

Exploring DC Agent in Depth

February 16, 2011

1. Q. Is dc agent run in conjunction with NTLM authentication or is it used instead of using NTLM?

A. The DC Agent is not involved in the NTLM auth process. DC Agent queries each domain controller for user logon sessions, where it obtains the user and computer name. For each logon session, DC Agent performs a DNS lookup to resolve the computer name to an IP address, and then stores the user name/IP address pair in its user map in local memory. This info is passed to the Filtering Service. The Filtering Service asks Websense User Service to look up group membership data from your directory services. The Filtering Service caches the User Service's reply, so that when traffic is seen again from the same end user, correct filtering policies may be applied faster.

2. Q. Can we change to less time to change that table?

A. By default, the DC Agent retains user names for 24 hours. You may reduce the amount of time that user names are retained via the TRITON – Web Security console within the User Identification > DC Agent settings. Select the Help button (on the DC Agent setting page) for specific details affecting this option.

3. Q. Do any customers change the user timeout setting?

A. Typically, the timeout setting is never changed. However as one example, I have seen a few customers try to use Websense to enforce security policies. This is not best practice, but it did work perfectly for in their specific situation.
The timeout or time-to-live setting (entry in the DC Agent's user map) is updated whenever the end user logs into the network or requests network resources. So potentially, an entry in the user map will be updated multiple times throughout the day. Best practice is to not change this value. However, if you want to experiment using different timeout values, then you will need to run ConsoleClient to pull the DC Agent user map throughout the day so as to assess your changes.

4. Q. Should we exclude all service accounts then?

A. Yes. Typically you should exclude all service accounts by identifying them in the ignore.txt file; such that, they will not appear in the DC Agent user map. You can determine if adding service accounts to the ignore.txt file is necessary by running an Investigative Report on all User Names. Locate a service account name and then expand to show the associated IP addresses. If you see only server IPs, then you are probably OK. If you see end user workstation IP addresses in the report, then you should add the service account name to the ignore.txt file. If not, then not all traffic generated by the end user will be reported under that end user's name.

5. Q. Can you use LDAP to a OU in the ignore.txt file? Or do I manually have to add every service account? vm_user___ is a good example for this.

A. Sorry, no. You have to add entries manually. However, you do have grouping and wildcarding options. For example:

johnsmith
admin,WKSTA-NAME
*, WKSTB-NAME
*, 10.209.34.56
*, 10.203.34.1-10.203.34.255

For details, see page 41 in the [Transparent Identification white paper](#).

6. Q. What about ignoring the anonymous account with 2008 servers?

A. Excellent question. I did not cover this in the Webinar. Are you seeing the anonymous account showing up in reports? If so, then you should add it to the ignore.txt file. Your goal is to not see service accounts added to the DC Agent user map, thereby replacing the actual user who is logged onto the workstation. See the 'Should we exclude all service accounts then?' questions (two above) for an expanded explanation.

7. Q. Is the XID User Map PrintSelf the same as the dcmmap.txt?

A. In my example in the Webinar, Yes. When I ran the ConsoleClient utility, it asked for a file name to dump the data too. I provided the name 'dcmmap.txt' as the file to receive the data when dumping the DC Agent cached map.

8. Q. Where is the dcmmap.txt file? I do not have that on my install.

A. The dcmmap.txt file was generated as a dump file when I ran the ConsoleClient utility. So if you have not run the utility, the file will not exist. The dump file could have been any name. When I ran the ConsoleClient utility, it asked for a file name to dump the data too. I provided the name 'dcmmap.txt' as the file to receive the data when dumping the DC Agent cached map. When the file is generated, it resides in the \Websense\bin directory. To see details for running the ConsoleClient tool, see the [Troubleshooting DC Agent with ConsoleClient](#) article.

9. Q. If users lock their machines throughout the week and maybe perform a reboot or shutdown at the end of the week. Are users going to experience issues with filtering because they are locking their machines vs. logging off?

A. Possibly yes, but not always. This depends on if the user make requests for network resources during the day. If he\she does, then their name is picked up and refreshed in the user map. It takes 24 hours, by default, for names to expire from the user map.

10. Q. Do I understand correctly that WebSense does not support cached credentials? All users have to log off and log back on every morning (not very feasible)?

