Tech Note 150

Configuring a PowerDsine Midspan

With

Cisco ACS RADIUS Server (v4.2)

Revision 1.1
Catalog Number 06-0034-81

Introduction

This paper describes the procedures to be followed when using a Cisco ACS RADIUS server (v4.2) to configure access to a Midspan device. Remote Authentication Dial In User Service (RADIUS) is a networking protocol that provides centralized access management for computers to connect to and use Midspan devices.

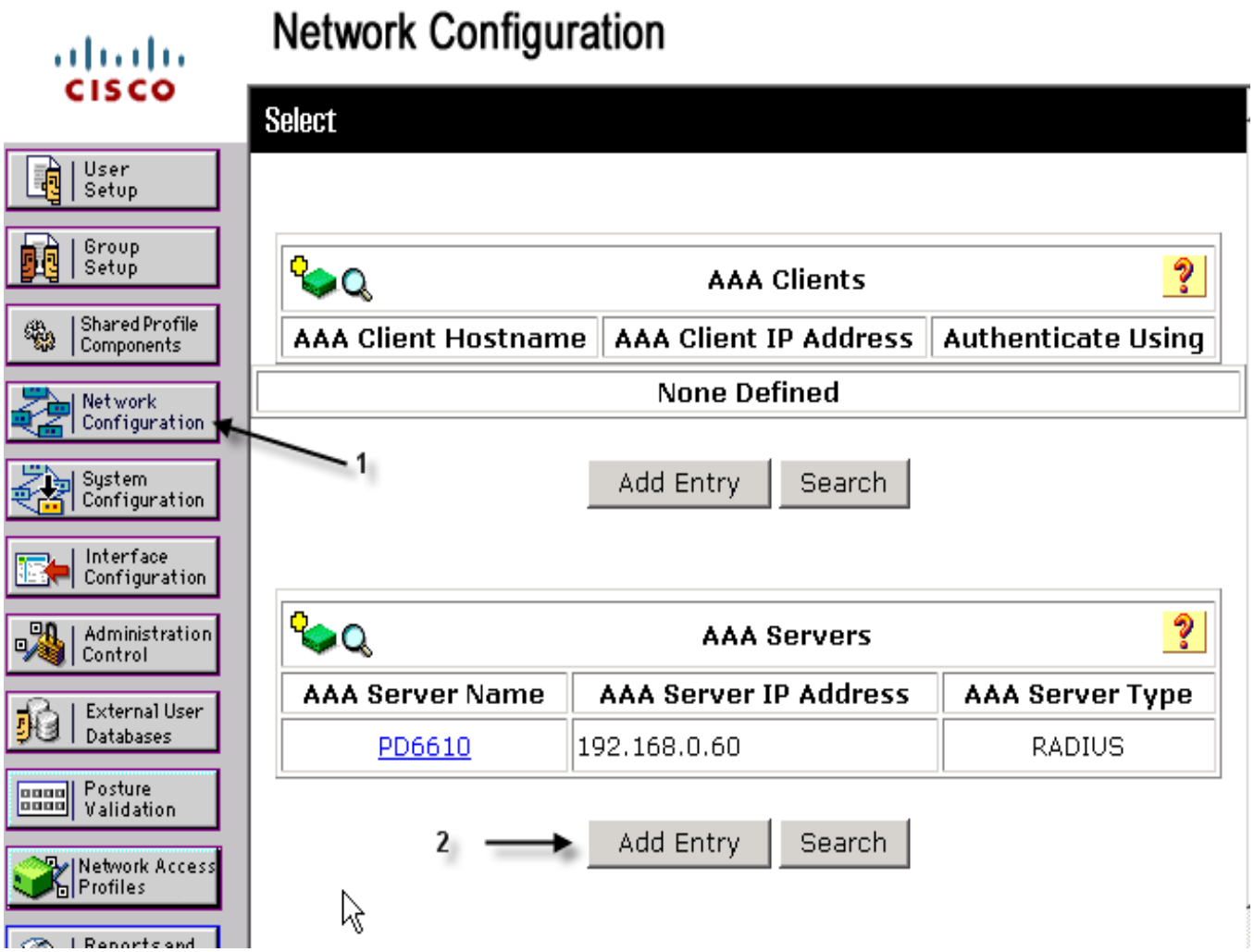
Configuration consists of:

