v8.5.3 Release Notes for Web Protection Solutions

Release Notes | Forcepoint Web Security and Forcepoint URL Filtering |30-Nov-2018

Use the Release Notes to find information about what's new and improved for Forcepoint Web Security and Forcepoint URL Filtering in version 8.5.3.

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 (v8.2.x or 8.3.x) or Forcepoint Web Security (8.4.x or 8.5), 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), 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 v8.5.3 are supported from v8.2, v8.3, v8.4, and v8.5. 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 8.4.x*	Upgrade to 8.5.x	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				
v8.5.0	Upgrade to 8.5.3				
*** 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 6.8 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 |30-Nov-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 8.5.3.

In addition, numerous code changes were made to better handle directory service credentials as they are passed between Web Security components.

Protected cloud apps enhancements (Web Security only)

Integration of Forcepoint Web Security with Forcepoint CASB has been enhanced.

- A link to the CASB SSL certificate needed for the CASB integration has been added to the **Settings** > **CASB Configuration** > **Protected Cloud Apps** page of Security Manager.

  Use the new **Download Forcepoint CASB Certificate** link to copy the certificate to the local downloads folder. From there, deploy it to client machines as well as each Content Gateway server machine.
- A new message displays on the **Settings** > **CASB Configuration** > **Protected Cloud Apps** page of Security Manager if the initial connection to the CASB server subsequently fails. The message is also intended to remind users that any edits made to the list of cloud applications would not be saved if the connection is lost.

Report Center enhancements

The Report Center tools now include new functionality and features.

Report Catalog enhancements

- Reports can now be shared with other administrators.

  From the My Reports folder:

  - Click the down arrow next to a report or folder name and select **Sharing** from the menu.

    or

  - Check the box next to one or more reports or folders and click **Share**.
  - From the Sharing pane, select:
    - **Not shared** to remove sharing from the selection.
    - **View only** to allows others to run but not make changes to the report.
    - **Allow editing** to allow others to both run and makes changes to the report.

  Shared reports are added to a **Shared by Others** folder. Each report or folder is marked with a sharing icon. Hover over the icon to view the assigned sharing permissions. Icons that include a lock indicate editing is not allowed.

  When a folder is shared, the reports in the folder are added to a new folder which is listed under **Shared by Others** and named using the name of the user who shared the folder.

Report Builder and Transaction Viewer enhancements

- Accessing Transaction Viewer by clicking an entry in a bandwidth related metrics column in the Report Builder now adds the corresponding metric column to the Transaction Viewer report.
- Two new tabs have been added to the **Detail view** of Transaction Viewer and will appear when the log record contains the corresponding details.
  - **Threat Details** has been added to provide the details about any threat that may be associated with the request.

    By default, 30 days of Threat Data is maintained in the Log Database. This value can be configured on the **Web > Settings > Reporting > Dashboard** page of Forcepoint Security Manager.
  - **Forensics Data** has been added and includes information about files associated with threat activity and attempts to access them.

    When available, forensics data is included in the output when one of the export options is used.

    Forensic data is available only if **Store forensic data about Threat incidents for further investigation** is selected on the **Web > Settings > Reporting > Dashboard** page of Forcepoint Security Manager. The type of data collected and length of time to store the data is also configured on that page.

  Access to these tabs is based on the delegated administrator role and the Reporting Permissions assigned to it.

Report Center Scheduler enhancements

- New columns have been added to the Scheduler page.
  - A new **State** column has been added to indicate whether a job is **Enabled** (runs according to the defined recurrence pattern) or **Disabled** (inactive and does not run).
  - The new **History** column provides a link to the new **Job History** page described below.
  - A new **Next Scheduled** column replaces the Started column and shows the date and time for the next run of the job. If the job is not rescheduled to run again, the column is empty.

    As a result of the addition of this option, a change to the **Status** values was made. If a job has been rescheduled, that will be reflected in the reported job status.
    - Complete is now **Completed (Rescheduled)** to indicate that the previous job run completed and the job has been rescheduled.
    - Failed is now **Failed (Rescheduled)** to indicate that the previous job run failed but the job has been rescheduled.

    Completed or **Failed** continue to be used for jobs that are not rescheduled.
- New options have been added to **Run Now**, **Enable**, or **Disable** a job.

  Select a job and open the **More** drop-down menu to run the job now, enable a disabled job, or disable a job to discontinue running it but keep it in the job list.

- Jobs now include a configurable **Start Time** that is included on the Scheduling Options page when adding or editing a job.