A. The DC Agent picks up user names when network resources are requested; such as, logging into the network, mapping a drive, etc. You can easily check if a problem exists by running an Investigative Report on User Names for a single day. If no IP addresses are displayed, then DC Agent is working fine in your environment. Typically however, you will see some IP addresses displayed. These IPs should be your domain controllers and servers because no one is logging on locally and/or their service accounts are NOT added to the ignore.txt file. What do NOT want to see IP addressed (in reports) of end user workstations where you know normal work activity is being done—a user name should be displayed.

11. Q. If I install just the DC Agent component on a remote site Domain Controller, does it require a restart?

A. Well our documentation says yes, 'a restart is required when installing DC Agent.' However, in real-life troubleshooting, this was not always the case. I generally installed the DC Agent, check if the dc_config.txt file was created and properly configured, then ran ConsoleClient to pull the user map. At times the map is blank and only by restarting the domain controller would names appear.

12. Q. If your domain servers are 2008, does the windows server running DC agent need WINS enabled?

A. If a WINS server is available, then add it to the NIC properties on the DC Agent server. Otherwise, at least ensure that NetBIOS is enabled on all your domain controllers and server where DC Agent is installed. The symptom we see with NetBIOS issues, is that the dc_config.txt file fails to generate or fails to have all the domain controllers listed. When a WINS server is not available, DC Agent asks the User Service to locate the domain controllers.

13. Q. So does this mean I must set one to off?

A. To reduce unnecessary network traffic, you should set all domain controllers, that appear in the dc_config.txt file, to '=off' so that only the domain controllers listed set to '=on' are the servers that your users (who are filtered by Websense) will actually log onto. DO NOT DELETE the domain controller entries, from the dc_config.txt file, that your users do not log into. These domain controllers will reappear during the next discovery process.

14. Q. I have two dc agents, when a new dc is added to the domain its updated on both dc_config.txt.

A. Yes, this is how the process works, the DC Agent should populate the dc_config.txt file with your new domain controllers. However, the DC Agent only performs a domain discovery process upon service restart or at midnight (once a day), so there is potentially a partial day where the DC Agent will not know about the new domain controller. If the domain discovery process is disabled, not the default behavior, then all new domain controllers need to be manually added.

15. Q. What potential issues could arise if modifying the "Use entry timeout" under Domain Controller Polling from 24 hours to something greater, say 72 hours?

A. The 'potential' is that a new user's Internet traffic may be logged as the previous user who is listed in the DC Agent user map. Generally, all new users need to log into the network, so this is not a problem.

16. Q. I have child domains and domain controllers for each of those and currently all DCs at all Domains are turned on. Is this ok?

A. I hope the list of domain controllers is under 15. But what is really important is that DC Agent does not miss users logging into to your network. Run an Investigative Report for the current day on User Names. If no IP addresses are displayed, then DC Agent is working fine in your environment. Typically however, you will see some IP addresses displayed. These IPs should be your domain controllers and servers because no one is

logging on locally and/or their service accounts are NOT added to the ignore.txt file. What do NOT want to see IP addressed (in reports) of end user workstations where you know normal work activity is being done—a user name should be displayed.

17. Q. Is it recommended to run the DC Agent on a domain controller?

- A. No, but this was the suggested install method for DC Agent years ago in our v3.x and v4.x releases. You may still see a KB that suggests this, but the recommendation is to install DC Agent on a member server. So try to locate a member server first. If that is not possible, then go ahead and install the DC Agent on one of your domain controllers. In some troubleshooting cases, I could not get the DC Agent to work on a member server and then moving it to a domain controller resolved the problem.

18. Q. Are you saying we should have a DC Agent on each of these sites?

- A. This depends on your connection to your remote site. If bandwidth it never an issue, then you most likely do not need a DC Agent hosted at the remote site. However, if you installed a domain controller at your remote site to resolve issues of slow network logins, then you may benefit from installing a DC Agent remotely. See the question above to look at Investigative reports for checking the effectiveness of DC Agent.

19. Q. We have over 30 sites with their own domain controllers.

- A. See the answer to the previous question. If you do not have network issues and bandwidth is not a problem, then I would suggest installing two DC Agent and configuring each agent to monitor only 15 domain controllers each.

20. Q. For how long will I be able to see an idle user?

- A. By default, users names are retained for 24 hours.

