Windows Server Update Services (WSUS)

WSUS (Windows Server Update Services) is a **free tool from Microsoft** that helps IT administrators manage **Windows updates** across many computers in a network and provides a way for IT administrators to **deploy** the latest Microsoft product updates.

Without WSUS:

- Each computer **connects** to the internet and **downloads updates from Microsoft**.

With WSUS:

- **Only the WSUS server downloads updates from Microsoft**.

- All the other computers (called **clients**) in your company download the updates **from the WSUS server**, not from the internet.

This saves **bandwidth**, gives **more control**, and improves **security**.

A WSUS server provides features that we can use to **manage and distribute updates through a management console**.

A WSUS server can also be the **update source** for other WSUS servers within the organization.

The WSUS server that acts as an update source is called an **upstream server**.

In a WSUS implementation, **at least one WSUS server** on your network must be **able to connect to Microsoft Update** to get available update information.

As an administrator, we can determine based on **network security and configuration** how many other WSUS servers connect directly to Microsoft Update.

Maintain WSUS while supporting Configuration Manager current branch version 1906 and later versions

Step 1: If we are using Configuration Manager current branch version 1906 or later versions, we should **enable the WSUS Maintenance options** in the **software update point** configuration to **automate the cleanup** procedures after each synchronization.
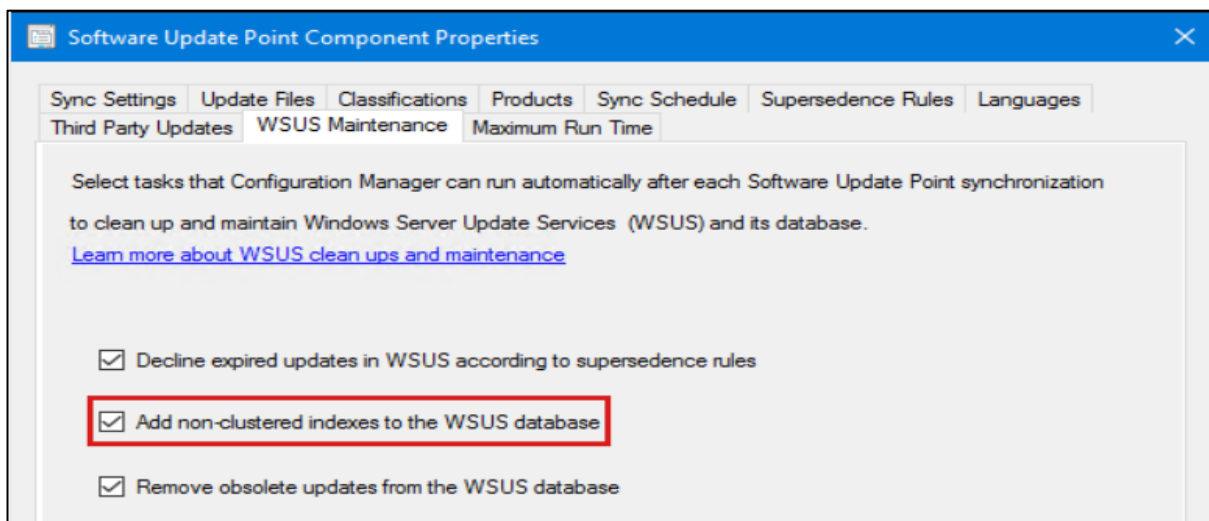
Step 2: When we are using WSUS along with **downstream servers**, WSUS servers are **added from the top down** but they should be **removed from the bottom up**. When syncing or adding updates they go to the **upstream** WSUS server first then replicate down to the **downstream** servers. When performing a cleanup and removing items from WSUS servers we should start at the bottom of the hierarchy (Updates go top to bottom and Cleanups should go bottom to top).

Step 3: WSUS maintenance can be performed simultaneously on **multiple servers** in the same tier. When doing so we should ensure that **one tier** is done before moving onto the **next one**. The **cleanup** and **reindex** steps should be run on all WSUS servers regardless of whether they are a replica WSUS server or not.

