Allmon2
Allstar Monitoring and Managing Tool
by Tim Sawyer, WD6AWP

Allmon2 is web server software for monitoring and managing AllStar/app_rpt nodes and RTCM devices. It provides a real-time view of connected nodes which is dynamically updated as links connect, disconnect and transmit.

Currently transmitting nodes are highlighted with a green background. Connecting nodes are highlighted with an orange background. Transmitting nodes are moved to the top of the list so you always know which node last keyed your system. The RTCM capabilities of Allmon2 provide a live view of the signal strength of each receiver in your system.

Logged in users have additional capabilities including the ability to connect, disconnect, monitor or monitor local nodes and operate the control panel.

The control panel can do anything that can be done from the Asterisk client (CLI). That may even include sending commands to your node for which there is no touch tone equivalent thus providing an additional level of security for sensitive commands. The Allmon control panel comes with a set of default commands. You can add or subtract to those as you wish via INI settings.

Allmon2 can be run on a web server to monitor and control one or more remote AllStar/app_rpt systems.

Allmon2 is open source software and available from https://github.com/tsawyer/allmon2

Allmon2 is pre-installed on all hamvoip Raspberry Pi 2/3 images

Here are the instructions on how to configure it on the RPi2/3 systems.

1. Create a password for Allmon to login to the Asterisk Manager

Enter the /etc/asterisk directory

cd /etc/asterisk

Edit the manager.conf file

nano manager.conf

Add a secure password where it shows 'secret =' under the [admin] stanza, for example:

secret = iad1og3carb7e

Restart asterisk.

    astres.sh

2. Configure Allmon with your node number and Asterisk Manager password

Change to the allmon2 directory

    cd /srv/http/allmon2

Edit the allmon.ini.php file

    nano allmon.ini.php

Change the xxxxx to your node number. Also change the passwd= line and replace password2 with the password your chose in step 1.

3. Create a password for users to login to Allmon

Change to the allmon2 directory if not already there.

    cd into /srv/http/allmon2

Add an htpasswd file

    htpasswd -cB .htpasswd <userID>

Supply a password of your choice when prompted. Use a secure password including upper/lower alpha, numeric, and special characters. Security is important!

<userID> is the login ID and can be any username you would like to assign; your callsign or admin for example.

You can even have more than one login and password. If assigning additional passwords the 'c' create file switch must be dropped. In this case use:

    htpasswd -B .htpasswd <userID>

To start Allmon in your browser enter your server's IP address/allmon2 in the address bar. If your servers IP address was 192.168.1.100 then:

http://192.168.1.100/allmon2

The local database used by Allmon2 (and lsnodes) is updated once daily at a random time between 3:15 and 3:45 AM to avoid server overload. If node information changes it will not be displayed until the next 24 hour update. To manually update the local database execute the 'astdb.php' command manually at the Linux prompt. Please limit updates to avoid server overload.

Possible errors and pitfalls

"Could not connect to Asterisk manger" generally means the ID and password in /srv/http/allmon2/allmon.ini.php does not match the ID and password in /etc/asterisk/manager.conf. Make sure they match and restart Asterisk.

The default AMI configuration (/etc/asterisk/manager.conf) is to **NOT** allow network connections. **When opened to the Internet Asterisk AMI has been known to be a security risk.** Unless you understand the risks and how to configure remote connections please leave the IP address in /etc/asterisk/manager.conf and in /srv/http/allmon2/allmon.ini.php at 127.0.0.1 when you are running Allmon locally.

3/20/17 – Updated to change encryption type to Blowfish (-B) when using htpasswd.
5/12/2017 – corrected spelling error of htpasswd