Websense Support Webinar: Questions and Answers

Configuring Websense Web Security v7 with Your Directory Service

Question: Can updating to Native Mode from Active Directory (AD) Mixed Mode affect transparent user identification?

Answer: Transparent identification is not affected by a change to Active Directory (AD) Native Mode. No changes are required for the Websense transparent ID agents. Users continue to be identified as they were previously.

Question: Why do I need to use an admin account for Active Directory? All it should be doing is querying AD, so an admin ID should not be necessary.

Answer: User Service needs to query for client group membership. Some networks require a domain administrator account to accomplish this. Please use the command

NET USER /DOMAIN > U.TXT

or

NET GROUP /DOMAIN > G.TXT

to verify that you are able to see all objects.

Question: Global catalogs contain users from all domains in the forest, so why do we need to add the individual child domains in a multiple-domain Native Active Directory mode?

Answer: Actually, "a global catalog server replicates a full attribute set for all objects in its own domain, but only a partial attribute set for the objects in other domains in the Active Directory tree or forest. For these other domains, the global catalog server contains only information commonly used for search queries. This partial attribute set does NOT include users' Global group membership information."

Question: Can we support multiple, unrelated domains (no parent-child relationship)? What is the performance impact of multiple domains? Are they searched in parallel?

Answer: Create an entry for each domain in Websense Manger. For each domain, identify a domain controller (non-Global Catalog server). Enter an administrator account and Root Context from each domain. In a medium-sized network, performance should not be a concern, because User Service calls are small.

Question: I have two separate domains. Do I need to install Policy Server on two separate machines, one in each domain?

Answer: Websense software may be installed in one domain. Within the Websense Manager Directory Service settings, enter one entry for each domain, and ensure that a valid root context is also included.

Question: How do I filter non-employees using non-domain computers (guests, vendors, and the like) who connect to our network and acquire an IP address via DHCP?

Answer: Users who do not log on are filtered by the Websense Default policy. Websense software can also prompt non-domain users to provide domain credentials by enforcing Manual Authentication (set up within Websense Manger). For these manually prompted users, you can provide general guest domain logon accounts. Alternatively, you can force all users to provide credentials, with the exception of specific IPs. You can assign specific IPs to your non-domain users individually.

Question: How does the Websense server fit in the network? Is it a proxy, span port, pass through, other?

Answer: Websense Web Security is not an *in-line* product. It expects traffic to be sent to it by a proxy or firewall, or a span port. Once it sees traffic, then it filters according to your policies.

Question: Are there any advantages to configuring user authentication with AD Native Mode, as opposed to Mixed Mode?

Answer: Setting Websense software to work with AD Native Mode takes advantage of advances in LDAP that are not available in an NTLM directory service.

Question: I am using Windows 2008 Active Directory. I have DC Agent and Logon Agent set up, but Web filtering is still not working as I expected. Does version 7 support Active Directory 2008?

Answer: For Websense Web Security v7.0, DC Agent is not supported in a Windows 2008 Active Directory environment. To identify users successfully, you need to employ Logon Agent and modify NTLM Security permissions. Windows 2008 AD uses NTLM-2 (version two). Websense transparent agents were designed using NTLM (version one). DC Agent is scheduled to work with Windows 2008 Directory Service in a version of Websense Web Security expected later in 2009.

Question: What is the upgrade path from v6.3 to 7.x regarding user services?

Answer: All prior Directory Service settings are retained. However, the Logon Directory settings are new to v7.0. Configure **Settings > Logon Directory** information, and then add your account to **Main > Delegated Administration** for logging on to Websense Manger.

Question: How do I set up transparent identification to support multiple domains? Can the domains be in separate forests?

Answer: Install a transparent identification agent in each domain. You can confirm that your agent is picking up user names by following KB article 3343. ((http://kb.websense.com/article.asp?article=3343&p=12)

Additionally, if you are using DC Agent, then optimize which domain controllers are polled by following KB article 3602. (http://kb.websense.com/article.asp?article=3602&p=12)

Question: We use eDirectory Agent. Have you made any improvements for that?

Answer: As of 3 February 2009, one hotfix exists for eDirectory Agent in v7.0. This hotfix increases user name accuracy. Please log on to www.mywebsense.com and install the Hotfix.

Question: Can Websense software be configured to support DC Agent first, then LDAP second (if not found by the DC Agent)?

Answer: Transparent identification and adding LDAP objects into Websense Manger are linked. If transparent identification works successfully, then you will see correct filtering for LDAP objects added to Websense Manger. Conversely, if transparent identification fails to identify users, then filtering will not occur as expected for LDAP objects added to the Manager.

