**Security baseline (FINAL) for Chromium-based Microsoft Edge, version 80**

Microsoft is pleased to announce the enterprise-ready release of the recommended security configuration baseline settings for the next version of Microsoft Edge based on Chromium, version 80. The settings recommended in this baseline are identical to the ones we recommended in the version 79, with one new setting that we have added and that we will discuss below. We continue to welcome feedback through the [Baselines Discussion site](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/bd-p/Security-Baselines).

The baseline package is now available as part of the [Security Compliance Toolkit](https://www.microsoft.com/download/details.aspx?id=55319). Like all our baseline packages, the downloadable baseline package includes importable GPOs, a script to apply the GPOs to local policy, a script to import the GPOs into Active Directory Group Policy, and all the recommended settings in spreadsheet form, as Policy Analyzer rules, and as GP Reports.

Version 80 of the Chromium-based version of Microsoft Edge has 270 enforceable Computer Configuration policy settings and another 254 User Configuration policy settings. Following our streamlined approach, our recommended baseline configures a grand total of *twelve* Group Policy settings. You can find full documentation in the download package’s Documentation subdirectory.

The one addition to this baseline since version 79 is that we have added the recommendation to enforce a new setting “Configure Microsoft Defender SmartScreen to block potentially unwanted apps”. Potentially Unwanted Apps (PUA) was first introduced with our Microsoft Defender Antivirus (MDAV) baseline as part of Windows 10. PUA are not considered viruses, malware, or other types of threats, but they might perform actions on endpoints which adversely affect endpoint performance or use (such as adware or other low-reputation applications, you can see more PUA criteria [here](https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/criteria#potentially-unwanted-application-pua)). Starting with Microsoft Edge 80, you can now block PUA downloads and associated resource URLs. By default, PUA is an opt-in setting, meaning a user must deliberately configure this. Well-managed enterprises should ensure positive control of necessary security settings, and therefore we have enabled this setting as part of the baseline (as we have with the MDAV recommendation).