Step 4: Ensure that **SUPs** (Software Update Points) **don't sync during the maintenance** process as it may cause a **loss of some work** already done. **Check** the SUP **sync** schedule and temporarily set it to **manual during this process.**
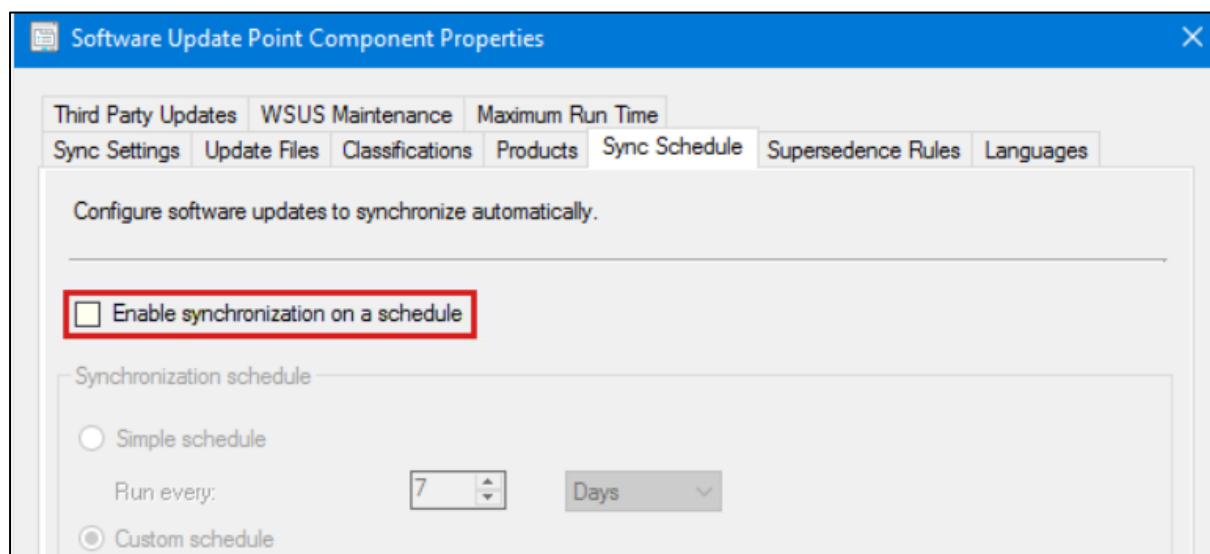
Step 5: If we have **multiple SUPs** of the primary site or central administration site (CAS) which don't share the **SUSDB**, consider the **WSUS server that syncs with the first SUP** on the site.

For example, we have two SUPs:

1. The one named New syncs with Microsoft Update, it would be my top tier i.e. **Tier1.**

2. The server named 2012 syncs with New and it would be considered in the second tier i.e. **Tier2**

Perform WSUS Maintenance

The basic steps necessary for proper WSUS maintenance include:

1. **Back up the WSUS database**

We can back up the WSUS database (SUSDB) by using the desired method.

These are few recommendations:

- As a database increases in size, full database backups take more time to complete and require more storage space. For large databases, consider full database backups with a series of **differential database backups**.

- Estimate the size of a full database backup by using the **sp_spaceused** system stored procedure.

- By default, every successful backup operation adds an entry in the SQL Server error log and in the system event log. If we back up frequently, success messages will accumulate quickly, resulting in huge error logs, making finding other messages difficult. In such cases, we can suppress these backup log entries by using **trace flag 3226** if none of our scripts depend on those entries.

But there are few limitations and restrictions to it as well.

The limitations are as followed:

- The **BACKUP** statement isn't allowed in an explicit or implicit transaction.

- Backups created by a more recent version of SQL Server can't be **restored** in earlier versions of SQL Server.

