

SIEMENS

SIMATIC

Process Control System PCS 7 Patch management and security updates

Commissioning Manual

Preface

1

Patch management and
security updates

2

Practical information

3

12/2011

A5E02657552-02

Legal information

Warning notice system

This manual contains notices you have to observe in order to ensure your personal safety, as well as to prevent damage to property. The notices referring to your personal safety are highlighted in the manual by a safety alert symbol, notices referring only to property damage have no safety alert symbol. These notices shown below are graded according to the degree of danger.

⚠ DANGER
indicates that death or severe personal injury will result if proper precautions are not taken.
⚠ WARNING
indicates that death or severe personal injury may result if proper precautions are not taken.
⚠ CAUTION
with a safety alert symbol, indicates that minor personal injury can result if proper precautions are not taken.
CAUTION
without a safety alert symbol, indicates that property damage can result if proper precautions are not taken.
NOTICE
indicates that an unintended result or situation can occur if the relevant information is not taken into account.

If more than one degree of danger is present, the warning notice representing the highest degree of danger will be used. A notice warning of injury to persons with a safety alert symbol may also include a warning relating to property damage.

Qualified Personnel

The product/system described in this documentation may be operated only by **personnel qualified** for the specific task in accordance with the relevant documentation, in particular its warning notices and safety instructions. Qualified personnel are those who, based on their training and experience, are capable of identifying risks and avoiding potential hazards when working with these products/systems.

Proper use of Siemens products

Note the following:

⚠ WARNING
Siemens products may only be used for the applications described in the catalog and in the relevant technical documentation. If products and components from other manufacturers are used, these must be recommended or approved by Siemens. Proper transport, storage, installation, assembly, commissioning, operation and maintenance are required to ensure that the products operate safely and without any problems. The permissible ambient conditions must be complied with. The information in the relevant documentation must be observed.

Trademarks

All names identified by ® are registered trademarks of Siemens AG. The remaining trademarks in this publication may be trademarks whose use by third parties for their own purposes could violate the rights of the owner.

Disclaimer of Liability

We have reviewed the contents of this publication to ensure consistency with the hardware and software described. Since variance cannot be precluded entirely, we cannot guarantee full consistency. However, the information in this publication is reviewed regularly and any necessary corrections are included in subsequent editions.


Table of contents

1	Preface	5
1.1	Structure and organization of the document.....	5
1.2	Special notes.....	6
2	Patch management and security updates	7
2.1	Definitions	7
2.2	Which patches should be installed?	9
2.3	Patch management.....	10
2.3.1	Patch management with the WSUS server	10
2.4	Patch management strategy	13
2.5	Installing the WSUS server	14
2.5.1	WSUS server	14
2.5.2	WSUS client.....	15
3	Practical information	17
3.1	General information	17
3.2	Special information	18


Preface

1.1 Structure and organization of the document

The PCS 7 and WinCC Security Concept consists of several parts:

-  The basic document forms a central overview and guide for the PCS 7 & WinCC Security Concept.

It provides a systematic description of the basic principles and strategies of the security concept. All additional detail documents assume the reader has read the basic document.

-  The detail documents (such as this document) explore specific principles, solutions and their recommended configuration in detail, always focusing on a particular topic. These detail documents are supplemented, updated and published separately to ensure they are always up to date.

1.2 Special notes

Aims of the PCS 7 & WinCC Security Concept

In automation, top priority is given to maintaining production and process control. These must not be negatively influenced by any measures taken to prevent the propagation of a security threat.

As security threats are constantly developing, the security concept cannot be guaranteed to provide 100%, uninterrupted protection, even when implemented in its entirety. Regular evaluation of the implemented security measures is therefore recommended.

The PCS 7 & WinCC Security Concept is intended to ensure that only authenticated users are allowed to perform authorized (permitted) operations on authenticated devices based on the operating options assigned to them. These operations should only be performed via defined and planned access routes to ensure safe production or coordination of a job without risk to humans, the environment, product, goods to be coordinated or the business of the enterprise.