21. Q. How can you check to see which hotfixes have been installed/applied in your environment?

- A. This can be kind of tricky. I look at the properties of the executable files that are replaced by the hotfix. Generally, the files have a version number or differ by the size of the file. You will have to download the latest hotfix to compare against files existing on your server. If you are not sure, it does not hurt to reply the hotfix.

22. Q. What is the actual process that Websense uses using DC Agent when polling the dc to obtain the user name? How does it obtain a user name from the info collected from the dc?

- A. Excellent question. If you want to know the exact details in-depth, then please see our white paper starting at page 11: *Introduction to Transparent User Identification*
B. http://www.websense.com/content/support/library/web/v75/user_id/first.aspx

23. Q. DC Agent often fails to work for our roaming laptops. Either on our VPN network or remote offices. This is because the map file has the ip that they are using mapped to another user. How do I resolve this issue?

- A. I apologize for not bringing up this scenario during the Webinar. For roaming users, you are better served by also employing Logon Agent. It can be used along side of DC Agent. It has a higher priority over DC Agent, so the name pick up by DC Agent is superseded by user names obtained by Logon Agent.

24. Q. Is TestLogServer going to be integrated into one of the GUI interfaces in the future?

25. Q. When is Websense going to have a nice GUI to run these commands rather than using command line?

- A. I used TestLogServer to display and test because the data is immediately available. The same data is also available in reports. If you run an Investigative Report on IP addresses, then look at a single user, you will see the same data. The catch is that there is a couple minutes delay as the logging data is cached, moved, and inserted in the log database. I have not heard of a GUI for it as of yet. I know that a GUI is not part of our next v7.6 release. Please email suggest@websense.com to request this feature.

26. Q. Can ConsoleClient commands be scripted?

- A. Absolutely, but this is something you will have to create on your own. Here is a link to the ConsoleClient debug article: [Troubleshooting DC Agent with ConsoleClient](#)

27. Q. Did I understand correctly that WebSense username recognition relies on NetBIOS? Since Microsoft is considering NetBIOS a legacy unsupported protocol will WebSense be upgrading to a support protocol?

- A. Websense must identify users to apply group and user policies to traffic. The process to identify users is essential for web filtering. The majority of our customer base employs DC Agent, so when NetBIOS support ends, either DC Agent will already be modified or another agent will be available. So sorry, I do not have an answer as to what we are doing next, but because of the importance of identifying users, a remedy will exist.

28. Q. How does disabling NetBIOS over TCP/IP affect this?

- A. Typically, we see the dc_config.txt file not generate. Also, the DC Agent must then rely on the User Service to resolve user names.

29. Q. Non related Websense question - Please advise app name that shows server spec & details on presenter's desktop.

- A. Visit www.sysinternals.com and search for BGInfo.

30. Q. Where can I get those batch files for stopping and starting the WS 7.5 Services

- A. To stop services, save the following to with a file with .bat extension:

```
@ECHO OFF
ECHO This job stops Websense services!
Pause
net stop "Apache2Websense"
net stop "ApacheTomcatWebsense"
net stop "Websense Usage Monitor"
net stop "Websense Reporter Scheduler"
net stop "Websense Logon Agent"
net stop "Websense DC Agent"
net stop "Websense RADIUS Agent"
net stop "Websense Explorer Report Scheduler"
net stop "Websense Information Service for Explorer"
net stop "Websense Log Server"
net stop "Websense Network Agent"
net stop "Websense Filtering Service"
```

```
net stop "Websense User Service"  
net stop "WebsenseControlService"  
net stop "Websense Policy Server"  
net stop "Websense Policy Broker"  
net stop "Websense Policy Database"
```

To start services, save the following data to a file with a .bat extension:

```
@ECHO OFF  
ECHO This job Starts Websense services!  
Pause  
net start "Websense Policy Database"  
net start "Websense Policy Broker"  
net start "Websense Policy Server"  
net start "WebsenseControlService"  
net start "Websense User Service"  
net start "Websense Filtering Service"  
net start "Apache2Websense"  
net start "ApacheTomcatWebsense"  
net start "Websense Network Agent"  
net start "Websense Log Server"  
net start "Websense Usage Monitor"  
net start "Websense Reporter Scheduler"  
net start "Websense Logon Agent"  
net start "Websense DC Agent"  
net start "Websense RADIUS Agent"  
net start "Websense Explorer Report Scheduler"  
net start "Websense Information Service for Explorer"
```

I built these scripts myself. In the future, essentially you will need to update the service name shown above in quotes. Look at the service properties for the Display Name. Some services names do change in our next version, and additional service are also available. So you will need to update the script to account for new\changed service properties' Display Names as seen when running *services.msc* at the run box.

