
# SteelEye Protection Suite for Windows

# v7.6

## Installation Guide

**June 2013**

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

# SteelEye Protection Suite Installation Introduction

The topics in this Installation Guide will assist in defining your SteelEye Protection Suite cluster environment. Once your requirements have been determined and your SteelEye Protection Suite configuration has been mapped, these topics will assist you in setting up, licensing and installing SteelEye Protection Suite.

# Chapter 1: Planning Your SteelEye Protection Suite Environment

This section will assist you in defining your SteelEye Protection Suite cluster environment enabling you to successfully achieve your high availability goals quickly and effectively.

## Planning Server Communication

Determine and document server communication in a configuration map similar to the one below, using the following guidelines:

- Cluster requirements - To avoid a single point of failure, SteelEye Protection Suite requires at least two communication paths (also called “comm paths” or “heartbeats”) between servers in a cluster. See Communication Path Considerations below for more details.

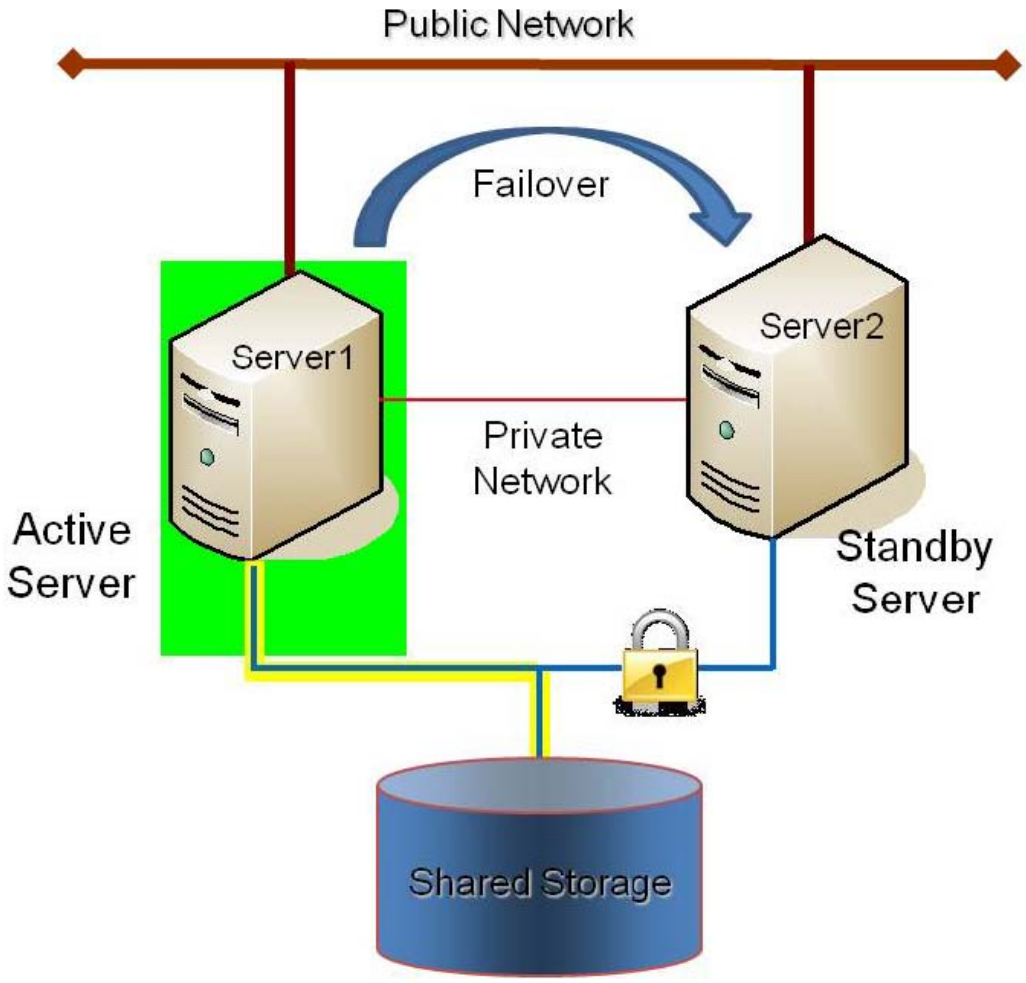



Figure 1 - Sample Configuration Map for SteelEye Protection Suite Pair

This is a very simple configuration map depicting a pair of SteelEye Protection Suite servers sharing a disk array subsystem. Under normal circumstances, Server 1 runs the application(s) and is considered the primary or active server. Server2 is the secondary or standby server. In this case, there is no contention for disk resources because only one server at a time reserves an entire volume of the disk array.

This sample cluster also shows TCP/IP communication paths configured on the public network and on the private network. On your configuration map, label the IP addresses associated with each TCP/IP comm path.

A pair of servers is the simplest SteelEye Protection Suite configuration. When planning a cluster consisting of more than two servers, a configuration map is even more critical to ensure that the appropriate connections exist between and among servers. Each server must have a physical communication path to every other server in the cluster in order to provide cascading failover capability.

**Note**: If using replicated storage rather than shared storage, refer to SteelEye DataKeeper for additional information on configuring hardware and software for replication.

## Communication Path Considerations

SteelEye Protection Suite comm paths are used to communicate the state of protected resources in a cluster and to manage failovers. Each comm path is assigned a priority number with the lowest number designated as the “highest”priority.

The recommended configuration is two separate LAN-based (TCP/IP) comm paths configured on independent subnets. The primary comm path should be configured on the private network. **A switchable IP address should not be configured on the Network Interface Card (NIC) carrying the primary comm path**.

### Redundant Comm Paths

SteelEye Protection Suite strongly recommends redundant comm paths whenever possible. If a single comm path is used and that comm path fails, then SteelEye Protection Suite hierarchies may come into service on multiple systems simultaneously. This is known as a false failover or a “split-brain” scenario. In the split-brain scenario, each server believes it is in control of the application and thus can access and write data to the shared storage device.

### Primary Comm Path (Private Network)

A private TCP/IP comm path provides reliable communication between systems that is not affected by any communication occurring on the public network. For this reason, it is recommended that the primary comm path be configured on a private network and the secondary comm path on the public network. Private network addresses must not be registered with DNS. The "**Register this connection's address with DNS**" checkbox must not be checked for private network addresses.

TCP/IP comm paths are configured in SteelEye Protection Suite using static IP addresses and subnet masks. The cabling may consist of either a crossover cable for a two-node cluster or a small hub for clusters of three or more nodes.

**Note**: It is very important that private network connections are not registered with DNS. DNS should normally publish only the public network connection for each server. This is essential when connecting a local LifeKeeper GUI admin client to a remote SteelEye Protection Suite system. Refer to Verifying Network Configuration for network configuration details.

# Recovery Kit Requirements

Each of the SteelEye Protection Suite Recovery Kits has requirements that you should consider in planning and connecting all the components of your SteelEye Protection Suite cluster. While the SteelEye Protection Suite for Windows Release Notes provides technical requirements for each kit such as program versions and disk space requirements, you will find detailed configuration information in the Recovery Kit section.

The Core recovery kits (Volume, IP, LAN Manager, File Share, DNS, Microsoft Internet Information Services (IIS) and Generic Application) are documented throughout the SteelEye Protection Suite for Windows Technical Documentation.

**Note**: All separately packaged (optional) SteelEye Protection Suite Recovery Kits require a software license key in order to function with LifeKeeper v4.3 and higher. You can install the license key by running the License Key utility from Start->All Programs->SteelEye->LifeKeeper->License Key Installer.

