GYTPOL

GYTPOL Validator

High Level Architecture

Doc: GYT-TEC-001
Release: 7

Total pages:	20

Doc. Title:	GYTPOL Validator High Level Architecture

Doc. No.:	GYT-TEC-001	**Classification:**	Confidential
Revision:	7	**Restriction:**	GYTPOL and approved recipients
Date:	26th May 2023	**Customer:**	

Owner:	Tal Kollender	**Reviewers/ Approvers:**	Matthew Album Gilad Raz Yakov Kogan
Author:	Tal Kollender		

Contents

Introduction

This document provides an overview of GYTPOL Validator technical architecture and major data flows.

GYTPOL is a comprehensive cybersecurity solution designed to secure and optimize your digital assets. It's versatile and robust and can function across various operating systems, including Windows, Linux, and macOS. – Whether you're operating on desktops, laptops, or servers, and regardless of whether these are virtual or physical – our solution seamlessly integrates and protects.

The product automates the following use cases:

- Continuously detects device security misconfigurations, caused by Operating Systems, human errors and 3rd party applications, with auto-remediation and zero impact.
- Revert remediation actions if necessary.
- Suggests better ways to harden your devices.
- Validates that computers and user Group Policies have been correctly applied to all endpoints, at all times. (InTune policy will be supported soon)
- Benchmarking configuration versus the industry security standards such as CIS and NIST.
- Enhanced security of the Active Directory and Group Policy.
- Optimizing Group Policy definitions (e.g., finding duplicated and conflicting GPOs)
- Identifying Group Policies that are slowing down computer start up time and user login time.

How GYTPOL Validator Works – General Overview

GYTPOL Validator can be deployed on-prem or SaaS:

- In case GYTPOL is deployed **on-prem**, the customer should provide a dedicated physical or virtual MS Windows Server for GYTPOL Validator Server deployment. Please refer to the GYTPOL Validator System Requirements documents for the exact specifications.
- In case GYTPOL is deployed in the **SaaS** – a tenant is being created for the customer in their region, and the UI access is based on the customer's email addresses (MFA is supported).

In both cases (on-prem or SaaS), a semi-client (less than 5MB) needs to be installed on each device (Windows, Linux and macOS).

We elaborate on the GYTPOL Server and GYTPOL Client in more details below.

How GYTPOL Validator Works: On-Prem

As mentioned earlier, there is a need for a dedicated server (the server can be hosted in the private cloud or in the datacenter).
Once the server commissioned, the customer will receive an EXE file for installing the GYTPOL server. It takes just a few minutes to install and will lead the user through a series of simple steps.

During the installation, MS localDB is installed and there is no need to have a dedicated MS SQL Server for a deployment of up to 3500 devices.
For deployments over 3500 devices, we recommend installing a dedicated MS SQL server.

The next deployment step is to distribute the client installer **(Windows/Linux/macOS > less than 5MB)** using the organization's software distribution tools such as Microsoft SCCM/InTune, jamf, Tanium, BigFix, Chef, Puppet, Invanti, PDQDeploy etc.

Once deployed, GYTPOL Client installer will collect the misconfigurations data and within a few minutes send it to the server as a gzip format in HTTPS (data is encrypted with a public key that gets pulled first, then the file is sent using the latest TLS supported version; file size is less than 30kb).

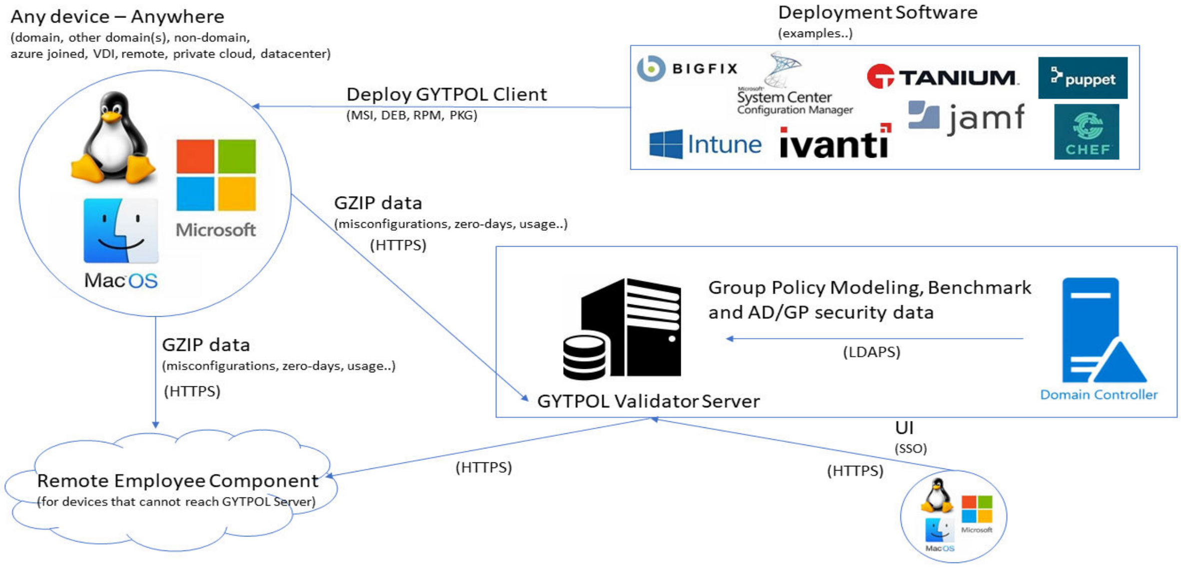

Any device – Anywhere
(domain, other domain(s), non-domain, azure joined, VDI, remote, private cloud, datacenter)
Microsoft
MacOS
Deploy GYTPOL Client
(MSI, DEB, RPM, PKG)
Deployment Software
(examples..)
BIGFIX
Microsoft System Center Configuration Manager
TANIUM
puppet
jamf
Intune
ivanti
CHEF
GZIP data
(misconfigurations, zero-days, usage..)
(HTTPS)
Group Policy Modeling, Benchmark and AD/GP security data
(LDAPS)
Domain Controller
GYTPOL Validator Server
GZIP data
(misconfigurations, zero-days, usage..)
(HTTPS)
UI
(SSO)
(HTTPS)
(HTTPS)
Remote Employee Component
(for devices that cannot reach GYTPOL Server)
Microsoft
MacOS

