Command Quick Reference

See the Tripwire for Servers User Guide for exhaustive information on command modes and options.

				tripwire					twadmin								twprint	
				Database Initialize	Integrity Check	Database Update	Policy Update	Test	Create Config	Print Config	Create Policy	Print Policy	Remove Encryption	Encrypt	Examine Encryption	Generate Keys	Print Report	Print Database
				--init	--check	--update	--update-policy	--test	--create-cfgfile	--print-cfgfile	--create-polfile	--print-polfile	--remove-encryption	--encrypt	--examine	--generate-keys	--print-report	--print-dbfile
				-m i	-m c	-m u	-m p	-m t	-m F	-m f	-m P	-m p	-m R	-m E	-m e	-m G	-m r	-m d
Reporting	--verbose	-v		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
	--silent	-s		●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
Input/ Output	--dbfile	-d	*database*	●	●	●	●											●
	--report-file	-r	*report*		●	●											●	
	--cfgfile	-c	*cfgfile*	●	●	●	●	●	●	●	●	●	●	●	●		●	●
	--polfile	-p	*polfile*	●	●		●				●	●						
	--visual	-V	*editor*		●	●												
	--site-keyfile	-S	*sitekey*	●	●	●	●		●		●	●	●	●	●	●		
	--local-keyfile	-L	*localkey*	●	●	●	●						●	●	●	●	●	●
Output	--report-level	-t	0|1|2|3|4														●	
	--report-format	-F	classic| html|xml		●												●	
	--email-report	-M			●													
	--email-report-level	-t	0|1|2|3|4		●													
	--text-report-level	-T	0|1|2|3|4		●													
	--no-tty-output	-n			●													
	--interactive	-I			●													
	--output-file	-o	*output file*		●												●	●
	--output-level	-t	0|1|2															●
	--output-format	-F	classic| html|xml															●
	--base64	-b			●	●											●	●
Scope of Operation	--rule-name	-R	*rule*		●	●											●	
	--properties	-P	*properties*														●	●
	--severity	-l	*level|name*		●												●	
	--section	-x	*section*		●	●											●	●
	--ignore	-i	*properties*		●													
Security Settings	--signed-report	-E			●													
	--secure-mode	-Z	low|high			●	●*											
	--no-encryption	-e		●					●		●							
Unattended Operation	--accept-all	-a				●												
	--site-passphrase	-Q	*passphrase*				●		●		●		●	●		●		
	--local-passphrase	-P	*passphrase*	●	●	●	●						●	●		●		
Testing	--email	-e	*address*					●									●	
	--snmp	-N						●										
	--syslog	-l						●										
	--execute	-X	*object*					●										
Files	Files in brackets are optional. All other files are REQUIRED.				[object] [object]	[object] [object]	text policy file		text config file		text policy file		file [file] ...	file [file] ...	file [file] ...		[object] [object] ...	[object] [object] ...

* tripwire Policy Update mode also supports --secure-mode/-Z **medium**

TRIPWIRE®

Tripwire for Servers

for UNIX

Quick Reference Card

Tripwire, Inc.
326 SW Broadway
3rd Floor
Portland, OR 97205
tel: 877.TRIPWIRE (toll-free)
fax: 503.223.0182

Tripwire Policy File Quick Reference

See the Tripwire Reference Guide for exhaustive information on policy file syntax.

RULES

```
object -> property ;
/usr/bin/passwd -> +pinugs ;
```

EXCLUSIONS

```
! object ;
! /usr/bin/tmp ;
```

PREDEFINED VARIABLES

Variable	Included Properties
`ReadOnly`	+pinugsmdbfCMAG
`Dynamic`	+pinugdfAG
`Growing`	+pinugdlfAG
`IgnoreAll`	*reports on existence of object only (disappearance of object causes a violation)*
`IgnoreNone`	*checks all properties*
`Device`	+pugsdrfA

RULE ATTRIBUTES

```
object -> property (attribute = value,...);
/usr/mail -> +pinug (rulename = "mail",severity = 50);
```

Attribute	Purpose
`rulename`	Assigns a name to a rule. Default value (if no other is specified) is the last element of an object name.
`severity`	Assigns a numeric severity level to a rule.
`emailto`	Sends e-mail notification of violations. See the Email Reporting section.
`recurse`	Controls recursion for directories. `True`, `false`, and numeric values > 0 are valid.
`onviolation`	Executes a command if the rule is violated.
`match`	Specifies wildcard pattern matching of file types for integrity checks.

TW1007-03

PROPERTIES

Property	Checks
a	Access timestamp
b	Number of blocks allocated
c	Inode creation/modification timestamp
d	ID of device on which inode resides
e	Report events related to this object (from the audit log facility)
f	Flags (additional permissions on object—varies by OS)
g	Group ID of owner
i	Inode number
l	Growing file
m	Modification timestamp
n	Number of links
p	Permission and file mode bits
r	ID of device pointed to by inode (valid only for device objects)
s	File size
u	User ID of owner
A	ACL settings
C	CRC-32 hash
G	Inode generation number
H	HAVAL hash
M	MD5 hash
S	SHA hash

DIRECTIVES

```
@@directive arguments
@@print "Scanning user directory"
```

Directive	Purpose
`@@section`	Designates a section of the policy file.

`@@ifhost`
`@@else`
`@@endif`
	Allows conditional interpretation of the policy file.

`@@print`	Prints a message to *stdout*.
`@@error`	Prints a message to *stdout* and exits.
`@@end`	Marks the logical end-of-file.

Tripwire Reporting Quick Reference

EMAIL REPORTING

To use email reporting, you must do all of these:

- Set the MAILMETHOD, MAILPROGRAM, SMPTHOST, and SMTPPORT parameters in the configuration file. After setting these parameters, you can test them from the command line with the Test mode of the `tripwire` command (see the Tripwire for Servers User Guide for more information).
- Specify email recipients in one of two ways: use `emailto` rule attributes (in the policy file) or the GLOBALEMAIL parameter (in the configuration file).
- Use the `-M` or `--email-report` option of the `tripwire` command when you run an integrity check.

LEVEL OF REPORT DETAIL

To specify the level of detail for a Tripwire report:

- Set your desired default report levels via the EMAILREPORTLEVEL and REPORTLEVEL configuration parameters
- Specify a level for a single e-mail report via the `-t` or `--email-report-level` option to the tripwire command when running an integrity check
- Specify a level for a single report via the `-T` or `--text-report-level` option to the tripwire command when running an integrity check
- Specify a level for a single report via the `-t` or `--report-level` option to the twprint command when printing a report file

To specify the level of email report file for an integrity check:

```
tripwire --check --email-report-level  [0 | 1 | 2 | 3 | 4]
```

To specify the level of report file for an integrity check:

```
tripwire --check --text-report-level  [0 | 1 | 2 | 3 | 4]
```

Report Levels	Report
0	single line summary report; lists total adds, removes and changes
1	parsable list of all violated objects
2	summary report; lists violations by section and rule name
3	**default report level;** shows expected and observed properties for each violated object but more concisely than a level 4 report
4	full report; maximum level of detail