SIOS Protection Suite for Windows

v8.5

Release Notes

January 2017

To maintain the quality of our publications, we welcome your comments on the accuracy, clarity, organization, and value of this document.

Address correspondence to:
ip@us.sios.com

Table of Contents

SIOS Protection Suite for Windows

Version 8.5

(Version 8 Update 5)

Important!!

Read This Document Before Attempting To Install Or Use This Product!
This document contains last minute information that must be considered before, during and after installation.

To maintain the quality of our publications, we welcome your comments on their accuracy, clarity, organization and value.

Introduction

This information is provided for the person who installs, configures and/or administers the SIOS Protection Suite (SPS) for Windows product and contains important information such as version requirements, last-minute changes to instructions and procedures, product restrictions and known issues. It is important that you review this document before installing and configuring the SIOS Protection Suite software.

SIOS Protection Suite Product Descriptions

SIOS Protection Suite for Windows is a software bundle that integrates high availability clustering and data replication functionality to protect mission-critical data and applications and includes DataKeeper (DK), LifeKeeper (LK) and optional Recovery Kits.

LifeKeeper for Windows

LifeKeeper for Windows continues SIOS Technology Corp.'s tradition of providing world-class reliability for mission critical applications. LifeKeeper for Windows leverages over a decade of experience with high availability platforms by providing customers the ability to cluster multiple servers in order to monitor and restore their applications. In the event of a failure, LifeKeeper recovers all network interfaces, data and applications. Recovery occurs automatically and is transparent to clients, thus minimizing downtime and loss of business.

LifeKeeper for Windows enables continuous operations during planned downtime as well as in the event of a system or application failure. With LifeKeeper, the amount of downtime required for common maintenance tasks and upgrades is significantly reduced or eliminated.

DataKeeper for Windows

SIOS DataKeeper is a highly optimized host-based replication solution which ensures your data is replicated as quickly and as efficiently as possible from your source server across the network to one or more target servers.

New Features of SIOS Protection Suite for Windows Version 8

Feature	Description
New in This Release	
CHANGEMIRRORTYPE	This EMCMD command is used to change the mirror type of a mirror that is part of a DataKeeper job.
Microsoft SQL Server 2016 support	The SIOS Protection Suite SQL Server Recovery Kit supports Microsoft SQLServer 2016.
Tunable bitmap block size	Users can modify the effective size of an entry in the DataKeeper intent log (bitmap) by changing the BitmapBytesPerBlock registry value.
General maintenance	See Bug Fixes below.
New in Version 8.4	
Target Bitmap File	Target writes are now tracked in a persistent target bitmap file.
General maintenance	See Bug Fixes below.
New in Version 8.3	
DataKeeper Notification Icon	The DataKeeper Notification Icon shows a summary of your DataKeeper mirrors in the Windows Notification Tray. In addition to the display functions, the DataKeeper Notification Icon also serves as a shortcut to managing your DataKeeper mirrors.
Oracle 12c and Oracle 12c Standard Edition 2	SIOS Protection Suite for Windows Version 8.3 and later supports Oracle 12c and Oracle 12c Standard Edition 2 (excluding pluggable database).
Powershell cmdlet support	Powershell cmdlets that can be used to create job(s), create mirror(s), remove job(s), remove mirror(s) and fetch information about a volume used in DataKeeper (New-DataKeeperMirror, New-DataKeeperJob, Remove-DataKeeperMirror, Remove-DataKeeperJob, Add-DataKeeperJobPair, Get-DataKeeperVolumeInfo).
mirrorcleanup.cmd	This command will remove all remnants of a mirror for a selected volume on the local system only and should only be run when recommended by SIOS Support.
DKHEALTHCHECK	Support status and issue identification tool. Provides command line interface for basic mirror status and problem detection.

