



Web Security On-prem and URL Filtering

8.5.6

Release Notes

Contents

- [Introduction](#) on page 2
- [New Features](#) on page 2
- [System requirements](#) on page 3
- [Security Updates](#) on page 4
- [Enhancements](#) on page 7
- [Third-party platform and product support](#) on page 7
- [Resolved and known issues](#) on page 8
- [Find product documentation](#) on page 8

Introduction

This document details product updates and new features added to Forcepoint Web Security On-prem and URL Filtering in this v8.5.6 release.



Note

The Content Gateway component is not included in Forcepoint URL Filtering deployments. Content Gateway information applies only to Forcepoint Web Security.



Note

Direct upgrade from 8.5.4 to 8.5.6 for DLP customer is not supported. To upgrade successfully from 8.5.4 to 8.5.6, first upgrade to DLP version included in 8.5.5 unified installer and then login to FSM to switch to DATA and allow the policies to be updated. After that upgrade to 8.5.6.

See the [Forcepoint Appliances Release Notes, v8.5.6](#) guide to find the supported versions of appliance.

Customers currently using a Red Hat Enterprise Linux version earlier than 7.9 will need to upgrade their operating system prior to upgrading the product.

New Features

New categories related to Artificial Intelligence (AI) and Machine Learning (ML) added

New categories related to AI and ML are added to the existing set of categories used by the Forcepoint URL Database.

Four new sub categories are added within the "**Information Technology**" parent category for easy and fine-grained policy management.

Customers can get more benefits and protect themselves against the potential risks coming with the game changing innovations happening in the field of AI and ML technologies.

The new categories are listed below:

Category Name	Description
Other AI ML Applications	Sites that provide tools or services related to AI and ML. Includes sites hosting applications with personal productivity or business purposes using AI but not typically capable of generating new content.
Generative AI – Multimedia	Sites that specialized in machine-generated multimedia content such as images, videos, or audios. Includes sites that provide information, tools, or services related to text-to-speech, video, music, sound, or image editing applications using AI with the ability to generate new content.
Generative AI - Conversation	Sites that specialized in machine-generated conversational content for the purpose of general information, user assistance, or entertainment. Includes sites hosting virtual agents and limited domain conversational applications using AI with the ability to generate new content.
Generative AI - Text & Code	Sites that provide machine-generated text with large domain applications (including code and translation) using AI and generating new content. Includes sites that provide tools or services that make suggestions, edits, reviews, or create summaries based on the user prompts and interactions.

Integrated CCA with Trellix engine

In this release, CCA is integrated with a new analytic engine **Trellix**. Two features [Decompression] and [MIME] are added to the existing configurations as an enhancement and to increase the overall efficacy of the product.

System requirements

To use this product, your system must meet the basic hardware and software requirements, see [System requirements for this version](#) in the Deployment and Installation Center guide.

**Note**

The EIP 10.2 installer requires both 32 and 64 bit Microsoft Visual C++ Redistributable packages to be installed.

Browser support

See the [Certified Product Matrix](#) for the latest list of supported browsers.

Security Updates

Forcepoint Security Labs Analysts continually assess potential security vulnerabilities which can be introduced by third-party libraries. Security improvements have been made in several areas in version 8.5.6.

Updates	Description
Missing Oracle critical patch updates for Java.	Java upgrades to the latest version to fix the following CVEs post 1.8.0.242: <ul style="list-style-type: none"> ■ CVE-2020-14803 ■ CVE-2021-23841 ■ CVE-2021-3450 ■ CVE-2021-2161 ■ CVE-2021-2163 ■ CVE-2020-14664 ■ CVE-2020-14583 ■ CVE-2020-14593 ■ CVE-2020-14562 ■ CVE-2020-14621 ■ CVE-2020-14556 ■ CVE-2020-14573 ■ CVE-2020-14581 ■ CVE-2020-14578 ■ CVE-2020-14579 ■ CVE-2020-14577 ■ CVE-2020-14792 ■ CVE-2020-14781 ■ CVE-2020-14782 ■ CVE-2020-14797 ■ CVE-2020-14779 ■ CVE-2020-14796 ■ CVE-2020-14798

Updates	Description
Apache Tomcat detects the default error page version number.	Apache Tomcat running on the remote host, reported its version number on the default error pages making it vulnerable to attack. To fix this issue, default error pages are replaced with custom error pages to hide the version number.
Apache ZooKeeper updates to latest.	<p>Apache ZooKeeper upgrades to the 3.4.14 version to fix the following security vulnerabilities that occurred due to out of date:</p> <ul style="list-style-type: none"> ■ CVE-2016-5017 ■ CVE-2017-5637 ■ CVE-2018-8012 ■ CVE-2019-0201
Vulnerable version of plexus-utils (CASB).	Plexus-utils upgrades to the 3.0.14 version to fix the CVE-2017-1000487 vulnerability.
Apache Tomcat Denial of Service (DoS) vulnerability.	A vulnerability in Apache Tomcat allows an attacker to remotely trigger a DoS. This issue is fixed by upgrading to the Apache Tomcat 10.1.0-M6, 10.0.12, 9.0.54, 8.5.72 versions or to the latest version of Apache Tomcat.
Host header handling via proxy.	Restricting multiple host headers via Proxy.
Forcepoint deprecated TLS version and SSL/TLS cipher policy violation.	Postgres running on port 6432 on Forcepoint Security Manager uses deprecated TLS versions and SSL/TLS cipher suites that are not Forcepoint approved.
Apache commons text Java library vulnerable to RCE (CVE-2022-42889).	Upgraded the version specified in CASB download 8.5.5 to the latest version to fix the Apache commons text Java library vulnerable (CVE-2022-42889) issue.
Multiple vulnerabilities in Apache 2.4.54.0.	Web Security Apache version 2.4.54.0 needs to be upgraded to Apache 2.4.55 to fix the multiple vulnerabilities in Apache 2.4.54.0.
Apache vulnerabilities CVE-2023-25690, CVE-2023-27522.	Web Security Apache version 2.4.55 or prior needs to be upgraded to Apache 2.4.56 to fix these Apache vulnerabilities CVE-2023-25690, CVE-2023-27522.

