About MxToolBox

The MxToolBox API is a RESTful Web Service allowing MxToolbox customers to query the status of their monitors and run lookups (blacklist, smtp, mx, etc.).

Using MxToolBox Function

We have included one rule and one workflow as an example. Below the list of possible commands available:

The following MxToolbox commands can be executed:

- blacklist : Check IP or host for reputation
- smtp : Test mail server SMTP (port 25)
- mx : DNS MX records for domain
- a : DNS A record IP address for host name
- spf : Check SPF records on a domain
- txt : Check TXT records on a domain
- ptr : DNS PTR record for host name
- cname : DNS canonical host name to IP address
- whois : Get domain registration information
- arin : Get IP address block information
- soa : Get Start of Authority record for a domain
- tcp : Verify an IP Address allows tcp connections
- http : Verify a URL allows http connections
- https : Verify a URL allows secure http connections
- ping : Perform a standard ICMP ping
- trace : Perform a standard ICMP trace route
- dns : Check your DNS Servers for possible problems

Additional workflows and rules are required in order to implement different types of commands.

Environment

To install in "development mode", run `pip install -e ./fn_mxtoolbox/`

The distribution file can be installed using `pip install fn_mxtoolbox-<version>.tar.gz`

Import the package into Resilient by running `resilient-circuits customize`

To configure the MXToolbox parameters, run `resilient-circuits config [-u | -c]`. Then edit the `[fn_mxtoolbox]` template with the URL and basic authentication settings.

Run with: `resilient-circuits run`.

To uninstall, run: `pip uninstall fn_mxtoolbox`

Resilient Configuration

Follow the steps to add a fn_mxtoolbox section to your `app.config` file by running `resilient-circuits config [-u | -c]` and updating the fields:

```
[fn_mxtoolbox]
url=https://api.mxtoolbox.com/api/v1/Lookup
api_token=<your-api-token>
```