2. **Create custom indexes**

This process greatly **improves performance during subsequent cleanup operations**. If we are using Configuration Manager current branch version 1906 or a later version, then we use Configuration Manager to create the indexes. To create the indexes, configure the **Add non-clustered indexes to the WSUS database** option in the software update point configuration.
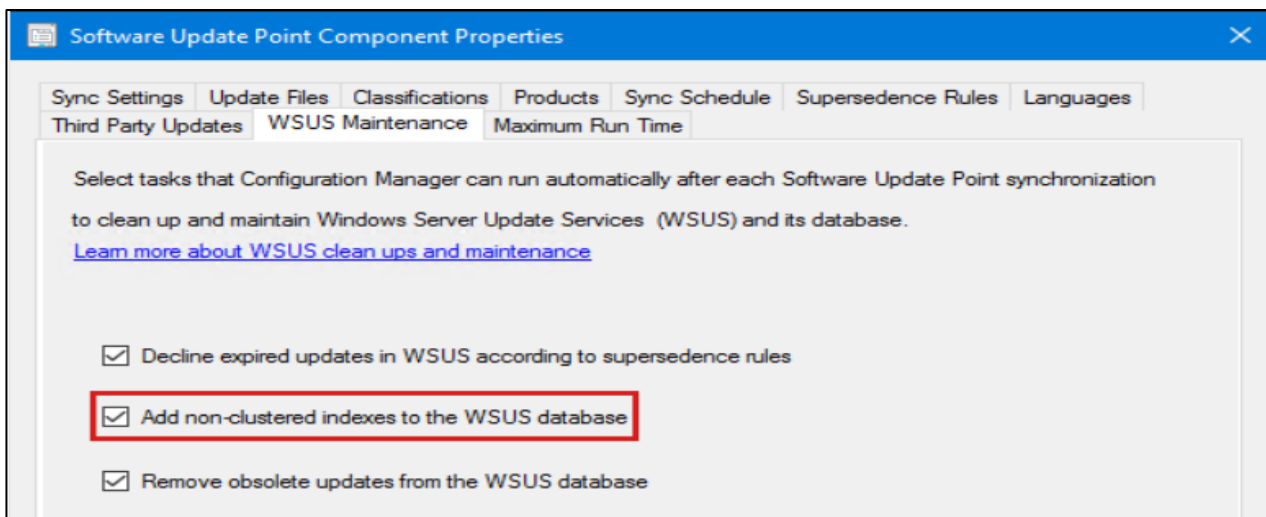
3. Reindex the WSUS database

The steps to connect to SUSDB and perform the reindex differ depending on whether SUSDB is running in **SQL Server** or **Windows Internal Database (WID)**. To determine where SUSDB is running, check the value of the **SQLServerName** registry entry on the WSUS server located at the **HKEY_LOCAL_MACHINE\Software\Microsoft\Update Services\Server\Setup** subkey.

If the value contains just the **server name** or **server\instance**, **SUSDB is running on a SQL Server**. If the value includes the string **##SSEE** or **##WID** in it, **SUSDB is running in WID**.
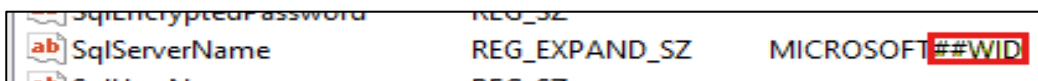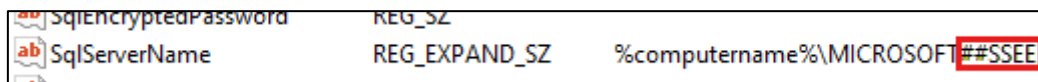
- If SUSDB was installed on WID, **SQL Server Management Studio Express** must be installed locally to run the reindex script.

- If SUSDB was installed on full SQL Server, launch **SQL Server Management Studio** and enter the **name of the server (and instance if needed)** when prompted.

To run the script in either **SQL Server Management Studio** or **SQL Server Management Studio Express**, select **New Query** and paste the script in the window and then select **Execute**. When it's finished, a **Query executed successfully** message will be displayed in the status bar. And the Results pane will contain messages related to what indexes were rebuilt.
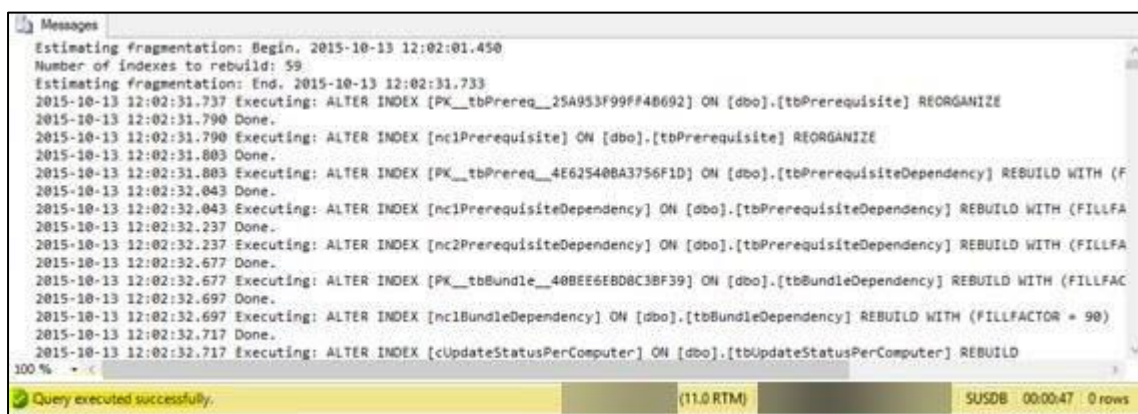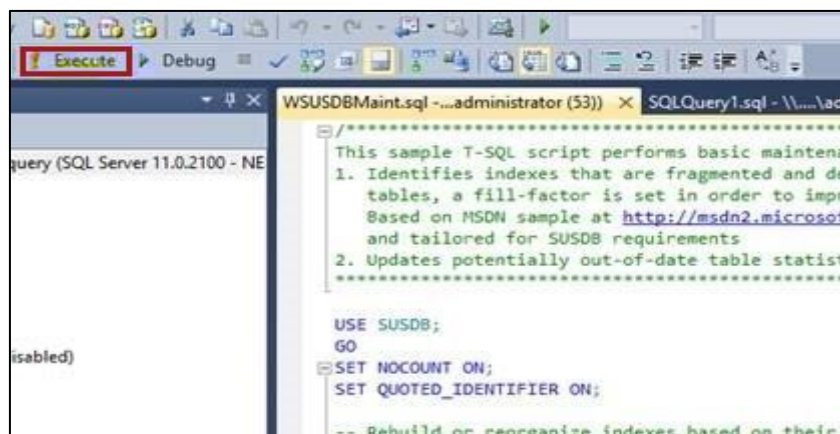
Decline superseded updates in the WSUS server to help clients scan more efficiently. Before declining updates, ensure that the superseding updates are deployed and that superseded ones are no longer needed. Configuration Manager includes a separate cleanup which allows it to expire superseded updates based on specified criteria.