Feature	Description
General maintenance	See Bug Fixes below.
New in Version 8.2.1	
General maintenance	Bug Fixes.
New in Version 8.2	
General maintenance	Bug Fixes.
New in Version 8.1	
Microsoft Windows Server 2012 R2 Support	LifeKeeper Version 8.1 and later supports Windows Server 2012 R2.
General maintenance	Bug Fixes.
New in Version 8.0.1	
General maintenance	Bug Fixes.
New in Version 8.0	
General maintenance	Bug Fixes.

Bug Fixes

The following is a list of the latest bug fixes and enhancements.

	Description
3629	Provide a tunable VSS quiesce timeout
4061	New-DataKeeperJob cmdlet should fail when passed invalid strings for volume letters
4062	EMCMD CREATEJOB and EMCMD UPDATEJOB commands should fail when passed invalid strings for volume letters
4063	EMCMD CREATEJOB and EMCMD UPDATEJOB commands should fail when passed invalid strings for mirror types
4089	Implement two-phase device removal logic
4098	Added check to CREATEMIRROR to verify bytes per sector on the source and the target match
4134	Implement a VSS Provider to properly quiesce source system during target snapshot initialization
4136	Fixed BSOD in NDIS / TCP driver accessing a buffer that ExtMirr had freed
4149	Prevent BSOD during resync with an inaccessible disk
4154	Updated LifeKeeper to JRE1.8.0_101
4156	Improved product license expiration warnings in the event log
4157	dksupport.cmd Event Log entries are viewable on non-DataKeeper servers
4160	SQL Kit: Cannot protect optional services during named instance Resource Create

	Description
4161	SQL Kit: SQL CurrentVersion not found correctly
4162	SQL Kit: deepchk could not access the ReportServer database
4166	Corrected issue storing and retrieving information from LifeKeeper registry
4167	SQL Kit: The Optional Services to Protect List during SQL Server resource create is incomplete for a Named Instance
4169	Implement Disable/Enable Status Updates option in EMTray
4170	lksupport.cmd Event Log entries are viewable on non-LifeKeeper servers
4174	Automatically create BitmapBaseDir path if folders don't exist
4176	dksupport.cmd archive includes the msinfo database

Product Requirements

Operating System

Important: SIOS Technology Corp. recommends that users use Domain accounts that have local administrator privileges on all servers running SIOS Protection Suite. If local accounts are being used, the user names and passwords must match on all servers running SIOS Protection Suite. This recommendation is for all editions and all platforms.

Note: All servers within a cluster should be running the same version of Windows.

Product	Operating Systems	Additional Software
SIOS Protection Suite (Server Components)	See the SPS Support Matrix	n/a
SIOS Protection Suite (User Interface)	See the SPS Support Matrix	MMC 3.0 - download from: http://support.microsoft.com/kb/907265

Product	Operating Systems	Additional Software
Virtual Environments	The operating system versions listed above are supported for guests running on the following virtual platforms: • Amazon EC2 (AWS) • VMware vSphere 4.0 or later • Microsoft Hyper-V Server 2008 R2 or later • Citrix XenServer 5.5 or later • KVM with Kernel 2.6.32 or later	
64-bit versions (x64, no Itanium) of all of the listed OS platforms are supported		

Requirements for Windows 2008 R2 and 2012

While installing SIOS Protection Suite on Windows 2008 R2, a dialog box will prompt whether the installer should make the system configuration changes described below. If the installer is not allowed to make these changes, they will need to be made manually after installation is complete.

- Windows Firewall
- The **Distributed Link Tracking Client** must be **disabled**

For systems running SIOS Protection Suite for Windows and Microsoft FTP Service 7.5 for IIS 7.0, Windows 2008 R2 or later is required.

In addition, if your Windows 2008 R2 and 2012 servers are not in a domain, the Local Security policy setting "***Network Access: Let Everyone permissions apply to anonymous users***" must be enabled. If the servers are in a domain, then this setting is not required.

SIOS Protection Suite Requirements

The following table shows requirements applicable to the SIOS Protection Suite core and recovery kits.

