Web Protection Reporting FAQ

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

Use this collection to find answers to frequently asked questions about the reporting tools included with TRITON AP-WEB and Web Filter & Security:

If this collection does not include the information you need, considering the following related resources:

- Investigative Reporting Quick Start
- Presentation Reporting Quick Start
- Real-Time Monitor (v8.2) or (v8.3)
- Log Server Troubleshooting Guide
- Log Server Error Reference
- Manually Creating the Log Database

How does the logging process work?

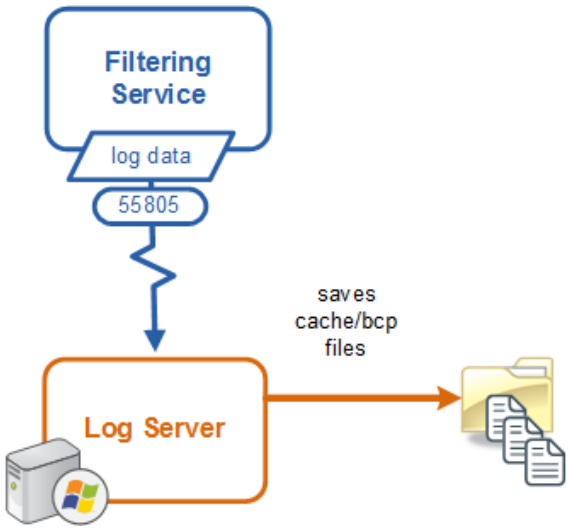
Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

When users browse the Web, their activity as recorded as log data:

1. Network Agent, Content Gateway, or a third-party integration forwards the Internet request to Filtering Service.
2. Filtering Service determines the appropriate response to the request.
3. By default, Filtering Service forwards a copy of the transaction for logging.
   - In v8.3, the transaction goes through Multiplexer to reach Log Server and (if configured) the integrated SIEM tool.
   - In v8.2, the transaction is sent directly to Log Server, unless you have enabled integration with a third-party SIEM tool. Then, the request is sent via Multiplexer to both Log Server and the SIEM tool.

See the *Security Information Event Management (SIEM)* paper (v8.3 or v8.2) for more information.

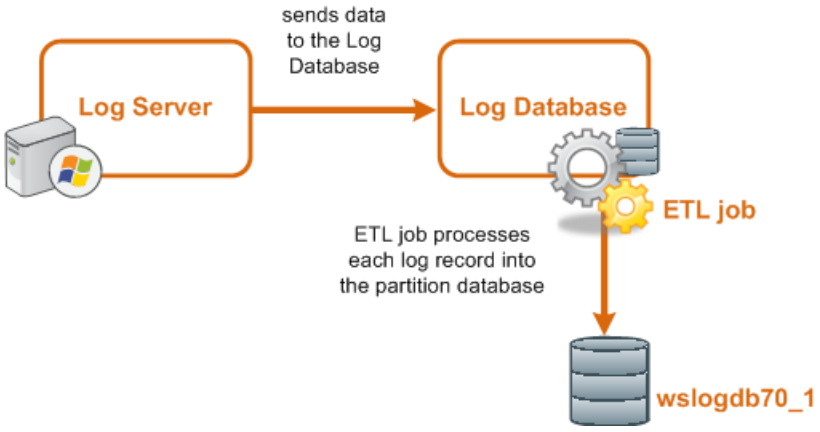
1. Log Server stores the data in temporary cache or BCP files on the local hard disk.



2. When the load of incoming data is not too heavy, Log Server performs preprocessing on the cached files and forwards them to the Log Database. Log Server can:
   - Process multiple, similar log records into a single record in a process called log record consolidation
   - Combine the elements that make up a web page (like advertisements, graphics, and text) into a single record using visits processing

   Information about Log Server preprocessing options can be found in the *Administering TRITON Databases* paper (v8.3 or v8.2).
3. The Log Database temporarily stores each log record in a table in the catalog database.

4. Database jobs move the data to various tables in the partition databases. For more information about how the jobs work, see *Database jobs* in Administrator Help (v8.3 or v8.2).



Data in the partition databases can be used in dashboard, investigative, and presentation reports (see *Use Reports to Evaluate Internet Activity*, v8.3 or v8.2).

