

WebKeeper™ 网站监测与自动恢复系统

**WebKeeper™ Web Site
Monitoring & Recovery System
Version 4.0**

产 品 说 明 书

北京启明星辰信息技术有限公司

2002 年 5 月

说 明

非常感谢您使用“Webkeeper”网站监测与自动恢复系统，我们将竭诚为您的网络安全提供全面服务。

本手册及其中所包含的内容的版权属北京启明星辰信息技术有限公司所有，未经许可，不得对此手册全部或部分内容复制、改编或做其他用途的使用。

“Webkeeper”网站监测与自动恢复系统是由北京启明星辰信息技术有限公司自主开发的专用信息安全产品，其版权受中华人民共和国版权法保护。

启明星辰公司尽最大的努力保证本册的准确性和完整性。如果您在使用中发现问题，希望你能及时将情况反馈给我们以完善产品，我们将非常感谢您的支持。

北京启明星辰信息技术有限公司
2002 年 5 月

目 录

第一章 关于 WEBKEEPER	5
1.1 系统概述	5
1.2 WEBKEEPER 的主要功能	5
1.3 WEBKEEPER4.0 版本的特色	6
1.4 WEBKEEPER 的管理架构	6
1.5 产品资质证书	7
第二章 WEBKEEPER4.0 安装与卸载	8
2.1 系统运行环境	8
2.1.1 硬件环境要求	8
2.1.2 软件环境要求	8
2.1.3 软件安装说明	8
2.2 监测端安装	8
2.3 控制台安装	14
2.4 IIS 配置	15
2.4.1 IIS5.0 的配置方法	15
2.4.2 IIS4.0 的配置方法	15
2.5 系统卸载	16
2.5.1 卸载注意事项	16
2.5.2 监测端卸载	16
2.5.3 Web 控制台卸载	18
第三章 系统操作指南	18
3.1 启动控制台	18
3.2 连接/断开主机	19
3.2.1 第一次连接主机	20
3.2.2 再次连接主机	20
3.3 启动/停止监测	21
3.4 系统设置	22
3.4.1 标准选项	22
3.4.2 自动恢复选项	23
3.4.3 日志维护	24

3.5 添加保护.....	25
3.6 编辑/删除保护.....	27
3.6.1 编辑保护.....	27
3.6.2 删除保护.....	28
3.7 网站正常更新的几种方式.....	29
3.7.1 网站更新.....	29
3.7.2 增量备份.....	30
3.7.3 校验备份.....	30
3.8 用户管理.....	31
3.9 静态恢复/校验备份.....	32
3.9.1 静态恢复.....	32
3.9.2 校验备份.....	32
3.10 备份库管理器.....	33
3.11 WEBKEEPER 服务管理器.....	35
第四章 技术名词解释.....	36
第五章 用户常见问题解答（FAQ）.....	37
5.1 产品正常使用流程.....	37
5.2 使用注意事项.....	38
5.3 常见问题解答.....	39
5.4 严重问题处理流程.....	41
第六章 产品技术支持与服务.....	42

第一章 关于 WebKeeper

1.1 系统概述

随着通讯和计算机技术的迅猛发展，计算机网络向世界的各个角落延伸，Internet 日益成为人们生活中不可缺少的部分。建设网站，通过 WEB 网页树立公众形象、开展业务，已经成为政府办公和企业发展的重要手段。然而人们在享受网络带来的便捷和机遇的同时，也越来越关注时有发生黑客入侵事件，如何确 Web 网站的安全是亟需解决的问题。

WebKeeper? WEB 站点监测与恢复系统是北京启明星辰信息技术有限公司针对国家政府机关、ICP、ISP、部分企事业单位的网站易受外部黑客和内部成员攻击的特性专门设计开发的具有自主知识产权的网络安全产品，它采用多种难以仿造的信息摘要算法，提供对 WEB 网站进行一天 24 小时，一周 7 天的不间断监测与恢复，有效保障网站数据的完整性和真实性。

WebKeeper? 系统管理员管理能够对不同操作者分配不同的权限，将某些系统管理员的某些不必要的权限过滤掉从内部保障了网站的安全；系统对于指定的内容设定了特定的合法修改权限；系统提供强大的日志管理功能，记录所有对网站指定部分的合法或非法修改，便于实时监控和事后审核、跟踪；系统由监测端和远程控制端两部分组成，可以只使用监测端，也可以在远程安装控制端，用户可以根据自己的实际情况灵活使用；提供完善的系统用户管理功能，确保只有合法的用户能够启动或中指本系统的运做，以进一步保障系统的安全。

WebKeeper 获得了公安部《计算机信息系统安全专用产品销售许可证》，系统强大的功能，简单的操作，友好的用户界面，全面的技术支持解除了您的后顾之忧，是值得信赖的信息安全产品。让 WebKeeper 成为您的网站的看护神，安全地维护着您的形象和利益！

1.2 WebKeeper 的主要功能

作为网站保护的产品，WebKeeper4.0 主要有以下几个功能：

★ **实时监测：**对远程敏感信息进行实时的操作监测与保护。

★ **自动阻断：**对网站的重要文件与文件系统进行实时的监测与保护，能有效的阻断来自网上的非法用户对文件所进行的非法操作。

★ **自动恢复：**能够通过实时监控和定期扫描对已被非法修改的文件进行自动恢复。

★ **实时报警：**具有实时告警信息显示，同时形成日志，为用户日后查阅提供依据。

★ **远程管理**：管理员可以从本地或也可以通过简单、方便的浏览器方式从远程进行管理、监测与运行网站的监测与保护系统。

★ **身份认证**：采用身份认证以及多种签名方式来保证操作的安全性。

★ **日志管理**：日志信息详细记录了所有对保护文件的非法操作，包括被修改文件名称、修改时间、恢复时间、恢复结果、监测模块等，供管理员审计。

1.3 WebKeeper4.0 版本的特色

WebKeeper 到目前为止，已开发了 1.0、2.0、3.0、3.2 等多个版本，在用户需求的强烈推动下，启明星辰公司最新推出 WebKeeper 网站监测和自动恢复系统的 4.0 版。WebKeeper 4.0 在总结了前几个版本的成功经验和对广大用户的进行了细致的需求调查以后，加入了更多的新功能，同时增加了许多更贴近用户的细节处理，主要特色如下：

- 全新的界面设计，更加方便用户的日常管理和维护操作。
- 支持中/英文 WindowsNT、Windows2000 系列和 WindowsXP 等多种平台。
- 系统运行采用开启服务的方式，实现了真正的无界面运行。
- 增加了多端控制功能。
- 提高了监测端自身和远端管理的安全性。
- 易于远程管理，采用 Web 管理方式，用户不需要安装任何专用程序，通过 IE 浏览器即可方便地进行远程管理。
- 提供全面的二次开发接口，满足了用户在自己的产品中对 WebKeeper 进行管理的需求。
- 对备份库进行了充分的保护。
- 对用户的正常的页面更新实时进行增量备份。
- 对核心功能进行全面的改进，运行效率高、稳定性可靠。

1.4 WebKeeper 的管理架构

WebKeeper 主要用来监测与保护服务器端的文件，分为监测端和控制台两部分，其工作方式如图：

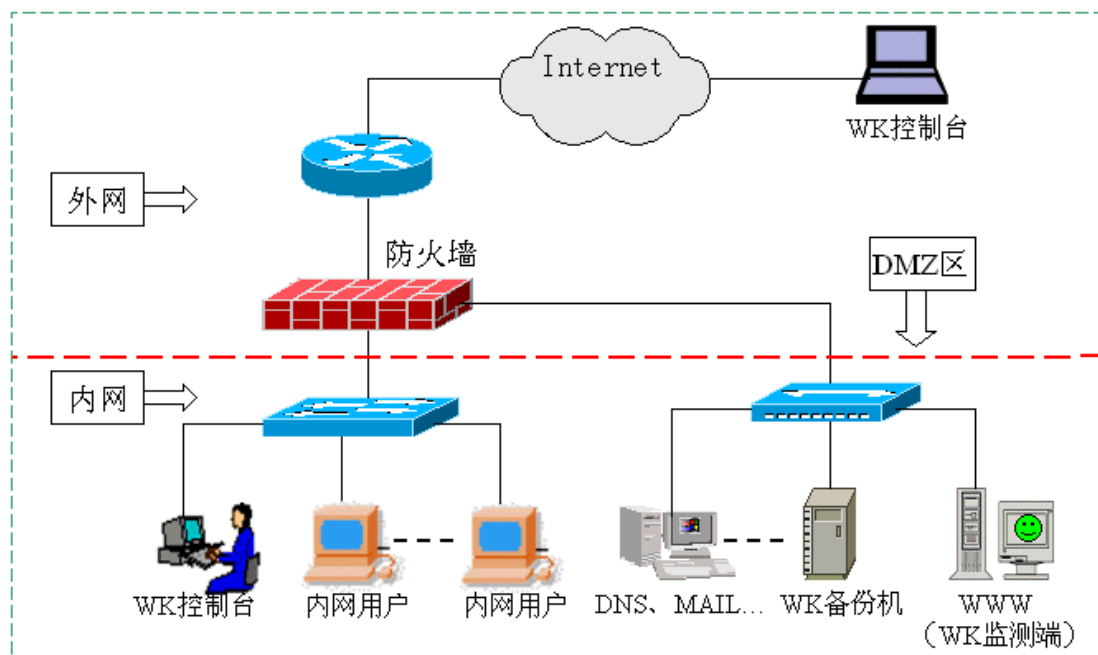


图 (1.41)

监测模块是系统的核心，运行于需要保护的 Web 服务器上，控制台是居于 Web 页面的远程操作控制界面，运行于企业内局域网（Intratnet）或国际互连网上的任意一台机器，控制台机器必须安装 IE4.0 以上版本浏览器，控制端是通过远程连接登陆到监测端来完成远程监测及控制任务的。