The PCS 7 & WinCC Security Concept therefore recommends the use of the latest available security mechanisms. To achieve the highest possible security, plant-specific configurations must never contradict the basic principles of this security concept.

The PCS 7 & WinCC Security Concept is intended to facilitate cooperation between network administrators of company networks (IT administrators) and automation networks (automation engineers), so that both can benefit from the advantages provided by the networking of process control technology and the data processing of other production levels without increasing security risks at either end.

Required knowledge

This documentation is intended for personnel involved in configuring, commissioning and servicing automation systems with SIMATIC. It is assumed that readers have appropriate administration knowledge of office IT.

Validity

The PCS 7 & WinCC Security Concept gradually replaces the previous documents and recommendations "PCS 7 Security Concept" and "WinCC Security Concept" and is valid as of WinCC V6.2 and PCS 7 V7.0.

Patch management and security updates

Regular and prompt installation of software updates (patches) represents a vital element of a comprehensive security concept. Patches contribute toward stable system operation and/or eliminate known security vulnerabilities.

2.1 Definitions

Patch

According to Microsoft, the generic term "patch" refers to all kinds of updates, service packs, feature packs and similar, whether these relate to security or not.

Security updates

The term "security update" refers exclusively to security-related vulnerabilities.

Critical updates

The term "critical updates" encompasses all updates that eliminate critical errors but not any security-related vulnerabilities.

WSUS

Windows Server Update Services - system administrators can use this software to manage the updates provided by Microsoft and to distribute them to computers.

Microsoft Update

The Update Services components connect to this website for updates for Microsoft products.

Update Services server

The update files are stored centrally on the Update Services server. The Update Services server provides features required by administrators to manage and distribute the updates. The Update Services server can also be used as an update source for other Update Services servers.

Automatic Update

Client component that is integrated in the Windows 2000 SP4, Windows XP and Windows Server 2003 operating systems. Automatic Update enables computers to download updates from Microsoft Update or from a server that is running Update Services.

2.2 Which patches should be installed?

With the introduction of WSUS and the expansion of Windows Update (operating system patches only) to Microsoft Update (patches for a variety of Microsoft products), Microsoft has created new classifications for the patches:

- Definition updates
- Feature packs
- Service packs
- Security updates
- Tools
- Drivers
- Update rollups
- Critical updates
- Updates

Many of the patches in these classifications are neither important nor essential for secure and stable plant operation. Definition updates provide pattern files for proprietary Microsoft security programs such as "Windows Defender". These are currently not approved for operation with SIMATIC software. Feature packs and tools usually introduce new functionalities, however these cannot be used by the SIMATIC software. Update rollups are simply collections of previously published patches. Drivers are the latest hardware drivers, however you should always use the drivers released and supplied by Siemens. Service packs can lead to substantial modification of the operating system and are only approved by Siemens with new versions. Updates eliminate minor flaws in a program. For this reason, only the critical updates and security updates are relevant to automation systems. Siemens runs tests on these two classes of patches immediately after their release by Microsoft. The test results are published immediately on the Internet (see below). Customers are informed of any problems found during the tests by means of a newsletter or FAQ entries.

Microsoft provides patches for almost all of its products, including products which are of no relevance to SIMATIC software. This documentation only covers patches approved for use with the relevant SIMATIC software, i.e. for Windows Workstation operating system, Windows Server operating system, Internet Explorer, SQL Server and Microsoft Office.

General Siemens statements relating to Microsoft patches, information on restrictions and a list of the patches tested for compatibility are available on the Internet at

<http://support.automation.siemens.com/WW/view/en/18490004>.

A charge will be made for Siemens support if any problems develop after you install Microsoft product patches that are not included in the compatibility list.

2.3 Patch management

Although it is possible for each computer to download patches directly from Microsoft Update or to install patches separately on each computer using a CD or network drive, these methods are rather laborious or require Internet access for each computer. A central solution for patch distribution is therefore recommended. Siemens recommends the Windows Server Update Service.

