December Customer Webinar Questions

1. **When updating from 7.6.5 on 10k to 7.7, do you need to update the SQL database?**
   A. Yes, the SQL database needs to be upgraded as well. It has new tables and dashboard elements (e.g. wslogdb70_amt_1). Ensure you back up your SQL database before attempting an upgrade.

2. **Please explain again how you ran testlogserver without stopping logging. It would seem that when you changed it in TRITON for the logserver, it would stop logging. Please provide a link to a document that explains this. Thanks.**
   A. If you recall, I started the TestLogServer utility before making changes in the TRITON manager—so essentially the TestLogServer utility was running and waiting to receive and then redirect traffic back to the Log Server.
   B. Below is the related link. In the TRITON console, you point to the Log Server and it forwards the traffic back to the SQL database.
   C. http://www.websense.com/support/article/kbarticle/How-Do-I-Run-Testlogserver-Without-Stopping-Logserver-Service

3. **What is the first Websense version that had the security override feature?**
   A. The first Websense version to include Security Override I believe was 7.1. However, only in v7.7 was the security override feature inserted into the TRITON management console. Previously, it was available via an .ini file.

4. **Does regex entry take priority over URL or Keyword blocking?**
   A. Yes, Websense filtering looks for matches with Regex entries before checking standard URL categorizations.

5. **What is the browser compatibility for latest 7.7? Does it works well with IE8 or Latest Firefox version?**
   A. Yes, it works with IE8 and Firefox 13.x.
   B. See the following link for full system requirements.
   C. http://www.websense.com/content/support/library/deployctr/v77/dic_sys_req.aspx

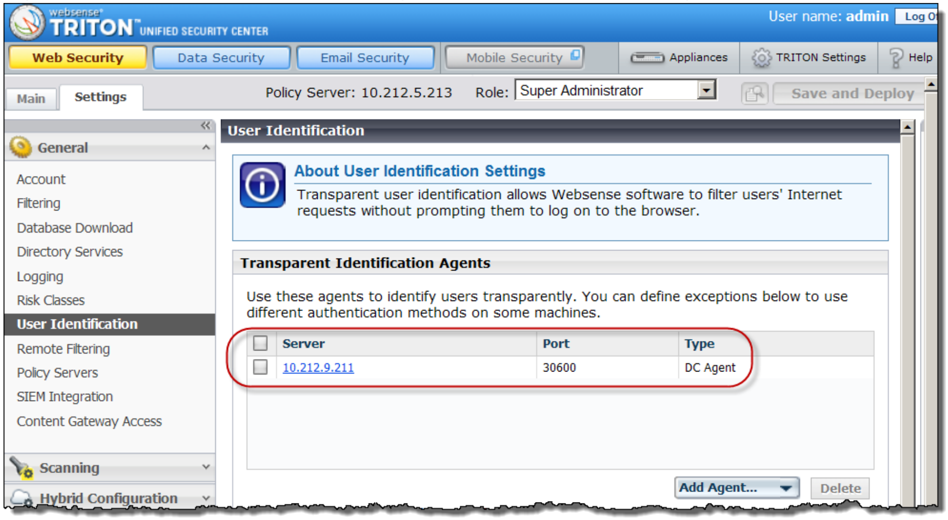
6. **Are there specific logs which would show a specific block access per user & per policy statement applied (e.g. specific block)?**
   A. In Investigative Reports, you can select the drop down 'by user' then click on the yellow button drop down and select blocked by categories.

7. **Absent a custom filtering policy, can the default policy be modified to exclude specific URLS, or will the exceptions only work on the custom policies?**
   A. The Policy exception is a global setting. If you want to be more granular, then you can modify default policy and re-categorize to a custom category, which can be excluded.
   B. The default policy can be modified and configured just like any other policy. It differs, such that when no other policy applies, then it applies.

C. Yes, you can set blocking within the default policy and if an exception to permit traffic applies to an identified client, then that client is permitted to the site even if the default policy applies.

