

# Required Server Addresses for Proper AMP Operations

## Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Required Server Addresses for Proper AMP Operations](#)

[Server Locations](#)

[North America](#)

[Europe](#)

[Asia Pacific, Japan, China](#)

[Static IP Addresses](#)

[Related Information](#)

## Introduction

This document describes the servers that are required in order to enable the Cisco Advanced Malware Protection (AMP) product to communicate and complete updates, lookups, and reports. In order to complete the operations successfully, your firewall must allow connectivity from the Connector 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.

## Prerequisites

### Requirements

Cisco recommends that you have knowledge of the Cisco Firepower Management Center (also known as *Defense Center*) and these AMP products:

- Cisco AMP Appliances
- Cisco AMP for Firepower
- Cisco AMP for Network Virtual Appliance
- Cisco FireAMP Private Cloud Virtual Appliance
- Cisco FireAMP for Endpoints

### 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 AMP Operations

### Server Locations

The AMP servers are located in three different locations:

- North America
- Europe
- Japan

### 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
Public Cloud Endpoint	Cloud Server	4.x Windows only: cloud-ec.amp.cisco.com	4.x: TCP 443 or 32137
		cloud-ec-asn.amp.cisco.com cloud-ec-est.amp.cisco.com	TCP 443
	FireAMP Console Management Server	console.amp.cisco.com mgmt.amp.cisco.com	TCP 443 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	update.amp.cisco.com	TCP 80 and 443
	OSX Clam Definitions	defs.amp.sourcefire.com	TCP 80
Android Connector	Advanced Custom Detections	custom-signatures.amp.cisco.com	TCP 443
	Remote File Fetch	rff.amp.cisco.com	TCP 443
	Cloud Server	android.amp.sourcefire.com	TCP 443
AMP Private Cloud	Upstream Cloud Server <v2.4	cloud-pc.amp.sourcefire.com	TCP 443 or 32137
	Upstream Cloud Server >v2.4	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com cloud-pc.amp.cisco.com	TCP 443
	Yum Server	packages.amp.sourcefire.com packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
	Support Session	support-sessions.amp.sourcefire.com	TCP 22
Firesight/Firepower	Cloud Server	5.x: cloud-dc.amp.sourcefire.com 6.x: cloud-sa.amp.sourcefire.com	TCP 443 or 32137

	FireAMP Events	export.amp.sourcefire.com	TCP 443
	FireAMP API	api.amp.sourcefire.com	TCP 443
	Dynamic Analysis	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443
ESA/WSA	File Reputation	cloud-sa.amp.sourcefire.com (Legacy) cloud-sa.amp.cisco.com	TCP 443 or 32137
Meraki	Cloud Server	cloud-meraki-asn.amp.cisco.com cloud-meraki-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	Server	Port
		4.x Windows Only: cloud-ec.eu.amp.cisco.com	4.x: TCP 443 or 32137
	Cloud Server	cloud-ec-asn.eu.amp.cisco.com cloud-ec-est.eu.amp.cisco.com	TCP 443
Public Cloud Endpoint	FireAMP 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.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	update.amp.cisco.com	TCP 80 and 443
	OSX Clam Definitions	defs.amp.sourcefire.com	TCP 80
	Advanced Custom Detections	custom-signatures.eu.amp.cisco.com	TCP 443
Android Connector	Remote File Fetch	rff.eu.amp.cisco.com	TCP 443
	Cloud Server	android.eu.amp.sourcefire.com	TCP 443
	Upstream Cloud Server <v2.4	cloud-pc.eu.amp.sourcefire.com	TCP 443 or 32137
AMP Private Cloud	Upstream Cloud Server >v2.4	cloud-pc-est.eu.amp.cisco.com cloud-pc-asn.eu.amp.cisco.com cloud-pc.eu.amp.cisco.com	TCP 443
	Yum Server	packages.amp.sourcefire.com packages-v2.amp.sourcefire.com pc-packages.amp.cisco.com	TCP 443 TCP 443 TCP 443
Firesight/Firepower	Support Session	support-sessions.amp.sourcefire.com	TCP 22
	Cloud Server	5.x: cloud-dc.eu.amp.sourcefire.com 6.x: cloud-sa.eu.amp.sourcefire.com	TCP 443 or 32137
	FireAMP Events	export.eu.amp.sourcefire.com	TCP 443
	FireAMP API	api.eu.amp.sourcefire.com	TCP 443
	Dynamic Analysis	5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443
ESA/WSA	File Reputation	cloud-sa.amp.sourcefire.com (Legacy) cloud-sa.eu.amp.cisco.com	TCP 443 or 32137
Meraki	Cloud Server	cloud-meraki-asn.eu.amp.cisco.com (AWS IP)	TCP 443

