



# ZipDial Service with Microsoft® RADIUS on Windows NT 4.0 Server

*Last Revised: 06/09/99  
Written and compiled by Lawrence Bates (lbates@ziplink.net).*

## ZipLink ZipDial

ZipDial is ZipLink's fast and affordable wholesale dial-up network solution for ISPs looking to expand their national footprint, or companies who need to provide remote network access to a large number of employees.

Through ZipLink's own high-availability, high-speed nationwide backbone and dial-up service, ZipDial is the wholesale partnership that quickly allows you to take full advantage of our infrastructure and transparently connect your users to the Internet.

For more information on ZipLink's ZipDial Service, please refer to the ZipDial web pages at <http://www.ziplink.net/zipdial>

**Note: Comment entries in this document discuss configuration information specific to the ZipDial service.**

## Using Microsoft® RADIUS on Windows NT 4.0 Server

If you are familiar with Microsoft® Windows NT Server 4.0 you may have already upgraded your server with the **Windows NT 4.0 Option Pack**. If so, then you have the core components needed to successfully authenticate using the Remote Authentication Dial-In User Server protocol (RADIUS). This allows you to successfully authenticate the users in your NT domain database with ZipLink's RADIUS servers, allowing your users access to ZipLink's network.

If you have not installed the NT 4.0 Option Pack and wish to use Microsoft's RADIUS, you can obtain it from the following sources:

## Obtaining Microsoft RADIUS and Windows NT Server 4.0 Option Pack

Microsoft's implementation of Remote Authentication Dial-In User Server (RADIUS) is included on the **Windows NT Server 4.0 Option Pack**. The Option Pack can be obtained as a supplemental CD-ROM with the purchase of the **NT 4.0 Service Pack 4**, or as a download from Microsoft's Web site:

<http://www.microsoft.com/NTServer/all/downloads.asp>

The Option Pack includes **Internet Connection Services for Microsoft Remote Access Service (RAS)**, A collection of software applications designed to help corporations and Internet Service Providers (ISPs) build comprehensive Internet access solutions, including dial-up Virtual Private Networks (VPN).

Included in the Internet Connection Services for Microsoft RAS are a group of software components referred to as the **Internet Authentication Services (IAS)**. IAS provides a way for Internet Service Providers to control access to their service. IAS uses the RADIUS protocol to authenticate users and track how much time they spend online. IAS also lets Internet Service Providers control which areas of the network their individual subscribers can access.

## Installation and Configuration of Windows NT Server 4.0 Option Pack

Microsoft recommends that you install your server software in the following order for best results with Windows NT 4.0 Option Pack:

<u>Component:</u>	<u>Location:</u>
1. Windows NT Server 4.0	Windows NT Server CD
2. Windows NT 4.0 Service Pack 3	Option Pack CD
3. Microsoft Internet Explorer 4.01	Service Pack 4 CD
4. Windows NT 4.0 Option Pack	Option Pack CD
5. Windows NT 4.0 Service Pack 4	Service Pack 4 CD