Figure 1. GYTPOL Validator (on-prem) Data Flow

The main GYTPOL Validator data flow takes the following steps:

1. GYTPOL Server is installed, and a license has been loaded.
2. GYTPOL Client runs once a day, at random times with less than 5 minutes intervals
3. During the run – it collects misconfigurations, un-patched zero-days and for MS devices it also collects Group-Policy data (rsop). (Intune configs for any device will be added soon).
4. GYTPOL Client then compresses the data, encrypts it with the public key and tries to reach the GYTPOL Server to send the data.
5. In case the device cannot reach the GYTPOL Server – it will send the data to GYTPOLs Remote-Employee component in the cloud (the region the organization agreed on), and the GYTPOL Server pulls the data from there. This can be optionally disabled.
6. Upon receiving data from a GYTPOL Client, The data is analyzed by the GYTPOL Server using our proprietary GYTPOL Analyzer. The Analyzer not only scrutinizes the data but also archives the findings in a dedicated database, keeping you abreast up to date of any potential security risks.
7. IT and Security teams review the findings using Web UI (Chrome/NewEdge).
8. GYTPOL Server has several integrations, for example; public APIs, Ticketing Systems (e.g. ServiceNow) and SIEM.
   a. GYTPOL Server sends certain events to a SIEM system such as MicroFocus ArcSight, IBM QRadar, Sentinel or Splunk.

GYTPOL Server Components

The GYTPOL Server is implemented mostly as a set of .NET Core and Node.js microservices interacting with each other through HTTP based REST APIs. Most GYTPOL Server components (i.e. microservices) are deployed as Windows Services allowing granular control over user permissions under which these microservices run.

The functional role and deployment details of each microservice are listed below.

Component	**Platform**	**Port**	**Runs As**	**Role**
UI	Node.js	9093	Windows Service	React.js UI
Reverse Proxy	Node.js	9093	Windows Service	Detach microservices
Update	.NET core	9374	Windows Service	Devices that can't reach GYTPOL Server and send to the GYTPOL Cloud-Component
Validator	.NET core	8080	Windows Service	Group Policy discrepancies between actual and planned
Analyzer	.NET core	8083	Windows Service	Misconfigurations, as well as AD and Benchmark
RsopRepository	.NET core	8082	Windows Service	Intermediate Repo to store the raw data
GpmcProxy	.NET core	5000	Windows Service	Retrieve GP Modeling from DC(s)
AD Security Analysis	PowerShell	9090	Windows Task	Retrieve AD, GP and Benchmark data

Database

Validator, Analyzer and RsopRepository store data in a MS SQL database (local or external). The exact MS SQL connection string is configured during the product installation in the **appsettings.json** file.

The above microservices are automatically created (and upgraded when required) in the underlying databases using the provided connection string.

The following databases are created on the MS SQL server (local or external):

Validator - gytpol_validator, gytpol_profiler, gytpol_joblog
Analyzer - gytpol_analyzer
RsopRepository - gytpol_rsop_reports

How GYTPOL Validator Works: SaaS

As mentioned, GYTPOL Server can be deployed as a SaaS. The biggest difference between SaaS and on-premise solutions is that SaaS solutions are hosted and maintained by a third-party provider, while on-premise solutions are hosted in-house.

GYTPOL SaaS has several regions, and the tenant will be created upon the customer's request.

Once the tenant is created, we request the customer to provide end user email addresses that will be able to access the UI, and an MFA method (OKTA, Azure, Ping, Google, etc) for set up and for group creation via the Access Management.

Similar to the on-prem, the next product deployment step is for distributing client installer **(Windows/Linux/macOS > less than 5MB)** using the organization's software distribution tools such as Microsoft SCCM/InTune, jamf, Tanium, BigFix, Chef, Puppet, Invanti, PDQDeploy etc.

Once deployed, GYTPOL Client installer will collect the misconfigurations data and within a few minutes send it to the server as a gzip format in HTTPS (encrypted; the file is sent to a dedicated container; file size is less than 30kb).

In order to get enhanced security on the Active Directory/Group Policy security items, as well as the benchmark (CIS/NIST), the customer has to install a small component on an on-prem server in order for the data to be sent to a dedicated API for further analysis and action within the tenant.

