
# Customer WSUS Setup Instructions

**For Breast & Skeletal Health Products**

RD-04022 Revision 001

HOLOGIC®

# Table of Contents

# Introduction

This document provides instructions for configuring Hologic Breast and Skeletal Health product systems, running Windows 10 or Windows Server 2016/2019, for automatic installation of Windows security updates by utilizing an existing customer Windows Server Update Service (WSUS) Server. Updates approved for installation within the customer WSUS Server should include only Hologic validated patches for the product. A list of validated security patches for Breast and Skeletal Health products are typically published each month and can be found at the following cybersecurity web portal:

*https://www.hologic.com/support/usa/Breast-Skeletal-Products-Cybersecurity*

Navigate to the address provided above and select **Validated Microsoft Monthly Critical Patch Releases**. Locate the Monthly Validated Patches section for the current date, for example, October 2020. Under that section, select the link(s) that match your current Product(s) and Operating System(s).

**Supported Products:** All Windows 10 and Windows Server 2016/2019 Breast and Skeletal Health products, with validated patch lists on the cybersecurity web portal linked above, are supported by this document and can be configured to receive validated patches using an existing WSUS Server managed by the customer.

# Requirements

- Existing WSUS Server hosted and managed by the Customer.
- Support of an IT or System Administrator to perform, or at least assist with, configuring the Hologic product system and the WSUS Server.
- Network firewall exceptions configured to allow WSUS traffic between the WSUS Server and the product system (client).
- WSUS Server connectivity information. If the WSUS Server utilizes SSL/TLS connections (recommended), access to the appropriate certificate for installation on the product system.

# Recommendations

- Create a new computer group on the WSUS Server for each Hologic product (for example, Hologic-Dimensions, Hologic-AffirmProne) and assign Hologic product systems to the appropriate group as they are configured. To facilitate optimal operation of Hologic product systems, only security patches validated by Hologic should be applied to the product systems. Each month, the customer can review validated patches listed on the web portal below for all appropriate products and approve new patches via WSUS Server for the appropriate product groups.
  *https://www.hologic.com/support/usa/Breast-Skeletal-Products-Cybersecurity/Validated-Patches*
- Typically, Hologic only validates security updates. Applying non-validated driver, third-party, or feature updates to Hologic product systems is not recommended.
- Instructions provided in this document configure the Hologic product system to download and install updates during off hours to limit interruption to the product system. To support this configuration, leave the Hologic product system running overnight to allow for maintenance

tasks to occur, for example, Windows Updates and Disk Defrag. Restart the product system each morning before active use.

- If Hologic product systems are on a Domain, you may apply the client-side group policy changes discussed in this document from the Domain controller.
- Hologic encourages the use of TLS/SSL for connectivity between the WSUS Server and the product system (client). To configure TLS/SSL connections to the WSUS Server, follow the instructions in the Configure Windows Update Group Policy Settings and Install SSL/TLS Certificate sections.

# Configuring Hologic Product Systems

Instructions provided within this section are applied to the product system (as the WSUS client) receiving/installing Windows security patches.

