Forcepoint

Email Security

8.5.7

Release Notes

Revision A

Contents

Contents

Introduction

Forcepoint Email Security is an appliance-based system that prevents malicious email threats from entering an organization's network, and protects sensitive data from unauthorized email transmission. The Forcepoint Email Security solution is available on a V Series appliance, an X Series appliance security blade, or a virtual appliance, which can be downloaded from the Forcepoint Customer Hub downloads menu. See the Forcepoint Appliances Getting Started Guide for detailed information about configuring any Forcepoint appliance.

See the Administrator Help for detailed information on Forcepoint Email Security operations.

New Features

Service Management migration to systemd on ESG Appliance

In Email Security Gateway (ESG) On-Prem v8.5.7, service management tool is changed from **daemon-tools** to **systemd**. As a result, legacy commands such as `svc` and `svstat` are no longer available after root login.

To align with this change, the following updated commands are now supported for managing services:

- Start all services managed by systemd: `esg_system_stl start`
- Stop all services managed by systemd: `esg_system_stl stop`
- Check service status managed by systemd: `esg_system_stl status`

Alternatively, you can use the following scripts:

- Start all service: `esg_boot.sh`
- Stop all service: `esg_restart.sh`

Security Updates

Version 8.5.7 includes the following security updates

Updates	Description
SameSite cookie attribute update.	Sensitive cookies were missing the `SameSite` attribute, which could allow cross-site request forgery (CSRF). This issue is fixed with a cookies update to include the `SameSite=Lax` attribute.
Spring Framework denial of service (DoS) vulnerability.	The product used an outdated Spring Framework version vulnerable to DoS via crafted SpEL expressions (CVE-2022-22950). This issue is fixed with a framework upgrade to a secure version.
Apache Tomcat 7.0.x Security End of Life vulnerability.	Apache Tomcat 7.0.109 is no longer supported, exposing the system to unresolved security vulnerabilities. This issue is fixed with an upgrade to the latest available version.
Spring Security RegexRequestMatcher authorization issue.	Spring Security versions prior to 5.5.7 and 5.6.4 could allow authorization bypass due to misconfigured regular expressions (CVE-2022-22978). This issue is fixed with an upgrade to version 5.5.7, 5.6.4, or later.
libcurl cookie injection vulnerability.	libcurl versions prior to 8.4.0 allowed attackers to inject cookies into requests (CVE-2023-38546). This issue is fixed with an upgrade to version 8.4.0 or later.
Real Time Monitor cross-site scripting (XSS) vulnerability.	Real Time Monitor versions prior to 8.5.5 Hotfix 3 were vulnerable to stored XSS in email log entries. This issue is fixed with input sanitization and improved validation based on OWASP guidance for XSS prevention.
Log Database password disclosure in ESG.	ESG versions prior to 8.5.5 allowed saved database passwords to be exposed through the Log Database status check feature. This issue is fixed with an update to the authentication mechanism to prevent password leakage.
Missing Oracle Java Critical Patch Updates (CPUs) in ESG.	ESG used a Java version without required Oracle security patches, exposing it to vulnerabilities including CVE-2020-14803, CVE-2021-23841, CVE-2021-3450, CVE-2021-2161, and CVE-2021-2163. This issue is fixed with an update to a supported Java version that includes all required CPUs.
Tomcat version disclosure in Policy Enforcement Module (PEM) and Web Security Module (WSM) application ports.	A vulnerability in PEM and WSM allowed Tomcat version details to be exposed through unsupported HTTP methods, potentially aiding further attacks. This issue is fixed with an update to the `ServerInfo.properties` file to suppress version disclosure.

