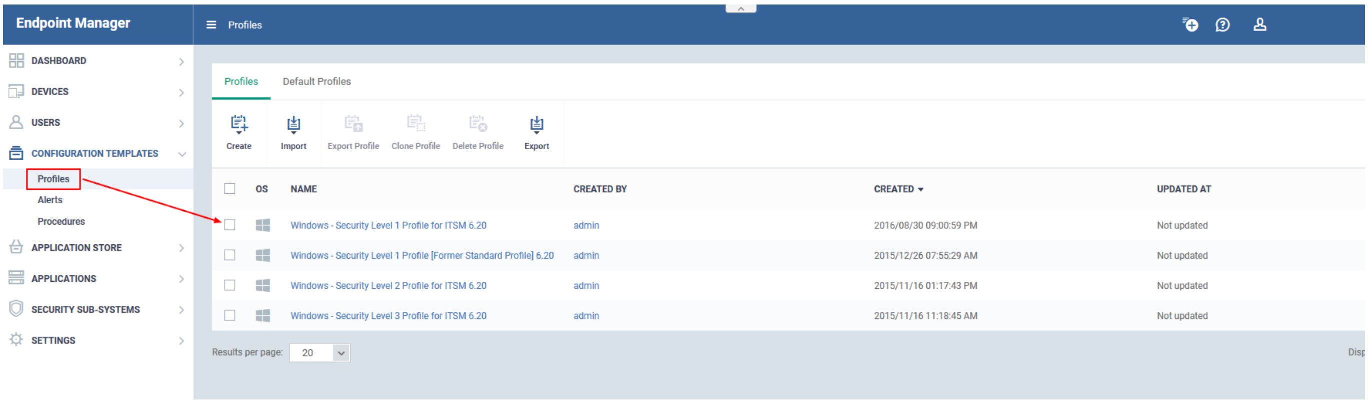
Endpoint Manager new profiles are optimized for security and usability. The profiles are based on three levels of security as follows:

- ‘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"→ "CONFIGURATION TEMPLATES"→ "Profiles".

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



☐	OS	NAME	CREATED BY	CREATED ▾	UPDATED AT
☐		Windows - Security Level 1 Profile for ITSM 6.20	admin	2016/08/30 09:00:59 PM	Not updated
☐		Windows - Security Level 1 Profile [Former Standard Profile] 6.20	admin	2015/12/26 07:55:29 AM	Not updated
☐		Windows - Security Level 2 Profile for ITSM 6.20	admin	2015/11/16 01:17:43 PM	Not updated
☐		Windows - Security Level 3 Profile for ITSM 6.20	admin	2015/11/16 11:18:45 AM	Not updated

Windows - Security Level 1

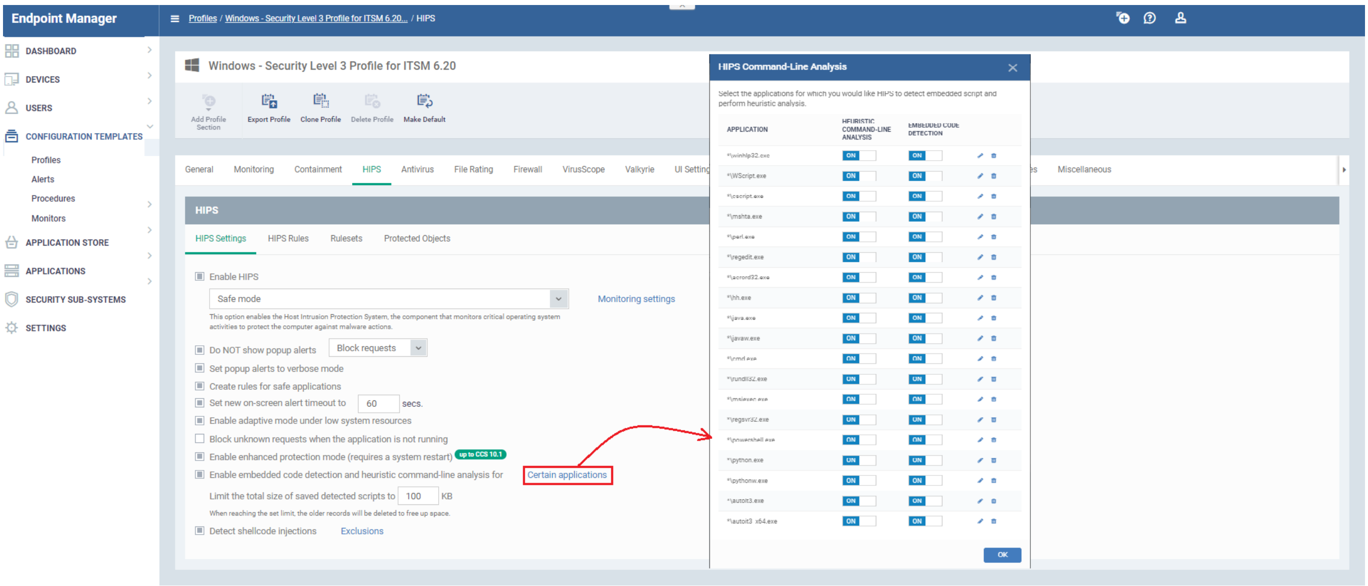
- Replaces ‘Optimum Windows Profile’ with the following addition:
    - HIPS is enabled with ‘Safe Mode’ + ‘Allow Request active
- This is now the default profile unless you designate a new default

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 It also means CCS is capable of detecting zero-day malware even if the local database is out-of-date.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:



☑ Enable HIPS

Safe mode

This option enables the Host Intrusion Protection System, the component that monitors critical operating system activities to protect the computer against malware actions.

Monitoring settings

☑ Do NOT show popup alerts: Block requests

☑ Set popup alerts to verbose mode

☑ Create rules for safe applications

☑ Set new on-screen alert timeout to 60 secs.

☑ Enable adaptive mode under low system resources

□ Block unknown requests when the application is not running

☑ Enable enhanced protection mode (requires a system restart) up to CCS 10.1

☑ Enable embedded code detection and heuristic command-line analysis for Certain applications

Limit the total size of saved detected scripts to 100 KB

When reaching the set limit, the older records will be deleted to free up space.

☑ Detect shellcode injections Exclusions

HIPS Command-Line Analysis

Select the applications for which you would like HIPS to detect embedded script and perform heuristic analysis.

APPLICATION	HEURISTIC COMMAND-LINE ANALYSIS	EMBEDDED CODE DETECTION
*\winhlp32.exe	ON	ON
*\WScript.exe	ON	ON
*\cscript.exe	ON	ON
*\mshta.exe	ON	ON
*\perl.exe	ON	ON
*\regedit.exe	ON	ON
*\acrord32.exe	ON	ON
*\hh.exe	ON	ON
*\java.exe	ON	ON
*\javaw.exe	ON	ON
*\cmd.exe	ON	ON
*\rundll32.exe	ON	ON
*\msiexec.exe	ON	ON
*\regsvr32.exe	ON	ON
*\powershell.exe	ON	ON
*\python.exe	ON	ON
*\pythonw.exe	ON	ON
*\autoit3.exe	ON	ON
*\autoit3_x64.exe	ON	ON

Windows – Security Level 1 [Former Standard Profile]

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