

S08- SIMPLer RADIUS RADIUS Server Integration

Azotel Technologies Ltd,
3rd Floor, River House,
Blackpool Park,
Cork,
Ireland.

Azotel Canada Inc.
325 Vulcan Avenue
NS B1P 5X1
Sydney
Canada

Azotel Poland
PLAC Powstancow
Slaskich 17A/222
53-329
Wroclaw
Poland

Phone (EMEA): +353-21-234-8100
Phone (North America): +1-902-539-2665 / +1-312-239-0680
Phone (Poland): +48-71-710-1530
Phone (UK): +44-20-719-3417
Phone (South Africa): +27-11-083-6900
Fax: +353-21-467-1699

info@azotel.com

www.azotel.com

Contents

Contents	2
1 Introduction	4
2 SIMPLer RADIUS Solution Overview	6
3 Setting up RADIUS server database interface in SIMPLer	7
3.1 Default RADIUS database interface	7
3.2 Operator-wise RADIUS database override	7
3.3 WIB RADIUS interface settings	8
4 Setting up RADIUS server database interface in SIMPLer	10
4.1 RADIUS Databases	10
4.2 Network Access Servers (NAS)	11
4.3 IP Pools	12
4.4 Individual Check	13
4.5 Individual Reply	14
4.6 Post Authorization	15
4.7 User / Group Assignment	16
4.8 Group Details	17
4.9 Group Check	17
4.10 Group Reply	18
4.11 Usage Details	20
5 Customer RADIUS Settings Management	21
5.1 Customer Details Page	21
5.2 Customer Details Page: Updates	22
5.3 Customer RADIUS Details page	23
5.4 Customer RADIUS Usernames	25
5.5 Deleting IP Details When Disconnecting Customers	25
5.6 Generate Default Password Option	26
5.7 Customer RADIUS Checks	27
5.8 Customer RADIUS Replies	29
5.9 Customer IP Table synchronization	30
5.10 Customer Account Links on Management Pages	31
6 Dictionary references	32
7 Quick Start	34
7.1 Set UP NAS in the SIMPLer platform	34
7.2 Setup the NAS to talk with the RADIUS server	36
7.3 Group Setup	38
7.4 Gateway Setup	44
7.5 Customer Setup	46
7.6 Test the setup	50
8 RADIUS Proxy Setup	51
8.1 FreeRADIUS installation on CentOS system	51
8.2 NAS setup in SIMPLer	51
8.3 FreeRADIUS setup	52
8.4 RADIUS: Service Log	52
8.5 Auto RADIUS Groups (From Traffic Shaping Buckets)	54
Annex A: References	58
A.1 Document References	58

A.2	Link References	58
Annex B:	Definitions and abbreviations	58
B.1	Definitions	58
B.2	Abbreviations	58
Annex C:	Sample proxy.conf file	58
Annex D:	Change history.....	63

1 Introduction

The purpose of this document is to provide detailed instructions on how to use the Azotel SIMPLer system with RADIUS Server additions integrated with a FreeRADIUS server instance which can either be Azotel's SIMPLer embedded FreeRADIUS server or a remote FreeRADIUS server instance hosted by the operator. The integration of the RADIUS services to the Azotel SIMPLer platform was driven by requirements of a number of WISPs.

RADIUS is a networking protocol providing centralized Authentication, Authorization, and Accounting (AAA) management information services for the end-user equipment to connect and use a network service. RADIUS protocol is broadly supported and has a ubiquitous nature due to which it is often used by ISPs to manage access to the Internet, internal networks, wireless networks or even e-mail services. Various devices can benefit from using RADIUS: modems, DSL, access points, VPNs, wireless networks, etc.

FACT: RADIUS provides three key functionalities:

- **authenticating** users or devices before granting them access to a network
- **authorizing** users or devices for certain network services, resources
- **accounting** for usage of previously authorized services

By design RADIUS is a client/server protocol using UDP packets as transport. Each *Network Access Server* (Access Point, PPPoE server, DSL server, hotspot controller, network switch with port-based authentication, VPN server etc.) has a RADIUS client module to communicate with the RADIUS server.

The AAA concept of managing networks is based on a two-step process:

- **step one- Authentication and Authorization.** In this step the end-user sends a request containing access credentials to a NAS in order to gain an access to a particular resource. Depending on the NAS type this operation takes place using a different link-layer protocol i.e. *https web form* in case of hotspots or *via PPP* packets in case of DSL or dialup. In turn, the NAS sends an "**Access Request**" message to the RADIUS server. This request contains access credentials typically in the form of a username and password provided by the end-user. There might be some additional information about the user added by the NAS to the access request i.e. IP address, MAC address of the user etc. The RADIUS server verifies the received information against the "Check" attributes defined against the respective end-user account. Usually username and password credentials are verified but there might be some additional checks performed if there are more "Check" attributes specified i.e. MAC address or resources current usage limit might be verified. Depending on the result the RADIUS server returns one of three responses to the NAS:
 - **Access Reject** – access denied to all network resources requested
 - **Access Challenge** – some additional information is requested. This response is usually sent in more complex authentication dialogs where access credentials are hidden from the NAS, in such cases the additional information is sent via a secure tunnel established between the end-user and RADIUS
 - **Access Accept** – access is granted. The RADIUS server often will perform a set of checks once the user is authenticated to verify what network resources the user is authorized to use. In other words what is the end-users level of service. All this information is passed back to the NAS in the "**Access Accept**" reply. Examples of the information passed back in the Access Accept reply would be:
 - user Quality of Service (QoS) settings
 - traffic allowances
 - user dedicated IP address
 - session termination time
 - access lists
 - and many more

For further information please refer to RFC 2865 regulation: <http://tools.ietf.org/html/rfc2865>

- **step two- Accounting.** Once access to network resources is granted to the end-user by the NAS an “**Accounting Start**” package is sent by the NAS to the RADIUS server and this signals the start of the end-user session. In most cases the session data sent over will contain usage data information, unique session identifier, unique network identification (MAC address, IP address), details of the NAS the end-user is connecting through etc. For each open session “**Interim Update**” records are sent by the NAS to the RADIUS server periodically. These records update the session usage data on the RADIUS server. When the user access is closed the NAS will send an “**Accounting Stop**” packet to the RADIUS server which closes the particular session with the final usage data (session time, packets transferred, data transferred, disconnection reason etc).

Each accounting packet is answered by the RADIUS server with an “**Accounting Response**” packet acknowledgement.

For further information please refer to RFC 2866 regulation: <http://tools.ietf.org/html/rfc2866>

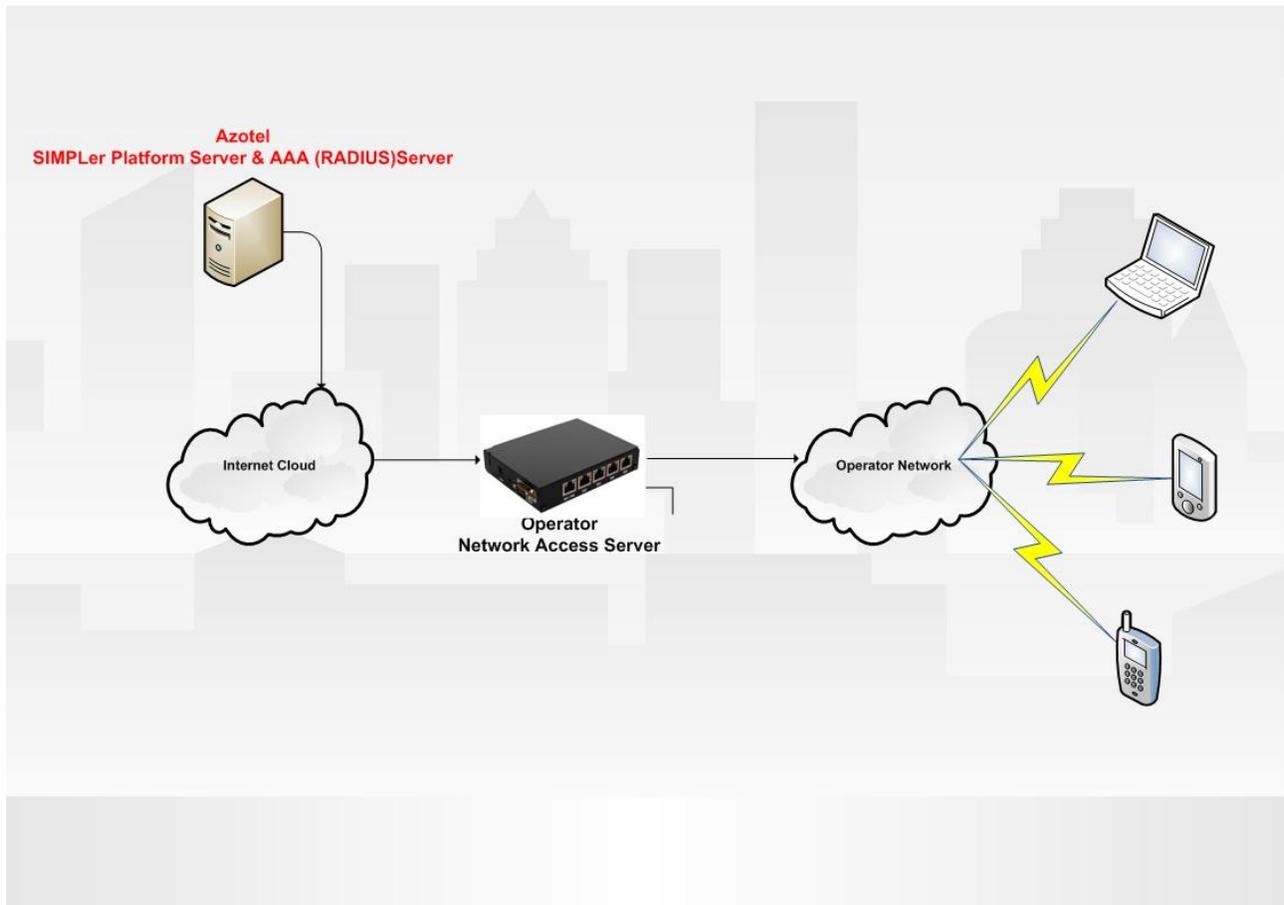


Figure 1-1 Basic RADIUS server based operator network layout

2 SIMPLer RADIUS Solution Overview

Every SIMPLer platform server has a RADIUS server instance installed and already integrated with the SIMPLer software. It provides RADIUS services on the respective SIMPLer server IP address via UDP on following, default ports:

- *port 1812* - used for authentication and authorization
- *port 1813* - used to collect accounting data

NOTE: Only the host specified in the NAS table will be allowed to use the SIMPLer server embedded RADIUS services on ports 1812 and 1813. Adding RADIUS clients to NAS table is outlined in chapter 4.2 of this manual.

The RADIUS server embedded in the SIMPLer platform is based on a FreeRADIUS software release which is a de facto standard for majority of current RADIUS server deployments.

The SIMPLer software can also interface with an external FreeRADIUS database / server giving a full flexibility when integrating already existing networks with the billing platform. In many cases operator may prefer to use his own FreeRADIUS server as there may be some specific configuration set on the server required to interface with the managed equipment. In such cases the only thing required from SIMPLer perspective would be a remote access to RADIUS database. Both postgresSQL and MySQL database engines are supported with other database interfaces could be added if required.

Other option to integrate a remote RADIUS server (especially if other than FreeRADIUS) would be to use the RADIUS proxy capabilities.

3 Setting up RADIUS server database interface in SIMPLer

3.1 Default RADIUS database interface

The SIMPLer system will use the embedded FreeRADIUS server by default for all operators. Operator can interface to the embedded RADIUS server by setting up the Network Access Equipment to use:

- SIMPLer platform server IP address as a RADIUS server IP address (i.e. wib.azotel.com)
- Port 1812 for the Authentication and Authorization
- Port 1813 for the Accounting
- Password as specified under NAS section in the SIMPLer – outlined in section 4.2 of this document

Using the SIMPLer’s embedded RADIUS server is the fastest way to get up and running, but for some more specific solutions, where certain authentication methods are to be used between RADIUS and the NAS, Azotel would encourage to use a hosted FreeRADIUS solution as no operator-specific changes will be made to the SIMPLer embedded RADIUS server configuration.

Note: RADIUS settings need to be defined for a gateway in SIMPLer platform before the AAA services can be assigned to a customer account in the SIMPLer platform. For more details please refer to 3.3 chapter of this manual

3.2 Operator-wise RADIUS database override

Operator can decide to use his own, dedicated FreeRADIUS based AAA server that would only be used by operators equipment. In such scenario SIMPLer would interface with the remote server’s database. There are two conditions to be met in this scenario:

- Remote RADIUS server has to be **FreeRADIUS software based**
- **Postgresql** or **MySQL** database engines are to be used and a remote access to the database needs to be granted for the SIMPLer platform IP address

The remote RADIUS server details can be specified for an operator in SIMPLer platform under the “**RADIUS Server Settings**” section of the “**Modify WISPs**” page (“**Settings -> Modify WISP details >>**”).

The screenshot shows a web interface for configuring RADIUS server settings. At the top, there is a header with 'FTP Server: Username' and a dropdown menu set to 'no', and a text input field containing 'azotel'. Below this is a section titled 'Radius Server Settings ?' with a red border. The settings are organized into two columns. The first column lists various RADIUS parameters, and the second column contains input fields, dropdown menus, and checkboxes. The 'Override SIMPLer Default Radius Server (demo.azotel.com)' checkbox is checked. Below the RADIUS settings is a section for 'Hotspot Settings ?' with an 'External Radius Server: Database Name' field.

Figure 3.2-1 “RADIUS Server Settings” section on the “Modify Operator Details” page

Note: If the override option is not enabled, SIMPLer platform will use embedded FreeRADIUS database by default

Following details need to be specified in order to set up the remote FreeRADIUS server database interface:

- **Override SIMPLer Default RADIUS Server** – system will override the SIMPLer default RADIUS server details and use a remote RADIUS server settings if this option is set, otherwise SIMPLer will interface with embedded RADIUS server database
- **RADIUS Server IP Address** – remote RADIUS servers IP address. Note, that this IP address is used to access the FreeRADIUS database remotely (not the server itself), hence in some cases (when the database is separate to the actual FreeRADIUS server implementation) this might be different, that the RADIUS service servers IP address.
- **RADIUS Server Database** – remote RADIUS servers database name
- **RADIUS Server Database Type** – remote RADIUS servers database engine type. Two database engines with a possibility to add additional engines in a limited timeframe are currently supported by the system:
 - PostgreSQL
 - MySQL
- **RADIUS Server Username** – username used to connect with the remote RADIUS server database
- **RADIUS Server Password** – password used to authenticate the username when connecting with the remote RADIUS server database

3.3 WIB RADIUS interface settings

SIMPLer is built around a concept of gateways. A gateway may be an actual piece of equipment (i.e. a WIB-C controller) or just a “virtual” device used to define a set of parameters to a customer account. The set of RADIUS server services is defined for each gateway and subsequently to each customer account that has the particular gateway assigned. Current set of gateways RADIUS services can be modified under “*network -> gateways details -> modify gateway*” page. This in turn defines which RADIUS services will be available to a customer that has the gateway assigned. There are three base RADIUS modules:

- **Authentication Module** – base RADIUS service, it has to be enabled in order to use remaining RADIUS services (Authorization, Accounting). Authentication provides a set of values required to authenticate the user i.e. define a username / password token and maybe some additional checks (in some special cases)
- **Authorization Module** – RADIUS service that authorizes a set of services to the equipment. e.g. the maximum upstream speed, the maximum downlink speed, traffic allowance etc. There is a set of generic attributes that might (but does not have to) be supported by various equipment, there may also be a ‘per-equipment-type’ dictionaries required in some cases (i.e. QoS classes definitions for Motorola P320). Turning this option on in SIMPLer platform will add RADIUS Reply options when setting up a customer
- **Accounting Module** – RADIUS service that gathers customer session data. If this option is checked, SIMPLer will generate customer usage graphs (and summary bucket and gateway traffic graphs for “virtual” gateways) from the RADIUS accounting data. Otherwise SIMPLer will generate the graphs based on traffic data polled from WIB-C client. Note that SIMPLer system will collect and store the session data in the freeRADIUS database regardless of this setting.

To add more flexibility to the system, there is an “*Override Operator Default RADIUS Server*” option available to specify a RADIUS server override on per-wib client basis. Such option would come in handy when operator is dealing with multiple networks spread geographically and using a dedicated RADIUS server for each of deployments. Using this feature operator will be in position to address all his remote deployments keeping the RADIUS databases separate for each geographical deployment. Again note that SIMPLer will only interface with FreeRADIUS software based on the PostgreSQL or MySQL database engines. Following details need to be specified in order to set up the per-wib remote RADIUS server interface override:

- **Override SIMPLer Default RADIUS Server** – system will override the operator RADIUS server details and use a remote RADIUS server settings if this option is set, otherwise SIMPLer will interface with operator default RADIUS server accordingly to the settings described in chapter 3.2 of the following manual
- **RADIUS Server IP Address** –remote RADIUS servers IP address. Note, that this IP address is used to access the FreeRADIUS database remotely (not the server itself), hence in some cases (when the database is separate

to the actual FreeRADIUS server implementation) this might be different, that the RADIUS service servers IP address.

- **RADIUS Server Database** – remote RADIUS servers database name
- **RADIUS Server Database Type** – remote RADIUS servers database engine type. Two database engines with a possibility to add additional engines in a limited timeframe are currently supported by the system:
 - PostgreSQL
 - MySQL
- **RADIUS Server Username** – username used to connect with the remote RADIUS server database
- **RADIUS Server Password** – password used to authenticate the username when connecting with the remote RADIUS server database

Network Details

Public IP address / ?

Upstream gateway

Secondary gateway

Primary DNS

Secondary DNS

RADIUS Server

Authentication Module Enabled ?

Authorization Module Enabled ?

Accounting Module Enabled ?

Override Operator Default Radius Server

Send COA / Disconnect Packets to NAS

Radius Server IP Address

Radius Server Database

Radius Server Database Type

Radius Server Username

Radius Server Password

Override Operator Default Accounting Database

Accounting Database IP Address

Accounting Database Name

Accounting Database Type

Accounting Database Username

Accounting Database Password

[WIB Gateway Log Files ?](#)

Figure 3.3-1 “RADIUS Server” section on the “Modify Gateway Details” page

4 Setting up RADIUS server database interface in SIMPLer

The base page for managing the RADIUS servers can be found under the **“RADIUS”** link in the SIMPLer platforms’ top menu. From there operator can browse, add and change every aspect of each FreeRADIUS database SIMPLer interfaces with. The management pages will give a full insight at what is the current configuration of the RADIUS database.