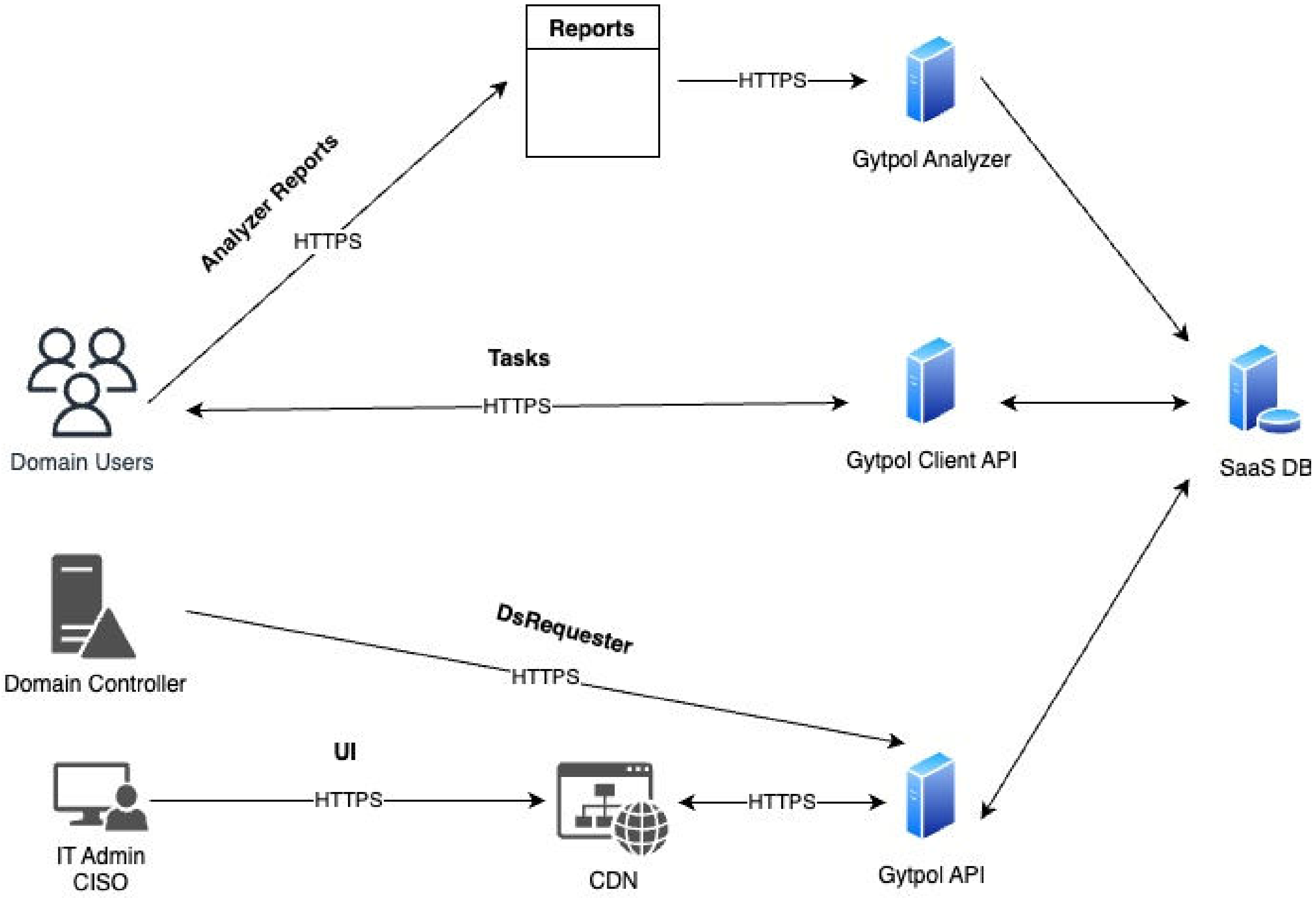


Figure 1. GYTPOL Validator (on-prem) Data Flow

The main GYTPOL Validator data flow takes the following steps:

1. The Customer provides a list of email addresses to access the UI.
   a. The customer can integrate GYTPOL with IDP that is currently used, for example OKTA, Azure AD, Ping and more.
2. The user accesses the UI in HTTPS (highly reliable CDN).
3. GYTPOL provides a list of FW rules (443 port only to SaaS URLs) to whitelist in case of blocks.
4. GYTPOL provides the links to the clients per OS (Windows, Linux and macOS packages).
   a. The clients can also be downloaded from GYTPOL UI.
5. Once the client is installed – it will run once a day, at random times (less than 5 minute duration).
6. During the run – it collects misconfigurations, un-patched zero-days and for MS devices, it also collects Group-Policy data (rsop). (Intune configs for any device will be added soon).

7. GYTPOL Client then compresses the data, encrypts it and sends the data to a dedicated container (HTTPS).
8. The data is analysed by our proprietary GYTPOL Analyzer. The Analyzer not only scrutinizes the data but also archives the findings in a dedicated database, keeping you up-to-date of any potential security risks.
9. In the event that the customer has a Domain Controller and wants to get the Active Directory security analysis and benchmarks like CIS and NIST – another API will be created and a small installation package will be delivered (upon request).
10. GYTPOL Server has several integrations, like: public APIs, ServiceNow and SIEM that will be delivered upon the customer's request.

GYTPOL SaaS Server Components

The GYTPOL Server is implemented as a set of .NET microservices. GYTPOL Server SaaS components (i.e. microservices) are deployed as Kubernetes pods allowing granular control over permissions, network policies and resource limits under with these microservices run.

The functional role and deployment details are listed below.

From	To	Port	Reason
Computers that need UI access	Client UI	443	The UI URL
Computers that need UI access	Client UI	443	URL of the WebSocket API which lets the UI know when fresh data is available
Computers that need UI access	Client UI	443	URL of the API GW that the UI uses for API queries
Endpoints (Clients)	Client UI	443	S3 bucket where reports are sent to
Endpoints (Clients)	Client UI	443	The AWS endpoint of kinesis in their region, used to send metadata of the report and handle the reports queue
Endpoints (Clients)	Client UI	443	URL of the API GW which the agent query to get keys to sign the report
Both	Client UI	443	WebSocket, API queries, client API (soon)

GYTPOL Clients

GYTPOL Supports the following operating systems:

- Windows
- Linux
- macOS

GYTPOL Client runs once a day for a few minutes. During the run – it collects the misconfigurations data, zero-days that weren't addressed properly as well as third party software that are obsolete in their usage.

