v8.2.0 Release Notes for Web Protection Solutions

Release Notes | TRITON AP-WEB and Web Filter & Security |27-Apr-2016

Use the Release Notes to find information about what's new and improved for TRITON® AP-WEB and Web Filter & Security in version 8.2.0.

- *New in Web Protection Solutions*, page 2
- *Resolved and known issues*, page 14

For information about endpoint client software, please refer to the Release Notes for TRITON AP-ENDPOINT.

Note

The Content Gateway component is not included in Web Filter & Security deployments. Content Gateway information applies only to TRITON AP-WEB.

Refer to the following when installing or upgrading to v8.2.

- Installing TRITON AP-WEB
- Installing Web Filter & Security
- When upgrading Web Security Gateway/Anywhere (v7.8.4) or TRITON AP-WEB (v8.0.x or v8.1.x), see Upgrade Instructions for TRITON AP-WEB
- When upgrading Web Filter *or* Web Security (v7.8.4) or Web Filter & Security (v8.0.x and v8.1.x), see Upgrade Instructions for Web Filter & Security
- 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 8.0

New in Web Protection Solutions

Release Notes | TRITON AP-WEB and Web Filter & Security | 27-Apr-2016

- *TRITON APX*
- *Security enhancements*
- *Look and feel enhancements*
- *Threat Protection integration*
- *Advanced File Analysis reporting*
- *Single Sign-on support for Microsoft Active Directory Federation Services (AD FS) (hybrid)*
- *Policy exceptions based on HTTP referer header*
- *Threats dashboard includes hybrid log data*
- *Advanced user search in Toolbox options*
- *Browser support*
- *Logon application support*
- *Third-party platform and product support*

The TRITON Settings Help, TRITON AP-WEB Administrator Help, and Content Gateway Help are available in Japanese as well as English for 8.2.x. The language selection for Help for modules of TRITON Manager (including TRITON AP-WEB) can be changed on the **TRITON Settings** > **My Account** page. The language selection for Content Gateway Help can be changed on the **Configure** > **My Proxy** > **UI Setup** > **General** page in the Content Gateway manager.

TRITON APX

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

Original Name	New Name
Web Filter	Web Filter & Security
Web Security	Web Filter & Security
TRITON Web Security Gateway	TRITON AP-WEB
TRITON Web Security Gateway Anywhere	TRITON AP-WEB with: ● Web Hybrid Module ● Web DLP Module ● Web Sandbox Module (if purchased)

Security enhancements

Research to assess potential vulnerabilities or security issues has continued. Miscellaneous security improvements have been made in version 8.2.0, including an upgrade to OpenSSL version 1.0.1q.

Look and feel enhancements

To support the transition from Raytheon | Websense to Forcepoint LLC, TRITON Manager has a new look and feel. The colors and logos, as well as the logon screen and the toolbar, have been updated to reflect the Forcepoint brand.

In addition, if you are using the default block and notification pages, end users will see that the Websense logo has been replaced by the Forcepoint logo. If you have previously changed the default logo or customized your notification pages, however, your changes remain in effect and end users will not see any change.

These changes do not affect product functionality.

Over time, you may notice the branding extended to other areas, such as the Help system, as well as to external content, such as the Knowledge Base.

✓ **Note**

When you connect to any TRITON management console (TRITON Manager, Appliance Manager, Content Gateway Manager), you are presented with a self-signed certificate. The certificate names Websense, Inc., as the Organization (O). This will change to Forcepoint LLC in a future release.

Because browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch a TRITON management console from a new browser. To avoid seeing this error, install or permanently accept the certificate in the browser. After the security certificate is accepted, the manager logon page is displayed.

Threat Protection integration

A second option for file analysis is available on the **Settings** > **Scanning** > **Scanning Options** page of the TRITON Manager. Users who have purchased Threat Protection

Appliance can now integrate it with their TRITON AP-WEB deployment and use it for advanced file analysis.

Note

Threat Protection is a new option that provides analysis of files posing potential threats to your network. Contact your Forcepoint Sales professional for more details.

