ARPMiner

Installation & Configuration Guide
Version 3.4

Document Revision 2.5

https://www.kaplansoft.com/

ARPMiner is built by Yasin KAPLAN

Read "Readme.txt" for last minute changes and updates which can be found under application directory.

Table of Contents

Introduction

ARPMiner is a multi-purpose access control software runs under Windows *(Vista/7/810, 2008-2019 Server)*. Major features;

- Simple design and easy to use user interface.
- Simple interface for user definitions.
- Real time monitoring of connected users.
- NAT and bridge operation modes for HotSpot Captive Portal.
- PPPoE Server with MPPE *(40/128 bits)* Encryption.
- PAP, CHAP, MS-CHAP-v1 and MS-CHAP-v2 authentication methods.
- Built-in HTTP server with enhanced SSL and CGI/1.1 support, built-in DHCP server and DNS proxy.
- RADIUS AAA support *(Commercial editions only)*. ARPMiner accepts Packet of Disconnect *(PoD)* from RADIUS servers.
- Sponsored authorization *(Commercial editions only).*
- RADIUS MAC authentication.
- DNS redirection.
- Client Id *(Ethernet MAC address)* in DNS requests *(Experimental)*.
- WISPr authentication and partial RADIUS dictionary support.
- Customizable HTTP interface
- Performance monitoring through Windows Performance Monitor.

ARPMiner consists of a GUI and a service application called TekSpot. TekSpot has its own built-in PPPoE, HTTP, DHCP server and a proxy DNS server. TekSpot uses its built-in NAT engine.

RADIUS AAA and PPP encryption are supported in only SP edition.

System Requirements

- A Windows system *(Vista, 7, 8, 10, 2008-2016 Server)* with at least 2 GB of RAM.
- Microsoft.NET Framework 4.6.1.
- 8 MB of disk space for installation.
- One Ethernet interface for Private *(Hotspot)* zone and another for the Internet *(Public)* connection.
- Administrative privileges.
- You must have installed a packet driver prior to install ARPMiner. Such as;
  - https://nmap.org/npcap/ [1]
  - https://www.winpcap.org/
  - http://www.win10pcap.org/

[1] Npcap must be installed in Winpcap API compatible mode.

Installation

Unzip “ARPMiner.zip” and click “Setup.exe” comes with the distribution. Follow the instruction of setup wizard. Setup will install ARPMiner and TekSpot Service, add a shortcut for ARPMiner to desktop and the start menu.

Configuration

Run ARPMiner from Start Menu / Program Files / ARPMiner. ARPMiner automatically configures itself at first run.

Settings Tab

Click Settings Tab to start configuration. Settings tab has four sub sections. Enter following information:

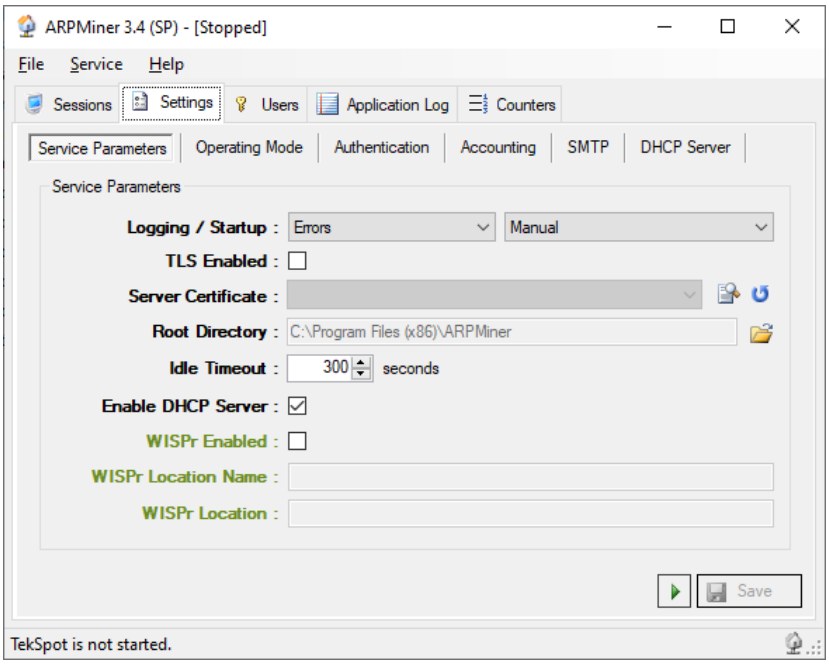


Figure - 1. ARPMiner Settings tab

- **Logging / Startup:** Select logging level of TekSpot. Select “None” if you do not want logging, select “Errors” to log errors and select “Sessions” to log session information and errors. Log files are located under <Application Directory>\Logs directory. Set TekSpot service startup mode, Manual or Automatic. You can also disable service startup.
- **TLS Enabled:** You can use HTTPS for HotSpot login form when you enable TLS. You must select a server certificate after enabling TLS.
- **Server Certificate:** Select server certificate for TLS.
- **Root Directory**: You can set directory where alternative login, info and error message html file resides. Please see User Defined Login Interface section of this manual.
- **Idle Timeout:** Set idle timeout in seconds. User will be assumed offline after this amount of time if no network activity occurs.

- **Enable DHCP Server:** Set this option if you prefer to use built-in DHCP server of ARPMiner. The DHCP server automatically assigns IP addresses to all wired or wireless devices from the IP address pool of in the DHCP Server tab.
- **WISPr Enable:** You can enable WISPr authentication by setting this option. ARPMiner will add WISPr-Location-ID and WISPr-Location-Name to RADIUS accounting requests.
- **WISPr Location Name:** Enter a descriptive name for HotSpot location**.**
- **WISPr Location:** Enter a description for HotSpot location**.**

Address Translation Tab

Click Address Translation Tab to configure Internet connection and Private Network *(Wireless e.g.)* connection interface. ARPMiner supports three modes of operation for access control; Network Address Translation *(NAT)*, bridge mode and PPPoE server mode.

