GYTPOL Validator

SaaS onboarding

Doc: GYT-TEC-012
Release: 4
Date: 25th July 2023

Confidential: GYTPOL and approved recipients

Total pages:	18

Doc. Title:	GYTPOL Validator SaaS onboarding

Doc. No.:	GYT-TEC-012	**Classification:**	Confidential
Revision:	4	**Restriction:**	GYTPOL and approved recipients
Date:	25th July 2023	**Customer:**	

Owner:	Mark Zuk	**Reviewers/ Approvers:**	Matthew Album Gilad Raz Tal Kollender
Author:	Mark Zuk		

Contents

Introduction 4

Preliminary steps and ongoing 4

New Customers (PoC or Production) 5

Existing On-Prem Customers, migrating to SaaS 5

Supported Operating Systems 6

Client download (latest versions) 7

Windows OS 8

- Pre-Installation 8
- Manual Installation 8
- Post-Installation 9
- Uninstalling 10

Linux 11

- Pre-Installation 11
- Manual Installation 11
- Post-Installation 11
- Uninstalling 13

macOS 14

- Pre-Installation: 14
- Installation: 14
- Post-Installation 16
- Uninstalling 18

Introduction

The purpose of this document is to provide instructions for the SaaS onboarding of a new customer or existing customer migrating to GYTPOLs SaaS.

Preliminary steps and ongoing

1. The Customer will provide a list of email addresses that should access the UI.
    a. The customer can integrate GYTPOL with IDP that is currently used, for example OKTA, AzureAD and more.
2. In case the Customer needs to set up different access levels, please mention the needed access level, i.e Full Admin, Windows Servers – read, Linux Debian – write etc.
3. Make sure the target operating system is supported and a part of the list below.
4. Once the SaaS tenant is created, GYTPOL will provide you with the username (email address provided) and initial password that must be changed upon the first login.
5. GYTPOL will provide a list of FW rules (443 port only to SaaS URLs) to whitelist in case of blocks.
6. GYTPOL will provide the links to the clients per OS (Windows MSIs, Linux and macOS packages).
    a. The clients can also be downloaded from GYTPOL UI.

For Customers who wish to see Active Directory / GPO data and CIS/NIST benchmarks:

7. Please set up a server (can be a shared server) according to the dsRequester system requirements: https://gytpol.com/resource/dsrequester-installation-requirements/

For SaaS POC:

8. The PoC license is limited to 50 devices and 21 days. It is a fully working license, including all our modules and functions: detection, remediation and revert functionality.
9. During the PoC we will conduct several meetings, including an onboarding session to review any initial findings and UI overview, a status call for a more advanced and technical discussion and a PoC summary call to

review the findings, present the results to the stakeholders and decision-makers and discuss next steps.

New Customers (PoC or Production)

Once the dsRequester server is ready (if needed) and all the FW rules are created, the customer should deploy GYTPOL client on a group of devices within licensing limitations.
After the device is scanned, the data is sent to GYTPOL, and the metrics are shown in the UI.
The software is equipped with full functionality, including remediation. We recommend you be mindful when choosing your targeted devices for remediations. It is recommended to test remediations on a few devices prior to jumping into large-scale targets.

Existing On-Prem Customers, migrating to SaaS

GYTPOL will provide a new client (higher version) and the new client will update the existing installation, will recreate the configuration files, and redirect the data to SaaS instead of the local server.
The new client deployment can be done using any deployment tool currently used, such as SCCM, BigFix or GPO. You can also use GYTPOL to deploy the new client using GYTPOL internal Auto-Update mechanism.
After the device is scanned, the data is sent to GYTPOL SaaS instead of the local server, and the metrics are shown in the UI. The updated device will be reporting to the new GYTPOL SaaS but will be still visible in the old server for another 14 days (in case you choose to use GYTPOLs auto-update).
Please note that data migration is not possible, and all Remediation tasks and Mutes must be recreated in the new UI. Same goes for Roles and Permissions.

Supported Operating Systems

Microsoft:

Endpoints: Windows 7 (x32/x64) and later

Servers: Windows Server 2008 and later

Microsoft Client / OS support matrix:

OS	Detection	Remediation / Revert
Windows 7	V	X
Windows 8 / 8.1	V	X
Windows 10 / 11	V	V
Windows Server 2008 / 2008 r2	V	X
Windows Server 2012 / 2012 r2	V	X
Windows Server 2016 / 2019 / 2022	V	V

Note: Remediation is supported on older versions of Microsoft Windows and Servers if Powershell v5.1 and later is installed.