1. Navigate to the **Settings** > **Scanning** > **Scanning Options** page and locate the Advanced File Analysis section.
2. Check the box next to **Enable Advanced File Analysis**.
3. Select **Threat Protection** as the **File analysis platform**.

   By default, images and txt files are not sent to Threat Protection.
4. Enter the IP address of the Threat Protection Controller (prod1 interface) in the **Controller IP address** entry field.
5. Click **Check Status** to confirm that Threat Protection is installed at that IP address.

Alerts are the mechanism used to send information about files found to be malicious by advanced file analysis. To configure alerts for Advanced File Analysis and receive either an email or SNMP alert when analysis determines a file is malicious:

1. On the **Settings** > **Alerts** > **Enable Alerts** page of the TRITON Manager,
   a. Mark **Enable email alerts** and configure the email settings to send advanced file analysis alerts via email.
   b. Mark **Enable SNMP alerts** and provide information about your SNMP Trap system to deliver the advanced file analysis messages using SNMP.
   c. Click **OK** and then **Save and Deploy** to save your changes.
2. Navigate to **Settings** > **Alerts** > **Suspicious Activity** and locate the Advanced File Analysis section.
3. Check the box under **Email** to enable email alerts and under **SNMP** to enable SNMP alerts from advanced file analysis.
4. Click **OK,** then **Save and Deploy**.

Note

Usage Monitor must be installed as part of the TRITON AP-WEB deployment to support Advanced File Analysis alerts.

The email alert produced when a file is analyzed and found to be malicious includes a link to a File Analysis report or to the Threat Protection Appliance and a detailed report. If Threat Protection was installed using a hostname, the link will work only if the hostname is resolvable on the network.

Advanced File Analysis reporting

Advanced File Analysis report

A new **Reporting** > **Advanced File Analysis** option is available when Advanced File Analysis is enabled on the **Settings** > **Scanning** > **Scanning Options** page. The option opens a report that provides specific information about the results of advanced file analysis. The report is designed to provide visibility into suspicious files accessed through your network and sent for advanced file analysis to either the File Sandbox or to Threat Protection.

Use the options above the table to filter the data that is displayed.

- The **Time period** for the report.
  - Select Today, 2 days, 7 days (the default), 14 days, 30 days, 60 days, or 90 days from the drop down.

    If you are using Microsoft SQL Express, the maximum time period is 30 days.
  - The **Total number of incidents** reported for that time period is provided.
- The threat levels to be reported. Check the box next to:
  - **Malicious** to include files that analysis has found to be malicious.
  - **Suspicious** to include files found to have suspicious characteristics.
  - **No threat detected** to report on files in which analysis did not find any malicious or suspicious characteristics.

  The number of files included in the table is provided for each threat level.

The top (up to 200) results that match your filter are displayed in a table. By default, the following columns are included:

- **Threat Level**: an assessment of the level of threat (malicious, suspicious, or none) associated with a file.

  Click a link in this column to:
  - (if the File Sandbox is doing the analysis) open a File Sandbox Analysis report detailing the information provided in that row.
  - (if Threat Protection is doing the analysis) access the Threat Protection machine and view a detailed Threat Protection report. You may first be prompted for logon credentials.

  ✓ **Note**

  If Threat Protection was installed using a hostname, the link will work only if the hostname is resolvable on the network.
- **Incident time**: the date and time the file was sent for analysis.
- **User**: the user name (or IP address) associated with the activity that prompted the file analysis.

- **Source**: the IP address of the client machine in your network that sent or received the file.

  Click an IP address to open an Investigative Report that will provide more details for the browsing being done by that source IP on the day the file was analyzed.
- **Destination**: the IP address of the recipient of the HTTP request.
- **URL**: the URL from which the file is being downloaded or to which the file is being posted.

  In some cases the URL may be truncated. Hover over the entry to view the complete URL.
- **Analyzed by:** the IP address of the Threat Protection cluster or the location of the File Sandbox data center.

