

Moving the TRITON Reporting Databases

Topic 50530 | Web, Data, and Email Security | Versions 7.7.x, 7.8.x | Updated 06-Nov-2013

If you need to move your Microsoft SQL Server database to a new location (directory, drive, or machine), this article describes procedures you can use to move your Websense reporting databases to minimize risk of data corruption or loss. Consult your database administrator to determine whether either of these procedures is appropriate for your organization.

- ◆ *(Recommended)* You can back up your Websense Web Security, Data Security, and Email Security databases in their current location, and restore them to the new location. See [Backup and restore the TRITON reporting databases, page 3](#).
- ◆ You can detach your Websense Web Security, Email Security, and Data Security databases from their current location and reattach them in a new location. See:
 - [Detach and reattach the Web or Email Security Log Database, page 7](#)
 - [Detach and reattach the Data Security databases, page 10](#)

If you are performing this procedure while upgrading to a newer Websense software version, be sure to upgrade your Websense software first.

For Websense Web and Email Security solutions, regardless of which procedure you choose, once the databases are in their new location, you must:

1. Recreate the Websense SQL Server Agent jobs.
2. Update the Log Server connection to the Log Database and configure the Log Database to create new database partitions in the correct (new) location. See [Update Log Server and Log Database settings, page 12](#).

The steps provided in this article are specific to Microsoft SQL Server **2008** and **2005**, though they include the option of moving to SQL Server **2012**.



Warning

Before beginning, make sure that the destination SQL Server instance's **collation** setting matches that of the source SQL Server instance.

To check, in SQL Server Management Studio:

1. Right-click the SQL server instance name and select **Properties**.
2. Under the General tab, check the **Server Collation** value.

Only move the SQL Server databases if the collation values match.

Backup and restore the TRITON reporting databases

Topic 50531 | Web, Data, and Email Security | Versions 7.7.x, 7.8.x | Updated 06-Nov-2013

Version 7.8 introduces support for the Websense TRITON reporting databases (Web Security Log Database, Data Security Incident and Configuration Database, and Email Security Log Database) on Microsoft SQL Server 2012.

For Websense Web Security solutions, v7.8 also ends certification for Microsoft SQL Server 2005.

Before upgrading an existing installation of Microsoft SQL Server to a new version or migrating to a new machine, back up your Websense TRITON reporting databases to a safe location.

If you are **upgrading in place**, the upgrade process should not affect the reporting databases, but it is a best practice to make a backup copy to safeguard against corrupted data or other data loss.

If you plan to **migrate your databases** to a new Microsoft SQL Server installation on another machine, to minimize downtime, start by installing and configuring SQL Server in the new location.

The upgrade or migration process begins with a backup of your existing reporting databases. Because the backup process can be quite time consuming, the instructions in this document ask you to perform the backup in 2 stages.

For Web Security and Email Security:

- ◆ The initial backup can be performed while the Log Database is online, processing data.
- ◆ The second, incremental backup is performed on just the active partition (the partition currently receiving new records) and catalog database for your Web or Email Security solution.

The intent is to minimize the database downtime required for the upgrade or database migration.

1. Perform a full database backup

1. Open SQL Server Management Studio (**Start > All Programs > Microsoft SQL Server 2005 or 2008 > SQL Server Management Studio**) and log onto the SQL Server instance that hosts your Websense TRITON reporting databases.
2. In the Object Explorer, under **Databases**, locate your Websense TRITON databases. The default database names are:
 - For Web Security solutions, **wslogdb70_n** and **wslogdb70_amt_1** (partition databases) and **wslogdb70** (the catalog database)

- For Email Security solutions, **esglogdb76_n** (partition databases) and **esglogdb76** (the catalog database)
- For Data Security solutions, **wbsn-data-security** and **wbsn-data-security-temp-archive**

In the Web and Email Security examples, “n” is the partition number. The higher the number, the newer the partition.

3. Right-click each database, expand the **Tasks** menu, and select **Back Up**.
4. In the Back Up Database window, you can either accept the default backup **Destination**, or click **Add** and specify a new path for the backup file. When you are finished, click **OK** to run the backup.
5. Repeat steps 3 and 4 to back up each of the remaining databases.

At the end of this process, you have full backups of all of your older partition databases, and recent backups of your active partition (the one that new log records are being added to) and catalog databases. Continue to the next section when you are ready to temporarily stop database processing.

2: Back up the catalog database and active partition (Web and Email Security)

1. Stop all **Websense Log Server** or **Websense Email Security Log Server** instances in your deployment.
2. Disable the Web Security or Email Security database jobs.
 - a. In the left navigation pane, click the **SQL Server Agent** folder for the instance hosting the Log Database.
 - b. Click **Jobs**, and disable each of the Websense jobs by right-clicking the job and selecting **Disable**.