2.3.1 Patch management with the WSUS server

In addition to the configuration and administration of the WSUS server and clients, the location of the WSUS server and the strategy for update distribution are important for good patch management. Not all computers require the same updates and certain computers must not receive specific updates.

There are two different types of WSUS configuration:

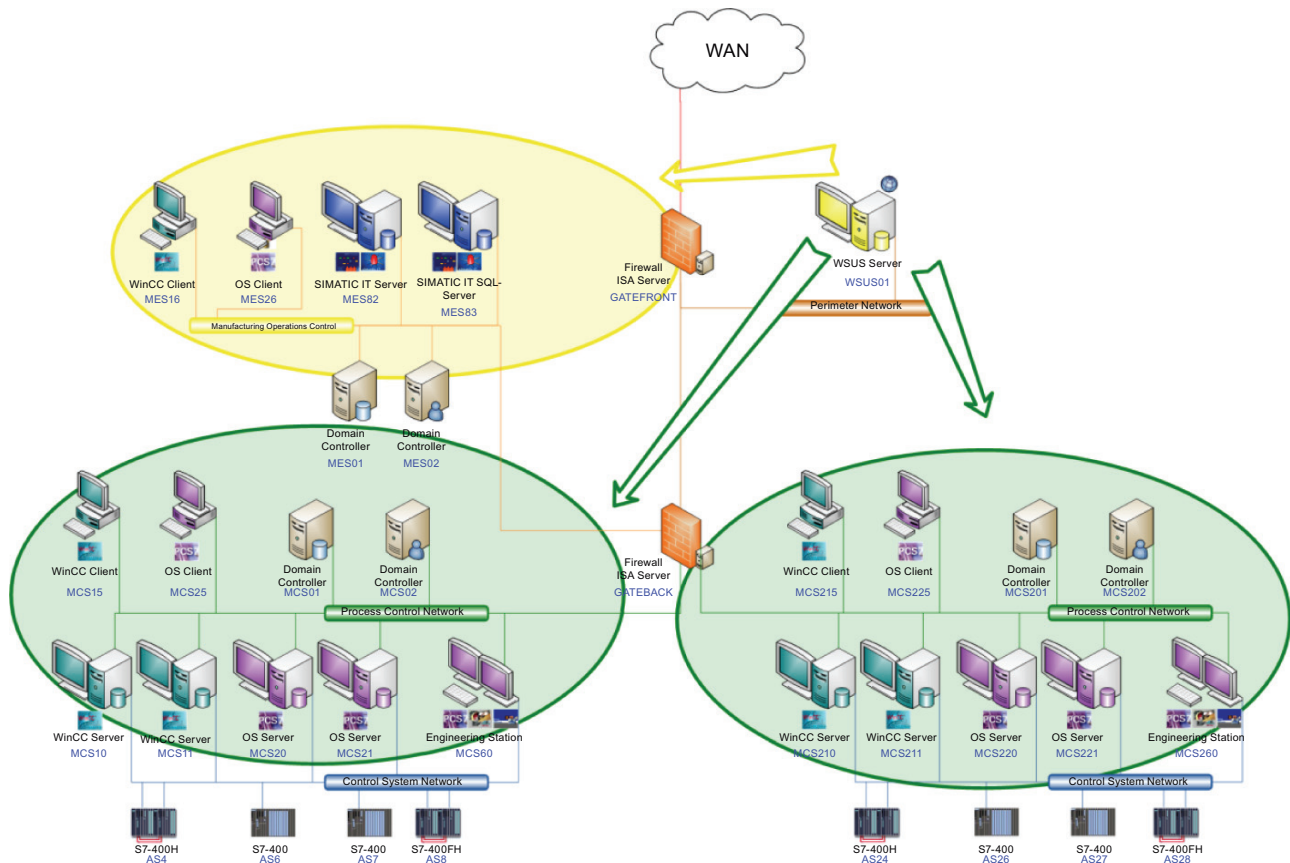
- A central WSUS server for complete management of the updates
- A hierarchy comprising several WSUS servers

To simplify matters, the following examples show complete security zones or networks configured as WSUS groups. In practice, the grouping should be broken down further. You can find more information in the chapter Patch management strategy (Page 13).

