Radmin® Radius User Administration

Administrator Help for RAdmin version 1.19

RAdmin

Table of Contents

1. Introduction

This document contains help and information for users of the RAdmin Radius User Administration System.

RAdmin provides a Web interface to a Radius user database. You can use RAdmin to add, configure and remove the users who are allowed to log into your network. You can use RAdmin to change their password, control how much time they are permitted to use, and also to set up a static IP address.

You can also use RAdmin to:

- get usage summaries for all your users
- check the login history of your users
- investigate problems in your user authentication system
- generate modem usage reports

RAdmin is not a user billing or invoicing system.

‘RAdmin’ and the RAdmin logo are registered trademarks of Open System Consultants Pty Ltd, a subsidiary of Radiator Software Oy

2. How it works

RAdmin works together with your Radiator® AAA Server to control who is permitted to log in to your network. Whenever a user connects and authenticates to an access server in your network, the access server send an “access request” to Radiator. Radiator looks in your RAdmin user database to check the password. If the password is correct, Radiator tells the terminal server to let the user in. If the password is not correct, or some other precondition is not satisfied, the user is rejected. You can use RAdmin to add and remove users, and to change their password and other login preconditions.

After the user is connected, the terminal server sends an “accounting request” to Radiator with details about the new session that has been started. Radiator saves this information in the RAdmin usage database.

When the user finally disconnects, the terminal server sends another “accounting request” to Radiator with details about the completed session, including the total session time and bytes counts. Radiator also saves this information in the RAdmin usage database. You can use RAdmin to get total usage summaries for your users, and to drill down to details for each session.

If during its operation, Radiator detects any problems, or gets any errors, they will be logged in the RAdmin Message Log. You can use RAdmin to investigate the Message Log.

3. General information

Following chapters describe general RAdmin information, for example various date and time formats and functionalities like toolbar and searches.

3.1. Access control and permissions

In order to access your RAdmin web pages, your system administrator may have enabled access control to your web site. That will mean you will have to enter a username and password before you can get to any of the RAdmin web pages.

Your system administrator will tell you the username and password you will need to enter to get access. Your system administrator can also individually tailor access to specific pages and functions in RAdmin. If you are unable to access a function, or an expected menu item does not appear, its probably because your system administrator has disabled your access to that function.

3.2. The toolbar

At the top of each page in Radmin is a toolbar, which allows you to quickly get to the most commonly used pages in RAdmin. It usually contains the following links:

- List Users
- Add a User
- Log
- Usage Summary
- Current sessions
- Modem usage report

Your RAdmin administrator can customize the toolbar to suit your organization, and add links to other RAdmin pages that you wish to access frequently, or even to other administrative web pages that you commonly need to use in your organization.

3.3. Entering dates and times

RAdmin allows you to enter dates in a variety of formats, and includes many fast shorthand ways of entering dates in the past and the future. All times and dates are entered and displayed in your time zone’s local time.

All dates stored and displayed in RAdmin include both the date and the time. Wherever you can enter a date, you can also enter the time. If you do not specify a time, it always defaults to midnight at the beginning of the day you specify. If you enter a time it must be in the format hh:mm(:ss). The seconds are optional. Times are in 24 hour time format. Some examples are:

- 11:55
- 16:20:30
- 08:08
- 09:5
- 00:00 (i.e. midnight)

Dates are stored and displayed in RAdmin including the full 4 digit year. When entering dates, you can enter shorthand years, such as “99” or “00”, and RAdmin will make an educated guess about which year you mean.

During installation, your RAdmin administrator will have chosen the appropriate date format for your locality. This controls how dates are printed in RAdmin, and also how you must enter exact dates.

Many of the shorthand date formats allow you to use contractions. For example, instead of “1 week”, meaning 1 week in the future, you can enter “1w”. Instead of “today” you can enter “tod”.

Table 1. Permitted date/time formats

General date format	Meaning	Examples
now	The date and time of right now	now
today	The date of today, time defaults to midnight at the beginning of today.	tod today 10:55
tomorrow	The date of tomorrow	tom 9:20
forever	The largest possible time value, effectively the end of time	forever forev

n minutes	The number of minutes in the future.	1mi 3 minutes 5mins
n minutes ago	The number of minutes in the past.	2m ag 3 minutes ago 66mins ago
n hours	The number of hours in the future.	1h 3hours 5h
n hours ago	The number of hours in the past.	2hag 3 hours ago 6h ago
n days	The number of days in the future. “1 day” is the same as “tomorrow”	1d 3day 5d 12:00
n days ago	The number of days in the past. “1 day ago” is yesterday	2dag 3 day ago 6d ago
n weeks	The number of weeks in the future. If today is Wednesday, then “2 weeks” would be wednesday 2 weeks from today. “1 week” is the same as “7 days”	2 w 3 weeks 15:00
n weeks ago	The number of weeks in the past. “1 week ago” is the same as “7 days ago”	3wag 6week ago 3w ag 21:30
n months	This day of the month a number of months in the future.	2m 3month
n months ago	This day of the month a number of months in the past.	1mag 4 mon ago
n years	Todays date a number of years in the future. “1 year” is the same as “12 months”	1y 2 year
n years ago	Todays date a number of years in the past. “1 year ago” is the same as “12 months ago”	2yag 3 y ago
dd/mm/yyyy	(Only if your administrator has chosen your local date format as “dd/mm/yyyy”) The exact date given.	12/5/99 13:00 1/1/00 5/9/2001 08:00 30/12/1999
mm/dd/yyyy	(Only if your administrator has chosen your local date format as “mm/dd/yyyy”) The exact date given.	5/12/99 13:00 1/1/00 9/5/2001 08:00 12/30/1999

yyyymmdd	The exact date given.	20000101 12:00 20011225

3.4. Entering time intervals

Some data fields require an time interval to be entered to specify a period of time, as opposed to an exact date. time intervals can be entered in a variety of ways. Some examples are:

- 10
- 1h10m5s
- 1:10:5

Table 2. Permitted time interval formats

Time interval format (N is an integer)	Meaning	Examples
n	an exact number of seconds	10 12455
*n*s	Exact number of seconds	10s 12455s
*n*m	Exact number of minutes	5m 60m
*n*h	Exact number of hours	2h 155h
*n*h*n*m	Hours and minute	1h55m 10h5m
*n*m*n*s	Minutes and seconds	5m55s 1m5s
n:*n*	Minutes and seconds	5:55 1:5
*n*h*n*m*n*s	Hours minutes and seconds	1h55m10s 5h5m5s
n:*n*:*n*	Hours minutes and seconds	1:55:10 5:5:5

3.5. Using dates in searches

A number list pages allow you to search for items by date. You will see “date from” and “to” fields. For example, on the List Users page, you can search by the “Valid from” date. In these kind of date searches, you can limit the date range searched by entering a start date/time and/or an end date/time. If you enter neither the start nor the end date, then all the matching dates will be listed.

The dates and times you enter may be any of the supported date/time formats. See Entering dates and times on page 2.

Table 3. Example date ranges in searches

date from	to	Meaning

		All dates
now		Any time from right now
	now	Any time up until right now
	1 week	Any time up until midnight at the beginning of the day 1 week from today
1 d ago	1d	Any time from midnight at the beginning of yesterday to midnight at the end of today
1/1/99	tod 12:00	Any time from midnight at the beginning of January 1 1999 to midday today
now	1y	Any time from right now to 1 year from now
tod 8:00	tod 10:55	Any time from 8 am today to 10:55 am today.
tod	tom	Any time today (i.e from midnight at the beginning of today to midnight at the end of today)

3.6. Using text in searches

When you enter some text into a “text like” field on a list page. RAdmin will search for all items that contain that text. So if you entered “fred” it would match not only “fred” but also “frederick”, “Alfred” and “myfreddy”. Text searching is case sensitive, so “fred” would not match “Fred” or “AlfredD”.

RAdmin also supports wildcards when searching for text. The following wildcards are supported:

- % means any number of characters
- _ (underscore) means any single character

Table 4. Example text searches

text like	example matches
fred	fred Alfred frederick
al%ce	alice alce alsacelorraine balances
al%	alice alce alsacelorraine
fr_d	fred frod frud fr3d fridge
j__	jim jay jabberwocky major
	anything at all

3.7. Using numbers in searches

Some pages allow you to search certain fields by a numeric value. You will see “number from” and “to” fields. For example, on the List Users page, you can search by the “Login time left” field. In these kinds of searches, you can specify the lower and/or upper limit of the range you wish to match. If you enter neither the lower nor the upper limit, then all possible values will match.

Table 5. Example number searches

number from	to	Meaning
10		10 or more
	100	100 or less
11	11	exactly 11
1	10	1 to 10 inclusive
		anything at all

3.8. Resorting search results

After searching on a search page, you can re-search and sort by a different column by clicking on a column header.

3.9. Service Profiles and RADIUS Check and Reply items

RAdmin gives you detailed control over who can log in, under what circumstances, and to also control the characteristics of their session once they are connected.

Service Profiles allow you to group a number of users with similar login privileges together and to control their privileges easily. The RAdmin Administrator will usually set up a number of Service Profiles, one for each group of users. For example, you might set up a Service Profile for your normal subscribers, and a different Service Profile for your Operations Centre staff that has greater privileges, or can connect through a dedicated line.

When a user attempts to log in, Radiator/RAdmin will perform the following checks in this order:

- Bad Logins count has not been exceeded.
- The Valid From and Valid To dates are OK.
- The password is correct.
- If the user has a Service Profile, that any RADIUS Check Items in that Service Profile match.
- If there are any user-specific RADIUS Check Items for the user, that they match.

RAdmin allows you to easily set RADIUS Check and Reply items for users and Service Profiles.

RADIUS Check Items are checked when a user attempts to log in. All the Check items must be correct, otherwise the user will not be permitted to log in. There is a wide range of RADIUS attributes that may be used as Check Items. You should consult your NAS vendor documentation for information about which ones are supported by your NAS, and how they are used.

RADIUS Reply items are used to configure a user's session once they have successfully logged in. There is a wide range of RADIUS attributes that may be used as Reply Items. You should consult your NAS vendor documentation for information about which ones are supported by your NAS, and how they are used.

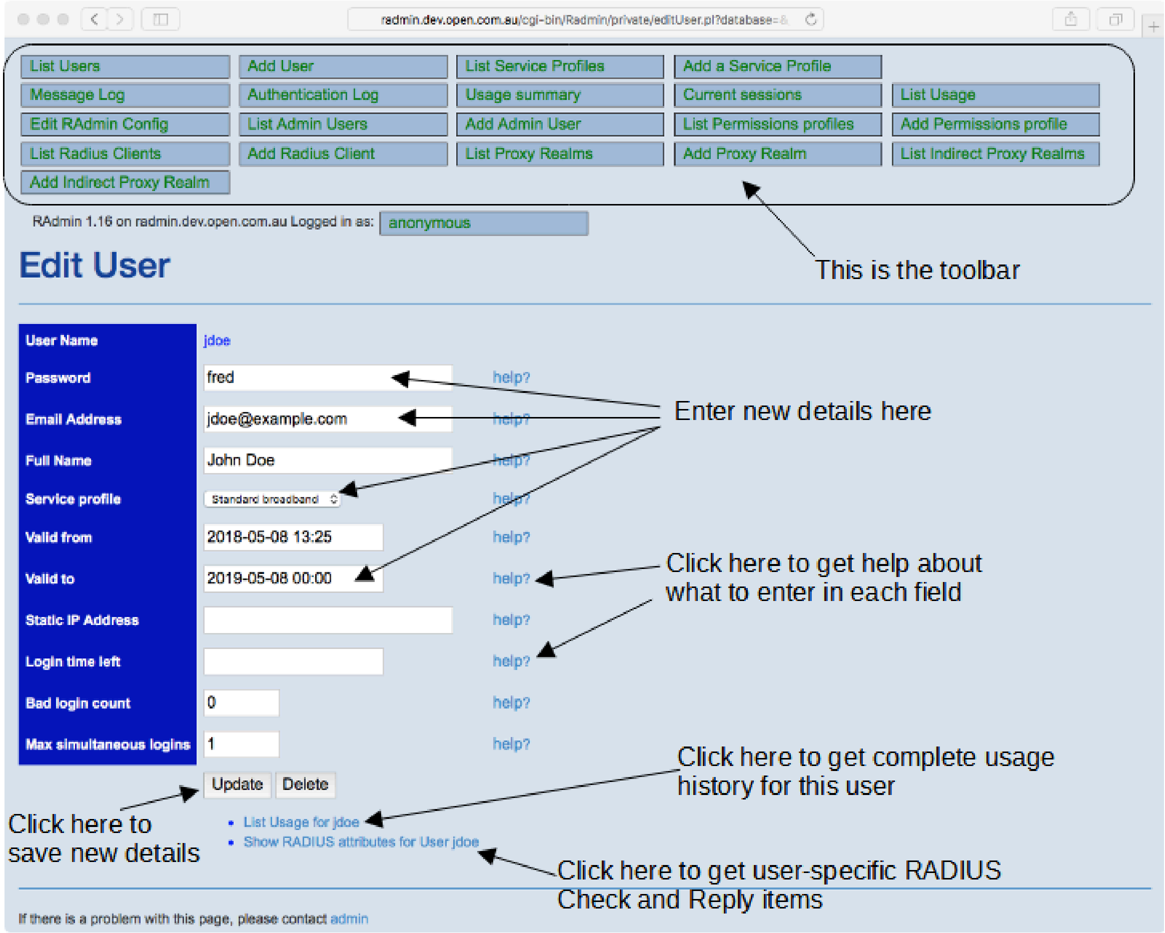
Tip

It is also possible to set Check and Reply items for all users in the Radiator configuration file.

4. Add a User, Edit a User

This page allows you to examine and change the details of a single user. You can set and change their password, and it will have immediate effect. New users can log in as soon as they are added. Users that are deleted will not be able to log in the future.

Figure 1. Edit a User page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Edit User

User Name	jdoe
Password	fred
Email Address	jdoe@example.com
Full Name	John Doe
Service profile	Standard broadband
Valid from	2018-05-08 13:25
Valid to	2019-05-08 00:00
Static IP Address	
Login time left	
Bad login count	0
Max simultaneous logins	1

If there is a problem with this page, please contact admin

This is the toolbar

Enter new details here

Click here to get help about what to enter in each field

Click here to get complete usage history for this user

Click here to save new details

Click here to get user-specific RADIUS Check and Reply items

4.1. Editable fields

The following chapters describe editable fields on Edit User page.

4.1.1. User name

This is the name that the user logs into your network with. Your user will normally have to configure the name into their authentication client software. To log in, they must enter the user name exactly as shown. It is not possible to change a users User Name with the Edit a User. To change a User Name, you would have to delete the old user and add a new one with the correct name.

Your RAdmin administrator may have configured a default value for this field to provide the normal realm for your organization.

4.1.2. Password

This is the password that the user must configure into their authentication client software. To log in successfully, they must enter the user name exactly as shown. Case is important. You can change their password and click **Update**, and their password will be changed immediately.

If you are adding a new user with Add a User, a new password will be automatically generated when the page appears. You can accept that password, or enter a new one if you like. We recommend that when you enter passwords, you adhere to your organization's password policy (if any). Your RAdmin administrator can change the format for automatically generated passwords, or turn off automatic password generation.

4.1.3. Email address

This field can be optionally used to record the user's email address(es). It has no effect on whether or how your user logs in. It is used to send email about subscription access changes if your RAdmin administrator has enabled Subscription Management in your RAdmin installation. Multiple email addresses can be separated by commas or spaces.

Your RAdmin administrator may have configured a default value for this field to provide the normal email domain for your organization.

4.1.4. Full name

This optional field allows you to record the users full name. It has no effect on whether or how your user logs in.

4.1.5. Service Profile

This field allows you to choose a ‘Service Profile’ for this user. A Service Profile describes a common set of RADIUS attributes shared by all the users with that profile. Your RAdmin Administrator will generally set up a separate Service Profile for each category of users your organization supports. If you select a Service Profile for a user, then the attributes from the Service Profile will be used to check and configure this user when they log in. User-specific attributes entered into this Edit User page will override the attributes from the Service Profile. If you choose the blank Service Profile, then there will be no Service Profile for this user, and their login attributes will be controlled by this Edit User page.

4.1.6. Valid from

This field specifies the earliest date and time the user is permitted to log in to your network. See Entering dates and times on page 2. If you enter a date/time that is in the future, the user will not be able to log in until that time.

The standard default value for this field when adding a new user is “now” (i.e. access is possible immediately), although your RAdmin administrator may have configured it differently for your organization.

4.1.7. Valid to

This field specifies the latest date and time the user is permitted to log in to your network. See Entering dates and times on page 2. If you enter a date/time that is in the past, the user will not be able to log in. You can use something like ‘20y’ (i.e 20 years into the future) for users whose accounts are to be valid for a long time.

The standard default value for this field when adding a new user is “1 year” (i.e. it expires one year from today), although your RAdmin administrator may have configured it differently for your organization.

4.1.8. Static IP Address

This optional field allows you to specify a static IP address for that user. You should only enter something in here if you want that user to always get the same IP address when they log in. If you don't enter anything in here (i.e. leave it blank) then the user will be allocated an IP address from the normal address pool. It will usually be different each time they log in. You can see which IP address a user gets by looking at their usage page.

Static IP Address must be entered as a dotted IP address like these examples:

- 10.1.1.5

- 203.63.154.1

4.1.9. Login time left

This optional field specifies the amount of online time (in seconds) the user has left. Each time the user logs out, the time they have used is subtracted from the time they have left. If they try to log in and there is no time left, they will not be permitted to log in at all. Each time they log in, their maximum session time will be set to the amount of time they have left, so they should not be able to overrun their time left. See Entering time intervals

If you leave this field blank, there are no limits placed on their online time.

4.1.10. Bad login count

This field keeps count of how many consecutive bad logins this user has had. It is used to lock out accounts that are being attacked by password guessers. Each time they enter their password incorrectly, this number will be increased. If it get to the bad login limit (usually 5), they will not be able to log in at all until you reset their count to 0. Each time the user logs in correctly, the count will be reset to 0 automatically. This means that users will be locked out if they enter a bad password 5 times in a row.

If you leave this field blank, then no bad login limits will be applied to this user.

4.1.11. Max simultaneous logins

This field specifies the maximum number of sessions the user can be logged in at the same time. Defaults to 1, which means they can log in once at a time. If they try to log in a second time without logging out, they will be rejected. If you leave this field blank, then no simultaneous-use limits will be applied.

If you set it to 0, then they wont be able to log in at all.

4.1.12. Update

Clicking on this button will cause your edits to take effect. Any changes to the password will take effect immediately. After the user database has been updated, the Edit a User page will be redisplayed with the result of your edits. You will note that the Valid from and Valid to dates will be displayed as the full date and time.

4.1.13. Delete

Clicking on this button will cause this user to be permanently removed from the database. It does not remove any usage records for this user from the usage table. If the user is currently logged on it will not log them out, only prevent them from logging in again in the future. The User Name may be reused for another user after deleting.

This button will not appear when adding a new user.

4.1.14. Usage link

Clicking on this link will show the List Usage page showing usage for this user.

This link will not appear when adding a new user.

4.1.15. Edit RADIUS attributes link

This link takes you to the RADIUS attributes page where you can view and edit specific RADIUS attributes for this user. You can add and remove both check and reply items, which means that you can tailor the RADIUS attributes for this user.

This link will not appear when adding a new user.

