Tripwire Manager & Tripwire for Servers

2.4.2

Installation Guide

TRIPWIRE

Tripwire, Inc.
326 SW Broadway, 3rd Floor
Portland, OR 97205

tel: 1.877.TRIPWIRE
fax: 503.223.0182
http://www.tripwire.com
tripwire@tripwire.com

TW1002-02

About This Guide

Document List

The **Tripwire Installation Guide** describes installation procedures for Tripwire Manager and Tripwire for Servers software.

The **Tripwire for Servers User Guide** describes configuration and operation of Tripwire for Servers software.

The **Tripwire Manager User Guide** describes configuration and operation of Tripwire Manager software, which is used to manage multiple installations of Tripwire for Servers software.

The **Tripwire Reference Guide** contains detailed information about the Tripwire configuration and policy files.

The **Quick Reference Cards** summarize important functionality of Tripwire for Servers software.

You can access PDF versions of the Guides from the *docs* directories on the Tripwire Manager and Tripwire for Servers CDs.

You can access **online help** from the Tripwire Manager interface.

Conventions

This Guide uses the following typographic conventions.

Bold in regular text indicates FTP and HTTP URLs, and emphasizes important issues.

Italic indicates file and directory names.

`Constant` in regular text shows commands and command-line options, and policy file rule attributes, directives, and variables.

Sans Serif in examples shows actual user input on the command line.

Sans Serif Italic in examples shows variables which should be replaced with context-specific values.

Ⓦ denotes sections of the text that apply only to Windows installations of Tripwire software. Unless otherwise specified, all references to Windows refer to both Windows NT and Windows 2000.

🅄 denotes sections of the text that apply only to UNIX or Linux installations of Tripwire software. Unless otherwise specified, all references to UNIX also refer to Linux.

[options] the command reference section shows optional command-line arguments in brackets.

{ 1 | 2 | 3 } the command reference section shows sets of possible options in braces, separated by the | character. Choose only one of the options.

Unless otherwise specified, command-line examples assume that the Tripwire *bin* directory is the current working directory.

Support

For the latest information and support for Tripwire products, visit the Tripwire website or contact Tripwire Technical Support.

Tripwire Support Website: **http://www.tripwire.com/support**

Tripwire Technical Support:

e-mail:	support@tripwire.com
toll-free:	1.866.TWSUPPORT (6am-6pm Pacific)
phone:	503.276.7663

General information: info@tripwire.com

Tripwire Professional Services

Tripwire Professional Services provides flexible service and support to meet your specific technical and deployment needs. If you would like Tripwire software deployment and implementation assistance, or additional training in using Tripwire software products, visit **http://www.tripwire.com** or contact your Tripwire Sales Representative.

Tripwire Educational Services

Obtain expert hands-on technical training and experience from a Tripwire Certified Instructor. Courses are offered by Tripwire Authorized Training Centers, and prepare you to install, configure, and maintain Tripwire software. Visit **http://www.tripwire.com** or contact your Tripwire Sales Representative for more information.

Contents

1

Installing Tripwire Manager

Overview

This chapter describes installation procedures for Tripwire Manager.

Topics include:

- system requirements
- things to know before installation
- installation procedures for UNIX and Windows systems
- uninstallation procedures

In the Tripwire system, Tripwire Manager manages Tripwire for Servers software on host machines. See chapter 2 to install Tripwire for Servers on UNIX. See chapter 3 to install Tripwire for Servers on Windows.

System Requirements

Tripwire Manager 2.4 runs only on these platforms:

- Windows NT 4.0 with SP4+
- Windows 2000
- Red Hat Linux 7.0 with 2.2 kernel
- Sun Solaris 7.0 or 8.0 (SPARC only)

Warning: The Tripwire Manager installer and Tripwire Manager software require a color palette display setting of 256 colors or more. Prior to installation, ensure that the machine's color palette display is set to a minimum of 256 colors.

System Recommendations

Tripwire Manager machines should have the following for optimal performance:

- On Windows or Red Hat Linux, an Intel Pentium III class or higher processor
- On Solaris, a Sun UltraSPARC III or higher processor
- On all platforms, 256 MB RAM
- On Red Hat Linux and Solaris, 115 MB disk space
- On Windows, 60 MB disk space
- Adobe Acrobat Reader to view PDF documentation

Before Installation

This section describes topics you should understand before you install Tripwire Manager.

Installing Tripwire Manager Securely

As with any other infrastructure management software, you should manage user access to Tripwire Manager. Techniques for limiting user access to Tripwire Manager include:

- physically securing machines where Tripwire Manager is installed
- installing Tripwire Manager only to specific users' directories
- using biometric or certificate-based access control technologies to manage user access to Tripwire Manager
- changing Tripwire passphrases regularly
- installing Tripwire Monitor (see page 6 of the Tripwire Manager User Guide) for users who should view Tripwire files, but not edit them

X Windows Requirements on UNIX

Tripwire Manager requires that an X Windows session be running when you run its installer, or the application itself.