We elaborate more on GYTPOL Client below.

GYTPOL Client for Windows

- Language-Code: a combination of C# and signed PowerShell
- Post-Install: Task Scheduler
- Permissions: the task schedulers run as a SYSTEM account (it does not need a username and password)
- Size: less than 5MB
- Network Traffic: up to 30KB per day (gzip format)
- Schedule Runs:
    - once a day up to 5 minutes duration (random time: End-User Device between 10am to 5pm; Server between 10pm to 4am);
    - once every hour you will receive a "keep-alive" message and it will pull new tasks for keeping up-to-date and secure (remediation / revert / updates / upgrades).
- Communication Protocol: Latest TLS supported on the device, HTTPS

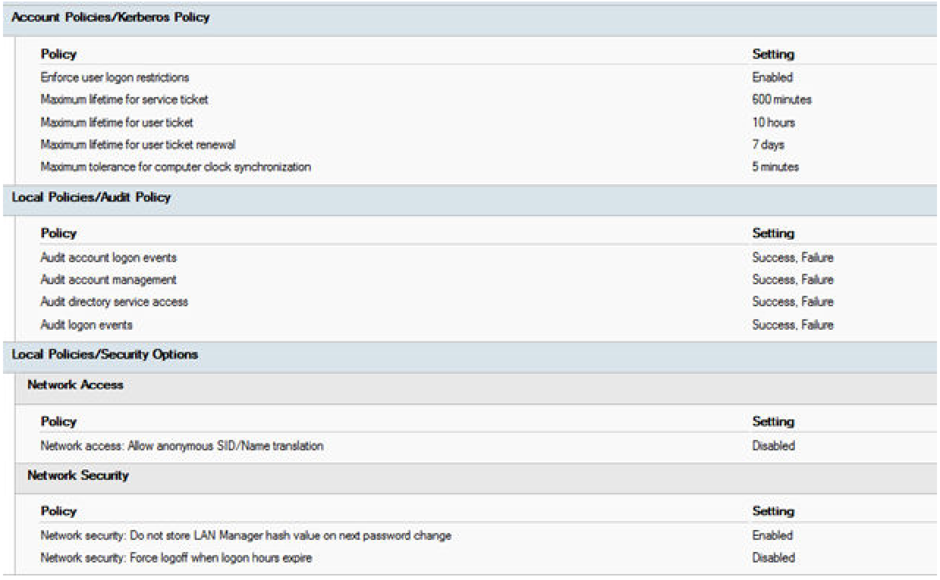
GYTPOL Client for Linux/macOS

- Language-Code: Go lang
- Post-Install: Linux: ***systemd***; macOS: ***launchd***
- Permissions: root user
- Size: less than 3MB
- Network Traffic: up to 30KB per day (gzip format)
- Schedule Runs:
  - once a day, at a random time up to 5 minutes in duration;
  - once in an hour sends "keep-alive" and pulls new tasks to stay up-to-date and secure (remediation/revert/updates/upgrades)
- Communication Protocol: latest TLS supported on the device, HTTPS.

Appendix A - About Microsoft Group Policy

Group Policy is the main, and in many cases the only mechanism to control the configuration of every Windows computer in an organization. It allows what users can and cannot do when using it.

Group Policies are configured in a tool called Group Policy Management Console (GPMC). This is the standard tool provided by Microsoft. GPMC allows you to create and edit Group Policies and configure their Settings. Once Group Policies and Settings are defined, they are applied to various groups of computers and users within my organization.



Account Policies/Kerberos Policy

Policy	Setting
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days
Maximum tolerance for computer clock synchronization	5 minutes

Local Policies/Audit Policy

Policy	Setting
Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	Success, Failure
Audit logon events	Success, Failure

Local Policies/Security Options

Network Access

Policy	Setting
Network access: Allow anonymous SID/Name translation	Disabled

Network Security

Policy	Setting
Network security: Do not store LAN Manager hash value on next password change	Enabled
Network security: Force logoff when logon hours expire	Disabled

Figure 1. Group Policy Settings in GPMC

There are thousands of Settings that control everything ranging from what IE version a user can open, to which locations on the network he can access, even down to what type of desktop wallpaper is compatible

Where a Setting has been modified, the change should be applied to all relevant computers and users that are set as the target for this policy, although there is no practical way to check that the change actually took place and was effective on all its targets, for a variety of reasons

1. When creating or modifying a Group Policy, GPMC doesn't give a clear picture of what the impact of each Setting is.
2. There is no indication when a Setting is irrelevant to the OS and other software installed on the targeted computers.
3. A change may not reach a computer or a user for various reasons, e.g. network outages.
4. The policy might not have been properly enabled and applied to the target group.
5. The computer might not be receiving policy updates because of a configuration problem.
6. Some Settings might be conflicting with other settings that were applied by another policy.

Appendix B - Remote Employees Solution (on-prem only)

Remote employees use computers owned by the employer to work from home, hotels, airports, etc. In many such cases an employee is not connected to the organizational network. Yet, organizations still want their endpoints to be secure. The GYTPOL Validator solution for Remote Employees addresses this use case.