1.5 产品资质证书

WebKeeper 获得了公安部《计算机信息系统安全专用产品销售许可证》和国家信息安全测评认证中心的《产品型号证书》。系统具有强大的功能、简单的操作、友好的用户界面等特点，同时，全面的技术支持和本地化的售后服务解除了您的后顾之忧，是值得信赖的信息安全产品。让 WebKeeper 成为您的网站的忠实看护神，安全地维护着您的形象和利益！

第二章 WebKeeper4.0 安装与卸载

2.1 系统运行环境

2.1.1 硬件环境要求

1、监测端（Web 服务器）：Celeron 300 以上，至少 128M 内存的兼容机（建议 256M 以上）。

2、控制台：Celeron 300 以上，至少 64M 内存（建议 128M 以上）的兼容机。

2.1.2 软件环境要求

1、监测端（Web 服务器）：Windows2000 Server/Advanced Server/Professional WindowsNT4.0(SP4 以上补丁、建议 SP6) 或 WindowsXP, IIS4.0 以上版本。

2、控制台：运行 Windows98 以上操作系统，IE4.01 以上版本。

2.1.3 软件安装说明

WebKeeper4.0 网站监测与自动恢复系统分为监测端和控制端，两个部分都安装在需要监测保护的服务器上，通过 IIS 将控制端发布（IIS 的配置请参考“2.4 IIS 配置”部分内容），用户可以通过浏览器进行远程管理。

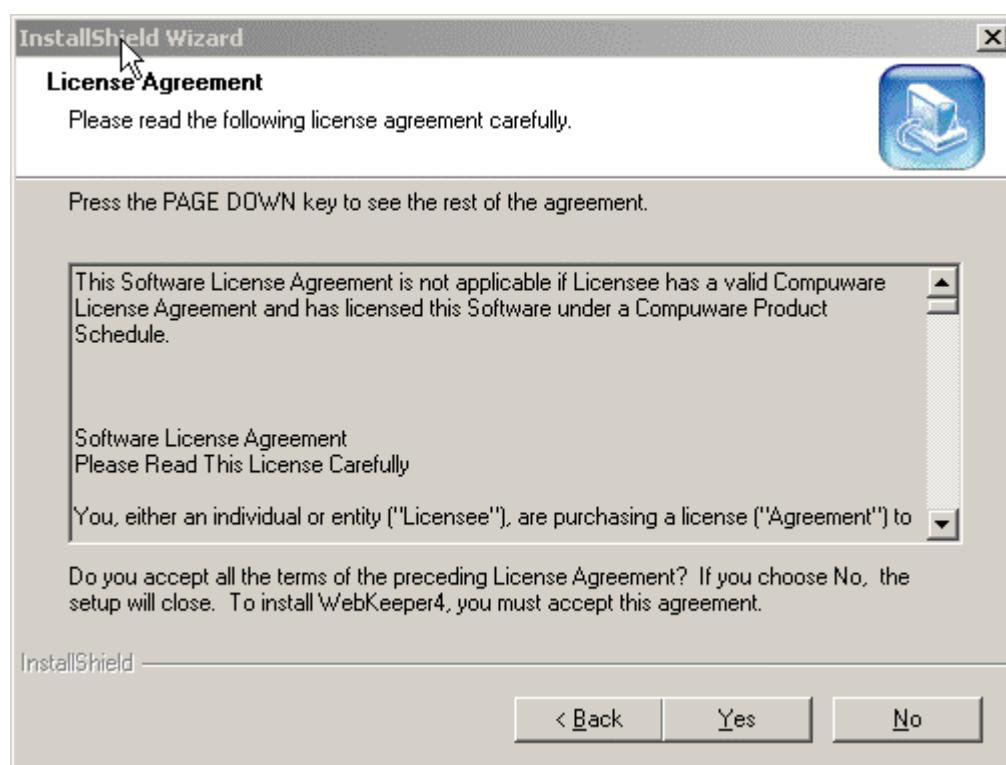
2.2 监测端安装

系统支持自动安装，将 WebKeeper 产品盘插入光驱，系统将自动启动安装程序，或者用户手动点击光盘上的 AutoSetup.exe 文件，启动安装界面入下图：



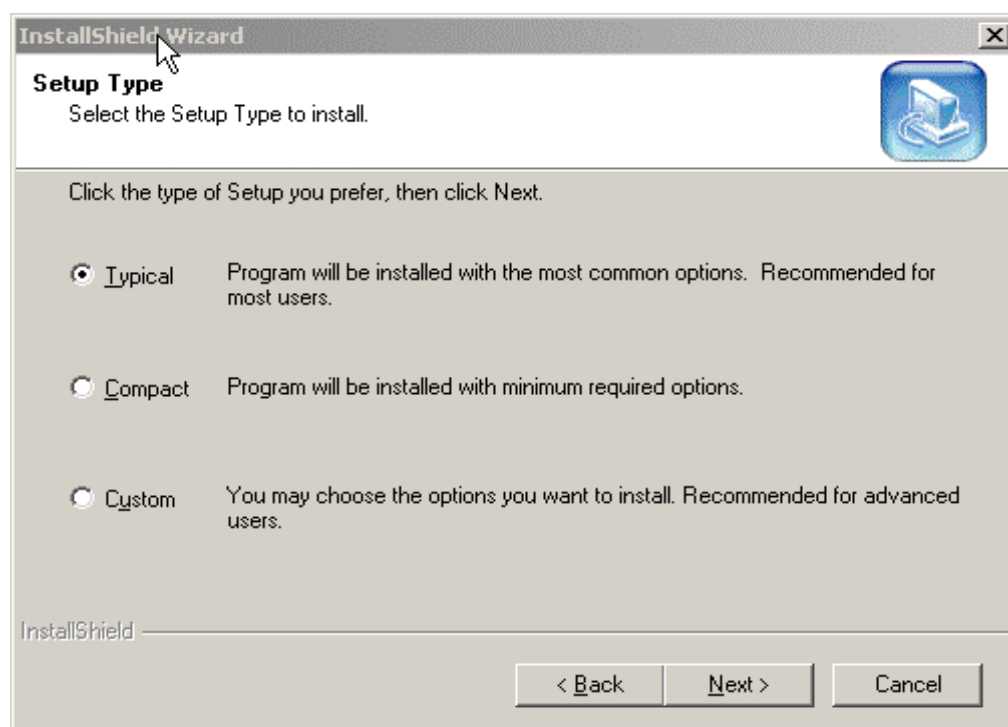
(图 2.21)

点击“WebKeeper”按钮开始安装监测端模块，下图是本产品的安装协议，包括本产品的适用范围、安装许可、用户权益、启明星辰公司责任范围和违约责任等方面的内容，用户同意本协议才能安装使用本产品。



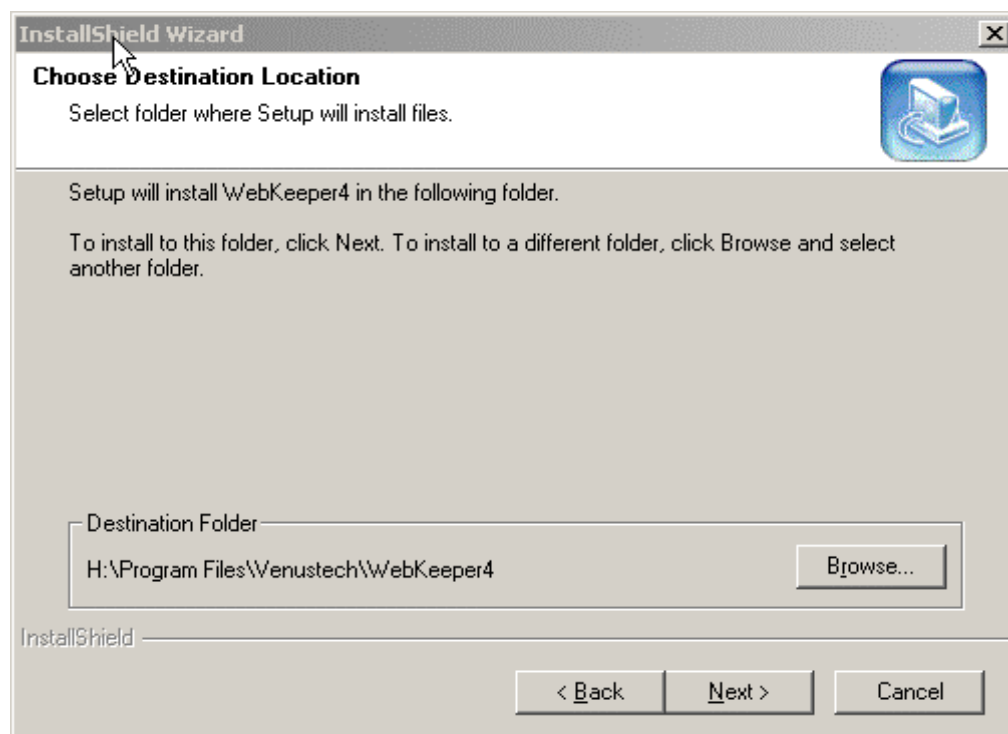
(图 2.22)

点击“YES”进入下一步安装，否则推出安装。

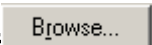


(图 2.23)

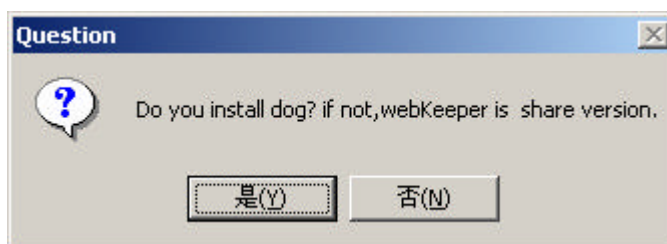
选择“Typical”进行典型安装：



(图 2.24)

