TRIPWIRE COMMAND REFERENCE

				tripwire					twadmin								twprint	
				Database Initialize	Integrity Check	Database Update	Policy Update	Test	Create Config File	Print Config File	Create Policy File	Print Policy File	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
Mode of Operation	--interactive	-I			●													
	--email	-e	*address*					●										
Reporting	--verbose	-v		●	●	●	●		●	●	●	●	●	●	●	●	●	●
	--silent	-s		●	●	●	●		●	●	●	●	●	●	●	●	●	●
Input/ Output	--dbfile	-d	*database*	●	●	●	●											●
	--twrfile	-r	*report*		●	●											●	
	--cfgfile	-c	*cfgfile*	●	●	●	●		●	●	●	●	●	●	●		●	●
	--polfile	-p	*polfile*	●	●	●	●				●	●						
	--visual	-V	*editor*		●	●												
	--site-keyfile	-S	*sitekey*	●	●	●	●		●		●	●	●	●	●	●		
	--local-keyfile	-L	*localkey*	●	●	●	●						●	●	●	●	●	●
Output	--report-level	-t	*level*														●	
	--email-report	-M			●													
	--email-report-level	-t	*level*		●													
	--no-tty-output	-n			●													
Scope of Operation	--rule-name	-R	*rule*		●													
	--severity	-l	*level|name*		●													
	--section	-x	*section*		●													
	--ignore	-i	*list*		●													
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*	●	●	●	●						●	●		●		
File(s)					[object 1] [object 2] ...		text policy file		text config file		text policy file		file1 [file2] ...	file1 [file2] ...	file1 [file2] ...			[object 1] [object 2] ...

TRIPWIRE

TRIPWIRE 2.3 QUICK REFERENCE CARD

TRIPWIRE COMMAND LINE SYNTAX

```
Command      Mode Selector      Flag {Argument}   Flag {Argument} ...      File(s)
./tripwire    -m i               --polfile ../policy/mypolicy.pol
./tripwire    --check            -M --email-report-level 4 --rule-name “My Files”
./twadmin     --create-cfgfile   -S ../key/site.key -Q pA55w0rd           myconfig.txt
./twadmin     -m e               --verbose --site-keyfile ../key/site.key thisfile thatfile
```

Tripwire Inc.
326 SW Broadway, 3rd Floor
Portland, OR 97205
www.tripwire.org
opensource@tripwire.org

TRIPWIRE POLICY FILE REFERENCE

NORMAL RULES

Format: *objectname* -> *propertymask* ;
Example: /usr/bin/passwd -> +pinugts ;

STOP POINTS

Format: ! *objectname* ;
Example: ! /usr/bin/tmp ;

RULE ATTRIBUTES

Single Object Format:
objectname -> *propertymask* (*attribute* = *value*,...);
Example 1:
/usr/mail -> +pinug (rulename = “mail”,severity = 50);
Multiple Object Format 2:
(*attribute* = *value*, *attribute* = *value*)
{
 objectname -> *propertymask* ;
 objectname -> *propertymask* ;
}

Attribute	Description
rulename	Associates a name with a rule. Default value is the last element of the objectname.
severity	Associates a numeric severity level with a rule. Range is from 0 to 1,000,000. Default is 0.
emailto	Sends email notification of rule violations. See the Email Reporting section.
recurse	Controls recursion for directories. true (-1), false (0), and numeric values > 0 are valid.

DIRECTIVES

Format: @@*directive arguments*
Example: @@print “Scanning user directory”

Directive	Description
@@section	Designates a section of the policy file.
@@ifhost @@else @@endif	Allow conditional interpretation of the policy file.
@@print	Print a message to *stdout*.
@@error	Print a message to *stdout* and exit.
@@end	Marks the logical end-of-file.

PROPERTY MASKS

Property	Description
-	Ignore the following properties
+	Check the following properties
p	Permission and file mode bits
i	Inode number
n	Number of links
u	User id of owner
g	Group id of owner
t	File type
s	File size
d	ID of device on which inode resides
r	ID of device pointed to by inode (valid only for device objects)
l	Growing file
b	Number of blocks allocated
a	Access timestamp (Mutually exclusive with +CMSH)
m	Modification timestamp
c	Inode creation/modification timestamp
C	CRC-32 hash
M	MD5 hash
S	SHA hash
H	HAVAL hash

PREDEFINED VARIABLES

Variable	Description
ReadOnly	File is read only: +pinugtsdbmCM-rlacSH
Dynamic	File changes: +pinugtd-srlbamcCMSH
Growing	File can grow, but not shrink: +pinugtdl-srbamcCMSH
IgnoreAll	Ignore all attributes: -pinugtsdrlbamcCMSH
IgnoreNone	Ignore no attributes: +pinugtsdrbamcCMSH-l
Device	Device file: +pugsdr-intlbamcCMSH

EMAIL REPORTING

To use Tripwire email reporting correctly:

- The MAILMETHOD, MAILPROGRAM, SMPTHOST, and SMTPPORT variables in the Tripwire configuration file must be set correctly. Use the Test mode of the `tripwire` command to check the settings.
- The `emailto` rule attribute must be specified for at least one rule in the policy file.
- The `-M`, or `--email-report` flag, of the `tripwire` command must be used when the integrity check is run.

SAMPLE POLICY FILE

```
MYMASK = +pinugsa;                                    # Variable defined using property flags.
HIGH  = $(ReadOnly) + S;                              # Variable defined using predefined variable.
HIGHER = $(HIGH) + H;                                 # Variable defined using user-defined variable.

(emailto = "admin1@company.com;admin2@company.com")   # Sends email reports for violations of rules
{                                                     # within brackets (here, the whole policy file).

/usr/TSS -> $(IgnoreNone) -ar;                        # Scan all properties for the Tripwire directory
!/usr/TSS/man;                                        # but don’t scan the Tripwire man directory.

  (rulename = Projects, severity = 80)                # These only apply to the two rules in brackets.

  {
   /proj     -> $(MYMASK) -a +H;                      # Variable used with individual properties.
   /proj/bob -> $(HIGH)(emailto = bob@company.com);  # Bob gets email only if this rule is violated.
  }

@@error “DEBUG TEST MARKER 1; ANY ERRORS?”           # Use to debug policy file, then comment out.

  (rulename = "Home directories",
   recurse = false, severity = 50,                  # Admin3 will only get reports of violations
   emailto = admin3@company.com)                    # of the rules in brackets.
  {
    /home           -> $(ReadOnly);
    /usr/home/bob   -> $(HIGHER)(severity = 90);    # Severity for this rule will be 90, not 50.
  }

@@ifhost ruby || topaz
  /bin              -> $(HIGH);                     # These two rules will only be applied to
  /bin/special      -> $(HIGHER)(rulename = special); # the hosts ruby and topaz.

@@else
  @@ifhost agate
    /bin            -> $(HIGHER);

  @@else                                            # This rule will be applied to all hosts
    /bin            -> $(HIGH);                     # other than ruby, topaz, and agate.

  @@endif
@@endif                                             # End of conditional section of policy file.
}
```