

Troubleshooting Logging and Reporting Issues for Websense Web Filter v7.x

Websense Support Webinar March 2010

Support Webinars

Goals and Objectives

- Log Server deployment scenarios
- Installing Log Server and other reporting components
- Troubleshooting installation problems
- Presentation and investigative reports
- Troubleshooting Log Server issues
- Troubleshooting presentation and investigative report errors
- Database maintenance best practices



Ravi Desai

- **Title:** Tech Support Specialist
- **Accomplishments:**
 - Over 2.5 years supporting Websense products
- **Education / Certifications:**
 - B.Eng (Hons) Computer Systems and Networks
 - MCP
 - CCNA
 - WCWSA – Websense Certified Web Security Associate
- **Qualifications:**
 - New Hire Training
 - v7 Tech Support Training
- **For additional information:**
www.websense.com/support/

Supported Platform	7.0 – 7.0.1	7.1
Windows Server 2003, Standard and Enterprise	✓ Yes	✓ Yes
Windows Server 2008, 32 bit only		✓ Yes
Red Hat Linux 3, 4, and 5	✓ Yes	✓ Yes

- Install only 1 Log Server per Policy Server.
 - Multiple Log Servers can send logs to a single Log Server instance.
 - Additional Policy Servers are required for more instances of Log Server.
- Log Server is not supported on VMware except for demonstration purposes.
- Microsoft does not support SQL Server or MSDE on VMWare.

- Reporting records are stored in the Log Database.
 - Supported database engines are SQL Server 2005 SP2 or SP3 (recommended), SQL Server 2000 SP4, and MSDE SP4.
 - The Linux version of Log Server can use MySQL 5.0.
 - For large environments, SQL Server is recommended.
 - SQL Express is not supported.
 - One instance of Log Server can log to only one database at a time.
 - SQL clusters are currently not supported.
 - It is possible to have a central database for multiple Log Server instances.

- A distributed logging environment is possible.
 - A central Log Server instance logs data from multiple remote Log Servers
 - Refer to KB 3466 for accurate steps to set up a distributed environment
 - Requires a high speed and reliable WAN link
 - Customers with slower WAN links can use distributed logging, preferably during off-peak hours

- Make sure that Microsoft SQL Server or MSDE is installed before installing Log Server.
- MSDE is not supported on Windows Server 2008.
 - Refer to the Websense Knowledge Base (kb.websense.com) for a download link and further instructions.
- To install just Log Server, select the Custom option during installation, and then select Log Server as the component to install.

- Enter the location of the database engine.
 - Provide machine host name or IP address .
 - If your SQL Server installation has an instance name specified, enter the name in the format Servername\Instancename
 - If you are using non-standard SQL port, enter Servername\Instancename,portnumber
- For example, for a SQL server named Webs with instance name Websense and SQL port 2323 enter:
- Webs\Websense,2323**
- Make sure that the SQL Server and SQL Server Agent services are running.

- Specify the account type (Windows trusted or SQL database) to use for the database connection.
 - The SQL account must have **dbo** and **dbcreator** permissions. For SQL 2005, the account running database jobs must also belong to one of these: SQLAgentUserRole, SQLAgentReaderRole, or SQLAgentOperatorRole.
 - The Windows trusted account must have local administrator privileges on the database machine.
 - Select an appropriate Log Database location on the SQL server machine.
- Select database management options to control the size of the database and maximize reporting speed.

■ Logging Web page visits

- This option logs one record per Web page visited.
- This helps to create a smaller database and increase reporting speed.
- If you do not select this option, a separate record is created for each item on each requested Web page. Reports will be more precise, but the database will be large, and report generation will be slower.

■ Consolidating log records

- Combines multiple visits by the same user to the same domain into a single log record.
- For example, if userA goes to different pages in the yahoo.com domain within a short period of time, only 1 record is created.
- This creates a smaller database but reports are less precise.

■ After installation

- If you installed Log Server separately from Websense Manager, restart the **Apache2Websense** and **ApacheTomcatWebsense** services on the Websense Manager machine.

Installing Other Reporting Components

- In version 7, reporting components are integrated into Websense Manager.
 - The components include Today and History page charts, presentation reports, and investigative reports.
 - These components are installed automatically when Websense Manager is installed on a Windows machine.
 - Adobe Flash player and an updated version of Java are required to display graphs on the Today page.
- As a best practice, install Websense Manager and Log Server on a different machine than filtering components .

- Go to the Settings > Logging page in Websense Manager to verify the Log Server IP address.
 - If both components are on the same machine, make sure that the machine IP address, not localhost, is shown.
- Websense Manager can be accessed via Internet Explorer 7 and Firefox 2.x and 3.0.x.
 - Internet Explorer 8 is currently not a supported browser.
- After installation, use the following URL to access Websense Manager:
`https://<IP_address>:9443/mng`

■ Database Connection Failed error

- Most common installation error
- Verify that the SQL Server or MSDE server name or IP address is correct.
- Verify that you have used the correct user name and password for the database account.
- If a named instance exists on the server, verify the format entered.
- Verify that the folder specified for the Log Database exists and is readable and writable.

