

The background image shows a man in a light blue shirt from the side, looking at a tablet. He is in a factory or industrial setting with various machines and equipment visible in the background. Overlaid on the image are several digital graphics: a '24/7' icon with a circular arrow, a 'NEWS' section with a person icon, a 'Home' button, and a large 'Industry Online Support' text. There are also binary code (0s and 1s) and network-like icons scattered throughout the digital overlay.

SIEMENS

Ingenuity for life

Windows updates on WinCC SCADA, IPC and other PC runtime systems

SIMATIC WinCC (TIA Portal), WinCC V7 and SIMATIC IPC

<https://support.industry.siemens.com/cs/ww/en/view/109754089>

Siemens
Industry
Online
Support



Legal information

Use of application examples

Application examples illustrate the solution of automation tasks through an interaction of several components in the form of text, graphics and/or software modules. The application examples are a free service by Siemens AG and/or a subsidiary of Siemens AG ("Siemens"). They are non-binding and make no claim to completeness or functionality regarding configuration and equipment. The application examples merely offer help with typical tasks; they do not constitute customer-specific solutions. You yourself are responsible for the proper and safe operation of the products in accordance with applicable regulations and must also check the function of the respective application example and customize it for your system.

Siemens grants you the non-exclusive, non-sublicensable and non-transferable right to have the application examples used by technically trained personnel. Any change to the application examples is your responsibility. Sharing the application examples with third parties or copying the application examples or excerpts thereof is permitted only in combination with your own products. The application examples are not required to undergo the customary tests and quality inspections of a chargeable product; they may have functional and performance defects as well as errors. It is your responsibility to use them in such a manner that any malfunctions that may occur do not result in property damage or injury to persons.

Disclaimer of liability

Siemens shall not assume any liability, for any legal reason whatsoever, including, without limitation, liability for the usability, availability, completeness and freedom from defects of the application examples as well as for related information, configuration and performance data and any damage caused thereby. This shall not apply in cases of mandatory liability, for example under the German Product Liability Act, or in cases of intent, gross negligence, or culpable loss of life, bodily injury or damage to health, non-compliance with a guarantee, fraudulent non-disclosure of a defect, or culpable breach of material contractual obligations. Claims for damages arising from a breach of material contractual obligations shall however be limited to the foreseeable damage typical of the type of agreement, unless liability arises from intent or gross negligence or is based on loss of life, bodily injury or damage to health. The foregoing provisions do not imply any change in the burden of proof to your detriment. You shall indemnify Siemens against existing or future claims of third parties in this connection except where Siemens is mandatorily liable.

By using the application examples you acknowledge that Siemens cannot be held liable for any damage beyond the liability provisions described.

Other information

Siemens reserves the right to make changes to the application examples at any time without notice. In case of discrepancies between the suggestions in the application examples and other Siemens publications such as catalogs, the content of the other documentation shall have precedence.

The Siemens terms of use (<https://support.industry.siemens.com>) shall also apply.

Security information

Siemens provides products and solutions with industrial security functions that support the secure operation of plants, systems, machines and networks.

In order to protect plants, systems, machines and networks against cyber threats, it is necessary to implement – and continuously maintain – a holistic, state-of-the-art industrial security concept. Siemens' products and solutions constitute one element of such a concept.

Customers are responsible for preventing unauthorized access to their plants, systems, machines and networks. Such systems, machines and components should only be connected to an enterprise network or the Internet if and to the extent such a connection is necessary and only when appropriate security measures (e.g. firewalls and/or network segmentation) are in place. For additional information on industrial security measures that may be implemented, please visit **Fehler! Linkreferenz ungültig..**

Siemens' products and solutions undergo continuous development to make them more secure. Siemens strongly recommends that product updates are applied as soon as they are available and that the latest product versions are used. Use of product versions that are no longer supported, and failure to apply the latest updates may increase customer's exposure to cyber threats.

To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed at: **Fehler! Linkreferenz ungültig..**

Table of contents

Legal information	2
1 Introduction	4
1.1 Overview.....	4
1.2 Principle of operation.....	5
2 Concept of Windows as a Service concept	7
2.1 Definitions.....	7
2.2 Different maintenance concepts.....	8
3 Explaining the Microsoft Windows Server Update Service (WSUS)	9
4 Update options.....	10
4.1 Manual loading of Windows updates	12
4.2 Using a WSUS server to distribute updates to multiple WinCC stations	15
4.2.1 Simple WSUS provision	15
4.2.2 Non-connected WSUS server (standalone operation)	15
4.3 Setting up the WSUS server	16
4.4 Setting up a WSUS client	18
4.4.1 Setting up a WSUS client within a domain.....	18
4.4.2 Setting up a WSUS client outside of a domain (in a workgroup)	18
5 Useful information	21
5.1 Windows 10 LTSC.....	21
5.2 Possible error codes of Windows clients.....	21
6 Appendix	22
6.1 Service and support	22
6.2 Links and literature	23
6.3 Change documentation	24

1 Introduction

1.1 Overview

SIMATIC IPCs and PC-based HMI systems

SIMATIC HMI systems are flexible and robust. The HMI systems are tested and approved for this purpose. The tests and approvals are generally carried out with defined Windows versions.

An overview of the compatibilities can be found in the compatibility tool.

www.siemens.com/kompatool

Availability and compatibility

One of the most important requirements of SIMATIC HMI systems is constant operability, and in the case of SIMATIC IPCs, constant availability.