If you want to launch the installer from the command line, you must first open an X Windows session. If you try to launch the installer without an X Windows session open, the installer fails to launch. This applies also when launching the Tripwire Manager uninstaller (see page 13)

System Patch Requirements on UNIX

If you are installing Tripwire Manager on Red Hat 7.0, you must update your system to a minimum of glibc 2.1.92, available from **http://www.redhat.com/support/errata.**

If you are installing Tripwire Manager on Solaris 7 or 8, your system requires OS patches to run the Java 2 SDK v 1.3. First, go to **http://access1.sun.com/patch.recommended/rec.html** and install all current recommended OS patches for Solaris 7 or 8.

Then go to **http://java.sun.com/j2se/1.3/install-solaris-patches.html** and install any additional Java-specific OS patches for Solaris 7 or 8.

License Files

You must install license files before you can use Tripwire Manager. Obtain your license files from **http://license.tripwire.com** before or after you install Tripwire Manager.

When you visit the website, you must have the License Authorization Code (LAC) associated with your purchase. If you ordered a Tripwire Manager software CD, your LAC is on a card inside your Tripwire software package. If you ordered Tripwire Manager software by download, the LAC is sent to you via e-mail.

After you visit the Tripwire website, Tripwire, Inc. sends your license files to you by e-mail. This e-mail contains installation instructions for the license files, or you can print installation instructions from the Tripwire website.

Installing on Windows

You must log in with administrator-level privileges to perform this procedure.

To install Tripwire Manager on Windows:

1. Exit from all Windows applications before installation.
2. Insert the Tripwire Manager CD into the CD-ROM drive.
3. Skip to step 5 if AutoRun automatically launches the installer.

   or

   Browse to the CD-ROM.
4. Double-click *install_windows.bat.*
5. Select a language to use for the installer. Click OK.
6. Read the Introduction screen. Click Next.

7. Read the license agreement. Click Next.

   You must accept the terms of the license agreement to continue the installation.

8. Read the information about license files. Click Next.

9. Click Next to accept the default installation path *C:\Program Files\tripwire\manager.*

   or

   Specify a different installation folder.

10. Choose a location for a Tripwire Manager shortcut.

11. Click Install to copy the Tripwire Manager files to your system.

Note: During installation, we check your system for previous versions of Tripwire Manager and the license server associated with these versions. If a previous version of Tripwire Manager is located, the installation replaces these files. If a license server is located, you are prompted to delete the server or not.

   This may take several minutes.

12. Press Done to exit the installer.

13. Install the license files for this Tripwire Manager.

    You must install the license files before you can use Tripwire Manager. See page 6 for information about license files and how to obtain them.

Installation is now complete. See After Installation on page 10 for information on starting to use Tripwire software.

Installing on UNIX

Tripwire Manager requires that an X Windows session be running when you run its installer, or the application itself. See page 5 for more information about this requirement.

If you are installing Tripwire Manager on Solaris 7 or 8, your system requires OS patches to run the Java 2 SDK v 1.3. See page 5 for more information about required patches.

Installation Recommendations

We recommend that you follow these guidelines when installing Tripwire Manager on a UNIX system.

- Do not install Tripwire Manager as root. Tripwire Manager does not require root access to perform any of its operations. If you install Tripwire Manager as root, the Tripwire administrator must log into the system as root to run Tripwire Manager.
- Install Tripwire Manager under the same user that will run Tripwire Manager. Tripwire Manager needs write access to all directories and files created by the installer.
- Install Tripwire Manager on a local partition, not a network-mounted partition. This way you can continue to run Tripwire Manager if network-mounted partitions (such as a user's home directory) become unavailable.
- If you install to a local directory that requires root access (such as */usr/local*), create an installation directory before installation and change ownership to the user who will install and run Tripwire Manager.

```
mkdir  /usr/local/tripwire/manager
chown userid  /usr/local/tripwire/manager
```

To install Tripwire Manager on UNIX:

1. Insert the Tripwire Manager CD into the CD-ROM drive.
2. Mount the Tripwire Manager CD.
3. Open a graphical shell.

   The installer requires that an X Windows session be running.
4. Navigate to the CD root directory.
5. Launch the installer in one of two ways.

   Type this command from a command prompt:

```
sh ./install_unix
```

   or

   Double-click *install_unix*.
6. Select a language to use for the installer. Click OK.
7. Read the introduction screen. Click Next.
8. Read the license agreement. Click Next.

   You must accept the terms of the license agreement to continue.
9. Read the information about license files. Click Next.
10. Click Next to accept the default path */usr/local/tripwire/manager.*

    or

    Select a different installation directory.
11. Choose a location for a symbolic link to Tripwire Manager.
12. Click Install to copy the Tripwire Manager files to your system.

Note: During installation, we check your system for previous versions of Tripwire Manager and the license server associated with these versions. If a previous version of Tripwire Manager is located, the installation replaces these files. If a license server is located, you are prompted to delete the server or not.

