Wireless Edge Services xl Module, you create trustpoints and load certificates into those trustpoints. Install the correct certificates before completing the following tasks for the RADIUS server:

■ selecting which of the module’s own digital certificates it should use to authenticate to users (mandatory)
■ selecting which of the module’s CA certificates it should use to authenticate users (for EAP-TLS)

See “Digital Certificates” on page 2-165 of Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module for instructions on creating trustpoints.
Then follow these steps:

1. Select **Network Setup > Radius Server** and click the **Authentication** tab.

2. In the **Cert Trustpoint** drop-down menu, select the trustpoint in which you have loaded the server certificate for RADIUS authentication.

   Selecting <Create a New Certificate> opens the Certificates Wizard and guides you through the creation or installation of certificates.

3. If you have selected EAP-TLS, choose a trustpoint from the **CA Cert Trustpoint** drop-down menu.

   Select the trustpoint in which you loaded the CA certificate for the CA that signs users’ digital certificates. This trustpoint should typically match the one you selected for the **Cert Trustpoint**.

   Again, you can select <Create a New Certificate> to open the Certificates Wizard.

4. Next choose the source for authentication data (explained in the section below). Or click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.

**Choosing the Source for User Credentials**

The RADIUS server can draw on one of two potential databases for authenticating users:

- **its local database**

  In addition to checking a user’s credentials against user accounts its local database, the RADIUS server verifies that the user is connecting at an allowed time (specified in the user’s assigned group).

  After authenticating a user, the Wireless Edge Services xl Module can place that user in a dynamic VLAN (also specified in the user’s assigned group).

- **an LDAP-compliant directory server**

  The module’s RADIUS server binds to the directory server and looks up users’ credentials.

To select the database, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
Figure 11-3. Choosing the Source for Credentials

2. In the **Auth Data Source** field, use the drop-down menu to select the source for policies and credentials, either **local** or **ldap**.

3. Click the **Apply** button and, when the screen is displayed asking you to restart the server, click the **Yes** button.

4. Click the **Save** link to copy the configuration to the startup-config.
Depending on your choice, you must complete one of the following tasks:

- configure the local database (see “Configuring the Local RADIUS Database” on page 11-12)
- configure LDAP server settings and at least one group in the local database (see “Using LDAP for the Data Source” on page 11-20)

Table 11-3 explains the requirements for configuring credentials for each EAP method, depending on whether the Wireless Edge Services xl Module uses its local database or an LDAP server for the data store.

### Table 11-3. Requirements for Credentials Depending on EAP Method

<table>
<thead>
<tr>
<th>EAP Method</th>
<th>Requirement for Credentials in Local Database</th>
<th>Requirement for Credentials on LDAP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>EAP-TLS</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Host certificates (issued by the same CA) loaded on the wireless stations&lt;br&gt;• CA certificate loaded on both the module and stations&lt;br&gt;• Usernames submitted with host certificates added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Host certificates (issued by the same CA) loaded on the wireless stations&lt;br&gt;• CA certificate loaded on both the module and stations&lt;br&gt;• Host certificate loaded in the user account on the LDAP server</td>
</tr>
<tr>
<td>EAP-TTLS with MD5</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>EAP-TTLS with PAP</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>PEAP with GTC</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
<tr>
<td>PEAP with MS-CHAP v2</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added to the module’s local RADIUS database</td>
<td>• Server certificate loaded on the module&lt;br&gt;• Usernames and passwords assigned to users and added as LDAP accounts</td>
</tr>
</tbody>
</table>
Configuring the Local RADIUS Database

You must complete the following tasks to configure the local database:

1. Create groups, which define policies for users.
2. Add user accounts to the group.

Creating a Group. A group defines policies on the Wireless Edge Services xl Module’s internal RADIUS database, including:

- the dynamic VLAN for authenticated users in this group
- when users in this group are allowed to connect to the network

You can create two types of groups:

- a normal group
- a guest group, which only allows temporary guest accounts

To configure a group, complete these steps:

1. Select **Network Setup > RADIUS Server** and click the **Groups** tab.

### Figure 11-4. Configuring RADIUS Server Groups

<table>
<thead>
<tr>
<th>Name</th>
<th>Guest Group</th>
<th>VLAN ID</th>
<th>Time of Access Start</th>
<th>Time of Access End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guests</td>
<td>✔</td>
<td>0 0001</td>
<td>000000</td>
<td>1659</td>
</tr>
<tr>
<td>Faculty</td>
<td>✗</td>
<td>8 0000</td>
<td>8 0000</td>
<td>2359</td>
</tr>
<tr>
<td>Students</td>
<td>✗</td>
<td>12 0000</td>
<td>12 0000</td>
<td>2359</td>
</tr>
</tbody>
</table>

**Time of access in days**

- ✔ Monday
- ✔ Tuesday
- ✔ Wednesday
- ✔ Thursday
- ✔ Friday
- ✔ Saturday
- ✗ Sunday
2. Click the Add button. The ADD screen is displayed.