4.2. Tasks using this page

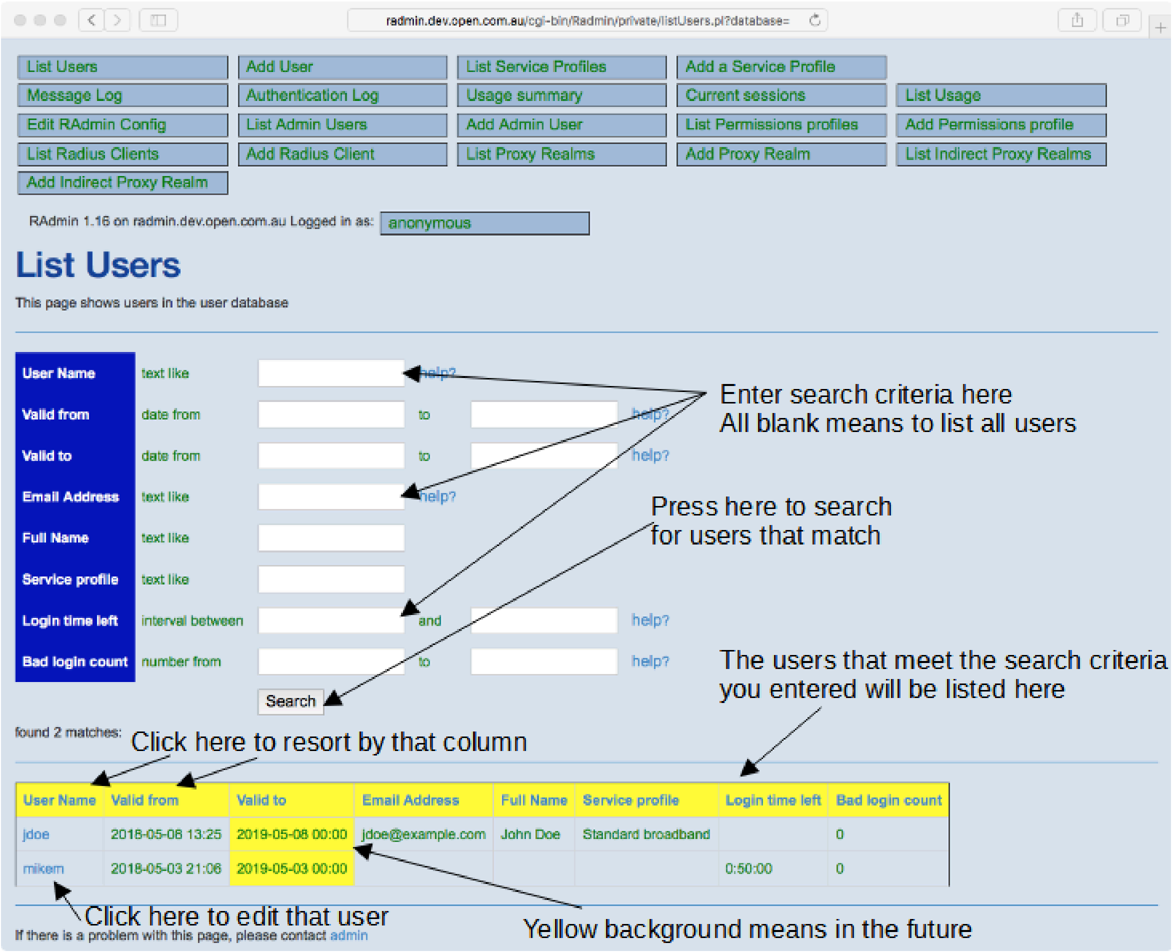
The following common tasks relate to this page:

- Adding a new user on page 48.
- Deleting a user on page 49.
- Changing a password on page 49.

5. List Users

This page allows you to search for and list users in your user database. The list shows the main information about each user, and you can drill down to detailed information for each user.

Figure 2. List Users page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Users

This page shows users in the user database

User Name	text like		help?		
Valid from	date from		to		help?
Valid to	date from		to		help?
Email Address	text like		help?		
Full Name	text like				
Service profile	text like				
Login time left	interval between		and		help?
Bad login count	number from		to		help?

Enter search criteria here
All blank means to list all users

Press here to search
for users that match

The users that meet the search criteria
you entered will be listed here

found 2 matches:

Click here to resort by that column

User Name	Valid from	Valid to	Email Address	Full Name	Service profile	Login time left	Bad login count
jdoe	2018-05-08 13:25	2019-05-08 00:00	jdoe@example.com	John Doe	Standard broadband		0
mikem	2018-05-03 21:06	2019-05-03 00:00				0:50:00	0

Click here to edit that user

Yellow background means in the future

If there is a problem with this page, please contact admin

5.1. Search Criteria

The top part of this page lets you enter search criteria to find particular users or groups of users. The bottom part displays the list of users that satisfy your criteria. You can limit the list of users displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), all the users in your user database will be listed.

5.1.1. User Name

This section restricts which users will be listed in the bottom part by specifying the User Names to match. See Using text in searches on page 5

5.1.2. Email Address

This section restricts which users will be listed in the bottom part by specifying the Email Address to match. See Using text in searches on page 5

5.1.3. Valid from

This section restricts which users will be listed in the bottom part by specifying a range of “Valid from” dates. See Using dates in searches on page 4

5.1.4. Valid to

This section restricts which users will be listed in the bottom part by specifying a range of “Valid from” dates. See Using dates in searches on page 4

5.1.5. Login time left

This section restricts which users will be listed in the bottom part by specifying a matching range of “Login time left”. See Using numbers in searches on page 5

5.1.6. Bad login count

This section restricts which users will be listed in the bottom part by specifying a matching range of “Bad login count”. See Using numbers in searches on page 5

5.2. User List

This section presents a list of users that match the search criteria you entered in the top section. By clicking on a User Name you can drill down to that users details displayed in the “Edit a User” page. See Add a User, Edit a User on page 7. Any “Valid from” or “Valid to” dates that are in the future are shown with a yellow background. Dates in the past are shown with a normal white background.

5.3. Tasks using this page

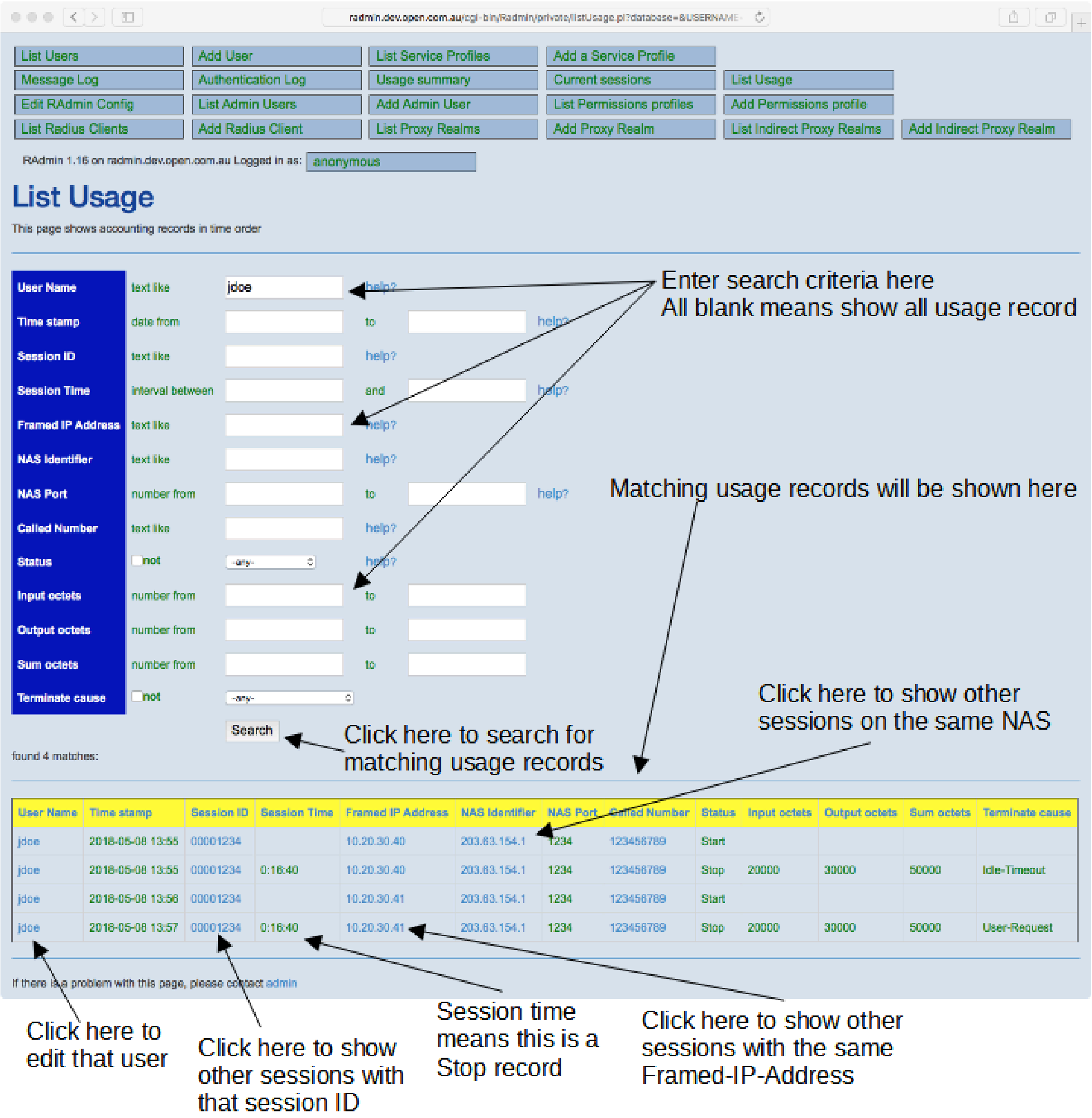
The following common tasks relate to this page:

- Finding a User on page 49.

6. List Usage

This page shows summaries of past login sessions for one or more users. From the usage list, you can drill down to see user details, see all the details of a single session, or see other logins to the same NAS. The list shows both session start and session stop records that match the criteria.

Figure 3. List usage page



User Name	text like	jdoe	help?		
Time stamp	date from		to		help?
Session ID	text like		help?		
Session Time	interval between		and		help?
Framed IP Address	text like		help?		
NAS Identifier	text like		help?		
NAS Port	number from		to		help?
Called Number	text like		help?		
Status	□ not	-any-	help?		
Input octets	number from		to		
Output octets	number from		to		
Sum octets	number from		to		
Terminate cause	□ not	-any-			

found 4 matches:

User Name	Time stamp	Session ID	Session Time	Framed IP Address	NAS Identifier	NAS Port	Called Number	Status	Input octets	Output octets	Sum octets	Terminate cause
jdoe	2018-05-08 13:55	00001234		10.20.30.40	203.63.154.1	1234	123456789	Start				
jdoe	2018-05-08 13:55	00001234	0:16:40	10.20.30.40	203.63.154.1	1234	123456789	Stop	20000	30000	50000	Idle-Timeout
jdoe	2018-05-08 13:56	00001234		10.20.30.41	203.63.154.1	1234	123456789	Start				
jdoe	2018-05-08 13:57	00001234	0:16:40	10.20.30.41	203.63.154.1	1234	123456789	Stop	20000	30000	50000	User-Request

If there is a problem with this page, please contact admin

Enter search criteria here
All blank means show all usage record

Matching usage records will be shown here

Click here to show other
sessions on the same NAS

Click here to search for
matching usage records

Click here to
edit that user

Click here to show
other sessions with
that session ID

Session time
means this is a
Stop record

Click here to show other
sessions with the same
Framed-IP-Address

6.1. Search Criteria

The top part of this page lets you enter search criteria to find particular sessions The bottom part displays the list of sessions that satisfy your criteria. You can limit the list of sessions displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), all the sessions in your accounting database will be listed.

6.1.1. User Name

The restricts the sessions to those belonging to users who match this field. See Using text in searches on page 5

6.1.2. Time stamp

This restricts the list to session that started or stopped during the date/time range given. See Using dates in searches on page 4

6.1.3. Session ID

This restricts the list to sessions that match the Session ID. See Using text in searches on page 5

6.1.4. Session Time

This restricts the list to sessions whose Session time (which is the time the session lasted in seconds) to the range given. Since only session Stop records have a Session Time, if you use this criteria, it will only list session Stops. See Using numbers in searches on page 5

6.1.5. Framed IP Address

This restricts the list to sessions that match the specified Framed IP Address (which is the IP address the user had for the duration of their session). See Using text in searches on page 5

6.1.6. NAS Identifier

This restricts the list to sessions that were authenticated by a certain NAS (i.e. Terminal Servers etc.). The NAS Identifier is an IP address like 203.63.154.1, not a DNS name. See Using text in searches on page 5

6.1.7. NAS Port

This restricts the list to sessions that had the specified NAS-Port, which identifies which interface, modem or port the session was connected to. See Using numbers in searches on page 5

6.1.8. Status

This restricts the list to sessions with the given Acct-Status-Type.

6.2. Usage List

This section presents a list of sessions that match the search criteria you entered in the top section. By default it shows both session Start and session Stop records. Session Start records can be identified by the fact that they do not have a Session Time.

The User Name column shows the exact user name they logged in with.

The Time stamp column shows the date and time that the session started or stopped (in your time zone's local time).

The Session ID is an identifying number that the NAS uses to identify a session. It allocates a new Session ID each time a new session starts. The Session ID will be the same for the Start and Stop of the same session. Session IDs are only unique until the NAS reboots. When a NAS reboots, it starts reusing Session IDs.

Session Time is the length of time the session lasted (in seconds). For session Start records, this will be blank.

Framed IP Address this is the IP address that the user was allocated for the duration of this session.

NAS Identifier is the IP address of the NAS the user was connecting to.

NAS Port is the number of the NAS's interface, modem or port that the user was connecting to.

You can click on the hotlinks in the following columns:

- User Name. This will take you to the Edit a User page for that user. See Add a User, Edit a User on page 7
- Session ID. This will take you to another List Usage page, showing sessions with the same Session ID.
- NAS Identifier. This will take you to another List Usage page, showing sessions with the same NAS Identifier. The NAS Identifier is the IP address of the NAS where the session was connected to.

6.3. Tasks using this page

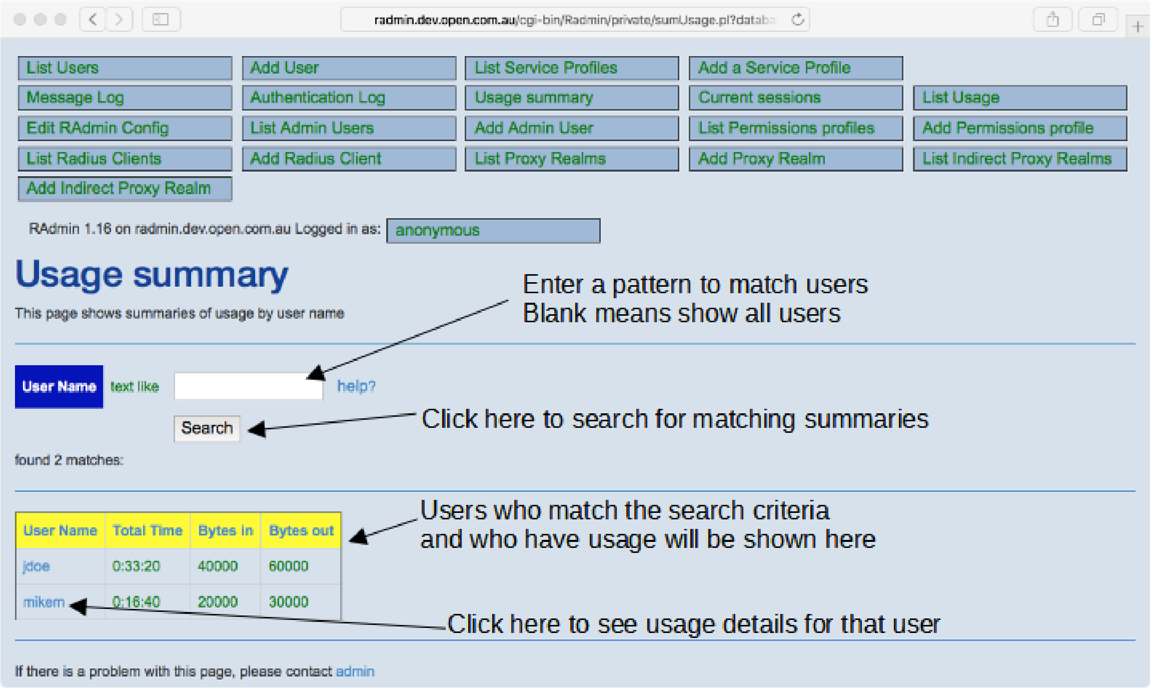
The following common tasks relate to this page:

- See Checking a user's session history on page 50.

7. Usage Summary

This page shows a summary of network usage for some or all of your users. It shows the total login time (in seconds) and total number of bytes in and out for a each user in the interval covered by your accounting table.

Figure 4. Usage summary page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Usage summary

This page shows summaries of usage by user name

Enter a pattern to match users
Blank means show all users

Click here to search for matching summaries

found 2 matches:

User Name	Total Time	Bytes in	Bytes out
jdoe	0:33:20	40000	60000
mikem	0:16:40	20000	30000

Users who match the search criteria
and who have usage will be shown here

Click here to see usage details for that user

If there is a problem with this page, please contact admin

7.1. Search Criteria

The top part of this page lets you enter search criteria to limit the users whose summaries you wish to see The bottom part displays a summary for each user matched. You can limit the list of users displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), summaries for all the user in your database will be listed.

7.1.1. User Name

This section restricts which users will be listed in the bottom part by specifying the User Names to match. See Using text in searches on page 5

7.2. Usage Summaries

This section presents usage summaries for all the user that matched the search criteria you entered in the top section. For each user it shows:

- Total time in seconds that the user was logged in for.
- The total number of bytes in (i.e. bytes transmitted from the user to your network).

- The total number of bytes out (i.e. bytes transmitted from your network to the user).

7.3. Tasks using this page

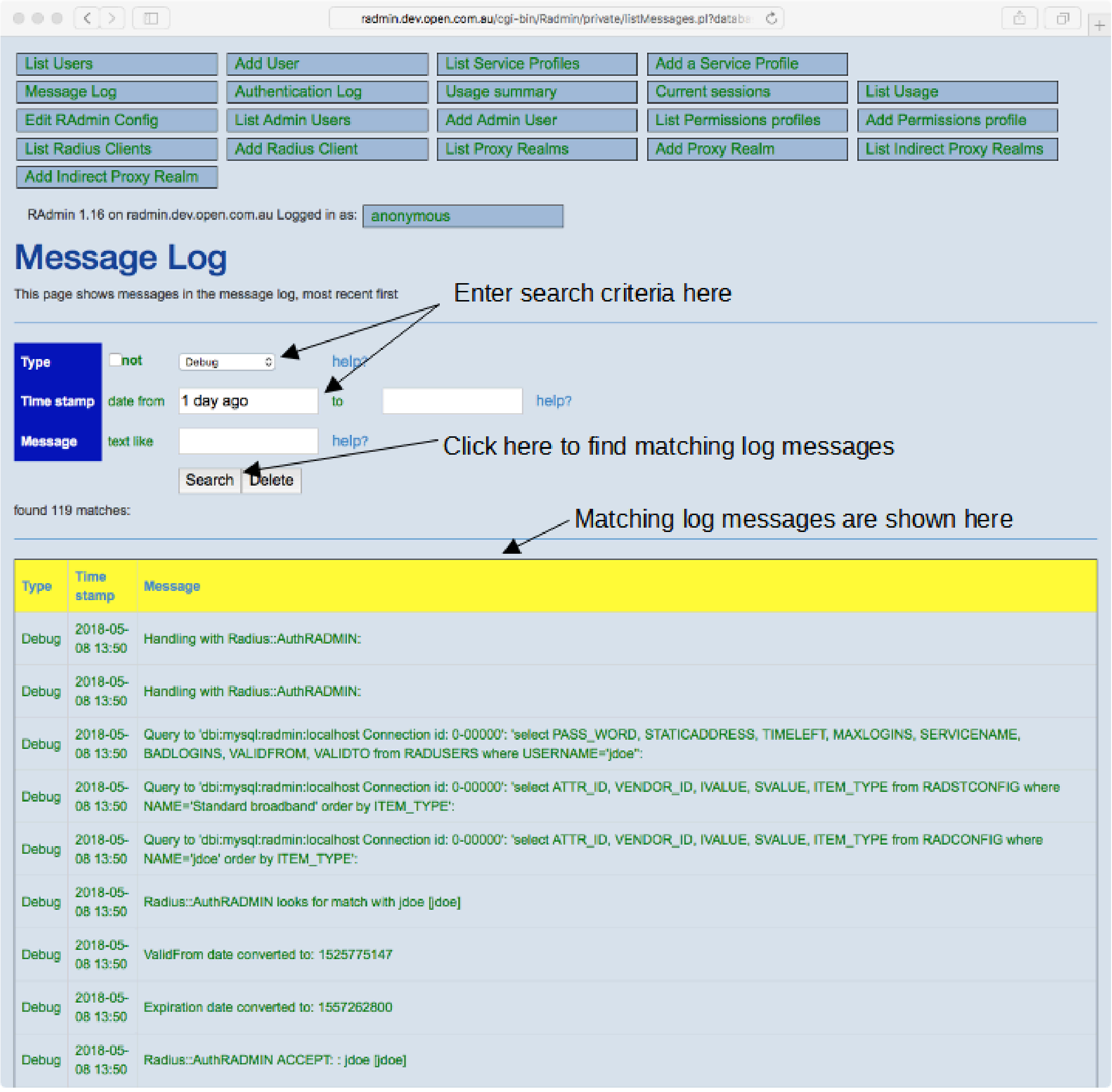
The following common tasks relate to this page:

- Checking usage summaries on page 50.

8. Log

This page allows you to see messages in the RAdmin/Radiator log. Each time Radiator detects a problem, it logs a message to the RAdmin log. This page allows you to look at some or all of those messages.

Figure 5. Log page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Message Log

This page shows messages in the message log, most recent first

Enter search criteria here

Type □not Debug help?

Time stamp date from 1 day ago to help?

Message text like help?

