RASExpress™

# Radius Server User Guide

Title: MTSLOGOK.FH5
Creator: FreeHand 5.0
CreationDate: Fri Aug 23 16:39:51 19

Radius Server User Guide

P/N S000030C, Revision C



Multi-Tech Systems, Inc. makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Multi-Tech Systems, Inc. reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of Multi-Tech Systems, Inc., to notify any person or organization of such revisions or changes.

| Revision | Date | Description |
|---|---|---|
| A | 12/3/99 | Manual released for Radius Server 1.00. |
| B | 10/3/00 | Manual revised for Radius Server 1.10. |
| C | 09/24/02 | Manual revised to clarify using Windows NT Server for authentication. |



Multi-Tech Systems, Inc.
2205 Woodale Drive
Mounds View, Minnesota 55112
(763) 785-3500 or (800) 328-9717
Fax (763) 785-9874
Technical Support (800) 972-2439
Internet Address: http://www.multitech.com

# Software User License Agreement

Radius Server is licensed by Multi-Tech Systems, Inc., to the original end-user purchaser of the product, hereafter referred to as "Licensee." The License includes the distribution disc, other accompanying programs, and the documentation. The Radius Server software, hereafter referred to as "Software," consists of the computer program files included on the original distribution disc.

Licensee agrees that by purchase and/or use of the Software, he hereby accepts and agrees to the terms of this License Agreement.

In consideration of mutual covenants contained herein, and other good and valuable considerations, the receipt and sufficiency of which is acknowledged, Multi-Tech Systems, Inc. does hereby grant to the Licensee a non-transferable and non-exclusive license to use the Software and accompanying documentation on the following conditions and terms: The software is furnished to the Licensee for execution and use on a single computer system only and may be copied (with the inclusion of the Multi-Tech Systems, Inc. copyright notice) only for use on that computer system. The Licensee hereby agrees not to provide or otherwise make available any portion of this software in any form to any third party without the prior express written approval of Multi-Tech Systems, Inc.

Licensee is hereby informed that this Software contains confidential proprietary and valuable trade secrets developed by or licensed to Multi-Tech Systems, Inc. and agrees that sole ownership shall remain with Multi-Tech Systems, Inc.

The Software is copyrighted. Except as provided herein, the Software and documentation supplied under this agreement may not be copied, reproduced, published, licensed, sub-licensed, distributed, transferred, or made available in any form, in whole or in part, to others, without expressed written permission of Multi-Tech Systems, Inc. Copies of the Software may be made to replace worn or deteriorated copies for archival or backup procedures.

Licensee agrees to implement sufficient security measures to protect Multi-Tech Systems, Inc. proprietary interests and not to allow the use, copying or transfer by any means, other than in accordance with this agreement. Licensee agrees that any breach of this agreement will be damaging to Multi-Tech Systems, Inc.

Licensee agrees that all warranties, implied or otherwise, with regard to this Software, including all warranties of merchantability and fitness for any particular purpose are expressly waived, and no liability shall extend to any damages, including consequential damages, whether known to Multi-Tech Systems, Inc. It is hereby expressly agreed that Licensee's remedy is limited to replacement or refund of the license fee, at the option of Multi-Tech Systems, Inc., for defective distribution media. There is no warranty for misused materials.

This package contains a compact disc. Neither this software nor the accompanying documentation may be modified or translated without the written permission of Multi-Tech Systems, Inc.

This agreement shall be governed by the laws of the State of Minnesota. The terms and conditions of this agreement shall prevail regardless of the terms of any other submitted by the Licensee. This agreement supersedes any proposal or prior agreement. Licensee further agrees that this License Agreement is the complete and exclusive statement of Agreement, oral, written, or any other communications between Multi-Tech Systems, Inc. and Licensee relating to the subject matter of this agreement. This

agreement is not assignable without written permission of an authorized agent of Multi-Tech Systems, Inc.

# Table of Contents

## 1 Introduction



## 2 Installation and Configuration

# 1 Introduction

# Introduction

This manual describes how to install, configure, and manage Multi-Tech Radius Server.

Radius Server is Multi-Tech System's implementation of the Remote Access Dial In User Server (RADIUS) protocol. It is designed to be installed on and to work with Microsoft Windows NT Server, and to work with RASExpress remote access servers.

RADIUS uses a single authentication server to centralize security on networks with large modem pools, especially those with multiple communication servers. By replacing multiple user databases (one on each communication server) with a single, central, easily managed user database, it simplifies the management of user data while eliminating the security risk of multiple entry points.

