HotSpot User AAA

Document revision 2.4 (February 6, 2008, 1:40 GMT)
This document applies to V3.0

Table of Contents

General Information

Summary

This document provides information on authentication, authorization and accounting parameters and configuration for HotSpot gateway system.

Specifications

Packages required: ***system***
License required: ***level1***
Home menu level: ***/ip hotspot user***
Standards and Technologies: ***RADIUS***
Hardware usage: *Local traffic accounting requires additional memory*

Description

HotSpot User Profiles

Home menu level: ***/ip hotspot user profile***

Description

HotSpot User profiles are used for common user settings. Profiles are like user groups, they are grouping users with the same limits.

Property Description

address-pool (*namenone*; default: **none**) - the IP pool name which the users will be given IP addresses from. This works like dhcp-pool method in earlier versions of MikroTik RouterOS, except that it does not use DHCP, but rather the embedded one-to-one NAT

- **none** - do not reassign IP addresses to the users of this profile

advertise (yes | no; default: **no**) - whether to enable forced advertisement popups for this profile

advertise-interval (*multiple choice: time*; default: **30m,10m**) - set of intervals between showing advertisement popups. After the list is done, the last value is used for all further advertisements

advertise-timeout (*timeimmediately* | *never*; default: **1m**) - how long to wait for advertisement to be shown, before blocking network access with walled-garden

advertise-url (*multiple choice: text*; default: **http://www.mikrotik.com/,http://www.routerboard.com/**) - list of URLs to show as advertisement popups. The list is cyclic, so when the last item reached, next time the first is shown

idle-timeout (*timenone*; default: **none**) - idle timeout (maximal period of inactivity) for authorized clients. It is used to detect, that client is not using outer networks (e.g. Internet), i.e., there is NO TRAFFIC coming from that client and going through the router. Reaching the timeout, user will be logged out, dropped of the host list, the address used by the user will be freed, and the session time accounted will be decreased by this value

- **none** - do not timeout idle users

incoming-filter (*name*) - name of the firewall chain applied to incoming packets from the users of this profile

incoming-packet-mark (*name*) - packet mark put on all the packets from every user of this profile automatically

keepalive-timeout (*timenone*; default: **00:02:00**) - keepalive timeout for authorized clients. Used to detect, that the computer of the client is alive and reachable. If check will fail during this period, user will be logged out, dropped of the host list, the address used by the user will be freed, and the session time accounted will be decreased by this value

- **none** - do not timeout unreachable users

name (*name*) - profile reference name

on-login (*text*; default: "") - script name to launch after a user has logged in

on-logout (*text*; default: "") - script name to launch after a user has logged out

open-status-page (*always* | *http-login*; default: **always**) - whether to show status page also for users authenticated using mac login method. Useful if you want to put some information (for example, banners or popup windows) in the alogin.html page so that all users would see it

- **http-login** - open status page only in case of HTTP login (including cookie and https login methods)
- **always** - open the status page in case of mac login as well once the user opens any web page

outgoing-filter (*name*) - name of the firewall chain applied to outgoing packets to the users of this profile

outgoing-packet-mark (*name*) - packet mark put on all the packets to every user of this profile automatically

rate-limit (*text*; default: **""**) - Rate limitation in form of rx-rate[/tx-rate] [rx-burst-rate[/tx-burst-rate] [rx-burst-threshold[/tx-burst-threshold] [rx-burst-time[/tx-burst-time] [priority] [rx-rate-min[/tx-rate-min]]]] from the point of view of the router (so "rx" is client upload, and "tx" is client download). All rates should be numbers with optional 'k' (1,000s) or 'M' (1,000,000s). If tx-rate is not specified, rx-rate is as tx-rate too. Same goes for tx-burst-rate and tx-burst-threshold and tx-burst-time. If both rx-burst-threshold and tx-burst-threshold are not specified (but burst-rate is specified), rx-rate and tx-rate is used as burst thresholds. If both rx-burst-time and tx-burst-time are not specified, 1s is used as default. Priority takes values 1..8, where 1 implies the highest priority, but 8 - the lowest. If rx-rate-min and tx-rate-min are not specified rx-rate and tx-rate values are used. The rx-rate-min and tx-rate-min values can not exceed rx-rate and tx-rate values.

session-timeout (*time*; default: **0s**) - session timeout (maximal allowed session time) for client. After this time, the user will be logged out unconditionally

- **0** - no timeout

shared-users (*integer*; default: **1**) - maximal number of simultaneously logged in users with the same username

status-autorefresh (*timenone*; default: **none**) - HotSpot servlet status page autorefresh interval

transparent-proxy (yes | no; default: **yes**) - whether to use transparent HTTP proxy for the authorized users of this profile

Notes

When idle-timeout or keepalive is reached, session-time for that user is reduced by the actual period of inactivity in order to prevent the user from being overcharged.

Example

HotSpot Users

Home menu level: ***/ip hotspot user***

Property Description

address (*IP address*; default: **0.0.0.0**) - static IP address. If not 0.0.0.0, client will always get the same IP address. A configured address implies, that only one simultaneous login for that user is allowed. Any existing address will be replaced with this one using the embedded one-to-one NAT

bytes-in (*read-only: integer*) - total amount of bytes received from user

bytes-out (*read-only: integer*) - total amount of bytes sent to user

email (*text*) - e-mail address. Only basic syntax checking is done to ensure validity of this field

limit-bytes-in (*integer*; default: **0**) - maximum amount of bytes user can transmit (i.e., bytes received from the user)

- **0** - no limit

limit-bytes-out (*integer*; default: **0**) - maximum amount of bytes user can receive (i.e., bytes sent to

the user)

- **0** - no limit

limit-bytes-total (*integer*; default: **0**) - maximum aggregate amount of bytes user can receive and send (i.e., the sum of the amount of bytes sent to the user and received from it)

