

Tripwire for Servers / Open Platform for Security (OPSEC)TM Integration Instructions

This paper describes the procedure for integrating Tripwire for Servers 2.4.2 and Check PointTM security software. This procedure describes integration with the NG version of the Check Point Management Console, used to manage Check Point VPN-1TM and FireWall-1[®] software.

The `tw2chkpt` application uses the `tripwire` and `twprint` executables to generate and send the results of Tripwire integrity checks to Check Point software using the ELA interface. The information is in the form of a one-line report (a Tripwire for Servers “level 0” report), which describes the number and type of violations, and the severity of violations found.

Requirements/Cautions

Tripwire for Servers / Check Point integration requires:

- Tripwire for Servers version 2.4.2 on Windows NT and 2000 and Solaris 7 and 8 **ONLY**
- NG version of the Check Point Management Console

For Windows systems, Tripwire integrity checks initiating from Tripwire Manager **WILL NOT** be logged to Check Point software. Integrity checks that initiate from Tripwire for Servers will be logged.

For Solaris systems, if you want to use Tripwire Manager with Checkpoint software, you must edit the agent configuration file on each Tripwire for Servers machine. See the final section of this document for more information.

Install OPSEC Integration Components

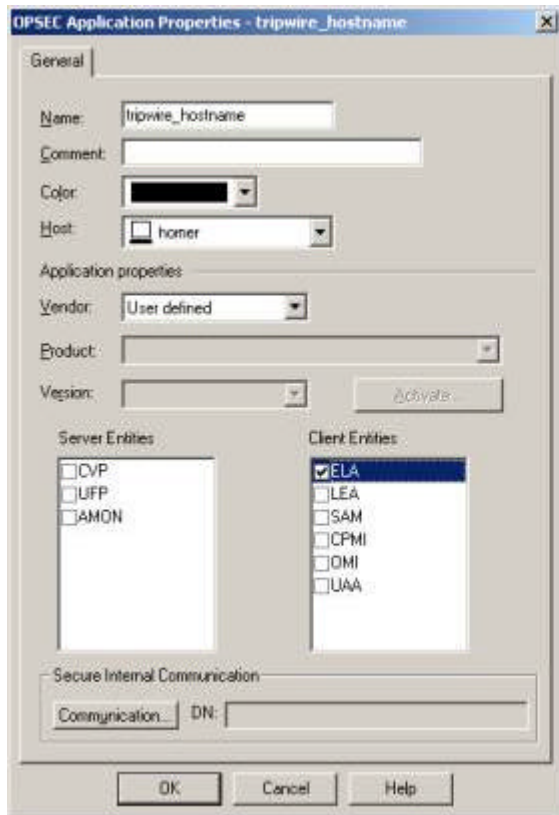
1. Download the Tripwire/OPSEC archive from the Tripwire website, and extract the following files to your Tripwire for Servers bin directory:
 - `opsec_pull_cert` (.exe on Windows)
 - `tw2chkpt` (.exe on Windows)
 - `tw2chkpt.cfg`

Configure OPSEC Manager and Tripwire OPSEC Configuration File

Configure OPSEC Manager in Check Point NG

2. In the Check Point Policy Editor, select Manage > Network Objects.
3. Click New, then select Workstation.
4. Enter the hostname of the machine where you installed Tripwire for Servers (the Tripwire host machine) for Name, click Get Address to get the IP address for the machine, then click OK.

5. Select Manage > OPSEC Applications, then click New and select OPSEC Application.
6. Enter the following information:
 - Name: `tripwire_hostname` (from step 4)
 - Host: select the Tripwire host machine (from step 4)
 - Client Entries: check ELA



7. Click Communication, enter and confirm a password, then click Initialize.
8. After initialization, click Close to close the Communication window, then click OK to close the application window.
9. Select Policy > Install, then click OK.

