

We are pleased to announce the enterprise-ready release of the security baseline for Microsoft Edge version 128!

We have reviewed the settings in Microsoft Edge version 128 and updated our guidance with the addition of two settings and the removal of two settings. A new Microsoft Edge security baseline package was just released to the Download Center. You can download the new package from the [Security Compliance Toolkit](#).

Dynamic Code Settings (Added)

This setting is part of our long-term strategy to prevent potentially-risky third-party code from interacting with the browser process by enabling Arbitrary Code Guard. Any attempts from third-party software to inject into Edge after start-up will fail. Note: there could potentially be an application compatibility impact to this change for environments where 3rd-party code is used for accessibility or other purposes. It is recommended to test with a subset of users before broad deployment.

Enable Application Bound Encryption (Added)

InfoStealer attacks (ones that harvest sensitive data) are on the rise, this setting will pair the encryption from the local data storage directly to Microsoft Edge. By enforcing this setting, the enterprise protects against a malicious app trying to obtain the encryption keys.

The following settings have been removed due to deprecation:

Microsoft Edge\Enhance images enabled

Microsoft Edge\Force WebSQL to be enabled

Microsoft Edge version 128 introduces 7 new computer settings and 7 new user settings. We have included a spreadsheet listing the new settings in the release to make it easier for you to find them.

As a friendly reminder, all available settings for Microsoft Edge are documented [here](#), and all available settings for Microsoft Edge Update are documented [here](#).

Please continue to give us feedback through the [Security Baseline Community](#) or in comments on this post.