Using WSUS servers

The WSUS server configuration allows various computers in a network to be grouped. A single WSUS server is therefore capable of providing selected updates to the computers in these groups. Since the WSUS server requires access to the Internet or to a higher-level WSUS server on the office network, it is advisable to install this server on a perimeter network that is kept separate by means of the back-end firewall, to provide additional protection for the plant.

Updates are released on this WSUS for installation in individual groups. In this example, the groups represent the respective networks. Needless to say, you can and should create more groups. In practice, it is usually not permitted to patch computers in a network at the same time or to skip installation of specific updates for some computers in a network.



Advantages

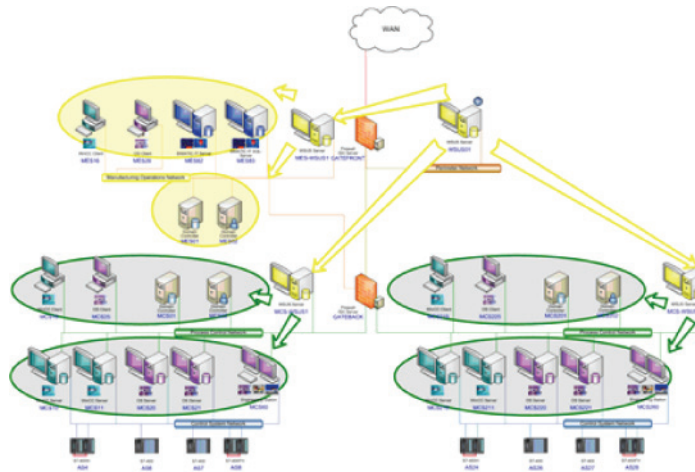
- You can save hardware costs, as only one computer is required for update distribution.
- The entire patch management process can be administrated from a central computer.

Disadvantages

- If the WSUS fails, plant computers no longer receive any updates and newly installed computers do not receive any updates at all.

Using several WSUS servers

Another option is to use secondary WSUS servers. In this scenario, the higher-level WSUS server is installed in the perimeter network as the computer requires access to the Internet or to a higher-level server in the office network. A separate WSUS is also installed in each network. These secondary servers fetch their updates from the WSUS server in the perimeter network, which, in turn, fetches them from its source. The secondary WSUS servers in the various networks then release the updates individually for their groups.



Advantages

- If the higher-level WSUS server fails, new plant computers in the network can at least receive all of the updates that were released up to the time of failure.
- If a secondary WSUS server fails, the computers in the other networks continue to receive updates.
- The reintegration of the higher-level and of a secondary server after failure is less complicated compared with the reintegration of the stand-alone WSUS server shown in the first example, as each server only has to manage a smaller number of groups and computers.