The solution relies on the online service provided by GYTPOL. The service runs on the public cloud infrastructure. It implements a secure pipeline delivering findings provided by the GYTPOL Client installed on the endpoint to the GYTPOL Server running on-prem. The solution is End to End Encrypted!

The solution implements the following steps:

- GYTPOL Client is enabled for the Remote Employees Solution during installation.
- GYTPOL Client runs its scan.
- GYTPOL Client identifies that the internal NW is not accessible.
- GYTPOL Client sends the results to the GYTPOL Online Service.
- GYTPOL Online Service receives data sent by GYTPOL Clients.
- GYTPOL Online Service keeps received data in the multitenant Data Store.
- GYTPOL On-prem Server periodically pulls new data from GYTPOL Online Service.
- GYTPOL Online Service sends data to GYTPOL On-prem Server.
- GYTPOL On-prem Server stores the new data.
- GYTPOL On-prem Server requests GYTPOL On-prem Server to delete the new data.
- GYTPOL Online Service deletes data upon a request from GYTPOL On-prem Server.
- GYTPOL Online Service deletes remaining data upon Time-To-Live expiration.

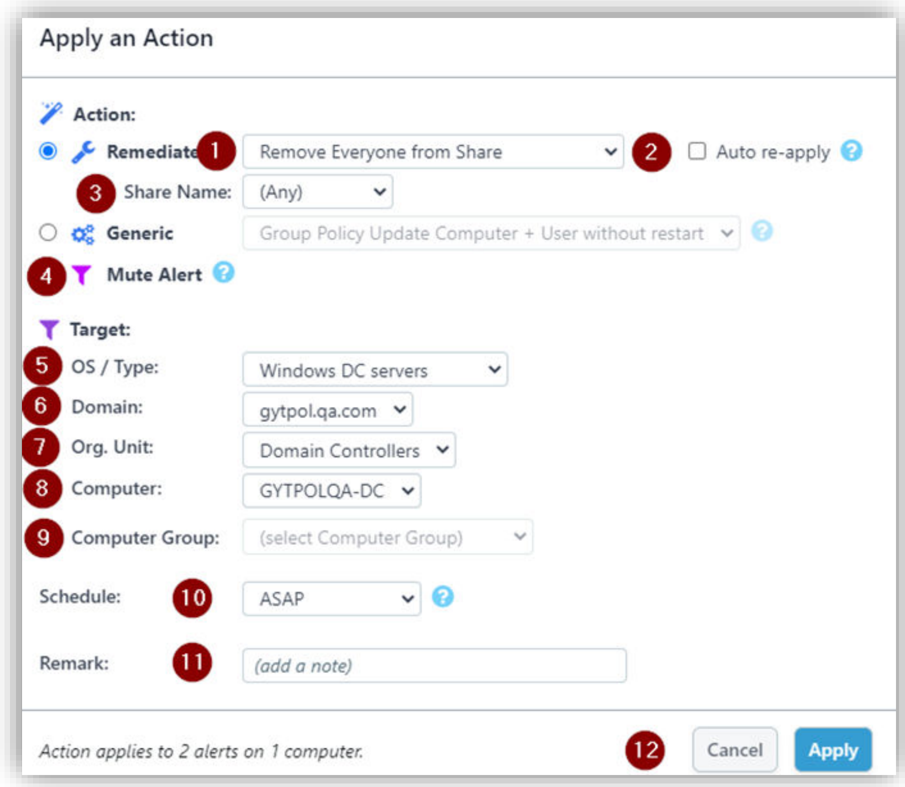
Appendix C – Taking Actions on GYTPOL

More information can be found under the User Guide on our website.

Once data is shown in the UI – necessary action is applied.
In GYTPOL we provide certain actions: remediation, auto-remediation, mute, generic actions and revert.

Remediation Action

After the wrench is clicked, please apply an action as needed:



Apply an Action

Action:

● Remediate: Remove Everyone from Share □ Auto re-apply

Share Name: (Any)

○ Generic: Group Policy Update Computer + User without restart

Mute Alert

Target:

OS / Type: Windows DC servers

Domain: gytpol.qa.com

Org. Unit: Domain Controllers

Computer: GYTPOLQA-DC

Computer Group: (select Computer Group)

Schedule: ASAP

Remark: (add a note)

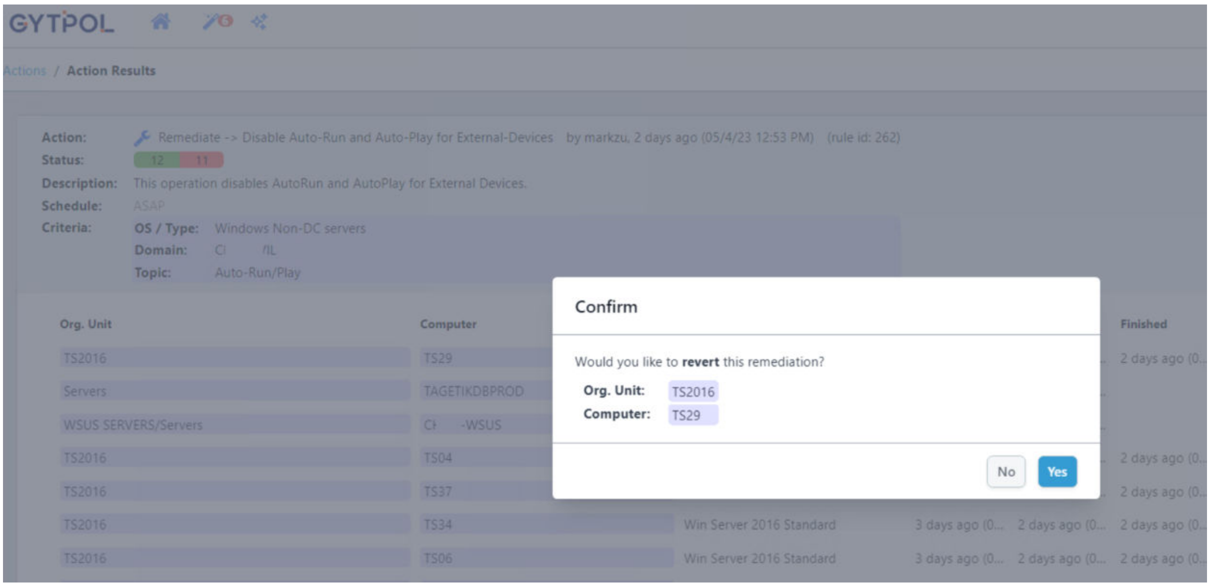
Action applies to 2 alerts on 1 computer.