31. Q. As you mentioned earlier, some users lock their workstations at night or hibernate, but the XID doesn't get updated until they query a DC. Is there an easy way to make this happen other than having the user access a network share, etc.?

- A. If you are seeing user names disappearing, you may consider turning on computer polling. This feature does not trouble all users, so you may find it works for you. Additionally, you can turn on manual authentication to force users to log in. Manual authentication can be annoying as it pings the user to log in when they open a new browser after ten minutes has expired. You also have the choice to use the Logon Agent to capture user names. This is quite effective for wireless, roaming, and user who do not log in often.

32. Q. Can the DC Agent correctly map MAC OSX systems authenticating through LDAP / OpenLDAP / Centrify or others?

- A. If a net session is passed on the domain controller then DC Agent will pick up the user name from a MAC. Simply log into the domain controller where the MAC user is logging into and view the net session data. You also have the option of enabling Manual authentication.
- 33. Q. If you ignore the Websense account in the ignore.txt file will that browse data still get populated in the presentation group reports? (e.g. total browse time for the company?)**
- A. All traffic is logged. If the user name is ignored, then the traffic is still logged with the associated IP address.
- 34. Q. I noticed your attempt to create a login request using a Mapped Drive. What constitutes a login request; i.e. a login the DC agent recognizes.**
- A. A net session must be generated on the domain controller. The name did appear, I failed to give it 30 seconds or so to work. I typed the following:
- i. Run the **NET USE %LOGONSERVER%** command.
 1. For example, type: **net use //<domain_controller_name>**
- 35. Q. Does the Computer Browser Service on Server 2008 need to be enabled on the domain controllers themselves?**
- A. Yes, on every domain controller and member server where you have DC Agent installed.
- 36. Q. Any issues- updating 7.1 to latest version?**
- A. Generally you should not have a problem when upgrading. Always back up Websense before starting. I have a checklist that I would be happy to provide you. Open an case and ask for Greg's handholding article for upgrading Websense. I point out how to avoid problems by checking your server for issue seen in Tech Support. It will be attached to next month Webinar on April 13th, 2011 as a downloadable attachment. Next month's Webinar topic is on upgrading.
- 37. Q. How do you get VPN users to filter using the DC Agent?**
- A. If they are logging into the network, then Websense picks them up like your internal users. If they are authenticating via a RADIUS server, then you will need to install our RADIUS agent to log their user names. See page 27 of the following white paper for details on RADIUS agent. [Introduction to Transparent User Identification](#)
- 38. Q. Is there any option to change the User Service updates group/OU every 3 hrs?**
- A. This feature is available manually in v7.6 by using a button, within the manager, to force an immediate update. V7.6 should be release in April 2011. See the following article for more information on your question: [No Filtering For A Few Minutes After Clicking Save Changes](#)
- 39. Q. You use the ignore .txt file in version 7.1?**
- A. Yes, the ignore.txt file is available for all versions of DC Agent.
- 40. Q. In some investigative reports we get two different name formats for the same person (e.g. Doe, John [jdoe] vs Doe\, John) Is that DC Agent related or is DC Agent always based on the logon name?**

