Using Diskeeper® with Windows® XP Service Pack 2, Windows Server® 2003 Service Pack 1 and Windows Vista

1.0 Introduction

Service Pack 2 (SP2) for Windows XP and Service Pack 1 (SP1) for Windows Server 2003 contain a number of security-related enhancements to their respective operating systems. Some of these enhancements affect the operation of certain network functionality in Diskeeper. This document describes the relevant security features of these service packs and what configuration changes are needed to allow Diskeeper to function in harmony with them. Additionally, Windows Vista contains similar security features, so configuration changes may also be necessary under that operating system

Please Note: For simplicity, this document refers to Windows XP SP2 throughout, although the information presented here also applies to Windows Server 2003 SP1 and Windows Vista.

2.0 SP2 Security Features that Affect Diskeeper

The following aspects of SP2 affect Diskeeper:

2.1 Windows Firewall

After the installation of SP2 the Windows Firewall is enabled by default, and is configured to close most network ports. The Windows Firewall acts to disallow unsolicited connections to any listening port unless that port, or the application that is listening on it, is specifically configured in the firewall to accept connections. This means that applications like internet browsers that use ports to connect OUT will work through the Windows Firewall as it is installed by default, and applications that listen to accept INCOMING connections (such as the IIS web server) won't.

Generally, client applications will work, and server applications won't. Even though client applications have incoming network communication to return data they have requested, since this data has been requested by the client it is allowed through the Windows Firewall on the client machine. Only truly unsolicited connection requests are stopped.

For more information, see the *Windows Firewall* link on this page of the Microsoft® web site: http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

Some Diskeeper Corporation products listen for unsolicited network connections for a number of reasons. For example, the Diskeeper service listens for connections from the Diskeeper Administrator to set new defragmentation policies on a machine.

2.2 Increased RPC Security:

Access control restrictions are increased for the Remote Procedure Call (RPC) facility in Windows XP after the installation of SP2. Some Diskeeper Corporation products, such as Diskeeper Administrator, use RPC and can be affected by these changes.

For more information, see the *RPC Interface Restrictions* link on this page of the Microsoft web site:
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

2.3 Increased DCOM Security:

Access control restrictions are increased for the Distributed Component Object Model (DCOM) facility in Windows XP after the installation of SP2. Diskeeper (v8.0 and earlier) uses DCOM and can be affected by these changes.

For more information, see the *DCOM Security Enhancements* link on this page of the Microsoft web site:
http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/sp2netwk.mspx

3.0 Configuration Methods

Several methods are available for configuring the Windows Firewall before, during and after the installation of Windows XP SP2. Several of these methods are covered in detail in a Microsoft document which can be downloaded from their web site: Deploying Windows Firewall Settings

Diskeeper Corporation recommends the use of Active Directory® Group Policy where possible to configure SP2 for Diskeeper Corporation products. This configuration method can be used either before or after installing SP2 on machines, and is easy and flexible. It is described in a separate document: *Diskeeper_Corporation_Group_Policy_Config.doc*, which is available on the Diskeeper Corporation website: http://www.diskeeper.com/sp2

For systems that are not members of an Active Directory Domain, batch scripts are available at www.diskeeper.com/sp2 to configure SP2 systems for compatibility with Diskeeper or Diskeeper Administrator. There are two scripts available for Diskeeper, *Diskeeper_Client_Firewall_Config.bat* and *Diskeeper_Admin_Firewall_Config.bat*, which configure the firewall for Diskeeper either Diskeeper or Diskeeper Administrator, respectively.

The scripts must be delivered to the target machines and run by some method worked out by the system administrator. This could involve the use of a system startup script, putting the script on a shared server disk and running it from there, or putting it on a floppy disc and invoking it on each of the target machines. The actions taken by the scripts require Administrator privileges, so the distribution method must take this into account.

The scripts are run in a command window by changing the current directory to the location of the script file and invoking it in a manner similar to the following:

```
C:\>DK_Admin_Firewall_Config
```

4.0 Diskeeper-Related SP2/SP1 Notes

This section contains specific information about Diskeeper on SP2/SP1 systems.

4.1 Product Impact

Diskeeper Home Edition is not affected by SP2.

Diskeeper Professional, Diskeeper Pro Premier, Diskeeper Server Standard, and Diskeeper EnterpriseServer editions are not affected in terms of performing their functions on the machine they are installed on.

Diskeeper Administrator is affected by SP2. The PushInstall™ software deployment feature requires file and print sharing or remote administration be enabled on remote machines. With SP2, the ports required to use these services are blocked.

The scheduling, polling, and network refresh features in Diskeeper Administrator are also affected by SP2. The additional DCOM restrictions placed on the machine with SP2 by default do not allow Diskeeper Administrator to send and receive data from the Diskeeper installations on the remote machines.

4.2 Requirements for Diskeeper

To deploy Diskeeper to a system using the PushInstall software deployment feature, File and Print Sharing must be allowed on the target machine.

To accept incoming connections to set defragmentation schedules, monitor fragmentation or other administrative type tasks. Diskeeper requires the following:

- DkService.exe is on the Windows Firewall Exceptions list as an allowed program. You can also specify that ports 31038 and 31058 be listed as an open port.