Websense Support Webinar: Questions and Answers

Working with Directory Services
Websense Enterprise™ Version 6.3.x

Question: Does the Websense User Service account need Domain Administrator rights?

Answer: Websense User Service can use a Domain User account to pull directory objects under most circumstances. However, if the Domain User account does not pull the directory objects as expected, then it may be necessary to use Domain Administrator account rights. See Websense KB 980 for additional information.

Question: Do I need User Service if I'm integrated with Microsoft ISA Server 2006?

Answer: User Service will still be required. However, transparent identification agents, such as DC Agent and Logon Agent, will not be required if ISA Server is set up for authentication.

Question: What port needs to be enabled again?

Answer: Default ports: 3268 (GCS), 389 LDAP, 3269 (LDAP over SSL for AD), 636 (LDAP over SSL for Novell).

Question: To configure Active Directory (AD) native mode, must User Service be configured as local account?

Answer: When running in Active Directory native mode, you can use a local system account as the domain credentials for User Service. Enter these credentials in the Directory Service settings of Websense Manager.

Question: How can I adjust how often the User Service communicates with the directory service to less than 3 hours?

Answer: The default setting is 3 hours. While this can be modified in the websense.ini parameters, it is *not* recommended. Please contact Websense Technical Services for details.

Question: After Active Directory services are configured, can Websense be configured to block access if a user is logged in locally on their computer rather than logging into the domain?

Answer: Yes, users can be blocked using a workstation IP or network range client object.

Question: I have 3 Novell servers replicating services. Does it matter which of the 3 servers I choose to connect to eDirectory?

Answer: It should not matter, as long as at least 1 server has the directory structure.

Question: I have Novell eDirectory in a K-12 environment. What is the best practice for configuring Websense to best detect student user logins since they log in and log out throughout the day?

Answer: Deploy the eDirectory Agent.

Question: Do you need to configure Windows mixed mode if your hierarchy contains Windows 2000 Domain Controllers (DCs)? If all DCs were Windows Server 2003, then it would be native mode, correct?

Answer: When running Windows 2000 in mixed mode, select mixed mode in the Directory Service settings in Websense Manager. However, if all DCs are Windows 2000 running in native mode or Windows Server 2003, select Active Directory native mode in the Directory Service settings.

Question: When using SSL, do you need to make any other changes?

Answer: Install SSL certificates and keys as required by your environment. Certificates and keys must be in a location where Websense software can access (please contact your Directory Service vendor for appropriate steps to create an SSL certificate). Ensure your environment also allows the SSL over LDAP port (port 3269 for AD; port 636 for Novell).

Question: Is there any way to configure multiple GC Servers for Websense? That is, what happens if the chosen GC Server goes down or is decommissioned since all objects in Websense integrate the GC Server name into their references?

Answer: The best solution is to create a DNS alias that points to all the GC Servers you want to reference. That way, it will round-robin between them in the event of a failure.

Question: Can you specify which AD group to go and search for when querying AD in native mode? We've had issues with users in a child domain due to users being part of distribution lists in A father domain. Thus, the user was denied internet access since the policy was linked to a group in the child domain.

Answer: Yes, the Root Context option is normally used when dealing with multiple child domains. If this field is left blank, Websense software begins searching at the top level of the Directory Service.

Question: So if the machine is already logged in as Admin, the services should be ok with it being a local system login?

Answer: In Windows Services, Websense User Service still needs to be configured to run under a Domain Admin account when AD is in mixed mode. However, when AD runs in native mode, User Service can run as a Local System account because the domain credentials will be configured in the Directory Service settings of Websense Manager.

Question: Are Websense Manager and User Service compatible with Windows Server 2008?

Answer: Windows Server 2008 is note supported at this time.

Question: If we don't install DC Agent or Logon Agent, can we still apply policies to users, groups, and OUs?

Answer: DC Agent and/or Logon Agent are not required if you've opted to use manual authentication or a proxy such as Microsoft ISA Server with authentication enabled.

Question: I have Websense with a Check Point firewall, and would like to identify users who are in a certain AD global group. Directory Service configuration has been set up along with installing the DC Agent. How will the flow for transparent identification be seen by each end user?

Answer: Users will not notice any difference.

Question: Can you switch between AD mixed mode and AD native mode in Websense Manager without any side affects? Will existing rules remain intact?

Answer: After switching to AD native mode, all directory objects in Websense Manager will need to re-added, because directory objects in Websense Manager are associated with the configured directory service.

Question: How do you configure the directory services for Apple MACs?

Answer: Apple MAC directory services are not supported.

Question: How do I manage or apply policy to the groups in AD mixed mode?

