v8.5.0 Release Notes for Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering |28-Feb-2018

Use the Release Notes to find information about what's new and improved for Forcepoint Web Security and Forcepoint URL Filtering in version 8.5.0.

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 Filter deployments. Content Gateway information applies only to Forcepoint Web Security.

Refer to the following when installing or upgrading to v8.5.

- Installing Forcepoint Web Security
- Installing Forcepoint URL Filtering
- When upgrading TRITON AP-WEB (8.1.x, v8.2.x or 8.3.x) or Forcepoint Web Security (8.4.x), see Upgrade Instructions for Forcepoint Web Security
- When upgrading Web Filter & Security (8.1.x, v8.2.x or 8.3.x) or Forcepoint URL Filtering (8.4.x), see Upgrade Instructions for Forcepoint URL Filtering
- Deployment and Installation Center

> **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 are supported from v8.1, v8.2, v8.3 and v8.4. 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.x
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.x
v7.6.x	Upgrade to 7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	
v7.7.x	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	none	
v7.8.1 v7.8.2 v7.8.3	Upgrade to 7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	none	
v7.8.4	Upgrade to 8.4.x	Upgrade to 8.5.x	none	none	
v8.0.x	Upgrade to 8.3.x*	Upgrade to 8.5.x	none	none	
v8.1.x	Upgrade to 8.5x	none	none	none	
v8.2.x	Upgrade to 8.5.x	none	none	none	
v8.3.x	Upgrade to 8.5.x	none	none	none	
v8.4.x	Upgrade to 8.5.x				
*** 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.**					

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 6.7 or earlier 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 |28-Feb-2018

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.

Protected cloud apps (Web Security only)

Integration with Forcepoint CASB is now available with Forcepoint Web Security. Customers who have purchased the new Forcepoint Web Security Cloud App Control module or licenses for Forcepoint CASB can integrate their Web Security product and forward requests made to the purchased assets (called managed cloud apps in the web products) directly to CASB for proper handling.

In the Forcepoint Security Manager, navigate to **Web > Settings > CASB Configuration > Protected Cloud Apps**.

1. Enable the feature by switching the **Enable connection with Forcepoint CASB** option to ON.
2. Click **Connect to Forcepoint CASB** and use the information received in the fulfillment letter you received from Forcepoint CASB to enter your:
   a. Access key ID.
   b. API key secret.
   c. Service URL
   d. Click **Connect** to generate a connection to Forcepoint CASB.
3. Select from the list of cloud applications provided . Any requests to those applications will be forwarded to and monitored by Forcepoint CASB.

   You are limited by the number of apps for which your CASB license is valid.
4. Use the buttons provided to navigate to the Forcepoint CASB portal.
   - **View Incidents.**
   - **View Access Policies.**
   - **View Assets.**
5. On the **Settings > General > Filtered Locations** page, add a list of all locations where Internet traffic is managed by an instance of Content Gateway.

> **Note**
> The Filtered Locations page is also used when configuring the Hybrid Service. Customers who have purchased the Hybrid Module should be aware of the new location for this Forcepoint Security Manager page.

A CA certificate will be provided to each Forcepoint CASB customer and automatically downloaded to your deployment. This certificate must be uploaded to each Content Gateway server machine as well as installed on each client.

Policy enforcement for managed sanctioned apps

Policy enforcement is provided by Filtering Service for cloud application requests. The new action code “Protected cloud app request forwarded” is applied to requests to the managed applications when the requests are forwarded to Forcepoint CASB.

When policies are enforced, the list of managed applications is used to determine which protected application requests should be forwarded.

- If access to a cloud application is explicitly blocked based on the cloud app filter applied, security override, or a policy exception, the request is blocked even if the application has been selected in the managed list.
- If a cloud application is explicitly permitted in the cloud app filter, not included in the cloud app filter, or explicitly permitted in a policy exception, the list of managed applications is read.
  - If the application was selected on the managed list, the request is forwarded to the CASB service and a log record is generated with the action code "Sanctioned app request forwarded".
  - If the application was not selected on the managed list, the remaining policy enforcement rules are applied.

    See Administrator Help for details.

Use reports to track requests to the managed apps by finding the log records that are assigned the new action code.

Report Center

A new set of reporting tools has been added with version 8.5. These tools allow you to create multi-level, flexible reports that can be used for analysis of logging data, including cloud apps data (provided on the **Cloud Apps** tab of the **Reporting > Applications** page of manager).

Navigate to **Web > Main > Report Center** in the Forcepoint Security Manager.