This may take several minutes.

13. Press Done to exit the installer.
14. Install the license files for this Tripwire Manager.

    You must install the license files before you can use Tripwire Manager. See page 6 for information about license files and how to obtain them.

Installation is now complete. See After Installation on page 10 for information on starting to use Tripwire software.

After Installation

We recommend that you perform the following security measures after you install Tripwire Manager.

- Copy the *console.key* file (located in the Tripwire Manager directory) to a floppy disk. Store the backup disk in a secure location.

  Tripwire Manager uses *console.key* to authenticate connections with Tripwire for Servers machines. If you accidentally delete this file and you do not have a backup, you must re-install Tripwire Manager.

- To prevent unauthorized modifications, change the permissions for the Tripwire Manager directory to Full Control for authorized administrators only.

Starting Tripwire Manager

Follow these procedures to start Tripwire Manager.

Ⓦ To start Tripwire Manager in Windows:

1. Navigate to the location you chose for the Tripwire Manager shortcut.
2. Double-click the *TW_Manager* shortcut.

   or

   Navigate to the Tripwire Manager installation folder (the default is *C:\Program Files\tripwire\manager.*
3. Double-click *TW_Manager.exe.*

U To start Tripwire Manager in UNIX:

1. In a graphical shell, open a command prompt.

   Tripwire Manager requires that an X Windows session be running when you run the application. See page 5 for more information about this requirement.
2. Type this command to launch the Tripwire Manager start script:

```
(tripwire install path)/TW_Manager
```

   or

   In a graphical shell, navigate to the Tripwire Manager installation directory (the default is *usr/local/tripwire/manager*).
3. Double-click *TW_Manager* to launch the Tripwire Manager start script.

Getting Started

If you have installed Tripwire for Servers on the host machines you want to monitor, proceed to page 31 in the Tripwire Manager User Guide to get started using your Tripwire system.

If you have not installed Tripwire for Servers, see chapter 2 for information about installing Tripwire for Servers on UNIX. See chapter 3 for information about installing Tripwire for Servers on Windows.

Uninstalling Tripwire Manager

The uninstaller does not remove files and folders generated by Tripwire Manager after you have installed it. You must manually delete them after you run the uninstaller.

Ⓦ To uninstall Tripwire Manager on Windows:

1. Browse to the *tripwire/manager/UninstallerData* folder.
2. Double-click *Uninstall TW_Manager.exe* to launch the uninstaller.
3. Click Uninstall.
4. Click Exit.

🅄 To uninstall Tripwire Manager on UNIX:

1. Open a graphical shell.
2. Navigate to the *tripwire/manager/UninstallerData* directory.
3. Launch the uninstaller in one of two ways.

   Type this command from a command prompt:

```
sh ./Uninstall_TW_Manager
```

   or

   Double-click *Uninstall_TW_Manager.*

4. Click Uninstall.
5. Click Exit.

2

Installing Tripwire for Servers on UNIX

Overview

This chapter describes procedures for installing Tripwire for Servers on UNIX. Topics include:

- recommended system requirements
- things to know before installation
- interactive installation
- customizing an installation
- unattended installation

In the Tripwire system, Tripwire for Servers may be managed by Tripwire Manager. See chapter 1 to install Tripwire Manager.

System Requirements

Tripwire for Servers runs only on these UNIX platforms:

- HP-UX 11.0 with PA-RISC 1.1 or higher processor
- IBM AIX 4.3 with RS/6000
- Solaris 2.6, 7.0, or 8.0 (SPARC only)
- GNU/Linux kernel 2.2 or higher with Pentium-class or higher processor
- freeBSD 4.2 and 4.3

Tripwire for Servers machines should have the following for optimal performance:

- 128 MB RAM
- 30 MB disk space on Solaris, 25 MB on AIX 4.3, HP-UX, GNU/ Linux, and freeBSD
- A text editor that can accept a file on the command line, exit with 0 status on success, and exit with non-0 status on error (both vi and emacs meet these requirements)

Before Installation

This section describes topics you should understand before you install Tripwire for Servers.

Installation Configuration File

The installation configuration file *install.cfg* contains parameters that the installer uses to create the Tripwire for Servers directory structure. The installer also uses *install.cfg* to create initial values for the Tripwire configuration files. You can customize an installation by editing a local copy of the *install.cfg* file. However, we recommend that you use the default *install.cfg* file the first time you install Tripwire for Servers.

Installation Methods

You can install Tripwire for Servers three different ways on UNIX. Before installation, determine which way you want to install the software.

Interactive (default)	During an interactive installation the installer prompts you for input. We recommend that you perform an interactive installation with the default *install.cfg* file the first time you install Tripwire for Servers. See page 20 for instructions.
Customized	You can customize installation options by editing values in the *install.cfg* file. See page 23 for instructions.
Unattended	You can use command-line options to the installer to run an unattended (non-interactive) installation. During an unattended installation, the installer does not prompt you for input. You can use the default *install.cfg* file or a customized *install.cfg* file for an unattended installation. See page 31 for instructions.

