Security baseline (Final) for Windows 10 and Windows Server v2004

We are pleased to announce the *final* release of the security configuration baseline settings for Windows 10 and Windows Server version 2004.

Please download the content from the [Microsoft Security Compliance Toolkit](https://www.microsoft.com/download/details.aspx?id=55319), test the recommended configurations, and customize and implement as appropriate. If you have questions or issues, please let us know via the [Security Baseline Community](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/bd-p/Security-Baselines).

This Windows 10 feature update brings very few new policy settings, which we list in the accompanying documentation. Only one new policy meets the criteria for inclusion in the security baseline (described below), and we are removing one setting from the baseline. There are two additional policies we are not including in the baseline because of compatibility concerns, but which you may want to consider for your organization.

# LDAP Channel Binding Requirements: Policy added to baseline.

In the Windows Server version 1809 Domain Controller baseline we created and enabled a new custom MS Security Guide setting called Extended Protection for LDAP Authentication (Domain Controllers only) based on the values provided [here](https://support.microsoft.com/help/4034879). This setting is now provided as part of Windows and no longer requires a custom ADMX. An [announcement](https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV190023) was made in March of this year and now all supported Active Directory domain controllers can configure this policy. The value will remain the same in our baseline, but the setting has moved to the new location. We are deprecating our custom setting. The new setting location is: *Security Settings\Local Policies\Security Options\Domain controller: LDAP server channel binding token requirements*.

Note: this new policy requires the March 10, 2020 security update. (We assume that, as security conscious baselines users, you are patching!) Details of that patch are [here](https://support.microsoft.com/en-us/help/4520412/2020-ldap-channel-binding-and-ldap-signing-requirements-for-windows).

# Microsoft Defender Antivirus File Hash: Policy worth considering.

Microsoft Defender Antivirus continues to enable new features to better protect consumers and enterprises alike. As part of this journey Windows has a new setting to compute file hashes for every executable file that is scanned, if it wasn’t previously computed. You can find this new setting here: *Computer Configurations\Administrative Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature*.

You should consider using this feature to improve blocking for custom indicators in Microsoft Defender Advanced Threat Protection (MDATP). This new feature forces the engine to compute the full file hash for all executable files that are scanned. This can have a performance cost, which we minimize by only generating hashes on first sight. The scenarios where you may want to test more thoroughly for performance include devices where you frequently create new executable content (for example, developers) or where you install or update applications extremely frequently.

Because this setting is less helpful for customers who are not using MDATP, we have not added it to the baseline, but we felt it was potentially impactful enough to call out. If you chose to enable this setting, we recommend throttling the deployment to ensure you measure the impact on your users’ machines.

# Account Password Length: Policy worth considering.

In the Windows 10 1903 security baselines we [announced](https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-final-for-windows-10-v1903-and-windows-server/ba-p/701084) the removal of the account password expiration policy. We continue to invest in improving this experience. With Windows 10 2004, two new security settings have been added for password policies: *‘Minimum password length audit’* and ‘*Relax minimum password length limits’*. These new settings can be found under *Account Policies\Password Policy*.

Previously, you could not require passwords/phrases greater than 14 characters. Now you can! Being able to require a length of more than 14 characters (maximum of 128) can help better secure your environment until you can fully implement a multi-factor authentication strategy. Our vision remains unchanged in achieving a password-less future, but we also recognize that this takes time to fully implement across both your users and your existing applications and systems.

You should be cautious with this new setting because it can potentially cause compatibility issues with existing systems and processes. That’s why we introduced the ‘*Minimum password length audit’* setting, so you can see what will happen if you increase your password/phrase length. With auditing you can set your limit anywhere between 1 and 128. Three new events are also created as part of this setting and will be logged as new SAM events in the System event log: one event for awareness, one for configuration, and one for error.

This setting will not be added to the baseline as the minimum password length should be audited before broad enforcement due to the risk of application compatibility issues. However, we urge organizations to consider these two settings. Additional details about these new settings will be found [here](https://go.microsoft.com/fwlink/?LinkId=2097191), once the new article get published in the coming days.

(NOTE: As of the today the link is not yet live, we are actively working to ensure it gets posted soon!)

As a reminder, length alone is not always the best predictor of password strength, so we strongly recommend considering solutions such as the [on-premise Azure Active Directory Password Protection](https://docs.microsoft.com/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy) which does sub-string matching using a dictionary of known weak terms, and rejects passwords that don’t meet a certain score.

# Turn on Behavior Monitoring: Policy removed from baseline.

In keeping with our principals of criteria for baseline inclusion we have found that the following setting does not need to be enforced; there is no UI path to the setting, you must be a privileged account to make the change, lastly we do not feel a mis-informed Admin would change this setting. Based on these principals we are removing *Computer Configuration\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Real-time Protection\Turn on behavior monitoring*

# Tooling updates

Finally, we do have some enhancements for LGPO and Policy Analyzer coming very shortly after this release! We will go into more details on these enhancements in a future blog post!

# Baseline criteria

We follow a streamlined and efficient approach to baseline definition [when compared with the baselines we published before Windows 10](https://blogs.technet.microsoft.com/secguide/2015/11/18/changes-from-the-windows-8-1-baseline-to-the-windows-10-th11507-baseline/). The foundation of that approach is essentially:

* The baselines are designed for well-managed, security-conscious organizations in which standard end users do not have administrative rights.
* A baseline enforces a setting only if it mitigates a contemporary security threat *and* does not cause operational issues that are worse than the risks they mitigate.
* A baseline enforces a default only if it is otherwise likely to be set to an insecure state by an authorized user:
  + If a non-administrator can set an insecure state, enforce the default.
  + If setting an insecure state requires administrative rights, enforce the default only if it is *likely* that a misinformed administrator will otherwise choose poorly.

For further illustration, see the “Why aren’t we enforcing more defaults?” section in [this blog post](https://blogs.technet.microsoft.com/secguide/2015/11/18/changes-from-the-windows-8-1-baseline-to-the-windows-10-th11507-baseline/).

As always, please let us know your thoughts by commenting on this post.