SIEMENS
Ingenuity for life

Handling Windows Updates with WinCC SCADA Systems

SIMATC WinCC / V7/TIA / WSUS Windows Updates

https://support.industry.siemens.com/cs/ww/de/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 https://www.siemens.com/industrialsecurity.

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: https://www.siemens.com/industrialsecurity.

Table of contents

1 Introduction

1.1 Overview

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 can not 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.

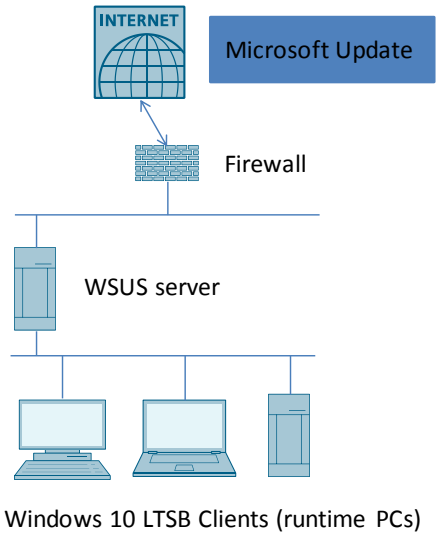
This document addresses the concept of Windows as a Service and demonstrates the possible options for getting Windows updates and the limitations inherent in this or the risks for WinCC Runtime stations.

Apart from this, we will explain different variants or Servicing Channels of Windows 10 and demonstrate why Windows10 LTSB in conjunction with SIEMENS visualization software is much less risky than the other Servicing Channels.

1.2 Mode of operation

This example application is intended to show you how to configure a Microsoft Windows Server Update Service (WSUS) and the Windows clients for receiving Windows Updates via the WSUS. In the end, a possible scenario for providing updates for Windows 10 LTSB Clients could look like this:

Figure 1-1



1.3 Components used

This application example has been created using the hardware and software components below.

This configuration is an example. You can use all of the operating systems that Microsoft supports with the WSUS server.

Hardware used

Table 1-1

Components	Quantity	Article number	Note
Windows Server 2016 (used as a WSUS)	1	-	Windows Server 2012 R2 is also possible
Windows10 LTSB (Build 1507)	1	-	Any other LTSB operating system is possible

Software used

This applies in general to all of the SIMATIC WinCC Software (TIA Portal Advanced, TIA Portal Professional) published by Siemens.

Table 1-2

Components	Quantity	Article number	Note
WinCC V7.4 SP1	1	6AV63.1-....7-4...	Update 2

2 Windows as a Service concept[1]

Windows as a Service is a new concept that was introduced in Windows 10. While Windows as a Service is explained in detail in a comprehensive range of documents, this document will give you 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).
- Contain new functions for Windows 10.

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.
- 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 Semi-Annual Channel receives feature updates twice per year (Current Branch and Current Branch for Business).
- The Long-Term Servicing Channel (LTSC) has been developed exclusively for use with specialized devices. It is given new function 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 provisions.

For more information on this topic, refer to the overview of "Windows as a service".

You can find a more detailed overview of the various Servicing Channels on the Microsoft pages.

[1] https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview retrieved 27.12.2017

2.2 Different maintenance concepts[2]

To align with this new update provision concept, Windows10 has three Servicing Channels. In each case, these channels demonstrate a different degree of flexibility for transferring these updates to client computers.

Follow the link below to visit a description of how to configure your Windows 10 system to the Current Branch for Business Servicing Channel:

https://docs.microsoft.com/en-us/windows/deployment/update/waas-configure-wufb

Microsoft never issues function updates on devices running Windows10 Enterprise LTSB. Instead of this, the company generally offers new LTSC versions every two to three years. Over a lifecycle of ten 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 all three branches on a regular basis.

Note

Since no function updates are installed with LTSB, unforeseen incompatibilities can occur with WinCC. This means that we expressly recommend using this Servicing Channel (LTSB) for WinCC.

NOTICE

If you do not use a WSUS server to 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, this can lead to the following problems:

- **Data loss of archive data**
- **Associated incompatibilities due to Feature Updates**

[2] https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview#servicing-channels

The table below shows the different servicing options with Siemens recommendations:

Table 2-1

Servicing Option	Availability of the feature upgrades	Minimum length of the service period	Main benefits	Supported versions	Recommended in conjunction with SIEMENS visualization software
Current Branch (CB)	Immediately after being published by Microsoft	Approximately 4 months	Makes functions available to users as quickly as possible	Home, Pro, Education, Enterprise, IoT Core, Windows 10 IoT Core Pro (IoT Core Pro)	No
Current Branch for Business (CBB)	Approximately 4 months after being published by Microsoft	Approximately 8 months	Provides additional time to test new feature upgrades before provision	Pro, Education, Enterprise, IoT Core Pro	No
Long-Term Servicing (LTSB)	Immediately after being published by Microsoft	10 years	Makes it possible to provide selected Windows 10 versions in the long-term in configurations with fewer changes	Enterprise LTSB	Yes

3 Explaining the Microsoft Windows Server Update Service (WSUS)[3]

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 the group policy (for more information on this topic, refer to chapter 4.4) to refer Windows 10 client devices to the WSUS server for your updates. At regular intervals, updates are downloaded from there to the WSUS Server where they are managed and approved and made available via the WSUS administration console or the group policy, which makes it easy to make update administration settings.

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

[3] https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus (retrieved 2017-12-27)

4 Update options[4]

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
Runtime PCs on the Internet	Very high	Very low	Very high	Not recommended for ES or OS due to possible data loss because of unplanned reboot
Runtime PCs offline without manual updates	Not available	None	Very high	Not recommended
Runtime PCs offline with manual updates	Not present, since user-controlled	Very high	Low	Not recommended for large-scale IT infrastructures, since more effort is needed to load updates manually (see 4.1)
Using one WSUS server to distribute updates to several WinCC stations (WSUS online, RT PCs offline)	Not present, since user-controlled	Low	Low	Recommended, since there are no unplanned reboots and current tested updates are supplied (see 4.2)
Using one WSUS server to distribute updates to several WinCC stations (WSUS offline, RT PCs offline)	Not present, since user-controlled	Medium	Low	Recommended (if standalone operation is desired), since there are no unplanned reboots and current tested updates are supplied (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.

[4] https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview#servicing-channels retrieved 27.12.2017

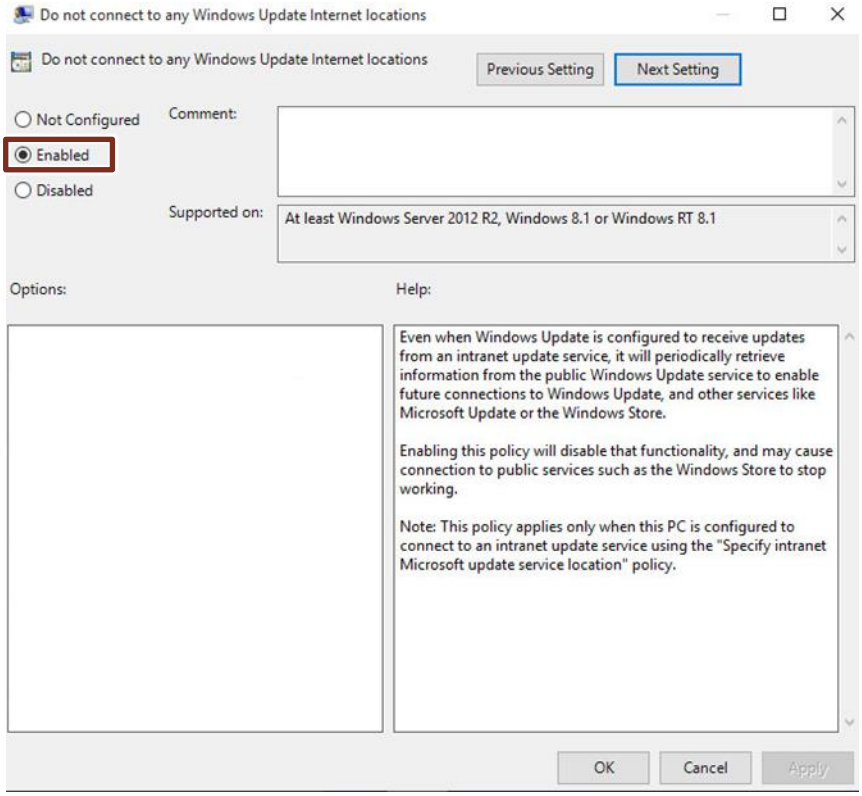
4.1 Manual loading of Windows updates

Note If your runtime PC is connected to the Internet and you have deactivated automatic updating, you are responsible for installing security updates yourself.

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.

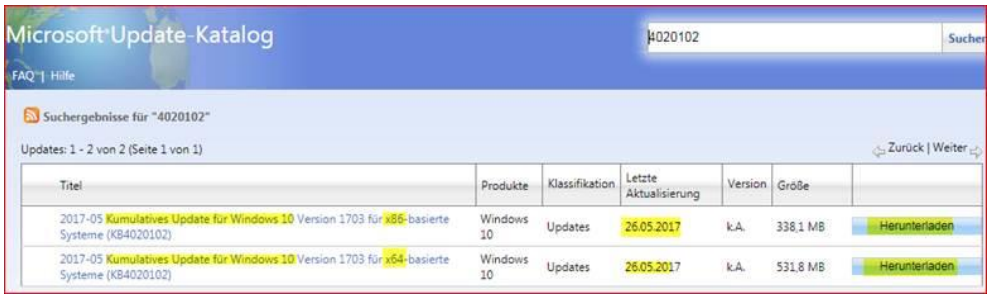
4.1.1 Option 1: Download to another PC via Microsoft Update Catalog

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

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

Requirement: You know the patch designation (e.g. KB4020102), so that you can search for it in the Microsoft Update Catalog.

Figure 4-2



You can use an external medium 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. After this, it generates file: "UpdateInstaller.exe" that must be started on an (offline) target computer. The file can also be located on a USB stick or a USB hard drive.

