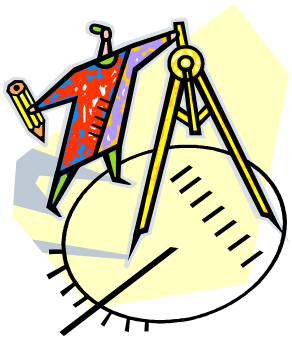
RADIUS Test Client



For Windows, Linux, Solaris & FreeBSD

Version 4.0.41

IEA SOFTWARE

Administrative & Support Office
P.O. BOX 1170
Veradale, Washington 99037
Phone: (509) 444-BILL

sales@iea-software.com
support@iea-software.com

Software License Agreement

By purchasing or installing RADIUS test client, you indicate your acceptance of the following License Agreement.

Ownership of Software You acknowledge and agree that the computer program(s) and associated documentation contained with RADIUS test client (collectively, the Software) are owned exclusively by IEA Software, Inc. and/or its licensors. The Software contained in the package is protected under copyright laws and all copyright and other intellectual property rights relating to the Software are and remain the exclusive property of IEA Software, Inc. and/or its licensors. You may not rent or lease the Software, but you may transfer the Software and accompanying materials on a permanent basis provided you retain no copies and the recipient agrees to the terms of this Agreement.

License IEA Software, Inc. grants to you, and you accept, a limited, non-exclusive and revocable license to use the Software. You agree to use the Software in machine-readable object code form only as authorized in this License Agreement. This License Agreement does not convey any title or interest in the Software to you.

Scope of License You may not make any changes or modifications to the Software, and you may not de-compile, disassemble, or otherwise reverse engineer the Software. You may not lend, rent, lease or sublicense the Software or any copy to others for any purpose. You are not permitted to make any uses or copies of the Software that are not specifically authorized by the terms of this License Agreement. Your adherence to this License Agreement will allow IEA Software, Inc. to continue developing innovative and useful products and providing a high level of customer service and support. If you do not comply with the terms of this License Agreement, your license will be revoked.

Updates and Support All software updates and fixes are available via the IEA Software, Inc. Web site. Technical support is currently available via methods listed on our Web site Support section at http://www.iea-software.com/support.

Restricted Rights The Software is provided with U.S. Governmental Restricted Rights. Use, duplication, or disclosure by the Government is subject to restrictions set forth in subparagraph ©(1)(ii) of The Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraphs ©(1) and (2) of the Commercial Computer Software - Restricted Rights at 48 CFR 52.227-19 as applicable. The Software is also protected by International Treaty Provisions. Manufacturer is IEA Software, Inc. PO BOX 1170 Veradale WA, 99037.

Miscellaneous This License Agreement shall be construed, interpreted and governed by the laws of the State of Washington. Should any term of this License Agreement be declared void or unenforceable by any court of competent jurisdiction, enforcement of the remaining terms shall not be affected. Failure of either party to enforce any rights or to take action against the other party in the event of any breach of this Licensing Agreement shall not be deemed a waiver of any subsequent enforcement of rights.

Limitations of Liability and Remedies In no event shall IEA Software, Inc. or its licensors be liable for any loss of profit or any other commercial damage, including but not limited to special, incidental, consequential or other damage, even if IEA Software, Inc. or its licensors are advised, in advance, of the possibility of such damages. IEA Software, Inc. and its licensor's entire liability and your exclusive remedy shall be, at IEA Software's option, either (a) return of the price paid, or (b) repair or replacement of the Software. To the maximum extent permitted by applicable law, IEA Software, Inc. and its licensors disclaim all other warranties, either express or implied, including but not limited to, implied warranties with

regard to the Software and the accompanying material. This Limited Warranty is void if failure of the Software has resulted from accident, abuse or misapplication. You may have other specific legal rights, which vary from state/jurisdiction to state/jurisdiction.

Return Policy It is our goal to provide customers with the highest level of satisfaction possible. In order to ensure that our products work well in your environment, IEA Software offers a 45-day FULL functioning software trial that includes documentation and support. If you require more than 45 days to evaluate the software, we are happy to work with you to extend the trial to a length that fits your timetable. This gives you, the user, an opportunity to ensure that the product fully meets your needs. In light of the trial period and opportunity to fully test our software, IEA Software maintains the policy that no refunds will be offered. We will, however, address any problems with the software.

Should a software anomaly occur, our Development and Support Teams will work to correct the problem. Please note that you must be using the application normally, as defined, and you must ensure that the bug is not due to anomalies in other programs, the operating system, your hardware, or data.

In order to address any problems, please note that the bug must be able to be reproduced. Our Development and Support Teams will require full documentation of the steps taken by the user that caused the error in the software as well as necessary data and scenario files to reproduce the error.

Contact Should you have any questions concerning this license agreement, please contact IEA Software, Inc. PO BOX 1170 Veradale, WA 99037 U.S.A. (509) 444-BILL (2455).

Information in this document is subject to change without notice. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, without the express written consent of IEA Software, Inc.

Trademarks

Emerald Management Suite, RadiusNT and *RadiusX* are trademarks of IEA Software, Inc. All images, photographs, animations, audio, video and text incorporated into the Software are owned by IEA Software, Inc., unless otherwise noted by Trademark. *Alpha AXP* is a registered trademark of Digital Equipment Corporation. *Intel* is a registered trademark of Intel Corporation. *Transact-SQL* is a registered trademark and *DB-Library* is a trademark of Sybase, Inc. *Sparc Solaris* are trademarks of Sun Microsystems. *Cisco* is a trademark of Cisco Systems. All other trademarks are the property of their respective owners.

Table Of Contents

Introduction

The RADIUS test client is an easy to use tool to simulate, debug and monitor most RADIUS and Network Access Servers (NAS).

IEA Software is a world-leading provider of billing, customer care, and authentication solutions for ISPs, VISPs, wireless and VOIP. Please visit our web site (http://www.iea-software.com) or contact our sales staff to learn more.