Upgrading Tripwire Software

Tripwire data files (such as database files and policy files) migrate from Tripwire for Servers versions 2.2.1 and higher.

Go to the Tripwire Support website at **http://www.tripwire.com/services_and_support/upgrade** for more information.

System Patch Requirements

If you are installing Tripwire for Servers on Solaris2.6, 7 or 8, your system requires the Sun recommended OS patches. Go to **http://access1.sun.compatch.recommended/rec.html** and install all current recommended OS patches for Solaris 2.6, 7, or 8.

Installer Backup Behavior

If the installer detects any files in an installation directory, it prompts for your permission continue the installation. If you proceed, the installer renames the existing directory and continues the installation. The new directory name is the old name with the installer's process identification number (PID) appended.

```
tripwire.34452      # example
```

Warning: Do not install directly to */usr/bin* or any other system directory because the installer may try to rename it during installation.

Interactive Installation

You must perform this installation procedure with root or administrative privileges. The default installation path is */usr/local/tripwire/tfs.*

To perform an interactive installation with the default *install.cfg* file:

1. Insert the Tripwire for Servers CD into the CD-ROM drive.
2. Mount the CD.
3. Navigate (change directory) to the applicable platform-specific directory in the Tripwire for Servers CD root.

```
/sun_sparc
/hp-ux
/ibm_aix
/linux_intel
/freeBSD
```

4. Type this command to launch the installer.

```
./install.sh
```

5. Carefully read the license agreement.
6. Type the word `accept` to accept the license agreement.

   You must accept the terms of the license agreement to continue the installation.
7. Type `yes` to continue installation if the installer detects files in the installation directory.
8. Specify a site passphrase.

   The site passphrase protects the site key. The site key cryptographically signs site-specific Tripwire data files.

Passphrases should be at least eight characters long. Do not use words that can be found in a dictionary. Use a combination of uppercase and lowercase letters, numbers, and symbols. Do not use wildcard characters or quotes.

Warning: We recommend that you use different passphrases for the site and local keys. This decreases the possibility of an intruder gaining access to all site machines with a single passphrase.

9. Specify a local passphrase.

   The local passphrase protects the local key. The local key cryptographically signs machine-specific Tripwire data files.

10. Wait while the installer generates site and local keys, the configuration file, and a default policy file. **This may take several minutes.**

    The configuration file contains parameters that control Tripwire for Servers operation. See chapter 1 in the Tripwire Reference Guide for more information about configuration file and Agent configuration file parameters.

    A default policy file monitors only basic components common to all versions of your OS. It does not monitor version-specific OS components or the files and applications specific to your system.

    We **strongly** recommend that you replace the default policy file with an OS version-specific policy file before you run your first integrity check (this is not necessary on AIX or HP-UX). See page 20 in the Tripwire for Servers User Guide for more information about replacing the default policy file.

11. Specify a port number for communication with Tripwire Manager.

    You must specify a port number even if you do not use Tripwire Manager.

    We recommend that you use port 1169, the registered Tripwire port. If you do not use 1169, we recommend that you specify only a known available port. Ports below 1024 are restricted to system access, so do not use them.

12. Wait while the installer generates the Agent configuration file.

    The Agent configuration file contains parameters that control Tripwire Agent operations. The Tripwire Agent manages communication between Tripwire for Servers and Tripwire Manager.

    The Agent configuration file is not used if you run Tripwire for Servers as a standalone application.

13. Type `yes` to start the Tripwire Agent if you plan to connect to this machine with Tripwire Manager.

    or

    Type `no` if you plan to run Tripwire for Servers as a standalone application. You should not start the Tripwire Agent. Starting the Tripwire Agent introduces a security risk. See page 33 for more information.

Installation is now complete. See After Installation on page 33 for information about getting started using Tripwire for Servers.

Customizing Installation

You can customize an installation by editing the values in the installation configuration file *install.cfg*. The installer uses the parameters in the *install.cfg* file to create the Tripwire for Servers directory structure and set initial values in the Tripwire software configuration files.

To edit the *install.cfg* file:

1. Insert the Tripwire for Servers CD into the CD-ROM drive.
2. Mount the CD.
3. Navigate (change directory) to the applicable platform-specific directory in the Tripwire for Servers CD root.

```
/sun_sparc
/hp-ux
/ibm_aix
/linux_intel
/freeBSD
```

4. Copy the *install.cfg* file from the CD to your hard drive.

```
cp ./install.cfg /tmp/myinstall.cfg
```

5. Edit and save the local *myinstall.cfg* in a text editor.

   See page 25 for brief descriptions of the *install.cfg* parameters. See chapter 1 in the Tripwire Reference Guide for more information about the configuration file parameters set by the *install.cfg* parameters.