Note: there is one assumption that has been made across all RADIUS management pages in SIMPLer platform. All groupnames, NAS shortnames and IP Pool names will be preceded with the **“operatorname_”** prefix (i.e. in case of **“testss”** operator the prefix used across the board will be **“tests_”**). This assumption has been made to enable sharing one RADIUS database / server instance by multiple operators. All prefixes will be added automatically, so this does not require any additional action from operator. SIMPLer will present only a subset of data relevant to the operator using these prefixes as a filter.

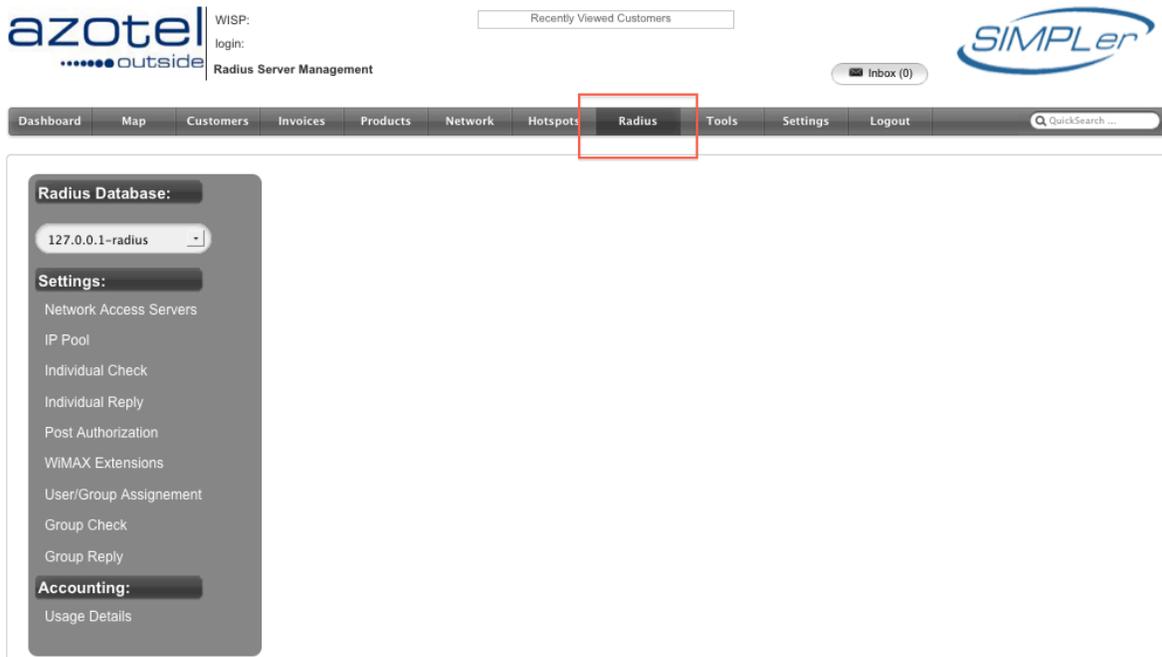


Figure 4-1 “RADIUS Server Management” page

4.1 RADIUS Databases

By default there will be only one RADIUS database (local **“RADIUS”** database for embedded FreeRADIUS server) available under the operator account in SIMPLer. Given the operator can define a separate RADIUS database instance for each gateway position and by this use multiple RADIUS server database instances, using the **“RADIUS Server Database”** dropdown on each of the pages, operator can define which database he wants to work at the moment. This dropdown menu is available across all the RADIUS management pages.

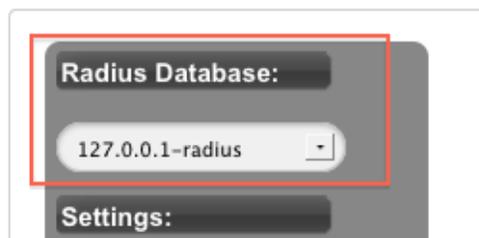


Figure 4.1-1 Dropdown menu with available databases

4.2 Network Access Servers (NAS)

A **Network Access Server (NAS)** is a device that provides access to network resources. It may also be known by the name **Remote Access Server (RAS)** or **Terminal Server**. Acting as a gateway the NAS guards access to a protected network resource (i.e. Internet, access to AP, email account etc). NAS stores no information about the customers and resources that are available for them. External AAA server is required for NAS to work. The typical session authenticating and authorizing the end user starts with the client connecting to the NAS device which in turn connects to the RADIUS server asking whether the client's supplied username and password are valid (there might be some other checks involved, but this is a bare minimum). Based on the answer given the NAS then allows or denies access to the requested resource (such as Internet). NAS may also utilize some additional information sent from the AAA server and set some service specific parameters according to these. When authenticated, NAS will start sending session usage data to the RADIUS server.

Figure 4.2-1 “Network Access Servers” page

Note: Each NAS server has to be added to the NAS table in SIMPLer otherwise any query coming from the particular NAS will not be processed by FreeRADIUS server.

Operator can add a NAS to the RADIUS database from “radius -> Network Access Server” page. There is following set of parameters to be set for each new NAS position:

- **IP Address / Hostname** – (**mandatory**) network address the NAS will access the RADIUS server from. This information needs to be accurate as otherwise NAS will not be able to process any RADIUS queries. **Note** this address needs to be the address that RADIUS requests will appear to be coming from. If the NAS is behind a NAT firewall, the IP address would be that of the firewall, and not the private IP address assigned to the NAS.
- **Name** – (**mandatory**) NAS name under which it will be displayed in the system. It can be set up to operator liking as it does not take part in the NAS authentication process, though it is required for cross-referencing in the SIMPLer platform
- **Type** – (**mandatory**) NAS device type. RADIUS server has a predefined set of the equipment it works with. If the equipment type is not on the list it is safe to use “**other**” type (default). The equipment type defines if there are any equipment specific method to use to query the NAS for simultaneous use information
- **Secret** – (**mandatory**) secret word the NAS will use to “encrypt” and “sign” packets between NAS and FreeRADIUS. Note that the same secret word has to be used on the NAS in the RADIUS server configuration section
- **Port** – the port number RADIUS connect to the NAS. Might be required in some cases, but this should be left blank in vast majority of cases. Might be required when using IP Pools
- **Community** - The community string used by the NAS for queries via snmp. Might be required in some cases, but this should be left blank in vast majority of cases
- **Description** – description field

Note: When adding a new NAS (hotspot, PPPoE gateway, AP with authentication support) to operator network it is essential to add a respective position to the “*Network Access Server*” in SIMPLer and than in turn filling out the RADIUS server section on the NAS with the respective data.

4.3 IP Pools

Note: The IP Pools module may not be available on every FreeRADIUS servers instance. Only available where rlm_ippool module is installed. The FreeRADIUS server embedded in SIMPLer platform server supports this feature.

FreeRADIUS software supports ability to assign dynamic IP address to RADIUS sessions in cases where the particular NAS controller supports assigning the IP addresses based on the information acquired from RADIUS server. Such feature can be utilized widely by PPP servers and all other types of dialup access. There is also a possibility to interface to the RADIUS server from certain DHCP servers resulting in a fully scalable network addressing solution.

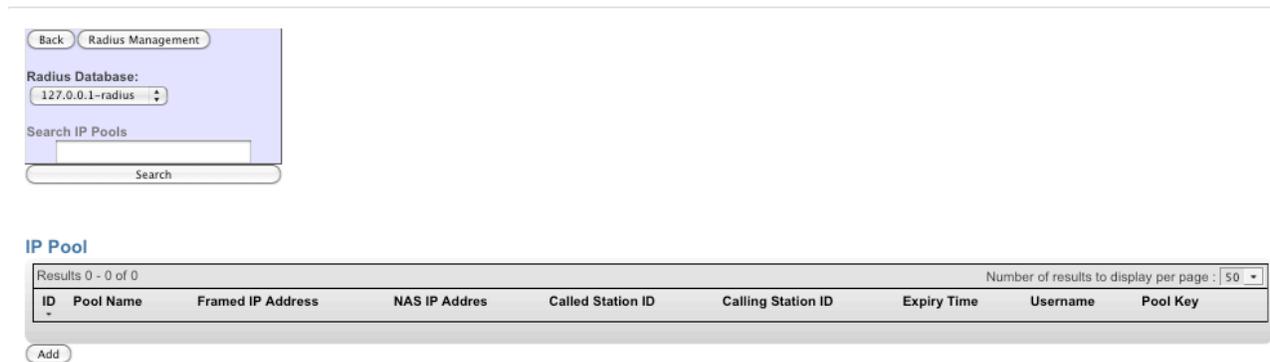


Figure 4.3-1 “IP Pools” page

IP Pools are assigned with the specific Pool-Name attribute. This name is than used to assign a customer or a usergroup a Pool by using two (one RADIUS check and one RADIUS reply) attributes (adding RADIUS checks and replies is covered in chapter 4.4, 4.5, 4.9, 4.10, 5.4, 5.5 of this manual):

- Pool-Name := POOLNAME
- Fall-Through = Yes

There is following set of parameters to be set for each new IP Pool position. Each IP Pool table row represents one IP address of an IP pool. The only fields required are **Pool Name** and **Framed IP address**. Note that addresses do not need to be contiguous and there is no restriction on which IP addresses or ranges may be in the same pool

- **Pool Name - (mandatory)** IP Pool name under which it will be displayed in the system. It can be set up to operator liking. The pool name than will be used to assign it to user (customer) or usergroup.
- **Framed IP Address - (mandatory)** a single IP address in the pool
- **NAS IP Address** – Using this parameter we can assign an IP Pool positions to defined NAS devices. This means that there might be a different sets of IP addresses handled within one IP Pool based on the NAS the query came from
- **Called Station ID** – Usually a MAC address of the NAS. Using this parameter we can assign an IP Pool positions to defined NAS MAC addresses. This means that there might be a different sets of IP addresses handled within one IP Pool based on the NAS the query came from
- **Calling Station ID** – Usually a MAC address of the User device. Using this parameter we can assign an IP Pool positions to defined user equipment MAC addresses. This means that there might be a different sets of IP addresses handled within one IP Pool based on the user equipment the query came from
- **Expiry Time** – Date the IP Pool position expires
- **Username** - Using this parameter we can assign an IP Pool positions to defined username (SIMPLer customer). This will create a set of IP addresses available only to a particular customer

- **Pool Key** – this variable allows to select which attribute is unique according to your NAS setup. On a standard Ethernet or wireless network most probably it will be “Calling-Station-Id” but on a dialup NAS this is going to be “NAS-Port”. It is required for the key to be unique. It also must be received in both Access-Request and Accounting packets. Reason for above is that system must know to clear the IP lease when session disconnects.

Figure 4.3-2 “Modify IP Pool” page

4.4 Individual Check

This section of SIMPLer RADIUS pages lists the “*check*” attributes. Note that these can be added to the system only from the actual SIMPLer customer account radius section as described in 5.4 section of this manual. The general “Individual Chack” page only allows to edit the existing positions. The attributes of this type are taking part in the Authentication process. All these attributes will be checked before RADIUS authenticates the end-user. Depending on the result of these checks end-user will be granted or rejected access to the network. A good example of a check attribute usage is “*Cleartext-Password*” attribute which defines the password for a particular user and by that it defines an effective username / password access token in the RADIUS server.

ID	Username	Attribute	Op	Value
3331	00:11:22:33:44:55	Cleartext-Password	:=	
3332	testss_IB1	Cleartext-Password	:=	test1
13371	testss_Bill2	Cleartext-Password	:=	

Figure 4.4-1 “Individual Checks” page

Full list of the FreeRADIUS basic check / reply attributes combined can be found under the below pages:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

There is following set of parameters describing each RADIUS check position:

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Username** – unique username as defined in the SIMPLer’s customer account
- **Attribute** – attribute we wish to assign. SIMPLer uses FreeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from dropdown menu. “*Dictionary*” dropdown can be

used to narrow down the Attributes listed in the Attribute dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (*FreeRADIUS-Internal*, *WISPr*, *RFC2865* and *RFC2866*) in the “Dictionary” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value to check against

Figure 4.4-2 “Modify Individual Checks” page

4.5 Individual Reply

This section of SIMPLer RADIUS pages manages the “reply” attributes. Note that these can be added to the system only from the actual SIMPLer customer account radius section as described in 5.5 section of this manual. The general “Individual Reply” page only allows to edit the existing positions. The attributes of this type are taking part in the Authorization process. All these attributes will be used by RADIUS server to authorize network resources or level of service to the customer. A good example of a reply attribute usage is “*Framed-IP-Address*” attribute which defines an IP address the NAS gateway should assign to a the particular customer given that this feature is supported.

ID	Username	Attribute	Op	Value
149	testss_JB1	Framed-IP-Address	=	84.203.148.72

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 4.5-1 “Individual Reply” page

Full list of the FreeRADIUS basic check / reply attributes combined can be found under the below pages:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

<http://tools.ietf.org/html/rfc2866>

There is following set of parameters describing each RADIUS reply position:

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Username** – unique username as defined in the SIMPLer’s customer account
- **Attribute** – attribute we wish to authorize. SIMPLer uses FreeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from dropdown menu. “*Dictionary*” dropdown can be

used to narrow down the Attributes listed in the Attribute dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (*FreeRADIUS-Internal*, *WISPr*, *RFC2865* and *RFC2866*) in the “Dictionary” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value the authorization attribute is set to

Figure 4.5-2 “Modify Individual Replies” page

4.6 Post Authorization

RADIUS Post Authorization page provides a listing tool to a respective table in the FreeRADIUS database. This page lists all the Authentication / Authorization attempts regardless of the result. It may be used for example as a nice tool to identify the failed / successful authentication attempts. Each Post Authorization position contains following details:

- **ID** - unique identifier assigned automatically by SIMPLer system
- **Username** – username the end-customer attempted to authenticate with
- **Password** – password the end-customer attempted to authenticate against the username
- **Reply** – the reply message as send to the NAS. Can be one of the following:
 - Access Reject
 - Access Challenge
 - Access Accept
- **Auth Date** – the exact date and time the request was processed by the RADIUS server

Figure 4.6-1 “Post Authorization” page

4.7 User / Group Assignment

SIMPLer RADIUS implementation supports grouping customers. Customer account inherits all the settings from the group he is assigned to. There might be a several groups defined in the system.

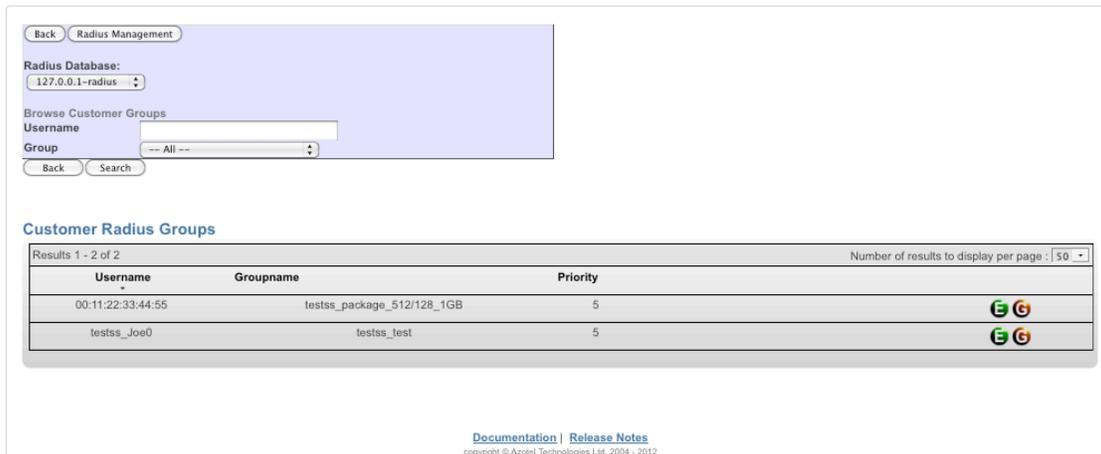
Note: Using groups as much as possible is a recommended approach for creating service level profiles using RADIUS servers i.e. defining QoS settings like the upload, download speeds and traffic limits where supported.

Note that a single customer can have multiple groups assigned. In such case the priority of a group decides which attribute value takes precedence in case of a multiple occurrence of an attribute across the groups.

Also note that individually defined attributes take precedence over any group attributes. RADIUS server will evaluate all the “check” and “reply” attributes assigned to all the groups of the end-user account along with his individually defined checks and replies.

Each row in the “User / Group Assignment” page represents one user to group assignment with a priority defined. From this page operator can edit the assignment details through the green “E” button or edit the particular group attributes such as “check” and “reply” items under “G” button. Operator can also browse the existing entries using the embedded search facility.

Note that new User / Group assignment can be added to the system only from the actual SIMPLer customer account radius section as described in 5.2 section of this manual. The general “User / Group Assignment” page only allows to edit the existing positions.



