

# SIEMENS

## SIMATIC

### Process Control System PCS 7 Patch management and security updates

Commissioning Manual

Security information

1

Preface

2

Patch management and  
security updates

3

Practical information

4

## 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.

<b>⚠ DANGER</b>
indicates that death or severe personal injury <b>will</b> result if proper precautions are not taken.

<b>⚠ WARNING</b>
indicates that death or severe personal injury <b>may</b> result if proper precautions are not taken.

<b>⚠ CAUTION</b>
indicates that minor personal injury can result if proper precautions are not taken.

<b>NOTICE</b>
indicates that property damage can result if proper precautions are not taken.

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:

<b>⚠ WARNING</b>
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

<b>1</b>	<b>Security information.....</b>	<b>5</b>
<b>2</b>	<b>Preface.....</b>	<b>7</b>
2.1	Structure and organization of the document.....	7
2.2	Special notes.....	7
<b>3</b>	<b>Patch management and security updates.....</b>	<b>9</b>
3.1	Definitions.....	9
3.2	Which patches should be installed?.....	10
3.3	Patch management.....	10
3.3.1	Patch management with the WSUS server.....	11
3.4	Patch management strategy.....	14
3.5	Installing the WSUS server.....	15
<b>4</b>	<b>Practical information.....</b>	<b>17</b>
4.1	General information.....	17
4.2	Special information.....	18



## 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 only form one element of such a concept.

Customer is responsible to prevent unauthorized access to its plants, systems, machines and networks. Systems, machines and components should only be connected to the enterprise network or the internet if and to the extent necessary and with appropriate security measures (e.g. use of firewalls and network segmentation) in place.

Additionally, Siemens' guidance on appropriate security measures should be taken into account. For more information about industrial security, please visit:  
<http://www.siemens.com/industrialsecurity>

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



To stay informed about product updates, subscribe to the Siemens Industrial Security RSS Feed under:  
<http://www.siemens.com/industrialsecurity>



# Preface

## 2.1 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.  
This document describes the basic principles and security strategies of the security concept in systematized form. 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.
- PCS 7 Compendium F: Compendium F describes in detail how the solutions can be implemented in the PCS 7 environment. You can find this documentation on the Internet at: <https://support.industry.siemens.com/tf/ww/en/posts/69921/> (<https://support.industry.siemens.com/tf/ww/en/posts/69921/>)

## 2.2 Special notes

### Aims of the PCS 7 & WinCC Security Concept

In automation, top priority is given to maintaining production and process control. Measures intended to prevent the spread of a security threat must not impair this aim.

The security concept PCS 7 & WinCC is intended to provide support in creating a plant in which only authenticated users can perform authorized (permitted) operations using operating options assigned to them for authenticated devices. 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.

## 3.1 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 integrated in Windows operating systems. Automatic Update enables computers to download updates from Microsoft Update or from a server that is running Update Services.

## 3.2 Which patches should be installed?

With the introduction of WSUS and the further development of Windows Update (patches for operating systems only) to Microsoft Update (patches for numerous Microsoft products), Microsoft has created new classifications for the individual 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 sometimes result in major changes and are only released 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.

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

<https://support.industry.siemens.com/cs/ww/en/view/18490004> (<https://support.industry.siemens.com/cs/ww/en/view/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.