System Requirements

Browser

- Any web browser supporting CSS2 (Netscape 6+ or Internet Explorer 6+)

Linux

- PERL (required for installation)
- x86 based CPU

Solaris

- PERL (required for installation)
- Solaris 2.6 or higher
- Sparc based CPU

Windows

- Any edition of Windows NT4, 2000, XP, Vista/7, 2003 and 2008/R2

Installation

Linux

Download the Radlogin 4 archive (radlogin4_linux.tar.gz) into a temporary folder.
To un-archive the file type:
tar –zxf radlogin4_linux.tar.gz

Next, run the installer:
./install.pl

Press 'C' then 'Enter' to continue.

To start the server: reboot or run /usr/local/radius/radlogin.
To access the web interface browse to http://localhost:8020

Solaris

Download the Radlogin 4 archive (radlogin4_solaris.tar.gz) into a temporary folder.
To un-archive the file type:
gzip –d radlogin4_solaris.tar.gz
tar –xf radlogin4_solaris.tar

Next, run the installer:
./install.pl

Press 'C' then 'Enter' to continue.

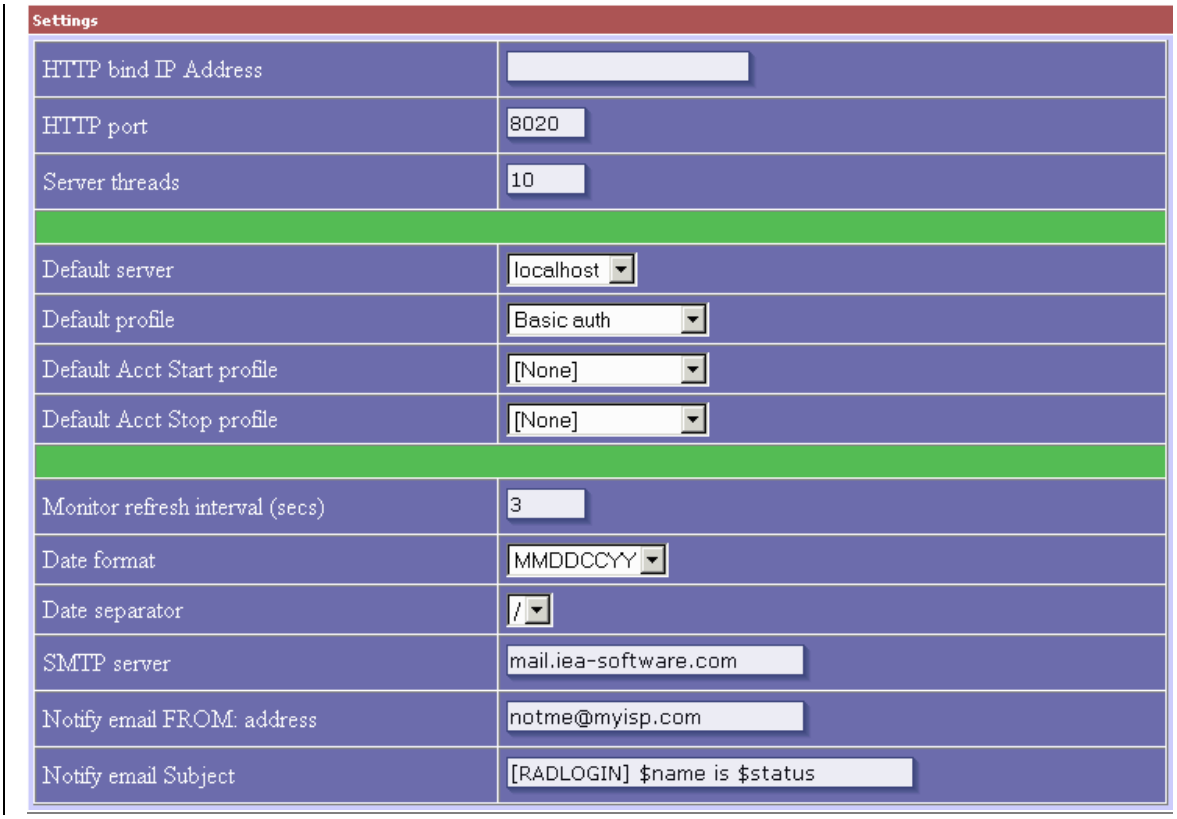
To start the server, run /usr/local/radius/radlogin.
To access the web interface browse to http://localhost:8020

Windows

Download the Radlogin 4 archive (radlogin4.exe) into a temporary folder.
Run radlogin4.exe
Follow the prompts.
The web interface can be accessed by selecting ‘Programs’ / ‘RadiusNT’ / ‘Radius test client’ from the windows START menu.

