

# o vESA não pode transferir e aplicar atualizações para Antispam ou Antivirus

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[o vESA não pode transferir e aplicar atualizações para Antispam ou Antivirus](#)

[Ajuste o dispositivo para usar o host dinâmico correto URL](#)

[Verificar](#)

[Troubleshooting](#)

[Informações Relacionadas](#)

## Introdução

Este documento descreve quando uma ferramenta de segurança virtual do email (vESA) não transfere e aplica atualizações para o motor do antispam de Cisco (CASO) ou o antivirus de Sophos e/ou da McAfee, mesmo que o dispositivo virtual esteja licenciado corretamente.

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Ferramenta de segurança do email (ESA)
- vESA, ferramenta de segurança do web virtual (vWSA), dispositivo virtual do Gerenciamento de segurança (vSMA)
- AsyncOS

### Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- o vESA, esse executa AsyncOS 8.0.0 e mais atrasado
- o vWSA, esse executa AsyncOS 7.7.5 e mais atrasado
- o vSMA, esse executa AsyncOS 9.0.0 e mais atrasado

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

# o vESA não pode transferir e aplicar atualizações para Antispam ou Antivirus

Quando você atualiza o antispam ou o antivirus, os processos não podem alcançar para fora e atualizar o motor ou os rulesets do serviço, mesmo se você incorpora o comando da **força da atualização**.

Um destes comandos pôde ter sido incorporado diretamente do CLI no vESA:

```
> antispamupdate ironport
>antispamupdate ironport force
>antivirusupdate force
>updatenow force
```

Quando você executa **updater\_logs da cauda**, os erros considerados são similares a estes:

```
Mon Oct 21 17:48:43 2013 Info: Dynamic manifest fetch failure: Received invalid
update manifest response
```

Isto indica que o host dinâmico URL associado à configuração da atualização não pode alcançar corretamente o updater apropriado manifesto. O host dinâmico URL é ajustado dentro do comando do **updateconfig**. O subcommand, **dynamichost**, é um comando oculto dentro do **updateconfig**, como destacado aqui:

```
myesa.local> updateconfig
Service (images): Update URL:
-----
Feature Key updates http://downloads.ironport.com/asyncos
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
IMS Secondary Service rules Cisco IronPort Servers
Service (list): Update URL:
-----
McAfee Anti-Virus definitions Cisco IronPort Servers
RSA DLP Engine Updates Cisco IronPort Servers
PXE Engine Updates Cisco IronPort Servers
Sophos Anti-Virus definitions Cisco IronPort Servers
IronPort Anti-Spam rules Cisco IronPort Servers
Intelligent Multi-Scan rules Cisco IronPort Servers
Outbreak Filters rules Cisco IronPort Servers
Timezone rules Cisco IronPort Servers
Service (list): Update URL:
-----
Cisco IronPort AsyncOS upgrades Cisco IronPort Servers
Update interval: 5m
Proxy server: not enabled
HTTPS Proxy server: not enabled
Choose the operation you want to perform:
- SETUP - Edit update configuration.
[ ]> dynamichost

Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]>
```

# Ajuste o dispositivo para usar o host dinâmico correto URL

Há duas o host dinâmico diferente URL que são usados para os clientes baseados em como são associados através de Cisco:

- update-manifests.sco.cisco.com:443
- Uso: VESA do cliente, vWSA, vSMA

**Nota:** As ferramentas de hardware (C1x0, C3x0, C6x0, e X10x0) devem SOMENTE usar o host dinâmico URL ofupdate-manifests.ironport.com:443. Se há uma configuração de grânulos com o ESA e o vESA, o **updateconfig** deve ser configurado a nível da máquina e então confirmar que o **dynamichost** está ajustado em conformidade.

- stage-stg-updates.ironport.com:443
- Uso: Friendlies, beta virtual e ferramentas de hardware

**Nota:** Os clientes devem somente usar o server URL da atualização da plataforma se acederam a preprovisioning através de Cisco para o beta uso somente. Se você não tem uma licença válida aplicada para o beta uso, seu dispositivo não receberá atualizações dos server da atualização da plataforma.

Como uma continuação do **updateconfig** e do subcommand do **dynamichost**, incorpore o host dinâmico URL como necessário, retorno à alerta principal CLI, e comprometa as mudanças:

```
Enter new manifest hostname : port
[update-manifests.sco.cisco.com:443]> stage-stg-updates.ironport.com:443
[]> <<<HIT RETURN TO GO BACK TO THE MAIN CLI PROMPT>>>
```

```
myesa.local> commit
```

## Verificar

A fim verificar que o dispositivo alcança agora para fora ao host dinâmico apropriado URL e às atualizações é bem sucedido, termine estas etapas:

1. Aumente os **updater\_logs** para debugar. Currently configured logs:> logconfig

```
Log Name Log Type Retrieval Interval
-----
1. antispam Anti-Spam Logs Manual Download None
[SNIP FOR BREVITY]
28. updater_logs Updater Logs Manual Download None
29. upgrade_logs Upgrade Logs Manual Download None
Choose the operation you want to perform:
- NEW - Create a new log.
- EDIT - Modify a log subscription.
- DELETE - Remove a log subscription.
- SETUP - General settings.
- LOGHEADERS - Configure headers to log.
- HOSTKEYCONFIG - Configure SSH host keys.
[]> edit
Enter the number of the log you wish to edit.
[]> 28 [NOTE, log # will be different on a per/appliance basis]
Please enter the name for the log:
[updater_logs]>
Log level:
```

```
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]> 4
[SNIP FOR BREVITY]
```

```
myesa_2.local> commit
```

2. Execute uma atualização da força no antispam (**força do antispamupdate**) ou no antivírus (**força do antivirusupdate**). myesa.local> antivirusupdate force

```
Sophos Anti-Virus updates:
Requesting forced update of Sophos Anti-Virus.
```

3. Finalmente, os **updater\_logs da cauda** e asseguram-se de que o dispositivo possa alcançar o **dynamichost** como indicado: Mon Oct 21 18:19:12 2013 Debug: Acquiring dynamic manifest from stage-stg-updates.ironport.com:443

## Troubleshooting

Termine estas etapas a fim de pesquisar defeitos em todas as edições:

1. Assegure-se de que o **updateconfig** do padrão esteja usado. Se o vESA ou o host são atrás de um Firewall, assegure-se de que as [atualizações com um server estático](#) estejam no uso.
2. Assegure-se de que você possa **telnet** ao host dinâmico URL como escolhida: > telnet

```
Please select which interface you want to telnet from.
```

```
1. Auto
2. Management (172.16.6.165/24: myesa_2.local)
3. new_data (192.168.1.10/24: myesa.local_data1)
```

```
[1]>
```

```
Enter the remote hostname or IP address.
```

```
[> stage-stg-updates.ironport.com
```

```
Enter the remote port.
```

```
[25]> 443
```

```
Trying 208.90.58.24...
```

```
Connected to stage-stg-updates.ironport.com.
```

```
Escape character is '^'.
```

```
^] ["CTRL + ]"
```

```
telnet> quit
```

```
Connection closed.
```

## Informações Relacionadas

- [Elevações ou atualizações satisfeitas da ferramenta de segurança com um server estático](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)