## **Notes on configuring NT 4.0 Server for use with Microsoft RADIUS and ZipLink's ZipDial Service**

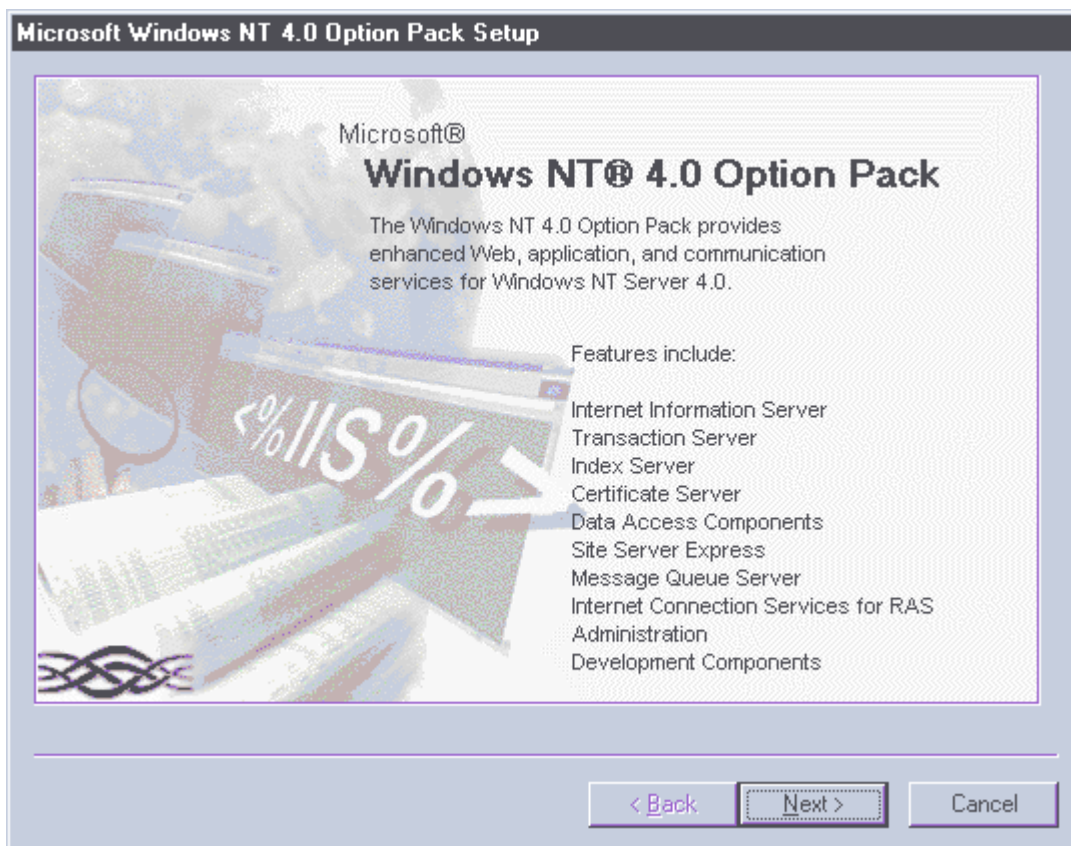
- It is important that you set up your NT Server as a **Domain Controller** during NT installation. Microsoft's RADIUS defaults to authenticating against the NT server's database of domain users. Users are added as regular NT domain users and reside in the default domain's user database.
- When you become a ZipDial customer, you are asked to fill out a **Proxy RADIUS (Realms) Set-Up Form**. On this form you are required to provide a realm name, normally in the format *username@realm*. You have the option to choose a configuration that strips the *@realm* suffix

from the username. Removing the *@realm* suffix before a RADIUS proxy request is sent to your server allows a ZipDial login to authenticate against the NT domain username. If you are using the default configuration, setting the Microsoft RADIUS service to authenticate against your NT server's domain database, **you must choose to strip the realm**.

- NT Domain users who authenticate using the RADIUS protocol must have the option for **Grant dialin permission to user** enabled. This is done when adding the user through the NT Administration Wizard or in the Dialin configuration section of the User Manager. It can also be set through the RAS Administration tool after an account has been created.

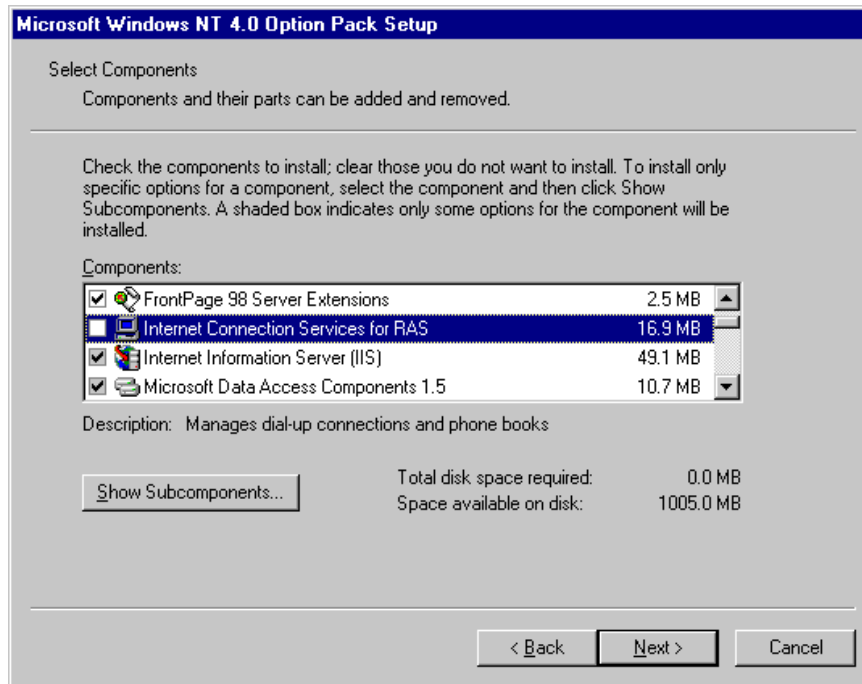
### **To Install Internet Authentication Services**