Network Address Translation, NAT *(Routed)* Operation Mode

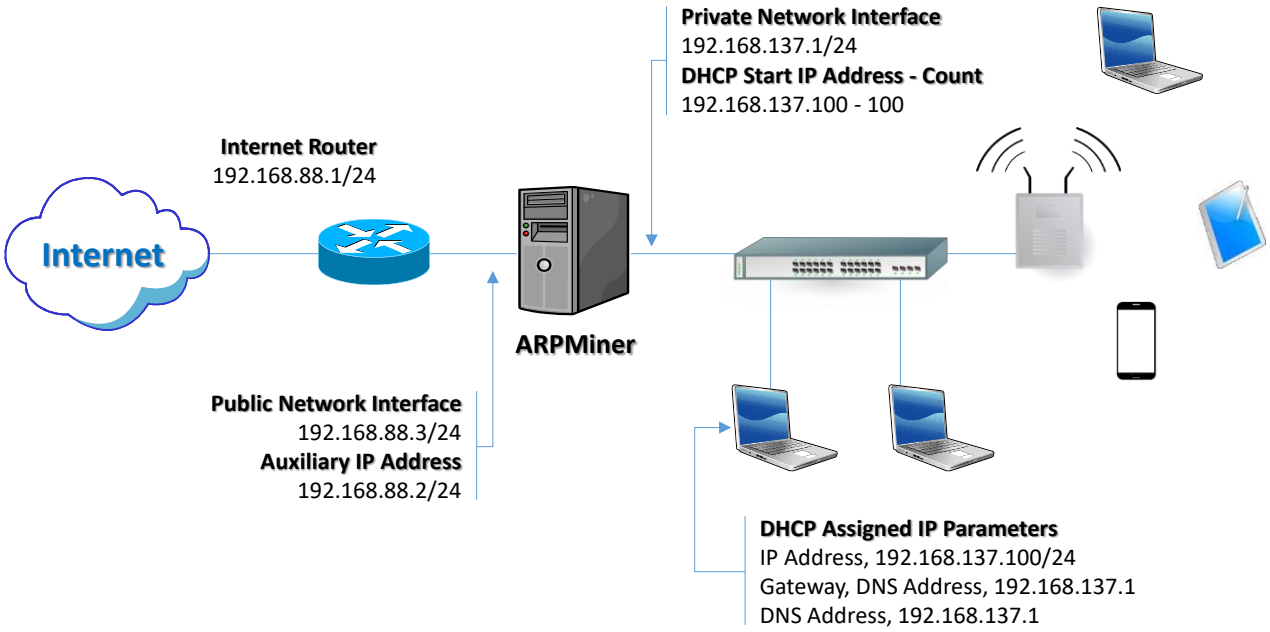


Figure - 2. Sample NAT *(Routed)* Configuration

ARPMiner will translate source IP address and port number *(Port translation is performed when it's needed, ARPMiner performs symmetric NAT by default)* while forwarding a packet from Private Network to the Internet. ARPMiner will stop Windows Internet Connection Sharing *(ICS)* at startup if it is enabled. Please also make sure that IP routing is disabled on ARPMiner installed machine.

ARPMiner uses an Auxiliary IP address *(192.168.88.2/24 in the example above)* for IP address translation on the Public Network side. Windows machine would reject return packets from the Internet if the translation was performed using public interface IP address *(192.168.88.3/24 in the example above)*.

Auxiliary IP address is chosen automatically but you can also set it manually. You must set it to an IP address which is not used in the public network when you set it manually for proper operation.

Built-in DHCP server deployment is optional. Built-in DHCP server will assign an IP address from its IP pool to the client on the private network *(Either wireless or wired)*. Assigned IP subnet mask will be the same with the Private Interface of the ARPMiner installed machine. DNS server and gateway IP address will be assigned as the Private Network IP address of the ARPMiner running machine.

You must set gateway IP address as the Private Network IP address of the ARPMiner running machine and set a DHCP IP pool range with same subnet of the IP address as the Private Network IP address when you choose to use an external DHCP server on the private network.

ARPMiner allows you set private interface IP address and subnet mask directly from the management interface. IP address and subnet mask of interface will be changed at operating system level when you save the settings changes in ARPMiner.