When all is set up correctly, you have the following filtering hierarchy:

1. User Names
2. Computer IP
3. Network IP Range
4. Groups
5. OUs
6. Domains
7. Websense Default Policy

When the user is not identified, then you have the following filtering hierarchy:

1. Computer IP
2. Network IP Range
3. Websense Default Policy

Question: Why is the root context optional?

Answer: If you are entering data for a single domain, then the root context is optional, because User Service will discover the domain. However, in a large network with thousands of directory objects, then you may see a warning returned in the Websense Manager interface, indicating that a wait time is required to show directory objects. In a large domain, entering a root context helps user service display user objects more quickly, because the starting point of the query is defined by the root context.

Question: Is Websense Web Filter supported on ESX or Hyper-V, or do you recommend a dedicated server?

Answer: Depending on the size of your network, you may need additional servers. Small networks may user a single server. Please review the Websense Deployment Guide for specifics for your network. Operating systems not listed in that guide are not supported.

Question: Do you need to install and run User Service to browse Active Directory in Native Mode?

Answer: Yes, and more specifically, installing User Service is required for browsing any supported directory service.

Question: You mentioned that User Service needs domain permissions to browse the domain. Does DC Agent need these permissions also?

Answer: The administrator account assigned within Websense Manger for Directory Service settings is independent of DC Agent. In most situations, DC Agent requires domain admin permissions to perform Workstation Polling. Workstation Polling is the second method by which DC Agent identifies users. This feature reads the Windows Logon registry key to confirm logon credentials. If the logon key is blank, DC Agent grabs the workstation SID and then does a reverse lookup against a Domain Controller. These steps require administrator rights.

Question: In Websense Enterprise v6.3.2, there are 3 files that have all your settings for backup. Is this the same case for 7.0?

Answer: Websense Web Security v7 includes a new backup feature. For details, select Help within Websense Manger and search for the topic, *backup*.

Question: We currently have Websense software running on an Active Directory server. Is there a problem with version 7 and transparent user identification?

Answer: Transparent identification in v7 works the same as you experienced in earlier versions.

Question: Does this software run on an appliance or Windows server? Pass through or proxy? How is it implemented?

Answer: Please review the Websense Deployment Guide and Websense Installation guides for details.

Question: Where do you recommend installing the DC Agent? Should DC Agent be installed on the Websense Policy Server computer or on a domain controller?

Answer: DC Agent requires a server-based operating system. It can be installed on a domain controller, but is typically installed on the computer that houses Websense Filtering Server. Please review the Websense Deployment Guide and Websense Installation guides for details.

Question: Does DC Agent need to be running with a domain admin account in Windows NT Mixed Mode?

Answer: The DC Agent service requires a domain admin account when it runs in either Native or Mixed Mode.

Question: Is it necessary join the Websense server to the domain?

Answer: To perform queries, the server where User Service is installed must be a domain member. Other Websense services may be installed on non-member servers.

Question: Will Websense Explorer logons show in the audit log in v7?

Answer: Yes, if you create a role for users who log on to Websense Manager only to run reports, the audit log shows logons for these limited users.

Question: In our current Websense software v6.3.2, when a user is logging into a Citrix Server via remote session, Websense software shows only the last person logged into the Citrix server, which is "Administrator" instead of user name. Does version 7.0 fix this problem?

Answer: In v6.3.2 as well as v7.0, Websense software can identify Citrix users if the version of Citrix is supported by Websense. Essentially, Websense software installs a plug-in on each Citrix server to send user names to Websense components. Please review the Websense installation guide for use with Citrix products for details.

Question: Why do you need to keep IP addresses to monitor to a minimum? What are the issues that could be experienced if there are many IP addresses or IP ranges added?

Answer: You can enter many individual IP addresses in Websense Manger without experiencing problems, but we don't recommend it. What you would lose is the ease of applying Websense filtering policies to group objects added to the Manger. Also, you would need to track individual IP addresses and ensure that they do not change (are static). In a very small network, this is manageable. In a medium-sized company, managing everyone by IP address can be overwhelming. Managing by groups simplifies your job as the Websense administrator.

Question: Is there a way to apply policies to groups that are applied to computers (instead of to users)? Some of our policies are based on locations on campus, rather than on who is using the devices. I know I could apply settings to each IP address, but that is a bit cumbersome, and DHCP adds a lot of overhead for that sort of configuration.

Answer: Websense software cannot apply policies to computer names. Regarding the overhead of managing DHCP, you need to ensure everyone logs on to the network. If you find users are logging on locally, you can stop that by setting the Default policy to block all access. With the Default policy set this way, users need to log on and be identified to access the Internet.

Question: What about correct identification through VPN?

