Tvheadend - Feature #5796

Disable WEB UI from IP except allowed list

2019-12-20 10:58 - saen acro

Status:	New	**Start date:**	2019-12-20
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:	User Interface	**Estimated time:**	0.00 hour
Target version:			

Description

Option is needed to disable brute-force attacks.
Independent from user profile IP access.

Eventual workaround is different from standard :9981 just for administration.
Not shure with one is easy to implement.

History

#1 - 2019-12-20 12:02 - Flole Systems

Fail2Ban would be the better way to prevent bruteforce attacks in my opinion.

#2 - 2019-12-20 12:30 - saen acro

Example?

#3 - 2019-12-20 15:09 - Flole Systems

Download Fail2Ban, install it, configure it, add a "authentication failed from x.x.x.x" log entry to tvheadend, done.

#4 - 2019-12-20 15:33 - saen acro

Not secure for stolen credentials.

#5 - 2019-12-20 15:55 - Flole Systems

You wrote that wanted to prevent bruteforce attacks though, you never mentioned that stolen credentials are a problem for you aswell. Iptables is your friend for that though.

#6 - 2019-12-20 18:45 - saen acro

let's patch will be practical why need to allow possible doors to unwanted person.
In your scenario even you will ban yourself with wrong entered credentials.

about stolen credentials
its easy to download full playlist with credentials from single channel.

#7 - 2019-12-20 20:17 - Flole Systems

So you just want to limit a user to a specific IP or IP Range? That's already possible if I remember correctly.

#8 - 2019-12-20 20:26 - saen acro

Flole Systems wrote:

> So you just want to limit a user to a specific IP or IP Range? That's already possible if I remember correctly.

No I want to disable ADMIN UI globaly aka access to "extjs.html" and allow allow acces to admin ip range ONLY
Problem is that HTTP admin UI and streamer are on same port :9981

When some one open
http:/tvh.ip:9981
not to receive credentials window, except when his ip is in allowed ip-s.

#9 - 2019-12-20 20:39 - Flole Systems

So you can just limit all your admin/webui users to the list of allowed IPs. They will still see the window but it doesn't matter what they enter they won't get access.

#10 - 2019-12-22 10:22 - kodiaq kodiaq

+1 - Anyone can access WEB UI on port 9981 than log in without being noticed by admin, because there is no information being logged in the tvh.log file.

Simply there is currently no "traceability" of who accessed the WEB UI on port 9981 and this opens door for various speculations...

#11 - 2019-12-22 12:06 - Flole Systems

The feature already exists, so no need to +1....

#12 - 2019-12-22 12:42 - saen acro

Flole Systems wrote:

> The feature already exists, so no need to +1....

Explain where it exists?
pictures video etc.

on individual user can be disabled web ui but it must be reversed.
if TVH have public ip anyone can see login credentials form.

#13 - 2019-12-22 13:30 - Flole Systems

You really need all information spoon fed.... It's literally the first result on Google if you would search for it.

Anyways: See https://docs.tvheadend.org/webui/config_access/

There is even an example to only allow admin access from LAN.

#14 - 2019-12-22 14:21 - saen acro

Are you realy try to understand request I started?

In you suggesting i need to add 0.0.0.0/0,:0/0 to user "*" and bloch access?
it not work
User A can see from IP 10.11.12.13/32
but his ip is dinamical and next time can't access

next suggestion will be "IP Blocking Record's"
cool ic can enter ~8500 /22 records to ban China access

so many solution not to block few simple links

```
extjs.html
/playlist
/xmltv
```

user can be happy with

```
/stream
```

only
rest use :9982

#15 - 2019-12-22 14:30 - Flole Systems

Please read the page again, including the examples, I am not going to spoon feed the solution to you, a little bit of effort on your side can be expected, especially if it's just reading a wiki page (or just scrolling down to the examples and reading those). I never suggested what you tried, you clearly didn't read the page. The functionality to limit a users access to a list of IPs or IP Ranges is already there, so there is nothing that needs to be implemented.

#16 - 2019-12-22 19:41 - kodiaq kodiaq

@saen acro - Do you mean to have possibility to disable initial "credential prompt" sequence from WEB UI for anonymous IP? Do I get it right?

#17 - 2019-12-23 09:14 - Pablo R.

It is not related, but it would be interesting to separate the webui from the channel urls. In different ports, for security.

#18 - 2019-12-23 09:50 - saen acro

kodiaq kodiaq wrote:

> @saen acro - Do you mean to have possibility to disable initial "credential prompt" sequence from WEB UI for anonymous IP? Do I get it right?