4.2 Using one WSUS server to distribute updates to several WinCC stations[5]

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

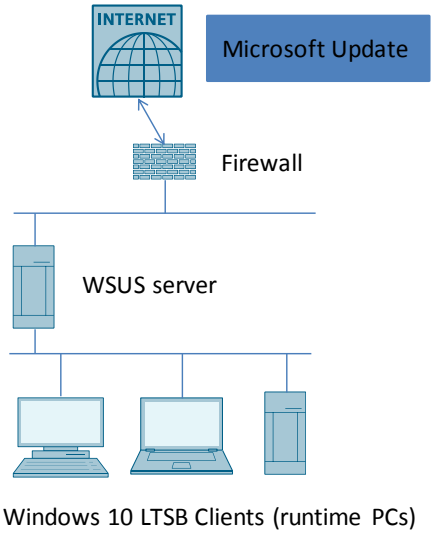
4.2.1 Simple WSUS provision

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 4-3



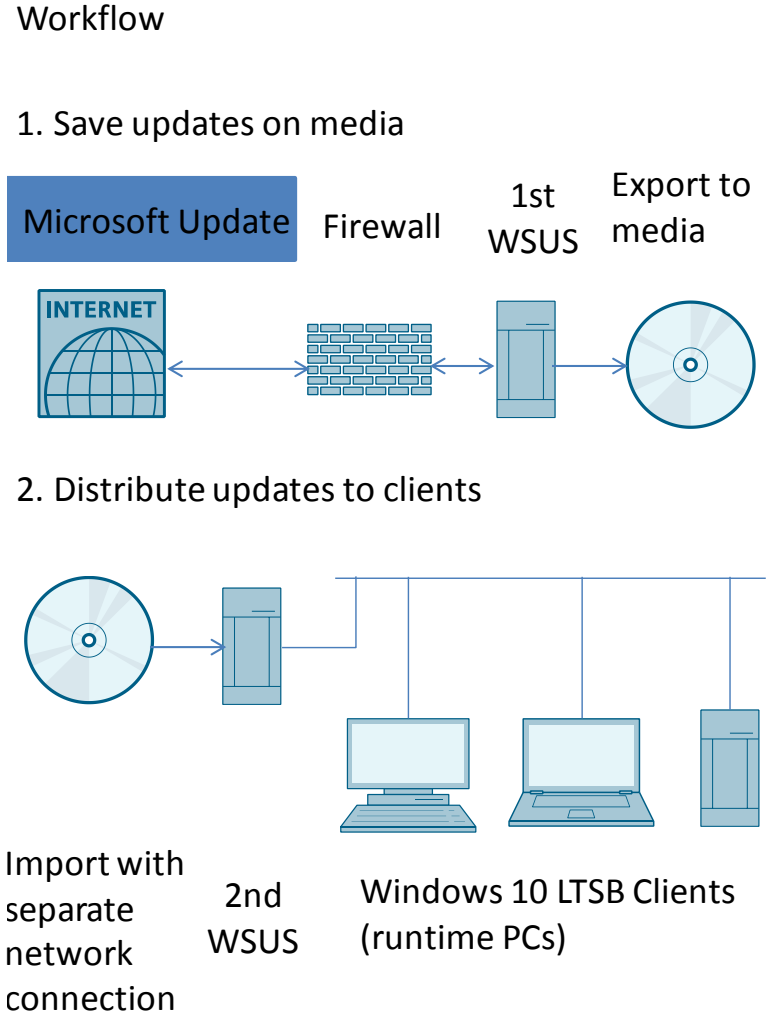
4.2.2 Non-connected WSUS server (standalone operation)

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.

[5] https://msdn.microsoft.com/en-us/library/hh852344(v=ws.11).aspx retrieved 27.12.2017

Note This variant lends itself to use in standalone operation.

Figure 4-4



Note To find out about possible WSUS server deployment scenarios, visit:
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852344(v=ws.11)

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

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852344(v=ws.11)

Step 2: Install the WSUS server role

https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852338(v=ws.11)

Step 3: Configure WSUS

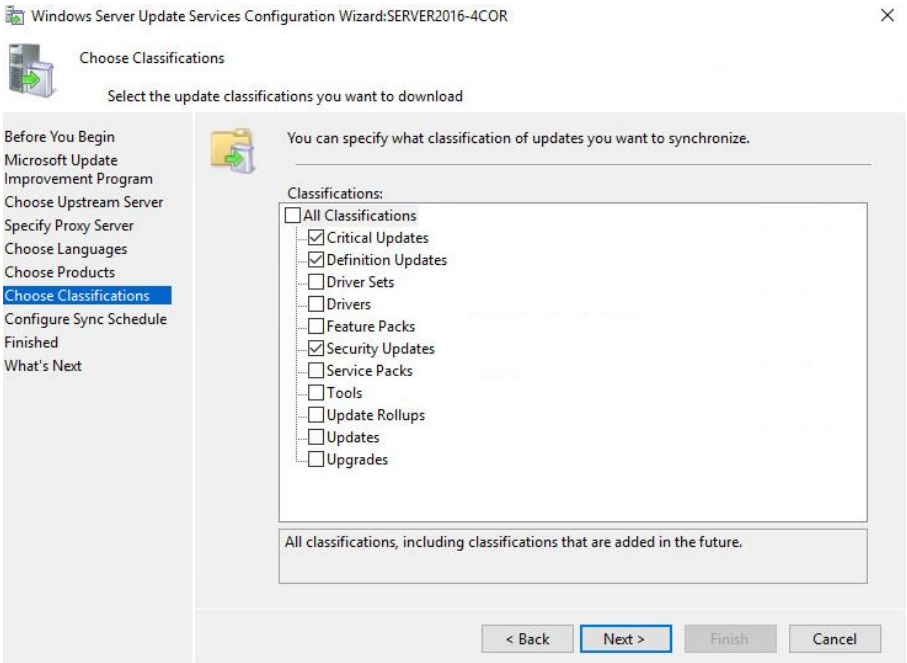
https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852346(v=ws.11)

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 updates service configuration wizard:

Figure 4-5



Note

These settings prevent feature updates.

Step 4: Approve and deploy WSUS updates

The link below shows you 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 CB or CBB, this allows you to block feature.