8. **How to block the traffic in Websense Web Security 7.0.1? We have already blocked the category but still users are able to access the internet through or software.**
   A. Troubleshooting will be needed. Look at how you deployed your integration. What policies are set and the type of user identification being used. It is best to contact tech support at this point.
   B. Also, confirm if Websense actually sees all requests going to the Internet. Recall, some integrations only send http traffic to Websense. You may need to install Websense Network Agent to pick up non-http traffic.

9. **How can I find out if I'm using the DC agent? I don't think there's any agent that is installed on user's machines.**
   A. DC Agent is most commonly installed on the Websense server. Typically, you just need one DV Agent in a network. You can look into the Windows services to check if Websense DC Agent is installed. You call also log into the TRITON management console as shown:



Policy Server: 10.212.5.213 Role: Super Administrator

User Identification

About User Identification Settings

Transparent user identification allows Websense software to filter users' Internet requests without prompting them to log on to the browser.

Transparent Identification Agents

Use these agents to identify users transparently. You can define exceptions below to use different authentication methods on some machines.

□	Server	Port	Type
□	10.212.9.211	30600	DC Agent

   B.

10. Occasionally some users who are part of a group that is unrestricted gets blocked and without changing anything they'll have access again, this just happened yesterday. Any reason which may cause that to happen?

A. It depends on the transparent identification in use. If you are using the common DC Agent, there is a time-to-live (TTL) period. User names can expire from the Websense user identification map. This period is 24 hours by default. The most common case is where the users do not logoff, and therefore do not create a new 'net session' on the domain controller. As a result, their username is not refreshed and they fall off the DC Agent user name map after the timeout occurs. Run an investigative report the end user's IP address (like I did in the presentation) and check if you more than one user name.

11. Why does the filtering service allow a page during a certain time and blocked the next on the same user? We use active directory not IP addresses.

A. There can be several reasons for this and troubleshooting is needed. One scenario is where a time is set on the policies and the user applied to that time based policy. The more common reason is a failure with user identification. Earlier version of Websense could display this symptom when updating its user directory cache. Upgrade to the latest version of Websense to resolve this issue.

12. I have to move TRITON off my V-Series appliance in order to use the Forensics Data tool. What exactly does this tool provide to us?

A. You can look at the details of the captured or quarantined files. See the following link for an explanation.
http://www.websense.com/content/support/library/web/v77/triton_web_help/threat_forensics.aspx

13. My client list shows some IP addresses as well as user names. Most of the IP addresses are associated with users already listed. Why does it show IP addresses?

A. At some point, that machine was logged as an IP address. There could be several reasons depending on the transparent identification used. If there are updates while a user is logged out, it will be recorded as IP address. If the user does not log out, a timeout occurs and user is unidentified. If that is the case, most people use logon agent in conjunction with DC Agent.

14. For non-HTTP Data, is it a global Block/Permit, or can we block specific non-HTTP sites? For example, we block 'http://www.facebook.com' but since we need to have HTTPS (secure) sites permitted, we have to allow 'https:www.facebook.com', which students have learned very quickly.

A. You need Web Security Gateway proxy to decrypt SSL traffic. Otherwise you have to custom recategorize by IP address (e.g. https://<ip adress>:443). This entails more work—there can many IP addresses for any given domain.

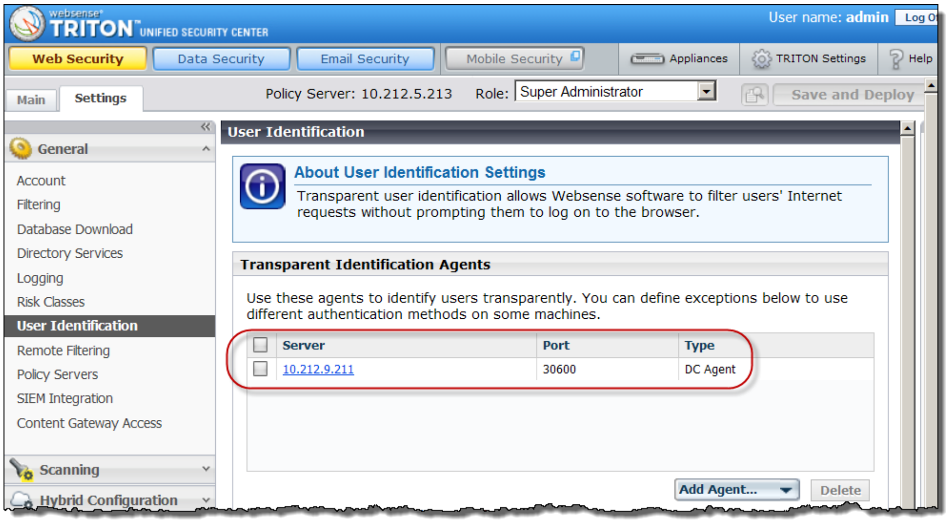
15. When using the TestLogServer tool, do we lose the ability to log and store current activity?