Configuring

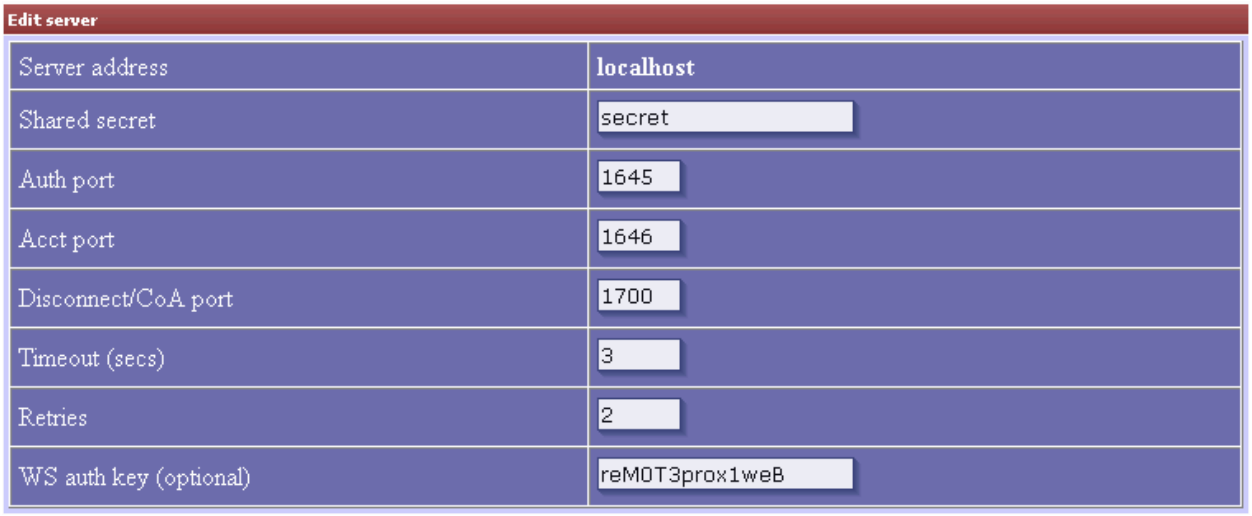
Settings



Option	Description
HTTP bind IP Address	Local IP Address the web server will listen for incoming http requests. By default the server listens on all available interfaces. Note you can restrict access to only local clients by setting the bind address to the local loop back interface (127.0.0.1)
HTTP port	TCP port to listen for incoming http requests.
Server threads	Number of concurrent requests the server can process at any one time. There is no limit however its unlikely you will ever need more than 10.

Default server	Selects the RADIUS server that should be used when radlogin is used from the command line interface.
Default profile	Selects the default authentication profile attributes to use when radlogin is used from the command line interface. If None is selected a default set of attributes is used.
Default Acct Start profile	Selects the default accounting profile to use when radlogin start requests are sent from the command line interface. If None is selected a default set of attributes is used.
Default Acct Stop profile	Selects the default accounting profile to use when radlogin stop requests are sent from the command line interface. If None is selected a default set of attributes is used.
Monitor refresh interval	Controls how often to refresh the server-monitoring scoreboard display. In seconds.
Date format	Internal date format used when displaying date/time strings.
Date separator	Internal date format separator used when displaying date/time strings.
SMTP server	SMTP mail server used to send status notifications. (See Server monitoring)
Notify email FROM: address	Email address status notifications will be sent from (See Server monitoring)
Notify email Subject	The subject line of a notification. The following variables can be used on the subject line. $name – monitor name $server – server name $status – Current server status (UP or DOWN) $profile – Attribute profile name The default notify subject is: [RADLOGIN] $name is $status (See Server monitoring)

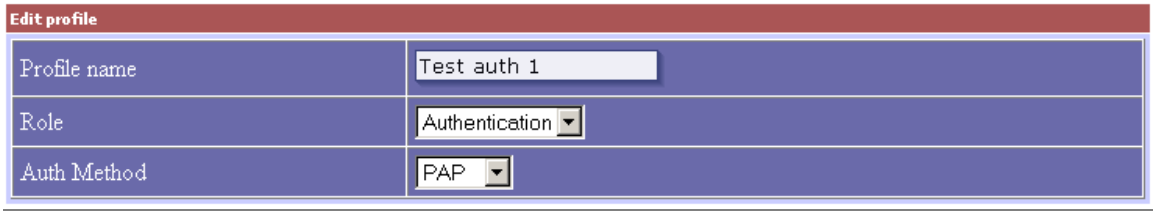
RADIUS servers



Option	Description
Server address	IP Address or hostname of the RADIUS server.
Shared secret	RADIUS shared secret, the server must have the same secret configured for requests coming from the radlogin test client.
Auth port	Port used to send authentication requests. The official RADIUS authentication port is 1812. Unofficially 1645 is still quite popular.
Acct port	Port used to send accounting requests. The official RADIUS accounting port is 1813. Unofficially 1646 is still quite popular.
Disconnect/CoA port	Port used to send Disconnect or CoA requests to an Access server. The official Disconnect port is 3799. Unofficially 1700 is popular.
Timeout (secs)	Number of seconds to wait for a response from the RADIUS server.
Retries	Number of times to resend a request if there is no response within the Timeout period above.
WS auth key	When set web service requests may query this server provided the requestor provides an authkey matching the key specified in this field. If not set web service requests for this client are disabled.

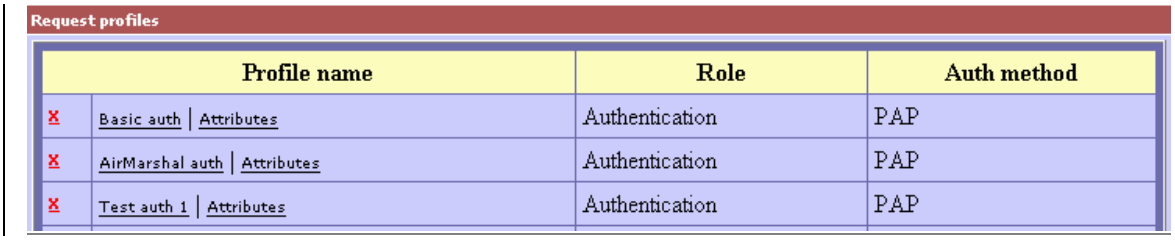
Request profiles

Request profiles optionally define the list of attributes sent to the RADIUS servers as well as various authentication and accounting options. At least one request profile is required in order to use 'Server monitoring' or 'Radlogin' features.