Bridge Operation Mode

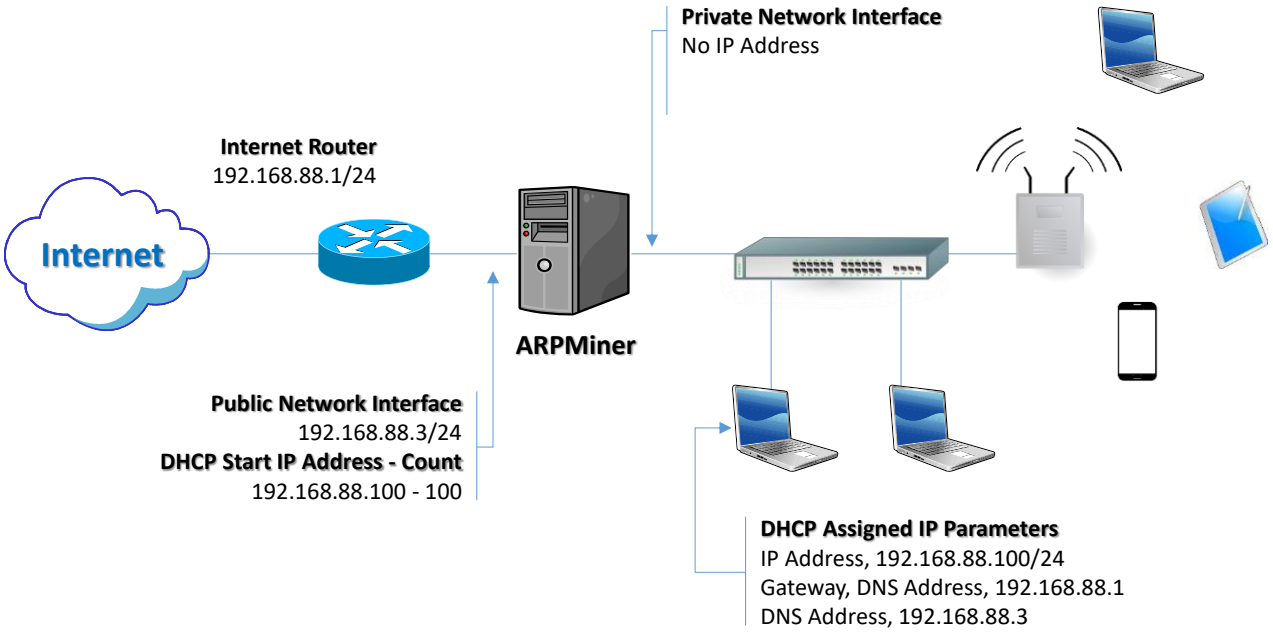


Figure - 3. Bridge Mode Configuration

ARPMiner acts as a bridge in bridge operation mode. ARPMiner transparently performs packet forwarding between public and private networks and maintains its own MAC address table for the private network.

This operation mode enables you to perform access control for the private network without any topology change in your network. NAT should be performed by the Internet router if it's needed. You do not need to assign an IP address to the private network interface of ARPMiner installed machine and ARPMiner will reset private interface IP address to an IP address in 169.254.0.0/16 subnet automatically when this operation mode is set.

Built-in DHCP server deployment is also optional in this operation mode. Built-in DHCP server will assign an IP address from its IP pool to the client on the private network *(Either wireless or wired)*. Assigned IP subnet mask will be the same with the Public Interface of the ARPMiner installed machine. DNS server as the Public Network IP address of the ARPMiner running machine and Gateway as the default gateway of the ARPMiner running machine will be assigned to the DHCP clients.

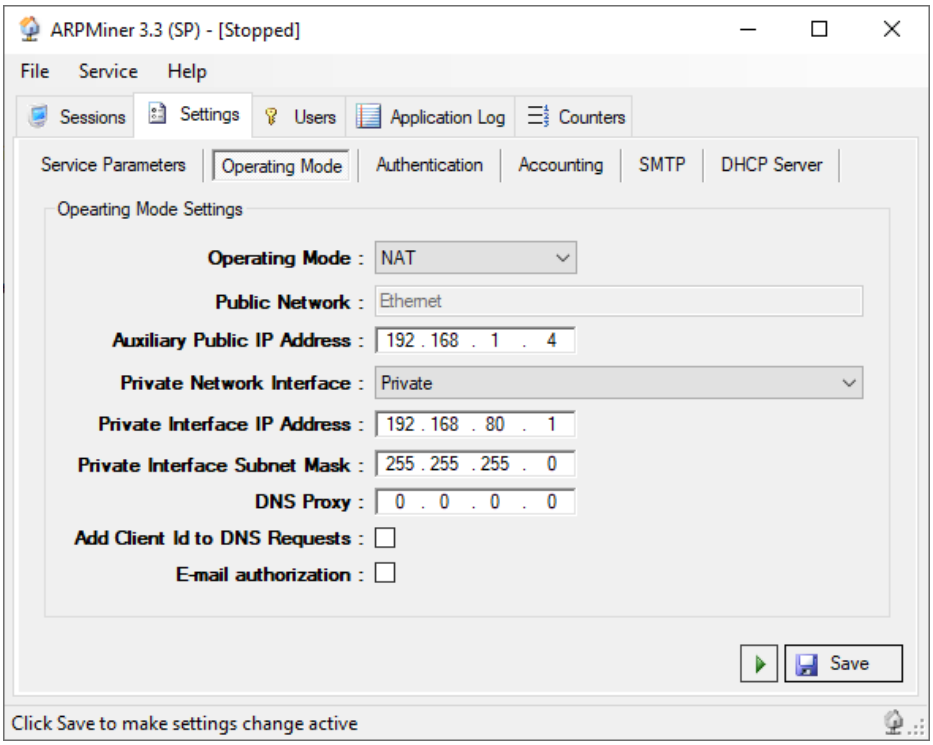


Figure - 4. ARPMiner Settings / Operating Mode tab

ARPMiner will stop Windows Internet Connection Sharing *(ICS)* at startup if it is enabled. Please also make sure that IP routing is disabled on ARPMiner installed machine.

You can redirect all DNS requests from clients to a specific DNS server. Leave Proxy DNS set to 0.0.0.0 if you do not use this option. ARPMiner can add client Ethernet MAC address as client id to DNS requests from clients. This feature is experimental and its usage is not recommended currently.

You can enable Sponsored Authorization allow HotSpot users to request access from a corporate employee via e-mail. ARPMiner sends a request for access on behalf user to user specified sponsor e-mail address. Please see Sponsored Authorization section for more details. You need also configure an SMTP account in SMTP tab for this feature. Local or RADIUS authentication will not be used when this feature is enabled. This feature can be used only with NAT and Bridge operating modes.

PPPoE Server Operation Mode

ARPMiner does not perform Network or MAC address translation in PPPoE Server Operation Mode. TekRADIUS authenticates user sessions using PAP, CHAP, MS-CHAP-v1 or MS-CHAP-v2 authentication methods based on client preference. MS-CHAP-v1 or MS-CHAP-v2 must be set as authentication method in client settings for MPPE encryption. Encryption level *(40/128 bits)* is also determined by either client settings or MS-MPPE-Encryption-Types attribute received in RADIUS authorization response.

Authentication Tab

Authentication is enabled by default and ARPMiner uses built database to keep user accounts. SP license of ARPMiner provides RADIUS authentication. Please also see supported RADIUS attributes section.