6. To perform an interactive installation, type this command from the applicable platform-specific directory in the CD root.

```
./install.sh /tmp/myinstall.cfg
```

or

To perform an unattended installation, type this command from the applicable platform-specific directory in the CD root, replacing *site* and *local* with the passphrases you want to use for this installation.

```
./install.sh -s site -l local -n /tmp/myinstall.cfg
```

See page 31 for more information about unattended installation.

Installation is now complete. See After Installation on page 33 for information about getting started using Tripwire for Servers.

Installation Parameters and Values

The *install.cfg* file contains parameters you can edit to customize a Tripwire for Servers installation. The * character denotes required parameters that must be present and defined in *install.cfg* for the software to run. All values except numerical values are case-sensitive.

See chapter 1 in the Tripwire Reference Guide for more information about the configuration file parameters set by *install.cfg* parameters.

Parameter and Value Type	**Description and Default Value**
TWROOT * *path*	sets the initial Tripwire for Servers root directory Default value: /usr/local/tripwire/tfs
TWBIN * *path*	sets the directory that contains Tripwire for Servers binaries, the configuration file *tw.cfg* and the Agent configuration file *twagent.cfg* Default value: ${TWROOT}/bin
TWPOLICY * *path*	sets the directory that contains Tripwire for Servers policy files Default value: ${TWROOT}/policy
TWMAN *path*	sets the directory that contains Tripwire for Servers man pages Default value: ${TWROOT}/man
TWDB * *path*	sets the directory that contains Tripwire for Servers database files Default value: ${TWROOT}/db
TWSITEKEYDIR * *path*	sets the directory that contains the cryptographic site key file Default value: ${TWROOT}/key
TWLOCALKEYDIR * *path*	sets the directory that contains the cryptographic local key file Default value: ${TWROOT}/key
TWAUTHDIR * *path*	sets the directory that contains the Tripwire Agent authentication key file Default value: ${TWROOT}/key

Parameter and Value Type	**Description and Default Value**
TWREPORT *path*	sets the directory that contains report files generated by Tripwire integrity checks Default value: ${TWROOT}/report
TWLOG *path*	sets the directory that contains the Tripwire Agent log file Default value: ${TWROOT}/report
TWSCHEDFILE * *path*	sets the directory that contains the Tripwire Agent schedule files Default value: ${TWROOT}/db
TWTASKFILE * *path*	sets the directory that contains the Tripwire Agent task cache Default value: ${TWROOT}/db
TWPOLICYRIGHTS *octal number*	sets the POLICYRIGHTS value in the *tw.cfg* file POLICYRIGHTS sets absolute access permissions to policy files. System umask settings do not modify these permissions. Default value: 644
TWDBRIGHTS *octal number*	sets the DBRIGHTS value in the *tw.cfg* file DBRIGHTS sets absolute access permissions to database files. System umask settings do not modify these permissions. Default value: 644
TWREPORTRIGHTS *octal number*	sets the REPORTRIGHTS value in the *tw.cfg* file REPORTRIGHTS sets absolute access permissions to report files. System umask settings do not modify these permissions. Default value: 644
TWSCHEDULERIGHTS *octal number*	sets the SCHEDULEFILERIGHTS value in the *agent.cfg* file SCHEDULEFILERIGHTS sets absolute access permissions to schedule files. System umask settings do not modify these permissions. Default value: 644

Parameter and Value Type	**Description and Default Value**
TWLOGRIGHTS *octal number*	sets the LOGFILERIGHTS value in the *agent.cfg* file LOGFILERIGHTS sets absolute access permissions to log files. System umask settings do not modify these permissions. Default value: 644
TWAUTHKEYRIGHTS *octal number*	sets the AUTHKEYRIGHTS value in the *agent.cfg* file AUTHKEYRIGHTS sets absolute access permissions to the *authentication.dat* file. System umask settings do not modify these permissions. Default value: 644
TWTASKRIGHTS *octal number*	sets the TASKFILERIGHTS value in the *agent.cfg* file TASKFILERIGHTS sets absolute access permissions to task files. System umask settings do not modify these permissions. Default value: 644
TWMAILMETHOD *text string*	sets the MAILMETHOD value in the *tw.cfg* file MAILMETHOD specifies a mail protocol for e-mail reports. Default value: SENDMAIL
TWMAILPROGRAM *path*	sets the MAILPROGRAM value in the *tw.cfg* file MAILPROGRAM specifies the program used by sendmail. Default value: /usr/lib/sendmail -oi -t
TWSMTPHOST *numerical IP address* *or* *text string (host name)*	sets the SMTPHOST value in the *tw.cfg* file SMTPHOST specifies a host for SMTP e-mail reports. Default value (commented out): mail.domain.com
TWSMTPPORT *port number*	sets the SMTPPORT value in the *tw.cfg* file SMTPPORT specifies a port for SMTP e-mail reports. Default value (commented out): 25