# How Does Radius Server Work?

Radius Server uses a client / server approach, with one or more RASExpress servers acting as the clients of the RADIUS authentication server. Users are authenticated through the following series of exchanges between the RASExpress client and the RADIUS server.

1. The user dials in to a modem connected to a RASExpress server.
2. When the connection is established, RASExpress prompts the user for a user name and password.
3. RASExpress creates a data packet from this information called the authentication request. The packet identifies the RASExpress server sending the request, the port being used by the modem, and the user name and password. This information is encrypted with a shared secret password, which should *never* be sent over the network.
4. The data packet is sent over the LAN or WAN from the RASExpress server to the RADIUS server. If the RADIUS server is unavailable, RASExpress can route the data packet to a backup server.
5. Radius Server validates the request and compares the decrypted user name and password in the request to the contents of the Users file in the Radius Server folder.
6. If the user name and password are correct, Radius Server returns to the RASExpress server an authentication acknowledgement that includes encrypted information on the user's network and service requirements, which are stored with the user name and password in the Users file. If the user name or password is incorrect, Radius Server sends an authentication reject packet to the RASExpress server, and the user is denied access to the network.
7. If the RASExpress server receives an authentication acknowledgement, then it decrypts the information in it and uses it to deliver the specified network services to the user.

# Typographic Conventions

Certain typographic conventions have been adopted throughout the text of this manual to illustrate keyboard input, screen display dialogs, and special vocabulary.

- Text entered by you is shown in bold. Example: **supervisor**.
- Code examples and screen messages are shown in a `monospace` font.
- Italics are used for important new terms, for book and manual titles, and when terminology is explained, introduced, or emphasized. Example: "The word *bit* is a contraction of the words *binary digit*.").
- Names of keyboard keys are shown in small caps. Example: SHIFT.
- Certain keys and key combinations may be abbreviated as follows:

  <CR> Means press the carriage return key, which can be represented on the keyboard by a broken left-pointing arrow or the words *Enter* or *Return*. The ENTER key, or carriage return, is used to activate most commands.

  ALT+X Means to hold down the ALT key while you press the key represented by X.

  CTRL+X Means to hold down the CTRL (control) key while you press the key represented by X.

- Please notice the difference between the capital letter *O* and the number *0*.

# 2 Installation and Configuration

# Requirements

Radius Server requires a 486-66 MHz or faster computer, preferably running Microsoft Windows NT Server. Though Radius Server can also run on Windows 95, Windows 98, and Windows NT 4.0 Client, on those operating systems it is not possible to use the NT Server user database. The computer should have a hard disk, a CD-ROM drive, and LAN or WAN access.

Radius Server requires approximately 420KB on the hard disk, plus space for the user database.