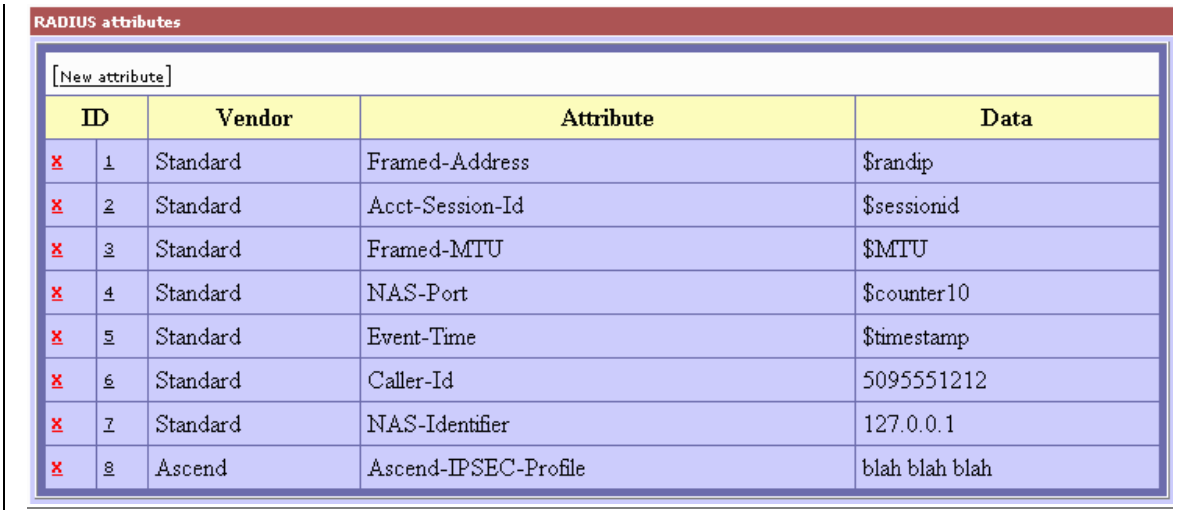
Option	Description
Profile name	Name to identify your request profile by.
Role	Sets whether RADIUS requests sent using this profile should be an authentication, accounting, disconnect or CoA request.
Auth Method	If an authentication request will be sent, should PAP or CHAP be used to send for password authentication? PAP (Password Authentication Protocol) works with any backend database. CHAP (Challenge Handshake Authentication Protocol) requires the RADIUS server have access to the users unencrypted text password.
Asterisk Event	When role is Asterisk Acct event sets the name of the Asterisk Manager API event the profile is to listen for. Typically event name is 'Cdr' for Call Detail records.

After creating a new request profile you can begin adding attributes to your profile.
Click the attributes link to begin adding them.



Request profiles

	Profile name	Role	Auth method
x	Basic auth | Attributes	Authentication	PAP
x	AirMarshal auth | Attributes	Authentication	PAP
x	Test auth 1 | Attributes	Authentication	PAP



RADIUS attributes

[New attribute]

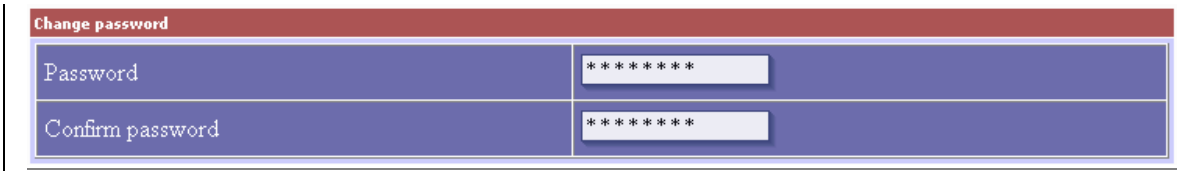
	ID	Vendor	Attribute	Data
x	1	Standard	Framed-Address	$randip
x	2	Standard	Acct-Session-Id	$sessionid
x	3	Standard	Framed-MTU	$MTU
x	4	Standard	NAS-Port	$counter10
x	5	Standard	Event-Time	$timestamp
x	6	Standard	Caller-Id	5095551212
x	7	Standard	NAS-Identifier	127.0.0.1
x	8	Ascend	Ascend-IPSEC-Profile	blah blah blah

In the example above you will notice variables in the Data column. Radlogin provides several built-in variables to provide unique data helping to simulating multiple requests. Variables and what they do can be found in the table below. If you specify a variable not in this table, you will be prompted to provide a value for that variable while using the Radius login feature.

Variable	Description
$counter	Starting at one increments by one for each request
$counter2	Counter2 resets to 1 after reaching 2.
$counter3	Counter3 resets to 1 after reaching 3.

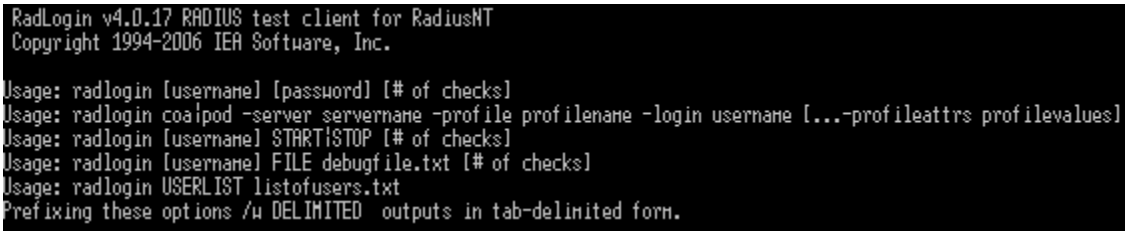
$counter10	Counter10 resets to 1 after reaching 10.
$counter100	Counter100 resets to 1 after reaching 100.
$counter1000	Counter1000 resets to 1 after reaching 1000.
$counteraz	Counteraz displays a single letter starting at ‘a’ and resetting after ‘z’
$randaz	Randaz displays a single random character
$randaiz5	Randaz5 displays 5 random characters
$randaz10	Randaz10 displays 10 random characters
$randip	RandIP displays a random IP Address
$timestamp	Timestamp is the current time as the number of seconds past January 1, 1970 00:00 UTC
$sessionid	A unique 16-character string. Makes a good Session-ID.

Change password



The admin password used to login to the radlogin web interface can be changed by entering a new password here. If you have other IEA software products such as Emerald or RadiusNT/X installed on the same computer changing the admin password for radlogin will also cause the admin password all other web based admin interfaces to change as well.