- A. Generally, this occurs because when you originally installed Websense, it was configured for winNT. Later on sometime, Websense was configured for Active Directory. Your reporting log database most likely contains information from NT and Active Directory. To correct this, create a complete new reporting database by following this article: [Can I Manually Create A New Catalog Database?](#)
Another, but slight possibility is that you changed the display name structure in your network. Use the same remedy provided one sentence above.
- 41. Q. is it possible to bypass authentication by example: client or network list?**
- A. Yes, selective authentication is available from with the Web Security manager under Settings > User Identification.
- 42. Q. In the dc_config file, does the DC Agent check the DC's in a specific order?**
- A. It round robins the list, sending out queries only to DC's listed with a '=on' status.
- 43. Q. You mentioned earlier a user who just locks their wkstn rather than logging off. How exactly would the user map get populated the next day when they return without a domain logon?**
- A. Generally, the user is using network resources, so the name is updated quite often throughout the day.
- 44. Q. If you have multiple DC Agents per filtering server that don't overlap DC's in polling, are the two user maps just combined into one XID User Map? And is there a time interval in updating the XID User Map or is it in real-time?**
- A. All your DC Agents update the Filtering Service. Each DC Agent only has a portion of the user map, for the users it detected. Only the Filtering Service contains a full copy of the user mapping.
- 45. Q. Also, our websense.log is in the Websense\tomcat\logs folder.**
- A. You will want to review the websense.log file in the \Websense\bin directory for errors.
- 46. Q. Can DC agent be used in conjunction with additional authentication methods. (LDAP, NTLM, ect.)**
- A. Yes, DC Agent is just grabbing a machine name and resolving it to a User name, then pairing it with the associated IP address from the net session. The net session info, that DC Agent is monitoring, displays a machine name and IP address.
DC Agent is not concern with directory structure. The user name\ip address pairs are passed to Filtering Service. Filtering Service then asks User Service to locate group info from your directory service.
- 47. Q. Please let us know if Websense supports users with the same name belonging to different domains in multi-domain environment. Let's assume that we do have correct configuration in Settings | Directory Service. Simply if there is a user John Doe in Dom1.companyx.com and another user with the same name in Dom2.companyx.com if DC Agent and User Service will be able to differentiate them and Filtering Service to apply policies properly?**
- A. Not by default. All names need to be unique within each domain and across all domains. A configuration file needs to be modified to force DC Agent to retain the domain. You

need to enable the *UseDomainMap* parameter via the *websense.ini* file. See the following forum post: <http://community.websense.com/forums/t/2078.aspx>

Also, each domain needs to be identified in Web Security manger under directory services with the proper root context. For details, see the prior Webinar: [Configuring Websense with your Directory Service](#)

48. Q. Are the hotfixes referring to 7.5.x?

A. Yes, but for DC Agent, you will still want to check if a hotfix is available for your version.

49. Q. Do we have a version for 6.3.3 for the drop issues between Filter services and DC Agents if so, what is it?

A. Good question, no this was a v7.x issue only.

50. Q. However, how does that work with Vista/7 where you can have more than one user logged in? Does it take the last logged in user?

A. Websense picks up the new login when users switch on the same workstation. It always uses the last user logged in unless the name appears in the *ignore.txt* file.

51. Q. Our filtering service is not located on the same box as the DC Agent (it is on the V10000 box) Does this make any difference?

A. No problem with DC Agent and Filtering Service being on different servers. The concepts discussed in the Webinar still apply.

52. Q. What should be the problem when you are running the DC agent diagnostic and get server Timeout occurred.

A. Please see page 10 in the following document: [Debugging Websense Services Using ConsoleClient](#)

53. Q. Can you connect to the Filter Service on a V10000 with the ConsoleClient command?

A. Yes, but you need to enable\open the Troubleshooting ports. This is done within the Appliance Manager.

54. Q. When would you use Logon Agent instead of Dc Agent?

A. Most commonly used for identifying wireless users who move between access points. However, it can always used in conjunction with DC Agent.

55. Q. How often does DC Agent contact my list of Domain Controllers? Can this be configured?

A. Every 10 seconds by default. This is because the life of a logon net session is short and we want to ensure that the DC Agent does not miss it. Yes, although it is NOT recommended.

56. Q. What ports does DC Agent use to communicate with my Domain Controllers?

A. You will also see communication over TCP ports 139 and 445

57. Q. If I log off my workstation and another user log on to the same workstation after me, what happens to my user map?

- A. A new user map is created for the workstation IP along with the new user's name. The previous user map is overwritten.

58. Q. My DC Agent user map is set to timeout at the default 24 hrs. However, I stay logged on for days and my user map is still present and updated. Why is this?

- A. If you have computer (workstation) polling enabled, it will update your user map every 15 min, even though the DC Agent identified you initially when you logged on to the workstation the last time. Also if you access any network resources such as a network share this also requires authentication to a domain controller which in turn creates another logon session that the DC Agent will "pickup," which results in creating another user map entry with a NEW 24 hr timeout/time-to-live value.

