v8.5.4 Release Notes for Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 8-June-2020

Use the Release Notes to find information about what's new and improved for Forcepoint Web Security and Forcepoint URL Filtering in version 8.5.4.

For information about endpoint client software, please refer to the Release Notes for Forcepoint Web Security Endpoint.

Note

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

Refer to the following when installing or upgrading to v8.5.4.

- Installing Forcepoint Web Security
- Installing Forcepoint URL Filtering
- When upgrading TRITON AP-WEB (v8.2.x or 8.3.x) or Forcepoint Web Security (8.4.x or 8.5.x), see Upgrade Instructions for Forcepoint Web Security
- When upgrading Web Filter & Security (v8.2.x or 8.3.x) or Forcepoint URL Filtering (8.4.x or 8.5.x), see Upgrade Instructions for Forcepoint URL Filtering
- Deployment and Installation Center

3

Important

V-Series appliance users:

Some older V10000 and V5000 appliances are not supported with version 8.0.0 and higher.

See V-Series appliances supported with version 8.x

Upgrades to v8.5.4 are supported from v8.4, v8.5, and v8.5.3. If you have an earlier version, there are interim steps to perform. These are shown below.

Your current version	Step 1	Step 2	Step 3	Step 4	Step 5
v7.1.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4
v7.5.x	Upgrade to 7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4
v7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4	
v7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4		
v7.8.1 v7.8.2 v7.8.3	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4		
v7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.4			
v8.0.x	Upgrade to 8.3.x*	Upgrade to 8.4.x	Upgrade to 8.5.4		
v8.1.x	Upgrade to 8.4.x	Upgrade to 8.5.4			
v8.2.x	Upgrade to 8.4.x	Upgrade to 8.5.4			
v8.3.x	Upgrade to 8.4.x	Upgrade to 8.5.4			
v8.4.x	Upgrade to 8.5.4				
v8.5.x	Upgrade to 8.5.4				
*** TRITON AP-WEB customers upgrading from v8.0.x to v8.3 should install Content Gateway v8.3 Hotfix 3 if v8.3 will be used in production prior to upgrading to v8.5.4.**					

Important

If you are currently running a Web Security Gateway or Gateway Anywhere version earlier than v7.8.4, upgrade to v7.8.4 first. See this upgrade guide for instructions.

- Content Gateway Hotfix 94 must be applied to v7.7.x prior to upgrading Content Gateway (software or appliance) to v7.8.4. This retains the default Sync Mode setting for real-time analysis, and can prevent latency.
- Appliance Hotfix 90 must be applied to v7.7.x prior to upgrading the appliance to v7.8.4. See the v7.8.x Upgrade Instructions.

Customers currently using Red Hat Enterprise Linux 6.8 or earlier, 7.0, 7.1, or 7.2 will need to upgrade their operating system prior to upgrading the product.

New in Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 8-June-2020

Product mapping

Version 8.0 was the first product release that used a new, simplified product naming and grouping of the familiar product line.

Version 8.4 then reset the product names to better align with the company vision.

v8.4 Product Name	v8.0 Product Name
Forcepoint URL Filtering	Web Filter & Security
Forcepoint Web Security	TRITON AP-WEB
Forcepoint Web Security with: • Forcepoint Web Security Hybrid Module • Forcepoint Web Security DLP Module • Forcepoint Advanced Malware Detection (if purchased)	TRITON AP-WEB with: • Web Hybrid Module • Web DLP Module • Web Sandbox Module (if purchased)

Security enhancements

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 8.5.4.

A security update done for the v8.5.4 product release has resulted in a new requirement for a specific dynamic-link library (dll) when installing or upgrading

v8.5.4 Forcepoint Web Security or Forcepoint URL Filtering software on a Windows platform.

If you have not recently downloaded the Visual C++ Redistributable Package from Microsoft, it is likely that the installation/upgrade will prompt with the error "Installation failed with error code 3004". The log file generated by the installation/upgrade process, available in the Temp folder of the user running the installer, will contain a line similar to:

```
java.lang.UnsatisfiedLinkError:
C:\Users\Administrator\AppData\Local\Temp\2\I1588276985\Wind
ows\resource\jre\bin\freetype.dll: Can't find dependent
libraries
```

The dependency referenced in this log entry is for **vcruntime140.dll**, a file that is part of the Redistributable Package.

Should the error occur during the install/upgrade process:

1. Close the error window but do NOT stop the install/upgrade process. Leave the installer window open.
2. Locate the latest 64-bit Redistributable Package for your Windows version from this site.
3. Download and install the package.
4. Return to the installation/upgrade window and continue the process.

Content Gateway enhancements

Enhancements have been made to Content Gateway.

- By default, all authentication for HTTPS requests is done over HTTP, using port 8080. A setting has been added to Content Gateway manager that enables authentication of HTTPS requests over HTTPS, using port 4443.

  Open Content Gateway manager and navigate to **Configure > Security > Access Control** and select **Global Authentication Options**. A new **Redirect Options** section contains the **Redirect Hostname** entry field as well as new options for **Redirect for HTTPS Authentication**.

  This new option is disabled by default. Click **Enabled** to direct all HTTPS requests to authenticate over HTTPS in transparent proxy deployments.

  Changing the manager options also resets a new records.config variable.

  ```
  proxy.config.auth.ssl_auth_url
  ```

- Content Gateway Manager currently offers either **Web DLP** or **ICAP** as the **Integration** options on the **Configure > My Proxy > Basic > General** page when Content Gateway is deployed with the DLP Module. By default, the options are provided with radio buttons, making them mutually exclusive.