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:

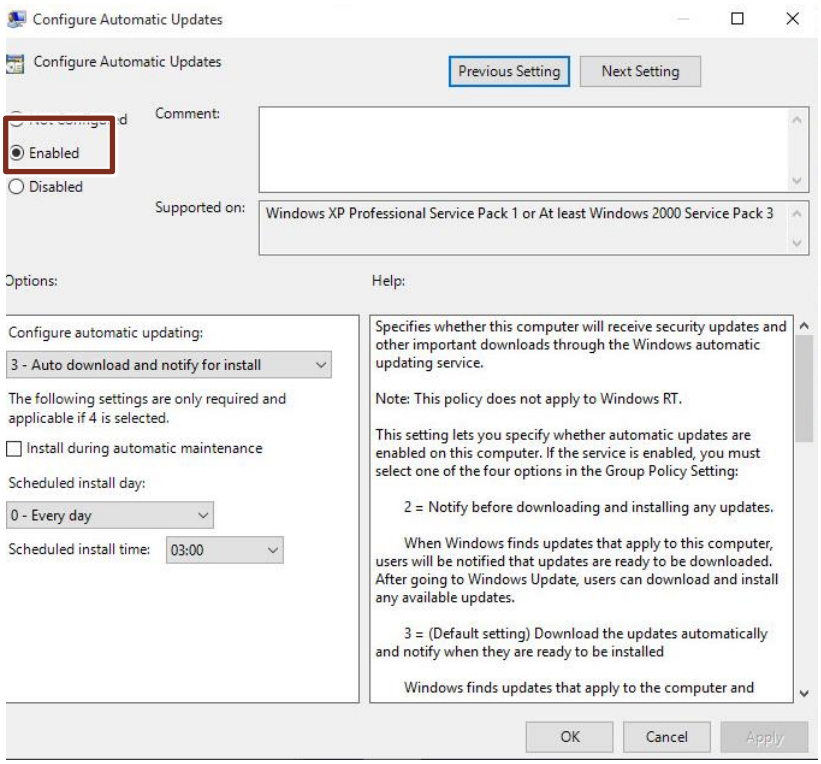
https://docs.microsoft.com/en-us/windows/deployment/update/waas-manage-updates-wsus

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 LTSB client. To make the correct settings on the client, proceed as follows:

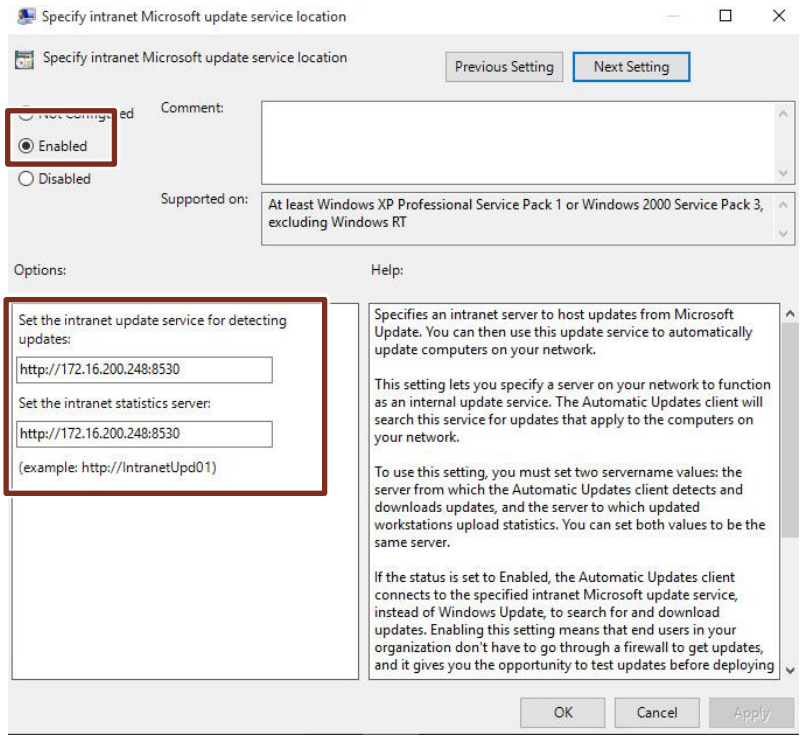
1. Press the Windows key on your keyboard and start the editor for local group policies by entering gpedit.msc. The editor for local group policies opens.
2. Navigate to Computer Configuration >Administrative Templates>Windows Components>Windows Update.
3. In the “Settings”, double-click to open “Configure Automatic Updates”. The "Configure Automatic Updates" dialog opens.

