

# Guide to Deploying Microsoft Windows Server 2003 Service Pack 1 on Dell PowerEdge Servers

Microsoft® Windows Server™ 2003 Service Pack 1 (SP1) incorporates a set of security enhancements and tools designed to help administrators more effectively manage the security of their server installations when upgrading to SP1 on Windows Server 2003 systems or installing Windows Server 2003 with SP1 integrated. This article provides recommendations on the deployment process for Dell™ PowerEdge™ servers and discusses the key security features and remote management changes implemented in Windows Server 2003 SP1.

BY MIN-JOHN LEE, SCOTT M. CALLAWAY, AND JEFF FERRIS

## Related Categories:

*Change management*

*Dell OpenManage*

*Dell PowerEdge servers*

*Microsoft Windows Server 2003*

*Microsoft Windows  
Operating system (OS)*

*Remote management*

*Security*

*System deployment*

*Systems management*

Visit [www.dell.com/powersolutions](http://www.dell.com/powersolutions)  
for the complete category index to  
all articles published in this issue.

Deploying Microsoft Windows Server 2003 Service Pack 1 (SP1) can help enhance security and reliability, and simplify administrative tasks in environments using systems such as the Dell PowerEdge 1850, PowerEdge 2850, PowerEdge 6650, and PowerEdge 6850 servers as well as the PowerEdge 1855 blade server. Windows Server 2003 SP1 is the first cumulative service pack upgrade for the Windows Server System™ 2003 release. Although many of the security enhancements in SP1 have already been introduced in Microsoft Windows® XP Service Pack 2 (SP2) for the client environment, the server environment is characterized by specific traits that necessitated the SP1 release for Windows Server 2003. SP1 introduces certain features that require hardware-level support in the server, including data execution prevention (DEP) and demand-based switching (DBS).

Dell and Microsoft engineers worked together closely to support holistic SP1 software and hardware development, and performed extensive testing across supported Dell PowerEdge servers and Dell PowerVault™ network attached storage (NAS) servers to help ensure the compatibility and

stability of Dell software and hardware. In addition, Dell plans to release version 4.4 of the Dell OpenManage™ infrastructure in May 2005 to support the security enhancements and features in Windows Server 2003 SP1.

Dell supports Windows Server 2003 SP1 on server platforms that support the original Windows Server 2003 release—including third-generation through seventh-generation Dell PowerEdge servers as well as eighth-generation PowerEdge servers. This article is intended to help guide administrators in deploying SP1 on Dell PowerEdge servers and PowerVault NAS servers by examining two deployment scenarios: upgrading to SP1 on existing Windows Server 2003 systems and installing Windows Server 2003 with SP1 integrated.

In addition, this article addresses application compatibility and server manageability issues relating to the following major technologies in SP1:

- The DEP feature
- Windows Firewall
- Remote systems management

## Best practices for SP1 deployment

The first step in any deployment process is a careful evaluation of the existing IT environment. Documenting infrastructure—such as system BIOS, system and device firmware, and device driver versions; applications; and network components—is key to a successful service pack upgrade. In addition, administrators must first back up critical data and check systems for spyware and other unwanted software before upgrading to another service pack.

Performing essential housecleaning before deployment also helps smooth the migration process. Administrators should always perform BIOS, firmware, and driver updates prior to an OS upgrade.<sup>1</sup> The latest BIOS, firmware, and drivers are available from the Dell Web site or the Dell OpenManage management suite.

Besides updating BIOS, firmware, and drivers, administrators should check application compatibility before deploying any service pack. For an application compatibility evaluation, administrators can visit the Microsoft Windows Application Compatibility Web site and download the latest Application Compatibility Toolkit.<sup>2</sup>

### Deployment path for upgrading to SP1 on existing Windows Server 2003 systems

Before proceeding with deployment, administrators should note that specific Dell PowerEdge hardware configurations with factory-installed Windows Server 2003 operating systems may have a registry issue with the Windows Server 2003 SP1 upgrade. Administrators should run the Dell Registry Preparation tool (regprep) for these configurations prior to upgrading to SP1. For more information about the regprep utility and which servers may require preparation, visit [support.dell.com/support/topics/global.aspx/support/kb/en/document?c=us&cs=555&DN=1092292&l=en&s=biz](http://support.dell.com/support/topics/global.aspx/support/kb/en/document?c=us&cs=555&DN=1092292&l=en&s=biz). When upgrading current Windows Server 2003 systems to SP1, administrators have the following options:

- Upgrade from local media using the SP1 installation CD
- Install from a network share containing the installation files
- Upgrade over the Internet using Microsoft Windows Update<sup>3</sup>
- Automate the deployment process by using an enterprise software deployment tool such as Microsoft Systems Management Server 2003 (SMS 2003)

Upgrading from local media is the simplest method of installing Windows Server 2003 SP1. Upgrading from a network share is also a simple installation method and eliminates the need for media.