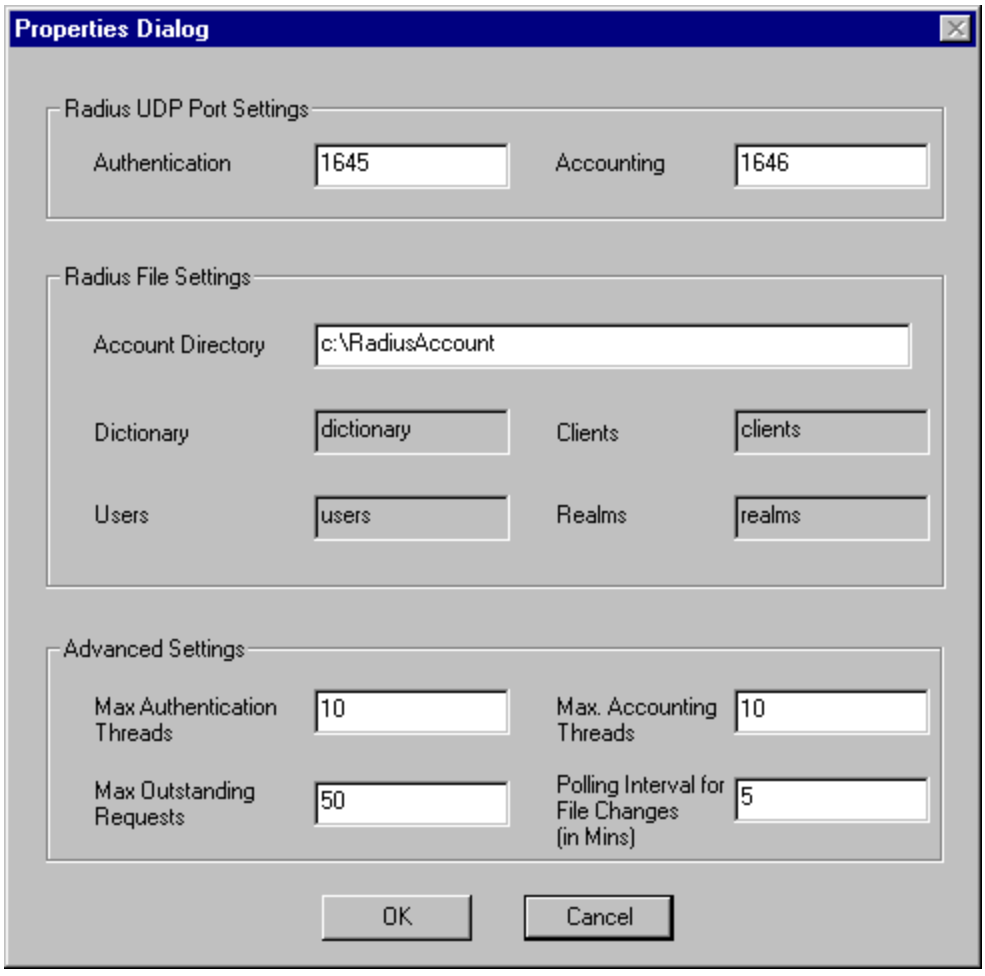
# Installing Radius Server

1. On the Radius Server computer, exit all Windows programs except Windows Explorer.
2. Insert the compact disc supplied with your Multi-Tech Systems communications server into the computer's CD-ROM drive.
3. If Autorun does not display the installation menu, find Autorun.exe in the root folder of the compact disc, and double-click it. The installation menu appears.
4. In the **Install Software** option, select **Radius Server**. The Multi-Tech Radius Server Setup wizard appears.
5. Follow the instructions in the Setup wizard to install Radius Server.
6. When the **Settings** dialog box appears, click **OK**. You can change these settings anytime whenever Radius Server is running.
7. Click **Finish**.
8. Reboot the computer. By default, Multi-Tech Radius Server runs automatically on startup; however, you can also start it manually from the Start Menu.

# Configuring Radius Server

## Radius Server Properties

When Radius Server is running, the Radius Server icon appears in the Taskbar tray. To configure Radius Server, right-click the icon and select **Properties** from the context menu. The following dialog box appears:




**Authentication**
The RADIUS server port number. The default port number (1645) is required for Radius Server to work with RASExpress.

**Accounting**
The RADIUS accounting port number. The default port number (1646) is required for Radius Server to work with RASExpress.

**Account Directory**
The path where accounting logs are stored.

### Dictionary
The name of the dictionary file. The dictionary file is an ASCII text file containing translations for parsing requests and generating responses. This name cannot be changed.

### Clients
The name of the clients file. The clients file is an ASCII text file containing the IP addresses and shared secrets of the clients (RASExpress servers) served by Radius Server. This name cannot be changed.

### Users
The name of the users file. The users file is an ASCII text file that lists authentication and configuration information for each user. This name cannot be changed.

### Realms
The name of the realms file. The realms file is an ASCII text file that lists authentication servers to which a specific authentication request can be forwarded. This name cannot be changed.

### Max Authentication Threads
The maximum number of threads that can be run at one time to perform authentication operations.

### Max Accounting Threads
The maximum number of threads that can be run at one time to perform accounting operations.

### Max Outstanding Requests
The maximum number of requests that can be queued up for processing.

### Polling Interval for File Changes
The period in minutes after which the configuration files (users, realms, clients) are polled to check whether they have been modified recently. If they have been modified, the corresponding data structures are then dynamically updated.

# Editing the Configuration Files

After installing Radius Server, you must customize the Radius Server configuration files. There are four configuration files in the C:\Program Files\Multi-Tech Systems\Radius Server folder: Clients, Dictionary, Realms, and Users. All are text files that can be edited with any text editor, such as Notepad.

## Clients File

The Clients file contains the IP addresses and shared secrets of the client RASExpress servers served by Radius Server. Entries should be in the following format:

```
<IP address of the client><blank(s) or tab(s)><shared
secret><new line>
```

The IP address should be in dotted decimal notation only; names are not permitted.

Example: **`192.168.1.26  abcd`**

The installed Clients file contains example entries, which should be replaced by actual entries.