- **Encrypt Passwords:** Set this option to keep the endpoint passwords in encrypted form in SQLite database TekSpot.db3 under ARPMiner application directory.
- **Blacklist IP Endpoints:** If selected, ARPMiner monitors failed login attempts from suspicious endpoints and blacklists them.
- **Cache Sessions:** ARPMiner can cache user credentials for a specified period. ARPMiner will auto provide login if client browser submits a valid HTTP cookie.
- **PPP Encryption:** Click to enable PPP *(MPPE)* encryption. PPP encryption will be used based on client preference.
- **Use RADIUS:** If you prefer to direct authentication requests to a RADIUS Server, check this option. If you do not check this option, TekSpot will use the local users database to authenticate the login attempts.
- **RADIUS Server:** Enter a valid IPv4 address for the RADIUS server.
- **RADIUS Port:** Enter the UDP port number of the RADIUS server. Default is UDP port 1813.
- **RADIUS Secret:** Enter the RADIUS secret key for the RADIUS Server.
- **RADIUS Timeout / Retry:** You can set an amount of time which TekSpot waits for a reply for the RADIUS accounting packets from the RADIUS Server. You can also specify how many attempts will be made by TekSpot to deliver RADIUS accounting packets to the RADIUS server.
- **MAC Authentication:** ARPMiner can bypass portal login for specific MAC addresses. You need to have user profiles in your RADIUS server for these MAC addresses without a password. Please make sure that you have anti-spoofing measures deployed on your network prior to enable this option.

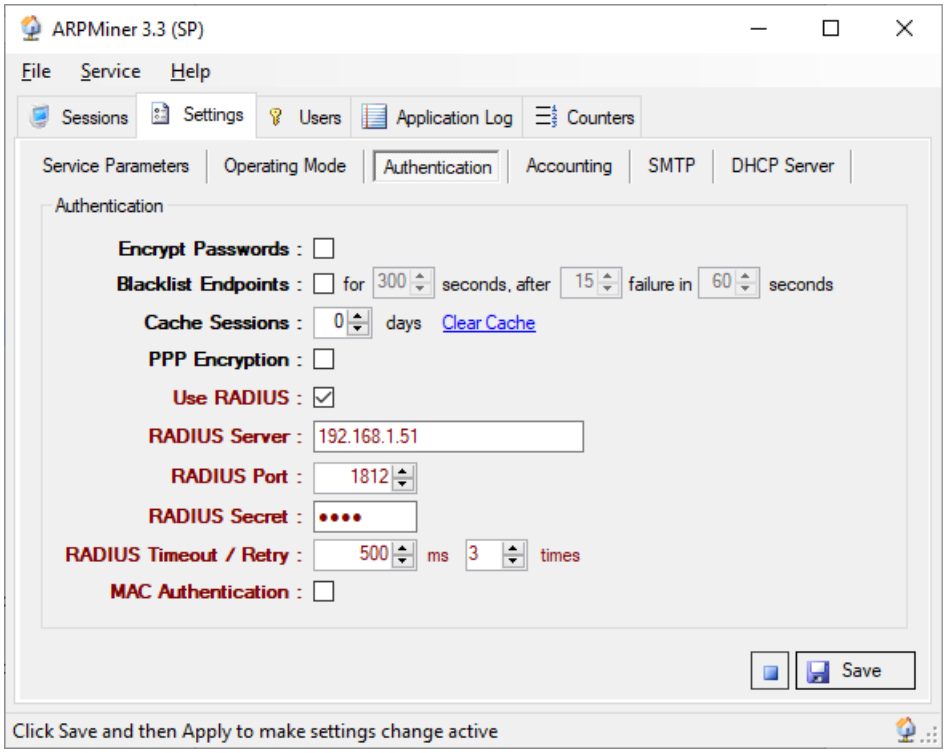


Figure - 5. ARPMiner Settings / Authentication tab

Accounting Tab

Accounting is available in only SP editions of ARPMiner. Please also see supported RADIUS attributes section

- **Accounting Enabled:** RADIUS accounting is disabled by default. Click "Accounting Enabled" to enable RADIUS accounting.
- **Stop Only:** If you prefer to send only RADIUS Accounting stop messages to the RADIUS server, select this option.
- **RADIUS Server:** Enter a valid IPv4 address for the RADIUS server.
- **RADIUS Port:** Enter the UDP port number of the RADIUS server. Default is UDP port 1813.
- **RADIUS Secret:** Enter the RADIUS secret key for the RADIUS Server.
- **RADIUS Timeout / Retry:** You can set an amount of time which TekSpot waits for a reply for the RADIUS accounting packets from the RADIUS Server. You can also specify how many attempts will be made by TekSpot to deliver RADIUS accounting packets to the RADIUS server.

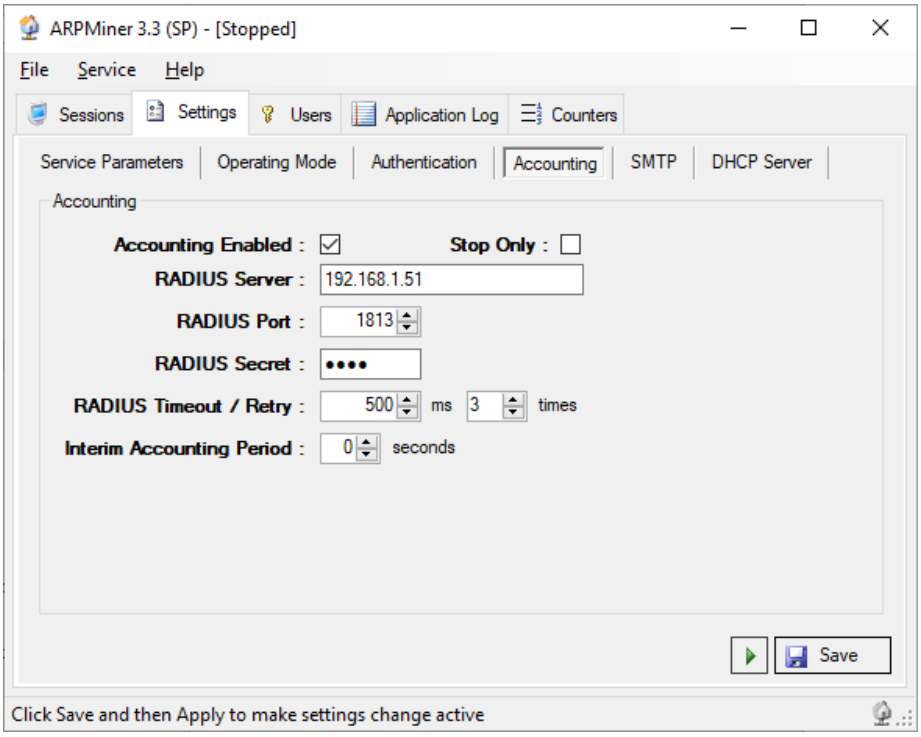


Figure - 6. ARPMiner Settings / Accounting tab

SMTP Tab

SMTP settings are required for Sponsored Authorization. It is recommended to create a special SMTP account for ARPMiner authorization messages. ARPMiner sends authorization messages using the account specified in **Mail From** parameter. You can test SMTP settings prior to save settings.

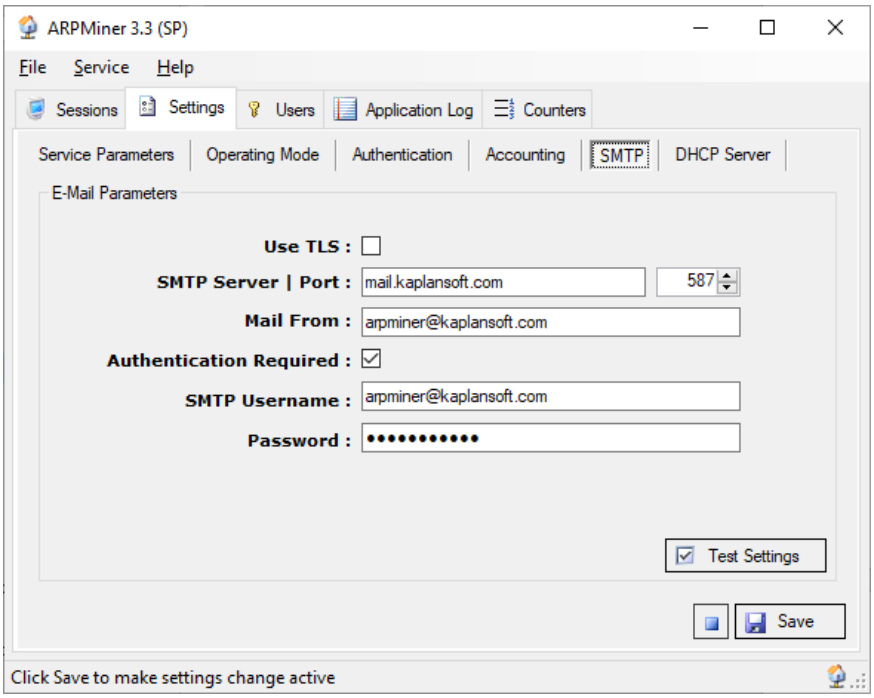


Figure 7. - ARPMiner Settings / DHCP Server tab

DHCP Server

ARPMiner has a built-in DHCP server to assign IP addresses to the wired or wireless devices on the private network, and accessed via the **DHCP Server** tab. Within this tab, it is possible to define a DHCP IP address pool, and monitor IP address usage and active DHCP assignments.

! *The **DHCP** tab is only available if the DHCP server has been enabled in the **Settings / Service Parameters** tab.*

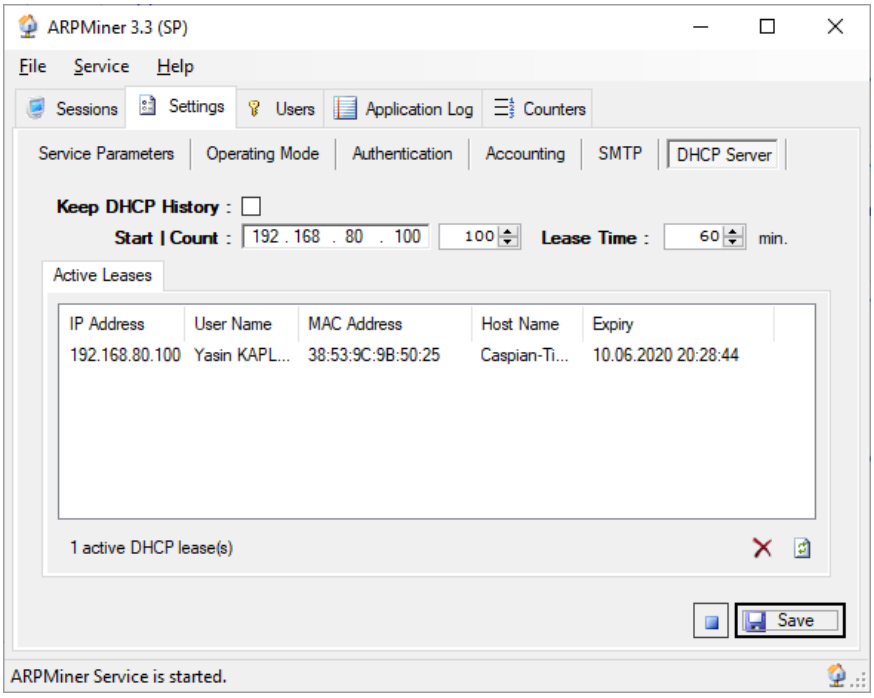


Figure 8. - ARPMiner Settings / DHCP Server tab

Counters

ARPMiner provides numerous counters to monitor activity performed.

