Websense Support Webinar: Questions and Answers

Leveraging Websense Explorer to
Optimize Internet Use and Minimize Security Threats

Websense Enterprise™ Version 6.3.x

Question: If I'm using Websense Explorer, how do I refresh the data?

Answer: The data is stored in the Log Database. The data is shown when you run a query against that database. So, refreshing Websense Explorer means refreshing your Web browser (usually with [F5]). As an alternative, you can simply rerun the query by re-selecting the report.

Question: Will reports available in Websense Reporter someday be available in Websense Explorer?

Answer: Most of the reports you are accustomed to using will be available in future versions. Websense Explorer currently works as a forensic, investigative tool, and many customers appreciate that format. Many also welcome trend analysis reporting. The architecture of Websense Reporting Tools is currently being reviewed; many investigative reports will be available in the future in an even richer reporting environment.

Question: I have changed the date selection in Websense Explorer and am now getting blank reports. Why is this?

Answer: Most likely there is no data for this period of time for the user/group or category selected, or perhaps even for that Risk class. So, as shown in the Webinar demonstrations, we advise you to start by viewing all dates, and then drill down to see if there is any data for that specific date.

Question: How much data can be displayed in the main page of Websense Explorer?

Answer: There is a limit to the amount of information that can be shown on the main page. However, when this limit is reached, additional pages are available for view from a page number link or **Next** button at the top of the page.

Question: Can I let my users view their own browsing data that is logged about them?

Answer: Yes. In fact, this is a legal requirement in some countries to allow users to see the data that is collected about them. To enable this, go to **Settings** on the right of your screen in the Web Reporting Tools Portal and select the **Self Reporting** check box. This allows users to log on to Websense Explorer and see reports for their own Web browsing only.

Question: How can I see all the date ranges available in the database? Is there a report for doing this?

Answer: Yes. At the top left of the main page in **Websense Explorer**, use the **Internet Use by:** drop-down box and select **Day**. Then, in the **View** drop-down box, choose **All**. This displays a report by day for all users and for all available dates in the database. The sequence of the rows is based on date order, with the oldest date on the first row.

Question: Browse Time does not show for most users. It does record for the system. Is that normal?

Answer: Check the IBT job among the Websense-related SQL Server Agent jobs. This is the job responsible for Internet Browse Time calculations. If this job is running as expected, then the issue is most likely a setup issue related to filtering and logging.

Question: Websense Explorer is installed on Disk 1 on my reporting server. The Microsoft SQL Server database is on Disk 2. When I select a database, the database is found. But when I try to create reports, it shows that the database is empty. I can see that the database is growing during the day. What can I do so that Websense Explorer finds the database for creating my reports?

Answer: Please check the ODBC settings for the connection to the Websense Log Database.

Question: My user activity detail returns this CGI error:

"The specified CGI application misbehaved by not returning a complete set of HTTP headers."

The headers it did return are: Cannot handle date (0, 0, 0, 23, 3, 2038) at timeline.pl line 167.

Answer: This is a known issue for which a Hotfix is available online. Please see Knowledge Base article 1935 at: www.websense.com/SupportPortal/KnowledgeBase/

Question: Is there a way to detect if my users are trying to use proxy sites to get around Websense software?

Answer: Yes. Check for the Proxy Avoidance category in your reports.

Question: If I change my report to show how many bytes have tried to go out, will it show only attempts?

Answer: It will show you whatever information your integration software passes to Websense software. So, the answer depends on which product you have integrated with Websense filtering.

Question: Why are some of my users showing as the localsystem user name in reports?

Answer: This is most likely because Workstation Polling is activated in the DC Agent configuration. Open Websense Manager, navigate to **Server > Settings > User Identification > DC Agent**, and disable Workstation Polling.

Question: Is archiving available through Websense Explorer?

Answer: You can export the data in individual reports to a variety of formats. If you are asking about Archiving the entire Log Database, then you want to use the **Database Administration** feature (last button on the **Websense Reporting Tools Portal**) to manage your database partitions. Then, use the standard Microsoft SQL Server tools to back up the Log Database as you would back up any other Microsoft SQL database.

Question: Is there a way to monitor only certain users/groups and not monitor others?

Answer: Yes, create a Role in Websense Manager. Assign selected users/groups to that Role. Then, assign an individual as administrator of this Role, and allow that individual to Report on these users/groups only.

Question: If a category is blocked, why is the report showing access?

Answer: The report shows you that a user tried to access the site. Depending on the software you have integrated with Websense filtering, we might be able to show you how many bytes have tried to go out.

Question: Some of my users show as IP addresses rather than user names. Why is this?

Answer: This could be caused by problems during the authentication of the users. Check the setup for your Directory Service, DC Agent, eDirectory Agent, Logon Agent, Radius Agent, and Websense User Service.

Question: Can I add custom categories to the Risk Classes?

Answer: Yes, you can add Custom Categories to the default categories selected for Risk Classes. Open Websense Manager and navigate to **Server > Settings > Risk Classes**.