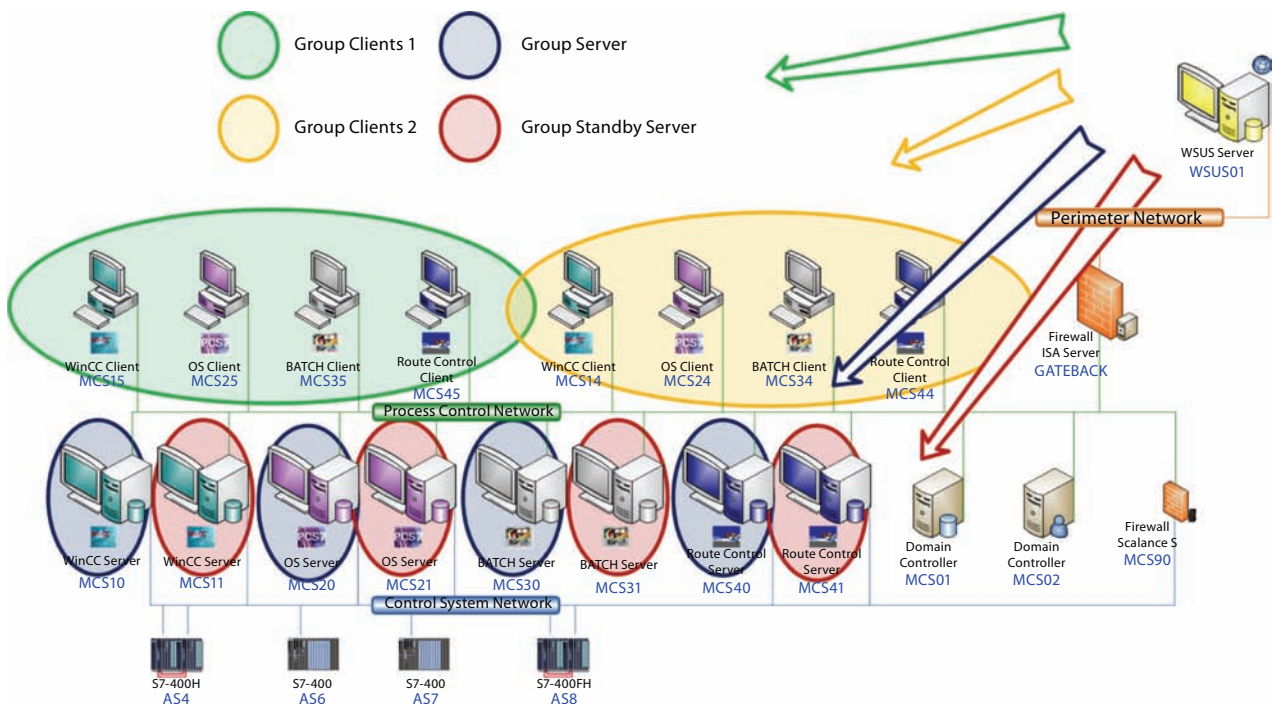
Disadvantages

- High hardware costs, as a WSUS server is required for each network.
- Administration is more complex, as several computers participate in patch management.

2.4 Patch management strategy

To avoid any negative effects on plant operation and to take precautions against the minor, yet possible risk of "harmful" updates, the following patching procedure is advised:

- When patches are released by Microsoft, you are advised to wait several days before installing them in the plant. You can find more information about Siemens' position regarding compatibility of new patches at <http://support.automation.siemens.com/WWW/view/en/18490004>.
- Configuration of a small-scale virtual system that covers the essential functions of the plant. You can install new patches on this virtual system first and test their compatibility.
- All servers and clients should be operated in redundant mode.
- You should create at least two groups for each network on the WSUS server. Each group contains one server of the pair and half of its clients.
- If no faults occur after a certain number of days and neither Microsoft nor Siemens have issued any objections in terms of the update, you can patch a group in each network. This will not interfere with plant operation, since at least one server and half the number of clients are still operating in runtime mode.
- If no negative effects are observed after another period of several days, you can patch the second group of each network.



This procedure allows for efficient and safe installation of all required updates without the risk of adverse effects on operations.

2.5 Installing the WSUS server

You can find a description of the WSUS server and a variety of helpful and detailed descriptions and installation instructions at:

<http://www.microsoft.com/germany/windowsserver2003/technologien/updateservices/default.aspx>

2.5.1 WSUS server

Default installation is recommended for the WSUS. To save costs, you should only load Microsoft patches that Siemens has approved for SIMATIC software (see section 2.2). You can find information on the recommended group configurations in the patch management section.

There are basically three types of installation/configuration:

- A stand-alone server that downloads the patches directly from Microsoft. You can customize this type of installation and specify exactly which patches should be downloaded from Microsoft. This configuration is particularly suited as a master WSUS server for one or more plants.
- A stand-alone server that downloads the patches from another WSUS server. Although you can customize this type of installation, you cannot specify which patches should be downloaded. All patches fetched by the higher-level WSUS server are passed to the sublevels. This configuration is particularly suitable when there are several different plants, which should each have a separate WSUS server, but the patches should only be downloaded once from Microsoft to save costs or when a WSUS server is already available in a plant or corporate network.
- A mirrored server that fetches its settings and patches from another WSUS server. This configuration is only suitable when there are several plants separated by great distances and each requires a separate WSUS server, but there is only one patch administrator for all plants.

The computers in the network to be patched can be divided into groups. This allows you to release the updates separately for each group. You can also decide when the group should be updated or whether or not to install the update for a group. To assign individual computers to specific groups, you can either move them directly on the WSUS server or use the group policies (local or domain policies). It is not possible to use both methods. The method to be used must be selected during installation/initial configuration on the WSUS server. However, it is advisable to define the groups manually on the WSUS server to maintain a clearer overview.

2.5.2 WSUS client

The following settings should be made for the update clients in the local or domain policies, depending on the plant configuration.

You can find the policies under "Computer configuration/Administrative templates/Windows components/Windows Update":

- Do not display 'Install Updates and Shut Down' option in Shut Down Windows dialog box:
display option when shutting down the computer (recommended setting: not configured)
- Do not adjust default option in 'Install Updates and Shut Down' option in Shut Down Windows dialog box:
display option when shutting down the computer (recommended setting: not configured)
- Configure Automatic Updates:
Option that defines how to handle the updates. Automatically download and install or notify (recommended setting: 2 – do not install or download patches during process mode, as this can lead to adverse effects (e.g. loss of performance or computer restart))
- Specify internal path for the Microsoft Update Service:
URL of the WSUS server in the plant
- Enable Client-side Targeting:
Option of allowing computers to add themselves to a group on the WSUS server, based on group policies (recommended setting: administrator decision, depending on the system)
- Reschedule Automatic Update scheduled installations:
Waiting time after restart until an update installation is repeated (recommended setting: 5 minutes)
- No automatic restart for scheduled installations:
User must restart the computer on completion of the installation; no automatic restart (recommended setting: enabled)
- Detection frequency for automatic updates:
defines how long (in hours) the client waits before scanning for updates (recommended setting: 22)
- Install Automatic Updates immediately:
Installs updates automatically (recommended setting: disabled – do not install anything on the process computers during runtime mode)
- Delay restart for scheduled installations:
waiting time after patch installation before automatic restart (recommended setting: not configured)

2.5 Installing the WSUS server

- Re-prompt for restart with scheduled installations:
(recommended setting: disabled – event dialog boxes could interfere with runtime mode)
- Allow non-admins to receive update notifications:
In addition to administrators, users and power users can receive notifications of new updates and install them (recommended setting: disabled – only system administrators should be authorized to install updates)