## Storage and Adapter Requirements

SteelEye Protection Suite configurations may use the facilities of shared SCSI host adapters and shared disk hardware to switch resources from a failed server to a designated backup server. A Fibre Channel Storage Area Network (SAN) may also be used to switch resources from a failed server to a designated backup server.

Determine your storage and host adapter requirements using the following guidelines:

**Storage Devices** - Based on your application's data storage requirements,you will need to determine the type and number of data storage devices required by your configuration. Your shared files should reside on a disk array subsystem (Redundant Array of Inexpensive Disks, or RAID). SteelEye Protection Suite supports a number of hardware RAID peripherals for use in SteelEye Protection Suite configurations. The primary requirement is that the device is supported by Microsoft. See the Microsoft Hardware Compatibility List.

**IMPORTANT**: Consider the following issues when planning the configuration of your storage devices:

- SteelEye Protection Suite manages resources at the volume level, making the resources on each volume available to only one server in the configuration at a time. As a result, it is a good idea to plan disk allocations before you begin to configure SteelEye Protection Suite.

**Adapters** - Based upon the type of configuration and the number of peripherals, determine the types and number of SCSI or Fibre Channel Host Adapters required. It is important that any adapter you choose be supported by Microsoft so that there is a driver available. See the "Cluster" categories in the Microsoft Hardware Compatibility List for Microsoft-supported adapters and peripherals.

For reference purposes, you should add the host adapter specifications to your configuration map.

## Verifying Server Specifications

Ensure that you have the correct version and/or capacity of the following components for each SteelEye Protection Suite server:

- Windows 2003 R1 and R2 Operating System (32- or 64-bit)

  **Note**: If you plan to use the LAN Manager Recovery Kit, be sure that the File and Printer Sharing for Microsoft Networks component is installed. This component is installed and enabled by default.

- Windows 2008 R1 and R2 Operating System (32- or 64-bit)

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

  **Note**: File and Printer Sharing is enabled for Lan Manager AND for use with DataKeeper replicated volumes. During the installation procedure, SteelEye Protection Suite can automatically configure the Windows 2008 firewall so that ports it needs are opened, and so that ICMP is enabled.

  **Note**: The Local Security Policy "**Network Access: Let Everyone permissions apply to anonymous users**" must be **Enabled** if you plan to use DataKeeper replicated volumes with SteelEye Protection Suite. This policy will be enabled by LifeKeeper installation.

**Note**: By default, firewall is enabled. During installation, if a firewall is detected, the appropriate rules will be added to windows firewall. However,if the firewall is disabled during installation and re-enabled at a future time, the setup firewall script needs to run to add the rules. This script is installed as *%LKROOT%\support\firewallSetup.bat*. To run the command from the command line, type `firewallSetup.bat %LKROOT%`

- Ethernet TCP/IP-supported network interface card(s) for LAN-based cluster heartbeat(s)
- Disk arrays and storage adapters (SCSI or Fibre Channel) if you are using shared storage.
- Memory. See the *SteelEye Protection Suite for Windows Release Notes* for minimum memory requirements for SteelEye Protection Suite.

  **Note**: Additional memory (beyond that required for SteelEye Protection Suite) is required to run user applications.
- Disk space. See the *SteelEye Protection Suite for Windows Release Notes* for minimum disk space requirements for SteelEye Protection Suite and recovery kits.
- LifeKeeper Graphical User Interface (GUI) platforms and browsers
- Power Requirements. To maximize the availability of your SteelEye Protection Suite servers, it is strongly recommended that you use Uninterruptible Power Supplies (UPSs), or at a minimum, separate the electrical sources to your servers.
- Application software to be protected by SteelEye Protection Suite.

Determine the server names, processor types, memory and other I/O devices for your configuration. When you specify a backup server, you should ensure that the server you select has the capacity to perform the processing should a failure occur on the primary server.

# Chapter 2: Setting Up Your SteelEye Protection Suite Environment

Now that you have determined your requirements and mapped your SteelEye Protection Suite configuration, you can start setting up the components of your SteelEye Protection Suite environment.

**Note**: Although it is possible to perform some setup tasks in a different sequence, this list provides the recommended sequence.

## Configuring Your Storage

SteelEye Protection Suite may be used with either shared storage or with replicated storage. Follow the instructions that apply to your configuration below.

### Shared Storage Configuration

If you are using shared storage, then after your Windows environment is installed, you should set the host adapter and shared peripheral addressing. Refer to the documentation accompanying your adapter and storage device for specific details. Perform the following tasks to configure your shared storage for access by all servers in the SteelEye Protection Suite cluster:

1. Because all disks placed under SteelEye Protection Suite protection must be partitioned, your shared disk arrays must now be configured into partitions (volumes) using the Windows Disk Management utility. You should also format the partitions with the NTFS file system.

   **Note**: To safely configure your shared storage, it is recommended that you follow the procedure in Safe Creation of Shared Disk Volume Instances.

   You should refer to your disk array software documentation for detailed instructions.

2. If you plan to use a Shared Disk comm path, designate a small raw (unformatted) partition to use for the comm path. One MB should be a sufficient size.

3. Power on the other server(s) in the cluster and verify that all servers recognize the shared disks. From the backup server(s), make drive assignments for the shared volumes exactly the same as the first server. It is recommended that you have the Disk Management utility open on only one server at a time.

4. If you have created file shares on the shared volumes, you will need to turn on the file sharing attribute of these folders on each server in the cluster.

### Replicated Volume Configuration

If you are using SteelEye DataKeeper for Windows, create your disk partitions (volumes) to be replicated using the Windows Disk Management utility. You should also format the partitions with the NTFS file system.

Be sure to assign the same drive letter to the source volume (on the primary server) and target volume (on the backup server).

## DNS Resource Requirements

The DNS Recovery Kit included with the SteelEye Protection Suite for Windows Core product provides a mechanism to update DNS A and PTR records of the primary server or an alias name on the DNS servers in your configuration. The DNS resource allows the user to select the A record of the primary server or an alias name in DNS which will be modified along with the PTR record (if exists) with the IP address of a backup server when failover or switchover occurs. Using a DNS resource allows clients to connect to the servers in a WAN environment when a failover or switchover occurs. When SteelEye Protection Suite servers are in different network subnets, it is not possible to use a switchable IP address. In this type configuration, a DNS resource should be used to provide client connectivity. For details on creating DNS resources, refer to Creating a DNS Resource Hierarchy in the SteelEye Protection Suite for Windows Technical Documentation.

**Restriction**: SteelEye Protection Suite servers should not be configured as Domain Controllers or DNS Servers. Creating a DNS resource that points to a DNS server on the same system will fail with the following error message: `"User credentials cannot be used for local connections."`

### TTL of DNS Records

When the SteelEye Protection Suite for Windows DNS Recovery Kit updates the A record of the primary server or alias name in DNS, the A record on the caching DNS servers' cache is not updated. These caching DNS servers are those who do not hold the zone that the SteelEye Protection Suite protected A record belongs to. The A record in the cache stays until the TTL is expired or the cache is cleared manually. Therefore, the clients of those caching DNS servers will not get the updated value of the A record in timely fashion. For SteelEye Protection Suite protected DNS resources, it is recommended that the TTL value of the A record of the primary server or alias name should be set to a lower value.

If SteelEye Protection Suite creates the A and PTR records for a DNS resource, the TTL of those records is set to 5 minutes. This value can be changed using the Microsoft DNS management console (dnsmgmt.msc). However, changing the value to a higher value will make the A record live in the cache longer on caching DNS servers.

For DNS A and PTR records created prior to creating the SteelEye Protection Suite DNS resource hierarchy, it is recommended that the TTL value be set to a lower value like 5 minutes.