Answer: Please review the installation documentation for identifying users using the Websense RADIUS agent.

Question: Can Transparent User Identification be set up to work with Terminal Services?

Answer: Depending on the remote terminal application you are using, one of two situations can occur.

- The user using the terminal application is identified correctly.
- The user using the terminal application is not identified correctly.

You can determine if Websense software picked up your user by examining the view source info hidden on the block page. For details: http://kb.websense.com/article.asp?article=3192&p=12

Question: Can Websense software take advantage of nested groups in Native Mode?

Answer: Please review the Websense KB article titled *Active Directory group-based policies with multiple domains and/or nested group* for details. http://kb.websense.com/article.asp?article=2912&p=12

Question: If we have multiple domains, do we need a User Service running for each domain?

Answer: This webinar provides an example of a multiple-domain configuration using a single User Service.

Question: What are the minimum privileges required? A service account as Domain Admin is not an option.

Answer: This depends on the network. At times, a simple domain user account is sufficient. However, most installations require increased privileges. Test using the NET USER /DOMAIN and NET GROUP /DOMAIN commands as shown in the webinar, to ensure that all objects are displayed.

Question: If you are in AD Mixed Mode because of defaulting to that, how do you switch to Native Mode?

Answer: This is a frequently-asked question and is covered in detail in this webinar. Please review the Native Mode setup section.

Question: So is Websense filtering at v7.x any different from v6.x, where network-based (IP-based) policies had priority over user /group-based policies?

Answer: The logical hierarchy for applying policies in v6.x and v7.x is identical:

1. User Names
2. Computer IP
3. Network IP Range
4. Groups
5. OUs
6. Domains
7. Websense Default Policy

Question: Can you configure an LDAP connection to a trusted domain?

Answer: Yes, trusted domains are supported.

Question: Do you have to recreate your catalog DB in SQL when you switch from Mixed Mode to Native Mode?

Answer: No. Creating a new database partition after switching to Native Mode is not required. Note that the day you switch to Native Mode, the user names in your reports display differently.

Question: Does Websense software work with Active Directory in real-time and pick up group changes in AD as soon as they occur?

Answer: No. Depending on your network AD replication, it may take Websense software up to three hours to be fully aware that you have moved a user to a new group. If you need Websense software to be aware of a change in your directory service immediately, restart Websense User Service.

Question: If we have Websense Enterprise version 6.3, and a maintenance contract, is version 7.0 a free upgrade?

Answer: If you have a third party supporting your Websense installation, check with that provider for technical support. However, upgrading Websense Web Filter is available to all customers with valid subscription keys. Websense does not charge for the new version. A valid key ensures that you can use the latest release.

Question: Can we exclude servers from our Websense subscription?

Answer: Yes. Ensure that the Websense Filtering Service does not see traffic from any servers you want excluded from your subscription. Recall that every unique IP address that Websense Filtering Service encounters counts toward your subscription limit. This count is reset to zero nightly.

Question: Is there a way that I can transfer my SurfControl database into Websense software?

Answer: The database schemas are not compatible. Please review the KB article titled: *v7: SurfControl Web Filter to Websense Web Security Transition Kit* http://kb.websense.com/article.asp?article=3743&p=12

Question: Do active directory groups have to be Universal for filtering? Can local groups be used?

Answer: Websense can filter Global groups; however, you may find situations where your groups must be Universal Security groups for proper filtering. For details, please review KB article 2912. http://kb.websense.com/article.asp?article=2912&p=12

Question: I have 3 domains with 2-way trusts and no parent domain. Do I still configure User Service in the same way that you configured it for the multiple-domain model in this webinar?

Answer: Insert an entry for each domain within Websense Manger, along with specific root context, and admin accounts. However, use port 389 for all domains.

Question: If I am using eDirectory service, is it necessary to identify all replica servers?

Answer: Yes, all replicas need to be identified within Websense Manger.

Question: Where can I find DC Agent and Logon Agent?

Answer: If these services are not installed, simply run the v7 installer and choose Add Filtering Components. If they are already installed in your network, then they are listed in Websense Manger. Select Settings > User Identification to view the location of all installed transparent identification agents.

Question: Is it the case that Websense software cannot manage clients by hostname?

Answer: Correct. Websense software does not filter by computer names.

Question: What causes my reports to show only IP address for some users, but also show some specific user names?

Answer: Websense software is unable to identify all users, or some users may be logging in locally. Check to ensure that your identification agents are working properly.

Question: I know this session covers v7, but I am using v6.3 and have a question. Where would I look to troubleshoot intermittent failure of the DC Agent or User Service? Intermittently, our users are not filtered by their custom policy but instead fall into the Default policy. Once we restart the DC Agent service and User Service, the filtering policy works again.

