Harmony Endpoint Cloud Client Connectivity Requirements

Product
Harmony Endpoint - General

Version
Cloud

Last Modified
2025-02-26

Solution

Introduction

Harmony Endpoint requires access to the Internet (either directly, or via configured proxy).

The table below lists the relevant connectivity requirements for each blade,
as well as how to test it in order to verify the connectivity.

* Notes:

- Authenticated proxies which require username and password are not supported.
- The new tool *CheckConnectivity.exe* is supplied with client versions E85.10 and higher. It helps to determine that all the online services which are required by the Endpoint client are accessible. This tool is located under the Endpoint folder: **C:\Program Files (x86)\CheckPoint\Endpoint Security\Endpoint Common\bin**.

Windows Client URLs

Show / Hide this section

#	Hostname/URL	Protocol	Used For (Version)	Verifying Connectivity (Run command listed below. You will get a response if connectivity is OK)
			General	
1	*.epmgmt.checkpoint.com See comment 1 below	https	• Client-Server communication • Load Balancing and Failover Routing purposes • -hap2 & -hap21 (Ireland, EU) • -hap5 & -hap51 (London, United Kingdom) • -hap1 & -hap11 (N. Virginia, USA) • -hap3 & -hap31 (Sydney, Australia) • -hap4 & -hap41 (Mumbai, India) • Exporting log to SIEM solutions • Patch management feature in clients • During HEP upgrades Source of files • Server Profiles Feature • Forensic reports upload • Updates for endpoint • Application Control	
2	dl3.checkpoint.com See comment 2 below	https	SBA Signature updates	`curl_cli [--proxy <IP_or_HostName:Port>] -v -k dl3.checkpoint .com`

3	gwevents.checkpoint.com	https	Statistics collection	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k gwevents.checkpoint.com**
4	ftp-proxy.checkpoint.com	https	Uploading CPInfo	
5	teadv.checkpoint.com See comment 1 below	https	US-DHS and EU compliant Anti-Malware engine and signature updates	**curl -v -k -X GET http://teadv.checkpoint.com/epupdates/86.50/0190/v1.xml**
6	updates.checkpoint.com	https	SBA Signature updates	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k updates.checkpoint.com**
7	sc1.checkpoint.com	http https	Retrieve URL for bot detection server Retrieve Firefox Browser Extension and Browser Extension feature flags	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k** http://sc1.checkpoint.com/EPcws/TCUrlsFormat.txt
			Anti-Bot and URL Filtering	
8	cws.checkpoint.com	https	Anti-Bot URL reputation	curl -v http://cws.checkpoint.com/Malware/SystemStatus/type/short
9	secureupdates.checkpoint.com	http	Signatures database updates	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k** http://secureupdates.checkpoint.com/AMW/Version
			Anti-Malware E2 (US-DHS and EU compliant)	
10	sophosxl.com s.sophosxl.net	dns	Live Protection (E87.50 and higher)	
			Anti-Ransomware, Behavioral Guard and Forensics	
11	Show / Hide this section See comment 3 below	https	Threat Hunting data upload	
			Threat Emulation	
12	*.iaas.checkpoint.com See comment 4 below	https	• File reputation service (Horizon IOC) • URL reputation service (Horizon IOC) • Malware service (Horizon IOC) • Interaction with Threat Emulation cloud	
13	rep.checkpoint.com	https	ThreatCloud File Reputation service	
			Browser Extension	
14	cloudinfra-gw.portal.checkpoint.com	https	Uploading files for scanning JWT generation for Zero Phishing JWT generation for DLP JWT generation for EDR	
15	web-rep.checkpoint.com	https	Zero Phishing	
16	microsoftedge.microsoft.com edge.microsoft.com	https	Microsoft Store	
17	www.google.com/chrome/ clients2.googleusercontent.com clients2.google.com	https	Google services	

macOS Client URLs

Show / Hide this section

#	Hostname/URL	Protocol	Used For (Version)	Verifying Connectivity (Run command listed below. You will get a response if connectivity is OK)
			General	
1	*.epmgmt.checkpoint.com See comment 1 below	https	• Client-Server communication • Load Balancing and Failover Routing purposes • -hap2 & -hap21 (Ireland, EU) • -hap5 & -hap51 (London, United Kingdom) • -hap1 & -hap11 (N. Virginia, USA) • -hap3 & -hap31 (Sydney, Australia) • -hap4 & -hap41 (Mumbai, India) • Offline reputation updates (E88.10 and higher) • Forensic reports upload • Anti-Malware engine and signature updates • Uploading CPInfo	
2	gwevents.checkpoint.com	https	Statistics collection	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k gwevents.checkpoint.com**
3	rep.checkpoint.com	https	ThreatCloud File Reputation service	
			Anti-Bot and URL Filtering	
4	cws.checkpoint.com	https	Anti-Bot URL reputation	curl -v http://cws.checkpoint.com/Malware/SystemStatus/type/short
			Anti-Malware	
5	sophosxl.com s.sophosxl.net	dns	Live Protection	
			Anti-Ransomware and Forensics	
6	Show / Hide this section See comment 3 below	https	Threat Hunting data upload	
			Browser Extension	
7	cloudinfra-gw.portal.checkpoint.com	https	Uploading files for scanning JWT generation for Zero Phishing JWT generation for EDR	
8	sc1.checkpoint.com	https	Retrieve Firefox Browser Extension and Browser Extension feature flags	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k** http://sc1.checkpoint.com/EPcws/TCUrlsFormat.txt
9	web-rep.checkpoint.com	https	Zero Phishing	
10	microsoftedge.microsoft.com edge.microsoft.com	https	Microsoft Store	
11	www.google.com/chrome/ clients2.googleusercontent.com clients2.google.com	https	Google services	