## Temporarily Disable Windows Update Service

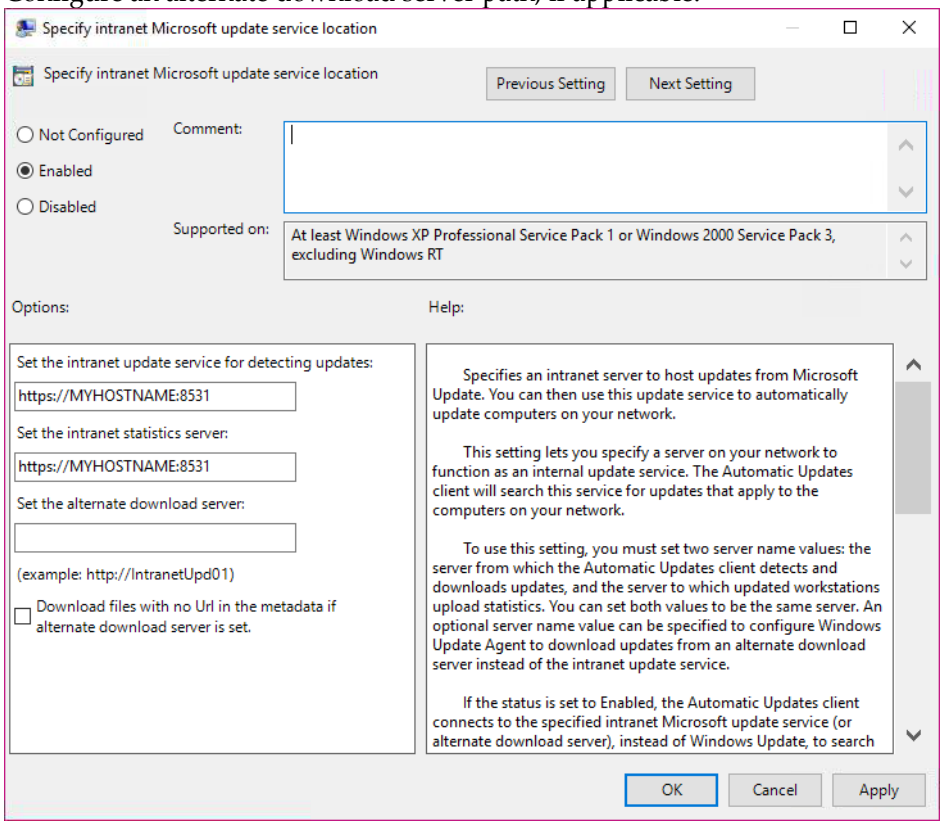
Hologic products are typically set by default to disable the Windows Update service, so that non-validated patches are not installed directly from Microsoft. These instructions make sure the service is disabled while preparing the system for a custom WSUS Server connection.

1. Log into Windows on the product system as a system administrator, for example, HologicService.
2. Right-click the Windows Start button and select **Computer Management** from the menu.
3. In the *Computer Management* window, select **Services and Applications** and double-slick **Services**.
4. In the list of Services, locate and double-click **Windows Update**.
5. In the *Windows Update Properties* window, set the 'Startup type' to **Disabled**, select **Stop**, and then select **OK** to save changes.
6. Close all open windows.

## Configure Windows Update Group Policy Settings

1. Right-click the Windows Start button and select **Search**. Type `Edit group` and select **Edit group policy** in the list of matches.
2. In the *Local Group Policy Editor* window, expand each item to navigate to **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
3. Configure WSUS Server connectivity settings.
    a. Double-click the **Specify intranet Microsoft update service location** setting.
    b. Select the **Enabled** option.
    c. In the Options section, configure the intranet update service and intranet statistics server paths by providing IP/Port or Hostname/Port. For example, https://BSHWSUS01:8531. Hologic encourages using SSL (HTTPS). Details required for these connection paths should be provided by IT or the System Administrator.
    **NOTE:** The hostname provided in the connection string needs to exactly match the configured Common Name (CN) in the SSL certificate.

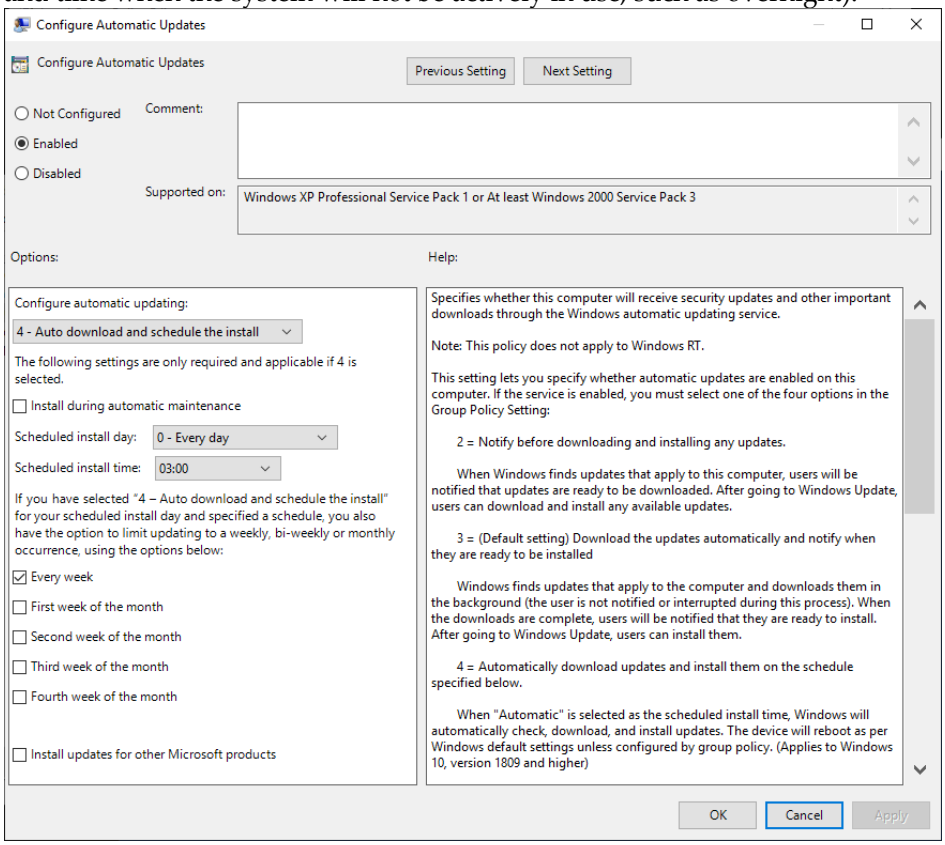
d. Configure an alternate download server path, if applicable.