ODBC and BCP

Log Server can forward log records to the Log Database using either of 2 formats:

- With **ODBC** (Open Database Connectivity), Log Server inserts records into the database individually. The data stored in Log Server cache files is moved directly to the database.
- With **BCP** (Bulk Copy Program), Log Server inserts the data in batches. To do this, Log Server starts by moving the data from the cache files into a new set of storage files. From there, the data is moved to the database.

Configure data insertion options in the Web module of the TRITON Manager on the **Settings > Reporting > Log Server** page.

For more information about ODBC and BCP, see *Specify how log records are processed into the database* (v8.3or v8.2).

Can I hide user-identifying information in reports?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

There are 2 ways to configure your software to omit user-identifying information from reports:

- If you sometimes need to generate reports that contain user information, but sometimes need to generate anonymous reports, use the **Anonymous** option at the top of the Investigative Reports page in the TRITON Manager to hide user names and, optionally, source IP addresses temporarily.
- If some administrators need access to reports that include user information, but other administrators should never see user information, use delegated administration roles to control reporting access. You can configure roles to grant access to investigative reports, but hide user names in reports.
- The most absolute method is to prevent the logging of user names and source IP addresses. In this case, no user-identifying information is recorded in the Log Database, making it impossible for investigative or presentation reports to include the information. See *Anonymous logging*, page 5, for instructions.

Anonymous investigative reports

To hide user names in investigative reports, click **Anonymous** at the top of the **Web > Main > Reporting > Investigative Reports** page in the TRITON Manager.

By default, this hides only user names, continuing to show source IP addresses in reports. To also hide source IP addresses:

1. On the TRITON management server machine, open the **wse.ini** file in a text editor. (By default, this file is located in the C:\Program Files (x86)\Websense\Web Security\webroot\Explorer directory.)
2. Add the following line under the **[explorer]** heading:

   ```
   encryptIP=1
   ```
3. Save and close the file.

Now, any time you click Anonymous, all user-identifying information is hidden.

When you click Anonymous, and then move to a different view of the data, such as detail view or outliers, user names remain hidden in the new report. However, to return to the summary view with the names hidden, you must use the links at the top of the report, not the breadcrumbs in the banner.

Anonymous logging

To prevent Filtering Service from including user names, source IP addresses, or hostnames (TRITON AP-WEB only) in the records that it forwards to Log Server:

1. Log on to the TRITON Manager and connect to the Web module.
2. Navigate to the **Settings** > **General** > **Logging** page.
3. Under Reporting Log Records, clear the check boxes next to one or all of the following options:
   - Log IP addresses
   - Log user names
   - Log hostnames
4. Click **OK** to cache your changes, then click **Save and Deploy**.

If you clear all 3 check boxes, no user-identifying information is saved in the Log Database, and no user-identifying information appears in reports.

How do I correct investigative report display or PDF export problems?

Internet Explorer cannot download ws_irtp.exe

When Internet Explorer is not configured to save encrypted pages to disk, attempts to display investigative reports or export them to PDF cause the following error message:

```
Internet Explorer cannot download ws_irpt.exe from <hostname
or IP address>
```

The message specifies the TRITON management server hostname or IP address.

To resolve the problem, first verify your Internet Explorer settings:

1. In Internet Explorer, open the **Tools** menu and select **Internet Options**.
2. Select the **Advanced** tab.
3. Under Settings, scroll down to the **Security** section and determine whether **Do not save encrypted pages to disk** is selected.
   - If the option is selected and you have the necessary permissions to change the setting on the local machine, deselect the option, then click **OK**.
   - If the option is selected and Internet Explorer options are restricted by a Group Policy Object, the administrator or group responsible for GPOs may have to make a change to allow investigative reports to display on specific machines.

     The Group Policy Object configuration is performed under **Computer Configuration** > **Administrative Templates** > **Windows Components** > **IE** > **Internet Control** > **Advanced** in the Group Policy Management tool.

Exporting a large detail report to PDF is very slow

When a very long investigative detail report is exported to PDF, the PDF may take a very long time to generate, or the report may time out before report generation is complete.

There are two solutions to this problem:

- Filter the information in the report so that it contains fewer rows.
- If the large detail report is absolutely needed, configure the **sendMulti** parameter in the investigative reports **wse.ini** file.