![Figure 11-5. Adding a RADIUS Server Group](image)

3. In the Name field, enter a meaningful name—for example, “Faculty.”

4. In the VLAN ID field, enter the dynamic VLAN for users in this group.
   
   If you enter 0, the Wireless Edge Services xl Module assigns the user to
   the VLAN configured for the user’s WLAN.

   You should not use dynamic VLANs with Web-Auth. The user’s station
   receives an IP address in the static VLAN before the user can log in and
   receive the dynamic VLAN assignment.

   **Note**
   
   You must enable dynamic VLANs in the WLAN to which users connect for this
   setting to take effect. See “Enabling Authentication to the Internal Server on
   a WLAN” on page 11-33.
5. Specify the times of day when users in this group can connect to the wireless network.
   a. In the **Time of Access Start** field, enter the earliest time that users can connect.
   b. In the **Time Access End** field, enter the latest time users can connect.

Always enter times in four digits, the first two digits being the hour in the 24-hour clock and the second two digits being the minutes.

As shown in Figure 11-5, by default, users can connect at any time of the day or night.

6. In the **Time of access in days** section, check the boxes to specify the days of the week when users in this group can connect to the wireless network. By default, network access is available every day.

7. Check the **Guest Group** box if you want this group to be for guests.

   Guests have temporary accounts. (See “Creating User Accounts” on page 11-15.)

8. Click the **OK** button.

The group is displayed in the top section of the **Network Setup > Local RADIUS Server > Groups** screen. Information and policies for the group are listed in these columns:

- **Name**—the name of the group
- **Guest Group**—displays a red X for normal groups and a green check for guest groups
- **VLAN ID**—the dynamic VLAN for users in this group (if dynamic VLANs are enabled for the WLAN to which the user associates)
- **Time of Access Start**—the time at which users in this group can begin connecting to the network
- **Time of Access End**—the time at which users in this group can no longer connect to the network (even if they enter the correct password)

The **Time of access in days** section of the **Network Setup > Local RADIUS Server > Groups** screen includes a box for each day of the week. When you select a group, the boxes are checked for days on which users in that group can connect to the network.

You can modify these settings for a group:

- **VLAN ID**
- **time of access start and end**
- **days access is allowed**
To modify a group, select it and click the **Edit** button. In the **EDIT** screen that is displayed, configure the settings just as you would for a new group. (However, you cannot change the group’s name nor whether it is a normal or guest group.) When you are finished, click the **OK** button.

To delete a group, select it in the **Network Setup > Local RADIUS Server > Groups** screen and click the **Delete** button. The Web browser interface asks you to restart the RADIUS server for the change to take effect.

**Creating User Accounts.** You must configure a user account for every user allowed to connect to your network. This requirement holds true whether the internal RADIUS server authenticates users with passwords or with digital certificates.

Just as the Wireless Edge Services xl Module’s RADIUS server defines two types of groups, it defines two types of user accounts:
- a normal account
- a guest account

Normal users can only join normal groups, and guest users can only join guest groups.

You configure the following parameters for user accounts:
- username
- if you are using TTLS or PEAP, a password
- if the account is a guest account, an expiration time

To configure an account, complete these steps:
1. Select **Network Setup > Local RADIUS Server** and click the **Users** tab.
2. Click the **Add** button. The **ADD** screen is displayed.
3. In the **User ID** field, enter the username. The username can be up to 64 characters and can include alphanumeric and special characters.

4. Check the **Guest User** box if this is a temporary account for a guest.

5. In the **Password** and **Confirm Password** fields, specify the user’s password. The password can be up to 21 characters and can include alphanumeric and special characters.
By default, this password is displayed in plaintext in the Wireless Edge Services xl Module’s configuration. To learn how to encrypt the password, see “Password Encryption” on page 2-105 of Chapter 2: Configuring the ProCurve Wireless Edge Services xl Module.

