

Customer WSUS Setup Instructions

For Breast & Skeletal Health Products RD-04022 Revision 001



Table of Contents

Introduction	3
Requirements	3
Recommendations	3
Configuring Hologic Product Systems	4
Temporarily Disable Windows Update Service	4
Configure Windows Update Group Policy Settings	4
Restrict Download Hours for Windows Updates	10
Install SSL/TLS Certificate	11
Clear WSUS Client Cache	
Configure Windows Update Services	
Test WSUS Connection	13
Resources	13

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 nonvalidated 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**.

configured Common Name (CN) in the SSL certificate.

- 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

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

Specify intranet N	Aicrosoft update s	ervice location	· · ·	—		×	
Specify intranet N	Microsoft update s	ervice location	Previous Setting Next Setting				
O Not Configured	Comment:						
Enabled							
 Disabled 						\sim	
	Supported on:	At least Windows X excluding Window	vice Pack 3,	,	$\hat{}$		
Options:			Help:				
Set the intranet upda	te service for dete	ting updates:	Specifies an intranet server to host undates f	from Micro	soft	~	
https://MYHOSTNAME:8531			Update. You can then use this update service to automatically update computers on your petwork				
Set the intranet statis	tics server:		This set is a later set of the se				
https://MYHOSTNA	ME:8531		function as an internal update service. The Autor	matic Upda	tes		
Set the alternate download server:			client will search this service for updates that app computers on your network.	bly to the			
			To use this setting, you must set two server	name value	es: the		
(example: http://lntra	anetUpd01)		server from which the Automatic Updates client downloads updates, and the server to which upd	detects and lated works	1 tations		
Download files wit	th no Url in the me	tadata if	upload statistics. You can set both values to be the	he same ser	rver. An		
alternate downloa	d server is set.		optional server name value can be specified to co Update Agent to download updates from an alte server instead of the intranet update service.	onfigure Wi rnate down	indows iload		
			If the status is set to Enabled, the Automatic	Updates cl	lient		
			connects to the specified intranet Microsoft upd alternate download server), instead of Windows	ate service Update, to s	(or search	~	
			ОК	Cancel	Appl	ly	

- 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).

Configure Automatic Update	es	- 0	×
Configure Automatic Update	es f	Previous Setting Next Setting	
O Not Configured Comment	t:		
Enabled			
O Disabled			~
Supporte	ed on: Windows XP Professional Servi	ce Pack 1 or At least Windows 2000 Service Pack 3	$\hat{\mathbf{v}}$
Options:		Help:	
Configure automatic updating:		Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.	^
4 - Auto download and schedule	e the install v	Note: This policy does not apply to Windows RT.	
selected.	equired and applicable if 4 is	This setting lets you specify whether automatic updates are enabled on this	
Install during automatic main	tenance	Group Policy Setting:	
Scheduled install day: 0 - Even	ry day 🗸 🗸	2 = Notify before downloading and installing any updates.	
Scheduled install time: 03:00	~	When Windows finds updates that apply to this computer, users will be	
If you have selected "4 – Auto d for your scheduled install day an	download and schedule the install" nd specified a schedule, you also	users can download and install any available updates.	
have the option to limit updating occurrence, using the options be	g to a weekly, bi-weekly or monthly elow:	3 = (Default setting) Download the updates automatically and notify when they are ready to be installed	
Every week		Windows finds updates that apply to the computer and downloads them in	
First week of the month		the background (the user is not notified or interrupted during this process). When the downloads are complete, users will be notified that they are ready to install.	
Second week of the month		After going to Windows Update, users can install them.	
Third week of the month		4 = Automatically download updates and install them on the schedule specified below.	
Fourth week of the month		When "Automatic" is selected as the scheduled install time. Windows will	
Install updates for other Micro	osoft products	automatically check, download, and install updates. The device will reboot as per Windows default settings unless configured by group policy. (Applies to Windows 10, version 1809 and higher)	~
		OK Cancel Appl	ly

- 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.

No auto-restart w	vith logged on use	rs for scheduled automatic updates installations	×
No auto-restart w Previous Setting	vith logged on use Next Setting	ers for scheduled automatic updates installations	
O Not Configured	Comment:	[~
Enabled			
○ Disabled			× .
	Supported on:	Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3	$\stackrel{\wedge}{\downarrow}$
Options:		Help:	
		Specifies that to complete a scheduled installation, Automatic Updates will wait for the computer to be restarted by any user who is logged on, instead of causing the computer to restart automatically. If the status is set to Enabled, Automatic Updates will not restart a computer automatically during a scheduled installation if a user is logged in to the computer. Instead, Automatic Updates will notify the user to restart the computer Be aware that the computer needs to be restarted for the updates to take effect.	^
		If the status is set to Disabled or Not Configured, Automatic Updates will notify the user that the computer will automatically restart in 5 minutes to complete the installation. Note: This policy applies only when Automatic Updates is	
		the "Configure Automatic Undates" policy is disabled this OK Cancel App	bly

- 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.