1. Start the Setup program for Microsoft Windows NT 4 Option Pack Master Setup compact disc.

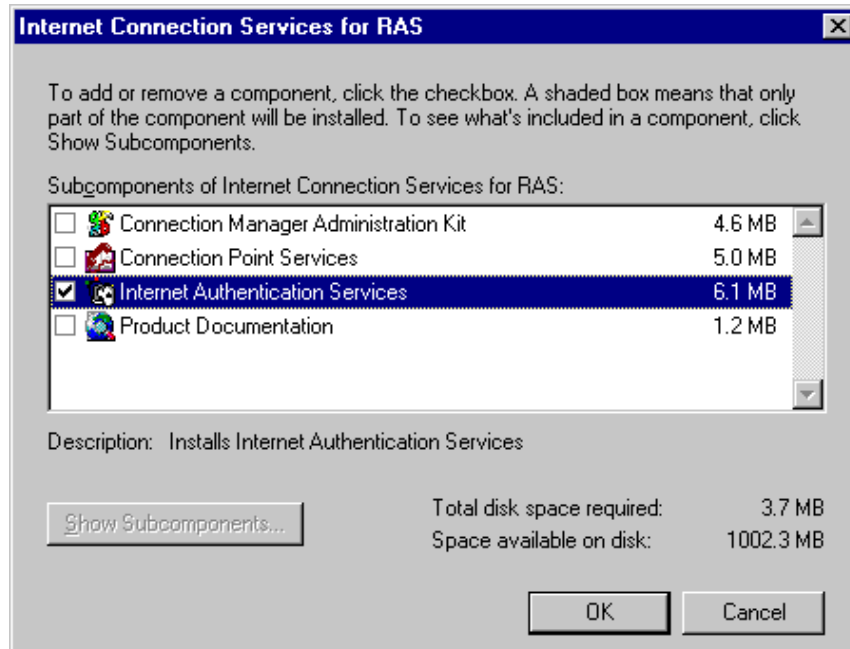


2. Read the license agreement, and if you accept it, click Accept.
3. When prompted, click **Custom**. (If you installed any part of Windows NT 4.0 Option Pack previously, click Add/Remove).

- In the **Select Components** dialog box, click **Internet Connection Services for RAS** in the list of components, then click **Show Subcomponents**,



Make sure that **Microsoft Internet Authentication Services** is selected. Then click **OK**.



When Setup is finished, click **OK** to restart your computer.

Once you have installed the Internet Authentication Services on your server, you will need to perform the following:

- **Start Internet Authentication Service**
- **Set authentication service properties.**