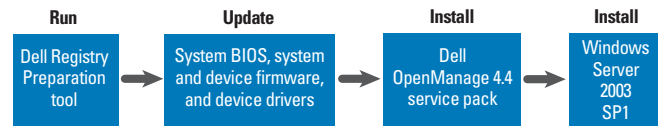


Figure 1. Recommended installation process on servers running Dell OpenManage 4.3

To use Microsoft Windows Update for SP1 deployment, administrators should go to the Windows Update Web site, install the update plug-in for Internet Explorer, and then install SP1. Service packs are listed in the High Priority Updates section. Administrators can configure updates to download automatically and then install applicable service packs and hot fixes either automatically or manually.

Each of the three preceding options—upgrading from local media, installing from a network share, and upgrading over the Internet using Windows Update—may entail a lengthy process for organizations that have many servers to upgrade. Thus, the fourth option—automating the process using an enterprise software deployment tool—is the preferred method for most large and midsize organizations. Many enterprise management tools exist; however, Microsoft SMS 2003 is designed to streamline SP1 upgrades with its integrated Distribute Software Updates Wizard. After authorizing Microsoft Windows Server 2003 SP1 in the SMS 2003 administration console, administrators can configure SMS 2003 to identify any systems joining the managed network and then deploy SP1 without manual intervention. Administrators can also configure SP1 settings by establishing group policies or by using an additional package distributed by SMS.<sup>4</sup>

To upgrade to SP1 on an existing system running Windows Server 2003, Dell supports the two following deployment paths:

- **Dell OpenManage 4.3:** Administrators should run the regprep tool;<sup>5</sup> update the system BIOS, system and device firmware, and device drivers; install the Dell OpenManage service pack for version 4.4 (which will be available at [support.dell.com](http://support.dell.com)); and then install SP1 (see Figure 1).

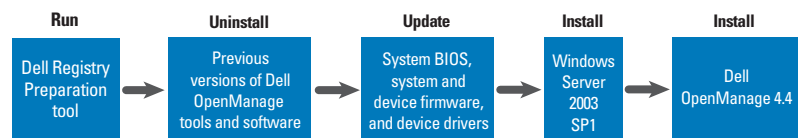


Figure 2. Recommended installation process on servers running Dell OpenManage 4.2 or earlier

<sup>1</sup> For information about BIOS, firmware, and driver updates on specific Dell PowerEdge and PowerVault NAS servers, visit [support.dell.com](http://support.dell.com).

<sup>2</sup> For information about application compatibility, visit [www.microsoft.com/windows/appcompatibility/default.mspx](http://www.microsoft.com/windows/appcompatibility/default.mspx). To download the Microsoft Windows Application Compatibility Toolkit, visit [msdn.microsoft.com/library/en-us/dnanchor/html/appcompat.asp](http://msdn.microsoft.com/library/en-us/dnanchor/html/appcompat.asp).

<sup>3</sup> For Windows Update information and downloads, visit [windowsupdate.microsoft.com](http://windowsupdate.microsoft.com).

<sup>4</sup> For more information about incorporating SMS 2003 into a deployment strategy, visit [www.microsoft.com/sms/server](http://www.microsoft.com/sms/server).

<sup>5</sup> For more information about regprep use, visit [support.dell.com](http://support.dell.com) and search on the keyword "regprep."

- **Dell OpenManage 4.2 or earlier:** Administrators should run regprep; uninstall the previously installed Dell OpenManage tools and software; update the system BIOS, system and device firmware, and device drivers; install SP1; and then install Dell OpenManage 4.4 (see Figure 2).

For the latest SP1 upgrade information or compatibility alert, visit [www.dell.com/microsoft](http://www.dell.com/microsoft).