Use the **Customize** option to add or remove columns from the table. In the window provided, check the box next to the column headings you want to include. Uncheck the box next to any column heading you want to remove.

- **Platform**: The platform that provided the file analysis (Threat Protection or File Sandbox).
- **Severity**: the level of severity of the threat, on a scale of 1 to 10.
- **Result Type**: indicates whether there was a **Hash match** or this was considered **New analysis**.

  Hash match means that the file hash (not the file) was actually sent for analysis and was found in the records of the analysis platform. The file is recognized and the Threat Level is known.

  New analysis means we have don’t have a record of having seen the file before so the entire file was sent for analysis. Analysis shows whether or not the file contains a threat.
- **Protocol**: the protocol used to transfer the file.
- **File Name**: the name of the file sent for analysis.
- **File Hash**: an SHA1 hash of the file sent for analysis.
- **File Size (KB)**: the total file size, in kilobytes.
- **File Type**: the type of file sent for analysis. Types include PDF, Image, Executable, Document, and Web Page as well as others.
- **Content Gateway**: the IP address of the Content Gateway machine that sent the file for analysis

Note that customized column selections are not stored. The columns reset each time you exit and return to the page.

Note

URL hostnames and file names that contain foreign characters may not display properly in the report.

Use the other links and options to:

- Change the sort order. (Default sort is by Threat Type).

  Use the arrows beside a column heading to change the report's sort order.

- Export the contents of the report to a CSV file.

  Click **Export to CSV** to add the data to a file named excel.csv, by default. If the displayed data has been filtered, the same filter is used. All columns are included in the exported data, even if not previously selected for the report.

  A maximum of 10,000 rows can be included in the exported data. Any data that exceeds the limit will not be included in the spreadsheet.

- Navigate between report pages.

  Use the paging options below the table to display other report pages.

- Refresh the data.

  Click **Refresh** to update the displayed data to include information that was added to the log database files since the report was initially displayed.

Delegated administrator access to the Advanced File Analysis report is determined by the **Access investigative reports** and **Report on all clients** options in the Reporting Permissions section of the **Delegated Administration** > **Edit Roles** page. The menu option Advanced File Analysis report will not be available to administrators whose role does not have both options selected.

Advanced File Analysis in the dashboard

When the Advanced File Analysis feature is enabled, the number of requests processed by Advanced File Analysis displays on the **Threats** tab of the **Status** > **Dashboard**. The number is generated based on the Time period displayed on the Advanced File Analysis report. Click the link to navigate directly to the **Reporting** > **Advanced File Analysis** page and view the details.

Note that this entry displays only for Super Administrators. It is not displayed to delegated administrators regardless of the options used to define their role.

Advanced File Analysis data

New temporary data files for the advanced file analysis data are created by Filtering Service and forwarded to Log Server. Log Server then handles the data files based on settings configured on the **Settings** > **Reporting** > **Log Server** page.

- The temporary data files are created based on the **Cache file creation rate** and **Maximum cache file size** options that also apply to log cache files.

- The data files are processed into the database using either **ODBC (Open Database Connectivity)** or **BCP (Bulk Copy Program),** depending on the **Log Record Creation** settings on the **Settings** > **Reporting** > **Log Server** page.

  The exception to this is the first file analysis temporary data file. That file is always processed using ODBC.

Note that Filtering Service does not forward the log records created for advanced file analysis data to Usage Monitor for inclusion in the Real-Time Monitor display nor to any SIEM integration.

To support the new data, new tables have been added to the Log Database and stored in the catalog database. The tables are populated by the **Advanced Malware Threat (AMT) ETL** job, that is also used to populate the tables used by the Threats dashboard.

Advanced file analysis data is maintained for 120 days.The database maintenance job purges data that is older than 120 days.

Single Sign-on support for Microsoft Active Directory Federation Services (AD FS) (hybrid)

TRITON AP-WEB customers who purchase the Hybrid module and for whom single sign-on is enabled, can now use Microsoft AD FS as a single sign-on identity provider.