- Defining the Radius AAA Server
- Defining the RADIUS AAA Client
- Defining the User Access Level
- Enabling Midspan Radius Authentication

Defining the Radius AAA Server

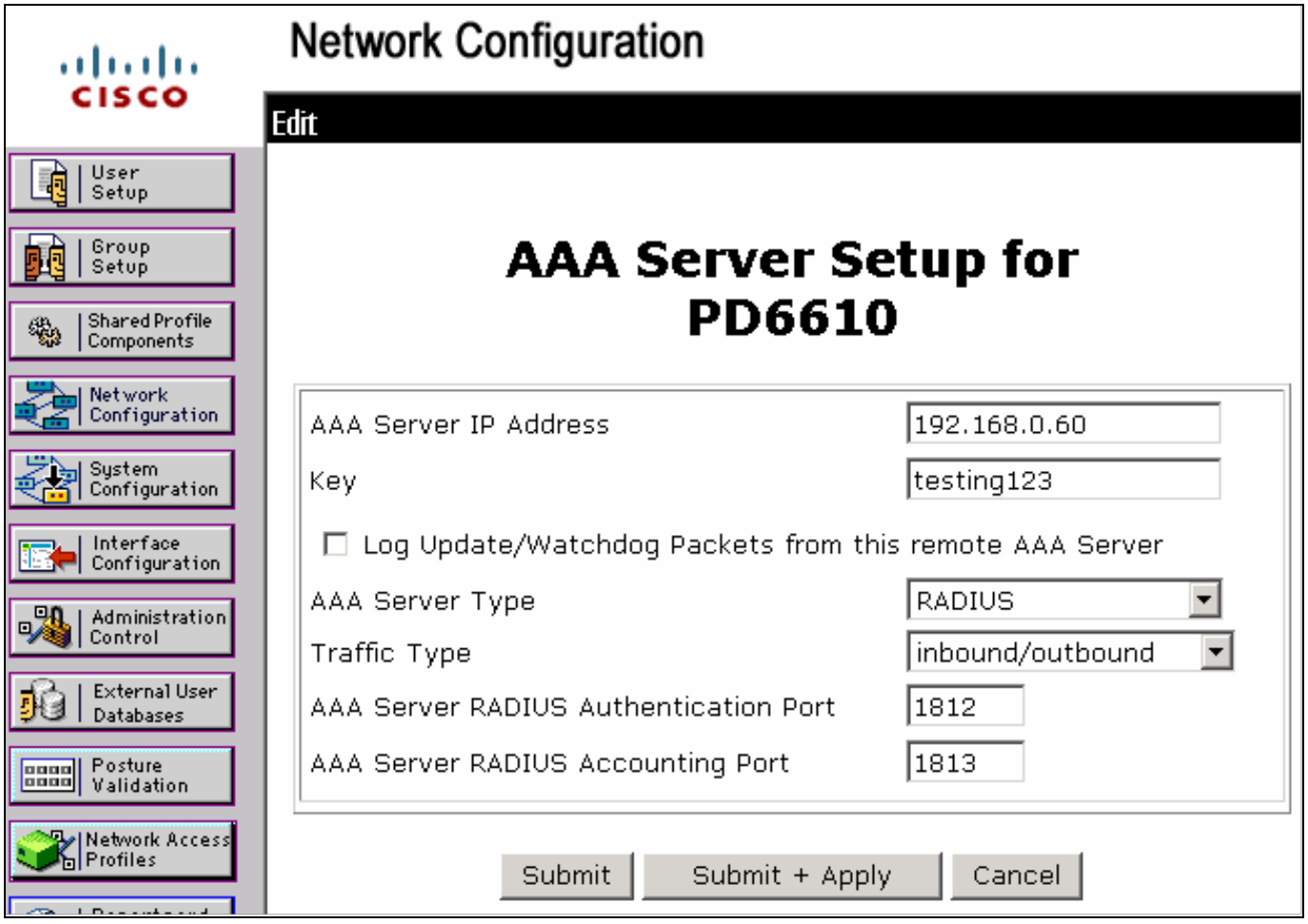
All servers must be must be added to Cisco ACS *AAA Servers* list

1. In the ACS RADIUS software, click **Network Configuration**.
2. Select an AAA Server.
3. Click Add Entry.
4. The AAA Server Setup dialog box appears.



