Troubleshooting Guide for Forcepoint Security Appliance Manager

Troubleshooting | Forcepoint Security Appliance Manager | v2.x

Overview

Use this Troubleshooting Guide to find solutions to common Forcepoint Security Appliance Manager (FSAM) issues before contacting Technical Support.

The Forcepoint Support site features an extensive Knowledge Base and customer forums. Search for topics by keyword or phrase, or browse content by product and version.

For more information about FSAM, see the Forcepoint Security Appliance Manager User Guide.

For deployment and installation information, see the Forcepoint Security Appliance Manager Installation Guide.

To learn about what is new and improved for the latest version of FSAM, see the Forcepoint Security Appliance Manager Release Notes.

Contents

Troubleshooting instructions are grouped into the following sections:

FSAM troubleshooting best practices

- Verify that all appliances are registered in Forcepoint Security Manager (FSM, formerly called TRITON Manager), with SSO enabled.
- Verify compatibility between appliance versions and FSAM version.
- Verify that all of the correct hotfixes are installed.

- Verify that the issue you are experiencing is not a CLI or API issue before troubleshooting FSAM.
- Refresh the browser page. This refreshes the connection to each appliance.
- Before making any changes to the Security Manager, such as an upgrade or uninstall/reinstall, be sure to uninstall FSAM. Then make the changes to the Security Manager and reinstall FSAM.
- If you have recently uninstalled and reinstalled (or upgraded) FSAM and notice unexpected behavior, log out, clear the browser cache, and then log back in to FSAM.

Troubleshooting logs

There are several logs that are useful for troubleshooting FSAM.

bulk_processor.log

Location: <install location>\SAM\server\bulk_processor\logs

Each bulk action log is in the directory that matches its ID (for example: 20180918194933761_hotfix)

In this directory, you will find a file named “download.log”, “install.log”, or “uninstall.log” for each individual part of the bulk action.

eip_api.log

Location: <FSAM install location>\SAM\server\eip_api\log

ssl_error.<timestamp>.log

Location: <TRITON install location>\EIP Infra\apache\logs

Appliance logs

Location: /var/log/appliance

Use the files named “uwsgi.log” and “api.log” for debugging FSAM.

General FSAM issues

Any unexpected error

For any unexpected error, see the *FSAM troubleshooting best practices* section. If it is necessary to contact Technical Support, follow these steps to gather information:

1. Enable the browser console log and try the action again.
2. Use the “inspect” function and on the console type: “commonMethods.consoleToggle(true)”
3. Copy, paste, and save the resulting log into a text file.

4. In the **Inspect** window, click the **Network** tab, refresh the browser, then right click the **Network** tab to save the HAR file.

FSAM stuck on screen with "Loading..." message

After opening the Forcepoint Security Appliance Manager (FSAM) and logging on, the screen gets stuck and just shows a "Loading..." message indefinitely.

This issue may be related to unregistered Appliances. To resolve this issue, if the Windows firewall is enabled and running:

1. Log on to the Forcepoint Security Manager (FSM) where the FSAM is installed.
2. Click Start and search for Windows Firewall with Advanced Security.
3. Click Inbound Rules on the left side menu.
4. Click New Rule on the right side menu.
5. Select Port and click Next.
6. Select TCP, type 9443 in the Specific local port box, and click Next.
7. Select Allow the connection and click Next.
8. Leave Domain, Private and Public selected. Select them if they are not.
9. Name the rule as desired and click Finish.
10. Perform steps 3-9 for Outbound Rules as well.
11. Log on to the Forcepoint Security Manager.
12. Click Appliance > Register Appliance to register the new appliance.

The issue may also involve required hotfixes or other updates. Please refer to the most recent FSAM Release Notes and to *Upgrade and hotfix issues*.

Appliance/Security Manager issues

FSAM Appliances are showing the wrong version or grayed out

After installing the Forcepoint Security Appliance Manager (FSAM), one or more appliances are either showing as an older version, or they are grayed out in the manager itself.

The two primary causes are showing the version (8.2 or prior) or having a hotfix installed for a version of FSAM that is not installed.