## Dictionary File

The Dictionary file contains translations for parsing requests and generating responses. Generally, it should not be necessary to edit the dictionary. However, you may wish to open it to identify legal attribute-value pairs for the Users file. Note that lines starting with the # character are comment lines.

**Caution:** Modifying the contents of the Dictionary file incorrectly can cause Radius Server to fail to authenticate users correctly or cause other problems.

## Realms File

The Realms file lists authentication servers to which a specific authentication request can be forwarded. It is used when Radius Server acts as a proxy client to other RADIUS servers or other kinds of authentication servers.

With proxy RADIUS, a RADIUS server forwards an authentication or accounting request from a client remote access server to a remote RADIUS server, and returns the reply of the remote RADIUS server to the client remote access server. The choice of which server to forward the request to is based on the authentication “realm.” A realm can be based on part of the user name, for example, the part following an @ character (a “named realm”), or a called-station-ID (a “numbered realm”), or whatever other criteria the forwarding server is configured to use.

The Realms file uses only the part following an @ character. The file contains a list of realm names linked to remote authentication systems that can be used to authenticate a user. Entries should be in the following format:

```
<realm><blank(s) or tab(s)><IP address of the remote RADIUS
server><new line>
```

The IP address should be in dotted decimal notation only; names are not permitted.

Example: **`mul  192.168.2.50`**

In this example, whenever a remote access server such as RASExpress sends an authentication request for a user named "user1@mul," the request is forwarded to the remote server 192.168.2.50. The response from the remote server to Radius Server is then forwarded to the remote access server.

The installed Realms file contains the above example entry, which should be replaced by actual entries.

## Users File

The Users file stores authentication and configuration information for all users authenticated by Radius Server. Each user is represented by a profile that consists of three parts: the user name**,** a checklist, and a list of reply items.

User profiles must be separated from each other by an empty line. The first line of a user profile consists of the user name followed by the checklist. The user name is separated from the check items by a tab or spaces. This first line must not exceed 255 characters. All subsequent lines of the profile are individual reply items. Each reply item line must begin with a space or tab. Each reply item, except for the final line in the profile, must end with a comma.

You can add comments to the Users file by beginning comment lines with the **#** character. However, do not place comments within a user profile, since they will prevent any reply item following the comment from being processed and sent to the client.

The contents of each user profile are case-sensitive. Valid attributes and values are listed in the Dictionary file, and can be viewed with any text editor.

### User Name

The user name must start in the first column of the first line. It consists of no more than eight printable ASCII characters. White spaces, including trailing spaces, are not allowed in a user name, and will cause the authentication request to be rejected if entered by the user. The first line must not exceed 255 characters.

### Checklist

Checklist items are also listed on the first line. They follow the user name and are separated from it by a tab or spaces. Checklist items must be separated by commas; however, do not place a comma after the final checklist item.

The checklist can contain the following attribute-value pairs:

**Auth-Type =** {**Local** | **System**}
States whether authorization is done locally by Radius Server or the system server (Windows NT only). If this item is omitted, local authentication is assumed.

**Password = "***user password***"**
The Password attribute is used when PAP is the authentication protocol. The user password must be enclosed within double quotation marks.

**CHAP-Password = "***user password***"**
The CHAP-Password attribute is used when CHAP is the authentication protocol. The user password must be enclosed within double quotation marks.

The checklist also can contain a prefix or suffix or any other attribute-value pair that the RASExpress server can send as part of the authetication request. See the Dictionary file for valid attribute-value pairs

**Note:** If no checklist items are included in the user profile, the user is rejected.

### Reply Items

Reply items are attribute-value pairs placed one per line. Each line begins with a tab or space and ends with a comma and newline, except for the final reply item.

Reply items give the RASExpress server configuration information about the user's connection—for example, whether PPP or SLIP is used or whether the user's IP address is negotiated.

Only if all checklist items in the user profile are satisfied by the authentication request does Radius Server send the reply items to the RASExpress server to configure the connection.