When this parameter is enabled, large detail reports are divided into small PDF files, each containing 10,000 rows. These files are zipped together for delivery to designated recipients.

To do this:

1. Navigate to **webroot\Explorer** directory on the TRITON management server (by default, C:\Program Files (x86)\Websense\Web Security\webroot\Explorer).
2. Use a text editor to open the **wse.ini** file.
3. Locate the **[explorer]** section of the file.
4. Change the value of the **sendMulti** parameter to **1**.

   If you later need to disable this option, return the parameter to its default value (0).
5. Save your changes and close the file.

Why don’t reports contain the data I expected?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

Unexpected results in reports may indicate that a report needs to be generated differently, or that a problem exists elsewhere in your deployment.

Reports contain incorrect or inconsistent totals

Because a category may be assigned to multiple risk classes, reports based on risk class assignments may include data for some categories multiple times. This may appear to inflate the report totals.

To avoid this issue, generate the same report at the category or user level to produce a total that contains no duplication.

There are more Uncategorized requests than expected

A new web protection installation includes a small, partial URL database that allows policy enforcement to begin as soon as the installation is complete. This limited database includes primarily URL information related to security sites. As a result, non-security URLs are unlikely to be found in the database and are therefore assigned to the “Miscellaneous - Uncategorized” category.

As soon as you enter a valid subscription key in the management console, Filtering Service begins to download the full Master Database. Once the download is complete, the partial database is no longer used and URLs are categorized properly. (Note that log records that are already in the database are not updated to assign correct categories.)

While Forcepoint researchers pride themselves on their ability to categorize websites, new or rarely accessed URLs may be assigned to the Miscellaneous - Uncategorized category for a time. To help limit the number of uncategorized sites, enable WebCatcher and allow it to forward uncategorized URLs to Forcepoint researchers for review. See *What is WebCatcher?* (v8.3 or v8.2) for more information.

Reports do not have any bandwidth information

Web Filter & Security may be integrated with a number of third-party firewall, proxy, and caching products. Some of these integrations do not send bandwidth information to Filtering Service when users request a URL. As a result, no bandwidth data is recorded in the Log Database, and reports cannot include bandwidth information.

If you are using an integration product that does not send bandwidth information to Filtering Service, install Network Agent and enable enhanced logging to log bandwidth data. Once Network Agent is configured to see outbound traffic, it can gather and send the bandwidth information that the integration doesn't include.

See the Network Agent Quick Start for information about installing and configuring Network Agent.

Is it possible to save presentation reports to a custom folder?

Scheduled presentation reports are automatically saved to disk on the TRITON management server machine. By default, they are saved in the **C:\Program Files (x86)\Websense\Web Security\ReportingOutput** directory.

Use the **Main > Reporting > Presentation Reports > Review Reports** page in the Web module of the TRITON Manager to view these saved reports from within the management console. Since the file names assigned to report files bear no relation to the report name, the Review Reports page is the best way to locate and print or view previously-generated scheduled reports.

If the default reporting output location does not work for your organization (for example, because the files are using significant disk space but you need to retain them), you can specify a custom location as follows:

1. On the TRITON management server machine, navigate to the **C:\ Program Files (x86)\Websense\Web Security\tomcat\conf** directory.
2. Open the **catalina.properties** file in a text editor.
3. Locate the line that begins with **reporting.output**.
4. Change the default entry to specify a different location.

Important

Use the file path format used in the default entry: two path separator characters ("\") are required between folder names.

A missing \ character will cause the scheduled report to fail.

5. Save your changes.

The next time a scheduled presentation report runs, the file is stored in the new location.

Note that changing **reporting.output** value means that older reports no longer appear on the Review Reports page. Only reports in the specified location are displayed.

What does it mean when the Log Database page shows partitions in red?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

You can configure the Log Database to automatically delete partitions when they pass a specified age. Manage this option on the **Settings > Reporting > Log Database** page in the Web module of the TRITON Manager, under **Database Maintenance**.

When this option is enabled and a partition exceeds the specified automatic deletion age, the partition is listed in red in the Available Partitions list to indicate that automatic deletion is pending. The age of the partition is based on its end date (not its start date).

The next time the maintenance job runs, the partition will be deleted.