59. Q. I have installed DC Agent on Windows Server 2008 and the service is not starting, what am I missing?

- A. You need to make sure that the Computer Browser service is up and running on the Active Directory machine. Furthermore, the Windows Firewall **MUST** be turned off in order for the Computer Browser service to start. See the article: [Installing User Service, DC Agent, or Logon Agent on Windows Server 2008](#)

60. Q. With DC Agent configure to poll my Domain Controllers every 10 seconds, how much data is transferred?

- A. Yes, the DC Agent uses TCP (Transmission Control Protocol) to transmit data. The user data that DC Agent sends to other Websense software components equals roughly 80 bytes per user name/IP address pair. On average, DC Agent uses 2.5 MB of RAM on the server it is installed, but this varies by number of logon sessions per network domain controller. The following table shows average quantities of data transferred per day, by network size:

Number of users	Data transmitted
250	30 KB
2000	240 KB
10,000+	1200 KB+

See this article for details: [How Much Data Is Transferred Per Day By DC Agent?](#)

61. Q. I have multiple Websense Servers and each has its own Policy Server, Filtering Service, User Service, and DC Agent. In Websense Manager, I have configured each Policy Server to point to each available DC Agent on my other servers. Will each Filtering Service be able to pull user maps from DC Agents running on my other Websense Servers?

- A. Yes, each Filtering Service can pull user maps from each DC Agent. However, the DC Agent **MUST** be properly configured and successfully generating user map entries. Even though they are registered to separate Policy Servers, the Filtering Service will still be able to pull user maps from a DC Agent. See this article for further details: [Usermap Failover With Multiple Filtering Services And DC Agents](#)

- 62. Q. I have Computer Polling and DC Polling enabled for DC Agent. Which user map takes precedence?**
- A. When Computer Polling and DC Polling entries exist in the user map for the same IP address, then Computer (Workstation) Polling takes precedence over DC Polling.
- 63. Q. Which takes precedence, DC Agent or Logon Agent?**
- A. Logon Agent
- 64. Q. In the User Identification page, can both domain controller polling and computer polling be checked? What is the best practice?**
- A. Yes, so long as you are using a domain administrator account for the DC Agent service to run with, they can both be enabled, and this is the default setting. The domain administrator account is required for computer polling to access the registry on the end user's workstation.
- 65. Q. Will the computer polling feature show Agent type:WKSPOLLING in the XID? Could this also account for incorrect assignments? Licenses?**
- A. Answer: Yes, when workstation (computer) polling is enabled, the Agent type listed within a Transparent Identification (XID) user map will show as WKSPOLLING.
 - B. Answer: Yes, this could account for incorrect Policy/Filtering assignments.
 - C. Answer: No, this will not affect licensing, as Websense calculates a license as any unique IP address seen by the Filtering Service. Now, if you are switching from wired to wireless, it could affect licensing as you are now assigned a different (new) IP address. When you disconnect from the wired (LAN), you pick up a wireless IP which will be counted as an additional license since it is a new unique IP address.
- 66. Q. Is the recommendation to disable computer polling because there are problems with it?**
- A. If the DC Agent is not running with a domain administrator account, then yes you should disable computer polling as it may affect the Policy/Filtering for your end-users. Without admin privileges, computer polling may incorrectly insert a blank entry for the user name.
- 67. Q. Can we enable computer polling?**
- A. Yes, the default setting has computer polling enabled. It is only disabled if someone physically disables it by unchecking the check box within the Triton – Web Security (Websense Manager).
- 68. Q. What is the benefit of computer polling?**
- A. If you have users that do not log off/on daily (i.e. lock workstation), computer polling will query the end-user(s) computer registry, by default every 15 minutes, to identify the user logged in, in order to provide the correct Policy/Filtering/Reporting.
- 69. Q. Do you recommend enabling Computer Polling? I see it was not checked in the settings on that box.**
- A. Computer polling is enabled by default. If it is unchecked, either the Websense Administrator or Websense Technical Support disabled it due to an issue with incorrect identification of users which caused incorrect Policy/Filtering/Reporting.

