Using Diskeeper® Corporation Products 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 Corporation's Diskeeper, Undelete® and Sitekeeper® products. This document describes the relevant security features of these Service Packs and what configuration changes are needed to allow each Diskeeper Corporation product 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 Corporation Products

The following aspects of SP2 affect Diskeeper Corporation products:

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. Examples are the Diskeeper service listening for connections from the Diskeeper Administrator to set new defragmentation policies on a machine, or the Undelete service listening

for requests from remote Undelete User Interface applications to access the Recovery Bin on that 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 Sitekeeper, 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. Some Diskeeper Corporation products, such as earlier versions of Diskeeper, use 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.pdf*, which is available on the Diskeeper Corporation web site: http://www.diskeeper.com/sp2

For systems that are not members of an Active Directory Domain, you can download product-specific batch scripts to configure SP2 systems for compatibility with Diskeeper Corporation products from www.diskeeper.com/sp2.

The these batch scripts are designed to be run on any Windows XP SP2 machines that are running or will be running any of the following Diskeeper Corporation products:

Diskeeper 2007 (all except Home Edition)
Diskeeper 10.0 (all except Home Edition)
Diskeeper 9.0 (all except Home Edition)
Undelete 5.0 (all except Home Edition)
Undelete 4.0 (all except Home Edition)
Sitekeeper 3.5
Sitekeeper 3.1

In most situations, only one of these approaches (Group Policy changes or the configuration script) needs to be used. If a machine is covered by Active Directory Group Policy, there is no

need to also run the script on that machine. (Keep in mind you can use Group Policy to push the script out to remote machines as a login script.)

The script must be delivered to the target machine 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 script require Administrator privileges, so the distribution method must take this into account.

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

```
C:\>Diskeeper_Firewall_Config
```

Most of the configuration changes from running the script are visible from, and can be modified or undone, via the Windows Firewall configurations screens accessed by double clicking "Windows Firewall" in the Windows Control Panel.

4.0 SP2 Issues by Product

This section contains the configuration requirements by product for those Diskeeper Corporation products affected by SP2.

4.1 Diskeeper:

4.1.1 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.

4.1.2 Requirements for Diskeeper 9 through Diskeeper 2007

To deploy Diskeeper 9, Diskeeper 10, or Diskeeper 2007 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.

4.1.3 Requirements for Earlier Diskeeper Versions

If you are using a version of Diskeeper prior to Diskeeper 9 on a networked system running SP2, contact Diskeeper Corporation Technical Support at tech_support@diskeeper.com for information about configuring the system for Diskeeper operation.

4.2 Undelete:

4.2.1 Product Impact

Undelete Home Edition does not accept incoming connections, and is therefore not affected by SP2.

Undelete Professional Edition running on the "target machine" will accept properly authorized incoming remote connections from remote copies of Undelete Server Edition. Over one of these connections an administrator can change Undelete properties, modify the exclusion list, access the Recovery Bin or search for actually deleted files directly from disk on the target machine. To accept such connections the Undelete service listens on a network port. This listen operation is stopped by the default Windows Firewall settings.

Undelete Server Edition running on a target machine accepts incoming connections from remote copies of Undelete Professional or Server to directly access files in the Recovery Bin deleted from mapped shares located on the target machine. Undelete Server Edition also accepts the administrative type connections from other Undelete Server copies as described above for Undelete Professional Edition. Both types of incoming connections require listening on the network port, which is stopped by default by Windows Firewall.

The Undelete PushInstall features copies an agent and the package to be installed to the target machine, and then runs the agent to start the installation of the software. The default security changes in SP2 block the transfer of the agent and the install package to the target machine.

4.2.2 Requirements

Undelete Server Edition requires that the Undelete service, UdServe.exe be added to the Windows Firewall Exceptions list to accept incoming mapped-share type connection requests to access the Recovery Bin. In addition, to accept incoming administrative type requests from other copies of Undelete Server, Remote Administration exceptions must be allowed. If Undelete Server is to be deployed to a system using PushInstall, Remote Administration exceptions must be allowed on the target machine.

Undelete Professional Edition requires no changes to run with SP2 unless Undelete Server is used to administer it remotely or the product is deployed using PushInstall. If incoming connections from Remote Server are desired, UdServe.exe must be on the Windows Firewall Exceptions list and Remote Administration exceptions must be allowed. If Undelete Professional is to be deployed to a system using PushInstall, Remote Administration exceptions must be allowed on the target machine.

If administrative-type connections are to be made between Undelete Server Edition running on a Windows NT 4.0 machine and Undelete Server or Professional running under SP2, or if Undelete is to be PushInstalled from Windows NT 4.0 or Windows XP SP1, the SP2 machine must have File and Print Sharing enabled in the Windows Firewall.

Undelete Home Edition does not require any changes to run with SP2.

The ‘Connect to Remote Computer’ functionality in Undelete 3.0 Server edition is not supported under Windows XP SP2.

4.3 Sitekeeper:

4.3.1 Product Impact

Sitekeeper Agent running on the client machine will accept properly authorized incoming remote connections from remote copies of the Sitekeeper Console. The Sitekeeper Console sends requests over these connections to the Sitekeeper Agent to scan the machine, to access the network shared folder for software deployment and to change the agent properties. To accept such connections, the Sitekeeper Agent listens on a network port. This listening operation is stopped by the default Windows Firewall settings.

The Sitekeeper Console, running on a console machine, accepts incoming connections from remote Sitekeeper Agents on client machines. Over these connections remote agents send data back to the Sitekeeper console. These incoming connections require listening on a network port, which is stopped by default by the Windows Firewall.

The Sitekeeper Console also uses Windows services such as remote WMI access and remote registry access running on remote machines to acquire software and hardware inventory data. Those services are blocked by the default Windows Firewall settings.

4.3.2 Requirements

To run with Windows XP SP2, Sitekeeper 3.1 Build 190 or later must be used.

If Sitekeeper is installed on a target machine with XP SP2, TCP port 31041 must be enabled through the firewall for Sitekeeper remote agents to connect back to the console.

If a target computer without Sitekeeper agent installed has XP SP2, File and Print Sharing exceptions must be enabled through the firewall, and TCP port 31040 must be on the exceptions list, for Sitekeeper to deploy software to the target machine.

If a target computer running XP SP2 has Sitekeeper agent installed, TCP port 31042 must be on the exceptions list for Sitekeeper to perform inventory scanning of the target or to deploy software to it.

If IP security is enabled on the network, UDP ports 4500 and 500 must be on the exceptions list on every target computer running SP2 that Sitekeeper manages. If the computer on which Sitekeeper is installed is running SP2, these ports must be on the exceptions list on that computer as well.

No Windows Firewall changes are needed for Sitekeeper to scan the system on which it is installed.

If the following ports are on the Windows Firewall exceptions lists on the target machines with XP SP2, Sitekeeper Build 190 and above will be able to scan these machine for inventory data and deploy software to these machines without issues:

- TCP Port 31041 to enable RPC connections.
- TCP Port 31040 to enable RPC connections.
- TCP Port 31042 to enable RPC connections.

- UDP Port 4500 to enable IPSec use
- UDP Port 500 to enable IPSec use
- File and Print Sharing for inventory scan and PushInstall.

If Sitekeeper needs to access SQL server on a different machine which is running XP SP2, the following must be on the exceptions list of the machine running SQL server:

- File and Print Sharing exception must be enabled
- UDP Port 1434