Not in allowed list no access to admin part,
not as now check in user profile to disable UI

Pablo R. wrote:

> It is not related, but it would be interesting to separate the webui from the channel urls. In different ports, for security.

This is a part of request, it will be best if is possible to set own port.

#19 - 2019-12-23 15:02 - Flole Systems

saen acro wrote:

> Not in allowed list no access to admin part,
> not as now check in user profile to disable UI

This feature already exists! Just read the wiki and configure it.... It might need configuration for each admin user but since this gives even more flexibility and security that's even better.

#20 - 2019-12-23 15:14 - saen acro

Flole Systems wrote:

> saen acro wrote:
>
> > Not in allowed list no access to admin part,
> > not as now check in user profile to disable UI
>
> This feature already exists! Just read the wiki and configure it.... It might need configuration for each admin user but since this gives even more flexibility and security that's even better.

This function work for user **A** user **B** can access.
Also to work credentials needed.

Wizard second step wink.png

#21 - 2019-12-23 15:31 - Flole Systems

You need to define it for all users that have access to the Web UI of course. This allows giving each admin access from different ranges aswell, which is superior to your request.

#22 - 2019-12-23 15:52 - saen acro

ok am bad gui wit know ip:port of you service
frite script to curl 1000 times per second your service
what is your solution

A. firewall
not possible without strict L7 rule
B. firewall with addresses range
client will not see service if its out of allowed range (mobile operator roaming etc)
C. NGINX
not so simple, need powerful pc

D. run vpn concentrator and do it as you suggest.

#23 - 2019-12-23 17:55 - Flole Systems

So you are trying to mitigate a DOS attack here? In that case an IDS/IPS is the right choice. Or sign up for cloudflare and have them take care of it. Or configure fail2ban. Or super simple: A rate limit iptables rule. Think of your own solutions instead of having someone else spoon feed you.

Originally you wanted to limit access to the Webinterface to a specific IP or a range of IPs, which is already possible. You keep coming up with

different scenarios which might cause problems, but those problems are completely out of scope of tvheadend, we can't implement a DOS protection and all that kind of stuff, that should not be part of tvheadend (just like Apache doesn't have it and just like nginx doesn't have it and just like openssh doesn't have it and so on).

#24 - 2019-12-23 18:32 - saen acro

Am writing slow to understand
Inversion of current function of access is enough
its blocked to all and allowed to accept list

Same as bsd and linux firewall by default
one allow all other block all by default inverted idea both do same at all.

#25 - 2019-12-23 19:18 - Flole Systems

Again, the feature to limit a users access to a specific IP is already there. Default is allow all but you can also specify a list of IPs and IP Ranges (or both). I already spoon fed you the exact doc page that describes exactly what you want to do as an example. What else should I do to help you?

#26 - 2019-12-23 19:55 - saen acro

I don want to limit specific user I wont to block all and then to allow specific user.

#27 - 2019-12-23 20:01 - saen acro

have you read tasks
https://tvheadend.org/issues/4061
https://tvheadend.org/issues/2914
https://tvheadend.org/issues/4345

#28 - 2019-12-23 21:24 - Flole Systems

Unfortunately we can't help you as you refuse to read the docs and configure accordingly. The feature is already there.

And by the way: #2914 is not a Task as its considered invalid. #4345 is about adding profiles to make configuration easier (it does not mention any additional options), so completely unrelated. While that would make this simpler, what you want is still possible today. #4061 is explicitely for streaming and not for the admin interface.

Please stop trolling around here. And someone please mark this feature request invalid as it already exists and saen acro is just not willing to read and configure accordingly.

#29 - 2019-12-23 22:04 - saen acro

Actualy you flood without understand what is request for.

#30 - 2019-12-23 22:15 - Flole Systems

You want to prevent unauthorized access to the Webinterface for example with stolen credentials by limiting the IP addresses that are allowed to access it.

And that is already possible (and there are even more options available for other usecases). You just refuse to configure it. Which is why this feature request can be considered invalid.

#31 - 2019-12-23 22:21 - saen acro

Please test before suggest.

#32 - 2019-12-23 22:28 - Flole Systems

Please read the docs before opening a feature request. Or at least read them after someone points out that it already exists. Or at least read them after someone tried to spoon feed you the information.

Anyways, you are the one who wants this feature, I don't care anymore. I pointed out the solution, I even spoon fed it to you but you are refusing to configure it, so you can continue to wait for someone to implement this while it's already there.

And someone please mark this as invalid.

#33 - 2019-12-23 22:45 - saen acro

i read them multiple times but not satusfy my neads,
you dont want to understand question.

#34 - 2019-12-23 22:53 - Flole Systems

Ok, then wait for someone to implement this.