

Security baseline for Windows 10, version 21H2

We are pleased to announce the release of the Windows 10, version 21H2 security baseline package!

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

This Windows 10 feature update brings very few new policy settings. One setting has been added for this release for printer driver installation restrictions (which was also added to the Windows 11 release). Additionally, all Microsoft Edge Legacy settings have been removed.

Restrict Driver Installations

In July a [Knowledge Base article](#) and subsequent patch was released for CVE-2021-34527, more commonly known as “PrintNightmare”. We have added a new setting to the MS Security Guide (*Administrative Templates\Printers\Limits print driver installation to Administrators*) and enforced the enablement. Note this setting was previously a custom setting in SecGuide.admx/l and has since moved inbox.

Microsoft Edge Legacy

Microsoft Edge Legacy (EdgeHTML-based) reached end of support on March 9, 2021 and is not part of Windows 10 21H2. Therefore, the settings that supported it have been removed from the baseline. Going forward, please use the new Microsoft Edge (Chromium-based) baseline, which is on a separate release cadence and available as part of the [Microsoft Security Compliance Toolkit](#).

Tamper Protection

While you are enabling the Microsoft Security Baseline, make sure to enable Microsoft Defender for Endpoint's "[Tamper Protection](#)" to add a layer of protection against Human Operated Ransomware.

As a reminder, our security baselines for the endpoint also include [Microsoft 365 Apps for Enterprise](#), which we recently released, as well as [Microsoft Edge](#) and [Windows Update](#).

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