图 2.24 提示用户选择系统的安装路径,用户可以通过点击  从本地硬盘上选择安装路径(需要用户手动建立安装路径然后才选),选择“下一步”安装程序将自动拷贝系统文件。

系统文件拷贝完毕后,会弹出以下对话框,提问用户是否安装加密狗:



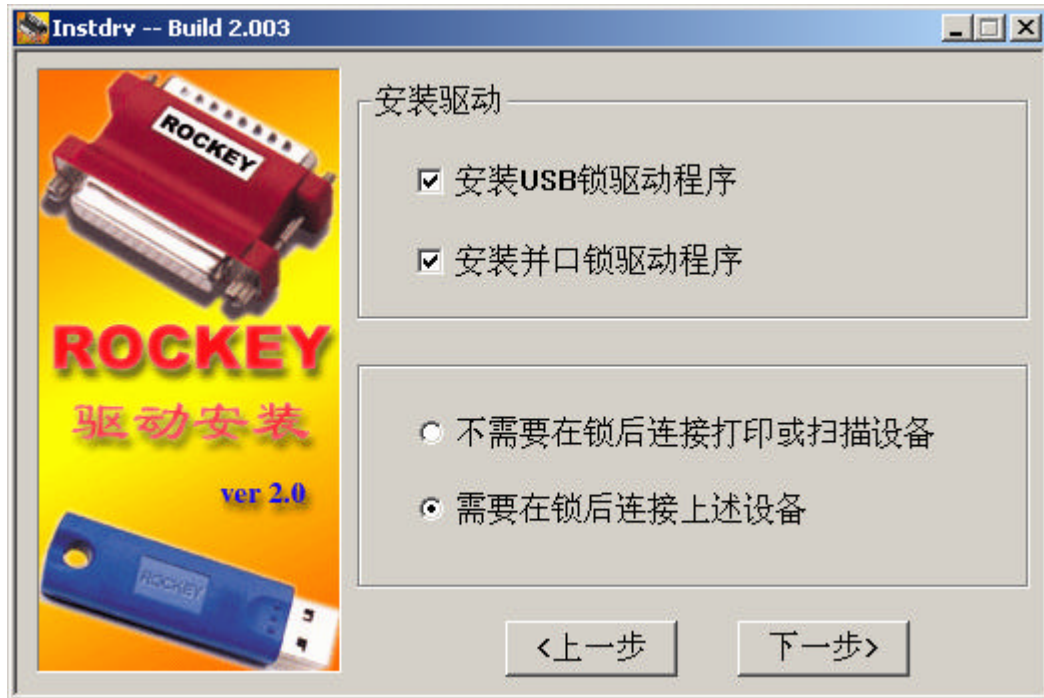
(图 2.25)

加密狗是 WebKeeper 系统的版权控制设备,每套产品必须配有一个加密狗,产品出货的时候随附,如果不安装加密狗的话 WebKeeper 将是一个限时版,这能正常试用一个月。选择“是(Y)”进入加密狗安装



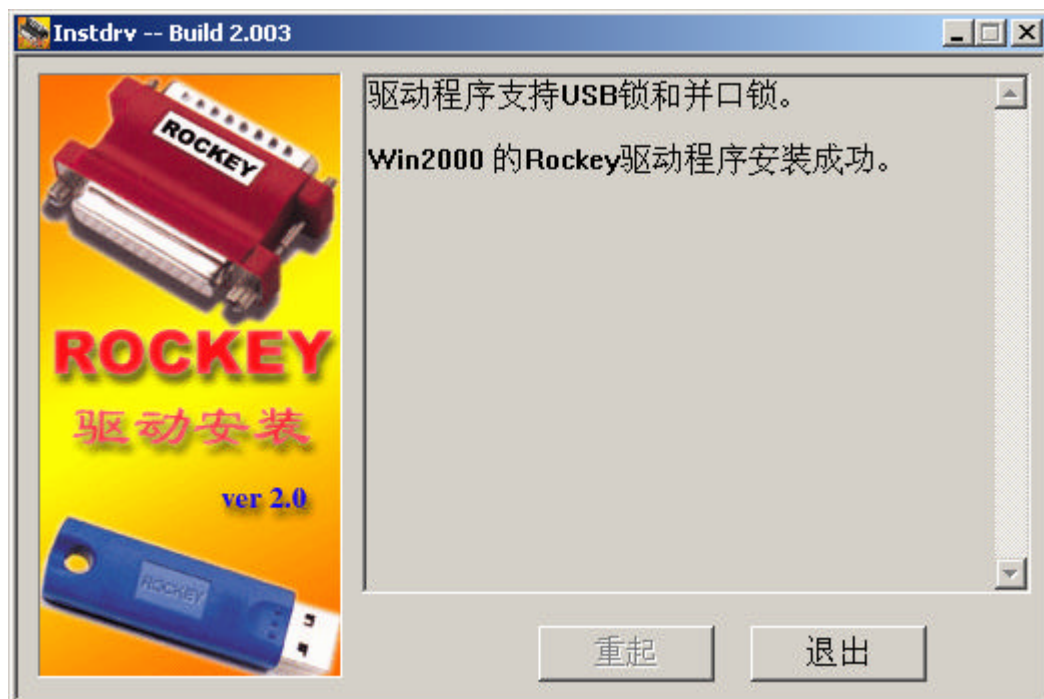
(图 2.26)

选择开始安装



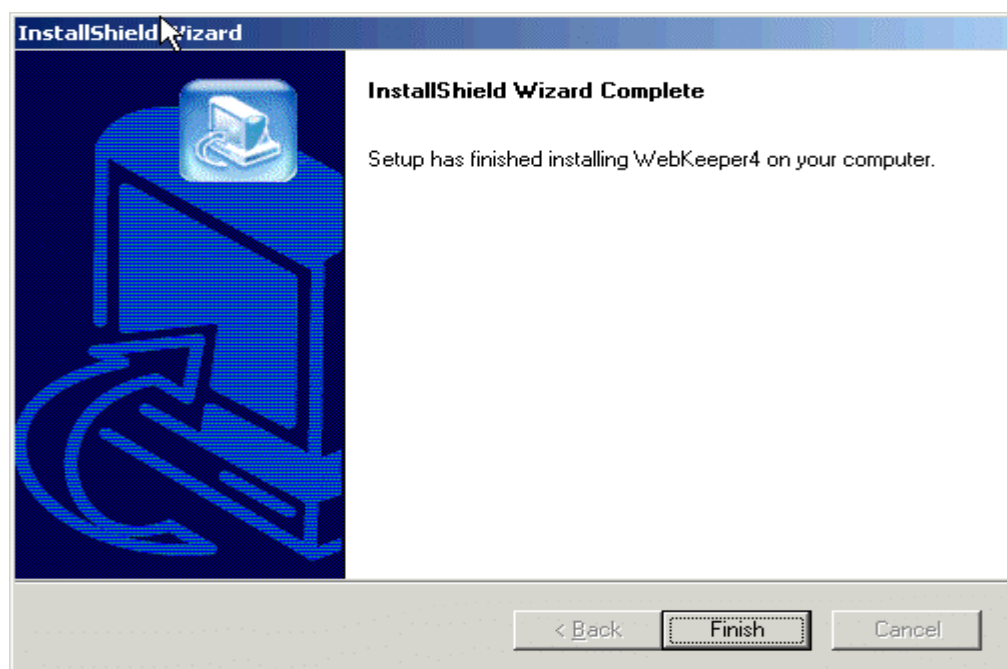
(图 2.27)

加密狗有两种，一种是支持 USB 接口的便携式，另外一种支持并口的加密狗，请根据产品配附的具体型号选择安装，或者完全采用默认安装即可，选择“下一步”



(图 2.28)

加密狗安装完成后点击“退出”



(图 2.29)

至此，点击“Finish”，监测端安装结束。

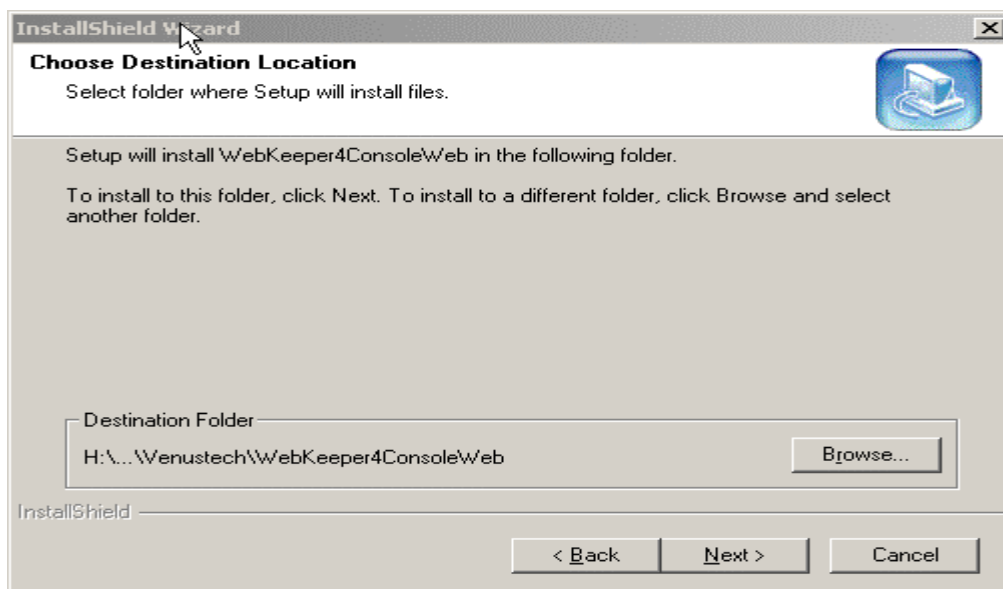
2.3 控制台安装

Web 控制台是 WebKeeper 系统通过浏览器方式提供给用的可视管理界面，用户必须安装此模块才能进行各种配置管理工作，点击下图中的“控制端”按钮即可安装，其安装细节跟监测端安装大致相同，用户可以参考“监测端安装”部分内容。



