

v1.2.0 Release Notes for Forcepoint Security Appliance Manager

Release Notes | Forcepoint Security Appliance Manager | v1.2.0

Overview

Forcepoint is pleased to announce version 1.2 of the Forcepoint™ Security Appliance Manager (FSAM), a browser-based console that provides a central, graphical user interface for the configuration and management of your appliances.

The Security Appliance Manager allows you to configure settings and manage services of your Forcepoint V / X Series appliances and the Virtual Appliance for Web and Email security (versions 8.3.0 and later) in one place.

For more information about this release, see the [Forcepoint Security Appliance Manager User Guide](#).

For deployment and installation information, see the [Forcepoint Security Appliance Manager Installation Guide](#).

Use these Release Notes to learn about what is new and improved for v1.2 of the Forcepoint Security Appliance Manager.

Contents

["New in FSAM v1.2" on the next page](#)

["Benefits" on page 5](#)

["Key Features" on page 6](#)


["Known issues for Forcepoint Security Appliance Manager" on page 7](#)


New in FSAM v1.2

Version 1.2 of the Forcepoint Security Appliance Manager is required to manage v8.4 and later V Series, X Series, and Virtual Appliances for Web and Email security.

FSAM v1.2 includes enhanced functionality, allowing you to:

- ▶ Applying software upgrades directly to target appliance
- ▶ Applying hotfixes directly to target appliance
- ▶ Launch backup/restore directly to target appliance
- ▶ Customizable, user-friendly appliance information table
- ▶ Monitoring resource usage for selected appliance

 **Note:** The recommended screen resolution is 1920 x 1080.

 **Note:** Unless otherwise noted, FSAM does not support virtual appliances deployed in the public cloud, such as Microsoft Azure.

Parity features for long-term TRITON customers

For customers who are using appliance software versions 8.2 or earlier, Forcepoint Security Appliance Manager version 1.2 brings improved usability and appliance management capabilities without sacrificing any controls provided by the previous appliance management tool set. This allows customers to plan their software upgrades for the latest security enhancements without fear of losing appliance control and visibility. Block page customization, system log, and some troubleshooting commands in the legacy appliance local user interface are not yet implemented in this FSAM release, but these functions are fully accessible through the appliance CLI.

C interface IP address warning

Do not change the C interface IP address.

If you must change the C interface IP address, please contact Forcepoint Technical Support for assistance.

Changing the C interface IP address breaks the communication path to critical off-appliance Architecture components.

Upgrading to Forcepoint Security Appliance Manager v1.2

To upgrade to Forcepoint Security Appliance Manager v1.2, simply reinstall the FSAM using the installer tool. See the [Forcepoint Security Appliance Manager Installation Guide](#).

The installation of Forcepoint Security Manager v8.4 can cause FSAM v1.2 to fail. If you plan to upgrade the Forcepoint Security Manager (formerly named TRITON Manager) to v8.4, perform the following steps:

1. Uninstall FSAM v1.1 before or after upgrading Forcepoint Security Manager to v8.4

2. Install FSAM v1.2

If you have already upgraded the Forcepoint Security Manager to v8.4 and FSAM to v1.2:

1. Uninstall FSAM 1.2
2. Re-install FSAM 1.2

Benefits

Benefits of the Forcepoint Security Appliance Manager include:

- ▶ Centralized management for both physical and virtual appliances for Web and Email Security. This is particularly useful for those planning to move to the Cloud, allowing them to replace aging appliances with virtual appliances as an interim solution so they can maximize the return on their total appliance investment without sacrificing visibility or control.
- ▶ No need for additional investments because it resides in the same server as the Forcepoint Security Manager.
- ▶ Powerful and secure remote access by IT personnel from anywhere at any time: based on pure HTML5 with SSL support and decrypted authentication, it supports the full range of popular web browsers.

Key Features

Forcepoint Security Appliance Manager v1.2.0 features include:

- ▶ **Appliance information:** Information about all registered appliances, including status, hostname, IP settings, version, security mode, installed hotfix information, hardware platform, service tag, and latest appliance backup information. Additional appliance information is editable, including host-name, description, time zone, and date and time. Starting with version 1.2, administrators can also view real-time resource usages information.
- ▶ **Services status:** Status information about services for Proxy, Web Security, Network Agent, and Email Security services, as well as start/stop/restart functionality.
- ▶ **Interface information:** Editable network interface and domain name system (DNS) setting information.
- ▶ **Routing information:** Editable static IPv4/IPv6 route and component route information.
- ▶ **Backup and restore:** The ability to backup and restore appliances from a remote appliance or a centralized filestore.
- ▶ **Upgrades and hotfixes:** The ability to install appliance upgrades and hotfixes, and to view the history of installed upgrades and hotfixes.
- ▶ **Remote access capabilities:** The ability to toggle on or off SSH functionality for remote technical support access into the Command Line Interface (CLI).
- ▶ **SNMP features:** Editable SNMP setting and event functionality for Appliance Controller, Proxy, Web Security, Network Agent, and Email Security modules.
- ▶ **Configuration summary:** The ability to gather data from the appliance and generate a file that can be sent to Forcepoint Technical Support for analysis and debugging.

Known issues for Forcepoint Security Appliance Manager

A list of [known issues](#) in this release is available to Forcepoint customer.