### User Profile Examples

**Example 1**

This profile is for a locally authenticated user with PAP authentication:

```
user1  Auth-Type = Local, Password = "user1"
       Service-Type = Framed-User,
       Framed-Protocol = PPP,
       Framed-IP-Address = 255.255.255.254,
       Framed-Routing = None,
       Framed-MTU = 1534,
       Framed-Compression = Van-Jacobson-TCP-IP
```

**Example 2**

This profile is for a locally authenticated user with CHAP authentication and a limit of two concurrent logins. Note that because the Auth-Type atttribute is omitted, local authentication is assumed:

```
user2 CHAP-Password = "user2", Simultaneous-Use = 2
       Service-Type = Framed-User,
       Framed-Protocol = PPP,
       Framed-IP-Address = 255.255.255.254,
       Framed-Routing = None,
       Framed-MTU = 1534,
       Framed-Compression = Van-Jacobson-TCP-IP
```

**Example 3**

This profile is for a system-authenticated user with PAP authentication and session and idle timeouts. Note that CHAP will not work with system authentication. For system authentication to work on Windows NT, the user who has logged on to NT should have the rights “Act as part of the operating system” and “Log on as batch job.” The domain name in which the user is authenticated can also be included in the checklist. The domain name must be a string enclosed within double quotes:

```
user3  Auth-Type = System, Password = "user3", Domain-Name = "multitech"
       Service-Type = Framed-User,
       Framed-Protocol = PPP,
       Framed-IP-Address = 255.255.255.254,
       Framed-Routing = None,
       Framed-MTU = 1534,
       Framed-Compression = Van-Jacobson-TCP-IP
       Session-Timeout = 10
       Idle-Timeout = 10
```

### DEFAULT User Profiles

You can use a DEFAULT user profile to match on all user names. When Radius Server receives a login name from a RASExpress server, it scans the users file for a matching user name, starting from the top of the file. If a match is found, Radius Server attempts to authenticate the user with the information in the matching user profile. If a matching user profile is not found during the scan, but a DEFAULT profile is located, Radius Server attempts to use the DEFAULT profile for authentication. The DEFAULT profile is typically used when the Auth-Type is System or SecurID.

**Caution:** You must place DEFAULT profiles at the end of the users file. Radius Server stops scanning profiles when a matching DEFAULT profile is found, and ignores any user profiles located after a DEFAULT user profile unless **`Fall-Through = 1`** is included in the reply list.

In place of a user name, the first line of DEFAULT profiles starts with the word **`DEFAULT`**, all in upper case. You can use this for multiple DEFAULT profiles if **`Fall-Through = 1`** is included in the reply lists. In the following example, whatever the name of the user who issues a request to the Radius Server, he will be authenticated as long as he supplies the password “def”.

```
DEFAULT  Password = "def"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 255.255.255.254,
         Framed-Routing = None,
         Framed-MTU = 1534,
         Framed-Compression = Van-Jacobson-TCP-IP
```

If you have more than one DEFAULT user profile, you can force Radius Server to examine the next one by adding **`Fall-Through = 1`** to the reply list of the preceding DEFAULT user profile , as in the following example:

```
DEFAULT  Password = "def"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 255.255.255.254,
         Framed-Routing = None,
         Framed-MTU = 1534,
         Framed-Compression = Van-Jacobson-TCP-IP
         Fall-Through = 1
```

### Prefixes and Suffixes

Prefix and Suffix checklist items can be used with DEFAULT user profiles to allow a network user to access multiple services by adding characters to the beginning or end of his user name. Prefix and Suffix strings must consist of 16 or fewer nonspace, ASCII characters, which must be contained within double quotation marks.

When a user logs in, Radius Server searches through the Users file for a profile that matches the login. If a profile has a Prefix or Suffix checklist item, the server strips away the specified prefix or suffix character(s) from the login name before checking the password. If the server does not find a profile that matches the login, the RADIUS server tries to match the login against a DEFAULT user profile. For example:

```
Muser1   Auth-Type = System, Prefix = "M"
         Service-Type = Framed-User,
         Framed-Protocol = PPP,
         Framed-IP-Address = 255.255.255.254,
         Framed-Routing = None,
         Framed-MTU = 1534,
         Framed-Compression = Van-Jacobson-TCP-IP
```

In this example, user1's user name and password are stored in a system password file. If user1 specifies a user name of **Muser1** when attempting to connect to the RASExpress server, Radius Server looks up the user name. When the profile for user1 is found, the Prefix checklist item matches because the login name begins with an *M*. This cues the server to strip away the specified prefix character and check the system password file for user1's password. If a password match is found, **Muser1** is connected as a PPP user.

```
DEFAULT  Auth-Type = System, Suffix = "%slip"
         Service-Type = Framed-User,
         Framed-Protocol = SLIP,
         Framed-IP-Address = 255.255.255.254,
         Framed-Routing = None,
         Framed-MTU = 1534,
```

In the preceding example, if user1 specifies a user name of **user1%slip** when he logs in, Radius Server finds no match until it gets to the DEFAULT profile. The Suffix checklist item matches because the login name ends with **%slip**. This cues the server to strip away the specified suffix characters and check the system password file for user1's password. The server next checks the system password for user1. If a password match is found for user1, **user1%slip** is connected as a SLIP user.