Updates	Description
Directory traversal vulnerability in ESG using TIBCO JasperReports Library.	ESG was using TIBCO JasperReports Library version 6.0.3, which was affected by a directory traversal vulnerability (CVE-2018-18809) that could allow users to access host system contents. This issue is fixed with an update to version 6.3.5 or later.
OpenJDK multiple vulnerabilities.	ESG was using OpenJDK versions earlier than 8u362, 11.0.18, 17.0.6, and 20.0.1, which are affected by multiple vulnerabilities including CVE-2023-21930, CVE-2023-21937, CVE-2023-21938, CVE-2023-21939, CVE-2023-21954, CVE-2023-21967, and CVE-2023-21968. This issue is fixed with an update to a supported version of OpenJDK that includes all required security patches.
Legacy login page displayed when accessing Forcepoint Security Manager (FSM) using `/esg` path.	While accessing FSM with the `/esg` path, an outdated Websense login page was displayed, which could expose deprecated content. This issue is fixed with an update to redirect the path to the appropriate interface.
Subscription key displayed in plain text on **Subscription** page	The subscription key was visible in plain text on the **Subscription** page under **Email** > **General**, which could expose sensitive information. This issue is fixed with an update to mask the subscription key from the user interface.
Vulnerability in OpenSSL version 1.0.2y on application hosts.	A vulnerability in OpenSSL 1.0.2y was identified on application hosts, potentially leading to buffer overread and exposure of sensitive memory. This issue is fixed with an update to OpenSSL 3.014, which addresses the referenced security advisory.
Incorrect filename displayed for attachment downloaded from **Log Details**.	Downloading a quarantined attachment from the **Log Details** page showed an incorrect filename, which could affect traceability or misrepresent potentially malicious content. This issue is fixed with an update to preserve and display the original attachment name accurately.
Privilege escalation via unquoted service path in WebsenseEsgStunnel.	An unquoted service path in the WebsenseEsgStunnel service allowed potential privilege escalation by executing unintended binaries. This issue is fixed with an update to enclose the service path in quotes to prevent unintended execution.
XSS vulnerability through attachment name in **Blocked Messages**.	An XSS vulnerability allowed execution of malicious scripts when viewing malicious attachment names in **Blocked Messages**. This issue is fixed with an update that sanitizes attachment names to prevent script execution.
Input validation issue in PEM login page.	Input submitted to the PEM login page was reflected in server responses, indicating insufficient input validation. This issue is fixed with an update that properly sanitizes input to prevent reflection.

Enhancements

The following improvements have been made for the appearance and usability of Forcepoint Email Security:

Enhancement	Description
OS upgrade to Oracle Linux 8.	Added support for deploying and running ESG on Oracle Linux 8 with a unified installer to ensure OS compliance.
OpenSSL upgrade to 3.0.14	Upgraded OpenSSL to version 3.0.14
Mail Transfer Agent (MTA) Postfix upgrade to 3.9.	Upgraded MTA Postfix from version 2.6 to 3.9 to ensure compatibility with Oracle Linux 8 and OpenSSL 3.
Python upgrade to 3.9.	Upgraded ESG to support Python 3.9 and resolved related issues.
PostgreSQL upgrade to 9.15.	Upgraded PostgreSQL from an unsupported version to 9.15 for ongoing support and security.
Google Noto font replacement.	Replaced Arial Unicode with Google Noto font to address licensing and compatibility.
Policy Engine upgrade to 10.3.	Upgraded the Policy Engine in ESG to version 10.3 to ensure compatibility with Oracle Linux 8.
Endpoint Integration Protection (EIP) agent upgrade to 10.3.	Upgraded the EIP agent in ESG to ensure compatibility, stability, and continued support.

System Requirements

On-premises Email Security is supported on the following platforms.

- Forcepoint V Series appliance: V20000 G1, V10000 G4 (R1 and R2), V5000 G4 (R1 and R2), V5000 G5, V10000 G5, or V20000 G5
- Forcepoint X Series modular chassis security blade: X10G G2 (R1 and R2)
- Virtual appliance

Download the appropriate image file from the Forcepoint Customer Hub downloads menu. See the Forcepoint Appliances Getting Started Guide for system requirements and deployment information.

Version 8.5.7 Email Virtual Appliances are certified and supported for VMware ESXi 8 / 7 / 6.7 / 6.5 / 6.0. A stable release of ESXi is recommended to avoid unexpected issues.

Note

For ESXi 8, 7 and 6.7, users must use the v8.5.5 OVA file to create a new VM. Versions 8.5.3 and earlier will not deploy and are not supported on ESXi 7 or 6.7.

The Forcepoint Security Manager and Email Log Server are hosted on a separate Windows Server machine. This server must be running an English language instance of Windows Server.

