Websense Support Webinar: Questions and Answers

Diagnostic and debugging tools
Websense Web Security™ Version 7

Question: Can we use some of the debugging tools from this Webinar with Websense Enterprise version 6.3.1?

Answer: Yes. Apart from the Websense Manager Toolbox (which is new to version 7), all of the tools are available in older versions of Websense Enterprise.

Question: Should all domain controllers be listed in **DC_config.txt**?

Answer: Yes, all domain controllers in your network that you want DC Agent to poll need to be included in the **DC_config.txt** file.

Question: Can you remove items from the **DC_config.txt** file if "workgroups" are listed? Or is it better to leave them in the file and set =off?

Answer: It is best to leave the entries in the file. Change the lines you don't want to use so that they say =off. After you have made the changes, then restart DC Agent.

Question: You add a domain controller by adding it in **DC_config.txt**, but do you need to add it if you already have the global catalog there?

Answer: The DC Agent service will auto-discover any new domain controllers that are added into your network. However, if you wish to manually add a domain controller into the file, you may do so by adding it and then marking it as =on. Be sure to restart the DC Agent service after you change the file. Note that there must be a blank line at the end of the file.

Question: We use Script Logic in our environment, and this service uses SLUSER as the account that it runs under. We frequently see Websense software report that SLUSER is the user instead of the login person. Are you familiar with this issue?

Answer: This is something that we have seen. What happens is that DC Agent discovers this other service account and records that in its map. To stop this from happening, you can add the service account into the file named **ignore.txt** (located in the \websense\bin folder). After you change the file, restart the DC Agent service.

Question: Can Websense Web Security be run from a Windows XP box?

Answer: No. Websense Web Security is not supported on Windows XP. For currently supported operating systems, please see the Deployment Guides available on our Web site.

Question: Is Websense Web Security 7.0 a free upgrade for Websense Enterprise version 6.3 users?

Answer: Yes. With a current subscription, you can download the v7 installer from our Web site.

Question: What is the default output folder for any diagnostic and debugging files?

Answer: By default all Websense debugging and diagnostic files are stored in the \websense\bin folder.

Question: When I am using the ConsoleClient tool, is there a way to change the directory of the output from something other than BIN (such as c:\temp)?

Answer: Yes. When you navigate through the initial options for the ConsoleClient tool, use the "Filename" parameter to enter the output path and file name (such as c:\temp\test.txt).

Question: On the Websense Support site, is there a listing of the different dump levels and what they can provide?

Answer: Always use Dump Level as 3 when you use ConsoleClient.

Question: Why does Websense Log Server have to be stopped in order for us to run the TestLogServer tool?

Answer: TestLogServer provides a way of viewing the data being sent from the Filtering Service to the Websense Log Server. You need to stop Log Server, because the TestLogServer tool listens on the same port as Log Server.

Question: Can you run WebsensePing with a specific user ID or IP?

Answer: You can run WebsensePing with various options. To view the list of available options, run **websenseping.exe –h**. Full details are available from http://kb.websense.com/article.asp?article=2917&p=12

Question: Can WebsensePing be used on a workstation other than the Websense Filtering Service machine?

Answer: No. WebsensePing can be used only on the Websense Filtering Service machine.

Question: Does WebsensePing differ from the Websense URL Category tool?

Answer: WebsensePing provides more options and can provide a more detailed output. The URL Category tool shows you only the category that the URL falls into.

Question: Will WebsensePing work with SSL/HTTPS sites as well as HTTP?

Answer: Yes. You can use WebsensePing with HTTPS sites.

Question: When I use WebsensePing, how do I know which policy may be getting applied?

Answer: WebsensePing does not show which policy is being applied.

Question: What's the correct order for stopping and starting the Websense services?

Answer: Please refer to KB article http://kb.websense.com/article.asp?article=2957&p=12

Question: Can unique block pages be configured for different policies, or is there only one set of block pages for the entire system

Answer: The block pages are the same system-wide for all users and policies.

Question: Should the **DC_config.txt** file have the remote (WAN) DCs listed?

Answer: This depends on your Websense software and your network setup. You can raise this query with Technical Support, and we can have a look at this with you and provide a definitive answer.

Question: How do you put the TestLogServer on a different port? Can I show only IP address?

Answer: If you ever forget the options, you can always enter **testlogserver.exe –h** from the command line. This shows you all of the options. If you want TestLogServer to listen on a different port, and then show traffic only from machine IP 192.168.0.1, you would enter:

testlogserver.exe -port 55999 -onlyip 192.168.0.1

Remember: if you are changing TestLogServer to listen on a different port, then you need to change the setting in Websense Manager to point the logging towards this new port.

Question: When I use WebsensePing, what does it use to determine the disposition of the URL? How does it know which policy to base that on?

Answer: WebsensePing queries the Websense Filtering Service with the details that you provide it from the command prompt. If you provide no user/workstation details, then it provides results based on the Default policy.