Parameter and Value Type	**Description and Default Value**
TWMAILNOVIOLATIONS *true / false*	sets the MAILNOVIOLATIONS value in the *tw.cfg* file MAILNOVIOLATIONS causes Tripwire for Servers to report that it found no violations during an integrity check. If set to false, Tripwire for Servers does not send an e-mail report when it finds no violations. Default value: true
TWMAILFROMADDRESS *SMTP e-mail address*	sets the MAILFROMADDRESS value in the *tw.cfg* file MAILFROMADDRESS provides a resolvable From address for SMTP e-mail reports to ensure proper delivery by the mail server. Default value (commented out): root@domain.com
TWEMAILREPORTLEVEL *numerical*	sets the EMAILREPORTLEVEL value in the *tw.cfg* file EMAILREPORTLEVEL specifies the level of detail shown in e-mail reports. See the Tripwire Reference Guide for report level samples. Default value: 3
TWREPORTLEVEL *numerical*	sets the REPORTLEVEL value in the *tw.cfg* file REPORTLEVEL specifies the level of detail shown in printed reports. See the Tripwire Reference Guide for report level samples. Default value: 3
TWGLOBAL_EMAIL *address1, address2, ...*	sets the GLOBALEMAIL value in the *tw.cfg* file GLOBALEMAIL specifies an e-mail address to receive a complete e-mail report after each integrity check. Default value (commented out): address@company.com;address2@company.com
TWEMAIL_ENCODING *text string*	sets the MAILENCODING value in the *tw.cfg* file MAILENCODING specifies a character set for Tripwire e-mail reports sent by SMTP or sendmail. Default value (commented out): auto Valid values: auto (detect OS character set), none (do not specify a character set), or ISO-2022-JP

Parameter and Value Type	**Description and Default Value**
TWLATEPROMPTING *true / false*	sets the LATEPROMPTING value in the *tw.cfg* file LATEPROMPTING delays the prompt for passphrases on the command line until the last possible moment. Default value: false
TWLOOSEDIRCHK *true / false*	sets the LOOSEDIRECTORYCHECKING value in the *tw.cfg* file LOOSEDIRECTORYCHECKING causes Tripwire for Servers to ignore changes to directories caused by changes to files within them to reduce report noise. Default value: true
TWTRAVERSE_MOUNTS *true / false*	sets the TRAVERSEMOUNTS value in the *tw.cfg* file TRAVERSEMOUNTS allows Tripwire for Servers to cross file system mount points during integrity checks. Default value: false
TWEDITOR *path*	sets the EDITOR value in the *tw.cfg* file EDITOR specifies a text editor for interactive integrity checks. Default value: */bin/vi*
TWTEMP *path*	sets the TEMPDIRECTORY value in the *tw.cfg* file The TEMPDIRECTORY stores Tripwire for Servers temp files. If the default directory does not exist on your system, you must create the default directory or specify a different directory. Default value: */tmp*
TWIPADDRESS *numerical IP address*	sets the IPADDRESS value in the *agent.cfg* file IPADDRESS specifies a particular IP address for the Tripwire Agent to listen on. Default value (commented out): 127.0.0.1
PORT_NUM * *numerical*	sets the PORTNUMBER value in the *agent.cfg* file PORTNUMBER specifies the port used for communicating with Tripwire Manager. Default value: none (if no value is specified, Tripwire for Servers defaults to its default port 1169)

Parameter and Value Type	**Description and Default Value**
TWSNMPHOST *numerical IP address* *or* *text string (host name)*	sets the SNMPHOST value in the *tw.cfg* file SNMPHOST causes Tripwire for Servers to send an SNMP trap to a specified host after integrity checks. Default value (commented out): 127.0.0.1
TWSNMPPORT *numerical*	sets the SNMPPORT value in the *tw.cfg* file SNMPPORT specifies a port for SNMP traps sent by Tripwire for Servers. Default value (commented out): 162
TWSNMPCOMMUNITY *text string*	sets the SNMPCOMMUNITY value in the *tw.cfg* file SNMPCOMMUNITY specifies a community name for SNMP traps sent by Tripwire for Servers. Default value (commented out): public
TWSYSLOG *true / false*	sets the SYSLOGREPORTING value in the *tw.cfg* file SYSLOGREPORTING causes Tripwire for Servers to log events to the syslog. Default value: false
TWSYSLOGREPORTLEVEL *numerical*	sets the SYSLOGREPORTLEVEL value in the *tw.cfg* file SYSLOGREPORTLEVEL sets a level of detail for log entries. Default value (commented out): 0
TWAUDITLOG *true / false*	sets the AUDITLOG value in the *tw.cfg* file AUDITLOG is for integrating Tripwire for Servers with CyberSafe Centrax on Solaris only. See the Tripwire Reference Guide for more information. Default value: false

Unattended Installation

You can use command-line options to the installer to bypass interactive prompting. When you run an unattended installation, you agree to the terms of the license agreement by default. If you do not specify a port number for the Tripwire Agent in the *install.cfg* file, an unattended installation uses the default Tripwire port 1169.

If you do not alter the value for the `TWROOT` parameter in the install.cfg file, the default installation path is */usr/local/tripwire/tfs.*

The format for the unattended install command is:

```
./install.sh -s site -l local -n install.cfg
```

Option	Meaning
-s *site passphrase*	Use the specified site passphrase
-l *local passphrase*	Use the specified local passphrase
-n	No prompting The -n option causes the installer to create and populate its target directories without prompting for verification. This mode requires the site and local passphrase arguments.
install.cfg	Use the specified install.cfg file for installation values. By default the installer uses the values in *install.cfg* for installation if no other file is specified on the command line. To run an unattended install with a customized *install.cfg* file, specify the name of a customized *install.cfg* file on the command line.

To perform an unattended installation:

1. Insert the Tripwire for Servers CD into the CD-ROM drive.
2. Mount the CD.
3. Navigate (change directory) to the applicable platform-specific directory in the CD root.

```
    /sun_sparc
    /hp-ux
    /ibm_aix
    /linux_intel
    /freeBSD
```

4. Launch the installer in one of two ways.

   To use the default *install.cfg* file, type this command, replacing *site* and *local* with the passphrases you want to use for this installation.

```
./install.sh -s site -l local -n
```

   or

   To use a customized *install.cfg* file, type this command, replacing *site* and *local* with the passphrases you want to use for this installation.

```
./install.sh -s site -l local -n /tmp/myinstall.cfg
```

   Wait while the installer copies files.

   If you want to run Tripwire for Servers as a standalone application, the installation is now complete. See page 33 to get started using Tripwire for Servers.

   If you want to manage this machine with Tripwire Manager, proceed to step 5.

5. Navigate to the Tripwire for Servers *bin* directory.

6. Type this command to start the Tripwire Agent.

```
twagent --start
```

Installation is now complete. See page 33 for information about how to get started using Tripwire for Servers.

After Installation

We recommend that you change the permissions for the Tripwire for Servers directory and files to Full Control for authorized administrators only.

If you installed Tripwire Agent and you do not plan to use Tripwire Manager, we recommend that you remove the *twagent* executable from your system. This executable makes it possible for a Tripwire Manager to register and take control of your Tripwire for Servers installation.

Getting Started

If you have already installed Tripwire Manager, see page 31 of the Tripwire Manager User Guide to get started using your Tripwire system. You can perform all remaining configuration tasks for this installation through Tripwire Manager.

See chapter 1 for information about installing Tripwire Manager.

See page 15 of the Tripwire for Servers User Guide to get started using Tripwire for Servers as a standalone application from the command line.

3

Installing Tripwire for Servers on Windows

Overview

This chapter describes the procedure for installing Tripwire for Servers on Windows. Topics include:

- recommended system requirements
- things to know before installation
- installation procedure
- uninstallation procedures

In the Tripwire system, Tripwire for Servers may be managed by Tripwire Manager. See chapter 1 for information about installing Tripwire Manager.

System Requirements

Tripwire for Servers runs only on the following Windows platforms:

- Windows NT 4.0 with SP4+
- Windows 2000

Tripwire for Servers machines should have the following for optimal performance:

- 128 MB RAM
- 20 MB disk space

Before Installation

This section describes topics you should understand before you install Tripwire for Servers.

Upgrading Tripwire Software

Tripwire data files (such as database files and policy files) migrate from Tripwire for Servers versions 2.2.1 and higher.

Go to the Tripwire Support website at **http://www.tripwire.com/services_and_support/upgrade** for more information.

Installer Backup Behavior

If the installer detects Tripwire key files in an installation folder, it prompts for permission to rename them with a *.bak* extension. If *.bak* files already exist, the installer deletes them and replaces them with the newer *.bak* files. Tripwire software allows only one backup copy for each file. You cannot disable or change this feature.

Installing Tripwire for Servers

You must log in with administrator-level privileges to perform this installation.

To install Tripwire for Servers:

1. Exit from all Windows applications.
2. Insert the Tripwire for Servers CD into the CD-ROM drive.
3. Skip to step 6 if AutoRun automatically launches the installer.

   or

4. Browse to the CD-ROM.
5. Double-click *Setup.exe*.
6. Read the Welcome screen. Click Next.
7. Carefully read the license agreement. Click Yes.

   You must accept the terms of the license agreement to continue the installation.

8. Click Next to accept the default installation folder *C:\Program Files\Tripwire\TFS.*

   or

   Click Browse to browse to a different folder.

   The installer does not allow you to install over an existing Tripwire software installation. See page 38 for more information about upgrading an existing Tripwire software installation.

9. Select a mail protocol for Tripwire e-mail reports.

   If you select SMTP, you must specify the SMTP server name, and a port number for SMTP mail. You can also specify a resolveable SMTP e-mail address for the From field of e-mail reports.