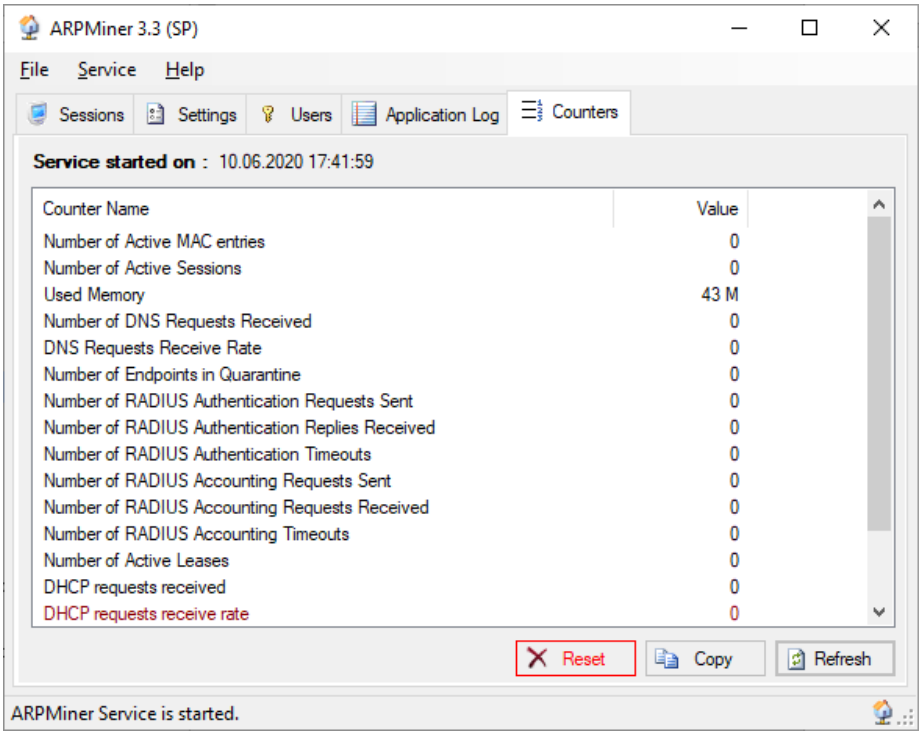


Figure 9. - ARPMiner Settings / Counters tab

ARPMiner provides numerous counters:

- Number of Active MAC entries
- Number of Active Sessions
- Used Memory
- Number of DNS Requests Received
- DNS Requests Receive Rate
- Number of Endpoints in Quarantine
- Number of RADIUS Authentication Requests Sent
- Number of RADIUS Authentication Replies Received
- Number of RADIUS Authentication Timeouts
- Number of RADIUS Accounting Requests Sent
- Number of RADIUS Accounting Requests Received
- Number of RADIUS Accounting Timeouts
- DHCP requests received
- Number of Active Leases
- DHCP requests receive rate
- DHCP errors
- DHCP errors rate

These counters can also be monitored through ARPMiner within the **Counters** tab.

Users

You can define users in “Users” tab. Enter a username in the bottom leftmost textbox, enter the password to the textbox at the right of the username entry and a session duration in seconds. Idle timeout is 5 minutes and it cannot be changed.

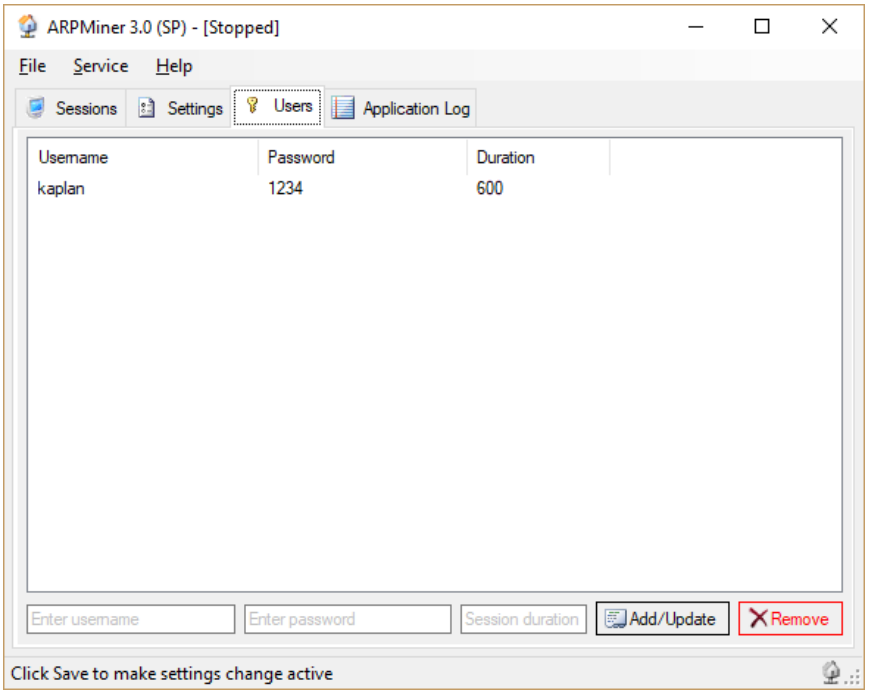


Figure - 10. Users Tab

Application Log

You can monitor system events in Application Log tab. You can manually refresh log entries and clear log entries. Click Enable Auto Refresh option to refresh log list every second.