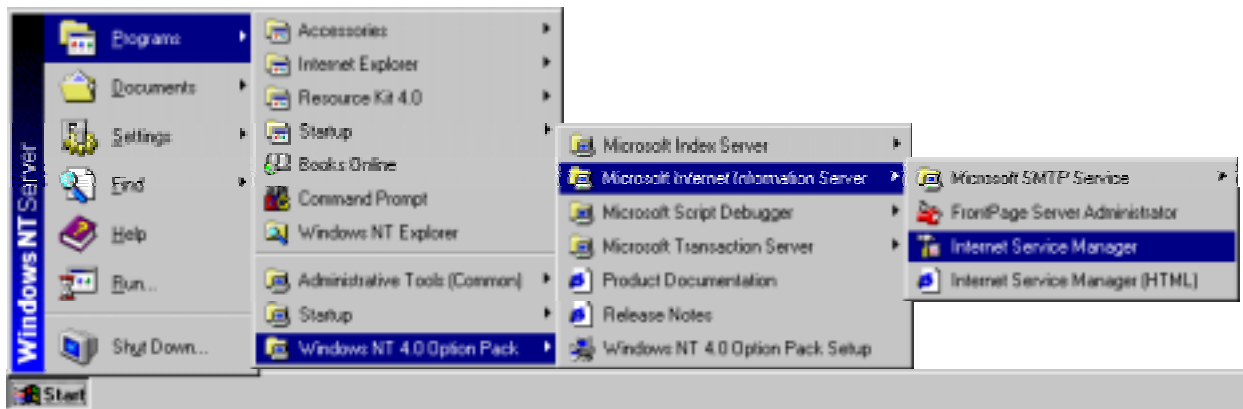
### Displaying Internet Authentication Service Properties

You access the administration user interface from Microsoft Management Console in Internet Information Server.

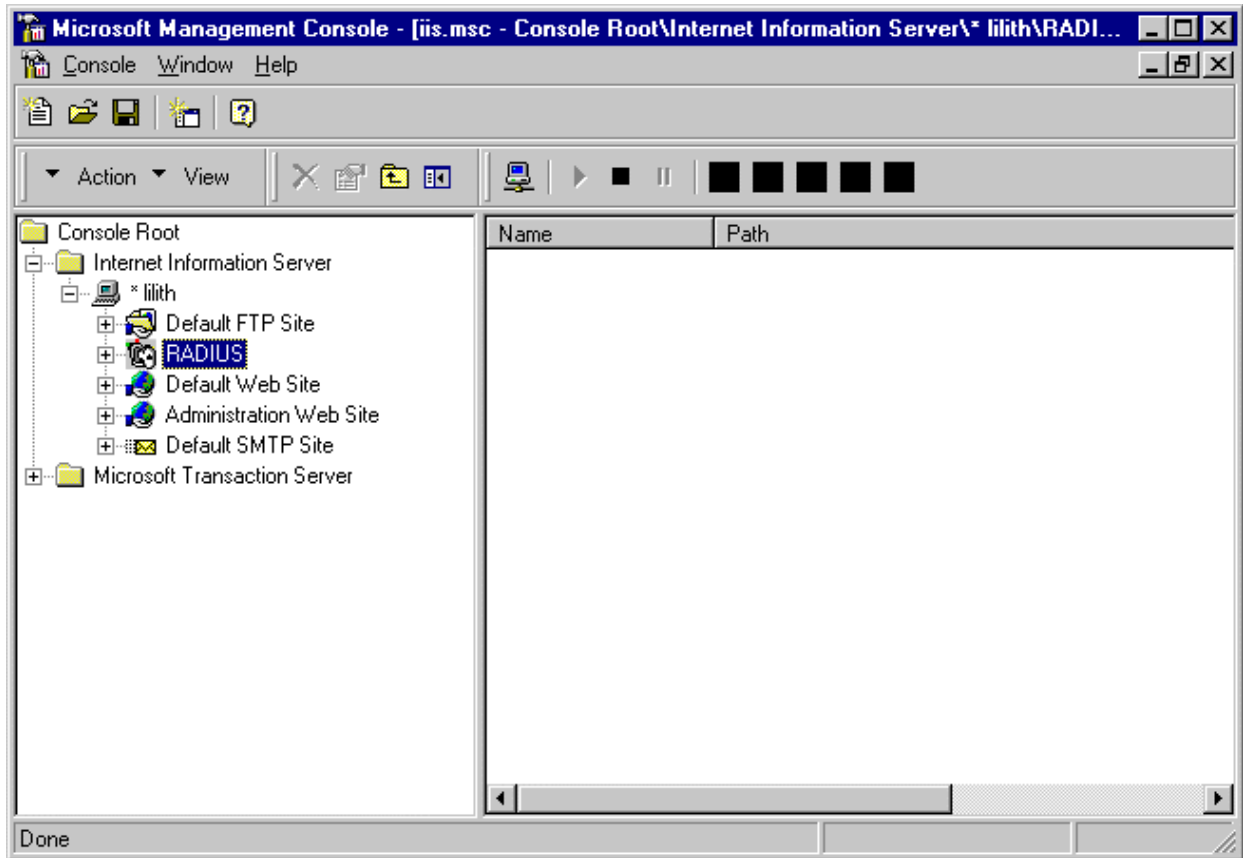
### To view Internet Authentication Service Properties