Click here to find matching log messages

found 119 matches:

Matching log messages are shown here

Type	Time stamp	Message
Debug	2018-05-08 13:50	Handling with Radius::AuthRADMIN:
Debug	2018-05-08 13:50	Handling with Radius::AuthRADMIN:
Debug	2018-05-08 13:50	Query to 'dbi:mysql:radmin:localhost Connection id: 0-00000': 'select PASS_WORD, STATICADDRESS, TIMELEFT, MAXLOGINS, SERVICENAME, BADLOGINS, VALIDFROM, VALIDTO from RADUSERS where USERNAME='jdoe'':
Debug	2018-05-08 13:50	Query to 'dbi:mysql:radmin:localhost Connection id: 0-00000': 'select ATTR_ID, VENDOR_ID, IVALUE, SVALUE, ITEM_TYPE from RADSTCONFIG where NAME='Standard broadband' order by ITEM_TYPE':
Debug	2018-05-08 13:50	Query to 'dbi:mysql:radmin:localhost Connection id: 0-00000': 'select ATTR_ID, VENDOR_ID, IVALUE, SVALUE, ITEM_TYPE from RADCONFIG where NAME='jdoe' order by ITEM_TYPE':
Debug	2018-05-08 13:50	Radius::AuthRADMIN looks for match with jdoe [jdoe]
Debug	2018-05-08 13:50	ValidFrom date converted to: 1525775147
Debug	2018-05-08 13:50	Expiration date converted to: 1557262800
Debug	2018-05-08 13:50	Radius::AuthRADMIN ACCEPT: : jdoe [jdoe]

8.1. Search Criteria

The top part of this page lets you enter search criteria to find particular log messages The bottom part displays the list of messages that satisfy your criteria. You can limit the list of log messages displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), *all* the log messages in your accounting database will be listed.

8.1.1. Type

The section allows you to restrict what message types are listed. The message types for a message is one of the following numbers:

Table 6. Log Message types

Type	Description
0	ERR. Error conditions. Serious and unexpected failures
1	WARNING. Warning conditions. Unexpected failures
2	NOTICE. Normal but significant conditions.
3	INFO. Informational messages.
4	DEBUG. Debugging messages.

See Using numbers in searches on page 5

8.1.2. Time stamp

The limits the range of date/times that are to be listed. For each message, the Time stamp is the local time that the message was logged.

See Using dates in searches on page 4

8.1.3. Message

This limits the text of the messages to be displayed.

See Using text in searches on page 5

8.2. The List

This section shows the messages that match the search criteria you entered in the top section.

Type is the message type number. See Log Message types on page 16.

Time stamp is the time the message was logged, in your time zone's local time.

Message is the text of the log message. It describes the error or event that was logged.

8.3. Tasks using this page

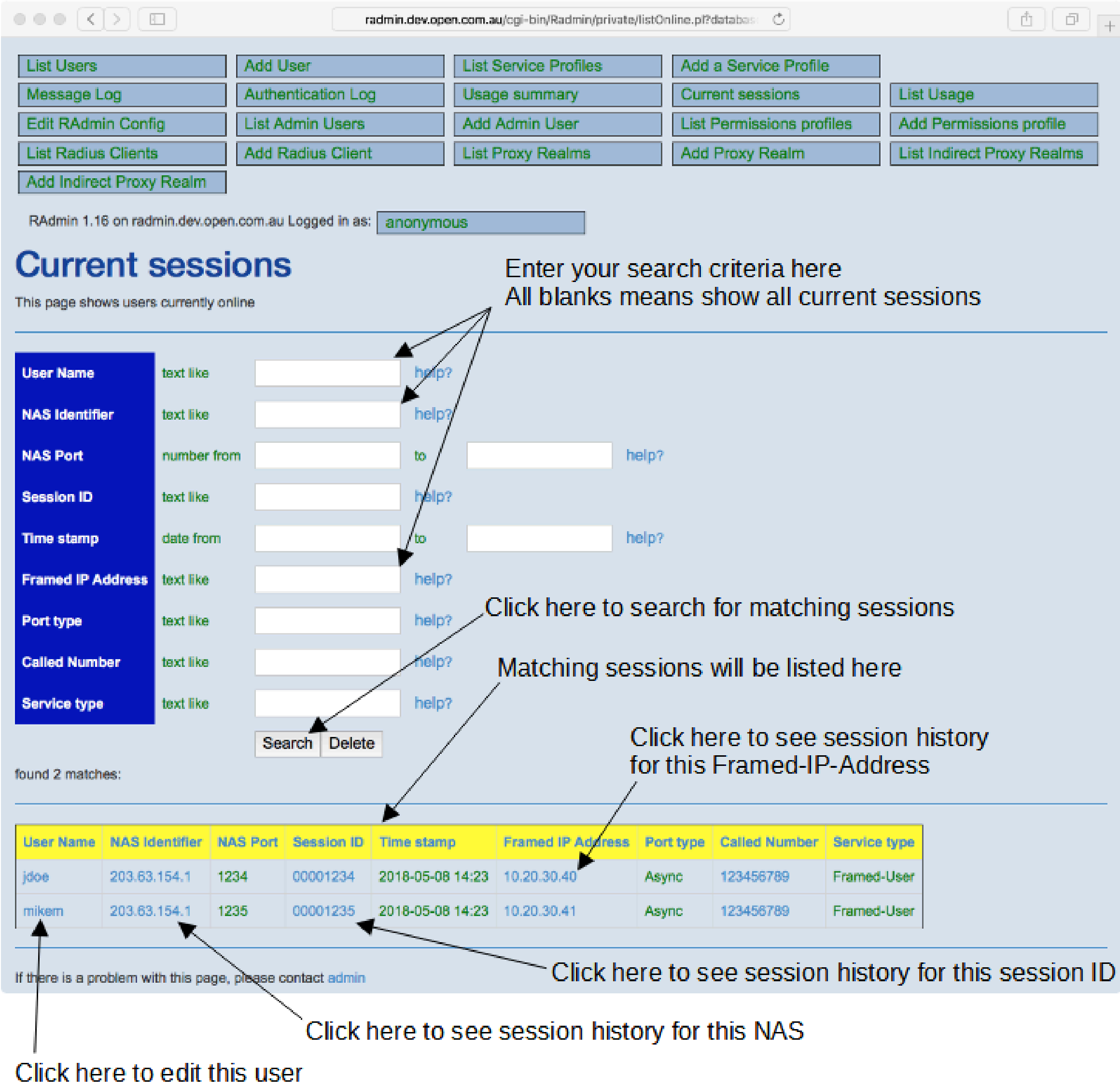
The following common tasks relate to this page:

- Checking the message log on page 50.

9. Current sessions

This page lists some or all of the sessions that are currently online (i.e. user sessions that have started, but not yet finished). You can drill down to see details of the user, or the history of sessions with the same NAS Identifier or the same Session ID.

Figure 6. Current sessions page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Current sessions

This page shows users currently online

User Name	text like		help?		
NAS Identifier	text like		help?		
NAS Port	number from		to		help?
Session ID	text like		help?		
Time stamp	date from		to		help?
Framed IP Address	text like		help?		
Port type	text like		help?		
Called Number	text like		help?		
Service type	text like		help?		

found 2 matches:

User Name	NAS Identifier	NAS Port	Session ID	Time stamp	Framed IP Address	Port type	Called Number	Service type
jdoe	203.63.154.1	1234	00001234	2018-05-08 14:23	10.20.30.40	Async	123456789	Framed-User
mikem	203.63.154.1	1235	00001235	2018-05-08 14:23	10.20.30.41	Async	123456789	Framed-User

If there is a problem with this page, please contact admin

Enter your search criteria here
All blanks means show all current sessions

Click here to search for matching sessions

Matching sessions will be listed here

Click here to see session history
for this Framed-IP-Address

Click here to see session history for this session ID

Click here to see session history for this NAS

Click here to edit this user

9.1. Search Criteria

The top part of this page lets you enter search criteria to find particular sessions or groups of sessions. The bottom part displays the list of current sessions that satisfy your criteria. You can limit the list of sessions displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), *all* the current sessions will be listed.

9.1.1. User Name

The restricts the sessions to those belonging to users who match this field.

See Using text in searches on page 5

9.1.2. NAS Identifier

This restricts the list to sessions that were connected to a certain NAS (i.e. Terminal Servers etc.). The NAS Identifier is an IP address like 203.63.154.1, not a DNS name.

See Using text in searches on page 5

9.1.3. NAS Port

This restricts the list to sessions that had the specified NAS-Port, which identifies which interface, modem or port the session was connected to. See Using numbers in searches on page 5

9.1.4. Session ID

This restricts the list to sessions that match the Session ID. See Using text in searches on page 5

9.1.5. Time stamp

This restricts the list to sessions that started during the date/time range given. If Interim-Update (also known as Alive) messages are enabled, this may also be Alive message time stamp. See Using dates in searches on page 4

9.1.6. Framed IP Address

This restricts the list to sessions that match the specified Framed IP Address (which is the IP address the user had for the duration of their session). See Using text in searches on page 5

9.1.7. Port type

This restricts the list to sessions with port types that match. The port type describes what type of connection this session is using. Usually one of:

- Sync
- Async
- ISDN
- Virtual

See Using text in searches on page 5

9.1.8. Service type

This restricts the list to sessions with port types that match. The service type describes what type of session this is. Usually one of:

- Login user
- Framed user
- Administrative-User (a router administrator telnetted into the router)

9.2. The List

This section shows each current session that matches the search criteria you entered in the top section.

You can click on the hotlinks in the following columns:

- User Name. This will take you to the Edit a User page for that user. See Add a User, Edit a User on page 7.
- NAS Identifier. This will take you to another List Usage page, showing sessions with the same NAS Identifier. The NAS Identifier is the IP address of the NAS where the session was connected to.

- Session ID. This will take you to another List Usage page, showing sessions with the same Session ID.

9.3. Tasks using this page

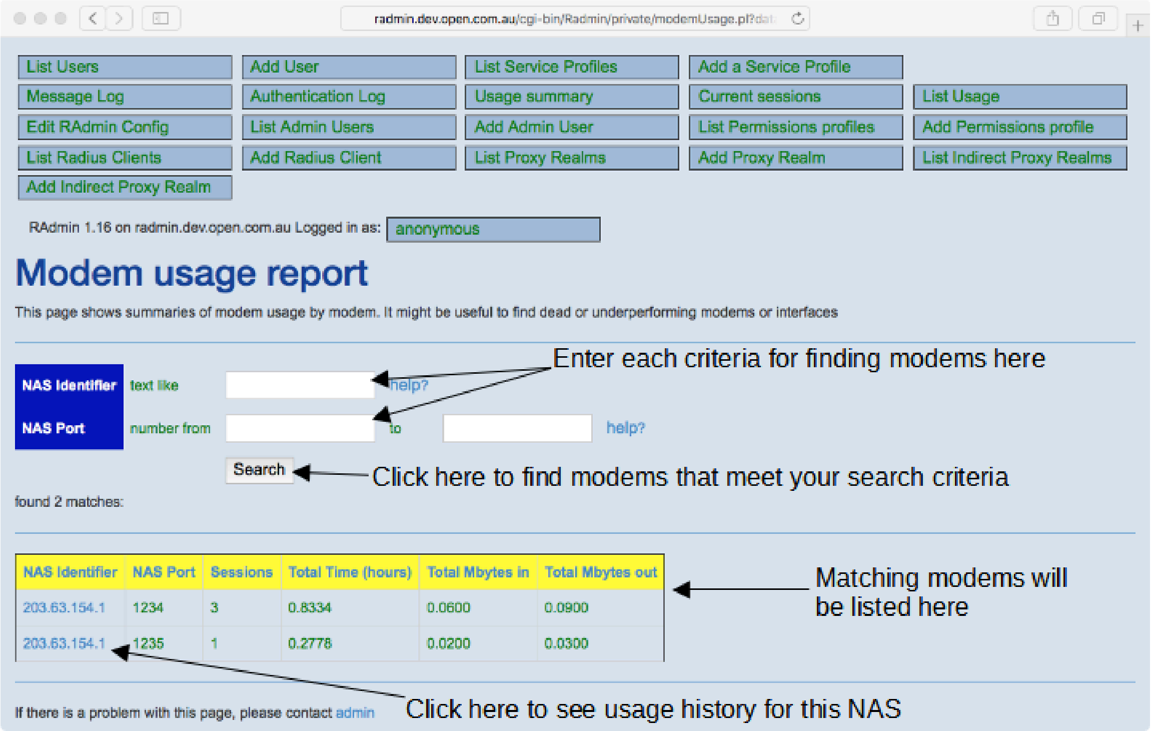
The following common tasks relate to this page:

- Checking who is currently on-line on page 50.

10. Modem usage report

This page summarizes the usage of each modem or interface on your NASs, It is useful for finding dead or underutilized modems.

Figure 7. Modem usage report



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Modem usage report

This page shows summaries of modem usage by modem. It might be useful to find dead or underperforming modems or interfaces

Enter each criteria for finding modems here

Click here to find modems that meet your search criteria

found 2 matches:

NAS Identifier	NAS Port	Sessions	Total Time (hours)	Total Mbytes in	Total Mbytes out
203.63.154.1	1234	3	0.8334	0.0600	0.0900
203.63.154.1	1235	1	0.2778	0.0200	0.0300

Matching modems will be listed here

If there is a problem with this page, please contact admin

Click here to see usage history for this NAS

10.1. Search Criteria

The top part of this page lets you enter search criteria to find particular modems or groups of modems. The bottom part displays the list of modems that satisfy your criteria. You can limit the list of modems displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), usage summaries for *all* your modems will be listed.

10.1.1. NAS Identifier

The section limits the usage summary to NASs that match this pattern. See Using text in searches on page 5

10.1.2. NAS Port

This section limits the usage summary to modems that match the pattern. See Using text in searches on page 5

10.2. Modem usage list

This section presents a usage summary for each NAS and Port selected by the search criteria you entered in the top section. It summarizes session Stops that are currently in your accounting database.

Sessions is the total number of sessions that have completed in the time interval covered by your accounting database.

You can click on the hotlinks in the following columns:

- NAS Identifier. This takes you to the List Usage page showing sessions with the same NAS Identifier. See List Usage on page 11.

10.3. Tasks using this page

The following common tasks relate to this page:

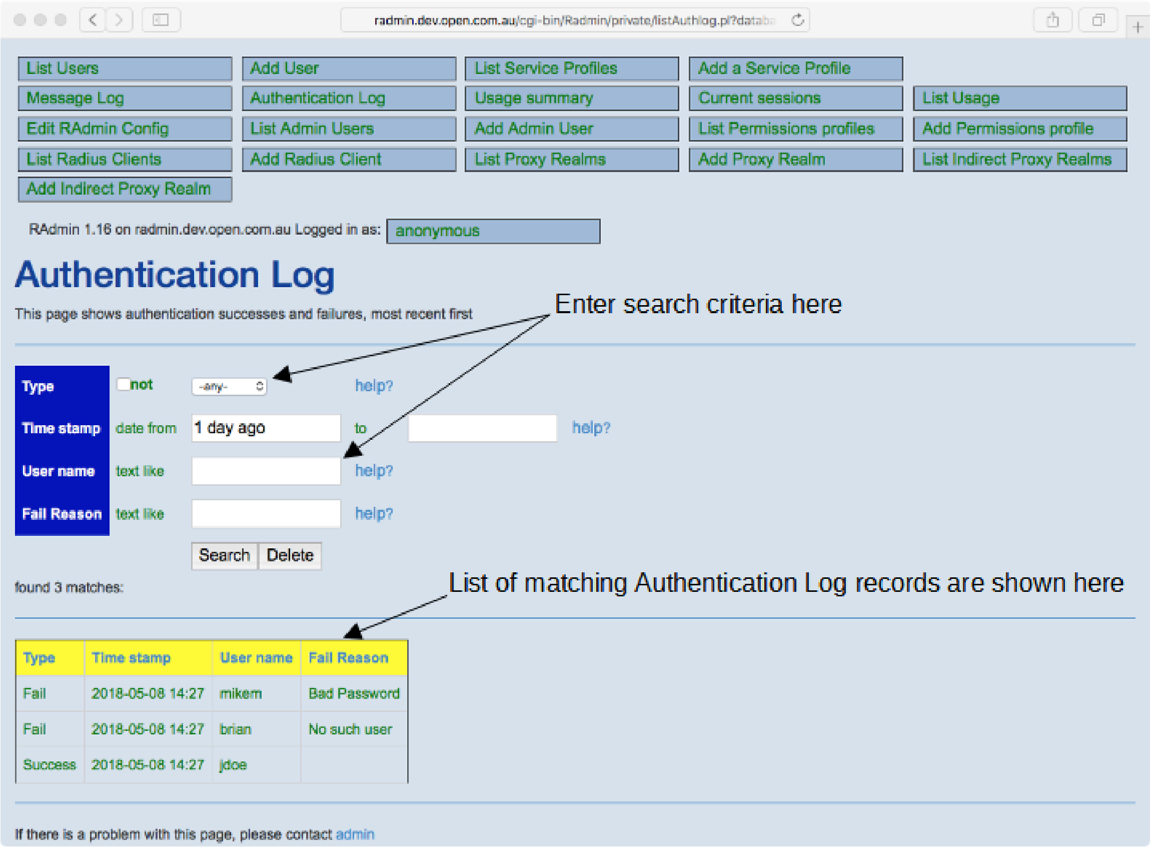
- Checking modem usage on page 50.

11. Authentication Log

Your Radiator administrator may have configured Radiator to add entries to the Authentication Log when a user attempts to authenticate through Radiator. This means that whenever a user tries to log in, you can see whether they succeed or fail, and if they fail, why they failed.

The Authentication Log page can be very useful when trying to help people with login problems. If a customer reports that they cannot log in, search for all records with their user name for the last day, and you will see all the authentication attempts and the reasons for failures.

Figure 8. Authentication Log



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Authentication Log

This page shows authentication successes and failures, most recent first

Enter search criteria here

Type	□ not	-any-	help?		
Time stamp	date from	1 day ago	to		help?
User name	text like		help?		
Fail Reason	text like		help?		

found 3 matches:

List of matching Authentication Log records are shown here

Type	Time stamp	User name	Fail Reason
Fail	2018-05-08 14:27	mikem	Bad Password
Fail	2018-05-08 14:27	brian	No such user
Success	2018-05-08 14:27	jdoe	

If there is a problem with this page, please contact admin

11.1. Search Criteria

The top part of this page lets you enter search criteria to find particular Authentication Log records. The bottom part displays the list of records that satisfy your criteria. You can limit the list of records displayed in the lower section by entering one or more restrictions on the search and clicking **Search**. If you do not enter any search criteria (i.e. if you leave all the search criteria fields in the top part blank), all Authentication Log records will be listed.

11.1.1. Type

This section limits whether you want to see authentication successes, failures or both.

11.1.2. Time stamp

This section limits the range of times to display. The default is for the last day.

11.2. Authentication Log list

This section presents a list of all the Authentication Log records that match the search criteria you entered in the top section. Type indicate whether it was a successful login attempt or not. Time stamp indicates the date and time that the attempt occurred. User name is the login name that was used, and Fail reason is the reason the login was rejected if it was a Failure. Success records do not have a Reason.

11.3. Tasks using this page

The following common tasks relate to this page:

- Checking modem usage on page 50.

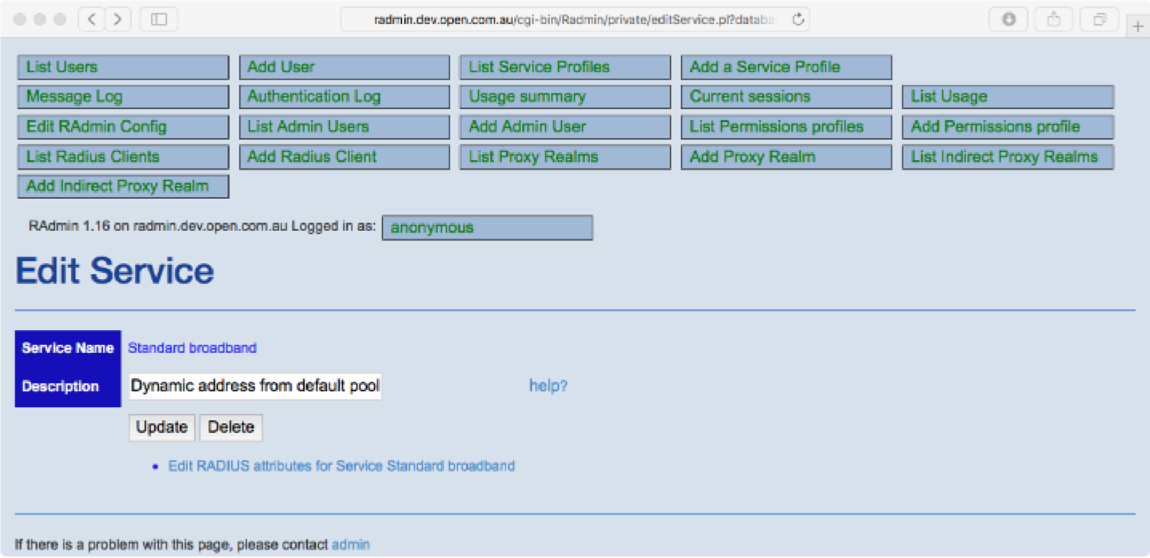
12. Add Service Profile, Edit Service Profile

This page allows you to add or change details of a Service Profile. A Service Profile is a group of users that all share the same RADIUS check and reply items. You can use Service Profiles to ensure all the users have the same authentication requirements, and you can easily configure or change a user's authentication requirements by changing their Service Profile on the Edit User page.