Core	Requirement(s)
SIOS Protection Suite License	One license is required for every server on which SIOS Protection Suite runs. This applies to both physical and virtual servers.
LAN Manager Recovery Kit	Requires the "**File and Print Sharing for Microsoft Networks**" component (lanmanserver) to be installed on the Windows server. NetBIOS must also be enabled. Otherwise, the LAN Manager resource will not come in service.
Memory Requirements	The minimum memory requirement for a system supporting SIOS Protection Suite for Windows is based on the memory requirements for the operating system being used. Additional memory is required to run user applications in addition to that required for SIOS Protection Suite.
GUI	**Ports:** SIOS Protection Suite uses Port 82 for Remote Method Invocation (RMI) communication between the GUI server and client. The LifeKeeper GUI uses Port 81 for its administration web server which should be different from any public web server. This is used by the GUI when run as a Java applet on a remote client. In the event of conflict with an existing application, these ports can be changed by editing the `RMI_PORT` or `WEB_PORT` entries in the `SIOS\LIFEKEEPER\JAVAGUI\SERVER` registry key.

Optional Recovery Kits

All optional SIOS Protection Suite Recovery Kits require a software license key in order to function with SIOS Protection Suite.

Kit Name	Versions/Requirements
Microsoft SQL Server Recovery Kit	See the SPS Support Matrix
Oracle Recovery Kit	See the SPS Support Matrix

GUI Requirements, Platforms and Browsers

LifeKeeper requires that the Java Runtime Environment (JRE) be installed on each server. The 32-bit Windows JRE 1.8.0_101 is installed with the SIOS Protection Suite Core software. JRE 1.8.0_101 has been fully tested with the LifeKeeper GUI Server and GUI Application components.

SIOS Protection Suite can be administered from a system outside the SIOS Protection Suite cluster by running the SIOS Protection Suite web client. Included in the following table is a list of the supported platforms and browsers for the SIOS Protection Suite web client. As in the case of the server, we have tested with JRE 1.8.0_101, but we expect that the client will work equally well with future JRE updates. Updating the client

JRE only affects that machine, so it is not as critical to test for safety as when you are updating the server JRE. We do recommend that you test updates before committing to them, and that you prepare to roll them back if a problem occurs.

Operating System	Internet Explorer 5.5+, 6.0	Internet Explorer 7.0, 8.0	Internet Explorer 9.0	Internet Explorer 10.0	Internet Explorer 11.0	Mozilla Firefox 1.5, 2	Mozilla Firefox 3
Windows 2012 R2				X	X		
Windows 2012				X	X		
Windows 2008 R2		X					
Windows 7		X					
Linux	N/A	N/A	N/A	N/A	N/A	X	X

Note: Other recent platforms and browsers will likely work with the SIOS Protection Suite web client, but they have not been tested by SIOS Technology Corp.

Installing and Removing SIOS Protection Suite for Windows

SIOS Protection Suite for Windows uses InstallShield to provide a standard installation interface with choices for **Typical**, **Compact** or **Custom** installation. See the SIOS Protection Suite Installation Guide for details about installing, removing or upgrading your SIOS Protection Suite software.

IMPORTANT

- Customizations made to SIOS Protection Suite scripts must be reapplied after upgrading to all releases of SIOS Protection Suite for Windows v8.
- Make sure you obtain the correct licenses; the old licenses will remain on the system and can be deleted with the license installer tool.
- SIOS does not support upgrading SIOS Protection Suite from more than one major version back. If upgrading from a version prior to LifeKeeper for Windows v7.x to SIOS Protection Suite for Windows v8, uninstall the old version of LifeKeeper and reinstall SIOS Protection Suite for Windows v8.

Technical Notes

lkstart

This program starts LifeKeeper on the current system if it is not currently running. `lkstart` modifies entries in the *`%LKROOT%\etc\LKinit.config`* file pertaining to the LifeKeeper daemons so that they will be respawned if they die.