If you don't want the partition to be deleted, you can either increase the age at which partitions are deleted, or disable the automatic deletion option.

How do I verify that WebCatcher is working?

WebCatcher collects URLs that are either unrecognized (not assigned to a category) or security related, and submits them to Forcepoint Security Labs for analysis.

- Uncategorized URLs are reviewed for assignment to a category.
- Security-related URLs are analyzed for what they can reveal about active Internet threats.

After WebCatcher data is analyzed, the results are used to update the Master Database.

WebCatcher writes the data it collects to an XML file that it sends to Forcepoint LLC via HTTP post. To understand what data is being collected and sent, you can opt to keep a copy of the file as follows:

1. Log on to the TRITON Manager and navigate to the **Web > Settings > General > Account** page.
2. Under WebCatcher, mark the **Save a copy of the data being sent to Forcepoint** check box.
3. Click **OK** and **Save and Deploy** to cache and save your changes.

The next time WebCatcher runs, a copy of its XML file or files is saved in the web protection **bin** directory (C:\Program Files)\Websense\Web Security\bin\, by default) on the Log Server machine.

The file name indicates whether it contains uncategorized URL information or security-related URL data, and includes the date and time that WebCatcher created the file.

In addition, a **webcatcher.log** file is created in the **Websense\Web Security\bin** directory on the Log Server machine. Review this file to verify that WebCatcher was able to send URL information, and to find information about any errors that might have occurred.

Can I review Log Server cache files?

Log Server creates temporary cache files (ODBC cache files or BCP files) to hold Internet activity data until it is forwarded to the Log Database. As each cache file is processed, it is deleted.

If you need to review cache files for troubleshooting, Log Server can be configured to move the files instead of deleting them:

1. Use the Windows Services tool to stop the **Websense Log Server** service.
2. Navigate to the web protection **bin** directory (C:\Program Files\Websense\Web Security\bin\, by default) on the Log Server machine.
3. Open the **logserver.ini** file in a text editor.
4. In the **[LogFile]** section, change the **MoveCacheFile** parameter to **TRUE**.

   ```
   MoveCacheFile = TRUE
   ```

5. Set the **MoveCacheFilePath** to a valid path. This path can be on the local machine or be a mapped drive, but the directory must already exist. For example:

   ```
   MoveCacheFilePath = H:\WebsenseLogs\Cache\
   ```

6. Save and close the file.
7. Use the Windows Services tool to start the **Websense Log Server** service.

The next time Log Server forwards cache file information to the Log Database, the temporary cache files are moved to the new location rather than deleted.

When you enable this option, it may require significant disk space. When you are finished troubleshooting your issue, repeat the above steps, but reset the value of **MoveCacheFile** to **FALSE**.

How do I archive Log Database partitions (or bring archived partitions back online)?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

Many organizations have older Log Database partitions that are no longer used (or rarely used) for reporting. The organization may want to preserve the data, but don't want it taking up space on the Microsoft SQL Server machine.

It is possible to archive database partitions, removing them from the SQL Server host. If it later becomes necessary to report on data in the archived partition, you can restore and re-enable the partition.

Archiving a Log Database partition

To archive older data, start by using the Microsoft SQL Server backup process, then take the partition offline and move it to a longer-term storage location.

1. Open SQL Server Management Studio (Start > All Programs > Microsoft SQL Server 2008 *or* 2012 > SQL Server Management Studio) and log on to the SQL Server instance that hosts your Log Database.
2. In the Object Explorer, under Databases, locate the partition you want to archive. By default, the name takes the format **wslogdb70_n**, where "n" is the partition number).
3. Right-click the partition and expand the **Tasks** menu, then select **Back Up**.
4. In the Back Up Database window, you can either accept the default backup **Destination**, or click **Add** to specify a new path for the backup file.
5. When you are finished, click **OK** to run the backup.
6. When a prompt indicates that the backup process is complete, click **OK**.
7. Right-click the partition in the Object Explorer again, then select **Take Offline**.
8. Close Microsoft SQL Server Management Studio.
9. Move the partition to your long-term storage location.

Reporting on an archived partition

To run reports on a partition that you have previously archived and taken offline, use the Microsoft SQL Server restore process, then enable the partition.