Linux Client URLs

Show / Hide this section

#	Hostname/URL	Protocol	Used For (Version)	Verifying Connectivity (Run command listed below. You will get a response if connectivity is OK)
			General	
1	*.epmgmt.checkpoint.com See comment 1 below	https	• Client-Server communication • Load Balancing and Failover Routing purposes • -hap2 & -hap21 (Ireland, EU) • -hap5 & -hap51 (London, United Kingdom) • -hap1 & -hap11 (N. Virginia, USA) • -hap3 & -hap31 (Sydney, Australia) • -hap4 & -hap41 (Mumbai, India) • Exporting log to SIEM solutions • During HEP upgrades Source of files	
2	*.iaas.checkpoint.com	https	Threat Hunting authorization	
3	gwevents.checkpoint.com	https	Statistics collection	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k gwevents.checkpoint.com**
4	rep.checkpoint.com	https	ThreatCloud File Reputation service	
5	secureupdates.checkpoint.com	http	Packages download Signatures database updates	**curl_cli [--proxy <IP_or_HostName:Port>] -v -k** http://secureupdates.checkpoint.com/AMW/Version
6	teadv.checkpoint.com	https	Anti-Malware engine and signature updates	**curl_cli -v -k http://teadv.checkpoint.com/epupdates/86.50/0190/v1.xml**
7	Show / Hide this section See comment 3 below	https	Threat Hunting data upload	

Comments

Show / Hide this section

1. *.epmgmt.checkpoint.com:
   - <Connection Token>.epmgmt.checkpoint.com
     For example: HEPDemo-d9e265f1-hap2.epmgmt.checkpoint.com
   - <server name-auto generated characters-region>
     - For example: HEPDemo-d9e265f1-hap21
     - Main URL used for Client-Server Communication (Ireland, EU): HEPDemo-d9e265f1-hap2
     - Main URL used for Client-Server Communication (London, United Kingdom): HEPDemo-d9e265f1-hap5
     - Secondary URL used for Client-Server Communication (Ireland, EU): HEPDemo-d9e265f1-hap21
     - Secondary URL used for Client-Server Communication (London, United Kingdom): HEPDemo-d9e265f1-hap51
   - <server name-auto generated characters-region>
     - For example: HEPDemo-d9e265f1-hap11
     - Main URL used for Client-Server Communication (N. Virginia, USA): HEPDemo-d9e265f1-hap1
     - Secondary URL used for Client-Server Communication (N. Virginia, USA): HEPDemo-d9e265f1-hap11
   - <server name-auto generated characters-region>
     - For example: HEPDemo-d9e265f1-hap31
     - Main URL used for Client-Server Communication (Sydney, Australia): HEPDemo-d9e265f1-hap3
     - Main URL used for Client-Server Communication (Mumbai, India): HEPDemo-d9e265f1-hap4
     - Secondary URL used for Client-Server Communication (Sydney, Australia): HEPDemo-d9e265f1-hap31
     - Secondary URL used for Client-Server Communication (Mumbai, India): HEPDemo-d9e265f1-hap41
   - During HEP upgrades Source of files: endpoint-cdn.epmgmt.checkpoint.com

- Server Profiles Feature: ep-repo.epmgmt.checkpoint.com
- Forensic reports upload: sba-data-collection.iaas.checkpoint.com (this URL is specifically required, in addition to *.epmgmt.checkpoint.com, for Windows versions below E88.10 and macOS versions below E88.30)
- Updates for endpoint: teadv.checkpoint.com (this URL is specifically required, in addition to *.epmgmt.checkpoint.com, for Windows versions below E88.10)
- Application Control: teadv.checkpoint.com (this URL is specifically required, in addition to *.epmgmt.checkpoint.com, for Windows versions below E88.30)
- US-DHS and EU compliant Anti-Malware engine and signature updates: teadv.checkpoint.com (this URL is specifically required, in addition to *.epmgmt.checkpoint.com, for Windows versions below E88.50 and macOS versions below E88.20)
- Offline reputation updates (E88.10 and higher): updates.checkpoint.com (this URL is specifically required, in addition to *.epmgmt.checkpoint.com, for macOS versions below E88.30)
- Uploading CPInfo (these URLs are specifically required, in addition to *.epmgmt.checkpoint.com, for macOS versions below E88.20):
  - ftp-proxy.checkpoint.com
  - services.checkpoint.com

