Security baseline (FINAL) for Windows 10 v1809 and Windows Server 2019

Microsoft is pleased to announce the *final* release of the security configuration baseline settings for Windows 10 October 2018 Update (a.k.a., version 1809, “Redstone 5” or “RS5”), and for Windows Server 2019.

Download the content here: link

The downloadable attachment to this blog post includes importable GPOs, a PowerShell script for applying the GPOs to local policy, custom ADMX files for Group Policy settings, documentation in spreadsheet form and as a set of Policy Analyzer files. In this release, we have changed the documentation layout in a few ways:

* *MS Security Baseline Windows 10 v1809 and Server 2019.xlsx* – multi-tabbed workbook listing all Group Policy settings that ship in-box with Windows 10 v1809 or Windows Server 2019. Columns for “Windows 10 v1809,” “WS2019 Member Server,” and “WS2019 DC” show the recommended settings for those three scenarios. A small number of cells are color-coded to indicate that the settings should not be applied to systems that are not joined to an Active Directory domain. Cells in the “WS2019 DC” columns are also highlighted when they differ from the corresponding cells in the “WS2019 Member Server” column. Another change from past spreadsheets is that we have combined tabs that used to be separate. Specifically, we are no longer breaking out Internet Explorer and Windows Defender AV settings into separate tabs, nor the settings for LAPS, MS Security Guide, and MSS (Legacy). All these settings are now in the Computer and User tabs.
* A set of Policy Analyzer files:
  + *MSFT-Win10-v1809-RS5-WS2019-FINAL.PolicyRules* – a Policy Analyzer file representing all the GPOs in the combined Windows 10 and Server 2019 baselines.
  + *MSFT-Win10-v1809-RS5-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows 10 v1809.
  + *MSFT-WS2019-MemberServer-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows Server 2019, Member Server.
  + *MSFT-WS2019-DomainController-FINAL.PolicyRules* – a Policy Analyzer file representing the GPOs intended to be applied to Windows Server 2019, Domain Controller.
* *BaselineDiffs-to-v1809-RS5-FINAL.xlsx* – This Policy Analyzer-generated workbook lists the differences in Microsoft security configuration baselines between the new baselines and the corresponding previous baselines. The Windows 10 v1809 settings are compared against those for Windows 10 v1803, and the Windows Server 2019 baselines are compared against those for Windows Server 2016.
* *Windows 10 1803 to 1809 New Settings.xlsx* – Lists all the settings that are available in Windows 10 v1809 that were added since Windows 10 v1803. (We used to highlight these settings in the big all-settings spreadsheets.)
* *Server 2016 to 2019 New Settings.xlsx* – Lists all the settings that are available in Windows Server 2019 that were added since Windows Server 2016. (We used to highlight these settings in the big all-settings spreadsheets.)

Highlights of the differences from past baselines, which are listed in BaselineDiffs-to-v1809-RS5-FINAL.xlsx:

* Added two new Attack Surface Reduction rules in Windows Defender Exploit Guard: “Block Office communication applications from creating child processes” (which includes Outlook), and “Block Adobe Reader from creating child processes.” Note that these were added since the draft release of these baselines.
* Since the draft baseline, we removed the “Turn off printing over HTTP” setting in “Computer Configuration\Administrative Templates\System\Internet Communication Management\Internet Communication settings.” This setting had been in our baselines at least as far back as Windows XP because of the mistaken belief that it distinguished between HTTP and HTTPS. Enabling this setting also disables printing over HTTPS, which breaks legitimate and necessary functionality for no security benefit.
* The MS Security Guide custom setting protecting against potentially unwanted applications (PUA) has been deprecated, and is now implemented with a new setting under Computer Configuration\...\Windows Defender Antivirus.
* We have enabled the “Encryption Oracle Remediation” setting we [had considered for v1803](https://blogs.technet.microsoft.com/secguide/2018/04/30/security-baseline-for-windows-10-april-2018-update-v1803-final/). At the time we were concerned that enabling the newly-introduced setting would break too many not-yet-patched systems. We assume that systems have since been brought up to date. (You can read information about the setting [here](https://support.microsoft.com/help/4093492) and [here](https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0886).)
* Changes to Virtualization-Based Security settings (used by Credential Guard and Code Integrity):
  + “Platform Security Level” changed from “Secure Boot and DMA Protection” to “Secure Boot.” If system hardware doesn’t support DMA protection, selecting “Secure Boot and DMA Protection” prevents Credential Guard from operating. If you can affirm that your systems support the DMA protection feature, choose the stronger option. We have opted for “Secure Boot” (only) in the baseline to reduce the likelihood that Credential Guard fails to run.
  + Enabled the new System Guard Secure Launch setting which will enable Secure Launch on new capable hardware. Secure Launch changes the way windows boots to use Intel Trusted Execution Technology (TXT) and Runtime BIOS Resilience features to prevent firmware exploits from being able to impact the security of the Windows Virtualization Based Security environment.
  + *Disabled* the “Require UEFI Memory Attributes Table” option. This is a change from the draft release, and is intended to increase compatibility.
  + Removed Credential Guard from the Domain Controller baseline, while retaining the rest of the VBS settings. This is implemented in a new DC-only GPO named “MSFT Windows Server 2019 - Domain Controller Virtualization Based Security.” Note that this is a change from the draft baseline in which we had removed all VBS settings from the DC baseline. (Credential Guard is not useful on domain controllers and is not supported there.)
* Enabled the new Kernel DMA Protection feature described [here](https://docs.microsoft.com/windows/security/information-protection/kernel-dma-protection-for-thunderbolt). The “External device enumeration” policy controls whether to enumerate external devices that are not compatible with DMA-remapping. Devices that are compatible with DMA-remapping are always enumerated.
* Removed the BitLocker setting, “Allow Secure Boot for integrity validation,” as it merely enforced a default that was unlikely to be modified even by a misguided administrator.
* Removed the BitLocker setting, “Configure minimum PIN length for startup,” as new hardware features reduce the need for a startup PIN, and the setting increased Windows’ minimum by only one character.
* Since the draft release, we removed “Prevent users from modifying settings” from “Computer Configuration\Administrative Templates\Windows Components\Windows Security\App and browser protection,” as it merely enforced a default that non-admins could not override.
* Enabled the new Microsoft Edge setting to prevent users from bypassing certificate error messages, bringing Edge in line with a similar setting for Internet Explorer.
* Removed the block against handling PKU2U authentication requests, as the feature is increasingly necessary.
* Removed the configuration of the “Create symbolic links” user rights assignment, as it merely enforced a default, was unlikely to be modified by a misguided administrator or for malicious purposes, and needs to be changed to a different value when Hyper-V is enabled.
* Removed the deny-logon restrictions against the Guests group as unnecessary: by default, the Guest account is the only member of the Guests group, and the Guest account is disabled. Only an administrator can enable the Guest account or add members to the Guests group.
* Removed the disabling of the xbgm (“Xbox Game Monitoring”) service, as it is not present in Windows 10 v1809. (By the way, consumer services such as the Xbox services have been removed from Windows Server 2019 with Desktop Experience!)
* Created and enabled a new custom MS Security Guide setting for the domain controller baseline, “Extended Protection for LDAP Authentication (Domain Controllers only),” which configures the LdapEnforceChannelBinding registry value described [here](https://support.microsoft.com/help/4034879).
* The Server 2019 baselines pick up all the changes accumulated in the four Windows 10 releases since Windows Server 2016.

We received and have been evaluating recommendations for more extensive changes to the baselines that we are continuing to evaluate for future releases.

We have replaced the collection of .cmd batch files for applying the baselines to local policy with a single PowerShell script that takes one of these five command-line switches to indicate which baseline you want to apply:

.\BaselineLocalInstall.ps1 -Win10DomainJoined - for Windows 10 v1809, domain-joined

.\BaselineLocalInstall.ps1 -Win10NonDomainJoined - for Windows 10 v1809, non-domain-joined

.\BaselineLocalInstall.ps1 -WS2019Member - for Windows Server 2019, domain-joined

.\BaselineLocalInstall.ps1 -WS2019NonDomainJoined - for Windows Server 2019, non-domain-joined

.\BaselineLocalInstall.ps1 -WS2019DomainController - for Windows Server 2019, domain controller

A couple of important notes about using the BaselineLocalInstall.ps1 script:

* PowerShell execution policy must be configured to allow script execution. You can configure this with a command line such as the following:  
  Set-ExecutionPolicy RemoteSigned
* LGPO.exe must be in the Tools subdirectory or somewhere in the Path. LGPO.exe is part of the Security Compliance Toolkit and can be downloaded from this URL:  
  <https://www.microsoft.com/download/details.aspx?id=55319>

Windows 10 v1809 has greatly expanded its manageability using Mobile Device Management (MDM). The Intune team is preparing documentation about the Microsoft Windows MDM security baseline and how to use Intune to implement the baseline, and will publish it very soon. We will post information to this blog when that happens.