The operability can be restricted if the Windows Update topic is not observed! For example, by unplanned installation of updates and a spontaneous restart of the system.

This application example deals with this and keeps your SIMATIC IPC and your SIMATIC HMI software at maximum availability.

Windows as a Service

Windows as a Service has changed the procedure for distributing Windows updates. Rather than delivering individual updates (KBs), Microsoft now supplies "Monthly Rollups". This type of update contains all of the updates of the previous months, which is why they are called cumulative updates.

Apart from this, the setting options for Windows updates have been changed. As standard, you cannot just install specific updates (KBs) but, rather, only the complete update packages. By contrast with the previous situation, the cumulative update process means that it is no longer possible to select individual or newer KBs.

Using the Microsoft Windows Server Update Service (WSUS), you can select individual classifications or updates to be installed, which gives you the option of selecting various updates.

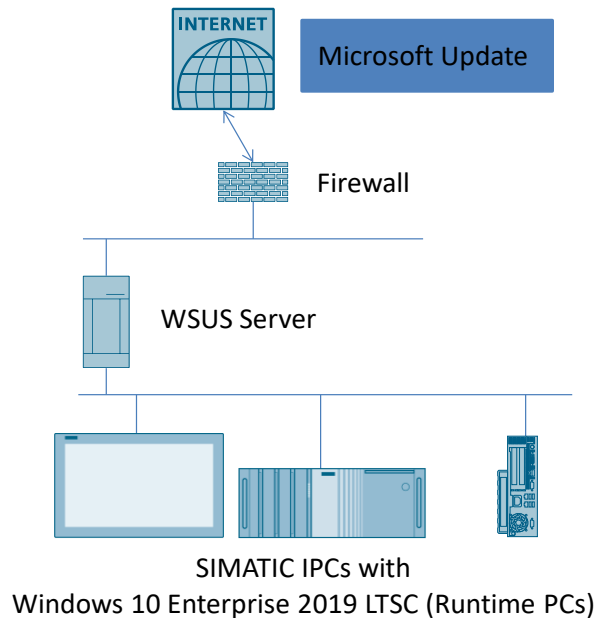
This document addresses the concept of Windows as a Service and demonstrates the possible options for getting Windows updates and the limitations inherent in this or the risks for the availability of WinCC Runtime stations.

Furthermore, different variants or servicing channels of Windows 10 are explained; it will be shown why Windows 10 Enterprise 2019 LTSC in connection with visualization software or SIMATIC IPCs from SIEMENS pose much lower risks than the other servicing channels.

1.2 Principle of operation

This application example is intended to show you how to configure a Microsoft Windows Server Update Service (WSUS) and set up the Windows clients for receiving Windows Updates via the WSUS. Ultimately, a possible scenario for updating Windows 10 Enterprise 2019 LTSC could look like this:

Figure 1-1



Components used

The application example was created and tested with Windows 10 Enterprise 2019 LTSC. Unless otherwise noted, all screenshots and instructions refer to Windows 10 Enterprise 2019 LTSC.

Theoretically, the described configurations and procedures are also possible with other Windows 10 versions or Windows 7.

Note

If you use versions other than Windows 10 Enterprise 2019 LTSC, test the functions thoroughly.

Software used

This generally applies to any SIMATIC WinCC software offered by Siemens, such as WinCC Runtime Advanced, WinCC Runtime Professional or WinCC V7.

Table 1-1

Component	Quantity	Item number	Note
WinCC V7.4 SP1	1	6AV63.1-....7-4...	Update2
Windows Server 2019 (used as a WSUS)	1		WSUS server
Windows 10 Enterprise 2019 LTSC	1		Any other Windows LTSC is possible.

Note

As of 2019, Microsoft will name the recommended Windows 10 Servicing Channel "LTSC" (Long-Term Servicing Channel) and no longer "LTSB" (Long-Term Servicing Branch).

This document refers to the operating systems released at the time of creation and still uses the term "LTSC". In this document, the two terms "LTSC" and "LTSB" are to be regarded as synonyms.

2 Concept of Windows as a Service concept

"Windows as a Service" is a new concept introduced with Windows 10. While "Windows as a Service" is explained in detail in a comprehensive [documentation series](#), this document provides an overview of the most important concepts.

2.1 Definitions

Within the scope of Windows as a Service, Microsoft has introduced several new terms:

Feature updates (Creators Updates)

- These updates are published twice a year (in March and September approximately).
- Include new features for Windows 10.
- In comparison to older versions of Windows, a Creators Update is equivalent to a new version of Windows. (For example, Windows Vista to Windows 7)

Quality Updates

- Are published monthly.
- In addition to security patches, they also contain other patches.
- Are cumulative.

Insider Preview Builds

- They are made available during the development of functions that will be part of the next function update (Feature Update).
- This make it possible for organizations to check new functions and their compatibility with existing apps and infrastructure components.
- It is possible to give feedback to Microsoft about problems.

Servicing Channels

- Make it possible for organizations themselves to choose the time for providing new features.
- The Long-Term Servicing Channel (LTSC) has been developed exclusively for use with specialized devices. It is given new functional versions approximately every three years.

Deployment rings

These are groups of devices that are initially used in an organization for pilot provisions of individual function updates (feature updates) and then for general deployments of the same.

Further information can be found here in the overview "[Windows as a Service](#)". You can find a more detailed overview of the various Servicing Channels on the [Microsoft pages](#).