1. Open SQL Server Management Studio (Start > All Programs > Microsoft SQL Server 2008 *or* 2012 > SQL Server Management Studio) and log on to the SQL Server instance that hosts your Log Database.
2. Right-click the **Databases** node and select **Restore Database**.

3. On the General page, use the **From database** field to specify the location of the archived partition backup file.
4. Select the **Options** page, then verify that the **Restore As** column shows the correct location for the destination (restored) partition.
5. Click **OK** to restore the database.
6. When a prompt indicates that the restore process is complete, click **OK**.
7. Close Microsoft SQL Server Management Studio.
8. Log on to the TRITON Manager and navigate to the **Web > Settings > Reporting > Log Database** page.
9. Under Available Partitions, select the newly restored partition and click **Enable**.

   The partition is now available for use in reports.

When you are finished reporting on the historical data, you can take the partition offline and remove it from the SQL Server machine again.

What are application reports?

Application reports provide information about the web browser applications and operating system platforms in your network. With version 8.3, the use of the cloud applications is also provided. The browser and operating system information is gathered based on the **user agent string** associated with HTTP requests originating from users in your network. (A user agent string is an HTTP header that identifies the client software from which an Internet request is made.)

Application reports include:

- A combination of graphical charts and tables that provide a count of the browsers and platforms being used to originate Internet requests in your network.
- For v8.3, summary and detail reports that provide visibility into the use of cloud applications by users in your networks, and the potential risks associated with their use.
- A search feature that lets you investigate activity associated with any specified user agent string.

Access application reports from the **Main > Reporting > Applications** page in the Web module of the TRITON Manager.

Use application reports to:

- Locate potential vulnerabilities. For example:
  - Older browsers that may present a security vulnerability because they are no longer being patched.
  - Machines in your network that may be vulnerable when a zero-day exploit is discovered.
  - Cloud applications use that may put your network at risk. (version 8.3)
- Track adoption of new browsers or operating systems.
- Track the use of cloud applications. (version 8.3)

Use the User Agents search feature to:

- Identify machines in your network on which a specific application is running by searching for the user agent string associated with the application.
- Identify machines that may be at risk by searching for a user agent string associated with malware or suspicious activity.

Refer to “Application Reporting” in Administrator Help (v8.3 or v8.2) for more information about application reports and how to use them.

Why are v8.3 application reports missing data?

If the charts on the Client Apps and Operating Systems tabs on the **Web > Main > Reporting > Applications** page of the TRITON Manager show no data, or if some of the data you expect to see doesn't appear, check the sections below for more information.

No data appears on the Applications page

Application reports data is not available for deployments that are integrated with a third-party proxy, cache, firewall, or other device. The integration product does not send user agent strings to Filtering Service.

Some data is missing from the Applications pages

1. Traffic originating from unsupported browser applications or operating system platforms may not appear in application reports because the associated user agent strings are not recognized. In some cases, an unsupported browser or platform that is very closely related to a supported browser or platform may appear as if it were its supported cousin.

   Use the Search tab to view data related to browsers or platforms that do not appear on the Browser or Source Platform tabs.

2. The application browsing data that Log Server receives includes the user agent header, user name, and source IP address. If Log Server is configured to perform data reduction tasks (like recording visits, or consolidating records), the appropriate algorithms are applied and the data is forwarded to the Log Database.

   See "Adjust database sizing settings" in the Configuring Log Server section of Administrator Help for information about visits and consolidation.

3. If you have set the time period to **Today**, the trend charts do not show any data. This occurs because the smallest unit of time plotted on the trend chart is one day. Select a longer time period to populate the chart.

4. When new instances of Policy Server or Log Server are installed, or if a Policy Broker mode is changed, it may take as much as 10-15 minutes for new cloud application data to be forwarded to the Log Database.

Why are v8.2 application reports missing data?

Reporting FAQ | Web Protection Solutions | v8.2.x | 12-Aug-2016

If the charts on the Browser and Source Platform tabs on the **Web > Main > Reporting > Applications** page of the TRITON Manager show no data, or if some of the data you expect to see doesn't appear, check the sections below for more information.

No data appears on the Applications page

1. If you have just installed or upgraded to a version that includes application reports, the database job that populates the Browser and Source Platform tables and charts may not have run yet.

   As users connect to the Internet, new user agent strings appear on the Search tab, but are not parsed into recognized browsers or platforms until a nightly job runs.