(图 2.31)

选择“控制端”并按照安装提示进行。



(图 2.32)

2.4 IIS 配置

系统安装完毕后，为了正常发布控制端同时又不影响 Web 站点的正常发布，需要对 IIS 进行配置。另外，为了保障控制端与监测端服务器之间的通存数据的安全，建议用户将监测端的 IIS 发布系统配置成 SSL 加密通讯方式。

2.4.1 IIS5.0 的配置方法

若用户使用的是 Windows2000 IIS5.0 的话，其配置如下：

- 1、打开 Internet 服务管理器（以 Windows 2000 server 为例）：[开始]—> [程序] —> [管理工具] —> [Internet 服务管理器]；
- 2、创建 WebKeeper 虚拟发布目录：[默认 Web 发布站点] —> [点击鼠标右键] —> [新增] —> [虚拟目录] —> [目录别名 (WebKeeper)] —> [路径 (指向控制端安装目录)] —> [完成]；
- 3、配置默认发布文档：[选中 WebKeeper 虚拟目录] —> [点击鼠标右键] —> [属性] —> [文档] —> [添加 Default.asp 为默认文档] —> [应用] —> [退出 Internet 服务管理器]。

2.4.2 IIS4.0 的配置方法

若用户使用的是 WindowsNT IIS4.0 的话，需要进行以下两步配置：

- 1、WebKeeper 的发布目录配置：

配置方法跟 IIS5.0 的配置方法大致相同，用户可以参考“2.4.1 IIS5.0 的配置方法”部分内容。

- 2、IIS4.0 管理控制台的配置：

- 1) 开始—> 运行—> 输入 cmd (回车) //进入 DOS 状态；
- 2) cd C:\WINNT\system32\inetmgr\adminsamples> <回车> //进入 IIS 管理员配置路径 (这里假设 C:\为 windows 的系统盘)；
- 3) adsutil set w3svc/AspAllowOutOfProcComponents True <回车> //具体配置；
- 4) net stop iisadmin /y <回车> //停止 IIS 服务；

5) net start w3svc <回车> //重新启动 www 服务。

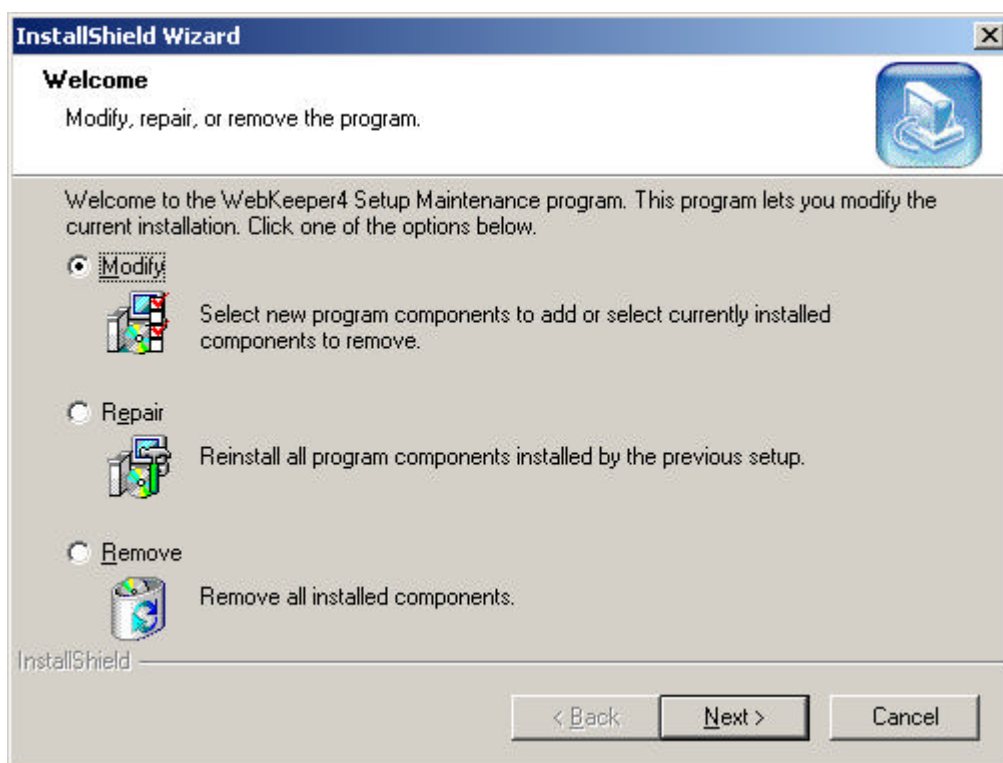
2.5 系统卸载

2.5.1 卸载注意事项

卸载前应该退出 Web 控制台，而且要确认 WebKeeper 监测服务处于停止状态，用户可以通过 WebKeeper 服务管理器或[开始]--> [程序]--> [管理工具]--> [服务]来查看 WebKeeper 服务状态。另外，通过[任务管理器]--> [进程]检查一下是否有 WebKeeper 进程在运行，若有的话请结束进程。

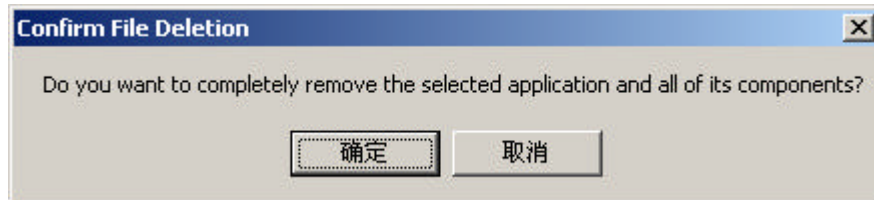
2.5.2 监测端卸载

[开始]--> [设置]--> [控制面板]--> [添加/删除程序]--> [WebKeeper4]-->[更改/删除]



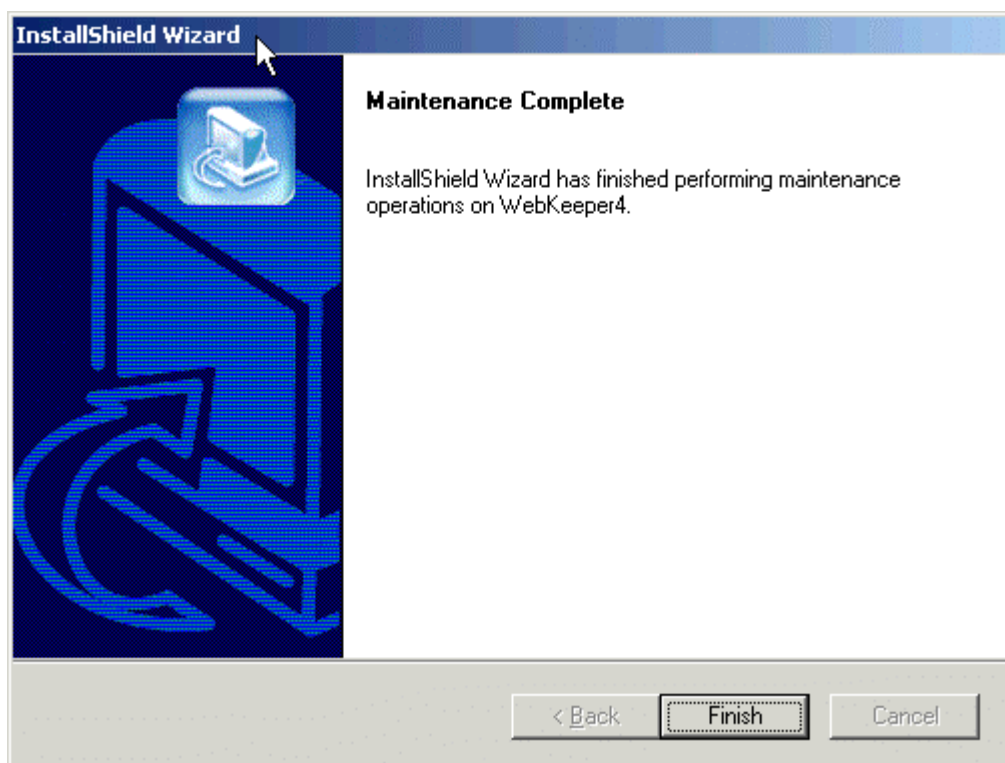
(图 2.41)

选择“Remove”，点击下一步，卸载程序会提问您是否真正删除，见下图：



(图 2.42)

点击确定，系统会自动删除 WebKeeper 组件。



(图 2.43)

至此，点击“Finish”，系统卸载完毕。

2.5.3 Web 控制台卸载

[开始]--> [设置]--> [控制面板]--> [添加/删除程序]-->

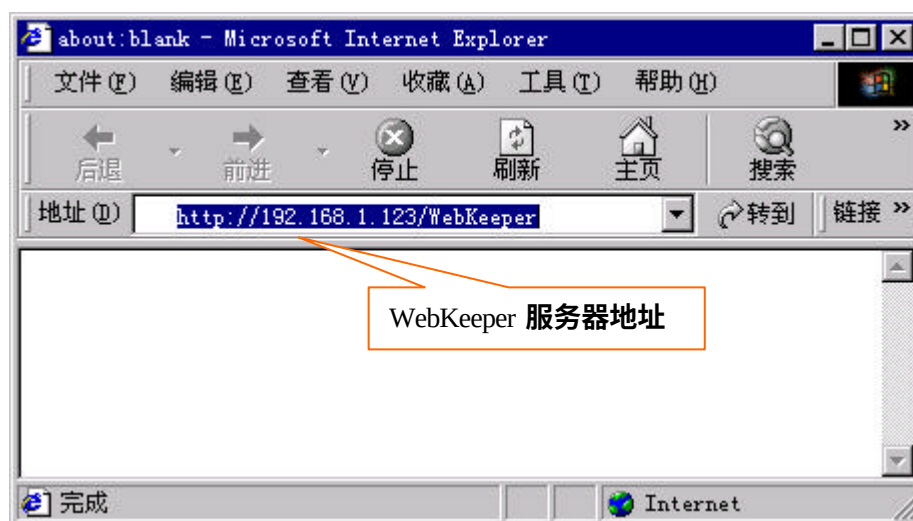
[WebKeeper4ConsoleWeb]-->[更改/删除]。Web 控制台的卸载细节跟监测端卸载一样。