The job names are in the format “Websense_xxx_<catalog database name>” where xxx is the type of job and <catalog database name> is the actual name of your catalog database (by default, wslogdb70 or esglogdb76).

Make sure that **all Websense jobs are completed** before continuing. This could take several minutes or a few hours, depending on the details of your installation. Contact your database administrator if you need assistance determining whether the jobs are completed.

3. Perform a differential backup of the catalog database (**wslogdb70** or **esglogdb76**). This will back up anything that has changed since the initial backup performed in Part 1 of this procedure.
4. Perform a differential backup of the active database partition (the one that is still receiving new log records). Its name is something like wsglogdb70_10 or esglogdb76_5).

3a: Upgrade in place

If the machine hosting your database engine is adequate to host an upgraded version of SQL Server:

1. Stop the Data Security server. The Web and Email Security Log Servers are already stopped.
2. Upgrade your Microsoft SQL Server installation, following the instructions in your Microsoft documentation.
3. Once installation is complete, enable the Websense SQL Server Agent jobs.
 - a. In the left navigation pane, click the **SQL Server Agent** folder for the instance hosting the Log Database.
 - b. Click **Jobs**, and enable each of the Websense jobs by right-clicking the job and selecting **Enable**.

The job names are in the format “Websense_xxx_<catalog database name>” where xxx is the type of job and <catalog database name> is the actual name of your catalog database (by default, wslogdb70 or esglogdb76).

4. Start all **Websense Log Server** or **Websense Email Security Log Server** instances in your deployment.
5. Start the Data Security server.

Log Server resumes sending data to the Log Database, and the ETL job begins processing the Web Security or Email Security records into the active partition.

3b: Migrate the database to a new SQL Server host

If you are moving the reporting database to SQL Server on another machine:

1. Install the desired version of SQL Server on the new machine.
2. Open SQL Server Management Studio (**Start > All Programs > Microsoft SQL Server 2008 or 2012 > SQL Server Management Studio**) and log on to the SQL Server instance that will host your Websense TRITON reporting databases.
3. Restore the reporting databases from their backup location:
 - a. In Object Explorer, right-click **Databases** and select **Restore Database**.
 - b. Enter the database name in the **To database** field.
 - c. Select **From device**, then click the browse (...) button.
 - d. With **File** selected (the default), click **Add** and browse to the backup location.
 - e. Select the databases you want to restore from the **Select the backup sets to restore** list.
 - f. Select the **Options** page of the restore window, then verify that the **Restore As** column shows the correct location for the destination (restored) partition.
 - g. Repeat steps a through f until all databases have been restored.

4. Recreate the Web Security or Email Security database jobs on the new SQL Server installation.

- a. Open the **Query** window and point to the Websense catalog database (default name wslogdb70 or esglogdb76).

- b. Execute the following stored procedures:

```
exec dbo.usp_update_views;
```

```
go
```

```
exec dbo.usp_create_background_jobs;
```

```
go
```

If you are migrating a Web Security or Email Security Log Database, continue with [Update Log Server and Log Database settings, page 12](#).

5. Direct the Data Security management components to the new database server. To do this, run the TRITON Setup installer and select **Modify**.
6. Direct Email Security to the new database server by navigating to **Settings > Reporting > Log Database** and changing the configuration.

Detach and reattach the Web or Email Security Log Database

Topic 50532 | Web and Email Security | Versions 7.7.x, 7.8.x | Updated 06-Nov-2013

If you want to move the Log Database by detaching it, manually moving files, and then reattaching the files in a new location, use the following procedure.

1: Detach the Log Database

To prepare to move the Web or Email Security Log Database, stop all of the SQL Server Agent jobs and wait for them to stop, then detach the database from its current SQL Server location.

1. On the Log Server machine, use the Windows Services tool to stop the **Websense Log Server** or **Websense Email Security Log Server** service.
2. On the SQL Server machine, open Microsoft SQL Server Management Studio:
 - **Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**
 - **Start > Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**
 - **Start > Programs > Microsoft SQL Server 2012 > SQL Server Management Studio**
3. Log into the SQL Server instance that hosts the Log Database.
4. Disable all Websense-related SQL Server Agent Jobs as follows:
 - a. In the left navigation pane, click the **SQL Server Agent** folder for the instance hosting the Log Database.
 - b. Click **Jobs**, and disable each of the Websense jobs by right-clicking the job and selecting **Disable**.

The job names are in the format “Websense_xxx_<catalog database name>” where *xxx* is the type of job and <catalog database name> is the actual name of your catalog database (by default, wslogdb70 or eslogdb76).