5. Enter the following Radius Server information:
   - **AAA Server IP Address**: Radius Server IP address.
   - **Key**: Shared Secret string. Thus string must match Midspan shared secret string.
   - **AAA Server Type**: RADIUS.
   - **Traffic Type**: Select inbound/outbound from the drop-down list.
   - **AAA Server RADIUS Authentication Port**: Type **1812**. This number must match the Midspan Authentication UDP port.
   - **AAA Server RADIUS Accounting Port**: Type **1813**. This number must match the Midspan Accounting UDP port.
6. Click **Submit + Apply**.

   The server is defined

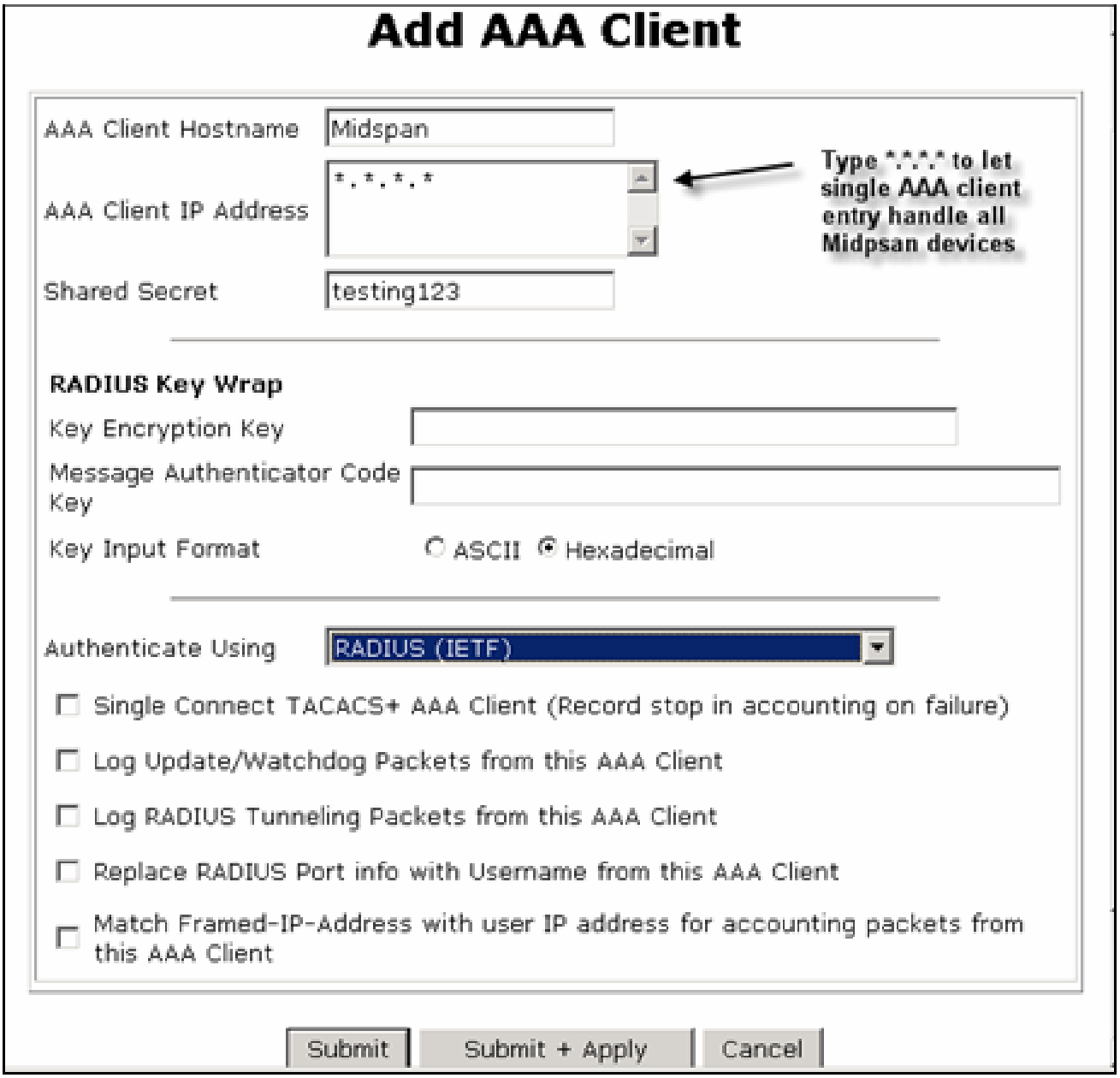


Defining the RADIUS AAA Client

All Midspan devices which were configured to use Radius Authentication must be added to Cisco ACS *AAA Clients* list