- The **Report Catalog** offers a set of pre-defined **Standard Reports** for common scenarios, a list of all reports that have been marked as frequently used (**Favorites**), as well as the list of saved custom reports (**My Reports**).

  The **Standard Reports** are pre-defined templates which can be used as defined or as a starting point for new reports. They cannot be edited or deleted.
  - Use the toolbar options to create a new report or folder, copy, schedule, or delete a report, or to search for a report.
  - Use menu options to run, edit, copy, rename, delete, or schedule a report or to copy, rename, or delete folders.
  - When a report folder is selected, the reports pane is populated with the **Name**, **Type**, **Date Range**, and last **Modified** date for each report in the folder.

    The table is sorted by **Name** (with folders listed first). The sort can be changed by selecting one of the other columns.
- Use the **Report Builder** to create or view high-level reports from scratch.
  - Use the toolbar options to create, save, save as, or export a report.
  - Select the data elements from the list of **Attributes**.
  - Select the metrics to be included on the report from the **Metrics** list.

Requests is part of each report, by default.

- Add attributes to the Grouping field to define the data groupings for the report.

  Up to two attributes can be used to group the data.
- Use **Filters** to refine the report so that it includes the data you are specifically interested in.

  Filters can be used with both logging and cloud app data and can be applied to metrics as well as to attributes.
- Use **Date range** to define the time period to be covered by the report.

  Select a standard time period (between today and 3 months) or a specific date and time range.
- Select a chart option to display the data in chart format.
- Use drill down options such as “Filter Out”, “Show Only”, or “View Transactions” by selecting items to drill down into.

- Use the **Transaction Viewer** to create reports that offer more detailed information.
  - Use the toolbar options to create, save, save as, or export a report.
  - Select an attribute or metric report column to change the default sort.
  - Add filters to the report by dragging attributes or metrics in to the Filters field.
  - The **Date range** defines the time period (a standard time period or specific date and time) covered by the report.
  - Use the **Columns** drop-down to add columns to the report.
  - Enable **Detail View** or double click a row to open the **Transaction Details** page and view specifics about each transaction.
- The **Scheduler** allows you to add, maintain, and monitor jobs that will generate specified reports at defined times.
  - Select the reports to include in the job.
  - Define the schedule for the job.
  - Add a list of email addresses to which the reports in the job should be sent.
  - Select delivery options.

Within the Report Builder or the Transaction Viewer:

- Drag and drop functionality makes it easy to add and relocate report columns as well as add filters.
- Use **Search** to search for attributes to add to the report.
- **Export** options can be used to generate a PDF file or a comma separated list (CSV) that can be loaded into a spreadsheet.The exported data can include all or selected transactions, as well as detail data.

  A maximum of 20,000 table rows can be exported. Data exported from the detail view can include a maximum of 20 rows.
- Use the paging options provided on multiple page reports to navigate between pages.

- View the total number of rows in the report at the top of the page.

> **Note**
> In organizations that use the delegated administration reporting features, access to Report Center and its tools is defined for each administrator role.

Office 365 bypass

New bypass options have been added to Forcepoint Security Manager to allow requests to Office 365 to bypass either Content Gateway user authentication, the Content Gateway proxy, or both.

The **Web > Settings > Scanning > SSL Decryption Bypass** page of Security Manager has been renamed **Bypass Settings** and additional features have been added.

- Select the **SSL Decryption Bypass** tab to specify clients, websites, and website categories that are not subject to decryption and analysis as they flow through the proxy.
- On the **Authentication Bypass** tab, select **Office 365 and related applications** to allow requests to Office 365 applications to bypass the authentication process configured in Content Gateway manager.

> **Note**
> **Authentication bypass** for Office 365 is supported with explicit proxy deployments. Transparent proxy deployments are supported only if Content Gateway bypass for Office 365 and SSL decryption bypass for "Office - Collaboration" categories are not enabled.

  When this feature is enabled, appropriate rules are automatically added to the Content Gateway filter.config file for use by the proxy.
- Select **Office 365 and related applications** on the **Content Gateway Bypass** tab to allow requests to Office 365 applications to bypass the Content Gateway server completely.

> **Note**
> **Content Gateway bypass** is supported for transparent proxy deployments only.

Content Gateway enhancements

Enhancements have been made to Content Gateway.

- Content Gateway manager now provides an option to add a list of exceptions to authentication caching.

  > **Note**
  > This feature is supported only for explicit proxy deployments.

  A list of IP addresses or address ranges can be entered on the **Configuration > Security > Access Control > Global Authentication Options**.

  1. In the new Credential Caching section, select **Do not cache authentication requests from the specified IP addresses**
  2. Enter the IP addresses for which you do not want authentication information cached.