- 70. Q. When is computer polling used, and how does manual authentication prompt the user?**
- A. Computer (workstation) polling is enabled by default when Websense is installed. When Manual Authentication is enabled, users who are not identified transparently are prompt for authentication. The Filtering Service forces your directory service to prompt the end-user to enter their username/password before proceeding.
- 71. Q. Does computer polling allow the user map to remain accurate when users are locking computers, not logging off, as the presenter described?**
- A. Yes, so long as you are using a true domain admin for the DC Agent to run with, it should be able to pull the correct user even for those who lock their workstations. However, it could take up to 15 min before they are identified, if the DC Agent timeout occurred.
- 72. Q. What are the consequences when DC Agent runs without domain admin rights?**
- A. Without proper domain admin rights, users may not be properly identified transparently or identified as a blank user name. This results in incorrect filtering/reporting.
- 73. Q. Does DC Agent need domain admin settings to run correctly, or can it use a lower security account?**
- A. Per our deployment guide, Websense requires domain admin privileges in order to work properly.
- 74. Q. Does the DC Agent support users across domain trusts?**
- A. Yes. If not trusted, then the domain administrator account used for DC Agent must reside in each domain with the same password, or an enterprise domain administrator account must be assigned to DC Agent.
- 75. Q. Can you elaborate on what DC Agent does that requires Admin privileges?**
- A. There are many things that DC Agent does; specifically it looks for net sessions on your domain controller. This allows transparently identifying your Active Directory (AD) users to apply proper filtering and logging of activity. Furthermore, in AD infrastructures with elevated security levels a Domain User or read-only LDAP user will not suffice.
- 76. Q. How about when I have two domains?**
- A. If the domains are trusted, then the DC Agent should be able to pull users from both domains. If not trusted, then the domain administrator account used for DC Agent must reside in each domain with the same password, or an enterprise domain administrator account must be assigned to DC Agent.
- 77. Q. Can the DC agent be run on the V5000 appliance? If so does it need domain admin credentials to run properly?**
- A. The DC Agent cannot be installed on any V-Series appliance. It **MUST** be on a Windows operating system. It is NOT supported on a Linux operating system.
- 78. Q. Discover interval is in seconds not minutes right?**
- A. Yes, the DiscoverInterval parameter within the transid.ini is in seconds. The value 86400 calculates to 24 hrs.

79. Q. In the v5k, would it use the second DC Agent listed if the first one is unavailable?

- A. Yes. But it does not matter if you are running web filtering on an appliance or on a server. If you have multiple DC Agents and they are both monitoring the same domain controllers listed in the dc_config.txt file, then they will both identify the same users. This is a redundancy scenario.

80. Q. How long it will take to get reflect in Websense or dc agent, if we remove a user id from one sec group to another sec group?

- A. By default, the User Service does lookups every 3 hours. Thus, it could take up to 3 hours to apply the correct policy for a user that has been moved to another AD Group or OU. Moving users within your AD does not affect DC Agent. DC Agent has the end user IP address and User name. This does not change when you are moving users within AD structure. Open TRITON – Web Security manager and press save to have your group changes updated within Websense. In v7.6, a button for updated user\grouping info is available within the management interface.

81. Q. Timeout, the session reverts to default? Not re-auth?

- A. Correct, if the user has not re-authenticated by the time the DC Agent timeout occurs, the user name is removed from the map and the user identified by IP only. You can, as a backup, configure manual authentication should the transparent identification fail.

82. Q. If I add a new DC do I have to load an agent on it or will Websense discovery it?

- A. As long as you have not disabled the DiscoverInterval parameter within the transid.ini, the DC Agent should discover it and add it to the dc_config.txt. However, domain discovery is performed once a day at midnight or upon DC Agent service restart. Potentially, a partial day may pass before DC Agent learns of the new DC.

83. Q. We have over 50 domain controllers. Do we need to include every one of them in dc_config.txt?

- A. Websense recommends a DC Agent for every 10-15 domain controllers. Therefore, we recommend deploying 5 or more DC Agents, and configuring each DC Agent's dc_config.txt to only monitor those 10-15 domain controllers.

84. Q. What would be a reason to turn some of those domain controllers to OFF in the dc_config.txt file?

- A. If you have multiple DC Agents deployed throughout your network, it is somewhat easier to identify and troubleshoot which DC Agent(s) are having an issue when one presents itself. Furthermore, if a domain controller is set to =off the DC Agent will not identify those users from those domain controllers.

85. Q. Are there any benefits to reducing the "user entry timeout" value to something lower than 24 hours?

- A. No

86. Q. If I have multiple DCs in my environment, do I have to set them all up in Websense or can I point to just 1.

- A. The dc_config.txt should be populated with your list of domain controllers during installation. However, if it should fail, you can manually create the dc_config.txt with the

list of domain controller(s) you wish the DC Agent to transparently identify your user-base. DC Agent only needs to monitor the domain controllers that user, who you want filtered by Websense, will be logging into.