6. For a guest user, you must specify the period during which the account is active.

As soon as you check the Guest User box, the OS creates a default period, which begins at the current time (shown in the Current Switch Date field) and ends 24 hours after the current time. See Figure 11-7.
The guest account is active only for the period between the two times. To alter the times, follow these steps:

a. In the **Start Date & Time** field, enter the date and time at which this account is enabled.

   Enter the date in this format, in which MM is the number of the month, DD is the date, and YYYY is the year:
   
   MM/DD/YYYY

   After the date, enter a hyphen (-) and the time in this format, in which HH is the hour in the 24-hour clock and MM is the minutes:
   
   HH:MM

   For example, enter:
   
   02/17/2007-08:00

   By default, the account’s start date and time is the current time.

b. In the **Expiry Date & Time** field, enter the date and time at which this account is disabled.

   Use the same format as for the **Start Date and Time** field. Of course, the expiry time must be later than the start time.

   After the account expires, it may remain listed in the **Network Setup > Local RADIUS Server > Users** screen. The Wireless Edge Services xl Module automatically clears out expired accounts every 24 hours. In the meantime, however, no one can use the expired account to connect.

7. In the **Available Groups** section, which lists all groups configured for this type of user, select a group and click the **Add** button. The group enters the **Configured Groups** section.

   For example, in Figure 11-6, the user is a normal user (the **Guest User** box is not checked), so the normal groups are displayed.

8. You can repeat step 6 and assign the user to multiple groups. However, it is recommended that you assign the user to one group only.

   Only assign a user to more than one group when the groups allow access at mutually exclusive times. The policy configured for the group that currently allows access takes effect.

   For example, you could create a Weekdays group and a Weekend group and assign the groups to different VLANs. A user that is a member of both groups would be placed in the Weekdays VLAN on Friday, but in the Weekend VLAN when she logs in on Saturday.
You must never assign a user to groups with overlapping access days or times; such a configuration prevents you from determining which policy applies to the user during the overlapping times. For example, if one group allows access at all times and another group allows access only during normal work hours, you cannot assign a user to both groups. During the day, the policies would conflict.

9. Click the OK button.

The user account is displayed in the Network Setup > Local RADIUS Server > Users screen. Information about the account is listed in these columns:
- User ID—the username
- Guest User—displays a red X for normal accounts and a green check for guest accounts
- Start Date—the date and time at which a guest account becomes active (not applicable to normal accounts, which are immediately active)
- Expiry Date—the date and time at which the guest account becomes no longer active (not applicable to normal accounts, which are permanent)

When you select an account, the group or groups for the user are displayed in the Assigned Groups section.

To modify an account, select it and click the Edit button. The EDIT screen, which is similar to the Add screen, is displayed.

In the EDIT screen, you can change the user’s password and group assignments. However, you cannot alter the username or the definition of the account as a normal or guest account. When you have finished your modifications, click the OK button.

To delete an account, select it in the Network Setup > Local RADIUS Server > Users screen and click the Delete button. When prompted, click OK to restart the RADIUS server and apply the change.

Every 24 hours, the Wireless Edge Services xl Module checks the local RADIUS server database and removes any expired guest accounts.
Using LDAP for the Data Source

The Wireless Edge Services xl Module’s internal RADIUS server can authenticate users against an LDAP data source. To authenticate successfully, a user must meet these conditions:

- has an account stored on the directory server
- enters a password that matches the password in this account (or, for TLS, has a valid digital certificate)
- is listed in the directory as member of a group currently allowed access

The internal RADIUS server verifies that these conditions are met. To do so, it must bind to the LDAP server and perform searches, looking up the user’s account and group memberships and verifying the user’s password. See “Configuring the Internal RADIUS Server to Bind to an LDAP Server” on page 11-20.

To determine whether the user’s group is currently allowed access, the server checks the policy stored for that group on its internal database. See “Configuring Groups for Use with an LDAP Server” on page 11-24.

Configuring the Internal RADIUS Server to Bind to an LDAP Server.

If you select LDAP as the source for policies and user accounts, you must enable the Wireless Edge Services xl Module to communicate with your company’s LDAP server.

The internal RADIUS server performs these functions:

- It binds to the LDAP server.
  
  To complete the binding, the server submits a distinguished name and password to the LDAP server. You must specify the name and password of an account with administrative rights. In addition, you must specify the base directory in which the administrator account is stored.

- It searches the LDAP server’s directory to check the user’s credentials and group memberships.