Command-line interface

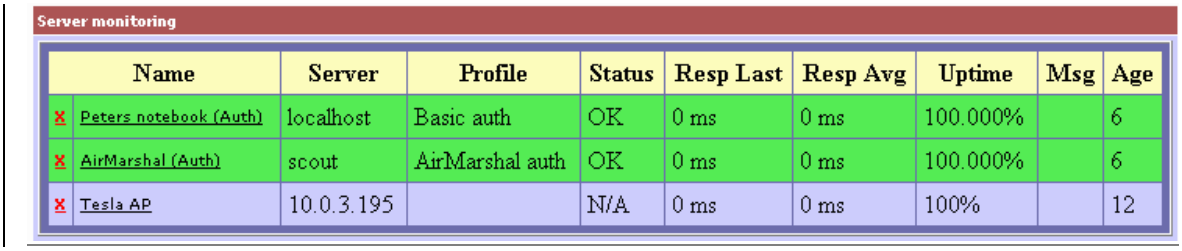


Running radlogin -? Displays available command line options.

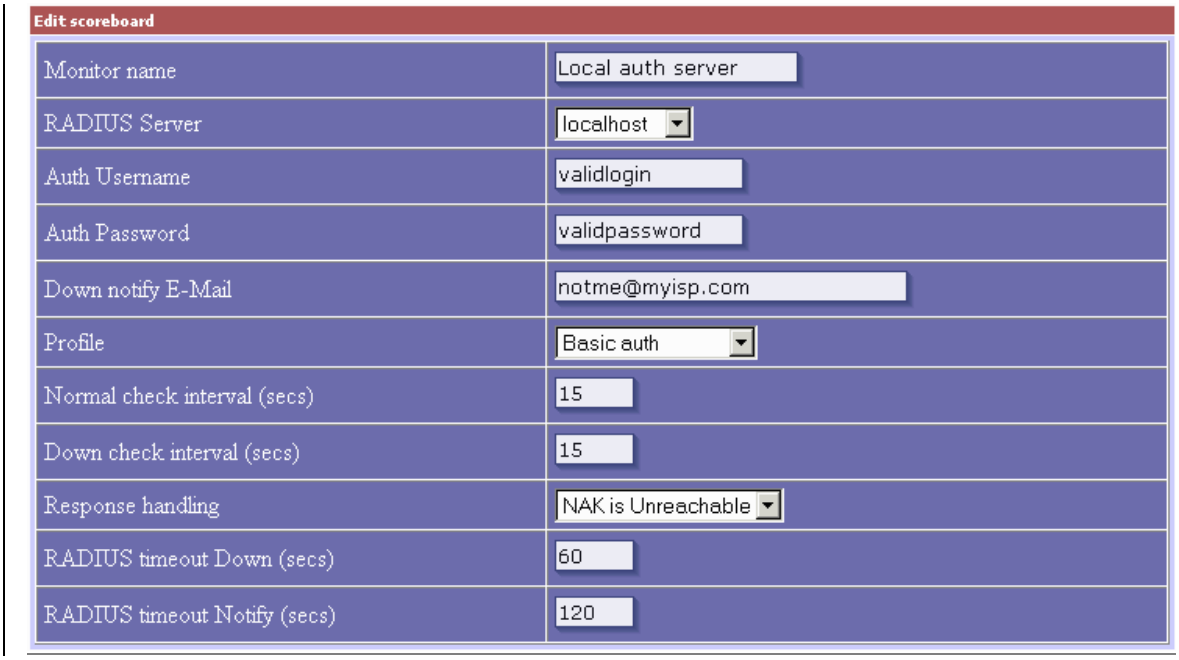
Example	Description
./radlogin neila test123	Sends a single PAP authentication request for the user neila with a password of test123.
./radlogin neila START	Sends a single Accounting START request for the user neila.
./radlogin neila STOP	Sends a single Accounting STOP request for the user neila.
./radlogin neila test123 1000	Sends 1000 PAP authentication requests for the user neila with a password of test123.
./radlogin neila test123 CHAP	Sends a single CHAP authentication request for the user neila.
./radlogin neila FILE raddebug58.txt	Sends an authentication request using the file raddebug58.txt. FILE must contain a hex dump

	of RADIUS AVPs (Attribute-Value-Pairs) (See Packet decoding)
./radlogin DELIMITED neila test123 1000	Sends 1000 PAP authentication requests for the user neila with a password of test123 using tab delimited output mode. This makes it easy to import the results of the test into a spreadsheet or database.
./radlogin coa|pod|auth|acct –server servername –profile profilename –login loginname –password password –variable1 value1 –example2 exvalue2 –variable3 value3	Sends a RADIUS request using named parameters. The first parameter is informational only and should be one of coa, pod, auth or acct depending on the type of request expected. The "-server" parameter is the name of a server defined in the RADIUS Servers section of the test client web interface. The "-profile" parameter is the name of the profile defined in the Request profiles section of the test client web interface. "-login" represents the User-Name attribute to send in the request and "-password" represents the password to send. All other named parameters can be used to match parameter variable names in the chosen profile. (See Request profiles)

