

# Required Server Addresses for Proper Cisco Secure Endpoint & Malware Analytics Operations

## Contents

---

### [Introduction](#)

### [Prerequisites](#)

[Requirements](#)

[Components Used](#)

### [Required Server Addresses for Proper Cisco Secure Endpoint Operations](#)

[Server Locations](#)

[North America](#)

[Europe](#)

[Asia Pacific, Japan, China](#)

### [Required Server Addresses for Proper Cisco Secure Malware Analytics Cloud Access](#)

### [Required Server Addresses for Proper Orbital Use](#)

[North America Cloud \(NAM\) Cloud](#)

[European \(EU\) Cloud](#)

[Asia Pacific, Japan, China \(APIC\) Cloud](#)


### [Static IP Addresses](#)

---


## Introduction

This document describes the servers that are required in order to enable the Cisco Secure Endpoint (formerly Cisco AMP) product and Cisco Secure Malware Analytics (formerly Threat Grid) product to communicate and complete updates, lookups, and reports. In order to complete the operations successfully, your firewall must allow connectivity from the Connector/Appliance to the required servers.

---

 **Caution:** All of the servers use a round-robin IP address schema for load balancing, fault tolerance, and uptime. Therefore, the IP addresses might change, and Cisco recommends that the firewall be configured with *CNAME* instead of an IP address.

---

 **Caution:** Any traffic coming towards Cisco servers cannot be subjected to the TLS decryption.

---

## Prerequisites

### Requirements

This Tech Zone article applies to the following Cisco Products integrating with Cisco Secure Endpoint (AMP) product and Malware Analytics(Threat Grid):

- Cisco Secure Endpoints for Networks (Firepower Management Center and Sensors)
- Cisco Secure Endpoint Private Cloud
- Cisco Secure Endpoint Public Cloud

- Cisco Secure Email Appliance and Cisco Email Security (ESA and CES)
- Cisco Secure Web Appliance (WSA)
- Cisco Secure Malware Analytics Cloud and/or Appliance (Threat Grid)
- SDWAN/IOS-XE

## Components Used

This document is not restricted to specific software and hardware versions.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Required Server Addresses for Proper Cisco Secure Endpoint Operations

### Server Locations

The Cisco Secure Endpoint and Cisco Secure Malware Analytics servers are located in three different locations:

- North America (Cisco Secure Endpoint and Cisco Secure Malware Analytics)
- Europe (Cisco Secure Endpoint and Cisco Secure Malware Analytics)
- Japan (Cisco Secure Endpoint only)

### North America

This table lists the server locations for North America. Based on the account creation date, the server addresses might be different:

Category	Purpose	Server	Port
Cisco Secure Endpoint: Public Cloud	Disposition Server	cloud-ec-asn.amp.cisco.com	TCP 443
		cloud-ec-est.amp.cisco.com	
		enrolment.amp.cisco.com	
	Console	console.amp.cisco.com	TCP 443
	Management Server	mgmt.amp.cisco.com	TCP 443
	Event Server	intake.amp.cisco.com	TCP 443
	Policies	policy.amp.cisco.com	TCP 443
	Connector Downloads and Updates	upgrades.amp.cisco.com	TCP 80 and 443
	Error Reporting	crash.amp.cisco.com	TCP 443
Endpoint IOCs	ioc.amp.cisco.com	TCP 443	
TETRA Update Server	tetra-defs.amp.cisco.com	TCP 80 and 443	

		commercial.ocsp.identrust.com validation.identrust.com	
	macOS and Linux Clam Definitions	clam-defs.amp.cisco.com	TCP 80 and 443
	Advanced Custom Detections	custom-signatures.amp.cisco.com	TCP 443
	Remote File Fetch	rff.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Behavior Protection	apde.amp.cisco.com	TCP 443
	Device Control	endpoints.amp.cisco.com	TCP 443
Android Connector	Disposition Server	cloud-android-asn.amp.cisco.com	TCP 443
CSC/iOS Connector	Disposition Server	cloud-ios-asn.amp.cisco.com cloud-ios-est.amp.cisco.com	TCP 443
Cisco Secure Endpoint: Private Cloud	Upstream Disposition Server <v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Upstream Disposition Server >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum Server	packages-v2.amp.sourcefire.com	TCP 443
		pc-packages.amp.cisco.com	TCP 443
	Support Session	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Disposition Server (from FMC)	6.0 - 6.2.x: cloud-sa.amp.sourcefire.com	TCP 443
		6.3.x + : cloud-sa.amp.cisco.com	
	Events (from FMC)	5.x - 6.2.x: export.amp.sourcefire.com	TCP 443
		6.3.x +: export.amp.cisco.com	
	API (from FMC)		TCP 443

		5.x - 6.2.x: api.amp.sourcefire.com 6.3.x + : api.amp.cisco.com AND api.amp.sourcefire.com	
	Dynamic Analysis (from Sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com AND fmc.api.threatgrid.com  *Depending on the 6.x patch version, either URL can be used	TCP 443
ESA/WSA/SMA	File Reputation (ESA/WSA)	>= 15.x: cloud-esa-asn.amp.cisco.com cloud-esa-est.amp.cisco.com  < 15.x: cloud-sa.amp.cisco.com	TCP 443
	File Analysis (ESA/WSA/SMA)	panacea.threatgrid.com	TCP 443
	API (ESA)	>= 15.x: api.amp.cisco.com  < 15.x: N/A	TCP 443
	Event Server (ESA)	>= 15.x: intake.amp.cisco.com  < 15.x: N/A	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.amp.cisco.com  < 15.x: N/A	TCP 443
Meraki	Disposition Server	cloud-meraki-asn.amp.cisco.com cloud-meraki-est.amp.cisco.com	TCP 443
SDWAN	Disposition Server	cloud-isr-asn.amp.cisco.com cloud-isr-est.amp.cisco.com	TCP 443

## Europe

This table lists the server locations for Europe. Based on the account creation date, the server addresses might be different:

Category	Purpose Disposition Server	Server	Port
----------	-------------------------------	--------	------

Cisco Secure Endpoint: Public Cloud		cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com enrolment.eu.amp.cisco.com	TCP 443
	Console	console.eu.amp.cisco.com	TCP 443
	Management Server	mgmt.eu.amp.cisco.com	TCP 443
	Event Server	intake.eu.amp.cisco.com	TCP 443
	Policies	policy.eu.amp.cisco.com	TCP 443
	Connector Downloads and Updates	upgrades.eu.amp.cisco.com	TCP 80 and 443
	Error Reporting	crash.eu.amp.cisco.com	TCP 443
	Endpoint IOCs	ioc.eu.amp.cisco.com	TCP 443
	TETRA Update Server	tetra-defs.eu.amp.cisco.com commercial.ocsp.identrust.com validation.identrust.com	TCP 80 and 443
	macOS and Linux Clam Definitions	clam-defs.eu.amp.cisco.com	TCP 80 and 443
	Advanced Custom Detections	custom-signatures.eu.amp.cisco.com	TCP 443
	Remote File Fetch	rff.eu.amp.cisco.com submit.amp.cisco.com	TCP 443
	TETRA	nimbus.bitdefender.net	TCP 443
	Behavior Protection	apde.eu.amp.cisco.com	TCP 443
Device Control	endpoints.eu.amp.cisco.com	TCP 443	
Android Connector	Disposition Server	cloud-android-asn.eu.amp.cisco.com	TCP 443
CSC/iOS Connector	Disposition Server	cloud-ios-asn.eu.amp.cisco.com cloud-ios-est.eu.amp.cisco.com	TCP 443
Cisco Secure Endpoint: Private Cloud	Upstream Disposition Server <v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com	TCP 443
	Upstream Disposition Server	cloud-pc-est.eu.amp.cisco.com	TCP 443

	>v2.4	cloud-pc-asn.eu.amp.cisco.com	
	Yum Server	packages-v2.amp.sourcefire.com	TCP 443
		pc-packages.amp.cisco.com	TCP 443
	Support Session	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Disposition Server (from FMC)	6.0 - 6.2.x: cloud-sa.eu.amp.sourcefire.com 6.3.x+: cloud-sa.eu.amp.cisco.com	TCP 443
	Events (from FMC)	5.x - 6.2.x: export.eu.amp.sourcefire.com 6.3.x+: export.eu.amp.cisco.com	TCP 443
	API (from FMC)	5.x - 6.2.x: api.amp.sourcefire.com AND api.eu.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com AND api.eu.amp.cisco.com	TCP 443
	Dynamic Analysis (from Sensor)	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.eu AND fmc.api.threatgrid.eu Depending on 6.x patch version, either URL can be used	TCP 443
ESA/WSA/SMA	File Reputation (ESA/WSA)	>= 15.x: cloud-esa-asn.eu.amp.cisco.com cloud-esa-est.eu.amp.cisco.com < 15.x: cloud-sa.eu.amp.cisco.com	TCP 443
	File Analysis (ESA/WSA/SMA)	panacea.threatgrid.eu	TCP 443
	API (ESA)	>= 15.x: api.eu.amp.cisco.com < 15.x: N/A	TCP 443
	Event Server (ESA)	>= 15.x: intake.eu.amp.cisco.com < 15.x: N/A	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.eu.amp.cisco.com < 15.x: N/A	TCP 443

SDWAN	Disposition Server	cloud-isr-asn.eu.amp.cisco.com cloud-isr-est.eu.amp.cisco.com	TCP 443
-------	--------------------	--	---------

## Asia Pacific, Japan, China

This table lists the server locations for the Asia Pacific, Japan, and China:

Category	Purpose	Server	Port
Cisco Secure Endpoint: Public Cloud	Disposition Server	cloud-ec-asn.apjc.amp.cisco.com	TCP 443
		cloud-ec-est.apjc.amp.cisco.com	
		enrolment.apjc.amp.cisco.com	
	Console	console.apjc.amp.cisco.com	TCP 443
	Management Server	mgmt.apjc.amp.cisco.com	TCP 443
	Event Server	intake.apjc.amp.cisco.com	TCP 443
	Policies	policy.apjc.amp.cisco.com	TCP 443
	Connector Downloads and Updates	upgrades.apjc.amp.cisco.com	TCP 80 and 443
	Error Reporting	crash.apjc.amp.cisco.com	TCP 443
	Endpoint IOCs	ioc.apjc.amp.cisco.com	TCP 443
	TETRA Update Server	tetra-defs.apjc.amp.cisco.com	TCP 80 and 443
		commercial.ocsp.identrust.com validation.identrust.com	
	macOS and Linux Clam Definitions	clam-defs.apjc.amp.cisco.com	TCP 80 and 443
Advanced Custom Detections	custom-signatures.apjc.amp.cisco.com	TCP 443	
Remote File Fetch	rff.apjc.amp.cisco.com	TCP 443	
	submit.amp.cisco.com		
TETRA	nimbus.bitdefender.net	TCP 443	
Behavior Protection	apde.apjc.amp.cisco.com	TCP 443	

	Device Control	endpoints.apjc.amp.cisco.com	TCP 443
Android Connector	Disposition Server	cloud-android-asn.apjc.amp.cisco.com	TCP 443
CSC/iOS Connector	Disposition Server	cloud-ios-asn.apjc.amp.cisco.com cloud-ios-est.apjc.amp.cisco.com	TCP 443
Cisco Secure Endpoint:  Private Cloud	Upstream Disposition Server < v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Upstream Disposition Server > v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Yum Server	packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Support Session	support-sessions.amp.cisco.com	TCP 22
AMP for Networks: Firepower	Disposition Server	6.0 - 6.2.x: cloud-sa.apjc.amp.sourcefire.com (Static IP) 6.3.x+: cloud-sa.apjc.amp.cisco.com	TCP 443
	Events	5.x - 6.2.x: export.apjc.amp.sourcefire.com 6.3.x+: export.apjc.amp.cisco.com	TCP 443
	API	5.2 - 6.2.x api.apjc.amp.sourcefire.com AND api.amp.sourcefire.com 6.3.x+: api.amp.sourcefire.com AND api.apjc.amp.cisco.com	TCP 443
	Dynamic Analysis	There are currently no Threat Grid datacenters in APJC, therefore the	TCP 443



		European or North American hostnames must be used.	
ESA/WSA/SMA	File Reputation (ESA/WSA)	>= 15.x: cloud-esa-asn.apjc.amp.cisco.com cloud-esa-est.apjc.amp.cisco.com < 15.x: cloud-sa.apjc.amp.cisco.com	TCP 443
	File Analysis (ESA/WSA/SMA)	There are currently no Threat Grid datacenters in APJC, therefore the European or North American hostnames must be used.	TCP 443
	API (ESA)	>= 15.x: api.apjc.amp.cisco.com < 15.x: N/A	TCP 443
	Event Server (ESA)	>= 15.x: intake.apjc.amp.cisco.com < 15.x: N/A	TCP 443
	Management Server (ESA)	>= 15.x: mgmt.apjc.amp.cisco.com < 15.x: N/A	TCP 443
SDWAN	Disposition Server	cloud-isr-asn.apjc.amp.cisco.com cloud-isr-est.apjc.amp.cisco.com	TCP 443

## Required Server Addresses for Proper Cisco Secure Malware Analytics Cloud Access

For details on Secure Malware Analytic Cloud and Appliance, please refer to this article: [Required IPs and Ports for Secure Malware Analytics](#)

## Required Server Addresses for Proper Orbital Use

Static IPs for Orbital 1.7+

### North America Cloud (NAM) Cloud

Hostname	IP	Port
orbital.amp.cisco.com	54.71.115.87	443
	54.68.234.245	
	54.200.174.54	

ncp.orbital.amp.cisco.com	52.88.16.211	443
	52.43.91.219	
	54.200.152.114	
update.orbital.amp.cisco.com	54.71.197.112	443
	54.188.114.190	
	54.188.131.5	
NAT IPs for Remote Data Store		
	34.223.219.240	High random port number
	35.160.108.105	
	52.11.13.222	

For more information, please check the orbital help guide: <https://orbital.amp.cisco.com/help/>

## European (EU) Cloud

Hostname	IP	Port
orbital.eu.amp.cisco.com	3.120.91.16	443
	18.196.194.92	
	3.121.5.209	
ncp.orbital.eu.amp.cisco.com	18.194.154.159	443
	18.185.217.177	
	18.184.249.36	
update.orbital.eu.amp.cisco.com	3.123.83.189	443
	18.184.240.159	
	35.158.29.104	
NAT IPs for Remote Data Store		
	52.29.47.197	High random

	52.57.222.67	port number
	52.58.172.218	

For more information, please check the orbital help guide: <https://orbital.eu.amp.cisco.com/help/>

## Asia Pacific, Japan, China (APJC) Cloud

Hostname	IP	Port
orbital.apjc.amp.cisco.com	3.114.186.175 52.198.6.9 18.177.242.101	443
ncp.orbital.apjc.amp.cisco.com	18.177.250.245 13.230.62.75 18.176.196.172	443
update.orbital.apjc.amp.cisco.com	54.248.22.154 18.178.184.79 54.95.125.218	443
NAT IPs for Remote Data Store		
	52.194.143.206 52.69.138.67 54.95.9.136	High random port number


For more information, please check the orbital help guide: <https://orbital.apjc.amp.cisco.com/help/>

## Static IP Addresses

If your firewall blocks outbound TCP connections on port 443 (which is usually not the case), you must change your firewall settings before you update any policies. If your account was established after February 2016, you already have static IP addresses written into the standard policies. If your account was established prior to February 2016, you can contact the Cisco Technical Assistance Center (TAC) to request a migration of the policies to the static IP addresses.



**Note:** In order to ensure continuity of operations, and to ensure that the detected file malware dispositions are the same on both of the Firepower Management Centers, both the Primary and Secondary Management Centers must have access to the servers listed in this document.

 **Note:** The Cisco Secure Endpoint Console does not use Static IPs and must be accessed through DNS.

Static IP Addresses in North America	Static IP Addresses in Europe	Static IP Addresses in APJC
23.23.197.169	46.51.181.139	54.250.127.0
23.23.198.191	46.51.182.195	52.197.2.58
23.23.224.83	46.51.182.202	52.197.22.41
	46.137.99.242	52.69.16.172
50.16.242.171	52.16.63.115	13.112.137.80
50.16.244.193	52.16.95.58	52.198.208.254
	52.16.105.95	13.112.162.167
50.16.250.236	52.16.166.193	54.249.244.218
52.0.55.209	52.16.177.94	54.249.246.210
52.2.63.194	52.16.193.225	54.249.243.85
52.2.128.246	52.16.220.180	54.249.240.219
52.3.149.24	52.17.93.43	54.248.98.94
52.3.178.163	52.17.102.100	176.34.47.0
52.3.190.47	52.17.106.35	52.192.82.189
52.4.98.101	52.17.179.163	52.68.180.106
52.4.151.41	52.17.211.190	52.196.247.47
52.4.245.162	52.17.233.49	52.196.185.158
52.4.246.178	52.18.9.153	52.197.74.4
52.5.92.125	52.18.28.229	52.69.39.127
52.6.103.57	52.18.79.226	54.248.113.224
52.6.197.200	52.18.109.209	54.238.55.12
52.20.14.163	52.18.187.129	54.249.248.16
52.20.123.238	52.18.187.166	52.197.50.93
52.20.141.147	52.18.223.41	52.193.124.132
52.21.52.149	52.19.84.244	52.69.108.228
52.21.117.50	52.19.167.56	52.197.72.147
52.21.134.210	52.30.25.70	52.197.22.165
52.22.64.192	52.30.74.163	52.68.82.200
52.22.156.183	52.30.124.82	52.197.35.73
52.23.13.34	52.30.160.113	52.197.39.251
52.23.16.199	52.30.175.205	52.68.251.104
52.23.73.146	52.30.179.236	54.249.253.42
52.23.87.4	52.30.196.206	54.249.253.65
52.23.107.89	52.30.208.114	176.34.60.211
52.23.134.105	52.30.217.4	52.192.198.119
52.23.140.222	52.30.217.226	52.196.96.41
52.70.11.137	52.30.255.133	54.248.116.199
52.70.13.27	52.31.30.249	52.196.117.29
52.70.35.37	52.31.66.59	52.196.134.7
52.70.47.45	52.31.83.94	176.34.60.30
52.70.56.136	52.31.119.97	52.192.145.214
52.70.58.10	52.31.122.77	52.192.221.107
52.70.59.59	52.31.127.190	52.193.182.191
52.70.59.121	52.31.137.201	52.193.201.169
52.70.60.74	54.195.248.52	52.193.223.43
52.70.61.174	54.195.249.18	52.193.233.17
52.70.61.181	54.217.232.226	52.196.115.166
52.70.61.193	54.217.232.234	52.196.31.86
52.70.63.25	54.217.232.241	52.197.121.237

54.83.45.221	54.217.232.244	52.198.147.230
54.88.208.235	54.217.232.249	52.198.195.125
54.204.8.61	54.228.250.255	52.198.202.24
54.221.210.7	54.246.88.192	52.198.221.53
54.221.255.190	54.247.189.117	52.198.223.169
54.225.226.117	54.74.229.75	52.198.225.221
54.225.227.9	107.21.250.31	52.198.226.104
54.225.227.30	107.21.236.143	52.198.26.36
54.225.227.45	107.21.236.143	52.198.94.104
54.225.227.105	52.2.128.246	52.199.124.11
54.225.228.145	52.18.202.103	52.199.127.80
54.225.228.166	52.18.119.87	52.199.92.142
54.225.228.244	192.111.5.0/24	52.68.1.146
54.227.247.102	34.249.48.182	54.248.107.84
107.20.158.55	34.248.52.55	54.248.109.124
107.20.203.8	99.81.233.22	54.248.126.98
107.20.229.191	3.123.83.189	54.248.236.127
107.20.234.220	18.184.240.159	54.248.236.141
107.21.212.157	35.158.29.104	54.248.236.144
107.21.217.202	192.35.177.23	54.248.236.151
107.21.218.60	104.18.39.201	54.248.237.93
128.177.8.0/24	172.64.148.55	54.249.246.7
174.129.203.65	104.18.4.5	54.250.127.131
54.161.128.60	104.18.5.5	192.111.6.0/24
54.234.131.176	52.3.48.165	54.248.22.154
52.206.206.244	52.6.245.67	18.178.184.79
34.225.208.192	34.120.67.236	54.95.125.218
52.22.120.193	34.98.122.109	192.35.177.23
34.199.250.32		104.18.39.201
34.199.238.4		172.64.148.55
34.194.224.132		18.180.25.43
34.198.112.150		54.95.253.127
34.224.236.198		54.249.195.77
52.20.233.31		104.18.4.5
192.111.4.0/24		104.18.5.5
192.111.7.0/24		52.3.48.165
54.71.197.112		52.6.245.67
54.188.114.190		34.120.67.236
54.188.131.5		34.98.122.109
192.35.177.23		
104.18.39.201		
172.64.148.55		
104.18.4.5		
104.18.5.5		
52.3.48.165		
52.6.245.67		

34.120.67.236 34.98.122.109		
--------------------------------	--	--