### Deployment path for installing Windows Server 2003 with SP1 integrated

For a new deployment of Windows Server 2003 with SP1 integrated, Dell offers several methods for ordering and installing Microsoft operating systems on Dell PowerEdge servers:

- Dell factory installation
- Dell OpenManage Server Assistant 8.6
- Dell Professional Services
- Altiris Deployment Solution for Dell Servers
- Microsoft Windows provisioning methods

**Dell factory installation.** Dell engineers worked closely with Microsoft engineers to validate and incorporate the latest Dell-qualified and Microsoft-qualified drivers into preinstallation OS images. If organizations order a Dell PowerEdge server with the option to have Windows Server 2003 with SP1 preinstalled, Dell deploys a custom OS image when the system is built in the Dell manufacturing facility. This option is designed to ensure that purchased systems integrate the latest Dell BIOS, firmware, and drivers as well as the latest version of Dell OpenManage infrastructure.

**Dell OpenManage Server Assistant 8.6.** Bundled with Dell OpenManage 4.4, Dell OpenManage Server Assistant (DSA) 8.6 supports a clean OS installation of Windows Server 2003 with SP1 on Dell PowerEdge servers. The System Update Utility in the Dell OpenManage 4.4 release also contains system BIOS updates, firmware, drivers, and utilities that administrators require to deploy and manage PowerEdge servers. Dell includes DSA with PowerEdge servers and also makes DSA available through the Dell OpenManage Subscription Service.<sup>6</sup>

**Dell Professional Services.** Dell offers many fee-based custom solutions that can be tailored to help reduce the impact of server upgrades and deployments on the supporting IT organization.<sup>7</sup>

**Altiris Deployment Solution for Dell Servers.** Dell and Altiris have collaborated to provide a simple-to-use deployment solution called the Altiris Deployment Solution for Dell Servers.<sup>8</sup> This approach provides administrators with easy-to-modify deployment scripts that can be used to manage system deployment for Dell PowerEdge servers.

**Microsoft Windows provisioning methods.** Microsoft has designed the following four tools to help automate SP1 deployment and customize installations:<sup>9</sup>

- Microsoft System Preparation (sysprep.exe)
- Unattended Setup (winnt32.exe)
- Remote Installation Services (RIS)
- Automated Deployment Services (ADS)

Sysprep.exe, which is included with the Microsoft Windows OS, helps administrators perform image-based installations of identical operating systems and software configurations on multiple systems quickly and efficiently. For unattended installation, Microsoft offers several tools that use answer files to automate the installation process. Answer files enable administrators to quickly install the Microsoft OS in Unattended Setup mode on multiple servers. Because answer files contain the required setup information—including system name, network adapter configuration, and Windows Firewall configuration—they enable administrators to easily perform unattended installations of Microsoft operating systems on multiple servers.

RIS and ADS are designed to permit network-initiated setup, enabling administrators to deploy both client and server operating systems on bare-metal servers that support Preboot Execution Environment (PXE).<sup>10</sup> Starting in SP1, network-based OS deployment is more secure because, during OS installation, the OS installation program applies a lock-down policy to the network interface to help prevent network-based attacks from occurring before security settings have been configured.

### Application compatibility and server management

The security enhancements, features, and changes in SP1 may lead to application compatibility and server manageability concerns. This section addresses compatibility and manageability issues for three main aspects of SP1: the DEP feature, Windows Firewall, and remote systems management. In addition, this section discusses

<sup>6</sup> For more information about the Dell OpenManage Subscription Service, visit [www1.us.dell.com/content/topics/global.aspx/services/en/om\\_subscr\\_svc?c=us&cs=04&l=en&s=bsd](http://www1.us.dell.com/content/topics/global.aspx/services/en/om_subscr_svc?c=us&cs=04&l=en&s=bsd).

<sup>7</sup> For more information about Dell services, visit [www.dell.com/services](http://www.dell.com/services) or contact a Dell sales representative.

<sup>8</sup> For more information about systems management products from Dell and Altiris, visit [www.dell.com/altiris](http://www.dell.com/altiris) and see "Simplifying IT Operations with Altiris Deployment Solution for Dell Servers" by Todd Muirhead; Dave Jaffe, Ph.D.; and Landon Hale in *Dell Power Solutions*, May 2005.

<sup>9</sup> For more information about Windows OS provisioning methods, see "Guide to Deploying Microsoft Windows Server 2003 on Dell PowerEdge Servers" by the Dell Server Operating Systems Engineering Group in *Dell Power Solutions*, Special Issue, May 2003.