e. Select **OK** to apply policy settings.

4. Configure Automatic Updates.
   a. Double-click the **Configure Automatic Updates** setting.
   b. Select the **Enabled** option.
   c. In the Options section set automatic updating to **4 - Auto download and schedule the install**. Configure with this option to avoid installing updates during active product system use.

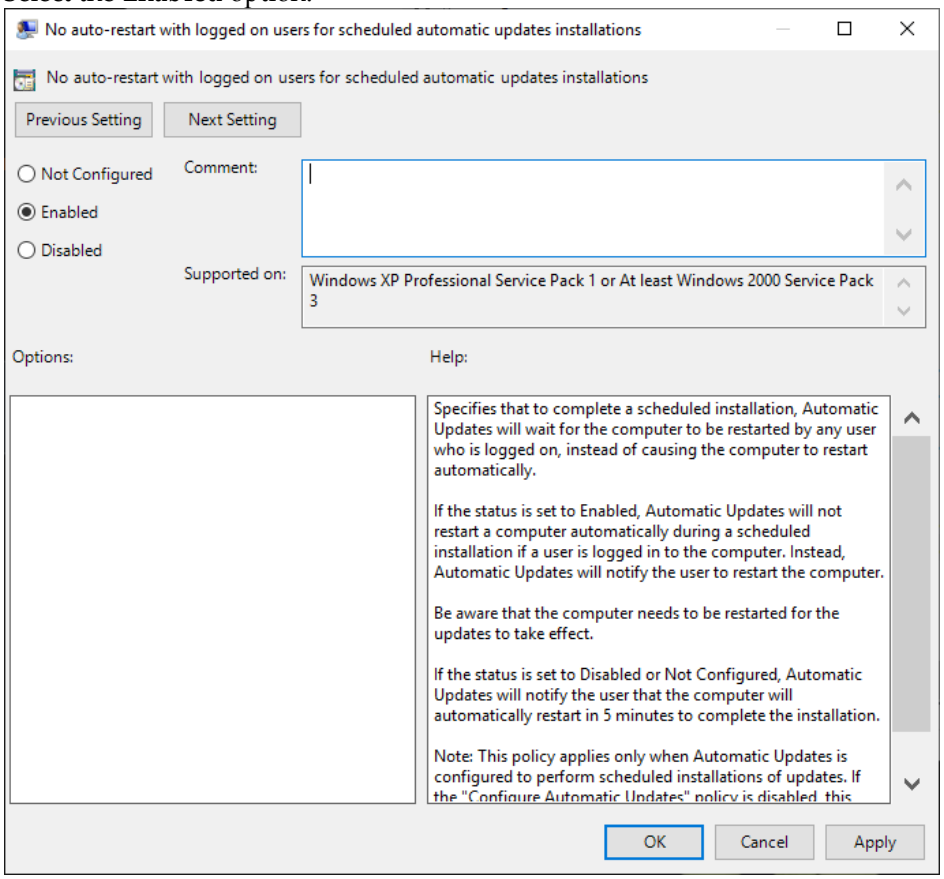
d. Configure the scheduled install day and time to best meet your needs (for example, a day and time when the system will not be actively in use, such as overnight).




e. Select **OK** to apply policy settings.

5. Disable automatic restart after installing updates.
   a. Double-click the **No auto-restart with logged on users for scheduled automatic updates installations** setting.