2.2 Different maintenance concepts

Windows 10 has two servicing channels for alignment with this new concept of update provisioning. In each case, these channels demonstrate a different degree of flexibility for transferring these updates to client computers.

Microsoft currently offers the following two servicing options.

- **SAC:** Semi-Annual Channel (Standard)
- **LTSC:** Long-Term Servicing Channel
→ Recommended with SIMATIC IPCs which run critical runtime software. An example are WinCC SCADA systems.

Microsoft does not release function updates (Feature Updates) on devices that are running Windows 10 Enterprise LTSC. Instead of this, the company generally offers new LTSC versions every 2 to 3 years. Over a lifecycle of 10 years, organizations can decide whether they want to install these versions as direct upgrades or skip them completely.

Security updates and hotfixes are delivered immediately for both Servicing Channels on a regular basis.

Note

Because **no function updates (Feature Updates) are installed with Windows 10 Enterprise LTSC**, no unforeseen incompatibilities with WinCC will occur. Therefore, this Servicing Channel (LTSC) is recommended when using WinCC and other runtime software on SIMATIC IPCs.

CAUTION

If you do not use a WSUS server to install the updates, this can result in unplanned reboots. Since the change in Windows update behavior, updates may be loaded on an unplanned basis.

In conjunction with SIMATIC WinCC products or your applications on SIMATIC IPCs, this can lead to the following problems:

- **Data loss of archive data**
- **Associated incompatibilities through Feature Updates**

3 Explaining the Microsoft Windows Server Update Service (WSUS)

WSUS is a Windows Server role that is available in Windows server operating systems.

Properties of WSUS:

- Provides a central hub for Windows updates within an organization.
- Allows companies to defer updates and to approve them selectively.
- Administrators choose the time of provision and specify it.
- Administrators choose the devices that are to be updated.
- Provides additional control over Windows Update for Business; however, it does not contain all of the time planning options and flexibility at provision that you get with the System Center Configuration Manager.

When selecting WSUS as the source for Windows updates, use Group Policy (see 4.4) to direct Windows 10 client devices to the WSUS server for their updates. From there, updates are periodically downloaded to the WSUS server and managed, approved, and deployed through the WSUS Management Console or Group Policy, simplifying update management settings.

Note

There are no additional license costs, since WSUS is a component of a licensed Windows Server operating system.

4 Update options

Amongst others, the options listed below are available to obtain updates for Microsoft-supported operating systems:

Table 4-1

Option	Risk of unplanned reboots	Effort	Security risk	Recommended
PC runtime systems / IPCs on the internet	Very high	Very low	Very high	Not recommended for ES or OS due to possible data loss because of unplanned reboot
PC runtime systems / IPCs offline without manual updates	Not available	None	Very high	Not recommended
PC runtime systems / IPCs offline with manual updates	Not present, since user-controlled	Very high	Low	Not to be recommended for large IT infrastructures, as high effort is required for manual import of updates (see 4.1)
Using a WSUS server for distributing updates to multiple WinCC stations (WSUS online, PC runtime systems / IPCs offline)	Not present, since user-controlled	Low	Low	Recommended, since no unplanned restarts, but support with current and tested updates (see 4.2)
Using a WSUS server for distributing updates to multiple WinCC stations (WSUS offline, PC runtime systems / IPCs offline)	Not present, since user-controlled	Medium	Low	Recommended (if island operation is desired) due to no unplanned restarts and support with current and tested updates (see 4.2)

Depending on the number of clients (with runtime) that there are on your network, you need to decide whether it is sensible to use a WSUS or you prefer to load updates manually.

CAUTION

Do not use Windows 10 Enterprise 2019 LTSC, but Windows 10 SAC will get Windows 10 updates from other Windows 10 PCs on the local network that have already received this update.

(This is a new feature of the Windows 10 Update concept.)

This may cause you to lose compatibility with SIMATIC WinCC.

Chapters 4.1 or 4.4 describe different ways to avoid this behavior.