Updates	Description
Apache Tomcat 9.0.70 vulnerabilities.	<p>Apache Tomcat versions prior to 9.0.70 were vulnerable as stated in these CVEs:</p> <ul style="list-style-type: none"> ■ CVE-2023-46589 ■ CVE-2023-45648 ■ CVE-2023-42795 ■ CVE-2023-42794 ■ CVE-2023-44487 ■ CVE-2023-41080 ■ CVE-2023-28708 <p>Tomcat version 9.0.86 was sourced from the official Apache Tomcat site: https://tomcat.apache.org/index.html</p> <p>All SWG references to Tomcat were updated to point to the new version.</p> <p>All Tomcat server.xml files were updated to reflect SWG cipher restrictions and TLS standards.</p>
Logjam on Port 55866.	<p>The LOGJAM vulnerability allows man-in-the-middle attackers to conduct cipher-downgrade attacks by rewriting a ClientHello with DHE replaced by DHE_EXPORT and then rewriting a ServerHello with DHE_EXPORT replaced by DHE, aka the "Logjam" issue.</p> <p>We have now restricted the ciphers on port 55866 to "TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256" and "TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384". ECDHE ciphers are not vulnerable to the Logjam exploit.</p>
Persistent Cross-Site Scripting via user agent field.	<p>Cross-Site Scripting (XSS) is an attack in which an attacker injects malicious executable scripts into the code of a trusted application or website.</p> <p>The Forcepoint Security Manager was vulnerable to XSS via the user agent field which can be manipulated by the end user and displayed in the transaction viewer.</p> <p>The XSS vulnerability was mitigated by the use of HTML encoding of the user agent text. HTML encoding replaces certain characters that are semantically meaningful in HTML markup, with equivalent characters that can be displayed to the user. HTML encoding ensures that text is displayed correctly in the browser and not interpreted by the browser as HTML.</p>

For the basic hardware and software requirements for your system to use this product, see [System requirements for this version](#) in the Deployment and Installation Center.

Enhancements

Improvements have been made for the Hybrid Module of the Forcepoint Web Security.

Enhancement	Description
Refresh of the user interface styling.	The overall styling of the Forcepoint Security Manager has been refreshed for ease of navigation and clarity. Some error messages have also been updated to outline that solutions and articles can be found within Forcepoint customer hub .
Increase allowable size of the header in the Web Security Content Gateway.	Increased allowable size of the header to allow more than 8000 characters which needs to be added in the Web Security Content Gateway for restrict access to tenants for MS office.
Make secure auth as default, remove user interface option to disable it.	Secure auth is enabled by default.
In Web Security Content Gateway, search in code/config to find all reference to technical support.	Updated Web Security Content Gateway alarm links with actions/knowledge base links.
Add additional logging for debug purposes to ApplianceModeManager and associated classes.	Debugging logs are now added for mode switch error detection.
Winbind Recovery Script modifications for better handling Messages file.	If mutex error happens, Winbind recovery script (<code>/opt/WCG/contrib/samba/winbind_recovery</code>) takes a backup of messages file and restarts Winbind. Some times, if Mutex error happens continuously, then lot of messages files can be created of small size.
DLP Policy Engine upgrade.	DLP Policy Engine version is upgraded to version 10.2
CA tree upgrade.	Upgraded CA tree in this version 8.5.6 release.

Third-party platform and product support

All components

This version adds support for:

- Microsoft Windows Server 2022
- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Red Hat Enterprise Linux 7.9 and the corresponding version of CentOS
- VMware ESXi 8.0

This version ends support for:

- Microsoft Windows Server 2012 (all versions)
- Red Hat Enterprise Linux 7.6 and the corresponding version of CentOS

See the full list of supported operating systems [here](#).

See the [Certified Product Matrix](#) for the latest list of supported browsers.

Content Gateway

This version is supported on:

Red Hat Enterprise Linux 7.9 (and corresponding CentOS versions).



Important

Forcepoint Web Security customers using Red Hat Enterprise Linux or CentOS 7.x must disable firewalld prior to installing Content Gateway.

On the machine where Content Gateway will be installed, execute the following:

```
systemctl stop firewalld
systemctl disable firewalld
```

As a best practice, Red Hat Enterprise Linux systems that host Content Gateway should be registered with Red Hat Network and kept up-to-date with the latest security patches.



Important

You can update packages on your Red Hat Enterprise Linux installations and patch kernels if the underlying kernel upgrade does not change the kernel API.



Important

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

For a complete platform requirements information, see [System requirements for this version](#) in the Deployment and Installation Center.

Resolved and known issues

For a list of resolved and known issues in this product release, see Knowledge Base article [Resolved and Known Issues for Forcepoint Web Security On-prem, v8.5.6](#).

Find product documentation

In the Forcepoint Customer Hub, you can find information about a released product, including product documentation, technical articles, and more.

You can get additional information in the [Forcepoint customer hub](#) and support for your product in the [Contact Support](#) page. In Customer hub, you can access product documentation, release notes, knowledge base articles, downloads, cases, and contact information.

You might need to log on to access the Forcepoint Customer Hub. If you do not yet have credentials, create a customer account.