第三章 系统操作指南

3.1 启动控制台

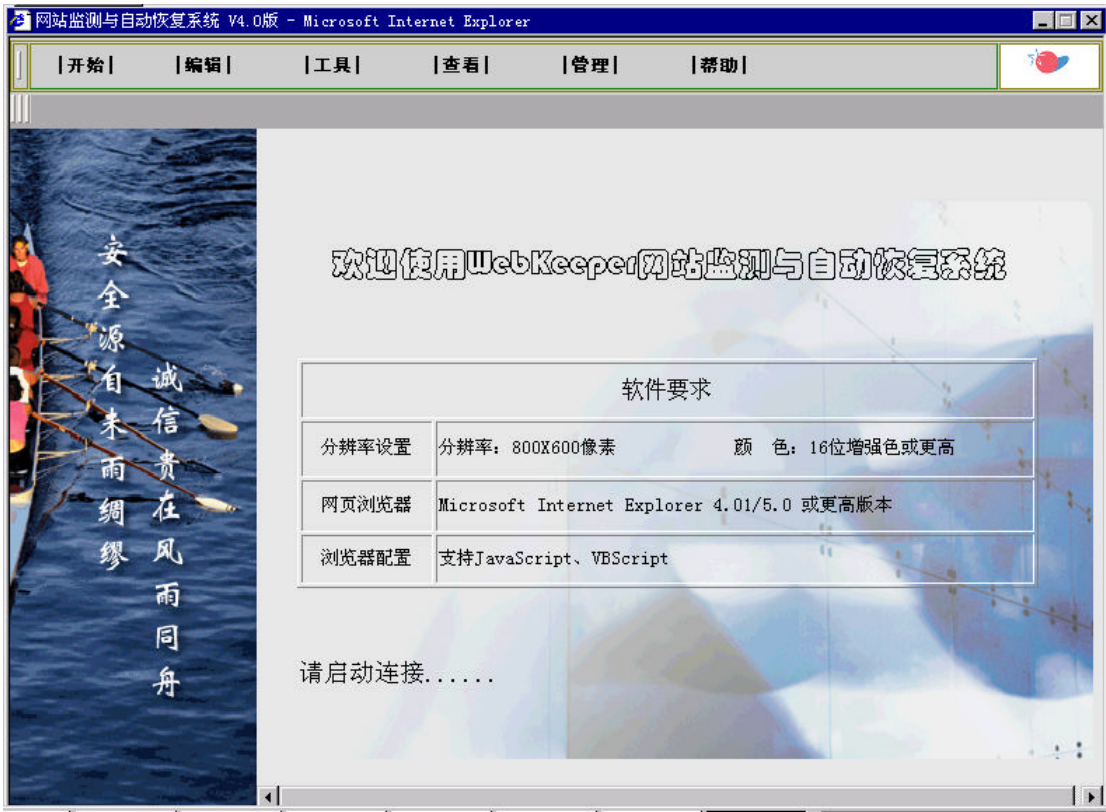
1、打开浏览器：开始菜单--> 程序--> Internet Explorer,或双击桌面上的快捷图标；

2、在浏览器的地址栏输入您安装 WebKeeper 控制端的发布地址(URL)，如下图：



(图 3.11)

3、浏览器自动通过局域网 (Intranet) 或互联网 (Internet) 登陆到 WebKeeper 的控制台，控制台的主界面如下图：

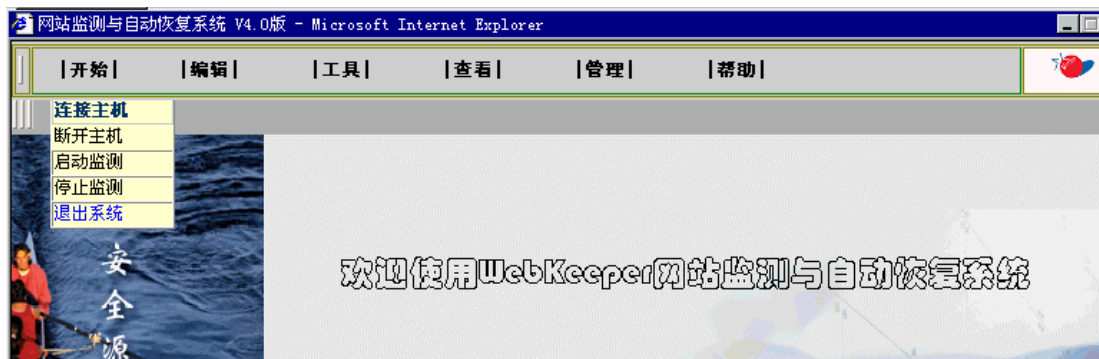


(图 3.12)

菜单的具体内容将在以后的操作指南中逐一介绍。

3.2 连接/断开主机

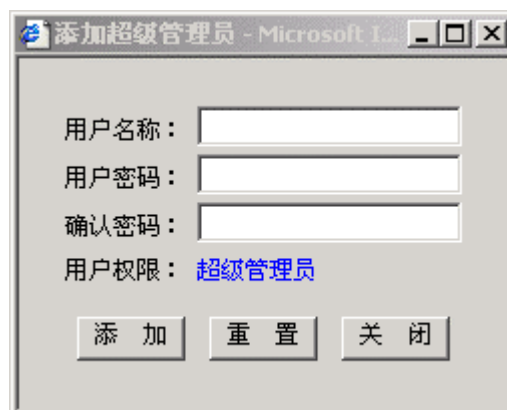
用户登陆到控制台后，需要连接主机才能进行添加保护、系统设置等操作，用户只要选择控制台主界面（图 3.21）中的开始-->连接主机，系统便弹出用户/口令验证对话框，如图 3.22 和图 3.23：



(图 3.21)

3.2.1 第一次连接主机

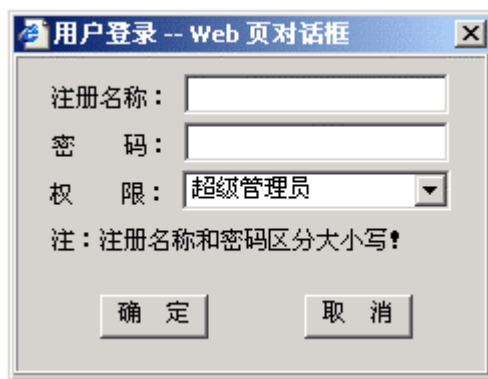
因为是第一次连接主机，系统没有任何账户信息，用户需要建立一个超级管理员账户，在下图对话框中键入超级管理员账户名称/密码/密码确认，这里输入的用户名称应该小于等于 40 字节、用户密码应该大于等于 8 字节而且小于等于 40 字节，正确填写后点击“添加”键便完成了创建管理员工作。**这是系统唯一的超级管理员账户，由于超级管理员是具有最高权限（可以进行所有的操作），所以用户应该牢记超级管理员账户和密码。**



(图 3.22)

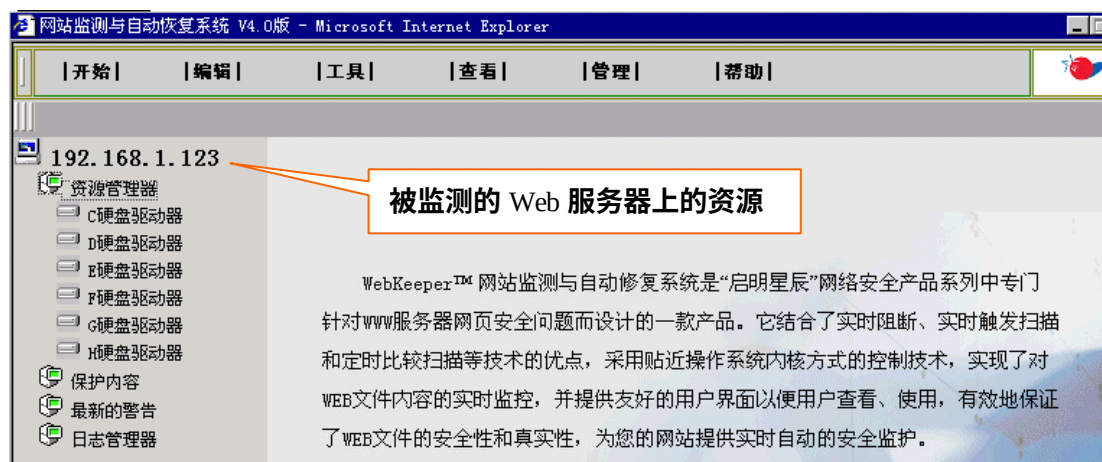
3.2.2 再次连接主机

再次连接主机时会直接进入以下登陆界面（见图 3.23），用户只需输入注册名称、密码、权限后点击确认便可连接。



(图 3.23)

连接主机成功后，控制台菜单将显示监测端主机的资源管理器和保护信息，如下图所示：



(图 3.24)

3.3 启动/停止监测

一、启动监测

用户进行系统设置、添加保护等操作结束后需要启动监测才能真正启动了 WebKeeper 系统的监测保护模块，选择控制台的开始菜单--> 启动监测，见(图 3.21)。

