

# Security baseline for Microsoft 365 Apps for enterprise (v2306, June 2023)

Microsoft is pleased to announce the release of the recommended security configuration baseline settings for Microsoft 365 Apps for enterprise, version 2306. Please download the content from the [Microsoft Security Compliance Toolkit](#), test the recommended configurations, and implement as appropriate.

This baseline builds on the previous [Office baseline we released June 2022](#). The highlights of this baseline include:

- Added a new setting to Microsoft Publisher around blocking macros from the internet
- Added a new setting around Basic Authentication
- Added a block for Excel XLL add-ins
- Added a new encryption format for Information Rights Management

The recommended settings in this security baseline correspond with the administrative templates version 5391, released on 3/20/2023.

## Deployment options for the baseline

IT Admins can apply baseline settings in different ways. Depending on the method(s) chosen different registry keys will be written and they will be observed in order of precedence: Office cloud policies **will override** ADMX/Group Policies which **will override** end user settings in the Trust Center.

- **Cloud policies** may be deployed with the [Office cloud policy service](#) for policies in HKCU. Cloud policies apply to a user on any device accessing files in Office apps with their AAD account. In Office cloud policy service, you can create a filter for the Area column to display the current Security Baselines, and within each policy's context pane the recommended baseline setting is set by default. [Learn more about Office cloud policy service](#).
- **ADMX policies** may be deployed with [Microsoft Endpoint Manager](#) (MEM) for both HKCU and HKLM policies. These settings are written to the same place as Group Policy, but managed from the cloud in MEM. There are two methods to create and deploy policy configurations: [Administrative templates](#) or the [settings catalog](#).
- **Group Policy** may be deployed with on premise AD DS to deploy Group Policy Objects (GPO) to users and computers. The downloadable baseline package includes importable GPOs, a script to apply the GPOs to local policy, a script to import the GPOs into Active Directory Group Policy, updated custom administrative template (SecGuide.ADMX/L) file, all the recommended settings in spreadsheet form and a Policy Analyzer rules file.

## GPOs included in the baseline

Most organizations can implement the baseline's recommended settings without any problems. However, there are a few settings that will cause operational issues for some organizations. We've broken out related groups of such settings into their own GPOs to make it easier for organizations to add or remove these restrictions as a set. The local-policy script (Baseline-LocalInstall.ps1) offers command-line options to control whether these GPOs are installed.

"MSFT Microsoft 365 Apps v2306" GPO set includes "Computer" and "User" GPOs that represent the "core" settings that should be trouble free, and each of these potentially challenging GPOs:

- "DDE Block - User" is a User Configuration GPO that blocks using DDE to search for existing DDE server processes or to start new ones.
- "Legacy File Block - User" is a User Configuration GPO that prevents Office applications from opening or saving legacy file formats.

- "Legacy JScript Block - Computer" disables the legacy JScript execution for websites in the Internet Zone and Restricted Sites Zone.
- "Require Macro Signing - User" is a User Configuration GPO that disables unsigned macros in each of the Office applications.

#### **Allow Basic Authentication prompts from network proxies**

HTTP Basic Authentication is a non-secure authentication method that relies on sending the username and password to the server in plaintext (base64). When Basic Authentication is used over non-secure HTTP connections, the credentials can be trivially stolen by others on the network. The security baseline will now enforce a value of **Disabled** to ensure organizations maintain a level of security. Additional information on this change may be found [here](#).

#### **Block macros from running in Office files from the internet**

Microsoft Publisher now supports a configurable setting to block macros from running in Office files from the internet. To maintain consistency across applications the security baseline will enforce the default of **Enabled**.

#### **Encryption mode for Information Rights Management (IRM)**

Cryptography is an ever-changing space and it is now time to modernize these defaults used to protect data and improve the security posture for our customers. In preparation for the new default encryption mode, the security baseline is going to move early and will now enforce a value of **Enabled: Cipher Block Chaining (CBC)**. Additional information on this change may be found [here](#).

#### **Block Excel XLL Add-ins that come from an untrusted source**

Untrusted add-ins can lead to security risks. A new setting has been added to prevent the loading of untrusted XLL add-ins which will further protect enterprises from malware attempts. The security baseline will now enforce the default value of **Enabled: Block**. Additional information on this change may be found [here](#).

If you have questions or issues, please let us know via the [Security Baseline Community](#) or this post.