You must configure filter strings, which the internal RADIUS server uses to retrieve information from the directory:

- With the user login filter, the internal RADIUS server verifies that the supplicant has an account and that his or her password matches the password in that account.
With the group login filter, the internal RADIUS server checks that the supplicant is a member of a group that is allowed access.

You must also specify the names of attributes that the RADIUS server retrieves during these searches, including the password and group memberships.

To configure LDAP settings, complete these steps:

1. Select **Network Setup > Local RADIUS Server** and click the **Authentication** tab.
2. From the **Auth Data Source** drop-down menu, select **ldap**.
3. In the **LDAP Server Details** section, click the **Primary** tab.

![Network Setup > Local RADIUS Server](image)

**Figure 11-8. Configuring LDAP Settings**

11-21
4. In the **IP Address** and **Port #** fields, specify your LDAP server's IP address and port.

The port number can be from 1 through 65535. The default port for LDAP is 389.

5. Configure the information that the internal RADIUS server submits to bind to the LDAP server:
   a. In the **Bind DN** field, enter the distinguished name for an administrator account on the LDAP server.

   For example, enter:
   
   `cn=Administrator,cn=Users,dc=mydomain,dc=com`

   The administrator account must be in the domain that you specify in step 5.

   b. In the **Bind Password** field, enter the password for the name that you specified above.

6. In the **Base DN** field, enter the name of the domain in which the module begins searching for user accounts.

   For example, enter:
   
   `cn=Users,dc=mydomain,dc=com`

7. In the **User Login Filter** field, enter a filter string that searches for a user's account based on the username submitted during EAP.

   An example of a user login filter is:
   
   `(sAMAccountName=%{Stripped-User-Name})`

   Another example is:
   
   `(uid=%{Stripped-User-Name};%{User-Name})`

   The purpose of this filter is to verify that the LDAP server has a particular user account—an account that matches the username that the user enters.

   The syntax follows that for standard LDAP searches.

   First, you enter the name of the attribute that your LDAP server uses to store a username. This attribute might be “uid,” “sAMAccountName,” or “cd.”

   Next, set the attribute equal to the username submitted through EAP. This username is specified by one or both of the following:
   
   • `%{Stripped-User-Name}`

   • `%{User-Name}`
These strings configure the internal RADIUS server to submit the username without appending a domain name. Make sure that the attribute you chose lists the username in this form.

8. In the **Password Attribute** field, specify the attribute that stores a user’s password.

When looking up a user’s account, the internal RADIUS server also requests a check on the user’s password (or, depending on the EAP type, a hash of that password). The string that you enter in the **Password Attribute** field determines the attribute name that the server requests.

Match the attribute name used by your LDAP server—commonly “user-Password” or “User-Password.”

9. In the **Group Filter** field, enter a filter string that searches for the groups to which the users belongs.

This purpose of the group filter is to verify that the user is a member of the group on the local RADIUS server that currently allows access.

An example of a group filter is:

```
&(objectClass=Group)(member=%{Ldap-UserDn}))
```

The first part of this filter tells the internal RADIUS server to search only for group type objects. “Group” is one example of the name for this object class. Other examples include:

- GroupOfUniqueNames
- GroupOfNames

The second part of the filter configures the internal RADIUS server to search only for groups in which this user is a member. First enter the name of the attribute that your LDAP server uses to list the members of a group. In this example, that attribute is “member.” Another example is “unique-member.” Next, set this attribute equal to this variable:

```
%{Ldap-UserDn}
```

This variable configures the module to submit the username as an LDAP distinguished name. To create this name, the module adds the username to the base distinguished name. For example:

```
cn=user,cn=Users,dn=mydomain,dn=com
```

Make sure that the name produced is the user’s correct distinguished name.

The internal RADIUS server automatically adds this string to the filter:

```
(<group attribute>=<local group name>)
```
The RADIUS server replaces <group attribute> with the string that you enter in the Group Attribute field. (See step 11). The server replaces <local group name> with the name of the group configured in the local RADIUS database.

10. In the Group Membership Attribute field, specify the attribute that stores a user's group memberships.

The internal RADIUS server requests this attribute in the search for the user accounts. The attribute is commonly named “memberOf” or “radius-GroupName.”

11. In the Group Attribute field, specify the attribute that your LDAP server uses to store the name of a group object.

The internal RADIUS server uses this attribute as part of the search with the group filter. See step 9 for more information about this search.

12. In the Net Timeout field, enter a time from 1 through 10 seconds.

If the Wireless Edge Services xl Module does not receive a response within this time, it considers the LDAP server unreachable. If you have configured a secondary LDAP server, the module contacts it. Otherwise, authentication fails.