4.1 Manual loading of Windows updates

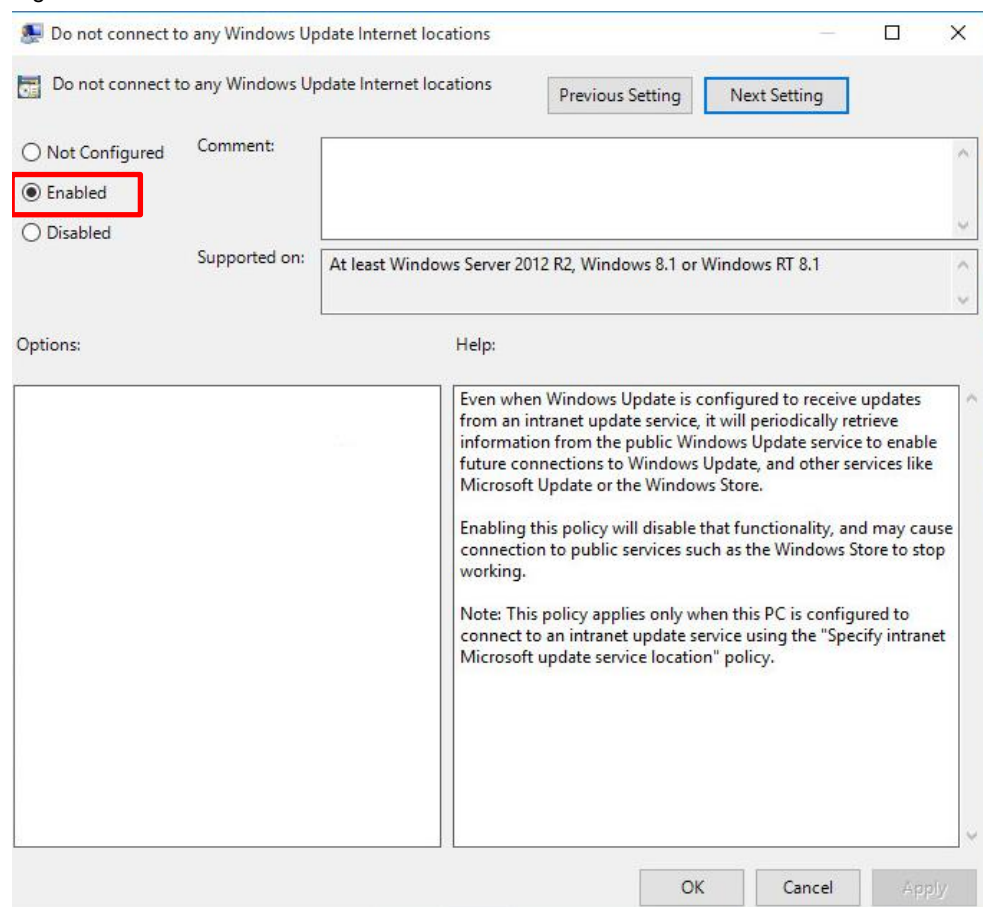
Note

If your PC runtime system / IPC is connected to the internet and automatic updates are disabled, you are responsible for installing your own Security Updates.

If you decide to load updates manually, proceed as follows:

In the editor for local group policies (gpedit.msc), navigate to Computer Configuration>Administrative Templates>Windows Components>Windows Update and make the following setting:

Figure 4-1

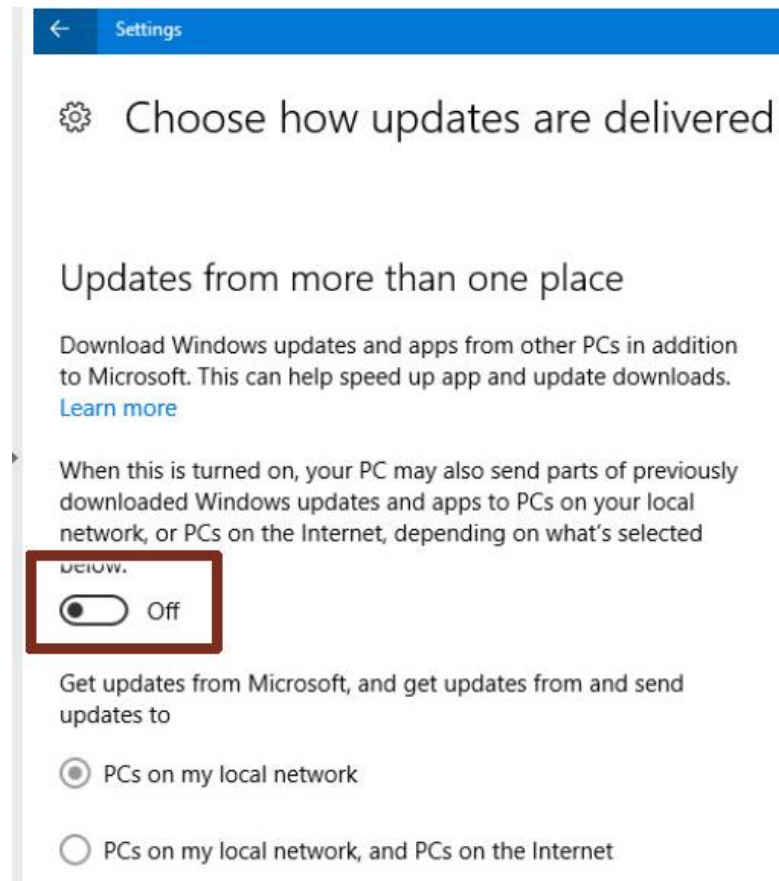


Alternatively, the computer is disconnected from the internet and updates are loaded using another computer.

For Windows 10 SAC, an additional setting must be made at this point. This is because updates can be obtained from other PCs that have already downloaded Windows Update. To do this, you have to navigate to Windows Update -> Advanced Options -> Choose how updates are delivered.

Disable this option to prevent your PC from downloading a newer Windows Update from another PC on the local network.

Figure 4-2



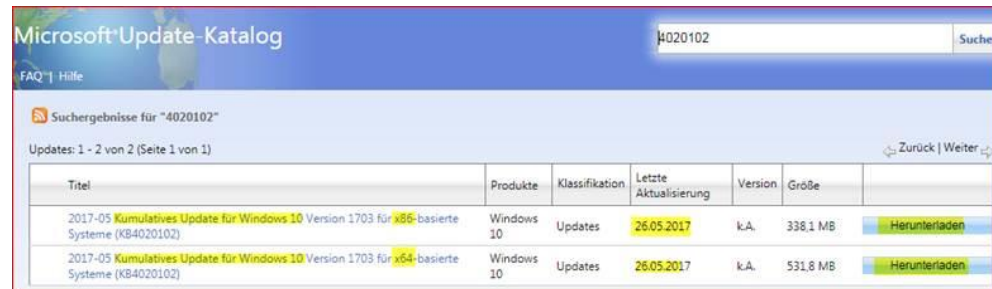
Option 1: Download to another PC via Microsoft Update Catalog

Visit the link below (Microsoft Update Catalog) to choose the updates that you want to install:

<http://www.catalog.update.microsoft.com/Home.aspx>

Requirements: The patch name is known in order to be able to search for it in the Microsoft Update Catalogue (e.g.: KB4020102).