Showing the wrong version can be caused by installing the FSAM before upgrading an appliance. The solution is to re-register the appliance in the Manager GUI:

1. Click appliances or the Plug icon User-added image at the top right of the screen in the Forcepoint Security Manager (formerly known as the TRITON Manager).
2. Click X Unregister.
3. Click + Register Appliance at the top left.

4. Type the C interface IP address.
5. Enable Single Sign On.
6. Enter the admin password used to log in when using CLI with Putty.
7. Click Okay.
8. Launch the FSAM again and check the appliance.

If the correct version is displayed, but the appliance is grayed out, first attempt the steps above to resolve Single Sign On (SSO). If the issue continues, it may be hotfix related. See *Upgrade and hotfix issues*.

Appliance cannot be reached (displays as “No registered Appliances found”)

After installing Forcepoint Security Appliance Manager (FSAM), a warning displays, saying that no registered Appliances are found. To resolve this issue:

1. Verify that the FSM server can reach the appliance in question.
   a. Use the Curl command (execute from a Linux machine that can reach FSM):
   curl -ik -X GET -u admin 'https://<triton IP>:9443/api/app/v1/appliances/<appliance IP>/sys'
   b. Capture data coming in on the API port:
   tcpdump -nni eth0 tcp port 443
   c. Look at uwsgi logs on unreachable appliance:
   /var/log/appliance/uwsgi.log
   Verify API calls coming in

Networking issues

To troubleshoot networking issues:

1. Check traffic coming to the appliance: tcpdump -nni eth0 tcp port 443.
2. Run wireshark on the Windows machine simultaneously to capture traffic on the FSAM interface. Filter on port 9443.
3. Reload, restart, and check the status of the nginx service on the appliance.

   #systemctl reload nginx
   #nginx -t && systemctl restart nginx
   #systemctl status nginx

Upgrade and hotfix issues

> **Note**
> Before making any changes to the Security Manager, such as an upgrade or uninstall/reinstall, be sure to uninstall FSAM. Then make the changes to the Security Manager and reinstall FSAM.Solution information

To troubleshoot upgrade or hotfix issues:

1. Verify that all of the correct hotfixes are installed. See the FSAM Release Notes for your version of FSAM.

> **Note**
> There is a special situation for upgrading appliances from v8.3 to v8.4. Prior to FSAM v1.2.1, after upgrading an appliance from v8.3 to v8.4, the user was required to unregister the appliance from FSM and then re-register the appliance with SSO. FSAM even displays a special message box detailing this requirement. With FSAM 1.2.1 and later, it is still necessary to unregister and re-register the appliance, but there is now the additional requirement of installing Appliance v8.4 Hotfix 004 before FSAM will work.

Known issues

This section lists the known issues in the current release of the Forcepoint Security Appliance Manager. If no resolution is listed, please contact Technical Support.

- If a restore fails while another appliance is being upgraded, the user must refresh the FSAM in order to see an accurate upgrade status.
- After an appliance is upgraded, the appliance version displays incorrectly for a short period of time. To resolve this issue, refresh the appliance list.
- If a second edit window is open in the Interface tab, and an error occurs and is corrected, auto refresh remains active rather than remaining disabled.
- The Edit Appliance Info window stays open in Firefox. To resolve this issue, click on the Status tab and then on the Appliance Info link. The Edit Appliance Info window will now close.
- Manually setting the time to two hours ahead of the current time will cause the appliance to display an “unauthorized” error. To resolve this issue, refresh the browser or reboot the appliance.
- When an appliance’s date and time is set to manual, it still displays as synchronized with an NTP server. The Edit button indicates that the time is being set manually.

- If a server is first saved to the secondary or tertiary DNS field, and then subsequently a DNS server is saved to the primary DNS field, the DNS server that was intended to be saved to the secondary or tertiary DNS field (added first) will actually save to the (back-end) primary field, and the DNS server intended to be saved to the primary field will overwrite the DNS server saved to the (back-end) primary field. To resolve this issue, refresh the Interfaces tab.
- Attempting to import a large binary file may cause a “system unavailable” or similar error message. To resolve this issue, click any button in the Import Static IPv4 Routes dialog box.
- Interface status shows incorrect IPv6 enabled/disabled status.
- There are no backup files listed from the Forcepoint Security Appliance Manager. However, they are visible in CLI.