Linux Client / OS support matrix:

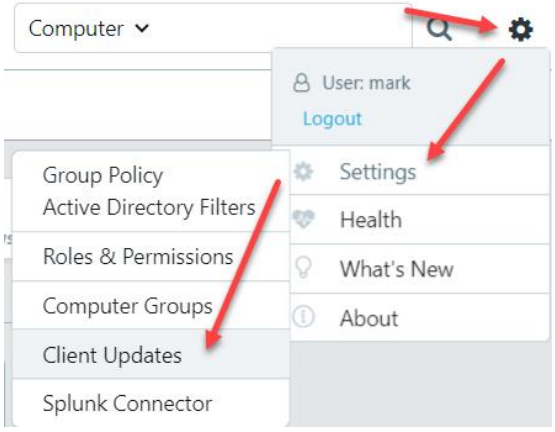
OS	Detection	Remediation / Revert
Ubuntu 16 and later	V	V
RHEL 7 and later	V	V
Centos 7 and later	V	V
Rocky 9 and later	V	V
SUSE 12 and later	V	V
Ubuntu 16 and later	V	V

macOS Client / OS support matrix:

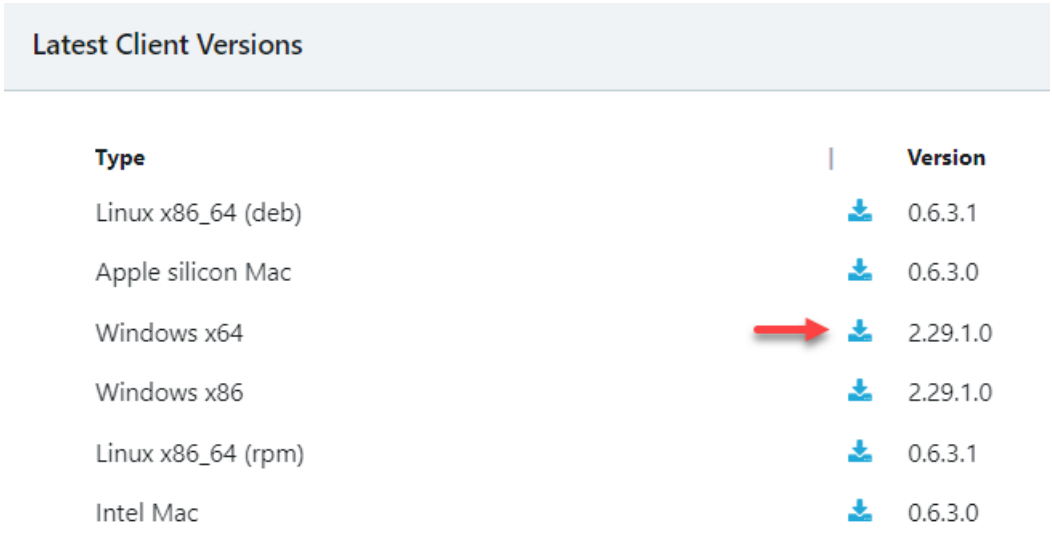
OS	Detection	Remediation / Revert
Catalina 10.15 (x64) and later	V	V

Client download (latest versions)

To get the latest version of any client, please follow this:



In this screen, you will find the latest versions of the client available for download. Click on the download icon, relevant to the operating system and follow the installation instructions below:



Windows OS

Pre-Installation

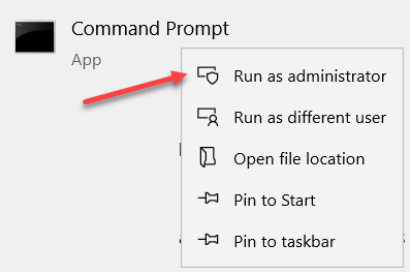
Ports to open:
GYTPOL Client to GYTPOL SaaS - port 443