   If your web solution is managing or monitoring traffic in your network, and raw strings are appearing on the Search tab, check the charts on the Browser and Source Platform pages again tomorrow.

   Note that once a string has been parsed and recognized, future requests originating from that browser or platform are added to application reports without the overnight delay.
2. Application reports data is not available for deployments that are integrated with a third-party proxy, cache, firewall, or other device. The integration product does not send user agent strings to Filtering Service.
3. In a distributed logging environment, remote Log Server instances cannot pass user agent string information to the central Log Server, so application reporting is not available.

Some data is missing from the Applications page

1. The data that appears on the Browser and Source Platform tabs of the Applications page is generated by a nightly database job. As users connect to the Internet, new user agent strings appear on the Search tab, but are not parsed into recognized browsers or platforms until that job runs.

   Once a string has been parsed and recognized, future requests originating from that browser or platform are added to application reports without the overnight delay.
2. Traffic originating from unsupported browsers or platforms may not appear in application reports because the associated user agent strings are not recognized. In some cases, an unsupported browser or platform that is very closely related to a supported browser or platform may appear as if it were its supported cousin.

Use the Search tab to view data related to browsers or platforms that do not appear on the Browser or Source Platform tabs.

3. Log Server receives browsing data that includes the user agent header, user name, and source IP address. All requests that share the identical user agent, user, and source IP address during a 60-second period are combined into a single record that provides the total number of requests and the volume of bandwidth associated with those requests. That record is then forwarded to the Log Database.

   Log Server holds in memory the user agent information that it combines to create the record sent to the database. If Log Server is restarted while user agent information is held in memory, that data is lost and cannot be recovered. It is expected that user agent strings for the same browser and source platform have been or will be generated so the basic discovery and reporting of browsers or platforms will not be impacted. The total requests and bandwidth, however, will be affected.

4. If you have set the time period to **Today** on the Browser or Source Platform page, the Browser Use Trend and Platform Use Trend charts do not show any data. This occurs because the smallest unit of time plotted on the trend chart is one day. Select a longer time period to populate the chart.

How do I export the Suspicious Event Summary?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

The Suspicious Event Summary on the Threats Dashboard lists information about threat-related events in your network. To export the event data to a CSV file, click the **Export To CSV** link above the summary table.

If your system has more than 100,000 threat-related event records, the management console cannot generate the CSV file directly. Instead, you are prompted to export the records directly from the Log Database.

To do this:

1. Connect to the Microsoft SQL Server machine that hosts the Log Database.
2. Open SQL Server Management Studio (Start > All Programs > Microsoft SQL Server 2008 *or* 2012 > SQL Server Management Studio) and log on to the SQL Server instance that hosts your Log Database.
3. In the Object Explorer, under Databases, select the catalog database (**wslogdb70**, by default).
4. Click **New Query** at the top of the window.
5. When the query window displays, enter:

   ```
   select * from amt_UI_log_details
   ```

6. Click **Execute.**

   A Results pane will display the data in a table format.

7. In the Results pane, right-click and select **Save Results As** to output the results to a file.

How do I configure services to use a trusted connection?

Reporting FAQ | Web Protection Solutions | v8.2.x, v8.3.x | 28-Oct-2016

If, while installing TRITON AP-WEB or Web Filter & Security, you chose to use a trusted connection to access the Log Database, you must configure the **Websense TRITON - Web Security**, **Websense Web Reporting Tools** services to log on using the trusted account specified during installation. These services are located on the TRITON management server.

For v8.3, **Websense Cloud App Service** also needs to be configured to log on using the trusted account. That service is located on the Log Server machine.

To configure each service to use the trusted account:

1. Go to the TRITON management server machine and open the Windows Services tool (**Start > Administrative Tools > Services** or **Server Manager > Tools > Services**).
2. In the list of services, right-click **Websense TRITON - Web Security** and select **Properties**.
3. In Properties dialog box, select the **Log On** tab.
4. Under **Log on as**, select **This account** and enter the domain\username and password of the trusted account.
5. Click **OK**.
6. Repeat this process (from Step 2) for the **Websense Web Reporting Tools** service.
7. For version 8.3, repeat the same process for the **Websense Cloud APP** service.