A. If you use TestLogServer with the forward option, you do not lose any current activity. For more information, see the following article.
http://www.websense.com/support/article/kbarticle/How-Do-I-Run-Testlogserver-Without-Stopping-Logserver-Service

16. If the investigation report only displays IP addresses and not user name, where can I find my user service or dc agent?

A. Look in Windows services on the Websense server. See this link for details:
http://www.websense.com/support/article/t-kbarticle/Troubleshooting-DC-Agent-with-ConsoleClient

B.



Policy Server: 10.212.5.213 Role: Super Administrator

User Identification

About User Identification Settings

Transparent user identification allows Websense software to filter users' Internet requests without prompting them to log on to the browser.

Transparent Identification Agents

Use these agents to identify users transparently. You can define exceptions below to use different authentication methods on some machines.

	Server	Port	Type
□	10.212.9.211	30600	DC Agent

17. What was the test site's URL? I didn't catch it. Thanks,

A. For HTTP: http://testdatabasewebsense.com

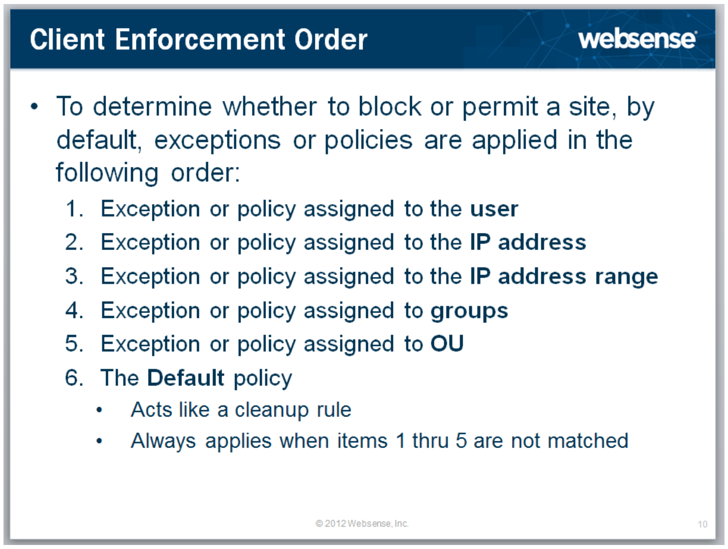
B. For HTTPS, look here: https://testdatabasewebsense.com

18. Is Realtime monitoring an option in version 7.5?

A. Real-Time Monitor is available in versions 7.6 and later.

19. How do I know whether the policy order hits the user first, then IP address, then IP address range?

A. By default, the policy checks for User first, IP address, group, then IP address range. Slide 10 contained this information.



Client Enforcement Order

- To determine whether to block or permit a site, by default, exceptions or policies are applied in the following order:
  1. Exception or policy assigned to the **user**
  2. Exception or policy assigned to the **IP address**
  3. Exception or policy assigned to the **IP address range**
  4. Exception or policy assigned to **groups**
  5. Exception or policy assigned to **OU**
  6. The **Default** policy
     - Acts like a cleanup rule
     - Always applies when items 1 thru 5 are not matched

© 2012 Websense, Inc. 10

20. How do I check whether I set up my policy by User?

A. You can refer to the Client section in TRITON – Web Security manager or use the Check Policy Tool located on the right of the TRITON manager.