Question: How do I produce a report in PDF format?

Answer: To see the data in PDF format, select the PDF Output icon.

Question: Apart from the differences in the user interface, what are the differences between the **Web Reporting Tools Portal** and Websense Reporter?

Answer: The **Web Reporting Tools Portal** is Web-based. This makes it available to users who are not on the Windows operating system. The functionality is also more robust.

Question: What is the password to access Websense Explorer?

Answer: It is the same password used at your site to connect to Websense Manager.

Question: Do you recommend blocking uncategorized sites (by default)?

Answer: No. Customers who have done this have not generally been pleased with the results. A significant percentage of uncategorized sites are legitimate business sites. We do categorize these, after we categorize new, malicious sites.

Question: If you click on the Visits icon, will it show the visited sites?

Answer: Yes. Take care not to do this from an unprotected machine, especially if you are checking potentially dangerous sites.

Question: Do you have instructions somewhere on a Web site showing how to use Websense Explorer?

Answer: Yes. Instructions for using Websense Explorer are provided in the product documentation available in your Websense\Documentation directory and are posted on the Support Portal at www.websense.com. Information is also available in the online help, accessed from the Help link in the top right corner of most Websense Explorer pages.

Question: If I'm in Websense Explorer, sometimes I want to see which Web site I just visited in another browser window. Typically I exit Websense Explorer, wait, then log back in to see the latest information. Is there a better way?

Answer: Yes. Although there is a small time lag for updating the tables, you do not need to log off. As the summary jobs run, click on the Websense Explorer link to rerun the query to retrieve the latest data. Then, drill down into a report selection to view the latest information.

Question: Does full URL logging represent a significant increase in database size or system draw?

Answer: By default, full URL logging is disabled. This helps to prevent the Log Database from growing too quickly, and reduces the number of system resources used on the machine where Log Server is installed.

Question: Is there a way to show user count for a particular category?

Answer: Not at this time. We can show all the users who requested a particular category at a particular point in time. Then, you need to manually count the number of users per page.

Question: I don't seem to have the User Activity Detail by Day view. Is this because I have version 6.3.1?

Answer: Version 6.3.1 of Websense Enterprise includes this feature. Drill down to a particular user on a particular date. Be sure to drill down far enough to reach the User Activity report. Alternatively, choose the User by Day/Month link in the toolbar.

Question: We are not seeing Bandwidth on our Websense Explorer reports.

Answer: Bandwidth usage data depends on the integrated software you set up to filter non-HTTP protocols. Some products do not pass Websense software the Sent/Received data that is used to build the bandwidth reports.

Question: How do I identify when a workstation actually gets infected with a keylogger or spyware? I know that the role of Websense software is to block malicious code before this can happen, but what does Websense software do if an infection actually takes place?

Answer: In Websense Manager, navigate to **Security Risk > Security PG Spyware > URL Hostname** to identify spyware hosts. From the URL Hostname, select **Source IP** to show which client is generating the traffic; that client is probably infected.

Question: Cisco Pix has an issue with providing bandwidth information. Does ASA have a similar issue?

Answer: Yes.

Question: I have A user showing 0.0.0.0 instead of user name. How do we track this user?

Answer: Use the **TestLogServer** tool from Websense to track down this user. Instructions for **TestLogServer** are available at kb.websense.com.

Question: Can you create a custom security class that contains a list of destination IP addresses? I then want to report on all users who are sending data to those IP's.

Answer: You would need to create a custom category in Websense Manager with those IP addresses specified. Then, you can run a report on that particular category to see user information.

Question: Is it possible to run a Websense Explorer Report for a range of IP addresses, such as an IP subnet used on one of our sites?

Answer: In the search text box you can enter a partial address and the subnet will be returned. Then, you will see data for that address range.

Question: Does this work on Windows NT 4.0?

Answer: No. Please review the Websense Deployment guide and Websense Reporting Administration guide for supported platforms.

Question: Are you ever considering exporting reports to Microsoft Access. No line limits, easier to group etc.

Answer: Not at this time. You can submit a Request For Enhancement to the following link: http://www.websense.com/global/en/ProductsServices/feedback/

Question: We have several IP addresses and URLs that are friendly: known intranet sites, or web applications within our wide area environment. How can we REMOVE these friendly sites from reporting? In other words, generating reports in PDF format is extremely slow. Can this be sped up?

Answer: If you are using Stand-Alone Edition, update the Network Agent settings by adding Internal IP Address ranges that are not to be reported on. Otherwise, you have to configure your firewall or Integration to not forward internal requests to Websense.

Question: Sometimes I drill down into a figure I see at a high-level, but when I drill down and click the horizontal bar to see the URLs, there is no data. Why is this?

Answer: Make sure you drill down by Day to make sure there is data for the date range you selected.

Question: Why are most of the reporter links red? And it takes a long time to generate a report?

Answer: When there are more than 100,000 rows for a particular selection, its link will be red to warn you that selecting this report at this point will take extra time. You should drill down further into the report to reduce the data set. When the number of rows is reasonable, the links will be in blue.