Answer: Add the groups as directory objects in Websense Manager. Then, apply the appropriate policy.

Question: If your Websense machine is located in a DMZ, will it have to be moved out of the DMZ and into the LAN for LDAP to work?

Answer: Websense components are not recommended for deployment in a DMZ, with the exception of Remote Filtering Server.

Question: What happens when a client is a member of two groups, and different policies are applied to these two groups? Which one takes precedence?

Answer: By default, Websense will apply the least restrictive policy unless the option for more restrictive blocking is enabled in the Websense Manager Settings.

Question: Will changing an AD group name break filtering until the cache updates (3 hours)?

Answer: If renaming a group in AD, you must add the new group directory object in Websense Manager.

Question: Can we add groups, rather than individual users, to Websense Manager, when AD is configured to run in mixed mode,?

Answer: Yes, group directory objects can be added in Websense Manager when AD is configured to run in mixed mode.

Question: For the forest root global catalog setting, is there a specific FSMO role the server needs to hold, or can it be any Global Catalog Server?

Answer: Any Global Catalog Server can be used.

Question: One slide mentioned that it is recommended to have universal security groups. Our groups are global security. Is this a problem?

Answer: In an Active Directory environment that includes multiple domains, Websense software does not always recognize Windows group memberships. This behavior is a Windows feature. Windows Global group membership information is not stored in the Global Catalog for all other domains. Therefore, since the Global Catalog Server is potentially unaware of group membership information outside of its own domain, Websense User Service is also unaware of that information. See Websense KB 1733 for additional information.

Question: Is there a benefit to configuring Active Directory for native mode versus mixed mode?

Answer: Websense software will apply policies more accurately if configured in the correct mode of the organization.

Question: Can you configure the Active Directory native mode settings to see more than 1 Active Directory forest?

Answer: You must add each distinct domain from each forest to the directory services in Websense Manager, and it should work correctly. Also, you need to use port 389 and a root context for each DC. The root context for training.websense.com would be dc=training,dc=websense,dc=com.

Question: Under NetWare, do you have to establish Websense as a trusted application?

Answer: Not required.

Question: When using AD mixed mode or AD native mode, will users who are added to AD be automatically added in Websense Manager?

Answer: Websense communicates directly to the directory service. Directory objects will need to be added in Websense Manager separately if you are planning to apply policies by user or group.

Question: What is needed to do cross-domain user authentication?

Answer: Each domain must be defined in Websense Manager Settings under Directory Services. However, you cannot have the same user name in 2 domains. For example; domain1 has JoeUser and domain2 has JoeUser2. Websense User Service will have problems enumerating similar user names from 2 different domains.

Question: Currently we have a flat network with User Service and DC Agent installed on the same server. When we move to a subnetted environment will we need to install User Service and DC Agent on devices on all subnets?

Answer: User Service and DC Agent will need to be installed on a server with network access to the Directory Service.

Question: Can you have more than one domain in AD native mode? We are migrating.

Answer: Yes multiple domains can be listed using AD native mode.

Question: Is there going to be full support for eDirectory Workstation Objects in Websense software?

Answer: There is no ETA at this time.

Question: With many disparate child domains, does the hook to the GC substantially increase network traffic?

Answer: This causes a minimal increase in traffic.

Question: How does all of this differ if we're using a Resilience (Linux) appliance?

Answer: Websense, Inc., recommends installing User Service on a Windows machine. However, it can be installed on Linux or Solaris if needed.

Question: How does having Apple computers on the network change the configuration of Directory Service?

Answer: Having Apple computers does not affect the way you configure Directory Services in Websense Manager. Directory Services should always be configured to match the Directory Service that is currently running.

Question: Will the users still have Internet access if our Directory Service goes down?

Answer: Users will default to the Global policy configured in Websense Manager.

Question: If the computer names are not being displayed in reports, what and where should the settings be done?

Answer: Identification by workstation name is not currently supported.

Question: AD was just changed to native mode from mixed mode. Will I need to remove my previous NTLM objects and add them again?

Answer: Yes, you will need to add the directory objects in Websense Manager because the native mode objects will be in LDAP.

Question: Is there a tool or log that shows the results returned from the Websense eDirectory query?

Answer: You can use a Websense utility called “consoleclient” to view the eDirectory Agent’s user/IP mappings. Please contact Technical Support for details on running the utility.

Question: How do we require a login prompt before access to Internet?

Answer: Enable manual authentication in Websense Manager.

Question: What is the order of in which Websense handles filtering each request?

Answer: The order of filtering for Websense is as follows: User, IP, Group, and then Global policy.