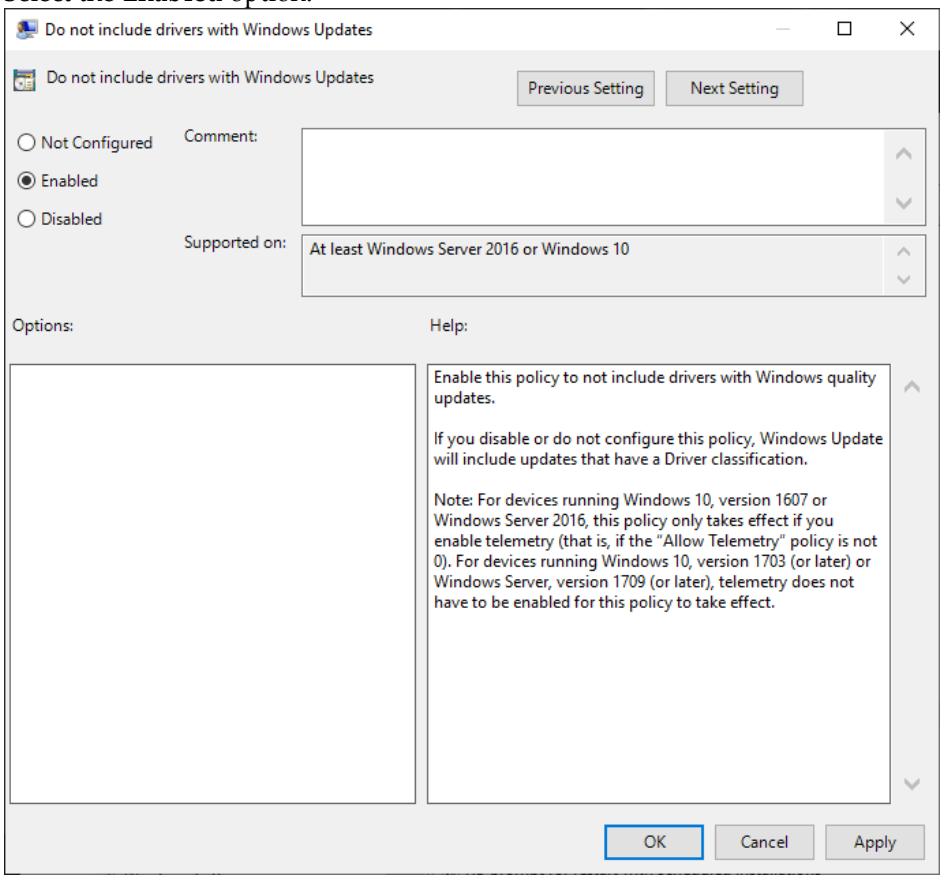
b. Select the **Enabled** option.




c. Select **OK** to apply policy settings.

6. Disable inclusion of drivers with Windows Updates. Hologic should make all driver updates to promote optimal functioning of the product system.
    a. Double-click the **Do not include drivers with Windows Updates** setting.