Figure 4-6



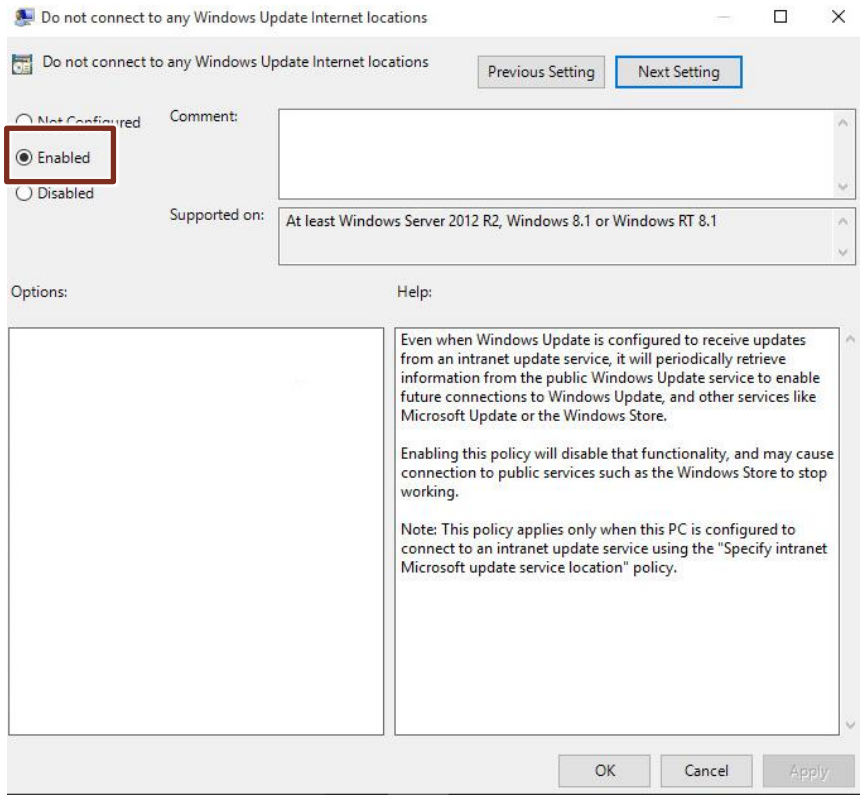
4. In the Options area, specify the Microsoft update service location:

Figure 4-7



5. Not Allowing Access to Windows Update Internet Locations

Figure 4-8



Note

The "Next Setting" pushbutton allows you to click through the different settings and to confirm them by clicking on "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.

5 Useful information

5.1 Windows10 LTSB

The Windows 10 LTSB is intended for companies that purchase Windows 10 Enterprise.

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

Via In Place Upgrade, customers can migrate from one LTSB to the next one; in addition, it is possible to skip an LTSB.

Note

We expressly recommend using Windows 10 LTSB in conjunction with SIMATIC WinCC products, since no Feature Updates (Creators Updates) are loaded in this case.

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:
https://support.industry.siemens.com/cs/sc

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:
https://support.industry.siemens.com/cs/ww/en/sc/2067

6.2 Links and Literature

Table 6-1

No.	Topic
\1\	Siemens Industry Online Support https://support.industry.siemens.com/cs/start?lc=en-WW
\2\	Link to the entry page of the application example https://support.industry.siemens.com/cs/ww/de/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-wufb
\7\	Visit the (Microsoft Update Catalog) link below to 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://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852344(v=ws.11)
\9\	Prepare WSUS deployment https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852344(v=ws.11)
\10\	Install the WSUS server role https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852338(v=ws.11)
\11\	Configure WSUS https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852346(v=ws.11)
\12\	Approve and deploy WSUS updates https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh852348(v=ws.11)
\13\	Deploy Windows 10 updates using 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

6.3 Change documentation

Table 6-2

Version	Date	Modifications
V1.0	02/2018	First version