## Using Windows NT Server for Authentication

The Multi-Tech RADIUS server provides the flexibility to use its own User database or the Windows NT system database to authenticate a User.

The following examples describe in detail, the steps involved in setting up the Multi-Tech RADIUS server to authenticate a user using the Windows NT User Database.

```
Userx     Auth-Type = Local, Password = "userx"
          Service-Type = Framed-User,
          Framed-Protocol = PPP,
          Framed-IP-Address = 255.255.255.254,
          Framed-Routing = None,
          Framed-MTU = 1534,
          Framed-Compression = Van-Jacobson-TCP-IP
```

The first attribute in the above example shows the “Auth-Type” set to “Local”. To use the Windows NT System database, the Auth-Type should be set to “System”, as shown below. If there is an NT domain, replace the Password=”userx” with the Domain-Name =”Domain” and the “Domain” in quotes being the real name of your domain. The Password=”userx” will not will used, as the Password in Windows NT User Database will be used.

```
DEFAULT    Auth-Type = System, Domain-Name = "Domain"
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-IP-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1534,
           Framed-Compression = Van-Jacobson-TCP-IP
```

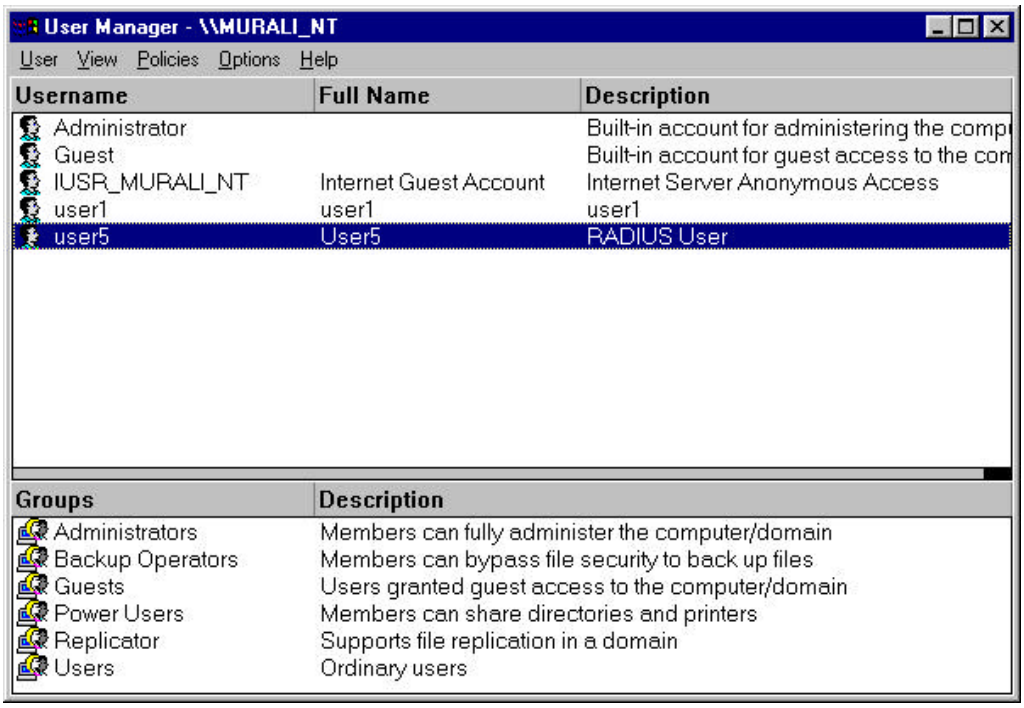
The DEFAULT entry must be the last entry in the users file. It can be the only entry with "DEFAULT" as a username.

This is the only required change in the Multi-Tech RADIUS Server. The rest of the process involves configuration of the NT server.