Figure 4-3



The screenshot shows the Microsoft Update Catalog search results for the update KB4020102. The search bar at the top contains the text '4020102'. Below the search bar, the results are displayed in a table with columns: Titel, Produkte, Klassifikation, Letzte Aktualisierung, Version, Größe, and a download button. Two results are shown, both for Windows 10 Version 1703.

Titel	Produkte	Klassifikation	Letzte Aktualisierung	Version	Größe	
2017-05 Kumulatives Update für Windows 10 Version 1703 für x86-basierte Systeme (KB4020102)	Windows 10	Updates	26.05.2017	k.A.	338,1 MB	Herunterladen
2017-05 Kumulatives Update für Windows 10 Version 1703 für x64-basierte Systeme (KB4020102)	Windows 10	Updates	26.05.2017	k.A.	531,8 MB	Herunterladen

You can use an external device to transfer the file to your runtime computer and install it there.

4.1.2 Option 2: Installation using "WSUS Offline Update" open-source software:

You can download the software by visiting one of the following links:

- <https://www.heise.de/download/product/wsus-offline-update-ct-offline-update-38170>
- http://www.chip.de/downloads/WSUS-Offline-Update_38943162.html
- <http://www.wsusoffline.net/docs/>

The "update generator" downloads all of the current updates for different operating systems or for the ones you select. Then he creates the file: "UpdateInstaller.exe" which must be started on a (offline) target computer. The file can also be located on a USB drive or a USB hard drive.

4.2 Using a WSUS server to distribute updates to multiple WinCC stations

Amongst other things, it offers the options below for supplying clients with updates:

4.2.1 Simple WSUS provision

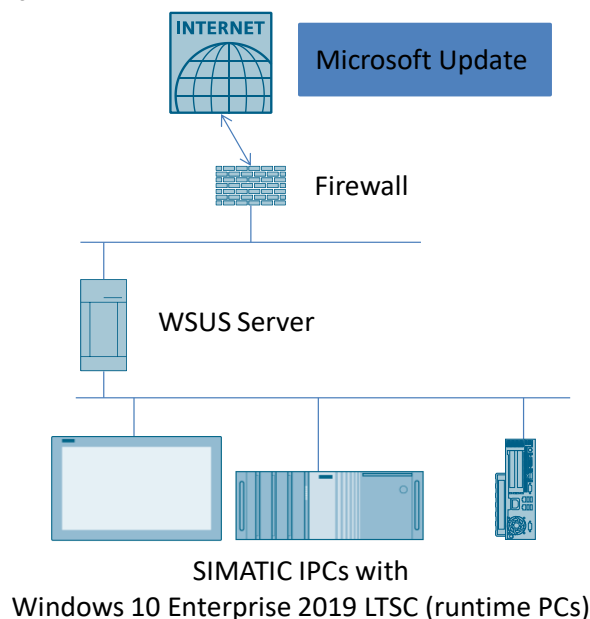
The simplest WSUS provision option consists of a server inside a company firewall that processes updates for client computers on a "private" Intranet. The WSUS connects to Microsoft Update to download updates. This process is called synchronization.

During synchronization, the WSUS checks whether new updates have become available since the last synchronization. At initial synchronization of WSUS, all of the updates are available for downloading.

The illustration below shows a simple WSUS server scenario in which the administrator has set up a server with WSUS inside the company firewall. This WSUS synchronizes directly with the Microsoft update service and distributes the updates to the client computers.

The illustration below shows the workflow in schematic form:

Figure 4-4



4.2.2 Non-connected WSUS server (standalone operation)

If access to the Internet is limited due to company guidelines or for any other reasons, administrators can set up an internal server for WSUS. An example of this is if a server is connected to the Intranet but is isolated from the Internet. After the updates have been downloaded to this server and been tested and approved, administrators export update metadata and contents to data media. After this, the

update metadata and contents are imported from the data carrier or media to the WSUS server on the Intranet.

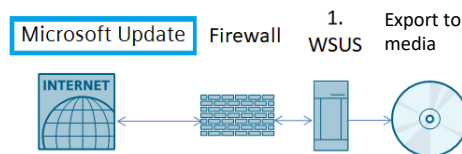
Note

This variant lends itself to use in standalone operation.

