GYTPOL Validator

SaaS onboarding

Doc: GYT-TEC-012
Release: 1
Date: 28th February 2023

Confidential: GYTPOL and approved recipients

Total pages:	15

Doc. Title:	GYTPOL Validator SaaS onboarding

Doc. No.:	GYT-TEC-012	**Classification:**	Confidential
Revision:	2	**Restriction:**	GYTPOL and approved recipients
Date:	28th Feb 2023	**Customer:**	

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

@ GYTPOL Limited 2023. All rights reserved. PROPRIETARY AND CONFIDENTIAL.

This document may include reference to technologies that use patents (pending or granted) which are owned by GYTPOL Limited or third parties. The use of such patents shall be subject to express written license terms. You shall not copy, disclose, reproduce, store in a retrieval system, or transmit in any form or by any means whether in whole or in part this document. GYTPOL Limited accepts no liability and offers no warranty in relation to the use of this document, or any technology referenced herein as well as associated intellectual property rights except as it has otherwise agreed in writing.

All trademarks and brands are the property of their respective owners, and their use is subject to license terms.

Contents

Introduction 4

Preliminary steps and ongoing 4

Supported Operating Systems 5

Windows OS 6

Pre-Installation 6

Installation 6

Post-Installation 7

Uninstalling 9

Linux 10

Pre-Installation 10

Installation 10

Post-Installation 10

Uninstalling 12

macOS 13

Pre-Installation: 13

Installation: 13

Post-Installation 13

Uninstalling 15

Introduction

The purpose of this document is to provide instructions for the SaaS onboarding of a new customer to GYTPOL.

Preliminary steps and ongoing

1. The Customer will provide a list of email addresses that should access the UI.
2. In case the Customer need to setup 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 AWS 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 you with the FW rules (443 port only to AWS URLs) to whitelist in case of blocks.
6. GYTPOL will provide the links to GYTPOL client per OS (Windows, Linux and macOS).
7. PoC license is limited to 50 devices and 21 days. It is a fully working license, including all of our modules and functions: detection, remediation and revert functionality.
8. 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.

Supported Operating Systems

Microsoft:

Endpoints: Windows 7 (x32/x64) and later

Servers: Windows Server 2008 and later

Linux:

Ubuntu 16 and later

RHEL 7 and later

Centos 7 and later

Rocky 9 and later

SUSE 12 and later

macOS:

Catalina 10.15 (x64) and later

Windows OS

Pre-Installation

Ports to open:

GYTPOL Client to GYTPOL server on-Prem - port 9093

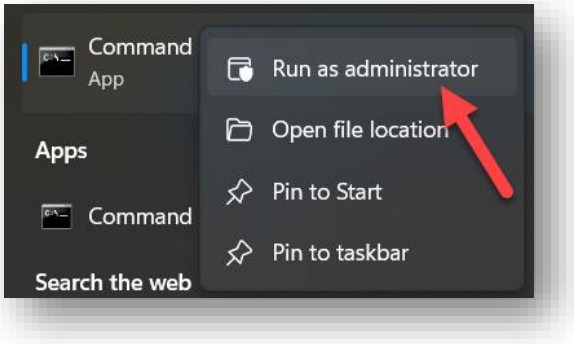
GYTPOL Client to GYTPOL SaaS - port 443

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

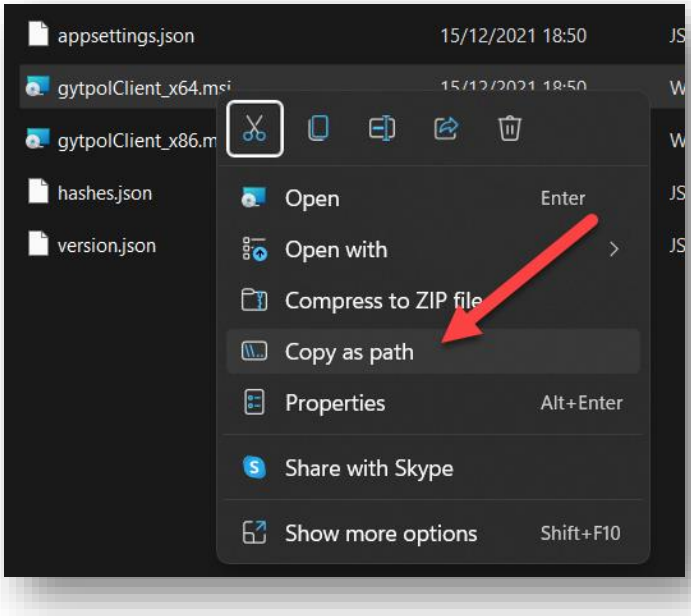
No

Installation

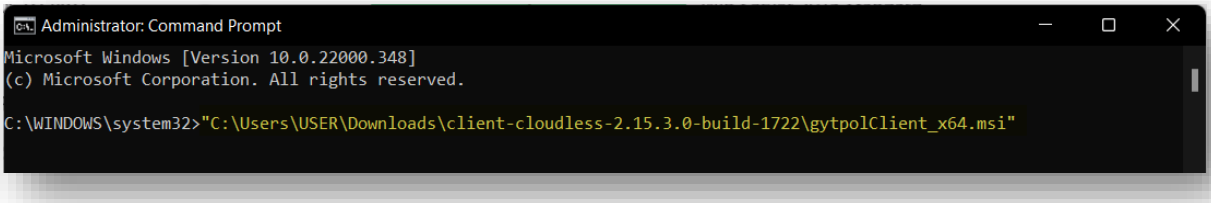
Open **elevated CMD** (r. click on CMD > Run as Administrator).



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



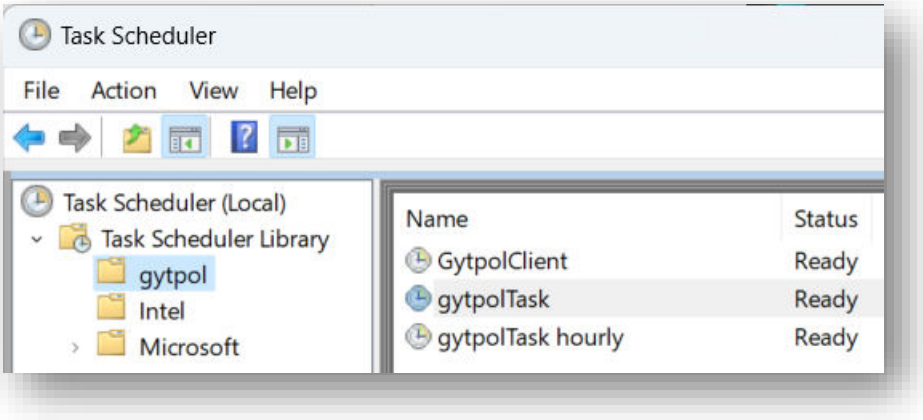
Go to the elevated CMD you opened in step 1 and paste the path into the CMD window > **Enter**.



Once finished, the progress window will be disappeared.

