Microsoft

Microsoft® Windows Server™ 2003 Service Pack 1

# Datasheet

Windows Server 2003 Service Pack 1 is a collection of updates and security enhancements to the current Windows Server 2003 operating system. Service Pack 1 (SP1) incorporates a set of security technologies that will help to reduce the attack surface of Windows Server systems and ease administrative tasks associated with configuring server security.

**For more information on Windows Server 2003 Service Pack 1, visit**

http://www.microsoft.com/windowsserver2003/downloads/servicepacks/default.mspx

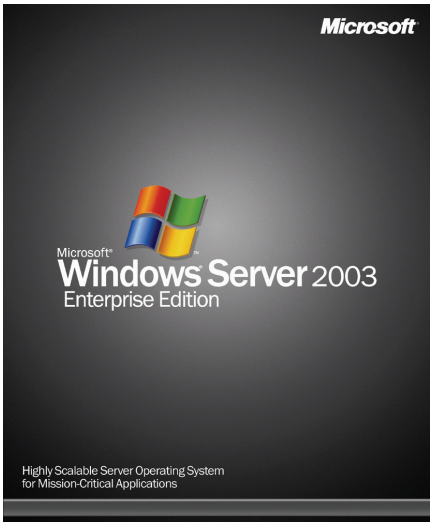
## Security Benefits

A secure computing infrastructure is a strategic business asset. As a leader in the computing industry, Microsoft is working to deliver secure products and to help its customers deploy and efficiently maintain their IT environments in a more secure state. A result of this commitment is Windows Server 2003 Service Pack 1which enables businesses to provide more secure access anytime, anywhere, with any device, while helping to protect information assets against unauthorized access.

- Security Configuration Wizard (SCW) provides guided attack surface reduction for your server. It is highly recommended for configuring Windows Firewall and for creating security templates for role-based server lockdown.
- Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits.
- A range of new features provide increased security for Internet Explorer and Outlook Express.
- Computer wide DCOM restrictions address COM server exposure issues and give an administrator the capability to disable incoming DCOM activation, launch, and calls.
- Post-Setup Security Updates is designed to protect the server from risk of infection between the time the server is first installed and the application of the most recent security updates from Windows Update.
- Prompts used for file downloads, mail attachments, shell process execution, and program installation have been modified to be clearer and more consistent.
- Changes in the Remote Procedure Call (RPC) service help make RPC interfaces secure by default and reduce the attack surface of Windows Server 2003.
- Users can now log on to WebDAV servers for remote file access without fear of transmitting their password in the clear (unencrypted).
- Windows Firewall is not enabled by default. Only on new installations will Windows Firewall be enabled, which provides the computer more protection from many network-based attacks while it is being set up and configured.
- Users are now able to view and control the list of add-ons that can be loaded by Internet Explorer with more detailed control than before. In addition, crashes related to an add-on are detected and relevant information is presented to users.

## Did you know?

- By default, Windows Firewall is engaged during start-up on new installations of Windows Server 2003 Service Pack 1.
- Code with invalid signatures cannot be installed.
- SP1 helps to prevent code execution from data pages such as the default heap, various stacks, and memory pools.
- The ability is limited for malicious code to create distributed denial-of-service attacks and to send TCP/IP packets with a forged source IP address (or spoofed packets).




Microsoft Windows Server 2003

## Key Features

| Feature | Information |
|---|---|
| **Windows Firewall** | Now on by default in systems with new installations of Windows Server 2003 that include Service Pack 1 (also known as a slip-stream release). By default Windows Firewall is not enabled on upgrades to existing Windows Server 2003 installations, in order to maintain stable production configurations already in place and to avoid application compatibility issues on the server. Windows Firewall provides network protection after install while users update their system with the latest patches using the new Post-Setup Security Updates feature. |
| **Security Configuration Wizard** | A new feature in Windows Server 2003 with Service Pack 1 that provides guided attack surface reduction for your server. |
| **Post-Setup Security Update** | Designed to protect the server from the risk of infection between the time the server is first started and the application of the most recent security updates are applied from Windows Update. If Windows Firewall is enabled and the administrator did not explicitly enable Windows Firewall using an unattended-setup script or Group Policy, Post-Setup Security Updates opens the first time an administrator logs on. |
| **Data Execution Prevention** | A new set of hardware and software technologies that perform additional checks on memory to help protect against malicious code exploits. With Service Pack 1, an additional set of DEP security checks, known as software-enforced DEP, have been added to Windows Server 2003. |
| **Internet Explorer Information Bar** | Replaces many of the common dialog boxes that prompted users for information in previous versions and provides a prominent area for displaying information that users may want to view or act upon. |
| **Internet Explorer Pop-up Blocker** | Designed to block most unwanted pop-up windows from appearing. Pop-up windows opened when the end user clicks a link will not be blocked. |
| **WebDAV Redirector** | Allows computers running Windows Server 2003 to use WebDAV (Web-based Distributed Authoring and Versioning) servers, such as Windows SharePoint Services and MSN Communities, as if they were standard file servers. |

## SP1 Enhancements

Many of the new features available in SP1 are technologies that were first introduced with Windows XP Service Pack 2 (SP2), but many are specific to the Windows Server family of operating systems.

New features for Windows Server 2003 SP1 are:
- Security Configuration Wizard
- Post-Setup Security Updates

In addition, the implementation of a feature on the server operating system may differ from the implementation on the desktop operating system. Features included in Windows XP SP2, but that exhibit different behavior in Windows Server 2003 SP1 are:
- Data Execution Prevention
- Windows Firewall
- RPC Interface Restriction. This service pack also includes updates designed to improve the performance and stability of several Windows features.

## Examples

- Windows Firewall—Windows Firewall provides network protection while users update their system with the latest patches using the new Post-Setup Security Updates enhancement on new installation of Windows Server 2003 with Service Pack 1 (Slipstream installation only)
- Buffer Overflow Protection—Windows Server 2003 Service Pack 1 includes a set of hardware and software technologies, called Data Execution Prevention (DEP), that perform additional checks on memory to help protect against malicious code exploits. DEP detects code that is running from these locations and raises an exception when execution occurs. If the exception is unhandled, the process will be terminated.
- Attack Surface Reduction—Attack surface reduction is a fundamental security best practice, yet it is often difficult for server administrators to find the time to properly secure, test, and deploy a Windows server without breaking required functionality, which can lead to vulnerable servers within an organization. Security Configuration Wizard is a new feature in Windows Server 2003 Service Pack 1 that provides guided attack surface reduction for your server.
- Enhanced File Download Protection—The prompts that are used for file downloads, mail attachments, shell process execution, d program installation have been modified to be more consistent and clearer than they were in previous versions of Windows Server.

For more information about Windows Server 2003 Service Pack 1, visit http://www.microsoft.com/windowsserver2003/downloads/servicepacks/default.mspx. For the latest developer news and more information on Microsoft's broad range of resources for developers, including support programs, events, training, and the MSDN Library Online, visit MSDN Online at http://msdn.microsoft.com/.



0205 Part Number X11-17714