用户可以通过观察系统的“WebKeeper 服务”的状态来判断是否启动监测（以 Win2000 为例，开始--> 程序--> 管理工具--> 服务），启动监测前“WebKeeper 服务”处于停止状态，启动监测后“WebKeeper 服务”处于启动状态。

二、停止监测

选择控制台的开始菜单--> 停止监测，见(图 3.21)。

注意：如果不是要卸载 WebKeeper4.0 系统或整理网站的话，建议用户不要轻易使用停止监测功能，以免给不速之客（黑客）提供可乘之机。

3.4 系统设置

系统选项提供了包括标准选项、自动恢复配置、日志维护、报警方式设置等重要的系统维护内容。选择 WebKeeper 系统控制台主菜单上的[管理]--> [系统选项]即可进入系统选项的配置。

3.4.1 标准选项

标准选项界面见图 3.41，包括警告内容存盘周期、备份目录、被篡改的文件目录等三个设置项：



(图 3.41)

◆ **警告内容存盘周期**：是指系统将最新警告信息写入日志文件的时间间隔，以秒为单位。

◆ **备份目录**：是指系统备份库的存放路径，需要用户手动输入，注意要输入 WebKeeper 服务器（监测端）的路径，同时，要给备份目录分配足够的硬盘空间（建议 100M，用户可以根据保护文件的大小来确定），系统默认的备份目录为安装路径下的 LIB 目录。

◆ **被篡改的文件目录**：在保护文件被非法修改后，为保存修改现场而将被修改的文件另存起来的路径，注意要输入 WebKeeper 服务器（监测端）的路径，系统默认的被篡改的文件目录为安装路径下的 Tampered 目录。

3.4.2 自动恢复选项

自动恢复选项包括扫描间隔、扫描类型、扫描灵敏度等三个配置项。



(图 3.42)

◆ **扫描间隔**：WebKeeper4.0 系统应用了阻断、自动恢复等先进的保护技术，但也继承了定时扫描恢复这种传统的网站保护技术，形成了三道保护防线。扫描间隔就是设置了定时扫描的周期，在每个周期内，系统将自动扫描一遍保护文件，已发现是否被非法修改。

◆ **扫描类型**：扫描类型也是针对定时扫描来说的，用来设置扫描器的扫描内容，包括文件属性、文件属性和内容两个选项，为提高系统工作效率、控制服务器的资源占用，建议用户选择扫描文件属性。

◆ **扫描灵敏度**：是指 WebKeeper 对非法操作作出恢复响应的时间，它是以刻度的形式来表示的（一共有 10000 个分隔），最高和最低之间的时间间隔为 1 分钟，在设定的时间段内捉到的其他修改信息不进行恢复。灵敏度的设置要根据保护对象大小和服务器的性能而定，太高会造成报警信息过多而且很容易造成系统死循环，过低会影响系统效率而且容易漏处理非法操作，所以适当的灵敏度设置需要用户耐心的调试而定。

3.4.3 日志维护

日志维护内容包括日志文件最大容量、日志文件保存天数、日志目录和保存日志类型等四项配置内容，见（图 3.43）：



（图 3.43）

◆ **日志文件最大大小**：设置了日志文件的最大容量，如果日志文件超过了最大容量，则系统自动删除最早的日志信息。用户根据实际的日志量来定，但是由于目前日志是以文件形式存储的，日志文件太大的话会影响日志信息的存取速度，建议定义在 20M 以内。同时，为保持日志的完整性，用户应该定时另存日志文件。

◆ **日志文件保存天数**：定义了日志文件的最长保留天数，系统将自动删除最长天数以前的日志信息。用户应根据实际需要而定。

◆ **日志目录**：设置日志文件的存放目录，用户应根据日志文件最大大小设置来确定分配给日志目录足够的硬盘空间。

◆ **保存日志类型**：日志信息类型有：全部、不保存、所有合法操作、合法修改、合法删除、合法重命名、合法添加、所有非法操作、非法修改、非法删除、非法重命名、非法添加等 12 种，用户根据实际需要确定保存日志类型。

3.5 添加保护

为了达到 WebKeeper 系统对您网站的静态页面的保护目的，用户需要将您的 Web 服务器上的需要保护的文件/目录添加到保护列表里边，并选择一种保护方式（如阻断、自动恢复等），具体操作分以下两步来进行：

1、选中需要添加的目标文件/目录。点击资源管理器-->选择本地硬盘（该硬盘的详细文件列表会显示在控制台的右半窗口）-->选中需要添加的文件/目录（点击该文件/目录行）。选中的文件/目录所在行会变成绿颜色，如下图中选中的目录 test。

◆ **排除目录**：是指在所选保护目标（目录）内的某些用户不需要保护的内容，需要用户在这里指出来（这里要求输入文件的绝对路径），这些内容将不受 WebKeeper 系统的保护；若同时排除多个目录/文件的话，请用分号将其隔开。

3.6 编辑/删除保护

3.6.1 编辑保护

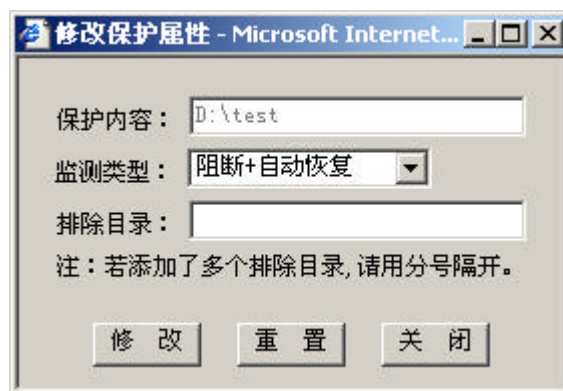
编辑保护是指修改某个保护对象的保护属性，包括保护类型、不受保护的文件/子目录、可以修改保护对象的程序等几个选项。编辑保护需要分两步来进行：

1、先选中需要编辑的保护对象。点击“保护内容”按钮，所有的保护对象都以下拉方式显示在“保护内容”按钮下方，此时点击您需要编辑的保护对象，其保护属性将详细显示在右窗口，而且被选中的保护对象会变成绿色。如图 3.61 中被选中的目录 test。



(图 3.61)

2、编辑保护。点击控制台的编辑菜单--> 编辑保护，系统会弹出修改保护对话框，见下图：



(图 3.62)

编辑完需要修改的信息后点击“修改”键便完成了编辑保护。

3.6.2 删除保护

删除保护也须分两步来进行，首先也是选择需要删除的保护对象，其操作跟编辑保护的第一步完全一样，接下来是删除保护：编辑-->删除保护，此时系统会弹出一个确认对话框，如下图：



(图 3.63)

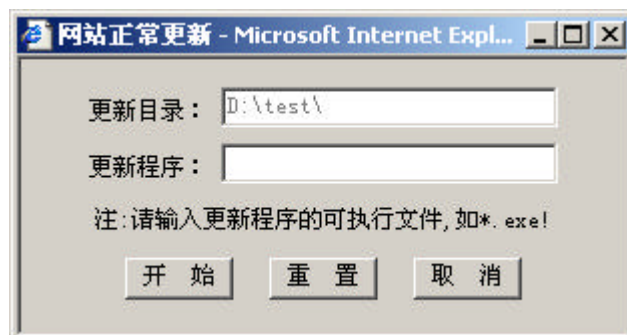
用户只要点击“确认”便可删除成功。

注意：一旦对保护对象进行了删除保护操作，该对象将不受 WebKeeper 系统的任何保护，所以敬请用户慎重使用“删除保护”功能。

3.7 网站正常更新的几种方式

3.7.1 网站更新

网站更新是系统管理员日常的维护工作，这是我们推荐的一种更新方式，当网站需要正常更新的时候，先选中需要更新的保护目录，在点击编辑菜单中的“网站更新”按钮（只有在启动监测的时候改按钮才被激活），系统弹出以下对话框：



(图 3.71)

更新目录就是您需要更新的内容，更新程序是您指定的更新文件的工具，在这里需要输入的是一个可执行文件，如：使用资源管理器来更新的话，则在这里输入 Explorer.exe，若想采用 Word 直接修改某个文件内容的话，则需要键入 Winword.exe，以此类推，WebKeeper 系统将该工具对保护文件的操作认为合法修改，而不给予阻断或恢复，其他的程序对保护文件的修改则作为非法操作一概阻断或恢复。指定更新工具后点击“开始更新”，WebKeeper 系统进入更新状态，用户可以开始对网站进行更新了，同时，，WebKeeper 系统会将您所做的改动以增量方式相应的更新备份库。

注：用户必须在这里键入一个工具，否则将视为没有特权工具，不予更新网站。



(图 3.72)

更新完毕后，一定要及时的点击“结束更新”。

3.7.2 增量备份

当网站需要正常更新的时候，先选中需要更新的保护目录，在点击编辑菜单中的“编辑保护”按钮，将该保护目录的保护方式修改为“增量备份”，然后即可对网站进行更新，更新完毕后再将其保护方式恢复回来原来的方式。注意更新后要比一下备份库，看备份库的内容是否跟源文件一致，若不一致的话则需要校验备份（校验备份操作请参阅 3.9 部分内容）。

3.7.3 校验备份

当网站需要正常更新的时候，先停止监测，再对保护目录/文件进行更新，然后校验备份（校验备份操作请参阅 3.9 部分内容），检查备份库内容与源文件内容以之后启动保护。