The `-w` option, with `waitperiod` in seconds, can be used to change the timeout interval. Use the `-w` argument to specify a wait period before the startup.

The LifeKeeper service can also be started using the Microsoft Services MMC under Administrative Tools or from a command prompt using either "`sc start LifeKeeper`" or "`net start LifeKeeper`".

Note: This program must be run from the console.

Running `CHKDSK.EXE` on SIOS Protection Suite Protected Volume

Microsoft recommends running the utility `chkdsk.exe` to check and correct file system or disk errors on volumes that have not been cleanly shut down. However, depending on the extent of errors, the utility may take a very long time to complete. It may take several hours or even days for `chkdsk` to completely check the volume, or it may hang while checking the volume. Due to these reasons, SIOS Protection Suite does not run the `chkdsk` utility on protected volumes. SIOS Protection Suite does run the Microsoft utility `chkntfs.exe` to check whether a volume is dirty or not before bringing the volume in service. If a protected volume is found dirty, SIOS Protection Suite will log an error to the event log.

It is recommended that administrators periodically run **`chkdsk`** on SIOS Protection Suite protected volumes on the server where the volume resource(s) are in service. Administrators should take all the applications using the volume resource(s) out-of-service prior to running `chkdsk`.

Running `CHKDSK.EXE` During System BootSIOS

Protection Suite protected volumes are typically not eligible for the`chkdsk` utility to run on them at system boot time because LifeKeeper and DataKeeper need to be able to lock the volumes. If a SIOS Protection Suite protected volume needs to be checked at boot time, the steps below can be performed on the active node.

For Mirrored Volumes or SDRS Volumes (shared at one site, replicated to a remote site)

1. `"%ExtMirrBase%\emcmd" . getconfiguration <drv>` (save the number reported on the first line of output for later use after reboot)
2. `"%ExtMirrBase%\emcmd" . setconfiguration <drv> 32`
3. `"%LKBIN%\lkstop" -f`
4. `sc stop ExtMirrSvc`
5. `sc config lifekeeper start= demand`
6. `sc config ExtMirrSvc start= demand`
7. `chkntfs /D`
8. `chkntfs /c <drv>`
9. reboot

   Perform the following steps after reboot.
10. `sc config lifekeeper start= auto`
11. `sc config ExtMirrSvc start= auto`

12. `sc start ExtMirrSvc`
13. `"%ExtMirrBase%\emcmd" . setconfiguration <drv>` (number reported by `emcmd getconfiguration` in step 1).
14. reboot

For Shared Volumes

1. `"%LKBIN%\volume" -U <drv>`
2. `"%LKBIN%\lkstop" -f`
3. `chkntfs /c <drv>`
4. reboot

   Perform following steps after reboot.

5. `"%LKBIN%\volume" -p <drv>`
6. `"%LKBIN%\lkstop" -f`
7. `"%LKBIN%\lkstart"`

For Replicated Volumes

1. `"%LKBIN%\lkstop" -f`
2. `chkntfs /D`
3. `chkntfs /c <drv>`
4. reboot

Communication Paths Over Fibre Channel

When building a SIOS Protection Suite cluster using shared storage, it is important to maintain working communication paths between the nodes in the cluster. Communication paths should be created using TCP communication protocols. Normally, TCP communication paths are built on Ethernet network devices. SIOS Protection Suite, however, can use any type of connection on which the TCP protocol can run. If a shared storage cluster is being created using a Fibre Channel SAN, it is possible (and desirable) to use the Fibre Channel SAN as a SIOS Protection Suite communication path.

QLogic provides a miniport driver and an IP driver for Windows that will allow a QLogic Fibre Channel storage adapter to also run the TCP/IP protocol. This, in effect, allows the QLogic Fibre Channel adapter to function both as a storage adapter and as a network adapter. Once this driver is in place, the QLogic card can be configured, as any network card would, using standard network configuration techniques.