     All requests made from these IP addresses will be authenticated.
- The option of **TLSv1** on the **Configure > SSL > Decryption/Encryption** page (Inbound and Outbound tabs) and on the **Configure > Security > FIPS** page of Content Gateway Manager is no longer a default selection.

  Options for **TLSv1.1** and **TLSv1.2** have been added and enabled by default.
- Content Gateway now supports tunneling of WebSocket protocol traffic. (APWEB-10374, APWEB-10376, APWEB-10378, APWEB-10830)

SIEM enhancements

Improvements have been made to the way data that is forwarded to a supported Security Information and Event Management (SIEM) solution.

- New health alerts have been added to help ensure that all log data is successfully forwarded to a configured SIEM solution.
- New attributes have been added and new keys are available that will allow more information for hybrid log data to be included.

Reporting optimizations

Changes have been made to some of the reporting components, including the Log Database and Log Server, to provide improved functionality for logging and reporting.

General enhancements

Changes have been made in order to make the product more user friendly and to better protect our customers.

- Use of version 1 of Server Message Block (SMBv1) file protocol has been discontinued. SMBv2 is being used.
  - Active Directory Mixed Mode is no longer supported and is no longer an option on the **Web > Settings > General > Directory Services** page of Forcepoint Security Manager. See *Removed in this version* below.
  - User Service is now installed with Active Directory (Native Mode) as the default directory service.

    When upgrading to v8.5, deployments configured to use Active Directory Mixed Mode will be modified to use Active Directory (Native Mode).

    Re-add client information and re-assign clients to existing policies after the upgrade completes.

    In order for policy enforcement to be applied correctly immediately after upgrade, go to the **Web > Settings > General > Directory Services** page of the Forcepoint Security Manager prior to upgrade and configure the Global Catalog server for user and group based policies.
  - Logon Agent's NTLM authentication process now uses SMBv2.
  - DC Agent has been modified to remove the use of SMBv1 for domain discovery.

    When upgrading, the new DC Agent settings will overwrite the current configuration. Customers preferring to use SMBv1 can reset the appropriate settings in transid.ini. See Using DC Agent for Transparent User Identification for information.

    In conjunction with this change, the default selection for **Domain Discovery**, when the feature is enabled on the **Settings > General > User Identification > DC Agent** page of Forcepoint Manager, is **DC Agent**.
- Downloads of the Master Database and all other databases used by the product are now done over a secure HTTPS connection
- The results pane of the Test Filtering tool has been updated to include information for cloud applications.
- The password used for the **Password Override** feature enabled on the **Policy Management > Clients > Edit Clients** page of Security Manager now has the following requirements:
  - Must be between 8 and 255 characters
  - Must contain upper case characters
  - Must contain lower case characters
  - Must contain numbers
  - Must contain non-alphanumeric characters

Install and upgrade improvements

Improvements have been made to the installation and upgrade screens and process.

- The Linux installer for Web Security or URL Filtering has been updated to require haveged. When the installation is launched, a check is done to see if haveged is on the machine. If not, instructions for installing it are provided.

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.

Removed in this version

- Technical support for Windows Active Directory in mixed mode ended with v8.4. For version 8.5, full functionality has been removed. The **Windows Active Directory (Mixed Mode)** option has been removed from the **General > Settings > Directory Services** page of Forcepoint Security Manager.
  - **Active Directory (Native Mode)** is now the default selection on the **Directory Services** page.

  See Product Support Life Cycle for additional information about planned support of existing products.
- The **Advanced Detection** option has been removed from the **Settings > Scanning > Scanning Options** page of Forcepoint Security Manager. Other analytic features will take the place of this option. (APWEB-10118, APWEB-9390)

  Corresponding elements of the **Scanning Data Files** list on the **Monitor > My Proxy > Summary** page of Content Gateway Manager have also bee removed. (APWEB-9390)

Third-party platform and product support

All components

This version adds support for:

- Microsoft Windows Active Directory 2016
- Microsoft SQL Server 2017
- Microsoft SQL Server 2016 Express SP1 (replaces Microsoft SQL Server 2008 R2 Express SP2)
- Red Hat Enterprise Linux 6.9, 7.3, and 7.4

This version ends support for:

- Red Hat Enterprise Linux 6.5, 6.6, 6.7, 7.0, and 7.1.

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 6.8, 6.9, 7.2, 7.3, and 7.4 (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
  ```

- V-Series appliances

  Important

  Customers currently using Red Hat Enterprise Linux 6.7 or earlier will need to upgrade their operating system prior to upgrading the product.

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 |28-Feb-2018

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