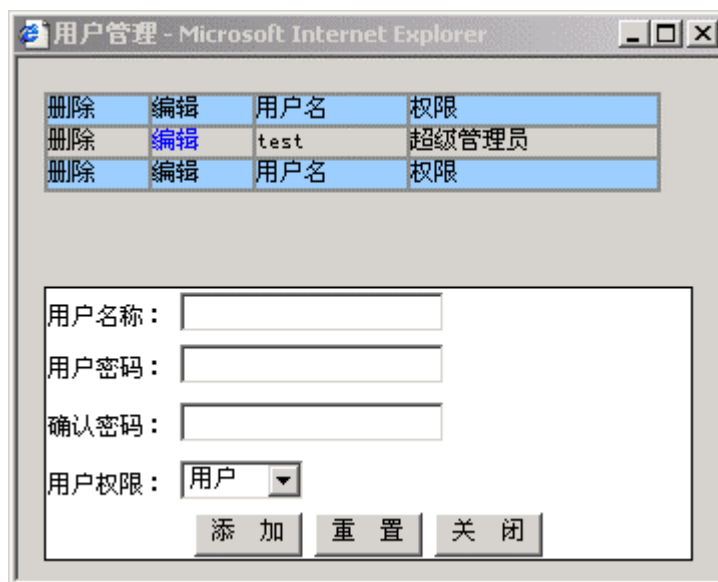
以上三种网站更新方式各有所长，前两种对服务器的性能要求比较高，但相对比较安全，校验备份方式相对来说存在一定的安全隐患，但确是最有效的方法。用户在使用过程中根据具体情况选用。

3.8 用户管理

WebKeeper4.0 允许多个用户同时管理，用户权限分超级管理员、管理员和用户三种，权限分配遵循以下几点规则：

- a、第一次连接时建立的超级管理员账户是系统唯一的超级管理员，具有最高的权限，用户只能对此账户进行修改，不能删除；
- b、登录系统的用户不能删除自身；
- c、超级管理员编辑/删除管理员或用户账户不需要认证；
- d、管理员编辑其他管理员账户时需要密码认证，管理员编辑/删除用户账户不需认证；
- e、用户编辑其他用户账户需要认证，但不能编辑/删除超级管理员或管理员账户。

选择管理--> 用户管理，系统弹出以下对话框：



(图 3.81)

用户需要编辑/删除某个账户，则点击该账户前的编辑或删除键，若需要添加账户，则在对话框中填写相应的账户信息，点击“添加”按钮即可。

3.9 静态恢复/校验备份

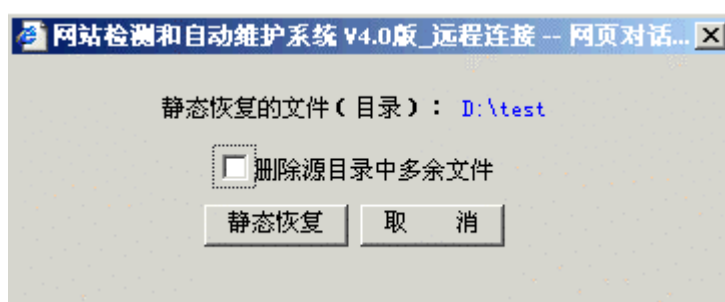
WebKeeper 系统除了阻断、自动恢复功能以外还提供了静态恢复和校验备份等功能：

★ 静态恢复：为了确认保护对象的完整性，系统给用户提供的随时可以手动恢复的功能。

★ 校验备份：为了确保备份库的真实有效，系统给用户提供的随时可以手动校验备份库功能。

3.9.1 静态恢复

首先选中需要恢复的保护对象（具体操作请参照“添加保护”章节），然后点击工具-->静态恢复，弹出属性框如下图：

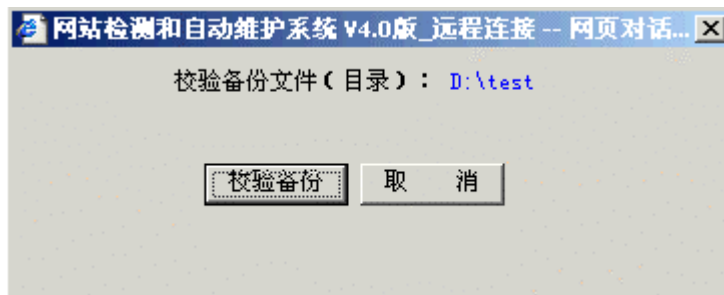


(图 3.91)

其中的删除源目录中多余文件栏，如果选中的话，则恢复后源目录中多余的文件（原目录中有而备份库里没有的文件）被删除，否则保留。

3.9.2 校验备份

首先选中需要恢复的保护对象（具体操作请参照“添加保护”章节），然后点击工具-->校验备份，弹出属性框如下图：



(图 3.92)

点击“校验备份”系统开始自动校验，校验备份是跟静态恢复相反方向的操作。

3.10 备份库管理器

备份库是 WebKeeper4.0 为了保护备份数据的安全而设置的以文件（LIBRARY）形式集中存放保护内容的备份手段，备份库受到 WebKeeper 系统的阻断保护，普通用户不能打开/查看备份库内容，超级管理员可以通过系统提供的备份库管理器来进行备份库日常维护。

[开始]—>[程序]—>[Venustech]—>[WebKeeper4.0]—>[备份库管理器]，启动备份库管理器时需要用户身份认证（只有超级管理员能够使用），见下图：



(图 3.101)

在此输入 WebKeeper 的超级管理员账户和密码，点击确定即可进入，备份库管理器的主界面如下图：



(图 3.102)

左窗口以树形显示您的备份库列表，用鼠标点击某一节点，右窗口便会显示该节点下的详细内容，包括文件名、引用计数、大小、偏移位置、属性、创建时间、修改时间、访问时间等信息。若用鼠标双击右窗口中的某一个文件的话，可以执行该文件或打开文件查看内容，下脚的状态栏显示备份库文件的大小、记录数（文件个数）等统计数据。

文件名：保护文件/目录的名称。

应用计数：该文件/目录的保护标志，1-表示受保护，0-表示已删除保护。

大小：即文件/目录的大小，以 B 为单位。

偏移位置：文件/目录在备份库中的存放位置。

属性：文件/目录的属性，分数字属性和可读属性。

创建时间、修改时间、访问时间：文件/目录的创建、修改和访问时间。

添加/编辑/删除保护：提供本地的添加/编辑/删除保护的功能，相对于 Web 控制台中的添加/编辑/删除保护功能来说，该功能的安全性比较好，因为服务器的本地资源信息不用通过远程传输，所以建议用户使用本功能来添加/编辑/删除保护。

静态恢复/校验备份：跟控制台的静态恢复/校验备份功能一样，备份库管理器也具有静态恢复/校验备份功能，而且可以实现比控制台更细的静态恢复/校验备份操作，即您可以用鼠标选中左窗口的某个目录或右窗口中的某一个文件，然后点击工具栏的静态恢复/校验

备份进行局部的静态恢复/校验备份。

整理备份库：以当前保护内容为准，删除备份库中多余的文件/目录。WebKeeper 系统对从控制台“删除保护”的保护内容，并未真正从备份库中删除，超级管理员可以使用整理备份库功能来删除备份库中相应部分内容。

备份库比较：根据您选中的保护目录/文件，比较备份库和源文件，比较内容包括属性比较和内容比较，比较结果将在“比较列表”标签页中显示。

查询：提供了一个对备份库中的子目录/文件的一个条件查询工具，使用户很方便就能找到自己想看的文件。

3.11 WebKeeper 服务管理器

WebKeeper 服务管理器类似于 SQL 的服务管理器，为管理员提供开启/停止 WebKeeper 系统服务的简捷工具。

双击 Windows 任务栏的  按钮，或点击[开始]—>[程序]—>[Venustech] —> [WebKeeper4.0] —> [服务管理器]，启动 WebKeeper 服务管理器，界面如下图：



(图 3.111)

WebKeeper 服务管理器具有开始、暂停、停止 WebKeeper 服务和 WebKeeperManager 服务的功能，同时，通过刷新服务来获取服务的当前状态。

第四章 技术名词解释

- 1、**用户密码**：每个帐户都有一个登陆密码，密码长度在 8~40 字节之间，用户应该定时或不定时修改密码，以提高密码的安全性。
- 2、**实时监测**：这是 WebKeeper 的主要功能和基本特色，即对被保护文件进行不间断的监测，一旦发现删除、修改、重命名等非法操作，则依据用户设置的保护类型做出响应：阻断、自动恢复，并发出告警信息，使用户能及时发现非法操作。
- 3、**备份目录**：为有效自动恢复，系统需要将被保护对象进行备份（建立备份库），备份目录则是备份库存放的路径，备份目录必须用全路径描述。
- 4、**自动恢复**：一旦被保护的文件遭到破坏后，系统将自动从备份库中将原始备份的文件拷贝到被保护的目录中，从而修复被损坏的文件。
- 5、**静态恢复**：是系统提供的可供用户手动恢复的功能，它需要指定恢复对象。
- 6、**校验备份**：为了确保备份库的真实有效，系统给用户提供的随时可以手动校验备份库功能。
- 7、**警告内容存盘周期**：系统的所有警告信息都是以文件的方式来存储的，存盘周期是由用户设定的，以秒计，到指定的时间后自动保存警告信息的时间间隔。
- 8、**增量备份**：它是 WebKeeper 系统的一种保护类型，是为了方便日常网页更新工作而设的，选择了增量备份的保护方式，对保护对象所作的任何操作（包括删除、修改等），系统都认为是合法的，并且相应的更新备份库的内容。
- 9、**扫描灵敏度**：是指 WebKeeper 对非法操作作出恢复响应的的时间，它是以刻度的形式来表示的（一共有 10000 个分隔），最高和最低之间的时间间隔为 1 分钟，在设定的时间段内捉到的其他修改信息不进行恢复。灵敏度的设置要根据保护对象大小和服务器的性能而定，太

