Webinar: Identifying Users with Logon Agent: Implementation and Troubleshooting

May Webinar Question/Answer

Q 1: Why would I need the Logon Agent if I have the DC Agent configured correctly?

A: If you have clients using shared workstations. Upon log on, the DC Agent may not "immediately" pick up the user name whereas Logon Agent will pick up the user name immediately. DC Agent authentication accuracy is good to very good, whereas Logon Agent is very good to excellent.

Q 2: Are we going to talk about NTLM?

A: We will briefly discuss configuring NTLM with Logon Agent. Yet, if you are looking for specific directory service NTLM authentication configuration information, it is not covered in this presentation.

Q 3: What is the advantage of using Logon Agent?

A: Logon Agent maximizes accuracy. This is achieved by identifying users as they log on to the network. In contrast DC Agent identifies users by querying domain controllers continuously in a round-robin fashion for passive logon session information. Logon Agent identifies users in real-time as they log on to the domain. This eliminates the possibility of missing users logon due to a query timing issue.

Q 4: How is logon agent different from DC agent? Which is better if we want to provide transparent authentication for our users?

Logon Agent maximizes accuracy. This is achieved by actively identifying users as they actually log on to the network. In contrast, DC Agent passively identifies users by querying domain controllers continuously in a round-robin fashion for logon session information. As Logon Agent identifies users in real-time as they log on to the domain, this eliminates the possibility of missing a user's logon due to a query timing issue. DC Agent and Logon Agent can be used concurrently. The name provided by Logon Agent takes precedence over names supplied by DC Agent.

Q 5: How does Logon Agent work if a user logs into several different desktops/servers at the same time?

A: I assume that you are referring to users being logged on to multiple desktops/servers with the same user name. If this is the case, Logon Agent will identify the user on ALL desktops/servers.

Q 6: Is it necessary to put the /LOGOUT parameter at the end of the line in the logoff.bat?

A: Yes, the /LOGOUT parameter is required in the logout script.

Q 7: Please explain when the /LOGOUT is used?

A: It is used to increase accuracy. Removing a user name from the Logon Agent user map reduces the likely hood of logging traffic under an incorrect user name.

Q 8: Is the Logon Agent more accurate in identifying users than the network agent?

A: Network Agent is a sniffer for protocol traffic--it does not identify users. Did you mean to ask if Logon Agent is more accurate than DC Agent? If so, then the answer is "yes."

Q 9: Will there be or is there currently a similar webinar in regard to DC Agent?

A: Yes there is a recent Webinar on DC Agent. If you look at the archived Webinars, you will find one for DC Agent. Look for the Webinar titled: Exploring DC Agent in Depth (February 16, 2011 Webinar)

Q 10: What if a user logs on to the wired network in the morning getting one IP, and later on in the day goes wireless getting another IP—no logon or log off. Will that cause an issue as no logon is performed when going wireless?

A: Picking up a new IP address is detected when using the /DHCP switch while running the Logon Application in persistent mode. When an IP change is detected, Logon Application (LogonApp.exe) updates the user/ip pairing with Logon Agent service.

Q 11: What if WINS is not available?

A: You do not need WINS to use Logon Agent. It is only for those that use WINS does it need to be configured. Yet some customers still use it. Thus, we identify it to alert them how to identify their WINS server.

Q 12: Is LogonApp and Logon Agent required with a V-Series appliance? Using only AD (Native).

A: If you want to filter users by Groups or User directory objects and also run reports to display user names, then you must identify users in your network. Logon Agent is just one of the available user identification methods. As an identification agent, it is the most accurate method to identify users. You may also use DC Agent concurrently if you chose. If you are running the Websense V-Series proxy, then you have additional user identification options available.

Q 13: I missed some of the presentation - where is the /DHCP switch used?

A: That is okay, this presentation will be available to view again from the beginning. It will be under the archived Webinars. The /DHCP switch is used in the logon script when running LogonApp.exe (Logon Application) in persistent mode.

Q 14: What if there is a service account running a task during a session while the user is still log on? How will Websense Web Security respond?

A: I assume you are referring to experiences with DC Agent picking up service account IDs. Logon Agent is only invoked at log on. Logon Agent identifies actual users as they log on to the domain. It does not pickup service accounts making resource requests. Additionally, when DC Agent and Logon Agent have identified different users, Logon Agent takes precedence over DC Agent.