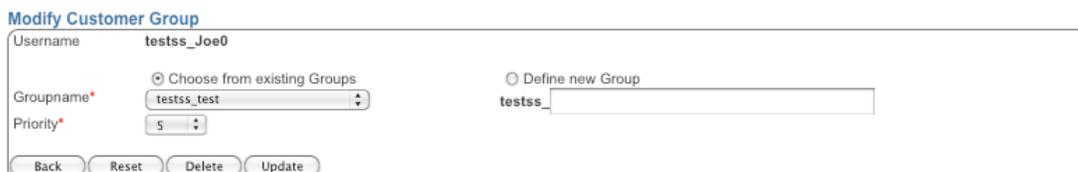
The screenshot shows the 'Radius Management' section with a search form for customer groups. Below the search form is a table titled 'Customer Radius Groups' with the following data:

Username	Groupname	Priority	
00:11:22:33:44:55	testss_package_512/128_1GB	5	 
testss_Joe0	testss_test	5	 

Figure 4.7-1 “User Groups” page

Each User Group position is described by following details:

- **Username** - unique username representing a SIMPLer customer. Generated by combining operator name with the customer nickname (defined under customer details).
- **Groupname** – defines group the customer will be assigned to. There are two ways to specify a group name. It can be chosen from the groups already existing in the system or operator can choose to create a new group by selecting the “Define new Group” radiobutton and filling out the entry box below
- **Priority** – priority of the group to user assignment. The priority field of the group table defines the order in which groups are processed – lower number equals higher priority. In another words this value will be used to create a precedence in case of one attribute being defined across multiple groups



The screenshot shows the 'Modify Customer Group' form with the following fields and options:

- Username: testss_Joe0
- Groupname: Choose from existing Groups (dropdown menu showing 'testss_test') or Define new Group (text input field with 'testss_' prefix)
- Priority: 5
- Buttons: Back, Reset, Delete, Update

Figure 4.7-2 “Modify User Group” page

Operator can define the attributes assigned to a group using the “G” button which links to “Group Details” page used to manage the group settings as defined in chapter 4.8 of this manual

4.8 Group Details

The “Group Details” page that can be accessed from various other RADIUS management pages, lists all settings relevant for a particular group, such as:

- Customer accounts assigned to the group
- Check attributes assigned to the group
- Reply attributes assigned to the group

Note: When working with RADIUS databases containing large numbers of groups, operator can modify the “checks” and “reply” items assigned to a particular group more efficiently via this page than via “Group Check” or “Group Reply” pages described respectively in chapters 4.9 and 4.10 of this manual. As when editing these positions from this page, the groupname field will be automatically filled in when editing the “check” or “reply” positions from this page.

Group Details

Groupname	testss_test
Assigned to	1 customer(s)
Radius Checks	0
Radius Replies	2

Back Back to customer

Radius Checks (modify...)

ID	Groupname	Attribute	Op	Value
No entries found in the database				

Radius Replies (modify...)

ID	Groupname	Attribute	Op	Value
427	testss_test	Framed-Pool	=	authenticatedCustomer
429	testss_test	Idle-Timeout	=	200

Customers Assigned

Username
testss_Joe0

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 4.8-1 “Group Details” page

4.9 Group Check

This section of SIMPLer RADIUS pages manages the “check” attributes defined for a particular group. The attributes of this type are taking part in the Authentication process. Operator can assign “check” attributes to a particular group using the “Group Check” page. When authenticating end-user account RADIUS server in addition to the individual “checks” will search for all groups assigned to the particular account and use in the process all the “check” defined for them. Depending on the result of these checks end-user will be granted or rejected access to the network.

A good example of a group check attribute usage is “Simultaneous-Use” attribute which defines whether the user can login using the same token for multiple devices simultaneously. Full list of the FreeRADIUS base check / reply attributes combined can be found under the below page:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

Back Radius Management

Radius Database:
127.0.0.1-radius

Browse Group Checks
Attribute
Value
Search

Group Check

Results 1 - 3 of 3 Number of results to display per page: 50

ID	Groupname	Attribute	Op	Value	
171	testss_package_512/128_1GB	Simultaneous-Use	:=		E
172	testss_package_512/128_1GB	Acct-Input-Octets	<=	1000000000	E
173	testss_package_512/128_1GB	Acct-Output-Octets	<=	1000000000	E

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 4.9-1 “Group Check” page

There is following set of parameters to be set for each group check position. Note that all the fields are required to create a valid table entry.

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Groupname** –name of a group the attribute is assigned to. There are two ways to specify a group name. It can be chosen from the groups already existing in the system or operator can choose to create a new group by selecting the **“Define new Group”** radiobutton and filling out the entry box below
- **Attribute** – attribute we wish to assign. SIMPLer uses FreeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from the dropdown menu. **“Dictionary”** dropdown can be used to narrow down the Attributes listed in the main **“Attribute”** dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (**FreeRADIUS-Internal**, **WISPr**, **RFC2865** and **RFC2866**) in the “Dictionary” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value to check against

Add Group Radius Check

Choose from existing Groups Define new Group

Groupname* testss_package_512/128_1GB testss_

Attribute* Simultaneous-Use Dictionary

Op* := FreeRADIUS-Internal

Value*

Back Reset Add

Figure 4.9-2 “Add Group Check” page

4.10 Group Reply

This section of SIMPLer RADIUS pages manages the **“reply”** attributes defined for a particular group. The attributes of this type are taking part in the Authorization process. Operator can assign “reply” attributes to a particular group using the **“Group Reply”** page. When authorizing end-user services RADIUS server in addition to the individual “reply” attributes will search for all groups assigned to a particular account and use in the process all “reply” items defined for them. The information about authorized services is then sent to the NAS which in turn grants the end-user a personalized access to the network resources.

A good example of a group reply attribute usage is **“WISPr-Bandwidth-Max-Down”** attribute from **“WISPr”** attributes dictionary which defines the maximum authorized download speed for the end-user. If the NAS supports this feature it

will limit the end-user download speed to the value specified for this attribute. Full list of the FreeRADIUS base check / reply attributes combined can be found under the below page:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

<http://tools.ietf.org/html/rfc2866>

ID	Groupname	Attribute	Op	Value
386	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Down	=	512000
387	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Up	=	128000
427	testss_test	Framed-Pool	=	authenticatedCustomer
428	testss_package_512/128_1GB	Idle-Timeout	=	120
429	testss_test	Idle-Timeout	=	200

Figure 4.10-1 “Group Reply” page

There is following set of parameters to be set for each group check position. Note that all the fields are required to create a valid table entry.

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Groupname** –name of a group the attribute is assigned to. There are two ways to specify a group name. It can be chosen from the groups already existing in the system or operator can choose to create a new group by selecting the “**Define new Group**” radiobutton and filling out the entry box below
- **Attribute** – attribute we wish to assign. SIMPLer uses FreeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from the dropdown menu. “**Dictionary**” dropdown can be used to narrow down the Attributes listed in the main “**Attribute**” dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (**FreeRADIUS-Internal**, **WISPr**, **RFC2865** and **RFC2866**) in the “Dictionary” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value of the authorize attribute

Figure 4.10-2 “Add Group Reply” page

4.11 Usage Details

Usage details section of the RADIUS server management section is an interface to a RADIUS accounting data. As described the RADIUS has an ability to store the usage data of each session established through the NAS controllers. Note that the NAS needs to support this feature (i.e. Motorola P320 does not send any accounting data to the RADIUS servers, but vast majority of the RADIUS enabled equipment will). SIMPLer displays following session data from the RADIUS database:

- **Username** –unique username representing a SIMPLer customer account the session is created against. Generated by combining operator name with the customer nickname (defined under customer details).
- **Session Start** – exact date and time the session has been started
- **Session Stop** – exact date and time the session has been terminated. Note that for active sessions this parameter will be undefined
- **Session Time** – period the session is / was established for
- **Upload** – the uploaded amount of data
- **Download** – the downloaded amount of data
- **Calling Station ID** – the unique network identifier of the end-user equipment (i.e. MAC address)
- **IP Address** – the IP address of the end-user equipment

Username	Session Start	Session Stop	Session Time	Upload	Download	Calling Station ID	IP address	NAS IP Address
_radiusdest	2012-02-13 15:07:31+00	2012-02-13 16:17:17+00	01h 09m 45s	96.3 MB	343.9 MB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-13 10:20:44+00	2012-02-13 10:37:39+00	00h 16m 54s	423.6 KB	0.2 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-09 21:30:30+00	2012-02-09 21:31:20+00	00m 00m 50s	5.9 KB	0.1 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-09 21:28:21+00	2012-02-09 21:30:13+00	00m 01m 52s	18.2 KB	0.1 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-06 09:44:59+00	2012-02-06 09:46:25+00	00m 01m 26s	43.4 KB	0.1 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-06 09:43:09+00	2012-02-06 09:44:10+00	00m 01m 02s	60.0 KB	0.1 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-06 09:40:12+00	2012-02-06 09:40:53+00	00m 00m 42s	4.8 KB	0.1 KB	00:1E:68:E3:72:EF		
_radiusdest	2012-02-03 10:47:28+00	2012-02-03 10:49:15+00	00m 01m 46s	29.9 KB	0.1 KB	00:1E:68:E3:72:EF		

Figure 4.11-1 “Usage Details” page

The “Usage Details” page gives the operator the ability to browse through the session account data. As the quantity of this information builds to over time, when looking for specific information it is important to use the search abilities from the menu on top of the page to narrow down the results. Results can be narrowed to entries from the specified time period using the “Start Date” and “End Date” form fields or containing a string defined in the “Search” entry field. Using the blue menu of the left hand side, operator can define what session data to browse:

- **Active Sessions** – Browse the currently active sessions data. Using this option operator can quickly identify the users that are actively using the system.
- **All Sessions** – Gives access to all the session data recorded by the system from day one.
- **Unique Tokens** – Browse the summary usage data for the unique usernames – SIMPLer customers.

Operator can use the “Export Report” option on the “Usage Details” page to export the current data set as an Excel Spreadsheet. The exported data can then be mangled in an external software giving customized reports.

5 Customer RADIUS Settings Management

The RADIUS server is effectively authorizing, authenticating and accounting the data against the end-user account. Once the RADIUS system is set up and groups with their attributes are defined the majority of the RADIUS related actions are managing the customer settings. The recommended approach is to move as many “*check*” and “*reply*” attributes towards the groups as possible. In turn the groups should be assigned with the customer accounts. Individually assigned “checks” and “replies” should only be used when there is no other option. The only ‘per-customer’ defined attribute should be the password (which has a dedicated interface in the SIMPLer system described in chapter 5.3 of this manual).

To reiterate: The recommended approach to working with the SIMPLer interface to the RADIUS server is to use the RADIUS management pages to:

- Define the NAS entries
- Define IP Pools
- Define Groups and Group details
- Browse the Usage and Post Authorization data

While customer related actions (i.e. assigning groups, check and reply) are performed from the “*Customer Details*” page rather than from the generic “RADIUS” server pages. When accessing the “check”, “reply” attributes or assigning a group from “customer pages”, along with the customer information being displayed on each page the username field will be automatically filled in and locked down, which greatly improves the process with larger customer databases. Also this approach makes sure, that the customer related RADIUS records are put to a correct database in multi-database environments.

5.1 Customer Details Page

“*Customer Details*” page in SIMPLer platform contains a “*RADIUS Details*” in the “*Network*” section which lists all the relevant information about the RADIUS services available for the particular customer. Note that the RADIUS services and their respective management pages are available for a SIMPLer customer account only when the gateway assigned to the account has the particular services enabled. Hence the modules currently enabled on the gateway such as RADIUS Authentication, RADIUS Authorization or RADIUS Accounting are listed in the RADIUS Details section of the customer details page to enable operator spotting any possible issues with this part of customer RADIUS setup quickly.

Customer Network Details

Network Details (modify) (history)

Monitor	no monitor
Gateway	Test Gateway (wib-100) 172.16.9.241
Bucket	Res 1M_20_1 - A (1024912)
Equipment Graphs	Disabled
Colour	
TCP Blocked Ports	12,15,56,32
UDP Blocked Ports	123,456,789
P2P Restricting	true
TCP Connection Limit	2000
Usage Blackout Period	Off
SAND	Overriden

Usage Summary (Daily Usage Details)

Monthly Allowance (CAP)	1000.0000 GB
Current Allowance Usage	0
Download	0
Upload	0
1 day	0
2 days	0
1 week	0
1 month	0

Customer Usage Summary Graph (Daily Usage Details)

Reset ALL usage

RADIUS Details (modify) (history)

Gateway	Test Gateway (wib-100) 172.16.9.241	127.0.0.1-radius	Radius Groups	View..
Radius Authentication	Yes	RADIUS Credentials	Radius Checks	View..
Radius Authorization	Yes	Username	Radius Replies	View..
Radius Accounting	No	00-11:22:33:44:55 (View Details..)		
		testss_JB1 test1 (View Details..)		

Equipment Details (modify) (history)

Equipment nickname	Type	IP address	MAC address	Real Time	Colour	Freq.	More Details..
N05	Norotation SIM	1.1.1.1		Signal Strength			E P S P
S1	Canopy CMA	155					E P

Customer IP Table (modify) (history)

IP Address	IP Type	MAC Address	Hostname / Label	Usage Summary (Month)	Graphs
94.203.148.71	Private			Download 9 Upload 0	R G U P

Email/FTP Details (modify) (history)

Username	First Name	Last Name	Status	Type
No email/FTP Details available				

Figure 5.1-1 “Network” section of “Customer Details” page

The *username* and *password* are required check attributes for the customer - these usually are also required to put on the end-user equipment to authorize it with the NAS. Both these attributes are listed on the customer details page for an easy reference. One customer account can have multiple usernames assigned to it.

The “**RADIUS Details**” section also covers the rest of the RADIUS relevant information.

- **Groups** assigned to the customer account
- Individual **Check** attributes assigned to the customer account
- Individual **Reply** attributes assigned to the customer account

The detailed information on the above is displayed in a hover window available when hovering above “**View Details..**”

RADIUS Details “**Modify**” link leads to “**Customer RADIUS Details**” page from where operator can define all the RADIUS relevant information for a particular account (described in chapter 5.2 of this manual).

5.2 Customer Details Page: Updates

The 'Radius Details' section of the customer details page has been updated with:

- small layout changes - in order to make this section a bit easier to read
- RADIUS Sessions (Last 10) - section that lists the last 10 sessions reported for any of the customer usernames

There are four sections on the 'RADIUS Details' page:

- Gateway Settings - list all gateway related information important for RADIUS integration
- RADIUS Configuration - this section lists running RADIUS configuration for a specified customer
- RADIUS Credentials - covers all username / password accounts customer is set with
- RADIUS Sessions (Last 10) - lists the last 10 RADIUS sessions reported in RADIUS database for a customer

There is a set of actions an operator can execute from the 'Radius Details' section:

1. 'modify..' link (highlighted with '1' on the Fig. 5.2-1) - opens a "Radius Management pages" for a specified customer from where all RADIUS related settings can be amended
2. 'View..' Radius Configuration (highlighted with '2' on the Fig. 5.2-1) - when hover over the View link a small window will be presented to a user that will cover RADIUS setup related to respectively: RADIUS Groups, RADIUS Checks or RADIUS Replies for all customer RADIUS credentials
3. 'View Sessions..' link (highlighted with '3' on the Fig 5.2-1) - opens a page with a detailed RADIUS sessions breakdown for a specified username
4. 'Reload' icon (highlighted with '4' on the Fig 5.2-1) - clicking on this icon will reload the 'RADIUS Sessions (Last 10) window
5. 'D' button (highlighted with '5' on the Fig 5.2-1) - brings up a console from where a 'current' session can be disconnected

Radius Detail (modify...) (history...)

Gateway Settings: Gateway PPPoE (wib-141), Radius Database 127.0.0.1-radius, Radius Authentication Yes, Radius Authorization Yes, Radius Accounting Yes.

RADIUS Configuration: Radius Groups View.., Radius Checks View.., Radius Replies Not Defined.

RADIUS Credentials: Username airwave_2944, Password, Auto Group Yes View Sessions..

RADIUS Sessions (Last 10)

ID	Username	Session Start	Session Stop	Session Time	Upload	Download	Calling Station ID	IP Address	NAS IP Address	NAS Session ID
673375	airwave_2944	2013-04-16 11:54:24	current	00h 00m 00s	0.0 KB	0.0 KB	A0F3.C1.A7.83.77	10.252.254.24	93.95.87.135	0109022f
671930	airwave_2944	2013-04-15 22:36:17	2013-04-16 11:54:08	13h 17m 51s	26.6 MB	820.0 MB	A0F3.C1.A7.83.77	10.252.254.24	93.95.87.135	01090a0f
670901	airwave_2944	2013-04-15 13:52:18	2013-04-16 22:34:08	08h 43m 50s	12.0 MB	306.5 MB	A0F3.C1.A7.83.77	10.252.254.24	93.95.87.135	0109081e
669426	airwave_2944	2013-04-14 22:38:04	2013-04-15 13:48:00	15h 09m 56s	35.9 MB	1021.5 MB	A0F3.C1.A7.83.77	10.252.254.24	93.95.87.135	01090506
661910	airwave_2944	2013-04-10 21:54:28	2013-04-13 13:12:18	2 09j(5) 15h 17m 47s	125.3 MB	2.3 GB	A0F3.C1.A7.83.77	10.252.254.40	93.95.87.135	01094a22
661902	airwave_2944	2013-04-10 21:50:51	2013-04-10 21:53:53	00h 00m 06s	129.5 KB	405.5 KB	A0F3.C1.A7.83.77	10.252.254.40	93.95.87.135	0109490c
661888	airwave_2944	2013-04-10 21:39:01	2013-04-10 21:49:21	00h 10m 22s	684.7 KB	810.6 KB	A0F3.C1.A7.83.77	10.252.254.40	93.95.87.135	01094997
659540	airwave_2944	2013-04-09 12:03:53	2013-04-10 21:38:11	1 09j(5) 09h 34m 16s	107.2 MB	2.6 GB	A0F3.C1.A7.83.77	10.252.254.40	93.95.87.135	01090a84
659534	airwave_2944	2013-04-09 12:01:41	2013-04-09 12:03:06	00h 01m 25s	130.8 KB	5.7 MB	A0F3.C1.A7.83.77	10.252.254.40	93.95.87.135	01090a51

Equipment Details (modify...) (history...)

Fig.5.2-1 'Radius Details' section

5.3 Customer RADIUS Details page

The “*Customer RADIUS Details*” page enables operator to list and define all the customer relevant RADIUS server details. The top part of the page covers the most important user RADIUS details such as: username, password and individual check and reply attributes. Bottom part of the page is used to manage groups user is assigned to. The page also contains a set of buttons giving access to most important RADIUS related system sections such as:

- **Customer Details** – directs back to “customer details” page
- **Change Radius Usernames** – links to a “*Customer RADIUS Usernames*” page described in 5.3 chapter of this manual where operator can define multiple radius access credentials – username / password pairs.
- **User RADIUS Checks** – customer account individual “check” attributes. Note that it is recommended not to add any positions in here unless it is something user specific, it is better to assign the check items against groups instead
- **User RADIUS Replies** - customer account individual “reply” attributes. Note that it is recommended not to add any positions in here unless it is something user specific, it is better to assign the reply items against groups instead

Customer Bill2 (19)

ID	19
Name	Billing Test2
Nickname	Bill2
Invoicing ID	Bill2

Customer RADIUS Details

RADIUS Credentials	Username	Password
	testss_Bill2	[redacted]
Individual RADIUS Checks	View	
Individual RADIUS Replies	Not Defined	

Customer Details | Customer RADIUS Usernames | Individual RADIUS Checks | Individual RADIUS Replies

Browse Customer Groups

Group: -- All --

Back Search

Customer RADIUS Groups

Results 0 - 0 of 0 Number of results to display per page : 50

Username	Groupname	Priority
-	-	-

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 5.2-1 “Customer RADIUS Details” page

Bottom part of the “*Customer RADIUS Details*” page covers managing groups assigned to the customer. Operator can use the search facility to browse groups assigned to customer using specific group or priority as filters. Using this page operator can also add (using the “*Add*” button) and modify (using the “*E*” button) a group to the customer. The “*G*” button links to group details page (as described in 4.8 chapter of this manual) from where operator can verify and manage the group “*check*” and “*reply*” attributes.