Click **Start**, point to **Programs**, and then point to **Windows NT 4.0 Option Pack**.

1. Click **Internet Information Server**, and then click **Internet Service Manager**. The system displays the Microsoft Management Console (MMC).



2. In the left pane, double-click **Console Root**. The tree expands and displays the IIS folder.
3. Double-click **IIS**. The tree expands and shows the name of your computer.
4. Double-click your computer name. The tree expands and shows RADIUS or IAS.



5. Right-click **RADIUS**, and then click **Properties**. Internet Authentication Services Properties appear

### Setting Internet Authentication Service Properties

The Service tab stores basic settings, including maximum threads, User Datagram Protocol (UDP) port numbers for RADIUS authentication and RADIUS accounting, and packet choices for capture to the Application Log window of the Windows NT Event Viewer.

1. Click the Service tab.
2. In the Maximum threads box, enter the maximum number of authentication requests that will be processed concurrently. This value must be between 1 and 63. (IAS will only use as many threads as necessary, up to the value of this setting.)
3. If your RADIUS authentication and RADIUS accounting UDP ports differ from the default values provided, enter your port setting in the Authentication and Accounting boxes. The default values are set to the commonly defined RADIUS standards (numbers represent Internet RFC): 1645 for authentication and 1646 for accounting. The most

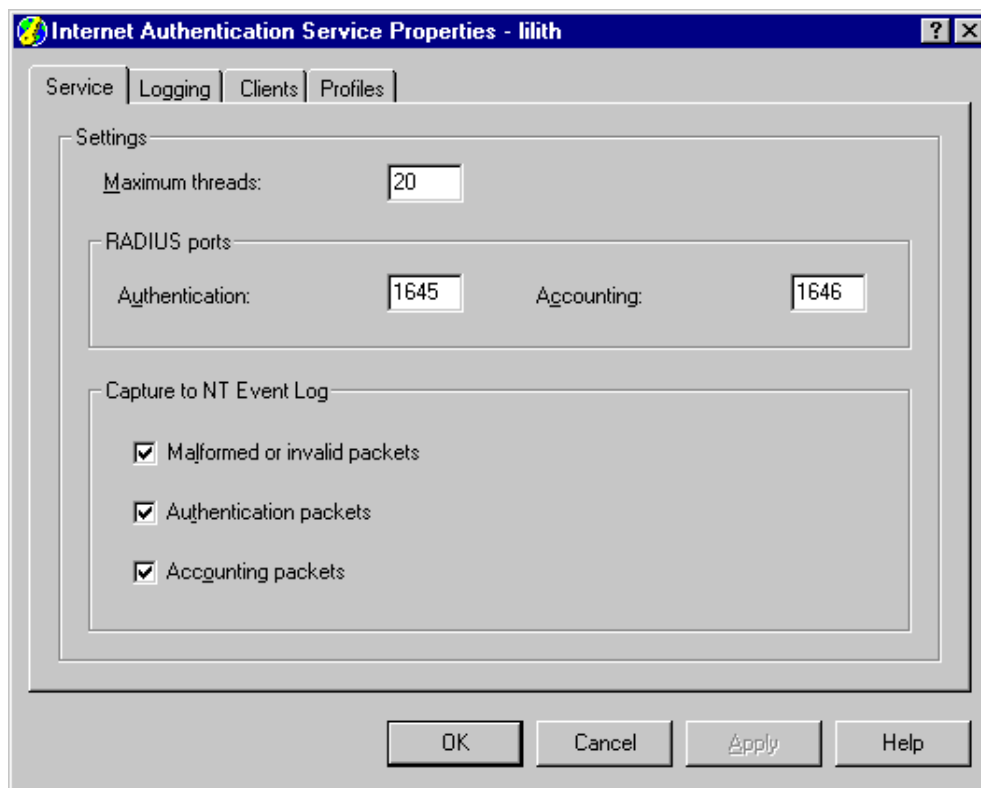
recently defined RADIUS standards at the time of this publication are 1812 for authentication and 1813 for accounting. If you are unsure of port settings, refer to your NAS documentation.

