Cymulate

PoC Pre-Requirements

Technical Document

Cymulate agent requirements

Before running assessments that test your cybersecurity posture, you first need to deploy the Cymulate agent.

- **Service-based agent** – This agent is service-based and has a more scalable and modular architecture. One of the main benefits of the service-based agent is that the user does not need to be logged in to run assessments. Currently available for Windows 64-bit systems only.

The following system requirements are relevant for both legacy and service-based agents.

System requirements

Criteria	Minimum Requirement	Recommended
CPU	2 Cores	4 Cores
Memory (RAM)	8 GB	16 GB
Disk Space	30 GB	60 GB
Network	One Network Interface	One Network Interface

Communication requirements

The following communication requirements are relevant for both legacy and service-based agents.

To perform security assessments on a network, it is necessary for the Cymulate Agent to be able to communicate with the Cymulate platform. This communication requires HTTPS and is required for managing agents and performing attacks.
If a firewall is present between the Cymulate Agent and the Cymulate platform, certain ports need to be opened either directly or through a proxy to enable the required communication.

Source	Destination	Port	Description
Cymulate Agent Machine	Cymulate Cloud Domain ***.app.cymulate.com** ***.us-app.cymulate.com**	443 HTTPS	Essential communication between the Cymulate Agent and the Cymulate cloud platform

Supported operating systems for Cymulate Agent (SBA)

OS type	OS	Version	Architecture
Windows	Windows 10 Client	1607+	x64,
	Windows 11	22000+	x64
	Windows Server	2012+	x64
	Windows Server Core	2012+	x64
	Nano Server	1809+	x64
Mac	Mac	10.15+	x64
Linux	Alpine Linux	3.12+	x64
	CentOS	7+	x64
	Debian	10+	x64
	Fedora	33+	x64
	openSUSE	15+	x64
	Red Hat Enterprise Linux	7+	x64
	SUSE Enterprise Linux (SLES)	12 SP2+	x64
	Ubuntu	16.04, 18.04, 20.04+	x64

Important Note:

Remember that if your mainly case is Security Control Validation, we must have a baseline computer from your company. You can use for example the same image is deployed to every new employee, it also must include all applications that the users use (Microsoft Office and Adobe for example) also it must include your official Antivirus Solution Installed.

It`s recommended also you have a dedicated domain username account with password (to be inserted in the platform) and a dedicated user mailbox for the PoC. (As this mailbox will receive a lot of samples of malwares it is not recommended you use production ones).

If the company have a proxy, please be sure this computer access the internet though proxy also.

Based on that explanation, please see the following checklist for your PoC Computer:

Item	Description
Company Anti-Virus (EPP, ERD) Installed	If one of the use cases is check your Endpoint Security posture please have it.
Proxy Access (If Applicable)	If the company have a proxy, please be sure this computer access the internet though proxy also
Acrobat Reader (If Applicable)	If users usually have Acrobat Reader installed on their computer, install it.
Microsoft Office (If Applicable)	If the company use Microsoft Office, install it.
Dedicated Mailbox	If one of the use cases is check your Mail Security posture please have it.
Dedicated Network Username	Malwares behaviors will be simulated with the account logged on the computer. To be sure not to impact any production account, we recommend you to have a dedicated account.

Exclusions

The HTTPS/443 traffic between the Cymulate agent and the Cymulate platform should be excluded from any mechanisms such as anti-malware, URL filtering ,etc.

EU URL exclusions

The following list displays the required EU URL exclusions and what they are relevant for.

- **app.cymulate.com** - Access to Cymulate platform
- **ws.app.cymulate.com** - Web socket
- **agent.app.cymulate.com** - For **legacy agent** to cloud communication, getting instructions, and updating results and statuses from the agent.
- **agents.app.cymulate.com** - For **service-based agent** to cloud communication, getting instructions, and updating results and statuses from the agent.
- **cyagent.app.cymulate.com** - For **service-based agent** to cloud communication, for getting instructions and updating results and statuses from the agent.
- **agentlogs.app.cymulate.com** - The **service-based agent** sends logs to this URL.
- **api.app.cymulate.com** - For users that use the **Cymulate REST API**.
- **edr-resources.app.cymulate.com** -Where the agent downloads resources for **Endpoint Security** assessments.
- **dlp-resources.app.cymulate.com** - Where the agent downloads resources for **Data Exfiltration** assessments.
- **cypy.app.cymulate.com** - Advanced Scenarios

US URL exclusions

The following list displays the required US URL exclusions and what they are relevant for.