## 3.3 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.

### 3.3.1 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

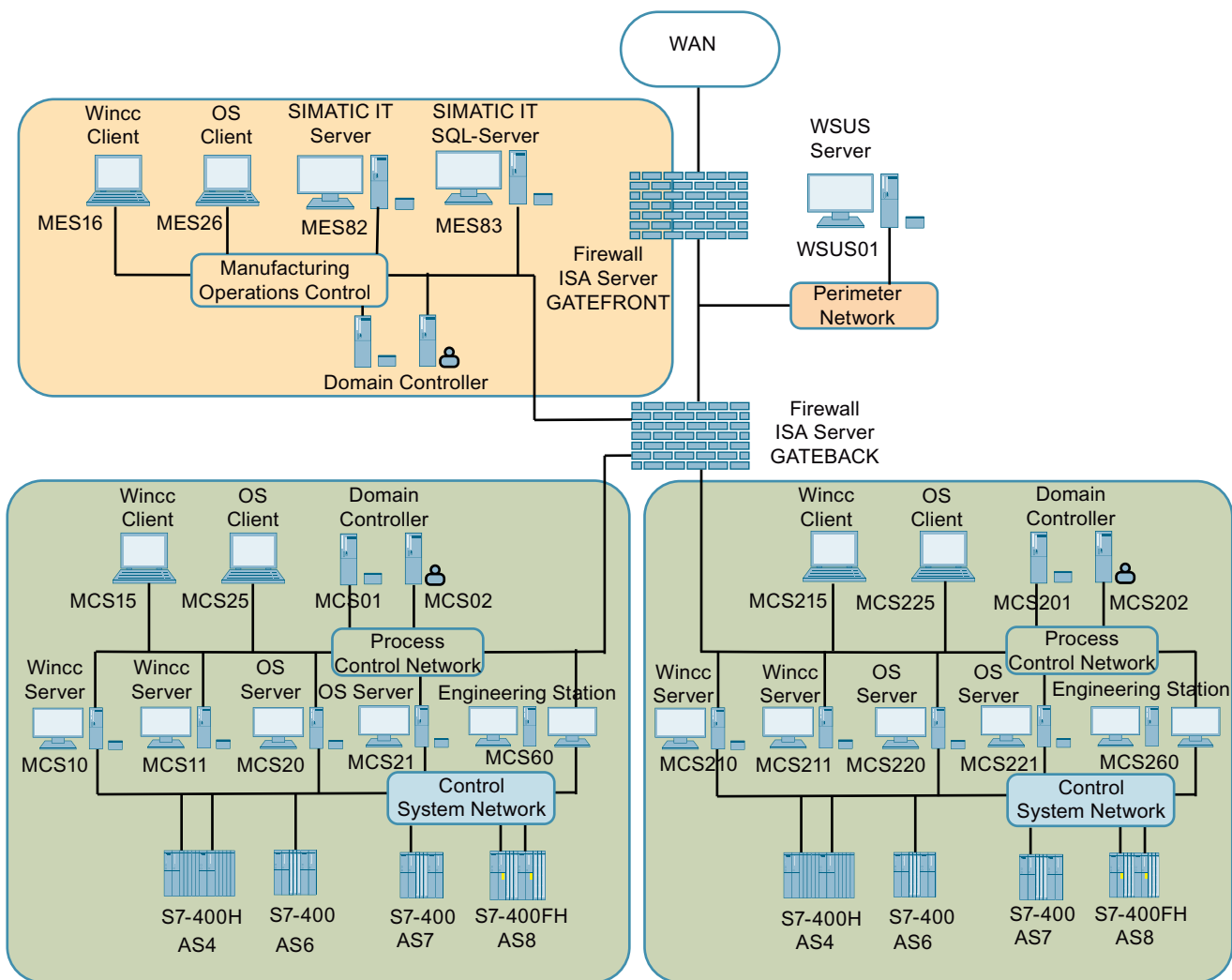
To simplify matters, the following examples show complete security zones or networks configured as WSUS groups. In practice, the grouping should be broken down further. This is handled in detail in the section Patch management strategy (Page 14).

#### WSUS server for complete management

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.