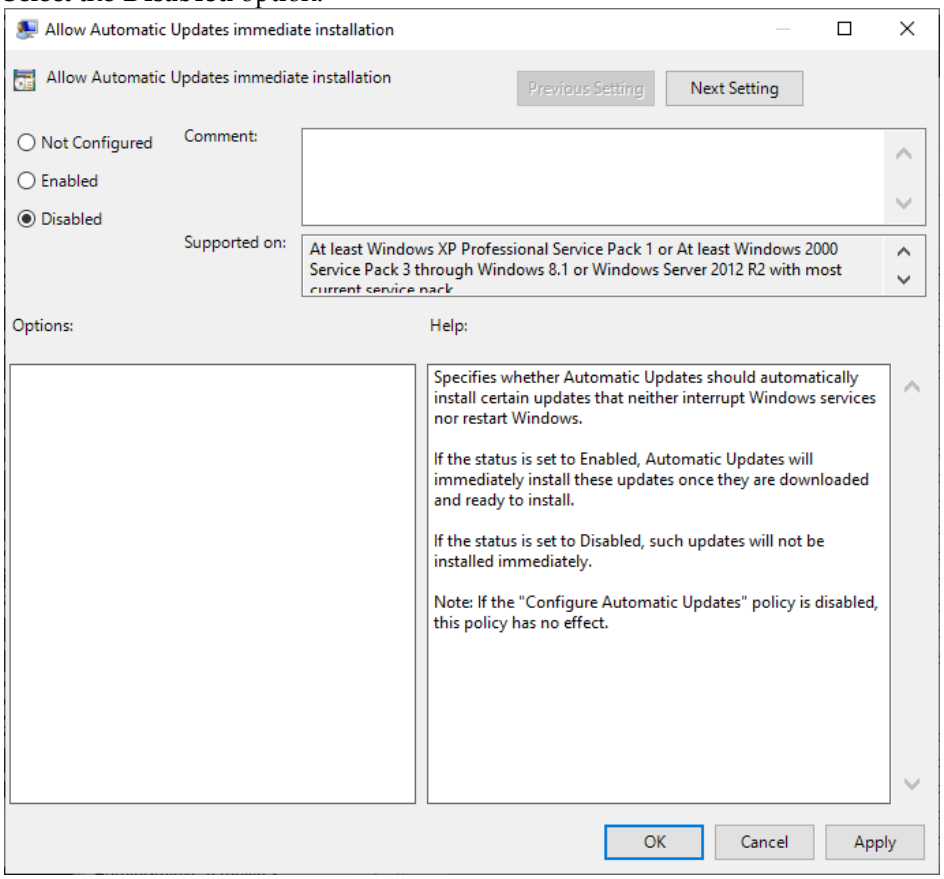
b. Select the **Enabled** option.




c. Select **OK** to apply policy settings.

7. Disable immediate installation of updates.
   a. Double-click the **Allow Automatic Updates immediate installation** setting.

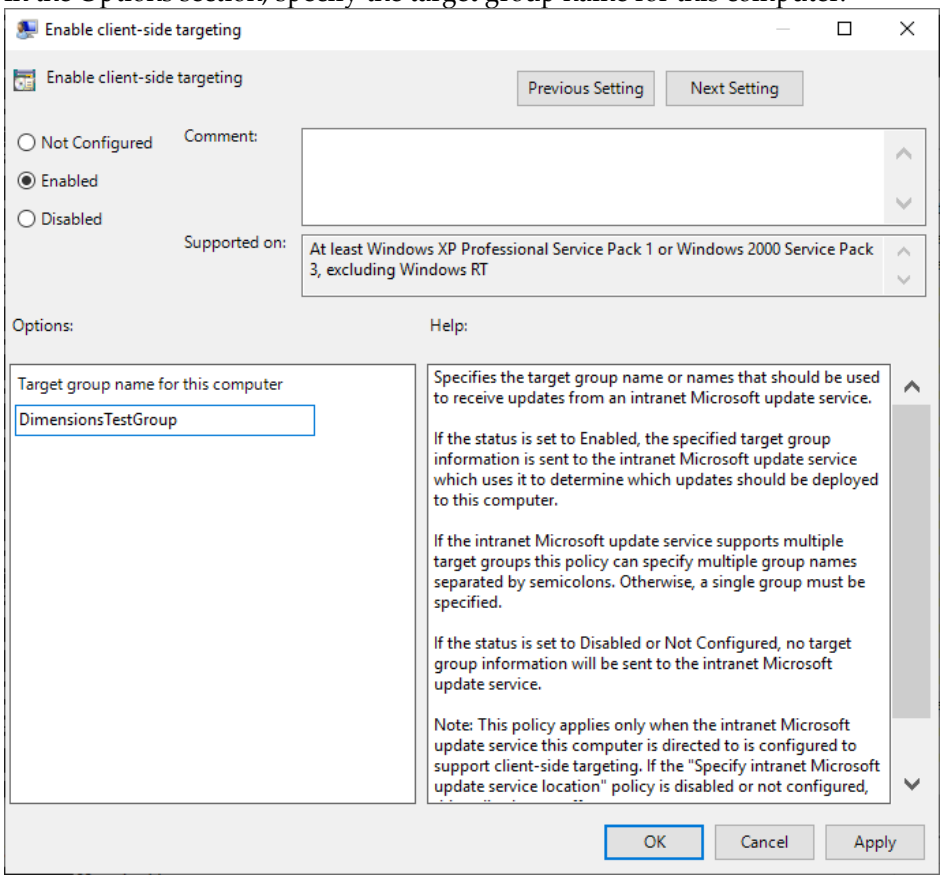
b. Select the **Disabled** option.




c. Select **OK** to apply policy settings.

