

UNCLASSIFIED



**ADOBE ACROBAT READER DOCUMENT CLOUD (DC)
CONTINUOUS TRACK
SECURITY TECHNICAL IMPLEMENTATION GUIDE
(STIG) OVERVIEW**

Version 1, Release 6

26 July 2018

Developed by 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 DISA of any non-Federal 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	2
1.4 STIG Distribution.....	2
1.5 SRG Compliance Reporting.....	2
1.6 Document Revisions	2
1.7 Other Considerations.....	3
1.8 Product Approval Disclaimer.....	3
2. REFERENCE DOCUMENTS	4
3. CONCEPTS AND TERMINOLOGY CONVENTIONS	5
3.1 Operational View	5

LIST OF TABLES

	Page
Table 1-1: Vulnerability Severity Category Code Definitions	2
Table 2-1: Reference Documentation	4

1. INTRODUCTION

1.1 Executive Summary

Adobe Acrobat Reader DC incorporates capabilities other than just a PDF reader. Adobe Acrobat Reader DC incorporates an interface to Adobe's document cloud and Adobe's online services.

Adobe Acrobat Reader DC has two product tracks: Continuous and Classic. This STIG was written for the Continuous track.

- The Continuous track provides updates for new features, security and platform enhancements, and bug fixes when available in a silent update.
- The Classic track does not provide new features in the updates. Updates, security and platform enhancements, and bug fixes are only available on a quarterly basis.

There are two ways to verify which Adobe Acrobat Reader DC product track is installed:

- The Continuous track is installed by default on C:\\Program Files (x86)\\Adobe\\Acrobat Reader DC or navigate to Programs and Features >> Adobe Acrobat Reader DC.
- With the Classic track, the user has the option to install on any directory: <Drive Letter>:\\Program Files (x86)\\Adobe\\Acrobat Reader 2015 or navigate to Programs and Features >> Adobe Acrobat Reader MUI.

The Adobe Acrobat Reader DC Continuous Track STIG was written for the free version of Adobe Acrobat Reader DC and a default install.

The Adobe Acrobat Reader DC Continuous Track STIG was also written for a Windows environment and published as a tool to improve the security of Department of Defense (DoD) information systems. This document is meant for use in conjunction with the Windows Operating System (OS) STIG and any appropriate STIG(s) applicable to the system.

1.2 Authority

DoD Instruction (DoDI) 8500.01 requires that "all IT that receives, processes, stores, displays, or transmits DoD information will be [...] configured [...] consistent with applicable DoD cybersecurity policies, standards, and architectures" and tasks that Defense Information Systems Agency (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, 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 need to 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

	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 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 SRG Compliance Reporting

All technical NIST SP 800-53 requirements were considered while developing this STIG. Requirements that are applicable and configurable will be included in the final STIG. A report marked For Official Use Only (FOUO) will be available for those items that did not meet requirements. This report will be available to component Authorizing Official (AO) personnel for risk assessment purposes by request via email to: disa.stig_spt@mail.mil.

1.6 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.

1.7 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 Authorizing Official. 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 Department of Defense. While other agencies and organizations are free to use it, care must be given to ensure that all applicable security guidance is applied both at the device hardening level as well as the architectural level due to the fact that some of the settings may not be able to be configured in environments outside the DoD architecture.

1.8 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). DoD Authorizing Officials (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 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) (<http://www.niap-ccevs.org/>) IAW CNSSP #11
- National Institute of Standards and Technology (NIST) Cryptographic Module Validation Program (CMVP) (<http://csrc.nist.gov/groups/STM/cmvp/>) IAW Federal/DoD mandated standards
- DoD Unified Capabilities (UC) Approved Products List (APL) (<http://www.disa.mil/network-services/ucco>) IAW DoDI 8100.04

2. REFERENCE DOCUMENTS

The following table enumerates the documents and resources referenced:

Table 2-1: Reference Documentation

Document Description	Source
Application Security Overview	https://www.adobe.com/devnet-docs/acrobatetk/tools/AppSec/index.html
Enterprise Administration Guide	https://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/index.html
Online features	https://www.adobe.com/devnet-docs/acrobatetk/tools/Wizard/WizardDC/online.html
Adobe Unveils New Acrobat “DC” (ver. 12) – with Document Cloud	http://prodesigntools.com/adobe-acrobat-dc-document-cloud.html
Acrobat Customization Wizard DC	https://www.adobe.com/devnet-docs/acrobatetk/tools/Wizard/WizardDC/
Adobe Acrobat DC Document Cloud Product Tracks	http://www.adobe.com/devnet-docs/acrobatetk/tools/AdminGuide/whatsnewdc.html#reader-dc-tracks

3. CONCEPTS AND TERMINOLOGY CONVENTIONS

3.1 Operational View

Adobe Acrobat Reader DC is free software that can be used for viewing and printing PDF documents. Adobe Acrobat Reader DC is the successor to Adobe Reader 11. Unlike the older versions of Adobe Acrobat Reader, Adobe Acrobat Reader DC is more than just PDF reader software.

Adobe Acrobat Reader DC incorporates Adobe's cloud services and online tools. This introduces a potential security risk or attack to the DoD infrastructure. Users within the DoD are restricted access to non-DoD resources.

The default install for Adobe Acrobat Reader DC installs all the Adobe Acrobat Document Cloud Service components. Adobe does provide a free automation tool, Acrobat Customization Wizard DC, that can be used to automate and streamline the task of configuring (customizing) the installer prior to deployment. Components are enabled or disabled based on the loaded installer file. A custom install could be configured to disable and lock features that use Adobe's Document Cloud. The Acrobat Customization Wizard DC can be used for the free version of Adobe Acrobat Reader DC. Per Adobe, Adobe does not support users in customizing the wizard for the free version of Adobe Acrobat Reader DC. Adobe does support licensed versions and will assist in customizing an install.