The

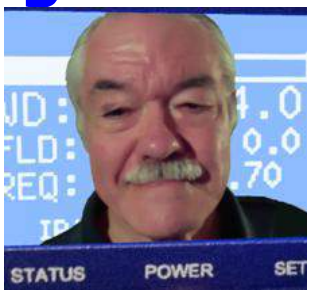
Broadcasters' Desktop Resource

www.theBDR.net

... edited by Barry Mishkind – the Eclectic Engineer

Tech Tip

Using The Sage ENDEC White List



By Dave Kline

[May 2020] Ensuring that all mission critical equipment stays secure is important. A few weeks ago, someone posted hundreds of IP addresses for EAS boxes, harvested from the Shodan site. Dave Kline took the opportunity to review his EAS box security.

The FCC recently issued an advisory about securing EAS equipment connected to the Internet.

This was a timely posting as I was dealing with some potential issues of my own.

During that process I ran across a feature on the Sage EN-DEC that was included with the V95 upgrade. This allows you to white-list devices for acces-sing the web interface of your ENDEC.

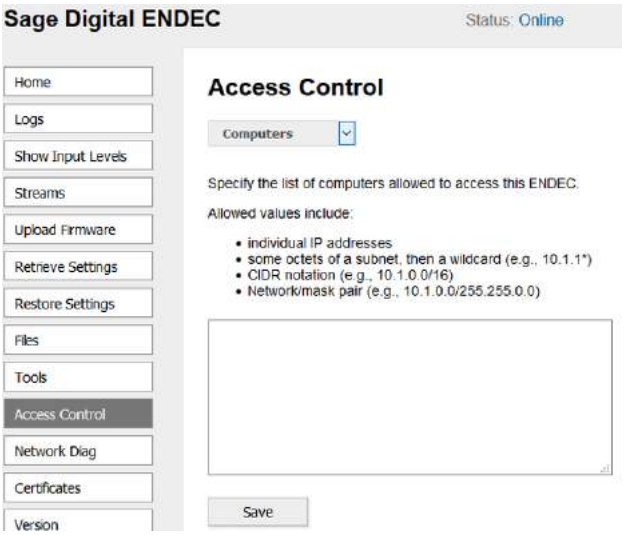
The V95 release notes mention this briefly: "You can also use the access control dropdown box to set a white list of IP addresses that can connect to the ENDECs web page."

WHITELISTING ACCESS

The fact that I could easily do this is testament to its simplicity. (In any room, I am the last guy you want to call on to answer IT questions.)

Here is the drill:

- Log in to your ENDEC as the admin. (You did change the default user name and password, right?)
- On the left side of the screen click on the ACCESS CONTROL button.
- Then using the pull-down menu at the top of the screen, select COMPUTERS.
- A blank box will appear with some in-structtions about formatting your entries.



The Sage Access Control Screen

Using this screen, I added the IP address for the computer at the studio that is on the same LAN as the ENDEC.

NO OUTSIDE ACCESS

Once I did this, my Sage blocked any web GUI access from other computers.

To test it, I tried logging in from home. This has always worked in the past, but not any longer. I can still get to my Sage from remote locations by logging in to the local computer first. It is a bit more trouble for me, but worth it.

I would suggest to those who are more proficient at IT stuff, to investigate the other options of this feature. I assume they provide more flexibility while helping to keep some of the bad guys out.
Also, this should not be your only measure to lock down your gear. Proper firewalls and all that other juicy IT stuff, of which I know very little, are advised.

For someone like me however, this seems like a good start.

- - -

Dave Kline, is an engineer at KVNO / University of Nebraska at Omaha. You can contact Dave at: dkline@unomaha.edu

- - -

Has this article been of value to you? The one-time-a-week BDR Newsletter is designed to let you know when more are posted. You are invited to subscribe: takes just 30 seconds if you click here.

- - -

- - -

Return to The BDR Menu