Windows 11, version 23H2 security baseline

Microsoft is pleased to announce the release of the security baseline package for Windows 11, version 23H2!

Please download the content from the Microsoft Security Compliance Toolkit, test the recommended configurations, and customize / implement as appropriate.

This release includes several changes to further assist in the security of enterprise customers. Changes have been made to provide additional protections to the local admin account, Microsoft Defender Antivirus updates, and a new setting in response to an MSRC bulletin.

Re-introducing the Local Administrator Password Solution (LAPS)

LAPS is a feature that has been around for some time but was always a bolt-on solution. The legacy version of Microsoft LAPS has been deprecated as of October 23, 2023 as noted in our article on Microsoft LAPS deprecation. We have now moved the control for Windows LAPS natively inbox and its settings are located under Administrative Templates/System/LAPS. We have configured three settings:

- `Configure password backup directory` to a value of Enabled: Active Directory
- `Enable password backup for DSRM accounts` to a value of Enabled
- `Enable password encryption` to a value of Enabled

For the backup directory setting, we have selected the option to backup to Active Directory as the baselines are already targeted as such. For Microsoft Entra ID, the best selection will be the Azure Active Directory option which will be reflected in the Intune security baseline when it releases.

For additional details on Windows LAPS, see the Windows LAPS overview, the Windows LAPS skilling snack, and the recent announcement, Windows LAPS with Microsoft Entra ID now Generally Available.

X.509 Certificate Padding

A new custom setting has been added to the `SecGuide.admx/l`, `Enable Certificate Padding`. Certificate Padding was first introduced in 2013 and republished in January of 2022. This setting affects Portable Executables and should be tested before implementation to a more secure state. At this time, the security baseline does not intend to enforce stricter verification behaviors. For additional information on Certificate Padding, see CVE-2013-3900 - Security Update Guide - Microsoft - WinVerifyTrust Signature Validation Vulnerability.

Microsoft Defender Antivirus

With each release the security baseline a full settings review is completed, based on the latest review we are updating the recommended settings for Microsoft Defender Antivirus (MDAV) with the addition of ten settings. These settings are as follows:

- `Microsoft Defender Antivirus\Configure local administrator merge behavior for lists` - set to a value of Disabled
- `Microsoft Defender Antivirus\Control whether or not exclusions are visible to Local Admins` - set to a value of Enabled
- `Microsoft Defender Antivirus\Turn off routine remediation` - set to a value of Disabled
- `Microsoft Defender Antivirus\MAPS\Send file samples when further analysis is required` - set to a value of Enabled: Send all samples
- Added `Configure monitoring for incoming and outgoing file and program activity` - set to a value of Enabled: bi-directional
- Added `Monitor file and program activity on your computer` - set to a value of Enabled
- Added `Turn on process scanning whenever real-time protection` is enabled - set to a value of Enabled
- Added `Scan packed executables` - set to a value of Enabled

There is an additional setting located at `Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash computation feature` that should be configured to an enabled state as long as you have Microsoft Defender for Endpoint deployed as this setting is used in conjunction with File Hash Allow/Block.

Controlled folder access

Controlled folder access (CFA) is a very powerful feature to help protect data from nefarious activity like ransomware. `Configure Controlled folder access` is not configured in the baseline but it is highly encouraged for the organization to set it to Enabled: Audit Mode for a period of time, until enough logging has occurred to make informed decisions. From there organizations are encourage to fully configure CFA and move from Audit Mode to Block state. For additional information on CFA, see Enable controlled folder access.

Tamper protection

While you are enabling the Microsoft Security Baseline, a friendly reminder to make sure to enable Microsoft Defender for Endpoint tamper protection for an additional layer of protection against human-operated ransomware. Want to learn more? See Protect security settings with tamper protection.

Other changes

The MSS Legacy custom administrative template titles were changed to remove the recommendation from the actual setting name. Based on feedback this was causing confusion as the settings changed over time but the recommendation in the title was static. The legacy Microsoft LAPS admx/l have been removed due to its deprecation.

`Advanced Audit Policy\Audit Policies\Privilege Use\Audit Sensitive Privilege Use` is being changed to success only (removing failure) from the baseline as we are seeing an increase in noise coming from the failure option. There is low security value to keep both Success and Failure at this point.

Please let us know your thoughts by commenting on this post or through the [Security Baseline Community](#).