  Note that if multiple jobs are scheduled to run at the same time, one or more may fail. In this case, use the **Run Now** option to run the failed job and consider changing the **Start Time** for that job.
- An option as been added to the Scheduler page that will allow a Super Administrators to view only their own jobs.

  By default, the **View only my jobs** toggle is off when a Super Administrator opens the page and all jobs are listed. Toggle the switch to On to display jobs owned by the Super Administrator.
- Access to Report Center Scheduler is now available from the Report Builder and the Transaction Viewer.
  - On the Report Builder page or in Transaction Viewer, create and save a new report, then click the Schedule icon. The Report Center Scheduler > Add Job > Report Selections window opens and the new report is automatically included in the Scheduled Reports list.
  - From the Report Catalog, select an existing report to drill down to either the Report Builder or Transaction Viewer. Click Schedule to navigate to the Report Selections window and continue to add a new job.

  The availability of the **Schedule** icon is based on the delegated administrator permissions to use the Report Center Scheduler. The **Schedule reports** option must be selected in order to navigate to the Report Center Scheduler.
- The Scheduler page now sorts alphabetically by job name by default.

  Select a different heading to change the sort. Select the heading a second time to reverse the sort. Note that sorting is not available on the Recurrence column.
- New paging options have been added.

  Use the paging options at the top of the page to navigate through the list of jobs.
- The email sent by Scheduler has been enhanced.
  - The details provided in the email reflect both the reports that ran successfully and those that failed to generate.
  - Smaller reports that ran successfully are attached to the email. If the total size of all report files exceeds 5MB, a link to the reports is provided.

    Reports that exceed a predefined maximum number of rows (by default, 100,000 for PDF files, or 300,000 for CSV), are attached but truncated.

    If an email is sent with files attached, but the email fails, it is assumed that the mail server was not able to handle the attachments and a second email is sent that includes links to the reports.
  - The customizable email text and the content of the emails has changed to better reflect the results of the job.
  - If a job fails to run, an email notification is sent to the address defined in the new **Specify the recipients of failure notification** field on the Recipients page when adding or editing a job.

    At least one entry is required in this field.

- If report generation fails for one report assigned to a job, the job continues to generate the remaining reports.

  If at least one report fails, but others are successful, the job status is set to **Failed**. A failure email is also sent, but includes the reports (or links to the reports) that completed successfully.
- Deleting a job will not also delete the reports that were generated by that job. The reports remain available for review. See *A Review Reports feature has been added.* below.
- Column width on the Scheduler page can now be changed.

Job History is now available.

- On the **Scheduler** page, for a specific job, click the **Details** link in the new History column to open a page that includes:
  - **Report Name** -- the title of each report created each time the job ran.
  - **Start Date** -- the date and time the report started running.
  - **End Date** -- the date and time the report was complete.
  - **Status** -- indicates whether the report succeeded or failed.
  - **Message** -- provides relevant information about the job.
- Change the column width to make the page easier to view.
- When a job is deleted, the history is deleted as well.
- Use the **Refresh** button to update the history info with more recent job information.
- Use the paging options to navigate to other history pages.
- By default, the records are ordered by Start Date, with the most recent activity listed first.

  Select any column heading to change the sort to that column. Select a column again to reverse the sort.
- Use the **Back** button provided on the details page to return to the Scheduler page.

  Breadcrumbs at the top of the page are also available to use to navigate back to the Scheduler page.

A Review Reports feature has been added.

When a scheduled job runs, the reports it generates are forwarded to the report recipients in an email and are now also stored in a folder on the disk. A record is also created in the Log Database.

- Click **Review Reports** on the Scheduler page to open the new Review Reports window and view a list of all of the reports that were created each time a scheduled job ran successfully. Details include:
  - **Report Name** - the name of the generated report. This is typically the name of the report that is displayed in the Report Catalog.
  - **Job Name** -- the name of the job that generated the report.

- **Creation Date** -- the date the report was generated.
- **Requestor** -- the name of the administrator who scheduled the report.
- **Purge Date** -- the date the report will be deleted from the disk.

  The purge date is calculated based on the length of time configured on **Settings > Reporting > Preferences**.
- **File Size** -- the size of the report file stored on the disk.

  File size is converted and reported in an appropriate measurement (bytes, KB, MB, etc.). Each reported value includes two decimal places.

The list provided contains the reports created by scheduled jobs owned by the user accessing the page. This is also true for the Super Administrator. Unlike the list of scheduled jobs, the Review Reports page will include only the reports generated by the jobs owned by "admin".