13. Optionally, click the Secondary tab in the LDAP Server Details section. Repeat steps 4 through 12 to configure the secondary LDAP server.

14. Click the Apply button.

15. Click the Save link to save your configuration to the startup-config.

You can edit LDAP setting by changing the appropriate fields and clicking the Apply button. Whenever you change a setting, you must re-enter the bind password.

You can also remove all settings for a particular LDAP server at once:

1. Click the server's tab (Primary or Secondary).

2. Check the Delete Primary Ldap server or Delete Secondary Ldap server box.

3. Click the Apply button and save your configuration to the startup-config.

**Configuring Groups for Use with an LDAP Server.** To authenticate users, the Wireless Edge Services xl Module's internal RADIUS server requires at least one group policy. If you are using an LDAP server as the data source, the group name must match the name of wireless users' group as stored on the LDAP server.
Follow these steps to configure the group and set policies for it:

1. Select **Network Setup > Radius Server** and click the **Groups** tab.
2. Click the **Add** button, The **ADD** screen is displayed.

   ![Figure 11-10.Adding a RADIUS Server Group](image)

3. In the **Name** field, enter a name that matches the name of a group on your directory server. This is the group that is allowed wireless access; make sure that all potential wireless users are members. (Or create multiple groups.)

   The name you assign the group must match *exactly* the group name as stored on your LDAP server. The LDAP server might use several attributes to name the group. The **Group Attribute** field, in the LDAP bind settings, specifies the attribute that the group name matches. (See step 9 on page 11-23.)

   For example, you specify “cn” for the group attribute. The cn of the group for wireless users is listed as “Wireless Users” on the directory server. So you enter “Wireless Users” in the **Name** field.

4. In the **VLAN ID** field, enter the dynamic VLAN for users in this group.

   If you leave the ID at 0, the Wireless Edge Services xl Module assigns the user to the static VLAN associated with the user’s WLAN.
You should be careful when using dynamic VLANs with Web-Auth. The user’s station receives an IP address in the static VLAN before the user can login and receive the dynamic VLAN assignment. So you must set the lease for the DHCP address in the static VLAN very low. Then the station will automatically renew its address soon after it receives the dynamic assignment.

**Note**

You must enable dynamic VLANs in the WLAN to which users connect for this setting to take effect. See “Enabling Authentication to the Internal Server on a WLAN” on page 11-33.

5. Specify the times of day when users in this group can connect to the wireless network.
   a. In the **Time of Access Start** field, enter the earliest time that users can connect.
   b. In the **Time Access End** field, enter the latest time users can connect.

Always enter times in four digits, the first two digits being the hour in the 24-hour clock and the second two digits being the minutes.

If a user is already logged in, and the end access time passes, the user remains logged in. However, the next time the user’s station re-authenticates, the re-authentication fails. You can require period re-authentication in the WLAN’s RADIUS settings. See “Enabling Authentication to the Internal Server on a WLAN” on page 11-33.

As shown in Figure 11-5, by default, users can connect at any time of the day or night.

6. In the **Time of access in days** section, check the boxes to specify the days of the week when users in this group can connect to the wireless network.

   By default, network access is available every day.

7. Click the **OK** button.

For more information about managing groups, see “Creating a Group” on page 11-12.

**Specifying a Domain Proxy RADIUS Server**

The Wireless Edge Services xl Module’s internal RADIUS server can query external RADIUS servers to authenticate users in a different domain.

To specify the proxy RADIUS server, complete these steps:

1. Select **Network Setup > Local RADIUS Server > Configuration**.
2. In the lower section of the screen, click the Domain Proxy Servers tab.
3. Click the Add button. The ADD screen is displayed.
4. In the **Realm Name** field, enter the domain name for users who authenticate to the domain proxy server.

When a user submits his or her username, the Wireless Edge Services xl Module's internal server checks the domain name. If this name matches the name in the **Realm Name** field, the internal RADIUS server queries the proxy server specified below.

For example, you enter “procurve.com” in the **Realm Name** field. If a user enters “Joe” as his username, the internal RADIUS server uses its local database to authenticate him. If the user enters “Joe@procurve.com,” the internal server uses the proxy server to authenticate Joe.

The internal RADIUS sends the username to the proxy server with the full domain extension.

The domain name can be up to 50 alphanumeric and special characters.

5. In the **IP Address** and **Port Number** fields, specify the external RADIUS server's IP address and port. The default port for RADIUS is 1812.