## Installing and Setting Up Database Applications

If your environment includes a protected database application such as SQL Server, you should install the application using the documentation provided with the database. Ensure that the database is on a shared or replicated file system and that the configuration files are on a shared or replicated file system. The executables may either be on each local or a shared file system. Refer to SteelEye Protection Suite Microsoft SQL Server Recovery Kit Technical Documentation for additional installation and setup considerations

regarding SQL Server.

Although it is possible to install your application after SteelEye Protection Suite is installed, you should test the application to ensure it is configured and operating properly before placing it under SteelEye Protection Suite protection.

## Safe Creation of Shared Disk Volume Instances

In order to safely create a shared-storage volume resource, the user must ensure that only one system at a time has write access to the volume at any time. This includes the time prior to the creation of the SteelEye Protection Suite instance.

Since SteelEye Protection Suite cannot recognize that the volume is shared before an instance is created, manual steps must be taken to ensure that the volume is never writable on two or more systems at the same time.

To protect the volume from simultaneous write access, use the following procedure. In this example, two systems - SYSA and SYSB - are connected to shared storage. This storage is configured with two volumes which should be assigned drive letters E and F on both systems, then protected with SteelEye Protection Suite volume instances.

1. Power on SYSA, while leaving SYSB powered off.
2. Install LifeKeeper if it has not been installed.
3. Assign drive letters E and F to the volumes; format with NTFS if not formatted yet.
4. Power off SYSA.
5. Power on SYSB.
6. Install LifeKeeper if it has not been installed.
7. Assign drive letters E: and F: to the shared volumes.
8. In a command prompt, run the following commands:

```
%LKBIN%\volume -p E

%LKBIN%\volume -p F
```

9. Reboot SYSB. It will come up with the E: and F: drives locked.
10. Power on SYSA. It will come up with the E: and F: drives writable.
11. Create volume resources for E: and F: on SYSA and extend to SYSB.

An alternative to powering the systems off is to use Disk Management to take the shared physical disk offline.

## Verifying Network Configuration

It is important to ensure that your network is configured and working properly before you install SteelEye

Protection Suite. There are several tasks you should do at this point to verify your network operation:

1. You must ensure that every network interface card (NIC) has one permanent IP address in order to create a TCP/IP comm path or protect an IP address.
2. If your server has more than one NIC (recommended), you should configure them to be on different subnets. If the adapters are on the same subnet, TCP/IP cannot effectively utilize the second adapter.
3. Your IP addresses should be configured as follows, assuming at least two NICs in each server (one on a private network and one on the public network):
    a. In the **Control Panel**, click on **Network Connections**. Right-click **Open**.
    b. From the **Advanced** menu, select **Advanced Settings**.
    c. Ensure that the NIC connected to the public network is in the topmost position of the **Connections** list.
    d. Do not register private network connections with DNS. Uncheck the **"Register this connection's address with DNS**" checkbox for the private network adapter as follows:

        Internet Protocol (TCP/IP) Properties-> Advanced -> DNS Tab

        Since no DNS servers are needed for the private network connection, none should be listed.

        This prevents the browser from occasionally getting confused when switching over LAN Manager computer names.
4. From each server, ping the local server, and ping the other server(s) in the cluster. If the ping fails, then do the necessary troubleshooting and perform corrective actions before continuing.
5. To ensure that the LifeKeeper GUI server and client components can effectively communicate ensure that *localhost* is resolvable by each server in the cluster.
    - If DNS is not implemented, edit the ***%windir%\system32\etc\drivers\hosts*** file and add an entry for the localhost name. This entry can list either the IP address for the local server, or it can list the default entry (127.0.0.1). If *localhost* is not resolvable, the LifeKeeper GUI may not work.
    - If DNS is implemented, verify the configuration to ensure the servers in your SteelEye Protection Suite cluster can be resolved using DNS.
6. Ensure each server's hostname and networking addressing information is correct and will not change after SteelEye Protection Suite is installed. If changing the hostname after SteelEye Protection Suite is in operation, you must run the `lk_chg_value` utility to modify the computer name in the SteelEye Protection Suite configuration files. If changing the networking configuration after SteelEye Protection Suite is in operation, you must run the `lk_chg_value` utility to modify existing SteelEye Protection Suite comm paths and resource hierarchies after re-configuring your network information.

**Note**: If you are using SteelEye DataKeeper for Windows, refer to the SteelEye DataKeeper section of the documentation for additional information on specifying the network cards to be used for replication and comm path considerations.

## Switchable IP Address

Most SteelEye Protection Suite configurations use the IP Recovery Kit, which defines a switchable IP address. A switchable IP address is a “virtual” IP address that can be switched between servers. It is separate from the IP address associated with the network interface card of each server. Applications under SteelEye Protection Suite protection are associated with the switchable IP address. Then, if there is a failure on the primary server, the switchable IP address “switches” to the backup server.

If you plan to configure resource hierarchies for switchable IP addresses, you must do the following on each server in the cluster:

- Verify that the computer name is correct and will not be changed.
- Verify that the switchable IP addresses are unique using the **`ping`** command.
- If you wish to assign a hostname to the switchable IP address, you must edit the ***`%windir%/system32/etc/drivers/hosts`*** file on each server to add an entry for each switchable IP address and associated hostname.

**Note**: If using teaming software or if network cards are changed after creating a switchable IP resource, the switchable IP resource should be deleted and recreated as the associated index number for the card can change.

**Note**: By default, network broadcast pings are used to verify network presence before failing over an IP resource. If no broadcast pingable equipment is on your network or if you prefer not to test for network presence this way you may disable this test by setting the following registry value to 0 (disabled). Reinstalling SteelEye Protection Suite will restore the default value of 1(enabled).

```
HKEY_LOCAL_MACHINE\SOFTWARE\Steeleye\LifeKeeper\RK\IP\BroadcastPing
```

## Switchable IP Addresses, DNS and LifeKeeper GUI Considerations

Special network considerations must be made when a "virtual" IP address is used on the server's main NIC and DNS registration is enabled on the NIC. When a "virtual" IP address is created by SteelEye Protection Suite on a registered NIC, DNS will add this additional IP address for the server and start using it for host name resolution on the network. However, SteelEye Protection Suite protected "virtual" IP addresses are switchable across cluster nodes. Therefore, precautions must be taken to prevent the LifeKeeper GUI from also using DNS registered "virtual" IP addresses to get updates from local and remote cluster nodes.

To keep LifeKeeper GUI connections to local and remote systems stable when using "virtual" IP addresses, there are two options:

1. Use a network *hosts* file on each SteelEye Protection Suite node.
    - In the *hosts* file, identify the permanent IP address for every other remote cluster node.
    - Do this on every SteelEye Protection Suite system in the cluster.

    As explained above, these addresses must be on the highest priorty network used for LifeKeeper GUI binding.

2. Use an alternate network and associated alternate NIC for LifeKeeper GUI connections to all other nodes in the cluster. This option differs from the simpler recommendations explained above.
    - Enable DNS registration on the alternate network and NIC.
    - Make the alternate network the highest priority in the *Network Connections -> Advanced -> Advanced Settings* selection in the **Adapters and Bindings** tab. The LifeKeeper GUI will use this highest binding network.
    - The highest priority SteelEye Protection Suite comm path should also use this network.
    - Do this on every SteelEye Protection Suite system in the cluster.

    The LifeKeeper GUI will use this alternate network for connections to all cluster nodes. With no virtual IPs assigned to this alternate network, the address registration will be stable. DNS registration may also be used for the main/public NIC on the server as needed.

**Note**: After making network configuration changes, the "`ipconfig /flushdns`" command may be used to remove obsolete cached DNS information.

## IP Local Recovery Configuration

SteelEye Protection Suite provides the ability to monitor local switchable IP addresses and move them to another network adapter in the same system when a failure is detected. This functionality, called IP Local Recovery, imposes additional requirements and limitations on the system configuration.

