AdiIRC - Bug #3874

SSL Certificate Warning isn't recording auto-accept

04/23/2018 01:31 AM - Cassio Luz S.

Status:	New	**Start date:**	04/22/2018
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:	3.1		
Operative System:	All	**Regression:**	No

Description

If you want try connect to a server with the SSL Certificate Expired, it appears a dialog asking if you trust it
Optionally you may enable the option to automatically accept it, but AdiIRC doesn't record it.

It's odd, to be honest. The impression i am having is: Sometimes it records fine, sometimes not.

History

#1 - 04/23/2018 01:49 AM - Per Amundsen

Are you using the 3.1 beta? It has a related fix.

If you are. you can try open config.ini and check the "[Certs]" section, there should be an entry based on the resolved hostname (Connecting to irc.network.com (xx.xx.xx.xx)).

Example entry:

```
irc.network.com,certificatehash
```

If the entry is there, compare the certificatehash with the "SHA1 fingerprint:" in the certificate popup dialog.

Keep in mind connecting to a round robin host containing multiple ip addresses, each individual server must be stored since they in most cases have different hostnames.

example:

irc.network.com points to
server1.network.com
server2.network.com
server3.network.com

AdiIRC must validate and save the certificate for each serverN.network.com independently since they are not the same server.

let me know if that helps, if not, I need to know the network where this happens so I can test myself.

#2 - 04/23/2018 04:06 AM - Cassio Luz S.

Per Amundsen wrote:

> Are you using the 3.1 beta? It has a related fix.
>
> If you are. you can try open config.ini and check the "[Certs]" section, there should be an entry based on the resolved hostname (Connecting to irc.network.com (xx.xx.xx.xx)).
>
> Example entry:
>
> [...]
>
> If the entry is there, compare the certificatehash with the "SHA1 fingerprint:" in the certificate popup dialog.
>
> Keep in mind connecting to a round robin host containing multiple ip addresses, each individual server must be stored since they in most cases have different hostnames.
>
> example:
>
> irc.network.com points to
> server1.network.com
> server2.network.com

server3.network.com

AdiIRC must validate and save the certificate for each serverN.network.com independently since they are not the same server.

let me know if that helps, if not, I need to know the network where this happens so I can test myself.

I am using the most recent beta version.

The server that i am having the issue is: ceres.dk.eu.irchighway.net

Actually, i connect on IRCHighWay only using this server.

Not sure, but looks like AdiIRC only records the auto-accept if you reconnect on the server in your current session. If you close AdiIRC and re-open it, it will not have the auto-accept recorded.

#3 - 04/23/2018 11:47 PM - Cassio Luz S.

I've just realized that even if i try connect directly to ceres.dk.eu.irchighway.net, it sometimes redirects me to a different server.

But today i got the lucky to connect on ceres.dk.eu.irchighway.net and i did the test you asked me.

Actually, the SHA1 Fingerprint on my config.ini for that server is different than the one shown on SSL Certificate Warning (for that server)

I will check if enabling the option does update that. But i am 90% convinced that: It doesn't update.

#4 - 04/24/2018 12:42 AM - Per Amundsen

Try write that fingerprint down somewhere, the next time you connect to that specific server and see the dialog, compare the hash with the one you saved, then one in config.ini and the one in the dialog, it's possible that the certificate was changed/updated.

#5 - 04/30/2018 05:12 PM - Cassio Luz S.

I didn't ignore this thread

Temporary i am not connecting on IRCHighWay often, but if i discover something, i will report.

By the way: i've only reported the issue after a long period dealing with it (the probability of a fingerprint change may exist, but i think the issue is a bit more complex than it looks like)

#6 - 08/18/2018 03:10 PM - Per Amundsen

I recently discovered that SNI domains in server certificates was not always validated correctly, this might be related to that.