■ Database Connection Failed error (continued)

- If SQL Server uses a non-standard port, make sure the format is `Servername\instancename,portnumber`
- If Log Server and SQL Server are on different machines, make sure that there is no firewall between them.
 - Firewalls like ISA will need a specific rule allowing communication between the two machines.

■ Error in Database creation

- Verify that there is enough disk space on the SQL Server partition to create the database.
- Make sure the database path is correct.

■ Error in Database creation (continued)

- Verify that the account used has rights to create the database.
- Check model database size. If it is greater than 100 MB, try reducing the size of the model database.
- Check the account used to run the SQL Server and SQL Agent services.
 - An account with inappropriate permissions can cause this error.
 - Try running the services as local system.
- Verify that folder compression is not enabled on the folder selected for the Log Database. SQL Server does not support compression.

- **Could not configure Websense Manager**
 - Requires reinstallation of Websense Manager.
 - Remove the component using Add/Remove Programs, reboot.
 - Verify that Windows Data Execution Prevention (DEP) is set to Off.
 - Stop any antivirus software running on the machine.
 - If installation is done via RDP, ensure that /console switch is used.
 - Run the installation program again.

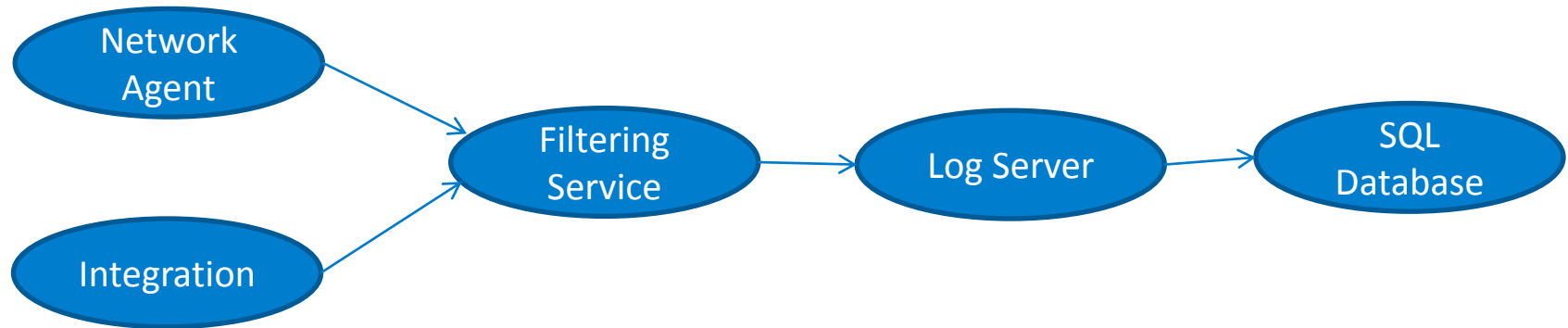
■ Presentation reports

- Offers a list of pre-defined reports
- Includes reports in tabular format and a combination of bar chart and tables
- Reports can be exported to PDF, HTML, and XLS formats
- Can be customized and scheduled

■ Investigative reports

- Allows browsing through log data interactively
- Main page shows summarized report which can be drilled down for a greater level of detail
- Allows report to be saved a favorite and can be scheduled
- Reports can be exported to PDF and XLS formats

Log Server Information Flow



- An integration product passes traffic to Filtering Service
- Filtering Service processes the request and passes to Log Server. Information comes in the form of tmp files in the Cache directory.
- Tmp files are processed and information is logged to the database.

■ Log Server service stops

- To start Log Server debugging:
 1. Open the Windows Services dialog box.
 2. Right- click Websense Log Server and select **Properties**.
 3. Enter **-debug** under Start Parameters .
 4. Restart the service.
- A file called **debug.txt** is created in the Websense **bin** directory.
- Analyze debug.txt for service initialization or connection errors.
- Verify that **Logserver.ini** is not corrupted.
- Verify that port **55805** is not in use by another program.

- Cache files are building up in the cache directory.
 - Run Log Server debug and analyze the debug.txt file for errors encountered during processing of tmp files.
 - Verify that there is adequate disk space on the SQL Server machine.
 - Verify that SQL Server Agent service is running.
 - Verify that the ETL job is being executed, and check ownership and permissions for the account running ETL.
 - A few corrupt cache files could result in those and subsequent files not being processed. Processing occurs sequentially.