Create OPSEC Authentication Certificate

10. On the Tripwire client machine, navigate to the Tripwire bin directory.

UNIX:

```
cd /usr/local/tripwire/tfs/bin
```

Windows:

```
cd C:\Program Files\Tripwire\TFS\bin
```

11. Type this command to get an OPSEC authentication certificate:

```
opsec_pull_cert -h OPSEC_Manager_Machine -n tripwire_hostname -p password
```

12. When the certificate is successfully created, the full entity SIC name is listed. **Copy this name or write it down.**

Edit Tripwire Check Point Configuration File

13. In the Tripwire bin directory, open the configuration file `tw2chkpt.cfg` in a text editor. It should look like this:

```

C:\PROGRAM~1\Tripwire\TFS\Bin>type tw2chkpt.cfg
#####
# Example Configuration file for tw2chkpt. #
# #
# Make sure you edit this file and replace: #
# #
# TRIPWIRE_OPSEC_NAME #
# TRIPWIRE_INSTALL_DIR #
# SERVER_HOSTNAME #
# SERVER_SIC_NAME #
# #
#####

#-----
# This is the DN <SIC name> created for the OPSEC
# application when it was defined using
# the UPN-1/FireWall-1 Policy Editor:
#-----
opsec_sic_name "CN=TRIPWIRE_OPSEC_NAME,O=SERVER_SIC_NAME"

#-----
# Directory for OPSEC generated files
#-----
opsec_shared_local_path "TRIPWIRE_INSTALL_DIR/bin"

#-----
# This is the name of the certificate file to be
# loaded by tw2chkpt. (Use the opsec_pull_cert tool
# to obtain this file)
#-----
opsec_sslca_file "TRIPWIRE_INSTALL_DIR/bin/opsec.p12"

#-----
# The Check Point management server we are connecting to.
#-----
ela_server auth_port 18187
ela_server auth_type sslca
ela_server host SERVER_HOSTNAME
# Or ela_server ip XXX.XXX.XXX.XXX
ela_server opsec_entity_sic_name "CN=cp_mgmt,O=SERVER_SIC_NAME"
C:\PROGRAM~1\Tripwire\TFS\Bin>_
  
```

14. Change the following values in the configuration file. Be sure to double-quote all values.

Configuration File Variable	Value
opsec_sic_name	SIC name from step 12
opsec_shared_local_path	path to the Tripwire for Servers bin directory
opsec_sslca_file	path to the file in the Tripwire for Servers bin directory
ela_server opsec_entity_sic_name	"CN=cp_mgmt,O=(from SIC in step 12)"
ela_server_host	hostname of the machine where Check Point Manager server is installed
ela_server ip	(optional) Use this instead of ela_server_host
ela_server auth_port	18187 (by default)*
ela_server auth_type	sslca (by default)*

*Refer to the OPSEC API Specification document for information on alternate methods of client-server authentication and encryption.

15. Save and close the configuration file.

Run Integrity Checks

Now that you have installed, configured, and connected the Tripwire and Check Point software, the results of integrity checks can be logged to the Check Point Log Viewer.

When you want Tripwire for Servers to log the results of an integrity check to Check Point software, use the `tw2chkpt` executable when running and scheduling integrity checks instead of the `tripwire` executable.

The `tw2chkpt` executable accepts the same command-line parameters that the `tripwire` executable accepts in integrity check mode. You **must** use the report file (`-r`) command-line parameter with a report file name (e.g. `-r checkpoint.twr`) if you want to log reports to Check Point software. For example:

```
tw2chkpt -m c -r checkpoint.twr
```

Using Tripwire Manager with Check Point Software (Solaris 7 & 8 Only)

You can use Tripwire Manager to manage Tripwire for Servers on Solaris machines and log the results of integrity checks to Check Point software. To do this, you need to edit the agent configuration file on each Tripwire for Servers machine.

1. Install and configure the Check Point integration components on each Tripwire for Servers machine, as described above.
2. Find and stop the `twagent` process.
3. Print a plain text version of the Agent configuration file.

```
twagent --print-cfgfile > agentcfg.txt
```

4. Change the value of the `TRIPWIRE` setting to the path to the `tw2chkpt` executable, and save the file. For example:

```
TRIPWIRE=/usr/local/tripwire/tfs/bin/tripwire.exe
```

becomes

```
TRIPWIRE=/usr/local/tripwire/tfs/bin/tw2chkpt.exe
```

5. Encode and sign the text file to install it as the new agent configuration file.

```
twagent --create-cfgfile --site-keyfile ../key/site.key agentcfg.txt
```

6. Start the `twagent` daemon.

```
twagent --start
```

This procedure DOES NOT work with Windows versions of Tripwire Manager.