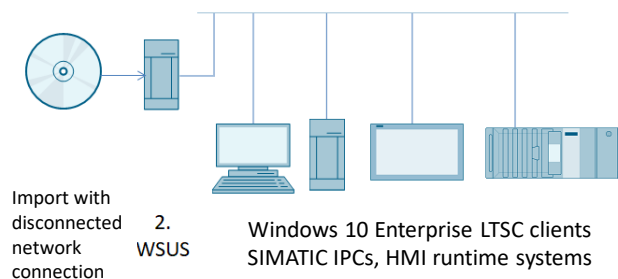
Figure 4-5

Workflow

1. Backup updates to medium



2. Distributing updates to clients



Note

To find out about possible WSUS server deployment scenarios, visit:

[https://msdn.microsoft.com/en-us/library/hh852344\(v=ws.11\).aspx](https://msdn.microsoft.com/en-us/library/hh852344(v=ws.11).aspx)

4.3 Setting up the WSUS server

On the Microsoft Pages, you can find a detailed guide that shows you how to install and configure the WSUS:

Step 1: Prepare WSUS deployment

- Windows Server 2019 and older: <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/deploy-windows-server-update-services>

Step 2: Install the WSUS server role

- Windows Server 2019 and older: <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/1-install-the-wsus-server-role>

Step 3: Configure WSUS

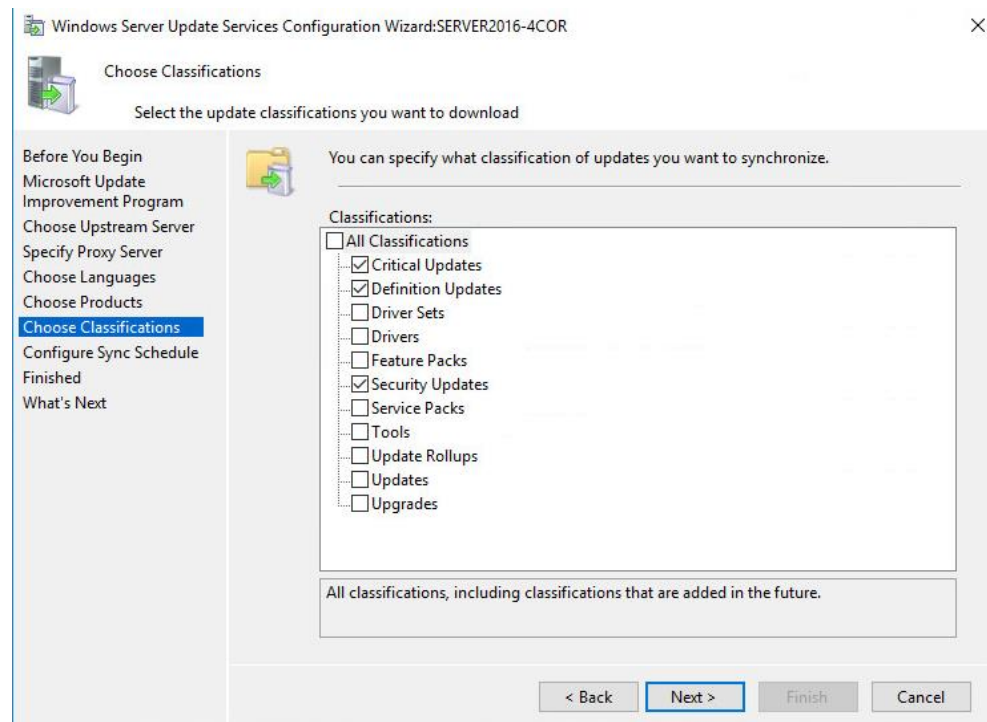
- Windows Server 2019 and older: <https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/deploy/2-configure-wsus>

Note

Use the Windows Server Updates Services Configuration wizard to make it easier to configure the WSUS servers. This guides you to your goal on a step-by-step basis. Please be aware that establishing contact with the Microsoft upstream server for the first time (step 3 in the Windows server updates service configuration wizard) can take some time.

Note that you must make the classifications below in the Windows Server Update Services Configuration Wizard:

Figure 4-6

**Note**

These settings prevent feature updates.

Step 4: Approve and deploy WSUS updates

Follow the link below to see how to approve updates for Windows 10 clients in a domain.

<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus>

Note

By approving updates, you choose which updates are to be installed on your clients. If you are using Windows 10 SAC, the Feature Updates can be "blocked".

4.4 Setting up a WSUS client

4.4.1 Setting up a WSUS client within a domain

For more information on this topic, visit the link below and refer to the point entitled Configure automatic updates and update service location:

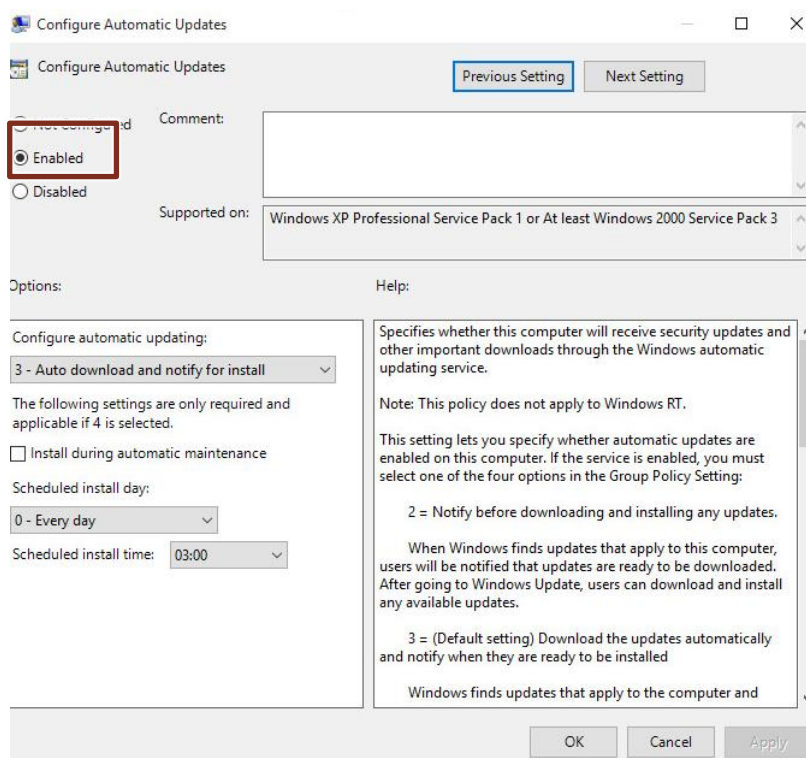
<https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus>