Customer Bill2 (19)

ID	19
Name	Billing Test2
Nickname	Bill2
Invoicing ID	Bill2

Add Customer Group

Username* testss_Bill2

Groupname* testss_package_512/128_1GB

Priority* 5

Choose from existing Groups Define new Group

testss_ [input field]

Back Reset Add

Figure 5.2-1 “Add / Modify Customer Group” page

When adding or modifying a group to customer account operator can choose whether to use one of the existing groups from the dropdown menu or to *create a new group*. Each User Group position contains following details:

- **Username** - unique usernames as defined for the SIMPLer customer under “*Customer RADIUS Usernames*” as described in 5.3 chapter of this manual
- **Groupname** – defines group the customer will be assigned to. There are two ways to specify a group name. It can be chosen from the groups already existing in the system or operator can choose to create a new group by selecting the “*Define new Group*” radiobutton and filling out the entry box below
- **Priority** – priority of the group to user assignment. This value will be used to create a precedence in case of one attribute being defined across multiple groups

Note: “*Customer RADIUS Details*” page is designed to provide operator with all tools required to setup all relevant RADIUS parameters from one, single page, minimizing the effort required.

5.4 Customer RADIUS Usernames

The “*Customer RADIUS Usernames*” page, which can be accessed from the “*Customer RADIUS Details*” page provides tools to set / modify the radius credentials – usernames and password pairs. From the RADIUS server standpoint it is done via the “*Cleartext-Password*” check attribute. Using this page the operator can add, modify and delete a username / password access credentials for a SIMPLer customer account. Note that multiple usernames can be assigned against a single SIMPLer account.

Figure 5.3-1 “Customer RADIUS Username” page

Note: only the “current” customers can use the RADIUS server services and management pages. When changing the customer status from “current” to anything else, SIMPLer system will void all customer passwords to deny the end-user an access to network resources.

5.5 Deleting IP Details When Disconnecting Customers

There is an option in the SIMPLer system that allows RADIUS operators to choose from following two behaviours on customer being disconnected:

- leave his IP details in the database - so that his connection keeps the same IP details when in disconnected state - this will require some additional measures (i.e. Marks) being passed to the NAS
- remove his IP details from the database - this will enable disconnection to a 'Disconnected' IP-Pool that in 90% of cases is the easiest way to implement walled garden

Fig.5.4-1 Delete IP details from Radius

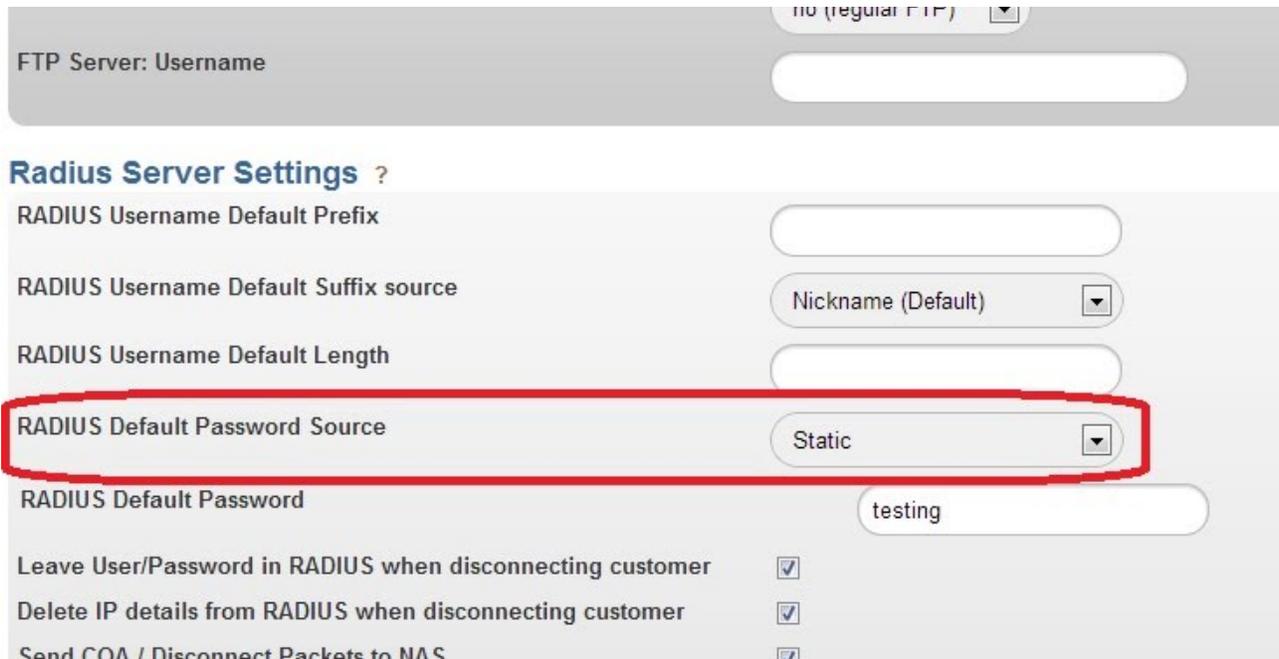
5.6 Generate Default Password Option

There is a feature that allows operators to choose the way passwords for auto-generated RADIUS usernames should be created. The password auto-generation takes place in following cases:

- Auto-Provisioning
- Adding a first RADIUS username to customer account via 'Modify Radius Usernames'
- When a new customer is added (and a RADIUS account added in automatically) where 'New Customer "Dynamic IP addresses when RADIUS"' option is set under operator details

There are two password sources possible:

- Static - (Fig. 1) the default password will be filled out as per 'RADIUS Default Password' - this can be used when a same 'service' password should be assigned to all usernames
- Password Generator - (Fig. 2) the default password will be filled out using a generated, secure password of length defined in 'RADIUS Default Password Length' field. If the length is not specified it will default to 10.



The screenshot shows a web interface for configuring RADIUS server settings. At the top, there is a section for 'FTP Server: Username' with a dropdown menu set to 'no (regular FTP)' and an empty text input field. Below this is the 'Radius Server Settings' section, which includes several configuration options:

- RADIUS Username Default Prefix:** An empty text input field.
- RADIUS Username Default Suffix source:** A dropdown menu set to 'Nickname (Default)'.
- RADIUS Username Default Length:** An empty text input field.
- RADIUS Default Password Source:** A dropdown menu set to 'Static', which is highlighted with a red rectangular box.
- RADIUS Default Password:** A text input field containing the value 'testing'.
- Leave User/Password in RADIUS when disconnecting customer:** A checked checkbox.
- Delete IP details from RADIUS when disconnecting customer:** A checked checkbox.
- Send COA / Disconnect Packets to NAS:** A checked checkbox.

Fig. 5.5-1 RADIUS Default Password Source: Static

FTP Server: Username

Radius Server Settings ?

RADIUS Username Default Prefix

RADIUS Username Default Suffix source

RADIUS Username Default Length

RADIUS Default Password Source

RADIUS Default Password Length

Leave User/Password in RADIUS when disconnecting customer

Fig.5.5-2 RADIUS Default Password Source: Password Generator

5.7 Customer RADIUS Checks

The “*Customer RADIUS Checks*” page manages individual “*check*” attributes assigned to SIMPLer customer account. The attributes of this type are taking part in the Authentication process. Note that to make the RADIUS server management simple, besides defining an individual password for the customer account operator should try avoiding adding any customer specific “*check*” attributes unless absolutely necessary. Groups assigned to customer account (as described in chapter 5.6 of this manual) should be used instead.

The “*check*” attributes will be evaluated before RADIUS authenticates the end-user. Depending on the result of these checks end-user will be granted or rejected access to the network. A good example of a check attribute usage is “*Cleartext-Password*” attribute that defines an individual password for a particular customer which effectively creates a username / password token in the RADIUS server. Full list of the FreeRADIUS base check / reply attributes combined can be found under the below pages:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

<http://tools.ietf.org/html/rfc2866>

Customer Bill2 (19)

ID: 19
Name: Billing Test2
Nickname: Bill2
Invoicing ID: Bill2

Back

Browse Individual Checks

RADIUS Credentials: Username: testss_Bill2, Password: []
Attribute: []
Value: []

Search

Customer RADIUS Checks

Results 1 - 1 of 1

ID	Username	Attribute	Op	Value
13371	testss_Bill2	Cleartext-Password	:=	

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 5.4-1 “Customer RADIUS Checks” page

Operator can add new positions using the “Add” button on the bottom of the “*Customer RADIUS Checks*” table or use the “E” button to edit each position details. There is following set of parameters to be set for each customer RADIUS check position. Note that all the fields are required to create a valid table entry.

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Username** – unique usernames as defined for the SIMPLer customer under “*Customer RADIUS Usernames*” as described in 5.3 chapter of this manual
- **Attribute** – attribute we wish to assign. SIMPLer uses freeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from dropdown menu. “**Dictionary**” dropdown can be used to narrow down the Attributes listed in the Attribute dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (*FreeRADIUS-Internal*, *WISPr*, *RFC2865* and *RFC2866*) in the “Dictionary” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value to check against

Customer JB1 (21)

ID: 21
Name: Joe Bloggs
Nickname: JB1
Invoicing ID: SJS-5011

Back

Add RADIUS Check

Username*: 00:11:22:33:44:55
Attribute*: Acct-Session-Start-Time
Dictionary: FreeRADIUS-Internal
Op*: :=
Value*: []

Back Reset Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 5.4-2 “Modify Customer RADIUS Checks” page

5.8 Customer RADIUS Replies

The “*Customer RADIUS Replies*” page manages individual “*reply*” attributes assigned to SIMPLer customer account. The attributes of this type are taking part in the Authorization process. Note that to make the RADIUS server management simple operator should avoid adding any customer specific “*reply*” attributes unless absolutely necessary. Groups assigned to customer account (as described in chapter 5.6 of this manual) should be used instead.

The “*reply*” attributes will be used by RADIUS server to authorize network resources or level of service to the end-user. A good example of an individual reply attribute usage is “*Session-Timeout*” attribute which defines when the individual session should be terminated. Full list of the FreeRADIUS base check / reply attributes combined can be found under the below page:

<http://freeradius.org/rfc/attributes.html>

<http://tools.ietf.org/html/rfc2865>

<http://tools.ietf.org/html/rfc2866>

Customer JB1 (21)

ID	21
Name	Joe Bloggs
Nickname	JB1
Invoicing ID	SJS-5011

Back

Browse Individual Replies

RADIUS Credentials	Username	Password
	00:11:22:33:44:55 testss_JB1	test1
Attribute		
Value		

Search

Customer Radius Replies

Results 1 - 1 of 1 Number of results to display per page : 50

ID	Username	Attribute	Op	Value
149	testss_JB1	Framed-IP-Address	=	84.203.148.72

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 5.5-1 “Customer RADIUS Replies” page

Operator can add new positions using the “*Add*” button on the bottom of the “*Customer RADIUS Replies*” table or use the “*E*” button to edit each position details. There is following set of parameters to be set for each RADIUS reply position. Note that all the fields are required to create a valid table entry.

- **ID** – unique identifier assigned automatically by SIMPLer system
- **Username** – unique usernames as defined for the SIMPLer customer under “*Customer Radius Usernames*” as described in 5.3 chapter of this manual
- **Attribute** – attribute we wish to authorize. SIMPLer uses freeRADIUS dictionary files to generate and group attributes. Operator can choose the appropriate entries from dropdown menu. “**Dictionary**” dropdown can be used to narrow down the Attributes listed in the Attribute dropdown. **References for the most common dictionaries can be found in 6 chapter of this manual.**

Note: most of the relevant attributes on a day-to-day management can be found under top four dictionaries (*FreeRADIUS-Internal*, *WISPr*, *RFC2865* and *RFC2866*) in the “*Dictionary*” dropdown field

- **Op** – attribute to value operator as described under: <http://wiki.freeradius.org/Operators>
- **Value** – value to set the authorization to

Customer JB1 (21)

ID	21
Name	Joe Bloggs
Nickname	JB1
Invoicing ID	SJS-5011

[Back](#)

Add Radius Reply

Username*

Attribute* Dictionary

Op*

Value*

[Back](#) [Reset](#) [Add](#)

[Documentation](#) | [Release Notes](#)
 copyright © Azotel Technologies Ltd. 2004 - 2012

Figure 5.5-2 “Customer RADIUS Replies” page

5.9 Customer IP Table synchronization

The “*Customer IP Table*” has a “*Synchronize Radius*” option for Radius enabled customers. This option is selected by default when modifying a customer’s account IP table. If selected IP rows with “RADIUS Username” value defined will be synchronized to the RADIUS server. The customer then will be assigned an address automatically if this feature is supported by the NAS operator uses.

Customer Network Details QuickSearch ...

Network Details [\(modify\)](#) [\(history\)](#)

Monitor: no monitor

Gateway: Test Gateway (wib-100)
172.16.9.241

Bucket: Res 1M - 20-1 - A (1024/512)

Equipment Graphs: Disabled

Colour: []

TCP Blocked Ports: 12,15,56,32

UDP Blocked Ports: 123,456,789

P2P Restricting: true

TCP Connection Limit: 2000

Usage Blackout Period: Off

SAND: Overridden

Usage Summary [\(Daily Usage Details...\)](#)

Monthly Allowance (CAP): 1000.0000 GB

Current Allowance Usage: 0

	Download	Upload
1 day	0	0
2 days	0	0
1 week	0	0
1 month	0	0

Customer Usage Summary Graph [\(Daily Usage Details...\)](#)

Reset ALL usage

Equipment Details [\(modify\)](#) [\(history\)](#)

Equipment nickname	Type	IP address	MAC address	Real Time	Colour	Freq.	More Details..
N56	Nanostation SM	1.2.3.1		S Signal Strength			E P S P
S1	Canopy CMM	N/A					E P

Radius Details [\(modify\)](#) [\(history\)](#)

Gateway: Test Gateway (wib-100) 127.0.0.1-radius
172.16.9.241

RADIUS Credentials

Username	Password	Radius Groups	View..
00:11:22:33:44:55		Radius Checks	View..
testss_JB1	test1	Radius Replies	View..

Customer IP Table [\(modify\)](#) [\(history\)](#)

IP Address	IP Type	MAC Address	Hostname / Label	Usage Summary (Month)	Graphs
84.203.148.71	Private			Download: 0 Upload: 0	R G U P

Email/FTP Details [\(modify\)](#) [\(history\)](#)

No email/FTP Details available

Username	First Name	Last Name	Status	Type
No email/FTP Details available				

Azotel Confidential Proprietary

Figure 5.5-2 “Customer IP table” page

5.10 Customer Account Links on Management Pages

Customer names and links to their respective accounts were added to the following RADIUS related pages:

- Individual Radius Checks
- Individual Radius Reply
- Post Authorisation
- Usage Details

ID	Customer	Username	Attribute	Op	Value
3822	VBT1 - VolP Billing Test #1	ts_VBT1	Cleartext-Password	:=	macior

Fig. 5.9-1. Individual Radius Checks

6 Dictionary references

Dictionaries are used to define all the “check” and “reply” attributes supported by the FreeRADIUS server. Below find quick references to all the most commonly used dictionary files.