Server monitoring

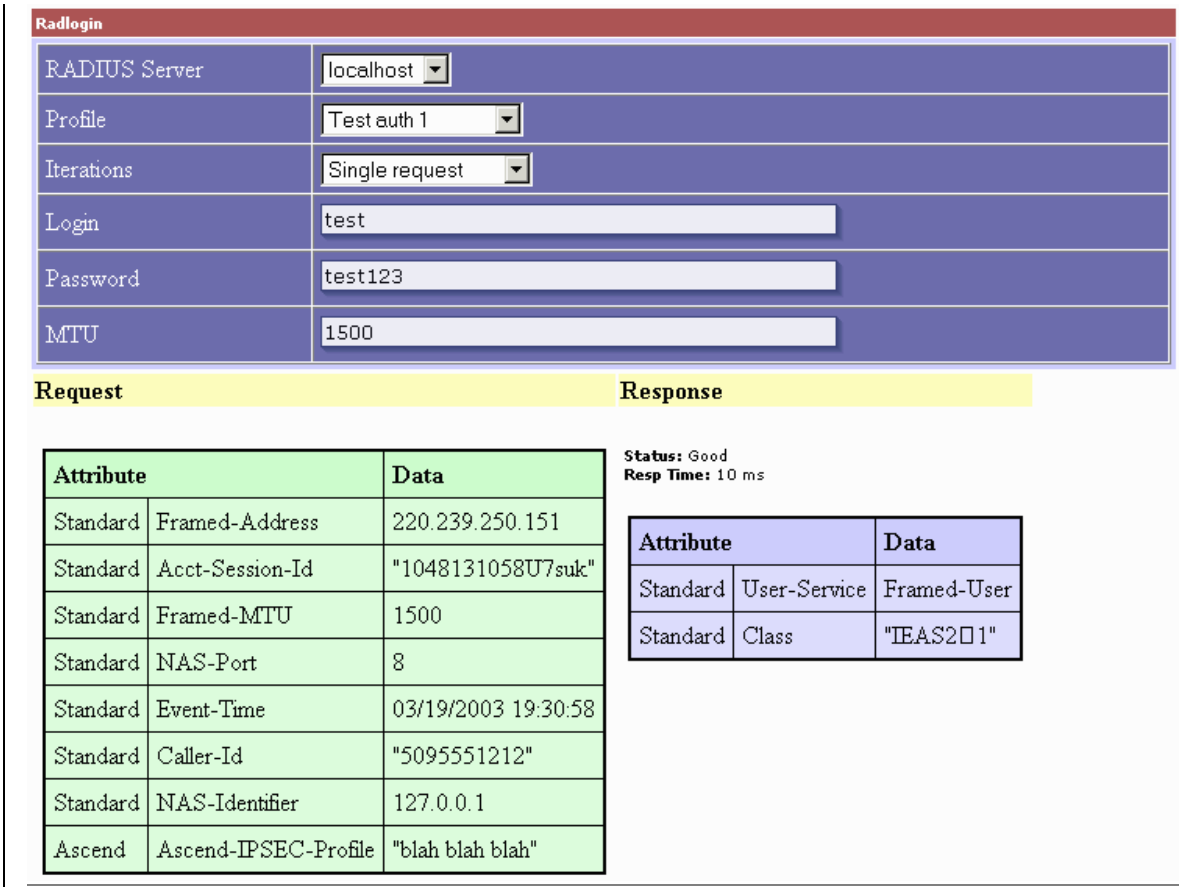


Server monitoring periodically polls RADIUS servers, testing their ability to respond to authentication or accounting queries. The 'scoreboard' shows a list of servers being monitored, their current status, statistics such as response times in Milliseconds and average uptime. The Age field displays the number of seconds since the server was last polled. In addition to the web interface, radlogin can also send email notifications if the server stops responding.



Option	Description
Monitor name	Name of the system being monitored
RADIUS Server	RADIUS server to send requests
Auth Username	Username for authentication requests
Auth Password	Password for authentication requests
Down notify E-Mail	If specified an email will be sent to this address whenever the server cannot be contacted.
Profile	Request profile controlling the type of RADIUS request to send
Normal check interval	Number of seconds between sending consecutive server requests. This setting is in effect when the server status is OK.
Down check interval	Number of seconds between sending consecutive server requests. This setting is in effect when the server status is DOWN.
Response handling	Controls whether a NAK in response to a RADIUS request should be considered an error or since the RADIUS server responded to the request its status should be considered OK.
RADIUS timeout Down	Number of seconds from last successful contact to consider the server DOWN.
RADIUS timeout Notify	Number of seconds from last successful contact to send an Email notification stating the server is down. Note the server must be in a down state before an Email notification can be sent out.

RADIUS login



Option	Description
RADIUS Server	Selecting 'All' will use the first available RADIUS server to perform the query. (See RADIUS servers)
Profile	(See Request profiles)
Iterations	Indicates the number of requests to simulate. If you choose more than a single request a summary of activity is displayed every 2.5 seconds. If you wish to do load testing we recommend you open several browser windows and run tests simultaneously in each window since radlogin currently cannot track more than one outstanding request per window.
Login	User-Name to send for authentication or accounting requests.
Password	Password to send for authentication requests.
MTU	MTU is a dynamic field added by the existence of $MTU in the 'test auth 1' profile. (See Request profiles).

Web Service Requests

In addition to the interactive RADIUS login and command line interfaces the test client supports an HTTP interface for automated RADIUS requesting from a scripting language or application framework.

A web service request consists of submitting a GET or POST request to `http://myradloginserver:8020/request` - containing the following HTTP request variables:

Variable Name	Required	Description
Server	Yes	Server Hostname or IP Address as configured from the RADIUS servers menu. Note: Server name must exactly match the name of the configured server.
Profile	Yes	Profile name as configured from the Request profiles menu. Profiles determine the type of RADIUS request to be issued.
Authkey	Yes	WS authorization key provides authorization to issue requests to Server. Authkey must exactly match the WS auth key field configured via the RADIUS servers menu.
Login	Required for Auth or Acct	Based on selected profile type - Login provides User-Name RADIUS attribute for authentication, accounting and Disconnect/CoA.
Password	Required for Auth	When the selected profile type is authentication Password determines the password sent in the RADIUS request.
*	No	Any other attribute name sent in the request can match a request profile variable allowing values for additional RADIUS request attributes to be configured in the web service request. See Request profiles for more information on configuring request variables.

Example Request:

```
http://myradloginserver:8020/request?server=localhost&profile=Basic+auth&authkey=reM0T3prox1weB&login=testuser&password=testpass
```

A response to the web service request consists of a URL Encoded string of response variables. The following variables may be returned in response to a RADIUS request.

Variable Name	Description
Retcode	Request status code 0=Good request/ACK, 1=Authentication Failure/Auth NAK, 2=Request timeout, 3=Request failure/error
Msg	String describing the overall request status
Resptime	Duration of RADIUS request measured in milliseconds 1000 MS = 1 Second
*	Any other variables returned consist of RADIUS reply attributes as named in the RADIUS dictionary. Note: The dash '-' character is omitted from attribute names.