Q 15: What happens during logon if the LogonApp isn't accessible on the remote share?

A: If Logon Agent is not accessible, then Logon Agent will not work correctly. Additionally, if this occurs, it will not hang the log on process.

Q 16: Would this speed up the authentication process allowing users slightly quicker access when using WS integrated with Cisco Routers for filtering?

A: The integration type and user identification method do not affect Internet access speed. The user identification process will not slow down filtering unless you have manual authentication enabled. It enabled, the user can be prompted for identification if their user name is not found in the Filtering Service user map.

Q 17: How long does it "wait"?

A: If you are asking about the logon process, it is relatively instantaneous and seamless to end-users.

Q 18: In our case where we have only DC agent, it should show whatever DC agent is reporting, correct?

A: Yes, it should. Yet in some cases, where there is a service account running a task, DC Agent may identify an incorrect user. Logon Agent takes precedence and will supply the correct user name. However, if Logon Agent fails to identify a user, DC Agent will then identify the user.

Q 19: Is there a list of parameters (and their uses) available for LogonApp.exe?

A: Yes, a Transparent Identification white paper available and list available parameters.

Q 20: What about VPN users? i.e. We use Cisco AnyConnect. Users log into their laptops using cached credentials. They browse to the URL and are authenticated using AD. Will this log in show up with the Logon Application?

A: Yes, they should be identified.

Q 21: What if you don't have a WINS server enabled?

A: You do not have to have WINS enabled. It's only mentioned for those that do.

Q 22: Can I implement V-Series without any agents (e.g., DC Agent, Logon Agent). Since I am using IWA, I thought that no agents were required.

A: You are correct. If you are using IWA, you do NOT need any agents.

Q 23: We have a central policy server and several distributed enforcement websense 7.0 servers. Do we have to install Logon Agent on the central policy server or ALL the servers?

A: I would recommend ALL servers and force your remote locations to user their local Logon Agent service via separate GPOs. This way your users do not need to transmit user name data across the wire.

Q 24: Will Websense Web Security associates both users on the same IP address?

A: If you are asking if DC Agent and Logon Agent will map users to the same IP address, then the answer is yes. When this occurs, only the user name supplied by Logon Agent is used.

Q 25: Should DC agent be removed after deploying logon agent?

No, removing DC Agent is not necessary. They can be used in tandem.

Q 26: Does Logon Agent only work with Active Directory?

A: Logon Agent works with Windows NT or Active Directory, directory services.

Q 27: After the logoff of the service account, is the IP be given back to the previous account and a license made available again?

A: The IP address is only removed from the Logon Agent user map. Logon Agent does not “free-up” or “use” licenses. Logon Agent has no relationship or contribution for managing or using up licenses.

The Websense Filtering Service determines when a license is used. For each “new” IP address that the Filtering Service encounters, it counts one license used. Licenses are freed up once a day—at midnight.

Q 28: May I install multiple instances of Logon Agent on the same machine?

A: You cannot install multiple instances of Logon Agent on the same machine. However, you can run multiple instances of Logon Agent within your network. Each instance must be installed on a separate Linux or Windows server and be able to communicate with Websense Filtering Service.

Q 29: What is the impact to workstations? CPU and Memory usage on client?

A: The resource impact on the client machine is minimal.

Q 30: I noticed that the \bin directory was under “Websense\Websense Security\” in the demonstration. My \bin directory is directly under “\Websense” directory. Is that just a version difference?

A: Yes, it is just a version difference. Version 7.6.2 was used in the demonstration. Starting in v7.6, the directory structure changed. **“Websense Security”** was added to the path to distinguish the filtering files and folders from the new TRITON management infrastructure.

Q 31: Is a service account with domain admin really necessary? Or is this similar to DC Agent – the domain admin account is not necessary but you receive an error.

A: No, using a domain admin account is typically not necessary. Logon Agent can run as local system. Yet in some cases where a customer’s AD security is raised, Logon Agent may require an admin account.

Q 32: With /COPY switch, is the executable copied down again if it already exists?

A: Yes. This allows you to replace or update the executable with a later version. However, it takes logging into the domain for the executable to be successfully re-downloaded to the client machine. You can add the /COPY in the logoff.bat script to remove the executable when a user logs out.

Q 33: With the persistent Logon Agent, does that free up a license if a user logs off?