Make sure that **all Websense jobs are completed** before continuing. This could take several minutes or a few hours, depending on the details of your installation. Contact your database administrator if you need assistance determining whether the jobs are completed.

5. Use T-SQL commands or a SQL Server backup tool to create a backup of the database.

Before continuing, verify that the backup files are valid.
6. If you are simply copying the database files to a new directory or disk, and will then reattach them, continue to step 7.

If you plan to move the database to a new instance of SQL Server, it is strongly recommended that you delete the Websense SQL Server Agent jobs after disabling them. To do this:

- a. In SQL Server Management Studio, connect to the old instance and expand the **SQL Server Agent > Jobs** tree.
 - b. Right-click each Websense job associated with **wslogdb70** or **eslogdb76** and select **Delete**. (The number of jobs depends on your product version.)
7. In SQL Server Management Studio, use the following steps to detach the catalog database (default name wslogdb70 or eslogdb76), each standard logging partition database (wslogdb70_x or eslogdb76_x) and the Web Security threats (AMT) partition database (wslogdb_amt_1):
- a. Expand the **Databases** folder.
 - b. Right-click one of the Websense databases, and then select **Tasks > Detach**.
 - c. Repeat this process for each database until the catalog database and all partition databases have been detached. The order does not matter because the Websense SQL Server Agent Jobs are disabled (not running).

The Websense Log Database has now been detached from its original location.

2: Move the Log Database

Once the Log Database has been detached from its original location, move it to the new location, reattach it to SQL Server, and recreate the SQL Server Agent jobs.

1. Navigate to the directory you selected for the Log Database during Log Server installation.
2. Move all database files ending in **.mdf** and **.ldf** to the new location.
There should be an mdf file and an ldf file for each database that you detached in the previous procedure.
3. On the SQL Server machine, open Microsoft SQL Server Management Studio for the new SQL Server instance, then attach each standard logging (wslogdb70_x or eslogdb76_x) and the Web Security threats (AMT) partition database (wslogdb_amt_1) as follows:
 - a. Expand the nodes in the left navigation pane until you reach the **Databases** folder, and then right-click that folder.
 - b. Select **Attach**, then click **Add**.
 - c. Navigate to the location of the Log Database mdf and ldf files, then select a partition database **mdf** file.
 - d. Repeat this process for each standard logging and threats partition database.
 - e. Click **OK** when all partition databases have been selected.
4. Use the same procedure to attach the catalog database (by default, wslogdb70 or eslogdb76).
5. To create the SQL Server Agent jobs:

- a. Open the **Query** window and point to the Websense catalog database (default name wslogdb70 or eslogdb76).
- b. Execute the following stored procedure:

```
exec dbo.usp_update_views;  
go  
exec dbo.usp_create_background_jobs;  
go
```

If you are migrating a Web Security or Email Security Log Database, continue with [Update Log Server and Log Database settings, page 12](#).

Detach and reattach the Data Security databases

Topic 50900 | Data Security | Versions 7.8.x | Updated 06-Nov-2013

If you want to move the Data Security databases by detaching them, manually moving files, and then reattaching them in a new location, use the following procedure.

1: Detach the databases

1. Log off of the TRITON console.
2. On the TRITON management server, use the Windows Services tool to stop the **Websense TRITON - Data Security** service (DSSManager).
3. Change the service startup type to **Disabled**.
4. On the SQL Server machine, open Microsoft SQL Server Management Studio:
 - **Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio**
 - **Start > Programs > Microsoft SQL Server 2008 > SQL Server Management Studio**
 - **Start > Programs > Microsoft SQL Server 2012 > SQL Server Management Studio**
5. Log onto the SQL Server instance that hosts the Data Security database.
6. Detach the **wbsn-data-security** and **wbsn-data-security-temp-archive** databases as follows:
 - a. Expand the **Databases** folder.
 - b. Right-click one of the Websense databases, and then select **Tasks > Detach**.
 - c. Repeat this process for the other databases. The order does not matter.

The Data Security database has now been detached from its original location.

2: Move the database

Once the Data Security database has been detached from its original location, move it to the new location, reattach it to SQL Server, and modify TRITON settings.

1. Copy the following files from the /Data folder on the source SQL Server machine to the /Data folder on the target SQL Server machine:
 - wbsn-data-security.mdf
 - wbsn-data-security_log.LDF
 - wbsn-data-security-temp-archive.mdf
 - wbsn-data-security-temp-archive_log.LDF

2. On the target SQL Server machine, open Microsoft SQL Server Management Studio.
3. Attach the **wbsn-data-security.mdf** and **wbsn-data-security_log.LDF** databases as follows:
 - a. Expand the nodes in the left navigation pane until you reach the **Databases** folder, and then right-click that folder.
 - b. Select **Attach**, then click **Add**.
 - c. Navigate to the location of the mdf and ldf files, then select a partition database **mdf** file.
 - d. Repeat this process for each database.
 - e. Click **OK** when all databases have been selected.
4. On the TRITON management server, run the TRITON Setup wizard, select **Modify**, and then modify the settings to use the target SQL Server.