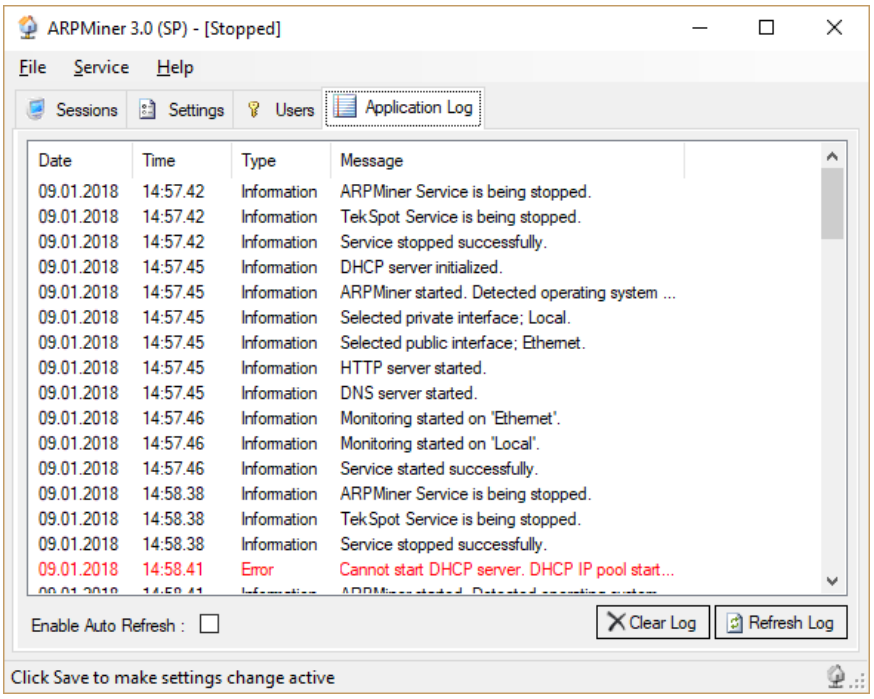


Figure – 11. Application Log Tab

User Defined Login Interface

You can use your own defined login, info and error pages. ARPMiner uses built in html resources for these pages. ARPMiner looks for alternative login.html, info.html and error.html files in the **Root Directory** specified in Settings / Service Parameters. If any of them found, ARPMiner uses user defined html file. Login.html must have following form and form objects;

```
<form name="LoginForm" method="post" action="tslogin" id="HotSpotLoginForm">
<input name="Username" type="Text" id="Username">
<input name="Password" type="Password" id="Password">
<input type="submit" name="Login" value="Login" id="Login">
```

You can display user's connection date and remained credit by adding `%connected%` and `%remained%` variables to info.html. You can optionally add `%url%` variable if you would like to provide an option user to continue web browsing. TekSpot will replace last tried URL with `%url%` variable in info.html. TekSpot will replace real values of these variables prior to send html response.

You can display TekSpot generated error message in error.html file using `%message%` variable.

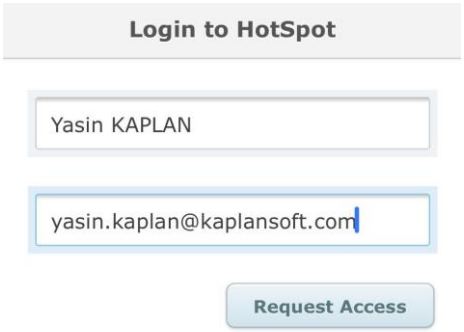
Here is a sample login.html;

```
<html>
<head>
    <title>HotSpot Login</title>
</head>
<body style="font-size: 12px; font-family: Arial">
    <form name="LoginForm" method="post" action="tslogin" id="HotSpotLoginForm">
        <table id="FormTable border="2" style="color: black;
            background-color: lightgray; border-color: lightgray; border-collapse: collapse;">
            <tr style="color: White; background-color: Navy; border-color: lightgray;">
                <td colspan="2">
                    <b>HotSpot Login%message%</b></td>
            </tr>
            <tr style="background-color: lightgray; border-color: lightgray;>
                <td colspan="2" style="background-color: lightgray; border-color: lightgray;">
                    <font size="1px"> </font></td>
            </tr>
            <tr style="background-color: lightgray; border-color: lightgray;">
                <td align="right" style="background-color: lightgray; border-color: lightgray;>
                    <b>Username : </b>
                </td>
                <td style="background-color: lightgray; border-color: lightgray; width: 141px">
                    <input name="Username" type="Text" id="Username" style="width: 200px;" /></td>
            </tr>
            <tr style="background-color: lightgray; border-color: lightgray;">
                <td align="right" style="background-color: lightgray; border-color: lightgray;>
                    <b>Password : </b>
                </td>
                <td style="background-color: lightgray; border-color: lightgray; width: 141px">
                    <input name="Password" type="Password" id="Password" style="width: 200px;" />
                    <input name="Host" type="hidden" value="%url%" /></td>
            </tr>
            <tr style="background-color: lightgray; border-color: lightgray;">
                <td style="background-color: lightgray; border-color: lightgray;>
                     </td>
                <td align="right" style="background-color: lightgray; border-color: lightgray;>
                    <input type="submit" name="Login" value="Login" id="Login" /> </td>
            </tr>
        </table>
    </form>
    <br />
</body>
</html>
```

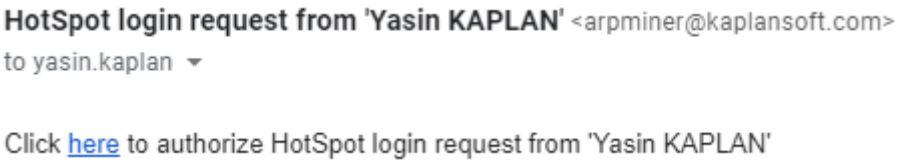
You can also run CGI scripts *(.php, .pl, .bat, .vbs, etc.)* placed in HTTP root directory of ARPMiner.

Sponsored Authorization

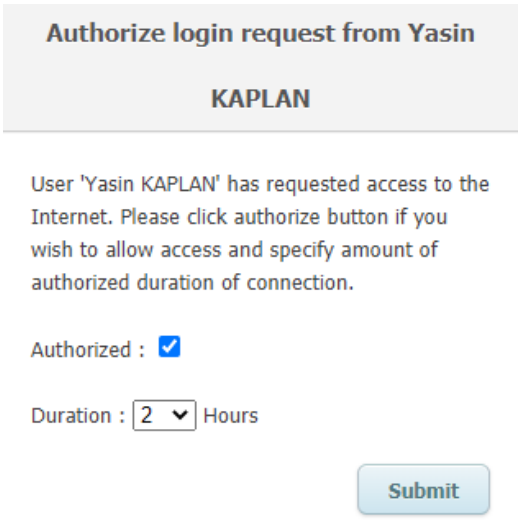
When Sponsored Authorization enabled ARPMiner requests access request on behalf of HotSpot users by sending an e-mail to sponsor e-mail address specified by the user when HotSpot login form is displayed;



ARPMiner sends authorization message to sponsor as soon as the user clicks **Request Access** button;



Sponsor clicks in the e-mail message and an authorization form is displayed;



Sponsor can deny by simply clicking **Submit** button without setting Authorized option. Sponsor can select authorized amount of session duration up to 24 hours in hourly steps.

