

UNCLASSIFIED



MICROSOFT OFFICE 365 PROPLUS SECURITY TECHNICAL IMPLEMENTATION GUIDE (STIG) OVERVIEW

Version 2, Release 12

24 April 2024

Developed by Microsoft and DISA for the DOD

UNCLASSIFIED

Trademark Information

Names, products, and services referenced within this document may be the trade names, trademarks, or service marks of their respective owners. References to commercial vendors and their products or services are provided strictly as a convenience to our users, and do not constitute or imply endorsement by the Defense Information Systems Agency (DISA) of any nonfederal entity, event, product, service, or enterprise.

TABLE OF CONTENTS

	Page
1. INTRODUCTION.....	1
1.1 Executive Summary.....	1
1.2 Authority.....	1
1.3 Vulnerability Severity Category Code Definitions.....	1
1.4 STIG Distribution.....	2
1.5 Document Revisions.....	2
1.6 Other Considerations.....	2
1.7 Product Approval Disclaimer.....	3
2. OFFICE 365 PROPLUS BASELINE NOTES.....	4
3. ASSESSMENT CONSIDERATIONS.....	5
3.1 Manual Review.....	5
3.2 Other Considerations.....	6

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2

1. INTRODUCTION

1.1 Executive Summary

Office 365 ProPlus is the full version of Office that is installed on a user's local computer and runs locally. System requirements are similar to prior Office versions.

Office 365 ProPlus uses the Click-to-Run installation technology and by default installs as one package. However, it can be configured to exclude or remove certain Office 365 ProPlus products from client computers. Many of the same tools used to deploy and configure previous Office versions are used for Office 365 ProPlus.

The Microsoft Office 365 ProPlus Security Technical Implementation Guide (STIG) provides the technical security policies, requirements, and implementation details for applying security concepts to the Office 365 ProPlus application, as installed on a user's local computer. This document is intended to improve the security of Department of Defense (DOD) information systems.

Individual STIGs for each Office application program will not be created; instead, all requirements for all Office application programs will be included in this one STIG.

1.2 Authority

Department of Defense Instruction (DODI) 8500.01 requires that "all IT [information technology] that receives, processes, stores, displays, or transmits DOD information will be [...] configured [...] consistent with applicable DOD cybersecurity policies, standards, and architectures." The instruction tasks that DISA "develops and maintains control correlation identifiers (CCIs), security requirements guides (SRGs), security technical implementation guides (STIGs), and mobile code risk categories and usage guides that implement and are consistent with DOD cybersecurity policies, standards, architectures, security controls, and validation procedures, with the support of the NSA/CSS [National Security Agency/Central Security Service], using input from stakeholders, and using automation whenever possible." This document is provided under the authority of DODI 8500.01.

Although the use of the principles and guidelines in these SRGs/STIGs provides an environment that contributes to the security requirements of DOD systems, applicable NIST SP 800-53 cybersecurity controls must be applied to all systems and architectures based on the Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253.

1.3 Vulnerability Severity Category Code Definitions

Severity Category Codes (referred to as CAT) are a measure of vulnerabilities used to assess a facility or system security posture. Each security policy specified in this document is assigned a Severity Category Code of CAT I, II, or III.

Table 1-1: Vulnerability Severity Category Code Definitions

Category	DISA Category Code Guidelines
CAT I	Any vulnerability, the exploitation of which will directly and immediately result in loss of Confidentiality, Availability, or Integrity.
CAT II	Any vulnerability, the exploitation of which has a potential to result in loss of Confidentiality, Availability, or Integrity.
CAT III	Any vulnerability, the existence of which degrades measures to protect against loss of Confidentiality, Availability, or Integrity.

1.4 STIG Distribution

Parties within the DOD and federal government's computing environments can obtain the applicable STIG from the DOD Cyber Exchange website at <https://cyber.mil/>. This site contains the latest copies of STIGs, SRGs, and other related security information. Those without a Common Access Card (CAC) that has DOD Certificates can obtain the STIG from <https://public.cyber.mil/>.

1.5 Document Revisions

Comments or proposed revisions to this document should be sent via email to the following address: disa.stig_spt@mail.mil. DISA will coordinate all change requests with the relevant DOD organizations before inclusion in this document. Approved changes will be made in accordance with the DISA maintenance release schedule.

1.6 Other Considerations

DISA accepts no liability for the consequences of applying specific configuration settings made on the basis of the SRGs/STIGs. It must be noted that the configuration settings specified should be evaluated in a local, representative test environment before implementation in a production environment, especially within large user populations. The extensive variety of environments makes it impossible to test these configuration settings for all potential software configurations.

For some production environments, failure to test before implementation may lead to a loss of required functionality. Evaluating the risks and benefits to a system's particular circumstances and requirements is the system owner's responsibility. The evaluated risks resulting from not applying specified configuration settings must be approved by the responsible AO. Furthermore, DISA implies no warranty that the application of all specified configurations will make a system 100 percent secure.