Answer: For the users who are filtered incorrectly, look at the hidden info on the block page. (http://kb.websense.com/article.asp?article=2540&p=12) You will notice either an unexpected name or no user name at all. If you see a service account showing up, you can set DC Agent to ignore it by following KB article 3351. (http://kb.websense.com/al/12/1/article.asp?aid=3351&n=4&tab=search&bt=4&r=0.5564341&s=1&searchstring=ignore.txt#1)

Depending on your network environment, the DC Agent Workstation Polling feature may be picking up incorrect user names. Try disabling Workstation Polling. Examining the user names mapped by DC Agent can also be helpful to identify problems. Follow article 3343 see the users' names collected by DC Agent. (http://kb.websense.com/article.asp?article=3343&p=12)

Question: One the biggest problems I have is that users seem to "lose" their permissions. Which is better: NTLM or LDAP? I'm currently using NTLM.

Answer: This issue is independent of the Directory Service. Users should not be losing their permissions. Please view the hidden information on the block page to determine if Websense software has identified the user correctly (http://kb.websense.com/article.asp?article=3192&p=12). Review the previous question for troubleshooting user identification.

Question: Can I add users to the groups in AD to add them to policies?

Answer: Yes. After group objects have been added to Websense Manger, and a filtering policy has been applied, then users in your network who are in the groups are filtered by the corresponding policy.

Question: Are there any special requirements for upgrading from v6.3.2 to v7.0.1?

Answer: v7 requires additional server resources, and a new reporting database is created. Please review the v7 deployment and installation guides available on the Websense Support Web site.

Question: What happens if a user is in two groups in AD?

Answer: By default, the least restrictive group policy applies. You can change this setting in Websense Manger. Select Settings > User Identification. Note the setting for the option "Use most restrictive group policy."

Question: Can we upgrade to v7 from v6 with ease?

Answer: Yes. Websense Enterprise v6.x.x can be upgraded to v7. Direct (one-hop) upgrades are supported for v6.2 and higher. Versions 5.5.x and 6.1.x require two hops for upgrade. Please review the KB article titled *v7: Upgrading to v7 from previous versions of Websense Enterprise.* http://kb.websense.com/article.asp?article=3690&p=12

Question: Is DC Agent required to authenticate users?

Answer: If you enable manual authentication in Websense Manger, then DC Agent is not required. However, a Websense transparent identification agent (such as DC Agent) is required to identify users, if manual authentication is not enabled.

Question: Do DC Agent and Logon Agent both need to be deployed?

Answer: No. You may deploy either agent individually. They may also be used together. Typically, only DC Agent is deployed in the network. It's easy to install and requires only an administrator account. Logon Agent requires a small logon script. Of the two agents, Logon Agent has precedence over DC Agent when user names are collected.

Question: Is there an easy way to deploy the agent to end-user computers?

Answer: If Logon Agent is enabled to run in *persist* mode, it is deployed to each machine and remains running after users log on to the network.

Question: Is port 389 used in Websense Enterprise version 6.3?

Answer: The example in this webinar for configuring Directory Service v7.0 within Websense Manger is the same for earlier versions.

Question: How are cached credentials handled with regard to identifying the users?

Answer: Cached credentials are used when users are manually authenticated. As long as the end user maintains active and does not close the browser, the user is not prompted for authentication. If the user opens and closes browsers, then the user is prompted every ten minutes by default.

Question: What are the differences between v6.3.2 and v7.0 on the setup of User Identification?

Answer: With the exception of the new Websense Manager interface and the Logging settings, the configuration of Directory Services remains the same.

Question: We need to use manual authentication and want to use the agent also; can the manual auth be set as the default, and exceptions handled by the agent?

Answer: Manual authentication is applied globally. Please see the Help topic on this feature within Websense Manger for details.

Question: Does Websense Web Security provide MAC address filtering?

Answer: No. MAC address filtering is not supported.

Question: Is anything else required (such as LOGON batch files), to transparently identify all Active Directory users?

Answer: If users are forced to log on to the network (not allowed to log on locally), then Websense software should be identifying all of your users.

Question: Can Websense software use both Active Directory and eDirectory simultaneously?

Answer: Websense software can be configured with only one directory service.

Question: If I want the bind account to use SSL, what port do I have to use?

Answer: Port 636 is used when you enable SSL (for secure directory server binds).

Question: Can you explain how Websense software displays users' names?

Answer: User names are seen as the whole WinNT name, or the full canonical LDAP name, not just as the logon name or display name. This is why you must delete and re-add objects in the Clients section after you upgrade to Active Directory Native mode.