6. In the **Shared Secret** field, enter a string, which can include up to 31 alphanumeric and special characters.

The Wireless Edge Services xl Module must be configured as a RADIUS client on the external RADIUS server, and the client configuration must include this exact shared secret.

7. Click the **OK** button.

The external RADIUS server is now displayed in the **Domain Proxy Servers** section.
8. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

**Specifying Global RADIUS Settings**

Global RADIUS settings regulate the Wireless Edge Services xl Module's RADIUS server’s communications with proxy RADIUS servers.

To configure these settings, follow these steps:

1. Select **Network Setup > Local RADIUS Server > Configuration**.

2. In the **Timeout** field, specify how long, in seconds, the module should wait for a response to a request to a domain proxy server.

   The default timeout is 5 seconds, and the valid range is from 5 to 10 seconds. You might select a longer time for a busy network.
3. In the Retries field, specify the number of times the module should re-send a proxy request that times out.

   The default number of retries is 3 (which means that the module will send up to four requests). Valid values are from 3 to 6.

4. Click the OK button to apply the settings, remembering to save your configuration by clicking the Save link.

Adding RADIUS Clients

The Wireless Edge Services xl Module’s internal RADIUS server typically authenticates wireless users connecting to its own WLANs. But it can also authenticate users throughout your network—on both the wireless and the wired side. Simply add the NASs for those users as RADIUS clients. For example, you can add a ProCurve Intelligent Edge Switch, or you can add another Wireless Edge Services xl Module.

To specify a RADIUS client, complete these steps:

1. Select Network Setup > Local RADIUS Server > Configuration.

2. In the lower section of the screen, click the Clients tab.

3. Click the Add button. The ADD screen is displayed.

4. In the IP Address/Mask fields, enter the client device’s IP address, including the CIDR prefix length for its subnetwork.

   If you specify a subnetwork address and prefix length, any device in that subnetwork can act as a RADIUS client (as long as it sends the correct password, specified in step 5). For example, you specify 10.4.10.0/24. NASs with IP addresses 10.4.10.10 and 10.4.10.120 can both contact the Wireless Edge Services xl Module’s RADIUS server.
If the client has more than one IP address, make sure to specify the address that it includes in RADIUS requests.

5. In the Shared Secret field, enter the client’s password.
   Of course, you must specify this same password when you configure the client device to query this module.

6. Click the OK button. The client is displayed in the Network Setup > Radius Server > Configuration screen under the Clients tab.

7. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

Starting and Stopping the RADIUS Server

You must restart the RADIUS server for configuration changes to take effect. The Web browser interface automatically asks you to restart the server whenever you make a configuration. You can also manually stop and start the server from the Network Setup > Radius Server > Configuration screen.

The Global Settings section indicates whether the server is running:

- “Start the RADIUS server”—The server is currently disabled.
- “Stop the RADIUS server”—The server is currently enabled.

To change the RADIUS server’s status, click link portion of the indication. To disable the server, click the Stop link. To re-enable a stopped server, click the Start link.

In either case, a screen is displayed, informing you of the change in status.

Click the OK button to close the screen, remembering to save your configuration by clicking the Save link.
RADIUS Server

RADIUS Authentication

Enabling Authentication to the Internal Server on a WLAN

WLANs that use the following authentication methods require authentication to a RADIUS server:

- 802.1X
- Web-Auth
- MAC Authentication

In *Chapter 4: Wireless Local Area Networks (WLANs)*, you learned how to configure a WLAN to require authentication to an external RADIUS server.

This section explains how to configure the Wireless Edge Services xl Module’s internal RADIUS server to take over authentication.

You must enter 127.0.0.1 for the RADIUS server’s IP address. You do not enter a shared secret.

**Note**

You can enter the module’s management interface IP address instead of its loopback address (127.0.0.1). However, this option adds complexity because you must then add the management interface address as a client. (See “Adding RADIUS Clients” on page 11-31.) Also, if you choose this option, you must set a shared secret in the WLAN’s RADIUS server settings, and you must match the client’s shared secret to that secret.

To configure 802.1X authentication to the internal RADIUS server, complete these steps:

1. Select **Network Setup > WLAN Setup > Configuration**.
2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.
3. If you have configured the RADIUS server to place users in dynamic VLANs, check the **Dynamic Assignment** box.