1. In the ACS RADIUS software, type the following AAA Client information:
   - **AAA Client Hostname**: Any string which describes your client type.
   - **AAA Client IP Address**: *.*.*.* Enables handling all Midspan devices via a single AAA client.
   - **Shared Secret**: Must match Midspan shared secret string.
2. Click **Submit + Apply.**

The client is defined



Microsemi
Analog Mixed Signal Group
1 Enterprise, Aliso Viejo, CA 92656, USA; Within the USA: (800) 713-4113, Outside the USA: (949) 221-7100 Fax: (949) 756-0308

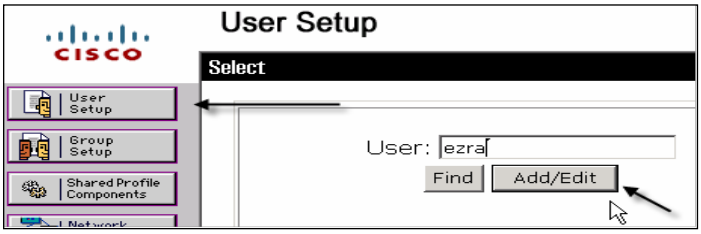
User Access Level

A remote user can have one of two access levels:

- View access level
- Configuration access level

Defining a Remote User with View Access Level

This procedure defines how to configure View access level. A remote user with View access level can only view sections under Telnet/SSH/Web (as view-status Web Page).



1. Click **User-Setup**.
2. In the User field, type the user name.
3. Click **Add/Edit**.

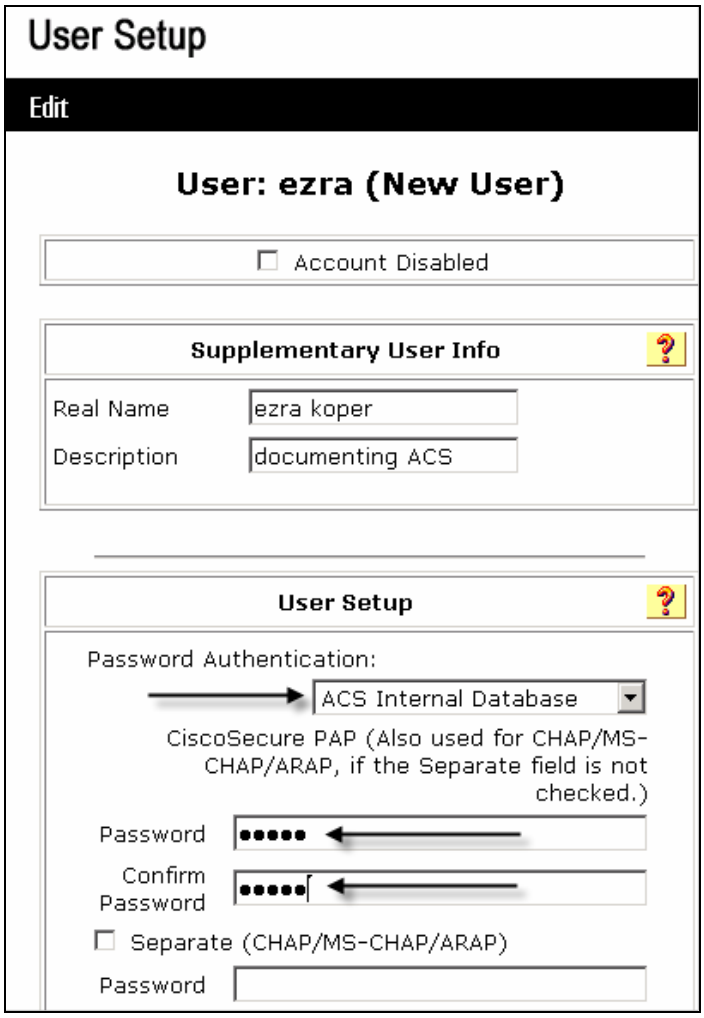
The User Setup dialog box appears.

4. Enter the following information:
   - **Real Name**: Type any string.
   - **Description**: Type any string.
   - **Password Authentication**: Select ACS Internal Database from the drop down list.