4. Select one or more check boxes under Capture to NT Event Log to capture packet traffic processed by IAS:

**ZipDial uses the commonly defined RADIUS ports: 1645 for authentication and 1646 for accounting.**

- Click **Malformed or invalid packets** to capture problematic packets. Packets are generally malformed as a result of password incompatibility between the client and the server.
- Click **Authentication packets** to capture authentication requests, access approvals, and access denials. This can help to alert you to problems with transaction volume and attempts to access unauthorized resources.
- Click **Accounting packets** to capture accounting requests, approvals, and denials. This can help to alert you to accounting-software compatibility problems between the NAS and IAS.

The information collected in the NT Event Viewer is valuable for evaluating server performance and for troubleshooting.



**Note:**

The default setting for the Windows NT event log is to reserve 512 kilobytes for the event log file. This may be insufficient if you are logging a significant amount of network traffic.

To log more traffic, click **Start**, point to **Administrative Tools**, and then click **Event Viewer**. Then, on the **Log** menu in **Event Viewer**, click **Log Settings**, and then change the Maximum Log Size setting.

To log only the most recent events, follow the same procedure, and then click **Overwrite events as needed**.

When viewing the event log using the Event Viewer, click **View** and then click **Refresh** to dynamically update the log entries.

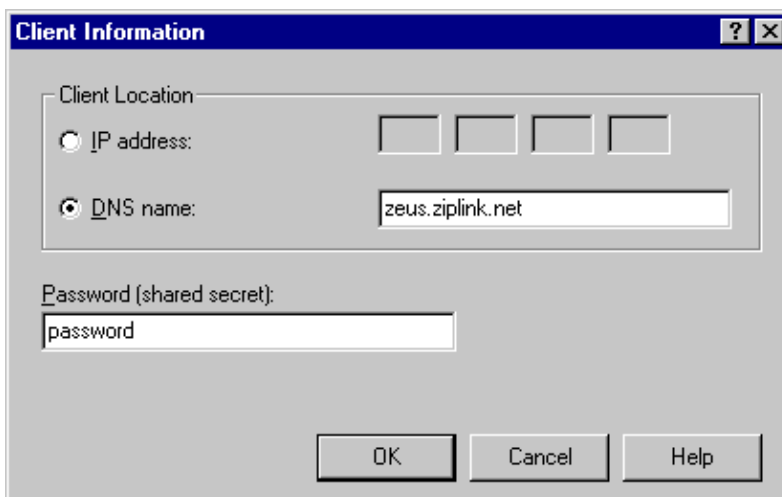
**Registering Clients of This Server**

The Clients tab allows you to add, remove, or edit the Internet addresses, DNS names, and passwords (also called *shared secrets*) of the clients of this IAS server. Clients can be NAS devices or RADIUS proxies.

**To register clients of this server:**

1. Click the **Clients** tab.
2. Click **Add**.
3. Click IP Address or DNS Name, and then enter the appropriate values.  
ZipLink ZipDial uses the following RADIUS servers for authentication:

DNS Name	IP Address
zeus.ziplink.net	206.15.168.72
athena.ziplink.net	206.15.158.137



