

GYTPOL Validator

Client installation

Doc: GYT-TEC-011 Release: 2 Date: 28th February 2023

Confidential: GYTPOL and approved recipients



www.gytpol.com



Total 14 pages:

Doc.	GYTPOL Validator
Title:	Client installation

Doc. No.:	GYT-TEC-011	Classification:	Confidential
Revision:	2	Restriction:	GYTPOL and approved recipients
Date:	28 th Feb 2023	Customer:	

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

@ GYTPOL Limited 2022. 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
Supported Operating Systems	4
Windows OS	5
Pre-Installation	5
Installation	5
Post-Installation	6
Uninstalling	8
Linux	9
Pre-Installation	9
Installation	9
Post-Installation	9
Uninstalling	11
macOS	12
Pre-Installation:	12
Installation:	12
Post-Installation:	12
Uninstalling	14





Introduction

The purpose of this document is to provide instructions how to install the GYTPOL Validator client on various OS (Windows, Linux and macOS).

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



www.gytpol.com





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".



www.gytpol.com





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:



(D) Task Scheduler		
File Action View Help		
 Task Scheduler (Local) Task Scheduler Library 	Name () GytpolClient	Status Ready
	A 177 1	Dead

Where will I see the scanned machine?

Under 'Windows' tab in the GYTPOL UI:

						·	CIS	14151	
	207 Servers				12 DCs				2,054 Endpoints
MISC	ONFIGURA	FIONS Gyt	pol Comp	liance bas	ed on MI	TRE AT	F&CK to (detect risks	that hackers might e
			TOP ALE	RTS	Office Fo	ollina Att	ack		
		SERVERS		— 2	Credenti	al Mana	ger		
		0.20%	H	7	Antivirus	Servers			
		92% alerts	H	- 16	IIS Crede	entials 🎓	•		
			H	- 4	Connect	ion Strin	g Passwor	d	
								Viewa	all

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

Programs and Features					
$\leftrightarrow \rightarrow \sim \uparrow \square \circ \circ$	ntrol Panel > All Control Panel Items > Programs and Featu	ıres ~ C			
Control Panel Home	Uninstall or change a program				
View installed updates	To uninstall a program, select it from the list and then	click Uninstall, Change, or Repair.			
Turn Windows features on or off					
	Organize • Uninstall				
	Name Uninstall this program.	Publisher	Installed On	Size	Version
	Google Workspace Sync™ for Microsoft Outlook® 4.3	Google, Inc.	27/10/2022	46.0 MB	4.3.53.0
	Google Workspace Sync™ for Microsoft Outlook® 4.3	Google, Inc.	27/10/2022	46.0 MB	4.3.53.0
		gytpol	30/01/2023	10.3 MB	2.28.1.0







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:

ws Linux Mac		C 120109 pm
1 Debian	1 Red Hat	2 5055
1009 ALBERS DEMAN 1000 Stress 1000 Stress	2	TOPALSTS TOPALSTS TOPALSTS TO Con Directories Remaines TO Con Directories Remaines TO Con Directories Remaines TO Con Directories Remaines TOPALSTS
	TOP ALSES SUSE 1000	





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" : 1000000000,
  "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:

	2 Mac
ISCONFIGURATIONS Gytpol Compliance based on MITRE ATT&CK to detect risks that hackers might ex	oit
	TOP ALERTS
	MAC [] Q 2 SMBy1 Client
	100% 🕅 🖵 2 Admin User
	alerts 0 🖵 1 NFS
	App Layer Firewall Incoming Connection View all





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" : 1000000000,
  "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
```