2. In China use: dl3.checkpoint.com.cn
3. For DT1 use: europe-west1-datatube-240519.cloudfunctions.net
4. *.iaas.checkpoint.com:
   - File reputation service (Horizon IOC): file-rep.iaas.checkpoint.com
   - URL reputation service (Horizon IOC): url-rep.iaas.checkpoint.com
   - Malware service (Horizon IOC): threatcloud.iaas.checkpoint.com
   - Interaction with Threat Emulation cloud: te.iaas.checkpoint.com
5. For LogExporter use the following inbound rules:
   - Ap-south-1:
     - 13.237.215.109
     - 3.25.28.241
     - 3.105.14.157
     - ap-south-1.allowed-ips.checkpoint.com:
       - 15.206.182.35
       - 35.154.171.21
   - Ap-southeast-2:
     - 13.237.215.109
     - 3.25.28.241
     - 3.105.14.157
     - ap-southeast-2.allowed-ips.checkpoint.com:
       - 52.64.37.249
       - 3.105.139.243
       - 3.105.14.157
   - Eu-west-1:
     - 34.248.94.75
     - 54.220.66.248
     - 54.228.200.90
     - eu-west-1.allowed-ips.checkpoint.com:
       - 46.51.203.128
       - 52.210.248.134
       - 54.220.66.248
   - Eu-west-2:
     - 34.248.94.75
     - 54.220.66.248
     - 54.228.200.90
     - eu-west-2.allowed-ips.checkpoint.com:
       - 18.168.7.234
       - 18.171.117.185
   - Me-central-1:
     - 34.248.94.75

        - 54.220.66.248
        - 54.228.200.90
        - me-central-1.allowed-ips.checkpoint.com:
            - 40.172.21.113
            - 51.112.130.15
    - Us-east-1:
        - 3.225.217.140
        - 52.205.49.189
        - 50.17.39.153
        - us-east-1.allowed-ips.checkpoint.com:
            - 18.205.54.240
            - 50.17.39.153
            - 3.224.33.252
6. Other URLs:
    - FedRAMP: s3-fips-r-w.us-east-1.amazonaws.com

References

- Harmony Endpoint product page
- sk108695 - Check Point SandBlast Agent for Browsers
- sk83520 - How to verify that Security Gateway and/or Security Management Server can access Check Point servers?

Comments Internal only

Reference case : 6-0004158683
The command was not working

curl -v -k -X GET http://teadv.checkpoint.com/epupdates/86.50/0190/v1.xml

After modifying the syntax the command was running successfully on the On-Premise Endpoint Server

The command which worked was :

curl_cli -v -k http://teadv.checkpoint.com/epupdates/86.50/0190/v1.xml

[Expert@H01VSPEDR01:0]# curl_cli -v -k http://teadv.checkpoint.com/epupdates/86.50/0190/v1.xml

Trying 104.120.134.72...

TCP_NODELAY set

Connected to teadv.checkpoint.com (104.120.134.72) port 80 (%30)

HTTP/1.1 200 OK Accept-Ranges: bytes Content-Type: application/xml ETag: "4f6a583a432fdc5195f59bba74bc6f2d:1722182764.080692" Last-Modified: Sun, 28 Jul 2024 15:49:19 GMT

Server: Akamai NetStorage Content-Length: 990 Date: Mon, 30 Dec 2024 11:04:50 GMT Connection: keep-alive-epupdate_file> Compliance_e86.50 /86.50/GenericOperation.dll replace Compliance.exe in E86.50

05hlwax8yJAni2x/J/NgaMPeg7ZJ1+908Mv3mh45dCbdRJTN4FknvLOZIU8k2fd1506evMMvk0MND7tIGSS07g301u0+CD2enD+OmHcR9EWarT2/C/mP50rON1Q+ko99KCDkIbW9nc 0EXRYkS5KagH1Q17XijNVwYZLc0589tWg/skFbSqp15jDNA8P6qwj164Q4ZhZeYJALDVHWS8vMIb4WrzZpX+4sZWpPLby6c1po2g4Wy51YOYyeXDD0oJlkiy3QzI2KC/kaGKw6s1JLLXJL80QOBPXW2HPg/PDmZJCJuaAb183bZ0GOznTLUb+2as21d/nrllaix/x+40goJNPesDn4p93ccTk0iH9+a2300m60GP7pUJhsdN3SZztcZuG/mimscGix21pNzt7NIVRxZUjtBvqvUjnZpDRrhr3Vjblo4TAO/uEQWtL5g+E6Vd

g4CsQs/hL7VZM4/yNfBnXxle SmEzlliflGfYriCOD8X1+Sm+0kCUzAnrILAryHbPKkFmpCY4JzRtKYr9UxFLul3sIp20TBke2L/YfgFW71y3vy/AHTUsgBBgqnFxvtgo7u3WfvRgrsHeXh70TJ3qTgoIXpVC

vLt6LQjP8myFJOkhTUGnle4sEncNaf3VyoN+0fkUGAC3zuPJTp1dN97LuL6spxDAZeckj4wR4= Connection #0 to host teadv.checkpoint.com left intact /
epupdate_file>

[Expert@H01VSPEDR01:0]#