8. Enable client-side targeting. Alternately, add the product system to a custom computer group on the WSUS Server before enabling the Windows Update service.
   **NOTE:** Configuring this option will depend on customer preference and WSUS Server configurations. Work with the System Administrator to configure this setting, if appropriate.
   a. Double-click the **Enable client-side targeting** setting.
   b. Select the **Enabled** option.

c. In the Options section, specify the target group name for this computer.



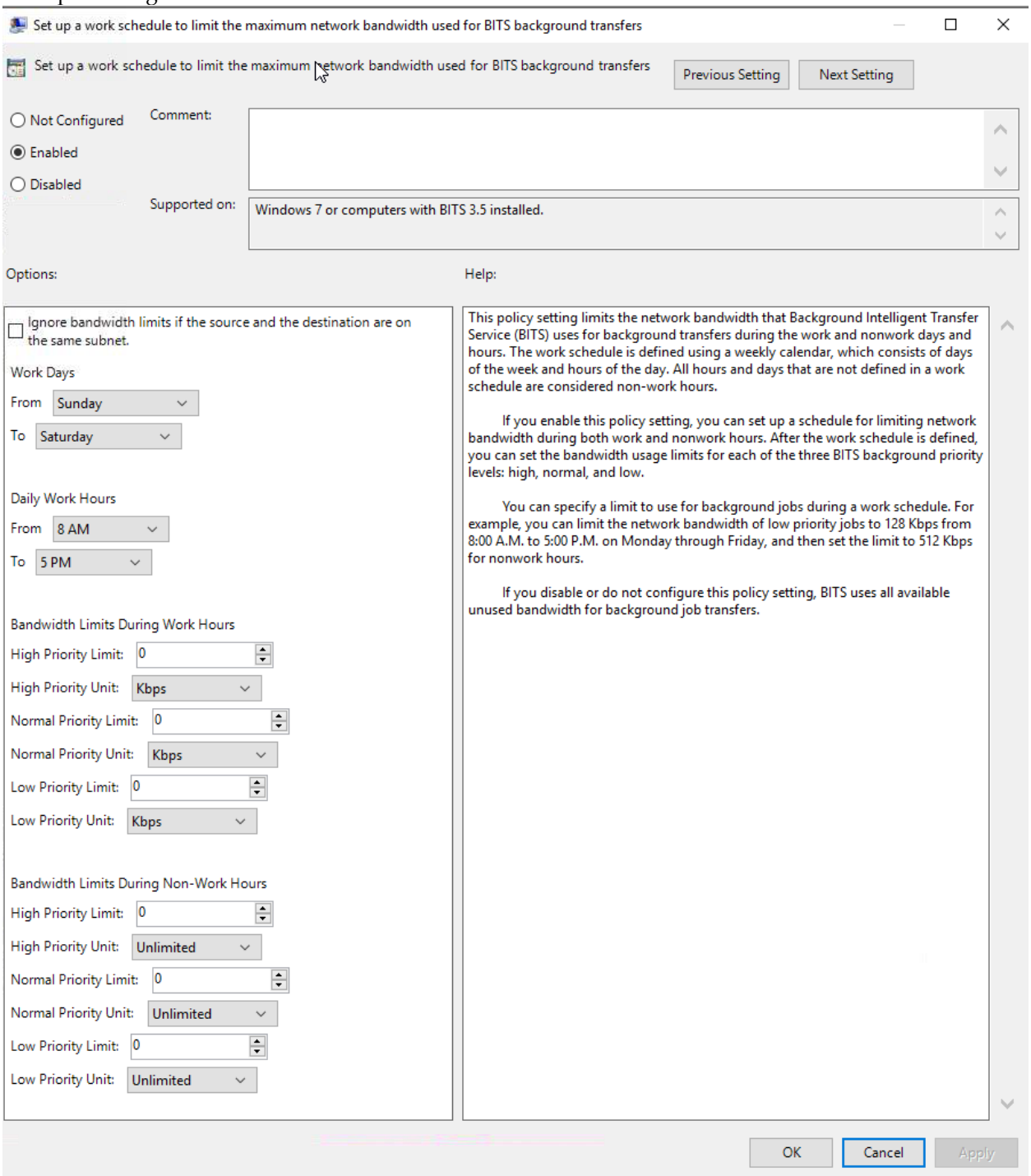

d. Select **OK** to apply policy settings.