The backup adapter, also known as the Local Recovery Adapter where the switchable address will become active after a failure of the primary adapter,must be configured as follows:

- Both adapters must be connected to the same physical subnet.
- For routing purposes, all addresses on the Local Recovery Adapter must be on a different logical subnet than any permanent addresses on the Primary adapter. They must also be on a different logical subnet than any SteelEye Protection Suite-protected switchable addresses that are configured on the Primary adapter.
- Cabling and network routing must be configured to permit a ping command issued from either logical subnet to reach the protected IP address and its associated subnet when it is placed on either the primary network card or the local recovery network card. This can be verified by manually issuing a ping command from other systems on each logical subnet. A failed ping command indicates a network routing problem.
- IP Local Recovery can only be enabled at the time the IP resource is created. Local Recovery cannot be added to an IP resource by modifying its resource attributes after the resource has been created.
- IP Local Recovery may be disabled for an IP resource by using the "`ins_setlocalrecovery`" command line utility. This utility is located in the SteelEye Protection Suite `\bin` directory (`C:\LK\bin` by default). From a command prompt, type "`ins_setlocalrecovery`" for the usage and switch options.

## How IP Local Recovery Works

When IP Local Recovery is enabled, and the IP resource fails its deepcheck (a periodic extensive check of the IP resource) then SteelEye Protection Suite will do the following:

- First, SteelEye Protection Suite will attempt to bring the IP address back in-service on the current network adapter.
- If that fails, SteelEye Protection Suite will check the resource instance to determine if there is a backup (Local Recovery Adapter) available. If so, it will then attempt to move the IP address to the backup interface.
- If all local recovery attempts fail, SteelEye Protection Suite will perform a failover of the IP address and all dependent resources to a backup server.

Even if you do not have a backup adapter, you can enable Local Recovery so that SteelEye Protection Suite will retry the primary network interface before initiating failover to a backup server.

# Chapter 3: Installing SteelEye Protection Suite

If you have completed planning and setting up your SteelEye Protection Suite environment, you should be ready to install the SteelEye Protection Suite software on each server in your cluster.

## SteelEye Protection Suite Core Software

The SteelEye Protection Suite Core software is available via ftp download. The SteelEye Protection Suite Core is comprised of:

- The basic LifeKeeper software, including:
    - Perl (CPAN v5.8.8)
    - Cygwin
    - International version of Java Runtime Environment (JRE) v1.5.0 Update 6
    - SUperior SU 2.0.0.6 and SUperior SU Patch 2.0.0.18
    - LifeKeeper GUI (both server and client)
    - Microsoft Visual C++ 2008 Redistributable package (v 8.0.56336
- Core recovery kits:
    - Volume
    - IP
    - DNS
    - LAN Manager
    - File Share
    - Generic Application
    - Internet Information Services (IIS)
- DataKeeper
    - DataKeeper Driver (ExtMirr.sys)
    - DataKeeper Service (ExtMirrSvc.exe)
    - Command Line Interface (EMCMD.exe)

- DataKeeper GUI (Datakeeper.msc)
- Packaging files, SteelEye Protection Suite scripts, help files, etc.

## Installing the SteelEye Protection Suite Core Software

SteelEye Protection Suite uses the Flexera InstallShield product to provide a standard installation interface. A license must be obtained and installed for each server in the cluster.

We recommend that you read the SteelEye Protection Suite for Windows Release Notes before installing and configuring SteelEye Protection Suite.

To install SteelEye Protection Suite software, run the setup program delivered with the SteelEye Protection Suite for Windows product. The InstallShield Wizard will first install LifeKeeper for Windows. Once the LifeKeeper installation is complete, SteelEye DataKeeper for Windows will be installed. Follow the setup instructions on each screen. Some explanatory notes are included below.

### LifeKeeper Installation Notes

- You must have administrative privileges to install the LifeKeeper software. While non-administrative users will not be prohibited from running the setup program, the installation will exit immediately due to lack of special permissions required during setup.
- Installing LifeKeeper on your shared storage is **not** supported. Each server should have its own copy installed on its local disk.
- The SUperior SU installation is called from the LifeKeeper installation program.
- The default LifeKeeper installation path is *C:\LK*. You may change this path, but due to some scripting issues, **be sure to choose a path with NO EMBEDDED SPACES and containing eight characters or less**. For instance, `C:\Program Files\LK` and `C:\LifeKeeper` are invalid choices that will result in application errors.
- Two Windows registry changes are made during the installation of LifeKeeper: `DisableStrictNameChecking` and `DisableLoopbackCheck`. Both of these changes are required to allow access to servers using an alias name.

#### Setup Type

Choose one of the following:

- **Typical** installs the LifeKeeper Core and all Core recovery kits (recommended). **Note**: DHCP Media Sense for TCP/IP will be disabled by default.
- **Compact** installs the LifeKeeper Core only (which includes the Volume Recovery Kit).
- **Custom** allows you to select from the list of LifeKeeper components to install: Core files (always required), IP Recovery Kit, DNS Recovery Kit, LAN Manager Recovery Kit, File Share Recovery Kit, Generic Application Recovery Kit and IIS Recovery Kit. The Custom option will ask the following questions:

- "Disable DHCP Media Sense for TCP/IP?"
- "Do you wish to start the LifeKeeper Services?" See Starting LifeKeeper Services below for details.

## Firewall Change Prompt (Windows 2008 Systems)

LifeKeeper cannot function properly if the firewall settings for the source and target machines are not configured correctly. During installation of LifeKeeper, you will be prompted to allow the installer to configure your firewall rules needed by LifeKeeper, as well as to configure other system settings that are required by LifeKeeper. If you choose to allow the installer to make these changes, you will not need to configure your firewall manually. Please refer to Troubleshooting in the SteelEye Protection Suite for Windows Technical Documentation for more information.

LifeKeeper requires the following ports / protocols / processes to be open or enabled:

**TCP Ports**: 81, 82, 1500, 3278, 3279

**Processes**: %LKROOT%\jre1.5\bin\java.exe

**Protocols**: ICMP Echo

## Starting LifeKeeper Services

If you choose the **Custom** installation option, you will be asked, "Do you wish to start the LifeKeeper Services?" In most cases you should answer **Yes** so that LifeKeeper will be started automatically when the system is booted. Answering **No** will cause LifeKeeper not to be started after installation, and it will set the **Startup Type** for the LifeKeeper services to **Manual**.

If you select **No** and you later wish to start the LifeKeeper services, you should do so using the **Services** tool in the **Windows Control Panel**. (You should start both LifeKeeper and LifeKeeper External Interfaces.) In addition, you can set the **Startup Type** to **Automatic** by right-clicking on each service and selecting **Properties**, then changing the **Startup Type** option to **Automatic**. This will tell LifeKeeper to always start at system boot time.

**Question**: In what situation would it make sense to answer **No** to starting the LifeKeeper services?

**Answer**: Choosing not to start the LifeKeeper services may be useful in a staging environment where you are not ready to configure your network addresses but you wish to install LifeKeeper and replicate it across a number of systems prior to final installation of the cluster.

**Explanation**: When LifeKeeper is started the FIRST time, the system's network configuration information is written into the **LifeKeeper Configuration Database** (LCD). Changing your network configuration AFTER LifeKeeper is started requires deleting and re-creating your comm paths and resource hierarchies. Therefore, by choosing NOT to start the LifeKeeper services at install time, you can install LifeKeeper and associated recovery kits, then configure your network later.

## SUperior SU installed with LifeKeeper Core

The LifeKeeper for Windows core product installs the SUperior SU 2.0.0.6 and Patch 2.0.0.18 software by Stephan Kuhr. The SUperior SU software provides a robust switch user utility currently available at no charge

from Stephan Kuhr on the Internet at http://www.stefan-kuhr.de/cms/index.php?option=com_content&view=article&id=62&Itemid=73. The SUperior SU service is disabled during the install of the software since the service is not currently needed by the LifeKeeper core or SteelEye Protection Suite Recovery Kits.

SteelEye Protection Suite Recovery Kit scripts are executed using the Windows "Local System" account, which has no standard ID or password associated with it and by default has no desktop privileges either. Some applications protected by SteelEye Protection Suite require queries and other operations to monitor and manage them. To perform these operations as needed without user intervention, some SteelEye Protection Suite Recovery Kits must assume the role of a valid user during the restore and monitoring processes. The SUperior SU software provides a programmatic "`Switch User`" or "`Run As User`" utility program that allows the recovery kit to perform these operations without user intervention. User accounts to be used for monitoring purposes by SteelEye Protection Suite must have login privileges that are valid on every system where the protected application may be placed in service.

**Note**: Superior SU can launch a desktop application on Server 2003 only.

**Note**: Removal of SteelEye Protection Suite software does NOT uninstall SUperior SU. SUperior SU can be removed separately. The SUperior SU patch should be removed prior to uninstalling the SUperior SU software. You can contact SIOS Technology Corp. support for assistance in uninstalling the Superior SU program on a Windows 2008 environment. However, you can use the **Add/Remove Programs** feature to remove SUperior SU in a Windows 2003 environment.

## DataKeeper Installation Notes

Once LifeKeeper installation is complete, the InstallShield Wizard will begin installing SteelEye DataKeeper for Windows. You will be prompted to select the DataKeeper features to install. A typical installation includes both features.

- DataKeeper Server Components
- DataKeeper User Interface

During installation of DataKeeper Server Components:

1. Configure firewall settings.
2. Select a DataKeeper Service log on account type.
    - If **Domain or Server account** is selected, provide DataKeeper Service log on ID and Password .
3. Install licensing via the **License Manager**.

Reboot your server and begin using DataKeeper. See the DataKeeper Technical Documentation for further information on using DataKeeper.

The **SteelEye DataKeeper User Interface and Server Components Feature** can be installed independently, and the installation can be modified later to include any feature that has not previously been installed.

**Important**: The SteelEye DataKeeper User Interface feature and the target snapshot feature require Microsoft MMC 3.0 and Microsoft .NET Framework 3.5 SP1 to be installed. You can download .NET Framework from

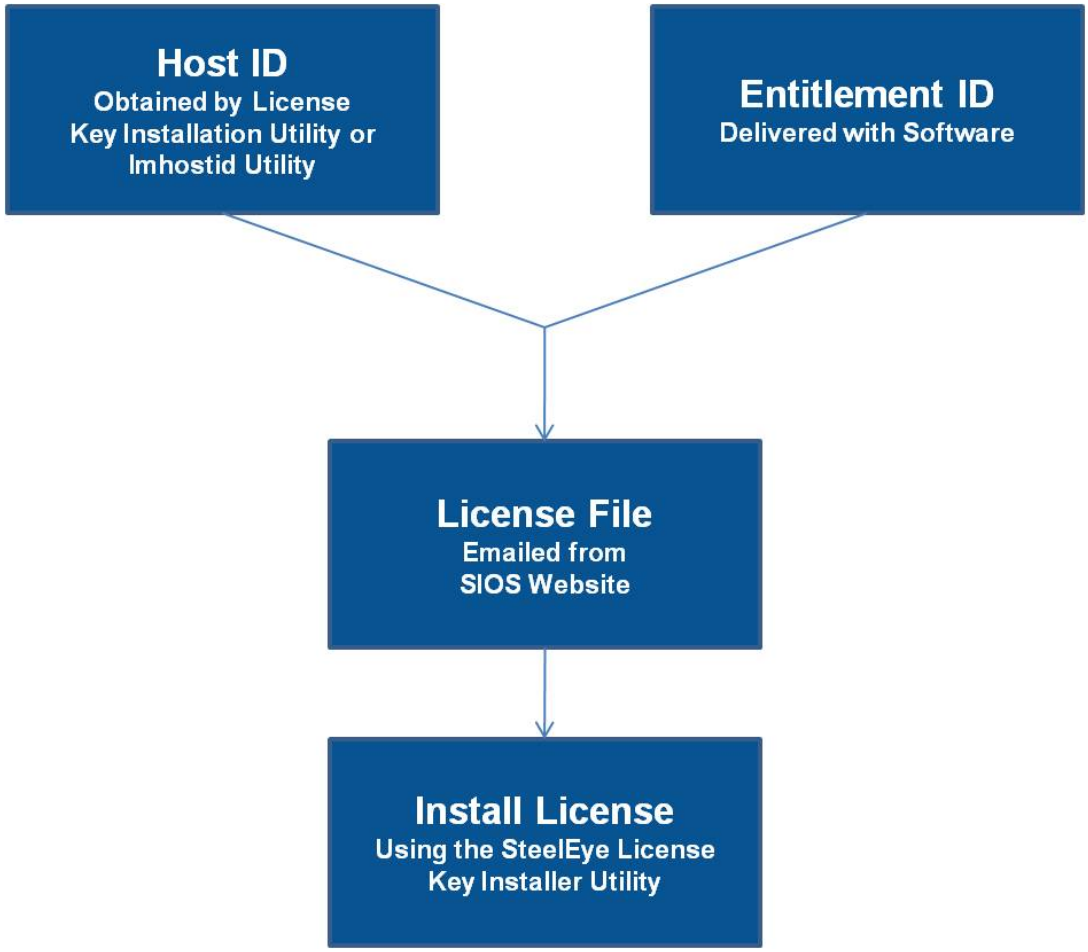
http://www.microsoft.com/net. If the SteelEye Protection Suite install is attempted prior to installing these proper versions, an error will be received and the installer will be stopped. SteelEye Protection Suite will need to be uninstalled and the SteelEye Protection Suite install process will need to be restarted.

**Note**: For Windows 2008 R2 and 2012, use "Server Manager" to enable the .NET Framework 3.5.1 features.

## Obtaining and Installing the License

SteelEye Protection Suite requires a unique license for each server. The license is a run-time license which means that you can *install* it without the license, but the license must be installed before you can successfully *start* and *run* SteelEye Protection Suite.

The final screen of the **InstallShield installation utility** displays the Host ID of your server. The **Host ID**, along with the **Entitlement ID** (Authorization Code) that was provided with your SteelEye Protection Suite software, is used to obtain the license required to run SteelEye Protection Suite. The process is illustrated below.



## License Key Manager

In addition to installing SteelEye Protection Suite product licenses, the **License Key Manager** allows you to perform the following functions:

- View all licenses currently installed on your system.
- View all expiration notifications (days remaining) for each time-expiring license.
- Identify invalid licenses that are currently installed.
- Delete any installed licenses (right-click on the license and select **Delete**).
- Delete all expired licenses as a group (press the **Delete Expired License** button).
- **Refresh** the Installed License list when installing software or upgrades.