1. Specifies the necessary action. In our example we want to remediate **SMB Everyone Shares**.
2. The **auto re-apply** option will apply the same remediation to any new GYTPOL client that is reporting for the first time or falling under the criteria of the selected remediation.
3. Shows the **share name** we want to remediate, either individually or "Any" which will remediate every share on the selected scope of devices.
4. **Mute Alert**: if we are aware of the finding and we want to suppress the alert (it won't be shown in the UI).

5. **OS / Type**: shows which operating system we want to perform the remediation In. In this example, it is our Domain controllers.
6. In a case where we have several domains reporting to the UI, we can choose in which **domain** to perform the remediation.
7. **Org. Unit**: shows which organization unit we want to perform the remediation. If we choose 'Any', it will be processed on any organization unit.
8. **Computer**: shows which server or endpoint we want to perform the remediation. If we click on 'Any' it will be processed on all the computers that are in the same organization unit.
9. **Computer Group**: Here, you can create your own groups, based on name masks, OUs etc. This group isn't a part of the OUs structure and can be modified at any time.
10. **Schedule:** The remediation can be performed ASAP (based on an hourly trigger) or can be scheduled to another time slot that is more convenient to perform the operation at.
11. **Remark**: gives the option to add an internal comment regarding the change.
12. **Apply / Cancel**: whether to confirm or cancel the remediation.

Revert Action

This is processed via the actions screen, and can be executed on all the devices in scope or only one selected device.



Actions / Action Results

Action: Remediate -> Disable Auto-Run and Auto-Play for External-Devices by markzu, 2 days ago (05/4/23 12:53 PM) (rule id: 262)
Status: 12 11
Description: This operation disables AutoRun and AutoPlay for External Devices.
Schedule: ASAP
Criteria: OS / Type: Windows Non-DC servers
Domain: Cl /IL
Topic: Auto-Run/Play

Org. Unit	Computer				Finished
TS2016	TS29				2 days ago (0...
Servers	TAGETIKDBPROD				
WSUS SERVERS/Servers	Cł -WSUS				
TS2016	TS04				2 days ago (0...
TS2016	TS37				2 days ago (0...
TS2016	TS34	Win Server 2016 Standard	3 days ago (0...	2 days ago (0...	2 days ago (0...
TS2016	TS06	Win Server 2016 Standard	3 days ago (0...	2 days ago (0...	2 days ago (0...

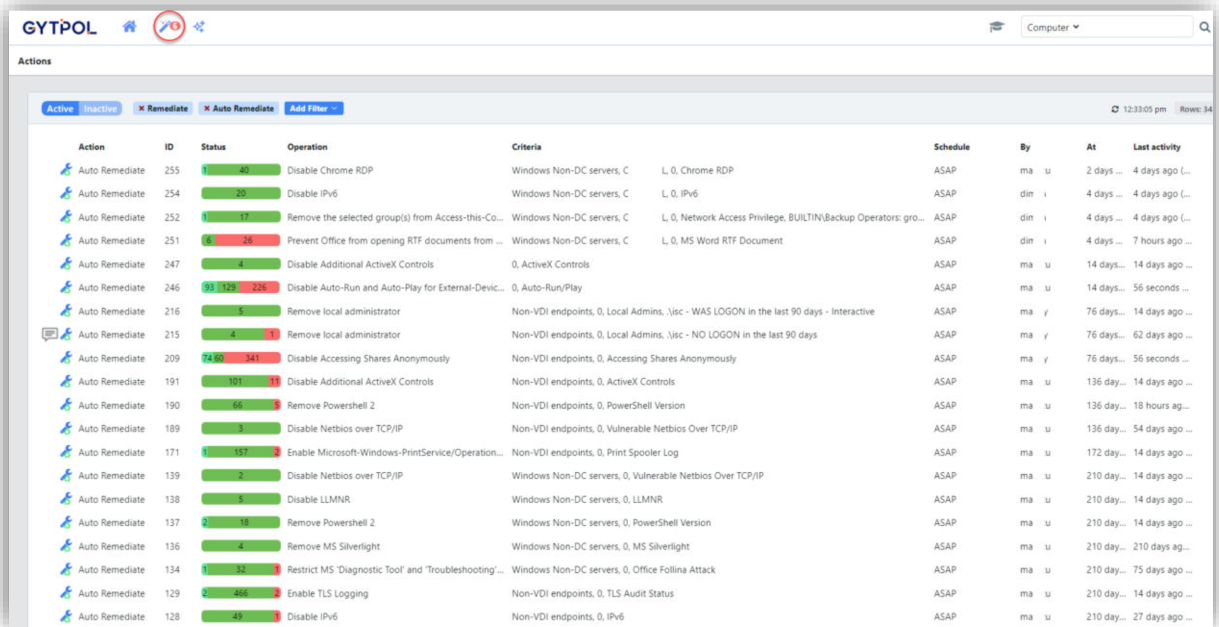
Confirm

Would you like to **revert** this remediation?