Security guidance is provided for the DOD. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied at both the device hardening level and the architectural level due to the fact that some settings may not be configurable in environments outside the DOD architecture.

1.7 Product Approval Disclaimer

The existence of a STIG does not equate to DOD approval for the procurement or use of a product.

STIGs provide configurable operational security guidance for products being used by the DOD. STIGs, along with vendor confidential documentation, also provide a basis for assessing compliance with cybersecurity controls/control enhancements, which supports system assessment and authorization (A&A) under the DOD Risk Management Framework (RMF). Department of Defense AOs may request available vendor confidential documentation for a product that has a STIG for product evaluation and RMF purposes from disa.stig_spt@mail.mil. This documentation is not published for general access to protect the vendor's proprietary information.

AOs have the purview to determine product use/approval in accordance with (IAW) DOD policy and through RMF risk acceptance. Inputs into acquisition or pre-acquisition product selection include such processes as:

- National Information Assurance Partnership (NIAP) evaluation for National Security Systems (NSS) (<https://www.niap-ccevs.org/>) IAW CNSSP #11.
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<https://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DOD mandated standards.
- DOD Unified Capabilities (UC) Approved Products List (APL) (<https://www.disa.mil/network-services/ucco>) IAW DODI 8100.04.

2. OFFICE 365 PROPLUS BASELINE NOTES

This document and STIG represent the recommended security configuration baseline settings for Microsoft Office 365 ProPlus, version 1908. This Office 365 ProPlus STIG builds on the baseline released in early 2018 by Microsoft, as overhauled in June 2019.

Microsoft's updated baseline highlights comprehensive blocking of legacy file formats as well as blocking Excel from using Dynamic Data Exchange (DDE).

The Security Compliance Toolkit on Microsoft's website includes importable Group Policy Objects (GPOs), a script for applying GPOs to local security policies, a script to import GPOs into Active Directory, the recommended settings in a spreadsheet, and Office 365 ProPlus administrative templates.

This document is also intended to be used for Office 2019 installations. Networks without access to the Internet, such as labs and classified networks, will need to run Office 2019.

3. ASSESSMENT CONSIDERATIONS

This document is based on Microsoft Office 365 ProPlus on Windows 10 SAC. Microsoft Office 365 ProPlus system requirements can be found at <https://products.office.com/en-us/office-resources#coreui-heading-5dcqzx4>.

This document and associated STIG have set forth requirements based on having a secured Windows environment, for which requirements can be found in the appropriate Windows STIG. Failure to apply all these requirements will significantly diminish the value of the specifications in this document, as well as the overall security posture of the asset to which these settings apply.

The requirements set forth in this document are intended as a minimum setting. More restrictive settings may exist, and in such cases those settings would meet the intent of the STIG requirements in this document.

Security controls applied to the underlying operating system platform will directly affect the strength of the security that surrounds desktop application.

The security requirements detailed in this document target applications installed on the Microsoft Windows 10 platform only, using the traditional Windows installer-based (MSI) method of installing and updating Office.

3.1 Manual Review

To conduct a manual review of compliance with the Microsoft Office STIG requirements, it is necessary to use some tools that are provided with the Windows operating system. Some of these tools are as follows:

- Windows Explorer.
- Windows Registry Editor.
- Group Policy Object Editor.
- Microsoft Management Console (MMC).
- Microsoft Security Configuration and Analysis snap-in (used with MMC).

Registry paths and values identified in each control assume the use of Group Policy Object Editor in the Microsoft Management Console, with installation of the Microsoft Office 365 ProPlus Administrative Templates.

Installations not using Group Policies to administer Microsoft Office 365 Pro Plus products may observe alternate registry paths for stored configuration values. Instructions for the manual remediation of vulnerabilities, including adding, deleting, and modifying settings, can be found in the “Fix” information.

The policy path will be slightly different depending on the tool being used to check/generate the policy. If using the Group Policy Management console on a domain controller, the path is

Computer/User Configuration >> Policies >> Administrative Templates >> <path>. If using gpedit.msc on a non-DC system, the path is Computer >> User Configuration >> Administrative Templates >> <path>.

If only one application of the Microsoft Office suite is installed (i.e., Microsoft Office Word only or Microsoft Office Excel only), the Microsoft Office System STIG settings must also be applied, along with the STIG settings for the installed application.

Please note that Microsoft is using the Office 2016 Administrative Templates and related registry paths to configure Microsoft Office 365 ProPlus.

Because this STIG covers all Office application programs, any STIG requirement specifically for an application program the site has not installed on the client computer would be Not Applicable.

3.2 Other Considerations

The guidelines specified should be evaluated in a local, representative test environment before implementation within large user populations. The extensive variety of environments makes it impossible to test these guidelines for all potential software configurations. For some environments, failure to test before implementation may lead to a loss of required functionality.

It is especially important to fully test with specific and legacy applications that are dependent on the Microsoft Office applications for functionality, as well as Microsoft Office add-ins that are currently used in the environment.