Practical information

3.1 General information

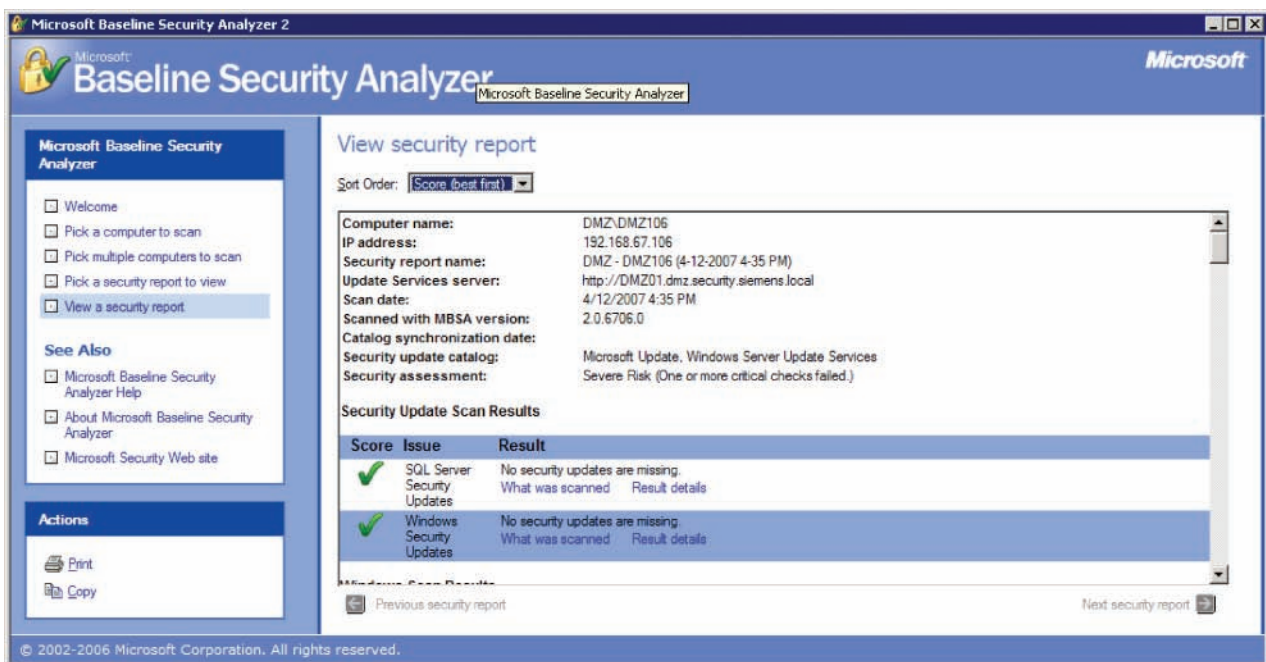
Microsoft Baseline Security Analyzer

You can also use the "Microsoft Baseline Security Analyzer" (MBSA) to check whether all released patches have been installed on a specific plant PC. In addition to other settings referred to in the relevant sections, this tool checks whether all patches released by Microsoft are installed on a specific computer.

In order for the check to be performed, the computer on which MBSA is installed must be connected to the Internet or the latest patch information must have been manually downloaded from Microsoft.

You can download the latest version of MBSA, including the associated descriptions, from the following link:

<http://www.microsoft.com/mbsa>



Report functionality of the WSUS server

The WSUS server provides an integrated, comprehensive report functionality. If a WSUS server is used for patch distribution, these reports can be used to monitor the status of all network computers registered on the WSUS server. You can also use it to check whether all released patches have been installed on the computers.

3.2 Special information

Accelerating the "Updates" download

After re-installation of a computer or after new patches have been released on the WSUS server, it can take some time to notify the client of the download and installation pending. This is because the clients do not constantly scan the WSUS server for new patches. Enter the following command to speed up the process:

"Wuauclt.exe /resetauthorization /detectnow"

This command makes the client immediately report its status to the WSUS server and request new patches. However, this action does not make new patches immediately available to the client. To prevent a large number of computers from simultaneously downloading patches, a random timer is triggered on the WSUS server (0 to 30 minutes) at each client request. Patches are only made available once this timer has expired.

Simplifying administration of new patches

The "Configure Automatic Updates" setting described in chapter WSUS client (Page 15) is the most reliable method of ensuring fault-free process mode. However, this method is also highly time consuming, as the download and installation of the updates must be confirmed manually on each computer. To simplify matters, you can select option 3 (automatic download without installation) or option 4 (automatic download and installation). However, note that computers will immediately load the patches released for a group and, depending on the option selected, install them automatically. It makes no difference whether or not PCS 7 or WinCC is currently in runtime mode. For this reason, when using one of these options, the administrator must ensure that he only releases patches for groups of computers that are not involved in process mode.