- **FreeRADIUS-Internal** - Non Protocol Attributes used by FreeRADIUS.
<http://freeradius.org/rfc/attributes.html>
- **FreeRADIUS-Compat** - Obsolete names for backwards compatibility with older users files.
- **WISPr** - Wi-Fi Alliance - Wireless ISP Roaming - Best Current Practices
http://marcelotoledo.com/wp-content/uploads/2007/12/wispr_v10.pdf
- **RFC-2865** - Remote Authentication Dial In User Service (RADIUS)
<http://www.ietf.org/rfc/rfc2865.txt>
- **RFC-2866** – RADIUS Accounting
<http://www.ietf.org/rfc/rfc2866.txt>
- **RFC-2867** – RADIUS Accounting Modifications for Tunnel Protocol Support
<http://www.ietf.org/rfc/rfc2867.txt>
- **RFC-2868** – RADIUS Attributes for Tunnel Protocol Support
<http://www.ietf.org/rfc/rfc2868.txt>
- **RFC-2869** – RADIUS Extensions
<http://www.ietf.org/rfc/rfc2869.txt>
- **RFC-3162** – RADIUS and IPv6
<http://www.ietf.org/rfc/rfc3162.txt>
- **RFC-3576** – Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)
<http://www.ietf.org/rfc/rfc3576.txt>
- **RFC-3580** – IEEE 802.1X Remote Authentication Dial In User Service (RADIUS)
<http://www.ietf.org/rfc/rfc3580.txt>
- **RFC-4590** – RADIUS Extension for Digest Authentication
<http://www.ietf.org/rfc/rfc4590.txt>
- **RFC-4675** – RADIUS Attributes for Virtual LAN and Priority Support
<http://www.ietf.org/rfc/rfc4675.txt>
- **RFC-4679** – DSL Forum Vendor-Specific RADIUS Attribute
<http://www.ietf.org/rfc/rfc4679.txt>
- **Mikrotik**
http://www.mikrotik.com/documentation/manual_2.9/dictionary
- **ChilliSpot**
<http://www.chillispot.info/features.html>

- **Motorola** – Motorola Canopy BAM
<http://www.canopywireless.pl/files/File/brochures/BAM%202.0.pdf>
- **Motorola-PMP320** – Motorola Canopy PMP320
<http://motorola.wirelessbroadbandsupport.com/software/>
- **Waverider**
<http://www.waverider.com>
- **Tropos**
http://gridcom.tropos.com/docs_import/support/UserGuide.pdf
- **3gpp** – 3GPP related attributes
ftp://ftp.3gpp.org/specs/2002-06/R1999/29_series/29061-3a0.zip
- **3gpp2** – 3GPP2 related attributes
http://www.3gpp2.org/Public_html/specs/X.S0011-005-C_v2.0_050708.pdf

7 Quick Start

The purpose of this section is to outline a process of setting up a simple RADIUS based network solution from the scratch and integrating it with the embedded SIMPLer RADIUS server. See the 7-1 figure for a network scheme of this very basic, RADIUS based network. This process would describe the minimum number of steps required to connect up the first customer. The assumptions used for the purpose of this quick startup guide are:

- Customers are authenticated using the Captive Portal embedded to the pfSense software
<http://www.pfsense.org/>
- NAS (pfSense) is using the RADIUS server embedded to SIMPLer platform servers
- SIMPLer platform used to manage following customer-level aspects of the connection:
 - *Access Credentials* (username and password)
 - QoS – *Upload and Download speed*
 - QoS – *Upload and Download limits*

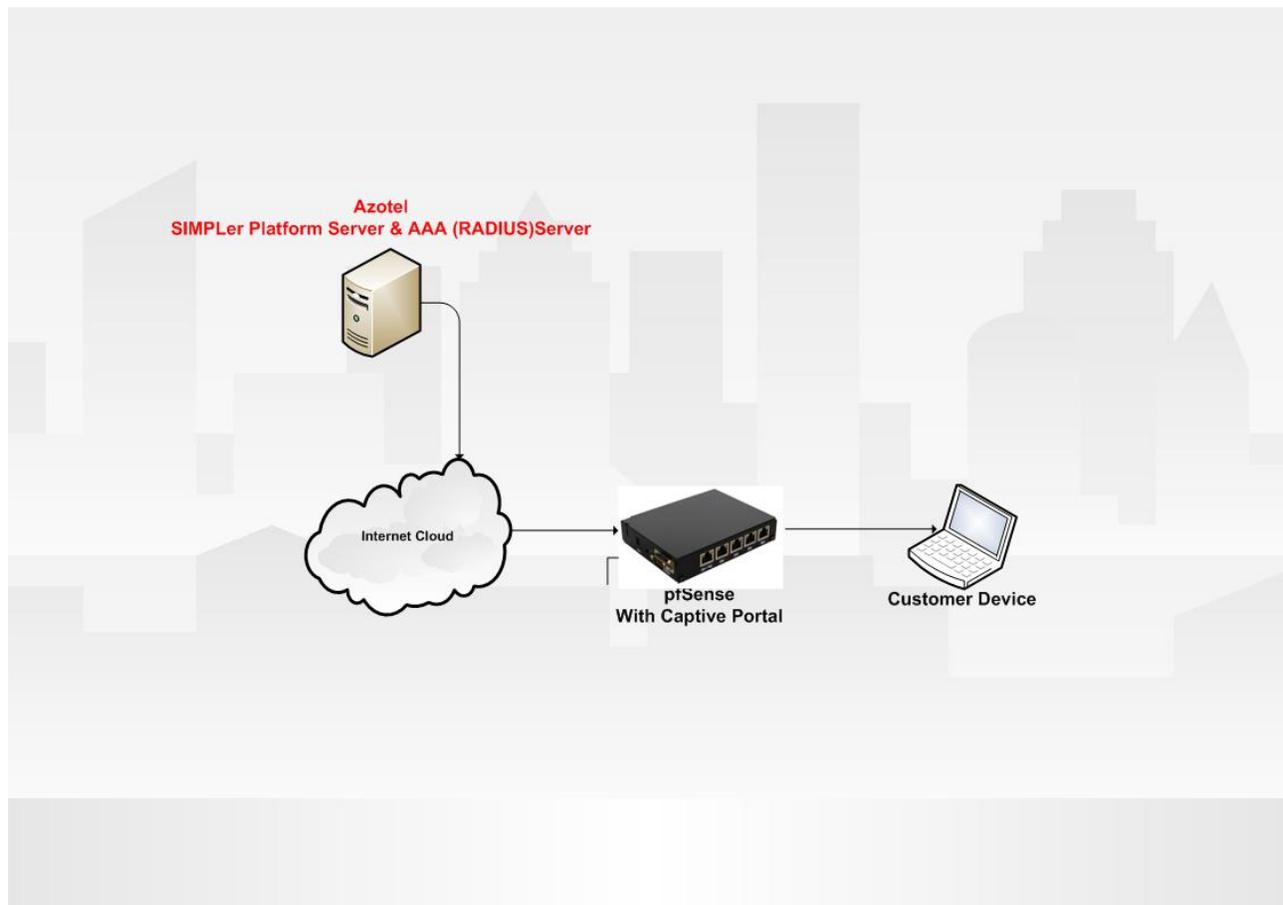


Figure 7-1 Network setup as described in Quick Start chapter

Below find the steps required to set up the most basic RADIUS managed solution

7.1 Set UP NAS in the SIMPLer platform

Adding a NAS to the system is a first step when setting up a RADIUS authenticated network.

1. Click on the "*radius*" link from the SIMPLer main menu to get to the "*RADIUS Server Management*" page and from there click the "*Network Access Servers >>*" link

The screenshot shows the Azotel RADIUS Server Management web interface. At the top, there is a navigation bar with the Azotel logo, WISP login information, a 'Recently Viewed Customers' field, and the SIMPLer logo. Below this is a main navigation menu with items: Dashboard, Map, Customers, Invoices, Products, Network, Hotspots, **Radius** (highlighted with a red box and a red '1'), Tools, Settings, and Logout. An 'Inbox (0)' notification is also visible. The main content area shows a sidebar with sections: 'Radius Database:' (containing a dropdown menu with '127.0.0.1-radius'), 'Settings:' (expanded, with 'Network Access Servers' highlighted by a red box and a red '2'), and 'Accounting:' (containing 'Usage Details').

2. Add a new position to the “*Network Access Servers*” page:

- Make sure that you are updating the RADIUS server embedded to SIMPLer server – only the “**127.0.0.1-radius**” entry in the Database field represents the embedded database
- Press the “**Add Blank Row**” button to add new row to the NAS table
- Fill Out the data for your new NAS device:

- a. **IP Address / Hostname** – **Public IP address** of the NAS device (pfSense in the following example) from which the RADIUS requests to the SIMPLer platform’s embedded RADIUS server will be coming from. In case of using a private network you can verify this by connecting a laptop in place of the NAS equipment and verifying the Public IP address using the below page:

<http://www.whatismyip.com/>

- b. **Name** – Can be set to operator liking
- c. **Type** – As the pfSense is not a known device type, we use “other” option, which will be working just fine in 95% of the cases
- d. **Secret** – **This is a shared secret used on both RADIUS server and the NAS** to encrypt the transmission.

Note that the exact same value has to be put to a dedicated field (usually called SharedSecret or Secret) field on the NAS, otherwise no RADIUS transmissions will be successful.

- Press “**Update Table**” button to submit the changes

WISP: Test
login: justyna
Network Access Servers

Recently Viewed Customers

SIMPLer

Inbox (0)

Dashboard Map Customers Invoices Products Network Hotspots Radius Tools Settings Logout QuickSearch ...

Back Radius Management

Radius Database: 127.0.0.1-radius 1

Update Table 4

Network Access Servers

IP Address / Hostname*	Name*	Type*	Secret*	Port	Community	Description	Delete
1.2.3.4	test_justyna	other	test 3				

Add Blank Row 2

7.2 Setup the NAS to talk with the RADIUS server

The NAS vendor chosen for purpose of this manual is a free, open source pfSense software for use as a firewall and router. It can be downloaded from here:

<http://www.pfsense.org/>

<http://doc.pfsense.org/index.php/Tutorials>

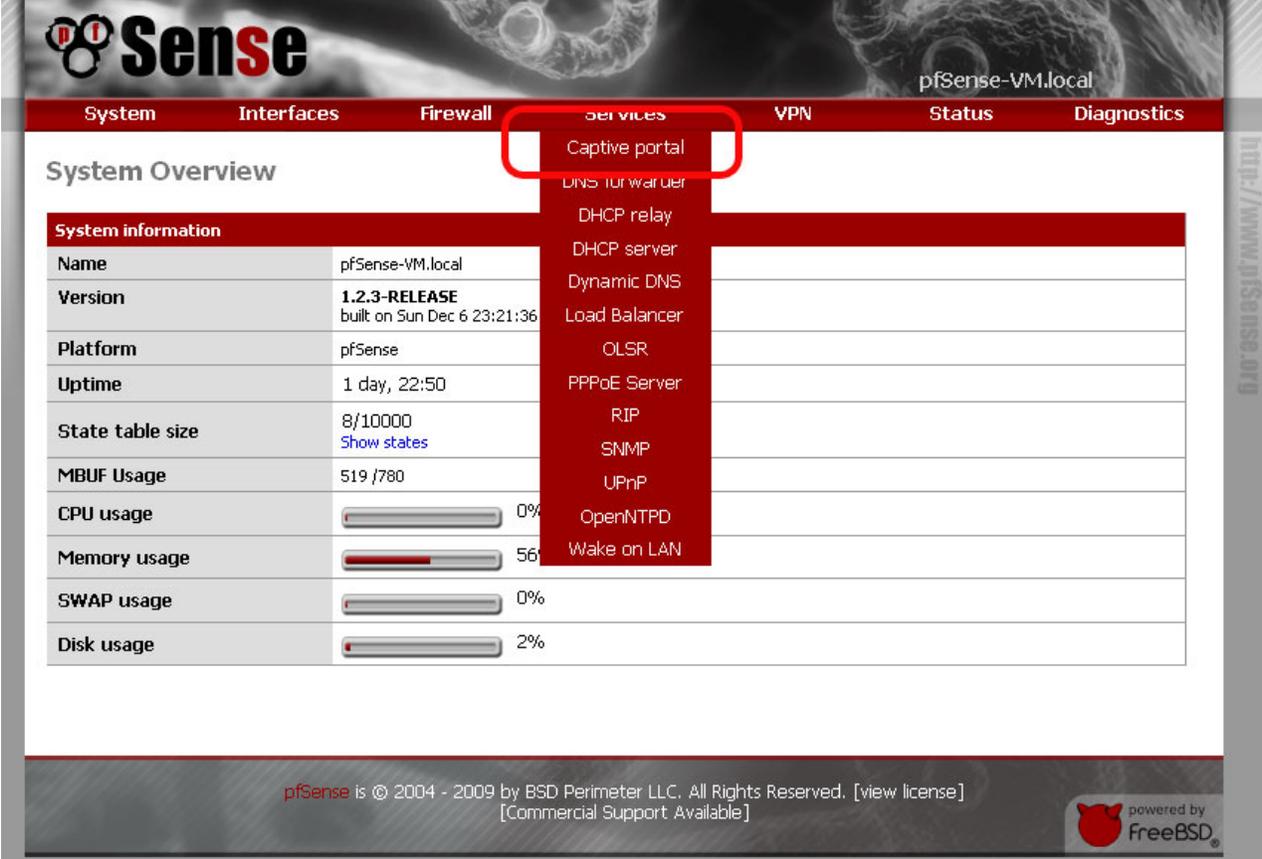
http://doc.pfsense.org/smiller/Captive_Portal.htm

Please refer to the above pages for manuals, tutorial and exact instructions on installing the pfSense software on various hardware releases. For the purpose of this manual we have been using a PC with two network interfaces to host the pfSense software. This chapter works on following assumptions:

- *pfSense software is already installed* on a piece of hardware and is up-and-running
- *operator can access the WEB Interface* of the pfSense software
- *WAN interface is setup* and pfSense is *connected to the internet*
- *LAN interface is setup as DHCP* server for the clients connecting to the Captive Portal

For the simplicity of this chapter we have used the “*Captive Portal*” service embedded to the pfSense software as a client to the RADIUS server. Below find steps outlining the relevant setup performed via the pfSense GUI pages:

1. Navigate to “*Captive Portal*” page via the “*Services*” tab



The screenshot displays the pfSense web interface. At the top, the 'pfSense' logo is on the left, and the hostname 'pfSense-VM.local' is on the right. A navigation bar contains tabs for 'System', 'Interfaces', 'Firewall', 'Services', 'VPN', 'Status', and 'Diagnostics'. The 'Services' tab is selected and highlighted with a red box. A dropdown menu is open under 'Services', listing various services: Captive portal, DNS forwarder, DHCP relay, DHCP server, Dynamic DNS, Load Balancer, OLSR, PPPoE Server, RIP, SNMP, UPnP, OpenNTPD, and Wake on LAN. The 'Captive portal' option is highlighted in red. Below the navigation bar, the 'System Overview' section is visible, featuring a table of system information and several progress bars for resource usage.

System information	
Name	pfSense-VM.local
Version	1.2.3-RELEASE built on Sun Dec 6 23:21:36
Platform	pfSense
Uptime	1 day, 22:50
State table size	8/10000 Show states
MBUF Usage	519 /780
CPU usage	 0%
Memory usage	 56%
SWAP usage	 0%
Disk usage	 2%

pfSense is © 2004 - 2009 by BSD Perimeter LLC. All Rights Reserved. [view license]
[Commercial Support Available]

powered by
FreeBSD®

Figure 7.2-1 pfSense – navigating to “Captive Portal” from the main page

The screenshot shows the pfSense Captive Portal configuration page. The 'Interface' is set to 'LAN'. Under 'Authentication', 'RADIUS authentication' is selected. The 'Primary RADIUS server' is configured with IP address '84.203.220.3', port '1812', and a shared secret 'test1234567890'. The 'Accounting' section has 'Send RADIUS accounting packets' checked and 'Accounting port' set to '1813'. A 'Save' button is highlighted at the bottom of the page.

- 512kbps download speed limit
- 128kbps upload speed limit

2. On the “Captive Portal” page:

- Select “**Enable captive portal**” option to turn on the Captive Portal service on the pfSense

- Select the interface to run the Captive Portal services on. It is set to “**LAN**” port by default

- In the “**Authentication**” section select the “**RADIUS authentication**” to choose the RADIUS server as an authentication server. Set to “**no authentication**” by default.

- In the “**Primary RADIUS server**” part of the “**Authentication section**”:

- a. Fill out the “**IP address**” field with the respective SIMPLer platform server IP address. In this example we have used 84.203.220.3 IP → wib.azotel.com. Note that it is better to use the IP address rather than the respective DNS name as this may speed up RADIUS queries in certain cases

- b. Verify the “**Port**” field (default: 1812). Note that all RADIUS servers embedded to SIMPLer use the default port for RADIUS queries

- c. Fill out the “**Shared secret**” field with the password defined in “**secret**” field for the NAS under SIMPLer platform (see chapter 7.1 for reference)

- In the “Accounting” part of the “**Authentication section**”:

- a. Select the “**send RADIUS accounting packets**” option to send the accounting data to RADIUS server. This data will then be used in example for graphing in SIMPLer. This option is disabled by default.

- b. Verify the “**Accounting Port**” field (default:1813). Note that all RADIUS servers embedded to SIMPLer use the default port for RADIUS queries

- Press “**Save**” button on the bottom of the page to submit the changes

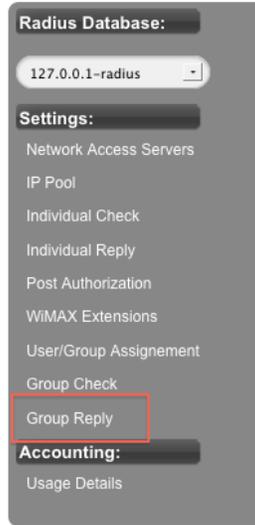
7.3 Group Setup

Next step is to set up and configure a customer group in the RADIUS database that will define the QoS details for the particular customer such as:

- 1G up/down traffic limits

Below find the steps to set up a sample group:

1. Click on the **“radius”** link from the SIMPLer main menu to get to the **“RADIUS Server Management”** page and from there click the **“Group Reply >>”** link



2. Click on the **“Add”** button on the **“Group Reply”** page to add a new RADIUS reply attribute (sent to the NAS in the “Authorization” replies).

The screenshot shows the 'Browse Group Reply' form. It has a 'Radius Database' dropdown menu set to '127.0.0.1-radius'. Below it are two input fields labeled 'Attribute' and 'Value'. A 'Search' button is located at the bottom left of the form.

Group Reply

Results 1 - 5 of 5 Number of results to display per page: 50

ID	Groupname	Attribute	Op	Value	
386	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Down	=	512000	
387	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Up	=	128000	
427	testss_test	Framed-Pool	=	authenticatedCustomer	
428	testss_package_512/128_1GB	Idle-Timeout	=	120	
429	testss_test	Idle-Timeout	=	200	

Add

3. Fill out the data for new RADIUS reply position – *512kbps download limit*:
 - a. Select the **“Define new Group”** radiobutton. We want to create new group as we are adding a new radius group position. In the field below fill in the new group name. In the following example we have decided to use **“package_512/128_1GB”** description
 - b. Choose the **“WISPr”** position from the **“Dictionary”** dropdown and wait for the **“Attribute”** dropdown to populate with dictionary entries (this may take couple seconds depending on the link). The WISPr dictionary defines many attributes usefull for an ISP.
 - c. Select **“WISPr-Bandwidth-Max-Down”** from the **“Attribute”** dropdown
 - d. In the **“Op”** field select **“=”** or **“:=”** as an operator
 - e. Set the **“Value”** field to **“512000”**.

Note that the **“Value”** field is given in bits for the **“WISPr-Bandwidth-Max-Down”** attribute hence 512000 value represents 512 kbps.
 - f. Click on **“Add”** button to add the **“Group Reply”** entry to the RADIUS database. This also redirects back to the **“Group Reply”** page

Add Group Radius Reply

Choose from existing Groups

Groupname*

Attribute*

Op*

Value*

Back Reset Add

Define new Group

testss

Dictionary

FreeRADIUS-Internal

1

2

3

4

5

4. Click on the **“Add”** button on the **“Group Reply”** page to add a next RADIUS reply attribute

Back Radius Management

Radius Database:

127.0.0.1-radius

Browse Group Reply

Attribute

Value

Search

Group Reply

Results 1 - 5 of 5

Number of results to display per page: 50

ID	Groupname	Attribute	Op	Value
386	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Down	=	512000
387	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Up	=	128000
427	testss_test	Framed-Pool	=	authenticatedCustomer
428	testss_package_512/128_1GB	Idle-Timeout	=	120
429	testss_test	Idle-Timeout	=	200

Add

5. Fill out the data for new RADIUS reply position – *128kbps upload limit*:
 - a. Use the **“Choose from existing Groups”** radiobutton to select **“package_512/128_1GB”** group from the dropdown list
 - b. Choose the **“WISPr”** position from the **“Dictionary”** dropdown and wait for the **“Attribute”** dropdown to populate with dictionary entries (this may take couple seconds depending on the link). The WISPr dictionary defines many attributes usefull for an ISP.
 - c. Select **“WISPr-Bandwidth-Max-Up”** from the **“Attribute”** dropdown
 - d. In the **“Op”** field select **“=”** or **“:=”** as an operator
 - e. Set the **“Value”** field to **“128000”**.

