Advanced Settings

User Idle Timeout

Set the amount of time in minutes, after which, if no update is received for this user, it will be considered offline and the session will close. This number should be at least 2 minutes higher than the interim-update amount in your NAS. For example, if the interim update (accounting interval) was 1 minute in your NAS, then you should set the User Idle Timeout to 2 or 4 minutes.

Note that when SAS closes the session, and the user is actually online in your NAS, it will not be disconnected. However, if any new accounting-update packet is received from NAS for the same session id, then SAS will reopen the same session instead of creating a new one.

default: 4 minutes

Mikrotik Interim Update

(Mikrotik Only) This will set the interim-update time in Mikrotik. If you have already set the value in your Mikrotik, then it will ignore this option. This value represents the time interval in which Mikrotik sends accounting-update packets to the RADIUS server. For stable wired networks (FTTH/DSL) we recommend 2~4 minutes. For WISP, a 1 minute is recommended. The lower this number is, the higher the load will be put on the server.

default: 1 minute

Remote Control Method

Set the method in which SAS opens the tunnel for remote access. Remote access sometimes is needed so support personnel from Snono Systems can log in to the server from behind firewalls to provide the needed technical support. We recommend setting this option to SSH as it is more robust nowadays.

default: SSH

Lock Prepaid Cards To Owner

When enabled, prepaid cards generated from SAS will work only if the owner of the user (parent manager) is the same as the owner of the used card.

default: enabled

Disconnect On Activation

When enabled, SAS will disconnect the user session on service activation. We recommend always enabling this feature so users get their new attributes on service activation.

default: enabled

Disconnect On Update

When enabled, SAS will disconnect the user session on any update operation made on the user, such as changing profile, password, name...etc

default: enabled

Lock user MAC on Login

If enabled, the MAC login option will be set automatically for the user on dial-up. This might not work well with hotspots and modern phones if they have a random mac address feature enabled by default.

default: disabled

Reset User Traffic On Profile Change

This will ignore any remaining traffic in the user balance on activation. It will also reset it if the user has a negative data balance.

default: disabled

Radius Username Case Sensitivity

Determine if users can log in with usernames that ignore case sensitivity. If this feature is turned on, users must enter their username in the exact case as registered in the SAS database.

default: enabled

Accept Invalid Users

Allows invalid users trying to dial into the system to log in and go online. SAS will map the invalid logged-in user into an existing user which you chose. The mapped user should have enough simultaneous sessions to allow login for as many users as possible. This feature is useful for emergency cases where you want to allow any user to get connected, such as when losing the database and installing a fresh new system.

default: disabled

Limit User Activation via Reward Points/Month (times)

Some ISPs prefer to limit the number of times a user can be activated via reward points per month. A value of 0 means an unlimited number.

default: 0

Add Random Delay to User Authentication

This will add a random delay of 1~2 second for each dial-up request. It is a trick to prevent cheating on the system by some clients trying to log in multiple times using the same username. Usually, Freeradius will not catch users doing such a trick if they were fast enough, however, adding random delay will solve this issue without much of a delay to the actual process. Enable it only if you see multiple users online using the same account.

default: disabled

Manager Session Time

Set the number of hours for manager sessions in the admin portal.

default: 1 hour

Webhook Notifications

When enabled, SAS will send all system events happening in the admin portal to a URL of your choice. The provided URL shall receive HTTP POST with a JSON object holding the event data. This feature is very useful for integrating SAS with 3rd party systems such as ERP or accounting systems.

default: disabled

RouteGuard

This is very similar to Webhook, but this will send the event data before it happens in the backend. This feature is for very advanced system administrators. When enabled, you get to choose the URL to post your data to. The URL will receive the event data from the user interface before it reaches the backend.

default disabled

Revision #15
Created 14 June 2023 07:50:57 by Admin
Updated 15 June 2023 12:16:55 by Admin