4.4.2 Setting up a WSUS client outside of a domain (in a workgroup)

Refer to the settings below as an example for a Windows 10 LTSC client. To make the correct settings on the client, proceed as follows:

1. Press the Windows key on your keyboard and start the editor for local group policies by entering gpedit.msc. The editor for local group policies opens.
2. Navigate to Computer Configuration>Administrative Templates>Windows Components>Windows Update.
3. Open "Configure Automatic Updates" in the settings by double-clicking. The "Configure Automatic Updates" dialog opens.

Figure 4-7



- In the "Options" area, specify the "Microsoft update service location":

Figure 4-8

Specify intranet Microsoft update service location

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3, excluding Windows RT

Options:

Set the intranet update service for detecting updates:

Set the intranet statistics server:

 (example: http://IntranetUpd01)

Help:

Specifies an intranet server to host updates from Microsoft Update. You can then use this update service to automatically update computers on your network.

This setting lets you specify a server on your network to function as an internal update service. The Automatic Updates client will search this service for updates that apply to the computers on your network.

To use this setting, you must set two servername values: the server from which the Automatic Updates client detects and downloads updates, and the server to which updated workstations upload statistics. You can set both values to be the same server.

If the status is set to Enabled, the Automatic Updates client connects to the specified intranet Microsoft update service, instead of Windows Update, to search for and download updates. Enabling this setting means that end users in your organization don't have to go through a firewall to get updates, and it gives you the opportunity to test updates before deploying

OK Cancel Apply

- Not Allowing Access to Windows Update Internet Locations

Figure 4-9

Do not connect to any Windows Update Internet locations

Previous Setting Next Setting

☐ Not Configured ☒ Enabled ☐ Disabled

Comment:

Supported on: At least Windows Server 2012 R2, Windows 8.1 or Windows RT 8.1

Options:

Help:

Even when Windows Update is configured to receive updates from an intranet update service, it will periodically retrieve information from the public Windows Update service to enable future connections to Windows Update, and other services like Microsoft Update or the Windows Store.

Enabling this policy will disable that functionality, and may cause connection to public services such as the Windows Store to stop working.

Note: This policy applies only when this PC is configured to connect to an intranet update service using the "Specify intranet Microsoft update service location" policy.

OK Cancel Apply

Note

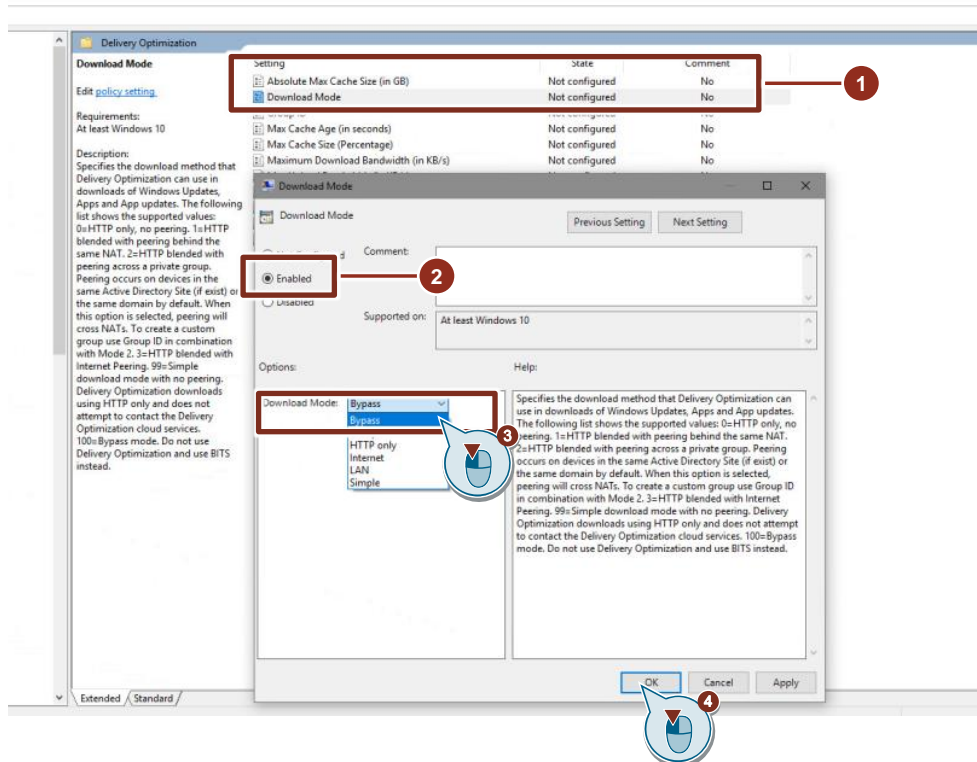
With the button "Next Setting" you can click through the different settings and confirm with "Apply".

Result

After restarting the Windows client, the policies are active and you can manage updates on a central basis from the WSUS server. This means that you must release the updates on the server.

