Troubleshoot vESA Unable to Download and Apply Antispam or Antivirus Updates

Contents

Introduction

Prerequisites and Warnings

- Requirements
- Components Used
- Important Notes

Symptoms

Set the Correct Dynamic Host URL

Verify Appliance Update Functionality

Troubleshooting Steps

Related Information

Introduction

This document describes why vESA fails to update antispam or antivirus engines, despite having valid licensing.

Prerequisites and Warnings

Requirements

Ensure familiarity with these products and concepts:

- Email Security Appliance (ESA)
- vESA, virtual Web Security Appliance (vWSA), virtual Security Management Appliance (vSMA)
- AsyncOS

Components Used

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, ensure that you understand the potential impact of any command.

Important Notes

- Hardware appliances (C190, C195, C390, C395, C690, and C695) must use the dynamic host URL **update-manifests.ironport.com:443** only.
- Only use staging update server URLs if Cisco has provisioned access for Beta usage. Without a valid Beta license, updates will not be received from staging servers.
- In cluster configurations with both ESA and vESA, configure **updateconfig** at the machine level and confirm the **dynamichost** is set accordingly.

Symptoms

vESA does not successfully download or apply updates for antispam or antivirus engines, even when properly licensed. Running update commands such as:

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

does not resolve the issue. Reviewing logs with **tail updater_logs** displays errors similar to:

```
Mon Oct 21 17:48:43 2025 Info: Dynamic manifest fetch failure: Received invalid update manifest respons
```

This indicates the appliance cannot reach the correct updater manifest at the dynamic host URL configured via the **updateconfig** command. The **dynamichost** subcommand, available within **updateconfig**, defines which update server the appliance will use.

Set the Correct Dynamic Host URL

Configure the dynamic host URL according to your appliance type and support status:

1. **update-manifests.sco.cisco.com:443**
    - Use for vESA, vWSA, and vSMA appliances.
2. **stage-stg-updates.ironport.com:443**
    - Use for friendlies, Beta virtual, and hardware appliances with explicit Cisco Beta authorization only.

To set the dynamic host URL, use the **updateconfig** command, access the hidden **dynamichost** subcommand, enter the desired host and port, then commit the changes.

<#root>

esa.example.com>

updateconfig

[]>

dynamichost

```
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>>>

esa.example.com> commit

Verify Appliance Update Functionality

Use these steps to confirm the appliance is updating from the correct dynamic host URL:

1. Increase the **updater_logs** log level to **debug** to capture detailed update activity:

```
<#root>

esa.example.com>

logconfig

[...]
28.

updater_logs

 Updater Logs Manual Download None
[...]
[]>

edit

Enter the number of the log you wish to edit.
[]>

28

Please enter the name for the log:
[updater_logs]>
Log level:
1. Critical
2. Warning
3. Information
4. Debug
5. Trace
[3]>

4

[...]
esa.example.com>

commit
```

Note: The log number can differ on each appliance.

---

2. Run a forced update to test connectivity and update functionality:

```
<#root>

esa.example.com>

updatenow force
```

```
Success - Force update for all components requested
```

3. Review **updater_logs** to confirm a successful connection to the correct dynamic host:

```
Mon Oct 21 18:19:12 2025 Debug: Acquiring dynamic manifest from stage-stg-updates.ironport.com:443
```

Troubleshooting Steps

1. Confirm that the default **updateconfig** is being used. If vESA or its host is behind a firewall, ensure updates are configured to use a static server as described in the Content Security Appliance Upgrades or Updates with a Static Server document.
2. Test connectivity to the dynamic host URL using Telnet to verify network reachability:
<#root>

```
esa.example.com>
```

```
telnet
```

```
Please select which interface you want to telnet from.
1. Auto
2. Management (172.16.6.165/24: esa-mgmt.example.com)
3. Data (192.168.1.10/24: esa-data.example.com)
[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.
```

Related Information

- **Content Security Appliance Upgrades or Updates with a Static Server**
- **Technical Support & Documentation - Cisco Systems**