Microsoft SQL Server is used for the Email Log Database. See System requirements for this version for detailed information about supported applications and versions.

Important

Although a version 8.0 and later Security Manager can allow an earlier version appliance (e.g., version 7.8.4) to be added on the Email Appliances page, the management settings for that appliance are read-only and cannot be modified.

For optimal system efficiency and performance, we strongly recommend that manager console and appliance versions match.

If your Microsoft SQL Server installation uses a named instance, port 1433 is opened on the firewall even if you specify a different port during Email Security installation. You must manually change this port setting after installation is complete.

See Installing Forcepoint Email Security for installation procedures.

Third-party platform and product support

This version adds support for:

- Microsoft SQL Server 2022
- VMware ESXi 8.0
- VMware ESXi 7.0
- Microsoft AD 2022

This version ends support for:

- Microsoft Windows Server 2016 (all versions)

See the Certified Product Matrix for information about all supported platforms.

Upgrade Paths

- If you are running Forcepoint Email Security version 8.5.5, you can upgrade directly to Forcepoint Email Security version 8.5.7. You must perform intermediate upgrades if you are running any other previous version of Email Security Gateway or TRITON AP-EMAIL.
- To migrate from Forcepoint Email Security version 8.5.4 or 8.5.5 to Forcepoint Email Security version 8.5.7, you must first install Forcepoint Email Security version 8.5.5 HF 302.
- To upgrade the virtual appliance to Forcepoint Email Security version 8.5.7, you must add a 26 GB virtual hard disk to the virtual appliance.

- To upgrade from Forcepoint Email Security version 8.5.5 to Forcepoint Email Security version 8.5.7, you must install the Appliance version 8.5.5 HF 300.
- To upgrade from Forcepoint Email Security version 8.5.6 to Forcepoint Email Security version 8.5.7, you must install the Appliance version 8.5.6 HF 300.

Resolved Issues, Known Issues, and Known Limitation

Resolved issues

The following issues have been resolved in this v8.5.7 release:

Issue Number	Description
ESG-17994	Inbound emails could not be delivered as the Simple Mail Transfer Protocol Daemon (smtpd) process stopped due to a memory overflow issue.
ESG-17452	Random messages were dropped into the exception queue with the `Exception Abort` error.
ESG-16910	The policy log view details in message logs showed repetitive URLs when multiple partitions were used in SQL.
ESG-17451	A security concern was raised regarding the storage of clear-text passwords in the `catalina.properties` file, with a recommendation to implement encryption.
ESG-17453	The filter crashes when processing non-decodable URLs or URLs longer than 2048 bytes.
ESG-17990	Duplicated and incomplete recipient names in the ESG Filter daemon occurred.
ESG-17997	Multiple users within the same network group received super administrator access simultaneously.
ESG-18097	Domain groups and IP addresses added were not listed in FSM, although their counts were visible.
ESG-17702	The limit for adding appliance in FSM increased to 42.
ESG-18383	The issue of improper authorization on encrypted email has been resolved.

Known issues

The current list of known issue is as follows:

Issue Number	Description
ESG-18434	The **Resume Processing** functionality for quarantined messages under **PEM** > **General Settings** is currently non-functional.
ESG-18120	For some emails, when the mail client does not encode them correctly, the filtering process still attempts to decode the emails using the default charset.
ESG-18435	Alerts are not generated in the Forcepoint Email Security when using a stripped-down license.

Known limitation

The current list of known limitation is as follows:

- Forcepoint Email Security version 8.5.7 does not support FIPS mode. If customers have it enabled, FIPS mode will be disabled by default after upgrading or migrating to Forcepoint Email Security version 8.5.7.

Find Product Documentation

You can find product documentation, release notes, knowledge base articles, downloads, and case management in the Forcepoint customer hub. For further assistance, visit the Contact Support page.

You must log in to access the Forcepoint Customer Hub. If you don't have credentials, you can create an account.

© 2025 Forcepoint
Forcepoint and the FORCEPOINT logo are trademarks of Forcepoint.
All other trademarks used in this document are the property of their respective owners.
Published 13 November 2025