It is common to set up a small number of Service Profiles, one for each major grouping of users, for example, one Service Profile for normal users, and one for NOC staff, where the NOC staff are required to login via a certain Called-Station-ID, and who get a special NAS filter.

The Edit Service Profile page allows you to edit the name and description of the profile. The RADIUS attributes for the profile are edited with the Edit RADIUS Attributes page. See Edit RADIUS Attributes on page 23

Figure 9. Edit Service Profile Page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Edit Service

Service Name: Standard broadband

Description: Dynamic address from default pool

- Edit RADIUS attributes for Service Standard broadband

If there is a problem with this page, please contact admin

12.1. Editable Fields

The following chapters describe the editable fields of Edit Service.

12.1.1. Service Name

This is the short name of the Service Profile. It will be listed in the menu of Service Profiles you select in the Edit User page.

12.1.2. Description

This is a brief description of the purpose of the Service Profile. It is for Radmin user information only and is not used anywhere else.

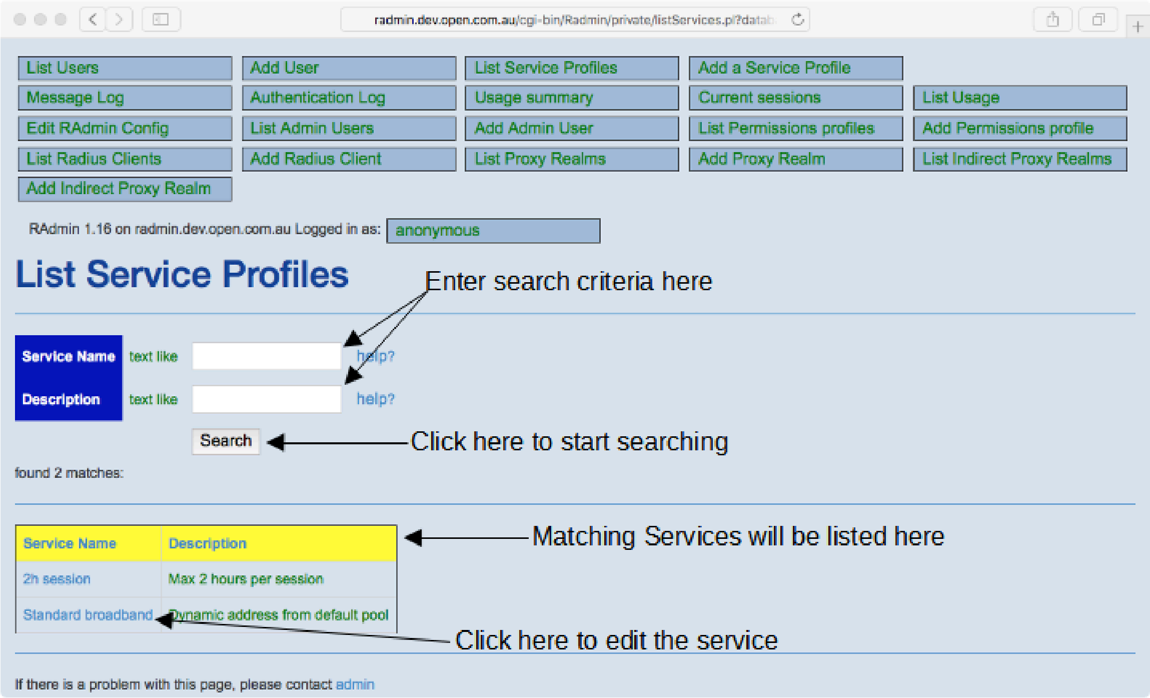
12.1.3. Edit RADIUS Attributes

This link takes you to the Edit RADIUS Attributes page for this Service Profile. It will allow you to add, change and remove RADIUS Check and Reply items for this Service Profile.

13. List Service Profiles

This page allows you to search for and list the Service Profiles in your user database. The list shows the main information about each Service Profile, and you can drill down to detailed information about each Service Profile.

Figure 10. List Service Profiles



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Service Profiles

Enter search criteria here

Service Name text like

Description text like

Click here to start searching

found 2 matches:

Service Name	Description
2h session	Max 2 hours per session
Standard broadband	Dynamic address from default pool

Matching Services will be listed here

Click here to edit the service

If there is a problem with this page, please contact admin

14. Edit RADIUS Attributes

This page allows you to add, change or delete RADUS attributes for a User or Service Profile. See Service Profiles and RADIUS Check and Reply items on page 6 for more information about RADIUS attributes. You can reach this page by clicking on the Edit RADIUS Attributes link on an Edit User page, or the Edit RADIUS Attributes link on an Edit Service Profile page. The page will display the current RADIUS attributes for that user or Service Profile.

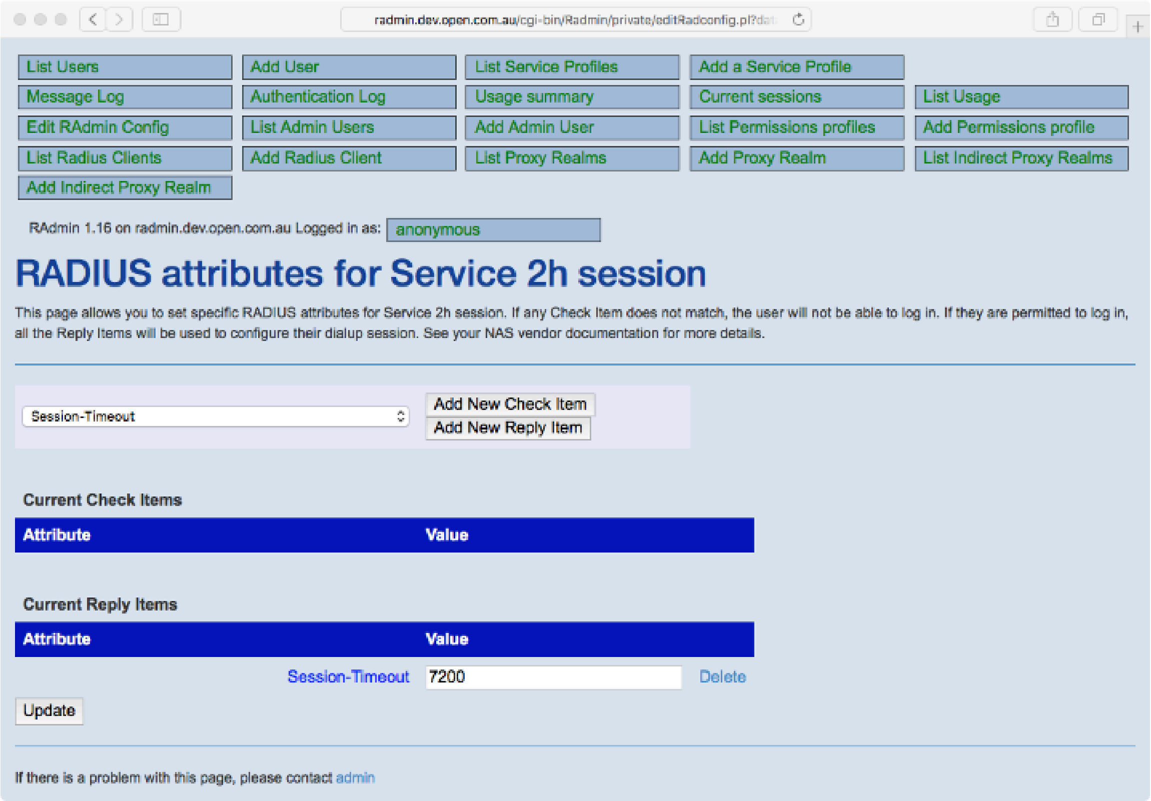
You can change the value of a RADIUS attribute by altering the field in the ‘Value’ column and then pressing the **Update** button.

You can add a new Check Item by selection the type of attribute required for the new Check Item, then pressing the **Add New Check Item** button. The Edit RADIUS Attributes page will appear with the new Check item added to the end of the list. You can then set the Value of the new attribute and press **Update**.

You can add a new Reply Item by selection the type of attribute required for the new Reply Item, then pressing the **Add New Reply Item** button. The Edit RADIUS Attributes page will appear with the new Reply item added to the end of the list. You can then set the Value of the new attribute and press **Update**.

The example page below shows the RADIUS attributes for a Service Profile. There is one Check Item, requiring that the Called-Station-Id for all logins must be *98767676*. Users that log in successfully will have their Filter-Id set to ‘*standard*’. See your NAS vendor for details about what RADIUS attributes are available for your NAS and how they can be used.

Figure 11. Edit RADIUS Attributes



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

RADIUS attributes for Service 2h session

This page allows you to set specific RADIUS attributes for Service 2h session. If any Check Item does not match, the user will not be able to log in. If they are permitted to log in, all the Reply Items will be used to configure their dialup session. See your NAS vendor documentation for more details.

Current Check Items

Attribute	Value

Current Reply Items

Attribute	Value	
Session-Timeout	7200	Delete

If there is a problem with this page, please contact admin

15. Add Radius Client, Edit Radius Client

This page allows you to Add, Change and Delete Radius clients from your database. A Radius client specifies details about a NAS that your Radiator Radius Server will listen to and honour requests.

Most of the editable fields on this page are required for advanced use only. You will probably only need to set the name/address and the Shared secret.

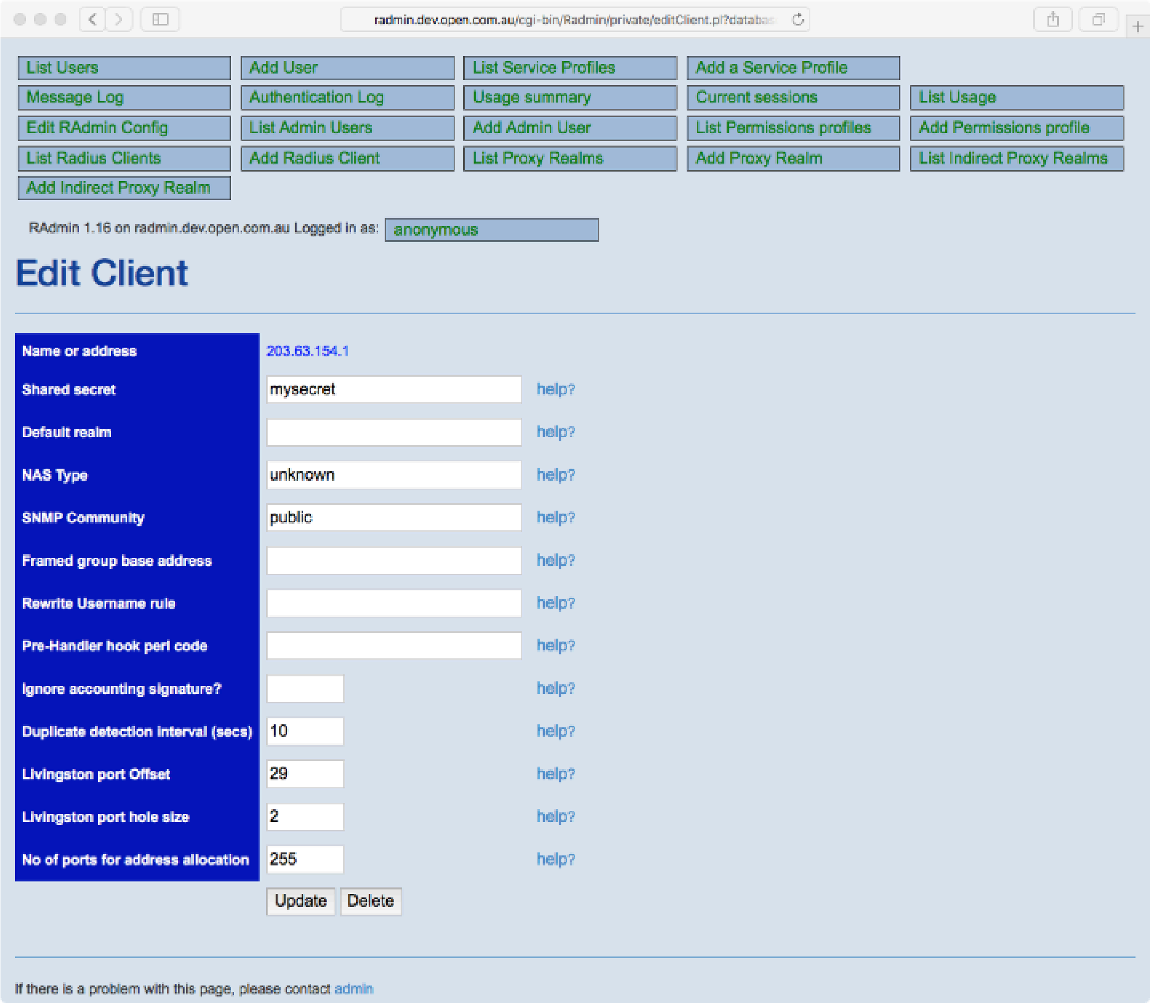
Tip

Radiator only takes notice of the Radius clients configured into this page if the <ClientListSQL> clause is present in your Radiator configuration. See the Radiator reference manual [https://files.radiatorsoftware.com/radiator/ref/index.html] for more details.

Tip

After adding or changing Radius client details with this page, you will need to restart or signal your Radiator before it will use the new details.

Figure 12. Edit RADIUS Client page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Edit Client

Name or address	203.63.154.1	
Shared secret	mysecret	help?
Default realm		help?
NAS Type	unknown	help?
SNMP Community	public	help?
Framed group base address		help?
Rewrite Username rule		help?
Pre-Handler hook perl code		help?
Ignore accounting signature?		help?
Duplicate detection interval (secs)	10	help?
Livingston port Offset	29	help?
Livingston port hole size	2	help?
No of ports for address allocation	255	help?

If there is a problem with this page, please contact admin

15.1. Editable Fields

The following chapters describe the editable fields of Edit Service.

15.1.1. Name or Address

This is the IP address or DNS name of the NAS that will be sending requests to your Radiator. It is required.

15.1.2. Shared Secret

This is the shared secret that will be used to encrypt passwords sent by the NAS. The shared secret is a secret word or sentence that is used to protect all information passed between the NAS and Radiator. It must be configured here and also configured into the NAS. It must be configured exactly the same the NAS. It is case-sensitive. We recommend that you use a shared secret containing mixed case letters and number of about 16 characters.

15.1.3. Default Realm

For advanced operations only.

This optional field specifies a Realm that will be added automatically to the user name of login requests from this NAS if the user name does not already contain a Realm. See the Radiator reference manual for more details.

For example, if you enter *open.com.au* as the Default Realm, and a user attempts to log in to the NAS as *mikem*, then the user name will be automatically converted to *mikem@open.com.au* before being authenticated.

15.1.4. NAS Type

For advanced operations only.

This optional field specifies the manufacturer and type of this NAS. It is only required for strong multiple-login prevention. See the Radiator reference manual for more details.

15.1.5. SNMP Community

For advanced operations only.

This optional field specifies SNMP community for SNMP access to this NAS. It is only required for strong multiple-login prevention. See the Radiator reference manual for more details.

15.1.6. Framed Group Base Address

For advanced operations only.

This optional field specifies the base IP address for automatically setting IP addresses for logins from this NAS. See the Radiator reference manual for more details.

15.1.7. Rewrite Username rule

For advanced operations only.

This optional field allows you to automatically rewrite user names before authentication. See the Radiator reference manual for more details.

15.1.8. Pre-Handler hook perl code

For advanced operations only.

This optional field allows you to enter a Perl code hook that will be invoked before authentication or accounting request from this NAS are handled. See the Radiator reference manual for more details.

15.1.9. Ignore accounting signature

For advanced operations only.

This optional field allows you to work around certain NASs with broken software, where the signature in accounting requests is set incorrectly. See the Radiator reference manual for more details.

15.1.10. Duplicate detection interval

For advanced operations only.

This optional field allows you to change the time period that Radiator uses to detect duplication of Radius request packets. See the Radiator reference manual for more details.

15.1.11. Livingston port offset

For advanced operations only.

This optional field allows you to tailor information about ports on Livingston NASs. It is not required and is ignored for most types of NAS. See the Radiator reference manual for more details.

15.1.12. Livingston port hole size

For advanced operations only.

This optional field allows you to tailor information about ports on Livingston NASs. It is not required and is ignored for most types of NAS. See the Radiator reference manual for more details.

15.1.13. No of ports for address allocation

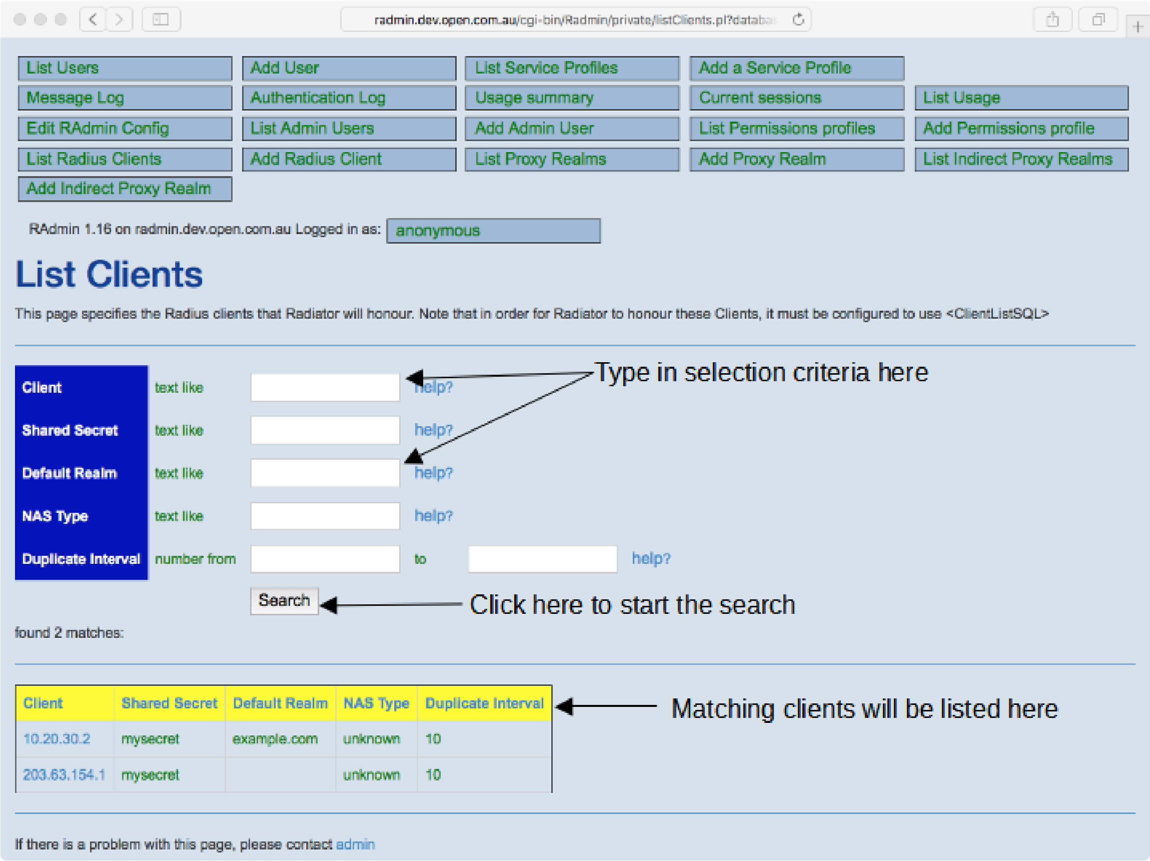
For advanced operations only.

This optional field specifies how many ports can be allocated an IP address in a class C block. It is only required if Framed Group Base Address is used to compute IP address automatically for this NAS. See the Radiator reference manual for more details.

16. List Radius Clients

This page allows you to search for and list Radius Clients that meet certain criteria.

Figure 13. List Radius Clients page



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Clients

This page specifies the Radius clients that Radiator will honour. Note that in order for Radiator to honour these Clients, it must be configured to use <ClientListSQL>

Client	text like		help?		
Shared Secret	text like		help?		
Default Realm	text like		help?		
NAS Type	text like		help?		
Duplicate Interval	number from		to		help?

Search

Type in selection criteria here

Click here to start the search

found 2 matches:

Client	Shared Secret	Default Realm	NAS Type	Duplicate Interval
10.20.30.2	mysecret	example.com	unknown	10
203.63.154.1	mysecret		unknown	10

Matching clients will be listed here

If there is a problem with this page, please contact admin

17. Subscription Management

If your RAdmin system administrator has enabled Subscription Management in your RAdmin system, you will (depending on specific permissions) have access to a number of Subscription Management pages.

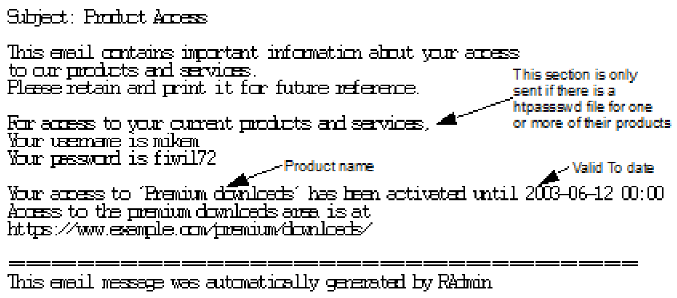
RAdmin Subscription Management automatically adds and removes users from password files in the same format that Apache and other applications require. This means that you can use RAdmin to administer access to various parts of a web site (for example), according to what product(s) your customer has bought. This is in addition to the normal user access management that RAdmin always performs.

The Subscription Management pages allow you to define subscription type products, to subscribe users to each product for varying periods of time, and to search for and list subscriptions. At the end of a users subscription period, their access to the product can be automatically disabled by the expire program, which your RAdmin administrator may also have set up.

17.1. Email to users

If a user has one or more email addresses, RAdmin Subscription Management will automatically send email to those addresses at various times:

- When a product State is changed to Trial or Approved from any other State. No mail is sent when changing from Trial to Approved or vice versa. Mail will contain the product’s ‘Message for new subs’ text if defined on the Edit Product page. The text of the email will be something like this:



```
Subject: Product Access

This email contains important information about your access
to our products and services.
Please retain and print it for future reference.

For access to your current products and services,
Your username is mikem
Your password is fiwil72

Your access to 'Premium downloads' has been activated until 2003-06-12 00:00
Access to the premium downloads area is at
https://www.example.com/premium/downloads/

=====================================
This email message was automatically generated by RAdmin
```

This section is only sent if there is a htpasswd file for one or more of their products
Product name
Valid To date

Note

Many part of the email text are configurable by the RAdmin administrator, so the exact content may be different in your installation.

- When a product State is changed from Trial or Approved from any other State. Mail will contain the product's ‘Message for stopped subs’ text if defined on the Edit Product page
- When a product in Trial or Approved State has its Valid To date extended prior to the expiry date. Mail will contain the product's ‘Message for extended subs’ text if defined on the Edit Product page.
- When a product in Trial or Approved State is automatically expired by the expire program.

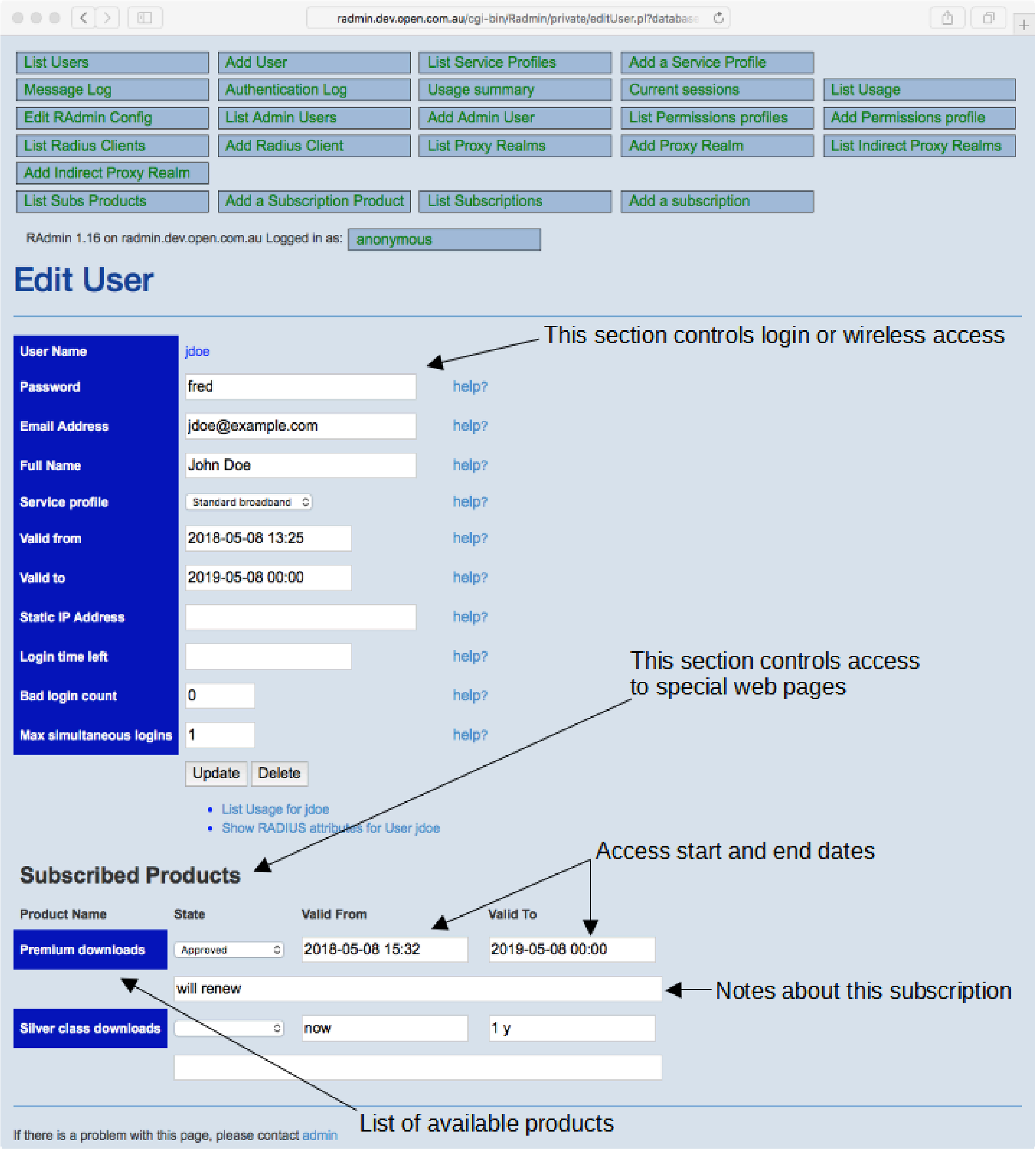
If multiple products are enabled or disabled at the same time, only a one email will be sent to the user containing details of each product enabled or disabled.

The following sections describe the Subscription Management pages.

18. User subscriptions

If your RAdmin administrator has enable Subscription Management, the Add and Edit User pages will look slightly different than described in Add and Edit User pages on page 7. IN addition, you will see a list of available products (defined with the ‘Add a Subscription Product’ page), and details of the user's subscription for each product.

Figure 14. Edit User with Subscription Management



radmin.dev.open.com.au/cgi-bin/Radmin/private/editUser.pl?databas

List Users	Add User	List Service Profiles	Add a Service Profile	
Message Log	Authentication Log	Usage summary	Current sessions	List Usage
Edit RAdmin Config	List Admin Users	Add Admin User	List Permissions profiles	Add Permissions profile
List Radius Clients	Add Radius Client	List Proxy Realms	Add Proxy Realm	List Indirect Proxy Realms
Add Indirect Proxy Realm				
List Subs Products	Add a Subscription Product	List Subscriptions	Add a subscription	

RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Edit User

This section controls login or wireless access

User Name	jdoe	
Password	fred	help?
Email Address	jdoe@example.com	help?
Full Name	John Doe	help?
Service profile	Standard broadband	help?
Valid from	2018-05-08 13:25	help?
Valid to	2019-05-08 00:00	help?
Static IP Address		help?
Login time left		help?
Bad login count	0	help?
Max simultaneous logins	1	help?

Update Delete

- List Usage for jdoe
- Show RADIUS attributes for User jdoe

This section controls access to special web pages

Subscribed Products

Access start and end dates

Product Name	State	Valid From	Valid To
Premium downloads	Approved	2018-05-08 15:32	2019-05-08 00:00
	will renew		
Silver class downloads		now	1 y

Notes about this subscription

List of available products

If there is a problem with this page, please contact admin

18.1. Editable Fields

The following chapters describe the editable fields of Edit Service.

18.1.1. State

This field describes the current subscription state for this product. In the standard Radmin system, the available states are:

- -blank-

  User has no subscription and has never expressed an interest in it.

- Enquiry

  User has made some enquiries about the product.

- Wait for approval

  User has ordered but not paid for the product. Record the order details in the Notes

- Trial

  Temporary and short-term access to the product has been granted. Will be automatically Expired at the end of the Valid To period.

- Approved

  Access to the product has been granted. Will be automatically Expired at the end of the Valid To period.

- Expired

  The Valid To date has passed, and the product has been automatically expired

- Disabled

  Access has been temporarily disabled. Record the reason why in the Notes.

- Transferred

  The access privileges have been transferred to another user. Record the user in the Notes

- Closed

  Access has been permanently closed. Record the reason why in the Notes.

When you add enable a subscription (i.e. in Trial or Approved states), the user will be able to access the protected web pages between the ‘Valid From’ and ‘Valid To’ dates. At the end of their subscription period the expire program will change their State to Expired, automatically remove them from the access password file, and they wont be able to access the protected web pages any more.

The other states (Enquiry, Wait for approval etc.) are place-holders that allow you to record where you are in the sales cycle for this product to this customer. Access to the protected area is only possible in Trial and Approved states.

Tip

if multiple subscription products are configured with the same non-empty Product Group name, then only one of those products can be enabled at any time. If you attempt to enable more than one such product, you will receive an error message and the user will not be updated.

18.1.2. Valid From

This is the first date which access will be granted. Any of the date formats described in Entering dates and times on page 2 are permitted. The default value is set by the ‘Default valid from time’ field in the ‘Edit Product’ page.

18.1.3. Valid To

This is the last which access will be granted. Any of the date formats described in Entering dates and times on page 2 are permitted. The default value is set by the ‘Default valid to time’ field in the ‘Edit Product’ page.

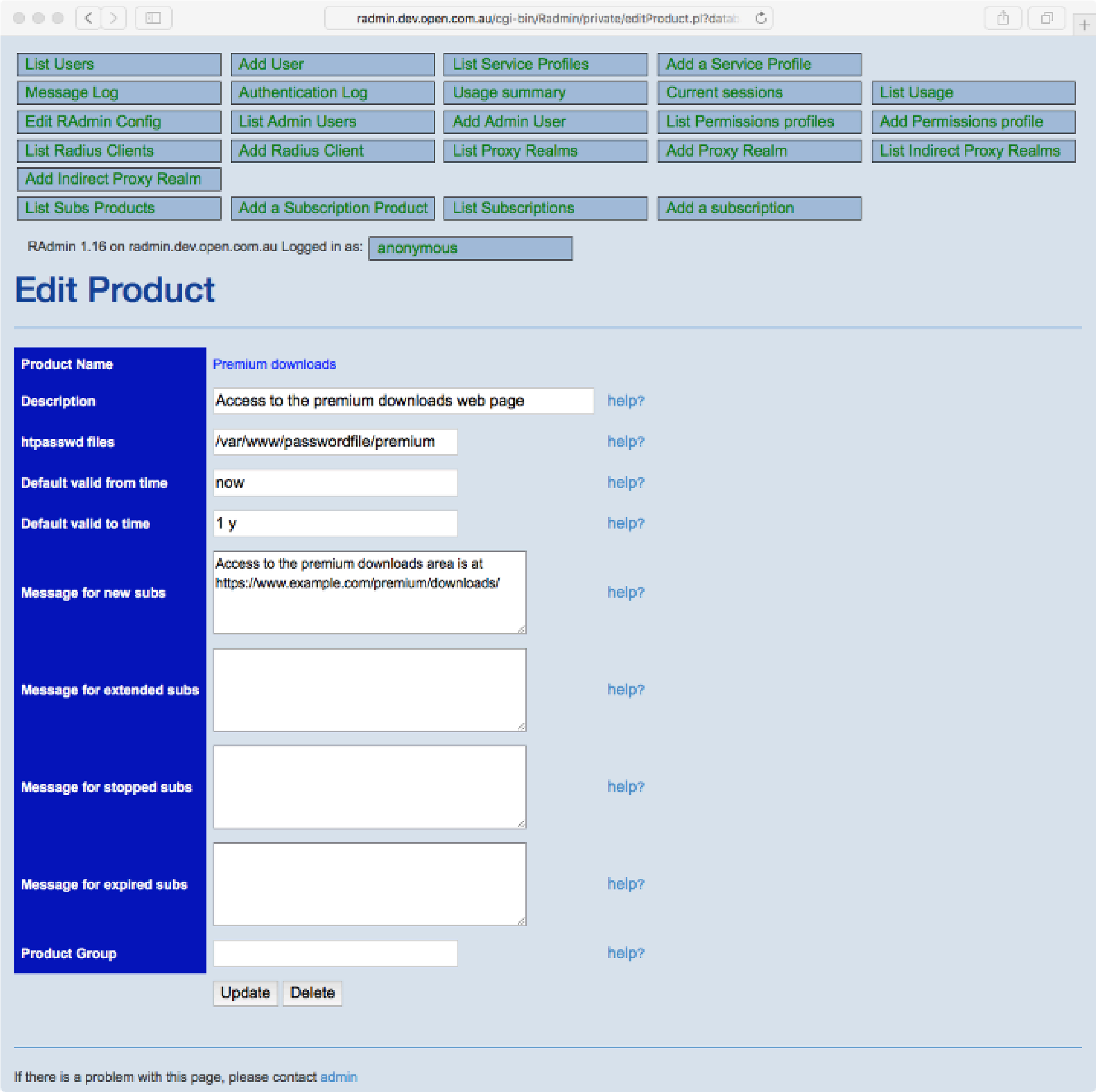
18.1.4. Notes

This section contains notes about the users subscription to this product.

19. Add a Product, Edit a Product

This page allows you to define and alter subscription products. For each product, you can define the location of the access password file, the default values for the from and to dates, and optional messages to be sent by email to a user when their access to the product changes.

Figure 15. Edit a Product



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Edit Product

Product Name	Premium downloads	
Description	Access to the premium downloads web page	help?
htpasswd files	/var/www/passwordfile/premium	help?
Default valid from time	now	help?
Default valid to time	1 y	help?
Message for new subs	Access to the premium downloads area is at https://www.example.com/premium/downloads/	help?
Message for extended subs		help?
Message for stopped subs		help?
Message for expired subs		help?
Product Group		help?

If there is a problem with this page, please contact admin

19.1. Editable Fields

The following chapters describe the editable fields of Edit Service.

19.1.1. Product Name

This is a short product name. It will appear on the Edit User page, and also in emails sent to the user.

19.1.2. Description

This is a brief description of the product for reference only. It is not displayed anywhere but here.

19.1.3. htpasswd files

This is a list of password files that will be automatically managed when users are subscribed or unsubscribed to this product. The file is in htpasswd format as required by Apache and other systems, one line per valid user. Multiple file names can be specified separated by colons. If multiple file names are specified, subscribed users will be added to all the files named.

19.1.4. Default valid from time

This is the default Valid From for new subscriptions. Any text is permitted, but a relative date in one of the date formats described in Entering dates and times on page 2 are recommended, such as ‘now’, ‘tomorrow’, ‘1 year’ etc. The date will appear on the Edit User page, but can be changed to another value there.

19.1.5. Default valid to time

This is the default Valid To for new subscriptions. Any text is permitted, but a relative date in one of the date formats described in Entering dates and times on page 2 are recommended, such as ‘now’, ‘tomorrow’, ‘1 year’ etc. The date will appear on the Edit User page, but can be changed to another value there.

19.1.6. Message for new subs

This message will be added to the email sent when a user is subscribed to a product (i.e is changed to Trial or Approved State). You might use it to describe how to access the product.

19.1.7. Message for extended subs

This message will be added to the email sent when a user’s existing subscription is extended before it expires. You might use it to thank them or provide information about product changes.

19.1.8. Message for stopped subs

This message will be added to the email sent when a user is unsubscribed from a product (i.e is changed from Trial or Approved State to any other State). You might use it to describe how to resubscribe the product.

19.1.9. Message for expired subs

This message will be added to the email sent when a user is automatically expired from a product (i.e is changed from Trial or Approved State to Expired State by the expire program). You might use it to describe how to resubscribe the product.

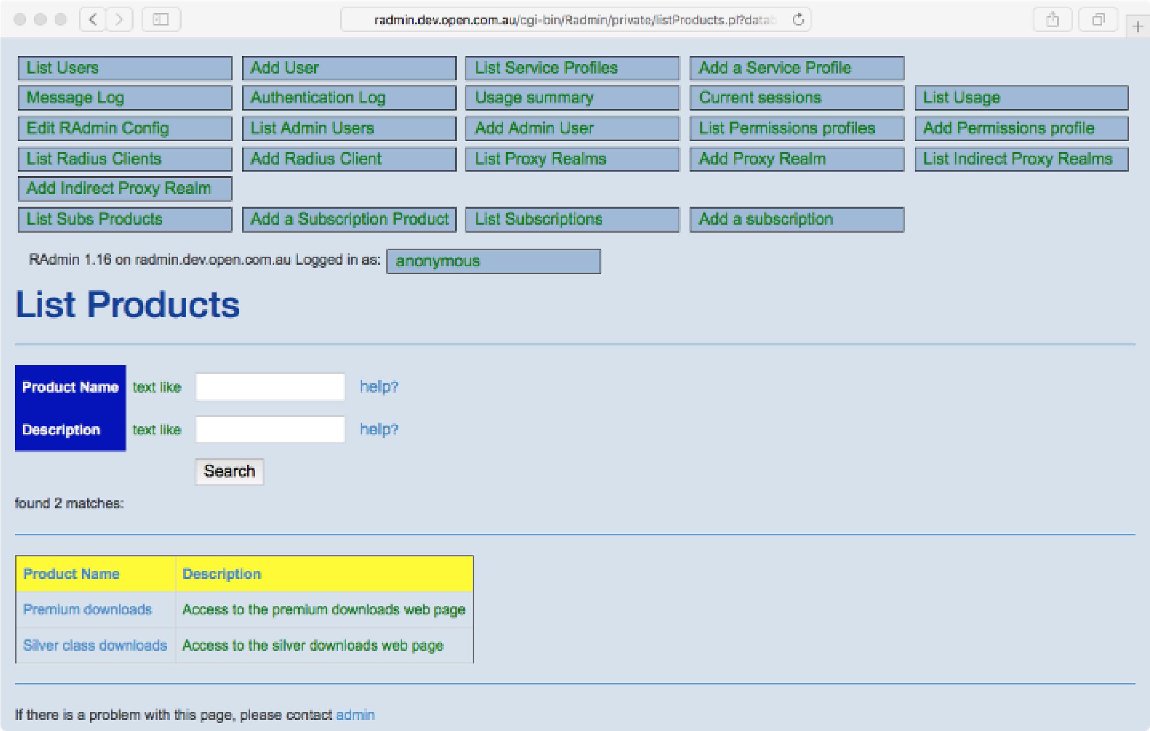
19.1.10. Product Group

This optional field allows you to group subscription products so that at most one of the group can be enabled at a time. If multiple products exists with the same non-empty Product Group name, then only at most on such product can be enabled on the Edit User page.

20. List Products

This page allows you to search for and list the currently defined subscription products.

Figure 16. List Products



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Products

Product Name text like help?

Description text like help?

found 2 matches:

Product Name	Description
Premium downloads	Access to the premium downloads web page
Silver class downloads	Access to the silver downloads web page

If there is a problem with this page, please contact admin

21. Vasco Digipass support

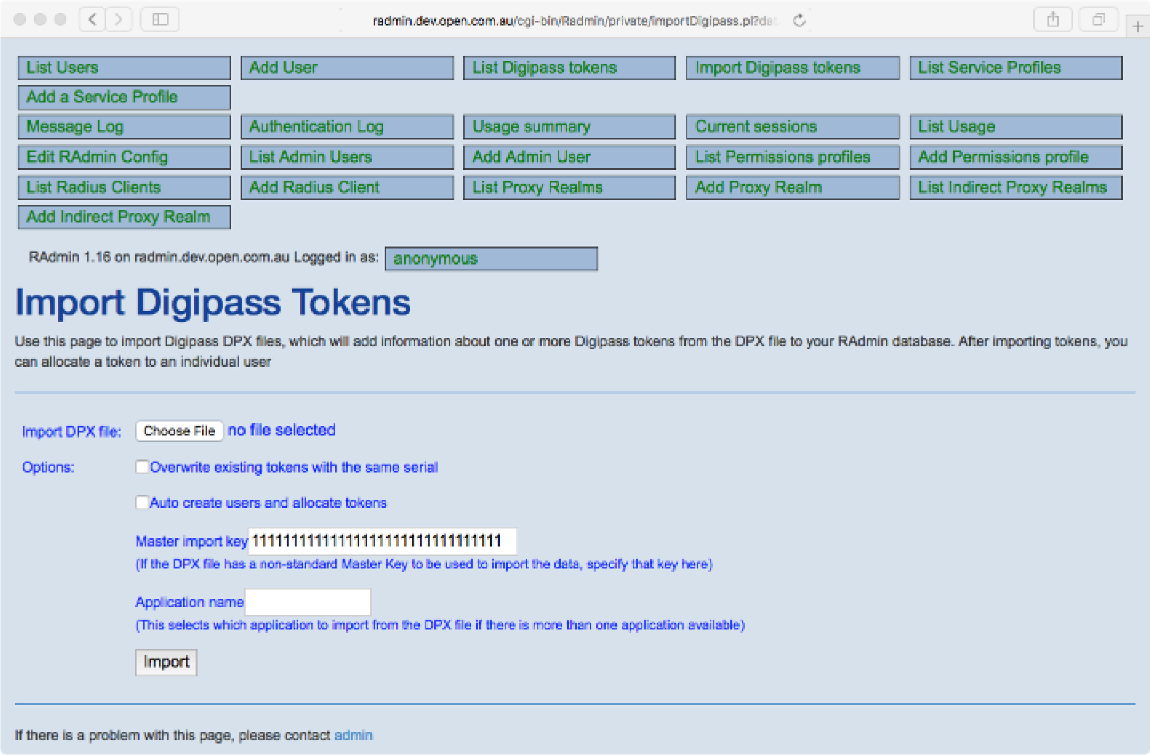
RAdmin can optionally support Vasco Digipass tokens (http://www.vasco.com). Digipass tokens are small handheld devices that generate one-time-passwords that change every minute. They can be purchased from Vasco and issued to your users. Such tokens provide much higher levels of security than static passwords. Additionally, with some types of token, users can set up individual PINs, which provides even higher levels of security with two-factor authentication. Some types of Digipass token can operate in a Challenge-Response mode. Vasco Digipass is supported by RAdmin on Solaris, Linux and Windows. Your organization may require the issue of Vasco Digipass tokens to some or all users. If so, you should follow these instructions for administering Digipass tokens, and for assigning tokens to RAdmin users.

When you purchase a Digipass token or tokens from Vasco, you will also be supplied with a DPX file that contains important data about the token(s). This DPX file must be imported into the AuthBy DIGIPASS database before the tokens can be assigned to a user and authenticated by Radiator. A DPX file may contain data for one or more tokens, and for one or more applications. A Digipass application is a particular method of using a token. Your tokens will usually only be configured for one application.

21.1. Import Digipass Tokens

Before you can administer a token or assign it to a user, you must import the token data into the RAdmin database. This page allows you to import data for one or more tokens from a token DPX file.

Figure 17. Import Digipass Tokens



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Import Digipass Tokens

Use this page to import Digipass DPX files, which will add information about one or more Digipass tokens from the DPX file to your RAdmin database. After importing tokens, you can allocate a token to an individual user

Import DPX file: no file selected

Options: □ Overwrite existing tokens with the same serial

□ Auto create users and allocate tokens

Master import key 11111111111111111111111111111111

(If the DPX file has a non-standard Master Key to be used to import the data, specify that key here)

Application name

(This selects which application to import from the DPX file if there is more than one application available)

If there is a problem with this page, please contact admin

21.1.1. Import DPX File

Enter the name of the DPX file to import. This must exist on the machine where your browser is running. Most browsers provide a browse button to the right of this field allowing you to select the DPX file from a file dialog.

21.1.2. Overwrite existing tokens with same serial

If this option is set, then the import will overwrite and erase any previously imported data for the same tokens as included in the DPX file. If you receive the error message ‘failed: Duplicate entry’ or similar, it means that token has already been imported, and you may need to set the ‘Overwrite existing tokens with same serial’ in order to import it.

21.1.3. Auto create users and allocate tokens

If this option is set, for each token imported, a matching user is automatically created and allocated to the token. The name of the user is derived from the token serial number: leading zeroes are stripped and any trailing spaces and alpha characters (such as APPL1) are removed. The new user will be created with validity dates from the current time to the same date and time next year.

21.1.4. Master import key

This specifies the key that has been used to encrypt the DPX file. Defaults to ‘11111111111111111111111111111111’, but some organizations may use a different import key. Consult your system administrator is you get the error message ‘Master Key content is incorrect’.

21.1.5. Application name

This specifies the name of the Digipass application data to import from the DPX file. If there is only one application. Defaults to ‘APPL1’, which is a common Digipass application name. If the application data is not present in the DPX file when you import it, you will see an error message and a list of the application names available in that file. If there are several applications present in your import file and you don't know which one to choose, consult your system administrator.

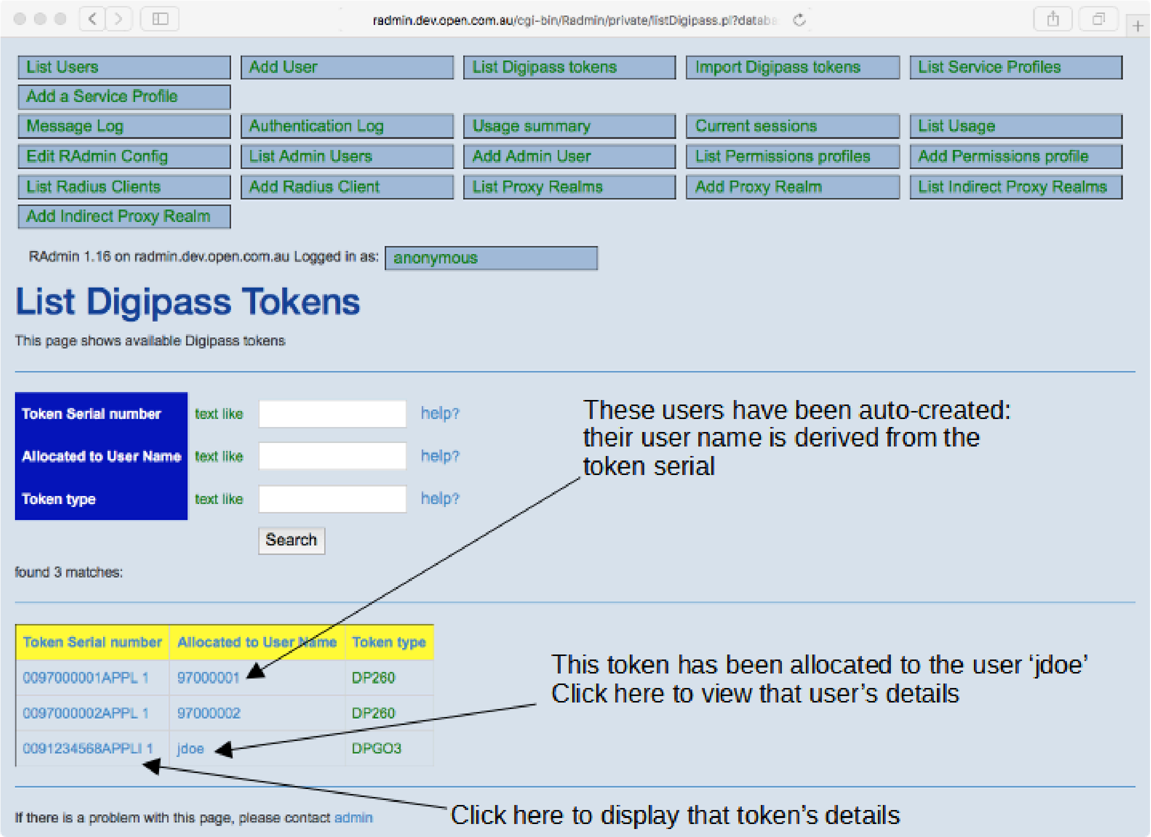
21.1.6. Import

When you click on Import, the DPX file you selected will be transmitted to the RAdmin web server, where the DPX data will be imported into the RAdmin database. If this is successful, the ‘Import Digipass Tokens’ page will be displayed again with one or more messages in green saying something like ‘imported token 0097123456APPL 1’ where 0097123456APPL 1 is the token's serial and application name it imported.

21.2. List Digipass Tokens

This page allows you to see which Digipass tokens have been imported into RAdmin, and which ones are available for allocation to a user. A user can't use their token for authentication until it has been allocated to them in RAdmin.

Figure 18. List Digipass Tokens



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Digipass Tokens

This page shows available Digipass tokens

Token Serial number	text like		help?
Allocated to User Name	text like		help?
Token type	text like		help?

found 3 matches:

Token Serial number	Allocated to User Name	Token type
0097000001APPL 1	97000001	DP260
0097000002APPL 1	97000002	DP260
0091234568APPLI 1	jdoe	DPGO3

If there is a problem with this page, please contact admin

These users have been auto-created: their user name is derived from the token serial

This token has been allocated to the user ‘jdoe’ Click here to view that user’s details

Click here to display that token’s details

21.2.1. Token Serial number

This specifies the unique token number for a token. The token number includes the application name: the application name is part of the complete serial number.

21.2.2. Allocated to User Name

This indicates whether the token has been allocated to a given user.

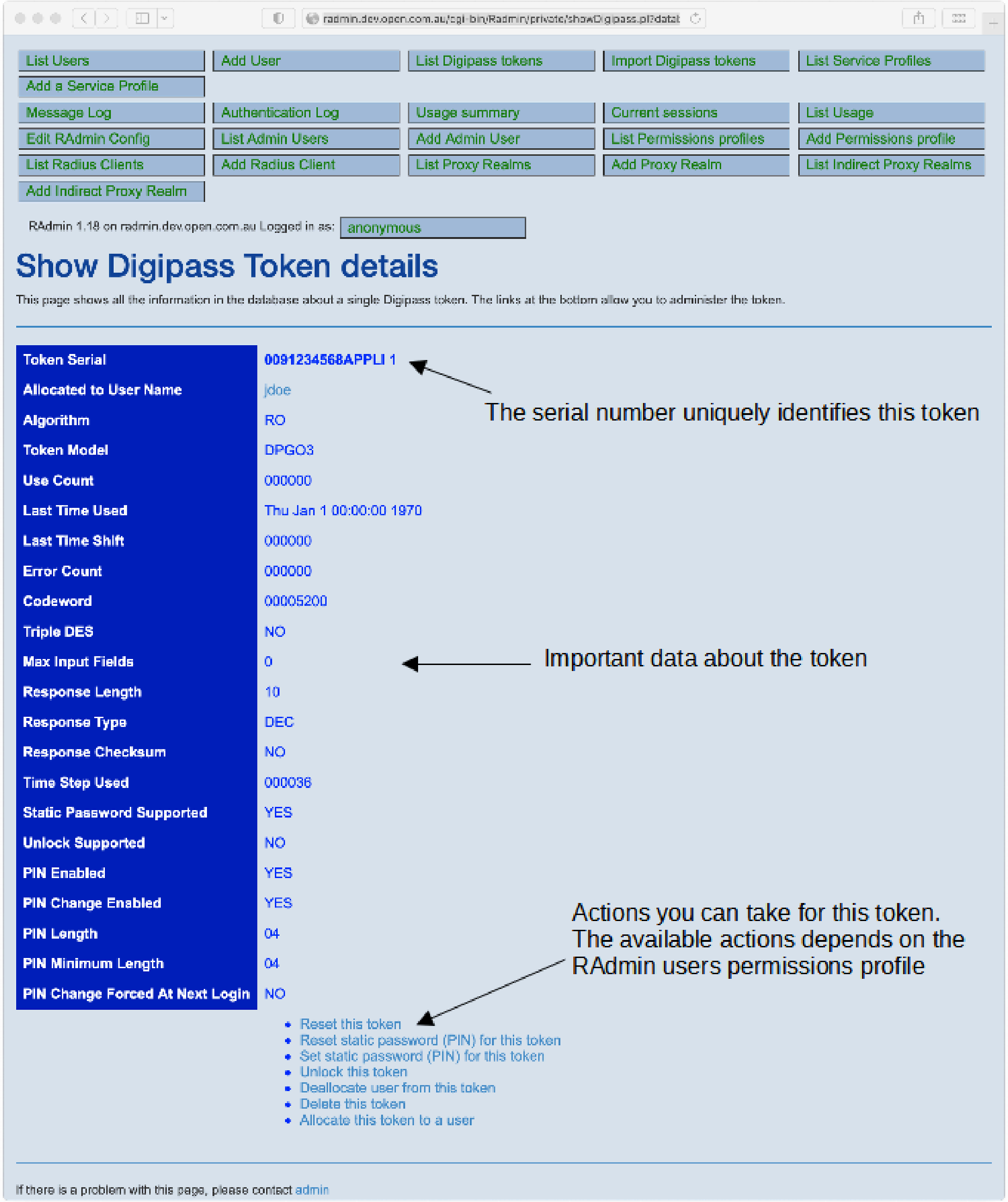
21.2.3. Token type

This indicates the type of Digipass token. Possibilities are: AKII, AUTCD, DP100, DP300, DP500, DP600, DP700 etc.

21.3. Show Digipass Token details

This page shows important details about a single Digipass token. These details are encoded in the RAdmin database for each token. Importing a token with the 'Overwrite existing tokens with same serial' option set will reset all these details..

Figure 19. Show Digipass Token details



RAdmin 1.18 on radmin.dev.open.com.au Logged in as: anonymous

Show Digipass Token details

This page shows all the information in the database about a single Digipass token. The links at the bottom allow you to administer the token.

Token Serial	0091234568APPLI 1
Allocated to User Name	jdoe
Algorithm	RO
Token Model	DPGO3
Use Count	000000
Last Time Used	Thu Jan 1 00:00:00 1970
Last Time Shift	000000
Error Count	000000
Codeword	00005200
Triple DES	NO
Max Input Fields	0
Response Length	10
Response Type	DEC
Response Checksum	NO
Time Step Used	000036
Static Password Supported	YES
Unlock Supported	NO
PIN Enabled	YES
PIN Change Enabled	YES
PIN Length	04
PIN Minimum Length	04
PIN Change Forced At Next Login	NO

The serial number uniquely identifies this token

Important data about the token

Actions you can take for this token.
The available actions depends on the
RAdmin users permissions profile

- Reset this token
- Reset static password (PIN) for this token
- Set static password (PIN) for this token
- Unlock this token
- Deallocate user from this token
- Delete this token
- Allocate this token to a user

If there is a problem with this page, please contact admin

21.3.1. Token Serial

The unique serial number for this token. It includes the application name. There can be multiple tokens with the same digits and different applications.

21.3.2. Allocated to User Name

If this token has been allocated to a user, the user name will appear here. A user cannot user their token to authenticate unless it has been allocated to them.

21.3.3. Algorithm

This identifies what sort of mode the Digipass token operates in. Possibilities are:

- RO: Response Only. The token generates a response each time it is activated. This Response is used as the password for the user to log in.
- CR: Challenge/Response. For each authentication, Radiator sends a challenge to the user. The user enters the challenge into the token using its keypad, and the token generates a matching Response, which is used as the password for the user to log in.
- SG: Signature. The token can be used to generate a digital signature, and is usually not used for logging in via Radiator.

Radiator supports authentication by both RO and CR tokens.

21.3.4. Token Model

Indicate what type of Digipass token this is. Possibilities are: AKII, AUTCD, DP100, DP300, DP500, DP600, DP700 etc.

21.3.5. Use Count

Indicates how many times this token has been authenticated since being imported.

21.3.6. Last Time Used

Indicates the last time this token was used. If the token has never been used, it will show ‘Thu Jan 1 00:00:00 1970’.

21.3.7. Last Time Shift

Indicates the time shift in seconds the last time the token was used.

21.3.8. Error Count

Indicates how many consecutive authentication errors have been detected. If this exceeds a certain threshold (check with your Radiator administrator) this user will not be able to authenticate.

21.3.9. Codeword

Describes the crypto algorithm used by this token.

21.3.10. Triple DES

Indicates if this token uses triple-DES. YES or NO.

21.3.11. Max Input Fields

If this token can be used for signatures, indicates the maximum number of fields that can be signed.

21.3.12. Response Length

Indicates how many characters in the tokens response.

21.3.13. Response Type

Indicates whether the tokens response is hexadecimal or decimal. HEX or DEC.

21.3.14. Response Checksum

Indicates whether the response has a checksum digit.

21.3.15. Time Step Used

Indicates the size of the timestep this token uses.

21.3.16. Reset this token

This link resets a number of Digipass counters, including Last Time Used, Last Time Shift and Error Count. Digipass provides automatic clock synchronization between Radiator and the Digipass token, but if a token has not been used for a long time, its clock may be out of synchronization. Resetting the token will allow new clock synchronization at the next authentication. Also if authentication has been locked because of too many incorrect authentications, Resetting will clear the error count.

21.3.17. Reset static password for this token

This can be used with a Digipass that has a static password (e.g Digipass GO 1). After clicking on ‘Reset static password for this token’, the user will have to define a new static password at their next authentication.

21.3.18. Set static password for this token

This can be used with a Digipass that has a static password (e.g Digipass GO 1). After clicking on ‘Set static password for this token’, RAdmin prompts you for a new static password that the user will have to use at their next authentication.

21.3.19. Unlock this token

Some types of Digipass require the user to enter a PIN into the Digipass before it can be used to generate a response. If the wrong PIN is entered into the Digipass too many times, it will be come locked, and you will have to use this function to unlock the token. When the token becomes locked, it will display a random number, which you must enter into the unlock token field. When you click on the /Unlock this token’ link, a new page will appear with a field where you enter the number displayed by the token, and click ‘Unlock’. The resulting Unlock Code must be entered by the user into their Digipass in order to unlock it.

21.3.20. Deallocate user from this token

This link deallocates the currently allocated user from this token, allowing it to be allocated to another user. After Deallocating a user, they will not be able to authenticate with that Digipass token.

21.3.21. Delete this token

This link deletes the Digipass token from the Radmin database.

21.3.22. Allocate this token to user xxxxx

This link will only appear during the process of allocating a token to a user. In order to allocate a token to a user, you must first go to the ‘Edit User’ page, click on the ‘Allocate a Digipass token to xxxx’, then search for and select a token and then click on the ‘Allocate this token to user xxxxx’ link.

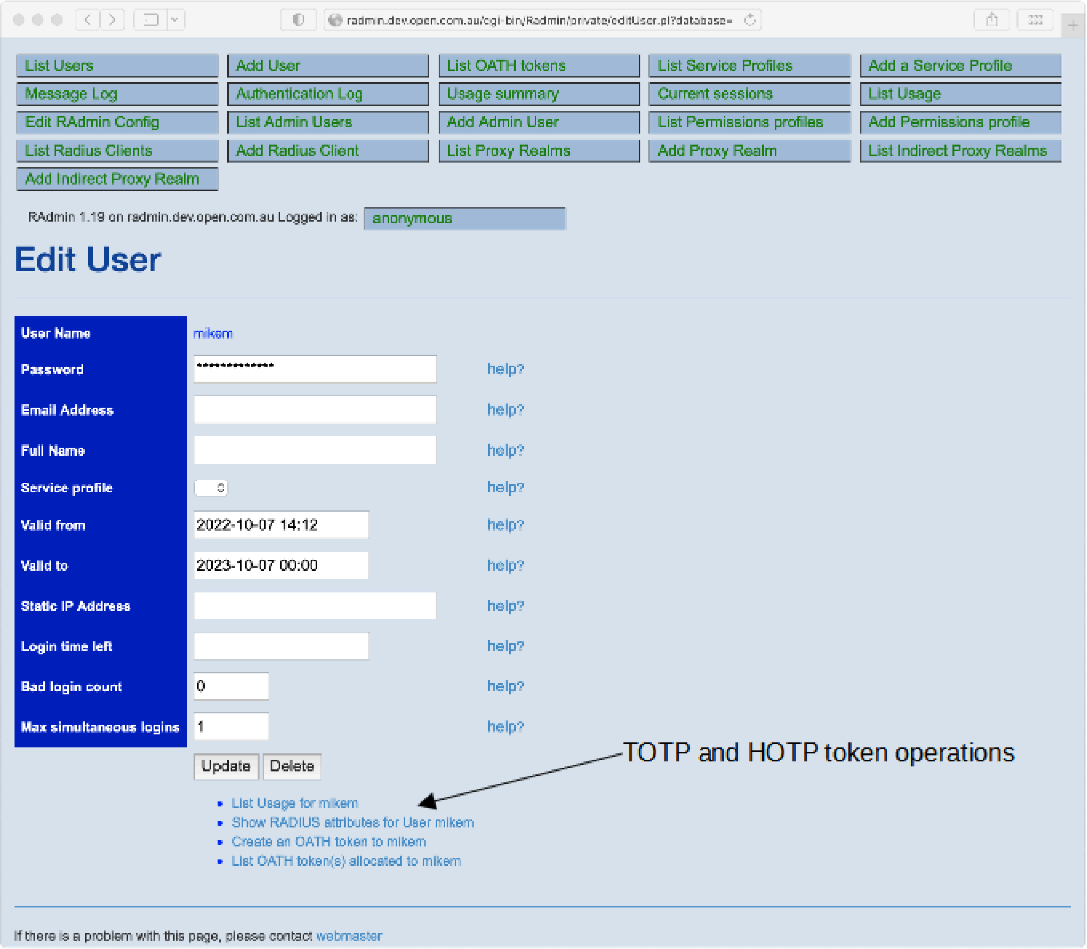
22. TOTP and HOTP (OATH) support

RAdmin can optionally support TOTP and HOTP tokens developed by OATH [https://openauthentication.org/ [https://openauthentication.org/]]. TOTP and HOTP are defined by RFCs 6238 and 4226, respectively. Such tokens provide much higher levels of security than static passwords. These tokens are created by RAdmin OATH tokens are supported on all RAdmin platforms. These tokens are typically provisioned to a mobile device app, such as Google Authenticator or Microsoft Authenticator.

