Microsoft is pleased to announce the *final* release of the recommended security configuration baseline settings for Microsoft Office 365 ProPlus, version 1908. Please evaluate this proposed baseline and send us your feedback through the [Baselines Discussion site](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/bd-p/Security-Baselines).

This baseline builds on the overhauled [Office baseline we released in early 2018](https://blogs.technet.microsoft.com/secguide/2018/02/13/security-baseline-for-office-2016-and-office-365-proplus-apps-final/). The highlights of this baseline include:

* Componentization of GPOs so that “challenging” settings can be added or removed as a unit.
* Comprehensive blocking of legacy file formats
* Blocking Excel from using Dynamic Data Exchange (DDE)

Also see the announcements at the end of this post regarding the new Security Policy Advisor and Office cloud policy services.

**Download the content from the** [**Security Compliance Toolkit**](https://www.microsoft.com/en-us/download/details.aspx?id=55319)**.**

The downloadable baseline package includes importable GPOs, a script to apply the GPOs to local policy, a custom administrative template (ADMX) file for Group Policy settings, all the recommended settings in spreadsheet form and as Policy Analyzer rules. The recommended settings correspond with the Office 365 ProPlus administrative templates version 4909 released on September 5, 2019 that can be downloaded [here](https://www.microsoft.com/en-us/download/details.aspx?id=49030).

**Componentization of GPOs**

Most organizations can implement most of the baseline’s recommended settings without any problems. However, there are a few settings that will cause operational issues for some organizations. We have 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, BaselineLocalInstall.ps1, offers command-line options to control whether these GPOs are installed.

The “MSFT Office 365 ProPlus 1907” GPO set includes “Computer” and “User” GPOs that represent the “core” settings that should be trouble free, and each of these potentially challenging GPOs, each of which is described later:

* “Legacy File Block – User” is a User Configuration GPO that prevents Office applications from opening or saving legacy file formats.
* “Require Macro Signing – User” is a User Configuration GPO that disables unsigned macros in each of the Office applications.
* “Excel DDE Block – User” is a User Configuration GPO that blocks Excel from using DDE to search for existing DDE server processes or to start new ones.

**Comprehensive blocking of legacy file formats**

In the previous Office baseline we published, we tried to end the use of legacy file formats, including all the old Office document formats such as \*.doc, \*.xls, and \*.ppt. However, we missed some important ones. So we just went ahead and fixed the glitch.

One of the threats of these old binary file formats is that their inherent complexity too often led to exploitable bugs in their parsers. The bigger threat is that many of these formats can include macros or other executable instructions that are easily abused. By contrast, macros are disabled with the most-commonly used Office Open XML (OOXML) document formats, which were first introduced with Office 2007. Only macro-enabled formats such as \*.docm and \*.xlsm support macros, and these can be filtered at the point of ingress.

While fixing the glitch, however, we also recognized that many organizations cannot entirely end their use of legacy Office document formats, so we broke out the file-blocking settings into a separate GPO, so they can be added or removed as a cohesive unit.

**Blocking Excel from using DDE**

Dynamic Data Exchange (DDE) is a *very* old interprocess communication method that is still used in some parts of Windows and remains supported for applications to use, primarily for backward compatibility. A few years ago, malware authors began embedding specially-formed DDE references in Office documents that were sent to victims and that would run attacker-chosen code. Since then, most Office apps have disabled the use of DDE. Excel by default blocks the ability to launch arbitrary DDE servers and now also supports user-configurable settings to enable DDE server process lookup and launch. These can now be configured through Group Policy, and this baseline recommends disabling both settings. Because of the likelihood that some organizations still depend on this functionality, we have broken out “Excel DDE Block” as a separate GPO.

**Macro signing**

The baseline also retains the “VBA Macro Notification Settings” options from our previous baselines that require that macros embedded in Office documents be signed by a trusted publisher. We recognize that some organizations have had workflows and processes relying on such macros for a long time, and that enforcing these particular settings can cause operational issues. It can also be challenging to identify all the documents and VBA projects that need to be signed. We have decided at this time to move these settings into a separate GPO to make it easier to switch the settings on or off without affecting the rest of the baseline.