Do not include drivers with Windows Updates						×		
📆 Do not include dr	ivers with Window	/s Updates		Previous Setting	Next Setting			
O Not Configured	Comment:						~	
Enabled								
O Disabled							\sim	
	Supported on:	At least Window	t least Windows Server 2016 or Windows 10					
Options:			Help:					
			Enable this updates. If you disal will include Note: For o Windows S have to be	policy to not include ole or do not configur e updates that have a l levices running Windo erver 2016, this policy metry (that is, if the "// ces running Windows erver, version 1709 (or enabled for this policy	drivers with Windo e this policy, Windo Driver classification ows 10, version 160° only takes effect if Allow Telemetry" pr 10, version 1703 (o r later), telemetry dr y to take effect.	ws quality ws Update 7 or you blicy is not r later) or bes not	~	
				ОК	Cancel	Арр	ly	

- 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.

Allow Automatic Updates immediate installation — 🛛 🔿						×		
Allow Automatic	Updates immediat	e installation		Previous Setting	Next Setting			
O Not Configured	Comment:							~
O Enabled								
Disabled								× .
	Supported on:	At least Window Service Pack 3 t	t least Windows XP Professional Service Pack 1 or At least Windows 2000 ervice Pack 3 through Windows 8.1 or Windows Server 2012 R2 with most urrent service pack					
Options:			Help:					
			Specifies wi install certa nor restart V If the status immediatel and ready t If the status installed im Note: If the this policy I	hether Automatic Up in updates that neith Windows. : is set to Enabled, Au y install these update o install. : is set to Disabled, su mediately. "Configure Automat has no effect.	dates should auti er interrupt Wind itomatic Updates es once they are d ich updates will n tic Updates" polic	omati lows s will lownlo oot be	cally ervices oaded isabled,	∧
				ОК	Cance	I	Арр	ly

- 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.

Enable client-side	targeting				-	_		×
Enable client-side	targeting			Previous Setting	Next Setting			
O Not Configured	Comment:							~
Enabled								
 Disabled 								\sim
	Supported on:	At least Window 3, excluding Wi	ws XP Profess ndows RT	ional Service Pack 1	or Windows 2000	Servi	ce Pack	$\hat{}$
Options:			Help:					
Target group name fo	r this computer		Specifies th	e target group name updates from an intra	e or names that shanet Microsoft up	nould date	be used	^
DimensionsTestGroup	0		If the status information which uses to this com If the intrar target grou separated b specified. If the status group infor update serv Support clin update serv	s is set to Enabled, the n is sent to the intran it to determine whice puter. Set Microsoft update post his policy can sp by semicolons. Other s is set to Disabled or mation will be sent t rice. policy applies only w rice this computer is ent-side targeting. If rice location" policy	e specified target tet Microsoft upd th updates should service supports ecify multiple gro wise, a single gro Not Configured, to the intranet Mi when the intranet Mi directed to is cor the "Specify intra e dirabled or not	auto are see at a see a b e d multi oup n up m no ta croso Micro figur net N	ip invice leployed ames aust be arget ft osoft ed to dicrosoft invired	
			<u> . </u>	Oł	K Cance	el	Арр	ly

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.

- 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.

Customer WSUS Setup Instructions

For Breast & Skeletal Health Products

7. Example settings:

		\sim
Set up a work schedule to limit the maximum betwork bandwidth us	sed for BITS background transfers Previous Setting Next Setting	
O Not Configured Comment:		~
Enabled		
O Disabled		<u> </u>
Supported on: Windows 7 or computers with B	ITS 3.5 installed.	$\hat{\mathbf{v}}$
Options:	Help:	
Ignore bandwidth limits if the source and the destination are on the same subnet. Work Days From Sunday To Saturday Daily Work Hours From 8 AM To 5 PM Bandwidth Limits During Work Hours High Priority Limit: 0	This policy setting limits the network bandwidth that Background Intelligent Transfer Service (BITS) uses for background transfers during the work and nonwork days and hours. The work schedule is defined using a weekly calendar, which consists of days of the week and hours of the day. All hours and days that are not defined in a work schedule are considered non-work hours. If you enable this policy setting, you can set up a schedule for limiting network bandwidth during both work and nonwork hours. After the work schedule is defined, you can set the bandwidth usage limits for each of the three BITS background priority levels: high, normal, and low. You can specify a limit to use for background jobs during a work schedule. For example, you can limit the network bandwidth of low priority jobs to 128 Kbps from 8:00 A.M. to 5:00 P.M. on Monday through Friday, and then set the limit to 512 Kbps for nonwork hours.	^
High Priority Unit: Kbps Normal Priority Limit: 0 Normal Priority Unit: Kbps Low Priority Limit: 0 Low Priority Unit: Kbps Bandwidth Limits During Non-Work Hours		
High Priority Limit: 0 High Priority Unit: Unlimited Normal Priority Limit: 0 Normal Priority Unit: Unlimited Low Priority Limit: 0 Low Priority Unit: Unlimited Low Priority Unit: Unlimited		~

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
 <u>https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/4-configure-group-policy-settings-for-automatic-updates#BKMK_PolSettings</u>
- WSUS Best Practices
 <u>https://support.microsoft.com/en-us/help/4490414/windows-server-update-services-best-practices</u>
- Guidance for Configuring WSUS
 <u>https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus</u>