22.1. Create and assign a TOTP or HOTP Token

To create a new token and assign it to a user, start by searching for the user with ‘List User’ page. If the user doesn't exist yet, create a new user with ‘Add User’ page. New token is created from the ‘Edit User’ page.

Figure 20. Add or view user's TOTP or HOTP token



RAdmin 1.19 on radmin.dev.open.com.au Logged in as: anonymous

Edit User

User Name	mikem	
Password	*************	help?
Email Address		help?
Full Name		help?
Service profile		help?
Valid from	2022-10-07 14:12	help?
Valid to	2023-10-07 00:00	help?
Static IP Address		help?
Login time left		help?
Bad login count	0	help?
Max simultaneous logins	1	help?

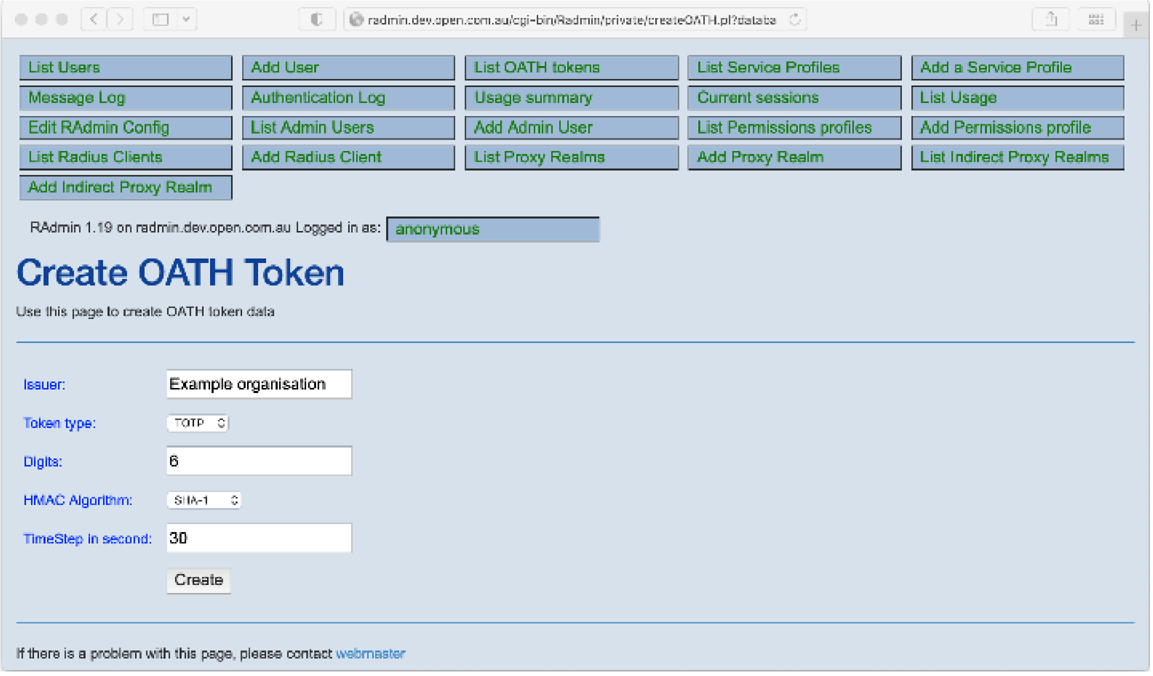
TOTP and HOTP token operations

- List Usage for mikem
- Show RADIUS attributes for User mikem
- Create an OATH token to mikem
- List OATH token(s) allocated to mikem

If there is a problem with this page, please contact webmaster

When you click ‘Create an OATH token to ...’ link, the ‘Create OATH Token’ page allows you to define additional token settings, such as ‘Issuer’ which defaults to ‘RAdmin’. Parameter ‘TimeStep in seconds’ is not applicable to HOTP tokens. In most cases only the ‘Issuer’ should be set and the other parameters can be left to their default values.

Figure 21. Adding a new TOTP token



RAdmin 1.19 on radmin.dev.open.com.au Logged in as: anonymous

Create OATH Token

Use this page to create OATH token data

Issuer: Example organisation

Token type: TOTP

Digits: 6

HMAC Algorithm: SHA-1

TimeStep in second: 30

If there is a problem with this page, please contact webmaster

22.1.1. Issuer

Typically the name of organisation, organisation unit or service the token relates to. The client apps display this information to help the user to select the correct token. The issuer values does not affect how the token values are calculated. Default to ‘Radmin’.

22.1.2. Token type

Type of OATH token, its value is **totp** or **hotp**. TOTP tokens are the most common type.

22.1.3. Digits

Number of digits the client app calculates and server requires for authentication. Defaults to 6. Other values are permissible but may not be supported by all client apps.

22.1.4. HMAC Algorithm

Typically SHA1. Other values are permissible but may not be supported by all client apps.

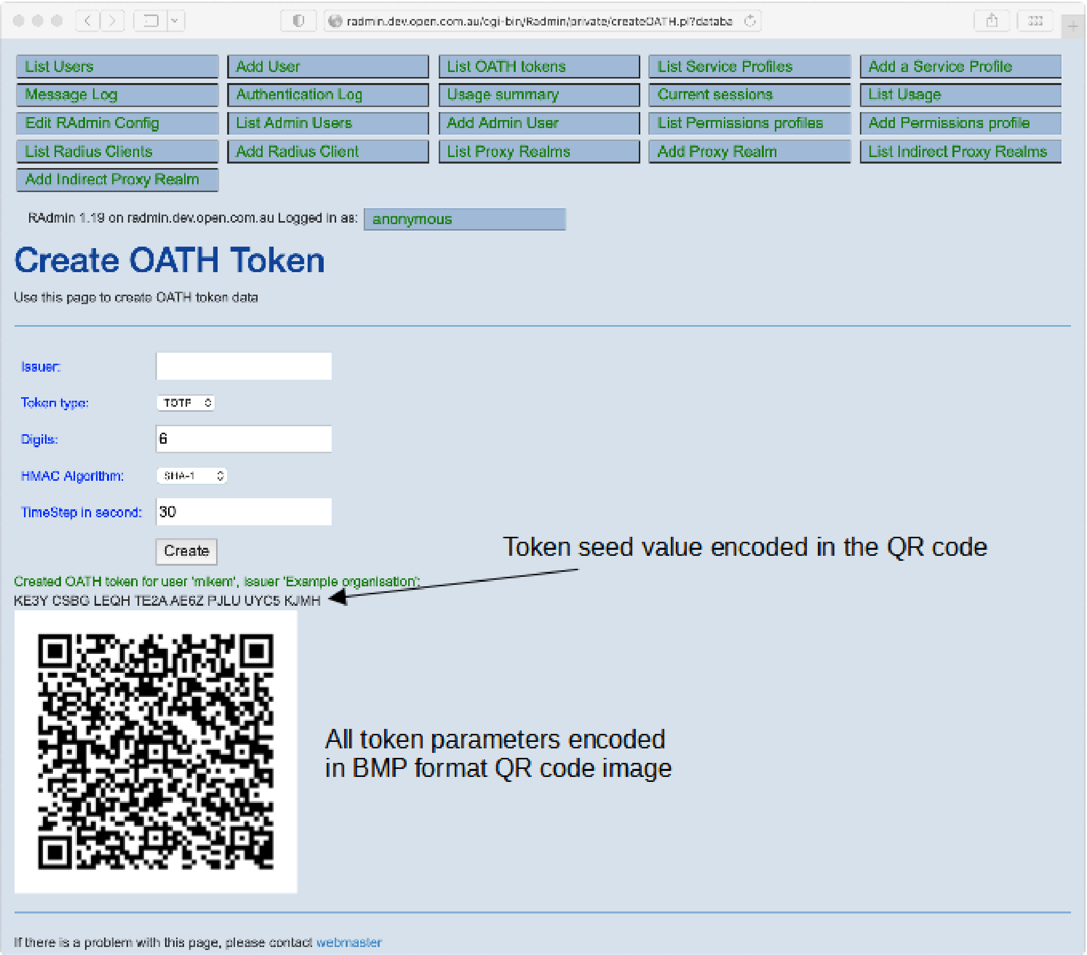
22.1.5. Timestep in seconds

Time interval in seconds when client app and server calculate a new token. Defaults to 30 seconds. Other values are permissible but may not be supported by all client apps.

When you click ‘Create’, RAdmin creates the token, writes its details into the RAdmin database and displays token provisioning information in text and QR code image format. The QR code is in Windows BMP format. If you save the image, name it with **.bmp** suffix.

The code displayed above QR code image is the token seed in Base32 format. This format is accepted by most, if not all, applications as an alternative for QR code based provisioning.

Figure 22. Newly created TOTP token provisioning information



RAdmin 1.19 on radmin.dev.open.com.au Logged in as: anonymous

Create OATH Token

Use this page to create OATH token data

Issuer:

Token type: TOTP

Digits: 6

HMAC Algorithm: SHA-1

TimeStep in second: 30

Created OATH token for user 'mikem', issuer 'Example organisation':
KE3Y CSBG LEQH TE2A AE6Z PJLU UYC5 KJMH

Token seed value encoded in the QR code

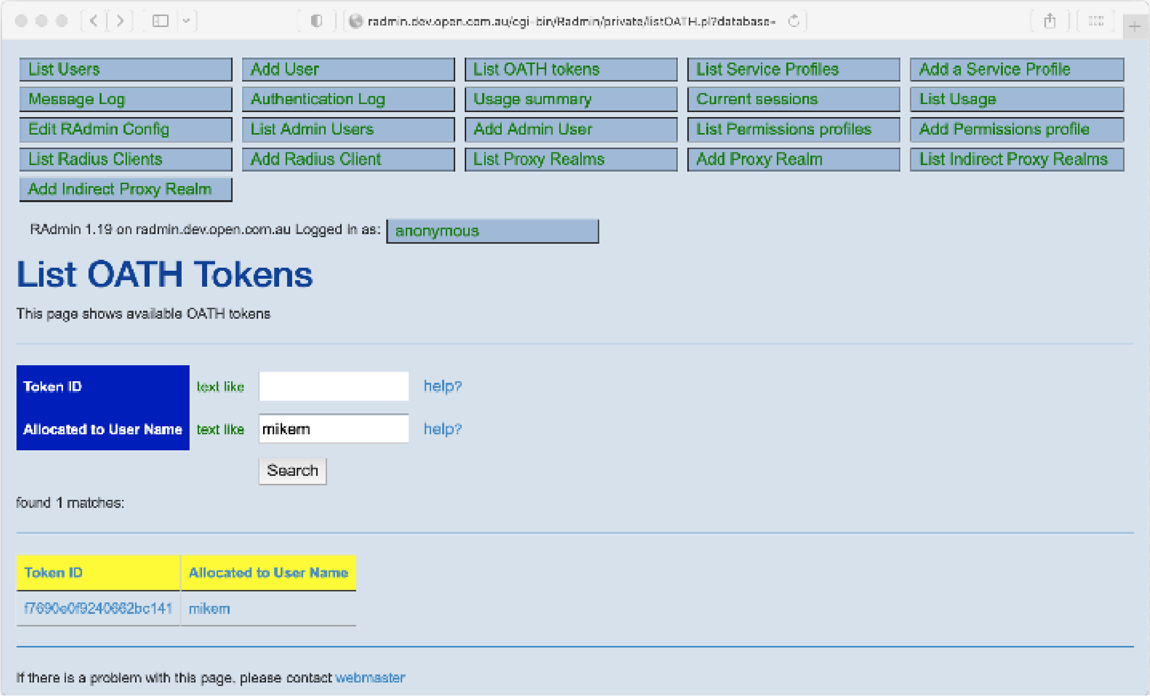
All token parameters encoded
in BMP format QR code image

If there is a problem with this page, please contact webmaster

22.2. List, re-assign and delete TOTP and HOTP Tokens

Use ‘List OATH tokens’ page to search and locate one or more tokens by token IDs or usernames. The search results show token ID which is a random string created by RAdmin. The token ID is not the token seed. The token seed is not displayed after the token is created.

Figure 23. OATH token search results



RAdmin 1.19 on radmin.dev.open.com.au Logged in as: anonymous

List OATH Tokens

This page shows available OATH tokens

Token ID	text like	
Allocated to User Name	text like	mikem

found 1 matches:

Token ID	Allocated to User Name
f7690e0f9240862bc141	mikem

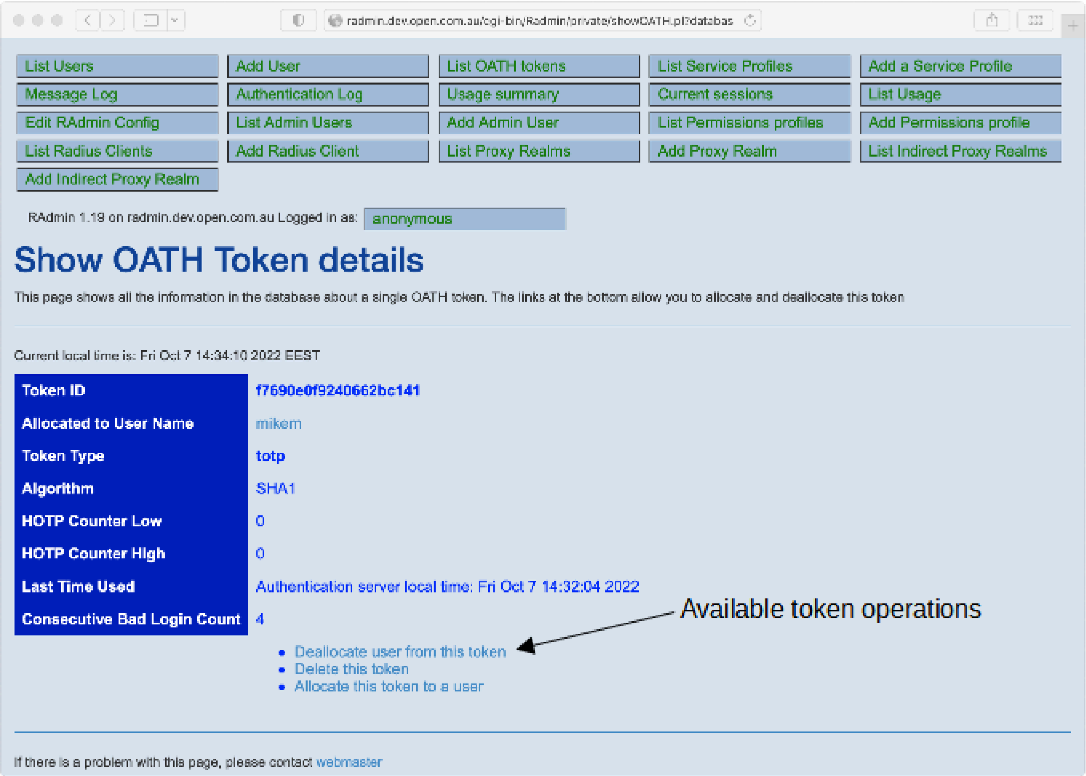
If there is a problem with this page, please contact webmaster

22.3. Show OATH Token details

When you click a ‘Token ID’ on the ’List OATH Tokens’ page, you can see the token details. The date and time values use RAdmin server's settings and are local to the server RAdmin runs on.

The token detail page allows changing the token assignment and provides the possibility to completely delete a token.

Figure 24. OATH token details



RAdmin 1.19 on radmin.dev.open.com.au Logged in as: anonymous

Show OATH Token details

This page shows all the information in the database about a single OATH token. The links at the bottom allow you to allocate and deallocate this token

Current local time is: Fri Oct 7 14:34:10 2022 EEST

Token ID	f7690e0f9240662bc141
Allocated to User Name	mikem
Token Type	totp
Algorithm	SHA1
HOTP Counter Low	0
HOTP Counter High	0
Last Time Used	Authentication server local time: Fri Oct 7 14:32:04 2022
Consecutive Bad Login Count	4

- Deallocate user from this token
- Delete this token
- Allocate this token to a user

If there is a problem with this page, please contact webmaster

22.3.1. Token ID

Random unique ID for the OATH token. This is not the token seed.

22.3.2. Allocated to User Name

This indicates whether the token has been allocated to a given user.

22.3.3. Token type

Type of OATH token. Its value is **totp** or **hotp**. The value is set when the token is created.

22.3.4. Algorithm

Typically SHA1. Other values are permissible but may not be supported by all client apps. The value is set when the token is created.

22.3.5. HOTP Counter Low and HOTP Counter High

Current values for counters HOTP uses. Not used with TOTP tokens.

22.3.6. Last time used

This timestamp tells when the token information in the DB was last used to verify a token. It's the timestamp of last successful or failed token verification.

22.3.7. Consecutive Bad Login Count

How many times token verification has failed after the last successful verification.

23. Yubikey support

RAdmin can optionally support Yubikey tokens from Yubico (http://www.yubico.com [http://www.yubico.com]). Yubico tokens are small USB devices that act like a keyboard and which type in a one-time-password when the button is pressed. They can be purchased from Yubico and issued to your users. Such tokens provide much higher levels of security than static passwords. Yubikey is supported on all RAdmin platforms.

Each Yubikey token has a unique Token ID (also called the public identity in Yubico documentation), and a secret AES cryptographic key. In order to authenticate a Yubikey token, the RAdmin database must contain a Yubikey record containing both the Token ID and the AES secret for that key. You can add new tokens into the RAdmin database with the RAdmin ‘Import Yubikey Tokens’ page. After a token is imported, it must be allocated to a user before that user can use the token to authenticate.

23.1. Import Yubikey Tokens

Before you can administer a token or assign it to a user, you must import the token data into the RAdmin database. This page allows you to import data for one or more tokens.

It is necessary to use the Yubico Personalization Tool (https://www.yubico.com/products/services-software/personalization-tools/use/ [https://www.yubico.com/products/services-software/personalization-tools/use/]) to manually initialise each Yubikey with a new Token ID and AES Secret, and then cut-and-paste them into the RAdmin ‘Import Yubikey Tokens’ page.

Note

Support for Windows COM/ActiveX browser plugin for intialising Yubikeys was removed in RAdmin 1.16.

The following chapters describe the fields available on the Import Yubikey Tokens page.

23.1.1. Token ID

Enter the unique Token ID (also called the public identity in Yubico documentation). This is a 12 character Hex string, with optional spaces.

Note

If you would like to use private identity as Token ID, do not enable ‘Auto create user and allocate token’ and allocate tokens separately. You may also need to modify Radiator configuration. AuthSelect in AuthBy SQLYUBIKEY clause must return TOKEN_ID that is needed for CheckSecretId configuration parameter to work. See AuthBy SQLYUBIKEY in Radiator reference manual for more information.

23.1.2. Token AES Secret

Enter the token AES secret. This is a 32 character Hex string, with optional spaces.

23.1.3. Overwrite existing tokens with the same Token ID

If there is already a Yubikey token with this Token ID is already in the RAdmin database, this flag will cause it key to be overwritten. If this flag is not set, the import operation will fail.

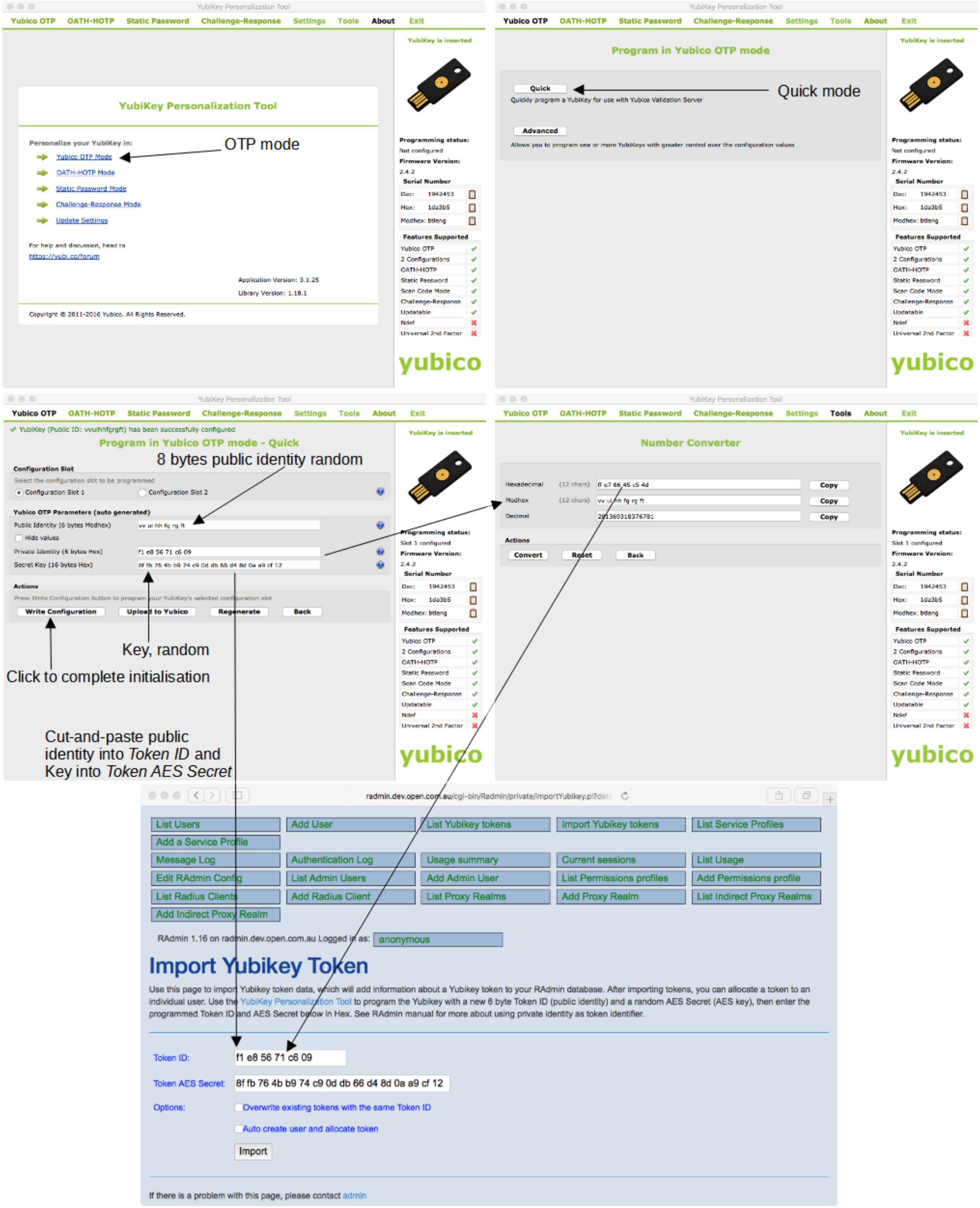
23.1.4. Auto create user and allocate token

If this option is set, the Import will both add the token to the RAdmin database and also create a new user whose user name is the same as the Token ID, and will allocate the token to that user. The new user will be created with validity dates from the current time to the same date and time next year.

23.2. Initialising Tokens with Yubico Personalization Tool

You must use the Yubico Personalization Tool to manually initialise the Yubikey, and then cut-and-paste the new token details into the Import form. The Yubico Personalization Tool can be downloaded from http://www.yubico.com/developers/personalization/ [http://www.yubico.com/developers/personalization/].

Figure 25. Initialising and Importing Yubikey token using Yubico Personalization Tool



OTP mode

Quick mode

8 bytes public identity random

Key, random

Click to complete initialisation

Cut-and-paste public identity into *Token ID* and Key into *Token AES Secret*

For help and discussion, head to https://yubi.co/forum

Application Version: 3.1.25

Library Version: 1.18.1

Copyright © 2011-2016 Yubico. All Rights Reserved.

Quickly program a YubiKey for use with Yubico Validation Server

Allows you to program one or more YubiKeys with greater control over the configuration values

Programming status: Not configured

Firmware Version: 2.4.2

Serial Number

Dec: 1942453

Hex: 1da3b5

Modhex: btleng

✓ YubiKey (Public ID: vvuihhfgrgft) has been successfully configured

Select the configuration slot to be programmed

● Configuration Slot 1 ○ Configuration Slot 2

Public Identity (6 bytes Modhex): vv ui hh fg rg ft

□ Hide values

Private Identity (6 bytes Hex): f1 e8 56 71 c6 09

Secret Key (16 bytes Hex): 8f fb 76 4b b9 74 c9 0d db 66 d4 8d 0a a9 cf 12

Press Write Configuration button to program your YubiKey's selected configuration slot

Programming status: Slot 1 configured

Hexadecimal (12 chars) f1 e7 66 45 c5 4d

Modhex (12 chars) vv ui hh fg rg ft

Decimal 281360318376781

Features Supported	
Yubico OTP	✓
2 Configurations	✓
OATH-HOTP	✓
Static Password	✓
Scan Code Mode	✓
Challenge-Response	✓
Updatable	✓
Ndef	✗
Universal 2nd Factor	✗

radmin.dev.open.com.au/cgi-bin/Radmin/private/importYubikey.pl?data

RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Import Yubikey Token

Use this page to import Yubikey token data, which will add information about a Yubikey token to your RAdmin database. After importing tokens, you can allocate a token to an individual user. Use the YubiKey Personalization Tool to program the Yubikey with a new 6 byte Token ID (public identity) and a random AES Secret (AES key), then enter the programmed Token ID and AES Secret below in Hex. See RAdmin manual for more about using private identity as token identifier.

Token ID: f1 e8 56 71 c6 09

Token AES Secret: 8f fb 76 4b b9 74 c9 0d db 66 d4 8d 0a a9 cf 12

Options: □ Overwrite existing tokens with the same Token ID

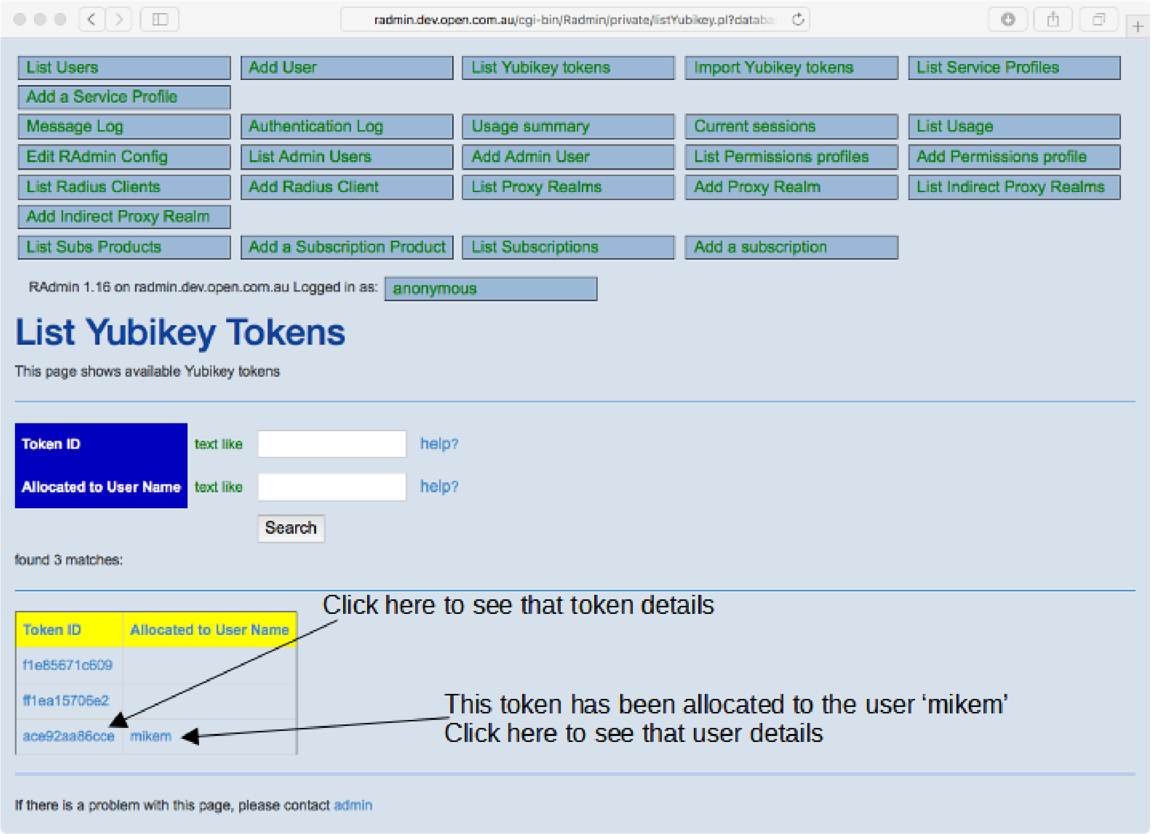
□ Auto create user and allocate token

If there is a problem with this page, please contact admin

23.3. List Yubikey Tokens

This page allows you to see which Yubikey tokens have been imported into RAdmin, and which ones are available for allocation to a user. A user can't use their token for authentication until it has been allocated to them in RAdmin.

Figure 26. List Yubikey Tokens



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

List Yubikey Tokens

This page shows available Yubikey tokens

Token ID	text like		help?
Allocated to User Name	text like		help?

Search

found 3 matches:

Token ID	Allocated to User Name
f1e85671c609	
ff1ea15706e2	
ace92aa86cce	mikem

Click here to see that token details

This token has been allocated to the user ‘mikem’
Click here to see that user details

If there is a problem with this page, please contact admin

23.3.1. Token ID

This specifies the unique Token ID number for a token.

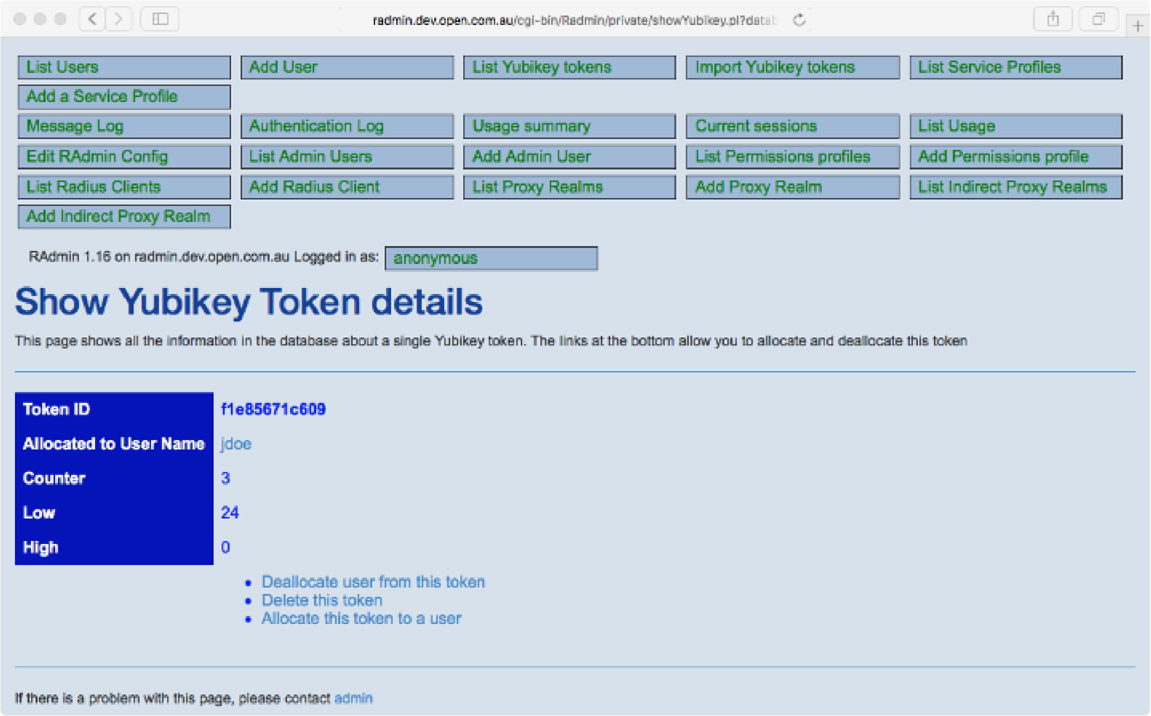
23.3.2. Allocated to User Name

This indicates whether the token has been allocated to a given user.

23.4. Show Yubikey Token details

This page shows important details about a single Yubikey token. These details are encoded in the RAdmin database for each token. Importing a token with the ‘Overwrite existing tokens with same Token ID’ option set will reset all these details.

Figure 27. Show Yubikey Token details



RAdmin 1.16 on radmin.dev.open.com.au Logged in as: anonymous

Show Yubikey Token details

This page shows all the information in the database about a single Yubikey token. The links at the bottom allow you to allocate and deallocate this token

Token ID	f1e85671c609
Allocated to User Name	jdoe
Counter	3
Low	24
High	0

- Deallocate user from this token
- Delete this token
- Allocate this token to a user

If there is a problem with this page, please contact admin

23.4.1. Token ID

The tokens unique Token ID.

23.4.2. Allocated To User Name

The user this token is allocated to (if any).

23.4.3. Counter

If the token has been authenticated by Radiator at least once, this field will contain the Yubikey session counter of the last authentication.

23.4.4. Low

If the token has been authenticated by Radiator at least once, this field will contain the key use counter for this Yubikey session.

23.4.5. High

This parameter is not currently used. Low and High fields were used differently with old Radiator versions. See Radiator revision history for the details.

24. Some common tasks

The following chapters describe some of the common tasks.

24.1. Adding a new user

1. Click on [Add a User] in the toolbar. You will get the Add a User page. See Add a User, Edit a User on page 7.

2. Enter a user name. This will be the name the user must use to log in with.
3. Make sure the automatically generated password is suitable.
4. Choose a suitable Service Profile from the set of Service Profiles configured into your RAdmin system.
5. Enter a suitable Valid to date. This will be the last date/time the user will be allowed to log in. Don't forget that the default time is midnight at the beginning of that day.
6. If the user needs a static IP address, enter it as an IP address, in the format 203.63.154.1
7. If the user is to be limited to a maximum amount of usage, enter the number of seconds in Login time left field. If there is no limit, leave it blank.
8. Click on the **Add** button.
9. The user should now be able to log in, using the user name and password you entered.

24.2. Changing a password

1. Find the user you are interested in, perhaps by using the List Users page. See Finding a User on page 49. See List Users on page 10
2. Click on the user name to get the Edit a User page. See Add a User, Edit a User on page 7
3. Delete the old password and enter a new one.
4. Click on the **Update** button.
5. The new password is now in effect. The user will have to use the new password next time they log in. Any current sessions are unaffected.

24.3. Finding a User

1. Click on [List Users] in the toolbar. You will get the List Users page, including a list of all your current users. See List Users on page 10.
2. Enter your search criteria in the top section.
3. Click on the **Search** button.
4. When the page reappears, look in list in the bottom section for the user you are interested in. If you still cant see them, change your search criteria and press the **Search** button again.
5. When you find the user you are interested in, click on the User Name, this will take you to the Edit a User page for that user. See Add a User, Edit a User on page 7.

24.4. Deleting a user

1. Find the user you are interested in, perhaps by using the List Users page. See Finding a User on page 49. See List Users on page 10
2. Click on the user name to get the Edit a User page. See Add a User, Edit a User on page 7.
3. Click on the **Delete** button.
4. The user has now been removed from the database and they will not be able to login in again. Note that this has no effect on any current sessions they may have: if they are already logged in, this will not force them to disconnect.

24.5. Checking who is currently on-line

1. Click on [Current sessions] in the toolbar. You will get the Current sessions page. See Current sessions on page 16
2. At the bottom of the page is a list of all the current sessions.
3. If you have lots of sessions and can’t find the one you are interested in, enter some search criteria in the top section and click on the **Search** button.

24.6. Checking a user's session history

1. Find the user you are interested in, perhaps by using the List Users page. See Finding a User on page 49. See List Users on page 10.
2. Click on the user name to get the Edit a User page. See Add a User, Edit a User on page 7.
3. Click on the “Usage for ...” hotlink at the bottom right. You will get a List Usage page showing all sessions for that user in the database. See List Usage on page 11.

24.7. Checking usage summaries

1. Click on [Usage summary] in the toolbar. You will get the Usage summary page. See Usage Summary on page 14.
2. At the bottom of the page is a list of all users that have sessions in your accounting table. For each table you will see the total time online (in seconds), plus the total bytes transferred in and out (in means into your network, out means out to the user).
3. If you have lots of users and can't find the one you are interested in, enter some search criteria in the top section and click on the **Search** button.

24.8. Checking the message log

1. Click on [Log] in the toolbar. You will get the Log page. See Log on page 15.
2. Log messages will be shown in the bottom part of the page. The most recent messages will be shown near the top of that section.
3. If you cant find the message(s) you are interested in, you can limit the search be entering search criteria in the top part of the page and pressing the **Search** button.

24.9. Checking modem usage

1. Click on [Modem usage report] in the toolbar. You will get the “Modem usage report” page. See Modem usage report on page 19.
2. Usage summaries by NAS and Port will be shown in the bottom part of the page. If you see any ports with an unusually low “Session” count, it may be because the associated modem is dead.

24.10. Help a user with login problems

1. Click on [Authentication Log] in the toolbar. You will get the “Authentication Log” page. See Authentication Log on page 20.
2. Enter the user name into the User name field.
3. Click on the **Search** button. You will see a list of recent authentication successes and failures. The Failure messages will have a Failure reason that will help identify the user's problem.

24.11. Import Digipass tokens from a DPX file

1. Ensure the DPX file is on your workstation: the computer where your web browser is running.
2. Click on [Import Digipass tokens] in the toolbar. You will get the “Import Digipass Tokens” page. See Import Digipass Tokens on page 33.
3. Enter the name of the DPX file into ‘Import DPX File: field or clicking on the file browser button.
4. Click on the **Import** button.

24.12. Allocating a Digipass token to a user

1. Ensure the tokens data has been imported. See Import Digipass tokens from a DPX file on page 51.
2. Ensure the user has been created. See Adding a new user on page 48.
3. Using the List Users page, find the user you wish to allocate a token to. Click on the User Name. You will get the “Edit User” page. See Add a User, Edit a User on page 7.
4. Click on the ‘Allocate a Digipass token to xxxx’ link near the bottom of the Edit User page. You will get the ‘List Digipass Tokens’ page. See List Digipass Tokens on page 35.
5. Click on the **Search** button. The “List Digipass Tokens” page will appear again, showing the tokens that matched your search criteria. You will be able to see which tokens do not have a user allocated to them.
6. Select the token you wish to allocate to the user by clicking on the token serial number. You will get the “Show Digipass Token Details” page. See Show Digipass Token details on page 36.
7. Click on the “Allocate this token to user xxxx” link near the bottom of the page. You will get the “Show Digipass Token Details” page again showing the user’s name in the “Allocated to User Name” field.
8. Ensure the user is given the physical token matching the one you allocated.

24.13. Import a Yubikey token

1. Ensure the YubiKey Personalisation Tool is installed on your browser host.
2. Open the Import Yubikey Token page.
3. Insert a Yubikey token into a USB port on your browser host. Launch the Personalisation Tool. Initialise the token. See Initialising Tokens with Yubico Personalization Tool on page 45. When the token is initialised, enter new TokenID and AES Secret into the Import form.
4. Click on Import. This will add the token details to the RAdmin database.

24.14. Allocating a Yubikey token to a user

1. Ensure the token data has been imported. See Import a Yubikey token on page 51.
2. Ensure the user has been created. See Adding a new user on page 48.
3. Using the List Users page, find the user you wish to allocate a token to. Click on the User Name. You will get the “Edit User” page. See Add a User, Edit a User on page 7.
4. Click on the ‘Allocate a Yubikey token to xxxx’ link near the bottom of the Edit User page. You will get the ‘List Yubikey Tokens’ page. See List Yubikey Tokens on page 46.
5. Click on the **Search** button. The “List Yubikey Tokens” page will appear again, showing the tokens that matched your search criteria. You will be able to see which tokens do not have a user allocated to them.
6. Select the token you wish to allocate to the user by clicking on the token serial number. You will get the “Show Yubikey Token Details” page. See Show Yubikey Token details on page 47.

7. Click on the “Allocate this token to user xxxx” link near the bottom of the page. You will get the “Show Yubikey Token Details” page again showing the user’s name in the “Allocated to User Name” field.
8. Ensure the user is given the physical token matching the one you allocated.