# How to use windows - security level profiles in Endpoint Manager

Endpoint Manager new profiles are optimized for security and usability. The profiles are based on three levels of security as follows:

- 'Windows Security Level 1 Profile' (replaces 'Optimum Windows Profile')
- 'Windows Security Level 1 Profile [Former Standard Profile]' (replaces 'Standard Windows' profile)
- 'Windows Security Level 2 Profile' (replaces 'Hardened Windows Profile')
- 'Windows Security Level 3 Profile' (new profile max. security)

Step [1] : To view the profiles go to "Endpoint Manager"  $\rightarrow$  "CONFIGURATION TEMPLATES"  $\rightarrow$  "Profiles".

• More details on each profile are under the next screenshot.

Endpoint Manager	■ Profiles			<b>ē</b> ② ≗
DASHBOARD >				
DEVICES >	Profiles Default Profiles			
Susers >	Ê Ê Ê Ê Ê			
CONFIGURATION TEMPLATES	Create Import Export Profile Clone Profile Delete Profile Export			
Profiles Alerts	OS NAME	CREATED BY	CREATED -	UPDATED AT
Procedures	Windows - Security Level 1 Profile for ITSM 6.20	admin	2016/08/30 09:00:59 PM	Not updated
APPLICATION STORE >	Windows - Security Level 1 Profile [Former Standard Profile] 6.20	admin	2015/12/26 07:55:29 AM	Not updated
APPLICATIONS >	Windows - Security Level 2 Profile for ITSM 6.20	admin	2015/11/16 01:17:43 PM	Not updated
SECURITY SUB-SYSTEMS	Windows - Security Level 3 Profile for ITSM 6.20	admin	2015/11/16 11:18:45 AM	Not updated
<pre>\$\$\$ SETTINGS &gt;</pre>	Results per page: 20 ¥			Dis

### Windows - Security Level 1

- Replaces 'Optimum Windows Profile' with the following addition:
  - HIPS is enabled with 'Safe Mode' + 'Allow Request active
- This is now the default profile unless you designate a new default

### Windows – Security Level 2

- Replaces 'Hardened Windows Profile' with the following additions:
  - HIPS is enabled with 'Safe Mode' + 'Block Request active
  - Auto-containment is active with logging enabled

#### Windows - Security Level 3

- · New profile featuring highest security settings
- Same as 'Windows Security Level 2' with the following additions:
  - Antivirus settings 'Use Cloud While Scanning' is enabled by default in 'Full Scan'. The cloud database is the most up-to-date version of the virus database, so antivirus scans are more accurate. It also means CCS is capable of detecting zero-day malware even if the local database is out-of-date.

• HIPS settings – all interpreters are enabled under 'Heuristic Command Line Analysis' and 'Embedded code detection:

ndpoint Manager	Profiles / <u>Mindows - Security Level 3 Profile for ITSM 6.20</u> / HIPS					🄄 🕜 🛓
DASHBOARD >	Windows - Security Level 3 Profile for ITSM 6.20	HIPS Command-Line Analysis $\qquad \qquad \qquad$				
USERS	'이 바랍 바랍 바랍 바중 바중 Add Profile Expant Profile Class Profile Deless Profile Nake Default	Select the applications for which you would like HIPS to detect embedded script and perform heuristic analysis.				
	Add Prome Export Prome Liente Prome Liente Prome Liente Prome Liente Prome Liente Prome Liente Prome	APPLICATION	HEURISTIC COMMAND-LINE ANALYSIS	EMBEDDED CODE DETECTION		
Profiles		*winhlp32.exe	ON	ON	1.0	
Alerts	General Monitoring Containment HIPS Antivirus File Rating Firewall VirusScope Valkyrie UI Settin	*\WScript.exe	ON	ON	1.0	es Miscellaneous
Procedures		*\cecript.exe	ON	ON	1.0	
Monitors	HIPS	*\mshta.exe	ON	ON	1.0	
APPLICATION STORE	HIPS Settings HIPS Rules Rulesets Protected Objects	*lparl.axe	ON	ON	1.0	
>		*\regedit.exe	ON	ON	1.0	
APPLICATIONS	Enable HIPS	*\scrond22.exe	ON	ON	1.0	
SECURITY SUB-SYSTEMS	Safe mode  V Monitoring settings	"\hh.exe	ON	ON	1.0	
SETTINGS	This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.	*ljava.exe	ON	ON	1.0	
	Do NOT show popup alerts     Block requests     V	"jianaw.eze	ON	ON	1.0	
	Set popup alerts to verbose mode	*\cmd exe	ON	ON	1.0	
	Create rules for safe applications	*\rundi/32.exe	UN	UN	× •	
	Set new on-screen alert timeout to     60     secs.	*/msiezec.eze	ON	ON	1.0	
	Enable adaptive mode under low system resources	*'uregsvr32.exe	UN	UN	1.1	
	Block unknown requests when the application is not running	"(prisershell ase	ON	ON	1.0	
	Enable enhanced protection mode (requires a system restart)     (19 6 CC5 101)     Enable embedded code detection and heuristic command-line analysis for     Certain applications	"\python.exe	UN	UN	× •	
	Limit the total size of saved detected scripts to 100 KB	*\pythonw.exe	ON	ON	1.0	
	When reaching the set limit, the older records will be deleted to free up space.	*\sutoit3.exe	ON	ON	1.0	
	Detect shellcode injections     Exclusions	*\autoit3 x64.exe	ON	ON	× *	
					OK	

## Windows – Security Level 1 [Former Standard Profile]

- Replaces 'Windows Standard' profile.
- Implements the same security settings as mentioned in 'Windows Security Level 1'