4. Configure other WLAN settings as described in Chapter 4: Wireless Local Area Networks (WLANs).

5. In the **Authentication** section, select **802.1X EAP**, **Web-Auth**, or **MAC Authentication**.

6. Click the **RADIUS Config**… button at the bottom of the screen. The **Radius Configuration** screen is displayed.
7. Specify 127.0.0.1 in the primary RADIUS server's RADIUS Server Address field.

8. Do not enter anything in the RADIUS Shared Secret field.

By default, the module can communicate with the internal server. If you enter a string in this field, the module's internal server will no longer work on this WLAN. If you do change the secret, you can fix the problem in one of two ways:

- Clear the RADIUS Shared Secret field and click OK. The secret returns to the default.
- Configure the loopback interface (127.0.0.1) as a client for the internal RADIUS server. Specify the new secret for the client. See “Adding RADIUS Clients” on page 11-31.
9. If you want the module’s RADIUS server to periodically re-authenticate stations, check the **Re-authentication** box. Then specify how often (in seconds) stations re-authenticate in the **Re-authentication Period** field.

   The valid range for the re-authentication period is 30 to 65535 seconds (about 18 hours). The default setting is 3600 seconds (1 hour).

10. Choose **CHAP** or **PAP** for the **Authentication Protocol**.

    This setting determines how the Wireless Edge Services xl Module forwards MAC authentication or Web-Auth credentials to an external server. The module’s internal RADIUS server supports both protocols. However, if you choose PAP, users’ passwords display in plaintext in logs. Generally, you should choose CHAP for higher security.

11. Click the **OK** button.

12. On the **Edit** screen, click the **OK** button.

13. Click the **Save** link at the top of the Web browser interface to save the changes to the startup-config.

---

**RADIUS Accounting**

RADIUS accounting tracks users’ activity and consumption of network resources. NASs, such as the Wireless Edge Services xl Module, send reports that summarize users’ activity to a centralized RADIUS accounting server. A company might analyze the reports for security auditing and traffic management. Or the company might submit the reports to a billing server in order to charge users for wireless access.

The Wireless Edge Services xl Module can implement RADIUS accounting in one of two ways:

- It can report to an external RADIUS server.
- It can report to its internal RADIUS server.

The module can send the following messages:

- **Stop messages**—when a station disconnects from a wireless LAN (WLAN)
- **Start messages**—when a station connects to a WLAN
- **Interim messages**—at set intervals throughout the station’s session

You choose which messages the module sends.
A message includes information such as the identity of the user, the duration of the session, and the bandwidth consumed. Table 11-4 shows a complete list of fields in the report. Some fields are present in all messages; others are specific to certain types of messages.

Table 11-4. Information in a RADIUS Accounting Log

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>User-Name</td>
<td>user’s username</td>
</tr>
<tr>
<td>Acct-Status-Type</td>
<td>state of connection and type of message—start, stop, or interim</td>
</tr>
<tr>
<td>Acct-Session-ID</td>
<td>unique ID for each session</td>
</tr>
<tr>
<td>Calling-Station-ID</td>
<td>station’s MAC address</td>
</tr>
<tr>
<td>Called-Station-ID</td>
<td>MAC address of the port to which the station connects—for a wireless connection, the radio’s MAC address</td>
</tr>
<tr>
<td>NAS-Port</td>
<td>ID of the NAS’s port—for example, the port number on a switch</td>
</tr>
<tr>
<td>NAS-Port-Type</td>
<td>the type of connection—for example Wireless 802.11</td>
</tr>
<tr>
<td>NAS-IP-Identifier</td>
<td>NAS’s IP address—when the module is the NAS, 127.0.0.1</td>
</tr>
<tr>
<td>NAS-Identifier</td>
<td>NAS’s hostname</td>
</tr>
<tr>
<td>Event-Timestamp</td>
<td>date and time (including timezone) at which the event that triggered the message occurred</td>
</tr>
<tr>
<td>Acct-Delay-Time</td>
<td>specifies how long the RADIUS client has attempted to transmit the message</td>
</tr>
<tr>
<td>Acct-Authentic</td>
<td>the method by which the station authenticated</td>
</tr>
<tr>
<td>Client-IP-Address</td>
<td>IP address of the RADIUS client (typically the NAS, but sometimes another RADIUS server) that forwarded this message</td>
</tr>
<tr>
<td>Acct-Unique-Session-Id</td>
<td>a value that identifies the station’s session; all messages for a particular session have the same ID</td>
</tr>
<tr>
<td>Timestamp</td>
<td>message’s timestamp</td>
</tr>
<tr>
<td>Acct-Input-Packets</td>
<td>• number of packets received by the station over the entire duration of the session (stop message)</td>
</tr>
<tr>
<td></td>
<td>• number of packets received by the station since the beginning of the session (interim message)</td>
</tr>
</tbody>
</table>
Enabling Accounting to the Internal RADIUS Server on a WLAN

To activate accounting to the internal RADIUS server, follow these steps:

1. Select **Network Setup > WLAN Setup > Configuration.**
2. Select the WLAN from the list and click the **Edit** button. The **Edit** screen for the WLAN is displayed.