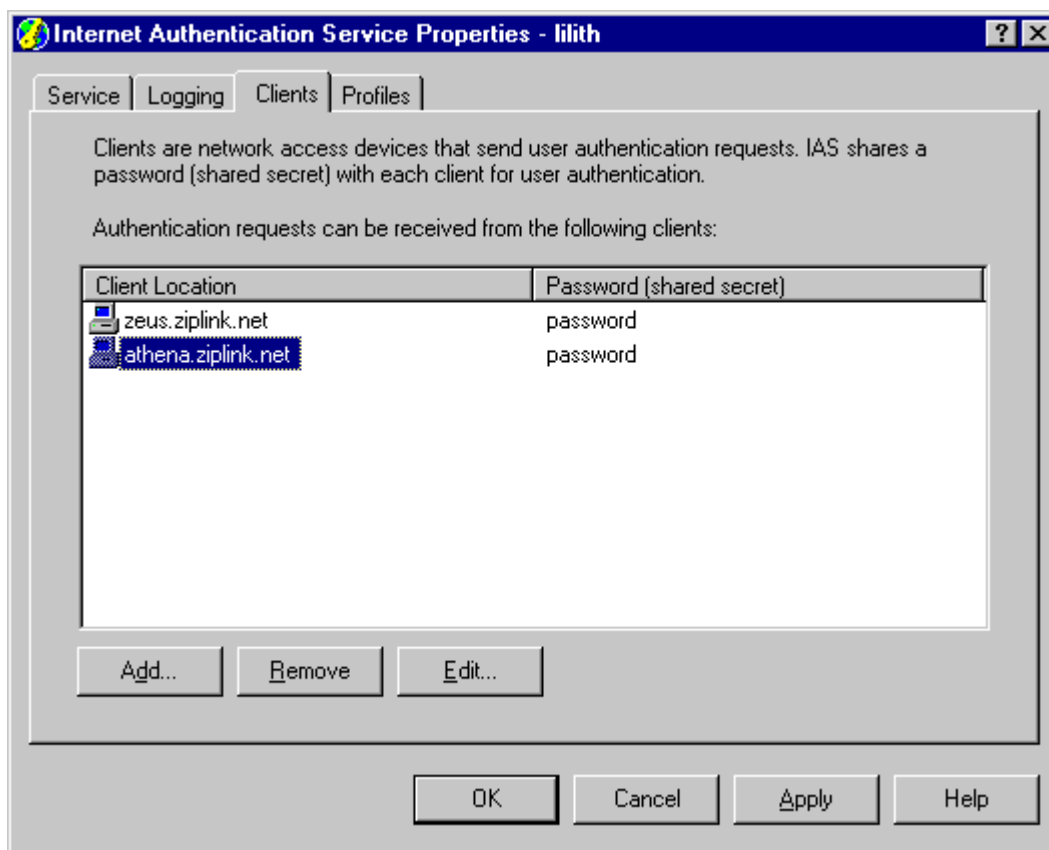
4. Enter the shared secret for the client in the **Password (shared secret)** box.

Your shared secret will be the password you chose on the [Proxy RADIUS \(Realms\) Set-Up Form](#)

**Note:**

Passwords (shared secrets) are case-sensitive. Be sure that the client's password (shared secret) and the password (shared secret) you enter in this field are identical to each other and conform with the password (shared secret) rules listed in "Deploying Internet Authentication Services."

5. Click **OK**, you should see either the client DNS Names or IP Addresses, depending on which entry you chose to configure, and the passwords (shared secrets) for each.



## Creating New or Using Existing RADIUS Profiles

The default RADIUS profiles set up during installation are correct profiles for use with ZipLink's ZipDial service. There is no need to create a custom RADIUS profile.

At this point you have successfully installed Microsoft's® RADIUS for use with ZipLink's ZipDial Service. Users entered using the NT Server Administrative Wizards will now be authenticated as valid ZipDial users.

*ZipLink makes reasonable efforts to ensure the information provided in this document is correct and up-to-date as of the last revision date. However, all information is provided "as is", and ZipLink makes no warranties as to its accuracy or completeness. ZipLink does not assume liability or responsibility for errors or omissions.*

*Portions of this document are ©Copyright 1998-99 by Microsoft, Inc. Microsoft, Windows NT, and all related product names mentioned herein are trademarks or registered trademarks of Microsoft. Portions of this document, especially information specific to ZipDial services, is ©Copyright 1999 by ZipLink, Inc. Information in this document may be copied, reproduced and/or distributed for personal or other non-commercial purposes only. Any commercial use or reproduction in whole or part in any form without prior written permission of Microsoft or ZipLink is prohibited.*