3.3 Patch management



**Advantages**

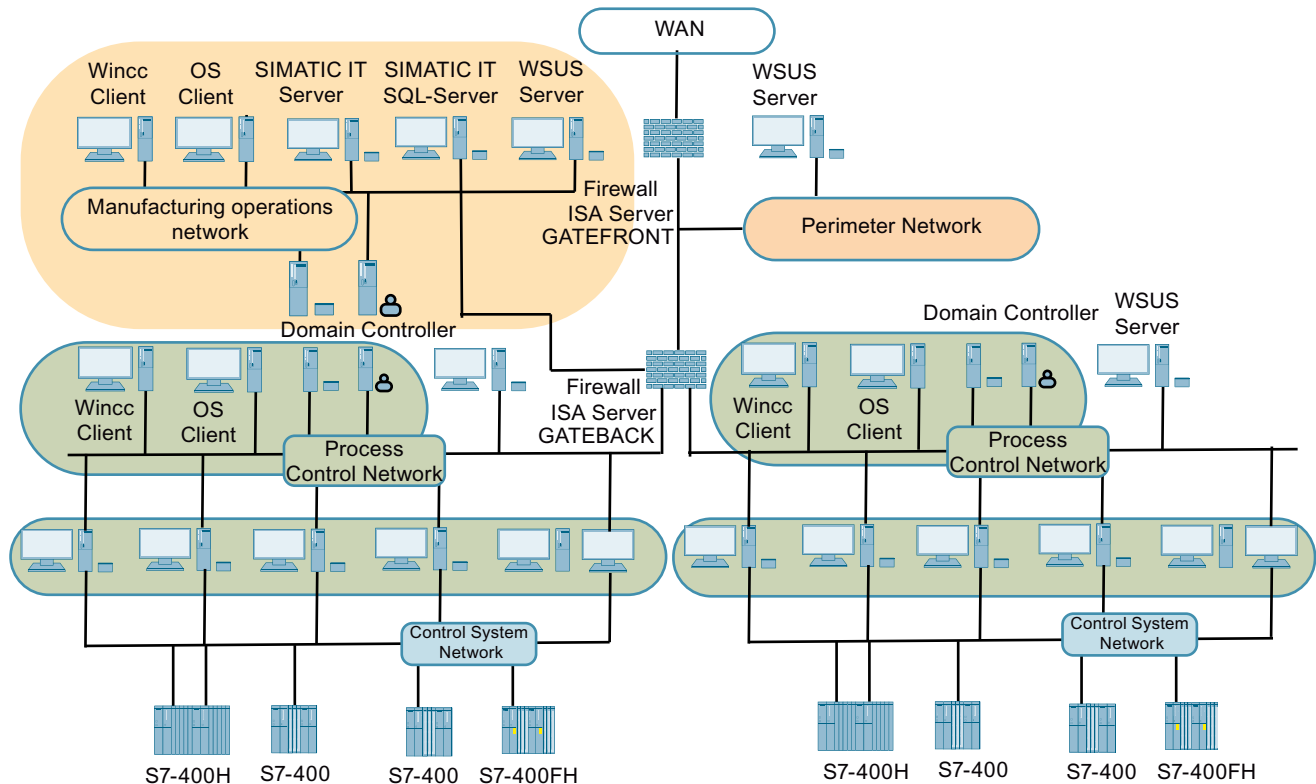
- Only one computer is used for the update distribution, which saves on hardware.
- The entire patch management process can be administrated from a central computer.

**Disadvantages**

- If the WSUS server fails, computers in the plant obtain no new updates and newly installed computers get no updates at all.

## Applying the hierarchy on multiple WSUS servers

With this update distribution system, the higher-level WSUS server is placed in the perimeter network, since the computers require access to the Internet or 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.