Perform the following steps to obtain and install your licenses for each server in the SteelEye Protection Suite cluster:

1. Get your **Host ID**. At the end of the SteelEye Protection Suite installation, make note of the **Host ID** displayed by the **License Key Installer** utility as shown below. The Host ID may also be obtained by running **`%LKROOT%\bin\lmhostid`** (where *`%LKROOT%`* is the LifeKeeper installation path, by default `C:\LK`) or **`%ExtMirrBase%\bin\lmhostid`** (where *`%ExtMirrBase%`* is the DataKeeper installation path, by default *`C:\Program Files (x86)\SteelEye\DataKeeper`*) on the system (s) that you are obtaining licenses for. (If you need to obtain your Host ID again at a later time, you may do so by running the **License Key Installer** utility from the **Start-Programs** menu **Start-All Programs-SteelEye-LifeKeeper (or DataKeeper) -License Key Installer**.)
2. Write the **Host IDs** in a notebook or save them in a file. If saved in a file, copy that file to a system with internet access. Otherwise, take your notebook with you to the system with internet access.
3. Ensure you have your SteelEye Protection Suite **Entitlement ID** (Authorization Code). You should have received an email with your software containing the Entitlement ID needed to obtain the license.
4. Obtain your licenses from the SIOS Technology Corp. Licensing Operations Portal.
    a. Using the system that has internet access, navigate to the SIOS Technology Corp. Licensing Operations Portal and log in entering your **User Name** and **Password**.
    b. Select **Manage Entitlements**.

       **Note**: If changing password, use the **Profile** button in the upper right corner of the display.
    c. Find your **Entitlement ID** and select each **Activation ID** associated with that Entitlement ID by checking the box to the left of the line item.
    d. Select the **Activate** tab.
    e. Define the required fields and select **Next**.
    f. Click on **Select Existing Host** to choose an already defined host or create a new host by selecting **Add New Host**.
    g. Enter the **Host ID** and click **Okay**.

h. Check the box to the left of the **Host ID** and select **Generate**. The **Fulfillment ID** will display on the **License Summary** screen.

i. Check the box to the left of the **Fulfillment ID** and select the **Email License** tab.

j. Enter a valid email address to send the license to and select **Send**.

k. Select **Complete**.

l. Retrieve the email(s).

m. Copy the file(s) to the appropriate system(s).

5. Install your license(s). To install your license(s), choose one of the following options. **Note**: If you received your license after July 23, 2010, use **Option B**.

   a. Install via the **License Key Installer**.

      - On each system, run the **License Key Installer** from the **Start-Programs** menu (**Start-All Programs-SteelEye-LifeKeeper-License Key Installer**).
      - Press the **Install License File…** button on the main screen of the **License Key Installer**.
      - Browse to the location of the license file that you saved in **Step 4** above.
      - Click on the license file name. It will become highlighted.
      - Press the **Install License File…** button that appears in that dialog box below the file names. A license detection confirmation popup will be displayed.

      or

   b. Copy the license file(s) to the appropriate directory manually.

      On each system, copy the license file(s) to `%windir%\system32\LKLicense` on x86, or `%windir%\SysWOW64\LKLicense` on x64 (where `%windir%` is the Windows installation path, by default `C:\Windows`). If the `LKLicense` directory does not already exist, it will need to be created prior to copying the files. **Note**: It is recommended that this file(s) be renamed to `YYYYMMDD.lic` format to distinguish the day the license was activated.

6. Repeat on all additional servers. You must install a license on the other SteelEye Protection Suite server(s) using the unique Host ID for each server.

7. Reboot your system.

## Primary Network Interface Change May Require a License Rehost

The Host ID used by the License Key Installer utility is obtained from the SteelEye Protection Suite server's primary network interface card (NIC). SteelEye Protection Suite will check for a valid license each time it starts. If your SteelEye Protection Suite server should require a NIC replacement in the future that would cause the Host ID to change, then the next time LifeKeeper or DataKeeper is stopped, a License Rehost must be performed before starting either again. Log in to the SIOS Technology Corp. Licensing Operations Portal

and select **Support Actions/Rehost** from the **Manage Licenses** screen to perform this rehost. (**Note**: A rehost can be performed one time per six-month period without contacting support.)

## Subscription Licensing

A subscription license is a time-limited license with renewal capability. Similar to an evaluation license, it will expire after a set amount of time unless renewed. This renewal process can be set up to renew automatically by following the procedure below:

1. Install the subscription license program by entering:

   `%LKROOT%\bin\lmSubscribe.exe` or

   `%ExtMirrBase%\lmSubscribe.exe`

2. Enter **User ID** and **Password** (from **SIOS Technology Corp. Customer Registration**). These credentials are saved in an encrypted file.

3. Select **OK**.

If the previous steps run successfully, the subscription renewal service will now run, in the background, periodically checking renewal status. If licenses are found that will be expiring in a certain number of days (90, 60,30, 20, 10, 5, 4, 3, 2, 1), a warning notification will be sent to the **Windows Event Viewer** and an attempt will be made to renew the license. If a new license activation is available (a new activation has been purchased for this system's Entitlement), it will be automatically fulfilled and the new licenses will be installed on the system replacing the old licenses. As long as licenses for this system are renewed (Activations purchased), the service will ensure that the licenses are upgraded on the system without user intervention.

## Troubleshooting

If errors are encountered, please try the following before contacting Support:

- Review the error messages in the **Windows Event Viewer**.
- Verify credentials by logging in to the SIOS Technology Corp. Licensing Operations Portal. Enter **User ID** and **Password**. Run `%LKROOT%\bin\lmSubscribe.exe` or `%ExtMirrBase%\lmSubscribe.exe` again using the correct **User ID** and **Password**.
- To force a manual check for a license renewal, stop and restart the service. (**Note**: To find the service, bring up the view for all of the Windows services and search for "**SteelEye Subscription Licensing**".)
- If ownership of the license certificate has changed, please contact SIOS Technology Corp. Support personnel to have the certificate moved to the new owner. Once ownership has been moved, the automatic license renewal service will need to be updated with these new credentials by running the above command again using the new **User ID** and **Password**.

# Installing LifeKeeper for Windows Localized Language Supplement

LifeKeeper for Windows Localized Language Supplements are available to support LifeKeeper running in localized environments. Each Localized Language Supplement contains translated LifeKeeper GUI text strings and context-sensitive help in the localized language. For LifeKeeper v4.2, a Japanese Language Supplement was available. For LifeKeeper v7.2.1, language supplements are available for Chinese and

Japanese languages. The international version of Java Runtime Environment (JRE) is required to support running the LifeKeeper GUI in localized environments. The SteelEye Protection Suite for Windows Core installation program installs the required version of JRE.

For LifeKeeper v7.2.1, the Chinese Localized Language Supplement includes language content for the SteelEye Protection Suite including LifeKeeper and DataKeeper v7.2.1 products. The administrator can select which product to update. However, the Japanese Language Supplement will update only LifeKeeper v7.2.1. A standalone DataKeeper v7.2.1 product will be available in Japanese. Also, the DataKeeper mmc-based GUI requires the Windows language pack be installed unless the complete localized OS is already installed.

The LifeKeeper for Windows Localized Language Supplement, like the SteelEye Protection Suite Core, is installed via InstallShield. The installation requires no selection for Typical/Compact/Custom options. To install the LifeKeeper for Windows Localized Language Supplement, run the setup program shipped with the Localized Language Supplement product.

To repair an existing installation of LifeKeeper for Windows Localized Language Supplement, run the setup program and choose **Repair** from the list of InstallShield options.

To remove LifeKeeper for Windows Localized Language Supplement, run **Add/Remove Programs** from the **Windows Control Panel**. The Localized Language Supplement must be removed before removing the LifeKeeper core product.

## Silent Installation of SteelEye Protection Suite

You can install SteelEye Protection Suite for Windows silently through the use of the `-silent` command line option. This option suppresses both the wizard and launcher user interfaces (UIs) resulting in what is considered a "silent installation." This is how an installation is performed without any information displaying to or requiring any interaction with the end user. **Response files**, also known as "*options*" files, are used to pass command line options at installation. This is done as you would normally specify them on the command line to represent the responses to dialogs and/or to set the value of a property or variable. The options specified in the **response/options** file are executed after the execution of the options that were entered directly on the command line.