Note that the “*Value*” field is given in bits for the “*WISPr-Bandwidth-Max-Up*” attribute hence 128000 value represents 128 kbps.

- f. Click on “*Add*” button to add the “*Group Reply*” entry to the RADIUS database. This also redirects back to the “*Group Reply*” page

Add Group Radius Reply

Groupname* Choose from existing Groups
 1

Attribute* 3

Op* 4

Value* 5

Define new Group

 Dictionary
 2

6. Verify the “*Group Reply*” attributes set with the below screenshot and click on “*Radius Management*” button to go back to “*Radius Server Management*” page

Radius Database:

Browse Group Reply
 Attribute

 Value

Group Reply

Results 1 - 5 of 5 Number of results to display per page: 50

ID	Groupname	Attribute	Op	Value	
386	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Down	=	512000	<input type="button" value="E"/>
387	testss_package_512/128_1GB	WISPr-Bandwidth-Max-Up	=	128000	<input type="button" value="E"/>
427	testss_test	Framed-Pool	=	authenticatedCustomer	<input type="button" value="E"/>
428	testss_package_512/128_1GB	Idle-Timeout	=	120	<input type="button" value="E"/>
429	testss_test	Idle-Timeout	=	200	<input type="button" value="E"/>

7. Click on the “*Group Check >>*” link

Radius Database:

Settings:

- Network Access Servers
- IP Pool
- Individual Check
- Individual Reply
- Post Authorization
- WIMAX Extensions
- User/Group Assignment
-
- Group Reply

Accounting:
 Usage Details

8. Click on the “*Add*” button on the “*Group Check*” page to add a new RADIUS check attribute – verified as a part of the Authentication process.

Back Radius Management

Radius Database:
127.0.0.1-radius

Browse Group Checks
Attribute
Value
Search

Group Check

Results 1 - 3 of 3 Number of results to display per page: 50

ID	Groupname	Attribute	Op	Value
171	testss_package_512/128_1GB	Simultaneous-Use	:=	
172	testss_package_512/128_1GB	Acct-Input-Octets	<=	1000000000
173	testss_package_512/128_1GB	Acct-Output-Octets	<=	1000000000

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

9. Fill out the data for new RADIUS check position – *Simultaneous Use limit*:

- Use the “*Choose from existing Groups*” radiobutton to select “*package_512/128_1GB*” group from the dropdown list
- Choose the “*FreeRADIUS-Internal*” position from the “*Dictionary*” dropdown and wait for the “*Attribute*” dropdown to populate with dictionary entries (this may take couple seconds depending on the link).
- Select “*Simultaneous*” from the “*Attribute*” dropdown
- In the “*Op*” field select “*:=*” as an operator. Note that “*=*” should not be used for “*check*” attributes
- Set the “*Value*” field to “*0*”.
- Click on “*Add*” button to add the “*Group Check*” entry to the RADIUS database. This also redirects back to the “*Group Check*” page

Add Group Radius Check

Choose from existing Groups Define new Group

Groupname* tests_package_512/128_1GB

Attribute* Acct-Session-Start-Time

Op* :=

Value*

Dictionary
FreeRADIUS-Internal

Back Reset Add

10. Click on the “*Add*” button on the “*Group Check*” page to add a next RADIUS check attribute

11. Fill out the data for new RADIUS check position – *upload traffic 1GB limit*:

- Use the “*Choose from existing Groups*” radiobutton to select “*package_512/128_1GB*” group from the dropdown list
- Choose the “*RFC2866*” position from the “*Dictionary*” dropdown and wait for the “*Attribute*” dropdown to populate with dictionary entries (this may take couple seconds depending on the link).
- Select “*Acct-Input-Octets*” from the “*Attribute*” dropdown
- In the “*Op*” field select “*<=*” as an operator
- Set the “*Value*” field to “*1000000000*”.

Note that the “*Value*” field is given in bytes for the “*Acct-Input-Octets*” attribute hence 1000000000 value represents approximately 1 GB.

- Click on “*Add*” button to add the “*Group Check*” entry to the RADIUS database. This also redirects back to the “*Group Check*” page

The screenshot shows the 'Add Group Radius Check' form. Red boxes and numbers highlight the following fields:

- 1: Groupname dropdown menu (selected: testss_package_512/128_1GB)
- 2: Dictionary dropdown menu (selected: FreeRADIUS-Internal)
- 3: Attribute dropdown menu (selected: Acct-Session-Start-Time)
- 4: Operator dropdown menu (selected: <=)
- 5: Value text input field (empty)

12. Click on the “Add” button on the “Group Check” page to add a next RADIUS check attribute

13. Fill out the data for new RADIUS check position – *upload traffic 1GB limit*:

- a. Use the “Choose from existing Groups” radiobutton to select “package_512/128_1GB” group from the dropdown list
- b. Choose the “RFC2866” position from the “Dictionary” dropdown and wait for the “Attribute” dropdown to populate with dictionary entries (this may take couple seconds depending on the link).
- c. Select “Acct-Input-Octets” from the “Attribute” dropdown
- d. In the “Op” field select “<=” as an operator
- e. Set the “Value” field to “1000000000”.

Note that the “Value” field is given in bytes for the “Acct-Input-Octets” attribute hence 1000000000 value represents approximately 1 GB.

- f. Click on “Add” button to add the “Group Check” entry to the RADIUS database. This also redirects back to the “Group Check” page

This is a duplicate of the screenshot above, showing the 'Add Group Radius Check' form with red boxes and numbers 1-5 highlighting the Groupname, Dictionary, Attribute, Operator, and Value fields.

14. Verify the “Group Check” attributes set with the below screenshot

The screenshot shows the RADIUS Management interface. At the top, there are buttons for 'Back' and 'Radius Management'. Below that, the 'Radius Database' is set to '127.0.0.1-radius'. There is a section for 'Browse Group Checks' with 'Attribute' and 'Value' input fields and a 'Search' button.

The main part of the screenshot is a table titled 'Group Check' showing the results of a search. The table has 5 columns: ID, Groupname, Attribute, Op, and Value. There are 3 results shown.

ID	Groupname	Attribute	Op	Value	
171	testss_package_512/128_1GB	Simultaneous-Use	:=		
172	testss_package_512/128_1GB	Acct-Input-Octets	<=	1000000000	
173	testss_package_512/128_1GB	Acct-Output-Octets	<=	1000000000	

At the bottom of the table, there is an 'Add' button. Below the table, there are links for 'Documentation' and 'Release Notes', and a copyright notice: 'copyright © Azotel Technologies Ltd. 2004 - 2012'.

Reassuring: A group with following QoS parameters has been set:

- o Download speed – 128 kbps

- Upload speed – 512 kbps
- No simultaneous usage
- 1 GB download traffic limit
- 1 GB upload traffic limit

7.4 Gateway Setup

Next step is to set up a “virtual” gateway in the SIMPLer platform and enable it with RADIUS modules.

Click on the “*network*” link from the SIMPLer main menu and then on “*Gateway details*” tab to get to the “*Gateway Details*” page. Then click the “*Add*” button on bottom of the table to add a new gateway to the system

Gateway ID	Name	WIB number	Status	Active Subscribers	Subscribers License	Traffic Shaping Bucket	WIB routes	Graphs	Info
1	Test Gateway	100	active	7	200	Table view	Routes View	Graph view	E F B R H H G
2	Stephen Test	101	active	2	400	Table view	Routes View	Graph view	E F B R H H G
3	GWTest1	250	active		400	Table view	Routes View	Graph view	E F B R H H G
4	GWTest2	251	active		400	Table view	Routes View	Graph view	E F B R H H G
5	GWTest3	252	active		400	Table view	Routes View	Graph view	E F B R H H G
6	GWTest4	253	active		400	Table view	Routes View	Graph view	E F B R H H G
7	RadiusGateway_1	105	active		400	Table view	Routes View	Graph view	E F B R H H G

[Add](#)

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

1. Set the new gateway up as a “*virtual*” gateway with all RADIUS modules enabled. Fill out following, minimum set of details:
 - a. *Name* – can be set to operator liking
 - b. *WIB number* – please contact Azotel if the dropbox is empty. This field is required.
 - c. *Status* – must be set to “*active*”
 - d. *WIB Type* – set it to “*virtual*” which means there is no WIB-C hardware required
 - e. *Public IP Address*
 - f. Set the RADIUS Server details:
 - *Enable Authentication* Module
 - *Enable Authorization* Module
 - *Enable Accounting* Module
 - g. Submit the changes by pressing the “*Add*” button

Add a New Gateway

Gateway Static Settings

Name:

WIB number:

Status:

WIB Type:

WIB group name:

Network Details

Public IP address:

Upstream gateway:

Secondary gateway:

Primary DNS:

Secondary DNS:

RADIUS Server

Authentication Module Enabled:

Authorization Module Enabled:

Accounting Module Enabled:

Override Operator Default Radius Server:

Send COA / Disconnect Packets to NAS:

Radius Server IP Address:

Radius Server Database:

Radius Server Database Type:

Radius Server Username:

Radius Server Password:

Override Operator Default Accounting Database:

Accounting Database IP Address:

Accounting Database Name:

Accounting Database Type:

Accounting Database Username:

Accounting Database Password:

Back Reset **Add**

2. Click on the “B” button in the respective gateway – “RadiusGateway_1” row to access the bucket details

Gateway ID	Name	WIB number	Status	Active Subscribers	Subscribers License	Traffic Shaping Bucket	WIB routes	Graphs	Info
1	Test_Gateway	100	active	7	200	Table view	Routes View	Graph view	E F B R H H G
2	Stephen_Test	101	active	2	400	Table view	Routes View	Graph view	E F B R H H G
3	GWTest1	250	active		400	Table view	Routes View	Graph view	E F B R H H G
4	GWTest2	251	active		400	Table view	Routes View	Graph view	E F B R H H G
5	GWTest3	252	active		400	Table view	Routes View	Graph view	E F B R H H G
6	GWTest4	253	active		400	Table view	Routes View	Graph view	E F B R H H G
7	RadiusGateway_1	105	active		400	Table view	Routes View	Graph view	E F B R H H G

Results 1 - 7 of 7 Search: Number of results to display per page:

Add

3. Rename the bucket and click the **“Update Buckets Table”** button

The screenshot shows the 'Gateway RadiusGateway_1 (wib 105)' configuration page. The 'Traffic Shaping Buckets' section contains a table with the following data:

ID	Description	Downlink rate (kbits/s) Burst rate (kbit/s) / Size (Kb)	Uplink rate (kbits/s) Burst rate (kbit/s) / Size (Kb)	Throttling (%)	Usage (Throttled)	Priority
9	Traffic Group #1	512	512		0 (0)	Customers Graphs
						Add

Below the table, there is a 'Back' button and an 'Update Buckets Table' button, both highlighted with red boxes. A note at the bottom states: 'Note : Buckets 'In use' cannot be deleted.'

7.5 Customer Setup

Setting up the customer account is the last step required to get the customer online using a RADIUS server based solution. This step needs to be carried out for each subsequent customer.

1. On the **“Customer Details”** page verify that the customer account is in **“current”** status. If not use the **“modify..”** link next to the **“Customer Account”** label and set the customer to **“current”**. Note that customer account must be in **“current”** state to be active on the RADIUS server.

The screenshot displays the 'Customer Details' page for Customer ID 21. The 'Customer Account' section shows the status as 'current' (changed 01/12/09). The 'Contact Details' section includes email addresses and telephone numbers. The 'Financial Summary' shows prepayments and credits. The 'Address' section lists billing and installation addresses. A map is visible in the bottom right corner.

Customer Account (modify..) (history..)

Customer ID: 21
 Invoicing ID: SJS-5011
 Nickname: JB1
 Name: Joe Bloggs
 Status: **current** (Changed: 01/12/09)

Contact Details (modify..) (history..)

Email: maciej.gawfowski@gmail.com
 Accounts Email: accounts@macka.net
 Supports Email: supports@macka.net
 Telephone: 021 467 1602
 Fax: 021 467 1699
 Website: www.macka.net
 Contacts: (P) Macka
 SD: email@macka.net

Financial Summary (statement..)

Prepayments (Amount Remaining): EUR 220.00 CR
 Credits (Amount Remaining): EUR 1000.00 CR
 Customer Balance: **EUR 0.00 DR**

Address (modify..) (history..)

Billing Address: Street 12 Drive, Lough, Town New Orlean, County Some County, Post Code NO24-TH3, State California, Country United States
 Installation Address: Street Apt. 27 Granary Court, Lady's Well, Town Cork, County Co. Cork, Post Code none, State Delaware, Country United States

Installation Area: IA 7
 Community Code: CC 90
 GPS Coordinates: ✓

- Navigate to the “**NETWORK**” section of the “**Customer Details**” page

Customer Network Details QuickSearch ...

Network Details (modify..) (history..)		Usage Summary (Daily Usage Details..)	
Monitor	monitor	Monthly Allowance (CAP)	4.8276 GB
Gateway	No Gateway assigned	Current Allowance Usage	0
Bucket	No Bucket assigned		Download Upload
Equipment Graphs	Disabled		1 day
Colour			2 days
TCP Blocked Ports			1 week
UDP Blocked Ports			1 month
P2P Restricting	True	Radius Details (modify..) (history..)	
TCP Connection Limit		Gateway	No Gateway assigned
Usage Blackout Period	Off	Radius Authentication	No
		Radius Authorization	No
		Radius Accounting	No

Equipment Details [\(modify..\)](#) [\(history..\)](#)

Equipment nickname	Type	IP address	MAC address	Real Time	Colour	Freq.
No equipment Details available						

Customer IP Table [\(modify..\)](#) [\(history..\)](#)

IP Address	IP Type	MAC Address	Hostname / Label	Usage Summary (Month)	Graphs
No IP Details available					

Email/FTP Details [\(modify..\)](#) [\(history..\)](#)

Username	First Name	Last Name	Status	Type
No email/FTP Details available				

- If customer has no gateway assigned, click on the “**modify..**” link next to “**Network Details**” to assign both a **gateway** and a **bucket** to customer account. Then click on “**Update Customer**” button to submit the changes.

General | Contact details | Banking details | **Network details** | Custom Fields

Back | Back to Customer Details | Update Customer

Customer Identification

Name: Joe Bloggs
 Invoicing ID: SJS-5011
 Nickname: JB1

Main Network Details

Installation Date: Jul 23 2008 Customer Equipment Graphs ?

Gateway: RadiusGateway_1 - wib 1 Tower / Site: [dropdown]

Traffic Shaping Bucket: Traffic Group #1, 512, 51 Monitor: no monitor [dropdown]

Auto-Provision

IP Type: Public [dropdown] NAT ?

IP Number: 1 Generate RADIUS Account(s) ?

Dynamic IP addresses when RADIUS ?

Set PPPoE ?

Network Protocols Handling

TCP: 12,15,56,32 P2P Restricting: true [dropdown] ?

UDP: 123,456,789 DHCP Options: [text area] ?

TCP Connection Limit: 2000

Network Subscriber Auto Notification/Disconnection

Customer Traffic Limit (GB): 1000 ?

Time of Day Data Usage Exemption: off [dropdown] ?

Prorate the CAP in the first month: default [dropdown]

Carry over overage Top-Ups to the next period: default [dropdown]

Status: Off [dropdown] ?

Back | Back to Customer Details | **Update Customer**

- Click on “*modify..*” link next to the “*Radius Details*” label to get to the “*Customer RADIUS details*” page

Customer Network Details

Network Details (modify..) (history..)
 Monitor: no monitor
 Gateway: Test Gateway (wib-100) 172.16.9.241
 Bucket: Res 1M - 20:1 - A (1024/512)
 Equipment Graphs: Disabled
 Colour: [blank]
 TCP Blocked Ports: 12,15,56,32
 UDP Blocked Ports: 123,456,789
 P2P Restricting: true
 TCP Connection Limit: 2000
 Usage Blackout Period: Off
 SAND: **Overridden**

Usage Summary (Daily Usage Details..)
 Monthly Allowance (CAP): 1000.0000 GB
 Current Allowance Usage: 0
 Download: 0 Upload: 0
 1 day: 0 0
 2 days: 0 0
 1 week: 0 0
 1 month: 0 0

Customer Usage Summary Graph (Daily Usage Details..)
 Bits per second vs. Time (Hours)

Radius Details (modify..) (history..)
 Gateway: Test Gateway (wib-100) 172.16.9.241
 RADIUS Authentication: Yes
 RADIUS Authorization: Yes
 RADIUS Accounting: No
 RADIUS Credentials: 127.0.0.1-radius
 Username: 00:11:22:33:44:55
 Password: tests_JB1 test1

Equipment Details (modify..) (history..)
 Equipment nickname: NS6
 Type: Nanostation SM
 IP address: 1.2.3.4
 MAC address: [blank]
 Real Time: [Signal Strength icon]

Customer IP Table (modify..) (history..)
 IP Address: 84.203.148.71
 IP Type: Private
 MAC Address: [blank]
 Hostname / Label: [blank]
 Usage Summary (Month): Download: 0 Upload: 0

Email/FTP Details (modify..) (history..)
 Username: [blank]
 First Name: [blank]
 Last Name: [blank]
 Status: [blank]
 Type: [blank]
 No email/FTP Details available

- Click on the “*Customer Radius Usernames*” button on the “*Customer RADIUS details*” page to set the RADIUS credentials – username / password pair.