Does the Endpoint need to be a member of the domain?
No

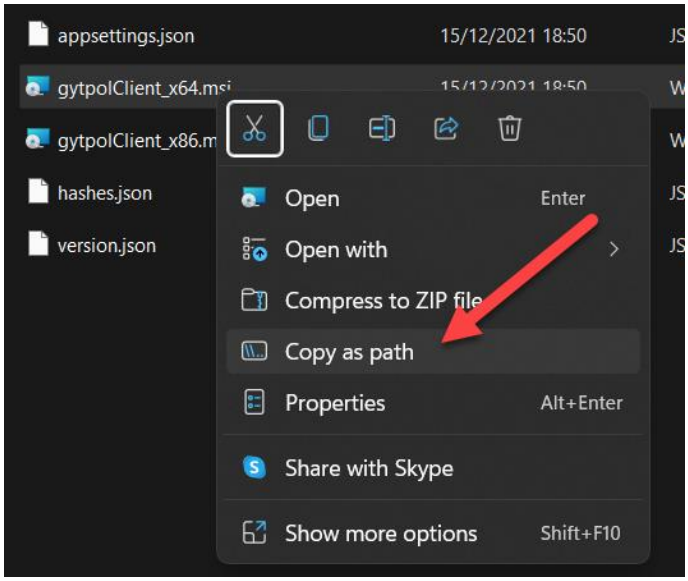
Can I use software deployment tools to install the client across my network?
Yes – you can use any tool that can deploy and install the package, such as SCCM, BigFix and many more.
GPO deployment is also supported using this guide:
https://gytpol.com/resource/client-deployment-using-gpo/

Manual Installation

Open **elevated Command Prompt** (r. click on Command Prompt > Run as Administrator).



Once opened, please go to the MSI file you wish to install > hold L. Shift > r. click it > click "**Copy as Path**".

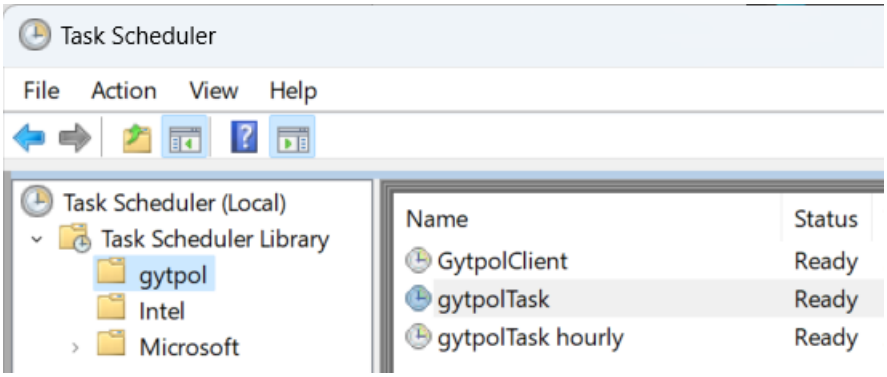


Go to the elevated CMD you opened in step 1 and paste the path into the CMD window > **Enter**.

Once finished, the progress window will be disappeared.