If you are moving the database from a local SQL Express to a remote Standard or Enterprise Edition, edit **/Websense/EIP Infra/EIPSettings.xml** before running modify. Set the External value to true:

```
<External>true</External>
```
5. Run the Modify wizard for the Data security component and modify the settings for **Temporary File Location**. (Verify that all UNC path are accessible.)
6. Delete the content of the following folders from the management server:
 - %dss_home%\tomcat\work
 - %dss_home%\tomcat\temp
7. Using the Windows Services tool, set the **Websense TRITON - Data Security** service startup type back to “Automatic” and start the service.
8. Log onto the Data Security manager and verify you can see data from the database—for example, the incidents database or resources list.

Update Log Server and Log Database settings

Topic 50533 | Web and Email Security | Versions 7.7.x, 7.8.x | Updated 06-Nov-2013

Once the Log Database has been moved and the SQL Server jobs have been created, configure Log Server to send data to the new database location, and configure the Log Database to use the new location when it creates new partitions.

Web Security Log Server and Log Database settings

1. Log onto the TRITON console and select the **Web Security** module.
2. Navigate to the **Settings > Reporting > Log Server** page.
3. Under **Log Database Connection**, update all of the connection information to enable communication with the new SQL Server installation.
4. Click **Test Connection** to validate the new connection information.
5. Click **OK**, then **Save and Deploy** to implement the changes.
6. Log off of the TRITON console and use the Windows Services tool to restart:
 - Websense TRITON Web Security
 - Websense Log Server
7. When the TRITON service has restarted, log on to the TRITON console again.
8. On the **Settings > Reporting > Log Database** page, under Partition Management, update the **Data** and **Log File Path** entries as needed.

This ensures that new database partitions are created in the correct (new) location.

Email Security Log Server and Log Database settings

Update TRITON Unified Security Center and Email Security Log Server to use the new Log Database location.

1. Log on to the TRITON Unified Security Center and click **Email Security**.
2. Go to **Settings > Reporting > Log Database** and enter the IP address of the new SQL Server installation in the **Log database** field.
3. Click **OK** (in the Log Database Location area of the screen).
4. On the machine running Email Security Log Server, start the Email Security Log Server Configuration utility (**Start > All Programs > Websense > Email Security > Email Security Log Server Configuration**).
5. In the **Database** tab, click **Connection** to open the **Select Data Source** dialog box.
6. Select the **Machine Data Source** tab and click **New** to open the Create New Data Source dialog box.

You will create a new data source connection to the new Email Security database location.

7. Select **System Data Source (Applies to this machine only)** and then click **Next**.
8. In the list of drivers, select **SQL Server** and then click **Next**.
9. In the next dialog box, click **Finish**.
10. In the **Create a New Data Source to SQL Server** wizard, enter a **Name**, **Description**, and the **Server** IP address for the new data source connection. Then click **Next**.

The server IP address should be the new IP address of the machine on which the Email Security database is located.

11. In the next dialog box, select options as described below.
 - a. Select an authentication method for connecting to the database:
 - **With Windows NT authentication using the network login ID:** to use a Windows trusted account.
 - **With SQL Server authentication using a login ID and password entered by the user:** to use a SQL Server account.
 - b. Enable **Connect to SQL Server to obtain default settings for the additional configuration options**.
 - c. Enter the **Login ID** and **Password** of the **sa** SQL Server account if you selected SQL Server authentication in [Step a](#) above).
 - d. Click **Next**.
12. In the next dialog box, enable **Change the default database to** and then select **esglogdb76** from the drop-down menu. Then click **Next**.
13. In the next dialog box, accept the default settings and click **Finish**.
14. Click **Test Data Source** to test the connection. Upon test success, click **OK**.
15. Click **OK**, then click **OK** once more.
16. In the SQL Server Login dialog box, enter a **Login ID** (by default, sa) and **Password**. Then click **OK**.

If you choose to **Use Trusted Connection** (i.e., Windows NT authentication), Login ID and Password are not necessary.
17. In the Email Security Log Server Configuration utility, click **Apply** and then **OK** to the warning message about stopping and restarting Log Server.
18. On the **Connection** tab, under **Service Status**, click **Stop**.

This stops Email Security Log Server.
19. Click the same button (it now is labeled **Start**).

This starts Email Security Log Server. It is now configured to use the new Email Security database location.
20. Click **OK** to close the Email Security Log Server Configuration utility.