21. What is the purpose of Security Override? You keep mentioned it several times.

A. Security Override is a safety feature. If an administrator re-categorizes a URL to a permitted category, Security Override checks to see if that URL's original category is marked as a Security Risk. Security Override's job is to check if the original category is safe before you allow access to sites. If the URL is unsafe and/or compromised; it then blocks the URL.

22. I can't seem to find the hidden block page data on Firefox. How do I find this?

A. Navigating in Firefox is slightly different. In the upper pane of the block page, right-click in the window and select "This Frame". From second drop down menu, select then "This Frame Source". The moreBlockInfo page should then appear.

23. Which browser should I use to test the moreblockpage information and filtering results?

A. When viewing the moreBlockInfo data, you most likely will be in a remote session with an end user. It is best to use the same browser the client is using. This ensures the closet the possible recreation of the issue when diagnosing a problem. While the steps you perform to actually retrieve the moreBlockInfo data is slightly different in IE, as compared to Firefox, the resulting information is the same.

24. Is there a way to prevent a client from accidently falling to the default policy? In other words, have some sort of redundant measure?

A. Typically, not detecting a user name results in your clients receiving the Default policy. To avoid this problem you can install additional DC Agents and configure them to poll the same domain controllers that your users log onto. You can also install Logon Agent to identify users; it can work in conjunction with DC Agent. The Logon Agent / DC Agent combination is one of the more common deployment methods for redundancy.

B. If name resolution fails, you can have 'backup policies' based on IP address or IP ranges. I have spoken to many Websense administrators who provide their executives with static IP addresses on their workstations, and then assign those executives redundant IP address based policies.

25. Does TestLogServer display all protocols that are being passed?

A. Typical integrations generally only send http, https, and ftp traffic. Network Agent is required to pass non-http traffic to the Filtering Service. When Websense is first installed, only some protocols are set to be logged. Protocols not set to be logged do not show up in your reports.

B. To directly answer your question, TestLogServer may not show all protocols. If you configured some protocols to not log, and by default some protocols are set to not log, then Filtering Service removes this logging data before streaming it out to Log Server.

26. Can Network Agent with port mirroring enabled work in conjunction with third party integrations?

A. Yes, and this is best practice to provide the highest security for your network. In integrated mode, the Network Agent receives traffic from the port span and only filters the non-HTTP protocols. The third party integration is responsible for filtering HTTP traffic. This is one of the more common setups.

27. What happens to the quota time if you have two different filtering services? Does the user receive different quota times if they are redirected to another filtering service?

A. The answer is yes for any version prior to 7.7. In version 77, we now have the new State Server service. This service keeps track of quota times across multiple filtering services.

28. How often does Websense sync with Active Directory. For example, if I move a user from one group to another, when is the Policy for that user in the new group implemented?

A. By default, Websense syncs with Active Directory on user group information every 4 hours. After the user cache is updated, the user will receive their new policy.

B. You can clear the User Cache earlier.

29. Can I add multiple policies to the group? If so, how does it behave?

A. Yes, as mentioned in an earlier slide, there is an option to apply most restrictive filtering. If checked, the policy with the most restrictive filtering, among the multiple different policies, is applied to the multiple groups.

30. Do you have to restart the filtering service if you modify the UserGroupIpPrecedence?

A. Yes, In order for the Filtering Service to implement the change, you need to restart the service. Most changes to .ini files require restarting the associated service. You can follow the steps in a KB by searching "UserGroupIpPrecedence".

31. Can you unblock part of a site and leave the main site blocked? For example, permitting a specific YouTube video?

A. This can accomplish this easily in version 7.7; however, you need Websense Web Security Gateway. The proxy has the ability to add headers and use Google's header string to allow certain videos. This was created mainly for Google/YouTube educational videos for schools.

32. How do I determine what integration is sending the traffic if I run testlogserver?

A. Look at the Server IP address in TestLogServer output. This is will be the IP address of the integration sending look up requests to Filtering Service.

33. Why do you keep using purple.com in your demonstration? I think I missed the significance of that URL.

A. Purple.com is categorized as Educational Institutions, which is a safe category and URL to test with. It is an easy site to demonstrate as it has very little content, no offensive material, and easy to search for when I want to identify users in reports. It also happens to be generally a unique word, such that when searching I rarely receive false-positives.