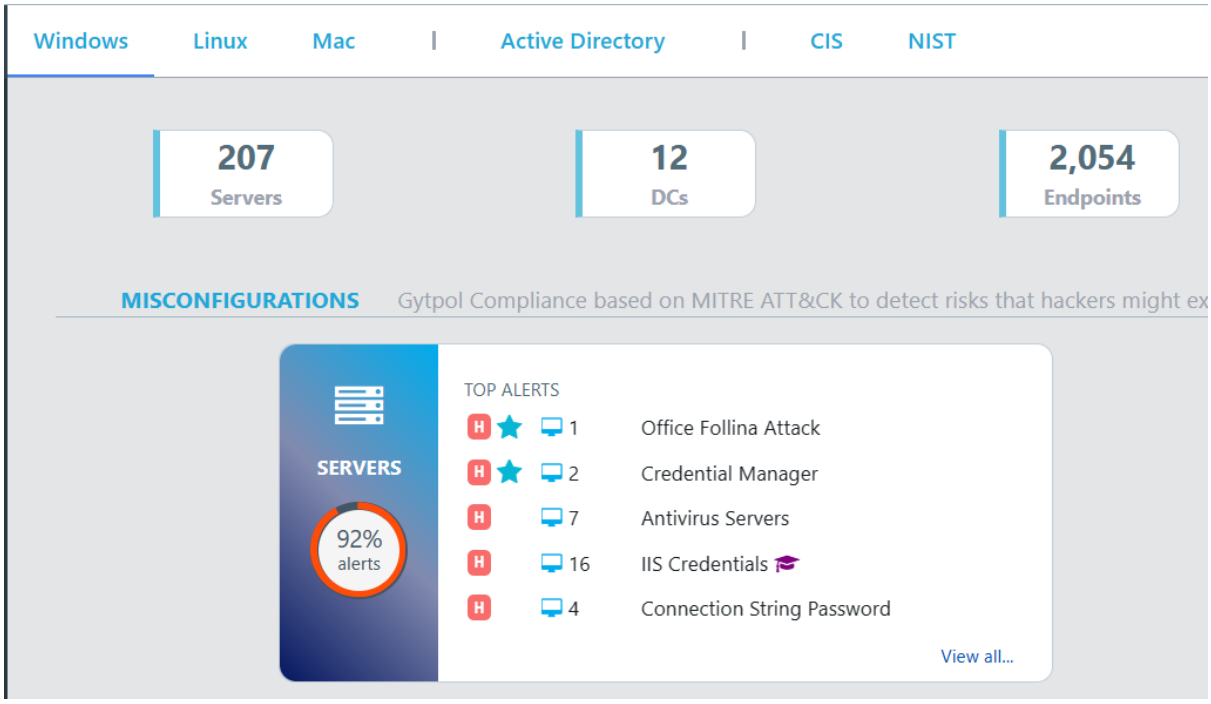
Post-Installation

To check if the client was successfully installed, please open Task Scheduler as Administrator and check for **gytpol** folder under the main Task Scheduler Library. Expand it and you should see 3 tasks as shown in the example below:



Where will I see the scanned machine?

Under 'Windows' tab in the GYTPOL UI:



Where is the installation path?

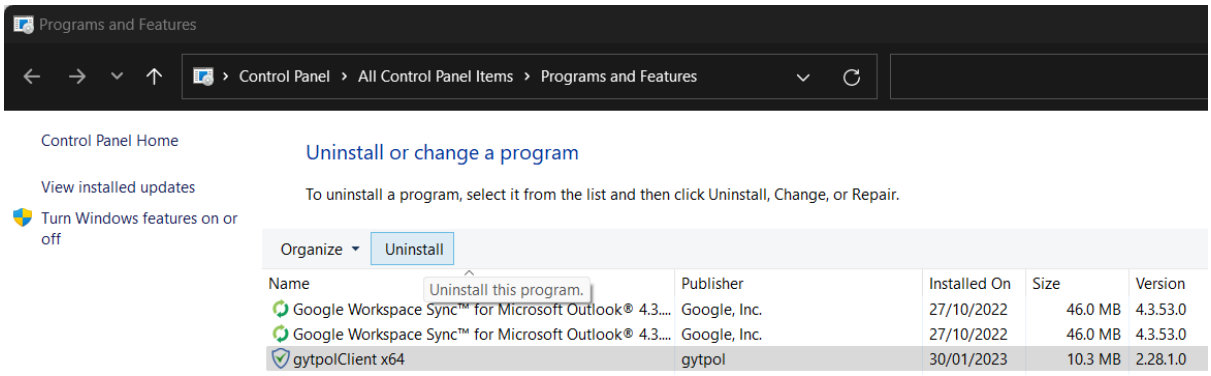
C:\Program Files\WindowsPowerShell\Modules\gytpol

Where are the logs?

C:\Program Files\WindowsPowerShell\Modules\gytpol\log

Uninstalling

Please remove the **gytpolClient** from Program and Features > Uninstall



Linux

Pre-Installation

Ports to open:

GYTPOL Client to GYTPOL SaaS - port 443

Does the Endpoint need to be a member of the domain?

No

Can I use software deployment tools to install the client across my network?

Yes – you can use any tool that can deploy and install the package, such as Chef, Puppet, Ansible and many more.

Manual Installation

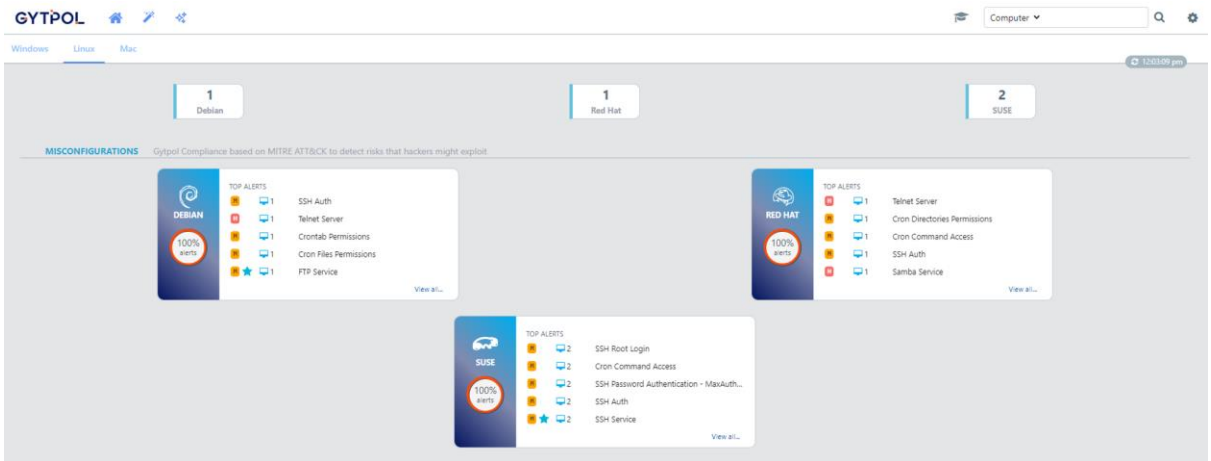
Command to run:

- Debian: sudo dpkg -i <gytpol-client-path>
- Redhat: sudo rpm -ivh <gytpol-client-path>

Post-Installation

Where will I see the scanned machine?

Under 'Linux' tab in the GYTPOL UI:



How do I see and change the service status?

systemctl stop/start/status gytpol-client

Where is the installation path?

/opt/gytpol

Where are the logs?

/opt/gytpol/logs

Where are the configuration folder?

“config.json ” for client’s configuration to a dedicated server

“metrics.json” for metrics configuration.

config.json

This file contains client’s configuration:

```
{
   "HttpVerifyCert" : false,
   "HttpTimeout" : 10000000000,
   "ServerAddress" : "_gytpol",
   "ArchiveFolderPath" : "archive"
}
```

```
"cloudCfg": {
    "Region": "<AWS_REGION>",
    "AccessKeyID": "<AWS_ACCESS_KEY_ID>",
    "SecretAccessKey": "<AWS_ACCESS_KEY_SECRET>",
    "ReportsBucket": {
      "scanner-report": "<TENANT_REPORTS_BUCKET>",
      "remediation-report": "<TENANT_REPORTS_BUCKET>"
    },
    "ReportsStream": {
      "scanner-report": "<TENANT_REPORTS_STREAM>",
      "remediation-report": "<TENANT_REPORTS_STREAMT>"
    }
  }
```

Fields explanations:
HttpVerifyCert - Indicate whether to validate the server's certificate when using HTTP requests.
HttpTimeout - Determine the timeout (in Nano Seconds) for HTTP requests.
ServerAddress - The address of the GYTPOL server.
ArchiveFolderPath - Folder (relative to /opt/gytpol) in which reports are being saved to before sending them to the server.

Uninstalling

Commands to run:

Debian: sudo dpkg —remove gytpol-client
* Use the "—purge" instead of "—remove" to also delete the logs, archive etc.

Redhat: sudo rpm -e gytpol-client

Both rpm & dpkg commands that are listed above may delete some configuration files related to Gytpol.
Deleting files that may lead to loss is at your own risk, please make sure that nothing important is being removed before deleting!
It's always a good idea to take a backup of important data before making any changes to the system.

macOS

Pre-Installation:

Ports to open:
GYTPOL Client to GYTPOL SaaS - port 443

Does the Endpoint need to be a member of the domain?
No

Can I use software deployment tools to install the client across my network?
Yes – you can use any tool that can deploy and install the package, such as Jamf, JumpCloud and many more.

Installation:

Before running installation, identify the platform architecture. This can be achieved by checking the 'About this Mac':

Or by running a terminal command uname -p.

Identify and choose the right package according to the table below:

Platform	Architecture	Terminal output	Package file
macOS	**Intel** chipset	i386	gytpol-client-<version>**_amd64**.pkg
macOS	**Apple** silicon	arm	gytpol-client-<version>**_arm64**.pkg

Command to run:
sudo /usr/sbin/installer -pkg <pkg_path> -target /

example:
sudo /usr/sbin/installer -pkg ~/Downloads/gytpol-client-0.5.1.0-0_arm64.pkg -target /

To check that the launch daemon is running run:

sudo launchctl list | grep com.gytpol.gytmac

If the daemon is running, you will see its process ID (PID) on the left (highlighted in red):

```
❯ sudo launchctl list | grep com.gytpol.gytmac
46750   0       com.gytpol.gytmac
```

For further information run:
sudo launchctl list com.gytpol.gytmac

If you're running the client on an intel processor, please make sure that you are running the correct binary (_amd64 i.e.: gytpol-client-1.2.1.2-28_amd64.pkg).

Note: An amd64 binary will run on an arm64 processor but is not recommended and not officially supported.