The following SQL query can be run against the SUSDB database to quickly determine the number of superseded updates. If the number of superseded updates is higher than 1500 it can cause various software update related issues on both the server and client sides.

Select COUNT(UpdateID) from vwMinimalUpdate where IsSuperseded=1 and Declined=0

5. Run the WSUS Server Cleanup Wizard

The **WSUS (Windows Server Update Services) Server Cleanup Wizard** is used to **remove** <u>outdated or unnecessary updates and data from the WSUS database</u>. This helps **improve** <u>performance</u> and ensures only relevant updates are stored and managed.

WSUS server Cleanup Wizard provides options to clean up the following

- Unused updates and update revisions (also known as Obsolete updates)
- Computers not contacting the server
- Unneeded update files
- Expired updates
- Superseded updates

In a Configuration Manager environment **"Computers not contacting the server"** and **"Unneeded update files"** are **not relevant** because Configuration Manager (SCCM) **manages** devices and update content directly

These options become **relevant** if either of them is **enabled** under **Software Update Sync Settings "Create all WSUS reporting events"** and **"Create only WSUS status reporting events"**

If one of these is configured, it's recommended to **automate WSUS Server Cleanup** to include **Cleaning up devices not contacting the server** and **removing unneeded update files**

If you're using **Configuration Manager Version 1906** and Later version, the following options are available and should be **enabled:**

1. Decline expired updates in WSUS according to supersedence rules: This option handles declining of Expired updates and Superseded updates based on supersedence rules defined in Configuration Manager

2. Remove obsolete updates from the WSUS database: This Option handles the cleans up of Unused updates and update revisions (Obsolete updates) it also helps optimize WSUS database performance.
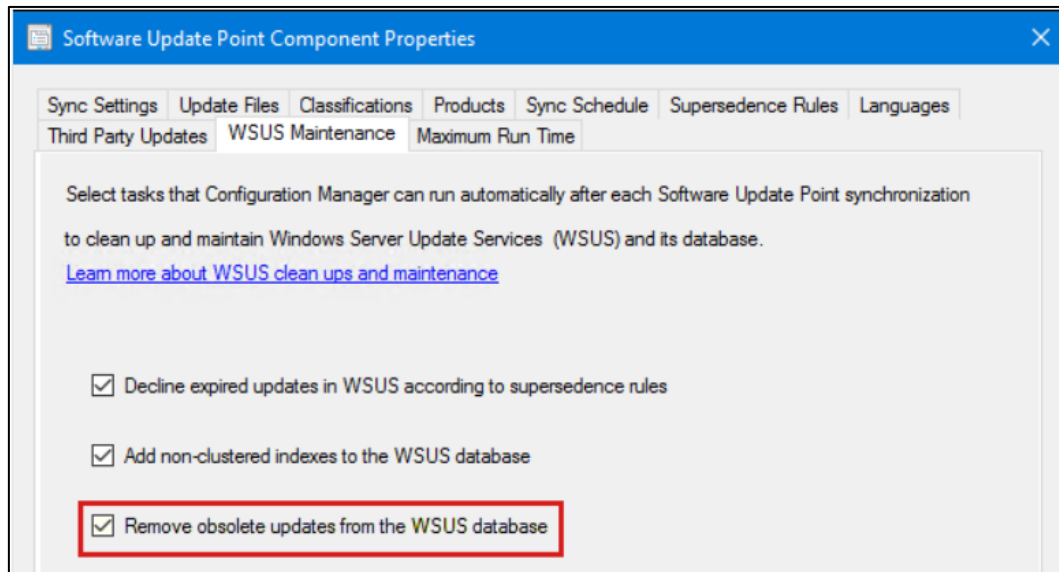
If the **WSUS cleanup has never been run before**, the process might **time out** due to the large amount of outdated data. In such cases, check the **WsyncMgr.log** file and consider using a **Microsoft-recommended SQL script** to complete the initial cleanup.