## Restrict Download Hours for Windows Updates

To limit negative performance impact to the Hologic product, limit download bandwidth for Windows Updates during hours of active use for the product.

1. In the *Local Group Policy Editor* window, expand each item to navigate to **Computer Configuration > Administrative Templates > Network > Background Intelligent Transfer Service (BITS)**.
2. Double-click the **Set up a work schedule to limit the maximum network bandwidth used for BITS background transfers** setting.
3. Select the **Enabled** option.
4. In the Options section, set 'Work Days' to appropriate values, for example, from Sunday to Saturday.
5. Set 'Daily Work Hours' according to active use hours of the product system, for example, from 8 AM to 5 PM.
6. Set 'Bandwidth Limits During Work Hours' to limit 0 and unit Kbps (no download) for all options.

7. Example settings:

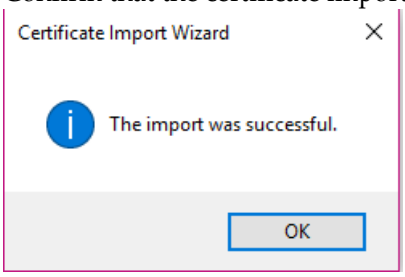



8. Select **OK** to save configurations.

## Install SSL/TLS Certificate

If the customer WSUS Server is configured to support or require SSL/TLS connections (recommended), the instructions within this section can be used to install the required certificate on the Hologic product system. Otherwise, skip this section.

1. Transfer the required certificate file (provided by IT or System Administrator) to the product system.
2. Double-click the certificate file. The *Certificate* window opens.
3. Select the **Install Certificate...** button.
4. In the *Certificate Import Wizard* window, select **Local Machine** and select **Next**.
5. In the Certificate Store dialog box, select **Place all certificates in the following store** and select **Browse**.
6. In the Selection dialog box, select **Trusted Root Certification Authorities** and select **OK**.
7. Select **Next**.
8. In the Completing dialog box, select **Finish**.
9. Confirm that the certificate import was successful and select **OK**.




10. Close all open windows.

## Clear WSUS Client Cache

When configuring a custom WSUS Server, the product system may discover stale updates prepared for installation. Follow these instructions to limit the updates installed to only those approved through the new custom WSUS Server.

1. Open File Explorer and navigate to the **C:\Windows\SoftwareDistribution\Download** directory.
2. Highlight all files and folders in this directory and delete them.

## Configure Windows Update Services

Once the product system has been configured to receive security patches from the custom WSUS Server, the Windows Update service needs to be enabled, set to automatically start, and be started.

1. Right-click the Windows Start button and select **Computer Management** from the menu.
2. In Computer Management, expand "Services and Applications" and select **Services**.
3. In the list of Services, locate and double-click the **Windows Update** service.
4. In the *Properties* window, set the startup type to **Automatic**, select **Apply**, select **Start**, and then select **OK** to save changes.
5. Confirm that the **Background Intelligent Transfer Service** is set to either start manually or automatically. Defaults to Manual startup type.
6. Confirm that the **Update Orchestrator Service** is set to either start manually or automatically. Defaults to Manual startup type.
7. Close all open windows.

## Test WSUS Connection

Now that all system configurations have been made, test the ability to connect to the custom WSUS Server and install updates.
**NOTE:** It can take a significant amount of time for the product system (WSUS client) to establish a connection with the WSUS Server that has been configured. Run the wuauclt command, as instructed below to perform an immediate sync before checking for updates.

1. Right-click the Windows Start button and select **Shut down or sign out > Restart**.
2. Log into Windows on the product system as a system administrator, for example, HologicService.
3. Open a command window and run the following command:
   `wuauclt /resetauthorization`
4. Right-click the Windows Start button and select **Search**. Type `update` and select **Check for updates** in the list of matches.
5. In the *Settings* window for Windows Update, select the **Check for updates** button. This may take several minutes to complete.
6. Confirm that no error messages are displayed and that available updates, if any, are downloaded and installed.
7. In the *Settings* window for Windows Update, the 'Last checked' details should match the current day and time.

# Resources

- Windows Update Group Policy Settings
  *https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#BKMK_PolSettings*

- WSUS Best Practices
  *https://support.microsoft.com/en-us/help/4490414/windows-server-update-services-best-practices*

- Guidance for Configuring WSUS
  *https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus*