ESA FAQ: How do I force a download of Sophos or McAfee Anti−Virus updates immediately?

TAC **Document ID: 118062**

Contributed by Scott Roeder and Robert Sherwin, Cisco TAC Engineers.
Jul 24, 2014

Contents

Introduction

This document describes how to manually update the anti−virus process for the Cisco Email Security Appliance (ESA).

How do I force a download of Sophos or McAfee Anti−Virus updates immediately?

Although anti−virus updates happen at regular intervals as configured from the appliance service updates, if you are waiting for an update you can initiate an anti−virus update yourself. By default, the updater service will check for updates every five minutes. Cisco recommends to leave this set to the default update interval.

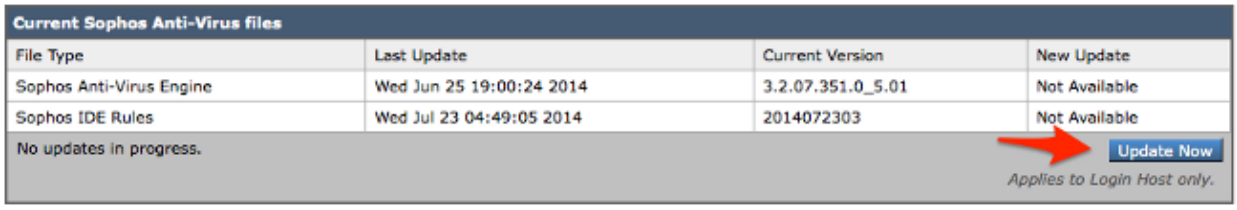
You can review the appliance service updates from GUI, ***Security Services*** > ***Service Updates***. From the CLI run ***updateconfig.*** This will be listed as the ***Update Interval***.

To update the anti−virus process directly, please choose one of the following methods:

GUI

From the GUI, you can initiate an update from the ***Security Services*** > ***Anti−Virus***, and choose either ***Sophos*** or ***McAfee***. From the ***Current Anti−Virus Files*** table, click the ***Update Now*** button.

Example, using Sophos Anti−Virus:



CLI

From the CLI, you can initiate an immediate virus update with the CLI command ***antivirusupdate***, and choose the anti−virus process you have licensed, ***sophos*** or ***mcafee***.

```
> antivirusupdate


Choose the operation you want to perform:
− MCAFEE − Request updates for McAfee Anti−Virus
− SOPHOS − Request updates for Sophos Anti−Virus
[]> sophos

Requesting check for new Sophos Anti−Virus updates.
```

On the CLI you can also force a complete update via the command ***antivirusupdate force***. A complete update is when the ESA will reach out to the Cisco update servers and pull the complete and most recent IDE, and also will pull the complete and most recent anti−virus engine, and reapply this in the background on your appliance.

```
> antivirusupdate force

Sophos Anti−Virus updates:
Requesting forced update of Sophos Anti−Virus.
McAfee Anti−Virus updates:
Requesting update of virus definitions
```

Verification

You can view the process of the anti−virus updates my running ***tail updater_logs*** from the CLI on the ESA. This assure you of the appliance's communication with the Cisco update servers and manifest, and allow you to see the update complete.

```
Wed Jul 23 09:38:58 2014 Info: Server manifest specified an update for sophos
Wed Jul 23 09:38:58 2014 Info: sophos was signalled to start a new update
Wed Jul 23 09:38:58 2014 Info: sophos processing files from the server manifest
Wed Jul 23 09:38:58 2014 Info: sophos started downloading files
Wed Jul 23 09:38:58 2014 Info: sophos waiting on download lock
Wed Jul 23 09:38:58 2014 Info: sophos acquired download lock
Wed Jul 23 09:38:58 2014 Info: sophos beginning download of remote file
 "http://updates.ironport.com/sophos/ide/1406116201"
Wed Jul 23 09:39:03 2014 Info: sophos released download lock
Wed Jul 23 09:39:03 2014 Info: sophos successfully downloaded file "sophos/ide/1406116201"
Wed Jul 23 09:39:04 2014 Info: sophos waiting on download lock
Wed Jul 23 09:39:04 2014 Info: sophos acquired download lock
Wed Jul 23 09:39:04 2014 Info: sophos beginning download of remote file
 "http://updates.ironport.com/sophos/libsavi/1402438439"
Wed Jul 23 09:41:07 2014 Info: sophos released download lock
Wed Jul 23 09:41:07 2014 Info: sophos successfully downloaded file
 "sophos/libsavi/1402438439"
Wed Jul 23 09:41:07 2014 Info: sophos started applying files
Wed Jul 23 09:41:08 2014 Info: sophos updating component ide
Wed Jul 23 09:41:12 2014 Info: sophos updating component libsavi
Wed Jul 23 09:41:12 2014 Info: sophos updated engine,ide links successfully
Wed Jul 23 09:41:12 2014 Info: sophos cleaning up base dir /data/third_party/sophos
Wed Jul 23 09:41:12 2014 Info: sophos sending version details {'sophos': {'version': '5.01',
 'ide': '2014072303'}} to hermes
Wed Jul 23 09:41:13 2014 Info: sophos verifying applied files
Wed Jul 23 09:41:13 2014 Info: sophos updating the client manifest
Wed Jul 23 09:41:13 2014 Info: sophos update completed
Wed Jul 23 09:41:13 2014 Info: sophos waiting for new updates
```

You will want to assure that you see the highlighted lines above, which will indicate the successful request and update of the requested anti−virus updates.

Cisco encourages customers who enable Sophos Anti−Virus scanning to subscribe to Sophos alerts on the Sophos site at http://www.sophos.com/virusinfo/notifications/. Subscribing to receive alerts directly from Sophos will ensure you are apprised of the latest virus outbreaks and their available solutions.

Related Information

- ***Technical Support & Documentation − Cisco Systems***

Updated: Jul 24, 2014 Document ID: 118062