### Field Meanings

<table>
<thead>
<tr>
<th>Field</th>
<th>Meaning</th>
</tr>
</thead>
</table>
| Acct-Output-Packets    | • number of packets sent by the station over the entire duration of the session (stop message)  
                          |   • number of packets sent by the station since the beginning of the session (interim message) |
| Acct-Input-Octets      | • number of bytes received by the station over the entire duration of the session (stop message)  
                          |   • number of bytes received by the station since the beginning of the session (interim message) |
| Acct-Output-Octets     | • number of bytes sent by the station over the entire duration of the session (stop message)  
                          |   • number of bytes sent by the station since the beginning of the session (interim message) |
| Acct-Terminate-Cause   | the reason that the station’s session ended (stop messages only)—for example, the user might log off (User-Request) or the session might time out due to inactivity |
3. In the **Advanced** section, in the **Accounting Mode** field, use the drop-down menu to select **Radius**.

4. Click the **Radius Config** button. The **Radius Configuration** screen is displayed.
To enforce RADIUS accounting, the WLAN must use 802.1X authentication, Web-Auth, or MAC authentication for the Authentication mode.

5. Configure settings for the primary accounting server in the Primary column of the Accounting section.
   a. Specify the server’s IP address in the Accounting Server Address field.
      To use the Wireless Edge Services xl Module’s internal server for accounting, enter 127.0.0.1. You can use the internal RADIUS server for accounting both when the internal RADIUS server is the authentication server and when an external server is the authentication server.
   b. Leave the default port: 1813.
c. You should not specify a key when you use the module's internal server. If you have already specified a key, erase the Accounting Shared Secret field.

6. Optionally, configure settings for a secondary server by completing the fields in the Secondary column of the Accounting section.

7. From the Accounting Mode drop-down menu, choose when the Wireless Edge Services xl Module forwards a message to its internal server:
   - Start-Stop—when a station connects to this WLAN and when it disconnects
   - Stop-Only—only when a station disconnects
   - Start-Interim-Stop—when a station connects to this WLAN, periodically for as long as the connection persists, and when the station closes the connection

8. If you have selected Start-Interim-Stop for the Accounting Mode, enter a value in the Interval field.
   This setting determines how often, in seconds, the module sends periodic reports on user activities. (It applies only when you select Start-Interim-Stop.) The default value is 60 seconds, and the valid range is from 60 to 3600 seconds (1 hour).

9. Click the OK button.

10. In the WLAN’s Edit screen, click the OK button.

11. Click the Save link at the top of the Web browser interface to save the changes to the startup-config.

Viewing the Internal RADIUS Server’s Accounting Logs

When you set up RADIUS accounting to the Wireless Edge Services xl Module’s internal server, the module stores messages about user activity as accounting logs. The directory for the logs is flash:/log/radius.

To view the log file in the Web browser interface, select Network Setup > Local RADIUS Server and click the Accounting Logs tab.
The panel at the left of the screen shows the directories in the main RADIUS accounting directory (flash:/log/radius). By default, RADIUS reports are logged to the radacct directory, which you can see in Figure 11-20. Double-click the directory name to view log files within the directory.
The screen displays the following information for each log file:

- **Filename**—accounting.log, for the default file
- **Type**—Log, for logged reports
- **Size**—the size of the file in bytes

A log file might include multiple RADIUS accounting messages. As the Wireless Edge Services xi Module’s internal RADIUS server receives the messages, it adds them to the log file.

The **Network Setup > Local RADIUS Server > Accounting Logs** screen shows log file names; it does not show information contained within a file. To actually view the logged messages, you must export the log file: select the file and click the **Transfer Files** button. You can transfer the file to an FTP or TFTP server and from that server to a billing or auditing server. You can also open the file in a text editor or word processor and view the logged messages.
Note

The module only creates accounting logs for its own activities as RADIUS server if you specifically enable RADIUS accounting to the internal server on a WLAN. See “Enabling Accounting to the Internal RADIUS Server on a WLAN” on page 11-38.