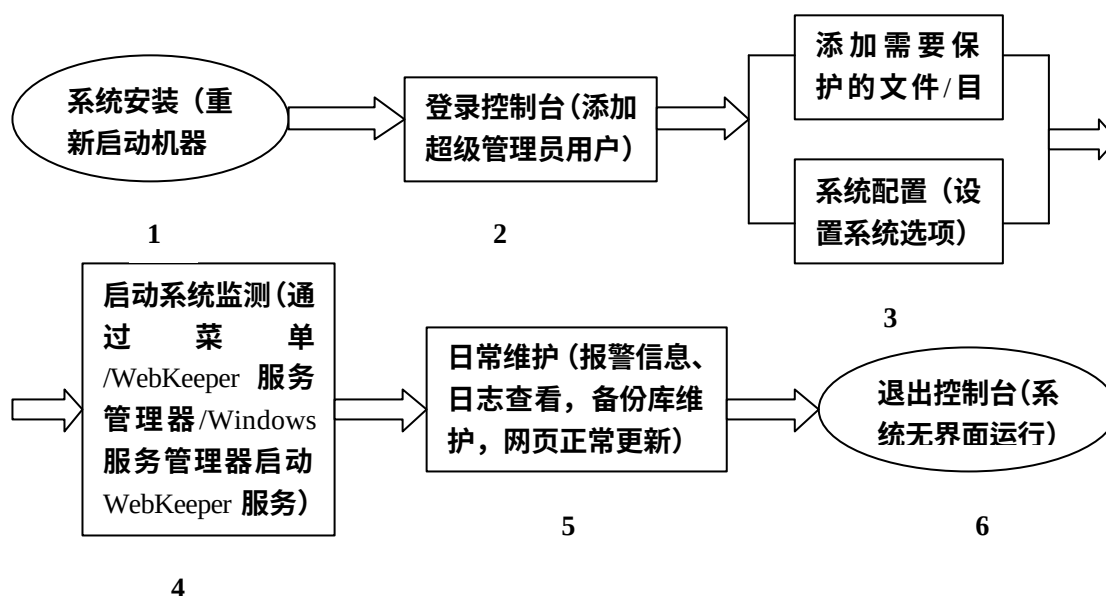
高会造成报警信息过多而且很容易造成系统死循环,过低会影响系统效率而且容易漏处理非法操作,所以适当的灵敏度设置需要用户耐心的调试而定。

10、扫描间隔：WebKeeper 系统对文件有三层保护：阻断、自动恢复和扫描恢复。扫描恢复是指系统定时对保护对象进行扫描，若发现被修改文件则进行恢复，它是系统的最后一道防线。扫描间隔就是系统两次扫描开始的时间间隔。

11、扫描类型：是对扫描恢复来说的，指系统进行定时扫描是对文件的哪一部分进行扫描：文件属性或文件内容。文件属性扫描的效率比较高、占用系统资源较小，文件内容扫描结果比较可靠，但效率低。

第五章 用户常见问题解答（FAQ）

5.1 产品正常使用流程



5.2 使用注意事项

- A、安装系统时要先关闭 Windows 系统自带的“服务”对话框；卸载系统时要关闭控制台，同时进入服务管理器停止 WebKeeper 的两个系统服务，再进行卸载操作。
- B、权限的管理：对于一个网站或一个内部网，尽量避免将某一目录设成共享，这将严重影响 WebKeeper 的系统保护作用。
- C、使用中避免保护操作系统使用的资源(如 WinNT、system32 目录等)，以免造成保护过强，影响整个系统运行。
- D、自动恢复的灵敏度一定要设为较为合适的值，建议在使用前应当进行一些测试。测试方法见“系统设置”的相关部分。
- E、用户应该分配给备份目录足够大的硬盘空间(建议 200M 以上)；另外，如果报警信息不太多的情况下，建议用户保存所有的报警日志。
- F、Web 服务器的管理员兼任 WebKeeper 的超级管理员，同时保护好 Windows 系统的 Administrator 帐户的密码，以免其他人获取停止 WebKeeper 系统服务的权限，增强 WebKeeper 系统的自身安全性。
- G、为了使 WebKeeper 的 Web 控制台能正常发布而又不影响网站的正常发布，系统安装完毕，必须对发布系统(IIS)进行必要的配置，在默认发布目录下创建一个虚拟目录，并将其主目录指向控指台的安装路径(WebKeeper4ConsoleWeb)即可(请参考 2.4 部分内容)。
- H、WebKeeper 系统的 Web 控制台对服务器的对象调用采用进程外调用方式，若用户的平台是 WindowsNT4.0/ IIS4.0 的话，需要对 IIS4.0 做配置，使它允许进程外调用服务器对象。若用户平台为 Windows2000 则不存在此问题(请参考 2.4 部分内容)。

5.3 常见问题解答

1、WebKeeper4.0 版相对于 3.2 版有哪些技术改进？

答：WebKeeper4.0 所做的技术改进主要有以下几个方面：

- a、系统从原来的程序方式改为服务方式，实现了无界面运行，同时大大增加了系统的安全性。
- b、增加了多个用户多个控制端同时管理一个 WebKeeper 服务端的功能。
- c、实现了保护方式的多样性、灵活性，各个保护对象可以设置成不同的保护类型。
- d、加强了备份库的安全性，备份库作为 WebKeeper 的默认保护对象，只要系统服务一开启，备份库 就处于阻断保护状态。
- e、采用了 COM/DCOM 技术，实现监测端不需另开端口即可以接受远端控制，而不会降低服务器的安全，同时可方便地提供二次开发接口，满足了用户在自己的产品中对 WebKeeper 进行管理的需求。
- f、实现了日志导入/导出功能。

2、保护目录或文件与系统或其他软件发生冲突，怎么办？

答：避免保护过强。如果保护设置过强，将会涉及到系统或其他软件使用的文件设为保护，则会发生共享冲突或引起不应有的故障，这时请先删除保护，将需要保护的内容与系统或其他软件使用的内容分离开来，然后添加需要保护的内容。

3、为何从浏览器登陆不了控制台？

答：WebKeeper 系统是通过 Web 方式来登陆控制台的，这就需要两个条件：一、登陆端机器跟 WebKeeper 服务器处于连通状态；二、安装 WebKeeper 系统的服务器安装了发布系统，而

且已经启动了（这一点用户可以不考虑，因为所保护的是网站，发布系统是必需的）；三、WebKeeper 系统的远端控制模块安装路径选择为发布系统的发布主目录。所以遇到上述问题，请用户着重从上述三方面来检查，另外，要确认一下您的 IE 版本是否高于 4.0，否则需要升级。

4、为什么点击“静态恢复和校验备份”菜单，系统没有响应？

答：静态恢复和校验备份功能都是针对某一个保护对象来说的，用户需要先选中某一个保护对象才能执行静态恢复和校验备份功能。

5、系统选项中的灵敏度的作用是什么？

答：是指 WebKeeper 对非法操作作出恢复响应的的时间，它是以刻度的形式来表示的（一共有 10000 个分隔），最高和最低之间的时间间隔为 1 分钟，在设定的时间段内捉到的其他修改信息不进行恢复。灵敏度的设置要根据保护对象大小和服务器的性能而定，太高会造成报警信息过多而且很容易造成系统死循环，过低会影响系统效率而且容易漏处理非法操作，所以适当的灵敏度设置需要用户耐心的调试而定。

6、为什么在控制台上查看服务器资源时由某个盘符的内容看不到？

答：这是因为该盘符的安全配置问题，按照以下步骤进行配置一下：选中该盘符→属性→安全→删除其他的账户→添加→System 或 Everyone 账户→完全控制→高级→去掉“允许将来自父系的可继承权限传播给该对象”选项→选上“重置所有子对象的权限并允许传播可继承权限”选项→确定。

7、为什么有些目录添加不成功？

答：添加失败的原因有以下三种：

1、添加的文件/目录权限不够，请配置一下您添加的文件/目录的安全权限（选中文件/目录-->右键-->属性-->安全），添加 system 账户并使其完全控制；

2、确认一下该文件/目录是否已经添加；

3、检查一下该文件/目录名称是否带有“+”号，若是请重命名在添加保护。

8、为什么添加保护以后，我的保护目录并没有真正受到保护（还可以随意被修改）？

- 1) 检查一下是否已经启动监测，系统必须处在监测状态才起保护作用；
- 2) 检查一下保护方式，确保是阻断、自动恢复或阻断+自动恢复方式；
- 3) 请检查一下服务器是否感染了 VBS 病毒，若是的话请先查杀病毒再做保护。

5.4 严重问题处理流程

用户若在使用过程中出现了比较严重的程序问题（BUG），先不要紧张，请按照以下几点做好现场保护和求救工作，以保证我们能在最短时间内为您排除故障。

一、收集系统域环境资讯

- 1、收集硬件相关信息，如服务器型号、CPU、内存、硬盘空间和网络环境等。
- 2、收集软件应用系统信息，如系统运行平台及版本、补丁情况、其他应用软件及版本等。
- 3、收集 WebKeeper 相关信息，如 WebKeeper 版本号、BUILD 号、保护文件大小以及一些其他相关配置。

二、系统错误记录

- 1、检查 Windows 系统的 Event.log，使用[开始]--> [程序]--> [管理工具]--> [事件查看器]，将 Event.log 中有关 WebKeeper 系统的错误信息记录下来。
- 2、记录 WebKeeper 系统出错的位置以及出错前的具体操作，做好将出错的画面拷贝下来，以便将来技术人员查找错误原因。

三、请求支援

尽快与启明星辰信息技术有限公司的技术服务部取得联系，并以 E-MAIL 或传真的形式将您记录下来的错误信息发给我们，具体联系方式见“技术支持和服务”部分内容。

第六章 产品技术支持与服务

如果用户在安装和使用 WebKeeper4.0 网站监测与自动修复系统时遇到了问题，请及时与我们联系，我们将全力帮助用户解决所遇到的问题，最大限度的保护用户的权益。

如在使用过程中需要得到北京启明星辰公司的技术支持，请与启明星辰公司技术支持部联系：

E—mail：support@venustech.com.cn

电话：(010) 62149966

传真：(010) 62146778

地址：北京市中关村南大街 12 号 188#

或者登陆我们的网站：<http://www.venustech.com.cn/>