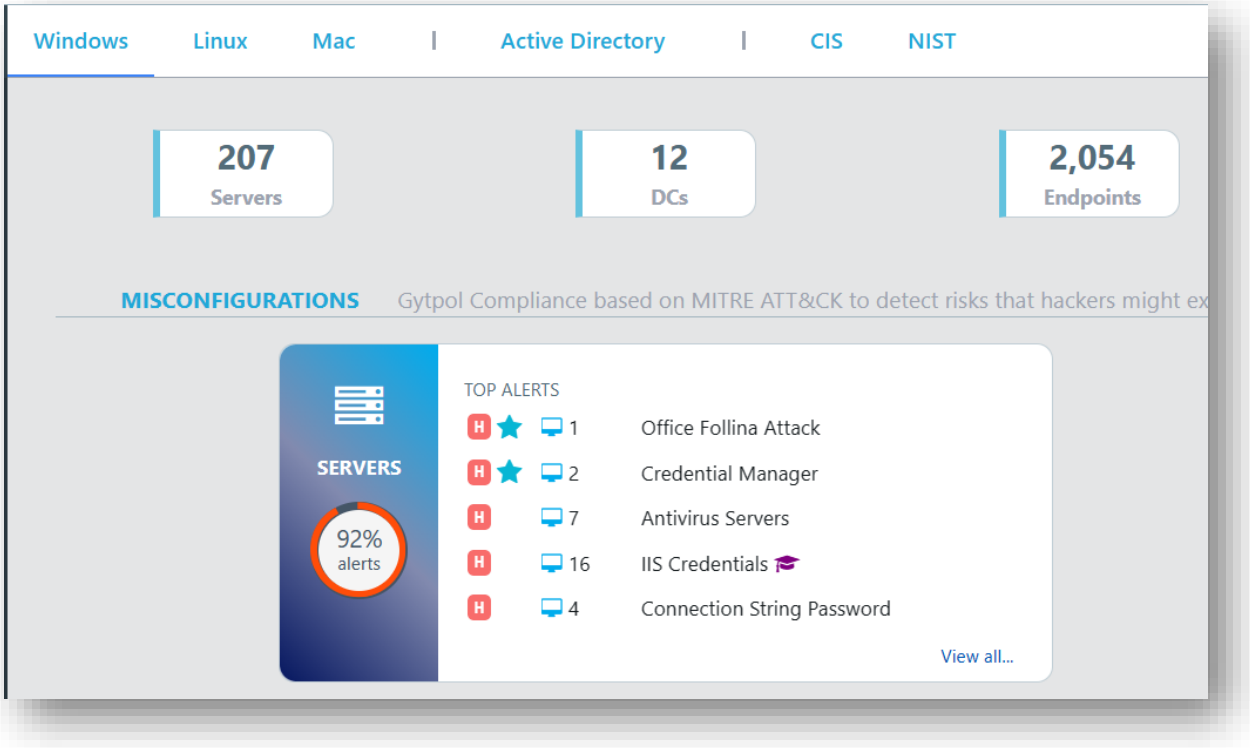
Post-Installation

To check if the client was successfully installed, please open Task Scheduler as Admininstrator and check for **gytpol** folder under the main 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?

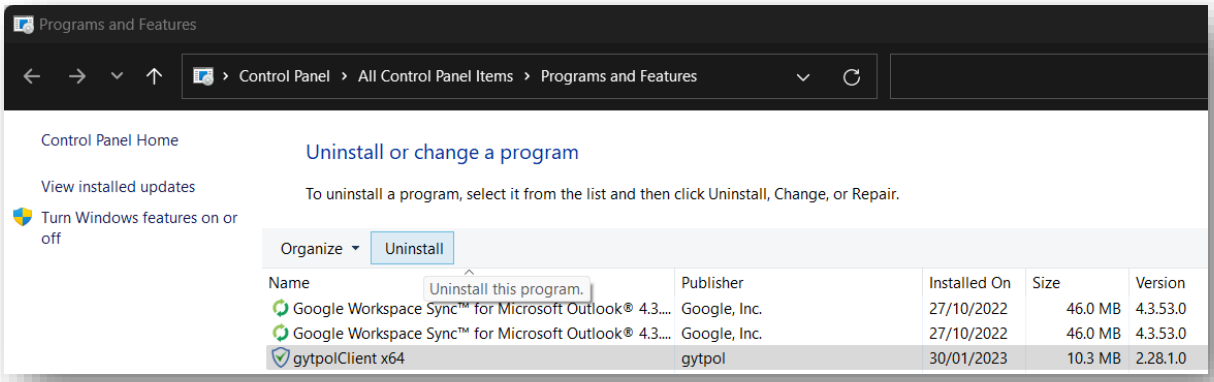
C:\Program Files\WindowsPowerShell\Modules\gytpol