<sup>10</sup> For a list of the operating systems that can be deployed using RIS or ADS and for a comparison of RIS and ADS, visit [support.microsoft.com/?kbid=842564](http://support.microsoft.com/?kbid=842564).

two security tools introduced in SP1 to help provide post-installation server security management:

- **Security Configuration Wizard:** This tool is designed to allow system administrators to easily create and deploy security policies.
- **Post-Setup Security Updates:** This tool is designed to allow the newly installed OS to safely connect to the Internet and perform security updates.

See the “Windows Firewall” and “Remote systems management” sections in this article for more information about these two post-installation server security management tools.

### Data execution prevention

DEP describes a set of technologies that help protect against malicious exploits by using a combination of hardware- and software-enforced memory protection methods. Hardware DEP implementations are available for 32-bit platforms running Physical Address Extension (PAE) or 64-bit extended architecture. Hardware-based DEP requires no-execute (NX)-capable processors. Dell PowerEdge servers shipped since October 2004 have NX-capable processors.<sup>11</sup>

In hardware DEP implementations, the processor keeps track of virtual memory pages, determining on a per-page basis whether a memory page should contain executable code. If a page reserved for nonexecutable code attempts to execute code, the hardware catches the exception and prevents the code from running.

Software-enforced DEP under Windows Server 2003 SP1 augments hardware DEP by providing an additional layer of security checks to prevent potential malicious exploitation of the exception-handling mechanisms in Windows Server 2003. Software DEP works alone or with compatible microprocessors to mark memory locations as NX. If a program tries to run any code—malicious or not—from a protected NX memory location, DEP closes the program and notifies the administrator.

To support hardware DEP, the system processor must support NX technology, the system BIOS must be NX-aware, and required PAE modules must be loaded during OS boot. Because the default setting in SP1 is to turn on hardware and software DEP for both OS kernel services and application levels, it is critical that administrators evaluate driver and application compatibility before deploying SP1. Many 64-bit device drivers were written for 64-bit versions of Windows and were required to be DEP- and PAE-compliant to function properly. Administrators should use the Dell Software Update Utility CD to update device drivers before upgrading to Windows Server 2003 SP1. *Note:* On 32-bit

Windows versions running on systems supporting hardware DEP, device drivers may encounter technical issues caused by DEP or PAE mode being enabled. However, Dell has performed extensive testing and Microsoft Windows Hardware Quality Labs (WHQL) qualification on all supported device drivers.

For application compatibility, software developers must explicitly define executable memory segments in their application code.<sup>12</sup> If a business application encounters a compatibility issue after upgrading to SP1, developers can add the application to the DEP application exception list until the issue is resolved. To access the DEP administrative page in the system applet, administrators can right-click on My Computer, select the Properties menu item, click the Advanced tab, select Settings from the Performance section, and click the DEP tab.

**BIOS requirements for NX and DBS support.** Because hardware DEP requires memory protection-capable processors, Dell servers equipped with NX-capable Intel® processors require a BIOS update. A BIOS update is also required to support DBS. By throttling down processor frequency when the OS determines the processor utilization rate is low, DBS can help save power. DBS support in the OS leverages Enhanced Intel SpeedStep® Technology<sup>13</sup> and is dependent on the processor model, frequency, and stepping. To determine whether a given Dell PowerEdge server supports DBS, administrators can check the CPU Information menu in the BIOS settings. If the Demand-Based Power Management option is editable, then all processors in the system support DBS. If the option is not editable, at least one processor in the system does not support DBS. To turn on the DBS feature in the OS, select the Power Options icon in the Control Panel, and then select the “Server Balanced Processor Power and Performance” power scheme.

**Mitigation.** For server systems engineers, many system-level DEP configuration options can be controlled using the `/noexecute=DEP_option` switch specified in the boot.ini file, where `DEP_option` can be one of the following:

- `OptIn`: DEP is enabled for Windows programs and system services, and for other applications that have been explicitly identified.
- `OptOut`: DEP is enabled for applications and services. Specific applications can be excluded from DEP using the DEP application exception list or using the Microsoft Application Compatibility Toolkit as a reference.
- `AlwaysOn`: DEP applies to processes, with no exceptions.
- `AlwaysOff`: DEP does not apply to processes, and the processes will not run in PAE mode unless the `/PAE` switch is specifically included in the boot.ini entry.

<sup>11</sup> For more information about NX-capable processors, visit [www.intel.com/business/bss/infrastructure/security/xdbit.htm](http://www.intel.com/business/bss/infrastructure/security/xdbit.htm).