### LifeKeeper Response File

To create a response file for LifeKeeper, open a command window and run the LifeKeeper setup program using the command **`LK-{version}-Setup.exe -r /f1C:\setup.iss`**. The responses entered to the dialogs will be recorded into the file *`setup.iss`*.

To perform a silent install using the created response file, open a command window and run the **LifeKeeper setup program** using the command:

```
LK-{version}-Setup.exe -s /f1C:\setup.iss /f2C:\setup.log
```

### DataKeeper Response File

To create a response file for DataKeeper, open a command window and run the **SteelEye DataKeeper setup program** using the command:

```
DK-{version}-Setup.exe /r /f1C:\setup.iss
```

The responses entered to the dialogs will be recorded into the file *setup.iss*.

**Note**: When creating the initial *setup.iss* file, if a local user server account is used for the DataKeeper service, you must edit the *setup.iss* file for use on other servers. This change can be made by opening the *setup.iss* file in Notepad and changing the name of the server found within the szName field. (i.e.- szName=<serverName>\Administrator). When using the **Local Service account** or a **Domain account** that is the same across all installations, changing the *setup.iss* file is not required.

To perform a silent install using the created response file, open a command window and run the **SteelEye DataKeeper setup program** using the command:

```
DK-{version}-Setup.exe /s /f1C:\setup.iss /f2C:\setup.log.
```

Results from the silent install are stored in the file *setup.log*. "ResultCode=0" indicates a successful install.

When the SteelEye Protection Suite install is finished, run the **License Key Installer** utility from the **Start-Programs** menu to install the license key.

```
Start->All Programs->SteelEye->DataKeeper->License Key Installer.
```

Reboot the server.

## Third Party Product Files

The following third party files were not developed by SIOS Technology Corp. but are installed during the SteelEye Protection Suite/DataKeeper installation process.

| Path and File Name | Provider | Purpose |
|---|---|---|
| <datakeeper dir>/lmdiag.exe<br><datakeeper dir>/lmhostid.exe<br><datakeeper dir>/lminstall.exe<br><datakeeper dir>/motdk_libFNP.dll | Flexera | License Management |
| <datakeeper dir>/SnapIn/IronPython.dll (.Net python language implementation)<br><datakeeper dir>/SnapIn/IronPython.Modules.dll (.Net python modules) | codeplex.com<br>(Microsoft open source) | Testing/Debugging |
| <datakeeper dir>/SnapIn/J832.Common.dll<br><datakeeper dir>/SnapIn/J832.Wpf.BagOTricksLib.dll | Kevin Moore, http://j832.com/bagotricks/ | Utilities and controls for WPF development |
| <datakeeper dir>/SnapIn/log4net.dll (.Net logging library) | Apache Software Foundation | Application logging |

| Path and File Name | Provider | Purpose |
|---|---|---|
| <datakeeper dir>/SnapIn/Microsoft.Scripting.Core.dll<br><br><datakeeper dir>/SnapIn/Microsoft.Scripting.dll | codeplex.com<br><br>(part of IronPython) | |
| <datakeeper dir>/SnapIn/MMCFxCommon.dll<br><br><datakeeper dir>/SnapIn/microsoft.managementconsole.dll | Microsoft | MMC managed snap-in library |
| <datakeeper dir>/VSSHelper/VSSHelper.exe<br><br><datakeeper dir>/VSSHelper/AlphaVSS-license.txt<br><br><datakeeper dir>/VSSHelper/AlphaVSS.51.x86.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.52.x64.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.52.x86.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.60.x64.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.60.x86.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.60.x86.xml<br><br><datakeeper dir>/VSSHelper/AlphaVSS.Common.dll<br><br><datakeeper dir>/VSSHelper/AlphaVSS.Common.xml<br><br><datakeeper dir>/VSSHelper/log4net.dll<br><br><datakeeper dir>/VSSHelper/log4net.xml<br><br><datakeeper dir>/VSSHelper/cfg/log4net.Config.xml | Pete Palotas, http://alphavss.codeplex.com/ | Alpha VSS provider |

## Application Directory Anomaly

The following file is installed in a directory other than the default directory that you selected during the DataKeeper installation procedure. This exception occurs when the operating system installs performance monitor counters.

| Path and File Name | Purpose |
|---|---|
| *<windows dir>/in-f/ExtMirr/ExtMirrCounters.h*: | Performance monitoring. This file contains counter names and definitions |

# Uninstalling SteelEye Protection Suite for Windows

## Before Removing LifeKeeper

Included below are the requirements for removing LifeKeeper software.

1. **Move or stop applications.** Before removing the software, verify that applications requiring SteelEye Protection Suite protection are not on the server. Never remove LifeKeeper from a server where an application resource hierarchy is in service. Removing LifeKeeper removes all configuration data, such as equivalencies, resource hierarchy definitions and log files. See Transferring Resource Hierarchies for additional information.
2. **Ensure LifeKeeper is running.** Recovery Kits may require LifeKeeper to be running when you remove the recovery kit software. Use the **Services MMC** snap-in to ensure that LifeKeeper services are running. If it is not running, the removal process cannot remove the resource instances from other SteelEye Protection Suite servers in the cluster which would leave the servers in an inconsistent state.
3. **Remove resource hierarchies.** Unextend or delete any resource hierarchies from the server where LifeKeeper will be removed. Never remove a Recovery Kit from a server where the resource hierarchy is in service. This will corrupt current hierarchies and they will need to be recreated when reinstalling the Recovery Kit.
4. **Remove all packages.** If removing the LifeKeeper core, first remove other packages that depend upon LifeKeeper; for example, SteelEye Protection Suite Recovery Kits. It is recommended that before removing a SteelEye Protection Suite Recovery Kit, first remove the associated application resource hierarchy.

## Before Removing DataKeeper

If planning to uninstall DataKeeper and reinstall a previous version, all jobs/mirrors must be deleted on each node prior to uninstalling. These will need to be recreated once software is reinstalled.

## Uninstall SteelEye Protection Suite

- In **Windows Control Panel,** find your list of installed programs and select **SteelEye DataKeeper or LifeKeeper**.
- Select **Uninstall**.

Once the uninstall process is complete, rebooting the system is required.

**Note:** Uninstalling automatically stops the SteelEye DataKeeper and/or LifeKeeper services and clears the registry entries.

Once removed, the following files will not be removed by the uninstall procedure.

| Path and File Name | Definition and Special Considerations |
|---|---|
| *<windows dir>/System32/LKLicense*<br>or<br>*<windows dir>/SysWOW64)/LKLicense* | Common license file directory for SIOS Technology Corp. products. This is where license files are installed and licenses for multiple SIOS Technology Corp. products may be installed here at any given time. We don't remove this at uninstall so as to not disturb the installed licenses.<br>Safe to remove manually, but the license will need to be reinstalled if the software is reinstalled at a later time. |
| *<windows dir>/System32/PerfStringBackup.ini*<br>or<br>*<windows dir>/SysWOW64)/PerfStringBackup.ini* | A backup file created by Windows when new performance monitor counters are installed. This is created when we install the perfmon counters.<br>This should probably be left alone since it is a file created by Windows itself. |
| *<windows dir>/inf/ExtMirr/0011/ExtMirrCounters.ini* | This file describes the DataKeeper performance monitor counters. This file can be removed or left alone. It is not an executable. |

### Notes

- **Important**: Uninstallation of SteelEye Protection Suite software requires that the Microsoft Visual C++ 2008 Redistributable package be installed. Do not remove this package until SteelEye Protection Suite has been uninstalled.
- **Modify** or **Repair** must be run from the SteelEye Protection Suite setup program.
- Removal of LifeKeeper does NOT remove SUperior SU. SUperior SU can be removed separately using **Add/Remove Programs**.
- Removal of SteelEye Protection Suite may NOT delete the SteelEye Protection Suite directory. This directory can be deleted manually after the **Add/Remove** operation is complete.
- A reboot of the system is required to completely remove SteelEye Protection Suite remnants.