■ No logging

- No tmp files are created in the cache directory.
- Verify Log Server settings in Websense Manager
- Verify that an integration product or Network Agent is sending traffic to Filtering Service.
- If using Network Agent, ensure that Network Agent settings are correctly configured in Websense Manager.

- Unable to connect to the Log Database
 - Verify that the Websense Log Server service is running.
 - Check the account permissions for the SQL account.
 - If Websense Manager and Log Server service are installed on separate machines, run the Apache2Websense, ApacheTomcatWebsense, and Websense Log Server services with an Admin account. This may also be required if you are using a trusted connection.

- Presentation Reports Scheduler could not connect to the Log Database.
 - Alert appears on the Status > Today page in Websense Manager.
 - Do not create scheduled presentation reports jobs while this error appears.
 - Usually seen when Log Server starts after the ApacheTomcatWebsense service has already started
 - Restart ApacheTomcatWebsense to resolve the issue.
 - For permanent resolution, you may need to set up a service dependency.

- **A General Error has occurred**
 - This is usually accompanied by an error code.
 - Check for the error code in the tomcat\logs\tomcat.log file.
 - If the error contains messages that indicate a missing function within SQL Server, copy the error and send it to Websense Technical Support.
 - The error occurs due to a specific function missing from the database, and can be addressed by running a SQL script.

- Scheduled jobs missing from presentation reports
 - Jobs disappear after machine was restarted.
 - During system restart, the ApacheTomcatWebsense service tries to contact the Presentation Reports Scheduler service.
 - If these services cannot communicate any jobs created are only stored temporarily and not written to the database.
 - Restart the ApacheTomcatWebsense service and create a job, verify after rebooting.

■ Could not connect to the Log Database

- Verify that the Log Server service is running and that it can connect to the SQL database.
- Verify the account permissions for the SQL account.
- If using a trusted connection, ensure that the SQL services are running with an account that has local admin privileges.
- If using non-standard SQL port, verify that the port number is specified correctly.
- Check Investigative Reports settings.

- No data in investigative reports
 - If ODBC is being used as insertion method, check the Cache folder to verify that files are moving.
 - If Bulk Copy Program (BCP) is being used, check the cache and then BCP folder and verify that files are moving.
 - Verify that the SQL Server Agent service is running.
 - Check the job history for ETL job in SQL Manager. Verify that this job is running correctly.
 - If using SQL 2005, the owner for running database jobs must have one of these settings checked: SQLAgentUserRole, SQLAgentReaderRole, or SQLAgentOperatorRole.

- No user names in reports
 - This is typically a user identification issue.
 - Verify that user-based policies are working as expected.
 - If not, follow the troubleshooting steps for user identification.
 - This can occur if Log Server cannot get updates from User Service regarding user and group information.

■ Software error:

Could not append to buffer c:/ExplorerJava/temp/991180.buf at /<C:\Program Files\WebSense\webroot\Explorer\ws_irpt.exe>

- Appears due to invalid file paths in one of the wse.ini files
 1. Go to \Program Files\WebSense\Webroot\Explorer\wse.ini.
 2. Open the file and make sure the following paths are correct:
fopdir=C:\Program Files\WebSense\webroot\Explorer\fop
javadocir=C:\Program Files\WebSense\uninstall\jvm\bin
jfreechartdir=C:\Program Files\WebSense\webroot\Explorer
installdir=C:\Program Files\WebSense\webroot\Explorer
tempdir=C:\Program Files\WebSense\webroot\Explorer\fop\tmp

- Configure Log Server Settings in Websense Manager after install.
- Database rollover options: Smaller organizations can set rollover on a monthly basis. Larger organizations may want to set rollover by size.
- Enabling full URL logging results in more precise reports but a larger database.
- Database maintenance options control when older partitions are deleted and when the maintenance task runs.

- Set the database path for mdf and ldf files. Different paths can be selected for mdf and ldf.
- Set the SQL Server database recovery mode to Simple Recovery.
 - Ensures that ldf files do not grow too large
 - Also enable Auto Shrink to control ldf file size.
- For faster log insertion, use Bulk Copy Program insertion.
- If moving databases between SQL Server installations, ensure that both SQL Servers have the same collation type.

- Track Websense maintenance task in SQL Server to ensure that important tasks like indexing and rollover are happening correctly.
- Make sure that the SQL account used for the Log Database does not have domain password policy enforced.
 - This could result in the database becoming inaccessible if the account gets disabled.



Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.



Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.



ask.websense.com

- Create and manage support service requests using our online portal.



Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

Webinar Update

Websense presents Tech Talk!

Title: Identifying and solving the most common Web Security issues: User Identification, Reporting, and Network Agent

Date: April 21, 2010

Time: 8:30 AM Pacific Time

How to register:

<http://www.websense.com/content/SupportWebinars.aspx>

Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location
- For more information, please send email to:
readiness@websense.com

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Questions?