Question: How do I search on multiple user groups?

Answer: You can first select Group as your primary report choice from the upper left corner of the report main page, and then select the user groups you are interested in by ticking the box next to the group name. You can then drill down into the reports for those groups.

Question: How can I avoid logging Microsoft updates?

Answer: Create a custom category for these URLs. Then, in Websense Manager, navigate to **Server > Settings > Logging** and deselect this custom category, so that it is not logged.

Question: How can I tell the difference between something that someone was not supposed to access that just happened to come up on a Web page, and when the user was actually seeking it out?

Answer: The best way is to use the User Activity Detail report feature to see if this request for a bad site is an isolated incident, or if you can spot a trend of searches and/or similar bad sites prior to the request for the bad site in question.

Question: Is there any way to speed up the generation on Websense reports in PDF form?

Answer: Yes, by limiting the range of the data, either in term of number of users, or by date range or even categories. People tend to run reports on a very large population at one time, even when the report is only going to be used to check a small set of traffic/people/dates.

Question: If a user minimizes a window, then after 2 hours clicks on a link, does the time in Websense count it as 2 hours of browse time?

Answer: No. It will count as 2 sessions of 3 minutes each. So 6 minutes browse time in all. This value of 3 minutes is the default one; it can be changed in the Internet Browse Time settings.

Question: I have issues with the dates that are available. It seems every once in a while it stops logging or keeping the data. The date states the last available date is April 1. What would cause this?

Answer: The issue is upstream from the Web server. Log Server might have an issue pushing the data to the database for several possible reasons. Or the data is not processed once in the Incoming Buffer table, in which case you want to check the Websense ETL Job, and make sure that the Microsoft SQL Agent is properly configured and running.

Question: When is the data written to the database for viewing in Websense Explorer?

Answer: Log Server will push the data to the database every 1 minute or when its cache file reaches 1 MB, by default. This will vary if you are using BCP, and both values are changeable in the Log Server Configuration utility. Once in the database, the data has to be processed by a SQL job called ETL. This job runs every 10 seconds by default, and should thus publish the data in a viewable format only minutes after the traffic is handled by the Filtering Service.

Question: Are pop-ups and banners shown in these reports?

Answer: Yes, anything that generates a Web request will be analyzed, filtered and then logged by Websense. Now, the reports will not be able to tell you for how long a popup –or any Web browser window for the matter- has been left opened.

Question: Do we need enhanced logging turned on in order to see the User Activity Detail by Day report?

Answer: No, this is not necessary. Enhanced logging is aimed at ensuring no duplicate records are in the Log Database after a shutdown.

Question: How are risk classes accumulated by Websense?

Answer: Risk classes should be seen as groups of categories. You can change which categories are assigned to which risk class in the Websense Manager.

Question: Is there any way to add custom risk classes?

Answer: No, you cannot add any risk classes.

Question: What exactly is a "Hit"?

Answer: A Hit represents each image, text block, advertisement, and other files that are returned when a Web browser requests a URL. So, for one simple Web page you can potentially have lots of Hits.

Question: Will you please explain Hits versus Visits?

Answer: A Visit is expressed as a view of the Web site, whereas each returned image, text block, advertisement, and other file, etc., is regarded as a hit.

Question: What is the size of records for one user with full URL logging enabled (approximately)?

Answer: It depends on the size of the URLs, potentially 70 KB, but usually about a 1-2 KB.

Question: How and where do I turn on full URL logging?

Answer: To enable full URL logging: In Websense software versions 6.3 and later, use the Database Administration tool.

In versions 6.2 and earlier, use the Log Server Configuration utility.

Question: I was late, how did you get into the interface with the icon with the magnifying glass?

Answer: By selecting the User Activity by Day report once we drilled down to a users’ activity for a particular date.

Question: One of my concerns is finding how many employees exceed a certain browse-time threshold. For example, how many employees exceed browse-time of one-hour on a particular day. Is there a report that can show users whose browse time exceeds a stated amount of time? If not, can such a report be created and how difficult would it be?

Answer: This sounds more like a trend analysis report. What we offer you is to select the day you want to report on, then select Browse time. In the Internet Use by list select User. Unfortunately, this will show all the users in ascending order and there is no way to set a limit of one hour. As we drill down to the day level it reports the total amount of browse time spent online. This is similar to the Standard Report for “Which users spent the most time online?”

General Questions

Question: Is there much of an advantage to using 6.3.2 over 6.3.1?

Answer: Yes, Websense Enterprise version 6.3.2 is a stability release with all the patches and customer requests released after version 6.3.1.

Question: What is the number one thing I should be doing with Websense software to protect me from Internet threats?

Answer: Use the reporting capabilities to review the logs generated by Websense, and modify your Websense policy to reduce identified threats.

Question: Where can I go for self-help on troubleshooting the DC Agent?

Answer: The best answer source is the Websense Knowledge Base (kb.websense.com). Search for DC Agent, and you will find many helpful articles.