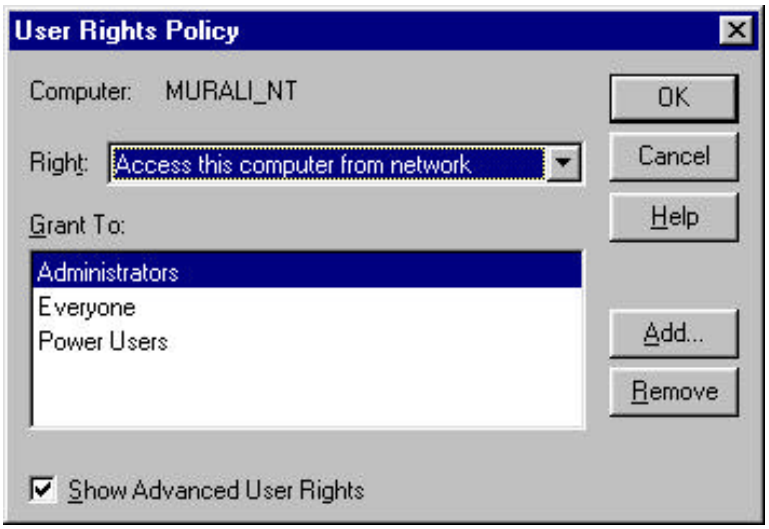
After the necessary changes are made, restart the Multi-Tech RADIUS server service from the Services Management Console, for the changes to take affect.

After the service is restarted, add the user in the Windows NT server, and configure the user with default / custom values. There are only two additional settings to be done, for the Multi-Tech RADIUS server to use the Windows NT System Username & Password.

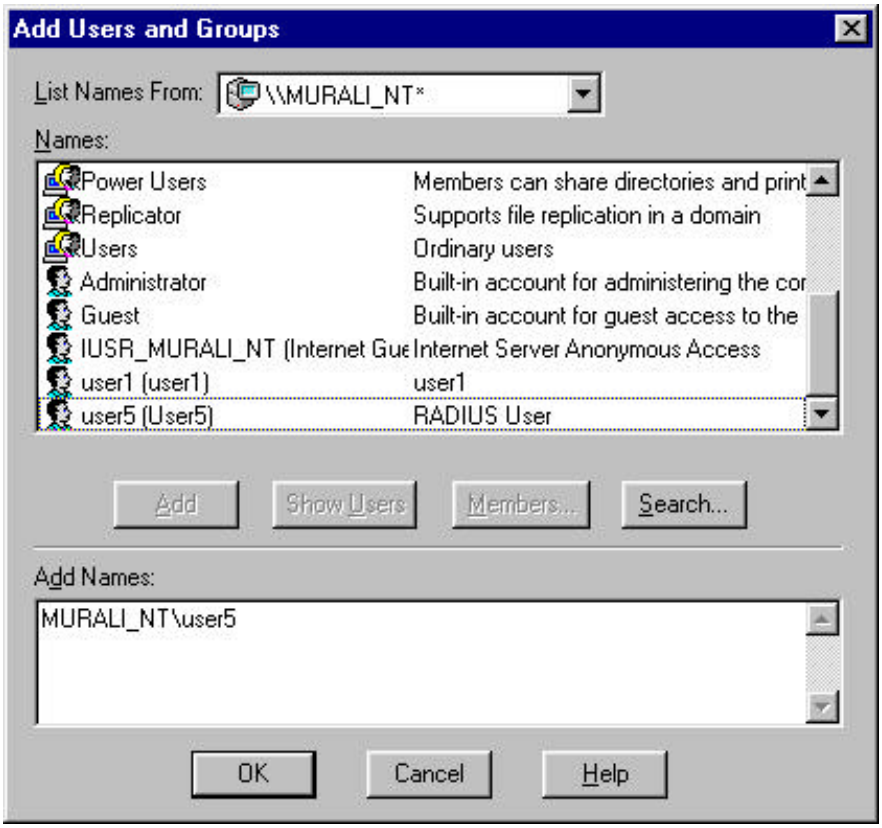
The following Image shows the Windows NT User Management windows, showing which User / Groups can be added / modified / deleted. (For our example / explanation, we will consider user5 in the RADIUS Users file & Windows NT System Database).



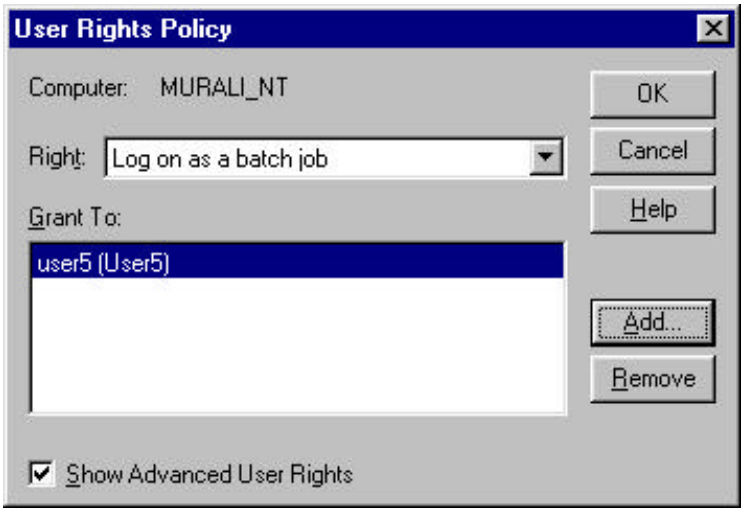

After the User is successfully added, select the sub-menu ***User Rights*** from the ***Policies*** Menu. This will pop-up a window as shown below.




