

Detect rogue DHCP servers

If your clients experience network access problems due to incorrectly leased IP addresses & incorrect options, you probably have a rogue DHCP server on the network. Rogue DHCP servers are those DHCP servers that are misconfigured, unauthorized unknowingly or those that are configured with a malicious intent for network attacks.

Rogue detection tool is a GUI tool that checks if there are any rogue DHCP servers in the local subnet.

Following are the features with this tool:

1. The tool can be run one time or can be scheduled to run at specified interval.
2. Can be run on a specified interface by selecting one of the discovered interfaces.
3. Retrieves all the authorized DHCP servers in the forest and displays them.
4. Ability to validate (not Authorize in AD) a DHCP server which is not rogue and persist this information
5. Minimize the tool, which makes it invisible. A tray icon will be present which would display the status.
6. When you start the program, it queries the AD and lists all authorized DHCP servers.

Read the article source [here](#). Download the program [here](#).

From:

<https://wiki.plecko.hr/> - **Eureka Moment**

Permanent link:

https://wiki.plecko.hr/doku.php?id=windows:net:rouge_dhcp

Last update: **2019/10/31 09:06**