QLogic's driver can be downloaded from the following web site:

http://driverdownloads.qlogic.com/QLogicDriverDownloads_UI/DefaultNewSearch.aspx

Using iSCSI Storage with SIOS Protection Suite

iSCSI storage can be used as shared storage and protected by SIOS Protection Suite. For shared storage environments, the iSCSI target device must be configured so that all server initiators have access to the disk. The vendor of the iSCSI storage device provides the interface and commands needed to configure the iSCSI device. A dependency on the Microsoft iSCSI Initiator service (MSiSCSI) should be added to the LifeKeeper service. This will ensure that the shared volume is available before LifeKeeper attempts to access the volume.

To create a dependency on MSiSCSI for the LifeKeeper service, use the registry editor "*regedt32.exe*" and select the subkey representing the LifeKeeper service under *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LifeKeeper*. The service key has a value name "DependOnService" with one value "EISM". Double-click the value name "DependOnService" to open for editing. When the dialog box appears, add the service name "MSiSCSI" for Microsoft iSCSI Initiator service on a new line and click **OK**.

To verify that the dependency was created, open *Administrative Tools->Services* MMC snap-in. Go to LifeKeeper service and double-click to bring up the "**Properties**" dialog. When the dialog box appears, go to "**Dependencies**" page and verify that "**Microsoft iSCSI Initiator**" service is listed along with "**LifeKeeper External Interface**" in the "**depends on**" field.

System Load Considerations for Quickcheck and Deepcheck

SIOS Protection Suite launches a separate thread to monitor each protected resource in the system. These threads operate independently of one another. Typically, system load from Quickcheck and Deepcheck script execution will be randomly distributed. SIOS Protection Suite also works to distribute resource monitoring load by skipping a Quickcheck execution whenever a Deepcheck for the same resource is scheduled to run at the same time. However, because the check load is randomly distributed, there will occasionally be peaks in system load from resource monitoring. The more protected resources in the system, the larger these peaks will be and the more often they may occur. The largest peak will occur when LifeKeeper is started and Deepcheck scripts for each active resource are first launched. If the server can handle this first load peak in a satisfactory way, then there should not be a performance problem later.

VSS Shadow CopySIOS

Protection Suite support for VSS Shadow Copy requires that shadow copies must NOT be stored on the SIOS Protection Suite protected volumes. However, shadow copies may be saved on another non-protected volume.

Restrictions and Known Issues

Restrictions

SCVMM 2012

If using DataKeeper with SCVMM 2012, you must use SCVMM 2012 SP1.

Server with Microsoft Failover Cluster Installed

SIOS Protection Suite is not supported on Enterprise or DataCenter class servers with Microsoft Cluster Server or Microsoft Failover Cluster features installed. It should never be the case that two “Clustering” solutions are deployed on the same group of servers. As part of this restriction, SIOS Protection Suite communication paths will not function using IP addresses (169.254.xxx.xxx) that are hosted by the Microsoft Failover Cluster Virtual Adapters (Virtual NICs).

Exchange 2007 Circular Logging and Rewind

The SIOS Protection Suite Rewind feature is not supported if **Circular Logging** is enabled in Microsoft Exchange 2007 Server. This restriction is a result of the way Exchange overwrites its log files when circular logging is enabled, which interferes with SIOS Protection Suite's ability to calculate a consistent rewind point.

FAT File System Support

SIOS Protection Suite does not support protection for volumes using the FAT or FAT32 file systems.

Fault Tolerant Disk Sets

While SIOS Protection Suite replicated volumes are supported using Windows fault tolerant disk sets (Software RAID), SIOS Protection Suite shared volumes are not compatible with Windows fault tolerant disk sets. Fault tolerant disk sets must be set up with dynamic disks and dynamic disks cannot be shared between two systems.