A: The IP address is only removed from the Logon Agent user map. Logon Agent does “free-up” or “use” licenses. Logon Agent has no relationship or contribution for managing licenses.

The Websense Filtering Service determines when a License is used. For each “new” IP address encountered, the Filtering Service counts one license used. Licenses are freed up once a day—at midnight.

Q 34: Is this webinar available for download?

A: The recording and Webinar slides will be available on our support webinar page within 24 hours at: http://www.websense.com/content/SupportWebinars.aspx. Answers to all submitted questions will be posted within a week.

Q 35: What is the packet size of Logon Agent per check-in?

A: The exchange is 6 small packets. See the “What does a successful Logon Agent authentication packet capture look like?” article for details.

Q 36: How do we identify users on Mac OS?

Please see this article: How do I use Websense Web Security solutions to authenticate or identify Mac users for user- or group-based filtering?

Q 37: Is the WINS Server option a requirement for the V-Series. Can you provide documentation page or KB reference for additional reading.

A: Please see this article: LogonApp cannot reach the AuthServer in the final attempt

Q 38: Does the user have to be a local admin to use the /COPY command?

A: No. Typically you are not required to use a local admin account with the /COPY command. However, if you are encountering issues getting Logon agent to work, then use a local admin account as one of your troubleshooting steps. If successful, it points you in a direction for resolving the problem.

Q 39: Can the Logon/Logoff information be saved for forensic research?

A: Using Websense logging and tracing options for anything other than short time testing is not supported. If left running long term, the logging files will continue to grow and may exceed available disk space. To monitor your logon/logoff scripts, you need to explore options available in your directory service or use a third party tool.

Q 40: Does logonapp.exe use RPC to communicate with workstations?

A: The LogonApp.exe executes on the client machine and contacts the Logon Agent service. The Logon Agent then makes an NTLM authentication challenge. LogonApp.exe (Logon Application) responds with cached user credentials.

Q 41: What makes up the ID Logon Agent gets from the Domain Controller? Username and host name or username and IP address? Wondering if DNS lookup is done after grabbing ID.

A: The NTLM Authentication Challenge response includes the senders source IP address and user name. If the user name is verified, the IP address/name pair are mapped as presented.

DC Agent does a DNS lookup to resolve machine names to IP addresses. This DNS lookup process is not required when using Logon Agent.

Q 42: Will Logon Agent work on Windows XP clients?

A: Yes.

Q 43: When running Logon Agent with the /NOPERSIST switch, the timeout is 24 hours. How will the user be seen if they have not re-authenticated to the domain?

A: If the end-user has NOT re-authenticated to the domain after 24 hours, then as no user name is present in the user map (for filtering purposes), they will be seen as only an IP address and filtered accordingly.

Q 44: What is the default tcp port for Logon Agent? What about the diagnostic port when troubleshooting Logon Agent issue(s)?

A: The TCP port that the Logon Agent listens on is 30602 by default. The diagnostic port for Logon Agent is 1 port higher (30603).

Q 45: Does Logon Agent support the NTLM v2 response using session security?

A: Using NTLM v2 is supported in Websense v7.6.2, but using NTLM v2 with session security is not supported. Session security does not offer superior security protection.

Q 46: When debugging Logon Agent using the /VERBOSE switch, I have seen Errors in first, second handshake or final attempt. What exactly does that mean?

A: The **first handshake** is the client workstation (Logon Application/LogonAppl.exe) communicating to the Websense server where the Logon Agent (AuthServer.exe) resides.

The **second handshake** is when AuthServer.exe communicates to the domain controller and verifies the user against Active Directory.

The **final handshake** is when the domain controller communicates back to AuthServer.exe.

Q 47: If I add a new client machine to the network, does Logon Agent detect it?

A: The logon script activates the logon application (LogonApp.exe) when a user logs on to the domain. The Logon Application detects the logon session, and then sends that information to Logon Agent.

Q 48: Why does Logon Agent only work for one person in a terminal server environment?

A: With terminal servers, where every virtual sessions gets its own IP addresses, Logon Agent still runs once for the entire machine. This effectively prevents user identification for all other users on the terminal server. The LogonApp.exe process is specifically designed to die if a existing logonApp.exe process is detected.

With regards to properly identifying users in a terminal server environment, Websense recommends using the Websense Content Gateway (WCG) proxy mechanism for transparent identification of terminal server users.