For **older Configuration Manager versions** or **standalone WSUS servers**, it's important to **run the cleanup wizard regularly**. If the WSUS Server Cleanup Wizard has never been run and the WSUS has been in production for a while, the cleanup may time out. In that case, reindex with Step 2 and Step 3 first, then run the cleanup with only the **Unused updates and update revisions** option checked.

Start by running it with only the **"Unused updates and update revisions"** option this may take **several attempts**. Once successful, run the **other cleanup options one by one**, and finally do a **full cleanup with all options selected**. If timeouts persist, **repeat the process** or use **SQL scripts**. **Reindexing the WSUS database before cleanup** can also help improve success.

The WSUS Server Cleanup Wizard runs from the WSUS console. It is located under **Options**, as shown here:
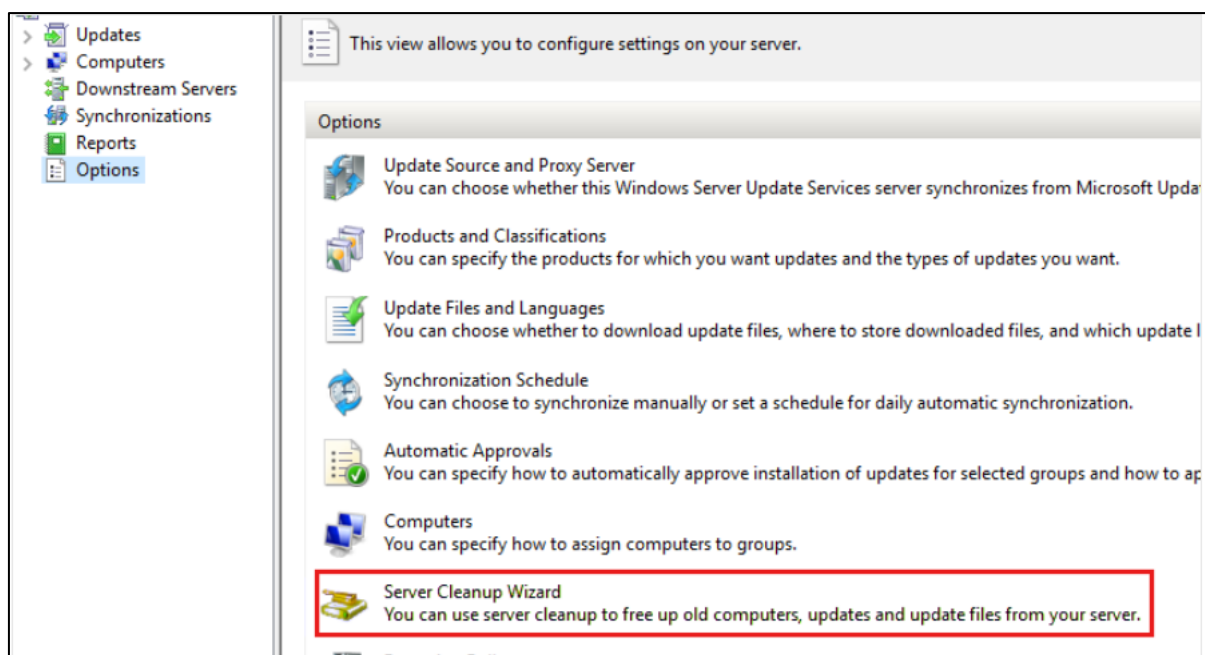
For more information, see **Use the Server Cleanup Wizard.**

After it reports the number of items it has removed, the cleanup finishes. If you do not see this information returned on your WSUS server, it is safe to assume that the cleanup timed out. In that case, you will need to start it again or use the **SQL alternative.**