Enable the "**Show Advanced User Rights**" check box (*Disabled* by default), which will populate the **Right:** combo box with additional values. From the **Right:** combo box, select the "**Log on as a batch job**", click the Add button and add the user (*User5).* In this example. you could add all the users / groups that have to be authenticated using the System Database to the Users list, as shown in the Image below.



The above window shows all the available Users & Groups in the Windows NT Server. The above window will initially show only the Groups & System created Users. Click on "Show Users" to show / list all the users. Add the required Users & Groups.




Similarly, from the **Right:** combo box, select the "**Act as part of the Operating System**" item, and add the required Users / Groups (user5 in our example) to the **Grant To:** List. Click "Ok" and exit from the User Management Window.

These simple steps complete the configuration of the Multi-Tech RADIUS server using the Windows NT Server's User Database. From now on, to authenticate any user, whose "Auth-Type" is set to "System", will be authenticated using the Windows NT System Database, and the Multi-Tech RADIUS Server Database.

**Note:** Only PAP authentication is possible using this technique. CHAP AUTHENTICATION IS NOT POSSIBLE WITH NT USER DATABASE.

The following is an example of a Multi-Tech RADIUS Server's Users.txt file showing users, user1-user3, using the Local Database (PAP & CHAP supported) and all other users using the Windows NT System Database (Supports PAP only) for authentication. The DEFAULT user (all other Usernames not listed in the Users.txt file) Auth-Type is set to System.

```
User1      Auth-Type = Local, Password = "user1"
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-IP-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1534,
           Framed-Compression = Van-Jacobson-TCP-IP
```

```
User2      Auth-Type = Local, CHAP-Password = "user2"
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-IP-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1534,
           Framed-Compression = Van-Jacobson-TCP-IP

User3      Auth-Type = Local, Password = "user3
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-IP-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1534,
           Framed-Compression = Van-Jacobson-TCP-IP

DEFAULT    Auth-Type = System
           Service-Type = Framed-User,
           Framed-Protocol = PPP,
           Framed-IP-Address = 255.255.255.254,
           Framed-Routing = None,
           Framed-MTU = 1534,
           Framed-Compression = Van-Jacobson-TCP-IP
```

# Installed Files

The Radius Server folder contains the following files:

| | |
|---|---|
| RADSERVER.EXE | The Radius Server executable file. |
| BINARY | Created from the Users file during the process of Btree creation. |
| BTREE.DLL | Used to create the Btree for users. |
| DELFILES.DLL | Used to clean up the folders during the process of uninstallation. |
| MFC42.DLL | Microsoft library file. |
| MFC42D.DLL | Microsoft library file. |
| MFCO42D.DLL | Microsoft library file. |
| MSVCIRT.DLL | Microsoft library file. |
| MSVCRT.DLL | Microsoft library file. |
| MSVCRT40.DLL | Microsoft library file. |
| MSVCRTD.DLL | Microsoft library file. |
| MY_USERS | An ASCII file created from the Users file during the process of Btree creation. |
| ODBC32.DLL | Microsoft library file. |
| ODBCINT.DLL | Microsoft library file. |
| RADIUS.LOG | An ASCII file containing a log of Radius Server activities. |
| README.TXT | Readme file. |
| UNINST.ICO | Uninstall icon. |

The following files are used to configure Radius Server :

| | |
|---|---|
| CLIENTS | A text file that lists the clients allowed to send authentication requests to Radius Server and their shared secret encryption keys. The default Clients file contains only sample entries. |
| DICTIONARY | A sample text file that contains dictionary translations for parsing requests and generating responses. All transactions are composed of Attribute-Value pairs. |
| REALMS | A text file that lists authentication servers to which an authentication request from a specific realm can be forwarded. The default Realms file contains only a sample entry. |
| USERS | A text file that lists authentication and configuration information for each user. The user database. The default Users file contains several sample entries. |