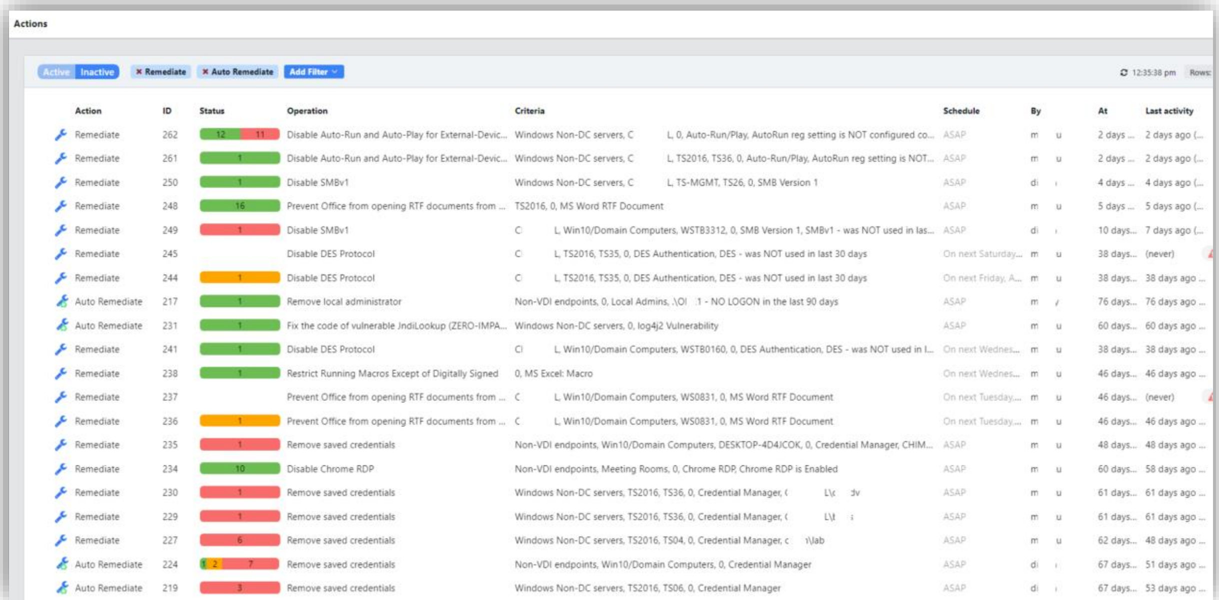
Org. Unit: TS2016
Computer: TS29

Action Screen

Screen that shows all the running devices (one-time or auto-reapply) or finished tasks.



Action	ID	Status	Operation	Criteria		Schedule	By		At	Last activity
Auto Remediate	255	1 40	Disable Chrome RDP	Windows Non-DC servers, C	L, 0, Chrome RDP	ASAP	ma	u	2 days ...	4 days ago (...
Auto Remediate	254	20	Disable IPv6	Windows Non-DC servers, C	L, 0, IPv6	ASAP	dir	ı	4 days ...	4 days ago (...
Auto Remediate	252	1 17	Remove the selected group(s) from Access-this-Co...	Windows Non-DC servers, C	L, 0, Network Access Privilege, BUILTIN\Backup Operators: gro...	ASAP	dir	ı	4 days ...	4 days ago (...
Auto Remediate	251	6 26	Prevent Office from opening RTF documents from ...	Windows Non-DC servers, C	L, 0, MS Word RTF Document	ASAP	dir	ı	4 days ...	7 hours ago ...
Auto Remediate	247	4	Disable Additional ActiveX Controls	0, ActiveX Controls		ASAP	ma	u	14 days...	14 days ago ...
Auto Remediate	246	93 129 226	Disable Auto-Run and Auto-Play for External-Devic...	0, Auto-Run/Play		ASAP	ma	u	14 days...	56 seconds ...
Auto Remediate	216	5	Remove local administrator	Non-VDI endpoints, 0, Local Admins, .\isc - WAS LOGON in the last 90 days - Interactive		ASAP	ma	y	76 days...	14 days ago ...
Auto Remediate	215	4 1	Remove local administrator	Non-VDI endpoints, 0, Local Admins, .\isc - NO LOGON in the last 90 days		ASAP	ma	y	76 days...	62 days ago ...
Auto Remediate	209	74 60 341	Disable Accessing Shares Anonymously	Non-VDI endpoints, 0, Accessing Shares Anonymously		ASAP	ma	y	76 days...	56 seconds ...
Auto Remediate	191	101 11	Disable Additional ActiveX Controls	Non-VDI endpoints, 0, ActiveX Controls		ASAP	ma	u	136 day...	14 days ago ...
Auto Remediate	190	66 5	Remove Powershell 2	Non-VDI endpoints, 0, PowerShell Version		ASAP	ma	u	136 day...	18 hours ag...
Auto Remediate	189	3	Disable Netbios over TCP/IP	Non-VDI endpoints, 0, Vulnerable Netbios Over TCP/IP		ASAP	ma	u	136 day...	54 days ago ...
Auto Remediate	171	1 157 2	Enable Microsoft-Windows-PrintService/Operation...	Non-VDI endpoints, 0, Print Spooler Log		ASAP	ma	u	172 day...	14 days ago ...
Auto Remediate	139	2	Disable Netbios over TCP/IP	Windows Non-DC servers, 0, Vulnerable Netbios Over TCP/IP		ASAP	ma	u	210 day...	14 days ago ...
Auto Remediate	138	5	Disable LLMNR	Windows Non-DC servers, 0, LLMNR		ASAP	ma	u	210 day...	14 days ago ...
Auto Remediate	137	2 18	Remove Powershell 2	Windows Non-DC servers, 0, PowerShell Version		ASAP	ma	u	210 day...	14 days ago ...
Auto Remediate	136	4	Remove MS Silverlight	Windows Non-DC servers, 0, MS Silverlight		ASAP	ma	u	210 day...	210 days ag...
Auto Remediate	134	1 32 1	Restrict MS 'Diagnostic Tool' and 'Troubleshooting'...	Windows Non-DC servers, 0, Office Follina Attack		ASAP	ma	u	210 day...	75 days ago ...
Auto Remediate	129	2 466 2	Enable TLS Logging	Non-VDI endpoints, 0, TLS Audit Status		ASAP	ma	u	210 day...	14 days ago ...
Auto Remediate	128	49 1	Disable IPv6	Non-VDI endpoints, 0, IPv6		ASAP	ma	u	210 day...	27 days ago ...