Customer JB1 (21)

ID: 21
 Name: Joe Bloggs
 Nickname: JB1
 Invoicing ID: SJS-5011

Customer Radius Details

RADIUS Credentials
 Username: 00:11:22:33:44:55 tests_JB1
 Password: test1

Individual Radius Checks: View
 Individual Radius Replies: View

Customer Details | **Customer Radius Usernames** | Individual Radius Checks | Individual Radius Replies

Browse Customer Groups
 Group: -- All --
 Back Search

Customer Radius Groups

Results 1 - 1 of 1
 Number of results to display per page : 50

Username	Groupname	Priority
00:11:22:33:44:55	testss_package_512/128_1GB	5

Add

[Documentation](#) | [Release Notes](#)
 copyright © Azotel Technologies Ltd. 2004 - 2012

6. Fill out the **“Password”** field on the **“RADIUS Usernames”** page and click the **“Update Table”** button. If there are no usernames defined for a particular user, system will suggest the default username merged from the operator name and customer nickname

Customer JB1 (21)

ID	21
Name	Joe Bloggs
Nickname	JB1
Invoicing ID	SJS-5011

Back Update Table

Username*	Password*	Priority*	
00:11:22:33:44:55		5	Delete
testss_JB1	test1	5	Delete

Add Blank Row

7. Click on the **“Add”** button on the bottom of **“Customer Radius Groups”** table to add a new group assignment to customer account

Customer JB1 (21)

ID	21
Name	Joe Bloggs
Nickname	JB1
Invoicing ID	SJS-5011

Customer Radius Details

RADIUS Credentials	Username	Password
	00:11:22:33:44:55	
	testss_JB1	test1

Individual Radius Checks [View](#)
Individual Radius Replies [View](#)

Customer Details Customer Radius Usernames Individual Radius Checks Individual Radius Replies

Browse Customer Groups

Group: -- All --

Back Search

Customer Radius Groups

Results 1 - 1 of 1 Number of results to display per page : 50

Username	Groupname	Priority
00:11:22:33:44:55	testss_package_512/128_1GB	5

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

8. Fill out the data for new customer group assignment
- Verify the username – there might be multiple usernames assigned to a customer account
 - Use the **“Choose from existing Groups”** radiobutton and select **“tests_package_512/128_1GB”** group from the dropdown list
 - Set the **“Priority”** field. Default priority is 5
 - Click on **“Add”** button to add the **“Customer Group”** entry to the RADIUS database. This also redirects back to the **“Customer Radius Details”** page

Customer JB1 (21)

ID	21
Name	Joe Bloggs
Nickname	JB1
Invoicing ID	SJS-5011

Add Customer Group

Username* 00:11:22:33:44:55

Groupname* Choose from existing Groups tests_package_512/128_1GB Define new Group tests_

Priority* 5

Back Reset Add

9. On the “*Customer Radius Details*” page:

- Verify “*RADIUS Username*” and “*RADIUS Password*” fields are populated. Note down these credentials to use them on a Client device – Laptop
- Make sure “*Customer Group*” is assigned to the customer account
- Click on “*Customer Details*” link to navigate back to “*Customer Details*” page

Customer JB1 (21)

ID 21
Name Joe Bloggs
Nickname JB1
Invoicing ID SJS-5011

Customer Radius Details

RADIUS Credentials

Username 00:11:22:33:44:55 Password test1
tests_JB1

Individual Radius Checks View
Individual Radius Replies View

Customer Details Customer Radius Usernames Individual Radius Checks Individual Radius Replies

Browse Customer Groups

Group -- All --

Back Search

Customer Radius Groups

Results 1 - 1 of 1 Number of results to display per page: 50

Username	Groupname	Priority
00:11:22:33:44:55	tests_package_512/128_1GB	5

Add

[Documentation](#) | [Release Notes](#)
copyright © Azotel Technologies Ltd. 2004 - 2012

7.6 Test the setup

After successful completion of steps described in the previous chapters, test the setup by connecting a laptop to LAN interface of the pfSense device. Laptop should be assigned a dynamic IP address. When attempting to browse captive portal should be presented. Fill out the form with the credentials set for the customer account in the 7.5 chapter of this manual. You should be able to login and browse.

pfSense captive portal - Bon Echo

File Edit View History Bookmarks Tools Help

http://10.10.10.1:8000/index.php?redirurl=http%3A%2F%2Fpolonia.wp.pl%2Fkat%2C10102Z DSL DSL Search

Damn Small Linux DSL Forums DSL Wiki DSL Store DSL Market Public Radio LibriVox Latest Headlines

pfSense captive portal

Welcome to the pfSense Captive Portal! This is the default page since a custom page has not been defined.

Username: tests_Joe0
Password: *****

Continue

Azotel Confidential Proprietary

8 RADIUS Proxy Setup

The purpose of this section is to outline a process of setting up a remote, FreeRADIUS based server, that will act as a proxy RADIUS enabling operator with a local RADIUS server while synchronizing all RADIUS data with SIMPLer server. Azotel encourages all operators, to setup up their own set of RADIUS servers set in the PROXY mode, so that their network benefits from local, low latency RADIUS services preferably with a possibility of adding redundancy measures such as multiple, failover RADIUS servers. SIMPLer RADIUS server instance would act as a master RADIUS server for all remote RADIUS server instances.

8.1 FreeRADIUS installation on CentOS system

This chapter outlines steps required to install a minimalistic FreeRADIUS server edition, that can be configured as a proxy/failover RADIUS server. It can be skipped if a running instance of FreeRADIUS is available to the operator already. For fresh installation Azotel recommends using CentOS system in case of any remote expertise is required at any stage. The below command installs the FreeRADIUS server on a clean install of CentOS 5.X series OS. Please refer to <http://www.centos.org/> for details on installing the system.

```
yum install freeradius -y
```

8.2 NAS setup in SIMPLer

This chapter outlines steps required setup a NAS (Network Access Server) entry in SIMPLer to allow RADIUS traffic from the proxy Radius server. Note that without a respective NAS entry proxy RADIUS server will not be able to submit any RADIUS queries with the SIMPLer's RADIUS server. SIMPLer RADIUS server will NOT respond to any queries from unknown source.

In the SIMPLer system please add a respective entry in the NAS table, that will correspond to the proxy free radius server. Four important details to pay attention here are:

- **IP address** – must match the IP address the RADIUS queries will be send to the master RADIUS server (SIMPLer server IP address) from.
- **Name** – can be set to anything as it has only descriptive role on the SIMPLer server
- **Type** – must be set to “other” in case of using FreeRADIUS as a proxy server
- **Secret** – secret used here must than be also used in the proxy.conf file of the proxy Radius server

Note: Please refer to chapter 4.2 of this manual for the full process outlining adding a new NAS table entry to the system

IP Address / Hostname*	Name*	Type*	Secret*	Port	Community	Description
188.121.0.12	testss_maciej	other	testing123			

Figure 8.2-1 Example entry for proxy radius server in the “Radius NAS” table

Note: All NAS related changes will be applied to the radius server within 5 minutes from being submitted in the system

8.3 FreeRADIUS setup

This chapter outlines steps required setup a FreeRADIUS server as a proxy. This can be set on any existing FreeRADIUS server instance. First thing to find is where the FreeRADIUS configuration files are being stored. In case of a standard CentOS install the configuration files will be located in the /etc/raddb folder. For any other system please replace the /etc/raddb folder with appropriate location. All relevant proxy setup can be found in the proxy.conf file. To edit this file on CentOS system please execute:

```
vim /etc/raddb/proxy.conf
```

The section, that needs to be defined in there in case we want to proxy all local standard requests (w/o domain) is the real NULL section. The details in the section must match respective NAS details put into SIMPLer. The example below is specified for the proxy RADIUS server working with wib.azotel.com server:

```
realm NULL {
    type          = radius
    authhost      = wib.azotel.com:1812
    accthost      = wib.azotel.com:1813
    secret        = MacDev2652
}
```

Please note that a sample proxy.conf file can be found in the “Annex C” part of this manual.

When the configuration process is finished please restart the proxy server to submit the changes. To do this on the CentOS system please execute following command:

```
/etc/init.d/radiusd restart
```

8.4 RADIUS: Service Log

There is a feature that allows operator to access a RADIUS server log that covers requests coming from 'unknown' NAS'es. This log might help operator resolving typical issues with adding a new NAS into the network, when in some cases the IP address on the NAS will not correspond to the IP address seen at the RADIUS server. The feature can be accessed from the 'RADIUS' part of SIMPLer system under 'Service Log' button as shown on Fig. 8.4-1

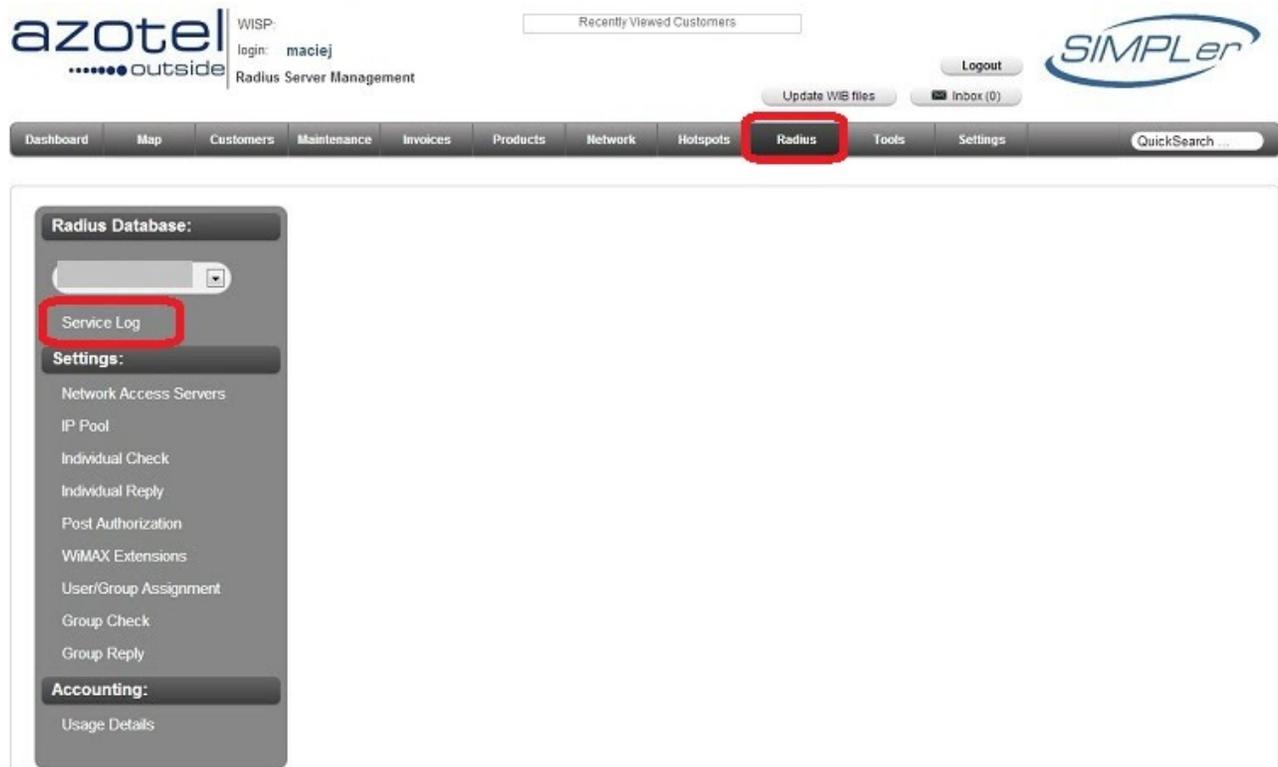
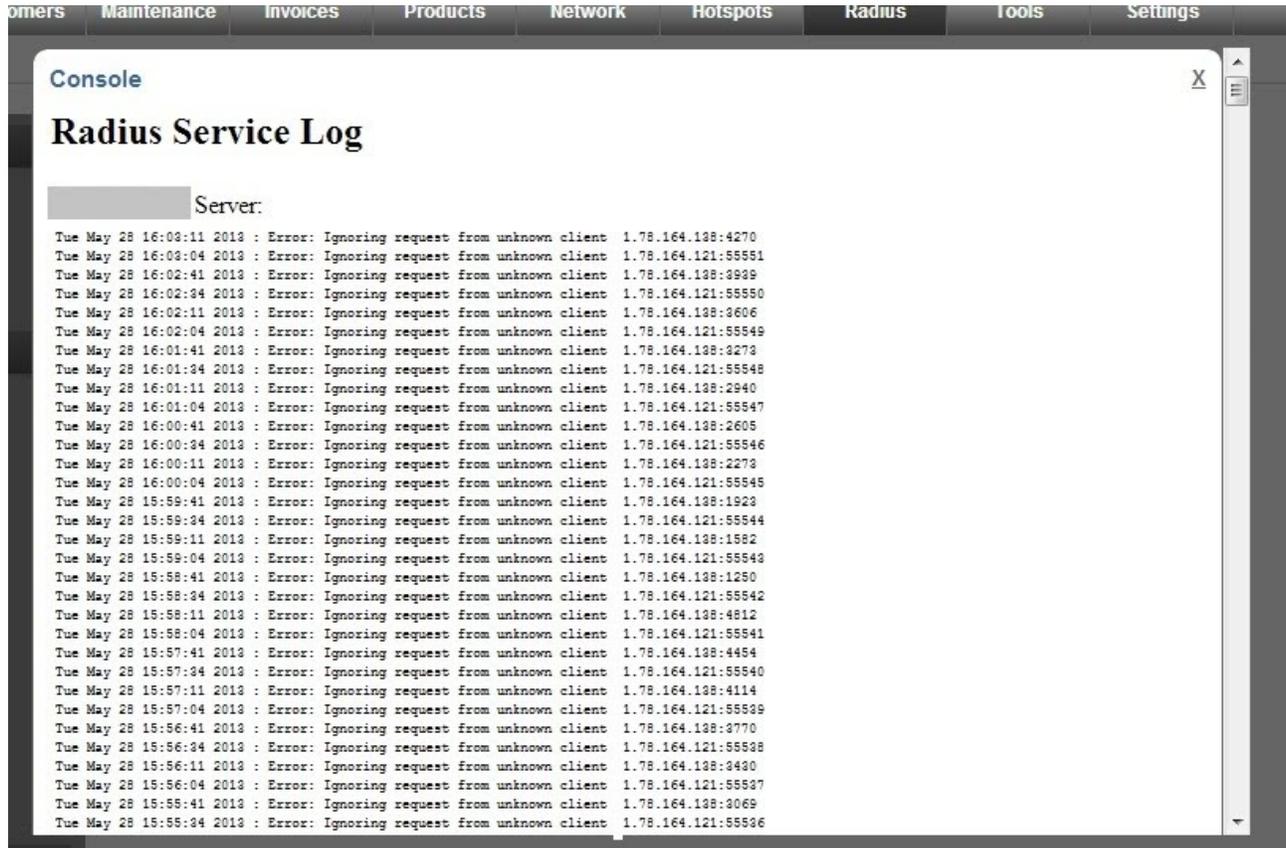


Fig.1. SIMPLer: 'RADIUS' page

The log as presented on Fig.2. will cover the all 'unknown NAS' requests from the last 1000 entries in the RADIUS server log sorted by date (descending)



The screenshot shows a web application interface with a navigation menu at the top containing 'Users', 'Maintenance', 'Invoices', 'Products', 'Network', 'Hotspots', 'Radius', 'Tools', and 'Settings'. The 'Radius' tab is selected. Below the menu is a 'Console' window titled 'Radius Service Log'. The log content is as follows:

```
Server:
Tue May 28 16:03:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:4270
Tue May 28 16:03:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55551
Tue May 28 16:02:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:3939
Tue May 28 16:02:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55550
Tue May 28 16:02:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:3606
Tue May 28 16:02:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55549
Tue May 28 16:01:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:3273
Tue May 28 16:01:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55548
Tue May 28 16:01:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:2940
Tue May 28 16:01:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55547
Tue May 28 16:00:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:2605
Tue May 28 16:00:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55546
Tue May 28 16:00:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:2273
Tue May 28 16:00:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55545
Tue May 28 15:59:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:1923
Tue May 28 15:59:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55544
Tue May 28 15:59:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:1582
Tue May 28 15:59:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55543
Tue May 28 15:58:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:1250
Tue May 28 15:58:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55542
Tue May 28 15:58:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:4812
Tue May 28 15:58:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55541
Tue May 28 15:57:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:4454
Tue May 28 15:57:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55540
Tue May 28 15:57:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:4114
Tue May 28 15:57:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55539
Tue May 28 15:56:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:3770
Tue May 28 15:56:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55538
Tue May 28 15:56:11 2013 : Error: Ignoring request from unknown client 1.78.164.138:3430
Tue May 28 15:56:04 2013 : Error: Ignoring request from unknown client 1.78.164.121:55537
Tue May 28 15:55:41 2013 : Error: Ignoring request from unknown client 1.78.164.138:3069
Tue May 28 15:55:34 2013 : Error: Ignoring request from unknown client 1.78.164.121:55536
```

Fig.2. SIMPLer: RADIUS Server Log

8.5 Auto RADIUS Groups (From Traffic Shaping Buckets)

This new feature allows operators to set up a fully automated RADIUS groups assignment based on the Traffic Shaping buckets a customer is assigned to. Using this feature, operators can make sure that all customer RADIUS usernames, based on his current Traffic Shaping Bucket, will be assigned with an appropriate RADIUS groups. Using this feature is highly recommended unless operators prefer to manage all RADIUS information manually.

It is important to note that by default this feature is turned off - leaving operators to assign the RADIUS groups manually. To enable this feature please follow below steps:

Step One: Go to Modify WISP on your instance in SIMPLer. (See fig. 8.5-1)

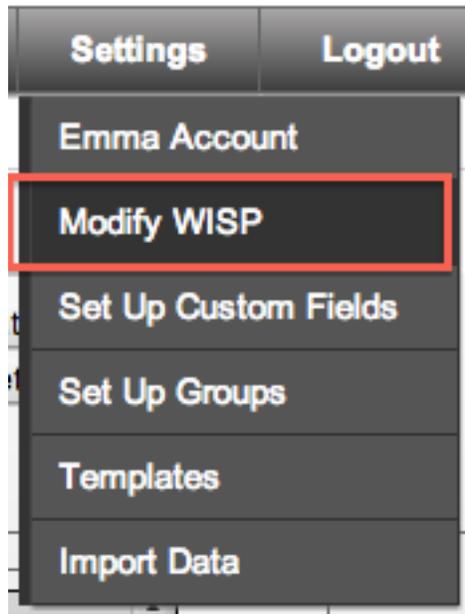


Fig. 8.5-1 Modify WISP

Step Two: Scroll down to the 'Auto update Traffic Shaping Buckets / RADIUS Groups' section. The following settings related to Auto Radius Groups setup can be found in there: (Fig. 8.5-2)

1. Synchronise Radius Groups from Buckets - turns the feature on/off
2. Automated Daily Check - when set to 'on', the system will execute the 'Auto Radius Groups' routine in the daily database maintenance run. It is highly recommended to enable this option when using Auto Radius Groups
3. Synchronise Radius Groups from Buckets - Action when no groups are assigned to a bucket - when a customer is assigned to a bucket that does not have any Radius Groups assigned there, the SIMPLer system can either:
 - o Leave Current RADIUS groups - leaving customer setup intact
 - o Remove all RADIUS groups - remove Radius groups from Radius accounts
4. Reassign RADIUS groups only if bucket's changed - (Not recommended) This option is to be used carefully as it is advised to leave it off and keep everything synchronised. If enabled - system will only synchronise Radius groups in cases where a bucket has changed for a customer.