<sup>12</sup> For the most up-to-date application compatibility information, visit [msdn.microsoft.com](http://msdn.microsoft.com).

<sup>13</sup> For more information about Enhanced Intel SpeedStep Technology, visit [www.intel.com/cd/ids/developer/asm-na/eng/195910.htm](http://www.intel.com/cd/ids/developer/asm-na/eng/195910.htm).

For scripted deployments, the preceding DEP options can be specified through the unattend.txt file.

## Windows Firewall

Windows Server 2003 SP1 is designed to enable the same firewall features for servers that Windows XP SP2 provides for desktop computers. The default firewall setting is “Off” after a clean installation of Windows Server 2003 with SP1 integrated.

For an SP1 upgrade, firewall settings honor the pre-SP1 configuration. If administrators enable the firewall after an SP1 upgrade, they must identify which applications and network ports are required for the servers in the environment to provide services to network clients. Administrators can add these applications and network ports to the firewall exception list, identify which network clients can access specific services or applications, and control exceptions independently for each network interface card (NIC) in the system.

Once administrators have identified necessary exceptions, they can configure firewall options on individual systems by selecting the Windows Firewall applet from the Control Panel or by using the `netsh firewall set portopening TCP 3389 ENABLE` command allows connections to TCP port 3389—the default port for Windows Terminal Server and Remote Desktop for Administration. The configuration set using either the applet or command line will be persistent unless it conflicts with options configured through a domain group policy. In a Microsoft Active Directory® directory service domain environment, group policy can be used to enable or disable Windows Firewall and configure exceptions for groups of servers.

The Security Configuration Wizard (SCW) is a server-specific tool introduced in SP1 that allows system administrators to easily create a set of security policies based on the server role, and apply the security policy set to one server or a group of servers. A SCW security policy includes Windows Firewall configuration, configuration of the system registry, and turnoff of unused system services to reduce attack surface.<sup>14</sup>

## Remote systems management

Post-Setup Security Updates (PSSU) is a feature introduced in SP1 that enables Windows Firewall services and runs automatically in the console session directly following a clean installation of Windows Server 2003 with SP1 integrated. The purpose of this feature is to allow a system to safely connect to the Internet and perform security updates. The default network security policy is to block incoming traffic on every network port except network ports required to perform PSSU over the Internet.

Because the network connection to the target system is blocked during a remote OS deployment, the system administrator must physically visit the system console or use a Dell remote access controller (RAC) to finish the PSSU. After the PSSU, the network security policy is unloaded and Windows Firewall services will be turned off to the default state.

TCP port 445 is blocked when Windows Firewall is first enabled. As a result, many of the Microsoft Management Console (MMC) snap-ins will fail when attempting to administer remote systems, as will the Find Users and Computers utility, resource kit utilities, and other utilities and third-party products that depend on the Server Message Block (SMB) protocol over TCP/IP. Examples of MMC snap-ins and utilities that depend on this TCP port include:

- Computer Management (compmgmt.msc)
- Device Manager (devmgmt.msc)
- Event Viewer (eventvwr.msc)
- Group Policy Results (gpresult.exe)
- Resultant Set of Policy (rsop.msc)
- Net services commands (net.exe)

Administrators who use Windows Terminal Server or Remote Desktop for Administration to remotely administer servers will also need to open TCP port 3389 unless they have configured Terminal Server to use an alternate port.

## Toward successful upgrades to SP1

Unlike previous Microsoft OS service pack releases, Windows Server 2003 SP1 introduces major changes and features that can help significantly enhance the security of the OS. Carefully considering the deployment paths explored in this article and evaluating the application compatibility and server management issues identified will help administrators plan and execute the optimal route to smooth deployment in their organizations. [➤](#)

**Min-John Lee** is a software engineering consultant in the Server Operating Systems Engineering department in the Dell Product Group—Enterprise Software Development. Min-John has an M.S. in Electrical and Computer Engineering from Northwestern University.

**Scott M. Callaway** is a software engineer in the Server Operating Systems Engineering department in the Dell Product Group—Enterprise Software Development. Scott has a B.S. in Management from Stephen F. Austin State University.

**Jeff Ferris** is a manager in the Dell IT Engineering department. Jeff has a B.S. in Computer Information Systems from Southwest Missouri State University.

<sup>14</sup> For more information about how to use SCW, select Help and Support from the Start menu.