Action	ID	Status	Operation	Criteria		Schedule	By		At	Last activity
Remediate	262	12 11	Disable Auto-Run and Auto-Play for External-Devic...	Windows Non-DC servers, C	L, 0, Auto-Run/Play, AutoRun reg setting is NOT configured co...	ASAP	m	u	2 days ...	2 days ago (...
Remediate	261	1	Disable Auto-Run and Auto-Play for External-Devic...	Windows Non-DC servers, C	L, TS2016, TS36, 0, Auto-Run/Play, AutoRun reg setting is NOT...	ASAP	m	u	2 days ...	2 days ago (...
Remediate	250	1	Disable SMBv1	Windows Non-DC servers, C	L, TS-MGMT, TS26, 0, SMB Version 1	ASAP	di	ı	4 days ...	4 days ago (...
Remediate	248	16	Prevent Office from opening RTF documents from ...	TS2016, 0, MS Word RTF Document		ASAP	m	u	5 days ...	5 days ago (...
Remediate	249	1	Disable SMBv1	C	L, Win10/Domain Computers, WSTB3312, 0, SMB Version 1, SMBv1 - was NOT used in las...	ASAP	di	ı	10 days...	7 days ago (...
Remediate	245		Disable DES Protocol	C	L, TS2016, TS35, 0, DES Authentication, DES - was NOT used in last 30 days	On next Saturday...	m	u	38 days...	(never)
Remediate	244	1	Disable DES Protocol	C	L, TS2016, TS35, 0, DES Authentication, DES - was NOT used in last 30 days	On next Friday, A...	m	u	38 days...	38 days ago ...
Auto Remediate	217	1	Remove local administrator	Non-VDI endpoints, 0, Local Admins, .\OI 1 - NO LOGON in the last 90 days		ASAP	m	y	76 days...	76 days ago ...
Auto Remediate	231	1	Fix the code of vulnerable JndiLookup (ZERO-IMPA...	Windows Non-DC servers, 0, log4j2 Vulnerability		ASAP	m	u	60 days...	60 days ago ...
Remediate	241	1	Disable DES Protocol	Ci	L, Win10/Domain Computers, WSTB0160, 0, DES Authentication, DES - was NOT used in l...	On next Wednes...	m	u	38 days...	38 days ago ...
Remediate	238	1	Restrict Running Macros Except of Digitally Signed	0, MS Excel: Macro		On next Wednes...	m	u	46 days...	46 days ago ...
Remediate	237		Prevent Office from opening RTF documents from ...	C	L, Win10/Domain Computers, WS0831, 0, MS Word RTF Document	On next Tuesday....	m	u	46 days...	(never)
Remediate	236	1	Prevent Office from opening RTF documents from ...	C	L, Win10/Domain Computers, WS0831, 0, MS Word RTF Document	On next Tuesday....	m	u	46 days...	46 days ago ...
Remediate	235	1	Remove saved credentials	Non-VDI endpoints, Win10/Domain Computers, DESKTOP-4D4JCOK, 0, Credential Manager, CHIM...		ASAP	m	u	48 days...	48 days ago ...
Remediate	234	10	Disable Chrome RDP	Non-VDI endpoints, Meeting Rooms, 0, Chrome RDP, Chrome RDP is Enabled		ASAP	m	u	60 days...	58 days ago ...
Remediate	230	1	Remove saved credentials	Windows Non-DC servers, TS2016, TS36, 0, Credential Manager, (L\c dv		ASAP	m	u	61 days...	61 days ago ...
Remediate	229	1	Remove saved credentials	Windows Non-DC servers, TS2016, TS36, 0, Credential Manager, (L\t		ASAP	m	u	61 days...	61 days ago ...
Remediate	227	6	Remove saved credentials	Windows Non-DC servers, TS2016, TS04, 0, Credential Manager, c \lab		ASAP	m	u	62 days...	48 days ago ...
Auto Remediate	224	1 2 7	Remove saved credentials	Non-VDI endpoints, Win10/Domain Computers, 0, Credential Manager		ASAP	di	ı	67 days...	51 days ago ...
Auto Remediate	219	3	Remove saved credentials	Windows Non-DC servers, TS2016, TS06, 0, Credential Manager		ASAP	di	ı	67 days...	53 days ago ...