   Note: This step is only done where no external data base is in use.

   - **Password**: Type the remote user password.
   - **Confirm Password**: Type the remote user password.
5. Click **Submit**.

   The user has been defined as having view access level only.



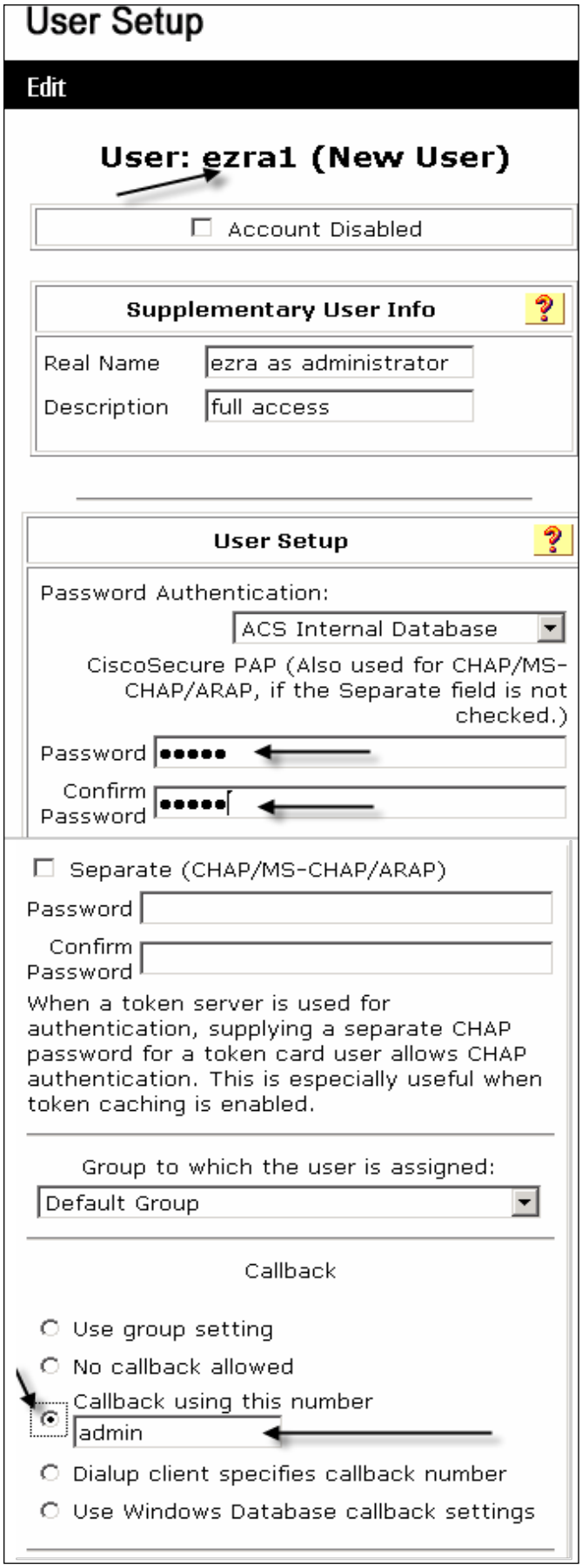
Microsemi
Analog Mixed Signal Group
1 Enterprise, Aliso Viejo, CA 92656, USA; Within the USA: (800) 713-4113, Outside the USA: (949) 221-7100 Fax: (949) 756-0308

Defining a Remote User with Configuration Access Level

A remote user with Configuration access level has full access to all Telnet/SSH/Web sections.