You can use your own defined login, info and sponsor pages. ARPMiner uses built in html resources for these pages. ARPMiner looks for alternative sponsored-login.html, sponsored-info.html and sponsored-authorize.html files in the **Root Directory** specified in Settings / Service Parameters. You can download sample html resources from;

http://www.kaplansoft.com/arpminer/html-samples.zip

Supported RADIUS Attributes

ARPMiner RADIUS authentication request packet contains following RADIUS attributes;

- User-Name
- User-Password or CHAP-Password
- NAS-IP-Address
- Called-Station-Id
- Calling-Station-Id *(User Ethernet MAC address)*

ARPMiner expects following RADIUS attributes in an Access-Accept reply;

- Session-Timeout
- Idle-Timeout

ARPMiner RADIUS accounting start packets contains following RADIUS attributes;

- Acct-Status-Type = Start
- Calling-Station-Id
- Called-Station-Id
- Framed-IP-Address
- NAS-IP-Address
- Acct-Session-Id
- User-Name
- Connect-Info *(Added only when sponsored authorization is enabled. It reports sponsor e-mail address)*

ARPMiner recognizes following RADIUS attributes in PPPoE Server Operation Mode;

- MS-MPPE-Encryption-Types
- MS-CHAP2-Success
- MS-CHAP-MPPE-Keys
- MS-MPPE-Send-Key
- MS-MPPE-Recv-Key
- MS-Primary-DNS-Server
- MS-Secondary-DNS-Server
- MS-Primary-NBNS-Server
- MS-Secondary-NBNS-Server

ARPMiner RADIUS accounting stop packets contains following RADIUS attributes;

- Acct-Status-Type = Stop
- Acct-Terminate-Cause
- Acct-Session-Time
- Calling-Station-Id
- Called-Station-Id
- Framed-IP-Address

- NAS-IP-Address
- Acct-Input-Octets
- Acct-Output-Octets
- Acct-Session-Id
- User-Name
- Connect-Info *(Added only when sponsored authorization is enabled. It reports sponsor e-mail address)*

Starting ARPMiner Service (TekSpot)

Click "Service" menu and select "Start" to run ARPMiner Service after making necessary configuration and saving configuration. If service starts successfully you will see "TekSpot is started" message at bottom left message section of ARPMiner. Optionally you can start/stop TekSpot using the button on Settings tab. When you make any change(s) in configuration, TekSpot will be restarted when you save the settings.

If TekSpot cannot start, please examine Application Log tab as well as TekSpot log file under <Application Directory>\Logs if you were enabled logging in Settings tab.

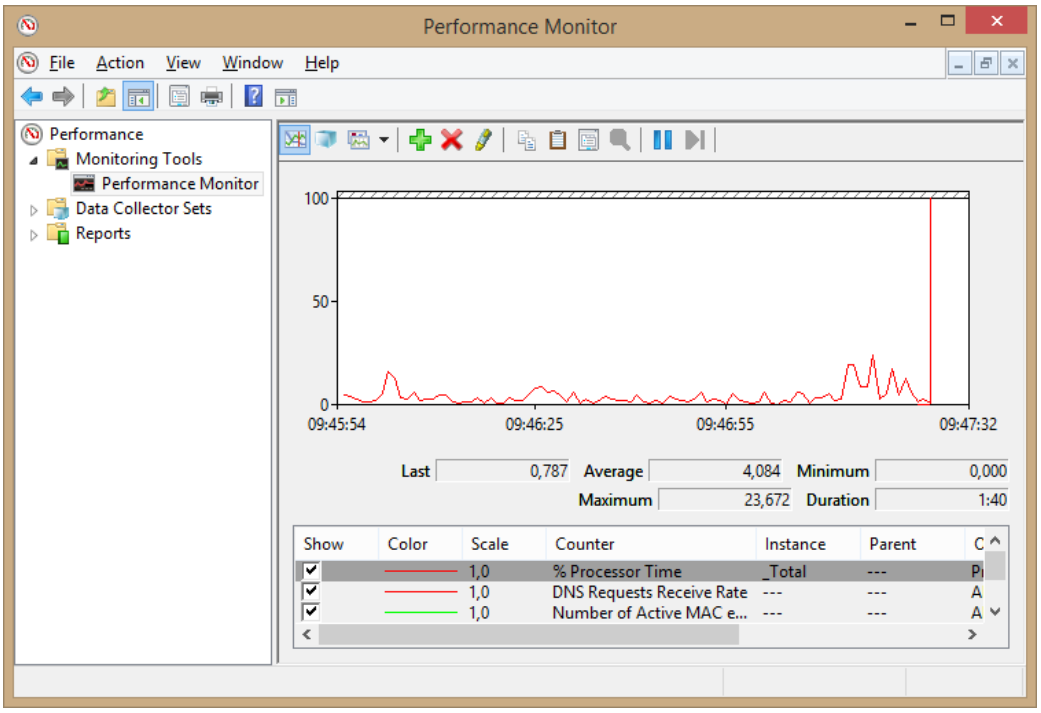


Figure - 12. TekSpot on Windows Performance Monitor

Troubleshooting

TekSpot provides many messages when problems occur. You can see error messages on ARPMiner Status bar or in the log file of TekSpot service. You can enable logging in Settings Tab. There are three levels of logging; None, Errors, Sessions. If you select Errors, TekSpot logs just error messages. If you select Sessions both Session and Error messages will be logged. You have to save or apply settings changes if you change logging level setting. Log files are located under <Application Directory>\Logs directory.

TekSpot Messages in TekSpot logs

ARPMiner Service x.y.0.0 (Revision 0) is being started (<Windows version>).

This message notifies that TekSpot is being started.

Registration Key is valid; running in commercial mode.

You see this message when a valid Registration.key file exists under ARPMiner application directory.

User defined login form read into memory

You see this message when a valid user defined login form html file exists under Root Directory.

Cannot obtain an auxiliary external IP address

ARPMiner requires an auxiliary IP address for the NAT operation mode. ARPMiner service cannot start if it cannot obtain a suitable address.

Index