If you provide user or workstation credentials, then it provides results based on the policy for that user/workstation IP.

Question: Can I use the ConsoleClient tool to debug other agents like the RADIUS Agent?

Answer: You can use ConsoleClient to connect to the diagnostics ports for each service, which then enables you to perform further diagnostics.

Diagnostic Ports:

PolicyServer – 55810

Filtering Service – 15869

DC Agent – 30601

Logon Agent – 30603

RADIUS Agent – 30801

Network Agent – 55870

Question: Does TestLogServer have a way to show only blocked pages for a particular IP address?

Answer: You can ask TestLogServer to show you traffic coming **from** a particular workstation IP address or a range of IP addresses. If you want to search for blocked pages, export the traffic information to a file by using the **–file** option. You can then open this file and examine it for blocked pages.

websense®

Question: Is there a way to debug Log Server running on Linux?

Answer: Yes. To debug Websense Log Server running on Linux:

1. cd /usr/local/Websense/UnixExplorer/bin

2. ./logserverdctl stop

3. Then, run: ./logserverd –d

This runs Log Server in debug mode.

Question: When I am troubleshooting a particular user, the user information is not displayed, as if Websense software can't determine who the user is. What could cause this, and what would be the best way to troubleshoot for one user?

Answer: If you are using DC Agent, execute ConsoleClient on port 30601. When you have the output, you can then verify whether DC Agent is picking up the correct user details, or whether it is picking up a service account or something else.

Question: After I add a user in Active Directory, how soon should I expect Websense Web Security to know that the user exists?

Answer: If you add a new client, be sure to add the client in Websense Manager (if the new user doesn't already fall under a directory group or OU that's been added previously).

If you have added a new user into a group or OU that exists in Websense Manager, then the software picks up that change in approximately 3 hours.

Question: What can cause the **DC_config.txt** file and the **xiddcagent.bak** files not to be created when DC Agent is running?

Answer: We have seen this happen when the DC Agent service is installed with an account that doesn't have the correct rights to be able to poll the domain controllers. In that case, the files never get created, and the file **DC_config.txt** has to be created manually.

Question: Where can I get information about upgrading to Websense Web Security v7? Is there a migration document available? We are concerned that our current hardware will not be enough.

Answer: Search for Deployment Central in the Websense Knowledge Base for server specifications. Upgrade instructions for v7 are provided at the following link: http://kb.websense.com/article.asp?article=3690&p=12

Question: If Filtering Service and Policy Server are on different servers, how much latency can be allowed between them? How do I determine if that latency is causing problems with the Filtering Service? This assumes the filter and the firewall are on the same subnet, to optimize their performance.

Answer: Please log this question with Technical Support. We would be pleased to assist you.

Question: Is there any way that we could block https:///www.facebook.com without actually blocking all HTTPS traffic?

Answer: Yes it is possible, and this depends on your integration. For advice on setting up custom URLs for HTTPS sites, please see the NOTE at the bottom of this article: http://kb.websense.com/article.asp?article=2414&p=12

Question: If a user belongs to groups to which two separate policies are applied, only one will be applied to the user, correct?

Answer: Yes. Only one policy can be applied to a user. If a user belongs to two separate groups that have different policies, then by default Websense software applies the least restrictive policy. You can change this to most restrictive by going into the Websense Manager and navigating to Settings > Filtering.

Question: I've read that User Service caches DC lookups (for Group/OU membership) for 3 hours. We have a pool of accounts that change OU frequently. Is it possible to reduce the cache from 3 hours to 1 hour?

Answer: Yes. To change this, first make a backup copy of the file **websense.ini** located in the \websense\bin folder. Then add the following lines to the file:

 [USERGROUPS]
Update=1

Save and close the file, and then restart Websense User Service.

Question: Is the Windows 2003 Small Business Server (SBS) edition supported for Websense Expresss?

Answer: No. Small Business Server is not supported.

Question: I'm doing a Juniper Netscreen integration. When I use ConsoleClient to do a trace of WISP, I may see: ID 55555 Invalid Request. What causes this? I get these warnings repeatedly.

Answer: Some third-party integration software checks to see if the Websense Filtering Service is alive by sending a probe on port 15868. Websense software sees this request; however, it doesn't understand the probe if it was not sent in an expected format. This can show up as an Invalid Request. You can safely ignore this.

Question: How does DC Agent populate the **DC_config.txt** file? Specifically, how does it get the domain name (or names)? I have seen very odd domains in this file (and in the application log). For example:

0x1558000: System error while enumerating the domain controllers. domain: MAINT

Answer: DC Agent searches for new domain controllers and domains in your network and adds these into the **DC_config.txt** file. DC Agent may have located a machine that was (for example) in the MAINT workgroup/domain and added this into the file. You can turn auto-discovery off.

İnformation on this can be found in http://kb.websense.com/article.asp?article=3602&p=12