87. Q. Why would you need more than 1 dc agent?

A. For fault tolerance, or if you have more than 10-15 domain controllers in your environment.

88. Q. Can I add a second DC Agent on another server for redundancy for transparent authentication?

A. Absolutely, it is also recommended.

89. Q. Do I need to add all of my DCs in the /Settings/Directory Services/Global Catalog Servers list?

A. No. Only one Global Catalog Server (GCS) is entered per domain. See my prior Webinar for details: [Configuring Websense v.7 with Your Directory Service](#)

90. Q. When running ConsoleClient I get a Server Timeout Occurred error.

A. This could be due to either an incorrect parameter being set, the service not running, or a port not open.

91. Q. How does the user entry timeout work?

A. By default, the user entry timeout is 24 hours. Yet within a ConsoleClient PrintSelf you may find that the timeout is anywhere from 24-30 hours from the time the user was identified transparently. This is by design, so that not all of your users are timing out at the exact same time. With that being said, if a user has not re-authenticated (i.e. logged off / logged on) since the last time the DC Agent identified the user, then all the Filtering Service will see in its request is an IP and no user name, thus causing incorrect policies being applied and logging will no longer show user names, only IP will be seen.

92. Q. Sometimes DC agents needs to be restart it if the network agent gets reboot it. Why it happens?

A. This should not be the case. However, if you have configured dependencies for Websense services, which Websense does NOT recommend, that may explain this behavior. Additionally, check if a hotfix is available for the DC Agent.

93. Q. Can you turn off some DCs in the DC_config.txt file? we have a large flat domain with multiple controllers, not all need to be accessed.

A. Yes. Do not remove the entries as they will re-appear with a =on status. Simply set the DCs to =off.

94. Q. Does starting that "TestLogServer" actually STOP logging to the database then?

A. No, logging to the database is not stopped by starting TestLogServer. In order to run the TestLogServer utility on the same server where the LogServer is installed, then the Log Server needs to be stopped as they utilize the same port. TestLogServer could also be called FakeLogServer where it is mimicking the behavior of LogServer. There is a knowledge base article (KBA) that indicates how you can forward traffic to another port without stopping the Log Server service. This allows for not losing logging data. [Click](#)

here.

95. Q. For multiple policy servers, does each one need its own dc agent ?

- A. Ideally, it is recommended, but you can have multiple Policy Servers using the same DC Agent, so long as you have added the DC Agent within User Identification section of the Manager for those Policy Servers. This entry is where each Filtering Service associated with the policy server learns the location of DC Agent that it needs to poll to get the user map.

96. Q. Does it matter which domain controllers are listed first, second, third in the dc_config.txt?

- A. No, the DCs on the list are continually in a round-robin fashion.

97. Q. Can DC Agent and eDirectory agent be used simultaneously?

- A. Not on the same server. Each agent requires each own Policy Server and User Service so you can configure their unique Directory Service (per Policy Server).

98. Q. How come dc_config.txt needs to be manually configured many times?

- A. This is because either the UserService failed the domain discovery during installation or a proper domain admin username and password was not used, or permission was not sufficient to create and write to the file.

99. Q. Can I get a list of hotfix just mentioned about user authentication issue?

- A. All hotfixes are located on <http://www.mywebsense.com>.

100. Q. Does the DC Agent need to be installed on the Policy Server?

- A. No, but typically most customers choose to install it there.

101. Q. When domain default with user 1 or defined user is logged into the network and is being filtered by a policy, a service starts up on that user's machine. The service assumes the user in order to contact the domain controller and causes filtering issues in my config. This can be fixed by ignoring particular "names" under that user, correct? Is it that simple?

- A. Yes. A service will starting up before a user logs on to the domain can cause an incorrect policy to be applied. Run a DC Agent or Filtering Service PrintSelf to identify the service account identified. Add that service account, as displayed in the PrintSelf output, into the ignore.txt file, then delete the XidDcAgent.bak file and restart DC Agent service. This clears the user map and resolves this issue.

102. Q. Is there the ability to exclude all users base on the container OU that they exist in?

- A. No.