What can I Expect if I Have no Credentials

You can certainly run a discovery without any valid credentials on the devices within the network, however, the information retrieved will be a very small subset of what Open-AudIT has the ability to retrieve with credentials.

If you run discovery upon a subnet that the Server (or Collector) ***is not*** directly installed on, you can expect the following for responding devices:

- IP Address
- DNS Hostname and FQDN (assuming working and client populated DNS)
- Open ports
- An educated guess to the identity and type of device

If you run discovery upon a subnet that the Server (or Collector) ***is*** directly installed on, you can expect the following for responding devices:

- IP Address
- MAC Address
- Manufacturer (derived from Mac Address)
- DNS Hostname and FQDN (assuming working and client populated DNS)
- Open ports
- An educated guess to the identity and type of device

If you have working credentials, you can expect the full amount of information possible.

Obviously, the best way to use Open-AudIT is to have working credentials for the devices being discovered (be they WMI, SSH, or SNMP credentials).

We also have a page on auditing without credentials. How and Why is Open-AudIT "more secure"?#Agent?Discovery?Credentials?

In my personal opinion, the best way to find and audit every single item on your network is a Seed Discovery for each subnet, restricted to that subnet (using credentials). Seed Discoveries use switch, router and computer MAC Address tables to not miss a single device. If it is connected to the network and uses TCP/IP, a switch/router/computer has to know it is there - that's just how TCP/IP works. Combine that with custom TCP and/or UDP ports and you should then be able to determine the device type as well. But that's just my personal preference 🙂