To use this feature, open the **Settings** > **Hybrid Configuration** > **Hybrid User Identification** page of TRITON Manager and locate the Single Sign-on section.

1. Use the link provided to download and install the hybrid SSL certificate to ensure seamless authentication to HTTPS sites.

   If the certificate is not installed for single sign-on users, they receive a certificate error when they browse to an HTTPS site. If they then select the "Continue to this website (not recommended)" link, they must authenticate using NTLM identification or manual authentication, depending on the settings on the Hybrid User Identification page
2. Select **Use identity provider for single sign-on** to enable the single sign-on feature.
3. For **Identity provider**, select Active Directory Federation Services.
4. Once single sign-on is configured and the SSL certificate is installed on clients, copy the metadata URL from the identity provider’s metadata and enter it in the **Metadata URL** field.

See Integrating the hybrid service with a single sign-on identity provider in Administrator Help for more information.

Policy exceptions based on HTTP referer header

A new setting has been added to the Add Exceptions and Edit Exceptions pages that will allow for an exception that will permit access to URLs only when they are accessed from a specific site (a referer).

Use this new exception setting, for example, when access to YouTube is blocked for your employees, but you want to allow them to view a video that is linked on your company intranet.

✓ **Note**

If the security settings on the client's browsers have referer headers turned off, this feature will not work as expected. Access to the URL can be permitted only if the referer can be confirmed.

Open the **Policy Management** > **Exceptions** > **Add Exception** or **Edit Exception** page.

1. Enter the unique **Name** for the exception.
2. List the **URLs** that should be permitted by the exception.

   The URLs entered should be those that will be added as links and accessed from the specified site. If, however, there will be multiple links to the same hostname, enter the hostname in the **URLs** list. Leave the list blank to permit access to all links that are included on the specified site.

   In our example, enter the full URL to the video that is linked on your intranet site or enter www.youtube.com. If www.youtube.com is normally blocked by category, access is permitted only to videos specifically linked on your intranet site. Access to any video from www.youtube.com will not be permitted.

   ✓ **Note**

   When Network Agent is being used (Web Filter & Security standalone) or if SSL decryption is not enabled (TRITON AP-WEB), sites may not be permitted when accessed by an HTTPS referer site.

3. Check **Permit only when accessed via a specific site** and then, under **Approved Referer URLs,** enter the sites from which access should be granted.

   Note that access to the referer URLs must be permitted by an existing policy or exception. This exception does not imply permitted access to the referer URLs.

   Following our YouTube example, you would enter something like intranet.company.com.

   By default, a maximum of 10 referer URLs can be added. An eleventh entry will not be accepted. You need to add another referer exception for it.

   HTTP and HTTPS are the only protocols supported for referer URLs.
4. Specify which **Clients** are affected by this exception.
5. Note that **Permit** has been selected and cannot be changed.
6. Indicate when the exception **Expires** and determine the exception **State**.

7. Click **Advanced** to

   a. Change the default selection for **Block URLs that become a security risk, even if they are permitted by exception**. (Not recommended)

      When this option is checked, this setting also applies if a URL permitted by this exception is associated with a Security Risk category. The URL is filtered based on the active policy.

   b. Add regular expressions to define URLs that should be permitted by this exception.

8. Click **OK** to cache and save your changes and return to the Exceptions page. Changes are not implemented until you click **Save and Deploy**.

   If the **URLs** and **Regular expressions** lists are both empty when you click **OK**, a message will display asking if you intended to create an exception that will allow access to all links on the referer URL pages. Remembering that this may open a security hole, click **OK** on the message window to leave the URLs and Regular expressions blank. Click **Cancel** to close the window, return to the exception, and add URLs or regular expressions to it.

The Exceptions table will display the new referer exception with the usual permit icon but the mouse over will indicate that the exception is “Permitted by referer”. In addition, when a referer exception has been added:

- A new Referer column is added to the table.

  If a single approved referer URL was added to the exception, the URL is displayed. If multiple referer URLs were added, the number of URLs is displayed. Click the link to open a complete list of approved referer URLs.