Note that the “[Block macros from running in Office files from the Internet](https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/?source=mmpc)” settings we [turned on in the previous baseline](https://blogs.technet.microsoft.com/secguide/2018/02/13/security-baseline-for-office-2016-and-office-365-proplus-apps-final/) are retained in the main GPOs and should be enforced by all security-conscious organizations.

Also see below about how the new Security Policy Advisor service can provide tailored recommendations for VBA macro policies.

**Other changes in the baseline**

“Block macros from running in Office files from the Internet” is now supported for Access, so we added it.

Implemented new settings to block the opening of certain untrusted files and to open others in Protected View.

Enabled the new “Macro Runtime Scan Scope” setting.

Removed the file block setting for “PowerPoint beta converters,” as Office no longer implements that block.

**Changes in the baseline since the draft release**

First, thanks to everyone who took the time to evaluate our draft baseline and provide us with feedback. Based on your feedback, we have made several minor adjustments to the baseline since publishing [the draft release](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/Security-baseline-for-Office-365-ProPlus-v1907-July-2019-DRAFT/ba-p/771308) in July:

* Changed several User Configuration settings from “Disabled” to Enabled with specific choices, as we have found that doing so is more effective at enforcing the desired policies:

|  |  |  |
| --- | --- | --- |
| **Path** | **Policy Name** | **New value** |
| Microsoft Office 2016\Security Settings | ActiveX Control Initialization | Enabled + 6 |
| Microsoft Office 2016\Security Settings | Load Controls in Forms3 | Enabled + 1 |
| Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security | Remove file extensions blocked as Level 1 | Enabled + empty list of extensions |
| Microsoft Outlook 2016\Security\Security Form Settings\Attachment Security | Remove file extensions blocked as Level 2 | Enabled + empty list of extensions |

* Removed the User Configuration setting, “Configure trusted add-ins” (in Microsoft Outlook 2016\Security\Security Form Settings\Programmatic Security\Trusted Add-ins) from the baseline, as we determined that it did not mitigate a contemporary security threat. In particular, the concept of “trusted” merely grants the COM add-in the ability to invoke Outlook Object Model interfaces without triggering user prompts. However, these add-ins can’t be installed without administrative privileges, and once installed they can also invoke more powerful Extended MAPI interfaces without triggering prompts.
* Removed the User Configuration setting, “Always open untrusted text-based files in Protected View” (in Microsoft Excel 2016\Excel Options\Security\Trust Center\Protected View) for the time being, as we discovered a bug in its implementation. We anticipate adding this policy control back into the baseline at a later time.
* Removed the User Configuration setting, “Excel 2007 and later binary workbooks” (in Microsoft Excel 2016\Excel Options\Security\Trust Center\File Block Settings) because it’s not needed to block legacy Excel file formats (unlike the similarly-titled Word policy) and it blocks use of the Personal Macro Workbook (personal.xlsb).

**Deploy policies from the cloud, and get tailored recommendations for specific security policies**

In addition to being able deploy these policies through Active Directory Group Policy or through Local Group Policy, you now have a new way to deploy user-based policies from the cloud to any Office 355 ProPlus client through the new Office cloud policy service.

The [Office cloud policy service](http://aka.ms/o365clientmgmt) allows administrators to define policies for Office 365 ProPlus and assign these policies to users via Azure Active Directory security groups. Once defined, policies are automatically enforced as users sign in and use Office 365 ProPlus. No need to be domain joined or MDM enrolled, and it works with corporate-owned devices or BYOD. To learn more about Office cloud policy service, check out the announcement here: <https://aka.ms/ocpsannouncement>.

We also have a new service called [Security Policy Advisor](https://aka.ms/spaannouncement) that can help you with deploying security policies. Security Policy Advisor can provide you with tailored recommendations for specific security policies based on how Office is used in your enterprise. For example, in most customer environments, macros are typically used in specific apps such as Excel and only by specific groups of users. Security Policy Advisor can help you identify groups of users and applications where macros can be disabled with minimal productivity impact, and optionally integrate with [Office 365 Advanced Threat P](https://docs.microsoft.com/en-us/office365/securitycompliance/office-365-atp)rotection to provide you information on who is being attacked. To learn more about Security Policy Advisor, check out the announcement here: <https://aka.ms/spaannouncement>.