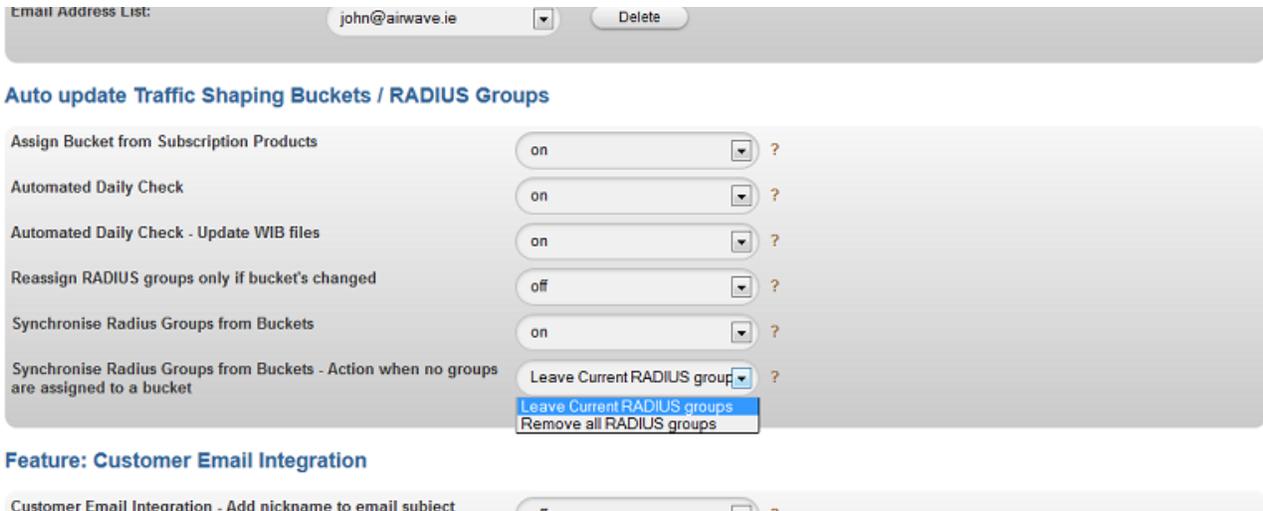


Fig. 8.5-2 Auto update Traffic Shaping Buckets' section in operator settings

Step Three: Once you have chosen what you need from each of these options click Update WISP at the top or bottom of this page. (See Fig. 8.5-3)

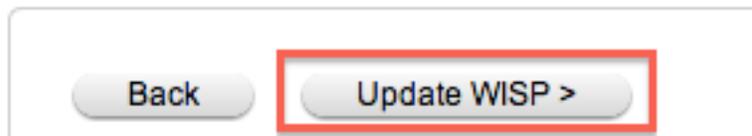


Fig. 8.5-3 Update WISP

Step Four: Once the feature is enabled, there will be a new "Radius Groups" button available for each bucket defined under on the "Traffic Shaping Buckets" page. (See Fig. 8.5-4). This page allows operators to assign radius groups to a traffic shaping bucket. The radius groups then will be updated automatically for each Radius username set for a customer accordingly to a traffic bucket account it is assigned to.

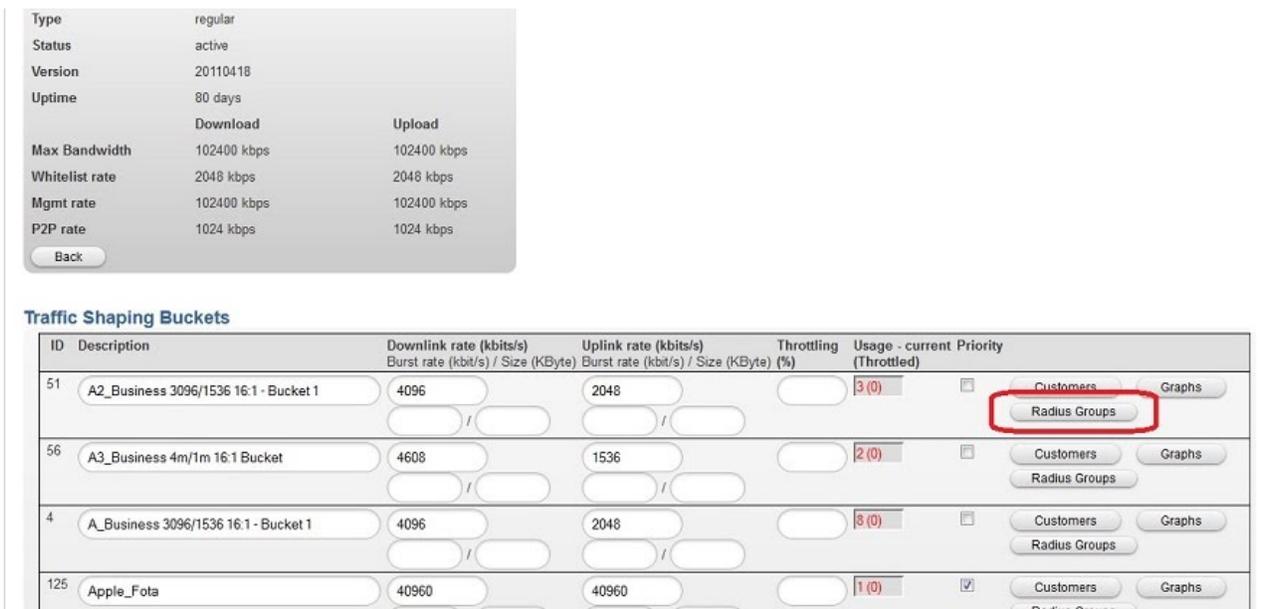


Fig. 8.5-4 Traffic Shaping Buckets page

Multiple radius groups can be assigned to a single bucket. (See Fig. 8.5-5). Every group defined here will be used to setup each Radius username under a customer account that has the particular traffic shaping bucket set the account with. Using the 'Type' variable of the Radius Group assignments - operator can define different Radius Group sets a customer should be put when the account is in:

- Current
- Throttled
- Disconnected

i.e. using the Type might be very useful - first to put a customer to a slower speed group when throttled and disconnected group when customer is disconnected (provided that the 'Leave User/Password in RADIUS when disconnecting customer' option is selected under 'Radius Server Details' section in 'WISP details' (see fig. 8.5-6) as otherwise customer accounts will be removed from Radius server once a customer account is 'disconnected' in SIMPLer)

Note that when using 'Throttled' - a throttle option must be defined under a Traffic Shaping Bucket

The screenshot shows a 'Console' window with the following content:

Bucket Details

Description	123
Downlink rate (kbits/s)	1024
Uplink rate (kbits/s)	1024

RADIUS Groups assigned to the bucket

Results 1 - 4 of 4 Number of results to display per page : 50

ID	Type	Groupname	
12	Current	testss_SandvineControlAttribute	
41	Current	testss_SECOND GROUP	
6	Disconnected	testss_87	
5	Throttled	testss_SECOND GROUP	

Buttons: Add

Fig. 8.5-5: Multiple Radius Groups

The screenshot shows the 'Radius Server Settings' form with the following fields:

- RADIUS Username Default Prefix:
- RADIUS Username Default Suffix source:
- RADIUS Username Default Length:
- RADIUS Default Password:
- Leave User/Password in RADIUS when disconnecting customer:

Fig. 8.5-6: Radius Server Details

The radius groups are recalculated on the following occasions:

1. When an operator changes customers subscriptions in their subscription details. (See Fig. 8.5-7) - note that this will recalculate this single customer account only.
2. On any customer status changes.
3. During daily Radius Group recalculation - if this option is enabled (recommended) under "Modify WISP" page. (See step Two - part 2).
4. By a manual execution of the '**Update Radius Groups from Buckets**' from tools in SIMPLer. (See Fig. 8.5-7)
5. On each SAND - customer status change.



Fig. 8.5-7: Tools: 'Update Radius Groups from Buckets' option

Note: Under a customer account - only username groups with **Default Priority** will be a subject to Auto changes. Groups set manually under customer account with priorities different than 5 (Default) will remain intact. Using this approach enables operator to define groups dedicated to a customer - such as a 'private or public IP' groups that should never be a subject to changes.

Annex A: References

A.1 Document References

A.2 Link References

- [L1] <http://www.azotel.com/>
Azotel homepage.
- [L2] <http://www.freeradius.org/>
FreeRADIUS server homepage

Annex B: Definitions and abbreviations

B.1 Definitions

B.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

SIMPLer Azotel's integrated Operators platform

Annex C: Sample proxy.conf file

```
#
# proxy.conf - proxy radius and realm configuration directives
#
# This file is included by default. To disable it, you will need
# to modify the PROXY CONFIGURATION section of "radiusd.conf".
#
#
# Proxy server configuration
#
# This entry controls the servers behaviour towards ALL other servers
# to which it sends proxy requests.
#
proxy server {

#
# If the NAS re-sends the request to us, we can immediately re-send
# the proxy request to the end server. To do so, use 'yes' here.
#
# If this is set to 'no', then we send the retries on our own schedule,
# and ignore any duplicate NAS requests.
#
# If you want to have the server send proxy retries ONLY when the NAS
# sends it's retries to the server, then set this to 'yes', and
# set the other proxy configuration parameters to 0 (zero).
#
# Additionally, if you want 'failover' to work, the server must manage
# retries and timeouts. Therefore, if this is set to yes, then no
# failover functionality is possible.
#
    synchronous = no
```

```
#
# The time (in seconds) to wait for a response from the proxy, before
# re-sending the proxied request.
#
# If this time is set too high, then the NAS may re-send the request,
# or it may give up entirely, and reject the user.
#
# If it is set too low, then the RADIUS server which receives the proxy
# request will get kicked unnecessarily.
#
    retry_delay = 5

#
# The number of retries to send before giving up, and sending a reject
# message to the NAS.
#
    retry_count = 3

#
# If the home server does not respond to any of the multiple retries,
# then FreeRADIUS will stop sending it proxy requests, and mark it 'dead'.
#
# If there are multiple entries configured for this realm, then the
# server will fail-over to the next one listed. If no more are listed,
# then no requests will be proxied to that realm.
#
#
# After a configurable 'dead_time', in seconds, FreeRADIUS will
# speculatively mark the home server active, and start sending requests
# to it again.
#
# If this dead time is set too low, then you will lose requests,
# as FreeRADIUS will quickly switch back to the home server, even if
# it isn't up again.
#
# If this dead time is set too high, then FreeRADIUS may take too long
# to switch back to the primary home server.
#
# Realistic values for this number are in the range of minutes to hours.
# (60 to 3600)
#
    dead_time = 120

# An ldflag attribute for all realms to be included in a round-robin
# setup must be specified, and that ldflag must be the same for all
# realms of the same name.
# Currently (0 or fail_over) and (1 or round_robin) are the
# supported values for ldflag. Fail over is the default setup.
#
# DO NOT INCLUDE LOCAL AUTH/ACCT HOST REALMS IN A ROUND-ROBIN QUEUE.

#
# If all exact matching realms did not respond, we can try the
# DEFAULT realm, too. This is what the server normally does.
#
# This behaviour may be undesired for some cases. E.g. You are proxying
# for two different ISP's, and then act as a general dial-up for Gric.
# If one of the first two ISP's has their RADIUS server go down, you do
# NOT want to proxy those requests to GRIC. Instead, you probably want
# to just drop the requests on the floor. In that case, set this value
# to 'no'.
#
# allowed values: {yes, no}
#
    default_fallback = yes

#
# Older versions of the server would pass proxy requests through the
# 'authorize' sections twice; once when the packet was received
# from the NAS, and again after the reply was received from the home
# server. Now that we have a 'post_proxy' section, the replies from
# the home server should be sent through that, instead of through
# the 'authorize' section again.
#
# However, for backwards compatibility, this behaviour is configurable.
# The default configuration is 'no', because this option is deprecated
# and will be removed in the future.
```

```

#
# allowed values: {yes, no}
#
#     post_proxy_authorize = no
#
}

```

```

#
# Configuration for the proxy realms.
#
# The information given here is used in conjunction with the 'realms'
# file. This format is preferred, as it is more flexible. The realms
# listed here take priority over those listed in the 'realms' file.
#
# A standard realm entry. A request from "user@company.com" will be
# sent to radius.company.com as "user", unless the 'nostrip'
# configuration item is specified. If the 'nostrip' configuration
# item is specified, then the request will be proxied as
# "user@company.com"
#
#realm company.com {
#     type           = radius
#     authhost       = radius.company.com:1600
#     accthost       = radius.company.com:1601
#     secret         = testing123
#}

# A realm entry with an optional fail-over realm. A request from
# "user@isp2.com" will be sent to radius.isp2.com as "user@isp2.com",
# because the 'nostrip' directive is specified for this realm.
#
#realm isp2.com {
#     type           = radius
#     authhost       = radius.isp2.com:1645
#     accthost       = radius.isp2.com:1646
#     secret         = TheirKey
#     nostrip
#}
#
# The fail-over realm for isp2.com
#
#realm isp2.com {
#     type           = radius
#     authhost       = radius2.isp2.com:1645
#     accthost       = radius2.isp2.com:1646
#     secret         = TheirKey2
#     nostrip
#}

#
# 1st node serv.com...set up for round-robin.
#
# The load balancing 'ldflag' attribute can be used to perform
# load balancing. Allowed values are 'fail_over' and 'round_robin'.
#
# If there is no ldflag attribute, or it is set to 'fail_over', then
# the realms are treated as "fail-over". That is, the first matching
# realm is used, unless it is down, in which case the realm "fails
# over" to the second matching realm. The process continues until an
# active matching realm is found, OR the DEFAULT realm is returned.
#
# If the ldflag attribute is set to 'round_robin', then all active
# realms of the same name are put into a pool internally in the
# server, and the proxied requests are evenly divided among the
# realms in the pool. For this to work, all realms of the same name
# MUST have the same value of their 'ldflag' attributes. Mixing up
# different types of load balancing schemes for the same realm will
# cause problems.
#
# The round_robin load balancing method is a probabilistic method
# which evenly scatters the requests among the home servers.
#
# Note that you CANNOT include local auth/acct host realms in a
# round-robin queue. Having a server load balance requests to itself
# doesn't make any sense, as it only doubles the amount of work
# which is needed to be done.
#

```

```

#realm serv.com {
#   type           = radius
#   authhost       = radius.serv.com:1645
#   accthost       = radius.serv.com:1646
#   secret         = TheirKey
#   ldflag         = round_robin
#   nostrip
#}

#
# Another node for serv.com
#
#realm serv.com {
#   type           = radius
#   authhost       = radius2.serv.com:1645
#   accthost       = radius2.serv.com:1646
#   secret         = TheirKey2
#   ldflag         = round_robin
#   nostrip
#}

#
# A third round-robin node realm for serv.com
#
#realm serv.com {
#   type           = radius
#   authhost       = radius3.serv.com:1645
#   accthost       = radius3.serv.com:1646
#   secret         = TheirKey2
#   ldflag         = round_robin
#   nostrip
#}
#
#
#
# This is a local realm.  The requests are NOT proxied,
# but instead are authenticated by the RADIUS server itself.
#
# You don't need a secret if BOTH 'authhost' and 'accthost' are
# set to LOCAL.
#
#realm bla.com {
#   type           = radius
#   authhost       = LOCAL
#   accthost       = LOCAL
#}

#
# This is a sample entry for iPass.
#
#realm IPASS {
#   type           = radius
#   authhost       = ipass.server.hostname:11812
#   accthost       = ipass.server.hostname:11813
#
#   # The shared secret here must be the same
#   # value as the secret of the NetServer found in the
#   # /usr/ipass/raddb/clients file of your NetServer software.
#   secret         = mysecret
#   nostrip
#}

#
# This realm is used mainly to cancel proxying.  You can have
# the "realm suffix" module configured to proxy all requests for
# a realm, and then later cancel the proxying, based on other
# configuration.
#
# For example, you want to terminate PEAP or EAP-TTLS locally,
# you can add the following to the "users" file:
#
# DEFAULT EAP-Type == PEAP, Proxy-To-Realm := LOCAL
#
#realm LOCAL {
#   type           = radius
#   authhost       = LOCAL
#   accthost       = LOCAL

```

```
#}

#
# This realm is for requests which don't have an explicit realm
# prefix or suffix.  User names like "bob" will match this one.
#
realm NULL {
    type          = radius
    authhost      = wib.azotel.com:1812
    accthost      = wib.azotel.com:1813
    secret        = MacDev2652
}

#
# This realm is for ALL OTHER requests.
#
#realm DEFAULT {
#    type          = radius
#    authhost      = wib.azotel.com:1812
#    accthost      = wib.azotel.com:1813
#    secret        = MacDev2652
#}
```

Annex D: Change history

Change history				
Date	Author(s)	Subject/Comment	Old	New
06-Sep-10	Maciej	Initial Version	n/a	001
16-Sep-10	Maciej	First Revision	001	002
21-Sep-10	Maciej	Quick Start chapter, Customer IP Table chapter	002	003
02-Dec-10	Tim	Minor formatting changes.	003	004
22-Dec-10	Maciej	Proxy RADIUS Setup	004	005
20-Jun-11	oharej	Formatting	005	100
16-Feb-12	justyna	Updating screenshots	100	101
17-Jun-13	paul	Changed doc's title, copyright and correct year, doc num on all pages	101	200
17-Jul-13	paul	Feature Updates	200	201
20-Aug-13	paul	Feature Updates	201	202