- **us-app.cymulate.com** - Access to Cymulate platform
- **ws.us-app.cymulate.com** - Web socket
- **agent.us-app.cymulate.com** - For **legacy agent** to cloud communication, getting instructions, and updating results and statuses from the agent.
- **agents.us-app.cymulate.com -** For **service-based agent** to cloud communication, getting instructions, and updating results and statuses from the agent.
- **cyagent.us-app.cymulate.com** - For **service-based agent** to cloud communication, for getting instructions and updating results and statuses from the agent.
- **agentlogs.us-app.cymulate.com** - The **service-based agent** sends logs to this URL.
- **api.us-app.cymulate.com** - For users that use the **Cymulate REST API**.
- **edr-resources.us-app.cymulate.com** - Where the agent downloads resources for **Endpoint Security** assessments.
- **dlp-resources.us-app.cymulate.com** - Where the agent downloads resources for **Data Exfiltration** assessments.
- **cypy.app.cymulate.com** - Advanced Scenarios

Private tenant exclusions

The following list displays the private tenant URL exclusions and what they are relevant for.

- **{tenantName}-agent.cymulate.com** - Legacy agent
- **{tenantName}-cyagent.cymulate.com** - Service-based agent

Directory exclusions

Some directories must be excluded/whitelisted for the assessments to run properly. Based on your operating system, exclude the following directories **(and their sub-folders)** on your security controls. Your security controls must also allow downloading encrypted files to these paths.

- Windows -Legacy agents (x64 and x86)
  - **C:\Program Files\Cymulate\Agent**
  - **C:\ProgramData\cymulate\Agent**
- Windows – Service-based agents (x64)
  - **C:\Program Files\Cymulate\Agent**
  - **C:\ProgramData\Cymulate\Agent**
- Mac
  - **/Applications/Cymulate/Agent**
  - **/Users/Shared/Cymulate/Agent**
- Linux
  - **/usr/lib/Cymulate/Agent/**
  - **/usr/share/Cymulate/Agent/**

Cymulate Mac and Linux Agents must be installed and run with root privileges.
For more information on adding exclusions in your security products, see Configuring Exclusions in Security Products.

Module-specific requirements

Email Gateway requirements

1. Set up a dedicated mailbox under your email domain (ex. cymulate@example.com).
2. Exclude one of the following from anti-spam filtering:
   - IP address - **168.245.119.24**
   - Domain - **cymulatemailgateway.com** (EU users only).

Supported email platforms

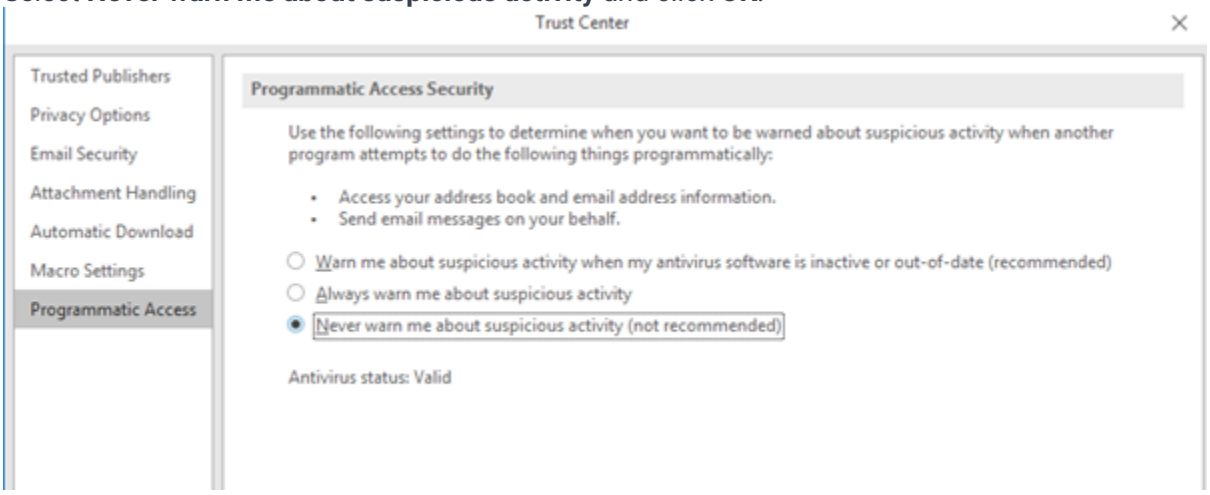
The Cymulate Agent supports multiple communication options with a dedicated mailbox:

- **Microsoft Exchange** - HTTP connection to Microsoft Exchange (Preferred). The agent will prompt for user mailbox credentials and exchange server IP/Hostname address.
- **Office 365** - HTTP connection via Office 365 API (Preferred).
- **Gmail** - IMAP connection via GSuite. To configure Gmail to work with the Cymulate agent, please refer to the Gmail push notifications configuration guide.
- **Outlook client (SMTP)*** - available for legacy agents and Windows OS only - Connecting to an Outlook application running on the local machine that the Cymulate agent is installed. The Cymulate agent will use Outlook COM object to monitor incoming /outgoing email traffic using Outlook (Outlook 2010 and above is required).

Please follow the next steps to enable Cymulate Agent to use the Outlook API:

1. Add cymulate.com domain to Safe Senders List in Outlook (How Do I Add a Domain to Safe Senders in Outlook?)
2. In Outlook, go to **File > Options**.
3. Click **Trust Center,** and then click **Trust Center Settings**.
4. Click **Programmatic Access.**

5. Select **Never warn me about suspicious activity** and click **OK**.



Web Application Firewall (WAF) requirements

Exclude the following IP addresses from anti-bot/anti-DDoS protection:

- EU
  - **54.217.50.18**
  - **52.208.202.111**
  - **52.49.144.209**
- US
  - **54.237.172.129**
  - **35.169.219.115**
  - **52.4.48.52**

Endpoint Security requirements

If your security control is unable to whitelist *.app.cymulate.com/*.us-app.cymulate.com whitelist the following URL:

- EU
  - **edr-resources.app.cymulate.com**
- US
  - **edr-resources.us-app.cymulate.com**

Data Exfiltration requirements

If your security control is unable to whitelist *.app.cymulate.com/*.us-app.cymulate.com whitelist the following URL:

- EU
  - **dlp-resources.app.cymulate.com**
- US
  - **dlp-resources.us-app.cymulate.com**

Exclude the following from URL filtering/firewall controls to perform Data Exfiltration assessments **(EU users only):**

- EU
    - **52.212.231.13**
    - **54.74.6.42**
    - **p3ns.cymulatedlp.com**
    - **p4ns.cymulatedlp.com**
    - **allports.cymulatedlp.com**

Some exfiltration methods test network security controls, while others test the DLP solution. You may need to exclude the above IPs/Domains so that the methods are not blocked by the network security controls and can be tested properly by the DLP solution.

Advanced Scenarios requirements

Whitelist the following URL:

- EU and US:
    - **cypy.app.cymulate.com**

Phishing Awareness requirements

Exclude the following from anti-spam or anti-phishing protection:

- EU:
    - **168.245.71.63.**
    - **support-eu.lionnets.com**
- US:
    - **168.245.71.63.**
    - **support-us.lionnets.com**

Hopper requirements

Whitelist the Hopper binary hash on all machines in the network:

File Name: CymulateLM.exe
MD5: 7e1c9df044bcafe8e5a4372793985368
SHA-256: db5f25b745f701d905d5d6f3979f9d4aec2ae22ad8f5bb66c428324b5e25b0a4
SHA-1: 18076280e739af9c4c8c93ef99e6a20777c80ff5

File name: CymulateLM64.exe

MD5: 62b9e0dfd0ef2cd88fdcd412523c7d9f
SHA256: 2a01f07131420d454f9da5742b33e3ec755b4499199269a75fbf1476e18c18c6
SHA1: 34332fb1cb2035c1f11d15e6765d334588dba836