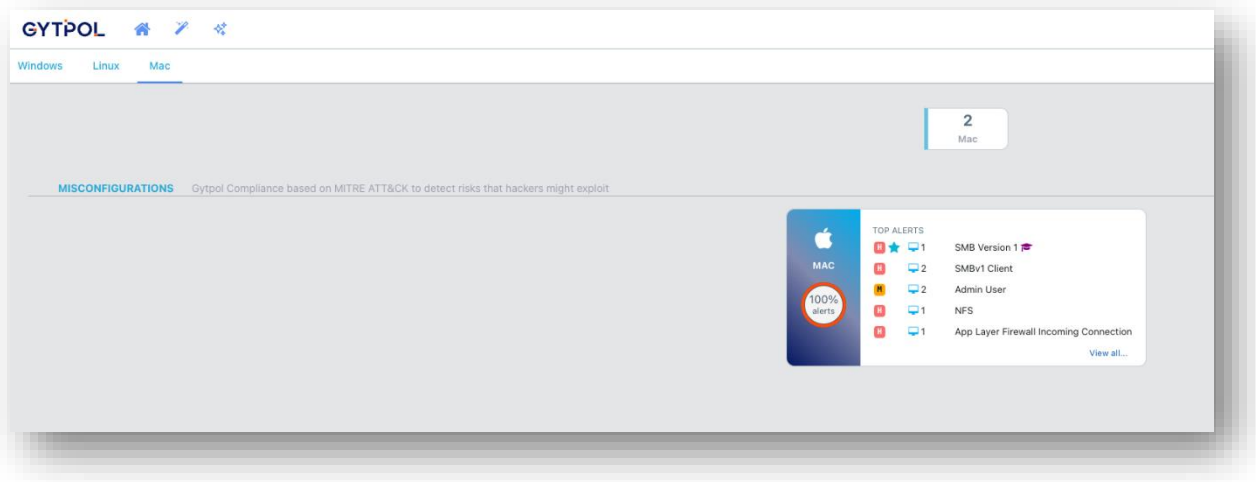
Your output should look like this:

```
❯ sudo launchctl list | grep com.gytpol.gytmac
46750   0       com.gytpol.gytmac
❯ sudo launchctl list com.gytpol.gytmac
{
        "StandardOutPath" = "/tmp/gytmac.stdout";
        "LimitLoadToSessionType" = "System";
        "StandardErrorPath" = "/tmp/gytmac.stderr";
        "Label" = "com.gytpol.gytmac";
        "OnDemand" = true;
        "LastExitStatus" = 0;
        "PID" = 46750;
        "Program" = "/opt/gytpol/gytmac";
        "ProgramArguments" = (
                "gytmac";
                "-poc";
        );
};
```

Post-Installation

Where will I see the scanned machine?

Under 'Mac' tab in the GYTPOL UI:



How do I see and change the service status?

sudo launchctl stop/start/list com.gytpol.gytmac

/opt/gytpol/config/config.json (you may need to create the 'config' folder and the config.json file). See the file example below.

Where is the installation path?
/opt/gytpol

Where are the logs?
/opt/gytpol/logs

Where are the configuration folder?
"config.json " for client's configuration to a dedicated server
"metrics.json" for metrics configuration.

config.json
This file contains client's configuration:

```
{
   "HttpVerifyCert" : false,
   "HttpTimeout" : 10000000000,
   "ServerAddress" : "_gytpol",
   "ArchiveFolderPath" : "archive"
}
```

Fields explanations:
HttpVerifyCert - Indicate whether to validate the server's certificate when using HTTP requests.
HttpTimeout - Determine the timeout (in Nano Seconds) for HTTP requests.
ServerAddress - The address of the GYTPOL server.
ArchiveFolderPath - Folder (relative to /opt/gytpol) in which reports are being saved to before sending them to the server.

Uninstalling

1. Stop the launch daemon.

   sudo launchctl stop com.gytpol.gytmac

2. Unload the launch daemon from launchctl.

   sudo launchctl unload -w /Library/LaunchDaemons/com.gytpol.gytmac.plist

3. Delete the lauanch daemon configuration plist file.

   sudo rm -rf /Library/LaunchDaemons/com.gytpol.gytmac.plist

4. Remove folder (including all sub-directories & sub-files).

   sudo rm -rf /opt/gytpol

5. Discard receipt data.

   sudo pkgutil --forget com.gytpol.gytmac

NOTE: Deleting files that may lead to loss and is at your own risk, please make sure that nothing important is being removed before deleting!