

Elevação do cargo-AsyncOS, dos “antivirus sophos - O base de dados anti-vírus neste sistema é” mensagem de advertência expirado

Índice

[Introdução](#)

[Elevação do cargo-AsyncOS, dos “antivirus sophos - O base de dados anti-vírus neste sistema é” mensagem de advertência expirado](#)

[Verifique a versão atual de Sophos](#)

[Force a atualização Sophos](#)

Introdução

Este documento descreve porque Cisco envia por correio eletrônico o administrador da ferramenta de segurança (ESA) recebe um mensagem de advertência de um dispositivo após uma elevação essa indica que o base de dados anti-vírus de Sophos está expirado.

Contribuído por Dominic Yip e Stephan Bayer, engenheiros de TAC da Cisco.

Elevação do cargo-AsyncOS, dos “antivirus sophos - O base de dados anti-vírus neste sistema é” mensagem de advertência expirado

Em um ESA, depois que você promove a uma nova versão de AsyncOS e termina a repartição exigida, um administrador pôde receber um mensagem de advertência similar a este:

The Warning message is:

```
sophos antivirus - The Anti-Virus database on this system is expired. Although the system will continue to scan for existing viruses, new virus updates will no longer be available. Please run avupdate to update to the latest engine immediately. Contact Cisco IronPort Customer Support if you have any questions.
```

Current Sophos Anti-Virus Information:

```
SAV Engine Version 5.33  
IDE Serial Unknown  
Last Engine Update Tue Mar 7 01:19:08 2017  
Last IDE Update Tue Mar 7 01:19:08 2017
```

```
Version: 11.0.0-028  
Serial Number: 111A80C64EA901221AAA-1A11EB54A111  
Timestamp: 13 Mar 2017 14:57:21 -0400
```

Este mensagem de advertência indica que o base de dados do motor anti-vírus e o pacote

associados das regras não são atuais para a versão atualizada de AsyncOS na altura da partida do dispositivo. O ESA verificará para ver se há atualizações anti-vírus de motor depois que vem em linha e atualizará à versão atual.

Verifique a versão atual de Sophos

A fim verificar a versão do motor de Sophos, inscreva **sophos do antivirusstatus** (ou, **sophos do avstatus**) no CLI a fim ver a versão anti-vírus atual do motor.

```
myesa.local> avstatus sophos
```

```
SAV Engine Version 3.2.07.366.3_5.36  
IDE Serial 2017032603  
Last Engine Update 26 Mar 2017 13:24 (GMT +00:00)  
Last IDE Update 26 Mar 2017 13:24 (GMT +00:00)
```

Compare a versão do mensagem de advertência recebido mais cedo às saídas de versão do motor do comando status. Depois que você valida que o dispositivo alcançou para fora e atualizado, você pode com segurança ignorar este mensagem de advertência.

Atualização Sophos da força

Você pode igualmente incorporar a **força do avupdate** do comando a fim pedir uma atualização imediata ao motor e às regras anti-vírus. Depois que você incorpora o comando da força, incorpore **updater_logs da cauda** a fim ver a atualização em andamento. Isto pôde tomar alguns minutos para alcançar para fora ao updater, para obter os pacotes apropriados, e então para transferi-los e instalá-los como necessários. Um exemplo deste é:

```
(myesa.local)> avupdate force
```

```
Sophos Anti-Virus updates:  
Requesting forced update of Sophos Anti-Virus.  
McAfee Anti-Virus updates:  
Requesting update of virus definitions  
(Machine 122.local)> tail updater_logs
```

```
Press Ctrl-C to stop.
```

```
Sun Mar 26 09:20:39 2017 Info: Server manifest specified an update for sophos  
Sun Mar 26 09:20:39 2017 Info: sophos was signalled to start a new update  
Sun Mar 26 09:20:39 2017 Info: sophos processing files from the server manifest  
Sun Mar 26 09:20:39 2017 Info: sophos started downloading files  
Sun Mar 26 09:20:39 2017 Info: sophos waiting on download lock  
Sun Mar 26 09:20:39 2017 Info: sophos acquired download lock  
Sun Mar 26 09:20:39 2017 Info: sophos beginning download of remote file  
"http://stage-updates.ironport.com/sophos/4.4/ide/default_esa/1490526336"  
Sun Mar 26 09:20:41 2017 Info: sophos released download lock  
Sun Mar 26 09:20:41 2017 Info: sophos successfully downloaded file  
"sophos/4.4/ide/default_esa/1490526336"  
Sun Mar 26 09:20:41 2017 Info: sophos waiting on download lock  
Sun Mar 26 09:20:41 2017 Info: sophos acquired download lock  
Sun Mar 26 09:20:41 2017 Info: sophos beginning download of remote file  
"http://stage-updates.ironport.com/sophos/libsave/1488816512"  
Sun Mar 26 09:24:58 2017 Info: sophos released download lock  
Sun Mar 26 09:24:58 2017 Info: sophos successfully downloaded file
```

"sophos/libsavi/1488816512"

```
Sun Mar 26 09:24:58 2017 Info: sophos started applying files
Sun Mar 26 09:24:58 2017 Info: sophos updating component ide
Sun Mar 26 09:24:58 2017 Info: sophos updating component libsavi
Sun Mar 26 09:24:58 2017 Info: sophos updated engine,ide links successfully
Sun Mar 26 09:24:58 2017 Info: sophos cleaning up base dir /data/third_party/sophos
Sun Mar 26 09:24:58 2017 Info: sophos sending version details
{'sophos': {'version': '5.36', 'ide': '2017032603'}} to hermes
Sun Mar 26 09:24:58 2017 Info: sophos verifying applied files
Sun Mar 26 09:24:58 2017 Info: sophos updating the client manifest
Sun Mar 26 09:24:58 2017 Info: sophos update completed
Sun Mar 26 09:24:58 2017 Info: sophos waiting for new updates
```

A chave nos updater_logs a procurar é da “as linhas de registro das atualizações novas terminadas” e “de esperas” atualização. Uma vez que aqueles são indicados, você pode entrar nos **sophos do avstatus** comanda outra vez a fim verificar que a versão e as datas estão atualizadas.