## Upgrading SteelEye Protection Suite

You may upgrade from previous versions of SteelEye Protection Suite for Windows while preserving your resource hierarchies and mirrors by using the procedure below.

## Upgrade Procedure

The following scenario illustrates the upgrade process when upgrading both LifeKeeper and SteelEye DataKeeper. The upgrade should be performed on LifeKeeper prior to upgrading SteelEye DataKeeper. The LifeKeeper Services and SteelEye DataKeeper Service will be stopped during the upgrade process. A system reboot is required after upgrading both LifeKeeper and SteelEye DataKeeper.

Given two systems (Sys1 and Sys2), with Sys1 being the primary (active) server, perform the following steps to upgrade LifeKeeper and SteelEye DataKeeper:

## Upgrading the Backup Server

1. Exit the LifeKeeper GUI and SteelEye DataKeeper GUI on backup server *Sys2*.
2. Open a command window and enter `$LKROOT\bin\lkstop` (where *$LKROOT* is the SteelEye Protection Suite installation path, by default *C:\LK*) to stop all the LifeKeeper services. Wait until you see "`LIFEKEEPER NOW STOPPED`" before continuing.
3. Upgrade LifeKeeper for Windows on the backup server *Sys2* by running the setup program. Click **Yes** to continue upgrading LifeKeeper.
4. The existing LifeKeeper files will be overwritten by the LifeKeeper installation. You should install your new LifeKeeper license (if necessary) using the **License Manager** utility – pre-7.0 LifeKeeper licenses will not work with LifeKeeper 7.0. Do not reboot the backup server until SteelEye Data Replication is upgraded to SteelEye DataKeeper.
5. Upgrade SteelEye DataKeeper for Windows on the backup server *Sys2* by running the setup program. Click **Yes** to continue upgrading SteelEye DataKeeper. You should install your new DataKeeper license (if necessary) using the **License Manager** utility – SteelEye Data Replication licenses will not work with SteelEye DataKeeper.
6. Reboot the backup server *Sys2*.
7. Upgrade the Language Supplement Package (if required) and any optional recovery kits at this time by running the appropriate installation program.

For additional backup servers in your cluster, follow these steps on each server.

**Note**: Newer versions of SteelEye Protection Suite contain links to the SIOS Technical Documentation in lieu of being included in the install package. When performing an upgrade from previous versions which contained the Online Product Manual within the product, the upgrade will not uninstall the old Online Product Manual files. If you would like for these files to be removed, you will need to manually uninstall the OLPM package.

## Upgrading the Primary Server

8. Once backup server has been rebooted, allow mirror(s) to resync and return to the **Mirroring** state.
9. Perform a switchover. This will bring the active resource hierarchies In Service on *Sys2* and will reverse the role of the mirror(s) allowing the primary server *Sys1* to be upgraded.
10. The above procedure will be repeated on the primary server *Sys1*. Exit the LifeKeeper GUI and

SteelEye DataKeeper GUI.

11. Open a command window and enter `$LKROOT\bin\lkstop` (where *`$LKROOT`* is the LifeKeeper installation path, by default *`C:\LK`*) to stop all the LifeKeeper services. Wait until you see "`LIFEKEEPER NOW STOPPED`" before continuing.
12. Upgrade LifeKeeper for Windows on the primary server *`Sys1`* by running the Setup program. Click **Yes** to continue upgrading LifeKeeper.
13. The existing LifeKeeper files will be overwritten by the LifeKeeper installation. You should install your new LifeKeeper license (if necessary) using the **License Manager** utility – pre-7.0 LifeKeeper licenses will not work with LifeKeeper 7.0. Do not reboot the server until SteelEye DataKeeper is upgraded.
14. Upgrade SteelEye DataKeeper for Windows on the primary server *Sys1* by running the Setup program. Click **Yes** to continue upgrading SteelEye DataKeeper. You should install your new DataKeeper license (if necessary) using the **License Manager** utility – SteelEye Data Replication licenses will not work with SteelEye DataKeeper.
15. Reboot the primary server *`Sys1`*.
16. Upgrade the Language Supplement Package (if required) and any optional recovery kits at this time by running the appropriate installation program.
17. Start the LifeKeeper GUI on *`Sys1`* by clicking **Start**, and then point to **Programs**, then **LifeKeeper**, then **LifeKeeper GUI** and log in to *`Sys1`*.

## Upgrading from SteelEye Data Replication v6.2x to DataKeeper

Because DataKeeper incorporated a new structure called a "job", upgrading from SteelEye Data Replication to DataKeeper requires that you delete your existing mirrors before upgrading to DataKeeper and then recreate them after the upgrade is complete. This insures that the job and mirror information gets set up properly for DataKeeper.

DataKeeper also requires updated licensing, so you will have to install your new DataKeeper licenses when the License Manager screen is presented. We also recommend removing your old SDR v6.2x licenses at this time.

The procedure is exactly the same as the upgrade procedure above, with two exceptions underlined below.

### Upgrade Procedure

1. In the SteelEye Data Replication UI, **delete all existing mirrors**.
2. Close the Steeleye DataKeeper Replication UI if it is currently running.
3. Perform the upgrade procedure listed above and **apply new licensing on each server when prompted**.
4. Bring up the DataKeeper UI and recreate your mirrors.

## Reinstalling SteelEye Protection Suite

To reinstall SteelEye Protection Suite, perform the same procedures as above, the only exception being that when Setup presents a list of InstallShield options, select **Repair**.

## Repair

The Install process also allows repairing the SteelEye Protection Suite software. Use this option if the software that was previously installed was accidentally deleted or if the user is performing a point release upgrade. This option copies all the files from the setup folder and prompts the user to reboot the system.

## Starting LifeKeeper

With a typical installation, LifeKeeper is started automatically when the server is booted. Your applications are brought up in a protected state.

When LifeKeeper starts, it also starts the LifeKeeper GUI Server. The LifeKeeper GUI client is launched from a web browser or from the ***Start->All Programs->SteelEye->LifeKeeper->LifeKeeper (Admin Only)***, and is described in detail in the LifeKeeper GUI section of SteelEye Protection Suite for Windows Technical Documentation.

### Starting and Stopping LifeKeeper Processes

Because LifeKeeper is started automatically when the server is booted, you should not normally need to start/stop LifeKeeper. In the rare event that you need to start or stop LifeKeeper manually, you can do so in one of two ways:

#### Services MMC Snap-In

You can stop and start LifeKeeper services using the **Services MMC** snap-in under **Administrative Tasks**.

LifeKeeper consists of two services:

- LifeKeeper
- LifeKeeper External Interfaces

Generally, these two services should be stopped and started together. However, since LifeKeeper External Interfaces is a dependency of the LifeKeeper service, stopping it will also stop the LifeKeeper service. Likewise, it must be started before the LifeKeeper service can be started.

#### Command Line

When stopping LifeKeeper, there are a number of related services that must be stopped. This process can take several seconds, although the Services tool does not reflect exactly when all the services are stopped. Using the command line to enter `$LKROOT\bin\lkstop` will show the services as they are being stopped, and when completed, the message "`LIFEKEEPER NOW STOPPED`" will display as confirmation.

**Caution**: Stopping LifeKeeper takes all protected hierarchies out of service. This means that any protected applications will not be accessible.

# Index