Example Error Response:

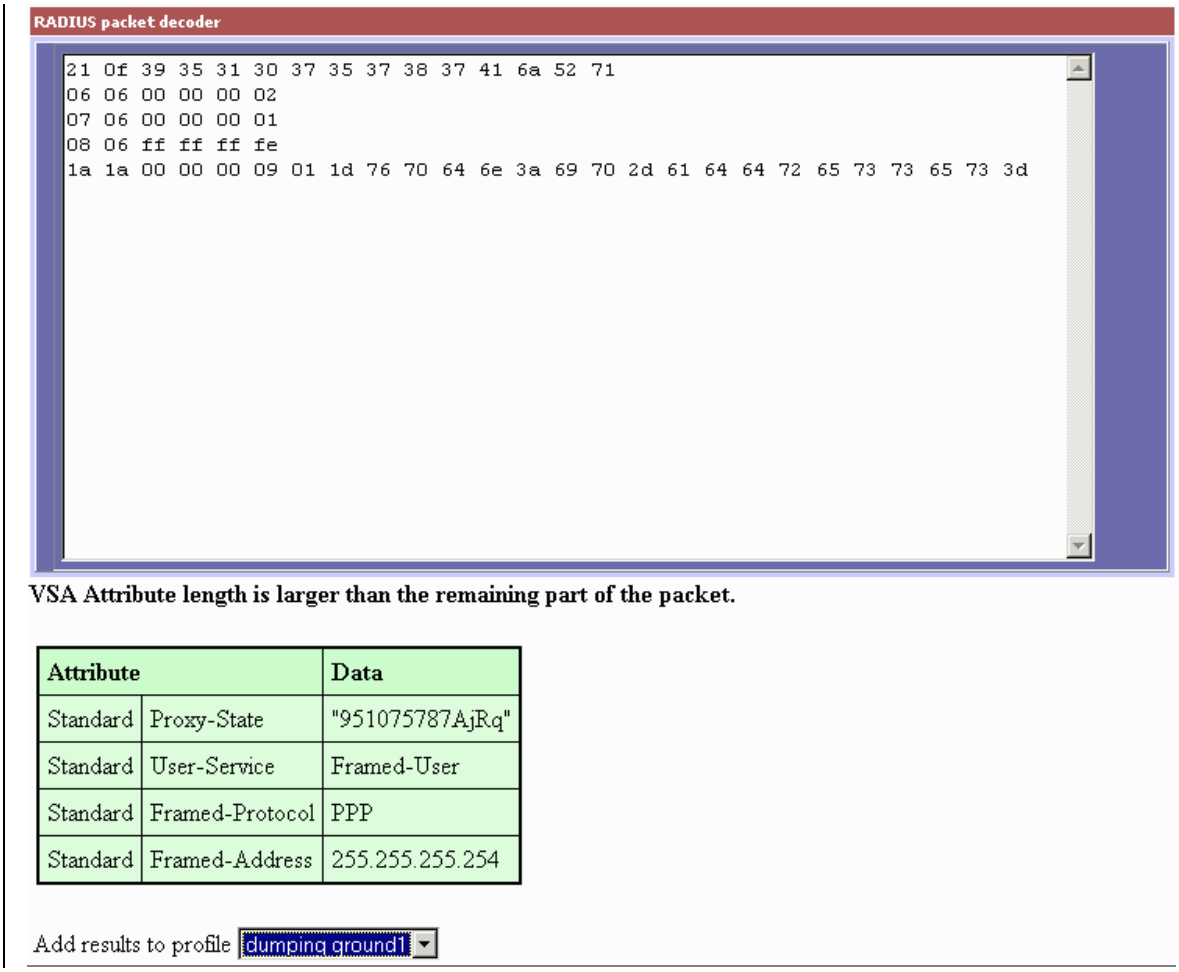
```
retcode=3&msg=Invalid+response+authenticator+%28check+shared+secrets%29
```

Example Access Reject Response:

```
retcode=1&msg=NAK&resptime=16
```

Example Access Accept Response:
`FramedFilter=test4&UserService=Framed%2DUser&FramedProtocol=PPP&retcode=0&msg=ACK&resptime=0&Class=IEAS44511%0112%011`

Packet decoding



Many NAS, RADIUS servers and network monitoring applications such as MS Network Monitor or Wireshark allow you to dump RADIUS AVPs (Attribute-Value-Pairs) in a raw hexadecimal format. The packet decoder allows you to take this information, check for errors and display in a human readable format. Using the decoder AVPs can be bulk imported into existing Request profiles to quickly allow you to simulate or replay requests from a wide range of NASes.

Note: RadiusNT/X packet debug is enabled by including the '–X' flag from the command line. For example 'radius –x15 –X' starts radius in debug 15 mode with packet debugging enabled.

Accounting Listeners

Listeners provide a means of monitoring remote systems for important events. Once received these events are translated into RADIUS/AAA accounting requests for reporting and billing purposes.

Asterisk Call Detail Records (CDR)

Currently the Asterisk Manager API is the only supported listener type enabling an Asterisk PBX system to collect CDR and other available event data in real-time.

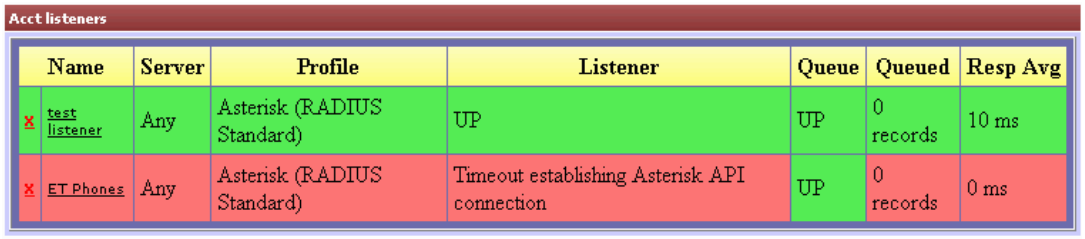
The request profile system translates data collected by the listener to RADIUS attributes needed to communicate events as RADIUS accounting messages. See request profiles for more information configuring profiles. All event data available as variables in each event; built-in profile variables and the table of special request variables below can be used within the profile for each listener.