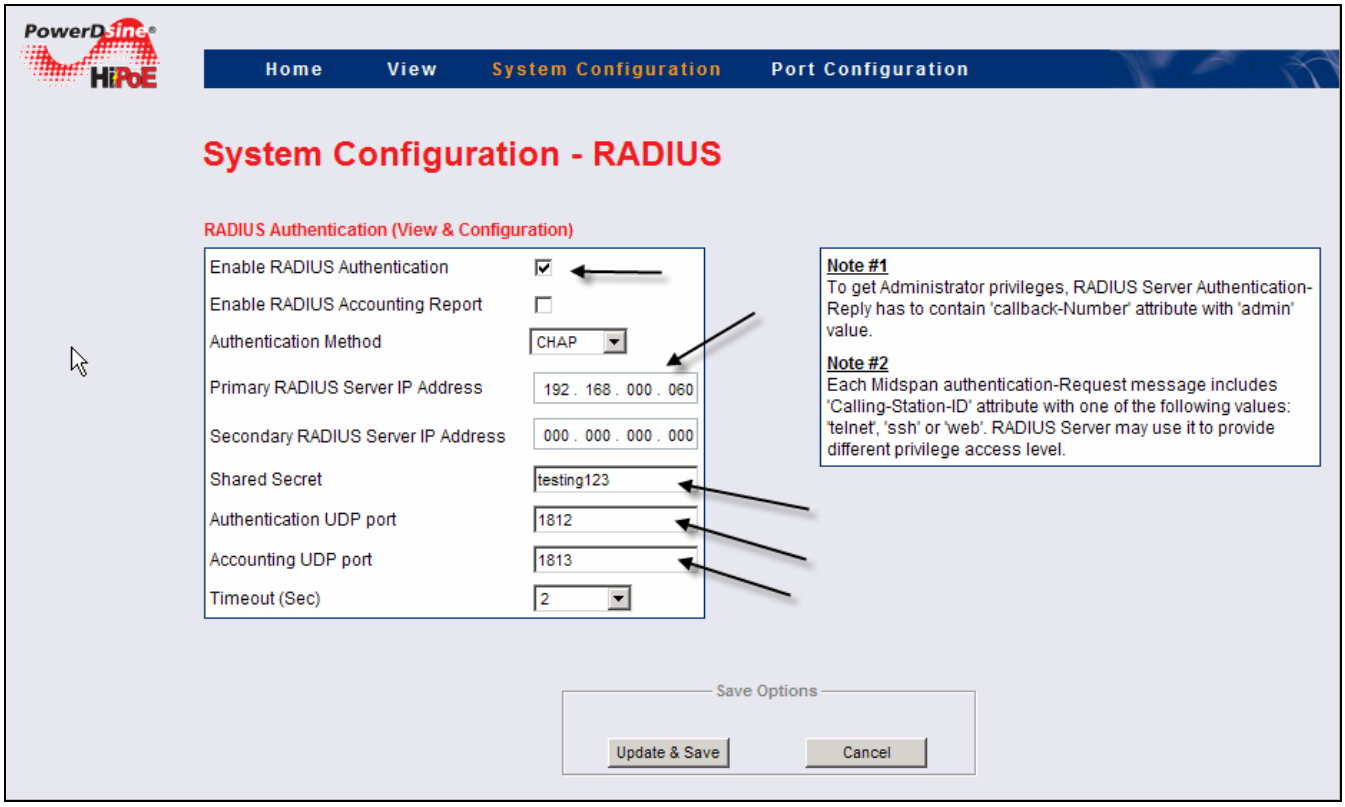
1. Click **User-Setup**.
2. In the User field, type the user name.
3. Click **Add/Edit**.
4. Enter the following information:
   - **Real Name**: Free text.
   - **Description**: Free text.
   - **Password Authentication**: Select **ACS Internal Database** from the drop down list (in case no external data base is in use).
   - **Password**: Type the remote user password.
   - **Confirm Password**: Type the remote user password
5. Under Callback, select **Callback using this number**.
6. In the field below, type *admin* as the callback number.
7. Click Submit.

   The user has been defined as having configuration access level.



Enabling Midspan Radius Authentication

1. In a web browser, type the device IP address to access the Midspan Radius Configuration Web page.
2. Fill in the following fields:
   - **Mark** Enable Radius Authentication.
   - **Authentication Method**: CHAP.
   - **Primary Radius Server IP Address**: Cisco ACS Server IP Address.
   - **Shared Secret**: Must match the same shared secret as defined in Cisco ACS Server (see Step #1 and Step #2).
   - **Authentication UDP Port**: Must match the Authentication UDP port entered in Step #1.
   - **Accounting UDP Port**: Must match the Accounting UDP ports entered in Step #1.
3. Click **Update & Save**.



Revision History

Revision Level / Date	Para. Affected	Description
Rev 1.0		Release
Rev 1.1 / 4-Nov-11	Entire Document	Formatting

For support contact: customer.care_AMSG@microsemi.com

Visit our web site at: www.microsemi.com/powerdsine

Catalog Number: 06-0034-081