- Text in the URLs column is specifically set for any referer exception that does not contain specific URLs or regular expressions.

When editing multiple exceptions at the same time, if one of the selected exceptions contains referer information and you change the exception type to Block, the change will not be applied to the referer exception. Referer exceptions can only be defined with a **Type** of Permit. Any other changes will be carried to all selected exceptions.

✓ **Note**

Exceptions defined with referer sites are not used by the Hybrid service to apply policies.

Threats dashboard includes hybrid log data

In previous releases of TRITON AP-DATA with the Web Hybrid module, the **Threats** tab of the **Status** > **Dashboard** page did not include hybrid reporting data.

An enhancement has been added so that hybrid reporting data is now included in the information provided on the Threats dashboard.

Advanced user search in Toolbox options

An advanced search feature has been added to the **Find User** option available with the Check Policy and Test Filtering Toolbox tools.

Now, on the Find User page:

1. Enter all or part of the user **Name**.
2. Use the **Search for** list to specify how to perform the search:
   - Select **Entries containing search string** to find all directory entries that contain the search term you entered.
   - Select **Exact search string only** to find only the directory entry that precisely matches the search term.
3. Expand the Directory Entries tree and browse to identify a search context.

   You must click a folder (DC, OU, or CN) in the tree to specify the context. This populates the field below the tree.
4. Click **Search**. Entries matching your search term are listed under **Search Results**.
5. Click a user name to select a user, or click **Search Again** to enter a new search term or context.

   To return to browsing the directory, click **Cancel Search**.
6. When the correct fully qualified user name appears in the User field, click **Go**.

If you are using the Test Filtering tool, make sure that a URL or IP appears in the **URL** field before you click **Go.**

Browser support

TRITON Manager and Content Gateway Manager are now supported on the following browsers:

- Microsoft Edge 15, 20, and 25
- Mozilla Firefox 43 and 44
- Google Chrome 48 and 49

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.

This release adds logon application support for:

- Microsoft Windows 10

The logon application also 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)

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:

- Mozilla Firefox 43 and 44
- Google Chrome 48 and 49
- Microsoft Edge 15, 20, and 25

Note that installing web protection components on Windows Server 2012 or 2012 R2 requires Microsoft .NET Framework v3.5. Install .NET Framework v3.5 before running the TRITON Unified Installer.

Content Gateway

This version is supported on:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.7: 2.6.32-573
  - Kernel version for 6.6: 2.6.32-504
- the corresponding CentOS version

In addition, Content Gateway is certified on the following 64-bit platforms:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.5: 2.6.32-431

    ✓ **Note**

    Product testing encountered a kernel bug in version 2.6.32-431 that can impact performance. However, Content Gateway features were tested on this version of the OS and passed the certification tests.

  - Kernel version for 6.4: 2.6.32-358
- V-Series appliances

Content Gateway is also supported on the corresponding CentOS versions, including update 4 (CentOS version numbers have a one-to-one correspondence with Red Hat Enterprise Linux version numbers)

Support for the following version has been dropped with this release:

- Red Hat Enterprise Linux 6 series, 64-bit, Basic Server
  - Kernel version for 6.3: 2.6.32-279

Important

Customers currently using Red Hat Enterprise Linux 6.3 will need to upgrade their operating system prior to upgrading the product.

Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

```
/bin/uname -r
```

Only kernels listed above are certified or supported.

"Best effort" support for the version of Red Hat Enterprise Linux and CentOS listed above is provided. Under "best effort" support, Technical Support makes a best effort to troubleshoot cases in standard fashion until the issue is deemed a Red Hat Enterprise Linux- or CentOS-specific issue, at which point you must contact Red Hat directly for assistance.

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 ABI.

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 | TRITON AP-WEB and Web Filter & Security | 27-Apr-2016

A list of resolved and known issues in this release is available to TRITON AP-WEB and Web Filter & Security customers.

If you are not currently logged in to your forcepoint.com account, clicking the link brings up a login prompt. Log in to view the list.