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 server on-Prem - port 9093

GYTPOL Client to GYTPOL SaaS - port 443

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

No

Installation

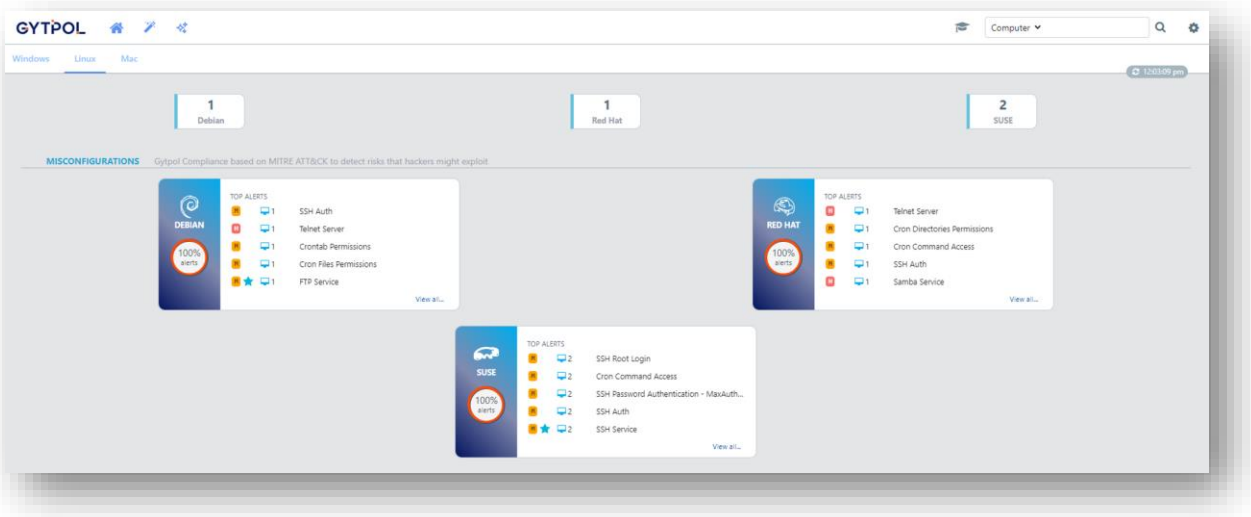
Command to run:

- 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"
}
```

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 commends 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 server on-Prem - port 9093

GYTPOL Client to GYTPOL SaaS - port 443

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

No

Installation:

Command to run:

```
sudo /usr/sbin/installer -target /opt/gytpol -pkg <pkg_path>
```

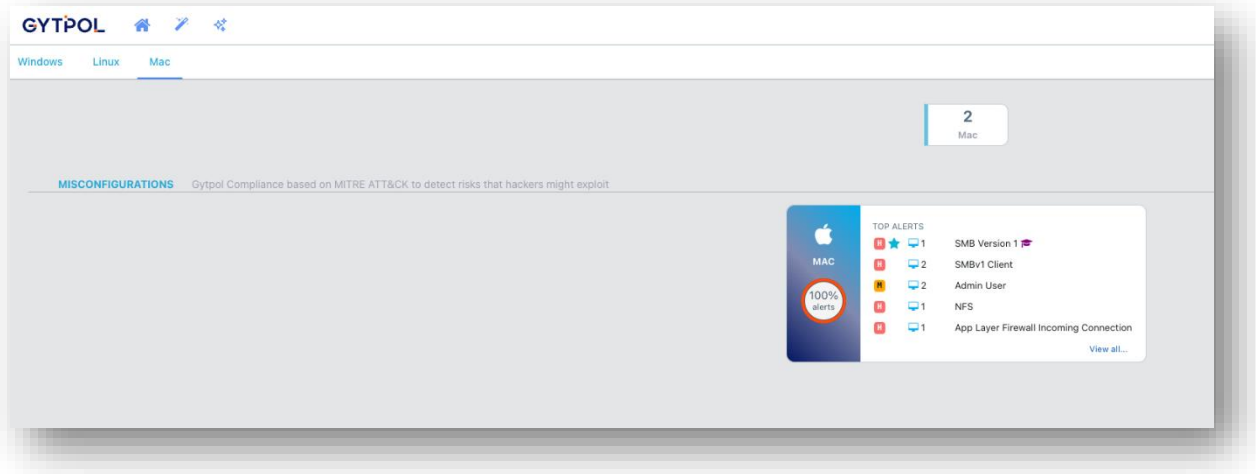
example:

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

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

Command to run

First remove the installed files and their directories:

```
# Validite the files that we're going to delete
$ pkgutil --only-files --files com.gytpol.gytmac

# Delete the Files
$ pkgutil --only-files --files com.gytpol.gytmac| tr '\\n' '\\0' | xargs -
n 1 -0 sudo rm -f

# Validite the directories that we're going to delete
$ pkgutil --only-dirs --files com.gytpol.gytmac

# Delete the directories
$ pkgutil --only-dirs --files com.gytpol.gytmac | tail -r | tr '\\n' '\\0'
| xargs -n 1 -0 sudo rmdir
```

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!

Once you've uninstalled the files, you can remove the receipt with:

```
$ sudo pkgutil --forget the-package-name.pkg
```