

AMP for Endpoints: ClamAV Virus Definition Options in Linux

Contents

[Introduction](#)

[Backwards Compatibility](#)

[Changing the ClamAV Virus Definitions Option](#)

[Verifying the New Setting at the Endpoint](#)

Introduction

Starting with Linux Connector version 1.11.0, AMP for Endpoints now offers two ClamAV Virus Definition configuration options:

1. Linux-only
2. Full ClamAV

Prior to the Linux-only option becoming available, the Linux Connector scanned files using the full ClamAV virus definition set. This set includes malware signatures for Linux, macOS, Windows and Android. Although this provides comprehensive coverage, it also requires significant runtime resources (i.e., CPU time and memory). Some Linux systems can benefit from configuring AMP to use the smaller Linux-only ClamAV virus definition set.

The Linux-only virus definition file size is less than 10% of the full set. Using a smaller set reduces computing overhead and makes it possible to run AMP on resource constrained systems. Despite the performance advantages, reduced coverage for non-Linux malware makes this configuration only suitable for some applications. E.g., It would be suitable for servers that only host/store Linux files (such as application servers) but would not be suitable for servers that also host/store non-Linux files (such as FTP, mail and SMB file servers). The system administrator must balance this trade-off to choose the appropriate set of virus definitions.

IMPORTANT!

It is highly recommended that all endpoints be upgraded to Connector version 1.11.0 or newer before using the new Linux-only virus definition option. While 1.10.x and older Connector versions will accept the new option, its behavior in some cases will not be intuitive. Refer to the *Backwards Compatibility* section for details.

Backwards Compatibility

There is an important backwards compatibility issue to consider before configuring endpoints to use the new Linux-only virus definition option: 1.10.x and older Connectors will continue to use the full virus definition if the full set had already been downloaded. If configured to use the new Linux-only virus definition option, the Connector will stop updating the full virus definition set and will only update the Linux virus definition set thereafter. This can result in the endpoint using up-to-date

Linux virus definitions but out-of-date macOS, Windows, and Android definitions.

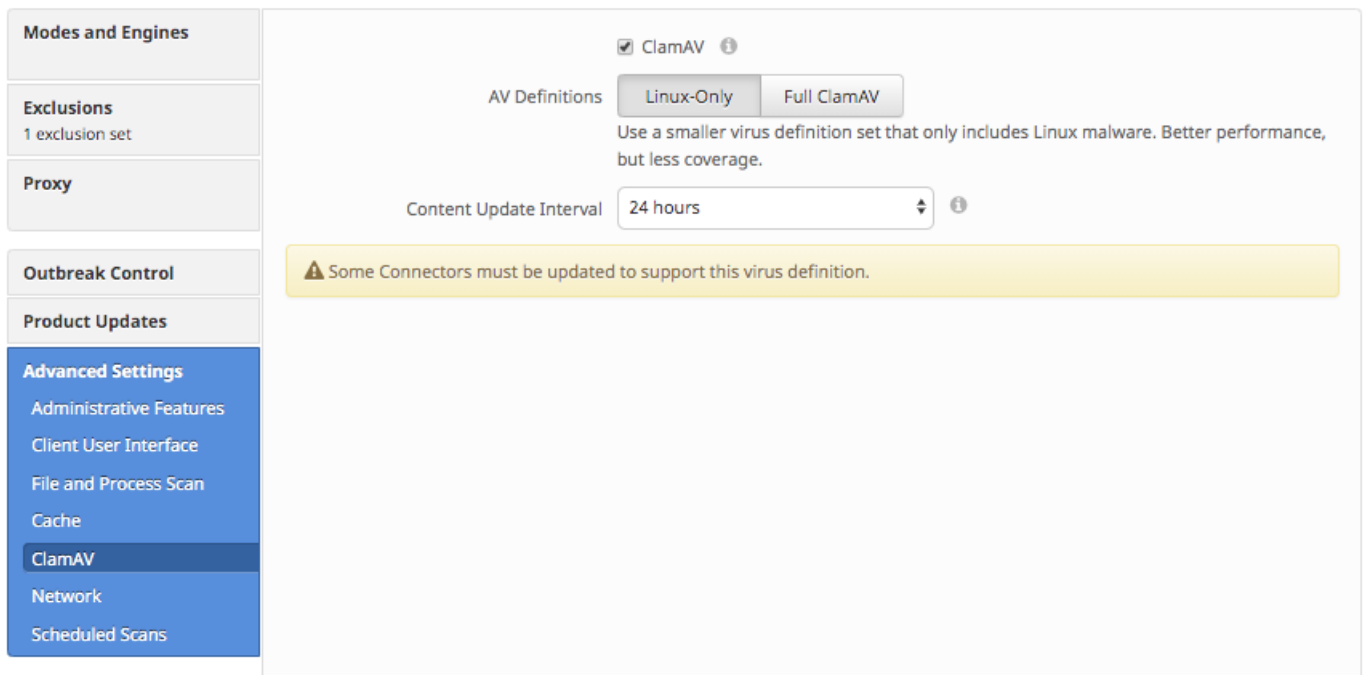
There are two possible resolutions:

1. Upgrade the Connector to 1.11.0 or later.
2. Change the ClamAV Virus Definition setting back to Full ClamAV.

Changing the ClamAV Virus Definitions Option

The ClamAV Virus Definition option can be configured using the AMP for Endpoints web portal. The option for each policy can be changed by navigating to:

Management > Policies > [Linux Policy] > Edit > Advanced Settings > ClamAV



The screenshot displays the AMP for Endpoints web portal interface for configuring ClamAV settings. On the left is a navigation sidebar with the following sections: Modes and Engines, Exclusions (1 exclusion set), Proxy, Outbreak Control, Product Updates, and Advanced Settings. The Advanced Settings section is expanded, showing options for Administrative Features, Client User Interface, File and Process Scan, Cache, ClamAV (selected), Network, and Scheduled Scans. The main content area shows the ClamAV configuration. A checkbox labeled 'ClamAV' is checked. Below it, the 'AV Definitions' section has two buttons: 'Linux-Only' (selected) and 'Full ClamAV'. A descriptive text below the buttons reads: 'Use a smaller virus definition set that only includes Linux malware. Better performance, but less coverage.' The 'Content Update Interval' is set to '24 hours' in a dropdown menu. A yellow warning banner at the bottom of the configuration area states: 'Some Connectors must be updated to support this virus definition.'

After the AV Definitions policy setting is changed, the new setting takes effect on the endpoints at the next scheduled virus definition update. That delay is governed by the `Content Update Interval` policy setting.

The "Some Connectors must be updated to support this virus definition" warning may appear in the ClamAV Advanced Settings screen if at least one Connector managed by the policy is running an incompatible Linux Connector version. It is highly recommended to upgrade the Connectors and resolve this warning before using the Linux-only definitions setting.

Verifying the New Setting at the Endpoint

When configured to use Linux-only definitions, the combined resident memory size of the two AMP Connector processes should be below 100 MB.

This can be examined using the following command:

```
top -p `pidof ampdemon` -p `pidof ampscansvc`
```

The following is a sample output:

```
top - 23:52:51 up 15:11, 7 users, load average: 0.36, 1.10, 0.83
Tasks:  2 total,  0 running,  2 sleeping,  0 stopped,  0 zombie
%Cpu(s):  2.5 us,  0.5 sy,  0.0 ni, 97.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem : 3861508 total, 309220 free, 1732560 used, 1819728 buff/cache
KiB Swap: 2097148 total, 2064116 free,  33032 used. 1629348 avail Mem
```

PID	USER	PR	NI	VIRT	RES	SHR	S	%CPU	%MEM	TIME+	COMMAND
88910	root	20	0	1323172	32904	6752	S	0.7	0.9	3:20.16	ampdaemon
88937	cisco-a+	20	0	258764	8400	2704	S	0.0	0.2	1:23.73	ampscansvc