**Asia Pacific, Japan, China**

This table lists the server locations from January 27th, 2017:

<b>Category</b>	<b>Purpose</b>	<b>Server</b>	<b>Port</b>
		4.x Windows only: cloud-ec.apjc.amp.cisco.com	4.x: TCP 443 or 32137
	Cloud Server	cloud-ec-asn.apjc.amp.cisco.com cloud-ec-est.apjc.amp.cisco.com	TCP 443
Windows/Mac Connector	FireAMP Console Management Server	console.apjc.amp.cisco.com	TCP 443
	Event Server	mgmt.apjc.amp.cisco.com	TCP 443
	Policies	intake.apjc.amp.cisco.com	TCP 443
	Connector Downloads and Updates	policy.apjc.amp.cisco.com	TCP 443
	Error Reporting	upgrades.amp.cisco.com	TCP 80 and 443
	Endpoint IOCs	crash.apjc.amp.cisco.com	TCP 443
	TETRA Update Server	ioc.apjc.amp.cisco.com	TCP 443
Android Connector	OSX Clam Definitions	update.amp.cisco.com	TCP 80 and 443
	Advanced Custom Detections	defs.amp.sourcefire.com	TCP 80
	Remote File Fetch	custom-signatures.apjc.amp.cisco.com	TCP 443
	Cloud Server	rff.apjc.amp.cisco.com	TCP 443
AMP Private Cloud	Upstream Cloud Server < v2.4	android.apjc.amp.cisco.com	TCP 443
	Upstream Cloud Server > v2.4	cloud-pc.amp.sourcefire.com	TCP 443 or 32137
Firesight/Firepower	Yum Server	cloud-pc-est.amp.cisco.com cloud-pc-asn.amp.cisco.com	TCP 443
	Support Session	cloud-pc.amp.cisco.com	TCP 443
	Cloud Server	packages.amp.sourcefire.com	TCP 443
ESA/WSA	FireAMP Events	packages-v2.amp.sourcefire.com	TCP 443
	FireAMP API	pc-packages.amp.cisco.com	TCP 443
	Dynamic Analysis	support-sessions.amp.sourcefire.com	TCP 22
Meraki	File Reputation	5.x: cloud-dc.apjc.amp.sourcefire.com 6.x: cloud-sa.apjc.amp.sourcefire.com (Static IP)	TCP 443 or 32137
	Cloud Server	export.apjc.amp.sourcefire.com	TCP 443
		api.apjc.amp.sourcefire.com	TCP 443
		5.x: intel.api.sourcefire.com 6.x: panacea.threatgrid.com	TCP 443
		cloud-sa.amp.sourcefire.com (Legacy) cloud-sa.apjc.amp.cisco.com	TCP 443 or 32137
		cloud-meraki-asn.apjc.amp.cisco.com (AWS IP) cloud-meraki-est.apjc.amp.cisco.com (AWS IP)	TCP 443

**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.

#### **Static IP Addresses in North America**

23.23.197.169  
23.23.198.191  
23.23.224.83  
50.16.244.193  
52.0.55.209  
52.2.63.194  
52.2.128.246  
52.3.149.24  
52.3.178.163  
52.3.190.47  
52.4.98.101  
52.4.151.41  
52.4.245.162  
52.4.246.178  
52.5.92.125  
52.6.103.57  
52.6.197.200  
52.20.14.163  
52.20.123.238  
52.20.141.147  
52.21.52.149  
52.21.117.50  
52.21.134.210  
52.22.64.192  
52.22.156.183  
52.23.13.34  
52.23.16.199  
52.23.73.146  
52.23.87.4  
52.23.107.89  
52.23.134.105  
52.23.140.222  
52.70.11.137  
52.70.13.27  
52.70.35.37  
52.70.47.45  
52.70.56.136  
52.70.58.10  
52.70.59.59  
52.70.59.121  
52.70.60.74

#### **Static IP Addresses in Europe**

46.51.181.139  
46.51.182.195  
46.51.182.202  
46.137.99.242  
52.16.63.115  
52.16.95.58  
52.16.105.95  
52.16.166.193  
52.16.177.94  
52.16.193.225  
52.16.220.180  
52.17.93.43  
52.17.102.100  
52.17.106.35  
52.17.179.163  
52.17.211.190  
52.17.233.49  
52.18.9.153  
52.18.28.229  
52.18.79.226  
52.18.109.209  
52.18.187.129  
52.18.187.166  
52.18.223.41  
52.19.84.244  
52.19.167.56  
52.30.25.70  
52.30.74.163  
52.30.124.82  
52.30.160.113  
52.30.175.205  
52.30.179.236  
52.30.196.206  
52.30.208.114  
52.30.217.4  
52.30.217.226  
52.30.255.133  
52.31.30.249  
52.31.66.59  
52.31.83.94  
52.31.119.97

#### **Static IP Addresses in APJC**

54.250.127.0  
52.197.2.58  
52.197.22.41  
52.69.16.172  
13.112.137.80  
52.198.208.254  
13.112.162.167  
54.249.244.218  
54.249.246.210  
54.249.243.85  
54.249.240.219  
54.248.98.94  
176.34.47.0  
52.192.82.189  
52.68.180.106  
52.196.247.47  
52.196.185.158  
52.197.74.4  
52.69.39.127  
54.248.113.224  
54.238.55.12  
54.249.248.16  
52.197.50.93  
52.193.124.132  
52.69.108.228  
52.197.72.147  
52.197.22.165  
52.68.82.200  
52.197.35.73  
52.197.39.251  
52.68.251.104  
54.249.253.42  
54.249.253.65  
176.34.60.211  
52.192.198.119  
52.196.96.41  
54.248.116.199  
52.196.117.29  
52.196.134.7  
176.34.60.30  
52.192.145.214

52.70.61.174  
52.70.61.181  
52.70.61.193  
52.70.63.25  
54.83.45.221  
54.88.208.235  
54.221.210.7  
54.221.255.190  
54.225.226.117  
54.225.227.9  
54.225.227.30  
54.225.227.45  
54.225.227.105  
54.225.228.145  
54.225.228.166  
54.225.228.244  
54.227.247.102  
107.20.158.55  
107.20.203.8  
107.20.229.191  
107.20.234.220  
107.21.212.157  
107.21.217.202  
107.21.218.60  
128.177.8.0/24  
174.129.203.65  
54.161.128.60  
54.234.131.176  
52.206.206.244  
34.225.208.192  
52.22.120.193  
34.199.250.32  
34.199.238.4  
34.194.224.132  
34.198.112.150  
34.224.236.198  
52.20.233.31

52.31.122.77  
52.31.127.190  
52.31.137.201  
54.195.248.52  
54.195.249.18  
54.217.232.226  
54.217.232.234  
54.217.232.241  
54.217.232.244  
54.217.232.249  
54.228.250.255  
54.246.88.192  
54.247.189.117  
54.74.229.75  
54.74.195.196  
107.21.250.31  
107.21.236.143  
52.2.128.246  
52.18.202.103  
52.18.119.87

52.192.221.107  
52.193.182.191  
52.193.201.169  
52.193.223.43  
52.193.233.17  
52.196.115.166  
52.196.31.86  
52.197.121.237  
52.198.147.230  
52.198.195.125  
52.198.202.24  
52.198.221.53  
52.198.223.169  
52.198.225.221  
52.198.226.104  
52.198.26.36  
52.198.94.104  
52.199.124.11  
52.199.127.80  
52.199.92.142  
52.68.1.146  
54.248.107.84  
54.248.109.124  
54.248.126.98  
54.248.236.127  
54.248.236.141  
54.248.236.144  
54.248.236.151  
54.248.237.93  
54.249.246.7  
54.250.127.131

## Related Information

- [Technical Support & Documentation - Cisco Systems](#)