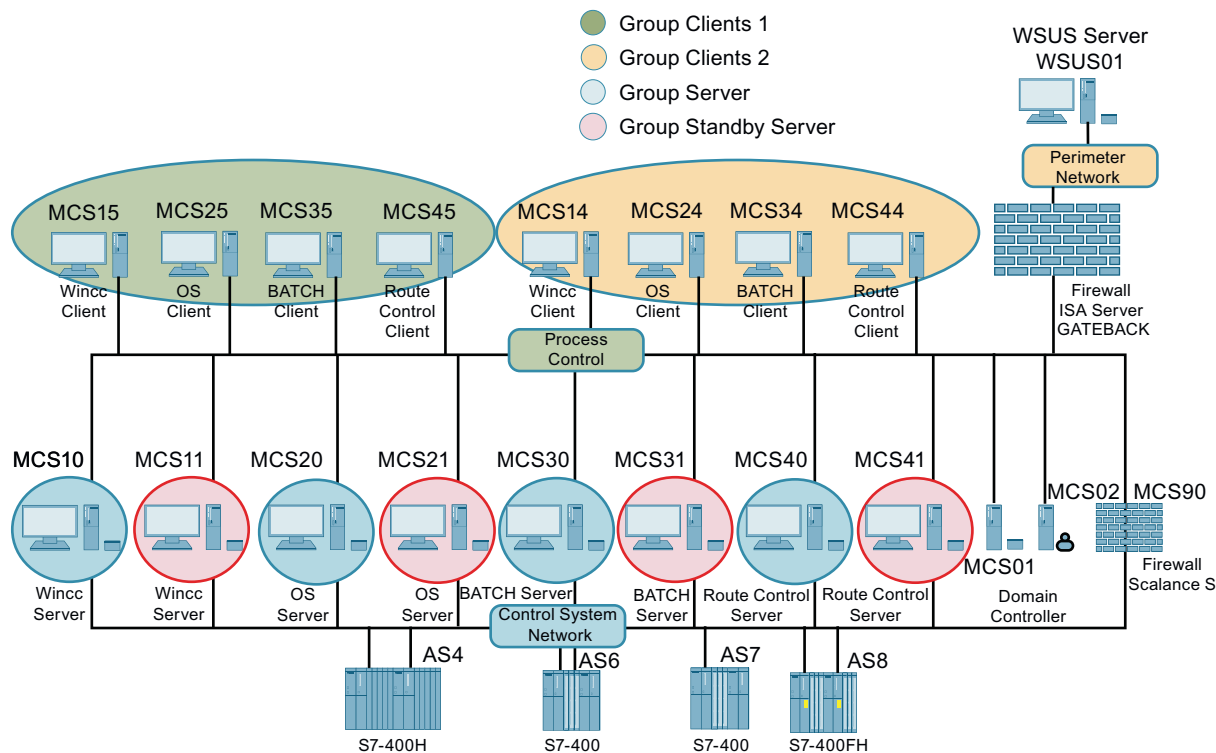
### Disadvantages

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

### 3.4 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. Siemens' statements on the compatibility of the new patches can be found at the link <https://support.industry.siemens.com/cs/ww/en/view/18490004> (<https://support.industry.siemens.com/cs/ww/en/view/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.

## 3.5 Installing the WSUS server

See Compendium F

<https://support.industry.siemens.com/tf/ww/en/posts/69921> (<https://support.industry.siemens.com/tf/ww/en/posts/69921>)

*3.5 Installing the WSUS server*



## Practical information

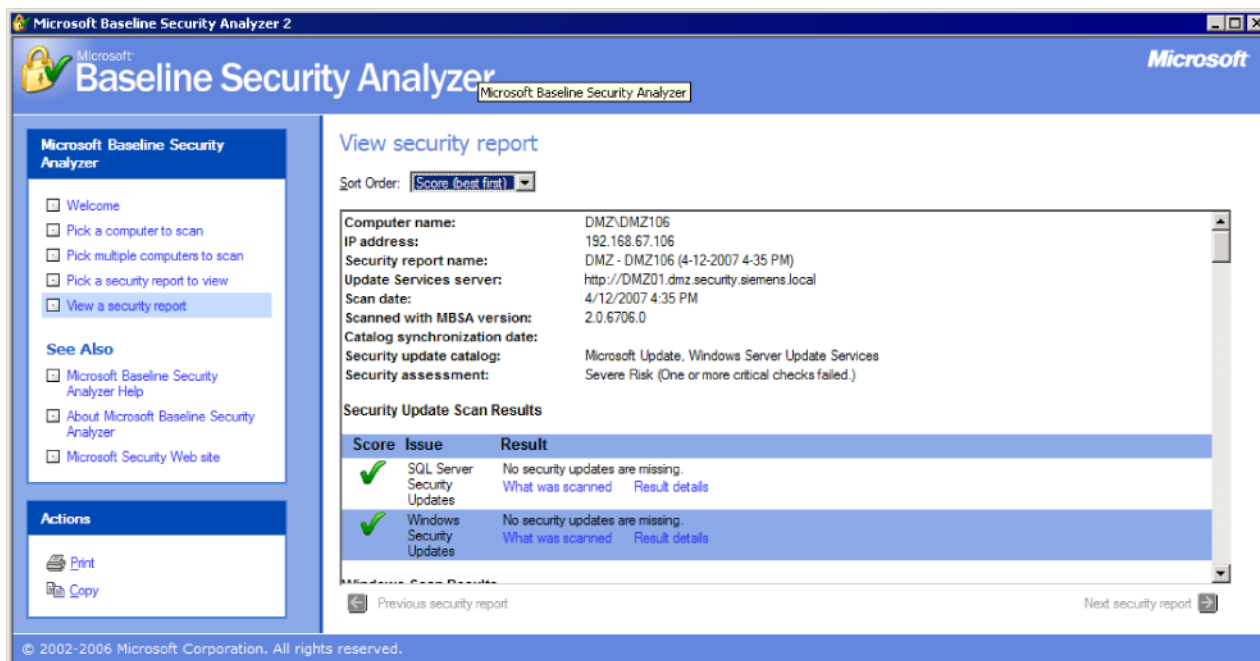
### 4.1 General information

#### 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.

The latest version of MBSA and corresponding descriptions can be downloaded from the following link: <http://www.microsoft.com/mbsa> (<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.

## 4.2 Special information

### Accelerating "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.