10. Select SNMP settings that Tripwire for Servers will use to communicate with network management tools.

11. Select a method of operation for Tripwire for Servers.

    You can communicate with Tripwire Manager through any IP address.

    or

    You can specify a particular IP address if a machine has multiple network interface cards (NICs).

    or

    If you run Tripwire for Servers as a standalone application you do not need to specify an IP address. Skip to step 14.

12. Specify a port number for the Tripwire Agent service to use.

    We recommend that you use port 1169, the registered Tripwire port. If you do not use 1169, we recommend that you specify only a known available port. Ports below 1024 are restricted to system access, so do not use them.

13. Select a user account for the Tripwire Agent service.

    By default the Tripwire Agent service runs as user LocalSystem.

Warning: The Tripwire Agent user account creates and therefore owns the Tripwire data files (such as database and policy files). Only the owner of a Tripwire database file can access it to run an integrity check. Future changes to the user account may cause existing database files to become inaccessible.

14. Review the summary of the options and values you selected.

    Click Back now to make any changes.

    or

    Click Next if the summary meets your expectations.

15. Wait while the installer copies files to the installation directory.

16. Specify a site key passphrase.

    The site passphrase protects the site key. The site key cryptographically signs site-specific Tripwire data files.

    Passphrases should be at least eight characters long. Do not use words that can be found in a dictionary. Use a combination of uppercase and lowercase letters, numbers, and symbols. Do not use wildcard characters or quotes.

Warning: We recommend that you use different passphrases for the site and local keys. This decreases the possibility of an intruder gaining access to all site machines with a single passphrase.

17. Specify a local key passphrase.

    The local passphrase protects the local key. The local key cryptographically signs machine-specific Tripwire data files.

18. Wait while the installer generates the site and local keys. **This may take several minutes.**

    If site and local keys exist from an earlier installation, the installer gives you the option to overwrite them.

Warning: If you overwrite existing site and local keys, any files signed with them become inaccessible. Tripwire, Inc. cannot help you recover the files in this case.

19. Wait while the installer generates the configuration files.

20. Wait while the installer generates a default policy file.

    The default policy files monitors only the basic components of your operating system. We **strongly** recommend that you replace the default policy file with the full-featured policy file for Windows NT or Windows 2000 before you run the first integrity check.

    See page 20 of the Tripwire for Servers User Guide for more information about replacing a default policy file.

21. Click Yes to add the path to the Tripwire for Servers executable files to your user's environment path.

    or

    Click No if you want to add the path to the Tripwire for Servers executables to your user's environment path manually later.

Installation is now complete. See After Installation on page 43 for information about getting started using Tripwire for Servers. If you want to register this machine with Tripwire Manager, first verify that the Tripwire Agent service is running.

To verify that Tripwire Agent is running in Windows NT:

1. Select Start > Settings > Control Panel > Services.
2. Scroll down to Tripwire Agent.
3. If the Tripwire Agent's Status column does not show Started, select Tripwire Agent and click Start.
4. Close the Services window.

To verify that Tripwire Agent is running in Windows 2000:

1. Select Start > Settings > Control Panel > Administrative Tools > Services.
2. Scroll down to Tripwire Agent.
3. If the Tripwire Agent's Status column does not show Started, right-click on Tripwire Agent and select Start.
4. Close the Services window.

After Installation

We recommend that you perform the following security measures after you install Tripwire for Servers.

- Change the Windows directory and file permissions on the Tripwire directories and files. For the highest security, give write and execute permissions only to users who are authorized to administer Tripwire software.
- If you chose to run the Tripwire Agent service as a specific user, ensure that the user account has read and write permission for all Tripwire for Servers directories and files.
- If you installed Tripwire Agent but you do not plan to use Tripwire Manager, we recommend that you remove the *twagent* executable from your system.

  This executable makes it possible for any Tripwire Manager on your network to register and take control of your Tripwire for Servers installation.

Getting Started

If you have already installed Tripwire Manager, see page 31 of the Tripwire Manager User Guide to get started using your Tripwire system. You can perform all remaining configuration tasks for this installation through Tripwire Manager.

See chapter 1 for information about installing Tripwire Manager.

See page 15 of the Tripwire for Servers User Guide to get started using Tripwire for Servers as a standalone application from the command line.

If you want to move data files from an existing Tripwire software installation to Tripwire for Servers, go to the Tripwire website at **http://www.tripwire.com/services_and_support/upgrade** for more information.

Uninstalling Tripwire for Servers

The uninstaller does not remove files and folders created by Tripwire software after installation.You must manually delete them after you run the uninstaller.

To uninstall Tripwire for Servers on Windows:

1. Select Start > Settings > Control Panel > Add/Remove Programs.
2. Select Tripwire for Servers 2.4 from the list of applications.
3. Click Remove.

   InstallShield uninstalls Tripwire for Servers.
4. Close the Add/Remove Programs window.
5. Manually delete any Tripwire for Servers data files.

Index