- **0** - no limit

limit-uptime (*time*; default: **0s**) - total uptime limit for user (pre-paid time)

- **0s** - no limit

mac-address (*MAC address*; default: **00:00:00:00:00:00**) - static MAC address. If not 00:00:00:00:00:00, client is allowed to login only from that MAC address

name (*name*) - user name. If authentication method is trial, then user name will be set automaticly after following pattern "T-MAC_adress", where MAC_address is trial user Mac address

packets-in (*read-only: integer*) - total amount of packets received from user (i.e., packets received from the user)

packets-out (*read-only: integer*) - total amount of packets sent to user (i.e., packets sent to the user)

password (*text*) - user password

profile (*name*; default: **default**) - user profile

routes (*text*) - routes that are to be registered on the HotSpot gateway when the client is connected. The route format is: dst-address [[gateway] [metric]] (for example, 10.1.0.0/24 10.0.0.1 1). Several routes may be specified separated with commas. If gateway is not specified, the remote address is used. If metric is not speciefied, the metric of 1 is used

server (*nameall*; default: **all**) - which HotSpot server is this user allowed to log in to

uptime (*read-only: time*) - total time user has been logged in

Notes

In case of **mac** authentication method, clients' MAC addresses can be used as usernames (without password)

The byte limits are total limits for each user (not for each session as at **/ip hotspot active**). So, if a user has already downloaded something, then session limit will show the total limit - (minus) already downloaded. For example, if download limit for a user is 100MB and the user has already downloaded 30MB, then session download limit after login at **/ip hotspot active** will be 100MB - 30MB = 70MB.

Should a user reach his/her limits (bytes-in >= limit-bytes-in or bytes-out >= limit-bytes-out), he/she will not be able to log in anymore.

The statistics is updated if a user is authenticated via local user database each time he/she logs out. It means, that if a user is currently logged in, then the statistics will not show current total values. Use **/ip hotspot active** submenu to view the statistics on the current user sessions.

If the user has IP address specified, only one simultaneous login is allowed. If the same credentials are used again when the user is still active, the active one will be automatically logged off.

Trial users will have dynamic records here with their **name** written as "T-[mac]" (where [mac] is the user's MAC address, without the brackets), **email** set to the password the user has supplied, **mac-address** - the client's MAC address, **profile** and **limit-uptime** - the respective values of **trial-user-profile** and **trial-uptime** limit properties of the HotSpot server profile. The entries will be automatically removed once

the trial user times out (after **trial-uptime** reset time).

Example

To add user **ex** with password **ex** that is allowed to log in only with **01:23:45:67:89:AB** MAC address and is limited to 1 hour of work:

```
[admin@MikroTik] ip hotspot user> add name=ex password=ex \
\... mac-address=01:23:45:67:89:AB limit-uptime=1h
[admin@MikroTik] ip hotspot user> print
Flags: X - disabled
 #   SERVER     NAME                      ADDRESS         PROFILE UPTIME
 0              ex                                        default 00:00:00
[admin@MikroTik] ip hotspot user> print detail
Flags: X - disabled, D - dynamic
 0   name="ex" password="ex" mac-address=01:23:45:67:89:AB profile=default
limit-uptime=1h uptime=0s bytes-in=0 bytes-out=0 packets-in=0 packets-out=0
[admin@MikroTik] ip hotspot user>
```

HotSpot Active Users

Home menu level: ***/ip hotspot active***

Description

The active user list shows the list of currently logged in users. Nothing can be changed here, except user can be logged out with the **remove** command.

Property Description

address (*read-only: IP address*) - IP address of the user

blocked (*read-only: flag*) - whether the user is blocked by advertisement (i.e., usual due advertisement is pending)

bytes-in (*read-only: integer*) - how many bytes did the router receive from the client

bytes-out (*read-only: integer*) - how many bytes did the router send to the client

domain (*read-only: text*) - domain of the user (if split from username)

idle-time (*read-only: time*) - the amount of time has the user been idle

idle-timeout (*read-only: time*) - the exact value of idle-timeout that applies to this user. This property shows how long should the user stay idle for it to be logged off automatically

keepalive-timeout (*read-only: time*) - the exact value of keepalive-timeout that applies to this user. This property shows how long should the user's computer stay out of reach for it to be logged off automatically

limit-bytes-in (*read-only: integer*) - maximal amount of bytes the user is allowed to send to the router

limit-bytes-out (*read-only: integer*) - maximal amount of bytes the router is allowed to send to the client

limit-bytes-total (*read-only: integer*) - maximal aggregate amount of bytes the router is allowed to send to the client and receive form it

login-by (*multiple choice, read-only: cookie | http-chap | http-pap | https | mac | trial*) - authentication method used by user

mac-address (*read-only: MAC address*) - actual MAC address of the user

packets-in (*read-only: integer*) - how many packets did the router receive from the client

packets-out (*read-only: integer*) - how many packets did the router send to the client

radius (*read-only: flag*) - whether the user was authenticated via RADIUS

server (*read-only: name*) - the particular HotSpot server the used is logged on at.

session-time-left (*read-only: time*) - the exact value of session-time-left that applies to this user. This property shows how long should the user stay logged-in (see uptime) for it to be logged off automatically

uptime (*read-only: time*) - current session time of the user (i.e., how long has the user been logged in)

user (*read-only: name*) - name of the user

Example

To get the list of active users:

```
[admin@MikroTik] ip hotspot active> print
Flags: R - radius, B - blocked
 #    USER         ADDRESS         UPTIME       SESSION-TIME-LEFT IDLE-TIMEOUT
 0    ex           10.0.0.144      4m17s        55m43s
[admin@MikroTik] ip hotspot active>
```