For **Windows 10 SAC** (version 1511 onward) a further setting must be made here in connection with the WSUS. To do this, navigate to Computer Configuration > Administrative Templates > Windows Components > Delivery Optimization and set the Download Mode policy so that the client uses "Bypass" mode to transfer Windows updates only from WSUS.¹

Figure 4-10

**Note**

With newer Windows versions the download mode is called "Bypass (100)".

¹ <https://blogs.technet.microsoft.com/mniehaus/2016/08/16/windows-10-delivery-optimization-and-wsus-take-2/> retrieved on 2/8/2019

5 Useful information

5.1 Windows 10 LTSC

Security updates and fixes are provided at regular intervals. Customers in the Long Term Servicing Channel (LTSC) receive security updates and critically fixes for a period of 10 years.

Customers can migrate from one Windows 10 Enterprise LTSC to the next via In Place Upgrade, and a Windows 10 Enterprise LTSC version can also be skipped.

Note

The use of Windows 10 Enterprise LTSC in connection with SIMATIC WinCC products is expressly recommended, as in this case no Feature Updates (Creators Updates) are installed.

It is advisable to manage the tested updates using WSUS or to load them manually to ensure system availability.

The more extensive the IT infrastructure is, the more sensible it is to update manually or to use the WSUS.

5.2 Possible error codes of Windows clients

There are a number of possible error codes.

To get more detailed information, it is helpful to check your Windows Update logs to localize the error and to eliminate it.

To do this, open the Power Shell with administrator rights and enter "Get-WindowsUpdateLog".

The system saves the log to the administrator's Desktop; the file usually contains further information.

To find solutions, please contact Microsoft Support or visit the Microsoft Forum.

6 Appendix

6.1 Service and support

Industry Online Support

Do you have any questions or need assistance?

Siemens Industry Online Support offers round the clock access to our entire service and support know-how and portfolio.

The Industry Online Support is the central address for information about our products, solutions and services.

Product information, manuals, downloads, FAQs, application examples and videos – all information is accessible with just a few mouse clicks:

<https://support.industry.siemens.com>

Technical Support

The Technical Support of Siemens Industry provides you fast and competent support regarding all technical queries with numerous tailor-made offers – ranging from basic support to individual support contracts. Please send queries to Technical Support via Web form:

www.siemens.com/industry/supportrequest

SITRAIN – Training for Industry

We support you with our globally available training courses for industry with practical experience, innovative learning methods and a concept that's tailored to the customer's specific needs.

For more information on our offered trainings and courses, as well as their locations and dates, refer to our web page:

www.siemens.com/sitrain

Service offer

Our range of services includes the following:

- Plant data services
- Spare parts services
- Repair services
- On-site and maintenance services
- Retrofitting and modernization services
- Service programs and contracts

You can find detailed information on our range of services in the service catalog web page:

Fehler! Linkreferenz ungültig.

Industry Online Support app

You will receive optimum support wherever you are with the "Siemens Industry Online Support" app. The app is available for Apple iOS, Android and Windows Phone:

Fehler! Linkreferenz ungültig.

6.2 Links and literature

Table 6-1

No.	Subject
\1\	Siemens Industry Online Support https://support.industry.siemens.com
\2\	Link to the article page of the application example https://support.industry.siemens.com/cs/ww/en/view/109754089
\3\	A comprehensive range of documentation about Windows as a Service https://docs.microsoft.com/en-us/windows/deployment/update/index
\4\	Overview of Windows as a Service https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview
\5\	Overview of the various Servicing Channels. https://blogs.technet.microsoft.com/askpfeplat/2016/08/30/a-bit-about-the-windows-servicing-model/
\6\	Configuring Windows Update for Business https://docs.microsoft.com/en-us/windows/deployment/update/waas-configure-wuflb
\7\	Visit the link below (Microsoft Update Catalog) to choose the updates that you want to install. http://www.catalog.update.microsoft.com/Home.aspx
\8\	To find out about possible WSUS server deployment scenarios, visit https://msdn.microsoft.com/en-us/library/hh852344(v=ws.11).aspx
\9\	Prepare WSUS deployment https://msdn.microsoft.com/en-us/library/hh852344(v=ws.11).aspx
\10\	Install the WSUS server role https://msdn.microsoft.com/en-us/library/hh852338(v=ws.11).aspx
\11\	Configure WSUS https://msdn.microsoft.com/en-us/library/hh852346(v=ws.11).aspx
\12\	Approve and deploy WSUS updates https://technet.microsoft.com/en-us/library/hh852348(v=ws.11).aspx
\13\	Deploying Windows 10 updates with Windows Server Update Services https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus
\14\	Compatibility list https://support.industry.siemens.com/kompatool/pages/main/index.jsf?sitc=wwdfi10001
\15\	Windows 10 Delivery Optimization without WSUS https://support.microsoft.com/en-us/help/4468254/windows-update-delivery-optimization-faq
\16\	Windows 10 Delivery Optimization with WSUS https://blogs.technet.microsoft.com/mniehaus/2016/08/16/windows-10-delivery-optimization-and-wsus-take-2/

6.3 Change documentation

Table 6-2

Version	Date	Change
V1.0	02/2018	First version
V1.2	02/2019	Windows 10 Delivery Optimization for Windows 10 CB and CBB updated
V1.3	07/2020	Update and adaptation for Service Channel SAC