File Share Recovery Kit

- The File Share Recovery Kit is supported only in an Active Domain environment, not in a Workgroup environment. File share permissions granted to local machine accounts, either in a workgroup environment or a domain environment, will not be preserved during failover because local User IDs are valid only on the local system where they originated; other systems will not recognize them. Even if two local User IDs are spelled the same way on two different machines, they will be treated as two different accounts and valid only on the system where they originated. Domain accounts, on the other hand, are identifiable and usable on any system in the domain.
- The File Share Recovery Kit will not work if more than 9999 file shares are defined on the system. Any attempt to protect eligible file shares under SIOS Protection Suite will fail if the total number of user-defined shares exceeds 9999. This restriction also applies to editing file share resources. You will not be able to alter the list of protected shares if more than 9999 shares are defined on the system.

LAN Manager Recovery Kit

Microsoft supports LAN Manager functions only over the first IP address per network interface card (Microsoft bug SRX#9704116-48). This prohibits using LAN Manager functions over SIOS Protection Suite protected IP addresses. Therefore, the only way to switch over an alias computer name using the TCP/IP protocol is to allow dynamic IP#-to-LAN Manager name mapping for your clients. The recommended solution is to use a WINS server. You will need to make the SIOS Protection Suite servers (and all computers accessing the protected LAN Manager name) WINS clients of the same WINS server.

Low Virtual Memory Degrades System State

SIOS Protection Suite depends on memory being available when it is needed. If your system is reporting that it is low on virtual memory, that need must be resolved immediately.

A virtual memory shortage serious enough to degrade or delay communications and other internal system functions will very likely cause SIOS Protection Suite to malfunction. For instance, `deepcheck` of TCP/IP communication resources may be impacted enough to cause a false failure, and thus a failover of the resource to the backup server.

If SIOS Protection Suite communication with other servers in the cluster is degraded, it could cause a manually initiated switchover to fail. However, this will not affect SIOS Protection Suite's ability to fail over protected resources when a server completely fails.

GUI interoperability

The LifeKeeper GUI may only be used to administer SIOS Protection Suite on Windows servers. Note that you can *connect to* and *monitor* a SIOS Protection Suite for Linux cluster. However, performing administrative tasks such as creating resources, editing properties, bringing servers in and out of service, is **not** supported at this time.

Discontinuing Serial Port Communication Paths

SIOS Protection Suite discontinued support for TTY communication paths in Version 7.2. Though SIOS does not recommend it, if currently using TTY communication paths, this option can be re-enabled by removing the (#) symbol on the `TTYCA.EXE` line in the */etc/lkinit.config* file as shown below:

```
# … /bin/TTYCA.EXE|-t  1  X  X  X  X  X  X    <=
 (TTY Comm Paths Disabled)
   … /bin/TTYCA.EXE|-t  1  X  X  X  X  X  X    <=
 (TTY Comm Paths Enabled)
```

To enable or disable the TTY communication path feature, the LifeKeeper service must be stopped and restarted after editing *lkinit.config*. To stop LifeKeeper, run command `{c:\lk}\bin\lkstop.exe -f` (c:\lk being the LifeKeeper installation path). Make sure the GUI is closed and all processes associated have stopped. Restart LifeKeeper by entering `{c:\lk}\bin\lkstart.exe`.

The TTY technology is obsolete. TTY communication paths are not supported and should be replaced with TCP/IP communication paths.

Console Application Management

Launching console applications from SIOS Protection Suite is not supported on Windows Server 2008 and later. Server architecture and security improvements in Server 2008 including UAC and memory management, prevent background processes such as SIOS Protection Suite from starting console applications.

Bitlocker Does Not Support DataKeeper

According to Microsoft, Bitlocker is not supported to work with Software RAID configurations. Since DataKeeper is essentially a software RAID 1, Microsoft does not support Bitlocker working with DataKeeper.

The specific article and section can be found here:

http://technet.microsoft.com/en-us/library/ee449438#BKMK_R2disks

Known Issues

For additional known issues, see the Troubleshooting section of SIOS Protection Suite for Windows Technical Documentation.