- To view any report, click the report name.

  The report is downloaded to the local downloads folder. Open or save the file to view it.
- Use the paging options to navigate to other report pages.
- Change the column width to make the page easier to view.
- Limit the list to those reports that will be deleted soon by enabling **Show only reports due to be purged**.

  Reports are stored on the management server machine for a length of time configured on the **Setting > Reporting > Preferences** page of Forcepoint Security Manager. Use the **Store report for** drop-down list to indicate how long reports are stored (5 days, by default). Also, define how long a warning is displayed on the Review Reports page before a report is deleted (3 days, by default).

  To support this feature, the **Setting > Reporting > Preferences** page has been edited to reflect support of these options for both Presentation Reports and Report Center Reports.
- If a recently created report does not display, click **Refresh** to update the page.

  Configured sorts are maintained when using **Refresh**.
- The page sorts by **Creation Date**, by default, with the most recent report listed first.

  Select any column heading to change the sort to that column. Select a column again to reverse the sort.
- Reports are saved to the C:\Program Files (x86)\Websense\Web Security\ReportingOutput\ReportCenterOutput folder of the Management Server. A record is also added to the Log Database for each report.

  Report files are saved as zip files in order to use the least amount of disk space. Reports that fail to generate due to insufficient disk space report "Low disk space" in the message column of the job history page.

  If a report record fails to be added to the Log Database, the file is not saved to disk.

- Delete a report by selecting it and clicking **Delete**. The report is removed from the management server and from the Log Database.

  Reports that are stored for the length of time configured on the **Setting > Reporting > Preferences** page are then automatically deleted from the disk and the corresponding record is deleted from the Log Database.

  If the job associated with a report is deleted, the report remains on the disk.
- Click **Back** or use the breadcrumb at the top of the page to return to the Scheduler page.

Delegated administration with Report Center

To support delegated administration with the new Report Center features, the Reporting Permissions section of the **Delegated Administration > Add Role > Edit Role** page of Security Manager had changed.

- The **Access the Threats dashboard** option has been moved and renamed to **Access Threat data (Threats dashboard + Report Center)**.
- Similarly, **Access forensics data in the Threats dashboard** has been renamed to **Access forensics data**.

  Use the new options to allow administrators to view the data in the two new tabs for the Detail view of the Transaction Viewer as well as to view the same data in the Threats dashboard.
- **View user names and hostnames in reports** has been added under **Access the Report Center**. This option allows administrators to view user information when creating or viewing reports. When unchecked, an internally assigned user identification number displays wherever user would appear in a report. A hash of the hostname appears in place of the true hostname in Transaction Viewer details.

  By default, the option is unchecked. For upgrades to 8.5.3:

  - The option will be on for upgrades from v8.5.

    The Schedule Reports option will continue to be enabled if it was enabled in the v8.5 settings.
  - When upgrading from any other version, the value of the option is determined by the current setting for **View user names in investigative reports**. or **Access presentation reports.** The new option will be enabled for all delegated administrators who previously had permission to view user names in investigative reports or to access presentation reports.

  If the option is not enabled for a delegated administrator:

  - A message displays when the administrator opens Report Builder or Transaction Viewer as a reminder that a user ID and a hash of the hostname will be used in all reports.

    The same message appears in emails sent for scheduled reports.
  - The User attribute cannot be used as a Filter in any report.
  - In Report Builder and in Transaction Viewer, a user ID displays in place of a user name in any report, including exported reports, that includes a User column.

This is also true of any Report Builder bar, trend, or pie chart generated for the same data.

- When viewing a Report Builder report that was created with User in the **Grouping** field, the options to **Show Only**, **Filter Out**, or **View Transactions** are disabled.
- The details provided for a selected transaction on the Transaction Viewer displays a user ID in the User Name field and the hash of the Hostname.

  The same is true if those details are exported.
- Reports containing user information that were created prior to the option being disabled can no longer be viewed, edited, or run. The only Report Catalog option available to the delegated administrator after permissions are removed is to delete the report.

  However, scheduled jobs that were created prior to the option being disabled continue to be available for viewing, editing, and running. Scheduled jobs created when the option is disabled cannot include reports that include user information.
- Shared reports that contain user information will not be available for viewing or use.

For delegated administrators assigned to multiple roles, the most restrictive role is used. Viewing the User and Hostname is denied if the option is unchecked for any of the assigned roles.

When a change is made to the setting, a message displays reminding the Super Administrator of the impact of the change.

General enhancements

The Health Alert associated with low disk space when generating reports has been updated to include reports generated from the Report Center as well as presentation reports.