A new variable has been added that changes the radio buttons to check boxes, making them both selectable. To enable the ability to select both options, add the following to records.config (in /opt/WCG/config, by default).

```
CONFIG proxy.config.dss_and_icap.enabled INT 1
```

When this variable is enabled (1), the UI will allow both check boxes to be selected. Change the value to 0 to disable the feature and change the selections back to radio boxes.

- When Content Gateway analysis returns a file type of "unknown", file type blocking is not done because there is no match for that value in the **Block file types** list configured for the category being used for policy enforcement.

  A new variable has been added that allows Content Gateway to send "unknown" as a valid file type to Filtering Service. To enable this feature, add the following to records.config (in /opt/WCG/config, by default).

  ```
  CONFIG wtg.config.filter_unknown_file INT 1
  ```

  Reset the value to 0 to disable the feature.

  In addition, when this variable is enabled, "unknown" is included in the list of file types displayed when creating a **Block file types list** for a specific category on the **Policy Management > Filters > Add/Edit Category Filter** page of Forcepoint Security Manager.

- Support for Integrated Windows Authentication (IWA) with Captive Portal authentication has been added.

  When a domain list that includes an IWA domain is used in rule-based authentication, the Captive Portal option is no longer disabled.

- SSL configuration settings for inbound and outbound traffic have been updated to remove support for SSL v2.

- The Session Cache section, previously available on **Configure > SSL > Decryption / Encryption** > **Outbound,** has been removed to avoid Content Gateway restarts. Upgrades to v8.5.4 will automatically disable these options if they had been previously enabled.

  Note that no significant performance differences were found after removing these caching options.

SIEM enhancements

Improvements have been made in Forcepoint Web Security to the Security Information and Event Management (SIEM) Integration feature.

- The **Settings > General > SIEM Integration** page of Security Manager now supports the entry of up to 10 SIEM integrations.

  The main page provides details for each of the SIEM solutions that have been added. Use the **Add** button to continue adding or click the link that is the IP Address of an existing entry to edit it.

Note that, with v8.5.4 and this new functionality, data from each Policy Server is no longer forwarded to all SIEM solutions configured for other Policy Servers assigned to the same Policy Broker.

- Web protection software provides an audit trail showing which administrators have accessed the Web module of Security Manager, as well as any changes made to policies and settings. Currently, these audit log records can be viewed on the **Status > Audit Log** page of Security Manager, or exported to an Excel spreadsheet.

  With 8.5.4, a new option has been added to the **Settings > General > SIEM Integration** page to support the ability to send audit log records to a SIEM integration defined for the primary Policy Server.

  In the new **Audit Log Data** section, check **Enable SIEM integration for this Policy Server** to enable the feature, then complete the remainder of the section.

  Note that this feature is available only for the primary Policy Server and does not appear if you are logged into a secondary Policy Server.

> **Important**
> SIEM Integration feature enhancements may result in the loss of SIEM data during an incremental upgrade. There is no loss of reporting data.
>
> See the Incremental Upgrade Guide for more information.

Other reporting enhancements

Enhancements have been made for some of the other reporting tools.

- Investigative Reports performance.
- Log database creation and upgrade process.
- Display issues in Investigative Reports.

Forcepoint Web Security Endpoint

New Forcepoint Web Security Endpoint builds are frequently released and we advise Forcepoint Web Security customers who use the Hybrid Module or whose deployment includes Forcepoint DLP to select the Downloads option from the My Account page to download the latest Endpoint build.

On the Downloads page:

1. Locate Endpoint Security.
2. Under Forcepoint One Endpoint, select the most recent build.
3. Follow the instructions in the Installation and Deployment Guide for Forcepoint Endpoint Solutions to install and deploy the latest build.

Browser support

See the Certified Product Matrix for the latest list of supported browsers.

Logon application support

Logon Agent communicates with the logon application (LogonApp) on client machines to identify users as they log onto or off of Windows domains.

- Logon Agent now supports Server Message Block versions 2 (SMBv2).

The logon application supports the following operating systems:

- Mac OS X 10.10 (64-bit)
- Microsoft Windows 8.1 Update 1 (32-bit and 64-bit; Windows 8.1 RT is not supported)
- Microsoft Windows 10

For more information about Logon Agent and the logon application, see the Using Logon Agent for Transparent User Identification white paper.

Third-party platform and product support

All components

This version adds support for:

- Red Hat Enterprise Linux 7.6 and the corresponding version of CentOS
- CentOS 7.7
- Microsoft Windows Server 2019
- Active Directory 2019
- VMware ESXi 6.7

This version ends support for:

- Red Hat Enterprise Linux 6.9, 7.3, and 7.4
- Microsoft Windows Server 2012 R2 DataCenter Edition
- Microsoft SQL Server 2008 SP2, 2012 SP2, and 2014 SP1
- Active Directory 2012
- VMware ESXi 5.5

See the full list of supported operating systems here.

See the Certified Product Matrix for the latest list of supported browsers.

> **Note**
> Newer versions of Google Chrome block Flash content. In order to successfully use your web solutions product, you will need to disable the blocking or use a different supported browser.

Note that installing web protection components on Windows Server 2012 or 2012 R2 requires Microsoft .NET Framework v.35 and v4.5. Install both and turn them both on before running the Forcepoint Security Installer.

Content Gateway

This version is supported on:

- Red Hat Enterprise Linux 6.9, 7.3, 7.4, and 7.5 (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

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering | 8-June-2020

A list of resolved and known issues in this release is available to Forcepoint Web Security or Forcepoint URL Filtering customers.