McAfee Host IPS 8.0 ClientControl.exe Utility

This command line utility helps automate upgrades and other maintenance tasks when third-party software is used to deploy Host Intrusion Prevention on client computers.

NOTE: The utility is installed as part of Host IPS 8.0 and is no longer a separate download.

Function and Setup

This utility allows administrators to perform the following on the McAfee Host IPS client:

- Start the HIPS service.
- Stop the HIPS service (requires administrator or time-based password). See **Stopping Host IPS services**, below.
- Change log settings (requires administrator or time-based password).
- Start/stop the HIPS engines (requires administrator or time-based password).
- Export the activity log to a formatted text file.
- Export the HIPS policy to a text file
- Reset the HIPS configuration to default. (requires administrator or time-based password).
- Display the NaiLite license data residing in the registry on the client computer.
- Export the IPS boot-time policy to a text file.
- Display application information (i.e. path, signer, fingerprint, and description) for an arbitrary application.
- Enable/Disable FireCore's (NDIS) pass-through mode on/off.

The utility records its activities to **ClientControl.log** at:
C:\Documents and Settings\All Users\Application Data\McAfee\Host Intrusion Prevention. (Windows platforms other than Vista)
C:\ProgramData\McAfee\Host Intrusion Prevention. (Windows Vista platforms)

Stopping Host IPS services

1. The **/stop** parameter stops Host IPS services if the user has administrative authority to stop services. If the user has authority to stop services on the computer, the following will occur:
    a. Host IPS services are turned off. The **Host IPS** checkbox on the IPS Policy tab is automatically deselected.
    b. Host IPS services are not stopped. An entry is made in **ClientControl.log**.
    c. The ePO agent enforces policies at next policy enforcement interval.

    Important: If the ePO agent enforces policies while you are engaged in an activity that requires that protection be disabled (e.g. patching Windows), your activity may be blocked by the enforced policies.
2. Even if stopping Host IPS services is successful, policy settings may allow the ePO agent to restart them at the next Agent-Server Communication Interval (ASCI). To prevent this:

a. In ePO, open the Host Intrusion Prevention: General policy.
b. Select the **Advanced** tab.
c. Deselect **Perform product integrity check**.
d. Run an agent wake-up call.

Command Line Syntax

Conventions:

- [] means **required**.
- [xxx, ...] means **one or more**.
- <> means **user-entered data**.

Major arguments:

Only one of the following *major* arguments is allowed per invocation:

- /help
- /start
- /stop
- /log
- /engine
- /export

However, you can specify more than one log option when changing log settings.
Running the utility with the **/help** command provides the most up-to-date help information and notes.

Usage:

```
clientcontrol [arg]
```

Argument Definitions:

- `/help` – Displays command-line syntax and notes.
- `/start`
- `/stop <password>`
- `/log <password> [log type] [log option, ...]` – Log options are processed in order.
- `/engine <password> [engine type] [engine option]`
- `/export <path of export file>`
- `/readNaiLic`
- `/exportConfig <path of export file> <option>`
- `/defConfig <password>`
- `/startupIPSProtection <path of export file>`
- `/execInfo <path of executable file>`
- `/fwPassthru <password> <option>`

Log type definitions:

- 0 = HIPS (i.e. HipShield.log)
- 1 = Firewall (i.e. FireSvc.log)

Log option definitions:

- 0 = off
- 1 = all
- 2 = info
- 3 = warning
- 4 = error
- 5 = verbose (6.X Firewall only) / debug (7.X Firewall only).
- 6 = debug (IPS only)
- 7 = security violation (IPS only)

Engine type definitions:

- 0 = all
- 1 = Buffer Overflow
- 2 = Logon (6.X only)
- 3 = Sql (server only)
- 4 = Registry
- 5 = Services
- 6 = Files
- 7 = Http (server only)
- 8 = HIP API
- 9 = Get Admin
- 10 = Illegal Use
- 11 = Program

Engine option definitions:

- 0 = off
- 1 = on

Sample Workflows

Applying a patch to a computer protected by McAfee Host IPS

1. Open a command shell.
2. Run `clientcontrol.exe /stop <password>`
3. Perform your maintenance activity.
4. Run `clientcontrol.exe /start` (to restart Host IPS services).

Exporting the Host IPS Activity Log to a text file.

1. Open a command shell.
2. Run `clientcontrol.exe /export <path of export file>`
3. Copy the exported log file to another computer for collection, analysis, etc.

Turn on logging as part of a troubleshooting exercise

1. Open a command shell
2. Run `clientcontrol.exe /log <password>` [log type] [log option, ...]
3. Perform activity to generate log entries.
4. Review HipShield.log or FireSvc.log for relevant information.

Turning off specific Host IPS engines as part of a troubleshooting exercise

1. Open a command shell
2. Run `clientcontrol.exe /<password>` [engine type] [engine option]
3. Perform activity to generate reactions and log entries.
4. Review HipShield.log or FireSvc.log for relevant information.