Content Gateway enhancements

Enhancements have been made to Content Gateway.

- The certificate verification engine (CVE) has been enhanced.
  - Alternate paths have been added for certification verification.
  - Additional fields are now copied from the original certificates to dynamic certificates.
- A new variable has been added that allows for tunneling of TLSv1.3-only connections, which are those SSL connections that offer only TLSv1.3 in their “Client Hello”.

  Enable this feature by adding the following to records.config (located in /opt/WCG/config, by default):

  ```
  CONFIG proxy.config.ssl_decryption.tunnel_TLSv13 INT 1
  ```

The current decryption process is applied to SSL connections whose "Client Hello" contains TLSv1.3 with other protocols supported by the WCG (such as TLSv1.2).

- Content Gateway will no longer accept nor download SHA-1 intermediate certificates. SHA-1 certificates that were added by Content Gateway will be removed during an upgrade to v8.5.3. Note that SHA-1 certificates that were manually added will not be deleted.

  This feature is enabled using the following record.config variable:

  ```
  CONFIG proxy.config.ssl.cert.verify.denysha1cert INT 1
  ```

  With this setting, an error appears in Content Gateway Manager if an attempt is made to add a SHA-1 intermediate certificate.

  Edit records.config (located in /opt/WCG/config, by default) and change the value to 0 to disable the feature and continue to use SHA-1 intermediate certificates.

- A new feature has been added that can be used to change the way cookie caching works. Cookie caching allows a user to re-access the system without authentication until the cookie is no longer valid. When this new feature is enabled, cookies expire when the user ends a session.

  Navigate to **Configure > Security > Access Control > Global Authentication Options** in Content Gateway Manager, and find the new **Cookie Expiration** section. Select **Delete cookies upon logout** to enable this new feature.

  This feature is recommended in deployments where multiple users share a machine.

- A new feature has been added that will allow customers to provide custom dynamic certificate keys.

  In earlier versions, Content Gateway sends a pregenerated dynamic certificate, generated using a predefined key pair, to clients, based on the Root CA. This new feature allows customers to specify their own base64-encoded key pair that is used, in place of the predefined pair, to generate the dynamic certificate.

  A new **Custom Certificate Key** option has been added to **Configure > SSL** in the Content Gateway Manager. Select that option to:

  - Import Custom Certificate Key.
    - Use **Choose File** to browse and locate the key to be imported.
    - Enter a **Passphrase** and then **Confirm Passphrase**.
    - Click **Import Custom Certificate Key**.
  - Create Custom Certificate Key.
    - Enter the **Key length**.
    - Enter a **Passphrase** and then **Confirm Passphrase**.
    - Click **Generate and Deploy Custom Certificate Key**.
  - Back up Custom Certificate Key.

    Click **Save Custom Certificate Key** to create a backup of the key that was imported or created.

The key format must be PKCS#8. See this article for information about converting to a PKCS#8 key type.

- When credential caching is done using IP addresses, Content Gateway now performs lookups for sites that have been added to the Authentication Bypass rules. If the user is found, the appropriate user-based policy is applied.

Other reporting enhancements

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

- In the Advanced File Analysis report:
  - Customized column selections are now stored and no longer reset each time you navigate away from the page. The columns will reset to the default selections with each log on to the Forcepoint Security Manager.
  - The number of files associated with each threat level no longer resets to zero if the threat level is not included in the report.
- Reports viewable from the **Cloud Apps** tab of **Main > Reporting > Applications** have been updated to display the user information in format used by Investigative Reports.

  In addition, special characters can now be included in a user name when using the Search feature provided by the Cloud App reports.

General enhancements

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

- The **Domain Discovery** section of the **Settings > General > User Identification > DC Agent** page of Security Manager has been changed to remove the component selections for domain discovery. Domain discovery will always be done by DC Agent.
- Master Database enhancements have been made, including additional URL entries. These enhancements have greatly increased the size of the database files that are downloaded daily (by default).

  When upgrading to v8.5.3, the new database files will replace the existing files. Customers should be aware of the size difference and, prior to upgrading, confirm there is at least 6 GB of additional free space available on the Filtering Service machine.

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 7.5
- Microsoft SQL Server 2017 Express

This version ends support for:

- Red Hat Enterprise Linux 6.8 and 7.2
- Microsoft Windows Server 2008 R2
- Microsoft SQL Server 2016 SP1 Express
- Microsoft SQL Server 2008 (all versions)
- Active Directory 2008

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 |30-Nov-2018

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