Variable Name	Type	Event	Description
Listenipaddress	Asterisk	All Events	IP Address of configured listener typically used as NAS-IP-Address (NAS-Identifier)
Listenusername	Asterisk	Cdr	Reflects users phone number by matching Source/Destination against 'from-internal' Context.
Listencallerid	Asterisk	Cdr	Reflects users calling number by matching Source/Destination against 'from-internal' Context.
Listendnis	Asterisk	Cdr	Reflects users called number or 'INCOMING CALL' for incoming calls by matching Source/Destination against 'from-internal' Context.

Two asterisk request profiles are included by default. 'Asterisk (RADIUS Standard)' translates asterisk CDR events to standard attributes all RFC 2866 compliant RADIUS/AAA systems understand. If you will be integrating Asterisk with the Emerald Management Suite this profile should be used. A secondary profile 'Asterisk (Digium VSA)' is also available which translates CDR events to asterisk specific VSAs for systems specifically requiring them. Each of the default request profiles can be customized as needed to provide the desired RADIUS accounting attributes.

Note: CDR manager event logging must be enabled by editing the file /etc/asterisk/cdr_manager.conf on the asterisk server to reflect the following setting:

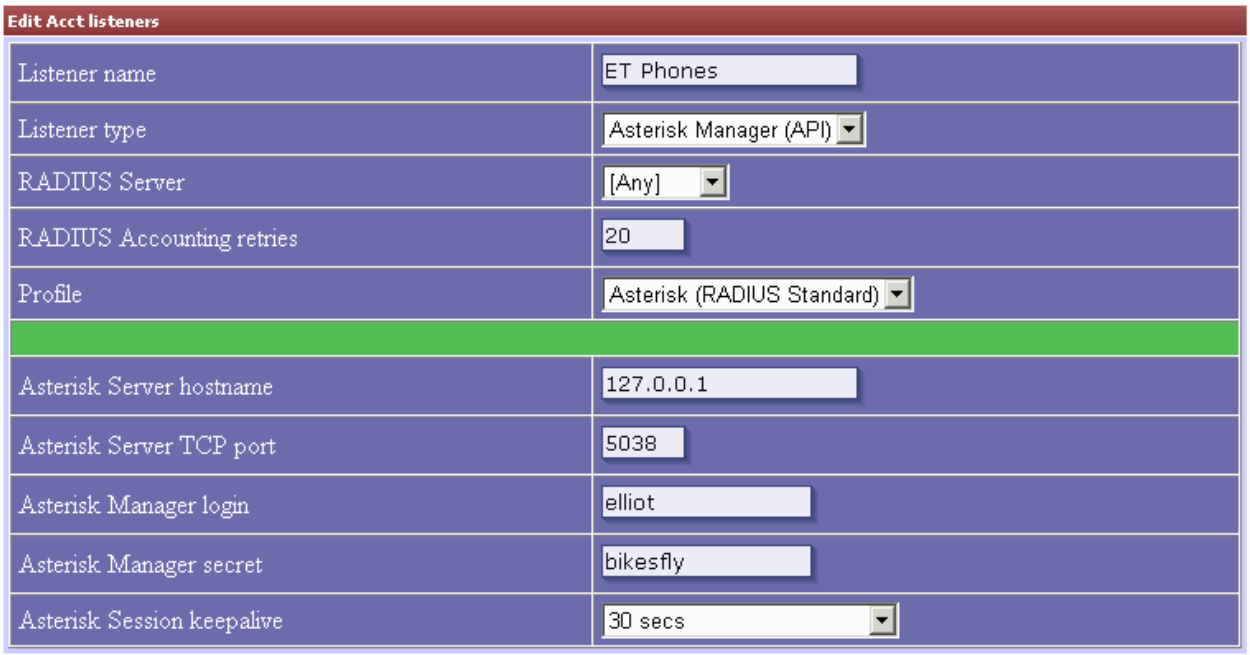
```
[general]
enabled = yes
```



Option	Description
Name	Listener server description

Server	RADIUS server(s) accounting requests are to be routed.
Profile	Request profile used by the listener to map events to RADIUS attributes
Listener	Listener status normally 'UP' with a green background indicates good connection with the listener actively receiving events. If the listener field has a red background the text contained within indicates an error condition that must be resolved before events can be recorded.
Queue	RADIUS accounting queue status normally 'UP' with a green background indicates accounting messages are successfully being record by the RADIUS server. If the Queue field has a red background the text contained within indicates an error condition that must be resolved before queued accounting records can be delivered successfully to the RADIUS server.
Queued	Number of listener event messages currently queued for upload to the RADIUS server.
Resp Avg	Average response time in milliseconds to RADIUS accounting requests sent to the RADIUS server.

To add a new listener click the add link besides the Listener menu item.



Option	Description
Listener name	Short text describing the asterisk server and purpose of the listener.
Listener type	Type of listener, currently Asterisk Manager API is the only available type.
RADIUS Server	Specifies RADIUS server collected event are to be sent. If RADIUS Server is set 'Any' all configured and available RADIUS servers can be used to provide fault tolerance.
RADIUS Accounting retries	Number of accounting retries attempted before discarding a queued accounting record. Note: Each try in this context counts as failures of the entire failover and retry policy configured within the Radius Servers menu. A dynamic back-off mechanism is used between each try.

Profile	Request profile used to translate listener events to RADIUS attributes. For asterisk listeners the included Asterisk (RADIUS Standard) profile is the recommended default.
Asterisk Server hostname	IP address or hostname of the Asterisk server / manager API
Asterisk Server TCP port	TCP port number of the Asterisk server (default: 5038)
Asterisk Manager login	Asterisk Manager login name. Account must have permissions to read “Cdr” events. Write access is not required.
Asterisk Manager secret	Asterisk manager password for login field above
Asterisk Session Keepalive	Interval application keepalives are sent over the Asterisk Manager interface to verify connection status and application state during periods where no events are actively sent. The default and recommended value is 30 seconds.