

Tripwire Command Reference

| | | | 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 <i>database</i> | ● | ● | ● | ● | | | | | | | | | | | ● |
| | --report-file | -r <i>report</i> | | ● | ● | | | | | | | | | | | ● | |
| | --cfgfile | -c <i>cfgfile</i> | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | ● | | ● | ● |
| | --polfile | -p <i>polfile</i> | ● | ● | | ● | | | | ● | ● | | | | | | |
| | --visual | -V <i>editor</i> | | ● | ● | | | | | | | | | | | | |
| | --site-keyfile | -S <i>sitekey</i> | ● | ● | ● | ● | | ● | | ● | ● | ● | ● | ● | ● | | |
| | --local-keyfile | -L <i>localkey</i> | ● | ● | ● | ● | | | | | | | ● | ● | ● | ● | ● |
| 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 <i>output file</i> | | ● | | | | | | | | | | | | ● | ● |
| | --output-level | -t 0 1 2 | | | | | | | | | | | | | | | ● |
| | --output-format | -F classic html xml | | | | | | | | | | | | | | | |
| --base64 | -b | | ● | ● | | | | | | | | | | | ● | ● | |
| Scope of Operation | --rule-name | -R <i>rule</i> | | ● | ● | | | | | | | | | | | ● | |
| | --properties | -P <i>properties</i> | | | | | | | | | | | | | | ● | ● |
| | --severity | -l <i>level name</i> | | ● | | | | | | | | | | | | ● | |
| | --section | -x <i>section</i> | | ● | ● | | | | | | | | | | | ● | ● |
| | --ignore | -i <i>properties</i> | | ● | | | | | | | | | | | | | |
| Security Settings | --signed-report | -E | | ● | | | | | | | | | | | | | |
| | --secure-mode | -Z low high | | | ● | ● | | | | | | | | | | | |
| | --no-encryption | -e | ● | | | | | ● | | ● | | | | | | | |
| Unattended Operation | --accept-all | -a | | | ● | | | | | | | | | | | | |
| | --site-passphrase | -Q <i>passphrase</i> | | | | ● | | ● | | | ● | ● | | ● | | | |
| | --local-passphrase | -P <i>passphrase</i> | ● | ● | ● | ● | | | | | ● | ● | | ● | | | |
| Testing | --email | -e <i>address</i> | | | | | ● | | | | | | | | | ● | |
| | --snmp | -N | | | | | ● | | | | | | | | | | |
| | --syslog | -l | | | | | ● | | | | | | | | | | |
| | --execute | -X <i>object</i> | | | | | ● | | | | | | | | | | |
| 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 for Servers for UNIX

Quick Reference Card

Tripwire, Inc.
326 SW Broadway
3rd Floor
Portland, OR 97205
tel: 800.TRIPWIRE (toll free)
fax: 503.223.0182

Tripwire Policy File Reference

NORMAL RULES

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

STOP POINTS

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

RULE ATTRIBUTES

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

(attribute = value, attribute = value)
{
  object -> property ;
  object -> property ;
}
```

| Attribute | Description |
|-------------|--|
| rulename | Associates a name with a rule. Default value is the last element of the object name. |
| severity | Associates a numeric severity level with a rule. Range is from 0 to 1,000,000. Default is 0. |
| 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. |

DIRECTIVES

```
@@directive arguments
@@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 <i>stdout</i> . |
| @@error | Print a message to <i>stdout</i> and exit. |
| @@end | Marks the logical end-of-file. |

PROPERTIES

| 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-srlbamCMSH |
| Growing | File can grow, but not shrink: +pinugtdl-srbamCMSH |
| IgnoreAll | Ignore all attributes: -pinugtsdrlbamCMSH |
| IgnoreNone | Ignore no attributes: +pinugtsdrbamCMSH-I |
| Device | Device file: +pugsdr-intlbamCMSH |

EMAIL REPORTING

To use email reporting correctly, you must:

- set the MAILMETHOD, MAILPROGRAM, SMTPHOST, and SMTPPORT parameters in the configuration file correctly. You can test these settings with the Test mode of the tripwire command.
- specify recipients using the emailto rule attribute in the policy file, or the GLOBALEMAIL configuration file parameter
- use the -M or --email-report option of the tripwire command when you run an integrity check

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/local/tripwire -> $(IgnoreNone) -ar; # Scan all properties for the Tripwire directory
  !/usr/local/tripwire/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", # Admin3 will only get reports of violations
recurse = false, severity = 50, # of the rules in brackets.
emailto = admin3@company.com)
{
  /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.
}
@@end
```

© 2002 Tripwire, Inc. Tripwire is a registered trademark of Tripwire, Inc. All rights reserved.