Frequently Asked Questions

Can I change my SIOS Protection Suite configuration database setting including resource values without reinstalling SIOS Protection Suite or rebuilding my resources?

Yes. Use the `lk_chg_value.ksh` command.

Can I upgrade my existing SIOS Protection Suite hierarchies from a previous version of SIOS Protection Suite for Windows to v8?

You may upgrade your existing SIOS Protection Suite for Windows software while preserving your resource hierarchies. Please refer to the Upgrading SIOS Protection Suite topic for the correct upgrade procedure. **Note**: SIOS does not support upgrading SIOS Protection Suite from more than one major version back. If upgrading from a version prior to LifeKeeper for Windows v7.x to SIOS Protection Suite for Windows v8, uninstall the old version of LifeKeeper and reinstall SIOS Protection Suite for Windows v8.

Does SIOS Protection Suite operate in a cluster with Microsoft Cluster Services (Windows 2003) or Windows Server Failover Cluster (Windows 2008 and later)?

No. SIOS Protection Suite v8.0.1 is an alternative clustering product and does not support either Microsoft Cluster Service or Windows Server Failover Clustering.

Does SIOS Protection Suite require that all servers in the cluster be identically configured?

No. As long as all servers are powerful enough to run any application that may run on them as the result of a failover operation and meet all other SIOS Protection Suite requirements, a cluster can be built. SIOS Protection Suite does not require identical hardware, but the software should be the same and configured with the same service pack levels.

Does SIOS Protection Suite for Windows support 64-bit environments?

Yes. SIOS Protection Suite for Windows supports only 64-bit platforms.

How do I change permissions on SIOS Protection Suite protected File Share resources?

The `EditFileShareResource` utility can be used to update a file share resource with all current file shares and permissions on the associated volume(s). This can be useful in environments where there are a large number of file shares, and file shares have been added or deleted since the resource was created or permissions have been modified. Using the utility can prevent the need to delete and re-create the file share resource. The `EditFileShareResource` utility is located under *`%LKROOT%\bin`* directory.

To invoke the utility, on the command line enter:

```
EditFileShareResource <Tag name>
```

where <Tag name> is the tag name of a file share resource that is currently in service.

The utility protects **all** eligible file shares defined on the volumes that are associated with the file share hierarchy. It deletes any previously protected shares that have been deleted from the system and adds newly defined shares (meeting the eligibility criteria) to the list. It will also update the file share permissions defined on the file share.

Documentation

A complete reference providing instructions for installing, configuring, administering and troubleshooting SIOS Protection Suite for Windows is available in the Protection Suite for Windows Technical Documentation. The following sections cover every aspect of SIOS Protection Suite for Windows:

Quick Start Guides

To get started using SIOS Protection Suite for Windows, refer to the SIOS Protection Suite for Windows Quick Start Guide and the DataKeeper Quick Start Guide.

Training

SIOS Protection Suite training is available through SIOS Technology Corp. or through your SIOS Protection Suite provider. Contact your sales representative for more information.

Technical Support

As a SIOS Technology Corp. customer with a valid Support contract, you are entitled to access the SIOS Technology Corp. Support Self-Service Portal.

The SIOS Technology Corp. Support Self-Service Portal offers you the following capabilities:

- Search our **Solution Knowledge Base** to find solutions to problems and answers to questions
- Always on 24/7 service with the SIOS Technology Corp. Support team to:
    - **Log a Case** to report new incidents.
    - **View Cases** to see all of your open and closed incidents.
    - **Review Top Solutions** providing information on the most popular problem resolutions being viewed by our customers.

Contact SIOS Technology Corp. Support at support@us.sios.com to set up and activate your Self-Service Portal account.

You can also contact SIOS Technology Corp. Support at:

1-877-457-5113 (Toll Free)

1-803-808-4270 (International)

Email: support@us.sios.com